



MyQ Advanced User Management Guide

REVISION 2

Table Of Content

1. Basic Information	1
1.1. About this Guide	1
2. User Import and Synchronization	2
2.1. How does the user synchronization work?	2
User properties in MyQ	3
User synchronization options	4
2.2. User synchronization from LDAP servers	5
2.2.1. Creating an LDAP synchronization	6
2.2.2. Setting up the LDAP synchronization	7
1) General tab: Creating the synchronization	7
2) Users tab: Selecting base DN, assigning attributes and additional settings ..	9
3) Groups tab: Importing groups	12
2.3. User synchronization from CSV files	17
2.3.1. Creating new CSV synchronization	17
2.3.2. CSV synchronization setup options	18
2.3.3. Syntax of the CSV file	20
2.4. Manual and scheduled run of synchronizations	23
Manually running a synchronization	23
Scheduled run of the synchronization	23
2.5. User synchronization from Azure Active Directory	24
3. Detecting job owners	26
3.1. Identifying the job owner with the computer name	27
3.2. Using a DNS server to resolve the job owner	27

3.3. Detecting the job owner from the job name	28
3.3.1. Additional settings	29
3.4. Detecting the job owner from the job's PJI header	30
3.5. Enabling case sensitivity for the job owner detection in MyQ	31
3.6. Using Regular expressions	31
4. ID Card Transformation	32
4.1. Entering the transformation	33
4.2. Defining the transformation	33
Table of commands:	34
5. Using External Authentication Servers for Authentication in MyQ	38
5.1. Registering authentication servers in MyQ	38
5.2. Setting the external user authentication option	40
Automatically selecting the external authentication option	40
Manually selecting the external authentication option	42
6. MyQ Smart Job Manager: Advanced Setup	43
7. Appendix: Overview of Changes	44
Revision 2	44
Changes in topics	44
8. Business contact	45

1. Basic Information

1.1. About this Guide

This document provides its readers with information about the advanced features and settings of user accounts in MyQ. It contains detailed information about features that are already introduced in the Basic Installation Guide: user import and synchronization from LDAP servers, detecting job owners and external authentication. Furthermore, it introduces several advanced options of user administration: user import and synchronization from CSV files, ID card transformation, using regular expressions for detection of job owners and advanced setup of the MyQ Smart Manager.

The basic setup of MyQ and the general terms describing the system are described in the MyQ Basic Installation Guide. To fully understand the following topics, we recommend you to read the Basic Installation Guide first.

2. User Import and Synchronization

User synchronization is a method of synchronizing the user related data in the MyQ database with the data in external sources, such as LDAP servers or CSV files. Importing new users is an optional part of the synchronization process. In settings of a synchronization, you can activate or deactivate the import of new users; if you deactivate it, MyQ only updates accounts of the users that already are in its database.

This topic provides detailed information about the synchronization from the external sources. It fully describes two methods of import and synchronization available in MyQ and presents two options of running the synchronizations:

- [User synchronization from LDAP servers](#)
- [User synchronization from CSV files](#)
- [Manual and scheduled run of synchronizations](#)

Furthermore, it shows you how to set up user synchronization from Azure Active Directory:

- [User synchronization from Azure Active Directory](#)

2.1. How does the user synchronization work?

First, you need to add the new synchronization source. Overall, there are four possible types of synchronization sources: LDAP server, CSV file, MyQ Master server and Custom script, but in this topic, we will discuss only the first two types. The synchronization from the Master server is used on the Master/Server architecture installations of MyQ and is explained in the guide **Managing MyQ on Multiple Servers - Master and Site Architecture Guide**. The synchronization from the custom script is used only in very specific cases; for information about this option, please contact your MyQ support.

As soon as you add the synchronization source, MyQ opens its properties panel where you can set up the synchronization. Although they differ in their sources, all synchronizations have one thing in common, their goal is to adequately synchronize the user data in the source with the user data in MyQ.

An important part of the synchronization setup is pairing user attributes in the synchronization source with their counterparts in MyQ. This can be done by setting the corresponding properties in the **Properties** section of the **Users** tab of the **LDAP synchronization** settings tab or by defining the corresponding fields in the CSV file.

Apart from that, you might want to select some additional options, such as adding new users, deactivating users that are not in the synchronization source, or converting user names to lowercases. These options can be selected in the **Options** section of the **Users** subtab of the **LDAP synchronization** settings tab or on the properties panel of the CSV synchronization.

Also, you can import groups of users or even whole group tree structures. This can be done by setting the groups on the **Groups** subtab of the **LDAP synchronization** settings tab or by defining the groups inside the CSV synchronization file.

The following two sections describe the user properties and synchronization options:

User properties in MyQ


- **User name** — Name of the user account in MyQ, in Active directory and Open LDAP, this property corresponds to the **samaccountname** user attribute on the LDAP server.
- **Full name** — MyQ Advanced User Management Guide this is the full name of the user, in Active directory and Open LDAP, this property corresponds to the **cn** user attribute on the LDAP server. Usually, it is the given name and the surname of the user.
- **Alias** — In addition to their user name, each user can have a number of aliases. MyQ treats the aliases as alternative user names. You can use aliases for example if you need to enable one user to send jobs to MyQ from different OS accounts.
- **Card** — Number of the user identification card. It can be either imported from LDAP or added to MyQ on the properties panel of the user. Also, it can be registered by an administrator on a card reader connected to PC USB slot or registered by the user on an embedded terminal.
- **PIN:** MyQ personal identification number is used for access to MyQ Web Interface and MyQ terminals.
- **Personal number** — The personal number can be used as the user ID in MyQ. The primary ID is the **user name** property. If you select the **Pair by the personal number** property during the user synchronization, the personal number is used instead.
- **Email** — Primary email of the user.
- **Notes** — You can use this text box to enter additional notes concerning the user.

- **Language** — Language used on the user's MyQ Web Interface and their home screen on the embedded terminal.
- **User's scan storage** — You can select a folder or one or more emails where MyQ sends scans of the user. Depending on the scanning setup, scans can be sent here, to the user primary email set in the **Email** property text box, or to other sources defined in MyQ or entered by the scanning users.

User synchronization options

- **Deactivate missing users** — If you select this option, MyQ deletes users that are imported from the current synchronization source and that are not in the source anymore. To delete users that were added from different sources, select the **Ignore synchronization** source option together with this option.
- **Add new users** — If you select this option, MyQ adds new users from the current synchronization source. If you do not select it, MyQ updates accounts of the users who are already in MyQ, but do not add any new users.
- **Convert user name to lowercase** — Unlike some other systems that do not differ between two words with the same letters but different cases (such as "Pear", "pear"), MyQ is case sensitive. You can use the **Convert user name to lowercase** option to prevent creating multiple accounts for one user.
- **Use authentication server** — If you select this option and a user logs in by entering their username and password, the credentials are not authenticated against MyQ database, but instead against an LDAP or Radius server. If you synchronize users with LDAP, the source LDAP server is automatically assigned as the authentication server. If you synchronize users with CSV, you can select the authentication server from the list of predefined authentication servers.
- **Pair by the personal number** — If you select this option, MyQ identifies users by their personal number instead of their user names. This way you can keep track of a single user with different names in different sources or a user whose name has changed for some reason. For example, if this option is activated and a username in LDAP changes from cat.stevens to yusuf.islam, MyQ does not create a new user account, but recognizes the old user by his personal number.

- **Ignore synchronization source** — If this option is not selected, MyQ recognizes two users from different synchronization sources as two different entities. This can cause conflicts during synchronizations from multiple sources. If it is selected, MyQ ignores the synchronization sources and treats all users the same, regardless of their synchronization source. For example, if you run a synchronization and MyQ would import/update a user that has been already added from a different synchronization source, it does not update the user. Instead, it shows the message **"The name/alias "X" is already used by the user "X"** among the synchronization results. After you select the **Ignore synchronization source** option, the user is updated by the latest synchronization.


 **WARNING:** If you select this option together with the **Deactivate missing users** option, all users that were added from different sources and are not in the current synchronization source are deleted during the synchronization.

- **Append the domain name to the username (username@domain.local)** — With this option selected, the name of the domain can be retrieved from the MyQ username. The information about the domain can be needed for example when scanning to users' home folders is used on an embedded terminal. (For more information about this feature on a particular embedded terminal, see the embedded terminal's MyQ manual.)

2.2. User synchronization from LDAP servers

LDAP server contains a database that stores all user accounts, passwords and other user related data of an organization. On the LDAP Synchronization settings tab on the MyQ Web Interface, you can synchronize users directly from the server database.

MyQ can communicate with as much as five LDAP servers at the same time (with the BusinessPro license). It supports Active Directory, OpenLDAP, Novell and Lotus Domino. To synchronize the users, you need to add the synchronization source first and then setup the synchronization. After the synchronization is set up, you can either run it manually on the **User Synchronization** settings tab or set it as a regular task on the **Task Scheduler** settings tab.

 **WARNING:** All settings described in this section apply only to Active Directory, although the settings for OpenLDAP, Novel and Lotus Domino are similar.

2.2.1. Creating an LDAP synchronization

NOTICE: Before creating the synchronization, you have to add the LDAP server to MyQ. This can be done on the **Network** settings tab, under **Authentication servers**. For information about how to add LDAP servers, see "Authentication servers" under "MyQ® System Settings" in the Basic Installation Guide.

To create a new LDAP synchronization

1) Add the new synchronization

- I. On the **User synchronization** settings tab, click **+Add Sync source**. A drop-down box appears.

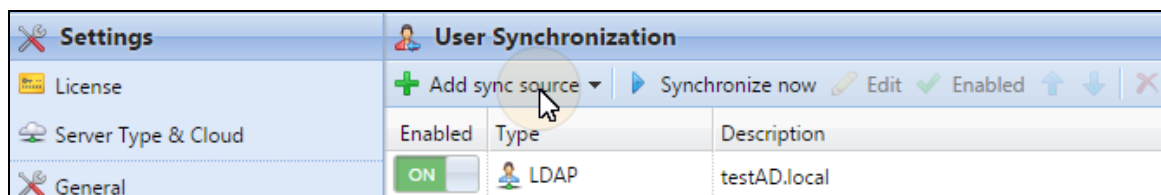


FIGURE 2.1. Adding new synchronization source on the **User Synchronization** settings tab

- II. In the drop-box, click **+Add LDAP source**. The **LDAP synchronization** properties panel opens. On the panel, you can set up the synchronization.

2) Set up the synchronization on the LDAP synchronization properties panel

- Set up the synchronization on three tabs on the **LDAP synchronization** properties panel. On each of the tabs, click **Save** after changing the settings. For information about the synchronization setup, see "Setting up the LDAP synchronization" on the next page.

INFO: The synchronization is created when you save the settings on the **General** tab of the **LDAP synchronization** properties panel.

3) Return to the User synchronization settings tab

- The new LDAP synchronization is displayed on the list of synchronizations on the **User synchronization** settings tab.

2.2.2. Setting up the LDAP synchronization

The setup consists of three parts: creating the synchronization on the **General** tab, setting import of users on the **Users** tab and setting import of groups on the **Groups** tab. You can swap between these tabs on the bar at the upper-left corner of the **LDAP synchronization** properties panel.

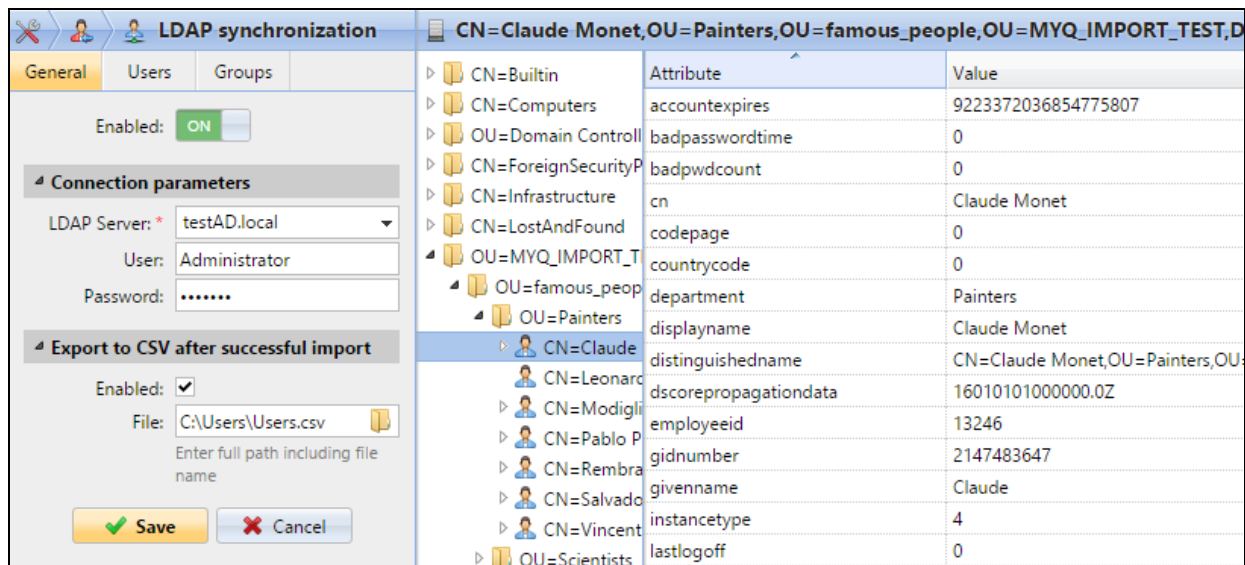


FIGURE 2.2. LDAP synchronization properties panel with the LDAP database browser to its right side.

For detailed description of the LDAP synchronization setup and its options, see the three following sections: "1) General tab: Creating the synchronization" below, "2) Users tab: Selecting base DN, assigning attributes and additional settings" on page 9 and "3) Groups tab: Importing groups" on page 12.

1) General tab: Creating the synchronization

On the **General** tab, set the general properties of the synchronization: enable or disable the synchronization, select the LDAP server domain, enter user name and password for access to the server, eventually select to export the imported users to a CSV file. See the list below for description of individual settings.

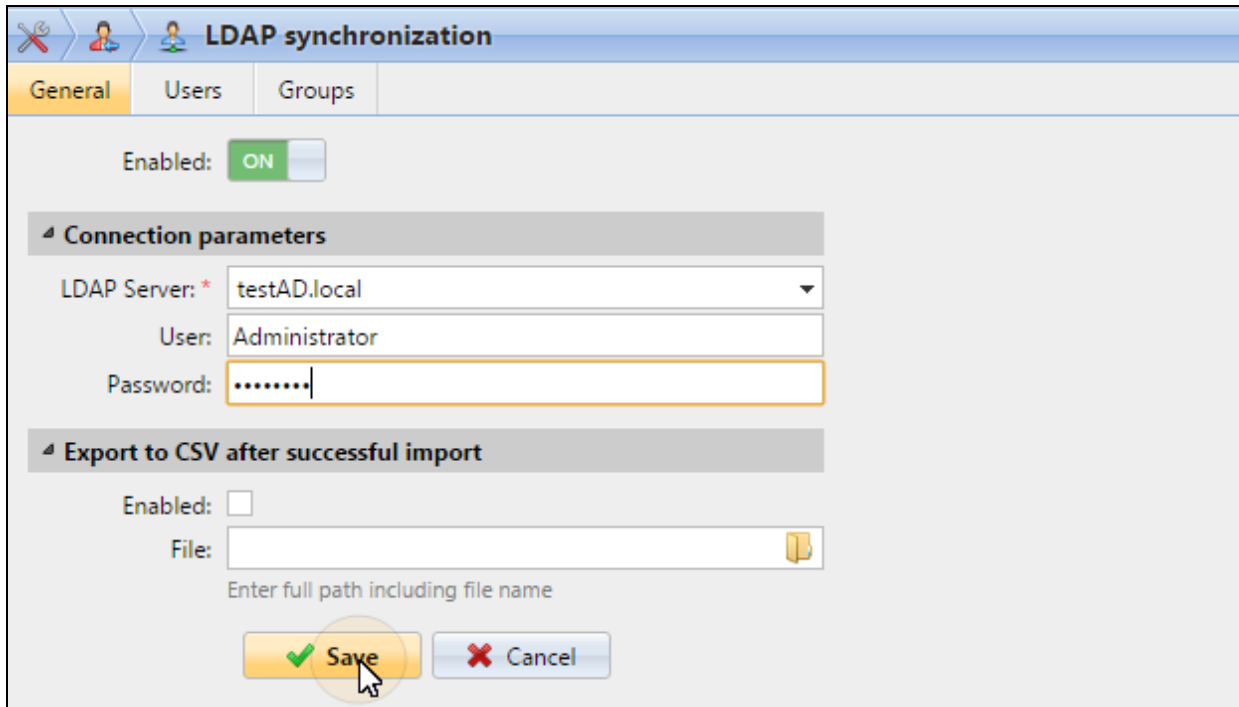


FIGURE 2.3. Saving the settings on the **General** tab

Enabled — Here you can enable or disable the synchronization.

Connection parameters:

LDAP Server — Here you can select the domain from which you want to synchronize.

User — Enter user name for access to the LDAP domain server here.

Password — Enter password for access to the LDAP domain server here.

Export to CSV after successful import:

Enabled — If you enable this option, MyQ creates a CSV file with the imported users after the synchronization.

File — Select the folder where you want to save the created file.

INFO: After you correctly set the connection parameters (LDAP server, username and password) and save the settings, the LDAP browser opens on the right side of screen.

2) Users tab: Selecting base DN, assigning attributes and additional settings

On the **Users** tab, pick one or more base DNs from which you import the users. In addition, you can assign user attributes from the LDAP server to user properties in MyQ and select additional options concerning the synchronization.

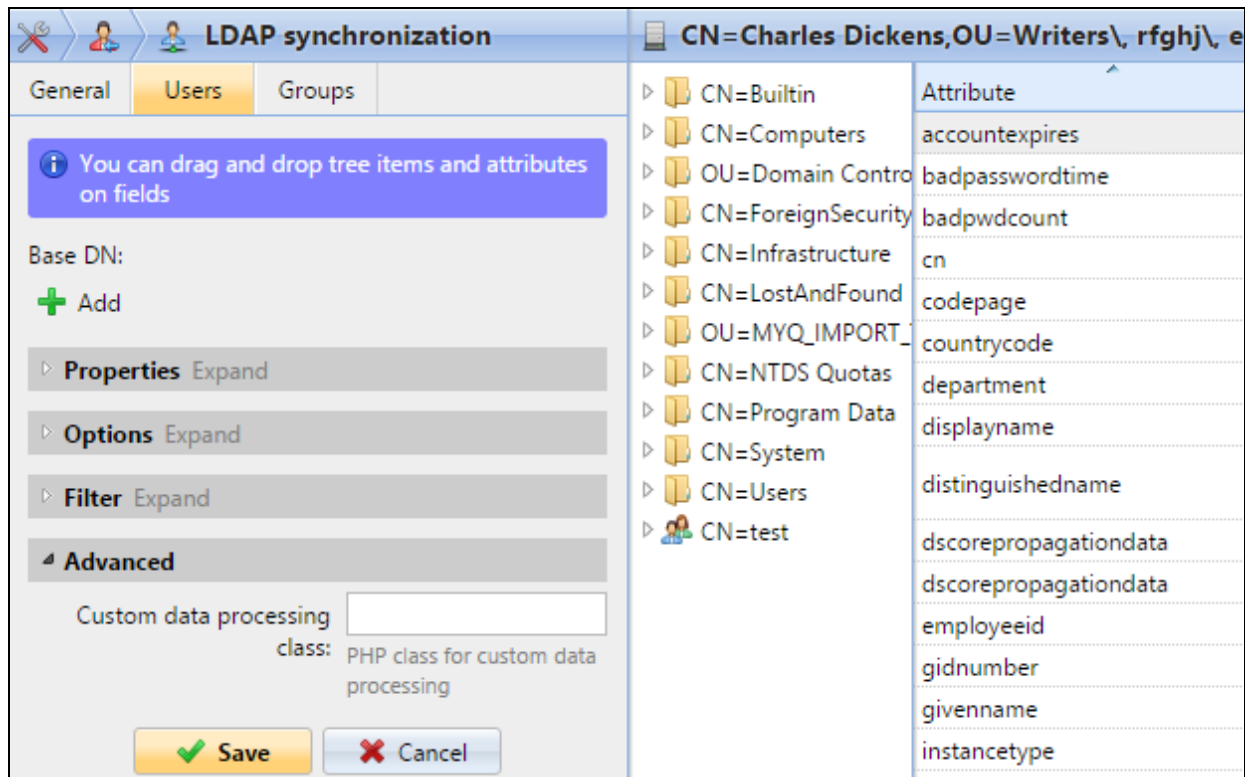


FIGURE 2.4. The **Users** tab on the LDAP synchronization properties panel

The users import options are described in the list starting on the next page.

INFO: During the setup, you can use the **drag and drop** feature to move items and attributes from the LDAP browser to corresponding text boxes on the tab on the left.

Base DN — Here you can pick the base domain or domains from which you import users.

Click **+Add** to add a text box for the new base DN, and then drag a group from the database browser and drop it in the text box. You can add multiple domains this way.

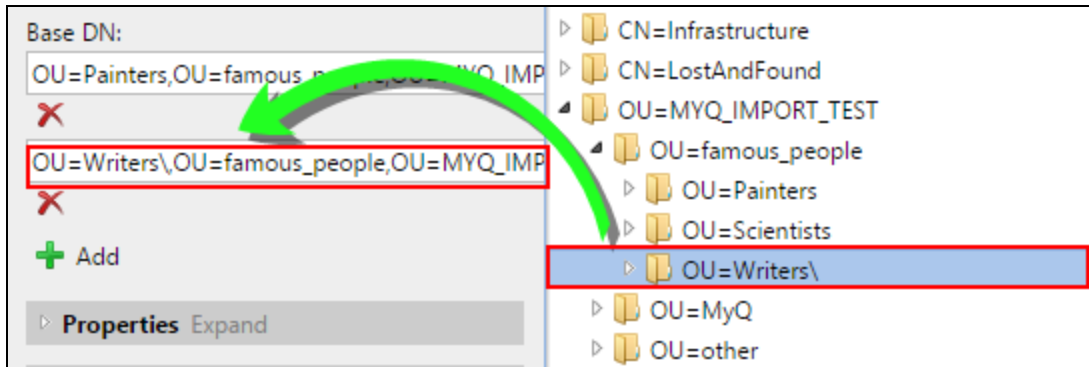


FIGURE 2.5. Dragging and dropping a domain

Properties:

These are properties of every individual user. MyQ will automatically find and assign the user's **SAM account name** to **user name**, **cn** to **full name** and **mail** to **email** (this applies to Active directory and Open LDAP only). The user name property is the only one that cannot be changed.

To assign an attribute to a property, write the name of the attribute in the property text box or drag the attribute from the attributes of any individual user and drop it in the text box.

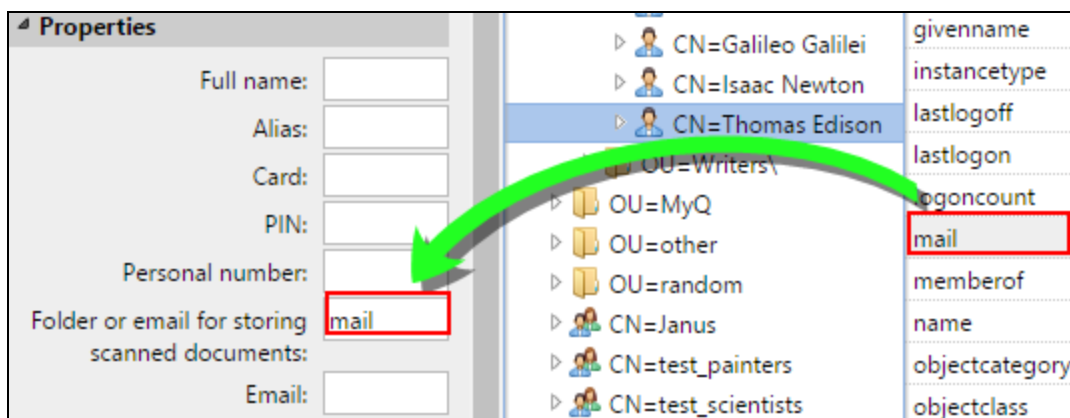


FIGURE 2.6. Dragging and dropping an attribute

For assigning default languages of users, you have to use an attribute from the LDAP server which has abbreviations of languages as its values. For example, you can create and use an attribute called **lang** with values **en** for English, **hr** for Croatian etc. The list of the abbreviations used in MyQ can be found in the Basic Installation Guide in "Appendix II — List of available languages and their abbreviations".

Options: For description of the common synchronization options, see "User synchronization options" on page 4.

In addition to the basic options that are common for both the synchronization from LDAP servers and for synchronization from CSV files, there is one specific option that belongs only to the import from LDAP servers: **append the domain name to the username (username@domain.local)**. This option enables you to save the information about the LDAP server in the user name. For more information about this option, contact your MyQ support.

Filter — You can filter the import of users by specifying values of attributes. Add the conditions in form:

Attribute=Value. Users with different value of this attribute are not accepted and are filtered out of the import.

You can use the * symbol to search for substrings. The symbol can be appended from both sides. For example, if you add a cn=*in* condition, only users whose common name attribute contains "in" are accepted.

Add one condition per one row. Users are accepted if they satisfy at least one condition.

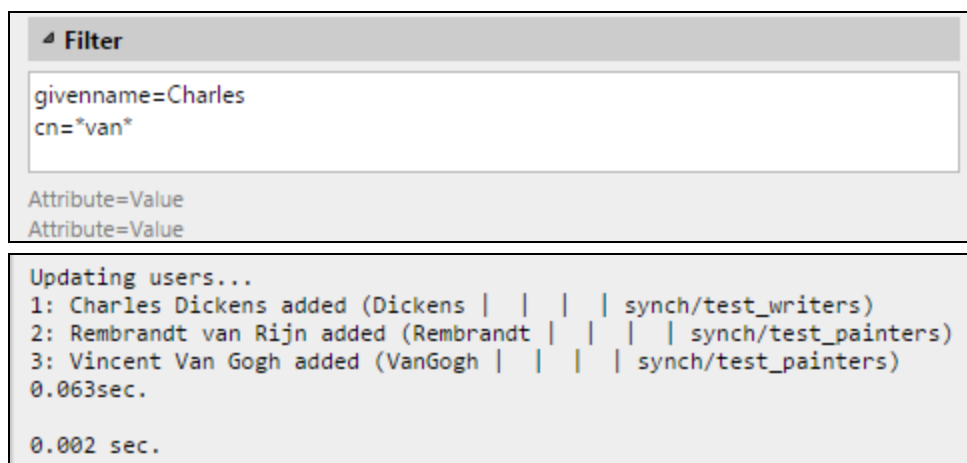


FIGURE 2.7. Example of a filter and the resulting synchronization

Advanced:

Custom data processing class — For further information about this option, contact your MyQ support.

⚠ NOTICE: After you change the settings, click **Save** to submit the changes.

3) Groups tab: Importing groups

On this tab, you can import groups and the group structure from the LDAP source. There are four different methods of specifying which groups are imported. You can use multiple different methods together and by each method, you can create different groups of users. You can also select to import the groups under an existing group in MyQ.

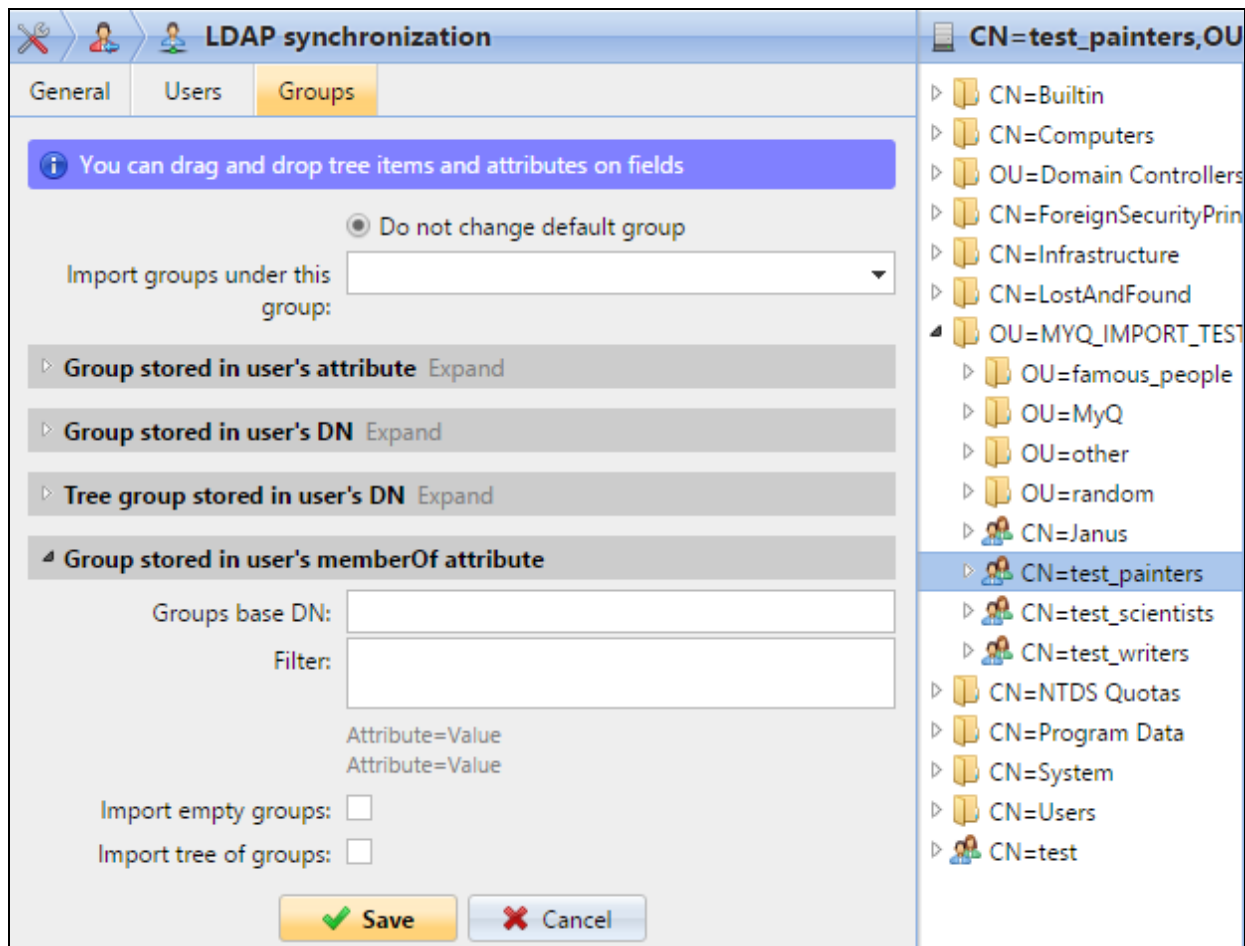


FIGURE 2.8. The **Groups** tab on the LDAP synchronization properties panel

The groups import options are described in the list starting on the next page.

Do not change default group — A user can be member of multiple groups but all their prints, copies and scans are accounted to only one group: the **Default group** of the user.

If you select this option, the default group of the selected user does not change during the synchronization.

Import groups under this group — You can select an existing group in MyQ under which you import the groups from the LDAP database.

Groups stored in user's attribute:

Attribute — You can select this option if you want to use an attribute that defines groups in the LDAP database.

To add the attribute, type the name of the attribute in the property text box or drag the attribute from the attributes of any individual user and drop it in the **Attribute** text box.

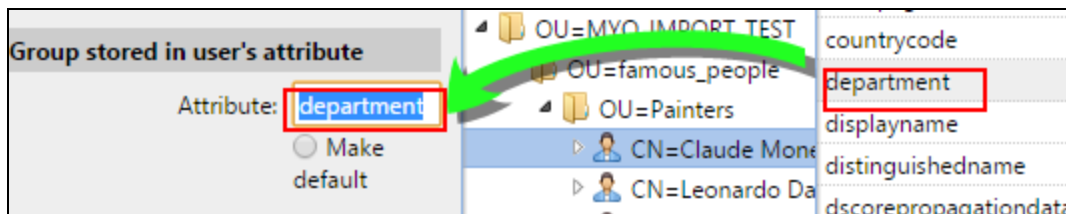


FIGURE 2.9. Dragging and dropping an attribute

You can also create groups by combining multiple attributes. To create such group, put each of the attributes between two percentage signs (%). For example, the combination of attributes **%attribute1%_%attribute 2%** , imports a new group named **value1_value2**.

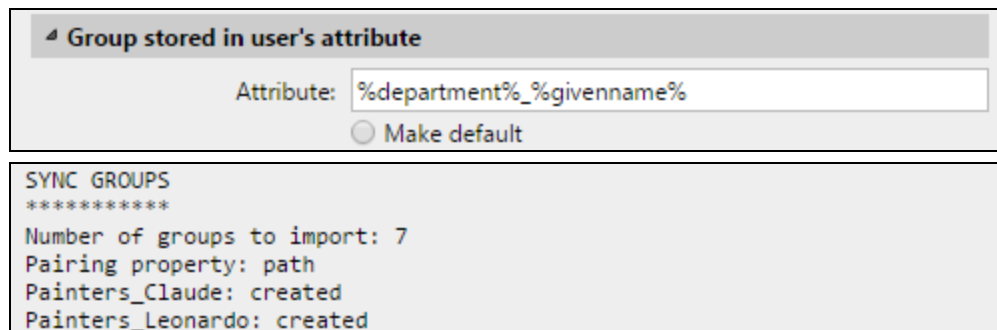


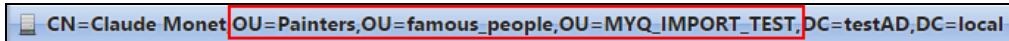
FIGURE 2.10. Example of a combined attribute group definition and the resulting synchronization

Furthermore, you can create tree structures of groups by separating the attributes with vertical bars. For example, the combination of attributes **%attribute1|%attribute 2%**, imports a group attribute1, and its sub-group **attribute 2**.

Make default — If you select this option, the group becomes the default group of the imported user.

Group stored in user's DN:

OU component index — Here you can select a group by its OU (organizational units) index among the DN components. The index is counted from right to left — the first OU group from right has index 1, the second from right has index 2 and so on.



CN=Claude Monet,OU=Painters,OU=famous_people,OU=MYQ_IMPORT_TEST,DC=testAD,DC=local

FIGURE 2.11. DN Components with three OU groups (Painters, famous_people and MYQ_IMPORT_TEST)

On the picture above, there are three OU groups: **MYQ_IMPORT_TEST** has index 1 (as it is the first OU group from right), **famous_people** has index 2 and **Painters** has index 3. The other components are not OU and therefore have no index.

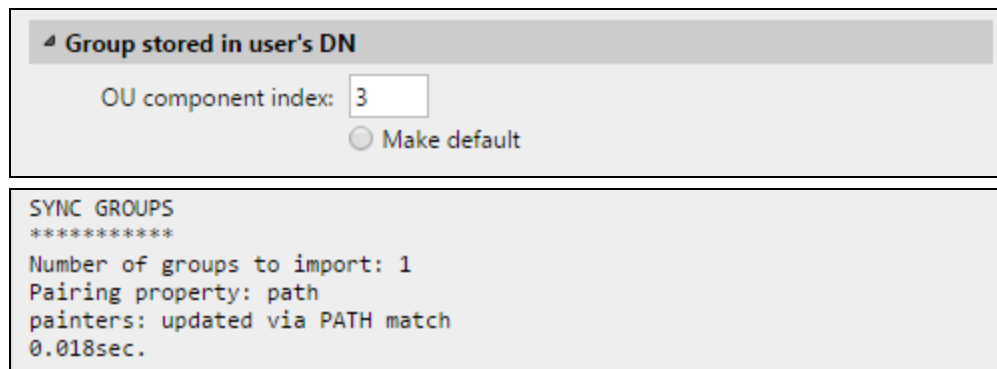


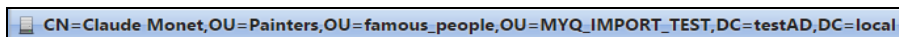
FIGURE 2.12. Example of an import of a group stored in user's DN

Make default — If you select this option, the group becomes the default group of the imported user.

Tree group stored in user's DN:

Here you can import the whole tree structure of groups. You can restrict the import to any part of the structure by stripping the DN components from left and from right. In the respective text boxes, enter the amount of components to be striped from left and from right side.

You have to strip at least one component from left (the user CN component) and one component from right (the right-most DC component).



CN=Claude Monet,OU=Painters,OU=famous_people,OU=MYQ_IMPORT_TEST,DC=testAD,DC=local

FIGURE 2.13. DN Components

On the picture above, there are six components. If you strip one component from left and one from right, you import the following structure of groups: **testAD > MYQ_IMPORT_TEST > famous_people > Painters**.

By stripping components from left, you remove the groups from bottom to top of the structure. By stripping components from right, you remove the groups from top to bottom of the structure.

Make default — If you select this option, the bottom group of the imported structure becomes the default group of the imported user.

Group stored in user's memberOf attribute:

Group base DN — MyQ can import security and distribution groups stored in the user's **memberOf** attribute. The security groups are used to define access permissions granted to their members. Distribution groups can be used for sending emails to a group of users.

To specify which groups should be taken in consideration during the import, you have to insert the groups base DN. MyQ import only groups that are included in the base DN, other groups stored in the **memberOf** attribute are ignored. The group base DN does not have to be the same organizational unit as the users base domain.

If a user is member of more than one group on the LDAP server, all the groups are stored in the **memberOf** attribute. Therefore, the **Make default** option, which requires a single value, is not available for this method of import.

To add the groups base DN, drag it from the database browser and drop it in the **Group base DN** text box.

Filter — You can filter this import by specifying values of attributes. Add the conditions in form: Attribute=Value. Groups with different value of this attribute are not accepted and are filtered out of the import. You can use the * symbol to search for substrings. The symbol can be appended from both sides. For example, if you add a **cn=*in*** condition, only users whose common name attribute contains "in" are accepted. >Add one condition per one raw. Groups are accepted if they satisfy at least one condition.

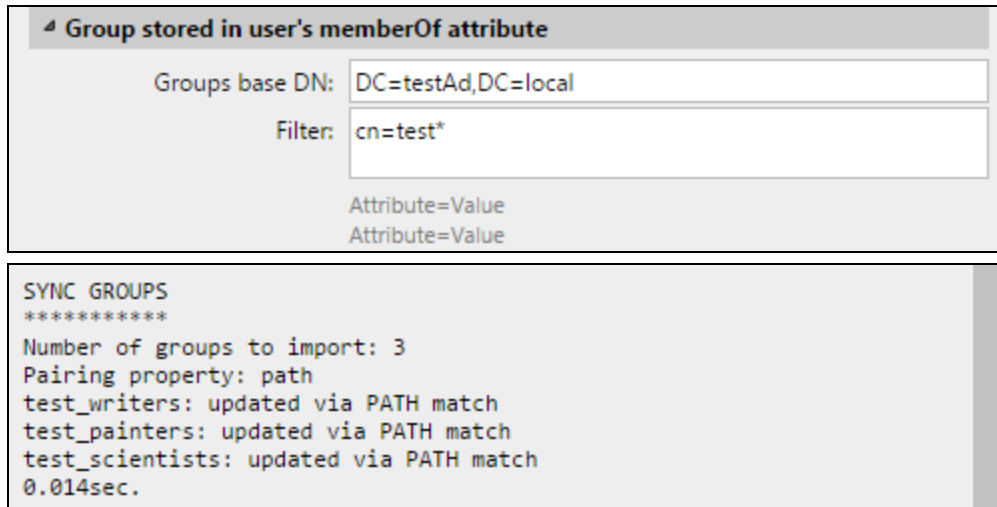


FIGURE 2.14. Example of an import of groups stored in memberattribute with the **cn=test*** filter applied

Import empty groups — If you select this option, groups from the Group base DN are imported even if there is no user having them in their memberOf attribute.

Import tree of groups — If you select this option, the whole tree structure is imported. Otherwise all groups are added separately; not as a part of a tree structure.

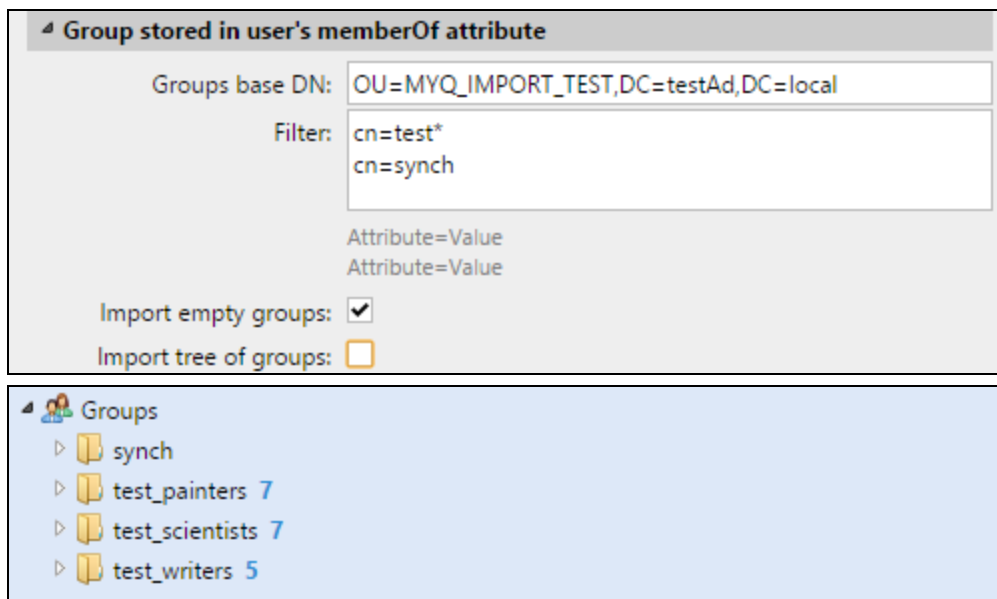


FIGURE 2.15. Import of groups stored in memberOf attribute with the **Import tree of groups** option deselected

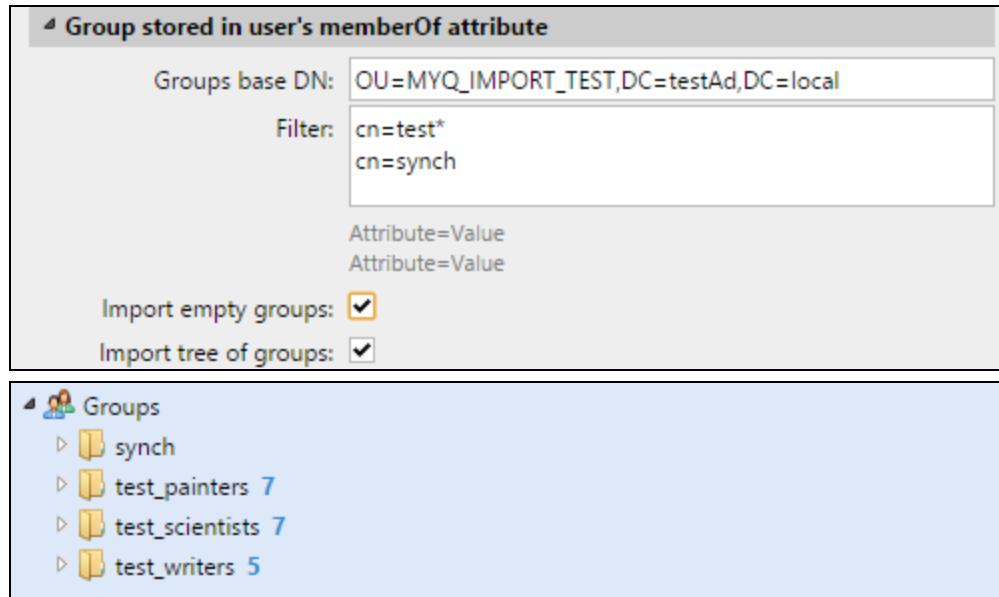


FIGURE 2.16. Import of groups stored in memberOf attribute with the **Import tree of groups** option selected

2.3. User synchronization from CSV files

Another method of storing user data is saving the data in CSV files. Each line of the file corresponds to one user and each field corresponds to one property of the user. To synchronize users from the CSV file, you have to create a new CSV synchronization on the **User Synchronization** settings tab and on the synchronization properties panel, add the source file and set properties of the synchronization.

After the synchronization is set up, you can either manually run it on the **User Synchronization** settings tab or set it as a regular task on the **Task Scheduler** settings tab.

2.3.1. Creating new CSV synchronization

To create a new synchronization, do the following:

1) Open the new synchronization

- On the bar at the top of the **User synchronization** setting tab, click **+Add Sync source**, and then click **+Add CSV source**. The **CSV synchronization** properties panel appears on the right side of screen.

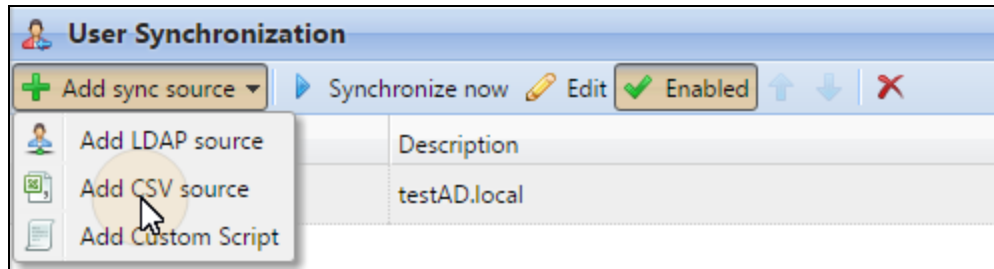


FIGURE 2.17. Adding new synchronization source on the **User Synchronization** settings tab

2) Set up the synchronization

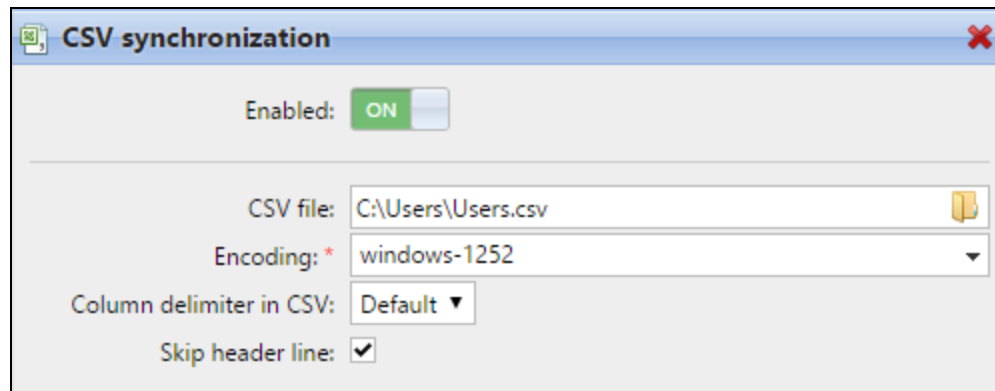


FIGURE 2.18. The **CSV synchronization** properties panel

- On the **CSV synchronization** properties panel, set the path to the CSV file and configure the synchronization. For information about the synchronization options, see "CSV synchronization setup options" below.

3) Save the setup

2.3.2. CSV synchronization setup options

These are the options of the CSV synchronization:

Enabled — Here you can enable or disable the synchronization.

CSV file — Here you can set the path to the CSV file on the MyQ server.

Encoding — Select the encoding that is used in the CSV file. The default value depends on the OS settings of the computer on which you access the MyQ Web Interface.

Column delimiter in CSV — Select the delimiter that is used in the CSV file.

If you select the **Default** option, MyQ scans for the delimiter set on the **Column delimiter in CSV** drop-down list box on the **General** settings tab. For more information about the general settings, see "General" under "General settings tab" in the Basic Installation Guide.

Skip header line — In case the CSV file contain a header line, you need to select this option and skip the first line of the file during the synchronization. All lists of users exported from MyQ contain the header line.

Import under MyQ group — Here you can select an existing group in MyQ under which you import the groups from the CSV file.

Synchronization source — Here you can specify a different source than the CSV to be marked as the synchronization source by the MyQ system. For example, you can insert an LDAP server domain.

Ignore synchronization source — If you select this option together with the **Deactivate missing users** option, all users that are not in the current synchronization source are deleted.

Use authentication server — If you select this option, an LDAP or Radius server is used for authentication of the imported users.

Select the domain for the authentication on the setting below.

Authentication server — Here you can select the LDAP or Radius domain for the user authentication.

Deactivate missing users — If you select this option, MyQ deletes users that are imported from the current synchronization source and that are not in the source anymore.

To delete users that were added from different sources, select the **Ignore synchronization source** option together with this option.

Add new users — If you select this option, MyQ adds new users from the current synchronization source.

Pair users by personal number — If you select this option, multiple accounts with a single personal number are paired.

Convert user name to lowercase — If you select this option, all letters in user names are converted to lowercase.

Cards / PIN / Groups — In each of the three drop-down boxes, you can select from these synchronization options for the respective parameter (CARDS, PINS, GROUPS):

- Do not synchronize: Value of the respective parameter in MyQ is not changed.
- Full synchronization: Value of the respective parameter in MyQ is always replaced by the value in the CSV file. If the value in the source file is empty, the value in MyQ is erased.
- Synchronize if not empty: If the respective field in the CSV file is not empty, the parameter value in MyQ is replaced by the value in the CSV file. Otherwise, the parameter value remains unchanged. **This is the default setting.**
- Add new: If the parameter is already set in MyQ, it is not replaced. Only new values are added.

2.3.3. Syntax of the CSV file

```
"FULLNAME"; "USERNAME_ALIASES"; "EMAIL"; "CARDS"; "GROUPS"; "CODE";  
"SCANSTORAGE"; "PIN"; "MANAGED_GROUPS"; "AUTHSERVER"; "PHONE";  
"LANG"; "PWD"; "EXTID"; "DELEGATES"  
"Thomas Pinapple"; "Tom, Tomy, Apple"; "t.pinapple@domain.com";  
7E9700C9; "Imported Users, Activities|Outdoors|Swimming,  
Activities|Outdoors|Birdwatching"; 22212; "\\Users\Tomy";  
14BFA6BB14875E4; Birdwatching; testAD.local; 080008020; en;  
ldapAuth;; "Carol, Kohei, Eliot";
```

FIGURE 2.19. CSV file opened in a text editor

In the list below, you can find information about individual fields of the CSV file.

NOTICE: A single word or a plain number can be put in the CSV fields as they are, while more complex strings, such as full name or email address, have to be bounded by quotes.

FULLNAME — Name of the user in double quotation marks, for example "**Thomas Pinapple**".

USERNAME_ALIASES — Login of the user and eventually their aliases.

The login should be the same as the user's domain login name, for example **Tom**.

When you import multiple aliases, separate them with commas, for example "**Tom, Tomy, Apple**".

EMAIL — Email of the user, for example "**t.pinapple@domain.com**".


CARDS — Number of the user's authentication card/chip. It has to be inserted in the form in which it is read by the card/chip reader, for example **7E9700C9**.


GROUPS — Here you can add user groups.

You can import a whole branch of the groups tree structure. The groups on the imported branch have to be separated by vertical bars.

If you want to import multiple groups (or groups tree branches), separate them by commas.

For example, if you add two branches separated by a comma: "**Activities|Outdoor|Swimming, Activities|Outdoor|Birdwatching**", MyQ imports a single parent group **Activities** with a single child group **Outdoor**, with two child groups **Swimming** and **Birdwatching**. (Activities>Outdoor>Swimming, Birdwatching)

NOTICE: If you are using a clear installation of version 5.1 or higher, groups on  branches are separated by a vertical bar. System which is upgraded from an older version uses slash instead.

NOTICE:  Commas and vertical bars cannot be used in group names as they are used as group delimiters.

CODE — The personal number of the user. The ID number must be unique for each user.

This parameter is very useful when using multiple sync sources.

SCANSTORAGE — The folder or email where the user wants their scans to be sent, for example "**\\Users\Tomy**".

For more information about scanning, see "Scan Management" in the Basic Installation Guide.

PIN — You can define one or more PINs to be assigned to users within the synchronization process. It is not absolutely necessary as PINs may also be generated later within the setup of the user account. The PINs should be in the hashed MD5 format, for example **14BFA6BB14875E4**.

MANAGED_GROUPS — You can make the user manager of a particular group by adding the group or path to the group here in the way in which you would import the group. If you want the user to be a manager of a child group, enter a whole branch ending with this group.

For example, enter the branch "**Activities|Outdoor|Swimming**" to make the user a manager of the **Swimming** group. If there are no parents of the group in the group structure, enter just the group name, e.g. **Activities**.

NOTICE: If you are using a clear installation of version 5.1 or higher, groups on branches are separated by a vertical bar. System which is upgraded from an older version uses slash instead.

NOTICE: Commas and vertical bars cannot be used in group names as they are used as group delimiters.

AUTHSERVER — In this field you may define the domain for user authentication, for example "**testAD.local**".

PHONE — The user's phone number, for example **080008020**.

LANG — Default language of the user, for example **en**.

PWD — If you want the user to be authenticated against an LDAP server, insert the parameter **ldapAuth**. If not, let this parameter undefined.

EXTID — '**EXTID**' is an internal MyQ parameter. This field has to be left empty.

DELEGATES — For each user, you can import any number of delegates.

If you import multiple delegates, separate them with commas, for example "**Carol,Kohei,Eliot**".

For information about delegates in MyQ, see "Delegated printing" under "Methods of Printing" in the MyQ Basic Installation Guide.

2.4. Manual and scheduled run of synchronizations

The synchronization can be manually run on the **User Synchronization** tab of the MyQ Web Interface, or it can be set as a scheduled task on the **Task Scheduler** tab. The two options are described in the sections below.

Manually running a synchronization

On the **User synchronization** setting tab, enable the synchronizations that you want to run, and then click **Synchronize now** on the bar at the top of the tab.

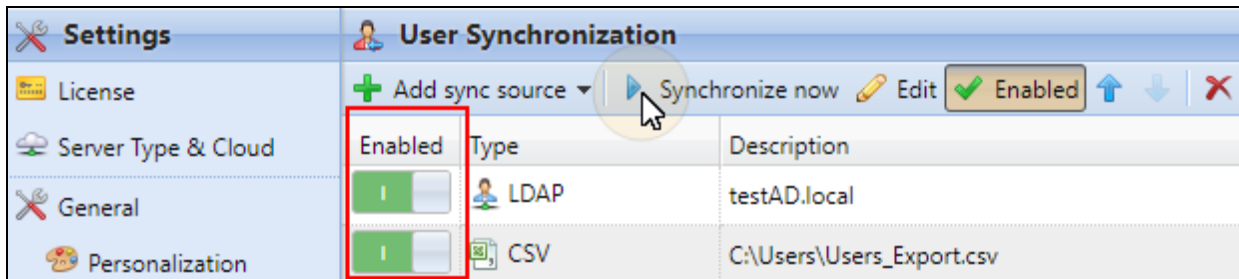


FIGURE 2.20. Manual run of the user synchronizations

Scheduled run of the synchronization

On the **Task scheduler** settings tab, you can setup scheduled run of the synchronization. For more information about this option, see "Task Scheduler settings tab" under "MyQ® System Settings" in the Basic Installation Guide".

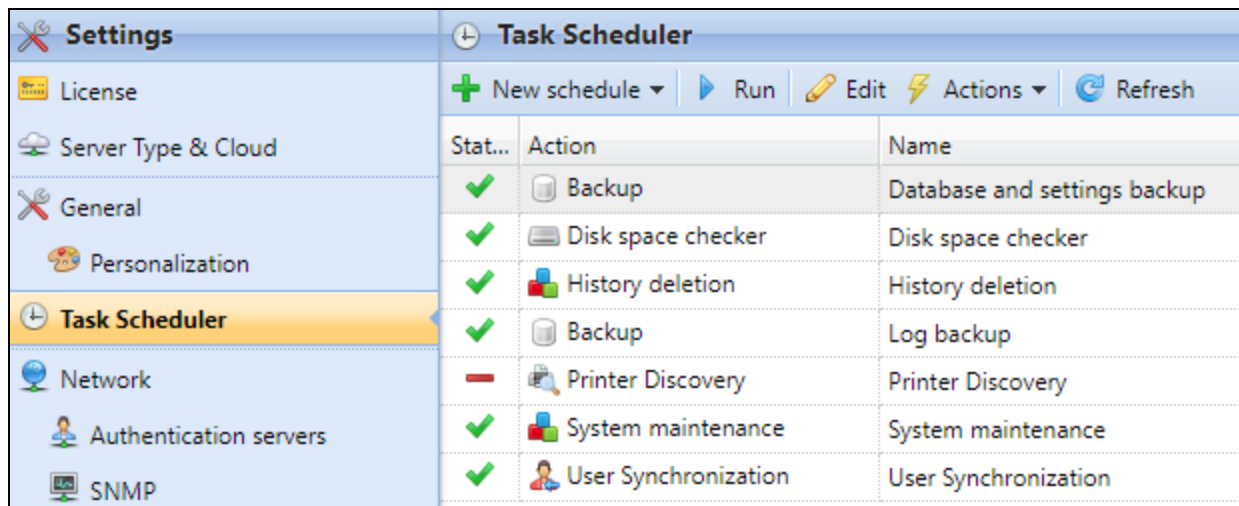


FIGURE 2.21. Scheduled tasks in MyQ

2.5. User synchronization from Azure Active Directory

Azure Active Directory is a service accessed from the Microsoft Azure Portal. It has to be enabled and configured in Azure Active Directory Domain Services.

Activation and setup of the service are described in the following Microsoft guides:

- To enable and configure Azure Active Directory Domain Services:
<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-getting-started>
- Configure Azure AD Domain Servers to use SLDAP:
<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-admin-guide-configure-secure-ldap>

After you activate the Azure Active Directory, you need to add it to MyQ and set up the synchronization in the standard way (see "Authentication servers settings tab" in the MyQ Basic Installation Guide and "User synchronization from LDAP servers" on page 5 of this guide). When setting up the Authentication server in MyQ, you need to make sure that parameters of the LDAP server are set to the following values:

- Domain = **DNS DOMAIN NAME** of the Azure AD Domain
- Security: **SSL**
- Server = **SECURE LDAP EXTERNAL IP ADDRESS** of the Azure AD Domain

Home > myqdev.onmicrosoft.com - Properties

myqdev.onmicrosoft.com - Properties

Azure AD Domain Services

Search (Ctrl+)

- Overview
- Activity log
- Access control (IAM)

Manage

- Properties**
- Secure LDAP
- Health
- Notification settings

Troubleshooting + Support

- Troubleshoot
- New support request

DNS DOMAIN NAME
myqdev.onmicrosoft.com

LOCATION
West Europe

AVAILABLE IN VIRTUAL NETWORK/SUBNET
[MyQDevNetwork/MyQDevTestSubnet](#)

NETWORK SECURITY GROUP ASSOCIATED WITH SUBNET
[AADDS-myqdev.onmicrosoft.com-NSG](#)

IP ADDRESS ON VIRTUAL NETWORK
10.0.0.5 10.0.0.4

SECURE LDAP
Enabled

SECURE LDAP CERTIFICATE THUMBPRINT
B3085415B5ABA88C04742B4D4D1F2F66F8E87025

SECURE LDAP CERTIFICATE EXPIRES
Sat, 05 Oct 2019 06:35:17 GMT

SECURE LDAP EXTERNAL IP ADDRESS
81.144.175.119

FIGURE 2.22. The relevant settings of the Azure AD Domain

3. Detecting job owners

One of the essential functions of MyQ is to identify the owner of a sent print job. In fact, MyQ rejects and discards all jobs where it cannot detect the owner.

You can select from a number of identification methods. The two commonly used ways of detecting owners — identification of the as the user account of the OS from which the job was sent and identification via MyQ Smart Manager— are described in the Basic Installation Guide. Apart from them, you can select from the following identification methods: identifying the job owner as the name of the computer from which the print job was sent, specific case, when DNS server is used to resolve the computer name to be taken as the job owner, detecting the job owner from the name of the print job and detecting the job owner from the job PJI header of the printed job.

The screenshot shows a configuration window titled "Jobs". It contains several settings:

- Default printer language:** * Autodetect (dropdown menu)
- Username case sensitive:**
- User detection method:** * Sender's computer name (dropdown menu, highlighted with a red border)
- Regular expression:** (empty text field)
- Get job name from PJI:** *
- Job metadata mode:** * Not required (dropdown menu)
- Computer detection method:** * Default protocol (dropdown menu)

FIGURE 3.1. The **User detection method** setting on the properties panel of a queue

These options are described in the following sections:

- [Identifying the job owner with the computer name](#)
- [Using DNS server to resolve the job owner](#)
- [Detecting the job owner from the job name](#)
- [Detecting the job owner from the job PJI header](#)

The last section shows how to enable case sensitivity for the job owner detection in MyQ:

- [Enabling case sensitivity for the job owner detection in MyQ](#)

3.1. Identifying the job owner with the computer name

With the **Sender's computer name** option selected, the job owner is identified as the name of the computer from which the job is sent. This way it does not matter on which OS account the sending user is logged and all jobs are accounted on the computer.

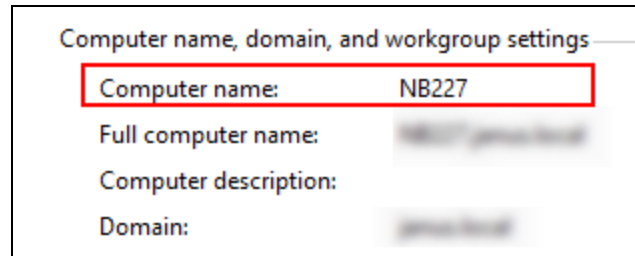


FIGURE 3.2. Computer name is displayed in Windows system settings.

06/08/2...	Info	LP...	10.1.3.11...	Job received: id=2890 time=1s size=19KB user=NB227 project= name=user16@documentxy.com:B01&1&&05R hostname=NB227 queue=Test
------------	------	-------	--------------	---

FIGURE 3.3. Log message informing about the received jobs shows user **NB227**, which is the sender's computer name

INFO: By default, the **Computer detection method** is set to **Default mode**.
💡 This is the standard setting that works in almost all cases. For information about the alternative option, please contact your MyQ support.

💡 **INFO:** A regular expression can be used to capture a part of the detected string. See "Using Regular expressions" on page 31.

3.2. Using a DNS server to resolve the job owner

With the two options: **Print server's DNS name** and **Sender's computer DNS name**, a DNS server is used to resolve the job owner as one of the two respective values:

1) **Print server's DNS name:** The computer or server where the print driver is installed. If the DNS server succeeds in resolving the server IP address, the job owner is identified with the server name, otherwise the job owner is identified with the IP address.

05/31/2...	Info	LPR ...	10.1.3...	Job received: id=2770 time=1s size=88KB user=WIN-GOMOSMT0AO9, .local project= name=user16 hostname=10.1.3.110 queue=Test
------------	------	---------	-----------	--

FIGURE 3.4. Log message informing about the received jobs shows user **WIN-GOMOSMT0AO9.xxxx.local**, which is the print server's DNS name

2) **Sender's computer DNS name:** The computer from which the job is sent. If the DNS server succeeds in resolving the computer IP address, the job owner is identified with the computer name, otherwise the job owner is identified with the IP address.

05/31/2...	Info	LPR ...	10.1.3...	Job received: id=2772 time=1s size=88KB user=10.1.3.110 project= name=user16 hostname=10.1.3.110 queue=Test
------------	------	---------	-----------	---

FIGURE 3.5. Log message informing about the received jobs shows user 10.1.3.110, which is the IP address of the sender's computer

The actual value depends on the location where the print driver is installed. For example:

If the print driver is installed on the print server **Server 1** and shared with the computer **laptop100** from which the user prints, the values are different:

- When you select the **Print server's DNS name** method, the job owner is identified with the server, e.g. Server1.domain.com,
- When you select the **Sender's computer DNS name** method, the job owner is identified with the computer, e.g. Computer100.domain.com.

If the computer does not use shared drivers but sends the jobs via its own drivers, both values are the same.



INFO: A regular expression can be used to capture a part of the detected string. See "Using Regular expressions" on page 31.

3.3. Detecting the job owner from the job name

With the **Detect user from job name** option, the job owner is identified with the name of the print job. This method can be used for in cases where jobs are automatically generated and sent to print by external systems, such as ERP systems. These jobs can have a specific form where the user name is part of the job name, for example **user16@documentxy.com**.

User detection method: *	Detect user from the job name ▼
Regular expression:	
Only for LPR user:	

FIGURE 3.6. The **Detect user from job name** option and two related settings below

05/31/2...	Info	LPR ...	10.1.3...	Job received: id=2778 time=1s size=88KB user=user16 project= name=user16 hostname=10.1.3.110 queue=Test
------------	------	---------	-----------	---

FIGURE 3.7. Log message informing about the received jobs shows user **user16**, which is the job name



INFO: A regular expression can be used to capture a part of the detected string. See "Using Regular expressions" on page 31.

3.3.1. Additional settings

Only for LPR user

The **Only for LPR user** setting is displayed after you select the **Detect user from job name** option. This setting allows you to combine the **Detect user from job name** method with the **Jobs sender** identification method. The job owner is first detected as the job sender and only if the username matches the name entered in the **Only for LPR user** text box, it is identified the job owner with the job name.

This advanced user identification may be required, for example, for some prints from the SAP system. Prints from SAP are usually not sent directly to printing devices, but first to Windows spooler (SAP LPD or SAP Print) which processes and forwards the prints to the device. This service usually runs under the system account (SYSTEM), and therefore the job sender detected from each such job is SYSTEM.

In such case, you can enter the user **SYSTEM** in the **Only for LPR user** text box. MyQ detects the sender and if it is **SYSTEM**, it identifies the job owner with the job name.

Get job name from PJL

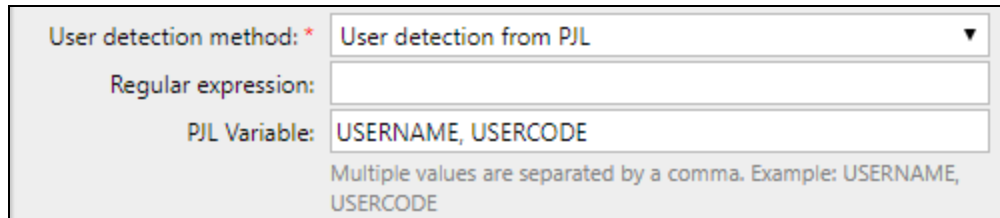
If this option is selected, MyQ takes the job name from the **@PJL JOB NAME** parameter in the PJL header instead of detecting it from the LPR protocol.



WARNING: The job name in the PJL header may differ from the name of the printed document.

3.4. Detecting the job owner from the job's PJJ header

With the **User detection from PJJ** identification option, MyQ detects the job owner from one of the command lines of the print job's PJJ header.



The screenshot shows a configuration window for user detection. It has three main input fields: 'User detection method: *' with a dropdown menu set to 'User detection from PJJ', 'Regular expression:' which is empty, and 'PJJ Variable:' containing 'USERNAME, USERCODE'. Below these fields is a note: 'Multiple values are separated by a comma. Example: USERNAME, USERCODE'.

FIGURE 3.8. User detection from PJJ

To select the line that is used for the definition of the job owner, you need to enter the variable (USERNAME, USERCODE etc.) in the **PJJ Variable** field. If you enter two or more variables separated by a comma, MyQ tries to find a PJJ line containing the first (leftmost) variable, and then eventually repeats the search for the next variable until it either finds a non-empty value with the definition of the job owner or there are no more variables to search for.

```
!R!SEM6;EXIT;+%-12345X@PJJ JOB NAME="something 1 tom 051116 113449735"  
@PJJ SET TIMEOUT=300  
@PJJ SET RESOLUTION=600  
@PJJ SET BITSPERPIXEL=4  
@PJJ COMMENT="INFO:NUP 1; DUPLEX OFF; QTY 1; COLORMODE COLOR;"  
@PJJ COMMENT="APP:C:\Program Files\Windows NT\Accessories\WORDPAD.EXE;"  
@PJJ SET ECONOMODE=OFF  
@PJJ SET USERNAME="Kai"  
@PJJ SET JOBNAME="Something 051116 113449735"  
@PJJ SET QTY=1  
@PJJ SET KCOLORMODE=COLOR  
@PJJ SET KGLOSS=LOW  
@PJJ SET KTRAPPING=2
```

FIGURE 3.9. The PJJ header can be found at the beginning of the job PRN file.

Similarly to the combination of the **Jobs sender** and the **Detect user from job name** detecting methods described in the previous section, you might need to select this option for print jobs sent to MyQ from the SYSTEM account.



INFO: A regular expression can be used to capture a part of the detected string. See "Using Regular expressions" on the next page.

3.5. Enabling case sensitivity for the job owner detection in MyQ

If you have a case sensitive operational system, such as LINUX, where you can create two users whose user names differ only in cases, for example users **juliette** and **Juliette**, you might need to select the **Username case sensitive** option.



FIGURE 3.10. Username case sensitive option selected on properties panel of a queue

With this option selected, MyQ differs between two users that differ only in cases. For example, if a user **Kohei** is registered in MyQ (and user **kohei** is not) MyQ rejects jobs sent from OS account **kohei**.

3.6. Using Regular expressions

You can use regular expressions to capture a part of the string that MyQ detects within any of the detection methods. To do this, define the expression in the **Regular expression** field of the **Jobs** section.

MyQ searches for the desired job owner name in two steps. First, it finds the leftmost match for the regular expression, and then it identifies the job owner with the leftmost group captured in the match. This way you can search for a string and define which part of it will be identified as the job owner. For example, you can use the regular expression to find an email address in the detected name string and use the group capturing to save just the part preceding the @ symbol.

4. ID Card Transformation

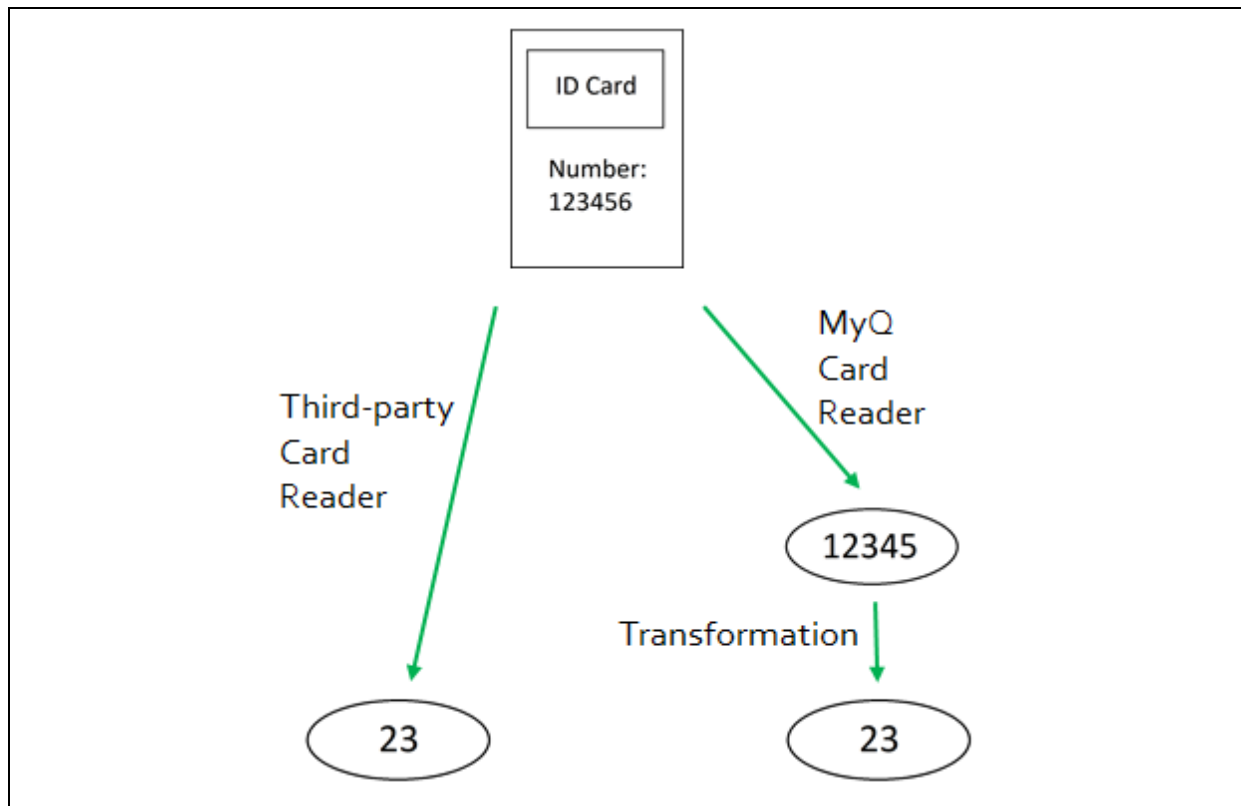


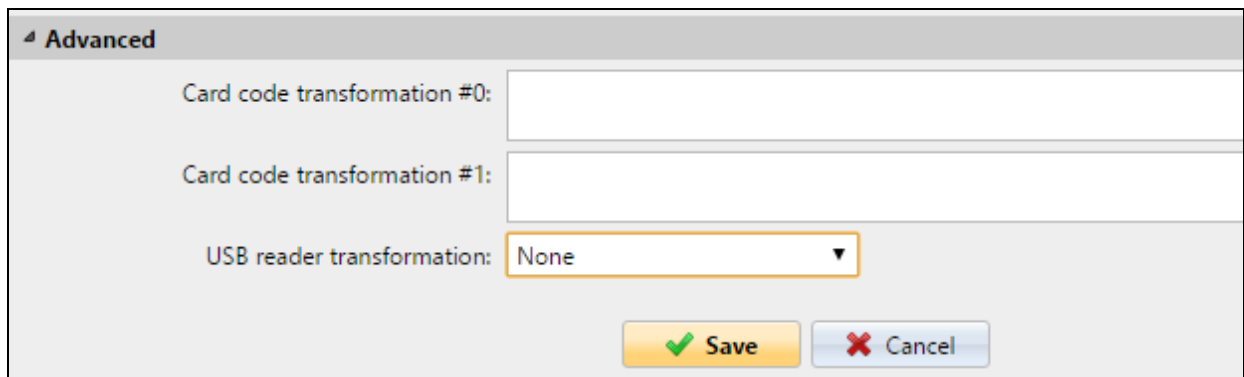
FIGURE 4.1. Scheme of the ID Card Transformation

This topic discusses the ID Card transformation feature in MyQ. The transformation might be necessary if the customer needs to import card numbers from a third-party SW database and the card number format in this database doesn't match the format read by MyQ card reader.

The third-party system card readers can give output in a different format than the card readers used in MyQ. In consequence, users card numbers imported from the third-party system can differ from the card numbers read by the MyQ card readers. To unify the format of the two outputs, you can define a specific sequence of commands that transforms the output of the MyQ card readers to the format used in the database of the third-party system.

INFO: With most of the MyQ card readers, you can use the card reader configuration software to set the format directly on the reader. However, it is simpler and faster to set one or two universal MyQ transformations than to separately change settings of each card reader.

4.1. Entering the transformation



The screenshot shows a window titled "Advanced" with three input fields. The first two are "Card code transformation #0:" and "Card code transformation #1:", both with empty text boxes. The third is "USB reader transformation:" with a dropdown menu showing "None". At the bottom right, there are two buttons: "Save" (with a green checkmark) and "Cancel" (with a red X).

FIGURE 4.2. The **Advanced** section of the **Printers** settings tab

On the **Printers** settings tab, under **Advanced**, you can define and use up to two transformations for card readers and select to use one of them on a USB reader connected to the administrator PC. The second transformation can be used in case where you have a hardware terminal with two card readers attached to it. The USB reader can be used to recharge credit or associate cards.

Available options:

- Card code transformation #0: This transformation is used by Embedded terminals (with USB readers connected directly to the device) and by the reader for HW terminal that is connected as #0 (usually primary reader).
- Card code transformation #1: This transformation is used by the reader for HW terminal that is connected as #1 (usually secondary reader).
- USB reader transformation: The transformation selected here (#0 or #1) will be applied to card readers connected to PC USB slot. These card readers are usually used to recharge credit or to associate cards with user accounts.

4.2. Defining the transformation

You can define the transformation by adding commands from the table below. The commands have to be separated by semicolon and are read and executed from left to right, for example in the transformation **CommandX;CommandY**, the **Command X** is executed first and the **Command Y** second.

All commands, except for the + command, are applied in the following way:

The first command of the transformation and each command immediately behind the **+** command are applied to the initial card number. All other commands are applied to the result of their predecessors.

For application of the + command, see the description in the Table of commands below.

Table of commands:

ltrim(number of characters) — Remove the first X characters from left.
ltrim(2): 123456 → 3456
rtrim(number of characters) — Remove the first X characters from right (the last X characters).
rtrim(2): 123456 → 1234
prepend(character string) — Add the string in front of the card number.
prepend(AB): 123456 → AB123456
append(character string) — Add the string behind the card number.
append(AB): 123456 → 123456AB
left(number of characters) — Select the first X characters from left (and remove the rest).
left(2): 123456 → 12
right(number of characters) — Select the first X characters from right.
right(2):123456 → 56
mid(number of characters, number of characters) — Remove X characters from left, remove Y characters from right and leave the characters in the middle.
mid(2,2): 123456 → 34

<p>lpad(number of positions, symbol) — Complete the string to the length specified by the number of positions parameter by adding value of the symbol parameter to the left (in front of the card number).</p>
<p>lpad(12,0): 123456 —> 000000123456</p>
<p>hex2dec() — Transform the card number from hexadecimal mode to decimal mode.</p>
<p>hex2dec(): 1000AB —> 1048747</p>
<p>dec2hex() — Transform the card number from decimal mode to hexadecimal mode.</p>
<p>dec2hex(): 1048747 —>1000AB</p>
<p>hex2bin — Transform the card number from hexadecimal mode to binary mode.</p>
<p>hex2bin(): 1000AB —> 100000000000010101011</p>
<p>bin2hex — Transform the card number from binary mode to hexadecimal mode.</p>
<p>bin2hex(): 100000000000010101011 —> 1000AB</p>
<p>dec2bin — Transform the card number from decimal mode to binary mode.</p>
<p>dec2bin(): 100023 —> 11000011010110111</p>
<p>bin2dec — Transform the card number from binary mode to decimal mode.</p>
<p>bin2dec(): 11000011010110111 —> 100023</p>
<p>reverse() — Reverse the byte sequence, i.e. take all characters by two and reverse the order of the pairs. (The last pair goes first, the second last goes second etc.)</p>
<p>reverse(): 1234AB —> AB3412</p>

reverseString() — Reverse the character sequence. (The last character goes first, the second last goes second etc.)

reverseString(): 1234AB → BA4321

reverseNibbleBits() — Convert each character from hexadecimal mode to binary mode, reverse the character sequence of each quadruple and convert the result back to hexadecimal mode.

reverseNibbleBits(): 10AB → 0001 0000 1010 1011 → 1000 0000 0101 1101 → 805D

upper(): Converts the string to upper case.

upper():Abcd → ABCD

plugin(reference): Calls a card transformation plugin with the given reference.

This option enables using custom PHP scripts for the transformation. For more information about this option, contact your MyQ support.

asciiCode2ascii — Converts ASCII characters encoded as hex-digits to ASCII characters.

asciiCode2ascii(): 414F → AO

"string 1" + "string 2" — Merges strings in front and behind this command.

"string 1":

- Either the initial card number (if there are no commands preceding the + symbol),
- or the result of the last command before the + symbol (if there are no + commands preceding the + symbol),
- or the result of the previous + command.

"string 2":

- Either the initial card number (if there are no commands behind the + symbol or if the next command is another + command),
- or the result of the last command of the transformation (if there are no + commands behind the + symbol),
- or the result of the last command before another + command.

Here is an example of a transformation:

Card number: 10AB

Transformation: `hex2bin();lpad(16,0);reverseString();ltrim(8);reverseString();bin2hex() + ltrim(4);lpad(4,10AB)`

Result: 1010AB

Transformation process:

("10AB" → "1 0000 1010 1011" → "0001 0000 1010 1011" → "1101 0101 0000 1000" → "0000 1000" → "0001 0000" → "10") + ("10AB" → "" → "10AB") ==> "1010AB"

5. Using External Authentication Servers for Authentication in MyQ

In addition to the internal MyQ authentication methods (password, PIN or a card added to the MyQ system), you can use two types of external authentication servers: LDAP and Radius.

With the two external methods, MyQ does not use the internal MyQ PIN or password for user authentication, but instead authenticates users against an LDAP or Radius server. After the user enters their credentials during the authentication, the credentials are sent to be verified directly by the external server. If there is no online connection with the LDAP or Radius server, users cannot log in.

To enable this method of authentication, you have to take two steps: register authentication servers in MyQ and select to use them for authentication of users. The later can be done automatically during import of the users from an LDAP server or a CSV file or manually on the properties panels of individual users.

5.1. Registering authentication servers in MyQ

The servers can be viewed and added on the **Network** settings tab, under **Authentication servers**.

To add a new LDAP server:

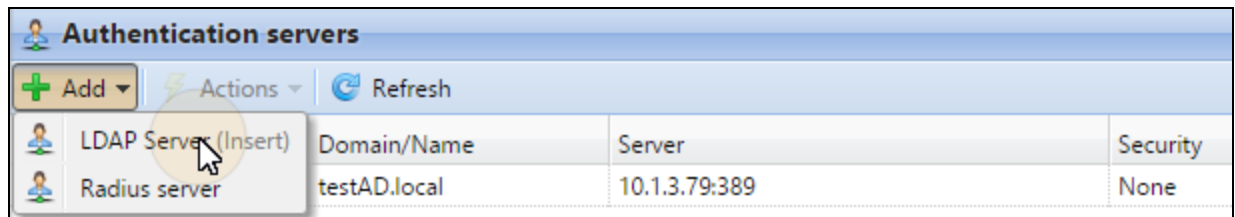


FIGURE 5.1. Adding a new LDAP server on the **Network** settings tab, under **Authentication servers**

1. Click **+Add** and select the **LDAP server** option. The new LDAP server properties panel opens on the right side of screen.
2. Enter the LDAP domain.
3. Select the LDAP type. You can select from **Active Directory**, **Novell**, **OpenLDAP** and **Lotus Domino**.
4. If you want the communication with the LDAP to be secured, select the protocol that you want to use.
5. Enter IP address or hostname of the server and communication port.

6. If you have more addresses related to one LDAP server, you can add them by clicking **Add**.
7. Click **Save**. The LDAP server appears on the list of servers.

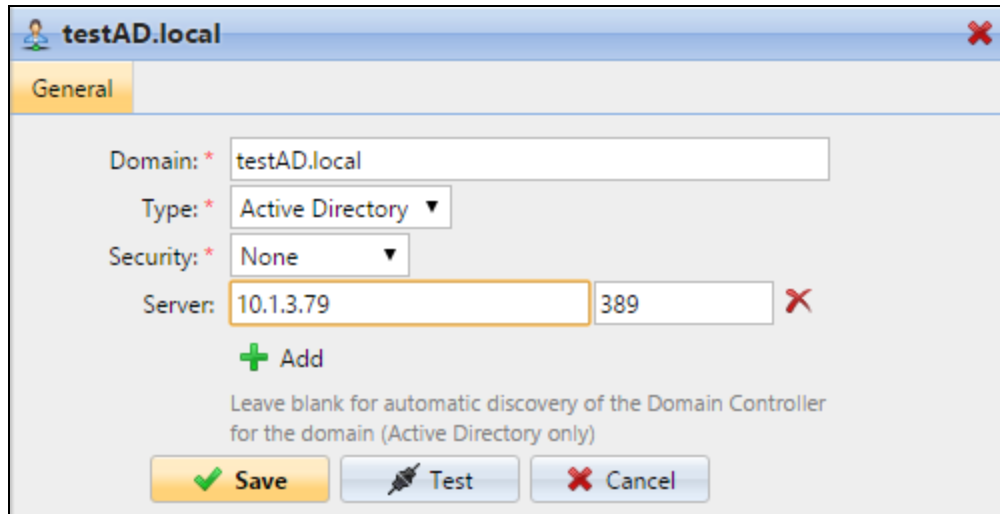


FIGURE 5.2. The LDAP server properties panel

To add a new Radius server

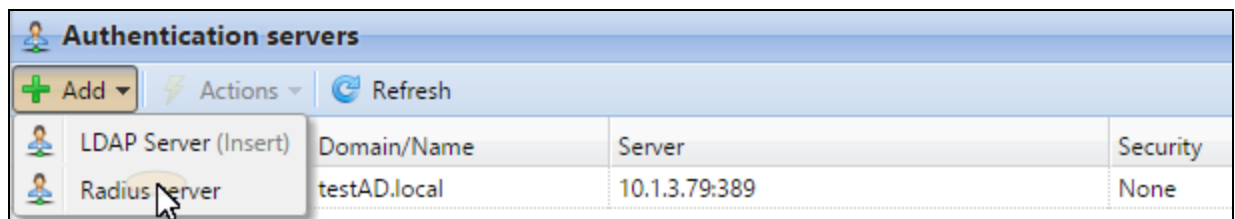


FIGURE 5.3. Adding a new Radius server on the **Network** settings tab, under **Authentication servers**

1. Click **+Add** and select the **Radius server** option. The new Radius server properties panel opens on the right side of screen.
2. Enter the Radius server name.
3. Enter IP address or hostname of the server, communication port and Shared secret.
4. If you have more addresses related to one Radius server, you can add them by clicking **+Add**.
5. Click **Save**. The Radius server appears on the list of servers.

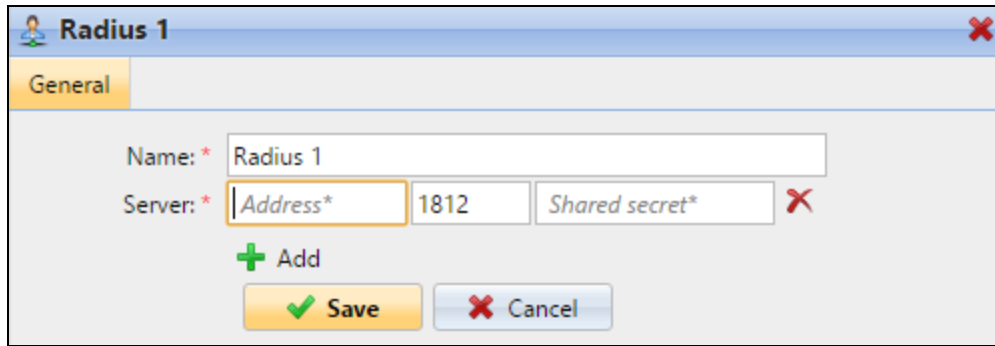


FIGURE 5.4. The Radius server properties panel

To edit a server:

1. Double-click the server on the list. The server properties panel opens on the right side of screen.
2. On the panel, change the settings, and then click **Save**.

To delete a server:

- Right-click the server on the list, and then click **Delete** on the shortcut menu.

5.2. Setting the external user authentication option

There are two ways of setting the external user authentication option and assigning the servers to users. The first way is to select to use the external authentication option during import of users from an LDAP server or a CSV file. The second way is to manually select this option on properties panels of individual users.

Automatically selecting the external authentication option

Importing users from a CSV file

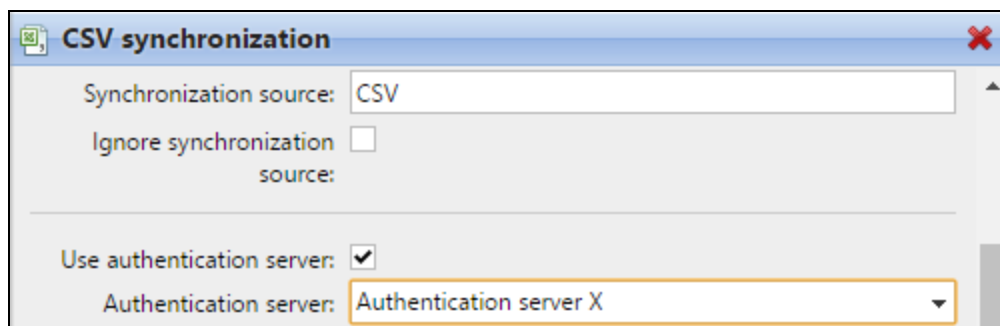


FIGURE 5.5. Selecting the authentication server for the users imported from the CSV file

When you import users from a CSV files, you have two options of selecting the authentication server for the users:

1. You can select the **Use authentication server** option and select the server during setup of the synchronization on the synchronization properties panel.
2. You can specify the Authentication server for a particular user in the **AUTHSERVER** field of the CSV file. If the field is not empty, its value has priority over the value selected on the properties panel.

For more information about importing users from CSV files, see "User synchronization from CSV files" on page 17.

To enable the authentication option for users imported from an LDAP server

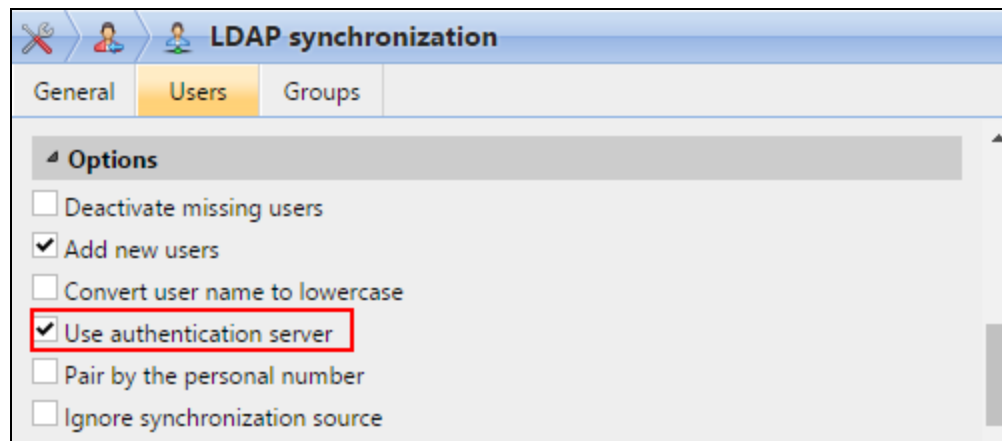


FIGURE 5.6. Selecting to authenticate the imported users from the LDAP server

During the import from an LDAP server, you can select the **Use authentication server** option, to use the current synchronization source server for authentication of users. For information about importing users from LDAP servers, see "User Import and Synchronization" on page 2.

INFO: Unlike the **Use authentication server** setting for the import from a CSV file, which allows you to select the authentication server, the **Use authentication server** setting here gives you a single option — users will be authenticated against the LDAP server from which they are imported.

Manually selecting the external authentication option

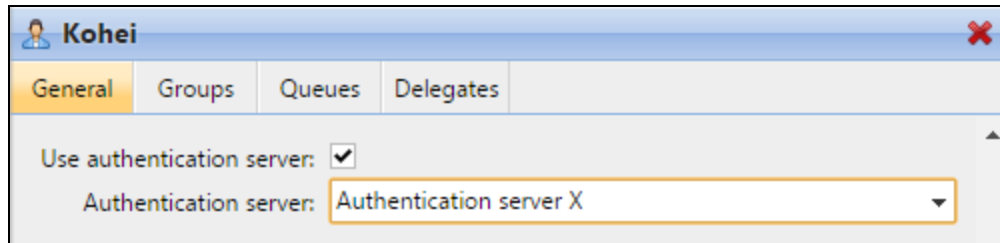


FIGURE 5.7. The Authentication server settings on the **General** tab of the user properties panel

To manually select the external authentication option

1. Open the **Users** settings tab and double-click the user. The user's properties panel opens on the right side of screen.
2. On the panel, select the **Use authentication server** option. The **Authentication server** setting appears on the panel.
3. On the **Authentication server** drop-down box, select the server that you want to use, and then click **Save** at the bottom of the panel.

6. MyQ Smart Job Manager: Advanced Setup

Within the Windows installation of the Smart Job Manager, the settings of the application are stored in Windows registry under HKEY_LOCAL_MACHINE. Depending on the Windows system, it can be found under one of the following paths:

- Path for 32bit system: **Software\MyQ\Smart Job Manager\Settings**
- Path for 64bit system: **Software\WOW6432Node\Smart Job Manager\Settings**

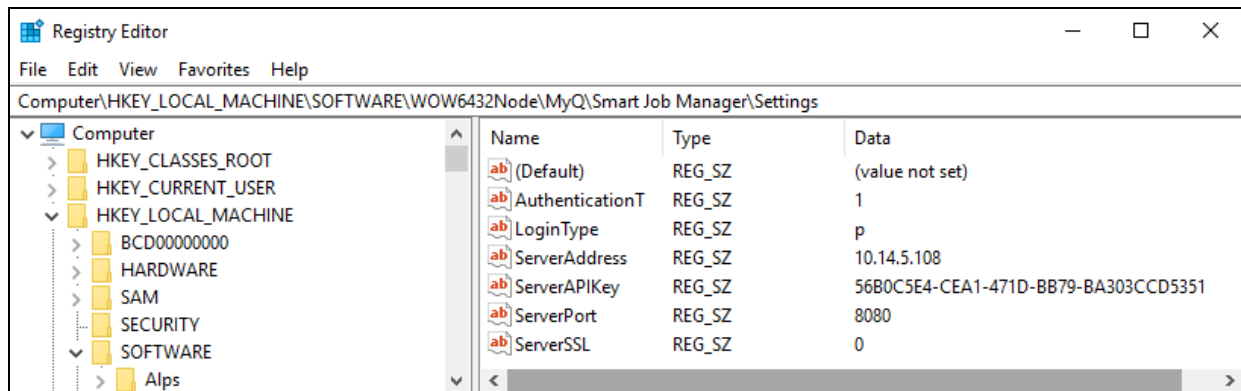


FIGURE 6.1. The **Smart Job Manager\Settings** Windows Registry key under HKEY_LOCAL_MACHINE

In specific cases where you do not want to use the local machine settings and instead want to set different properties of the application for the currently logged user, you can create a new key under HKEY_CURRENT_USER with the following path:

- **Software\MyQ\Smart Job Manager\Settings**

The settings and their values correspond to the parameters described under "Silent Installation" in the Guide to MyQ Smart Job Manager for Windows.

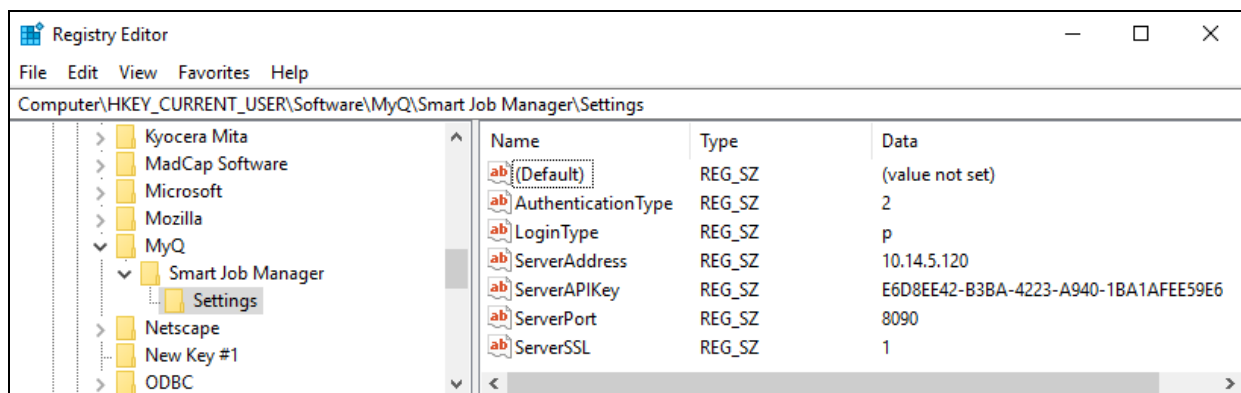


FIGURE 6.2. The **Smart Job Manager\Settings** Windows Registry key under HKEY_CURRENT_USER

7. Appendix: Overview of Changes

This topic shows the changes made within revisions of the guide.

Revision 2

Changes in topics

User Import and Synchronization

- "2.2. User synchronization from LDAP servers": Added the section "2.3. User synchronization from Azure Active Directory"; added information on how to create tree structures of groups via the **Groups stored in user's attribute** setting.

8. Business contact

MyQ® Manufacturer	<p>MyQ® spol. s r.o.</p> <p>Harfa Office Park, Ceskomoravska 2420/15, 190 93 Prague 9, Czech Republic</p> <p>MyQ® Company is registered in the Companies register at the Municipal Court in Prague, division C, no. 29842</p>
Business information	<p>www.myq-solution.com</p> <p>info@myq-solution.com</p>
Technical support	<p>support@myq-solution.com</p>
Notice	<p>MANUFACTURER WILL NOT BE LIABLE FOR ANY LOSS OR DAMAGE CAUSED BY INSTALLATION OR OPERATION OF THE SOFTWARE AND HARDWARE PARTS OF THE MyQ® PRINTING SOLUTION.</p> <p>This manual, its content, design and structure are protected by copyright. Copying or other reproduction of all or part of this guide, or any copyrightable subject matter without the prior written consent of MyQ® Company is prohibited and can be punishable.</p> <p>MyQ® is not responsible for information content of this manual, particularly regarding its integrity, currency and commercial occupancy. All the material published here is exclusively of informative character.</p> <p>This manual is subject to change without notification. MyQ® Company is not obliged to make these changes periodically nor announce them, and is not responsible for currently published information to be compatible with the latest version of the MyQ® printing solution.</p>
Trademarks	<p>MyQ® including its logos is registered trademark of MyQ® company. Microsoft Windows, Windows NT and Windows Server are registered trademarks of Microsoft Corporation. All other brand and product names might be registered trademarks or trademarks of their respective companies.</p> <p>Any use of trademarks of MyQ® including its logos without the prior written consent of MyQ® Company is prohibited. The trademark and product name is protected by MyQ® Company and/or its local affiliates.</p>