

# KYOCERA Net Manager Installation Guide

2024.02

KNMBIGKDEN101



# Table of Contents

<b>1</b>	<b>Release Notes.....</b>	<b>10</b>
1.1	10.1 (patch 8).....	10
1.2	10.1 (patch 7).....	10
1.3	10.1 (patch 6).....	11
1.4	10.1 (patch 5).....	12
1.5	10.1 (patch 4).....	13
1.6	10.1 (patch 3).....	13
1.7	10.1 (patch 2).....	14
1.8	10.1 (patch 1).....	15
1.9	10.1 RTM .....	15
1.10	10.1 RC2 .....	16
1.11	10.1 RC .....	17
1.12	10.1 BETA3 .....	18
1.13	10.1 BETA2.....	19
1.14	10.1 BETA .....	20
<b>2</b>	<b>Basic Information .....</b>	<b>25</b>
2.1	KYOCERA Net Manager Servers and applications .....	25
2.2	Print Server from the OS process perspective .....	25
2.3	Network Communication Architecture .....	26
<b>3</b>	<b>System Requirements .....</b>	<b>28</b>
3.1	Installed parts and possible conflicts.....	32
3.2	Main Communication Ports.....	32
3.3	Windows Server Performance Monitor.....	36
<b>4</b>	<b>Installation.....</b>	<b>39</b>
4.1	Installation in Private Cloud .....	39
4.2	Installing the KX Driver .....	40
4.3	Installing KYOCERA Net Manager Port Monitor .....	42
<b>5</b>	<b>KYOCERA Net Manager Easy Config.....</b>	<b>50</b>
5.1	Services .....	51

5.2	Passwords.....	51
5.3	KNM Windows Services Account.....	52
5.4	Data and Jobs Folders .....	53
5.5	Security .....	54
5.6	Database Backup and Restore .....	55
5.7	Changing KNM Web server ports .....	57
5.8	Cleaning Cache and Temp folders.....	58
<b>6</b>	<b>KYOCERA Net Manager Web Interface .....</b>	<b>59</b>
6.1	Accessing the KNM Web Interface .....	59
6.2	Logging in as an administrator.....	59
6.3	Main menu and Settings menu.....	61
6.4	Home Dashboard.....	61
6.5	KNM Log .....	66
6.6	KNM Audit Log .....	68
<b>7</b>	<b>KYOCERA Net Manager System Settings .....</b>	<b>70</b>
7.1	Server Type Settings.....	70
7.2	General Settings.....	71
7.3	Personalization Settings .....	72
7.4	Task Scheduler Settings .....	74
7.5	Network Settings .....	76
7.6	Connections Settings.....	80
7.7	Authentication Servers Settings.....	98
7.8	Accounting Settings.....	100
7.9	External Reports .....	102
7.10	REST API Apps .....	103
7.11	Log Settings.....	103
7.12	System Management Settings .....	106
7.13	Security settings in config.ini .....	108
<b>8</b>	<b>Licenses.....</b>	<b>110</b>
8.1	Adding licenses .....	110
8.2	Activating Licenses .....	112

8.3	Deleting licenses .....	114
8.4	Extending software assurance licenses .....	114
8.5	Migrating old licenses to KNM X.....	116
8.6	VMHA License.....	118
<b>9</b>	<b>Printers.....</b>	<b>119</b>
9.1	Printers and Terminals settings.....	120
9.2	Manually adding printing devices .....	164
9.3	Configuration profiles .....	165
9.4	Discovering printing devices .....	167
9.5	Activating and deactivating printing devices .....	171
9.6	Deleting and undeleting printers .....	172
9.7	Editing printers .....	173
9.8	Printer groups .....	176
9.9	Exporting and importing printers.....	177
9.10	Monitoring network printers in offline mode .....	178
9.11	Monitoring local printers .....	179
9.12	Printer Events .....	179
9.13	SNMP profiles.....	183
<b>10</b>	<b>Users.....</b>	<b>186</b>
10.1	List of users .....	186
10.2	Automatic user registration .....	186
10.3	Add users manually.....	188
10.4	Deleting and undeleting users.....	188
10.5	Editing user accounts.....	189
10.6	Enable user profile editing .....	192
10.7	User groups.....	193
10.8	Exporting users .....	194
10.9	Securing KNM users personal data .....	194
10.10	User import and synchronization .....	196
10.11	User Authentication.....	210
10.12	Policies .....	218

10.13 Rights .....	222
10.14 Users Settings .....	224
<b>11 Queues.....</b>	<b>227</b>
11.1 List of queues .....	227
11.2 Queue types .....	228
11.3 Adding and deleting queues .....	230
11.4 Editing queues .....	230
11.5 Online/Offline queues.....	233
11.6 Personal Queues.....	234
11.7 Advanced queue options .....	236
<b>12 Printing to KNM .....</b>	<b>260</b>
12.1 Windows settings.....	260
12.2 MacOS settings .....	261
<b>13 Methods of Printing.....</b>	<b>264</b>
13.1 Direct printing .....	264
13.2 Print&Follow printing .....	264
13.3 Delegated printing .....	265
13.4 Printing from email and from the KNM Web UI .....	265
13.5 Print from Chromebooks, Chrome and other Google apps.....	269
13.6 AirPrint and Mopria Print Service .....	269
13.7 Microsoft Universal Print .....	271
13.8 Client Spooling .....	276
13.9 Device Spooling.....	280
13.10 Offline Login .....	283
13.11 Fallback Printing .....	285
<b>14 Jobs .....</b>	<b>289</b>
14.1 Jobs settings tab.....	289
14.2 List of jobs.....	291
14.3 Editing jobs .....	292
14.4 Page Description Languages (PDL) .....	292

14.5	Job Parser.....	292
14.6	Notifying the admin and users about refused jobs .....	293
14.7	Jobs Preview .....	294
14.8	Job Archiving.....	294
14.9	Jobs via IPPS .....	295
14.10	Job Privacy.....	303
14.11	Watermarks .....	304
<b>15</b>	<b>Reports.....</b>	<b>308</b>
15.1	Report Types .....	308
15.2	Reporting sources.....	347
15.3	Report values description .....	347
15.4	Creating and editing reports.....	348
15.5	Generating reports.....	352
<b>16</b>	<b>Connection to BI tools.....</b>	<b>354</b>
16.1	Embedded Database Connection Configuration.....	354
16.2	Creating Reports.....	356
<b>17</b>	<b>Scanning and OCR .....</b>	<b>369</b>
17.1	Scan to Me .....	369
17.2	OCR.....	372
<b>18</b>	<b>Code Books.....</b>	<b>375</b>
18.1	LDAP Source Code Books .....	375
18.2	Internal Code List.....	376
18.3	MS Exchange Address Book .....	378
<b>19</b>	<b>Credit.....</b>	<b>382</b>
19.1	Activation and setup.....	382
19.2	Manual credit recharge.....	383
19.3	Recharging credit by vouchers .....	386
19.4	Recharging credit via PayPal .....	388
19.5	Recharging credit via WebPay .....	390
19.6	Recharging credit via CASHNet.....	392

19.7	Recharging credit via SnapScan.....	395
19.8	Bulk credit recharge .....	396
19.9	Manual reset of users' credit on the KNM Web Interface .....	397
19.10	Credit accounting reports.....	398
<b>20</b>	<b>Quota.....</b>	<b>399</b>
20.1	Activation and general setup .....	399
20.2	Creating quotas .....	400
20.3	Editing quotas .....	400
20.4	Boosting quotas.....	402
<b>21</b>	<b>Projects .....</b>	<b>404</b>
21.1	Projects activation and setup .....	404
21.2	Creating projects .....	404
21.3	Project management.....	405
21.4	Importing projects from CSV files .....	406
21.5	Assigning projects to print jobs .....	407
<b>22</b>	<b>Price List.....</b>	<b>409</b>
22.1	Adding price lists .....	409
22.2	Editing price lists.....	409
22.3	Discounts .....	411
<b>23</b>	<b>System health check.....</b>	<b>413</b>
23.1	Using system health check .....	414
<b>24</b>	<b>Updating KNM.....</b>	<b>415</b>
<b>25</b>	<b>Uninstalling KNM .....</b>	<b>416</b>
<b>26</b>	<b>KNM and MS Cluster.....</b>	<b>417</b>
26.1	About.....	417
26.2	System Requirements .....	417
26.3	Licenses.....	418
26.4	Setup .....	418
26.5	Additional Setup.....	425
26.6	Configuration and Maintenance .....	426

26.7 Backup and Restore..... 428

26.8 Upgrading KNM ..... 429

26.9 Recommended Troubleshooting..... 429

27 Available languages.....430

## **KYOCERA Net Manager Server 10.1**

**KYOCERA Net Manager** is a server-based web application that manages your printing devices and user policies to provide secure printing and copying, and to provide accounting of print-related expenses. Efficient use of your printing resources is provided by the **Print&Follow** function, which allows users to securely print to any printer managed by **KYOCERA Net Manager**.

**KYOCERA Net Manager** offers many advantages:

### **Authentication**

Access printers using a PIN or an ID card, or user name and password combination. **KYOCERA Net Manager** can be set to use a two-step authentication combination such as ID card and PIN.

### **Security**

Secure printing, data encryption, and the **Print&Follow** function ensure that your documents can only be accessed and printed by authorized people.

### **Reporting**

**KYOCERA Net Manager** keeps detailed statistics about all aspects of printing and printers, scanning and copying, projects, accounting, and users and groups.

### **Personalized Features**

**KYOCERA Net Manager** allows **KNM** admins to show different functions and applications per user based on the user's requirements.

### **Easy Scan**

One click changes the destination of your scanned documents and their metadata. You may choose between your home folder, fax server, or email address.

### **Mobile printing**

Print documents from your mobile device by sending the job to the **KYOCERA Net Manager** server.

# 1 Release Notes

---

## KYOCERA Net Manager Print Server 10.1

- Minimum required support date: **1st of February 2023**
- Minimum required version for upgrade: **8.2**

### 1.1 10.1 (patch 8)

15 January, 2024

#### Security

- Added option in Easy Config to lock/unlock Queue's Scripting (PHP) settings for changes, improves security by allowing you to keep these settings in read-only mode at all times (resolves CVE-2024-22076).

#### Improvements

- Added option to add an additional column "Project code" to reports in the Projects category.
- Password field for SMTP settings can accept up to 1024 characters instead of 40.

#### Bug Fixes

- A job with mixed color and B&W pages uploaded via Web Interface is recognized as a full color document.
- Easy Scan to Email fails when more than one recipient is used.
- Parsing of specific PDF files can fail.
- Purchase date description text can be displayed multiple times.
- Reinstalling **KNM** to a different path without deleting the data folder first results in the Apache service not able to start.
- Scan to FTP uses additional port 20.
- Some reports can display different values on Site Server and Central Server.
- The User Rights settings dialog window is continuously moving if the window does not fit in the screen.
- When creating a new price list or editing an existing one, the Cancel button does not work correctly.

---

### 1.2 10.1 (patch 7)

15 December, 2023

#### Improvements

- List of characters allowed to be used in project code expanded. Upgrade of Central Server to 10.1 (patch 7) and 10.2 (patch 6) is required beforehand for replications to work correctly.
- New permission Delete Cards added, allowing to give users or user groups the option to be able to delete ID cards without them having access to other user management features.
- Improved logging to reflect the result of cloud service connection (in case of refresh token is not received).
- Traefik updated to version 2.10.5.
- OpenSSL updated to version 3.0.12.

#### Changes

- When settings are being restored in Easy Config, licenses are also removed.

- In Easy Config's Data Encryption settings, expired certificates are now marked as expired and cannot be selected.
- Queue's default user detection method changed from "KX Driver/App" to "Job sender".

### **Bug Fixes**

- Codebook operations using OpenLDAP fail due to incorrect username formats.
- Monthly reports for the whole year can have incorrectly sorted months.
- Favorite items in Codebooks are not displayed first on the Embedded Terminal.
- User synchronization from Azure AD can fail in case of a large number of groups.
- Job marked favorite while Projects were enabled cannot be unfavorited after Projects are disabled.
- Disabled terminal actions that are in a folder are still displayed on the Embedded Terminal.
- Project's rights for "All users" are not assigned properly when imported from a CSV.
- It is not possible to add rights for "All users" to an Internal Codebook in case when rights were previously removed.
- Upgrade of the terminal package does not remove the pkg file of the previous version in the Program Data folder.
- While searching in LDAP Codebooks on the Embedded Terminal, the search only matches items that begin with the query instead of searching full-text.
- Price for A3 print/copy jobs may be incorrect in reports marked as beta.
- The Help widget on the dashboard does not display the custom title specified in the settings.
- Searching a codebook on the embedded terminal does not work for the query "0", no result is returned.
- Report "Credit and quota - Quota status for user" takes too long to generate in some cases.

## **1.3 10.1 (patch 6)**

14 November, 2023

### **Improvements**

- Users who have available OneDrive Business or SharePoint destinations now can browse their entire storage when using Easy Print and Easy Scan, allowing them to select/enter any file/folder they have access to. If Folder browsing is disabled on this destination, scanned files are saved in the root folder of the storage.
- Optimizations of Azure AD synchronization via Microsoft Graph API connector that should prevent slowdowns and skipping users.
- OpenSSL updated to version 3.0.11.
- Apache updated to version 2.4.58.
- CURL updated to version 8.4.0.
- Firebird updated to version 3.0.11.

### **Bug Fixes**

- Jobs via Web are printed always in mono when Job Parser is set to Basic.
- Easy Scan to a shared folder with selected authentication as "User doing the scan" does not work in some cases.
- Report period parameter accepts negative value.
- Job preview of invalid job could cause Embedded Terminal to freeze.
- Duplex option does not work when printing from Linux with some drivers.
- Not possible to use advanced processing features (like watermarks) on some PDF jobs.
- Deleted printers are shown in Reports.
- Print of specific PDF via Web upload could cause Print Server service to crash.

- Credit actions drop-down menu options on Users tab is incorrectly aligned (cut off).
  - Filter for printer group in Environmental - Printers report does not correctly filter printers to be included in the report.
  - User with rights to edit scheduled reports can not select other attachment file format than PDF.
  - Missing Chinese languages in Easy Config language selection.
- 

## 1.4 10.1 (patch 5)

20 September, 2023

### Improvements

- HTTPS is used for external links from the Web Interface.
- Traefik updated to version 2.10.4.
- OpenSSL updated to version 1.1.1v.
- PHP updated to version 8.0.30.

### Bug Fixes

- Printers filter for Terminal Actions placed in a folder is not correctly applied, resulting in these actions being displayed on all devices.
- Synchronized users who are members of groups with identical names to **KNM** built-in groups in the source, are wrongly assigned to these built-in groups due conflicting names.
- In rare cases, Web Server Error could be displayed to a user after login due to multiple memberships in the same group.
- Credit statement in CSV cannot be downloaded.
- License plan of License widget contains label "EDITION".
- "Operation failed" error could be shown when user is connecting Google Drive storage.
- New user is not registered after a card swipe with "Register a new user by swiping an unknown ID card" enabled.
- The server could crash during a continuous high-level print load.
- Manually set Cost Centers for users are removed after user synchronization from Azure AD and LDAP.
- Easy Fax appears as an available destination in the Easy Scan Terminal Action settings.
- Two groups with identical names are indistinguishable in reports.
- Installation of the Kyocera Embedded Terminal does not configure secure SMTP communication in the device when secure-only communication is enabled in **KNM**.
- In Job privacy mode, Administrators and users with Manage reports rights can see only their own data in all reports, resulting in the inability to generate organization-wide reports for group accounting, projects, printers, and maintenance data.
- In Job privacy mode, user running a report is excluded when Exclude filter is not used.
- Some groups reports are not possible to save when only Accounting group filter is set with error "User may not be empty".

### Device Certification

- Added support for some Olivetti models - d-COPIA 5524MF, d-COPIA 4524MF plus, d-COPIA 4523MF plus, d-COPIA 4524MF, d-COPIA 4523MF, PG L2755, PG L2750, PG L2745.
  - Added support for Kyocera TASKalfa M30032 and M30040.
-

## 1.5 10.1 (patch 4)

7 August, 2023

### Improvements

- Added the option to [exclude specific user\(s\) from Reports](#).
- MAKO updated to version 7.0.0.

### Bug Fixes

- Refresh token for Exchange Online expires due to inactivity in spite of the system being actively used.
  - Connecting OneDrive Business cloud account may end with error that the storage cannot be read.
  - Missing Scan and Fax columns in report Projects – User Session details.
  - User synchronization for user with invalid UTF value causes PHP exceptions.
  - Parsing of some PDF files fails because of unknown font.
  - Site Server's print service crashes, when Job roaming jobs are requested for deleted user.
- 

## 1.6 10.1 (patch 3)

17 July, 2023

### Improvements

- **NEW FEATURE** Possible to export server settings and import them into another server.
- PHP updated to version 8.0.29.
- Printer Status Check now also checks coverage counters (for devices, where it is applicable).
- Certificates in PHP updated.
- Apache updated to version 2.4.57.
- Installation via Printer Discovery initiated by the Embedded Terminal is now supported (requires to be also supported by the Embedded Terminal).
- Job Preview is now generated in higher image quality.
- Purchased Assurance Plan is displayed on the Dashboard of the **KNM** Web Interface.
- Added unique session identifiers to replication data to prevent differences in reports between Sites and Central. Upgrade of Central Server to version 10.1 (patch 2) is recommended to be done first for full utilization of this improvement.

### Changes

- Attempt of reading printer's OID which is not available is logged as Debug message instead of Warning.

### Bug Fixes

- Cloud service name missing in Connect dialogue.
- Document with multiple paper sizes (i.e. A3+A4) is printed on only one size (i.e. A4).
- Some rows could be skipped during replication on a Site that had active user sessions, causing inconsistencies in reports.
- Some documents are parsed and showing as B&W on Terminal but are printed and accounted as color.
- In some cases, printer cannot be activated with SQL error "Malformed string".
- Invalid SMTP port configuration (same port for SMTP and SMTPS) prevents **KNM** Server from receiving print jobs.
- Delegates of user groups are not synchronized from Central Server.

- Job files of not replicated jobs to Central Server are never deleted.
  - Aliases are incorrectly escaped in exported users CSV file.
  - User synchronization from Central to Site can fail in some cases when using user delegates.
  - Some internal tasks (which takes less than few seconds) can be executed twice instead of only once.
  - Credit account type is not translated.
- 

## 1.7 10.1 (patch 2)

12 May, 2023

### Security

- Domain credentials are stored in plain text in PHP session files.

### Improvements

- Added support for CPCA PCL6 jobs.
- Validity of generated refresh tokens increased from 1 day to 30 days. Used i.e. by Mobile Application for remembering login (logging in is required once in 30 days instead of every day).

### Bug Fixes

- Email that cannot be sent blocks all other emails from being sent.
- User is redirected from IP to hostname when Sign in with Microsoft is used causing logging in to fail.
- Easy Scan to Folder terminal action does not work after upgrade to 10.1 because of empty Title of terminal action.
- Searching for Printer or User with some specific characters causes Web Server Error.
- System maintenance's Database sweeping could not be started when Print Server is installed on the same server as Central Server.
- Duplex is not applied during job release on Embedded Lite for jobs uploaded via Web UI.
- Easy Config crashes when some service is not able to start with the "Start All" button.
- Parser has trouble recognizing color/mono of print files produced by Fiery print driver.
- Report Meter reading via SNMP grid view is not generated.
- User's jobs coverage level2 and level3 have incorrect values in Reports.
- Moving favorite job to different queue in Web UI removes the job's favorite attribute.
- User synchronization from Azure AD with more than 20 user groups doesn't finish successfully.
- Install Windows Printer from Queue - Printer models cannot be loaded from provided INF file.
- User synchronization - LDAP export to CSV after successful import is not working, causing Web Server Error.
- Password-protected Office files printed via Email or Web User Interface are not parsed and stop the processing of the following print jobs.
- User selection boxes sometimes do not show build in groups ("All users", "Managers", "Unclassified" options).
- Parsing of some XPS file fails.
- Incorrect link to REST API Apps in queue settings for receiving jobs via MS Universal Print instead of Connections settings.
- User synch from Azure AD fails caused by group name which contains the colon character.
- Users Export - Export of specific group does not work. All users are exported.
- Refresh token is not invalidated in case pin/card is removed.
- Progress bar for Restore database is not displayed immediately after confirmation of restore..
- Jobs remain paused state when printing via DC and with credit enabled.
- Large Easy Scan to email can cause errors in log and delivering scan multiple times.

- Scan to FTP results in 0kb file when TLS session resumption is enforced.
- 

## 1.8 10.1 (patch 1)

30 March, 2023

### Improvements

- Improved Easy Scan logging for further investigation in case of unexpected error.
- Parser of CPCA jobs improved.
- Traefik updated to version 2.9.8.
- OpenSSL updated to version 1.1.1t.
- PHP updated to version 8.0.28.
- Apache updated to version 2.4.56.

### Changes

- Changed "**KNM** Local/Central credit account" to "Local credit account" and "Central credit account" so it takes less space on terminals.

### Bug Fixes

- Report Projects - Project groups total summary does not display paper format values.
  - Easy Scan - Sending email to the Fax server destination fails.
  - Version of old terminal packages in not displayed in "Printers & Terminals" after upgrade.
  - Small UI improvements and fixed labels on login screen.
  - User without rights for project "No Project" cannot set/remove print jobs from favorites.
  - Cannot start user session (error Invalid parameter) on some terminals after upgrade to 10.1.
  - Authentication attempt by Azure AD credentials on Terminal causes Print Server service to crash.
  - PCL5e print files from Kyocera KX driver 8.3 get corrupted and contain garbled text on final print out.
  - Invalid External credit account settings causes internal server error API response.
  - Scan to SharePoint - Change of SharePoint URL in Connections is not applied immediately.
  - Watermarks on PCL6 job - document has wrong dimensions in landscape mode.
  - Cannot connect to Azure if HTTP proxy server was previously configured.
  - Some types of network adapters are ignored for the installation of the terminal.
  - Opening details of exception log message causes Web Application Error.
- 

## 1.9 10.1 RTM

2 March, 2023

### Security

- Refresh token is visible in log for refresh\_token grant\_type.

### Improvements

- Added **KNM** logo into IPP server.
- Used Google sign-in branding for Google connectors.
- Tenant ID and Client ID fields are in different order in each connector.
- Unified naming of Azure connection/auth server/sync source to Azure AD.

## Changes

- **MANUAL SETUP REQUIRED** New SharePoint setup required - After upgrade from older **KNM** versions, SharePoint connectors can stop working as a result of API change.

## Bug Fixes

- Printed job was not archived.
- Using codebook with MS exchange for Easy scan causes Internal server Error.
- HW-11-T - Cannot convert string from UTF-8 to ASCII.
- Easy scan - password parameter - the **KNM** web UI language is used for the string of password parameter.
- Removing Date filter for fixed range causes Web Server Error.
- Failed scan to incorrect email address may blocks outgoing email traffic.
- SMTP test dialogue stays open and the position is not correct when scrolling.
- Printer filter does not filter devices correctly in some cases.
- **KNM** Desktop Client not updating when enabling/disabling Credit or Quota when **KNM** Desktop Client is already connected to Print Server.
- Date and Time settings in the Fixed range filter acts differently.
- LDAP Code Book Favorites not on top.
- Parameters in Easy Scan - Codebooks - Exchange Address book causes Web Application Error.

---

## 1.10 10.1 RC2

14 February, 2023

### Security

- Fixed issue where any user could export users by using URL.

### Improvements

- Added support for CPCA print jobs.
- Apache updated.
- Added help text about unsupported variables to folder browsing terminal action.
- Possible to install **KNM** Central Server and Site Server on one server (smaller installation).

### Changes

- Increased [default sslProtocol](#) from SSL2 to TLS1.0.
- Site server - Removed option to add Authentication Servers.

### Bug Fixes

- Audit log export fails with an error.
- MS Universal Print - cannot print from Win 11.
- Job preview over Ghostscript finish with error.
- macOS Ventura AirPrint - stuck in the "Preparing..." message box.
- Sign in with Microsoft (SSO) from the mobile login page gives invalid grant.
- Jobs via email - Pooling interval cannot be changed.
- Easy Print - cannot print PNG file.
- Codebooks - Archived codes are still visible on Embedded terminal.
- Panel Scan fails to deliver - Attempt to read property "filenameTemplate" on null.
- Settings > Network - Test email dialog can be opened multiple times.
- Counters in Reports do not match on central after site replication in some rare cases.
- Terminal actions - Embedded terminal ignores user's language settings.

- Upgrade from 10.0 - Resetting dashboard to the default layout might cause Web Server Error.
- Easy Config - Service's state labels sizes are not unified.
- Cannot open Settings > Jobs after upgrade from 10.0 when Jobs via email are enabled.
- OneDrive Business cannot be configured as a single-tenant application.
- Login screen - Special License edition is not displayed.
- Easy scan - Filename Template - Space between variables is replace with "+" symbol.
- System History Deletion is deleting favorite codebooks.
- RefreshSettings is called every time when replications are requested.
- Terminal actions - Action needs to be saved twice to change name.
- Untranslated error messages on login screen - Authentication failed and Account locked.
- Sign in with Microsoft (user synchronized with upnPrefix as username) - Exception after login attempt.
- Fix of memory leak.

## 1.11 10.1 RC

### Improvements

- Site Server - Unused authentication servers are removed when users are synchronized from Central Server.
- PHP updated.
- Custom Theme - Terminal Actions settings reflect modified text from Theme Editor 1.2.0.
- Security improved.
- Traefik updated.
- Automatically prefilled the OAuth user in Email settings taken from Connection settings.
- [Database views](#) - Added Single color copy to Fact Session counters view.
- Network - [Connections](#) - Added additional information columns (Connected account and Details).
- Parser updated.
- Setting specific SSL protocol in [config.ini](#) also apply minimum version for traefik (traefik minimum version is TLS1 - i.e. when using SSL2 in config.ini, traefik will still use TLS1).
- Updated light themes (font color, centered labels).

### Changes

- Removed Parameters for panel scan to email from Scanning & OCR.
- Firebird version reverted back to 3.0.8.

### Bug Fixes

- Easy Scan - "Default" Filename template (%username%\_%scanId%) does not work.
- No translation of "No project" in metadata XML of scans.
- Report Project groups - Total summary wrongly contains user-related columns.
- Untranslated string appears when searching in project groups.
- Easy print - downloading remote files from Google Drive occasionally fails.
- Error when user connects box.com storage.
- Authentication to Exchange Online is not successful sometimes.
- Jobs via Email does not work when Network > **KNM** SMTP Server is disabled.  
Change - **KNM** internal SMTP Server is kept enabled, but firewall rules are removed when disabled.
- Easy Print from network location does not work - wrong path error.
- Security improvement.
- Easy Scan to network folder doesn't work.

- MS Azure sync source can be added on Site.
- System maintenance task is not deleting failed email attachments.
- Report Printers - Total summary - data are not grouped correctly.
- Job parser could fail in some specific cases.
- Web server error after user changes own password and navigates through Web UI.
- Possible to save deleted SMTP connection which was deleted before saving SMTP settings.
- Terminal action's text parameter is not validated by specified regEx validator.
- Server ignores state parameter in authorization grant request from Mobile application using SSO.
- Not possible to mark job as favorite.
- Setting rights for users on Site to "Manage project" does not allow user to "Manage Projects" on site.
- Site server mode - Possible to create User rights with keyboard shortcut.
- Job Roaming - roaming job is canceled right after download if there is more than 10 sites.

## 1.12 10.1 BETA3

### Improvements

- Added support multiline text field in terminal vendor specific settings.
- Simplified adding new [reports](#).
- Translations - Unified translation strings for quota period.
- Added new translation string for "remaining" (required by some languages with different sentence composition).
- Improved debug logging for SMTP server with OAuth login.
- Firebird updated.
- Added support for Bearer token authentication on the IPP Server.
- OpenSSL updated.
- Added new option for IPP (mobile application) to enable both punch and staple at once.
- Security improved.
- Traefik updated.
- Removed Prescribe when printing from Kyocera drivers to non Kyocera devices.
- **NEW FEATURE** [DB views](#) - Added new view for Printer events.
- **NEW FEATURE** [DB views](#) - Added new view for Toner replacements.
- [DB views](#) added new view FACT\_PRINTERJOB\_COUNTERS\_V3.
- [DB views](#) - added more information to DIM\_USER and DIM\_PRINTER.
- Added option to set custom **KNM** CA certificate validity period (in config.ini).
- Easy Scan - Possible to set Filename template on General tab for all destinations of Easy Scan.
- Added support for SSO for mobile login page.

### Changes

- PHP upgraded to version 8.0.
- Removed option to sort jobs by sites.
- [SMTP Settings](#) separated for Gmail and MS Exchange Online.

### Bug Fixes

- Disconnected printers are still in the status Ready.
- Payment account interaction is not Disabled if accounting is switched from Accounting group to Cost center mode.
- Cannot create Report Quota status for groups/Users with empty filter.

- **KNM** Service could crash in some very rare cases during releasing of jobs when one user had 2 user sessions active.
- Reports "General- Monthly Statistic/Weekly Statistics" - values for same week/month of different year is merged to one value.
- Saving changes under Method of printing (Settings - Jobs) does not work, it defaults to Convert to PDF.
- Printer discovery - Actions - cannot add printer model for Windows printer.
- CSV User import may fail when updating existing users.
- Deleted themes appear again in the list of themes.
- Helpdesk.xml file is invalid.
- Google Drive scan storage destination may appear as disconnected in Web UI.
- Fulltext search of specific job takes too long.
- Sorting users (with credit enabled) by specific column takes too long.
- Export of 100K users takes hours.
- Account lockout triggered after fewer attempts than set.
- No terminal can be searched for by "n" but not by "no".
- Print Server changes finishing options for booklet (Kyocera drivers).
- Easy scan - scan to multiple email recipients - email addresses are not split.
- Credit and Quota right-click menus on Users tab requires page refresh after enabling Credit/Quota to be available.
- Printer discovery is in loop when invalid filename template file is used.
- Wrong Synchronization of user accounting group/Cost center after changing Accounting mode on Central Server.
- traefik.exe security improved.
- Terminal package status is not updated after Health check detected some problem which was resolved.
- Security improvement.

## 1.13 10.1 BETA2

### Improvements

- PHP updated.
- Warning message about incompatible terminal version has been improved.
- New icon for Easy Print terminal action.
- Traefik updated.
- Web Administrator links are using icons from Easy Config.
- Folder browsing - behavior when setting up multiple destination improved.
- Central-Site communication without VPN improved.
- CounterHistory replication performance improved.

### Changes

- Reports in PDF do not contain seconds in time (other formats has time including seconds).
- Quick setup guide widget is collapsed when all steps are Done with option to remove this widget.
- Possible to set how long to keep Audit log records ([System Management](#) > History) instead of deleting it with Log records.
- Simplified adding External [Connection of Gmail](#).
- Easy Config UI change to match Red theme of Print Server UI.
- Task Scheduler - shortest period can be set to 5 minutes (instead of 1 minute).
- Search field in Audit log removed.

## Bug Fixes

- Unable to start Print Server if Email refresh token is missing.
- Standalone mode - Jobs settings contain Job roaming settings.
- Easy Print - print job defaults - Copies can go to negative and above 999.
- MPA - not possible to print other formats than A4 (requires MPA 1.3 (patch 1)).
- Not possible to export Audit log.
- Easy Scan to OneDrive fails.
- User cannot manage reports even with manage reports rights.
- Relogging to Web UI opens page from where user/admin logged out.
- Labels in Easy config were empty for some languages..
- Easy Scan - Scanning to second destination fails if the first one has folder browsing enabled.
- Date selection for Reports, Logs for fixed date is not save correctly.
- Printer discovery with CSV name template is stuck on adding printer from CSV.
- User synchronization from Central - Inherited manager for nested groups in not synchronized.
- Kyocera terminal wasn't possible to install with default server certificates on newer devices.
- MS Azure authentication server - creating new connection is not automatically set to be used.
- Credit Statement and Credit reports data are deleted based on settings of "Delete logs older than".
- Cannot set duplex option on embedded terminal for jobs via email or web upload.
- User synchronization fails when group name contains half-width and full-width characters.
- Possible to assign project to user without rights to project via Web UI Jobs.

## Device Certification

- Changed device name of P-3563DN to P-C3563DN and P-4063DN to P-C4063DN.
- 

## 1.14 10.1 BETA

### Improvements

- **NEW FEATURE** Added banner for expired or to be expired assurance (perpetual license only).
- **NEW FEATURE** Added printer pages for last 30 days widget.
- **NEW FEATURE** Environmental Impact widget.
- System status in displayed on the dashboard as a normal widget.
- **NEW FEATURE** Mixed size parameter for Easy copy is supported.
- Added digital signature to EasyConfigCmd.exe.
- Email Printing - feature is disabled when invalid configuration is given.
- Job via File upload and Easy Print - Job properties description added.
- **NEW FEATURE** BI tools - New database views for Session and Job environmental impact.
- Settings form for Jobs via Email improved.
- **NEW FEATURE** High Contrast UI Theme for improved accessibility.
- Notify the Desktop Client about paused jobs when the client is registered into the server.
- <https://myq-online-help.atlassian.net/wiki/spaces/PS/pages/957776266> - UI improvements.
- Date Range control UX and accessibility improved.
- AutocompleteBox UX and accessibility improved.
- **NEW FEATURE** Easy print from Box.com.
- Support of punching, stapling, paper format attributes via IPP printing.
- **NEW FEATURE** [New default theme](#).
- Server Health Checks UI improved.
- **NEW FEATURE** Easy print from Dropbox.
- Web UI - Removed loading animation after health checks.

- **NEW FEATURE** Easy scan to DropBox- option to browse subfolders (to select final destination).
- **NEW FEATURE** Toner replacement [report](#).
- **NEW FEATURE** Easy scan to SharePoint - option to browse subfolders (to select final destination).
- **NEW FEATURE** Easy print from local and network folder.
- **NEW FEATURE** Easy print from Google Drive.
- **NEW FEATURE** Easy print from SharePoint.
- **NEW FEATURE** Easy print from OneDrive for business.
- **NEW FEATURE** Easy print from OneDrive.
- Web UI performance of Jobs page improved in case of big amount of jobs.
- **NEW FEATURE** [Azure AD](#) user synchronization via MS GRAPH API.
- **NEW FEATURE** Easy Print (requires embedded terminal 10.1+).
- **NEW FEATURE** Added option to edit filename of scanned document (enabled in Easy scan action).
- Gmail External system - possible to re-add External system using same id and key.
- Traefik updated.
- OpenSSL updated.
- Security improved.
- Replacing expired Certificate of PM Server.
- Renamed "SPS/SJM" log subsystem to "**KNM** Desktop Client".
- Added "Edit Columns" action in the Tools menu in the Credit Statements.
- **NEW FEATURE** New report '[Project - User Session details](#)'.
- Simplified dialog for reprinting jobs in Web UI > Jobs.
- User synchronization - invalid syntax of PIN of one user won't interrupt the whole synchronization.
- License error notification emails is sent after 3 failed connection attempt instead of first one.
- When removing user's rights for project, delete this project from all user's jobs.
- Project assignment to the existing print jobs when enabling/disabling Project accounting.
- Deleting specific project - project assignment is removed from jobs using this deleted project.
- Changed some System health check messages to be more clear.
- Gmail and MS Exchange Online - possible to use different email accounts for send and receive emails.
- Print jobs encryption.
- User Synchronization - removed spaces in the email field before import (email with spaces is considered invalid).
- Performance of Health checks improved.
- Performance of Web UI improved.
- **NEW FEATURE** Easy scan to Google Drive - option to select root folder and browse subfolders.
- **NEW FEATURE** Easy scan to OneDrive and OneDrive for business - option to browse subfolders (to select final destination).
- **NEW FEATURE** Easy scan to folder - option to browse subfolders (to select final destination).
- Increase character limit of Printer Event actions email body and subject.
- Possible to specify port range for FTP communication in Network settings.
- Create relation between new and old accounting table in the DB for External Reports.
- **NEW FEATURE** Jobs and Log database encryption.
- Errors/Alerts of Easy Config (i.e. Embedded terminal services not running) are registered by System Health Check.
- **NEW FEATURE** Job preview for Embedded terminals and Mobile application.
- Easy Config's setting and database tab performance improved.
- **NEW FEATURE** [Toner replacement monitoring](#) report.

- **NEW FEATURE** Mixed size parameter for Easy copy is supported..
- **NEW FEATURE** Option to use device's serial number as device admin password.
- Server performance improved after importing large number of users.
- System Maintenance error after upgrade - recalculate indices individual table and log individual problems.
- Adding terminal package - Added note, that newly added terminal will run under localsystem account even **KNM** services are running under defined user account.
- **NEW FEATURE** Added option to [always display job price](#).
- MAKO (job parser) updated.
- **NEW FEATURE** 3 levels of [Job Parser settings](#).
- **NEW FEATURE** [Sign in with Microsoft](#) to Web UI.
- **NEW FEATURE** Added "Print grayscale with black toner" switch to queue setting.

## Changes

- [New dashboard default layout](#).
- Self signed **KNM** CA certificate is valid for 730 days (because of **KNM** Desktop Client for Mac).
- External systems UI moved and renamed to [Connections](#).
- AWS - Moved bucket and region configuration from scan profile destination to Cloud service definition.
- Hide Job receiving tab for Easy Print, Web and Email queues.
- Quick setup - Removed step Queues.
- New built-in queue for Easy Print.
- Possible to move job to another queue in Web UI > Jobs.
- User properties - renamed "User's scan storage" to "User's storage".
- Removed information about **KNM** version from **KNM** Web UI login screen.
- Remove toner related columns from database Printers table (moved to supply table).
- VC++ runtime updated.
- Renamed Smart job manager firewall rule to "**KNM** Desktop Client".
- Job actions in Web UI - Renamed "Push to print queue" action in Jobs menu to "Resume".
- Projects - User can login to terminal when user has no project assigned.
- OCR formats using Abby engine deleted after upgrading to OCR Server v3+ (supported formats are PDF, PDF/A, TXT).
- Maximum upload file size separated for Jobs (moved to Settings > Jobs > Jobs via Web) and other (i.e. uploading terminal package).
- **SYSTEM REQUIREMENT** .NET6 is required.
- System users are hidden in Web UI (except option to set \*admin as email recipient).
- Empty groups with active rules are not automatically deleted during user synchronization.
- Removed option to use custom PHP scripting on the metadata file in Job archiving feature.

## Bug Fixes

- Built-in Certificate Authority generate from PS not working on macOS.
- User CSV export/import does not reflect multiple Cost Centers.
- Codebooks - when searching value by "Code", no result is found.
- Upgrade of terminal package activates/installs even deactivated printers.
- LDAP User Synchronization - switching tab without server/username/pwd filled causes web server error.
- Space in user name causes failure to upload the scanned file to OneDrive Business.
- Error when scanning with ProjectId=0.
- HW Code contains same hash for CPU and UUID.
- Database upgrade could fail in some cases.
- Log highlights are not exported to Data for support.
- Scan via SMTP - Scan does not arrive when Printer is saved under Hostname.

- LPR Server stops accepting print jobs.
- "Service **KNM**\_XXX not running" is falsely reported right after services have started.
- System management - Maximum upload file setting is present.
- Possible to save invalid value (null) in database, when enabling jobs via email (OAuth) causing web server error.
- Duplicated login prompt for user login of **KNM** Desktop Client, when job is paused and projects enabled.
- Release blocked credit in user's detail does not work.
- Print server crash when database is unreachable during job accounting.
- Web UI - Columns in sidebar grids behave inconsistently.
- Easy config health checks exceeded the timeout of 10 seconds.
- Parsing of specific PDF document failed (document trailer not found).
- Counters history is never successfully replicated when printer has no MAC address.
- Refreshing filtered (some timeframe) Log causes Web server error.
- Terminal actions - Code Book parameter's Default value is removed after change of a field or 2nd save.
- Renaming a project does not affect print jobs that have already been printed with this project.
- Delete operation is inconsistent in **KNM** web UI.
- MS Exchange Address Book connection does not work.
- Missing translation of Job rejection reason 1009.
- Log export to Excel: accented characters are corrupted.
- DB upgrade could fail in some cases when upgrading 10.0 Beta to 10.0 RC1 and RC2.
- Job roaming - Issue downloading larger job files to other sites.
- Report preview fails with any language other than English.
- Offline login - Synchronized data not invalidated after PIN/card deletion.
- Using LDAP server with auto-discovery causes Web server error when adding user synchronization.
- In some cases System health check fails (Failed to create COM object `Scripting.FileSystemObject`).
- System health check takes too long in some cases and may time out.
- Second level context menu is too transparent in Edge/Chrome browser.
- Cost Centers: Quota account is not reported when the same user is logged in into two devices using the same quota account.
- Adding support license deactivates licenses for a brief time.
- Upgrade from 8.2 - Database upgrade fails if database is encrypted.
- Job scripting - queue policies are not applied when MoveToQueue method is used.
- Adding MS Exchange SMTP Server in Network settings causes error.
- Wrongly displayed Color settings of job on terminal for B&W document uploaded via Web UI.
- Running print discovery immediately again causes Web server error.
- DB encryption of larger DB - statusbar hangs and does not finish.
- Services may not start after silent upgrade in some cases.
- Apache is not reconfigured when hostname is changed.
- Terminal uninstallation - Recent jobs (last 1 minute) are accounted once more to \*unauthenticated user.
- Widgets - Graphs are disproportional.
- "Revert force mono/Force mono" of job displayed on terminals in Color option instead of BW/Color.
- Printer Events > Toner Status Monitor event - history is missing status of each toner.
- Printer properties - Password can be only 16 characters (conf profile accept up to 64 chars).
- Easy Config crashes on Open file dialog for db restore location when link with location was opened prior to restore.
- Health checks are spamming the log when they're not resolved.
- Web Printing - color selection displays incorrect options.

- Terminal Actions - External Workflow - URL is empty when action is reopened.
  - Reports - aggregate column's Average operation is not working (shows sum).
  - Replication stops working after Site is restored from DB backup.
  - Mopria print is not working.
  - Error when adding column in User group membership Report.
  - Column "Personal number" can be added 2 times in Projects per user report.
  - Reports - Incorrect error message when file with logo was deleted.
  - Log Notifier - Rule text in e-mail multiplied.
  - Reports - Row summary "Sum" for countless fields is available.
  - Reports - Different results for Auto Align of columns of same type (left or right).
  - Reports with job privacy - different results in report preview and fully generated report.  
Note that summary reports of jobs and printers only shows jobs owned by the user.
  - Printer activation successful but with logged message "Printer registration failed with code #2:".
  - Parsing of specific job could fail.
  - It's possible to add one element several times in autocomplete box.
  - Quota - print job (bw+color pages) allowed when Color + Mono quotas are monitored and only bw or color quota is remaining.
  - Easy Config - incomplete Network path for DB backup folder when path is set in Task Scheduler.
- 
-

## 2 Basic Information

---

### 2.1 KYOCERA Net Manager Servers and applications

**KNM** is a distributed system made of servers and client applications. Here you can find a description of all the components and main communication channels. Each component usually runs on its own computer be it a server, a PC, a mobile phone, or a printer.

The **Central Server** is responsible for **Site Servers** configuration, reporting, and licensing. Site Servers still need additional individual configuration.

A **Site Server** is responsible for print job spooling, scan delivering, user interaction with printers, printer monitoring, and many more.

**KNM Desktop Client** is an additional application running on users PCs. It offers user authentication and identification, project and cost-center selection, local printers monitoring (mostly USB), client spooling and many other features.

The **OCR Server** is used for Optical Character Recognition on scan jobs. An OCR server uses lots of resources, so it usually runs on its own machine.

**Mobile Print Agent** gives users access to printers via AirPrint (for iOS), and Mopria Print Service (for Android smart phones or tablets). It usually runs on its own machine with access to a Wi-Fi network where mobile devices can discover it.

### 2.2 Print Server from the OS process perspective

This is a description of what OS processes are running on a Print Server, and what the main communication channels are.

The heart of the system is the **Print Server**. It's based on the WSF Platform – **KNM**'s platform for network services development. **KNM** specific logic is implemented as Platform services, which are packaged in **plugin\*.dll** files. These plugins are written in C++ and a few of them also in C#. WSF Platform also supports services implemented in PHP. PHP doesn't support DLLs, so the platform services implemented in PHP are invoked via a set of **php.exe** workers.

The **Print Server** also manages a set of **Job Processor** workers which are used for job parsing. The **Job Processor** is running as a process and not as a part of the **Print Server**, to avoid its failure in case of the **Job Processor's** failure.

As a network server, **Print Server Service** is responsible for receiving print jobs via LPR, IPP, and other protocols. It also handles Messages, which is our push-notifications engine. Messages are used to notify clients about events in the system.

**Apache** is an HTTP server for our Web UI and **KNM** REST API. Both applications are implemented in PHP. Apache is maintaining a set of **php-cgi.exe** workers to handle execution.

**HTTP Router** is our reverse proxy through which all incoming HTTP based traffic flows. It's main functionality is TLS termination.

**Terminal Packages** implement the embedded terminal for a specific vendor. They expose their own API used by the printers.

**PM Server** is a component created by Kyocera. It provides API to configure Kyocera devices and to install the embedded terminal application. PM Server uses the Thrift technology to implement its API. **KNM** is also providing part of its API via Thrift, so PM Server can access it.

Many of the components use the **Database Server** to store data. Furthermore, many of the components including Firebird, store their data in the **KNM Data Folder** which is located by default in *C:\ProgramData\Kyocera\KYOCERA Net Manager\Data*. In production, this folder is typically located on a network drive.

## 2.2.1 Executable names

Friendly name	Executable name	Alternative names
HTTP Router	traefik.exe	Traefik
HTTP Server	httpd.exe	Apache
Database Server	firebird.exe	Firebird
Print Server	KNM.exe	
Kyocera Provider	knum.server.exe	PM Server
*Terminals	KNM*Terminal.exe	Terminal Package
Job Processor	KNMJobProcessor.exe	

\*used for vendor name

## 2.3 Network Communication Architecture

This is a description of the main network communication channels.

**KNM --> License server:** An external connection to the **KNM** license server is required for license activation.

The connection is protected via 443 TCP. If a connection to the license server is not possible, there is also the possibility of offline activation.

**KNM <--> Active Directory:** User synchronization (LDAP/ Open LDAP) takes place via port 389 or 636 by default.

**KNM --> Email Server:** Scans/emails are first transmitted from the MFP to **KNM** server. This server acts as a relay for emails and forwards the emails to the stored customer email server. The required ports are individual, depending on the corresponding settings of the customer email server.

**KNM --> KNM Web UI:** HTTP protocol for accessing the **KNM** web interface as well as communication with embedded terminals and job roaming between **KNM** servers:

*https://:serverhostname:8090*

If needed, the unsecure connection can be enabled in **KNM** Easy Config, using port 8080.

**KNM --> Print job Release:** The output of the print jobs from **KNM** server to the MFP is done via RAW 9100 by default (can be changed if required LPR, IPP, IPPS, MPP, MPPS).

The device status of the printing systems, as well as toner and ink stands, are read out via SNMP UDP 161. (SNMP protocol can be changed if required SNMP v1, SNMP v2, SNMP v3).

**KNM <-- Scanning via MFP:** All scans (email/folder) are done via port 25 by default, FTP port 21 if required.

**KNM <-- BYOD:** For working with smartphones/tablets, with AirPrint/Mopria, ports 8632 and 8090 are required.

**KNM <-- User Clients:** Printing to a **KNM** queue is done via a print object configured for this purpose. By default, printing to the **KNM** server is done via LPR port 515.

## 3 System Requirements

**⚠** The operating system and other software require their own additional system resources. The system requirements described below are only for **KNM**.

### KNM Print Server - Standalone mode

#### KNM Print Server HW requirements up to 600 devices:

	1-10 devices	11-100 devices	101-300 devices	301-600 devices
<b>Physical Core*</b>	3	4	6	8
<b>RAM</b>	6GB	8GB	12GB	14GB
<b>Storage space</b>	30GB	33GB - 350 GB	380GB - 1TB	1,4TB - 2TB

\*It is recommended to use +1 physical core if Credit/Quota is used.  
(calculated with AMD Ryzen Threadripper 1920X 3,5GHz)

#### Valid for a typical use case:

- Print job spooling via Windows spooler or directly to **KNM** print queue
- Integrated Firebird database - installed automatically
- Activated Job Parser
- Activated Job Archiving
- High number of Office documents printed via email/web/mobile
- Use of **KNM** Desktop Client
- Watermarks used in queues
- Heavy usage of **KNM** API
- 170 users per device (up to 100 000 users total)
- Heavy printing
- 30% active user sessions at once
- Embedded terminal installed on all devices

#### Recommendations:

- Install Windows updates out of working hours.
- Always monitor the server performance during peak usage hours and adjust the settings accordingly.

### KNM Print Server - Site mode (Central Server & Site Servers architecture)

#### Site servers HW requirements up to 30 000 devices:

	1-10 devices	11-100 devices	101-300 devices	301-600 devices	601 - 30 000 devices
<b>Physical Core</b>	5	6	8	10	10
<b>RAM</b>	6GB	8GB	12GB	14GB	14GB
<b>Minimum number of servers</b>	1x Central server 1x Site server	1x Central server 1x Site server	1x Central server 1x Site server	1x Central server 1x Site server	1x Central server More Site servers with max 600 devices each
<b>Storage space</b>	30GB	33GB - 350GB	380GB - 1TB	1,4T - 2TB	2TB per 600 devices

(calculated with AMD Ryzen Threadripper 1920X 3,5GHz)


For the **KNM Central Server** HW specification, check the **KNM Central Server** guide.

**Valid for a typical use case:**

- Print job spooling via Windows spooler or directly to **KNM** print queue
- Integrated Firebird database - installed automatically
- Activated Job Parser
- Activated Credit Accounting
- Activated Quota
- Activated Job Archiving
- High number of Office documents printed via email/web/mobile
- Use of **KNM** Desktop Client
- Watermarks used in queues
- Heavy usage of **KNM** API
- 170 users per device (up to 100 000 users total)
- Heavy printing
- 30% active user sessions at once
- Embedded terminal installed on all devices
- User synchronization from Central Server
- Data replication to Central Server

**Recommendations:**

- Install Windows updates out of working hours.
- Always monitor the server performance during peak usage hours and adjust the settings accordingly.

 It is possible to install **KNM** Central Server and **KNM** Site Server on one Server, but it is recommended only for small installations (small Site Server). In this case, the HW requirements for both **KNM** Central and **KNM** Site Server need to be taken into account.

**Storage:**

The **KNM** Print Server installation files are approximately 700MB.

The annual printing volume for 1 printer is approximately 10,000 jobs; it is possible to multiply this value for the particular number of printers.

KNM data folder (jobs, main database, and log database increasing):		
10k jobs	100k jobs	1M jobs
35GB	300GB	3,5TB

Counted for jobs with 2,9MB size.

By default, jobs are deleted every 7 days.

The Job archiving feature needs additional free space in data storage due to used configuration.

A dedicated disk for **KNM** Data storage (jobs, main database and log database) is recommended.

During upgrades of the **KNM** Print Server system, the actual size of the **KNM** installation on the server (including **KNM** database) may temporarily grow up to four times.

The size of the **KNM** database depends on the size and complexity of your printing environment (number of users, printing devices, sent jobs etc.).

#### **Storage performance:**

- minimum 100 IOPS required.
- RAID data storage supported.
- for systems with a large number of direct queues, it is strongly recommended using SSD.

#### **KNM Desktop Client:**

If there are 100 - 1000 or more client computers using **KNM** Desktop Client, the **KNM** Print Server requires 2+ physical cores just for the **KNM** Desktop Client operations. The recommended configuration may vary according to the system load.

#### **Recommended no. of users and groups:**

**Users:** up to 100,000 (30,000 - 60,000 per one synchronizing line). Depends on the length and number of fields for synchronization.

**Groups:** up to 40,000/10 tree levels (group in group in group). Each user can be in up to 50 groups.

#### **Operating System:**


Windows Server 2012/2012 R2/2016/2019/2022, with all the latest updates; only 64bit OS supported.  
Windows 8.1/10/11\*\*, with all the latest updates; only 64bit OS supported. Be aware of the connection limit of up to 20 clients ([Windows EULA](#)).

\*\*For the trouble-free running of the machine, it is strongly recommended using a Windows Server OS.

#### **Additional software required:**

- [Microsoft .NET Core 6.0](#)
- [Microsoft .NET Framework](#) (any version recommended by Microsoft)


- For Windows Server 2022, it is necessary to install Server Core App Compatibility Feature on Demand (FOD) ( <https://docs.microsoft.com/en-us/windows-server/get-started/server-core-app-compatibility-feature-on-demand> )  
It can be installed from PowerShell as a Windows Update using this command: "**Add-WindowsCapability -Online -Name ServerCore.AppCompatibility~~~~0.0.1.0**" and then restart.

 Microsoft .NET Core 6.0 is installed automatically at the beginning of the **KNM** installation. If the installation fails, the installer cannot proceed, and the installation is terminated. In such cases, .NET Core 6.0 has to be manually installed prior to the **KNM** installation.

Microsoft .NET Framework is not automatically installed and needs to be installed prior to running the **KNM** installation.

### Web browser:

- Microsoft Edge 91 or higher (Recommended)
- Google Chrome 91 or higher
- Mozilla Firefox 91 or higher
- Apple Safari 15 or higher
- Opera 82 or higher
- Internet Explorer and MS Edge Legacy are no longer supported

 WebSocket notifications only work with valid certificates in some browsers. Some **KNM** features may have limited functionality without them, and it's recommended to have them valid and installed on all client devices.

### Security:

DigiCert Global Root CA certificate (required for Installation Key license activation) → <https://www.digicert.com/kb/digicert-root-certificates.htm#roots>.  
It should be included by default in the latest updated Windows versions.  
Supported Public Key Infrastructure for asymmetric cryptography.

### KNM installation in Private cloud:

**KNM** can also be installed in Private Cloud. For requirements and further details, see [Installation in Private Cloud](#).

### Limitations:

- To make sure that the **KNM** system runs smoothly, you need to set an exception for **KNM** in your antivirus setup.
- **KNM** should not be installed on a Domain Controller.

## 3.1 Installed parts and possible conflicts

The installation file contains, besides the **KNM** system itself, installations of a Firebird database server, an Apache web server, PHP runtime, and PM server. With the Scan Management function activated, the **KNM** system uses its own SMTP server.

If there are other systems that run on the same server and use databases, web interfaces, PHP, or email servers, there is a risk of system conflicts. These conflicts can cause malfunctions on one or more of the systems. Therefore, we recommend you install **KNM** on a server with a clean OS installation.


**KNM** fully supports installation on virtual servers.

## 3.2 Main Communication Ports

If you need to adjust your firewall, it is recommended to allow **KNM** processes in the firewall and not particular ports. If you allow particular ports, **KNM** may stop working if:

1. you change port settings in **KNM**, or
2. you upgrade to a newer version and the port specification has changed.

Terminal packages may use additional ports. Check the particular terminal package specification for details.

 Make sure to create an exception that allows ICMP Echo Requests/Replies (Ping) through your Windows Firewall, as **KNM** uses it by default to check the printers' status.

### 3.2.1 Incoming Ports

The server is listening on the following ports (does not include private ports):

Protocol	Port	Configurable	Description
TCP	21	Yes (WebUI)	FTP protocol for receiving scans. The server runs only in passive mode and each data connection runs over a dynamic port in the 49152 - 65535 range.
TCP	25	Yes (WebUI)	SMTP protocol for Scan Management function, receiving email notifications from printers, and for receiving emails with jobs.
TCP	587	Yes (WebUI)	SMTPS protocol. Used in the same scenarios as SMTP.
TCP	515	Yes (WebUI)	LPR protocol for print job transmission to the <b>KNM</b> server.
TCP	9100	Yes (WebUI)	RAW protocol for print job transmission to the <b>KNM</b> server.

Protocol	Port	Configurable	Description
TCP	8631	Yes (WebUI)	IPPS protocol for print job transmission to the <b>KNM</b> server.
TCP	8632	Yes (WebUI)	AirPrint/MOPRIA protocol for print job transmission to the <b>KNM</b> server.
TCP	8090	Yes (Easy Config)	HTTP protocol for accessing <b>KNM</b> web interface, communication with Embedded terminals and job roaming among <b>KNM</b> servers.
UDP	11112	No	Communication with <b>KNM</b> Desktop Client. The answer is returned on a dynamic port in the 49152 - 65535 range.
UDP	11108	No	Communication with old terminals (7.6 and older).
TCP	8080	Yes (Easy Config)	Upgrade only. Obsolete HTTP protocol for accessing <b>KNM</b> web interface, communication with Embedded terminals and job roaming among <b>KNM</b> servers. Can be removed in Easy Config and only 8090 can be used.

### PM Server:

Protocol	Port	Configurable	Description
TCP	631	No	Port for Mobile print via IPP.
TCP	717	No	Port for Mobile print via IPPS.
TCP	9090, 9091	No	Necessary for remote setup of Kyocera embedded terminals.
TCP	9092	No	Felica reader
TCP	9093	Yes (WebUI)	Authentication / Authorization.
TCP	9094	No	Driver access, mobile access.
TCP	9095	Yes (WebUI)	Spooler service.

Protocol	Port	Configurable	Description
TCP	9097	Yes (WebUI)	Log information event.
TCP	9098	Yes (WebUI)	Job status event.
TCP	9099	Yes (WebUI)	Thrift access.
TCP	9101	No	User session service.

### 3.2.2 Outgoing Ports

The server is connecting to the following ports (does not include localhost connections):

Protocol	Port	Description
TCP	443	<ul style="list-style-type: none"> <li>• IPPS protocol for print job transmission from <b>KNM</b> to printing devices.</li> <li>• License activation server.</li> <li>• Other enabled services from Settings → Connections (Microsoft Universal Print, One Drive, ...)</li> </ul>
TCP	515	LPR protocol for print job transmission from <b>KNM</b> to printing devices.
TCP	631	IPP protocol for print job transmission from <b>KNM</b> to printing devices.
TCP	9100	Raw protocol for print job transmission from <b>KNM</b> to printing devices.
TCP	10040	MPP/MPPS protocol for print job transmission from <b>KNM</b> to printing devices.
UDP	11108	Communication with old terminals (7.6 and older).

You can also setup additional services that require further configuration and their port will often differ:

Protocol	Port	Default	Description
TCP	Custom	110	Connection to email server via POP3 protocol for receiving jobs via email.
TCP	Custom	143/993	Connection to email server via IMAP/IMAPS protocol for receiving jobs via email.

Protocol	Port	Default	Description
TCP	Custom	25/465/587	Connection to SMTP server for sending outgoing emails from <b>KNM</b> .
TCP	Custom	389/636/1812	Connection to Authentication server(s) (LDAP, Radius, ...) for user authentication/synchronization.
TCP	Custom	8093	Connection to <b>KNM</b> Central Server.
UDP	Custom	161	SNMP protocol for communication with printing devices. Answer from printer is returned on a dynamic port.
TCP	Custom	-	Connection to External credit account.


**KNM** can connect to dynamic ports in the following contexts:


Protocol	Port	Description
UDP	Dynamic	Communication with <b>KNM</b> Desktop Client. The port range is 49152 - 65535.

### 3.2.3 Embedded Packages Ports

Kyocera	
<b>If SSL is on, it's used for the following events:</b>	Events are notified internally to the embedded application. No network communication is used.
<b>KNM Server (Protocol: Port - Description)</b>	<ul style="list-style-type: none"> <li>• HTTP or HTTPS: 8090 (default) - it depends on the configuration in <b>KNM</b> Easy Config.</li> <li>• SMTP: 25 (default) - it depends on the port configured in <b>KNM</b>, Settings, Network, SMTP. Used for Panel Scan to email)</li> </ul>
<b>Package (Protocol: Port - Description)</b>	<p>HTTP: (IN) 8081 to 8089 (default) - It depends on the port selected during the installation of the package on the server. This is used only in localhost.</p> <p>TCP: (OUT) 11108 - TCP link to device. Send request to Printers.</p> <p><b>Kyocera 8.0+</b> A random TCP port is opened on each package service start/restart, to be used for receiving scans over FTP. The package then tries to configure the Windows firewall to open the port for outside connections.</p>

<b>Printer (Protocol: Port - Description)</b>	<p>TCP: (IN/OUT) 11108 - TCP link to device. Usage: Receive requests from Package.</p> <p>TCP: (IN) 10040 - Usage: Use printer as a proxy for TCP communication.</p> <p>UDP: (IN) 11108 in - UDP Link to device. Multipurpose. It dispatches all the received UDP packages. Usage: Receive requests to get local jobs.</p> <p>UDP: (OUT) 11108 - Send broadcast to printers. GetJobs (Local Spooling)</p> <p>TCP: (IN/OUT_ 10030 - TCP link to device. Usage: Receive requests or responses from other devices.</p> <p>TCP: (IN) 10010 - Usage: Receive raw data of print jobs for local direct print job.</p> <p>TCP: (IN) 10011 - Usage: Receive raw data of print jobs for local hold job.</p> <p>TCP: (IN) 10013 - Usage: Receive raw data of print jobs for local delegate job.</p> <p>TCP: (IN) 10020 - Usage: Receive raw data of print jobs for local LPR jobs.</p> <p>TCP: (IN) 10012 - Usage: Receive raw data of print jobs for local Print&amp;Follow jobs (Print&amp;Follow).</p> <p><b>Note:</b> Other ports used by the printer (common for all printers. Eg. 9100 for raw printing, etc.).</p>
---	--

 Some of the above mentioned ports can be changed in case of conflicts with other applications.

 Conflicts of the communication ports with other software will be revealed by the **Windows socket error 10048** error message.

### 3.3 Windows Server Performance Monitor

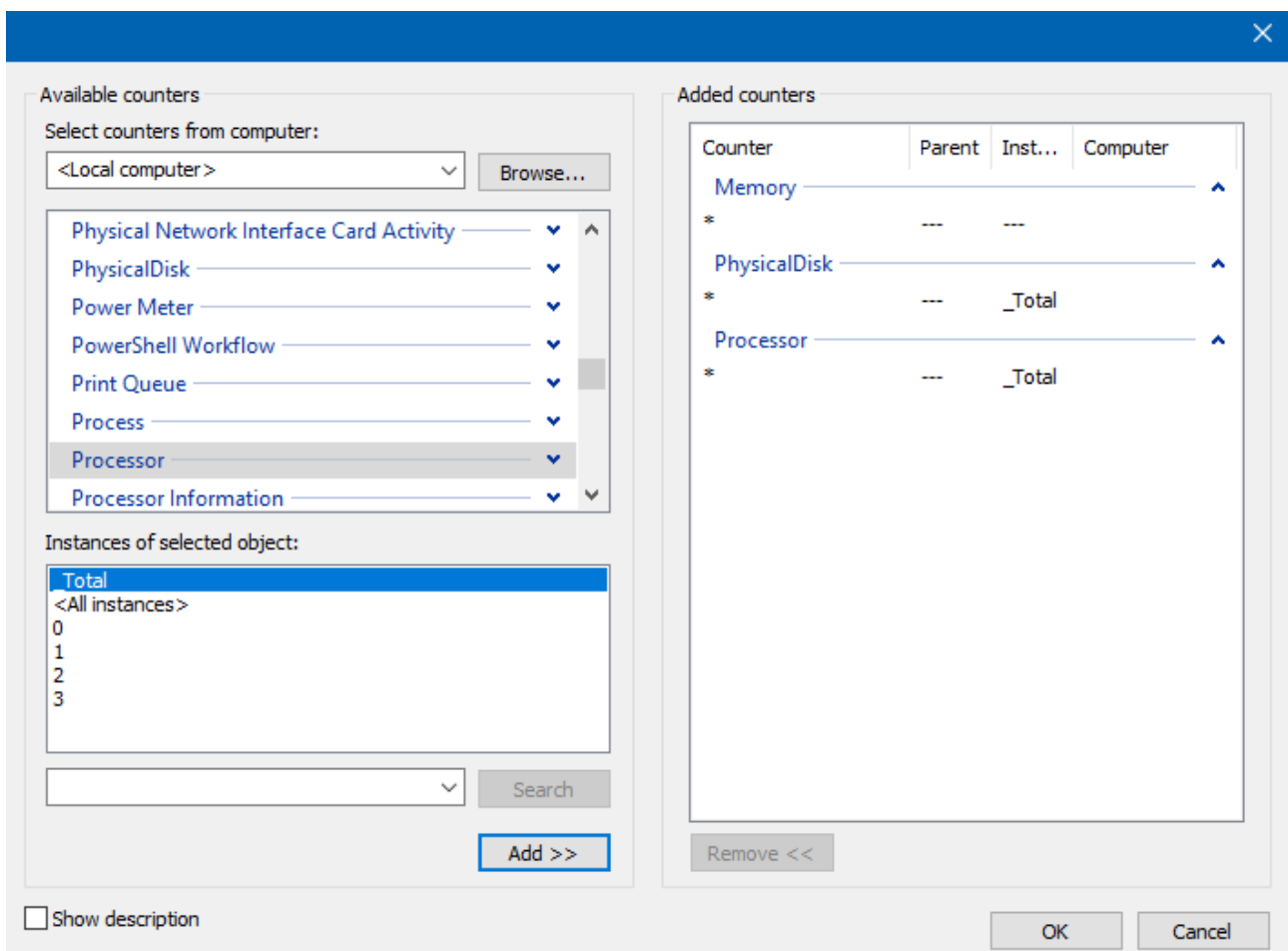
You can use Windows Server Performance Monitor to gather system performance information that can help your support to troubleshoot **KNM** server performance issues.

The following procedures describe how to configure Performance Monitor to log processor, disk, and memory performance information, respectively.

#### Enabling performance counters for processor, disk, and memory objects:

- Connect to the **KNM** server, using an account with administrator rights.
- On the Windows taskbar, select **Start > Run**.
- In the **Run** dialog box, type *perfmon*, and then click **OK**.
- In **Performance Monitor**:
  - In the panel on the left, expand **Data Collector Sets**.
  - Right-click **User Defined**, and then select **New > Data Collector Set** in the contextual menu.
  - In the first **Create new Data Collector Set** wizard dialog box:
    - In the **Name** box, type *KNMPerformanceSet*.
    - Select **Create manually (Advanced)**.

- Click **Next**.
- In the second **Create new Data Collector Set** wizard dialog box:
  - Select **Create data logs**.
  - Select the **Performance counter** checkbox.
  - Click **Next**.
- In the third **Create new Data Collector Set** wizard dialog box:
  - Click **Add**.
  - In the dialog box that appears, in the **Available counters** list, successively select the following performance counters, clicking **Add** for each of them:
    - **Memory**
    - **PhysicalDisk**
    - **Processor**
  - Click **OK**.
  - Click **Finish**.



When you are ready to start gathering performance information, in the main panel on the right, right-click **KNMPerformanceSet**, and then select **Start** in the contextual menu.

When you are ready to stop gathering performance information, in the main panel on the right, right-click **KNMPerformanceSet**, and then select **Stop** in the contextual menu.

To review the logged performance information, in Windows Explorer, locate and double-click the **.blg** file indicated in the **Output** column in **Performance Monitor**.

The **Performance Monitor** opens showing the collected data. Send the *.blg* file to your support.

## 4 Installation

This chapter shows you how to install the **KYOCERA Net Manager** system.

**F** Before you start the installation, make sure your system is up to date and meets the requirements as described in [System Requirements](#).

1. Download the latest available version of **KNM**.
2. Run the executable file. The **Select Setup Language** dialog box appears.
3. Select your language and click **OK**. The Select Destination Location dialog box appears.
4. Select the folder where you wish to install **KNM**. The default path is:  
`C:\Program Files\Kyocera\KYOCERA Net Manager\.`
5. Click **Install**. **KNM** is installed on the server.
6. Click **Finish**. Depending on the OS settings on the server, you might be asked to restart the computer. If you are asked to restart the computer, you need to do so in order to finish the installation. After the restart, the **KYOCERA Net Manager** Easy Config application opens and the **KNM** database is upgraded. If not, you can select to directly run the **KNM** Easy Config application by keeping the **Finish installation in KYOCERA Net Manager Easy Config** option selected.

### 4.1 Installation in Private Cloud

**KNM** Server can be installed and run, besides on-premises servers, also on an Azure Virtual Machine, with a VPN tunnel connecting the physical network and Azure's virtual network.

#### Environment Requirements:

- The minimum recommended virtual machine is B4ms, with a dedicated (non system disk) standard HDD.
  - The recommended CPU, RAM and HDD resources are the same as a standard installation and can be found in [system requirements](#).
- VPN tunnel (100mbps line is recommended) connecting the physical network and Azure's virtual network where the **KNM** Server is installed.
- Outgoing communication on ports used by **KNM** must be allowed on Azure's Network security group. See [main communication ports](#) for a full list.
- The geolocation of the cloud server should be as physically close as possible.
- The Ping answer from printers to the cloud server should be within 750 ms (max 1 second, can be adjusted in config.ini)

**i** For more information about *Azure - Extend an on-premises network using VPN*, see:  
<https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/vpn#architecture>

Once you set up the Azure virtual environment, follow the [Installation](#) instructions to install **KNM**.

#### About **KNM** in Private Cloud


Customers using Microsoft 365 as a private cloud hosting their internal systems can add **KNM** to the list of IT services they no longer need to have installed on an on-premises server.

Part of the leased private cloud space can be dedicated to **KNM** server(s), and **KNM** running in Azure can make use of [Azure Active Directories](#).

The single sign-on feature already used by users to access applications in the Microsoft cloud can also cover cloud printing with **KNM**, without the need to use a VPN connection.

[MS Universal Print](#) is also fully integrated in **KNM**, offering mobility, quick printer discovery, and no need for a VPN connection.

What is more, **KNM**'s Universal Print connector can work with older devices, so there's no need to invest into upgrading your fleet with more recent models which would natively support Universal Print.


 A VPN tunnel connecting the physical network and Azure's virtual network is also required when using Microsoft Universal Print. Thanks to this VPN tunnel, there is no need for a VPN connection from the client's side to the **KNM** Server.

## 4.2 Installing the KX Driver

After **KNM** is installed, install the KX Driver on user computers. **KNM** uses the KX Driver for some of its features and must be installed on user computers.

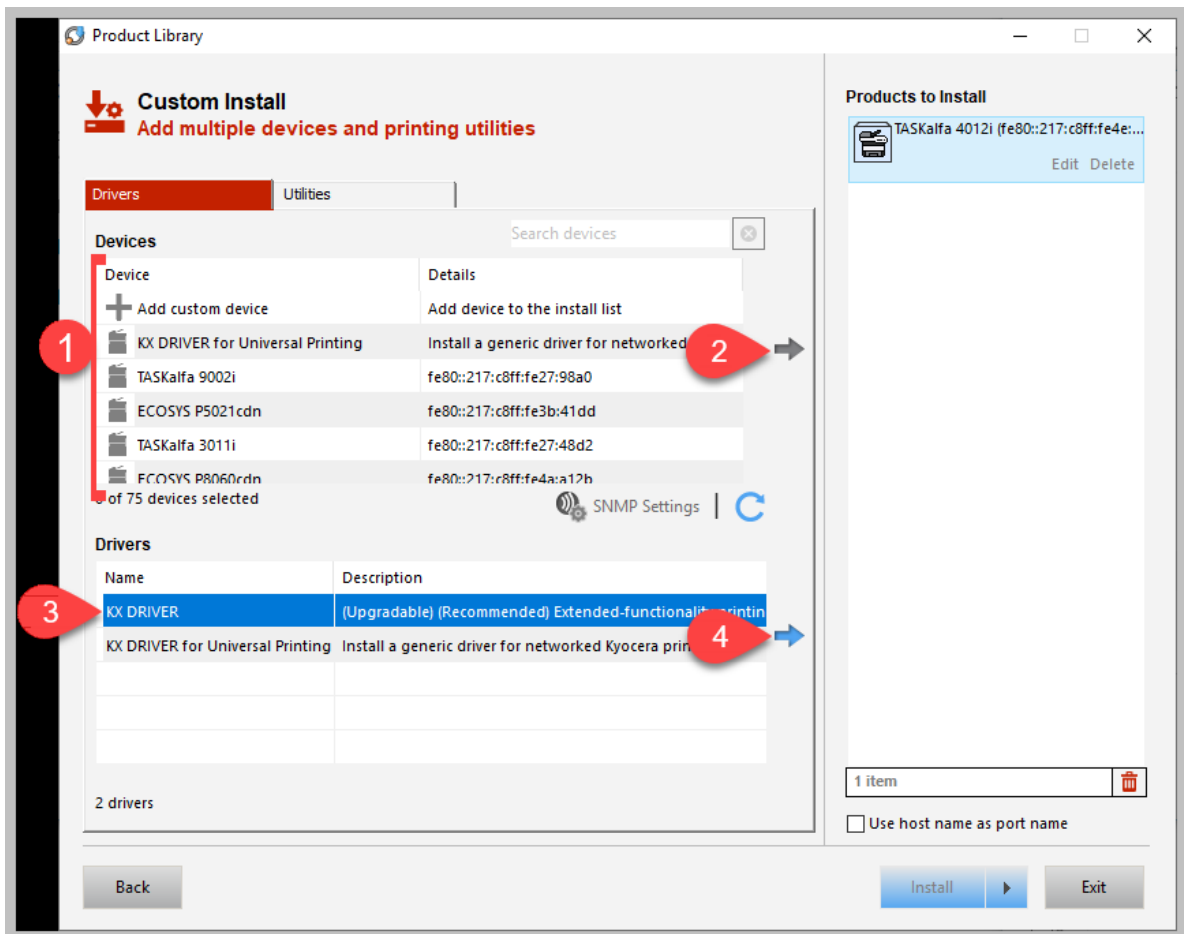
There are two parts to this installation:

1. Install the KX Driver.
2. Integrate the KX Driver with the Net Manager plugin.

 Only PCL jobs for KX v4 driver can be parsed. XPS jobs are not supported.

### 4.2.1 Install the KX Driver

1. Open the **Setup.exe** file.
2. If the User Account Control window displays, select **Yes**.
3. Select **Accept** at the Product Library window.
4. Review the **Resource and Energy Savings** information tabs, and click **OK**.
5. Select **Custom Install**.
6. In the Devices area (1) select your printing device and select the arrow (2) to move it into the Products to Install list. Use the Search devices box to search for devices by name or IP address. (If you do not have any connected devices at this time, you can select the Universal Printing device and Universal Printing driver. You can select more than one device to install at the same time.)



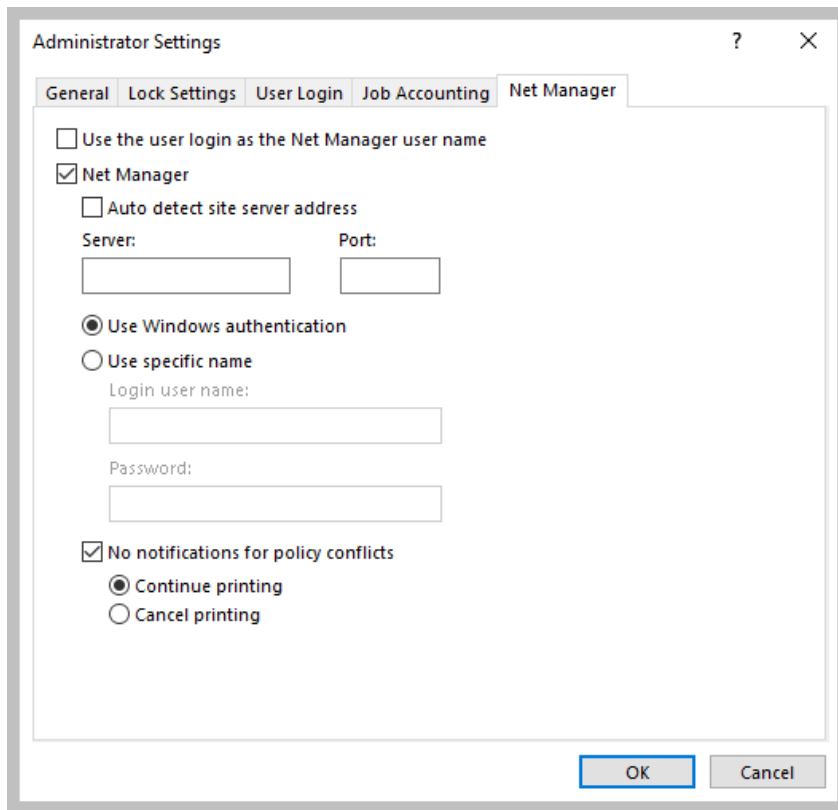
7. In the Drivers area select the KX Driver (3) and select the arrow (4) to move it into the Products to Install list.
8. Select **Install**.
9. When the installation is complete, select **Finish**. The Product Library is displayed.

Leave the Product Library window open and proceed to the next step where the KX Driver is integrated with the Net Manager plugin.

## 4.2.2 Integrate the KX Driver with the Net Manager plugin

In order to use all of the features of the KYOCERA Net Manager server, the Net Manager plugin must be integrated with the KX Driver.

1. In the Product Library, select **Maintenance > Optional Printer Components > Run**.
2. Select the devices that will have Net Manager integration and select **Next**.
3. Review your choices and select **Install**. After the installation completes, click **Close**.
4. Open Windows Settings and select **Devices > Printers & scanners**.
5. From the list of printers, select a printer where you installed the integration and then select **Manage**.
6. Select **Printer properties** and go to the Device Settings tab.
7. Click on **Administrator**. There is now a Net Manager tab in Administrator Settings.

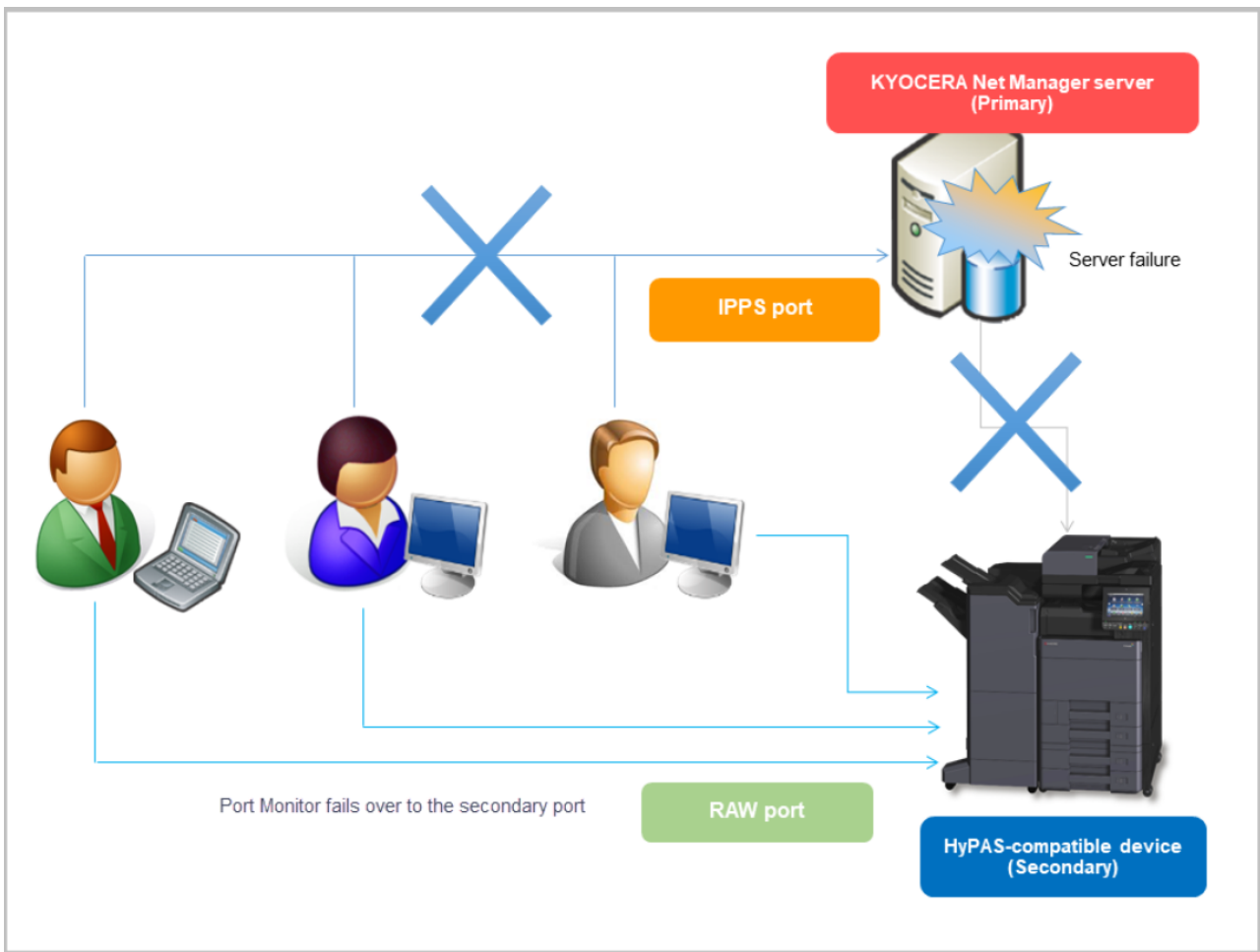


8. Select the **Net Manager** checkbox.
9. In the **Server** text box, enter the IP address or the hostname of the server and click **OK**.

The driver is now installed and integrated. How you configure the Port Settings tab depends on how you set up **KNM**. For example, **KNM** Desktop Client, Port Monitor, and Jobs via RAW protocol all require different port settings.

### 4.3 Installing KYOCERA Net Manager Port Monitor

Port Monitor for **KYOCERA Net Manager** is installed on client computers and provides ports for a printing environment that uses **KYOCERA Net Manager**: one port is for **KYOCERA Net Manager** server (Primary), and the other port is for a HyPAS-compatible device (Secondary). It normally operates with the port for **KYOCERA Net Manager** server. However, in the event of a server failure, it provides a failover feature that automatically switches to the secondary device port and continues processing jobs. When this happens, jobs are forwarded using the RAW protocol. Port Monitor can also divert jobs of a certain size or larger directly to the device bypassing the **KYOCERA Net Manager** server, so network traffic can be reduced and document workflow performance can be improved.



### 4.3.1 System requirements

Port Monitor for **KYOCERA Net Manager** operates in the following environment. Review these requirements before the installation.

Item	Description
Supported Devices	Devices supporting HyPAS features
Supported OS	Windows 8.1, Windows 10, Windows 2012 Server, Windows 2012 Server R2, Windows 2016 Server 64 bit)
CPU	CPUs that can run the above OS without problems

The following software products or settings are also required:

- **KYOCERA Net Manager**
- KX Driver 7.2 and later.

- Make sure that driver is set to use **KYOCERA Net Manager** by integrating the driver with the Net Manager plugin (see [Installing the KX Driver](#)).

On the **KNM** server, make sure that the queue being used for Port Monitor has the "**User detection method**" set to *KX Driver/Kyocera Mobile Print*.

### 4.3.2 Installation using the wizard

The following products are required before installing Port Monitor:

- **KYOCERA Net Manager**
- KX Driver 7.2 and later
- printer that supports Embedded Terminal features

Follow these steps to install **KYOCERA Net Manager** Port:

1. Open setup.exe in the **KYOCERA Net Manager** Port setup folder.
2. The license agreement screen displays. To review the license agreement, select **View License Agreement**. Read the License Agreement, select **Accept**, and then click **Next**. The Confirm Settings screen displays.
3. Click **Install** to start the installation.
4. Click **Finish** to complete the installation.

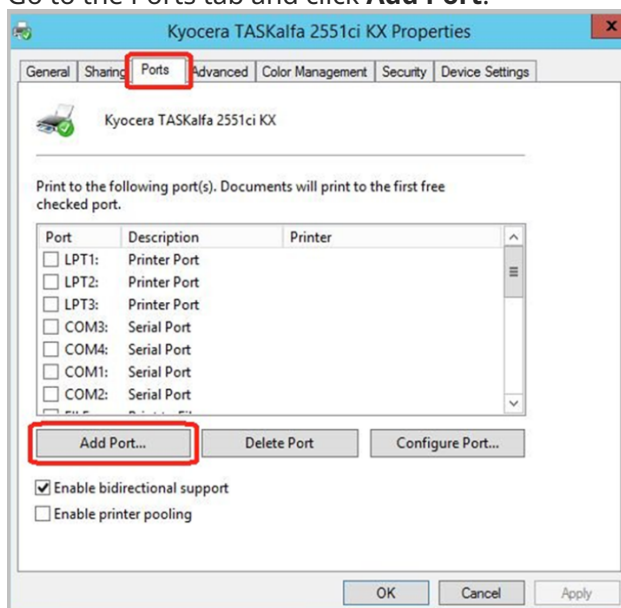
### 4.3.3 Configuration

After installing Port Monitor for **KYOCERA Net Manager**, you must add **KNM** Port to the target device's KX Driver.

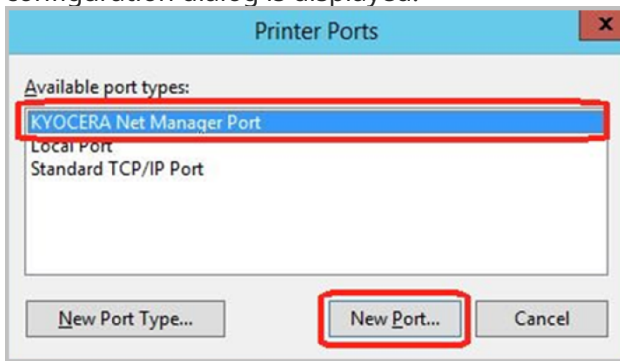
This section explains how to add, change the configuration of, or delete **KNM** Port.

#### Add KNM Port

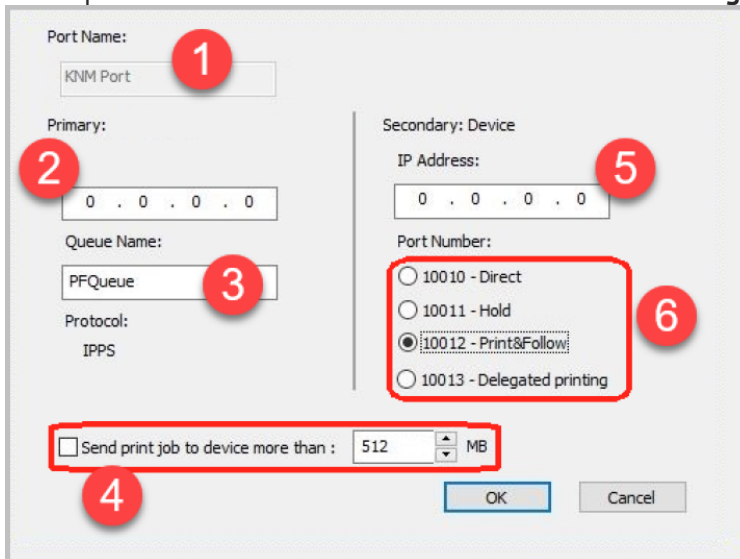
- Locate the printer in Windows Settings or Control Panel and open Printer properties.
- Go to the Ports tab and click **Add Port**.

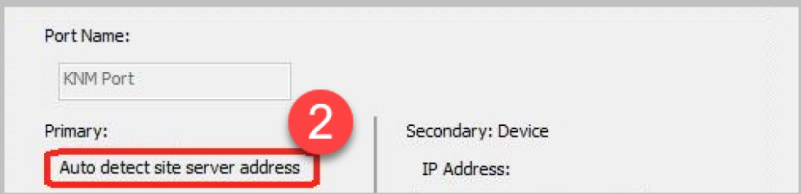


- Select KYOCERA Net Manager Port then click **New Port**. The **KYOCERA Net Manager Port** configuration dialog is displayed.



- Configure the settings. When the configuration is finished, click **OK**. The numbers in the image correspond to the commands in the **KYOCERA Net Manager Port** configuration table below.



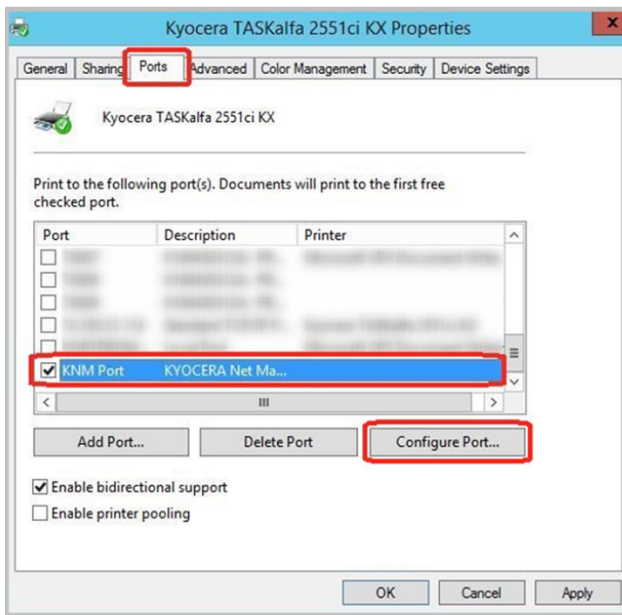
Number	Item	Description
1	Port Name	You can enter up to 32 single-byte alphanumeric characters. Once entered, the port name cannot be changed. The default is <b>KNM Port</b> .
2	Primary IP Address	IP address of the <b>KYOCERA Net Manager</b> server. When Auto detect site server address is on, this value will be shown as "Auto detect site server address". 

Number	Item	Description
3	Queue Name	Enter the queue name set up on the <b>KYOCERA Net Manager</b> server for Port Monitor. You can enter a maximum of 64 single-byte alphanumeric characters. The queue on the server must have "User detection method" set to "KX Driver/Kyocera Mobile Print" for Port Monitor to work.
4	Send print job to device more than _ MB	When cleared, all jobs are sent to the <b>KYOCERA Net Manager</b> server. This is the default setting. When checked, jobs larger than the specified size are sent directly to the secondary device. The range is 1-9999 MB. The default is 512 MB.
5	Secondary: Device IP address	The device's IP address.
6	Port Number	
	10010: Direct	The job is released immediately.
	10011: Hold	The job is stored on the printing device and released when the user logs into it.
	10012: Print&Follow	The job is stored on the device. A user can release it on the printing device or on another client device that designates the device as its device server.
	10013: Delegated printing	A delegated user can release a job sent by another user and print it.

- In the Printer Port dialog, click **Close**.
- In Printer Properties, click **Apply**, and then click **OK**.

### Configure or change **KNM** Port settings

- Locate the printer in Windows Settings or Control Panel and open Printer properties.
- Go to the Ports tab, select **KNM** Port, and click **Configure Port**. The **KYOCERA Net Manager** configuration dialog is displayed.



- Change the settings as needed and click **OK**.
- In the Printer Properties dialog, click **Apply**, and then **OK**.

### Delete KNM Port

- Locate the printer in Windows Settings or Control Panel and open Printer properties.
- Go to the Ports tab, select **KNM Port**, and click **Delete Port**.
- Click **OK** on the confirmation screen.
- In the Printer Properties dialog, click **Apply**, and then **OK**.

### 4.3.4 Silent installation

The silent installation finishes all the installation and configuration steps in one action by directly entering commands from the Windows command prompt. Silent installation is convenient when installing on multiple computers with the same settings.

The KX Driver for the target printer must be installed on the client computer before executing these steps to run silent installation.

- In Windows, open a Command Prompt window with Administrator privileges.
- Navigate to the folder containing the Port Monitor installer file (setup.exe), and then enter and execute the commands as shown.

```
setup.exe CREATEPORT -s -portname "KNM Port" -pri_addr
"10.10.10.10" -pri_queue "Queue1" -com_jobforward "1"
-com_jobsize "512" -sec_addr "10.10.10.11" -sec_port
"Print&Follow"
```

In this example, the port name is "KNM Port", the primary port's address is "10.10.10.10", the queue name is "Queue1", jobs larger than 512 MB are sent directly to the device (Secondary), the secondary port's address is "10.10.10.11", and the port is specified as "Print&Follow".

If you have turned on Autodetect Site server address in KX Driver, use "10.00.00.00" for -pri\_addr as a dummy Site server address.

The silent installation commands are detailed in the table below.

Command	Description	Corresponding setting in KX Driver
setup.exe CREATEPORT -s	Explicitly indicates silent installation.	-
-portname " "	Port name for Port Monitor. Specify the port name in quotes (" ").	1
-pri_addr " "	Primary port's IP address. Specify the address in quotes (" ").	2
-pri_queue " "	Divert by job size: 0: No, 1: Yes Jobs larger than the specified size are sent directly to the secondary device.	3
-com_jobsize " "	Size to divert. Specify job size in quotes (" "). The range is 1-9999 MB. Jobs larger than the specified size are sent directly to the secondary device.	4
-sec_addr " "	Secondary port's IP address. Specify the address in quotes (" ").	5
-sec_port " "	Secondary Port Number. Specify one of the below in quotes (" "): <ul style="list-style-type: none"> <li>• Direct</li> <li>• Hold</li> <li>• Print&amp;Follow</li> <li>• Delegated printing</li> </ul>	6

- Associate the Port Monitor ports with the port in the target device's KX Driver.
- Open a Command Prompt window and change the location to:  
C:\ProgramFiles(x86)\Kyocera\KYOCERA Net Manager\PMServer
- From the command prompt, type the following and execute:

```
kminst64 SETPRN -p "device name" -pt "KNM Port"
```

For "device name," enter the printer name shown in KX Driver properties.

For "KNM Port," select the port name shown in KX Driver properties.

- The silent installation is now finished.

### 4.3.5 Uninstallation

The uninstallation process is the same whether you used the wizard or the silent install method to install the software.

- In Windows, navigate to Program or App controls in Control Panel or Settings, depending on the Windows version.
- Find KYOCERA Net Manager Port and the option to uninstall.
- When the Uninstall dialog box displays, click **Uninstall**.
- When the Uninstall Complete dialog box displays, click **Next**. The Restart Your System dialog displays.
- To finish the uninstallation, close all running programs and restart the computer.

## 5 KYOCERA Net Manager Easy Config

This topic introduces the **KYOCERA Net Manager Easy Config** application and briefly describes its main features. Furthermore, it guides you through the following basic procedures:

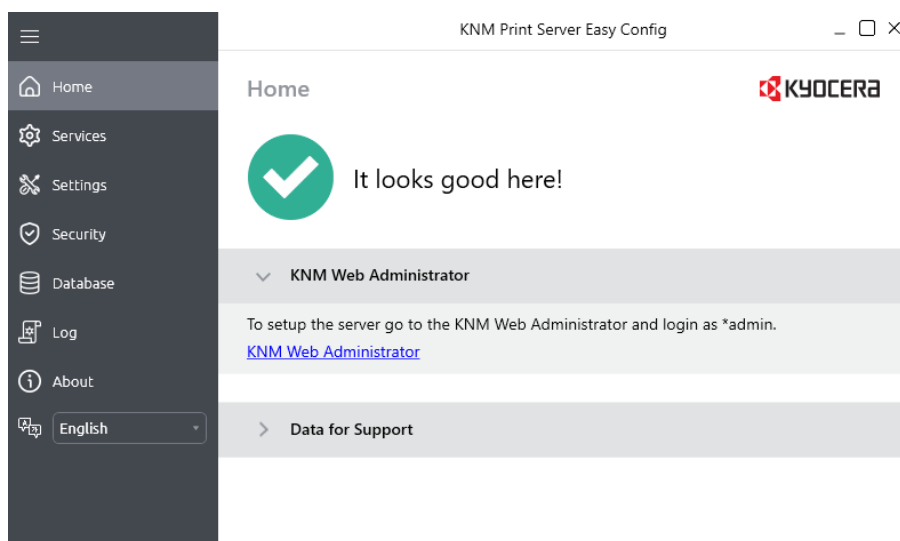
- how to manage KNM services
- how to change KNM passwords
- how to encrypt your KNM data
- how to relocate you Data and Jobs folders
- how to back up and restore your KNM database
- how to change KNM Web server ports
- how to clean up your Cache and Temp folders

The **KNM Easy Config** application is the basic environment for the setup of essential parts of the **KNM** server, such as the **KNM** database.

It automatically opens if you keep the **Finish installation in KNM Easy Config** option selected during the installation of the server. Otherwise, you can find it on the Apps screen in Windows 8.1+, Windows Server 2012 and newer. After you open the application, you see its menu on the left side. From this menu, you can access the following settings:

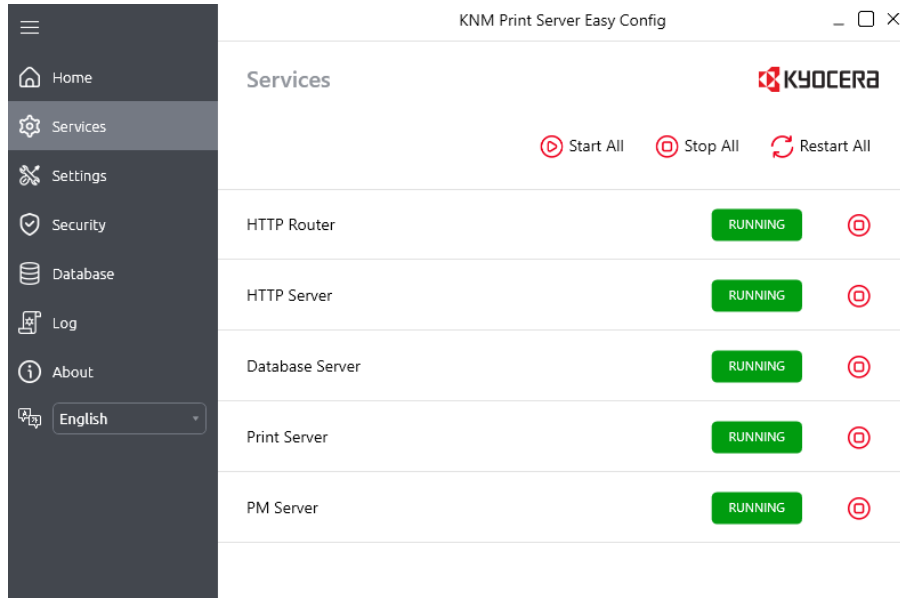
- On the **Home** tab, you can quickly change the default passwords for the Server and Database Administrator accounts, and generate data for support. You can also be redirected to the **KNM** Web Administrator Interface to finish the server setup.
- On the **Services** tab, you can view and control the **KNM** services.
- On the **Settings** tab, you can modify the Windows Services, Server administrator, and Database Administrator accounts, change file paths of the **KNM** system data and jobs files, change the port configuration of the **KNM** server, and clean up your Cache and Temp folders.
- On the **Security** tab, you can enable/disable unsecure communication, and manage the **KNM** DB, the Log DB, and print jobs encryption.
- On the **Database** tab, you can view information about the Main and Log Databases, as well as backup, and restore your database.
- On the **Log** tab, you can overview all the operations executed by the **KNM** system.
- On the **About** tab, you can view information regarding the current version of **KNM**.
- Lastly, you can select the **KNM** Easy Config display language from the drop-down list.

If there are no issues, the *"It looks good here!"* message is displayed on the Home tab:



## 5.1 Services

On the **Services** tab you can stop, start, and restart the services of the **KNM** server.



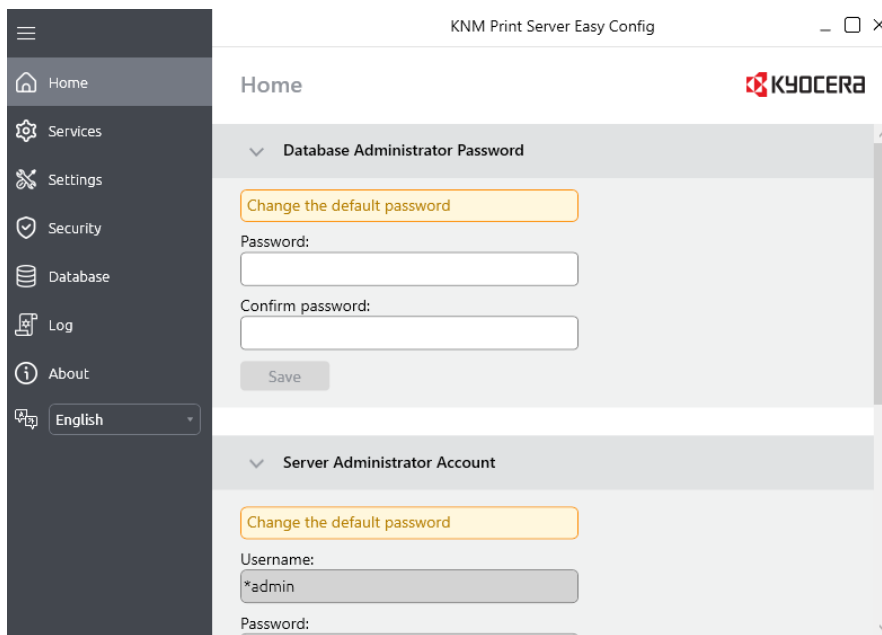
## 5.2 Passwords

Once you open the **KNM** Easy Config application for the first time, you should change the Server Administrator Account's password, which is the password for accessing the **KNM** web administrator interface.

**i** The **KNM** web administrator interface access user name is *\*admin* and its default password is 1234.

### Changing the password on the Home tab

The first time you open the application, on the **Home** tab, you can see the **Server Administrator Account** section. To change the password, type the new password, confirm the password, and then click **Save**.



After you change the password for the first time, its initial setup section disappears from the **Home** tab.

### Changing passwords on the Settings tab

As soon as you replace the default password, the section disappears from the **Home** tab and the password can no longer be changed there.

It can be changed at any time on the **Settings** tab under the **Server Administrator Account** section.

You can also change the database administrator's account password under the **Database Administrator Password** section.

The **KNM** database access user name is *SYSDBA* and its default password is *masterkey*.

### Unlocking the KNM Administrator account

After 5 consecutive failed login attempts to the **KNM** administrator account, the account is locked.

The admin can see a warning that the *\*admin* account is locked, and unlock it, in the **Server Administrator Account** section on the **Settings** tab. Once they click **Unlock**, the account is unlocked.

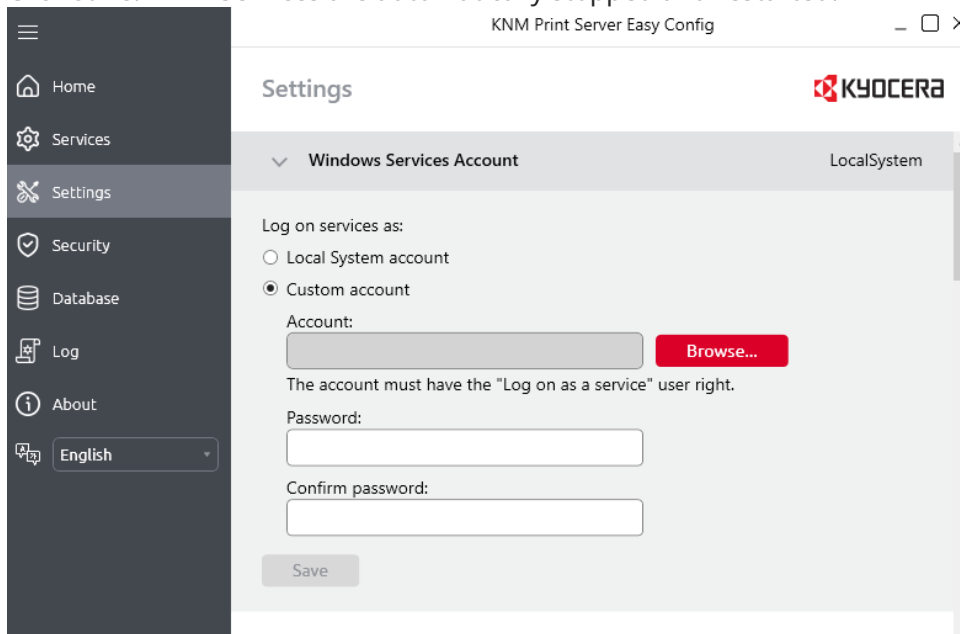
## 5.3 KNM Windows Services Account

**KNM** Windows Services run, by default, under the *Local System* account, meaning the account that was used during the installation.

This can be changed in the **Settings** tab, in the **Windows Services Account** section:

- Under *Log on services as*, select **Custom account**.

- Click on **Browse**, select the user account to be used for Windows services and click **OK**. The selected user account should have "Local administrator" rights or be a member of the Local Administrators Group. It should also already have rights to "Log on as service".
- Type the account's password and then confirm it in the next field.
- Click **Save**. **KNM** Services are automatically stopped and restarted.



- To change back to the default account, select **Local System account**, and click **Save**. **KNM** Services are automatically stopped and restarted.

## 5.4 Data and Jobs Folders

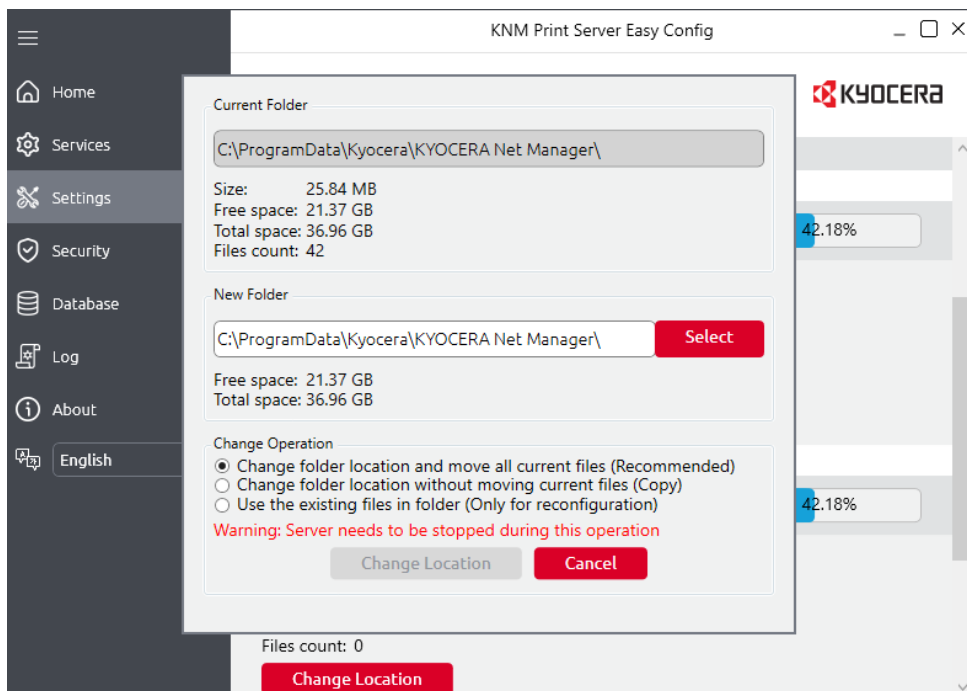
On the **Settings** tab, you can see the folder locations of **KNM** database and **KNM** print jobs.

The default folders are:

*C:\ProgramData\Kyocera\KYOCERA Net Manager\* for the database, and *C:\ProgramData\Kyocera\KYOCERA Net Manager\Jobs* for the print jobs.

Under normal circumstances, there is no need to change these locations. In case you have to do it, for example when there is not enough space on the system disk, follow the instructions below:

1. On the **Settings** tab, in the respective section, click **Change Location**. The **Change folder location** dialog box appears.



2. In the dialog box, under **New folder**, enter the path to the new folder or click the browser icon and find the folder location.
3. Under **Change Operation**, select the required method of existing data relocation, and then click **Change location**. Keep in mind that the server needs to be stopped during the change. The folder is moved to the new location.

**⚠** If you relocate your Data and Jobs folder to a network drive, be aware that Apache or Firebird service cannot access network drives created by the Administrator or other users. The network drive needs to be created by the "nt authority\system" user. You can do this using this guide: <https://stackoverflow.com/questions/182750/map-a-network-drive-to-be-used-by-a-service/4763324#4763324> or it should work when you mount the drive on Windows startup.

## 5.5 Security

On the **Security** tab, you can enable/disable unsecure communication, encrypt/decrypt the **KNM** DB, the Log DB, as well as print jobs, and manage the modification of PHP scripting.

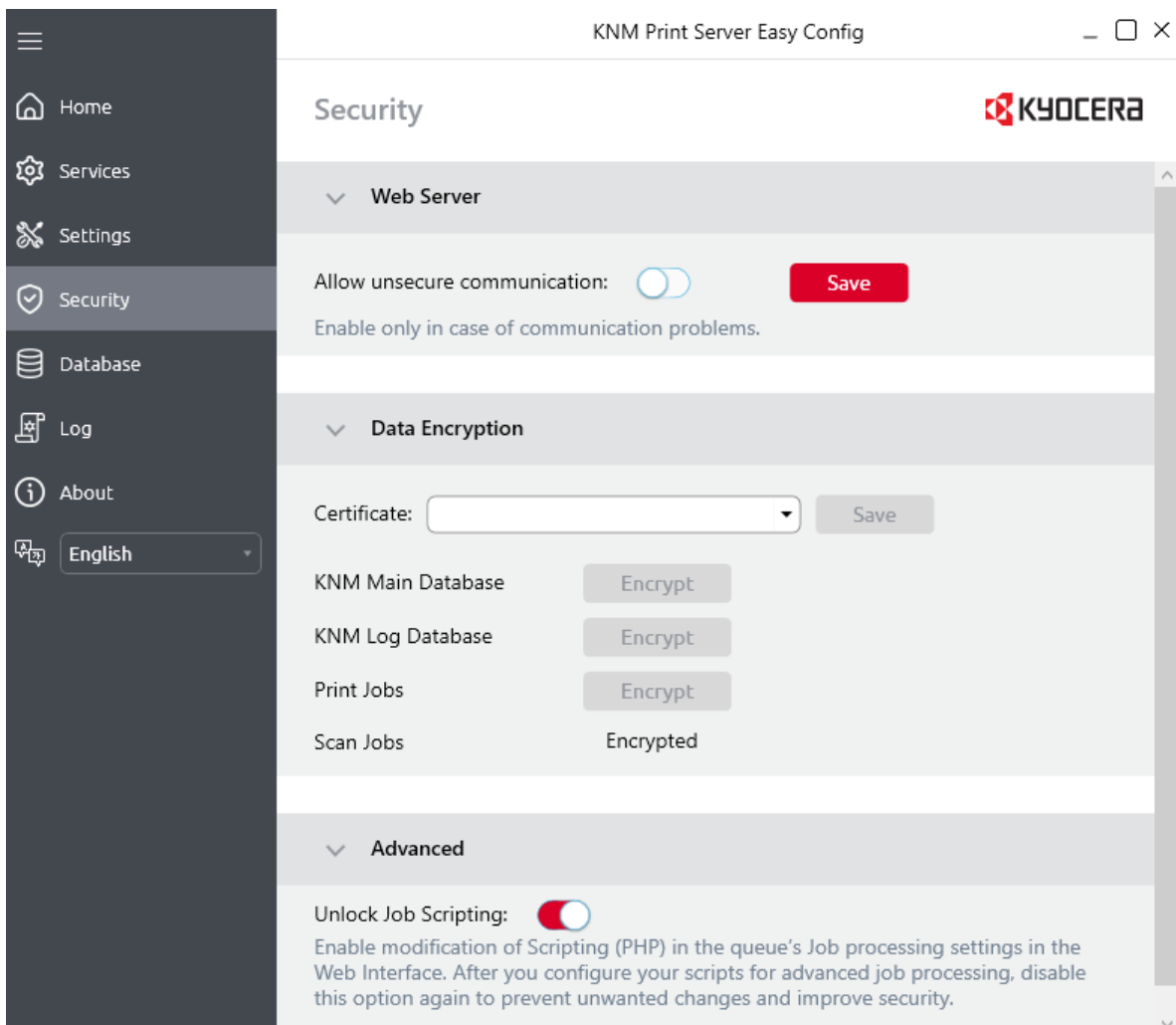
In the **Web Server** section, you should enable **Allow unsecure communication** only in case of communication problems.

In the **Data Encryption** section, for better security, you can encrypt the main database, the log database, and print jobs using a certificate. **KNM** does not provide these certificates. You should install and use your own. The certificate used for the encryption needs to have the "Encrypting File System" Enhanced Key Usage (EKU), it must be valid, and it must be located in one of the following computer certificate stores:

- Personal
- Trusted Publishers
- Third-Party Root Certification Authorities
- Other people

Once installed, it will be visible in the **Certificate** drop-down.

Expired certificates are visible but are marked as expired and cannot be used.



Click **Encrypt** next to **KNM Main Database**, **KNM Log Database**, or **Print jobs**. **Scan Jobs** are encrypted by default.

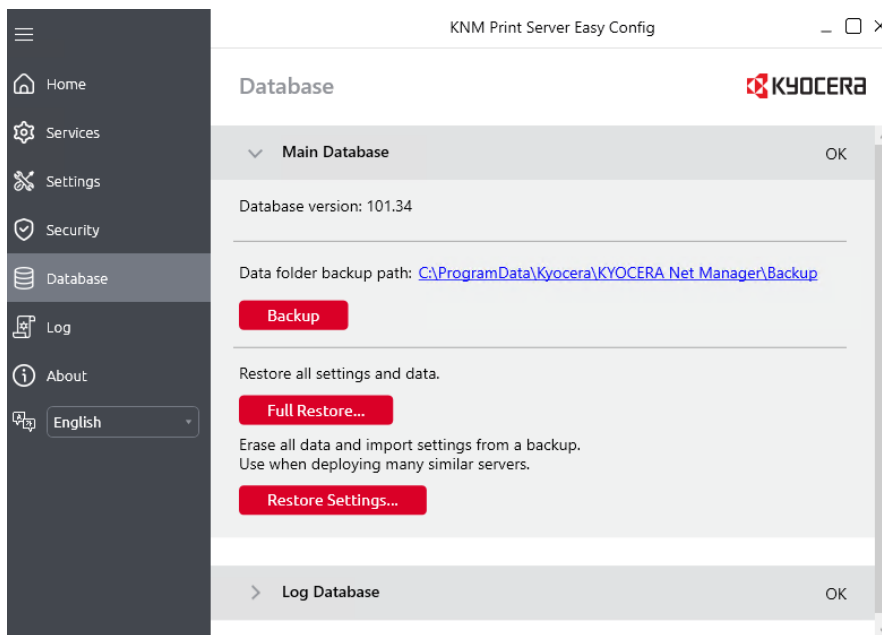
During the encryption, other services will not be available. A busy indicator will let you follow the encryption/decryption process:

After the encryption, the **Encrypt** button will change to **Decrypt** so you can reverse the action.

In the **Advanced** section you can enable or disable **Unlock Job Scripting** (modification of PHP job scripting in a queue's Job processing settings in the Web Interface). This option is disabled by default.

## 5.6 Database Backup and Restore

On the **Database** tab, you can check the main and log database's status, perform backup and recovery, and import settings from a different **KNM** installation. You can also see information about the current version of the database, available updates, and also a warning in case there is a need for an upgrade.



## 5.6.1 Backing up KNM data

To back up your **KNM** data:

1. Open the **Database** tab.
2. In the **Main Database** section, click **Backup**.
3. Provide and confirm a password to protect the backup. If skipped, the backup will be created unprotected.
4. A new backup file is created, called *database\_\*.zip*. The file contains the **KNM** database and additional files with data used by the **KNM** system, such as reports, certificates, or the *config.ini* file.

**[-]** Print jobs (by default in C:\ProgramData\Kyocera\KYOCERA Net Manager\Jobs) are not part of the backup, because of size.

If required (especially favorite jobs could be required by users after restoring **KNM** on the new server), they must be copied and backed up manually or by a 3rd-party software.

## 5.6.2 Restoring KNM Data

**[-]** If you had manually backed up print jobs, then when restoring a backup, it is necessary to first copy the print jobs to the Jobs folder and then restore the **KNM** backup using **KNM** Easy Config.

To restore your **KNM** data:

1. Open the **Database** tab.

2. In the **Main Database** section, click **Full Restore....** Select the *database\_\*.zip* file and click **Open**. If the backup is password protected, there is a prompt to provide the password. The database is restored and, if needed, upgraded as well.

### 5.6.3 Importing settings from another KNM installation

This feature simplifies large-scale deployments as it allows using one **KNM** installation as a “template” to set up more installations without the need to manually configure most of the settings.

#### Creating a database template basics

- Use groups for any assignation such as Rights, Policies, etc. User and Printer groups are kept in contrast with specific users or printers.

#### What the import does

During the import, the database is restored in the normal way, but the following data are changed:

- deleted users (groups are kept),
- deleted printers (groups are kept)
- deleted accounting data,
- deleted jobs,
- deleted payments, credit events,
- deleted vouchers and voucher batches,
- deleted quota boosts and quota periods,
- deleted reports execution history,
- deleted audit log records,
- deleted sites,
- new installation UUID,
- updated hostname,
- updated server name (if Site),
- non archived price lists get new UUIDs,
- licenses removed.

#### Limitations

- Terminal packages need to be reinstalled after the settings import. This process is not automated.

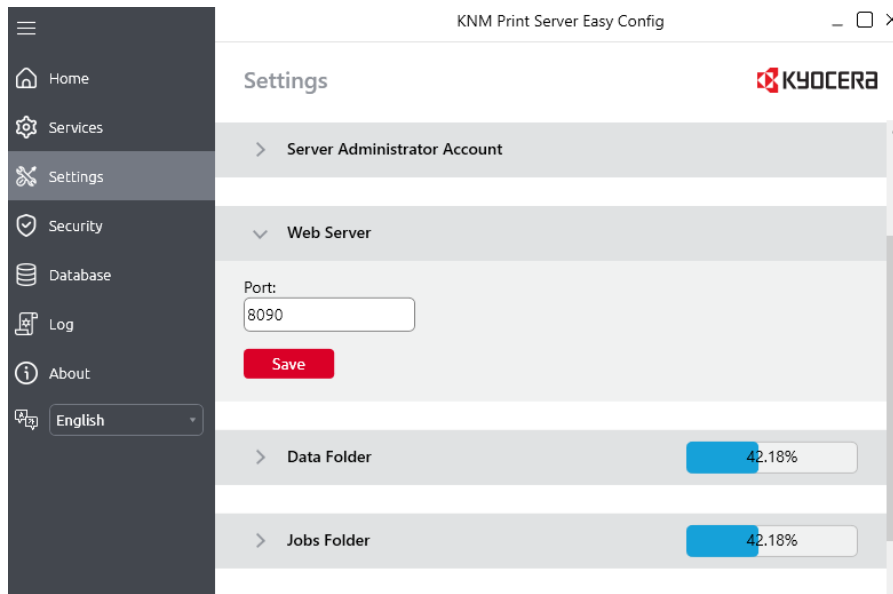
To import settings from a different **KNM** installation:

1. Open the **Database** tab.
2. In the **Main Database** section, click **Restore Settings....** Select your “template” backup *database\_\*.zip* file and click **Open**. If the backup is password protected, there is a prompt to provide the password. The database is restored and, if needed, upgraded as well.

## 5.7 Changing KNM Web server ports

On the **Settings** tab, under **Web Server**, you can change the port for the connection to the **KNM** Web server:

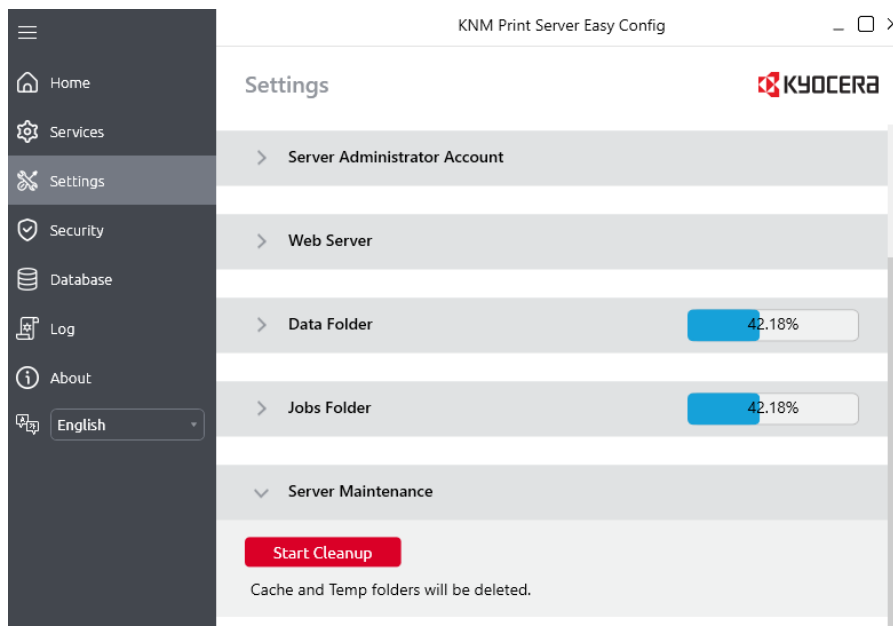
- **Port:** communication port for the **KNM** HTTP server; the default value is 8090.



## 5.8 Cleaning Cache and Temp folders

In the **Server Maintenance** section of the **Settings** tab, you can clean up your Cache and Temp folders. This might be necessary in cases when problems with the temporary files affect the **KNM** system.

To delete the two folders, click **Start Cleanup**.



## 6 KYOCERA Net Manager Web Interface

---

This topic describes the **KNM** Web Interface where you manage most of **KNM** functions. It shows you how to access the web interface and the two menus where you can access all settings and functions on the web interface: the **Main** menu, and the **Settings** menu. Furthermore, it describes the web interface's **Home dashboard** and shows you how to perform the initial **KNM** setup. The last two sections introduce two **KNM** logs: the **KNM Log** and the **KNM Audit Log**.

### 6.1 Accessing the KNM Web Interface

To access the **KNM** Web Interface, you need to open it in your web browser and log in as an administrator:

There are three ways to open the **KNM** Web Interface:

1. Open your web browser, and then enter the web address in the form:  
*https://\*KNMserver\*:8090*, where *KNMserver* represents the IP address or the host name of your **KNM** server and *8090* is the default port for access to the server.

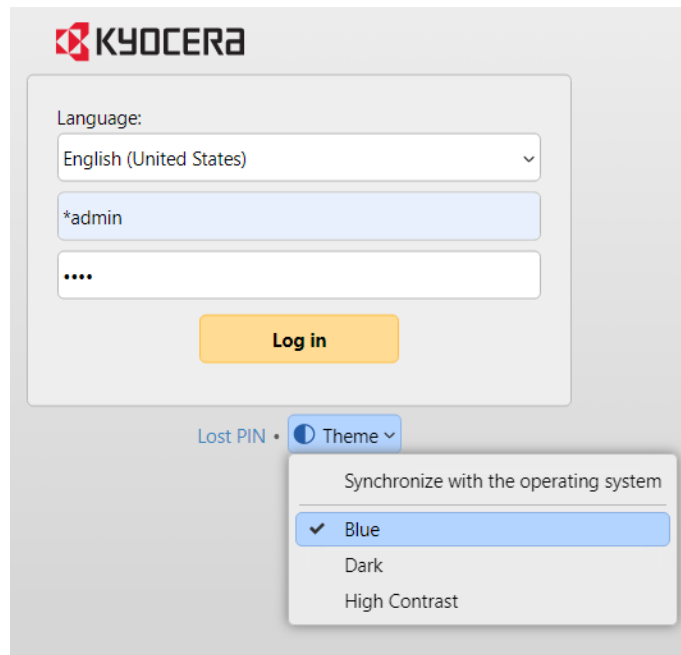
<https://10.14.5.816:8090>

2. Log on to the interface from the **KNM** Easy Config **Home** tab, by clicking on the **KNM Web Administrator** link in the **KNM Web Administrator** section.
3. Open the **KNM** Web Administrator application. You can find this application on the Apps screen in Windows 8.1+, Windows Server 2012 and newer.

### 6.2 Logging in as an administrator

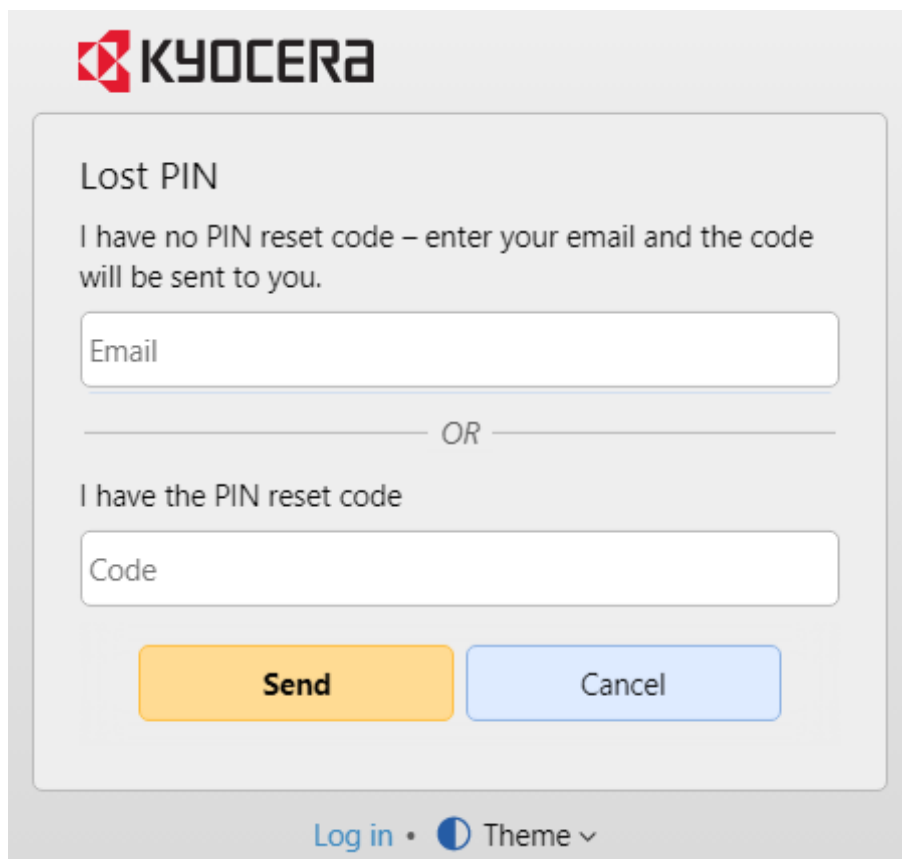
Enter the Server administrator name (*\*admin*) and the password that you have set in the **KNM** Easy Config application, and then click **Log In**. If you have not changed the default password yet (not recommended), enter the default one: *1234*.

In the drop-down at the top of the login window, you can select your preferred language.



Before logging in, you can click **Theme** to choose the theme for the interface. The options are: *Synchronize with the operating system, Blue (default), Dark, High Contrast.*

Click **Lost PIN** and you are taken to a window where you can either enter your email in order to receive a PIN reset code or if you already have the code, you can type it and reset your PIN.



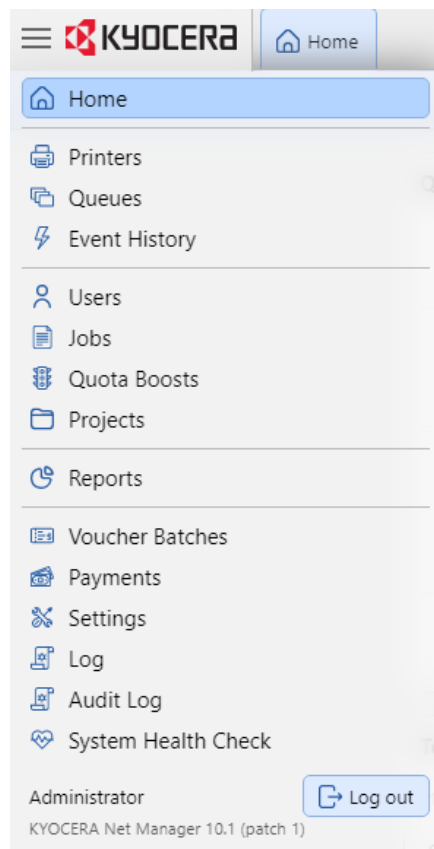
## 6.3 Main menu and Settings menu

There are two menus where you can access all the features and settings of the **KNM** server: the **Main (KYOCERA)** Menu and the **Settings** menu.

In this guide, all the tabs accessed from the Main menu, except for the Home screen and Settings menu, are called main tabs as opposed to settings tabs that are accessed from the Settings menu.

### Main Menu

To open the **Main** menu, click the **KYOCERA** logo at the upper-left corner of the screen. From there, you can access the **Home dashboard**, the **Settings** menu, and a number of tabs where you can manage and use **KNM** functions.



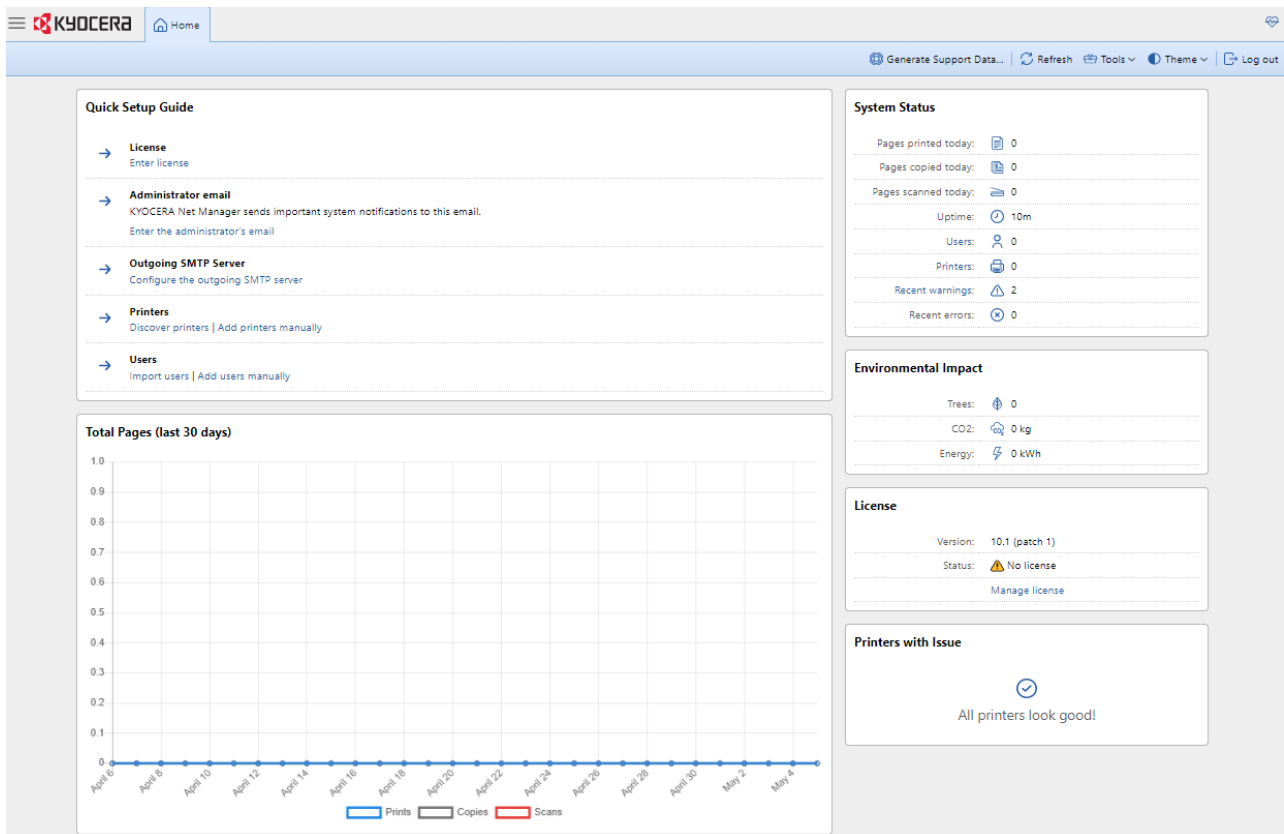
### Settings menu

To open the **Settings** menu, click **Settings** on the **Main** menu.

The tabs that are accessed from the Settings menu serve for the global setup of the **KNM** server.

## 6.4 Home Dashboard

On the **Home** dashboard, you can perform the initial **KNM** setup. After the setup, you can use the dashboard to directly access **KNM** key features, display statistics, and generate support data.



The dashboard is fully adjustable; it consists of multiple building blocks (widgets) that can be added and removed from the screen. You can use the blocks to customize both the layout and functionality of the dashboard.

By default, there are six widgets on the dashboard: **Quick Setup Guide**, **System Status**, **Total Pages (last 30 days)**, **Environmental Impact**, **License**, and **Printers with Issue**. Apart from these, you can also add the following widgets:

- **Quick Links:** From the **Quick Links** widget, you can directly access the most important tabs of the **KNM Web Interface**: Jobs, Printers, Users, Reports, Settings, and Log.
- **Top Active: Printers:** Shows the most active printing devices.
- **Top Active: Groups:** Shows the most active printing groups.
- **Top Active: Users:** Shows the most active users.

The **Quick Setup Guide** walks you through the initial **KNM** setup.

In **System Status**, you can see the following system status information:

Name	Description
<b>Pages printed today</b>	Number of printed pages over the last 24 hours. Cached every 60 seconds.

Name	Description
<b>Pages copied today</b>	Number of copied pages over the last 24 hours. Cached every 60 seconds.
<b>Pages scanned today</b>	Number of scanned pages over the last 24 hours. Cached every 60 seconds.
<b>Uptime</b>	KNM system uptime, in hours.
<b>Users</b>	Number of active users. Clicking opens the <b>Users</b> page overview.
<b>Printers</b>	Number of printers where the status is not: Local, replicated or deleted. Cached every 15 seconds. Clicking opens the <b>Printers</b> page.
<b>Recent warnings</b>	Number of warning log messages over the last 24 hours. Cached every 30 seconds.
<b>Recent errors</b>	Number of error and critical log messages over the last 24 hours. Cached every 30 seconds.

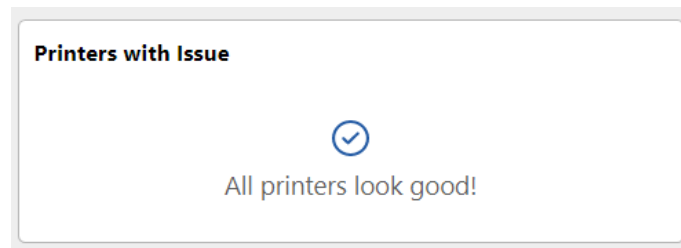
In the **Total Pages (last 30 days)** widget, you can see a graph of the prints, copies, and scans in the last 30 days.

The **Environmental Impact** widget shows your environmental impact in Trees, CO<sub>2</sub>, and Energy.

*1 tree = 8333 pages / 1 page = 12.7g of CO<sub>2</sub> / 1 page = 48Wh of energy / 1 recycled page = 32Wh of energy*

The **License** widget shows license information and can redirect you to the **License** settings tab.

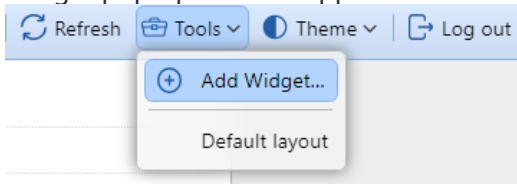
**Printers with Issue** shows unreachable active printers and active printers with unresolved alerts. You can also see these issues in the **Issues** column, in the **Printers** overview (**KYOCERA, Printers**).



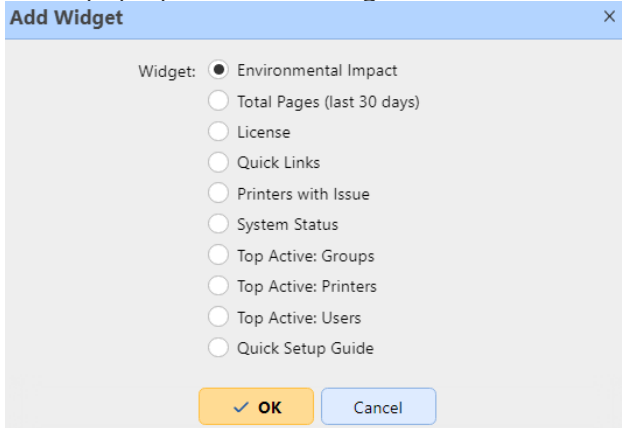
### Adding new widgets and moving widgets on the dashboard

To add a new widget:

1. Click **Tools** at the top-right corner of the dashboard, and then click **Add Widget**. The Add Widget pop-up window appears.



2. In the pop-up, select the widget, and then click **OK**. The new widget is displayed on the board.



To move widgets, drag and drop them on the board.

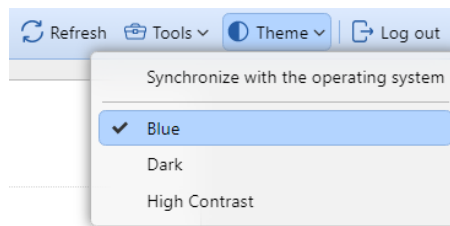
To delete widgets, click on the three dots at the top-right corner of the widget, and click **Remove**.

Select **Default layout** in the **Tools** menu, to restore the dashboard to its default layout.

## Changing the theme

To change the **KNM** Web UI theme, click on **Theme** at the top-right corner of the dashboard. The available options are:

- Synchronize with the operating system
- Blue (default)
- Dark
- High Contrast



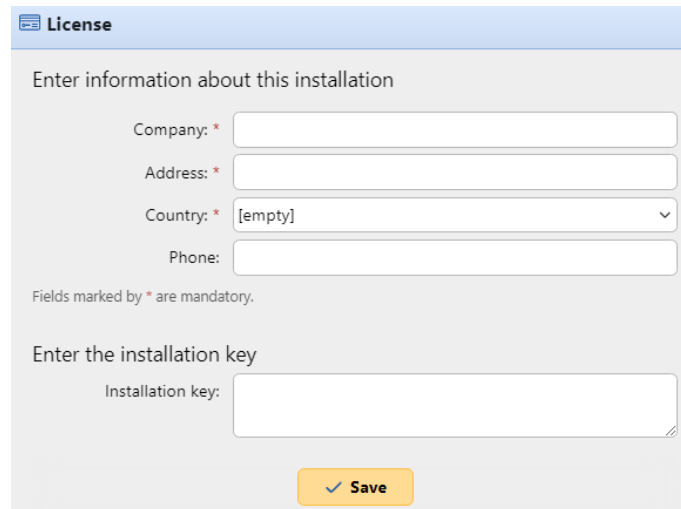
### 6.4.1 Quick Setup Guide

On the **Quick Setup Guide** widget, you can set the basic and most important features of the **KNM** system:

#### License

Adding and activating licenses

Click **Enter License**. The **License** settings tab opens. You are asked to enter the following information about your installation:



Then, **Enter the installation key** in the field and activate your licenses.

### Administrator email

By clicking **Enter the administrator's email**, you open the **General** settings tab, where you can set the administrator email. Important system messages (disk space checker warnings, license expiration etc.) are automatically sent to this email.

### Outgoing SMTP server

By clicking **Configure the outgoing SMTP server**, you open the **Network** settings tab, where you can set the outgoing SMTP server.

### Printers

Adding printers:

- By clicking **Discover Printers**, you open the **Printer Discovery** settings tab, where you can discover and add printing devices.
- By clicking **Add printers manually**, you open the **Printers** main tab, where you can manually add printing devices.

Activating added printers:

Click **Activate** to activate all the added printing devices.

### Users

- By clicking **Add users manually**, you open the **Users** main tab, where you can manually add users.
- By clicking **Import users**, you open the **Users synchronization** settings tab, where you can import users from the **KNM** Central server, from LDAP servers, or from a CSV file.

## 6.4.2 Generate Support Data

In case you encounter a problem that requires help your support team, you may be asked to provide more information about your **KNM** system configuration, licenses, printer devices, terminals, etc. In such case, you need to generate a *KNMhelpdesk.zip* file, which contains multiple files with all the necessary information, and send it to your support team.

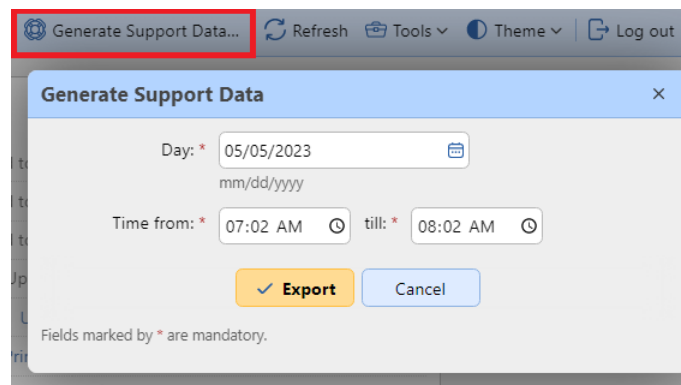
The *.zip* file includes the **Logs** folder which contains:

- error logs from Apache and PHP,
- the **KNM** log file *log\_dateandtime.xlsx*,
- the Windows Event log,
- the *statsData.xml* file,
- *httperr\*.log* files,
- and the *KNM-helpdesk.xml* file with **KNM** system information.

The **KNM** log file corresponds to the **KNM** log that can be displayed on the **KNM** Web Interface or in the **KNM** Easy Config application, but they differ from each other.

To generate the *KNM-helpdesk.zip* file:

1. Click **Generate Support Data** on the bar at the top of the **Home** dashboard. The Generate Support Data dialog box appears.
2. In the dialog box, specify the **Day** and the exact **Time** span of the **KNM** events to include in the *KNM-helpdesk* file, and then click **Export**. The file is generated and saved to your *Downloads* folder.



## 6.5 KNM Log

In the **KNM** server log, you can find information about all parts of the **KNM** server: the **KNM** server, **KNM** Web UI, etc. Log messages are sorted into these types *Critical*, *Error*, *Warning*, *Info*, *Notice*, *Debug*, *Trace* and you can select the types that you want to be displayed.

You can also set the log to display only messages informing about specific **KNM** subsystems, such as the Web UI, remote printer setup, user sessions on **KNM** terminals, and also about a specific context, for example, direct printing or a specific printing device.

Time	Type	Subsystem	Context	A...	Text
05/05/2023 8:03:05 AM	Debug	Direct Print			Checking new direct print jobs
05/05/2023 8:03:02 AM	Debug	Direct Print			Checking new direct print jobs
05/05/2023 8:02:59 AM	Debug	Direct Print			Checking new direct print jobs
05/05/2023 8:02:56 AM	Debug	Direct Print			Checking new direct print jobs
05/05/2023 8:02:53 AM	Debug	Direct Print			Checking new direct print jobs
05/05/2023 8:02:50 AM	Debug	Direct Print			Checking new direct print jobs
05/05/2023 8:02:47 AM	Debug	Direct Print			Checking new direct print jobs
05/05/2023 8:02:44 AM	Debug	Direct Print			Checking new direct print jobs
05/05/2023 8:02:41 AM	Debug	Direct Print			Checking new direct print jobs
05/05/2023 8:02:40 AM	Trace	Scheduler	System Health Check   id=63	<a href="#">🔗</a>	OUT   MyQ\Schedule\SchedulerService:ru
05/05/2023 8:02:40 AM	Notice	Scheduler	System Health Check   id=63		System Health Check did not find any new
05/05/2023 8:02:40 AM	Debug	Web Service	fe80::50c1:3f69:52c8:3acc   id=5927   ssl=yes	<a href="#">🔗</a>	OUT: GET /api/v3/server/status   status=21

The log is updated in real time, but you can pause it by clicking **Watch live**, and select to show messages from a specific time period, such as yesterday, this week, last week, last X hours, last X weeks, etc.

## Opening the Log

On the **KNM** Web User Interface, go to **KYOCERA, Log**, or on the **Home** dashboard, click **Log** on the **Quick links** widget.

## Pausing/Refreshing the log

To pause or resume the real time run of the log, click **Watch live** on the bar at the top of the **Log** tab. To refresh the log up to the current moment, click **Refresh** on the same bar.

## Filtering the log: selecting time period, types of information, subsystem or context

You can filter the log on the panel:

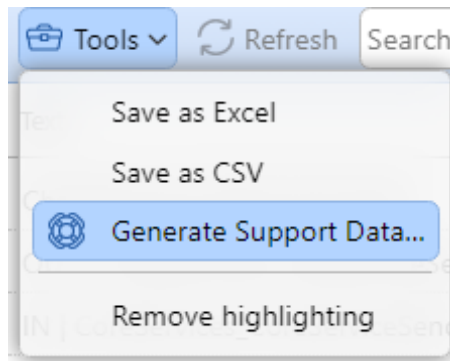
- After you pause the log, you can select the period in the **Date** combo box.
- The types can be selected and deselected on the panel at the right side of the **Log** tab.
- On the **Subsystem** combo box, you can select/type one or more subsystems to be displayed in the log.
- In the **Context** text box, you can type the context you want to view.

After the filters are set, click **Search** to submit them.

## Exporting the log/Generating support data

Click **Tools** on the bar at the top of the **Log** tab, and then select one of the following export options:

- **Save as Excel** — export the log as an Excel file.
- **Save as CSV** — export the log as a CSV file.
- **Generate Support Data** — generates a **.zip** file with multiple files for **KNM** support.



### Highlighting log messages

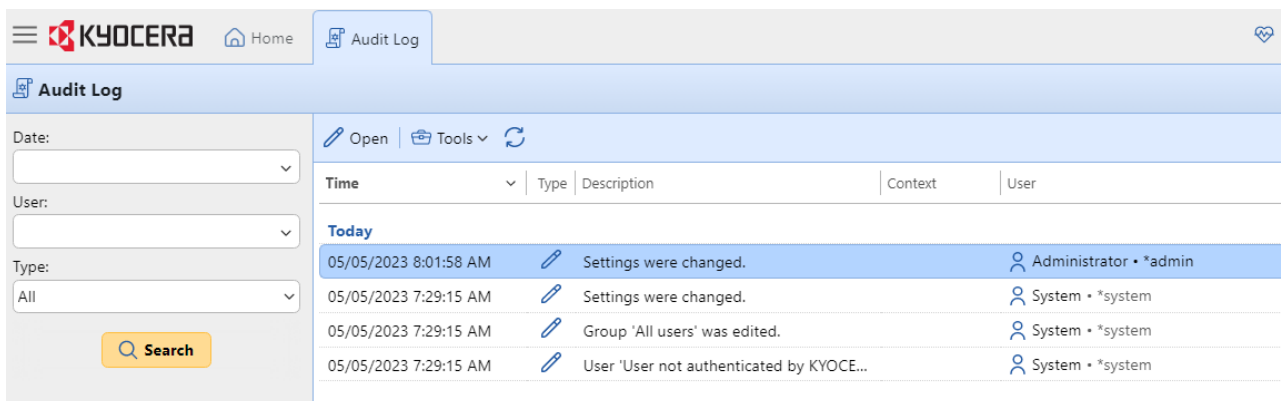
You can highlight particular log messages. To do so, select the message that you want to highlight and then press the **SHIFT + SPACE** keyboard shortcut.

Time	Type	Subsystem	Context	A...	Text
09/13/2022 4:41:14 AM	Debug	Direct Print			Checking new direct print jobs
09/13/2022 4:41:11 AM	Debug	Direct Print			Checking new direct print jobs
09/13/2022 4:41:08 AM	Debug	Direct Print			Checking new direct print jobs
09/13/2022 4:41:05 AM	Debug	Direct Print			Checking new direct print jobs
09/13/2022 4:41:02 AM	Debug	Direct Print			Checking new direct print jobs
09/13/2022 4:40:59 AM	Debug	Direct Print			Checking new direct print jobs

To remove all highlights, click **Tools** on the bar at the top of the **Log** tab, and then click **Remove highlighting**.

## 6.6 KNM Audit Log

In the **KNM Audit Log**, you can view all the changes of **KNM** settings, along with information about who made the changes, the time when they were made, and which subsystem of **KNM** was affected by them.



### Opening the Audit Log

On the **KNM Web User Interface**, click **KYOCERA**, and then click **Audit Log**.

## Filtering the Audit Log: selecting time period, user and type of event

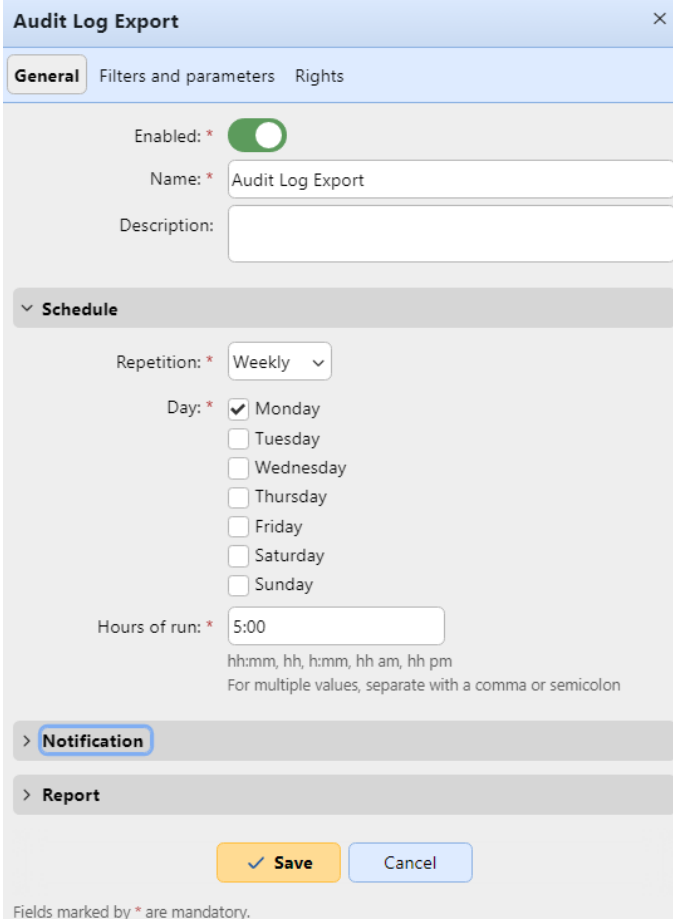
The displayed data can be filtered by a time period, the user who made the changes and the type of the event.

To display additional information about a particular change, double-click the change. A panel with the detailed information opens on the right side of the **Audit Log** tab.

## Exporting the Audit Log

You can export the **Audit Log** by clicking **Tools** and then **Export** on the main ribbon. The log is instantly generated and downloaded.

You can also click **Schedule Export** to have the log regularly exported. The schedule's properties panel open to the right, where you can set its parameters.



The screenshot shows the 'Audit Log Export' dialog box with the following configuration:

- General** tab is selected.
- Enabled:** \*  (toggle switch is turned on)
- Name:** \* Audit Log Export
- Description:** (empty text box)
- Schedule** section is expanded:
  - Repetition:** \* Weekly
  - Day:** \*  Monday,  Tuesday,  Wednesday,  Thursday,  Friday,  Saturday,  Sunday
  - Hours of run:** \* 5:00
  - Format: hh:mm, hh, h:mm, hh am, hh pm
  - Note: For multiple values, separate with a comma or semicolon
- Notification** and **Report** sections are collapsed.
- Save** (yellow button) and **Cancel** (blue button) buttons are at the bottom.
- Footer text: Fields marked by \* are mandatory.

# 7 KYOCERA Net Manager System Settings

This topic discusses basic system settings of the **KNM** system. The settings are located on separate tabs, accessed from the Settings menu:

- On the **General** settings tab, you can set the administrator email, change regional settings, and other general settings.
- On the **Personalization** settings tab, you can add custom help links and custom logos to be used in various parts of the **KNM** system.
- On the **Network** settings tab, you can modify network settings such as certificates, server ports, etc.
- On the **Authentication servers** settings tab, you can add LDAP, Azure AD, and Radius servers for user authentication.
- On the **Task scheduler** settings tab, you can add new task schedules, change their settings and run scheduled tasks.
- On the **Log** settings tab, you can set the Log notifier feature, which enables sending notifications about selected log events to the administrator and/or any number of **KNM** users.
- On the **System management** settings tab, you can change settings of the **KNM** history, set the maximum size of files that can be uploaded on the **KNM** Web Interface, delete data from the **KNM** database, and also reset **KNM** components to apply settings previously made on other tabs.

## 7.1 Server Type Settings

In the **Server Type** settings tab, the **KNM** administrator can set the type of server to use:

The screenshot shows the 'Settings: Server Type' page in the KYOCERA Net Manager interface. The left sidebar contains a 'Settings' menu with various options like Terminal Actions, Events, Users, Policies, etc. The main content area is titled 'Server Type' and includes the following sections:

- Standalone server:** licensed separately.
- Site server:** Production KYOCERA Net Manager server, licenses are allocated from the Central Server.
- Server Type:** Radio buttons for 'Standalone server' and 'Site server'. 'Site server' is selected.
- Connection settings:** Includes fields for 'Site name', 'Central Server address', 'Enable secure connection' (checked), 'Port' (8093), and 'Password for communication'. A note states: 'Password is used for communication between Central server and Site servers.'
- Licenses:** Includes fields for 'Embedded terminals' and 'Embedded Lite terminals', both set to 0.

At the bottom right, there are 'Save' and 'Cancel' buttons. A note at the bottom left states: 'Fields marked by \* are mandatory.'

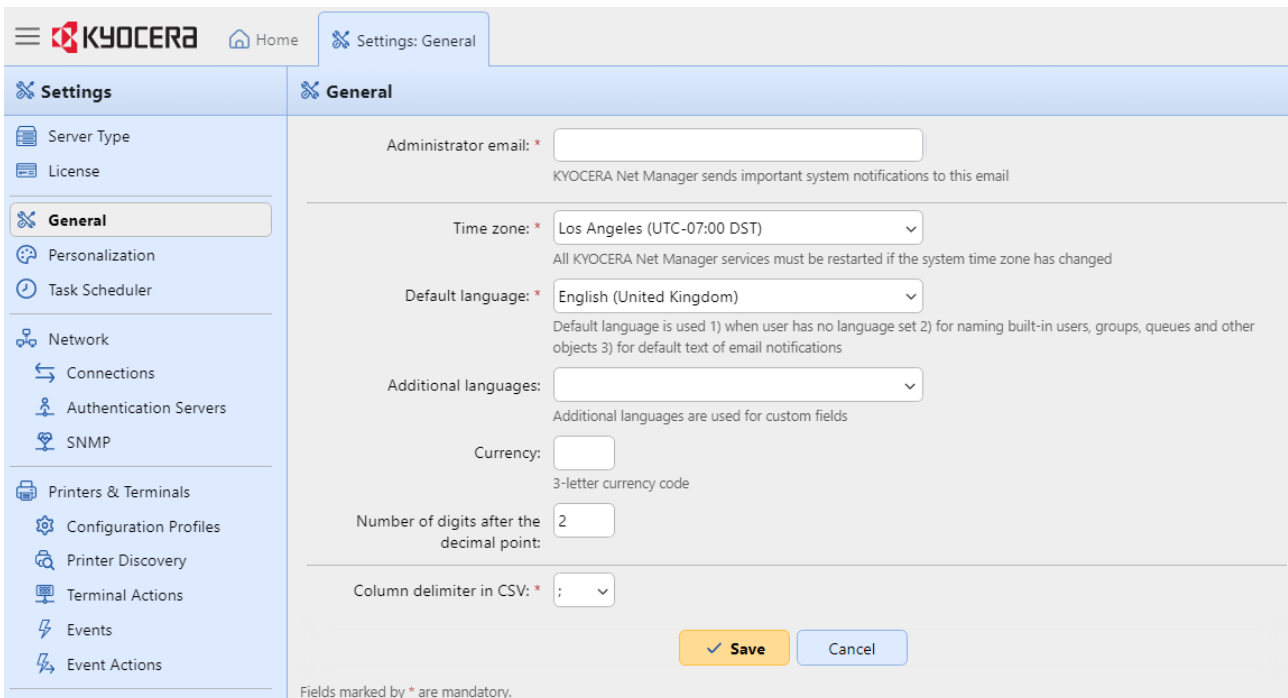
- **Standalone server** - this is enabled by default. It corresponds to the **KNM** Print server.

- **Site server** - this option can only be used within a **KNM** Central server installation.
  - **Site name** - add a name for your site server.
  - **Central Server address** - add the Central server's host name or IP address.
  - **Enable secure connection** - enabled by default. The connection between the Central server and the Site servers is secure.
  - **Port** - 8093 by default.
  - **Password for communication** - password used for the communication between the **KNM** Central server and Site servers.
  - **Embedded terminals** - add the number of embedded terminal licenses to be used on this Site server (distributed by the Central server).
  - **Embedded Lite terminals** - add the number of embedded lite terminal licenses to be used on this Site server (distributed by the Central server).

**⚠** In older versions, in the **Server type** settings tab, it was possible to switch between the Standalone server, a Site server, or a Central server. This is no longer available, as the **KNM** Print server and **KNM** Central server are different products and use separate installers. If you have such a setup and plan to upgrade to **KNM** Central server 8.2+, be advised that the upgrade will not be successful. It is required to upgrade your system to version 8.1, download the latest **KNM** Central server installer, and **migrate** your setup (described in detail in **KNM** Central Server).

## 7.2 General Settings

In the **General** settings tab, you can set the administrator email, time zone, default and additional languages, currency, and the column delimiter in CSV files.



The screenshot shows the 'Settings: General' tab in the KYOCERA Net Manager interface. The left sidebar lists various configuration categories, with 'General' selected. The main panel displays the following settings:

- Administrator email:** A text input field with an asterisk (\*) indicating it is mandatory. Below it, a note states: "KYOCERA Net Manager sends important system notifications to this email".
- Time zone:** A dropdown menu set to "Los Angeles (UTC-07:00 DST)". A note below reads: "All KYOCERA Net Manager services must be restarted if the system time zone has changed".
- Default language:** A dropdown menu set to "English (United Kingdom)". A note below reads: "Default language is used 1) when user has no language set 2) for naming built-in users, groups, queues and other objects 3) for default text of email notifications".
- Additional languages:** An empty dropdown menu. A note below reads: "Additional languages are used for custom fields".
- Currency:** An empty text input field. A note below reads: "3-letter currency code".
- Number of digits after the decimal point:** A text input field containing the value "2".
- Column delimiter in CSV:** A dropdown menu set to ";". It has an asterisk (\*) indicating it is mandatory.

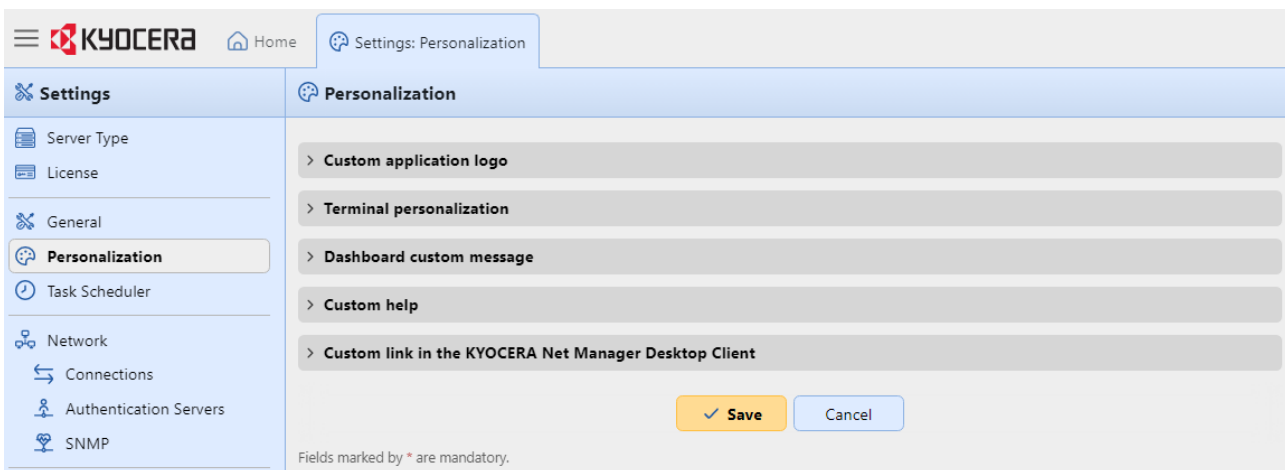
At the bottom right of the settings panel are two buttons: "Save" (with a checkmark icon) and "Cancel". At the bottom left, a note states: "Fields marked by \* are mandatory."

- **Administrator email:** The administrator email receives important system messages (disk space checker warnings, license expiration, etc.) automatically sent from **KNM**.

- **Time zone:** For the proper functioning of the **KNM** system, make sure that the time zone set here is the same as the time zone set in the Windows operating system. After changing the time zone, you will be asked to restart the web server.
- **Default Language:** The default language setting determines the language (list of [available languages](#)) of all emails that are automatically sent from **KNM** and the language used on all connected terminals and interactive readers.
- **Additional languages:** You can set additional languages that will be used for custom fields. This way you can enter different names of the fields to be used in different languages.
- **Currency:** In the currency setting, you can enter the 3-letter currency code of the currency that you want to use in your pricelist.
  - The **Number of digits after the decimal point** option can be set from 0 to 5 (default is 2).
- **Column delimiter in CSV:** The column delimiter in CSV files setting determines the delimiter in source and destination files used for all the import and export operations to and from the CSV file format. The default value is based on the regional settings of your operating system.

## 7.3 Personalization Settings

On this tab, you can set a custom message to be shown on the Web accounts of **KNM** users, add links to your own custom help, add custom application logos to be used in **KNM**, on **KNM** terminals, and in **KYOCERA Net Manager Desktop Client**, and personalize your terminals with the available themes.



### 7.3.1 Custom application logo

Here you can add your company's logo to be used in the **KNM** system. The logo will appear on the upper-right corner of the **KNM** Web Interface, on **KNM** credit vouchers, in **KNM** Desktop Client, and on reports.

Supported picture formats are *JPG/JPEG/PNG/BMP* and the recommended size is *398px x 92px*.

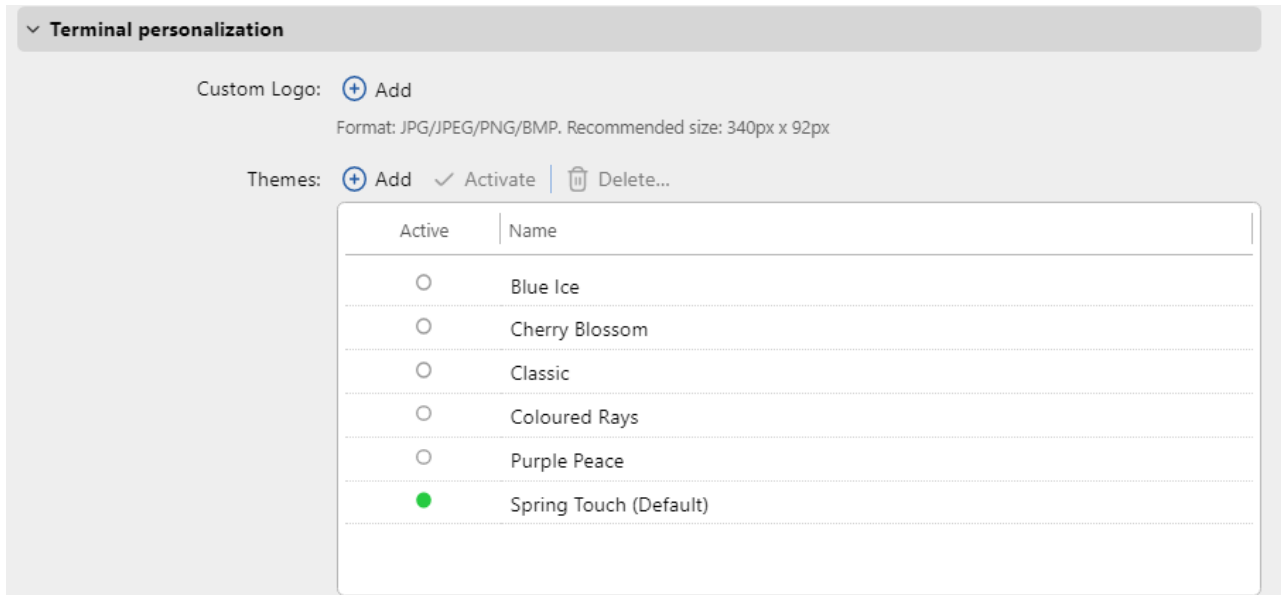
To import the logo, click **+Add, Browse** for the file and **Open** it, and then click **Save** at the bottom of the tab. A preview of the new logo is displayed on the tab.

## 7.3.2 Terminal personalization

Here you can add your company's logo to be used on all your **KNM** embedded terminals.

Supported formats are *JPG/JPEG/PNG/BMP* and the recommended size is *340px x 92px*.

To import the custom logo, click **+Add, Browse** for the file and **Open** it, and then click **Save** at the bottom of the tab. A preview of the new logo is displayed on the tab.



The screenshot shows the 'Terminal personalization' settings tab. It features a 'Custom Logo' section with an 'Add' button and a note about supported formats (JPG/JPEG/PNG/BMP) and recommended size (340px x 92px). Below this is a 'Themes' section with 'Add', 'Activate', and 'Delete...' buttons. A table lists available themes with radio buttons for selection.

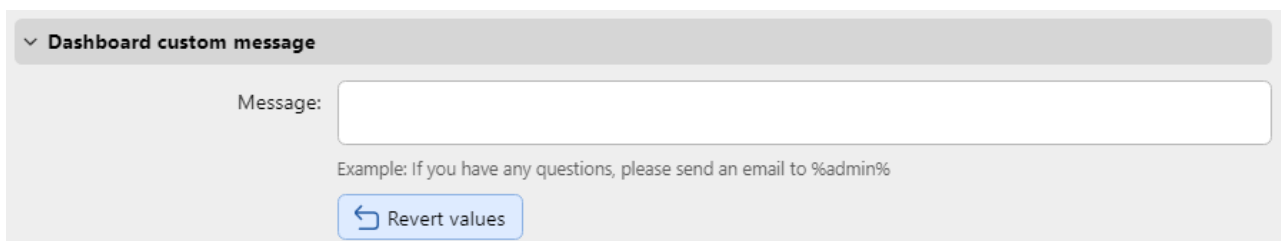
Active	Name
<input type="radio"/>	Blue Ice
<input type="radio"/>	Cherry Blossom
<input type="radio"/>	Classic
<input type="radio"/>	Coloured Rays
<input type="radio"/>	Purple Peace
<input checked="" type="radio"/>	Spring Touch (Default)

To change the theme, select one of the available themes, click **Activate**, and then click **Save**.

## 7.3.3 Dashboard custom message

Here you can enter a message to be displayed on the **KNM** users web accounts. After you change the message, click **Save** at the bottom of the **Personalization** settings tab.

The `%admin%` parameter can be used to display the email address of the **KNM** administrator within the message (the Administrator email set on the **General** settings tab).



The screenshot shows the 'Dashboard custom message' settings tab. It contains a text input field for the message, an example text 'Example: If you have any questions, please send an email to %admin%', and a 'Revert values' button.

## 7.3.4 Custom help

Here you can add a link to your own web-based help that will be displayed as a widget on the user's **KNM** home page.

To add a custom help link, enter the title and the link of your custom help, and then click **Save** at the bottom of the tab.

**Custom help**

The link is displayed on the user's KYOCERA Net Manager home page

Title:

Link:

### 7.3.5 Custom link in the KYOCERA Net Manager Desktop Client

Here you can add a link to your own web-based help (weblink, network path or local path) that will be displayed in **KNM Desktop Client**.

To add the custom help link, enter the title and the link of your custom help, and then click **Save** at the bottom of the tab.

**Custom link in the KYOCERA Net Manager Desktop Client**

The link is displayed in the KYOCERA Net Manager Desktop Client. It can be a weblink, a network path or a local path.

Title:

Link:

## 7.4 Task Scheduler Settings

The **Task Scheduler** settings tab serves as an interface for planning regular tasks in **KNM**. There are seven predefined tasks:

**Database and settings backup, Log backup, System Health Check, History deletion, Printer Discovery, System maintenance, and User Synchronization.**

Apart from these, you can import projects from CSV files, add scheduled reports, and execute external commands.

External commands are disabled by default. To enable them, switch the **scheduleExternalCommand** parameter in the *config.ini* file from *0* (disabled) to *1* (enabled).

Status	Action	Name	Period	Last run	Next run
<input checked="" type="radio"/>	Backup	Database and settings backup	Daily	05/09/2023 5:53:57 AM	05/10/2023 3:00:00 AM
<input checked="" type="radio"/>	History deletion	History deletion	Daily	05/09/2023 5:53:58 AM	05/10/2023 3:00:00 AM
<input type="radio"/>	Backup	Log backup	Daily	Never	-
<input type="radio"/>	Printer Discovery	Printer Discovery	Daily	Never	-
<input checked="" type="radio"/>	System Health Check	System Health Check	Minute	05/09/2023 6:09:06 AM	05/09/2023 6:14:00 AM
<input checked="" type="radio"/>	System maintenance	System maintenance	Daily	05/09/2023 5:54:00 AM	05/10/2023 3:00:00 AM
<input type="radio"/>	User Synchronization	User Synchronization	Daily	Never	-

## 7.4.1 Running and setting task schedules

### To manually run a task schedule:

- Select the task schedule that you want to run.
- Click **Run** on the **Task Scheduler** toolbar.

Or

- Right-click the task schedule.
- Click **Run** on the shortcut menu.

### To set a task schedule:

Double-click the task schedule that you want to set (or right-click it, and then click **Edit** in the actions shortcut menu). The respective task schedule properties panel opens on the right side of the screen. The task schedule properties panel is divided into four sections:

The screenshot shows a window titled "History deletion" with a close button (X) in the top right corner. The window is divided into four sections:

- General:** Contains an "Enabled" toggle switch (currently off), a "Name" field with the value "History deletion", and a "Description" field.
- Schedule:** Contains a "Repetition" dropdown menu set to "Daily", an "Every N-th day" field with the value "1", and an "Hours of run" field with the value "3". Below these fields is a note: "hh:mm, hh, h:mm, hh am, hh pm" and "For multiple values, separate with a comma or semicolon".
- Notification:** Contains a "Send a notification after performing the task:" dropdown menu set to "\*admin", a "Select a user or enter an email" label, and a checked checkbox for "Only in case of an error or warning:".
- Buttons:** At the bottom are "Save" and "Cancel" buttons.

At the bottom of the window, it says "Fields marked by \* are mandatory."

- In the uppermost section, you can enable or disable the schedule, enter its **Name**, and write its **Description**.

- In the **Schedule** section, you must set a period of **Repetition** for the task run and change the exact time of the task run start.
- In the **Notification** section, you can select to send an email notification. You must also choose if you want to send the notification every time or just in case of an error.
- The bottom section, if present, is particular to the type of task.

After you set the schedule, click **Save**.

## 7.4.2 Providing rights for task schedules

You can provide users with rights to change some task schedules settings themselves.

To provide users with rights to change settings of a task schedule:

1. Double-click the schedule that you want to set. The respective schedule properties panel opens on the right side of the screen.
2. On the bar on the upper-left corner of the panel, click **Rights**. The **Rights** tab opens.
3. Click **+Add user**. The Select user or group dialog box appears.
4. Select the user or the group of users that you want to provide with the rights, and then click **OK**.

## 7.4.3 Automatic database and log backup

There are two automatic backup tasks on the **Task Scheduler** tab. The database and settings backup and the log backup. The backup process is automatic. The files are compressed and saved to the **Backup** folder.

### Backup settings

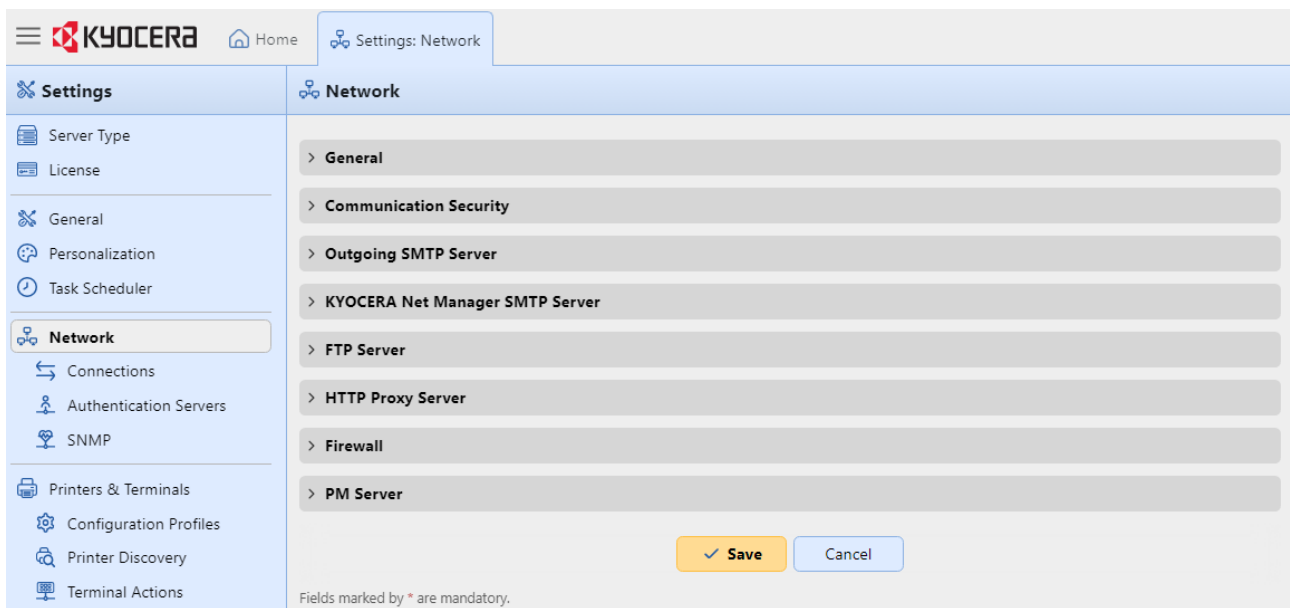
- **Destination folder:** The folder that stores the backup data.
- **Backup Password:** Password-protect the backup. If this field is left empty, the created backup is unprotected.
- **Confirm Password:** Confirm the above password.
- **Delete backup after \_\_\_ days:** The days after which the data are deleted from **KNM**.

The screenshot shows a 'Backup' settings panel with the following fields and values:

- Destination folder:** \* %app%\Backup (with a note: %app% is the KYOCERA Net Manager data folder)
- Backup password:** (empty field, with a note: If empty, unprotected backup is created)
- Confirm password:** (empty field)
- Delete backup after:** \* 7 days

## 7.5 Network Settings

On the **Network** settings tab, you can manage the network communication between the **KNM** server and other parts of **KNM**. It is divided into the following sections: **General**, **Communication Security**, **Outgoing SMTP Server**, **KYOCERA Net Manager SMTP Server**, **FTP Server**, **HTTP Proxy Server**, **Firewall**, and **PM Server**.



## 7.5.1 General

In this section, you can enter the hostname of the **KNM** Print server. This hostname is used by external components of the **KNM** system, such as embedded terminals or **KNM** Desktop Client, for communication with the **KNM** server.

▼ **General**

This server hostname: \*

Terminals, KYOCERA Net Manager Desktop Client and other components use this hostname when communicating with the server. It must match the certificate.

**i** During remote setup, the server hostname should be a valid hostname or IP address. A licenses update might change the hostname to **KNM.local**. Then the remote setup will fail and result in an error message.

## 7.5.2 Communication Security

In this section, you can choose how your security certificates are managed.

**KNM** offers three different certificate management modes:

1. **Built-in Certificate Authority** - This is the default mode for new installations. **KNM** creates a self-signed CA certificate and uses it to sign server and client certificates. The public key of the CA certificate can be exported (click the **Export CA certificate** button) to install it to clients, so they trust **KNM** server. It is possible to specify the **Subject Alternative Name (SAN)**, which is set as a comma separated list of domain names and/or IP addresses. In case the certificate is compromised, click the **Generate new CA certificate** button, to generate a new one.
2. **Company Certificate Authority** - Your company CA generates an intermediate CA certificate which **KNM** uses to sign certificates for the server and clients. To generate an intermediate CA

certificate click **Create CSR** to create a Certificate Signing Request (CSR), sign it by your CA and click **Finish CSR** to finish CSR by importing signed certificate. If the intermediate CA certificate does not contain a CA root certificate in its chain, the administrator is prompted to upload the public key of the CA root certificate as well (the **Import CA root certificate** button appears).

3. **Manual Certificate Management** - Provide a certificate for the **KNM Server**. **KNM** creates no certificates; all certificates are managed by you. Click **Import Server certificate** to upload it. The certificate can be uploaded in *PEM* (public + private key separately) or in *PFX* format. The *PFX* format may be password encrypted. This mode is recommended only for expert users.

**Communication Security**

KYOCERA Net Manager secures communication with certificates which is an industry standard. Choose how certificates are managed.

Certificate authority mode: \*

- Built-in Certificate Authority**  
Server and clients are secured by certificates generated by the built-in certificate authority (CA). The CA certificate is self-signed. Export the CA certificate and install it to clients so they trust KYOCERA Net Manager Server. If the CA certificate is compromised, generate a new one. Server certificate will be regenerated automatically.  
[Generate new CA certificate](#) [Export CA certificate](#)
- Company Certificate Authority**  
Your company CA generates an intermediate CA certificate which KYOCERA Net Manager uses to sign certificates for the server and clients. To generate an intermediate CA certificate create Certificate Signing Request (CSR), sign it by your CA and finish CSR by importing signed certificate. Server certificate will be regenerated automatically.
- Manual Certificate Management**  
Provide a certificate for the KYOCERA Net Manager Server. KYOCERA Net Manager creates no certificates, all certificates are managed by you.

Server alternative names:

Comma separated list of DNS names and/or IP addresses. To set new Subject Alternative Name (SAN) for KYOCERA Net Manager Server generate new Server certificate. Server hostname is included automatically.

[Generate new Server certificate](#)

When upgrading an existing **KNM** installation, the **Certificate Authority mode** is selected according to the existing server certificate:

- if the certificate is not CA, then the mode is set to **Manual Certificate Management**.
- if it was generated by **KNM** before, then the mode is set to **Built-in Certificate Authority**.
- in other cases, the mode is set to **Company Certificate Authority**.

### 7.5.3 Outgoing SMTP Server

To send email reports, send error messages to users, send automatically generated PIN to users, and forward scanned documents, you have to configure the email server where all the emails are forwarded to.

To configure the server, do the following:

Select a **Type** from *Classic SMTP Server*, *Microsoft Exchange Online* or *Gmail*.

For *Classic SMTP Server*:

1. Enter the server hostname or IP address in the **Server** text box. If the email server listens to other than the 25 TCP port, change the **Port** setting to the correct value.
2. Choose between the *Prefer StartTLS (default)*, *Implicit TLS*, and *Require StartTLS Security* options.
3. Optionally choose to **Validate certificate** or not.
4. If credentials are required, enter the **User** and **Password**.
5. Enter the address that you want to be displayed as the **Sender email** on PIN, alert and report messages.

6. After you enter the data, you can click **Test** to test the connection to the email server, and click **Save** to save your changes.

For *Microsoft Exchange Online*:

1. If you have already set up a Microsoft Exchange Online server in the **Connections** settings, the server is available in the **Connections** field drop-down. If not, you can click on the **Connections** field and then click **Add new** to add your Microsoft Exchange Online server connection. For more information, check [Microsoft Exchange Online Setup](#).

The screenshot shows the 'Outgoing SMTP Server' configuration window. Under the 'Type' section, 'Microsoft Exchange Online' is selected with a radio button. The 'Connections' dropdown menu is open, showing 'Microsoft Exchange Online' as the selected option. Below it, the 'User' field has a dropdown menu with 'Add new...' selected. The 'Sender email' field contains 'Microsoft Exchange Online'. A 'Test' button is located at the bottom of the form.

2. If credentials are required, enter the **User**.
3. Enter the address that you want to be displayed as the **Sender email** on PIN, alert and report messages.
4. After you enter the data, you can click **Test** to test the connection to the email server, and click **Save** to save your changes.

For *Gmail*:

1. If you have already set up a Gmail server in the **Connections** settings, the server is available in the **Connections** field drop-down. If not, you can click on the **Connections** field and then click **Add new** to add your Gmail server connection. For more information, check [Gmail with OAuth2 Setup](#).

The screenshot shows the 'Outgoing SMTP Server' configuration window. Under the 'Type' section, 'Gmail' is selected with a radio button. The 'Connections' dropdown menu is open, showing 'Gmail' as the selected option. The 'User' field is empty. The 'Sender email' field contains 'KNM@KNM.local'. A 'Test' button is located at the bottom of the form.

2. If credentials are required, enter the **User**.
3. Enter the address that you want to be displayed as the **Sender email** on PIN, alert and report messages.
4. After you enter the data, you can click **Test** to test the connection to the email server, and click **Save** to save your changes.

## 7.5.4 KYOCERA Net Manager SMTP Server

In this section you can view and modify the SMTP server settings.

- **SMTP (STARTTLS)** - Enable when using unsecure communication or secure communication over STARTTLS. Port 25 by default.
- **SMTPS(SSL/TLS)** - Enable when using secure communication over SSL/TLS. Port 587 by default.

If scanning to **KNM** is enabled, set the port shown here in the device's SMTP settings.

## 7.5.5 FTP Server

In this section, you can set the **FTP server port** that terminals use when sending scan jobs to **KNM** over the FTP protocol. The FTP port is **21** by default, and the range is **0 to 65535**. If you click the **Generate new password** button, there is a confirmation pop-up informing that if a new password is generated, all the terminals need to be reconfigured.

## 7.5.6 HTTP Proxy Server

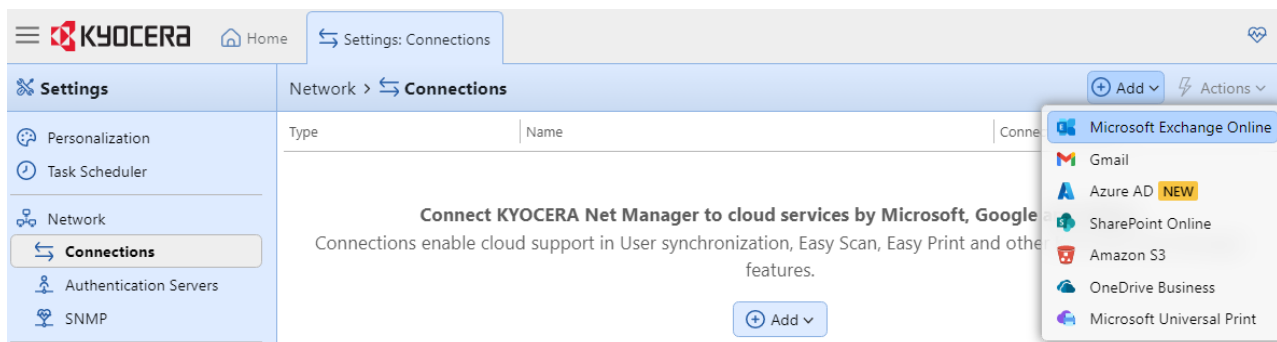
In this section, you can set up a **KNM Proxy server** which can be used for activating a license. Mandatory fields are **Server** (name) and **Port**. After changing ports, restart all **KNM** services.

## 7.5.7 Firewall

In this section, you can **Allow editing firewall rules** of the Microsoft Windows Firewall and you can also **Reset firewall rules**.

## 7.6 Connections Settings

On the **Connections** settings tab, you can connect **KNM** to external cloud services.



Click **Add** and select one of the following available services:

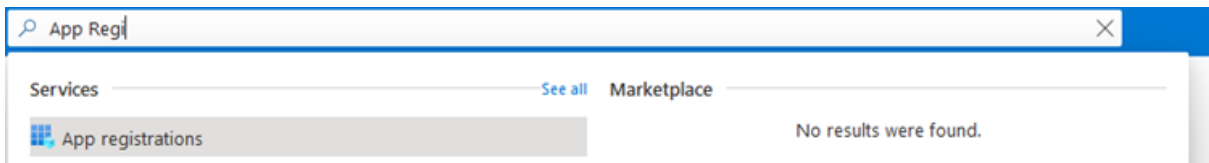
- Microsoft Exchange Online
- Gmail
- Azure AD
- SharePoint Online
- Amazon S3
- OneDrive Business
- Microsoft Universal Print
- the **KNM** and ScannerVision integration (embedded terminals are required)

### 7.6.1 Microsoft Exchange Online Setup

It is first needed to set up Microsoft Exchange Online in Microsoft Azure, and then configure it in **KNM**.

#### Microsoft Exchange Online setup in Microsoft Azure

1. Log in to the [Microsoft Azure portal](#) and go to **App registrations**.



2. Create a **New registration:**  
**App registrations**



3. Create an Azure application:
- Name** - The name for this application (this can be changed later). For example, *MS Exchange Online*. It is important to use the same name as the one used in **KNM** under Connections.
  - Supported account types** - Who can use this application or access this API? Select the *Accounts in this organizational directory only ({{Tenant name}} only - Single tenant)* option. Multitenant application can also be used if required, depending on the target audience of the application (what account will be used for authorization in **KNM**).
  - Redirect URI (optional)** - The authentication response is returned to this URI after successfully authenticating the user. Select the *Public client/native (mobile&desktop)* option from the drop-down and fill in <https://login.microsoftonline.com/common/oauth2/nativeclient> as the redirect URI.
  - Click **Register**.

**Register an application** ...

\* Name  
The user-facing display name for this application (this can be changed later).

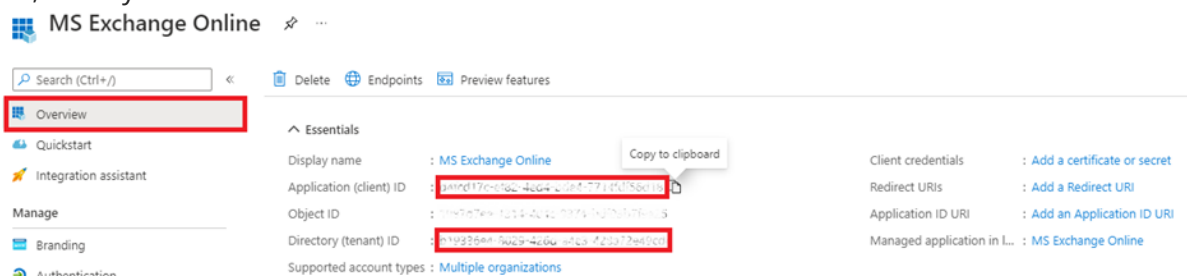
Supported account types  
Who can use this application or access this API?  
 Accounts in this organizational directory only ( [redacted] only - Single tenant)  
 Accounts in any organizational directory (Any Azure AD directory - Multitenant)  
 Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)  
 Personal Microsoft accounts only  
[Help me choose...](#)

Redirect URI (optional)  
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

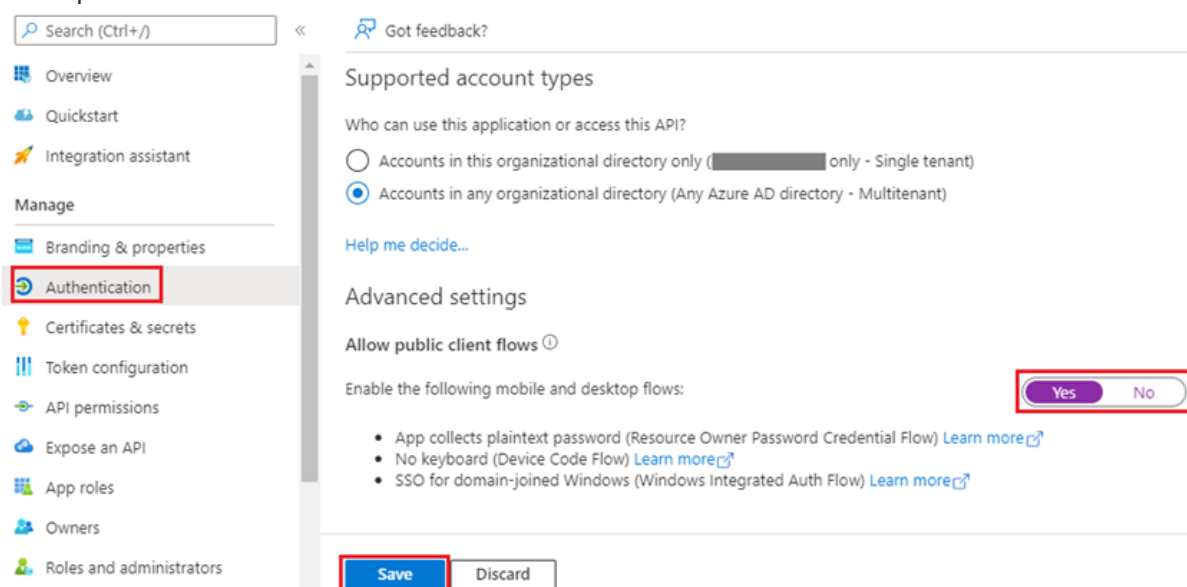
Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

- The new app overview page opens. Copy the **Application (client) ID** and the **Directory (tenant) ID**, as they are needed for the connection to **KNM**.



- On the left-hand menu, click **Authentication**. In Advanced settings, under Allow public client flows, select **Yes** next to Enable the following mobile and desktop flows, and then click **Save** at the top.



- On the left-hand menu, click **API permissions** and add the additional permissions required for the correct functionality:
  - Microsoft Graph: **offline\_access** - Allows the app to see and update the data you gave it access to, even when you are not currently using the app. This does not give the app any additional permissions.
  - Microsoft Graph: **User.Read** - Sign in and read user profile.
  - Microsoft Graph: **IMAP.AccessAsUser.All** - Allows the app to read, update, create and delete email in your mailbox. Does not include permission to send mail.
  - Microsoft Graph: **POP.AccessAsUser.All** - Allows the app to read, update, create and delete email in your mailbox. Does not include permission to send mail.
  - Microsoft Graph: **SMTP.Send** - Allows the app to send emails on your behalf from your mailbox.

Search (Ctrl+) Refresh Got feedback?

Overview  
Quickstart  
Integration assistant

Manage  
Branding  
Authentication  
Certificates & secrets  
Token configuration  
**API permissions**  
Expose an API  
App roles

Configured permissions

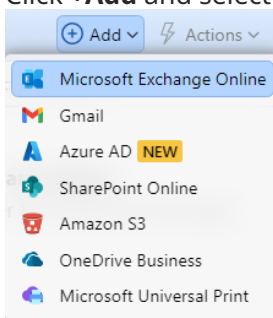
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (5)				
IMAP.AccessAsUser.All	Delegated	Read and write access to mailboxes via IMAP.	No	...
offline_access	Delegated	Maintain access to data you have given it access to	No	...
POP.AccessAsUser.All	Delegated	Read and write access to mailboxes via POP.	No	...
SMTP.Send	Delegated	Send emails from mailboxes using SMTP AUTH.	No	...
User.Read	Delegated	Sign in and read user profile	No	...

## Microsoft Exchange Online setup in KNM

1. Log in to the **KNM** web administrator interface, and go to **KYOCERA, Settings, Connections**.
2. Click **+Add** and select *Microsoft Exchange Online* from the list.



3. In the pop-up window, fill in the required fields:

- a. **Title** - add the name you chose during App registration in MS Azure; for example, *MS Exchange Online*.
  - b. **Directory (tenant) ID** - the **Directory (tenant) ID** you copied during the MS Azure setup.
  - c. **Application (client) ID** - the **Application (client) ID** you copied during the MS Azure setup.
4. Click **OK**.
  5. After setting up the external system in **KNM**, you are requested to confirm a **code** through the Microsoft website (<https://microsoft.com/devicelogin>). The code you need to confirm is shown in the pop-up window, just below the link to the Microsoft website. There is timeout for confirming the code (usually it is 15 minutes).

**⚠ The email functionality will not work until the confirmation is successfully completed.**  
*This confirmation must be done with the Microsoft account that owns the email box (email address), which is used to connect to the exchange (Sender email in the KYOCERA, Settings, Network tab).*  
For example, if you use the sender email "print@somedomain.com", then you need to authenticate on the Microsoft website as this user during this step.

Microsoft Exchange Online is now connected to **KNM** and is ready to be used in the **Network** settings tab, as an Outgoing SMTP server, and in the **Jobs** settings tab, in Jobs via Email as a POP3 or IMAP server.

## Additional Settings

Send scan as the logged-in user

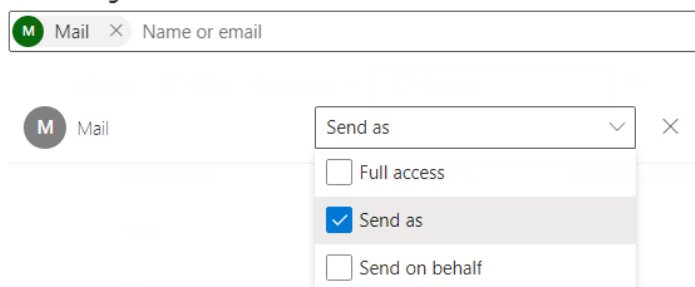
If **KNM** is set to send scans as the logged-in user in **KYOCERA**, Settings, Scanning & OCR - Default settings of an email with scan - Sender, the mailbox authenticated in **KNM** has to have a *Send As* permission for all users.

1. Log in to [Exchange admin center](#).
2. Go to Mailboxes, select all users.
3. Click on "**Mailbox delegation**".
4. Select the mailbox that has been authenticated in **KNM** when the MS Exchange Online connector was created (you can find it in **KYOCERA**, Settings, Connections).
5. Choose "**Send as**" permission.

### Manage mailbox delegation

Apply these changes to the 6 selected recipients

Add a delegate \*



The screenshot shows the 'Add a delegate' interface. At the top, there is a search bar with a green 'M' icon and the text 'Mail' followed by a close button 'X' and the placeholder text 'Name or email'. Below this, a dropdown menu is open for a selected mailbox, showing three options: 'Full access' (unchecked), 'Send as' (checked), and 'Send on behalf' (unchecked). The 'Send as' option is highlighted in grey.

6. Click Save.

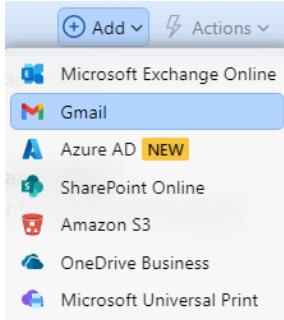
Your selected mailbox for outgoing emails has now been assigned the rights to send scanned documents on behalf of the user who scanned them.

If you select to send emails as the default sender, this change is not required.

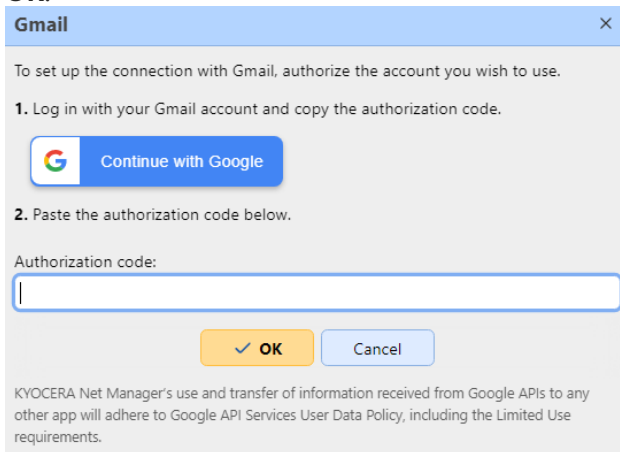
## 7.6.2 Gmail with OAuth2 setup

To configure Gmail with OAuth2 in **KNM**:

1. Log in to the **KNM** web administrator interface, and go to **KYOCERA, Settings, Connections**.
2. Click **+Add** and select **Gmail**.



3. In the pop-up window, you are requested to authorize the connection by clicking **Continue with Google**, copying the generated code, pasting it in the **Authorization code** field, and clicking **OK**.

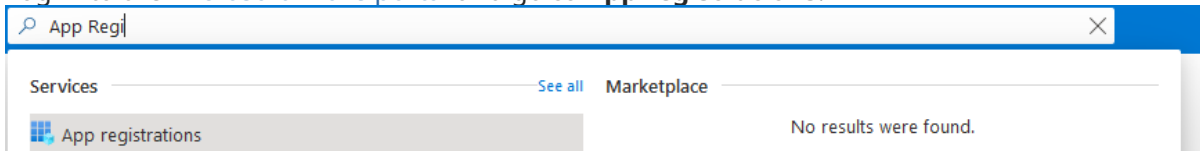


Gmail is now connected to **KNM** and is ready to be used in the **Network** settings tab as an Outgoing SMTP server, and in the **Jobs** settings tab, in Jobs via Email as a POP3 or IMAP server.

## 7.6.3 Azure AD with Microsoft Graph setup

### Azure Application Configuration

1. Log in to the [Microsoft Azure portal](#) and go to **App registrations**.



2. Click **New registration** to create a new application or select an existing application.
3. If you are creating a new application, set the **Name** and in **Supported account types** select *Accounts in this organizational directory only ({{Tenant name}} only - Single tenant)* option if all your

users are members of your tenant. Multitenant application can also be used if required, depending on the target audience of the application.

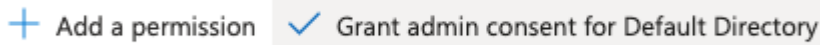
4. You can skip the **Redirect URI** settings for now (described in step 7). Click **Register** to create the application.
5. From the application's Overview screen, go to **API Permissions** and select **Microsoft Graph API** and the required type of permission (**Delegated** or **Application**) as illustrated below. The required permissions are:

*Microsoft Graph \ Group.Read.All, Microsoft Graph \ User.Read, Microsoft Graph \ User.Read.All*

+ Add a permission    ✓ Grant admin consent for Default Directory

API / Permissions n...	Type	Description	Admin consent req...	Status
▼ Microsoft Graph (3) ...				
Group.Read.All	Application	Read all groups	Yes	✓ Granted for Default Directory ...
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for Default Directory ...
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for Default Directory ...

6. The status "*Granted for Default Directory*" needs to be set on all permissions that require them. All needed permissions can be added and configured with the buttons at the top of the list of permissions.



Use **"Add a permission"** to add new permission.

Use **"Grant admin consent for Default Directory"** to set the status of the permission as "Granted for Default Directory".

7. Go to the **Authentication** settings, and under Platform configurations, click **Add a platform**. Then select **Web**, and list all redirect URLs for your Azure application. For the actual URLs, use the hostname (and port) of your server in the following format: *https://{hostname:port}/auth* and click **Configure**.

8. In the application's overview page, save the **Application (client) ID** and the **Directory (tenant) ID**, as they are needed for the **KNM** configuration.

9. Click **Add a certificate or secret** next to **Client credentials** and complete the following steps:

## Add a client secret

Description: Enter a description for this client secret

Expires: Custom

Start:

End:

- Recommended: 180 days (6 months)
- 90 days (3 months)
- 365 days (12 months)
- 545 days (18 months)
- 730 days (24 months)
- Custom

- Click **New client secret**.
- Add a **Description**.
- Set the expiration for the key.
- Click **Add**.
- Save the **client secret key Value**, because you need it for the configuration in **KNM** and you cannot retrieve it later.

## Configuration in KNM

Go to **KYOCERA, Settings, Connections** to connect **KNM** to Azure AD. Click **Add** and select *Azure AD* from the list. In the pop-up window, fill in the required information:

Azure AD

Title: \* Azure AD

Directory (tenant) ID: \* Directory (tenant) ID from MS Azure

Application (client) ID: \* Application (client) ID from MS Azure

Security key: \* \*\*\*\*\*

OK Cancel

Fields marked by \* are mandatory.

- **Title:** Add a title for the connection.
- **Directory (tenant) ID:** Add the **Directory (tenant) ID** you saved from Azure.
- **Application (client) ID:** Add the **Application (client) ID** you saved from Azure.
- **Security key:** Add the (secret) **Value** you saved from Azure.

Click **Save** and your Azure AD connection is now complete.

Synchronization and authentication through an Azure AD with Microsoft Graph can be used via the following steps:

1. [Adding an Azure AD authentication server in KYOCERA, Settings, Authentication Servers.](#)
2. [Adding an Azure AD synchronization source in KYOCERA, Settings, User Synchronization.](#)

## Microsoft single sign-on

To use Microsoft single sign-on:

1. Enable "**Use as an authentication server**" in **Azure AD synchronization source - Users tab** prior to synchronizing users or enable Azure as an authentication server manually for selected users in their details on the **Users** main page.
2. In the Azure authentication server settings, enable displaying the '**Sign in with Microsoft**' login method.

What happens when a user tries to sign in with Microsoft in the **KNM** Web UI:

- The user clicks the single sign-on button.
  - If the user is not signed in to Microsoft in the browser, they are forwarded to the Microsoft login page to sign in, and then logged into **KNM** with the provided account.
  - If the user is signed in to Microsoft with one account only, they are automatically logged into **KNM** with this account (limitation).
  - If the user is signed into two Microsoft accounts, they are forwarded to the Microsoft login page and are given a choice to select the account to continue with.
- Logout in **KNM** Web UI signs out the user only locally, not from Microsoft.

When Microsoft single sign-on is enabled, the **Sign in with Microsoft** button is always displayed on the **KNM** Web UI login page, but only users who use Azure AD as their authentication server can use it to log in. Any attempt to use Microsoft single sign-on by a user who does not use the Azure AD authentication system will end with an error.

## Limitations

- Only **the first 20 groups per user are synchronized**. A group is created in **KNM** only if it is among the first 20 groups for at least one user in Azure AD.
- Only one instance of an Azure AD authentication server and Azure AD synchronization source can be created in **KNM**.
- If a user uses the **Sign in with Microsoft** button and they are currently signed into one Microsoft account in the browser, they are automatically logged into **KNM** with this account. There is no option to switch to another account. To use another account, the user has to sign out on any Microsoft services first, and upon the next use of the single-sign-on button, they will be asked for a new login.

Users using Azure AD authentication server cannot sign in on the **KNM** Web User Interface with a PIN. However, they can use their PIN on the **KNM** Embedded terminals or in **KNM** Desktop Client.

## 7.6.4 Smart Workflows

In order to create a Smart Workflow you need to install and configure the ScannerVision server to work with the **KNM** server.

ScannerVision is a solution to automate document workflows, by capturing, processing, and storing scanned documents. This may include bar code reading, recognizing texts with the help of Optical Character Recognition (OCR), or converting documents to another format. Storage possibilities include a network folder, a database, cloud storage or storing as an e-mail attachment.

ScannerVision extends the features of **KNM** by allowing the user to perform a customized and personalized scan workflow, and can utilize the user's credentials to access the storage where the scanned document will be placed, making not only secure printing possible, but also secure scanning.

## Requirements

Minimum requirements prior to the installation:

- License for the **KNM** server + license for ScannerVision
- Two servers setup (one for the **KNM** server, one for the ScannerVision server). In case of a **KNM** Central Server setup, one server can be used.
- ScannerVision server 9.1+
  - **KNM** Embedded 7.5.9
  - **KNM** Embedded 8.1.1+

## ScannerVision Server Installation

.NET Framework 4.8 has to be installed on the server before installing ScannerVision. If it is not installed, open Server Manager and install it.

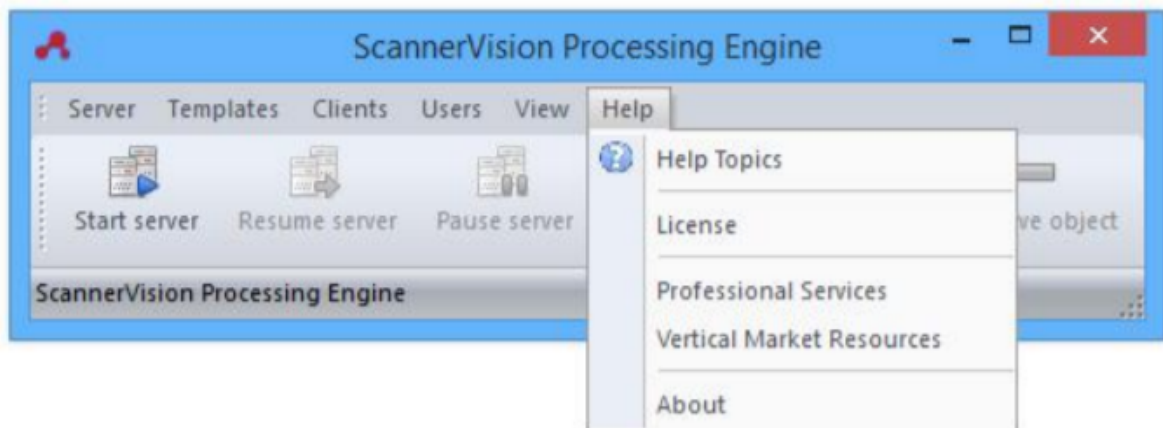
To install the ScannerVision server:

1. Run the ScannerVision installer.
2. Follow the installation wizard's instructions and install the server.
3. Activate the product.

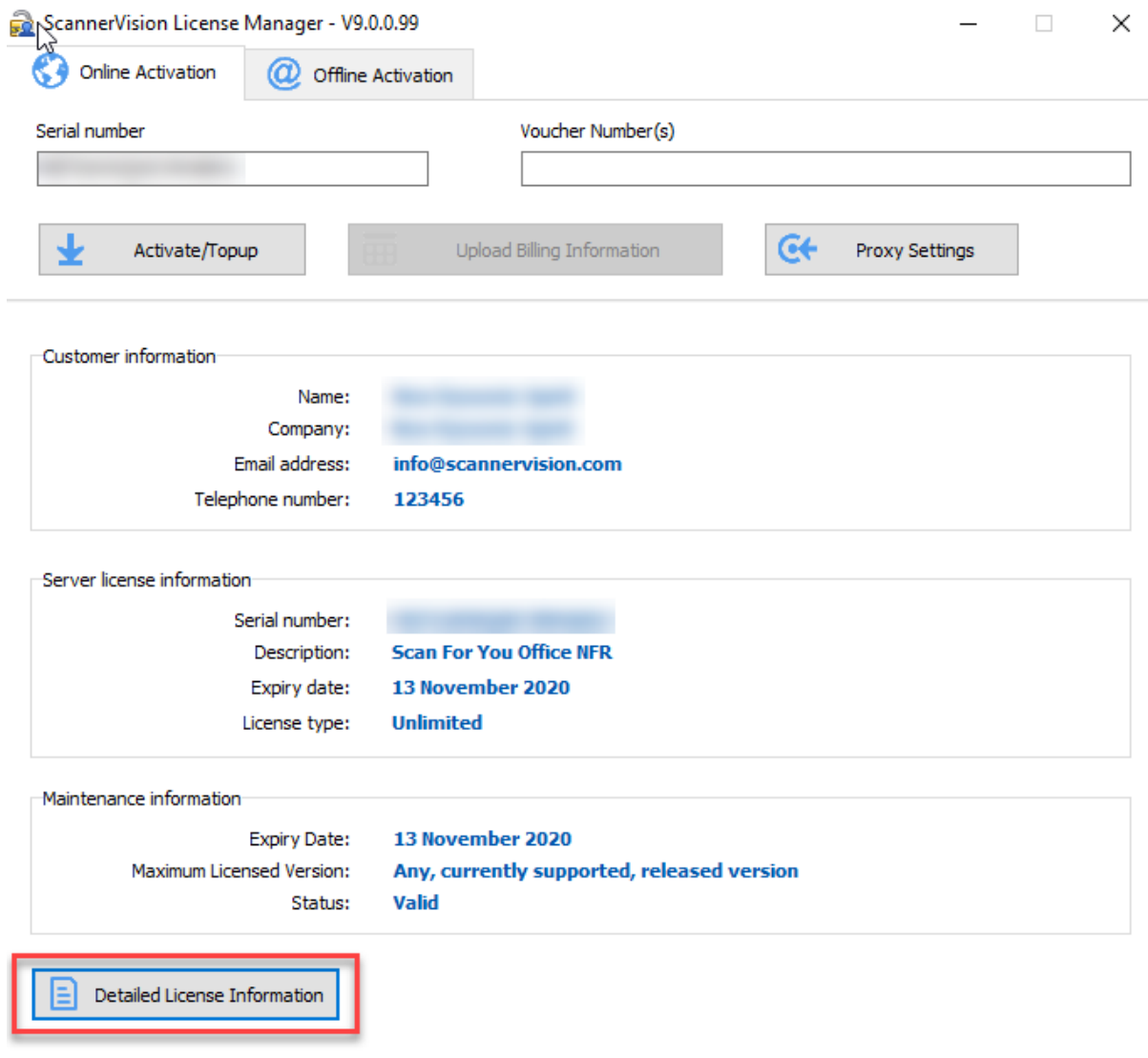
## License check

Once the ScannerVision server is installed and activated, verify the license information:

- Open the ScannerVision Processing Engine user interface application.
- On the top menu, click **Help, License**.



- ScannerVision License Manager opens. Click **Detailed License Information**.



- Check if the number corresponds to the **KNM** device licenses number.

## Configuration

Once the ScannerVision server is installed, there are configuration steps to be done, both in **KNM** and in ScannerVision:

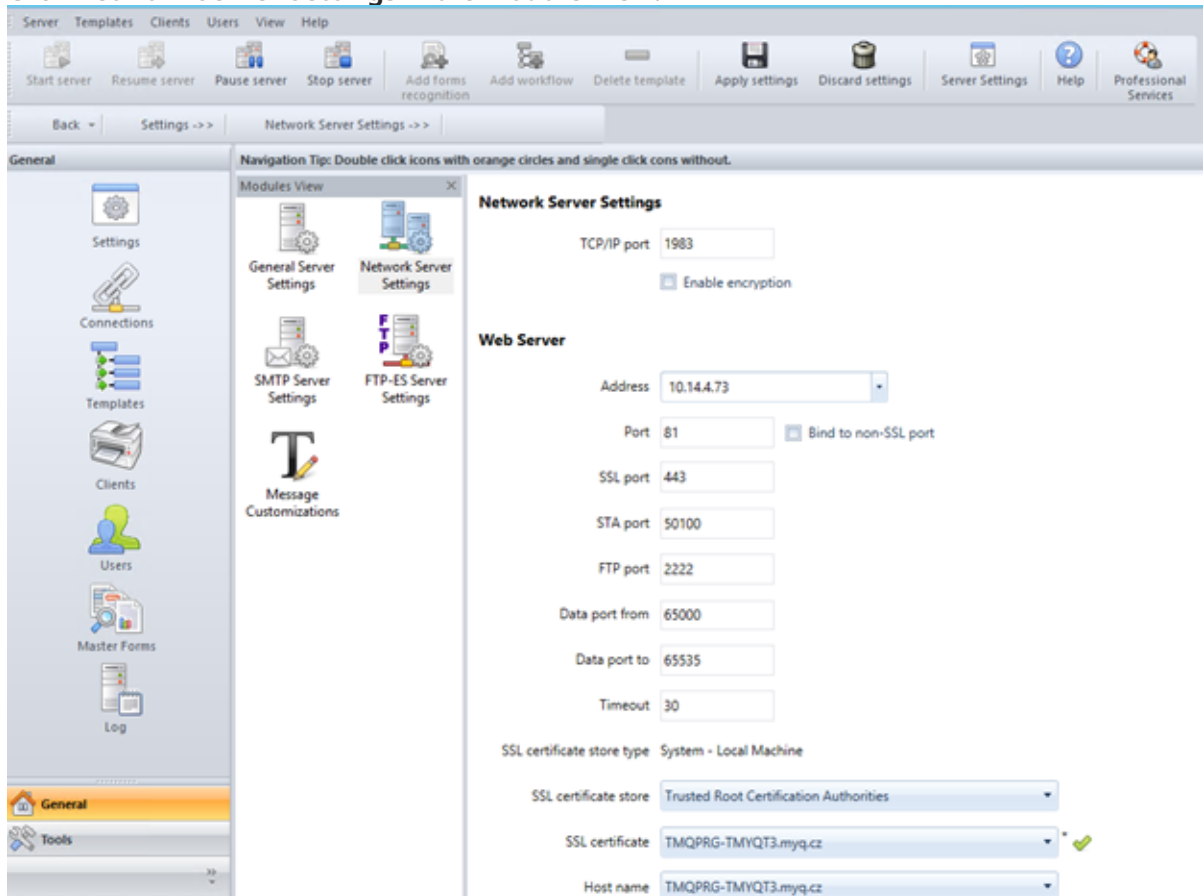
- [Configuring ScannerVision](#)
  - [Templates](#)
  - [Clients](#)
  - [Users](#)
- [Adding ScannerVision as a terminal action in KNM](#)

### Configuring ScannerVision

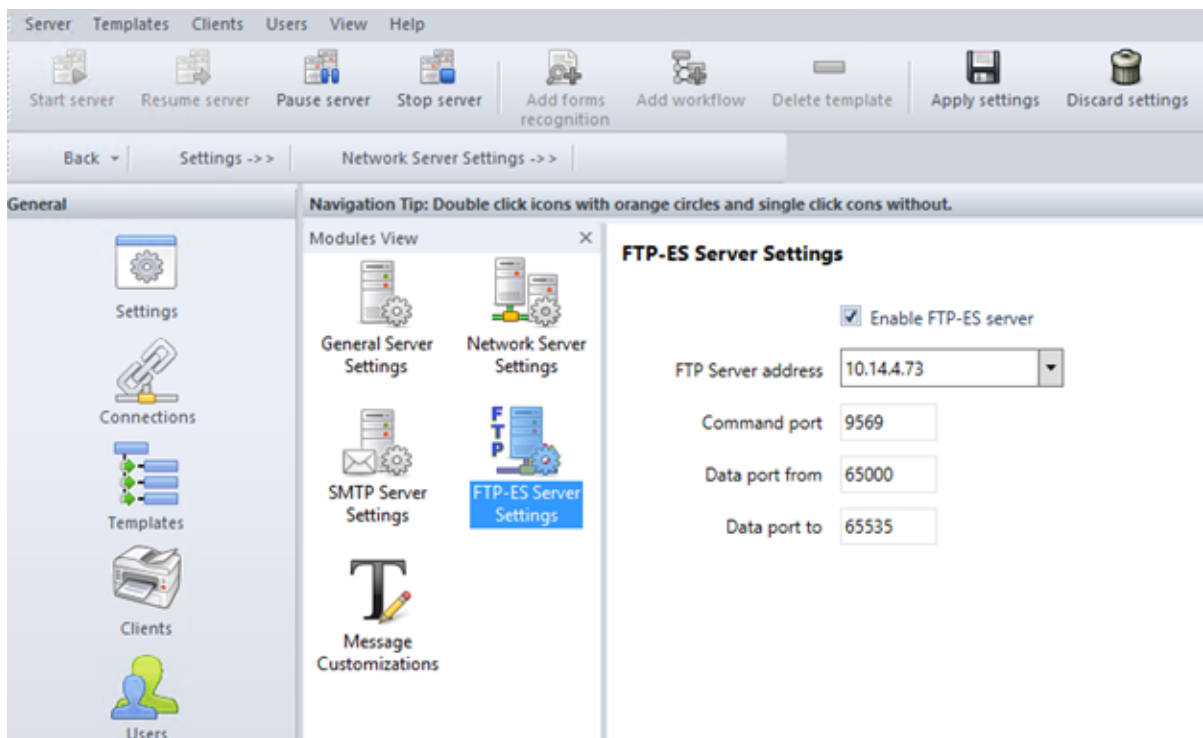
In order to set ScannerVision properly, you need to configure Network settings, [Templates](#), [Clients](#) and [Users](#).

## Network Settings

1. Open ScannerVision. **Settings** is shown by default.
2. Click **Network Server Settings** in the **Module View**.



3. Add the IP address or hostname of the ScannerVision Web Server in the **Address** field.
4. Change the preset ports if necessary.
5. Enable/disable non SSL.
6. Configure the **FTP-ES server settings**:



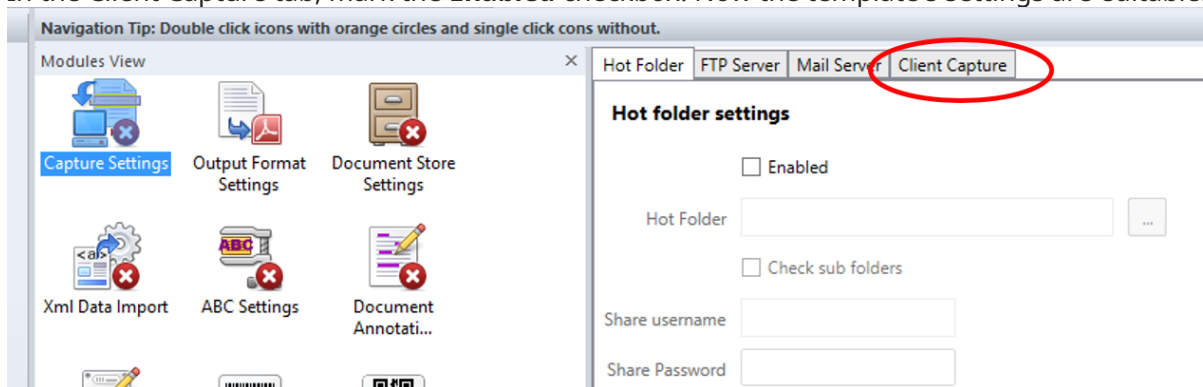
7. **Save** your settings.

## Templates

Templates control what actions ScannerVision performs. They determine where documents come from, what processing is done on them and where they ultimately end up. Multiple templates can be defined and assigned to users and groups.

To add a new template:

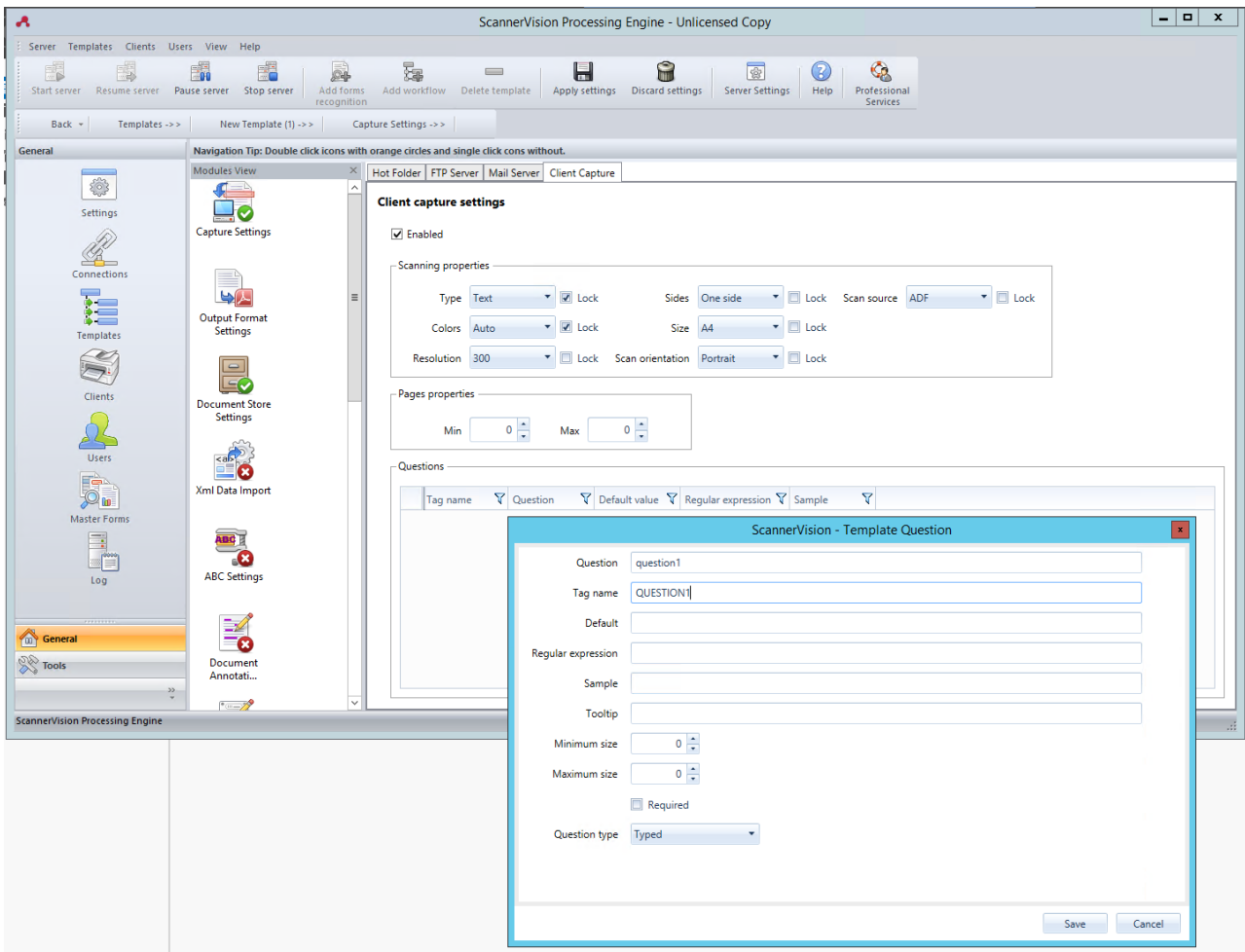
1. Open ScannerVision Processing Engine and click **Templates** in the **Navigation Pane**.
2. Click **Add Workflow** on the top menu.
3. **Name** the new template and mark it as **Enabled**.
4. Click **Apply Settings** on the top menu.
5. Once saved, double-click on the new template. In the right tab of the window, select **Client Capture**.
6. In the Client Capture tab, mark the **Enabled** checkbox. Now the template's settings are editable.



## Adding Questions on a Template

Questions are used to capture necessary document information. To add a new **Question** to a template, in the Client Capture tab:

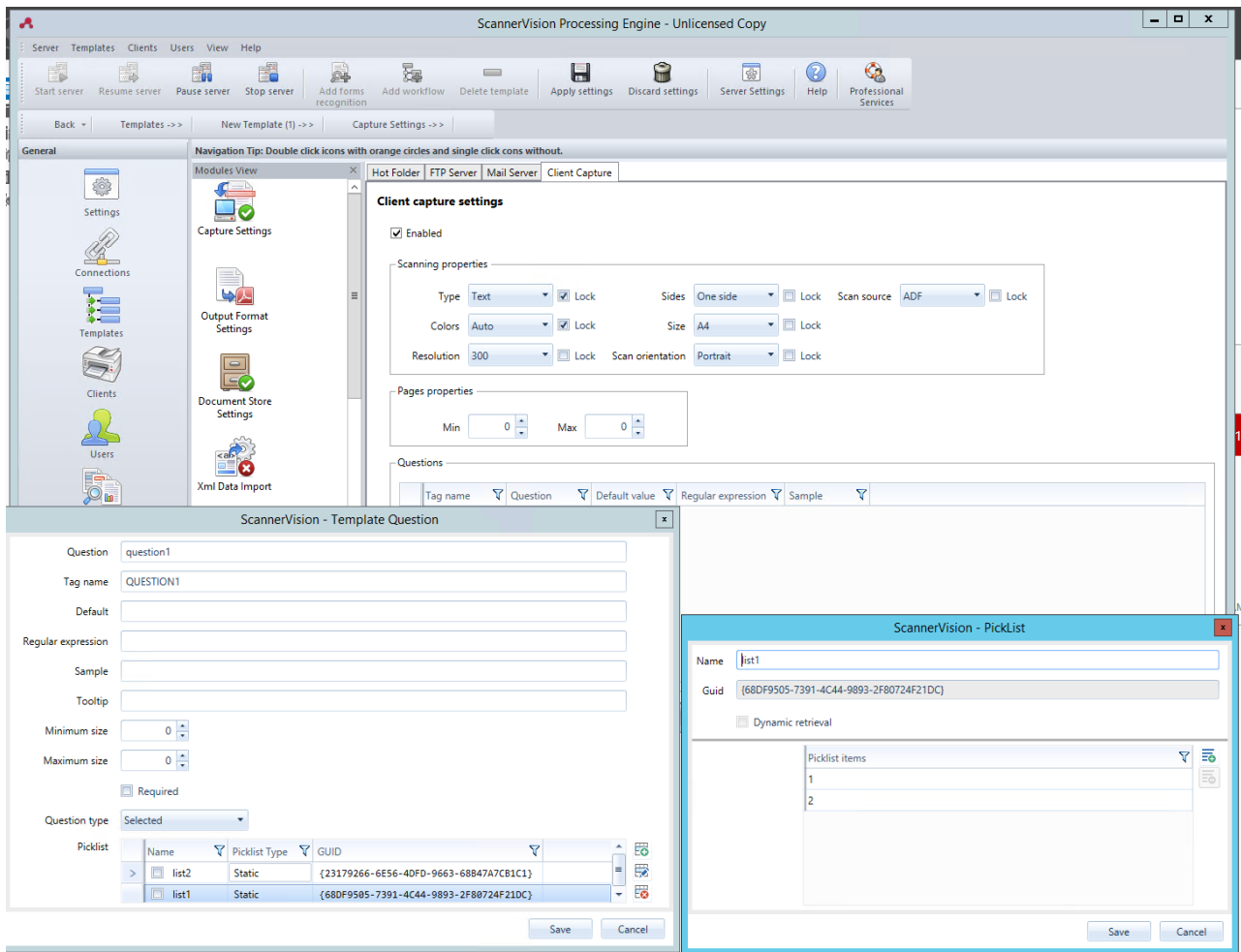
1. Right click on the **Questions** area.
2. Select **Add question**.
3. In the new Template Question window, fill in the **Question**, **Tag name**, and **Default** text fields, and any other of the optional fields.
4. In **Question Type** select *Typed*.
5. Click **Save**.



### Adding a PickList to a Question

A **PickList** can be added to a **Question** within a template, if the **Question Type** selected is *Typed*. To add a **PickList**:

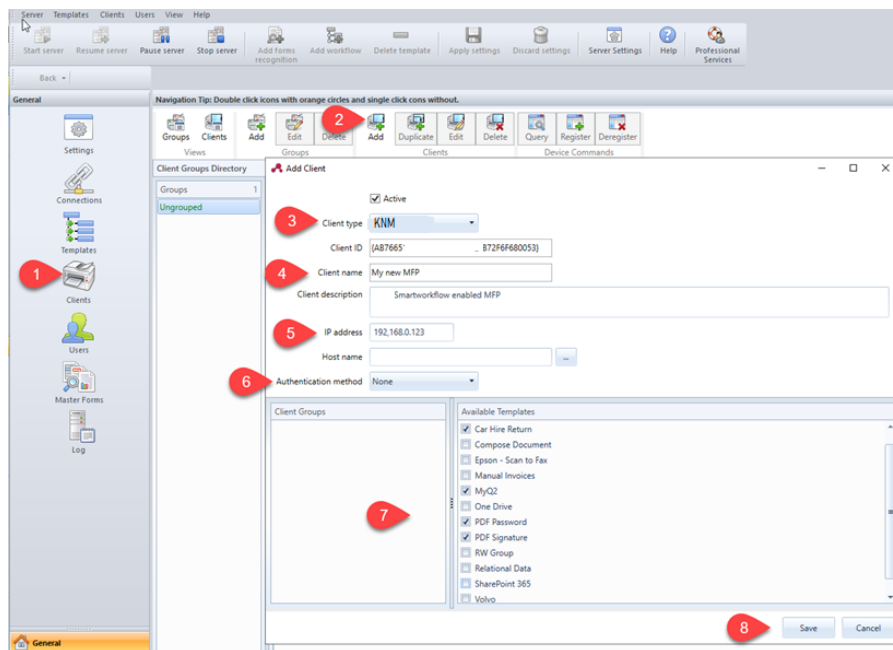
1. Click on the **Add PickList** button on the right.
2. Once there, select *Static* as the **PickList Type**.
3. In the Picklist window, enter a **Name** for the picklist.
4. Add picklist items by pressing the plus (+) button on the right.
5. Click **Save**.
6. Once saved, select the picklist(s) to be displayed for this question and click **Save**.



## Clients

The clients you configure here represent the **KNM** terminals connected to ScannerVision. To add a client, go to ScannerVision Processing Engine and:

1. Click **Client** on the **Navigation Pane**.
2. Click **Add** under the **Clients** view.
3. Choose **KNM** as the **Client type**.
4. Optionally add a **Client name** and **Client description**.
5. Add the printing device's **IP address** (make sure to use the device's IP address and not the **KNM** server one).
6. Choose an **Authentication method** from:
  - a. *None* - everyone can access the same templates
  - b. *ScannerVision* - Used for Single Sign On; Users have customized template lists.
7. Choose the templates to be accessed by everyone, in case *None* was the authentication method of choice.
8. Click **Save**.

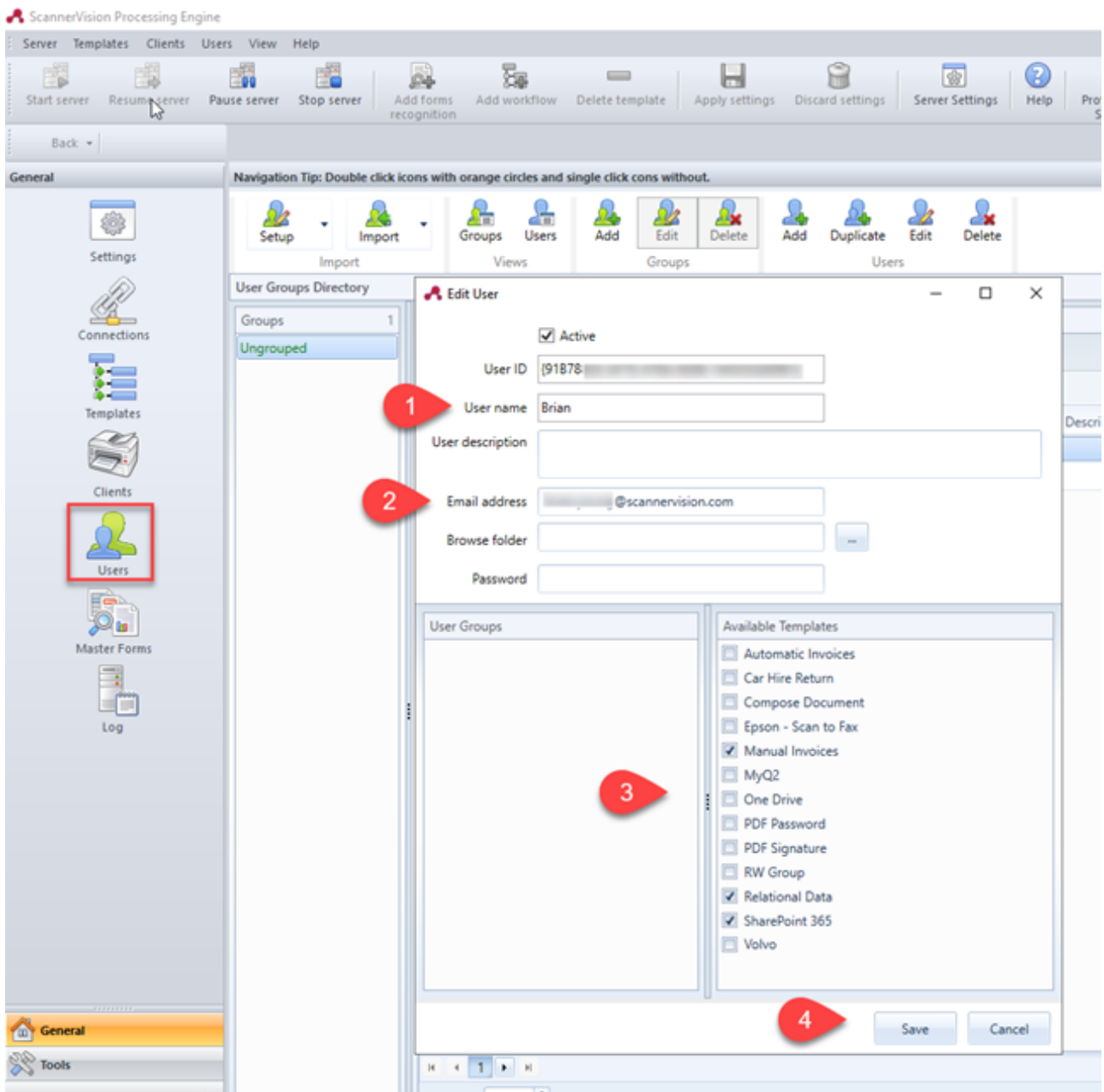


## Configuring Users

Users can be imported from a Windows Server, LDAP, AD or they can be manually added. For further instructions, please check the *ScannerVision User Manual*. Users also need to have templates assigned to them.

Whichever method is chosen, the users in ScannerVision have to match **KNM** Users. If users are imported, their properties such as names and email addresses will match, however **Templates** will still need to be assigned to them. To check and make necessary modifications, go to ScannerVision Processing Engine, click **Users** on the **Navigation Pane** and:

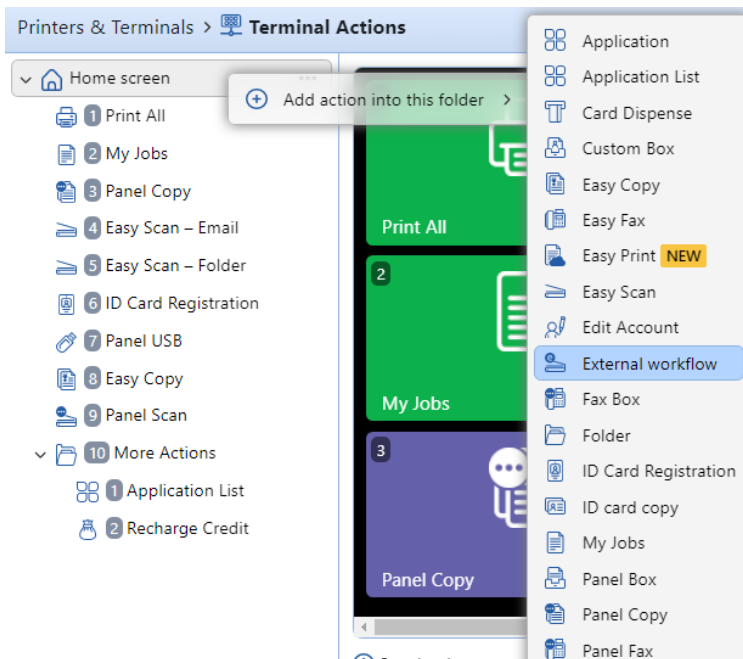
1. Make sure that the **User name** matches the **KNM** user name (if users were manually added).
2. Make sure that the **Email address** matches the **KNM** user's email address (if users were manually added).
3. Select templates for the user from the **Available Templates**.
4. Click **Save**.



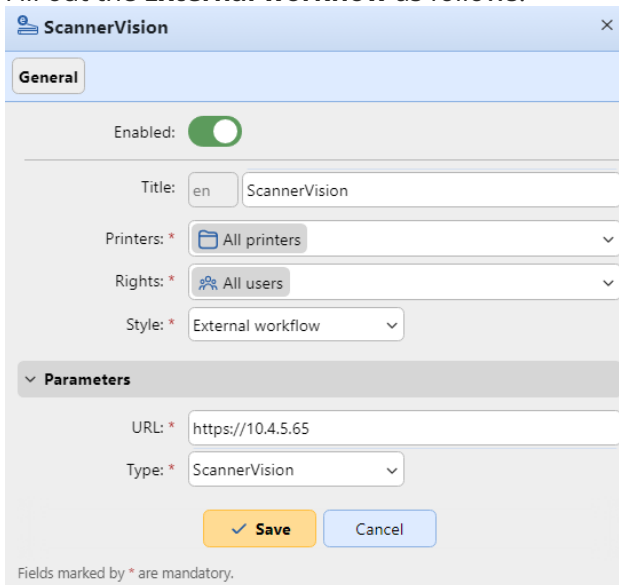
### Adding ScannerVision as a Terminal action in KNM

After configuring ScannerVision (network settings, templates, clients, users), you should create a Smart Workflow in **Terminal Actions**.

1. Go to **KYOCERA, Settings, Terminal Actions**.
2. Right-click on **Home screen**, select **Add action into this folder**, and then click on **External workflow** on the list of actions. The action is added to the list and the terminal preview. Double-click on it to modify its settings. The node's properties panel opens on the right side.



3. Fill out the **External workflow** as follows:



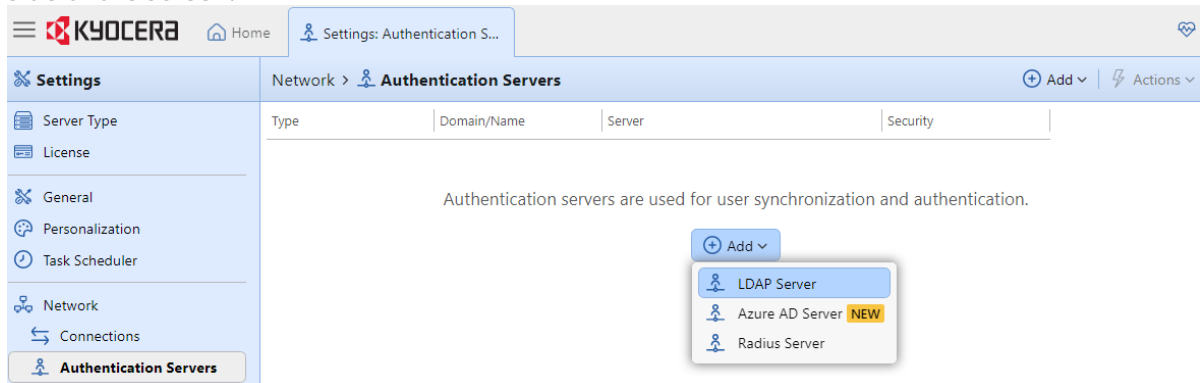
- a. Enter a **Title**. After saving, this will be shown as the name of the **External workflow** action in the **Home** screen pane and on the terminal preview.
- b. Enter the **URL** of the ScannerVision server; *ScannerVisionServer:port*. *http* or *https* depends on the ScannerVision server settings.  
The port number is not required if the default settings (80 for non SSL and 443 for SSL) are used on the ScannerVision server. If the port was changed, the port number is required.  
For example: *https://10.14.5.125* for SSL only with the default port used and *http://10.14.5.125:81* for non SSL and the port was changed from 80 to 81.
- c. Change the **Printers** and/or **Rights** if you want to create a specific Smart Workflow.
- d. Click **Save**.

## 7.7 Authentication Servers Settings

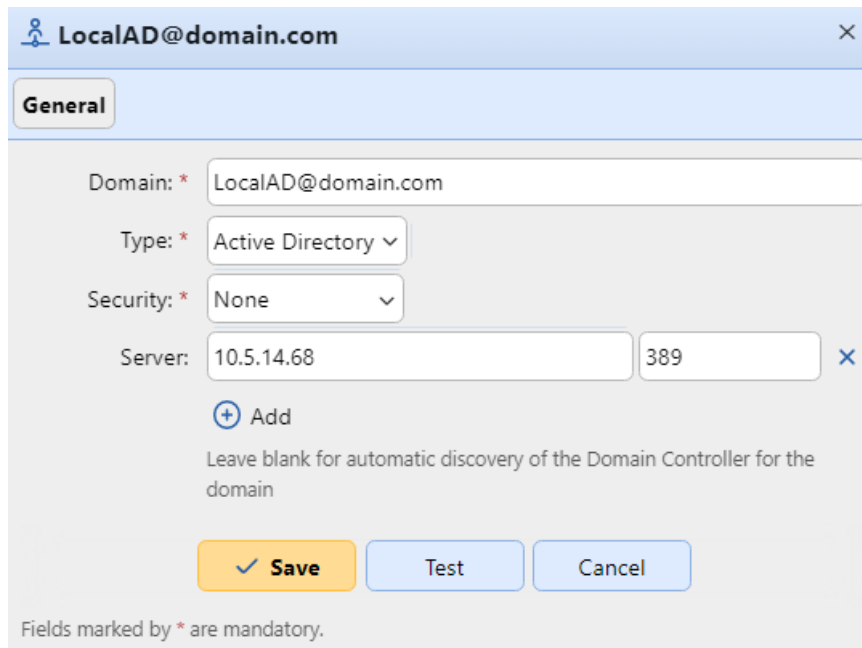
If you want to authenticate users against an LDAP server, synchronize users from an LDAP server, synchronize users from your Azure AD and use Microsoft SSO for the **KNM** web UI or authenticate users against a Radius server, you have to add all the servers on this tab.

### 7.7.1 Adding a new LDAP server:

1. Click **+Add** and select **LDAP Server**. The new LDAP server properties panel opens on the right side of the screen.



2. Enter the LDAP **Domain**.
3. Select the LDAP **Type**. You can select from *Active Directory*, *Novell*, *OpenLDAP*, and *Lotus Domino*. (For *Active Directory* you must select **SSL** in the **Security** field and the **Server** port must be 636)
4. If you want the communication with the LDAP to be secured, select the **Security** protocol that you want to use.
5. Enter the **Server** IP address or hostname and the communication port. (For *Active Directory* you can leave the IP address or hostname empty if you do not know them. The server will then be saved as Auto-discover)
6. If you have more addresses related to one LDAP server, you can add them by clicking **Add**.
7. Click **Save**. The LDAP server now appears on the list of servers.



**LocalAD@domain.com**

**General**

Domain: \* LocalAD@domain.com

Type: \* Active Directory

Security: \* None

Server: 10.5.14.68 389

+ Add

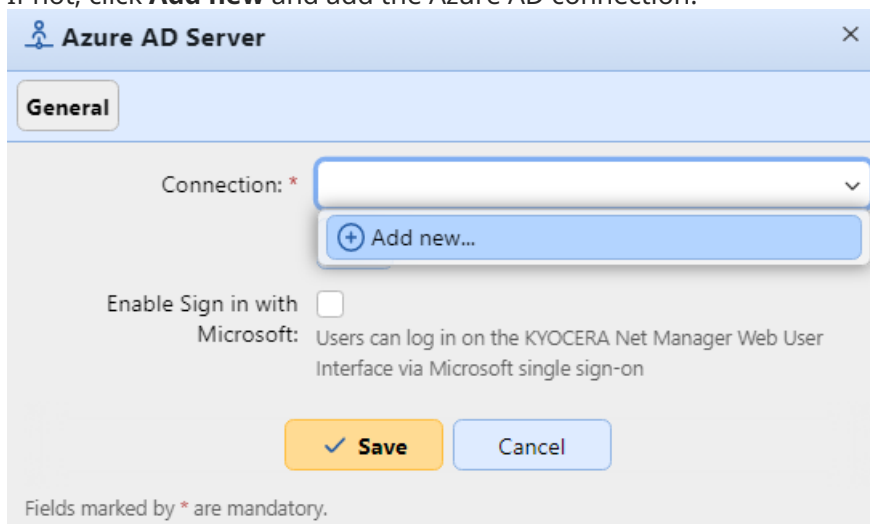
Leave blank for automatic discovery of the Domain Controller for the domain

✓ Save Test Cancel

Fields marked by \* are mandatory.

## 7.7.2 Adding a new Azure AD Server:

1. Click **+Add** and select **Azure AD Server**. The new Azure AD server properties panel opens on the right side of the screen.
2. If you have already added Azure AD in the **Connections** settings, the server appears on the list. If not, click **Add new** and add the Azure AD connection.



**Azure AD Server**

**General**

Connection: \*

+ Add new...

Enable Sign in with

Microsoft: Users can log in on the KYOCERA Net Manager Web User Interface via Microsoft single sign-on

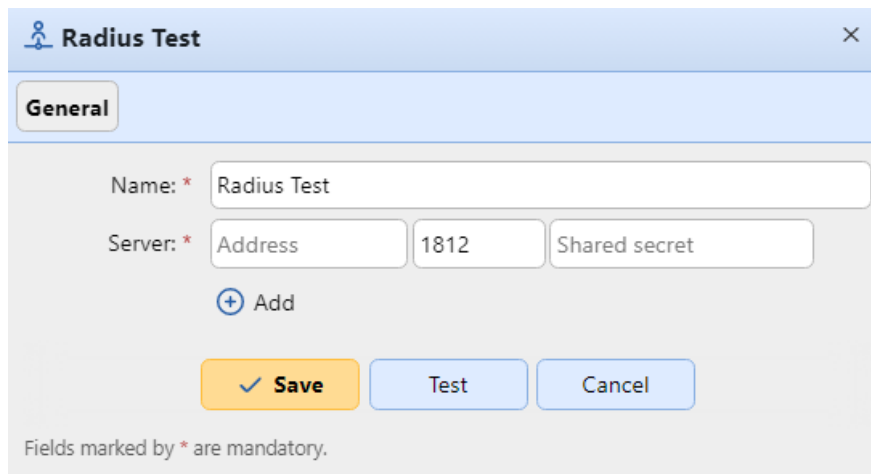
✓ Save Cancel

Fields marked by \* are mandatory.

3. If you want your users to be able to log in on the **KNM** Web UI via Microsoft single-sign-on, select the **Enable Sign in with Microsoft** checkbox.
4. Click **Save**. The Azure AD Server now appears on the list of servers.

### 7.7.3 Adding a new Radius server:

1. Click **+Add** and select **Radius server**. The new Radius server properties panel opens on the right side of the screen.
2. Enter the Radius server **Name**.
3. Enter the **Server** IP address or hostname, the communication port and the 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 now appears on the list of servers.



The screenshot shows a dialog box titled "Radius Test" with a close button (X) in the top right corner. Below the title bar is a "General" tab. The form contains the following fields and controls:

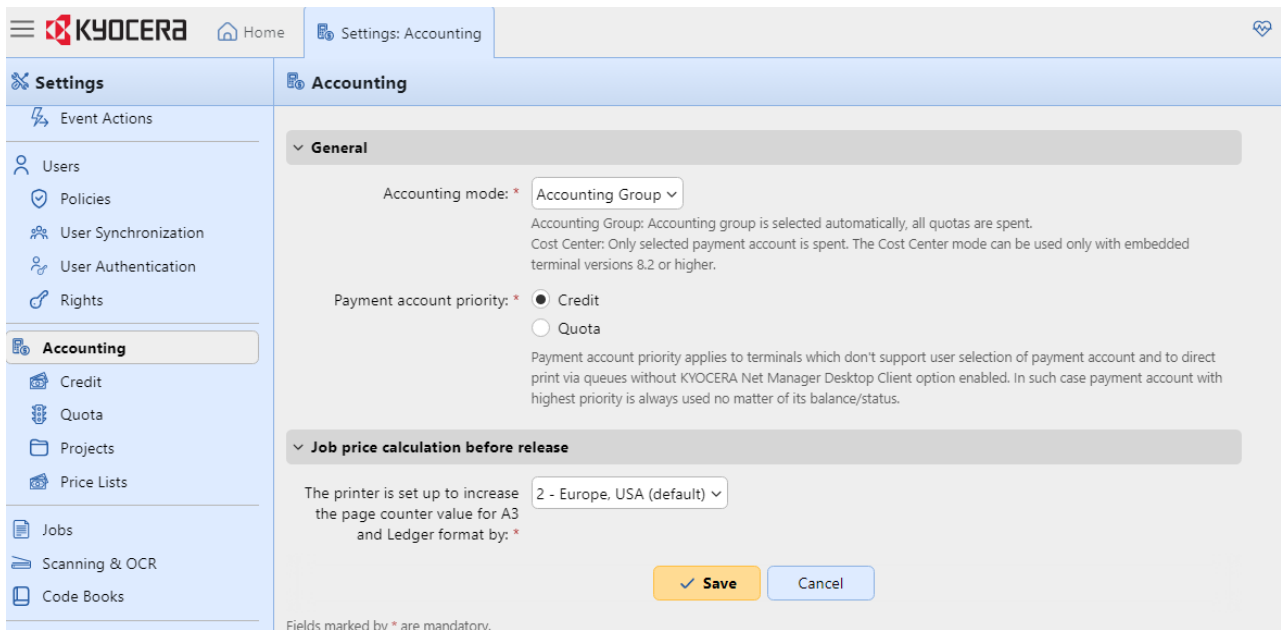
- Name:** A text input field with a red asterisk (\*) indicating it is mandatory, containing the text "Radius Test".
- Server:** A group of three input fields, each with a red asterisk (\*). The first is labeled "Address" and is empty. The second contains "1812". The third is labeled "Shared secret" and is empty.
- + Add:** A button with a plus sign icon and the text "Add".
- Save:** A yellow button with a checkmark icon and the text "Save".
- Test:** A light blue button with the text "Test".
- Cancel:** A light blue button with the text "Cancel".

At the bottom left of the dialog, there is a note: "Fields marked by \* are mandatory."

## 7.8 Accounting Settings

In the **Accounting** settings tab, in the **General** section, the **KNM** administrator can set:

- the **Accounting mode KNM** will be using:
  - **Accounting Group** - This is selected by default. In this mode, all quotas are available and can be spent.
  - **Cost Center** - In this mode, only the selected (cost center) payment account is spent.
- the **Payment account priority**, which applies to terminals that don't support user selection of payment accounts, and to direct queues without the **KNM** Desktop Client option. The payment account with the highest priority is always used in such cases:
  - Credit
  - Quota



## Limitations:

- The **Cost Center** mode does not work on printers without a terminal.
- **The Cost Center mode can be used only with embedded terminal versions 8.2 or higher.**
- In the **Cost Center** mode, if a user has more than one account, the job is paused and the account must be selected via **KNM Desktop Client** (v.8.2 or higher). If there is only one account, the account is assigned automatically.

**⚠** If you use the **Cost Center** mode on embedded terminals with a version older than 8.2, the terminals activation fails. The following error message can be found in the log: *"Terminal is incompatible | reason=Terminal version must be at least 8.2 in cost center mode"*.

If you switch to the **Cost Center** mode on embedded terminals with a version older than 8.2, the following warning can be found in the log: *"This terminal is not supported in cost center accounting mode. Upgrade terminal at least to version 8.2"*.

Switch to the **Accounting Group** mode or upgrade your embedded terminals to version 8.2 for the terminals to be successfully activated and work properly. If you choose to switch, your terminals need to be re-activated. This can be done automatically by clicking **OK** in the Apply Settings pop-up, or manually on each device.

## Comparison between Accounting Group and Cost Center

Accounting group	Cost center
Max 1 accounting group per user	Multiple cost centers can be assigned to a user
If multiple quotas are assigned to a user, all of them are spent.	Only one quota is spent. If credit, or a cost center without quota is selected, no quota is used.

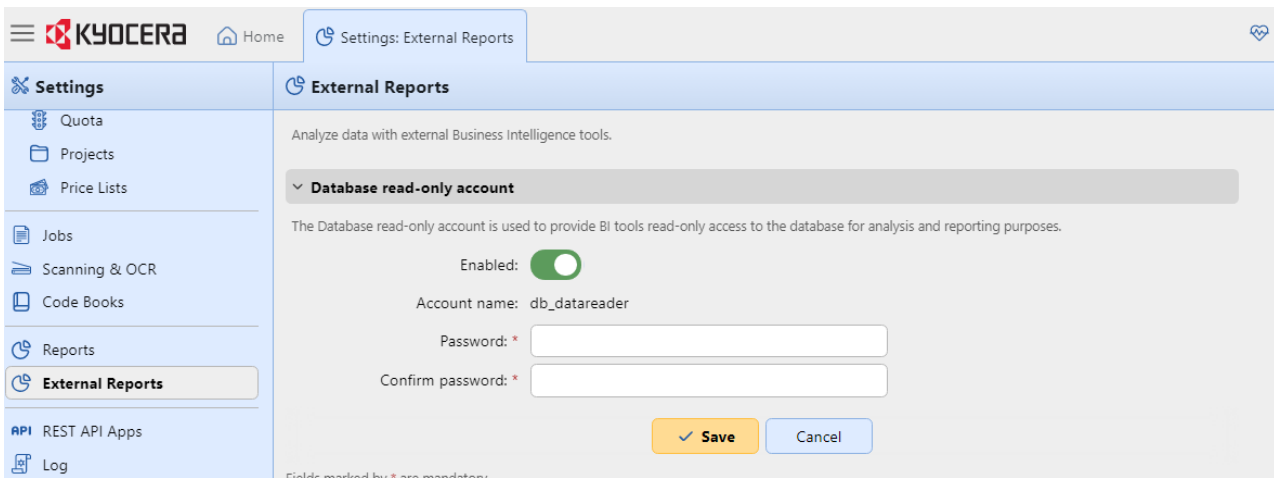
Accounting group	Cost center
If credit or personal quota is selected, the job is still accounted to the accounting group	If credit or personal quota is used, no cost center is accounted.
Every job performed by user is accounted to their Accounting group	A job is accounted to the cost center only if selected, or if it is the only account the user has.

In the **Job price calculation before release** section, the **KNM** administrator can select between *1 - Japan*, or *2 - Europe, USA (default)* for **The printer is set up to increase the page counter value for A3 and Ledger format by** setting.

## 7.9 External Reports

By default, the only access to the **KNM** Firebird database is via the *SYSDBA* account. Since this account has full read/write rights, it is not secure to use it for accessing the database from 3rd-party software (for example BI tools for reporting). A read-only access account is needed to avoid unintentional database corruption.

In the **External Reports** settings tab, the administrator can enable a **database read-only account** to be used with external reports.



Activating the **Enabled** switch automatically creates a read-only access account to the **KNM** Firebird database with the following settings:

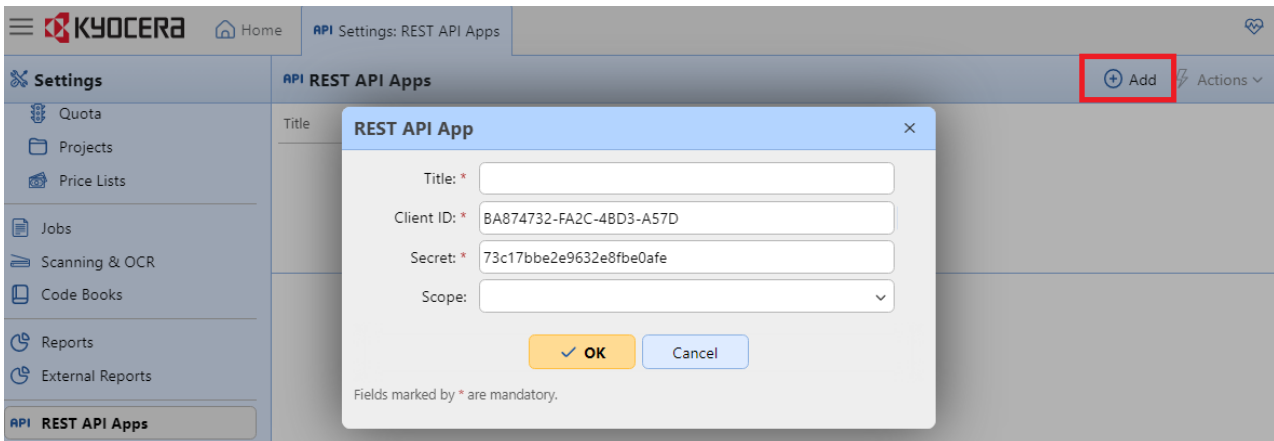
- **Account name:** *db\_datareader*. This is the newly created read-only database user. The account name cannot be changed.
- **Password:** password for the *db\_datareader* account, set by the administrator. A new password must be set every time when switching from the **Disabled** to **Enabled** state.
- **Confirm password:** confirmation of the above password.

Enabling the database read-only account automatically enables a Windows Firewall rule to allow incoming connections to the **KNM** Firebird database. If disabled, the rule is deleted.

- After restoring a backup using **KNM Easy config**, the Windows Firewall rule and the *db\_datareader*'s account password will be restored if the account state was **Enabled** when the backup was created. If the account state was **Disabled**, then the existing Windows Firewall rule will be deleted and the user account will be dropped in the restored Firebird database.

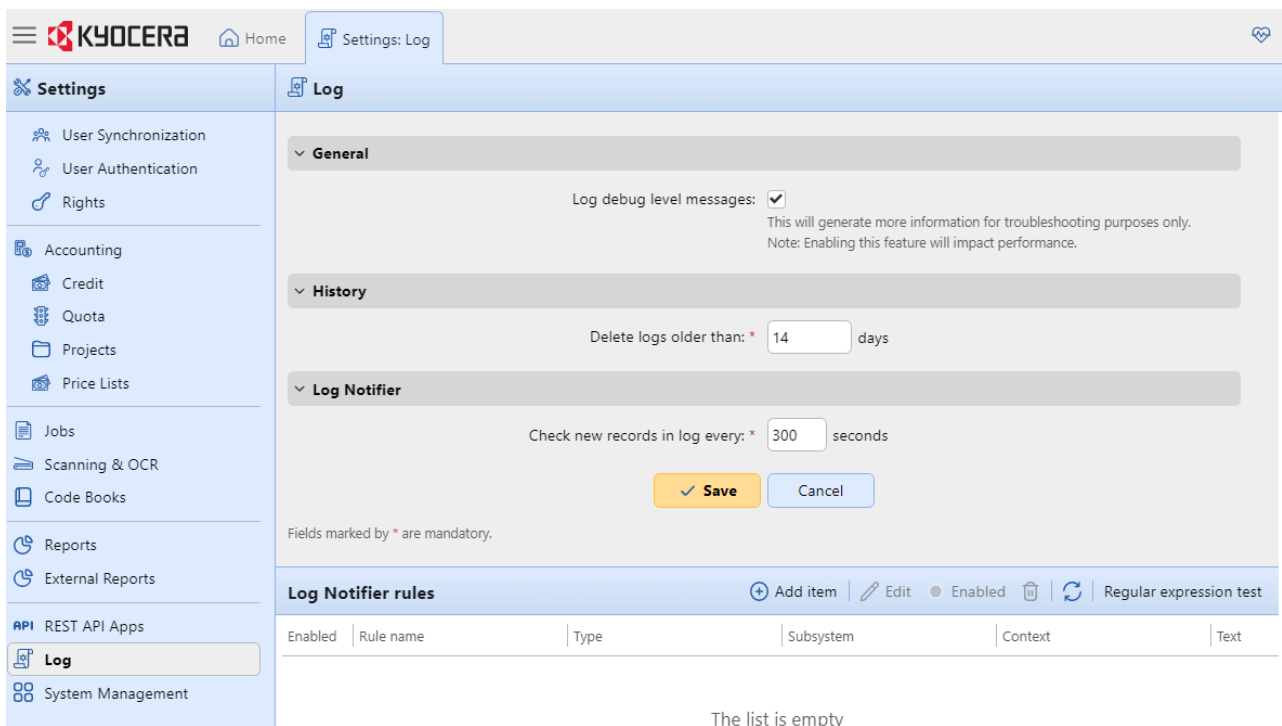
## 7.10 REST API Apps

In the **REST API Apps** settings tab you can add applications to **KNM** by clicking **+Add** and filling in the **Title** and **Scope**. The **Client ID** and **Secret** fields should be used for the application's configuration.



## 7.11 Log Settings

On this tab, you can set the **Log Notifier** feature, which enables sending notifications about selected log events to the administrator and/or any number of **KNM** users. The notifications can be sent via email or they can be sent to Windows Event Viewer.



**General** – If you select the **Log debug level messages** option, the system will generate more information for troubleshooting. The information will be shown in the **KNM Log**.

However, this feature will impact your system's performance. Therefore, we recommend you to enable it only in case of a system malfunction or if it is requested by your support.

**History** – Here you can set when the logs should be deleted (in days).

**Log Notifier** – The notifications and their destinations are both specified by log notifier rules.

Under **Log Notifier**, you can set the period after which the log is checked for new events in the **Check new records in log every: ... seconds** text box (300 by default).

### 7.11.1 Management of the Log Notifier Rules

To add a new rule, click **+Add item** at the upper-left corner of the **Log Notifier rules** widget. The properties panel of the new rule opens on the right side of the tab. On the tab, edit and save the rule.

To open the editing options of a rule, double-click the rule (or right-click the rule, and then click **Edit** on the shortcut menu). The following settings can be changed:

- **Enabled:** activate, deactivate the rule.
- **Rule name:** name of the rule.
- **Type:** the available event types are: *Info, Warning, Error, Notice, Debug, Critical*.
- **Subsystem:** subsystems of the **KNM** application (*Terminal, SMTP Server, CLI, etc.*).
- **Context:** specific part of the subsystem.
- **Text:** text of the log event message; you can use Regular expressions to search for specific patterns.

After you set the rule, click **Save**. The rule is saved and you can select its destinations.

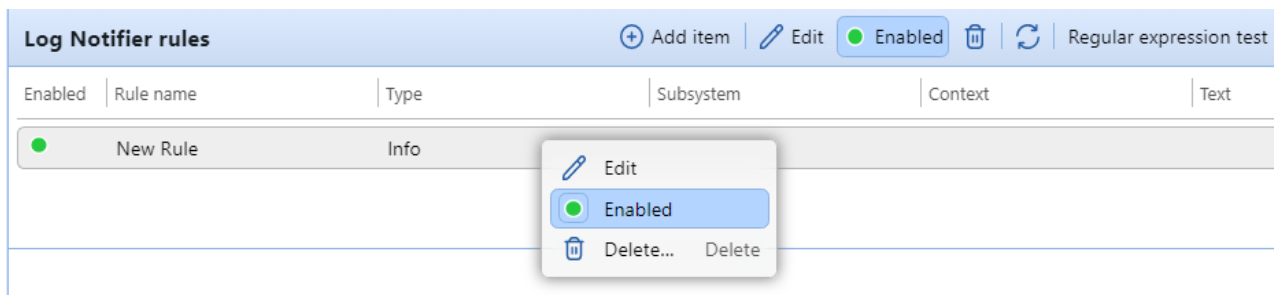
To add the destination, click **+Add item** under **Destinations**.

You can select between two destination options: **E-mail** and **Windows Event Log**. If you select the **E-mail** destination, you need to add one or more recipients; you can either select them from the list of **KNM** users in the **Recipients** drop-down or directly type the addresses there. After you set the destination, click **Save**.

The new rule is displayed on the tab.

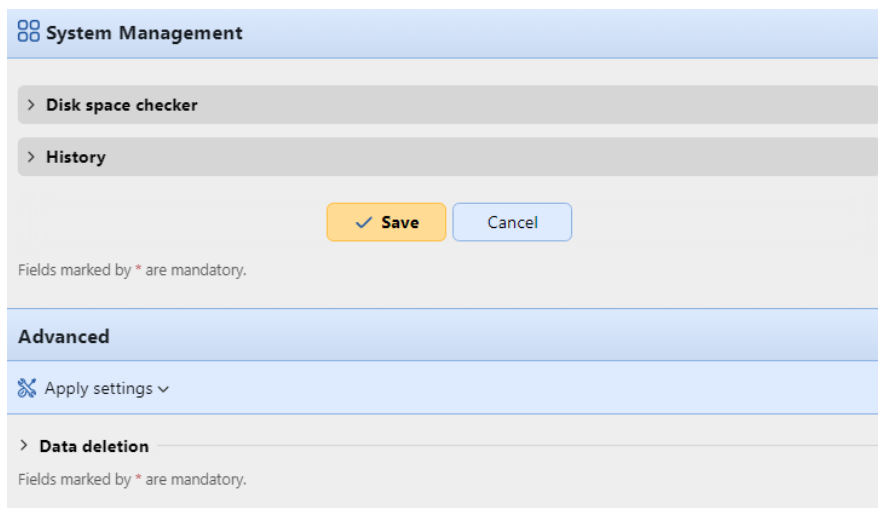
To enable/disable Log Notifier rules:

1. Right-click on the rule.
2. Select **Enabled** (or **Disabled**) on the shortcut menu.



## 7.12 System Management Settings

On the **System Management** settings tab, you can change the settings of the **KNM** history, reset **KNM** components to apply settings previously made on other tabs, and also delete data from the **KNM** database.



### 7.12.1 Disk space checker

The disk space checker protects the system against failure caused by insufficient disk space. You can set two levels of alert:

- **Warning level:** If the disk space reaches this level, the administrator gets an alert email message.
- **Critical level:** If the disk space reaches this level, the administrator gets an alert email message and the **KNM** services are automatically stopped to prevent corruption of the **KNM** databases.

### 7.12.2 History

In the **History** section, you can change the periods after which data stored on the **KNM** server is deleted. You can set time periods for the following data:

- **Delete jobs older than:** Jobs remain on the **KNM** server for the period set here. Older jobs (except for Favorite jobs) are deleted and cannot be printed. Favorite jobs stay on the server until they are manually deleted by the user or by the **KNM** administrator.

- **Delete local scans older than:** Local scans (the scans stored on the **KNM** server) remain on the **KNM** server for the period set here. Older local scans are deleted and cannot be downloaded.
- **Delete history older than:** This setting determines the time period for storing data of user sessions, alerts on printing devices, the device counter history, and closed alerts. Older data are deleted from the **KNM** database and cannot be used in **KNM** reports.
- **Delete archived reports older than:** Reports are archived for the period set here. Older reports are deleted.
- **Delete Audit log older than:** The audit log stores information about change in **KNM** settings for the period (in days) set here. Anything older is deleted.

To change the values, enter new values to the particular text box, and then click **Save**.

**History**

Delete jobs older than: \*  hours  
Favorite jobs will not be deleted.

Delete local scans older than: \*  hours  
Older scans cannot be downloaded.

Delete history older than: \*  days  
Reports can be created only within this period. Older data is deleted.

Delete archived reports older than: \*  days  
Reports are archived so you can download them without executing them again.

Delete Audit log older than: \*  days  
Audit log stores information about changes in KYOCERA Net Manager settings within this period.

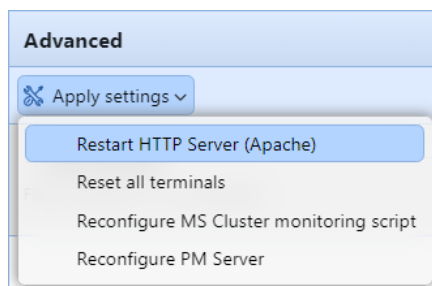
### 7.12.3 Advanced

In the **Advanced** section, you can reset **KNM** components to apply settings previously made on other tabs, delete all users without a session, and permanently remove inactive users, printers, groups and user data from the **KNM** database.

#### Applying changes

Some changes of the **KNM** server require a reset of some of the server's components. When you save these changes, the system proposes to automatically perform the reset. If you decide to skip this action, you need to reset the components later.

Via the **Apply settings** button, you can reset the components at any time. After you click the button, click a component that you want to reset and the settings will be applied without further notice.



## Data deletion

The delete/remove buttons perform the following actions. These actions cannot be undone. It is recommended you backup your data before performing any of them.

- **Delete users:** Deletes all users without user sessions.
- **Delete projects:** Removes projects that were never used.
- **Deleted inactive users and groups:** Permanently removes all inactive users and all groups with no active users from the **KNM** database.
- **Deleted printers:** Removes all printers which are deleted and have never been activated from the **KNM** database.
- **User data: User Sessions, Jobs, Groups, Users, Vouchers:** Removes all user related data from the **KNM** database.

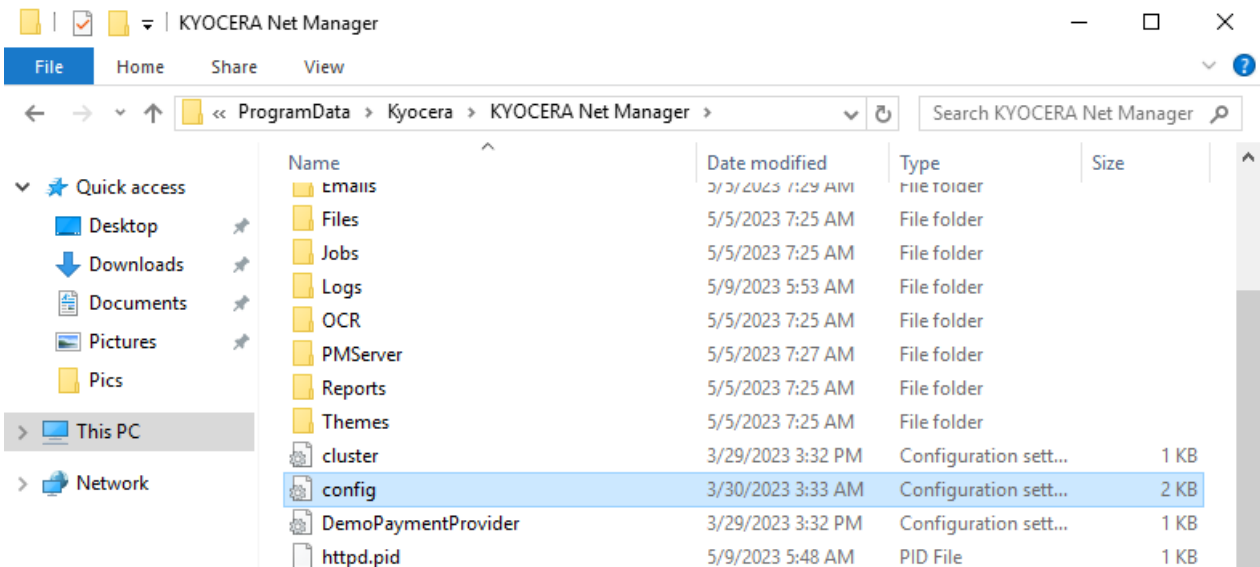
The screenshot shows the 'Advanced' settings page with a 'Data deletion' section. It contains five rows of deletion options, each with a count, a button, and a warning:

- Users to delete: 0**  
Button: **Delete users without sessions**  
Warning: Users with user sessions will not be deleted.
- Projects to delete: 0**  
Button: **Remove projects without sessions**  
Warning: Only the projects that never were used will be deleted. This action cannot be undone.
- Deleted inactive users and groups: 0**  
Button: **Permanently remove deleted users and groups**  
Warning: Deleted inactive users and groups will be permanently removed. This action cannot be undone.
- Deleted printers: 0**  
Button: **Remove deleted printers**  
Warning: Only the printers that never were active before will be deleted. This action cannot be undone.
- User data: User Sessions, Jobs, Groups, Users, Vouchers**  
Button: **Delete user data**  
Warning: This action cannot be undone. We recommend that you make a backup.

## 7.13 Security settings in config.ini

The config.ini file can be used for further configuration of the **KNM** Print Server. It contains sections with parameters and values for multiple settings, however it is highly recommended to always consult with your Support before editing the file.

Config.ini is a text file, located by default in *C:\ProgramData\Kyocera\KYOCERA Net Manager*, and you can edit it in Notepad or any other text editor.



After you edit and save the file, all services need to be restarted for the changes to take effect.

### 7.13.1 Security section

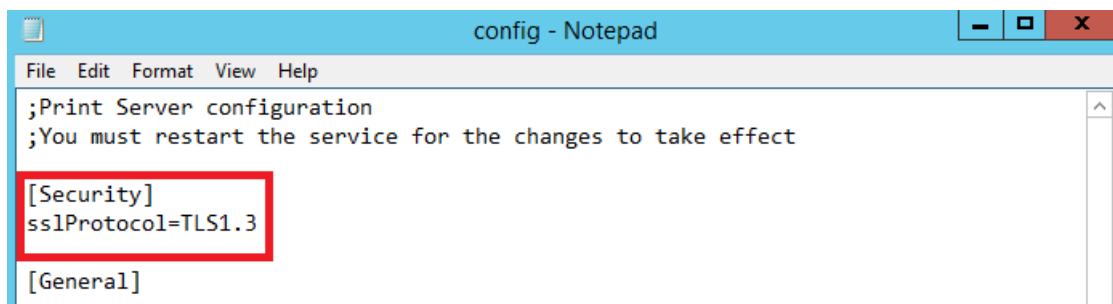
The configuration files *traefik.custom.rules.yaml* or *httpd.conf* manage secure communication with the web server, however there are other components using secure communication and they have a separate setting in the config.ini file. Those components are: SMTP, IPP, LPR, Messages (WebSockets), and HTTP Router. The Traefik configuration is also affected since **KNM** Print Server 10.1 RC1.

When a Traefik custom rules file exists in the installation with the TLS version specified, it takes precedence over the config.ini option. The config.ini settings apply to other **KNM** components, but Traefik TLS is set by the custom rules file.

To specify the minimum security protocol to be used for communication, go to *C:\ProgramData\Kyocera\KYOCERA Net Manager* and open the config.ini file in a text editor.

Add a section called **[Security]** and in a new line under that, add the parameter **sslProtocol** with the value you want. The possible values are: *SSL2*, *SSL3*, *TLS1.0*, *TLS1.1*, *TLS1.2*, and *TLS1.3* (since **KNM** Print Server 10.1 RC2+, the default value is *TLS1.0*).

For example, you can add *sslProtocol=TLS1.3*



Save the file and restart all services for the change to take effect.

## 8 Licenses

---

There are two ways of licensing in **KNM**. The one that has been used so far (old licensing model), with separate keys for each license, and the new **KNM X** licensing model -in use since **KNM Server 8.0** (patch 4)-, that introduced the use of an Installation Key per **KNM** setup.

This topic discusses the following subjects:

- [how to add and activate licenses](#)
- [how to delete licenses](#)
- [how to extend software assurance licenses](#)
- [how to migrate old licenses to KNM X](#)
- [VMHA License](#)

### 8.1 Adding licenses

You can add new licenses either on the **Home** screen during the initial setup of **KNM**, or anytime on the **License** settings tab.

After activation, the license is linked with the hardware configuration of the server where **KNM** is installed. If the configuration changes (for example after you reinstall **KNM** on a different server or after you change any of the hardware components of the server), the license becomes invalid and you have to reactivate it within seven days.

The total number of devices allowed to be activated at the same time is equal to the number allowed by your purchased licenses (For example: a license allowing ten printing devices + a license allowing one printing device + a license allowing five printing devices = sixteen printing devices allowed to be activated).

Non-MFPs printers are automatically assigned with an Embedded lite license (2x non-MFPs printers = 0,5 EMB lite + 0,5 EMB lite = 1xEMB license).

Having licenses for 40 printing devices automatically allows an unlimited number of printing devices to be activated at the same time on the server. This does not apply to embedded terminal licenses.

#### 8.1.1 Adding licenses on the Home screen

The first time you set up the **KNM** system, you can add new licenses on the **Home** screen, in the **Enter license** section, under the [Quick Setup Guide](#).

#### 8.1.2 Adding licenses on the License settings tab

On the **License** settings tab, you are asked to enter the following information about your installation:

- **Company** - Your company's name
- **Address** - The company's address
- **Country** - Select the country from the drop-down
- **Phone** - Your phone number (optional)

Then, add your Installation key in the **Enter the installation key** field and click **Save**, and then **Activate**.

- If you are connected to the internet and you have used an Installation key, your licenses are now added and activated.
- If you have used license keys, your licenses are added but need to be activated. Follow the activation steps below.
- If you want to manually activate your licenses, see the steps below.

You can see the newly added licenses on the **License** settings tab, under **License**.

If you are using a subscription license, you can see when the subscription is expiring or when it is going to be automatically prolonged:

10 days before the expiration, a banner message appears on the interface, reminding you to prolong your subscription:

*"Your subscription is about to expire soon, all services will stop in 10 day(s). Please prolong your subscription"*

If you don't prolong it on time, your licenses will expire and **KNM** will stop working. The banner message is displayed: *"KNM is not running: There is an issue with your license. Check details on the 'Settings > License' page."*

If the **KNM** server cannot connect to the License server:

- After the first unsuccessful connection, the **KNM** server starts displaying the alert banner "*KNM server cannot connect to License server, subscription cannot be prolonged and all services will stop in X days. Check internet connection and try to connect manually*". X = number of days until the expiration + 10.
- If the **KNM** server can't connect to the License server for 10 subsequent days after the subscription has expired, the **KNM** server will stop working and display the alert banner "*Server stopped working, because it cannot reach License server to update the subscription. Check internet connection and try to connect manually.*"

**F** If you have more than one Embedded licenses and you are using them, for example, as 3 Embedded lite licenses, the status bar in your Licenses overview will show that you are using one Embedded license, since the number is rounded down.

## 8.2 Activating Licenses

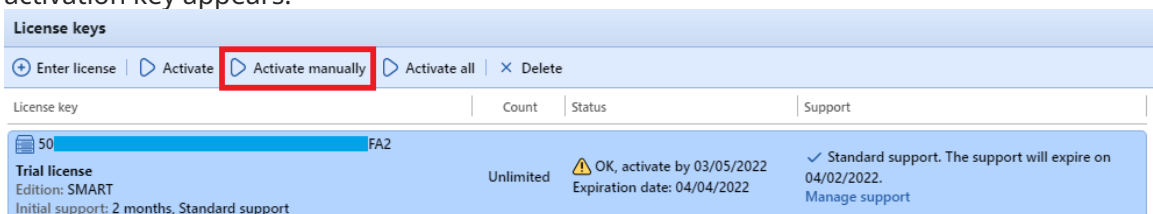
The HTTP Proxy Server setting for license activation is not supported for License Keys generated on the **KNM X Partner** portal. Manual (offline) activation must be used instead.

Installation Keys are automatically activated as soon as they are added (if connected to the Internet).

### 8.2.1 To manually activate a license:

If you are using the old licensing model (with license keys):

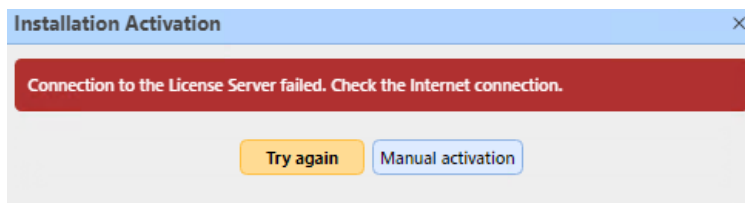
1. Generate the *KNM-helpdesk.zip* file. For information about how to do this, see [Generate data for support](#).
2. Send a request for an activation key to your technical support with the *KNM-helpdesk.zip* file attached. You will get an email response with the generated activation key.
3. Go to the **License** settings tab. Under **License**, click **Activate manually** (or right-click the license, and then click **Activate manually** on the shortcut menu). A dialog box for entering the activation key appears.



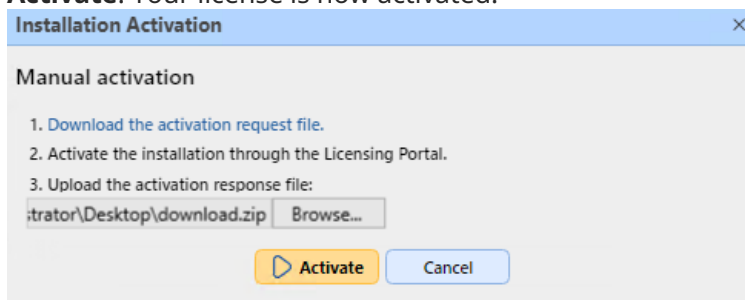
4. In the dialog box, enter the received activation key, and then click **OK**. Your license is now activated.

If you are using the new licensing model (with Installation Keys):

1. Go to the **KNM** Web Administrator interface, in **KYOCERA, Settings, Licenses**. Add your Installation Key and click **Next**. Click **Activate**. The online activation fails and you get the following message. Click on **Manual activation**.



2. In the newly opened window, click on **Download the activation request file**.
3. Upload the file in the **KNM X Partner** portal and download the activation response file.
4. Go back to the **KNM Web Administrator** interface, upload the activation response file and click **Activate**. Your license is now activated.



## 8.2.2 Reactivating Licenses in case of Hardware change

**When moving a KNM installation from an old server to a new server, a Support task needs to be created with your support for license installation key reactivation**

Steps:

1. Prepare the **new server** with a clean **KNM** installation.
2. Create a backup of **KNM** (**KNM Easy Config**\Database\Backup) on the **old KNM server**.
  - a. Print jobs (by default in C:\ProgramData\Kyocera\KYOCERA Net Manager\Jobs) are not part of the backup, because of size.
  - b. If required (especially favorite jobs could be required by users after restore **KNM** on the new server), they must be copied and backed up manually or by a 3rd-party software.
  - c. When restoring a backup, it is necessary to first copy the print jobs to the Jobs folder and then restore the **KNM** backup using **KNM Easy Config**.
3. Restore the backup file from step 2 on the **new KNM server** (**KNM Easy Config**\Database\Restore).
4. With the Installation key now in **KYOCERA**\Settings\License on the **new KNM server**, you should request for license installation keys activation in 10 days.
5. Generate the Helpdesk support file from the new **KNM** server installation (**KYOCERA**\Log\Tools\Generate data for support).
6. Contact your support for reactivating the installation key with attached Helpdesk support file.
7. When reactivation is confirmed in the task, activate the installation key in **KYOCERA**\Settings\License on the **new KNM server**.

Notes:

- A valid Software Assurance is required for the period when these changes are made.
- In case of offline activation, provide the Helpdesk support file from the old **KNM** server as well.
- Be sure that you are not using 2 **KNM** servers with the same database at the same time.

- Licenses on the old **KNM** server will no longer be activated (there is a 10 days period from deactivation).

**When significant hardware changes are done on the KNM server and KNM installation key required activation in 10 days (KNM Web UI\Settings\License), a Support task needs to be created with your support for license installation key**

Steps:

1. Check **KYOCERA\Settings\License** in case any HW changes are done on **KNM** server.
2. If the installation key in **KYOCERA\Settings\License** requires activation in 10 days or less, continue with the next steps.
3. Generate the Helpdesk support file (**KYOCERA\Log\Tools\Generate data for support**).
4. Contact your support for reactivating the installation key with the Helpdesk support file attached.
5. When reactivation is confirmed in the task, activate the installation key in **KYOCERA\Settings\License**.

Notes:

- A valid Software Assurance is required for the period when these changes are made.

## 8.3 Deleting licenses

To delete a license:

On the **License** settings tab, under **License**, select the license that you want to delete and click **Delete**. (Or right-click the license, and then click **Delete** on the shortcut menu.)

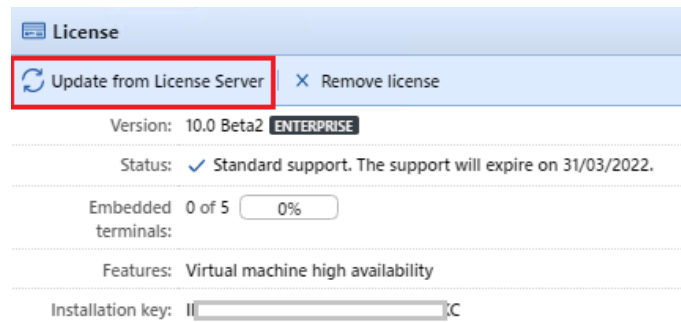
License key	Count	Status	Support
5C [redacted] :FA2 Trial license Edition: SMART Initial support: 2 months, Standard support	Unlimited	⚠ OK, activate by 03/05/2022 Expiration date: 04/04/2022	✓ Standard support. The support will expire on 04/02/2022. Manage support

## 8.4 Extending software assurance licenses

You can extend the software assurance period by assigning a software assurance license to the particular main license. This can be done at any time, even before your current assurance period expires. In this case, the service is extended from the last day of validity of the current software assurance license.

### 8.4.1 New licensing model (with Installation keys)

You can order to prolong your software assurance on the **KNM X Partner** portal. Once your order is approved, go to the **KNM Web Administrator** interface, in **KYOCERA, Settings, License** and click the **Update from License Server** button to update your prolonged Software Assurance license. If the new date is not displayed, refresh the webpage.



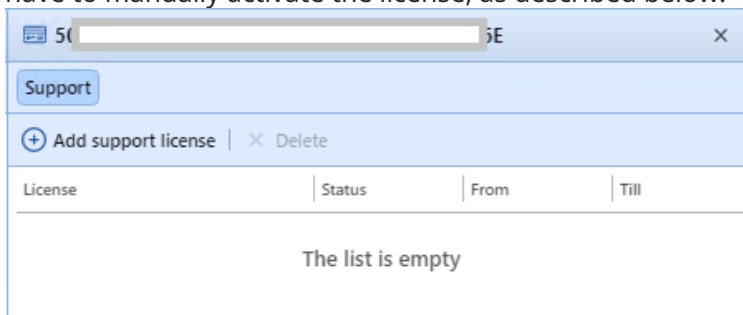
## Manual activation

1. Once your additional licenses order is approved, go to the **KNM** Web Administrator interface, in **KYOCERA, Settings, License**, and click the **Update from License Server** button. Since there is no network, you will be prompted to **Download** the activation request file.
2. After you download the file, go to the **KNM X** Partner portal, under your Project, in the Installations tab. Click **Offline activation**.
3. In the pop-up window, upload the *offlineActivation.zip* file you downloaded from the **KNM** Web Administrator interface, and click **OK**. The activation response file is then automatically downloaded.
4. Go back to the **KNM** Web Administrator interface, upload the activation response file and click **Activate**. Your additional licenses are added and activated.

### 8.4.2 Old licensing model (with license keys)

The licenses can be extended on the **License** settings tab.

1. On the **License** settings tab, under **License**, click **Manage Support**. The license properties panel opens on the right side of the screen.
2. On the panel, click **+Add support license**. The Add support license dialog box appears. You have to manually activate the license, as described below.



### 8.4.3 Manual activation

1. Generate the *KNM-helpdesk.zip* file.
2. Send a request for an activation key to your support with the *KNMhelpdesk.zip* file attached. You will get an email response with the generated activation key.
3. Add the support license key in the Activate support license dialog box, select the **Activate manually** option, enter an activation key, and then click **OK**.

## 8.5 Migrating old licenses to KNM X

If you are using older **KNM** editions, it is recommended to migrate your licenses to **KNM X**.

Compared to older editions, **KNM X** offers a new price list with updated and new functionalities, one Installation key containing all the license information instead of multiple license keys, a fast and automated license ordering process, and a complete overview in the **KNM X** Partner portal of all the products and their software assurance.

Moreover, if you use embedded lite licenses, during the license migration to **KNM X**, their price is halved (two embedded lite = one embedded license). If you have an odd number of embedded lite licenses, the total is rounded up, and then halved (eleven lite = twelve lite = six embedded licenses).

The software assurance expiration date is recalculated during the migration:

1. Expiration dates are converted to a real number and the average is computed.  
(for example, you have 100 x Embedded (E) and 200 x Embedded Lite (EL) | so  $100 \times \text{'expiration date' of (E)} + 200/2 \times \text{'expiration date' of (EL)} / \text{count of ((E) + (EL/2))}$ )
2. The computed average is a real number and, converted back to the date format may produce, for example, 23h:56min - for this reason 1 day is added.
3. From the average corrected date, only the month + year are used, without day + time, and one month is added to the final date.

License Type	Pcs	Software Assurance Expiration	SA Days till Expiration (from today, 5.10.2020)	SA Days of all Pcs
Embedded	40	04.11.2020	30,00	1 200,00
Embedded	10	28.07.2021	296,00	2 960,00
Embedded	8	19.12.2021	440,00	3 520,00
Embedded	1	20.02.2022	503,00	503,00
<b>TOTAL of Embeddeds</b>	<b>59</b>			<b>8 183,00</b>
Lite	10	04.11.2020	30,00	300,00
Lite	1	19.12.2021	440,00	440,00
<b>TOTAL of Lites</b>	<b>11</b>			<b>740,00</b>
Round up to an even number of Pcs	12			807,27
<b>Conversion of Lites to Embeddeds (2-in-1)</b>	<b>6</b>			<b>403,64</b>
<b>TOTAL Enterprise &amp; Support</b>	<b>65</b>	<b>14.02.2021</b>	<b>132,10</b>	<b>8 586,64</b>
<b>FINAL Enterprise &amp; Support</b>	<b>65</b>	<b>01.03.2021</b>		

The prerequisites for license migration are:

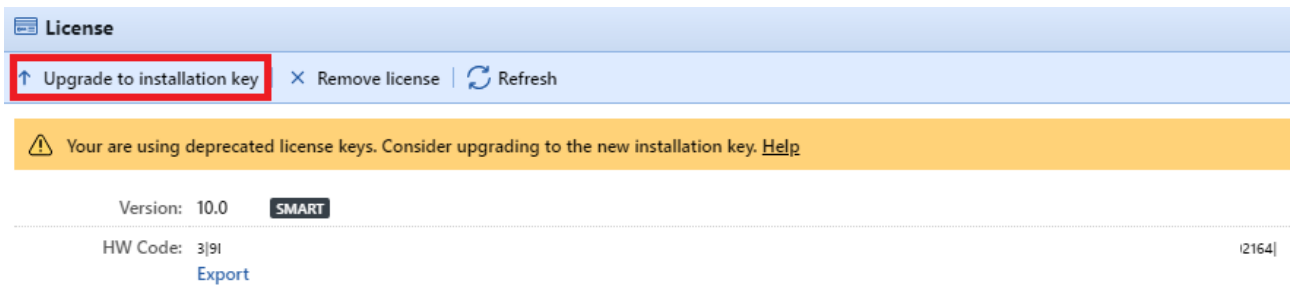
- **KNM** Print Server or **KNM** Central Server 8.2 or higher installed (valid support required).
- Valid support required; support date for version 8.2 is 15 January 2021, but it is recommended having valid support all the time, especially when there are planned system changes and your support would be contacted.
- Access to the **KNM X** Partner portal (Partner ID and password. If you do not have access, contact your Sales representative).

With the above prerequisites fulfilled, you can start the [Migration Process](#).

### 8.5.1 Migration Process

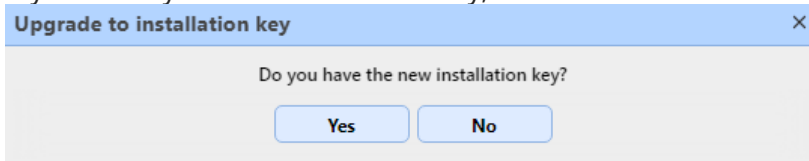
You can start the license migration process in the **KNM** web administrator interface.

Go to **KYOCERA, Settings, License**. At the top bar, click **Upgrade to installation key**.

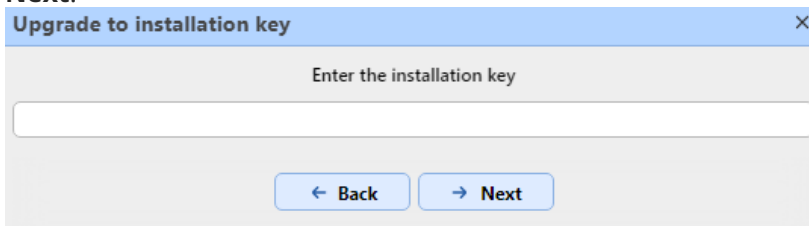


The Upgrade to installation key wizard starts, guiding you through the upgrade:

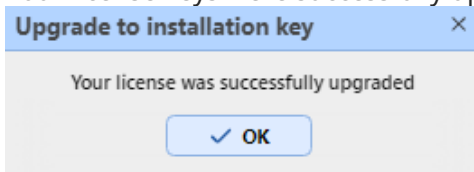
1. If you already have an Installation Key, click **Yes** and continue to step 4. If not, click **No**.




2. The **KNM** server will now export the *KNM-licenses.xml* file. You need this file to generate the new installation key at the **KNM X Partner Portal**. Click **Next**.
3. The *KNM-licenses.xml* file has been downloaded. Go to the **KNM X Partner portal** and follow the process to generate a new installation key. Once you generate it, your old license keys cannot be used again.
4. Back in the **KNM** web administrator interface, insert the installation key in the field, and click **Next**.



5. **KNM** is contacting the License server to get the license information. In case you have no internet connection, click **Manual activation** to [manually activate the license](#).
6. Check the overview and if everything is correct, click **Activate**; otherwise, click **Cancel**.
7. Your license keys were successfully upgraded to an installation key and are now activated.



You can see your new licenses overview in the **License** settings tab.

 If the activation fails due to connection issues, or for any other issues with the migration, contact your Support.

## 8.6 VMHA License

Normally, the hardware signature of the server hosting **KNM** is occasionally verified to make sure that the license is still installed on the same server and isn't misused. In certain scenarios, the underlying hardware may change and so a license reset is required to re-activate the license. If the hardware changes often (which is common when the server is hosted in a virtual environment), the Virtual Machine High Availability (VMHA) feature may be required.

- The VMHA license is included free of charge in **KNM** Enterprise 8.0+ licenses.
- For the VMHA feature to function, a domain environment is mandatory - the server running **KNM** must be a member of a domain. For **KNM** installed in an MS Azure environment, a domain is not required. Changing the domain or migrating to a completely different server will still require a license reset.

To verify that the VMHA feature is available, go to **KYOCERA, Settings, License**.

With old license keys, once the VMHA license is registered and activated, you can enable the VMHA feature in **KYOCERA, Settings, Network**. Once enabled, the license verification mechanism will no longer check for changes in the hardware when checking the HW license signature key.

With the new licensing model, with installation keys, VMHA is enabled by default in a Print Server or Central Server setting. If you are using Site servers, you have to enable the feature in each Site server.

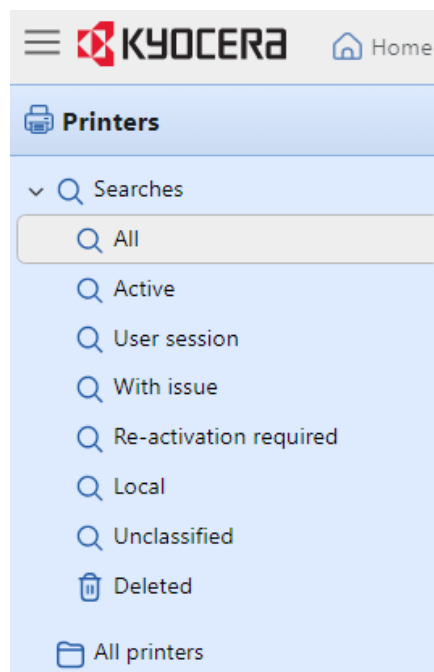
## 9 Printers

This topic discusses one of the key functions of **KNM** — setup and management of printing devices. It covers the following subjects:

- [Printers and Terminals](#) settings.
- Overview, adding, activating and deleting printing devices: [Manually adding printing devices](#), [Discovering printing devices](#), [Activating and deactivating printing devices](#), [Deleting and undeleting printers](#).
- Individual device settings, creating groups of printing devices and exporting the list of printing devices: [Editing printers](#), [Printer Groups](#), [Exporting printers](#).
- Monitoring of offline and local printing devices: [Monitoring network printers in offline mode](#), [Monitoring local printers](#).
- Sending email notifications of printing device alerts: [Printer Events](#).
- Creating and assigning SNMP profiles: [SNMP profiles](#).

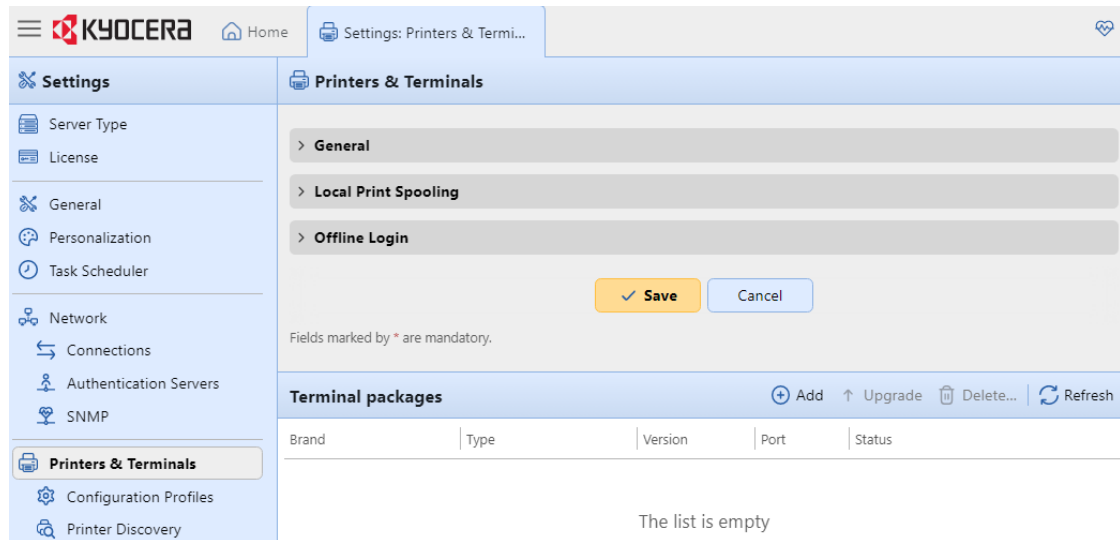
On the **Printers** main tab, you can see printing devices and information about them. With the **All** search option selected, you see all printing devices that are currently in the system. Apart from this option, you can select from the following:

- **Active** - select to display only active printing devices.
- **User session** - select to display only printing devices that are currently in use.
- **With issue** - select to display only printing devices with a reported issue (these printers are also listed on the **Home** page).
- **Re-activation required** - select to display the printing devices that must be activated again.
- **Local** - select to display only locally connected printing devices (USB, LPT).
- **Unclassified** - select to display only printing devices that do not belong to any group.
- **Deleted** - select to display only deleted printing devices.



## 9.1 Printers and Terminals settings

On the **Printers & Terminals** settings tab, you can manage your terminal packages, and configure multiple settings. The settings are divided in the **General**, **Local Print Spooling**, **Offline Login**, and **Terminal packages** sections.



### 9.1.1 General

In this section, the following settings are available:

▼ **General**

Keep printing after logging out:

Allow a color job on a B&W printer:

Print all jobs after logging in:

Always display job price:

- **Keep printing after logging out** - if enabled, all jobs requested for release will be released even if the user logs out. If this option is disabled, then once the user logs out from the terminal:
  - the releasing of the requested jobs to the printer will be stopped.
  - not yet released jobs will be returned to the Ready status.
  - the terminal will also try to stop all already active print jobs (if this operation is supported by the terminal).
- **Allow a color job on a B&W printer** - if enabled, color jobs can be printed on B&W printers.
- **Print all jobs after logging in** - if enabled, a **Print all jobs after logging in** checkbox is displayed on the terminal's Log in screen, and it is selected by default. If the user keeps it selected, all their jobs from the **Ready** tab are automatically printed as soon as they successfully log in. If the user disables the option, no jobs are printed automatically upon login.
- **Always display job price** - if enabled, a job's price on an Embedded terminal is displayed even when Credit or Quota are disabled. If disabled, a job's price on an Embedded terminal is not displayed unless Credit or Quota are enabled.

To enable any of the settings, select the checkbox next to them, and click **Save** at the bottom of the tab.

### 9.1.2 Local Print Spooling

In this section, you can enable the Local Print Spooling feature for your embedded terminals, and set it up.

Local Print Spooling

Local Print Spooling allows printers with the Embedded Terminal to receive print jobs and securely release them when user logs in. This significantly lowers network traffic to the KYOCERA Net Manager server.

Enabled:

Delete ready jobs older than: \*  hours

Print&Follow:

- **Enabled** - enable/disable the **Local Print Spooling** feature (disabled by default).
- **Delete ready jobs older than \_\_ hours** - period of time after which the locally spooled jobs are deleted. The default is 12 hours, and the allowed range is 1 to 72.
- **Print&Follow** - if enabled, you can use Print&Follow printing.

### 9.1.3 Offline Login

Offline Login allows to use printers with Embedded terminals even if the network connection to the KNM server is unavailable. In this section, you have the following settings:

Offline Login

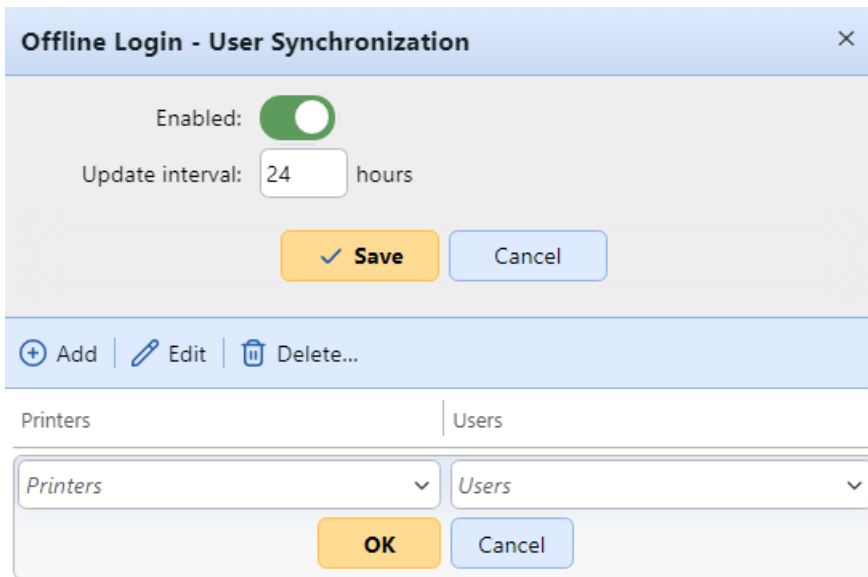
Offline Login allows to use printers with the Embedded terminal even if the network connection to the KYOCERA Net Manager server is unavailable.

Enabled:

Cache user credentials for: \*  hours

[User Synchronization](#)

- **Enabled** - enable/disable the **Offline Login** feature (disabled by default).
- **Cache user credentials for \_\_ hours** - the terminal caches user credentials for the given time, allowing them to log in while offline. The default is 72 hours, and the allowed range is 1 to 168.
- **User Synchronization** - if enabled, the users information can be synchronized to printers without the need for the user to log in to the printer first.

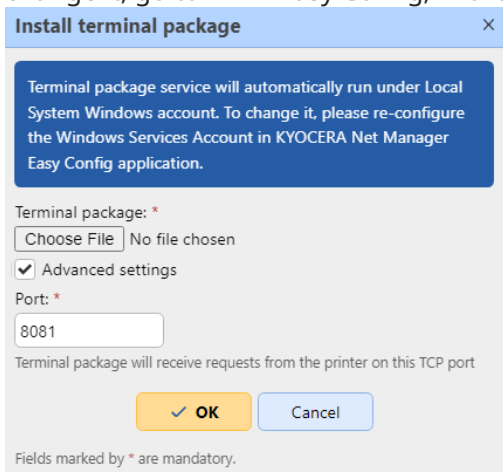


- **Enabled** - enable/disable offline login user synchronization.
- **Update interval** - set the interval of user synchronization between 1 and 168 hours.
- **Add, edit, delete** printers and users - configure the printers and users for the offline login user synchronization.

### 9.1.4 Terminal packages

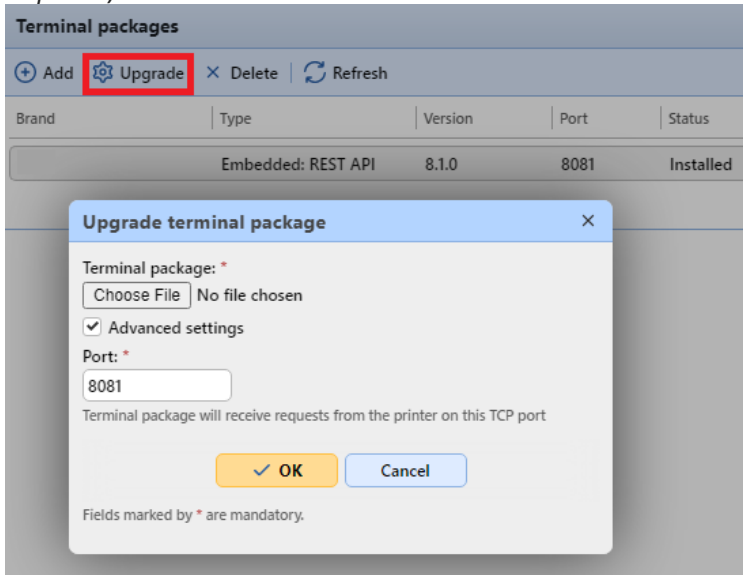
In this section, you can manage your terminal packages.

- Click **+Add** to upload a terminal package to the server. In the pop-up window, browse and open the terminal package, and click **OK**. You can optionally select **Advanced settings** to set a specific **Port** for the terminal. The terminal package is uploaded and installed. (Note that the terminal package service will automatically run under the Local System Windows account. To change it, go to **KNM Easy Config**, in the [Settings](#) tab.)



- If you are trying to add a later version of the same terminal package, a pop-up informs you that you can upgrade your installation. Click **Yes** to continue. The terminal package is uploaded and installed, and the device is automatically reactivated. (**KNM Server 8.2 patch 6 or higher is required**)

- Select an installed terminal package and click **Upgrade** to upgrade it to the latest version. In the pop-up window, browse and open the terminal package, and click **OK**. You can optionally select **Advanced settings** to set a specific **Port** for the terminal. The terminal package is uploaded and installed, and the device is automatically reactivated. (*KNM Server 8.2 patch 6 or higher is required*)



- Select an installed terminal package and click **Delete** to uninstall it from the server.

For specific terminal packages information and limitations, check the embedded terminal manuals:

- **KNM Embedded Guide**
- **KNM Embedded Lite Guide**

## 9.1.5 Terminal Actions Settings

In the **Terminal Actions** settings tab on the **KNM Web** administrator interface, you can view and manage embedded terminals features. The features are called actions and can be accessed from action nodes on the terminal. The action nodes correspond to buttons on the printing device display.

You can configure the layout of the display screen, as well as the behavior of each button. Therefore, you are free to choose any combination of available actions and their positions on the screen. The layout is displayed on a WYSIWYG (*What You See Is What You Get*) terminal preview and can be configured there.



Terminal actions are arranged vertically in blocks of three. A maximum of eighteen (18) terminal actions per level is allowed. If the amount of terminal actions is greater than nine (9), the buttons are stretched to show arrows that allow switching between pages. This, however, depends on the terminal display and smaller screens have a lesser number of top menu actions per page, as well as either pagination on the left or dotted pagination at the bottom.

Additional layout options are provided by the possibility to create folders and put action nodes inside. Folders can be used to group actions of the same type, such as scanning to different destinations, or to enable users to access a higher number of actions.

Users and groups can be given rights to different actions. This way, you can configure individual home screens for each user or group of users.

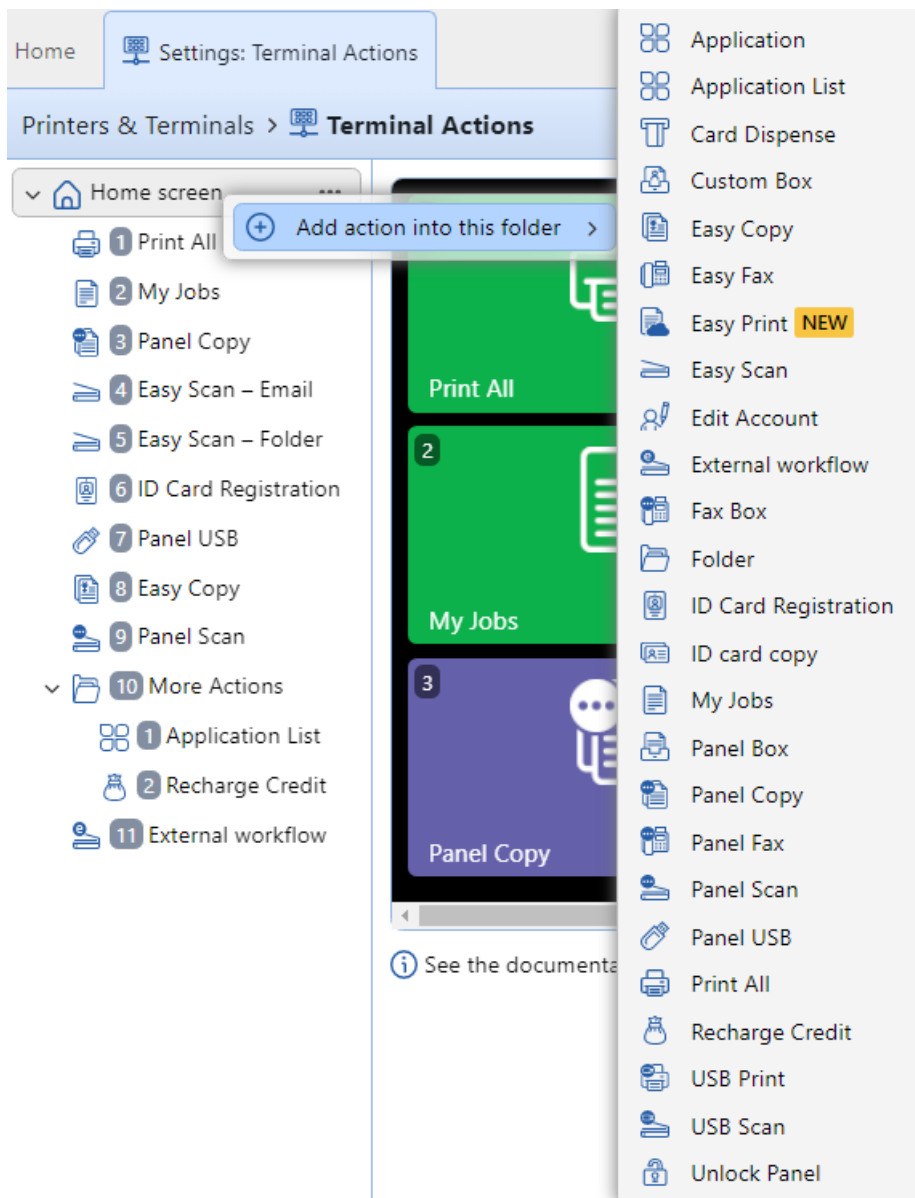
The terminal action nodes can be managed either under **Home screen** on the list of actions or directly on the terminal screen preview.

## Adding new terminal action nodes

### Adding new action nodes on the list of actions

To add a new terminal action node:

1. Right-click on **Home Screen**, and point to **Add action into this folder** in the shortcut menu. Another sub-menu with a list of available action nodes opens to the right.
2. On the sub-menu, select the new action node. The new action node properties panel opens on the right side of the screen.

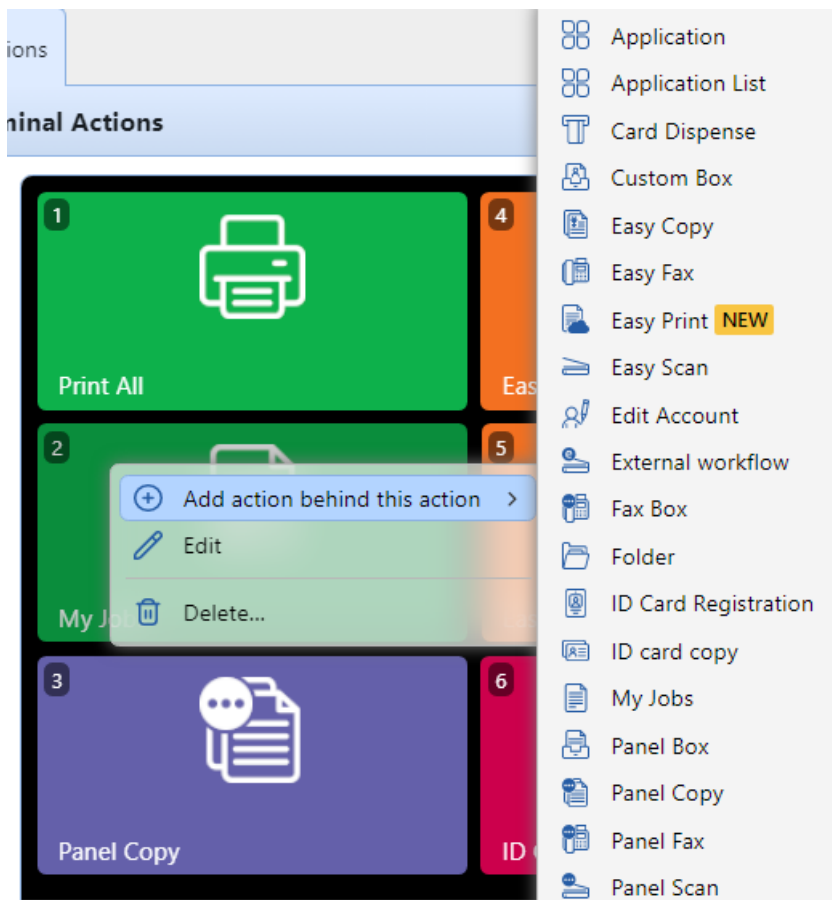


3. On the properties panel, you can rename and edit the node. For information about editing options, see [Editing action nodes](#). Once you save your changes, the new action node is displayed on the action nodes list and on the terminal screen preview.

### Adding new action nodes on the terminal screen preview

To add a new terminal action node:

1. Right-click any item on the preview and point on **Add action behind this action** in the shortcut menu. A sub-menu with a list of available action nodes opens to the right.
2. On the sub-menu, select the action node. The new action node properties panel opens on the right side of the screen.



3. On the properties panel, you can rename and edit the node. For information about editing options, see [Editing action nodes](#). Once you save your changes, the new action node is displayed on the action nodes list and on the terminal screen preview.

## Editing terminal action nodes

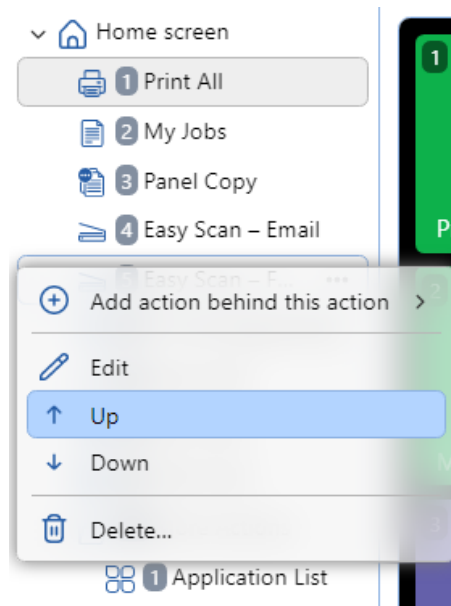
Each action can be edited on its properties panel. To access the panel, double-click the terminal action node on the list of nodes or on the terminal screen preview. On the properties panel, you can see up to three settings tabs (depending on the particular action): **General**, **Destinations**, and **Parameters**. The Destinations and the Parameters tabs are mostly used in Easy Scan action nodes and are described there.

### General tab

- **Enabled** - If you disable the node, it is not displayed on the terminal and cannot be used there.
- **Title** - Here you can change the action node's name. If you do not change it, the default name is used. Depending on the number of additional languages set on the **KNM** Web administrator interface, you can use different names in different languages. (The additional languages can be set on the **General** settings tab.)
- **Printers** - Here you can select the printers the action node will be available on. All printers are assigned by default. To add more printers, select them from the **Printers** drop-down.
- **Rights** - Here you can select the users or the groups of users that will be able to see the action node. Due to this setting, the layout and available features of the embedded terminal can vary depending on user's rights to particular nodes. By default, the right to see the node is given to all users. To provide an additional user or a group of users with rights to the action node, select the user or group from the **Rights** drop-down.
- **Style** - Select the action node's predefined style from the drop-down.

## Changing the terminal action nodes layout

To change the action nodes layout, you can either move the action nodes up and down the order on the list, or drag and drop them directly on the terminal screen preview.



If there are more than ten action nodes defined on the home screen or in any folder, move the scroll bar at the bottom of the preview screen to view the additional action nodes.

## Deleting terminal action nodes

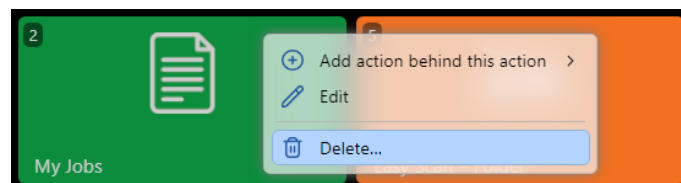
You can delete terminal action nodes either from the action nodes list or from the terminal screen preview. Both actions have the same result: when you delete the node, it disappears from both places.

### Deleting action nodes from the home screen list

On the list of actions on the **Terminal Actions** settings tab, right-click the action node that you want to delete, and then click **Delete** on the shortcut menu. The action node disappears both from the list, and the terminal screen preview.

### Deleting action nodes from the terminal screen preview

On the terminal screen preview, right-click the action node that you want to delete, and then click **Delete** on the shortcut menu. The action node disappears both from the screen preview, and the action nodes list.



## Restoring the original layout

On the bar at the top of the **Terminal Actions** settings tab, click **Tools**, and then click **Restore defaults**. All your layout changes are reverted to the default settings.

## Easy Scan settings

This section describes the settings needed to enable the **Easy Scan** action and define its destinations and parameters. They can be changed on three tabs on the **Easy Scan** properties panel: **General**, **Destinations**, and **Parameters**.

The properties panel is automatically opened after the **Easy Scan** action node is created. You can also access it by double-clicking the terminal action node on the list of nodes or on the terminal screen preview.

- The **General** tab settings are described in Editing terminal action nodes.
- The **Destinations** tab settings are described in [Easy Scan destinations](#).
- The **Parameters** tab settings are described in [Easy Scan parameters](#).

## General Limitations

- Not all Easy Scan parameters are supported by all vendors/machines.
- The "Allow custom values", "Allow multiple values" server scan settings are not supported automatically, they need to be enabled by the server administrator.
- Easy Scan supports only one folder-browsable destination, all the rest of the connected destinations on the server are supposed to work as they worked before.

## Easy Scan destinations

On the **Destinations** tab of the Easy Scan action node properties, you can define where the scanned file is sent.

To add a new destination, click **+Add**. The Destination panel opens where you can set the target destination.

Depending on the selected destination type, the panel contains the **General**, **Parameters** and **Advanced** sections.

### General section

- **Type** - Select the destination type from the drop-down. Available options: *Cloud storage, Custom destination, Email, FTP, Fax Server, Folder, Secured link, User's email, User's storage*.
- **Filename Template** - Here you can create the template of the scanned file name. The text of the template can be combined with **KNM** parameters to provide additional information about the scanned file. The following parameters are available: *%username%, %fullname%, %timestamp%, %date%, %time%, %originalSubject%, %ipaddress%, %scanId%, %usernotes%, %printerName%, %location%, %serialNumber%, %assetNo%, %printerContact%, %counter%*.
- **Title** - Add a title for the destination.
- **Attach metadata file** - If this option is selected, **KNM** sends the scanned file with an XML file attachment, containing the scanned file's metadata.

### Parameters section

This section depends on the selected destination type. The available fields differ for each type. Some types share parameters, and some times use unique parameters. Custom parameters can also be created, in the **Parameters** tab.

### Shared Parameters

Parameter	Description
%username%	The value is taken from the <b>User name</b> field of the user's properties panel.
%fullname%	The value is taken from the <b>Full name</b> field of the user's properties panel.
%timestamp%	Date and time of the scan.
%date%	Date of the scan.
%time%	Time of the scan.
%originalSubject%	This value is taken from the subject set on the printing device.
%ipaddress%	This value is taken from the <b>IP address/Hostname</b> field of the printing device's properties panel.
%scanId%	This value is an unique scan identification number generated on the KNM server.
%usernotes%	This value is taken from the <b>Notes</b> field of the user's properties panel.
%printerName%	This value is taken from the <b>Name</b> field of the printing device's properties panel.
%location%	This value is taken from the <b>Location</b> field of the printing device's properties panel.
%serialNumber%	This value is taken from the <b>Serial number</b> field of the printing device's properties panel.
%assetNo%	This value is taken from the <b>Asset number</b> field of the printing device's properties panel.
%printerContact%	This value is taken from the <b>Contact</b> field of the printing device's properties panel.

## Unique Parameters

Parameter	Description
%counter%	If the <b>Scan Separation</b> parameter is set to <b>Separate each page</b> , this value shows the number of scanned pages. This parameter can be used only to create the filename template.
%originalBody%	This value is taken from the signature set on the printing device. It is used in the <b>User's email</b> destination type only.
%recipient%	The fax recipient. It is used in the <b>Fax Server</b> destination type only.
%number%	Fax number. It is used in the <b>Fax Server</b> destination type only.
%empty%	This parameter is used in the <b>Fax Server</b> destination type only. It ensures that the subject/message is empty; it is used in very specific cases.

### Scan to FTP

Scanned documents can be sent to a folder defined on an FTP server.

Setting the connection in the **Parameters** section:

- **Server:** Enter the IP address or hostname of the FTP server
- **Port:** Enter the port used for the FTP protocol, the default port is 21
- **Use SSL:** Select if you want to use secure communication
- **User:** Name of the user with an account on the server
- **Password:** The user's password
- **Destination folder:** You can specify the subfolder where the outgoing scan files will be stored (optional).

You can use the following parameters when defining the destination folder:

- *%username%*: User name of the user session owner
- *%fullname%*: Full name of the user session owner
- *%date%*: Date and time when the scan was taken
- *%originalSubject%*: The default subject set on the printing device
- *%ipaddress%*: IP address of the printing device
- *%scanId%*: Unique scan identification number generated on the **KNM** server

After you fill the required parameters, you can click **Test** to test the FTP connection. **KNM** tries to upload a dummy file named *rightsCheck.dat* to the defined destination folder under the defined user name and password, and informs you about the result.

## Scan to a Fax Server

Scanned documents can be sent as emails to a fax server, which processes them and sends faxes to appropriate Fax numbers.

**Fax Server**

**General**

Title: \* Fax Server

Attach metadata file:

Filename template: \*  Default  
%username%\_%scanId%

You can edit the template on the terminal action's General tab.

Allow to edit filename **NEW**  
Users will be able to customize the filename on the terminal

Custom

**Parameters**

Parameters: %assetNo%, %date%, %fullName%, %ipaddress%, %location%, %originalSubject%, %printerContact%, %printerName%, %serialNumber%, %time%, %timestamp%, %username%, %usernotes%

Fax address template: \*  
Address template for sending a fax through a network fax server.  
Example: fax%number%.%recipient%.%username%@example.com

Sender: Default sender

Subject:

Message:

> **Advanced**

✓ Save Cancel

To send the document to a fax server, enter the appropriate email address template in the **Fax address template** field. You can use the following parameters:

- *%username%*: Name of the user session owner
- *%recipient%*: Fax recipient
- *%number%*: Fax number
- *%empty%*: This parameter ensures that the subject/message is empty; it is used in very specific cases
- *%ipaddress%*: IP address of the printing device
- *%scanId%*: Unique scan identification number generated on the **KNM** server

In the **Sender** drop-down, you can select one of the following addresses to be used as the fax sender:

- *Default sender*: The email set on the Network settings tab, under Outgoing SMTP server
- *KNM@KNM.local*: The sender is defined as *KNM@KNM.local*
- *Logged user*: Name of the user session owner
- *Printer contact*: The printing device contact email address set on its Web User Interface

You can also define the email's subject in the **Subject** text box, and the email's body in the **Message** text box.

## Scan to User's storage

Outgoing scan files are stored in the folder set in the **Folder or email for storing scanned documents** text box on the user properties panel.

**User's storage**

✕

▼ **General**

Title: \*

Attach metadata file:

Filename template: \*  Default

You can edit the template on the terminal action's General tab.

Allow to edit filename **NEW**

Users will be able to customize the filename on the terminal

Custom

▼ **Parameters**

Browse folders **NEW**

Only one destination folder can be browsed on the device at a time. When enabled, variables in the folder path are not supported

Connect as: \*  KYOCERA Net Manager Print Server service

Make the user doing the scan the owner of the file

User doing the scan

Other user

> **Advanced**

Fields marked by \* are mandatory.

Select the **Browse folders** option so users can browse one of their cloud destinations folder on the device.

The **Connect as** parameter determines in which way the scan will be stored in the folder:

- If you select the **KYOCERA Net Manager Print Server service** option, the rights for access to the destination folder have to be provided to the account under which the **KNM** service runs. This account will also be set as the owner of the scanned file.
  - If you select the **Make the user doing the scan the owner of the file** option, the user doing the scan will be set as the owner of the scanned file.
- If you select the **User doing the scan** option, **KNM** will expect the folder to be a shared folder on the domain account of the user doing the scan, and will use the entered password to access this folder. The user doing the scan will also be set as the owner of the scanned file.
- If you select the **Other user** option, **KNM** will expect the folder to be a shared folder on the domain account of the specified user and will use the entered username and password to access the folder. The user specified here will also be set as the owner of the scanned file.
  - If you select the **Make the user doing the scan the owner of the file** option, the user doing the scan will be set as the owner of the scanned file.

**KNM** cannot change the owner of scanned files that are stored under the **Users** folder or any of its subfolders. If you want to use the **Make the user doing the scan the owner of the file** option, use a different folder than **Users** (or its subfolders) as the scan destination.

## Scan to User's email

Scans are sent to the user's primary email address set in the **Email** text box on the user's properties panel (on the **Users** main tab of the **KNM Web Interface**).

In the **Parameters** section, you can define the subject of the emails sent to this destination in the **Subject** text box, and the body of these emails in the **Message** text box. The subject or body can contain the following parameters: *%username%*, *%fullName%*, *%date%*, *%originalSubject%*, *%ipaddress%*, *%usernotes%*, *%printerName%*, *%location%*, *%serialNumber%*, *%assetNo%*, *%printerContact%*.

## Scan to Email

Scans are sent to the email address specified here.

In the **Parameters** section, in the **Recipient** text box, you need to define the email recipient (or recipients).

In addition, you can add recipients of a copy in the **Copy** text box, recipients of a blind copy in the **Blind copy** text box, the subject of the email in the **Subject** text box, and the body of the email in the **Message** text box.

From **KNM** server 10.0+ the *%empty%* parameter can be used in the **Subject** and **Message** text boxes. If used, the subject and/or the body of the email are left empty.

The text boxes under can contain the following parameters: *%username%*, *%fullname%*, *%date%*, *%originalSubject%*, *%ipaddress%*, *%usernotes%*, *%printerName%*, *%location%*, *%serialNumber%*, *%assetNo%*, *%printerContact%*, *%empty%*.

### Scan to Folder

Scans are sent to the folder specified here.

**Folder**

▼ **General**

Title: \* Folder

Attach metadata file:

Filename template: \*  Default  
  
 You can edit the template on the terminal action's General tab.  
 Allow to edit filename **NEW**  
 Users will be able to customize the filename on the terminal

Custom

▼ **Parameters**

Parameters: %assetNo%, %date%, %fullname%, %ipaddress%, %location%, %originalSubject%, %printerContact%, %printerName%, %serialNumber%, %username%, %usenotes%

Destination folder: \*   
 Browse folders **NEW**  
 Only one destination folder can be browsed on the device at a time. When enabled, variables in the folder path are not supported

Connect as: \*  KYOCERA Net Manager Print Server service  
 Make the user doing the scan the owner of the file  
 User doing the scan  
 Other user

> **Advanced**

In the **Destination folder** field, type or browse and select the destination folder.

You can use the following parameters: *%username%*, *%fullname%*, *%date%*, *%originalSubject%*, *%ipaddress%*, *%scanId%*, *%counter%*, *%usenotes%*, *%printerName%*, *%location%*, *%serialNumber%*, *%assetNo%*, *%printerContact%*.

Select the **Browse folders** option so users can browse one of their cloud destinations folder on the device.

The **Connect as** parameter determines in which way the scan will be stored in the folder:

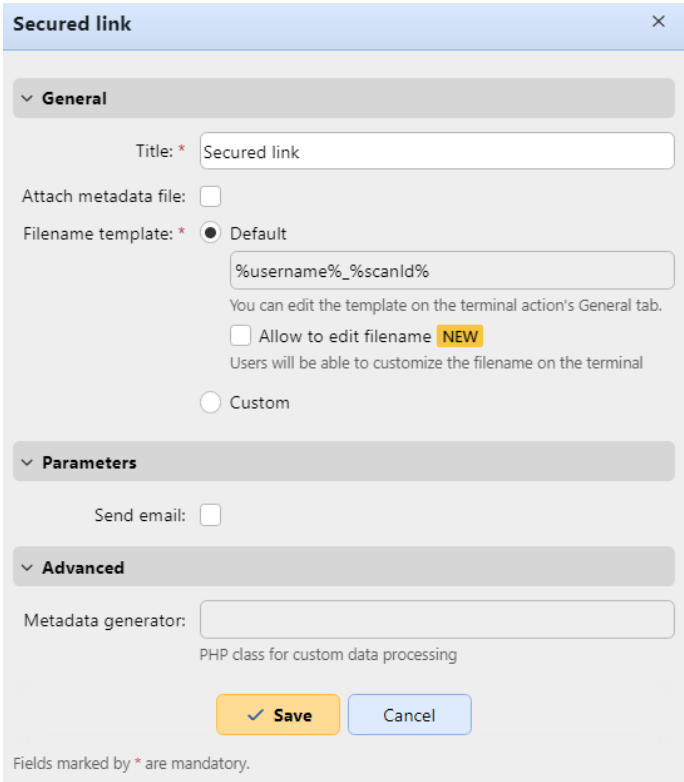
- If you select the **KYOCERA Net Manager Print Server service** option, the rights for access to the destination folder have to be provided to the account under which the **KNM** service runs. This account will also be set as the owner of the scanned file.
  - If you select the **Make the user doing the scan the owner of the file** option, the user doing the scan will be set as the owner of the scanned file.
- If you select the **User doing the scan** option, **KNM** will expect the folder to be a shared folder on the domain account of the user doing the scan, and will use the entered password to access this folder. The user doing the scan will also be set as the owner of the scanned file.
- If you select the **Other user** option, **KNM** will expect the folder to be a shared folder on the domain account of the specified user and will use the entered username and password to access the folder. The user specified here will also be set as the owner of the scanned file.

- If you select the **Make the user doing the scan the owner of the file** option, the user doing the scan will be set as the owner of the scanned file.

**i** **KNM** cannot change the owner of scanned files that are stored under the **Users** folder or any of its subfolders. If you want to use the **Make the user doing the scan the owner of the file** option, use a different folder than **Users** (or its subfolders) as the scan destination.

## Scan to Secured link

An email with a link to the scanned file is sent to the user's primary email address set in the **Email** text box on the user's properties panel (on the **Users** main tab of the **KNM** Web Interface). Sending scans to this destination works in a similar way as sending them to the **User's Email** destination, with one important exception: instead of the scanned file, the email contains a secure link to the file, which is stored on the **KNM** server, and can be downloaded via this link.



**Secured link** [X]

**General**

Title: \* Secured link

Attach metadata file:

Filename template: \*  Default  
%username%\_%scanId%

You can edit the template on the terminal action's General tab.

Allow to edit filename **NEW**  
Users will be able to customize the filename on the terminal

Custom

**Parameters**

Send email:

**Advanced**

Metadata generator:   
PHP class for custom data processing

Fields marked by \* are mandatory.

## Scan to OneDrive

To enable scanning to OneDrive:

1. Select the **Cloud storage** option in the **Type** drop-down.
2. Select the **OneDrive** option in the **Type** drop-down under **Parameters**. Select the **Browse folders** option if you want users to be able to browse one of their cloud destinations folder on the device.
3. Click **Save**.

**Cloud storage** ✕

**General**

Title: \*

Attach metadata file:

Filename template: \*  Default  
  
You can edit the template on the terminal action's General tab.

Allow to edit filename **NEW**  
Users will be able to customize the filename on the terminal

Custom

**Parameters**

Type: \*  ▼

Browse folders  
Only one destination folder can be browsed on the device at a time

**Advanced**

Metadata generator:

PHP class for custom data processing

Fields marked by \* are mandatory.

If the following two conditions are met, the cloud storage widget is displayed on the **Home** screen of the user logged on the **KNM Web Interface**:

- There is at least one **Easy Scan** terminal action with this destination.
- The user has rights to see the **Easy Scan** button or is connected to cloud drive.

Cloud storage			
Type	Status	Action	
OneDrive	Connected	<a href="#" style="color: #0070c0; text-decoration: none;">Disconnect</a>	

To be able to store the outgoing scan file on OneDrive, the user has to be connected.

To connect to OneDrive, the user has to perform the following actions:

1. Log in to the **KNM Web User Interface** with your user account.
2. On the **Cloud storage** widget, click **Connect**. The Cloud storage dialog box appears.
3. Click **Login to the cloud storage**.
4. Sign-in to OneDrive and confirm permissions (when asked about the permissions, click **Yes**).
5. Copy the given code.
6. Paste the code to the **KNM Cloud storage login dialog**.
7. Click **OK** to connect the cloud storage to **KNM**. The OneDrive connection status changes to **Connected**.

### Scan to OneDrive for Business

The feature has to be enabled in three steps:

1. First you have to provide **KNM** with access to your Azure AD.
2. Then, you have to create and set the OneDrive for Business destination.
3. Lastly, users have to connect their **KNM** accounts to OneDrive for Business.

### Setting up KNM access to Azure AD

To set up the access, you have to create a new Azure AD app registration to be used by **KNM**, and enter the Azure AD **Application ID** and **Secret** on the **Connections** settings tab in the **KNM** Web administrator interface.

In Azure AD, you need to create and set a new Azure Active Directory App registration to be used by **KNM**. After the registration is created, you set permissions and create a secret key. You need the Tenant ID, the Application ID and the secret key to create a Connection for OneDrive for Business on the **KNM** Web Interface. The secret key populates the Security key field.

1. Go to <https://portal.azure.com/> and log in with your global admin user account.
2. In the Azure dashboard, in the left navigation pane, click **Azure Active Directory** and on the left menu, click **App registrations**.
3. To create a new application, click **New registration**. The Register an application page appears.
4. In the **Name** box, type a name for the application.
5. Choose **Supported account types**.
6. In the Redirect URI box, choose **Web** and <https://netmanager-redirect.kyods.com/>.
7. Click **Register**.
8. Set the permissions:

API / Permissions name	Type	Description	Admin Consent Re...	Status
<div style="display: flex; justify-content: space-between; align-items: center;"> <span>Microsoft Graph (2)</span> <span>...</span> </div>				
<a href="#">Files.ReadWrite</a>	Delegated	Have full access to user files	-	...
<a href="#">User.Read</a>	Delegated	Sign in and read user profile	-	...

- a. On the preview screen, click **View API permissions**.
  - b. Click **Add a permission**. The Request API permissions pane appears.
  - c. **User.Read** permissions are added by default. Add **Delegated** permissions to **Files.ReadWrite** for the Microsoft Graph.
9. Back on the preview screen, click **Overview**, and then copy and save the **Application ID**, because you need it in the next steps.



10. On the preview screen, click **Certificates and secrets**, and complete the following steps:

Add a client secret

Description

Expires

In 1 year

In 2 years

Never

- a. Click **New client secret**.
  - b. Add a **Description**.
  - c. Set the expiry for the key to *Never*.
  - d. Click **Add**.
  - e. Save the **client secret key value**, because you need it in the following steps and you cannot retrieve it later.
11. Open the **Connections** settings tab on the **KNM Web Interface (KYOCERA, Settings, Connections)**.
  12. Click **+Add** and select **OneDrive Business** from the menu.
  13. Add a **Title**. This will be used to identify the Cloud Storage Destination.
  14. Add the **Tenant ID** (or write *common* for multi-tenant setups), the **Application ID**, and the client secret key value as **Security key** that you previously copied and saved, and click **OK**.

#### Create and set the OneDrive for Business destination

- Create a new destination (edit or create an Easy Scan terminal action; on its properties panel, in the **Destinations** tab, click **+Add**).
- On the new destination's properties panel, under **General**, select the *Cloud Storage* option in the **Type** drop-down.
- In the **Parameters** section, in the **Type** drop-down, select *OneDrive for Business* or any other **Title** you defined in the **Connections** settings in the previous steps.
- Select the **Browse folders** option if you want users to be able to browse one of their cloud destinations folder on the device.
- Click **Save**.

#### Connect a user's KNM account to OneDrive for Business

If the following two conditions are met, the cloud storage widget is displayed on the **Home** screen of the user logged on the **KNM Web Interface**:

- There is at least one **Easy Scan** terminal action with this destination.
- The user has rights to see the **Easy Scan** button or is connected to cloud drive.

Cloud storage		
Type	Status	Action
 OneDrive Business	Connected	<a href="#">Disconnect</a>

To be able to store the outgoing scan file on OneDrive for Business, the user has to be connected.

To connect to OneDrive for Business, the user has to perform the following actions:

1. Log in to the **KNM** Web User Interface with your user account.
2. On the **Cloud storage** widget, click **Connect**. The Cloud storage dialog box appears.
3. Click **Login to the cloud storage**.
4. Sign-in to OneDrive for Business and confirm permissions (when asked about the permissions, click **Yes**).
5. Copy the given code.
6. Paste the code to the **KNM** Cloud storage login dialog.
7. Click **OK** to connect the cloud storage to **KNM**. The OneDrive for Business connection status changes to **Connected**.

### Scan to Google Drive

To enable scanning to Google Drive:

1. Select the *Cloud Storage* option in the **Type** drop-down.
2. Select the *Google Drive* option in the **Type** drop-down in the **Parameters** section. Select the **Browse folders** option if you want users to be able to browse one of their cloud destinations folder on the device.
3. Click **Save**.

The screenshot shows a 'Cloud storage' dialog box with three sections: General, Parameters, and Advanced. In the General section, the Title is 'Cloud storage', Attach metadata file is unchecked, and the Filename template is '%username%\_%scanId%' with 'Default' selected. In the Parameters section, the Type is 'Google Drive' and 'Browse folders' is unchecked. In the Advanced section, the Metadata generator is empty. At the bottom, there are 'Save' and 'Cancel' buttons. A note at the bottom left states 'Fields marked by \* are mandatory.'

If the following two conditions are met, the cloud storage widget is displayed on the **Home** screen of the user logged on the **KNM** web interface:

1. There is at least one **Easy Scan** terminal action with this destination.
2. The user has rights to see the **Easy Scan** button or is connected to Google drive.

Cloud storage		
Type	Status	Action
 Google Drive	Connected	<a href="#">Disconnect</a>

To be able to store the outgoing scan file on Google Drive, the user has to be connected.

To connect to Google Drive, the user has to perform the following actions:

1. Log in to the **KNM** Web user interface with your user account.
2. On the Cloud storage widget, click **Connect**. The Cloud storage dialog box appears.
3. Click **Login to the cloud storage**.
4. Sign-in to Google Drive and confirm permissions. (When asked about the permissions, click **Allow**).
5. Copy the given code.
6. Paste the code to the Cloud storage login dialog.
7. Click **OK** to connect the cloud storage to **KNM**. The Google Drive connection status changes to **Connected**.

A single Google user account can be connected to only one server at a time. If the user wants to connect the account to another server, they need to remove **KYOCERA Net Manager** from the connected applications. This can be done on the **Apps with access to your account tab** under **My Account/Sign in & security/Apps with account access/MANAGE APPS**.

### Scan to Box.com

To enable scanning to Box.com:

1. Select the *Cloud Storage* option in the **Type** drop-down.
2. Select the Box.com option in the **Type** drop-down in the **Parameters** section. Select the **Browse folders** option if you want users to be able to browse one of their cloud destinations folder on the device.
3. Click **Save**.

**Cloud storage**

▼ **General**

Title: \* Cloud storage

Attach metadata file:

Filename template: \*  Default  
%username%\_%scanId%

You can edit the template on the terminal action's General tab.

Allow to edit filename **NEW**  
Users will be able to customize the filename on the terminal

Custom

▼ **Parameters**

Type: \* Box.com

Browse folders  
Only one destination folder can be browsed on the device at a time

▼ **Advanced**

Metadata generator:   
PHP class for custom data processing

Fields marked by \* are mandatory.

If the following two conditions are met, the cloud storage widget is displayed on the **Home** screen of the user logged on the **KNM** Web Interface:

1. There is at least one **Easy Scan** terminal action with this destination.
2. The user has rights to see the **Easy Scan** button or is connected to cloud drive.

Cloud storage		
Type	Status	Action
box Box.com	Connected	Disconnect

To be able to store the outgoing scan file on Box.com, the user has to be connected.

To connect to Box.com, the user has to perform the following actions:

1. Log in to the **KNM** Web user interface with your user account.
2. On the Cloud storage widget, click **Connect**. The Cloud storage dialog box appears.
3. Click **Login to the cloud storage**.
4. Sign-in to Box.com and confirm permissions (when asked about the permissions, click **Yes**).
5. Copy the given code.
6. Paste the code to the **KNM** Cloud storage login dialog.
7. Click **OK** to connect the cloud storage to **KNM**. The Box.com connection status changes to **Connected**.

### Scan to Dropbox

To enable scanning to Dropbox:

1. Select the *Cloud Storage* option in the **Type** drop-down.
2. Select the *Dropbox* option in the **Type** drop-down in the **Parameters** section. Select the **Browse folders** option if you want users to be able to browse one of their cloud destinations folder on the device.
3. Click **Save**.

**Cloud storage** [X]

**General**

Title: \* Cloud storage

Attach metadata file:

Filename template: \*  Default  
%username%\_%scanId%

You can edit the template on the terminal action's General tab.

Allow to edit filename **NEW**  
Users will be able to customize the filename on the terminal

Custom

**Parameters**

Type: \* Dropbox

Browse folders  
Only one destination folder can be browsed on the device at a time

**Advanced**

Metadata generator:   
PHP class for custom data processing

Fields marked by \* are mandatory.

If the following two conditions are met, the cloud storage widget is displayed on the **Home** screen of the user logged on the **KNM** web interface:

1. There is at least one **Easy Scan** terminal action with this destination.
2. The user has rights to see the **Easy Scan** button or is connected to cloud drive.

Cloud storage		
Type	Status	Action
Dropbox	Connected	Disconnect

To be able to store the outgoing scan file on Dropbox, the user has to be connected.

To connect to Dropbox, the user has to perform the following actions:

1. Log in to the **KNM** Web User Interface with your user account.
2. On the **Cloud storage** widget, click **Connect**. The Cloud storage dialog box appears.
3. Click **Login to the cloud storage**.
4. Sign-in to Dropbox and confirm permissions (when asked about the permissions, click **Yes**).
5. Copy the given code.
6. Paste the code to the **KNM** Cloud storage login dialog.

7. Click **OK** to connect the cloud storage to **KNM**. The Dropbox connection status changes to **Connected**.

### Scan to SharePoint Online

The feature has to be enabled in three steps:

1. First you have to register the **KNM** app in SharePoint.
2. Then you have to create and set the SharePoint Online destination.
3. Lastly, users have to connect their **KNM** accounts to SharePoint.

### Enabling access to SharePoint

To set up the access, you have to create a new Azure AD app registration to be used by **KNM**, and enter the Azure AD **Application ID** and **Secret** on the **Connections** settings tab in the **KNM** Web administrator interface.

In Azure AD, you need to create and set a new Azure Active Directory App registration to be used by **KNM**. After the registration is created, you set permissions and create a secret key. You need the Tenant ID, the Application ID and the secret key value to create a Connection for SharePoint on the **KNM** Web Interface. The secret key value populates the Security key field.

1. Go to <https://portal.azure.com/> and log in with your global admin user account.
2. In the Azure dashboard, in the left navigation pane, click **Azure Active Directory** and on the left menu, click **App registrations**.
3. To create a new application, click **New registration**. The Register an application page appears.
4. In the **Name** box, type a name for the application.
5. Choose **Supported account types**.
6. In the Redirect URI box, choose **Web** and <https://netmanager-redirect.kyods.com/>.
7. Click **Register**.
8. On the preview screen, click **View API permissions**. Click **Add a permission**. The Request API permissions pane appears. Select the "Microsoft Graph API" and choose **Delegated permissions** for your application.
  - a. Required permissions: *Sites.Read.All* and *Sites.ReadWrite.All*

Home > App registrations > My SharePoint Application

## Request API permissions

**Delegated permissions**  
Your application needs to access the API as the signed-in user.

**Application permissions**  
Your application runs as a background service or daemon without a signed-in user.

Select permissions expand all

Search: Sites

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Permission	Admin consent required
Sites (2)	
<input type="checkbox"/> Sites.FullControl.All Have full control of all site collections	Yes
<input type="checkbox"/> Sites.Manage.All Create, edit, and delete items and lists in all site collections	No
<input checked="" type="checkbox"/> Sites.Read.All Read items in all site collections	No
<input checked="" type="checkbox"/> Sites.ReadWrite.All Edit or delete items in all site collections	No

9. Back on the preview screen, click **Overview**, and then copy and save the **Application ID**, because you need it in the next steps.
10. On the preview screen, click **Certificates and secrets**, and then click **New client secret**. Add a **Description**, set the expiry for the key to *Never*, and click **Add**.
11. Save the client secret key **Value**, because you need it in the following steps and you cannot retrieve it later.

Home > App registrations > My SharePoint Application

## My SharePoint Application | Certificates & secrets

Search: Got feedback?

Got a second to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (1)** Federated credentials (0)

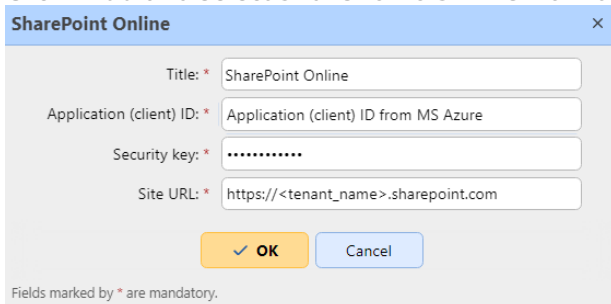
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
Secret	8/14/2023	L_...jX ...	5f...f ...

12. Open the **Connections** settings tab on the **KNM Web Interface (KYOCERA, Settings, Connections)**.

- Click **+Add** and select **SharePoint Online** from the menu.



- Add a **Title**. This will be used to identify the Cloud Storage Destination.
- Add the **Application ID** and the client secret key **value** as **Security key** that you previously copied and saved.
- Add the **Site URL**: `https://<tenant_name>.sharepoint.com` (to access the root SharePoint site) or `https://<tenant_name>.sharepoint.com/sites/<site_name>` (to access a specific site from the tenant's collection) and click **OK**.

#### Create and set the SharePoint Online destination

- Create a new destination (edit or create an Easy Scan terminal action; on its properties panel, in the **Destinations** tab, click **+Add**).
- On the new destination's properties panel, under **General**, select the *Cloud Storage* option in the **Type** drop-down.
- In the **Parameters** section, in the **Type** drop-down, select *SharePoint Online*, and click **Save**.

#### Connect a user's KNM account to SharePoint Online

If the following two conditions are met, the cloud storage widget is displayed on the **Home** screen of the user logged on the **KNM Web Interface**:

- There is at least one **Easy Scan** terminal action with this destination.
- The user has rights to see the **Easy Scan** button or is connected to cloud drive.

Cloud storage		
Type	Status	Action
 SharePoint Online	Connected	Disconnect

To be able to store the outgoing scan file on SharePoint Online, the user has to be connected.

To connect to SharePoint Online, the user has to perform the following actions:

- Log in to the **KNM Web User Interface** with your user account.
- On the **Cloud storage** widget, click **Connect**. The Cloud storage dialog box appears.
- Click **Login to the cloud storage**.
- Sign-in to SharePoint Online and confirm permissions (when asked about the permissions, click **Yes**).
- Copy the given code.
- Paste the code to the **KNM Cloud storage login dialog**.
- Click **OK** to connect the cloud storage to **KNM**. The SharePoint Online connection status changes to **Connected**.

## Scan to Amazon S3

In order to scan to Amazon S3, you need to:

- Set up a bucket on the Amazon console. Your scans will be stored in this bucket.
- Create a user who will be used in the **KNM** Web UI.
- Give the created user rights to the bucket.
- Fill in the **Client ID** and **Security Key** in the **KNM** web administrator interface.
- Set up an Easy Scan terminal action to scan to Amazon S3.

### Setting up a bucket on the Amazon S3 console

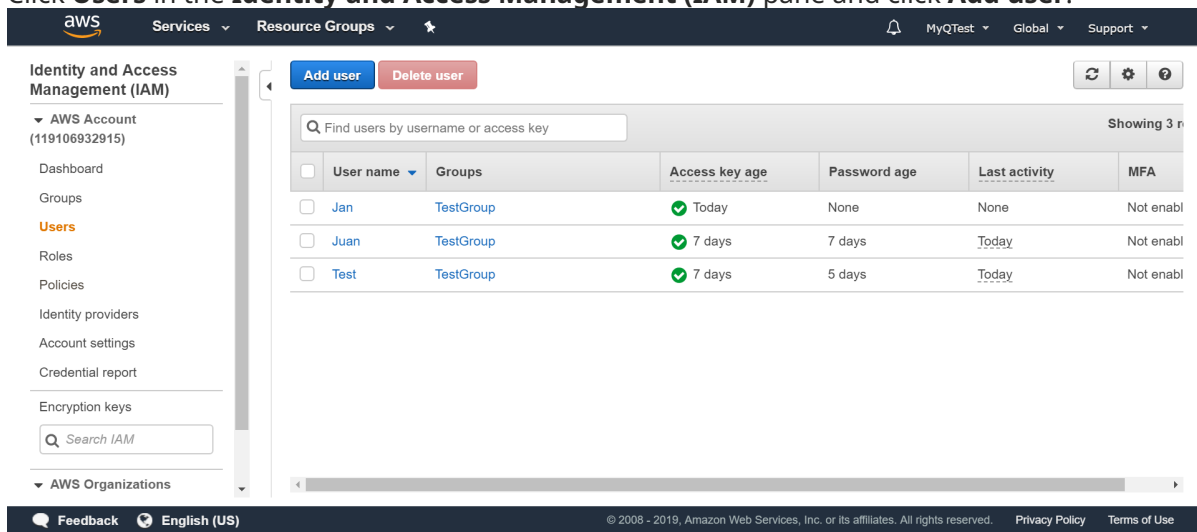
You need an Amazon account to create a bucket to store the scans in. **KNM** does not require any specific settings for scanning to an S3 bucket.

1. Login to <https://console.aws.amazon.com/s3> and sign in with your Amazon account or create a new account. You need a credit card as proof of name. The credit card will also be used to charge the use of Amazon S3.
2. Use the <https://docs.aws.amazon.com/AmazonS3/latest/gsg/s3-gsg.pdf> to guide you through creating a S3 bucket.

### Create a user in Amazon S3

You need to create a user to make a connection between Amazon S3 and the **KNM** Web UI.

1. Log in to the Amazon console.
2. Click the arrow next to your login name and select **My Security Credentials** from the drop-down menu.
3. Click **Users** in the **Identity and Access Management (IAM)** pane and click **Add user**.



The screenshot shows the AWS IAM console interface. The left sidebar contains navigation options: Identity and Access Management (IAM), AWS Account (119106932915), Dashboard, Groups, Users (highlighted), Roles, Policies, Identity providers, Account settings, Credential report, Encryption keys, and AWS Organizations. The main content area shows a table of users with columns for User name, Groups, Access key age, Password age, Last activity, and MFA. The table lists three users: Jan, Juan, and Test, all belonging to the TestGroup. The Access key age for Jan is Today, for Juan is 7 days, and for Test is 7 days. The Password age for Juan is 7 days and for Test is 5 days. The Last activity for all users is Today. The MFA status for all users is Not enabled. The top navigation bar includes Services, Resource Groups, MyQTest, Global, and Support. The bottom footer contains Feedback, English (US), and copyright information.

<input type="checkbox"/>	User name	Groups	Access key age	Password age	Last activity	MFA
<input type="checkbox"/>	Jan	TestGroup	Today	None	None	Not enabled
<input type="checkbox"/>	Juan	TestGroup	7 days	7 days	Today	Not enabled
<input type="checkbox"/>	Test	TestGroup	7 days	5 days	Today	Not enabled

4. Follow the instructions to create the user.
5. Copy and save the **Client ID** and the **Access Key ID** of the created user, as you need them in the following steps.

### Give user access rights to the bucket

To give bucket permission to the user, you can follow the [official instructions](#), or follow the short procedure below:

1. Click **Policies** in the **Identity and Access Management (IAM)** pane. Click **Create a new Policy**. The policy settings should be set as in the image below. If you do not want to provide the user with access to all buckets: deselect **Any** and click **Add ARN** to enter a specific bucket.

Visual editor | JSON | Import managed policy

Expand all | Collapse all

▼ S3 (32 actions) | Clone | Remove

▶ Service S3

▶ Actions Write

AbortMultipartUpload	PutAnalyticsConfiguration	PutMetricsConfiguration
CreateBucket	PutBucketCORS	PutObject
CreateJob	PutBucketLogging	PutObjectLegalHold
DeleteBucket	PutBucketNotification	PutObjectRetention
DeleteBucketWebsite	PutBucketObjectLockConfiguration	PutReplicationConfiguration
DeleteObject	PutBucketRequestPayment	ReplicateDelete
DeleteObjectVersion	PutBucketVersioning	ReplicateObject
GetBucketObjectLockConfiguration	PutBucketWebsite	RestoreObject
GetObjectLegalHold	PutEncryptionConfiguration	UpdateJobPriority
GetObjectRetention	PutInventoryConfiguration	UpdateJobStatus
PutAccelerateConfiguration	PutLifecycleConfiguration	

▼ Resources  Specific  All resources [close](#)

bucket ?	Any resource of type = bucket	<input checked="" type="checkbox"/> Any
job ?	Any resource of type = job	<input checked="" type="checkbox"/> Any
object ?	Any resource of type = object	<input checked="" type="checkbox"/> Any

▶ Request conditions [Specify request conditions \(optional\)](#)

[Cancel](#) [Review policy](#)

2. Click **Groups** in the **Identity and Access Management (IAM)** pane. Click **Create New Group**. Give the group a name and **Save** it.
3. Click **Add Users to Group** and add the created user to the group.
4. Click the **Permissions** tab and click **Attach Policy**. Select the policy you just created and **Save** it all. The user now has **Write** access to the created bucket.

### Setup a connection between KNM and Amazon S3

1. Open the **Connections** settings tab of the **KNM Web Interface (KYOCERA, Settings, Connections)**.
2. Click **+Add** and select **Amazon S3** from the menu.
3. Add a **Title**. This will be used to identify the Cloud Storage Destination.
4. Add the **Access Key ID**, the **Security key** that you previously copied and saved, the **Region**, and **Bucket** and click **OK**.

### Create and set the Amazon S3 destination

- Create a new destination (edit or create an Easy Scan terminal action; on its properties panel, in the **Destinations** tab, click **+Add**).
- On the new destination's properties panel, under **General**, select the *Cloud Storage* option in the **Type** drop-down.
- In the **Parameters** section, in the **Type** drop-down, select *Amazon S3* or any other **Title** you defined in the **Connections** settings in the previous steps and click **Save**.
- Fill in the fields:
  - **Bucket**: the name of the Amazon S3 bucket to store the scans in.

- **Region:** the region you have set when creating the bucket.
- **Folder path:** enter the path of a sub folder.

### Easy Scan Parameters

On the **Parameters** tab, you can set the scanned file's parameters, such as resolution and format. You can select from a number of options for each parameter.

There are predefined parameters, but you can also create your own parameters.

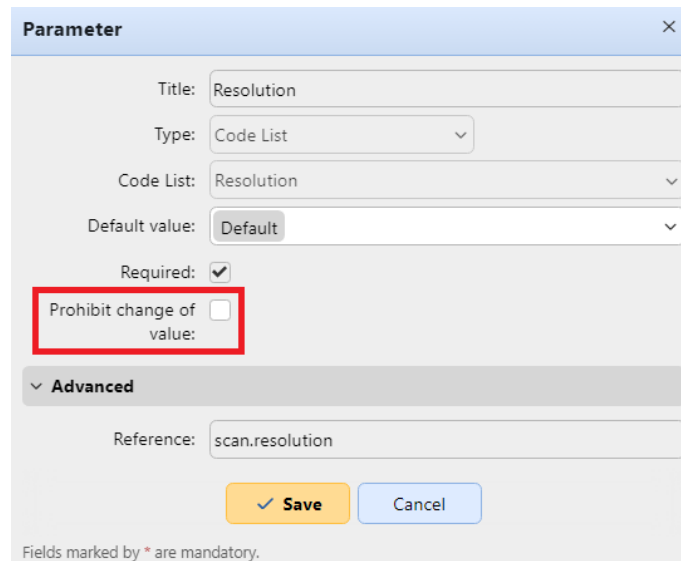
**⚠** All parameters are dependent on the particular printing device type. Therefore, some parameters and/or values might not be available.

R...	Title	Value	Type
	Resolution	Default	Code List
	Color	Default	Code List
	Format	Default	Code List
	Duplex	Default	Code List
	Continuous scan	Disabled	Code List
	Scan Separation	Default	Code List
	Original Image	Default	Code List
	Original Orientation	Default	Code List
	Density	Default	Code List
	Size	Default	Code List
	Mixed size	Default	Code List
	Skip blank pages	Default	Code List

Some parameters (e.g. resolution, color) significantly influence the scanned file's size. For example, a combination of higher resolution and full color will dramatically increase the file size.

You can allow users to change their scan settings from the terminal screen.

To do this, you have to modify the settings of the particular parameter on the **Parameters** tab on the **Easy Scan** action node properties panel. Open the parameter properties panel, uncheck the **Prohibit change of value** option (checked by default) and **Save**.



**Parameter** [X]

Title: Resolution

Type: Code List

Code List: Resolution

Default value: Default

Required:

Prohibit change of value:

**Advanced**

Reference: scan.resolution

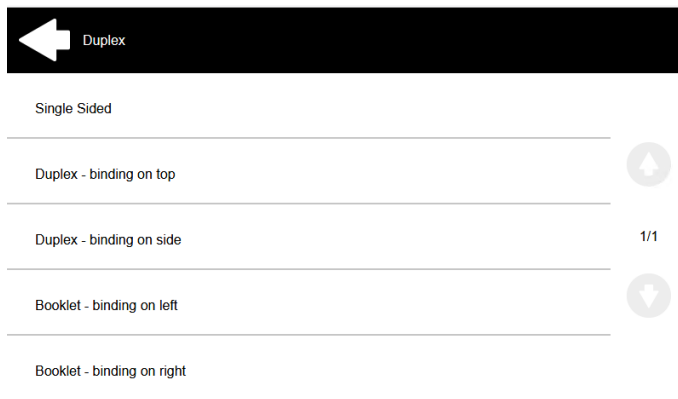
[Save] [Cancel]

Fields marked by \* are mandatory.

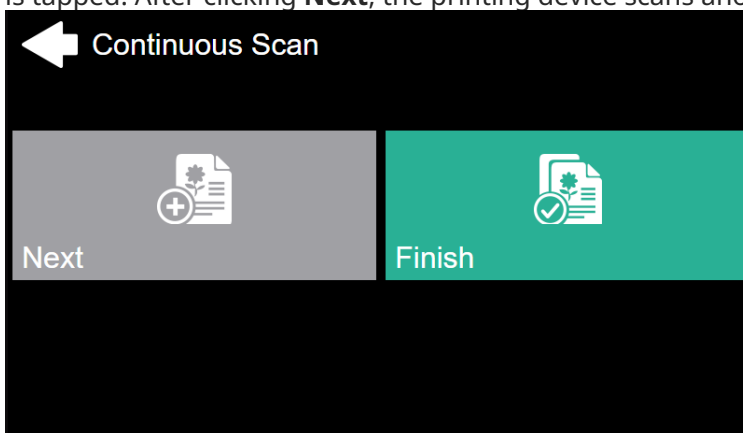
## Predefined Parameters

Each parameter has a *Default* option. If selected, the actual values are taken from the default scan settings of the printing device.

- **Resolution** - The outgoing file's resolution. You can select from the following options:
  - 100 dpi
  - 200 dpi
  - 300 dpi
  - 400 dpi
  - 600 dpi
  - Default
- **Color** - The outgoing file's color scale. You can select from the following options:
  - Color
  - Grayscale
  - B&W (two tones)
  - Automatic
  - Default
- **Format** - The outgoing file's format. You can select from the following options:
  - PDF
  - JPEG
  - TIFF
  - XPS
  - HCPDF
  - Default
- **Duplex** - Simplex and Duplex scanning options. You can select from the following:
  - Single Sided
  - Duplex - binding on top
  - Duplex - binding on side
  - Booklet - binding on left
  - Booklet - binding on right
  - Default



- **Continuous scan** - With the continuous scan option *Enabled*, scan jobs are not sent until **Finish** is tapped. After clicking **Next**, the printing device scans another page.



You can select from the following:

- Disabled
- Enabled
- Default
- **Scan separation** - If a document with multiple pages is scanned, scanned pages can be stored either separately (each page in a separate file) or all together in one file. You can select from the following options:
  - All pages together
  - Separate each page
  - Default
- **Original Image** - Determines the way in which the printing device is going to process the scanned page. You can select from the following options:
  - Text + Photo
  - Photo
  - Text
  - Default
- **Original Orientation** - Determines the scanned page's orientation in the outgoing file. The paper's position is relative to the person standing at the printing device. You can select from the following options:
  - Top Edge on Top: The page is displayed in a horizontal position (top edge of the page opposite to the person)
  - Top Edge on Left: The page is displayed in a vertical position (top edge of the page on the left hand side of the person)
  - Default

- **Density** - The picture's density in the outgoing file. The higher it is, the darker the resulting picture is. You can select from the following options:
  - Automatic
  - Lowest
  - Lower
  - Low
  - Normal
  - High
  - Higher
  - Highest
  - Default
- **Size** - The scanned output's size. This determines the size of the scanning area, therefore it should correspond to the actual size of the scanned paper. You can select from the following options:
  - Automatic
  - A3
  - A4
  - A5
  - A6
  - Folio
  - Ledger
  - Letter
  - Legal
  - Oficio II
  - Statement
  - Default
- **Skip blank pages** - With this parameter, you can select to skip blank pages in the scanned document. You can select from the following options:
  - Default
  - Yes
  - No

### Create custom parameters

You can create new parameters to be used in the scan metadata, or as parts of file names, addresses, subjects and email bodies, and as paths to folders, passwords to folders etc.

The following parameter types can be created: *Text, Password, Yes/No, KYOCERA Net Manager Users, Code Book, User Properties, Device Properties.*

To create a custom parameter:

1. On the action node properties panel, go to the **Parameters** tab.
2. On the tab, click **+Add**. The new Parameter properties panel opens on the right side of the screen.
3. Set the parameter, and then click **Save**. The new parameter is now displayed on the list on the **Parameters** tab.

Parameter Settings:

- **Title** - The parameter's name.
- **Type** - Select the parameter's type from the drop-down:
  - *Text* - Text (string) typed by the user on the embedded terminal. You can use these parameters in a variety of strings in **KNM**: names of files, addresses, subjects or email bodies, paths to folders and many other. In the **Validator** field, regular expressions can be used to define or limit the user's input.

- *Password* - Password to a user's account. This parameter is used together with the **Logged user** option for the **User's storage** destination type. Users type the password to their domain account to access their shared folder there.
- *Yes/No* - Boolean parameter with the options: *Yes*, *No*. You can use these parameters in the scan metadata file to provide answers on Yes-No questions concerning the scan, such as if the scan is private or if it should be archived.
- *Code Book* - The parameter uses a list of values from internal code lists. Users can select options from lists of values used in metadata and destinations.
  - **Internal code list:** You can predefine code lists with values and use the values as options available for users.
  - **LDAP sourced list:** This parameter enables selecting scan recipients directly from an LDAP server by importing the codes from the server.
  - **MS Exchange Address Book:** You can use this code book to get personal contacts from an MS Exchange server. The contacts are retrieved using an account defined by the administrator in the **KNM** Web UI. This account requires special rights on the MS Exchange server that allow it to access other users' mailboxes. The user sees the first 50 contacts on the terminal. To look for more contacts they would have to use the search function.
- *User Properties* - The parameter can represent **KNM** user properties within the metadata file of the scanned document. You can select one of the following values to be represented by the parameter:
  - User name
  - Full name
  - Email
  - User's storage
  - Personal number
  - Phone
  - Notes
  - Accounting Group
- *Device Properties* - The parameter can represent **KNM** printing device's properties within the metadata file of the scanned document. You can select one of the following values to be represented by the parameter:
  - Name
  - Location
  - IP address
  - Brand
  - Model
  - Serial number
  - Asset number
  - Notes
- **Default value** - A predefined value/option that will be used if nothing else is selected.
- **Required** - The parameter value has to be defined. If the parameter does not have a default value, users are not allowed to print before this value is entered in the particular text box on the terminal screen.
- **Prohibit change of value** - If this option is selected, the parameter cannot be changed by the users on the terminal screen.
- **Reference** - String that is used as a reference to the parameter. A parameter with the *parameterX* reference is referred to as *%parameterX%* in **KNM**. For example, the reference of the often used user name parameter is *username*; the parameter is referred to as *%username%*.

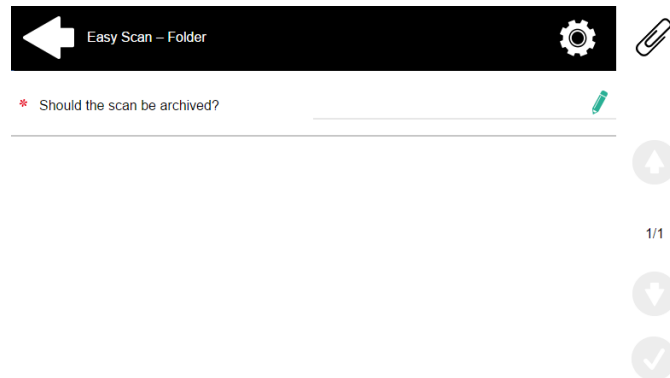
### Custom parameters examples

These are some examples of using custom parameters.

## Providing additional information in a metadata file

In this example, you can see how to use parameters for obtaining additional information about the scan file or any other data provided by users. The parameter's **Type** can be *Text* or *Yes/No*.

As an example, we will create a *Yes/No* **Type** parameter, called **Should the scan be archived?**.



1. The **Title** will be shown on the screen, therefore we name it **Should the scan be archived?**.
2. The **Type** is *Yes/No*.
3. The **Required** option is selected by default and cannot be deselected as it always has a value.
4. The **Default value** is left unchecked..
5. We do not have to use the reference, as the parameter is not going to be used in any string in **KNM**. Therefore, we can **Save** the parameter settings.

A screenshot of the 'Parameter' configuration dialog box. The dialog has a title bar with 'Parameter' and a close button. Inside, there are several fields and checkboxes:

- Title: \* Should the scan be archived? (text input)
- Type: \* Yes/No (dropdown menu)
- Default value:
- Required:
- Prohibit change of value:

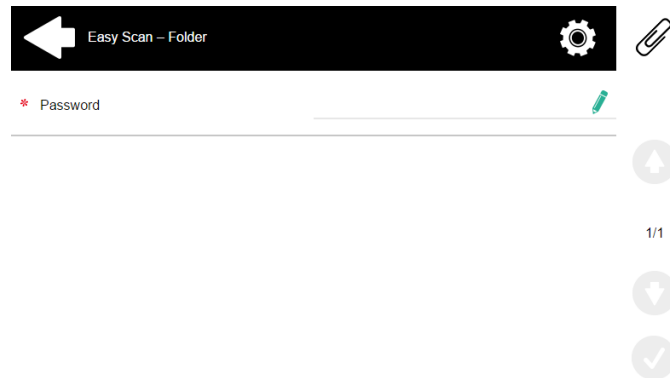
Below these fields is a section labeled '> Advanced'. At the bottom, there are two buttons: 'Save' (with a checkmark) and 'Cancel'. At the very bottom, there is a note: 'Fields marked by \* are mandatory.'

The following two figures show two possible values of the **Should the scan be archived?** parameter. A DMS software can automatically archive the scans with value *1* into a predefined folder.

```
- <field>
  <name>Should the scan be archived?</name>
  <reference/>
  <value/>
</field>
- <field>
  <name>Should the scan be archived?</name>
  <reference/>
  <value>1</value>
</field>
```

### Enabling users to scan to their home folder protected by password

If you do not want to give to the **KNM** server universal access to users' shared folders, but instead want to provide each user with separate rights to access their shared folder from **KNM**, you can enable the scanning users to enter the password to their LDAP domain account to access the shared folder there.



To be able to access their shared folders, users should have the LDAP domain defined in **KNM**. The information about the domain is taken either from the **Authentication server** setting on the user's properties panel in **KNM**, or from the user's **KNM** user name (if the name is in the form *LDAPusername@domain.local*).

During the scanning, after the password is entered and submitted, **KNM** takes the name of the user's domain (either from the **Authentication server** setting, or from the back part of the user name) and attempts to log on the user's account on this domain (either the whole user name, or its front part). If the password is correct, **KNM** saves the scan in the shared folder; otherwise it displays the error message *"Error while delivering a scan X/Y. Unable to write to the folder."*

On the **Parameters** tab, create a parameter with the following properties: **Title:** Password, **Type:** Password, **Required:** selected, **Reference:** password.

A screenshot of the 'Parameter' configuration dialog box. The dialog has a blue header bar with the title 'Parameter' and a close button (X). The main area is light gray and contains the following fields: 'Title: \*' with a text input field containing 'Password'; 'Type: \*' with a dropdown menu showing 'Password'; 'Required:' with a checked checkbox; an expanded 'Advanced' section with a 'Reference:' text input field containing 'password'; and two buttons at the bottom: a yellow 'Save' button with a checkmark and a blue 'Cancel' button. At the bottom left, there is a note: 'Fields marked by \* are mandatory.'

On the **Destinations** tab, set the **User's storage** destination type. In the **Parameters** section, select the **Connect as: User doing the scan** option and select the newly created *password* parameter in the drop-down.

**User's storage** ✕

**General**

Title: \*

Attach metadata file:

Filename template: \*  Default

You can edit the template on the terminal action's General tab.

Allow to edit filename **NEW**

Users will be able to customize the filename on the terminal

Custom

**Parameters**

Browse folders **NEW**

Only one destination folder can be browsed on the device at a time. When enabled, variables in the folder path are not supported

Connect as: \*  KYOCERA Net Manager Print Server service

User doing the scan
 

Password ▼

Select a password parameter, so user will be prompted for the password on the terminal.

Other user

### Enabling users to select the output folder from a code book

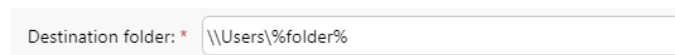
In this example, you can see how to enable users to select the scan destination folder from a predefined code book. For this example, we have already created and saved the Easy Scan action node, and we have created a code book named *Folders*, which has names of folders as its values. The next step is to add and set up a new **Code Book** type parameter and a new **Folder** destination type for the Easy Scan action. The parameter is then used as a part of the path to the folder.



On the **Parameters** tab create a parameter with the following settings: **Title:** Output folder, **Type:** Code Book, **Code Book:** Folders, **Default value** (optional), **Prohibit change of value:** deselect, **Reference:** folder. If you want to allow users to select multiple recipients, select **Allow multiple values**.

If you want to allow users to enter their own value, select **Allow custom values**. If you don't want to allow empty values, select the **Required** option so that users have to enter its value before sending the file. Optionally, you can select a default value to define the folder where the output files will be saved, if users don't change it.

On the **Destinations** tab, create and set up a new destination. For this destination, you can use the parameter as any part of the destination path set in the **Destination folder** text box. To use the parameter, enter its reference name bounded in percentage signs as part of the path. In our example, we used a parameter with the reference name *folder* as the folder where the files are stored (*\\Users%folder%*).



Destination folder: \* \\Users%folder%

### Enabling users to search recipients via LDAP Source code books

In this example, you see how to enable users to search for recipients on LDAP servers via LDAP Source code books. LDAP Source code books contain two parameters: **Title** and **Value**. The value of the **Title** parameter is used as an input for searching in the LDAP database and the **Value** parameter defines the value returned by the database. We use an LDAP Source code book with the **cn** attribute assigned to the **Title** parameter and the **mail** attribute assigned to the **Value** parameter. We also create a new parameter and a new folder destination for the feature. The scanning user types a string to be used in a search query. **KNM** sends the query to the LDAP database to search for user accounts, whose **cn** begins with the entered string. The scanning user can select from the returned accounts. After they select the account, the value of the **mail** attribute of the account is used as the scan destination.



All Users

Enter a search query

1/1

On the **Parameters** tab, create a parameter with the following settings: **Title:** Recipients, **Type:** Code Book, **Code Book:** Emails (or the LDAP source code book that you want to use), **Prohibit change of value:** deselect, **Reference:** recipients. If you want to allow users to select multiple recipients, select **Allow multiple values**. If you want to allow users to enter their own value, select **Allow custom values**. If you don't want to allow empty values, select the **Required** option so that users have to enter its value before sending the file.


On the **Destinations** tab, create an **Email** destination type and enter the parameter in the **Recipient** text box, enclosed in percent signs (*%recipients%*).

## Easy Copy settings

With the **Easy Copy** feature, users do not have to go to the often complicated and confusing copy screen of the printing device — they can copy directly from the **KNM** terminal home screen with a single touch. Upon tapping the button, **KNM** can simply proceed copying using the default settings of the printing device, or it can use different values of the Easy Copy action parameters.

By adding multiple Easy Copy action nodes and giving rights to different users or groups, you can create a variety of copying options for the selected users and groups.

On the **Parameters** tab, you can select from a number of options for each parameter.

 All parameters are dependent on the particular printing device type. Therefore, some parameters and/or values might not be available.

## Easy Copy Parameters

- **Copies** - Predefine the number of copies to be available 1-99.
- **Color** - Color scale of the outgoing file. You can select from the following options:
  - Color
  - Monochrome
  - Automatic
  - Default
- **Duplex** - Simplex and Duplex scanning options. You can select from the following options:
  - Single Sided
  - Duplex
  - 1-sided to 2-sided
  - 2-sided to 1-sided
  - Default
- **Original Orientation** - Determines the page's orientation in the outgoing file. The paper's position is relative to the person standing at the printing device. You can select from the following options:
  - Top Edge on Top: The page is displayed in a horizontal position (top edge of the page opposite to the person)
  - Top Edge on Left: The page is displayed in a vertical position (top edge of the page on the left hand side of the person)
  - Default
- **Density** - Density of the picture in the outgoing file. The higher it is, the darker the resulting picture is. You can select from the following options:
  - Automatic
  - Lowest
  - Lower
  - Low
  - Normal
  - High
  - Higher
  - Highest
  - Default
- **Size** - Size of the scanned input. It determines the size of the scanning area; therefore, it should correspond to the actual size of the scanned paper. You can select from the following options:
  - Automatic
  - A3

- A4
- A5
- A6
- B4
- B5
- B6
- Folio
- Ledger
- Letter
- Legal
- Statement
- Oficio II
- Default
- **Magnification** - With this parameter, you can determine the size of the copy. This way, you can make it smaller or larger than the original file. You can select from the following options:
  - Default
  - Same as original
  - A3
  - A4
  - A5
  - A6
  - B4
  - B5
  - B6
  - Folio
  - Ledger
  - Letter
  - Legal
  - Statement
- **Skip blank pages** - With this parameter, you can select to skip blank pages in the copied document. You can select from the following options:
  - Default
  - Yes
  - No
- **Mixed size** - This parameter enables automatic paper size recognition when different sizes of paper are used during copying.
  - Yes: The output paper size parameter will be ignored and be decided by the device itself depending on the scanned image size.
  - No: The output paper size must be set (everything but Auto) and the image will be zoomed and scanned to the same size.
  - Default



The Mixed size parameter can be used only for papers of the same group with a side of the same length. KNM server 10.0 patch 7+ and devices with HyPAS 2.1.5+ are required.

### General Limitations

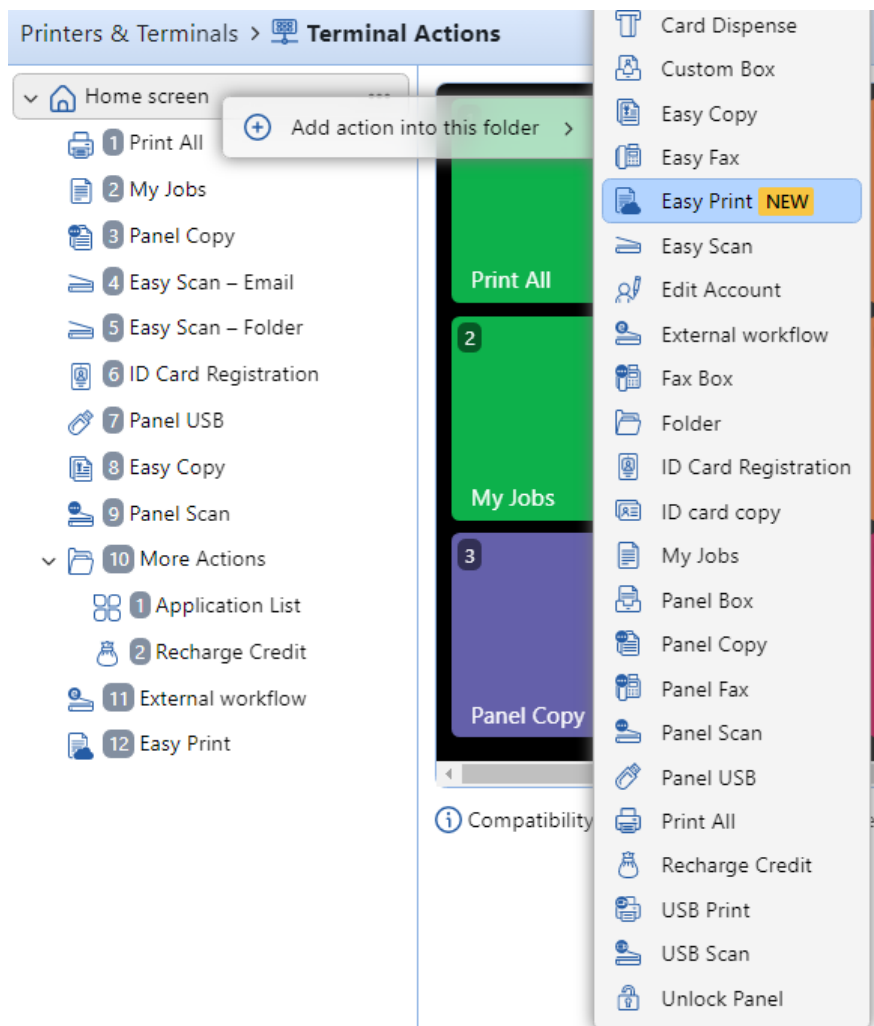
- The exact list of supported parameters for Easy Copy depends on each vendor/machine.
- Continuous Scan is not supported by all machines even within the same brand.

- Continuous Scan jobs consisting of different formats may account the whole job as one format or different formats depending on SDK abilities. The final format (in case of single format accounting) also depends on SDK abilities.

## Easy Print settings

The Easy Print terminal action allows users to print files without sending them first to **KNM**. These files can be printed from multiple destinations, like several cloud storages, network drives or local drives, and the user's default storage.

In order to use Easy Print, a new terminal action has to be created in **KYOCERA, Settings, Terminal Actions**.



1. Right-click on **Home Screen**, and point to **Add action node into this folder** in the shortcut menu. Another sub-menu with a list of available action nodes opens to the right.
2. On the sub-menu, select **Easy Print**. The new action node properties panel opens on the right side of the screen.

On the properties panel you can configure which destinations should be available for the user, and the default release options. It is possible to create multiple instances of the Easy Print action, each one with different settings.

In the General tab, you can configure the **Printers** and **Rights** for the Easy Print terminal action, and define the **Default print properties**: *Color, Duplex, Staple, Punch, Toner saving, and Copies*.

The screenshot shows the 'Easy Print' configuration window with the 'General' tab selected. The 'Enabled' toggle is turned on. The 'Title' field is set to 'en Easy Print'. The 'Printers' dropdown is set to 'All printers' and the 'Rights' dropdown is set to 'All users'. The 'Style' dropdown is set to 'Easy Print'. Below these is a section for 'Default print properties' with a note: 'Final job settings are a combination of these default print properties, policies set on the Easy Print queue, user policies, and changes made on the embedded terminal.' The properties are: Color (Color), Duplex (Simplex), Staple (No), Punch (No), Toner saving (No), and Copies (1). At the bottom are 'Save' and 'Cancel' buttons. A note at the very bottom states 'Fields marked by \* are mandatory.'

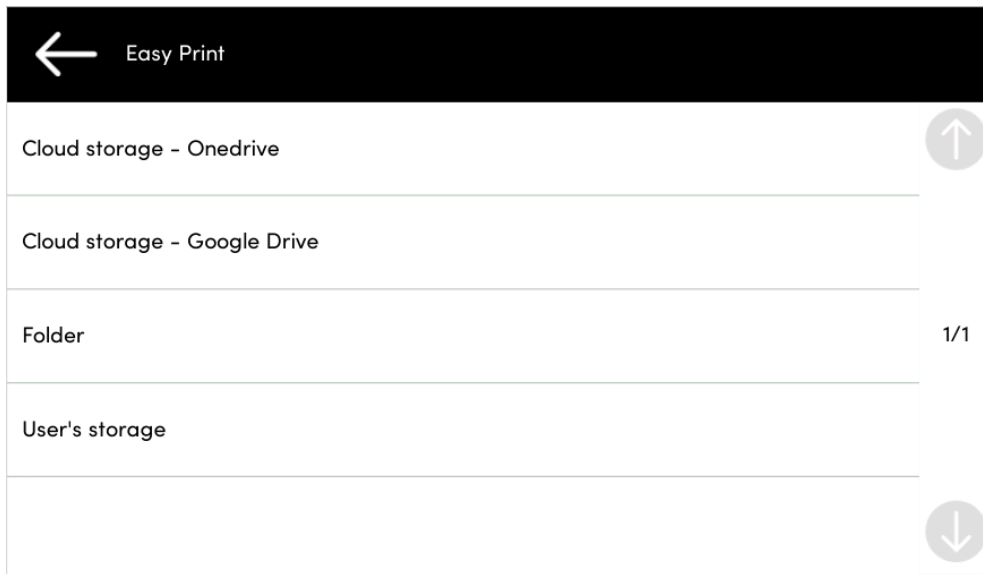
In the Storages tab, click **Add** to add a new storage type. You can select from **Cloud storage, Folder, and User's storage**.

The screenshot shows the 'Easy Print' configuration window with the 'Storages' tab selected. The 'Add' button is highlighted, and a dropdown menu is open showing three options: 'Cloud storage', 'Folder', and 'User's storage'. Below the menu, the text 'The list is empty' is displayed, and another 'Add' button is visible at the bottom.

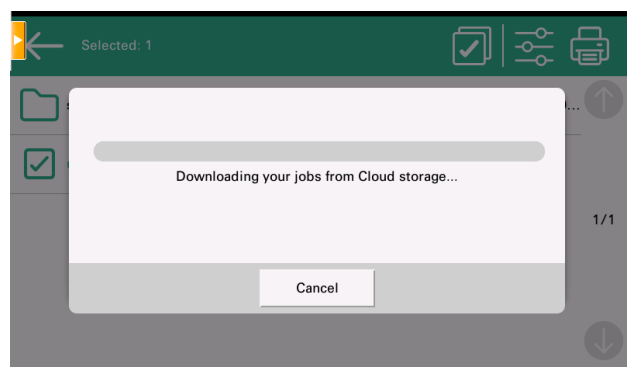
The supported formats for Easy Print are: *bmp, jfif, jpe, jpeg, jpg, mime, png, tif, tiff, txt, urf, and pdf*.

If Microsoft Office suite or Libre Office are installed on the server, the **Microsoft formats** *doc*, *docx*, *xls*, *xlsx*, *ppt*, *pptx* and **Libre Office formats** are also supported. These are converted into PDF based on the settings in *Jobs - General - Office file formats*.

When Easy Print is used on the terminal, the user is presented with a list of possible destinations associated with this action (this is skipped in case of a single destination). After the destination is selected, the user can browse it and select files for printing.



After pressing the print button, the files are downloaded from the destination to the server, processed through the default Easy Print queue, and released immediately to the printer without any further interaction. It is also possible to cancel the whole downloading and printing process. In this case, files that have already been downloaded, but not printed are deleted from the server. Files that have already been printed remain on the server and it is possible to reprint them.



## 9.2 Manually adding printing devices

To manually add a device:

1. On the **Printers** main tab, click **+Add printer**. A drop-down box appears.

2. In this drop-down box, click **+Add printer**. The new printing device properties panel opens on the right side of the screen.
3. On the panel, enter the device name and IP address, and then click **Save**.

## 9.3 Configuration profiles

A configuration profile is used for multiple printers configuration. It is where you can add an installation package and attach it to printers to equip them with embedded terminals.

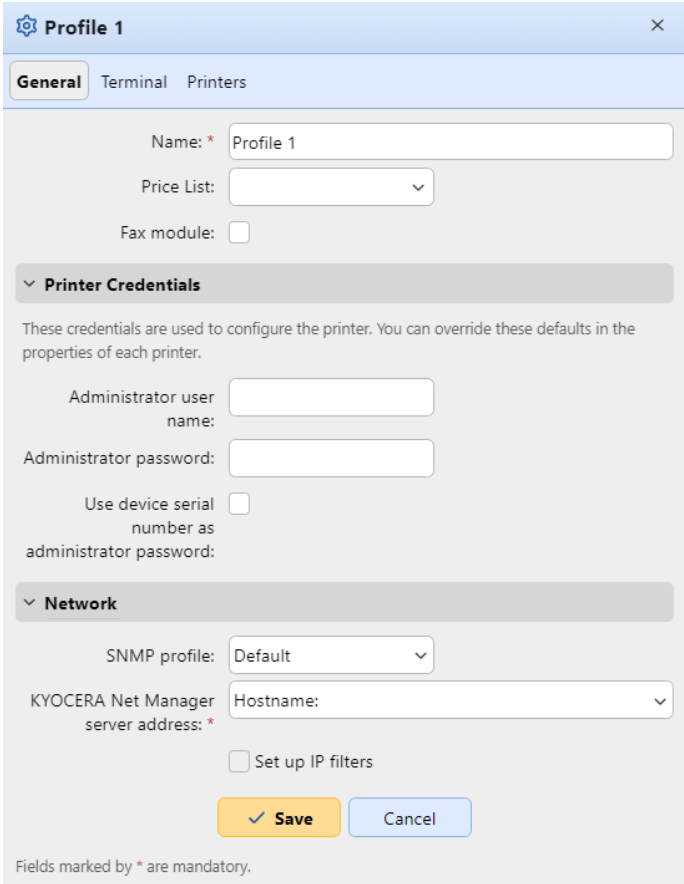
It is recommended to create a configuration profile per printer type if you have different printer types.

For a quicker setup you can clone your configuration profiles. With minimal editing you can then create a new profile. Printers will not be cloned to this new configuration profile. Go to **KYOCERA, Settings, Configuration Profiles**, select a configuration profile and click **Clone** on the menu bar (or right click and clone).

Configuration profiles are needed for printer discovery.

The following settings can be configured:

### General tab



- **Name** - It is mandatory to give the profile a name.
- **Price List** - Select a price list from the drop-down. For more information on price lists, see [Price Lists](#).
- **Fax module** - If selected, all printed faxes are charged on the FAX user account. It is available only for devices with the FAX option. Select only if the device has a fax module.

- **Printer Credentials** - The credentials are used to configure the printer(s) attached to the profile. You can override the defaults with the **Printer Credentials** in the properties of each printer.
- **Network** - Here you can add an SNMP profile: see [SNMP profiles](#), and in **KYOCERA Net Manager server address** select if the network should use the IP address or the Hostname (Hostname is used by default).

## Terminal tab

The screenshot shows the 'Terminal' tab of the configuration profile editor for 'Profile 1'. It features a tabbed interface with 'General', 'Terminal', and 'Printers' tabs. The 'Terminal' tab is active, showing a 'Terminal type' dropdown menu currently set to 'None'. Below the dropdown is a link labeled 'Install terminal package'. At the bottom, there are 'Save' and 'Cancel' buttons. A note at the bottom left states 'Fields marked by \* are mandatory.'

- **Terminal type** - Select a terminal type from the drop-down. If the type you want is missing, click **Install terminal package**. Once the package is installed, select it from the drop-down.
  - **Copier operation panel idle time**: time (in seconds) for idle logout (mandatory field).
  - **Automatic configuration**: leave this option unchecked if you want to configure the device manually.

## Printers tab

The screenshot shows the 'Printers' tab of the configuration profile editor for 'Profile 1'. It features a toolbar with 'Add', 'Edit', 'Clone', and 'Refresh' icons. A search box is visible with 'OK' and 'Cancel' buttons. The 'Printers' tab is active, showing a list of printers with 'Add' and 'Remove' buttons. The 'Name' field is visible at the bottom.

Click **Add** to add printers to the configuration profile from your printers list.

Select the added printers and click **Remove** to remove them from the configuration profile.

## Additional options

The following options become available according to the installed terminal package. It depends on brand and model if they will function on your printer:

- Login methods
- Guest Account
- Guest screen
- Local administration PIN
- Log debug messages
- Language selection
- Display numeric keypad

- ID Card reader type
- FeliCa Card Reader Parameters
- Display My Jobs action right after logging in
- Coverage accounting
- Custom options

**i** For further details about the above options, check the **KYOCERA Net Manager Embedded** guide.

## 9.4 Discovering printing devices

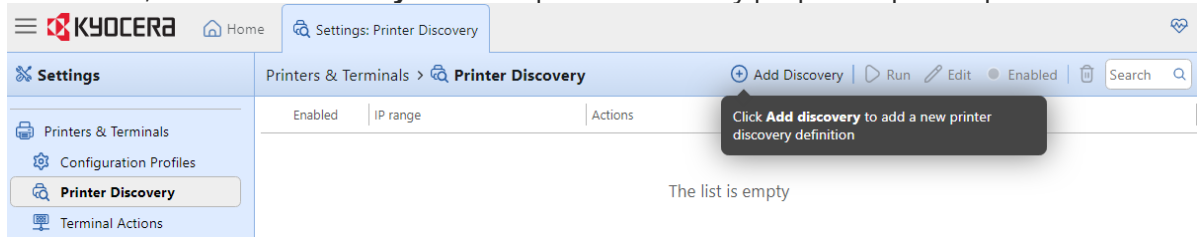
On the **Printer Discovery** settings tab, you can create and run print discoveries to search for all network printing devices within a defined IP range of your company's network. You can create multiple discoveries for different subnets.

### 9.4.1 Automated printer discovery

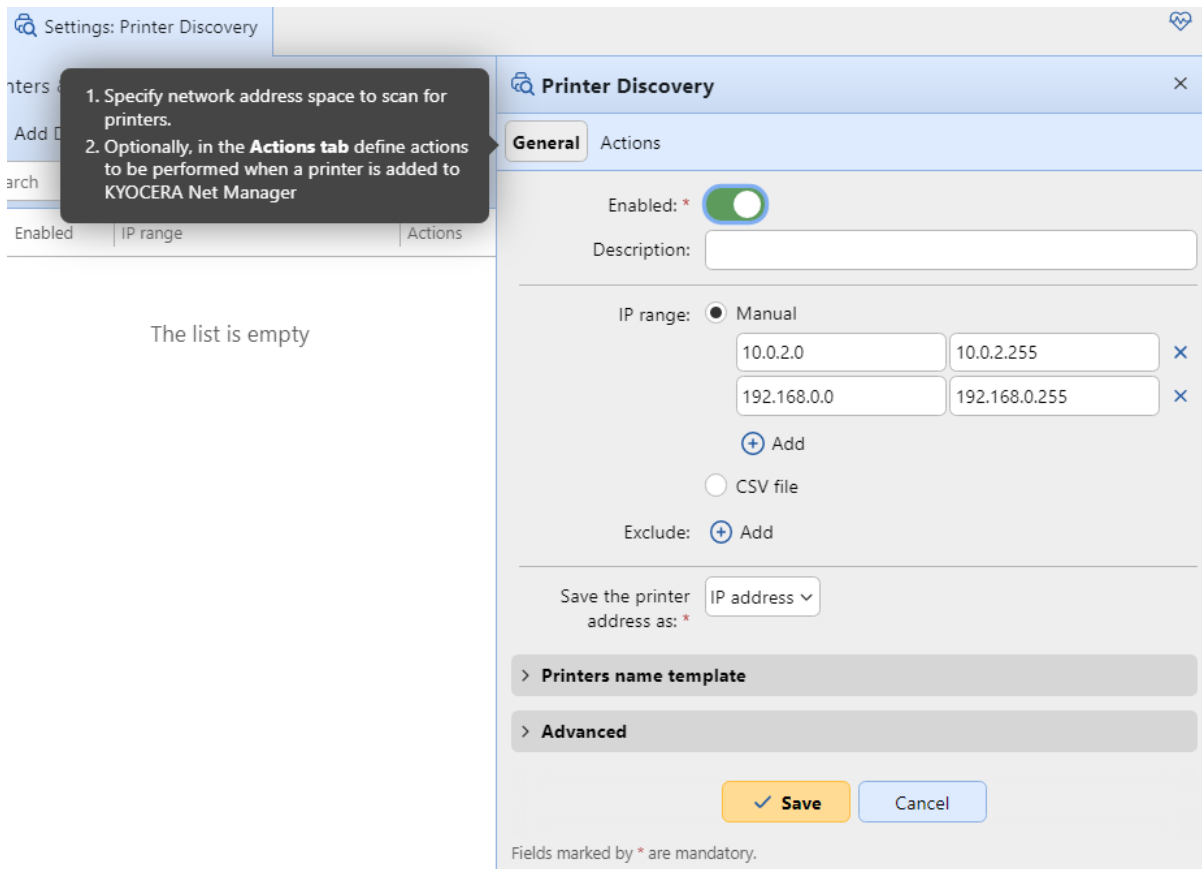
It is possible to add an **Action** to your printer discovery. In that way you can add a **Configuration profile** to your printer discovery, or select to activate the discovered printers when you **Run** the printer discovery.

To add a print discovery, do the following:

1. On the **Home** tab, click **Discover printers** in the **Quick Setup Guide** section (or go to **KYOCERA, Settings, Printer Discovery**).
2. On this tab, click **Add Discovery**. The new printer discovery properties panel opens.



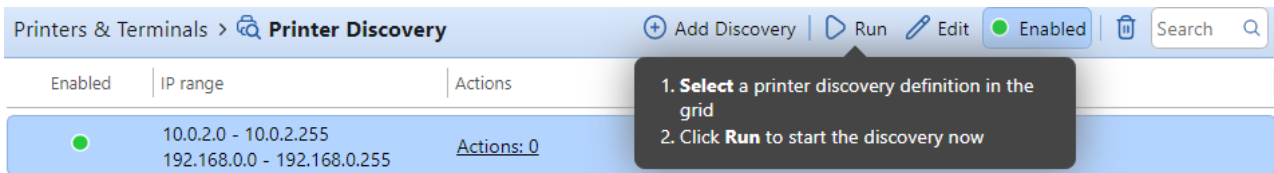
3. On the panel, you can change the **General** discovery configuration (described below).



4. You can also set special **Actions** to be performed during the discovery; see [Printer discovery actions](#).
5. Click **Save**. The new printer discovery appears on the list on the **Printer Discovery** settings tab.

## 9.4.2 To run a discovery and add printing devices:

On the **Printer Discovery** settings tab, select the printer discovery that you want to use, and then click **Run**.



The Discovering tab with a list of discovered printing devices opens. You can choose to add either all of the discovered devices or just a selection of them:

- If you want to add all discovered devices, click **+Add to KYOCERA Net Manager**, and then click **+Add all** in the drop-down. You can see the added printing devices on the **Printers** main tab.
- If you want to add selected devices, select the devices that you want to add, click **+Add to KYOCERA Net Manager**, and then click **+Add selected**. You can see the added printing devices on the **Printers** main tab.

### 9.4.3 Printer discovery general configuration

The configuration options mentioned below are basic and commonly used options of printer discovery. Options that are not mentioned here are connected with advanced **KNM** features. You can find information about those options in the **KNM** Embedded terminal manuals.

- **Enabled:** If you enable the discovery, it is included in the scheduled run of print discoveries.
- **Description:** Here you can add your own description of the discovery.
- **IP range:**
  - **KNM** automatically detects the IP range from the IP address of the server.
  - If you want to use a different IP range, you can either manually change it or import it from a CSV file.
  - You can add additional IP ranges by clicking **+Add** under IP range.
  - You can delete IP ranges by clicking the delete button.
  - You can exclude particular IP addresses by clicking **+Add** next to **Exclude**.
- **Save the printer address as:** Here you can select if you want to save the printing device address as an IP address a Hostname or a FQDN.
- **Printers name template:** You can create a name template for each of the discovered printing devices; multiple parameters can be used to compose the name of the new device:
  - **%model%:** Model of the printing device.
  - **%ipByte4%:** The last byte of the device's IP address.
  - **%sn%:** Serial number of the printing device.
  - **%id%:** ID of the printing device in the **KNM** database. If the printer name template contains the **%id%** parameter and you run discovery and add the same printer again, the name will not be updated.
  - **%hostname%:** This parameter corresponds to the hostname resolved by DNS server.
  - **%snmpHostname%:** This parameter corresponds to the hostname of the printing device set in the MIB table. The value of this parameter is obtained via SNMP protocol within the discovery of each printing device.
  - **%FQDN%:** Fully Qualified Domain Name of the printer

If you select the CSV file option, you must enter the name of the CSV file as IP address/Hostname or serial number;printer name.

- **SNMP:** Here you can select the **SNMP profile** and set the **SNMP timeout** period in milliseconds. This setting determines how long the **KNM** system waits for a response from a printing device.
- **Initiated by terminal:** Check this box when you have Java based terminals that need to be setup. Java based terminals can be installed and configured on the printer manually without a need to create a printer in **KNM** and execute Remote Setup. When an embedded terminal connects to **KYOCERA Net Manager** and there is no printer with the same IP address, **KNM** will execute a Printer Discovery whose IP address range matches the IP address of the terminal.

### 9.4.4 Printer discovery actions

The actions mentioned below are basic actions that are commonly performed during printer discoveries.

Go to the **Actions** tab and click **+Add action**. The Actions properties panel opens.

## Filter

Here you can specify the printing device models or the types of devices on which this action is performed during the discovery.

- Enter the model on which you want to perform the action. If you want to add more models, you have to separate them by commas (,).
- You can also select types of devices: color or B&W devices, and distinguish between copiers.

## Every run actions

- **Add to queue:** Here you can select one or more queues where the device will be automatically added to.
- **Set configuration profile:** Here you can select a configuration profile from the dropdown or create a new one by selecting **+Add new**. It gives you the option to install a terminal package and set the login method for the printers in the discovery.
- **Add printer to group:** Here you can select a group where the device will be automatically added.
- **Remove current groups:** If you select this option, the device is removed from all of its current groups.
- **Location:** Here you can set the location of the printing device. There are three options:
  - You can manually define the location by entering any text. Each printing device discovered or updated within this printer discovery will contain this location.

- You can automatically obtain the location via SNMP protocol by entering the **%location%** parameter. In such cases, the location is taken from the location parameter defined on the Web User Interface of each particular device discovered or updated within this printer discovery.
- You can leave this setting empty. In this case, the location of the printing device is not set/updated during the discovery. Updated printers maintain their current location and new printing devices have the location parameter undefined.

The location of a printing device is displayed and can be changed on its properties panel.

You can add multiple filters for performing discovery actions: every filter specifies the type of printers the actions will be performed on and which actions will be included.

### First run actions

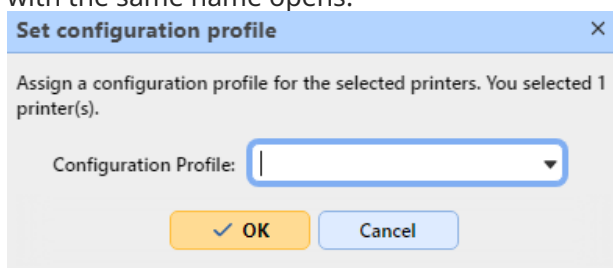
- **Activate:** Automatically activates the device if the current license allows it.
- **Create direct queue:** If you select this option, **KNM** will automatically create a direct queue for the device. The name of the queue is the same as the system name of the device. For more information about print queues, see [Queues](#).
- **Copy settings from the queue:** Here you can enter or select a direct queue from which the settings of the newly created queue are copied.
- **Print test page:** The **KNM** server will automatically send a test page to the newly created direct queue.
- **Print as:** If you select the **Print test page** option, you have to select a user account under which the test page will be printed.
- **Windows printer:** In this section you can automatically install a print port and printer driver on the **KNM** server.

## 9.5 Activating and deactivating printing devices

Unless it was automatically activated during printer discovery, a newly added device is not active in **KNM** and some of its data is not displayed (its serial number, type, counters, etc.). The next step is to activate the device. Although there is no limit to the number of printing devices you can add to the **KNM** system, you cannot activate more printing devices than your license allows.

### To activate selected printers:

1. After selecting the printers, right-click and click **Set configuration profile**. A pop-up window with the same name opens.



2. Select a profile from the drop-down and click **OK**.
3. With your selection still intact, right-click once more and select **Activate**.

### To activate all printers:

1. On the bar at the top of the **Printers** main tab, click **Actions**. The Actions drop-down appears.
2. Click **Activate all**.

### To deactivate printing devices

1. On the list of printers on the **Printers** main tab, select the devices that you want to deactivate, and then click **Actions**. The Actions drop-down appears.
2. In the drop-down, click **Deactivate**.

## 9.6 Deleting and undeleting printers

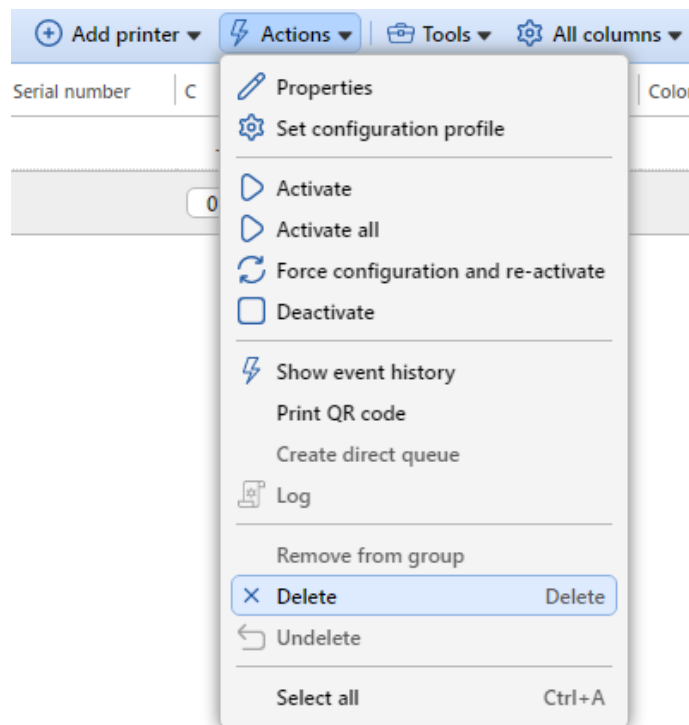
If you delete a printing device, you will not be able to use it, but its data will be permanently stored in the **KNM** database.

It is not possible to add the same device twice as its MAC address is unique and there cannot be two devices with an identical MAC address in the system. If you want to use the deleted device again, you have to undelete and reactivate it.

### 9.6.1 Deleting printers

To delete selected printing devices:

1. Select the printing devices you want to delete from the list on the **Printers** main tab.
2. Click **Actions**. The Actions drop-down appears.
3. Click **Delete**. You can find the deleted printing devices under the **Deleted** search option.

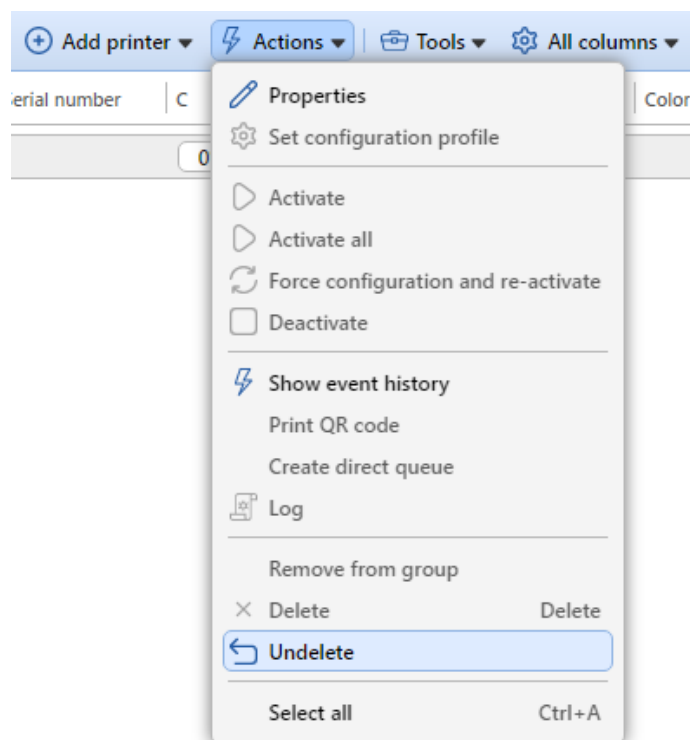


### 9.6.2 Undeleting printers

To undelete selected printing devices:

1. On the group tab on the left side of the **Printers** main tab, under **Searches**, select the **Deleted** search option. The list of deleted printing devices appears.
2. On the list, select the printing devices that you want to undelete, and then click **Actions**. The Actions drop-down appears.

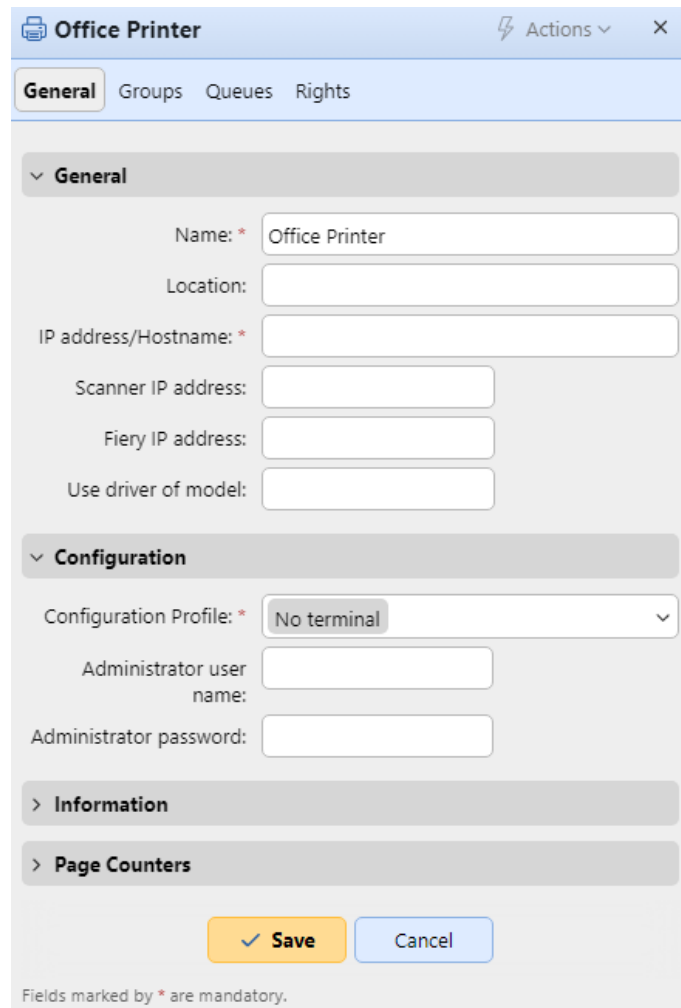
3. In the drop-down, click **Undelete**. The undeleted printing devices are not active; you have to activate them again.



## 9.7 Editing printers

Each individual printing device has its own properties panel. To open the panel, double-click the printing device on the list of printing devices on the **Printers** main tab. The properties panel opens on the right side of screen. There you can **Deactivate** it or perform some specific **Actions** on this printer.

The panel is divided into four tabs: **General**, **Groups**, **Queues** and **Rights**. On the **General** tab, you can change the printing device settings, on the **Groups** tab, you can add the device to groups, on the **Queues** tab, you can add the printing device to queues and on the **Rights** tab you can give user rights to the device.



**Office Printer** Actions

General Groups Queues Rights

**General**

Name: \* Office Printer

Location:

IP address/Hostname: \*

Scanner IP address:

Fiery IP address:

Use driver of model:

**Configuration**

Configuration Profile: \* No terminal

Administrator user name:

Administrator password:

> Information

> Page Counters

Save Cancel

Fields marked by \* are mandatory.

## 9.7.1 Printer information and settings

The settings mentioned below are basic printer settings displayed on each printer's properties panel.

### General section

- **Name\*** - Name of the printing device, any string can be used.
- **Location** - If it is required, you can specify the location of the printing device here.
- **IP address/Hostname\*** - The IP address or hostname of the printing device.
- **Scanner IP address** - The IP address of the scanner (if the device scanner has a different IP than the printing device).
- **Fiery IP address** - The IP address of the Fiery module (if the device is equipped with it).
- **Use driver of model** - Alternative model name. If your printing device is not listed in the current database of supported models, you can enter the type of supported printing device which stands close to your model. For more information, please contact your support.

### Configuration section

- **Configuration Profile** - Select a profile from the drop-down or create a new one to embed the printer by clicking **+Add new**. Then add a **Name**, install the **terminal package**, set the **Login methods** and the **Printer credentials**, as applicable to the printer.

- **Administrator user name** - Enter the admin user name. If you embed the printer separately this user name should match the one in the configuration profile.
- **Administrator password** - Enter the admin password. If you embed the printer separately this password should match the one in the configuration profile.

### Information section

- **Brand** - Information about the printing device manufacturer. It is automatically detected from the device.
- **Model** - Information about the printing device model name. It is automatically detected from the device.
- **Serial number** - The printing device serial number. It is automatically detected from the device.
- **MAC address** - The printing device MAC address. It is automatically detected from the device and it is used as a unique identification of the device in the **KNM** system. Therefore, only one device with a particular MAC address can be activated.
- **Asset number** - Additional option for identification of the printing device.
- **Contact** - Contact info of the person responsible for the printing device maintenance.
- **Purchase date** - Purchase date of the printing device.
- **Notes** - Additional information about the printing device.

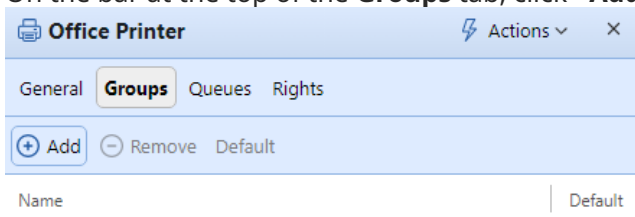
### Page Counters section

- **Black & White Print** - Total amount of B&W pages printed on the device.
- **Color Print** - Total amount of color pages printed on the device.
- **Black & White Copy** - Total amount of B&W pages copied on the device.
- **Color Copy** - Total amount of color pages copied on the device.
- **Single color copy** - Total amount of single color pages copied on the device.
- **Scanner** - Total amount of pages scanned on the device.
- **Fax** - Total amount of incoming faxes printed on the device
- **Print total counter adjust for load balancing** - The entered value is added to the printed pages counter to evenly spread print load between devices in tandem queues.

## 9.7.2 Adding/removing printers to groups

### To add a printer to a group:

1. On the bar at the top of the **Groups** tab, click **+Add**. The Select group dialog box appears.



The list is empty

2. In the **Select group** dialog box, select the groups, and then click **OK**.

Printers can also be added to a group on the **Printers** main tab using drag and drop. Drag the printer and drop it on the group icon on the groups tab on the left side of the screen.

### To remove a printer from a group:

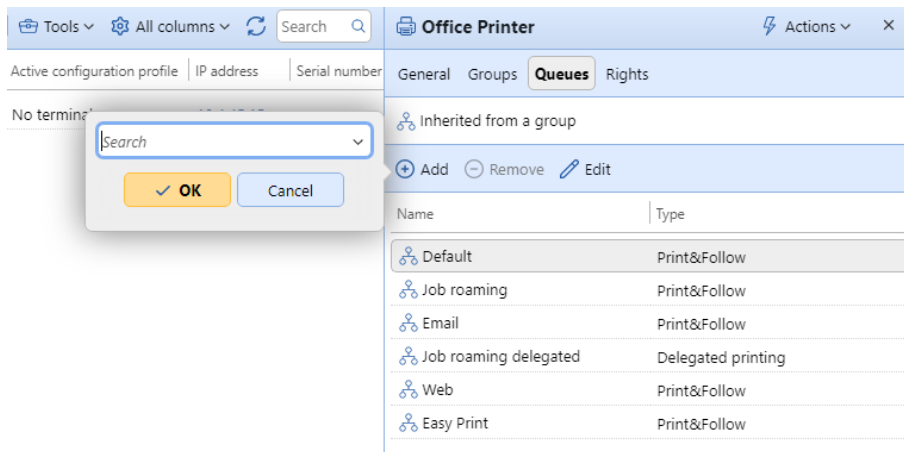
On the bar at the top of the **Groups** tab, click **-Remove**. The group disappears from the **Groups** tab.

To remove selected printing devices from a group on the **Printers** main tab, select the group there, select the printing devices that you want to remove, click **Actions**, and then click **Remove from group** in the **Actions** drop-down (or right-click the printer and click **Remove from group**).

### 9.7.3 Adding/removing printers to queues

**To add a printer to a queue:**

1. On the bar at the top of the **Queues** tab, click **+Add**. A search box appears to the left.
2. In the search box, find the queue where you want to add the device to, and then click **OK**.



**To remove a printer from a queue:**

On the bar at the top of the **Queues** tab, click **-Remove**. The queue disappears from the **Queues** tab.

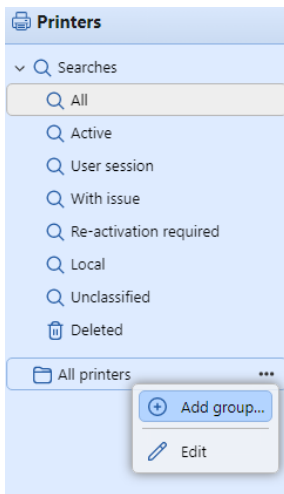
## 9.8 Printer groups

All printing devices in **KNM** can be divided into groups based on their location, model, vendor, category, etc.

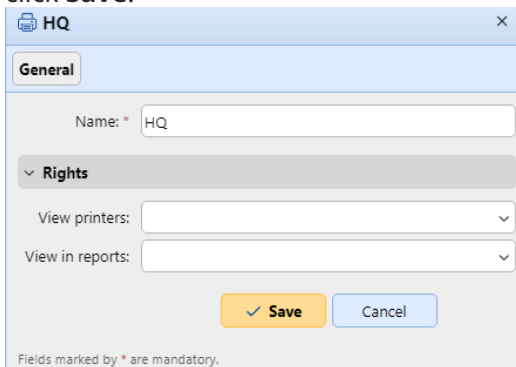
On the **Printers** main tab, you can create new groups of printing devices. There are a number of **KNM** functions where groups are used, for example, they can be assigned to particular print queues (see [Queues](#)), users can be given rights and restrictions concerning particular groups (see [Rights](#)) and reports can be set about particular groups only (see [Reports](#)).

### 9.8.1 Creating printer groups

1. On the left side of the **Printers** main tab, right-click **All printers**, and then click **+Add group** on the shortcut menu. The new group properties panel opens on the right side of the screen.



2. On the panel, enter a name of the new group, give rights to users or groups of users, and then click **Save**.



### Printer group rights:

- **View printers:** The right to see and manage printers from this group on the web user interface.
- **View in reports:** The right to see this group of printers in reports.

**i** If you want the new group to be placed under an already existing group, select the parent group, and then click **+Add Group** (or right-click the parent group, and then click **+Add Group** on the shortcut menu).

## 9.8.2 Deleting printer groups

To delete a group of printing devices:

On the group tab on the left side of the **Printers** main tab, right-click the group you want to delete, and then click **Delete** on the shortcut menu.

## 9.9 Exporting and importing printers

On the **Printers** main tab, you can export the list of printing devices with all the information that are displayed on the current view to a CSV file.

To export the list of printing devices:

1. On the toolbar at the top of the **Printers** main tab, click **Tools**; the tools drop-down box appears.
2. On the drop-down box, click **Export**.

The supported columns in the export are:

printer, location, IPAddress, scannerIP, terminalID, slaveTerminalID, enforcedModel, assetNumber, contact, purchaseDate, Model, Serial number, MAC, B&W print, Color print, B&W copies, Color copies, Scans, Fax  
 C, M, Y, K, A4 paper, A3 paper, A5 paper, B4 paper, B5 paper, Other paper, Folio paper, Ledger paper, Legal paper, Letter paper, Statement paper, Rest of paper, Print color pages (L1), Print color pages (L2), Print color pages (L3), Copy color pages (L1), Copy color pages (L2), Copy color pages (L3).

You can also import a list of printers from a CSV file containing at least the printer's name and IP address.

The supported columns for the import are:

printer, location, IPAddress, scannerIP, terminalID, enforcedModel, assetNumber, contact, Serial number, MAC.

The CSV's header should be **printer;IPAddress**, as seen in the below example:

	A	B	C	D	E	F	G
1	printer	location	IPAddress	scannerIP	terminalID	assetNumber	contact
2	Test		1.1.1.1				
3							

To import the list of printing devices:

1. On the toolbar at the top of the **Printers** main tab, click **Tools**; the tools drop-down box appears.
2. On the drop-down box, click **Import**.
3. **Browse** for your CSV file and click **OK**.

Your printers are now imported and visible in the **Printers** tab.

## 9.10 Monitoring network printers in offline mode

The usual way of communication between the **KNM** system and a printing device is via SNMP protocol. In case this method cannot be used, for example if the printing device does not support the SNMP protocol, you can use the **KNM** parser to monitor the number of pages and other basic properties of jobs sent to be printed on a printing device. This accounting method is referred to as **Offline accounting**.

A disadvantage of the offline accounting feature is its inaccuracy. Due to the fact that the communication of **KNM** and the printing device is one-sided and restricted to sending print data to the device, it is not possible to check if the data is actually printed. Therefore, **KNM** charges the print job based on the information from the job parser received after the job is sent to the printing device. Even if the print job is canceled halfway through the print, it is charged as a whole.

To enable the offline accounting mode of a printing device:

1. On the **Printers** main tab, double-click the printing device to open its properties panel.
2. On the panel, in the **Use driver of model:** text box, enter the value *offline*, and then click **Save**.

Fiery IP address:	<input type="text"/>
Use driver of model:	<input type="text" value="offline"/>


Before enabling the offline accounting mode, deactivate the printing device. The **Use driver of model:** setting cannot be changed on activated printing devices. Once you enable the offline accounting mode, reactivate the printing device. See [Activating and deactivating printing devices](#) for more information.

## 9.11 Monitoring local printers

Besides [monitoring network printers](#), **KNM** is able to monitor the number of printed pages on devices connected locally, via a parallel port or a USB port. In such cases, the number of printed pages is extracted from the print spooler as it is being processed by the print driver.

To extract the data provided by the spooler, you need to install the **KYOCERA Net Manager Desktop Client for Windows** application to all the computers that you print from to **KNM**, and set up **Local Print Monitoring** there. All jobs sent to selected types of ports will be detected from the print spooler.

A disadvantage of the local print monitoring feature is its inaccuracy. As the communication of **KNM** and the local printing device is one-sided and restricted to sending print data to the device, it is not possible to check if the data is actually printed. Therefore, **KNM** charges the number of pages extracted from the spooler when they are sent to the printing device. Even if the print job is canceled halfway through the print, it is charged as a whole.

 Local printing devices monitoring is available only on computers with MS Windows.

### 9.11.1 Accounting on local printers

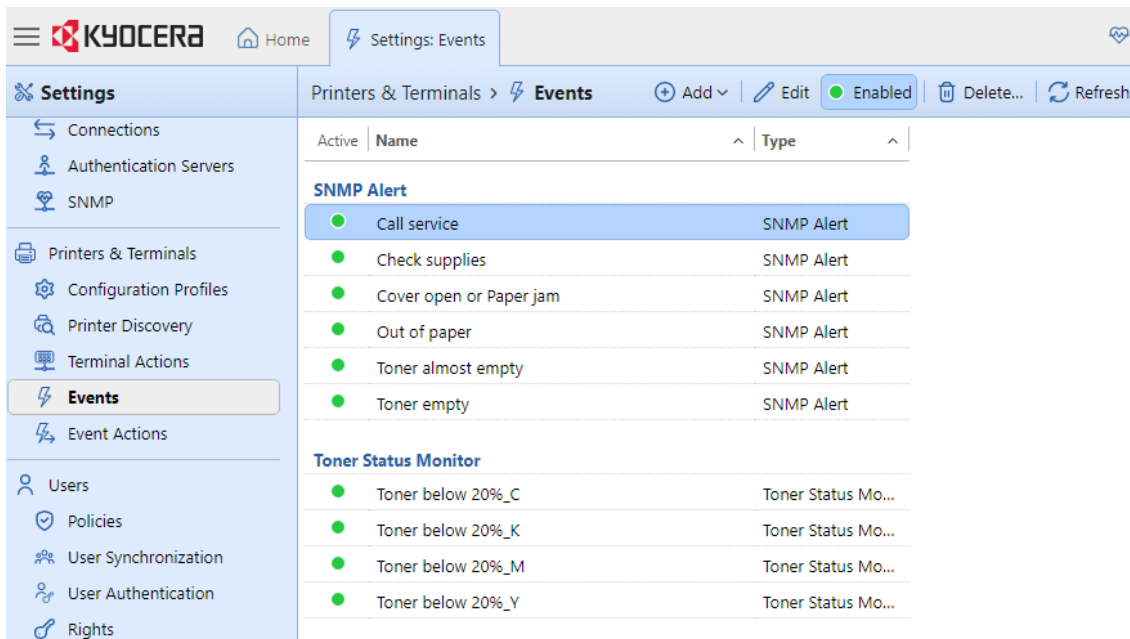
After a print job is sent to one of the local printing devices, the number of pages and other information about the print job are saved to the **KNM Desktop Client** folder of the particular registry file. Once the connection with the **KNM** server is established, all the information is automatically transferred to the **KNM** server and deleted from the registry. Therefore, it is not necessary to be permanently connected to the **KNM** Server online.

Once the server is connected and data is sent to the server, information about the job appear in an **Info** entry in the **KNM** log. Each entry contains information about the user who printed, the printing device that the user printed on and the number of printed pages. The **KNM** server automatically creates a new local type printing device. Its name has the following form: *printer@computer*.

An appropriate price list can be set for local printing devices. Therefore, they can be included in the monetary reports. If the user that prints on the local printing device already exists, their prints are simply assigned to them. Otherwise, the job is accounted to the **\*unauthenticated user**.

## 9.12 Printer Events

**Printer Events** are customizable actions initiated by specific events, which are based on printing devices alerts. The alerts are set up by first defining the events, and then selecting and setting the actions triggered by these events. The actions are of two kinds: as a response to an event on a printing device, **KNM** can send an email notification to one or more persons, or it can terminate the user session on the embedded terminal of the device.



The events can be set on the Printer **Events** settings tab and the event actions on the **Event Actions** settings tab.

**i** A report with the Event History type can be created, which informs about all events on selected printers or groups of printers during a certain period of time.

### 9.12.1 Events

There are ten predefined alerts on the **Events** settings tab. These correspond to common situations, such as empty toner or a printer out of paper, or to states of printing devices that require particular actions, such as technical support or supply check. They are triggered by the following states of a printing device:

- **Call service** — The printing device requires authorized technical service.
- **Check supplies** — Consumables of the printing device need to be checked.
- **Cover open or Paper jam** — Either a device cover is open or a paper is jammed.
- **Out of paper** — The printing device is out of paper.
- **Toner almost empty** — One or more toners on the device are almost empty.
- **Toner empty** — One or more toners on the device are empty.
- **Toner below 20%\_C** — The Cyan toner on the device is below 20%.
- **Toner below 20%\_K** — The Black toner on the device is below 20%.
- **Toner below 20%\_M** — The Magenta toner on the device is below 20%.
- **Toner below 20%\_Y** — The Yellow toner on the device is below 20%.

#### Changing the toner level to be monitored

The toner level to be monitored is set to 20% by default but can be easily changed following the instructions below:

1. On the alerts list on the **Events** tab, double-click the alert. The properties panel opens on the right side of the screen.

2. Change the value in the **Level below** field (in %).
3. Change the name of the alert according to the new monitored level.

## Creating new events

To create a new event, click **+Add** and select the type of event to be created.

Available event types:

- **SNMP alert** - The SNMP alert event occurs when at least one of the predefined filter passes. If the event has no filters defined, it's never open. You can define the following filters: *Code from, Code to, Severity, Training, Group, Group Index, Brand, Model*.
- **Toner Status Monitor** - The event occurs when the toner level decreases below a predefined threshold. When the toner level rises again to or above the threshold, the event is closed. The monitored toner (*Black toner, Color toner, Any toner*) can be configured.
- **Total Counter Increase** - The event monitors when the print and copy counters on a device repeatedly reach a certain value. For each such event, two values need to be specified:
  - which type of counters should be monitored by this event; possible values are *Print & Copy total, Print & Copy mono, Print & Copy color*.
  - which repeatedly reached values should be monitored - this means that a value X needs to be specified and whenever the counters on a device reach a value that is evenly divisible by X, the actions are triggered

A properties panel opens to the right side of the screen. Fill in the mandatory information and click **Save**.

## 9.12.2 Event Actions

The two available actions are sending an email and logging the user out of an embedded terminal. Each action can be either applied to all printers, or it can be restricted to specific groups of printers.

There are four predefined event actions: **Toner below 20%\_C, Toner below 20%\_M, Toner below 20%\_Y, Toner below 20%\_K**. These actions apply to all printers and respond to the **Toner below 20%\_C, Toner below 20%\_M, Toner below 20%\_Y, Toner below 20%\_K** events.

Active	Name	Type	Event	Printer group	Delay
<input type="radio"/>	Toner below 20%_C	Send email	Toner below 20%_C	All printers	0 min
<input type="radio"/>	Toner below 20%_M	Send email	Toner below 20%_M	All printers	0 min
<input type="radio"/>	Toner below 20%_Y	Send email	Toner below 20%_Y	All printers	0 min
<input type="radio"/>	Toner below 20%_K	Send email	Toner below 20%_K	All printers	0 min

**To create a new event action:**

1. Go to **KYOCERA, Settings, Event Actions** and click on **+Add action**. Select the type of action from the drop-down: **+Send email** or **Log out user**.
2. On the panel, set all the options of the action and click **Save**.

## Setting event actions

The parameters described below belong to the **Send email** and **Log out user** event actions.

- **Enabled** - Enable or disable the event action.
- **Name** - Add a name for the action
- **Event** - Select the event that will initiate this action.
- **Printer Group** - Select the printer group(s) that the action applies to from the list.
- **Delay** - Set a time period after which the email is sent (in minutes).
- **Recipient** - Enter the email recipient(s). You can use the `%PRN.CONTACT%` parameter to send the email to the device's contacts.
- **Subject + Message** - Enter the email's subject and message. You can use the following parameters
  - `%PRN.NAME%` — name of the printer
  - `%PRN.IP_ADDRESS%` — IP address of the printer
  - `%PRN.SERIAL_NUMBER%` — serial number of the printer
  - `%PRN.MODEL%` — model name of the printer
  - `%PRN.PRINTER_MONO%` — counter of B&W pages printed on the device
  - `%PRN.PRINTER_COLOR%` — counter of color pages printed on the device
  - `%PRN.COPIER_MONO%` — counter of B&W pages copied on the device
  - `%PRN.COPIER_COLOR%` — counter of color pages copied on the device
  - `%PRN.SCANNER%` — counter of scanned pages sent to email or folder
  - `%SUPPLY.INFO%` — all of the toner supply identifiers separated by semicolon
  - `%TONER_C.LEVEL%` — C toner level in percentage
  - `%TONER_M.LEVEL%` — M toner level in percentage
  - `%TONER_Y.LEVEL%` — Y toner level in percentage
  - `%TONER_K.LEVEL%` — K toner level in percentage
  - `%PRN.ASSET_NO%` - the asset number of the printer
  - `%EVENT.TONER.LEVEL%` - toner level information
  - `%EVENT.TONER.INFO%` - toner information

## Event History

The **KNM** administrator can view the **Event History** on the **KNM** Web Administrator interface, in **KYOCERA, Event History**.

The screenshot shows the 'Event History' interface. On the left, there are search filters for 'Event', 'Created', 'Resolved', and 'Printer'. The main area displays a table with columns: Printer, Event, Type, Created, Resolved, and Event details. The table lists several events, including 'Check supplies', 'Out of paper', and 'Toner almost empty'.

Printer	Event	Type	Created	Resolved	Event details
<b>Check supplies</b>					
	Check supplies	SNMP Alert	10/02/2022 09:33:30	10/02/2022 09:37:21	⚠ Marker: Toner Almost Empty • Marker: Supplies
	Check supplies	SNMP Alert	10/02/2022 09:45:26	-	⚠ Marker: Toner Almost Empty • Marker: Supplies
<b>Out of paper</b>					
ECOSYS P8060cdn_5	Out of paper	SNMP Alert	10/02/2022 09:33:25	-	⚠ Input: Media supply empty • Input
ECOSYS M3540dn_7	Out of paper	SNMP Alert	10/02/2022 09:33:25	-	⚠ Input: Media supply empty • Input
	Out of paper	SNMP Alert	10/02/2022 09:33:30	-	⚠ Input: Media supply empty • Input
<b>Toner almost empty</b>					
	Toner almost empty	SNMP Alert	10/02/2022 09:33:30	10/02/2022 09:37:21	⚠ Marker: Toner Almost Empty • Marker: Supplies
	Toner almost empty	SNMP Alert	10/02/2022 09:45:26	-	⚠ Marker: Toner Almost Empty • Marker: Supplies
<b>Toner below 20%_K</b>					
ECOSYS M3540dn_7	Toner below 20%_K	Toner Status Mon...	10/02/2022 09:38:51	-	19%

On the left side, there are the *Event*, *Created*, *Resolved*, and *Printer* search parameters that can be set to view specific events.

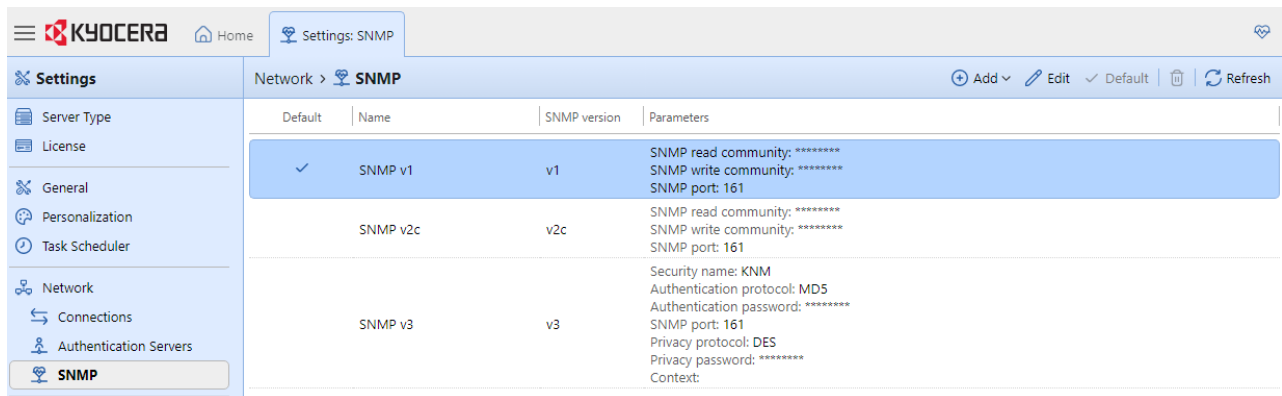
In **Tools - Save as CSV**, the Event History can be exported.

## 9.13 SNMP profiles

By default, the SNMP v1 protocol is used for communication with printing devices in the **KYOCERA Net Manager** system. Instead of it, you can use the more recent SNMP v2c protocol or the SNMP v3 protocol, which significantly increases the communication security with a printing device.

Multiple SNMP profiles can be created in **KNM**, and each printing device can be assigned one of the profiles. This way, you can have one profile for all printing devices with a particular SNMP configuration.

The default SNMP profile can be changed. To make any SNMP profile the default one, select it on the **SNMP** settings tab, and then click **Default** on the bar at the top of the tab (or right-click the profile, and then click **Default** on the shortcut menu).

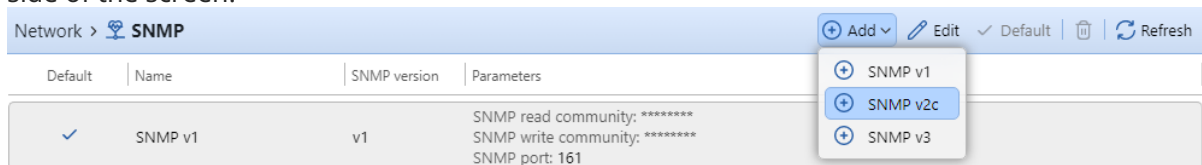


### 9.13.1 Adding and editing SNMP v1 and v2c profiles

With the SNMP v1 and v2c protocols, a single string called "*SNMP Community string*" is used to allow access to the device. Only two parameters need to be set in **KNM**: the **SNMP read community** parameter and the **SNMP write community** parameter. Their values have to match the values of their counterparts on the printer's Web User Interface (Read Community, Write Community).

#### To add a new SNMP v1 or v2c profile:

1. On the **KNM** Web Admin Interface, open the **SNMP** settings tab (**KYOCERA, Settings, SNMP**).
2. On the bar at the top of the **SNMP** tab, click **+Add SNMP profile**, and then click **+SNMP v1** or **+SNMP v2c** on the shortcut menu. The new SNMP profile properties panel opens on the right side of the screen.

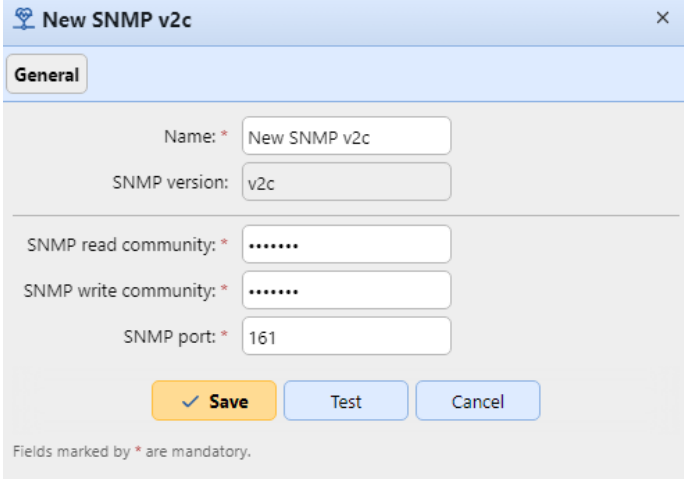


3. On the panel, enter the name of the profile, set the parameters, and then click **Save**. The new profile is displayed on the list on the SNMP settings tab.

#### To open and edit a SNMP v1 or v2c profile

1. To open the SNMP profile properties panel, select the profile on the **SNMP** settings tab, and then click **Edit** (or right-click the profile, and then click **Edit** on the shortcut menu, or double-click on the profile). The profile's properties panel opens on the right side of the screen.

2. On the SNMP profile properties panel, you can change the profile's name and enter the values of the **SNMP read community** parameter and the **SNMP write community** parameter, according to the values that are set on the printer's Web User Interface.
3. Click **Save** to submit and store the changes.



### 9.13.2 Adding and editing SNMP v3 profiles

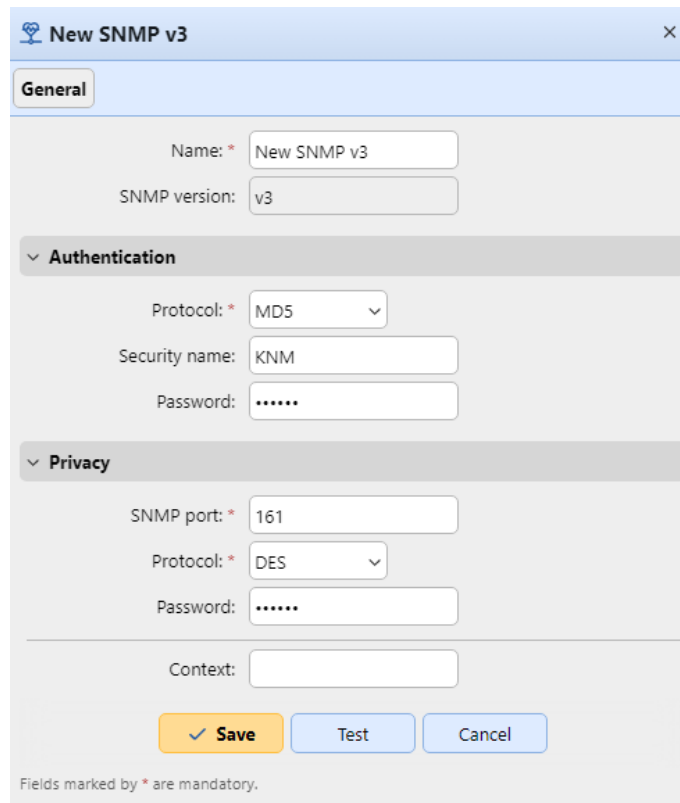
The SNMP v3 protocol contains additional elements of security, such as authentication and encryption. Each of these elements is set on the printing device and needs to be accordingly set in **KNM**.

#### To add a new SNMP v3 profile:

1. On the **KNM** Web Interface, open the **SNMP** settings tab. (**KYOCERA, Settings, SNMP**).
2. On the bar at the top of the **SNMP** tab, click **+Add SNMP profile**, and then click **+SNMP v3** on the shortcut menu. The new SNMP profile's properties panel opens on the right side of screen.
3. On the panel, enter the name of the profile, set the parameters, and then click **Save**. The new profile is displayed on the list on the **SNMP** tab.

#### To open and edit a SNMP v3 profile:

1. To open the SNMP profile properties panel, select the profile on the **SNMP** settings tab, and then click **Edit** (or right-click on the profile, and then click **Edit** on the shortcut menu). The properties panel opens on the right side of the screen.
2. On the SNMP profile properties panel, you can change the profile's name, set its authentication parameters, its privacy parameters and eventually enter a context name. The values of all of the parameters have to match the values that are set on the printer's Web User Interface.
3. Click **Save** to submit and store the changes.



**New SNMP v3**

**General**

Name: \* New SNMP v3

SNMP version: v3

**Authentication**

Protocol: \* MD5

Security name: KNM

Password: .....

**Privacy**

SNMP port: \* 161

Protocol: \* DES

Password: .....

Context:

✓ Save Test Cancel

Fields marked by \* are mandatory.

### 9.13.3 Attaching SNMP profiles to printers

1. On the **KNM** Web Administrator Interface, open the **Printers** main tab (**KYOCERA, Printers**).
2. On the tab, select the printing device, click **Actions**, and then click **Properties**. The printing device's properties panel opens on the right side of the screen.
3. On the panel, go to the **Configuration** section.
4. Select a **Configuration Profile** that has the SNMP profile attached to it. In case of doubt, go to **KYOCERA, Settings, Configuration Profiles** and check the profiles.

Printers & Terminals > Configuration Profiles

Name	Printers	Configuration Profile
Profile 1	⚠ No printer	Price List: - Terminal type: None Automatic configuration: Yes <u>SNMP profile: SNMP v3</u> KYOCERA Net Manager server address: Hostname

## 10 Users

---

This topic discusses one of the key **KNM** functions: setting and management of users (user accounts). It covers the following subjects:

- Overview, registration, adding, importing, synchronizing and deleting users: [List of users](#), [Automatic user registration](#), [Add users manually](#), [Deleting and undeleting users](#)
- PIN generation: [Generating PIN](#)
- Individual user settings: [Editing user accounts](#), [Enable user profile editing](#), [User Groups](#), [Exporting users](#)
- Job policies concerning users and printers: [Policies](#)
- Special administrative rights: [Rights](#)
- Securing the personal data of **KNM** users, anonymization: [Securing KNM users personal data](#)
- User synchronization from LDAP, CSV files, or Azure Active Directory, together with manual and scheduled runs of synchronizations: [User import and synchronization](#).
- User authentication using an LDAP or Radius server: [Using External Authentication Servers](#).
- Identifying the owner of a sent job: [Detecting job owners](#).

### 10.1 List of users

On the **Users** main tab, you can see users and information about them. With the **All users** search option selected, you see a list of all the users that are currently in the system. System users are hidden from the list of users in the **KNM** web UI.

Apart from this search option, you can also choose from:

- **Unclassified** - select to display only the users that do not belong to any group
- **Managers** - select to display only group managers
- **Locked** - select to display users whose accounts have been locked
- **Deleted** - select to display only deleted users

#### Default system users

The database of every installation of **KNM** contains five default system users. These users are used for administration of the **KNM** system and cannot be deleted.

1. **\*admin** - This is the **KNM** administrator account. It is used for administration of the **KNM** system on the Web Administrator User Interface.
2. **\*api** - **KNM** uses this account to connect to external applications.
3. **\*fax** - All printed faxes are charged to this account.
4. **\*unauthenticated** - If there are any printed, copied or scanned pages that for some reason cannot be assigned to concrete users, they are charged to this account. This can happen, for example, if the print server is not available and users print in an emergency, offline mode on a printing device. It can also happen if someone prints directly on a printing device, bypassing the **KNM** system. In such cases, you might need to check the printing device security settings.
5. **\*system** - All the actions performed by the **KNM** system are charged to the **\*system** user.

### 10.2 Automatic user registration

Usually, only registered users can access the **KNM** system and use the services there.

However, in some exceptional cases, it might be useful to enable automatic registration and thus provide all users with access to **KNM**. Users can be automatically registered to the **KNM** system in two ways:

- either they can register themselves on the **KNM** Web User Interface or on an embedded terminal,
- or they can be automatically registered after sending a job to **KNM** from their computer or via email as an attachment.

On the **Users** settings tab, under **New user registration**, you can enable and disable these options, and for each option, you can select one or more groups where the registered users will be added to.

▼ **New user registration**

Register by swiping an unknown ID card:  Add to group:

Register in the Web user interface:  Add to group:

Register by receiving a job via LPR/IPPS/RAW protocols:  Add to group:

Register by receiving a job via email:  Add to group:

Register by receiving local job meta data (LPM):  Add to group:

▶ **Email for new registered users**

### Register by swiping an unknown ID card

With this option selected, users can register themselves at a printing device with an embedded terminal by swiping an unknown ID card at the card reader.

After they swipe the card, a new account called **anonymX** (anonym1, anonym2, etc.) is created and they are automatically logged in to the terminal. There, they can edit the account using the **Edit Account** embedded action. If the **Enable user profile editing** option is enabled on the **Users** settings tab, under general, they can change their full name, email and language; otherwise they can only change the language.

### Register on the **KNM** Web User Interface

With this option selected, users can create accounts on the **KNM** Web User Interface.

1. Click **New Account** at the bottom-left corner of the **KNM** login window. The New Account registration widget opens.
2. Enter a name and email address.
3. Click **Register**. The newly created account is given the same name as the email address entered.

After creating the account, the **New account created** message box appears. After clicking **Show PIN** there, the user can see their user name and password.

The user receives an email with information about the new account. The default message contains their user name and PIN. You can change the message in the **Email for new registered users** section.

### Register by receiving a job via LPR/IPPS/RAW protocol

With this option selected, users can register themselves by sending a print job from their computer via the LPR, IPPS or RAW protocol.

After a user sends the job, **KNM** detects their name according to the currently set method of user detection, checks whether the user is already registered, and in case of an unknown sender user

name, it creates a new account. The newly created account is given the same name as the job sender name detected this way.

The user receives an email with information about the new account. The default message contains the user name and PIN. You can change the message in the **Email for new registered users** section.

### Register by receiving a job via email

With this option selected, users can register themselves by sending an email with an attached printable document. For more information about sending print jobs via email, see [Printing from email and from the KNM Web UI](#).

The name of the newly created account is the email address that the email was sent from.

The user receives an email reply with information about the new account. The default message contains the user name and PIN. You can change the message in the **Email for new registered users** section.

### Email for new registered users

Here you can change the email body that informs the new users about their account.

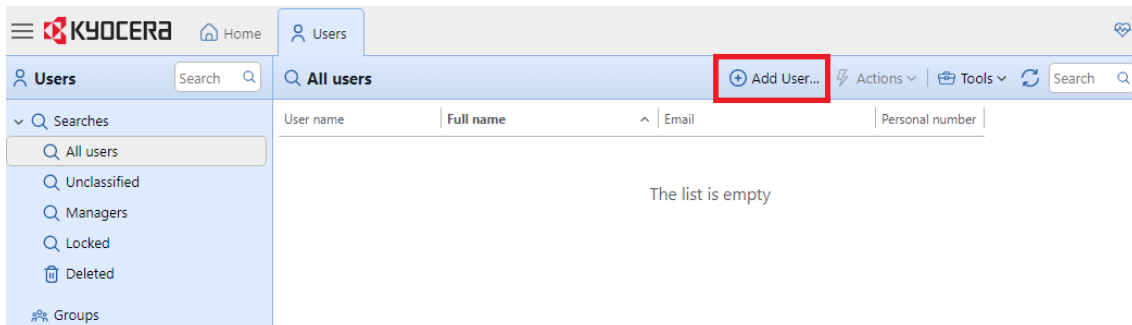
The values of the **%pin%**, **%username%** and the **%realname%** parameters are the user's PIN, user name and real name.

By clicking **Revert values**, you can reset the email body to the default.

## 10.3 Add users manually

To manually add a new user, follow these steps:

1. On the **Users** main tab, click **+Add User**. The properties panel of the new user opens on the right side of the screen.
2. On the panel, enter the username and full name of the user, and eventually set other data of the user account (see [User information and settings](#)), and then click **Save**.



## 10.4 Deleting and undeleting users

When you delete a user, they are removed from all groups (including **All users**) and are marked **Deleted**. They are not completely removed from the **KNM** database and can be undeleted.

### Deleting users

To delete a user:

1. On the **Users** main tab, select the users that you want to delete, and then click **Actions**. The **Actions** drop-down box appears.

2. In the **Actions** drop-down box, click **Delete**. You can find the deleted users under the **Deleted** search option.

## Undeleting users

To undelete a user:

1. On the **Users** main tab, under searches, select the **Deleted** search option. The list of deleted users appears.
2. On the list, select the users that you want to undelete, and then click **Actions**. The **Actions** drop-down box appears.
3. Click **Undelete**.

## 10.5 Editing user accounts

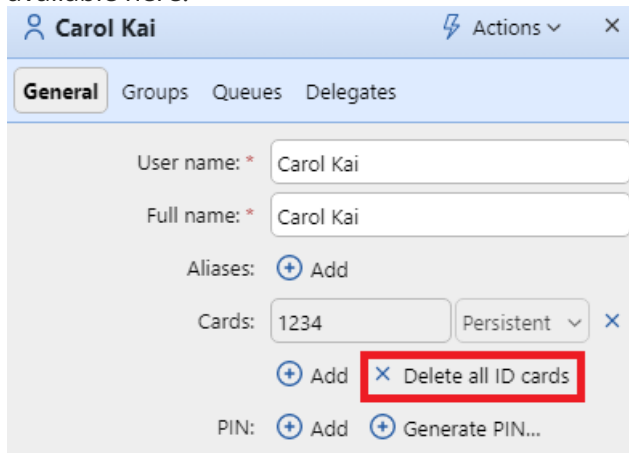
Each individual user has their own properties panel. To open the panel, double-click the user on the list on the **Users** main tab (or right-click the user, and then click **Edit**). The properties panel opens on the right side of the screen. The panel is divided into four tabs: **General**, **Groups**, **Queues**, and **Delegates**. If Credit accounting is enabled for the user, the **Credit** tab is also available.

The screenshot shows a user properties panel for 'Carol Kai'. The 'General' tab is active, displaying various user information fields. Mandatory fields are marked with an asterisk (\*). The 'Cards' field includes a dropdown menu set to 'Persistent'. The 'Use authentication server' checkbox is unchecked. The 'Authentication server' is set to 'None'. The 'Notes' and 'Synchronization source' fields are empty. At the bottom, there are 'Save' and 'Cancel' buttons. A footer note states: 'Fields marked by \* are mandatory.'

### 10.5.1 User information and settings

- **User name** - Here you can enter or change the user name. This entry is mandatory. It is unique and is used to identify the user. It is compared to the parameter obtained from the **User detection method**. For more information, see [User detection methods](#).
- **Alias** - In addition to their user name, each user can have a number of aliases. **KNM** treats the aliases as alternative user names.

- **Card** - Here you can set the number of the user's identification card. If the **Enable deleting all ID cards** option is enabled in **KYOCERA, Settings, Users**, the **Delete all ID cards** button is available here.

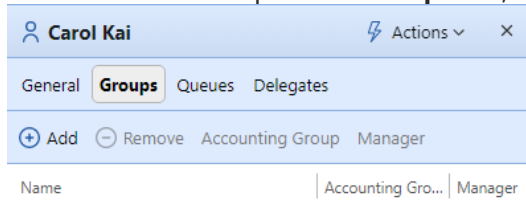


- **PIN** - Here you can manually create or automatically generate new PIN code for the user and remove existing ones. An unlimited number of PINs can be added.
- **Full name** - Here you can enter or change the user's full name. This entry is mandatory.
- **Email** - Here you can enter or change the user's email.
- **Phone** - Here you can set the user's phone number
- **Personal number** - The personal number can be used as the user ID in **KNM**. The primary ID is the **user name** property.
- **Default language** - Here you can select the language of the user's sessions on **KNM** embedded terminals.
- **User's storage** - Here you can set the folder or email, where scanned documents are saved. For more information, see [Scan to Me](#).
- **Use authentication server** - If you select this option, an LDAP server is used for the user authentication. The user uses their LDAP credentials to authenticate to **KNM** instead of having a password set in **KNM**. Select the domain for the authentication on the setting below.
- **Authentication server** - Here you can select the server for user authentication.

## 10.5.2 Adding/removing users from groups

To add a user to a group on the user properties panel, in the **Groups** tab:

1. On the bar at the top of the **Groups** tab, click **+Add**. The Select group dialog box appears.



2. In the Select group dialog box, select the groups where you want to add the user to.
3. Click **OK**.

A user can also be added to a group on the **Users** main tab using drag and drop. Drag the user and drop it on the group icon on the groups tab on the left side of the screen.

### Default group and Group manager options

On the bar at the top of the **Groups** tab, you can see two options: **Accounting** and **Manager**.

The **Accounting** group is the group where the user is counted in reports (see [Reports](#)) and it is set to every user by default.

If you make a user the **Manager** of a certain group, the user can see jobs and reports of all the users from the group. If this group contains subgroups, the user inherits the Manager role also for all these subgroups. To make the user a manager of a group, select the group and click **Manager**.

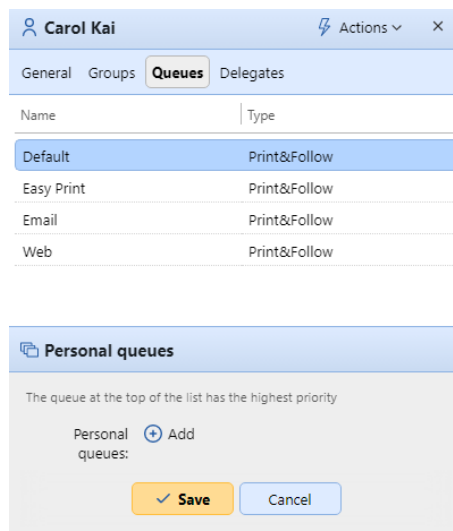
#### To remove a user from a group:

On the bar at the top of the **Groups** tab, click **-Remove**. The group disappears from the **Groups** tab.

To remove selected users from a group on the **Users** main tab, select the group there, select the users that you want to remove, click **Actions**, and then click **Remove from group** in the **Actions** drop-down box.

### 10.5.3 Queues tab overview

On the **Queues** tab, you can see all the queues where the user can send jobs to.



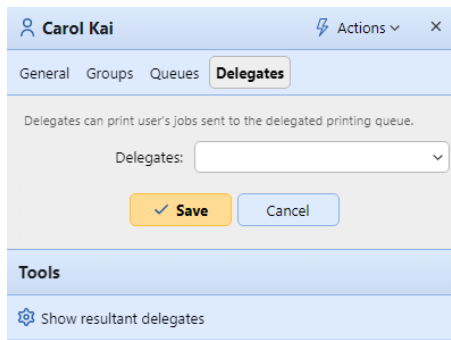
### 10.5.4 Selecting user delegates

On the **Delegates** tab, you can select delegates (users or groups) who are able to print all of the delegating user jobs sent to a **Delegate** printing type of queue. The delegate will see the jobs on the embedded terminal. The print jobs are displayed in the form: *(Sending user\*\*Name of the print job)*. For more information about the delegate printing feature, see [Delegated printing](#).

Users need to have rights to a delegate printing type queue to be able to select delegates.

#### To select delegates:

On the bar at the top of the **Delegates** tab, in the **Delegates** combo box, enter the user (or the group of users), and then click **Save**. This way, you can add multiple users (or groups of users).



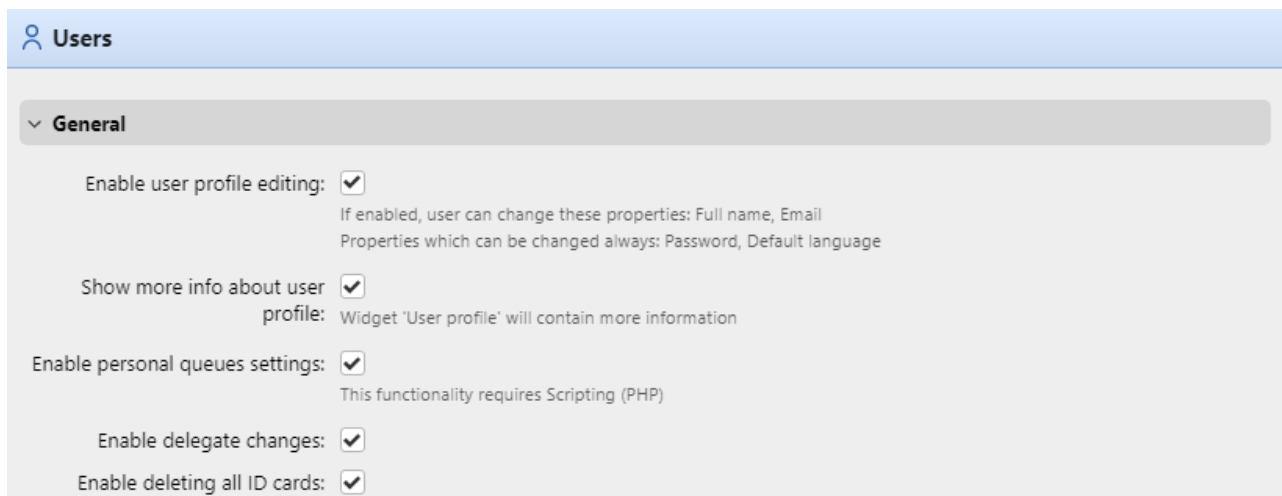
### To deselect delegates:

On the bar at the top of the **Delegates** tab, in the **Delegates** combo box, point to the user (or group of users) that you want to deselect, and then click the remove button (X) on the right side of the user (or group of users).

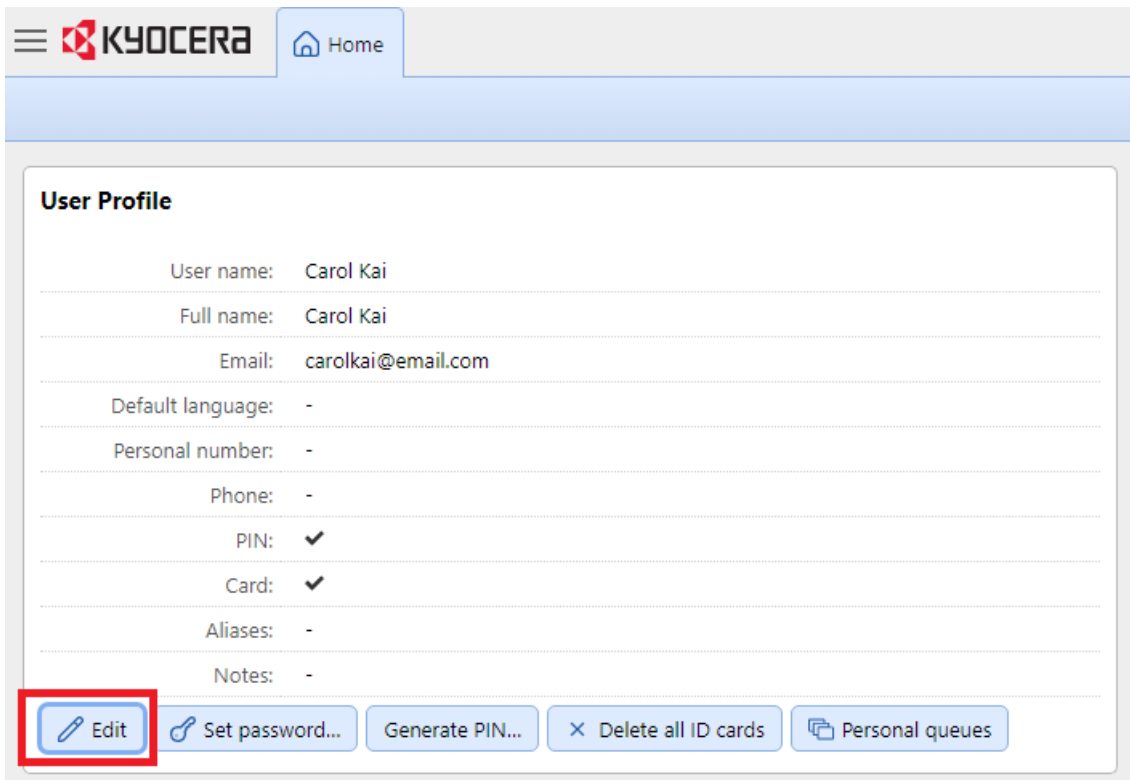
## 10.6 Enable user profile editing

By default, all users can change their default language on their **KNM** Web accounts and on some embedded terminals, while the rest of their properties can be changed only by the administrator. On the **Users** settings tab, you can provide users with additional editing options: change their full name and email.

To enable users to change their full name and email, select the **Enable user profile editing** option.



Once user profile editing is enabled, users can open their profile management options by clicking **Edit** at the bottom-left corner of the **User profile** widget on their **KNM** Web accounts.



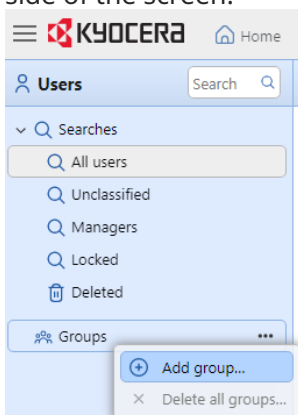
## 10.7 User groups

On the **Users** main tab, you can create new user groups. In **KNM**, different groups of users can be given different access rights to print queues (see [Queues](#)), print functions, such as color printing or scanning (see [Policies](#)), and reports (see [Reports](#)).

### Creating user groups

To create a group, do the following:

1. On the group tab on the left side of the **Users** main tab, point on the group under which you want to create the new group. A drop-down box appears to the right.
2. On the drop-down box, click **+Add Group**. The new group properties panel opens on the right side of the screen.



3. Enter a name for the new group.

4. Click **Save**.

To select delegates for the group:

1. Open the group properties panel by double-clicking on the group.
2. On the bar at the top of the **Delegates** tab of the group properties panel, in the **Delegates** combo box, enter or select the user (or the user group).
3. Click **Save**. This way you can add multiple users (or the user group).

To deselect delegates for the group:

On the bar at the top of the **Delegates** tab, in the **Delegates** combo box, point to the user (or user group) that you want to deselect, and then click the remove button (**X**) on the right side of the user (or user group).

### Deleting user groups

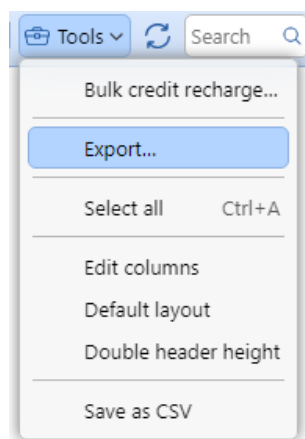
1. On the group tab on the left side of the **Users** main tab, right-click the group that you want to delete.
2. Click **Delete**.

## 10.8 Exporting users

In case you need to export the list of **KNM** users to a CSV file — for example if you want to use the CSV file for user synchronization — you can do so on the **Users** main tab of the **KNM** Web Interface.

To export the list of users:

1. Click **Tools** on the toolbar at the top of the **Users** main tab.
2. Click **Export** in the **Tools** drop-down. The Users Export dialog box appears.
3. In the dialog box, select the group you want to export and click **OK**. The file is downloaded to your default *Downloads* folder.



You can also export all the users by selecting **Save as CSV** in **Tools**.

## 10.9 Securing KNM users personal data

Except for the data shown in **KNM** reports, everything stored in **KNM** is necessary for the functioning of the system. The data can be accessed only by people with administrator rights in **KNM** and are not processed by the system or disclosed to third parties. As to the information shown in **KNM** reports, it

is fully under the control of the **KNM** administrator, who can provide certain users with rights to view information related to other users or groups.

**KNM** users can access their personal data within the **KNM** system and upon their request, the **KNM** administrator can erase the data by anonymizing the user. The following sections show how the users can access the data and how to anonymize the users.

These options are closely related to the General Data Protection Regulation (GDPR), which aims to protect the personal data of EU citizens. For more information about how the GDPR is implemented in **KNM**, contact your Support.

### 10.9.1 Providing users with their personal data

On their **KNM** Web accounts, **KNM** users can see the **User profile** widget with the personal information stored in **KNM**.

On their Web account, **KNM** users can generate reports related to their activity within **KNM**, such as printing, copying and scanning to see what information is available in these reports (see [Reports](#)).

Users may also contact the **KNM** administrator with a request to provide them with the data.

The **KNM** administrator can create a custom dashboard message informing all users about the data protection options and include the admin email contact via the **%admin%** parameter (see [Personalization](#)).

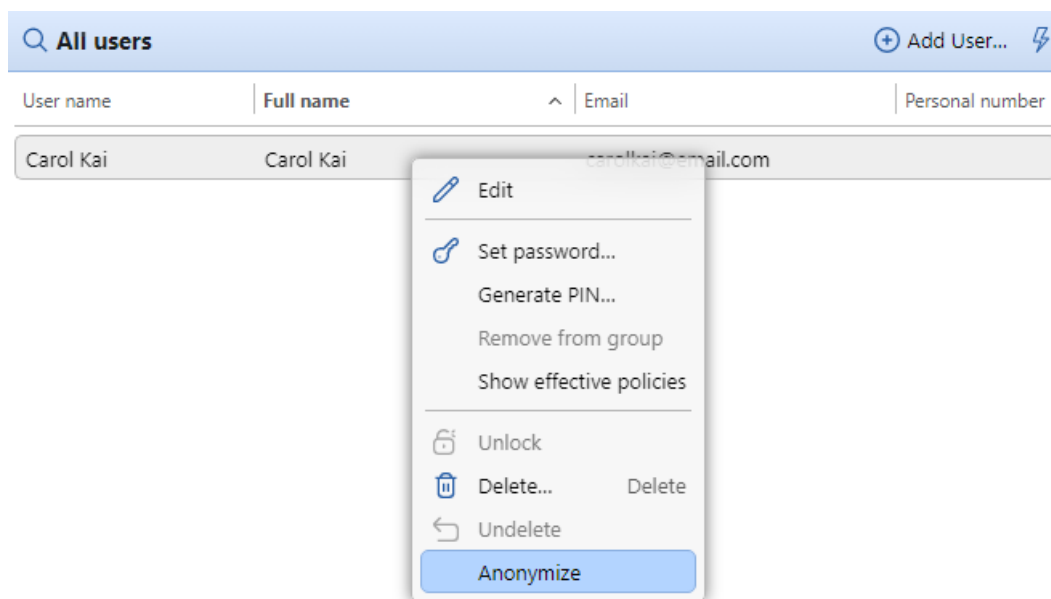
### 10.9.2 Anonymizing users

After the anonymization, the user is completely removed from the system and replaced by a randomly generated name in all of the relevant **KNM** reports.

After a user is anonymized, all of their personal data (including username and email) are permanently erased from the system and cannot be retrieved.

To anonymize a user:

On the **Users** main tab of the **KNM** Web Interface, select the users that you want to anonymize, then click **Actions** (or select the users, and then right-click any of them), and finally click **Anonymize**.




## 10.10 User import and synchronization

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

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

- [User synchronization from LDAP servers](#)
- [User synchronization from Azure AD with Microsoft Graph](#)
- [User synchronization from CSV files](#)
- [User synchronization from Azure AD with SLDAP](#)
- [Using external authentication servers](#)
- [Manual and scheduled synchronization run](#)

 User passwords are not synchronized/stored in the **KNM** Database in case of LDAP/Azure synchronizations.

### 10.10.1 How does the user synchronization work?

First, you need to add a new synchronization source. Overall, there are the following possible types of synchronization sources: LDAP server, Azure AD, CSV file, **KNM** Central server, and Custom script, but in this topic, we will discuss only the first three types. The synchronization from the Central server is used on the Central/Site server architecture installations of **KNM** and is explained in the **KNM** Central Server Installation Guide. The synchronization from a custom script is used only in very specific cases; for information about this option, please contact your Support.

As soon as you add the synchronization source, **KNM** opens its properties panel where you can set it up. 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 users' data in **KNM**.

An important part of the synchronization setup is pairing user attributes in the synchronization source with their counterparts in **KNM**. 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 lowercase. These options can be selected in the **Options** section of the **Users** sub-tab 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** sub-tab of the LDAP synchronization settings tab or by defining the groups inside the CSV synchronization file.

### User properties and synchronization options

#### User properties in **KNM**

- **User name:** Name of the user account in **KNM**. In Active directory and Open LDAP, this property corresponds to the **samaccountname** user attribute on the LDAP server.

- **Full name:** 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. **KNM** treats aliases as alternative user names. You can use aliases, for example, if you need to enable one user to send jobs to **KNM** from different OS accounts.
- **Card:** The number of the user's identification card. It can be either imported from LDAP or added to **KNM** on the user's properties panel. Also, it can be registered by an administrator on a card reader connected to a USB slot or registered by the user on an embedded terminal.
- **PIN:** The **KNM** personal identification number is used for access to **KNM** Web Interface and **KNM** terminals.
- **Personal number:** The personal number can be used as the user ID in **KNM**. 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:** The user's primary email address.
- **Notes:** You can use this text box to enter additional notes concerning the user.
- **Language:** The language used on the user's **KNM** Web Interface and their home screen on the embedded terminal.
- **User's storage:** You can select a folder or one or more email addresses where **KNM** sends the user's scans. 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 **KNM** or entered by the scanning users.

### User synchronization options

- **Deactivate missing users:** If you select this option, **KNM** 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, **KNM** adds new users from the current synchronization source. If you do not select it, **KNM** updates the user accounts of the users who are already in **KNM**, but does 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"), **KNM** 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 the **KNM** database, but instead against an LDAP or Radius server. If you synchronize users via LDAP, the source LDAP server is automatically assigned as the authentication server. If you synchronize users via CSV, you can select the authentication server from the list of predefined authentication servers.
- **Pair by the personal number:** If you select this option, **KNM** 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*, **KNM** does not create a new user account, but recognizes the old user by their personal number.
- **Ignore synchronization source:** If this option is not selected, **KNM** recognizes two users from different synchronization sources as two different entities. This can cause conflicts during synchronizations from multiple sources. If it is selected, **KNM** ignores the synchronization sources and treats all users the same, regardless of their synchronization source. For example, if you run a synchronization and **KNM** 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.

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 **KNM** username. The information about the domain may be needed for example, when scanning to users' home folders is used on an embedded terminal.

## 10.10.2 User synchronization from LDAP servers

An 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 **KNM** Web Interface, you can synchronize users directly from the server database.

**KNM** can communicate with as much as five LDAP servers at the same time. 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.

**i** The settings described here apply only to Active Directory, although the settings for OpenLDAP, Novell and Lotus Domino are similar.

**⚠** OpenLDAP, with its default settings, limits the number of returned entries and the maximum total time for a query. The default size limit is 500 entries and the default time limit is one hour. In case of a larger customer installation with OpenLDAP, you must adjust these limits appropriately in the OpenLDAP settings, otherwise the user sync will give incomplete results. For more details see: <https://www.openldap.org/doc/admin24/limits.html>

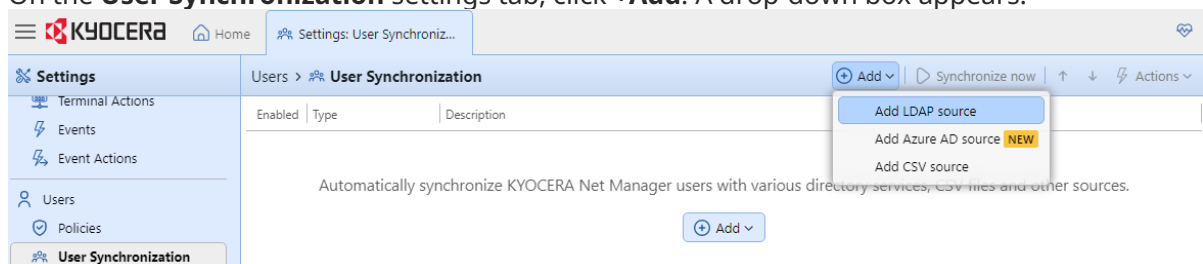
## Creating an LDAP synchronization

Before creating the synchronization, you have to add the LDAP server to **KNM**. You do this on the **Authentication Servers** settings tab. Set **Security** to **SSL** and the server port to **636**.

To create a new LDAP synchronization:

1. Add the new synchronization:

On the **User Synchronization** settings tab, click **+Add**. A drop-down box appears.



In the drop-down, 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 all three tabs on the LDAP synchronization properties panel. On each of the tabs, click **Save** after changing the settings. For more information, see [Setting up the LDAP synchronization](#).
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.

## 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.

### 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 a description of individual settings.

The screenshot shows the 'LDAP Synchronization' settings panel with the 'General' tab selected. The 'Enabled' toggle is turned on. Under 'Connection parameters', the 'LDAP Server' is set to 'LocalAD@domain.com', 'User' is 'admin', and 'Password' is masked with dots. Under 'Export to CSV after successful import', the 'Enabled' checkbox is unchecked, and the 'File' path is '%app%\Data\Export\Users\_LDAP\_%datetime%'. The 'Parameters' field contains '%app%', '%datetime%'. There are 'Save' and 'Cancel' buttons at the bottom. A note at the bottom states 'Fields marked by \* are mandatory.'

- **Enabled:** Here you can enable or disable the synchronization.
- **LDAP Server:** Here you can select the domain that you want to synchronize from.
- **User:** Enter the username for access to the LDAP domain server.
- **Password:** Enter the password for access to the LDAP domain server.
- **Enabled:** If you enable the **Export to CSV after successful import** option, **KNM** creates a CSV file with the imported users after the synchronization.
- **File:** Select the folder where you want to save the created file.

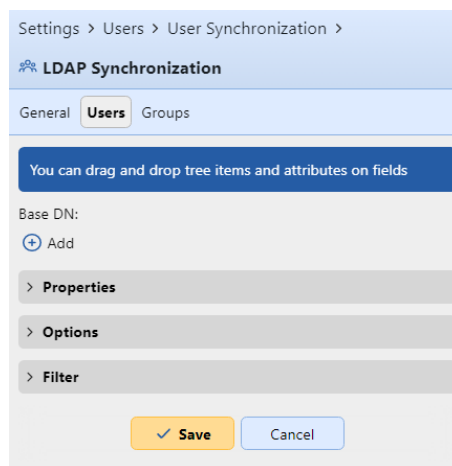
After you correctly set the connection parameters (LDAP server, user and password) and save the settings, the LDAP browser opens on the right side of the screen.

**In the **User** setting, a sub-domain user account with enough rights can also be used for authentication, but the sub-domain has to be specified in the username.**

For example, the user *Administrator* connects to the *testAD.local* LDAP server, but their account is in the *cz.testAD.local* sub-domain. For successful authentication, the filled in username should be:  
*Administrator@cz.testAD.local*

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

On the **Users** tab, pick one or more base DN's (distinguished names) from which you import the users. In addition, you can assign user attributes from the LDAP server to user properties in **KNM** and select additional options concerning the synchronization.



- **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.
- **Properties:** These are the properties of every individual user. **KNM** 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 OpenLDAP 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 it from the attributes of any individual user and drop it in the text box. The following properties support adding multiple values to them, separated by a semicolon (;):
  - **Alias**
  - **PIN**
  - **Card**

For example, in the **Alias** property, you could add *alias1;alias2;alias3*.

The AD attribute name should not contain the semicolon (;) character. If a semicolon is part of the attribute's name, that attribute will not be synchronized in **KNM**.

For assigning default languages to users, you have to use an attribute from the LDAP server that has the language abbreviations as its values. For example, you can create and use an attribute called **lang** with the values *en* for English, *hr* for Croatian, etc. The list of the abbreviations used in **KNM** can be found here.

- **Options:** For a description of the common synchronization options, see [User information and settings](#). 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 support.

- **Filter:** You can filter the users import by specifying the values of attributes. Add the conditions in the form: **Attribute=Value**. Users with a different value on this attribute are not accepted and are filtered out of the import.

For attributes where the values are strings, such as the **cn** attribute, 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 row. Users are accepted if they satisfy at least one condition.

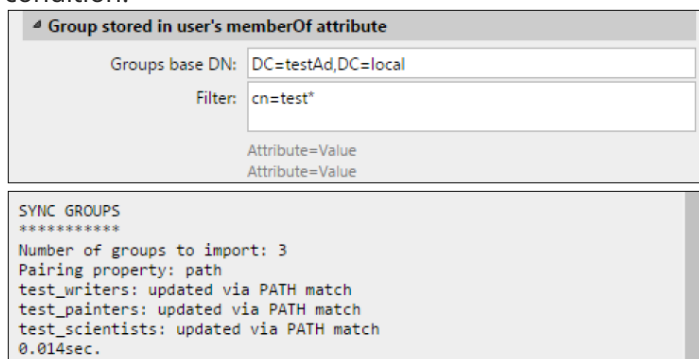
### Groups tab: Importing groups

On this tab, you can import groups and the group structure from the LDAP source. There are four different ways 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 **KNM**.

The screenshot shows the 'LDAP Synchronization' configuration page, specifically the 'Groups' tab. At the top, there is a breadcrumb trail: 'Settings > Users > User Synchronization > LDAP Synchronization'. Below this, there are three tabs: 'General', 'Users', and 'Groups', with 'Groups' being the active tab. A blue instruction box states: 'You can drag and drop tree items and attributes on fields'. Below this, there is a radio button labeled 'Make default' which is selected. Underneath is a dropdown menu labeled 'Import groups under this group:'. Below the dropdown are four expandable options, each with a right-pointing chevron: 'Group stored in user's attribute', 'Group stored in user's DN', 'Tree group stored in user's DN', and 'Group stored in user's memberOf attribute'. At the bottom of the form are two buttons: a yellow 'Save' button with a checkmark and a light blue 'Cancel' button.

- **Do not change default group:** A user can be a member of multiple groups but all their prints, copies and scans are accounted to only one group: the default (accounting) 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 **KNM** 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 it, type the name of the attribute in the property text box or drag the attribute from any individual user and drop it in the **Attribute** text box. You can also create groups by combining multiple attributes. To create such groups, put each of the attributes between two percentage signs (%). For example, the combination of attributes `%attribute1%_%attribute2%`, imports a new group named `value1_value2`. Furthermore, you can create tree structures of groups by separating the attributes with vertical bars. For example, the combination of attributes `%attribute1%|%attribute2%`, imports a group `value1`, and its sub-group `value2`.
  - **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 unit) index among the DN components. The index is counted from right to left: the first OU group from the right has index 1, the second from the right has index 2 and so on.
- **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 the left and from the right. In the respective text boxes, enter the amount of components to be striped from the left and from the right side. You have to strip at least one component from the left (the user CN component) and one component from the right (the right-most DC component).
  - **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: KNM** 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 into consideration during the import, you have to insert the groups base DN. **KNM** imports 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 in 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 the values of attributes. Add the conditions in the form: *Attribute=Value*. Groups with a different value on 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. You can add one condition per row. Groups are accepted if they satisfy at least one condition.



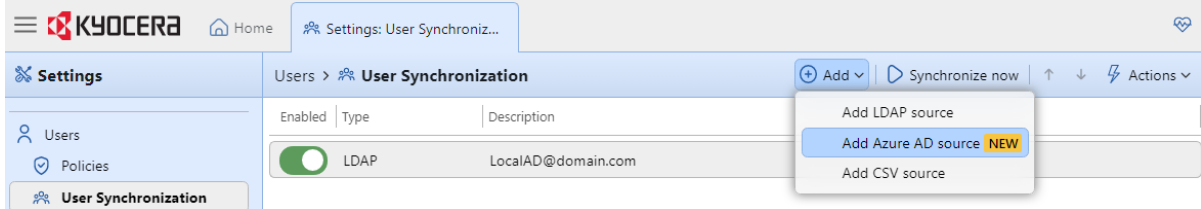
- **Import empty groups:** If you select this option, groups from the **Group base DN** are imported even if there is no user having them in their **memberOf** attribute.
- **Import tree of groups:** If you select this option, the whole tree structure is imported. Otherwise all groups are added separately; not as a part of a tree structure.

### 10.10.3 User synchronization from Azure AD with Microsoft Graph

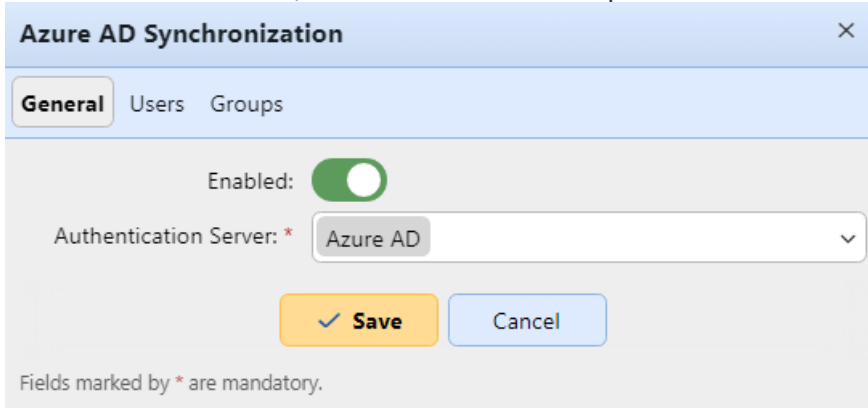
Azure AD with Microsoft Graph is a service accessed from the Microsoft Azure Portal, where it has to be **enabled and configured**.

Once the Azure AD connection is established, go to **KYOCERA, Settings, User Synchronization**.

1. Click **Add**, and then click **Add Azure AD source**.



2. In the Azure AD Synchronization properties panel to the right, in the **General** tab, if you have already set up an Azure AD connection, the Azure AD server is already in the **Authentication Server** field. Otherwise, click **Add new** and set up an Azure AD connection.



3. Click **Save**.
4. In the **Users** tab:

**Azure AD Synchronization** [X]

General **Users** Groups

Users to import:  All users  
 Users from selected groups

▼ **Properties**

User name: userPrincipalName ▼  
Alias: ▼  
Card: None ▼  
PIN: None ▼  
Personal number: None ▼

▼ **Options**

Use as authentication server  
If enabled, users will be using their credentials from Azure AD and can use the Sign in with Microsoft to log in.

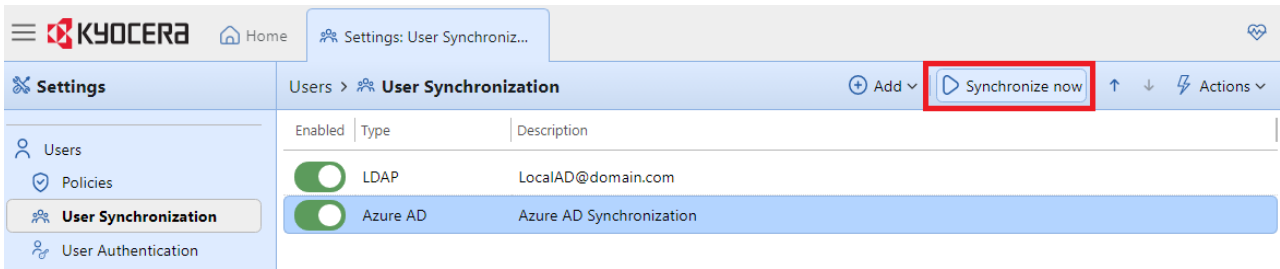
- a. You can map user information from Azure AD to the credentials in **KNM**.
  - b. If you plan to authenticate users towards Azure using Active Directory credentials and use the Microsoft single sign-on option, select the **Use as authentication server** option and click **Save**.
5. In the **Groups** tab, you can select what Active Directory groups you want to remove from synchronization using the **Ignore groups** and **Ignore groups containing string** fields.

**Azure AD Synchronization** [X]

General Users **Groups**

Ignore groups: ▼  
Ignore groups containing string:   
Place each string on a new line. Matching is case insensitive.

Users can be now synchronized by selecting your Azure AD source from the list and clicking **Synchronize now**.



## 10.10.4 User synchronization from CSV files

To synchronize users from a 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.

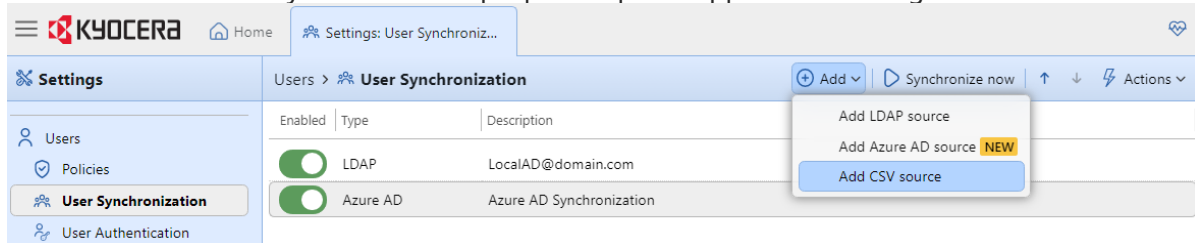
CSV synchronization:

- [Creating a new CSV synchronization](#)
- [CSV synchronization setup options](#)
- [CSV file syntax](#)

### Creating a new CSV synchronization

To create a new synchronization:

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



2. **Set up the synchronization:** On the CSV synchronization properties panel, set the path to the CSV file in the **CSV file** field, and configure the synchronization. For information about the synchronization options, see "CSV synchronization setup options" below.

**CSV synchronization** ✕

Enabled:

---

CSV file: \*   
Parameters: %app%

Encoding: \*

Column delimiter in CSV:

Skip header line:

3. **Save** the setup.

## CSV synchronization setup options

These are the CSV synchronization setup options:

- **Enabled:** Here you can enable or disable the synchronization.
- **CSV file:** Here you can set the path to the CSV file on the **KNM** server.
- **Encoding:** Select the encoding that is used in the CSV file. The default value depends on the OS settings of the computer where you access the **KNM** Web Interface on.
- **Column delimiter in CSV:** Select the delimiter that is used in the CSV file. If you select the **Default** option, **KNM** scans for the delimiter set on the **Column delimiter in CSV** drop-down list box on the **General** settings tab.
- **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 **KNM** contain the header line.
- **Import groups under this group:** Here you can select an existing group in **KNM** 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 **KNM** 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 the authentication of the imported users.
- **Authentication server:** Here you can select the LDAP or Radius domain for the user authentication.
- **Deactivate missing users:** If you select this option, **KNM** 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, **KNM** 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/Delegates:** In each of the mandatory drop-down boxes, you can select from these synchronization options for the respective parameter (Cards, PIN, Groups):
  - **Do not synchronize:** The value of the respective parameter in **KNM** is not changed.
  - **Full synchronization:** The value of the respective parameter in **KNM** is always replaced by the value in the CSV file. If the value in the source file is empty, the value in **KNM** is erased.
  - **Synchronize if not empty:** If the respective field in the CSV file is not empty, the parameter value in **KNM** 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 **KNM**, it is not replaced. Only new values are added.

## CSV file syntax

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

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 Pineapple"*.
- **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.pineapple@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"*, **KNM** imports a single parent group *Activities* with a single child group *Outdoor*, with two child groups *Swimming* and *Birdwatching* (*Activities>Outdoor>Swimming,Birdwatching*). 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 to, for example *"\Users\Tomy"*.
- **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 the 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*. 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 to use the **KNM** password, insert the password in the hashed MD5 format, for example *18BFA6BB14875E8*. If you are using a different authentication server (i.e. LDAP server), you can leave it empty.
- **EXTID:** EXTID is an internal **KNM** 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"*.

```
"FULLNAME"; "USERNAME_ALIASES"; "EMAIL"; "CARDS"; "GROUPS"; "CODE";
"SCANSTORAGE"; "PIN"; "MANAGED_GROUPS"; "AUTHSERVER"; "PHONE";
"LANG"; "PWD"; "EXTID"; "DELEGATES"
```

```
"Thomas Pineapple"; "Tom, Tommy, Apple"; "t.pineapple@domain.com";
7E9700C9;"Imported Users, Activities|Outdoor|Swimming,
Activities|Outdoor|Birdwatching";22212;"\Users\Tomy";
14BFA6BB14875E4;Birdwatching;testAD.local;080008020;en; 18BFA6BB14875E8; ;"Carol,Kohei,Eliot";
```

## 10.10.5 User synchronization from Azure AD with SLDAP

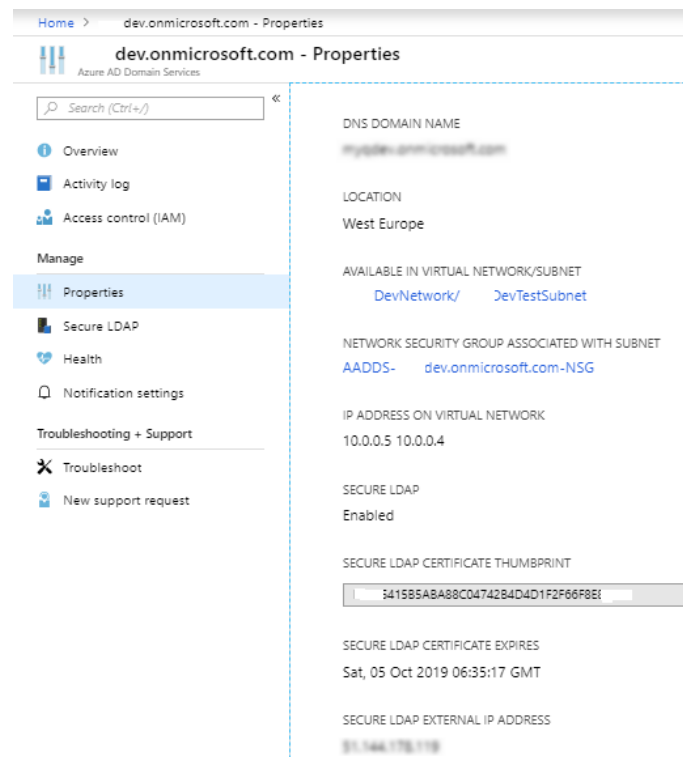
Azure AD with SLDAP is a service accessed from the Microsoft Azure Portal. It has to be enabled and configured in Azure Active Directory Domain Services.

The 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/tutorial-create-instance>
- Configure Azure AD Domain Servers to use SLDAP:  
<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/tutorial-configure-ldaps>

After you activate the Azure AD, you need to add it to **KNM** and set up the synchronization in the standard way (see [User Import and synchronization](#)). When setting up the **Authentication server** in **KNM**, you need to make sure that the LDAP server parameters 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



## 10.10.6 Using external authentication servers

In addition to the internal **KNM** authentication methods (password, PIN or ID card), you can use two types of external authentication servers: LDAP and Radius.

With the two external methods, **KNM** does not use the internal **KNM** 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:

1. register the external authentication servers in **KNM**
2. select to use them for user authentication

To register external authentication servers in **KNM**, see [Authentication Servers Settings](#).

Selecting to use the registered external authentication servers for user authentication, can be done either automatically during the user import from an LDAP server or a CSV file, or manually on the properties panels of individual users.

## Automatically selecting the external authentication option

### Importing users from a CSV file

When you import users from a CSV file, 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 the synchronization setup 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](#).

### Importing users from an LDAP server

During the users import from an LDAP server, you can select the **Use authentication server option**, to use the current synchronization source server for users authentication. For information about importing users from LDAP servers, see [User synchronization from LDAP servers](#).

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 where they are imported from.

## Manually selecting the external authentication option

To manually select the external authentication option

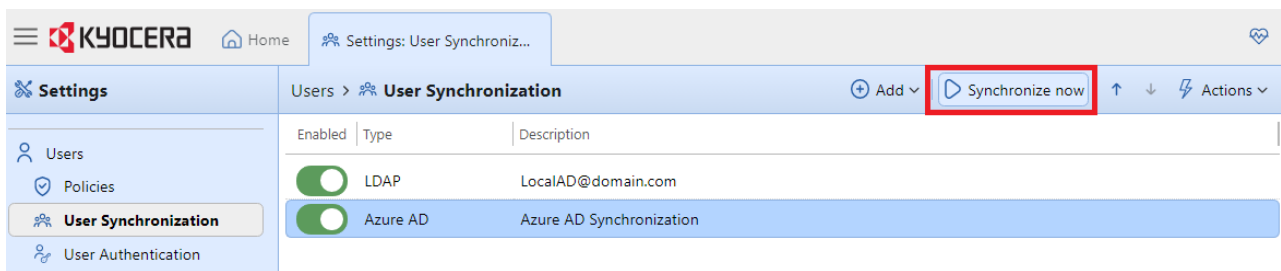
1. Open the **Users** main tab and double-click the user. The user's properties panel opens on the right side of screen.
2. On the panel, select the **Use authentication server** option. The Authentication server setting becomes available.
3. On the Authentication server drop-down box, select the server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

## 10.10.7 Manual and scheduled synchronization run

The synchronization can be manually run on the **User Synchronization** tab of the **KNM** Web Interface, or it can be set as a scheduled task on the **Task Scheduler** tab.

### Manual synchronization run

On the **User Synchronization** settings tab, select the synchronizations that you want to run, and then click **Synchronize now** on the bar at the top of the tab.



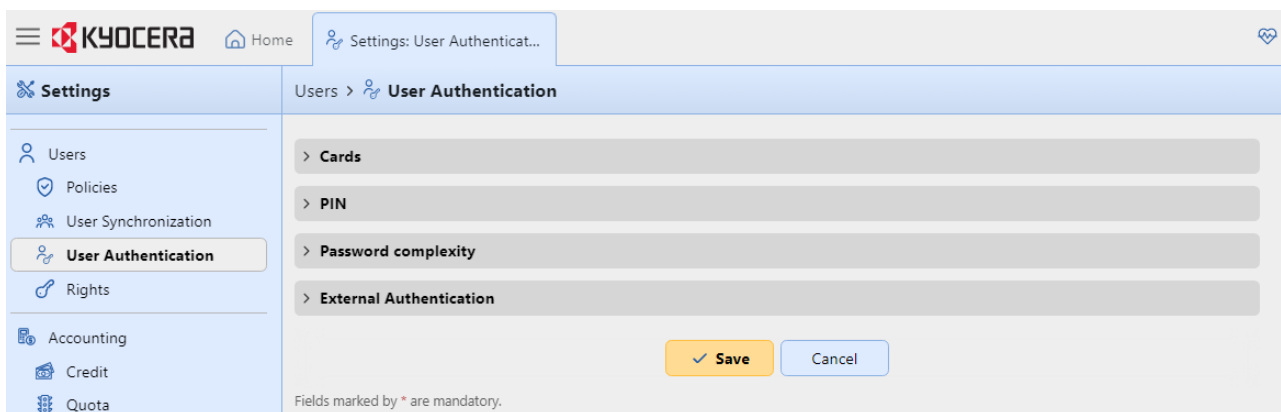
### Scheduled synchronization run

On the **Task scheduler** settings tab, you can setup a scheduled run of the synchronization. For more information about this option, see [Task scheduler](#).

## 10.11 User Authentication

In the **User Authentication** settings tab, the administrator can manage everything related to how users authenticate themselves in **KNM**:


- [ID Card management](#)
- [PIN management](#)
- [Password Complexity](#)
- [External Authentication](#)



### 10.11.1 ID Card Management

In the **User Authentication** settings tab, in the **Cards** section, there are the following ID Card management options:

- **Enable registration of multiple cards** - This is enabled by default. If disabled, when a new card is registered, the current cards are deleted.
- **Register cards as temporary** - If this is enabled, ID cards can be registered as temporary.
  - **Validity of temporary cards** - Set the duration of the temporary cards validity in hours.
- **Card code transformation** - This transformation is used by Embedded terminals (with USB readers connected directly to the device) and by the reader for a HW terminal that is connected, usually, as a primary reader.
- **USB reader transformation** - Check the box to apply the transformation to card readers connected to a PC USB slot. These card readers are usually used to recharge credit or to associate cards with user accounts.

Users >  **User Authentication**

▼ **Cards**

Enable registration of multiple  cards: If cleared, the current cards are deleted when a new card is registered.


Register cards as temporary:

Validity of temporary cards: \*  hours

▼ **Advanced**

Card code transformation:

USB reader transformation:

 Adding cards manually is not possible when cards are synchronized from an LDAP source. The manually added cards will be deleted during the next LDAP synchronization, and overwritten by the cards from the LDAP source.

[Adding multiple cards via the LDAP synchronization](#) is supported.

## ID Card Transformation

This topic discusses the ID Card transformation feature in **KNM**. 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 the **KNM** card reader.

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

With most of the **KNM** 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 **KNM** transformations than to separately change settings of each card reader.

How to setup the card transformation:

On the **User Authentication** settings tab, in the **Cards** section and under **Advanced**, you can define and use a transformation for card readers and select to use it on a USB reader connected to the administrator PC. The USB reader can be used to recharge credit or associate cards.

Available options:

- **Card code transformation:** This transformation is used by Embedded terminals (with USB readers connected directly to the device) and by the reader for a HW terminal that is connected, usually, as a primary reader.
- **USB reader transformation:** Check the box to apply the transformation to card readers connected to a PC USB slot. These card readers are usually used to recharge credit or to associate cards with user accounts.

Defining the transformation

You can define the transformation by adding commands that can be found on this [list](#). The commands have to be separated by a semicolon (;) and are read and executed from left to right. For example in the transformation *CommandX;CommandY*, *Command X* is executed first and *Command Y*, second.

All the 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.

### ID card transformation commands

- **ltrim(number of characters)** – Remove the first X characters from the left.  
*ltrim(2): 123456 → 3456*
- **rtrim(number of characters)** – Remove the first X characters from the 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 the left (and remove the rest).  
*left(2): 123456 → 12*
- **right(number of characters)** – Select the first X characters from the right.  
*right(2):123456 → 56*
- **mid(number of characters, number of characters)** – Remove X characters from the left, remove Y characters from the right and leave the characters in the middle.  
*mid(2,2): 123456 → 34*
- **lpad(number of positions, symbol)** – Complete the string to the length specified by the **number of positions** parameter by adding the value of the **symbol** parameter to the left (in front of the card number).  
*lpad(12,0): 123456 → 000000123456*
- **hex2dec()** – Transform the card number from hexadecimal mode to decimal mode.  
*hex2dec(): 1000AB → 1048747*
- **dec2hex()** – Transform the card number from decimal mode to hexadecimal mode.  
*dec2hex(): 1048747 → 1000AB*
- **hex2bin** – Transform the card number from hexadecimal mode to binary mode.  
*hex2bin(): 1000AB → 10000000000010101011*
- **bin2hex** – Transform the card number from binary mode to hexadecimal mode.  
*bin2hex(): 10000000000010101011 → 1000AB*
- **dec2bin** – Transform the card number from decimal mode to binary mode.  
*dec2bin(): 100023 → 11000011010110111*
- **bin2dec** – Transform the card number from binary mode to decimal mode.  
*bin2dec(): 11000011010110111 → 100023*
- **reverse()** – Reverse the byte sequence, i.e. take all the characters by two and reverse the order of the pairs. (The last pair goes first, the second last goes second, etc.)  
*reverse(): 1234AB → AB3412*
- **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 support.
- **asciiCode2ascii** – Converts ASCII characters encoded as hex-digits to ASCII characters.  
*asciiCode2ascii(): 414F → AO*
- **"string 1" + "string 2"** – Merges the strings in front of and behind the + 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.

#### **ID card transformation example:**

Card number: 10AB

Card code 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"`

### **10.11.2 Generating PIN**

On the **User authentication** settings tab, under **PIN**, you can select multiple options concerning PIN generation.

Users >  **User Authentication**

▼ PIN

User can change PIN:

Minimal PIN length: \*

Send new PIN via email:

Generate PIN for users created by synchronization or manual input:  \*Send new PIN via email\* will be automatically checked

▼ Email with a new PIN

Subject: \* KYOCERA Net Manager: Your new PIN

Message: \* Your new KYOCERA Net Manager PIN is: %PIN%  
Please contact the administrator at %admin% in case of further requests

Parameters: %pin%, %username%, %realname%, %admin%

[↶ Revert values](#)

▼ Email with the PIN reset code

Subject: \* KYOCERA Net Manager: PIN reset code

Message: \* Hello %realname%,  
Your PIN reset code is: %code%  
Go to the KYOCERA Net Manager website, click "Lost PIN" and enter the code.  
Your KYOCERA Net Manager  
Please contact the administrator at %admin% in case of further requests

Parameters: %code%, %username%, %realname%, %admin%

[↶ Revert values](#)

### User can change PIN

With this option selected, the users can generate a new PIN on their account on the **KNM** Web User interface, by clicking **Generate PIN** on the **Home** screen of their user account.

### Minimal PIN length

This option determines the mandatory minimum PIN length. The number can be set between 4 and 16.

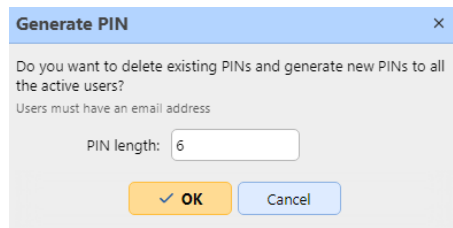
If the administrator creates the PIN manually, it cannot be shorter than the value set in this field. If the PIN is generated by the system, it cannot be shorter than the value in this field, and also cannot be shorter than the minimal value enforced by the number of users, described below.

The required minimal PIN length that depends on the number of **KNM** users is:

- < 1000 — 4-digit pin is required
- 1000 - 10 000 — 5-digit pin is required
- 10 000 - 100 000 — 6-digit pin is required

The required minimal length lowers the chance of randomly guessing the PIN. Also, trivial PINs, such as 1111 or 22222, are excluded from the automatic PIN generation process.

If the administrator increases the **Minimal PIN length** value, a pop-up will prompt them to generate new PINs for all the active users. If the administrator chooses to generate new PINs, the old PINs will be deleted and new PINs will be automatically sent via email to all the active users. Otherwise, the old, potentially shorter PINs will be kept.



## Generate PIN for users created in synchronization or manual input

With this option selected:

- A new PIN is generated for new, manually created users.
  - A manually created user without an email address will not receive the new PIN via email.
- During **User synchronization**, a new PIN is generated for every user that does not already have a PIN.
  - PINs are generated only for users with an email address. Users without an email address are skipped.

## Send new PIN via email

With this option selected, users are sent an email informing them about the new PIN every time a new PIN is generated.


This is automatically checked if the above option (**Generate PIN for users created in synchronization or manual input**) is selected.

There are also email templates you can use for informing the users about their new PIN (**Email with a new PIN**) or for providing them with a reset code in case of a lost/forgotten PIN (**Email with the PIN reset code**). The templates are editable and the values can be reset to their defaults if needed, by clicking **Revert values**.

## 10.11.3 Password complexity

In this section, the administrator manages the password complexity of **KNM** users accounts.

- **Minimum length** - set the minimum character length for the password, in range *1-100* (8 by default).
- **Enforce password complexity** - set how many of the four password complexity rules are to be enforced (2 by default):
  - At least one upper-case letter
  - At least one lower-case letter
  - At least one number
  - At least one special (non-alphanumeric) character

Users >  User Authentication

> Cards

> PIN

∨ Password complexity


Minimum length: \*

Enforce password complexity: \*  of 4 rules

- At least one upper-case letter
- At least one lower-case letter
- At least one number
- At least one special (non-alphanumeric) character

## 10.11.4 External Authentication

Administrators can benefit from **using external authentication servers** for authenticating users into **KNM**. This is helpful mainly in environments where an authentication service not natively supported by **KNM** is used.

 External Authentication is used for login on the **KNM** Embedded Terminal and **KNM** Desktop Client. The **KNM** Web User Interface requires credentials set in **KNM**.

### How it works

An API connector between **KNM** and the authentication service is set up. **KNM** requests authentication through this connector, and on the other side is the authentication service itself where users and their credentials are stored.

**1** User attempts to sign in on the **KNM** Embedded Terminal

- By swiping an ID card
- By entering a PIN

**2** The request is sent to the API connector, containing the login method type and the value

**3** The connector handles communication with the authentication service and returns the user who matches back to **KNM**

There are two modes of operation for External Authentication. Either it **can be the primary way of authenticating** users, or it can be configured **as a backup authentication** in case the authentication towards **KNM** fails. For this, the option "Use only if authentication against **KNM** DB fails" can be selected.

### Authentication request


#### Supported login methods

This setting **defines the login method** for which External Authentication is used. The other, unselected, login method authenticates the user against the credentials in **KNM**.

- ID Card
- PIN

**KNM** sends the type of login method together with the actual PIN/ID card value so that the API connector can recognize which user property should be used to find the correct user.

For example, if an ID Card is selected, and the user authenticates on the Embedded Terminal with an ID card, **KNM** sends out *loginType=1&loginValue=1234*. This can be interpreted as the ID card number 1234.

 If a card reader that emulates keystrokes is connected to the device and a user swipes their card, **KNM** cannot recognize if the value received is a PIN or ID card number. **KNM** indicates this to the API connector (*loginType=7*). The connector should be configured to handle these requests, e.g. by attempting to authenticate towards both user properties.

## Authentication response

### Supported user identifiers

The API connector has to respond in a JSON format with one of the values back to **KNM** to pair the correct user and log them into the client.

- Personal number of an existing user in **KNM**
- Username of an existing user in **KNM**

Example responses:

- *{"result":0,"personalNumber":"123456"}* means that the user was successfully identified by the authentication service and its personal number is 123456. The user with this personal number in **KNM** is authenticated.
- *{"result":0,"username":"JohnDoe"}* means that the user was identified and its username is JohnDoe. The user with this username in **KNM** is authenticated.

### Error states

- Invalid user (*{"result":1}*)-- the user was found, but their account is invalid (e.g. deactivated)
- No user found (*{"result":2}*)-- there is no user associated with the credentials

### Common use cases

The External API connector can be used in its most simple way to “translate” requests. But it also allows more advanced authentication workflows as the connector itself can perform a set of operations before it returns the matching user back to **KNM**.

**Example 1:** Authentication service not supported by **KNM** is required  
A connector that translates the API calls between **KNM** and the remote authentication service.

**Example 2:** Advanced authentication workflow – multiple identities  
External Authentication can be used in cases where some operation is required to happen between **KNM** and the authentication server. This can be transformation, advanced user recognition in multi-domain environments, and more.

## Setup External Authentication

External Authentication destination can be enabled and configured in **KYOCERA, Settings, User Authentication**.

Users > User Authentication

> Cards

> PIN

> Password complexity

External Authentication

Enabled:

URL: \*

User name:

Password:

Login method:  ID Card  
 PIN

Use only if authentication against KYOCERA Net Manager DB fails:

Test connection

Save Cancel

- **URL:** type the URL where the API connector is running
- **User name:** type the user name required for the connection to the external server via API
- **Password:** type the password required for the connection to the external server via API
- **Login method:** choose the users login method - *ID Card* or *PIN*
- **Use only if authentication against KNM DB fails:** this option defines whether the External Authentication will be the primary or secondary method for authentication
  - If enabled, the user is first authenticated towards the **KNM** Print Server, and only after it fails, the next attempt goes through the remote authentication service
  - If disabled, no authentication towards the **KNM** Print Server is performed, External Authentication service is always used

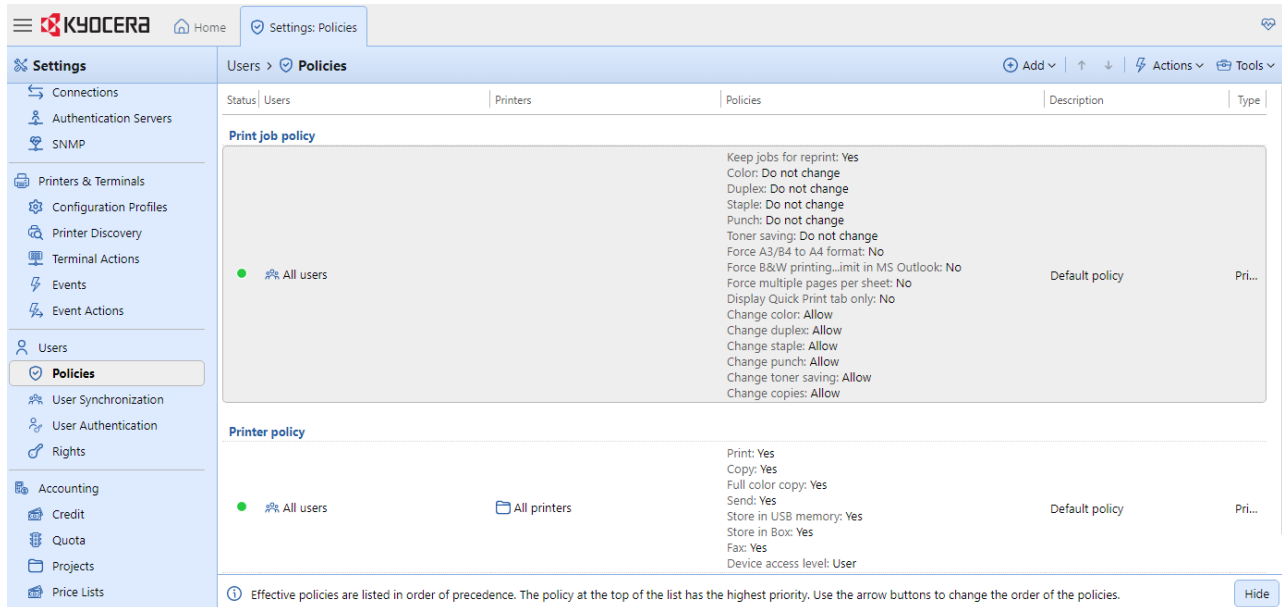
## 10.12 Policies

The **Policies** settings tab is divided into two sections. The **Print job policy** section contains settings that apply to all print jobs, all printers and selected users or groups.

The **Printer policy** section contains settings that apply to all queues, all print jobs, selected users (or groups) and selected printers.

**Print job policies** have the highest priority. Settings in the **Printer policy** section apply to all queues and all of the selected users, regardless of the settings of queues and print job policies.

Policies in both sections are listed in order of precedence: every policy has a higher priority than all the policies below it. If two policies are in conflict, the policy that is higher on the list applies. The default policy has the lowest priority and is always at the bottom of the list, other policies can be moved up and down the list by clicking the left or right arrow buttons on the **Policies** settings tab toolbar.



## 10.12.1 Print job policies

### Print job policies settings

To open a print job policy properties panel, double-click the print job policy on the **Policies** settings tab list, under **Print job policy**.

Each print job policy panel is divided into four sections:

- In the upper section, you can enable or disable the policy, select the **Users and Groups** of users that it will apply to, and add the policy's **Description**.
- In the **General** section, mark the checkboxes to be able to modify it and choose *Yes/No* if you want to **Keep jobs for reprint**.
- In the **Job Settings Defaults** section, mark the checkboxes to be able to modify the below settings:
  - **Color:** *Do not change, Force mono, Revert force mono*
  - **Duplex:** *Do not change, Simplex, Duplex long edge, Duplex short edge*
  - **Staple:** *Do not change, Yes, No*
  - **Punch:** *Do not change, Yes, No*
  - **Toner saving:** *Do not change, Yes, No*
- In the **Permissions** section, mark the checkboxes to be able to modify the settings and you can choose whether to *Allow* or *Deny* them:
  - **Change color**
  - **Change duplex**
  - **Change staple**
  - **Change punch**
  - **Change toner saving**
  - **Change copies**

Click **Save** and your new **Print job policy** appears in the **Policies** list.

## Default print job policy

The **Default policy** applies to all users and has no restrictions. Except for its name and scope, all the settings of this policy can be changed.

You can restore the default settings by clicking **Restore defaults** on the top-left corner of its panel.

The screenshot shows the configuration panel for the 'Default policy'. At the top, there is a 'Restore defaults' button. Below it, the 'Enabled' toggle is turned on. The 'Users and Groups' dropdown is set to 'All users', and the 'Description' field contains 'Default policy'. There are three main sections: 'General', 'Job Settings Defaults', and 'Permissions'. The 'Job Settings Defaults' section is expanded, showing various settings with dropdown menus: Color (Do not change), Duplex (Do not change), Staple (Do not change), Punch (Do not change), Toner saving (Do not change), Force A3/B4 to A4 format (No), Force B&W printing and page limit in MS Outlook (No), Force multiple pages per sheet (No), and Display Quick Print tab only (No). Each setting has a small note below it indicating which driver or software it applies to.

## Adding new print job policies

1. On the bar at the top of the **Policies** settings tab, click **+Add**, and then click **+Add print job policy**. The new print job policy properties panel opens on the right side of the screen.
2. On the panel, select the users or group of users that the policy will apply to, optionally write a description of the policy, change its settings, and then click **Save**.

The new policy appears on the **Policies** setting tab, under **Print job policies**.

With all the **Permissions** set to *Deny*, users are not able modify their jobs on the **KNM** Embedded terminals.

With the **Keep jobs for reprint** setting set to *No*, users are not able to add their jobs to **Favorites** on their account on the **KNM** Web Interface or on **KNM** Embedded terminals and they cannot reprint old jobs on the embedded terminals either.

The **Keep jobs for reprint** setting is also available when configuring a queue. The following combinations between the Keeps jobs for reprint Policy and Queue setting are available:

- Policy *ON* + Queue *ON* - The print job file is saved and can be reprinted even when not marked as favorite.
- Policy *ON* + Queue *OFF* - The print job file is saved only when marked as a favorite before printing. Favorite jobs can be reprinted.
- Policy *OFF* + Queue *ON* - The print job files are always saved, but because of the policy they cannot be reprinted or marked as favorite by the users. If the Policy is changed to *ON*, then the jobs can be reprinted later.
- Policy *OFF* + Queue *OFF* - The print job files are always deleted right after printing, cannot be reprinted or marked as favorite. If the Queue or Policy is changed to *ON*, jobs cannot be reprinted anyway.

## 10.12.2 Printer policies

### Printer policies settings

To open a printer policy properties panel, double-click the printer policy on the **Policies** settings tab, under **Printer policies**.

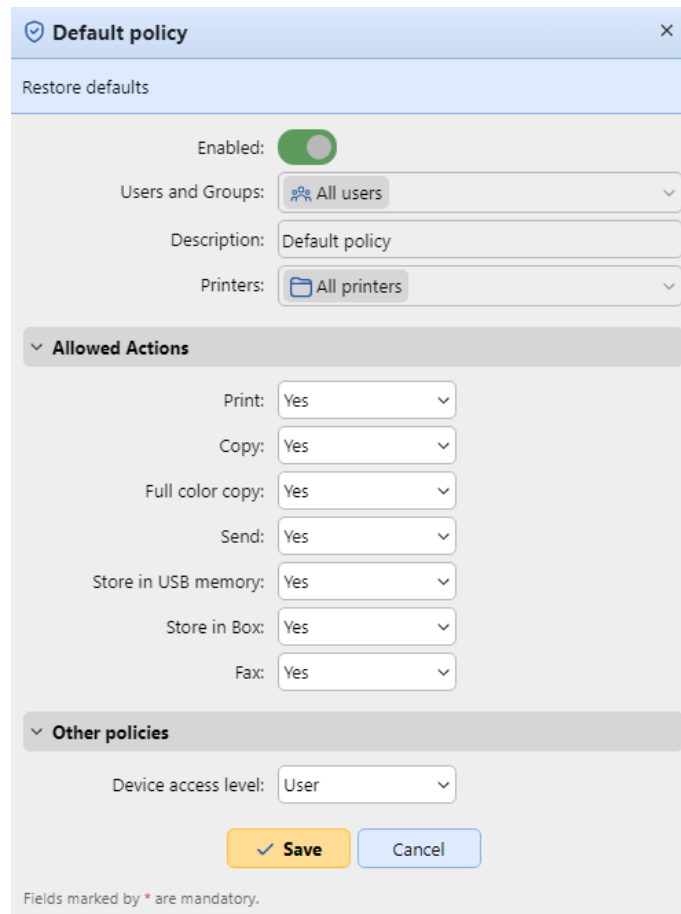
Each printer policy panel is divided into three sections:

- In the uppermost section, you can enable or disable the policy, select the **Users and Groups** of users that it will apply to, select the **Printers** that it will apply to, and write the policy description.
- In the **Allowed Actions** section, you can restrict access to particular operations on the selected printing devices. The available operations are:
  - **Print**
  - **Copy**
  - **Full color copy**
  - **Scan**
  - **Fax**
- In the **Other policies** section, you can provide users with administrator access to printing devices via the embedded terminal menu. For some devices, this option is not supported.

### Default printer policy

The **Default policy** applies to all users, all printers, has no restrictions and gives users **User access** to embedded terminals. Except for its name and scope (It applies to all users and all printers), all settings of this policy can be changed.

You can restore the **Default policy** default settings by clicking **Restore defaults** on the top-left corner of its panel.



## Adding new printer policies

1. On the bar at the top of the **Policies** setting tab, click **+Add**, and then click **+Add printer policy**. The new policy properties panel opens on the right side of screen.
2. On the panel, select the users or group of users that the policy will apply to, optionally write a description of the policy, change its settings, and then click **Save**. The new policy appears on the **Policies** settings tab, under **Printer policy**.

## 10.13 Rights

On the **Rights** settings tab, you can provide users or groups of users with administrator rights or provide them with rights to run one or more of the **KNM** agendas: they can perform actions, change settings or see information that are inaccessible under a standard user account. On the tab, you can add users or groups and provide them with the rights.

On the toolbar at the top, you can:

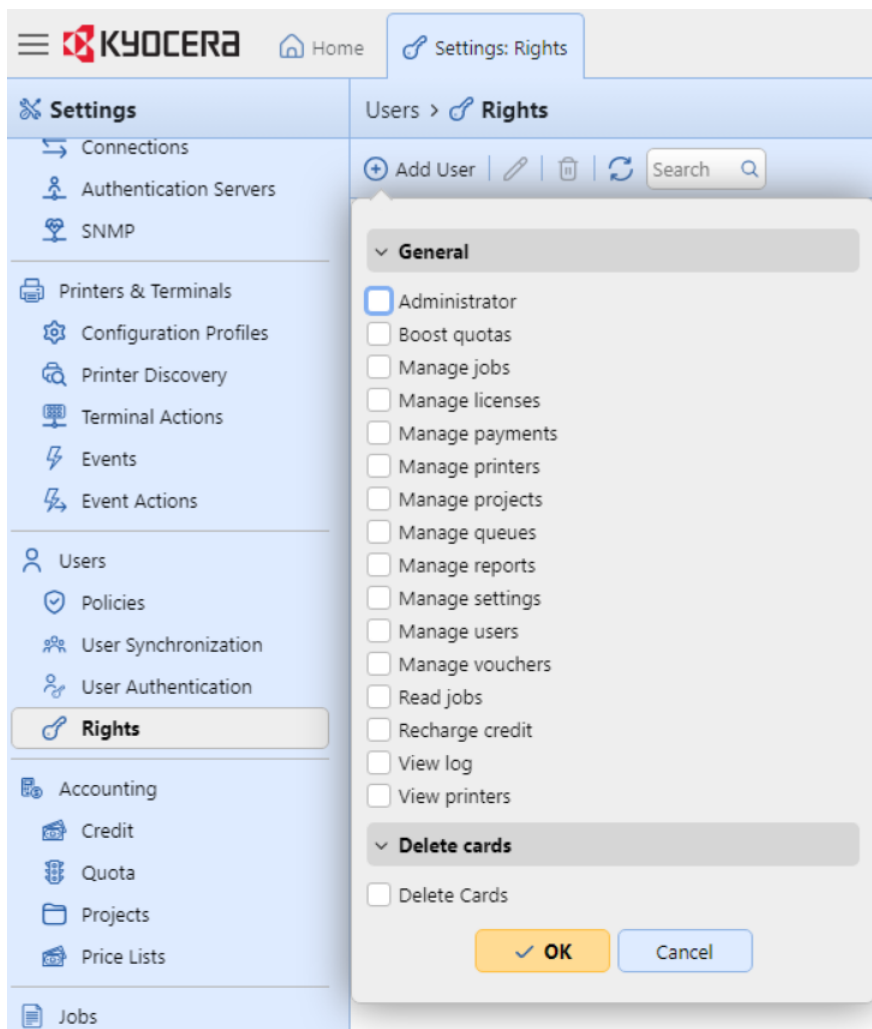
- **Add user** - add a new user or group with assigned rights.
- **Edit** - edit an existing user or group with assigned rights.
- **Delete** - delete a user or group with assigned rights.
- **Refresh** - refresh the list of users and groups.
- **Search** - search for a user or group with assigned rights. You can either use user names or rights for filtering your search results.

- If the server is used as a Site server, user rights are managed by the Central server. The rights are visible in the Site server's Rights settings, but are non-editable.

### 10.13.1 Providing users and groups with rights

To add a new user or a group of users to the list on the **Rights** settings tab:

1. Click **+Add User**. The Select user or group dialog box appears.
2. In the dialog box, select the user (or group) and click **OK**. The rights panel opens.
3. Select the user (or group) rights.
4. Click **OK**. The user (or group) appears on the list on the **Rights** settings tab along with the assigned rights.



## 10.13.2 Editing users' rights

To open the user rights properties panel (or the group rights panel), double-click the user (or the group) on the list of users and groups on the **Rights** settings tab. The panel appears on the left side of the screen.

In the user rights panel, under the **General** section, you can assign rights concerning the general run of **KNM**. These rights are described below:

- **Administrator** - The user is provided with administrator (\*admin) rights.
- **Boost quotas** - The user gets access to the **Quota Boosts** main tab.
- **Manage jobs** - The user can edit other users' jobs.
- **Manage licenses** - The user can view and manage **KNM** licenses on the **License** settings tab.
- **Manage payments** - The user gets access to the **Payments** main tab.
- **Manage printers** - The user gets access to the **Printers** main tab, to monitor printers and change their settings, as well as the **Printers & Terminals** settings tab and all its subsections, where they can modify settings.
- **Manage projects** - The user gets access to the **Projects** main tab, can add projects and change their settings.
- **Manage queues** - The user gets access to the **Queues** main tab and can change the settings there.
- **Manage reports** - The user can manage all reports.
- **Manage settings** - The user gets access to management of all settings on the **Settings** tab of the **KNM** Web interface except for the settings on the **Rights** tab.
- **Manage users** - The user gets access to the **Users** main tab, the **Users** settings tab and the **Policies** settings tab, can add users and change their settings and rights. The user also gets access to the **Accounting** settings tab, but cannot change the settings. Access to the **Credit** settings tab is granted, but the user is only allowed to change Users and Groups. Access to the **Quota** settings tab is granted, but but the user is only allowed to change Quota definitions, not Quota global settings.
- **Manage vouchers** - The user gets access to the **Voucher Batches** main tab.
- **Read Jobs** - The user can see other users' jobs.
- **Recharge credit** - The user gets access to the **Recharge credit** main tab.
- **View log** - The user can view the **KNM** log.
- **View printers** - The user gets access to the **Printers** main tab, to monitor printers.
- **Delete Cards** - If granted, the user has the **Delete all ID cards** button available on their User profile widget in the **KNM** web UI and they are able to delete all their ID cards.

## 10.14 Users Settings

In the **Users** settings tab (**KYOCERA, Settings, Users**), the **KNM** administrator can manage **KNM** users' **General** settings, **New user registration settings**, and **KNM Account lockout** options.

**Users**

**General**

Enable user profile editing:   
If enabled, user can change these properties: Full name, Email  
 Properties which can be changed always: Password, Default language

Show more info about user profile:   
Widget 'User profile' will contain more information

Enable personal queues settings:   
This functionality requires Scripting (PHP)

Enable delegate changes:

Enable deleting all ID cards:

**New user registration**

Register by swiping an unknown ID card:  Add to group:

Register in the Web user interface:  Add to group:

Register by receiving a job via LPR/IPPS/RAW protocols:  Add to group:

Register by receiving a job via email:  Add to group:

Register by receiving local job meta data (LPM):  Add to group:

> **Email for new registered users**

**Account lockout**

Attempts before lockout: \*

## General section

- **Enable user profile editing** - If enabled, users will be able to change their full name and email. For more information, check [Enable user profile editing](#).
- **Show more info about user profile** - If enabled, the User profile widget will contain more user-related information (Personal number, Phone, PIN, Card, Aliases, Notes).
- **Enable personal queues settings** - If enabled, users can use personal queues. For more information, check [Personal Queues](#).
- **Enable delegate changes** - If enabled, users will be able to change their delegates. For more information, check [Delegated Printing](#).
- **Enable deleting all ID cards** - If enabled, users will be able to delete all their ID cards.

If all of the above are enabled, the users can view additional user information, **Edit** their account, **Delete all ID cards**, and use **Personal Queues** in their User profile widget:

### User Profile

User name:	Carol Kai
Full name:	Carol Kai
Email:	carolkai@email.com
Default language:	-
Personal number:	-
Phone:	-
PIN:	✓
Card:	✓
Aliases:	-
Notes:	-

[Edit](#) [Set password...](#) [Generate PIN...](#) [Delete all ID cards](#) [Personal queues](#)

### New user registration section

In this section, the **KNM** administrator can enable automatic user registration to **KNM** in multiple ways, For more information, check [Automatic user registration](#).

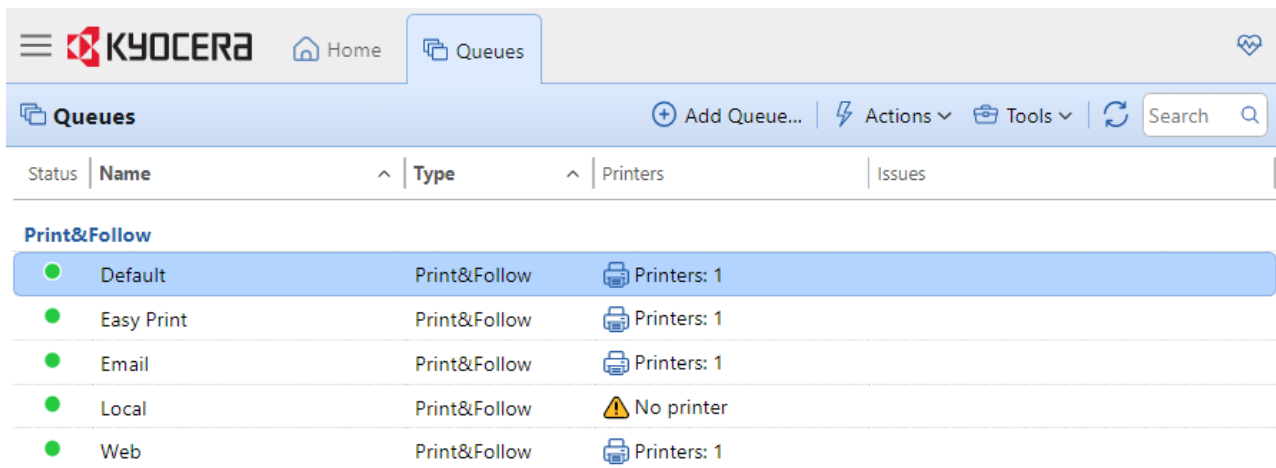
### Account lockout section

In this section, the **KNM** administrator can set the number of failed login **Attempts before lockout** (5 by default), and the **Lockout time** in minutes (15 minutes by default).

# 11 Queues

This topic discusses one of the key functions of **KNM**: setup and management of print queues. It covers the following subjects:

- Overview, adding and deleting queues: [List of queues](#), [Adding and deleting queues](#).
- Individual queues settings: [Editing queues](#).
- Direct, Tandem, Print&Follow, and Delegated printing queue types: [Queue types](#).
- Ways of detecting users: [User detection methods](#).
- You can create collections of watermarks and associate them with queues: [Watermarks](#).
- Some extra options for queues: [Advanced queue options](#).



Status	Name	Type	Printers	Issues
	<b>Print&amp;Follow</b>			
●	Default	Print&Follow	Printers: 1	
●	Easy Print	Print&Follow	Printers: 1	
●	Email	Print&Follow	Printers: 1	
●	Local	Print&Follow	No printer	
●	Web	Print&Follow	Printers: 1	

## 11.1 List of queues

On the **Queues** main tab, you can see queues and information about them. The queues are divided into groups according to their type: **Print&Follow**, **Direct**, **Tandem**, and **Delegated printing**.

Status	Name	Type	Printers	Issues
<b>Print&amp;Follow</b>				
●	Default	Print&Follow	Printers: 1	
●	Easy Print	Print&Follow	Printers: 1	
●	Email	Print&Follow	Printers: 1	
●	Local	Print&Follow	No printer	
●	Web	Print&Follow	Printers: 1	
<b>Direct</b>				
●	QueueX	Direct	No printer	
<b>Tandem</b>				
●	HQ	Tandem	No printer	
<b>Delegated printing</b>				
●	Assistants	Delegated printing	Printers: 1	

### 11.1.1 Default queues

After installing **KNM**, there are five default **Print&Follow** queues on the **Queues** main tab: **Default**, **Easy Print**, **Email**, **Local**, and **Web**.

- **Default:** Print&Follow queue where all users have access and all printers are assigned.
- **Easy Print:** Print&Follow queue using the Easy Print feature.
- **Email:** All jobs sent from email are assigned to this queue.
- **Local:** Used with locally connected printing devices (USB, LPT).
- **Web:** All jobs sent directly from the web user interface are assigned to this queue.

If you are using a **KNM** Central and Site servers environment, the following queues are also available by default:

- **Job Roaming:** Job Roaming enables users to transfer their jobs from one location to another. Jobs sent to one branch are automatically assigned to this system queue and can be printed on printing devices at any other branch. This queue can only be used in a **KNM** Central and Site servers environment; for more information, see the **KNM** Central Server Guide.
- **Job roaming delegated:** Delegated printing jobs used with job roaming are automatically assigned to this system queue. This queue can only be used in a **KNM** Central and Site servers environment; for more information, see the **KNM** Central Server Guide.

## 11.2 Queue types

For each queue, except for the default queues, you can select from four options as to what happens with the jobs that are sent there. This section describes these four queue types.

### 11.2.1 Direct queue type

A direct queue can have only one printing device assigned to it. Print jobs in this queue are sent directly to the printing device and are immediately printed.

When you add printers using printer discovery, you can automatically create a direct queue for every newly discovered device.

### 11.2.2 Tandem queue type

A tandem queue can be used on places with multiple printers and a higher printing volume. Jobs sent to this queue are evenly distributed among the devices and do not have to wait for one particular printer. This way, a large volume of print jobs can be spread between printers and printed in a significantly shorter time.

The queue can have multiple printing devices assigned to it. Print jobs from the queue are distributed among the printing devices that are not busy at the moment and they are immediately printed. If there are multiple idle printing devices, the print job is sent to the printer with the lowest printed pages counter.

To maintain a balanced printing device load, make sure that the printed page counters on all of the used printing devices are similar. Otherwise the printing devices with the lower printed page counter might be overused.

You can manually change the page counter on the **Printer total counter adjust for load balancing:** setting on the printing device properties panel on the **Printers** main tab. The number that you enter is added to the counter.

### 11.2.3 Print&Follow queue type

With this queue, users can send multiple jobs and print them when they want on any of the printers assigned to the queue.

The queue can have multiple printing devices assigned to it. All of the assigned printers have to be equipped with **KNM** terminals. Jobs sent to a Print&Follow queue are processed by the system and saved on the server.

Once the user logs in on any printer assigned to this queue, the print job is sent to this device and the user can print it.

To use a Print&Follow queue, an embedded terminal or a hardware terminal is required.

For more information on embedded terminals, see:

- **KNM** Embedded
- **KNM** Embedded Lite

### 11.2.4 Delegated printing queue type

The delegated printing feature enables users and groups of users to choose delegates who can print their print jobs. After the delegating user (or group of users) sends a job to the **Delegated printing** queue, all delegates can see the jobs and print them. For further information about the **Delegated printing** feature, see [Delegated printing](#).

The **Delegated printing** queue type works in the same way as the **Print&Follow** queue type, except that it supports the delegate printing feature.

The delegates do not need to have rights to the delegated printing queue where the job was sent.

## 11.3 Adding and deleting queues

### Adding a queue

1. On the **Queues** main tab, click **+Add queue**. The new queue properties panel opens on the right side of the screen.
2. On the panel, add a **Name** for the queue, select a **Type**, further modify the queue's settings (Queues general settings), and click **Save**.

### Deleting a queue

1. On the list of queues on the **Queues** main tab, select the queues that you want to delete, and then click **Actions** (or right-click the queue). The Actions drop-down box appears.
2. In the **Actions** drop-down box, click **Delete**. The queues disappear from the list.

## 11.4 Editing queues

Each individual queue has its own properties panel. To open the panel, double-click the queue on the list of queues on the **Queues** main tab (or right-click the queue, and then click **Edit**). The properties panel opens on the right side of the screen.

The screenshot shows the 'QueueX' configuration window with the 'General' tab selected. The window title is 'QueueX' and it has a close button (X) in the top right corner. The 'General' tab is highlighted, and other tabs like 'Job receiving', 'KYOCERA Net Manager Desktop Client', 'Job processing', 'Printers', and 'Rights' are visible. The 'Queue' section is expanded, showing the following settings:

- Name:** \* QueueX (with a text box containing 'QueueX' and a tooltip: '[a-Z] [0-9] . - \_ ^ \* \$ { }', 'Use this name also as the queue name in the LPR port settings in the print driver', and 'Only 32 character long name is allowed by Windows driver')
- Type:** \* Radio buttons for Direct, Tandem, Print&Follow (selected), and Delegated printing.
- Priority:** (empty text box)
- Keep jobs for reprint:** \* Yes (dropdown menu)

The 'Output to printer' section is also expanded, showing:

- Protocol:** \* Raw (dropdown menu)
- Port:** \* 9100 (text box)
- Use Fiery if available:**

The 'Policies' section is collapsed. At the bottom, there are 'Save' and 'Cancel' buttons.

The basic setup of a queue can be done in four tabs: the **General** tab, the **Job receiving** tab, the **Printers** tab, and the **Rights** tab.

### General tab settings

- **Name** - Enter a name for the queue. This is an essential parameter for directing print jobs to **KNM** and it is part of the print port setting. It is unique, case sensitive and cannot contain diacritics and spaces. This entry is mandatory.
- **Type** - Select a type for the queue. The available queue types are: *Direct*, *Tandem*, *Print&Follow*, and *Delegated Printing*. For more information, see [Queue types](#).

### Job receiving tab settings

- **User detection method** - Here you can set the user detection method. For more information, see [User detection methods](#).

- **Get job name from PJJ** - This gives you the option to discard a job when it comes without metadata.

The screenshot shows the QueueX configuration window for 'Job receiving'. The 'Job parsing' section is expanded, revealing several settings:

- Default printer language:** Set to 'Autodetect'. A note states: 'If there is no PJJ in the job specifying the print language, the default language is assumed.'
- Discard the job if no metadata:** An unchecked checkbox.
- User name is case sensitive:** An unchecked checkbox.
- User detection method:** Set to 'KX Driver/Kyocera Mobile Print'.
- Regular expression:** An empty text input field.
- Get job name from PJJ:** A checked checkbox.

Below the 'Get job name from PJJ' checkbox, there are buttons for '+ Add', 'Edit', 'Test', and a trash icon. A table lists the following PJJ variables:

PJJ Variable	Regular expression
JOBNAME	
JOB NAME	
SET JOBNAME	

At the bottom of the dialog are 'Save' and 'Cancel' buttons.

### Printers tab settings

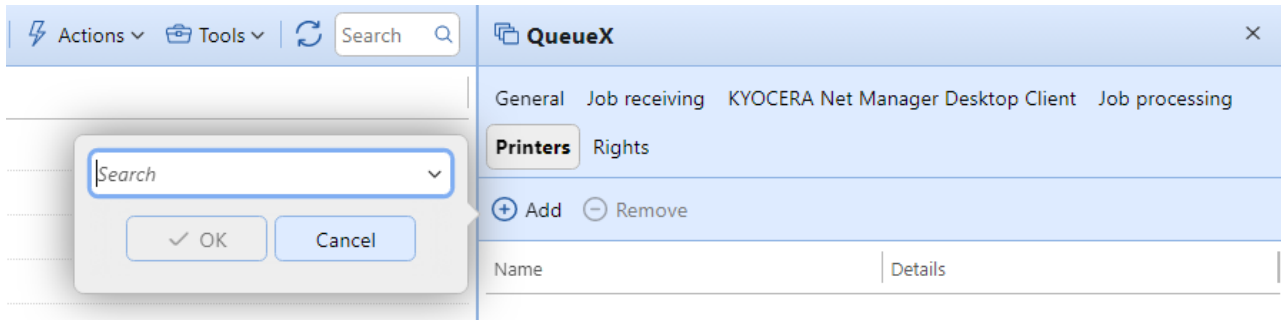
By default, the **All printers** group is automatically assigned to every queue. You can delete this group to restrict the number of assigned printers.

To add a printing device or a group of printing devices to the queue:

1. On the bar at the top of the **Printers** tab, click **+Add**. A search dialog box appears.
2. In the dialog box, find the printing device (or group of printing devices) that you want to add to the queue, and then click **OK**.

To remove a printing device or a group of printing devices from the queue:

1. On the bar at the top of the **Printers** tab, select the printing device (or group of printing devices), and then click **Remove**. The printing device (or group of printing devices) disappears from the **Printers** tab.

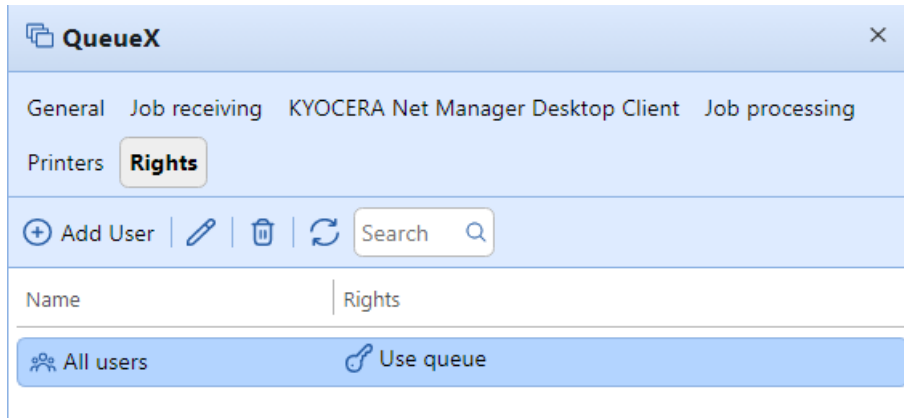


### Rights tab settings

By default, the **All users** group is automatically assigned to every queue. You can delete this group to restrict the number of users with the right to use the queue.

To provide a user or a group of users with rights to the queue:

1. On the bar at the top of the **Rights** tab, click **+Add User**. The Select user or group dialog box appears.
2. In the Select user or group dialog box, select the user (or group of users) that you want to provide with rights to the queue, and then click **OK**.



To remove the rights to the queue from a user or a group of users:

1. On the **Rights** tab, select the user (or group of users), and then click the remove button (X). The user (or group of users) disappears from the **Rights** tab.

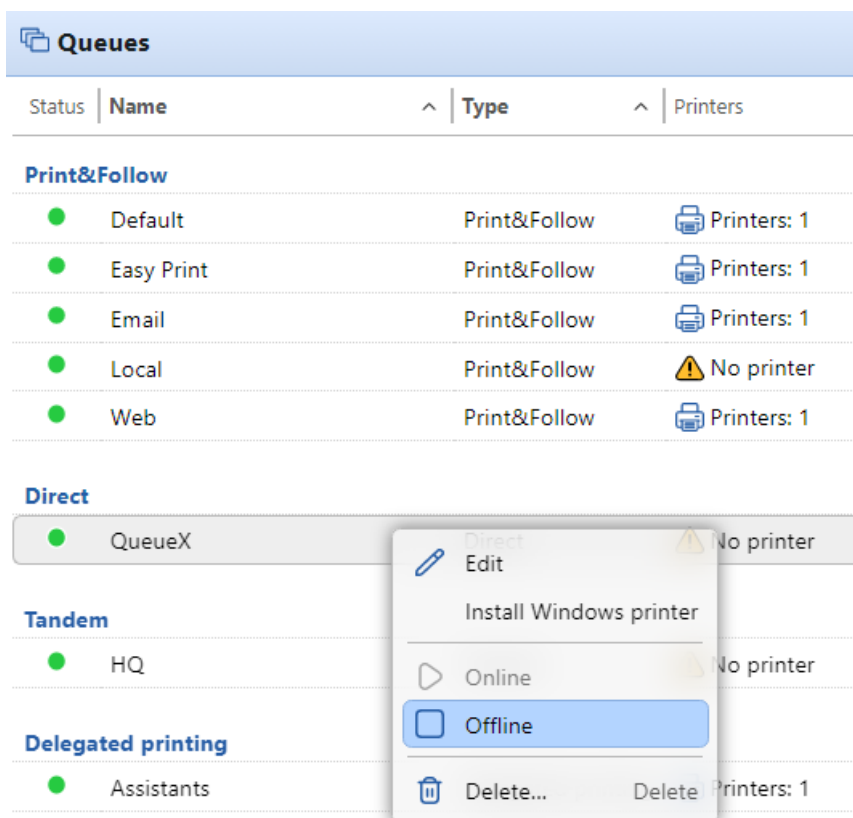
## 11.5 Online/Offline queues

While the default queues are always online, each of the manually added queues can be switched to the offline mode. Queues switched to the offline mode do not receive any print jobs. However, users can still print jobs that are already waiting in these queues.

Jobs sent to an offline queue are rejected with the log message: *"Unknown or inactive queue '!...!. The job was discarded."* displayed in the log, on the **Log** main tab of the **KNM** Web Interface.

To switch between the online and offline mode of a queue:

1. Select the queue from the list on the **Queues** main tab, and then click **Actions** (or right-click the queue). The Actions drop-down box appears.
2. In the Actions drop-down box, click **Offline** (or **Online**). The queue switches to the offline or (online mode).



## 11.6 Personal Queues

Personal queues in **KNM** enable users to select the queues where their print jobs are sent to. The users can create multiple queues to ascertain that at least one of them has available printing devices where the job can be released.

If a user is not allowed to send the job to the currently checked personal queue, **KNM** skips it and moves to the next one. If all personal queues are skipped, the job is sent to the queue set on the print port.

### 11.6.1 Activating the feature

To activate personal queues:

1. On the **Users** settings tab, select the **Enable personal queues settings** option.
2. On the properties panel of the queue where the user's jobs are sent to by the print driver, add the PHP script shown below. The script moves the jobs to the first available personal queue of the user.

```
// get all user's queues sorted by priority
$personalQueues = $this->owner->personalQueues;
// loop them
```

```
foreach ($personalQueues as $q) {  
  // skip queue if no printer is available  
  if ($q->isAnyPrinterAvailable() === false) {continue;}  
  // queue printer is available, move job to queue  
  $this->moveToQueue($q->name);  
  // job is moved, stop the loop  
  break;}  
}
```

After the feature is set up, each user can see a button for setup of their personal queues on their account on the **KNM** Web Interface.

## 11.6.2 Setting personal queues

Once the feature is activated, both the **KNM** users and the **KNM** administrator can add and delete personal queues.

### **KNM Users**

Users add and delete the personal queues on their user account on the **KNM** Web Interface. To do this, they need to log in to the interface, then click **Personal queues** there, and lastly set the queues in the Personal queues dialog box.

After the user sends the job, **KNM** checks the personal queues and sends the job to the first queue with available printing devices.

### **KNM Administrator**

The **KNM** administrator adds and deletes the user's personal queues on the **Queues** tab of the user's properties panel on the **Users** main tab in the **KNM** Web Administrator Interface. To access the tab, open the **Users** main tab (**KYOCERA, Users**), then double-click the user (or right-click the user, and then click **Edit** on the shortcut menu) to open the properties panel, and lastly click **Queues** on the panel.

On the **Personal queues** section, add and/or delete personal queues for the user.

Carol Kai		⚡ Actions ▾	✕
General Groups Queues Delegates			
Name	Type		
Assistants	Delegated printing		
Default	Print&Follow		
Easy Print	Print&Follow		
Email	Print&Follow		
HQ	Tandem		
QueueX	Direct		
Web	Print&Follow		

**Personal queues**

The queue at the top of the list has the highest priority

Personal queues:

- QueueX
- Assistants • Delegated printing
- HQ • Tandem
- QueueX • Direct

## 11.7 Advanced queue options

Once you have created a queue and set the basic options, like the name, type, printers and rights assignments, you can select some of the more advanced queue and job management features:

- General
- Job receiving
- Job processing
- KYOCERA Net Manager Desktop Client
- Job Scripting

### 11.7.1 General tab

Available advanced settings on a queue's general tab:

#### Queue section

- **Priority:** When multiple jobs from Print&Follow queues are to be released at the same time, the jobs that are sent to the queues with a higher priority are released before the jobs with lower

priority. For example, if there are three jobs waiting to be released on a printing device, one with a priority number 0, one with a priority number -1 and one with a priority number 2, the job with the priority number 2 is printed first, the job with the priority number 0 is printed second and the job with the priority number -1 is printed third.

- **Keep jobs for reprint:** *Yes, No*. The **Keep jobs for reprint** setting is also available when configuring a Print Job Policy. You can find the available combinations in [Print Job Policies](#).

### Output to printer section

- **Protocol:** By default, print jobs are sent from **KNM** to printing devices via the Raw protocol. Instead of it, you can use one of the alternative standard protocol options (*IPP, IPPS* or *LPR*) or the **KNM** printing protocol, which can be used in two versions:
  - **MPP:** jobs sent via this protocol are compressed
  - **MPPS:** jobs sent via this protocol are compressed and encrypted via SSL
- **Port:** Here you can change the port of the selected protocol.
- **Use Fiery if available:** If you use a Fiery module for processing Postscript jobs, make sure that this option is selected and set the IP address of the module on the properties panel of the printing device to which the module is connected. Otherwise, you can deselect the option.

### Policies section

The final job settings are a combination of these queue settings, user policies and user changes made on the embedded terminal. All settings are set to *Do not change* by default.

- **Color:** *Do not change, Color, B&W*
- **Duplex:** *Do not change, Simplex, Duplex long edge, Duplex short edge*
- **Staple:** *Do not change, No, Yes*
- **Punch:** *Do not change, No, Yes*
- **Toner saving:** *Do not change, No, Yes*

## 11.7.2 Job receiving tab

On the **Job receiving** tab of each queue, you can set how a job is parsed and other job receiving options.

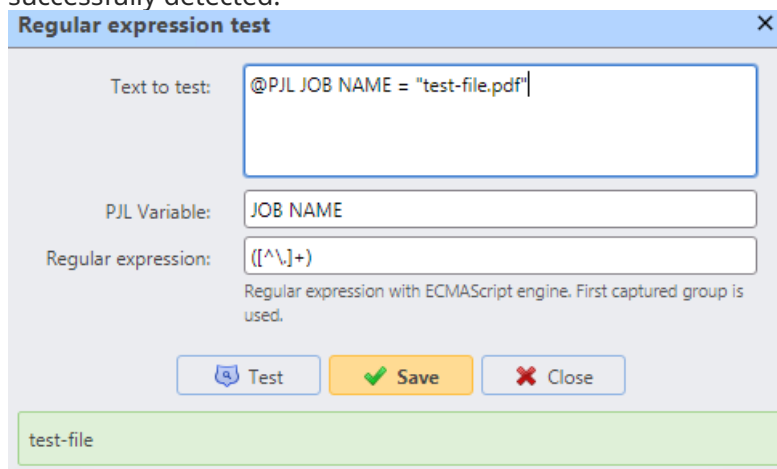
### Job parsing section

- **Default printer language:** Choose the default printer language from the drop-down menu. The available options are:
  - **Unknown**
  - **Autodetect** (default setting)
  - **PCL 5**
  - **PostScript**
  - **ESC/P**
  - **Prescribe**
  - **PCL 6**
  - **PDF**
  - **JPEG**
  - **XPS**If there is no PDL in the job specifying the print language, the default language is assumed.
- **Discard the job if no metadata:** If this option is selected, **KNM** discards all jobs that do not contain metadata from the Job Parser. It can be used together with the **Credit** or **Quota** features to prevent printing jobs without necessary information (number of pages, color etc.). When a job is discarded due to this setting, the following message appears in the **KNM** Log: "*Job*

metadata is required for the queue but the job parser is turned off. Job is canceled. | `queue=QueueX`". If you select this option, make sure that the Job Parser is enabled. In new installations the Job Parser is activated by default.

- **User name is case sensitive:** 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 should select the **User name case sensitive** option. With this option selected, **KNM** differentiates between two users that differ only in the case used. For example, if the user *Juliette* is registered in **KNM** (and the user *juliette* is not) **KNM** rejects jobs sent from the OS account *juliette*.
- **User detection method:** Select how the job owner is identified. Described in detail in [user detection methods](#).
- **Regular expression:** You can use regular expressions to capture a part of the string that **KNM** detects within any of the user detection methods. **KNM** uses regular expressions with the ECMAScript engine, meaning that the first captured group is used: first, **KNM** finds the first match for the regular expression, and then it identifies the job owner with the first 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.
- **Get job name from PJJL:** With this option enabled, **KNM** takes the job name from the `@PJJL JOB NAME` parameter in the PJJL header instead of detecting it from the LPR protocol. Click **+Add** to enter PJJL variables and regular expressions, **Edit** to modify any existing variables, **Test** to actually test if your regular expressions work, and **X** to delete a variable/regex set. The job name in the PJJL header may differ from the printed document's name. In the below example, you can see how a variable/regex set works, and if it manages to find the job name from the PJJL header:
  - In the **Text to test** field, there should be the text from the print job's PJJL header: `@PJJL JOB NAME = "test-file.pdf"`
  - In the **PJJL Variable** field, there should be the `JOB NAME` variable, or any other variable used to detect the job name.
  - In the **Regular expression** field, there should be the regular expression you want to use in order to detect the job name. In the example, the `([^\.]*)` regex takes all characters before it reaches dot (which is specified as `\.` - backslash is required in case of dot, because it is one of the special characters).

After clicking **Test**, the test result is displayed at the bottom. In this example, *test-file* was successfully detected.



- **Get computer name from PJJL:** With this option enabled, **KNM** takes the computer name from the PJJL header instead of detecting it from the LPR protocol. Click **+Add** to enter PJJL variables

and regular expressions, **Edit** to modify any existing variables, **Test** to actually test if your regular expressions work, and **X** to delete a variable/regex set.

In the below example, you can see how multiple variable/regex sets work, and if **KNM** manages to find the computer name from the PJL header:

- In the **Text to test** field, there should be the text from the PJL header:  
`@PJL SET JOBATTR = "JobAcct1=user"`  
`@PJL SET JOBATTR = "JobAcct2=NB-XYZ"`  
`@PJL SET JOBATTR = "JobAcct3=KNM"`
- In the **PJL Variable** field, there should be the `SET JOBATTR` variable, or any other variable used to detect the computer name.
- In the **Regular expression** field, there should be the regular expression you want to use in order to detect the computer name. In the example, there are three attributes, so the `JobAcct2=(.*)` regex is supposed to search and take all the characters from the `JobAcct2` attribute.

After clicking **Test**, the test result is displayed at the bottom. In this example, `NB-XYZ` was successfully detected.

## Jobs via Raw protocol section

The RAW protocol is the default protocol for systems that do not use Windows OS and for standard TCP/IP.

The advantage of this protocol is that it sends data without further processing and has smaller packet headers.

As RAW comes without any job metadata, you must use a different port for each queue (starting from port 9100). The used ports are added to Windows Firewall.

Click **+Add** next to **Port** and select a port.

Make sure that the queue has the following settings:

- **User detection method:** Select *User detection from PJL*, *KYOCERA Net Manager Desktop Client* or *Detect user from the job name*
- If *User detection from PJL* is selected, **+Add** the desired PJL variable(s) and regular expression(s)

**i** Because there are no metadata, the queue is determined by the TCP port, the user always from the PJL and the sending computer is the client's IP address.

## Jobs via hot folder section

In this section, you can associate the queue with one or multiple network folders where print jobs are stored.

If the folder is password protected, **KNM** will use the credentials of the account **KNM** service is running under.

The **KNM** server will regularly monitor the network folder for new files. If there is new job in the folder, the **KNM** server checks if it is supported for printing. Supported files will be downloaded and deleted from the folder, unsupported files will be deleted. The operation is logged in the **KNM** log ("*job 123.prn was downloaded from \\serverXYZ\folder1*", "*job 123.cpr was deleted from \\serverXYZ\folder1, file type is not supported*").

- Directly supported files: **.prn, .pcl, .ps, .eps, .pdf, .jpg, .bmp, .tif, .png, .txt**
- MS Office files are supported, but they are converted to PDF: **.doc, .docx, .xls, .xlsx, .ppt, .pptx, .odt, .ods, .odp**


Only the following user detection methods can be used: *Job sender*, *Detect user from the job name*, *User detection from PJI*.

Click **+Add** next to **Hot folder** and type the folder path.

## Jobs via MS Universal Print

In this section, you can associate the queue with MS Universal print.

To do that, set the option to **Enabled**, and click **Save**. After a few minutes, your queue will be available as a virtual printer in MS Azure Universal Print.

 To use this option, you first need to set up [MS Universal print](#).

## Jobs via AirPrint and Mopria

In this section, you can make the queue available in AirPrint and Mopria.

Switch **Enabled** on, and click **Save**.

 Only the *Job sender* user detection method can be used with this queue.

## User detection methods

One of the essential **KNM** functions is to identify the owner of a sent print job. You can select from a number of identification options. The most common way is to identify the user as the OS account where the job was sent from (*Job sender*). If there are many users who send their jobs from one account, you can use one of the three authentication options: *prompt for a PIN/card*, *prompt for a username and password* or *prompt the user to select from a list*.

Apart from the above-mentioned options, **KNM** offers several advanced identification options that can be used in special cases, such as if you want to use a DNS server to identify the user's computer or detect the user from the job name.

The available user detection methods are:

- [Job sender](#)
- [Sender's computer name](#)
- [Print server's DNS name](#)
- [Sender's computer DNS name](#)
- [Detect user from the job name](#)
- [KYOCERA Net Manager Desktop Client](#)
- [User detection from PJI](#)
- [KX Driver/Kyocera Mobile Print](#)

### Job sender

The basic and most common user detection method option is to identify the owner as the OS user account where the job was sent from.

If the user logs on the account **Eliot.Kate** and sends the job from there, **KNM** identifies them as **Eliot.Kate**.

### Sender's computer name

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

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 alternative options, please contact your support.

A regular expression can be used to capture a part of the detected string.

Computer name, domain, and workgroup settings				
			Computer name:	NB227
			Full computer name:	NB227-printserver
			Computer description:	
			Domain:	printserver
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

### Using a DNS server to resolve the job owner

With the two user detection method 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=WINGOMOSMT0AO9, .local   project=   name=user16   hostname=10.1.3.110   queue=Test
------------	------	---------	-----------	---

2. **Sender's computer DNS name:** The computer where the job is sent from. 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
------------	------	---------	-----------	---

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* where the user prints from, 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. laptop100.domain.com.

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

A regular expression can be used to capture a part of the detected string.

### Detect user from the job name

With the **Detect user from the job name** option, the job owner is identified with the name of the print job. This method can be used 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*.

The **Only for LPR user** setting is displayed after you select the **Detect user from the job name** option. This setting allows you to combine the **Detect user from the 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, the job owner is identified with the job name.


This advanced user identification method 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 the 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 cases, you can enter the user *SYSTEM* in the **Only for LPR user** text box. **KNM** detects the sender and if it is *SYSTEM*, it identifies the job owner as the job name.

### KYOCERA Net Manager Desktop Client

This option is available on computers with either Windows or macOS. It requires the **KYOCERA Net Manager** Desktop Client application running on the computer where the print job is sent from.

When a user sends a job to this queue, the job is automatically paused on the **KNM** server and remains in the **Paused** status with the *\*unauthenticated* user as the job owner, until the user authenticates themselves via the **KNM** Desktop Client application. Depending on the setting of the application's **Authentication method**, the user is prompted to either enter their PIN, swipe their card at a card reader, enter their user name and password, or select themselves on the list of all **KNM** users. After the user is authenticated, the job's status on the **KNM** server is changed to **Ready** and the job owner changes to the correct user name and it can be printed. If the user fails to authenticate themselves in **KNM** Desktop Client, the job is rejected.

For information on how to install and set up **KNM** Desktop Client, see the **KNM** Desktop Client for Windows or macOS manuals.

 In cases where there is no card reader connected to the computer where the users identify themselves from, users can type the card number instead of swiping it.

### User detection from PjL

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

```

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

```

To select the line that is used for the definition of the job owner, click **+Add** and enter the variable (*SET USERNAME*) in the **PJL Variable** field. You can enter multiple variable/regex sets by clicking **+Add** for each one in a new line. **KNM** tries to find a PJL line containing the first defined 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.

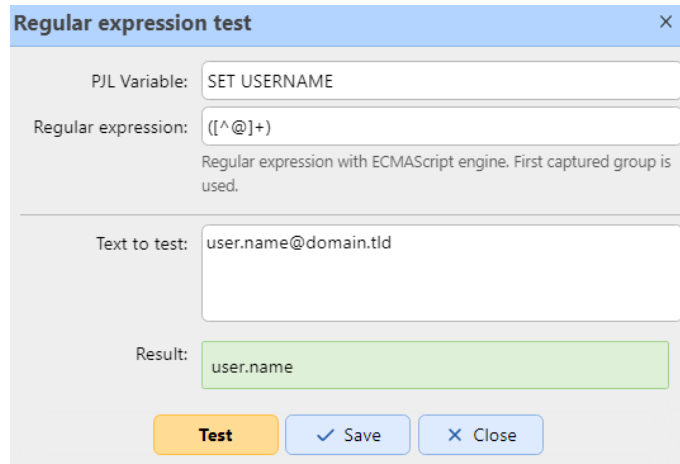
A regular expression can be used to capture a part of the detected string. If no regular expression is specified, the whole string of the PJL variable is used.

Click **Edit** to modify any existing variables, **Test** to actually test if your regular expressions work, and **X** to delete a variable/regex set.

In the below example, you can see how a variable/regex set works, and if it manages to find the user by searching for the username in the email address from the PJL header:

- In the **Text to test** field, there should be the text from the print job's PJL header:  
*user.name@domain.tld*
- In the **PJL Variable** field, there should be the *SET USERNAME* variable, or any other variable used to detect the job owner.
- In the **Regular expression** field, there should be the regular expression you want to use in order to detect the user name. In the example, the *([^\@]+)* regex checks if a character is not "@" and uses it, and "+" means to proceed with the next character. The result is that it takes all characters before it reaches "@".

After clicking **Test**, the test result is displayed at the bottom. In this example, *user.name* was successfully detected.



**Regular expression test** [X]

PJL Variable:

Regular expression:

Regular expression with ECMAScript engine. First captured group is used.

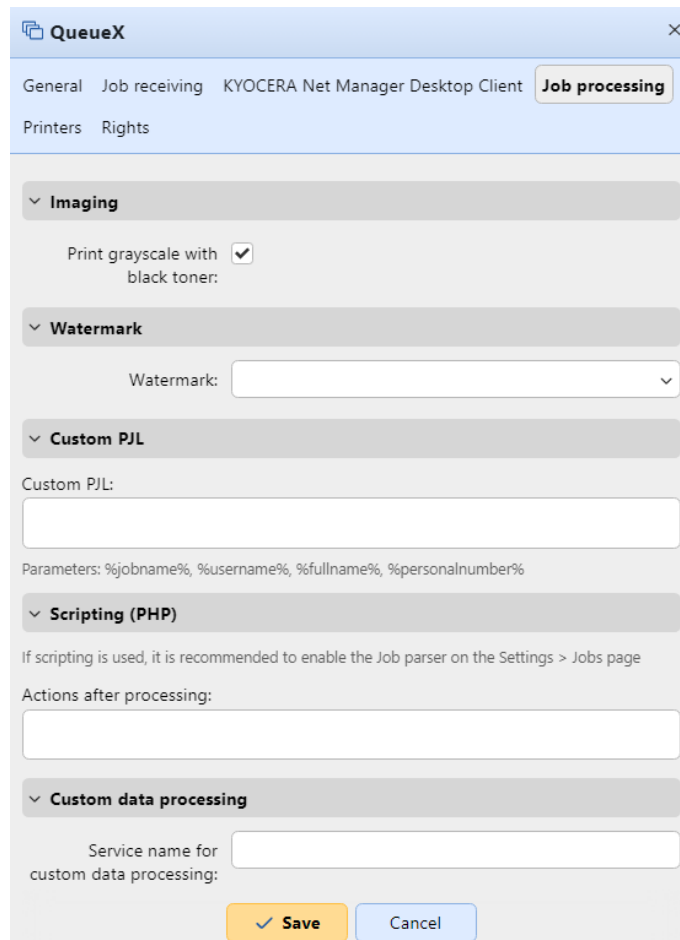
---

Text to test:

Result:

### 11.7.3 Job processing tab

On the **Job processing** tab of each queue, you can enforce additional job processing actions by selecting one or more of the predefined job settings or by creating any number of custom PJL commands.



**QueueX** [X]

General Job receiving KYOCERA Net Manager Desktop Client **Job processing**

Printers Rights

▼ **Imaging**

Print grayscale with  black toner:

▼ **Watermark**

Watermark:

▼ **Custom PJL**

Custom PJL:

Parameters: %jobname%, %username%, %fullname%, %personalnumber%

▼ **Scripting (PHP)**

If scripting is used, it is recommended to enable the Job parser on the Settings > Jobs page

Actions after processing:

▼ **Custom data processing**

Service name for custom data processing:

#### Imaging section

Mark the checkbox if you want to **Print grayscale with black toner**.

### Watermark section

Choose your saved watermarks from the **Watermark** drop-down.

### Custom PJI section

In the **Custom PJI** field, you can set custom PJI commands to enforce other actions or provide additional information to the **KNM** server. For example, you can use `@PJI SET PAPER=A4` to enforce the A4 paper format or `@PJI COMMENT="USERDOMAIN:somedomain.com;"` to provide the **KNM** server with the information about the domain of the printing user.

You can also use the following **KNM** variables: `%jobname%`, `%username%`, `%fullname%`, `%personalnumber%`.

When you enter your own PJI sequence, it is necessary to enter the correct syntax. The command should always start with **@PJI**.

To be applied, a PJI command has to be supported by the printing device where the job is released. The information on what PJI commands are supported by a particular model of printing devices can be found in the documentation provided by the device manufacturer.

### Scripting (PHP) section

You can use PHP scripts to further process the job after it is received by the **KNM** server. Together with the PJI options and customizable queues, PHP scripting provides you with a large variety of job management options, such as the distribution of jobs between printing devices based on their size or color.

Scripting is detailed in [Job Scripting](#).

### Prologue/epilogue section

You can find further details in [Prologue/epilogue](#).

## Prologue, Epilogue

Some printing devices brands support the Prescribe PDL (page description language), which can be used to set up special rules for additional modification of the printed output. For example, you can use Prescribe to add a custom header or footer to selected document pages or to the whole document.

In **KNM**, these rules are part of the options available on the properties panels of print queues. For each queue, you can create custom rules by importing a text file with a set of Prescribe commands and selecting the part of the printed document the commands should be applied to.

Multiple rules can be defined for each queue.

### Adding, editing, and deleting rules

The rules can be added and edited in the **Job processing** tab, on the **Prologue/epilogue** section of a queue's properties panel.

Go to the **Queues** main tab (**KYOCERA, Queues**), right-click on the queue where you want to set up the rules, and click **Edit** (or select the queue, click **Actions** on the bar at the top of the tab, and then click **Edit**, or double-click on the queue).

### Adding rules to a queue

1. Open the queue's properties panel.
2. On the panel, click **Job processing**. The Job processing tab opens.
3. On the tab, in the **Prologue/epilogue** section, click **+Add**. A panel with the settings of the new rule opens at the bottom.
4. Set up the rule (see editing a rule below), and then click **Save**. The new rule is added to the list of rules on the **Prologue/epilogue** section.

### Editing a rule

To open the settings of a rule, double-click the rule on the **Prologue/epilogue** section. The settings open at the bottom of the panel.

The available settings are:

- **Place:** The object defined by the Prescribe code can be placed to the *beginning of the document*, *end of the document*, *beginning of selected pages*, or *end of selected pages*.
- **Page type:** Here you can select the pages the Prescribe code will apply to: *All pages*, *Odd pages*, *Even pages* or *Custom pages*.
- **Custom Pages:** Here you can further specify the pages the Prescribe code will apply to.
- **File:** Here you can upload the text file with the Prescribe code.
- **Encoding:** Here you have to select the encoding that is used in the text file with the Prescribe code.
- **Description:** Here you can type a description of the rule. You will see this description in the rules overview.

### Deleting a rule

1. Open the queue's properties panel.
2. On the panel, click **Job processing**. The Job processing tab opens.

3. On the tab, in the **Prologue/epilogue** section, select the rule, click **Delete**, and then confirm the action in the confirmation dialog box. The rule is removed from the panel.

## 11.7.4 Job Scripting

PHP scripts can be used to further process a job after it is received by the **KNM** server ([Job Processor Scripting](#)) or to provide users with basic interaction options via **KYOCERA Net Manager** Desktop Client ([User Interaction Scripting](#)). An overview of classes and functions used can be found in [Job Scripting Reference](#).

### Job Processor Scripting

A Job Processor script is a PHP code, which runs in the context of a job being processed. The script runs after a job has been parsed and all user/queue policies have been applied. It runs before the job is made *ready* or *paused*.

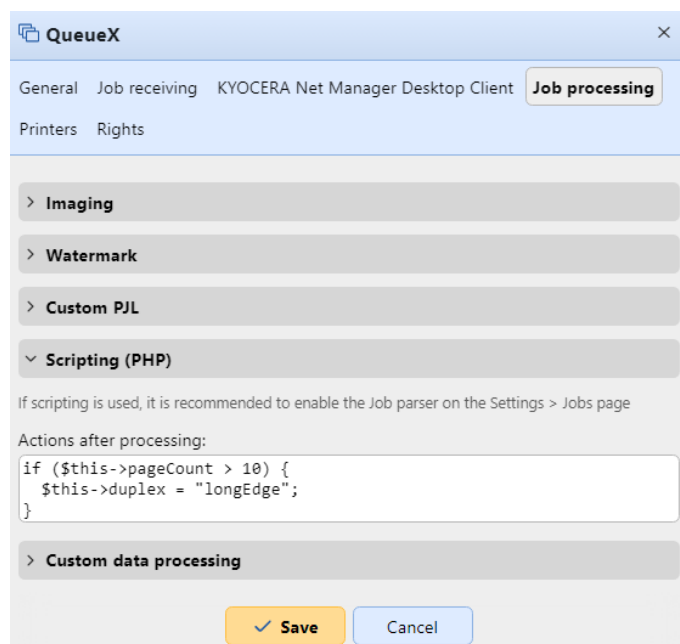
The typical usage of the script is the modification of the job based on its properties. For example:

```
if ($this->pageCount > 10) {  
    $this->duplex = "longEdge";  
}
```

In this example, if the job has more than 10 pages, it's released as duplex. *\$this* is the job being processed. It's an instance of the *Job* class.

Basic PHP functions can be used. For **KNM** specific classes and functions, see [Job Scripting Reference](#).

To set up processing via the PHP script, go to the properties panel of the queue where you want to use it, open the **Job processing** tab, and go to the **Scripting (PHP)** section. Under **Actions after processing**, enter the script in the box.



The screenshot shows the 'QueueX' configuration window with the 'Job processing' tab selected. The 'Scripting (PHP)' section is expanded, showing a text area for 'Actions after processing' containing the PHP code: `if ($this->pageCount > 10) { $this->duplex = "longEdge"; }`. Below the text area are 'Save' and 'Cancel' buttons.

## PHP scripts actions examples

In this section you can find examples covering a variety of job management options. These examples should give you an idea about how to use the PHP scripting in **KNM**. You can also substitute the properties and methods in the examples to use them as building blocks of more complex scripts.

### Actions based on the number of pages

Move jobs with a higher number of color pages to a monochrome queue.

```
if ($this->colorCount>20) {  
    $this->moveToQueue("ForceMonochrome");  
}
```

Delete jobs with a large number of pages.

```
if ($this->pageCount>500) {  
    $this->delete();  
}
```

### Actions based on the size of the job

Move large jobs to a dedicated queue.

```
if ($this->dataSize>1000000) {  
    $this->moveToQueue("LargeJobs");  
}
```

Delete oversized jobs.

```
if ($this->dataSize>5000000) {  
    $this->delete();  
}
```

### Actions based on paper format

Move jobs with the A3 paper format to a dedicated queue.

```
if ($this->paper===6) {  
    $this->moveToQueue("LargePaperFormat");  
}
```

### Actions based on the job owner

Move jobs of a certain owner to a dedicated queue.

```
if ($this->owner->name==="eliot.kate") {  
    $this->moveToQueue("EliotKate");  
}
```

Change the owner of the job.

```
if ($this->owner->name=="eliot.kate") {  
    $this->owner=KNM()->getUserByUserName("simon.kate");  
}
```

### Actions based on the duplex property

Move duplex jobs to a duplex queue.

```
if ($this->duplex) {  
    $this->moveToQueue("Duplex");  
}
```

Move simplex jobs to a simplex queue.

```
if ($this->duplex===false) {  
    $this->moveToQueue("Simplex");  
}
```

### Actions based on the color property

Move color jobs to a color queue.

```
if ($this->color) {  
    $this->moveToQueue("Color");  
}
```

### Actions based on the job name or the source application

Move jobs printed in MS Word to a dedicated queue.

```
if (strpos($this->name,"Microsoft Word")!=false) {  
    $this->moveToQueue("MSWord");  
}
```

Delete jobs sent from Facebook.

```
if (strpos($this->name,'Facebook")!=false) {  
    $this->delete();  
}
```

### Actions based on the rights to a queue

Move jobs of users who are not allowed to print to one queue to a different queue

```
if ($this->owner->canPrintToQueue(Color)===false) {
    $this->moveToQueue(Monochrome);
}
```

### Actions based on group membership

Move jobs sent by members of a group to a dedicated queue

```
if ($this->owner->hasGroup(Clerks)) {
    $this->moveToQueue(Clerks);
}
```

### Actions based on the PDL of the job

Move all jobs sent in a certain PDL to a dedicated queue

```
if ($this->lang===0) {
    $this->moveToQueue(UnknownPDL);
}
```

### Sending custom log messages to KNM

Send a log info message to KNM Log

```
KNM()->logInfo("This message appears in the KNM log.");
```

### Complex actions

If the number of pages multiplied by the number of copies exceeds a certain number, delete the job and inform the user

```
// get the number of pages and the number of copies
$page_number = $this->pageCount; $copies_number = $this->copies;
// if total (pagescopies) exceeds 500, delete the job and notify its owner
if ( $page_number $copies_number>500) {
    $this->delete(); $this->owner->sendNotification("error","Job refused", "Cannot
print jobs exceeding 500 pages.");
}
```

Move the job to a queue, if allowed

```
if ($this->color) {
    if ($this->owner->canPrintToQueue("JPS2")) {
        $this->moveToQueue("JPS2");
    } else {
```

```

        $this->owner->sendEmail("Job error", "Color printing denied");
        $this->delete();
    }
}

```

Move the job to the first available personal queue

```

// get all user's queues sorted by priority
$personalQueues = $this->owner->personalQueues;

// loop them
foreach ($personalQueues as $q) {
    // skip queue if no printer is available
    if ($q->isAnyPrinterAvailable() === false) {
        continue;
    }

    // queue printer is available, move job to queue
    $this->moveToQueue($q->name);
    // job is moved, stop the loop
    break;
}

```

## User Interaction Scripting

A User Interaction Script allows to program an interaction with the job owner and modify the job based on the user's response. Specifically, it allows to display a series of UI dialogs with questions and action buttons (*YES/NO*, *PRINT/NO*, *YES/NO/CANCEL*). Depending on the user selection, further dialogs can be displayed and actions can be taken. Finally when the last dialog is processed, the script is finished and the job is set as *ready* and can be released.

If a User Interaction Script is present, it must be first successfully executed before the job can be released. The job is forced in the *pause* state until then.

Basic PHP functions can be used, and almost all of those described in [Job Scripting Reference](#). The only two methods not supported by the feature are `$this->job->setPrinted()` and `$this->job->pause()`. Apart from the common classes, methods, and properties, you can use several additional functions to communicate with the **KNM** Desktop Client application.

### How to write a User Interaction Script

On the **KNM** Desktop Client tab of a queue, in the **User Interaction** section, add the script in the field, and click **Save**.

First, you need to define the `main()` function. This function decides if the dialog box should be opened (under which conditions) and which dialog box should be shown.

Then you can define on-click functions with reactions to the selected option: `onYes()`, `onNo()`, `onPrint()`, `onCancel()`.

Public properties are kept between calls. In fact, they are sent to the client and back.

### Script Structure

See the following script:

```
public $hasMoreThan10pages;

// script entry point
function main() {
    /** Job object */
    $job = $this->job;
    $this->hasMoreThan10pages = $job->pageCount > 10;
    // Show dialog if the job has more than 10 pages
    if ($this->hasMoreThan10pages === true) {
        $this->dialogYesNo("Job has more than 10 pages. Do you want to print in
duplex?");
    }
}

// If yes clicked
function onYes() {
    // $this->hasMoreThan10pages is available also here
    $this->job->duplex = 'longEdge';
}

// If no clicked
function onNo() {
    // nothing. Job will be released.
}
}
```

Using the above script, the "Job has more than 10 pages. Do you want to print in duplex? Yes or No" dialog is displayed in **KNM** Desktop Client:

If you are familiar with the PHP language, the script is actually a body of the *class UserScript {...}* statement.

You can define properties like *\$hasMoreThan10pages*. Properties are persistent among multiple script invocations for the same job. Use them to store a state between multiple dialogs.

There is the *main* function. It's called once when the script starts. Use it to display the first dialog.

Then there are the *onXXX* functions. They are the action handler called when an *XXX* button is pressed. For example, the *Yes* button is handled via the *onYes* function.

If you display no dialog, the script is finished.

## API Reference

See [Job Scripting Reference](#) on how to modify the job and also for many other operations you can perform.

The User interaction script runs in the context of the **User** class. The sent job can be accessed as *\$this->job*.

Objects from all classes, except for the Session class, can be accessed via the job object, for example the *owner \$this->job->owner*. Objects from the [Session](#) class can be accessed via the *KNM()* global feature; for example: *KNM()->logInfo("This message appears in the KNM log.");*.

## UserScript Class

User Interaction Script is the body of the *UserScript* class as described above. **KNM** also provides several built-in methods of the [User](#) class in addition to your own methods.

## Dialog Creation Methods

Function	Description
void <b>dialogYesNo</b> (string \$text)	Creates a dialog with the <i>\$text</i> as the content and Yes, No buttons.
void <b>dialogPrintNo</b> (string \$text)	Creates a dialog with the <i>\$text</i> as the content and Print, No buttons.
void <b>dialogYesNoCancel</b> (string \$text)	Creates a dialog with the <i>\$text</i> as the content and Yes, No, and Cancel buttons.
void <b>dialog</b> (string \$text, Field[] \$fields)	Creates a dialog with the <i>\$text</i> as the content and an array of custom fields. A field can be a button or any other field type, like a list, for example. Buttons are always displayed below other fields.
FieldButton <b>button</b> (string \$title, string \$id)	Creates a custom button which can be used in the <i>dialog()</i> function. <i>\$title</i> is a text displayed on the button. The button <i>\$id</i> is used when executing the button handler. KNM searches for an <i>onXXX</i> handler where <i>XXX</i> is the <i>\$id</i> .
FieldList <b>singleSelectList</b> (string \$name, array \$items)	Creates a list of options from which the user can choose only one (radio group). It can be used in the <i>dialog()</i> function. The <i>\$items</i> is an associative array where the key is an item's reference and the value is an item's display name visible in the UI.
FieldMultiSelectList <b>multiSelectList</b> (string \$name, array \$items)	Creates a list of options from which the user can choose multiple ones (check boxes). It can be used in the <i>dialog()</i> function. The <i>\$items</i> is an associative array where the key is an item's reference and the value is an item's display name visible in the UI.

## onCancel Method

*onCancel* handles the Cancel button and is provided by default. It calls *terminate()*. You can provide your own implementation to change the behavior.

## Other Methods

Function	Description
void <b>terminate</b> ()	Terminates the script processing. The script has not been executed successfully and the job stays in the <i>pause</i> state. The user must execute the script again.
mixed <b>getField</b> (string \$name)	Gets the value of the field with the <i>\$name</i> after the user has interacted with the dialog. The field must have been created by the methods <i>singleSelectList</i> (the result is a scalar value) or <i>multiSelectList</i> (the result is an array of values, which can be an empty array).

## User interaction script examples

### Print a color job in B&W

```
// script entry point
function main(){
// If the job is color, show a Yes/No dialog to ask if they want to print the job
in B&W.
  if ($this->job->color){
    $this->dialogYesNo("Jobs sent to this queue are printed in B&W,
    do you still want to send the job here?"); }
}

// If Yes clicked, the user is informed that the job was sent to the B&W queue via
a KNM Desktop Client
notification.
function onYes(){
  $this->job->owner->sendNotification("info","Job successfully sent","Your job was
sent
to the B&W queue.");
}

// If No clicked, the job is deleted and the user is informed about it via a KNM
Desktop Client
notification.
function onNo(){
  $this->job->delete(); $this->job->owner->sendNotification("info","Job deleted","Y
our
job was deleted.");
}
```

## Move job to a personal queue

```
// script entry point
function main() {
    /** Job object */
    $job = $this->job;

    // Get the personal queues and create a list
    $queues = $job->owner->getPersonalQueues();
    $queueList = [];
    foreach ($queues as $queue) {
        $queueList[$queue->name] = $queue->name;
    }

    $list = $this->singleSelectList('Personal queues', $queueList);

    $this->dialog('Select a queue', [
        $list,
        $this->buttonPrint(),
        $this->buttonCancel()
    ]);
}

// If print clicked
function onPrint($inputs) {
    $queue = $this->getField('Personal queues');
    $this->job->moveToQueue($queue);
}

// If cancel clicked
function onCancel() {
    // nothing. Job will be released.
}
```

## Job Scripting Reference

This is a reference of classes and functions you can use in [Job Processor Scripting](#) and [User Interaction Scripting](#).

There are five classes that can be used within the scripts: [Job](#), [User](#), [Queue](#), [Session](#), and [QuotaInfo](#). The object of the **Job** class represents the job sent to **KNM**, the object of the **User** class represents the job's owner, and the object of the **QuotaInfo** class represents quotas of the job's owner. The **Queue** class can be used to move the job to one of the personal queues of the job's owner and methods of the **Session** class may be used for additional specific tasks, such as sending a log message to **KNM**.

### Job class

The **Job** class has the following methods and properties:

## Methods

- this **pause()** - Pause the job.
- this **copyToQueue**(string \$queueName) - Copy the job to queue *\$queueName*. The new job is processed normally according to the rules in the target queue.
- this **moveToQueue**(string \$queueName) - Move the job to queue *\$queueName*. The new job is processed normally according to the rules in the target queue.
- this **setReleased()** - Set the job as released (printed) without actually releasing it. (*setPrinted* is still supported for BC).
- this **delete()** - Delete the job.

## Properties

Job Properties show how the job looks after applying user/quota policies. This is how the job will be released. The *null* value means that the job parser was not able to get the property from the job file.

By setting a property, you can modify how the job will be released. This overrides any user/quota policy. If you set a property to *null*, the job will be released as originally received.

Setting *monoCount*, *colorCount* or *paper* doesn't actually modify the job. The new values are used only for credit/quota calculations.

Name	Type	Writable	Description
name	string	yes	Name of the job
dataSize	int	yes	Data size of the job in bytes
queue	Queue	-	Job's queue
monoCount	int	yes	Count of the monochrome pages of the job
colorCount	int	yes	Count of the color pages of the job
pageCount	int	-	Total sum of the pages of the job
paper	string	yes	Format of the paper with the following strings as its values: 'a4' 'a3' 'other' 'a5' 'b4' 'b5' 'folio' 'ledger' 'legal' 'letter' 'statement' This variable is employed by the 'set' method in <b>KNM</b> . Use it in commands of the PHP script.

Name	Type	Writable	Description
duplex	Boolean	yes	Job is in duplex. Possible values: 'simplex' 'longEdge' 'shortEdge' Note: Changing this property only updates the metadata of the job. The job is not converted to simplex/duplex.
color	Boolean	-	Job is in color. Note: Changing this property only updates the metadata of the job. The job is not converted to B&W/color.
owner	User[ ]	yes	Owner of the job Note: The user policies are not updated; Projects are not updated.
copies	int	yes	Number of copies of the job Note: Changing this property only updates the metadata of the job. The number of copies to be released is not changed.
tonerSaving	Boolean	yes	Toner Saving mode enabled
filename	string	yes	A path including the filename of the job. The path is relative to the job folder. Note: The path must exist, otherwise the job is not parsed and is declared as "deleted".
lang	int	-	The PDL of the job with the following integers as its values: UNKNOWN = 0, PDL_PCL = 1, PDL_PS = 2, PDL_ESCP = 3, PDL_PRESCRIBE = 4, PDL_PCLXL = 5, PDL_PDF = 6, PDL_JPEG = 7

### User class

The **User** class has the following methods and properties:

#### Methods

- this **sendEmail**(*string \$subject, string \$body*) - Send an email to the user.
- bool **canPrintToQueue**(*string \$queueName*) - The user has the rights to send jobs to the queue.
- bool **hasGroup**(*string \$name*) - The user is a member of the group.
- this **sendNotification**(*string \$type, string \$title, string \$body*) - Send a notification to the user via **KNM** Desktop Client:

- type: info, warning, error
- title: notification title
- body: notification text (plain text format)
- QuotaInfo **getQuotaInfo()** - Get information about user's quotas.

### Properties

Name	Type	Writable	Description
name	string	-	Login name of the user
email	string	-	Email of the user
fullname	string	-	Name and surname of the user
delegates	User[ ]	-	Array of the user's delegates
notes	string	-	Notes
personalQueues	Queue[ ]	-	Array of personal queues ordered by priority

### Queue class

The **Queue** class has the following methods and properties:

#### Methods

- **bool isAnyPrinterAvailable()** - There is at least one printing device available to the queue.

#### Properties

Name	Type	Writable	Description
name	string	-	Name of the queue

### Session class

The session object is accessible via the *KNM()* global function. The **Session** class has the following methods:

#### Methods

- User **getUserByUserName(string \$userName)** - Find a **KNM** user by their user name. If no user is found, null is returned.
- this **logError(string \$message)** - Create an error message in the **KNM** log.
- this **logWarning(string \$message)** - Create a warning message in the **KNM** log.
- this **logInfo(string \$message)** - Create an info message in the **KNM** log.
- this **logNotice(string \$message)** - Create a notice message in the **KNM** log.
- this **logDebug(string \$message)** - Create a debug message in the **KNM** log.

- string **getJobsPath()** - Get the path to the folder on the **KNM** server where the print job is stored. Ends with a backslash.

### QuotaInfo class

The **QuotaInfo** class contains information about the user's current state of quotas. It has the following methods:

- bool **canColor()** - Check if the user can print or copy in color.
- bool **canPrint()** - Check if the user can print.
- bool **canCopy()** - Check if the user can copy.
- bool **canScan()** - Check if the user can scan.

## 11.7.5 KYOCERA Net Manager Desktop Client tab

On the **KYOCERA Net Manager Desktop Client** tab of each queue, you can set up accounting options and employ PHP scripts to set up interaction with **KNM** users via dialog boxes displayed in **KNM Desktop Client** on their computer.

The screenshot shows a configuration window titled "QueueX" with a close button in the top right. The window has several tabs: "General", "Job receiving", "KYOCERA Net Manager Desktop Client" (which is selected), and "Job processing". Below the tabs, there are "Printers" and "Rights" sections. A descriptive text states: "If any of KYOCERA Net Manager Desktop Client options is enabled, print jobs sent to this queue are paused and wait for authentication and user interaction via KYOCERA Net Manager Desktop Client." There are two main sections: "Accounting" and "User interaction". The "Accounting" section contains two checkboxes: "Ask for project:" and "Ask for payment account (credit, quota, cost center):". The "User interaction" section contains a checkbox for "User interaction" and a text input field. At the bottom, there are "Save" and "Cancel" buttons.

If you have any form of accounting enabled (Credit, Quota, Projects), the **Accounting** section is visible and you can modify the settings for newly created queues. If accounting options are disabled, the section is not visible. If you disable any form of accounting and then re-enable it, the settings in the MDC tab are remembered.

- Mark the **Ask for project** checkbox if you want users to select projects before printing a job.
- Mark the **Ask for payment account (credit, quota, cost center)** checkbox if you want users to select a payment account before printing a job (enabled by default).

For more information, check the **KNM Desktop Client** guides.

In the **User interaction** section, you can enable **User interaction** (described in [User Interaction Scripting](#)), add the script in the field, and click **Save**.

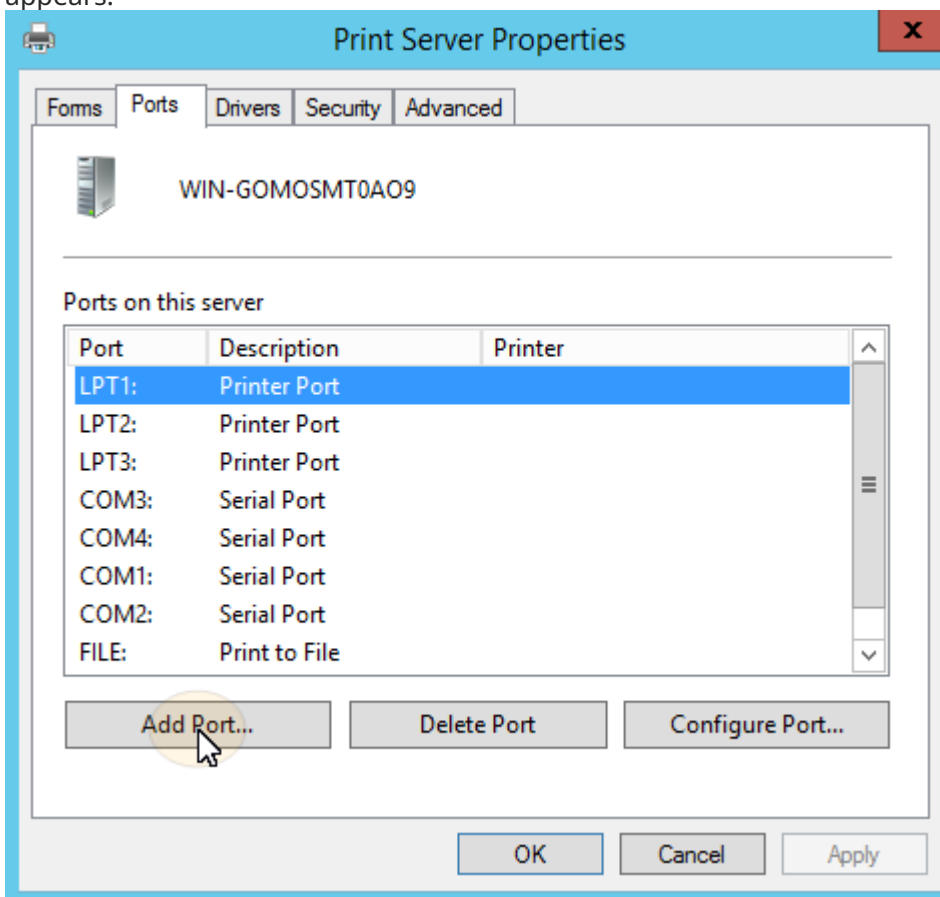
## 12 Printing to KNM

This topic discusses the settings that need to be done outside of **KNM** to enable **KNM** essential functions, such as monitoring jobs and detecting users.

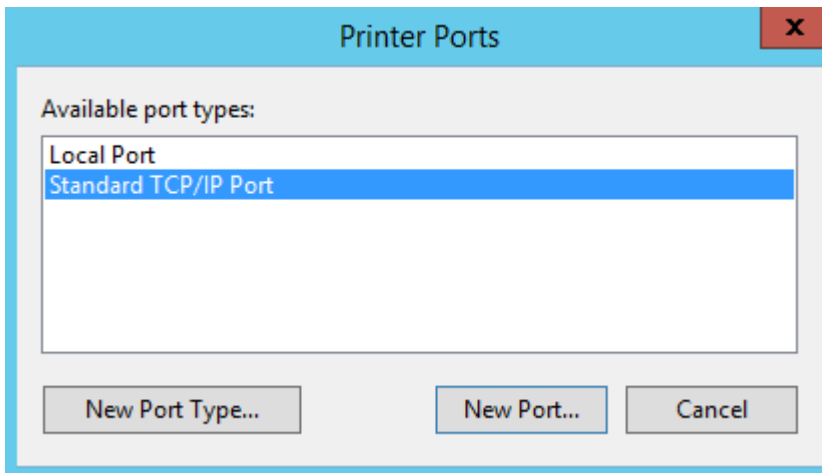
Microsoft Windows and MacOS settings are described below. Although the procedure of installing and setting the print drivers is different on other operating systems, the principle remains the same. You need to add a printer or print port, set the **KNM** server's IP address or hostname, and set the name of the queue where jobs are sent via this port.

### 12.1 Windows settings

1. In **Windows**, under **Devices and Printers**, select any printer, and then click **Print server properties**. The Print server properties dialog box appears.
2. In the dialog box, open the **Ports** tab, and then click **Add Port**. The Printer Ports dialog box appears.



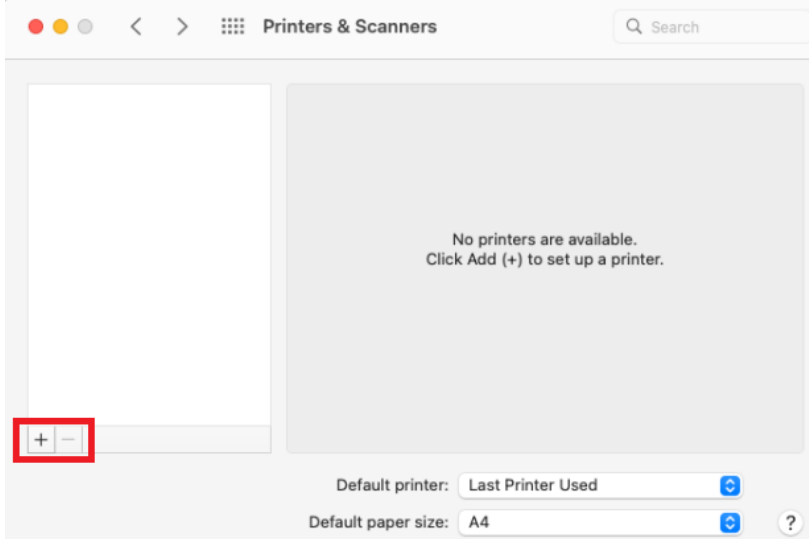
3. On the Printer Ports dialog box, select **Standard TCP/IP Port**.



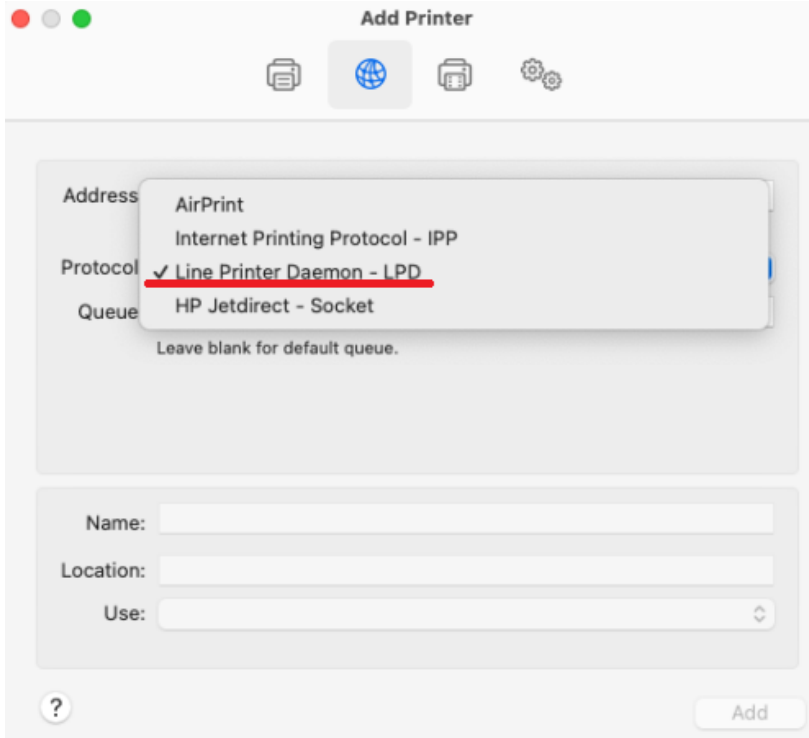
4. Click **New Port**. The Add Standard TCP/IP Printer Port Wizard dialog box opens.
5. Click **Next**.
6. Enter the IP address or the hostname of the **KNM** server.
7. Optionally change the **Port Name**.
8. Click **Next**. You are asked to provide additional port information.
9. Under **Device Type**, select **Custom**.
10. Click **Settings**. The Configure Standard TCP/IP Port Monitor dialog box appears.
11. In the dialog box, under **Protocol**, select the **LPR** option. Under LPR settings, enter the name of the **KNM** queue where you want to print to. Select the **LPR Byte Counting Enabled** option. Click **OK** after the settings are changed.
12. Back on the Add Standard TCP/IP Printer Port Wizard dialog box, click **Next**. You are informed about the characteristics of the new port.
13. Click **Finish**. The new port is added to the list of ports in the **Ports** section of the Print server properties dialog box.

## 12.2 MacOS settings

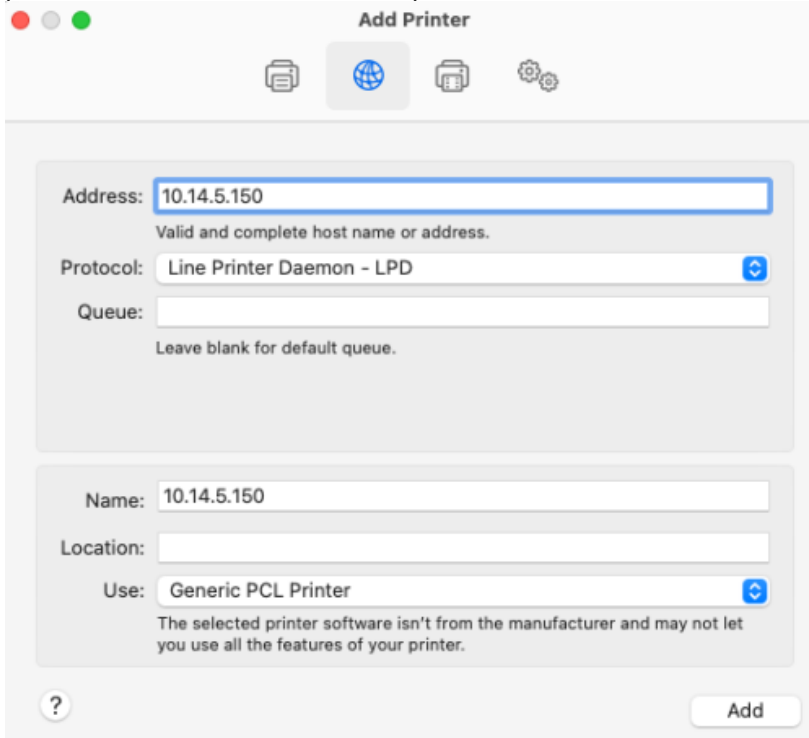
- Go to **Apple menu > System Preferences**, and then click **Printers & Scanners**.
- Click the plus button (+) to add a new printer.



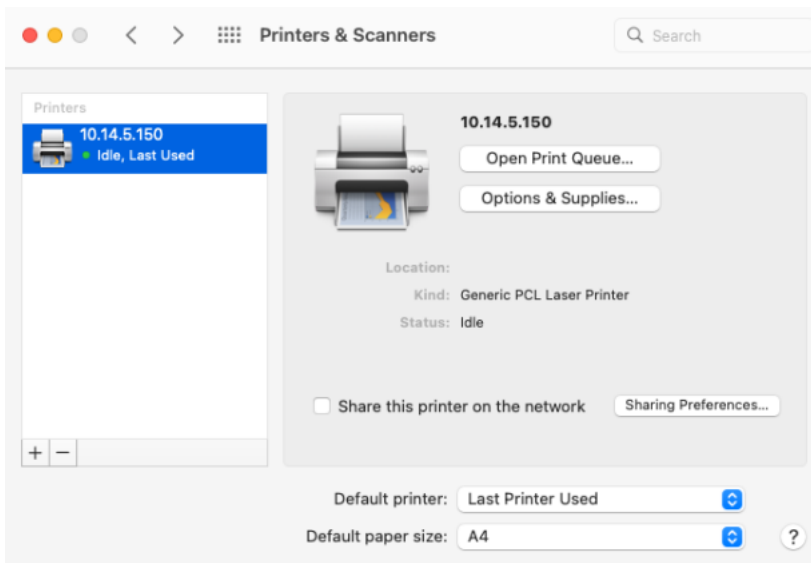
- In the **Protocol** field, select *Line Printer Daemon - LPD* from the list.



- In the **Address** field, add the IP address or host name of the localhost. In the **Queue** field, add a queue name according to the **KNM** server setting. Add a **Name**, and a **Location** for your printer. In the **Use** field, select a printer driver from the list. Click **Add** to setup the printer.



- Once the printer is set up, it appears on the Printers & Scanners list.



## 13 Methods of Printing

---

This topic presents several options of printing with the **KNM** system.

- Direct printing
- Print&Follow printing
- Delegated printing
- Printing from email and from the **KNM** Web User Interface
- Google Cloud Print to **KNM**
- AirPrint and Mopria Print Service
- Microsoft Universal Print
- Local Print Spooling
- Offline Login
- Fallback Printing

There are other printing options, related to advanced features of **KNM**, such as running **KNM** on multiple servers, or to a variety of embedded terminals that can be purchased together with the **KNM** system. Information about these options are provided in the respective guides describing these features and in the **KNM** embedded terminal manuals.

### 13.1 Direct printing

With the direct printing method, users can send their print jobs to be immediately printed on a particular printing device via a dedicated queue. The queue is created especially for this device and cannot have any other devices attached to it. As soon as **KNM** receives the job, it sends it to the printing device to be printed.

From the user's point of view, it works in the same way as the common method of print where the job is sent directly to a selected printing device. The main difference is that **KNM** collects the job data to be used for reports and accounting.

For information on how to create a direct print queue, see [Queues](#).

Users that send their jobs using this method do not need to be identified on the printing device and therefore no terminal is needed there.

### 13.2 Print&Follow printing

Whereas the direct printing method is intended to be direct and quick, the Print&Follow method is used for the opposite reasons. With this method, users can send a print job to be held on the **KNM** server for as long as they need and select from a number of printing devices where it can be printed.

To print the job, the user just needs to authenticate themselves on the printing device terminal. After the authentication, the job is either immediately printed or displayed on the terminal touch panel, where it can be managed by the user. Depending on the type and settings of the terminal, users might have either one, or both of these options.

For information on how to create a Print&Follow queue, see [Queues](#).

To use this method, an embedded terminal or a hardware terminal is required.

For more information on embedded terminals, see:

- **KNM** Embedded guide
- **KNM** Embedded Lite guide

## 13.3 Delegated printing

The delegated printing feature is an extension of the Print&Follow printing method that allows users to share their print jobs with a specified group of other users. These users can release the jobs on an embedded terminal in the same way they would release their own jobs.

The users that are allowed to print jobs of a certain user (or a certain group of users) are called their delegates. The delegates can be designated by the users themselves or by the **KNM** administrator. When a user sends a job to **KNM**, they can decide to share it with their delegates. Jobs that are to be shared have to be sent via the **Delegated printing** type queue.

Two settings are necessary to enable this feature: the delegates have to be defined and a **Delegated printing** queue has to be created and be accessible to the user or group.

For information on how to define the delegates, see [Selecting user delegates](#).

For information on how to create and set the **Delegated printing** queue, see [Queues](#).

## 13.4 Printing from email and from the KNM Web UI

**KNM** enables users to print documents from the **KNM** web user interface or by sending an email to a special email address. It supports printing the following source formats:

- pdf/a
- jpeg, bmp, tif, png
- txt (UTF8)
- MS Office and LibreOffice documents: doc, docx, xls, xlsx, ppt, pptx, odt, ods and odp. (You have to have the corresponding suite installed on the server.)
- email body in plain text and HTML

The minimal required version of MS Office is MS Office 2013 64bit with the latest service pack (MS Excel files using MS Office 2013 are not supported). This means that MS Office 2013, 2016, 2019 and O365 64bit are supported.

The minimal required version of LibreOffice is LibreOffice 6 64bit.

If only one of the tools (MS Office or LibreOffice) is installed, it is used for all formats. If both tools are installed, MS Office formats are used by MS Office and LibreOffice formats by LibreOffice (recommended solution).

After the MS Office/LibreOffice installation, **KNM** services need to be restarted in order to start recognizing these formats.

All print jobs sent from email are automatically assigned to the **Email** queue and can be printed only on printing devices assigned to this queue.

All print jobs sent from the web user interface are automatically assigned to the **Web** queue and can be printed only on printing devices assigned to this queue.

### 13.4.1 Printing from the web UI setup

To enable and setup the print:

On the **Jobs** settings tab, under **Jobs via Web**, set the following parameters:

1. Enable the **Jobs via Web** option.
2. Select the users that are allowed to use this feature.

Once the **Jobs via Web** option is enabled, all users with rights to the **Web** queue have the **Print File** button displayed on their web user interface account. They can click this button and insert print jobs directly to **KNM**. The job size limit is **120MB** by default and it's based on the **Maximum upload file size** setting (available in **KYOCERA, Settings, Jobs**, in the **Jobs via Web** section).

## 13.4.2 Printing from email setup

Once the **Jobs via Email** option is enabled, the users can print a document by attaching it to an email and sending it to a special email account dedicated to print. Jobs send via email are limited to **500MB** per email message, all attachments included.

Jobs via Email

Enabled:

Allowed users: \*

[Manage queue for these jobs](#)

Always generate a new PIN after a job is received:

Print email body:

Default print options:  B&W  Toner saving  Duplex

You can override the defaults by using keywords in the email subject

▼ Email box

KYOCERA Net Manager will periodically check the following email box for print jobs. The box will be emptied automatically.

Type:  Microsoft Exchange Online  
 Gmail  
 Generic IMAP server  
 Generic POP3 server  
 KYOCERA Net Manager SMTP Server

If you select the **Always generate a new PIN after a job is received** option, a new PIN is generated every time a user sends an email with a print job. If the user already has a PIN, it is replaced by the new one. If you select this option, make sure that you select the **Send new PIN via email** option on the **Users** settings menu, under PIN. Otherwise users do not receive the new PIN and cannot access their **KNM** accounts.

You can enable users to **Print email body** and restrict the print to *B&W*, *Toner saving* and/or *Duplex* mode by selecting one or more **Default print options**.

In addition, users can change their print job parameters by adding keywords to the email subject. These changes have priority over the **Default print options** selected in **KNM**. Users can choose from the following keywords: **#color** (color print), **#mono** (monochrome print), **#duplex** (print on both sides of a paper), **#simplex** (print on one side of a paper), **#ecoon** (toner saving print mode on), **#ecooff** (toner saving print mode off). They can be used as any part of the subject and do not have to be separated. For example, an email with the *MyPrintJob #mono#duplex* subject will force the job to be printed in monochrome and duplex.

There are two ways of receiving the print jobs sent via emails: you can either use **KNM** as an SMTP server and forward all emails with the print jobs there, or you can use **KNM** as an email client that fetches all emails from a specific email account on your server via POP3 or IMAP protocol.

## Forwarding emails to the KYOCERA Net Manager SMTP server

With this option, **KNM** listens on the **KNM** SMTP server port set on the **Network** settings tab and receives any email starting with print as the email with the print job. If you select this option, you need to take the following steps:

1. On your company mail server, create an email account for receiving print jobs.
2. Redirect the sent emails from this address to *print@[IP/hostname]*, where IP/hostname is either the IP address of **KNM** server, or its hostname. Any email received on this address will be processed as a print job and its owner will be identified by their email address.

## Receiving print jobs via POP3, IMAP, Gmail, MS Exchange Online

On your company mail server, create an email account for receiving print jobs.

On the **Jobs** settings tab of the **KNM** Web Interface, under **Jobs via Email**:

Under **Type**, select a type from *Generic POP3 server*, *Generic IMAP server*, *Microsoft Exchange Online* or *Gmail*.

For *Generic POP3/IMAP server*:

- Ensure that the protocol port is correctly set in the **Port** text box.
- If you want to secure the communication between **KNM** and the mail server, select one of the security options (*SSL*, *STARTTLS*).
- Enter the IP address or the hostname of the mail server in the **Server** text box.
- Enter the address of the email account that will receive the print jobs in the **User** text box.
- Enter the password of the email account in the **Password** text box.
- By changing the value of the **Polling interval** setting, you can change the interval after which **KNM** fetches new emails from the mail server.
- By clicking **Test**, you can test the connection to the mail server, and then click **Save** to save your changes.

For *Microsoft Exchange Online*:

- If you have already set up a Microsoft Exchange Online server in the **Connections** settings, that server is selected in the **Connection** field. If not, you can click on the **Server** field and then click **Add** to add your Microsoft Exchange Online server. In the pop-up, add a **Title** for your server, the **Client ID** and the **Tenant ID**, and click **OK**. For more information, check [Microsoft Exchange Online Setup](#).
- Set the **Port** setting to the correct value that the email server listens to. You can find the default Microsoft settings here <https://support.microsoft.com/en-us/office/pop-imap-and-smtp-settings-8361e398-8af4-4e97-b147-6c6c4ac95353> .
- Choose between the *SSL* and *STARTTLS* **Security** options.
- Enter the address of the email account that will receive the print jobs in the **User** text box.
- By changing the value of the **Polling interval** setting, you can change the interval after which **KNM** fetches new emails from the mail server.
- Click **Test** to test the connection to the mail server, and then click **Save** to save your changes.

For *Gmail*:


- If you have already set up a Gmail with OAuth2 server in the **Connections** settings, that server is selected in the **Connection** field. If not, you can click on the **Server** field and then click **Add** to add your Gmail server. In the pop-up, add a **Title** for your server, the **Client ID** and the **Security key**, and click **OK**. For more information, check [Gmail with OAuth2 setup](#).

- Set the **Port** setting to the correct value that the email server listens to.
- Choose between the *SSL* and *STARTTLS Security* options.
- Enter the address of the email account that will receive the print jobs in the **User** text box.
- By changing the value of the **Polling interval** setting, you can change the interval after which **KNM** fetches new emails from the mail server.
- Click **Test** to test the connection to the mail server, and then click **Save** to save your changes.

### 13.4.3 Processing documents in Office formats

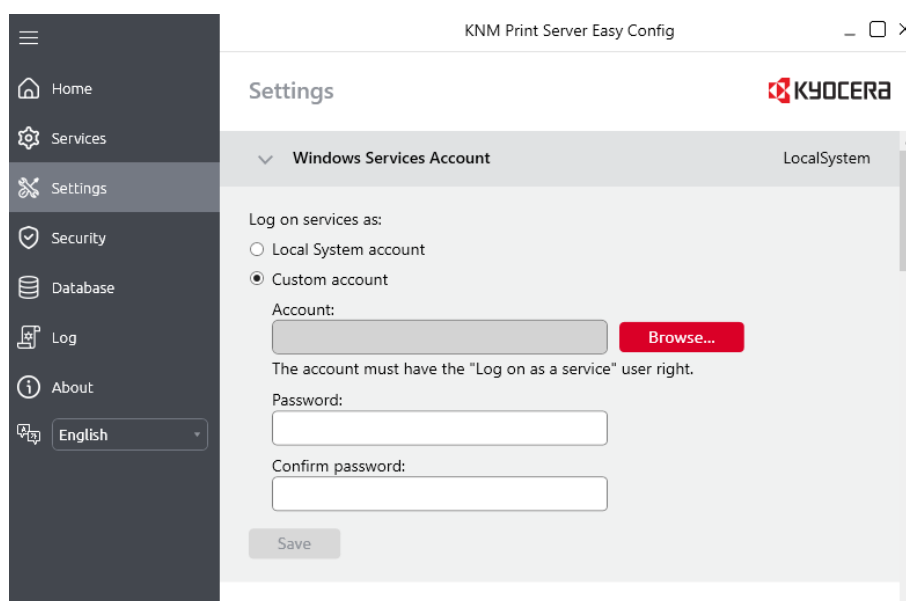
On the **Jobs** settings tab, under **Office file formats**, select a method of processing the Office format files. You can select from:

- **Convert to PDF** - **KNM** opens the document in the Office application, converts the job to PDF and sends it directly to the printing device. The printing device has to support direct print of the PDF format. The corresponding office package (in 64bit) has to be installed on the **KNM** account. For processing documents in MS Office formats, it is recommended to run **KNM** service under a new local admin account rather than the default Local System account.
- **Via a Windows printer** - **KNM** opens the document in the MS Office application and prints it using a selected windows printer (print driver). To select the printer, choose the printer that you want to use on the setting drop-down. You also have to change the printer security settings to allow **KNM** to print from that print driver. In **Windows**, under **Devices and Printers**, right-click the printer. In the printer's properties, open the **Security** tab and allow print and managing printers to the account that the **KNM** services are running under.

 After the MS Office/LibreOffice installation, **KNM** services must be restarted for the system to start recognizing these formats.

### Creating a new local admin account

1. Create a new local admin account with full administration rights (details can be found [here](#)).
2. Log on to the newly created account.
3. Install the corresponding Office package on the **KNM** server.
4. Run all the applications that will be used for the conversion (*Word, Excel, PowerPoint, LibreOffice, etc.*) and close all welcome screens and dialog boxes that might appear on the application startup.
5. Open the **KNM** Easy Config application and go to the **Settings** tab. Under **Windows Services Account**, select **Custom account**. Then, either browse for the user, or enter the user's credentials and click **Save**. **KNM** services are then automatically restarted.



## 13.5 Print from Chromebooks, Chrome and other Google apps

As Google ended their support for Google Cloud Print, **KNM** offers the following alternatives for secure printing or remote printing:

- [IPPS via Chromebook](#) - setting up printing via IPPS enables users to print from Google Chromebooks natively.
- [Printing from email/web](#) - print documents from the **KNM** web user interface or by sending an email to a special email address.

## 13.6 AirPrint and Mopria Print Service

AirPrint enables users to print photos and documents from their MacBook, iMac, iPhone, iPad, or iPod touch without having to install additional software (drivers).

Mopria Print Service does the same for users with an Android smart phone or tablet. Android users must download the Mopria Print Service app from Google Play.

As an administrator, you only have to install **KNM Mobile Print Agent 1.3+** once, to give your iPhone and/or Android users access to **KNM** queues.

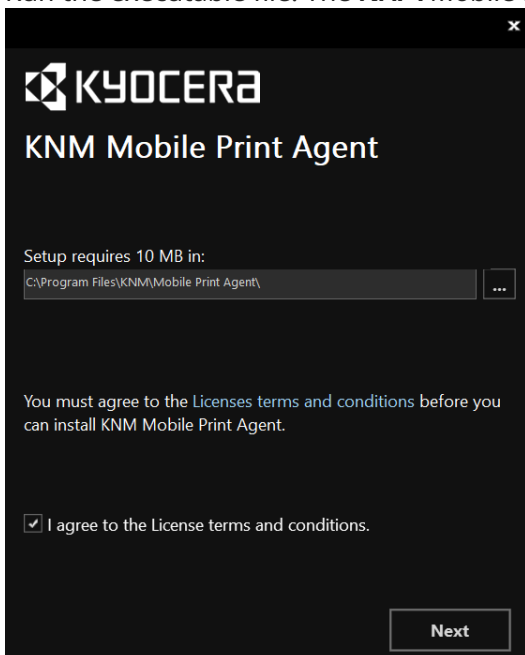
AirPrint and Mopria Print Service are working with **KNM** by exposing **KNM** print queues as AirPrint / Mopria Print Service printer devices. The **KNM** users connect to the company's Wi-Fi network, select the queue where they want to send the print job, and authenticate themselves with their **KNM** credentials. After the first authentication, the credentials are stored on the device. **Print&Follow** and **Delegated printing** queues are displayed as available printers on the users' device.

1. **KNM** Print Server 10+ requires **KNM** Mobile Print Agent 1.3+.

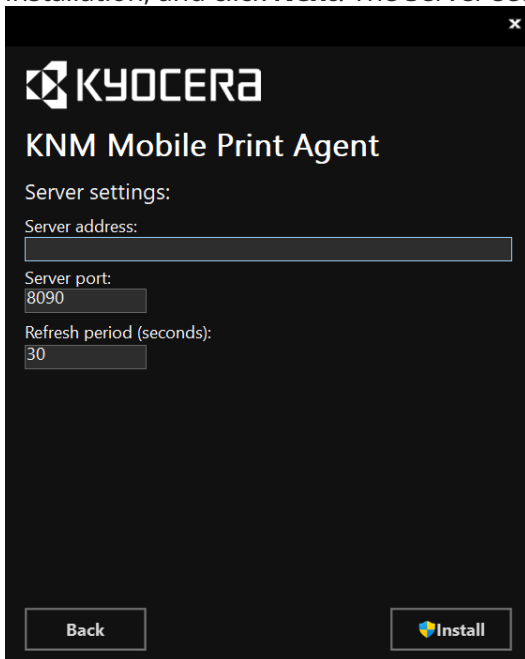
### Enable AirPrint and/or Mopria Print Service

1. Make sure that on the **KNM** Web UI, in **KYOCERA, Settings, Jobs**, the **Jobs via AirPrint/Mopria** setting is **Enabled** (it is enabled by default).

2. Download the latest **KNM** Mobile Print Agent installation file on your server.
3. Run the executable file. The **KNM** Mobile Print Agent installation wizard opens.



4. Select the folder where you want to install **KNM** Mobile Print Agent. The default path is: *C:\Program Files\KNM\Mobile Print Agent\*.
5. After this, you need to agree to the license terms and conditions to continue with the installation, and click **Next**. The Server settings window opens.



6. Enter the settings:
  - a. **Server address:** the IP address of the **KNM** Print Server.
  - b. **Server port:** the editable port that **KNM** Mobile Print Agent will use (8090 by default).
  - c. **Refresh period:** The time taken to refresh the connection with the **KNM** Print Server, in seconds (30 by default).

7. Click **Install**. **KNM** Mobile Print Agent is installed.
8. Click **Finish** to exit the installation wizard.

## 13.7 Microsoft Universal Print

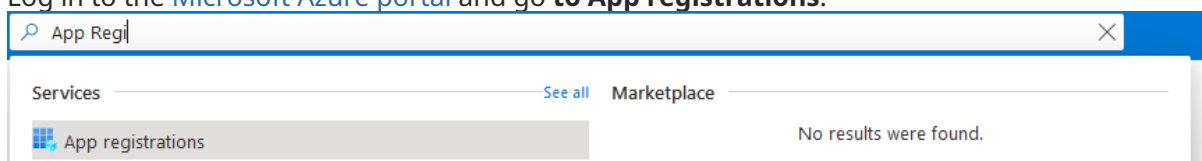
Microsoft Universal Print is a multi-tenant, cloud-based print service that enables cloud-only print solution for organizations.

**KNM** integrates MS Universal Print and allows administrators to create virtual printers in Microsoft Azure automatically. **KNM** checks periodically if there are any new jobs to be downloaded and if yes, they are downloaded to the associated user and queue, and they are handled as normal jobs in **KNM**.

It is first needed to [set up Universal Print in Microsoft Azure](#), and then [configure it in KNM](#).

### 13.7.1 Setting up Universal Print in Microsoft Azure

1. Log in to the [Microsoft Azure portal](#) and go to **App registrations**.



2. Click **New Registration** and fill in the new app details:
  - a. **Name** - The name for this application (this can be changed later). For example, *UP*.
  - b. **Supported account types** - Who can use this application or access this API? Select the *Accounts in any organizational directory (Any Azure AD directory - **Multitenant**)* option.
  - c. **Redirect URI (optional)** - The authentication response is returned to this URI after successfully authenticating the user. Select the *Public client/native (mobile&desktop)* option from the drop-down.
  - d. Click **Register**.

## Register an application

### \* Name

The user-facing display name for this application (this can be changed later).

 ✓

### Supported account types

#### Who can use this application or access this API?

- Accounts in this organizational directory only (MyQ spol. s r.o. - DevTest only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

[Help me choose...](#)

### Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

  ✓

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

- The new app overview page opens. Copy the **Application (client) ID** and the **Directory (tenant) ID**, as they are needed for the connection to **KNM**.

Overview

Quickstart

Integration assistant | Preview

Manage

Branding

Authentication

Delete Endpoints

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name : UP

Supported account types : Multiple organizations

Application (client) ID : [redacted]

Redirect URIs : 0 web, 0 spa, 1 public client

Directory (tenant) ID : [redacted]

Application ID URI : Add an Application ID URI

Object ID : d0d98be7-b33a-48fa-b2eb-24ee009292db

Managed application in l... : UP

- On the left-hand menu, click **Manifest** and modify the **\*\*requiredResourcesAccess**, **replyUrlsWithType**, **allowPublicClient** sections, according to the following:

```
"allowPublicClient": true,
"replyUrlsWithType": [
  {
    "url": "https://login.live.com/oauth20_desktop.srf",
    "type": "InstalledClient"
  }
],
```

```

"requiredResourceAccess": [
  {
    "resourceAppId": "00000003-0000-0000-c000-000000000000",
    "resourceAccess": [
      {
        "id": "93dae4bd-43a1-4a23-9a1a-92957e1d9121",
        "type": "Scope"
      },
      {
        "id": "06ceea37-85e2-40d7-bec3-91337a46038f",
        "type": "Scope"
      },
      {
        "id": "7427e0e9-2fba-42fe-b0c0-848c9e6a8182",
        "type": "Scope"
      }
    ]
  },
  {
    "resourceAppId": "da9b70f6-5323-4ce6-ae5c-88dcc5082966",
    "resourceAccess": [
      {
        "id": "3e306194-d6c5-43ad-afbb-0e7b16a9c10b",
        "type": "Scope"
      },
      {
        "id": "1c90a3a7-465b-49c4-adcc-c8ac83d3d3f8",
        "type": "Role"
      },
      {
        "id": "2b1bdd6b-9a0f-47c6-a806-b3e20cfd07a8",
        "type": "Role"
      },
      {
        "id": "b695614a-52ec-4835-9e13-bdf5ff4c7448",
        "type": "Role"
      },
      {
        "id": "11f87dac-027f-4d76-bd29-1ea1536b93da",
        "type": "Role"
      }
    ]
  }
]

```

5. On the left-hand menu, click **API permissions** and click **Grant admin consent** for the scopes seen in the image below:

Search (Ctrl+/) Refresh | Got feedback?

Overview

Quickstart

Integration assistant | Preview

Manage

Branding

Authentication

Certificates & secrets

Token configuration

**API permissions**

Expose an API

App roles | Preview

Owners

Roles and administrators | Preview

Manifest

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission  Grant admin consent for - DevTest

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (3)				
offline_access	Delegated	Maintain access to data you have given it access to	-	...
Printer.FullControl.All	Delegated	Register, read, update, and unregister printers	Yes	Not granted for
PrinterShare.ReadWrite.All	Delegated	Read and write printer shares	Yes	Not granted for
Universal Print (4)				
PrinterProperties.ReadWrite	Application	Read and write the properties and attributes of printers.	Yes	Not granted for
Printers.Read	Application	Read printers.	Yes	Not granted for
PrintJob.Read	Application	Read the metadata and payload of users' print jobs.	Yes	Not granted for
PrintJob.ReadWriteBasic	Application	Read and write the metadata of users' print jobs.	Yes	Not granted for

6. Go to Universal Print and enable **Document Conversion**.

**Universal Print | Document Conversion**

PREVIEW

Search (Ctrl+/) Universal Print offers automatic document converted to the printer supported format. Learn

Overview

**Document Conversion**  Enabled

Manage

Printers

Printer Shares

Connectors

**Document Conversion**

\*\* The changes in the JSON settings in step 4, set the required scopes for Universal Printing and change the application to be treated as public (Needed for requesting device code).

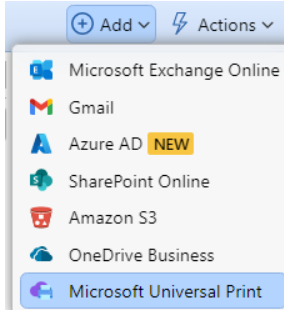
The table below shows the details of the required scopes:

Scope ID	Description
06ceea37-85e2-40d7-bec3-91337a46038f	Microsoft Graph: PrintShare.ReadWrite.All Read and write printer shares
7427e0e9-2fba-42fe-b0c0-848c9e6a8182	Microsoft Graph: offline_access Allows KNM to request the Access token via the complete MS OAuth2 flow only once, and then use Refresh token to exchange it for the Access token.
93dae4bd-43a1-4a23-9a1a-92957e1d9121	Microsoft Graph: Printer.FullControl.All Register, read, update, and unregister printers

Scope ID	Description
3e306194-d6c5-43ad-afbb-0e7b16a9c10b	UP: Printers.Create Create (Register) printers
1c90a3a7-465b-49c4-adcc-c8ac83d3d3f8	UP: PrinterProperties.ReadWrite Read and write the properties and attributes of printers.
2b1bdd6b-9a0f-47c6-a806-b3e20cfd07a8	UP: Printers.Read Read printers
b695614a-52ec-4835-9e13-bdf5ff4c7448	UP: PrintJob.Read Read the metadata and payload of users' print jobs.
11f87dac-027f-4d76-bd29-1ea1536b93da	UP: PrintJob.ReadWriteBasic Read and write the metadata of users' print jobs.

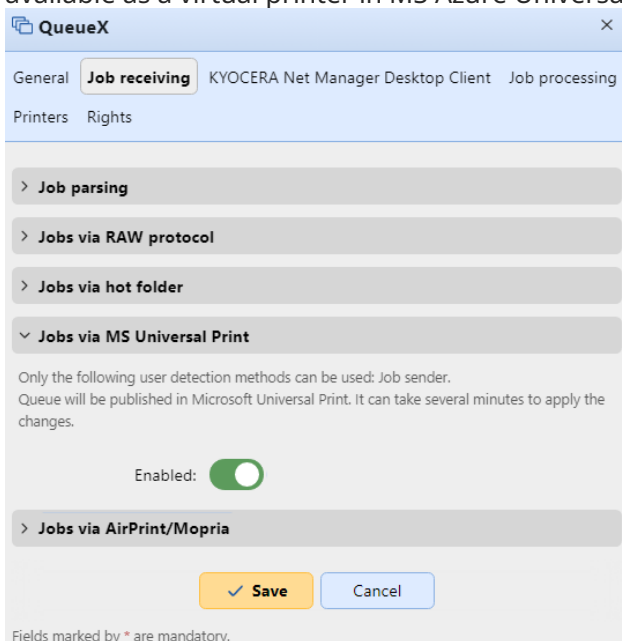
### 13.7.2 Setting up Universal Print in KNM

1. Log in to the **KNM** web administrator interface, and go to **KYOCERA, Settings, Connections**.
2. Click **+Add** and select *Microsoft Universal Print* from the list.



3. In the pop-up window, fill in the required fields:
  - a. **Title** - add a name for your Microsoft Universal Print connection; for example, *MS Universal Print*.
  - b. **Directory (tenant) ID** - the **Directory (tenant) ID** you copied during the MS Azure setup.
  - c. **Application (client) ID** - the **Application (client) ID** you copied during the MS Azure setup.
4. Click **OK**.

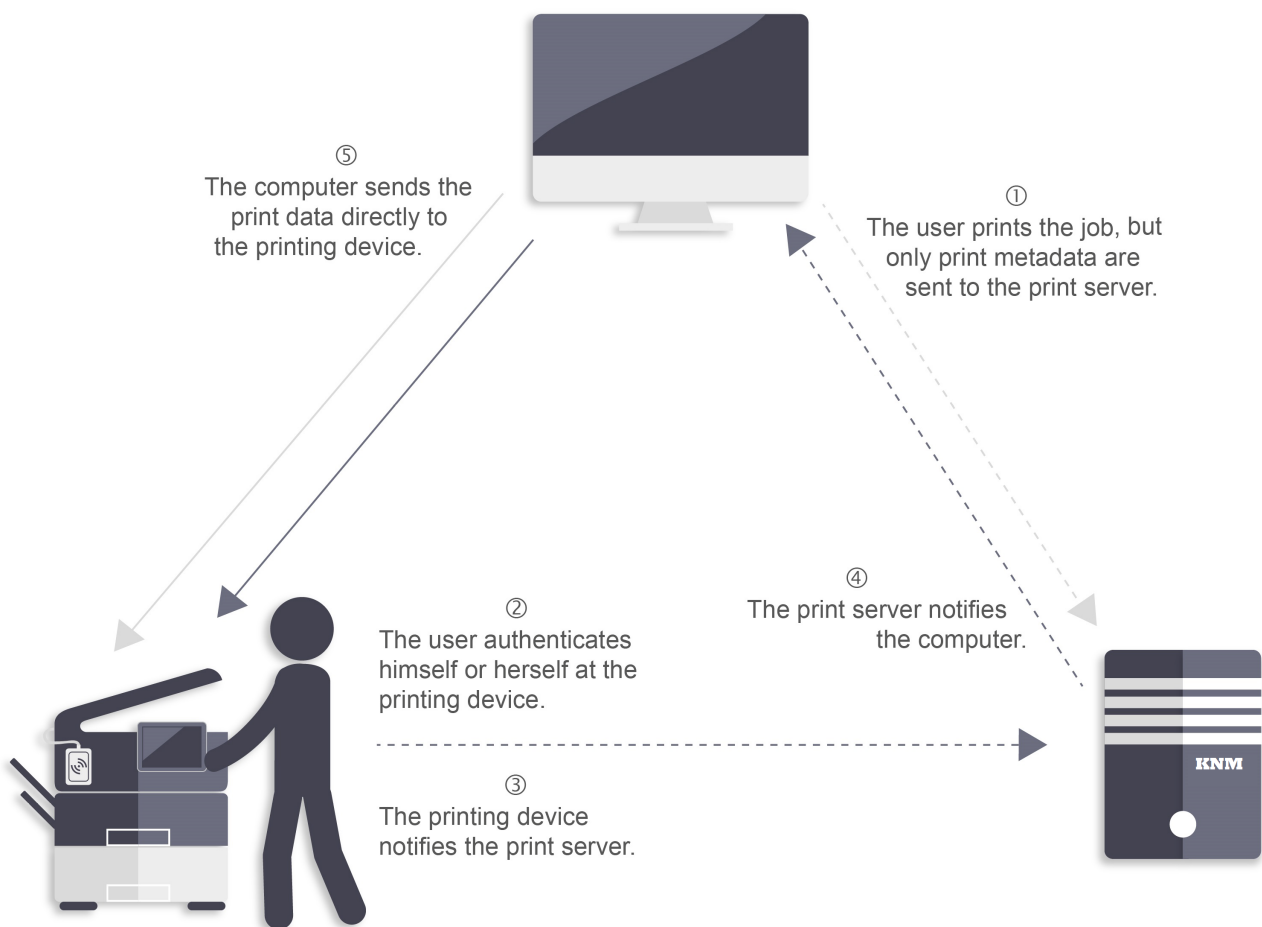
5. Copy the **Code** from the pop-up window, click on the URL, enter the code and follow any other instructions. Once done, **KNM** is connected to MS Azure Universal Print. (There is a 15min timeout for confirming the code. If it is not confirmed and a user tries to create a printer in Azure via **KNM**, a message appears in the *Issues* column in the Queues section, that it is needed to confirm the code. If the time for confirming the code is up, then when a user is trying to create the printer, the device code request will be generated again and there will be a message with a new user code in the *Issues* column).
6. Go to **KYOCERA, Queues** and select the queue(s) you want to associate with Universal Print. Double-click on the queue (or right-click and edit, or select the queue, click Tools and edit) and on the queue properties, click on the **Job receiving** tab. In the **Jobs via MS Universal Print** section, set the option to **Enabled**, and click **Save**. After a few minutes, your queue will be available as a virtual printer in MS Azure Universal Print.



## 13.8 Client Spooling

With the Client Spooling feature enabled, users' print jobs are not sent to the **KNM** server, but stay stored at the users' computer. After they authenticate themselves at a printing device and select the jobs to be printed, the jobs are released from the computer directly to the device. This method dramatically decreases traffic to **KNM** server and is suitable especially for small offices with limited network connection to the **KNM** server.

When a user prints their job while this feature is activated, only the print metadata are sent to the server and the actual print job does not leave the computer (it is stored there as a RAW file). It waits until the user authenticates themselves at a printing device and selects to print the job there. After that, the printing device notifies the server, the server notifies the computer and the computer sends the job directly to the printing device, where it is printed.



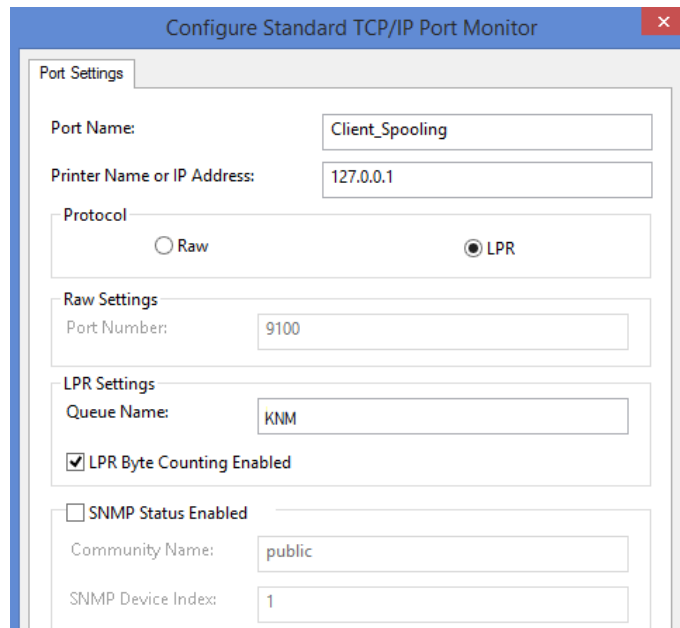
To enable this feature, you have to set a TCP/IP port for the service, install the **KNM** Desktop Client application on the client's computer and enable the Client Spooling feature. (For information on how to install and set up **KNM** Desktop Client on client's computers, see the **KNM** Desktop Client for Windows guide).

If the computer of the user is switched off during the sending of the job, the job is **Paused** on the server. The administrator can release the job once the user has switched on their computer again.

### 13.8.1 Windows settings

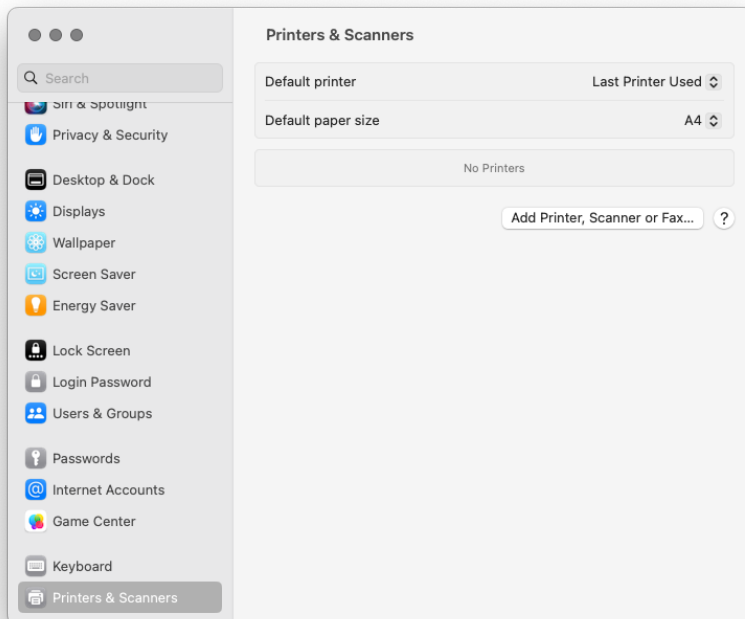
The settings in the Configure Standard TCP/IP Port Monitor dialog box (in the printer's settings) must have the following values:

- **Printer Name or IP Address:** *127.0.0.1* (IP address of the localhost in Windows) or *localhost*
- **Protocol:** Select *LPR*
- **Queue Name:** queue name according to the **KNM** server setting (same as if printing to the **KNM** server)
- **LPR Byte Counting Enabled:** *Selected*
- **SNMP Status Enabled:** *Deselected*

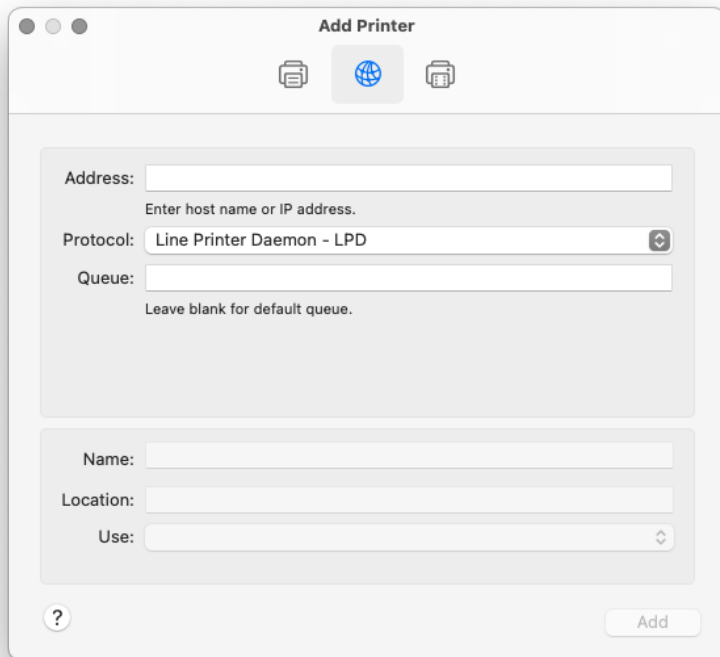


## 13.8.2 MacOS settings

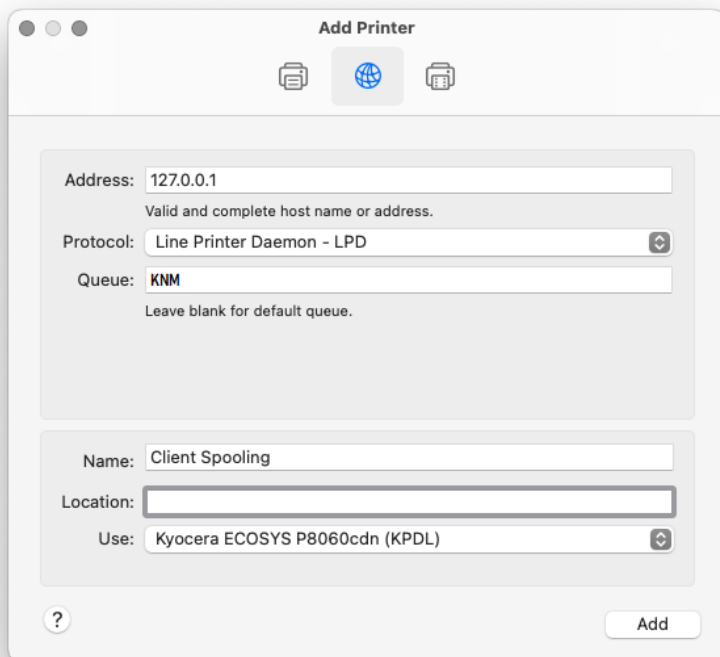
- Go to **Apple menu > System Preferences**, and then click **Printers & Scanners**.
- Click **Add Printer, Scanner or Fax** to add a new printer.



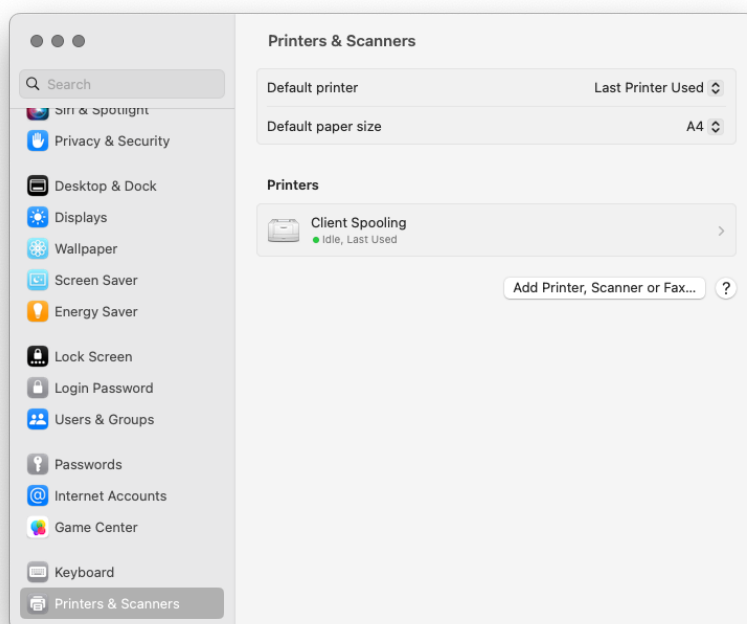
- In the ribbon, select the IP icon. In the **Protocol** field, select *Line Printer Daemon - LPD* from the list.



- In the **Address** field, add the IP address or hostname of the localhost. In the **Queue** field, add a queue name according to the **KNM** server setting. Add a **Name**, and optionally a **Location** for your printer. In the **Use** field, select a printer driver from the list. Click **Add** to setup the printer.



- Once the printer is set up, it appears on the Printers & Scanners list.



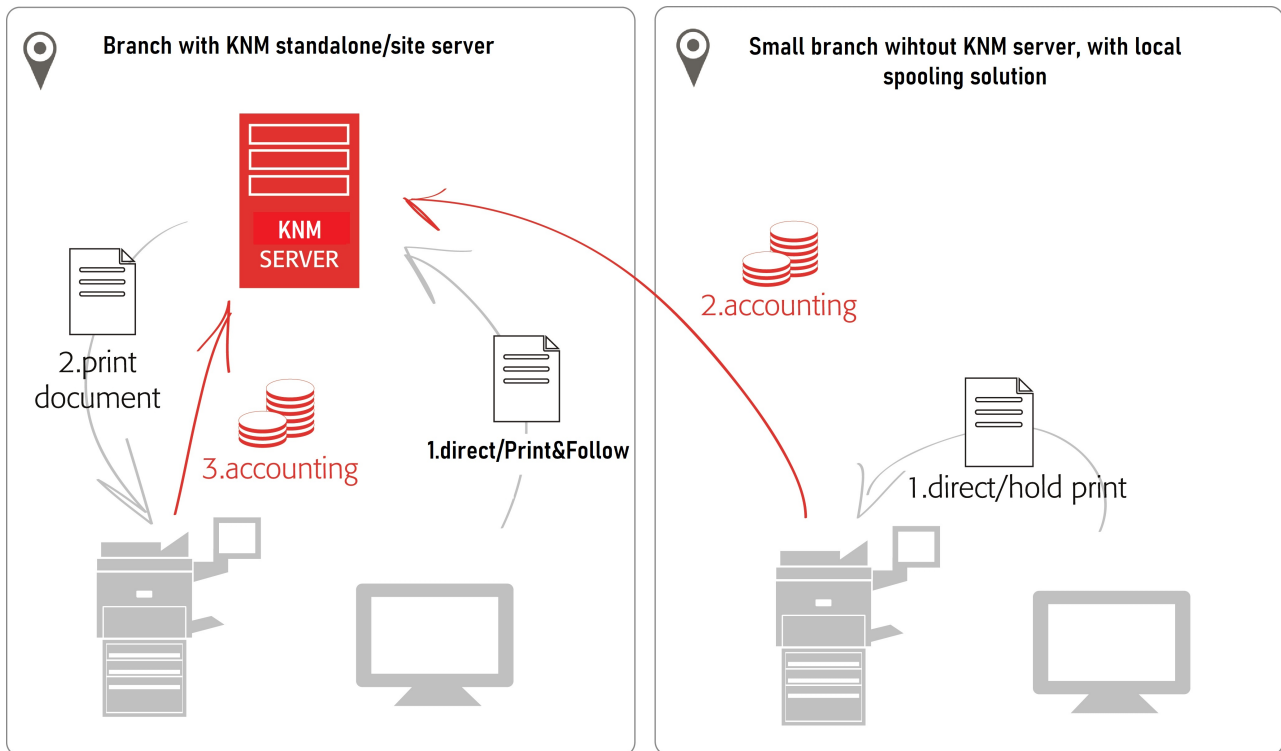
### 13.8.3 Limitations

- Job processing:
  - Jobs are not parsed (number of pages, color etc. is unknown).
  - User detection from PJI is not supported.
  - Computer detection from PJI is not supported.
  - Job name cannot be read from the PJI header.
  - Job processing defined on the queue cannot be applied.
  - User policies cannot be applied.
  - Prologue/epilogue is not supported
- If the client PC is offline, the job is not printed, but it is marked as printed on the server. User is not notified.
- Jobs cannot be marked as favorite.
- The user detection method currently only supports "Job sender".
- **KNM** Desktop Client can send the job to the printer only via the RAW protocol.
- The jobs are deleted after 7 days. The **Delete jobs older than** option on the **System maintenance** settings tab should be set to *168 hours* (as it is by default) in order to prevent discrepancy between the data stored in **KNM** and the data stored on the client computer.

## 13.9 Device Spooling

Under normal circumstances, print jobs are sent to the **KNM** server where they are stored and wait for release. It means that every print job has to be sent from a user PC to the **KNM** server and then from the **KNM** server to a printing device. This is fine for networks with a good bandwidth connection, but it might not be an optimal solution for customers with many small branches and limited bandwidth to the **KNM** Central server. In such cases, it is unproductive to send the job from the branch to **KNM** server and back.

Device Spooling is a feature that solves this problem. With Device Spooling enabled, a print job is sent directly to the device and saved to its hard disk. It waits there to be released in the standard way.

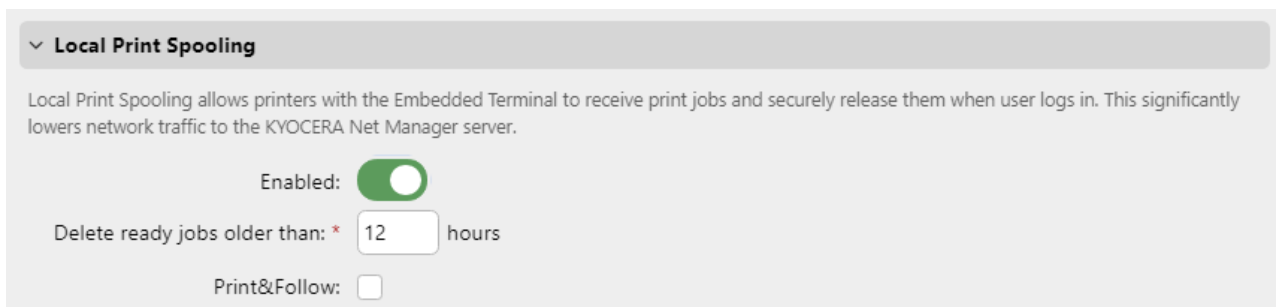


### 13.9.1 Limitations

- Project Accounting is not supported (print jobs have the *Without Project* option set)
- Favorite jobs are not supported
- Job Roaming is not supported
- Print job archiving is not supported
- Job preview is not supported

### 13.9.2 Setting up Device Spooling

To open the setup screen, go to **KYOCERA, Settings, Printers & Terminals**. Under **Local Print Spooling**, you can activate the feature and change its settings:

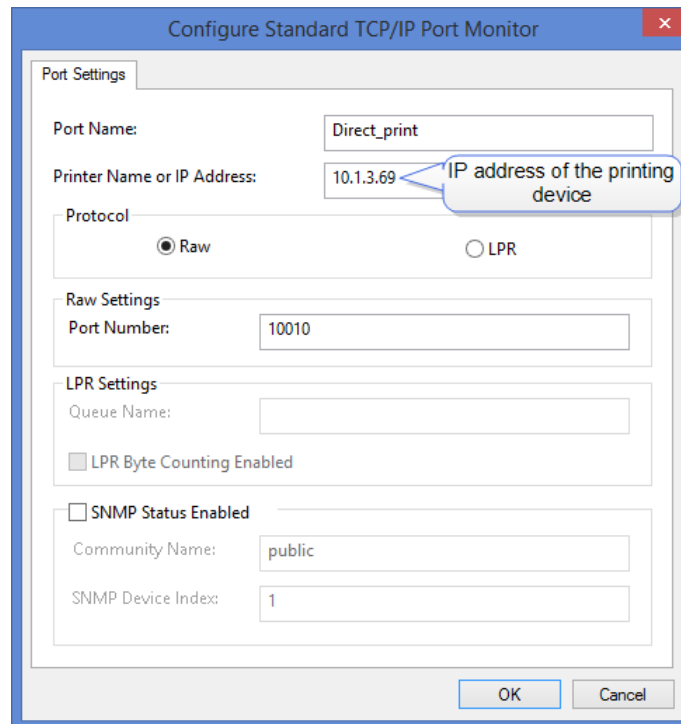


- **Enabled:** Click to enable or disable the feature.
- **Delete ready jobs older than \_\_\_ hours:** Hours to wait before the spooled jobs are deleted from the printing device's hard disk.
- **Print&Follow:** Select to activate Print&Follow for Device Spooling. With the Print&Follow extension activated, jobs sent to one printing device can be printed on any other printing device connected to the same local area network. If there are more mutually connected devices at the branch, the jobs spooled on the devices can be shared between them. In such cases, jobs sent to one device are displayed on the list of print jobs and can be printed on other devices. The Print&Follow feature is limited to devices on the same subnet.  
For the local Print&Follow functionality, it's necessary to have the same time set on all of the participating devices. The easiest way to do this is to synchronize the devices with a time server, such as *time.windows.com*, *time.nist.gov*, etc. You can do this in the Date/Time settings on the device Web UI.
- To submit the changes, click **Save** at the bottom of the tab. The Apply new settings dialog box appears. Keep the **Reset all terminals** option selected and click **OK**. The settings are then distributed to all connected terminals.

### 13.9.3 Print drivers for Device Spooling

To enable users to send jobs directly to the printing device and use Device Spooling, you have to create a new print port and set a port protocol and port number. When configuring the port, use the **Raw** protocol and one of the four following ports:

- **10010:** Port for direct print. The job is automatically printed after it is received by the printing device.
- **10011:** Port for secured hold print. The job is spooled by the printer and waits there until the user logs in and prints it. It is not possible to print this job on any other than this particular printing device.
- **10012:** Port for Device Spooling Print&Follow. The job is spooled by the printing device. Once the user logs on any of the devices connected to the same subnet, information about this job is provided and the job is displayed in the list of the available jobs and can be printed.
- **10013:** Port for Device Spooling delegated print. Works the same as the Device Spooling Print&Follow, except that the job can be printed by delegates of the sending user.



### 13.9.4 IP filters

To ensure proper functioning of the offline Print&Follow feature, you have to turn off IP filters or set a new IP filter which includes all the IP addresses of the printing devices, where the Print&Follow jobs can be stored.

### 13.9.5 Print languages supported by Device Spooling

The following print languages are supported by Device Spooling:

- PCL XL
- PCL5c
- KPDL
- PDF

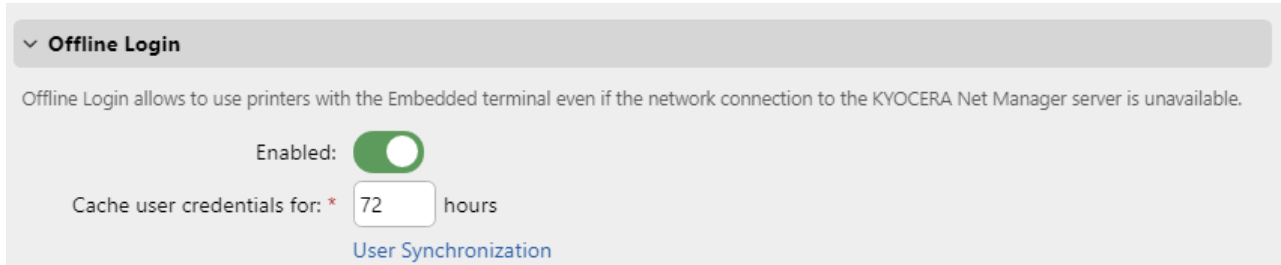
## 13.10 Offline Login

For **KNM** to operate properly, a 100% reliable network connection is necessary. Connection problems can lead to serious issues; for example, users may not be able to start their user sessions on the printing devices and perform any copy, print or scan actions. The **Offline Login** feature prevents such situations. User information, including credentials, are cached at the device and if the server is unavailable, cached data are used for user authentication. Users can then log in and perform all the actions that do not require network access to the **KNM** server.

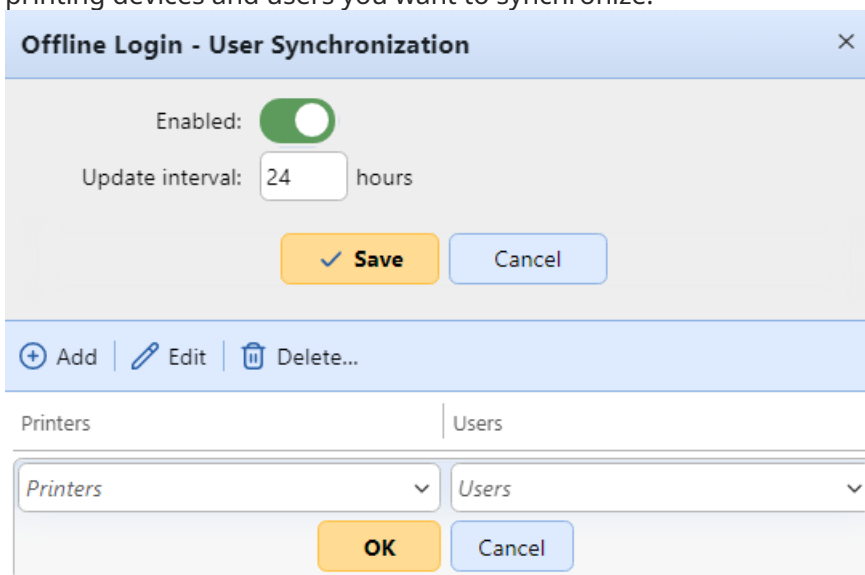
When combined with Client or Device Spooling, the offline login feature offers a robust backup plan for server outages.

### 13.10.1 Offline Login setup

Go to **KYOCERA, Settings, Printers & Terminals** on the **KNM** Web administrator interface. In the **Offline Login** section, you can enable the feature and change its settings:



- **Enabled:** Click to enable or disable the feature.
- **Cache user credentials for \_\_ hours:** The device remembers the credentials for the set time period (in hours); after the period ends, users cannot log in the offline mode anymore.
- **User Synchronization:** Opens the Offline Login - User Synchronization properties panel. On the panel, you can enable the user synchronization, set the update interval (in hours), and manage printing devices and users you want to synchronize.



You can synchronize max. 100 users to one printing device. If a group contains more users, only the first 100 users will be synchronized with the printing device.

It is possible to store 3 ID Cards and 3 PINs per user via User Synchronization. A user's credentials (ID Card or PIN) are also stored on the device if there was an active user session while the server was still online.

If after you change the settings the Apply new settings dialog box appears, keep the **Reset all terminals** option selected and click **OK**. The settings are then distributed to all connected terminals.

## 13.10.2 Offline Login via LDAP server credentials

When the offline login feature is enabled in a **KNM** printing environment where LDAP credentials are used for user authentication, information about the LDAP servers is automatically stored on the embedded terminal. In case the connection to the **KNM** server is lost, users can log in via their LDAP credentials in the offline mode. The credentials are verified against the LDAP server.

Requirements:

- The PIN or ID Card login methods are the only ones supported. This can be set in the printers' configuration profile.
- The connection needs to be secure.
- There must be a connection from the printing device to the LDAP server.

## 13.10.3 Offline Login Limitations

- Credit is not supported
- Quota is not supported;
- Projects - print jobs are set to the *Without Project* option

## 13.11 Fallback Printing

With **KNM** Desktop Client installed and running on the end user's workstation, you can select a backup printing device to be used for print when connection to the **KNM** server is lost. The **Fallback printing** feature serves as an important backup tool in case of a server outage. Furthermore, it can be combined with the **Client or Device Spooling** and the **Offline login** features on **KNM** embedded terminals to enable using hold print, Print&Follow, and delegated print on the printing device.

- For information on how to install and set up **KNM** Desktop Client on client's computers, see the **KNM** Desktop Client for Windows guide.
- For information about support and setup of the **Device Spooling** and the **Offline login** features on a particular **KNM** embedded terminal, see the respective **KNM** embedded terminal manual.

After the installation, you need to configure the print driver port to send print files to **KNM** Desktop Client, which then sends them either to the **KNM** server or directly to the printing device, depending on the availability of connection to the **KNM** server.

### 13.11.1 Windows settings

The settings in the Configure Standard TCP/IP Port Monitor dialog box must have the following values:

- **Printer Name or IP Address:** *127.0.0.1* (IP address of the localhost in Windows) or *localhost*
- **Protocol:** *LPR*
- **Queue Name:** queue name according to the **KNM** server setting (same as if printing to the **KNM** server)
- **LPR Byte Counting Enabled:** *Selected*
- **SNMP Status Enabled:** *Deselected*

Configure Standard TCP/IP Port Monitor ✕

Port Settings

Port Name:

Printer Name or IP Address:

Protocol

Raw  LPR

Raw Settings

Port Number:

LPR Settings

Queue Name:

LPR Byte Counting Enabled

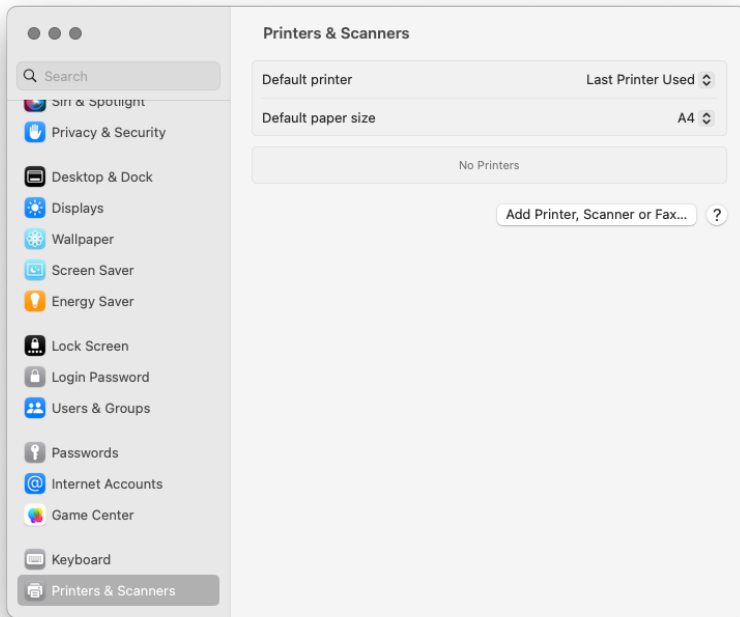
SNMP Status Enabled

Community Name:

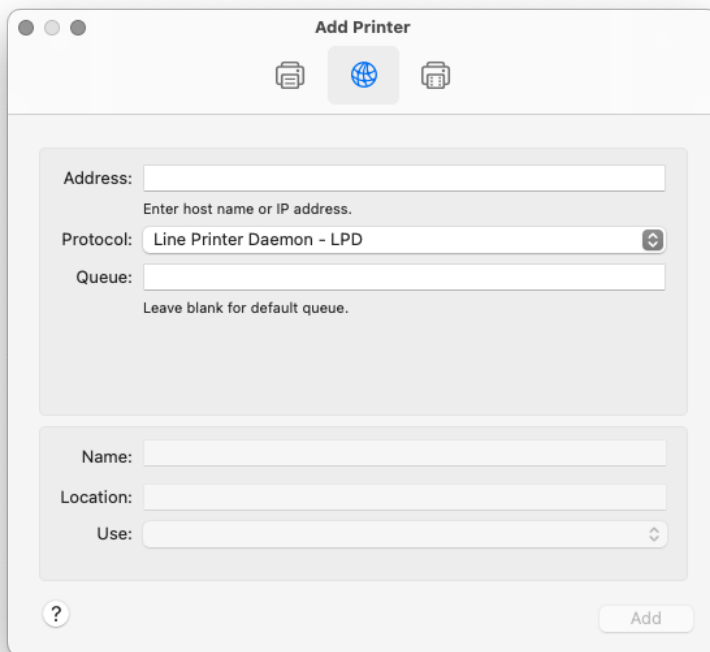
SNMP Device Index:

### 13.11.2 MacOS settings

- Go to **Apple menu > System Preferences**, and then click **Printers & Scanners**.
- Click **Add Printer, Scanner or Fax** to add a new printer.



- In the ribbon, select the IP icon. In the **Protocol** field, select *Line Printer Daemon - LPD* from the list.



- In the **Address** field, add the IP address or hostname of the localhost or **KNM** server's IP address. In the **Queue** field, add a queue name according to the **KNM** server setting. Add a

**Name**, and optionally a **Location** for your printer. In the **Use** field, select a printer driver from the list. Click **Add** to setup the printer.

The screenshot shows the 'Add Printer' dialog box with the following fields and values:

- Address:** 127.0.0.1 (Note: Valid and complete host name or address.)
- Protocol:** Line Printer Daemon - LPD
- Queue:** KNM (Note: Leave blank for default queue.)
- Name:** Fallback Printer
- Location:** (Empty field)
- Use:** Kyocera ECOSYS P8060cdn (KPDN)

- Once the printer is set up, it appears on the Printers & Scanners list.

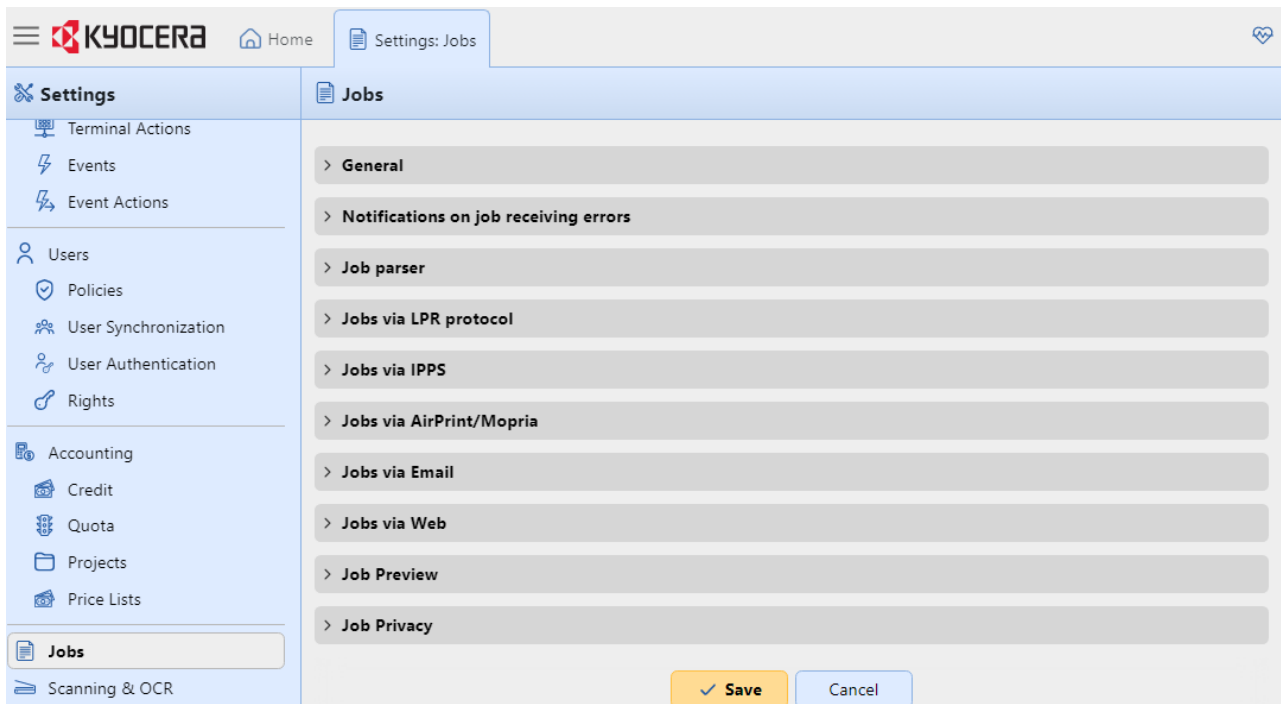
# 14 Jobs

This topic discusses one of the key functions of **KNM** — setting and management of print jobs. It covers the following subjects:

- Print jobs global settings: [Jobs settings tab](#)
- Print jobs list, individual jobs settings and deleting jobs: [List of jobs](#), [Editing jobs](#), [Deleting jobs](#)
- [Page Description Languages \(PDL\)](#)
- Print jobs parser: [Jobs Parser](#)
- Notifying users and the administrator about refused jobs: [Notifying the admin and users about refused jobs](#)
- Using PDL commands for additional job processing actions: [Processing Jobs via PDL Commands](#)
- You can use PHP scripts to further process the job after it is received by the **KNM** server: [Scripting \(PHP\)](#)
- When your brand supports PDL (page description language) check out this chapter: [Prologue, Epilogue](#)
- Setting up and previewing jobs: [Jobs Preview](#)
- When you have a dedicated Job Archiving license and the Job Preview feature set up on the **KNM** server, you can automatically archive all print jobs that are sent to **KNM**: [Job Archiving](#)

## 14.1 Jobs settings tab

On the **Jobs** settings tab, you can set the global properties of jobs in the **KNM** print environment.



### General

Here you can set the **Maximum job size** (default size is *600MB*).

In the **Office file formats** subsection, you can select the method of processing and printing the Office format files. You can select from *Convert to PDF* (default) and *Via a Windows printer*. For details check [Processing documents in Office formats](#).

### Notifications on job receiving errors

Check the **Notify the administrator via email** and/or the **Notify the job sender via email** boxes, to send notification emails about refused jobs.

The job sender is always notified via **KNM** Desktop Client, if installed.

### Job parser

Here you can activate, or deactivate the Job parser tool. You need to activate the Job Parser if you want to know job details (page count, color, paper size, etc.) before the job is printed. It is necessary for features like credit, quota and PHP scripting. If you don't use these features, you might want to disable the Job parser, as it is CPU intensive. The default setting is **Enabled**.

### Jobs via LPR protocol

Here you can enable the **Jobs via LPR protocol** feature (*enabled* by default). If it is deactivated, **KNM** cannot receive print jobs via LPR.

The server knows the job sender (to be able to notify **KNM** Desktop Client about job processing) through the hostname sent by the LPR protocol. The maximum length of the hostname is 31 characters.

The maximum job size received over LPR is *100GB*. Jobs with a size of over *2GB* are described as: "*More than 2GB*"; for jobs below *2GB*, the real size is displayed.

It is recommended to keep the **Jobs via LPR protocol** option enabled. If it is disabled, jobs sent from print drivers cannot be received by **KNM**.

You can also change the **port** here, although it is recommended to use the default setting (*515*).

### Jobs via IPPS

Here you can enable printing jobs via the IPPS protocol. You can also change the **port** here (default is *8631*).

For more information, see [Jobs via IPPS](#).

### Jobs via mobile devices

This feature allows you to use mobile printing via AirPrint or Mopria. It is enabled by default.

The standard **port** is *8632* and it's editable.

For more information, see [mobile printing via AirPrint or Mopria](#).

### Jobs via Email

Here you can enable or disable the **Jobs via Email** feature, which enables receiving print jobs sent via email. The email attachment is processed and sent as a print job (the email body can be processed as well). PDF/A, TXT and JPEG formats are supported. For MS Office formats, MS Office or LibreOffice must be installed on the **KNM** server.

For more information, see [Printing from email and from the KNM Web UI](#).

### Jobs via Web

Here you can enable or disable the **Jobs via Web** feature, which enables users receiving print jobs via the **KNM** web interface. You can also set the maximum job file size here between *20MB* to *120MB* (*120MB* by default).

For more information, see [Printing from email and from the KNM Web UI](#).

### **Job Preview**

Here you can enable/disable and set up **Job Preview**.

For more information, see [Jobs preview](#).

### **Job Privacy**

Here you can enable the **Job Privacy** feature.

For more information, see [Job Privacy](#).

### **Watermark collections section**

Here you can set up watermark collections.

For more information, see [Watermarks](#).

## **14.2 List of jobs**

On the list of jobs on the **Jobs** main tab, you can see all print jobs and information about them.

### **14.2.1 Jobs display options**

On the left side of the **Jobs** main tab, you can see the **All jobs** drop-down menu. On the menu you can select from the following options:

- **Ready** - Displays jobs ready to print.
- **Paused** - Displays paused jobs.
- **Printed** - Displays printed jobs.
- **Favorite** - Displays favorite jobs.
- **Failed jobs** - Displays failed jobs.
- **Deleted** - Displays deleted jobs.
- **All** - Displays all jobs.

### **14.2.2 Job status**

There are seven print job status types:

- **Processing** - The job is being examined and prepared for printing.
- **Ready** - The job has been placed on a print queue and is waiting for users to authorize it or for preceding jobs to finish.
- **Paused** - The job has been manually paused by the user or automatically by the **KNM** system.
- **Printing** - The job is being sent to the printing device.
- **Printed** - The job has been printed and is stored on the **KNM** server. The print job is marked as Printed when it was completely sent to the printer. On a printer where **KNM** can check actual printing results (printers with EMB terminal 8.1 and higher), this status is updated according to the printing results.
- **Failed** - The job was either not parsed correctly, failed to be processed or had no metadata (not allowed) and failed to be printed.
- **Deleted** - The job has been deleted from the **KNM** server.

### 14.2.3 Favorite jobs

All print jobs, except for the deleted ones, can be marked as **Favorite**. Favorite print jobs are not automatically deleted after the period set on the **System Maintenance** settings tab and remain permanently stored on the **KNM** server, except for favorite jobs from external code books that are no longer available at the code book's data source.

## 14.3 Editing jobs

To open a print job properties panel, double-click the job on the list on the **Jobs** main tab (or select the job, then click **Actions** on the toolbar above, and then click **Edit** in the job action dialog box). The panel opens on the right side of screen.

On the panel, you can see general information about the print job, such as its name and ID, size, its author and the IP address of the author's computer. If you use the **Job Parser** tool, you can see additional data such as the B&W total, color copies, number of copies, paper format, duplex, toner saving, staple, punch, the printer language used, and the price of the job. For more information, see [Job Parser](#).

You can also change the print job's **Owner** and **Project** in their respective list boxes.

Only an administrator and user group leaders can change the owner of a print job. The administrator can move jobs between all users and the user group leader can move jobs between members of their subordinate group.

If you change the job owner, the new owner has to have rights to the current queue and project. If you change the project, the current job owner has to have rights to the new project.

### 14.3.1 Deleting jobs

To delete selected jobs:

1. On the jobs list on the **Jobs** main tab, select the jobs that you want to delete, and then click **Actions**.
2. In the Actions drop-down box, click **Delete**. You can find the deleted jobs on the **Deleted** jobs list.

## 14.4 Page Description Languages (PDL)

A page description language (PDL) is a language that describes the appearance of a printed page. It receives a code of a document sent to a printing device, interprets it and uses it to instruct the printing device where and how to place text and graphics onto the print page.

The most common page description languages are **PCL 5**, **PCL 6 (XL)** and **PostScript**.

## 14.5 Job Parser

An embedded print job parser is a part of the **KNM** system. This tool provides you with additional information about individual print jobs.

Based on those, you can set additional print job rules, or control the job price before a job is printed. This is important, especially for credit accounting and quotas.

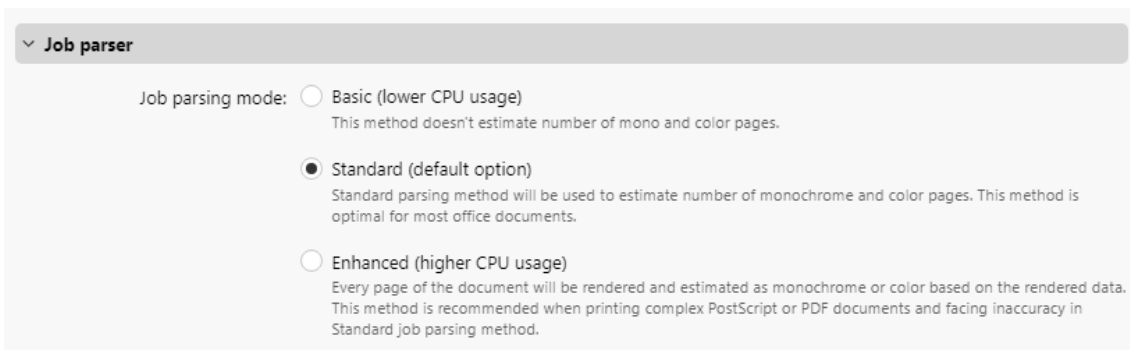
The job parser supports the majority of available printer drivers in PCL5, PCL6 and PostScript.

The job parser provides the following information:

- page description language (PDL)
- job name
- user name
- number of B&W pages
- number of color pages
- number of copies
- Simplex/Duplex option
- paper format
- staple
- punch
- toner saving

The job parser is activated by default on the **Jobs** settings tab during a new installation. An upgrade will keep the old setting.

There are three available **Job parsing modes**:



- **Basic (lower CPU usage)** - This method doesn't estimate the number of mono and color pages.
- **Standard (default option)** - The standard parsing method will be used to estimate the number of monochrome and color pages. This method is optimal for most office documents.
- **Enhanced (higher CPU usage)** - Every page of the document will be rendered and estimated as monochrome or color based on the rendered data. This method is recommended when printing complex PostScript or PDF documents and facing inaccuracy in the Standard job parsing method.

## 14.6 Notifying the admin and users about refused jobs

In case a print job is refused for some reason, for example if it was sent to a wrong queue, or if the user has been denied printing by a **KNM** policy, the job owner and the **KNM** administrator can both be informed about the event.

The administrator can be notified via email, and the user can be notified via email or via a small pop-up dialog box at the bottom-right corner of the screen. Users are just notified about the event, whereas the administrator is informed about the problem's details.

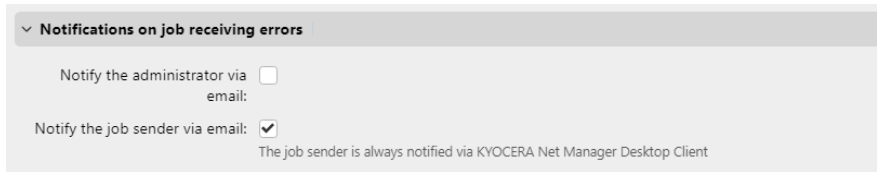
To be able to see the pop-up messages, users should have the **KYOCERA Net Manager Desktop Client** application installed and running on their computers.

### To activate the notifications via email

On the **Jobs** settings tab, under **Notifications on jobs receiving errors**, you can select two options:

- **Notify the administrator via email:** The email message is sent to the administrator's email address set on the **General** settings tab, under **General**.

- **Notify the job sender via email:** the email message is sent to the primary email address set as **Email** on the user's properties panel on the **Users** settings tab.



### To activate the notifications via the KYOCERA Net Manager Desktop Client pop-up window

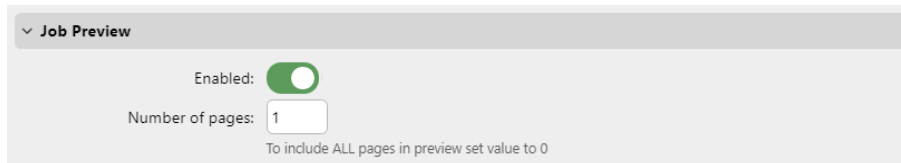
The only condition for activation of the pop-up notification for a user is for **KNM** Desktop Client to be installed and running on their computer.

For information on how to install and set up **KNM** Desktop Client, see the **KNM** Desktop Client for Windows or macOS guide.

## 14.7 Jobs Preview

The **Job Preview** feature is used to generate previews of jobs. The most common use case is viewing a job before printing it, be it in either the **KNM** Web UI or on an embedded terminal. In addition, it is also internally used during Job Archiving, where the Job Preview engine is used to generate a PDF/A preview of the given job.

To enable Job Preview, go to **KYOCERA, Settings, Jobs, Job Preview**.



It is possible to limit the **Number of pages** to be generated (*1* by default) in the preview. To include all the pages, set the value to *0*. When the number of pages is changed and there is an already existing generated preview for a job with the old number of pages, the next request to generate a preview will generate a new one with the currently selected number of pages.

## 14.8 Job Archiving

With a dedicated **Job Archiving** license and the **Jobs Preview** feature set up on the **KNM** server, you can automatically archive all print jobs that are sent to **KNM**. On selected brands of printing devices, you can also archive all copy and scan jobs.

This way you can have full control over what has been printed, scanned and copied within your printing environment, which can be required for example in high security areas in order to be able to identify sources of data leaks.

For information on how to acquire the **Job Archiving** license, please contact the your support.

### 14.8.1 Setting up job archiving

The feature is not part of the default setup of the **KNM** server and before the **Job archiving** license is added to the server, the settings of the feature on the **KNM** Web Interface are hidden from the administrator.

After you add the licenses, you can set up the feature on the **Jobs** settings tab, in the **Job archiving** section.

You can enable or disable the feature and change the **Archive folder**, where the jobs are archived (by default it is the *Archive* sub-folder of the **KNM** data folder).

In the **Resolution** drop-down, you can choose *72 (default)*, *100*, *200*, *300*, or *200 DPI*.

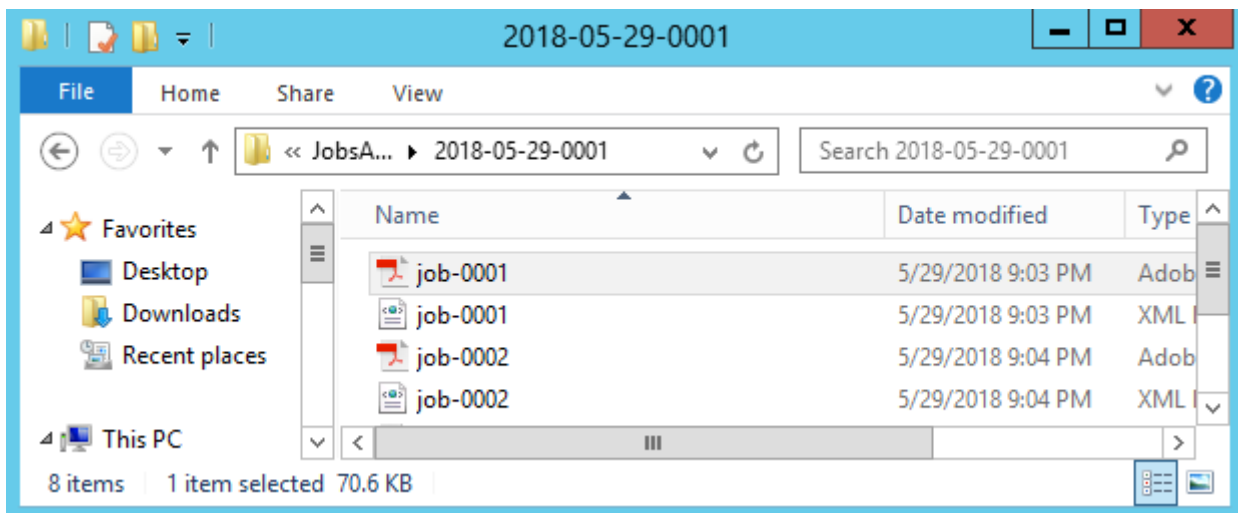
In the **Page range** drop-down, you can choose *All (default)*, *1*, *2*, *3*, *4*, *5*.

## 14.8.2 Viewing archived jobs

The jobs are stored in subfolders of the **Archive folder**, each of these sub-folders has the form: **YYYY-MM-DD-XXXX**, where the front part informs about the date when the sub-folder was created, while the number at the last part serves to sort sub-folders created in the same day.

In the subfolders, you can find two files for each of the printed, copied or scanned jobs:

- a PDF file with the preview of the job
- an XML file with basic information about the job, such as the type of the job or the username of the printing user.

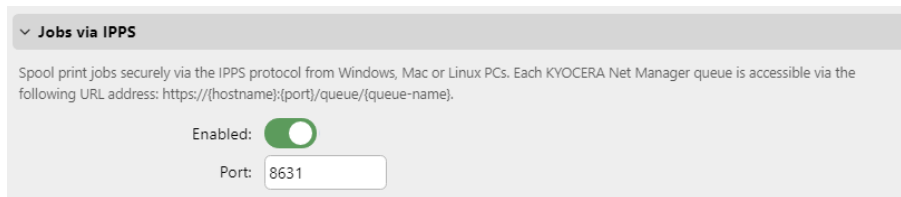


```
<?xml version="1.0" encoding="UTF-8"?>
- <data>
  <timestamp>2018-05-29 21:03:39</timestamp>
  <username>eliot.kate</username>
  <jobType>copy</jobType>
  <serverName>10.14.5.96</serverName>
  <serverVersion>7.1.0.366</serverVersion>
  <printerAddr>10.14.4.12</printerAddr>
  - <files>
    <file>job-0001.pdf</file>
  </files>
</data>
```

## 14.9 Jobs via IPPS

To use **Jobs via IPPS** you should first adjust the following:

- Make sure that the IPP client is enabled on your machine. For example, on Windows 10, this should be enabled by default, but on Windows Servers, you need to enable it explicitly:
  - Control Panel - Programs - Turn Windows features on or off - in the dialog, click **Next** until you get to the features tab - Install "Internet Printing Client", and Restart the machine.
- Next, you need to install the **KNM** certificate on your machine. For example, in **KNM** Server 8.2+, you can create a self-signed certificate in the following way (check [here](#) for more info):
  - Go to **KYOCERA, Settings, Communication Security**. Select *Built-in Certificate Authority*, add your host name as a Subject Alternative Name (SAN), click **Generate new**, click **Save**, and then **Export**.
  - Install the certificate and place it into Trusted Root Certification Authorities.
  - Restart all **KNM** services.
- Enable Jobs via IPPS in **KYOCERA, Settings, Jobs, Jobs via IPPS**.



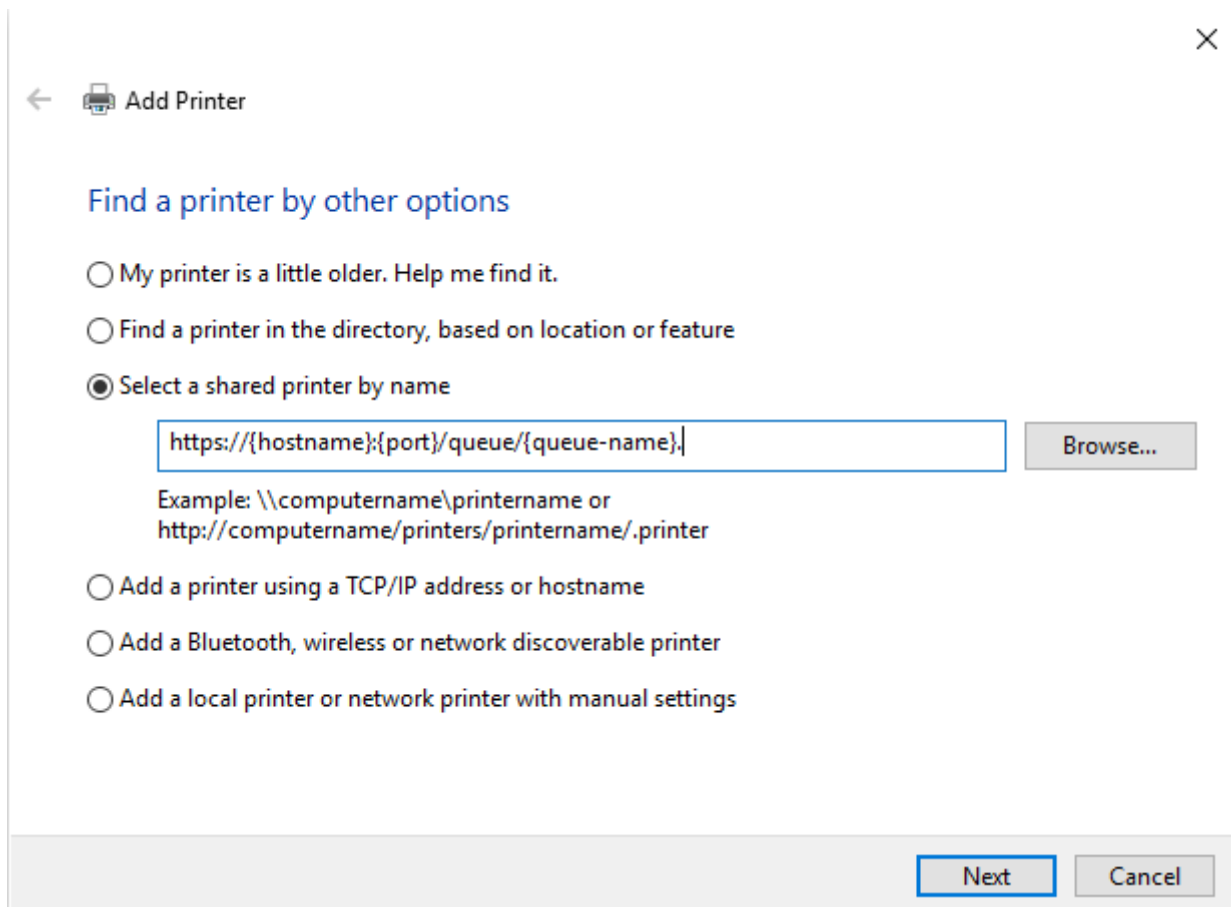
The feature is available on [Windows](#), [Linux](#), [Chromebooks](#) and [Mac PCs](#). For all of them you need to adjust the URL `https://{hostname}:{port}/queue/{queue-name}` to your own needs to get IPPS working. For the port number use the one set in **KYOCERA, Jobs, Jobs via IPPS** (8631 by default).

**⚠** PM Server uses the 631 port for IPP print and 717 for IPPS and cannot be changed (see **KYOCERA, Settings, Network, PM Server**), so these values cannot be used for **KNM** IPPS printing.

The maximum job size received over IPPS is unlimited.

### 14.9.1 IPPS via Windows

When you add a new network printer to be used with IPPS, make sure to search using the queue name, host name and port in the URL.




The sharing of a Windows IPPS printer is not supported.

## 14.9.2 IPPS via macOS

To add IPPS printing via macOS:

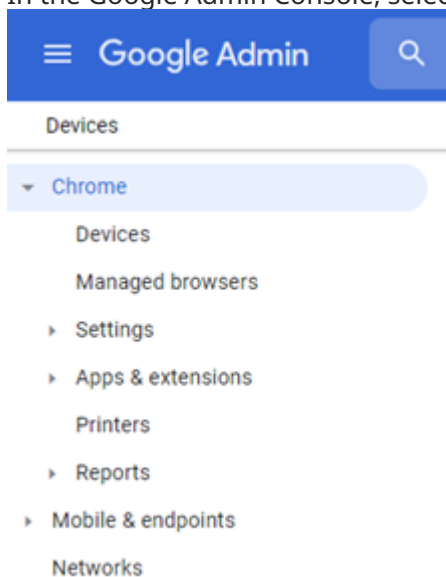
1. Go to the **Add printer** page.
2. Go to the **IP** tab on the ribbon.
3. Fill out the following fields:
  - a. **Address:** add the server IP or hostname and the server port in the following format: "ServerIP or hostname":"port". For example, *10.12.15.19:8631*
  - b. **Protocol:** select the **AirPrint** protocol.
  - c. **Queue:** add /queue/ and then the name of the **KNM** queue. For example, */queue/MarketingQueue*
4. Click **Add**.

 Since AirPrint is used, users are required to sign in to be able to print.

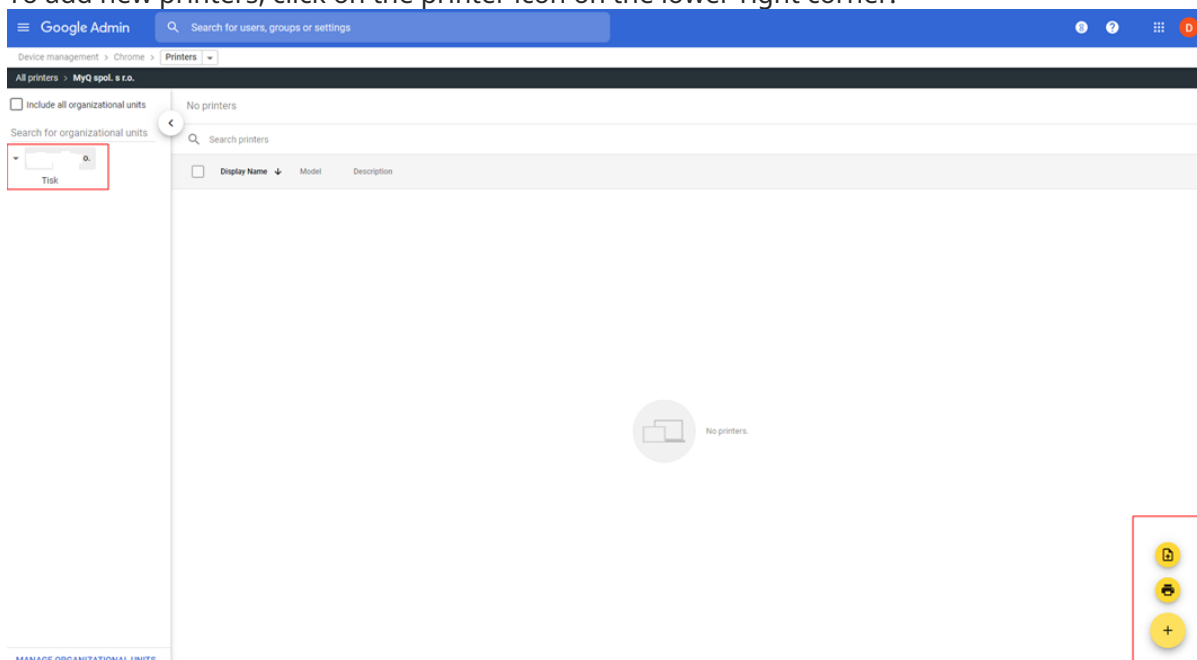
## 14.9.3 IPPS via Chromebook

To add IPPS printing via Chromebook:

1. In the Chromebook, sign in to your Google Admin Console in <https://admin.google.com/> using an administrator account.
2. In the Google Admin Console, select **Devices** and then **Chrome** and **Printers**.



3. To apply the IPPS setting to all the printers, select the top organizational unit on the list. Otherwise, select any of the child units.
4. To add new printers, click on the printer icon on the lower-right corner.



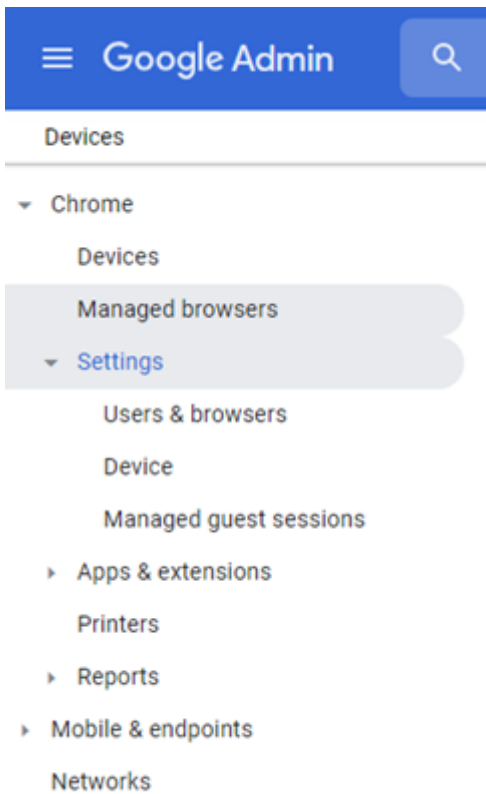
5. In the **Add Printers** window, fill in the mandatory fields and adjust the device URL `https://{hostname}:{port}/queue/{queue-name}` according to your own configuration.
6. Select **ADD PRINTER** and the new printer is now created.

7. Select the new printer to confirm if the IPPS settings are applied according to the organization's configuration.

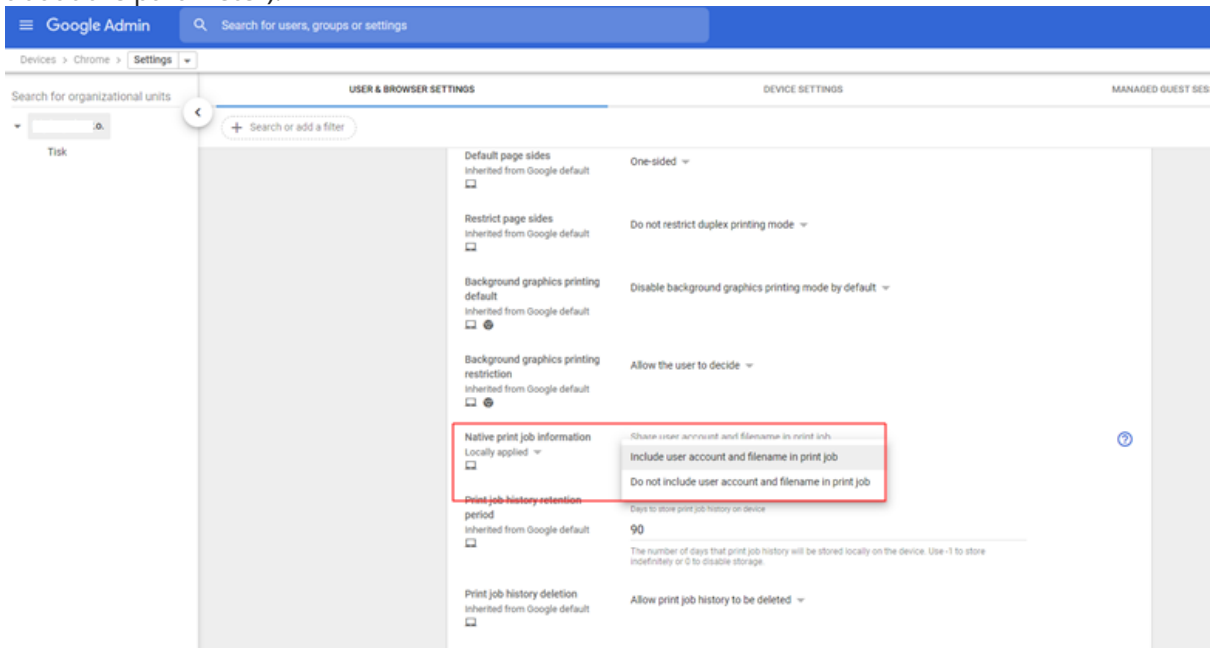
**⚠** The driverless configuration is not recommended as there might be jobs that cannot be printed this way. There is no error in the Chromebook when this happens and not on **KNM**'s side either, since the job never reaches **KNM**.

### To include user accounts and file names in the jobs printed via Chromebook:

1. In the Chromebook, sign in to your Google Admin Console in <https://admin.google.com/> using an administrator account.
2. In the Google Admin Console, select **Devices, Chrome, Settings** and then **Users & browsers**.

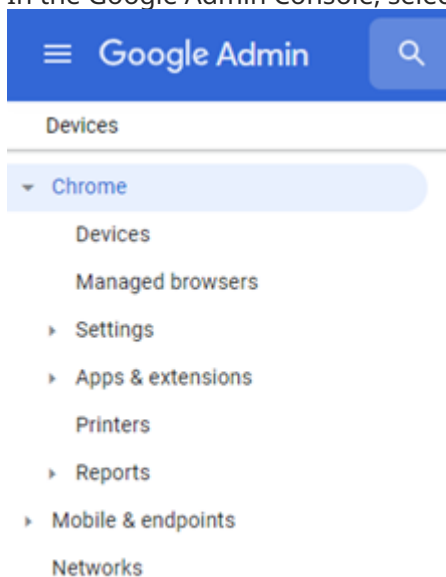


3. In the Users & browsers settings window, scroll down to **Printing – Native print job information**. From the drop-down, select *Include user account and filename in print job* (You can click on the question mark icon next to **Native print job information**, to see extra information about the parameter).

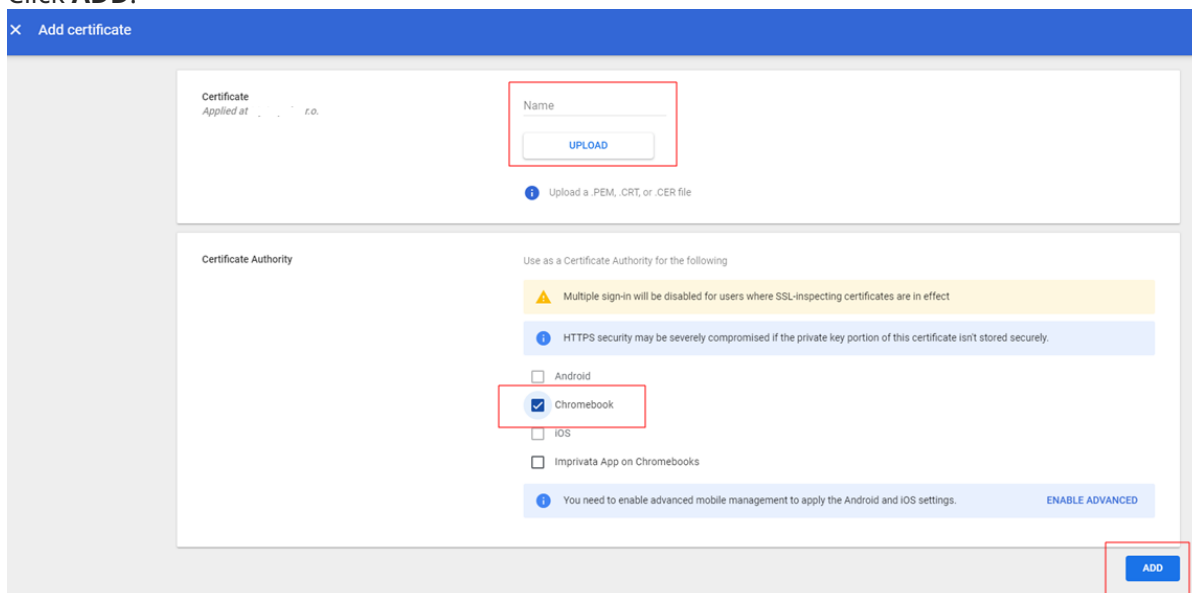


If you want to (optionally) deploy SSL certificates via the Google Admin Console:

1. In the Chromebook, sign in to your Google Admin Console in <https://admin.google.com/> using an administrator account.
2. In the Google Admin Console, select **Devices** and then **Chrome** and **Networks**.



3. In the Networks window, select **Certificates** and in the Certificates window, select **Add Certificate**.
4. Type a **Name** for the certificate and click Upload to upload your certificate.
5. In the Certificate Authority section, choose Chromebook.
6. Click **ADD**.

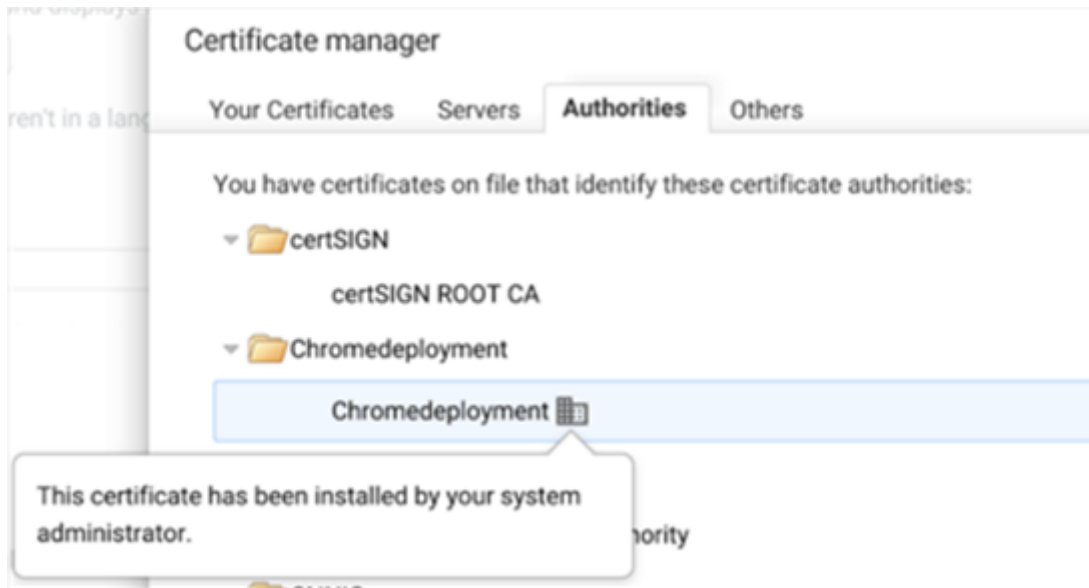


To deploy the certificate, use an open guest Wi-Fi network. Your Chrome devices will authenticate to Google and receive the TLS or SSL certificate. The pushed certificate will apply to all enrolled Chrome devices on the primary domain.

To verify the CA on managed Chrome devices:

- Go to *chrome://settings/certificates*.

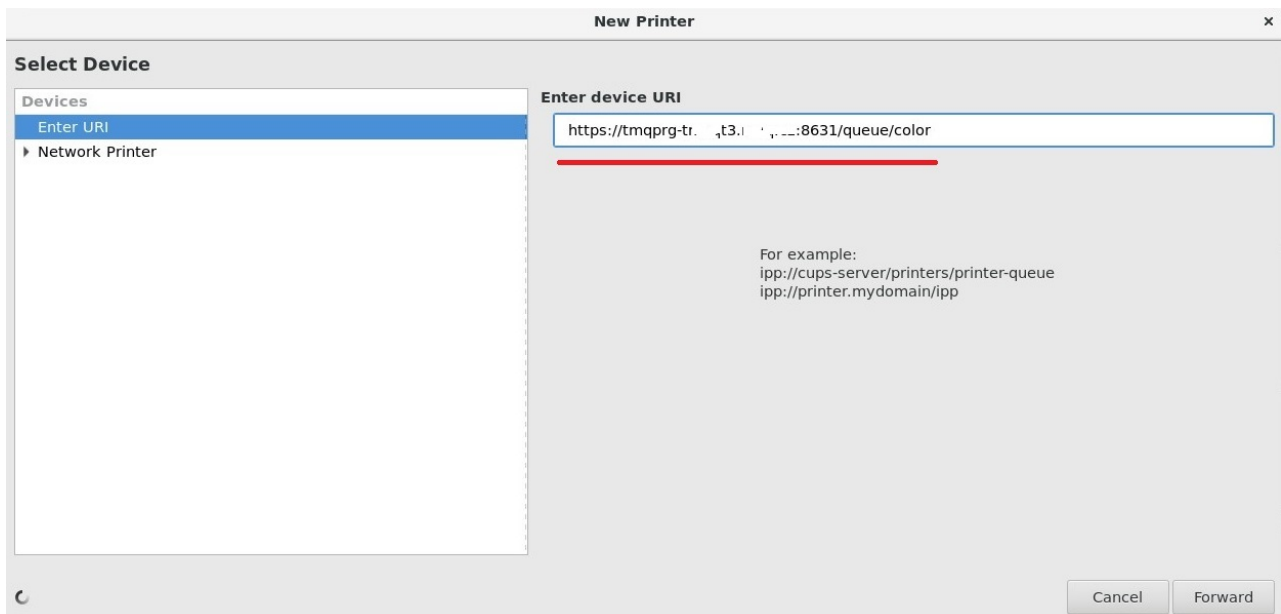
- Click **Authorities**.
- Scroll down to see the newly-added CAs. CAs setup in your Admin console is highlighted as follows:



#### 14.9.4 IPPS via Linux

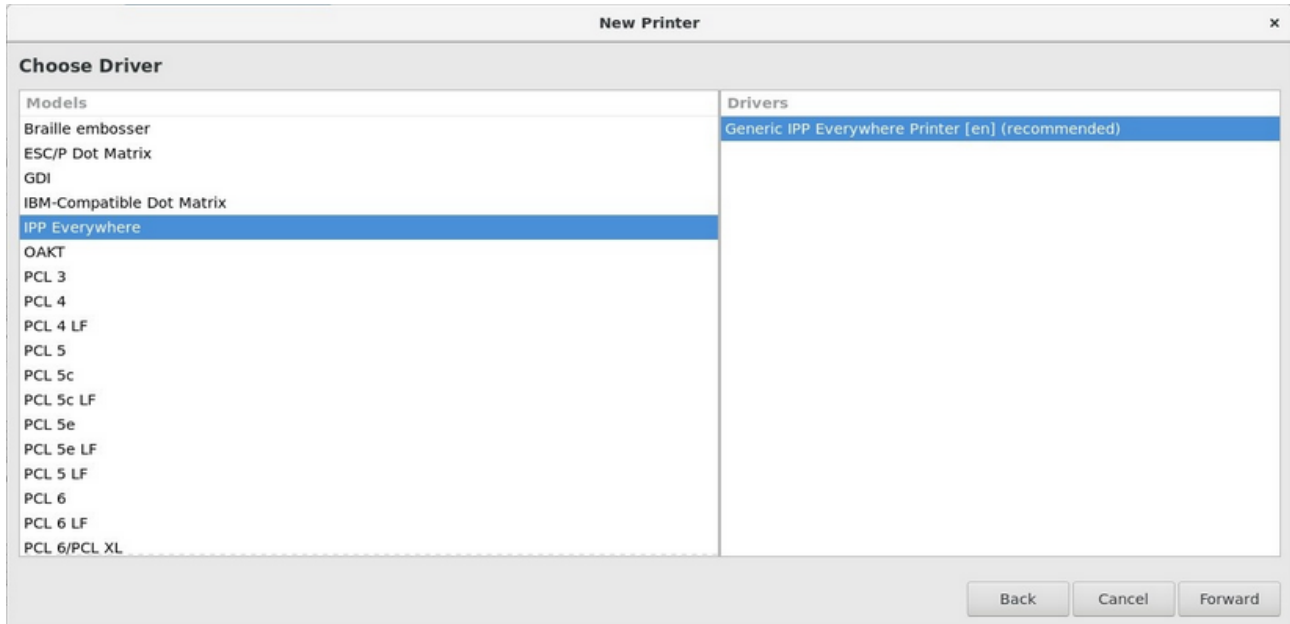
To add IPPS printing via Linux:

- Set up a CUPS service in order to add a printer.
- Add a printer with the **KNM** Print Server hostname.
- In the New Printer window, click **Enter URI**. Type the device URL in the **Enter device URI** field, in the *https://{hostname}:{port}/queue/{queue-name}* format.




- Click **Forward**.

- In the Choose Driver pane, mark **Select printer from database**, and then select *Generic*.
- Click **Forward**.
- In the next window, under **Choose Driver**, select *IPP Everywhere*. Although the selection option says IPP, this protocol is used for IPPS spooling.



- Click **Forward**.
- Enter the name of the printer.
- Click **Finish**.


 IPPS Authentication is not used (job is assigned according to username).

## 14.10 Job Privacy

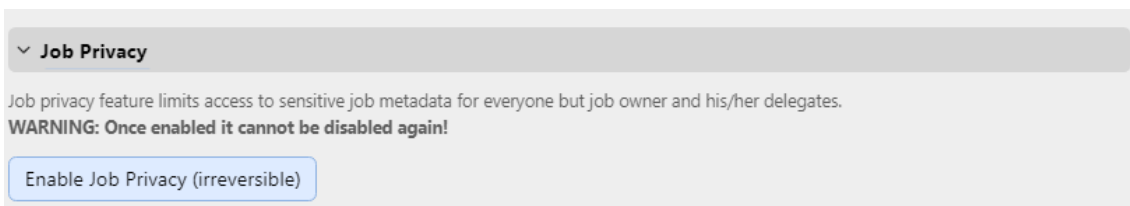
The Job privacy feature limits access to sensitive job metadata for everyone, except for the job owner and their delegates.

You can enable the feature in the **Jobs** settings tab (**KYOCERA, Settings, Jobs**).

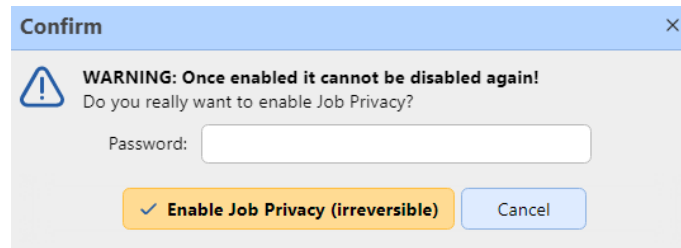
If you have a **KNM** Central server setup and Job Privacy is enabled at your Central server, it will be automatically enabled on all the connected Site servers.

 Once the Job Privacy feature is enabled, it cannot be disabled again!

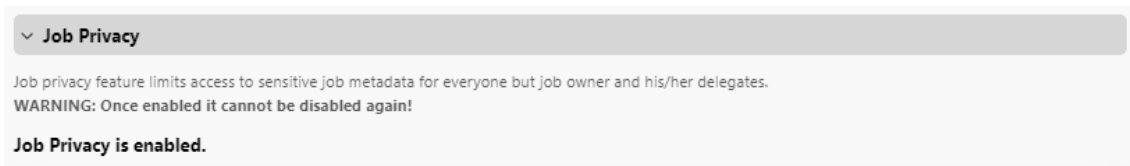
To use the feature, click on the **Enable Job Privacy (irreversible)** button.



In the confirmation pop-up, type your **KNM** administrator password in the **Password** field, and click **Enable Job Privacy (irreversible)**.



The Job Privacy feature is now enabled.



## 14.11 Watermarks

On the **KNM** Web Interface, you can create collections of watermarks and associate them with the queues where they will be used. Each collection can contain multiple watermarks and can be associated with any number of queues.

PostScript, PCL6 and PDF drivers are supported, but should be selected by the user when they want to see the watermarks printed in their document.

Jobs sent to a queue will have the watermarks of the associated collection printed on each page.

Individual watermarks can be positioned horizontally at the top of the page, horizontally at the bottom of the page, or diagonally. The text size of the watermark can be from 6 to 25. You can also represent the text of the watermark as a QR code or a Bar code.

A watermark collection cannot be deleted if there is at least one queue attached to it.

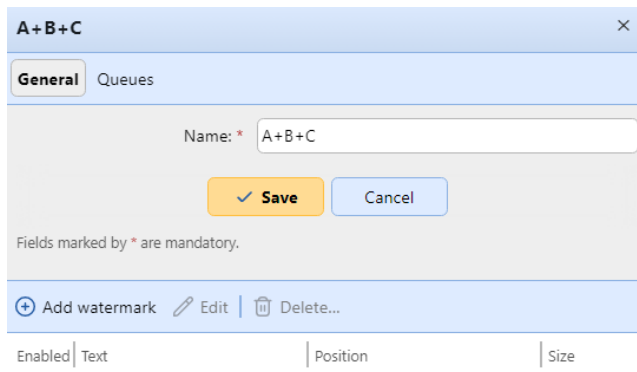
### 14.11.1 Creating, editing, and deleting watermark collections

The watermark collections can be created in the **Watermark collections** section at the bottom of the **Jobs** settings tab (**KYOCERA, Settings, Jobs**).

#### Creating a new watermark collection

To create a new watermark collection:

1. On the **Jobs** settings tab, in the **Watermark collections** section, click **+Add**. The properties panel of the new collection opens on the right side of the screen.
2. On the panel, enter the **Name** of the collection, then **Add watermarks** to it, and lastly click **Save**.



## Editing a watermark collection

The properties panel of the collection opens immediately after the collection is created. To open a properties panel of an already existing collection, select it on the list on the **Jobs** settings tab, under **Watermark collections**, and click **Edit**.

On the properties panel, you can rename the collection, create and remove watermarks, and assign or remove them from queues.

## Deleting a watermark collection

To delete a collection:

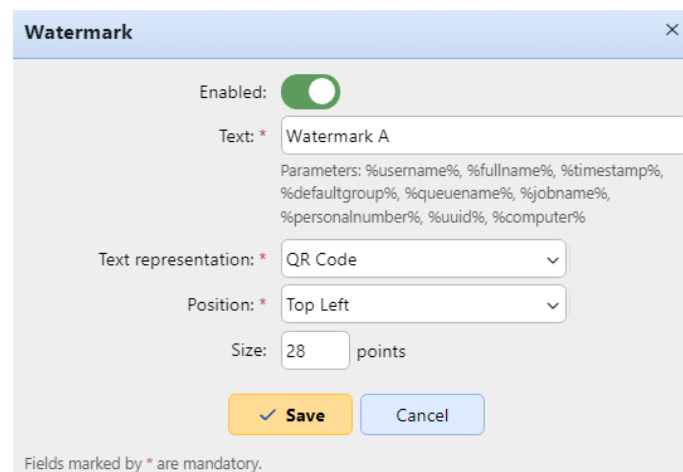
On the **Jobs** settings tab, under **Watermark collections**, select the collections that you want to delete, and then click **Delete**.

## 14.11.2 Adding, editing, and deleting watermarks

Within each watermark collection, you can create an unlimited number of watermarks. Each of the watermarks in the collection can be activated or deactivated.

### Creating a new watermark

On the properties panel of the watermark collection, on the **General** tab, click **+Add watermark**. The properties panel of the new watermark opens. On the panel, set up the watermark, and then click **Save**.



## Editing a watermark

The properties panel of a watermark opens immediately after the watermark is created. To open the properties of an already existing watermark, double-click it on the list on the **Jobs** main tab, under **Watermark collections**.

Each watermark has the following properties:

- **Enabled:** Enable/disable the watermark
- **Text:** Text of the watermark; max. length: 512 characters.
- **Text representation:** National characters which are included in the font (standard New Times Roman) are included for Text. The QR/Bar Codes support generally any Unicode text. Restrictions can be found here: [QR Code](#), [Code 128](#), [PDF417](#), and the most restrictive [Code 39](#). The text can be represented in the following forms:
  - Text
  - QR Code
  - BAR Code 128
  - BAR Code 39
  - BAR Code PDF417
- **Position:** The watermark's position on the page (the default is: *Bottom right*)
  - Top
  - Top Left
  - Top Right
  - Bottom
  - Bottom Left
  - Bottom Right
  - Diagonal: "Bottom to Top" (only available when *Text* is selected as **Text representation**; greyed out in *QR* and/or *BAR code*)
  - Diagonal: "Top to Bottom" (only available when *Text* is selected as **Text representation**; greyed out in *QR* and/or *BAR code*).
- **Size:** The watermark's text size (the default is: 28 and the **Font** is *Times New Roman*, which can be changed in the *config.ini*) should be a number from 6-85
  - 28 is small,
  - 57 is medium,
  - 85 is large.
- **Transparency:** Only visible when *Text* is selected as **Text representation**. The available values are:
  - Dark
  - Medium
  - Light



A watermark in Postscript does not reflect paper orientation. It always prints as portrait.

## Deleting a watermark

On the properties panel of the watermark collection, select the watermarks that you want to delete, and then click **Delete**.

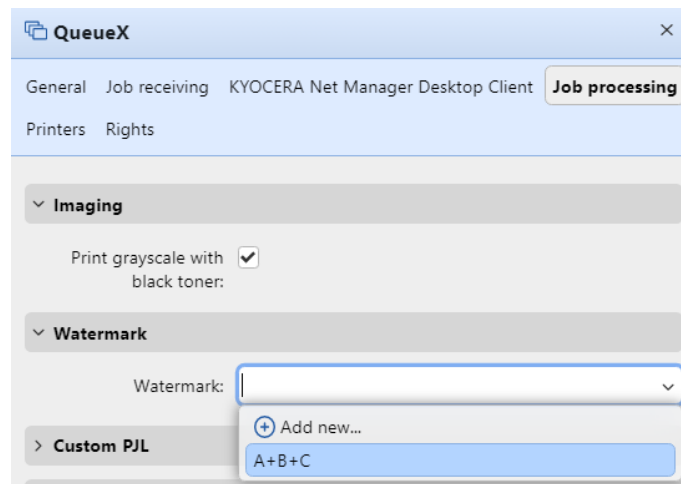
### 14.11.3 Attaching watermark collections to queues

You can attach a watermark collection to a queue either within the setup of the collection, or within the setup of the queue.

Each queue can have only one watermark collection attached to it.

#### Attaching watermark collections to queues within the setup of the queues

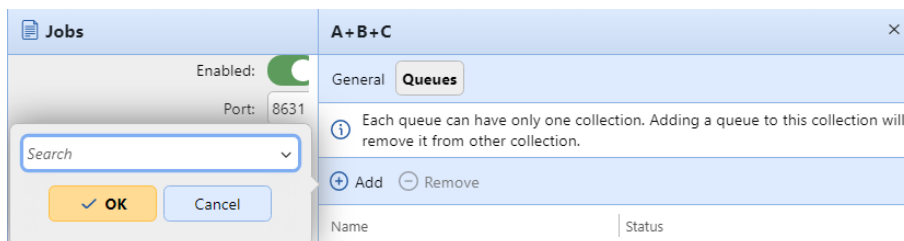
The collection can be selected on the **Job processing** tab of the properties panel of the queue. To open the properties panel, go to **KYOCERA, Queues**, and then double-click the queue on the list. On the **Job processing** tab, in the **Watermark** section, select the **Watermark** from the drop-down, and then click **Save**.



#### Attaching watermark collections to queues within the setup of the collections

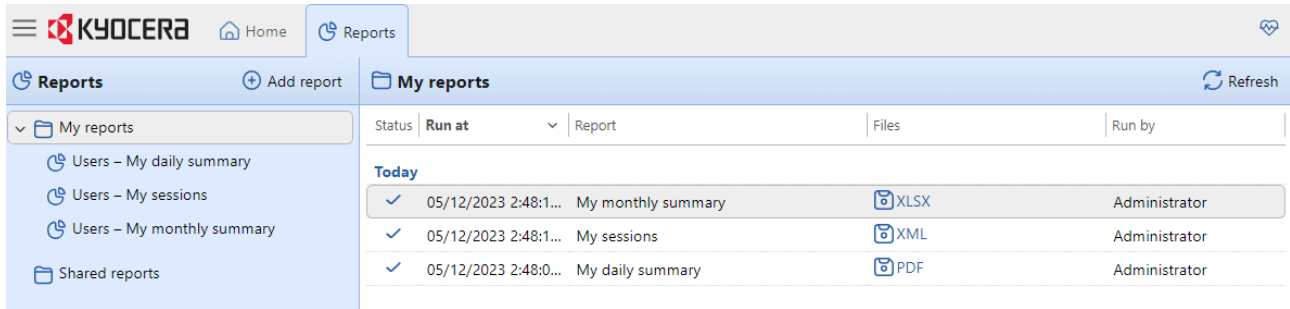
To assign a new queue to a watermark collection, select it on the on the list on the **Jobs** settings tab, under **Watermark collections**, and click **Edit**.

1. On the properties panel of the watermark collection, click **Queues**. The **Queues** tab opens.
2. On the tab, click **+Add**. A dialog box with a selection of queues appears.
3. Select the queue from the drop-down, and then click **OK**.



## 15 Reports

In the **KNM** web interface, on the **Reports** main tab (**KYOCERA, Reports**), you can create and generate reports with a variety of data concerning your printing environment. The reports can be related to users, printing devices, print jobs, etc.



Reports in **KNM** are divided into two main categories: **My reports** and **Shared reports**. **My reports** show users reports created by themselves, while **Shared reports** show them reports created by the administrator or by other users.

There are three default reports: **My daily summary**, **My sessions** and **My monthly summary**. These are displayed in the **My reports** folder of the **KNM** administrator, who can modify them, delete them or change their design. For all the other users, the default reports are displayed in the **Shared reports** folder and cannot be changed in any way.

In addition to the three default reports, the administrator can create an unlimited number of reports and sort them into sub-folders of the **My reports** folder. Users can create their own reports but they are limited to use only certain report types depending on the rights granted by the administrator.

Each report can be directly displayed on the web interface and saved in any of the following formats: *PDF*, *CSV*, *XML*, *XLSX* and *ODS*. The reports can be automatically generated and stored in a predefined folder. There is no data limitation for the generated report, it includes all the data from the specified period.

All the reports have the **KNM** logo displayed by default, but it can be replaced by your company's logo. To upload a custom logo go to **KYOCERA, Settings, Personalization**. In the **Custom application logo** section, click **+Add** next to **Custom logo** and upload your own file (supported formats - *JPG*, *JPEG*, *PNG*, *BMP* and recommended size - *398px x 92px*).

### 15.1 Report Types

When you are creating reports on the **Reports** main tab, you can choose from a large number of built-in report types that are sorted into multiple categories. Some of the types are included in more categories (for example, *Groups: Daily Summary*, *Print Jobs: Daily Summary*, etc.), while some of the types are particular to only one category (for example, *Device Alerts in Alerts Maintenance* or *Credit Balance in Credit & Quota*).

You can overview all of the report types on the **Reports** settings tab, under **Report types** (in **KYOCERA, Settings, Reports**).

Type	Name	Category
<b>Alerts and maintenance</b>		
Built-in	Counter analysis	Alerts and maintenance
Built-in	Event History	Alerts and maintenance
Built-in	Toner replacement	Alerts and maintenance
Built-in	Top N alerts summary	Alerts and maintenance
<b>Credit and quota</b>		
Built-in	Credit balance	Credit and quota
Built-in	Credit operations	Credit and quota
Built-in	Quota status for groups	Credit and quota
Built-in	Quota status for users	Credit and quota
<b>Environmental</b>		
Built-in	Expired and deleted jobs	Environmental
Built-in	Printers	Environmental
Built-in	User groups	Environmental
Built-in	Users	Environmental
<b>General</b>		

### Providing users with rights to use a report

The administrator can run all the built-in reports and provide other users and groups with rights to run them as well. In **KYOCERA, Settings, Reports**, right-click on a report and click **Edit**. On the **General** tab, in the **Permission for running the report** field, choose users and groups from the list and click **Save**.

You can also add custom report types developed by the **KNM** development team. To do so, just click **+Add**, upload the custom report definition file, select users or groups to access it, and click **OK**. For more information about custom report types, please contact your support.

### 15.1.1 Report Categories

- **Alerts and Maintenance** - These reports provide information about device alerts and unusual changes on device counters.
- **Credit and Quota** - These reports contain information concerning credit and quota, for example the remaining credit or the state of quota of selected users.
- **Environmental** - These reports inform about the environmental impact of printing. They show how many trees needed to be harvested, how much energy was spent and how much carbon dioxide was emitted during the production of the paper used for printing and copying within your company's printing environment.

Data sources vary in their estimations. **KNM** calculations in the report are based on the following data estimates:

- **Carbon dioxide for paper production:** 12,7 gram per paper sheet
- **Energy used for production:** 48 Wh per paper sheet or 32Wh for a recycled paper sheet
- **Trees:** 8333 paper sheets are counted as 1 tree.

- **General** - These reports provide general information about the **KNM** system, such as total counters statistics and printing peaks or comparison of price lists used for printers.
- **Groups** - These reports inform about groups of users. They can contain information about membership, printed pages, weekly stats etc.
- **Print Jobs** - These reports contain information about jobs printed in **KNM**, such as the list of all expired and deleted jobs over a certain period.
- **Printers** - These reports inform about all the printing devices in the **KNM** system (both local and network). Generated reports can contain graphs of the device usage, daily, weekly and monthly counters, etc.
- **Projects** - These reports contain information regarding projects and project accounting in **KNM**, such as daily summary of projects or projects assigned to selected users over a certain period.
- **Users** - These reports can contain various information about users. They can concern their print jobs, credit statements, printed pages etc.

## Alerts and Maintenance Reports

The reports included in the **Alerts and Maintenance** category are:

- **Counter analysis**
- **Event history**
- **Toner replacement\*\***
- **Top N alerts summary**

Parameters, filters and columns available:

Name	Parameters	Filters	Default Columns	Group by
<b>Counter analysis</b>	Period Page counter	Printer name User name User group Page counter value (<, =, >)	Printer name Full name Session finish date Page counter B&W pages Color pages Total pages Scans Total price (additional column: Administrator price)	User name
<b>Event history</b>	Period	Event name Printer name	Event name Event type Printer name Created Resolved	

Name	Parameters	Filters	Default Columns	Group by
<b>Toner replacement</b>	Period	Printer name	Printer name Toner color Installed Replaced Pages printed Total counters	
<b>Top N alerts summary</b>	Period N	Printer name	Alert name Alert training level Alert code Occurrences	Alert name

The above reports don't support aggregate columns.

Charts are not available, except for the **Top N alerts summary** report where a *Pie, Doughnut* or *Bar* chart can be selected with the **Alert name** and **Occurrences** values.

### \*\* Toner replacement report addendum

The number displayed in the Toner replacement report in the Pages printed and Total counters columns depends on the toner it relates to:

- **Pages printed** - The number of pages printed with the replaced toner. Only color pages for color toners (CMY) and all pages for black toners (K) are considered.
- **Total counters** - Total counters of the printer related to the replaced toner. Color pages for color toners (CMY) and all pages for black toners (K) are considered.

## Credit and Quota Reports

The reports included in the **Credit and Quota** category are:

- **Credit balance**
- **Credit operations**
- **Quota status for groups**
- **Quota status for users**

Parameters, filters and columns available:

Name	Parameters	Filters	Default Columns	Additional Columns
<b>Credit balance</b>		User name User group	User name Full name User group Credit balance	Personal number Phone Email Notes

Name	Parameters	Filters	Default Columns	Additional Columns
<b>Credit operations</b>	Period	User name User group	Full name User group Created (date & time) Credit charge Credit balance Operation type Charge method Charger name Voucher code	Personal number Phone Email Notes
<b>Quota status for groups</b>		User group	Quota name Quota period Counter type Counter limit Counter value Quota usage (%) Quota boosts Deny print Deny copy Deny scan Deny color print Deny color copy Deny mono print Deny mono copy	Quota valid from Quota valid till
<b>Quota status for users</b>		User name User group	Full name Quota name Target type Target name Quota period Counter type Counter limit Counter value Quota usage (%) Quota boosts Deny print Deny copy Deny scan Deny color print Deny color copy Deny mono print Deny mono copy	Quota valid from Quota valid till Personal number Phone Email Notes

The above reports don't support aggregate columns, they are all grouped by the **User name** parameter and charts are not available.

## Environmental Reports

The reports included in the **Environmental** category are:

- Expired and deleted jobs
- Printers
- User groups
- Users

Parameters, filters and columns available:

Name	Parameters	Filters	Default Columns	Additional Columns
<b>Expired and deleted jobs</b>	Period	User name Queue name	Queue name Job name Created (date & time) Job size (KB) B&W pages Color pages Total pages Job owner user name Job owner full name Trees CO2 (gram) Energy (Wh) Energy recycled (Wh)	
<b>Printers</b>	Period	Printer name	Printer name Total pages Trees CO2 (gram) Energy (Wh) Energy recycled (Wh)	
<b>User groups</b>	Period	Printer name User name User group	User group Total pages Trees CO2 (gram) Energy (Wh) Energy recycled (Wh)	
<b>Users</b>	Period	Printer name User name User group	User name Full name Total pages Trees CO2 (gram) Energy (Wh) Energy recycled (Wh)	Personal number Phone Email Notes

1 tree = 8333 pages / 1 page = 12.7g of CO2 / 1 page = 48Wh of energy / 1 recycled page = 32Wh of energy

The above reports don't support aggregate columns or charts.

## General Reports

The reports included in the **General** category are:

- **Day of the week**
- **Hourly activity**
- **Monthly statistics**
- **Price list comparison**
- **Weekly statistics**

Parameters, filters and columns available:

Name	Parameters	Filters	Default Columns	Chart
<b>Day of the week</b>	Period Page counter	Printer name User name User group	Period (Day) B&W pages Color pages Total pages Scans Total price Administrator price	Pie, Doughnut or Bar <b>Category:</b> Day of the week <b>Values:</b> Page counter
<b>Hourly activity</b>	Period Page counter	Printer name User name User group	Period (Hour) B&W pages Color pages Total pages Scans Total price Administrator price	Pie, Doughnut or Bar <b>Category:</b> Daily hours <b>Values:</b> Page counter
<b>Monthly statistics</b>	Period	Printer name User name User group	Period (Year - Month) B&W pages Color pages Total pages Scans Total price <b>(Additional columns:</b> Administrator price Simplex Duplex)	Line <b>X-axis:</b> Month & year <b>Y-axis:</b> Page counter
<b>Price list comparison</b>	Pricelist Item	Printer name	Printer name B&W price Color price	Bar <b>Category:</b> Printers <b>1st value:</b> Pricelist item

Name	Parameters	Filters	Default Columns	Chart
<b>Weekly statistics</b>	Period	Printer name User name User group	Period (Year - Week) B&W pages Color pages Total pages Scans Total price <b>(Additional columns:</b> Administrator price Simplex Duplex)	Line <b>X-axis:</b> Month & year <b>Y-axis:</b> Page counter

The above reports don't support aggregate columns.

## Groups Reports

The reports included in the **Groups** category are:

- **Counters by function and duplex(BETA)**
- **Counters by function and paper format(BETA)**
- **Counters by function paper format and duplex(BETA)**
- **Daily summary**
- **Day of the week**
- **Monthly summary**
- **Top N**
- **Total summary**
- **User group membership**

Parameters, filters and columns available:

Name	Filters	Default Columns	Additional Columns	Group by
<b>Counters by function and duplex(BETA)</b>	Printer name User name User group Project name Accounting group	Group name User name Full name Print B&W Simplex Print Color Simplex Print B&W Duplex Print Color Duplex Print Sheets Copy B&W Simplex Copy Color Simplex Copy B&W Duplex Copy Color Duplex Copy Sheets	Notes Personal Number Email Incoming Fax B&W Simplex Incoming Fax B&W Duplex Fax Sheets	Group name User name

Name	Filters	Default Columns	Additional Columns	Group by
<b>Counters by function and paper format(BETA)</b>	Printer name User name User group Project name Accounting group	Group name User name Full name Print A4 B&W Print A4 Color Copy A4 B&W Copy A4 Color Print A3 B&W Print A3 Color Copy A3 B&W Copy A3 Color	Notes Personal Number Email Incoming Fax A4 B&W Incoming Fax A4 B&W Print A5 B&W Print A5 Color Copy A5 B&W Copy A5 Color Incoming Fax A5 B&W Print B4 B&W Print B4 Color Copy B4 B&W Copy B4 Color Incoming Fax B4 B&W Print B5 B&W Print B5 Color Copy B5 B&W Copy B5 Color Incoming Fax B5 B&W Print Ledger B&W Print Ledger Color Copy Ledger B&W Copy Ledger Color Incoming Fax Ledger B&W Print Letter B&W Print Letter Color Copy Letter B&W Copy Letter Color Incoming Fax Letter B&W Print Legal B&W Print Legal Color Copy Legal B&W Copy Legal Color Incoming Fax Legal B&W Print Statement B&W Print Statement Color Copy Statement B&W Copy Statement Color Incoming Fax Statement B&W	Group name User name

Name	Filters	Default Columns	Additional Columns	Group by
<b>Counters by function paper format and duplex(BETA)</b>	Printer name User name User group Project name Accounting group	Group name User name Full name A4 B&W Simplex A4 Color Simplex A4 B&W Duplex A4 Color Duplex A3 B&W Simplex A3 Color Simplex A3 B&W Duplex A3 Color Duplex A4 Sheets A3 Sheets	Notes Personal Number Email Incoming Fax A4 B&W Incoming Fax A4 B&W Print A5 B&W Print A5 Color Copy A5 B&W Copy A5 Color Incoming Fax A5 B&W Print B4 B&W Print B4 Color Copy B4 B&W Copy B4 Color Incoming Fax B4 B&W Print B5 B&W Print B5 Color Copy B5 B&W Copy B5 Color Incoming Fax B5 B&W Print Ledger B&W Print Ledger Color Copy Ledger B&W Copy Ledger Color Incoming Fax Ledger B&W Print Letter B&W Print Letter Color Copy Letter B&W Copy Letter Color Incoming Fax Letter B&W Print Legal B&W Print Legal Color Copy Legal B&W Copy Legal Color Incoming Fax Legal B&W Print Statement B&W Print Statement Color Copy Statement B&W Copy Statement Color Incoming Fax Statement B&W	Group name User name

Name	Filters	Default Columns	Additional Columns	Group by
<b>Daily summary</b>	Printer name User name User group	Date B&W pages Color pages Total pages Scans Total price	Administrator price B&W prints B&W copies Color prints Color copies Single color copy A4 paper A3 paper A5 paper B4 paper B5 paper Other paper Folio paper Ledger paper Legal paper Letter paper Statement paper Rest of paper formats Fax B&W cost Color cost Color pages (L1) Color cost (L1) Color pages (L2) Color cost (L2) Color pages (L3) Color cost (L3) Print color pages(L1) Copy color pages (L1) Cost color pages(L1) Print color pages(L2) Copy color pages (L2) Cost color pages(L2) Print color pages(L3) Copy color pages (L3) Cost color pages(L3) Simplex Duplex	Group name

Name	Filters	Default Columns	Additional Columns	Group by
<b>Day of the week</b>	Printer name User name User group	Day B&W pages Color pages Total pages Scans Total price	Same as Daily summary + Day number	Group name
<b>Monthly summary</b>	Printer name User name User group	Period (Year - Month) B&W pages Color pages Total pages Scans Total price	Same as Daily summary	Group name Month & Year
<b>Top N</b>	Printer name User name User group	Group name B&W pages Color pages Total pages Scans Total price	Administrator price	
<b>Total summary</b>	Printer name User name User group Accounting group	Full name User name Group name Period (Year & Month) B&W print B&W copies Color print Color copies Total pages Scans Total price	Same as Daily summary	Accounting group
<b>User group membership</b>	User group Accounting group Managed group	User name Full name Group name Accounting group Managed group	Personal number Phone Email Notes	

The above reports all have the *Period* parameter, except for the **Top N** report that has the *Period*, *Page counter*, *N*, *Add remaining sum* parameters.

The above reports don't support aggregate columns except for the **Monthly summary** and the **Total summary** reports.

Charts are not available, except for the **Top N** report, where a Pie, Doughnut or Bar chart can be selected with the **Groups** and **Page Counter** values.

## Printers Reports

The reports included in the **Printers** category are:

- **Counters by function and duplex(BETA)**
- **Counters by function and paper format(BETA)**
- **Counters by function paper format and duplex(BETA)**
- **Daily summary**
- **Day of the week**
- **Meter reading via SNMP**
- **Monthly summary**
- **Top N**
- **Total summary**

Parameters, filters and columns available:

Name	Filters	Default Columns	Additional Columns	Group by
<b>Counters by function and duplex(BETA)</b>	Printer name User name User group Project name Accounting group	Printer Name Serial Number Group name User name Full name Print B&W Simplex Print Color Simplex Print B&W Duplex Print Color Duplex Print Sheets Copy B&W Simplex Copy Color Simplex Copy B&W Duplex Copy Color Duplex Copy Sheet	Notes Personal Number Email Incoming Fax B&W Simplex Incoming Fax B&W Duplex Fax Sheets	Printer name User name

Name	Filters	Default Columns	Additional Columns	Group by
<b>Counters by function and paper format(BETA)</b>	Printer name User name User group Project name Accounting group	Printer name Serial number Group name User name Full name Print A4 B&W Print A4 Color Copy A4 B&W Copy A4 Color Print A3 B&W Print A3 Color Copy A3 B&W Copy A3 Color	Notes Personal Number Email Location IP address Brand Model MAC Incoming Fax A4 B&W Incoming Fax A4 B&W Print A5 B&W Print A5 Color Copy A5 B&W Copy A5 Color Incoming Fax A5 B&W Print B4 B&W Print B4 Color Copy B4 B&W Copy B4 Color Incoming Fax B4 B&W Print B5 B&W Print B5 Color Copy B5 B&W Copy B5 Color Incoming Fax B5 B&W Print Ledger B&W Print Ledger Color Copy Ledger B&W Copy Ledger Color Incoming Fax Ledger B&W Print Letter B&W Print Letter Color Copy Letter B&W Copy Letter Color	Printer name User name

Name	Filters	Default Columns	Additional Columns	Group by
			Incoming Fax Letter B&W Print Legal B&W Print Legal Color Copy Legal B&W Copy Legal Color Incoming Fax Legal B&W Print Statement B&W Print Statement Color Copy Statement B&W Copy Statement Color Incoming Fax Statement B&W	
<b>Counters by            function paper            format and            duplex(BETA)</b>	Printer name User name User group Project name Accounting group	Printer name Serial number Group name User name Full name A4 B&W Simplex A4 Color Simplex A4 B&W Duplex A4 Color Duplex A3 B&W Simplex A3 Color Simplex A3 B&W Duplex A3 Color Duplex A4 Sheets A3 Sheets	Notes Personal Number Email Location IP Address Brand Model MAC A5 B&W Simplex A5 Color Simplex A5 B&W Duplex A5 Color Duplex A5 Sheets B4 B&W Simplex B4 Color Simplex B4 B&W Duplex B4 Color Duplex B4 Sheets	Printer name User name

Name	Filters	Default Columns	Additional Columns	Group by
			B5 B&W Simplex B5 Color Simplex B5 B&W Duplex B5 Color Duplex B5 Sheets Folio B&W Simplex Folio Color Simplex Folio B&W Duplex Folio Color Duplex Folio Sheets Ledger B&W Simplex Folio Color Simplex Folio B&W Duplex Folio Color Duplex Folio Sheets Ledger Color Simplex Ledger B&W Duplex Ledger Color Duplex Ledger Sheets Letter Color Simplex Letter B&W Duplex Letter Color Duplex Letter Sheets Legal Color Simplex Legal B&W Duplex Legal Color Duplex Legal Sheets Statement Color Simplex Statement B&W Duplex	

Name	Filters	Default Columns	Additional Columns	Group by
			Statement Color Duplex Statement Sheets Other Color Simplex Other B&W Duplex Other Color Duplex Other Sheets	

Name	Filters	Default Columns	Additional Columns	Group by
<b>Daily summary</b>	Printer name User name User group	User name Full name Date B&W pages Color pages Total pages Scans Total price	Administrator price B&W prints B&W copies Color prints Color copies Single color copy A4 paper A3 paper A5 paper B4 paper B5 paper Other paper Folio paper Ledger paper Legal paper Letter paper Statement paper Rest of paper formats Fax B&W cost Color cost Color pages (L1) Color cost (L1) Color pages (L2) Color cost (L2) Color pages (L3) Color cost (L3) Print color pages(L1) Copy color pages (L1) Cost color pages(L1) Print color pages(L2) Copy color pages (L2) Cost color pages(L2) Print color pages(L3) Copy color pages (L3) Cost color pages(L3) Simplex Duplex	Printer name

Name	Filters	Default Columns	Additional Columns	Group by
<b>Day of the week</b>	Printer name User name User group	Day B&W pages Color pages Total pages Scans Total price	Same as Daily summary + Day number	Printer name
<b>Meter reading via SNMP</b>	Printer name	Printer name IP address Serial number MAC address Model Location Terminal ID B&W prints B&W copies Color prints Color copies Scans Fax counter	A4 paper A3 paper A5 paper B4 paper B5 paper Other paper Folio paper Ledger paper Legal paper Letter paper Statement paper Rest of paper formats Start Mono Start Color Finish Mono Finish Color Printer ID Printer Group Finish M Print Finish C Print Finish M Copy Finish C Copy Finish Scan	
<b>Monthly summary</b>	Printer name User name User group	IP address Serial number MAC address Model Location B&W pages Color pages Total pages Scans Total price	Same as Daily summary	Printer name Month & Year

Name	Filters	Default Columns	Additional Columns	Group by
<b>Top N</b>	Printer name User name User group	Printer name B&W pages Color pages Total pages Scans Total price	Administrator price Printer ID Printer Group	
<b>Total summary</b>	Printer name User name User group	Printer name User group User name Full name Total pages B&W prints B&W copies Color prints Color copies Scans Total price	Same as Daily summary	Printer name

The above reports all have the *Period* parameter, except for the **Top N** report that has the *Period, Page counter, N, Add remaining sum* parameters.

Aggregate columns are supported in the above reports, except for the **Top N** and the **Monthly summary** reports.

Charts are not available, except for the **Top N** report, where a Pie, Doughnut or Bar chart can be selected with the **Printers** and **Page Counter** values.

## Print Jobs Reports

The reports included in the **Print Jobs** category are:

- **Daily summary**
- **Expired and deleted jobs**
- **Favorite jobs**
- **Printed jobs summary**

Parameters, filters and columns available:

Name	Filters	Default Columns	Additional Columns	Group by
<b>Daily summary</b>	User name Job name	Full name Created (date & time) Printed (date & time) Job name Document time	Queue name Personal number Phone Email Notes Total pages B&W pages Color pages	User name
<b>Expired and deleted jobs</b>	User name User group Queue name	Full name User name Job name Created (date & time) Document type Duplex Job size (KB) Total pages B&W pages Color pages	Personal number Phone Email Notes Trees CO2 (gram) Energy (Wh) Energy recycled (Wh)	Queue name
<b>Favorite jobs</b>	User name User group Queue name	Queue name Full name Job name Created (date & time) Job size (KB) B&W pages Color pages Total pages Min Price Max Price	Personal number Phone Email Notes	User name
<b>Printed jobs summary</b>	User name User group Job name	Full name Period Queue name Printed (date & time) Job name Document type	Personal number Phone Email Notes Total pages B&W pages Color pages	User name Month & Year

All the reports use the **Period** parameter.

Charts are not available.

The reports don't support aggregate columns except for the **Expired and deleted jobs** reports, where aggregate columns are available.

## Projects Reports

The reports included in the **Projects** category are:

- **Counters by function and duplex(BETA)**
- **Counters by function and paper format(BETA)**
- **Counters by function paper format and duplex(BETA)**
- **Daily summary**
- **Day of the week**
- **Monthly summary**
- **Print jobs per project**
- **Project groups total summary**
- **Projects per user**
- **Top N**
- **User project assignment**
- **Users per project**
- **User Session details**

Parameters, filters and columns available:

Name	Filters	Default Columns	Additional Columns	Group by
<b>Counters by function and duplex(BETA)</b>	Printer name User name User group Project name Accounting group	Project name Project code Group name User name Full name Print B&W Simplex Print Color Simplex Print B&W Duplex Print Color Duplex Print Sheets Copy B&W Simplex Copy Color Simplex Copy B&W Duplex Copy Color Duplex Copy Sheets	Notes Personal Number Email Incoming Fax B&W Simplex Incoming Fax B&W Duplex Fax Sheets	Project name User name

Name	Filters	Default Columns	Additional Columns	Group by
<b>Counters by function and paper format(BETA)</b>	Printer name User name User group Project name Accounting group	Project name Project code Group name User name Full name Print A4 B&W Print A4 Color Copy A4 B&W Copy A4 Color Print A3 B&W Print A3 Color Copy A3 B&W Copy A3 Color	Notes Personal Number Email Incoming Fax A4 B&W Incoming Fax A4 B&W Print A5 B&W Print A5 Color Copy A5 B&W Copy A5 Color Incoming Fax A5 B&W Print B4 B&W Print B4 Color Copy B4 B&W Copy B4 Color Incoming Fax B4 B&W Print B5 B&W Print B5 Color Copy B5 B&W Copy B5 Color Incoming Fax B5 B&W Print Ledger B&W Print Ledger Color Copy Ledger B&W Copy Ledger Color Incoming Fax Ledger B&W Print Letter B&W Print Letter Color Copy Letter B&W Copy Letter Color Incoming Fax Letter B&W Print Legal B&W Print Legal	Project name User name

Name	Filters	Default Columns	Additional Columns	Group by
			Color Copy Legal B&W Copy Legal Color Incoming Fax Legal B&W Print Statement B&W Print Statement Color Copy Statement B&W Copy Statement Color Incoming Fax Statement B&W	
<b>Counters by function paper format and duplex(BETA)</b>	Printer name User name User group Project name Accounting group	Project name Project code Group name User name Full name A4 B&W Simplex A4 Color Simplex A4 B&W Duplex A4 Color Duplex A3 B&W Simplex A3 Color Simplex A3 B&W Duplex A3 Color Duplex A4 Sheets A3 Sheets	Notes Personal Number Email Incoming Fax A4 B&W Incoming Fax A4 B&W Print A5 B&W Print A5 Color Copy A5 B&W Copy A5 Color Incoming Fax A5 B&W Print B4 B&W Print B4 Color Copy B4 B&W Copy B4 Color Incoming Fax B4 B&W Print B5 B&W Print B5 Color Copy B5 B&W Copy B5 Color Incoming Fax B5 B&W Print Ledger B&W	Project name User name

Name	Filters	Default Columns	Additional Columns	Group by
			Print Ledger Color Copy Ledger B&W Copy Ledger Color Incoming Fax Ledger B&W Print Letter B&W Print Letter Color Copy Letter B&W Copy Letter Color Incoming Fax Letter B&W Print Legal B&W Print Legal Color Copy Legal B&W Copy Legal Color Incoming Fax Legal B&W Print Statement B&W Print Statement Color Copy Statement B&W Copy Statement Color Incoming Fax Statement B&W	

Name	Filters	Default Columns	Additional Columns	Group by
<b>Daily summary</b>	Project name Printer name User name User group	Date B&W pages Color pages Total pages Scans Total price Project code	Administrator price B&W prints B&W copies Color prints Color copies Single color copy A4 paper A3 paper A5 paper B4 paper B5 paper Other paper Folio paper Ledger paper Legal paper Letter paper Statement paper Rest of paper formats Fax B&W cost Color cost Color pages (L1) Color cost (L1) Color pages (L2) Color cost (L2) Color pages (L3) Color cost (L3) Print color pages(L1) Copy color pages (L1) Cost color pages(L1) Print color pages(L2) Copy color pages (L2) Cost color pages(L2) Print color pages(L3) Copy color pages (L3) Cost color pages(L3) Simplex Duplex	Project name

Name	Filters	Default Columns	Additional Columns	Group by
<b>Day of the week</b>	Project name Printer name User name User group	Date B&W pages Color pages Total pages Scans Total price Project code	Same as Daily summary + Day number	Project name
<b>Monthly summary</b>	Project name Printer name User name User group	Period (year - month) B&W pages Color pages Total pages Scans Total price Project code	Same as Daily summary	Project name Month & Year
<b>Print jobs per project</b>	Project name Job name User name	Job name Printed (date & time) Document type Project code		Project name

Name	Filters	Default Columns	Additional Columns	Group by
<b>Project groups total summary</b>	Project name	Project name B&W pages Color pages Total pages Scans Total price Project code	Administrator price Group Phone Email Notes Color cost B&W cost Simplex Duplex A4 paper A3 paper A5 paper B4 paper B5 paper Other paper Folio paper Ledger paper Legal paper Letter paper Statement paper Rest of paper formats Fax B&W prints B&W copies Color prints Color copies Color pages (L1) Color cost (L1) Color pages (L2) Color cost (L2) Color pages (L3) Color cost (L3)	Project name
<b>Projects per user</b>	Project name Printer name User name User group	Full name Personal number Project name B&W pages Color pages Total pages Scans Total price Project code	Same as Daily summary	User name

Name	Filters	Default Columns	Additional Columns	Group by
<b>Top N</b>	Project name Printer name User name User group	Project name B&W pages Color pages Total pages Scans Total price Project code	Administrator price	
<b>User project assignment</b>	Project name Printer name User name User group	Full name Personal number Project name B&W pages Color pages Total pages Scans Total price Project code	Personal number Phone Email Notes	Project name

Name	Filters	Default Columns	Additional Columns	Group by
<b>Users per project</b>	Project name Printer name User name User group	User name Full name Project name Project code	Administrator price Group Phone Email Notes Color cost B&W cost Simplex Duplex A4 paper A3 paper A5 paper B4 paper B5 paper Other paper Folio paper Ledger paper Legal paper Letter paper Statement paper Rest of paper formats Fax B&W prints B&W copies Color prints Color copies Color pages (L1) Color cost (L1) Color pages (L2) Color cost (L2) Color pages (L3) Color cost (L3)	User name

Name	Filters	Default Columns	Additional Columns	Group by
<b>User Session details</b>	Project name User name Accounting group Printer name	Project Code Project Name Date Job Name User name B&W Print B&W Copy Color Print Color Copy Simplex Duplex B&W Pages Color Pages B&W Cost Color Cost Total Cost		Project name

The above reports all have the *Period* parameter, except for the **Top N** report that has the *Period, Page counter, N, Add remaining sum* parameters.

Aggregate columns are supported in the above reports, except for the **Print jobs per project, Top N** and the **User project assignment** reports.

Charts are not available, except for the **Top N** report where a Pie, Doughnut or Bar chart can be selected with the **Page Counter** values.

## Users Reports

The reports included in the **Users** category are:

- **Counters by function and duplex(BETA)**
- **Counters by function and paper format(BETA)**
- **Counters by function paper format and duplex(BETA)**
- **Daily summary**
- **Day of the week**
- **Monthly summary**
- **Session details**
- **Top N**
- **Total summary**
- **User Rights**

Parameters, filters and columns available:

Name	Filters	Default Columns	Additional Columns	Group by
<b>Counters by function and duplex(BETA)</b>	Printer name User name User group Project name Accounting group	Group name User name Full name Printer name Serial Number Print B&W Simplex Print Color Simplex Print B&W Duplex Print Color Duplex Print Sheets Copy B&W Simplex Copy Color Simplex Copy B&W Duplex Copy Color Duplex Copy Sheets	Notes Personal Number Email Location IP Address Brand Model Mac Incoming Fax B&W Simplex Incoming Fax B&W Duplex Fax Sheets	User name Printer name
<b>Counters by function and paper format(BETA)</b>	Printer name User name User group Project name Accounting group	Group name User name Full name Printer name Serial Number Print A4 B&W Print A4 Color Copy A4 B&W Copy A4 Color Print A3 B&W Print A3 Color Copy A3 B&W Copy A3 Color	Notes Personal Number Email Location IP Address Brand Model Mac Incoming Fax A4 B&W Incoming Fax A4 B&W Print A5 B&W Print A5 Color Copy A5 B&W Copy A5 Color Incoming Fax A5 B&W Print B4 B&W Print B4 Color Copy B4 B&W Copy B4 Color Incoming Fax B4 B&W Print B5 B&W Print B5 Color	User name Printer name

Name	Filters	Default Columns	Additional Columns	Group by
			Copy B5 B&W Copy B5 Color Incoming Fax B5 B&W Print Ledger B&W Print Ledger Color Copy Ledger B&W Copy Ledger Color Incoming Fax Ledger B&W Print Letter B&W Print Letter Color Copy Letter B&W Copy Letter Color Incoming Fax Letter B&W Print Legal B&W Print Legal Color Copy Legal B&W Copy Legal Color Incoming Fax Legal B&W Print Statement B&W Print Statement Color Copy Statement B&W Copy Statement Color Incoming Fax Statement B&W	

Name	Filters	Default Columns	Additional Columns	Group by
<b>Counters by function paper format and duplex(BETA)</b>	Printer name User name User group Project name Accounting group	Group name User name Full name Printer name Serial Number A4 B&W Simplex A4 Color Simplex A4 B&W Duplex A4 Color Duplex A3 B&W Simplex A3 Color Simplex A3 B&W Duplex A3 Color Duplex A4 Sheets A3 Sheets	Notes Personal Number Email Location IP Address Brand Model Mac A5 B&W Simplex A5 Color Simplex A5 B&W Duplex A5 Color Duplex A5 Sheets B4 B&W Simplex B4 Color Simplex B4 B&W Duplex B4 Color Duplex B4 Sheets B5 B&W Simplex B5 Color Simplex B5 B&W Duplex B5 Color Duplex B5 Sheets Folio B&W Simplex Folio Color Simplex Folio B&W Duplex Folio Color Duplex Folio Sheets Ledger B&W Simplex Folio Color Simplex Folio B&W Duplex Folio Color Duplex Folio Sheets Ledger Color	User name Printer name

Name	Filters	Default Columns	Additional Columns	Group by
			Simplex Ledger B&W Duplex Ledger Color Duplex Ledger Sheets Letter Color Simplex Letter B&W Duplex Letter Color Duplex Letter Sheets Legal Color Simplex Legal B&W Duplex Legal Color Duplex Legal Sheets Statement Color Simplex Statement B&W Duplex Statement Color Duplex Statement Sheets Other Color Simplex Other B&W Duplex Other Color Duplex Other Sheets	
<b>Daily summary</b>	Printer name User name User group	Full name Date B&W pages Color pages Total pages Scans Total price	Administrator price B&W cost Color cost Personal number Phone Email Notes B&W prints B&W copies Color prints Color copies	User name

Name	Filters	Default Columns	Additional Columns	Group by
			Single color copy A4 paper A3 paper A5 paper B4 paper B5 paper Other paper Folio paper Ledger paper Legal paper Letter paper Statement paper Rest of paper formats Fax B&W cost Color cost Color pages (L1) Color cost (L1) Color pages (L2) Color cost (L2) Color pages (L3) Color cost (L3) Print color pages(L1) Copy color pages (L1) Cost color pages(L1) Print color pages(L2) Copy color pages (L2) Cost color pages(L2) Print color pages(L3) Copy color pages (L3) Cost color pages(L3) Simplex Duplex	

Name	Filters	Default Columns	Additional Columns	Group by
<b>Day of the week</b>	Printer name User name User group	Full name Day B&W pages Color pages Total pages Scans Total price	Same as Daily summary + Day number	User name
<b>Monthly summary</b>	Printer name User name User group	Full name Period (year-month) B&W pages Color pages Total pages Scans Total price	Same as Daily summary	User name Month & Year
<b>Session details</b>	Printer name User name User group	User group Full name Printer name Job name Date Total pages Scans	Same as Daily summary except for Administrator price	User name
<b>Top N</b>	Printer name User name User group	User name Full name B&W pages Color pages Total pages Scans Total price		

Name	Filters	Default Columns	Additional Columns	Group by
<b>Total summary</b>	Printer name User name User group	User name Full name B&W prints B&W copies Color prints Color copies Total pages Scans Total price	Administrator price Single color copy Personal number Phone Email Notes B&W pages Color pages A4 paper A3 paper A5 paper B4 paper B5 paper Other paper Folio paper Ledger paper Legal paper Letter paper Statement paper Rest of paper formats Simplex Duplex	User name
<b>User Rights</b>	User Access Rights	User name Full name Assign access rights	Aliases Email Personal number Phone	User name

The above reports all have the *Period* parameter, and they don't support aggregate columns.

Charts are not available, except for the **Top N** report where a Pie, Doughnut or Bar chart can be selected with the **Users** and **Page Counter** values.

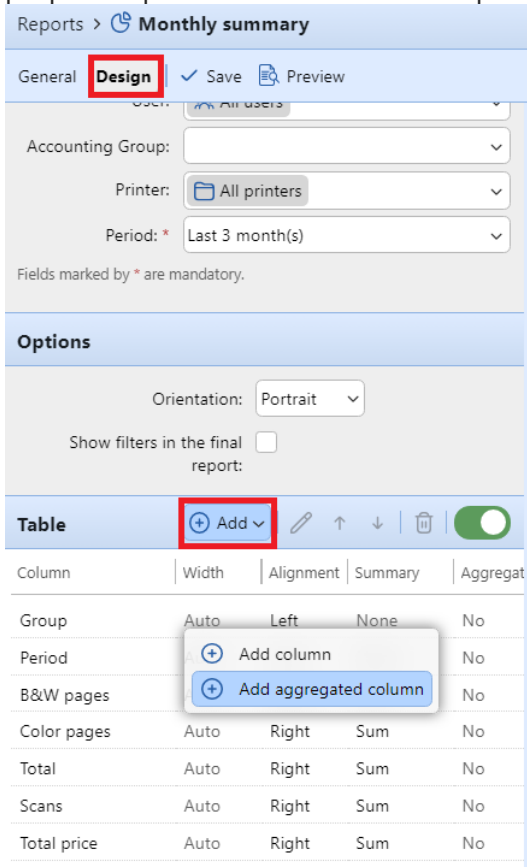
## 15.1.2 Creating new aggregated columns

For some types of reports, you can create any number of custom aggregated (summary) columns. An aggregated column can display either the sum or the average of a selection of any number of other columns available for the type.

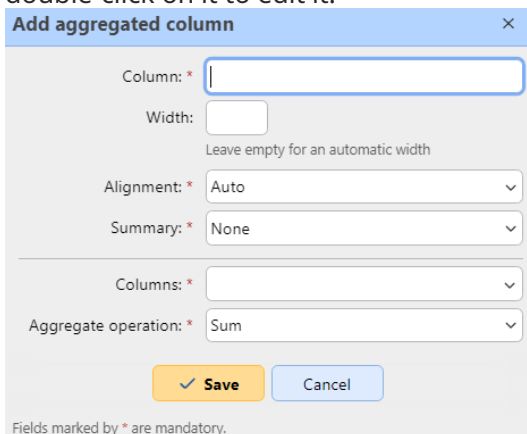
To create a new aggregated column for a report:

1. Go to **KYOCERA, Reports**. On the list of reports on the right side, select the report and click **Edit** on the ribbon (or right-click, edit). The report properties panel opens on a new window.
2. Go to the **Design** tab on the properties panel.

3. In the **Table** section, click **+Add**, and select **+Add aggregated column** from the list. The properties panel of the new column opens.



4. In the panel, set the properties, select the **Aggregate operation** you want to use (*Sum* or *Average*), and click **Save**. The new column is listed with the other table columns, and you can double-click on it to edit it.



### Supported types of reports for aggregated columns

The aggregated (summary) columns can be created for the following types of reports:

- From the **Groups** category: Monthly summary, Total summary
- From the **Print jobs** category: Expired and deleted jobs

- From the **Printers** category: Daily summary, Day of the week, Meter reading via SNMP, Total summary
- From the **Projects** category: Daily summary, Day of the week, Monthly summary, Project groups total summary, Projects per user, Users per project.

## 15.2 Reporting sources

Accounting in **KNM** depends on the **KNM** server version, the **KNM** embedded terminal version and the printing device. **KNM** 8.0+ currently uses the user-session architecture. The values in every report are based on user sessions (except for the **Meter reading via SNMP printers** report, described below).

- Counters are calculated in the following way:
  - B&W pages = B&W prints + B&W copies + Fax
  - Color pages = Color prints + Color copies + Single color copy
  - Total Pages = B&W pages + Color pages
  - Total prints = B&W prints + Color prints
  - Total copies = B&W copies + Color copies
- Price related columns include discounts.
- Any printers monitored via **KNM** Desktop Client are included in the reports.
- Any non-**KNM** users activity (\*unauthenticated) is included in the reports.
- **KNM** does not track deleted printers. If a deleted printer is later added and activated in **KNM**, the reports will not include any activity during the time the device was deleted.
- If a printer is deactivated but not deleted, the reports include information about the period it was inactive only after it is reactivated. In that case, after the reactivation, all the activity is accounted to users not authenticated in a single session. The reports cannot include printers' data while they are deactivated.
- When an embedded terminal is installed on the printing device, accounting is also done for any direct/tandem print queues of the device.
- When an embedded terminal is not installed or a device is used with a **KNM** Hardware terminal, accounting is done via SNMP by the **KNM** Print Server (depends on provided data via SNMP from the device).

### Values calculation in the Meter reading via SNMP printers report

The values in this report are based on counters read directly from the printers.

- Any printers monitored via **KNM** Desktop Client are **not** included in the reports.
- The highest and lowest values are compared for a selected period and printer/group of printers.
- The total value displayed in the report is the summary of all the subtotal values, without *Pages printed* while the device was deactivated.

## 15.3 Report values description

Description of values in the reports' default and additional columns and how they are accounted.

These values are accounted as page counts in the following way: 2 clicks for the A3/Ledger page format and 1 click for the rest (A4 etc.); in case of Duplex, it is 4 clicks for the A3 / Ledger format and 2 clicks for the rest (A4 etc.). L formats are coverage counters.

- B&W prints
- B&W copies
- Color prints
- Color copies

- Single color copy
- Total prints
- Total copies
- Fax
- Color pages (L1)
- Color cost (L1)
- Color pages (L2)
- Color cost (L2)
- Color pages (L3)
- Color cost (L3)
- Print color pages (L1)
- Copy color pages (L1)

**[-]** If discounts are used, they are not applied to all "cost" values in reports, e.g. *Color cost (L1)*, *"Color cost (L2)"* or *"Color cost (L3)"*. However, "Total cost", "Color cost" do reflect discounts.

These values are accounted as paper sheets in the following way: 1x A3 / 1x A4 etc.

- A4 paper
- A3 paper
- A5 paper
- B4 paper
- B5 paper
- Other paper
- Folio paper
- Ledger paper
- Legal paper
- Letter paper
- Statement paper
- Rest of the paper formats

These values are accounted as paper sheets as well, however, when a printing device is used without an installed Embedded terminal, this counter is specified via SNMP and depends on the counter used from the printing device.

- Simplex
- Duplex

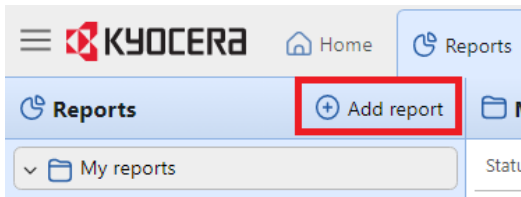
A job printed in 1x A3 monochrome sheet, on both sides in duplex mode, on a device where an Embedded terminal is installed, is accounted in **KNM** as 1x A3 paper + 4x print monochrome and 1x duplex. In the **KNM** log it will look like this:

*PM=4, A3=1, Duplex=1*

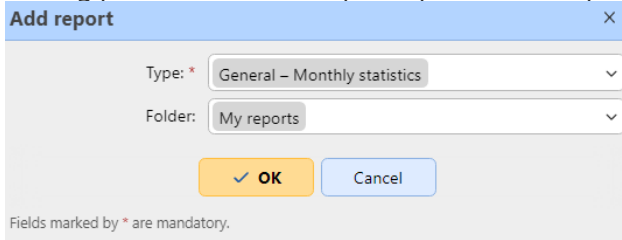
## 15.4 Creating and editing reports

You can create a new report in a few steps:

1. At the top-right corner of the **Reports** main tab, click **+Add report**. The Add report dialog box appears.

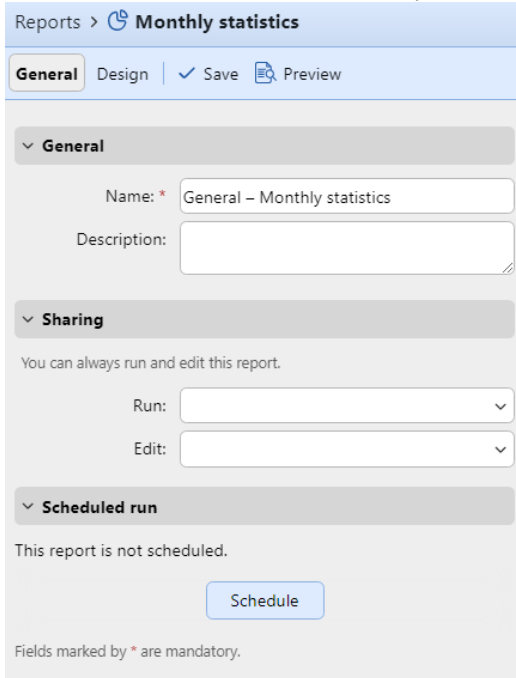


2. In the box, select the type of the new report and the folder to place it, and then click **OK**. The editing panel of the new report opens. On the panel, edit and save the report.



## 15.4.1 Editing a report

1. On the **General** tab of the report's editing tab, you can change the report's **Name**, add a **Description**, select **Sharing** rights, meaning the users or groups who will have the rights to **Run** the report and those who will have the rights to **Edit** the report. You can also click **Schedule** to set its scheduled run. Once done, click **Design** to open the Design tab of the report.



2. On the **Design** tab, you can set the report's layout, select the items (Users, Printers, etc.) to be included in the report, add or remove columns and change their order.

### Options

- **Orientation:** Select either the **Portrait**, or the **Landscape** orientation.

**Options**

Orientation:

Show filters in the final report:

- **Show filters in the final report:** Mark the checkbox if you want filters to be visible in the final report.

## Filters and parameters

Available filters and parameters differ depending on the report type. These are the main parameters available for most of the standard reports types:

**Filters and parameters**

User:

Accounting Group:

Printer:

Period: \*

▼ **Exclude data**

User:

Fields marked by \* are mandatory.

- **User:** Select the users to be included in the report. If you select the **Me** option and share this report with all users, each user can only see just the data that concern themselves; this way you can make personalized reports for each user.
- **Accounting Group:** Select the accounting groups of users to be included in the report.
- **Printer:** Select the printers to be included in the report.
- **Period:** Select the time period to be covered by the report.
- **Exclude data - User:** Select the users to be excluded from the report (only available in reports where *User* is one of the filters used).

## Table

Here you can enable and disable the table option.

Column	Width	Alignment	Summary	Aggregated
Period	Auto	Auto	None	No
B&W pages	Auto	Right	Sum	No
Color pages	Auto	Right	Sum	No
Total	Auto	Right	Sum	No
Scans	Auto	Right	Sum	No
Total price	Auto	Right	Sum	No

You can also add and remove columns to the table, edit them and change their order. For each column, you can change the width, alignment and the type of summary that will be shown on the final (bottom) row (Sum, Average or None).

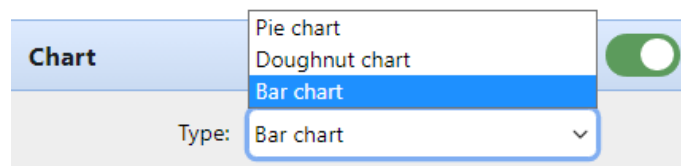
To add a new column, click **+Add**. To open the editing options of an existing column, double-click it (or select it, and then click **Edit**). To remove a column, select it and click **X**. To move a column up or down the order, select it, and then use the up/down arrows.

Period	B&W pages	Color Pages	Total	Scans	Total price
2017-3	5,621	9,189	14,810	5,506	\$5,440.000
2017-4	1,211	569	1,780	1,234	\$7,072.000
<b>Period</b>	<b>6,832</b>	<b>9,758</b>	<b>16,590</b>	<b>6,740</b>	<b>\$12,512.000</b>

Some reports do not include the option to use tables and their data can be displayed only in the chart form.

## Chart

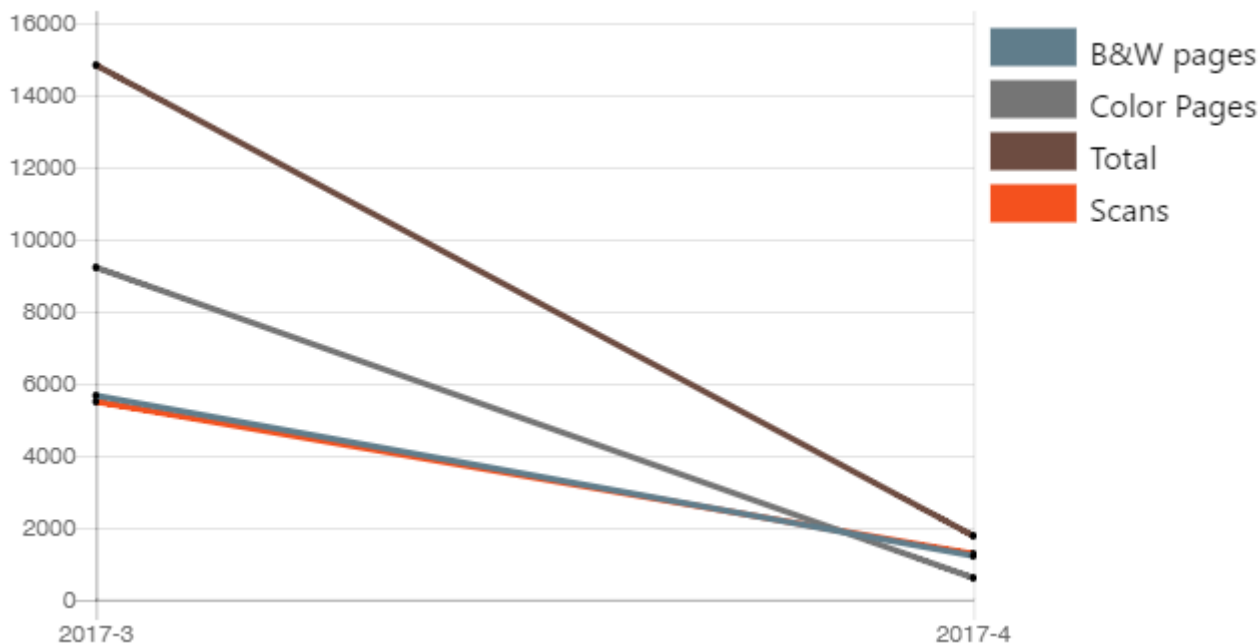
Here you can enable and disable the chart option.



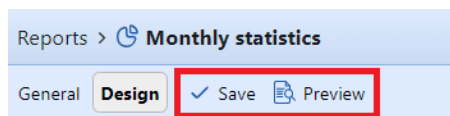
You can also select from the **Line**, **Bar**, **Pie** and **Doughnut** chart types. Furthermore, you can add and remove data types to be shown on the chart and select colors for each data type (depending on the report type).

To add a data type, click **+Add**. To open editing options of a data type, double-click it (or select it, and then click **Edit**). To remove a data type, select it and click **X**. To move a data type up or down the order, select it, and then use the up/down arrows.

Some reports do not include the option to use charts and their data can be displayed only in the table form.



Designing your own reports can be a bit tricky, since it always depends on many factors - amount of data included (columns), length of column names and values, report orientation etc. To get the best result, you can click **Preview** anytime during the report's creation to check what the new design will look like. Only after you are satisfied with the layout, click **Save** to save the report.



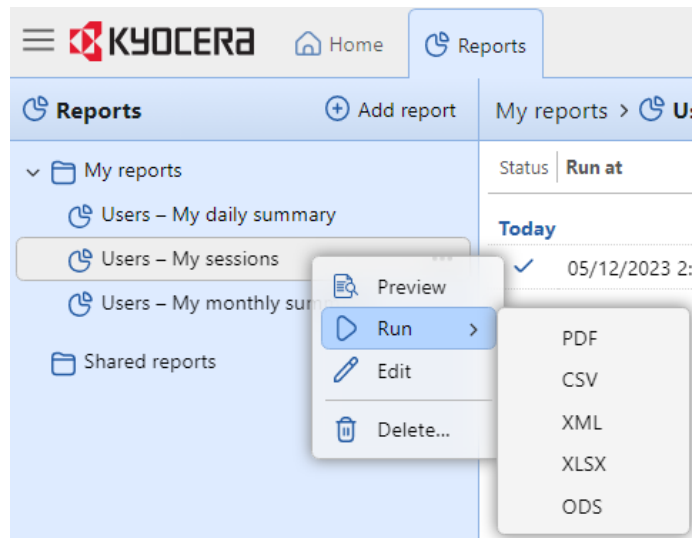
## 15.5 Generating reports

### To preview a report

Select the report and click **Preview** (or right-click it and click **Preview** on its shortcut menu). The report is shown in HTML format and the number of included data is limited. You can switch between Graphical view and Grid view.

### To run a report

Right-click the report and click **Run**. The report runs in the specified format (*PDF, CSV, XML, XLSX* or *ODS*) with no data limitation.



**To export the displayed report**

After the report is generated, click on the report's format link in the file column to download it.

My reports				
Status	Run at	Report	Files	Run by
<b>Today</b>				
✓	05/12/2023 2:48:1...	My monthly summary	XLSX	Administrator
✓	05/12/2023 2:48:1...	My sessions	XML	Administrator
✓	05/12/2023 2:48:0...	My daily summary	PDF	Administrator

## 16 Connection to BI tools

Starting from version 8.2 (patch 16), **KNM** Print Server exposes data to be analyzed with external BI tools (Business Intelligence tools).

The below information refers to the setup and use of Power BI by Microsoft, along with a **KNM** setup.

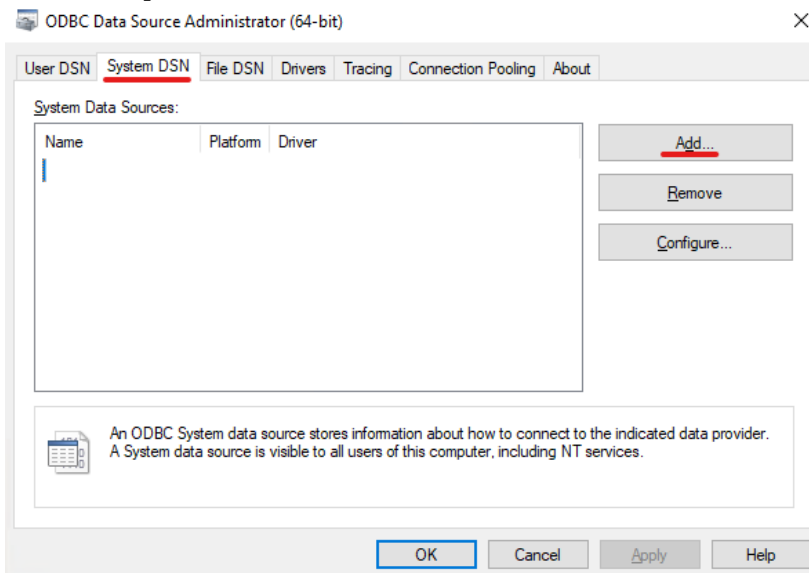
For further information about Power BI, visit:

<https://docs.microsoft.com/en-us/power-bi/fundamentals/desktop-getting-started>

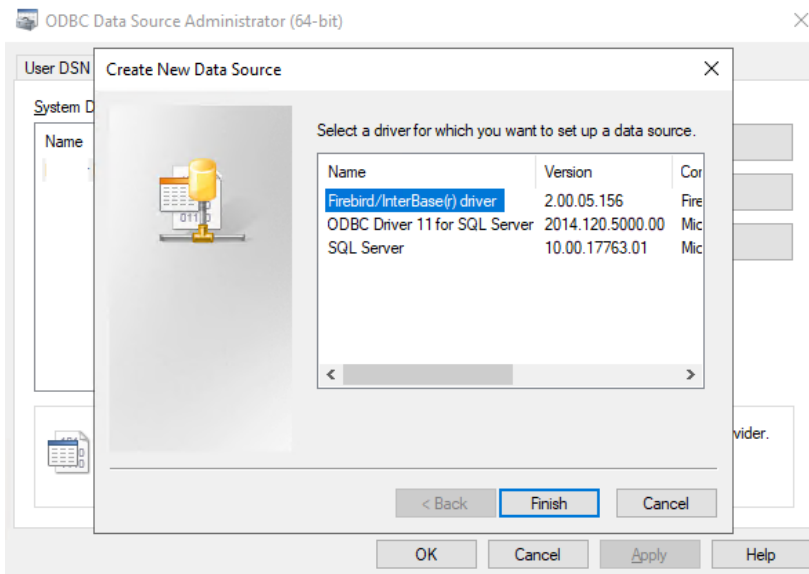
### 16.1 Embedded Database Connection Configuration

Power BI can access the **KNM** Embedded Database via ODBC. In order to create an ODBC data source:

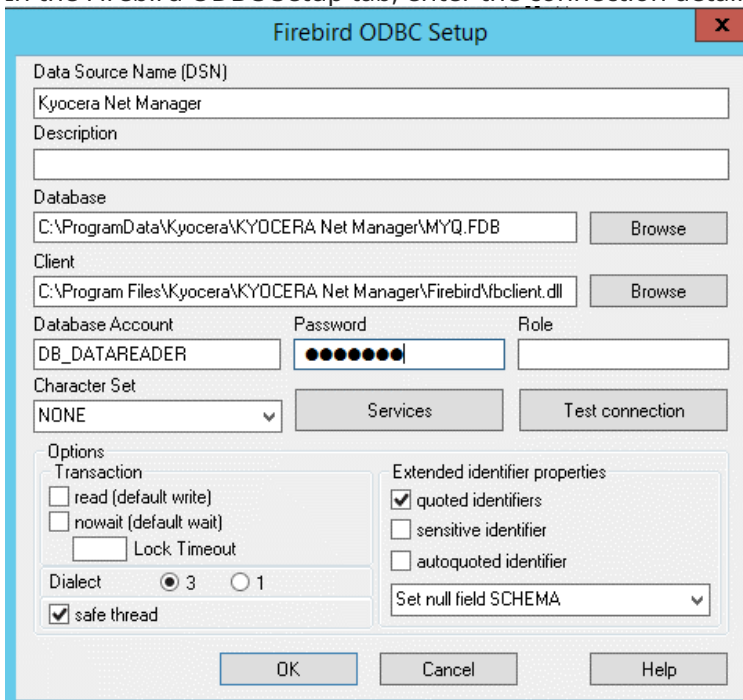
1. Download and install the latest ODBC driver for Firebird from:  
<https://firebirdsql.org/en/odbc-driver/>
2. Once installed, open the **ODBC Data Sources** application from the Windows Apps menu.
3. Go to the **System DSN** tab and click **Add**.



4. In the Create New Data Source window, select *Firebird/InterBase(r) driver* and click **Finish**.



5. In the Firebird ODBC Setup tab, enter the connection details:



- Data Source Name (DSN):** Add a name as an identifier for the connection
- Database:** Add the path to your database file (*C:\ProgramData\Kyocera\KYOCERA Net Manager\MYQ.FDB* by default)
- Client:** Add the path to the Firebird library client used for the connection. It is recommended to use the **KNM** Print Server client, found in *C:\Program Files\Kyocera\KYOCERA Net Manager\Firebird\Fbclient.dll* by default
- Database Account:** Add the Database Account user name. The default one is *SYSDBA*, but it is highly recommended not to use the default database account, but enable and use the **database read-only account** available in the [External Reports](#) settings tab.

- e. **Password:** Add the Database Account password. In case you are using the default database account (not recommended) and you haven't changed the password in **KNM Easy Config**, the default one is *masterkey*.
- f. The rest of the fields can be left unchanged. Click **Test Connection** and if successful, click **OK**.

## 16.2 Creating Reports

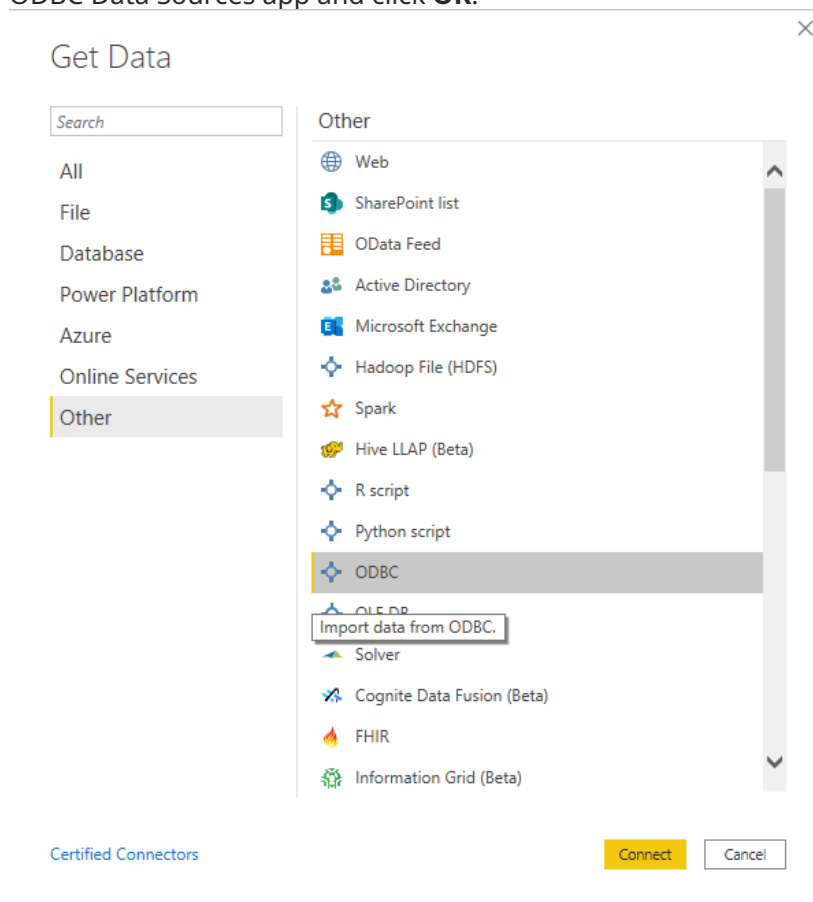
Reports can be created according to each customer's specific requirements. It is possible to create the reports manually, or create your own Power BI templates in order to generate reports quickly.

- [Manual reports creation](#)
- [Database Views description](#)

### 16.2.1 Manual Reports Creation

To manually create the reports, open Power BI and:

1. Establish the connection to your database:
  - a. Click **Get data, More....** In the new window, select **Other**, click on **ODBC** on the list, and click **Connect**. In the new prompt, select the Data source name (DSN) you created in the ODBC Data Sources app and click **OK**.



2. In the Navigator window, select all the options with the **DIM\_** and **FACT\_** prefixes and click **Load** (see [Database Views description](#)).

## Navigator

The Navigator tool displays a list of tables on the left and a data preview for the selected table, FACT\_SESSION\_COUNTERS, on the right.

**Display Options**

- ODBC (dsn=MyQ Master Embedded DB) [78]
- DIM\_ACCOUNTING\_GROUP
- DIM\_PRICELIST
- DIM\_PRINTER
- DIM\_PROJECT
- DIM\_PROJECT\_GROUP
- DIM\_SITE
- DIM\_USER
- FACT\_ALERT
- FACT\_JOB
- FACT\_SESSION\_COUNTERS**
- USERSESSION\_TOTALPAGES
- ACCESENTITY
- ACE
- ALERT
- ALIAS
- AUDITLOG
- AUDITLOGPROPERTY
- AUTHSERVER
- CARD

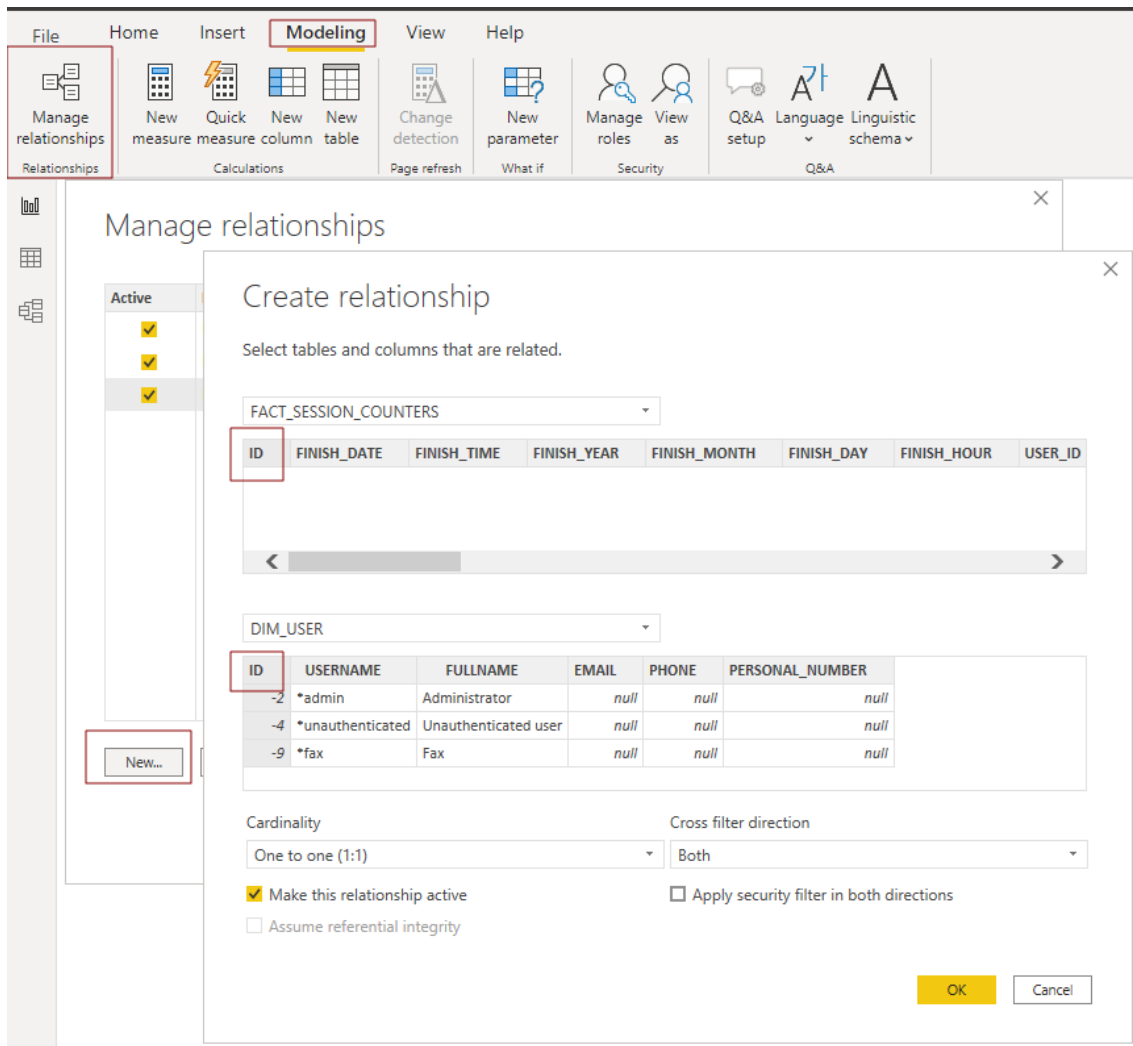
**FACT\_SESSION\_COUNTERS**

ID	FINISH_DATE	FINISH_TIME	FINISH_YEAR	FINISH_MONTH	FINISH
186353	10/20/2016	2:56:29 PM	2016	10	
186354	10/20/2016	2:56:30 PM	2016	10	
186355	10/20/2016	2:56:29 PM	2016	10	
186356	10/20/2016	2:56:30 PM	2016	10	
186357	10/20/2016	2:56:35 PM	2016	10	
186358	10/20/2016	2:56:51 PM	2016	10	
186359	10/20/2016	2:56:54 PM	2016	10	
186360	10/20/2016	2:57:00 PM	2016	10	
186361	10/20/2016	2:57:05 PM	2016	10	
186362	10/20/2016	2:57:24 PM	2016	10	
186363	10/20/2016	2:57:25 PM	2016	10	
186364	10/20/2016	2:57:26 PM	2016	10	
186365	10/20/2016	2:57:57 PM	2016	10	
186366	10/20/2016	3:00:40 PM	2016	10	
186367	10/20/2016	3:02:10 PM	2016	10	

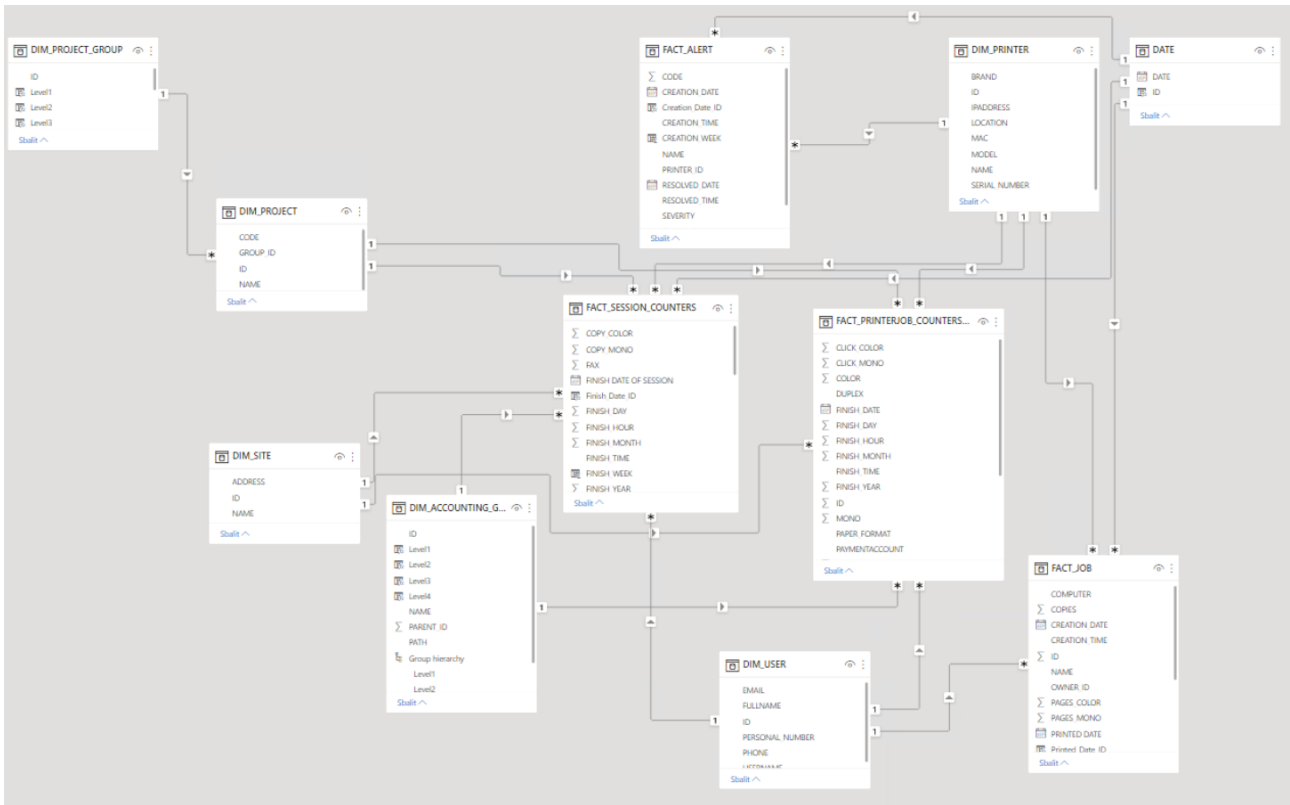
**i** The data in the preview has been truncated due to size limits.

Select Related Tables Load Transform Data Cancel

- Power BI loads the data, however the relationships between them must be created manually, since Power BI cannot extract them:
  - Go to the Modeling menu and click on **Manage relationships**.
  - Click **New...** and create the relationships between the views, selecting the IDs in each of them. Click **OK** once done.



4. Your model has been created and you can add visualizations to the report.



## 16.2.2 Database Views description

There are two groups of views; **dimensions** and **facts**. The fact views contain measures, numeric data which can be used in calculations for reports. The dimension views contain descriptive information used for the measures in the facts. Dimension views have the **dim\_** prefix and fact views have the **fact\_** prefix.

The IDs in the views are internal **KNM** IDs and can be used to establish relationships between views.

### Printer Dimension (dim\_PRINTER\_V2) - Information about the printer

Field Name	Description
ID	Printer ID
Name	Printer name
IP_Address	Printer IP address
MAC	Printer MAC address
Brand	Printer brand

Field Name	Description
Model	Printer model
Location	Printer location
Serial_Number	Printer serial number
ASSET_NUMBER	Printer asset number
CONTACT	Printer contact info
NOTES	Printer notes (memo text)
MODE	Printer mode. Values: 1 = <i>Offline</i> , 2 = <i>Online</i> , 8 = <i>Local</i>
IS_COLOR	Color printing. Values: 1 = <i>Color print available</i> , 0 = <i>Monochrome print only</i>
IS_COPIER	Copier function. Values: 1 = <i>Copier</i> , 0 = <i>Copier function is not available</i>
IS_A3	A3 paper format support. Values: 1 = <i>A3 format is supported</i> , 0 = <i>No A3 format support</i>
COPIER_COLOR_COUNTER	Total counter of color copies
COPIER_MONO_COUNTER	Total counter of monochrome copies
PRINTER_COLOR_COUNTER	Total counter of printed color pages
PRINTER_MONO_COUNTER	Total counter of printed monochrome pages
SCANNER_COUNTER	Total counter of scanned pages
FAX_COUNTER	Total counter of fax pages

**User Dimension (dim\_User)** - Information about the user

Field Name	Description
ID	User ID

Field Name	Description
USERNAME	KNM username
FULLNAME	User's name and surname
EMAIL	User's email
PHONE	User's phone number
PERSONAL_NUMBER	KNM user's personal number
CREDIT	Credit amount ( <i>null</i> - if credit is disabled for user)
LANGUAGE	User language
NOTES	Notes (memo text) to users account

**Printer Events Fact (fact\_PRINTER\_EVENTS)** - Information about printer events.

Field name	Description
Name	Name of the event
Type	Type of the event ( <i>alert</i> or <i>tonerLevel</i> or <i>totalCounter</i> or <i>tonerReplacement</i> )
Created	Date and time in which the event was created
Closed	Date and time in which the event was closed
Data	Data of the event (JSON example: <code>{"TONER_K.LEVEL":"8","EVENT.TONER.INFO":"TK-8305Y","TONER_C.LEVEL":"6","TONER_K.INFO":"TK-8305K","TONER_C.INFO":"TK-8305C","TONER_M.INFO":"TK-8305M","TONER_M.LEVEL":"0","TONER_Y.INFO":"TK-8305Y","TONER_Y.LEVEL":"6","SUPPLY.INFO":"TK-8305C;TK-8305M;TK-8305Y;TK-8305K","EVENT.TONER.LEVEL":"6"}</code> )
Printer_Id	ID of the printer where the event was raised

**Toner replacements (fact\_TONER\_REPLACEMENTS)** - It provides certain data about printer toners that have been replaced and currently installed. This view combines the results of **V\_TONERS\_REPLACED** and **V\_TONERS\_INSTALLED** into one view.

#### **V\_TONERS\_REPLACED**

Field name	Description
Name	Name of the toner
Type	Type of the toner ( <i>cyan or magenta or yellow or black</i> )
Installed	Date and time in which the toner was installed
Replaced	Date and time in which the toner was replaced
Counters	Total number of pages printed with the toner type of the toner until the toner was replaced
Period	Number of days from the toner installation to the toner replacement
Pages	Number of pages printed by the toner
Printer_Id	ID of the printer where the toner was installed

#### **V\_TONERS\_INSTALLED**

Field name	Description
Name	Name of the toner
Type	Type of the toner ( <i>cyan or magenta or yellow or black</i> )
Installed	Date and time in which the toner was installed
Replaced	NULL
Counters	Total number of pages printed with the toner type since the toner type installation
Period	Number of days since the toner installation
Pages	Number of pages printed by the toner
Printer_Id	ID of the printer where the toner was installed

**Printer jobs counter fact (fact\_PRINTERJOB\_COUNTERS\_V3)** - Information about printer jobs counters

Field name	Description
PRINTERJOB_ID	Printer job Id
USER_ID	User Id
USER_GROUP_ID	Group of users
PRINTER_ID	Printer Id
PROJECT_ID	Project Id (-56 for jobs without project)
SITE_ID	Site id
TYPE	Job type. Values: <i>print</i> , <i>copy</i> , <i>scan</i> , <i>faxRx</i> (Incoming fax -print), <i>faxTx</i> (Outgoing fax - scan)
PAYMENTACCOUNT	Payment Account. Values <i>Credit</i> , <i>Quota</i> , <i>Cost Center</i>
FINISH_DATE	Date when job was finished
FINISH_TIME	Time when job was finished
FINISH_YEAR	Year when job was finished
FINISH_MONTH	Month when job was finished
FINISH_DAY	Day of a month when job was finished
FINISH_HOUR	Hour when job was finished
PAPER_FORMAT	Paper format
DUPLEX	Duplex print. Values: <i>Yes</i> , <i>No</i>
SHEETS	Used sheets of paper
MONO	Monochrome print job
COLOR	Color print job
SINGLE	Single color print job

Field name	Description
PRICE	Job price
CLICK_MONO	Click mono
CLICK_COLOR	Click color
SESSION_ID	User session id
JOB_ID	Job id (Reference to user's job)

**Job Fact (fact\_job)** - Information about print jobs

Field Name	Description
ID	Job ID
SESSION_ID	Session ID
NAME	Job name
OWNER_ID	Job owner ID
PRINTER_ID	Printer ID where the job was printed. Null if not printed
COMPUTER	Computer name or address where the job was sent from
SIZE_IN_BYTES	Job size in bytes
PAGES_MONO	Number of pages in black and white
PAGES_COLOR	Number of pages in color
DUPLEX	Duplex print. Values: <i>1 = Duplex , 0 = Simplex</i>
COPIES	Number of copies
STATE	Job state. Values: <i>Ready, Printed, Expired or deleted</i>
PRINTED_DATE	Date when the job was printed

Field Name	Description
PRINTED_TIME	Time when the job was printed
CREATION_DATE	Date when the job was created
CREATION_TIME	Time when the job was created

**Session Fact (FACT\_SESSION\_COUNTERS) - Information about sessions**

Field Name	Description
ID	User session ID
FINISH_DATE	Date when session was finished
FINISH_TIME	Time when session was finished
FINISH_YEAR	Year when session was finished
FINISH_MONTH	Month when session was finished
FINISH_DAY	Day when session was finished
FINISH_HOUR	Hour when session was finished
USER_ID	User ID
PRINTER_ID	Printer id
PROJECT_ID	Project id
USER_GROUP_ID	User group id
TOTAL_PRICE_USER	Total price for the user
TOTAL_PRICE_ADMIN	Total price for the admin
TOTAL_PAGES	Total number of pages
PRINT_MONO	Printed pages in black and white

Field Name	Description
PRINT_COLOR	Printed pages in color
COPY_MONO	Copied pages in black and white
COPY_COLOR	Copied pages in color
COPY_SINGLECOLOR	Copied pages in single color
FAX	Faxed pages
SCAN	Scanned pages
PAPERA4	Pages in A4 paper format
PAPERA3	Pages in A3 paper format
PAPER_A5	Pages in A5 paper format
PAPER_B4	Pages in B4 paper format
PAPER_B5	Pages in B5 paper format
PAPER_FOLIO	Pages in folio paper format
PAPER_LEDGER	Pages in ledger paper format
PAPER_STATEMENT	Pages in statement paper format
PAPEROTHER	Pages in other paper format


**Session Environmental Impact Fact (fact\_Session\_Counters)** - Information about sessions' environmental impact

Field Name	Description
ID	User session ID
CREATION_DATE	Date of the session creation
FINISHDATE	Date when session was finished

Field Name	Description
TOTAL_A4	Converted to A4 paper size units total pages amount
USER_ID	User ID
GROUP_ID	User group id
PRINTER_ID	Printer id
TOTAL_TREES	Approximate amount of trees used per session
TOTAL_CO2_GRAMS	Approximate amount of CO2 was produced per session (in gram units)
TOTAL_ENERGY_WH	Approximate amount of Energy consumed per session (in watt-hour units)
TOTAL_ENERGY_WH_RECYCLE D	Estimated approximate amount of Energy will be consumed to recycle used amount of paper per session (in watt-hour units)

**Printer Job Environmental Impact Fact (FACT\_PRINTERJOB\_ENV\_IMPACT)** -Information about printer job's environmental impact

Field Name	Description
ID	Printer Job counter Id
PRINTERJOB_ID	Printer Job Id
TOTAL_TREES	Approximate amount of trees used per session
TOTAL_CO2_GRAMS	Approximate amount of CO2 was produced per session (in gram units)
TOTAL_ENERGY_WH	Approximate amount of Energy consumed per session (in watt-hour units)
TOTAL_ENERGY_WH_RECYCLE D	Estimated approximate amount of Energy will be consumed to recycle used amount of paper per session (in watt-hour units)

 There is a limitation that even if you are using a Job Privacy license, the data in the database are not changed by this feature and are still readable.

## 17 Scanning and OCR

---

The **KNM** system is able to automatically send scanned documents to the scanning user with the **Scan to Me** feature.

**KNM** also allows you to use Optical Character Recognition (**OCR**) by either integrating the **KNM** OCR server or using a custom 3rd-party application.

The first section of this topic shows you how to set up the **Scan to Me** feature on the **KNM** server, how to use it, and how to limit the size of emails with scans.

The second section shows you how to set up your **OCR** server.

### 17.1 Scan to Me

With the **Scan to Me** feature enabled, **KNM** serves as an email server — it receives a scanned job from printing devices via the SMTP protocol, detects the device where the job is sent from, finds the user that is currently logged on the device and sends the job to their folder or email (depends on the user's settings).

**Scan to Me** is also one of the essential features of the **KNM** Embedded terminals. Apart from it, the embedded terminals offer a large number of advanced destinations such as **Cloud** and **FTP servers**.

First, you need to set up the feature on the **KNM** server and on the printing device to enable the **KNM** users to use all of the scanning options. After that, you need to provide the users with an email addresses, where they can direct the scanned documents to.



The correct time and date must be set on the printing device to avoid issues with correct functionality.

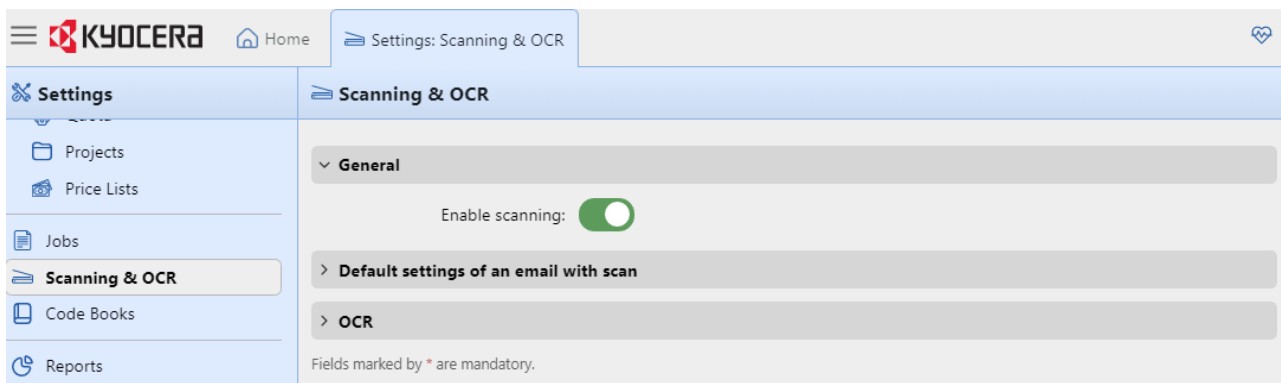
#### 17.1.1 Setting up the feature

To set up **Scan to Me**:

- Enable and setup scanning on the **KNM** server
- Set SMTP on the printing device
- Set the destinations for the **KNM** users on the **KNM** server

#### Enable and setup scanning on the **KNM** server

Go to the **Scanning & OCR** settings tab, under **General** and **Enable scanning**.



You can also change the subject and message of the email with the scanned document there. As the sender of the document, you can select either the email of the logged user or the default sender email set on the **Network** settings tab, under **Outgoing SMTP server**.

## Set SMTP on the printing device

The scanning function requires enabling the SMTP protocol, setting the SMTP server address and entering a sender email on the printing device web interface. For information about how to enter the printing device web interface and find the particular settings, see the printing device manual.

To enable the scanning function, take the following steps on the printing device web interface:

- Enable SMTP protocol.
- Enter the **KNM** server IP address or hostname.
- Ensure that the SMTP port is the same as the SMTP port in the **Network** settings tab, under **KYOCERA Net Manager SMTP server**. The default port in **KNM** is 25.
- Enter sender email address. The address value is arbitrary.

### 17.1.2 Set the destinations for the KNM users on the KNM server

On the properties panel of each individual **KNM** user (see [Editing user accounts](#)), you can set the destinations using three options: **Sending scans to the user's primary email**, **Sending scans to other predefined emails**, **Storing scans to the user's scan folder**.

To provide a user with these options, set the appropriate fields on their properties panel, according to the following table.

Option	Parameter	Value
Sending scans to the user's primary email	Email	User's primary email address
Sending scans to other predefined emails	User's storage	Any number of email addresses separated by commas (,)
Storing scans to the user's scan folder	User's storage	Folder where the document should be stored

### 17.1.3 Using the Scan to Me feature

To send the email to the desired destination, the scan needs to be directed to a specific receiver email address. There are two options to enable the **KNM** users to send the scans there: provide them with the respective receiver email address, or predefine these email addresses on the printing device's Web User Interface.

#### Email addresses for Scan to Me

- **Sending scans to the user's primary email** - The scanned document is sent to the user email set in the email text box on the user properties panel.  
The receiver email address has to be *email@KNM.local*.
- **Sending scans to other emails** - The scanned document is sent to all emails set in the **User's storage** text box (multiple emails should be separated by commas) on the user properties panel.  
The receiver email address has to be *folder@KNM.local*.
- **Storing scans to the user's scan folder** - You have to create a shared folder and ensure that **KNM** has access to this folder. After this, enter the folder's location to the **User's storage** text box. The scanned document is sent to **KNM**, and then stored in the shared folder via the SMB protocol. The stored document file name consists of the user account name, and the date and the time when the scan was sent.  
The receiver email address has to be *folder@KNM.local*.

To enable **KNM** to save the scan file in the user scan folder, you have to make sure that the folder is shared over your network and that the computer where you run **KNM** has all the necessary access rights to this folder.

#### Predefined list of the KNM destinations on the printing device

On the **Address List** on the printing device's web interface, you can predefine email addresses where the scanned documents are sent to.

### 17.1.4 Scan email size limits

Due to email size restrictions in some email servers, users might not be able to send scans exceeding a certain size to their emails. To prevent such situations, you can set the maximum size of emails with scans on the **KNM** Web Interface. Emails exceeding the limit are then replaced by emails with a secure link to the scan file, which is saved on the **KNM** print server.

▼ **Default settings of an email with scan**

Maximum email size: \*  MB  
 If the email exceeds the maximum size, a secure link to the document will be sent.

Sender: \*  ▼

Subject: \*   
 Parameters: %username%, %timestamp%, %originalSubject%, %originalBody%, %admin%

Message: **Scan in attachment** Scan as a secured link

Hello,

See the attachment for your scanned document.

Your KYOCERA Net Manager

Please contact the administrator at %admin% in case of further requests

[↶ Revert values](#)

- **Maximum email size** - Set the maximum size limit (in MB) of the email with the scan. The default value is *2047MB*.
- If the scan is bigger than the above limit, it will be sent as an email with a secure link to the scan.

You can edit the email **Sender**, **Subject**, and **Message** as well.

You can use multiple parameters, such as *%username%* *%timestamp%*, *%admin%*, etc.

The *%links%* parameter represents the actual link to the stored scan file.

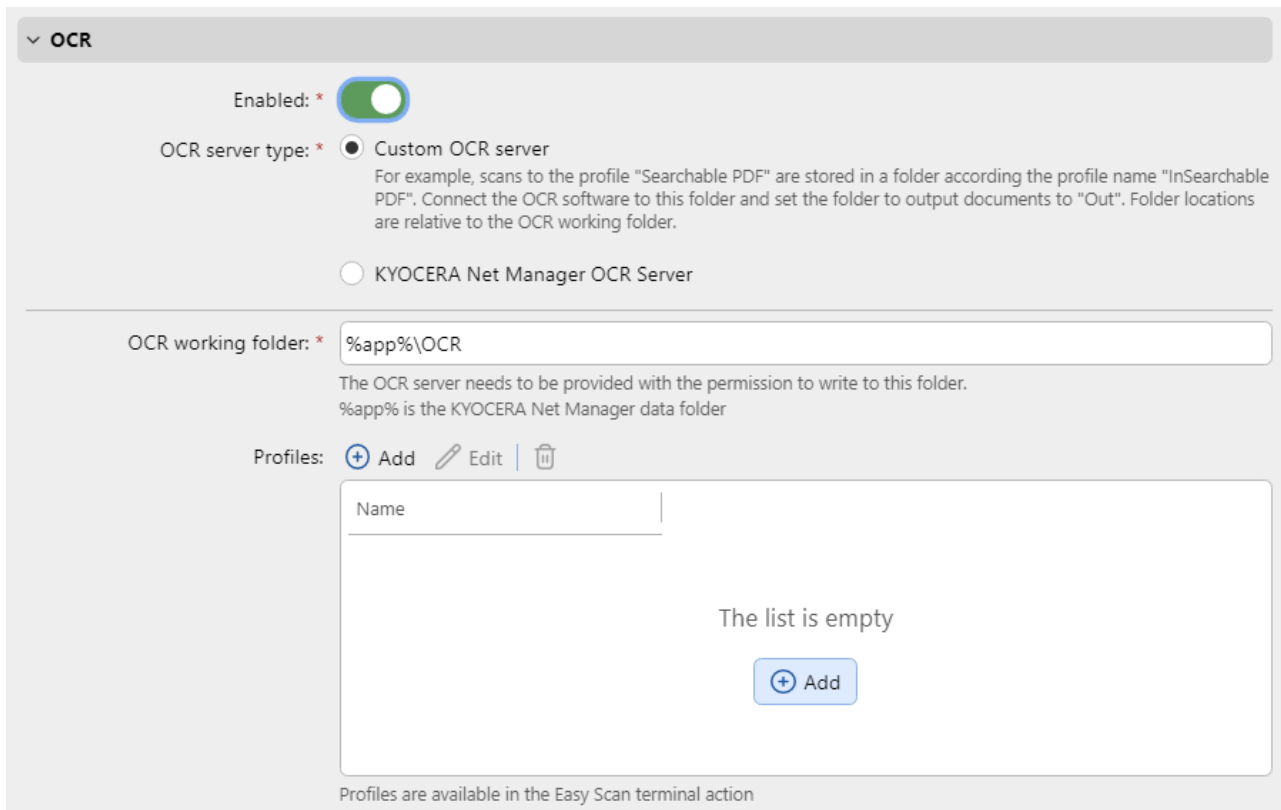
## 17.2 OCR

Optical Character Recognition (**OCR**) is a service that converts scanned documents to a searchable and editable format, such as a text document or a searchable PDF. To provide this functionality, you can either use the **KYOCERA Net Manager** OCR server, which is a part of the **KNM** solution, or you can employ a third-party application.

 **KNM** Print Server 10+ requires **KNM** OCR Server 3.0+.

### 17.2.1 Activation and setup

The OCR feature has to be enabled on the **Scanning & OCR** settings tab, under **OCR**.



Choose the **OCR server type**:

- *Custom OCR server* - select this option if you have your own Document Management System (DMS) for document processing or any other OCR-capable application.
- *KYOCERA Net Manager OCR Server* - select this option if you already have the **KNM** OCR Server set up and running.

You can change the folder where the scanned data is sent in the **OCR working folder** field. It is however, not recommended to change the default folder (*C:\ProgramData\Kyocera\KYOCERA Net Manager\OCR*).

The OCR folder contains two sub-folders: **in** and **out**. In the **in** folder, the scanned documents are stored before being processed. In the **out** folder, the processed documents are saved by the OCR software and are ready to be sent.

In the **Profiles** section, you can set up OCR profiles to be used in the Easy Scan terminal action.

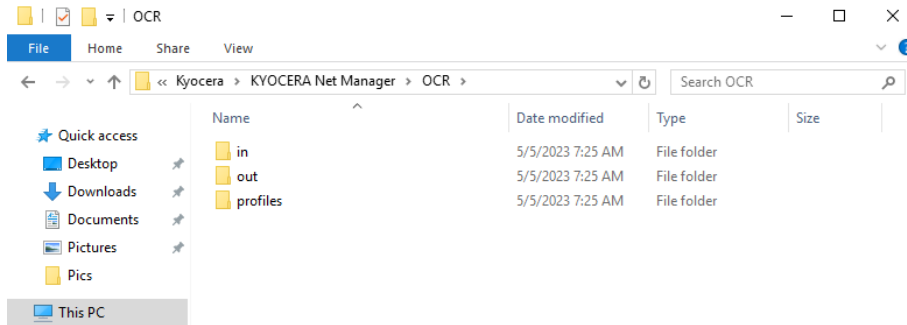
Click **Add**, set a **Name** for your new profile and select the **Output**, either *pdf*, *pdfa* or *text*, and click **Save**. You can now set this OCR profile as the **Default value** in the **Format** parameter of your Easy Scan terminal action.

A document sent to be processed by OCR is received with a certain delay, depending on the OCR software speed, and on the size of the document.

Running the OCR software on the same production server as **KNM** may affect your system's performance.

## 17.2.2 OCR processing

To send a scanned document to OCR, the entered receiver email address has to be in the form: **KNMocr.\*folder\*@KNM.local**, where *folder* is the folder where the document is saved before it is proceeded by the OCR software, for example *TXT* or *PDF*. If the folder is not there, **KNM** will create it.



The OCR software should listen to the document sub-folders of the **in** folder (*in\pdf, in\txt,...*), process the file that was sent there, save the converted document to the **out** folder and delete the source file from the *in\*folder\** folder.

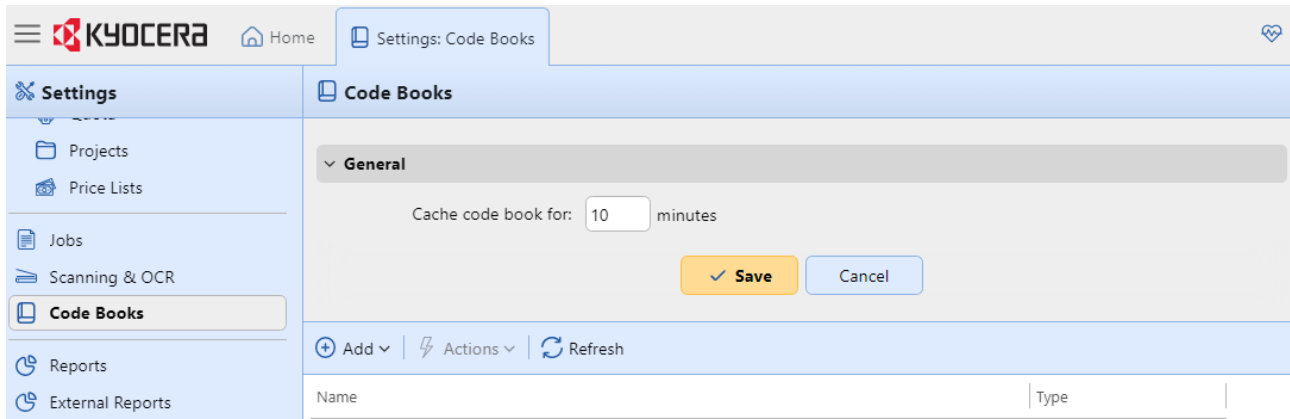
**KNM** listens to the **out** folder, sends the converted file to the user and deletes it from the folder.

The converted file is sent to the folder or email address listed in the **User's storage** text box, in the user properties panel.

The file sent to the **out** folder by the OCR software has to have the same name as the source file in the **in\*\*\*** folder. If the name of the converted file differs from the source file, it is deleted without being sent to the user.

## 18 Code Books

On the **Code Books** settings tab (KYOCERA, **Settings**, **Code Books**), you can add code books and code lists with defined values for each of them. These code books and lists can be used with your scan profiles in multiple ways, such as allowing users to use scan recipients from an LDAP source, set up output folders from an internal code list, search users from an MS Exchange address book, etc.

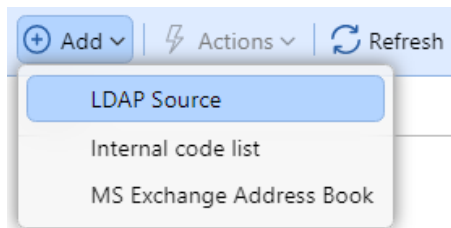


In the **General** section you can find the **Cache code book for: \_\_ minutes** setting. The value set here determines how long the code book will be cached in **KNM**, to be available in case of a lost connection between the **KNM** server and the LDAP server. The default value is *10* minutes.

Below that, you can add and modify your Code Books.

Three types of Code Books can be added:

- LDAP Source
- Internal code list
- MS Exchange Address Book



To add a new Code Book, click **+Add** and select the type you want to add from the drop-down.

To delete a Code Book, select it, click **Actions**, and select **Delete**, or right-click on the Code Book and select **Delete**.

To edit a Code Book, select it, click **Actions**, and select **Edit**, or right-click on the Code Book and select **Edit**, or double-click on the Code Book.

### 18.1 LDAP Source Code Books

On the **Code Books** settings tab (KYOCERA, **Settings**, **Code Books**), you can enable selecting scan recipients directly from an LDAP server by importing the codes from that server.

In the Code Books section, click **+Add** and select *LDAP Source* from the drop-down. The new code book's properties panel opens on the right side of the screen.

The screenshot shows a 'Folders' dialog box with the following fields and values:

- Title:** \* Folders
- Server:** \* LocalAD@domain.com
- User:** \* admin
- Password:** \* ....
- Base DN:** \* OU=import\_test
- Filter:** objectClass=user  
department=Managers
- Properties:**
  - Title:** \* cn
  - Value:** \* folder

Buttons: Save (highlighted in orange), Cancel.

Footnote: Fields marked by \* are mandatory.

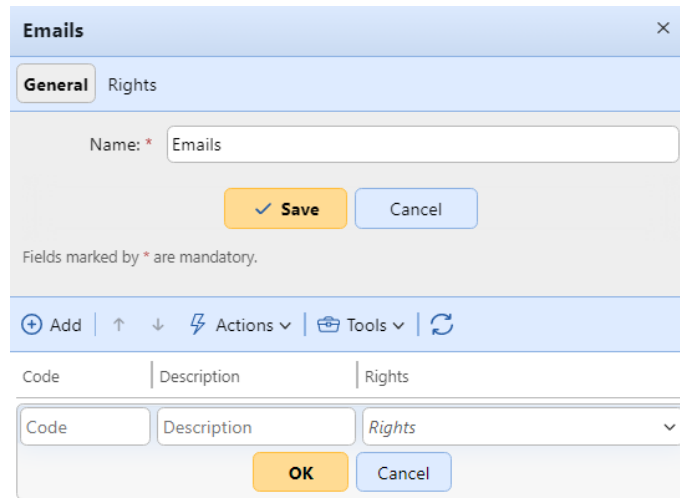
On the properties panel, fill in the required information, and click **Save**:

- **Title** - The code book's name.
- **Server** - The LDAP server that you want to import the attributes from.
- **User** - The user name for accessing the LDAP domain server.
- **Password** - The password for accessing the LDAP domain server.
- **Base DN** - The base domain(s) that you import the attributes from. Click **+Add** to add a text box for an additional base DN, and then enter the domain. You can add multiple domains this way.
- **Filter** - You can filter the users import by specifying the attributes' values. **Attribute=Value**. Users with different values in 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.
- **Properties: Title, Value** - Define the titles and values of the code for each user by entering their attributes from the LDAP database. For example, you can enter the *cn* attribute as the **Title** and the *folder* attribute as the **Value**. This way, each code will contain the user's folder and its title will be the user's full name.

## 18.2 Internal Code List

On the **Code Books** settings tab (**KYOCERA, Settings, Code Books**), you can predefine code lists with values and use the values as options available for users.

In the Code Books section, click **+Add** and select *Internal code list* from the drop-down. The new code book's properties panel opens on the right side of the screen.



On the properties panel, on the **General** tab, enter a **Name** for your new internal code list, and click **Save**. The new code list is added to the list on the **Code Books** settings tab.

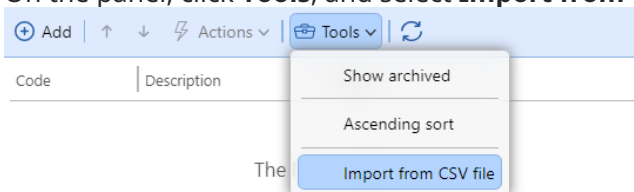
On the **Rights** tab, you can provide users or groups of users with the right to use the code list. Click **Add User** and select the user or group from the drop-down. Check the boxes for the rights you want to assign to them.

### Add new codes to an existing code list

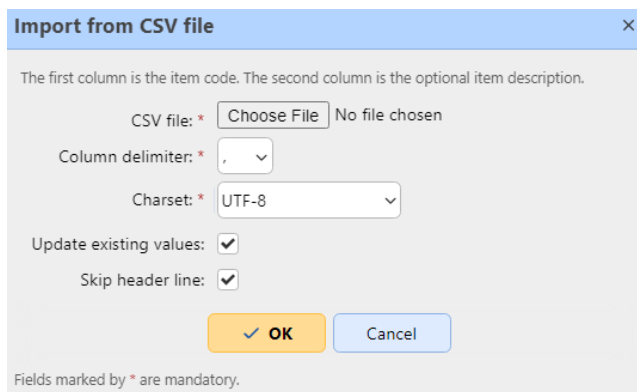
1. Double-click on the code list (or right-click the code list and click **Edit**). The code list's properties panel opens on the right side of the screen.
2. On the panel, click **+Add**.
3. Enter the **Code** name and its **Description** (the description will be shown on the terminal). You can also assign access **Rights** to this code to users or groups. Finally, click **OK**.

### Import codes from a CSV file

1. Double-click on the code list (or right-click the code list and click **Edit**). The code list's properties panel opens on the right side of the screen.
2. On the panel, click **Tools**, and select **Import from CSV file**.



3. In the Import from CSV file panel, browse and select the CSV file that you want to import, select the **Column delimiter** used in the file, select the character set (**Charset**) used in the file, choose if you want to **Update existing values** and/or **Skip header line**, and click **OK**.



Each line of the CSV file has to consist of either one, two or three columns. The first column contains the code, while the optional second and third columns contain the code's description and the users or groups with access to this code. For example:

```
Code1,This is Code 1,All users
Code2,This is Code 2,"eliot.kate"
Code3, This is Code 3
Code4
```

## 18.3 MS Exchange Address Book

You can use an MS Exchange Address Book to retrieve personal contacts from the user's mailbox from the MS Exchange Server. You can set parameters for Email, Fax and Phone.

The following versions are supported:

- MS Exchange Server 2013 SP1 (from build 15.0.847.32)
- MS Exchange Server 2016
- MS Exchange Server 2019

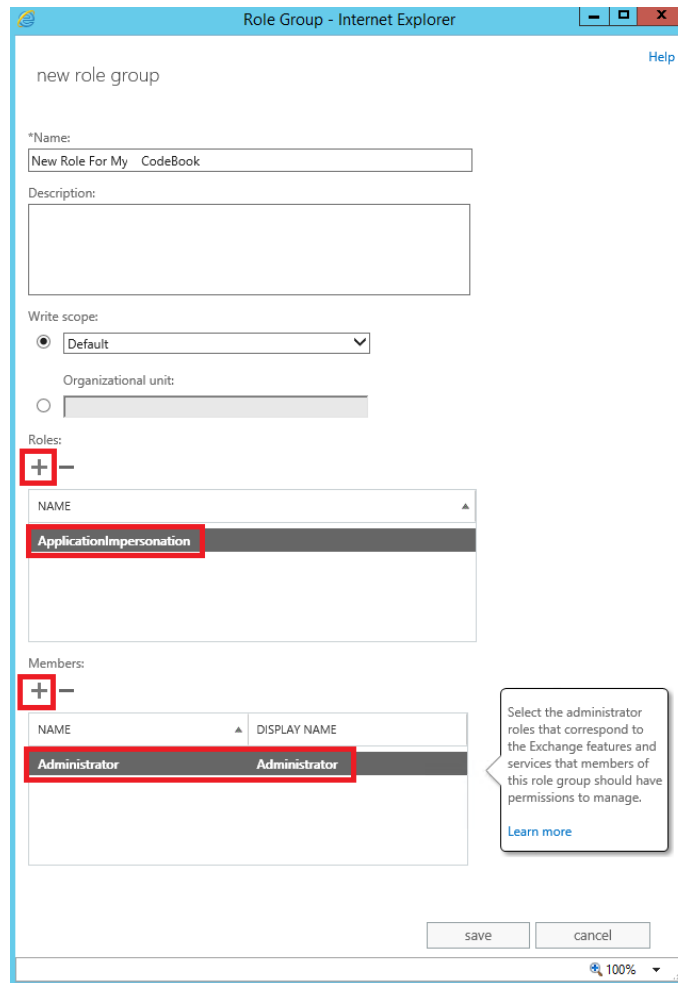
### 18.3.1 MS Exchange Server Configuration

All settings on IIS (Internet Information Services) have to be set up correctly to allow third-party applications (**KNM**) to communicate with the EWS service.

On your MS Exchange Server, the only necessary setting is configuring an account with the '**ApplicationImpersonation**' right, in order to be able to access other users' mailboxes.

To do that:

- Log in to your [Exchange Admin Center](#).
- Go to the **permissions** tab, and Create (+) a new **Admin Role**.
- In this new role, add the **ApplicationImpersonation** right.
- In this new role, add user/admin account that you want to use in **KNM** for accessing personal contacts of other users' mailboxes.



### 18.3.2 Adding a new MS Exchange Code Book in KNM

On the **Code Books** settings tab (**KYOCERA, Settings, Code Books**), in the Code Books section, click **+Add** and select *MS Exchange Address Book* from the drop-down. The new code book's properties panel opens on the right side of the screen.

On the properties panel, fill in the required information:


- **Name** - Add a name for the code book.
- **Server** - The host name or the IP address of the MS Exchange Server.
- **User** - The name of the user who has the required rights (*applicationImpersonation* to access other users' mailboxes) on the MS Exchange Server.
- **Password** - The above user's password.
- **Security** - Select *None* or *SSL*.

Click **Test** to check the connection to the MS Exchange Server, and click **Save** to make the new MS Exchange code book available.

### 18.3.3 Using MS Exchange Code Books on a KNM scan profile

Go to **KYOCERA, Settings, Terminal Actions** and create a new parameter for a scan profile of your choice. To do that, double-click the scan profile. In the properties panel that opens on the right side of the screen, go to the **Parameters** tab. Click **+Add** and fill in the required information to setup the new parameter.

- **Title** - Add a title for this new parameter.
- **Type** - Select *Code Book* from the drop-down.
- **Code Book** - Select your MS Exchange Address Book from the drop-down.
- **Default value** - Select the type of contact to be displayed for the user:
  - *Email* - Will display emails from retrieved contacts.
  - *Phone* - Will display phone numbers from retrieved contacts.
  - *Fax* - Will display fax numbers from retrieved contacts.
- **Required** - Mark the checkbox if you want to make this parameter mandatory.

 After opening the MS Exchange code book on a terminal, only the first 50 items are shown. Users can search for any non-listed items by using the name of the hidden contact. Email, Fax and Phone are separately shown.

## 19 Credit

With the credit accounting feature activated, users can copy, print and scan only if they have enough credit on their account in **KNM**. Printing is allowed only for print jobs that do not exceed the credit and copying is terminated immediately after the credit is exceeded. The credit system can be restricted to selected users and groups.

Users can view the current amount of credit on their accounts on the **KNM** Web Interface. If a printing device is equipped with an embedded terminal or a reader with an LCD display, the logged users check the current state of their credit there and are allowed to select only those jobs that do not exceed their credit.

Based on the setup and properties of the printing environment, a variety of recharge methods may be employed. The **KNM** administrator can manage the credit on the **KNM** Web Interface, and also provide the users with the option to recharge the credit themselves on embedded terminals, on recharging terminals, via recharging vouchers, or via a third-party payment method.

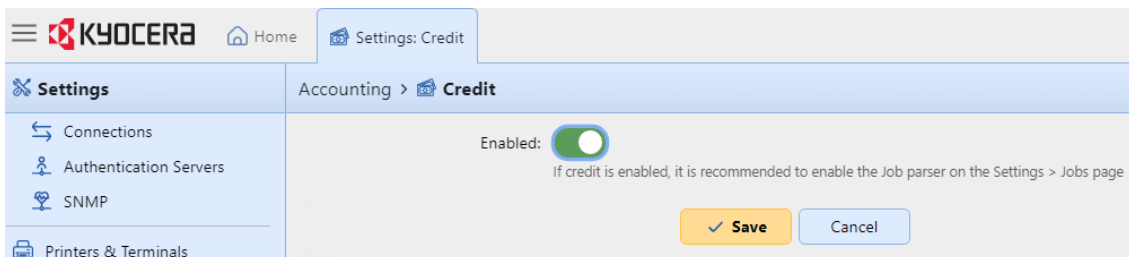
The **KNM** Administrator (and authorized **KNM** users) can also reset the credit to a specific amount on the **KNM** Web Interface.

### 19.1 Activation and setup

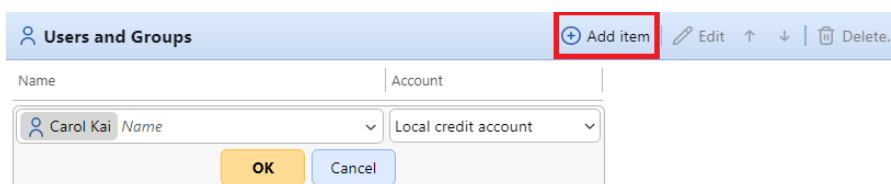
The activation and setup of credit accounting is managed on the **Credit** settings tab (**KYOCERA, Settings, Credit**).

To set up credit accounting:

**Enable** credit accounting on the **Credit** settings tab:



**Activate credit for a user or for a group of users:**



- Under **Users and Groups**, click **+Add item**. A new item appears on the list of users and groups on the **Credit** settings tab.
  - Select a **Name** from the drop-down list.
  - Select an **Account** from the drop-down list. The available options are:
    - Managed by the printer
    - External credit account
    - Local credit account
- Click **OK** to save the settings.

## Enable/disable payment methods for credit recharge

Available payment methods:

- Recharge Credit (on a terminal attached to a printer)
- Voucher
- PayPal
- External Payment Providers
- WebPay
- CASHNet
- SnapScan

To enable any of these options (if disabled), select it in the **Payment providers** section, and then click **Enabled** on the bar at the top of the section (or right-click the item, and then click **Enabled** on the shortcut menu).

Enabled	Name	Type
<b>Account</b>		
	Managed by the printer	Account
	External credit account	Account
	Local credit account	Account
<b>Credit recharge</b>		
<input type="radio"/> Disabled	CASHNet	Credit recharge
<input type="radio"/> Disabled	External Payment Providers	Credit recharge
<input checked="" type="radio"/> Enabled	PayPal	Credit recharge
<input type="radio"/> Disabled	Recharge Credit (on a terminal attached...	Credit recharge
<input type="radio"/> Disabled	SnapScan	Credit recharge
<input type="radio"/> Disabled	Voucher	Credit recharge
<input type="radio"/> Disabled	WebPay	Credit recharge

Make sure to refresh your browser (reload the page or press the F5 button) after enabling or disabling Credit to display/hide credit-related functions.

## 19.2 Manual credit recharge

The administrator (and users authorized to recharge credit) can manually recharge the credit of each user to a specific value. This can be done either on the **Credit Statement** main tab, or on the **Users** main tab in the **KNM** Web administrator interface.

On the **Credit Statement** tab, you first open the credit recharge action, and subsequently select the users and groups to recharge credit.

On the **Users** tab, first select the users or group, and then recharge their credit.

Users' credit can be reduced by entering a negative number in the recharge credit dialog box. By entering **-100**, the credit is decreased by 100.

## 19.2.1 Providing users with rights to recharge credit

By default, the only person who can recharge credit is the administrator. However, the administrator can authorize a **KNM** user to recharge credit as well. The user needs to be provided with the rights to access the credit settings and to recharge credit. This is done on the **Rights** settings tab of the **KNM** Web Interface.

To authorize a user to recharge credit on the **Credit Statement** tab, you need to provide them with the right to **Recharge credit**.

To authorize a user to recharge credit on the **Users** tab, you need to provide them with the right to **Recharge credit** and the right to **Manage Users**.

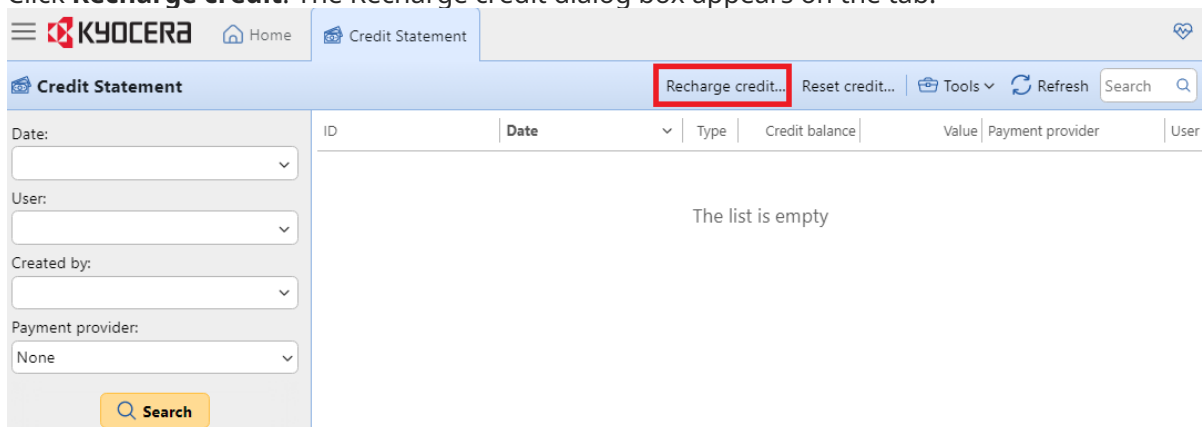
The authorized user can then recharge credit on their **KNM** Web interface in the same way as the **KNM** administrator.

## 19.2.2 Recharging credit on the Credit Statement tab

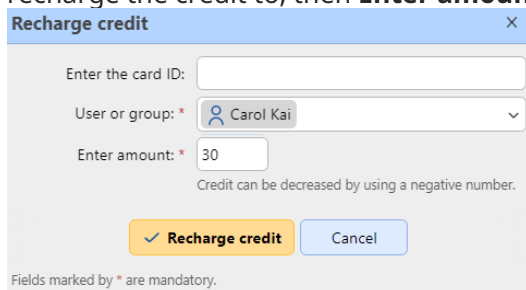
On the **Credit Statement** tab, you can overview the changes in the credit balance of **KNM** users, and also recharge credit to users and groups. To open the tab on the **KNM** Web administrator interface, go to **KYOCERA, Credit Statement**.

To recharge credit to users or groups:

1. Click **Recharge credit**. The Recharge credit dialog box appears on the tab.



2. In the dialog box, either **Enter the card ID** of a user card, or select the **User or group** to recharge the credit to, then **Enter amount** to be recharged, and lastly, click **Recharge credit**.

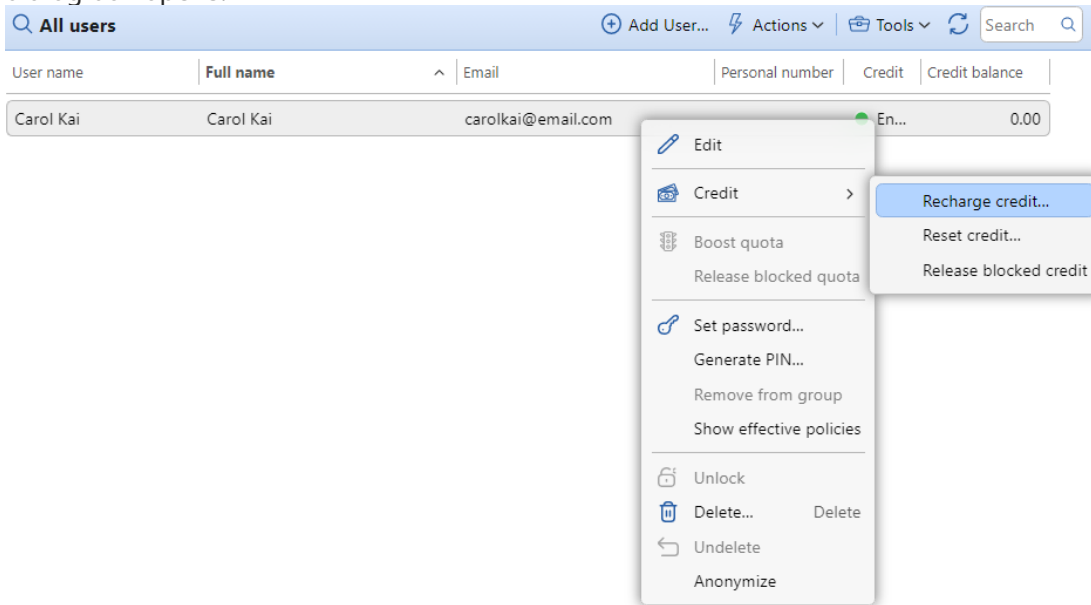


## 19.2.3 Recharging credit on the Users main tab

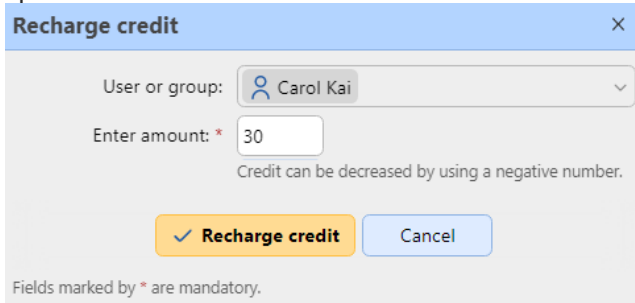
To open the **Users** main tab on the **KNM** Web administrator interface, go to **KYOCERA, Users**.

To recharge credit to selected users:

1. Select the users.
2. Click **Actions**.
3. Hover over **Credit** and click **Recharge credit** in the **Actions** drop-down. The Recharge credit dialog box opens.

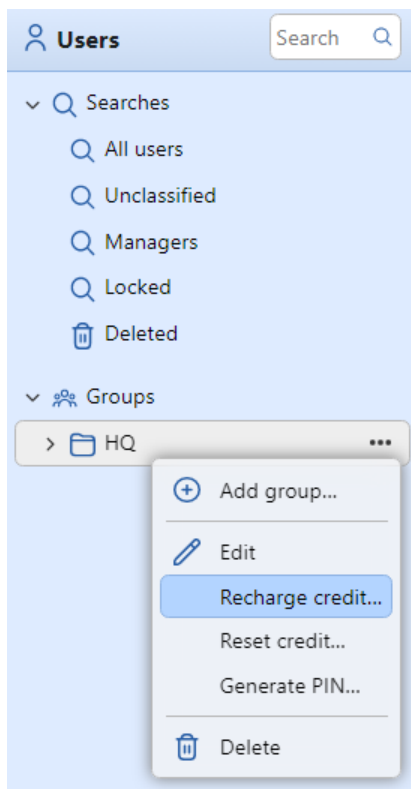


4. **Enter amount** to be recharged, and then click **Recharge credit**. The credit is increased by the specified amount.



To recharge credit to a group of users:

1. In the panel on the left side of the **Users** main tab, right-click the group, and select **Recharge credit**. The Recharge credit dialog box appears.



2. In the dialog box, **Enter amount** to be recharged, and click **Recharge credit**. The credit is increased by the specified amount.

## 19.3 Recharging credit by vouchers

The **KNM** administrator (and users authorized to manage vouchers) can generate and print any number of vouchers of a defined value to be distributed to users.

The vouchers can be sold to **KNM** users through any standard distribution channel. Once the user has the credit voucher, they can recharge their credit on their account on the **KNM** Web Interface, and on embedded terminals.

All generated and used vouchers are logged in the **KNM** database. The information about which voucher was used and for which user can be accessed on the **KNM** Web administrator interface. This ensures full control and transparency and enables the administrator to prevent possible misuse.

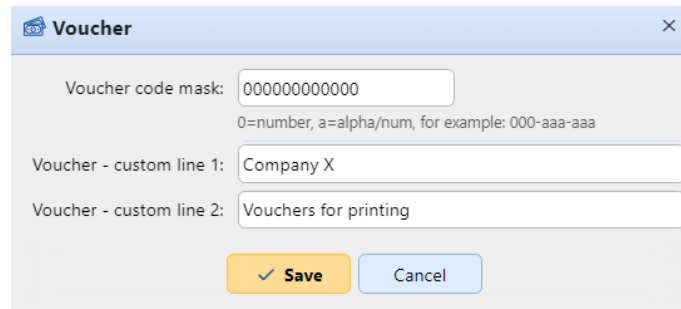
### 19.3.1 Setting the voucher format

Before the vouchers are generated, it is necessary to set the format of the voucher unique code and define the text printed on the voucher. These parameters can be set and modified on the **Credit** settings tab, under **Payment providers**. Select **Voucher** and mark it as **Enabled**. Then, double-click the **Voucher** item (or select the item and click **Edit**) to open the **Voucher** properties panel.

The unique code format can be defined by creating a **Voucher code mask** – a predefined code template consisting of zeroes and lower case a's. Zeroes are substituted by numbers and a's are substituted by upper case letters or numbers. For example, the *00a000aaa* mask will generate numbers such as *86D9841POE*, *03E8976E67*, etc.

Always set the code format adequate to the number of users and the frequency of the voucher generation process, to ensure a sufficient variety of codes. If the amount of the currently valid codes is large and the variety not sufficient, the chance of randomly guessing the valid code number is high and the credit system can be easily bypassed.

The text entered in the **Voucher-custom lines 1 and 2** fields is displayed on the printed vouchers. You can enter, for example, the name of your company and additional information.



Do not forget to set the currency on the **General** settings tab, if you have not set it earlier. The currency on the printed voucher is the same as the one set in **KNM**.

### 19.3.2 Custom logo for Credit Vouchers

If you want to use your own logo on **KNM** credit vouchers instead of the default **KNM** logo, you can import the new logo on the **Personalization** settings tab in the **KNM** Web Administrator Interface.

The file with the logo has to be in the *JPG*, *JPEG*, *PNG* or the *BMP* format; the recommended size of the logo is *398px x 92px*.

To import the logo:

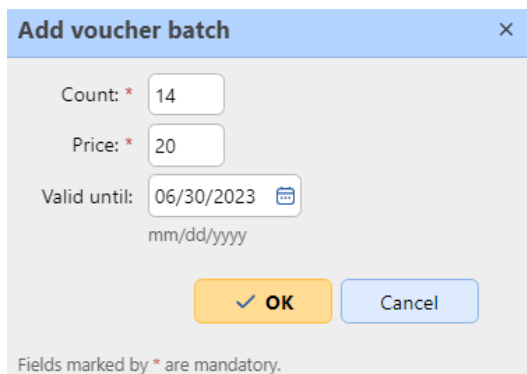
1. On the **KNM** Web administrator interface, open the **Personalization** settings tab. (**KYOCERA, Settings, Personalization**).
2. On the tab, under **Custom application logo**, click **+Add**, browse and upload the file with the logo, and lastly click **Save** at the bottom of the tab. A preview of the new logo is displayed on the tab.

### 19.3.3 Voucher Batches

Vouchers can be generated on the **Voucher Batches** tab of the **KNM** Web Interface. To open this tab, go to **KYOCERA, Voucher Batches**.

To generate new vouchers:

1. On the bar at top of the **Voucher Batches** tab, click **+Add**. The Add voucher batch dialog box appears.
2. In the dialog box, enter the number of vouchers to be generated in the **Count** field, the **Price** of the vouchers, add the validity period in the **Valid until** field, and then click **OK**.



The new voucher batch record is displayed in the voucher batches list. You can overview all of the vouchers by double-clicking a record.

### Managing Voucher Batches

Voucher batches can be filtered by serial number, date, creator, price, expiry date, etc. From the **Voucher Batches** main tab, you can export the list of voucher batches to a CSV, and display and print vouchers included in particular batches.

#### 19.3.4 Providing users with rights to manage vouchers

To enable users to manage vouchers on the **Voucher Batches** main tab, provide them with the **Manage Vouchers** rights.

For more information about rights and how to provide them, see [Rights](#).

#### 19.3.5 Vouchers usage overview

To open the table of all the vouchers generated in one batch, double-click the batch on the **Voucher Batches** main tab (or select the batch, and then click **Open** on the bar at the top of the tab).

In the table, you can see records of all of the generated vouchers with information such as the unique code, price, validity, the current status of the voucher usage, etc. If the number of records is too high to be displayed clearly, you can filter them by using filters on the left side. Vouchers can be filtered by code, voucher batch, price, etc.

To delete a voucher, select it on the table and click **Delete** on the bar at the top of the tab. When a voucher is deleted, the code on the voucher becomes invalid.

## 19.4 Recharging credit via PayPal

Another way of recharging credit in **KNM** is to let users directly buy the credit via PayPal on their accounts on the **KNM** Web interface.

A PayPal Business account is required to receive the payments.

The currency used on the PayPal account of the paying users has to match the currency set on the **KNM** server. In case someone pays in a different currency, the payment does not go through and stays in the pending transactions of the receiving PayPal account. In order to receive the payment, the administrator

has to approve the transaction on the PayPal account. After this, the credit must be manually recharged on the **KNM** server as the information about the payment is not sent to **KNM**.

## 19.4.1 Setting up the PayPal payment option

To set up PayPal as a payment option, you have to create a new App to link your company's PayPal business account with **KNM**, and then set up the PayPal payment option on the **KNM** Web Interface.

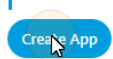
### Create a new REST API app in the PayPal Developer environment

1. Log in to the PayPal Developer environment (<https://developer.paypal.com/>) with your PayPal Business account's credentials, and then open the **Dashboard**.
2. On the **Dashboard**, under **MyApps & Credentials**, create a new REST API app. The new app's settings tab opens.

#### REST API apps

Create an app to receive REST API credentials for testing and live transactions.

**Note:** Features available for live transactions are listed in your [account eligibility](#).



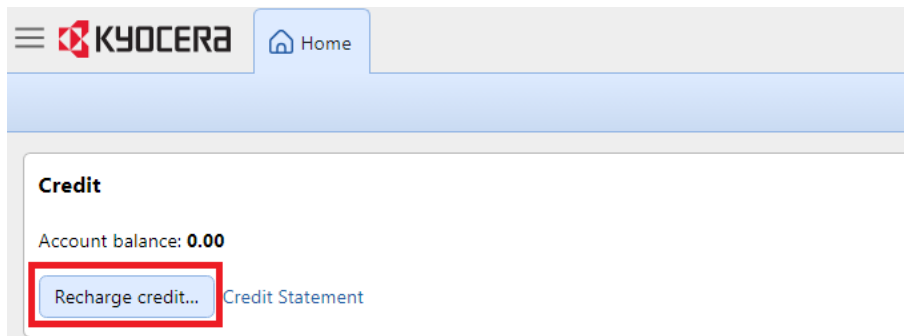
3. Select **Live** at the upper-right corner of the tab, and remember (copy) the app's **Client ID** and **Secret**. The credentials will be used to connect the account to **KNM**.

### Set up the PayPal payment option on the KNM Web Interface

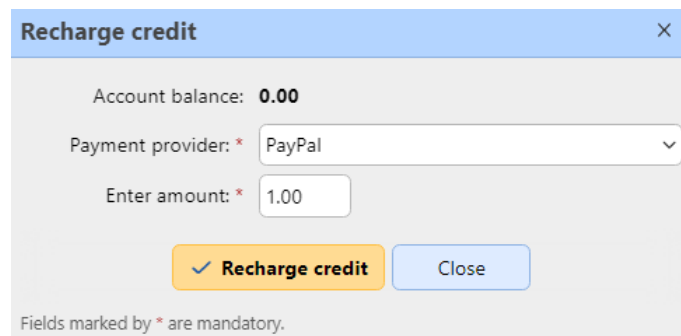
1. Open the **Credit** settings tab (**KYOCERA, Settings, Credit**).
2. On the tab, under **Payment providers**, double-click the **PayPal** payment provider. The **PayPal** properties panel opens on the right side of the tab.
3. The value of the **Currency** setting corresponds to the currency set on the **General** settings tab on the **KNM** Web Interface.
4. Type the minimal amount that users will have to pay when they buy credit.
5. Enter the **Client ID** of the REST API app into the **Client ID** text box on the PayPal properties panel and the **Secret** into the **Security key** text box below it.
6. Make sure that the **LIVE Mode** is selected, and then click **Save**. (The **SANDBOX** mode is used only for testing purposes).

## 19.4.2 Recharging credit via PayPal on the user's account on the KNM Web Interface

First of all, the user needs to log in to their account on the **KNM** Web Interface. To recharge the credit there, the user has to click **Recharge credit** under **Credit**. The Recharge credit dialog appears.



In the dialog box, the user has to select the **PayPal** payment provider, enter the amount of credit that they want to buy, and then click **Recharge Credit**.



A window with the PayPal payment options opens in the web browser; the rest of the steps correspond to the standard PayPal payment process.

After the payment is successfully sent to **KNM**, the **Payment successful** dialog box appears.

**F** PayPal tries to connect to the **KNM** server via the hostname or IP address that is set on the **Network** settings tab of the **KNM** Web Interface. In case a hostname is set on the tab and paying users receive the "This site can't be reached / XYZ's server DNS address could not be found. / DNS\_PROBE\_FINISHED\_NXDOMAIN" message, try to replace the hostname with the IP address of your server.

## 19.5 Recharging credit via WebPay

The WebPay payment gate enables customers to directly pay for their credit via a payment card or via a digital wallet.

### 19.5.1 Setting up WebPay

You need to have a WebPay account, get a public and a private key; the public key has to be uploaded to the WebPay server and the private one needs to be uploaded to **KNM**. Also, you need to remember/copy the password of the private key. You can either use your own keys (for more information, check the WebPay documentation) or use the WebPay tools to create new ones.

**KNM** needs the following data:

- **Merchant number:** The Merchant number can be found on the WebPay portal, under **Key management**.
- **Private key:** The private key can be generated on the WebPay portal, under **Key Management**. It can be in the *.key*, *.pem* or *.crt* format.
- **Private key password:** The private key password is the password that is provided to WebPay during private key generation, or the passphrase used to create the private key manually.

## 19.5.2 Setting up the WebPay payment option on the KNM Web Interface

1. Open the **Credit** settings tab (**KYOCERA, Settings, Credit**).
2. On the tab, under **Payment providers**, right-click the **WebPay** payment provider, and then click **Edit** on the shortcut menu. The **WebPay** properties panel opens on the right side of the tab.
3. The value of the **Currency** setting corresponds to the currency set on the **General** settings tab of the **KNM** Web Interface.
4. Type the **minimal amount** that users will have to pay when they will buy credit.
5. Enter the **Merchant number** of the REST API app into the **Merchant number** text box and set the **MODE** to *PRODUCTION*.

WebPay configuration panel showing:

- Merchant number: 8888880012
- Mode: PRODUCTION

6. Upload the **Private key** from WebPay (click **Choose File**, select the file, and then click **Open**), enter the **Private key password** provided during generating of the private key, and then click **Save**.

Private key configuration panel showing:

- Private key: Choose File gpwebpay-pvk.key
- Key is uploaded.
- Private key password: .....
- Buttons: Save, Cancel

## 19.5.3 Recharging credit via WebPay on the user's account on the KNM Web Interface

First of all, the user needs to log in to their account on the **KNM** Web Interface. To recharge the credit there, the user has to click **Recharge credit** under **Credit**. The Recharge credit dialog appears.

KYOCERA Net Manager interface showing the **Credit** section:

- Account balance: 0.00
- Buttons: Recharge credit..., Credit Statement

In the dialog box, the user has to select the **WebPay** payment provider, enter the amount of credit that they want to buy, and then click **Recharge Credit**.

A window with the **WebPay** payment options opens in the web browser; the rest of the steps correspond to the standard WebPay payment process.

After the payment is successfully sent to **KNM**, the **Payment successful** dialog box appears.

**F** WebPay tries to connect to the **KNM** server via the hostname or IP address that is set on the Network settings tab of the **KNM** Web Interface. In case a hostname is set on the tab and paying users receive the "This site can't be reached / XYZ's server DNS address could not be found. / DNS\_PROBE\_FINISHED\_NXDOMAIN" message, try to replace the hostname with the IP address of your server.

## 19.6 Recharging credit via CASHNet

The **CASHNet** payment gate enables customers to directly pay for their credit via a payment card or via a digital wallet.

To be able to integrate the **CASHNet** payment gate into **KNM**, you need to have a **Checkout store** created by the provider of the service. For the correct setup and **KNM** integration, you need to save the following data:

- **Operator ID, Password, Station, and Client Code** are necessary for logging in to the CASHNet Web User Interface.
- **Merchant name, Station, Store URL, and Item code** of the **Checkout store** are necessary for the integration into **KNM**.

### 19.6.1 Setting up the CASHNet payment option

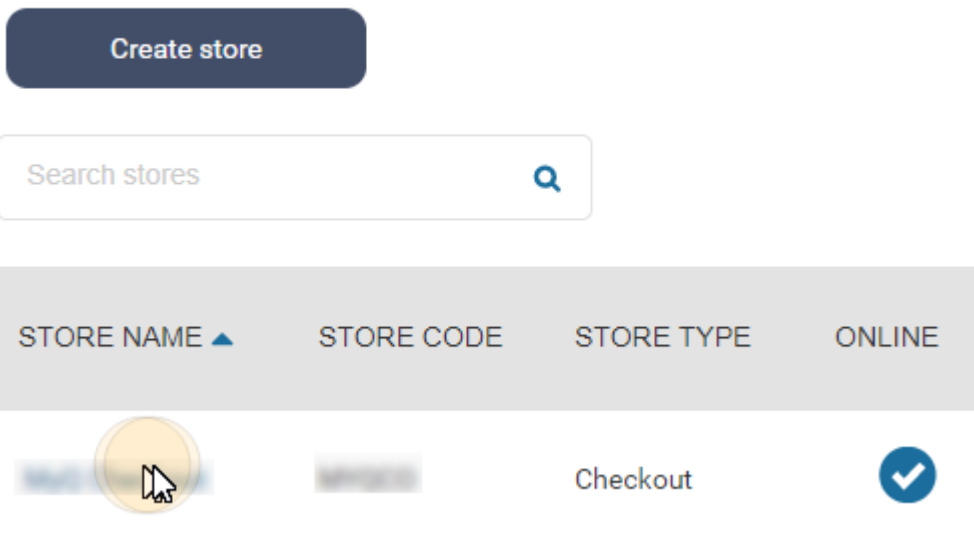
#### Set up the eMarket store on the CASHNet Web User Interface

1. Log in to the **CASHNet** Web User Interface.
2. Open the **Store Setup** tab.
3. On the tab, click the dark blue button with the text **Click here to use new eMarket store setup for Storefronts&Checkouts**. The eMarket store setup page opens.

Click here to use the new eMarket store setup for Storefronts & Checkouts

- On the page, double-click the **Checkout store** button to open its setup page.

## eMarket



- On the Checkout setup page, under **End of transaction behavior**, configure the following options:
  - Show receipt page:** *disable*
  - Use redirect URL(s):** *enable*
  - Redirect URL for successful transactions & successful online post responses:** leave empty
  - Redirect URL for unsuccessful transactions or non-responsive online post attempts:** leave empty
  - Append data to the redirect URL:** set to *Yes, and redirect using HTTP post*

### End of transaction behavior

Show receipt page

Use redirect URL(s)

Redirect URL for successful transactions & successful online post responses

Redirect URL for unsuccessful transactions or non-responsive online post attempts

Append data to the redirect URL  No  Yes, and redirect using HTTP get  Yes, and redirect using HTTP post

You can now leave the CASHNet Web User Interface.

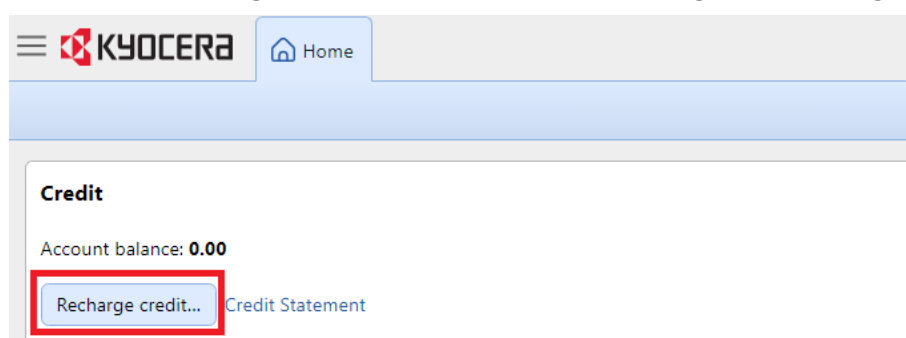
## Set up the CASHNet payment option on the KNM Web Interface

- Open the **Credit** settings tab (**KYOCERA, Settings, Credit**).

2. On the tab, under **Payment providers**, double-click the **CASHNet** payment provider (or right-click the **CASHNet** payment provider, and then click **Edit** on the shortcut menu). The **CASHNet** properties panel opens on the right side of the tab.
3. The value of the **Currency** setting corresponds to the currency set on the **General** settings tab of the **KNM** Web Interface.
4. Type the **Minimal amount** that users will have to pay when they buy credit.
5. Enter the **Merchant name**, **Station**, **Store URL**, and **Item Code** of the Checkout store, and then click **Save**.

## 19.6.2 Recharging credit via CASHNet on the user's account on the KNM Web Interface

First of all, the user needs to log in to their account on the **KNM** Web Interface. To recharge the credit there, the user has to click **Recharge credit** under **Credit**. The Recharge credit dialog appears.



In the dialog box, the user has to select the **CASHNet** payment provider, **enter the amount** of credit that they want to buy, and then click **Recharge Credit**.

A window with the **CASHNet** payment options opens in the web browser; the rest of the steps correspond to the standard **CASHNet** payment process.

After the payment is successfully sent to **KNM**, the **Payment successful** dialog box appears.

**F** CASHNet tries to connect to the **KNM** server via the hostname or IP address that is set on the Network settings tab of the **KNM** Web Interface. In case a hostname is set on the tab and paying users receive the "This site can't be reached / XYZ's server DNS address could not be found. / DNS\_PROBE\_FINISHED\_NXDOMAIN" message. Try to replace the hostname with the IP address of your server.

## 19.7 Recharging credit via SnapScan

With the **SnapScan** app, users can pay for their **KNM** credit via a QR code displayed in the app on their mobile phones.

To be able to connect **SnapScan** to **KNM**, you need to create a **Merchant Snapscan Account** and obtain the **Merchant Account API**. Within the setup of the connection on the **KNM** Web Interface, you must enter the **Merchant ID** and the **API key** of the account.

As **SnapScan** is a South African service, users need to use a phone with a South African Mobile number (+27) to be able to scan the QR code and pay for the credit.

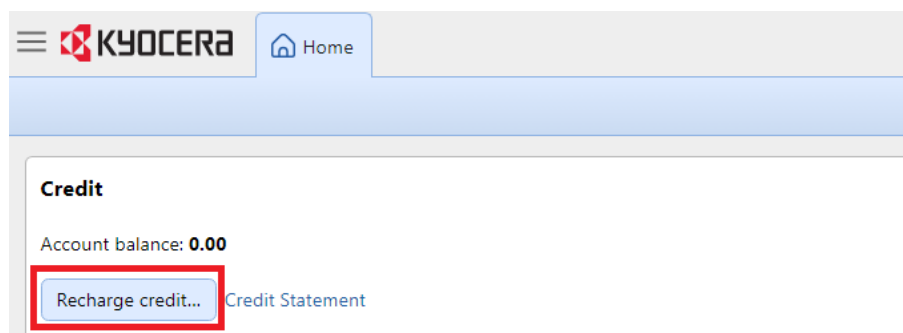
### 19.7.1 Setting up the SnapScan payment option

To set up the SnapScan payment option on the **KNM** Web Interface:

1. Open the **Credit** settings tab (**KYOCERA, Settings, Credit**).
2. On the tab, under **Payment providers**, double-click the **SnapScan** payment provider. The **SnapScan** properties panel opens on the right side of the tab.
3. The value of the **Currency** setting corresponds to the currency set on the **General** settings tab of the **KNM** Web Interface. For the SnapScan payment method to work, it needs to be set to **ZAR**.
4. Type the **Minimal amount** of money that has to be paid when a user buys the credit.
5. Enter the **Merchant ID**(Company Name) and the **API key** provided by SnapScan.
6. Set the **Time interval to get payments** (in seconds), and click **Save**. The **Time interval to get payments** setting limits the time for the recharge action; if **KNM** does not receive confirmation of the payment within the interval, the credit recharge is canceled. If the payment is successful but **KNM** does not receive the response within the time limit, the user has to contact the **KNM** administrator, who can manually recharge the credit.

### 19.7.2 Recharging credit via SnapScan on the user's account on the KNM Web Interface

First of all, the user needs to log in to their account on the **KNM** Web Interface. To recharge the credit there, the user has to click **Recharge credit** under **Credit**. The Recharge credit dialog appears.



In the dialog box, the user has to select the **SnapScan** payment provider, **enter the amount** of credit that they want to buy, and then click **Recharge Credit**.

A window with the SnapScan payment options opens in the web browser; the rest of the steps correspond to the standard SnapScan payment process.

After the payment is successfully sent to **KNM**, the **Payment successful** dialog box appears.

**[-]** SnapScan tries to connect to the **KNM** server via the hostname or IP address that is set on the Network settings tab of the **KNM** Web Interface. In case a hostname is set on the tab and paying users receive the *"This site can't be reached / XYZ's server DNS address could not be found. / DNS\_PROBE\_FINISHED\_NXDOMAIN"* message, try to replace the hostname with the IP address of your server.

## 19.8 Bulk credit recharge

In **KNM**, you can also import a bulk of credit from a bank statement or a CSV file.

The feature can be managed on the **Credit Statement** tab or on the **Users** main tab. To import a bulk of credit from a bank statement or CSV on either of the two tabs:

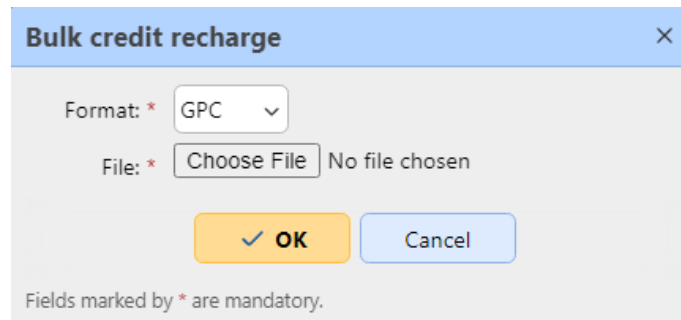
On the bar at the top of the tab (**Users** or **Credit Statement**), click **Tools**, and then click **Bulk credit recharge** in the **Tools** drop-down. The Bulk credit recharge dialog box opens.

### For bulk credit recharge from a bank statement:

The **KNM** system can process the data from a GPC file. The variable symbol from the bank statement is used as unique data for the pairing of the payment and the **KNM** user. The number must correspond to the user's personal number. The personal number can be imported or manually entered in the **Personal Number** field on the user properties panel, on the **Users** main tab.

On the bar at the top of the tab (**Users** or **Credit Statement**), click **Tools**, and then click **Bulk credit recharge** in the **Tools** drop-down. The Bulk credit recharge dialog box opens.

In the dialog box, select the **GPC** format option, choose the GPC file, and then click **OK**. Before importing the file, **KNM** checks whether the GPC file has not already been imported. This avoids duplication of the credit recharge.



If the system finds that the import of data from this file has already taken place, an error message appears and no data are imported. If **KNM** identifies the GPC file as new, it checks all the payments on the bank statement step by step, and if it finds a variable number equal to the personal number of a **KNM** user, the user's credit is increased by the corresponding amount from the bank statement. Once **KNM** checks the GPC file, it displays a new html page with a report. The report displays both the users with increased credit and the payments with variable number not corresponding to any personal number in **KNM**.

#### **For bulk credit recharge from a CSV file:**

On the bar at the top of the tab (**Users** or **Credit Statement**), click **Tools**, and then click **Bulk credit recharge** in the **Tools** drop-down. The Bulk credit recharge dialog box opens.

In the dialog box, select the **CSV** format option, choose the CSV file, and then click **OK**. You will be informed about the success of the operation and you can see the added amount of credit in the **Credit** columns on the user list.

Structure of the CSV file:

Each non-empty row has to consist of two entries separated by a delimiter:

*name of the user\*delimiter\*amount of credit*

The entered delimiter has to be the same as the delimiter set on the **General** settings tab, under **Column delimiter in CSV**.

## **19.9 Manual reset of users' credit on the KNM Web Interface**

The administrator (and users authorized to recharge credit) can manually reset the credit of each user to a specific value. This can be done either on the **Credit Statement** main tab, or on the **Users** main tab if the **KNM** Web interface.

On the **Credit Statement** tab, you first open the credit reset action, and subsequently select the users and groups whose credit is to be recharged. On the **Users** tab, you first select the users or the group, and then reset their credit.

To authorize a user to reset credit on the **Credit Statement** tab, you need to provide them with the rights to **Recharge credit**. To authorize a user to reset credit on the **Users** tab, you need to provide them with the rights to **Recharge credit** and to **Manage Users**. The authorized user can reset the credit on their **KNM** Web interface in the same way as the **KNM** administrator.

## 19.9.1 Resetting credit on the Credit Statement tab

On the **Credit Statement** tab, you can overview the changes in the credit balance of **KNM** users, and also reset credit to users and groups. To open the tab on the **KNM** Web Interface, go to **KYOCERA, Credit Statement**.

To reset credit to users or groups:

1. Click **Reset credit**. The Reset credit dialog box appears on the tab.
2. In the dialog box, either **Enter the card ID** of a user, or select the **User or group** to reset the credit to, then **Enter amount** of the credit, and click **Reset credit**.

## 19.9.2 Resetting credit on the Users main tab

To open the **Users** main tab on the **KNM** Web Interface, go to **KYOCERA, Users**.

To reset credit to a specific user:

1. Select the users, click **Actions**, hover over **Credit**, and then click **Reset credit** (or select the users, right click one of them, hover over **Credit**, and then click **Reset credit** on the shortcut menu.) The Reset credit dialog box opens.
2. In the dialog box, **Enter amount** of the new credit, and then click **Reset credit**. The credit is reset to the specified amount.

To reset credit to a group of users:

1. On the panel on the left side of the **Users** main tab, right-click the group, and then click **Reset credit** on the shortcut menu. The Reset credit dialog box appears.
2. In the dialog box, **Enter amount** of the new credit, and click **Reset credit**. The credit is reset to the specified amount.

The administrator can also release blocked credit for a user by selecting the user, clicking **Actions**, hovering over **Credit**, and then clicking **Release blocked credit** (or by right-clicking the user, hovering over **Credit**, and selecting **Release blocked credit**).

## 19.10 Credit accounting reports

On the **Reports** main tab, you can create, edit and generate two types of reports with information about credit:

- The **Credit balance** type of reports contains information about the actual state of the credit balances of the selected users (or members of the selected group). The data are ordered by user name.
- The **Credit operations** type of reports shows all changes of credit balance of the selected users (or members of the selected group) over a defined time period. It also contains information about the person who either spent or recharged the credit, the type of the recharge method and eventually about numbers of used credit vouchers. The data order is chronological.

## 20 Quota


---

With the quota feature activated, you can set a limit to the usage of print related services. You can either limit the number of printed or scanned pages, or set an overall cost limit for all the services using prices from a price list. If the limit is close to be reached, the user or group receive an email with a warning and if the limit is reached or exceeded, they can be prevented from further printing and copying.

Each quota can monitor one of the following parameters:

- the total number of printed and copied pages
- the number of printed and copied color pages
- the total number of printed and copied monochrome pages
- the total number of scanned pages
- the overall cost of print services

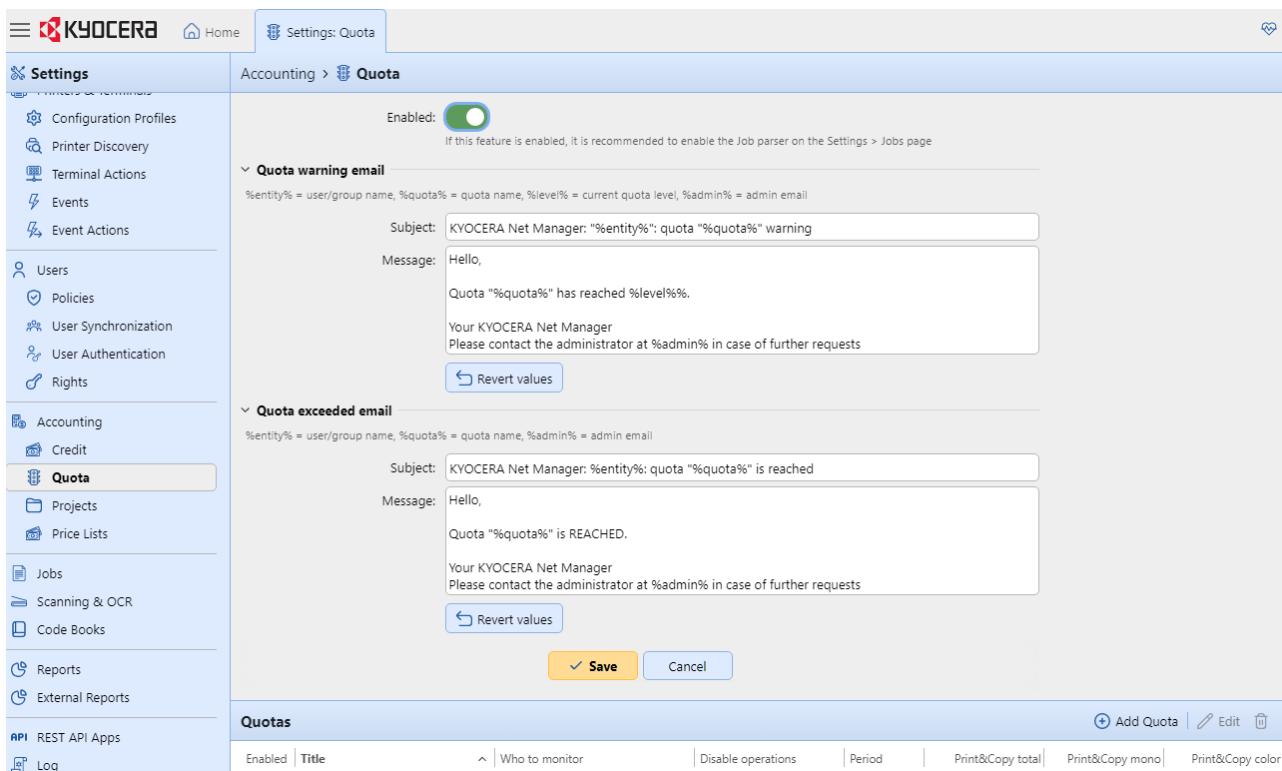
Quotas are active permanently until disabled and they reset after the specified interval. Users can check their quota status on their web user interface. If a printing device is equipped with an embedded terminal, users can see the current percentage of their quota status there.

 The quota on overall cost of print services requires setting a price list with prices of particular functions (print/copy/scan – B&W/color) on each printer. Both types of quota (the quota on the number of pages and the quota on the overall cost) require using the Job parser to get the print job metadata (number of pages, color etc.). For information about how to set the prices and how to activate the parser, see [Price List](#) and [Jobs](#).

### 20.1 Activation and general setup

You can enable the Quota feature by selecting the **Enabled** quota option at the top of the **Quota** settings tab (**KYOCERA, Settings, Quota**). Each quota can then be individually enabled or disabled on its properties panel.

On this tab, under **Quota warning email**, you can type the subject and the body of the email that is sent after reaching the preset warning (e.g. 80% of the quota) and, under **Quota exceeded email**, the subject and the body of the email that is sent when the limit of a user or group is reached or exceeded.



## 20.2 Creating quotas

To add a new quota:

1. On the bar in the bottom section of the **Quota** settings tab, click **+Add Quota**. The new quota properties panel opens on the right side of the screen.
2. On the panel, enter the quota name, set its parameters, and then click **Save**.

The new quota is enabled and appears on the **Quota** overview list (**KYOCERA, Settings, Quota**).

### Combining quotas

Quotas are independent of each other. Therefore, it is always the most strict quota that applies to a particular user or group.

For example: There are two quotas applied to a user. Both of them disable printing after a certain amount of printed pages – one after five printed pages and the other after ten printed pages. After the user prints five pages, the lower quota applies and they cannot print. The quota can be boosted, allowing the user to print more pages. If they print five more pages, the higher quota applies.

## 20.3 Editing quotas

The quota properties panel opens immediately after a new quota is created. To open an already existing quota, double-click on it on the list on the **Quota** main tab (**KYOCERA, Quota**). After you set the properties, click **Save** to submit the changes.

Each quota has the following set of properties:

### Basic settings: enabling and naming the quota

- Each quota is enabled by default. To disable or re-enable it, click the **Enabled** button.
- Enter the name in the **Title** text box.

### Time period

- In the **Period** list, select the reset period of the quota (*Day, Week, Month, Quarter, Half year, Year, Last X days*). The default period is *Month*. The *Last X days* period counts the number of pages or the overall cost over the last X days. For example, if the quota is 10 pages over three days and the user printed 5 pages the day before yesterday and two pages yesterday, they can print up to three pages today.
- In the **Period start** list, select the date when the period starts for the *Month, Quarter, Half year* and *Year Period*, day of the week for the *Week Period* or the number of days for the *Last X days Period*.
  - If you choose the *Day Period*, you must also set a time at the **Reset quota at** field.

### Monitored users or groups

You have to select from three options regarding the quota scope. It can apply to one user, to all members of one group, or to an accounting group/cost center.

- To select a user the quota applies to, select the **User** option, and then choose the user from the list.
- To select a group and apply the quota to all its members, select the **Members of a group** option, and choose the group from the list. This way, the quota applies to each user independently; If the limit is ten pages, every user can print ten pages.
- To select an accounting group or a cost center the quota applies to, select the **Accounting Group** or **Cost center** option, and then choose the accounting group or cost center group from the list (this option depends on the [Accounting](#) settings; the option selected there is displayed in Quota). This way, every member contributes to the total. If the limit is ten pages and one member prints seven pages, there are only three pages remaining for the group.

### Monitored value

- If you select *Cost* as the **Monitored value**, the quota is counted in amount of money spent.
  - Set the quota cost **Limit**
- If you select *Pages* as the **Monitored value**, the quota is counted in the amount of printed, copied and/or scanned pages.
  - Set the **Print&Copy total, Print&Copy color, Print&Copy mono** (supported by terminals 8.1 or newer) and **Scan total** in pages.

### Actions taken when the warning level is reached

- Enter the warning level (in %) in the **Warning level** text box. After the percentage of the overall limit is reached, a warning email is sent to the user.
- If you want someone else to be notified (for example the user's manager) once the warning level is reached as well, select or enter the users or email accounts in the **Send a notification to** combo box.

### Actions taken when the quota is reached

- You can disable one or more operations after the quota is reached or exceeded.
  - If the **Monitored value** is *Cost*, select them under **Disable operations**. The options are **Print, Copy, Color print** (on terminals 8.1 or newer), **Color copy** (on terminals 8.1 or newer), and **Scan**.
  - If the **Monitored value** is *Pages*, mark the **Disable operation** checkbox and the operation that has reached the limit will be disabled.
- Mark the **Terminate the current job when reached** checkbox if you want to interrupt the current job when the quota is reached. If both **Disable operation** and **Terminate the current job when reached** are checked, the job will be interrupted when the quota is reached and the

user will be redirected to the **KNM** home screen. If **Disable operation** is checked and **Terminate the current job when reached** is not, the current job will be finished and the user will be redirected to the **KNM** home screen.

- The action is not supported by scan quota
- If you want someone else to be notified (for example the user's manager) after the quota is reached as well, select or enter the users or email accounts in the **Send a notification to** combo box.

## 20.4 Boosting quotas

In situations when a user or a group of users have reached their quota and urgently need to print, you can boost the quota by a specific number of pages or by a specific amount. Quotas can be boosted on two tabs of the **KNM** Web Interface: the **Quota Boosts** main tab and the **Users** main tab. Records of the boosted quotas appear on the boost quota records list on the **Quota Boosts** main tab.

### 20.4.1 Boosting quotas on the Quota Boosts main tab

On the **KNM** Web Interface, go to **KYOCERA, Quota Boosts**. To boost a quota here:

1. On the bar at the top of the tab, click **+Add**. The Boost quota dialog box appears.
2. Select the **User or group** and the **Boost date**, and then click **OK**. The Boost quota dialog box extends – more sections are displayed. The first of the new sections shows the current availability of operations and the rest show the quotas applied to the user (or groups of users).

3. Enter the number of pages or the amount of money to the **Boost By** text box in the particular quotas sections (each quota has to be boosted separately), and then click **OK**.

### 20.4.2 Boosting quota of a particular user on the Users main tab

On the **KNM** Web Interface, go to **KYOCERA, Users**. To boost a quota here:

1. On the tab, select the user, click **Actions**, and then click **Boost quota** in the drop-down (or right-click the user, and then click **Boost quota** on the shortcut menu). The Boost quota dialog box appears with the user selected in the **User or group** drop-down.
2. Enter the number of pages or the amount of money to the **Boost By** text box in the particular quota sections (each quota has to be boosted separately), and then click **OK**.

The administrator can also release blocked quota for a user by clicking **Actions** and then clicking **Release blocked quota** (or by right-clicking the user and selecting **Release blocked quota**).

## 21 Projects

With the project accounting feature activated, users can assign print, copy, and scan jobs to particular projects and consequently distribute the print cost among the projects and charge it appropriately. Project accounting can also be used as another independent level of internal accounting in addition to devices, users, and groups. Projects can be manually created on the **KNM** web interface or imported from a CSV file. They can be assigned to print jobs in the **KNM** Desktop Client pop-up window, on the **KNM** web interface, on an embedded terminal, or on a touch panel of a HW terminal.



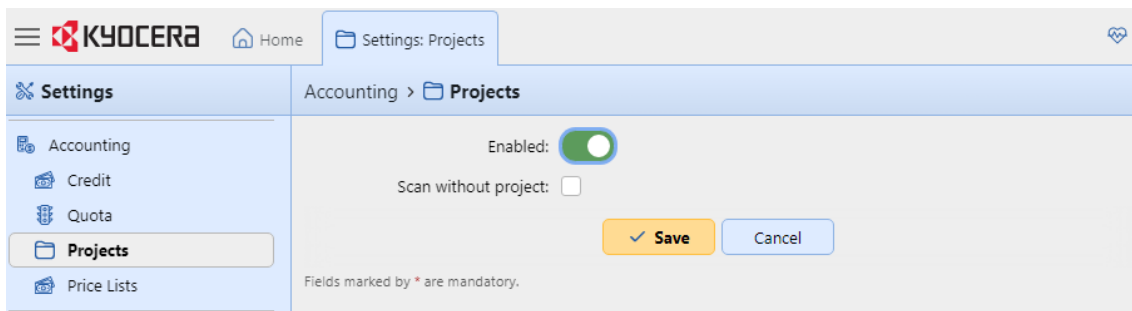
Status	Code	Name	Description
●	0	No Project	Enable operations without a project
●	1	HQ	Project for HQ
●	2	Marketing	Project for Marketing

### 21.1 Projects activation and setup

On the **Projects** settings tab (**KYOCERA, Settings, Projects**), you can enable, or disable projects. Furthermore, you can change the global settings of the projects feature there.

Select the **Enabled** option to globally activate project accounting.

**Scan without project:** Users scan directly when this option is selected. They have to select a project when the option is not selected.



### 21.2 Creating projects

To add new projects to **KNM**, go to **KYOCERA, Projects** and:

1. On the bar at the top of the **Projects** main tab, click **+Add project**. The new project properties panel opens on the right side of the screen.
2. On the **General** tab, enter the project **Name**, a unique project **Code**, optionally its **Description**, and then click **Save**.

**Project** [X]

General Rights

Name: \* Engineering

Code: \* 3  
0-9 a-z A-Z \_ / \ -

Description: Project for the Engineering team

Save Cancel

Fields marked by \* are mandatory.

3. Click on the **Rights** tab, to manage user rights to the project (all users have rights to a project by default). On the bar at the top of the **Rights** tab, click **+Add User**. The Select user or group dialog box appears, where you can select the user (or group of users) that you want to provide with rights to the project, and then click **OK**. To remove the rights from a user, select the user and click the trash can button. The user (or group of users) disappears from the **Rights** list.

**Project** [X]

General **Rights**

+ Add User [Edit] [Trash] [Refresh] Search

Name | Rights

All users Use project

## 21.3 Project management

After the projects are created, you can see them listed on the **Projects** main tab. Using the buttons on the bar at the top of the tab, you can add new projects, edit current projects, import projects from CSV files and display/hide deleted projects.

### Restoring deleted projects

1. Click **Tools** and select **Show deleted** to display any deleted projects.

+ Add project [Actions] [Tools] [Refresh] Search

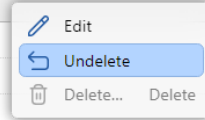
^ | Description

Enable operations without [Project]

Import...  
Show deleted

2. Select the project, click **Actions**, and then click **Undelete** in the Actions drop-down (or right-click and select **Undelete**).

Status	Code	Name	Description
●	0	No Project	Enable operations without a project
○	3	Engineering	Project for the Engineering team
●	1	HQ	Project for HQ
●	2	Marketing	Project for Marketing



### 21.3.1 Managing project groups

For bigger companies, it is easier to manage projects in groups on e.g. a functional or geographical level. The maximum is five levels deep. Rights set on the group level will automatically be inherited by sub-groups and/or the projects inside these groups. It is then possible to set specific rights to sub-groups or specific projects. After saving these rights they will not be overwritten by the default group rights.

#### Creating groups

1. Right-click **Project groups** and select **New group**.
2. Set the **Name** on the **General** tab of the project group in the right pane.
3. Click the **Rights** tab to add or delete users from the project group.
4. Click **Save**. The project group will be visible in the left pane.

#### Adding a project to a group

1. Select the group that you want to add a project to.
2. Click **New project** on the menu bar.
3. Enter the project details.
4. Click **Save**. The **Project group Code** will be upped by one.

## 21.4 Importing projects from CSV files

Another option of adding projects to **KNM** is to import them from CSV files. This can be done manually and also as a scheduled task.

- The manual import is described in [Manually importing projects](#).
- For information on how to set up the scheduled task, see [Setting up the Project synchronization scheduled task](#).
- You can find the required syntax of the CSV file in [Syntax of the projects' CSV file](#).

You can import projects with a hierarchy.

Within the CSV import, new projects are added and existing projects are updated. Projects already present in **KNM** that are not listed in the CSV file are left untouched. Each project is recognized by the value of its code, and updated only if the CSV file contains a row with the same code.

### 21.4.1 Manually importing projects

On the bar at the top of the **Projects** main tab, click **Tools**, and select **Import**. The Import dialog box appears.

In the dialog box, click **Choose File** and select the CSV file, and then click **OK**. After the import is done, imported projects are listed on the **Projects** main tab.

In addition, an information message appears at the top of the tab. By clicking log for details, you can display the import log.

Any errors occurring during the import can be related to incorrect syntax or non-existing users or group of users listed in the CSV file.

### 21.4.2 Setting up the Project synchronization scheduled task

1. On the **Task Scheduler** settings tab, click **+Add**, and then **Import projects from CSV**. The properties panel of the new schedule opens on the right side of the screen.
2. On the panel, set up the schedule, as described in [Task Scheduler](#).
3. In the **File** section, add the path to the **CSV file** (the file should be stored on the **KNM** server).
4. Click **Save**.

### 21.4.3 Syntax of the projects' CSV file

Each row must consist of six columns, separated by the delimiter set on the **General** settings tab, under **Column delimiter in CSV**. The file must contain a header row, otherwise an error occurs and the projects will not be imported. The order of the columns is irrelevant; each column is identified by its name in the header, which must always be in English, regardless of the language setting in **KNM**.

#### Values:

- **active:**
  - 1=project is added to **KNM**
  - 0 =project is not added to **KNM**
- **code:** unique code of the project
- **name:** name of the project
- **groups:** the path of the project in the hierarchy. Levels must be separated by the pipe character (|). If the column is empty, the project is created in or moved to the root of the hierarchy.
- **description:** internal description of the project
- **users** the users or groups of users allowed to use the project. Multiple entries should be separated by commas (,).

active	code	name	groups	description	users
1	300	Project1	parent child	Optional description	"All users"
0	400	Project 2			

## 21.5 Assigning projects to print jobs

If project accounting is enabled, unassigned print jobs are paused and have to be assigned to a project before they can be printed. They are displayed on the **Jobs** main tab, under **Paused**. You can assign them on the **Jobs** main tab, in the **KNM** Desktop Client pop-up window, or on an embedded terminal.

Users who want to print an unassigned job on an embedded terminal have to select one of their projects (projects they have rights to) or eventually select the **Without project** option there (if they are allowed to print without projects). The same applies to scanning and copying – users have to select one of the projects or the **Without project** option before opening the particular panel or performing a

quick action. The exact behavior of project accounting on embedded terminals can vary depending on vendor and device model. See the particular embedded terminal manual for further information.

- [How to assign projects in KNM Desktop Client](#)
- [How to assign projects on the Jobs main tab](#)

## 21.5.1 Assigning projects in KNM Desktop Client

This option is available on computers with either Windows or macOS. It requires the **KYOCERA Net Manager Desktop Client** application running on the computer where the print job is sent from.

**KNM Desktop Client** is running in the background and, unless Project accounting or any other features of the application are active for the logged user, all print jobs are sent to **KNM** without any intervention. Once the user has rights to more than one projects, all the jobs that they send are paused and the **KNM Desktop Client** pop-up window opens to offer the available projects to the user. If only one project is available to the user, it is automatically assigned, and the job is sent to the server.

The user can assign the job to an available project and print within that project. If printing without a project is allowed in **KNM**, the user can select the **No project** option; otherwise they have to select one of the available projects. If there are more jobs waiting in the queue, the user can check the ones to be printed to a particular project and jobs for another project can be printed in the next step.

For information about **KNM Desktop Client**, including installation, setup, and optional features of the application, see the **KNM Desktop Client for Windows or macOS** manuals.

## 21.5.2 Assigning Projects on the Jobs main tab

To assign a project to a print job:

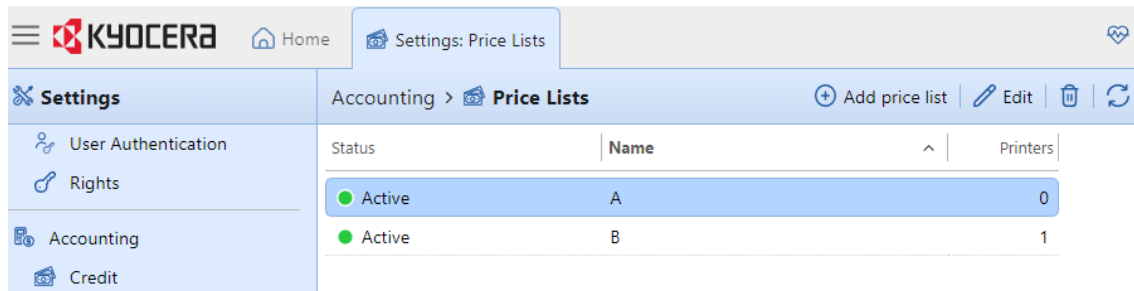
1. On the **Paused** list on the **Jobs** main tab, double-click the print job that you want to assign the project to. The print properties panel opens on the right side of the screen.
2. On the panel, select the **Project** that you want to assign to the job, and then click **Save**.

## 22 Price List

On the **Price Lists** settings tab, you can create price lists and attach them to configuration profiles. Price lists are used to assess the price of each printing device operation. That is necessary for monetary accounting and **KNM** advanced features such as credit accounting and monetary quotas.

You can also set discounts or increase price of print, copy, scan and fax services for particular users and groups.

To open the **Price Lists** settings tab, go to **KYOCERA, Settings, Price Lists**.



### 22.1 Adding price lists

1. On the bar at the top of the **Price Lists** settings tab, click **+Add price list**. The new price list properties panel opens on the right side of the screen.
2. On the panel, enter the price list name.
3. Set up the price list.
4. Click **Save**.

### 22.2 Editing price lists

On the properties panel of the price list, you can rename the price list, define prices of print, copy, scan and fax services and attach the price list to printing devices. To open the panel, double-click the price list on the list of price lists on the **Price Lists** settings tab.

The screenshot shows a window titled 'Configuration Profiles' with a 'General' tab. At the top, there is a 'Name' field with an asterisk and the value 'A'. Below that, there is a 'User' dropdown menu currently set to 'Administrator'. The main area contains several expandable sections: 'Print', 'Copy', 'Scan', 'Paper format', and 'Fax'. The 'Fax' section is expanded, showing a 'Printed fax' field with an asterisk and the value '0.00'. At the bottom, there are 'Save' and 'Cancel' buttons. A note at the very bottom states 'Fields marked by \* are mandatory.'

## 22.2.1 Setting prices of print, copy, scan and fax services

On the **General** tab of the price list's properties panel, you can set prices of print, copy, scan, paper format, and fax services. There are two sub-tabs: the **User** sub-tab, where you set prices for **KNM** users, and the **Administrator** sub-tab, where you set prices for the **KNM** administrator.

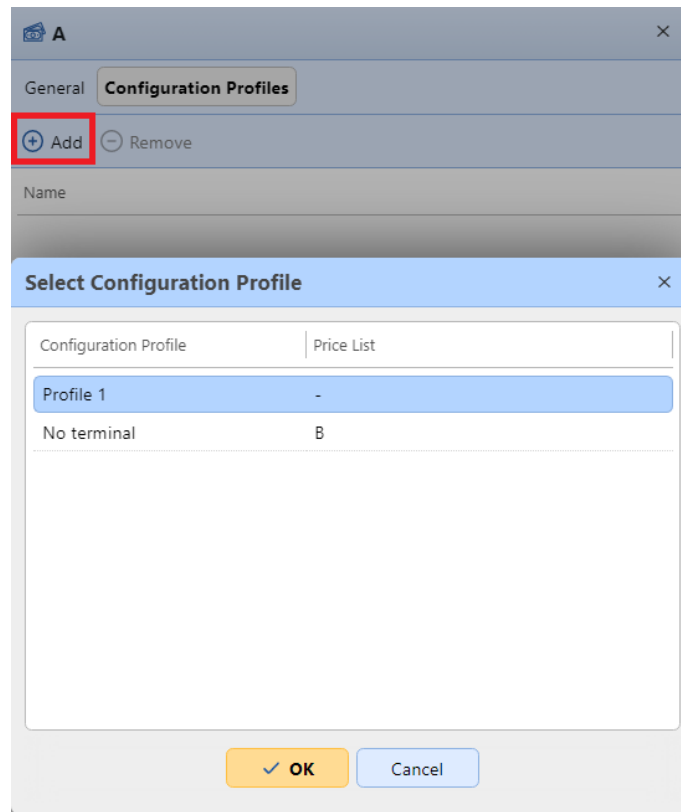
- **Print** - In this section, you can set the price per printed page for monochrome and full-color print. Some printing devices allow pricing according to coverage of paper. You can set prices for three states of coverage: **Low**, **Medium** and **High**.
- **Copy** - In this section, you can set the price per copied page for monochrome, full color and single color copying. Some printing devices allow pricing by coverage of paper. You can set prices for three states of coverage: **Low**, **Medium** and **High**.
- **Scan** - In this section, you can set the price per scanned page.
- **Paper format** - In this section, you can set the price per sheet for different paper formats.
- **Fax** - In this section, you can set the price per printed faxed page.

Some printing devices lack the counters necessary for obtaining information about some parameters, for example information about paper size. Those parameters are not counted in the final price of jobs that are carried out on these machines.

Whenever the price list is updated (its parameters values are changed and the price list is saved), a new price list is created. Pages printed with the previous version of the price list are counted according to the old settings.

## 22.2.2 Attaching price lists to printing devices

1. On the list of price lists on the **Price Lists** settings tab, double-click the price list. The new price list properties panel opens on the right side of the window.
2. Go to the **Configuration Profiles** tab.
3. Click **+Add**. The Select Configuration Profile window opens.
4. In the dialog box, select the configuration profile that you want to attach the price list to.
5. Click **OK**. The configuration profile appears on the printing devices list on the **Printers** tab.



You can also attach a price list to a configuration profile when you go to **KYOCERA, Settings, Configuration Profiles**. In the overview, double-click a profile and change the **Price List** in the right pane on the window.

You cannot attach more than one price lists to a single configuration profile. If you add a price list to a configuration profile that already has a different price list attached to it, the old price list is replaced by the new one.

## 22.3 Discounts

The prices set in price lists are applied to all users and groups without any distinction. To distinguish between particular users and groups, you can provide the users and groups with discounts, or increase the prices in the list for them.

The discounts are set in percent and are applied to all price lists. Within the discount, you can set a particular value for each print, copy, scan or fax price lists' item. The price of an action is increased by setting a negative discount for the item, for example a **-15%** discount.

The **Discounts** section, where the discounts are set, is also part of the **Price Lists** settings tab.

Discounts	
User or group	Discount
HQ	1.00%: PC, CC, A4, Fax 25.00%: Scan

### 22.3.1 Creating a new discount

1. Click **+Add discount** at the upper-left corner of the **Discounts** section. The new discount properties panel appears on the right side of the screen.
2. Set the discount.
3. Click **OK** to save it.

### 22.3.2 Editing a discount

To open the editing options of a discount, double-click the discount (or right-click the discount, and then click **Edit** on the shortcut menu, or select the discount and click **Edit**). The discount's properties panel appears on the right side of the screen.

For each discount, you need to set the user or group that it will be applied to, and the values of each item (such as B&W print or Full-color copy) of the discount in percent.

To increase the price of an item, set the discount to a negative number (such as -15%).

After the discount is set, click **OK** to save it.

The screenshot shows the 'Add discount' dialog box. It features a title bar with a lightning bolt icon, the text 'Add discount', and a close button. Below the title bar is a dropdown menu for 'User or group:' with 'Managers' selected. The dialog is organized into several expandable sections: 'Print' (expanded) with 'Black & White:' (0.00 % (PM)) and 'Full-color:' (1.00 % (PC)); 'Full-color by coverage' (collapsed); 'Copy' (collapsed); 'Full-color by coverage' (collapsed); 'Scan' (expanded) with 'Scan:' (30.00 % (Scan)); 'Fax' (collapsed); and 'Paper format' (collapsed). At the bottom are 'OK' and 'Cancel' buttons. A note at the bottom left says 'Fields marked by \* are mandatory.'

### 22.3.3 Deleting a discount

1. Select the discount.
2. Click the the trash can, or right-click and select **Delete**.

## 23 System health check

This option (available in **KYOCERA, System Health Check**) presents you with an overview of error messages with the level of severity added after some registered checks are done. The errors concern database health, disk space availability, PIN length settings, and time zone configuration, etc. They are listed in the table below.

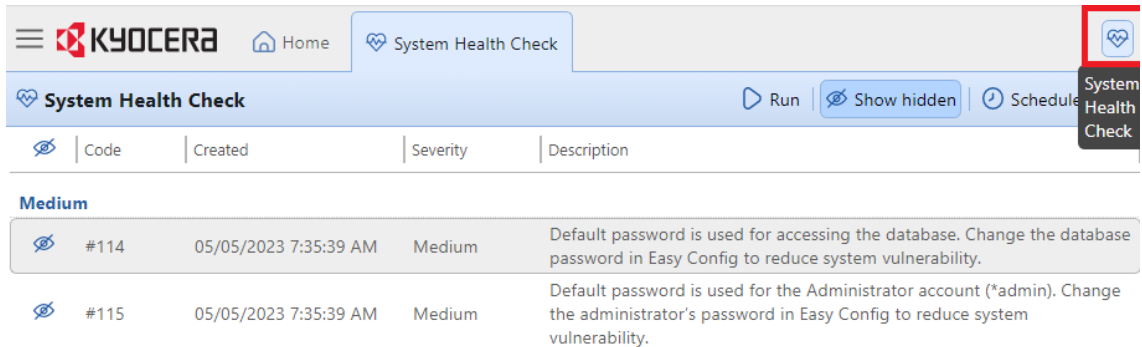
Code	Severity	Description
101	High	Main database health is not good; multiple messages can appear in the log
102	High	Log database health is not good; multiple messages can appear in the log
103	Medium	PIN length needs to be increased; see <a href="#">Generating PIN</a>
104	High	Disk space is on warning level; see <a href="#">Disk space checker</a>
105	Critical	Disk space is on critical level; see <a href="#">Disk space checker</a>
106	High	Time zones misconfiguration; see <a href="#">Time zone</a>
107	Medium	Queue(s) has an error
108	Medium	Obsolete terminal version
109	High	License subscription is going to expire
110	High	License Subscription expired
111	High	Contacting license server failed
112	High	At least one service is not running.
113	High	The logon account of at least one service doesn't match the configured account.
114	Medium	Database password is default.
115	Medium	Administrator password is default.

When the error message has a **Critical** severity, the administrator gets an email.

Every error message with a **Low** severity is logged in the **KNM** main log.

## 23.1 Using system health check

To access the system health check overview go to **KYOCERA, System Health Check** or click on the system health check button on the top-right side of the window.



The screenshot shows the KYOCERA System Health Check interface. The navigation bar includes 'Home' and 'System Health Check' tabs. Below the navigation bar, there are buttons for 'Run', 'Show hidden', and 'Schedule'. A table displays two medium severity checks with columns for Code, Created, Severity, and Description. A 'System Health Check' button is highlighted in the top right corner.

	Code	Created	Severity	Description
<b>Medium</b>				
	#114	05/05/2023 7:35:39 AM	Medium	Default password is used for accessing the database. Change the database password in Easy Config to reduce system vulnerability.
	#115	05/05/2023 7:35:39 AM	Medium	Default password is used for the Administrator account (*admin). Change the administrator's password in Easy Config to reduce system vulnerability.

Click **Run** to trigger the System health check **Task schedule** to perform a check.

Click **Show hidden** to view any hidden checks on the list.

Click **Scheduled task** to open the System Health Check task in Task Scheduler, where you can view and modify it.

## 24 Updating KNM

---

The **KNM** update to a higher version or reinstalling the same version is performed automatically after running the installation executable file.

Before a **KNM** update on Windows Server 2012/2012 R2/2016/2019 (or on Windows 8.1/10), make sure that the latest Windows updates are downloaded and installed on the server.

When upgrading or updating **KNM**, ensure all antivirus exclusions are made and that there are no running scan operations on the **KNM** directories structure.

It is strongly recommend to backup your database before the update.

 A direct upgrade to version 10.0 is only possible from version 8.2.

 **Limitation:**


Before an upgrade, go to **KNM** Easy Config and set the database password to the default "*masterkey*". Once the upgrade is complete, change the password again.

A direct upgrade to version 8.0 and higher versions from versions lower than 6.0 is no longer supported. These versions have to be upgraded via an intermediary version, for example via 6.2.

- For version 4.2 or lower, the intermediary versions are: 4.3 -> 5.2 -> 7.1.
- For version 5.2 to 5.10 the intermediary version is 7.1.

To update **KNM**:

1. Run the **KNM** software installation executable file. The Select Setup Language dialog box appears.
2. Select your language, and then click **Next**. The Setup dialog box appears. It informs you that there is an older version of **KNM** and that the installer will start the update process.
3. Click **Yes**. The Select Additional tasks dialog appears.
4. Select if you want a **KNM** Easy Config shortcut to be created and click **Next**. The rest of the update process is nearly identical to this of installing **KNM**, except that you are asked to choose upgrade options.

 More details are available in the **KNM** Upgrade manual.

## 25 Uninstalling KNM

---

To uninstall KYOCERA Net Manager:

1. Run **unins000.exe**. You can find this file in your **KNM** program folder (The default folder is: *C:\Program Files\Kyocera\KYOCERA Net Manager\*). The **KNM** Uninstall dialog box appears.
2. Click **Yes**.

All parts of **KNM** will be uninstalled except for the **Data Folder** and its **Job Folder**. You can delete these folders manually. In case you install **KNM** again, the installation program will ask if you want to use the old database files or replace them with new files.

## 26 KNM and MS Cluster

### 26.1 About

The **KNM** MS Cluster high-availability solution consists of multiple nodes in the active/passive configuration with the **KNM** Print server installed on each node. MS Cluster administrates the **KNM** services and if the currently active node becomes unavailable, it switches to one of the available passive nodes.

### 26.2 System Requirements

The fully detailed **KNM** Print Server system requirements can be found [here](#).

- Compatibility with Windows Servers

The **KNM** MS Cluster solution is supported by the following Windows Server versions and editions:

Windows Server	Editions
Windows Server 2012	Standard, Datacenter
Windows Server 2012 R2	Standard, Datacenter, Hyper-V® Server, Storage Server
Windows Server 2016	Standard, Datacenter
Windows Server 2019	Standard, Datacenter
Windows Server 2022	

- A prepared failover cluster with at least two nodes and storage for **KNM** data is needed. Each node must meet the system requirements of the **KNM** Print server and its components.
- The same time zone has to be set on each of the nodes.

**i** If your setup includes embedded terminals, make sure to have the required .NET framework version installed in each cluster node. If not, the embedded terminal installation will fail. Further information can be found in the related **KNM** Embedded terminal manuals.

**i** If the **KNM** Desktop Client is to be used on the **KNM** users workstations, the IP address or hostname of the cluster has to be set in the application (not the IP address or hostname of the nodes).

## 26.3 Licenses

With the new **KNM X** licensing model with **Installation Keys** used in MS Cluster, there is only one installation key needed. The HW code is taken from the whole cluster, not individual nodes, so the license is activated against the cluster's HW, and not a single node.

- i** With the old licensing model, when MS Cluster is used with the **KNM** Print server, the amount of licenses needed depends on the number of nodes used, as the licenses need to be added and activated separately on each node.
- **KNM** server in Site mode - licenses are received from the Central server automatically every day or during **KNM** service or Cluster Node restart.
  - **KNM** server in Standalone mode - needs an extra licenses set for each node; each licenses set must be activated only on one node.

## 26.4 Setup

### 26.4.1 Installing KNM Print Server in the cluster (all nodes)

On each cluster node, do the following:

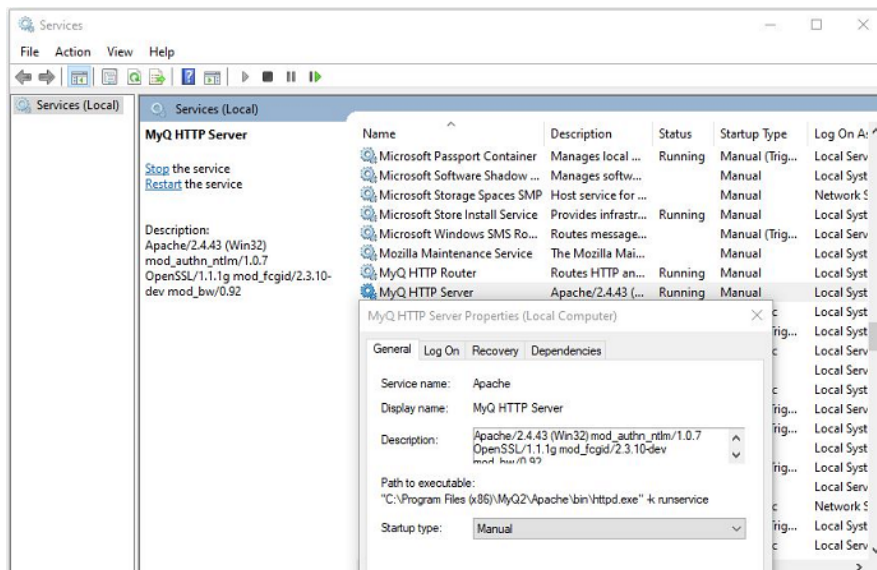
1. Run the **KNM** installation file and install **KNM** (details can be found [here](#)).
2. Make sure that the time zone set on the **KNM** server is the same as the time zone set on each node).
3. **Stop All KNM** services in the **KNM** Easy Config application.

### 26.4.2 Setting services to manual startup (all nodes)

All services used by the **KNM** server need to be set to manual startup, on every node.

The following services need to be changed this way:

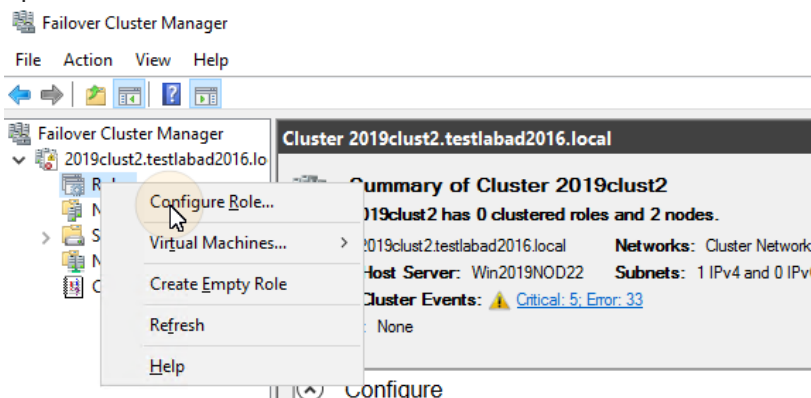
- HTTP Server
- HTTP Router
- Firebird Server - DefaultInstance
- Print Server
- Svc (not available in version 8.1+)
- PM Server
- Brand Terminals (only if embedded terminals are used)



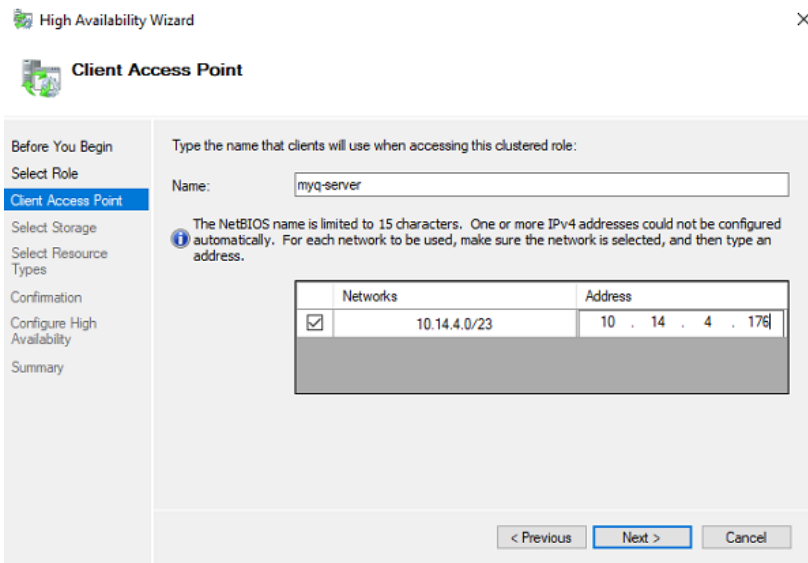
### 26.4.3 Creating the KNM server MS Cluster role (Failover Cluster Manager)

Open Failover Cluster Manager and do the following:

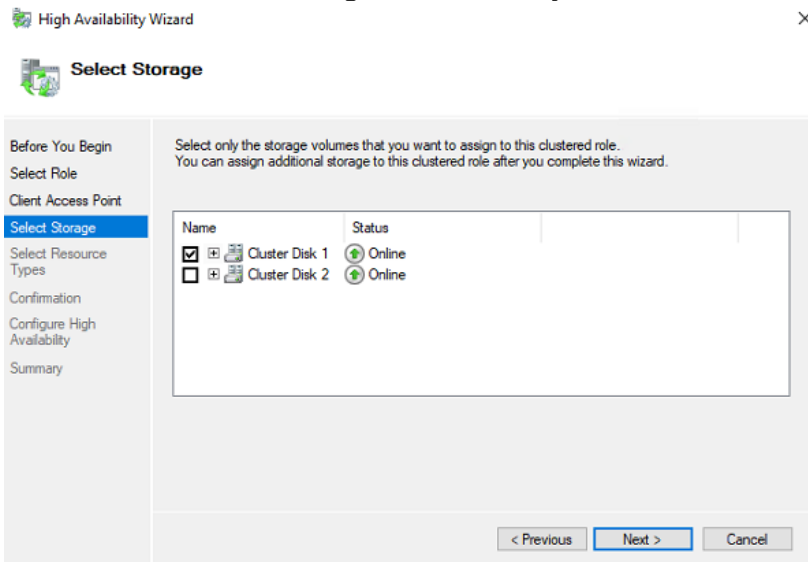
1. Right-click **Roles** and select **Configure Role** on the shortcut menu. The High Availability Wizard opens.



2. Click **Next**. The Select role tab opens.
3. On the tab, select **Other Server**, and click **Next**. The Client Access Point tab opens.
4. On the tab, type a new **Name** for the **KNM** server cluster, for example *KNM-server*, then enter an unoccupied IP address from the network to be used by the **KNM** server role, and lastly click **Next**. The Select Storage tab opens. **KNM** will use the hostname for communication with terminals, as the SMTP server in MFPs etc.



5. On the tab, select the storage volumes that you want to use for the **KNM** server.



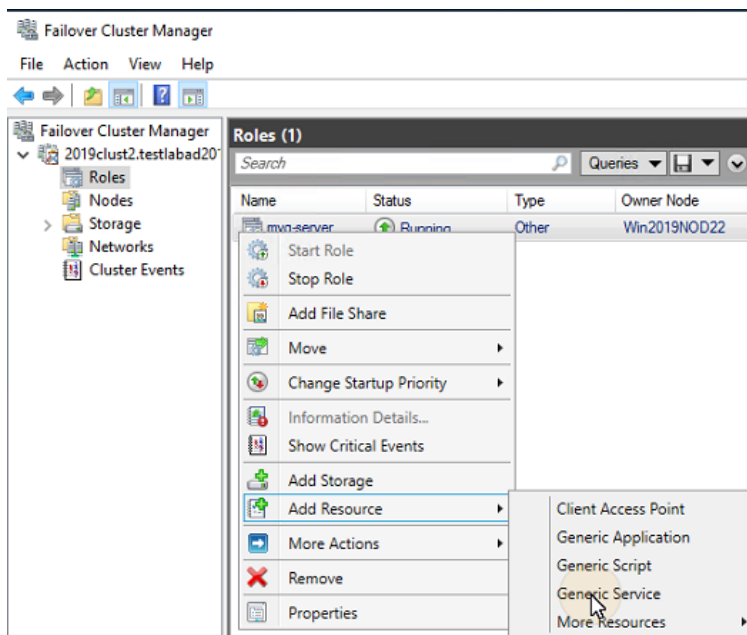
6. Click **Next** to finish the installation process.

## 26.4.4 Adding KNM resources (Failover Cluster Manager)

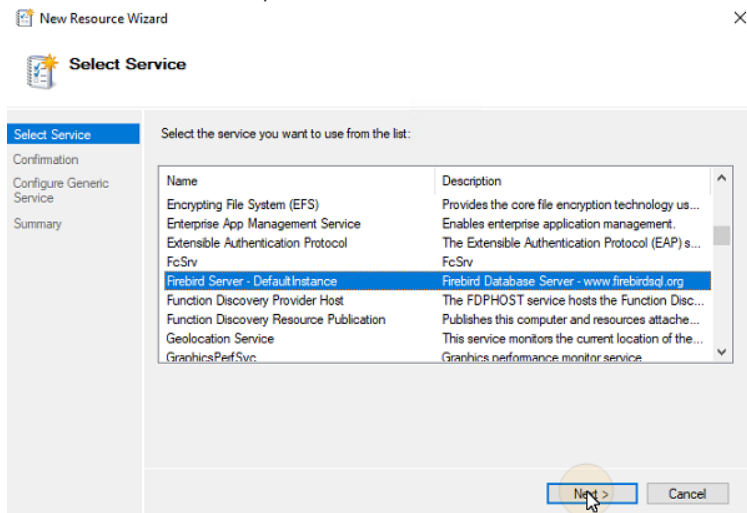
Once the **KNM** server role is created and configured, **KNM** resources need to be configured as well, in the **Roles** tab in Failover Cluster Manager.

### Add the Firebird server - DefaultInstance service to the **KNM** server role:

1. Right-click the **KNM** server role, then click **Add resource** on the shortcut menu, and click **Generic Service**. The New Resource Wizard opens.



2. In the list of services, select **Firebird Server - DefaultInstance**, and click **Next**.



3. On the **Confirmation** tab, click **Next** to create the service. The service is created and configured.
4. Click **Finish** to leave the setup.

### Add the [Apache Monitor](#) script to the **KNM** server role:

1. Right-click the **KNM** server role, click **Add resource** on the shortcut menu, and click **Generic Script**. The New Resource Wizard opens.
2. Enter the path to the **ApacheMonitor.js** script, located in the **KNM** installation folder, and click **Next**. The Confirmation tab opens. The default path to the script is:  
*C:\Program Files\Kyocera\KYOCERA Net Manager\Server\ApacheMonitor.js*
3. On the tab, click **Next** to create the service. The service is created and configured.
4. Click **Finish** to leave the setup.

## Add the MyQMonitor script to the KNM server role:

1. Right-click the **KNM** server role, click **Add resource** on the shortcut menu, and click **Generic Script**. The New Resource Wizard opens.
2. Enter the path to the **MyQMonitor.jse** script, located in the **KNM** installation folder, and click **Next**. The Confirmation tab opens. The default path to the script is:  
*C:\Program Files\Kyocera\KYOCERA Net Manager\Server\MyQMonitor.jse*
3. On the tab, click **Next** to create the service. The service is created and configured.
4. Click **Finish** to leave the setup.

## Add the TerminalsMonitor.jse script to the cluster (only if embedded terminals are used)

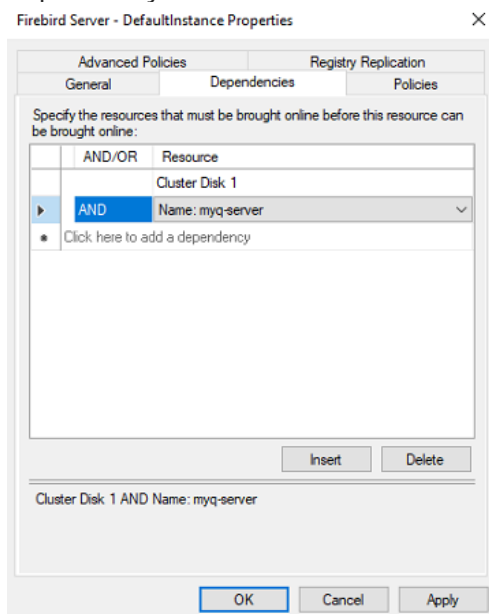
1. Right-click the **KNM** server role, click **Add resource** on the shortcut menu, and click **Generic Script**. The New Resource Wizard opens.
2. Enter the path to the **TerminalsMonitor.jse** script, located in the **KNM** installation folder, and click **Next**. The Confirmation tab opens. The default path to the script is:  
*C:\Program Files\Kyocera\KYOCERA Net Manager\Server\TerminalsMonitor.jse*
3. On the tab, click **Next** to create the service. The service is created and configured.
4. Click **Finish** to leave the setup.

## 26.4.5 Setting resources dependencies (Failover Cluster Manager)

After adding the services and scripts to the **KNM** server role, open the **Resources** tab of the **KNM** server role at the bottom of the **Roles** tab and set the dependencies of the **KNM** services and scripts.

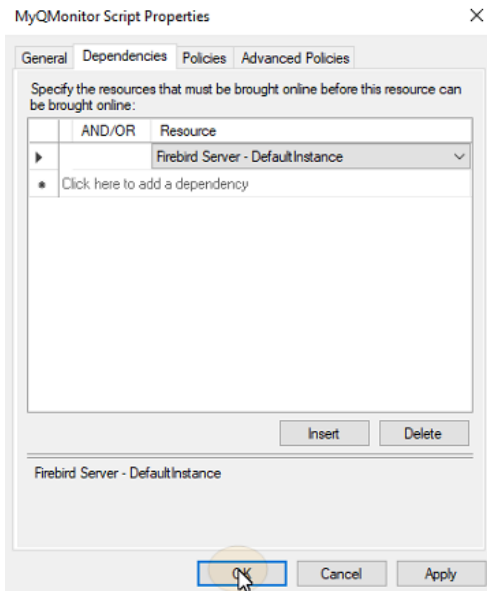
### Set the Firebird Server - DefaultInstance service dependency

1. In the list at the bottom of the tab, right-click **Firebird Server - DefaultInstance**, and click **Properties**. The Firebird Server - DefaultInstance Properties dialog box opens.
2. In the dialog box, open the **Dependencies** tab, add the shared disk drive (or NAS) where the system is supposed to work on, add the name of the **KNM** server role, and click **OK**. The dependency is set.



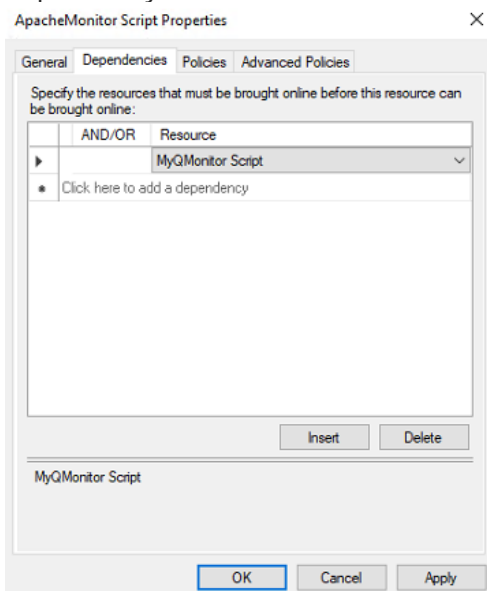
## Set the MyQMonitor script dependency

1. In the list at the bottom of the tab, right-click **MyQMonitor Script**, and click **Properties**. The MyQMonitor Script Properties dialog box opens.
2. In the dialog box, open the **Dependencies** tab, add the **Firebird Server - DefaultInstance**, and click **OK**. The dependency is set.



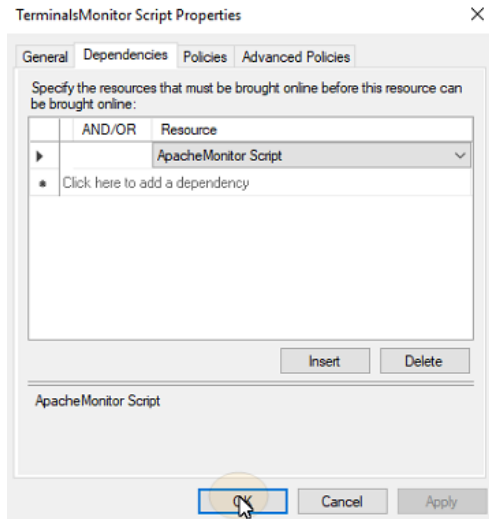
## Set the ApacheMonitor script dependency

1. In the list at the bottom of the tab, right-click **ApacheMonitor Script**, and click **Properties**. The ApacheMonitor Script Properties dialog box opens.
2. In the dialog box, open the **Dependencies** tab, add the **MyQMonitor Script**, and click **OK**. The dependency is set.



## Set the `TerminalsMonitor` script dependency (only if embedded terminals are used)

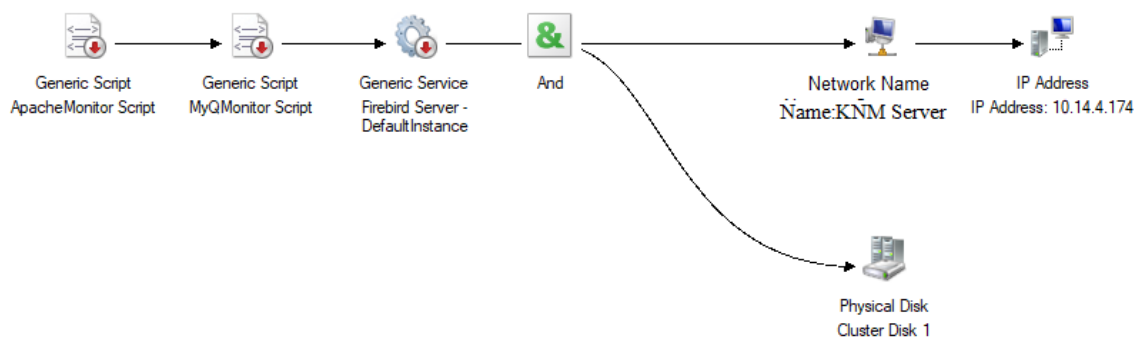
1. In the list at the bottom of the tab, right-click **TerminalsMonitor Script**, and click **Properties**. The TerminalsMonitor Script Properties dialog box opens.
2. In the dialog box, open the **Dependencies** tab, then add the **ApacheMonitor Script**, and click **OK**. The dependency is set.



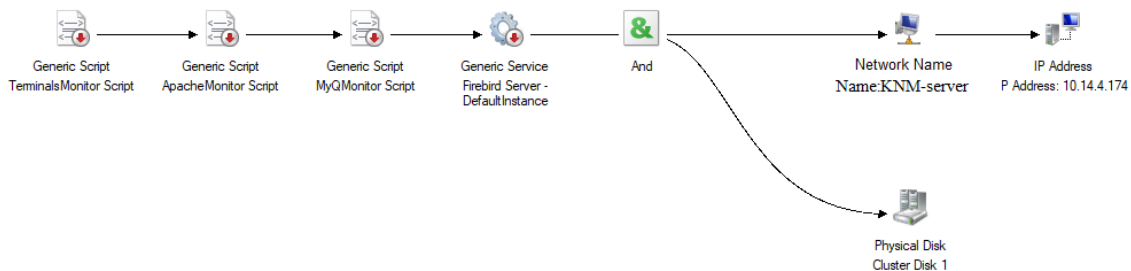
**i** Once you upload an Embedded terminal installation package on the **KNM** web administrator interface of the **KNM** cluster server, the cluster uses the script to distribute the package among all the other nodes.

### 26.4.6 Dependency Reports

To make sure that the dependencies are set correctly, you can check if the dependency report of the **KNM** server role corresponds to the below graphs:



**Dependency graph of the cluster on the KNM server**



## Dependency graph of the cluster with embedded terminal on the KNM server

To open the dependency report, right-click the **KNM** server role on the **Roles** tab of the cluster in Failover Cluster Manager, click **More Actions**, and click **Show Dependency Report**.

## 26.5 Additional Setup

Even though the installation is finished, there are some additional steps needed to setup the environment before bringing the resources online.

### 26.5.1 Setting up the KNM admin credentials (active node)

On the active node, open the **KNM** Easy Config application:

1. On the **Services** tab, **Start All** services.
2. On the **Home** tab, set the **Server Administrator Account** password and the **Database Administrator Password** (if the passwords have been changed before, they can be changed again on the **Settings** tab).
3. On the **Services** tab, **Stop All** services, and close the **KNM** Easy Config application.

### 26.5.2 Setting the location of the data folder (all nodes)

On each node of the cluster, you need to set the location of the **Data** folder and the **Jobs** folder, which require access to the shared cluster disk, so the node has to be active. Therefore, you need to switch the active mode between all of the nodes (move the **KNM** server role between the nodes).

To set the folders location, open **KNM** Easy Config on the currently active node and:

1. On the **Services** tab, **Start All** services.
2. On the **Settings** tab, under both the **Data** folder and the **Jobs** folder, click **Change location**, and then define the path to the shared cluster disk. (For more information about how to do this, check [here](#)).
3. On the **Services** tab, **Stop All** services, and then close the **KNM** Easy Config application.
4. In Failover Cluster Manager, move the **KNM** server role to the next node and repeat the process.

### 26.5.3 Running KNM in the MS Cluster environment

The following instructions have to be followed while **KNM** runs in the MS Cluster:

- You should not start, stop or restart **KNM** services while **KNM** is controlled by the MS Cluster (cluster resources are online). The services should only be managed by Failover Cluster Manager.
- When switching to a different node, **KNM** Easy Config should not be used on any node.

- When performing system maintenance (cluster resources are offline), but **KNM** services are online on any node (activated manually), do not switch to a different node. By doing so, you risk corrupting the **KNM** database.
- When switching to a different node, all services on the initial node are stopped by the MS Cluster.
- While **KNM** runs in the cluster, the IP address of the **KNM** server is the one that you have selected within the setup of the **KNM** server role, and the hostname of the **KNM** server is the one that you will set in the **KNM** web administrator interface after you bring the resources of the MS Cluster online.
- It is strongly recommended to always keep the **Storage** and **Server Name** resources online. In case you need to take them offline, make sure that all **KNM** services on the active node (the current owner of the **KNM** server role) are stopped in the **KNM** Easy Config application.
- After completing the setup (setup and additional setup) of the **KNM** server role (and eventually all of the Embedded terminals, if used), and also after each crucial change on the cluster, it is recommended to test the cluster by moving the ownership of the **KNM** server role between all nodes of the cluster.

## 26.5.4 Starting the system (Failover Cluster Manager)

To start the system, you have to bring the resources of the MS Cluster online. For information on how to do this, check [here](#).

## 26.5.5 Setting hostname of the KNM server role

On the **Resources** tab of the **KNM** server role in Failover Cluster Manager, you can see (and change) the DNS Name of the **KNM** server role. The **Full name** of the role (DNS + domain) needs to be used as the server hostname in **KNM**.

To see or change the DNS name of the **KNM** server role on the MS Cluster, do the following:

1. In the list at the bottom of the **Resources** tab of the **KNM** server role, under **Server Name**, right-click the server's name, and then click **Properties**. The Name:\*\*\* Properties dialog box opens.
2. On the **General** tab, you can see (and change) the DNS Name of the **KNM** server role.

To set the hostname of the **KNM** server role on the **KNM** cluster server, do the following:

1. On the **Network** settings tab of the **KNM** web administrator interface of the **KNM** cluster server, use the **Full name** (DNS + domain) of the **KNM** server in both of the following settings:
  - a. **This server hostname** under **General**.
2. Then click **Save** at the bottom of the tab.

## 26.6 Configuration and Maintenance

The below chapters show additional configuration and maintenance steps.

### 26.6.1 Bringing the resources of the MS Cluster online (Failover Cluster Manager)

To start the system, you need to bring all the MS Cluster resources online - the **Firebird Server - DefaultInstance** service, the **ApacheMonitor.js** script, the **MyQMonitor.js** script and the **Terminal Monitor** script (only if embedded terminals are used).

To bring a service or script online, open the Failover Cluster Manager application, go to **Roles**, right-click the service or script, and click **Bring Online** on the shortcut menu.

## 26.6.2 Taking the MS Cluster resources offline (Failover Cluster Manager)

To make sure that all the MS Cluster resources -except for **Storage** and **Server Name**- are offline, it is sufficient to take the **Firebird Server - DefaultInstance** service offline; all of the scripts will be taken offline due to their dependency on this service.

**⚠** The **Storage** and **Server Name** resources must stay online.

To take the **Firebird Server - DefaultInstance** service offline, open Failover Cluster Manager, go to **Roles**, right-click the **Firebird Server - DefaultInstance** service, and click **Take Offline** on the shortcut menu.

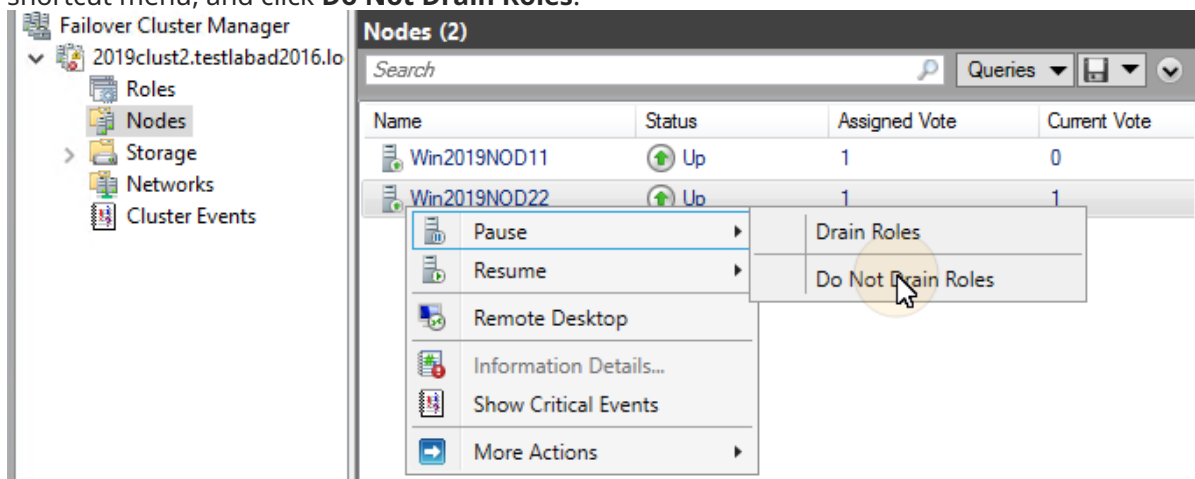
## 26.6.3 Restarting KNM services via the MS Cluster (Failover Cluster Manager)

To restart **KNM** services via the MS Cluster, take all the MS Cluster resources, except for **Storage** and **Server Name**, offline and then bring them online.

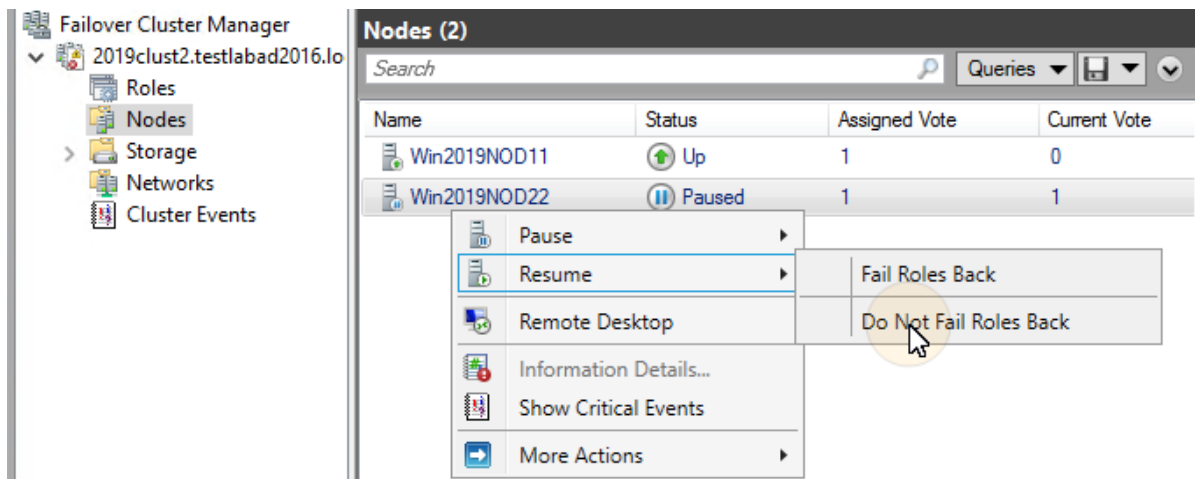
## 26.6.4 Changing the KNM admin credentials (active node)

To change the **Web Administrator Account** and **Database Administrator** passwords, you need to do the following on the currently active node (the current owner of the **KNM** server role):

1. Open the Failover Cluster Manager application.
2. Open the **Nodes** tab of the cluster, right-click the currently active node, right-click **Pause** on the shortcut menu, and click **Do Not Drain Roles**.



3. Take all the MS Cluster resources, except for **Storage** and **Server Name**, offline.
4. Open the **KNM** Easy Config application, start all services, change the passwords, stop all services, and lastly close the application.
5. Bring the resources of the cluster online.
6. Open the **Nodes** tab of the cluster in Failover Cluster Manager, right-click the node, right-click **Resume** on the shortcut menu, and lastly click **Do Not Fail Roles Back**.



## 26.7 Backup and Restore

### 26.7.1 Backing up the KNM database on the MS Cluster

The automatic and manual backup processes do not differ from the standard backup processes described in “Backing up KNM Data”. The only setting that requires special attention is the backup destination folder. It is recommended to save the backup files on the shared cluster disk.

### 26.7.2 Restoring the KNM database on the MS Cluster (all nodes)

Before restoring the **KNM** database, **KNM** has to be installed and set up on all the MS Cluster nodes.

Now you need to restore the **KNM** database and settings on the active node of the Cluster (the current owner of the **KNM** server role) via the following steps:

1. **Start All** services via **KNM Easy Config**.
2. Open the **Database** tab in **KNM Easy Config**.
3. In the **Main Database** section, click **Restore....** Select the *database\_\*.zip* file, and click **Open**. If the backup is password protected, there is a prompt to provide the password. The database is restored and, if needed, upgraded as well.
4. Repeat the process for all the other nodes.

### 26.7.3 Using Database Encryption

If you are using the **Database Encryption** feature in **KNM Easy Config**, it is necessary to perform the following steps after encrypting or restoring your database:

1. Stop all Cluster resources except for **Storage** and **Server Name**.
2. Open **KNM Easy Config** on the active node and start all services.
3. Enable DB encryption.
4. **Stop All** services in **KNM Easy Config**.
5. Copy the DB encryption key to all the other nodes. The key is located by default in “C:\Program Files\Kyocera\KYOCERA Net Manager\Firebird\plugins\keyholder.conf”.
6. **Start All KNM** services in **KNM Easy Config**, and bring all the resources online via Failover Cluster Manager.

## 26.8 Upgrading KNM

### 26.8.1 Necessary steps before the upgrade

Before starting the upgrade, make sure that you have an up-to-date and properly finished backup of the **KNM** database. The database can be backed up either manually in **KNM** Easy Config or automatically as a scheduled task in the **KNM** web administrator interface. To make sure that the backup file is preserved, it is recommended to copy the database backup file to a different location.

### 26.8.2 Upgrading KNM (all nodes)


The upgrade needs to be performed on each node of the cluster. To be able to upgrade **KNM** on a node, you need to have access to the shared cluster disk, so the node has to be active. Therefore, you need to switch the active mode between all of the nodes (move the **KNM** server role between the nodes).

Before upgrading **KNM** on the nodes, take all the MS Cluster resources, except for Storage and **Server Name**, offline.

To upgrade **KNM** on all nodes, start with the currently active node (the owner of the **KNM** server role) and do the following:

1. **Start All** services via **KNM** Easy Config.
2. Run the **KNM** installation file.
3. Finish the installation process.
4. **Stop All** services via **KNM** Easy Config, and then close the **KNM** Easy Config application.
5. Move the **KNM** server role to the next node and repeat all the steps.

After **KNM** is upgraded on all the nodes, bring all the MS Cluster resources online.

 During the installation, you might encounter a warning message about a problem related to updating the **KNM** database. In such cases, continue with the setup, as the problem does not impact the installation.

## 26.9 Recommended Troubleshooting

The MS Cluster solves issues on the currently active node which might affect the availability of the **KNM** server, by switching to one of the available passive nodes.

Problems related to the **KNM** server need to be treated manually. In case you encounter such problems, it is recommended to restart **KNM** services in the Failover Cluster Manager application. If the problem persists, contact your support.

In case the MS Cluster does not start, try taking all the MS Cluster resources, except for **Storage** and **Server Name**, offline, and then try to manually start **KNM** services. If successful, it is likely that the problem is on the cluster side; otherwise the problem is probably related to the **KNM** server, in which case contact your support.

## 27 Available languages

Language	Abbreviation
Arabic (Saudi Arabia)	ar
Bosnian (Bosnia & Herzegovina)	bs
Bulgarian (Bulgaria)	bg
Chinese (Simplified)	zh-cn
Chinese (Traditional)	zh-tw
Croatian (Croatia)	hr
Czech (Czech Republic)	cs
Danish (Denmark)	da
Dutch (The Netherlands)	nl
English (United Kingdom)	en
English (United States)	en-us
Estonian (Estonia)	et
Finnish (Finland)	fi
Flemish (Belgium)	nl-be
French (France)	fr
German (Germany)	de
Hungarian (Hungary)	hu
Icelandic (Iceland)	is
Italian (Italy)	it

Language	Abbreviation
Japanese (Japan)	ja
Korean (South Korea)	ko
Latvian (Latvia)	lv
Lithuanian (Lithuania)	lt
Norwegian (Norway)	no
Polish (Poland)	pl
Portuguese (Brazil)	pt-br
Portuguese (Portugal)	pt
Russian (Russia)	ru
Serbian (Serbia)	sr
Slovak (Slovakia)	sk
Slovenian (Slovenia)	sl
Spanish (Spain)	es
Spanish (United States)	es-us
Swedish (Sweden)	sv
Turkish (Turkey)	tr
Welsh (Wales)	cy

For the KYOCERA contact in your region, see Sales Sites sections here:

<https://www.kyoceradocumentsolutions.com/company/directory.html>