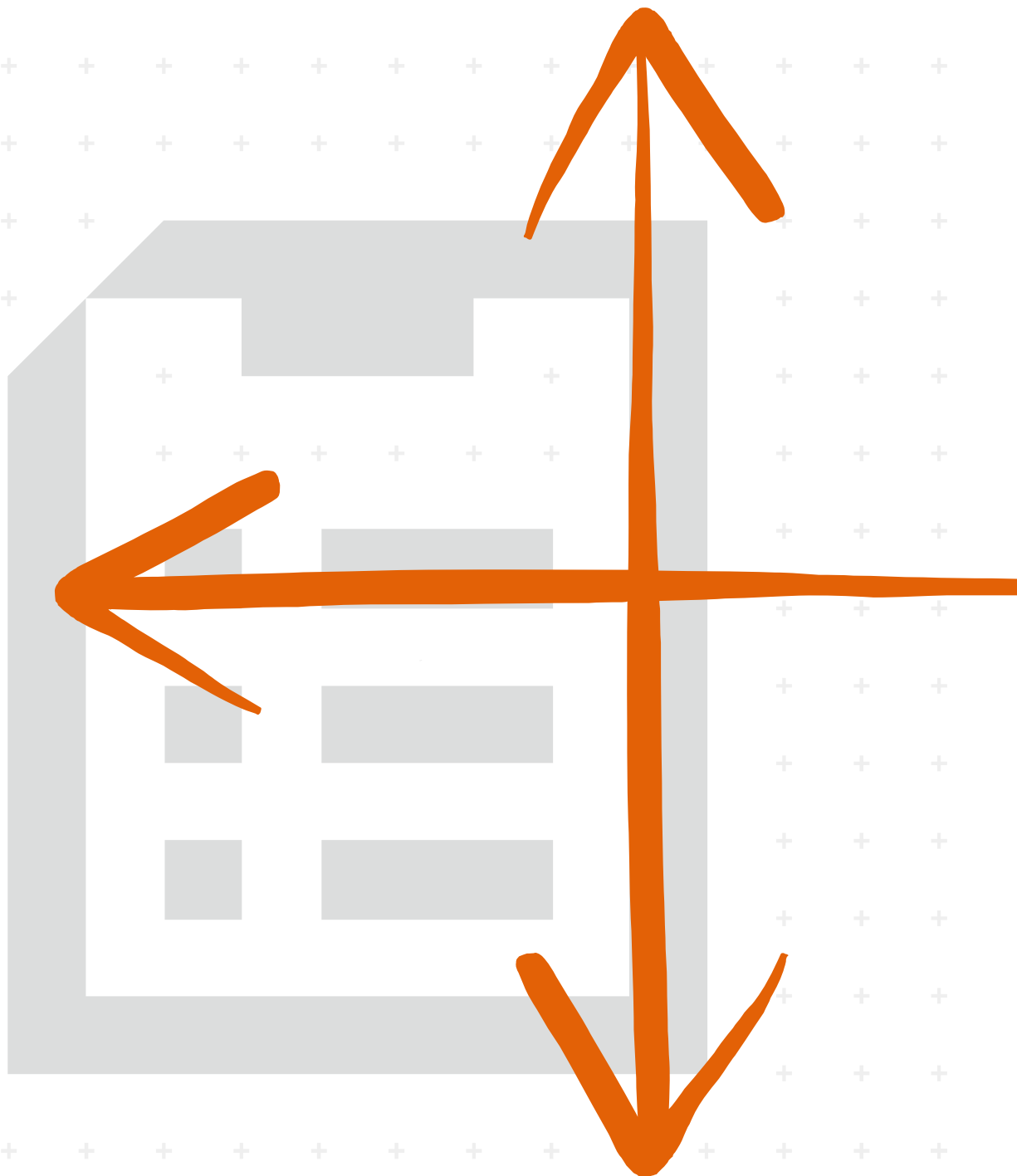


# KYOCERA Net Admin

## User Guide Supplement



## Legal Notes

Unauthorized reproduction of all or part of this guide is prohibited.

The information in this guide is subject to change without notice.

We cannot be held liable for any problems arising from the use of this product, regardless of the information herein.

© 2019 KYOCERA Document Solutions Inc.

## Regarding Trademarks

KYOCERA Net Admin is a trademark of KYOCERA Document Solutions Inc.

Microsoft®, Windows®, and Active Directory® are registered trademarks of Microsoft Corporation in the U.S. and/or other countries.

All other brand and product names herein are registered trademarks or trademarks of their respective companies.

Examples of the operations given in the "Microsoft SQL Server Setup" section in this guide support the Microsoft SQL Server 2008 R2.

The features described in this guide vary depending on your device model.

# Table of Contents

<b>Introduction .....</b>	<b>2</b>
Change History .....	2
Supported Operating Systems .....	3
<b>Approved Updates.....</b>	<b>4</b>
Login and Consoles .....	5
Administration .....	7
Device Manager .....	11
Multi-Set Template Editor .....	14

# Introduction

This supplement to the *KYOCERA Net Admin User Guide* provides information specific to the improvements and new features added to KYOCERA Net Admin, starting with software version 3.4.

This document is intended to complement, not replace, the existing guide. For general instructions not covered in this supplement, see the *KYOCERA Net Admin User Guide*.

## Change History

### KYOCERA Net Admin version 3.8

- Added support for Windows Server 2019
- Added firmware version polling
- Removed support for usage data collection

### KYOCERA Net Admin version 3.7

- Added support for adding networks using a script file
- Updated Legal Notes and Regarding Trademarks section
- Added Supported Operating Systems topic in Introduction

### KYOCERA Net Admin version 3.6

- Removed support for Windows 8

### KYOCERA Net Admin version 3.5

- Added support for usage data collection
- Added support for remote services and device registration to perform remote maintenance from the KYOCERA Fleet Services (KFS) Manager
- Updated the supported .NET Framework version from 4.0 to 4.5

### KYOCERA Net Admin version 3.4

- Added steps for resolving security certificate error when opening the application
- Updated the list of supported Windows operating systems:
  - Added support for Windows Server 2016
  - Removed support for Windows Vista, Windows Server 2003, and Windows XP
- Updated the supported version of Internet Explorer web browser

## Supported Operating Systems

KYOCERA Net Admin is compatible with the following Microsoft Windows operating systems:

- Windows 10
- Windows 8.1
- Windows 7
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008

# Approved Updates

This section contains only the updated information based on the changes included in KYOCERA Net Admin version 3.4 and later. For general instructions not covered in this section, see the *KYOCERA Net Admin User Guide*.

## Login and Consoles

KYOCERA Net Admin is a Web-based application that is opened with Microsoft Internet Explorer. You are required to log on to the application with a User name and Password.

### KYOCERA Net Admin Login

On the login page, you can use the following default login credentials:

Administrator

User name: **admin**

Password: **admin**

Read-only user

User name: **guest**

Password: **guest**

For greater security, we recommend changing the default passwords immediately after the first login.

You will be automatically logged off after the time of inactivity set by the administrator. The default time is 30 minutes.

---

**Note:** To prevent the browser from freezing, do not use the keyboard shortcut Ctrl+N to open a new window while the application is running.

---

### Starting and Logging In

You can start KYOCERA Net Admin from Internet Explorer 11.

- 1** In the browser, type the application's address in the format: `https://<computer name or IP address>:<port number>/netadmin/` or find the URL in the Favorites or browser history.
- 2** On the login page, type the **User name** and **Password**.
- 3** Choose a console to open from the list, or choose **Default Console**. You can change the default console after logging in.
- 4** Click **Log in**.

### Security Certificates

When using Windows Internet Explorer to access a secure HTTPS connection, a certificate error appears. This error indicates that the root certificate used for secure communication is not trusted. You may continue to access the secure website or resolve the certificate error to avoid getting the same error when reconnecting to the application.

## Resolving Security Certificate Error

- 1** In Windows Internet Explorer, click **Continue to this website (not recommended)**.
- 2** In the Address bar, click **Certificate error > View certificates**.
- 3** In the **Certificate** dialog box > **General** tab, click **Install Certificate**.
- 4** In the Certificate Import Wizard dialog box, click **Next**.
- 5** In the Certificate Store page, select **Place all certificates in the following store**, and then click **Browse**.
- 6** In the Select Certificate Store dialog box, select **Trusted Root Certification Authorities**, and then click **OK**.
- 7** Click **Next > Finish**.
- 8** In the Security Warning dialog box, click **Yes**.
- 9** In the Certificate Import Wizard dialog box, click **OK**.

To make sure that changes are applied, open the KNA application in a new window and reenter your login information.



## Administration

In the Administration console, you can manage roles and users, set properties and subscription views, and change network and discovery options. In this console, e-mail settings, database backup schedules and the device communication can be selected.

Your firewall must be properly configured to use these functions.

## Networks and Agents

With Networks and Agents, you can create device networks on both IPv4 and IPv6. IPv4 is the default selection. Properties can be displayed for the selected network, and discovery of printing devices can be started or stopped for one or more networks. Once multiple networks have been added, using the Select All button removes or changes the discovery mode for all networks at once.

For remote agents, install the agent remotely and save the agent details on the server. Once installed and registered, the remote agent can be reused for other networks and appears in the Add Network wizard. Network discovery is started through the assigned agent.

To ensure secure communication, the time setting must be no more than 1 minute apart on server and agent computers. For computers in different time zones, use a global time server or domain time server to ensure synchronized time settings.

### Adding Networks Using the Wizard

The **Add Network** wizard provides a quick method for adding new networks.

- 1 In the navigation area, select **Preferences > Networks and Agents**.
- 2 Click the **Add Network** icon.
- 3 In the **Add Network** wizard dialog box, type an alias for the network. If the **Alias** text box is left blank, the network IP address is used as the alias. If the application server is multihomed, you can choose and name a local network.
- 4 Type the address for the IPv4 or IPv6 network.

### Installing an Agent

- 1 On the Select an Agent page, select **Local Agent**, **New Agent**, or **Remote Agent**. Remote Agent appears if it was previously created through New Agent. Click **Next**.
- 2 On the Enter the Agent Details page, enter the required information for the agent:
  - For a local agent or remote agent, accept the displayed agent details.
  - For a new agent, type the agent details.
- 3 Click **Next**.

## Adding Networks Using a Script File

A script file allows you to export a list of networks and agents into CSV files. You can also import CSV files to the application.

---

**Note:** You must have administrator rights on the computer to change system settings and to run programs or files.

---

### Setting Up the Environment

**1** In Control Panel, navigate to:

**System > Advanced system settings > System Properties > Advanced > Environment Variables**

**2** In System variables, do the following:

- Select **New**, and then add **PSQL\_HOME** with the correct PostgreSQL database directory, for example, C:\Program Files\PostgreSQL\9.4.
- Select the **Path** variable, and then click **Edit**. In Variable value, add **%PSQL\_HOME%\bin** and **%PSQL\_HOME%\lib**.

---

**Note:** Use a semicolon (;) to separate each entry.

---

**3** In File Explorer, navigate to %Installation\_Directory%\bin.

---

**Note:** %Installation\_Directory% refers to the installation location of KYOCERA Net Admin, for example, C:\Program Files\Kyocera\NetAdmin\Admin.

---

**4** Verify that the following files exist:

- importExportNetworks.bat — Executes import and export commands.
- export.sql — Contains queries to export entries from PostgreSQL to CSV files.
- import.sql — Contains queries to import entries from CSV files to PostgreSQL.

---

**Note:** To avoid errors during file import or export, do not modify the import.sql and export.sql files.

---

### Exporting the Networks and Agents List to CSV Files

**1** In Command Prompt, change the directory to %Installation\_Directory%\bin.

---

**Note:** %Installation\_Directory% refers to the installation location of KYOCERA Net Admin, for example, C:\Program Files\Kyocera\NetAdmin\Admin.

---

**2** Run the **importExportNetworks.bat** script file, and then enter 1.

**3** Enter the database access password. The default password is **KMnetAdmin#2**.

If the file export is successful, then Export SUCCESSFUL appears. The AGENTS.csv and NETWORKS.csv files are saved in %Installation\_Directory%\net.

If the file export is not successful, then Export FAILED appears. No CSV files are generated.

---

**Note:** You can find the log files in %Installation\_Directory%\log\NetworksAgents.

---

### Importing CSV files to the Networks and Agents List

---

**Note:** After importing a deleted network with an uninstalled agent, the network is displayed in the Networks and Agents list with NOT CONNECTED status. To restore the network connection, install the agent. For more information, see Stand-alone Agent Installation in *KYOCERA Net Admin Installation Guide*.

---

**1** In File Explorer, navigate to %Installation\_Directory%\net.

---

**Note:** %Installation\_Directory% refers to the installation location of KYOCERA Net Admin, for example, C:\Program Files\Kyocera\NetAdmin\Admin.

---

**2** Verify that the following files exist:

- AGENTS.csv
- NETWORKS.csv

---

**Note:** To avoid errors during file import, make sure to close any open CSV files.

---

**3** In Command Prompt, change the directory to %Installation\_Directory%\bin.

**4** Run the **importExportNetworks.bat** script file, and then enter 2.

**5** Enter the database access password. The default password is **KMnetAdmin#2**.

If the file import is successful, then Import SUCCESSFUL appears. In KYOCERA Net Admin, navigate to **Preferences > Networks and Agents**, and then verify that the imported items are listed.

If the file import is not successful, then Import FAILED appears.

---

**Note:** You can find the log files in %Installation\_Directory%\log\NetworksAgents.

---

## USB Connections

The Local Device Agent (LDA) discovers and manages USB-supported Kyocera devices that are locally connected. USB connections require KYOCERA Net Admin installed and operating on the server. TCP port numbers 9000 and 9072 should be free and not blocked by a firewall. Microsoft .NET Framework 4.5 or later must be installed.

USB devices are displayed in the device list along with network-connected devices.

## Log View

With Log View, you can track and view the activities of various KYOCERA Net Admin operations. Log files can be created for maintenance tasks such as replacing toner. Once created, the log files can be saved for a maximum of three months. The log file default location is C:\Program Files\Kyocera\NetAdmin\Admin\log.

Before log files expire, they can be exported to an archive location in a .ZIP file. The archive default location is C:\Program Files\Kyocera\NetAdmin\Admin\temp\archived-log. The supported log files include the following:

- Agents upgrade**
- Certificate setup**
- Database backup**
- Database restore**
- Device configuration**
- Login**
- Manage applications**
- Manage optional functions**
- Model support update**
- Multi-Set**
- Restart devices**
- Role management**
- Send data**
- Register device**
- Upgrade firmware**
- User management**

## Device Manager

In the Device Manager console, you can access local device settings and monitor the status of multiple devices connected locally or through a network. You can create groups of devices, install firmware on a device or group of devices, display devices and properties in a list or on an office map, and send configuration parameters to multiple devices. You can also create reports for all device-related activities, and export a list of devices and their properties to a file.

## Preferences

You can set preferences for KYOCERA Net Admin in the navigation area toolbar.

### Polling defaults

Set default times for each polling option.

### Alert configuration

Create alert sets to send to users.

### Custom properties

Set custom printing device properties to appear in the Properties dialog box for each printing device.

### Edit default list views

View and modify the default list views.

## Polling Defaults

The administrator can set default times for each polling option. You can apply the default settings to current or new devices. Port 161 is used to request polling data.

### Setting Polling Defaults

- 1** In Device Manager, click **Preferences > Polling Defaults**.
- 2** Under **Enable Default**, select the polling type you want to set. Status Polling, Counter Polling, Toner Level Polling, and Firmware Version Polling are selected by default.
- 3** Under **Default Interval**, enter the default time within the range displayed under Minimum Range and Maximum Range.

---

**Note:** To restore the default settings, click **Reset**.

---

4 Click **Apply** to save your changes.

---

**Note:** To include current devices, select **Apply to all discovered devices**.

---

## Refresh

Printing device information, such as counters, toner levels, and firmware versions, are automatically updated according to the polling schedule. At any time, you can manually update this information by clicking Refresh. This process may take a few minutes.

## Multi-Set

With Multi-Set, you can send configuration parameters to multiple devices at once. You can configure device settings for a single device, multiple devices, or groups of Kyocera devices listed on the Supported Model List in the release notes. It does not support all device models.

From the Multi-Set icon in the toolbar, you can open the Multi-Set wizard. You can also download and open the Multi-Set Template Editor. The Multi-Set wizard can also be opened from the Groups menu in the navigation area.

## Multi-Set Wizard

With the Multi-Set wizard, you can configure one or more selected devices. Two modes are available:

### Quick mode

Copy settings to one or more device groups. All default settings are automatically applied when you use this mode. Settings can be copied only from a source device.

### Custom mode

Customize and copy settings to one or more device groups. You can select the settings you want to copy and the method that you will use to copy settings. Options may vary on the Multi-Set Settings page depending upon the destination device.

## Multi-Set Settings

When Custom mode is selected, the following configuration settings are available. Selections vary by device.

### Device System Settings

Basic device settings including operation panel language, timers, and security options including panel and interface locks. Some functions may require the device to be restarted.

### **Device Network Settings**

Basic settings for TCP/IP, security and network configurations. Some functions may require the device or the network to be restarted.

### **Device Default Settings**

Settings that define default behavior for print, copy, scan and FAX jobs including paper size, print and scan quality, and default media types.

### **Device Authentication Settings**

Settings that define local or network authorization for accessing a device.

### **Device User List**

Login user name, user name (and furigana, if applicable), password, e-mail address, account name, account ID on the device, and administrator access permission.

### **Device Address Book**

Number, name, furigana (if applicable), e-mail, FTP address, SMB address, FAX, internet FAX addresses, and address groups.

### **Device Document Box**

Users' custom and FAX boxes.

### **Device Network Groups**

Creation of groups used for group authorization, and enabling/disabling of groups.

### **Remote Services Settings**

Remote maintenance, including connection mode and proxy settings.

## **Register Device**

You can register a device to the KYOCERA Fleet Services (KFS) Manager for remote maintenance. Support for this feature varies by model and is enabled only if the device is not yet registered to the KFS Manager.

### **Registering a Device to the KFS Manager**

- 1** In the navigation area, select a group of devices (All Devices is the default setting).
- 2** In the device list, select a device.
- 3** In the toolbar, click **Register Device**.
- 4** In the Register device dialog box, enter the needed information.
- 5** Click **OK**.

## Multi-Set Template Editor

With Multi-Set Template Editor, you can create or change the template files. The template files specify settings for particular groups of devices that are managed by KYOCERA Net Admin. The Multi-Set function in KYOCERA Net Admin applies the templates to devices on a network.

Template files in XML or ZIP format are specific to groups of device models, and to groups of settings shared by those models.

XML format contains one Multi-Set setting.

ZIP format can contain multiple Multi-Set settings.

XML template files created in KYOCERA Net Viewer version 5.x can also be used. Address book files can also be saved in CSV format.

Several template files can be displayed at one time. You can select a file and click **Edit** to view and change the settings.

## Multi-Set Template Options

Each template supports a set of custom device settings. For some settings, the template can restart the device after the Multi-Set process is finished. Settings vary by device.

### **Device System Settings**

View and edit select device system settings.

### **Device Network Settings**

View and edit select network settings for TCP/IP, security, and network protocols.

### **Device Default Settings**

View and edit select device default settings for print, copy, scan, and FAX jobs.

### **Device Authentication Settings**

View and edit select authentication and authorization settings.

### **Device User List**

View and edit select user list settings.

### **Device Address Book**

View and edit select address book settings.

### **Device Document Box**

View and edit select document box settings for users' custom and FAX boxes.

### **Device Network Groups**

View and edit select network group settings.



## Remote Services Settings

View and edit remote services settings.

### Enabling Remote Connection to the KFS Manager

Support for this feature varies by model.

- 1** In the toolbar, click the **Multi-Set** icon, and then select **Multi-Set Template Editor**.
- 2** Select from the following options:
  - **Download the Multi-Set Template Editor** — Download and install the application.
  - **Launch the Multi-Set Template Editor** — Open the installed application. ActiveX controls must be enabled.
- 3** In Multi-Set Template Editor, click **File > New**.
- 4** In the Select Target Device Group dialog box, select the target device group for the template.
- 5** Select from the following template file types:
  - **XML template file** — Use when selecting only one setting.
  - **ZIP template file** — Use when selecting multiple settings.
- 6** In the list of Multi-Set settings, select **Remote Services Settings**.
- 7** In the Remote Services Newly Created dialog box, make your selections from the available options:
  - **Remote services** — Enable or disable device communication with the KFS Manager.
  - **Connection mode** — Manage or monitor the device from the KFS Manager.
  - **Proxy Settings** — Select proxy server settings to communicate with devices on remote networks.
- 8** Click **OK**.

The template appears in Multi-Set Template Editor as Newly Created\*.
- 9** Select **Newly Created\***, and then click **File > Save as**.

