# KYOCERA Net Admin
# User Guide

KYOCERA
Document Solutions

## 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.

## Regarding Trademarks

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

Microsoft®, Windows®, and Internet Explorer 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 this guide support the Microsoft Windows Server 2008 R2 and Server 2012 printing environments. Essentially the same operations are used for Microsoft Windows XP, Vista, Windows 7, Windows 8, and Windows 10 environments.

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

## Chapter 1 Login and Consoles


KYOCERA Net Admin Login ..... 1-1
Starting and Logging In ..... 1-1
Log Off ..... 1-1
Consoles ..... 1-2
Choosing a Console ..... 1-2
Changing the Default Console ..... 1-2


## Chapter 2 Administration


Roles and Users ..... 2-1
Adding a Role ..... 2-1
Adding a User ..... 2-1
User Properties ..... 2-2
Changing the Password ..... 2-2
Unlocking a User ..... 2-2
Subscriptions ..... 2-3
Adding an Alert Subscription ..... 2-3
Adding a Report Subscription ..... 2-3
Editing a Subscription ..... 2-4
Copying or Moving a Subscription ..... 2-4
Networks and Agents ..... 2-5
Adding Networks ..... 2-5
Deleting a Network ..... 2-8
Network Properties ..... 2-8
Start/Stop Discovery ..... 2-9
USB Connections ..... 2-9
Manage Installation Packages ..... 2-9
Uploading Installation Packages ..... 2-10
Upgrading an Agent ..... 2-10
Mail Server ..... 2-10
Selecting E-mail Settings ..... 2-11
Device Communication ..... 2-11
Database ..... 2-11
Backing Up a Database ..... 2-12
Restoring a Database ..... 2-12
Log View ..... 2-12
Creating a Log File ..... 2-13
Selecting Log File Storage ..... 2-14
Exporting a Log File Manually ..... 2-14
Scheduled Jobs ..... 2-14
Security ..... 2-15


## Chapter 3 Device Manager


Manage Groups ..... 3-1
Add Group ..... 3-1

Dynamic Groups ..... 3-1
Manual Groups ..... 3-2
Automatic Device Configuration ..... 3-3
Preferences ..... 3-5
Polling Defaults ..... 3-5
Alert Configuration ..... 3-6
Custom Properties ..... 3-7
List View ..... 3-8
User Preferences ..... 3-8
Global Characteristics ..... 3-8
Saving Changes ..... 3-8
Scrolling and Resizing the Window ..... 3-8
Set Rows per Page ..... 3-9
Edit Default List Views ..... 3-9
Add Tab ..... 3-10
Import Default Tab ..... 3-10
Edit Tab ..... 3-10
Deleting a Tab ..... 3-12
Map View ..... 3-12
Map View Toolbar ..... 3-12
Map Background ..... 3-13
Device Icon Properties ..... 3-14
Hide or View Waiting Area Icons ..... 3-15
Links ..... 3-15
Saving Map Settings ..... 3-16
Subscriptions ..... 3-16
Adding an Alert Subscription ..... 3-16
Adding a Report Subscription ..... 3-17
Adding Devices ..... 3-17
Refresh ..... 3-18
Select All ..... 3-18
Device Properties ..... 3-18
Displaying Device Properties ..... 3-18
Open Device Home Page ..... 3-20
Multi-Set ..... 3-20
Multi-Set Wizard ..... 3-21
Multi-Set Template Editor ..... 3-25
Multi-Set Log File ..... 3-25
Restart Devices ..... 3-25
Restarting a Device or Network ..... 3-25
Manage Applications ..... 3-26
Installing an Application ..... 3-26
Activating an Installed Application ..... 3-27
Deactivating an Installed Application ..... 3-28
Uninstalling an Installed Application ..... 3-29
Manage Optional Functions ..... 3-29
Activating an Optional Function ..... 3-30
Certificate Setup ..... 3-30
Importing a Certificate ..... 3-31
Deleting a Certificate ..... 3-31
Assigning a Device Certificate to Protocols ..... 3-32
Certificate Setup Log File ..... 3-33
Firmware Upgrade ..... 3-33
Risks and Recovery Options ..... 3-34
Upgrading the Firmware ..... 3-35
Send Data ..... 3-36
Sending Data by TCP or IPPS ..... 3-36

Manage Reports ..... 3-37
Creating a Device Manager Report ..... 3-37
Editing Device IDs and Device Properties ..... 3-38
Selecting a Report Template ..... 3-38
Create Report Subscriptions ..... 3-39
Export a Report ..... 3-39
Status Filter ..... 3-40
Setting a Status Filter ..... 3-40
Show or Hide Unmanaged Devices ..... 3-40
Search ..... 3-40
Searching for Printing Devices ..... 3-41

## Chapter 4 Multi-Set Template Editor

Creating New Settings ..... 4-1
Editing a Multi-Set Template ..... 4-1
Importing a CSV File ..... 4-2
Adding an Existing Template File ..... 4-2
Multi-Set Template Options ..... 4-3

# 1 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 7 or higher.

1. In the browser, click the application's address in the format: http://<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**.

### Log Off

To log off from the application, in the navigation area, click **Switch Console**, then select **Log off**.

A user is automatically logged off after the time of inactivity set by the administrator. The default time is 30 minutes.

# Consoles

You can choose a console when logging on to **KYOCERA Net Admin**, and you can change to a different console at any time.

If you select **Choose a console to open** when logging on, the console you select from the list is displayed.

The available consoles are:

**Administration**

A console for managing user accounts/roles, network/agent discovery, and system settings.

**Device Manager**

A console for managing device data, polling, alerts, and preferences.

## Choosing a Console

You can change to a different console at any time.

1. In any console, click **Switch Console**.
2. Select the desired console from the list.

## Changing the Default Console

If you select **Open the default console** and log on, your preferred console is displayed.

To change the default console:

1. Log on to **KYOCERA Net Admin**.
2. In the navigation area, click **Switch Console**, then select a console.
3. After the console has loaded, click **Switch Console** again and click **Set As Default Console**.

# 2 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.

## Roles and Users

The navigation area lists all roles and the users that belong to each role. There are several default roles and users created when the application is first installed. These default roles are **Administrators**, **Assistant Administrators**, **Help Desk**, **Subscribers**, and **Read-only**. The properties for the **Administrators** role are unavailable and cannot be edited. All default roles can be renamed except for **Administrators** and **Subscribers**. **Privileges** define what activities each role is permitted. Privileges for all roles can be edited, except for the **Administrators** role. The default users are **Administrator** and **Guest**.

There are different sets of privileges for each default role. The **Administrators** role is assigned all privileges by default. These privileges include options to edit **Administration** and **Device Manager** consoles.

### Adding a Role

You can add new roles to the existing default roles.

1. In the navigation area, select a role or user.
2. Click the **Add role** icon.
3. In the **Add role** dialog box, type a **Role name** for the new role. Do not use invisible Unicode or extended ASCII characters. The name must be unique.
4. For **Based on**, you can select a default role to base this new role on, or select **None**. If you select an existing role, the **Privileges** for that role are displayed below. You can modify these privileges for the new role you are adding.
5. Select the privileges to assign to the new role. Click the arrows next to the check boxes under **Privileges** to expand the list for more options.
6. Click **OK** to finish adding the role.

You can delete any role except **Administrators** and **Subscribers** by selecting the role, then clicking the **Delete role** icon.

### Adding a User

You can add a new user.

1 In the navigation area, select a role or user.

2 Click the **Add user** icon.

3 In the **Add user** dialog box, under **Select user type**, select **Login user** or **Subscribers (for receiving alerts and reports only)**.

Administrators can set privileges, a login name, and contact information.

The contact information is used for alert and report subscriptions by e-mail.

4 Under **Required Properties**, enter information as defined by user type and required by alerts. Do not use invisible Unicode or extended ASCII characters.

5 Under **Optional Properties**, enter optional user information.

6 Click **OK**.

## User Properties

**User Properties** displays and sets details about the user. You can view and edit properties, change a password, unlock a user, and delete or disable an account. An administrator or user must be selected in the navigation area.

### Changing the Password

An administrator or a user with **Modify Self** privilege can change the password used to log on to the application.

1 Select an administrator or user in the navigation area.

2 Select **User properties**.

3 Click **Change password**.

4 Type the new password, and type again to confirm.

5 Click **OK**.

### Unlocking a User

An administrator or a user with **Login users** / **Full Control** privilege can unlock login access for another user before the **User locking time** set in **Security** expires.

1 Select an administrator or user in the navigation area.

2 Select **User properties**.

3 Click **Unlock user**.

4 Click **OK**.

# Subscriptions

**Subscriptions** can be created for groups, and child groups inherit subscriptions from parent groups. **Inheritance** is only available for dynamic groups, and not for manual groups. A dynamic group is a device group established by user-defined device filters.

In the **Alert Sets** area, inherited subscriptions are shown in gray, and the parent group from which the subscription is inherited is shown in parenthesis.

Alert e-mails can be sent to any user. The application allows **Subscribers**, as well as **Administrators** and **Help Desk** users. **Subscribers** do not have access to the application, but can receive e-mail alerts.

Reports are created in the **Device Manager** console. Subscriptions to reports can be created in the **Administration** or **Device Manager** consoles.

**Note:** If pop-up blockers are enabled in your browser, **Add Alert Subscription**, **Add Report Subscription**, **Manage Reports**, the **About** page, and **Help** will not open.

## Adding an Alert Subscription

You can manage alert subscriptions.

1 In the navigation area, select a user.

2 Select the **User subscriptions** icon in the toolbar.

3 Click the **Add alert subscription** icon.

4 In the **Create Alert Subscription** dialog box, under **Groups**, select a group of devices.

5 Under **Alert Sets**, select the device status alerts.

6 Under **Destinations**, select at least one e-mail address. This address appears on the e-mail to the user or users who receive the message about the alert.

7 Under **Reply to**, type the e-mail address of the user who will respond to an alert e-mail. The e-mail will automatically be addressed to the same address. Multiple addresses can be entered when separated by semi-colons.

8 Click **OK**.

To make changes to the subscription, select it and click the **Edit subscription** icon.

To delete a subscription, select it and click the **Delete subscription** icon.

## Adding a Report Subscription

You can add a report subscription.

1 In the navigation area, select a user.

2 Select the **User subscriptions** icon in the toolbar.

3 Click the **Add report subscription** icon.

4 In the **Create Report Subscription** dialog box, in the **Groups** area, select a group of devices.

5 Under **Reports**, select from the reports list.

6 Select the file format for the report: PDF, HTML, XML, and CSV. File format options are limited for some reports.

7 Under **Destinations**, select at least one e-mail address. Reports can be sent to no more than two e-mail addresses.

8 Under **Schedule**, select an interval for receiving the subscription e-mail: **Daily**, **Weekly**, **Monthly**, **Quarterly**, or **Yearly**.

9 Click **OK**.

To make changes to the subscription, select it and click the **Edit subscription** icon.

To delete a subscription, select it and click the **Delete subscription** icon.

## Editing a Subscription

You can edit a subscription.

1 In the navigation area, select a user.

2 Select the **User subscriptions** icon.

3 Expand the desired subscription to display the device group.

4 Select a device group, then click **Edit Subscription**.

5 In the **Edit Alert Subscription** or **Edit Report Subscription** dialog box, edit the available options.

6 Click **OK**.

## Copying or Moving a Subscription

Subscriptions can be copied or moved to another user's list of subscriptions.

1 In the navigation area, select a user.

2 Click the **User subscriptions** icon in the toolbar.

3 Under **Alerts** or **Reports**, select the subscription, and then click the **Copy subscription** or **Move subscription** icon.

4 In the **Copy Subscription** or **Move Subscription** dialog box, select the recipient of the subscription, then click **OK**.

# 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

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.

### Adding an IPv4 Network

You can add an IPv4 network. Editing the network address or subnet mask may create an orphan device.

1 Type the IPv4 network **IP Address**. You can edit this field for all networks except the local network, or local networks if the server is multihomed.

2 Select the **Subnet Mask** from the list. Devices belong to a network based on the network range, not on the subnet of the device. For example, if the network address is 10.10.8.0, then 255.255.252.0 will contain any device with an IP address from 10.10.8.1 through 10.10.11.254. If you add a network address of 10.10.9.0 and a subnet mask of 255.255.255.0, then devices from 10.10.9.1 through 10.10.9.254 will appear on both networks.

3 Click **Next** to proceed to the **Select an Agent** page.

### Adding an IPv6 Network

You can add an IPv6 network. IPv6 options are not available if the IPv6 protocol is disabled or not supported on the server. Specify as much of the specific address and prefix as necessary to discover your device. The application uses a one-by-one discovery method for IPv6 addresses.

For example, in prefix 64 networks, to discover a device with the network address fd80:39f0:a2ae:82a:0:0:0:0150, it is sufficient to type the address as fd80:39f0:a2ae:82a:0:0:0:0100, and select 120 as the prefix. The discovery process will cover the range of the following addresses, and the device will be added:

**Start IP:** fd80:39f0:a2ae:82a:0:0:0:0100

**End IP:** fd80:39f0:a2ae:82a:0:0:0:01FF

1 Type the IPv6 network **IP Address**, for example, fd80:39f0:a2ae:82a:0:0:0:0100.

2 Select the **Prefix** for the network address. The prefix is an analog of the IPv4 subnet mask. Prefixes in the list range from 112 to 127. The default selection is 120.

For example, prefix 120 is selected. The first 120 bits then defines the subnet mask of the network. (Prefix 120 is the same as the ffff::ffff:ffff:ffff:ffff:ffff:ffff:ff00 IPv6 mask.)

3 Click **Next** to proceed to the **Select an Agent** page.

### Preparing Windows XP to Install a Remote Agent

1 To ensure a successful remote agent installation within a workgroup, go to **My Computer** > **Tools** > **Folder options**.

2 In the **Folder Options** dialog box, click **View**.

3 Under **Advanced Settings**, clear the **Use simple file sharing (Recommended)** check box.

4 Click **OK**.

### 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**.

**Note:** There are several prerequisite steps to perform before you install a remote agent within a workgroup on a Windows XP operating system. For more information, see Preparing Windows XP to Install a Remote Agent.

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**.

### Specifying Communication Settings

1 In the **Communication Settings** page, accept the default or type the number of **Retries** for connecting to the device.

2 Accept the default or type the **Timeout (seconds)** for communication between agents and devices.

3 Select **SNMP v1/2c**, or **SNMP v3**, or both.

4 Select the check box to make communication between the agent and the device use **SSL** for security.

5 Type a **Login user name** to access the device.

6 Type a **Password** to access the device.

7 Select the **Authentication mode switch**:

Select **Use local authentication** to authenticate using the login information on the device.

Select **Use settings on the device** to authenticate using the method specified on the device.

Click **Next**.

### Communication Settings for SNMP Version

Depending on the SNMP version chosen in the previous page, specify the following information in the **Communication Settings SNMP** page:

**SNMP v1/2c Settings**

Type the **Read Community** and the **Write Community** name of the device. **Write Community** sets its value in the application database when the device is first discovered.

**SNMP v3 Settings**

Select the desired **Security level**, and type the **Username**, and **Password**. Depending on the **Security level**, select from available **Hash** and **Encryption** options.

Click **Next**.

**Note:** When using an IB-23 network card, support is limited to the DES privacy option. The password in **Network Properties** must match the device's SNMP v3 password.

### Scheduling Discovery

After adding networks, you can schedule a device discovery.

1 To schedule device discovery, select **Schedule automatic device discovery on this network** on the **Activate Device Discovery** page. Click **Next**.

2 Select a daily or monthly schedule. For a discovery interval of **Days**, you can set up to three scheduled times. The list includes hours only. Click **Next**.

3 Confirm your selections and click **Finish**.

The server installs the agent on the remote computer, adds the new network, assigns the selected agent to the network, and starts discovery through the assigned agent.

## Deleting a Network

You can delete a network. This does not delete devices.

1 In the navigation area, select **Preferences** > **Networks and agents**.

2 Select a network.

3 Click **Delete Network**.

4 Select **Uninstall assigned agent from remote computer**, if you wish to suspend all polling of these devices by all consoles and delete the agent from the remote computer.

Devices that do not belong to any registered network appear under **All Devices** > **Networks** > **Orphan Devices** in the **Device Manager** console.

5 Click **OK** in the confirmation message.

## Network Properties

You can view properties for the selected network by selecting a network from the **Networks and Agents** list and clicking the **Network Properties** icon.

**General**

On the **General** tab, you can modify all properties for the selected managed network except the network address and the subnet mask of the **Local Agent**. If you clear the **Managed** check box, click **OK** to confirm, then the network will be unmanaged.

When a network is unmanaged:

Discovery is disabled.

You cannot modify any network property except for the alias.

You may create orphan devices.

**Note:** Devices that do not belong to any registered network will appear in the **All Devices\Networks\Orphan Devices** folder.

**Agent**

The agent status is displayed as **Connected** or **Not Connected**.

For **Local Agent**, you can only change the **Agent Timeout**.

For **Remote Agent**, you can change any property except **Status** and **Agent Port**.

You can create a new agent by selecting **New Agent** and entering all properties.

When there is no direct connection to a remote device, select **Use Proxy function to open Device Home Pages**.

**SNMP v1/v2c v3**

Select the **SNMP v1/v2c v3** tab to view and modify the SNMP options for the selected network.

**Discovery**

Select the **Discovery** tab to view and modify the device discovery schedules for the selected network.

### Start/Stop Discovery

The **Start Discovery** icon is available on all tabs when you select a single network or multiple managed networks. Discovery is a process for scanning a network for IP addresses of network printers to identify what devices are currently on the network. This function is independent from the discovery selection in **Network Properties**, whether you select to enable or disable discovery.

**Start Discovery**

Available when discovery is not in progress on any of the selected networks.

**Stop Discovery**

Available when discovery is in progress on any of the selected networks.

## 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 Windows XP SP3 or higher with Microsoft .NET Framework 4.0 or higher must be installed.

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

## Manage Installation Packages

You can view installation packages and upload available packages. Current installation packages are displayed at the top of the **Upgrade** view.

**Current versions**

Displays the application and **Local Agent** versions.

**Currently installed packages**

Displays the **Agent installation package**, **Agent version**, **Model update package**, and **Model support version** that are currently installed.

Under **Available installation packages**, you can upload, remove, and upgrade installation packages.

### Uploading Installation Packages

You can upload installation and update packages from the server and add them to the **Available installation packages** list.

1. In the navigation area, select **Preferences** > **Upgrade**.
2. Click **Upload package**.
3. Browse to a valid file name with an extension of .ZIP or .KNALU.
4. Click **OK** to upload the file.

You can remove an installation package by selecting it from the list and clicking **Remove package**.

### Upgrading an Agent

You can upgrade an agent in the **Available installation packages** list.

1. In the navigation area, select **Preferences** > **Upgrade**.
2. Click **Upload package**.
3. Browse for a valid upgrade file with an extension of .ZIP or .KNALU.
4. Click **OK** to upload the file.
5. Select an agent from the **Available installation packages** list and click **Upgrade**.

   Current agent information is displayed. Click **Next**.

   If the latest version is installed, a message appears. Click **Close**.
6. On the **Authorization** page, select an option for **User login** and **Password**. Click **Next**.
7. If **Use user login, password and domain from the KYOCERA Net Admin server** was selected, click **Next**.

   If **Manually enter user login, password and domain for each agent** was selected, type **User Login**, **Password**, and **Domain** for each agent. Click **Next**.

   If **Manually enter the same user login, password and domain for all agents** was selected, type **User Login**, **Password**, and **Domain** for all agents. Click **Next**.
8. On the **Confirmation** page, click **Upgrade**.

## Mail Server

KYOCERA Net Admin communicates with a mail server to send e-mail alerts and information to system administrators and subscribers.

**SMTP Server**

Defines an SMTP server for sending notifications. This information must be complete and correct for e-mail notifications to work. If alert e-mail fails to arrive, check your antivirus software. Adding port 25 or java.exe to the exception list in your antivirus software may resolve the issue.

**Authentication**

Specifies the **User name** and **Password**, if SMTP authentication is required.

**E-mail setup**

When alerts and status e-mails are sent out, the address entered in **Sender address** will appear in the e-mail address line.

### Selecting E-mail Settings

You can select settings for e-mail alerts and information to system administrators and subscribers.

1. In the navigation area, select **Preferences** > **Mail server**.
2. Under **SMTP Server**, enter the server name and port number.
3. Under **Authentication**, enter the **User name** and **Password**, when a SMTP server connection is required.
4. Under **E-mail setup**, enter the sender's e-mail address.
5. Click **Test Email** to make sure the e-mail feature works. In the **Test Email** dialog box, enter the recipient's e-mail address, and click **OK**. A test e-mail will be sent to the designated recipient.
6. Click **Apply** to save the e-mail settings, or click **Reset** to clear the settings.

## Device Communication

You can choose the device communication mode on the Device Communication page.

If **Devices are using static IP addresses (or reserved leasers)** is selected, the communication with devices is established by IP Address.

If **Device IP addresses are volatile and may change** is selected, the communication with devices is established by hostname or hostname.domain.

For DHCP, select **Device IP addresses are volatile and may change**.

**Note:** After the **Device Communication Mode** is changed, **KYOCERA Net Admin** will not work until after the next discovery. We strongly recommend changing **Device Communication Mode** only at a time when the network is not in use.

## Database

KYOCERA Net Admin database backup compresses files into a zip file and saves it to a folder called C:\KNetAdminBackup. The system administrator can schedule a single backup, immediate or recurring backups.

### Backing Up a Database

You can run a database backup from the **Administration** console.

1 In the navigation area, select **Preferences** > **Database backup**.

2 Select the time and interval for the backup:

**Manual**

Click **Create backup** to start the backup immediately.

**Single Backup in**

Select the interval in minutes or hours.

**Recurring**

Select **Monthly**, **Weekly**, or **Daily**, and select the **Day** and **Time**.

3 Click **Apply**.

### Restoring a Database

You can restore KYOCERA Net Admin information from a database backup. This restore uses a backup file (.ZIP) in the default backup location C:\KNetAdminBackup, or in another user-specified backup location.

1 In the **Administration** console, click **Preferences** > **Database restore**.

2 Select a backup file from the list, click the **Start Restore Process** icon, then click **OK**.

3 To restore a database from a previous KYOCERA Net Admin version or from a file located outside the default backup location, click the **Upload Backup File** icon.

4 Browse for a valid backup file (.ZIP), select it and click **Open** then click **OK**.

To change the name of a backup file, select it from the list, click the **Rename Backup File** icon, and type the new name.

To remove a backup file from the list, select it, or click **Select All** to include all the files in the list. Click **Delete Backup File**, and click **OK** to confirm.

To save a copy of a backup file, click **Download Backup File**, click **Save**, select a location, and click **Save**.

To change the location of the backup folder, click **Backup Folder Path**, type a new path, and click **OK**.

## 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**

**Upgrade firmware**

**User management**

The privilege to view, edit, and archive log files is determined by role. For example, the **Administrator** role can view, edit, and archive all log files, the **Help Desk** role can view and edit their own log files, and the **Read-only** role cannot view, edit, or archive log files.

## Creating a Log File

You can create log files for various KYOCERA Net Admin operations.

1. In the navigation area, select **Preferences** > **Log view**.
2. Click the **Create Log File** icon.
3. Type the **Operation Name**, or click **Select from list** and select from the list.
4. Type the **Device Serial Number**.
5. Type information about the task in **Log file content**.
6. Click **OK**.

The default location for log files is C:\Program Files\Kyocera\NetAdmin\Admin\log.

To view a log file, select it from the **Log view** list and click the **View Log File** icon.

To edit a log file created manually, select it from the **Log view** list and click the **Edit Log File** icon. A log file created automatically cannot be edited.

To delete a log file created manually, select it from the **Log view** list, click the **Delete Log File** icon, and then click **OK**. A log file created automatically cannot be deleted.

### Selecting Log File Storage

Log files are exported automatically to a default folder. Notification e-mails are sent to administrator users' e-mail addresses set up in **Mail Server**.

You can choose how long log files are stored on your system after they are created. Available options are 1 week, 1 month, and 3 months.

1. In the navigation area, select **Preferences** > **Log view**.
2. Click the **Log File Storage Settings** icon.
3. Select the desired time period in the **Storage period** list.
4. Accept the default file path, or type another path.
5. Click **OK**.

### Exporting a Log File Manually

You can export log files to an archive location in a .ZIP file.

1. In the navigation area, select **Preferences** > **Log view**.
2. Click the **Export Log File Manually** icon.
3. Save the exported log file to the desired location. The default log file name is: [date][time][kna-manually-archived-log].zip

## Scheduled Jobs

Some KYOCERA Net Admin tasks can be scheduled to run at selected intervals and appear in the **Scheduled Jobs** view. The supported tasks include:

**Network Discovery**

Set in the **Add Network** wizard in the **Preferences** list of the **Administration** console.

**Database Backup**

Set in the **Preferences** list of the **Administration** console.

**Multi-Set**

Set in the **Multi-Set** wizard in the **Device Manager** console.

**Upgrade firmware**

Set in the **Upgrade firmware** wizard in the **Device Manager** console.

**Device configuration**

Set in the **Device configuration** wizard in the **Groups** list of the **Device Manager** console.

To view scheduled jobs, in the navigation area, select **Preferences** > **Scheduled jobs**.

To change the name and schedule details of a scheduled job, select it and click **Edit Scheduled Job**.

To delete a scheduled job, select it and click **Delete Scheduled Job**.

To select all the scheduled jobs in the list, click **Select All**.

## Security

For greater security, you can set locking time for user login and select the server protocol setting.

**User locking time**

To prevent login by scripts, or when a wrong password is entered three times, login access is automatically locked. An administrator can set the time that login access remains locked, from 0 to 1440 minutes. The default time is 30 minutes. The default **admin** user cannot be locked.

When login access is locked, all administrator roles are notified by e-mail.

Login access is unlocked after the default lock time passes, or when the **KYOCERA Net Admin** server is restarted. A user with **Login users** / **Full Control** privilege can unlock access in **User Properties**.

**Session timeout**

An administrator can set the time of inactivity before a user is logged off automatically, from 10 to 120 minutes. The default time is 30 minutes.

**Protocol Settings**

The port numbers that appear in the installation wizard are default values. You can only change the values during installation. The port number range is 1 to 65535 and appears in the URL of the application in your browser. You can choose the server protocol setting.

**HTTP**

Faster than HTTPS. The HTTP port number is 7478 (default).

**HTTPS**

More secure than HTTP. The HTTPS port number is 7443 (default).

**Note:** When using HTTPS, the KYOCERA Net Admin server name must not be longer than 15 characters.

Click **Apply** to apply the settings, or **Reset** to return to default settings. Settings are applied the next time the application is started.

# 3 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.

## Manage Groups

You can create groups of devices so that you can view and modify them together. Once a group is created, you can revise group settings, delete a group, or convert a dynamic group to a manual group. **Groups** is located in the navigation area toolbar. These additional features are available:

**Upgrade firmware**

A guided method for installing the most current firmware on devices.

**Send data**

Sends files, text or device commands directly to one or more selected devices.

**Multi-Set**

Facilitates the sending of configuration parameters to multiple devices.

**Device configuration**

Manages device configuration policies for periodically updating the settings of multiple devices.

### Add Group

Use **Add group** to add a manual or dynamic device group to the **Device Manager** console. You must add devices to a manual group whereas a dynamic group adds devices automatically. **Add group** is located in the navigation area under **Groups**.

A dynamic group cannot have a manual group as a child.

### Dynamic Groups

A dynamic group is a device group established by user-defined device filters which select and add relevant devices to the dynamic group. Subscriptions can be inherited and can be created for groups. Child groups inherit subscriptions from parent groups. Inheritance is only available for dynamic groups, and not for manual groups.

#### Device Filters

Device filters determine the characteristics of a dynamic group. Setting device filters in the **Add Dynamic Group** dialog box lets you include only those devices that match a particular set of criteria. You can collapse or expand a device filter group at any time by clicking the icon to the right of the group heading.

### Adding a Dynamic Group

You can create a dynamic group.

1. Select a group in the navigation area. This is the parent group to the new group.
2. In the navigation area toolbar, click **Groups** > **Add group**.
3. In the **Add group** dialog box, select **Create a dynamic group**, and then click **OK**.
4. In the **Add Dynamic Group** dialog box, name the new group in the **Group Name** text box.
5. Define the device filters, and then click **OK**.

**Note:** A dynamic group applies its device filters to the member devices of its parent group. Only member devices of the parent group can be included in the new group.

You cannot drag devices to a dynamic group. To add a device to a dynamic group, change the device filters from the **Edit group** dialog box.

### Editing a Dynamic Group

You can edit dynamic groups.

1. In the navigation area, select the group you want to edit.
2. Click **Groups** > **Edit group**.
3. In the **Edit group** dialog box, edit the **Group Name** and **Device Filters**. You can use syntax to filter devices. Click **syntax examples** to see examples of operators and syntax.
4. Click **OK**.

### Converting a Dynamic Group

You can convert a dynamic group to a manual group. After conversion, you can drag and drop devices into the group or manually remove devices.

1. In the navigation area, select the dynamic group you want to convert.
2. In the navigation area toolbar, click **Groups** > **Convert group**, and then click **OK** to finish the conversion.

## Manual Groups

A manual group requires devices be added by drag and drop. It does not support device filters. Devices must be manually deleted. To add multiple devices, hold down the Ctrl key and select devices.

### Adding a Manual Group

You can create a manual group.

1. Select a group in the navigation area. This is the parent group to the new group.
2. In the navigation area toolbar, click **Groups** > **Add group**.
3. In the **Add group** dialog box, select **Create a manual group**, and then click **OK**.
4. In the **Manual Group** dialog box, name the new group in the **Group Name** text box, and then click **OK**.
5. Drag the devices you would like to include from the parent **List view** to the target group node in the navigation area.

**Note:** Dragging a device from one group to another does not remove that device from its original group.

### Editing a Manual Group

You can edit the group name for a manual group.

1. In the navigation area, select the group you want to edit.
2. Click **Groups** > **Edit group**.
3. In the **Edit group** dialog box, edit the group name and then click **OK**.

## Automatic Device Configuration

If you want to update settings to a large number of devices periodically, you may not want to configure the settings every time. To facilitate Multi-Set configuration on many devices, use the Automatic Device Configuration feature.

Automatic Device Configuration is available to the KYOCERA Net Admin user who has the **Device Manager** > **Devices** > **Device properties** > **Full Control, Multi-Set** privilege. By default, the **Full Control Multi-Set** privilege is selected for administrators, assistant administrators and help desk roles.

A device configuration policy consists of Multi-Set template file (ZIP or XML) to specify contents of device configuration, and a run schedule. You can select a manual group or a dynamic group, but the created policy for one group cannot be used for another group. As such, a policy for a parent group cannot be inherited by a subgroup. You can add, edit, or delete a Device Configuration policy. Target settings can be any of the settings supported by Multi-Set.

**Note:** Before configuration, the login and password of the target device should be set in the **Device Properties** dialog box in the **Communication** tab.

### Adding a Device Configuration Policy

1. In the navigation area, select a group of devices (**All Devices** is the default).

2 Click **Groups**, then click **Device configuration** to open the device configuration policy wizard.

3 To add a policy, in the policy list page click **Add**.

4 In the **Add template** page, click one option to select a template from the KYOCERA Net Admin server or from your local client. Browse to the location of the template.

5 Click **Next**.

6 In the next page select one option for when the Multi-Set should be performed. The options are:

**When device is added to group**

The Multi-Set job executes after the target device is added to the manual or dynamic group.

**One time**

Specify the **Time**, **Day**, **Month**, and **Year**. After the one time Multi-Set job is run, that policy and schedule is deleted.

**Recurring**

Specify the occurrence, **Monthly**, **Weekly**, or **Daily** and the respective time parameters.

7 In the next page, type the device configuration policy name. The maximum length is 128 characters. If you want to overwrite the settings on the target devices, select that check box. The **Overwrite settings** option appears only if the selected template file contains **Device Document Box**, **Device Address Book**, **Device User List**, or **Device Network Groups** settings.

8 In the **Confirmation** page, review your settings and then click **Save**.

9 After Multi-Set completes, an automatic device configuration log file is created in the C:\Program Files\Kyocera\NetAdmin\Admin\log\DeviceConfiguration folder. Each log will contain detailed information about the Multi-Set process for each target device.

To delete a device configuration policy, select it in the policy list wizard page and click **Delete**. Click **OK** in the confirmation message.

### Editing a Device Configuration Policy

1 In the navigation area, select a group of devices (**All Devices** is the default).

2 Click **Groups**, then click **Device configuration** to open the device configuration policy wizard.

3 To edit a policy, in the policy list page select a policy and click **Edit**.

4 In the **Replace template** page, to replace the template for the selected policy, select the check box.

5 Click one option to select a template from the KYOCERA Net Admin server or from your local client. Browse to the location of the template.

6 Click **Next**.

7 In the next page select one option for when the Multi-Set should be performed. The options are:

**When device is added to group**

The Multi-set job executes after the target device is added to the manual or dynamic group.

**One time**

Specify the **Time**, **Day**, **Month**, and **Year**. After the one time Multi-Set job is run, that policy and schedule is deleted.

**Recurring**

Specify the occurrence, **Monthly**, **Weekly**, or **Daily** and the respective time parameters.

8 In the next page, type the device configuration policy name. The maximum length is 128 characters. If you want to overwrite the settings on the target devices, select that check box. The **Overwrite settings** option appears only if the selected template file contains **Device Document Box**, **Device Address Book**, **Device User List**, or **Device Network Groups** settings.

9 In the **Confirmation** page, review your settings and then click **Save**.

10 After Multi-Set completes, an automatic device configuration log file is created in the C:\Program Files\Kyocera\NetAdmin\Admin\log\DeviceConfiguration folder. Each log will contain detailed information about the Multi-Set process for each target device.

## 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 view** tabs.

### Polling Defaults

The administrator can set default times for each polling option. You can apply the default settings to newly discovered devices. Devices discovered before will

not be changed to the new default times. Port 161 is used to request polling data.

### Setting Polling Defaults

The administrator can set default times for each polling option. The default settings are applied to newly-discovered printing devices.

1. In **Device Manager**, click **Preferences** > **Polling defaults**.
2. Under **Enable Default**, select the polling type you want to set. **Status Polling**, **Counter Polling**, and **Toner Level Polling** are selected by default.
3. Under **Default Interval**, enter the default time within the range displayed under **Minimum Range** and **Maximum Range**.
4. You can click **Reset** to display default settings.
5. Click **Apply** to save your changes.

## Alert Configuration

KYOCERA Net Admin polls supported devices for status information that can be sent by e-mail as alerts. Alert settings can be configured and customized.

### Creating a Custom Alert

Custom alerts can be set to notify you when the status of a device has changed.

1. In **Device Manager**, click **Preferences** > **Alert configuration**.
2. In the **Custom Alert Sets** list under **Modify**, select a name for the alert (**Custom 1** through **Custom 4**).
3. You can rename the custom list by clicking the **Rename Alert Set** icon in the toolbar and typing a new name.
4. Select items in the **Available Alerts** list and use the arrows to move them to the **Selected Alerts** list.
5. Click **Apply**.

### Special Settings

With **Special Settings**, you can create alerts for maintenance based on page count and for disconnected devices. For maintenance alerts, set the intervals for **Minor**, **Medium**, and **Major** for page count levels. Intervals are based on the number of pages printed.

You can set days and times for alerts to be sent, or select **24 hours per day, 7 days per week**. Selecting **Apply to all other alerts** applies this setting to all alerts.

You can prevent the same alert from being sent multiple times. Select **Enable suppressing repetitive alert**, select the number of days and hours, and click **Apply**.

### Alert Details

**Alert Details** helps you identify the device properties that will be reported in alert e-mails. The KYOCERA Net Admin server generates the alert using the top four selected device properties as the e-mail subject line. The **Selected Properties** list can be set in order using the up and down arrows. The device properties are transferred between the lists with the left and right arrows.

### Toner Level Alerts

You can set alerts for custom toner levels to a maximum of 10. In the **Toner level (%)** box, type a number from 1 to 100 and then click **Add New**. The custom toner level is added to the **Available Alerts** list in the **Custom Alert Sets** tab. It can be included in a custom alert set.

To change a custom toner level, select it in the **Saved Toner Level Alerts** list, type a different number, click **Update**, then click **OK** to confirm. To remove a custom toner level from the list, select it, click **Delete**, and then click **OK** to confirm.

## Custom Properties

The administrator can select custom device properties to appear in the **Properties** dialog box. When custom properties are included, they appear as a separate group under the **Device Settings** tab. **Custom properties** supports select properties for connected Kyocera devices only.

### Setting Custom Properties

You can assign custom properties to devices.

1. In **Device Manager**, click **Preferences** > **Custom properties**.
2. Use the arrows to move properties from **Available Properties** to **Selected Properties**.

   You can click **Reset** to go back to the original data that was in the dialog when you first opened it.
3. Click **Apply**.

### Removing Custom Properties

You can remove a custom property from **Device Manager**.

1. In **Device Manager**, click **Preferences** > **Custom properties**.
2. Select the property you want to remove from **Selected Properties**.
3. Click the left arrow to move the selected properties to the **Available Properties** list.

   You can click **Reset** to go back to the original data that was in the dialog when you first opened it.
4. Click **Apply**.

# List View

To display printing devices in a list, use **List view**. Named tabs display properties in ordered columns. You can add, modify, and delete tabs. Changes to the default **List view** can be made by a user with the full control privilege.

The **Manage tabs** menu contains the following choices:

**Add tab**

Add a tab or import a system default tab.

**Edit tab**

Edit an existing tab. You change the tab name, position, or columns to be included.

**Delete tab**

Remove a tab.

**Set rows per page**

Set the number of rows of devices per page.

## User Preferences

The first time you log in, the administrator-defined default tabs are automatically displayed. For all subsequent logins, **List View** uses your saved tabs and settings. When a guest user logs on, the default list views are displayed. Guest users cannot edit the default views.

## Global Characteristics

The following characteristics of **List view** apply to all device groups and are not saved on an individual group basis:

tab names

tab order

tab columns

order of tab columns

column sizing

rows per page

**List view** maintains the settings on the last viewed tab for each available device group. This is done to minimize the amount of user preference data transferred during login. **List view** preferences are saved for all users except guest users.

## Saving Changes

KYOCERA Net Admin automatically saves changes made outside the **Add Tab** and **Edit Tab** dialog boxes (column widths, column order, tab order, and rows per page). The settings are saved on the last viewed tab for each device group. Guest users can make changes during a session, but the default list view preferences will be displayed the next time any guest user logs on.

## Scrolling and Resizing the Window

If there are too many devices in the list to fit in the current view, the device rows are divided into "pages." Use the left and right arrows to navigate between pages of devices.

You can change the number of tabs displayed on each page by changing the size of the viewing area. You can change the size of the view in one of two ways:

Drag the divider between the navigation area and the right pane to the left or to the right.

Resize the window.

If you change the size of the viewing area, the currently-selected tab remains selected, but its position on the screen may change.

## Set Rows per Page

This selection lets you set the number of rows of displayed devices on each page. Guest users can change the selection in **Set Rows per Page**, but the new setting is not saved for the next session.

### Setting Rows per Page

You can set the number of rows that you can view per page.

1. From the **Manage tabs** list on the toolbar, select **Set rows per page**.
2. In the **Rows per Page** list box, select a number.
3. Click **OK**.

## Edit Default List Views

The **Edit Default List View Mode** check box lets administrators view and edit the default **List View** tabs. The default tabs in **List View** are displayed for the first time when you log in or use a guest account, or when you select **Reset all tabs to system defaults** in the **Edit Tab** dialog box.

Users with the **Full Control, Default List Views** privilege can modify the default tabs.

**Note:** Once a user has logged on for the first time, changes to the default list views do not affect that user's saved preferences. If that user chooses to reset all tabs to system defaults, **List View** displays the new default tabs.

### Editing Default List View Tabs

You can edit default **List view** tabs.

1. In the navigation area, select **Preferences** > **Edit default list views**.
2. Select the **Edit Default List View Mode** check box, and then click **Apply**.
3. In the navigation area, select **All Devices**.
4. Make changes to the default **List view** tabs.
5. In the navigation area, select **Preferences** > **Edit default list views**.
6. Clear the **Edit Default List View Mode** check box, and then click **Apply** to end this mode.

## Add Tab

In the **Add Tab** dialog box, you can create a new tab, or import and edit one of the system default tabs. There is a maximum of 32 tabs.

### Creating a Tab

You can create a new tab.

1. Select **Add tab** from the **Manage tabs** list on the toolbar.
2. In the **Add Tab** dialog box, select the **Tab Name** text box and type a name for your tab. Do not use invisible Unicode or extended ASCII characters.
3. Click the up and down arrows to the right of the **Tab Position** table to position the new tab.
4. Under **Available Columns**, select the items you want to include in the tab and click the right arrow.
5. To remove a column from the tab, select it under **Selected Columns**, and click the left arrow.
6. Click the up and down arrows to the right of **Selected Columns** to change the order of the columns in your tab.
7. Click **OK** or **Apply** to add the tab.

## Import Default Tab

Each user has a personal list of tabs and tab properties that are not affected by changes to the default list view. If an administrator creates a new tab in the default list view mode, it will become immediately available to all new users. However, existing users must import the new tab.

### Importing a Default Tab

You can import a system default tab.

1. Select **Add tab** from the **Manage tabs** list on the toolbar.
2. In the **Add Tab** dialog box, click **Import**.
3. Select one of the default tabs from the list.
4. Click **OK** to return to the **Add Tab** dialog box. You can edit the name, position, and contents of the imported tab.
5. Click **OK** or **Apply**.

## Edit Tab

You can rename, position or delete tabs, and select column content and order using the selections in **Manage tabs** > **Edit tab**.

### Renaming a Tab

You can rename a tab.

1. Select the tab you want to edit in the **List view** pane.
2. From the **Manage tabs** list on the toolbar, select **Edit tab**.
3. In the **Edit Tab** dialog box, type the new name in the **Tab Name** text box.
4. Click **OK**.

### Changing the Tab Order

You can change the tab order.

1. Select a tab you want to reposition.
2. From the **Manage tabs** list on the toolbar, select **Edit tab**.
3. Under **Tab Position**, use the up and down arrows to reorder the tabs.
4. Click **OK**.

### Changing the Column Content and Order

You can change the content and the order of a column.

1. Select the tab you want to edit in the **List view** pane.
2. From the **Manage tabs** list on the toolbar, select **Edit tab**.
3. To add a column in **Edit List View Tab**, highlight your selection under **Available Columns**, and then click the right arrow button, or double-click an item to move it to the other column.
4. To remove a column from the tab, highlight it under **Selected Columns**, and then click the left arrow button, or double-click an item to move it to the other column.
5. To change the position of the column, highlight it from **Selected Columns**. and then use the up and down arrows to move the column to another position.
6. Click **OK**.

### Resetting System Defaults

You can remove all tab customizations and revert back to the system default tabs.

1. From the **Manage tabs** list on the toolbar, select **Edit tab**.

2 In the **Edit Tab** dialog box, select the **Reset all tabs to system defaults** check box.

3 Click **OK**.

### Deleting a Tab

You can delete a tab, but you cannot delete the final tab. At least one tab should remain.

1 Select the tab you want to remove.

2 From the **Manage tabs** list on the toolbar, select **Delete tab**.

3 Click **OK** to confirm.

## Map View

Use **Map View** to display printing devices on a background map of your office. Printing device properties can be viewed and managed from this view. The use of an office map helps you to visualize the location of devices throughout an office. **Map View** is unavailable for groups with more than 250 printing devices. For Internet Explorer 7 and earlier, we recommend adding no more than 100 devices per map.

In the **Device Manager** console, click **Views** and then select **Map view**. If the selected group contains fewer than 250 devices, the initial view displays all the devices in that group as icons against a white background.

### Map View Toolbar

With the **Map View** toolbar, you can view and make changes to the **Map View**.

The following toolbar features are available:

**Views**

Select from the list to move between **List view**, **Map View**, or **View subscriptions**.

**Background options**

The **Background options** list contains the following options:

**Add/replace background**

Add a map background or change the current one.

**Remove background**

Removes the current map background and returns **Map View** to the default white background.

**Save map**

Saves the device positions on the current map background.

**Create link**

Creates a link between printing devices on the map. Linked devices are represented by a single link icon.

**Remove link**

Removes a link.

**Display settings**

Sets icon sizes and label properties.

**Map background size**

Sets the size of the map background image.

**Add device**

Adds a new device to the database.

**Remove device**

Removes selected devices from a manual group.

**Refresh**

Click to renew the **Map View** information from the network.

**Select All**

Click to select all the devices in the **Map View**.

## Map Background

With **Background options**, you can import an image of your office layout to display in **Map view**. The following image formats can be used: .JPG, .BMP, .PNG, or .GIF. A different image can be used for each group of printing devices, or groups can share an image.

### Adding or Replacing a Map Background

You can add or replace a map background.

1. Click the **Background options** icon, and then select **Add/replace background**.

2. In the **Add/replace background** dialog box, select an option for finding an image. **Select image from server** provides a list of previously selected images. With **Select local image (and copy to server)** you can browse for a new image file.

3. Click **OK**.

**Note:** The image initially appears in **Auto Fit** size. You can resize the image by selecting a percentage from the map background size list.

### Removing a Map Background

You can remove the current background image from the currently selected group in **Map view**.

1. Click **Background options** in the **Map view** toolbar.

2. Select **Remove background**.

3. Click **OK**.

Removing the image does not delete it from the server or remove printing device icons from **Map View**.

### Changing the Size of the Map Background Image

You can select from the following choices to change the map background image size:

Select a size percentage from the list, from 33% to 250%.

Select **Auto Fit** to display the entire image within the map viewer. Printing device icons that are still in the icon waiting area may cover part of the image.

If the image is distorted after changing its size, you can edit the image outside of the application and add it again (**Background options** > **Add/replace background**). You can also resize the map viewer by dragging the divider between the map viewer and the navigation area.

### Printing Device Icons in the Map Background

When a background image is imported into **Map view**, the printing device icons appear in a waiting area on the bottom or right of the **Map view**, depending on the shape of the map image. You can move an icon onto the map by dragging it to the appropriate office location.

Once you move an icon onto the map, it cannot be returned to the waiting area unless you replace the map background. When all icons have been moved onto the map, the waiting area is automatically removed.

At any time, you can change the position of a printing device icon in the **Map view**, by dragging it to the new position. If two groups share a background image, changing an icon position in one group will also reposition the image in the other group.

## Device Icon Properties

You can choose the appearance of device icons in **Map view**. The following properties can be selected:

**Icon size**

The icon size is displayed in **Map view**. It changes automatically as the background image view size changes.

**Icon Label**

Descriptive text below the icon.

**Pop-up Properties**

Descriptive text when the mouse pointer hovers over a device icon.

### Selecting Icon Properties

You can change the properties of device icons.

1. On the **Map view** toolbar, click **Display settings**.

2. In the **Icon size** list, select the desired size, from **Tiny** to **Huge**.

3. Under **Icon Label**, in the **Available** list select up to three items and click the right arrow button to add them to the **Selected** list. Use the up and down arrow buttons to change the list order.

4 Under **Pop-up Properties**, in the **Available** list select up to four items and click the right arrow button to add them to the **Selected** list. Use the up and down arrow buttons to change the list order.

**Note:** The **Hide icons for all linked group devices** option is used with links, a feature that lets you view printing devices by groups.

## Hide or View Waiting Area Icons

You can hide any unused icons that are in the waiting area. This can make the background image easier to see.

To hide waiting area icons, click the arrow button in the corner of the waiting area.

To view waiting area icons, click the arrow button again.

## Links

You can create links between selected printing devices, to view them by groups. This is useful for managing a large number of printers. You can create links with the parent group and its subgroup in **Map view**. For example, you can link all printing devices in a department, or link all color models. A printing device can be in more than one group. Once a link is created, the linked group icon represents all printing devices in the group. To make this option available, select **All Devices** or a parent group in the navigation area.

### Creating a Link

You can create a link between groups of printing devices.

1 In the navigation area, create one or more custom groups of printing devices.

2 In the navigation area, select **All Devices** or a parent group.

3 In **Map view**, click **Create link**.

4 In the **Create link** dialog box, select a group from the **Linked group** list.

5 Accept the default **Link name**, or type your choice of name. Click **OK**.

The linked group icon appears in the icon waiting area, before any printing device icons. You can drag the linked group icon into the office map.

### Hiding Icons for Linked Group Devices

After creating a linked group of printing devices, you can hide their individual icons.

1 In the **Map view** toolbar, click the **Display settings** icon.

2 Select **Hide icons for all linked group devices**.

You can clear the **Hide icons for all linked group devices** check box to restore all printing device icons.

### Removing a Link

You can remove a link in **Map view**. This action does not remove the printing devices in the group. Removing a linked group does not affect child groups.

1. In the **Map view**, select the linked group icon.

2. Click **Remove link**, then click **OK**.

   The linked group is removed from the map. If **Hide icons for all linked group devices** is selected in the **Display settings** dialog box, the group's individual printing device icons appear at their previous location in the map.

### Saving Map Settings

After changing **Map view** settings, click **Save map** to save the changes.

**Note:** If multiple users make simultaneous changes to a group's **Map view** settings, the last user's changes override all previously saved changes.

## Subscriptions

Printing devices are polled for information, and e-mail alerts can be sent out based on this status information. You can also generate reports, and users can subscribe to receive these reports on a regular schedule.

For example, a user can be notified when toner or paper is low in a particular device.

Alert e-mails can be sent to any user. In addition to **Administrators** and **Help Desk** users, **Subscribers** can be added even if they do not have access to KYOCERA Net Admin. These subscribers can receive e-mail alerts.

Reports are created in the **Device Manager** console. Subscriptions to reports can be created in the **Administration** or **Device Manager** console.

Alerts can be created for all the different types of users. Login users can log on and edit settings. **Subscribers** cannot log on and can only receive alerts and reports from devices.

**Note:** If pop-up blockers are enabled in your browser, **Add Alert Subscription**, **Add Report Subscription**, **Manage Reports**, the **About** page, and **Help** will not open.

### Adding an Alert Subscription

You can manage alert subscriptions.

1. Select the **View subscriptions** icon in the toolbar.

2. Click the **Add alert subscription** icon.

3. In the **Create Alert Subscription** dialog box, under **Recipients**, select a user or users who will receive the alert.

4. Under **Alert Sets**, select the user status alerts.

5 Under **Reply to**, type the e-mail address of the user who will respond to an alert e-mail. The e-mail will automatically be addressed to the same address. Multiple addresses can be entered when separated by semi-colons.

6 Click **OK**.

To make changes to the subscription, select it and click the **Edit subscription** icon.

To delete a subscription, select it and click the **Delete subscription** icon.

### Adding a Report Subscription

You can add a report subscription.

1 Select the **View subscriptions** icon in the toolbar.

2 Click the **Add report subscription** icon.

3 In the **Create Report Subscription** dialog box, under **Recipients**, select a user or users who will receive the report.

4 Under **Report Templates**, select from the reports list.

5 Select the file format for the report: PDF, HTML, XML, and CSV. File format options are limited for some reports.

6 Under **Schedule**, select an interval for receiving the subscription e-mail: **Daily**, **Weekly**, **Monthly**, **Quarterly**, or **Yearly**.

7 Click **OK**.

To make changes to the subscription, select it and click the **Edit subscription** icon.

To delete a subscription, select it and click the **Delete subscription** icon.

## Adding Devices

A device can be added manually if is not automatically discovered. This is useful if a device is located on a remote network that is not set up for automatic discovery.

1 In the navigation area, select a group of devices (**All Devices** is the default).

2 In **List view** or **Map view**, click **Add device**.

3 In the **Add Devices** dialog box, select a network from the list. You can change the **Read community name**.

4 Select a method to add selected targets:

You can type the IP address or host name of the device, and click **Add**.

You can specify a range of IP addresses by typing starting and ending IP addresses, and click **Add**.

You can paste IP addresses or host names from your clipboard by clicking **Paste**.

You can add IP addresses or host names from a TXT or CSV file. Click **Import**, and then click **Browse** to select a valid file with a .TXT or .CSV extension.

You can click **Remove** to delete any devices in your **Selected targets** list.

5 Click **OK** to submit the **Selected targets** list. The **Add Devices Result** dialog box appears with a status of all the devices submitted. A **Details** link refers you to the IP address or host name for each device submitted.

6 Click **Close**.

## Refresh

Printing device information, such as counters and toner levels, 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.

## Select All

Click **Select all** to select all displayed printing devices. **Select all** selects the devices currently displayed. Moving to another page to view additional devices will clear your current selection. This feature is available in **List view** and **Map view**.

## Device Properties

With **Device properties**, you can display the properties of printing devices. Some properties are fixed, while others can be managed by the software.

Some properties can be changed depending on your privilege level. Privileges are set in the **Administration** console.

### Displaying Device Properties

1 In the navigation area, select a group of devices (**All Devices** is the default).

2 In **List View** or **Map view**, select one or more printing devices.

3 Click **Device properties**.

4 In the **Properties** or **Multiple Device Properties** dialog box, view or modify the available settings.

5 Click **OK** when you are finished.

## Device Properties for a Single Device

Device Properties options let you view and set the properties of printing devices. The **Properties** dialog box displays detailed information about the selected network device. Some models do not display all options.

**Model name and home page**

Displays the device display name and IP address. You can click the **Device home page** icon to open the home page of the device.

**Printing device image**

Displays a 3-D image of the printing device showing installed paper options or finishers. Some models display a generic image.

**Operation Panel**

Displays the status of the device.

**Refresh**

Updates the display for all device properties.

**Current Status**

Displays the printing device status for the following parameters:

**Managed**

Indicates whether the printing device is being managed by the application. When the device is not managed, **Status** is blank and **sysUpTime** is hidden.

**Status**

Displays the current status of the printing device, such as **Ready**, **Printing**, or **Sleeping**.

**sysUpTime**

Displays the length of time the printing device has been on, in the format: days, hours, minutes, seconds.

**Connection Type**

Displays how the device is connected.

**Last Connection**

For **Not Connected** devices, displays the date and time the device was disconnected.

**Supplies** tab

Displays the current level of consumable supplies.

**Device Settings** tab

Displays all available printing device properties. For some models, click **Detailed counters** at the end of the **Counters** list to additional view counters by function and paper size.

**Troubleshooting** tab

Displays device errors and troubleshooting advice.

**Monitoring** tab

Lets you set a polling schedule, configure SNMP traps to monitor a device, and clear the suppressing repetitive alerts.

**Communication** tab

A user with privileges can change Simple Network Management Protocol (SNMP) and Web Services Description Language (WSDL) settings for device communication.

### Device Properties for Multiple Devices

With **Multiple Device Properties**, you can view and set the properties of devices. Support varies by model.

**Options for Multiple Devices**

The **Multiple Device Properties** dialog box displays polling and communication settings that can be changed for all selected devices at once.

Select the **Manage these devices** check box to enable polling options. The check box changes depending on settings of the selected devices.

If selected, then all selected devices are managed.

If shaded, then some selected devices are managed and some are not.

If cleared, then none of the selected devices are managed.

**Polling**

With the check box selected for **Manage these devices**, select the desired polling options, and set the time in seconds, minutes, or hours.

**General**

The **General** section applies only to Kyocera devices.

**SNMP**

A user with privileges can change SNMP and WSDL settings for device communication.

**Secure Protocol**

The **Secure Protocol** section is available if at least one device supports SSL. Any changed settings will affect those devices.

**Login**

The **Login** section is available if at least one device supports Device Login. Any changed settings will affect those devices.

**Alerts**

**Clear Alerts** removes the suppression on all alerts that are currently being suppressed. Alert suppression values can be adjusted in **Preferences** > **Alert Configuration** > **Special Settings**.

## Open Device Home Page

Click **Device home page** to open software on the device. Detailed device and status information, panel settings and device controls are available in the device software.

To access a device home page on a remote network, open the **Administration** console and select **Preferences** > **Networks and agents**, highlight the remote network, click the **Network Properties** icon and select the **Agent** tab. In the Agent tab, select **Use proxy function to open Device Home Pages**.

Port 80 is used by default to access the home page through HTTP. Port 443 is used by default to access the home page through HTTPS.

## 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** button 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 Options

When **Custom mode** is selected, the following configuration options 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. These settings vary by 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. The availability of these settings depends upon the device.

### Creating Settings in Quick Mode

You can copy all default settings automatically.

1 In the navigation area, select a group of devices (**All Devices** is the default).

2 In **List view** or **Map view**, select one or more devices to receive settings.

3 In the toolbar, click the **Multi-Set** icon, and select **Multi-Set**.

4 On the **Multi-Set Mode** page, select **Quick mode**. Click **Next**.

5 On the **Device Group** page, select one or more groups to which settings will be applied. Click **Next**.

6 On the **Select Device** page, select one source device from the list. Click **Next**.

If authentication is required, enter a login and password.

7 On the **Confirmation** page, review your selections. Click **Back** to make any changes.

8 Click **Set Devices** to configure the selected devices.

If the device must be restarted to save the settings, a message appears. Click **Yes** to close.

**Note:** The system uses the communication settings you saved on the **Communication** tab of the **Device Properties** dialog box. If these settings do not match with those on a device, an authorization failure message is recorded for that device in the log file.

9 On the **Finished** page, click **Export log** to export a Multi-Set log file in .CSV format, or click **Quit** to finish the configuration.

### Creating Settings from a Source Device

You can copy selected settings from a source device.

1 In the navigation area, select a group of devices (**All Devices** is the default).

2 In **List view** or **Map view**, select one or more devices to receive settings.

3 In the toolbar, click the **Multi-Set** icon, and select **Multi-Set**.

4 On the **Multi-Set Mode** page, select **Custom mode**. Click **Next**.

5 On the **Device Group** page, select one or more groups to which settings will be applied. Click **Next**.

6 On the **Multi-Set Settings** page, select one or more settings from the list. Click **Next**.

7 On the **Multi-Set Source** page, select **Copy from source device**.

For some options, you can select **Overwrite settings on target devices**. When selected, settings from the source device replace settings on the target device.

Click **Next**.

8 On the **Select Device** page, select one source device from the list. Click **Next**.

If authentication is required, enter a login and password.

9 You can save the settings as a template on the server. In the message box click **OK**, name the template file, and then click **Save**.

Click **Cancel** if you do not want to save a template file.

10 On the **When should Multi-Set be performed** page, select a run time:

**Run now**

Multi-Set runs immediately.

**Schedule to run**

Type the time using hh:mm in a 24 hour format, and then select the **Day**, **Month**, and **Year**.

The run time can be edited or the Multi-Set cancelled in **Administration** > **Preferences** > **Scheduled jobs**.

Click **Next**.

11 On the **Confirmation** page, review your selections. Click **Back** to make any changes.

12 Click **Set Devices** to configure the selected devices.

If the device must be restarted to save the settings, a message appears. Click **Yes** to close.

**Note:** The system uses the communication settings you saved on the **Communication** tab of the **Device Properties** dialog box. If these settings do not match with those on a device, an authorization failure message is recorded for that device in the log file.

13 On the **Finished** page, click **Export log** to export a Multi-Set log file in .CSV format, or click **Quit** to finish the configuration.

### Creating Settings from a Multi-Set Template File

You can copy selected settings from a Multi-Set template file.

1 In the navigation area, select a group of devices (**All Devices** is the default).

2 In **List view** or **Map view**, select one or more devices to receive settings.

3 In the toolbar, click the **Multi-Set** icon, and select **Multi-Set**.

4 On the **Multi-Set Mode** page, select **Custom mode**. Click **Next**.

5 On the **Device Group** page, select one or more groups to which settings will be applied. Click **Next**.

6 On the **Multi-Set Settings** page, select one or more settings from the list. Click **Next**.

7 On the **Multi-Set Source** page, select **Copy from Multi-Set template file**.

For some options, you can select **Overwrite settings on target devices**. When selected, settings from the source device replace settings on the target device.

Click **Next**.

8 On the **Select template** page, select a template file:

**Select template from KYOCERA Net Admin server**

Click **Browse** and select a template file from the Net Admin server. Select an .XML template file for a single setting, or a .ZIP template file for multiple settings.

**Select template from your local client**

Click **Browse** and select a template file from your computer or network. Select an .XML template file for a single setting, or a .ZIP template file for multiple settings.

Click **Next**.

9 On the **When should Multi-Set be performed** page, select a run time:

**Run now**

Multi-Set runs immediately.

**Schedule to run**

Type the time using hh:mm in a 24 hour format, and then select the **Day**, **Month**, and **Year**.

The run time can be edited or the Multi-Set cancelled in **Administration** > **Preferences** > **Scheduled jobs**.

Click **Next**.

10 On the **Confirmation** page, review your selections. Click **Back** to make any changes.

11 Click **Set Devices** to configure the selected devices.

If the device must be restarted to save the settings, a message appears. Click **Yes** to close.

**Note:** The system uses the communication settings you saved on the **Communication** tab of the **Device Properties** dialog box. If these settings do not match with those on a device, an authorization failure message is recorded for that device in the log file.

12 On the **Finished** page, click **Export log** to export a Multi-Set log file in .CSV format, or click **Quit** to finish the configuration.

### Multi-Set Template Editor

With the **Multi-Set Template Editor** application, you can create or change the template files.

In the toolbar, click the **Multi-Set** icon, and select **Multi-Set Template Editor**.

**Download the Multi-Set Template Editor**

If the **Multi-Set Template Editor** is not installed, click to download and install the application.

**Launch the Multi-Set Template Editor**

After **Multi-Set Template Editor** is installed, click to open the application. ActiveX controls must be enabled.

To view help in **Multi-Set Template Editor**, click **Help** > **Multi-Set Template Editor Help**.

### Multi-Set Log File

The Multi-Set log file records Multi-Set events in the format: Date, Time, Result (including the reason for any update failure), IP Address, Model/Group Name, Property to set. The log file is located in C:\Program Files\Kyocera\NetAdmin\Admin\log\MultiSet.

## Restart Devices

With **Restart devices**, you can restart one or more printing devices or device networks remotely. Devices must be managed. Users with the **Full Control, Multi-Set** privilege can use this feature.

**Device restart**

Restarts the selected printing devices.

**Network restart**

Restarts the network interface for the selected printing devices.

### Restarting a Device or Network

You can restart devices or networks remotely.

1. In the navigation area, select a group of devices (**All Devices** is the default).
2. In **List view** or **Map view**, select one or more devices.
3. In the toolbar, click **Restart**.
4. Select the type of restart: **Device restart** or **Network restart**. Click **Next**.
5. On the **Confirmation** page, review your selections.
6. Click **Finish**.

   If authentication is required, enter a login and password.

7 On the **Finished** page, you can click **Export log** to export a separate log file for each restart process. The log files are located in C:\Program Files\Kyocera\NetAdmin\Admin\log\RestartDevices\

## Manage Applications

You can install applications on one or more devices by using the **Manage Applications** feature. You can also uninstall applications and activate and deactivate applications remotely. Available features vary by model.

Before you install, activate, deactivate, or uninstall an application, you must enable SSL and IPP over SSL on the device. For some models, enable enhanced WSD over SSL. You must also enter the correct login and password in the **Communication Settings** for the device.

Applications are created by dealers or third-party companies to enhance printing, copying, or accounting features.

You can import .CSV files provided by a dealer. You can also create .CSV files with columns of device serial number and license key.

### Installing an Application

You can install applications remotely on multiple printing devices using the **Manage Applications** wizard. Once an application is installed, you can choose to start the application immediately or to leave it inactive. If an application is no longer needed, you can uninstall it.

1 In the navigation area, select a group of devices (**All Devices** is the default).

2 In **List View** or **Map View**, select one or more devices.

3 In the view toolbar, click the **Manage applications** icon.

4 In the **Manage Applications** wizard, select **Install application**. You can select the check box to activate the application after installation. Click **Next**.

5 Click **Browse** to find a valid application package file (.PKG), and click **Open**. Click **Next**.

6 If the **Activate application after installation** check box was selected and the selected application requires a license key, the **Apply license keys** page appears. Select a method to choose license keys provided to you from your administrator:

**Activate without a license key**

Activate the application without a license key.

**Use the following license key**

Select a device, and then type the 20-digit license key, separated by a hyphen for each 4 digits.

**Import license keys**

Browse to find a valid license key file (.CSV), and click **Open**. If the .CSV format is incorrect, click **Yes** in the message box. In the **License Keys Mapping** dialog box, select mapping values for each property. If the first line

of the .CSV file contains headers, select **File has headers**. The first line of the file is ignored and only the data is used.

You can click **Export license keys** to save a license key as a .CSV file. Name and save the file.

Click **Next**.

7 On the **Confirmation** page, review your settings.

8 Click **Manage** to install the application.

A log file is created for each **Manage Applications** process.

## Activating an Installed Application

If an application was installed on one or more printing devices without starting the application, you can activate it using the **Manage Applications** wizard.

1 In the navigation area, select a group of devices (**All Devices** is the default).

2 In **List View** or **Map View**, select one or more devices.

3 In the view toolbar, click the **Manage applications** icon.

4 In the **Manage Applications** wizard, click **Activate application**. Click **Next**.

5 On the **Select Method** page, select how to choose the application:

**Specify application package**

Click **Next**, and continue to step 6.

**Specify application installed on the device**

Click **Next**, and continue to step 7.

6 On the **Select an installation package** page, browse to find a valid installation package file (.PKG). Click **Next**, and continue to step 9.

7 On the **Select source device** page, select one device. Click **Next**.

If authentication is required, enter a login and password.

8 On the **Select the application to be activated** page, select an application from the list. Click **Next**.

9 If the application requires a license key, the **Apply license keys** page appears. For each device, select a method to choose license keys:

**Activate without a license key**

Activate the application without a license key.

**Use the following license key**

Select a device, and then type the 20-digit license key, separated by a hyphen for each 4 digits.

**Import license keys**

Browse to find a valid license key file (.CSV), and click **Open**. If the .CSV format is incorrect, click **Yes** in the message box. In the **License Keys Mapping** dialog box, select mapping values for each property. If the first line of the .CSV file contains headers, select **File has headers**. The first line of the file is ignored and only the data is used.

You can click **Export license keys** to save a license key as a .CSV file. Name and save the file.

Click **Next**.

10 On the **Confirmation** page, review your settings.

11 Click **Manage** to activate the application.

A log file is created for each **Manage Applications** process.

## Deactivating an Installed Application

You can deactivate an installed application using the **Manage Applications** wizard.

1 In the navigation area, select a group of devices (**All Devices** is the default).

2 In **List View** or **Map View**, select one or more devices.

3 In the view toolbar, click the **Manage applications** icon.

4 In the **Manage Applications** wizard, click **Deactivate application**. Click **Next**.

5 On the **Select Method** page, select how to choose the application:

**Specify application package**

Click **Next**, and continue to step 6.

**Specify application installed on the device**

Click **Next**, and continue to step 7.

6 On the **Select an installation package** page, browse to find a valid installation package file (.PKG). Click **Next**, and continue to step 9.

7 On the **Select source device** page, select one device. Click **Next**.

If authentication is required, enter a login and password.

8 On the **Select the application to be deactivated** page, select an application from the list. Click **Next**.

9 On the **Confirmation** page, review your settings.

10 Click **Manage** to deactivate the application.

### Uninstalling an Installed Application

You can uninstall an application using the **Manage Applications** wizard.

1. In the navigation area, select a group of devices (**All Devices** is the default).
2. In **List View** or **Map View**, select one or more devices.
3. In the view toolbar, click the **Manage applications** icon.
4. In the **Manage Applications** wizard, click **Uninstall application**. Click **Next**.
5. On the **Select Method** page, select how to choose the application:

   **Specify application package**

   Click **Next**, and continue to step 6.

   **Specify application installed on the device**

   Click **Next**, and continue to step 7.
6. On the **Select an installation package** page, browse to find a valid installation package file (.PKG). Click **Next**, and continue to step 9.
7. On the **Select source device** page, select one device. Click **Next**.

   If authentication is required, enter a login and password.
8. On the **Select the application to be uninstalled** page, select an application from the list. Click **Next**.
9. On the **Confirmation** page, review your settings.
10. Click **Manage** to uninstall the application.

## Manage Optional Functions

You can activate optional functions on one or more remote devices by using the **Manage optional functions** feature. These functions are included in the device firmware. The administrator has the 20-digit license key needed for activation. You can also choose a temporary trial version of this feature.

For more information about these functions, see the *Operation Guide*.

Users with the **Full Control, Multi-Set** privilege can use this feature.

You can import a valid license key from a .CSV file or enter the license key directly. You can use .CSV files provided by a dealer, or you can create .CSV files with columns of device serial number and license key. A license key can also be exported and saved.

**Note:** If authentication is enabled on the device, the **Login User Name** and **Password** must be set correctly in **Device properties** > **Communication** > **Login**.

### Activating an Optional Function

You can activate an optional function using the **Manage optional functions** wizard.

1. In the navigation area, select a group of devices (**All Devices** is the default).
2. In **List view** or **Map view**, select one or more devices.
3. In the toolbar, click **Manage optional functions**.
4. On the **Optional function** page, select a function name. Click **Next**.
5. On the **Activate mode** page, select **Official** or **Trial**. Click **Next**.

   With **Official** selected, continue to step 6.

   With **Trial** selected, continue to step 7.

6. On the **License key** page, select devices to add a license key. Devices can use the same or different license keys.

   Click **Add license key**, enter a 20-digit license key, and click **OK**.

   Click **Import license keys**, and then select a valid license key file (.CSV). If the .CSV format is incorrect, click **Yes** in the message box. In the **License Keys Mapping** dialog box, select mapping values for each property. If the first line of the .CSV file contains headers, select **File has headers**. The first line of the file is ignored and only the data is used.

   You can click **Export license keys** to save the license key to a .CSV file. Name and save the file.

   Click **Next**.

7. On the **Confirmation** page, review your settings.
8. Click **Start**.

   A log file is created for each **Manage optional functions** process. The log files are located in C:\Program Files\Kyocera\NetAdmin\Admin\log\OptionalFunction.

## Certificate Setup

For some models, you can manage certificates on multiple printing devices at the same time rather than separately on each device. You can import, assign, and delete valid (not expired) certificate files that contain encrypted information for device authentication and communication. Up to five device certificates and five root certificates can be installed on each device. A user must have the **Full Control, Multi-Set** privilege to use this feature.

**Certificate Setup** is supported if all the following conditions are true for at least one device in the selected group:

The target device exists in the supported model list.

The target device is managed.

The target device is not connected by USB.

The target device is connected with the network interface.

Two types of certificates can be installed:

**Device certificate**

A file that identifies the printing device.

**Root certificate**

A file the device uses for secure communication. Some applications can also use a root certificate as a server certificate.

For a **Device certificate**, you must provide two files on a local client. One file must be a configured .CSV file with data for each certificate in the following order: device serial number, file name of certificate file, password. The .ZIP file should contain at least one certificate file from the files listed in the .CSV file.

## Importing a Certificate

1. In the navigation area, select a group of devices (**All Devices** is the default).

2. In **List View** or **Map View**, select one or more devices, then click the **Certificate Setup** icon in the toolbar.

3. In the **Select action** page, select **Import certificate**. Click **Next**.

4. In the **Select the certificate type** page, select either **Device certificate** or **Root certificate**. Click **Next**.

5. If **Device certificate** was selected, in the **Select a certificate file** page, browse for a .ZIP file with certificate files, then browse for the configured .CSV file. As an option, you can assign a device certificate to protocols. Select each relevant protocol from the **Available protocols** list and move it to the **Selected protocols** list. Click **Next**.

   If **Root certificate** was selected, browse for a certificate file on the local client. Click **Next**.

6. In the **Confirmation** page, you can examine your final settings before actual processing with the target devices begins. To accept the settings, click **Set up**. To make any changes, click **Back**.

7. A message appears to inform you that the device network will restart automatically after processing is finished. Click **OK**.

   The processing page shows you the status of certificate processing. Processing may take several minutes.

8. After processing is complete and without errors, the **Finish** page displays automatically. If errors occurred, the **Finish** page displays an error notification. See the log file for details.

   To exit **Certificate Setup**, click **Quit**.

## Deleting a Certificate

1. In the navigation area, select a group of devices (**All Devices** is the default).

2 In **List View** or **Map View**, select one or more devices, then click the **Certificate Setup** icon in the toolbar.

3 In the **Select action** page, select **Delete certificate**. Click **Next**.

4 In the **Select the certificate type** page, specify the type of certificate you want to delete from the target devices, **Device certificate** or **Root certificate**. Click **Next**.

5 In the **Select a certificate to delete** page, select one of two options, **Specify subject of the certificate** or **Select certificate file**.

6 If **Specify subject of the certificate** is selected, type the subject of the certificate as a distinguished name (DN). Click **Next**.

If **Select certificate file** is selected. browse to a certificate that has the same subject as the certificate to be removed. Type the certificate password if selected device certificate requires it. Click **Next**.

7 In the **Confirmation** page, you can examine your final settings before actual processing with the target devices begins. To accept the settings, click **Set up**. To make any changes, click **Back**.

8 A message appears to inform you that the device network will restart automatically after processing is finished. Click **OK**.

The processing page shows you the status of certificate processing. Processing may take several minutes.

9 After processing is complete and without errors, the **Finish** page displays automatically. If errors occurred, the **Finish** page displays an error notification. See the log file for details.

To exit **Certificate Setup**, click **Quit**.

## Assigning a Device Certificate to Protocols

Only a **Device certificate** can be assigned to protocols.

1 In the navigation area, select a group of devices (**All Devices** is the default).

2 In **List View** or **Map View**, select one or more devices, then click the **Certificate Setup** icon in the toolbar.

3 In the **Select action** page, select **Assign device certificate to protocols** Click **Next**.

4 In the **Select a device certificate to assign** page, select one of two options, **Specify subject of the certificate** or **Select certificate file**.

5 If **Specify subject of the certificate** is selected, type the subject of the certificate as a distinguished name (DN).

If **Select certificate file** is selected. browse to a certificate that has the same subject as the certificate to be assigned. Type the certificate password if the selected certificate requires it.

6 Select each relevant protocol from the **Available protocols** list and move it to the **Selected protocols** list. Click **Next**.

7 In the **Confirmation** page, you can examine your final settings before actual processing with the target devices begins. To accept the settings, click **Set up**. To make any changes, click **Back**.

8 A message appears to inform you that the device network will restart automatically after processing is finished. Click **OK**.

The processing page shows you the status of certificate processing. Processing may take several minutes.

9 After processing is complete and without errors, the **Finish** page displays automatically. If errors occurred, the **Finish** page displays an error notification. See the log file for details.

To exit **Certificate Setup**, click **Quit**.

### Certificate Setup Log File

Each **Certificate Setup** operation is recorded in a log file, which is stored in C:\Program Files\NetAdmin\Admin\log\CertificateSetup. The log file contains detailed information about the Certificate Setup process, each target device, and the process result. A summary at the end lists the total number of target devices selected and the number of target devices that were successfully set up.

## Firmware Upgrade

The **Firmware Upgrade** wizard provides a guided method for firmware installation, upgrades, and downgrades on devices over a TCP/IP network. The firmware file must match the target model, or at least one device in a group update. For the latest firmware files, consult your administrator or dealer.

The **Firmware Upgrade** wizard can be opened from the **Upgrade firmware** button on the toolbar and from the **Groups** menu in the navigation area.

**Note:** For models using the firmware master file format, place the upgrade files on the KYOCERA Net Admin server. The default location is C:\Program Files\Kyocera\NetAdmin\Admin\firmwares.

Before sending firmware files to a device, ensure the following:

The port number on the target device is set to 9100.

The RAW Port option on the device's operation panel is enabled. The device requests firmware files from KYOCERA Net Admin server port that was specified during installation. The port number range is 1 to 65535. To verify the port number used, check the URL of the application in your browser.

The target device has a network interface card installed.

Port 21 is selected for sending firmware files to an IB-21 network card.

The Firmware Upgrade wizard initiates the upgrade on the client. Once you complete the upgrade instructions, the server controls the process. During a

firmware upgrade, the device icon and status change in **List view** and **Map view**.

If the firmware file version is older than the installed version, then the application downgrades the firmware.

## Risks and Recovery Options

Using the **Firmware Upgrade** wizard carries potential risks. As part of the upgrade, you must acknowledge, understand, and accept the potential risk of performing a firmware upgrade. When preparing a firmware upgrade, review the process with your dealer or service organization and establish contingency plans.

**Warning:** If a device is turned off or loses power at a critical point during the upgrade, the device could become inoperable and require servicing to replace damaged components.

Risks and recovery options can differ depending on the type of upgrade.

**Danger Period During Upgrade**

**Any Device**

Do not turn off the device while the firmware upgrade is being performed. During the firmware upgrade, the **Status** in **List view** or **Map view** shows the device is **Upgrading**. A status indicator, such as **Upgrading**, **Erasing**, or **Writing**, appears on the device's operation panel. Processing times will vary.

**IB-2x**

No indication of the upgrade appears on the device operation panel. Check for the new firmware version in **List view** or **Map view**.

**Upgrade Completion Indicators**

Use any of the following methods to check completion for any device:

Check the log file in **Preferences** > **Log view** in the **Administration** console.

Check the firmware version in **List view** or **Map view**.

Open the device's **Properties** page, and then view the firmware version in the **Device Settings** tab.

For **System** or **FAX**, the device's operation panel displays the new version number, or **Completed**.

**Upgrade Error Indicators**

**Any Device**

The result of the device upgrade is recorded in the log file as **Failed**.

**System**

The device fails the power-on self-test.

**FAX**

Faxing does not operate.

**IB-2x**

No link light appears. **Option** (for some models: **Network**) does not appear on the **Interface** menu on the operation panel.

**Upgrade Error Recovery**

**System**

You must replace the DIMM in the device. The old DIMM, however, is not physically damaged. You can erase and reload it using a DIMM writer.

**FAX**

You must replace the FAX board.

**IB-2x**

A special recovery mode for the IB-2x called Boot Loader mode is available. You can use a jumper setting to set IB-2x to Boot Loader mode: SW1 on IB-20/21 and IB-21E, or J2-1 on IB-22. Once in Boot Loader mode, you can use a Windows utility named IBVERUP to load a new firmware file.

## Upgrading the Firmware

If the firmware file version is older than the installed version, then the application downgrades the firmware. Though you can upgrade any number of devices, the maximum number depends on CPU and memory installed on the server.

1. In the navigation area, select a group of devices (**All Devices** is the default).

2. In **List view** or **Map view**, select one or more devices:

   To upgrade any number of similar devices, select the devices in the right pane.

   To upgrade a group of similar devices, select the group in the navigation area.

3. Depending on the selection in step 1:

   For devices selected in the right pane, click **Upgrade firmware** in the toolbar.

   For a group selected in the navigation area, select **Groups** > **Upgrade firmware**.

4. On the **Use With Caution** page, select the check box to acknowledge and accept the risks. Click **Next**.

5. On the **Select Firmware File** page, select a file:

   With **Select file from KYOCERA Net Admin Server** selected, click **Browse** to find the firmware file located on the KYOCERA Net Admin server.

   With **Select file from local client** selected, click **Browse** to find the file on your local system or network.

   With **Type the absolute URL of the firmware file** selected, type the path for the firmware file.

   Click **Next**.

   **Note:** For the latest firmware files, consult your administrator or dealer.

6. The **Retain Firmware File** page appears if you selected a URL or local client on the **Select Firmware File** page, and at least one device requires an upgrade. Select **Yes** to save the selected firmware file on the server for future use. Click **Next**.

7. On the **Confirm Selected Firmware** page:

Review the model and firmware information.

If **Proceed with firmware downgrade** appears, select the check box to downgrade the device to an older version.

Click **Next**.

8 On the **Set Communication Options** page, select the number of simultaneous upgrades, the port number, and retry options.

The port number value should match the port number specified in the device home page.

**Note:** For the logical printer used in the firmware upgrade, leave the **Start of Job String** empty in the device settings. For some models, you must disable **Banner Page** for the logical printer.

9 On the **When should Firmware Upgrade be performed** page, set an upgrade schedule:

Select **Run now** to upgrade the firmware immediately when you click **Upgrade**.

Select **Schedule to run** and set a time and date to upgrade the firmware.

10 On the **Confirm Upgrade Settings** page, review selected settings. The settings vary based on the model and the number of devices selected.

11 On the **Begin Upgrade** page, click **Upgrade**. You can click **Cancel** to abort any upgrade that has not yet started. This does not stop upgrades that are currently processing.

12 When upgrades are finished, you can view the log file in **Preferences** > **Log view** in the **Administration** console.

## Send Data

With **Send Data**, you can send files, text or device commands directly to one or more selected devices. It can be done by TCP port or IPPS URL transmission.

The **Send Data** wizard can be opened from the **Send data** button on the toolbar and from the **Groups** menu in the navigation area.

The KYOCERA Net Admin server saves the last ten files or strings sent to a device in a **File history** or **Text history** list.

**Warning:** **Send Data** is an advanced feature. Incorrect use can cause the device to become inoperable.

### Sending Data by TCP or IPPS

You can send data to the device.

1 In the navigation area, select a group of devices (**All Devices** is the default).

2 In the device list, select one or more devices.

3 In the toolbar, click **Send data**.

4 In the **Send data** dialog box, select the TCP port or IPPS path. You can select the default TCP port or specify a different port on the device. The port number must match that of one of the logical printers defined in the device home page. The range is 1 to 65535.

5 Select data to send:

To send data as text, select **Text** and type or paste the text into the box. To send a previously sent text string, click **Text history** and select text from the list. Use this option to send PRESCRIBE commands.

To send data from a file, select **File**, click **Browse local**, and select the file. To send a previously sent file, click **File history** and select a file from the list.

To send data to a document box, select both **Text** and **File**. In the **Text** box, type or paste a PJL command designating the box number. In the **File** box, specify a file to send to the document box.

**Note:** If you select both the **Text** and **File** check boxes, the application sends text data first and then file data. The application sends {#FILE#} commands and text in the order they appear in the **Text** box. Binary data can appear in text as bytes in hexadecimal form with the string **0x** prepended to it.

6 Click **OK** to send the data.

## Manage Reports

You can create reports for all printing activities in the network. Several types of reports are available, based on selected printing and device patterns. Current information is summarized in tables and graphics, using default or custom report templates.

Reports are available in HTML, PDF, XML, or CSV format.

In the **Device Manager** console, reports can be created from **List View**, **Map View**, and **View Subscriptions**. To ensure correct processing of reports using Internet Explorer, go to Tools > Internet Options > Advanced and verify the **Do not save encrypted pages to disk** setting is cleared.

**Note:** If pop-up blockers are enabled in your browser, **Add Alert Subscription**, **Add Report Subscription**, **Manage Reports**, the **About** page, and **Help** will not open.

### Creating a Device Manager Report

You can create a device manager report.

1 Click **Manage reports** from the toolbar.

2 Select the type of report under **Report type**.

Current identifying information for printing devices appears under **Device ID** or **Selected Properties**. This information can be edited in the **Edit Device ID** or **Edit Device Properties** dialog box.

3 Select options available for the selected report type under **Rank by**, **Selected Counters**, **Selected errors**, or **Sort by**.

4 Under **Report Period**, select the time frame for the report. This option is unavailable for **Device properties** reports.

**Range** lets you select the period of time for the report. The **Ending date** is automatically set to the end of the previous unit of time selected under **Range**. For example, with **Months** selected, the ending date is the last day of the previous month.

5 Under **Format**, select a file format for your report: HTML, PDF, XML, or CSV.

6 When all report options are set, click **Generate Now** to create the report.

## Editing Device IDs and Device Properties

You can select the device IDs or properties that appear in the report. Available options depend on the selected report type:

You can edit the **Device ID** for all report types except **Device Properties**.

You can edit the properties for the **Device Properties** report.

1 In the **Manage reports** dialog box, select the desired report option under **Report type**.

2 Click **Edit**.

3 Select desired options under **Available IDs** or **Available Properties**.

4 Click the right arrow to add the selected items to the **Selected IDs** or **Selected Properties** list. Use the up and down arrows to change the list order.

5 Click **OK**.

## Selecting a Report Template

You can use a report template that you have created based on your selected settings. To select a report template:

1 In the **Manage reports** dialog box, click **Open** to use an existing template.

2 In the **Open Report Template** dialog box, select a template and click **OK**.

The options associated with the selected template are selected in the **Manage reports** dialog box.

### Creating a Report Template

You can create or delete a report template.

1 In the **Manage reports** dialog box, select the desired report options under **Report Definition**, **Report Period**, and **Generate Report**.

2 Click **Save**.

3 In the **Save Report Template** dialog box, type a template name.

4 Under **Select formats available for subscriptions**, select one or more file types as available report formats: **HTML**, **PDF**, **XML**, or **CSV**.

5 Click **OK** to save the template. The saved template is added to the **Open Report Template** dialog box.

To delete a template, select it in the **Manage Report Template** dialog box and click **Delete**.

### Renaming a Report Template

1 In the **Manage reports** dialog box, click **Manage**.

2 In the **Manage Report Template** dialog box, change the name of a template by selecting it and clicking **Rename**.

3 In the **Rename Report Template** dialog box, type the new name, and click **OK**.

## Create Report Subscriptions

You can subscribe to receive a report. The report will be sent periodically based on the subscription settings you have specified for the selected report.

### Creating a Report Subscription for Groups

You can subscribe to receive regular reports about devices.

1 In the **Manage reports** dialog box, create a report and save the report template.

2 Click **Subscribe**.

3 In the **Create Report Subscription for group** dialog box, under **Recipients**, select the recipients for e-mail report subscriptions.

4 Under **Report Templates**, select the templates with the desired information for the new report subscription.

5 You can change the file type of the template. Some templates support limited file types.

6 Under **Schedule**, select interval settings for the subscription e-mail.

7 Click **OK**.

# Export a Report

You can export current information for all workspace devices to a .CSV or .XML file. The .CSV export uses UTF-8 encoding.

1 In the navigation area, select a group of devices (**All Devices** is the default).

2 In **List View**, select one or more devices.

3 In the view toolbar, click the **Export a report** icon.

4 Select **View as CSV** or **View as XML**.

5 Click **Open** or **Save**.

## Status Filter

You can set a filter that lets you view only the devices in a group that match a user-selected status.

### Setting a Status Filter

You can set a status filter.

1 Select **All Devices** or a device group to filter.

2 In the toolbar, click the **Status filter** funnel icon.

3 Select a status filter from the list.

**List view** or **Map view** displays all devices that have the selected filter.

### Show or Hide Unmanaged Devices

You can display or hide printing devices that are not being managed.

1 Select **All Devices** or a device group.

2 In the toolbar, click **Status filter**.

3 Select the **Show Unmanaged Devices** check box in the **Status filter** list to display both the managed and unmanaged devices. Clear the check box to show only the managed devices.

## Search

You can use the **Search** feature in **List view** or **Map view** to find all printing devices that match selected criteria.

**Search Scope**

**Current group**

Searches only the devices in the group selected in the navigation area.

**All devices**

Searches all printing devices, even if a sub-group is selected in the navigation area.

**Search Type**

**OR (match any)**

Searches for devices that match at least one of the search criteria.

**AND (match all)**

Searches for devices that match all of the search criteria.

**Search Criteria**

**Property**

Select from available device properties in the list.

**Condition**

Available conditions depend on the selected property.

**Value**

Select from the list or type a value in the box.

## Searching for Printing Devices

You can search for a group of selected devices, and create a group from the search results.

In **Map view**, save the map settings before searching. The search result devices appear in their saved position in the office map.

1. In the navigation area, select a group of devices (**All Devices** is the default).
2. In **List view** or **Map view**, click **Search**.
3. In the **Device Search** dialog box, under **Search Scope**, select the devices to search.
4. Under **Search Type**, select an operator to define the search logic.
5. Under **Search Criteria**, select device properties to find in the search.
6. Click **OK**.

# 4 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.

## Creating New Settings

You can create a new settings file from a blank template.

1. In **Multi-Set Template Editor**, click **File** > **New**.
2. In the **Select Target Device Group** dialog box, select the target device group for the template.
3. Select **XML template file** or **ZIP template file** as the file type.
4. Select from the available settings or options for the template:

   For XML, select one settings option.

   For ZIP, select more than one settings option.
5. Click **OK**. The template appears in **Multi-Set Template Editor** as **Newly Created***.
6. Select **Newly Created***, and then click **File** > **Save as**.

## Editing a Multi-Set Template

You can edit an existing template with updated settings.

1. In **Multi-Set Template Editor**, click **File** > **Open**.
2. Select an XML template file or a ZIP template file.

3 In the **Select Target Device Group** dialog box, specify the target device group for the template. Click **OK**. The source file, settings, and device group are shown on the right side. These values cannot be edited.

4 For an XML file, click **Edit**. For a ZIP file, select desired settings from the list and then click **Edit**.

5 Update settings in the open dialog box, and then click **OK**, **Apply**, or **Close**.

6 Click **File** > **Save** to save updated settings to the template file.

## Importing a CSV File

You can import **Device Address Book**, **Device User List**, and **Device Document Box** data from CSV files, and save them as XML template files in Multi-Set Template Editor. Address book files can also be saved in CSV format. Multi-Set Template Editor can only open CSV files saved with UTF-8 encoding.

1 In **Multi-Set Template Editor**, click **File** > **Import**.

2 Select the type of file to import.

3 Click **Browse** to find a valid CSV file. Click **Open**.

4 Select the target device. Click **Next**.

5 Select mapping options for each property. The required (*) properties must be mapped. Click **Next**.

If the Address Book (CSV) files are being imported from Net Viewer 4.x or 5.x Address Book (CSV) files, this step is skipped.

If the User List or Document Box (CSV) files are being imported from Net Viewer 5.x User List (CSV) files, this step is skipped.

6 Confirm your selections and click **Finish**.

The newly imported template appears in Multi-Set Template Editor, where it can be edited and saved.

## Adding an Existing Template File

You can add an existing XML template file to a ZIP template file.

1 In **Multi-Set Template Editor**, open an existing ZIP template file.

2 In the **Select Target Device Group** dialog box, specify the target device group for the template. Click **OK**.

3 Click **Add Existing**.

4 Browse to select a template file (.XML) that is not in the ZIP file.

5 Confirm your selections and click **Open**. The setting option appears in the **Settings** list, where it can be edited.

6 Click **File** > **Save as**.

You can create new settings to a ZIP template file by clicking **Create New**.

You can remove setting option from the ZIP template file by selecting it and clicking **Delete**.

## 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 groups settings.