KMnet Admin 3.0

User Guide

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

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 printing environment. Essentially the same operations are used for Microsoft Windows XP, Vista, and Windows 7 environments.

Table of Contents

Chapter 1 Login and Consoles

Chapter 2 Administration

Chapter 3 Device Manager

1 Login and Consoles

KMnet 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**.

KMnet 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.

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 **KMnet Admin** from Internet Explorer 7 or later.

1. In the browser, click the application's address in **Favorites** or history, or type the address in the format: http://<computer name>:7478/kmnetadmin/

2. On the login page, type the **User name** and **Password**.

3. Choose a console to open:

   Open the default console

   The default console is displayed. You can later change the console to set as the default.

   Choose a console to open

   Click this option, then choose a console from the list.

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 if the software is not used for 30 minutes.

Consoles

You can choose a console when logging on to **KMnet 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 **KMnet 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

The **Administration** console lets you 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, and delete or disable an account. An administrator or user must be selected in the navigation area.

Changing the Password

An administrator or user 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**.

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. Alerts can be sent to no more than two e-mail addresses.
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 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.

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

Networks and Agents lets you create printing system 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, the **Select All** button lets you remove or change 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 **Domain**. This text box is available only if the **Device Communication** option in the **Administration** console is set to **Device IP addresses are volatile and may change**. When the device is first discovered, the network domain is applied to the domain of the device.

5 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::fffff:fffff:fffff:fffff:fffff:ffff:ff00 IPv6 mask.)

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

Installing an Agent

You can install an agent for the network.

1. On the **Select an Agent** page, select **Local Agent**, **New Agent**, or **Remote Agent**. **Remote Agent** appears if it was previously created through **New Agent**. Click **Next**.

2. On the **Enter the Agent Details** page, enter the required information for the agent:

   For a local agent or remote agent, accept the displayed agent details.

   For a new agent, type the agent details.

3. Click **Next** to proceed to the **Enter the Agent Details** page.

Specifying SNMP Information

You can select the SNMP settings for the network.

1. In the **Enter the SNMP Information** page, accept the defaults or type the number of **Retries** and the **Timeout (seconds)** period for communication between agents and devices. Under **SNMP Version**, select **SNMP v1/2c**, or **SNMP v3**, or both. Click **Next**.

2. Depending on the SNMP version chosen in the previous page, select **Communication settings**:

   Communication settings SNMP v1/2c

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

   Communication settings SNMP v3

   Select the desired **Security level**, **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. If you clear the **Managed** check box, click **OK** to confirm.

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**.

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 KMnet Admin installed and operating on the server. TCP port numbers 9000 and 9072 should be free and not blocked by a firewall. Windows XP SP3 or later with .NET Framework 3.5 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 .KMNALU.
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 .KMNALU.

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 KMnet 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.

   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

KMnet 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

Device Communication uses **Host Name** and **Domain** name, if entered. Choose from a static or volatile IP address.

For DHCP, select **Device IP addresses are volatile and may change**. If this option is chosen, communication with the devices is established by using the host name rather than the IP address.

Note: After the **Device Communication Mode** is changed, **KMnet 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

KMnet Admin database backup compresses files into a zip file and saves it to a folder called C:\KMnetAdminBackup. 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:

   Immediate

   The backup starts 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 KMnet information from a database backup. This restore uses a backup file (.ZIP) in the default backup location C:\KMnetAdminBackup, 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 KMnet 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, 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**.

Web Server

You can choose the server protocol setting. The setting is applied the next time the application is started.

HTTP

Faster than HTTPS, it is a client/server Internet protocol used by browsers to transfer hypertext requests, which control the formatting and transmission of messages.

The HTTP port number is 7478.

HTTPS

More secure than HTTP, it is encrypted and uses a different port. It creates a secure channel over an unsecured network.

The HTTPS port number is 7443.

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

Log View

Log View lets you track and view the activities of various KMnet 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\KMnet Admin\log.

Log files can be created for the following operations:

Database backup

Database restore

Multi-Set

Send Data

Firmware Upgrade

Agents Upgrade

Model Support Update

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

Creating a Log File

You can create log files for various KMnet 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\KMnet Admin\log.

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

To delete a log file manually, select it from the **Log view** list, click the **Delete Log File** icon, and then click **OK**.

Selecting Log File Storage

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. Click **OK**.

Scheduled Jobs

Some KMnet 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 **Administration** console.

Database Backup

Set in the **Administration** console.

Multi-Set

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

Firmware Upgrade

Set in the **Firmware Upgrade** wizard in 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**.

3 Device Manager

Device Manager lets you access local device settings and monitor the status of multiple devices connected locally or through a network. It lets you 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. Two additional features are available:

Upgrade firmware

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

Send data

Lets you send files, text or device commands directly to one or more selected 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. If any subnode of **Networks** is selected, **Add group** is unavailable.

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**.

Preferences

You can set preferences for KMnet 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 discovered devices. 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. Click **Apply**.

Alert Configuration

KMnet 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

Special Settings 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.

Alert Details

Alert Details helps you identify the device properties that will be reported in alert e-mails. The KMnet 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.

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

KMnet 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.

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

The **Map View** toolbar lets you 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 the database.

Refresh

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

Map Background

Background options lets you 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.

Selecting Icon Properties

You can change the properties of printing system icons.

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.

To select printing system 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.

View 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 KMnet 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 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 **List view** or **Map view**, click **Add device**.

2. In the **Add Devices** dialog box, add selected targets:

   You can type the IP address or host name of the device, 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 text file. Click **Import**, and then click **Browse** to select a file with a .TXT or .CSV extension.

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

3. 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.

4. 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**.

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.

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.

Multi-Set

The **Multi-Set** wizard lets you send configuration parameters to multiple devices at once.

Multi-Set lets you 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.

To start **Multi-Set**, select a group of devices in the **List view** or **Map view**, then click **Multi-Set** in the toolbar.

Multi-Set Installation

In the pages of the Multi-Set wizard you can select the following settings:

Device Group

Select the device or group of devices you want to configure.

Multi-Set Settings

Displays device settings, such as **Device System Settings** and **Device User List**. Not all settings are available for some devices. You can only configure one group of settings at a time.

Multi-Set Source

If you select **Copy from source device**, then you must select a source device for the settings from the **Select Device** page. These settings can be saved as a Multi-Set template file. If you select **Copy from Multi-Set template file**, you must select a Multi-Set template file from the server or from your local client. Multi-Set template files can be saved from the Multi-Set wizard or created with the **Multi-Set Template Editor** tool.

Schedule

If you select **Run now**, Multi-Set configures the selected devices when you click **Set Devices** on the final page of the wizard. If you select **Schedule to run**, then you must define a time and date for the device configuration to take place. Type the time in the text box using hh:mm in a 24 hour format. Select the day, month, and year from the corresponding lists.

Confirmation

Displays a summary of the Multi-Set operation that will be performed.

Configuring Selected Devices

You can configure one or more selected devices.

1. Select the device or devices you want to configure from **List view** or **Map view**.

2. Click **Multi-Set** on the toolbar.

3. Select a device or device group. Click **Next**.

4. Select one settings option from the list. Click **Next**.

5. Select a source for the settings:

   Copy from source device

   Settings are copied from a device selected on the next page.

   Copy from Multi-Set template file

   Settings are copied from a template saved in the server or on your computer.

6. For some options, you can select **Override settings on target device**. When selected, settings from the source device replace settings on the target device. Click **Next**.

7. Depending on the selection in Step 5, select a source device or source template. Click **Next**.

8. If you selected a source device, you can save the settings as a template on the server. Click **OK** and name the template file, then click **Save**.

9. Schedule **Multi-Set** to run immediately by leaving **Run now** selected. Select **Schedule to run**, type the time using hh:mm in a 24 hour format, then select the **Day**, **Month**, and **Year**. Click **Next**.

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

Note: The system will use 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.

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\KMnet Admin\MultiSet.

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.

Note: For models using the firmware master file format, place the upgrade files on the KMnet Admin server. The default location is C:\Program Files\Kyocera\KMnet 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 KMnet Admin server port 7478.

The target device has a network interface card installed.

Select port 21 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**. Other indications are messages like **Upgrading**, **Erasing**, **Writing**, or similar 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 application processes a maximum of 10 devices at a time.

1. 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.

2. 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**.

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

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

With **Select file from KMnet Admin Server** selected, click **Browse** to find the firmware file located on the KMnet 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: Firmware files are provided or updated by an administrator or dealer.

5 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**.

6 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**.

7 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.

8 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.

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

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

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

Send Data

The **Send Data** feature lets you 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 KMnet 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 device list, select one or more devices.
2. In the toolbar, click **Send data**.
3. 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 Command Center for the device. The range is 1 to 65535.
4. Select data to send:

   To send data from a 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 as text, 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.
5. Click **OK** to send the data.

Device Properties

Device properties lets you 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 **List View** or **Map view**, select one or more printing devices.
2. Click **Device properties**.
3. In the **Properties** or **Multiple Device Properties** dialog box, view or modify the available settings.
4. Click **OK** when you are finished.

Device Properties for a Single Device

Device Properties options lets 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 software on 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** and **sysUpTime** are blank.

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.

Supplies tab

Displays the current level of consumable supplies.

Device Settings tab

Displays all available printing device properties.

Troubleshooting tab

Displays device errors and troubleshooting advice.

Monitoring tab

Lets you set a polling schedule or configures SNMP traps to monitor a device.

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

Multiple Device Properties lets you 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

With any option selected for the **Manage these devices** check box, 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 or Device Login. Any changed settings will affect those devices.

Login

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

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**.

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 reports related to device counters.

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 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**.

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 **List view** or **Map view**, click **Search**.
2. In the **Device Search** dialog box, under **Search Scope**, select the devices to search.
3. Under **Search Type**, select an operator to define the search logic.
4. Under **Search Criteria**, select device properties to find in the search.
5. Click **OK**.

4 Multi-Set Template Editor

Use the **Multi-Set Template Editor** to create or change the template files. The template files specify settings for particular groups of devices that are managed by KMnet Admin. The Multi-Set function in KMnet Admin applies the templates to printing systems on a network.

Template files in XML format are specific to groups of printing system models, and to groups of settings shared by those models. Template files created in KMnet Viewer version 5.x can also be used.

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. Click **File** > **New**.
2. In the **Select Target Device Group** dialog box, select the target device group for the template.
3. Select the settings group for the template.
4. Click **OK**. A dialog box for the selected settings appears.
5. Select from available settings or options for the template.
6. Click **OK**, **Apply**, or **Close**. The template appears in the left pane as **Newly Created***.
7. Select **Newly Created***, then click **File** > **Save as**.

Editing a Multi-Set Template

You can edit an existing template with updated settings.

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

4 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.

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.