

KYOCERA Fleet Services Gateway 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®, Microsoft Edge™, and Internet Explorer® are registered trademarks of Microsoft Corporation in the U.S. and/or other countries.

Java Runtime Environment and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Firefox® is a registered trademark of Mozilla Foundation.

Google Chrome™ is a trademark of Google Inc.

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

Table of Contents

Chapter 1 Overview

Gateway	1-1
---------------	-----

Chapter 2 Installation and Uninstallation

Installation Requirements	2-1
Downloading the Gateway for Windows Installer	2-1
Sending the Gateway Installer by Email	2-2
Installing Gateway for Windows	2-3
Uninstall Gateway for Windows	2-5

Chapter 3 Gateway Management

Gateway for Windows URL	3-1
Starting Gateway	3-1
Gateway for Windows View Icons	3-2
Restoring the Default Password	3-2
Gateway Upgrade Packages	3-2
Upgrading Gateway	3-2

Chapter 4 Gateway Preferences

Gateway Registration	4-1
Preferences View Icons	4-1
Automatic Gateway Registration	4-2
Creating Proxy Settings	4-2
Registering Gateway with KFS Manager	4-2
Setting Automatic Gateway Upgrade	4-3
Setting the Date and Time	4-3
Editing Discovery Settings	4-4
Deleting Discovery Settings	4-4
Refreshing Registered Devices	4-5
Creating User Account Lockout Settings	4-5
Modifying the Interval Setting	4-6

Chapter 5 Gateway Devices

Device Discovery Settings	5-1
Devices View Icons	5-1
Creating Discovery Settings Based on a Host Name	5-2
Creating Discovery Settings Based on IP Address	5-3
Creating Discovery Settings Based on IP Address Range	5-4
Creating Discovery Settings for a Local Network	5-5
Creating Discovery Settings for Network Printers	5-6
Selecting Saved Discovery Settings	5-7
Editing Saved Discovery Settings	5-7
Device Registration	5-8
Registering Devices with Remote Services firmware	5-9

Registering Legacy Devices and Devices by Other Manufacturers	5-9
Device Registration Results	5-10
Checking the Device Registration Result Details	5-10
Deleting Device Registration Logs	5-11
Opening Device Management for a Discovered Device	5-11
Creating Communication Settings for a Device	5-11
Searching Devices	5-12

Chapter 6 Gateway Logs and Passwords

Gateway Logs	6-1
Logs View Icons	6-2
Downloading Gateway Logs	6-2
Searching Gateway Logs	6-2
Deleting Gateway Logs	6-3
Changing a Password	6-3

Chapter 7 Local Agent

Local Agent View Icons	7-1
Downloading the Local Agent Installer	7-2
Installing Local Agent Manually	7-2
Installing Local Agent from Gateway	7-2
Configuring the Computer for Local Agent Installation	7-3
Disabling UAC Remote Restrictions in Windows	7-3
Discovering a Computer within a Domain	7-3
Discovering a Computer using Host Name	7-4
Discovering a Computer using an IP Address	7-4
Discovering a Computer within an IP Address Range	7-4
Local Agent Upgrades	7-5
Upgrading Local Agent from Gateway	7-5
Uninstalling Local Agent from Gateway	7-5

Chapter 8 Troubleshooting

Checking the JRE Connection	8-1
Configuring Ports for Legacy Device Firmware Upgrades	8-1
Restarting a Gateway	8-2
Restarting the Gateway for Windows service	8-2
Changing the Startup Type	8-2

1 Overview

KYOCERA Fleet Services (KFS) and Gateway work together to provide remote management of your devices, including legacy devices and devices by other manufacturers.

Gateway

A registered KFS Gateway can discover and register legacy devices, devices by other manufacturers, and devices with the Remote Services firmware. KFS Gateway must be registered to a group in KFS Manager. Devices connected by USB and an optional Network Interface Card (NIC) can also be discovered. KFS Manager works with the Gateway to manage devices on a local network. KFS Manager can directly manage registered devices with Remote Services firmware regardless of Remote Services firmware version.

Note: For devices with Remote Services firmware 1.0 version, you must set Remote Services to **ON** in advance.

2 Installation and Uninstallation

Installation Requirements

Operating Systems

Gateway for Windows runs on the following operating systems:

Windows 7 (x86 and x64)

Windows 8 (x86 and x64)

Windows 10 (x86 and x64)

Windows Server 2008 R2 (x64)

Windows Server 2012 R2 (x64)

Windows Server 2016 (x64)

Java Runtime Environment

The Gateway for Windows installation runs in a 32-bit or 64-bit Java Runtime Environment (JRE) v7 or v8 depending on the Gateway for Windows installer that is being used. If your environment is not compatible, you can install the required JRE in advance. Alternatively, the installer will direct you to the Java website where you can download JRE.

Supported Internet browsers

Gateway for Windows supports the following browsers:

Internet Explorer 11

Microsoft Edge

Firefox 40 or higher

Google Chrome 47 or higher

Customer Network Information Settings and Access

IP Address

Subnet mask

Default gateway

Domain name

If you are not sure that all of the above have been configured, check with your network administrator.

Downloading the Gateway for Windows Installer

System Administrators, Managers, and Service users can download the **Gateway for Windows** installer located in the **Product downloads** page. The installer is downloaded to your default download location.

- 1 In the top banner of KFS Manager, click **Product downloads**.

- 2 For the **KFS Gateway for Windows**, click **Download (32-bit)** or **Download (64-bit)**.
- 3 In your download folder, extract the ZIP file.

Sending the Gateway Installer by Email

In KFS Manager, System Administrators, Managers, and Service users can send the Gateway installer to specified email recipients. The email includes a download link to access the **Gateway for Windows** installer, information about what group the Gateway is associated with, and an XML configuration file attachment that can be imported into KFS Gateway. As an example, if the **Automatic device registration** option is enabled, any discovery settings included in the XML configuration file and run automatically. The email provides the KFS Manager URL for registering the Gateway and the **Access Code** associated with the selected group in KFS Manager. The download link expires after 7 days.

- 1 In the **Devices** view, click **Gateway**.
- 2 On the **Gateway** page, click **More > Send Gateway installer**.
- 3 In **Add recipients**, type the recipient's addresses in the **Email addresses** text box. For multiple recipients, separate each email with a semicolon.
- 4 Select the **Group** to associate with the registered Gateway.
- 5 Type an optional **Description**.
- 6 Select a **Connection mode**. This setting can be modified during the installation of **Gateway for Windows**.
 - **Manage** - Maintains open and constant communication between Gateway and KFS Manager through XMPP over HTTPS. Supports real time device status and alert updates.
 - **Monitor** - Communicates counter and consumable information through SNMP to the KFS device rest server. Counter and consumable information is set in the Group management settings and requires devices that support Gateway monitoring. KFS Manager does not communicate directly with the devices.
- 7 Select an hourly value to retrieve **Device information update interval: 6 hours, 12 hours, 24 hours**.
- 8 Select the checkbox for **Use Gateway as a single point of communication** if you want all devices registered by the Gateway to communicate with KFS Manager through the Gateway. This setting can be modified during the installation of **Gateway for Windows**.
- 9 Click **New discovery setting** or click the edit icon of an existing Discovery setting to modify, if desired.

- 10** In the **Add Discovery Settings** wizard, type a **Description** to a maximum of 256 characters.
- 11** Select a **Discovery method**, either **Via local network**, **By IP address or host name**, or **By IP address range** to search for devices.
- 12** Select an **IP** protocol, either **IPv4** or **IPv6** as supported by your network. **IPv6** must be configured before it can be used to search for devices.
- 13** If desired, select **Search for USB connected devices**.
- 14** If desired, select **Automatically register newly discovered devices**.
- 15** Type a **TCP/IP Port number** from 1024 through 65535 to match the port on the device.
- 16** Type a **Timeout** value from 5 through 120 (in seconds).
- 17** Type an **SNMP retries** value for the application retry attempts after a communication failure with the device. The valid range is from 0 to 5.
- 18** For the **SNMPv1/v2** type, type the names for **Read community name** and **Write community name**. The read community and write community names are sent with all SNMP receive and send requests, and must match the community names on the device.
- 19** For **SNMP v3** protocol, type the **User name** and **Password**.
For **SNMP Authentication** options, select from **SHA1** and **MD5**.
For **SNMP Privacy** options, select from **AES** and **DES**.
- 20** Select **Enable SSL protocol**.
- 21** Click **Save**. You can create a maximum of 10 discovery settings. They are included in the XML configuration file sent to the email recipient.
- 22** Click **Send**.

Installing Gateway for Windows

Before starting the installation, ensure that required Java Runtime Environment (JRE) v7 or v8 is installed on your computer and your computer has a minimum of 129 MB of free disk space. If you do not have JRE installed, download it from the Oracle Java SE site and install it on your computer.

- 1** Run the executable application file.
- 2** In the **Select Setup Language** dialog, select the language to be used during the installation, and then click **OK**.

- 3 In the **Welcome to the Gateway for Windows Setup Wizard** dialog, click **Next**.
- 4 In the **License Agreement** dialog, select **I accept the agreement**, and then click **Next**.
- 5 In the **Select Destination Location** dialog, accept the default folder or click **Browse** and select another folder to install Gateway for Windows. Click **Next**.
For the 32-bit Windows installer, the default folder is **C:\Program Files (x86)\Kyocera\Gateway for Windows**.
For the 64-bit Windows installer, the default folder is **C:\Program Files\Kyocera\Gateway for Windows**.
- 6 In the **Select Start Menu Folder** dialog, accept the default location, or click **Browse** to select another location. Select **Don't create a Start Menu folder** if you don't want to create a folder in the **Start** menu for Gateway shortcuts. Click **Next**.
- 7 In the **Select Additional Tasks** dialog, select **Create a Desktop icon** and **Create a Start Menu icon**, and then click **Next**.
- 8 In the **Registration Mode** dialog, select **Manual registration** or **Auto registration**. The XML configuration file is attached to an email sent from KFS Manager. To register devices automatically, click **Browse** and locate the XML configuration file, select **Automatic device registration**.

Note: Automatic device registration cannot be selected when the XML configuration file lacks discovery settings. Gateway registers devices automatically using discovery settings.

- 9 For **Connection mode**, you can select **Manage - Remote maintenance and Data collection** or **Monitor - Data collection only**. In **Manage** mode, Gateway supports all KFS task management features from KFS Manager. In **Monitor** mode, Gateway registers devices and collects data but offers no task management features from KFS Manager.
- 10 In the **Proxy Configuration** dialog, select **Direct connection** or **Use HTTP proxy**. If you select **Use HTTP proxy**, enter **Host name**, **Port**, **User name**, and **Password**. Select **Use Gateway as a single point of communication**, if you want to connect the device with Remote Services firmware through Gateway.
- 11 In the **Device firmware upgrade port** dialog, type the port number to be used, and then click **Next**.

Note: Contact your IT administrator to check the availability of the port.

- 12 Review the summary. Click **Back** to change settings. Otherwise, click **Install**.
- 13 Click **Finish**.

- 14 Clear **Launch Gateway for Windows** if you want to complete the installation without starting the application.

Uninstall Gateway for Windows

- 1 Click **Start > All Programs > Kyocera > Gateway for Windows > Uninstall Gateway for Windows**.
- 2 In the **Gateway for Windows Uninstall** dialog, click **Yes**.
- 3 Click **OK**.

The following message may be displayed:

“Some elements could not be removed. These can be removed manually.”
Some of the files created during installation may be in use. Delete these files manually.

3 Gateway Management

Gateway shares device information with KFS Manager. Gateway includes two accounts: **Admin** and **Service**. KFS Manager has five accounts: **System Administrator**, **Manager**, **Service**, **Analyst**, and **Customer**.

The **Access code** generated when a group is created in KFS Manager serves two purposes. It is first used to register Gateway to a group in KFS Manager. It can then be used in Gateway to register devices to a group in KFS Manager.

KFS System Administrators can refresh device information in KFS Manager. KFS Manager also supports Gateway upgrade.

KFS System Administrators, Managers, and Service users can archive or delete Gateway in KFS Manager. Archiving Gateway stops it from polling, sending, and receiving data while maintaining historical data. Deleting Gateway will remove the Gateway information and stops services to devices which were registered by it.

Gateway for Windows URL

Once the software has been successfully installed, you can access Gateway for Windows by clicking the desktop icon. When the **Certificate Error: Navigation Blocked** dialog is displayed, select the option **Continue to this website (not recommended)**.

You can also start Gateway for Windows by typing **https://localhost:8443/gatewayapp** in your browser. If you are using a different computer on the same network, you can also access Gateway for Windows by typing **https://<IPaddress>:8443/gatewayapp** in your browser. You only have to determine the **IP address** of the computer on which Gateway for Windows was installed (for example, **https://10.191.22.10:8443/gatewayapp**).

Starting Gateway

You must log in to Gateway to manage devices remotely. If you are unable to log in, use **Password assistance** to restore the default password.

- 1 Open a supported Internet browser, type the **Server URL** for Gateway, then press **Enter**.






Note: SSL certification warning screen may appear depending on the selected Internet browser. These warning screens vary according to your Internet browser. You must agree to the provision in the warning message before the login page is displayed.

- 2 On the login page, type your credentials for **User name** and **Password**.
- 3 Select **Remember me** to save your credentials to your browser's cache.

- 4 Click **Log in**.

Gateway for Windows View Icons

The Gateway for Windows application uses the following icons.

Description	Icon
Devices	
Local Agent	
Preferences	
Logs	
Change password	

Restoring the Default Password

Gateway Service users can restore passwords to the default settings. Admin users cannot reset their password.

- 1 On the Login page, click **Password assistance**.
- 2 In the **Reset Password** dialog, select **Admin** or **Service** for the **Target account to be reset**.
- 3 Type the **User name**, **Password**, and **Access code** of the KFS Manager server.
- 4 Click **OK**.

Gateway Upgrade Packages

A System Administrator or Manager in KFS Manager can create a Gateway upgrade package and upload the package to KFS Manager. A user with access to upgrade ZIP files can download the upgrade package from KFS Manager to a computer.

Upgrading Gateway

You can upgrade Gateway in KFS Manager. A Gateway upgrade package must be first uploaded to KFS Manager. An error is displayed if Gateway cannot be upgraded.

- 1** In the **Administration** view, click **Gateway**.
- 2** In the **Group** drop-down, select the desired group.
- 3** Select one or more Gateways which are **Online**.

Note: The selected Gateways must be the same **Gateway type** (PC or IB).

- 4** Click **Upgrade**.
- 5** In the **Gateway Upgrade** dialog, select **Notifications** to receive an upgrade email.
- 6** Click **Upgrade**.
- 7** Click **Close**.

4 Gateway Preferences

Preferences provide support for registering Gateway, creating **Network** settings, viewing **Network** information, **Proxy settings**, **Date and time** settings, **Discovery settings**, and **User account lockout settings**.

Gateway Registration

KFS Gateway is registered to a group in KFS Manager using a group **Access code**, or using both a group **Access code** and your **Manager login**. Registration appears in the **General** tab on the **Preferences** pane. In a proxy environment, add your proxy information before registering.





You can register Gateway even if the KFS Manager user account has a **Locked** status. You cannot register Gateway if the user status in KFS Manager is **Disable** or **Expired**.

Gateway registration information includes the **Gateway ID**, **Registration status**, **Connection status with Manager**, **Group name**, and **Manager URL**. **Manager authentication** information includes the **User name**, **Password**, **Access code**, and **Description**. Once Gateway is registered, these settings cannot be changed. After Gateway registration, the **Description** text is no longer displayed.

You can set **Connection mode**. Depending on the selected mode, KFS Gateway will switch the connection with KFS Manager. You can switch the **Connection mode** at any time.

Preferences View Icons

The Gateway for Windows application uses the following icons for Preferences.

Description	Icon
Edit discovery	
Delete discovery	
Refresh devices	
Refresh	

Automatic Gateway Registration

During Gateway for Windows installation, you can register Gateway manually or automatically. To automatically register Gateway for Windows during installation, you must use the configuration file (XML) that was sent with the Gateway Installer by email from KFS Manager. Proxy settings can also be set during installation.

If Gateway is registered, you cannot register Gateway manually without reinstalling Gateway.

Creating Proxy Settings

Proxy settings are only required for Gateway communications if you are using proxy settings on your network. Your network proxy settings must be added to Gateway. If the port is already available, then the latest proxy port entered will be the value displayed in the Port text box.

- 1 In the navigation pane, click **Preferences**.
- 2 Click the **Basic setup** tab.
- 3 In the **Proxy settings** section, type the **Host name**.
- 4 Type the **Port**.
- 5 Type the **User name**.
- 6 Type the **Password**.
- 7 Select **Use Gateway as a single point of communication**, if you want to connect the device with Remote Services firmware through Gateway.
- 8 Click **Save**.
Click **Reset** to change to the previously saved settings. After you make changes to any of the settings, **Reset** becomes active again.

Registering Gateway with KFS Manager

You can register Gateway with KFS Manager using an Access code, or using both an Access code and a Manager login. Gateway is registered to a group in KFS Manager.

- 1 In the **Preferences** view, click **General**.
- 2 Type the **KFS Manager URL**.
- 3 Type a group **Access code** and **Manager login**. Clear **Manager login** if you want to register Gateway with a group access code.
- 4 Type a **Description** for Gateway to a maximum of 256 alphanumeric characters.

- 5 For **Connection mode**, select **Manage - Remote maintenance and Data collection** or **Monitor - Data collection only**. In Manage mode, Gateway supports all KFS task management features from KFS Manager. In Monitor mode, Gateway registers devices and collects data but offers no task management features from KFS Manager. For Manage mode, you can set an expiration time period to change back to Monitor mode. The valid range is from 1 to 72 hours.
- 6 Click **Register**.

Note: If automatic registration is selected during installation, this procedure is not necessary.

Setting Automatic Gateway Upgrade

If you want to use newer Gateway version automatically, you can enable automatic Gateway upgrade. When Gateway has enabled automatic Gateway upgrade setting, Gateway will be upgraded automatically at a particular time if KFS Manager has newer Gateway upgrade package.

- 1 In the navigation pane, click **Preferences**.
- 2 Click the **Software upgrade** tab.
- 3 Select **Enable automatic upgrade**.
- 4 Select **Daily** or **Specified time** as timing to start automatic Gateway upgrade.
- 5 When you select **Specified time**, click the clock icon and use the up and down arrows to select the desired time.
- 6 Click **Save**.

Setting the Date and Time

You can change the date and time settings for the Gateway.

- 1 In the navigation pane, click **Preferences**.
- 2 Click the **Basic setup** tab.
- 3 In the **Time** text box, click the clock icon and use the up and down arrows to select the desired time.
- 4 In the **Date** text box, click the calendar icon and click the desired date.
- 5 Click **Change date and time** to save the settings.
- 6 Click **OK** to confirm settings. After the application resets, the login page is displayed.

- 7 To change the **Time zone**, log in to KFS Gateway and repeat steps 1 and 2.
- 8 In the **Time zone** list, select the desired time zone.
- 9 Click **Change time zone** to save the updated time zone.
- 10 Click **OK** to confirm settings. After the application resets, the login page is displayed.

Editing Discovery Settings

You can edit **Discovery settings** in Gateway Preferences.

- 1 In the navigation pane, click **Preferences**.
- 2 Click the **Discovery settings** tab.
- 3 Select the desired **Discovery settings**.
- 4 In the toolbar, click **Edit**.
- 5 In **Edit Settings**, change the desired Discovery method, and then click **Next**.
- 6 Make any desired changes to the **Communication settings**, and then click **Next**.
- 7 In the **Description** text box, update the text and select checkbox for **Automatic registration mode** if desired, and then click **Next**.
- 8 Confirm your settings, and then click **Back** to make any changes or click **Save**.

Deleting Discovery Settings

You can delete saved **Discovery settings** in Gateway.

- 1 In the navigation pane, click **Preferences**.
- 2 Click the **Discovery settings** tab.
- 3 Select the desired **Discovery settings**.
- 4 In the toolbar, click **Delete**.
- 5 Click **OK** to confirm.

Refreshing Registered Devices

Refresh the list of registered devices in Gateway to update their device information (e.g. host name) excluding counter and consumable information. Devices will also be automatically registered if the selected discovery setting has **Automatic registration mode** enabled. In Monitor mode, you can **Refresh devices** even if Gateway appears in **Offline status** in the Gateway UI.

- 1 In the navigation pane, click **Preferences**.
- 2 Click the **Discovery settings** tab.
- 3 Select the desired **Discovery settings**.
- 4 In the toolbar, click **Refresh devices**.
- 5 If no devices are found for the discovery setting, click **OK**.

Creating User Account Lockout Settings

You can create security settings for user login, user lock out, and audit log in Gateway.

- 1 In the navigation pane, click **Preferences**.
- 2 Click the **Security settings** tab.
- 3 For **Consecutive failed logins**, select a value between 1 and 5. A user cannot access Gateway if the number of consecutive failed logins is exceeded. The default value is 3.
- 4 For **Delay between consecutive logins**, select a value between 0 and 5 seconds.
- 5 For **Period of inactivity**, select a value between 1 minute and 60 minutes. The selected value establishes the length of inactivity before Gateway logs out the user.
- 6 For **Account locked**, select a value between 1 minute and 60 minutes. The selected value establishes the length of time a user is locked out after a failed login.
- 7 Select the **Audit log** check box to enable the recording of audit logs.
- 8 Click **Save**.

Click **Reset** to change to the previously saved settings. After you make changes to any of the settings, **Reset** becomes active again.

Modifying the Interval Setting

You can update the interval setting for retrieving Device information updates between KFS Manager and Gateway. Refresh devices interval setting can change the interval to update device information by using discovery settings.

- 1** In the navigation pane, click **Preferences**.
- 2** Click the **Advanced setup**.
- 3** Select an option for the **Refresh devices interval (Device information update interval)** option based on hourly values: 6, 12, and 24.
- 4** Click **Save**.

5 Gateway Devices

You must register legacy devices and devices by other manufacturers in Gateway, so that they can be remotely managed in KFS Manager. Gateway must be registered with KFS Manager before the devices can be registered with Gateway.

You can register up to a maximum of 1000 devices in Gateway. A maximum of 2000 registered and unregistered devices can be displayed in the Device list. The device connection status is refreshed every 10 seconds.

In the Devices list, the columns are organized by **Registration**, **Connection**, **Connection type**, **Registration type**, **Group name**, **Model name**, **Vendor name**, **Serial number**, **IP address**, **Host name**, and **MAC address**.






Device Discovery Settings

Discovery settings can be used to update device information for registered devices. Discovery settings can be created in KFS Manager or Gateway. Gateway must be registered with KFS Manager before device discovery can be used. A maximum of 10 discovery settings can be saved in the KFS Manager database.


Device discovery takes varying lengths of time based on the number of devices in the discovery path destination and discovery mode. Canceling Device discovery may be slower in some browsers.

Devices View Icons

The Gateway for Windows application uses the following icons for Devices.

Description	Icon
Add devices	
Register devices	
Command Center	
Communication settings	
View registration result	

— continued

Description	Icon
Refresh	

Creating Discovery Settings Based on a Host Name

You can create discovery settings based on a host name. Discovery settings can include a maximum of 100 host names. You can save and reuse these settings in both Gateway and KFS Manager. Discovery of USB connected devices requires installation and configuration of **Local Agent** on a PC which connects by USB cable to the USB device.

- 1 In the **Devices** view, click **Add devices**.
- 2 Select **New settings**, and then click **Next**.
- 3 Select **Search by host name or IP address > Host name**.
- 4 Type the **Host name**, and then click **Add**.
- 5 Select **Search for USB connected devices** if you want to search for USB devices connected by USB cable to computers installed and configured with **Local Agent**.
- 6 Click **Next**.
- 7 Type the **TCP/IP port** of the device. The valid range is from 1024 to 65535.
- 8 Type a **Timeout** value (in seconds) between attempts by the application to establish a connection with the device. The valid range is from 5 to 120.
- 9 Type an **SNMP retries** value for the application retry attempts after a communication failure with the device. The valid range is from 0 to 5.
- 10 In **SNMP v1/v2**, type the **Read community name** and **Write community name**. The community names are sent with all SNMP receive and send requests, and must match the community names on the device.
- 11 For **SNMP v3** protocol, type the **User name** and **Password**.
 Select **Authentication** options in the list for **None**, **SHA1**, and **MD5**.
 Select **Privacy** options in the list for **None**, **AES**, and **DES**.
- 12 Select **Secure protocol (SSL)** to use Hypertext Transfer Protocol Secure (HTTPS) for the device communication. Clear the check box to use Hypertext Transfer Protocol (HTTP) for the device communication.

- 13** In **Device login**, type the **User name** and **Password**. For **Authentication mode**, choose **Local authentication** (stored in KFS Manager) or **Device settings** (stored in the device). Click **Next**.
- 14** Select **Save settings**.
- 15** Type a **Description** to a maximum of 256 alphanumeric characters. Click **Automatic registration mode** if you want to register discovered devices automatically, and then click **Next**.
- 16** Confirm the settings, and then click **Start Discovery**. Click **Back** if you want to make changes to the settings.

Creating Discovery Settings Based on IP Address

You can create discovery settings based on an IP address. Discovery settings can include a maximum of 100 IP address entries. You can save and reuse these settings in both Gateway and KFS Manager.

- 1** In the **Devices** view, click **Add devices**.
- 2** Select **New settings**, and then click **Next**.
- 3** Select **Search by host name or IP address > IP address**.
- 4** Type the **IP address**, and then click **Add**.
- 5** Select **Search for USB connected devices** if you want to search for USB devices connected by USB cable to computers installed and configured with **Local Agent**.
- 6** Click **Next**.
- 7** Type the **TCP/IP port** of the device. The valid range is from 1024 to 65535.
- 8** Type a **Timeout** value (in seconds) between attempts by the application to establish a connection with the device. The valid range is from 5 to 120.
- 9** Type an **SNMP retries** value for the application retry attempts after a communication failure with the device. The valid range is from 0 to 5.
- 10** In **SNMP v1/v2**, type the **Read community name** and **Write community name**. The community names are sent with all SNMP receive and send requests, and must match the community names on the device.
- 11** For **SNMP v3** protocol, type the **User name** and **Password**.
Select **Authentication** options in the list for **None**, **SHA1**, and **MD5**.
Select **Privacy** options in the list for **None**, **AES**, and **DES**.

- 12 Select **Secure protocol (SSL)** to use Hypertext Transfer Protocol Secure (HTTPS) for the device communication. Clear the check box to use Hypertext Transfer Protocol (HTTP) for the device communication.
- 13 In **Device login**, type the **User name** and **Password**. For **Authentication mode**, choose **Local authentication** (stored in KFS Manager) or **Device settings** (stored in the device). Click **Next**.
- 14 Select **Save settings**.
- 15 Type a **Description** to a maximum of 256 alphanumeric characters. Click **Automatic registration mode** if you want to register discovered devices automatically, and then click **Next**.
- 16 Confirm the settings, and then click **Start Discovery**. Click **Back** if you want to make changes to the settings.

Creating Discovery Settings Based on IP Address Range

You can create discovery settings based on an IP address range. Discovery settings can include a maximum of 10 IP address ranges. You can save and reuse these settings in both Gateway and KFS Manager.

- 1 In the **Devices** view, click **Add devices**.
- 2 Select **New settings**, and then click **Next**.
- 3 Select **Search by host name or IP address > IP address range**.
- 4 Type the **Starting IP address** and **Ending IP address**, and then click **Add**.
- 5 Select **Search for USB connected devices** if you want to search for USB devices connected by USB cable to computers installed and configured with **Local Agent**.
- 6 Click **Next**.
- 7 Type the **TCP/IP port** of the device. The valid range is from 1024 to 65535.
- 8 Type a **Timeout** value (in seconds) between attempts by the application to establish a connection with the device. The valid range is from 5 to 120.
- 9 Type an **SNMP retries** value for the application retry attempts after a communication failure with the device. The valid range is from 0 to 5.
- 10 In **SNMP v1/v2**, type the **Read community name** and **Write community name**. The community names are sent with all SNMP receive and send requests, and must match the community names on the device.
- 11 For **SNMP v3** protocol, type the **User name** and **Password**.

Select **Authentication** options in the list for **None**, **SHA1**, and **MD5**.

Select **Privacy** options in the list for **None**, **AES**, and **DES**.

- 12** Select **Secure protocol (SSL)** to use Hypertext Transfer Protocol Secure (HTTPS) for the device communication. Clear the check box to use Hypertext Transfer Protocol (HTTP) for the device communication.
- 13** In **Device login**, type the **User name** and **Password**. For **Authentication mode**, choose **Local authentication** (stored in KFS Manager) or **Device settings** (stored in the device). Click **Next**.
- 14** Select **Save settings**.
- 15** Type a **Description** to a maximum of 256 alphanumeric characters. Click **Automatic registration mode** if you want to register discovered devices automatically, and then click **Next**.
- 16** Confirm the settings, and then click **Start Discovery**. Click **Back** if you want to make changes to the settings.

Creating Discovery Settings for a Local Network

You can create discovery settings for a local network. You can save and reuse these settings in both Gateway and KFS Manager.

- 1** In the **Devices** view, click **Add devices**.
- 2** Select **New settings**, and then click **Next**.
- 3** Select **Search by host name or IP address > Local network**.
- 4** Select **IPv4** or **IPv6** if your network supports the protocols. IPv6 must be configured on your system before it can be used for configuring devices.
- 5** Select **Search for USB connected devices** if you want to search for USB devices connected by USB cable to computers installed and configured with **Local Agent**.
- 6** Click **Next**.
- 7** Type the **TCP/IP port** of the device. The valid range is from 1024 to 65535.
- 8** Type a **Timeout** value (in seconds) between attempts by the application to establish a connection with the device. The valid range is from 5 to 120.
- 9** Type an **SNMP retries** value for the application retry attempts after a communication failure with the device. The valid range is from 0 to 5.

- 10** In **SNMP v1/v2**, type the **Read community name** and **Write community name**. The community names are sent with all SNMP receive and send requests, and must match the community names on the device.
- 11** For **SNMP v3** protocol, type the **User name** and **Password**.
Select **Authentication** options in the list for **None**, **SHA1**, and **MD5**.
Select **Privacy** options in the list for **None**, **AES**, and **DES**.
- 12** Select **Secure protocol (SSL)** to use Hypertext Transfer Protocol Secure (HTTPS) for the device communication. Clear the check box to use Hypertext Transfer Protocol (HTTP) for the device communication.
- 13** In **Device login**, type the **User name** and **Password**. For **Authentication mode**, choose **Local authentication** (stored in KFS Manager) or **Device settings** (stored in the device). Click **Next**.
- 14** Select **Save settings**.
- 15** Type a **Description** to a maximum of 256 alphanumeric characters. Click **Automatic registration mode** if you want to register discovered devices automatically, and then click **Next**.
- 16** Confirm the settings, and then click **Start Discovery**. Click **Back** if you want to make changes to the settings.

Creating Discovery Settings for Network Printers

You can create discovery settings for network printers. You can save and reuse these settings in both Gateway and KFS Manager.

- 1** In the **Devices** view, click **Add devices**.
- 2** Select **New settings**, and then click **Next**.
- 3** Select **Search for network printers**.
- 4** Select **Search for USB connected devices** if you want to search for USB devices connected by USB cable to computers installed and configured with **Local Agent**.
- 5** Click **Next**.
- 6** Type the **TCP/IP port** of the device. The valid range is from 1024 to 65535.
- 7** Type the **Timeout** value (in seconds) between attempts by the application to establish a connection with the device. The valid range is from 5 to 120.
- 8** Type an **SNMP retries** value for the application retry attempts after a communication failure with the device. The valid range is from 0 to 5.

- 9** In **SNMP v1/v2**, type the **Read community name** and **Write community name**. The community names are sent with all SNMP receive and send requests, and must match the community names on the device.
- 10** For **SNMP v3** protocol, type the **User name** and **Password**.
Select **Authentication** options in the list for **None**, **SHA1**, and **MD5**.
Select **Privacy** options in the list for **None**, **AES**, and **DES**.
- 11** Select **Secure protocol (SSL)** to use Hypertext Transfer Protocol Secure (HTTPS) for the device communication. Clear the check box to use Hypertext Transfer Protocol (HTTP) for the device communication.
- 12** In **Device login**, type the **User name** and **Password**. For **Authentication mode**, choose **Local authentication** (stored in KFS Manager) or **Device settings** (stored in the device). Click **Next**.
- 13** Select **Save settings**.
- 14** Type a **Description** to a maximum of 256 alphanumeric characters. Click **Automatic registration mode** if you want to register discovered devices automatically, and then click **Next**.
- 15** Confirm the settings, and then click **Start Discovery**. Click **Back** if you want to make changes to the settings.

Selecting Saved Discovery Settings

You can select saved discovery settings and start a new discovery. The list of saved setting includes column names for **Method**, **Description**, and **Last refresh**. Before starting the discovery process, you can review the settings for discovery, communications, security and **Device login**. The discovery process may take some time to finish.

- 1** In the navigation pane, click **Devices**.
- 2** In the toolbar, click **Add devices**.
- 3** Select **Saved settings**.
- 4** Select the desired **Discovery settings**.
- 5** Click **Next**.
- 6** Click **Start Discovery**.

Editing Saved Discovery Settings

As part of the **Add devices** task, you can edit saved discovery settings and start a new discovery.

- 1 In the navigation pane, click **Devices**.
- 2 In the toolbar, click **Add devices**.
- 3 Select **Saved settings**.
- 4 Select the check box of the desired **Discovery settings**.
- 5 Click **Edit**.
- 6 In **Add Devices**, make any desired changes to the **Discovery method**. Click **Next**.
- 7 Make any desired changes to **Communication settings** and **Device login**. Click **Next**.
- 8 Select **Save settings**.
- 9 Type a **Description** to a maximum of 256 alphanumeric characters. Click **Automatic registration mode** if you want to register discovered devices automatically, and then click **Next**.
- 10 Click **Start Discovery**.

Device Registration

System Administrators or Service users can register the following devices with KFS Manager: legacy devices, devices by other manufacturers, and devices with Remote Services firmware version 1.0 or higher. The status of a device that is registered by an Administrator changes to **Pending**. To change the status to **Managed** or **Unmanaged**, the System Administrator, Manager, or a Service user must access the KFS Manager group to which the device is registered and change the device status. The status of a device that is registered by a Service user is automatically set to **Managed**.

In **Manage** connection mode, Gateway cannot discover or display devices already registered in KFS.

In **Monitor** connection mode, for devices using Remote Services firmware version 1.3 or older and registered in KFS, Gateway registers the devices as associated devices. In KFS, associated devices display as **Monitoring**.

In **Monitor** connection mode, for devices using Remote Services firmware version 1.4 or higher and registered in KFS, Gateway cannot discover or display devices already registered in KFS.

Note: A device with Remote Services firmware version 1.0 or higher can be registered with KFS Manager. For devices with Remote Services firmware version 1.0, the customer must manually enable the Remote Service feature before registering the device.

Registering Devices with Remote Services firmware

You can register discovered devices with Remote Services firmware version 1.0 or higher in KFS Manager. In Manage mode, devices with the Remote Services firmware are removed from the Gateway device discovery list as soon as they are registered with KFS Manager. In Monitor mode, devices with a Remote Services firmware version below 1.4 are registered under Gateway and are monitored like a legacy device. You can only register devices with a **Registration** status of **Not registered**. If you enable proxy settings during the device registration, any proxy settings that are saved to the device will be overwritten.

1 In the **Devices** view, select the desired devices.

2 Click **Register devices**.

3 Type your **User name**, **Password**, and **Access code**.

Note: In the **Command Center login** dialog, type your **User name** and **Password** for devices with Remote Services firmware version 1.0 and 1.1.

4 For **Connection mode**, select **Manage - Remote maintenance and Data collection** or **Monitor - Data collection only**.

Note: In **Connection mode**, you can select devices with Remote Services firmware version 1.4 or higher.

5 Type a **Description**.

6 Select **Proxy settings** if the network where Device is located uses a proxy server. Type the **Host name**, **Port**, **User name**, and **Password** of the proxy server used for proxy server authentication.

Note: Saving proxy settings overwrites any existing proxy settings in a device with Remote Services firmware version 1.2.

7 In the **Do not use proxy for following domains** text box, add domains which will not use the configured proxy settings.

8 Click **OK**.

Registering Legacy Devices and Devices by Other Manufacturers

You can register legacy devices, and devices by other manufacturers with KFS Gateway.

When a legacy device or a device by other manufacturers is registered, device information is saved in KFS Gateway and KFS Manager.

Note: After registering, the management status in KFS Manager of the legacy device or a device by other manufacturers is **Pending** or **Managed**. In KFS Manager, a System Administrator, Manager, or Service user can open the group to which the device was registered and manually change the management status to **Managed** or **Unmanaged**.

- 1 In the navigation pane, click **Devices**.
- 2 Click **Add devices** in the toolbar to discover a list of devices.
- 3 Select the legacy devices or devices by other manufacturers that are **Not registered**.
- 4 In the toolbar, click **Register devices**.
- 5 Type the **Access code**. If you logged into Gateway as an Admin user, the selected devices are registered in KFS Manager with a **Pending** management status.
- 6 Click **OK**.

KFS Gateway displays a message above the Devices list indicating devices have been registered. If unsuccessful, a message is displayed that describes possible reasons for the devices not being registered.

Device Registration Results

Gateway records device registration results in **Registration result**, regardless of registration methods and registration types. Gateway shows device registration results in a list and displays detailed information for unsuccessful registrations. Gateway can display device registration results to a maximum of 2000 devices.

Checking the Device Registration Result Details

You can view the details of a device registration result to check for device registration error information.

- 1 In the navigation pane, click **Logs**.
- 2 Click the **Registration result** tab.
- 3 Select the check box for the desired device registration result.
- 4 In the toolbar, click **Details**.
You can only view details of failed registrations. Only 1 device detail can be viewed at a time.

- 5 View the details of the device registration result in the **Details** dialog.
- 6 Click **OK**.

Deleting Device Registration Logs

You can remove device registration results from Gateway.

- 1 In the navigation pane, click **Logs**.
- 2 Click the **Registration result** tab.
- 3 Select the desired device registration results.
- 4 In the toolbar, click **Delete registration result**.
- 5 Click **OK**.

Opening Device Management for a Discovered Device

You can access the device management interface for a discovered device in Gateway. For KYOCERA devices, this will be KYOCERA Command Center. For devices by other manufacturers, this will be their device management software.

- 1 In the navigation pane, click **Devices**.
- 2 Select a check box for one device.
- 3 In the toolbar, click **Command Center**.
- 4 After KYOCERA Command Center opens in a new window, you can view device and network settings. You must log in to KYOCERA Command Center before you can apply changes to the settings.

Creating Communication Settings for a Device

You can edit communication settings for a registered device in Gateway.

- 1 In the navigation pane, click **Devices**.
- 2 Select the check box for a registered device.
- 3 In the toolbar, click **Communication settings**.
- 4 In the **Network address** list, choose the IP address for the device from the drop-down list. Devices with multiple network interface cards will display multiple IP addresses.
- 5 Type the **TCP/IP port** of the device. The valid range is from 1024 to 65535.

- 6 Type a **Timeout** value (in seconds) between attempts by the application to establish a connection with the device. The valid range is from 5 to 120.
- 7 Type an **SNMP retries** value for the application retry attempts after a communication failure with the device. The valid range is from 0 to 5.
- 8 In **SNMP v1/v2**, type the **Read community name** and **Write community name**. The community names are sent with all SNMP receive and send requests, and must match the community names on the device.
- 9 For **SNMP v3** protocol, type the **User name** and **Password**.
Select **Authentication** options in the list for **None**, **SHA1**, and **MD5**.
Select **Privacy** options in the list for **None**, **AES**, and **DES**.
- 10 Select **Secure protocol (SSL)** to use Hypertext Transfer Protocol Secure (HTTPS) for the device communication. Clear the check box to use Hypertext Transfer Protocol (HTTP) for the device communication.
- 11 In **Device login**, type the **User name** and **Password**. For **Authentication mode**, choose **Local authentication** (stored in KFS Manager) or **Device settings** (stored in the device). Click **Next**.
- 12 Click **OK**.

Searching Devices

You can use search criteria to find matching devices in the current pages of devices. The length of the search term can be within a range of 1 to 64 characters.

- 1 In the navigation pane, click **Devices**.
- 2 In the **Search** text box, type a search term.
- 3 Click the search icon.

Click **x** in the **Search** text box to clear the search value and restore the view to the original list.

6 Gateway Logs and Passwords

Logs provide valuable information about the Gateway connection to KFS Manager, device communications, system errors, discovery and wrapper operations, and debug log and Gateway master log files. Gateway also provides a change password option for instituting new passwords.

Gateway Logs

Gateway logs provide information for KYOCERA Fleet Services developers to resolve Gateway issues.

discovery result log

Contains the results of the discovery operations

connection log

Contains connection errors between Gateway and KFS Manager

system error log

Contains system errors

wrapper log

Contains log information for wrapper operations

karaf log

Contains debug logs and logs for other applications

tdrs.gw.log

Contains Gateway Master logs for all operations performed in Gateway

alerts log

Contains alert information from devices

audit log

Log contains audit records, such as:

- User authentication/identification
- Resetting of Gateway local admin password
- Configuration of device discovery settings
- Configuration of security settings

counters log

Contains counter information from devices

consumables log






Contains consumable information from devices

installation log

Contains information about the installation

Logs View Icons

The Gateway for Windows application uses the following icons for Logs.

Description	Icon
Download logs	
Delete logs	
Details	
Delete registration result	
Refresh	

Downloading Gateway Logs

You can download Gateway logs and send them to KYOCERA Fleet Services developers for troubleshooting. The logs can be downloaded in a ZIP file.

- 1 In the navigation pane, click **Logs**.
- 2 Select the check boxes for the desired logs.
- 3 Click **Download logs** in the toolbar.
- 4 Use your browser options to save the ZIP file that contains the logs.

Searching Gateway Logs

You can search Gateway logs by their name or date. The length of the search term can be within a range of 1 to 64 characters. If no search criteria are met, a message is displayed that no matches were found.

- 1 In the navigation pane, click **Logs**.
- 2 In the **Search** text box, type a search term.
- 3 Click the search icon.

Click **x** in the **Search** text box to clear the search value and restore the view to the original list.

Deleting Gateway Logs

You can delete Gateway logs.

- 1 In the navigation pane, click **Logs**.
- 2 Select the Gateway logs you want to delete.
Select logs by **Name** or **Date created**. Click the column name head for **Name** or **Date created** then select logs after sorting.
Selects logs in groups. Change the view box to 10, 25, 50, or 100. Use the check box in the title bar to select all logs in the view.
- 3 In the toolbar, click **Delete logs**.
- 4 Click **OK**.

Changing a Password

You can change your password in Gateway. Passwords require a length between 8 and 20 ASCII characters with at least one upper case letter (A - Z), one number (0 - 9), and one symbol. Users will not be logged out after the change.

- 1 In the navigation pane, click **Change password**.
- 2 Enter your current password in the **Old Password** text box.
- 3 In the **New password** text box, enter a new password.
- 4 In the **Confirm new password** text box, enter the new password again.
- 5 Click **Save**.

7 Local Agent






Local Agent lets you discover a device that is connected to a computer by a USB cable and register the device to KFS Manager using Gateway. Local Agent retrieves information from the USB connected device and stores the data in Gateway.

You must discover the computer using **Add PC** in the **Local Agent** view. You can search for computers within the domain or workgroup where Gateway is located, by host name, IP address, or IP address range. The discovered computer is added to the **Local Agent** view. You can discover up to 2000 computers in Gateway. Computers that have previously been discovered are not added to the search results.


Local Agent installers are downloaded from KFS Manager and stored in Gateway. You will receive an error message if the version of the Local Agent installer that you are downloading from KFS Manager is older than the installer package stored in Gateway. The installer is downloaded to the **<Gateway for Windows installation directory>\data\localagent** folder. You can also manually run the installer and install Local Agent to a discovered computer so you can discover a device connected to that computer. Local Agent is supported with Gateway for Windows only.

Local Agent View Icons

The Gateway for Windows application uses the following icons for **Local Agent**.

Description	Icon
Add PC	
Download Local Agent	
Install Local Agent	
Upgrade Local Agent	
Uninstall Local Agent	

— continued

Description	Icon
Refresh	

Downloading the Local Agent Installer

You can download the **Local Agent** installer from KFS Manager and save the installer in Gateway.

- 1 In the **Local Agent** view, click **Download Local Agent**.
- 2 In the **Download Local Agent** confirmation dialog, click **OK**.

Note: The Local Agent installer is saved in the <Gateway for Windows installation directory>\data\localagent folder.

Installing Local Agent Manually

You can install Local Agent manually.

- 1 In the **Local Agent** view, click **Download Local Agent**. The installer is saved in the <Gateway for Windows installation directory>\data\localagent folder.
- 2 Copy the **localagent** folder to a USB drive.
- 3 Click **KyoceraAgent.msi** file located in the folder.
- 4 Run the wizard to install Local Agent.
- 5 Click **Start**, type **services.msc**, and then press **Enter**. Confirm that Local Agent is running.

Installing Local Agent from Gateway

You must install Local Agent to a discovered computer before you can discover a USB device connected to that computer. Also, when you want to install Local Agent to target computer remotely, you need some configurations. As for the configuration, please refer **Configuring the Computer for Local Agent Installation** and **Disabling UAC Remote Restrictions in Windows**.

- 1 In the **Local Agent** view, select the target computer.
- 2 Click **Install Local Agent**, and then click **Next**.
- 3 In the **Local Agent Installation** dialog, type the **Domain name** where the target computer is located.
- 4 Type the **User name** of the account that you are using to log in to the target computer.

- 5 Type the **Password** of the user account, and then click **OK**.

After the installation, Local Agent retrieves information from the connected USB device and sends the data to Gateway.

Configuring the Computer for Local Agent Installation

You must configure the target computer before installing, upgrading or uninstalling Local Agent remotely.

Make sure that Microsoft .NET Framework version 3.5 is installed on the target computer. Microsoft .NET Framework version 3.5 includes version 2.0 of the Common Language Runtime environment, which is needed to install Local Agent. Microsoft .NET Framework version 3.5 is not automatically installed with Windows 8 or higher. You must install Microsoft .NET Framework 3.5 if the target computer runs Windows 8 or higher.

Disabling UAC Remote Restrictions in Windows

You may need pre configure the target computer before installing, upgrading or uninstalling Local Agent remotely. Some Windows operating systems, such as Windows 10, require disabling the UAC remote restrictions. This task requires using the **Registry Editor** to modify the registry. Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any data on the computer.

- 1 Click **Start**, type **regedit** in the **Search programs and files** box, and then press **Enter**.
- 2 Locate and then click the following registry subkey:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
- 3 If the **LocalAccountTokenFilterPolicy** registry entry does not exist, create one by following these steps: In the **Edit** menu, click **New**, and then click **DWORD Value**. Type **LocalAccountTokenFilterPolicy**, and then press **Enter**.
- 4 Right-click **LocalAccountTokenFilterPolicy**, and then click **Modify**.
- 5 In the **Value data** box, type **1**, and then click **OK**.
- 6 Exit **Registry Editor**.

Discovering a Computer within a Domain

The discovered computers within a selected domain name or workgroup can be added to the **Local Agent** view. Discovery of USB connected devices requires installation and configuration of a **Local Agent** on a PC which connects by USB cable to the USB device.

- 1 In the **Local Agent** view, click **Add PC**.
- 2 In **Discovery method**, select **Search current domain**.

- 3 Click **Start Discovery**.

Discovering a Computer using Host Name

The discovered computers for a selected host name can be added to the **Local Agent** view. You can add a maximum of 100 host names per discovery. Discovery of USB connected devices requires installation and configuration of a **Local Agent** on a PC which connects by USB cable to the USB device.

- 1 In the **Local Agent** view, click **Add PC**.
- 2 In **Discovery method**, select **Host name**.
- 3 Enter the **Host name** of the desired computer, and then click **Add**. To discover another computer by **Host name**, repeat this step.
- 4 Click **Start Discovery**.

Discovering a Computer using an IP Address

The discovered computers located for a selected IP address can be added to the **Local Agent** view. You can add a maximum of 100 IP addresses per discovery. Discovery of USB connected devices requires installation and configuration of a **Local Agent** on a PC which connects by USB cable to the USB device.

- 1 In the **Local Agent** view, click **Add PC**.
- 2 In **Discovery method**, select **IP address**.
- 3 Enter the **IP address** of the desired computer, and then click **Add**. To discover another computer by **IP address**, repeat this step.
- 4 Click **Start Discovery**.

Discovering a Computer within an IP Address Range

The discovered computers located within an **IP address range** can be added to the **Local Agent** view. You can add a maximum of 10 IP address ranges per discovery. Discovery of USB connected devices requires installation and configuration of a **Local Agent** on a PC which connects by USB cable to the USB device.

- 1 In the **Local Agent** view, click **Add PC**.
- 2 In **Discovery method**, select **IP address range**.
- 3 Type the **IP address range**. To discover another computer by **IP address range**, repeat this step.
- 4 Click **Start Discovery**.

Local Agent Upgrades

You can upgrade Local Agent by installing a newer version of the Local Agent software in the target computer. You can download Local Agent installer packages from KFS Manager. The installer is saved in the **<Gateway for Windows installation directory>\data\localagent** folder. During the download, Gateway compares the version of the installer package that is stored in this folder with the version of the installer package that you are downloading. The download proceeds if the version of the Gateway installer package in the folder is older than the version of the installer package that you are downloading. When you want to upgrade Local Agent software manually, you do not need a configuration in advance on the target computer. For remote Local Agent software upgrade, you need some configuration on the target computer.

Upgrading Local Agent from Gateway

You can upgrade an older version of Local Agent.

- 1** In the **Local Agent** view, select the target computer.
- 2** Click **Upgrade Local Agent**.
- 3** Click **Next**.
- 4** In the **Upgrade Local Agent** dialog, type the **Domain name** where the target computer is located.
- 5** Type the **User name** of the account that you are using to log in to the target computer.
- 6** Type the **Password** of the user account, and then click **OK**.

Uninstalling Local Agent from Gateway

You can uninstall Local Agent. After uninstallation, devices connected to the computer can no longer be discovered and registered by Gateway.

- 1** In the **Local Agent** view, select the target computer.
- 2** Click **Uninstall Local Agent**.
- 3** Click **Next**.
- 4** In the **Uninstall Local Agent** dialog, type the **Domain name** where the target computer is located.
- 5** Type the **User name** of the account that you are using to log in to the target computer.
- 6** Type the **Password** of the user account, and then click **OK**.

8 Troubleshooting

This chapter provides an overview of the troubleshooting tasks you can undertake to address Gateway issues.

Checking the JRE Connection

If you cannot access Gateway for Windows after installation, ensure that the path for the JAVA_HOME Environment variable points to the correct Java Runtime Environment (JRE) installation directory.

- 1 Click **Start**, type **services.msc**, and then press **Enter**.
- 2 In **Services**, select **Gateway for Windows**, and then click **Stop**.
- 3 Click **Computer > Properties > Advanced system settings > Advanced tab > Environment Variables** and check if the JAVA_HOME variable is using the correct Java installation directory.
- 4 In **Services**, select **Gateway for Windows**, and then click **Start**.
- 5 Type **https://localhost:8443/gatewayapp** in your browser to check if Gateway for Windows is accessible.

To access Gateway for Windows from a different computer, type **https://<IPaddress>:8443/gatewayapp** in your browser, where the **IP address** matches the one on the computer where Gateway for Windows is installed.

Note: You can also use these steps to check the JRE connection if you installed Gateway for Windows with JRE 7 and you are upgrading to a newer JRE version. Gateway will automatically use the latest JRE version.

Configuring Ports for Legacy Device Firmware Upgrades

It may be necessary to change the **Gateway Port** used for firmware upgrades of legacy devices.

- 1 In your Windows desktop, click **Start > Control Panel > System and Security > Windows Firewall > Check Firewall status**.
- 2 Select **Advanced Settings**.
- 3 Select **Inbound Rules** and then verify the **Gateway Port** uses the correct port. The port number is displayed in the **Local Port** column.
- 4 To set a new port, click **Inbound Rules > New Rule**.

- 5 In the **Rule Type** dialog, select **Port**, and then click **Next**.
 - 6 In the **Protocol and Ports** dialog, select **TCP**.
 - 7 Select **Specific local ports** and then type the port number found in the FirmwareUpgradePort.properties file. Click **Next**.
-
- Note:** The file can be found in this location: <Gateway Win installation directory>\data (e.g. C:\Program Files (x86)\Kyocera\Gateway for Windows\data)
-
- 8 In the **Action** dialog, select **Allow the connection**, and then click **Next**.
 - 9 In the **Profile** dialog, select all the rule applications, and then click **Next**.
 - 10 Type a Name for the new rule, and then click **Finish**.

Restarting a Gateway

System Administrators, Managers, and Service users can restart one or more Gateways. Closing the progress window does not stop the Gateway restart process.

- 1 In the **Devices** view, click **Gateway**.
- 2 In the **Group name** list, select the desired group.
- 3 Select one or more Gateways, and then click **Restart**.
- 4 Select **Notifications** if you want to receive an email notification.
- 5 Click **Restart**.

Restarting the Gateway for Windows service

If Gateway cannot connect to KFS Manager correctly, restarting the **Gateway for Windows** service may solve the issue.

- 1 Click **Start**, type **services.msc**, and then press **Enter**.
- 2 In **Services**, right-click **Gateway for Windows**, and select **Restart**.

Changing the Startup Type

If you cannot start the Gateway for Windows service after starting up your computer, you can change the Startup type for the Gateway for Windows service.

- 1 Click **Start**, type **services.msc**, and then press **Enter**.

- 2** In **Services**, right-click **Gateway for Windows**, and then click **Properties**.
- 3** In the **General** tab, click the **Startup** type in the drop-down menu, and then select **Automatic (Delayed Start)**.
- 4** Click **Apply**, and then close the window.
- 5** In **Services**, select **Gateway for Windows**, and then click **Start**.

KYOCERA Document Solutions America, Inc.**Headquarters**

225 Sand Road,
Fairfield, New Jersey 07004-0008, USA
Phone: +1-973-808-8444
Fax: +1-973-882-6000

Latin America

8240 NW 52nd Terrace Dawson Building, Suite 100
Miami, Florida 33166, USA
Phone: +1-305-421-6640
Fax: +1-305-421-6666

KYOCERA Document Solutions Canada, Ltd.

6120 Kestrel Rd., Mississauga, ON L5T 1S8,
Canada
Phone: +1-905-670-4425
Fax: +1-905-670-8116

KYOCERA Document Solutions**Mexico, S.A. de C.V.**

Calle Arquimedes No. 130, 4 Piso, Colonia Polanco
Chapultepec, Delegacion Miguel Hidalgo,
Distrito Federal, C.P. 11560, México
Phone: +52-555-383-2741
Fax: +52-555-383-7804

KYOCERA Document Solutions Brazil, Ltda.

Alameda África, 545, Pólo Empresarial Consbrás,
Tamboré, Santana de Parnaíba, State of São Paulo, CEP
06543-306, Brazil
Phone: +55-11-2424-5353
Fax: +55-11-2424-5304

KYOCERA Document Solutions Chile SpA

Jose Ananias 505, Macul. Santiago, Chile
Phone: +562-2350-7000
Fax: +562-2350-7150

KYOCERA Document Solutions**Australia Pty. Ltd.**

Level 3, 6-10 Talavera Road North Ryde N.S.W, 2113,
Australia
Phone: +61-2-9888-9999
Fax: +61-2-9888-9588

KYOCERA Document Solutions**New Zealand Ltd.**

Ground Floor, 19 Byron Avenue, Takapuna, Auckland,
New Zealand
Phone: +64-9-415-4517
Fax: +64-9-415-4597

KYOCERA Document Solutions Asia Limited

13/F., Mita Centre, 552-566, Castle Peak Road Tsuen Wan,
New Territories, Hong Kong
Phone: +852-2496-5678
Fax: +852-2610-2063

KYOCERA Document Solutions**(China) Corporation**

8F, No. 288 Nanjing Road West, Huangpu District,
Shanghai, 200003, China
Phone: +86-21-5301-1777
Fax: +86-21-5302-8300

KYOCERA Document Solutions**(Thailand) Corp., Ltd.**

335 Ratchadapisek Road, Wongsawang, Bangsue,
Bangkok 10800,
Thailand
Phone: +66-2-586-0333
Fax: +66-2-586-0278

KYOCERA Document Solutions**Singapore Pte. Ltd.**

12 Tai Seng Street #04-01A,
Luxasia Building, Singapore 534118
Phone: +65-6741-8733
Fax: +65-6748-3788

KYOCERA Document Solutions**Hong Kong Limited**

16/F., Mita Centre, 552-566, Castle Peak Road Tsuen Wan,
New Territories, Hong Kong
Phone: +852-3582-4000
Fax: +852-3185-1399

KYOCERA Document Solutions**Taiwan Corporation**

6F., No.37, Sec. 3, Minquan E. Rd.,
Zhongshan Dist., Taipei 104, Taiwan R.O.C.
Phone: +886-2-2507-6709
Fax: +886-2-2507-8432

KYOCERA Document Solutions Korea Co., Ltd.

#10F Daewoo Foundation Bldg 18, Toegye-ro, Jung-gu,
Seoul, Korea
Phone: +822-6933-4050
Fax: +822-747-0084

KYOCERA Document Solutions**India Private Limited**

Second Floor, Centrum Plaza, Golf Course Road,
Sector-53, Gurgaon, Haryana 122002, India
Phone: +91-0124-4671000
Fax: +91-0124-4671001

KYOCERA Document Solutions Europe B.V.

Bloemlaan 4, 2132 NP Hoofddorp,
The Netherlands
Phone: +31-20-654-0000
Fax: +31-20-653-1256

KYOCERA Document Solutions Nederland B.V.

Beechavenue 25, 1119 RA Schiphol-Rijk,
The Netherlands
Phone: +31-20-5877200
Fax: +31-20-5877260

KYOCERA Document Solutions (U.K.) Limited

Eldon Court, 75-77 London Road,
Reading, Berkshire RG1 5BS,
United Kingdom
Phone: +44-118-931-1500
Fax: +44-118-931-1108

KYOCERA Document Solutions Italia S.p.A.

Via Monfalcone 15, 20132, Milano, Italy,
Phone: +39-02-921791
Fax: +39-02-92179-600

KYOCERA Document Solutions Belgium N.V.

Sint-Martinusweg 199-201 1930 Zaventem,
Belgium
Phone: +32-2-7209270
Fax: +32-2-7208748

KYOCERA Document Solutions France S.A.S.

Espace Technologique de St Aubin
Route de l'Orme 91195 Gif-sur-Yvette CEDEX,
France
Phone: +33-1-69852600
Fax: +33-1-69853409

KYOCERA Document Solutions Espana, S.A.

Edificio Kyocera, Avda. de Manacor No.2,
28290 Las Matas (Madrid), Spain
Phone: +34-91-6318392
Fax: +34-91-6318219

KYOCERA Document Solutions Finland Oy

Atomitie 5C, 00370 Helsinki,
Finland
Phone: +358-9-47805200
Fax: +358-9-47805212

KYOCERA Document Solutions**Europe B.V., Amsterdam (NL) Zürich Branch**

Hohlstrasse 614, 8048 Zürich,
Switzerland
Phone: +41-44-9084949
Fax: +41-44-9084950

KYOCERA Bilgitas Document Solutions**Turkey A.S.**

Gülbahar Mahallesi Otello Kamil Sk. No:6 Mecidiyeköy
34394 Şişli İstanbul, Turkey
Phone: +90-212-356-7000
Fax: +90-212-356-6725

KYOCERA Document Solutions**Deutschland GmbH**

Otto-Hahn-Strasse 12, 40670 Meerbusch,
Germany
Phone: +49-2159-9180
Fax: +49-2159-918100

KYOCERA Document Solutions Austria GmbH

Wienerbergstraße 11, Turm A, 18. OG, 1100 Wien,
Austria
Phone: +43-1-863380
Fax: +43-1-86338-400

KYOCERA Document Solutions Nordic AB

Esbogatan 16B 164 75 Kista, Sweden
Phone: +46-8-546-550-00
Fax: +46-8-546-550-10

KYOCERA Document Solutions Norge Nuf

Olaf Helsetsv. 6, 0619 Oslo, Norway
Phone: +47-22-62-73-00
Fax: +47-22-62-72-00

KYOCERA Document Solutions Danmark A/S

Ejby Industrivej 60, DK-2600 Glostrup,
Denmark
Phone: +45-70223880
Fax: +45-45765850

KYOCERA Document Solutions Portugal Lda.

Rua do Centro Cultural, 41 (Alvalade) 1700-106 Lisboa,
Portugal
Phone: +351-21-843-6780
Fax: +351-21-849-3312

KYOCERA Document Solutions**South Africa (Pty) Ltd.**

KYOCERA House, Hertford Office Park,
90 Bekker Road (Cnr. Allandale), Midrand, South Africa
Phone: +27-11-540-2600
Fax: +27-11-466-3050

KYOCERA Document Solutions Russia LLC.

Building 2, 51/4, Schepkina St., 129110, Moscow,
Russia
Phone: +7(495)741-0004
Fax: +7(495)741-0018

KYOCERA Document Solutions Middle East

Dubai Internet City, Bldg. 17,
Office 157 P.O. Box 500817, Dubai,
United Arab Emirates
Phone: +971-04-433-0412

KYOCERA Document Solutions Inc.

2-28, 1-chome, Tamatsukuri, Chuo-ku
Osaka 540-8585, Japan
Phone: +81-6-6764-3555
<http://www.kyoceradocumentsolutions.com>