KYOCERA

kyoceradocumentsolutions.com

# KYOCERA Fleet Services NetGateway
## User Guide

## Legal notes



## Regarding trademarks

# Table of Contents

# 1 Product Overview

NetGateway simplifies the registration of devices with KYOCERA Fleet Services so the devices can be managed and monitored. As a Microsoft .NET platform application, it can be configured to discover devices on a schedule or automatically. KYOCERA devices, legacy devices, and devices by other manufacturers are supported. The software solution includes a local agent that can be downloaded and installed on a remote computer. With the local agent, you can discover a device that is connected to the computer by a USB cable and register the device in KFS. Local agent retrieves information that is necessary for KFS to monitor or manage the USB-connected device.

## Documentation set

KYOCERA Fleet Services

| Guide | Description |
|---|---|
| KYOCERA NetGateway User Guide | Describes the settings, configurations, and concepts in NetGateway for registering devices in KFS. It also provides information about local agent installation and use. |
| KYOCERA Fleet Services User Guide | Describes a comprehensive device management solution in the cloud. You can monitor and manage KYOCERA devices and devices by other manufacturers. Some of the remote monitoring features include device counter collection, reporting, device monitoring, consumable status, and ordering. Task management activities include remote firmware upgrades, device diagnostics and troubleshooting, remote setup and maintenance. |

## Conventions

The following conventions may be used in this guide:

- **Bold text** is used for menu items and buttons
- Screen, text box, and drop-down menu titles are spelled and punctuated exactly as they are displayed on the screen
- *Italics* are used for document titles
- Text or commands that a user enters are displayed as text in a different font or in a text box as shown in these examples:

1. On the command line, enter `net stop program`
2. Create a batch file that includes these commands:

```
net stop program
gbak -rep -user PROGRAMLOG.FBK
```

- Icons are used to draw your attention to certain pieces of information. Examples:

This indicates information that is useful to know.

This indicates important information that you should know, including such things as data loss if the procedure is not done properly.

## System requirements

Refer to the *Release Notes* that accompany this product.

## System Overview

NetGateway provides a simple method to register KYOCERA devices, legacy devices, and devices by other manufacturers to KYOCERA Fleet Services (KFS). NetGateway is a .NET based agent that connects with KFS to monitor devices. You can register devices automatically as part of discovery. You can configure periodic device discovery to register devices automatically and update device information for registered devices. A device in pending status can be re-registered in KFS.

NetGateway can be registered to a group with a configuration key or with an Access code and KFS Manager authentication (User name and Password). The configuration key is generated for a group and sent by email to the NetGateway user. Once the NetGateway is registered, devices can be registered to the associated group.

If a device is registered by NetGateway with an Access code, then the device is displayed in pending status. A device in pending status can be re-registered by another NetGateway. If the NetGateway user includes KFS Manager authentication (User name and Password) for device registration and the Access code, then the registered device is displayed in managed status.

You can delete or archive NetGateway within KFS. To identify your NetGateway instance, open the NetGateway Status drop-down and then select **View NetGateway information**.

## Support information

NetGateway provides two methods for communicating device information to KFS based on the device registration method. The first method applies to devices registered as a Gateway device. In this way, NetGateway periodically retrieves information from devices, including devices by other manufacturers, and then sends the information to KFS. The second method applies to devices registered as a

KFS device with single point of communication. In this case, the device itself sends information to KFS via NetGateway which acts like a proxy server.

Based on the device registration method, the maximum number of supported devices varies.

| Device registration method | Supported devices (max.) |
|---|---|
| Gateway device | 2000 |
| KFS device with single point of communication | 300 |

# 2 Installation and Registration

## Installing NetGateway

The NetGateway installer can be downloaded from KFS or accessed via a link sent by a KFS user in an email. The email link includes a configuration key that is associated with a specific group in KFS.

1. Select the NetGateway installer filename.
2. Select the destination folder.
3. Select **Next**.
4. Select a synchronization option for device discovery settings.

   **Synchronize discovery settings with KFS (recommended)**

   Device identification will be shared with KFS.

   **Manually configure discovery settings**

   Device identification will not be shared with KFS.
5. Select **Next**.
6. Select **Install**.

   If a stored NetGateway database is found, you must decide where to import it.
7. Select **Finish**.

   If the Start application check box is selected, NetGateway opens to the license agreement which can be viewed or downloaded.
8. Select **Accept & Continue**.

The synchronization option cannot be changed after installation.

## Configuration keys

Configuration keys provide a quick method for registering NetGateway with a group in KFS. In KFS, a System administrator can send a link to the Gateway installer in an email. The NetGateway registration email includes both a download link for the NetGateway installer package and a configuration key that can be used to register the NetGateway. Once the software is installed, the configuration key can be pasted into the Automatic registration section of NetGateway setup. The key is associated with a group in KFS and discovery settings. If the key is not used within 7 days, it expires.

The alternative method for using a configuration key is manual registration.

## Registering NetGateway manually

You can register NetGateway using manual registration. The two requirements for this setting include the URL and an Access Code which is associated with a group.

1. In NetGateway Setup, select **Direct connection**.
2. Or, select the **Use HTTP Proxy** check box, enter the **Host name** and **Port**. Select **Enable authentication** and enter your **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 NetGateway. If you do not select proxy settings, then these settings are disabled when you register devices.

   A maximum 300 devices is supported for single point of communication.

3. Select **Next**.
4. Select **Manual registration**.
5. Enter the KFS **URL** and **Access code**.
6. Enter a **Description**.
7. Enter **KFS Manager authentication** as an option.
8. Enter your KFS **User name** and **Password**.
9. For registering KFS devices, select from two options:

   **Manage**

   Maintains open and constant bidirectional communication between KFS and KFS devices. This option supports real-time device status and alert updates.

   **Monitor**

   Communicates counter and consumable information in one direction through HTTPS to the KFS device rest server. KFS does not communicate directly with the devices.

10. Alternatively, select **Register KFS devices as legacy devices** to register the devices under NetGateway. In the device list, the registration type is shown as Gateway.
11. Select **Next**.
12. Review your settings and select **Complete setup and start NetGateway**.

# Device discovery and registration

You can register devices individually or in groups by selecting them from the discovered devices in the NetGateway list and selecting Register devices in the toolbar. You can enter the Access code to place the selected devices in Pending status. To set Managed status, you must enter the Access code associated with a group, select Manager authentication then enter your Manager-level User name and Password.

## Adding devices

1. Select **Add Devices** > **Add devices now**.
2. Select a **Discovery method**. The target varies based on the selected method. You cannot add duplicate host names, IP addresses, or IP address ranges. Select the plus button to add more addresses, address ranges, or host names.

   **By local network**

   Discovery of computers in a workgroup or local domain. You can select both IPv4 and IPv6.

   **By IP address or host name**

   Discovery of computers based on an IP address or host name of the devices. You can specify 200 IP addresses or host names.

   **By IP address range**

   Discovery of computers based on the specified IP address range. You can specify 10 IP address ranges.
3. For the discovery of USB devices, select **Discover USB-connected devices**.
4. Enter the **TCP/IP port**. The valid range is from 1024 to 65535.
5. Select **Enable SSL protocol** to use Hypertext Transfer Protocol Secure (HTTPS) for device communication.
6. For Communication timeout (seconds), enter a value between 5 and 120.
7. For SNMP connection retries, enter a value between 0 and 5.
8. If using the SNMPv1/v2 protocol, enter the **Read community name** and **Write community name** in the text boxes. 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.
9. If using the SNMPv3 protocol, enter the **User name** and **Password**, and **Context name**.

   Select **SNMP Authentication** options in the list for **SHA1** or **MD5**.
   Select **SNMP Privacy** options in the list for **AES** or **DES**.

10 In the second Discovery settings section of Add devices, select the **Save discovery settings** check box and enter a name for the discovery settings so you can reuse them. Discovery settings are never saved externally.

11 Select **Authentication type** as **Local authentication**, or **Device settings** (stored in the device).

12 For Authentication information, enter the **User name** and **Password**.

13 Select **Enable automatic registration** check box to register discovered devices as soon as they are discovered.

All unregistered devices discovered by NetGateway are registered when Automatic registration is selected.

14 Select **Run** to start the discovery process.

15 When the discovery process is finished, select **Close**.

Select **Reset** to set return all values to their default setting.

## Selecting saved discovery settings

You can use saved discovery settings in NetGateway.

1 Select **Add devices** > **Saved discovery settings**.

2 Select the saved discovery settings.

3 Select **Run**.

4 Select **Close** to close the dialog or select **Go to tasks** to download the detailed results of the finished task in .csv format.

You can also select **Stop** to stop the discovery process before it has finished. Once stopped, the cancellation process starts and the initial task cannot be resumed.

## Editing discovery settings

You can edit discovery settings.

1 Select **Add devices** > **Saved discovery settings**.

2 Select a saved discovery setting.

3 Select **Edit**.

4 Modify any of the existing settings.

5 Select **Save**.

### Deleting discovery settings

You can delete saved discovery settings in NetGateway.

1. Select **Add devices** > **Saved discovery settings**.
2. Select one or more of the saved discovery settings. To delete all, select the check box at the top of the left column.
3. Select **Delete**.
4. Select x to close the dialog.

## Changing the connection mode

You can change the connection mode for device monitoring and management.

1. Select **Settings** > **KFS device connection mode**.
2. For registering KFS devices, select from two options:

   **Manage**

   Maintains open and constant communication between KFS and KFS devices. This option supports real-time device status and alert updates.

   **Monitor**

   Communicates counter and consumable information through HTTPS to the KFS device rest server. KFS does not communicate directly with the devices.
3. Alternatively, select **Register KFS devices as legacy devices** to register the devices under NetGateway.
4. Select **Save**.

## NetGateway devices

NetGateway uses discovery settings to find devices and register them in KYOCERA Fleet Services (KFS) and NetGateway. Discovery settings can be created, named, and modified. NetGateway uses a variety of discovery methods (By current domain, By IP address or host name, By IP address range) to find printing devices and USB-connected devices on the network. Registered devices can be monitored or managed. Devices monitored as legacy devices only track counters, alerts, and consumables. NetGateway cannot register offline devices.

You can filter the device list by selecting any one of the color status boxes at the top.

**Offline registered**

All devices already registered in KFS but with no current connection with NetGateway.

**Not registered**

All discovered devices not registered in KFS.

**Online registered**

All discovered online devices registered in KFS.

**All discovered**

All discovered devices, except for excluded devices.

## Customizing the NetGateway device list

You can customize the device list view in NetGateway to display information you want to view immediately. The settings are not maintained after logout.

1. Select the plus sign at the top of the far right columns.
2. In addition to the default columns, you can choose from the following selections:
   - MAC address
   - Last posting result (Counters)
   - Last posting time (Counters)
   - Last posting result (Consumables)
   - Last posting time (Consumables)
   - Last posting result (Alerts)
   - Last posting time (Alerts)
   - SNMP
   - SSL

## Registering network devices in NetGateway

In NetGateway, you can discover and register network KFS devices to a group during the discovery process or select single or multiple unregistered network KFS devices.

1. In the NetGateway device list, select the check boxes of the devices to register.
2. Select **Register devices**.
3. Enter the **Access code** for the group where the devices will be registered.

   If only the Access code is provided, the devices are registered in a Pending state.

   To register devices in a Managed state, select **KFS Manager authentication**, then enter the **User name** and **Password**. This selection is optional.
4. Enter a **Description**.
5. If you are using a proxy server to communicate with KFS, select **Use proxy settings**, then enter the **Host name**, **User name**, **Port**, **Password**, and any domains you want excluded.

6 If the selected devices use supported firmware, select a Connection mode.

**Manage**

Maintains open and constant communication between KFS and KFS devices. This option supports remote maintenance, real-time device status and alert updates.

**Monitor**

Communicates counter and consumable information through HTTPS to the KFS device rest server. KFS does not communicate directly with the devices.

7 If the selected devices use older firmware, enter **User name** and **Password** for Command Center.

8 Select **Next**.

9 Select **Register**.

10 Select **Close** or **Go to tasks**.

In the Task list, you can download the registration results in .csv format. The filename uses a timestamp in its naming convention.

## Registering other devices in NetGateway

In NetGateway, you can discover and register USB-connected, legacy, competitor, NIC, and Fiery devices to a group during the discovery process or select single or multiple of the same unregistered devices.

1 In the NetGateway device list, select the USB-connected, legacy, competitor, NIC, and Fiery devices to register.

2 Select **Register devices**.

3 Enter the **Access code** for the group where the devices will be registered.

If only the Access code is provided, the devices are registered in a Pending state.

To register devices in a Managed state, select **KFS Manager authentication**, then enter the **User name** and **Password**. This selection is optional.

4 Select **Next**.

5 Select **Register**.

6 Select **Close** or **Go to tasks**.

In the Task list, you can download the registration results in .csv format. The filename uses a timestamp in its naming convention.

## Progress window for device discovery and registration

During device discovery and device registration with automatic registration, the progress window displays some of the following information:

**Time remaining**

A time estimate for the completion of discovery and registration.

**Discovered devices - new**

Displays the number of devices discovered during the current discovery.

**Deleted devices**

Displays the number of devices added to the excluded devices list as a result of the current discovery.

**Total devices**

Displays a total of all new, existing, and excluded devices.

**Total registered devices**

Displays a total of all registered devices.

## Registration status, type, and mixed devices

NetGateway applies registration settings separately based on the firmware support on the device. For a group of devices with mixed firmware types, you must add both Command Center login settings for devices with earlier firmware and Connection mode settings for devices with later firmware. If the device is registered as a legacy device, the displayed Registration status is Registered and the Registration type is Gateway. If the device with supported firmware is registered as a KFS device in manage mode, the displayed Registration status is Registered and the Registration type is Device (Managed). For registered USB-connected devices, the Registration type is Gateway.

## Using the NetGateway upgrade installer

If automatic upgrade is not enabled in the Settings menu, you can download and upgrade NetGateway from an installer file.

1. Select the NetGateway installer filename.
2. Select **Yes** in response to the User Access Control (UAC) notification. On some systems, this notification may not appear.
3. You can choose a different folder than the default Destination folder. Select **Upgrade**.
4. Select **Next**.
5. Select one of the options to **Restart now** or **Restart later**.
6. Select **Finish**.

After the system restarts, you can start NetGateway from the shortcut placed on your desktop.

# 3 Local Agent

You can download and install the local agent on remote computers. Using the local agent, you can discover a device that is connected to the computer by a USB cable and register the device in KFS. Local agent retrieves information that is necessary for KFS to monitor the USB-connected device.

In NetGateway, you can download the local agent, send a URL for local agent download to another KFS user, or install the local agent on a group of computers.

## Downloading local agent

You can download local agent and install it on your computer or a discovered computer.

1. Select **Manage computers**.
2. Select **Download local agent**.

If the version of local agent is current, the download is canceled and a message about the current status is displayed.

## Remote computer requirements

To install the local agent on remote computers, you must meet the following requirements on the remote computers:

**Administrator account privileges**

Credentials used in NetGateway's local agent connection must include administrator privileges on the remote computer/domain. The NetGateway administrator must have Administrator account privileges on the remote computer. The local user should belong to the local Administrators group. The domain user must be a domain administrator.

**Enable Remote Management**

If disabled, remote management can be enabled with a Windows PowerShell cmdlet:

```
Enable -PSRemoting - Force
```

By default, PowerShell remoting is enabled on Windows Server platforms.

**Enable WMI traffic using the Windows Firewall UI**

Inbound rules in the Windows Management Instrumentation (WMI) must be enabled in accordance with the network type.

**Installed Microsoft .NET Framework 2.0**

Computers that use the local agent must meet this requirement. In Windows, the .NET Framework is installed and enabled by default.

## Modifying the local agent connection

The settings for the local agent connection are saved once they have been entered. When the connection settings are opened next, you can modify the settings for the following:

1. Select **Manage computers**.
2. Select **Local agent connection**.
3. Enter the **Domain name** (255-character maximum).
4. Enter the **User name** (32-character maximum).
5. Enter the **Password** (32-character maximum).
6. Select **OK**.

## Adding computers and installing local agent

1. Select **Manage computers**.
2. Select **Add computers**.
3. Select **By current domain**, **By host name**, **By IP address**, or **By IP address range**.
4. Depending on the Target selection, enter a host name, IP address, or address range, and then select the + icon.
5. Select **Start discovery**.
6. After computers have been discovered, select one or more computers in the list.
7. Select **Install/upgrade local agent**.
8. Select **Install**.

You can discover a maximum of 2000 computers in NetGateway for installing the local agent. In the computer list, you can view the IP address, Host name, and Local Agent version.

In the Task list, you can download the results in .csv format. The filename uses a timestamp in its naming convention.

## Installing the local agent manually

You can download the local agent for registering USB-connected devices in KFS.

1. Select **Settings** > **Download local agent**.
2. In the download location, open the installer package.

## Upgrading local agent

You can upgrade local agent. If the local agent version is current, the application displays a message. If multiple computers require local agent upgrades, they are upgraded in parallel.

1. Select **Manage computers**.
2. Select one or more computers in the list.
3. Select **Install/upgrade local agent**.
4. Select **Install**.

## Uninstalling local agent

1. Select **Manage computers**.
2. Select one or more computers in the list.
3. Select **Uninstall local agent**.
4. Select **Uninstall**.

## Copying the local agent URL

You can send the NetGateway local agent by copying the URL and sending it by email to another KFS user. The link to the local agent will enable the KFS user to install the local agent on a computer that complies with local agent requirements. With the local agent installed, the KFS user can register USB-connected devices.

1. Select **Settings** > **Copy local agent URL**.
2. Paste the URL in an email to another user and send the email.

# 4 NetGateway Management

## Device home

Devices that contain web servers can display a web page containing information about the device's status and settings. The layout and information shown on this page differ by device. You can change the settings on the device if you have administrator credentials. The device home can be accessed for a single device at a time.

1. Select a device in the NetGateway device list.
2. Select **Device home**.
3. Enter the credentials for the device to view the device home page.

If the connection to a device is not secure, you must accept the prompt about the risk.

## Selecting device settings

Device settings are unavailable for USB-connected devices and competitor devices.

1. Select one or more devices in the list. If multiple devices are selected and one device in the group is offline or has communication problems, then Device settings is disabled.
2. Select **Device settings**. If a single device is chosen and the device settings are successfully retrieved, the settings for the selected device are displayed.
3. Select the check boxes for IPv4 (wired) and IPv6 (wired) as they apply to your network.
4. Select **Security settings** as they apply to your network. These settings include Client encryption settings, SSL client TLS version, Client hash, SSL certificate validation, and Hash.
5. Select **Apply**.

## Synchronizing Firmware tasks

NetGateway supports the capacity to upgrade device firmware based on Automatic firmware upgrade tasks configured in KFS. NetGateway reports the status to KFS as the upgrade is processed, completed, or failed.

1. Select **Settings**.

2 Select the **Scheduled tasks** check box to enable synchronization. When selected, synchronization is run for firmware tasks immediately then on a schedule of every three hours.

## Excluded devices

Devices that have been deleted or archived from KFS are displayed in the NetGateway excluded devices list. Excluded devices cannot be discovered or registered by the same NetGateway. Once deleted or archived, the devices move to the excluded devices list when the NetGateway service is restarted or when other devices are discovered and registered or no longer than the 24-hour synchronization period. After deletion, all device data is removed from the database, except for basic device information.

Any excluded devices can be included in the discovery and registration process again. You must select them in the excluded devices list and return them to the list of discoverable devices in NetGateway.

### Making excluded devices discoverable

You can add an excluded device to the list of discoverable devices in NetGateway.

1 Select **Excluded devices**.

2 Select one or more excluded devices.

3 Select **Include device**.
The selected excluded devices are removed from the list.

4 Select x to close the list.

The list of excluded devices can be sorted by selecting the column heading.

## Download task results

You can download task results in NetGateway. The View tasks button displays in both the device list and the local agent list views. The detailed results are saved in .csv format to your default download folder.

1 Select **View tasks**.

2 Select one task result in the list.

3 Select **Download**.

You can search the Task list by typing a search term in the search text box. The number of items displayed in the list can be set in increments of 15, 25, 50, 100.

## Refresh the NetGateway device and computer lists

You can refresh the NetGateway device and computer lists. When you select the Refresh icon, a blue border displays until the refresh process is finished. The items in the list are updated including ones below the visible field of view.

## Changing communication settings

You can change communication settings for a single device and multiple devices. You can also view communication settings for a single device. Select the device and select **Communication settings**.

If you select multiple devices and Communication settings, the template values are displayed. You can discover devices by other manufacturers by using Context name with SNMPv3. Context name is not available for SNMPv1/v2.

1. In the NetGateway device list, select one or more devices.
2. Select **Communication settings**.
3. Enter the **TCP/IP port**.
   The valid range is from 1024 to 65535.
4. Select **Enable SSL protocol** to use Hypertext Transfer Protocol Secure (HTTPS) for device communication.
5. For Communication timeout (seconds), enter a value between 5 and 120.
6. For SNMP connection retries, enter a value between 0 and 5.
7. If using the **SNMPv1/v2** protocol, enter the **Read community name** and **Write community name** in the text boxes.
   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.
8. If using the **SNMPv3** protocol, enter the **User name**, **Password**, and **Context name**.
   For SNMP authentication options, select from **SHA1** or **MD5**.
   For SNMP privacy options, select from **AES** or **DES**.
9. Select **Authentication type** as **Local authentication**, or **Device settings** (stored in the device).
10. For Authentication information, enter the **User name** and **Password**.
11. Select **Save**.

## Changing proxy settings

You can change the proxy settings to select direct connection or HTTP Proxy. If proxy settings were not selected when the NetGateway was registered, then these settings are unavailable.

1. Select **Settings** > **Proxy settings**.
2. Select **Direct connection** or **Use HTTP Proxy**.
3. For the proxy setting, you can enter a **Host name** and **Port name**. You can also select **Enable authentication** and enter your **User name** and **Password**.
4. Select **Use Gateway as a single point of communication** if you want devices with Remote Services firmware to communicate with KFS through NetGateway.

   A maximum 300 devices is supported for single point of communication.

5. Select **Save**.

## Creating automatic upgrade settings

You can create automatic upgrade settings in NetGateway. This method provides an alternative to upgrading NetGateway from a downloaded update installer.

1. Select **Settings** > **Automatic upgrade**.
2. Select **Enable automatic software upgrade**.
3. Select a schedule for the update: **Daily (at the time NetGateway was registered)** or at a **Specified time**.
4. Select **Apply**.

When an upgrade fails, an error message is displayed in the Automatic upgrade settings window and the upgrade is retried at the same time on the following day.

## NetGateway system logs

System logs contain all of the development log files generated in the last 24 hours. An additional file with a detailed summary of task results committed in the last 24-hour period is also included. This System log filename uses a timestamp. The file contains details about all discovery and device registration tasks and other NetGateway postings. The collection is downloaded in a .zip format.

### Downloading a system log

You can download a System log from the Settings menu in NetGateway.

1. Select **Settings** > **Logs**.

2 Select **System log**.

3 Select **Download**.

4 If necessary, select **OK** to save the log to your computer.

5 Select **Close**.

## NetGateway audit logs

An audit log is a document that records events in a system. In addition to documenting resources accessed, audit log entries include destination and source addresses, a timestamp and user login information. The audit log is maintained for one week.

NetGateway records the following events in the audit log:

- User authentication
- User logout
- User password change
- Add discovery settings
- Delete discovery settings
- Edit discovery settings
- Gateway registration
- Device registration
- Change proxy setting
- Auto Gateway upgrade
- Change of device IP address
- Add device
- Delete device
- Start application
- Shutdown application
- Auto device registration

### Download audit logs

You can download an Audit log from the Settings menu in NetGateway.

1 Select **Settings** > **Logs**.

2 Select **Audit log**.

3 Select **Download**.

4 Select **Close**.

## NetGateway connection status

NetGateway displays one of three connection states.

**Monitoring now**

NetGateway is connected to KFS and has retrieved information about registered devices.

**Processing**

NetGateway is running an active task such as device discovery, device registration, posting logs, or other tasks to KFS.

**Offline**

NetGateway has no connection with KFS. An offline state may be caused by a poor connection or Proxy server issues.

## Viewing NetGateway information

In the NetGateway information menu, you can view general information about NetGateway, KFS, versions, IPv4, and IPv6 settings. Select **Close** to exit the display.

## NetGateway passwords

You can change the password in NetGateway. Only letters, numbers, and symbols may be used. The password requires the following parameters:

- 8 characters in length or longer (64-character length maximum)
- At least one uppercase letter (A-Z)
- At least one number (0-9)
- At least 1 symbol (special character)

If any of the password requirements are unmet, the system displays a message about the missing requirement in red text.

If you forget your password, you can use the option on the login page to reset your password.

### Changing passwords

You can change the password in NetGateway.

1. Select **Admin** > **Change password**.
2. Enter the **Old password**.
3. Enter the **New password**.
4. In Confirm password, enter the new password.
5. Select **Save**.

If any of the password requirements are not met, the system displays a reminder of the missing requirement in red text.

## Resetting login for lost passwords

If you have lost or forgotten your password, you can reset it.

1. On the login page, select **I forgot my password**.
2. Enter your **Access code** and select the **KFS Manager authentication** check box.
3. Enter your **User name** and **Password**.
4. Select **Reset**.

# NetGateway reset

After a NetGateway has been archived or deleted, NetGateway is reset and the database is removed. To use NetGateway again, you must register it again, which includes accepting the End User License Agreement and finishing the setup.

For the KYOCERA contact in your region, see Sales Sites sections here

ご利用の地域でのお問い合わせ先については、下記リンクから京セラ本支店・営業所の一覧をご覧ください。

https://www.kyoceradocumentsolutions.com/company/directory.html



KFSNGUGKDEN200.2022.12