kyoceradocumentsolutions.com

Device Manager

Installation and Upgrade Guide

Legal notes

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

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

Regarding trademarks

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

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

Table of Contents

Chapter 1 Product overview

Documentation........ 1-1
Conventions........ 1-1
System requirements........ 1-2
  Prerequisites........ 1-2
  Supported operating systems........ 1-3
  Supported browsers........ 1-3
  Standard configuration hardware requirements........ 1-3
  Installation checklist........ 1-4

Chapter 2 SQL database installation and setup

Installing SQL Server Express edition........2-1
Installing SQL Server Enterprise edition........ 2-1
Installing SQL Server Management Studio........ 2-2
Configure SQL Server with SSMS........ 2-2
  Selecting a database instance........ 2-2
  Setting up authentication........ 2-3
  Adding a domain user........ 2-3

Chapter 3 Device Manager installation and setup

Installing Device Manager........ 3-1
Firewall configuration........ 3-1
Upgrading Device Manager........3-3
Connecting Device Manager to the database........3-3
  Troubleshooting SQL connection error........3-4
Making a domain user a local administrator........ 3-5
Additional configuration items........3-5

Chapter 4 Local Device Agent

Disabling Status Monitor........4-1
Installing LDA........4-2
Discovering USB-connected devices........4-2

1 Product overview

Device Manager is a server-based application that lets you monitor and manage printing devices. With this application, you can:

- Configure device settings
- Install applications on one or more devices
- Receive automated alert messages
- Check toner levels
- Upgrade firmware
- Generate device reports
- Arrange devices in groups

Features and options may vary depending on your device.

Documentation

Installation and Upgrade Guide

Provides instructions on how to install Device Manager, and configure this application to an internal or external database.

This guide is for IT professionals, and non-IT personnel with knowledge of database installation and configuration.

- This guide includes instructions on installing and configuring Microsoft SQL Server Enterprise and Express editions. Follow these instructions if you prefer to use Device Manager with an external database.
- This guide is not intended to replace the official documentation for Microsoft SQL. For more information, refer to the documentation in the Microsoft website.

User Guide

Provides instructions on how to use the features and settings of the application.

This guide is for IT administrators and service technicians.

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 is a NOTE icon. This indicates information that is useful to know.

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

System requirements

Prerequisites

- Microsoft .NET Core 2.2.6

- .NET Core installation prerequisite: Microsoft Visual C++ Redistributable for Visual Studio 2015.
- .NET Core is included in the installer package. For .NET Core to work properly, your system must have all the latest Windows updates.

- Depending on your system setup and preference, you can configure Device Manager with an internal or external database.

You can only configure Device Manager with one database.

Internal database: Embedded Firebird

This database is embedded with the application, and will be installed in the same computer as the application.

External database: Microsoft SQL Server

This database is installed and set up before installing the application. There is only one database administrator that will access the database locally.

The following versions are supported:

- SQL Server 2019
- SQL Server 2017
- SQL Server 2016

- SQL Server 2014
- SQL Server 2012
- SQL Server 2008 R2

Determine the SQL Server edition to install, based on your needs:

- Enterprise
- Standard
- Express

- This free edition has lower memory capacity compared to the Enterprise or Standard editions, with a maximum database size of 10 GB.
- For more information on the different Microsoft SQL Server editions, go to the Microsoft website.

Supported operating systems

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

Supported browsers

- Google Chrome 52 or later
- Microsoft Edge for Windows
- Firefox 53 or later
- Safari

Standard configuration hardware requirements

Recommended hardware	Number of supported devices	Database
• 4 GB RAM • 2 cores (physical) • 1.5 GHz CPU	Up to 100 devices	Internal
• 6 GB RAM • 4 cores (physical) • 3.6 GHz CPU	Up to 300 devices	Internal or external

Recommended hardware	Number of supported devices	Database
• 32 GB RAM • 8 cores • 2.2 GHz CPU • 1000 Mbps gigabit Ethernet adapter	Up to 10,000 devices	External

Installation checklist

Depending on your database preference, refer to the following chapters in the *Installation and Upgrade Guide*:

Database type	Chapters
Embedded Firebird (internal database)	*Device Manager installation and setup* Since the embedded Firebird database will be used, you do not need to install and set up Microsoft SQL Server and SQL Server Management Studio.
Microsoft SQL (external database)	**1.** *SQL database installation and setup* **2.** *Device Manager installation and setup*

2 SQL database installation and setup

Installing SQL Server Express edition

This section describes how to install Microsoft SQL Server Express edition. For more information, refer to official Microsoft documentation. If you are installing Microsoft SQL Server Enterprise edition, then go to the next section.

Steps and details may vary depending on the SQL Server version.

1. Run the installer.
2. Select the Basic option.
3. Read the license terms, and then select **Accept**.
4. Review or specify the installation location, and then select **Install**.
5. When the installation completes, select **Install SSMS**.

Installing SQL Server Enterprise edition

This section describes how to install Microsoft SQL Server Enterprise edition. For more information, refer to official Microsoft documentation. If you are installing Microsoft SQL Server Express edition, then go to the previous section.

Make sure that your product key is available.

Steps and details may vary depending on the SQL Server version.

1. Run the installer.
2. Select **Installation** > **New SQL Server stand-alone installation or add features to an existing installation**, and then follow the instructions.
3. When Install Rules completes, select **Next**.
   Ignore any warnings that may appear.
4. Select **Enter the product key**, provide the information, and then select **Next**.
5. Review the instance configuration details, and then select **Next**.
   - Accept the default instance.

- Select **Named instance**, and then provide the information.

6 In Database Engine Configuration, do the following:

a) Select an Authentication Mode:

- **Windows authentication mode**
- **Mixed Mode (SQL Server authentication and Windows authentication)**

> Specify a password for the SQL Server system administrator.

b) Manage the SQL Server administrator accounts:

- To add the active user currently logged onto the computer, select **Add Current User**.
- To add a different user, select **Add**.
- To remove, select an entry from the list, and then select **Remove**.

c) Select **Next**.

7 In Ready to Install, review your settings, and then select **Install**.

8 When the installation completes, select **Next** > **Close**.

In SQL Server Installation Center, select **Install SQL Server Management Tools**, and then go to the next section.

Installing SQL Server Management Studio

Manage your SQL database permissions with SQL Server Management Studio (SSMS). For more information, refer to official Microsoft documentation.

1 Run the installer.

2 Select **Install**.

3 When the installation completes, select **Restart**.

> If there is no Restart option, then manually restart your computer.

Configure SQL Server with SSMS

Before installing Device Manager, you need to create a user and set up server authentication in SSMS to manage the SQL Server database instance. You will need this information later to connect Device Manager to the SQL database.

Selecting a database instance

1 Run SSMS.

2 In Server name, select **Browse for more**.

3 In Database Engine, select a database instance.

> If you have more than one database instance, then make sure to select the correct instance for Device Manager.

4 Select **OK**.

Setting up authentication

> Make sure that SSMS is running.

1 In SSMS Object Explorer, expand the database object, and then go to **Security** > **Logins**.

2 Right-click **NT AUTHORITY\SYSTEM**, and then select **Properties**.

3 Select **Server Roles** > **dbcreator**.

> The dbcreator role should be associated with a user account, which Device Manager will use to connect to the database. Public should be selected by default. If that account is a domain user account, refer to *Adding a domain user*.

4 Select **OK**.

5 Right-click on the database instance, and then select **Properties**.

6 Select **Security**.

7 In Server authentication, select either **Windows Authentication mode** or **SQL Server and Windows Authentication mode**, and then select **OK**.

8 Restart the SQL Server database service.

a) In Windows, select **Start**, and then search for the Services app.
b) In Services, search for SQL Server.
c) Right-click on the service, and then select **Restart**.

Adding a domain user

> Make sure that SSMS is running.

1 In SSMS Object Explorer, expand the database object, and then select **Security**.

2 Right-click **Logins**, and then select **New Login**.

3. In Login - New, go to **General**, and then select **Windows authentication** > **Search**.
   a) In Select User or Group, select **Advanced**.
   b) In Select User, Service Account, or Group, select **Locations**.
   c) In Locations, select **Entire Directory** > **OK**.
   d) Select **Find Now**.
   e) In Search results, select a user account, and then select **OK**.
   f) In Select User, Service Account, or Group, verify that the correct user account is added, and then select **OK**.
   The selected domain user is specified in Login - New.
4. In Login - New, go to **Server Roles**, and then select **dbcreator**.

   Public is selected by default. Keep this selection.

5. Select **OK**.

3 Device Manager installation and setup

Installing Device Manager

If you plan to use the Device Manager application with an external database, make sure that SQL Server and SSMS are installed and configured before you install the application.

1. Run the installer.
2. Review the license agreement, and then select **Accept**.
3. Review or specify the installation location, and then select **Next**.
4. Review your settings, and then select **Install**.
   If previously stored files are detected, then select an option:
   - Select **Yes** to use configuration files from the previous installation, such as AuditLogs, DeviceUser, and Certificate.
   - Select **No** to replace the previous configuration files with new ones.
5. When the installation completes, select **Next**.

   Take note of the default login information.
6. Select **Finish** to restart your computer immediately, or you can restart later.

   If you prefer, you can specify to create a desktop shortcut. This shortcut opens Device Manager in your default browser.

Firewall configuration

After installing Device Manager, make sure that the following ports are accessible:

Device

Destination Port Number	Protocol	Description
80	TCP (HTTP)	Device home page
161	UDP (SNMP)	To request data from a device
162	SNMP	To request SNMP Trap data from a device

Destination Port Number	Protocol	Description
443	TCP (HTTPS)	Device secure home page
9000	TCP	Computer with local USB agent
9090	TCP (HTTP)	To request data from a device
9091	TCP (HTTPS)	To request data from a device
9100	TCP	To send a firmware upgrade PRESCRIBE command to a device, enable the Raw Port option on the Device Operation panel

Device Manager

Destination Port Number	Protocol	Description
800-899	TCP (HTTP)	To request the firmware files from the Device Manager server by a device
9191	TCP (HTTP)	Device Manager web page
9292	TCP (HTTPS)	Device Manager secure web page
9595	TCP (HTTP)	To manage internal Device Manager operations

- After installing Device Manager, make sure that ports 9191 and 9292 have been added.
- If you intend to use Device Manager in a private network environment, then change your Firewall settings to private.

External Server

Check the following ports only if the database and Device Manager are installed on separate computers.

Destination Port Number	Protocol	Description
25	TCP (SMTP)	Simple Mail Transfer Protocol (SMTP) port
1433	TCP	Microsoft SQL database server default port

Upgrading Device Manager

Some recommendations before upgrading:

- Apart from your current system, set up a parallel environment for the upgrade, to have a fail-safe and to test the upgrade integrity.
- Back up all current data and user information in the Device Manager database
- Consult a project manager to have a plan, considering the risks, resources, and impact to your organization

1. Run the installer.
2. Review the license agreement, and then select **Accept**.
3. Select **Upgrade**.
4. When the upgrade completes, select **Next**.
5. To restart, select **Yes** > **Finish**.

- After restarting the computer, make sure that the Device Manager service is running and firewall Inbound Rules are in place.
- Before starting Device manager, make sure to clear the browser cache.
- To retain current data, make sure to select the same database as the previous version.

Connecting Device Manager to the database

1. Open Device Manager.
   - Double-click the desktop shortcut.
   - Open a supported browser, and then go to https://localhost:9292/.
2. Review the license agreement, and then select **Accept & continue**.
3. Review the privacy policy for data collection, select a participation option, and then select **Apply**.
4. Depending on your system setup and preference, select a database type:

   Internal database

   The embedded Firebird database is used with Device Manager.

   External database

   The Microsoft SQL database is used with Device Manager.

   a. Specify the database server details.
   b. Select **Test Connection**.

Review the results and if necessary, modify the server details. If a Test Connection error appears, then refer to *Troubleshooting SQL connection error*.

5 Select **OK**.

6 Verify the connection settings:

a) Go to **System** > **System Settings** > **Database Connection**.

b) Depending on your database type, confirm the following:

Database type	Settings
Internal database	Server: (local) Port number: 0
External database	Depending on your database server information, make sure that Server, Port number, User ID, and Password are correct.

Troubleshooting SQL connection error

A connection error between your SQL Server and Device Manager application may be due to certain permission or environment settings.

1 In SSMS, make sure that the Remote connections setting is enabled.

a) In SSMS Object Explorer, right-click your database server instance, and then select **Properties**.

b) In Server Properties, select **Connections**.

c) In Remote server connections, make sure that Allow remote connections to this server is selected.

In Device Manager, repeat Test Connection. If the problem persists, then go to the next step.

2 Check the port and SQL browser service.

a) In TCP/IP Properties, go to **IP Addresses** > **IP1**, and then take note of the TCP Port.

b) Open that port in Firewall, and confirm that it is not blocked.

c) In Windows, open Computer Management, and then go to **Services and Applications** > **Services**.

d) Search for the SQL Server Browser service, and make sure that Status is Running and Startup Type is Automatic.

- Double-click **SQL Server Browser**, and then in Startup Type, select **Automatic**.
- If Service status is not Running, then select **Start** > **OK**.

e) Right-click **SQL Server Browser**, and then select **Restart**.

In Device Manager, repeat Test Connection. If the problem persists, then contact support.

Making a domain user a local administrator

Use Windows Computer Management to provide local administrator rights to a user in your domain.

1. In Computer Management, go to **System Tools** > **Local Users and Groups** > **Groups**, and then double-click **Administrators**.
2. Select **Add**.
   a) In Select Users, Computers, Service Accounts, or Groups, select **Advanced**.
   b) In From this location, verify that your domain location is correct.
   If necessary, select **Locations**, and then browse for the correct domain.
   c) Select **Find Now**.
   d) In Search results, select a target domain user, and then select **OK**.
   e) In Enter the object names to select, verify that the correct domain user is added, and then select **OK**.
3. In Members, verify that the correct domain user is added, and then select **OK**.
4. Restart Device Manager.

ℹ Use Windows Local Group Policy Editor to manage administrator approval mode.

1. In Local Group Policy Editor, go to **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **Security Options**.
2. Double-click **User Account Control: Run all administrators in Admin Approval Mode**, and then review the setting. Disabling this setting reduces the security of your computer.

Additional configuration items

In Device Manager:

- Review your security settings in **System** > **Security**.
- Configure SMTP settings for sending messages and notifications in **System** > **SMTP**.
- Manage notifications and reports in **Notifications**.
- Change the password by selecting the option from the user icon. If you are logging into a remote server or have configured security settings to require login for a local device installation, then change the administrator password.

4 Local Device Agent

Install the Local Device Agent (LDA) application on each host computer with a USB-connected device. This allows Device Manager to discover these devices. Before installing LDA, make sure that:

- .NET Framework v4.0 or later is installed.

For more information, go to the Microsoft website.

- In Device Manager, the device is removed from the list.
- The device is connected to the host computer with a USB cable.
- The host computer is restarted.

Disabling Status Monitor

If you plan to access a device that is connected to a host computer through USB cable, then you must disable Status Monitor.

1 Depending on your printer driver status, do the following:

Status	Actions
Printer driver is installed Make sure that the latest version is installed.	**a.** In Control Panel, select **Devices and Printers**. **b.** Right-click your device, and then select **Printing preferences**. **c.** Go to **Advanced** > **Status Monitor**, and then make sure that Enables event notifications is disabled. If the Status Monitor option is disabled, then go to the next step.
Printer driver needs to be installed Make sure that you have the latest version of the installer.	**a.** Run the installer. • In Express Install, make sure that Status Monitor is not selected. • In Custom Install, make sure that Status Monitor is not included in Products to Install. **b.** Follow the instructions. For more information, refer to the *Printer Driver User Guide*.

2 Verify that Status Monitor is disabled.

a) In Windows, run Task Manager.

b) From any application, send a print job.

You can send a print job with a blank page.

c) After sending a print job, go to Task Manager, and make sure that Status Monitor does not appear in **Processes** > **Apps**.

> If disabled, then the Status Monitor window does not appear. If the window appears, then go to **Settings** > **Notifications**, and then disable event notification.

Installing LDA

In each host computer with a USB-connected device, do the following:

1 In Device Manager, go to **Devices** > **List** > **More** > **Download the local agent**.

2 Save and extract the package.

3 Run the installer.

You may need to allow the installer to make changes to your computer.

4 Review or modify the Destination folder, and then select **Next**.

5 Confirm the settings, and then select **Install**.

6 Review the results, and then select **Close**.

7 Make sure that LDA is running.

In Task Manager, go to **Processes** > **Background processes**, and then search for LDAService.

Discovering USB-connected devices

After installing LDA in host computers with USB-connected devices, you can add these devices in Device Manager.

> Before adding a USB-connected device, make sure that:
>
> - Status Monitor is disabled in the host computer.
> - You have the IP address or host name of the host computer.
> - The device is not in sleep mode.

1 In Device Manager, go to **Devices** > **List** > **Add devices** > **Add devices now**.

2 In Discovery mode, select **By IP address or host name**.

3 In Target, specify the IP address or host name of the computer with the USB-connected device.

4 Review or modify other settings, and then select **Run**.

5 Review the results. If necessary, resolve any issues before repeating the process.
In Device list, confirm that the device has been added.

For USB-connected devices listed in Device Manager:

- You cannot edit the location and communication settings.
- You cannot open the device home page.
- In the host computer, make sure that LDAService is running and Status Monitor is disabled.

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