



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.

© 2019 KYOCERA Document Solutions Inc.

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 Introduction

Intended audience	1-1
Intended use	1-1
Conventions	1-1
Assumptions	1-2
Prerequisites	1-2
Installation checklist	1-2

Chapter 2 System Requirements

Prerequisites	2-1
Supported OS	2-1
Supported browsers	2-1
Standard configuration hardware requirements	2-2
Standard configuration hardware requirements	2-2

Chapter 3 SQL Database Installation and Setup

Microsoft SQL Server 2016 Enterprise Installation	2
Enterprise installation: Mixed authentication mode	2
Enterprise installation: Windows authentication mode	7

Chapter 4 Device Manager installation

Firewall configuration	4-1
Best practices before upgrading to a new version	4-2
Upgrade	4-3
Connect Device Manager to internal database (Firebird)	4-4
Connect Device Manager to SQL	4-4
Check SQL connection on Device Manager	4-5
Making a domain user a local administrator.	4-6
Final Configuration Items	4-10

Chapter 5 Local Device Agent (LDA)

LDA prerequisites	5-1
LDA: KX Driver express install	. 5-1
Install LDA	.5-2
Discover USB-connected printer in Device Manager	.5-3

Chapter 6 Troubleshooting

Establishing a remote connection with Windows Authentication	.6-1
Allow remote connections to the server	. 6-2
Protocols for MSSQL Server	. 6-4
Check Firewall	6-5

1 Introduction

Intended audience

This document is for IT professionals, non-IT or personnel with knowledge of database installation and configuration. This document is not intended to replace the official Microsoft documentation for Microsoft SQL.

Refer to the Microsoft website for more detailed and official Microsoft SQL Server resources: https://docs.microsoft.com/en-us/sql/database-engine/install-windows/ install-sql-server-from-the-installation-wizard-setup

Intended use

This document provides step-by-step instructions on how to install the Microsoft SQL database and the Device Manager application.

Conventions

The following conventions may be used in this guide:

- Menu items and buttons appear in **bold text**.
- Screen, text box, and drop-down menu titles are spelled and punctuated exactly as they appear on the screen.
- Document titles appear in *italics*.
- Text or commands that a user needs to enter 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 need to know, including such things as data loss if the procedure is not done properly.



This is a TIP icon. It indicates a small but useful piece of practical, non-essential information.

Assumptions

Firebird

- There is only one database installed on the machine, which is the one being used with Device Manager
- The Firebird database will be installed in the same machine as the Device Manager application

Microsoft SQL

• The Microsoft SQL database will be installed on the same machine as the Device Manager application.

For other configuration options, contact your support personnel for supplemental instructions.

- There is only one database administrator that will access the database locally.
- There is only one database installed on the machine, which is the one being used with Device Manager.

Prerequisites

Before you install the database, you must make sure all the prerequisites are satisfied.

- See System Requirements
- Determine the Microsoft SQL Server version to install based on your needs: Enterprise or Express.

(https://www.microsoft.com/en-us/sql-server/sql-server-2016)

- For Express: This entry-level version of Microsoft SQL Server has a small set of prerequisites. The maximum limit of the database is 10 GB.
- For Enterprise: The enterprise version must be purchased. Once purchased, be sure to write down the product key. Make sure you find the correct installer.

Installation checklist

The order of installation is as follows:

- 1. Install the SQL database (Express or Enterprise).
- 2. Install SQL Server Management Studio (SSMS).
- 3. Configure the instance with SSMS.
- 4. Install Device Manager and connect it to the database.

2 System Requirements

Prerequisites

• .NET Core 2.1.3

.NET Core installation prerequisite: Microsoft Visual C++ Redistributable for Visual Studio 2015

- Internal database: Embedded Firebird
- External database: Microsoft SQL 2008 R2/2012/2014/2016/2017 Express/ Standard/Enterprise editions



.NET Core is included in the installer package. For .NET Core to work properly, your system must have all the latest Windows updates.

Supported OS

- Microsoft Windows 7, 8/8.1, 10
- Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019

You may encounter an issue in installing Device Manager on Windows 2008 R2 OS. Use the following environment and follow the additional instructions:

- Make sure that .NET Framework 4.6.1 is included in Windows updates.
- Windows Server 2008 R2 SP1 or higher should be used.
- Microsoft Visual C++ Redistributable for Visual Studio 2015 Update 3 should be installed.
- The Device Manager service may not start after the installation is completed. Restart your computer to start the service.

Supported browsers

- Google Chrome 52 and higher
- Microsoft Internet Explorer 11
- Microsoft Edge for Windows
- Firefox 53 and higher
- Safari-compatible

Recommended hardware	Number of supported devices	Database
 4GB RAM 2 cores (physical) 1.5GHz CPU 	Up to 100 devices	Internal
 6GB RAM 4 cores (physical) 3.6GHz CPU 	Up to 300 devices	Internal/External
 32GB RAM 8 cores 2.2GHz CPU 1000Mbps gigabit Ethernet adapter 	Up to 10,000 devices	External

Standard configuration hardware requirements

3 SQL Database Installation and Setup

Microsoft SQL Server 2016 express installation

This section describes how to install Microsoft SQL Server 2016 Express. For more information, refer to official Microsoft documentation. This is a free version of Microsoft SQL but it has a storage limitation. If you are installing Microsoft SQL Server 2016 Enterprise, go to the next section.

- 1 Launch the SQLEXPRESS 2016 installer.
- 2 Select the Basic option.
- 3 Select Accept to accept the license terms.
- **4** Accept the installation location, or browse to select a location.
- 5 Select Install.
- 6 Once the installation is complete, select **Install SSMS**. Proceed to SQL Server Management Studio (SSMS.)

► SQL Server 2016 with SP1 Express Edition Installation has completed suc	What's New? 🙄 🗕 🗙
INSTANCE NAME SQLEXPRESS	CONNECTION STRING Server=localhost:SQLEXPRESS;Database=master:Trusted_Connection=Tru
INSTANCE ID SQLEDIPRESS	SQL SERVER INSTALL LOG FOLDER
SQL ADMINISTRATORS	C/Program Files/Microsoft SQL Server/130/Setup Bootstrap/Log/2017053
FEATURES INSTALLED	CASQLServer2016Media\Express
SQLENGINE	INSTALLATION RESOURCES FOLDER C\Program Files\Microsoft SQL Server\130\SSER\Resources
13.0.4001.0, Service Pack 1	
A computer restart i	s required to complete your installation.
	Customize Install SSMS Close

Microsoft SQL Server 2016 Enterprise Installation

Enterprise installation: Mixed authentication mode

This section describes how to install Microsoft SQL Server 2016 Enterprise with mixed SQL Server and Windows authentication modes. For more information, refer to official Microsoft documentation. This is a paid version of the database and requires a product key. It is assumed that the user will already have the installer package. If you are installing the free version of the software, go to the previous section.

- 1 Launch the Microsoft SQL Server 2016 Enterprise installer.
- 2 On the left panel, select **Installation**.
- 3 On the SQL Server Installation Center page, select New SQL Server standalone installation or add features to an existing installation.



4 When Install Rules is completed, select **Next**. If warnings appear, you can ignore them.

5 On the Product Key page, select Enter the product key and enter it. Select Next.

📸 SQL Server 2016 Setup				×
Product Key Specify the edition of SQL Se	ever 2016 to install.			
Global Rules Product Updates Install Setup Files Install Rules Product Key License Terms Feature Selection Feature Configuration Rules Ready to Install Installation Progress Complete	Validate this instance of SQL Server 2016 by entering the 25-character key fr of authenticity or product packaging. You can also specify a free edition of S Evaluation, or Express. Evaluation has the largest set of SQL Server features, Books Online, and is activated with a 180-day expiration. Developer edition of has the same set of features found in Evaluation, but is licensed for non-pro development only. To upgrade from one installed edition to another, run the O Specify a free edition: Evaluation © Enter the product key:	rom the Microso SQL Server: Deve as documented does not have a iduction databas e Edition Upgrad	oft certific: eloper, in SQL Se n expirati se applica de Wizard	ate erver on, tion I,
	< Back	Next >	Canc	el

- 6 On the Instance Configuration page, Default instance is selected. If you want to customize the name, select **Named instance** and enter the name. Select **Next**.
- **7** No changes need to be made for Server Configuration. Select **Next**.
- 8 On the Database Engine Configuration page, in the Authentication Mode section (1), select **Mixed Mode (SQL Server authentication and Windows authentication)** and enter a password for the system administrator account.
- 9 Under Specify SQL Server administrators, select Add Current User (2) to add the user currently logged on the computer, or select Add to specify another user. Select Next.

Database Engine Confi	guration	
Specify Database Engine authe	ntication security mode, administrators, data directories and TempDB	settings.
Global Rules	Server Configuration Data Directories TempDB FILESTREAM	
roduct Updates nstall Setup Files	Specify the authentication mode and administrators for the Data	abase Engine.
nstall Rules roduct Key icense Terms	Authentication Mode O Windows authentication mode O Mixed Mode (SQL Server authentication and Windows authen	tication)
eature Selection eature Rules	Specify the password for the SQL Server system administrator (sa	account.
istance Configuration erver Configuration	Enter password:	
atabase Engine Configuration	Confirm password:	
ature Configuration Rules	Specify SQL Server administrators	
eady to Install nstallation Progress Complete	HOST-25\SkyLab (SkyLab)	SQL Server administrators have unrestricted access to the Database Engine.
	Add Current User Add Remove	

- **10** On the Ready to Install page, review your settings. Select **Install**.
- **11** On the Installation Progress page, select **Next** when the installation is completed.
- **12** On the Complete page, select **Close**.
- **13** On the SQL Server Installation Center page, select **Install SQL Server Management Tools**. See the next section for further instructions.



SQL Server Management Studio (SSMS) installation

SQL Server Management Studio (SSMS) is needed to easily manage the SQL database permissions.

https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms

- 1 Run the SQL Server Management Studio installer.
- 2 Select Install.
- **3** Once the installation is finished, select **Restart**. At this point, the installer already created an instance. If there is no Restart button, manually restart the computer.

Configure database instance with SSMS

Before installing Device Manager, you need to create a user and set up server authentication on SSMS to manage Microsoft SQL Server 2016. You will need this information later to connect Device Manager to the SQL database.

Configure SSMS to the SQL server

- 1 Run SSMS.
- 2 In the Server name list, select **Browse** for more.

🖵 EConnect to Server		×
	SQL Server	
Server type:	Database Engine	~
Server name:		\sim
Authentication:	<browse for="" more=""></browse>	-
User name:	HOST-25\SkyLab	\sim
Password:		
	Remember password	
	Connect Cancel Help Options	»>

3 Select a database under Database Engine.

If you have more than one instance, select the newly installed instance for Device Manager.

4 Select OK.

Communication with Device Manager: Mixed Mode Authentication

- 1 Run SSMS.
- 2 Navigate to Access Security > Logins. Right-click NT AUTHORITY\SYSTEM.
- 3 Select Properties.
- 4 Select **Server Roles** and then select dbcreator. Public should be selected by default. Select **OK**.

The dbcreator role should be associated with a user account (may be a domain user account), which Device Manager will use to connect to the database. If that account is a domain user account, refer to *Add a Domain User: Windows Authentication Mode*.

- **5** Right-click on the database, and select **Properties**.
- 6 In the left pane, select **Security**.

	Server Properties - KW-12-9020-2\KDMSQL
Select a page © General © Memory © Processors © Security © Connections © Database Settings © Advanced © Permissions	Script Pelp Server authentication Windows Authentication mode SQL Server and Windows Authentication mode Login auditing None Failed logins only Successful logins only Both failed and successful logins Server proor account
Connection	Enable server proxy account
Server: KW-12-9020-2\KDMSQL	Proxy account:
Connection: KTD-KYOCEBA COM\kwong	Options
v v View connection properties	Enable Common Criteria compliance Enable C2 audit tracing Cross database ownership chaining
Progress	
Ready	
	OK Cancel

7 In the Server authentication section, select SQL Server and Windows Authentication mode and select OK.

	Server Properties - KW-12-9020-2\KDMSQL
Select a page % General % Memory % Processors % Security % Connections % Database Settings % Advanced % Permissions	Server authentication Windows Authentication mode SQL Server and Windows Authentication mode Login auditing
Conn Serve	Failed logins only Microsoft SQL Server Management Studio x onfiguration changes will not take effect until SQL Server is restarted. OK
KW-1 Connection: KTD-KYOEERA.COM%kwong YY View connection properties Progress Executing	Options Enable Common Criteria compliance Enable C2 audit tracing Cross database ownership chaining
	OK Cancel

8 Select OK.

9 Restart the SQL Server service under Services.

Services File Action View ★ ★ □	/ Help ③ 🗃 🛛 🛐 🕨 💷 🕪					
🔍 Services (Local)	Services (Local)					
	SQL Server (SQLEXPRESS)	Name	Description	Status	Startup Type	Log On As
		🖏 SQL Server (SQLEXPRESS)	Provides sto	Running	Automatic	NT Service
	Stop the service	SQL Server Agent (SQLEXPRESS)	Executes jo		Disabled	Network S
	Restart the service	🖏 SQL Server Browser	Provides SQ	Running	Automatic	Local Service
		SQL Server CEIP service (SQLEXPRESS)	CEIP service		Automatic	NT Service
		Q SQL Server VSS Writer	Provides th	Running	Automatic	Local Syste

Enterprise installation: Windows authentication mode

This section describes how to install Microsoft SQL Server 2016 Enterprise with Windows Authentication. For more information, refer to official Microsoft documentation. This is a paid version of the database and requires a product key. It is assumed that the user will already have the installer package. If you are installing the free version of the software, go to the previous section.

- 1 Launch the Microsoft SQL Server 2016 Enterprise installer.
- 2 On the left panel, select **Installation**.
- **3** On the SQL Server Installation Center page, select **New SQL Server stand**alone installation or add features to an existing installation.



- 4 When Install Rules is completed, select Next. If warnings appear, you can ignore them.
- **5** On the Product Key page, select **Enter the product key** and enter it. Select **Next**.

🐮 SQL Server 2016 Setup							-3		×
Product Key Specify the edition of SQL Se Global Rules Product Updates Install Setup Files Install Rules	Validate th of authent Books Onl has the sa	is instance of SC icity or product , or Express. Eva ine, and is activa me set of feature	QL Server 2016 1 packaging, You luation has the ted with a 180 s found in Eval	by entering th can also spec largest set of day expiratio uation, but is	e 25-character ify a free editic SQL Server feat Developer ec licensed for no	key from th n of SQL Se tures, as doo lition does n n-productio	e Microsof rver: Devel umented i ot have ar n database	it certifica oper, in SQL Se n expiratio e applicat	ite rver on, ion
Product Key License Terms Feature Selection Feature Rules Feature Configuration Rules Ready to Install Installation Progress Complete	developm O Specify Evalu (a) Enter th	ent only. To upg a free edition: uation ee product key:	rade from one i	nstalled editio	on to another, r	un the Editio	on Upgrad	e Wizard.	
					< Back	Nex	ct >	Cance	el

- 6 On the Instance Configuration page, Default instance is selected. If you want to customize the name, select **Named instance** and enter the name. Select **Next**.
- 7 No changes need to be made for Server Configuration. Select Next.

- 8 On the Database Engine Configuration page, in the Authentication Mode section (1), select **Windows authentication mode**.
- 9 Under Specify SQL Server administrators, select Add Current User (2) to add the user currently logged on the computer, or select Add to specify another user. Select Next.

1	SQL Server 2016 Setup
Database Engine Confi	guration
Specify Database Engine authe	ntication security mode, administrators, data directories and TempD8 settings.
Product Key License Terms Global Rules Product Updates Install Setup Files Install Rules Feature Selection Feature Rules Instance Configuration	Server Configuration Data Directories TempDB FILESTREAM Specify the authentication mode and administrators for the Database Engine. Authentication Mode • Windows authentication mode • Mixed Mode (SQL Server authentication and Windows authentication) Specify the password for the SQL Server system administrator (sa) account.
Server Configuration Database Engine Configuration Feature Configuration Rules	Confirm password: Specify SQL Server administrators
Ready to Install Installation Progress Complete	KTD-KYOCERA.COM\kwong (Kelly Wong) SQL Server administrators have unrestricted access to the Database Engine. Add Current User Add
	< Back Next > Cancel

- **10** On the Ready to Install page, review your settings. Select **Install**.
- **11** On the Installation Progress page, select **Next** when the installation is completed.
- **12** On the Complete page, select **Close**.
- **13** On the SQL Server Installation Center page, select **Install SQL Server Management Tools**. See the next section for further instructions.

Configure SSMS to the SQL server

- 1 Run SSMS.
- 2 In the Server name list, select **Browse** for more.

교 ^문 Connect to Server		×
	SQL Server	
Server type:	Database Engine	~
Server name:	1	\sim
Authentication:	Browse for more>	_
User name:	HOST-25\SkyLab	\sim
Password:		
	Remember password	
	Connect Cancel Help Options >	>>

3 Select a database under Database Engine.If you have more than one instance, select the newly installed instance for

Device Manager.

4 Select OK.

Communication with Device Manager: Windows Authentication

- 1 Run SSMS.
- 2 Navigate to Access Security > Logins. Right-click NT AUTHORITY\SYSTEM.
- 3 Select **Properties**.
- 4 Select **Server Roles** and then select dbcreator. Public should be selected by default. Select **OK**.



- **5** Right-click on the database, and select **Properties**.
- 6 In the left pane, select **Security**.

	Server Properties - KW-12-9020-2\KDMSQL
Select a page & General & Memory & Processors & Security & Connections & Database Settings & Advanced & Permissions	Script Help Server authentication Windows Authentication mode SQL Server and Windows Authentication mode Login auditing
Connection	None Failed logins only Successful logins only Both failed and successful logins Server proxy account Enable server proxy account
Server: KW-12-9020-2\KDMSQL Connection: KTD-KYOCEBA COM\kwong	Proxy account: L
vi View connection properties	Enable Common Criteria compliance Enable C2 audit tracing Cross database ownership chaining
Progress Ready	
	OK Cancel

7 In the Server authentication section, select **Windows Authentication mode** and select **OK**.

	Server Properties - KW-12-9020-2\KDMSQL
Select a page % General % Memory % Processors % Security % Connections % Database Settings % Advanced % Permissions	Script Help Server authentication Windows Authentication mode SQL Server and Windows Authentication mode Login auditing None Failed logins only
Conn Serve	Microsoft SQL Server Management Studio
KW- Connection: KTD-KYOCERA.COM\kwong ∳ ¥ View connection properties Progress Executing	Options
	OK Cancel

8 Select OK.

9 Restart the Device Manager database service.

9,		Services						- 🗆 X
File Action View	Help							
(= =) 📰 🖾) 🗟 🔢 🖬 🕨 🔳 🕪							
🤹 Services (Local)	Services (Local)							
	SOL Server (KDMSOL)	Name	•	Description	Status	Startup Type	Log On As	^
	Ste Server (nomste)	SQL Server (KDMSQL)		Provides sto	Running	Automatic	NT Service\MSSQL\$KDMS	QL

Add a Domain User: Windows Authentication Mode

1 Run SSMS.

- Object Explorer τĻΧ Connect - 🛱 🎽 🔳 🝸 🖒 🪸 □ R DIMATESTSQL\SQLEXPRESS (SQL Server 14.0.1000 - KY-TEST\Administrator) 🗄 💼 Databases 🖃 💼 Security 🖃 💼 Logins New Login... × .ogin## × in## Filter ۲ Start PowerShell Reports ۲ μ. up-For-MS-SQL Refresh • 2 NT Service\MSSQL\$SQLEXPRESS NT SERVICE\SQLTELEMETRY\$SQLEXPRESS ٩ NT SERVICE\SQLWriter • NT SERVICE\Winmgmt • sa 🗄 💼 Server Roles 🗄 🛑 Credentials
- **2** Open the Security folder, right-click the **Logins** folder, and select **New Login**.

3 In the Login - New / General dialog, select **Windows authentication** and select **Search...**.



4 In the Select User or Group dialog, select Advanced....

Select User or Group		>
Select this object type:		
User or Built-in security principal		Object Types
From this location:		
ky-test.local		Locations
Enter the object name to select (<u>examples</u>):		
		Check Names
J		
<u>A</u> dvanced	OK	Cancel

5 In the dialog that opens, select **Locations...**.

Select User, Servic	e Account, or Gro	oup		×
Select this object ty	/pe:			
User or Built-in sec	urity principal		Object Types	
From this location:			 	
ky-test.local			Locations	
Common Queries			OK Cance	el
Name	In Folder	E-Mail Address		^
				~

6 In the Locations dialog, select **Entire Directory** and select **OK**.

7 Select Find Now. Select a user account from the search results, and select OK.

Select User, Serv	ice Account, or Grou	qu				×
Select this object	type:					
User or Built-in se	ecurity principal			Object	Types	
From this location	:					
Entire Directory				Locat	ions	
Common Querie	s					
N <u>a</u> me:	Starts with \lor				<u>C</u> olumns	
Description:	Starts with \sim				Find <u>N</u> ow	
Disa <u>b</u> led a	ccounts				Stop	
Non expirin	ig password					
Days since las	t logon: 🔍 🗸				P	
				ОК	Cancel	
Search res <u>u</u> lts:		1				_
lame	In Folder	E-Mail Address				^
DIALUP						
Digest Authen.	 ku test le sel /l lesm					
Dima Test	kytest local/Users					
Dima Testo	ky-test.local/Users		-			
aributed C	ky-test.local/Buil					
ENTERPRIS						
Event Log Re.	ky-test.local/Buil					
Everyone						
Presti public k.						×

8 Select OK.

Select User, Service Account, or Group	×
Select this object type:	
User or Built-in security principal	Object Types
From this location:	
ky-test.local	Locations
Enter the object name to select (examples):	
Dima Test2 (dima-test2@ky-test.local)	Check Names
<u>A</u> dvanced	OK Cancel

9 The selected domain user displays on the Login - New / General page.

Login - New			-		×
Select a page	🖵 Script 🔻 😮 Help				
 Server Roles User Mapping Securables 	Login <u>n</u> ame:	KY-TEST\dimatest2		Search	I
Status	O SQL Server authentication	and the second second		A	
	อนไสน์ไปเอกฐมีอยู่ชี	AP	~		
			ОК	Cano	el

10 Select **Server Roles**, select **dbcreator** (public will already be selected), and then select **OK**.

Login - New		-		×
Select a page	🖵 Script 👻 😯 Help			
Server Roles User Mapping Securables	Server role is used to grant server-wide security privileges to a user.			
🖌 Status	Server roles:			
	Dulkadmin ✓ dbcreator □ ciskadmin			
	processadmin			
	secuntyadmin serveradmin setupadmin			
	sysadmin			
Progress				M
Ready				
	0	K	Cano	el

4 Device Manager installation

Once the SQL Server is installed and configured, you can install Device Manager.

- 1 Run the installer.
- 2 Select Accept.
- 3 On the Choose Destination page, accept the installation location, or browse to select a location. Select Next.
- **4** On the Confirm Settings page, confirm your settings, and select **Install**. If previously stored files are detected, choose how to handle them.
 - Select **Yes** to use configuration files from the previous installation, such as AuditLogs, DeviceUser, and Certificate.
 - Select No to remove the previous files and replace with new configuration files.
- **5** Once the installation is complete, select **Finish**.
- 6 On the Restart Your Computer page, select **Finish** to restart your computer immediately, or you can restart later.

Firewall configuration

When Device Manager installation is completed, the following ports should be 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
443	TCP (HTTPS)	Device secure home page
9000	TCP	Computer with local USB agent
9090	TCP (HTTP)	To request data from a device

Destination Port Number	Protocol	Description
9091	TCP (HTTPS)	To request data from a device
9100	ТСР	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



If Device Manager is used in a private network environment, the Firewall setting has to change to private.



*After installing Device Manager, check that these two ports (9191 and 9292) have been added.

External Server

(Only applicable if Database and Device Manager are installed on separate computers)

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

Best practices before upgrading to a new version

Have two environments

Having two environments is recommended: one, your current system; the other, a new installation running in parallel. Too many organizations do not make the time or have the infrastructure to support two environments running at the same time. Having a

separate installation for the new software version provides a fail-safe method in case something goes wrong during the upgrade process. With two environments, users would not be impacted and administrators are able to confidently test all the required features without any impact on the current environment.

Always make backups

Software compatibility is a critical component of the upgrade process. Therefore, before upgrading, the new version needs to be checked to make sure that it can operate with other peer and dependent software within the enterprise. If any software is not compatible or supported, a decision needs to be made if that software needs an upgrade of its own. It is not uncommon for IT to be managing several upgrades simultaneously to ensure compatibility between different vendors' software.

Backup all current data and user information in the following databases:

- Microsoft SQL (Device Manager database)
- Firebird (Device Manager database)

Plan, test and execute

Upgrading enterprise software can be complex and requires a lot of processing and planning; upgrading needs to be treated and managed as a project. A project manager would be required to get business and technical buy-in, plan the different activities from installation, testing, and cut over, and execute the activities by performing regular status checks. Resources would need to be assigned to do regression testing particularly those programs which touch other systems, which are critical to the business operation and which are complex in terms of logic and application.

Be sure to choose the correct database options used in the current environment.

There are currently two database options:

- Microsoft SQL
- Firebird

Upgrade

When upgrading, you must choose the same database.

- 1 Select Setup.exe.
- 2 Select Accept to accept the license agreement.
- **3** Select **Upgrade** to perform the upgrade process.
- 4 Once the upgrade is complete, select **Next**.
- 5 On the Restart Your Computer page, select **Yes**, restart my computer now, and select **Finish** to complete the upgrade.

E

After restarting the computer, make sure the Device Manager service is running and firewall Inbound Rules are in place.



Be sure to clear the browser cache after completing an upgrade.

Data is retained when you select the same database type during an upgrade.

Connect Device Manager to internal database (Firebird)

If you are using the internal Firebird database with Device Manager, follow these steps to configure it when starting Device Manager for the first time.

- 1 Use the Device Manager shortcut on the desktop to open a browser (see supported browsers in System Requirements) and browse to the Device Manager instance. If accessing via URL, enter https://localhost:9292/
- 2 On the End User License Agreement page, select **Accept & Continue** to accept the License Agreement.
- 3 On the Anonymous Data Collection page, select a participation option. Select **Apply**.
- **4** On the Database Setup page, select the radio button for Internal database.

There will be a warning about selecting a slow database and a limit on number of supported devices.



If using the internal Firebird database, we recommend that you not plan to support more than 300 devices.

5 Select OK.

Device Manager configures the local Firebird database, which can take a few minutes.

Once the database is established, the Device Manager user interface appears.

Connect Device Manager to SQL

If you are using an external SQL database with Device Manager, follow these steps to configure it when starting Device Manager for the first time.



The Device Manager service might take some time to start. Check Windows Services to confirm that the Device Manager service started before opening Device Manager in the browser.

- 1 Use the Device Manager shortcut on the desktop to open a browser (see supported browsers in System Requirements) and browse to the Device Manager instance. If accessing via URL, enter https://localhost:9292/
- 2 On the End User License Agreement page, select **Accept & Continue** to accept the License Agreement.
- 3 On the Anonymous Data Collection page, select a participation option. Select **Apply**.

4 On the Database Setup page, select **Test Connection** and to automatically populate the server (local) or enter specified server (computer name\instance name).

Database Setup		×
External database		
Server:	of remote database.	
Port number:		
User ID:	Password:	
Test Connection		ок
This assumes the SQL	Server is installed on the province of the server is server is application.	same local system

5 If the test is successful, select **OK**.

Once the connection is established, the Device Manager user interface appears.

Check SQL connection on Device Manager

If Device Manager connects correctly to the SQL database, the System tab in Device Manager should look like the screenshot below regardless of the database version.

Smart Pulling Security Security Security Audit Log Vers Dol Collection Learne Environge Audit Log	
overs Dara Cellection uzense Database Connection Proxy Settings Database Connection Settings	(
Database Connection Nettings	
	∕ tâi
lever	
(red)	
Portnumber	
Uw D	
Present	



This assumes there is only one SQL database instance installed on the system system.

Making a domain user a local administrator

1 Open Windows Computer Management with administrator rights, expand Local Users and Groups, select Groups and then open Administrators.

🚁 Computer Management			-	×
<u>File</u> <u>Action</u> <u>View</u> <u>H</u> elp				
🗢 🔿 🙍 📷 🗙 🗟 🖡	?			
Computer Management (Local	Name	Description	Actions	
V System Tools	Access Control Assist	Members of this group can remotely query authorization attributes and permi	Groups	-
Kernet Viewer	Administrators Backup Operators	Administrators have complete and unrestricted access to the computer/doma Backup Operators can override security restrictions for the sole purpose of ba	More Actions	•
> 12 Shared Folders	Recryptographic Operat	Members are authorized to perform cryptographic operations.	Administrators	
 ✓ @ Local Users and Groups ○ @ Performance ♂ @ Performance ✓ @ Storage ✓ @ Storage ✓ @ Storage ✓ @ Services and Applications ⊘ Services ∅ WMI Control 	Device Owners Device Owners Device Owners Device Owners Device Owners Device Owners Device Owner Device Owner Device Owner Device Owner Users Performance Monitor Device Over Users Remote Desktop Users Remote Management Remote Management Replicator System Managed Acc Su Users	Backup Operators can override security restrictions for the sole purpose of ba Members are authorized to perform cryptographic operations. Members of this group can change system-wide settings. Members of this group can read event logs from local machine Cuests have the same access as members of the Users group by default, excep Members of this group have complete and unrestricted access to all features Built-in group used by Internet Information Services. Members in this group can have some administrative privileges to manage co Members of this group can access performance counters, enabl Members of this group can access performance counter data locally and rem Power Users are included for backwards compatibility and posses limited ad Members of this group can access Will resources over management protocol Supports file replication in a domain Members of this group can access Will resources over management protocol Supports file replication in a domain	More Actions	•

Administrators Pr	operties			?	×
General					
Admini	strators				
Description:	Administrators to the compute	have comple er/domain	te and unrestrict	ed acces	s
Members:					
In the second s					
Add	Remove	Changes to are not effe user logs o	a user's group n active until the ne n.	nembersł ext time tł	nip ne
	ОК	Cancel	Apply	He	lp

2 Select Add in Administrator Properties.

3 Select **Advanced...** in the Select Users, Service Accounts, or Groups dialog.

Select Users, Computers, Service Accounts, or Groups	×
Select this object type:	
Users, Service Accounts, or Groups	Object Types
From this location:	
ky-test.local	Locations
Enter the object names to select (<u>examples</u>):	
	Check Names
Advanced OK	Cancel

4 In the next dialog box, select a target domain as a location, select **Find Now**, select a target user account, and select **OK**.

Users, Service	Accounts, or Groups			Object	Types
From this location	on:				
ktd.com				Locat	tions
Common Que	ries				
Name:	Starts with $\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$	vong			Columns
Description:	Starts with $\ \!$				Find Now
Disabled	accounts				Stop
Non expi	ring password				
Days since I	ast logon: 🛛 🗸 🗸				27
		-			*
Search results:			(ок	Cancel
lame	E-Mail Address	Description	In Folder		

5 Select **OK** in the Select Users, Computers, Service Accounts, or Groups dialog.

Select Users, Computers, Service Accounts, or Groups	×
Select this object type:	
Users, Service Accounts, or Groups	Object Types
From this location:	
ktd.com	Locations
Enter the object names to select (<u>examples</u>):	
Kelly Wong (Kelly.Wong@dda.kyocera.com)	Check Names
Advanced OK	Cancel

6 The selected domain user is added in the Administrators Properties window. Select **OK**.

Administrators Pr	operties			?	\times
General					
Admini:	strators				
Description:	Administrate to the comp	ors have comp uter/domain	plete and unrestrict	ed acce	ess
Members: admin Administrato KTD-KYOCI KTD-KYOCI	r ERA.COM\Do ERA.COM\kw	main Admins ong			
Add	Remove	Changes are not e user logs	to a user's group r ffective until the ne on.	members ext time t	hip the
	ОК	Cancel	Apply	He	elp



7 Modify Windows Local Group policy using the Group Policy console to match the following screens.

8 Restart the Device Manager host.

Final Configuration Items

- Make desired changes to security settings in System > Security
- Configure SMTP for sending messages and notifications in System > SMTP.
- Configure Notifications.
- Change the password. If you are logging into a remote server or have configured security settings to require login for a local device installation of Device Manager, change the Admin password.



Password requirement is 4 characters with at least one lower case letter, one uppercase letter, one number, and one special character. An error message appears if your password does not meet these requirements.

5 Local Device Agent (LDA)

In order for Device Manager to be able to discover printers that are connected to computers by USB cables, install the Local Device Agent on each computer with a USB-connected printer.

LDA prerequisites

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



- Remove the printer to be managed with LDA from Device Manager, if it was previously added.
- · Connect the printer directly to the computer with a USB cable.
- Reboot the computer.
- Install the latest version of KX Driver on the computer with the USB-connected printer.



LDA: KX Driver express install

- 1 Select Express Install from the KX Driver Product Library.
- 2 Select the printer that is connected by USB cable from the list and clear **Status Monitor 4**.

3 Select Install.

- C						
De	vice		Details			
	TASKalfa 3510i		U\$8001			
	TASKalfa 7052ci		fe80::217:c8ff:fe27:93fc			
	TASKalfa 6052ci		fe80::217:c8ff:fe24:514f			
iii	ECOSYS P5021cd	N .	fe80::217:c8ff:fe3b:4208			
Ì	ECOSYS P3060dn		fe80::217:c8ff:fe2e:7ff5			
Ħ	ECOSYS M5526cd	in	fe80::217:c8ff:fe3b:41a4			
t	TASKalfa 3011i		fe80::217:c8ff:fe27:48d2			
2 0	evices		7 88 343 807 3 1487	@		lane
2 d	evices ge host name as po	ort name ou want to use with this device.		🚯 sn	MP Sett	ings
2 d	evices ise host name as po ict the features y Name	ort name ou want to use with this device. Description		🔥 sn	MP Sett	lings
2 d U ele	vices ye host name as p ict the features y Name ICC DRIVER	ort name ou want to use with this device. Description (Recommended) Extended-functionality printing		🚯 SN	MP Sett	lings
2 d U ele	evices ge host name as po ect the features y Name KX DRIVER FONTS	ort name ou want to use with this device. Description (Recommended) Extended-functionality printing Screen fonts that match the printer's fonts		No sn	MP Sett	lings
	Exercises See host name as p- cct the features y Name KX DRIVER FONTS Status Monitor 4	ort name ou want to use with this device. Description (Recommended) Extended-functionality printing Screen fonts that match the printer's fonts Service for monitoring current printer status		R sv	MP Sett	ings
2 d 0 u iele	Exercises Sect the features y Name KX DRIVER FONTS Status Monitor 4	ort name ou want to use with this device. Description (Recommended) Extended-functionality printing Screen fonts that match the printer's fonts Service for monitoring current printer status		() , sv	MP Sett	ings

4 Select **Finish** when the installation is completed.

Install LDA

Install LDA on the computer with the USB-connected printer.

- 1 Log in to Device Manager.
- 2 Download LDA from Device Manager.



- **3** Unzip the downloaded package.
- 4 Run **Setup.exe** to install LDA.

- 5 Select **Next** on the first install screen.
- 6 Select **Install** on the Confirm Settings screen.
- 7 When installation is completed, select **Close**.
- 8 Verify that the Local Device Agent service is running under Windows Task Manager.

r∰ Task M File Optio	lanager ons View								
Processes	Performance	App history	Startup	Users	Details	Services			
Name	^	PID	Descr	iption				Status	
🕼 LocalDe	viceAgent	7368	KYOC	ERA Lo	cal Devic	e Agent	 	Running	_

Discover USB-connected printer in Device Manager

- 1 Log in to Device Manager.
- 2 Select Add Devices now after verifying that the printer to be discovered is not in sleep mode.



- **3** Select **By IP address or host name** as the Discovery method.
- **4** In **Target**, enter the IP address of the computer with the USB-connected printer.

5 Make any necessary changes to other settings on the Add Devices screen, and then select **Run**.

Add Devices		×
Discovery Settings		
Discovery method *	By IP address or host name ⊯	
Target *	IP address and host name 10.10.18.107	
Communication settings		
TCP/IP port Secure protocol (SSL)	9100	
	If you do not enable SSL, the connection to your device will not be secure. Data sent to your devices may be vulnerable.	
Communication timeout (seconds) Reset Save Settings	Run Cancel	

The Discovering Devices Successful screen displays.

Discovering Devices	×
Successful	
100%	
10078	
Discovered devices: 1	
Current devices: 104	
Deleted devices: 0	
Total devices: 105	
You can close this window and be notified when the discovery is complete.	

Device Manager now displays the added USB printer in the Device list.

De	evice list				
	Status	Model name	IP address 🔺	Host name	Toner level (K, C, M, Y)
	📀 Ready	TASKalfa 3510i	10.10.18.107 (USB)	kw-fc64-9020	K:37%

After installation of the LDA, Device Manager can monitor Device information, Status, Counter, Consumables, and Alerts on the device. Communication settings and location are not editable.



The device home page cannot be opened from Device Manager for USB-connected devices. The LDA service cannot be used at the same time with some other utilities, such as the Status Monitor. If the LDA service does not start, try disabling the Status Monitor and restarting the LDA service.

6 Troubleshooting

Establishing a remote connection with Windows Authentication

¢.	Connect to Server	x
	SQL Server	
Server type:	Database Engine	~
Server name:	KW-FC64-9020\SQLEXPRESS	~
Authentication:	Windows Authentication	~
User name:	KTD-KYOCERA.COM\kwong	~
Password:		
	Remember password	
	Connect Cancel Help Opti	ons >>

Error message

"A network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found or was not accessible. Verify that the instance name is correct and that SQL Server is configured to allow remote connections. (provider: Named Pipes Provider, error: 40 - Could not open a connection to SQL Server)"



The following are possible ways to resolve this issue. All of the following configurations are made on the computer running the SQL Server 2008 - 2016 instance.

Allow remote connections to the server

Check that Remote Connections are enabled on the SQL Server database. In SQL Server 2008 - 2016 do this by opening SQL Server Management Studio (SSMS).

1 Open Server Properties.

General Microsoft SQL Server Management Studio File Edit View Debug Tools Window	Help
G + O 12 + 12 + ≦ New Qu	Jery 🖨 🔊 🖓 였 🕅 였 🕅 (상 i) 4 i) 4 i)
Connect → ¥ ×¥ = ▼ C →	₹ 4 X
Connect ♥ ♥ ♥ ■ ♥ ♥ ♥ ♥ ♥ ■ Databases ♥ ■ Databases ♥ ■ Security ♥ ■ Server Objects ♥ ■ PolyBase ♥ ■ Management ♥ ₹ XEvent Profiler	Mont Connect Disconnect Register New Query Activity Monitor Start Stop Pause Restart Policies Facets Start PowerShell Reports Refresh
	Properties

2 Navigate to Connections and confirm that Allow remote connections to this server is selected.

Server Properties - KW-FC64	4-9020\SQLEXPRESS
Select a page General	🖵 Script 🔻 😯 Help
 Memory Processors Security Connections Database Settings Advanced Permissions 	Connections Maximum number of concurrent connections (0 = unlimited): Use query governor to prevent long-running queries Use query governor to prevent long-running queries Default connection options:
	implicit transactions cursor close on commit ansi wamings ANSI NULLS arithmetic abort arithmetic ignore quoted identifier no count ANSI NULL Default On ANSI NULL Default Off concat null yields null numeric round abort
Connection	xact abort
Server: KW-FC64-9020\SQLEXPRESS	Remote server connections
Connection: KTD-KYOCERA.COM\kwong	✓ Allow remote connections to this server Remote query timeout (in seconds, 0 = no timeout): 600
L	

3 Check to see if this solves the problem.

Protocols for MSSQL Server

Check the SQL Server Network Configuration.

- **1** Open the SQL Server Configuration Manager.
- 2 Unfold the node SQL Server Network Configuration.
- **3** Select Protocols for MSSQL Server (the name of your SQL Server instance).

4 Confirm that TCP/IP is enabled.

Sql Server Configuration Manager File Action View Help ← ➡ 2 1			
 SQL Server Configuration Manager (Local) SQL Server Services SQL Server Network Configuration (32bit) SQL Native Client 11.0 Configuration (32k SQL Server Network Configuration SQL Protocols for SQLEXPRESS SQL Native Client 11.0 Configuration 	Protocol Name Shared Memory Named Pipes TCP/IP	Status Enabled Disabled Enabled	

Check Firewall

If there is still no communication happening between the computer and the remote SQL Server, configure the firewall settings. Start by checking which port is being used by TCP/IP.

1 Navigate to TCP/IP Properties.

TCP/IP Properties		?	×
Protocol IP Addresses			
🖯 IP1			^
Active	Yes		
Enabled	No		
IP Address			
TCP Dynamic Ports	0		
TCP Port	1433		
E IP2			
Active	Yes		
Enabled	No		
IP Address			
TCP Dynamic Ports	0		
TCP Port			
E 1P3			
Active	Yes		
Enabled	No		
IP Address	10.10.18.107		
TCP Dynamic Ports	0		
TCP Port	1/33		~
TCP Port TCP port			
OK	Cancel Apply	y H	elp

- **2** Open that port in the Firewall.
- **3** Navigate to Computer Management to confirm that the SQL Browser service is running, and set to Automatic.

🌆 Computer Management										
File Action View Help										
Scomputer Management (Local	O Services									
V iii System Tools	SQL Server Browser	Name	Description	Status	Startup Type	Log On As				
> M Event Viewer		🙀 SQL Server Browser	Provides SQL Server connection information to client computers.	Running	Automatic	Local Service				
> 🕺 Shared Folders	Stop the service	SQL Server CEIP service (SQ	CEIP service for Sql server	Running	Automatic	NT Service\SQLTELEMETRY\$SQLE				
> 🜆 Local Users and Groups	Provides SQL Server connection information to client computers.	🖏 SQL Server VSS Writer	Provides the interface to backup/restore Microsoft SQL server thro	Running	Automatic	Local System				
> N Performance		SSDP Discovery	Discovers networked devices and services that use the SSDP discov	Running	Manual	Local Service				
📇 Device Manager		State Repository Service	Provides required infrastructure support for the application model.	Running	Manual	Local System				
🗸 🚰 Storage		Still Image Acquisition Events	Launches applications associated with still image acquisition events.		Manual	Local System				
📅 Disk Management		🖏 Storage Service	Provides enabling services for storage settings and external storag	Running	Manual (Trig	Local System				
 Services and Applications 		🍓 Storage Tiers Management	Optimizes the placement of data in storage tiers on all tiered stora		Manual	Local System				
Services		Superfetch	Maintains and improves system performance over time.	Running	Automatic	Local System				
WMI Control		Sync Host_d053d	This service synchronizes mail, contacts, calendar and various oth	Running	Automatic (D	Local System				
> () SQL Server Configuratic		System Event Notification S	Monitors system events and notifies subscribers to COM+ Event S	Running	Automatic	Local System				
		System Events Broker	Coordinates execution of background work for WinRT application	Running	Automatic (T	Local System				
		Task Scheduler	Enables a user to configure and schedule automated tasks on this	Running	Automatic	Local System				
		CP/IP NetBIOS Helper	Provides support for the NetBIOS over TCP/IP (NetBT) service and	Running	Automatic (T	Local Service				

4 Open Properties for the SQL Service Browser to change the Startup Type.

SQL Server Browser Properties (Local Computer)							
General Log On	Recovery Dependencies						
Service name:	SQLBrowser						
Display name:	SQL Server Browser						
Description:	Provides SQL Server connection information to client computers.						
Path to executable: "C:\Program Files (x86)\Microsoft SQL Server\90\Shared\sqlbrowser.exe''							
Startup type:	Automatic ~						
	Automatic (Delayed Start) Automatic						
	Manual Disabled						
Service status:	Running	* I					
Start	Stop Pause Resume						
You can specify the start parameters that apply when you start the service from here.							
Start parameters:]					
	OK Cancel Apply						

5 Restart the MSSQL Server service.

MSSQL is a Microsoft product. All resources are on the Microsoft website. Connections issues most likely relate to permissions and/or environment settings.

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, Suite 301 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, Ciudad de Mexico, C.P. 11560 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: +56-2-2670-1900 Fax: +56-2-2350-7150

KYOCERA Document Solutions

Australia Pty. Ltd.

Level 3, 6-10 Talavera Road North Ryde NSW, 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, Junggu, 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(0)20-654-0000 Fax: +31(0)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

Turkev A.S.

Altunizade Mah. Prof. Fahrettin Kerim Gökay Cad. No:45 34662 Üsküdar İstanbul, Turkey Phone: +90-216-339-0020 Fax: +90-216-339-0070

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

Borgarfjordsgatan 11, 164 40 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

Eiby Industrivei 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 (Ptv) 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 Czech, s.r.o.

Harfa Office Pari. Českomoravská 2420/15. Praha 9 Phone: +420-222-562-246

KYOCERA Document Solutions Inc.

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

