Kofax eCopy ShareScan

Installation Guide for Konica Minolta Devices

Version: 6.4.0

Date: 2021-09-08

KOFAX

Table of Contents

Preface

The Kofax eCopy ShareScan software extends the capabilities of digital copiers and scanners. When installing and setting up a ShareScan system, you must be familiar with the scanning device that you will use with ShareScan, the ShareScan software components, and the basic installation and configuration workflow.

This guide is intended for administrators responsible for the initial installation, configuration, and licensing of eCopy ShareScan. For the device-specific Pre-Installation Checklist (PICL), see the applicable vendor-specific Pre-Installation Checklist and Sizing Guide. For information pertaining to the ShareScan pre-installation, see this guide. For configuration and Administration Console usage, see the Administration Console Help (accessible via pressing F1 on the Administration Console).

This document is written under the assumption that readers are familiar with working within a server-client architecture and environment.

Product documentation

The full documentation set for Kofax eCopy ShareScan is available online:

https://docshield.kofax.com/Portal/Products/eCopy/6.4.0-gcd15cgg3d/eCopy.htm

The Kofax eCopy ShareScan documentation set includes the items listed in the following table.

Guide	Description
Kofax eCopy ShareScan Pre-installation Checklist (PDF)	Provides information on the issues to be addressed before deploying Kofax eCopy ShareScan.
Kofax eCopy ShareScan Installation Guide (PDF)	Provides information on how to install and upgrade Kofax eCopy ShareScan, along with hardware and software prerequisites.
Kofax eCopy ShareScan Administration Console Help	The integrated help of the application, covering the use of Kofax eCopy ShareScan beyond installation, including configuration information. **Note** The help is accessible by pressing **F1** on the ShareScan Administration Console.
Kofax eCopy ShareScan Troubleshooter User Guide (PDF)	Provides information on how to use the ShareScan Troubleshooter, a built-in diagnostic tool.

Guide	Description
Kofax eCopy ShareScan Release Notes (PDF)	Provides an overview of late-breaking details for the current product release.
Kofax eCopy ShareScan High Availability Deployment Guide (PDF) Kofax eCopy ShareScan	Provides guidance on how to deploy ShareScan to function in high availability mode.
Kofax eCopy ShareScan Glossary Editor Recommendations (PDF)	Contains information on proper use of the Glossary Editor Tool.

Training

Kofax offers both classroom and computer-based training to help you make the most of your eCopy ShareScan solution. Visit the Kofax website at www.kofax.com for details about the available training options and schedules.

Getting help with Kofax products

The Kofax Knowledge Base repository contains articles that are updated on a regular basis to keep you informed about Kofax products. We encourage you to use the Knowledge Base to obtain answers to your product questions.

To access the Kofax Knowledge Base, go to the Kofax website and select Support on the home page.

Note The Kofax Knowledge Base is optimized for use with Google Chrome, Mozilla Firefox or Microsoft Edge.

The Kofax Knowledge Base provides:

- Powerful search capabilities to help you quickly locate the information you need.

  Type your search terms or phrase into the **Search** box, and then click the search icon.
- Product information, configuration details and documentation, including release news.

  Scroll through the Kofax Knowledge Base home page to locate a product family. Then click a product family name to view a list of related articles. Please note that some product families require a valid Kofax Portal login to view related articles.
- Access to the Kofax Customer Portal (for eligible customers).

  Click the **Customer Support** link at the top of the page, and then click **Log in to the Customer Portal**.
- Access to the Kofax Partner Portal (for eligible partners).

  Click the **Partner Support** link at the top of the page, and then click **Log in to the Partner Portal**.
- Access to Kofax support commitments, lifecycle policies, electronic fulfillment details, and self-service tools.

  Scroll to the **General Support** section, click **Support Details**, and then select the appropriate tab.

Chapter 1

Pre-installation

This chapter describes important tasks to be performed prior to installing or upgrading eCopy ShareScan, along with requirements that must be met before product installation.

Note The eCopy ShareScan installer cannot be launched if any files from the installation package are blocked by the operating system for security reasons. You can unblock the files one by one on the respective Properties dialog box, or by running the following PowerShell command as an administrator from the root folder of the installation:

```
Get-ChildItem -Recurse | Unblock-File
```

Typical installation workflow

Kofax eCopy ShareScan supports three typical installation and upgrade scenarios, which are briefly outlined below. For a more detailed description, see Install ShareScan.

Install Kofax eCopy ShareScan 6.4.0 with no previous version already present

- Ensure that the eCopy ShareScan prerequisites (listed in the following chapter) are installed.
- Start the eCopy ShareScan installer, and follow the Installation Wizard prompts.

Upgrade from Kofax eCopy ShareScan 5.x to 6.4.0

Important A direct upgrade from eCopy ShareScan 5.0, 5.1 or 5.2 is not supported in a 5.x to 6.4.0 upgrade scenario.

Before you start the upgrade process, ensure that your current eCopy ShareScan installation is working properly. The easiest way to do this is to start the Administration Console and verify that it launches without errors.

Upgrade from versions pre-dating 5.4

If you are upgrading from a eCopy ShareScan version earlier than 5.4 (5.0, 5.1 or 5.2), you first need to upgrade to 5.4. Once you have a verified working installation of eCopy ShareScan 5.4, you are ready to proceed with the upgrade to version 6.4.0.

Upgrade from version 5.4 or higher

1. Exit eCopy ShareScan 5.x Administration Console.
2. Ensure that the eCopy ShareScan prerequisites (listed in the Pre-installation chapter) are installed.
3. Run the eCopy ShareScan 6.4.0 installer.

4. After the Welcome screen, select **Upgrade from previous version to 6.4** or **Custom upgrade from previous version to 6.4,** and then follow the prompts to finish the upgrade.

System requirements for eCopy ShareScan Manager computer

The installation media contains all the required dependency installer files under the `Redist` folder, which must be installed to ensure that eCopy ShareScan functions properly:

- Amazon Correto 8 Java Runtime (x86) – version 8.275.01.1
- Microsoft .NET Framework 4.8
- Microsoft Visual C++ 2012 Redistributable (x86) – version 11.0.61030.0
- Microsoft Visual C++ 2019 Redistributable (x86) – version 14.27.29016.0
- Microsoft Visual C++ 2019 Redistributable (x64) – version 14.27.29016.0
- Microsoft Visual J# 2.0 Redistributable

The installer skips any of the dependencies listed above if they are already installed on the target system, which considerably reduces installation time.

Note The Microsoft Visual J# 2.0 Redistributable must be manually installed from the installation media. Before installing this prerequisite, Microsoft .NET Framework 3.5 SP1 must also be manually installed.

Operating systems

- Windows 10 1803 or later (x64)
- Windows Server 2012 R2*
- Windows Server 2016*
- Windows Server 2019*

  * 64-bit support as a 32-bit application
- The ShareScan Administration Console and the ShareScan Manager cannot be installed on Linux, Solaris or Macintosh operating systems.

Note The eCopy ShareScan installer cannot be launched unless Microsoft .NET Framework 4.8 is installed on the target system. When trying to launch the installer with no .NET Framework or any version older than 4.8 installed, an error message appears to describe the dependency and the installation media path for the offline .NET Framework installer. To close the message and exit the installer, click **OK**. For more information on .NET Framework versions and operating system related dependencies, click here.

Database

- Microsoft SQL Server 2014 Express edition, or later

Database permissions

For working with the ShareScan databases in an upgrade scenario, you must use an account that has **db_owner** Database-Level Role permissions for the eCopy ShareScan database. An account with sysadmin Server-Level Role can be used, but it is not mandatory. For database permissions required for

a new installation, see "User rights necessary for ShareScan database creation" in your *Kofax eCopy ShareScan Installation Guide.*

Do not use an sa account as a ShareScan runtime account for database connection, as it does not work. Use only the eCopy account created by the ShareScan database installer, or a user having the same user rights as the eCopy account. If you use Integrated Windows Authentication for database connection, the user accounts specified during installation should have the proper rights.

Virtual environments

Important Installing eCopy ShareScan on a virtual machine with a Microsoft operating system has always been supported, but Kofax does not certify virtual platforms. As long as adequate resources are allocated to the virtual machine, eCopy ShareScan should function as expected. Ultimately, it is the customer's responsibility to ensure that the virtual environment is configured correctly. Avoid desktop class machines, since they do not have enough resources to support high-volume processing.

- VMware ESX Server 4.x and 5.x or higher
- VMware Workstation 7.x, 8.x, 9.x, 10.x, 11.x and 12.x or higher
- Microsoft Hyper Visor (Hyper-V) Server 2012 or higher

Memory configuration

This topic lists the required memory configurations for installation for the ShareScan Manager computer.

- 8 GB physical memory (minimum)
- 5 GB disk space (including SQL server and prerequisites)

For more details on recommended memory configuration, see the **Sizing recommendations for embedded configurations** section in the *Pre-Installation Checklist and Sizing Guide*.

Checklist for the ShareScan Manager computer

This topic lists all system requirements that must be met for installation on the ShareScan Manager computer.

- ShareScan installs a customized Apache Tomcat web service, as previously installed Tomcat installations are not supported.

  Important The original version of the Apache Tomcat web service is 9.0.41, which is a 32-bit installer. Also, If you do not want to install a web client during the installation, ignore any Apache Tomcat references. If you install the web client, the simulator function of the ShareScan Administration Console defaults to using the web client for the simulator.

- ShareScan 6.x licenses are installed to a SQL Server to allow easy management of devices. The ShareScan installer can install a local copy of SQL Server 2014 Express for managing licenses in

addition to storing configuration data. It can also create the appropriate database structure on an existing SQL server for consolidated key management.

Important Prior to installing ShareScan, it is important to determine if licenses will be managed individually from each ShareScan Manager, or if you prefer to manage all licenses from a single SQL Server.

Check	Description
☐	Ensure that ShareScan Manager is installed to a dedicated computer that is exclusively tasked for running ShareScan Manager.
☐	Run the Automatic Updates for the operating system before you start installing ShareScan. **Note** Make sure you turn OFF the Automatic Updates during the installation.
☐	When designing the network architecture, make sure you have Windows Server as an operating system if you plan to have more than 10 devices. **Note** Windows 10 can handle a maximum number of 20 concurrent network connections.
☐	If you have multiple NIC cards, you must select an IP address for ShareScan that will be used for device-server communication.
☐	Check if your file system format is NTFS.
☐	Ensure that Microsoft IIS is not installed or listening to the ports used by ShareScan (listed below).
☐	You must activate ShareScan 6.x license keys against a the Activation Server. Manual activation is available for servers that are unable to communicate directly with the Activation Server. **Note** • As licenses are tied to the ShareScan database, it is strongly recommended not to change the databases after ShareScan installation. • License keys can only be activated once, so you must inspect the setup carefully prior to activation. • All license keys provide a 30-day grace period before activation to ensure the license setup is as intended.
☐	If you plan to use the **Single Sign-On** feature of the Session Logon service, you must ensure the following: • The ShareScan Manager computer is a member of the domain for which Session Logon is configured. • The logged-in user running and configuring the Session Logon must be an Active Directory user with the necessary rights to read properties in Active Directory (this is a default value). • This Active Directory user must have the necessary rights to read Active Directory properties (generally this is a default behavior; however, this can be modified in Active Directory). • You use the Active Directory user account to log into this domain (and not into the local system).

Ports to be left open

If you plan to enable firewalls, you must leave the following ports open between ShareScan Manager and the multi-functional device.

Inbound	
TCP	443, 8080, 9030, 9600, 9610, 9650, 50002
UDP	9650
Outbound	
TCP	443, 8080, 9650, 50001, 50003
UDP	161 (SNMP), 8899, 9650

Note If any of these ports are in use, ShareScan displays a warning message. Ports in use do not block installation, but must be opened later for proper functionality.

Network configuration

Domains and Workgroups

eCopy ShareScan can be configured to run in either domain-based networks or workgroup environments. Windows 2012 or later domain environments are supported. A domain environment is recommended.

Subnets and VLANs

The ShareScan Manager computer can be on different subnets or VLANs from the multifunction devices, provided that the multifunction devices can communicate with the Manager computer using an IP address. If your multifunction devices span multiple subnets or VLANs, a router is required to pass packets back and forth. However, in these situations the UDP and the SNMP based device discovery mechanisms may not be functional. Also, consider that bi-directional communication is required between the ShareScan Manager and the MFPs (meaning both the devices shall be able to send TCP messages to the manager and vice versa), on the ports listed in section Checklist for the ShareScan Manager computer.

IP Addresses

Use static IP addresses for both the ShareScan Manager computer and the MFPs. To change the IP address of the Manager computer:

1. Remove all devices from the ShareScan Manager.
2. Stop all ShareScan related services.
3. Change the IP address of the NIC and make sure the network adapters use the new IP address (`ipconfig` command).
4. Start the services that you have stopped in step 2.
5. Re-add the devices to the ShareScan Manager.

Note If the IPv6 function is not in use, it should be disabled in the device settings to prevent first time connection errors such as the user cannot launch the application for the first start after sleep mode, as it runs into a connection error message.

Gateway Address

ShareScan does not require a gateway address.

Host Name

The host name must not exceed 60 characters. Device host names are resolved using DNS. This happens once you have added a device and confirmed it. If the device is not registered in the DNS, then its name in the Devices tab on the Administration Console may change after confirmation.

Note Changing the host name after installation can cause licensing and database issues, and is therefore not supported. If you must change the host name, you must re-install ShareScan.

Network Attached Storage Devices (NAS)

eCopy ShareScan 6.4.0 supports NAS drives and folders that are fully compatible with NTFS file system and Windows access control mechanisms.

Novell

ShareScan does not support direct communication between a ShareScan Manager computer and a multifunction device on Novell networks. However, when Novell client software is installed on the Manager computer, some Connectors (eCopy Quick Connect, and the eCopy Scan to Desktop) can bridge to a Novell server. A Novell client must be installed on the ShareScan Manager computer if Novell authentication of Scan Inboxes is required. The eCopy connector for LDAP/SMTP requires a Novell client to work properly with session logon.

Local Security Policy

To use the Administration Console on the ShareScan Manager computer, you require local administrator-level credentials. ShareScan Manager cannot be installed on a Domain Controller.

Support information

This section contains information about the various languages and third-party software supported by eCopy ShareScan.

Supported languages

Kofax eCopy ShareScan supports the following languages:

- English
- Brazilian Portuguese

- Dutch
- French
- German
- Italian
- Spanish
- Catalan (client only)
- Simplified Chinese (client only)
- Japanese (client only)

Note This list only refers to the languages available for the user interface. For the OCR process, the language support is much wider, comprising more than 100 languages.

Supported devices

For the most current information on supported devices, visit the Support Devices website.

Supported backend services

For a detailed list of supported versions for specific backend connectors, see eCopy connectors.

Chapter 2

Install ShareScan

The following chapter contains information on the various tasks associated with installing ShareScan

.

General procedure

To install, configure, and license eCopy ShareScan:

1. Install the ShareScan software on a network computer. You have the option to customize the database installation. For more information, see the Custom installation chapter of this guide.
2. Install ShareScan Client, if needed (for more information on installing the client, see the Client-side installation chapter of this guide).
3. Start the Administration Console.
4. Add licenses, add devices (if they do not appear automatically on the **Devices** tab), and/or set up scanners. The Model name (in the dialog that appears as part of device addition procedure) differs from the name of the Device (displayed in the tree control on the **Device** tab). The tree control on the **Device** tab contains the network (host) name of the devices (or the IP address of the devices, if the host name cannot be resolved). This ID is used as a unique identifier for the devices in the ShareScan system. This cannot be changed in the Administration Console, only via the Device administration user interface and / or in the network DNS (Domain name server).

   Note The Model name specified during device addition can be changed anytime via the **Modify Model Name** menu item in the Administration Console: **Devices tab > <<right click device name>> > Modify Model Name**).

5. Install and configure Services, Connectors, and Devices.

When you open the Administration Console, the **Welcome** page displays a list of the main feature highlights of the current version.

For in-depth information about configuring and managing the Services, Connectors, and Devices that ShareScan uses, refer to the Help.

To access the Help, click F1 or click the Help button that is located in the upper-right corner of the Administration Console.

Before you start

If you are about to deploy eCopy ShareScan as a High Availability system or want to enable eCopy ShareScan load balancing, consult the *Kofax eCopy ShareScan High Availability Deployment Guide*.

The present guide gives you guidance on installation in a basic or multi-manager setup.

Use the ShareScan installation program to install the software components on a network computer.

Note ShareScan is only compatible with the Apache Tomcat version included in the installation program. If you have Apache Tomcat already installed, remove it prior to installing ShareScan. If you have Skype installed, it can conflict with the Apache Tomcat installed by ShareScan. To avoid this issue, ensure that the **Use port 80 and 443 as alternatives for incoming connections** option is cleared in Skype.

Important Ensure that the ports used for both inbound and outbound network traffic are left open. See Ports to be left open.

ShareScan install scenarios

Note The eCopy ShareScan installer uninstalls previous version of ShareScan. With this, any separate eCopy products (Xerox TWAIN, ScanStation, Advanced FPE) are also uninstalled to facilitate proper operation of ShareScan. You have to manually re-install any of these required components.

Note Before running the ShareScan installer, you must ensure that you have the latest system updates on your computer and that automatic Windows updates are turned off.

Note Installing ShareScan to folders belonging to individual user profiles such as **My Documents** or **Documents and Settings** on older systems is not recommended.

If you are upgrading existing ShareScan versions, ShareScan performs a complete installation where you can only customize the installation location on **Destination Folder** screen and database access and service account credentials on the **Service Credentials** screen. When upgrading in a multi-manager deployment, it is recommended to upgrade the individual ShareScan managers one by one.

If you plan to deploy ShareScan in a high availability cluster with multiple ShareScan server nodes, follow the instructions in the *eCopy ShareScan Availability and Load Balancing Deployment Guide*. It is recommended to set up the individual ShareScan server nodes first, test their basic behavior and then move them into the high availability cluster as described in the *eCopy ShareScan High Availability and Load Balancing Deployment Guide*.

Note Do not use square brackets ([ ]) in the following since they are not handled correctly and are removed. If you need to use these characters in the password, please consider changing it for the time of the installation.

- User identifiers
- Passwords
- Database name fields

Follow these two basic scenarios when installing ShareScan.

Perform a new installation

The following topics contain scenarios about installing ShareScan to a clean system.

Complete installation

1. If you have a physical ShareScan installation media, insert it in the optical drive of your computer and browse to the folder where the `ShareScan6.4.exe` file is located. If you have a digital copy of the ShareScan installer, you can find the `ShareScan6.4.exe` file in the root folder.
2. Run `ShareScan6.4.exe`. The Choose Setup Language screen is displayed. Select a preferred language (English by default) from the list and click **Next**.
3. The Welcome screen is displayed. Click **Next**.
4. The installer displays the System Check screen. If prompted, select the preferred options from the lists. Click **Next**.

   Note This screen displays warnings on any possible issues that might have an impact on the proper operation of ShareScan and provides information on how to resolve them. If relevant, it also enables you to choose from more than one option such as the number of available network adapters for device-manager communication.

5. The Enter Product License Key screen is displayed. Provide your license key (22 characters with dashes). Click **Next**.
6. The End-User License Agreement (EULA) is displayed on the License Agreement screen. Accept the EULA and click **Next**.
7. The Setup Type screen is displayed. Select **Complete**. Automatic full installation is performed including the following features and settings:
   - **eCopy ShareScan Server** is installed
   - **Microsoft SQL Server** is installed
     - SQL Server 2017 Express is installed.

       Note Since you cannot connect to this type of database engine from another computer on the network, it is not recommended to use this option if you plan to share the installed database between multiple managers. In that case, select the Custom installation option.

   - **eCopy ShareScan configuration database** is created on the installed SQL Server
   - **eCopy ShareScan WebClient** is installed (including the Apache Tomcat server)

- Default eCopy credentials (username / password) is used for database access, with SQL server authentication
- `C:\Program Files (x86)\Kofax\ShareScan6.4\Server` is the default installation path

8. The Installation Configuration Summary screen is displayed. Review the information and if you are satisfied with the configuration click **Install**, otherwise click **Back** .
9. Click **Finish** when the Install Shield Wizard Completed screen appears. Alternately, you can click the Launch ShareScan System Checker tool to perform a check on the core components of the ShareScan system.

Custom installation

This task mentions the components that you must select or clear to perform a custom installation on a clean system.

Important In case you specify custom folders for all (or some) components such as for eCopy ShareScan and Apache Tomcat) during the installation, all selected folders must be different, otherwise the already installed system fails after the upgrade (such as a Service Pack installation).

1. Perform steps 1 - 6 as described in the Complete Installation section.
2. The Setup Type screen is displayed. Select **Custom**.
3. The Custom Setup screen is displayed. Select the program features you want to install and click **Next**. The following components can be selected for installation:
   - **eCopy ShareScan**: Mandatory component that you must install in all possible scenarios; you cannot clear it.
   - **Microsoft SQL Server** (selected by default): Select this component if you want a local installation of Microsoft SQL Server Express. These deployment options are recommended for small-scale deployments with a single manager. If you clear this component, the installer assumes you have an existing SQL Server installation either locally or on another server on the network to which you are planning to connect.
   - **eCopy ShareScan configuration database**: Select this component if you want to create a ShareScan configuration database. It is necessary to select this component:
     - if you install a single ShareScan Manager
     - if you plan to install multiple managers and you do not want to share the same database across them
     - if you plan to have multiple managers and you are installing the first ShareScan Manager.

     Note This component is selected by default. You can clear it only if the Microsoft SQL Server database engine component is cleared, but in this case you need to specify database properties on the Database Catalog Name and Database Server and Runtime Account Information screens.
   - **eCopy ShareScan WebClient** (selected by default): Select this component if you plan to use scanner devices with web browser enabled user interface.
4. The Select Java Runtime Environment screen is shown. Select your preferred environment:
   - **Amazon Corretto 8 Runtime (x86)**

- **Pre-installed Oracle Java SE Runtime Environment (x86) - version 1.8**.

Note If you select the second option you also need to specify the **JAVA_HOME path for Oracle JRE**. The installer detects your Oracle Java installation and populates this field with that path to its home folder. To modify this path click **Change**.

5. The Destination Folder screen is displayed. Click the **Change** button to modify the default destination folder for the ShareScan server, Kofax OmniPage Capture SDK, the Apache Tomcat web server installation (the Apache Tomcat web server is required for ShareScan Web client) or Amazon Corretto 8 runtime. Click **Next**.

Upgrade ShareScan

When the ShareScan 6.4 installer is run on a machine which has a previous version of ShareScan installed, it offers two upgrade options.

Note

- If **custom service credentials** is set for the Agent and Manager service, the eCopy ShareScan 6.4.0 installer prompts for the Agent service user password and Manager service user password.
- Using the eCopy ShareScan 6.4 server with devices that have v5.2 JAR clients installed on them is not supported.

Upgrade from a previous version

Note ShareScan v5.0, v5.1 and v5.2 are not supported in an 5.x to 6.4 upgrade scenario.

1. If you have a physical ShareScan installation media, insert it in the optical drive of your computer and browse to the folder where the **ShareScan6.4.exe** file is located. If you have a digital copy of the ShareScan installer, you can find the **ShareScan6.4.exe** file in the root folder.
2. Run **ShareScan6.4.exe**; the **Choose setup language screen** is displayed. Select a preferred language (English by default) from the list and click **Next**.
3. The **Welcome** screen is displayed. Click **Next**.
4. The End-User License Agreement (EULA) is displayed on the **License Agreement** screen. Accept the EULA and click **Next**.
5. The **Setup Type** screen is displayed; select **Upgrade from previous version to 6.4**:

   Note This option removes the older ShareScan version, then proceeds to install the new one, preserving configuration data.

   - The **eCopy ShareScan Server** is installed.
   - Existing **eCopy ShareScan configuration database** is updated to the 6.4 schema.
   - **eCopy ShareScan WebClient** is installed (including the Apache Tomcat server).
6. If the installer is not able to use the default ‘sa’ credentials and the current Windows user does not have the necessary rights granted for database access, then the **Administrative Credentials for Database Creation** screen appears, where the proper (administrator level) credentials must be provided.

7. The **Installation Summary** screen is displayed. Review the information and if you are satisfied with the configuration click **Install**, otherwise click **Back**
8. Click **Finish** when the **InstallShield Wizard Completed** screen appears.

Custom upgrade from a previous version

Note ShareScan v5.0, v5.1 and v5.2 are not supported in an 5.x to 6.4 upgrade scenario.

1. If you have a physical ShareScan installation media, insert it in the optical drive of your computer and browse to the folder where the **ShareScan6.4.exe** file is located.If you have a digital copy of the ShareScan installer, you can find the **ShareScan6.4.exe** file in the root folder.
2. Run **ShareScan6.4.exe**; the **Choose setup language screen** is displayed. Select a preferred language (English by default) from the list and click **Next**.
3. The **Welcome** screen is displayed. Click **Next**.
4. The End-User License Agreement (EULA) is displayed on the **License Agreement** screen. Accept the EULA and click **Next**.
5. The **Setup Type** screen is displayed; select **Upgrade from previous version to 6.4**:

   Note This option removes the older ShareScan version, then proceeds to install the new one, preserving configuration data.

   - The **eCopy ShareScan Server** is installed.
   - Existing **eCopy ShareScan configuration database** is updated to the 6.4 schema
   - **eCopy ShareScan WebClient** is installed (including the Apache Tomcat server).
6. The **Select Java Runtime Environment** screen is shown. Select your preferred environment:
   - **Amazon Corretto 8 Runtime (x86)**
   - **Pre-installed Oracle Java SE Runtime Environment (x86) - version 1.8**. If you select the second option, you also need to specify the **JAVA_HOME path for Oracle JRE**. The installer detects your Oracle Java installation and populates this field with the path to the home folder. To modify this path, click **Change**.
7. The **Destination Folder** screen is displayed. Click the **Change** button to modify the default destination folder for the ShareScan server, Kofax OmniPage Capture SDK, the Apache Tomcat web server installation (the Apache Tomcat web server is required for ShareScan Web client) or Amazon Corretto 8 runtime. Click **Next**.
8. Specify service credentials on the Service Credentials screen. Use predefined local accounts, or specify custom service accounts for the ShareScan Manager and ShareScan Agent services. Click **Next**.

   Note If the installer detects a LocalDB SQL server connection from the previous ShareScan installation, the **Service Credentials** screen is not displayed.

9. At this point, the user can be presented with the following options:
   - If the installer is not able to use the default ‘sa’ credentials and the current Windows user does not have the necessary rights granted for database access, then the Administrative Credentials for Database Creation screen appears, where the proper (administrator level) credentials must be provided.

- The Database Server and Runtime Account Information screen: in case the user selected custom service accounts, as in this case the user is necessary to specify what authentication method / account should be used for database connection.

Note

- If **Windows authentication credentials given to ShareScan Agent Windows service** is selected and the administrative database user has no **db_securityadmin** database-level role (cannot create logins), the database administrator has to create the database users manually. Otherwise, the installed system will not operate properly.
- If the authentication method for the database connection is not changed to Integrated Windows Authentication, then the user name / password should not be changed; otherwise, the database connection may fail after installation. The reason is that in case of upgrade, existing users will not be recreated or their passwords changed.

10. The Installation Configuration Summary screen is displayed. Review the information and if you are satisfied with the configuration click **Install**, otherwise click **Back** .
11. Click **Finish** when the **InstallShield Wizard Completed** screen appears.

Maintenance

If you re-launch the ShareScan installer after successful installation of ShareScan 6.4.0, the Program Maintenance screen is displayed after you select a preferred language from the list on the **Choose setup language** screen and click **Next**. The following option is available:

Remove

- Removes all 6.4.0 features (Server, WebClient). The so-called dependency packages (SQL Server, Apache Tomcat, and so forth) can be removed from the **Programs / Features** manager of Windows.

Note If you install ShareScan 6.4.0 over an existing ShareScan version, removing version 6.4.0 does not bring back the previous ShareScan version. Removing the WebClient feature of ShareScan also removes the Apache Tomcat server.

Upgrade multiple ShareScan Managers

When performing multi-manager upgrade and you start to use Integrated Windows Authentication (instead of the Existing SQL Server type database authentication), then you need to use:

- Integrated Windows Authentication on all the managers you connect to the same 6.4 database
- The same windows service accounts on all the Managers you upgrade.

After you upgraded the first Manager to 6.4 with Integrated Windows Authentication, you cannot use the default service accounts for the Agent and Manager services when you upgrade the second one, but you have to specify the same Windows users you used on the first Manager.

Note

- For the time of upgrading multiple managers in any environment (NLB or standard), all managers should be stopped for the time of upgrading the first manager. Database modification is also done during the upgrade. When this is complete, the rest of tha managers can be started and upgraded one by one.
- Performing a multi-manager setup (when more than one ShareScan Manager connect to the same database catalog) and then upgrading from version 5.x is similar to the Custom upgrade scenario.

1. If you have a physical ShareScan installation media, insert it in the optical drive of your computer and browse to the folder where the **ShareScan6.4.exe** file is located.If you have a digital copy of the ShareScan installer, you can find the **ShareScan6.4.exe** file in the root folder.
2. Run **ShareScan6.4.exe**; the **Choose setup language screen** is displayed. Select a preferred language (English by default) from the list and click **Next**.
3. The **Welcome** screen is displayed. Click **Next**.
4. The **Setup Type** screen is displayed; select **Custom upgrade from previous version to 6.4**: the installer performs a complete installation, preserving configuration data:
   - The **eCopy ShareScan Server** is installed.
   - Existing **eCopy ShareScan configuration database** is updated to the 6.4 schema or a clone (copy) of the currently used ShareScan database is updated to the 6.4 schema and put in use for the upgraded installation (the actual behavior is specified on the screen detailed in step 8 below).
   - **eCopy ShareScan WebClient** is installed (including the Apache Tomcat server).
5. The **Destination Folder** screen is displayed. Click the **Change** button to modify the default destination folder for the ShareScan server, the Apache Tomcat web server installation (the Apache Tomcat web server is required for ShareScan Web client) or Amazon Corretto 8 runtime. Click **Next**.
6. Specify service credentials on the **Service Credentials** screen. Use predefined local accounts, or specify custom service accounts for the ShareScan Manager and ShareScan Agent services. These accounts must be valid domain accounts (users). Click **Next**.
7. The **Administrative Credentials for Database Creation** screen is displayed. If the default 'sa' credentials do not work, or the actual Windows user running the installer does not have rights to update the database. Otherwise this screen is not shown.
8. The **Database Catalog Name** screen is displayed. You have three basic scenarios:
   a. If you select the **Use current catalog for database upgrade** radio button in the first manager upgrade installation sequence, the procedure is identical with the single manager Custom upgrade from a previous version installation scenario. In this case, the name of the database catalog remains the same (eCopyShareScan), but its structure changes hence if there are multiple managers, only the first Manager currently upgraded will be able to operate correctly, while the other Managers will not, until they are upgraded as well. As a consequence, selecting

this option is recommended if all the Managers connecting to the same database are stopped during the whole upgrade process (of all the Managers).

Note This option is also useful in scenarios when your database administrator (DBA) does not provide an administrative account eligible for backup/restore operations. In such case, the DBA must create a copy of the eCopyShareScan database catalog (with a different name) on the same database server (and on the same instance). Then you need to switch one of your Managers to this copied database (via the **Database configuration** option of the ShareScan Administration Console), and upgrade it by selecting this option. Further Managers can then be upgraded by selecting **Option iii** described below.

b. When upgrading the first Manager, select the **Copy current catalog to perform the upgrade on the following one** radio button and specify a database name. This option makes a copy of the already existing database catalog with outdated structure and upgrades the copy reconfiguring the Manager to use it. This way the other Managers are able to use the old catalog without any hindrance. To perform this successfully, the user must have **db_backupoperator** database-level role and DBCREATOR server level permission since these allow backup and restore operations.

c. When upgrading the second and all further Managers, select the **Use a different existing ShareScan catalog** radio button and select the newly created / updated database, already upgraded to 6.4 level. You have to select the database catalog name provided during the upgrade the first Manager.

Note The list only contains catalog names that are not the original ones and the ShareScan Manager to be currently updated is also listed; the Manager is reconfigured to use the new database catalog name.

Click **Next**.

9. The **Database Server and Runtime Account Information** screen is displayed if the service credentials were modified. You need to provide the runtime account information for the configuration database. Click **Next**.
10. The Installation Summary screen is displayed. Review the information and if you are satisfied with the configuration click **Install**, otherwise click **Back** .
11. Click **Finish** when the **InstallShield Wizard Completed** screen appears.

Custom installation scenarios

- How to install all components
- How to install without Microsoft SQL Server
- How to install the eCopy ShareScan Server and WebClient only

How to install all components

Note If you clear the eCopy ShareScan WebClient component, the installation scenario is comprised of the same steps described below, respectively.

This custom setup scenario installs all four components:

- eCopy ShareScan Server
- eCopy ShareScan configuration database
- Microsoft SQL Server
- ShareScan WebClient

1. Once you select all components and/or optionally clear the ShareScan WebClient component on the Custom Setup screen, click **Next**.
2. The Destination Folder screen is displayed. Click **Change** to modify the default destination folder for the ShareScan server or the Apache Tomcat web server installation. The Apache Tomcat web server is required for ShareScan WebClient. Click **Next**.
3. Specify service credentials on the Service Credentials screen. Use predefined local accounts, or specify custom service accounts for the ShareScan Manager and ShareScan Agent services. These accounts must be valid domain accounts (users). Click **Next**.

   Note When you provide valid non-default accounts for the manager and the agent and then click **Grant** after the installer detects that some local privileges are not granted to the service accounts, the installer tries to grant the missing privileges.

   If this cannot be successfully performed, the installer still detects that the privileges are missing and does not continue the installation. The user must exit from the installer, resolve the issue, and either grant the missing privileges manually or eliminate the blocking factor to allow the installer to grant them during the next run. Then the installer must be re-run.

4. Specify the password option for the system administrator (sa) of the SQL Server to be installed on the Local Database Server screen. Select **Use default password specified by ShareScan** or override the default password of the SQL Server system administrator (the sa password) by selecting **Specify a custom password**. If you do so, you must provide a password that complies with the password policy in effect. Click **Next**.
5. The Installation Summary screen is displayed. Review the information and if you are satisfied with the configuration click **Install**, otherwise click Back. **Install**.
6. Click **Finish** when the Install Shield Wizard Completed screen appears.

   Note

   - If the eCopy ShareScan WebClient component is selected, this scenario is equal to the complete installation scenario, since all four components are installed. You still need to specify related settings on the Destination Folder, Service Credentials, and Local Database Server screens. Or, you can click through these screens without updating the default settings.
   - If you specified **custom service credentials** in step 3, the eCopy ShareScan installer will prompt for the Agent service user password and Manager service user password.

How to install without Microsoft SQL Server

Note If you clear the eCopy ShareScan WebClient component, the installation scenario is comprised of the same steps described below, respectively.

This custom setup scenario installs the following three components:

- eCopy ShareScan Server
- eCopy ShareScan configuration database
- eCopy ShareScan WebClient

1. Once you clear the **Microsoft SQL Server** component and/or optionally clear the eCopy ShareScan WebClient on the Custom Setup screen, click **Next**.
2. The Destination Folder screen is displayed. Click **Change** to modify the default destination folder for the ShareScan server, the Apache Tomcat web server installation (the Apache Tomcat webserver is required for eCopy ShareScan WebClient) or Amazon Corretto 8 runtime. Click **Next**.
3. Specify service credentials on the Service Credentials screen. Use predefined local accounts, or specify a custom service account for the ShareScan Manager and ShareScan Agent services. These accounts must be valid domain accounts (users). Click **Next**.

   Note When you plan to use a SQL Server on a different computer than the one used for Manager installation (remote SQL Server) with integrated Windows authentication for the database connection, you must use (custom) domain accounts as service accounts, because the predefined local accounts cannot connect to a remote database via Integrated Windows authentication. Using the predefined local accounts with a remote SQL Server is still possible if (username / password based) SQL Server authentication is used.

4. The Administrative Credentials for Database Creation screen is displayed. On this screen, the hostname or IP (and optionally, the instance name) of the SQL Server must be specified. The credentials entered on this screen are required while installing or upgrading the database. The information is not stored; it is only required during the installation or upgrade process for the database connection. The following options are displayed:
   - SQL Server host / instance name input box — the host name and, optionally the instance name of the SQL Server to use must be specified, such as `SQLSRV-01, CORPSQL1\SHARESCAN, 10.140.1.23\SSCAN1`

   You need to select one of the following options:
   - SQL Server authentication credentials created by ShareScan.
   - The Windows identity of the user running the ShareScan installer.
   - Specifying a user ID and the corresponding password (use SQL Server authentication). This can be an `sa` account with the corresponding password, or it can be a completely different user ID that is valid on the SQL Server having the proper rights for the ShareScan database creation.

   Click **Next**.
5. The Database Catalog Name screen is displayed. Specify the ShareScan database name here or leave the default name. Click **Next**.

6. The Database Server and Runtime Account Information screen is displayed. You can specify a runtime account for the configuration database.

   You need to select a method how the ShareScan services connect to the SQL Server database:

   - Via **SQL Server authentication credentials with default eCopy database user**, using the default user name **eCopy** and the default password.
   - Via **Windows authentication credentials given to ShareScan Agent Windows service**, using the identity of the accounts running the ShareScan Agent Windows service available only if custom accounts were specified on the previous wizard screen.

     Note If this option is selected, and the administrative database user has no **db_securityadmin** database-level role (cannot create logins), the database administrator has to create the database users manually; otherwise, the installed system will not operate properly.

   - Via **SQL Server authentication credentials below**, you can specify the user name and password.

     Note If the runtime user (SQL server user or Windows login) exists on the SQL Server specified for any reason, you must provide the same user credentials / account existing on the SQL Server. If the provided credentials are valid, these are used during installation and as runtime connection accounts.

   Click **Next**.
7. The Installation Summary screen is displayed. Click **Install**.
8. Click **Finish** when the InstallShield Wizard Completed screen appears.

   Note If you specified **Custom Service Credentials** in step 3, the eCopy ShareScan installer will prompt for the Agent service user password and Manager service user password.

How to install Server and WebClient only

This custom setup scenario installs the following two components:

- eCopy ShareScan Server
- eCopy ShareScan WebClient

Note If the eCopy ShareScan WebClient component is cleared, the installation scenario is comprised of the same steps described below, respectively.

1. Once you clear the **Microsoft SQL Server** and **eCopy ShareScan configuration database** components and/or optionally clear the **eCopy ShareScan WebClient** component on the **Custom setup** screen, click **Next**.
2. The **Destination Folder** screen is displayed. Click **Change** to modify the default destination folder for the ShareScan server or the Apache Tomcat web server installation (the Apache Tomcat web server is required for ShareScan WebClient). Click **Next**.
3. Specify service credentials on the **Service Credentials** screen. Use predefined local accounts, or specify custom service accounts for the ShareScan Manager and ShareScan Agent services. These accounts must be valid domain accounts (users). Click **Next**.

4. The Database Catalog Name screen is displayed. On this screen, you must specify the hostname or IP and optionally, the instance name of the Microsoft SQL Server where the existing 6.4 ShareScan database is hosted. You must also specify the existing database name. Click **Next**.
5. The Database Server and Runtime Account Information screen is displayed. You need to provide the runtime account information for the configuration database. Click **Next**.

   Note If the **Windows authentication credentials given to ShareScan Agent Windows service** radio button is selected, the database administrator has to create the database users manually; otherwise, the installed system will not operate properly.

6. The Installation Summary screen is displayed. Review the information and if you are satisfied with the configuration click **Install**; otherwise, click **Back**.
7. Click **Finish** when the Install Shield Wizard Completed screen appears.

   Note If you specified custom service credentials in step 3, the eCopy ShareScan installer will prompt for the Agent service user password and Manager service user password.

   You are now ready to configure a connector profile.

User rights for database creation

These sections list the supported user rights scenarios for ShareScan database creation, from the least restrictive to the most restrictive.

Administrative account with 'sysadmin' fixed server-level role (sa)

Since eCopy ShareScan 5.1, `sa` rights are not required for database installation, supporting the cases listed below. Having `sa` rights simplifies the process, because you do not need to set anything on the SQL server.

Administrative account with ‘dbcreator’ and ‘securityadmin’ fixed server-level roles

These rights are enough to create both the ShareScan database and the login ID of the runtime account. If you are connecting to a corporate database server, and your database administrator is not providing you the credentials of the `sa` account, then the database administrator needs to provide another account for the ShareScan database installation with lower privileges, having the `dbcreator` and the `securityadmin` fixed server-level roles.

This administrative user will be a `db_owner` on the created ShareScan database.

Administrative account ONLY with ‘dbcreator’ fixed server-level role

If the security policy is stricter, the login ID in SQL Server for the ShareScan runtime account must be created by the database administrator manually. This manually created SQL Server login ID or Windows user name (if integrated authentication is used) must be used on the **Database Server and Runtime Account Information** screen of the ShareScan Installation Wizard. This manually created login needs to have a public fixed server-level role and it is not required to have it mapped to any database. It will be

mapped to the ShareScan database with a minimal set of user rights necessary for the proper operation of the ShareScan server.

This administrative user will be a `db_owner` on the createdShareScan database.

Most restrictive environment

The most restrictive scenario (if database access is considered) the ShareScan installer supports is similar to the previous scenario, with the following additional restrictions:

- The database administrator must create the empty ShareScan database. You can select any name.
- An account must be provided on the **Administrative Credentials for Database Creation** screen to enable the creation of the ShareScan database content. For this, the account needs to be a `db_owner` on the empty database.
- The account does not need to be a member of the `dbcreator` or `securityadmin` fixed server-level roles.

In any of the above cases, the Installer Wizard checks the server connection and the provided credentials, and it also checks if the accounts or users provided have the necessary rights granted. If the user rights are not set properly, the corresponding error message is displayed.

On the **Administrative Credentials for Database Creation** screen, you can select an option when the database creation is performed in the name of the Windows user currently running the ShareScan installer. In case of a centralized corporate database server, this option allows the database administrator to use a Windows (domain) account as the database creator, using any of the above options according to the security policy in place.

Profile tool

The Profile Tool allows you to manage connector, service profile information, watchers and data publishing maps between ShareScan Managers. You can export such profile information from a Manager, then start up another Manager, and import the profile information.

Unlike connector profiles, newly imported watchers do not automatically overwrite watchers with the same name already existing on the target machine. These imported watchers are created as new ones. To update a watcher via import, first you have to delete the current watcher on the target machine and then do the import.

To access the tool, go to **Administration Console** > **Advanced tab** > **Tools** > **Profile Tool.**

To perform profile export, see How to export connector profiles.

To perform profile import, see How to import connector profiles.

How to export connector profiles

To perform an export, do as follows:

1. Go to **Administration Console** > **Advanced tab** > **Tools** > **Profile Tool.**

2. On the Export pane, use the drop-down icons to browse the connector or service whose profile information you want to export.
3. Right-click the connector or service in question.
4. Select **Export connector profiles** or **Export service profiles** (as appropriate).
5. Browse the location where you want to save the file. The generated file automatically has the `.profile` extension.

How to import connector profiles

To perform an import, do as follows:

1. Go to **Administration Console** > **Advanced tab** > **Tools** > **Profile Tool.**
2. On the Import pane, browse to locate the profile file you want to import.
3. Double-click the file to start the import process.

Client-side installation

The following chapter contains information on installing device-specific embedded clients and ScanStation drivers.

Configure the Konica Minolta Device

This section contains information on installing and configuring the Konica Minolta device.

Before configuring the device, make sure that the Konica Minolta i-Option, which enables Web access and document management functions from the MFP control panel, has been installed. To verify that i-Option has been installed, go to the User Box of the device and make sure that "Web Browser" appears in the list of applications.

- **Internet Explorer**: If you are using Internet Explorer, make sure that you set the "Check for newer versions of stored pages" option for Temporary Internet Files to "Every time I visit the webpage" .
- **Cookies**: It is recommended that you configure the device to accept all cookies so that the device does not prompt users to accept cookies each time they use ShareScan. For instructions, refer to the device documentation.
- **Focus rectangle**: You may want to change the color of the focus rectangle. For instructions, refer to the device documentation.
- **Time-outs**: It is recommended that you set the following time-out settings on the device. For instructions, refer to the device documentation.

To make ShareScan time out after nine minutes of inactivity, set the System Auto Reset Time, Copy, and Web Browser timeout settings to nine minutes. This keeps the screen from timing out while a document is being scanned or processed.

In certain scanning environments it is recommended that you increase the WebDAV Client time-out setting on the device. With the default setting of 60 seconds, scanning large documents or scanning concurrently from multiple devices may cause the device to time out. You can increase the time-out setting up to 300 seconds. For instructions, refer to the device documentation.

Note

- If you experience any issues with the soft keyboard, eCopy recommends that you recalibrate the device. On the control panel, go to "User Box", press the Accessibility key, and then press Touch Panel Adjustment. Follow the instructions on the screen.
- If you need complete security, it is recommended that you enable SSL (Secure Sockets Layers) on devices running ShareScan. For information about configuring SSL on the device, refer to the Konica Minolta documentation.

The Konica Minolta Embedded client also provides a performance-related switch via the Administration Console, which allows you to toggle between these settings:

- Maximum Performance (use the native software keyboard/physical keyboard of the MFP).
- Optimal (use an optimized eCopy soft keyboard).
- Maximum Usability (use the standard eCopy soft keyboard).

Device authentication

To configure device authentication to work with Session Logon:

1. Using the device's Page Scope Web Connection utility, configure the device to use **External Server Authentication**. For instructions, refer to the device documentation.
2. In the ShareScan Administration Console, select **Services**.
   The Configure Services pane opens.
3. In the Device Services group, select **Session Logon**.
   The Configure Session Logon Service pane opens.

Note If you want to configure device authentication to work with the ShareScan Session Logon feature, the device and Session Logon must use the same authentication type. For example, if you configure the device to use an NDS server and you configure Session Logon to use Microsoft Active Directory, device authentication will not work with Session Logon.

4. Specify the same authentication type for Session Logon that you specified in step 1 (for the device).

Note You must also make sure that the search parameters used to retrieve user names is the same in both environments. For example, if you configure the device to return "John Smith", but Session Logon expects "JSmith", authentication will fail on the Session Logon screen.

5. Click **Save**.
   The system saves the Session Logon settings in the ShareScan database

Configure a card reader

If you use the card reader that is shipped with your device, you must perform the following steps after you install the ShareScan software. To configure a card reader:

1. Activate the card reader hardware on the device.
2. On the device, enable user authentication. Make sure that you select **ON (MFP)**.

3. In the ShareScan Administration Console, enable the **Session Logon** feature.

   Note When you use the card reader with Session Logon, it is strongly recommended that you select "Account Name" as the Search On setting; this is because the account name is unique. If you do not select "Account Name" as the Search On setting, make sure that you follow the guidelines in step 4.

4. Register the user's card using a Microsoft Active Directory user name.

   Note
   - The user name that you specify on the registration screen must match the string that appears on the Session Logon screen. If you select "Account Name" as the Search On setting, you can select the correct string.
   - If you do not select "Account Name" as the Search On setting, you must enter the exact string that appears on the Session Logon screen. For example, if you select "First Name" as the Search On setting, you may need to enter a string similar to the following string: Joan Smith (JSmith).

Add devices with installed ShareScan client

After adding a license file to the ShareScan system, you can add one or more embedded or integrated devices.

1. Start ShareScan Administration Console.
2. Click **Add Device** on the toolbar. You can also select **Devices** on the **Welcome** page and then right-click the **Device Configuration** window and select **Add Device**. The **Add Devices** window opens.
3. If your device does not appear in the list, select **SNMP** instead of the **UDP** option from the **Discovery** list. If the autodiscovery does not succeed, use TCP/IP to add it manually.
4. Select the device you want to add.
5. Click **OK**. The device registration dialog opens
6. Observe the following:
   - If Secure Client is installed and this is the first time the device is added to ShareScan after client installation, a ShareScan related secure connection password must be set. Provide the new password for secure connection in the **Password** and **Re-enter password** fields and select **Secure image uploading** if you want image uploading to happen in secure mode. Click **OK**.
   - If Secure Client is installed and the ShareScan related secure connection password is already set, specify the password in the **Password** field and select **Secure image uploading** if you want image uploading to happen in secure mode. Click **OK**.
7. Choose a device model from the **A known model** list on the **Specify device model** dialog and click **Close** to finish device adding.

Batch add devices

If you want to add multiple devices in a batch, follow the instructions below:

1. Start ShareScan Administration Console.
2. Click **Add Device**, or select **Add device** from the context menu (by right-clicking in the **Device Configuration** window).

3. Select **Import** from the **Discovery** list; a standard **Open file** dialog is displayed and you need to select a file that describes the devices to add. The file must be a `.csv` file, containing data in the following format:

   `IP/host, vendor, model, password(string)`

   Example: `10.140.202.70, KONICAMINOLTA, C654, 12345678`

   - `IP/host`: device IP address(or host name).
   - `vendor`: must be KONICAMINOLTA.
   - `model (or *)`: specific device model name (or * to get the model name automatically from the device).
   - `password(string)`: device administrator password used for device registration.

   Note It is recommended to manually add a device to the Administration Console for a proper understanding of the .csv file content describing the devices.

4. The Administration Conosle displays the file content in the **Batch add devices progress** window and starts adding the devices one by one.
5. When processing is finished, the results are displayed in the **Batch add devices progress** window.
6. When you are done, click **Close**to exit the window and check the devices on the **Devices** tab.

   Note For instructions about removing devices, refer to the ShareScan Help.

Device Calibration Connector

This connector is intended as a tool for Quality Assurance or end-users for creating exception rules for the rotation problems they face with their particular scanner models.

Prerequisites

To use the Device Calibration connector, the following criteria must be met:

- Add a device you want to calibrate.

  Note When you add a device to ShareScan, specify a model name for the device (default offered is the one reported by the device or the driver). The exception rules of the connector will be saved for this particular model name (except when defining a rule for a scanner vendor).

- Assign the Device Calibration Connector to the device in ShareScan Administration Console. No connector profile parameters are needed in the Administration Console to use the connector.

No special license is needed, as the connector is included in the ShareScan package.

Usage

To create calibration rules, do the following:

1. Insert a single sheet in the position that you want to calibrate – that is, in the orientation for which the system produces a not appropriate result.

2. Select the scanning options you have problems with via the scanner setting bar of the main ShareScan screen on the device. These include:
   - Color depth
   - Paper size
   - Output Orientation
   - Double side scan options
3. Push the connector button on the Main screen to scan the page, and the preview appears.
4. Rotate the page you have problems with, using the rotation buttons on the Preview form. If you have a problem with the double-sided scanning, ensure you performed the corrective rotations for both pages. Also check that the orientation is correct (only the final orientation is important for the calibration).
5. Click **Next**.

   On the displayed screen, you can review the following settings and information for the exception rule of your device:
   - The bottom part shows the settings you used.
   - The **Vendor** and **Model** radio buttons allow you to select between applying the settings to all devices of a given vendor, or a specific device model, respectively.
   - The **Use this setting for all paper sizes** check box deletes all rules defined for specific paper sizes, except the rules created for Auto (or Free, or Mixed) input paper sizes. Saving the rule will use that for all paper sizes.
   - If you want to use separate rules for specific paper sizes, set them up after you set up the above generic rule. Otherwise, the generic rule overwrites the specific rules.
6. Click **Save** to store the settings in the `UserRotationAngles.xml` and `UserScanStationRotationAngles.xml` files, located at `C:\ProgramData\Kofax\ShareScan` (for Windows XP, the files are located at `C:\Documents and Settings\All Users\Application Data\Kofax\ShareScan\`).
7. The defined rules will be available only after restarting the ShareScan Manager windows service.
8. To remove the exception rules, delete these files, and restart the ShareScan Manager windows service.

Devices in scope

Device calibration typically needs to be carried out in the compact devices (e.g. C3350, C3850FS, C3351, C3851, 4050 or 4750).

Chapter 3

eCopy connectors

We recommend that you match the application credentials for various backend applications with the computer login credentials. We also recommend creating a generic, email-enabled ShareScan account for use with eCopy ShareScan.

Note The backend applications listed in this section belong to their respective owners, and as such, additional in-depth information is available from the documentation for the applications, and not in the eCopy ShareScan documentation.

The following backend applications are supported:

- eCopy connector for Microsoft Exchange (Mail and/or Fax)
- eCopy connector for IBM Lotus Notes (Mail and/or Fax)
- eCopy connector for LDAP/SMTP (Mail and/or Fax)
- eCopy connector for Scan to Desktop
- eCopy connector for Quick Connect
- eCopy connector for OpenText Fax Server (RightFax edition)
- eCopy connector for Scan to Printer
- eCopy connector for Microsoft SharePoint
- eCopy connector for OpenText Documentum
- eCopy connector for iManage WorkSite
- eCopy connector for OpenText Content Server - eDOCS edition
- eCopy connector for OpenText Content Server

Supported versions

This section lists the supported versions for the backend applications that work with eCopy connectors.

Backend Applications	Supported Versions	Installation Prerequisites
Microsoft Exchange (Mail and/or Fax)	Microsoft Exchange 2010, 2013, 2016, 2019, Exchange Online for Office 365	eCopy connector for Microsoft Exchange (Mail and/or Fax)
IBM Lotus Notes (Mail and/or Fax)	• IBM Lotus Notes 8.0 / 8.5 • Lotus Domino 8.0 / 8.5	eCopy connector for IBM Lotus Notes (Mail and/or Fax)
LDAP/SMTP (Mail and/or Fax)	• Microsoft LDAP v3	eCopy connector for LDAP/SMTP (Mail and/or Fax)

Backend Applications	Supported Versions	Installation Prerequisites
	• Open LDAP v2.4	
Quick Connect	• Quick Connect supports Oracle Database 10g and 11g. When you install Oracle Client 10g/11g, select the Custom Installation option and then make sure that you select the Oracle Provider for OLE DB component. This enables Quick Connect to connect to the Oracle database and store scanned documents and other information. • For more information about supported databases, see the eCopy ShareScan Technical Specifications document. • For additional information on supported configurations of eCopy ShareScan, Quick Connect to Database, see the Quick Connect Database Recommended Usage document available for download from eSPN.	eCopy connector for Quick Connect
OpenText Fax Server (RightFax Edition)	OpenText Fax Server 16.2, 16.4, 16.6, 20.2	eCopy connector for OpenText Fax Server (RightFax edition)
Microsoft SharePoint	2013, 2016, 2019, SharePoint Online for Office 365	eCopy connector for Microsoft SharePoint
OpenText Documentum	OpenText Documentum 16.4, 16.7, 20.2, 20.3	eCopy connector for OpenText Documentum
iManage WorkSite	9.5, 10, 10.1, 10.2, 10.3 and above (including iManage Cloud)	eCopy connector for iManage WorkSite
OpenText Content Server - eDOCS Edition	16.1-16.7	eCopy connector for OpenText Content Server - eDOCS edition
OpenText Content Server (Livelink)	10.5, 16, 16.2	eCopy connector for OpenText Content Server

eCopy connector for Microsoft Exchange (Mail and/or Fax)

For supported versions of Microsoft Exchange, see Supported versions in this guide.

Installation prerequisites

- If configuring the Exchange connector using Exchange Web Services protocol, the Exchange server SSL certificate must be installed on the computer running ShareScan Manager. Certificates must be installed to the Trusted Root Certification Authorities on the local computer.
- To configure and use Exchange Web Services protocol, the user's logon and alias name must correspond, due to limitations of the Exchange Web Services. Therefore, LDAP/Exchange Web Services protocol is recommended.

eCopy connector for IBM Lotus Notes (Mail and/or Fax)

For supported versions of IBM Lotus Notes, see Supported versions in this guide.

Installation prerequisites

- The connector requires a Lotus Notes client to be installed on the computer running the ShareScan Manager.
- At the time of configuration, the end user must be prepared to provide an Active ID File, user name, password, and Domino server name.
- When the installer for the Lotus Notes client prompts to choose between the **Multi-User Install** option and the **Single User Install** option, the administrator must select the **Single User Install** option.

Note If **Send messages from personal mail account** is not enabled, all emails will be sent from the user name and password supplied for configuration purposes. Before sending email from a personal Lotus Notes account, the eCopy Mail pass-through database on a Domino HTTP server must be configured.

eCopy connector for LDAP/SMTP (Mail and/or Fax)

For supported versions of LDAP/SMTP, see Supported versions in this guide.

Installation prerequisites

- For configuring the eCopy connector for LDAP, the following information is required:
  - User Name and Password
  - IP Address
  - DNS Name or URL for the directory being used
  - Search Criteria for users and recipients
  - LDAP Attributes and Port Number
  - Base DN of the base or root directory in which to search
- For configuring the eCopy connector for SMTP, the following information is required:
  - SMTP server IP address and SMTP port number

- DNS Name that will be used for outgoing messages
- User Name and Password

eCopy connector for Scan to Desktop

Installation prerequisites

- Scan to Desktop involves several different components to enable users to scan and send documents to a designated network folder location for modification and storage. A `Scan Inbox` subfolder may be added to existing network home directories, or the eCopy ShareScan software can create Scan Inbox folder locations. The Inbox Root (Inbox Management directory) stores the user list (`userdirs.txt`) that indicates which users have scan inboxes using Scan to Desktop; and whether eCopy ShareScan has created Inbox folders that would also reside under this directory.
- For detailed information on configuring Scan to Desktop, see the eCopy ShareScan Help, which is accessible by clicking F1 on the Administration Console.

Note The `Inbox alternate path for folder root - DO NOT set it to the user's HOME folder` (see documentation) path pointing to the existing Network Home Directory Root Folder is not supported, since eCopy ShareScan modifies the permissions on the root folder.

Inbox Root Directory

The Inbox Root Directory can reside on the ShareScan Services Manager computer or on a network server. If the directory resides locally, it must be configured as a share on an NTFS drive. If the directory resides on a network server, it must be configured as a share on an NTFS drive or on a NetWare drive.

Note The Inbox Root Directory must not be pointing to a user's home directory. Choose the Scan to Desktop Home Directory option in the connector instead. Also, network home directories configured through a login script are not supported.

ShareScanAdmin Group

- An Administrative Group must be used to implement the required security. In previous versions of eCopy ShareScan, this group required the name ShareScanAdmin. This administrative group can now be given any name; however, if multiple services managers are pointing to the same userdirs.txt file in the Inbox Root Directory, the group to which the service account belongs must be identical on all those services managers.
- The administrative group must be created on the domain controller for domain-based networks, on NDS for Novell networks, or on the local machine if the customer is in a workgroup environment. eCopy ShareScan uses this group when assigning permissions to the Inbox Root Directory, scanning inboxes and requiring Full Control.
- Permissions assigned to the directory are as follows:

Windows (NTFS)	**Novell (Netware)**
Administrators – Full Control	Administrators – Full Control

Windows (NTFS)	Novell (Netware)
Domain Administrators – Full Control (not used in workgroup configurations) ShareScanAdmin – Full Control	ShareScanAdmin – Full Control
Inbox Owner – Read or Delete	Inbox Owner – Read or Delete

- An account for an administrative user should also be created and added to the administrative group to be used as the service account. This user should have a standard user profile with a user name and password. If running in a workgroup environment, a local account should be created for each Scan to Desktop user on the computer where the Inbox location resides.

eCopy connector for Quick Connect

For supported versions of Quick Connect, see Supported versions in this guide.

Installation prerequisites

- When selecting a network location as a Quick Connect destination, make sure that future users have access to the folder or folders being used as storage options. Alternatively, the administrator can use the Logon As function to supply login credentials.
- To deliver scanned documents to an access database, you must disable User Account Control (UAC). To disable UAC, type `c:\windows\System32\UserAccountControlSettings.exe` to the command line and select the appropriate slider setting.

eCopy connector for OpenText Fax Server (RightFax edition)

For supported versions of OpenText Fax Server, see Supported versions in this guide.

Installation prerequisites

- The administrator is prompted to enter a valid RightFax or NT Authentication user name and password. The RightFax server name must also be entered.
- Delegation of privileges, phone books, cover sheets, and billing codes must be configured on the RightFax server in order to be utilized by the eCopy connector for RightFax.

Note The RightFax client software must not be installed on the system where the ShareScan Manager is installed. Also, if **Send from personal account** is not enabled, all faxes will be sent from the user name and password supplied for configuration purposes.

eCopy connector for Scan to Printer

Installation prerequisites

In order for a printer to be configured for use with Scan to Print, the appropriate print driver must be installed where eCopy ShareScan is also installed.

eCopy connector for Microsoft SharePoint

For supported versions of Microsoft SharePoint, see Supported versions in this guide.

Installation prerequisites

- The administrator must enter a user name and password that will enable browsing to all destinations, display all index fields, and store documents if Login As authentication is used.
- If you are using SharePoint 2007, you must have Microsoft Office SharePoint Server (MOSS) 2007 or Windows SharePoint 2007 Services.
- If you are using SharePoint 2010, you must have Microsoft SharePoint Server 2010.
- If your organization uses a secure SharePoint site, you must install an SSL certificate on the ShareScan server.

Note

- Dates are validated by the client regional settings. Invalid date formats are not accepted.
- The connector does not fully support storing to workspaces. However, storing to an attendee's location is inconsistent and may result in failure to store the scanned document.
- The All Day Event, Recurrence, and Workspace check boxes will not appear in the calendar list.

eCopy connector for OpenText Documentum

For supported versions of OpenText Documentum, see Supported versions in this guide.

Installation prerequisites

- The eCopy connector for OpenText Documentum uses the Documentum REST Services to connect to the Documentum Server. To install Documentum REST Services, see your Documentum product documentation.
- For configuring the eCopy connector for OpenText Documentum, the Documentum REST Services URL is required first. Then the Repository, which is a document database on the Documentum server, must be selected from the menu. In the connector administration, all repositories available through Documentum REST Services will then be available. The administrator should then enter a user name

and password that enables browsing to all desired destination locations within the selected repository, and then store documents.

Suggestions

- It is strongly recommended that you store documents using the doctype named `dm_document` or a customized doctype that is based on `dm_document`.

eCopy connector for iManage WorkSite

For supported versions of iManage WorkSite, see Supported versions in this guide.

Installation prerequisites

- The iManage DeskSite (32-bit) client must be installed to ensure that this connector functions properly, as the profile destination is configured with COM API Protocol. If iManage DeskSite (32-bit) client is not installed, an error message displays if the user attempts to configure a new connector profile destination with COM API Protocol, or use the connector profile configured in an earlier ShareScan version.
- The administrator should enter a user name and password that enables browsing to all destinations, display all index fields and store documents if `Login As` authentication is used.
- When you use Novell trusted login, make sure that the Novell client configuration on the computer running the ShareScan Manager includes a value for the **Preferred Server** option.

Note If you leave this field blank or you enter an incorrect value, users will not be able to store scanned documents.

Suggestions

- For information on impersonation passwords, the administrator can refer to the WorkSite documentation.

Note Impersonation is only available when using trusted login and authenticating against Novell.

eCopy connector for OpenText Content Server - eDOCS edition

For supported versions of OpenText Content Server - eDOCS edition, see Supported versions in this guide.

Installation prerequisites

- Before installing the eCopy connector for OpenText Content Server, the administrator must install and configure the Windows Explorer DM Extension software for OpenText Document Management, eDOCS

Edition 5.1, 5.2 SP1, 6.0 or later or Hummingbird DM 5.1, 5.2 SP1, and 6.0 on the same computer as the eCopy ShareScan Manager. Once done, the administrator must run the DM Connection Wizard. All versions of the DM Extension software include the required DM API and the DM Connection Wizard.

- The administrator must install the Windows Explorer DM Extension component only (under Optional Components) and select **Intranet Mode** (the default mode).

  Note Do not select **Internet Mode**.

- After installation, launch the DM Connection Wizard and enter the name of your DM server.
- The eCopy ShareScan Services Manager must have the same domain as the DM server, for the DM Connection Wizard to establish a connection with the server.
- The administrator will need to enter a valid eDOCS DM user name and password that has the ability to store documents if `Login As` authentication is used.

  Note
  - When the eDOCS DM Extension Client v 5.1.0.5 SR6 or later is installed on the same computer as the ShareScan Manager (not in the same domain as the DM server), you cannot configure the eCopy connector.
  - Default values that are assigned by the eDOCS DM server appear in the client. To use a different value, you must remove the default value and then use the Search feature or the Search while typing option to specify the new value.
  - If a profile for an application does not appear, contact your administrator. The application may be disabled from within the eDOCS DM software.

Suggestions

- You must add the eCopy Document Type and Application ID to your eDOCS (Hummingbird) server. See your server documentation for details.
- For instructions about installing the DM Extension software, refer to your eDOCS documentation.

eCopy connector for OpenText Content Server

For supported versions of OpenText Content Server, see Supported versions in this guide.

Installation prerequisites

- The administrator must enter a user name and password that enables browsing to all locations, display all index fields, and store documents if Login As authentication is used.
- The eCopy connector for Livelink ECM uses the Web services protocol and / or Livelink API (LAPI) for communication with Open Text Content Server.
- LAPI supports TCP/IP direct connections with native Livelink authentication. It does not support HTTP or HTTPS connections or non-native authentication methods. Native authentication using LAPI supports Livelink authentication, NTLM authentication, and LDAP authentication. The Livelink server

is responsible for managing the authentication settings and the connector works transparently with the selected authentication mode

- In **Protocol** section of **Database & authentication** settings in the Connector configuration window, the Administrator will need to provide the following information to properly configure the connector:
  - If **Web services** is selected:
    - **Root URL**: The root URL of the web service granting access to the Livelink server. Example: https://TestContentServer:443/cws

      Note Web services protocol does not support Table Key Lookup attributes.

  - If **LAPI** is selected:
    - **Livelink server**: The Open Text Content Server-Enterprise Server name. The server entered in the Livelink Server field must be on the same network (LAN) or connected via a VPN (WAN) as the Services Manager. It cannot be a web-only connected server. The Livelink connector does not communication over HTTP or HTTPS; instead it uses TCP/IP and LAPI over the specified port. Even if port 80 is entered in the port field, it will not force the connector to communicate over HTTP or HTTPS.
    - **Database**: The Livelink database name. The Livelink Database information can be found on the Livelink Administrative Site under the *Database Administration* section.
    - **Port**: The port used by the server. The default is 2099.

      Note LAPI protocol is not supported by OpenText Content Server (Livelink) version 16 or higher.

  - If **Web services and LAPI** is selected:
    - All the options can be configured that are listed in **Web services and LAPI** protocol sections above.

      Note If **Web services and LAPI** protocol is selected, LAPI is used only for supporting Table Key Lookup attributes. Since **Web services** protocol does not support Table Key Lookup attributes, LAPI is used only for supporting Table Key Lookup attributes if **Web services and LAPI** protocol is selected in **Protocol** section of **Database & authentication settings** in the Connector configuration window. he eCopy Connector for Open Text Content Server does not support Table Key Lookup attributes for OpenText Content Server (Livelink) version 16 or higher since LAPI protocol itself is not supported by this server

- If the OpenText Content Server environment requires the user to change password at the next logon, the user must change the password at the workstation before using eCopy ShareScan. If the user does not change, the system displays a message that the password has expired and that the user will not be able to store the scanned documents.

Note

- .NET Framework 3.5 SP1 and Microsoft Visual J# 2.0 Redistributable must be installed for proper functioning of this connector. The connector main screen in the Administration Console displays a warning message if .NET Framework 3.5 SP1 and Microsoft Visual J# 2.0 Redistributable are not installed.

Suggestion

- For authentication methods outside of these constraints, refer to your eCopy technical consultant.

Chapter 4

About licensing devices

eCopy ShareScan includes a Licensing wizard, which handles the following license-related tasks.

Every device that you use with Kofax software requires a valid license. ShareScan uses a digitally signed license file, which contains a unique license key generated by manufacturing. The license key is a unique ID that is associated with the hardware ID (HID) of the computer where the ShareScan database is installed.

Note The licensing in this eCopy ShareScan version is different from ShareScan 4.x licensing, which was based on the association of a product key with a device. Licensing is no longer associated with a particular device, but the HID of the SQL server.

Site licenses valid for activation with a predefined number of devices are also available. After a license file is created for the specified number of devices, it cannot be modified to increase the number of devices. If you purchase additional devices, you need to purchase additional licenses, and those licenses will be delivered as separate license files. When you load the new license file, the Administration Console can merge the original license file with the new file.

Note After adding a license, you can add one or more embedded or integrated devices to the Manager. You can add these devices at any time. However, if you add them before activating the license, a 30-day grace period starts for the license.

The Licensing wizard in this eCopy ShareScan version handles the following license-related tasks:

- Loading licenses
- Activating licenses
- Loading activated licenses
- Reactivating licenses
- Removing licenses

How to load licenses

You can use the automatic license download function, or import the license files. If no internet connection can be detected, only the second option is available.

1. Click **Load License** on the License wizard.
   The Welcome screen is displayed.
2. Click **Next** to continue.
3. Select **Download license automatically** when specifying the source to display the Automatic license download screen.

4. Copy the license keys of the licenses to download, in the text box and click **Add** after each. When the list below is complete, click **Next**.
   The Select license files to load screen is displayed.
5. Click **Browse** to add new files to the list of files to be imported. When finished, click **Start Import**.
6. Click **Start** to begin loading licenses.
7. Click **Finish** to close the License wizard.

How to activate licenses

You need to activate a license only once. Thereafter, it is associated with the computer where the ShareScan database is installed.

1. Click **Activate** on the License wizard.
   The **Welcome** screen is displayed. Click **Next** to continue.
2. Specify the hardware ID and click **Next** to continue.
3. Select **Automatic activation** on the Select activation mode screen and click **Next** to continue.
   The Output file creation / Activation screen is displayed.
4. Click **Start** to begin activation.
   The Specify file output screen is displayed. Click **Next** to continue.
5. Click **Finish** to close the License wizard.

How to load activated licenses

Use this option when importing already activated licenses to ShareScan.

1. Click the **Load activated** button of the License wizard.
   The Welcome screen is displayed.
2. Click **Next** to continue.
   The Select license files to load screen is displayed.
3. Click the **Browse** button to add new files to the list of files to be imported. When finished, click **Start import**.
4. Click **Start** to begin loading licenses.
5. Click **Finish** to close the License wizard.

How to remove licenses

Use this option when transferring licenses from the current ShareScan installation. After the removal is complete, the licenses can be safely transferred and reactivated.

1. Click **Remove** on License wizard.
   The Welcome screen is displayed.
2. Click **Next** to continue.
   The Select Licenses screen is displayed.
3. Select the licenses you want to remove and then click **Next**.

4. Click **Start** to remove the selected licenses.
5. Click **Finish** to close the **License** wizard.

How to generate a license report

The license report helps you create a report of the installed licenses. It is recommended to generate a license report whenever you activate your licenses. Keep the report in a safe place in case you need to restore the license information or for troubleshooting purposes.

1. Click **License report** on the License wizard.
   A Save As dialog box is displayed.
2. Browse to a preferred location where you want store license report file (optional).
3. Specify the name of the license report file in the **File Name** field.
4. Click **Save** to save the license report file.

Chapter 5

Post-installation

Now that you have completed the basic installation, configuration, and licensing steps, you are ready to perform other tasks, including:

- Configuring system settings
- Installing and configuring additional connectors, services, and extenders
- Licensing additional devices and monitoring activity between devices and the Manager
- Accessing and configuring other Managers
- Configuring, backing up, and restoring the ShareScan database

ScanStation post-installation

The ScanStation device automatically appears on the Devices tab. Test your configuration either by using the built-in Simulator, or by verifying the configuration at the device.

After installation, configure the following options:

- **Configuration**: If Show Title Bar is not checked, the client runs in kiosk mode. You can use the Password (exit) option for clients in kiosk mode to set up a password that is required to exit the ScanStation client.
- **Scanner Defaults**: Configure according to the device you are using. For more information, refer to the Administration Console Help.
- **ScanStation Startup Configuration**: Configure the options for the ScanStation client startup.

Configure ScanStation (examples)

This section outlines the basic process to:

- Configure a service (Activity Tracking)
- Configure an Extender (Forms Processing Extender)
- Configure a connector profile (QuickConnect) using the already configured service and extender
- Test your saved profile in the built-in simulator

When a user presses a connector button, the connector uses the settings specified in the connector profile that is associated with the button, such as the button label and image, encryption of scanned documents, and the services to use with the connector.

The recommended workflow is to configure services and extenders first, so that they are available when you configure a connector profile, and then configure connector profiles.

You have the option to set up any connector with the Bypass redirect screen option. Using this option navigates the user back to the Main Form at the end of the session, or logs out automatically if Session Logon is enabled.

The procedure in this section provides you with enough information to complete the basic configuration process. For in-depth information, refer to *Help for Kofax eCopy ShareScan*.

Configure a service - Activity Tracking example

1. Start the ShareScan Administration Console by clicking **Start** > **Programs** > **eCopy Applications** > **ShareScan 6.4** > **ShareScan Administration Console.**
   The system initializes the .NET framework, retrieves configuration information from the ShareScan database, and then displays the ShareScan Administration Console.
2. Select the **Services** tab.
   The **Configure Services** pane displays a list of the installed services, including connector services, device services, and common services.
3. In the **Device Services** list, select **Activity Tracking**.
   The **Configure Activity Tracking Service** pane appears.
4. Select **Yes** for the **Configured** setting and then click **Save**.
   For more information about configuring the Activity Tracking service, search for the **Activity Tracking** service topic in the Help.

Configure an extender - Forms Processing Extender example

In this example, this Extender is used to process scanned forms, extract form data, and make it available for Quick Connect via data publishing (using batching).

1. Configure the Extender. Then create a template library, and a template.

   Important Make sure your template contains at least one uniquely named zone from which content can be passed to Quick Connect.

2. Test your template.
3. After you finish designing and testing your template, make sure you enable batching in the Extender by selecting the **Batch on Matched Templates** check box.
4. Save your configuration.

Configure a Quick Connect connector profile to use Forms Processing Extender data

1. Select the **Connectors** tab.
   The **Configure Connectors** pane displays a list of the available connectors.
2. Select **QuickConnect**.
3. The **Configure Connector (Quick Connect)** pane and the **Settings** pane open.
4. Select the **Destinations** tab and then click **New**. Name the destination, set its **Type** and **Location**, and then specify **Authentication** options.
5. Select the **File name** tab, and set the file naming convention for the connector.
6. Optionally, select the **Index file** tab, and then set the index file attributes.

7. Use the **Settings** pane to configure the following:
   - Display settings
   - Workflow settings
   - Document settings
   - Service to be associated
   - Extender to be associated
   - Scanner settings
8. Click the **Save Current Profile** button. For more information about configuring the settings for a connector, open the applicable Help topic.

Test the profile configuration

1. In the Administration Console, select the **Devices** tab. The **Device Configuration** pane displays the simulator and any installed devices.
2. Select the device simulator. The **Configure Connectors for Device - Simulator** pane lists the available profiles.
3. In the **Select Profile(s)** column, select the profile that you created for the Quick Connect connector, and then click **Save**.
4. On the **Ribbon**, click the **Simulator** button. The simulated Client screen displays the button for the connector you configured.
5. Click the **Quick Connect** icon on the simulated client screen. The **Preview** screen is displayed.
6. Click **Next** to continue. The **Forms Processing Extender** screen is displayed.
7. Check the field values and then click **Next** to continue.
8. Select a **Destination** and then click **Send** to continue.
9. Select the post-processing option you want to use.

Creating self-signed server certificates

As eCopy ShareScan is using a self-signed server certificate based on the IP address of the server and this certificate is of an unknown Certification Authority, the device starts to display certificate related warning messages (such as 'Certificate security credentials could not be verified') after an OpenAPI SSL Communication is initiated. To avoid these messages, create a self-signed certificate based on the Fully Qualified Domain Name (FQDN) of the server and install it on the browser running on the device as a root certificate. You can manually create a self-signed certificate following the steps described in the **Create the certificate manually** section or using the Certificate Manager tool (see Certificate Manager section below).

Note The described procedure is working only on devices which have installed a Firmware that supports the OpenAPI Setup Function Version 3.7 or higher.

To check whether your device supports the OpenAPI Setup Function 3.7, enter the `http:///OpenAPI/DeviceDescription/` URL in a browser, and search for the Setup string in the document. If the device supports it, there is a corresponding FunctionInfo node in it:

```
<FunctionInfo>
…   <FunctionName>Setup</FunctionName>
    <FunctionVersion>
```

```
        <Major>3</Major>
        <Minor>7</Minor>
…
    </FunctionVersion>
…
</FunctionInfo>
```

Create the certificate manually

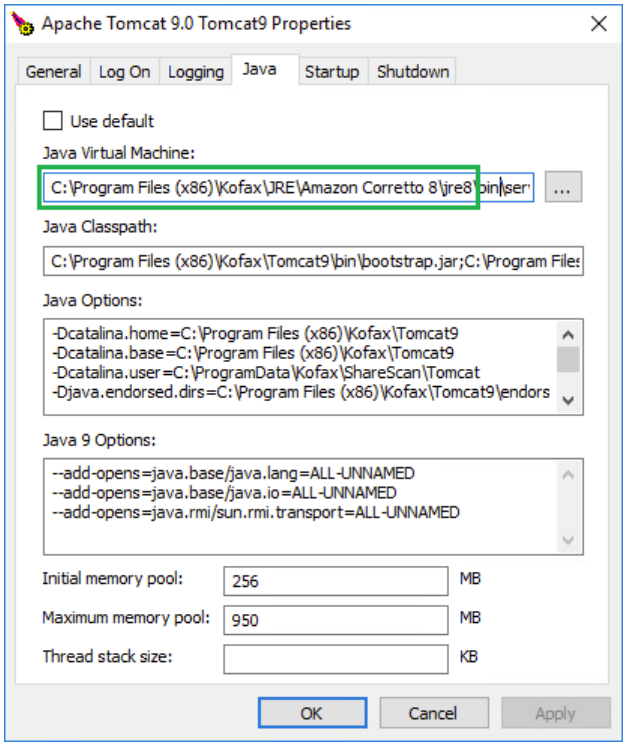
1. Stop the Tomcat service.
2. Generate the public and private key pair and export the public key to a *.der file.
   The following example refers to the Tomcat installation folder as TOMCAT_DIR (`%programfiles(x86)%\Kofax\Tomcat9`)
   a. Back up your current key files:
      - Back up `%TOMCAT_DIR%\conf\ecopy.key`
      - Delete `%TOMCAT_DIR%\conf\ecopy.key`
      - Back up `%TOMCAT_DIR%\webapps\ROOT\ecopy.pem`
      - Delete `%TOMCAT_DIR%\webapps\ROOT\ecopy.pem`
      - Back up `%TOMCAT_DIR%\webapps\ROOT\ecopy.cer`
      - Delete `%TOMCAT_DIR%\webapps\ROOT\ecopy.cer`
   b. Modify `%TOMCAT_DIR%\conf\createEcopyKey.bat`:
      - Change the `SET CERTIFICATE_COMMON_NAME= < ShareScan host IP address>` row to `SET CERTIFICATE_COMMON_NAME= < ShareScan host fully qualified domain name>`
      - Insert the `%KEYTOOL% -export %TOMCAT_ALIAS% -file "..\webapps\ROOT\ecopy.der"` row above the `%KEYTOOL% -export %TOMCAT_ALIAS% -file "..\webapps\ROOT\ecopy.cer"` row.
   c. Save and run `%TOMCAT_DIR%\conf\createEcopyKey.bat`.
   d. Restart the Tomcat service.
3. Install the certificate to the browser on the device you run ShareScan.
   a. Start the browser by pressing the **Application Menu** button and clicking **Web Browser**.
   b. Select **Address** on the browser toolbar, and enter `http://<ShareScan host IPaddress>:8080/ecopy.der`
   c. Enter the device password, then select **Root Certificate**.
4. Start ShareScan on the device to verify the results. There are no error messages but you might receive a "This page is protected" message; you can disable it with the check box under the message.

How to change the ShareScan Web client certificate to SHA1

On some older devices, an error message is displayed because this version of eCopy ShareScan uses SHA256 certificates by default. To avoid this error, administrators must generate SHA1 certificates the following way:

1. Locate the ShareScan Tomcat configuration folder. It is under `<KOFAX_INSTALL_FOLDER>\Tomcat9\conf\`. `<KOFAX_INSTALL_FOLDER>` is the folder in which ShareScan is installed. Its default value for this release is `c:\%programfiles%\Kofax`, but it can be changed when ShareScan is installed. The default Tomcat configuration folder for this release is `c:\%programfiles%\Kofax\Tomcat9\`.
2. Create a backup of the `createEcopyKey.bat` file found in this folder. The `eCopy.key` file contains the original SHA256 certificate. The `createEcopyKey.bat` script can be used to create a new one.
3. (Optional) Create a backup of the original SHA256 certificate and private keys if you want to restore the original certificates later. Back up the `eCopy.key` file located in the Tomcat configuration folder. Also back up the `eCopy.cer`, `eCopy.der`, and `eCopy.pem` files in the `<KOFAX_INSTALL_FOLDER>\Tomcat9\webapps\ROOT\`. The default location is `c:\%programfiles%\Kofax\Tomcat 9\webapps\ROOT\`.
4. Edit the `createEcopyKey.bat`. Replace the line `SET SIGALG=SHA256withRSA` with `SET SIGALG=SHA1withRSA.'`. Save the changed file. Administrator rights may be needed to save it.
5. Stop ShareScan Tomcat service. Open Windows Services and stop the Apache Tomcat 9.0 Tomcat9 service.
6. Delete the `eCopy.key file`.
7. Create the new certificate with `createEcopyKey.bat` file. This script needs 3 parameters, in this order:
   - The IP address of the host running the Tomcat service. You may also specify the FQDN instead of the IP address, but ShareScan was tested with IP-based certificates.
   - The location of the Java key tool. ShareScan installs a Java Runtime Environment (JRE) for itself, which contains a keytool that can be used. If you are not sure where the JRE is located run the

`<KOFAX_INSTALL_FOLDER>\Tomcat9\bin\Tomcat9w.exe` and check the Java tab in the opened application window.



The keytool is in the `<JRE_FOLDER>\bin` folder (for example, `'%programfiles(x86)%\Kofax\JRE\Amazon Corretto 8\jre8\bin\keytool.exe'`).

- The time period in days until the certificate is valid. 3650 days (10 years) is sufficient in most cases. An example running the script with correct parameters:

```
c:\%programfiles%\Kofax\Tomcat 9\conf>createEcopyKey.bat
10.140.25.107 '%programfiles(x86)%\Kofax\JRE\Amazon Corretto 8\jre8\bin
\keytool.exe'
3650
tomcat, Sep 25, 2017, PrivateKeyEntry,
Certificate fingerprint (SHA1):
30:C1:A3:2C:AC:18:27:A5:DE:DD:AE:B6:DB:0F:DF:47:80:FA:E2:6A
Certificate stored in file <..\webapps\ROOT\eCopy.der>
Certificate stored in file <..\webapps\ROOT\eCopy.cer>
Certificate stored in file <..\webapps\ROOT\eCopy.pem>
```

(Optional.) You can verify the signature algorithm name with the keytool running:

```
keytool -list -storepass changeit -v -keystore ./ecopy.key
```

8. From Windows Services, start the ShareScan Tomcat service.

Certificate Manager

The Certificate Manager is an add-on tool for eCopy ShareScan, which allows you to manage the certificates required by some devices. The tool is located in the <ShareScan installation folder>\Server \Tools folder, and can be launched by starting CertificateManager.exe.

When started, the Certificate Manager displays the following buttons in its window. Depending on your configuration, the first option (Configure Tomcat server.xml) may not be available:

- Configure Tomcat server.xml: This option allows you to customize the cryptographic protocols and ciphers used by ShareScan on a port-by-port basis by editing the server.xml file used by the Tomcat component of ShareScan. Clicking this button displays a new window, listing all ports currently used by ShareScan, and the cryptographic protocols assigned for the specific port, if that port uses SSL or TLS. You can use the server.xml item in the top-left corner to create a backup of the server.xml file you are using, or you can load a previously saved server.xml. To modify the protocols and ciphers assigned to a port, do the following:
  1. Click on the port whose properties you want to modify.
  2. Click the **Edit** button on the upper-right part of the window. A new screen is displayed, showing the currently used protocols and ciphers.
  3. Under **Enabled protocols**, select the cryptographic protocols you want to use (for example, TLSv1 or SSLv3).
  4. Under **Enabled Ciphers**, select the ciphers you want to use. For ease of use, a number of filter options are included with the tool and can be accessed via button push (for example, **Remove weak ciphers**, **Select Java 8 ciphers**, **Remove ciphers using CBC encoding**, and so on).
  5. Click **OK** to save the changes.
- **Re-generate certificate**: This option allows you to recreate your digital certificate. To create the certificate, you have to enter either the IP address (**Discover IP** button) or Fully Qualified Domain Name (**Discover FQDN** button) to the displayed field under **Certificate Common Name**, then click the **Generate** button on the lower-right part of the window.
- **Backup certificate**: This option creates a backup of your existing certificate. A Browse window is displayed, where you can select the location and file name of the certificate to be saved. Back up your certificates if you have imported your certificates manually to your devices (to prevent the warning from popping up), and do not want to repeat the process. Also, the recommended workflow when upgrading is to back up your certificate, upgrade ShareScan, then restore the certificate.
- **Restore certificate**: This option restores a certificate. A Browse window is displayed, where you can locate the certificate to be restored.

Next steps

After finishing the basic installation and configuration tasks, you can start using and customizing ShareScan via the Administration Console. In the Administration Console, all system functions are available on the ribbon and there are separate tabs for configuring services, connectors and devices.

System functions are available on the **Home** tab and the **Advanced** tab. The **Home** tab contains the most frequently used functions, such as managing the ShareScan Manager. The **Advanced** tab contains less frequently used functions and several new functions, such as managing the ShareScan database.

When you open the Administration Console, the **Welcome** page lists the main functions in the recommended order for performing each function:

- Configure one or more installed services, so that they will be available when you configure connectors and devices. There are three types of services:
  - Services that you apply to a connector
  - Services that you apply to devices or device groups
  - Services that you apply to connectors and devices
- Configure one or more profiles for the installed connectors that will be used on the scanning devices. You can create multiple profiles for each connector and you can activate each connector profile on multiple devices.
- Register ShareScan online.

When you click the services, connectors or devices links, a pane lists the items that you can configure. After you select an item, such as Session Logon, ShareScan opens one or more panes where you specify the appropriate settings.

Best practices

- Ensure that the `%temp%` environment variable is set.
- Ensure that all critical automatic updates are applied to target systems and that automatic updates are turned off for the time of installation.
- Do not wait too long to click **Install**, otherwise, the increased storage usage in the temp folder can trigger a cleanup process that causes installation failure.
- After installation, you may check to see whether the following services are running:
  - Apache Tomcat 9.0
  - ShareScan Agent
  - ShareScan Manager
  - ShareScan WatcherService
  - ShareScan Web Admin Host
  - PushKeyService
- There are other services which may not run by default, only if the respective functionality demands it:
  - Kofax Printer API
  - S2D Inbox Agent
- Tomcat service settings can be viewed/modified via: `%programfiles%\Kofax\Tomcat 9.0\bin\tomcat9w.exe`
- During the entire installation process, do not remove the original installation media from your optical drive, even though the installer has already extracted and decompressed the required components to a temporary location. This action can cause multiple failures depending on the stage of the installation during which the removal happens.
- To configure the Lotus Notes connectors (both Mail and Fax), you have to install the Lotus Notes Client on the computer. After installing, quit the client before running the ShareScan Administration Console, as the client locks the ID file, and a running client may cause issues with ShareScan.

- Ensure that there is no Apache Tomcat on the computer you want to install ShareScan on.
- Ensure that no ports used by ShareScan listed in the *Installation Guide* are used by other web services, as that may cause connectivity issues.
- Deploying the `RightFax FaxUtil` on the same machine on which ShareScan is running may cause issues, therefore it is not advised.
- If the Apache Tomcat component does not start after a Java update, a computer reboot solves the issue.
- If you use CAC, and get a Scanner is offline message after removing the CAC card during the scanning process, restart the ScanStation computer to return the system to normal state.
- If you have multiple ShareScan Manager computers in your deployment, it is recommended that you always use the same instance of the Administration Console to add, modify or remove connector profiles regardless of whether you are working in a cluster environment or not.

Technical support

This section contains guidelines on what information you must provide to Kofax support if you encounter issues when using ShareScan.

When contacting Technical Support (if a reseller) or your eCopy dealer (if an end-user), you must provide the following information to facilitate better and quicker interworking with Kofax Technical Support.

- eCopy system details:
  - ShareScan version number
  - Service Pack number (if applicable)
  - Product key and serial number
  - Approximate daily scanning load (pages/day)
  - Backend versions for all used connectors (for example, Exchange, Lotus Notes, or SharePoint)
- System specifications:
  - Server OS
  - Machine types
  - Jar versions
  - NIC speed settings
  - IP Addresses
- The exact workflow performed when the issue happens
- Does it happen to all users or just specific user accounts? (if specific only, please specify in details)
- A detailed description of the workflow which helps reproducing the issue
- The following files:
  - `msinfo32.nfo`
  - license dump (for license-related issues)
  - Logs from the ShareScan Troubleshooter Tool
  - Verbose trace file for the workflow
  - Client logs
  - If possible, the Wireshark logs

The **Tracing** service gives you the option to collect a variety of system data. On trace export, you can specify which sources to include in the output zip file (Troubleshooter log, configuration profiles and several other sources), which processes to dump and which device logs to pick.

Troubleshooting tips

Note Should you experience any of the following issues, consult the *eCopy ShareScan Troubleshooter User Guide* for a solution:

- Devices cannot be added in the Administration Console after upgrading to this eCopy ShareScan version.
- Administration Console does not work with devices added before the upgrade to this eCopy ShareScan version.
- Administration Console simulator does not work.

Below, you can find a number of known possible problem sources and solution tips:

- Ensure that there is no Apache Tomcat on the computer you want to install ShareScan on.
- Ensure that no ports used by ShareScan listed in the *Installation Guide* are used by other web services, as that may cause connectivity issues.
- Deploying the `RightFax FaxUtil` on the same machine on which ShareScan is running may cause issues, therefore it is not advised.
- If the Apache Tomcat component does not start after a Java update, a computer reboot solves the issue.
- Restoring database backups created via the ShareScan Troubleshooter is not possible via the ShareScan Administration Console. Use the relevant scripts for restoring such databases.
- When upgrading an existing ShareScan installation that has CAC configured, you must disable and re-enable CAC via the Administration Console after the upgrade process to this eCopy ShareScan version has finished.
- If you experience an infinite rebooting loop on your target machine, look for and delete the following registry keys:
  - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager Value: PendingFileRenameOperations`
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update Value: RebootRequired`