



# Tungsten eCopy ShareScan Pre-Installation Checklist

Version: 6.7.0

Date: 2024-04-24

**TUNGSTEN**  
**AUTOMATION**

© 2024 Tungsten Automation. All rights reserved.

Tungsten and Tungsten Automation are trademarks of Tungsten Automation Corporation, registered in the U.S. and/or other countries. All other trademarks are the property of their respective owners. No part of this publication may be reproduced, stored, or transmitted in any form without the prior written permission of Tungsten Automation.

# Table of Contents

<b>Introduction.....</b>	<b>5</b>
Product documentation.....	5
Training.....	6
Getting help with Tungsten Automation products.....	6
<b>Chapter 1: Pre-installation.....</b>	<b>8</b>
Typical installation workflow.....	8
System requirements for eCopy ShareScan Manager computer.....	9
Operating systems.....	9
Database.....	9
Virtual environments.....	10
Memory configuration.....	10
Checklist for the ShareScan Manager computer.....	10
Network configuration.....	12
Ports to be left open.....	13
Support information.....	16
Supported languages.....	16
Supported devices.....	17
Supported backend services.....	17
<b>Chapter 2: eCopy connectors.....</b>	<b>18</b>
Supported versions.....	19
eCopy connector for Microsoft Exchange (Mail and/or Fax).....	20
Installation prerequisites.....	20
eCopy connector for LDAP/SMTP (Mail and/or Fax).....	20
Installation prerequisites.....	20
eCopy connector for Scan to Desktop.....	21
Installation prerequisites.....	21
Inbox Root Directory.....	21
ShareScanAdmin Group.....	21
eCopy connector for Quick Connect.....	22
Installation prerequisites.....	22
eCopy connector for OpenText Fax Server (RightFax edition).....	22
Installation prerequisites.....	22
eCopy connector for Scan to Printer.....	23
Installation prerequisites.....	23

eCopy connector for Microsoft SharePoint.....	23
Installation prerequisites.....	23
eCopy connector for OpenText Documentum.....	23
Installation prerequisites.....	23
Suggestions.....	24
eCopy connector for iManage WorkSite.....	24
Installation prerequisites.....	24
Suggestions.....	24
eCopy connector for OpenText Content Server - eDOCS edition.....	24
Installation prerequisites.....	24
eCopy connector for OpenText Content Server.....	25
Installation prerequisites.....	25
Suggestion.....	26
<b>Chapter 3: Device checklists.....</b>	<b>27</b>
Canon device checklists.....	27
Checklist for using Canon devices with embedded clients.....	27
Checklist for using Canon devices with ScanStation.....	28
Epson device checklists.....	28
Fujifilm device checklists.....	29
HP device checklists.....	31
Recommendation.....	31
Konica Minolta device checklists.....	32
Checklist for using Konica Minolta devices with embedded clients.....	32
Checklist for using Konica Minolta devices with ScanStation.....	33
Ricoh device checklists.....	33
Checklist for using Ricoh devices with embedded clients.....	33
Checklist for using Ricoh devices with ScanStation.....	34
Xerox device checklists.....	34
Checklist for using Xerox devices with embedded clients.....	34
Checklist for using Xerox devices with ScanStation.....	35
<b>Chapter 4: Sizing recommendations.....</b>	<b>36</b>
General sizing recommendations.....	36
Support for high number of devices.....	37
Sizing recommendations for ScanStation configurations.....	38

# Introduction

This guide provides information to walk you through the process of verifying prerequisites before you proceed to install and use Tungsten eCopy ShareScan.

Once you successfully verify the checklist and review related information, use the *Tungsten eCopy ShareScan Installation Guide* to learn about:

- Requirements and installation steps for Tungsten eCopy ShareScan
- Procedure for setting up your devices to work with Tungsten eCopy ShareScan

After installation, you can use the online help (press **F1** in the Administration Console) for detailed configuration guidance.

For Epson devices, to enable eCopy ShareScan functionality on your Epson device, you need the following software components:

- **eCopy ShareScan:** This software provides a wide variety of workflows and integrations for document capture at the device.
- **Unified Client for Epson:** This component acts as the gateway to access the above mentioned eCopy workflows on the device.
- **Device Web Service (DWS):** This component manages and controls the Unified Client.
- **Device Registration Service (DRS):** This component provides a user interface for solution setup and configuration.

Each of these components has its own prerequisites to verify. This document provides the prerequisites of the eCopy ShareScan component. The other three components are part of the ControlSuite product and you can find their prerequisites in the Epson Unified Client chapter of the ControlSuite Clients Help. Detailed requirements for these components can be found in the product documents supplied with each.


## Product documentation

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

<https://docshield.tungstenautomation.com/Portal/Products/eCopy/6.7.0-u94fwgig3l/eCopy.htm>

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

Guide	Description
Tungsten eCopy ShareScan Pre-installation Checklist (PDF)	Provides information on the issues to be addressed before deploying Tungsten eCopy ShareScan.

Guide	Description
Tungsten eCopy ShareScan Installation Guide (PDF)	Provides information on how to install and upgrade Tungsten eCopy ShareScan, along with hardware and software prerequisites.
Tungsten eCopy ShareScan Online Help	<p>The integrated help of the application, covering the use of Tungsten eCopy ShareScan beyond installation, including configuration information.</p> <p> The help is accessible by pressing <b>F1</b> on the eCopy ShareScan Administration Console.</p>
Tungsten eCopy ShareScan Troubleshooter User Guide (PDF)	Provides information on how to use the eCopy ShareScan Troubleshooter, a built-in diagnostic tool.
Tungsten eCopy ShareScan Release Notes (PDF)	Provides an overview of late-breaking details for the current product release.
Tungsten eCopy ShareScan High Availability Deployment Guide (PDF)	Provides guidance on how to deploy eCopy ShareScan to function in high availability mode.
Tungsten eCopy ShareScan Glossary Editor Recommendations (PDF)	Contains information on proper use of the Glossary Editor Tool.

## Training

Tungsten Automation offers both classroom and computer-based training to help you make the most of your eCopy ShareScan solution. Visit the Tungsten Automation website at [www.tungstenautomation.com](http://www.tungstenautomation.com) for details about the available training options and schedules.

## Getting help with Tungsten Automation products

The [Tungsten Automation Knowledge Base](#) repository contains articles that are updated on a regular basis to keep you informed about Tungsten Automation products. We encourage you to use the Knowledge Base to obtain answers to your product questions.

To access the **Tungsten Automation Knowledge Base**, go to the [Tungsten Automation website](#) and select **Support** on the home page.

 The **Tungsten Automation Knowledge Base** is optimized for use with Google Chrome, Mozilla Firefox or Microsoft Edge.


The **Tungsten Automation 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 **Tungsten Automation 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 Tungsten Automation Portal login to view related articles.
- Access to the **Tungsten Automation 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 Tungsten Automation 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 Tungsten Automation 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.

 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

Tungsten eCopy ShareScan supports three typical installation and upgrade scenarios, which are briefly outlined below. For a more detailed description, see the "Install eCopy ShareScan" chapter in the *Tungsten eCopy ShareScan Installation Guide*.

### **Install Tungsten eCopy ShareScan 6.7.0 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 Tungsten eCopy ShareScan 5.x to 6.7.0**

 A direct upgrade from eCopy ShareScan 5.x to 6.7.0 is not supported.

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 6.0**

If you are upgrading from an eCopy ShareScan 5.4 version, you first need to upgrade to 6.5. Once you have a verified working installation of eCopy ShareScan 6.5, you are ready to proceed with the upgrade to version 6.7.0.

If you are upgrading from an 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 need to follow the upgrading from eCopy ShareScan 5.4 steps mentioned above.



### Upgrade from version 6.0 or higher

1. Exit eCopy ShareScan 6.x Administration Console.
2. Ensure that the eCopy ShareScan prerequisites (listed in this chapter) are installed.
3. Run the eCopy ShareScan 6.7.0 installer.
4. After the **Welcome** screen, select **Upgrade from previous version to 6.7** or **Custom upgrade from previous version to 6.7**, 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 Corretto 8 Java Runtime (x86) – version 8.402.08.1
- Microsoft .NET Framework 4.8
- Microsoft Visual C++ 2019 Redistributable (x86) – version 14.29.30139.0
- Microsoft Visual C++ 2019 Redistributable (x64) – version 14.29.30139.0

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

### Operating systems

- Windows 10 21H2 or later (x64) (max. 20 inbound connections in case of non-ScanStation clients)
- Windows 11 (max. 20 inbound connections in case of non-ScanStation clients)
- Windows Server 2016\*
- Windows Server 2019\*
- Windows Server 2022\*
- \* 64-bit support as a 32-bit application
- The eCopy ShareScan Administration Console and the eCopy ShareScan Manager cannot be installed on Linux, Solaris or Macintosh operating systems.

 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 2016 (also Express edition) or later

## Database permissions

For working with the eCopy 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 the "User rights necessary for eCopy ShareScan database creation" section in your *Tungsten eCopy ShareScan Installation Guide*.

Do not use an sa account as a eCopy ShareScan runtime account for database connection, as it does not work. Use only the eCopy account created by the eCopy 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

 Installing eCopy ShareScan on a virtual machine with a Microsoft operating system has always been supported, but Tungsten Automation 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 ESXi 7.0 or higher
- VMware Workstation 12.x or higher
- Microsoft Hyper Visor (Hyper-V) Server 2016 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" chapter in the *Pre-Installation Checklist*.


## 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.

 The original version of the Apache Tomcat web service is 9.0.87, 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 2022 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.

 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
<input type="checkbox"/>	Ensure that ShareScan Manager is installed to a dedicated computer that is exclusively tasked for running ShareScan Manager.
<input type="checkbox"/>	Run the Automatic Updates for the operating system before you start installing ShareScan.  Make sure you turn OFF the Automatic Updates during the installation.
<input type="checkbox"/>	When designing the network architecture, make sure you have Windows Server as an operating system if you plan to have more than 10 devices.  Windows 10 and 11 can handle a maximum number of 20 concurrent network connections.
<input type="checkbox"/>	If you have multiple NIC cards, you must select an IP address for ShareScan that will be used for device-server communication.
<input type="checkbox"/>	Check if your file system format is NTFS.
<input type="checkbox"/>	Ensure that Microsoft IIS is not installed or listening to the ports used by ShareScan (listed below).
<input type="checkbox"/>	You must activate ShareScan 6.x license keys against the Activation Server. Manual activation is available for servers that are unable to communicate directly with the Activation Server.  <ul style="list-style-type: none"> <li>• As licenses are tied to the ShareScan database, it is strongly recommended not to change the databases after ShareScan installation.</li> <li>• License keys can only be activated once, so you must inspect the setup carefully prior to activation.</li> <li>• All license keys provide a 30-day grace period before activation to ensure the license setup is as intended.</li> </ul>

Check	Description
<input type="checkbox"/>	<p>If you plan to use the <b>Single Sign-On</b> feature of the Session Logon service, you must ensure the following:</p> <ul style="list-style-type: none"><li>• The ShareScan Manager computer is a member of the domain for which Session Logon is configured.</li><li>• 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).</li><li>• 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).</li><li>• You use the Active Directory user account to log into this domain (and not into the local system).</li></ul>

## Network configuration

### Domains and Workgroups

eCopy ShareScan can be configured to run in either domain-based networks or workgroup environments. Windows 2016 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.


 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.

 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 eCopy ShareScan.

## Network Attached Storage Devices (NAS)

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

## Novell


eCopy 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, local administrator-level credentials are required. ShareScan Manager cannot be installed on a Domain Controller.

## Ports to be left open

If you plan to enable firewalls, leave the following ports open (between ShareScan Manager and the multifunctional device) for both inbound and outbound network traffic.

 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.

## When using Canon devices

Direction (manager computer)	Communication content	Non-secure	Secure	Comment
Outbound	<ul style="list-style-type: none"> <li>• Add device</li> <li>• Cost Recovery Credentials</li> <li>• Manager Started</li> <li>• Device setting change (change via Administration Console)</li> </ul>	9030	9032	
Inbound	-Image Upload	9610	9611	9610 and 9611 are the default values and can be changed via Advanced Settings/ ImageUploadPort and SecureImageUploadPort.
Inbound	<ul style="list-style-type: none"> <li>• Forms from Agent to Device</li> <li>• User entered data from Device to Agent</li> </ul>	9600	9621	
Inbound	Registration callback port	8080	9605	

## When using Epson devices

TCP	443, 8080, 9600, 9650, 9700, 9610, 80, 587, 8443
UDP	161 (SNMP), 8899, 9650

## When using Fujifilm devices

<b>Inbound</b>	
TCP	443, 8080, 9030, 9600, 9610, 9650
UDP	9650
<b>Outbound</b>	
TCP	443, 8080, 9650
UDP	161 (SNMP), 8899, 9650

## When using HP devices

<b>Inbound</b>	
TCP	443, 8080, 9030, 9600, 9610, 9650
UDP	9650

<b>Outbound</b>	
TCP	7, 443, 8080, 7626, 7627 (not used by HP S900), 9650
UDP	161 (SNMP), 8899, 9650

### When using Konica Minolta devices

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

### When using Olivetti devices

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

### When using Ricoh devices

<b>Direction (manager computer)</b>	<b>Communication content</b>	<b>Non secure</b>	<b>Secure</b>	<b>Comment</b>
Outbound	<ul style="list-style-type: none"> <li>• Add device</li> <li>• Cost Recovery Credentials</li> <li>• Manager Started</li> <li>• Device setting change (change via Administration Console)</li> </ul>	9030	9032	

Inbound	-Image Upload	9610	9611	9610 and 9611 are the default values and can be changed via Advanced Settings/ ImageUploadPort and SecureImageUploadPort.
Inbound	<ul style="list-style-type: none"> <li>Forms from Agent to Device</li> <li>User entered data from Device to Agent</li> </ul>	9600	9621	
Inbound	Registration callback port	8080	9605	

## When using ScanStation

<b>Inbound</b>	
TCP	2121, 9030, 9600, 9610, 9650
UDP	9650
<b>Outbound</b>	
TCP	9650
UDP	161 (SNMP), 8899, 9650

## When using Xerox devices

<b>Inbound</b>	
TCP	443, 8080, 9030, 9600, 9610, 9650
UDP	9650
<b>Outbound</b>	
TCP	443, 8080, 9650
UDP	161 (SNMP), 8899, 9650

## Support information

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


### Supported languages

Tungsten eCopy ShareScan supports the following languages:

- English
- Brazilian Portuguese
- Dutch



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

 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

# 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.

**i** 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 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 2016, 2019, Exchange Online for Office 365	<a href="#">eCopy connector for Microsoft Exchange (Mail and/or Fax)</a>
LDAP/SMTP (Mail and/or Fax)	<ul style="list-style-type: none"> <li>Microsoft LDAP v3</li> <li>Open LDAP v2.4</li> </ul>	<a href="#">eCopy connector for LDAP/SMTP (Mail and/or Fax)</a>
Quick Connect	<ul style="list-style-type: none"> <li>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.</li> <li>For more information about supported databases, see the <i>eCopy ShareScan Technical Specifications</i> document.</li> <li>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.</li> </ul>	<a href="#">eCopy connector for Quick Connect</a>
OpenText Fax Server (RightFax Edition)	20.2 or higher	<a href="#">eCopy connector for OpenText Fax Server (RightFax edition)</a>
Microsoft SharePoint	2016, 2019, SharePoint Server Subscription Edition, SharePoint Online for Office 365	<a href="#">eCopy connector for Microsoft SharePoint</a>
OpenText Documentum	20.2 or higher	<a href="#">eCopy connector for OpenText Documentum</a>
iManage WorkSite	10.3 or higher (including iManage Cloud)	<a href="#">eCopy connector for iManage WorkSite</a>
OpenText Content Server - eDOCS Edition	16.7 or higher	<a href="#">eCopy connector for OpenText Content Server - eDOCS edition</a>

Backend Applications	Supported Versions	Installation Prerequisites
OpenText Content Server (Livelink)	20.2 or higher	<a href="#">eCopy connector for OpenText Content Server</a>

## 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 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.

 The Inbox alternate path for folder root - DO NOT set it to the user's HOME folder 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.

 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 Web API Root URL 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.



- If **Send from personal account** is not enabled, all faxes will be sent from the user name and password supplied for configuration purposes.
- As the 'COM API' protocol is no longer supported, OpenText Fax Server connector profiles configured with 'COM API' protocol in earlier eCopy ShareScan version cannot be used. After upgrade, these profiles appears in Administration Console but cannot be modified and used on the clients.

## 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 your organization uses a secure SharePoint site, you must install an SSL certificate on the ShareScan server.



- 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.

 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.

 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 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).

 Do not select **Intranet 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.

- 
- When the eDOCS DM Extension Client 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 OpenText Content Server uses the REST API protocol or Web services protocol for communication with Open Text Content Server.

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

 As the 'LAPI' protocol is no longer supported, OpenText Content Server connector profiles configured with 'LAPI' or 'Web services and LAPI' protocol in earlier ShareScan version cannot be used. After upgrade, these profiles appears in Administration Console but cannot be modified and used on the clients.

## Suggestion

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

## Chapter 3

# Device checklists

Use the following checklists to review recommendations for using your devices with the embedded clients or with ScanStation.

- [Canon device checklists](#)
- [Epson device checklists](#)
- [Fujifilm device checklists](#)
- [HP device checklists](#)
- [Konica Minolta device checklists](#)
- [Ricoh device checklists](#)
- [Xerox device checklists](#)

This document is a checklist containing device-related pre-installation information only. When all of the pre-installation criteria are met, you are ready to consult the Installation Guide for:

- ShareScan-related pre-installation information
- ShareScan installation guidance
- Device-related installation guidance

## Canon device checklists

Use the following checklists to review recommendations for using Canon devices with embedded clients or with ScanStation.

- [Checklist for using Canon devices with embedded clients](#)
- [Checklist for using Canon devices with ScanStation](#)

### Checklist for using Canon devices with embedded clients

Check	Description
<input type="checkbox"/>	Confirm that the device and the firmware you are planning to use is supported.
<input type="checkbox"/>	When you are upgrading the device, follow this order: <ol style="list-style-type: none"><li>1. Remove the JAR file and the license from the device. Ensure that the previous JAR file is properly removed.</li><li>2. Reboot the device.</li><li>3. Install the JAR file and the license.</li></ol>

Check	Description
<input type="checkbox"/>	Verify whether your device is MEAP-enabled.
<input type="checkbox"/>	Ensure that network settings are configured properly on your device before installing the JAR file. A comprehensive description is available in the Installation Guide. Pre-installation highlights include: <ul style="list-style-type: none"> <li>• DHCP is not supported.</li> <li>• The use of static IP addresses is highly recommended.</li> <li>• Remember to power cycle the device so that your network setting configuration takes effect.</li> </ul>
<input type="checkbox"/>	Before installing the JAR file, make sure that you turn off the Department ID, the Single Sign-On (SSO) ID, or the Simple Device Login (SDL), if they are enabled. After installing the JAR file, you can turn on the IDs again.
<input type="checkbox"/>	Make sure that the device's Web Server is accessible.
<input type="checkbox"/>	If the devices and the ShareScan Manager computer are in different subnets, it is recommended to manually resolve IP addresses in the host file on the ShareScan Manager computer (located under C:\Windows\System32\drivers\etc\).

## Checklist for using Canon devices with ScanStation

Check	Description
<input type="checkbox"/>	If you are using ScanStation hardware, ensure that all required software components (including the Touchscreen driver) are installed and configured properly.
<input type="checkbox"/>	If you are using non-ScanStation hardware, the ShareScan Manager and the ScanStation client must be installed and function properly on the same computer.
<input type="checkbox"/>	ScanStation uses the proper driver to get input from a supported MFP. You must install and configure this driver next.
<input type="checkbox"/>	The Readme.txt file for Color Network ScanGear driver provides important information about where to install the driver for "Restricted Users". It also provides information about listing Color Network ScanGear and ScanGear Tool on the <b>Exceptions</b> tab in Windows Firewall.
<input type="checkbox"/>	Decide if you want to use TWAIN or ISIS scanning, and ensure that you only install the appropriate drivers.
<input type="checkbox"/>	If you are planning to use TWAIN scanning, run the driver installation executable as the next step.
<input type="checkbox"/>	If you are planning to use ISIS scanning, install the driver supplied with your device. Optionally, you can check the device manufacturer's website for driver updates, but only after you have installed the driver provided with the device.

## Epson device checklists

Verify that the following steps are completed to get your Epson device ready for deployment, using the Web Config for the device.

Check	Description
<input type="checkbox"/>	Verify that the Epson device you plan to use is supported for deployment. For the latest list of supported Epson models, consult your local Epson representative or refer to the Supported Device webpage ( <a href="https://knowledge.kofax.com/MFD_Productivity/00_Supported_Devices/Supported_Devices">https://knowledge.kofax.com/MFD_Productivity/00_Supported_Devices/Supported_Devices</a> ).
<input type="checkbox"/>	Verify the firmware version of the device: <ol style="list-style-type: none"> <li>1. On the Web Config for the device, select <b>Device Management</b> &gt; <b>Firmware Update</b> .</li> <li>2. Check the firmware version.</li> </ol>
<input type="checkbox"/>	Ensure that you have activated the Epson Open Platform 1.1: <ol style="list-style-type: none"> <li>1. Use the serial number of the device to acquire the product key at <a href="https://openplatform.epson.biz/license-op/inputInformation.html">https://openplatform.epson.biz/license-op/inputInformation.html</a>.</li> <li>2. On the Web Config for the device, click the <b>Epson Open Platform</b> tab and enter the acquired key.</li> <li>3. Set the Epson Open Platform version to 1.1.</li> </ol>
<input type="checkbox"/>	Verify that the administrator password set for the device in the <b>Product Security</b> tab is reflected in the <b>Username</b> and <b>Password</b> fields in the <b>Devices</b> tab of the Device Registration Service (DRS).
<input type="checkbox"/>	(Optional) Ensure that USB Card Reader access is enabled: <ol style="list-style-type: none"> <li>1. On the Web Config for the device, select <b>Product Security</b> &gt; <b>External Interface</b> .</li> <li>2. Set <b>Memory Device</b> to <b>Enabled</b>.</li> </ol>
<input type="checkbox"/>	Confirm the valid certificate status: <ol style="list-style-type: none"> <li>1. On the Web Config for the device, click <b>Network Security</b> tab.</li> <li>2. Under <b>SSL/TLS settings</b> group, select <b>Certificate</b>.</li> <li>3. Select <b>Self-signed Certificate</b> from the <b>Server Certificate</b> list.</li> <li>4. Click <b>Update</b>.</li> </ol>
<input type="checkbox"/>	Verify the date, time, and locale: <ol style="list-style-type: none"> <li>1. On the Web Config for the device, click the <b>Device Management</b> tab.</li> <li>2. Enter the information under <b>Date</b>, <b>Time</b>, and <b>Time Difference</b>.</li> </ol>

## Fujifilm device checklists

Be sure to review this checklist for using Fujifilm devices with embedded clients.

Check	Description
<input type="checkbox"/>	Confirm that the device you are planning to use is supported.

Check	Description
<input type="checkbox"/>	Verify that the default device UI language you are about to use is set to English. If you want to use eCopy ShareScan with Japanese or Simplified Chinese client language, set the device UI language to Japanese or Simplified Chinese.
<input type="checkbox"/>	Through the device's Web Administration Application, verify that SNMP v1/v2c protocols are enabled. On most devices, go to <b>Network &gt; Protocols &gt; SNMP</b> . On older devices, go to <b>Properties &gt; Connectivity &gt; Protocols &gt; SNMP Configuration</b> .
<input type="checkbox"/>	Check (through the device's Web Administration Application) if HTTPS (SSL) is enabled on the device (On most devices, go to <b>Properties &gt; Security &gt; SSL/TSL Settings</b> ). You may need to create a certificate and install it onto the device before you can turn on Secure HTTP. On most devices, creating a certificate can be performed at <b>System &gt; Security &gt; Certificate Settings</b> . On most older devices, certificate can be created at <b>Properties &gt; Security &gt; Machine Digital Certificate Management &gt; Create New Signed Certificate</b> . Consult the Fujifilm support site for your exact device's Administration Guide at <a href="https://support-fb.fujifilm.com">https://support-fb.fujifilm.com</a> .
<input type="checkbox"/>	In case the devices and the ShareScan Manager computer are in different subnets, it is recommended to manually resolve IP addresses in the host's file on the ShareScan Manager computer (located in the C:\Windows\System32\drivers\etc\ folder).
<input type="checkbox"/>	If you plan to use eCopy ShareScan with secure communication and/or secure file transfer features enabled, it might be necessary to disable Remote Server Certificate verification. On most devices, go to <b>System &gt; Security &gt; SSL/TSL Settings &gt; Verify Remote Server Certificate</b> . On most older devices, go to <b>Properties &gt; Security &gt; SSL/TSL Settings &gt; Verify Remote Server Certificate</b> .
<input type="checkbox"/>	By default, eCopy ShareScan installs Amazon Corretto Java Runtime Environment, which is required to ensure proper functionality. For the distributed/tested version, see <a href="#">System requirements for eCopy ShareScan Manager computer</a> in this guide.
<input type="checkbox"/>	Tungsten Automation suggests that administrators ensure that device and ShareScan Manager computer times match. This is especially important when working with SSL certificates. If this criterion is not met, you may experience improper functionality, such as rejection of certificates.
<input type="checkbox"/>	If you experience delayed reactions on the MFP UI, ensure that the network settings of the device are correct. You can contact your administrator, who can check the settings via: <ul style="list-style-type: none"> <li>• Via the Web interface: <ul style="list-style-type: none"> <li>• Browse to <code>http://&lt;device IP&gt;</code>.</li> <li>• Navigate to <b>Network &gt; Protocols</b>. On older devices, navigate to <b>Properties &gt; Connectivity &gt; Protocols</b>.</li> <li>• Check the following network protocol pages: TCP/IP, Proxy Server, Microsoft networking, SMTP Server, LDP, SIP, LDAP, POP3.</li> </ul> </li> <li>• On the device UI: <ul style="list-style-type: none"> <li>• Press the <b>Login</b> button on the device, and provide the administrator credentials as needed.</li> <li>• Press the <b>Settings (cogwheel)</b> button (or the <b>Tools</b> button for older devices) on the touch screen.</li> <li>• Navigate to <b>Device &gt; Network Settings &gt; Protocol Settings</b>. On older devices, navigate to <b>System Settings &gt; Connectivity &amp; Network Setup &gt; Protocols</b>.</li> <li>• Check each specific network protocol page, disable all unused protocols and use IP addresses where possible.</li> </ul> </li> </ul>

## HP device checklists

Be sure to review this checklist for using HP devices with embedded clients.

Check	Description
<input type="checkbox"/>	Confirm that the device and the firmware you are planning to use are supported.
<input type="checkbox"/>	Verify whether the device you are about to use is OXPd 1.6 capable.
<input type="checkbox"/>	If needed, update device firmware to support OXPd 1.6.
<input type="checkbox"/>	Make sure OXPd 1.6 is enabled.
<input type="checkbox"/>	Confirm configuration of WebProxy settings.
<input type="checkbox"/>	Check configuration of the embedded web browser (timeouts and trusted sites list).
<input type="checkbox"/>	Check certification management in the OXPd 1.6 CA certificate store.
<input type="checkbox"/>	Verify that a valid certificate is installed on the device. This is necessary to support secure communication between the device and the ShareScan server.
<input type="checkbox"/>	Make sure the device has SNMPv2 read access and a Get Community Name (necessary to enable Device discovery function in the ShareScan Administration Console).
<input type="checkbox"/>	Set (via EWS) an administrator password to access some of the advanced device features. You will be prompted to supply this password during the ShareScan installation.
<input type="checkbox"/>	If the devices and the ShareScan Manager computer are in different subnets, it is recommended to manually resolve IP addresses in the hosts file on the ShareScan Manager computer (located under C:\Windows\System32\drivers\etc\).
<input type="checkbox"/>	When using the native keyboard, raise the device timers to 2 minutes in order to avoid timeout issues on complex ShareScan forms.
<input type="checkbox"/>	By default, eCopy ShareScan installs Amazon Corretto Java Runtime Environment, which is required to ensure proper functionality. For the distributed/tested version, see <a href="#">System requirements for eCopy ShareScan Manager computer</a> in this guide.

### Recommendation

- You can use HP Web Jetadmin or the built-in Embedded Web Server (EWS, an HTTP-based device management application) to configure your HP device. To configure several devices at once, it is recommended to use HP Web Jetadmin.
- Consult HP Imaging and Printing Security Best Practices and the NIST checklist (available at the NIST website). These documents will help you ensure that network security is optimized.

## Konica Minolta device checklists


Use the following checklists for information about using Konica Minolta devices with embedded clients or with ScanStation.

- [Checklist for using Konica Minolta devices with embedded clients](#)
- [Checklist for using Konica Minolta devices with ScanStation](#)

### Checklist for using Konica Minolta devices with embedded clients

Check	Description
<input type="checkbox"/>	Confirm that the device and the firmware you are planning to use are supported.
<input type="checkbox"/>	Make sure that the device's Web Server is accessible.
<input type="checkbox"/>	In case the devices and the ShareScan Manager computer are in different subnets, it is recommended to manually resolve IP addresses in the hosts file on the ShareScan Manager computer (located under C:\Windows\System32\drivers\etc\).
<input type="checkbox"/>	If you need complete security, it is recommended that you enable SSL (Secure Sockets Layers) on devices running eCopy ShareScan. For information about configuring SSL on the device, refer to the Konica Minolta documentation.
<input type="checkbox"/>	By default, eCopy ShareScan installs Amazon Corretto Java Runtime Environment, which is required to ensure proper functionality. For the distributed/tested version, see <a href="#">System requirements for eCopy ShareScan Manager computer</a> in this guide.
<input type="checkbox"/>	<p>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 <b>User Box</b> for the device and make sure that <b>Web Browser</b> appears in the list of applications. To configure the device to work with eCopy ShareScan, you set several options in the Internet Explorer browser and on the device.</p> <ul style="list-style-type: none"> <li>• <b>Internet Explorer:</b> If you are using Internet Explorer, make sure that you set the <b>Check for newer versions of stored pages</b> option for Temporary Internet Files to <b>Every time I visit the webpage</b>.</li> <li>• <b>Cookies:</b> 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 eCopy ShareScan. For instructions, see the device documentation.</li> <li>• <b>Focus rectangle:</b> You may want to change the color of the focus rectangle. For instructions, see the device documentation.</li> <li>• <b>Time-outs:</b> It is recommended that you set the following time-out settings on the device. On most devices, the timers are available under the <b>Utility &gt; Administrator settings &gt; System settings &gt; Reset Settings</b> path (for instructions on your actual model, see the device documentation).</li> </ul>



Check	Description
<input type="checkbox"/>	<p>To make eCopy ShareScan time out after nine minutes of inactivity, set the <b>System Auto Reset Time</b> (in <b>System Auto Reset &gt; System Auto Reset Time</b>), and the <b>Copy, Web Browser, Scan/Fax</b> and <b>User</b> box timeout values (in <b>Auto Reset &gt; Copy / Web Browser / Scan/Fax / User box</b>) settings to nine minutes. This keeps the screen from timing out while a document is being scanned or processed.</p> <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #add8e6;"> <p> In certain scanning environments, it is recommended that you increase the <b>WebDAV</b> 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, see the device documentation.</p> </div>

## Checklist for using Konica Minolta devices with ScanStation

Check	Description
<input type="checkbox"/>	If you are using ScanStation hardware, ensure that all required software components (including the Touchscreen driver) are installed and configured properly.
<input type="checkbox"/>	If you are using non-ScanStation hardware, the ShareScan Manager and the ScanStation client must be installed and function properly on the same computer.
<input type="checkbox"/>	ScanStation uses the proper driver to get input from a supported MFP. You must install and configure this driver next.
<input type="checkbox"/>	Use a web browser to check and download the specific TWAIN driver for your Konica Minolta bizhub device.

## Ricoh device checklists

Use the following checklists for details about using Ricoh devices with embedded clients or with ScanStation.

- [Checklist for using Ricoh devices with embedded clients](#)
- [Checklist for using Ricoh devices with ScanStation](#)

## Checklist for using Ricoh devices with embedded clients

Check	Description
<input type="checkbox"/>	Confirm that the device and the firmware you are planning to use is supported.
<input type="checkbox"/>	Make sure that the device's Web Server is accessible.
<input type="checkbox"/>	Ensure that the proper SDK/J version is installed on the device.
<input type="checkbox"/>	In case the devices and the ShareScan Manager computer are in different subnets, it is recommended to manually resolve IP addresses in the hosts file on the ShareScan Manager computer (located under <code>C:\Windows\System32\drivers\etc\folder</code> ).

**i** To have ShareScan started automatically on device startup, leave the Auto Start option selected during jar file installation.

## Checklist for using Ricoh devices with ScanStation

Check	Description
<input type="checkbox"/>	If you are using ScanStation hardware, ensure that all required software components (including the Touchscreen driver) are installed and configured properly.
<input type="checkbox"/>	If you are using non-ScanStation hardware, the ShareScan Manager and the ScanStation client must be installed and function properly on the same computer.
<input type="checkbox"/>	ScanStation uses the proper driver to get input from a supported MFP. You must install and configure this driver next.
<input type="checkbox"/>	Decide if you want to use TWAIN or ISIS scanning.
<input type="checkbox"/>	If you are planning to use TWAIN scanning, run the driver installation executable as the next step. (The driver is available on the eCopy ShareScan installation media.)
<input type="checkbox"/>	If you are planning to use ISIS scanning, install the driver supplied with your device. Optionally, you can check the device manufacturer's website for driver updates, but only after you have installed the supplied driver.

## Xerox device checklists

Use the following checklists to get information about using Xerox devices with embedded clients or with ScanStation.

- [Checklist for using Xerox devices with embedded clients](#)
- [Checklist for using Xerox devices with ScanStation](#)

## Checklist for using Xerox devices with embedded clients

Check	Description
<input type="checkbox"/>	Confirm that the device and the firmware you are planning to use are supported.
<input type="checkbox"/>	Verify that the device you are about to use is EIP capable.
<input type="checkbox"/>	Make sure Custom services / EIP is installed on your device. (It is pre-installed on most devices.)
<input type="checkbox"/>	Check (through the device's Web Administration Application) if HTTPS (SSL) is enabled on the device (on most devices, you can find it under <b>Security &gt; SSL</b> , <b>Security &gt; SSL/TLS Settings</b> , <b>Protocols &gt; HTTP</b> , or <b>Services &gt; Custom Services</b> ). Enabling Secure HTTP (SSL) requires a Machine Digital Certificate. You can upload a signed certificate onto the MFP or create a self-signed certificate directly on the MFP. The certificate's public key size has to be at least 1024 bits. Certain models offer a selection of different Digital Signature Algorithms if you plan to create a self-signed certificate through the device's Web Administration Application. If this is the case, make sure the RSA/SHA-2 algorithm is selected.

Check	Description
<input type="checkbox"/>	Verify (through the device's Web Administration Application) that SNMP v1/v2c protocols are enabled; on most devices, you can find it under <b>Protocols &gt; SNMP (Configuration)</b> .
<input type="checkbox"/>	Make sure (through the device's Web Administration Application) that Scan Template Management is enabled on the device (on most devices, you can find it under <b>Protocols &gt; HTTP</b> or <b>Network Scanning &gt; Scan Template Management</b> ).
<input type="checkbox"/>	Make sure that the device's Auto Refresh is not disabled (the Auto Refresh Interval must not be set to 0 (void) seconds). The name of this feature may differ across various devices. Most common variants include: System timeouts, Auto Resume, Auto Refresh Interval, and Touch User Interface System Timer.
<input type="checkbox"/>	If the devices and the ShareScan Manager computer are in different subnets, it is recommended to manually resolve IP addresses in the host file on the ShareScan Manager computer (located in the C:\Windows\System32\drivers\etc\ folder).
<input type="checkbox"/>	By default, eCopy ShareScan installs Amazon Corretto Java Runtime Environment, which is required to ensure proper functionality. For the distributed/tested version, see <a href="#">System requirements for eCopy ShareScan Manager computer</a> in this guide.
<input type="checkbox"/>	It is suggested that administrators should ensure that device and ShareScan Manager computer times match. This is especially important when working with SSL certificates. If this criterion is not met, you may experience improper functionality, such as rejection of certificates.

## Checklist for using Xerox devices with ScanStation

Check	Description
<input type="checkbox"/>	If you are using ScanStation hardware, ensure that all required software components (including the Touchscreen driver) are installed and configured properly.
<input type="checkbox"/>	If you are using non-ScanStation hardware, the ShareScan Manager and the ScanStation client must be installed and function properly on the same computer.
<input type="checkbox"/>	ScanStation uses the proper driver to get input from a supported MFP. You must install and configure this driver next.
<input type="checkbox"/>	Decide if you want to use the Remote Scan Module, the Scan to eCopy driver or an ISIS driver for scanning. The Remote Scan Module and the Scan to eCopy driver are available automatically after installing ShareScan. Remote Scan module can be used only with devices supporting EIP 2.5 or later. We highly recommend to use the Remote Scan Module if possible.
<input type="checkbox"/>	If you are planning to use ISIS scanning, install the driver supplied with your device. If you still experience less than optimal behavior, this might be due to the fact that some redistributable ISIS framework files are missing from your system. To remedy such situations, Tungsten Automation is ready to supply a package containing a set of these redistributable files in the form of a self-extracting archive: PIXTRAN.EXE. Usage: Launch this executable. If your Windows installation is not in the default location (C:\Windows), browse to your Windows installation directory afterwards.

## Chapter 4

# Sizing recommendations

The following sections describe the sizing recommendations for both embedded and ScanStation configurations.

## General sizing recommendations

This section contains sizing recommendations, assuming up to 50% of the MFPs are concurrently processing scanned documents; while the other 50% are idle, printing or copying. Operating systems installed to virtual machines must have the specified physical resources allocated to the virtual machine. These recommendations are for optimum performance. Exceeding this number of devices or load will reduce application responsiveness.

**i** For a server supporting multiple brand MFPs or varying user loads, consult your eCopy Technical Consultant for specific sizing recommendations. Enabling background processing positively impacts the scalability.

Client MFPs per ShareScan Manager	1-15	16-30	31-45	46-75	76-120
B&W Letter / A4 200 DPI No OCR	<b>Operating system:</b> Windows Server 2012 or Server 2016 or Server 2019 or Server 2022 <b>Minimum CPU:</b> Dual Core <b>Minimum RAM:</b> 8 GB	<b>Operating system:</b> Windows Server 2012 or Server 2016 or Server 2019 or Server 2022 <b>Minimum CPU:</b> Dual Core <b>Minimum RAM:</b> 8 GB	<b>Operating system:</b> Windows Server 2012 or Server 2016 or Server 2019 or Server 2022 <b>Minimum CPU:</b> Dual Core <b>Minimum RAM:</b> 8 GB	<b>Operating system:</b> Windows Server 2012 or Server 2016 or Server 2019 or Server 2022 <b>Minimum CPU:</b> Quad Core <b>Minimum RAM:</b> 10 GB	<b>Operating system:</b> Windows Server 2012 or Server 2016 or Server 2019 or Server 2022 <b>Minimum CPU:</b> Quad Core <b>Minimum RAM:</b> 10 GB

<b>Client MFPs per ShareScan Manager</b>	<b>1-15</b>	<b>16-30</b>	<b>31-45</b>	<b>46-75</b>	<b>76-120</b>
Color Letter/A4 300 DPI No OCR	<p><b>Operating system:</b> Windows Server 2012 or Server 2016 or Server 2019 or Server 2022</p> <p><b>Minimum CPU:</b> Dual Core</p> <p><b>Minimum RAM:</b> 8 GB</p>	<p><b>Operating system:</b> Windows Server 2012 or Server 2016 or Server 2019 or Server 2022</p> <p><b>Minimum CPU:</b> Dual Core</p> <p><b>Minimum RAM:</b> 8 GB</p>	<p><b>Operating system:</b> Windows Server 2012 or Server 2016 or Server 2019 or Server 2022</p> <p><b>Minimum CPU:</b> Quad Core</p> <p><b>Minimum RAM:</b> 10 GB</p>	<p><b>Operating system:</b> Windows Server 2012 or Server 2016 or Server 2019 or Server 2022</p> <p><b>Minimum CPU:</b> Quad Core</p> <p><b>Minimum RAM:</b> 10 GB</p>	<p><b>Operating system:</b> Windows Server 2012 or Server 2016 or Server 2019 or Server 2022</p> <p><b>Minimum CPU:</b> Quad Core</p> <p><b>Minimum RAM:</b> 10 GB</p>
B&W / Color Letter/A4 300 DPI with OCR	<p><b>Operating system:</b> Windows Server 2012 or Server 2016 or Server 2019 or Server 2022</p> <p><b>Minimum CPU:</b> Dual Core</p> <p><b>Minimum RAM:</b> 8 GB</p> <p>Max 4 OCR-ing</p>	<p><b>Operating system:</b> Windows Server 2012 or Server 2016 or Server 2019 or Server 2022</p> <p><b>Minimum CPU:</b> Quad Core</p> <p><b>Minimum RAM:</b> 10 GB</p> <p>Max 8 OCR-ing</p>	<p><b>Operating system:</b> Windows Server 2012 or Server 2016 or Server 2019 or Server 2022</p> <p><b>Minimum CPU:</b> Quad Core</p> <p><b>Minimum RAM:</b> 10 GB</p> <p>Max 8 OCR-ing</p>	<p><b>Operating system:</b> Windows Server 2012 or Server 2016 or Server 2019 or Server 2022</p> <p><b>Minimum CPU:</b> Quad Core</p> <p><b>Minimum RAM:</b> 10 GB</p> <p>Max 8 OCR-ing</p>	<p><b>Operating system:</b> Windows Server 2012 or Server 2016 or Server 2019 or Server 2022</p> <p><b>Minimum CPU:</b> Xeon 8 Core</p> <p><b>Minimum RAM:</b> 12 GB</p> <p>Max 10 OCR-ing</p>

## Support for high number of devices

The general Microsoft recommendations for server operation not to exceed 75-80% of overall CPU load for a long period of time are taken into consideration.

As specified above, with regard to memory and other resources, it is not recommended to exceed the maximum number of devices connected to a single ShareScan server, since different resources (some or more of the following: memory, disk I/O bandwidth, handle or thread count) can run short and may cause temporary or permanent performance and/or functional issues.

Support is not possible for systems if the number of devices connected to a single server exceeds the recommended maximum limitations.

If hardware or MS NLB is used for load balancing / high availability, the overall number of devices divided by the number of active server nodes in the cluster is considered as a "devices per server" measure.

## Sizing recommendations for ScanStation configurations

When using Windows 10 x64 operating system:

- Minimum CPU: Dual Core
- Minimum RAM: 4 GB
- Recommended RAM: 8 GB

When using Windows 11 x64 operating system:

- Minimum CPU: Dual Core
- Minimum RAM: 6 GB
- Recommended RAM: 10 GB