Kofax eCopy ShareScan
6.3
Pre-Installation Checklist for Konica-Minolta Devices

KOFAX

Licensing, Copyright, and Trademark Information

Contents

Introduction

Consult this checklist document **first**, if you are about to use ShareScan 6.3 with Konica Minolta devices, since it contains preliminary criteria to verify.

After you have verified the checklist, use the ShareScan Installation Guide to learn about

– pre-installation requirements and installation steps for ShareScan

– installation steps to set up your Konica Minolta device to work with ShareScan.

After you have successfully installed ShareScan and the device, use the Help document (press F1 in the Administration Console) for configuration guidance.

ShareScan Installation Guide

The 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 devices 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 ShareScan. For the device-specific Pre-Installation Checklist (PICL), see the relevant vendor-specific Pre-Installation Checklist and Sizing Guide.For information pertaining to the ShareScan (pre)install, see this guide. For configuration and Administration Console usage, refer to 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 in a server-client architecture and environment.

ShareScan Documentation

The following documentation is available for your perusal with ShareScan:

– **eCopy ShareScan Pre-installation Checklist and Sizing Guide** (this document) – provides info on the issues to be addressed before deploying ShareScan

– **eCopy ShareScan Installation Guide** (PDF) - contains information on installing eCopy ShareScan, including hardware and software prerequisites

– **eCopy ShareScan Administration Console Help** – the integrated help of the application, covering the use of ShareScan beyond installation, and provides configuration information. The help is accessible by pressing F1 on the ShareScan Administration Console

– **eCopy ShareScan Troubleshooter User Guide** (PDF) – contains information on how to use the ShareScan Troubleshooter, a built-in diagnostic tool of the product

– **eCopy ShareScan Release Notes** (PDF) – contains an overview of the changes for the given ShareScan release

– **eCopy ShareScan High Availability and Load Balancing Deployment Guide** (PDF) - provides guidance on how to deploy ShareScan to function in high availability mode

– **eCopy ShareScan Glossary Editor Recommendations** (PDF) - contains information on how to handle Glossary Editor Tool properly

Typical Installation Workflow

ShareScan 6.3 installation has three typical scenarios, which are briefly outlined below. For a more detailed description, read the **Installing ShareScan** section of the **Installation Guide**.

Installing ShareScan 6.3 with no previous version already present

1. Ensure that the ShareScan prerequisites (listed in the following chapter) are installed.

2. Start the ShareScan 6.3 installer, and click through the Installation Wizard.

Upgrading from ShareScan 5.x to 6.3

> **Important!**
> ShareScan v5.0, v5.1 and v5.2 are not supported in an 5.x to 6.3 upgrade scenario.

Before you start the upgrade process, ensure that your current ShareScan installation is working properly. The easiest way to do this is starting the Administration Console and verifying that it launches error-free.

Upgrading from versions pre-dating v5.4

If you are upgrading from a software version earlier than v5.4 - that is from v5.0, v5.1 or from v5.2 - first you need to upgrade to 5.4. Once you have a verified working installation of ShareScan v5.4 you are ready to proceed to upgrade to v6.3.

Upgrading from v5.4 or higher to 6.3

1. Exit ShareScan 5.x Administration Console.

2. Ensure that the ShareScan prerequisites (listed in the following chapter) are installed.

3. Run eCopy ShareScan 6.3 installer.

4. Choose **Upgrade from previous version to 6.3** or **Custom upgrade from previous version to 6.3** after the **Welcome** screen and click through the upgrade workflow.

Pre-installation

The following chapter contains information on the various tasks to be performed prior to installing ShareScan, as well as the requirements that must be met before product installation.

System Requirements for the ShareScan Manager PC

The ShareScan 6.3 install media contains all the required dependency installer files under **Install\ShareScan\SetupPrerequisites** in separate folders that must be installed to ensure ShareScan functions properly. These are the following:

- Amazon Corretto 8 Java Runtime (x86)

- Microsoft .NET Framework 4.7.1

- Microsoft Visual C++ 2012 Redistributable (x86) – version 11.0.61030

- Microsoft Visual C++ 2017 Redistributable (x86) – version 14.16.27027.1

- Microsoft Visual C++ 2017 Redistributable (x64) – version 14.16.27027.1

- Microsoft Visual J# 2.0 Redistributable

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

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

Operating Systems

For information on supported operating systems, consult the Technical Specifications document. The ShareScan Administration Console and the ShareScan Manager cannot be installed on Linux, Solaris or Macintosh operating systems.

Note:
The ShareScan 6.3 installer cannot be launched unless Microsoft .NET Framework 4.7.1 or a later 4.x version is installed on the target system. When trying to launch the installer with no .NET Framework or any version older than v4.7.1 installed, an error message pops up detailing the dependency and the install media path for the offline .NET Framework installer. This warning message must be closed by clicking **OK** and the installer quits. For more information on .NET Framework versions and their operating system related dependencies click here.

Database

For information on supported databases, consult the Technical Specifications document.

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 their virtual environment is configured correctly. Avoid desktop class machines, since they do not have enough resources to support heavy processing.

For information on supported virtual environments, consult the Technical Specifications document.

Memory Configuration

For information on memnory configuration, consult the Technical Specifications document.

For more details on recommended memory configuration, see the **Sizing recommendations for embedded configurations** section .

Checklist for the ShareScan Manager PC

– Ensure you are about to install the ShareScan Manager to a dedicated PC (that is, a PC exclusively tasked with the running of the ShareScan Manager).

– Run the Automatic Updates before you start installing ShareScan. **Pay extra attention that you have Automatic Updates of the operating system TURNED OFF during the installation.**

– ShareScan 6.3 installs a customized Apache Tomcat web service. Already existing Tomcat installations are not supported.

Note:
The original version of the Apache Tomcat web service is 9.0.36. This is a 32-bit installer.

– When designing the network architecture, note that Windows 10 can handle a maximum number of 20 concurrent network connections. If you plan to have more than 10 devices, you need Windows Server as an operating system.

– If you have multiple NIC cards, you need to 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 is not listening to the ports used by ShareScan (listed below).

– ShareScan 6.x licenses are installed to a SQL Server to allow easy management of devices. Prior to installing

6

ShareScan 6.x, it is important to determine if licenses will be managed individually from each ShareScan Manager, or if you would like to manage all licenses from a single SQL Server.
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.

– ShareScan license keys must be activated against an Activation Server. License keys can only be activated once, so 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. Manual activation is available for servers that are unable to communicate directly with the Activation Server.
As licenses are tied to the ShareScan database, it is not recommended tochange databases after ShareScan installation.

– If you plan to use the **Single Sign-On** feature of the **Session Logon** service, ensure that the ShareScan Manager PC 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). Ensure that you use the Active Directory user account to log in into this domain (and not into the local system). 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).

– If you plan to use the Session Logon service or User configuration, ensure that TCP port 3268 is open to access organizations, security groups and their data in Active Directory Global Catalog.

Ports to be left open

If you are planning to have firewalls enabled, leave the following ports open (between ShareScan Manager and the multifunctional device) for both inbound and outbound network traffic:

Inbound traffic:

– TCP: 443, 8080, 9030, 9600, 9650, 9700, 9610, 50002

– UDP: 9650

Outbound traffic:

– TCP: (SQL server default port, custom port can also be used instead), , 50001, 50003

– UDP: 161 (SNMP), 8899, 9650

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

Database Permissions

– For working with the ShareScan databases in case of upgrading, 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 clean installation scenario related database permissions, see the **User rights necessary for ShareScan database creation** section in your eCopy ShareScan Installation Guide.

– Do not use an **sa** account as a ShareScan runtime account for database connection, 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 specifed during installation should have the proper rights.

Note:
If Integrated Windows Authentication is used to connect to the database, and FPE (Form Processing Extender) or SFE (SmartForms Extender) profile is edited in the Administration Console (by using the template editor of the extenders), Profile Export/Import is used in the Administration Console,   then the database administrator must add the user (or users) to the allowed users of the ShareScan database. These users should have **db_owner** rights and must have their default schema set to 'ShareScan'.

Network

– **Domains and Workgroups:** ShareScan can be configured to run in either domain-based networks or workgroup environments. Windows 2012 or later domain environments are supported.
It is recommended to use a domain environment.

– **Subnets and VLANs:** The ShareScan Manager PC can be on different subnets or VLANs from the multifunction devices, provided that the multifunction devices can communicate with the Manager PC 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 duplex 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 PC.

– **IP Addresses:** Use static IP addresses for both the ShareScan Manager PC and the MFPs. To change the IP address of the Manager PC:
   a. remove all devices from the Manager

   b. stop all ShareScan related services

   c. change the IP address of the NIC and make sure the network adapters use the new IP (`ipconfig` command)

   d. start the services stopped in (b)

   e. re-add the devices

If your devices require a certificate to work, the workflow changes slightly when changing the Manager IP address:

8

a. remove all devices from the Manager

b. change the IP address

c. reboot the Manager PC

d. start the ShareScan Administration Console, and confirm the IP address change on the dialog that automatically opens

e. recreate the certificate(s)

f. re-add the devices to the Manager

Note:
If the IPv6 function is not in use, it should be disabled in the device settings. This way, first time connection errors can be prevented (e.g. 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 (Administration Console) may change after confirmation.
Note that 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 do a full reinstallation of ShareScan.

– **Network Attached Storage Devices (NAS):** ShareScan 6.3 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 PC and a multifunction device on Novell networks. However, when Novell client software is installed on the Manager PC 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 PC 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:** In order to use the Administration Console on the ShareScan Manager PC, you require local administrator-level credentials. ShareScan Manager cannot be installed on a Domain Controller.

– **SSDP Settings:** make sure you switch **SSDP Settings** to **ON**, otherwise device information cannot be queried:
1. Open the web page of the MFP and login as administrator.

2. Click the **Network** tab.

3. Select **SSDP Settings**.

4. Ensure that **SSDP** is switched to **ON**.

Support information

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

Supported languages

ShareScan 6.3 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 over 100 languages.

Supported devices

For the most current information on supported devices, go to the Support Website.

Supported backend services

For a detailed list of connector-specific backend version, see section eCopy connectors in this Installation Guide.

10

eCopy Connectors

It is recommended that application credentials (for Lotus Notes, Microsoft Outlook, SMTP, LDAP, and so forth) should be matched with the PC login credentials. Creating a generic, email-enabled "ShareScan" account for use by ShareScan is a recommended practice.

The backend applications listed in this section belong to their respective owners, and as such, any further, in-depth information you may need on the workings of these applications can be found in the application's own documentation, NOT in the ShareScan documentation.

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

For information on supported Microsoft Exchange versions, consult the Technical Specifications document.

Installation Prerequisites and Suggestions

– If configuring the Exchange connector using EWS or WebDAV protocols, the Exchange server SSL certificate must be installed on the PC running ShareScan Manager. Certificates should be installed to the **Trusted Root Certification Authorities** on the Local Computer.

– To configure and use EWS/EWS protocol, the user's logon name and alias must correspond, due to limitations of the Exchange web services. For this reason, using LDAP/EWS protocol is recommended.

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

For information on supported Lotus Notes versions, consult the Technical Specifications document.

Installation Prerequisites and Suggestions

– The connector requires a Lotus Notes client to be installed on the PC running the ShareScan Manager.

– At the time of configuration, the end user should be prepared to provide an Active ID File, user name, password, and Domino server name.

– When the installer of the Lotus Notes client prompts you to choose between the **Multi-User Install** option and the **Single User Install** option, make sure that you 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 information on supported LDAP versions, consult the Technical Specifications document.

Installation Prerequisites and Suggestions

– You will be prompted to enter the following information when configuring the eCopy connector for LDAP: User name, password and IP address, DNS name or URL for the directory being used, search criteria for users and recipients, LDAP Attributes, LDAP port number, and Base DN of the base or root directory in which to search.

– For configuring the eCopy connector for SMTP, you will need to enter the SMTP server IP address or DNS name that will be used for outgoing messages, user name and password, and the SMTP port number.

eCopy Scan to Desktop

Installation Prerequisites and Suggestions

– 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 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 ShareScan has created Inbox folders; these folders would also reside under this directory.

– For detailed information on configuring Scan to Desktop, see the ShareScan Help, accessible via pressing **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 ShareScan modifies the permissions on the root folder.

Inbox Root Directory

The Inbox Root Directory can reside on the ShareScan Services Manager PC 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 should not be pointing to a user's home directory. Choose the Scan to Desktop **Home Directory** option in the connector instead.

Note:
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 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 group used 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. ShareScan uses this group when assigning permissions to the inbox Root Directory and scan inboxes and requires Full Control. Permissions assigned to the directory are as follows:

Windows (NTFS)

- Administrators – Full Control

- Domain Administrators – Full Control (not used in workgroup configurations) ShareScanAdmin – Full Control

- Inbox Owner – Read or Delete

Novell (Netware)

- Administrators – Full Control

- ShareScanAdmin – Full Control

- 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 PC where the Inbox location resides.

eCopy Quick Connect

For information on supported configurations, consult the Technical Specifications document.

Installation Prerequisites and Suggestions

- When selecting a network location as a Quick Connect destination, make sure that the 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) on Windows 10, Windows Server 2012 or later. 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 information on supported RightFax versions, consult the Technical Specifications document.

Installation Prerequisites and Suggestions

– The administrator will be prompted to enter a valid RightFax or NT Authentication user name and password. The RightFax server name will also need to be entered.

– The RightFax client software must **NOT** be installed on the system where the ShareScan Manager is installed.

– Delegation 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:
If "Send from personal account" is not enabled, all faxes will be sent from the user name and password supplied for configuration purposes.

eCopy Scan to Printer

Installation Prerequisites and Suggestions

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

eCopy Connector for Microsoft SharePoint

For information on supported SharePoint versions, consult the Technical Specifications document.

Installation Prerequisites and Suggestions

– The administrator should enter a user name and password that will enable browsing to all destination locations, display all index fields, and store documents if "Login As" authentication is used.

– If you are using SharePoint 2007: Microsoft Office SharePoint Server (MOSS) 2007 or Windows SharePoint 2007 Services.

– If you are using SharePoint 2010: Microsoft SharePoint Server 2010.

– If your company 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. Storing to an Attendees location is inconsistent and may result in failure to store the scanned document.

– The All Day Event, Recurrence, and Workspace checkboxes will not appear in the calendar list.

eCopy Connector for EMC Documentum

For information on supported EMC Documentum versions, consult the Technical Specifications document.

Installation Prerequisites and Suggestions

– The eCopy connector for EMC Documentum uses the Documentum Foundation Classes (DFC) to connect to the Documentum Server. While all of the necessary DFC files are included with the connector, DFC needs to be configured as part of the installation process.

– For Configuring DFC the following information is required:

- The Primary *Connection Broker* Host Name: Broker Server Name

- Port number: Default = 1489

- Repository Name

- Login Name and Password to that Repository

- The DFC should be in the same domain as Documentum server

– The eCopy connector for EMC Documentum will then need the Repository chosen from the drop-down menu, as well as a user name and password. In the connector Administration, all Repositories available through that Connection Broker will now 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 store documents if "Login As" authentication is used.

– If you are using a firewall, you must add `SQLSERVER.exe` and UDP port 1434 to the exceptions list.

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

– **Connection Broker** – Named DocBroker in previous versions of Documentum. Connection Broker is a service that runs on a Documentum server; it is a connection point from the client.

– **Repository** - Named Docbase in previous versions of Documentum. It is a document database on the Documentum server. The Connection Broker establishes the connection between the connector and the Repository.

eCopy Connector for Autonomy iManage WorkSite

For information on supported Worksite versions, consult the Technical Specifications document.

Installation Prerequisites and Suggestions

– The administrator should enter a user name and password that enables browsing to all destination locations, display all index fields, and store documents if **Login As** authentication is used.

– For more information on Impersonation passwords, the administrator should refer to the WorkSite documentation. Note that Impersonation is only available when using Trusted Login and authenticating against Novell.

– When you use Novell Trusted Login, make sure that the Novell Client configuration on the computer running the

15

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.

eCopy Connector for Open Text Content Server - eDOCS Edition

For information on supported eDOCS versions, consult the Technical Specifications document.

Installation Prerequisites and Suggestions

– Before installing the eCopy connector for Open Text Content Server, the Administrator must install and configure the Windows Explorer DM Extension software for Open Text 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 PC as the eCopyShareScan Manager. After that, run the DM Connection Wizard.
All versions of the DM Extension software include the required DM API and the DM Connection Wizard.

– Install the Windows Explorer DM Extension component only (under 'Optional Components').

– You must select 'Intranet Mode' (the default mode). 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 be on 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.

– It is recommended that you add the eCopy Document Type and Application ID to your eDOCS (Hummingbird) server. See your server documentation for details.

– 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.

– For instructions about installing the DM Extension software, refer to your eDOCS documentation.

eCopy Connector for Open Text Content Server

For information on supported Open Text Content Server versions, consult the Technical Specifications document.

Installation Prerequisites and Suggestions

– The administrator must enter a user name and password that enables browsing to all destination 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. E.g.:
    `https://TestContentServer:443/cws`

> **Note:**
> **Web services** protocol supports Table Key Lookup attributes only in case of an OpenText Content Server (Livelink) 16.2 or later.

- 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 tocommunicate 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 supports Table Key Lookup attributes only in case of an OpenText Content Server (Livelink) 16.2 or later, 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.
> The 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 Open Text Content Server environment requires a user to change password at the next logon to the system, the user must change the password at the workstation before using ShareScan. If the user does not do this, the system will display a message that the password has expired and that the user will not be able to store the scanned documents.

– For authentication methods outside of these constraints, refer to your eCopy Technical Consultant.

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.

Konica Minolta client checklist

Checklist for using Konica Minolta devices with embedded clients

– Confirm that the device and the firmware you are planning to use is supported.

– Make sure that the device's Web Server is accessible.

– In case the devices and the ShareScan Manager PC are in different subnets, it is recommended to manually resolve IP addresses in the hosts file on the ShareScan Manager PC (located under **C:\Windows\System32\drivers\etc**).

– If you need complete security, it is recommended that you enable SSL (Secure Sockets Layers) on devices running ShareScan 6.3. For information about configuring SSL on the device, refer to the Konica Minolta documentation.

– 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. To configure the device to work with ShareScan, you set several options in the Internet Explorer browser and on the device.

  – **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. On most devices, the timers are available under the **Utility** > **Administrator settings** > **System settings** > **Reset Settings** path (for instructions on your actual model, refer to the device documentation).

  To make ShareScan time out after nine minutes of inactivity, set the **System Auto Reset Time** (in **System Auto Reset** > **System Auto Reset Time**), and the **Copy, Web Browser**, **Scan/Fax** and **User box** timeout values (in **Auto Reset** > **Copy** / **Web Browser** / **Scan/Fax** / **User box**) 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.

Checklist for using Konica Minolta devices with ScanStation

– If you are using ScanStation hardware, ensure that all required software components (including the Touchscreen driver) are installed and configured properly.

– If you are using non-ScanStation hardware, the ShareScan Manager and the ScanStation client must be installed and functioning properly on the same PC.

– ScanStation uses the proper driver to get input from a supported MFP. You must install and configure this driver next.

– Use www.mykonicaminolta.com to check and download the specific TWAIN driver for your Konica Minolta bizhub device.

This document is a checklist containing *device-related pre-installation information only*. When all above 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.

Hardware recommendations for HTTP clients

The following section contains hardware recommendations, assuming up to 50% of the MFPs are concurrently processing scanned documents; 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 the responsiveness of the application.

Note:
For a server supporting multiple brand MFPs or varying user loads please consult your eCopy Technical consultant for specific sizing recommendations.

Enabling background processing positively impacts the scalability.

Sizing recommendations

The table does not factor in background processing.

Client MFPs per ShareScan Manager	1-15	16-30	31-45	46-75	76-120
B&W Letter / A4 200 DPI No OCR	**Operating system**: Windows Server 2012 or Server 2016 or Server 2019 **Minimum CPU**: Dual Core or Core 2 Duo **Minimum RAM**: 4 GB			**Operating system**: Windows Server 2012 or Server 2016 or Server 2019 **Minimum CPU**: Quad Core **Minimum RAM**: 6 GB	

Client MFPs per ShareScan Manager	1-15	16-30	31-45	46-75	76-120
Color Letter/A4 300 DPI No OCR	**Operating system**: Windows Server 2012 or Server 2016 or Server 2019 **Minimum CPU**: Dual Core or Core 2 Duo **Minimum RAM**: 4 GB		**Operating system**: Windows Server 2012 or Server 2016 or Server 2019 **Minimum CPU**: Quad Core **Minimum RAM**: 6 GB		
B&W / Color Letter/A4 300 DPI with OCR	**Operating system**: Windows Server 2012 or Server 2016 or Server 2019 **Minimum CPU**: Dual Core or Core 2 Duo **Minimum RAM**: 4 GB Max 4 OCR-ing		**Operating system**: Windows Server 2012 or Server 2016 or Server 2019 **Minimum CPU**: Quad Core **Minimum RAM**: 6 GB Max 8 OCR-ing		**Operating system**: Windows Server 2012 or Server 2016 or Server 2019 **Minimum CPU**: Xeon 8 Core **Minimum RAM**: 8 GB Max 10 OCR-ing

Sizing recommendations for ScanStation configurations

Operating system: Windows 10 x64

Minimum CPU: Dual Core or Core 2 Duo

Minimum RAM: 2 GB

Recommended RAM: 4 GB