eCopy ShareScan 6.2

Pre-Installation Checklist and Sizing Guide for Epson Devices

Date: 2019-07-19

KOFAX

Licensing, Copyright, and Trademark Information

Customer Support Services

The support services are available to registered users of the software during the warranty period or for the duration of your software Maintenance and Support (M&S) agreement. Contact your supplier for details, as described in the M&S agreement.

In addition to support provided by your dealer or distributor, the eCopy Support website provides 24x7 access to a knowledge base. To access it, click the link on the main Support page.

Table of Contents

Chapter 1

ShareScan Pre-Installation Checklist and Sizing Guide for Epson Devices

Prerequisites - Overview

To enable eCopy ShareScan functionality on your Epson MFP, you need the following software components:

- eCopy ShareScan: this software provides a wide variety of workflows and integrations for document capture at the MFP
  - 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. For a quick list of requirements designed to provide a smooth user experience, consult the prerequisites section in the document **Unified Client for Epson – eCopy ShareScan Deployment Guide**. Detailed requirements can be found in the product documents supplied with the above components. This current pre-installation checklist contains detailed eCopy ShareScan prerequisite information.

About ShareScan pre-installation checklist and sizing 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, see the relevant vendor-specific *Pre-Installation Checklist and Sizing Guide* (PICL). 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 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.

Related documentation

The following documentation is available for your perusal with ShareScan:

Guide	Description
Pre-installation Checklist and Sizing Guide (PDF)	Provides information on the issues to be addressed before deploying ShareScan.
Installation Guide (PDF)	Provides information on installing ShareScan, including hardware and software prerequisites.
Administration Console Help	The integrated help of the application, covering the use of ShareScan beyond installation, and provides configuration information. **Note** The help is accessible by pressing F1 on the ShareScan Administration Console.
Troubleshooter User Guide (PDF)	Provides information on how to use the ShareScan Troubleshooter, a built-in diagnostic tool of the product.
Release Notes (PDF)	Provides an overview of the changes for the given ShareScan release.
High Availability and Load Balancing Deployment Guide (PDF)	Provides guidance on how to deploy ShareScan to function in high availability mode.
Capture Server Monitor Configuration Guide (PDF)	Provides information on how to use the Capture Server Monitor tool for monitoring ShareScan instances.

To view the PDF documentation, you must have a PDF reader application installed.

ShareScan Installation Prerequisites

The following topics contain 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

The ShareScan 6.2 install media contains all of the following required dependency installer files under `Install\ShareScan\SetupPrerequisites\` in separate folders that must be installed to ensure ShareScan functions properly.

- Java SE Runtime Environment 8 Update 144 (x86)
- Microsoft .NET Framework 4.6.2
- Microsoft Visual C++ 2012 Redistributable (x86) – version 11.0.61030

- Microsoft Visual C++ 2015 Redistributable (x86) – version 14.0.24123
- Microsoft Visual C++ 2015 Redistributable (x64) – version 14.0.24123
- Microsoft Visual J# 2.0 Redistributable

Note The ShareScan 6.2 installer cannot be launched unless .NET Framework 4.6.2, or a later Framework 4 version is installed on the target system. When trying to launch the installer without .NET Framework or any version older than v4.6.2 installed, an error message pops up detailing the dependency and the install media path for the offline .NET Framework installer. This error 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.

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.

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

How to install Windows security update

To install Microsoft Visual C++ 2015, Windows Security Update `KB3000483` must be installed on the target system. If the security update is not installed, the Microsoft Visual C++ 2015 installation might freeze without completion.

1. Uninstall Microsoft Visual C++ 2015 runtime redistributable (x86 / x64).
2. Download the `KB3000483` security update from https://www.microsoft.com/en-us/download/details.aspx?id=45570 and install it on the target system.
3. Choose **Restart** from the dialog that appears.
4. Re-install Microsoft Visual C++ 2015 runtime redistributable (x86 / x64).

Supported operating systems

- Windows 7 SP1 Home Premium, Professional and Ultimate Editions
- Windows 8.1
- Windows 10 Anniversary Update or later
- Windows Server 2008 R2 SP1*
- Windows Server 2012 R2*
- Windows Server 2016*

  *64 bit support as a 32 bit application

Note The ShareScan Administration Console and the ShareScan Manager cannot be installed on Linux, Solaris or Macintosh operating systems.

Supported database

- Microsoft SQL Server 2008 Express or later edition
- Non Express edition

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.

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

Required memory configuration

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

- 4 GB physical memory (minimum); 6 GB recommended (8 GB recommended for systems using 100+MFPs)
- 5 GB disk space (including SQL server and prerequisites)

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

Required open ports

If you are planning to have firewalls enabled, you must leave the following ports open between ShareScan Manager and the multifunctional device for:

Direction (manager PC)	TCP	UDP
Inbound	• 443: Main secure communication channel for web based devices • 8080: Used to connect to Web Services on the devices, when HTTPS not used • 9600: In case of web-based devices requests are sent by the Tomcat Web server to the ShareScan Manager Service on the same machine • 9650: Used in multi manager / HA setups, for Manager to Manager communication • 9700: Management port, when Capture Server Monitor is used to test this ShareScan server • 9610: Image upload port • 80: Device port used for HTTP connections • 587: SMTP email server port used if TLS is enabled • 8443: TLS connections between DWS and the MFP	• 9650: Port for ShareScan managers to communicate about output creator processes. Also, a maintenance service port for ShareScan managers in multi-manager setups.
Outbound	• 1433: SQL server default port • 9650: Used in multi manager / HA setups, for Manager to Manager communication	• 161: Standard port of SNMP protocol • 8899: Used by ShareScan device discovery • 9650: Port for ShareScan managers to communicate about output creator processes. Also, a maintenance service port for ShareScan managers in multi-manager setups.

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

Database permissions

- In case of upgrading the eCopy ShareScan database, you must use an account that has `db_owner` Database-Level role permissions for the database. For clean installation scenario related database permissions, see the *User rights necessary for ShareScan database creation* section of the *Installation Guide*.

  Note An account with `sysadmin` Server-Level role can be used, but it is not mandatory.

- Use only the eCopy account created by the ShareScan database installer, or a user having the same 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.

  Note Do not use an `sa` account as a ShareScan runtime account for database connection as it will not work.

Note If Integrated Windows Authentication is used to connect to the database, and Form Processing Extender (FPE) or SmartForms Extender (SFE) profile is edited in the Administration Console (by using the template editor of the extenders), 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 configuration

Domains and Workgroups

ShareScan can be configured to run in either domain-based networks or workgroup environments. Windows 2008 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 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 ShareScan Manager.

IP Addresses

Use static IP addresses for both the ShareScan Manager PC and the MFPs. To change the IP address of the Manager PC, refer to How to modify IP address.

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

Gateway Address

ShareScan does not require a gateway address.

Host Name

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

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

Network Attached Storage Devices (NAS)

ShareScan 6.2 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.

How to modify IP address

This topic briefs you on how to modify the IP address for devices that work with and without certificate:

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

Modify IP address (certificate required)

1. Remove all devices from the ShareScan Manager.
2. Change the IP address.
3. Reboot the ShareScan Manager PC.
4. Start the ShareScan Administration Console, and confirm the IP address change on the dialog that automatically opens.
5. If your devices require a certificate to work, recreate the certificate(s).
6. Re-add the devices to the Manager.

Checklist for ShareScan Manager

This topic briefs you about all the system requirements that must be met for installation of ShareScan Manager PC.

- ShareScan 6.2 installs a customized Apache Tomcat web service, as previously installed Tomcat installations are not supported. If you do not wish to install a webclient during the 6.2 installation or

later, ignore any Apache Tomcat references. If you install the web client, the simulator function of the ShareScan Administration Console defaults to using the web client for the simulator.

- ShareScan 6.x licenses are installed to a SQL Server to allow easy management of devices. The ShareScan installer can install a local copy of SQL Server 2014 Express for managing licenses in addition to storing configuration data. It can also create the appropriate database structure on an existing SQL server for consolidated key management.

  Note Prior to installing ShareScan 6.2, 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.

Check	Description
☐	Ensure that ShareScan Manager is installed to a dedicated PC which is exclusively tasked for the running of ShareScan Manager.
☐	Run the Automatic Updates of the operating system before you start installing ShareScan. **Note** Make sure you turn OFF the Automatic Updates during the installation.
☐	When designing the network architecture make sure you have Windows Server as an operating system, if you plan to have more than 10 devices. **Note** Windows 7 can handle a maximum number of 20 concurrent network connections.
☐	If you have multiple NIC cards, you must select an IP address for ShareScan that will be used for device-server communication.
☐	Check if your file system format is NTFS.
☐	Ensure that IIS is not installed or is not listening to the ports used by ShareScan listed below.
☐	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. **Note** • As licenses are tied to the ShareScan database, it is strongly recommended not to change the databases after ShareScan installation. • License keys can only be activated once, so you must inspect the setup carefully prior to activation. • All license keys provide a 30-day grace period before activation to ensure the license setup is as intended.
☐	If you plan to use the Single Sign-On feature of the Session Logon service, you must ensure the following: • The ShareScan Manager 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). • This Active Directory user must have the necessary rights to read Active Directory properties (generally this is a default behavior; however, this can be modified in Active Directory). • You use the Active Directory user account to log into this domain (and not into the local system).

Checklist for Epson device

This topic briefs you about all the steps you must perform to get your Epson device ready for deployment, using the Web Config of the device:

Check	Description
☐	Verify whether the Epson device you are planning to use is supported for deployment. For a latest list of supported Epson models, you may consult your local Epson representative or refer to the Supported Device Search webpage https://kofaximaging.custhelp.com/app/imaging/supported_devices.
☐	Verify the firmware version of the device. To do this: 1. On the Web Config of the device, click **Device Management** > **Firmware Update** . 2. Check the firmware version.
☐	Ensure that you have activated the Epson Open Platform 1.1. To do this, 1. Use the serial number of the device to acquire the product key at https://openplatform.epson.biz/license-op/inputInformation.html 2. On the Web Config of the device, click Epson Open Platform tab and enter the acquired key. 3. Set Epson Open Platform version to 1.1.
☐	Verify that the `Administrator Password` set for the device in the Product Security tab is reflected in the Username and Password fields in the Devices tab of DRS.
☐	Optional: Ensure that USB Card Reader access is enabled. To do this, 1. On the Web Config of the device, click **Product Security** > **External Interface** . 2. Set Memory Device to Enabled.
☐	Confirm the valid certificate status. To do this, 1. On the Web Config of the device, click Network Security tab. 2. Under SSL/TLS settings group, select Certificate. 3. Select Self-signed Certificate from the Server Certificate drop-down list. 4. Click Update.
☐	Verify date, time and locale. To do this, 1. On the Web Config of the device, click Device Management tab. 2. Enter the information under Date, Time and Time Difference.

Supported languages, devices and services

This section briefs you on the various languages and third-party software supported by ShareScan.

Supported Languages

ShareScan 6.2 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

To view a list of current devices, go to the Support Devices website.

Supported Backend Services

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

eCopy connectors for backend applications

It is recommended to match the application credentials for various backend applications with the PC login credentials. It is recommended to create a generic, email-enabled ShareScan account for use by ShareScan.

Note 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 working of these applications can be found in the application's own documentation and not in the ShareScan documentation.

The following backend applications are supported:

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

- eCopy connector for EMC Documentum
- eCopy connector for Autonomy iManage WorkSite
- eCopy connector for OpenText Content Server - eDOCS edition
- eCopy connector for OpenText Content Server

Supported versions

This topic briefs you about the supported versions of the backend applications to work with eCopy connectors. For detailed information on the supported versions, see the Compatibility Matrix available at the Kofax Navigator website.

Backend Applications	Supported Versions	Installation Prerequisites
Microsoft Exchange (Mail and/or Fax)	Microsoft Exchange 2007 / 2010 / 2013 / 2016 / Exchange Online for Office 365	eCopy connector for Microsoft Exchange (Mail and/or Fax)
IBM Lotus Notes (Mail and/or Fax)	• IBM® Lotus Notes® 8.0 / 8.5 / 9.0.1 • Lotus Domino 8.0 / 8.5	eCopy connector for IBM Lotus Notes (Mail and/or Fax)
LDAP/SMTP (Mail and/or Fax)	• Microsoft LDAP v3 • Open LDAP v2.4	eCopy connector for LDAP/SMTP (Mail and/or Fax)
Quick Connect	• Quick Connect supports Oracle® Database 10g and 11g. When you install Oracle Client 10g/11g, select the Custom Installation option and then make sure that you select the Oracle Provider for OLE DB component. This enables Quick Connect to connect to the Oracle database and store scanned documents and other information. • For more information about supported databases, see the eCopy ShareScan 6.2 Software Compatibility Matrix. • For additional information on supported configurations of eCopy Quick Connect to Database, reference the Quick Connect Database Recommended Usage document available for download from eSPN.	eCopy connector for Quick Connect
OpenText Fax Server (RightFax Edition)	OpenText Fax Server 9.0/9.3/9.4/10/10.5/10.6/16 E2/16 E4	eCopy connector for OpenText Fax Server (RightFax Edition)
Microsoft SharePoint	Microsoft SharePoint 2007, 2010, 2013, 2016, SharePoint Online for Office 365 / Microsoft SharePoint Server 2007,	eCopy connector for Microsoft SharePoint

Backend Applications	Supported Versions	Installation Prerequisites
	2010, 2013, 2016, (includes support for SharePoint BDC/BCS)	
EMC Documentum	EMC® Documentum® 6.6, 6.7, 7.0, 7.1, 7.2	eCopy connector for EMC Documentum
Autonomy iManage WorkSite	Autonomy (Interwoven) iManage (WorkSite) 8.0-9.0, 9.0SP1, 9.1, 9.2, 9.3, 10, 10.1, 10.2	eCopy connector for Autonomy iManage WorkSite
OpenText Content Server - eDOCS Edition	OpenText Document Management, eDOCS Edition /(Hummingbird) 5.1.05, 5.2, 5.3, 6.0.5, 10, 16.1	eCopy connector for OpenText Content Server - eDOCS edition
OpenText Content Server	Livelink (Enterprise Server) 9.7, 10.0, 10.5, 16, 16.2	eCopy connector for OpenText Content Server

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

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

Installation Prerequisites

- If configuring the Exchange connector using EWS or WebDAV protocols, 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 EWS/EWS protocol, the user's logon and alias name must correspond, due to limitations of the Exchange web services. Thus, it is recommended to use LDAP/EWS protocol.

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

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

Installation Prerequisites

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

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

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

For supported versions of LDAP/SMTP, see section Supported versions of 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 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 on clicking F1 on the Administration Console.

Note The `Inbox alternate path for folder root - DO NOT set it to the user's HOME folder` (see documentation) path pointing to the existing Network Home Directory Root Folder as it 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.

Note The Inbox Root Directory must not be pointing to a user's home directory. Choose the Scan to Desktop Home Directory option in the connector instead.

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 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. 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
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 PC where the Inbox location resides.

eCopy connector for Quick Connect

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

Installation Prerequisites

- 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 7, Windows Server 2008 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 supported versions of OpenText Fax Server, see section Supported versions of this guide.

Installation Prerequisites

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

Note The RightFax client software must not be installed on the system where the ShareScan Manager is installed.

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 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 ShareScan is also installed.

eCopy connector for Microsoft SharePoint

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

Installation Prerequisites

- The administrator must enter a user name and password that will enable browsing to all destinations, display all index fields, and store documents if `Login As` authentication is used.
- If you are using SharePoint 2003, you must have Microsoft SharePoint Portal Server 2003 or Microsoft Windows SharePoint Servers 2003.
- If you are using SharePoint 2007, you must have Microsoft Office SharePoint Server (MOSS) 2007 or Windows SharePoint 2007 Services.
- If you are using SharePoint 2010, you must have Microsoft SharePoint Server 2010.
- If your company uses a secure SharePoint site, you must install an SSL certificate on the ShareScan server.

Note

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

eCopy connector for EMC Documentum

For supported versions of EMC Documentum, see section Supported versions of this guide.

Installation Prerequisites

- The eCopy connector for EMC Documentum uses the Documentum Foundation Classes (DFC) to connect to the Documentum server. While all the necessary DFC files are included with the connector, the administrator needs to configure DFC 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 number is 1489
  - Repository Name
  - Login Name and Password to that Repository

  Note The DFC should have 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 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.

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 - Docbase Name 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.

Note Docbase Name is case sensitive.

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 Autonomy iManage WorkSite

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

Installation Prerequisites

- The administrator should enter a user name and password that enables browsing to all destinations, display all index fields and store documents if `Login As` authentication is used.
- When you use Novell trusted login, make sure that the Novell client configuration on the computer running the ShareScan Manager includes a value for the Preferred Server option.

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

Suggestions

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

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

eCopy connector for OpenText Content Server - eDOCS edition

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

Installation Prerequisites

- Before installing the eCopy connector for OpenText Content Server, the administrator must install and configure the Windows Explorer DM Extension software for OpenText Document Management, eDOCS Edition 5.1, 5.2 SP1, 6.0 or later or Hummingbird DM 5.1, 5.2 SP1, and 6.0 on the same computer as the eCopy ShareScan Manager. Once done, the administrator must run the DM Connection Wizard. All versions of the DM Extension software include the required DM API and the DM Connection Wizard.
- The administrator must install the Windows Explorer DM Extension component only (under 'Optional Components') and select Intranet Mode (the default mode).

  Note Do not select Internet Mode.

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

Note

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

Suggestions

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

eCopy connector for OpenText Content Server

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

Installation Prerequisites

- The administrator must enter a user name and password that enables browsing to all locations, display all index fields, and store documents if `Login As` authentication is used.
- The eCopy connector for Livelink ECM uses the Web services protocol and / or Livelink API (LAPI) for communication with Open Text Content Server.
- LAPI supports TCP/IP direct connections with native Livelink authentication. It does not support HTTP or HTTPS connections or non-native authentication methods. Native authentication using LAPI supports Livelink authentication, NTLM authentication, and LDAP authentication. The Livelink server is responsible for managing the authentication settings and the connector works transparently with the selected authentication mode
- In **Protocol** section of **Database & authentication** settings in the Connector configuration window, the Administrator will need to provide the following information to properly configure the connector:
  - If **Web services** is selected:
    - **Root URL**: The root URL of the web service granting access to the Livelink server. E.g.: https://TestContentServer:443/cws

      Note Web services protocol support 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. he eCopy Connector for Open Text Content Server does not support Table Key Lookup attributes for OpenText Content Server (Livelink) version 16 or higher since LAPI protocol itself is not supported by this server

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

Note

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

Suggestions

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

Sizing recommendations

The following topics brief you about the sizing and hardware recommendations for embedded configurations and the server configuration support required for large number of devices.

Sizing recommendations for embedded configurations

This section contains sizing 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 application responsiveness.

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.

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 2008 or 2012 or 2016 Minimum CPU: Dual Core or Core 2 Duo Minimum RAM: 4 GB			Operating system: Windows Server 2008 or 2012 or 2016 Minimum CPU: Quad Core Minimum RAM: 6 GB	
Color Letter/A4 300 DPI No OCR	Operating system: Windows Server 2008 or 2012 or 2016 Minimum CPU: Dual Core or Core 2 Duo Minimum RAM: 4 GB		Operating system: Windows Server 2008 or 2012 or 2016 Minimum CPU: Quad Core Minimum RAM: 6 GB		
B&W / Color Letter/A4 300 DPI with OCR	Operating system: Windows Server 2008 or 2012 or 2016 Minimum CPU:	Operating system: Windows Server 2008 or 2012 or 2016 Minimum CPU: Quad Core			Operating system: Windows Server 2008 or 2012 or 2016 Minimum CPU: Xeon 8 Core

Client MFPs per ShareScan Manager	**1-15**	**16-30**	**31-45**	**46-75**	**76-120**
	Dual Core or Core 2 Duo Minimum RAM: 4 GB Max 4 OCR-ing	Minimum RAM: 6 GB Max 8 OCR-ing			Minimum RAM: 8 GB Max 10 OCR-ing

Support for multiple devices

The above server configurations were tested with the published number of devices, using the document types / settings referenced.

The generic Microsoft recommendations for server operation not to exceed 75-80% of overall CPU load for a long period of time were also considered.

Also, with regards to memory and other resources, it is recommended to not exceed the above specified maximum number of devices connected to a single ShareScan server, since different resources such as memory, disk I/O bandwidth, handle or thread count can run short and may cause temporal or permanent performance and/or functional issues.

If hardware or Microsoft Network Load Balancing (NLB) is used for load balancing / high availability, the overall number of the devices divided by the number of active server nodes in the cluster is considered as device per server measure.

Note System support where the number of the devices connected to a single server exceeds these recommended maximum limitations is not possible.