Kofax eCopy ShareScan 6.2

Installation Guide for Epson Devices

Date: 2019-07-19

KOFAX

Table of Contents

ShareScan Installation Guide for Epson Devices

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.

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.

Other Components

The following components must be installed on separate servers other than the ShareScan Manager server for a complete eCopy ShareScan deployment for Epson:

- Device Web Server: A server that manages and controls embedded applications on web-based multifunction printers such as the Epson device. For more information, refer the <**DWS document name**>
- Device Registered Service: A web-based interface that enables you to manage Applications, Devices, and Device groups. This service is used to register the Unified Client on the Epson device. For more information, refer the <**DRS document name**>

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 rights

- In case of upgrading the eCopy ShareScan database, you must use an account that has `db_owner` rights for the database. For clean installation scenario related database rights, see the User rights for database creation section of this document.

  Note An `sa` level account 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.

Checklist for DWS

This topic briefs you about all the steps you must perform to install the Device Web Server:

Check	Description
☐	

Check	Description
☐	

Checklist for DRS

This topic briefs you about all the steps you must perform to install the Device Registration Service:

Check	Description
☐	Microsoft .NET 4.6.2
☐	

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.

About installing ShareScan

The following sections give a brief overview of basic installation workflow, various installation scenarios and detailed procedures to install.

Installation Overview

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

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

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

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

Important Ensure that the ports used for both inbound and outbound network traffic are left open. See section, Required open ports

Basic installation workflow

To install, configure, and license ShareScan perform the following actions:

- Install the ShareScan software on a network computer. You have the option to customize the database installation. For more information, see the Custom installation section of this guide.
- Client is automatically registered to the ShareScan database the first time when they start to communicate with the ShareScan Manager. For more information on auto-registration of client, see the Auto-registration of devices with Unified Client section of this guide.
- Start the Administration Console to add licenses and devices if they do not appear automatically on the Devices tab, and/or set up scanners. The model name in the dialog that appears as part of device addition procedure differs from the name of the device that is displayed in the tree control on the Devices tab. The tree control on the Devices tab contains the network (host) name of the devices or the IP address of the devices, if the host name cannot be resolved. This ID is used as a unique identifier for the devices in the ShareScan system. This cannot be changed in the Administration Console, only via the device administration user interface and / or in the network Domain Name Server (DNS).

  Note The model name specified during device addition can be changed anytime via Modify Model Name on the Administration Console. To do this, right click the added device in the Devices tab and select Modify Model Name.

- Install and configure services, connectors and devices.

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

For in-depth information about configuring and managing the services, connectors and devices that ShareScan uses, refer to the ShareScan Help. To access the Help, click F1 or click the Help button that is located in the upper right corner of the ShareScan Administration Console.

ShareScan install scenarios

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

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

If you are upgrading existing ShareScan versions, ShareScan 6.2 performs a complete installation where you can only customize the installation location on Destination Folder screen and database access and service account credentials on the Service Credentials screen. When upgrading in a multi-manager deployment, it is recommended to upgrade the individual ShareScan managers one by one.

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

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

- User identifiers
- Passwords
- Database name fields

How to do a complete installation

1. If you have a physical ShareScan installation media, insert it in the optical drive of your PC and browse to the folder where the `ShareScan6.2.exe` file is located. If you have a digital copy of the ShareScan installer, you can find the `ShareScan6.2.exe` file under the `Install/ShareScan` path.
2. Run `ShareScan.6.2.exe` installer. The Choose Setup Language screen is displayed. Select a preferred language (English by default) from the drop-down list and click **Next**.
3. The Welcome screen is displayed. Click **Next**.
4. The installer displays the System Check screen. If prompted, select the preferred option(s) from the drop-down list(s). Click **Next**.

   This screen displays warnings on any possible issues that might have an impact on the proper operation of ShareScan and provides information on how to resolve them. If relevant, it also enables you to choose from more than one option such as the number of available network adapters for device-manager communication.
5. The Enter Product License Key screen is displayed. Provide your license key (22 characters with dashes, or 18 without dashes; the system accepts either). Click **Next**.

6. Specify your location on the Choose Your Geographic Region screen. Click **Next**.
7. The End-User License Agreement (EULA) is displayed on the License Agreement screen. Accept the EULA and click **Next**.
8. The Setup Type screen is displayed. Select **Complete**. Automatic full installation is performed including the following installations:

- eCopy ShareScan 6.2 server is installed
- Microsoft SQL Server database engine is installed
  - SQL Server 2014 SP2 Express Local DB is installed.

    Note Since you cannot connect to this type of database engine from another computer on the network, it is not recommended to use this option if you plan to share the installed database between multiple managers. In that case, select the Custom installation option. Using LocalDB as a database server engine is only recommended in case of small-scale installations, if only a few devices are included.

- eCopy ShareScan configuration database is created on the installed SQL Server
- eCopy ShareScan 6.2 WebClient is installed (including the Apache Tomcat server)
- Default eCopy credentials (username / password) is used for database access, with SQL server authentication
- `C:\%programfiles%\Kofax\ShareScan6.2` is the default installation path

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

How to do a custom installation

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

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

1. Perform steps 1 - 7 as described in the Complete Installation section.
2. The Setup Type screen is displayed. Select **Custom**.
3. The Custom Setup screen is displayed. Select the program features you want to install and click **Next**. The following components can be selected for installation:
   - eCopy ShareScan 6.2 Server — a mandatory component that you must install in all possible scenarios as you cannot deselect it.
   - Microsoft SQL Server database engine (selected by default) — select this component if you want a local installation of Microsoft SQL Server Express or Express LocalDB. These deployment options are recommended for small-scale deployments with a single manager. If you deselect this

component, the installer assumes you have an existing SQL Server installation either locally or on another server on the network to which you are planning to connect.

- eCopy ShareScan configuration database — select this component if you want to create a ShareScan configuration database. It is necessary to select this component:
  - if you install a single ShareScan Manager
  - if you plan to install multiple managers and you do not want to share the same database across them
  - if you plan to have multiple managers and you are installing the first ShareScan Manager.

Note This component is selected by default. You can deselect it only if the Microsoft SQL Server database engine component is deselected, but in this case you need to specify database properties on the Database Catalog Name and Database Server and Runtime Account Information screens.

- eCopy ShareScan 6.2 WebClient (selected by default) – select this component if you plan to use scanner devices with web browser enabled user interface.

How to install all components

This custom setup scenario installs all four components:

- eCopy ShareScan 6.2 Server
- Microsoft SQL Server database engine
- eCopy ShareScan configuration database
- eCopy ShareScan 6.2 WebClient

Note If you deselect the eCopy ShareScan 6.2 WebClient component, the installation scenario is comprised of the same steps described below, respectively:

1. Once you select all components and/or optionally deselect the eCopy ShareScan 6.2 WebClient component on the Custom Setup screen, click **Next**.
2. The Destination Folder screen is displayed. Click **Change** to modify the default destination folder for the ShareScan server or the Apache Tomcat web server installation. The Apache Tomcat web server is required for ShareScan WebClient. Click **Next**.

3. Specify service credentials on the Service Credentials screen. Use default service accounts, or specify your custom service accounts for the ShareScan Manager and ShareScan Agent Windows services. These accounts must be valid domain accounts (users). Click **Next**.

   Note While the installer supports using custom accounts to run the services, using integrated Windows authentication for the local database connection is not supported by the installer when the ShareScan installer installs the SQL server. If you want to use integrated Windows authentication on a local SQL server, you have to install ShareScan first with the available installation type i.e. using default of custom credentials with SQL Server authentication and then later modify the service accounts and database permissions manually.

   Note Grant
   Grant after the installer detected that some local privileges are not granted to the service accounts, the installer tries to grant the missing privileges.
   If this cannot be successfully performed, the installer still detects that the privileges are missing and it does not continue the installation. The user must exit from the installer, resolve the issue either grant the missing privileges manually or eliminate the blocking factor to allow the installer to grant them during the next run, and then re-run the installer.

4. Specify the database type to install on the Local Database Server screen. Select the SQL server database engine. Regardless of the selected SQL Server type, you can override the password of the SQL Server system administrator that is, the `sa` password, by unmarking the check box at the bottom of the screen. If you do so, you must provide a password that complies with the password policy in effect. If you plan to have more than one manager to connect to this SQL server, than you should select SQL Server 2014 Express instead of local DB. Click **Next**.

   Note If you specified custom service accounts on the Service Credentials screen (**Use default service accounts** check box unmarked), the **Microsoft SQL Server 2014 Express Local DB** option is disabled, on the Local Database Server screen, since it cannot be used with custom service accounts.

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

   Note If the eCopy ShareScan 6.2 WebClient component is selected, this scenario is equal to the Complete Installation scenario, since all four components are installed, but you still need to specify related settings on the Destination Folder, Service Credentials, Local Database Server screens, alternately you can click through these screens leaving the default settings untouched.

   Note If you specified custom service credentials in step 3, eCopy ShareScan 6.2 installer will ask for agent service user password.

How to install without Microsoft SQL Server

This custom setup scenario installs the following three components:

- eCopy ShareScan 6.2 Server

- eCopy ShareScan configuration database
- eCopy ShareScan 6.2 WebClient

Note If the eCopy ShareScan 6.2 WebClient component is deselected, the installation scenario is comprised of the same steps described below, respectively.

1. Once you deselected the Install Microsoft SQL Server database engine component and/or optionally deselected the eCopy ShareScan 6.2 WebClient on the Custom Setup screen, click **Next**.
2. The Destination Folder screen is displayed. Click **Change** to modify the default destination folder for the ShareScan server, or the Apache Tomcat web server installation. The Apache Tomcat web server is required for ShareScan WebClient. Click **Next**.
3. Specify service credentials on the Service Credentials screen. Use default service accounts, or specify a different service account for the ShareScan Manager and ShareScan Agent. These accounts must be valid domain accounts (users). Click **Next**.

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

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

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

   Click **Next**.

   Note If the runtime database user (eCopy by default) already exists on a remote SQL server either from a previous installation or because it is created by the database administrator manually, a valid password must be specified for login.
5. The Database Catalog Name screen is displayed. Specify the ShareScan database name here or leave the default name. Click **Next**.
6. The Database Server and Runtime Account Information screen is displayed. You can specify a runtime account for the configuration database.

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

- via SQL Server authentication, using the default user name **eCopy** and the default password.
- via integrated Windows authentication, using the identity of the accounts running the services available only if custom accounts were specified on the previous wizard screen.

Note If this option is selected the **Use specified credentials given to Service Accounts for database connection** radio button and the administrative database user has no **db_securityadmin** database-level role (cannot create logins), the database administrator has to create the database users manually, otherwise the installed system will not operate properly.

- via SQL Server Authentication, using specified user name and password

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

Click **Next**.

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

   Note If you specified **Custom Service Credentials** in step 3, eCopy ShareScan 6.2 installer will ask for agent service user password.

How to install Server and WebClient only

This custom setup scenario installs the following two components:

- eCopy ShareScan 6.2 Server
- eCopy ShareScan 6.2 WebClient

Note If the eCopy ShareScan 6.2 WebClient component is deselected, the installation scenario is comprised of the same steps described below, respectively.

1. Once you deselected the **Install Microsoft SQL Server database engine** and **eCopy ShareScan configuration database** components and/or optionally deselected the **eCopy ShareScan 6.2 WebClient** component on the **Custom setup** screen, click **Next**.
2. The **Destination Folder** screen is displayed. Click **Change** to modify the default destination folder for the ShareScan server, or the Apache Tomcat web server installation (the Apache Tomcat web server is required for ShareScan WebClient). Click **Next**.
3. Specify service credentials on the **Service Credentials** screen. Use default service accounts, or specify a different service account for the ShareScan Manager and ShareScan Agent. These accounts must be valid domain accounts (users). Click **Next**.
4. The Database Catalog Name screen is displayed. On this screen, you must specify the hostname or IP and optionally, the instance name of the Microsoft SQL Server where the existing 6.2 ShareScan database is hosted. You must also specify the existing database name. Click **Next**.

5. The Database Server and Runtime Account Information screen is displayed. You need to provide the runtime account information for the configuration database. Click **Next**.

Note If the **Use specified credentials given to Service Accounts for database connection** radio button is selected, the database administrator has to create the database users manually, otherwise the installed system will not operate properly.

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

   Note If you specified custom service credentials in step 3, eCopy ShareScan 6.2 installer will ask for agent service user password.

   You are now ready to configure a connector profile.

User rights for database creation

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

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

Since ShareScan 5.1, `sa` rights are not required anymore for database installation, allowing the cases below. Having `sa` rights simplifies the process, as in that case you do not need to set anything on the SQL server.

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

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

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

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

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

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

Most restrictive environment

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

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

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

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

Maintenance

If you re-launch the ShareScan installer after successful installation of ShareScan 6.2, the Program Maintenance screen is displayed after you select a preferred language from the drop-down list on the Choose setup language screen and click Next. The following option is available:

Remove

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

Note If you installed ShareScan 6.2 over an existing ShareScan version, removing ShareScan 6.2 does not bring back the previously existing ShareScan version. Removing the WebClient feature of ShareScan also removes the Apache Tomcat server.

Profile tool

The Profile Tool allows you to manage connector, service profile information, watchers and data publishing maps between ShareScan 6.2 Managers. You can export such profile information from a Manager, then start up another Manager, and import the profile information.

Unlike connector profiles, newly imported watchers do not automatically overwrite watchers with the same name already existing on the target machine. These imported watchers are created as new ones. To

update a watcher via import, first you have to delete the current watcher on the target machine and then do the import.

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

To perform profile export, see How to export connector profiles

To perform profile import, see How to import connector profiles

How to export connector profiles

To perform an export, do as follows:

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

How to import connector profiles

To perform an import, do as follows:

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

Client-side auto-registration

The following sections provide information about auto-registration of Epson device with the Unified Client and the new feature of IP address filtering mechanism that eCopy 6.1 has introduced.

Auto-registration of devices with Unified Client

The Unified Client installed devices are managed through the Device Registration Service (DRS). As a result, such devices cannot be added to eCopy ShareScan through the usual Add Devices dialog which is otherwise used to register devices with ShareScan. For the Unified Client to be able to communicate with the ShareScan Manager, a Server configuration is specified in the DRS.

Unified Clients get automatically registered to the ShareScan database the first time when they communicate with the ShareScan Manager. During auto-registration, the devices are added under the Unified Clients user group that appears in the Devices tab of Administration Console. These auto-registered devices can be moved outside this group or they can be dropped to any other device group, if necessary.

Device Configuration

The list of devices in Administration Console is updated only upon successful registration of the device with the Unified Client. To know how a device is added in Administration Console, see How to add device to ShareScan Manager.

Connector profiles assigned to the Unified Clients group is the default set of workflows available for auto-registered devices. By moving the device out of this group, it becomes possible to assign connector profiles to individual devices or it can be moved to a different device group. To allow some control for the ShareScan administrator over the devices which use Unified Client, ShareScan provides a white list of IP addresses / ranges through which the administrator can allow / block devices with the specified IP addresses. This gives an extra security factor since ShareScan administrators have a tool to control the list of devices that can be served through the given ShareScan server. This IP address filtering is optional. If the IP address white list is not defined, ShareScan will not block any devices which have been registered in DRS previously.

How to add device to ShareScan Manager

1. Close the Administration Console on eCopy ShareScan server.
2. Launch the Device Registration Service (DRS) and add device details in respective fields.
3. Select **Register Device with Server Application** from the drop-down and click the green arrow button.
   If there are no technical issues observed, registration completes successfully.
4. On the Epson device, press the **Home** button to display the **Launcher**.
5. Log in at the Epson device with administrator credentials.
6. Acknowledge the notification message seen on the device screen and log out of the device.
7. Launch the Administration Console on eCopy ShareScan server.
   A new device group: **Unified Clients** is created in the **Devices** tab. The added device is listed under this group.
8. Select the group and choose the connectors that you want to be seen on the added device.
9. Click Save.
   Now you are ready to use the eCopy ShareScan connectors at the device.

Unified Client IP address filtering

ShareScan 6.2 introduces an IP address filtering mechanism to limit the IP addresses that devices can connect from. This IP filter can be configured in the ShareScan Administration Console. To configure the IP address filter, see How to configure IP address filter

The Manager uses this IP address filter configuration and refuses to serve the requests coming from other IP addresses. Since reading this IP address filter configuration in case of each request would cause a significant performance impact, the filter value is cached in ShareScan Manager service. The expiration time of this cached value can be configured as an advanced setting in ShareScan Administration Console. The value specified here is measured in minutes. If the Manager wants to use the IP address filter configuration to check if a request can be served or not, it will also check the age of the cached value. If the cached value is older than the configured expiration value, then the Manager reloads the IP filter configuration and uses the new value.

How to configure IP address filter

1. Right-click on the Device Configuration panel and select **Set Unified Client auto register filter** from the context menu.
2. Specify individual IP addresses or IP address ranges to the filter in the IP configuration dialog box.
3. Click **OK** to close the dialog box.

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, 2010, 2013, 2016, (includes support for SharePoint BDC/BCS)	eCopy connector for Microsoft SharePoint
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

Backend Applications	Supported Versions	Installation Prerequisites
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

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 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.

About licensing devices

ShareScan 6.2 includes a Licensing wizard, which handles the following license-related tasks.

Every device that you use with Kofax software requires a valid license. ShareScan 6.2 uses a digitally signed license file, which contains a unique license key generated by manufacturing. The license key is a unique ID that is associated with the hardware ID (HID) of the computer where the ShareScan database is installed.

Note ShareScan 6.2 licensing is different from ShareScan 4.x licensing, which was based on the association of a product key with a device. Licensing is no longer associated with a particular device, but the HID of the SQL server.

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

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

The Licensing wizard in ShareScan 6.2, handles the following license-related tasks:

- loading licenses
- activating licenses
- loading activated licenses
- reactivating licenses
- removing licenses

How to load licenses

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

1. Click **Load License** on the License wizard.
   The Welcome screen is displayed.
2. Click **Next** to continue.
3. Select **Download license automatically** when specifying the source to display the Automatic license download screen.
4. Copy the license keys of the licenses to download, in the text box and click **Add** after each. When the list below is complete, click **Next**.
   The Select license files to load screen is displayed.
5. Click **Browse** to add new files to the list of files to be imported. When finished, click **Start Import**.

6. Click **Start** to begin loading licenses.
7. Click **Finish** to close the License wizard.

How to activate licenses

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

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

How to load activated licenses

Use this option when importing already activated licenses to ShareScan.

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

How to remove licenses

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

1. Click **Remove** on License wizard.
   The Welcome screen is displayed.
2. Click **Next** to continue.
   The Select Licenses screen is displayed.
3. Select the license(s) you want to remove and then click **Next**.
4. Click **Start** to remove the selected license(s).
5. Click **Finish** to close the **License** wizard.

How to generate a license report

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

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

ShareScan post-install

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

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

Other configurations

This following sections outline the basic process to:

- Configure a service. See How to configure a service
- Configure an extender. See How to configure an extender
- Configure a connector profile (Scan to File) using the already configured service and extender. See How to configure a Scan to File connector profile
- Test your saved profile at the Epson device. See How to test profile configuration

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

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

You have the option to set up any connector with the Bypass redirect screen option. Using this option navigates the user back to the main form at the end of the session or logs out automatically if session logon is enabled.

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

The Epson client offers the following additional configuration option available via the ShareScan Administration Console:

- Suppress Preview and Settings - Enabling this setting reduces time spent at the device. Suppressed visuals are available to the user on-demand.

You can also choose from the following available authentication modes:

- CAP
- AAA
- Disabled

After changing the authentication mode, you need to manually restart the device.

How to configure a service

The following steps help you configure a service (example – Activity Tracking):

1. To start the Administration Console go to, **Start** > **Programs** > **eCopy Applications** > **ShareScan 6.2** > **ShareScan Administration Console** .
   The system initializes the .NET framework, retrieves configuration information from the ShareScan database, and then displays the ShareScan Administration Console.
2. Select the **Services** tab.
   The **Configure Services** pane displays a list of the installed services, including connector services, device services and common services.
3. In the **Device Services** list, select **Activity Tracking** to open the **Configure Activity Tracking Service** pane.
4. Select **Yes** for the configured setting and then click **Save**.

   For more information about configuring the activity tracking service, search for the Activity Tracking service topic in the eCopy ShareScan Administration Console Help.

How to configure an extender

The following steps help you configure an extender (example – Forms Processing Extender):
In this example, this extender is used to process scanned forms, extract form data, and make it available for Quick Connect via data publishing (using batching).

1. To onfigure the extender, create a template library and a template.

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

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

How to configure a Scan to File connector profile

The following steps help you configure a connector profile (example – Scan to File):

1. In the Administration Console, select the **Connectors** tab. The Configure connectors pane displays a list of the installed connectors.

2. Select the **Scan to File** connector.

3. Go to the **Destinations** tab in the Configure Connectors area and click **New**.
The Create a destination window opens.
4. Type a name for the connector and select the type of scan destination folder as the **Windows** folder.
5. Provide a scan destination path, such as `c://scans`.

   Note Make sure the scan destination folder has permissions as shared to **Everyone**.

6. Select **Logon As** from the **Authenticate User** list.
7. Provide the domain credentials of the user that are used to login on the eCopy ShareScan server.
8. Click **OK** to finish the configuration.
9. Save the currently configured connector as a new profile by clicking **Save current profile**.
The system saves your settings as part of the connector profile.
10. Select the device(s) listed under the **Devices** > **Device Groups** > **Unified Clients** in the Device Configuration pane on the left side of the Administration Console.
11. Assign the **Scan to File** connector to a device by selecting the specific connector profile in the Configure Connectors for Device pane.
12. Click **Save**.

How to test profile configuration

1. Login at the device as a domain user.
2. Tap the **Scan to File** connector on the device screen.

   Note The connector is displayed with the name that is entered in the Administration Console.

3. Place a sheet you wish to scan on the scanner tray of the device. A preview of the paper is seen on the screen, if enabled.
4. On the Folder Navigation screen, confirm the path of the shared network folder. If you wish to modify the scan destination tap **Change**, else tap **Next**.
5. On the Document routing screen, select the subfolder level at which you wish to create a scan folder.
6. Type a name for the scan folder and tap **Enter** to go back to the Document routing screen. The scan path is displayed. Tap **Next**.
7. On the File Name screen, the system-generated name for the scan file is displayed. If you wish to modify this file name tap on the screen to enter a new name. Tap **Enter** to go back to the File Name screen and tap **Next**.
8. On the Preview screen, a **Scan done** message is displayed in the **Notifications** bar. Exit the message by tapping the **X** icon.
9. A preview of the scanned document is displayed on the Preview screen. You may do any of the following:
   a. Tap **Finish** to complete the process.
   b. Tap **Home** to go back to Home screen of the device.
   c. Tap **Scan More** if you wish to scan more documents.
   d. Tap **Change** if you wish to modify the scan settings.

10. Tap **Done** on the Document submitted for processing screen.
    The connector scans the document to the folder you created in your shared network folder.

Next steps

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

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

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

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

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

Best practices

- Ensure that the `%temp%` environment variable is set.
- Ensure that all critical automatic updates are applied to target systems and that automatic updates are turned off for the time of installation.
- Do not wait too long to click Install, otherwise, the increased storage usage in the temp folder can trigger a cleanup process that causes installation failure.
- After installation, you may check to see whether the following services are running:
  - Apache Tomcat 8.5
  - ShareScan Agent
  - ShareScan Manager
  - ShareScan WatcherService
  - ShareScan Web Admin Host
  - PushKeyService

- There are other services which may not run by default, only if the respective functionality demands it:
  - Kofax Documentum API
  - Kofax Printer API
  - S2D Inbox Agent
- Tomcat service settings can be viewed/modified via: `%programfiles%\Kofax\Tomcat 8.5\bin\tomcat8w.exe`
- During the entire installation process, do not remove the original installation media from your optical drive, even though the installer has already extracted and decompressed the required components to a temporary location. This action can cause multiple failures depending on the stage of the installation during which the removal happens.
- To configure the Lotus Notes connectors (both Mail and Fax), you have to install the Lotus Notes Client on the PC. After installing, quit the client before running the ShareScan Administration Console, as the client locks the ID file, and a running client may cause issues with ShareScan.
- Ensure that there is no Apache Tomcat on the PC you want to install ShareScan on.
- Ensure that no ports used by ShareScan listed in the *Installation Guide* are used by other web services, as that may cause connectivity issues.
- Deploying the `RightFax FaxUtil` on the same machine on which ShareScan is running may cause issues, therefore it is not advised.
- If you are planning to use SharePoint Online with Windows Server 2012 as the operating system, ensure that you set the Windows Identity Foundation 3.5 feature to ON.
- If the Apache Tomcat component does not start after a Java update, a PC reboot solves the issue.
- On small-screen Epson devices, some buttons do not display the usual graphic icon due to limitations. These are the left-side buttons of the navigation form for Documentum and OpenText Content Server connectors, and the Page per Sheet button of the Page Layout dialog for the Scan to Printer connector. When using the hard keyboard, you may encounter issues accessing the calendar fields. To properly access calendar-type fields, press `F2` or `CTRL+F`.
- If you have multiple ShareScan Manager PCs in your deployment, it is recommended that you always use the same instance of the Administration Console to add, modify or remove connector profiles regardless of whether you are working in a cluster environment or not.

Technical support

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

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

- eCopy system details:
  - ShareScan version number
  - Service Pack number (if applicable)
  - Product key and serial number
  - Approximate daily scanning load (pages/day)
  - Backend versions for all used connectors (for example, Exchange, Lotus Notes, or SharePoint)

- System specifications:
  - Server OS
  - Machine types
  - Jar versions
  - NIC speed settings
  - IP Addresses
- The exact workflow performed when the issue happens
- Does it happen to all users or just specific user accounts? (if specific only, please specify in details)
- A detailed description of the workflow which helps reproducing the issue
- The following files:
  - `msinfo32.nfo`
  - license dump (for license-related issues)
  - Logs from the ShareScan Troubleshooter Tool
  - Verbose trace file for the workflow
  - Client logs
  - If possible, the Wireshark logs

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

Troubleshooting tips

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

- devices cannot be added in the Administration Console after upgrading to eCopy ShareScan 6.2
- Administration Console does not work with devices added before the upgrade to 6.2
- Administration Console simulator does not work

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

- Ensure that there is no Apache Tomcat on the PC you want to install ShareScan on.
- Ensure that no ports used by ShareScan listed in the *Installation Guide* are used by other web services, as that may cause connectivity issues.
- Deploying the `RightFax FaxUtil` on the same machine on which ShareScan is running may cause issues, therefore it is not advised.
- If the Apache Tomcat component does not start after a Java update, a PC reboot solves the issue.
- Restoring database backups created via the ShareScan Troubleshooter is not possible via the ShareScan Administration Console. Use the relevant scripts for restoring such databases.

- 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 the web interface:
  - Browse to `http://<device IP>`
  - Navigate to Network or Network Security tab
  - Check the following network protocol pages: TCP/IP, Proxy Server, Microsoft networking, SMTP Server, LDP, SIP, LDAP, POP3.

  on the device UI:
  - Press the Login button on the device, and provide the administrator credentials as needed.
  - Press the Settings button on the touch screen.
  - Navigate to **General Settings** > **Network Settings**
  - Check each specific network setting, disable all unused protocols and use IP addresses where possible.
- When upgrading an existing previous version installation that has CAC configured, you must disable and re-enable CAC via the Administration Console after the upgrade process to ShareScan 6.2 has finished.
- If you experience an infinite rebooting loop on your target machine, look for and delete the following registry keys:
  - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager Value: PendingFileRenameOperations`
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update Value: RebootRequired`
- When you are installing ShareScan in a Windows Server 2008 R2 environment, and the process fails due to the password being too short, see How to troubleshoot ShareScan installation failure

How to troubleshoot ShareScan installation failure

When you are installing ShareScan in a Windows Server 2008 R2 environment, and the process fails due to the password being too short, do the following:

1. Download SQL Server 2012 Express from the SQL Server home page on Microsoft web page (https://www.microsoft.com/).
2. Install it, and specify mixed mode authentication (this way, both SQL server authentication and Integrated Windows Authentication are enabled), and specify an `sa` level password that complies with your password policy.
3. Install ShareScan by selecting **Custom** installation, with no SQL server installation (uncheck the **Microsoft SQL Server database engine** option), and install the ShareScan database. For more information, see section Custom Installation.
4. During the ShareScan installation process, specify the SQL Server Express you installed, and provide the `sa` account and password you selected for your SQL Server Express.
5. When the Installer wizard asks for the runtime user credentials (the ecopy user), you can provide credentials that comply with your password policy.