



Tungsten eCopy ShareScan Installation Guide

Version: 6.7.0

Date: 2024-04-24

TUNGSTEN
AUTOMATION

© 2024 Tungsten Automation. All rights reserved.

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

Table of Contents

Preface	6
Product documentation.....	6
Training.....	7
Getting help with Tungsten Automation products.....	7
Chapter 1: Pre-installation	9
Typical installation workflow.....	9
System requirements for eCopy ShareScan Manager computer.....	10
Operating systems.....	10
Database.....	10
Virtual environments.....	11
Memory configuration.....	11
Checklist for the ShareScan Manager computer.....	11
Network configuration.....	13
Ports to be left open.....	14
Support information.....	17
Supported languages.....	17
Supported devices.....	18
Supported backend services.....	18
Chapter 2: Install eCopy ShareScan	19
General procedure.....	19
Before you start.....	20
eCopy ShareScan installation scenarios.....	20
Perform a new installation.....	21
Upgrade eCopy ShareScan.....	23
Maintenance.....	26
Upgrade multiple ShareScan Managers.....	26
Custom installation scenarios.....	28
How to install all components.....	28
How to install without Microsoft SQL Server.....	29
How to install eCopy ShareScan Server and WebClient only.....	31
User rights for database creation.....	32
Administrative account with 'sysadmin' fixed server-level role (sa).....	32
Administrative account with 'dbcreator' and 'securityadmin' fixed server-level roles....	32
Administrative account ONLY with 'dbcreator' fixed server-level role.....	32

Most restrictive environment.....	32
Profile tool.....	33
How to export connector profiles.....	33
How to import connector profiles.....	33
Client-side installation.....	34
Client-side installation for Canon devices.....	34
Client-side installation for Epson devices.....	38
Client-side installation for Fujifilm devices.....	40
Client-side installation for HP devices.....	42
Client-side installation for Konica Minolta devices.....	48
Client-side installation for Olivetti devices.....	51
Client-side installation for Ricoh devices.....	53
Client-side installation for Xerox devices.....	59
Drivers for ScanStation.....	62
Device Calibration Connector.....	65
Chapter 3: eCopy connectors.....	67
Supported versions.....	68
eCopy connector for Microsoft Exchange (Mail and/or Fax).....	69
Installation prerequisites.....	69
eCopy connector for LDAP/SMTP (Mail and/or Fax).....	69
Installation prerequisites.....	69
eCopy connector for Scan to Desktop.....	70
Installation prerequisites.....	70
Inbox Root Directory.....	70
ShareScanAdmin Group.....	70
eCopy connector for Quick Connect.....	71
Installation prerequisites.....	71
eCopy connector for OpenText Fax Server (RightFax edition).....	71
Installation prerequisites.....	71
eCopy connector for Scan to Printer.....	72
Installation prerequisites.....	72
eCopy connector for Microsoft SharePoint.....	72
Installation prerequisites.....	72
eCopy connector for OpenText Documentum.....	72
Installation prerequisites.....	72
Suggestions.....	73
eCopy connector for iManage WorkSite.....	73
Installation prerequisites.....	73

Suggestions.....	73
eCopy connector for OpenText Content Server - eDOCS edition.....	73
Installation prerequisites.....	73
eCopy connector for OpenText Content Server.....	74
Installation prerequisites.....	74
Suggestion.....	75
Chapter 4: About licensing devices.....	76
How to load licenses.....	76
How to activate licenses.....	77
How to load activated licenses.....	77
How to remove licenses.....	77
How to generate a license report.....	78
Chapter 5: Post-installation.....	79
ScanStation post-installation.....	79
Configure ShareScan (examples).....	79
Configure a service - Activity Tracking example.....	80
Configure an extender - Forms Processing Extender example.....	80
Configure a Quick Connect connector profile to use Forms Processing Extender data.....	80
Test the profile configuration.....	81
Creating self-signed server certificates for Konica Minolta and Olivetti devices.....	81
Create the certificate manually.....	82
How to change the ShareScan Web client certificate to SHA1.....	83
Certificate Manager.....	85
Key-in for Ricoh devices.....	85
How to use the key-in feature.....	86
Next steps.....	86
Best practices.....	87
Technical support.....	87
Troubleshooting tips.....	88

Preface

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

This guide is intended for administrators responsible for the initial installation, configuration, and licensing of eCopy ShareScan. For information pertaining to the eCopy ShareScan pre-installation, see *Tungsten eCopy ShareScan Pre-Installation Checklist*. For configuration and Administration Console usage, see the Online Help (accessible via pressing F1 on the Administration Console).


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

Product documentation

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

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

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

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

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

Training

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

Getting help with Tungsten Automation products

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

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

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

The **Tungsten Automation Knowledge Base** provides:

- Powerful search capabilities to help you quickly locate the information you need.
Type your search terms or phrase into the **Search** box, and then click the search icon.
- Product information, configuration details and documentation, including release news.
Scroll through the **Tungsten Automation Knowledge Base** home page to locate a product family. Then click a product family name to view a list of related articles. Please note that some product families require a valid Tungsten Automation Portal login to view related articles.
- Access to the **Tungsten Automation Customer Portal** (for eligible customers).
Click the **Customer Support** link at the top of the page, and then click **Log in to the Customer Portal**.
- Access to the Tungsten Automation Partner Portal (for eligible partners).

Click the **Partner Support** link at the top of the page, and then click **Log in to the Partner Portal**.


- Access to Tungsten Automation support commitments, lifecycle policies, electronic fulfillment details, and self-service tools.

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

Chapter 1

Pre-installation

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

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

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


Typical installation workflow

Tungsten eCopy ShareScan supports three typical installation and upgrade scenarios, which are briefly outlined below. For a more detailed description, see [Install eCopy ShareScan](#).

Install Tungsten eCopy ShareScan 6.7.0 with no previous version already present

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

Upgrade from Tungsten eCopy ShareScan 5.x to 6.7.0

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

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

Upgrade from versions pre-dating 6.0

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

If you are upgrading from an eCopy ShareScan version earlier than 5.4 (5.0, 5.1 or 5.2), you first need to upgrade to 5.4. Once you have a verified working installation of eCopy ShareScan 5.4, you need to follow the upgrading from eCopy ShareScan 5.4 steps mentioned above.

Upgrade from version 6.0 or higher

1. Exit eCopy ShareScan 6.x Administration Console.
2. Ensure that the eCopy ShareScan prerequisites (listed in this chapter) are installed.
3. Run the eCopy ShareScan 6.7.0 installer.
4. After the **Welcome** screen, select **Upgrade from previous version to 6.7** or **Custom upgrade from previous version to 6.7**, and then follow the prompts to finish the upgrade.

System requirements for eCopy ShareScan Manager computer


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

- Amazon Corretto 8 Java Runtime (x86) – version 8.402.08.1
- Microsoft .NET Framework 4.8
- Microsoft Visual C++ 2019 Redistributable (x86) – version 14.29.30139.0
- Microsoft Visual C++ 2019 Redistributable (x64) – version 14.29.30139.0

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

Operating systems

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

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

Database


- Microsoft SQL Server 2016 (also Express edition) or later

Database permissions

For working with the eCopy ShareScan databases in an upgrade scenario, you must use an account that has **db_owner** Database-Level Role permissions for the eCopy ShareScan database. An account with sysadmin Server-Level Role can be used, but it is not mandatory. For database permissions required for a new installation, see the "User rights necessary for eCopy ShareScan database creation" section in your *Tungsten eCopy ShareScan Installation Guide*.

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

Virtual environments

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

- VMware ESXi 7.0 or higher
- VMware Workstation 12.x or higher
- Microsoft Hyper Visor (Hyper-V) Server 2016 or higher

Memory configuration

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


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

For more details on recommended memory configuration, see the "Sizing recommendations" chapter in the *Pre-Installation Checklist*.


Checklist for the ShareScan Manager computer




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

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

 The original version of the Apache Tomcat web service is 9.0.87, which is a 32-bit installer. Also, if you do not want to install a web client during the installation, ignore any Apache Tomcat references. If you install the web client, the simulator function of the ShareScan Administration Console defaults to using the web client for the simulator.

- ShareScan 6.x licenses are installed to a SQL Server to allow easy management of devices. The ShareScan installer can install a local copy of SQL Server 2022 Express for managing licenses in addition to storing configuration data. It can also create the appropriate database structure on an existing SQL server for consolidated key management.

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

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

Check	Description
<input type="checkbox"/>	<p>If you plan to use the Single Sign-On feature of the Session Logon service, you must ensure the following:</p> <ul style="list-style-type: none">• The ShareScan Manager computer is a member of the domain for which Session Logon is configured.• The logged-in user running and configuring the Session Logon must be an Active Directory user with the necessary rights to read properties in Active Directory (this is a default value).• This Active Directory user must have the necessary rights to read Active Directory properties (generally this is a default behavior; however, this can be modified in Active Directory).• You use the Active Directory user account to log into this domain (and not into the local system).

Network configuration

Domains and Workgroups

eCopy ShareScan can be configured to run in either domain-based networks or workgroup environments. Windows 2016 or later domain environments are supported. A domain environment is recommended.


Subnets and VLANs

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

IP Addresses

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

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


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

Gateway Address

ShareScan does not require a gateway address.

Host Name

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

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

Network Attached Storage Devices (NAS)

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

Novell


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

Local Security Policy

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

Ports to be left open

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

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

When using Canon devices

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

When using Epson devices

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

When using Fujifilm devices

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

When using HP devices

Inbound	
TCP	443, 8080, 9030, 9600, 9610, 9650
UDP	9650

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

When using Konica Minolta devices

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

When using Olivetti devices

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

When using Ricoh devices

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

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

When using ScanStation

Inbound	
TCP	2121, 9030, 9600, 9610, 9650
UDP	9650
Outbound	
TCP	9650
UDP	161 (SNMP), 8899, 9650

When using Xerox devices

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

Support information


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

Supported languages

Tungsten eCopy ShareScan supports the following languages:

- English
- Brazilian Portuguese
- Dutch

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

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

Supported devices

For the most current information on supported devices, visit the [Support Devices](#) website.

Supported backend services

For a detailed list of supported versions for specific backend connectors, see [eCopy connectors](#).

Chapter 2

Install eCopy ShareScan


This chapter contains information on the various tasks associated with installing eCopy ShareScan.

General procedure

To install, configure, and license eCopy ShareScan:

1. Install the eCopy 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.
2. Install eCopy ShareScan Client, if needed (for more information on installing the client, see the [Client-side installation](#) section of this guide).
3. Start the Administration Console.
4. Add licenses, add devices (if they do not appear automatically on the **Devices** tab), and/or set up scanners.

The Model name (in the dialog that appears as part of device addition procedure) differs from the name of the Device (displayed in the tree control on the **Device** tab). The tree control on the **Device** tab contains the network (host) name of the devices (or the IP address of the devices, if the host name cannot be resolved). This ID is used as a unique identifier for the devices in the eCopy ShareScan system. This cannot be changed in the Administration Console, only via the Device administration user interface and/or in the network DNS (Domain name server).

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

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

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

For in-depth information about configuring and managing the Services, Connectors, and Devices that eCopy ShareScan uses, see the Administration Console Help.

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

Before you start

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

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

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

i eCopy 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 eCopy ShareScan. If you have Skype installed, it can conflict with the Apache Tomcat installed by eCopy ShareScan. To avoid this issue, ensure that the **Use port 80 and 443 as alternatives for incoming connections** option is cleared in Skype.

! Ensure that the ports used for both inbound and outbound network traffic are left open. See [Ports to be left open](#).

eCopy ShareScan installation scenarios

- i**
- The eCopy ShareScan 6.7.0 installer uninstalls previous version of eCopy ShareScan . With this, any separate eCopy products (Xerox TWAIN, ScanStation, Advanced FPE) are also uninstalled to facilitate proper operation of eCopy ShareScan 6.7.0. You have to manually re-install any of these required components.
 - Before running the eCopy ShareScan installer, you must ensure that you have the latest system updates on your computer and that automatic Windows updates are turned off.
 - Installing eCopy 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 eCopy ShareScan versions, eCopy ShareScan performs a complete installation where you can only customize the installation location on the **Destination Folder** screen and database access and service account credentials on the **Service Credentials** screen. When upgrading in a multi-manager deployment, we recommend that you upgrade the individual eCopy ShareScan managers one by one.

If you plan to deploy eCopy ShareScan in a high availability cluster with multiple eCopy ShareScan server nodes, follow the instructions in the *eCopy ShareScan High Availability and Load Balancing Deployment Guide*. We recommend that you set up the individual eCopy 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*.

i Do not use square brackets ([]) in the following values since they are not handled correctly and are removed. If you need to use these characters in the password, consider changing them temporarily during the installation.

- User identifiers
- Passwords
- Database name fields

Follow these two basic scenarios when installing eCopy ShareScan:

- [Perform a new installation](#)
- [Upgrade eCopy ShareScan](#)

Perform a new installation

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

- [Complete installation](#)
- [Custom installation](#)

Complete installation

This scenario is to perform a complete installation on a clean system when all the necessary components including SQL Server are installed by the ShareScan installer itself.

i If an SQL Server 2022 is already installed on the clean system before ShareScan installation, this installation scenario cannot be selected.


1. After you download and extract the eCopy ShareScan installer package to your computer, browse to the folder where the `ShareScan6.7.exe` file is located.
2. Run `ShareScan6.7.exe` installer. The **Choose Setup Language** screen appears. Select a preferred language (English by default) from the list and click **Next**.
3. When the **Welcome** screen appears, click **Next**.
The installer displays the **System Check** screen.
4. If prompted, select the preferred options from the lists, and click **Next**.

i This screen displays warnings on any possible issues that might have an impact on the proper operation of eCopy 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. When the **Enter Product License Key** screen appears, provide your license key (22 characters with dashes). Click **Next**.
6. The End-User License Agreement (EULA) is displayed on the **License Agreement** screen. Accept the EULA and click **Next**.

7. The **Setup Type** screen appears. Select **Complete**. Automatic full installation is performed, including the following features and settings:

- **eCopy ShareScan Server** is installed.
- **Microsoft SQL Server** is installed.
 - SQL Server 2022 Express is installed.

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


- **eCopy ShareScan configuration database** is created on the installed SQL Server.
- **eCopy ShareScan WebClient** is installed (including the Apache Tomcat server).
- Default eCopy credentials (username/password) is used for database access, with SQL server authentication.
- `C:\Program Files (x86)\Tungsten\ShareScan6.7\Server` is the default installation path.

8. The **Installation Configuration Summary** screen appears. Review the information and if you are satisfied with the configuration, click **Install**; otherwise, click **Back**.

9. Click **Finish** when the **Install Shield Wizard Completed** screen appears.

Custom installation

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

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

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

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

- **eCopy ShareScan WebClient** (selected by default): Select this component if you plan to use scanner devices with a web browser enabled user interface.
4. The **Destination Folder** screen appears. Click the **Change** button to modify the default destination folder for the ShareScan server, Tungsten OmniPage Capture SDK, the Apache Tomcat web server installation (the Apache Tomcat web server is required for the eCopy ShareScan Web client) or Amazon Corretto 8 runtime. Click **Next**.
 5. Specify service credentials on the **Service Credentials** screen. Use predefined local accounts, or specify custom service accounts for the ShareScan Manager and ShareScan Agent services. These accounts must be different valid domain accounts (users), and the user specified for the ShareScan Agent service must be different from the user who runs the installer. Click **Next**.

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

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

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

Upgrade eCopy ShareScan

When the eCopy ShareScan installer is run on a computer where a previous version is installed, it offers two upgrade options.



- If **custom service credentials** is set for the Agent and Manager service, the eCopy ShareScan 6.7.0 installer prompts for the Agent service user password and Manager service user password, and the installer must run with a different user as the one configured for Agent service. Otherwise, the system after the upgrade will not operate properly.
- Upgrading a previous eCopy ShareScan configured with LocalDB SQL Server is not supported when an SQL Server 2022 is also already installed on the target machine.
- Using the eCopy ShareScan 6.7.0 server with devices that have v5.x JAR clients installed on them is not supported.

Upgrade from a previous version



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

1. After you download and extract the eCopy ShareScan installer package to your computer, browse to the folder where the `ShareScan6.7.exe` file is located.
2. Run `ShareScan6.7.exe`. The **Choose setup language screen** appears. Select a preferred language (English by default) from the list and click **Next**.
3. The **Welcome** screen appears. Click **Next**.
4. The End-User License Agreement (EULA) is displayed on the **License Agreement** screen. Accept the EULA and click **Next**.
5. The **Setup Type** screen appears. Select **Upgrade from previous version to 6.7:**



This option removes the older eCopy ShareScan version, and then proceeds to install the new version while preserving configuration data.

- The **eCopy ShareScan Server** is installed.
 - Existing **eCopy ShareScan configuration database** is updated to the 6.7.0 schema.
 - **eCopy ShareScan WebClient** is installed (including the Apache Tomcat server).
6. If the installer is not able to use the default 'sa' credentials and the current Windows user does not have the necessary rights granted for database access, then the **Administrative Credentials for Database Creation** screen appears, where the proper (administrator level) credentials must be provided.
 7. The **Installation Summary** screen appears. Review the information and if you are satisfied with the configuration, click **Install**. Otherwise, click **Back**.
 8. Click **Finish** when the **Install Shield Wizard Completed** screen appears.


Custom upgrade from a previous version




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

1. After you download and extract the eCopy ShareScan installer package to your computer, browse to the folder where the `ShareScan6.7.exe` file is located.


2. Run `ShareScan6.7.exe`. The **Choose setup language screen** appears. Select a preferred language (English by default) from the list and click **Next**.
3. The **Welcome** screen appears. Click **Next**.
4. The End-User License Agreement (EULA) is displayed on the **License Agreement** screen. Accept the EULA and click **Next**.
5. The **Setup Type** screen appears. Select **Custom Upgrade from previous version to 6.7:**

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

- The **eCopy ShareScan Server** is installed.
 - Existing **eCopy ShareScan configuration database** is updated to the 6.7.0 schema.
 - **eCopy ShareScan WebClient** is installed (including the Apache Tomcat server).
6. The **Destination Folder** screen appears. Click the **Change** button to modify the default destination folder for the ShareScan server, Tungsten OmniPage Capture SDK, the Apache Tomcat web server installation (the Apache Tomcat web server is required for ShareScan Web client) or Amazon Corretto 8 runtime. Click **Next**.
 7. Specify service credentials on the **Service Credentials** screen. Use predefined local accounts, or specify custom service accounts for the ShareScan Manager and ShareScan Agent services. Click **Next**.

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

8. At this point, the user is presented with the following options:
 - If the installer is not able to use the default 'sa' credentials and the current Windows user does not have the necessary rights granted for database access, then the **Administrative Credentials for Database Creation** screen appears, where the proper (administrator level) credentials must be provided.
 - **The Database Server and Runtime Account Information** screen: if the user selected custom service accounts, as in this case the user is necessary to specify what authentication method/account should be used for database connection.



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


9. The **Installation Configuration Summary** screen appears. 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.

Maintenance

If you re-launch the ShareScan installer after successful installation of ShareScan 6.7.0, the **Program Maintenance** screen appears after you select a preferred language from the list on the **Choose setup language** screen and click **Next**. The following option is available:

Remove

- Removes all 6.7.0 features (Server, WebClient). The so-called dependency packages (SQL Server, Apache Tomcat, and so forth) can be removed from the **Programs/Features** manager of Windows.


 If you install ShareScan 6.7.0 over an existing ShareScan version, removing version 6.7.0 does not bring back the previous ShareScan version. Removing the WebClient feature of ShareScan also removes the Apache Tomcat server.

Upgrade multiple ShareScan Managers

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

- Integrated Windows Authentication on all the Managers you connect to the same 6.7 database
- The same Windows service accounts on all the managers you upgrade

After you upgrade the first Manager to 6.7.0 with Integrated Windows Authentication, you cannot use the default service accounts for the Agent and Manager services when you upgrade the second one. However, you do have to specify the same Windows users that are specified for the first Manager.

- 
- While upgrading multiple Managers in any environment (NLB or standard), all Managers should be stopped before you upgrade the first Manager. Database modification is also done during the upgrade. When complete, the rest of the Managers can be started and upgraded one by one.
 - Performing a multi-manager setup (when more than one ShareScan Manager connect to the same database catalog) and then upgrading from version 6.x is similar to the Custom upgrade scenario.

1. If you have physical ShareScan installation media, insert it in the optical drive of your computer and browse to the folder where the `ShareScan6.7.exe` file is located. If you have a digital copy of the eCopy ShareScan installer, you can find the `ShareScan6.7.exe` file in the root folder.
2. Run `ShareScan6.7.exe`.
The **Choose setup language screen** appears.
3. Select a preferred language (English by default) from the list and click **Next**.
4. The **Welcome** screen appears. Click **Next**.

5. The **Setup Type** screen appears. Select **Custom upgrade from previous version to 6.7**: the installer performs a complete installation, preserving configuration data:
 - The **eCopy ShareScan Server** is installed.
 - The existing **eCopy ShareScan configuration database** is updated to the 6.7.0 schema, or a clone (copy) of the currently used ShareScan database is updated to the 6.7.0 schema and put in use for the upgraded installation (the actual behavior is specified on the screen detailed in step 8 below).
 - **ShareScan WebClient** is installed (including the Apache Tomcat server).
6. When the **Destination Folder** screen appears, click the **Change** button to modify the default destination folder for the ShareScan server, the Apache Tomcat web server installation (the Apache Tomcat web server is required for ShareScan Web client) or Amazon Corretto 8 runtime. Click **Next**.
7. Specify service credentials on the **Service Credentials** screen. Use predefined local accounts, or specify custom service accounts for the ShareScan Manager and ShareScan Agent services. Click **Next**.

The **Administrative Credentials for Database Creation** screen appears, if the default 'sa' credentials do not work, or the actual Windows user running the installer does not have rights to update the database. Otherwise, this screen is not displayed.
8. When the **Database Catalog Name** screen appears, you have three basic options:
 - a. If you select **Use current catalog for database upgrade** in the first manager upgrade installation sequence, the procedure is identical with the single manager [Custom upgrade from a previous version](#) installation scenario. In this case, the name of the database catalog remains the same (eCopyShareScan), but its structure changes. Therefore, if there are multiple Managers, only the first Manager currently upgraded will be able to operate correctly, while the other Managers will not, until they are upgraded as well. As a consequence, selecting this option is recommended if all Managers connecting to the same database are stopped during the entire upgrade process (for all Managers).

i This option is also useful in scenarios when your database administrator (DBA) does not provide an administrative account eligible for backup/restore operations. In such a case, the DBA must create a copy of the eCopy ShareScan database catalog (with a different name) on the same database server (and on the same instance). Then you need to switch one of your Managers to this copied database (via the **Database configuration** option of the ShareScan Administration Console), and upgrade it by selecting this option. Further, Managers can then be upgraded by selecting Option c) described below.
 - b. When upgrading the first Manager, select **Copy current catalog to perform the upgrade on the following one** and specify a database name. This option makes a copy of the already existing database catalog with the outdated structure and upgrades the copy reconfiguring the Manager to use it. This way the other Managers are able to use the old catalog without any hindrance. To perform this task successfully, the user must have the db_backupoperator database-level role and DBCREATOR server level permission since they allow backup and restore operations.
 - c. When upgrading the second and all further Managers, select **Use a different existing ShareScan catalog** and select the newly created/updated database, already upgraded to 6.7 level. You have to select the database catalog name provided during the upgrade the first Manager.

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

Click **Next**.

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

Custom installation scenarios

- [How to install all components](#)
- [How to install without Microsoft SQL Server](#)
- [How to install the eCopy ShareScan Server and WebClient only](#)

How to install all components

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

This custom setup scenario installs all four components:

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

i When you provide valid non-default accounts for the manager and the agent and then click **Grant** after the installer detects that some local privileges are not granted to the service accounts, the installer tries to grant the missing privileges. If this cannot be successfully performed, the installer still detects that the privileges are missing and does not continue the installation. The user must exit from the installer, resolve the issue, and either grant the missing privileges manually or eliminate the blocking factor to allow the installer to grant them during the next run. Then the installer must be re-run.

4. Specify the password option for the system administrator (sa) of the SQL Server to be installed on the **Local Database Server** screen. Select **Use default password specified by ShareScan** or override the default password of the SQL Server system administrator (the sa password) by selecting **Specify a custom password**. If you do so, you must provide a password that complies with the password policy in effect. Click **Next**.
5. The **Installation Summary** screen appears. 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.

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

How to install without Microsoft SQL Server

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

This custom setup scenario installs the following three components:

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

services. These accounts must be valid domain accounts (users), and the user specified for the ShareScan Agent service must be different from the user who runs the installer. Click **Next**.

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

4. The **Administrative Credentials for Database Creation** screen appears. On this screen, the hostname or IP (and optionally, the instance name) of the SQL Server must be specified. The credentials entered on this screen are required while installing or upgrading the database. The information is not stored; it is only required during the installation or upgrade process for the database connection. The following options are displayed:

- SQL Server host/instance name input box — the host name and, optionally the instance name of the SQL Server to use must be specified, such as `SQLSRV-01, CORPSQL1\SHARESCAN, 10.140.1.23\SSCAN1`.

You need to select one of the following options:

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

Click **Next**.

5. The **Database Catalog Name** screen appears. Specify the ShareScan database name here or leave the default name. Click **Next**.
6. The **Database Server and Runtime Account Information** screen appears. You can specify a runtime account for the configuration database.

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

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

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

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

i 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 appears. Click **Install**.
8. Click **Finish** when the **Install Shield Wizard Completed** screen appears.

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

How to install eCopy ShareScan Server and WebClient only

This custom setup scenario installs the following two components:

- eCopy ShareScan Server
- eCopy ShareScan WebClient

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

1. Once you clear the **Microsoft SQL Server** and **eCopy ShareScan configuration database** components and/or optionally clear the **eCopy ShareScan WebClient** component on the **Custom setup** screen, click **Next**.
2. The **Destination Folder** screen appears. Click **Change** to modify the default destination folder for the ShareScan server or the Apache Tomcat web server installation (the Apache Tomcat web server is required for ShareScan WebClient). Click **Next**.
3. Specify service credentials on the **Service Credentials** screen. Use predefined local accounts, or specify custom service accounts for the ShareScan Manager and ShareScan Agent services. These accounts must be valid domain accounts (users), and the user specified for the ShareScan Agent service must be different from the user who runs the installer. Click **Next**.
4. The **Database Catalog Name** screen appears. On this screen, you must specify the hostname or IP and optionally, the instance name of the Microsoft SQL Server where the existing 6.7.0 ShareScan database is hosted. You must also specify the existing database name. Click **Next**.
5. The **Database Server and Runtime Account Information** screen appears. You need to provide the runtime account information for the configuration database. Click **Next**.

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

6. The **Installation Summary** screen appears. 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.

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

You are now ready to configure a connector profile.

User rights for database creation

This topic lists 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)

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

Administrative account with 'dbcreator' and 'securityadmin' fixed server-level roles

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

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

Administrative account ONLY with 'dbcreator' fixed server-level role

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

This administrative user will be a db_owner on the created 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 select any name.

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

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

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

Profile tool

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

Like connector profiles, also newly imported watchers automatically overwrite watchers with the same name already existing on the target machine.

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

To perform profile export, see [How to export connector profiles](#).

To perform profile import, see [How to import connector profiles](#).

How to export connector profiles

To perform an export, do as follows:

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

How to import connector profiles

To perform an import, do as follows:

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

3. Double-click the file to start the import process.

Client-side installation

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

Client-side installation for Canon devices

To learn about how to install the embedded client for Canon devices, see the following links.


- [Install the JAR file on a MEAP-enabled device](#)
- [Add devices with installed eCopy ShareScan client](#)
- [Batch add devices](#)

Install the JAR file on a MEAP-enabled device

This section contains information on installing the Canon Embedded (Canon MEAP) client.

The JAR file contains the ShareScan Client. Before you can acquire Canon MEAP-enabled devices for use, you must install the JAR file and the license file on the devices. Make sure you install the appropriate JAR file in accordance with your device's regional requirements. If you are unsure about the ShareScan JAR file, contact your Canon sales representative.

Before installing the JAR file, make sure that you turn off the Department ID, the Single Sign-On (SSO) ID, or the Simple Device Login (SDL), if they are enabled. After installing the JAR file, you can turn on the IDs again.

 The 5.x JAR clients are not supported.

In case of ShareScan clients released under Canon A1 license, the installation media contains a LAN file (LAN.txt) next to the JAR file. The LAN file contains a License Access Number for downloading the license file for ShareScan client from the Canon License Management System.

To use an earlier versions of the ShareScan client, their installation media contains the license file (.lic) itself instead of a LAN file.

To get an A1 license for the ShareScan client, do the following.

1. Open the LAN file (LAN.txt) that was included with the application JAR file and record the License Access Number (LAN) from it.
2. Record and add the serial number for each Canon MFP you want to license in a comma separated (CSV) file.
3. Open a web browser and navigate to the **Canon License Management System** (<http://www.canon.com/meap>).
4. Enter the **License Access Number** and click **Next**.
5. Verify the information and click **Apply to Issue a License**.

6. On the **Serial Number Registration** page:
 - **Enter Device Serial Number** to manually enter the serial number for each device up to 10 devices, or
 - **Batch Register Several Device Serial Numbers Using a File** to use the CSV file when registering more than 10 devices.
Up to 1000 devices can be registered at once with the CSV file.
When using batch registration, click **Choose File** to navigate to the CSV file on your local machine.
7. Click **Next** and follow the rest of the steps until a license (.lic) file is downloaded.

Install a JAR file

Use this procedure to install a JAR file.

1. Open a Web browser and point to the device's Web server. The server URL is typically `http://<device-IP-address>:8000/sms`.
2. Enter the device's login password, which is typically **MeapSmsLogin**, and then click **Log In**.
3. In the **Service Management Service** window, click **Install**.
4. In the **Application File** field, enter the location of the JAR file on the installation media.
5. In the **License File** field, enter the location of the license file (*.lic) which was downloaded from the **Canon License Management System**, or which is next to the JAR file on the installation media, in case of an earlier version of JAR.
6. On the confirmation screen, click **OK**.
7. Review the application information and then click **OK** to install the JAR file.
8. In the **Service Management Service** window, click **Application List**, select **ShareScan**, and then click **Start**.
9. Click **Log Out**.

Device setup for MEAP-enabled devices

These instructions describe how to obtain or configure the network settings on a MEAP-enabled device.

1. On the device keypad, press **Additional Functions**. (For iR-Advance devices, press **Settings/Registration**.)
2. Press **System Settings**. (For iR-Advance devices, press **Preferences**.)
3. Press **Network Settings**. (For iR-Advance devices, press **Network**.)
The **Network Settings** window appears.
4. Press **TCP/IP Settings**.
The **TCP/IP Settings** window appears.
5. Press **IP Address Settings**. (For iR-Advance devices, press **IPv4 Settings**.)
The **IP Address Settings** window appears.
6. Verify the following settings and then press **OK**.
 - **DHCP**: Not recommended in a domain-based network environment. Do not enable in a workgroup environment.
 - **IP Address**: Use of static IP addresses is highly recommended.

- **Subnet Mask:** Set according to site guidelines. This ShareScan version does not use this setting.
 - **Gateway Address:** Should be blank, unless another MEAP application requires a specific gateway address.
7. In the **TCP/IP Settings** window, press **DNS Server Settings**.
The **DNS Server Settings** window appears.
 8. Verify the following settings and then press **OK**
 - **Primary Server (DNS):** Not required in a domain-based network environment. However, if you do not specify a DNS server, the ShareScan Manager computer must have a static IP address. In a workgroup environment, this field must be blank.
 - **Secondary Server (DNS):** Leave this field blank.
 - **Host Name:** Enter a unique name for the device, up to 60 characters.
 - **Domain Name:** Enter a domain name, if applicable.
 - **Dynamic DNS Update:** Should be set to **On**.
 9. Press **Done** until the main screen appears.
 10. Power cycle the device so that the new settings will take effect.

Authentication information settings

Optimal performance of the Canon client is not guaranteed unless the following authentication information settings are specified, since otherwise it is unable to perform certain privileged operations (querying device capability, etc).

1. Install the ShareScan MEAP client. Before starting it, click the application name.
2. Click the **Authentication Information Settings** button.
3. Enter a valid Department ID and PIN. (Depending on the actual login application, you may be required to enter authentication information other than the Department ID and PIN. For example, SSO-H requires a valid user name, domain and password instead of Department ID and PIN).
4. Click the **Update** button.
5. Start the ShareScan MEAP client.

Troubleshooting

1. Department ID/PIN is not set. See above in **Step 3**.
2. Department ID/PIN was set before enabling the Login app (and then reboot after this) .
Normally, the order of the steps should be the following:
 - a. Enable the Login app.
 - b. Reboot the device.
 - c. Set the Department ID/PIN.

To check if this is/was the case, do the following:

- a. Click **MEAP Application Management**.
- b. Click **ShareScan**.
- c. Click the **Authentication Information Settings** button.

The "Authentication information is set" message is displayed.

- d. If the message in **Step 4** is not displayed:
 1. Set the message.
 2. Reboot the device.
3. Department ID/PIN was set after enabling the Login app, but there was no reboot between these two steps.

Make sure that you rebooted the device after enabling the Login app, but before setting the Department ID/PIN.
4. Department ID/PIN are invalid:

The system accepts an invalid Department ID/PIN combination as well that might cause issues later.

To check and confirm if Department ID/PIN are valid:

 - a. Go to the Remote UI web app of the device `http://<deviceip>:8000/`
 - b. Click the **Settings/Registration** button on the right side of the page.
 - c. Click the **User Management** link.
 - d. Click the **Department ID Management** link.

Add devices with installed eCopy ShareScan client

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

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

Batch add devices


To add multiple Canon devices in a batch, follow the instructions below:

1. Start ShareScan Administration Console.
2. Click **Add Device**, or select **Add device** from the context menu (by right-clicking in the **Device Configuration** window).
3. Select **Import** from the **Discovery** list; a standard **Open file** dialog box appears. Select a file that describes the devices to add. The file must be a `.csv` file, containing data in the following format:


`IP/host, Canon, model, password(string), Secure Image Uploading`

Example: `10.140.202.99,Canon,300,1111,true`

- `IP/host`: device IP address (or host name).
- `Canon`: must be Canon.
- `model` (or `*`): specific device model name (or `*` to get the model name automatically from the device).
- `password(string)`: secure device registration password.
- `Secure Image Uploading`: true or false (enable or disable secure image uploading).

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

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

 For instructions about removing devices, see the ShareScan Help.

Client-side installation for Epson devices

To learn about how to install the embedded client for Epson devices, see the following links.

- [Auto-registration of devices with the Unified Client](#)
- [How to add a device with the Unified Client to ShareScan Manager](#)
- [Unified Client IP address filtering](#)
- [How to configure the IP address filter](#)

Auto-registration of devices with the 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 box 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.

The 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 the Administration Console. These auto-registered devices can be moved outside this group or they can be dropped to any other device group, if necessary.

The list of devices in the Administration Console is updated only upon successful registration of the device with the Unified Client. To know how a device is added in the Administration Console, see [How to add a device with the Unified Client 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 or ranges through which the administrator can allow or 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 a device with the Unified Client to ShareScan Manager

1. Close the Administration Console on the 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 list 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

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

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

Client-side installation for Fujifilm devices

To learn about how to install the embedded client for Fujifilm devices, see the following links.

- [Configuring the Fujifilm device](#)
- [Add devices with installed eCopy ShareScan client](#)
- [Batch add devices](#)

Configuring the Fujifilm device

eCopy ShareScan supports JavaScript-capable Fujifilm devices.


Before you can use eCopy ShareScan with Fujifilm devices, you must install and/or enable the following components.

HTTPS

1. Go to the proper page of Web Administration application for the device (usually **Network > Protocols > HTTP**).
2. Configure the proper port for HTTPS (**Port Number (HTTPS)**).
3. Go to the proper page of Web Administration application for the device to configure remote server certificate verification (usually **Properties > Security > SSL/TSL Settings**).
4. Disable the **Verify Remote Server Certificate** option.

HTTPS (in case of older devices)

1. Go to the proper page of Web Administration application for the device (usually **Properties > Security > SSL/TSL Settings**).
2. Enable the **HTTP - SSL/TLS Communication** option.
3. Disable the **Verify Remote Server Certificate** option.

 You may need to create a certificate and install it onto the device before you can turn on Secure HTTP.

Simple Network Management Protocol (SNMP)

1. Go to the proper page of the Web Administration application for the device.
2. Enable SNMP v1/v2c protocols.

Default MFP UI language

1. At the device, log in as the administrator by pressing the **Log in/out** button and entering administrator credentials (default is: 11111).
2. Press the **Settings (cogwheel)** button on the device touch screen.
3. Select **Language** and make sure it is set to English.

Default MFP UI language (on older devices)

1. At the device, log in as the administrator by pressing the **Log in/out** button and entering administrator credentials (default is: 11111).
2. Press the **Services Home** button and go to **Tools > System Settings > Common Service Settings** and press **Screen/Button Settings**.
3. Check **10. Default Language** and make sure it is set to English.

Add devices with installed eCopy ShareScan client

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

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

Batch add devices

To add multiple Fujifilm devices in a batch, use the following procedure.


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

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


```
IP/host, vendor, model, username(string), password(string),  
SNMPGet(string), HTTPS(bool), AsyncBW(bool)
```

Example: 10.140.202.70, Fujifilm, C5570, admin, 11111, public, false, false

- IP/host: device IP address (or host name)
- vendor : must be Fujifilm or Fuji Xerox (in case of older devices).
- model: specific device model name (or * to get the model name automatically from the device).
- username(string): device administrator username used for device registration
- password(string): device administrator password used for device registration
- SNMPGet(string): SNMP get community name (public by default; if otherwise specified on the device web administration page, the same must be included here)
- HTTPS(bool): true or false (enable or disable secure communication and file transfer for the device)
- AsyncBW(bool): true or false (asynchronous scanning in B&W mode; for optimal performance, true is recommended)

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

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

 For instructions about removing devices, see the ShareScan Help.

Client-side installation for HP devices

To learn about how to install the embedded client for HP devices, see the following links.

- [Configure the HP Embedded client](#)
- [Add devices with installed eCopy ShareScan client](#)
- [Batch add devices](#)
- [Configure the HP S900 series client](#)

Configure the HP Embedded client

eCopy ShareScan supports OXPd 1.6-capable HP devices. For a list of supported devices, see the Supported Device lists. Before you can use eCopy ShareScan with HP devices, you must install and/or enable the following components:

- OXPd 1.6
 - Update device firmware to support OXPd 1.6, if necessary.
 - Enable OXPd 1.6 if needed.
 - Configure Web Proxy settings (used by OXPd 1.6 for http/s communications where the device is the client) and the eCopy ShareScan server.
 - Configure the embedded web browser (timeouts and trusted sites list).
 - Manage certificates in the OXPd 1.6 CA certificate store (used by OXPd 1.6 for https communications where the device is the client).
 - Due to the number of steps, it is recommended that you use HP Web Jetadmin when you must configure several devices at once.

You may use HP Web Jetadmin or the device Web Administration page, accessible via `http://<device-ip-address>/` for configuring the device.

The HP Embedded client also provides a switch via the Administration Console, which allows you to toggle between these settings:

- Use the native software keyboard/physical keyboard of the MFP
- Use the standard eCopy soft keyboard

It is recommended that you use background processing (enabled by default for all connector profiles) in all scenarios. Should you encounter a situation where online processing better serves your interests, it is recommended that you raise the **Device Inactivity Timeout** value to 300 secs. To do this, select the **Administration** option on the device, then choose **Display Settings** and **Inactivity Timeout**. Touch the textbox and enter 300 (secs) (5 minutes) as the **Inactivity timeout** value.

Network configuration

Make sure you have the IP address of the device so that you can access the device Web Administration page.

1. Open a Web browser and enter `http://<MFP IP address>` in the **Address** field.
2. Log in with your Admin credentials when prompted.
3. Go to **Networking > Network Identification** and configure the device correctly so that the eCopy ShareScan Manager's host name can be resolved.

SNMP configuration

To enable the **Device discovery** function in the Administration Console, the device must have SNMPv2 read access, and a Get Community Name. Set these in the following ways:

1. Go to **Networking > Mgmt.Protocols > SNMP**. Click **Enable SNMPv1/v2 read-write access**. Enter the community name in the **Set Community Name** field.

i You may disable the write access. eCopy ShareScan will need to read device properties. After setting up and installing the eCopy ShareScan application on the device, you may restore the SNMP settings. SNMP is used only during the initial eCopy ShareScan setup

2. Go to **Networking > Mgmt.Protocols > Other** . Select **Multicast IPv4** under **Enable Device Discovery** category.

Add devices with installed eCopy ShareScan client

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

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

Batch add devices

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


1. Start eCopy ShareScan Administration Console.
2. Click **Add Device**, or select **Add device** from the context menu (by right-clicking in the **Device Configuration** window).
3. Select **Import** from the **Discovery** list; a standard **Open file** dialog box appears and you need to select a file that describes the devices to add. The file must be a **.csv** file, containing data in the following format:

```
IP/host, HP, model, username(string), password(string), SNMPGet(string),  
HTTPS(bool), AsyncBW(bool)
```

Example: 10.140.202.70, HP, M4555, admin, 1111, public, false, false

- IP/host: device IP address(or host name).
- HP: must be HP.

- `model`: specific device model name(or * to get the model name automatically from the device).
- `username(string)`: device administrator username used for device registration.
- `password(string)`: device administrator username used for device registration.
- `SNMPGet(string)`: SNMP get community name (public by default; if otherwise specified on the device web administration page, the same must be included here).
- `HTTPS(bool)`: true or false (enable or disable secure communication and file transfer for the device).
- `AsyncBW(bool)`: true or false (asynchronous scanning in B&W mode; for optimal performance, true is recommended).

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

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

 For instructions about removing devices, see the eCopy ShareScan Help.

Configure the HP S900 series client

eCopy ShareScan supports MFPs in the HP S900 series. For a list of supported models, see the Supported Device lists.

The HP S900 series client also provides a switch via the Administration Console, which allows you to toggle between these settings:

- Use the native software keyboard/physical keyboard of the MFP
- Use the standard eCopy soft keyboard

It is recommended that you use background processing (enabled by default for all connector profiles) in all scenarios. Should you encounter a situation where online processing better serves your interests, it is recommended that you raise the **Automatic Logout Setting** value to **240** seconds. To do this, go to the Web administration page of the device, log in as administrator and then go to **User Control > Default Settings**. Select the check box next to **Automatic Logout Setting** and choose **240** from the list.

The Auto Clear function can also interfere with job processing. If the device is not used for the duration of time set here, the auto clear function will clear any settings that have been selected and return the screen to the base screen of copy mode or the job status screen as well as log the user out.

If you are the administrator, change the time setting of **Auto Clear** or disable it in **Auto Clear Setting**. Go to **System Settings > Operation Settings > Auto Clear Setting**. Select the check

box next to **Cancel timer** to disable it, or raise its value to **240** seconds, as in the case of **Automatic Logout Setting**.

Network configuration

Make sure you have the IP address of the device so that you can access the device Web Administration page.

1. Open a Web browser and enter `http://<MFP IP address>` in the **Address** field.
2. Log in with your Administration credentials when prompted.
3. Go to **Network Settings > General Settings** and configure the device correctly so that the eCopy ShareScan Manager's host name can be resolved.

SNMP configuration

To enable the Device discovery function in the Administration Console, the device must have SNMPv1 read access, and a **Get Community Name**. Set these in the following ways:

- Go to **Network Settings > Services Settings > SNMP**. To enable device discovery, set **SNMP v1 Settings** to **Enabled** and Read-write access for Access Method; do not forget to set the community name.

i HP S900 Series devices (for example, HP Color MFP S962dn) have a fixed value (mfpdirect) for **Context Name** parameter in SNMP v3 settings. If SNMP v3 is configured on HP S900 devices, then eCopy ShareScan can perform SNMP v3 discovery only if the **Context Name** parameter is set to empty in eCopy ShareScan SNMP v3 parameter set.

SSL settings

On the device web administration page, go to **Security Settings > SSL Settings** and ensure that **Redirect HTTP to HTTPS** in **Device Web Page Access** is cleared.

Add devices

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

1. Start eCopy ShareScan Administration Console
2. Click **Add Device** on the toolbar. You can also select **Devices** on the **Welcome** page and then right-click the **Device Configuration** window and select **Add Device**. The **Add Devices** window opens.
3. If your device does not appear in the list, select the instead of the **SNMP** option from the **Discovery** list. If the auto discovery does not succeed, use TCP/IP to add it manually.
4. Select the device you want to add.
5. Click **OK**. The device registration dialog opens.
6. Enter the device administrator credentials and specify **Device Settings**.
7. Click **Register**.
8. When the system prompts you to confirm the device that you want to add to the device list, click **OK**.

Troubleshooting tip: If your devices cannot be discovered and are not displayed in the list on the **Add device** dialog box with any of the protocols, then make sure that:

- The device is up and running.
- It is connected to the network (use the `ping >IP-address>` command in a command window).
- The required ports are open on a firewalls/routers.

i The automatic device discovery is supported via and SNMP. If the auto discovery does not succeed, use TCP/IP to add the device manually.

Batch add devices

If you want to add multiple HP S900 Series devices in a batch, follow the instructions below:

1. Start eCopy ShareScan Administration Console.
2. Click **Add Device**, or select **Add device** from the context menu (by right-clicking in the **Device Configuration** window).
3. Select **Import** from the **Discovery** list; a standard **Open file** dialog box appears and you need to select a file that describes the devices to add. The file must be a `.csv` file, containing data in the following format:

```
IP/host, HPS900, model, registrationmode(A|S), username(string),  
password(string), SNMPGet (string), HTTPSforUI(bool),  
HTTPSforFileTransfer(bool)
```

Example:10.140.202.142, HPS900, *, Administrator, Administrator, admin,
public, false, false

- `IP/host`: device IP address(or host name).
- `HPS900`: must be HPS900.
- `model`: specific device model name(or * to get the model name automatically from the device).
- `username(string)` device administrator username used for device registration.
- `password(string)` : device administrator password used for device registration.
- `SNMPGet(string)` : SNMP get community name (public by default; if otherwise specified on the device web administration page, the same must be included here).
- `HTTPSforUI(bool)` true or false (enable or disable secure communication for the device).
- `HTTPSforFileTransfer(bool)` true or false (enable or disable secure file transfer for the device).

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

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

 For instructions about removing devices, see the eCopy ShareScan Help.

Device User Authentication


Depending on the **User Authentication** settings on the MFP, device registration in the Administration Console (see below) requires different data.

On the device web administration page, go to **User Control > Default Settings** and check **User Authentication** settings:

- If set to **Disable in Administrator registration mode**, the **User Name** string is not validated, only the **Password**.
- If set to **Enable**, both the **User Name** and the **Password** are validated.

To check the administrator user name on the device, go to the device Home screen, press the **Select from List** button then press the **left** pointing arrow in the top right hand corner of the screen and choose **Admin Login**. The administrator name is displayed in the **Login Name** field.

By default, using the Administrator mode for device registration is sufficient. In certain cases (for example, when Equitrac is installed on the device), Service mode is required for successful device registration.

 To get the user credential information from the user authenticating via Session Logon service, the HPS900 devices must meet the following requirements:

- OSA version: 3.0 or later
- extension kit: MX-AMX2

Client-side installation for Konica Minolta devices

To learn about how to install the embedded client for Konica Minolta devices, see the following links.

- [Configure the Konica Minolta Device](#)
- [Add devices with installed eCopy ShareScan client](#)
- [Batch add devices](#)

Configure the Konica Minolta Device

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

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

- **Cookies:** It is recommended that you configure the device to accept all cookies so that the device does not prompt users to accept cookies each time they use ShareScan. For instructions, see the device documentation.

- **Focus rectangle:** You may want to change the color of the focus rectangle. For instructions, see the device documentation.
- **Time-outs:** It is recommended that you set the following time-out settings on the device. For instructions, see the device documentation.

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

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



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

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

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

Device authentication

To configure device authentication to work with Session Logon:

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



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

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

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

5. Click **Save.**

The system saves the Session Logon settings in the ShareScan database.

Configure a card reader

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

1. Activate the card reader hardware on the device.
2. On the device, enable user authentication. Make sure that you select **ON (MFP)**.
3. In the ShareScan Administration Console, enable the **Session Logon** feature.

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

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

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

Add devices with installed eCopy ShareScan client

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

1. Start eCopy ShareScan Administration Console.
2. Click **Add Device** on the toolbar. You can also select **Devices** on the **Welcome** page and then right-click the **Device Configuration** window and select **Add Device**. The **Add Devices** window opens.
3. If your device does not appear in the list, select **SNMP** instead of the **UDP** option from the **Discovery** list. If the auto discovery does not succeed, use TCP/IP to add it manually.
4. Select the device you want to add.
5. Click **OK**. The device registration dialog box opens.

6. Observe the following:
 - If Secure Client is installed and this is the first time the device is added to eCopy ShareScan after client installation, a eCopy ShareScan-related secure connection password must be set. Provide the new password for secure connection in the **Password** and **Re-enter password** fields and select **Secure image uploading** if you want image uploading to happen in secure mode. Click **OK**.
 - If Secure Client is installed and the eCopy ShareScan-related secure connection password is already set, specify the password in the **Password** field and select **Secure image uploading** if you want image uploading to happen in secure mode. Click **OK**.
7. Choose a device model from the **A known model** list on the **Specify device model** dialog box and click **Close** to finish adding the device.

Batch add devices


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

1. Start ShareScan Administration Console.
2. Click **Add Device**, or select **Add device** from the context menu (by right-clicking in the **Device Configuration** window).
3. Select **Import** from the **Discovery** list; a standard **Open file** dialog box appears and you need to select a file that describes the devices to add. The file must be a `.csv` file, containing data in the following format:


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

```
Example: 10.140.202.70, KONICAMINOLTA, C654, 12345678
```

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

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

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

 For instructions about removing devices, see the ShareScan Help.

Client-side installation for Olivetti devices

To learn about how to install the embedded client for Olivetti devices, see the following links.

- [Configure the Olivetti device](#)
- [Add devices with installed ShareScan client](#)

- [Batch add devices](#)

Configure the Olivetti device


This section contains information on installing and configuring the Olivetti device.

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

- **Cookies:** It is recommended that you configure the device to accept all cookies so that the device does not prompt users to accept cookies each time they use ShareScan. For instructions, see the device documentation.
- **Focus rectangle:** You may want to change the color of the focus rectangle. For instructions, see the device documentation.
- **Time-outs:** It is recommended that you set the following time-out settings on the device. For instructions, see the device documentation.

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

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

 If you need complete security, it is recommended that you enable SSL (Secure Sockets Layers) on devices running ShareScan. For information about configuring SSL on the device, see the Olivetti documentation.

Add devices with installed ShareScan client

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

1. Start ShareScan Administration Console.
2. Click **Add Device** on the toolbar. You can also select **Devices** on the **Welcome** page and then right-click the **Device Configuration** window and select **Add Device**.
3. If your device does not appear in the list, select **SNMP** instead of the **UDP** option from the **Discovery** list. If the auto discovery does not succeed, use TCP/IP to add it manually.
4. Select the device you want to add.
5. Click **OK**. The **Register ShareScan** dialog box opens.
6. Enter the Administrator password for the device and then click **Register**. (For default Administrator password, contact Olivetti product support.) The system creates Apache Tomcat folders and installs the Web application on the device. Before adding an Olivetti device, consult section **Configuring the Olivetti** device. If the ShareScan client is already registered on an MFP and the SSL settings need to be changed on the device - either from Non-SSL to SSL, or from SSL to Non SSL - you need to follow these steps:
 - Remove the device from the Administration Console.
 - Change the SSL settings on the device.

- Re-add the device through the Administration Console.
7. When the system prompts you to confirm the device that you want to add to the device list, click **OK**.

If your devices cannot be discovered and are not shown in the list on the **Add device** dialog box with any of the protocols, then make sure that:

- The device is up and running.
- It is connected to the network (use the `ping <IP-address>` command in a command window).
- The required ports are open on the firewalls/routers.

i The automatic device discovery is supported via and SNMP. If the auto discovery does not succeed, use TCP/IP to add the device manually. If the device model cannot be detected due to firewall/network restriction, a pre-populated list pops up the user can select from.

Batch add devices

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

1. Start ShareScan Administration Console.
2. Click **Add Device**, or select **Add device** from the context menu (by right-clicking in the **Device Configuration** window).
3. Select **Import** from the **Discovery** list. A standard **Open file** dialog box appears and you need to select a file that describes the devices to add. The file must be a `.csv` file, containing data in the following format:

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

```
Example:10.140.202.89,Olivetti,Olivetti,1234567812345678
```

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

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

i For instructions about removing devices, see the ShareScan Help.

Client-side installation for Ricoh devices

To learn about how to install the embedded client for Ricoh devices, see the following links.

- [Install the ShareScan Ricoh client](#)
- [Add devices with installed eCopy ShareScan client](#)
- [Batch add devices](#)
- [Install a Ricoh ScanStation Driver](#)

Install the ShareScan Ricoh client

This section contains information on installing the ShareScan Ricoh client.


ShareScan supports the following devices:

- v7 (Legacy only), v10, v11 and v12 (Legacy or Secure) devices running the latest SDK/J version.
- The ShareScan Ricoh client is available as a .zip file, downloadable from the Delivery site, named ShareScanRicoClient_<jar_version>.zip

This section describes two installation methods:

- Install the Ricoh client via the Administration Console.
- Use the Ricoh Web Image Monitor to install the ShareScan Ricoh client, by installing ShareScanRicoClient_<jar_version>.zip. For more instructions, consult your Web Image Monitor manual.

These procedures assume that the proper firmware and SDK/J version is installed on the device.

 If you are planning to use Card Authentication Package (CAP), consult the relevant CAP documentation on the specifics.

Install the ShareScan Ricoh client manually (without remote installation)

On a limited number of Ricoh devices, remote installation via the Add Device Wizard is not available, thus you have to install the JAR file manually. To do so, follow the instructions below.

1. Ensure that the Ricoh device is running.
2. Open a Web browser and connect to the device by entering the IP address of the device in the address of the device in the address bar of the browser.
The **Web Image Monitor** page opens, displaying information about the device.
3. Log in to the device:
 - a. Click **Login**, which is in the upper-right corner of the page.
 - b. Enter the device administrator credentials in the **Login User Name** and **Password** fields.
 - c. Click **Login**.
 - d. The **Administrator** page opens, enabling you to configure the device.
4. In the navigation pane, click **Configuration** and scroll down to the **Extended Feature Settings** area.
5. Select **Extended Feature Installation**.
6. To install the ShareScan client:
 - a. In the **Install** area, select **Local File** and click **Choose file**.
 - b. Go to the location of the downloaded zip file.
 - c. In the **Choose file** window, select the zip file and click **Open**.
 - d. Click **Display Extended Feature List**. The **Display Extended Feature List** page opens.
 - e. Under **Installation Target Settings**, select **Install Location**:
 - for v7, v10 models: **to SD card**

- for v11 and above models: **Flash memory**
- f. Set **Auto Start** to **On**.
- g. Select the ShareScan Xlet and then click **Install**.
- h. Review the information on the confirmation page, verifying that the startup location is correct, then click **OK** to start the installation.

When the installation is complete, the **Configuration** page opens.

7. Start the application:
 - a. When the **Configuration** page opens, scroll down to the **Extended Feature Settings** area.
 - b. Click **Extended Feature Info** to verify installation of the application and then click **Back**.
 - c. Under **Extended Feature Settings**, click **Startup Settings**, ensure that the ShareScan application is selected, and click the **Startup/Stop** button.
 - d. The status of the application changes to "Starting Up."
8. Log out of the Web Image Monitor, by clicking the **Logout** button in the upper-right corner of the page.

After you have successfully installed the ShareScan client, you are ready to add the device to the ShareScan manager.
9. Start the ShareScan Administration Console.
10. Click the **Settings** button, and then click **Advanced Settings**.
11. Expand the section named with the ShareScan manager name and IP address.
12. Set the **DoNotUseRxOPDeployment** value to **TRUE**.
13. Close the dialog box.
14. Add the devices by clicking **Add device** on the toolbar.
15. Click the **Settings** button and then click **Advanced Settings** on the Administration Console toolbar.
16. Expand the section named with the ShareScan manager name and IP address.
17. Reset the **DoNotUseRxOPDeployment** value to **FALSE**.
18. Close the dialog box.

Install the ShareScan Ricoh client via the ShareScan Administration Console (recommended)

1. Ensure that the Ricoh device is running.
2. Ensure that the ShareScan Administration Console is running.
3. Either right-click **Device configuration** and select the **Add device** menu item or click **Add device** on the ribbon bar.
4. The **Add devices** window opens, displaying the available devices.
5. If a device that you want to add does not appear in the list of available devices, select a protocol from the **Discovery** list and click **Refresh**. Select the device and click **OK**.
6. The **Add Device** dialog box displays the device's IP address. Provide the necessary credentials for a device administrator and click **Next**.

7. The following dialog box allows you to install a new, or upgrade an existing ShareScan Ricoh client on this device. Click **Browse** and locate the downloaded zip file.
8. Click **Install** to start installing the client.
 - If you are upgrading a previous version of the ShareScan Ricoh client (already installed on the device), first the old client will be removed and then the new client will be automatically installed.
 - The following steps are executed:
 - a. Stopping the old ShareScan Ricoh client.
 - b. Uninstalling the old ShareScan Ricoh client.
 - c. Rebooting the device.
 - d. Installing the new ShareScan Ricoh client.
 - e. Starting the new ShareScan Ricoh client.
9. If the installation is finished, click **Finish**.
10. Enter secure connection password (only required for secure client). Click **Enter**.
11. Accept or specify device model in the **Specify device model** dialog box.

Uninstall the ShareScan Ricoh client via a web browser

1. Make sure that the Ricoh device is running.
2. Open a Web browser and then connect to the device by entering the IP address of the device in the address bar of the browser.

The **Web Image Monitor** page opens, displaying information about the device.
3. To log in to the device:
 - a. Click the **Login** button, which is in the upper-right corner of the page.
 - b. Enter the device administrator credentials into the **Login User Name** and **Password** fields.
 - c. Click **Login**.
 - d. The **Administrator** page opens, enabling you to configure the device.
4. In the navigation panel, click **Configuration** and then scroll down to the **Extended Feature Settings** area.
5. Click **Extended Feature Info**.
6. The **Extended Feature Info** page displays information about the installed application. Click **Back** to return to the **Extended Feature Settings** area.
7. To uninstall the ShareScan Client:
 - a. In the **Uninstall** area, select the ShareScan application.
 - b. Click **Uninstall**.
 - c. Review the information on the confirmation page and then click **OK** to start uninstalling the application. Respond to any warning messages.
 - d. When the process is complete, the **Uninstall** page opens. The application no longer appears in the list of application.

8. Log out of the Web Image Monitor by clicking the **Logout** button in the upper-right corner of the page.
9. Turn off the main power switch.
10. Turn on the main power switch.

Add devices with installed eCopy ShareScan client

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

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

Batch add devices

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

1. Start ShareScan Administration Console.
2. Click **Add Device**, or select **Add device** from the context menu (by right-clicking in the **Device Configuration** window).
3. Select **Import** from the **Discovery** list. A standard **Open file** dialog box appears and you need to select a file that describes the devices to add. The file must be a `.csv` file, containing data in the following format:

```
IP/host, Ricoh, model, password(string), Secure Image Uploading
```

```
Example:10.140.202.70, Ricoh, MPC300, 1111, true
```

- `IP/host`: device IP address (or host name).
- `Ricoh`: must be Ricoh.
- `model`: specific device model name (or `*` to get the model name automatically from the device).
- `password(string)`: secure device registration password

- `Secure Image Uploading`: true or false (enable or disable secure image uploading).

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

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

i For instructions about removing devices, see the *Help for Tungsten eCopy ShareScan*.

Install a Ricoh ScanStation Driver

This section contains information on installing the Ricoh ScanStation driver.

The ScanStation uses a driver to get input from the device. You must install and configure the driver before licensing the device.

To ease your device configuration task, some settings may be disabled in the Scanner Setup Wizard.

Version 4.0 Ricoh TWAIN drivers include a Network Connection Tool. When you have multiple devices of the same model type, you use the tool to select the specific device on your network that you want to use with the driver. If you are using a version 3.0 Ricoh TWAIN driver, your system will automatically connect to the first device it finds on your network that uses the driver.

To install the driver:

1. Download the driver from the Internet.
2. Run the installation program, following the instructions on the screen.
3. When the installation is complete, click **Finish**.

To configure the driver:

1. Select **Start > Programs > driver_name > Network Connection Tool**.
2. Select **Use a specific scanner**.
3. Click **Search Scanner**. The **Search Scanner: Result** window lists all the devices on the network that can use the current TWAIN driver.
4. Select the Scanner that you want to use and then click **OK**. The **Network Connection Tool** window opens.
5. Click **OK**.



- If upgrading from a 5.x configuration, due to architectural changes, you have to configure TWAIN driver again even though it was configured before the upgrade. If ScanStation client is launched after upgrading without reconfiguration, a warning message appears and says "Before starting ScanStation for the first time, you have to configure the scanner in the Administrator Console. ScanStation will now quit."
- When custom upgrading a ScanStation with a remote database, and database connection is modified to use Windows Integrated Authentication, the Administrator user performing the ShareScan installation needs to grant the following rights manually to the specific registry hives after performing the upgrade installation; otherwise the Administration Console will not be able to start. Full access to (on a 32-bit OS) `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`; `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run` (on a 64-bit OS) `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon`; `HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run`). Afterwards, the Agent Service needs to be started in the Windows Service Control Manager and the ScanStation Client installer can be run to complete the system upgrade to this version.

ISIS drivers

In addition to scanning via TWAIN, ScanStation also supports ISIS-scanning. Install the ISIS driver supplied by the manufacturer of the device and then use the Scanner Setup Wizard to configure its use with ScanStation.

If any scanning issue occurs with ScanStation, test first whether you are able to scan into another ISIS supported application.

Client-side installation for Xerox devices

To learn about how to install the embedded client for Xerox devices, see the following links.

- [New EIP Job polling method](#)
- [Configure the Xerox device](#)
- [Add devices with installed eCopy ShareScan client](#)
- [Batch add devices](#)

New EIP Job polling method

eCopy ShareScan for Xerox devices uses EIP scan job polling method by default. It allows performing ShareScan scanning also in a network environment where SNMP is disabled and workflows can be run without using SNMP.

If there are older devices which do not support EIP version 2.0 or above, a Scanning error message appears during workflows and images cannot be transferred to the ShareScan Manager.


For these devices, it is possible for the ShareScan Manager to fall back on the earlier SNMP job polling mode which works with all Xerox devices but the SNMP must be enabled on network environment and it must be configured for all Xerox devices.

For configuring older devices, see [How to configure ShareScan Manager for older Xerox devices \(EIP 2.0 or above not supported\)](#) section in the Troubleshooting chapter.


Configure the Xerox device

ShareScan supports EIP-capable Xerox devices only. Before you can use ShareScan with Xerox devices, you must install or enable the following components:

- Custom Services (EIP) installation
 - Custom Services is usually pre-installed on most Xerox devices
- HTTPS
 - Navigate to the correct page of the device's Web Administration application (usually Properties/Connectivity/Protocols/HTTP)
 - Enable Secure HTTP (SSL)

 You may need to create a certificate and install it onto the device before you can turn on Secure HTTP. See Checklist for using Xerox devices with embedded clients section in the Pre-installation Checklist and Sizing guide.

- Custom Services (EIP) enabling
 - Navigate to the correct page of the device's Web Administration application
 - Enable Custom Services
- Simple Network Management Protocol (SNMP)
 - Navigate to the correct page of the device's Web Administration application
 - Enable SNMP v1/v2c protocols
- Scan Template Management
 - Navigate to the correct page of the device's Web Administration application
 - Scan Template Management

 To achieve proper functionality of ShareScan, the device's Auto Refresh must not be disabled (the Auto Refresh Interval must not be set to 0 (void) seconds). The name of this feature may differ across various devices. Most common variants include: System timeouts, Auto Resume, Auto Refresh Interval, and Touch User Interface System Timer.

Add devices with installed eCopy ShareScan client

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

1. Start eCopy ShareScan Administration Console.
2. Click **Add Device** on the toolbar. You can also select **Devices** on the **Welcome** page and then right-click the **Device Configuration** window and select **Add Device**. The **Add Devices** window opens.
3. If your device does not appear in the list, select **SNMP** instead of the **UDP** option from the **Discovery** list. If the auto discovery does not succeed, use TCP/IP to add it manually.
4. Select the device you want to add.
5. Click **OK**. The device registration dialog box opens.

6. Observe the following:
 - If Secure Client is installed and this is the first time the device is added to eCopy ShareScan after client installation, a eCopy ShareScan-related secure connection password must be set. Provide the new password for secure connection in the **Password** and **Re-enter password** fields and select **Secure image uploading** if you want image uploading to happen in secure mode. Click **OK**.
 - If Secure Client is installed and the eCopy ShareScan-related secure connection password is already set, specify the password in the **Password** field and select **Secure image uploading** if you want image uploading to happen in secure mode. Click **OK**.
7. Choose a device model from the **A known model** list on the **Specify device model** dialog box and click **Close** to finish adding the device.

Batch add devices


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

1. Start ShareScan Administration Console.
2. Click **Add Device**, or select **Add device** from the context menu (by right-clicking in the **Device Configuration** window).
3. Select **Import** from the **Discovery** list. A standard **Open file** dialog box appears and you need to select a file that describes the devices to add. The file must be a `.csv` file, containing data in the following format:


```
IP/host, Xerox, model, username(string), password(string),  
SNMPGet(string), HTTPS(bool), AsyncBW(bool)
```

Example: 10.140.202.70, Xerox, C8030, admin, 1111, public, false, false

- `IP/host`: device IP address(or host name).
- `Xerox`: must be Xerox.
- `model`: specific device model name(or * to get the model name automatically from the device).
- `username(string)`: device administrator username used for device registration.
- `password(string)`: device administrator username used for device registration.
- `SNMPGet(string)`: SNMP get community name (public by default; if otherwise specified on the device web administration page, the same must be included here).
- `HTTPS(bool)`: true or false (enable or disable secure communication and file transfer for the device).
- `AsyncBW(bool)`: true or false (asynchronous scanning in B&W mode; for optimal performance, true is recommended).

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

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

 For instructions about removing devices, see the ShareScan Help.

Drivers for ScanStation

This section contains information on drivers for scanning when ScanStation is used with an MFP.

The ScanStation uses a driver to get input from the device. You must install and configure the driver before using the device.

ShareScan installation also installs two drivers that are available for scanning: the **Send to eCopy driver** and the **Xerox Remote Scan Module**.

The **Sent to eCopy driver** can be used when the device is configured for scan to a shared (SMB) folder (local or network). For further information, consult the device documentation.

This driver can be configured in the ShareScan Administration Console with the following parameters:

- **Watch folder:** A local or network folder watched by the Send to eCopy service for incoming scanned images. Specify it manually or select a folder by clicking the ellipsis button. The device must be configured to send the image files to this folder.
- **Domain:** Domain of the user account to get access to the network watch folder.
- **User Name:** User name of the user account used to get access to the network watch folder.
- **Password:** Password of the user account used to get access to the network watch folder.
- **Filter:** File name and extension filter listing files to be processed. Unlisted files are ignored. For specifying more filter, use the vertical bar (|) as separator (for example *.jpg|*.pdf).
- **Instructions Image:** An instruction image is displayed on the device to help the user know how to perform scanning. Specify the full path of the instruction image manually or browse it by clicking on the ellipsis button.
- **Use Lock file:** Select this option to use a lock file for preventing other Send to eCopy service(s) on different ShareScan Manager computer(s) from monitoring the same watch folder.
- **Use Encryption:** Select this option to have encryption on files while they are in the watch folder. Encryption works for local watch folders based on Windows security settings only.
- **Inactivity Timeout:** If the images in the watch folder are stored longer than this time frame without being processed, Send to eCopy service deletes them. Its value must be specified in milliseconds.
- **First Page Timeout:** This value controls how long the ScanStation application waits for the first page of the scan job to arrive from the Send to eCopy service. The time counter starts after the **OK** button is pressed on the Instructions dialog. Its value must be specified in milliseconds.
- **Next Page Timeout:** This value controls how long the ScanStation application waits between receiving the additional pages of the scan job. Its value must be specified in milliseconds.
- **Session Timeout:** This value controls when the Send to eCopy service considers that the ScanStation application stopped working and terminates the session. This happens if there is no call from the ScanStation application to the Send to eCopy service within the time frame specified here. Its value must be specified in milliseconds.

The **Xerox Remote Scan Module** can be used only with Xerox devices supporting EIP 2.5 or later. For further information about configuring this module, see [Xerox Remote Scan Module Configuration Tool](#).

Xerox Remote Scan Module Configuration Tool

For newer Xerox devices (featuring Xerox EIP 2.5 or above), using Xerox Remote Scan Module is recommended for scanning. Xerox Remote Scan Module makes communication between ShareScan and the MFP device much simpler. Its configuration tool is located in the <Tungsten Ominpage Capture SDK 22.1 installation folder>\RSD folder (typically C:\Program Files\Tungsten\CSDK22.1\RSD) and can be launched by starting XeroxRemoteScanModuleConfigurationTool.exe. This tool has the following parameters:

- **Device hostname/IP:** The hostname or IP address of the device. Click the **Find** to identify the device.
- **Use HTTPS:** Select this option to use HTTPS connection.
- **Validate server certificate:** Select this option if you want to validate the certificate; only active if **Use HTTPS** is selected.
- **Client certificate file:** The location of the client certificate file; only active if **Use HTTPS** is selected.
- **Browse (...):** Click this button to browse for the client certificate file; only active if **Use HTTPS** is selected.
- **Input Edge Erase Units** (choose between mm and 1/100th of an inch): The area in mm or 1/100th of an inch that is cropped from the designated side of the page.

i If you specify areas larger than the actual page size or configure two opposing page areas that make up the full page area, the page will disappear.

- Side 1:
 - Left: crops the specified area from the left of the page.
 - Right: crops the specified area from the right of the page.
 - Top: crops the specified area from the top of the page.
 - Bottom: crops the specified area from the bottom of the page.
- Side 2:
 - Left: crops the specified area from the left of the page.
 - Right: crops the specified area from the right of the page
 - Top: crops the specified area from the top of the page
 - Bottom: crops the specified area from the bottom of the page
- Auto exposure: can be **Auto** or **Off**.

Install certificates on Xerox devices for secure SSL communication with Xerox Remote Scan Module

To make it possible for the Xerox device and the computer to communicate via secure SSL connection, a proper set of certificates should be installed on both sides. The recommended configuration is to install a root certificate on both the device and the computer. A certificate that

is signed with this root certificate should also be installed on the device and selected as a device certificate. Another certificate also signed with this root certificate should be exported to a `.cert` file and the path of this `.cert` file should be added to the configuration tool of Xerox Remote Scanning Module. Therefore the module will use this certificate when it tries to open an SSL connection.

1. Get a root certificate or create one with the tool mentioned above or with any other tool.
2. Export it to a `.cert` file.
3. Open the web administration page of the device in a browser, and sign in as an administrator.
4. Go to **Security Certificates** settings and select the **Root/Intermediate Trusted Certificate(s)**.

 The administration page may look different in case of other devices.

5. Click **Install Certificate** and install the root certificate.
6. Click **Create Certificate Signing Request (CSR)** and create a **Certificate Signing Request**.
7. Open this CSR by clicking **View/Export** and export it by clicking **Export (Base-64 Encoded -PEM)**.
8. Import this CSR in the XCA tool or the tool you use for creating certificates.
9. Sign the CSR with the root certificate and export the new certificate to a `.cert` file.
10. On the device administration page, click **Install Certificate** and install this certificate.
11. Go to **Connectivity > Setup settings** page.
12. Find HTTP and click **Edit**.
13. In the list under **Choose Device Certificate**, select your certificate and save the changes.
14. In the certificate tool, create another certificate for the computer. Sign it with the same root certificate.
15. Export it to a `.cert` file and select it as an **SSL certificate in the Xerox Remote Scan Module**.

After these steps, the Xerox Remote Scanning Module will be able to communicate with the device via a secure SSL channel.

TWAIN and ISIS drivers

In addition to scanning with the Xerox Remote Scan Module or the Send to eCopy driver, ScanStation also supports TWAIN and ISIS drivers. You must install and configure the driver before licensing the device. Install the TWAIN or ISIS driver supplied by the manufacturer of the device and then use the Scanner Setup Wizard to configure its use with ScanStation.

To ease your device configuration task, some settings may be disabled in the Scanner Setup Wizard. Drivers are typically included with scanners. However, you may need to update the driver if the driver version included with the scanner may not be the most current version. It is recommended that you go to the scanner vendor's website to verify that you have the latest available driver and, if necessary, download the driver, install it on the ScanStation, and then configure it as needed.

If any scanning issue occurs with ScanStation, test first whether you are able to scan into another TWAIN or ISIS supported application.

Device Calibration Connector

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

Prerequisites

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

- Add a device you want to calibrate.

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

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

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

Usage

To create calibration rules, do the following:

1. Insert a single sheet in the position that you want to calibrate – that is, in the orientation for which the system produces a not appropriate result.
2. Select the scanning options you have problems with via the scanner setting bar of the main ShareScan screen on the device. These include:
 - Color depth
 - Paper size
 - Output Orientation
 - Double side scan options
3. Push the connector button on the **Main** screen to scan the page, and the preview appears.
4. Rotate the page you have problems with, using the rotation buttons on the Preview form. If you have a problem with the double-sided scanning, ensure you performed the corrective rotations for both pages. Also check that the orientation is correct (only the final orientation is important for the calibration).
5. Click **Next**.

On the displayed screen, you can review the following settings and information for the exception rule of your device:

- The bottom part shows the settings you used.
- The **Vendor** and **Model** radio buttons allow you to select between applying the settings to all devices of a given vendor, or a specific device model, respectively.
- The **Use this setting for all color settings** check box deletes all the rules defined for specific color settings. Saving the rule will use that for all color settings.

- The **Use this setting for all paper sizes** check box deletes all rules defined for specific paper sizes, except the rules created for Auto (or Free, or Mixed) input paper sizes. Saving the rule will use that for all paper sizes.
 - If you want to use separate rules for specific paper sizes, set them up after you set up the above generic rule. Otherwise, the generic rule overwrites the specific rules.
6. Click **Save** to store the settings in the `UserRotationAngles.xml` and `UserScanStationRotationAngles.xml` files, located at `C:\ProgramData\Tungsten\ShareScan`.
 7. The defined rules will be available only after restarting the ShareScan Manager windows service.
 8. To remove the exception rules, delete these files, and restart the ShareScan Manager windows service.

Chapter 3

eCopy connectors

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

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

The following backend applications are supported:

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

Supported versions

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

Backend Applications	Supported Versions	Installation Prerequisites
Microsoft Exchange (Mail and/or Fax)	Microsoft Exchange 2016, 2019, Exchange Online for Office 365	eCopy connector for Microsoft Exchange (Mail and/or Fax)
LDAP/SMTP (Mail and/or Fax)	<ul style="list-style-type: none"> Microsoft LDAP v3 Open LDAP v2.4 	eCopy connector for LDAP/SMTP (Mail and/or Fax)
Quick Connect	<ul style="list-style-type: none"> 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 <i>eCopy ShareScan Technical Specifications</i> document. For additional information on supported configurations of eCopy ShareScan, Quick Connect to Database, see the Quick Connect Database Recommended Usage document available for download from eSPN. 	eCopy connector for Quick Connect
OpenText Fax Server (RightFax Edition)	20.2 or higher	eCopy connector for OpenText Fax Server (RightFax edition)
Microsoft SharePoint	2016, 2019, SharePoint Server Subscription Edition, SharePoint Online for Office 365	eCopy connector for Microsoft SharePoint
OpenText Documentum	20.2 or higher	eCopy connector for OpenText Documentum
iManage WorkSite	10.3 or higher (including iManage Cloud)	eCopy connector for iManage WorkSite
OpenText Content Server - eDOCS Edition	16.7 or higher	eCopy connector for OpenText Content Server - eDOCS edition

Backend Applications	Supported Versions	Installation Prerequisites
OpenText Content Server (Livelink)	20.2 or higher	eCopy connector for OpenText Content Server

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

For supported versions of Microsoft Exchange, see [Supported versions](#) in this guide.

Installation prerequisites

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

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

For supported versions of LDAP/SMTP, see [Supported versions](#) in this guide.


Installation prerequisites

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

eCopy connector for Scan to Desktop


Installation prerequisites

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

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

Inbox Root Directory

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

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

ShareScanAdmin Group

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

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

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

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

eCopy connector for Quick Connect

For supported versions of Quick Connect, see [Supported versions](#) in this guide.

Installation prerequisites

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

eCopy connector for OpenText Fax Server (RightFax edition)

For supported versions of OpenText Fax Server, see [Supported versions](#) in this guide.

Installation prerequisites

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



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

eCopy connector for Scan to Printer

Installation prerequisites

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

eCopy connector for Microsoft SharePoint

For supported versions of Microsoft SharePoint, see [Supported versions](#) in this guide.

Installation prerequisites

- The administrator must enter a user name and password that will enable browsing to all destinations, display all index fields, and store documents if Login As authentication is used.
- If your organization uses a secure SharePoint site, you must install an SSL certificate on the ShareScan server.



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

eCopy connector for OpenText Documentum

For supported versions of OpenText Documentum, see [Supported versions](#) in this guide.

Installation prerequisites

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

Suggestions


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

eCopy connector for iManage WorkSite

For supported versions of iManage WorkSite, see [Supported versions](#) in this guide.


Installation prerequisites

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

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

Suggestions

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

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

eCopy connector for OpenText Content Server - eDOCS edition

For supported versions of OpenText Content Server - eDOCS edition, see [Supported versions](#) in this guide.

Installation prerequisites


- Before installing the eCopy connector for OpenText Content Server, the administrator must install and configure the Windows Explorer DM Extension software for OpenText Document Management, eDOCS on the same computer as the eCopy ShareScan Manager. Once done, the

administrator must run the DM Connection Wizard. All versions of the DM Extension software include the required DM API and the DM Connection Wizard.

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

 Do not select **Intranet Mode**.

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

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

Suggestions

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


eCopy connector for OpenText Content Server

For supported versions of OpenText Content Server, see [Supported versions](#) in this guide.

Installation prerequisites

- The administrator must enter a user name and password that enables browsing to all locations, display all index fields, and store documents if `Login As` authentication is used.
- The eCopy connector for OpenText Content Server uses the REST API protocol or Web services protocol for communication with Open Text Content Server.

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

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

Suggestion

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

Chapter 4

About licensing devices

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

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

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

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

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

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

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

How to load licenses

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

1. Click **Load License** on the **License** wizard.
The **Welcome** screen appears.
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 appears.
5. Click **Browse** to add new files to the list of files to be imported. When finished, click **Start Import**.
6. Click **Start** to begin loading licenses.
7. Click **Finish** to close the **License** wizard.

How to activate licenses

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

1. Click **Activate** on the **License** wizard. The **Welcome** screen appears. 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 appears.
4. Click **Start** to begin the activation. The **Specify file output** screen appears. 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 eCopy ShareScan.

1. Click the **Load activated** button of the **License** wizard. The **Welcome** screen appears.
2. Click **Next** to continue. The **Select license files to load** screen appears.
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 eCopy ShareScan installation. After the removal is complete, the licenses can be safely transferred and reactivated.

1. Click **Remove** on the **License** wizard. The **Welcome** screen appears.
2. Click **Next** to continue. The **Select Licenses** screen appears.

3. Select the licenses you want to remove and then click **Next**.
4. Click **Start** to remove the selected licenses.
5. Click **Finish** to close the **License** wizard.

How to generate a license report

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

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

Chapter 5

Post-installation

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

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

ScanStation post-installation

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

After installation, configure the following options:

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

Configure ShareScan (examples)

This section outlines the basic process to:

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

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

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

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

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


Configure a service - Activity Tracking example

1. Start the ShareScan Administration Console by clicking **Start > Programs > eCopy Applications > ShareScan 6.7 > ShareScan Administration Console**.
The system initializes the .NET framework, retrieves configuration information from the ShareScan database, and then displays the ShareScan Administration Console.
2. Select the **Services** tab.
The **Configure Services** pane displays a list of the installed services, including connector services, device services, and common services.
3. In the **Device Services** list, select **Activity Tracking**.
The **Configure Activity Tracking Service** pane appears.
4. Select **Yes** for the **Configured** setting and then click **Save**.
For more information about configuring the Activity Tracking service, search for the **Activity Tracking** service topic in the Help.

Configure an extender - Forms Processing Extender example

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

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

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

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

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

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

7. Use the **Settings** pane to configure the following:
 - Display settings
 - Workflow settings
 - Document settings
 - Service to be associated
 - Extender to be associated
 - Scanner settings
8. Click the **Save Current Profile** button.


For more information about configuring the settings for a connector, open the applicable Help topic.

Test the profile configuration

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

Creating self-signed server certificates for Konica Minolta and Olivetti devices

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

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

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

```
<FunctionInfo>
...
  <FunctionName>Setup</FunctionName>
  <FunctionVersion>
    <Major>3</Major>
    <Minor>7</Minor>
  </FunctionVersion>
...
</FunctionInfo>
```

Create the certificate manually

1. Stop the Tomcat service.
2. Generate the public and private key pair and export the public key to a *.der file.

The following example refers to the Tomcat installation folder as TOMCAT_DIR (%programfiles(x86)%\Tungsten\Tomcat9)

- a. Back up your current key files:

- Back up %TOMCAT_DIR%\conf\ecopy.key
- Delete %TOMCAT_DIR%\conf\ecopy.key
- Back up %TOMCAT_DIR%\webapps\ROOT\ecopy.pem
- Delete %TOMCAT_DIR%\webapps\ROOT\ecopy.pem
- Back up %TOMCAT_DIR%\webapps\ROOT\ecopy.cer
- Delete %TOMCAT_DIR%\webapps\ROOT\ecopy.cer

- b. Modify %TOMCAT_DIR%\conf\createEcopyKey.bat:

- Change the SET CERTIFICATE_COMMON_NAME= < ShareScan host IP address> row to SET CERTIFICATE_COMMON_NAME= < ShareScan host fully qualified domain name>
- Insert the %KEYTOOL% -export %TOMCAT_ALIAS% -file "..\webapps\ROOT\ecopy.der" row above the %KEYTOOL% -export %TOMCAT_ALIAS% -file "..\webapps\ROOT\ecopy.cer" row.

- c. Save and run %TOMCAT_DIR%\conf\createEcopyKey.bat.

- d. Restart the Tomcat service.

3. Install the certificate to the browser on the device you run ShareScan.

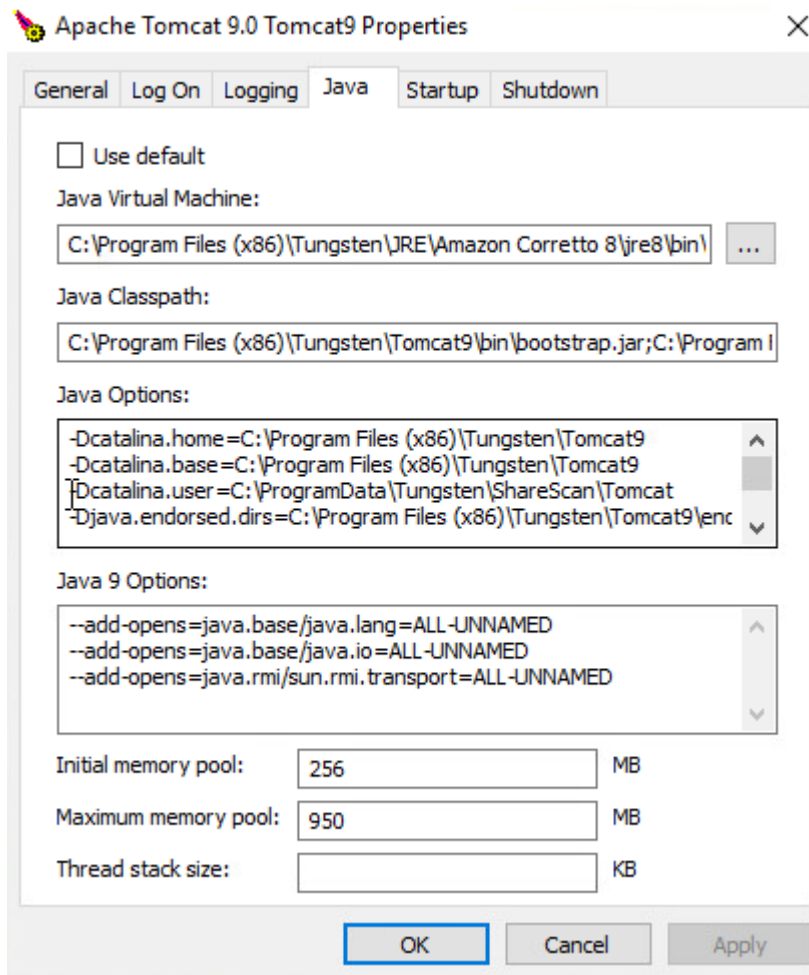
- a. Start the browser by pressing the **Application Menu** button and clicking **Web Browser**.
- b. Select **Address** on the browser toolbar, and enter `http://<ShareScan host IPAddress>:8080/ecopy.der`.
- c. Enter the device password, then select **Root Certificate**.

4. Start ShareScan on the device to verify the results. There are no error messages but you might receive a "This page is protected" message; you can disable it with the check box under the message.

How to change the ShareScan Web client certificate to SHA1

On some older web-based devices (Fujifilm, HP, Konica Minolta, Olivetti, Xerox), an error message is displayed because this version of eCopy ShareScan uses SHA256 certificates by default. To avoid this error, administrators must generate and configure SHA1 certificates either by using the Certificate Manager tool (see [Certificate Manager](#) below) or manually in the following way:

1. Locate the ShareScan Tomcat configuration folder. It is under `<INSTALL_FOLDER>\Tomcat9\conf\`. `<INSTALL_FOLDER>` is the folder in which ShareScan is installed. Its default value for this release is `c:\%programfiles(x86)%\Tungsten`, but it can be changed when ShareScan is installed. The default Tomcat configuration folder for this release is `c:\%programfiles(x86)%\Tungsten\Tomcat9\`.
2. Create a backup of the `createEcopyKey.bat` file found in this folder. The `eCopy.key` file contains the original SHA256 certificate. The `createEcopyKey.bat` script can be used to create a new one.
3. (Optional) Create a backup of the original SHA256 certificate and private keys if you want to restore the original certificates later. Back up the `eCopy.key` file located in the Tomcat configuration folder. Also back up the `eCopy.cer`, `eCopy.der`, and `eCopy.pem` files in the `<INSTALL_FOLDER>\Tomcat9\webapps\ROOT\`. The default location is `c:\%programfiles(x86)%\Tungsten\Tomcat9\webapps\ROOT\`.
4. Edit the `createEcopyKey.bat`. Replace the line `SET SIGALG=SHA256withRSA` with `SET SIGALG=SHA1withRSA`. Save the changed file. Administrator rights may be needed to save it.
5. Stop ShareScan Tomcat service. Open Windows Services and stop the Apache Tomcat 9.0 Tomcat9 service.
6. Delete the `eCopy.key` file.
7. Create the new certificate with `createEcopyKey.bat` file. This script needs 3 parameters in this order:
 - The IP address of the host running the Tomcat service. You may also specify the FQDN instead of the IP address, but ShareScan was tested with IP-based certificates.
 - The location of the Java key tool. ShareScan installs a Java Runtime Environment (JRE) for itself, which contains a `keytool` that can be used. If you are not sure where the JRE is located, run the `<INSTALL_FOLDER>\Tungsten\Tomcat9\bin\Tomcat9w.exe` and check the Java tab in the opened application window.



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

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

```
C:\Program Files (x86)\Tungsten\Tomcat9\conf>createEcopyKey.bat
10.140.25.107 'C:\Program Files (x86)\Tungsten\JRE\Amazon Corretto 8\jre8\bin
\keytool.exe'
3650
tomcat, Sep 25, 2017, PrivateKeyEntry,
Certificate fingerprint (SHA1):
30:C1:A3:2C:AC:18:27:A5:DE:DD:AE:B6:DB:0F:DF:47:80:FA:E2:6A
Certificate stored in file <..\webapps\ROOT\eCopy.der>
Certificate stored in file <..\webapps\ROOT\eCopy.cer>
Certificate stored in file <..\webapps\ROOT\eCopy.pem>
```

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

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

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

Certificate Manager

The Certificate Manager is an add-on tool for eCopy ShareScan, which allows you to manage the certificates required by web-based devices (Fujifilm, HP, Konica Minolta, Olivetti, Xerox). The tool is located in the <ShareScan installation folder>\Server\Tools folder, and can be launched by starting `CertificateManager.exe`.

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

- **Configure Tomcat server.xml:** This option allows you to customize the cryptographic protocols and ciphers used by ShareScan on a port-by-port basis by editing the server.xml file used by the Tomcat component of ShareScan. Clicking this button displays a new window, listing all ports currently used by ShareScan, and the cryptographic protocols assigned for the specific port, if that port uses SSL or TLS. You can use the server.xml item in the top-left corner to create a backup of the server.xml file you are using, or you can load a previously saved server.xml. To modify the protocols and ciphers assigned to a port, do the following:
 1. Click on the port whose properties you want to modify.
 2. Click the **Edit** button on the upper-right part of the window. A new screen appears, showing the currently used protocols and ciphers.
 3. Under **Enabled protocols**, select the cryptographic protocols you want to use (for example, TLSv1 or SSLv3).
 4. Under **Enabled Ciphers**, select the ciphers you want to use. For ease of use, a number of filter options are included with the tool and can be accessed via button push.
 5. Click **OK** to save the changes.
- **Re-generate certificate:** This option allows you to recreate your digital certificate. To create the certificate, you have to enter either the IP address (**Discover IP** button) or Fully Qualified Domain Name (**Discover FQDN** button) to the displayed field under **Certificate Common Name**, and to select the signing algorithm from the **Algorithm** list (SHA256 or SHA1), and then click the **Generate** button on the lower-right part of the window.
- **Backup certificate:** This option creates a backup of your existing certificate. A **Browse** window appears, where you can select the location and file name of the certificate to be saved. Back up your certificates if you have imported your certificates manually to your devices (to prevent the warning from popping up), and do not want to repeat the process. Also, the recommended workflow when upgrading is to back up your certificate, upgrade ShareScan, then restore the certificate.
- **Restore certificate:** This option restores a certificate. A **Browse** window appears, where you can locate the certificate to be restored.

Key-in for Ricoh devices

eCopy ShareScan allows you to utilize the Key-in feature on small-screen Ricoh devices, which is an input method allowing a texting-like approach to entering characters to the device forms. This option is mutually exclusive with the device soft keyboard; when one is set, the other is unavailable.

As multiple characters are keyed to each button, repeatedly pressing the same button cycles through the available options keyed to that particular button. This cycling is also presented in the preview in the top-left corner of the device screen.

To activate this feature:

1. Start the ShareScan Administration Console.
2. Go to the **Device** pane, and select the device you want to use.
3. Click **Key-in** to activate the feature.

How to use the key-in feature

- Check the top-left corner of the device screen for a preview of the next character.
- Use the touchscreen to focus on the field where you want to enter characters. The currently-focused field is displayed in yellow. You can enter characters in the focused field using the keyboard.
- Press another location on the touchscreen to change focus to that field.
- Press the **C** button to delete a character.
- Press the **#** button to tab between the controls on the page.
- Press any number key for a longer time to enter digits.
- Press ***** for a longer time to switch between uppercase and lowercase. The preview changes to reflect the change.
 - Press **key 1** to access the following characters: ' , ? , ! , \ , - , (,) , @ , / , : , _ , ; , + , & , % , * , = , < , > , € , £ , \$
 - Press **key 2** to access the following characters: a , b , c
 - Press **key 3** to access the following characters: d , e , f
 - Press **key 4** to access the following characters: g , h , i
 - Press **key 5** to access the following characters: j , k , l
 - Press **key 6** to access the following characters: m , n , o
 - Press **key 7** to access the following characters: p , q , r , s
 - Press **key 8** to access the following characters: t , u , v
 - Press **key 9** to access the following characters: w , x , y , z
 - Press **key 0** to access the following characters: 0 , <space>
 - Press **key *** to access the following characters: . , * , #

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 displays a list of the main feature highlights of the current version.

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

Best practices

- Ensure that the `%temp%` environment variable is set.
- Ensure that all critical automatic updates are applied to target systems and that automatic updates are turned off for the time of installation.
- Do not wait too long to click **Install**; otherwise, the increased storage usage in the temp folder can trigger a cleanup process that causes installation failure.
- After installation, you may check to see whether the following services are running:
 - Apache Tomcat 9.0
 - ShareScan Agent
 - ShareScan Manager
 - ShareScan WatcherService
 - ShareScan Web Admin Host
 - PushKeyService
- There are other services which may not run by default, only if the respective functionality demands it:
 - Tungsten Printer API
 - S2D Inbox Agent
- Tomcat service settings can be viewed/modified via: `%programfiles(x86)%\Tungsten\Tomcat9\bin\tomcat9w.exe`
- Ensure that there is no Apache Tomcat on the computer you want to install ShareScan on.
- Ensure that no ports used by ShareScan listed in the *Installation Guide* are used by other web services, as that may cause connectivity issues.
- Deploying the `RightFax FaxUtil` on the same machine on which ShareScan is running may cause issues, therefore it is not advised.
- If the Apache Tomcat component does not start after a Java update, a reboot solves the issue.
- If you use CAC, and get a "Scanner is offline" message after removing the CAC card during the scanning process, restart the ScanStation computer to return the system to normal state.
- If you have multiple ShareScan Manager computers in your deployment, it is recommended that you always use the same instance of the Administration Console to add, modify or remove connector profiles regardless of whether you are working in a cluster environment or not.

Technical support


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

When contacting Technical Support (if a reseller) or your eCopy dealer (if an end-user), please provide the following information to facilitate a quick resolution while working with Tungsten Automation Technical Support.

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

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

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

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

- Ensure that there is no Apache Tomcat on the computer you want to install eCopy ShareScan on.
- Ensure that no ports used by eCopy 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 eCopy ShareScan is running may cause issues, therefore it is not advised.
- If the Apache Tomcat component does not start after a Java update, a computer reboot solves the issue.
- When upgrading an existing eCopy ShareScan installation that has CAC configured, you must disable and re-enable CAC via the Administration Console after the upgrade process to this eCopy ShareScan version has finished.
- If you experience an infinite rebooting loop on your target machine, look for and delete the following registry keys:
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager Value: PendingFileRenameOperations
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update Value: RebootRequired

How to configure ShareScan Manager for older Xerox devices (EIP 2.0 or above not supported)

1. Open the `Xerox.properties` file for editing under `%programfiles(x86)%\Tungsten\Tomcat9\webapps\ShareScan\WEB-INF\classes`.
2. Insert this line to enable SNMP polling method: `- enable.eip.job.poll = false`. If this line is missing, EIP polling method is the default.
3. Save the file.
4. Restart the ShareScan services.

Xerox devices not supporting EIP2.0

- Phaser 3635 MFP.
- WorkCentre 5222/5225/5230
- WorkCentre 6400
- WorkCentre 7232/7242
- WorkCentre 7328/7335/7345
- WorkCentre 7346
- WorkCentre 7655/7665/7675 – Color
- Color 550/560
- D95/D110/D125
- ColorQube 9201/9202/9203
- WorkCentre 5135/5150
- WorkCentre 5325/5330/5335
- WorkCentre 5632/5638/5645/5655/5665/5675/5687
- WorkCentre 7120/7125
- WorkCentre 7425/7428/7435

- WorkCentre 7755/7765/7775