Kofax eCopy ShareScan
6.3
Installation Guide for Xerox Devices

KOFAX

Licensing, Copyright, and Trademark Information

Contents

ShareScan Installation Guide

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

This guide is intended for administrators responsible for the initial installation, configuration, and licensing of ShareScan. For the device-specific Pre-Installation Checklist (PICL), see the relevant vendor-specific Pre-Installation Checklist and Sizing Guide.For information pertaining to the ShareScan (pre)install, see this guide. For configuration and Administration Console usage, refer to the Administration Console Help (accessible via pressing **F1** on the Administration Console).

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

ShareScan Documentation

The following documentation is available for your perusal with ShareScan:

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

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

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

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

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

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

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

Typical Installation Workflow

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

Installing ShareScan 6.3 with no previous version already present

1. Ensure that the ShareScan prerequisites (listed in the following chapter) are installed.
2. Start the ShareScan 6.3 installer, and click through the Installation Wizard.

Upgrading from ShareScan 5.x to 6.3

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

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

Upgrading from versions pre-dating v5.4

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

Upgrading from v5.4 or higher to 6.3

1. Exit ShareScan 5.x Administration Console.
2. Ensure that the ShareScan prerequisites (listed in the following chapter) are installed.
3. Run eCopy ShareScan 6.3 installer.
4. Choose **Upgrade from previous version to 6.3** or **Custom upgrade from previous version to 6.3** after the **Welcome** screen and click through the upgrade workflow.

Pre-installation

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

System Requirements for the ShareScan Manager PC

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

– Amazon Corretto 8 Java Runtime (x86)

– Microsoft .NET Framework 4.7.1

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

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

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

– Microsoft Visual J# 2.0 Redistributable

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

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

Operating Systems

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

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

Database

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

Virtual Environments

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

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

Memory Configuration

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

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

Checklist for the ShareScan Manager PC

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

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

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

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

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

– If you have multiple NIC cards, you need to select an IP address for ShareScan that will be used for device-server communication.

– Check if your file system format is NTFS.

– Ensure that Microsoft IIS is not installed or is not listening to the ports used by ShareScan (listed below).

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

ShareScan 6.x, it is important to determine if licenses will be managed individually from each ShareScan Manager, or if you would like to manage all licenses from a single SQL Server.
The ShareScan installer can install a local copy of SQL Server 2014 Express for managing licenses (in addition to storing configuration data). It can also create the appropriate database structure on an existing SQL server for consolidated key management.

– ShareScan license keys must be activated against an Activation Server. License keys can only be activated once, so inspect the setup carefully prior to activation. All license keys provide a 30-day grace period before activation to ensure the license setup is as intended. Manual activation is available for servers that are unable to communicate directly with the Activation Server.
As licenses are tied to the ShareScan database, it is not recommended tochange databases after ShareScan installation.

– If you plan to use the **Single Sign-On** feature of the **Session Logon** service, ensure that the ShareScan Manager PC is a member of the domain for which Session Logon is configured. The logged in user running and configuring the Session Logon must be an Active Directory user with the necessary rights to read properties in Active Directory (this is a default value). Ensure that you use the Active Directory user account to log in into this domain (and not into the local system). This Active Directory user must have the necessary rights to read Active Directory properties (generally this is a default behavior; however this can be modified in Active Directory).

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

Ports to be left open

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

Inbound traffic:

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

– UDP: 9650

Outbound traffic:

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

– UDP: 161 (SNMP), 8899, 9650

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

Database Permissions

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

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

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

Network

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

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

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

a. remove all devices from the Manager
b. stop all ShareScan related services
c. change the IP address of the NIC and make sure the network adapters use the new IP (`ipconfig` command)
d. start the services stopped in (b)
e. re-add the devices

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

a. remove all devices from the Manager

b. change the IP address

c. reboot the Manager PC

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

e. recreate the certificate(s)

f. re-add the devices to the Manager

– **Gateway Address:** ShareScan does not require a gateway address.

– **Host Name:** The host name must not exceed 60 characters. Device host names are resolved using DNS. This happens once you have added a device and confirmed it. If the device is not registered in the DNS, then its name in the **Devices** tab (Administration Console) may change after confirmation.
Note that changing the host name after installation can cause licensing and database issues, and is therefore **not supported**. If you must change the host name, you must do a full reinstallation of ShareScan.

– **Network Attached Storage Devices (NAS):** ShareScan 6.3 supports NAS drives and folders that are fully compatible with NTFS file system and Windows access control mechanisms.

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

– **Local Security Policy:** In order to use the Administration Console on the ShareScan Manager PC, you require local administrator-level credentials. ShareScan Manager cannot be installed on a Domain Controller.

Support information

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

Supported languages

ShareScan 6.3 supports the following languages:

– English

– Brazilian Portuguese

– Dutch

– French

– German

– Italian

– Spanish

– Catalan (client only)

– Simplified Chinese (client only)

– Japanese (client only)

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

Supported devices

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

Supported backend services

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

Install ShareScan

The following chapter contains information on the various tasks associated with installing ShareScan.

Outline

To install, configure, and license ShareScan:

1. Install the ShareScan software on a network computer. You have the option to customize the database installation. For more information, see the Custom installation chapter of this guide.
2. Install ShareScan Client, if needed (for more information on installing the client, see the chapter 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 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).

   Note:
   The Model name specified during device addition can be changed anytime via the **Modify Model Name** menu item in the Administration Console: **Devices tab > <<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 ShareScan uses, refer to the ShareScan Help. To access the Help, click **F1** or click the **Help** button that is located in the upper-right corner of the ShareScan Administration Console.

Before you start

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

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

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

Notes:

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

Important!
Ensure that the ports used for both inbound and outbound network traffic are left open. See Ports to be left open topic.

Installation scenarios

Important!
The eCopy ShareScan 6.3 installer uninstalls previous version of ShareScan. With this, any separate eCopy products (Xerox TWAIN, ScanStation, Advanced FPE) are also uninstalled to facilitate proper operation of ShareScan 6.3. You have to manually re-install any of these required components.

Before running the ShareScan installer, ensure that you have the latest system updates on your machine and that Automatic Windows Updates are turned off.

Important!
Installing ShareScan to folders belonging to individual user profiles (e.g.: **My Documents**, **Documents and Settings** on older systems) is NOT recommended. When upgrading existing ShareScan versions using the relevant **Upgrade** options of the installer, ShareScan 6.3 always performs a complete installation; you can only customize the installation location (**Destination Folder** screen) and database access and Service account credentials (**Service Credentials** screen) in such cases. When you perform an upgrade on a multi-manager deployment, it is recommended that you upgrade the individual ShareScan Managers one by one. If you plan to deploy ShareScan in a High Availability cluster with multiple ShareScan server nodes, follow the instructions in the **eCopy ShareScan High Availability and Load Balancing Deployment Guide**. It is recommended to set up the individual ShareScan server nodes first, test their basic behavior and then move them into the High Availability cluster as described in the **eCopy ShareScan High Availability and Load Balancing Deployment Guide**.

Note:
Do not use square brackets (**[** and **]**) in

– user identifiers

– passwords

– database name fields

since they are not handled correctly and are removed. If you need to use these characters in the password, please consider changing it for the time of the installation.

Follow these two basic scenarios when installing ShareScan.

Install ShareScan to a clean system

Complete installation

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

   Note:
   This screen displays warnings on any possible issues that might have an impact on the proper operation of ShareScan and provides information on how to resolve them. If relevant, it also enables you to choose from more than one option such as the number of available network adapters for device-Manager communication.
5. The **Enter Product License Key** screen is displayed. Provide your Product 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 is displayed; select **Complete**:

   Automatic full installation is performed with the following features and settings:

   – **eCopy ShareScan server** is installed

   – **Microsoft SQL Server** is installed

   - SQL Server 2014 SP3 Express

   – **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

   – **%ProgramFiles(x86)%\Kofax\ShareScan6.3\Server** is the default installation path
8. The **Installation Summary** screen is displayed. Review the information and if you are satisfied with the configuration click **Install**, otherwise click **Back** .
9. Click **Finish** when the **InstallShield Wizard Completed** screen appears.

Custom installation

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

1. Perform steps 1 - 6 as described in the Complete Installation section above.
2. The **Setup Type** screen is displayed; select **Custom**.
3. The **Custom Setup** screen is displayed. Select the program features you want to install and click **Next**. The following components can be selected for installation:

   – **eCopy ShareScan Server** – mandatory component, installed in all possible scenarios, cannot be deselected. Appears disabled in the install screen.

   – **eCopy ShareScan configuration database** – select this component if you want to create a ShareScan configuration database.
   It is necessary to select this component
   – if you install a single ShareScan Manager

   – if you plan to install multiple Managers and you do not want to share the same database across them

   – if you plan to have multiple Managers and you are installing the first ShareScan Manager.

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

   – **Microsoft SQL Server** (selected by default) – select this component if you want a local installation of Microsoft SQL Server Express. Recommended for single-manager (small-scale) deployments. If you do not install this, you need to specify your SQL Server related information later.

   – **eCopy ShareScan WebClient** (selected by default) – select this component if you plan to use scanner devices with web browser enabled user interface.
4. The **Select Java Runtime Environment** screen is shown. Select your preferred environment:
   – **Amazon Corretto 8 Runtime (x86)**, or

   – **Pre-installed Oracle Java SE Runtime Environment (x86) - version 1.8**. If you select the second option you also need to specify the **JAVA_HOME path for Oracle JRE**. The installer detects your Oracle Java installation and populates this field with that path to its home folder. To modify this path click **Change**.
5. The **Destination Folder** screen is displayed. Click the **Change** button to modify the default destination folder for the ShareScan server, Kofax 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**.

Upgrade from previous version to 6.3

When the ShareScan 6.3 installer is run on a machine which has a previous version of ShareScan installed, it offers two upgrade options.

Note:
If Custom Service Credentials is set for the Agent and Manager service, the eCopy ShareScan 6.3 installer will ask for the Agent service user password.

Note:
Optimal performance is not guaranteed in case the eCopy 6.3 server is used with devices that have v5.2 JAR clients installed on them. Background Processing must be enabled for a functioning configuration of the different version server and client. This setup with legacy clients is only recommended until full transition from v5.2 to 6.3 happens.

Upgrade from previous version to 6.3

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

1. If you have a physical ShareScan installation media, insert it in the optical drive of your PC and browse to the folder where the **ShareScan6.3.exe** file is located.
   If you have a digital copy of the ShareScan installer, you can find the **ShareScan6.3.exe** file under the **Install/ShareScan** path.
2. Run **ShareScan6.3.exe**; the **Choose setup language screen** is displayed. Select a preferred language (English by default) from the dropdown list and click **Next**.
3. The **Welcome** screen is displayed. 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 is displayed; select **Upgrade from previous version to 6.3**:

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

   – **eCopy ShareScan server** is installed

   – existing **eCopy ShareScan configuration database** is updated to the 6.3 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 is displayed. Review the information and if you are satisfied with the configuration click **Install**, otherwise click **Back** .
8. Click **Finish** when the **InstallShield Wizard Completed** screen appears.

Custom upgrade from previous version to 6.3

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

1. If you have a physical ShareScan installation media, insert it in the optical drive of your PC and browse to the folder where the **ShareScan6.3.exe** file is located.
   If you have a digital copy of the ShareScan installer, you can find the **ShareScan6.3.exe** file under the **Install/ShareScan** path.
2. Run **ShareScan6.3.exe**; the **Choose setup language screen** is displayed. Select a preferred language (English by default) from the dropdown list and click **Next**.
3. The **Welcome** screen is displayed. 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 is displayed; select **Custom upgrade from previous version to 6.3**: the installer performs a complete installation, preserving configuration data:
   – **eCopy ShareScan server** is installed
   – existing **eCopy ShareScan configuration database** is updated to the 6.3 schema
   – **eCopy ShareScan WebClient** is installed (including the Apache Tomcat server)
6. The **Select Java Runtime Environment** screen is shown. Select your preferred environment:
   – **Amazon Corretto 8 Runtime (x86)**, or
   – **Pre-installed Oracle Java SE Runtime Environment (x86) - version 1.8**. If you select the second option you also need to specify the **JAVA_HOME path for Oracle JRE**. The installer detects your Oracle Java installation and populates this field with that path to its home folder. To modify this path click **Change**.
7. The **Destination Folder** screen is displayed. Click the **Change** button to modify the default destination folder for the ShareScan server, Kofax 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**.
8. Specify service credentials on the **Service Credentials** screen. Use default service accounts, or specify a different ShareScan Manager and ShareScan Agent. Click **Next**.

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

9. At this point, the user can be 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: in case the user selected custom service

accounts, as in this case the user is necessary to specify what connection method / account should be used for database connection.

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

Note:
If the connection type 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.

10. The **Installation Configuration Summary** screen is displayed. Review the information and if you are satisfied with the configuration click **Install**, otherwise click **Back** .
11. Click **Finish** when the **InstallShield Wizard Completed** screen appears.

Maintenance

If you re-launch the ShareScan installer after the successful installation of ShareScan 6.3, the **Program Maintenance** screen is displayed after you select a preferred language from the dropdown list on the **Choose setup language** screen and click **Next**. The the following options are available:

– Remove
Removes all ShareScan features (Server, WebClient). The so-called dependency packages (SQL Server, .NET runtimes, and so forth) can be removed from the **Programs / Features** manager of Windows.
Note that if you installed ShareScan 6.3 over an existing ShareScan version, removing ShareScan 6.3 DOES NOT bring back the previously existing ShareScan version.
Removing the WebClient feature of ShareScan also removes the Apache Tomcat server.

Upgrade multiple ShareScan managers

Important!
When performing multi-manager upgrade and you start to use Integrated Windows Authentication (instead of the Existing SQL Server type database authentication), then you need to use:

– Integrated Windows Authentication on all the managers you connect to the same 6.3 database

– the same windows service accounts on all the Managers you upgrade.

After you upgraded the first Manager to 6.3 with Integrated Windows Authentication, you cannot use the default service accounts for the Agent and Manager services when you upgrade the second one, but you have to specify the same Windows users you used on the 1st Manager.

Note:
For the time of upgrading multiple managers in any environment (NLB or standard), all managers should be stopped for the time of upgrading the first manager. Database modification is also done during the upgrade. When this is complete, the rest of tha 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 5.x is similar to the Custom upgrade scenario.

1. If you have a physical ShareScan installation media, insert it in the optical drive of your PC and browse to the folder where the **ShareScan6.3.exe** file is located.
   If you have a digital copy of the ShareScan installer, you can find the **ShareScan6.3.exe** file under the **Install/ShareScan** path.

2. Run **ShareScan6.3.exe**; the **Choose setup language screen** is displayed. Select a preferred language (English by default) from the dropdown list and click **Next**.

3. The **Welcome** screen is displayed. Click **Next**.

4. The **Setup Type** screen is displayed; select **Custom upgrade from previous version to 6.3**: the installer performs a complete installation, preserving configuration data:
   – **eCopy ShareScan server** is installed

   – existing **eCopy ShareScan configuration database** is updated to the 6.3 schema or a clone (copy) of the currently used ShareScan database is updated to the 6.3 schema and put in use for the upgraded installation (the actual behavior is specified on the screen detailed in step 8 below)

   – **eCopy ShareScan WebClient** is installed (including the Apache Tomcat server)

5. The **Destination Folder** screen is displayed. 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**.

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

7. The **Administrative Credentials for Database Creation** screen is displayed, 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 shown.

8. The **Database Catalog Name** screen is displayed. You have three basic scenarios:
   i. If you select the **Use current catalog for database upgrade** radio button in the first manager upgrade installation sequence, the procedure is identical with the single manager Custom upgrade from previous version to 6.3 installation scenario. In this case, the name of the database catalog remains the same (eCopyShareScan), but its structure changes hence 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 the Managers connecting to the same database are stopped during the whole upgrade process (of all the Managers).

Note:
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 case, the DBA must create a copy of the eCopyShareScan 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 iii** described below.

ii. When upgrading the first Manager, select the **Copy current catalog to perform the upgrade on the following one** radio button and specify a database name. This option makes a copy of the already existing database catalog with 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 successfully, the user must have **db_backupoperator** database-level role and DBCREATOR server level permission since these allow backup and restore operations.

iii. When upgrading the second and all further Managers, select the **Use a different existing ShareScan catalog** radio button and select the newly created / updated database, already upgraded to 6.3 level. You have to select the database catalog name provided during the upgrade the first Manager.

Note:
The dropdown 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 is displayed if the service credentials were modified. You need to provide the runtime account information for the configuration database. Click **Next**.
10. The **Installation Summary** screen is displayed. Review the information and if you are satisfied with the configuration click **Install**, otherwise click **Back** .
11. Click **Finish** when the **InstallShield Wizard Completed** screen appears.

Custom installation scenarios

ALL four components are installed (with WebClient optionally skipped)

Note:
If the **eCopy ShareScan WebClient** component is deselected, 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 selected all components (and/or optionally deselected the **eCopy ShareScan WebClient** component) on the **Custom setup** screen, click **Next**.
2. The **Destination Folder** screen is displayed. Click the **Change** button to modify the default destination folder for the ShareScan server, 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**.
3. Specify service credentials on the **Service Credentials** screen. Use default service accounts, or specify your custom service accounts for the ShareScan Manager and ShareScan Agent Windows Services. These accounts must be valid domain accounts (users). Note that while the installer supports using custom accounts to run the services, using Integrated Windows Authentication for the local database connection is NOT supported by the installer when the ShareScan Installer installs the SQL server. If you want to use Integrated Windows Authentication on a local SQL server, you have to install ShareScan first with the available installation type (i.e. using default of custom credentials with SQL Server Authentication) and then later modify the service accounts and database permissions manually. Click **Next**.

   Note:
   When you provide valid non-default accounts for the Manager and/or the Agent service and then click the **Grant** button (after the installer detected that some local privileges are not granted to the service accounts), the installer tries to grant the missing privileges.

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

4. **Use default password specified by ShareScan** or **Specify a custom password**. If you select **Specify a custom password**, you must provide a password that complies with the password policy in effect. Click **Next**.
5. The **Installation Summary** screen is displayed. Review the information and if you are satisfied with the configuration click **Install**, otherwise click **Back** .
6. Click **Finish** when the **InstallShield Wizard Completed** screen appears.

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

   Note:
   If you specified Custom Service Credentials in step iii, eCopy ShareScan 6.3 installer will ask for Agent service user password.

Microsoft SQL Server NOT installed (with WebClient optionally skipped)

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

This custom setup scenario only installs the following three components.

– eCopy ShareScan Server

– eCopy ShareScan configuration database

– eCopy ShareScan WebClient

1. Once you deselected the **Microsoft SQL Server** component (and/or optionally deselected the **eCopy ShareScan WebClient** component) on the **Custom setup** screen, click **Next**.
2. The **Destination Folder** screen is displayed. 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**.
3. Specify service credentials on the **Service Credentials** screen. Use default service accounts, or specify a different service account for the ShareScan Manager and ShareScan Agent. These accounts must be valid domain accounts (users). Click **Next**.

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

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

   You need to choose one from the following three options:

   – The default **sa** account and the default password used by ShareScan

   – The Windows identity of the user running the ShareScan installer

   – Specifying a user ID and the corresponding password (use SQL Server authentication). This can be an **sa** account with the corresponding password, or it can be a completely different user ID that is valid on the SQL Server having the proper rights for the ShareScan database creation.

   Click **Next**.

Note:
If the runtime database user (eCopy by default) already exists on a remote SQL server (either from a previous installation or because it is created by the database administrator manually), a valid password must be specified for login.

5. The **Database Catalog Name** screen is displayed. Specify the ShareScan database name here or leave the default name. Click **Next**.
6. The **Database Server and Runtime Account Information** screen is displayed. You can specify a runtime account for the configuration database.
   You need to select a method how the ShareScan services connect to the SQL Server database:

   – via SQL Server authentication, using the default user name 'eCopy' and the default password

   – via Integrated Windows Authentication, using the identity of the accounts running the services (available only if custom accounts were specified on the previous wizard screen)

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

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

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

   Click **Next**.
7. The **Installation Summary** screen is displayed. Review the information and if you are satisfied with the configuration click **Install**, otherwise click **Back** .
8. Click **Finish** when the **InstallShield Wizard Completed** screen appears.

Note:
If you specified Custom Service Credentials in step iii, eCopy ShareScan 6.3 installer will ask for Agent service user password.

ONLY eCopy ShareScan Server and eCopy ShareScan WebClient (optionally skipped) are installed

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

This custom setup scenario only installs the following two components:

– eCopy ShareScan Server

– eCopy ShareScan WebClient

1. Once you deselected the **Microsoft SQL Server** and **eCopy ShareScan configuration database** components (and/or optionally deselected the **eCopy ShareScan WebClient** component) on the **Custom setup** screen, click **Next**.
2. The **Destination Folder** screen is displayed. 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**.
3. Specify service credentials on the **Service Credentials** screen. Use default service accounts, or specify a different service account for the ShareScan Manager and ShareScan Agent. These accounts must be valid domain accounts (users). Click **Next**.
4. The **Database Catalog Name** screen is displayed. On this screen, you must specify the hostname or IP (and optionally, the instance name) of the SQL Server where the existing 6.3 ShareScan database is hosted. You must also specify the existing database name. Click **Next**.
5. The **Database Server and Runtime Account Information** screen is displayed.
   You need to provide the runtime account information for the configuration database. Click **Next**.

   Note:
   If the **Use specified credentials given to Service Accounts for database connection** radio button is selected, the database administrator has to create the database users manually, otherwise the installed system will not operate properly.
6. The **Installation Summary** screen is displayed. Review the information and if you are satisfied with the configuration click **Install**, otherwise click **Back** .
7. Click **Finish** when the **InstallShield Wizard Completed** screen appears.

   Note:
   If you specified Custom Service Credentials in step iii, eCopy ShareScan 6.3 installer will ask for Agent service user password.

   You are now ready to configure a connector profile.

User rights for database creation

This section lists the supported user right scenarios ShareScan database creation, from the least restrictive to the most restrictive.

Administrative account with 'sysadmin' fixed server-level role (e.g. 'sa')

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

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

These rights are enough to create both the ShareScan database and the login ID of the runtime account. If you are connecting to a corporate database server, and your database administrator is not providing you the credentials of the **sa** account, then the database administrator needs to provide another account for the ShareScan database installation (practically with lower

privileges), having the **dbcreator** and the **securityadmin** fixed server-level roles.

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

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

If security policy is stricter, the login ID in SQL Server for the ShareScan runtime account must be created by the database administrator manually. This manually created SQL Server login ID or Windows user name (if Integrated Authentication is used) must be used on the **Database Server and Runtime Account Information** screen of the ShareScan Installation Wizard. This manually created login needs to have a **public** fixed server-level role and it is not required to have it mapped to any database (it will be mapped to the eCopyShareScan 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 **eCopyShareScan** 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. Any name can be chosen.

– 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

The Profile Tool allows you to manage connector, service profile information, watchers and Data Publishing maps between ShareScan 6.3 Managers. You can export such profile information from a Manager, then start up another Manager, and import the profile information.

Unlike connector profiles, newly imported watchers do not automatically overwrite watchers with the same name already existing on the target machine. (These imported watchers are created as new ones.) To update a watcher via import, first you have to delete the current watcher (on the target machine) and then do the import.

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

To perform an export, do as follows:

1. Start the Administration Console.
2. Start the Profile Tool.
3. Remain on the **Export** pane.

4. Use the dropdown icons to browse to the connector or service whose profile information you want to export.
5. Right-click on the connector or service in question.
6. Select **Export connector profiles** or **Export service profiles** (as appropriate).
7. Browse to the location where you want to save the file; the generated file automatically has the .profile extension.

To perform an import, do as follows:

1. Start the Administration Console.
2. Start the Profile Tool.
3. Switch to the **Import** pane.
4. Click the **Browse** button to locate the profile file you want to import.
5. Double-click the file to start the import process.

Client-side Installation

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

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 Troubleshooting chapter.

Configuring the Xerox Device

ShareScan supports EIP-capable Xerox devices only.

Before you can use ShareScan with Xerox devices, you must install and/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).

Note:
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.

Note:
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 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 in 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 **SNMP** instead of the option from the **Discovery** list. If the autodiscovery does not succeed, use TCP/IP to add it manually.
4. Select the device you want to add.
5. Click **OK**. The device registration wizard 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 device(s) cannot be discovered and are not shown in the list on the **Add device** dialog 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.

Note:
The automatic device discovery is supported via and SNMP. If the autodiscovery 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 dropdown list pops up the user can select from.

Batch add devices

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

1. Start the 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** dropdown list; a standard **Open file** dialog is displayed 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), color (bool), a3ledger(bool), HTTPSforUI(bool), HTTPSforFileTransfer(bool)`

   Example: `10.140.200.249,Xerox,*,admin,1111,public,FALSE,FALSE,FALSE,FALSE`

   – `IP/host`: device IP address (or host name)

   – `Xerox`: must be Xerox

   – `model (or *)`: 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)`:

   – `SNMPGet(string)`: SNMP get community name (public by default; if otherwise specified on the device web administration page, the same must be included here)

   – `color(bool)`: true or false (depending on whether the device is color scan capable)

   – `a3ledger(bool)`: true or false (depending on whether the device can accept A3/ledger sizes)

   – `HTTPSforUI(bool)`: true or false (whether to use secure channel for device-server communication)

   – `HTTPSforFileTransfer(bool)`: true or false (whether to use secure channel for image transfer)

Note:
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.

Note:
For instructions about removing devices, refer to the ShareScan Help.

Install Xerox Driver for ScanStation

This section contains information on installing the Xerox ScanStation driver.

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

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

Prior to installing the Xerox drivers, install the ShareScan server; otherwise, the Xerox drivers will not work.

Make sure that you have the most current driver.

To install the driver:

1. Before running the installation program, make sure that Microsoft .NET Framework 3.5 SP1 is installed.
2. Run the installation program, `ScanStationXeroxTwain.exe`, following the instructions on the screen.

   The program installs the driver in the following location:

   `C:\%programfiles%\Kofax\Xerox Driver for ScanStation\`
3. When the installation is complete, click **Finish**.

Note:
Xerox Twain installer does not create some folders when ShareScan is installed with custom service accounts. If you have installed Xerox driver for ScanStation and your services run under custom account you have to create the missing **res\home** subfolders under **%programfiles(x86)%\Kofax\Tomcat 8.5\webapps\eCopy-Xerox\WEB-INF** path manually and set Full control rights to the custom service account before running the Configuration Tool.

To configure the driver:

1. Select **Start** > **Programs** > **eCopy Applications** > **Xerox Driver for ScanStation** > **Xerox Driver Configuration** tool. The **Xerox Driver for ScanStation Configuration** window opens.
2. On the **Device** tab, enter the host name or the IP Address of the Xerox device in the **IP Address** field.

3. In the **User Name** and **Password** fields, enter the user name and password for the device administrator.
4. Select the **Capabilities** tab and then specify the color capability of the device and whether the device supports A3/Ledger size paper.
5. Select the **SNMP** tab. The **GET** and **SET** community name values specified on this tab must match the values specified on the **SNMP Properties** page of the Xerox device. The default values on the device are “public” and “private”; if the default values have not been modified, you will not need to modify the values on this tab.
6. When you are finished configuring the driver, click **Save**.

Note:
If upgrading from a supported 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.'

Note:
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 version 6.3.

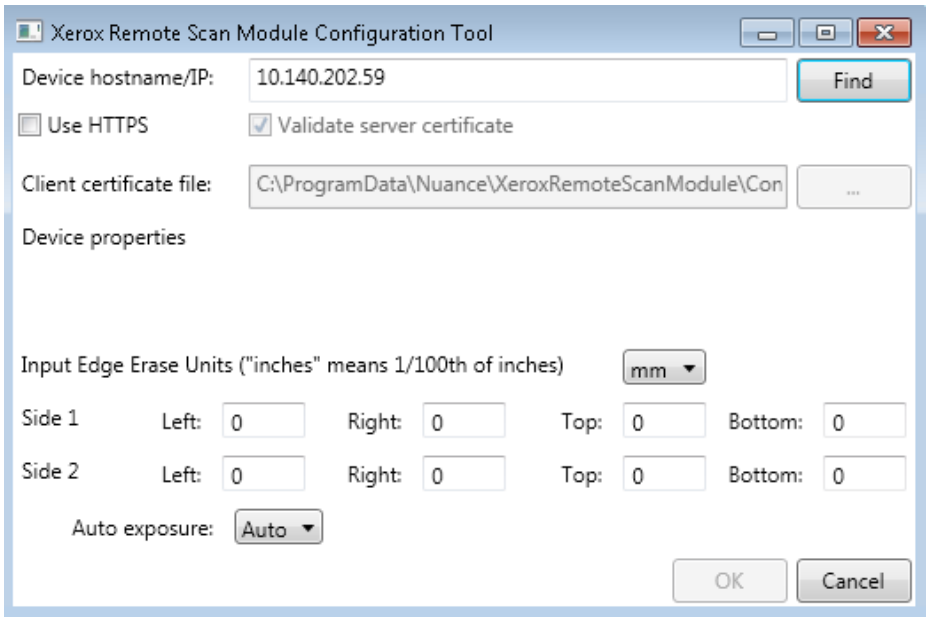
ISIS drivers

In addition to scanning via TWAIN, ScanStation also supports scanning via ISIS drivers. Please 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 problem occurs with ScanStation, please test first whether you are able to scan into another ISIS supported application.

Xerox Remote Scan Module Configuration Tool

For newer Xerox devices (featuring Xerox EIP 2.5 or above), the TWAIN driver installation is exchanged by the Xerox Remote Scan Module, which makes communication between ShareScan and the MFP device much simpler. Its configuration tool has the following parameters:



– Device hostname/IP: the hostname or IP address of the device; click the **Find** button to identify the device

– Use HTTPS: mark this checkbox to use HTTPS connection

– Validate server certificate: mark this checkbox if you want to validate the certificate; only active if **Use HTTPS** checkbox is marked

– Client certificate file: location of the client certificate file; only active if the **Use HTTPS** checkbox is marked

– browse '**...**' button: click this button to browse for the client certificate file; only active if the **Use HTTPS** checkbox is marked

– Device properties:???

– 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

Note:
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

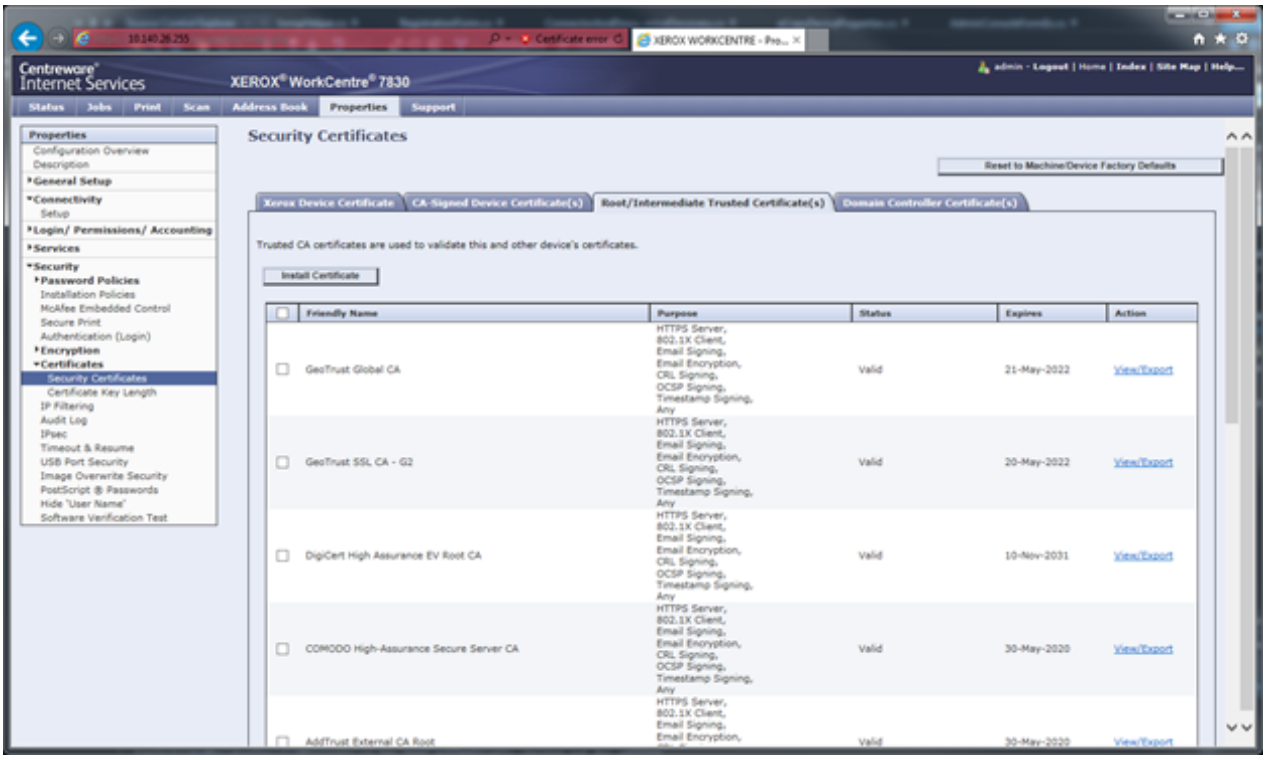
– Auto exposure: can be **Auto** or **Off**

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

In order to make it possible for the device and the PC 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 PC. 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 `.crt` file and the path of this `.crt` file should be added to the configuration tool of Xerox Remote Scan Module. Therefore the module will use this certificate when it tries to open an SSL connection.

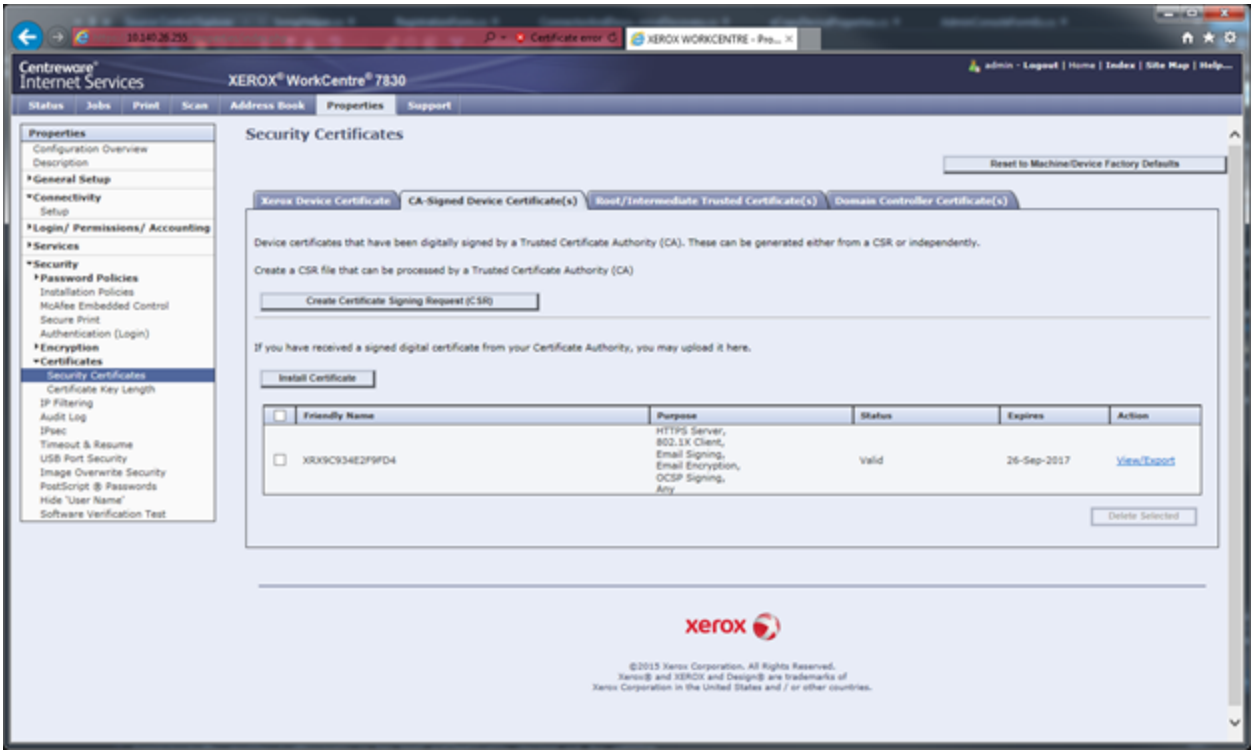
1. Get a root certificate or create one with the tool mentioned above or with any other tool.
2. Export it to a `.crt` file.
3. Open the web administration page of the device in a browser, and sign in as an administrator.
4. Go to **Security Certificates** settings and select the **Root/Intermediate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

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



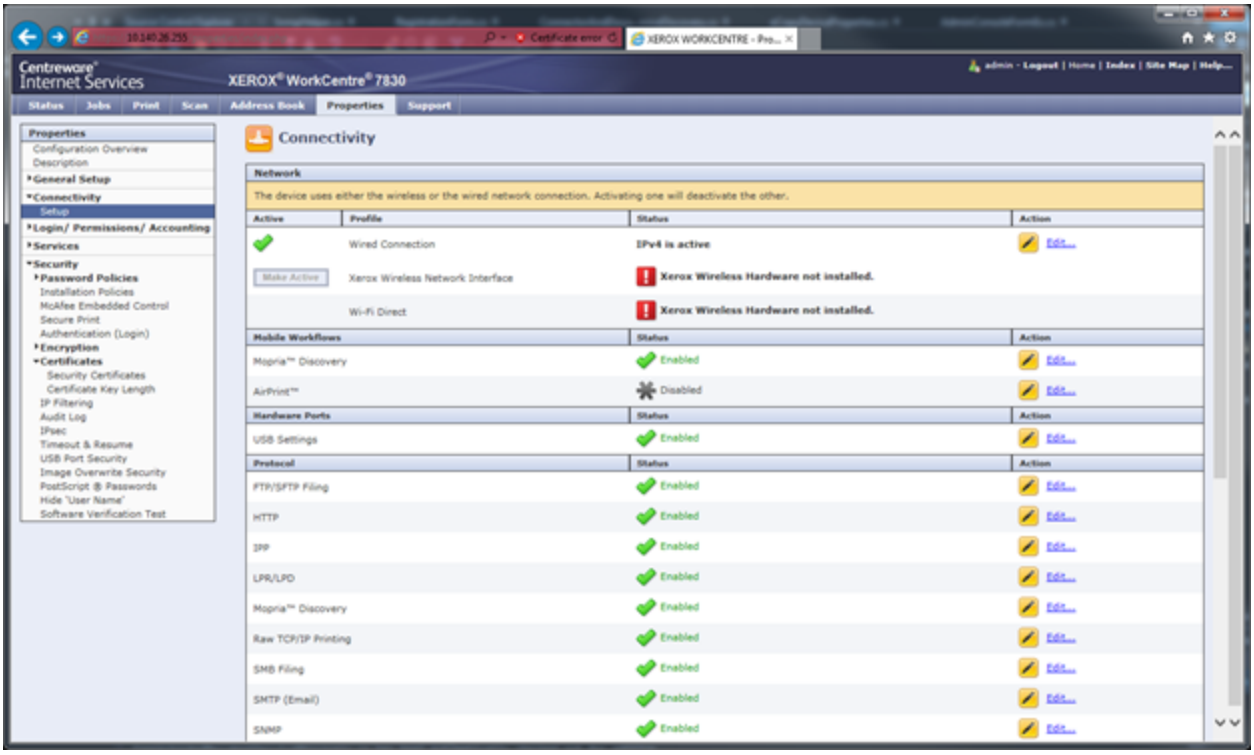
5. Click **Install Certificate** button and install the root certificate.

6. Go to **CA-Signed Device Certificate(s)** tab.

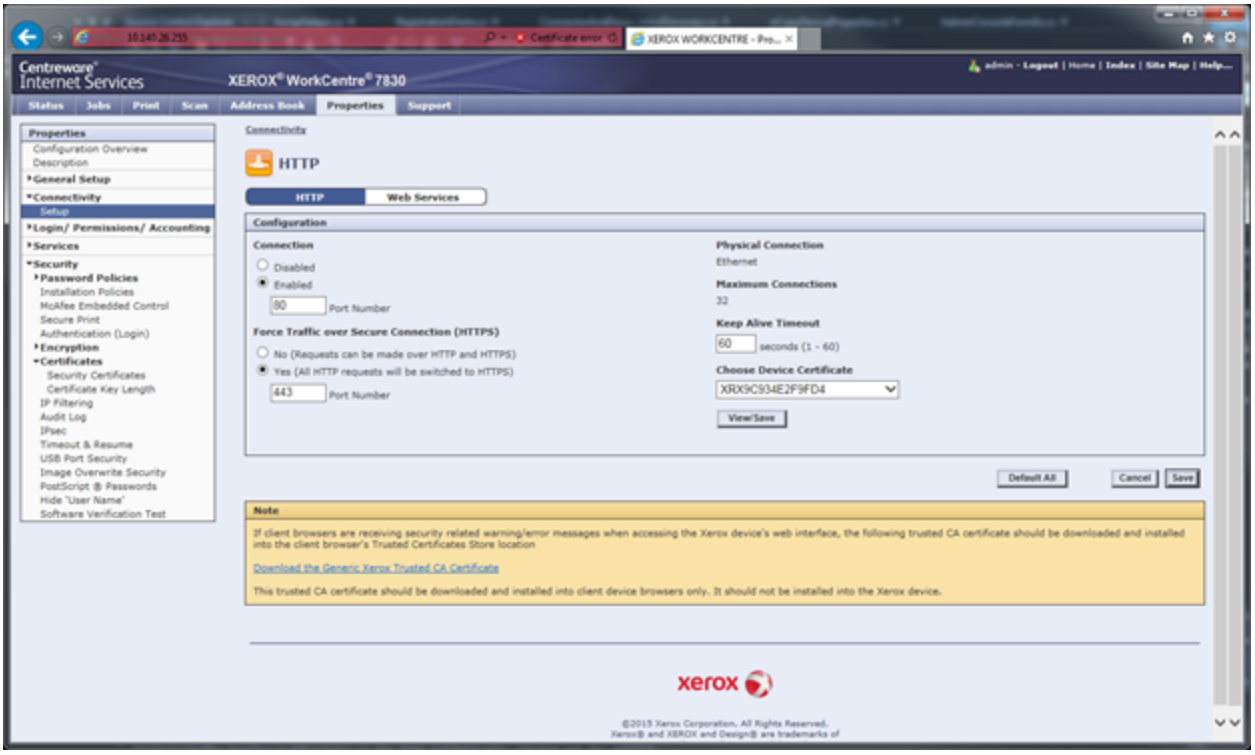


7. Click **Create Certificate Signing Request (CSR)** button and create a **Certificate Signing Request**.
8. Open this CSR by clicking **View/Export** and export it by clicking the **Export (Base-64 Encoded –PEM)** button
9. Import this CSR in the XCA tool or the tool you use for creating certificates.
10. Sign the CSR with the root certificate and export the new certificate to a `.crt` file
11. On the device administration page, press **Install Certificate** button and install this certificate.

12. Go to **Connectivity** -> **Setup** settings page.



13. Find **HTTP** and click **Edit...**



14. Open the dropdown below **Choose Device Certificate**, select your certificate and **Save** the changes.
15. In the certificate tool, create another certificate for the PC. Sign it with the same root certificate.
16. Export it to a `.crt` file and select it as an SSL certificate in the Xerox Remote Scan Module.

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

eCopy Connectors

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

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

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

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

Installation Prerequisites and Suggestions

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

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

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

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

Installation Prerequisites and Suggestions

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

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

– When the installer of the Lotus Notes client prompts you to choose between the **Multi-User Install** option and the **Single User Install** option, make sure that you select the **Single User Install** option.

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

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

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

Installation Prerequisites and Suggestions

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

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

eCopy Scan to Desktop

Installation Prerequisites and Suggestions

– Scan to Desktop involves several different components to enable users to scan and send documents to a designated network folder location for modification and storage. A “Scan Inbox” subfolder may be added to existing network home directories or the ShareScan software can create Scan Inbox folder locations. The Inbox Root (Inbox Management directory) stores the user list (`userdirs.txt`) that indicates which users have scan inboxes using Scan to Desktop and whether ShareScan has created Inbox folders; these folders would also reside under this directory.

– For detailed information on configuring Scan to Desktop, see the ShareScan Help, accessible via pressing **F1** on the Administration Console.

Note:
The Inbox **Alternate path for folder root - DO NOT set it to the user's HOME folder: (see documentation)** path pointing to the existing Network Home Directory Root Folder is NOT supported, since ShareScan modifies the permissions on the root folder.

Inbox Root Directory

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

The Inbox Root Directory should not be pointing to a user’s home directory. Choose the Scan to Desktop **Home Directory** option in the connector instead.

Note:
Network home directories configured through a login script are not supported.

ShareScanAdmin Group

An Administrative Group must be used to implement the required security. In previous versions of ShareScan, this group required the name “ShareScanAdmin”. This Administrative Group can now be given any name; however, if multiple Services Managers are pointing to the same `userdirs.txt` file in the Inbox Root Directory, the group to which the service account belongs must be identical on all those Services Managers.

The group used must be created on the domain controller for domain-based networks, on NDS for Novell networks, or on the local machine if the customer is in a workgroup environment. ShareScan uses this group when assigning permissions to the inbox Root Directory and scan inboxes and requires Full Control. Permissions assigned to the directory are as follows:

Windows (NTFS)

– Administrators – Full Control

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

– Inbox Owner – Read or Delete

Novell (Netware)

– Administrators – Full Control

– ShareScanAdmin – Full Control

– Inbox Owner – Read or Delete

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

eCopy Quick Connect

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

Installation Prerequisites and Suggestions

– When selecting a network location as a Quick Connect destination, make sure that the future users have access to the folder or folders being used as storage options. Alternatively, the administrator can use the **Logon As** function to supply login credentials.

– To deliver scanned documents to an Access database, you must disable User Account Control (UAC) on Windows 10, Windows Server 2012 or later. To disable UAC, type `c:\windows\System32\UserAccountControlSettings.exe` to the command line, and select the appropriate slider setting.

eCopy Connector for OpenText Fax Server (RightFax Edition)

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

Installation Prerequisites and Suggestions

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

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

– Delegation privileges, phone books, cover sheets, and billing codes must be configured on the RightFax server in order to be utilized by the eCopy connector for RightFax.

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

eCopy Scan to Printer

Installation Prerequisites and Suggestions

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

eCopy Connector for Microsoft SharePoint

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

Installation Prerequisites and Suggestions

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

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

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

– If your company uses a secure SharePoint site, you must install an SSL certificate on the ShareScan server.

– Dates are validated by the client regional settings; invalid date formats are not accepted.

– The connector does not fully support storing to workspaces. Storing to an Attendees location is inconsistent and may result in failure to store the scanned document.

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

eCopy Connector for EMC Documentum

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

Installation Prerequisites and Suggestions

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

– For Configuring DFC the following information is required:

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

- Port number: Default = 1489

- Repository Name

- Login Name and Password to that Repository

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

– The eCopy connector for EMC Documentum will then need the Repository chosen from the drop-down menu, as well as a user name and password. In the connector Administration, all Repositories available through that Connection Broker will now be available. The administrator should then enter a user name and password that enables browsing to all desired destination locations within the selected repository and store documents if “Login As” authentication is used.

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

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

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

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

eCopy Connector for Autonomy iManage WorkSite

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

Installation Prerequisites and Suggestions

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

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

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

ShareScan Manager includes a value for the **Preferred Server** option. If you leave this field blank or you enter an incorrect value, users will not be able to store scanned documents.

eCopy Connector for Open Text Content Server - eDOCS Edition

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

Installation Prerequisites and Suggestions

– Before installing the eCopy connector for Open Text Content Server, the Administrator must install and configure the Windows Explorer DM Extension software for Open Text Document Management, eDOCS Edition 5.1, 5.2 SP1, 6.0 or later or Hummingbird DM 5.1, 5.2 SP1, and 6.0 on the same PC as the eCopyShareScan Manager. After that, run the DM Connection Wizard.
All versions of the DM Extension software include the required DM API and the DM Connection Wizard.

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

– You must select 'Intranet Mode' (the default mode). Do not select 'Internet Mode'.

– After installation, launch the DM Connection Wizard and enter the name of your DM server.

– The eCopy ShareScan Services Manager must be on the same domain as the DM server, for the DM Connection Wizard to establish a connection with the server.

– The Administrator will need to enter a valid eDOCS DM user name and password that has the ability to store documents if 'Login As' authentication is used.

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

– When the eDOCS DM Extension Client v 5.1.0.5 SR6 or later is installed on the same computer as the ShareScan Manager (not in the same domain as the DM server), you cannot configure the eCopy connector.

– Default values that are assigned by the eDOCS DM server appear in the Client. To use a different value, you must remove the default value and then use the Search feature or the 'Search while typing' option to specify the new value.

– If a profile for an application does not appear, contact your administrator. The application may be disabled from within the eDOCS DM software.

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

eCopy Connector for Open Text Content Server

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

Installation Prerequisites and Suggestions

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

– The eCopy connector for Livelink ECM uses the Web services protocol and / or Livelink API (LAPI) for communication with Open Text Content Server.

– LAPI supports TCP/IP direct connections with native Livelink authentication. It does not support HTTP or HTTPS connections or non-native authentication methods. Native authentication using LAPI supports Livelink authentication, NTLM authentication, and LDAP authentication. The Livelink server is responsible for managing the authentication settings and the connector works transparently with the selected authentication mode.

– In **Protocol** section of **Database & authentication settings** in the Connector configuration window, the Administrator will need to provide the following information to properly configure the connector:

– If **Web services** is selected:

– **Root URL**: The root URL of the web service granting access to the Livelink server. E.g.: `https://TestContentServer:443/cws`

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

– If **LAPI** is selected:

– **Livelink server**: The Open Text Content Server-Enterprise Server name. The server entered in the **Livelink Server** field must be on the same network (LAN) or connected via a VPN (WAN) as the Services Manager. It cannot be a web-only connected server. The Livelink connector does not communication over HTTP or HTTPS; instead it uses TCP/IP and LAPI over the specified port. Even if port 80 is entered in the port field, it will not force the connector tocommunicate over HTTP or HTTPS.

– **Database**: The Livelink database name. The Livelink Database information can be found on the Livelink Administrative Site under the Database Administration section.

– **Port**: The port used by the server. The default is 2099.

Note:
LAPI protocol is not supported by OpenText Content Server (Livelink) version 16 or higher.

– If **Web services and LAPI** is selected:

– All the options can be configured that are listed in **Web services** and **LAPI** protocol sections above.

Note:
If **Web services and LAPI** protocol is selected, LAPI is used only for supporting Table Key Lookup attributes. Since **Web services** protocol supports Table Key Lookup attributes only in case of an OpenText Content Server (Livelink) 16.2 or later, LAPI is used only for supporting Table Key Lookup attributes if **Web services and LAPI** protocol is selected in **Protocol** section of **Database & authentication settings** in the Connector configuration window.
The eCopy Connector for Open Text Content Server does not support Table Key Lookup attributes for OpenText Content Server (Livelink) version 16 or higher since LAPI protocol itself is not supported by this server.

– If the Open Text Content Server environment requires a user to change password at the next logon to the system, the user must change the password at the workstation before using ShareScan. If the user does not do this, the system will display a message that the password has expired and that the user will not be able to store the scanned documents.

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

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

License devices

ShareScan 6.3 includes a Licensing Wizard, which handles the following license-related tasks.

Every device that you use with Kofax software requires a valid license. ShareScan 6.3 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 PC where the ShareScan database is installed.

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

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.)

For ScanStation systems, the local device is automatically added; then, when the administrator selects the driver, the system verifies the validity of the license file.

ShareScan includes a Licensing Wizard, which handles the following license-related tasks:

– loading licenses,

– activating licenses,

– loading activated licenses,

– reactivating licenses,

– removing licenses.

Load licenses

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

1. Click the **Load license** button of the License Wizard. The Welcome screen is displayed.
2. Click **Next** to continue.
3. Select **Download license automatically** when specifying the source. The **Automatic license download** screen is displayed.
4. Copy the license keys of the licenses to download in the text box. Click **Add** after each. When the list below is complete, click **Next**. The **Select license files to load** screen is displayed.
5. Click the **Browse** button 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.

Activate licenses

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

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

Load activated licenses

Use this option when importing already activated licenses to ShareScan.

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

Remove licenses

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

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

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

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, refer to 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 (QuickConnect) 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 logout automatically if **Session Logon** is enabled.

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

To configure a service (example – Activity Tracking)

1. Start the ShareScan Administration Console by clicking **Start > Programs > eCopy Applications > ShareScan 6.3 > 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 opens.
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.

To configure an extender (example – Forms Processing Extender)

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

1. 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 have finished designing and testing your template, make sure you enable batching in the Extender by marking the **Batch on Matched Templates** checkbox.
4. Save your configuration.

To 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 **QuickConnect**.
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**, **Location** and 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 set the index file attributes.
7. Use the **Settings** pane to configure the following:
   – display settings,
   – document settings,
   – service to be associated,
   – extender to be associated,
   – scanner settings, and
   – background processing settings.
8. Click the **Save Current Profile** button. For more information about configuring the settings for a connector, open the relevant Help topic.

To test the configuration of a profile

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 is displayed.
6. Click **Next** to continue. The Forms Processing Extender screen is displayed.
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.

Certificate Manager

The Certificate Manager is an addon tool for eCopy ShareScan, which allows you to manage the certificates required by some devices.

The tool is separate from the eCopy ShareScan installation, 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 via editing the `server.xml` file used by the Tomcat component of eCopy ShareScan.

Clicking this button displays a new window, listing all ports currently used by eCopy ShareScan, and the cryptographic protocols assigned for the specific port, if that port uses SSL or TLS.
You can use the **server.xml** dropdown 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 is displayed, 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 (for example, **Remove weak ciphers**, **Select Java 6 ciphers**, **Remove ciphers using CBC encoding**, and so forth).
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, then click the **Generate** button on the lower-right part of the window.

– **Backup certificate**: click this button to create a backup of your existing certificate. A **Browse** window is displayed, where you can select the location and filename of the certificate to be saved.

– **Restore certificate**: click this button to restore a certificate. A **Browse** window is displayed, where you can locate the certificate to be restored.

Next steps

After finishing the basic installation and configuration tasks, you can start using and customizing ShareScan via the Administration Console.

In the Administration Console, all system functions are available on the Ribbon and there are separate tabs for configuring services, connectors and devices.

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

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

– Configure one or more installed services, so that they will be available when you configure connectors and devices. There are three types of services: services that you apply to a connector, services that you apply to devices or device groups, and services that you apply to connectors and devices.

– Configure one or more profiles for the installed connectors that will be used on the scanning devices. You can create multiple profiles for each connector and you can activate each connector profile on multiple devices.

– Register ShareScan online.

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

When registering a Xerox device in the Administration Console, a dialog box is displayed, with the following options:

These options allow you to regulate the connection type between ShareScan and the Xerox device.

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 the **Install** button; 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:

- Kofax Documentum API

- Kofax Printer API

- S2D Inbox Agent

– Tomcat service settings can be viewed/modified via:
`%programfiles%\Kofax\Tomcat9\bin\tomcat9w.exe`

– During the entire installation process, do not remove the original installation media from your optical drive, even though the installer has already extracted and decompressed the required components to a temporary location. This action can cause multiple failures depending on the stage of the installation during which the removal happens.

– To configure the Lotus Notes connectors (both Mail and Fax), you have to install the Lotus Notes Client on the PC. After installing, quit the client before running the ShareScan Administration Console, as the client locks the ID file, and a running client may cause issues with ShareScan.

– Ensure that there is no Apache Tomcat on the PC you want to install ShareScan on.

– Ensure that no ports used by ShareScan (listed in the Installation Guide) are used by other web services, as that may cause connectivity issues.

– Deploying the RightFax FaxUtil on the same machine on which ShareScan is running may cause issues, therefore it is not advised.

– If the Apache Tomcat component does not start after a Java update, a PC reboot solves the issue.

– If you have multiple ShareScan Manager PCs in your deployment, it is recommended that you always use the same instance of the Administration Console to add, modify or remove connector profiles regardless of whether you are working in a cluster environment or not.

Technical support

This chapter contains guidelines on what information to provide to technical support if you encounter issues when using eCopy ShareScan.

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

– eCopy system details:

- ShareScan version number

- Service Pack number (if applicable)

- Version of ScanStation PC (if applicable)
- Product key and serial number
- Approximate daily scanning load (pages/day)
- Backend versions for all used connectors (for example, Exchange, Lotus Notes, or SharePoint)

– System specifications:

- Server OS
- Machine types
- Jar versions
- NIC speed settings
- IP Addresses

– The exact workflow performed when the issue happens

– Does it happen to all users or just specific user accounts? (if specific only, please specify in details)

– A detailed description of the workflow which helps reproducing the issue

– The following files:

- `msinfo32.nfo`
- license dump (for license-related issues)
- Logs from the ShareScan Troubleshooter Tool
- Verbose trace file for the workflow
- Client logs
- If possible, the Wireshark logs

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

Troubleshooting tips

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

– devices cannot be added in the Administration Console after upgrading to eCopy ShareScan 6.3

– Administration Console does not work with devices added before the upgrade to 6.3

– Administration Console simulator does not work

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

– Ensure that there is no Apache Tomcat on the PC you want to install ShareScan on.

– Ensure that no ports used by ShareScan (listed in the Installation Guide) are used by other web services, as that may cause connectivity issues.

– Deploying the RightFax FaxUtil on the same machine on which ShareScan is running may cause issues, therefore it is not advised.

– If the Apache Tomcat component does not start after a Java update, a PC reboot solves the issue.

– If no labels are displayed on a ScanStation deployed to a virtual machine, turn off 3D acceleration under the virtual machine settings.

– Restoring database backups created via the ShareScan Troubleshooter is not possible via the ShareScan Administration Console. Use the relevant scripts for restoring such databases.

– When upgrading an existing ShareScan 5 installation that has CAC configured, you must disable and re-enable CAC via the Administration Console after the upgrade process to ShareScan 6.3 has finished.

– If you experience slowness during authentication using Session Logon service, disabling NetBIOS over TCP/IP on the Advance TCP/IP Settings dialog of the network card can speed up the authentication process.

– 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 ManagerValue: PendingFileRenameOperations`

- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto UpdateValue: RebootRequired`

Re-enable SSLv3 in Tomcat and Java

Certain web-based MFP devices do not support TLSv1 or higher security protocols when communicating with the ShareScan Manager via HTTPS.

There are two approaches to work around this problem. Both require expert configuration skills.

1. Upgrade your device's firmware to the latest available version and verify if the desired security protocols are available.

If not, proceed as follows:

1. In Tomcat:

a. Launch the `Tomcat9w.exe` from **%PROGRAMFILES%\Kofax\Tomcat 9\bin**

b. Select the **Java** tab

c. Add the `-Djdk.tls.client.protocols=SSLv3,SSLv2Hello,TLSv1` line to **Java Options**

d. Click **OK**

e. Go to **%PROGRAMFILES%\Kofax\Tomcat9\conf** folder

f. Open the `sharescan.java.security` file for editing

g. Change the `jdk.tls.disabledAlgorithms=SSLv3, RC4, DH keySize < 768` line to `jdk.tls.disabledAlgorithms=`

h. Save the file

i. Restart services in the Administration Console.

Check if ShareScan works properly on the device after registration.

If not, then proceed to the following step:

You need to re-activate SSLv3 in Java (deactivated by default in Java Runtime Environment from ver. 1.7upd75) and in ShareScan/Tomcat as well. Exercise caution when doing these modifications.

2. In Java:

a. Go to the **<JAVA_HOME>** folder and open the `java.security` file for editing under **\lib\security**

b. The **<JAVA_HOME>** folder is typically %programfiles(x86)%\Kofax\JRE\Amazon Corretto 8\jre8

c. Remove **SSLv3** from the `"jdk.tls.disabledAlgorithms"` property. For example, change `"jdk.tls.disabledAlgorithms=SSLv3"` to `"jdk.tls.disabledAlgorithms="`

3. In Tomcat:

a. Go to the **<TOMCAT_HOME>** folder and open the `server.xml` file for editing under **\conf**

b. Locate `"<Connector port=443"`

c. Insert **SSLv3** into `sslEnabledProtocols`. For example, change `"sslEnabledProtocols="TLSv1, TLSv1.1, TLSv1.2, SSLv2Hello""` to `"sslEnabledProtocols="SSLv3, TLSv1, TLSv1.1, TLSv1.2, SSLv2Hello"`

4. Restart your system.

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 **C:\%programfiles%\Kofax\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 EIP 2.0

– Phaser 3635 MFP

– WorkCentre 5222/5225/5230

– WorkCentre 6400

– WorkCentre 7232/7242

– WorkCentre 7328/7335/7345

– WorkCentre 7346

– WorkCentre 7655/7665/7675

– 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