eCopy ShareScan® 5.1

Administration Console Help-as-PDF

1 - Welcome

Welcome to eCopy ShareScan. To access the Help-wide search function, open the Search panel.

Click here for information about getting started with the Administration Console.

Click here for information about Customer Support services.

The following documentation is available for your perusal with Nuance ShareScan:

- **Pre-installation Checklist and sizing guide** (PDF) – provides info on the issues to be addressed before deploying ShareScan.
- **Configuration Guide** (PDF) - provides vendor-specific information on seamless integration of ShareScan on various multifunction devices.
- **Installation Guide** (PDF) - contains information on installing Nuance ShareScan, including hardware and software prerequisites.
- **Administration Console help** (this document) – 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.
- **Troubleshooter Users Guide** (PDF) – contains information on how to use the ShareScan Troubleshooter, a built-in diagnostic tool of the product.
- **Release Notes** (PDF) – contains an overview of the changes for the given ShareScan release.
- **Offline Processing Guide** (PDF) - contains information on how to use the offline processing feature of ShareScan.
- **Profile Tool User Guide** (PDF) - contains information on how to use the Profile Tool to migrate ShareScan-related profiles and data between ShareScan Managers.

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

Licensing, Copyright, and Trademark information

Part of the software embedded in this product is gSOAP software.

The software in this product was in part provided by Genivia Inc and any express or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. in no event shall the author be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

Customer Support services

Customer Support services include the following components:

- Customer support for licensing, registration, and other non-technical issues
- Technical support
- Hardware RMA (Return Merchandise Authorization), where applicable

Note:

Nuance Communications does not provide hardware support. Contact your hardware dealer/distributor, or system integrator for support information.

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

The main Support page is at http://support.nuance.com, where you can obtain information about Customer Support services, hours of operation, contact information, policies, and process descriptions. In the list of products, select the eCopy product and then click **Go**. The Support Overview page opens.

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

If you purchased your software directly from Nuance Communications, check Ask eCopy for solutions to your technical problems. If necessary, open a ticket from the Ask eCopy Web site.

Contact information

US/North America

Corporate Headquarters Telephone: +1.781.565.5000

Customer Support Services Telephone: +1.781.565.4600

Outside North America

Please contact your local dealer or national sales organization.

2 - Getting Started

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, such as managing the ShareScan database.

Notes:

There is a functionality that runs only once, when the Administration Console is started for the first time: you have to specify a valid 22 character long license key during the product installation. When the Administration Console is started for the first time, it opens a dialog offering the installation of the license represented by that license key entered into the

installer Wizard screen. If you click **OK** on this dialog, the application tries to download the license from the Nuance license server, and install it (this is successful only if the computer running the Administration Console has a working Internet connection). If for any reason the download fails, you must add or import the license manually as described in the Licensing Wizard.
When the Administration Console is started, the system checks to see if the IP associated in the registry with the ShareScan Manager still exists. If not, an error message is displayed, and you have the option to update the IP address (this starts the services, but you have to reconfigure the clients), or you can close the Administration Console.

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

2.1- Configure the services

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. **Note**: Only the services that you have valid license for, will be shown in this pane.

1. Click the **Services** link.
2. Select the **Services** tab. The **Configure Services** pane displays a list of the installed services.
3. Select a service and then configure it. You can enable the service in the service's Configure pane or, later, in the Settings pane for the connector or device that will use the service.

2.2- Configure the connector profiles

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.

1. Select the **Connectors** tab. The **Configure Connectors** pane displays a list of the installed connectors. **Note**: Only the connectors that you have valid license for, will be shown in this pane. You can refresh the list of the available services by right clicking the Connectors pane and selecting **Refresh connectors** from the context menu.
2. Select the connector for which you want to configure a profile. [1]
3. Specify the settings for the connector profile and then click **Save current profile**.

2.3- Configure devices

Configure one or more eCopy devices. If you are using the simulator, proceed to step 3.

[1] Most connectors offer a Wizard option; eCopy recommends that you use the Wizard to initially configure a connector profile. You can create multiple profiles by clicking **Save current profile as**, entering a name for the new profile, and then clicking **Save**.

1. On the Ribbon, click **Add Device**. The **Discover and Select Device** window opens. For more information, see Adding devices.
2. Select the device or devices that you want to add and then click **OK**. You can also drag and drop devices onto the **Devices** tab.
3. Select one or more profiles to activate on the devices and then enable the services to be used on the devices. Click **Save**.
4. Test your configuration, either by using the built-in Simulator or by verifying the configuration at the configured devices.

3 - About the basic functions

There are four categories on the Home (basic) tab:

- Navigate
- System
- Devices
- Simulator

3.1- Navigate settings

The Navigate function enables you to navigate through the screens of the Administration Console using the **Next** and the **Previous** icons:

- Previous icon: When you click the button, the viewing area displays the previous screen where you came from.
- Next icon: When you click the button, the viewing area displays the next screen. This button is typically enabled when you go from screen **B** back to screen **A** (using the **Previous** button) and would like to return to screen **B**.

When clicked on the **Home** button, the viewing area displays the **Welcome** page:

3.1.1 - Welcome page description

Settings	Description
Link to the Services tab	Provides a link to the Services tab.
Link to the Connectors tab	Provides a link to the Connectors tab.
Link to the Devices tab	Provides a link to the Devices tab.
Link to Nuance's registration site	Provides a link to company's registration site.
Company/Product name/Link to Nuance's web site	Displays information on company, product name and provides a link to company's web site.

The primary use of the **Welcome** page is to get you started with the tool. You need to configure the Services first to be available for the Connectors and/or Devices. In addition, the Connectors need to be configured to be used for a device or devices.

3.2- About Devices

Functions in the Devices area help you to select eCopy-enabled devices, add them to the Device tab, and manage them.

You can also manage device licenses from here in the Administration Console. There are four functions in the Devices area:

- Licensing
- Add Device
- Manage
- Confirm

3.2.1 - Adding devices

This feature discovers and selects eCopy enabled device or devices using UDP, SNMP, or TCP/IP protocols and adds them to the **Device** tab.

This feature also allows you to manually detect a device. Each device that you add to the system is associated with a Manager.

Notes:

New devices from the same manufacturer inherit their initial settings from the default device.
When adding a device, be aware that the Administration Console resolves the name of the device via the DNS, and the name registered in the DNS is used to update the name of the device in the device tree. If the name registered in the DNS is different from the name that is given in the administration UI device. Thus, after adding the device to ShareScan, the name can change.

3.2.1.1 - To Add A Device To The Manager

1. Make sure that the device that you want to add is running and that the ShareScan Client is running on the device. For more information on ShareScan Client, see related Installation Guide documentation. **Note**: This is valid ONLY for the non-web (embedded clients). For web clients there is nothing additionally needed to get the device connected.
2. You can either right-click **Device configuration** and select the **Add device** menu item or click the **Add device** on the ribbon bar to discover and add eCopy-enabled devices.

   The **Add devices** window opens. The window displays available devices along with information such as the host name, the IP address, the Client software version, and the Manager that is currently managing the device.

3. If a device that you want to add does not appear in the list of available devices, choose from a drop-down list in **Discovery**, select a protocol, and click **Refresh**.
4. Select the device or devices that you want to license and then click **OK**.
5. When the system prompts you to confirm the device that you want to add to the device list, click **Yes**.

3.2.1.2 - Add Devices Settings

Settings	Description
Discovery	The following device discovery modes are available: UDP, SNMP, and TCP/IP. The default value is UDP.
Vendor	Select a vendor from a list (default value is none).
Device name/IP	If you choose TCP/IP in Discovery setting, enter a device name or IP address. **Note**: The value cannot be empty. The parameter name should follow a `hostNameOrAddress` pattern. If an invalid IP address is specified, a message `Failed to retrieve data for:` occurs.
IP range	The IP range value (From). The range of the valid IP addresses is defined by your network configuration. For detailed information, contact the IT personnel in your organization. Example: A valid IP Range is from `10.10.12.1` to `10.10.12.55`. Invalid/Unsupported IP Range is `10.10.12.1` to `10.10.13.5`.
To	The IP range value (To). The value follows an `xxx.xxx.xxx.xxx` pattern. **Note**: If you enter an invalid value, an `Invalid IP Range...verify and try again` message occurs.
Refresh	Clicking refresh button forces the Administration Console to scan the network for available devices.

Settings	Description
Devices group window	Check the checkbox on the dialog and click OK to add to the devices list. If no connectors are selected for the device, then an appropriate message is presented at the ShareScan Client. Devices list includes the following values: • Host name: The host name of the device where the client is running. Note: Not all types of devices provide the host name in this list. Instead, the IP address is shown as the host name. • IP address: The IP address of the device where the client is running. • Vendor: Vendor name of the device where the client is running. • Version: The current version of the client. In case of web-based clients, this is the current ShareScan version. • Manager: The name of the manager if the client is already configured. • Domain: The domain name in which the client is running. • Location: The location of the client, typically a description entered at the MFP. • Embedded: A flag indicating whether the client is embedded in the MFP or not (Yes/No).
Total	Total number of currently detected devices.
OK	Clicking the OK button adds any devices "checked" to the Devices tab. It does not add the devices to any group.
Cancel	Closes the dialog without adding any devices.
(Sorting)	Any column in the list can be sorted by clicking on the columns header. Once sorted, you can quickly search through the list (host names only) by clicking on the first column and start typing in the desired host name. Clicking the same column header toggles between ascending/descending order.

If the **Add Device** dialog is opened again, the devices which are already added are automatically checked and the font is in italic and has light blue background for that row, which is an indication that this device was detected in the network, but is already added to the current ShareScan Manager. **Note**: During the device addition, several Wizard screens or dialogs may appear, depending on the type of device being added.

Once the device is added and selected on the Device Configuration tab, the entire configuration UI is displayed in the viewing area (including Connector Profile selection, Settings, and Scanner).

The ShareScan Manager uses the model name to control the rotation behavior of the ShareScan Manager, when creating the output document (pages) from the scanned images. The different MFP vendors and the specific models of the vendors may show different behavior with regards the orientation of the scanned files in the different scanning modes, depending on paper size, single or double sided mode, feeding source etc.

Note:

The Model name differs from the name of the Device. The (network) name of the Device (host name) can not be changed in the Admin Console, only via the admin UI of the Device and / or in the network DNS (Domain name server).

The ShareScan Manager has a built-in configuration file called `RotationAngles.xml` (and a similar one for the ScanStation devices with the name `ScanStationRotationAngles.xml`). This describes the "factory default" values for the different vendors and models to ensure that the output pages have the correct orientation. These files are not to be changed by the user (administrator).

However, there can be new models and firmware updates that interfere with these settings and result in an unexpected rotation of the page(s) with specific combinations of the scanner settings. To resolve these issues without product updates and hotfixes, there is an override file to define rules for these special cases, called `UserRotationAngles.xml` (and `UserScanStationRotationAngles.xml`, respectively for ScanStation devices) .

If you have any issue with the orientation of the pages of the output document, contact Nuance technical support where you will be provided with appropriate documentation and support to set up the exception rules in the mentioned files.

To enable some model/device specific control features, a model name needs to be assigned after the successful addition of the device is completed. This is done on a dialog that appears automatically after the device addition. In this dialog, model names are offered to select from, but you also have the option to specify a unique name that can be any character string. This model name is used to properly set up some model-specific behaviors like rotation of scanned pages and so on.

3.2.2 - Licensing Wizard

Every device that you use with Nuance Communications software requires a valid license. ShareScan 5.1 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.

When you install a license key, you can activate the device's license immediately after you add it to the local license database (recommended), or you can activate it later. You have 30 days to activate the license after the first device is added to the system. During activation, a license is associated with a PC where the ShareScan database is installed.

It is also possible to designate a PC as a failover server that can be used in case of the failure of the PC that runs the database server used for the ShareScan system.

You need to activate a license only once. If you try to add more devices than the total number specified in the license file, the system displays an error. You need to purchase additional licenses for the additional devices.

In case you need to reinstall the ShareScan system including the creation of the configuration database, import the licenses you have activated previously on the same database server, and after the add/import, perform the activation for these licenses. Until the HID of the database server is the same, activate the licenses in case of a reinstall.

Notes:

ShareScan 5.1 licensing is different from ShareScan 4.x licensing, which was based on the association of a product key with a device. Licensing is no longer associated with a particular device, but the HID of the SQL server.

If you have reinstalled the operating system, changed the hard drive or modified the hardware of the computer used as a database server, or the database server is running on a totally different computer, then the activation will not be successful and you have to reactivate your licenses via Nuance technical support.

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

- loading licenses,
- activating licenses,
- loading activated licenses,
- reactivating licenses,
- removing licenses.

3.2.2.1 - Loading 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. Read the instructions carefully, and ensure that this is the operation you want to perform.
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 **Load** screen is displayed.
   If you selected **Import license from file** and clicked **Next**, the **Select license file to load** screen appears.
5. Click the **Browse** button to add new files to the list of files to be imported. When finished, click **Next**. The **Load** screen is displayed.
6. Click **Start** to begin loading licenses.
7. Click **Finish** to close the License Wizard.

3.2.2.2 - Activating Licenses

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

Note:

You do not need to activate the license(s) immediately to start to use ShareScan. You'll have a 30 day grace period that allows full functionality for ShareScan. Activate the license(s) only if you're sure that the SQL Server used for the ShareScan system (either the local one installed with ShareScan or an existing one) are the final one, as the activation process binds the licenses to the SQL Server machine.

1. Click the **Activate** button of the License Wizard. The Welcome screen is displayed. Read the instructions carefully, and ensure that this is the operation you want to perform.
2. Click **Next** to continue. The server name and the Hardware ID of the currently used database server are displayed on screen.
3. Check the **Use Failover Server ID for activatio**n checkbox, if you want to set up a failover database server. There are three options to specify the HWFP of the failover server:
    1. Use a previously specified ID (if there is one)
    2. Enter it manually, if you previously have run the **gethwfp.exe** tool on the PC where the failover database is installed, or will be installed. The command line tool displays a 12-character long ID you have to enter manually into this input field.
    3. If the SQL Server is already up and running on the PC you want to use as a failover machine, enter the server name (including the instance name separated with a backslash, if a named instance is used), the **sa** user name and password, then click the **Read ID** button. An **sa** account is required to perform the HWFP read operation.
4. Click **Next** to continue.
5. If you have an active Internet connection on the PC where you use the ShareScan Administrator Console, select **Automatic activation** on the **Select activation mode** screen, then click **Next**
6. Click **Start**. Automatic activation will be started via Internet. After finishing the automatic activation, the **Results** screen is displayed, showing the success or the error status of the individual licenses.
7. If you do not have an active Internet connection on the PC, select the **Manual activation** option.
8. Click **Next** to continue. The **Output file creation / Activation** screen is displayed.
9. Click **Start** to begin activation. The **Specify file output** screen is displayed.
10. Specify a folder and a file name for the ZIP file that contains the licenses to be activated. Transfer this file to a portable media or to a network share.
11. Upload the resulting file to the activation server via the Nuance activation website. Follow the instructions provided on the web page. After the successful activation, the server automatically sends

the files back and you can save and transfer the files back to the connectionless PC running the Administration Console.

12. Click **Load Activated licenses** to import the file.
13. Click **Next** to continue.
14. Click **Finish** to close the License Wizard.

3.2.2.3 - Loading 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. Read the instructions carefully, and ensure that this is the operation you want to perform.
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.

3.2.2.4 - Reactivating Licenses

Reactivation is necessary when the hardware running the database server is replaced, or when the whole system is rebuilt and the same licenses are re-used on the new system, having a different hardware for the SQL database Server. In the latter case, the licenses should be loaded to the empty system as described above, and they will not be activated on this new system. As those licenses have been activated previously, Reactivation is needed instead of automatic or manual activation.

1. Click the **Reactivate** button of the License Wizard. The Welcome screen is displayed. Read the instructions carefully, and ensure that this is the operation you want to perform.
2. Click **Next** to continue.
3. Check the **Use Failover Server ID** for activation checkbox. There are three options to specify the HWFP of the failover server:
    1. Use a previously specified ID (if there is one)
    2. Enter it manually, if you previously have run the **gethwfp.exe** tool on the PC where the failover database is installed, or will be installed. The command line tool displays a 12-character long ID you have to enter manually into this input field.
    3. If the SQL Server is already up and running on the PC you want to use as a failover machine, enter the server name (including the instance name separated with a backslash, if a named instance is used), the sa user name and password, then click the **Read ID** button. An **sa** account is required to perform the HWFP read operation.
4. Click **Next** to continue.

5. If you have an active Internet connection on the PC where you use the ShareScan Administrator Console, select **Automatic activation** on the **Select activation mode** screen, then click **Next**
6. Click **Start**. Automatic activation will be started via Internet. After finishing the automatic activation, the Results screen is displayed, showing the success or the error status of the individual licenses.
7. If you do not have an active Internet connection on the PC, select the **Manual activation** option.
8. Click **Next** to continue. The **Specify file output** screen is displayed.
9. Enter the output file name and the path of the collected licenses.
10. Click **Next** to continue. The **Output file creation** screen is displayed.
11. Click **Start** to create the output file.
12. Click **Finish** to close the License Wizard.
13. Send the resulting file to Nuance Technical Support with your reactivation request. After processing the request, the reactivated licenses will be sent back as a zip file, and can be loaded into the system via the **Load activated** function (described above).

3.2.2.5 - Removing 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. Read the instructions carefully, and ensure that this is the operation you want to perform.
2. Click **Next** to continue. The **Select licenses** screen is displayed.
3. Select the license(s) you want to remove, then click **Next**.
4. Click **Start** to remove the selected license(s).
5. Click **Finish** to close the License Wizard.

3.2.3 - Generating a license report

The license report helps you to 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.

3.2.3.1 - To Generate License Report

1. Select the **License information** tab.
2. Go to the **Advanced options** tab and click **License report** .
3. Browse and save the `*.DMP` file.

3.2.4 - Device connection management

The Manage function enables you to manage the connection of devices for which web-based management has been enabled. You do this using a web page that is provided by the device. The installation guide for your device provides you with information about support for web-based clients.

3.2.4.1 - To Manage The Connection Of A Device

1. On the Devices tab, select the device and right-click on it.
2. In the pop-up menu, click **Manage**. The Management screen appears. (The **Manage** menu item is grayed out if the device does not support web-based management).

Note:

This is only available for the devices with web-based Management enabled.

3.2.5 - Confirming connection of devices

By clicking the **Confirm** button in the **Devices** pane you can confirm connectivity of attached devices with current ShareScan Manager.

The device configuration window appears with the list of Devices and Device groups.

You can use this feature when the host name of a device has changed (on the device, via the web-based management of the device or in the network configuration) to make sure that the new name is read and stored in the ShareScan database. If the name of the device has changed, after the **Confirm** operation the device is presented with the new name in the **Devices** pane.

3.3- About the simulator

Click the **Simulator** button to access the ShareScan Client in Simulator mode.

The simulator is a web-based dynamic preview tool (Tomcat web server URL: http://127.0.0.1:8080/ShareScan).

Use it to:

- Test the settings you have specified in the Administration Console.
- Discover new features of the current program version.
- Learn and practice software usage.
- Verify issues: should you encounter problems while using a physical device, testing whether you experience the same in the simulator provides helpful information for technical support.

The main advantage of the simulator is that you do not have to publish your settings to a physical device every time you intend to test changes.

Notes:

Only Internet Explorer 7 or later is supported.

Ensure that http://127.0.0.1 is added to the list of Trusted sites of Internet Explorer.
If you install the web client, the Simulator function of the ShareScan Administration Console defaults to using the web client for the Simulator. If you want to use your ScanStation for the Simulator in this case, you must set the **UseScanStationAsSimulator** DWORD registry setting to 1 under **HKLM\SOFTWARE\Nuance\ShareScan**.

3.3.1 - Using the simulator

On the left side of the simulator you can choose from the following settings.

3.3.1.1 - The Simulator Settings

Settings	Description
Resolution	The following resolution types are available: 200, 300, 400 and 600 DPI.
Paper size	The following paper sizes are available: Auto, Letter, Legal, Ledger, Statement, or A4.
Output paper size	The following output paper sizes are available: Letter, Legal, Ledger, Statement, Executive, A3, A4, A5, A6, B4, B5, B6, or Auto.
Orientation	The following orientation options are available: Portrait, Landscape, Same as Originals.
Mirror	Set to Yes to flip pages horizontally.
Inverse	Select Yes to invert page colors.
Deskew	Set to Yes to straighten pages.
Scaling	Scaling is available between 10 and 100 percent.

The simulator is designed to be a generic presentation of a device display. The actual display on your MFP depends on its capabilities and may differ from the simulator. Using MFP device emulator programs inside the Administration Console is not supported.

Since the presence of an actual device is not required to use this tool, no actual scanning is performed during simulator use. The simulator uses sample TIF or JPEG images stored in the file system. Image parameters (size, color mode, etc) are read from the sample files, therefore scan settings (paper size, resolution, etc) inside the simulator may not take effect.

To replace sample simulator images, complete the following steps:

1. Install ShareScan.
2. Browse to the ShareScan installation directory.
3. Locate the `\Tomcat 7.0\webapps\ShareScan\WEB-INF\test` subfolder.
4. Replace the images with your own samples. All samples must be of the same format. Follow the naming convention `Image<n>.<ext>`, where '`n`' is a sequential number and `<ext>` is TIF or JPG..

Note:

Scanner settings (like paper size, resolution etc.) on the Simulator main screen have no effects on the images streamlined to the Manager for processing, as these images are coming from the folder described above.

3.4- About the System area

The system area provides access to the system related features and activities.

There are four categories on the System tab:

- Settings
- Activity monitor
- Reporting
- Starting, stopping, and restarting a ShareScan Manager .

3.4.1 - ShareScan Settings

The Settings area specifies properties that apply to all devices connected to the current ShareScan Manager. Clicking the **Settings** button brings up the UI in the viewing panel as a property grid with various categories.

3.4.1.1 - Configure Settings

The control used to display the data is a property grid, which is typically displayed with categories and properties. The categories are in bold and do not hold a control on the right hand side of the grid. Each category can have one or more properties and can contain multiple sub-categories. Clicking each property enables its control for typing (if it is an editable field) or for selection.

3.4.1.2 - Configure Settings Properties

Section	Field	Description
ShareScan Manager	Port number	ShareScan Manager's listening port number. The default value is 9600.
Scanning mode (embedded, non-web devices only)	Enable Start button	Enables the Start button to be used to initiate scanning on a device with ShareScan embedded (non-web client) software.
Encryption	Password minimum length	The minimum number of characters that make up the password. When you specify the minimum password length, remember that the longer the password, the more difficult it is to break. Minimum password size must be in the range 1 to 45. The default value is 1.

Section	Field	Description
Password must be alphanumeric	Requires that passwords include a combination of characters and numbers. Mark Yes to ensure that passwords are not dictionary words and are not easily guessed. The password must contain at least one character and number.	
Searchable text	OCR Languages	The language(s) you want the searchable text engine (OCR engine) to use. At least one language must be selected that will be used for scanning documents. Default is the language specified under Language in the Soft keyboards field.
	OCR Mode	Select faster or most accurate search. The default value is Faster.
Secure delete	Enable secure delete of temporary files	Enables complete deletion of temporary image files from the PC running the Services Manager. When this check box is selected (Yes), ShareScan writes over the files in the `ShareScanTemp` folder multiple times with random characters.

Section	Field	Description
Regional and language settings)	Client display language	Select a language from the list to be displayed at the Client. Default language is English (United States). Note: All the Clients connected to the Manager displays the same language. Selecting a language per device or client is not supported.
	Add language	Adds a new language to the System glossary. The Administration Console and the Clients can run in different languages. Selecting a Client Display language does not affect the Administration Console's language. Refer to the Glossary Tool for additional languages.
	Remove language	Removes a language from the System glossary. Removing language does not affect the Administration Console's language as the given languages cannot be removed. Note: BEFIGS languages cannot be removed.
	Formats	To change the way the client displays numbers, currencies, dates, and time, select an entry from the format list. The default format is English (United States).
	Soft keyboards	Select a keyboard from the list to change the input language at the Client.
	Language	Allows you to select a keyboard language to be used at the Client. Default language is English (United States).
	Default .com entry	The default extension for the `.com` key on the soft keyboard, such as `.com` (maximum four characters).
	Add more entries	Used to specify additional extensions presented to include in the list that appears when you press the arrow next to the `.com` key. Additional entries can contain more than eight characters. To add or remove extensions for the `.com` key: 1. Enter data directly into the list and press the `Enter` key to add more entries. 2. Select an entry and press the Delete key to remove an entry. 3. Choose between the following keys in a drop-down list: `.com`, `.edu`, or `.org`.

3.4.1.3 - Customer Information Settings

Settings	Description
Customer information	Browse and add a custom image to display at the client (MFP). The `PNG` and `GIF` file formats are supported. To delete the image, click the left side of the column and press the `Delete` key. Note: Image must not exceed 140x50 pixels.
Contact	Include the following contact information: • Phone: The phone number. • Fax: The fax number. • Email: The email address. • Support email: The support email address. • Web: The Web site URL.

The **Save** button is not enabled until a change is made in the property grid. Once the **Save** button is clicked, you are prompted to restart the Manager for the changes to take effect.

3.4.1.4 - Advanced ShareScan Settings

Settings	Description
... (Browse)	Click this button to access the **Advanced ShareScan settings** dialog.
Shared manager settings	Using these settings, you can micromanage numerous ShareScan-specific settings, which were previously controlled via editing the registry, including (but not limited to) automatically confirming devices, regulating client and device (re)connection timeouts, output creator behavior, and OCR behavior. As these settings are shared across all Managers connected to the specific Administration Console, only change them when you have created a backup of the existing settings. When you select a setting, the description text at the bottom of the dialog panel details the behavior of the setting.
<PC name> - <IP address>	Allows you to control the PC-specific ShareScan-related settings, which were previously controlled via editing the registry.
Refresh	Click this button to refresh the values of the settings.
Reset settings	Click this button to reset the ShareScan default settings.
Save and close	Saves your changes and closes the **Advanced ShareScan settings** dialog.
Cancel	Discards your unsaved changes and exits the dialog.

3.4.2 - Activity Monitor

The Activity Monitor enables you to monitor activity between one or more devices and the ShareScan Manager. This is useful for finding performance bottlenecks as it shows all activity and timing information in real time without the overhead of writing to a file.

To access and manage the activity log

1. Choose **Activity Monitor** in the **System** group of the **Home** tab. The **Activity** area displays a list of all requests and status information.
2. Click **Start monitoring** or **Stop monitoring**.
3. In the **Filter** list, select **Monitor all devices** to view activity for all ShareScan enabled devices or select a specific device whose activity you want to view.
4. Send a text version of the activity log to a file, right-click the list and then select **Send to file**.
5. The `Activity Monitor successfully written to file` message appears and you can see the location where the log file is saved. Click **OK**.
6. Click **Clear** to clear all existing entries from the activity log.

3.4.2.1 - Activity Monitor Settings

Settings	Description
Start Monitoring	Click this button to start monitoring.
Stop Monitoring	Click this button to stop monitoring.
Filter	Select none to view activity for all ShareScan enabled devices or select from a list a specific device whose activity you want to view.
Clear	Clears all entries.
Activity	Shows all Activity entries. You can send a text version of the activity log to a file by right clicking the list and selecting Send to file option.
Device	Shows a Device type.
Date/Time	Date is presented in `MM/dd/yyyy` and time in `AM/PM` format.
Devices Connected	Lists all connected devices. Refresh rate for this field is five seconds.

3.4.3 - Reporting

The Reporting function enables you to display the total number of pages scanned. The report includes activity for all devices connected to a ShareScan Manager or for a single device.

The Reporting function displays the total number of scans done from a device on a particular day in a graphical (Bar Graph) representation.

For all reports Previewing, Printing, and Exporting of base reporting data to XML is supported. If the report generates more than 10 data points (elements), the report is split across multiple pages and **Previous** and **Next** buttons are displayed for navigation.

3.4.3.1 - To View A Report Of Scanning Activity

1. In the console tree, under **System** select **Reporting**.
2. Select the appropriate option:

- Device: Displays the total number of pages scanned at the selected device. After selecting a device, specify the time period for which you want to create the report.
- Manager: Displays the total number of pages scanned at each device connected to the selected Manager.

3. Click **Print** to print the current bar graph or **Export** to save the data report in the XMLformat.
4. Click **Refresh** to update the graph to reflect recent activity.

3.4.3.2 - Reporting Settings

Settings	Description
Manager	Selects a Manager. The Select All option selects all Managers.
Device	Selects a Device or a Simulator.
Period	For Device reports, the Scans per Month or Day are displayed and the reports can be created for: Previous Day, Current Day, Previous Month, Current Month, Past 3 Months, Past 6 Months, Past 1 Year, and Date Range.
Type	For both ShareScan Manager and Device reports, the following types of charts are available: Vertical Bar chart, Horizontal Bar chart, and Pie chart .
Status	For Single Manager reports, the Devices can be filtered by: • Active only. • Inactive only. This feature is not available for reports with Multiple Managers selected.
From	Selects a starting date. The date is presented in MM/dd/yyyy.
To	Selects an ending date. The date is presented in MM/dd/yyyy.
Print	The ShareScan Reporting module allows you to print reports showing the Black and white, Color, and Total scans processed per device for selected ShareScan Managers or by individual devices based on the selected ShareScan Managers.
Preview	The ShareScan Reporting module allows you to preview reports showing the Black and white, Color, and Total scans processed per device for selected ShareScan Managers or by individual devices based on the selected ShareScan Managers. When the Preview button is selected, Page setup is displayed that prompts for selection of Print options. The following Page Setup settings are available: • Paper (Size and Source). • Orientation (Portrait and Landscape). • Margins (Left, Right, Top, and Bottom in inches). • Printer (connect to printer using a network or choose from a list). After selecting OK, a Print preview window displays all pages of the report before printing and the Final Report page displays summary page presenting data in a text format.

Settings	Description
Export	When the **Export** button is clicked, a **Save as** dialog is displayed. This allows the report data to be saved in the `XML` format to the specified file locations. The File name is pre-populated using a prefix based on the report type and a suffix based on the host name and IP address of the Manager or Device, for example `Report_Previous Day_TDC_00001(192.168.1.10).xml`.
Refresh	When the Refresh button is selected, the report is refreshed.
Display area	Displays Bar charts and reports data messages.

3.4.4 - Starting, stopping, and restarting a Manager

The ShareScan Manager runs as a Windows service. You can start, stop, and restart the ShareScan Manager from the Administration Console.

To switch between ShareScan Managers, click the **Remote Management** button, which displays a list of ShareScan Managers registered in the database to which the Administration Console is currently connected. The ShareScan Manager that you are configuring is grayed out.

Also, you can check the currently managed ShareScan manager instance if you look at the status bar of the Administration Console (at the left-lower edge of the window).

Double-click or search for a ShareScan Manager by specifying a name in the **Search by name** or **IP address** field. When the Manager name appears in the list, click the button next to it. The system prompts you to save any unsaved data and gives you an opportunity to terminate the operation. The status bar reflects the new Manager information. After confirmation, the configuration data of the selected Manager will be read into the Administration Console.

You can **Start**, **Stop,** or **Restart** the ShareScan Manager currently being configured.

Note:

This also involves starting, stopping, or restarting the Tomcat service.

4 - About the advanced functions

There are three categories on the **Advanced** tab:

- Configure (Timers, Auto Sync, Database, Preferences, and Tools)
- View details (Services, Connectors, Devices)
- Console language

These features are assumed to be used occasionally.

4.1- Timers

Configure the inactivity timers for the user interface presented at the device. Timer values are in seconds. Click **Timers** on the **Advanced** pane of Administration Console to open the **Configure Timers** window.

4.1.1 - Configure Timers

All the timers have a range 0 - 360.000 seconds, that is, 10 minutes maximum.

Note:

Only numeric numbers are allowed for the timers. Zero (0) implies that the timer is disabled.

The timers are affective as soon as the Session Logon/Main Form is displayed.

4.1.1.1 - Configure Timers Settings

Settings	Description
System forms	Configures system forms: • Session Logon: Default is 30 seconds. • Main: Default is 60 seconds. • Scan More: Default is 120 seconds. • Encryption: Default is 60 seconds. • Advance File Naming: Default is 60 seconds. • Additional Fields; Default is 60 seconds. • System Dialogs: Default is 30 seconds. • Redirect: Default is 30 seconds.
Connector forms	Configures Connector forms. By default, the timer defined in a Connector form is overridden by the values in the Connector forms category. If you want the timers defined in a Connector form to override, check this feature. If checked, and the Connector form does not have a timer defined, the timer in the previous window are added automatically. • Connector forms: All Connector Forms - applies to all Connectors. Default is 60 seconds. • Connector dialogs: All Connector Dialogs - applies to all Connectors. Default is 30 seconds. • Use Connector timers: Set to True if you would like the timer defined in a Connector (if present) to override the previous values.

Settings	Description
Auto restart ShareScan Manager	Automatically restarts ShareScan Manager: • Time: Sets the time when the ShareScan Manager should restart automatically. • Frequency: Sets the day when the ShareScan Manager should restart automatically. • Enabled: Enables/Disables the automatic ShareScan Manager restart. If set to Enabled, grays out the Time and Frequency options. In case of numerous or long offline jobs, ensure that the Auto Restart option is disabled to prevent the possibility of losing the offline jobs.
Save	Saves the changed data and closes the dialog.
Cancel	Cancels the configuration and closes the dialog.
Defaults	Set to Yes if you would like to restore to default timers that overwrite your existing settings.

If the client is already displaying any of these forms, a refresh code is sent out to the clients to get the form with the new timer values.

Note:

Manager restart is not required.

4.2- Auto Sync

You can automatically synchronize the configuration data for services and connectors across all the managers connected to the current database with the Auto Sync feature.

Note:

The Auto Sync feature is set to **Off** by default. Also, all connectors and their dependencies must be installed on all managers if AutoSync is to be used. If AutoSync is **On**, ensure that the device groups across the Managers in the system have unique names.

4.2.1 - Auto Sync settings

Settings	Description
On	When saving a profile when AutoSync is ON, edited on any of the Administration Consoles, the profiles are automatically published to all managers connected to the same database. Changes are reflected immediately on all devices currently using this profile. If the client is busy, changes are reflected when displaying the Session Logon/Main Form. All the devices across all the managers connected to this database share all the connector profiles. **Note**: You cannot choose a connector profile selectively to be shared across manager/devices (either you share all or none). **Important**: The first Administration Console that you turn on becomes the master to start with. Ensure that this setting is turned on only on a single Administration Console Once Auto Sync is set to On, you can save the profile (service/connector) from any Administration Console. That is, the profiles currently on the administering manager override any existing profiles across all managers. This means that in the database, all the connector profiles are shared among all the managers (instead of duplicating the profiles).
Off	When you enable the Auto Sync function, you share the configuration data for the services, connector profiles, and connector settings with all ShareScan managers in the current database. At any point of time if you choose not to share the profiles across managers, you can uncheck the Auto Sync feature that duplicates the profiles across managers and breaks the share. **Note**: Existing settings are now lost. You can backup your database before enabling Auto Sync to save existing settings. For example, if there are two Administration Consoles running (pointed to the same database) and if you turn Auto Sync on from Admin 1 and go to Admin 2 and try to save any profile, the following message occurs: `A new profile has been detected and the AdminConsole has to reload before saving any changes.` The changes made prior to the re-load are lost. At this point, the Administration Console reloads the new data (which was saved from Admin 1). You can now make changes and save it back. **Note**: The consequence of the previous behavior is that the concurrent editing of the profiles is, even if it is not prohibited, not encouraged. While managing the same system with two instances of the Administration Console concurrently from two different workstations is possible, it is not recommended, mainly because there are many pieces of information that are displayed in the Administration Console, but not refreshed immediately when the data is changed in the underlying database by another Administration Console.

4.3- Database Configuration

To take a backup or restore from a previous checkpoint, use database configuration option by selecting the relevant database. The entire configuration of each Manager is stored in the database.

From Administration console, click **Database** and launch the **ShareScan database configuration** window.

4.3.1 - ShareScan database configuration

ShareScan database configuration allows selection of a different database. Use ShareScan database configuration to detect and browse to any eCopy-enabled database.

The ShareScan agent and manager use SQL authentication when communicating with the ShareScan database. The ShareScan database uses the default SQL TCP port (1433) for communication.

4.3.1.1 - ShareScan Database Configuration Settings

Settings	Description
Server Name	The Server name. Select a SQL server instance in the network for your connection. By clicking the Server Name button you can detect eCopy-enabled SQL server instances.
User Name	The user name.
Password	The password.
Time-Out	Connection timeout in seconds, indicating the amount of time required to wait before the application can give up when connecting to the database. The default value is 30 seconds.
OK	Saves the changed data. The database connection string in the registry is set with the new SQL server details and the Administration Console will always connect to the new one.
Cancel	Cancels the configuration and closes the dialog.

4.4- Backing up the database

You can quickly perform a complete backup of the current configuration and also be able to restore the configuration from an existing checkpoint.

Enter the following connection and location information for your backup:

4.4.1 - ShareScan database backup settings

Settings	Description
Action	Choose Backup.
Data source	The data source is displayed.

Settings	Description
User name	The user name.
Password	The password.
Location	Displays location (for example `C:\Program Files\Microsoft SQL Server\MSSQL10.ECOPY\MSSQL\Backup`)
File name prefix	You can rename file name prefix. Default name is `Backup`. The file is saved as a `*.BAK` file.
File format	Default file format is `Prefix - Database - MMDDYYY - HHMMMAM/PM`.

4.5- Database Restore Wizard

ShareScan 5 provides a quick and easy way to restore databases by using the Database Restore Wizard, accessible via the Administration Console. To restore a database, follow the steps below.

1. Click the **Restore Database Wizard** menu item. The Welcome screen is displayed.
2. Click **Next**. The **Specify destination server** dialog is displayed.
3. Select the server to be restored.
4. Enter the username / password to access the server. Note that the user account must have administration (**sa**) rights on the target server, as a database is created and set to Trustworthy during the restore process.
5. Click **Test connection** to check the supplied credentials.
6. Click **Next**. The **Select backup file to restore** dialog is displayed.
7. Enter the folder path and file name of the backup file you want to restore. Note that the file has to be located on the computer itself running the SQL Database Server that is the target of the restore operation. That is, if you restore the database to a local SQL Server, the backup file can be on this machine, but if you want to perform the restore on a remote server, you have to ensure that the Backup file is on that remote server, and you have to specify the path of the backup file on that server.
8. Click **Start**. The **Results** screen is displayed.

4.6- System preferences

The Preferences function provides you with several user interface options. Clicking the **Preferences** button displays a list with three options:

4.6.1 - Minimize to tray on exit

When this option is selected and if you try to shutdown the Administration Console, the console hides itself by minimizing to the system tray. This means that the Administration Console is still running but is just not visible as a visible application on the desktop (does not show up on the taskbar).

The following message appears at the system tray:

```
Administration Console is still running. Right-click on the icon below to view options.
```

Complete one of the following options to re-launch the hidden Administration Console:

- Right-click the system tray icon, which brings up a small menu, and select **Open ShareScan Administration Console**.
- Double-click the system tray icon (Administration Console icon).
- Click the shortcut available in **Start** and then **Programs**, which launches the already running instance.

Complete one of the following options to shutdown the Administration Console:

- Click the **Minimize to tray on exit** function and right-click the **Close** button.
- Close the Administration Console, right-click its icon on the system tray, and select **Exit**.

4.6.2 - Show Welcome Page at startup

If you always want the Administration Console to remember the last page that you access and to redisplay it when you start the console, select this option. By default, this option is not selected, that is, the icon is not highlighted.

4.6.3 - Auto-Confirm Devices at startup

With this option selected, the Administration Console confirms the connectivity and configuration of all the devices at startup, and it also updates the device (network) name of the devices from the system DNS (Domain Name Servers). If you have numerous devices connected to the Manager the Admin Console is managing, it is not recommended to have this setting turned on, as the checking of devices may take a significant amount of time. You can always right-click an individual device, and select **Confirm**.

4.7- Data Publishing Mapping tool

Various components publish data using the ShareScan Manager Data Publishing interface. Connectors use this data to authenticate backend, to send the final document to its destination, and to store the final document. Potential data sources include ShareScan Manager, in-house document services, and third-party document services.

The Data Publishing Mapper tool in the ShareScan Administration Console enables you to map published values to values requested by connectors. ShareScan Clients, with a user interface or without a user interface, can use the mapping information.

To access the tool, select the **Advanced** tab, click **Tools** in the Configure area, and then select **Data Publishing Mapper**. The **Data Publishing Mapper** dialog box appears.

4.7.1 - Data Publishing Mapper settings

The keys published by the ShareScan Manager, by document services, and by third-party services, along with information about them, appear in the first three columns in the grid; connector keys, along with information about them, appear in the last three columns in the grid. The tool displays the warnings icon if source keys (published keys) and destination keys (connector keys) do not match. For the keys to match, their type and format must be the same.

The following table summarizes the settings you use to map a published key to a connector key.

Note:

You cannot modify the type or the format of keys published by ShareScan Manager or by Document Services.

Settings	Description
Published Key	You can add a key manually by typing a key name in the Published Key cell.
Type	You can edit the Type value only for published keys that you add manually. The following types are available: Boolean, Datetime, Float, Integer, and String.
Format	You can edit the Format value only for published keys that you add manually, and only for some types of keys. The following formats are available: • Date format (default is `MM/dd/yyyy`). • Time format (default is `None`). • String format (default is `None`). Note: You cannot modify the format of the Boolean, Float, and Integer types.
Display area	Displays the publisher of the key, such as "System", and any additional attributes.
Connector key	If a key name is duplicated in the Published Key list or the Connector Key list, the key name has an index associated with it in the list. At run time, the system uses the actual key name, not the key name with the index. At run time, ShareScan Manager converts incoming published keys to connector keys for the specified connector profile and adds them to the publishing interface. Connectors can access the values from the publishing interface.
Type	Not modifiable.
Format	Not modifiable.
Display area	Displays the publisher of the key, such as "System", and any additional attributes.
Open	Enables you to open an XML file to load publishers' keys.
Delete	Enables you to delete an entry.
Save	Enables you to save the mapping table.

Settings	Description
Filter	Enables you to filter the keys that appear in the table: • Published Keys: Enables you to select the filter that you want to apply to the Published Keys in the table. Show All displays all keys from all publishers and their profiles. Common Keys displays keys that are common to all the profiles for the System publisher. • Connector Keys: Enables you to select the filter that you want to apply to the connector keys in the table. Show All displays all keys from all publishers and their profiles. Common Keys displays keys that are common to all the profiles for the System publisher. Default displays only the keys that are specific to a connector profile. The filtered keys appear in a drop-down list in the Published Key and Connector Key columns. When you apply a filter and then click a new cell, the tool displays only the items that correspond to the filter.
Dialog Pin/UnPin button	Clicking the Pin button makes the window a topmost window, if its current status is "Not on Top". If the current status is "On Top" and you click the Pin button, the position is no longer "On Top".

4.7.2 - DataPublishing XML for Mapping

Third-party services can publish their mapping variables in an XML file. If the variables are not published in an XML document, you must enter them manually.

The keys can be published for specific profiles or can be published as common keys that are applicable to all the profiles. If a profile-specific key and a common key the same ID, the connector uses the profile-specific key. The ShareScan Manager uses the common key format for all other profiles at run time.

4.7.3 - Use case example

This use case scenario presents a way for configuring the SMTP Mail connector of ShareScan to use Data Publishing with the values derived from the Forms Processing Extender.

1. Start the ShareScan Administration Console.
2. Start the Forms Processing Extender.
3. Open the form you want to use.
4. Create three anchors on the document, as well as zones for the **To**, **From**, **Program**, and **Student ID** fields. The end result should look similar to this:
5. Save your changes.
6. Navigate to the Data Publishing Mapper, and map the the **To**, **From**, **Program**, and **Student ID** fields to the SMTP Mail connector, ensuring that the Published Keys for the respective fields are mapped to the correct connector keys: for example, Published Key **To (FormsProcessingExtender.ELS)** should be mapped to connector key **SMTPMail_To (LDAPandSMTP.auth)**.
7. Close the Data Publishing Mapper.

8. Navigate to the **Logon/SMTP** tab of the **Properties** menu of the SMTP Mail connector profile you want to use. Set **None: Send from generic e-mail address specified by Data Publishing** as **Authentication**, check the **Allow user to modify** checkbox, and enter the default generic email and SMTP server settings you want to use
   This will allow the connector to use the relevant Data Publishing values from the **From** field.
9. Configure the **Sending options** tab of the connector to utilize the **$$SUBJECT$$** (for **Default Subject** field) and **$$NOTE$$** (for **Default Note** field) tokens (Student ID and Program Data Publishing keys), and select **Default recipients and Data publishing** from the **Data publishing** dropdown menu.
10. Save the changes you made to the connector profile.
11. Send the document through the SMTP Mail connector. The validation screen of the Forms Processing Extender will display the correct values.
    The From form of the connector should also automatically recognize the relevant value based on Data Publishing.
    The **Send** form will display the relevant, configured **To**, **Subject** and **Notes** values.

4.7.4 - Batching in ShareScan

ShareScan allows you to implement batch-based routing and indexing in concert with Data Publishing for a number of connectors. For detailed, connector-specific steps, click here.

4.8- Activity Tracking report tool

The Activity Tracking report tool provides quick and easy access to the tracked activity in the form of an UI instead of writing to a flat file. If the Activity Tracking report is configured in the **Services** tab and enabled for a device, all the scan job activity information is recorded into the database and is presented with a user interface with all the information.

When the Activity Tracking function is enabled for a device, Manager generates a log file. This file is in XML format and enables easy processing with many of the available tools.

4.8.1 - To configure the Activity Logging function

1. In the console tree, select **Devices** > `<device name/IP address>`.
2. Select **Activity Tracking** in the **Services** tab and then **Enabled**.
3. Specify the settings and click **Save**.

From Administration Console, under **Advanced**, click the **Tools** section to open the Activity Tracking report tool. The Activity Tracking dialog appears.

4.8.2 - Activity Tracking settings

The Activity Tracking tool allows you to view the basic columns or extend the grid by right-clicking and selecting columns, such as File size, Document type, Total documents, and so on. Clicking an individual row displays additional information about the Scan Job in the bottom panel.

Settings	Description
Select Manager	This tool displays by default the activity for all the devices (which have the service enabled) connected to the selected Manager. Clicking it displays a list of Managers. Use this function to see the activity of devices configured for different Managers. This window does not list all the devices for every Manager. It is assumed that you know which device or devices are configured with which Manager.
Filter by	This is a filter based on a Device, Connector, Date Time, or the authenticated user (choose the filters appropriately). The filter works as an "and" condition and displays only those rows based on the condition selected. Once the filter settings are set, every further request will use those settings, until a new set of filters is created, replacing the old ones. Thus, only a single set of filter criteria can be activa at any given time. The Select one or more filters dialog appears. Enter the following values: • Date Time: Presents date and time of the job successfully sent. The display is locale-specific date and time. An icon (attachment) is visible in front of the Date Time field if Document Tracking is enabled. Date and time are presented in `MM/dd/yyyy` and `AM/PM` formats. • Device information: Device name and Device IP address of the device from where the job is performed. • Authenticated user: Session Logon username or the username published by the Connector. **Note:** The username published by the Connector supersedes the Session logon username. • Connectors: You can filter by the connectors used for this job. • Status: You can filter by All, Success, and Failure. • Apply: You can apply the settings.
Export	Exports the filtered list to an XML file. The export process uses the currently set filters when creating the xml file.
Refresh icon	Fetches the new transactions and scan job activity from the database.
Dialog Pin/UnPin	Clicking the Pin button makes the window a TopMost window. Unpinning it removes it from being a TopMost window.
Date Time	Date and time of the job successfully sent.
Device name	Device name and device IP address of the device from where the job is performed.
Authenticated user	Session logon username or the username published by the Connector.
Connector	Name of the Connector used for this job. Profile name and the button text (also known as display name) is displayed in the details panel when the row is clicked.
Total scans	Total number of pages scanned before any processing, page removal, and so on is applied.

Settings	Description
Destination	Filled in by the Connector in use. Example: If using Exchange connector, the recipients list will be displayed. If using a Fax Connector, either the recipients or the Fax numbers is displayed.
Status	For a successful job, this column has Success as the value. If the profile in use has Offline Processing enabled, this field will contain either the success or the failure message. For a Failure as the value, a detailed message is available.
Display area	Provides information on Activity Tracking entry settings.
Items per pages	Use this control to regulate how many records are displayed per page in the search results. You can use the arrow icons at the bottom of the table to navigate between the result pages, or you can enter the page number in the **Page** field to directly jump to a specific page.
Additional columns	To view additional fields in the columns, right-click in the list view control, to bring up a menu and either select each individual column or click Select all: • Document type: The following formats are supported: TIFF, PDF, and JPEG. • Document size: Size of the final document in kB. If multiple documents are generated due to batching, the size is the total size of all the documents combined. • Total documents: Total number of documents generated for the job. • Document encryption: Indicates whether the document created is encrypted or not (Yes/No). • Searchable text: Indicates whether searchable text is performed or not (Yes/No). • Blank Page removal: Indicates whether blank page removal is enabled or not (Yes/No). • Batching: Indicates whether batching is enabled or not (Yes/No). • Bates/Endorsement: Indicates whether Bates/Endorsement is enabled or not (Yes/No). • Select all: You can select all fields at once.

Any column can be sorted in an ascending or descending order by clicking the column header. Rearranging of the columns is not provided. Only Adding and Removing the extended columns is supported.

If Document tracking is enabled for any of the Connector Profiles, an icon is added to the first column of the row for that scan job, indicating that the document has been tracked. Hovering over the attachment icon will display the name and location of the tracked document.

Double-clicking the attachment prompts the Administration Console to open the document (with the default PDF viewer on the computer) if it has access to the Document tracked location. If the location cannot be accessed, an appropriate message indicating the error is displayed.

Final documents have the name of the final document or documents sent out by the Connector. If multiple documents were created with the same name, and the tracked copy already exists with the same name in the Document Tracking folder, the timestamp is appended to the file name to provide a unique name for the tracked copy.

If the Connector renames the file name passed to it by the Manager, it is the Connector's responsibility to publish that information to the Manager for tracking purposes. If the Connector does not publish the renamed files, the filename or filenames generated by the Manager are displayed.

4.8.3 - Activity Tracking operation

The scan job activity is written to the database after the Connector sends the final document to its destination successfully. By the time the Redirect form is displayed, the transaction is being written to the database in the background. In case of an error sending the document using the Connector, since the Redirect form is not displayed, the activity is not written to the database. This means that only successful transactions and activity are being recorded.

When a Connector profile has Offline processing enabled, the final document creation and processing is performed in the background (Error message or Redirect form status is not available).

In this case, the following scenario can happen:

- If the final document is created successfully, but could not be sent out to its destination using the Connector, the activity is logged into the database with an error message returned by the Connector along will all the additional information about the scan job.
- If the final document creation failed, then the activity is logged into the database with an error message returned by the Manager along with all the additional information about the scan job.
- If the final document was created successfully and sent to its destination using the Connector, the activity is logged into the database with a `Success` message along will all the additional information about the scan job.

A part of the Activity Report has the data filled in by the Connector at run time. It is the Connectors responsibility to fill this information using the Publishing Interface.

4.8.4 - Migrating Activity Tracking data

In case you want to use your already-existing Activity Tracking data on a newly-installed ShareScan version, you can migrate the data by following the steps below:

1. Launch the **ActivityTrackingReport.DataMigration.exe** tool, located in the **Server/Tools** folder of your ShareScan installation. The tool uses the current connection string from the registry, and uses that to create a new SQL table for the exported data, which will be available on the newly installed ShareScan Manager.
   Enter an **sa**-level **username/password** combination on the UI of the tool.
   You can use the following command line arguments for the tool:
   - /ConnectTimeout (only set if your database is large-scale, and has exceedingly slow connection)
   - /DataSource (by default, taken from the registry)
   - /InitialCatalog (by default, taken from the registry)

- /CommandTimeout (this parameter regulates the timeout period of the migration script)
- /BatchSize (this parameter regulates the number of records to migrate per copy operation)

4.9- Profile Tool

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

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.

4.10- Viewing details of services, connectors, and devices

The **View details** menu displays additional information in a grid view on Services, Connectors, and Devices. The following information is displayed for the currently configured Manager:

4.10.1 - View details settings

Settings	Description
Name	The name of Services, Connectors, and Devices.

Settings	Description
Description	The description of Services, Connectors, and Devices.
Version	The version number.
Vendor	The vendor's name.
Location	The location of Services, Connectors, and Devices.

Clicking a function displays the details in a window inside the Viewing Area and shows the Tab Control on the left side with the appropriate tab selected.

4.11- Console language

The **Console language** menu can be found in the Administration Console under the **Advanced** bar.

Console Language provides a quick access for you to change the locale of the Administration Console without re-installing the product.

4.11.1 - Changing the language of the Administration Console

The display language of the Administration Console can be switched between the given languages at any point of time by simply selecting the language from this category.

The Administration Console application must be restarted after changing the user interface language.

Note:
English (United States) language is a default language.

5 - About configuring services

The Administration Console enables you to configure and administer Managers, Connectors, Services, and scanning devices. You can create profiles for a service and associate them with Connector profiles. When you scan a document using a Connector with an associated service, the document is scanned, processed by the service, and then passed to the Connector workflow.

5.1- Document services

Document services are image and document processing add-ons. Document service is a type of Connector with an exception that this component does not send the documents to any destination. Document Services are used for:

- Enhanced Image Cleanup (punch hole removal, black border removal, and so on)
- Indexing
- Batching based on Barcode
- Document Building

Note:

Document service is a “Post Scan/Pre-Connector” component (always called/executed after scanning is done and after all the services are displayed, but before calling the Connector.
In ShareScan 5, the Document service operations are always performed before the first connector screen is displayed (if there is any), even if the connector profile is configured as offline.

To learn more about Document services, contact your ShareScan vendor.

5.2- About connector services

Connector services are services that can be applied to a Connector.

There are three categories in connector services:

- Bates/Endorsement services
- Image Control services, consisting of the following main parts:
  - Image Control service
  - Barcode Recognition service
- Document tracking services

5.2.1 - Document Tracking service

The Document Tracking service is located on the **Configure services** tab under the **Connector services** section.

If the Document Tracking service is enabled for any of the Connector profiles, an icon is added to the first column of the row for that Scan Job in Activity Tracking, indicating that the Document has been tracked. Hovering over the attachment icon displays the name and location of the tracked document. Double-clicking the attachment attempts the ShareScan Administration Console to open the document, if it has access to the location of the document. If the location cannot be accessed, an appropriate message indicating the error is displayed.

5.2.1.1 -

Setting	Description
Configured	Configuring Service: Document Tracking: • Checked (Yes): Allows a device to use the Document Tracking service. This option creates a black and white PDF file, without encryption or searchable text information. The file name for the document is added to the Activity Tracking log. • Unchecked: The device cannot use the Document Tracking service. All the fields and properties are disabled.

Setting	Description
Folder location	The full path and file name for the folder. The location must be in the current Windows domain or in a trusted Windows domain (it can be even on the local machine where the ShareScan Manager is running, but you have to make it a shared network folder with the proper access rights. Click the button on the far right side in the folder location value area to select file location. The Browse for folder window appears that allows you to browse the network for a shared folder. If you type in a folder location, make sure you use a UNC format (**\\servername\foldername**) – a mapped drive format cannot be used.
Credentials	You must have access rights to the specified location. Enter the following credentials to access the Activity Tracking folder: • User name: User's login name. • Password: User's password (hidden characters). • Domain: The domain associated with the user's login name and password.

5.2.2 - The eCopy Image Control service

The eCopy Image Control service is an eCopy document service designed to enhance the eCopy scanning and image capture process. This service enables you to make corrections and clean up scanned images and thus reducing the need to rescan documents. The functions include despeckling (removing noise), straightening pages, cropping, smoothing characters, removing halftones and colored backgrounds, and thickening/thinning scanned lines. Removing lines and enhancing text quality is often needed to prepare text in a scanned document for Optical Character Recognition (OCR) operations. For poor quality scans or documents, you may need to perform multiple functions such as straightening pages, despeckling, and removing lines.

5.2.3 - Configuring Image Control

The Image Control service enables you to save a collection of settings as a profile. You can then associate a Service profile with the Connector profiles, which allows the Connector to use the functionality of the service

The Image Control Service is installed with a default profile that you can modify. However, if you plan to use the service with multiple connector profiles, you may find it easier to create custom service profiles that match the requirements of the connector profiles. is installed with a default profile that you can modify. However, if you plan to use the service with multiple connector profiles, you may find it easier to create custom service profiles that match the requirements of the connector profiles.

5.2.3.1 - To Create A Service Profile

1. In the console tree, select **Configure services** > **Image Control**.
2. Select the **Image Enhancement** tab and then select the settings that you want to use to improve the readability of your document (see Image Enhancement Settings).

3. Click **Save** or **Save current profile as** to select or specify the profile name in the **Save Profile** window.
4. Click **Save**. The system saves your settings as part of the Service profile, or creates a new profile.
5. After creating a Service profile you must associate it with a Connector profile to enable the service functionality to be used by the Connector (see Associating a service profile with a Connector profile).

5.2.4 - Image Enhancement settings

Use the **Image Enhancement** tab to configure the settings that you want to apply to the scanned documents.

5.2.4.1 - Image Enhancement Tab

Option	Description
Convert to B&W	Converts color or grayscale images to black-and-white. This option opens the Black and white and Thicker • Auto threshold: Automatically defines threshold. • Manual threshold: The value us between 0 and 255. The default value is 50. Note: Higher values can cause the image to be darker. The exact value that you need depends on the pape scanner brightness setting.
Black and white	The Black and white option allows you to remove as follows: • Smooth characters: Smoothes the edges of text. This improves the image's appearance and reduces the and pits on the edges of characters. This option improves Optical Character Recognition (OCR) accurac storage needs. • Remove halftones: Black-and-white scanned images use dithering (often called "dot shading") to simulat removes areas of dot shading, including black-on-white shading. Use this feature to change a `TIFF` file fr • Remove lines: Removes all vertical and horizontal lines detected by the service. This can be useful whe • Despeckle: Removes speckles that are smaller than the pixel size defined in the Size in pixels field. This not touching anything else in the image. It allows you to remove very large speckles without harming text size that is too large, you can unintentionally remove small text and sequences of periods, called "dot lea Note: Because these operations cannot be undone, it is recommended that you initially specify a
Thicken or thin	Enhances scanned images that use too low a contrast threshold or too light a background. If scanned files enables you to thicken or thin the image: • None • Thin: Looks at every black pixel in the original image and removes one pixel around it. This makes single • Thicken: Looks at every black pixel in the original image and then adds one additional pixel around it in ev and along both diagonals). This makes single pixels "grow" into small dots, expanding the borders of text

Option	Description
Color and grayscale	The Image Enhancement feature in the Color and grayscale group box can be applied to all image types. Th black and white in order to use those functions that only work with black and white images. If the source im conversion is ignored. • Straighten page: During scanning, straightens the image using detected text as the basis for alignment. I alignment issues. • Auto-orient: Allows you to set the page orientation automatically. • Remove borders: Removes borders without page cropping. • Size in pixels: The size is between 0 and 100. The default value is 1.
Hole Punch removal	Automatically detects the location of the punch holes on the image and removes as follows: Remove left, R Remove bottom.

Notes:

Profile settings apply to all pages of a scanned file.

6 - The eCopy Barcode Recognition Service

The eCopy Barcode Recognition Service is an eCopy service designed to enhance the scanning and image capture process. The service enables you to split files at barcodes and use the barcode data to rename the file. Also, if your business workflow demands it, the service can pass scanned files to document management systems and legal applications.

The ShareScan Administration Console enables you to configure and administer ShareScan managers, connectors, services, and scanning devices. ShareScan enables administrators to create profiles for the service and associate them with connector profiles. When a user at the device scans a document using a connector with an associated service, the document is scanned, processed by the service, and then passed to the connector workflow.

6.1- Improving barcode quality

In the eCopy environment, the print quality of the original document as well as the scanner settings can have a significant impact on the ability of the software to read barcode data.

ShareScan then passes control of the scanned document to the service, which extracts the barcode information. The service passes the barcode information to ShareScan, which uses the information to split the document and name each of the resulting files. The service does not alter the image; therefore, if the original document is of poor quality, or if the scanning quality is poor, the service's ability to recognize the scanned barcodes is less accurate.

eCopy suggests the following practices to increase the quality of scanned barcodes:

- Visually inspect the barcodes in the original document. Look for bars that are touching each other or that are full of dots. Use an image processing tool to zoom in on or to magnify the barcodes.
- Print barcode pages on a laser printer at a resolution of at least 600 dpi.
- Increase the resolution of your scanning device to 300 dpi, or higher.
- Use the eCopy Image Enhancement Service to improve the quality of the image. For more information about this service, contact Nuance.

6.1.1 - Configuring batch-based indexing for Quick Connect

If you have eCopy Quick Connect, you can use batch-based index values. This enables you to create index files with separate barcode values for each batch by assigning a base name (**Data publishing** option in the **Template settings** window) to the position of the barcode.

All Publishing Names also have batch information available for eCopy Quick Connect™ to use.

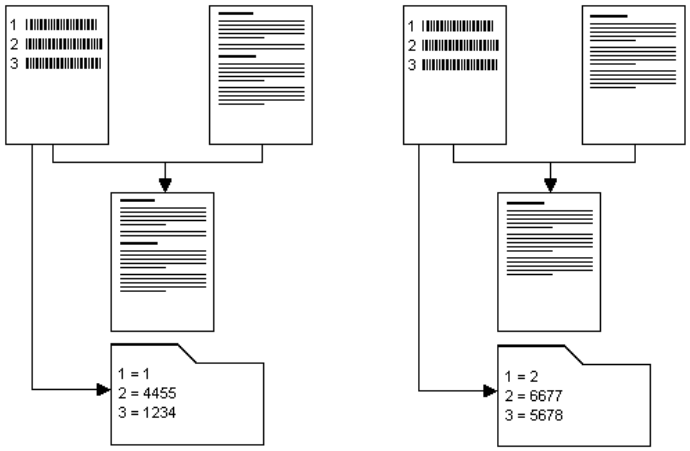
Note:
Only the first value found per publishing name is published for the session.

For example, a document is divided into two batches. It begins with a page that contains three barcodes and is split by another page that also contains three barcodes. On both pages the barcodes follow the same sequence but have different values:

Batch-based indexing example

Barcode Number	Batch-based index value	Index value, page 1	Index value, page 2
1	Document number	1	2
2	Locator	4455	6677
3	Extension	1234	5678

The following diagram shows the four page document and how, after processing, the scanned document is stored with the correct index information.



When you configure a device and select this connector profile, you must then select the corresponding Document service profile that you set up in the Barcode Recognition Service (see Associating a service profile with a connector profile).

6.2- Data Publishing

Data publishing functionality is used for:

- Passing specific metadata information from the device and services and between eCopy connectors.
- Configuring to map fields within any service or connector which can use the information.

This includes Bates numbering, fields captured using a Document service and metadata, filename and file path information that can then be tied to similar metadata fields or applied to the a body of text. Through the use of Document services or any other service or connector, information is "captured" and then categorized and mapped to fields in any connector, per document, real time, or asynchronously.

When a connector's profile is configured for "No User Interface", it would like to tell the ShareScan system and document sources about the data required to successfully send or store a document. A document source can use this information to ensure it sends required values and that data is formatted correctly (length, range, and so on). The ShareScan Administration Console uses this information to map published value names to those the connector's profile look for.

Indexing takes place before the document is split. The service calculates the barcode index number based on the sequential position of the barcode in the document. The first barcode has an index value of 1, the second has an index value of 2, and so on.

Indexing is done using the **Data publishing** option in the **Template settings** window. For more information, see Template settings.

6.3- Template settings

The **Page Templates** tab shows all the templates for your ShareScan Manager. The same template can be used by multiple profiles. You can move a template into the **Active Page Templates** list for use by the current profile. The purpose of this is to match the active templates to the scanned page based on their order in the active list.

Templates can be moved up and down to reorder the list. In general, the more restrictive or specific templates should be at the top of the list so they are matched before more general templates are tried.

Templates can also be removed from the **Page Templates** list. This deletes the template permanently and makes it unavailable to other profiles.

6.3.1 - Page templates settings

Option	Description
New template	Specifies the type of the full page template. The Barcode page dialog appears where you can specify the settings of the template.
Edit template	Modifies the settings of an existing template. The same dialog appears as in the previous case. It is initialized with the settings of the selected template.
Remove template	Allows deleting defined templates from the list.
Move up and down	Changes the order of active templates. The buttons have effect on the right side list only meaning that the client attempts to match the templates with pages in this order.

6.4- Specifying the full page template settings

Select and open one of the templates in the editor with the **Edit** button or click the **New** button to bring the **Template settings** dialog for initial setup. The **Template settings** dialog displays the following options:

6.4.1 - Template tab settings

	Description
	Specifies the name of the template. You can refer to the template by this property. This value also defines the name of the template file where the definition is saved.
	Defines the barcode properties on the given pages.

When you define a barcode based template the following controls have to be filled up:

	Description
	Specifies the types of the barcodes. **Note:** The types are not fully independent from each other. For example, if the UPC-A barcode type is selected, then the EAN-13 type is also selected automatically. If the EAN-13 type is deselected, then the UPC-A type is also deselected. This behavior comes from the limitation of the Aspose engine as it does not recognize UPC-A type if EAN-13 is turned off. The drop-down items checkboxes allow multiple selections (all types supported by Aspose engine are listed).
	Specifies the orientation of barcodes. The following options are available: • Horizontal • Vertical • Horizontal and vertical (default)
	You can set as many data publishing keys (maximum is 10) as many barcodes are expected on the page. The associated list box supplied with in-place editing capability shows the defined keys; the toolbar buttons control adding, editing, and removing the keys and also changing their order. Renaming the keys is possible by clicking the selected item.

6.4.2 - Barcodes tab settings

Group	Setting	Description
Layout search order		Layout search order defines the order in which multiple barcodes in the same zone are indexed. The options are as follows: • Top to Bottom • Left to Right (default) • Right to Left
Barcode indexing	**Delimiter**	The delimiter character splits a barcode into multiple barcodes at each delimiter. This allows more than one piece of information to be published from one barcode.
Barcode restrictions	**Always require checksum**	Set to always require checksum as barcodes can include a checksum to help validate the value. In this case, barcodes without a checksum are ignored.
	Length	Minimum and maximum length setting filters out bad matches. Select the following values to: • Minimum length: Set a minimum length between 2 and 16. The default value is 4. • Maximum length: Set a maximum length. The default value is 999.

Note:

Global Barcode settings defined on the **Barcodes** tab apply to all barcode zones.

6.5- Understanding document splitting

You can set up page handling rules for all the active templates in the **Document Splitting** tab.

6.5.1 - Document splitting display

Option	Description
Template	When a template matches a page, its rules are applied. Only one template is used per page (the first template in the list that matches).
Barcode page removal	ShareScan has a feature for page removal in a special case when the double-sided paper documents in a job are separated by full page barcode pages. Typically, the backside of the barcode page is blank and does not belong to the original document. This blank page has to be dropped from the batch if double-sided scanning job runs on the client. The Document Splitting tab on the main panel contains the list of the defined templates. The Barcode page removal column provides three options if the selected template is a barcode page: • Disabled (default) • Enabled • Enabled double-sided scan **Note:** The client workflow has to change accordingly. To apply the option to a batch, the connector checks if a double-sided scan job runs (see `IPublishing.DoubleSided` bool value). The blank page detection algorithm is applied to the page next to the barcode page and it is removed only if the page is really blank as it prevents from data loss.
Split at page	The document can be split into multiple documents at this page.
Split by value	This column indicates the regular expression that the recognized value of the barcode has to match. This value is not set by default when you create the data publishing field. If the value is not set, the document splitting is performed on pages matching with the template independently from the actual value of the barcode.
Override default file naming	The split document can be named according to the current ShareScan file naming settings, or they can be overridden here. The format of the filename is displayed and can be clicked to bring up the file naming dialog (see File naming).

6.6- File naming

On the **Document splitting** tab, if split on page is checked and override default file naming is checked, the file format string becomes a clickable link, which opens the **File Name Dialog** (FileNameDlg) window.

6.6.1 - File name dialog

Option	Description
Name/Type/Length/Default	By clicking these settings, the >File name field editor dialog window appears.
Format	Construct a name format out of multiple name fields. The `<yyyyMMdd>` value is default. Fields can be created, edited, removed, and reordered.
Preview	A preview is displayed.
If file name already exists	Create unique file name, for example `_1`, `_2`, and so on. All file name conflicts at runtime are resolved by appending a number to the end until it becomes unique.

Clicking **New** or **Edit** brings up the **File Name Filed Editor** dialog.

6.6.2 - File name field editor settings

Option	
Name	Displays a name.
Type	You can pick from a list of predefined field types plus each of the published data fields they hav • Alphanumeric: This type allows you to define a fixed string of text. • Batch number: This type displays the current batch index and lets you specify the number of • Date: You can pick from predefined date formats. The `<yyyyMMdd>` value is default. • Device name: This type displays the runtime device. You can choose a default name and a m • Page number: This type displays the page number and lets you specify the number of leading • Separator: Separator is a streamlined Alphanumeric which allows you to define a character to • Time: You can pick from predefined time formats. The `<HHmmss>` value is default. • Published data: This type displays published data. You can choose a default name and a max

6.7- About device services

Device services are services that can be applied to Device(s) or Device Groups.

The following categories are available in Device services:

- Activity Tracking
- Common Access Card (CAC)
- Cost Recovery

- Identification
- Session Logon

6.7.1 - Activity Tracking service

Activity Tracking service is accessed from the **Configure services** tab in the **Device services** section. Activity Tracking service tracks the success of the send, the recipients, and the one who sent the document. It provides quick and easy access to the tracked activity in the form of an UI.

The Activity Tracking service enables you to perform the following tasks:

- Configure the Activity Tracing function.
- Configure additional Activity Tracking fields.

The Activity Tracking service writes detailed information about each job to a log file. For more information, see Activity Tracking Report under **Advanced > Tools**.

6.7.1.1 - Activity Tracking Settings

Setting	Description
Configured	Allows the device to use the Activity Tracking service when selecting the Yes check box; or disables the device to use the Activity Tracking service (also disables all fields and properties).
Additional fields	Enables Additional Fields for the device when selecting the Yes check box. The Additional Fields row appears. Click the button on the far right in the Additional Field value area to generate a key. For more information, see **Configuring the Additional Fields function** below.
Enable for all devices	Enables the service for all devices when selecting the Yes check box; or disables the service for all devices.

Once you click the **Additional Fields** value area, the Additional Fields settings window appears.

6.7.2 - Configuring the Additional Fields function

The Additional Fields function enables you to obtain more tracking information, such as an account number or patient ID. The system prompts you to enter the information before the document is scanned. The system adds the information to each entry in the log file.

Note:

The Additional Fields function is not available if you are using the Cost Recovery service. If the eCopy Cost Recovery Service is supported on your device, you can integrate the device with an Equitrac or Copitrak terminal.

6.7.2.1 - To Configure Additional Activity Tracking Fields

1. In the Administration Console, select the **Configure services** tab.
2. Select **Activity Tracking** from the **Device services** pane.
3. In the **Configuring Service: Activity Tracking** setting, select the **Yes** option to allow a device to use the Activity Tracking service.
4. Enable the **Additional Fields** option by selecting **Yes**. The `No additional fields in list` message appears.
5. Click the button on the far right in the Additional Field value area to generate a key.
6. Click **Save**.

6.7.2.2 - Additional Fields Settings

Description
ttings.
he columns after you enter Field Editor settings: Field Name, Default, Minimum, Maximum, and User Modify.

Click **Done** when you are finished.

Note:
You need to have at least one field defined in the grid to close the dialog.

Once you click **New**, the **Field Editor** window appears.

Field Editor settings

6.7.2.3 - Field Editor Settings

Setting	Description
Name	The Field Name (required). The default value is `Name1`.

Setting	Description
Type	Set the following settings for alphanumeric or numeric type: • Minimum: Choose between 0 and 1000. • Maximum: Choose between 0 and 1000. • Remember: Choose between 0 and 1000. The default value is 0. Note: These settings represent the length of the alphanumeric or numeric string, and not interpreted as a range in case of the numeric field.
Default	The default field entry (optional). This value is presented on the client (MFP) form by default when you enter information into the Activity Tracking fields.
User Modify	If set to Yes (default), you are allowed to modify at the client (MFP).

Click **OK** once you are finished or click **Cancel** to cancel your selection.

6.7.3 - Identification service

The Identification service is located on the **Configure services** tab under the **Device services** section.

Identification services are available on compatible MFP devices that use identification devices such as card fingerprint readers or proximity cards. Identification service allows the user authentication credentials from the identification device to be encrypted and passed to ShareScan. This preserves security and streamlines the logon process by allowing you to avoid entering authentication credentials at the device.

Identification service enables the integration of ID devices with eCopy ShareScan by providing a way for the third-party applications to send credentials (username, password, domain, or userID) to ShareScan so that you are not challenged again.

The following settings are available for **Configuring Service: Identification**:

6.7.3.1 - Identification Settings

Setting	Description
Configured	Allows the device to use the Identification service when selecting the Yes check box; or prohibits the device to use the Identification service (this disables all the other fields and properties).
Keep connection alive	Keeps the TCP connection alive to communicate to the ID device: • Checked (Yes): Allows pulsing to occur between the ID device and the Identification service; the TCP socket connection stays open and connected until you log out, times out, ends the current session, or the ID device terminates its connection. • Unchecked: Drops its connection to the ID device after it receives the data packet.

Setting	Description
Port Number	The Port number that the ShareScan Manager listens to for ID device (client) connections. The default value is `9425`. Note: ShareScan Manager and the ID device should be configured for the same port.
Accept UserID only requests from External Services	Allows the device to accept User IDs provided by external services, for example Uniflow, as valid authentication means.

6.7.3.2 -

Setting	Description
Type	Enables encryption for your Identification service, if appropriate: • None: Passes credentials to ShareScan without encryption. Not recommended. • TripleDES: Enables you to encrypt the information from the application that is supplying the credentials to ShareScan. You can do this by creating an encryption key that you store on the computer where the Manager is running and on the ID device
Path	Set the path for the encryption type to the `eCopyKey.txt` file. This file contains the key specified in the Key field. The ID device should have a copy of this file and use the same key if encryption is TripleDES. It specifies a path to the storage destination for the encryption key on the device where the Manager is running.
Key	Generates the encryption key and stores it in the `eCopyKey.txt` file. You must manually copy this file to the device. If you regenerate the key, you must copy the new key to the device. The TripleDES key is used for encryption. Click the button on the far right side of the Key field value area to generate a key. Note: If the key value is changed, the ID device should take a new `eCopyKey.txt` file and use the new value for TripleDES encryption. Important: All devices that use Identification Services and are managed by the same Manager must use the same encryption key. After generating a key for the first device, when you configure subsequent devices you must select the same path you selected for the first device. ShareScan automatically recognizes the key file that is already in the storage destination.
Enable for all devices	Enables the service for all devices when selecting the Yes check box; or disables the service for all devices.
Save button	Saves the changes made in the Identification service page.

6.7.4 - eCopy Identification Service Terminal Emulator

eCopy Identification Service Terminal Emulator appears when you click **Test** in **Configuring Service: Identification**.

To configure the emulator, launch the dialog by clicking the **Config** button on the main dialog.

6.7.4.1 - Configuration Settings

	Description
	Specifies the name or IP address of the machine running the TCP server. The default value is `localhost`, which is the machine that the emulator is running on.
	Must match the port number set in ShareScan Administration Console. The default value is `9425`, which matches the default for ShareScan.
	Value in seconds until the terminal times out if no pulses are received from ShareScan Manager. The default value is 120 seconds.
	Specifies the IP address of device.
tials	The following ID device credentials are required: • Username: The login name of the user. • Password: The user's password (optional). • Domain: The Domain name you are a member of.
	The following ID device credentials are required: • XML name: Insert name for the attribute of the XML entry. • Value: Insert value that is matched with the XML label. You can add, view, and clear XML attributes: Add XML: Press this button to add the name or value pair to the XML attribute. This is added to the stream on the bottom of the dialog, that is, `aaa=111`, `bbb=222`, and so on (additional attributes that have been entered or saved that exist if the text is longer than the dialog box). View XML: Press this button to view the XML file that is sent to server. This includes the username, password, domain, email address and extra attributes added. Clear XML: This button clears all of the additional attributes to be passed to server.
	The type of encryption used to encrypt the XML data: • None: Passes credentials to ShareScan without encryption. • TripleDES: Enables you to encrypt the information sent from the application that is supplying the credentials to ShareScan. You can do this by creating an encryption key that you store on the computer where the Manager is running and on the Identification Service device.
	Browse for the path location of the `eCopyKey.txt` encryption file. This file contains the Secret key value used for TripleDES encryption.
	Saves all field data.

Once the emulator has been configured, it is ready for use.

Note:

The text at the top of the status window (a default value of `Waiting for server messages`) gives helpful tips about the state of the emulator.

6.7.4.2 - Terminal Emulator Settings

Setting	Description
Status Window	Displays the time-stamped status messages.
Connect	Connects to ShareScan using the server name and port configured in the configuration dialog. Note: This button is disabled once a connection has been established.
End	Only enabled once a connection has been established as disconnects from the TCP server.
Clear	Clears all text in the status window.
Keep connection alive	When checked, the TCP connection between the Emulator and Server is kept alive. If not checked, it terminates the TCP connection after the logon packet is sent to server and no timer or pulsing events occurs.
Original XML Format	When checked, the original `XML` format is used.
Top Most	When checked, the emulator is always displayed on top of any window. When unchecked, the emulator retains its normal order.
Seconds left until lock	Displays a running countdown in seconds until the emulator times out. When the emulator times out, it disconnects from the TCP server. Maximum timeout is 120 seconds.
Config	Enables the configuration dialog.
NetStat	Enables a command prompt window that runs the `netstat -a -p TCP` command .
Exit	Closes the application.

6.7.5 - Session Logon service

The Session Logon service is located on the **Configure Services** tab under the **Device Services** section.

The Session Logon service provides secure access to the application and avoids prompting you multiple times for credentials; that is, it provides a single sign-on for ShareScan.

Session Logon is provided as a single point of authentication for the entire workflow. If Session Logon is configured and enabled for a device, you need to log on only once into ShareScan. The logon information is effective for the entire session. You do not have to enter your logon information each time you select a connector during the current session. The ShareScan Manager passes the logon information to the Connector using an internal interface called "Credentials" in Data Publishing.

Note:

If you need to access different servers, and the logon credentials are not the same on those servers, the system prompts you to enter logon information, even when Session Logon is enabled.

If you enable Session Logon for the Quick Connect, LDAP/SMTP, or Fax via SMTP connectors, refer to the connector-specific configuration section for information about selecting the authentication type.

6.7.5.1 - Session Logon Settings

Setting	Description
Configured	Enables Session Logon in the Device pane when selecting the Yes check box; or disables Session Logon in the Device panel (this disables all the other fields and properties).
Directory services	Specifies the directory service that manages your list of users (Windows Active Directory or Novell Directory Services).
Type	The directory service type. The default type is Windows Active Directory. If the ShareScan Administration Console detects that the Novell client is installed, Novell Directory Services (NDS) is added to the list.
Domain	The domain associated with your login name and password (you can also specify another domain name): • Windows Active Directory: The current domain for the local machine is default. • Novell Directory services: You must specify the NDS Server and ID.
Bypass session logon (no authentication):	This option enables the ShareScan client to be configured to bypass the Session Logon form when only the user identification is received from the device, Cost Recovery or ID Services and the password is not provided. While a network authentication is not performed by ShareScan Session logon, if the username is provided it is used by the individual connectors when needed.
Bypass session logon (authenticate user):	This option enables a network authentication to be performed by ShareScan using the username and password provided by the device, Cost Recovery, ID Services or ShareScan Single Sign on Extender.
Search parameters	Specifies the parameters for searching the selected directory.
Search on	The search criterion by which the system searches the user list: • Windows Active Directory: First Name, Last Name, Display Name, or Account Name. • Novell Directory Services: First Name, Last Name, or User ID.
Automatic Base DN detection	If enabled, the Manager performs an auto-detection for the base DN in the domain when doing type-ahead search. In multi-domain environments, you must enable this option if you want to use LDAP authentication.
Base DN	The Base DN or directory root which is the starting point of the search. This option defaults to the root of the main tree. Use this option to select the specific DN or context where you want the search to begin.
Restrict users to this DN	Limits the scope of the search to the specified DN.
Scope	The scope of the search at one level down from the Base DN or down to the lowest level of the tree: Base, One level, and Subtree.

Setting	Description
Directory Access	Specifies the type of access required to retrieve user names from the directory.
Type	Specifies the type of access required to retrieve user names from the directory: Anonymous or Use credentials (User name and Password settings are required).
User name	The user name.
Password	The user password (hidden by asterisks).
Search while typing	Click Yes to enable the type-ahead feature when you start entering a user name at the device.
Disable manual credential entry on Session Logon form	This option is only required if neither ID services nor Cost Recovery is configured, and the user name is received from the device. If this checkbox is marked, the user name and domain fields are hidden on the MFP screen, and only the data received from the device are shown. This also happens if ID service or Cost Recovery is active and configured.
Hide Logout button	Use this to hide the **Logout** button on the MFP device screen when you use Cost Recovery or ID Services for authentication, and you do not want the user to disconnect from Session Logon, as the authentication is performed by an external system (the ID Services or Cost Recovery).
Enable for all devices	Select the Yes check box to enable the service for all devices; clear the check box to disable the service for all devices.

The **Test** button allows you to quickly verify the Session Logon configuration without having to wait to add the device and test the same details at the Client. It is enforced to use the Test feature successfully before saving the settings of the Session Logon Service.

6.7.5.2 - Test Session Logon Settings

You can verify configuration by entering your name and password, selecting the domain, and then clicking the **Logon** button.

Setting	Description
User name	The user name.
Password	The user password.
Domain	The domain in which you are testing the configuration.
Success/Failure message	A message indicating success or failure appears in the bottom of the pane. If the test fails, the following error message appears: `Error: Failed to authenticate the user - Logon failure: unknown user name or bad password.`
Logon	Attempts to log on using the specified credentials.
Cancel	Terminates the test session.

After Session Logon is configured, enabled for a device, and tested, **Session Logon** is the first screen that you see at the Client. You must enter a valid username and password to log on to the selected domain. The ShareScan Manager verifies the credentials and passes them to the selected Connector.

The Connector must also verify the credentials passed to. If the authentication fails, the Connector must challenge you for the credentials again. The Connector must also display an appropriate error message.

Note:
The ShareScan Manager does not retain the credentials entered for testing.

6.7.5.3 - Bypassing Session Logon

Alternatively, you can use the ShareScan Single Sign On Extender, which enables secure storage (password caching) of the user's network passwords for use in a single sign on workflow. This enables the user to swipe a card (or use any other available method to identify themselves) and have this log the user into eCopy ShareScan and to access network resources.

For more information on the Single Sign On Extender, click here.

Note:
If no password is provided, available or password caching is not enabled, the user is prompted to enter their password.

6.7.5.4 - Typical Session Logon Workflows

Below, a number of typical Session Logon scenarios are briefly described, walking the user through an overview of the displayed forms.

Case 1

Prerequisites: Session Logon is enabled, Bypass redirect screen is enabled, External Authentication is enabled (Equitrac, for example), Single Sign-On enabled, Logoff automatically is enabled, Bypass Session Logon is enabled.

Workflow: User swipes card, and logs into the External Authentication Provider. Selects the ShareScan application on the device screen. The Session Logon screen is displayed, with the relevant authentication data already filled in. The user clicks **Next**, is transferred to the Main form. After scanning, the relevant connector forms are displayed in order, then the Session Logon screen is displayed, after clicking through the final connector form. The Session Logon screen displayed at the end shows empty fields, as the user has logged off automatically.

Case 2

Prerequisites: Session Logon is enabled, Bypass redirect screen is enabled, External Authentication is enabled (Equitrac, for example), Single Sign-On enabled, Logoff automatically is disabled, Bypass Session Logon is enabled.

Workflow: User swipes card, and logs into the External Authentication Provider. Selects the ShareScan application on the device screen. The Session Logon screen is displayed, with the relevant authentication data already filled in. The user clicks **Next**, is transferred to the Main form. After scanning, the relevant connector forms are displayed in order, then the Main form is displayed, after clicking through the final connector form.

Case 3

Prerequisites: Session Logon is enabled, Bypass redirect screen is enabled, External Authentication is enabled (Equitrac, for example), Single Sign-On enabled, Logoff automatically is disabled, Bypass Session Logon is disabled.

Workflow: User swipes card, and logs into the External Authentication Provider. Selects the ShareScan application on the device screen. The Session Logon screen is displayed, with the relevant authentication data already filled in. The user clicks **Next**, is transferred to the Main form. After scanning, the relevant connector forms are displayed in order, then the Session Logon form is displayed, after clicking through the final connector form. The Session Logon screen displayed at the end shows the relevant authentication data.

Case 4

Prerequisites: Session Logon is enabled, Bypass redirect screen is disabled, External Authentication is enabled (Equitrac, for example), Single Sign-On enabled, Logoff automatically is disabled, Bypass Session Logon is disabled.

Workflow: User swipes card, and logs into the External Authentication Provider. Selects the ShareScan application on the device screen. The Session Logon screen is displayed, with the relevant authentication data already filled in. The user clicks **Next**, is transferred to the Main form. After scanning, the relevant connector forms are displayed in order, then the Redirect screen is displayed, after clicking through the final connector form.

Case 5

Prerequisites: Session Logon is enabled, Bypass redirect screen is enabled, External Authentication is enabled (Equitrac, for example), Single Sign-On disabled, Logoff automatically is disabled, Bypass Session Logon is disabled.

Workflow: User swipes card, and logs into the External Authentication Provider. Selects the ShareScan application on the device screen. The Session Logon screen is displayed, with the relevant authentication data already filled in. The user clicks **Next**, is transferred to the Main form. After scanning, the relevant connector forms are displayed in order, then the Session Logon screen is displayed, after clicking through the final connector form. The Session Logon screen displayed at the end shows empty fields.

Case 6

Prerequisites: Session Logon is disabled, Bypass redirect screen is enabled, External Authentication is enabled (Equitrac, for example).

Workflow: User swipes card, and logs into the External Authentication Provider. Selects the ShareScan application on the device screen. The Main form is displayed. After scanning, the relevant connector forms are displayed in order, then the Session Logon screen is displayed, after clicking through the final connector form. The Session Logon screen displayed at the end shows empty fields.

Case 7

Prerequisites: Session Logon is disabled, Bypass redirect screen is disabled, External Authentication is enabled (Equitrac, for example).

Workflow: User swipes card, and logs into the External Authentication Provider. Selects the ShareScan application on the device screen. The Main form is displayed. After scanning, the relevant connector forms are displayed in order, then the Redirect screen is displayed, after clicking through the final connector form.

6.7.6 - Common Access Card (CAC) service

The Common Access Card (CAC) service is located on the **Configure services** tab under the **Device services** section.

The CAC service is used as a general identification card as well as for authentication to enable access to United States Department of Defense (DoD) computers, networks, and certain DoD facilities. The CAC service enables the use of Public Key Infrastructure (PKI) authentication tools, and establishes an authoritative process for the use of identity credentials.

6.7.6.1 - Common Access Card Settings

Setting	Description
Configured	Allows a device to use the CAC service when selecting the Yes check box; or disables a device to use the CAC service (also disables all fields and properties).
Display warning in seconds	Shows the warning window for a certain period of time at the Client (the default value is 10).
Enable for all devices	Enables the service for all devices when selecting the Yes check box; or disables the service for all devices.

Click **Yes** to save your settings or click **Cancel** to cancel your selection.

6.8- About common services

Common services are built-in services that can be applied to Connectors and Devices/Device groups.

There are two categories on the Common Services tab :

- Notification services
- Tracing services

After creating a Service profile, you can associate Service with Connector profile in order to make Service's functionality available.

6.8.1 - Associating a Service profile with a Connector profile

After creating a Service profile, you associate it with a Connector profile so that the Service's functionality is available. For more information on creating Connector profiles, see the "Configuring the connector" topic for the connector with which you are working.

6.8.1.1 - To Associate Service And Connector Profiles

1. In the console tree, select **Devices** and choose an item in the list represented by its name and its IP by clicking on it.
   The **Configure Connectors for Device** window opens and displays all the Connectors associated with the device.
   The **Settings** pane opens with the **Services** tab and displays all the Services associated with the device.
2. Select the Connector with which you want to associate the Service.
3. Click **Save** and return to the **Device configuration** window.
4. Select the Service that you want to associate with the Device.
5. Click **Save** and return to the **Device configuration** window.

The Service profile is now associated with the Connector profile. When you scan a document using the Connector with the associated Document Service profile, the document is scanned, processed by the Document Service, and then passed to the Connector workflow for processing.

6.8.2 - Notification service

The Notification service is located on the **Configure Services** tab under **Common Services**.

The Notification service notifies the preconfigured recipients based on events occurring in ShareScan that are configured to use an SMTP notification.

This service provides the following main functions:

6.8.2.1 - Configuring Service:Notification Settings

ShareScan sends an SMTP message through the email server specified in the SMTP Server address. With a predefined setting, the message contains customized messages that display specific data, for example, Subject, Header, Body, and Footer. The notifications can be descriptions of errors, warnings, or informational data from completed scan jobs.

Setting	Description
Configured	Select the Yes check box so that a device can use the service. Clear the check box to prevent a device from using the service.

Setting	Description
SMTP Server Configuration	Contains the settings that you use to configure the SMTP server.
SMTP Server	The SMTP server name, which is the DNS name of the e-mail server that is used to send the SMTP message.
SMTP Server Authentication	The authentication method used to send SMTP mail to the SMTP server. In the second column, click the authentication option, Anonymous, or Use Credentials: • Anonymous: The default value. When Anonymous, pointer moves automatically to the Email address section. • Use Credentials: Activates the Username, Password, and Domain fields so that you can specify the values.
Username	The SMTP username.
Password	The SMTP password.
Domain	The SMTP domain.
Email address	All the addresses must be in the SMTP format (`admin@company.com`).
From	Email address from which email messages are sent (originator of the message).
To	Email address to which an email is delivered (recipient of the message). Semicolons are used to separate addresses.
Cc	Email address to which an email is delivered (carbon copied recipient of the message). Semicolons are used to separate addresses.
Send to session logon user	Select Yes to send a notification email to a Session Logon user or clear the check box if you do not want to send it.
Message	Specifies the settings for the components of a message.
Subject	Specifies the subject that appears in the email.
Header	Specifies the header to include in the email error message, which is appended to the top of the message. Press `Ctrl+Enter` to start a new line.
Body	Specifies the custom text that is included in the email error message, which is appended to the body of the message. Press `Ctrl+Enter` to start a new line.
Footer	Specifies the text that is included in the email error message appended to the bottom of the message. Press `Ctrl+Enter` to start a new line.
Message Type	The following SMTP message types are available: • Plain Text: The SMTP message is sent as a plain text. • HTML: The SMTP message is sent in an HTML format with background color and product logo as the signature.

6.8.2.2 - Enable For All Connector Profiles Settings

Setting	Description
Enabled	Select the Yes check box to enable the service for all Connector profiles. Clear the check box to disable the service for all Connector profiles.
Notification level	The notification levels are available: • All: Sends all messages by ShareScan. • Warnings: Warning messages sent by ShareScan. • Errors: Sends only error messages sent by ShareScan. • Job successfully sent: Sends a message containing details about the completed scan.

6.8.2.3 - Enable For All Devices Settings

Setting	Description
Enabled	Select the Yes check box to enable the service for all devices. Clear the check box to disable the service for all devices.
Notification	This feature is not supported yet.

6.8.2.4 - Enable For Licensing Notification

Setting	Description
Enabled	Select the Yes check box to enable licensing notification. Clear the check box to disable licensing notification.

When you click the **Test** button, and the Notification service is correctly configured, a test message appears. If the configuration includes an invalid email server or addresses, an error is not generated or reported.

To ensure that the service works correctly, send a test message and make sure that it is sent with the correct information. At run time, the ShareScan Manager uses the information to trigger an email notification based on the notification level.

6.8.3 - Tracing service

The Tracing service enables you to configure the capture of trace information in a log file; this information helps troubleshoot potential configuration and connector issues. You typically do this only when working with customer support as tracing slows down overall system performance.

You can safely have verbose tracing on up until you have finished configuring your ShareScan system.

The Tracing service provides a mechanism to ShareScan Manager, Connectors, and eCopy services to write messages and errors to log files while running inside the ShareScan Manager. ShareScan web clients and the ScanStation application also use the Trace Service.

Tracing service is located in Administration Console in the **Configure services** tab under **Common services** section.

6.8.3.1 - Tracing Settings

Setting	Description
Configured	Enables Tracing service when selecting the Yes check box; or disables a device to use the Tracing service. **Note**: Configuring this service enables non-verbose tracing on all devices and connectors.
Verbose	Enables detailed tracing when selecting the **Yes** check box or disables a detailed tracing. By default, the logging is NOT verbose; for troubleshooting purposes, verbose logging is recommended. When enabling verbose tracing for troubleshooting a specific issue, you may want to consider applying this tracing mode only for the device in question; this way, you can have verbose tracing on longer before overwriting the old tracing information. Thus, use the Device Settings, or Device Group Settings to regulate tracing for specific devices. Note that by default, verbose tracing when enabled, applies for all devices of a device group; therefore, if you want to switch tracing to verbose for only a specific device of the group, you have to lift that device from the group for the duration of the tracing process.
RSD Trace	Mark this checkbox to turn on RSD Tracing; RSD is the scanning module of the ScanStation application. If checked, the ScanStation application creates trace logs via the Trace service. You must restart your ScanStation after marking this checkbox and saving the setting in order to make the application read the new settings. Nuance recommends that you only turn RSD trace on for brief periods of investigating possible issues, as RSD tracing is very verbose and has a significant performance impact. The log files written by RSD are added to the zip file when user exports the trace information by clicking **Export**. Note that clicking **Delete Trace Files** does NOT delete RSD trace files.
Trace File options	Options to create the log files.

Setting	Description
File size (kB)	Tracing file size in kB. Minimum value is 500 kB, the default value is 500 kB, and maximum value is 51.200 kB. **Note:** As the tracing happens into an internal binary format, and the size specified here will determine the size of the binary file, the size specified here will not match the size of the exported trace file if the export target format is TXT. If you want to get trace files from the system for diagnostic or troubleshooting purposes, ensure that the file size is set to a minimum of 10.000 kB, because if this file size is set to too low, the important tracing information might not be recorded.
Enable for all devices	Enables the service for all devices when selecting the Yes check box; or disables the service for all devices.
Enable for all connector profiles	Enables the service for all connector profiles when selecting the Yes check box; or disables the service for all connector profiles.
Export	Using this option, you can export the internal trace file into a zipped archive. When you click the **Export** button, you must provide the following information: • A name and location of the archive to be created (you can use the **...** button to browse to the location you want to use). • Source files (mark the checkboxes of the files you want to include in the archive) • Device logs you want to include (mark the checkboxes of the devicesyou want to include in the archive)
Delete Trace Files	Click this button to delete all ShareScan trace files from your system.

Click **Yes** to save your settings or click **Cancel** to cancel your selection.

Table 1:

7 - About eCopy Connectors

A ShareScan system uses the following types of connectors:

- eCopy connectors included with ShareScan, such as mail and fax connectors for Microsoft Exchange, Lotus Notes, and SMTP via LDAP.
- The following connectors are available for download or purchase, depending on your version of ShareScan: Quick Connect; Open Text Fax Server, RightFax Edition; Microsoft® SharePoint®; iManage WorkSite; Open Text Document Management, eDOCS Edition; Open Text Content Server; and EMC® Documentum®.
- Third-party connectors, developed using the ShareScan Software Development Kit (SDK).

In addition, ShareScan supports Business Automation services that enable connectors to use Image Enhancement and Barcode Recognition.

You configure connectors by creating connector profiles that specify various settings, such as the appearance of the connector's button and the image format that you want to use during scanning. You can create multiple profiles for each connector and you can activate each connector profile on multiple devices.

7.1- Installing and removing connectors

During installation of the ShareScan software, you can install all the eCopy connectors supplied with the installation package purchased by your organization. After you license a device, you can activate any installed connectors.

7.2- About connector profiles

You can configure multiple profiles for each connector as each connector profile defines a set of configuration options for that connector. In addition, you can activate multiple profiles for each connector on a single device. For example, you can create two unique profiles for the Exchange connector and activate both on device x.

7.2.1 - Example of two profiles for the same connector activated on a single device

Profile name	Profile description	Device
Expense Reports	Scans and sends expense reports to a Payroll inbox.	Device x
Resumes	Scans and sends resumes to a Human Resources (HR) inbox.	Device x

For more information on configuring a connector profile, refer to the connector-specific *Configuring the connector* topic.

7.3- Planning connectors

To obtain the best result from your connector, you may want to consider the ways the connector is used in your work environment, as well as a number of other factors, for instance:

- **Saving time:** If you want to reduce the amount of time your users spend at the device, you can set up an Express connector profile that allows users to scan and send documents by simply pressing the connector button at the device.
  You can create multiple buttons and configure each to scan documents to, or store documents in a different destination. You can also control the number of destinations presented to the user at the device and the attributes for each destination.
  Users can also save time by not having to enter their credentials each time they use the device. To enable your users to skip this step in the scanning process, select the **Logon as** option on the **Authentication** tab when you configure the destination for your connector profile.
  You may also want to consider the ShareScan Session Logon feature, which - when set - allows users to bypass the Logon screen altogether.

- **Enhancing security:** If you want to keep track of the documents sent by each user, select the **Logon at runtime** option on the **Authentication** tab when you configure the destination for your connector profile. This forces users to log on each time they use the connector and allows the system to keep a record of the documents sent by each user in the log file.
- **Controlling access:** depending on the individual connectors, you can limit the accessible destinations in a number of ways, including
    - Configure connector profiles that allow access to a single destination, or to a limited set of destinations.
    - Disable the **Allow subfolder navigation** option if you do not want your users to have access to the folders and sub-folders of the configured destination.
    - Disable the **Enable navigation** option if you do not want your users to have access to the locations below the configured destination.
    - Select the **Logon at runtime** option at the **Authentication** tab when you configure the destination for your connector profile.
    - Configure connector profiles that only allow access to a single profile.
    - Configure connector profiles that allow access to a limited set of libraries.
    - Select **Session logon** and **Runtime** as the Authentication type when you configure the scanning destination for your connector profile.

7.4- Configuring connectors

After installing and activating a connector, it must be configured for use. The instructions below provide a general guideline for configuring the various connector profiles:

1. In the Administration Console, select the **Connectors** tab. The **Configure connectors** pane displays a list of the installed connectors.
2. Select the connector name. The **Configure connector** and the **Settings** panes open.
3. To create a new profile, click **Save current profile as**, enter a name for the profile, and then click **Save**. To modify an existing profile, select the profile name from the list.
4. Use the **Settings** pane to specify the following settings:
    - Display settings
    - Document settings
    - Services settings
    - Scanner settings
    - Offline processing settings

Note:

Each connector profile supports a unique group of settings. If a setting is not available for the connector you are configuring, it will be grayed out.

5. In the **Configure Connector** pane, under **Destinations**, click **New**. The **Create a destination** window opens.
6. Specify the destination settings. Each destination that you create for the profile appears in the Destinations list. When you select a destination, the settings configured for the destination and the screens that will be visible to the user at the device appear in the Summary list.
7. Click the **Save current profile** button. The system saves your settings as part of the connector profile.

7.4.1 - Configuring Express connector profiles (optional)

An Express connector profile allows you to control the number of screens that the user sees at the device. The profile that you create in the following procedure allows the user to scan and store the document by simply pressing the button on the Home screen. You can customize the profile so that the user sees as many or as few screens as you want. The following instructions present a generic guideline for Express connector settings; minor details may vary, depending on the connector in question.

1. In the Administration Console, select the **Connectors** tab.
2. Select the connector you want to configure.
3. To create a new Express profile, click **Save current profile as**, enter a name for the profile, and then click **Save**.
4. In the **Settings** pane, configure the **Display** settings and make sure that none of the other available settings is set to **User modify**.
5. Set the authentication method (**Login as** as the **Type** or configure **Session login**).
6. Enter the user name and password for the destination.
7. Click **Test**, if applicable.
8. Configure the connector-specific destination settings.
9. Under **Screen options**:
    - **Select profile**: Make sure that **Allow selection** is not selected.
    - **Display fields**: Select **None**.
    - Selecting these screen options, along with use of a profile that contains no required fields or that pre-fills fields, ensures that the user at the device does not see the **Profile selection** or the **Document profile** screens.
    - **Confirm storage**: Select **No**. This ensures that the user at the device does not see the storage confirmation message.

10. Confirm your settings.
11. Click **Save current profile** to save the profile.

7.4.2 - Defining a scanning destination (optional)

Defining a scanning destination enables you to control how the connector behaves during the Authenticate, Navigate, and Index phases at the device.

You must define at least one destination. If you define more than one destination, the connector will prompt the user to select one during the scanning process.

The **Destinations** tab displays a list of destinations that you can make available to the user on the Destinations screen at the device. The Destinations list displays the name and type of each destination. The Destinations list displays the destination name in the second column, and an icon in the first column for Express destinations. For more information on each destination, move the cursor over the destination name in the list.

Placing your cursor over a destination in the list displays information for that destination. You specify the information in the Destination window.

Selected destinations, indicated with a check mark, appear on the Destinations screen at the device.

Worksite and SharePoint connectors have specific considerations, click the links for more details.

To define a scanning destination:

1. On the **Configure** tab, click **New**. The **Create a destination** window opens and displays the **Authentication** tab.
2. Enter a **Name** for the new destination. This is the destination name that the user sees at the device
3. Select the relevant destination for this connector profile.
4. Specify the **Authentication** settings, if applicable.
5. Specify the **Location** settings.
6. Use the **If filename already exists** option to specify the connector behavior when the scanned document has the same name as another document stored in the scanning destination.
7. Click **OK** to save your destination settings and return to the **Destinations** tab.

7.5- Activating connector profiles

To make connector profiles available at a device, you activate the connectors and then select the connector profiles. Each connector profile that is activated on a device is represented by a separate button on the ShareScan Client screen.

7.5.1 - To activate connector profiles

1. In the Administration Console, select the **Devices** tab. The **Device configuration** pane displays a list of the available devices and device groups.
2. Select the device or device group on which you want to activate the connector. The **Configure connectors for device** and the **Settings** panes open. The **Configure connectors for device** pane has the following columns:
    - Select profiles: Select a default connector from the list.
    - Display name: Displays connector's name.
    - Configured: Choose **Yes** or **No**.
    - Layout: Numbers in order of selecting.
3. In the **Select profiles** column, select the connector profile that you want to activate. You can only select configured profiles which appear in black. Profiles that are not configured appear in red. Only the connectors that have valid licenses for the selected device will appear.
4. Click **OK** and then click **Save**.
5. Click the **Layout** button. The **Arrange layout** window opens with the following settings:
    - Connector
    - Profile
    - Display name
    - Order of appearance
6. Drag and drop the profiles to re-arrange the order of appearance of the connector buttons at the client and click **OK**.
7. Click **Save**. The profile is now activated on the device. Note that the web-browser enabled MFP devices and the simulator there may experience a minor delay (typically less than 30 seconds) until the new connector settings and connector associations are propagated.

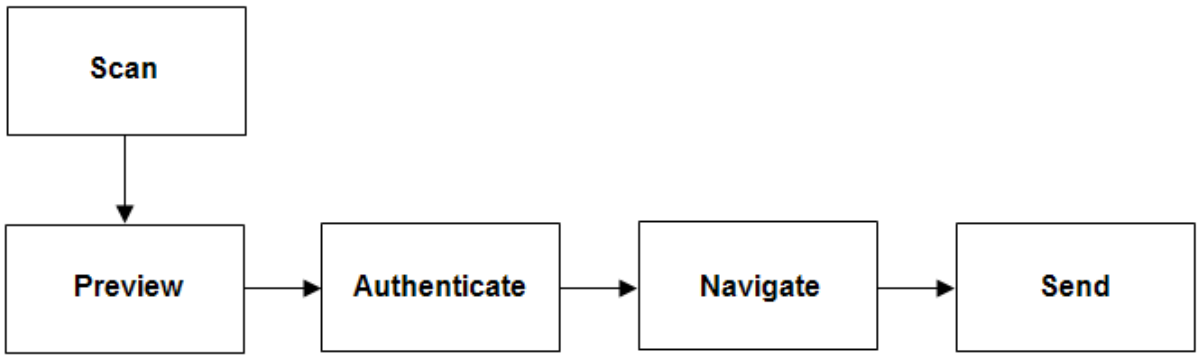
Note:

You can publish connector profiles individually or in groups to one or more eCopy-enabled devices.

7.6- Using connectors

Below, you can find a typical workflow, which provides an overview on how the connectors work. Depending on the connector, minor details may vary.

At the scanning device, the user follows the standard eCopy workflow to scan and send a document. If you configure a connector profile to use the Express function, users will not need to perform many of the steps included in the procedure in this section.



7.6.1 - Scan

1. Place your document in the feeder or on the glass.
2. If your system is configured to use the Session Logon feature, enter your user credentials on the **Login** screen and then press **Login**. If your Session login credentials are not valid, the **Login** screen for the connector will appear after you preview the scanned document.
   If **Search while typing** is enabled on the **Session login** tab, ShareScan will search for matching address list entries after each character you enter in the **User name** field. Select your name from the list that appears as you enter each character. If **Search while typing** is disabled on the **Device services** tab, it overrides this setting. However, even when **Search while typing** is disabled, you can still perform a search by entering characters and pressing the **Search** icon.
   When you have successfully logged in, the **Home** screen appears.
3. Review the default scanner settings in the left pane; use the down arrow button to view additional scanner options.
   To change a setting, select the option, such as "Paper size," and then select the setting on the toolbar that appears. ShareScan will use the modified scanner settings for all subsequent pages that you scan during this session, unless you change settings from the Preview screen.
4. Press the connector button.

7.6.2 - Preview

1. When the connector finishes scanning the document, review the scanned images. The buttons on the **Preview** screen enable you to view, delete, rotate, and change the magnification of the images.
2. If necessary, scan additional pages or re-scan any of the original pages by placing the pages in the feeder, or on the glass, and then pressing the **Scan more** button.
   When you scan additional pages, the client inserts them after the page that is currently displayed on the **Preview** screen. For example, if the client is displaying page 5 of an 8-page document and you scan two more pages, the client inserts the new pages after page 5.

3. To review and change the scanner settings, press the **Scanner settings** button on the **Preview** screen. The **Scanner settings...** screen appears. After changing the scanner settings, select **OK**.
4. To review and change the document settings, select the **Document settings** button on the **Preview** screen. After changing the document settings, press **OK**.
5. When you are ready to send or store the document, press **Next**.

7.6.3 - Authenticate and Navigate

1. If the **Logon** screen appears after you preview the document, enter your user credentials, then press **Next.**
2. If you configure the connector to allow navigation, the **Folder navigation** screen appears. The list can display 200 entries at one time.
3. Select the target subfolder in the destination folder.
4. Select sub-levels in the list until the complete path appears in the **Path** field at the top of the screen.
5. When you have selected the destination, press **Next**.

7.6.4 - Send

1. If the **Send** screen appears, specify the settings
2. Press **Next**.
3. Select one of the post-scanning options.

7.6.5 - Post-scanning options

Option	Description
Log out	Displays the Logon screen. Appears only when Session Logon is enabled.
Done	Displays the Home screen.
New document	Displays the Preview screen and enables you to scan a new document using the current settings. Place the new document in the feeder or on the glass and then press **Scan more**.
New destination	Enables you to send the scanned document to another connector. Press the button and then select the target connector from the list. The client opens the target connector and displays the scanned document on the Preview screen. Press **Next** and then follow the prompts provided by the target connector.

8 - Configuring devices

An eCopy-enabled device can be:

- A multifunction peripheral (MFP)
- A scanner that is connected to an eCopy ScanStation

- An MFP with eCopy software running in the device

The ShareScan Manager supports a single device connected to a ScanStation or multiple devices running the eCopy software.

Use the **Devices** tab in the Administration Console to manage the devices. The **Devices** tab provides you access to two main functions:

8.1- Device configuration

To perform the following device configuration functions, right-click the **Device configuration** area and choose the function:

- Add devices: Discover and select an eCopy-enabled device.
- Create device group: Create a group and add devices into this group.
- Rename device groups: Rename the group with a unique name.
- Model name assignment: Specify a new model name for the device selected or select an already defined setting from the drop-down list.
- Delete device group: Delete the group and all the devices inside this group.
- Lock/Unlock group: Lock or unlock the group.
- Find device: Find a device by name or IP address.
- Collapse/Expand all: Expand or collapse all the nodes.

8.2- User configuration

To perform the following user configuration functions, right-click the **User configuration** area and choose the function:

- Select organization: Select an organization unit from the Active directory.
- Remove organization: remove the organization unit from the list of User configurations.
- Restrict personalization: Restrict this organization from selecting connectors from All Users group.

For more information, see User configuration.

Configuring devices also involves:

- Activating connector profiles
- Configuring services for devices
- Configuring scanner settings for devices

8.3- Finding devices

You can quickly find a device in the device configuration list.

8.3.1 - To find a device

1. In the Administration Console, right-click the **Device configuration** tab and select **Find device**. The **Find device** window opens.
2. In the **Device name** field, enter a device name. As you enter each character, the Search while typing function searches for a matching device name. If it finds a match, it highlights the device on the **Devices** tab.
3. In the **Device IP** field, enter the complete ID address. The system searches for the device.

Note:

If a device is marked with a yellow question mark, it can be pinged, but is not yet ready for communication, or no longer ready for communication.

8.3.2 - Find Device settings

Option	Description
Device name	Enter a device name. Type-ahead feature is enabled for the Device Name field. Typing in a partial name, highlights the device on the Devices tab, if found. Note: The complete IP address needs to be entered in the Device IP field for the search to begin.
Device IP	Enter a device IP value. Type-ahead feature is enabled for Device IP field. The value should follow an `xxx.xxx.xxx.xxx` pattern.
Finding Devices window	The following values are displayed after the search: Device name, Device IP, Vendor, Version, and Location.

8.4- Creating and deleting device groups

You can quickly create and delete device groups in the device configuration list.

8.4.1 - To create a device group

1. In the Administration Console, right-click **Device configuration** tab and select **Create device group**. A **New entry** field is created under **Device groups**.
2. Rename a **New entry** field , if needed, and press `Enter`.
3. Once a group is created, drag and drop existing devices or add new devices (by dragging and dropping from within the **Add device** window) into the group.

Note:

When creating a device group, ensure that the name of the device group is unique (no device or group can have the same name).

8.4.2 - To delete a device group

1. In the Administration Console, right-click on a group name from a **Device groups** list and select **Delete group**.
2. Click **Yes** to delete the selected group.

8.5- Renaming device groups

You can quickly rename device groups at any time in the device configuration list.

8.5.1 - To rename a device group

1. In the Administration Console, right-click a group name from a **Device groups** list.
2. Select the **Rename device group** menu item to change the name of the group and then press `Enter`.

8.6- Locking device groups

You can quickly lock and unlock device groups in the device configuration list.

8.6.1 - To lock a device group

1. In the Administration Console, right-click on a group name from a **Device groups** list.
2. Select the **Lock group** menu item to lock all the devices.

   Note that any new devices that are added to the group are **not** locked.

8.6.2 - To unlock a device group

1. In the Administration Console, right-click on a group name from a **Device groups** list.
2. Select the **Unlock group** menu item to unlock all the devices.

8.7- User configuration

The User Configuration function is available to all devices and device groups for which Session Logon has been enabled. You use this function to select an organization and to configure connectors for all users:

- Organizations: Displays all the Organization units (departments) that are currently configured and enables you to select an organization:

8.7.1 - To select an organization

1. In the **User Configuration** pane, right-click **Organizations** and then click **Select Organization**. The Organization Units window displays organizations that are configured in the Active Directory.

The window includes domain and access information.

2. In the **Organizational Units** window, double-click the Organizational units to add to the list of departments for User configuration and click **OK**.

Note:

To remove an organization unit, right-click it and then click **Remove Organization**. To restrict an organization unit from selecting connectors that are available via the All Users group, select the organization unit and then click **Remove Personalization**.

- All Users: In addition to connectors selected for the Organization unit you belong to, this configuration is available to all users authenticated using Session Logon.

8.8- Role based configuration

With this feature you can allow specific Connectors to be displayed based on the Organizational Unit (OU) in the Windows Active Directory. Before you start, complete the following prerequisites:

- Session Logon must be configured to add an OU to this list.
- User configuration setting must be enabled for the device or group of devices.

Double-click an OU to add to the list. Now, the Connector Profile selection page is presented where you can select a set of Connector Profiles instead of the Connectors selected for the device.

The authenticated user (via Session Logon) is presented with the set of Connectors that are configured by you for the OU/Department the user belongs to.

8.8.1 - Role based configuration options

- If the OU the user belongs to is not configured with any Connectors, the Connectors in the All Users group are displayed at the Main form, along with the **My Config** button, where you can customize the selection of Connectors for your account.
- If the All Users group is not configured with any Connectors, the device's default set of Connectors is displayed.
- If the device is not configured with any Connectors, the `No Connectors are configured` message is displayed on the Main Form.
- If the OU/Department the user belongs to and the All Users group is configured with one or more Connectors, then by default (for the first time), the OU Connectors are displayed along with the **My Config** button, where you can customize the Connectors for your account.

You can restrict an OU/Department from not being able to customize the Connectors from the All Users group by right-clicking the OU and selecting **Restrict All Users**. This is useful, when you want to restrict certain departments from customizing the generally available Connectors from the All Users group.

8.8.2 - Role based configuration restrictions

- Renaming an OU is not allowed.
- An OU can be removed from the list by right-clicking the OU and selecting the **Remove Organization** menu item.
- The **Settings** and **Scanner** tabs are hidden when configuring this feature as they only apply to a Device/Device Group.

8.8.3 - Device/Role based configuration chart

Device	OU/Department	All Users	Connectors displayed on Main Form
Device A	None (no Active Connector profiles).	None (no Active Connector profiles).	Device Connectors.
Device A	One or more Active Connectors.	None (no Active Connector profiles).	Connectors in OU (default). Personalization is not available.
Device A	One or more Active Connectors.	One or more Active Connectors.	Connectors in OU (default). Personalization available via My Config button (Personalization button on the Main form, through which you can personalize your choice of Connectors at run time.
Device A	One or more Active Connectors. Restrict All Users (menu item, if checked, restricts the OU/Department from using the Connectors from the All Users group, that is, Personalization is restricted).	One or more Active Connectors.	Connectors in OU (default). Personalization is not available.
Device A	None (no Active Connector profiles).	One or more Active Connectors.	Connectors in All Users(default). Personalization is available via My Config button (Personalization button on the Main form, through which you can personalize your choice of Connectors at run time).

8.9- Personalization feature

With this feature you can configure Connectors, make them available for any user. This gives the user the ability to maintain the user's own personal set of Connector profiles based on the user's login information.

You can personalize the set of Connectors only when Session Logon along with the User Configuration options are enabled and if at least one or more Connectors are activated in the All Users group.

Note:

If there is only one active profile in the All Users group, the **My Config** button is still visible, even though you cannot access My Config at runtime.

When you log in for the first time, you are presented with Connectors selected for this department, along with the **My Config** button. You can click the **My Config** button to further select any generally available Connectors other than the departmental Connectors. Once you select the desired Connectors and click **OK**, the Main form is reflected with the changes immediately. At least one Connector profile must be selected for personalization

Note:

When the user first logs in Departmental Connectors, they always supersede Connectors listed in the All Users group. In other words, Connectors selected in the Department the user belongs to are displayed on the Main form and the user can customize Connectors by using **My Config**, where they are presented with both the Departmental and Connectors from the All Users group.

8.9.1 - Personalization restrictions

- If the same Connector profile is selected in both the Department and the All Users group, only one entry or instance of this profile is visible in the list presented in the **My Config** page (at the Client).
- If the Department does not have any Connectors selected, Connectors form the All Users group and are displayed by default on the Main Form, along with the personalization button (**My Config**).

From the main form you can continue with your activity and or log off at any time. The next time you log in, the Main form is presented with all the buttons configured in the previous login. You can choose to reselect any of the available Connectors via the **My Config** button.

If at any point of time you want to remove/modify a generally available Connector profile (from the All Users group), it is reflected immediately the next time you log into the system. In case of an unselected or deleted Connector profile, the profile is removed from your personal set of Connectors.

9 - About configuring scanners

When you configure a device, you also specify scanner settings for a device.

Select **Devices** > <*device name/IP address*> > **Settings** > **Scanner**.

9.1- Specifying default scanner settings

You can specify default scanner settings for devices.

9.1.1 - To specify default scanner settings for a device

1. In the Administration Console, select the **Devices** tab.
2. Select the device that you want to configure.

3. In the **Settings** pane, select the **Scanner** tab. The information that you see depends on the device you are using.
4. Specify the default scanner settings in **Scanner defaults**.
5. Click **Save**.

9.1.2 - Scanner defaults settings

Settings	Description
Resolution	The following resolution types are available: DPI 100, DPI 150, DPI 200, DPI 300, DPI 400, and DPI 600.
Input paper size	The following input paper sizes are available: Letter, Letter R, Legal, Ledger, Statement, Statement R, A4, A4 R, A3, A5, A5 R, B4, B5, B5 R, Auto, and Mixed.
Output paper size	The following output paper sizes are is available: Letter, Legal, Ledger, Statement, A4, A3, A5, B4, B5, and Auto (default value).
Orientation	The following orientation types are available: Portrait, Landscape, and Same as originals.
Scaling	Scaling can be adjusted between 25-100 percent.
Color	The following color options are available: Black and white (B&W), Grayscale, Full color, Auto color grayscale, and Auto color B&W.
Image mode	The following image modes are available: Text, Text photo, and Photo.
Two sided	The following two sided modes are available: Single sided, Double book, and Double calendar.
Image quality adjustment label	The following image quality adjustment labels are available: Remove background, Prevent bleedthru, and None.
Inverse	Enables inverse with Yes.
Deskew	Enables deskew with Yes.
Mirror	Enables mirror with Yes.
Two page separation	Enables two page separation with Yes.
Brightness	Brightness can be adjusted between 10-90 percent.
Sharpness	Sharpness can be adjusted between 10-90 percent.

Note:

The **User modify** option in the **Scanner defaults** tab enables you to specify whether or not the users at the device can override.

9.2- Configuring scanner settings for ScanStation

You can specify scanner settings for devices.

9.2.1 - To specify scanner settings for a device

1. In the Administration Console, select the **Devices** tab.
2. Select the device that you want to configure.
3. In the **Settings** pane, select the **Scanner** tab. The information that you see depends on the device you are using.
4. Specify the scanner settings in **Configuration**.
5. Click **Save**.

9.2.2 - Scanner configuration settings

Settings	Description
Driver name	Browse and select the driver to be used for scanning. The currently selected driver is shown. Click the row and click the right corner to open the Select scanner window. Nuance Scanner Setup Wizard automatically starts that helps you with scanner configuration. For more information, see Nuance Scanner Setup Wizard .
Type	Type of driver currently selected or in use (TWAIN or ISIS).
Show title bar	If a kiosk mode is not desired, setting this value to Yes creates a resizable window with a title bar.
Password (exit)	Prompted when you try to exit the ScanStation Client by pressing the `Exit` button in the kiosk mode.

9.3- Setting up scanning devices

Nuance Scanner Setup Wizard is used to configure ScanStation (a ShareScan Client) to communicate with a scanning device (scanner or network MFP) for the best possible scanning results.

9.3.1 - Scanning device settings

1. In the Administration Console, select **Devices** > <*device name/IP address*> > **Settings** > **Scanner**.
2. Click the **Driver Name** row and click the far right corner. The **Select Scanner** window appears with the list of all available scanning devices. In some cases, the scanning devices are located elsewhere in a network. The scanning devices fall into two categories: TWAIN and ISIS.
3. Select the scanning device to be used by ScanStation in the Wizard.

- Setup: Launches the Wizard in order to test your scanning device. The Wizard performs some tests, creates and stores hints, and returns to Administration Console.
- OK: Selects the scanning device and returns to Administration Console if the scanning device already has hints. Otherwise, launches the Wizard if there are no hints, that is, the setup has not been performed yet.
- Cancel: Aborts the operation.

Note:

Nuance recommends performing all tests in order to create necessary hints. Hints are scanning device specific data used for optimizing scanning process.

You select a TWAIN/ISIS driver when you license a TWAIN/ISIS scanning device. You select a different driver in the following cases:

- If you change the device.
- If you selected the wrong driver.

9.3.2 - Testing scanning device

You can test your scanning device in the Wizard to make sure it works properly and to perform additional tests.

There are only few scanning device drivers which fully meet the appropriate standard. Also, there are some ambiguities in the standards themselves. Therefore, the Wizard uses hints to cover these differences. These hints are stored in a database installed with the Wizard for all scanners which were tested by Nuance. When performing tests, the Wizard tests the connection between the computer and your scanning device and creates hints for the scanning devices.

9.3.2.1 - To Perform Tests

Before you start, make sure the scanning device is powered and the cable is connected and close any other applications that might be using your scanner. Also check that the device is set to online mode.

1. Select from the following options that you want to apply: Basic scan test (recommended), Check ADF capabilities, Paper sizes supported, Black and white scan test, Gray scan test, and Color scan test.

For advanced users: Additional tests, Advanced settings, and Hint editor (optimizes your scanner's performance but you risk degrading its performance or even disabling its scanning capability).

2. You are prompted a basic scan check and additional tests (for advanced users). Insert a test document or photograph in your scanning device, and then click **Next**.
3. When your scanning device's native user interface appears, choose all the default settings in one of the color modes and proceed through a complete scan.

4. After basic scan test has passed, if the scan appears to be correct, click **Next** to perform the next test. Otherwise, make the image correct with the following options: invert, rotate, flip horizontally, or flip vertically.
5. If the image is missing or incomplete, there may be an issue with your scanning device. In this case, check that you correctly inserted a document or photograph and that the page size setting is suitable and click **Next**.
6. Check the ADF capabilities: The Wizard determines your scanner type. If this is incorrect, select the appropriate type. This test checks how your scanner's ADF detects the presence of paper in its input. If the test fails, your scanner either continues to scan endlessly from the flatbed when the ADF becomes empty or a dialog from Administration Console appears on each page.
7. Check paper sizes supported: The Wizard determines your scanner type. If this is incorrect, select the appropriate type. You are presented some page sizes that your scanner supports by its flatbed. Click **Adjust** to change paper sizes.
8. Black and white scan test: If the Wizard detects that your scanner is capable to scan in black and white, it tries to scan in black and white (binary) mode.
9. After the scan test has passed, if the scan appears to be correct, click **Next** to perform the next test. Otherwise, make the image correct with the following options: invert, rotate, flip horizontally, or flip vertically.
10. The last two selections are repeated for grayscale and color modes.
11. Click **Finish** to go back to the **Select Scanner** window.

9.4- Startup Configuration for ScanStation

You can manage and configure the Client from the Administration Console by specifying ScanStation startup configuration.

9.4.1 - To specify ScanStation startup configuration

1. In the Administration Console, select the **Devices** tab.
2. Select the device that you want to configure.
3. In the **Settings** pane, select the **Scanner** tab. The information that you see depends on the device you are using.
4. Specify ScanStation configuration in **ScanStation startup configuration**.
5. Click **Save**.

9.4.2 - ScanStation startup configuration settings

Settings	Description
Automatic logon	At ScanStation startup, or when the device is restarted, automatically logs on to Windows using the specified user name, password, and domain. You can configure by clicking Yes to make the ScanStation to automatically start the Client and log on as a specified user whenever the ScanStation is started. Note: If you do not do this, you must start the Client manually each time you start the ScanStation.
User name	The user name.
Password	The user's password (hidden).
Domain	The domain.
Start ScanStation automatically	Starts the Client as soon as you log on to the ScanStation or after an automatic logon.

10 - The eCopy Bates/Endorsement Service

The eCopy Bates/Endorsement Service adds an electronic "stamp" to each page of the scanned document. The stamp comprises an endorsement, which includes a unique page number, a text message, which can include any standard required text, and the date and time. Two format types are supported:

- System formats: You can create a range of basic formats that can be used or modified.
- User formats: You can create formats at the device by modifying an existing system format and saving it under a new name. You can modify most of the format attributes except for the position and the margin. You can modify the text message only if you select the **Allow User Modify** option when you create the format.

10.1- Page numbering

When you create a Bates/Endorsement format, you specify the starting page number. By default, each document that is scanned using that format uses the same starting page number. However, you can control the page numbering by performing any of the following tasks:

- Manually specifying the starting page number when you select a Bates/Endorsement format.
- Using a checkpoint: When users want to number a collection of separate documents sequentially, you can create a Checkpoint identifier.
- Using the options available on the Document sent successfully screen.

10.2- Configuring the service

When you have enabled the service for the system, you can select and enable it for individual connector profiles, and can create numbering formats that users can select at the device.

To enable the service:

1. In the Administration Console, select the **Configure Services** tab. The tab displays a list of available services.
2. Select the service name. The service configuration and the settings pane open.
3. On the configuration pane, select **Configuring Service: Bates/Endorsement** and then click **Save**. The service is configured to use the formats shown in the format list.

Note:

To add more format options, create new formats.

To create a new Bates/Endorsement format:

1. On the configuration pane, click **New**. A new format is added to the format list with a default name of **New**.
2. Select the format and, under **Configure Format** on the **Settings** pane, and type a name for the new format.
3. Use the **Settings** pane to specify the format settings. As you specify the settings, the **Sample Document** area displays the results of the settings as they appear on the page.
4. When the format appears correctly, click **Save**. The new format is saved with your settings.

Note:

To modify an existing format, select the format in the list, modify the settings, and click **Save**. The change is that the settings take effect for all connector profiles that use the format.

10.2.1 - Bates/Endorsement format settings

The following settings are available for the Bates/Endorsement service:

10.2.1.1 - Configure Format Settings

Setting	Description
Configure format	The Bates/Endorsement format setting.
Format name	The Bates/Endorsement format name. Note: The Bates/Endorsement format name cannot be empty.

10.2.1.2 - Endorsement Settings

Endorsement settings always include the page number and can also include a prefix and a suffix. The service numbers pages are sequentially from the specified starting point. You can specify a Checkpoint and thus enable related documents to be numbered continuously.

Setting	Description
Prefix	The text to display before the page number.
Space left	The number of spaces to insert before the page number. The default value is 2.
Page	The starting page number. The default value is 00001.
Space right	The number of spaces to insert after the page number. The default value is 2.
Suffix	The text to display after the page number.
Date	The date to display after the suffix.
Time	The time to display after the date.

Note:

Auto-scale option allows you to auto-scale down the scanned image to allow the Bates number to be printed on each page without interfering with the scanned image during a single scanning session.

10.2.1.3 - Text Message Settings

The Text Message is a standard message that is stamped on every page, such as a copyright notice, a legal statement, or a disclaimer.

Setting	Description
Message (optional)	The text message that is printed on each page (optional). Press `Ctrl+Enter` to start a new line. Only two lines of text message are supported.
Allow user modify	Allows users to modify the message at the device by marking Enabled.

10.2.1.4 - Font And Justification Settings

You can configure the font and justification settings for the Endorsement and the Text Message separately. The same settings are available for each of them.

Setting	Description
Font	The font for the endorsement. When the Font dialog box pops up, use the drop down menu to set the following font attributes: • Type (the default value is Arial). • Style (the default value is Regular). • Size (the default value is 10) . • Effects (Strikeout and Underline options are available). • Color (the default value is Black). • Script (the default value is Western). Note: You can see text example in the Sample window.
Font style	The style (Bold or Italic) of the font.
Font effects	Enables underlining by marking Underline.
Justification	The position (Left, Right, or Center) for the endorsement or the text message. The default value is Right.

10.2.1.5 - Position Settings

Position settings specify where the Bates/Endorsement is put on the page.

Note:

You cannot modify position settings at the device.

Setting	Description
Align	The alignment (Top, Bottom, or Right). The default value is Bottom.
Margin	The distance to place text from the vertical edges of the page. The default value is 0.25.
Units	The unit of measurement (inches or millimeters) for the margin. The default value is inches.

10.3- Numbering related documents

The Checkpoints feature enables you to automatically add continuous page numbering to a set of related documents. Once you have configured a Checkpoint, you can scan any number of documents at any time and all the pages are numbered sequentially. For example, if you create a sequence called `KP1` and select this identifier before scanning each of two 10-page documents, the pages of the first document are numbered 1 through 10, and the pages of the second document are numbered 11 through 20.

Note:

You must create the Checkpoint identifier before you scan the first document. Also, because Checkpoints are device-specific, you cannot create a Checkpoint at device `A` and use the same sequence to scan from device `B`.

To create a new Checkpoint identifier:

1. On the main Bates/Endorsement screen, press **Checkpoint**.
2. In the **Checkpoints** field, enter a Checkpoint identifier.
3. Press **Open**.

Note:

Make sure that you select the Checkpoint identifier that you want to use before you scan the first document.

To continue numbering using an existing sequence:

1. On the main Bates/Endorsement screen, press **Checkpoint**.
2. In the **Checkpoints** list, select a Checkpoint.
3. Press the folder icon to return to the main Bates/Endorsement screen.

Note:

Since the software can only save a limited number of Checkpoints, make sure that you delete Checkpoints when you are finished using them.

To delete a Checkpoint:

1. On the main Bates/Endorsement screen, press **Checkpoint**.
2. In the **Checkpoints** list, select the Checkpoint that you want to delete.
3. Press the red **X** (Delete).
4. Press **Cancel** to close the dialog box and return to the main Bates/Endorsement screen.

10.4- Activating the service for connector profiles

After enabling the service on the system and creating endorsement formats, you can activate the service for one or more connector profiles.

To activate the service for a connector profile:

1. On the **Configure Connectors** pane, select the connector name.
2. Select the connector profile that you want to modify.
3. In the **Settings** pane, under **Services**, enable **Bates/Endorsement**.
4. Click the **Save current profile** button. The system saves your settings as part of the connector profile.
5. Repeat for any additional Connectors.

Note:

Bates/Endorsement works as follows for other services that you select:

- Batching: Numbering is continuous in a document that is split into several batches.
- Blank page removal: When this feature is enabled, blank pages are removed from the document and then Bates/Endorsement is applied, resulting in uninterrupted sequential numbering.

10.5- Scanning with the Bates/Endorsement Service

When Bates/Endorsement is available on the system and enabled for a Connector, the Bates/Endorsement button (a page with a rubber stamp) appears in the scan preview window on the eCopy-enabled device. You can press the button to activate the service for the current scan and choose the endorsement format that you want to use for the document.

Note:
If the Bates/Endorsement button does not appear on the screen, the service is not enabled for the connector profile that you are using.

To use the service:

1. Scan the document and review the scanned pages.
2. Press the **Bates/Endorsement** button on the **Preview** screen to view the default settings.
3. Use the **On/Off** button to enable or disable Bates/Endorsement for this scan job.
4. Select a format from the **Formats** list. The service displays the default settings for the format.
5. To modify the prefix, suffix, or page number, press the keyboard button next to the corresponding field, type the text, and press **OK**.
6. Press **Font** to configure the following settings:
    - To modify the amount of space before or after the page number use the up and down arrows..
    - To change the font size, or style, or set the position of the endorsement, enter the settings, and then press **OK**. (You cannot change the font name at the device).
7. To view or modify the text message and appearance, press **Text** on the main **Bates/Endorsement** screen.
8. Type any changes to the message, the alignment, and the font size and style, then press **OK**.
9. To set the date and time, use the **Date and time** lists to select the format.
10. When you finish specifying the settings, press **OK** to return to the scan preview screen.

    Note:
    The Checkpoint feature enables you to add continuous page numbering to a set of related documents.

11. When you have scanned and sent your document, you can use the post scanning options.

11 - The eCopyCost Recovery Service

The eCopyCost Recovery Service is compatible with major cost recovery systems. When cost recovery is enabled, scanning functions are unavailable until the user unlocks the cost recovery terminal or application and specifies the billing account information:

- Scan date and time.
- The name of the scanning device.
- The scanning function used (e-mail, fax, scan to desktop, and so on).
- The number of pages scanned.
- The size of the document.
- Sender and recipient information.
- Any additional information provided by the cost recovery system.

At the end of the session, you can log off using the terminal and ShareScan returns to the "locked" state.

11.1- Configuring the service

The ShareScan software includes timers that automatically log you off after a certain period of inactivity. However, when the Cost Recovery Service is enabled, these timers are disabled and you remain logged on until you press **End** or **Complete** on the terminal, or until the terminal times out.

To configure the service:

1. In the ShareScan Administration Console, select the **Configure services** tab. The tab displays a list of available services.
2. Select the service name. The service configuration and the settings pane open.
3. On the configuration pane, select **Configuring Service: Cost Recovery**. The Cost Recovery Service fields become active.
4. To use Encryption, specify the settings.
5. To use the Activity log, specify the settings.
6. To enable the service for all devices, select **Enabled**.
7. Click **Save**, then click **Test**. The eCopy Cost Recovery Terminal Emulator opens.

Note:

If you are passing user credentials from your cost recovery terminal to the eCopyCost Recovery Service, Session Logon must be set to **Enabled** in the **Enable for all devices** tab and **Configured** in the **Configuring Service: Session Logon** tab. This functionality is only available if you are using the Unicode/XML (v3) protocol.

To test the service:

In the eCopy Cost Recovery Terminal Emulator, click **Connect** to connect with your server.

11.2- Cost Recovery settings

The following table describes the settings available for the Cost Recovery Service.

11.2.1 - Cost Recovery settings

Setting	Description
Configure Cost Recovery service	Configures the Cost Recovery Service settings.
Configured	Enables all settings for the service.
Port number	Enters port number. The port number must match the TCP port configured for the cost recovery device. The default port is `9325`. Note: If you change the Port field, the Manager is automatically restarted after saving your settings.
Show Lock Button	Shows Lock Button at the client. This button allows you to lock the terminal from any screen during a session. This option is only available for ScanStation devices.
Protocols	Selects the protocol. This version of the service supports cost recovery terminals that were configured to work with previous versions of the eCopy Cost Recovery Service. • Unicode/XML (v3): Select this option if your terminal is configured to use the latest version of the Cost Recovery Service (recommended). • Auto detect (v1, v2): Select this option if your terminal is configured to work with earlier versions of the Cost Recovery Service. Note: All devices controlled by a Manager must use the same protocol.
Encryption	Encryption settings must be used if a password is included.
Type	The encryption type for Cost Recovery: • None: Passes credentials to ShareScan without encryption. • TripleDES: Enables you to encrypt the information from the application that is supplying the credentials to ShareScan. You can do this by creating an encryption key that you store on the computer where the Manager is running and on the Cost Recovery device.
Path	Set the path for the encryption key. Specifies a path to the storage destination for the encryption key on the device where the Manager is running.

Setting	Description
Key	Generates a new key. Generates the encryption key and stores it in the `eCopyCRSKey.txt` file. You must manually copy this file to the Cost Recovery device. If you regenerate the key, you must copy the new key to the Cost Recovery device. Important: All devices that use Cost Recovery Service and are managed by the same Manager must use the same encryption key. After generating a key for the first device, when you configure subsequent devices, you must select the same path you selected for the first device. ShareScan automatically recognizes the key file that is already in the storage destination.
Activity log	Includes the standard eCopy ShareScan user activity log information.
Configure	Track Cost Recovery using activity logging. Enables all settings for the service.
Location	Root folder for all Cost Recovery logs. The default location is `%ProgramData%\Nuance\ShareScan\costrecovery.log` or `%ProgramData%\Nuance\ShareScan\costrecovery.xml`.
Maximum log size	Maximum file size in kB. Maximum Log Size is 5000 kB.
File overflow type	Activity log file types. Enables file overflow for Cost Recovery, if appropriate: • Rolling filenames: `ShareScan001`, `ShareScan002`, and so on. • Overwrite oldest events: New events will overwrite the oldest events in the log.
Field separator	The field separator used in Cost Recovery activity logging. Adds a field separator ",".
Extended fields	Allows extended fields in Cost Recovery activity logging.
Device specific activity	Allows separate Cost Recovery activity logging for each spcific device.
Enable for all devices	Enables for all devices settings.
Enabled	Enables the service for all devices.

Note:

If the key is re-generated, the `eCopyCRSKey.txt` file must be copied to the Cost Recover terminal again. If a key mismatch occurs, the data is not decrypted correctly.

11.3- eCopy Cost Recovery Terminal Emulator

eCopy Cost Recovery Terminal Emulator appears when you click **Test** in **Configure Cost Recovery service**.

To configure the emulator, launch the dialog by clicking the **Config** button on the main dialog.

11.3.1 - Configuration settings

Setting	Description
Server name	Specifies the name or IP address of the machine running the TCP server. The default value is `localhost`, which is the machine that the emulator is running on.
Port number	Must match the port number set in ShareScan Administration Console. Default value is `9325`, which matches the default for ShareScan.
Timeout (seconds)	Value in seconds until the terminal times out if no pulses are received from ShareScan Manager. The default value is 120 seconds.
Device IP	Specifies the IP address of device.
CLID	Emulates the type of data fields (client identification) you enter in a terminal.
Delimiter	The field delimiter for the activity tracking and fake CLID and MID fields. This value matches the value set up in ShareScan Administration Console, the default is ",", which matches the default used in ShareScan.
MID	Emulates the type of data fields (Multiplex Identification) you enter in a terminal.
XML name	Inserts the XML name.
Value	Inserts values. Note: You can add, view, and clear the XML attributes.
Encryption type	The type of encryption used to encrypt the XML data: • None: Passes credentials to ShareScan without encryption. • TripleDES: Enables you to encrypt the information sent from the application that is supplying the credentials to ShareScan. You can do this by creating an encryption key that you store on the computer where the Manager is running and on the Cost Recovery device. If TripleDES encryption is enabled, the `eCopyCRSKey.txt` file must reside in the path location specified in the eCopyShareScan Administration (Activity Tracking, Cost Recovery tab). After this file is generated by the Administrator Console, the file is copied to the Cost Recovery Terminal so that it uses the same TripleDES key encryption value.
Key path	You can browse for the path location of the encryption `eCopyCRSKey.txt` file. This file contains the Initialization Vector (IV) key used to seed the encryption provider.
Protocol version	You can choose which eCopy protocol to send and receive data between the Cost Recovery terminal and ShareScan Manager. The following versions are available: v1, v2, and v3 (default).
Enter credentials	Click to bring up a dialog to enter the following user credentials for use: Username, Password, Domain, and UserID. Note: If UserID is being used, UserName, Password, and Domain must be blank.
Save and close	Saves all field data to `tcpclient.ini`. The emulator always tries to load any value held in this file, which is located in the same folder as the emulator executable.

Note:

The text at the top of the status window (default value of `Waiting for server messages`) gives helpful tips about the state of the emulator.

Once the emulator has been configured, it is ready for use.

11.3.1.1 - Terminal Emulator Settings

Setting	Description
Status window	Displays time stamped status messages.
Connect	Connects to ShareScan using the server name and port configured in the configuration dialog. Once a connection has been established, the emulator sends an `ECOPY_SCAN_BEGIN` message to ShareScan. The CLID, MID, and Device ID values are all passed with this message. Note: This button is disabled once a connection has been established.
End	Only enabled once a connection has been established. Sends an `ECOPY_LOCK_NOW` message, waits for an `ECOPY_LOCK` message from ShareScan, and then disconnects from the TCP server.
Clear	Clears all text in the status window.
Top most	When checked, the emulator is always displayed on top of any window. When unchecked, the emulator retains its normal order.
Seconds left until lock	Displays a running countdown in seconds until the emulator times out. When the emulator times out, it sends the `ECOPY_LOCK_NOW` message, waits for the `ECOPY_LOCK` message from ShareScan, and then disconnects from the TCP server. Maximum timeout is 120 seconds.
Config	Pops up the configuration dialog.
NetStat	Pops up a command prompt window that runs the `netstat -a -p TCP` command.
Exit	Closes the application.

12 - eCopy Forms Processing Extender

The eCopy Forms Processing Extender is the process component in the **Capture** -> **Process** -> **Store** workflow of ShareScan. It lets you scan documents and automatically capture data (using zonal optical character recognition) from the documents using your scanner or MFP device.

The availability of this feature depends on your license.

13 - Administration Console Configuration

The setup process involves the following steps:

1. Configure the eCopy Forms Processing Extender (FPE) server option.
2. Create a Template Library and Template(s) in a Template Library.
3. Define a document Template.
4. Map FPE output to any eCopy connector.

Associating Forms Processing Extender with connector profile:

1. Select the Connector.
2. From the Connector, select the Forms Processing Extender in the **Services** window.
3. Select the FPE Profile.

14 - Configuring the eCopy Forms Processing Extender

In order to setup the Forms Processing Extender, server properties must be configured prior to creating templates.

14.1- Specifying Server settings

1. Launch the **Administration Console** and select **Forms Processing Extender** in the **Services** tab.
2. Specify **Server Address**, that is, the local system where the extender is installed. Default value is "localhost".
3. Set **Port**: The default value is 19150. Click **Search** to search the local machine for Nuance installed components.

Upon completion of the search, the Server Type field will display "Nuance Capture" and the **Parameters** section is enabled.

14.1.1 - Server Address hints

When entering the Server Address, be aware of the following:

- If the **Server Address** field contains a valid IP address or DNS name, then the processing is done by the **FormsProcessingServer.exe** running on the identified machine.
- If the **Server Address** field contains "Nuance", the processing is done within the ShareScan Manager itself, and the process tries matching the scanned pages to the templates contained in the defined **Template Library**.
- If the **Server Address** field contains "Barcode", the processing is done within the ShareScan Manager itself. This processing does not use templates, instead it reads the first available barcode on the page (matching the type or regular expression defined for the processing).

14.2- Creating a Template Library

1. Click **Launch Configuration Utility** under **Parameters**.
2. The Template Library Manager window is displayed.

   You can set the following options here:

- **Image folder**: enter the UNC path of a Shared Folder, where Forms Processing Extender will store the images used for the template.

- **User name**, **Password**, **Domain**: These three fields allow you to enter the proper credentials for the Template Manager to access the shared folder. The credentials provided must have read-write access to the shared folder.

5. Create a Template Library by clicking **New** under the **Template libraries** group box. Note that the new library is automatically named, you can rename it by clicking on the template library name, or selecting the template library and clicking **Rename**.
   Clicking **Delete** deletes the selected template library.
   Clicking **Clone** creates a full copy of the selected template library, named **Clone -<template library name>**. The clone possesses all parameters and templates included in the original version.
6. Create a template and save in the template Library. Click **New** under **Templates** and specify a name. The name should represent the document/form that is going to be processed with this template.
7. Click **...** to browse to the file that will be used for template design. The sample images will be used as the base for all documents processed by this template. The images used for creating a template should be *scanned* images created from the device you plan on using. Be sure to use real business documents to maximize accuracy of the recognition. The available image format choices are: TIF, JPG, BMP, DIB, GIF, and PDF.
   The selected image will be automatically copied to the shared folder defined in step 2.
8. The Template Creation window opens. For details on how to use this tool, see section *Template Design*.
9. When done, go to **File** and choose **Save and Exit**. The Template Libraries you create are displayed in the **Template Libraries** group box.

If you want to process / recognize forms with different layouts, you need to create multiple templates in the library.

Note:
Template Library will only appear in the drop down menu for selection if a template contains a Static field.

14.3- Setting Image Cleanup parameters

1. To apply image enhancement to the output images mark the checkbox **Modify Output Images**. If you leave it unchecked, cleanup will only be applied to temporary images used in the recognition process.
2. Click **Add**.
3. Select from the available cleanup options, including:
   - **AutoRotate**: Determines the proper orientation.
   - **Deskew**: Auto-rotates the document so that the alignment is corrected.
   - **Remove Grid Lines**: Erases grid lines from the image.
   - **Despeckle**: Removes stray dots.

- **Smooth**: Softens outlines.
- **Thin**: Decreases line width.
- **Thicken**: Increases line width.
- **Rotate**: Rotates the image by 90, 180, or 270 degrees.

To apply multiple image modifications, click **Add** again and select another operation.

14.4- Post Recognition Processing Options

The following options are available:

Batching:

- **Batch on Matched Templates**: Support for batching documents using recognized forms.
- **Remove Matched Templates**: Optional removal of recognized forms (that is, Coversheets).

Validation:

- **Show/Skip Validation Screen**: Showing the validation screen gives the user the option to accept or modify the extracted values.
- **Only Show Errors** (available when **Show Validation Screen** is enabled): Showing errors only suppresses the view of any field that meets or exceeds the confidence value.
- **Treat Unmatched Pages as Exceptions**. Each page of a scanned document is processed to determine if it matches a template:
  - **Enabled**: The pages are placed in the **Exception Folder** if a template is not matched for later review.
  - **Disabled**: All unmatched pages are processed as part of the previously matched pages. Example: Three pages are scanned and page one and page three match defined templates on the page. Page two did not match any template so two documents are stored. Document one has two pages and document two has one page.
- **Treat low confidence pages as exceptions**. Each page of a scanned document is processed to determine if it contains zones recognized with Low Confidence:
  - **Enabled**: The pages are placed in the **Exception Folder**.
  - **Disabled**: All pages with low confidence zones are processed along with the rest of the recognized pages.

15 - Template Design

The basic unit of form recognition and data extraction is the template. It contains field mapping and data validation rules created by the forms designer.

Templates are based on the document to be processed and are stored in libraries. Each library must contain at least one template, and there is no limit to the number of templates within a single library. For the best user experience however, Nuance recommends that a library should not contain more than 10 templates.

Template Libraries are associated with connector profiles.

15.1- Template Design Overview

Once you have created a form template (see **Creating a Template Library**), the **Template Creation** window is displayed allowing you to design a template.

The **Template Creation** window consists of the following areas:

- Menu area (on the top). The following menu options are available:
  - **Save**: Saves the current state.
  - **Template properties**: Displays the Template properties window, allowing you to modify the background image and set the barcode engine to be used.
  - **Template manager**: Displays the **Template library manager**, allowing to select a new template for editing.
  - **Test template**: Displays the **Template tester** window.
- Image viewing area (on the left): To view the sample document with zooming support.
- Zone controls area (on the right). This contains the following areas:
  - "Zones": Add new zones, delete existing ones, or select one to change its properties.
  - "Zone Types": Legend for zone coloring on the image.
  - "Zone Properties": Set or modify all properties for the selected zone.

How to design a form template:

1. Create a Static field: either a **Static Text** or a **Static Barcode** field. This Static field is used to identify which form template in the template library that is used to process the document.
2. Define additional zones for recognition and data extraction. Make sure to select **Add Zone** prior to identifying a new zone area in the template to prevent inadvertent changes to existing Zone Properties.
   Note that zones should not overlap each other, as that may lead to recognition errors.
3. Label each extracted value so it can be used by an eCopy Connector.
4. Set properties for each zone. Make sure to select the zone on the template prior to setting the values in the Zone Properties. Values in Coordinates and Advanced may not be retained if they are changed before the zone area selection is identified.
5. Apply data filter on extracted values (optional):
   - Regular Expression filter
     Note that you can enter multiple regular expressions, with each one displayed in a

separate line. In these cases, the system accepts the zone as valid if the value meets the criterion of at least one regular expression.

- ODBC Database lookup filter

Template Creation Settings:

The **Template Creation** window displays the zones and properties. Each zone must have a zone type and a specific set of properties. As the zone type is changed during configuration the property panel displays the appropriate fields for the zone type:

- **Zones**: Lists all configured zones. Highlight any existing zone to view or change the Properties and add or delete a zone
- **Zone Types**: The "Zone Types" area is a definition for the color coding of the zones that are drawn on the form.

Zone Type Definitions:

- **Static** - Static value(s) are used to identify the template in the template library: it is recommended to use a text block that is always present on the page (if you do not use a filter). A drift parameter (a tolerance margin - can be increased or decreased) is automatically set to search for the static value in a larger area on the form. If you define multiple static field types (static text and static barcode), all fields and the exact data values need to be present on the form to match the template. In case of mismatch, the software will attempt to match the next template.
  If you use a filter in connection with a Static zone, the value is only accepted if it meets the set Regular Expression or ODBC criterion.
- **Text** - Use this zone type to have its contents recognized as text. The location of the field can move as long as it stays the same relative location to a Static or Static barcode zone that is referenced as the reference zone in the Text zone properties. Using a reference zone increases accuracy to compensate for feeder slip and drift of the fields when scanning.
- **Check** - The Check zone contains an area that is either marked or not marked on the form. It uses the "Threshold" property to determine what constitutes a marked area. The "Confidence" property defines the acceptable difference between the user-defined "Threshold" property and the recognized value on the scanned image. If the difference between these two properties is below the confidence value, then the zone returns a LowConfidence error.
- **Barcode** - This zone type must contain a barcode. During the configuration of a form template the processing engine will attempt to auto detect the barcode encoding and set the BarCodeType property. Advanced properties give you the option to set it manually. Depending on the selected barcode recognition engine, you can set different barcode types for Barcode and Static Barcode zones.
- **Static Barcode** - Static Barcode value(s) are used to identify the template in the template library. The zone's content should be a barcode value that is always present on the page (if you do not use a filter). A drift parameter (a tolerance margin - can be increased or decreased) is automatically set to search for the static barcode value in a larger area on the form. If you define multiple static field types

(static text and static barcode), all fields and the exact data values need to be present on the form to match the template. In case of mismatch, the software will attempt to match the next template.
If you use a filter in connection with a Static Barcode, the value is only accepted if it meets the set Regular Expression or ODBC criterion.
Depending on the selected barcode recognition engine, you can set different barcode types for Barcode and Static Barcode zones.

- **Search** - A Search zone will search the selected area for the first instance of text that matches the filter (either RegEx or Datasource) defined for the zone. It will then return this text as the zone's value.

Barcode recognition engine

You can select the barcode recognition engine in the following ways:

- Using the relevant option of the **Properties** window of the Template Editor.
  This option allows you to set the recognition engine on a template basis; allowing you to customize templates for different barcode or document types.
- Using the relevant option of the **Forms Processing Extender** tab, available from the **Document Services** pane of the ShareScan Administration Console.
  This option allows you to quickly switch between the recognition engines using the Administration Console itself, without needing to modify created templates.
- Using the relevant option of the **Edit** pane of the **Page Templates** tab of the **Image Control** service, available from the **Document Services** pane of the ShareScan Administration Console.
  This option allows you to customize the recognition engine for each template separately, similar to the Template Editor of the Extender. You can set **Layout Search Order** and **Barcode Restrictions** for both engines, with additional options for **Barcode Indexing** (Aspose) or **Barcode Enhancements** and **Barcode Confidence** (Softek).

The available barcode recognition engines are the Aspose Barcode for .NET and the Softek Barcode Reader Toolkit. By default, the Softek engine is offered as the barcode recognition engine.

The Aspose engine is optimized to support a wide variety of barcode types (including, for example, Databar, ITF-14, Patch codes, Planet, and QR). Nuance recommends using the Aspose engine if you have to work with a variety of common and rare barcode types, and speed of recognition is not the crucial issue. The Softek engine is optimized for speed, and support a number of common barcodes (including, for example, Codabar, Code 128, EAN8, and PatchCodes). Nuance recommends using the Softek engine if you work with a limited number of common barcodes, or if recognition speed is an important factor.

If you change the barcode engine for a document, check that all barcodes in the various zones are supported by the selected engine. If a barcode is not supported, the recognition will fail.

15.2- Zone Properties

Zone Properties consist of the following settings:

- **Main**:
  - **Name**: The name of the zone. It is used to define the value of the field that will be referenced and passed to eCopy connectors. Tip: keep these names on a reference list for easier identification.
  - **Type**: The definition of how the zone will be recognized and what properties are available.
  - **Value**: The recognized value of the zone (appears only after the zone is drawn on the sample page form to the left).
  - **Threshold** (check zone type only): This value sets the ratio of shading required to trigger the value to true.
- **Coordinates**:
  - **Height**: The height of the zone to be recognized.
  - **Width**: The width of the zone to be recognized.
  - **X**: The horizontal coordinate of the left side of the zone.
  - **Y**: The vertical coordinate of the top of the zone.
- **Advanced**
  - **Confidence**: The threshold that the recognition engine must meet. The value can be between 0 and 100. If the confidence value for the text in the zone is below this rating, the process will automatically report a Low Confidence error; thus, it can be used as an automatic validation tool.
  - **Drift (Static and Static Barcode only)**: Provides an extended area on the page that is searched for a static text value or a static barcode value. It is used to match values and identify the template.
  - **Width** is the adjustable horizontal size of the drift window.
  - **Height** is the adjustable vertical size of the drift window.
- **Error**: Displays errors or warnings associated with the zone:
  - If there are no errors with recognition or an applied filter the display is "None".
  - "RecognitionError" is displayed if an error is encountered recognizing the barcode or during the OCR of text.
  - "FilterError" is displayed if the value in the “Value” field does not match the filter settings.
  - "LowConfidence" is displayed if the difference between the user-defined “Threshold” property and the recognized value on the scanned image is below the confidence value.
- **Barcode and Static Barcode** fields will display an additional advanced property, “Barcode Type”.
  - **Barcode Type**: Select the barcode encoding used for the zone.

- **Reference Zone**: A defined static zone. It is used to locate the text or barcode. If the Reference Zone moves on the page all fields that reference it are adjusted to accommodate for the movement.
- **ShowValue**: The True/False field specifies if the field will be displayed on the validation screen.
- **Filter**: Allows the entry of a regular expression or database lookup to validate data that was OCR'd from a zone. A regular expression filter sample is provided in the Step by Step Invoice Example section of this guide.
    - **Regular Expression**: For details see pages like www.regular-expressions.info for information on building regular expressions.
    - **ODBC query**: these filters are used by the system to connect to a database and run simple queries. If the recognized text of the zone is included in the result list of the query, then the filter criterion is considered met; if not, a **Filter failed** error message is displayed. To use it, you have to enter the following data:
        - **Connection String**: SQL connection string, used to connect to the database. For example, an MS SQL Server 2008 connection string has the following format: **Driver={SQL Server Native Client 10.0}; Server=<your IP address or DNS>; Database=<your database name>; Uid=<your user account>; Pwd=<your password>;**
        - **Query**: enter an SQL query, which, when run, will compile the value list used to check the recognition results. The query may contain a **##value##** constant, which denotes the value recognized for the zone. For example:
          SELECT Value FROM dbo.CustomValues
          WHERE Id <> ##value##
        - **Test**: Displays the results of the query prior to saving the filter settings.

Zone Properties can be viewed in categorized or alphabetical order.

15.3- Testing Templates

The template design tool lets you open a sample form and visually verify the results without having to scan a page or run the ShareScan client. After a successful test we recommend that you also do actual scanner tests.

To test a template, follow the steps below:

1. Click **Test Template** in the editor. The Template Tester window is displayed.
2. Select the Template library you want to test via the dropdown list.
3. Select the image on which you want to test the process by clicking the **...** button next to the **Image file** field.
4. Optionally, you can set Image Cleanup settings via the **Image modification settings** pane by clicking the **Add** button and selecting the relevant cleanup operation (for example, Autorotate, Deskew, and so forth).
5. Click **Recognize** to start the test.

If the test yields results, the template name, recognition time, and the zone-specific text areas are displayed, along with any errors and the original image part used for recognition.

Tips for testing templates:

- Use different sample forms to test the template.
- Scan using the different scanner models that will be used in production.
- Test different resolutions or force the scanning resolution to a single setting only for the one scanning function in the connector profile.
- If devices are color and B&W, test using both color settings or force the scanning to B&W for the connector profile.
- Image Cleanup operations like Deskew may help in accelerating the recognition.

16 - Configuring Data Publishing

Once you have configured the extender and templates are available, you can associate the Forms Processing Extender with a connector. This enables the selected connector to work with values published by the extender.

The following section provides an example with **QuickConnect**.

There are two ways to configure QuickConnect for Data Publishing:

- Using batching.
- Using single documents.

16.1- Batching

Prerequisite: batching must be enabled in the Forms Processing Extender.

1. Go to the **Connectors** tab and select **QuickConnect**.
2. Create a new **File Name** or **Index file**.
3. Set the field type to **Batch-based index value**.
4. Set the **Published Key** to the name of the field you wish to use.

Note:

For **File name** fields, make sure that you leave the **Use Document Service's File Name** checkbox blank (at the bottom of the **File name** tab).

16.2- Single Documents

Prerequisite: The Forms Processing Extender is available with templates.

1. Configure the File name or index Files you wish to use. Do it in the relevant tabs of the Quick Connect connector (as above), but this time use Alpha Numeric field types.

2. Launch the Data Publishing Mapping tool from **Advanced** > **Tools** > **Data Publishing Mapper**.
3. Under **Published Key**, select the FPE field you wish to use.
4. Under **Connector Key** select connector field you wish to map the value to.
5. Set the field type to string and the format to **None**.
6. Click **Save**.

17 - Step by Step Invoice Example

Process an invoice from the invoice example. Static fields must be setup to ensure that the document scanned is from the correct vendor and it is, in fact, an invoice.

1. Go to the **Services** tab of the Administration Console and then click the Forms Processing Extender icon.
2. Click **Launch Configuration Utility**.
3. Click **New** under the **Template Library Manager**. Type "Invoice_example" as the file name.
4. Click New to add a new template, then set the image path you want to use.
5. Click **Add Zone** to create a new zone, and name it (as Invoice).
6. Set the Zone Type to **Static** and the ShowValue property to **False**, so it does not display on the validation screen.
7. Draw the first static zone on the image to identify the word “INVOICE” in the upper right.
8. Click **Add Zone** again, name the new zone as "InvoiceDate" , and set its type as **Text**.
9. Draw the zone on the page. Note that the ReferenceZone is automatically set to **InvoiceDate**.
10. Go to **Advanced Properties**, select **Filters**, and click "...".
11. Select the **RegEx Filter** radio button from the displayed list.
12. Enter the filter string to validate the text in the field is the proper date format, (0[1-9]|1[0-2])/(0[1-9]|[12][0-9]|3[01])/\d\d.
13. Click **OK**, and check/show with the cursor that the **Value** property is 11/05/2010, and the **Error** property displays **None**.
14. Click **Add Zone**, name the new Zone as "Invoice#", and leave the Zone Type as **Text**.
15. Click **Add Zone**, name the new Zone as "InvoiceTotal", and leave the Zone Type as **Text**.
16. Select the **Filter** property and the dialog box for filters will appear and select the **RegEx** radio button.
17. Type ^\$[0-9]{1,6}+(\.[0-9][0-9]).
18. Select **OK** to close the dialog box for filters and the value property should display $1,961.16 and the error "None".
19. Select **Save**, then **Exit** from the **File** menu.

20. Save the eCopy Forms Processing Extender by selecting **Save** and saving the extender profile as AP Forms.
21. Test the Form Template.
22. Scan Document testing.

17.1- Regular Expressions

The eCopy Forms Processing Extender can use a wide variety of regular expressions for filtering purposes.

Below you can find a number of examples:

- to check a car's plate number from a template: [A-Z0-9]+ or ([A-Z]{2}|([0-9]{3}))
- to get a phone number from a name+phone number combination: (?<=,)[0-9]+
- to search information on a given page after the Invoice Nbr.: (?<=invoice Nbr: *)[0-9]+

You can check this site for a number of pre-generated regular expressions; the site includes a tester application which you can use for checking customized regular expressions for validity.

For more information on modifying and creating regular expressions, this site is recommended.

18 - Use case example

This use case scenario presents a way for configuring the SMTP Mail connector of ShareScan to use Data Publishing with the values derived from the Forms Processing Extender.

1. Start the ShareScan Administration Console.
2. Start the Forms Processing Extender.
3. Open the form you want to use.
4. Create three anchors on the document, as well as zones for the **To**, **From**, **Program**, and **Student ID** fields.
5. Save your changes.
6. Navigate to the Data Publishing Mapper, and map the the **To**, **From**, **Program**, and **Student ID** fields to the SMTP Mail connector.
7. Close the Data Publishing Mapper.
8. Navigate to the **Logon/SMTP** tab of the **Properties** menu of the SMTP Mail connector profile you want to use. Set the Logon and SMTP server options.

   This will allow the connector to use the relevant Data Publishing values from the **From** field.
9. Configure the **Sending options** tab of the connector to utilize the **$$SUBJECT$$** and **$$NOTE$$** tokens (Student ID and Program Data Publishing keys).
10. Save the changes you made to the connector profile.

11. Send the document through the SMTP Mail connector. The validation screen of the Forms Processing Extender will display the correct values.

    The From form of the connector should also automatically recognize the relevant value based on Data Publishing.

    The **Send** form will display the relevant, configured **To**, **Subject** and **Notes** values.

19 - Troubleshooting

It is important to understand the relationship between the Templates, documents, and Template Libraries.

Template Libraries can contain multiple Templates as only the Template Library is specified during the FPE setup. This is because the Template is matched automatically to the scanned document based on content of the scanned documents.

The following points should be considered:

- Template documents should be unique if they are used within one scanning batch and/or Template Library.
- Even though Templates may have different Zones specified and different Static fields, the entire document is read for the purposes of matching. Therefore, if multiple templates have the same content, all Zone data may fail.

Example:

Two Purchase Order documents that are identical and have unique Templates in the same Library:

- Purchase Order 1 has a static zone for the top title.
- Purchase Order 2 has a static zone for the **Bill To** field.

If you scan a document as Purchase Order 1 + 2 pages, plus Purchase Order 2 + 2 pages, everything on both Purchase Orders matches both Templates and failures may occur.

Recommended action:

Create separate Template Libraries for the two templates and create two profiles within FPE.

19.1- No matching template

If the Forms Processing Extender cannot establish a template matching, you most likely face an issue with finding the static zones.

The possible reasons for this issue can be a wrong filter assigned to the static zone, a wrong barcode (if using static barcodes), or the zone being defined to the wrong location.

Recommended action:

Start the Template Editor, and use the **Template properties** window to browse to the image for which the recognition failed. You will be able to see the cause of the issue in the editor (wrong zone location, wrong filter, and so forth).

19.2- No connection to Nuance Forms Processor

In case you cannot connect to the Nuance Forms Processor, a client-side error message is displayed:

This issue may be caused by one of the following reasons:

- The Nuance Forms Processor service is not running on the machine denoted by the given IP address or DNS name.
- The machine in question is unavailable.
- The listed port is not open.
- The service is watching on another port.

To solve the issue, check the above list, and perform any corrections necessary accordingly.

19.3- Evaluating recognition results

The validation screen on the client side provides detailed information on the recognition errors.

The possible errors are as follows:

- **Low confidence**: the recognition surety of the zone text is below the **Confidence** attribute set for the particular zone. If the Treat low confidence pages as exceptions option is set, pages with such errors are automatically moved to the Exception folder.
- **Filter failed**: the text of the zone was recognized succesfully, but the text does not meet the **Filter** criteria set for the zone.
- **Recognition error**: the zone was not recognized succesfully; for example, a **Barcode** type zone does not contain a barcode.
- **Unknown error**: an unknown error, with no detailed information available.

20 - Best Practices

20.1- Determining the quality of an input document

Sometimes it is not easy to establish the boundary between Forms Processing Extender recognition issues as opposed to poor input paper quality.

To determine whether the selected image is acceptable, start the Template Editor, and define zones for the parts to be used for recognition. Then you should check if the current settings result in any errors for the zone, and if the text displayed under the **Value** property of the zone matches the actual text in the image.

If this is not the case, then the image quality is not optimal.

If a **Low confidence** message is displayed under the **Error** section of the zone, a decrease of the **Confidence** value may result in an improved recognition - but be aware that this can result in the process recognizing genuinely wrong text as correct.

21 - eCopy Highlight and Redact Extender

The eCopy Highlight and Redact Extender service is the process component in the **Capture** -> **Process** -> **Store** workflow of ShareScan: it lets you apply highlight or cross out markings to the output document, and do secure scanning of confidential documents by redacting ("blacking out") sensitive information.

The availability of this feature depends on your license.

Before you start

Be aware that once a file is saved with redacted items, there is no way of restoring the removed content – it can neither be viewed nor found by searching. If text to be redacted contains typing errors, it is possible that some sensitive data will not be removed by searching. It is recommended to review the resulting documents are to ensure the desired results.

For additional information about desktop PDF tools ask your eCopy reseller about eCopy PDF Pro Office.

22 - Configuration

22.1- Overview

The setup process involves the following steps:

1. Choose and configure a profile.
2. Associate Highlight and Redact Extender with a connector profile: Map extender output to any eCopy connector.
3. Scan with the service.

Note the following usage guidelines:

- Connector profiles that are used with the Highlight and Redact Extender Service must have **Searchable Text** enabled.
- The file formats supported for use with the Highlight and Redact Extender are .pdf, .doc, .docx, .xls, and .xlsx.
- Due to the processing required for document markup (highlight, redact, cross out) for the best performance on larger documents, Nuance recommends to use this Extender with offline processing enabled.
- Selecting highlight or cross out text may result in changes in the scanned image due to the OCR processing.
- The associated connector profile must either specify a supported file format or must allow the user to change the file format at runtime.

- The Highlight and Redact Extender does not support Encryption and Bates/Endorsement numbering. These settings will not be applied if the Highlight and Redact Extender is used.
- If using multiple extenders or services in a workflow, the Highlight and Redact Extender MUST be the last in the chain.
- You cannot specify the result document of a Highlight and Redact process as the input document of another Highlight and Redact process.

22.2- Service Configuration

Complete the following steps in order to configure the service:

1. Choose a preset from the drop-down list at the top of the configuration screen:
    - Default
    - BasicRedaction
    - BasicRedaction-NoModify
2. Define user modification settings:
    - Click a check box to modify the search terms for the specific document and the markup type at the control panel.
    - Leave it blank to allow the scanned documents to be processed automatically using the settings specified on this configuration page.
3. Define the **Terms to markup** option: List words and phrases. To mark up multiple terms, use a semicolon as a separator, for example `MFP;eCopy`. You can modify these depending on how you have set the option above.
4. Select **Markup type**: Specify the term display options for the output document (it tells the service how to mark up the text when found):
    - Highlight text
    - Redact text
    - Cross out text

Note:
The output document is a true representation of the original one when you use redaction. Highlight and cross out build a document from the OCR process changing the layout of the original image.

5. Select **Languages** on the **Extender Configuration** tab: This determines the language for recognizing and marking up the appropriate text as the Extender does not automatically select the OCR language based on the language set in the ShareScan Administration Console. Also, the Extender recognizes foreign and special characters for mark up with the corresponding language, such as `é`, `à`, `è`, or `@`, `®`.
6. Save the service profile.

Once the Highlight and Redact process is completed and the final document stored in the specified location, it can be viewed using any application supporting the specified file format.

Note:

The resulting final document cannot be used as an input document for another Highlight and Redact process.

23 - Associating Service with a Connector Profile

After creating a Service profile, you associate it with a Connector profile so that the Service's functionality is available.

To associate Document Service Profiles with a connector, see section *Associating a Service profile with a Connector profile* in *ShareScan Help*.

24 - Scanning with the service

After you have associated the Extender profile with the connector profile, the **Scanner** tab enables you to attach default scanner settings to the connector profile.

24.1- Configuring scanner settings

You can specify the settings in a profile so that the user at the device does not have to change them. If the device does not support a setting that you specify in the profile, the connector uses the device's default settings.

To configure the default scanner settings, see the relevant section in *ShareScan Help*.

25 - Single Sign On Extender

The Single Sign-On Extender allows you to use all client-side ShareScan functionalities after a single authentication, thus foregoing the need to authenticate yourself for each connector or service separately.

The availability of this feature depends on your license.

26 - Using the Extender

Follow the steps below to take the extender into use:

1. Via the Administration Console, the ShareScan Administrator ensures that you have the necessary access rights to all connectors to be used.
2. Enable the **Bypass Session Logon (authenticate user)** checkbox on the ShareScan Session Logon Service configuration screen of the Administration Console. For more information about bypassing the Session Logon, click here.
3. Sign in to the authentication application you are using. The Session Logon screen is displayed, with the User name field automatically filled in with the information from the card.
4. Type your Active Directory password into the relevant field.
5. Use all ShareScan workflows without further authentication needs until you press the **Logout** button. Pressing that button logs you out of ShareScan, thus you can use the device only for copying and print management, until you re-authenticate.
   If you log out of the authentication application, you cannot use the device until you reauthenticate.

Notes:

If you change your password, you have to go through the above process once more.
The authentication is only valid for connectors using the same Active Directory credentials you supplied on the Session Logon screen, and for connectors that are configured not to ask for credentials. You still have to authenticate separately if your card-based credentials are not the same as your credentials for logging in to the backend service of a connector (for instance, Lotus Notes).
You can test the username/password combination prior to enabling the Extender either via the built-in ShareScan Simulator, or at the device itself.

27 - Disabling the Extender

To disable the Single Sign-On Extender, disable Session Logon via the Administration Console.

28 - Database Lookup Extender

The Database Lookup Extender allows you to improve and customize any searches you plan to run on the various SQL databases connecting to your eCopy ShareScan Manager. You can use any connected MFP to run SQL queries on the servers connected to the particular Manager the device is attached to. The extender also allows you to get input data by selecting from options coming from a database or CSV file, and to enter data manually. In general, the purpose of the extender is to enable the configuration of complex business automation workflows, in most cases in conjunction with the usage of extenders (typically, Forms Processing Extender, or similar) and document services (for example, Image Control).

28.1- Configuring the extender

Before configuring the Lookup Extender, configure the Image Control or the FPE extenders (or the extenders and document services you want to use) to ensure that data publishing keys resulting from a barcode recognition or zonal OCR are set up properly.

As the extender interacts with databases supported by OLE DB, you must ensure that you have the relevant OLE DB driver installed when you plan to use a database type which is not supported by Windows by default (for example, Oracle).

The ShareScan software includes timers that automatically log you off after a certain period of inactivity. However, when the Cost Recovery Service is enabled, these timers are disabled and you remain logged on until you press **End** or **Complete** on the terminal, or until the terminal times out.

To configure the extender:

1. In the ShareScan Administration Console, select the **Configure services** tab. The tab displays a list of available services.
2. Select the **Database Lookup Extender**.
3. On the **Databases** tab, create a new connection (or select a database you want to connect to).
4. Use the **Lookup settings** tab to fine-tune the settings used when performing lookup queries on the connected database.

5. Use the **Settings** tab to regulate additional settings.
6. Click **Save**to save your settings.

28.2- Databases tab

Databases tab

28.2.1 - Databases settings

The following table describes the settings available on the **Databases** tab. The tab displays the name, type, and connection string for the stored database connections.

Setting	Description
New	Click this button to add a new database connection to the Extender. After clicking the **New** button, a dialog window is displayed, listing the already-existing connections. Clicking an existing connection, and selecting **OK** clones the connection. Clicking **New** displays the **Configure data source** window, allowing you to provide data for a new database connection.

Setting	Description
Configure data source	Access this window by clicking **New**, and selecting the **New** option on the displayed screen. You can set the following options: • **Database type**: use the dropdown menu to select your database. • **Settings**: depending on the selected database, the specific setting options will vary. The following settings are available (again, depending on the database type): • **Path to <database type>** database: type the folder path or click the **...** (browse) button to navigate to the location of the database file. • **Blank username and password**: check this option if you do not want to enter a specific set of credentials for accessing the database. If the option is checked, the user is prompted to enter credentials to access the database (usually this is not the preferred way of setting up the access, as administrators do not want to put the burden of an additional authentication on the user). • **SQL server**: use the dropdown menu to select the available SQL database instance. • **Catalog/Database**: use the dropdown menu to select the catalog you want to use. • **TNS name**: enter the TNS name of the Oracle server you want to use. • **Data Source Connection String**: enter the connection string of your database here. • **Build String**: click this button to put together a database-specific connection string. • **Test**: after specifying the connection settings, you must click Test to check whether the connection works. If the connection test is successful, you can click **OK** to create the database connection.
Data link properties	Access this window from the **Configure data source** screen, by selecting **Other** as the database type, and clicking **Build String**. Click through the options of this short Wizard to put together a connection string for your database: • On the **Provider** tab, select your OLE DB provider, and click **Next**. • On the **Connection** tab, enter the data source and login credentials into the appropriate fields, and click **Test Connection** to check the data. • On the **Advanced** tab, you can set the relevant network settings, connection timeout, and access permissions to the database. • On the **All** tab, you can check all the data link properties once more, and if so inclined, you can edit them here manually, by simply clicking the row you want to edit, and filling out the **Property Value**. • Click **OK** to finish setting up the data link properties.

Setting	Description
Remove	Click this button to remove a selected database connection.
Edit	Click this button to edit the properties of the selected database connection.

28.2.2 - Lookup settings

The following table describes the settings available on the **Lookup settings** tab. The tab allows you to create, customize, and modify lookup operations for your workflows.

Setting	Description
New	Click this button to add a new query to the Extender. Clicking the button opens the Lookup editor.

Setting	Description
Lookup editor	This editor allows you to create and modify queries. The following can be set: • **Lookup result key**: Enter the name of the data publishing key you want to use for finding the results. This key will be the output of the lookup operation. If left empty, and the rest of the dialog is filled, this field is populated automatically, based on the values of different fields; it can be edited any time if the dialog populates it automatically. • **Display label**: Enter a label of the text field that is displayed on the MFP UI for the specific field. If left blank, the field is populated automatically based on the value of the **Lookup result key** field. • **Lookup type**: allows you to select the type of lookup query to be used. The available choices are **Database lookup**, **Custom SQL query**, and **Expression**. By selecting **Database lookup**, you can use the simple user friendly editor to set up the lookup criteria. With **Custom SQL query**, you can use complex SQL queries (specified in a text editor window), while the **Expression** option allows you to specify C# expressions, allowing full flexibility in comparison and working logic. • **Lookup evaluation condition**: When the **always evaluated** option is selected, the lookup specified is always performed. If the other option is selected, the specified condition is evaluated – a selected data publishing key is checked if it is not blank, equal to a specified value, or matching a regular expression; the lookup operation is performed only when the result is true. • **Database**: use the dropdown menu to select the database on which the query will be run (referring to an item defined on the first tab). • **Data source**: use the dropdown menu to select the database table to be queried. • **Expression templates**: use the dropdown menu to select specific C# expression templates. When selected, you can click the pencil icon to copy the expression into the editor window. Clicking the **msdn** button opens a browser, and displays the expression-specific MSDN article (when you have an active Internet connection). • **Filter**: here, you can put together the filter methods used by the **Database lookup** queries. Use the **+** and **-** icons to add or remove search criteria. In the **Source field(s)** column, you can select a field (column) of the table of the selected database to compare with the value specified in the **Look up values(s)** column. By clicking the button with the ellipsis, you can specify a (constant) value right here, or by clicking on the button with the down-pointing arrow, you can select from the data publishing keys available. The second column is the place where the comparison operation can be defined. Rightmost column (Operator) comes into the picture when multiple lookup criteria is used (that is, there are more than one rows in the **Filter** table), and can have the AND or the OR value selected. • **Target field**: use the dropdown menu to select which database field will be used as the target criterion. • **Lookup behavior**: use this dropdown menu to set the number of results the query should consider. Select **One value only** if you are looking for a specific database entry; otherwise, select **Multiple values or not required**. When **One value only** is specified, and the result of the lookup was a single value, the UI interaction is initiated (at the MFP). If the lookup was not successful (value not found), the user has to enter a value into a text box at

28.2.3 - Settings

The following table describes the settings available on the **Settings** tab. The tab provides you with further configuration options for customizing the Extender workflows.

Setting	Description
Separator for multiple values	Use this to set the separator character for the query results. Used only if the **Lookup behavior** setting is set to **Multiple values or not required**.)
If lookup fails	Use this dropdown to set the behavior of the extender in case the lookup does not produce results. You can select the following: • **Abort workflow**: this option completely aborts the query workflow, and puts you back on the main extender screen. • **Consider as blank**: this option displays a blank results page, and you can re-run the query with the option of altering any parameters.
Force validation screens	Checking this option results in the extender displaying the validation screen on the MFP screen, allowing you to check the query settings once more prior to running the query.

29 - The eCopy Connector for Open Text Document Management, eDOCS Edition

The eCopy Connector for Open Text Document Management, eDOCS Edition enables users to scan documents directly into an Open Text document management system or a Hummingbird Enterprise DM document management system from an eCopy-enabled device.

Users can store documents in any eCopy-supported format (PDF, PDF/A, TIF Fax, TIF, JPG, DOC, DOCX, XPS, XLS, and XLSX).

29.1- Configuring the connector

For the generic connector configuration options, click here.

29.1.1 - Authentication settings

Field Name	Description
Type	Determines whether the user authenticates at the device. • Login as: Allows the user to use the connector without entering authentication information. The connector uses the specified user name and password as the authentication credentials at the device. • Runtime: Displays the Authentication screen at the device and requires users to enter their eDOCS user name and password each time they use the connector. If you use Session Logon and then select Runtime, the system will try to log in using the Session Logon credentials. If this fails, the connector Logon screen will appear and the user must enter the eDOCS DM credentials. This connector supports eDOCS Library, Windows and Novell authentication.
User name and Password	These credentials, which are required for use of the connector, are configured on your eDOCS system. They function differently depending on the type of authentication you select: • Login As: This account is used to access the connector at the device and to store the scanned documents. • Runtime: This account is used to retrieve the user list from the eDOCS server. The account must have rights to access all the libraries that you want to make available from the scanning device. **Note:** If you select Runtime authentication, the Author field at the device will display the name of the authenticated user.
Test	Tests the connection between eCopy ShareScan and the eDOCS server. You must test the connection before you can save your configuration. When the connection is tested successfully, the Library list displays the available libraries.

29.1.2 - Configure tab settings

Field Name	Description
Library list	Defines the libraries that are available to the user at the device. When you click **Test**, the list displays all the libraries that are available on the server. The libraries to which the user does not have access are disabled: • Enable: Includes the library in the list of libraries on the Login screen at the device. • Default: Displays the library as the initial selection in the list of libraries that the connector displays at the device. If you add a library to, or remove a library from your eDOCS server, you must test and save the connector profile to make the change visible at the device.

Field Name	Description
Select profile	Defines the behavior of the Profile selection screen at the device.
Display fields	Defines the behavior of the Document profile screen at the device: • All: The screen always appears and includes all fields. This is the default. • Required: Always displays the screen and includes only the fields designated as required in your eDOCS system. • None: If all required fields have default values, the screen does not appear and the document is stored with the default values. If any of the required fields do not have a default value, the screen appears and the user can provide values before storing the document.
Confirm storage	Defines the display of the storage confirmation screen at the device.
Use Cost Recovery values	Enables you to use values from the eCopy Cost Recovery Service as your default values for the client and matter fields instead of the values from the eDOCS server. This functionality requires the eCopyCost Recovery Service.

29.2- About profile selection

eDOCS allows you to create profiles that are used to collect information when documents are stored. These profiles are maintained on the eDOCS server and, depending on how you configure the connector and the version of eDOCS that you use, are available to the user at the device.

When you configure the connector to allow the user to select profiles, the user at the device can select the eDOCS profile for the scanned document from a list on the Select profile screen. To populate the list of profiles, the connector retrieves profiles stored on the eDOCS server. There are two types of profiles. The connector first searches for Type 1 profiles and then, if there are no Type 1 profiles, it searches for Type 2:

- Type 1: Profiles configured for groups to which the authenticated user belongs, and for the applications that correspond to the file type of the scanned document.
- Type 2:
  - eDOCS 6: Profiles not associated with any applications.
  - eDOCS 5: A single Primary profile.

Note:

The eDocs RM (Record Management) feature is not supported by the connector. If set to a group on the eDocs server, DM profile forms, RM profile forms and search forms (for example, LAWQBE) are displayed by the connector on the profile selection form, but selecting a search form or an RM profile form results in an error message, as the scanned

document cannot be stored. To avoid this situation, do not set RM profile form and search form to a group on the eDocs server.

29.2.1 - Profile selection settings

Version	Configuration selection	Profiles used
eDOCS 5	Allow selection	• Type 1 profiles. • If there is only one profile, the Profile selection screen does not appear. • If there are no Type 1 profiles, the Profile selection screen does not appear. The connector uses the Type 2 Primary profile.
	Use first form	• The connector uses the user's Primary profile and the Profile selection screen does not appear.
eDOCS 6	Allow selection	• Type 1 profiles. • If there are no Type 1 profiles, the system uses the first Type 2 profile and the Profile selection window does not appear. • If there is only one profile, the Profile Selection screen does not appear
	Use first form	• The connector uses the first Type 1 profile. • If there are no Type 1 profiles, the list includes Type 2 profiles.

Notes:

- If the authentication type is Login as, the authenticated user is the user specified on the **Configure** tab.
- The file type of the scanned document is set in the Administration Console, in **Settings > File Format**.
- If you are using eDOCS6 Server, a Profile type list also appears.

29.3- About related fields and default values

The fields and values available to the user at the device on the Document profile screen depend on how you have configured eDOCS.

29.3.1 - Related fields

If the fields in your database are linked together in a hierarchy of parent - child relationships, these relationships are reflected when the user selects values on the Document Profile screen at the device. Selecting a value in a field populates the fields above it in the hierarchy (parents, grandparents, and above) and in related fields at the same level (siblings). If the field is linked to fields lower in the hierarchy (children

and below), the values available in the lower fields are filtered to show only the values that are compatible with your selection.

29.3.2 - Default values

eDOCS also lets you specify default field values for the connector to use. You can specify default values at multiple levels, with a strict hierarchy that determine which default value takes precedence.

Note:

The connector always uses the strict hierarchy ordering rules followed by DM 5, even if you are using DM6.

Table 2: Default precedence values

Type	Assigned by	Applies to	DM5 Precedence
Group defaults	eDOCS administrator	All documents saved by all users in the specified group	1 (lowest)
Personal defaults	Individual user	All documents saved by that user	2
Group app. defaults	eDOCS administrator	All documents with a specific file extension saved by all users in the specified group	3
Personal app. defaults	Individual user	All documents with a specific file extension saved by that user	4 (highest)

29.4- Document security

The default ACL of a document stored using the connector will be the same as that for a document stored by the same user through the eDOCS Extensions Windows or Web clients.

On the Document profile screen, the user at the device can choose to activate document security. The following table shows the security selections available:

Table 3: Secure document settings

Type	Assigned by	Applies to
Unchecked	All	Full
Checked	Authenticated user	Full
	Author	Full
	Users and Groups in the default ACL	As specified in the default ACL

Note:
For more information on the use of ACLs by eDOCS, please consult the eDOCS product documentation.

29.5- Configuring an Express connector profile

To create an Express connector profile that does not display the Document Profile screen at the device, you must first create an eDOCS default profile for the user. The profile must either not contain any required fields or, if it contains required fields, the fields must be pre-filled with default values. For more information on configuring Express connector profiles, click here.

29.6- About searching on the Document profile screen

Some fields are followed by search (magnifying glass) buttons. You can use the button to open a Search screen that allows you to search the columns of the tables associated with the field.

To search for a document profile field value:

1. In the **Document profile** screen, click the search button of the field whose values you want to search for. The **Search** screen opens.
2. Use the **Filter** field to select the table column in which you want to search and then use the **By** field to search for specific information in the column. The filtered information appears in the list.
3. Select an item that you want to appear in the selected field on the **Document profile** screen. Information from all the other columns associated with the field appears on the right.
4. Click **OK**. The selected information appears in the field on the **Document profile** screen and related fields are either populated or filtered.

Note:
You do not need to configure the Search feature in the Administration Console.

30 - The eCopy Connector for EMC Documentum

The eCopy Connector for EMC® Documentum® allows users to scan documents directly into the EMC Documentum Repository of an EMC Documentum system from an eCopy-enabled device.

Users can store documents in any eCopy-supported format (PDF, PDF/A, TIF Fax, TIF, JPG, DOC, XPS, and XLS). For EMC Documentum server 6.0 or later, DOCX and XLSX formats are also supported.

30.1- Configuring the connector

For the generic connector configuration options, click here.

30.1.1 - Configuring a destination

The options available via the **Configure** tab allow you to configure the destinations used by the connector.

Field Name	Description
Express Wizard	Click this button to create an express destination via the Wizard. The express destination can be saved either to a new profile or to the current profile.
New	Displays the destination dialog for adding a new destination.
Edit	Displays the destination dialog for the selected destination, allowing you to edit its properties.
Copy	Copies the selected destination with a new name.
Remove	Deletes the selected destination from the list.
Move up	Moves the selected destination up the list.
Move down	Moves the selected destination down the list.
Summary	Displays the main settings. Every client form has a main row in this list with summary information according to its settings. The settings can be hidden by clicking the arrow icon.

30.1.1.1 - Destination Dialog, Generic Options

Field Name	Description
Destination name	Specify a unique destination name.
Express destination	If checked, the **Logon as** option is selected on the **Authentication** tab, **Store in specified cabinet or folder** is selected on the **Navigation** tab and the list on the **Doctypes** tab can contain only one document type which has no attributes to be shown.
If file name already exists	The following actions can be set: • Allow duplicated name • Create unique name (.1, .2, etc.) • Return error

30.1.1.2 - Destination Dialog, Authentication Tab

Field Name	Description
Logon as	If checked, a specified account is used to logon on the client side, thus the Authentication form is not shown. This is the express mode of the client authentication form

Field Name	Description
Logon at runtime	If checked, the Authentication form asks for user name, password and domain on the client side. This is the non-express mode of client authentication form, and the dialog enables selecting from the **Search while typing** dropdown list.
Repository	The dropdown list shows the connectable Repositories.
User name	Specifies the administrator's user name. Modifying the user name disables **Navigation**, **Doctypes** and **If file name already exists** settings, until a successful connection test.
Password	Specifies the administrator's password. Modifying the password disables **Navigation**, **Doctypes** and **If file name already exists** settings, until a successful connection test.
Domain	Specifies the administrator's domain name. The dropdown list shows domain names on the network, you can select one from there, or type it manually. Modifying the domain name disables **Navigation**, **Doctypes** and **If file name already exists** settings, until a successful connection test. This field is optional.
Test	Connects to the specified Repository with the specified administrator's account. If successful, **Navigation**, **Doctypes** and **If file name already exists** settings are enabled.
Search while typing	Connects to the Documentum server with the administrator's account and retrieves users list on runtime. The dropdown list becomes enabled when **Logon at runtime** is checked.

30.1.1.3 - Destination Dialog, Navigation Tab

Field Name	Description
Store in specified cabinet or folder	If checked, the document is stored in a specific cabinet/folder and the Location form is not shown. This is the express mode of the client location form.
Allow user to navigate	Enables you to select the types of cabinets that the user sees on the Location screen at the device. This is the non-express mode of the client location form.
Specific cabinet or folder	Sets the root point of the subfolder navigation to a specific location.
Entire Repository	Sets the root point of the subfolder navigation for the entire repository. The following values can be selected: • All Cabinets: shows all Cabinets. • Public and users private Cabinets: shows public Cabinets and private Cabinets owned by logged on users. • Users private Cabinets: shows only private Cabinets owned by logged on users.

Field Name	Description
Enable home cabinet	Displays the **Home cabinet** button on the Location screen at the device, allowing documents to be stored in the user's Home cabinet.
Enable subscriptions	Displays the **Subscriptions** button on the Location screen at the device, allowing documents to be stored in the user's subscription locations.
Enable subfolder navigation	Enables the user to navigate folders below the location chosen in the **Specify location** field. The user cannot access folders above the specified location.

30.1.1.4 - Destination Dialog, Doctypes Tab

Field Name	Description
Doctypes	The list view displays configured Doctypes. Note that at least one valid Doctype is required. • The first column indicates if the Doctype attributes are properly configured. • The second column displays the Doctype name • The third column displays the number of shown attributes from the selected attributes • The fourth column displays the defined file format of the document type. If a single Doctype is configured and the default format type corresponding to the scanned document type is specified, the Document form is skipped on the client.
New	Opens a window showing available doctypes.
Edit	Enables you to configure the attributes of the selected Doctype. The Doctype icon shows the Doctype as invalid until the attributes are configured, and the **OK** button is clicked. The attributes that you have configured and set as **Show** appear on the Attributes screen at the device.
Remove	Deletes the selected Doctype from the list.
Move up	Moves the selected Doctype up the list.
Move down	Moves the selected Doctype down the list.

30.1.2 - Express Wizard

This wizard enables creating an express destination in a new express profile (a profile which has only one express destination) or in the current profile step by step..

30.1.2.1 - Welcome Page

This page displays generic information on the aim of the Wizard.

30.1.2.2 - Destination Page

Field Name	Description
Create destination in a new profile	After finishing the wizard, all destinations are deleted and an express destination is created with the specified name in the current profile. The user can save the profile with a new name retaining the data of the current profile.
Create destination in the current profile	The destination is created in the current profile after finishing the wizard.
Destination name	Specify destination name. The destination name must meet the following criteria: • Must be unique in the profile. • Is case sensitive. • Name has to be specified. The length of name is not limited.

30.1.2.3 - Authentication Page

Field Name	Description
Repository	The dropdown list shows the connectable Repositories.
User name	Specifies the administrator's user name. Modifying the user name disables **Navigation**, **Doctypes** and **If file name already exists** settings, until a successful connection test.
Password	Specifies the administrator's password. Modifying the password disables **Navigation**, **Doctypes** and **If file name already exists** settings, until a successful connection test.
Domain	Specifies the administrator's domain name. The dropdown list shows domain names on the network, you can select one from there, or type it manually. Modifying the domain name disables **Navigation**, **Doctypes** and **If file name already exists** settings, until a successful connection test. This field is optional.
Test	Connects to the specified Repository with the specified administrator's account. If successful, **Navigation**, **Doctypes** and **If file name already exists** settings are enabled.

30.1.2.4 - Location Page

Field Name	Description
Specific cabinet or folder	Sets the root point of the subfolder navigation to a specific location.

30.1.2.5 - Doctypes Page

Field Name	Description
Doctypes	The list view displays configured Doctypes. Note that at least one valid Doctype is required. • The first column indicates if the Doctype attributes are properly configured. • The second column displays the Doctype name • The third column displays the number of shown attributes from the selected attributes • The fourth column displays the defined file format of the document type. If a single Doctype is configured and the default format type corresponding to the scanned document type is specified, the Document form is skipped on the client.
New	Open a window showing available doctypes.
Edit	Enables you to configure the attributes of the selected Doctype. The Doctype icon shows the Doctype as invalid until the attributes are configured, and the **OK** button is clicked. The attributes that you have configured and set as **Show** appear on the Attributes screen at the device.
Remove	Deletes the selected Doctype from the list.

31 - The eCopy Connector for Fax via Microsoft Exchange

The eCopy Connector for Fax via Microsoft Exchange enables users to scan and fax documents from an eCopy-enabled device through an email-to-fax gateway on the Microsoft Exchange server. To use this connector, you must have a network fax server and the appropriate Exchange server plug-in.

The recipient's fax number is included in the **To** field (on the ShareScan Client) in the format required by the fax server. The server plug-in recognizes the recipient address as a fax number and hands the request off to the network fax server for delivery as a fax.

While ShareScan always uses the ShareScan user account information to log on to the Exchange server and retrieve the Global Address List, it sends scanned documents from this account only if the **Login As** authentication option is selected.

31.1- About Exchange Environment connection protocols

The connector supports six combinations of connection protocols that can be used to connect to your Exchange server, depending on your environment. The Wizard automatically selects the protocol based on the Exchange environment information that you supply.

Protocol configuration	Microsoft Outlook required?	Description	Suggested use
MAPI/MAPI	Yes	Requires Exchange 5.5 server or later.	Use it to access old Exchange versions (Exchange 2003 or even older). MAPI requires a Microsoft mail client on the machine running the ShareScan Manager. MAPI protocol does not support saving new contacts to the users' Personal Contact list; queries against Personal Contacts can be executed.
LDAP/MAPI	Yes	Requires that the specified Service Account has access to a Global catalog server in the forest where the ShareScan Manager is running. Requires Exchange Server 2003 or later.	MAPI along with LDAP is recommended when your organizational unit uses old Exchange versions, but Global Catalog servers are available for GAL queries. You can restrict LDAP queries with profile settings for the organizational unit which uses a particular scanning device; queries are executed faster, and the result lists are considerably shorter.
LDAP/WEBDAV	No	Requires that the specified Service Account has access to a Global catalog server in the forest where the ShareScan Manager is running. Requires Exchange server 2003 or later.	WEBDAV along with LDAP is recommended when your company employs lot of people, uses Exchange 2007 or earlier Exchange servers, and needs simple firewall setups and communication over secured HTTPS. TCP ports 80 and 443 are supported (the latter for HTTPS communication). WEBDAV is not supported in Exchange versions above 2007, it was replaced by EWS in Exchange 2010.
WEBDAV/WEBDAV	No	Requires the front-end Exchange Server to be version 2003 or later.	WEBDAV is recommended when your company uses Exchange 2007 or earlier Exchange servers, and needs simple firewall setups and communication over HTTP/HTTPS. TCP ports 80 and 443 are supported (the latter for HTTPS communication). WEBDAV is not supported in Exchange versions above 2007, it was replaced by EWS in Exchange 2010.

Protocol configuration	Microsoft Outlook required?	Description	Suggested use
LDAP/EWS	No	Requires Exchange Server 2007 with Service Pack 1 or later.	EWS along with LDAP is recommended when your company employs a number of people, uses multiple Exchange servers, and you want to take advantage of the service URL autodiscover feature (administrator do not need to reconfigure ShareScan when the Exchange infrastructure is changed). You can restrict LDAP queries with profile settings for the organizational unit which uses a particular scanning device; queries are executed faster, and result lists are considerably shorter. Our LDAP protocol implementation autodetects the Global Catalog server, and supports SSL communication as well. EWS also supports cross domain setups, so can be used when ShareScan and the target Exchange server exist within separate domains.
EWS/EWS	No	Requires Exchange Server 2007 with Service Pack 1 or later.	Recommended when the ShareScan Manager works outside of Active Directory domains (can be used within the domain as well), and simple firewall setup is a requirement. Also the best choice when your Exchange server is hosted in a Datacenter, and you want to access that via HTTPS. EWS (Exchange Web Services) is based on SOAP/HTTPS, which transfers request and responses via TCP 443 port. EWS supports service URL autodiscovery, making it advantageous in environments where service endpoints change frequently. Limitations: supported versions are Exchange 2007 SP1 and above; **Search while typing** during login has limited functionality. Extras: Users can save new contacts into their Personal Contacts folder.

Notes:

When Microsoft Outlook is required, you must install it on the same computer as the ShareScan Manager so that the two applications can share common DLLs.
You must configure it as the default mail package. You must configure Microsoft Outlook 2000 to work with your Exchange server prior to using the ScanStation Client. eCopy also recommends that you configure Microsoft Outlook 2002, 2003, 2007, and 2010 to work with the Exchange server.

31.2- Configuring the connector

For the generic connector configuration options, click here.

31.2.1 - Exchange Profile Wizard settings

The Profile wizard helps the administrator to setup a basic protocol composite containing one or two protocols. The additional settings are set up with their defaults; any further tuning of the setting can be done by editing Properties.

Configuring via the Wizard follows the steps below:

1. **Select protocol composite**

Field Name	Description
Protocol	Select the protocol combination to be used.
User name	Enter the user name.
Password	Enter the password.
Domain	Enter the selected domain name.
Authentication	Select the type of authentication to be used.
Search user names	Turn the **Search while typing** function on or off.

2. **Configure selected composite**
   The components of this page differ according to the selected protocol combination.

Field Name	Description
LDAP settings	The following options can be set via the LDAP settings page: • Locate server at runtime: allows you to select an LDAP server during runtime. • Always use the following server: allows you to set an LDAP server to be used. • LDAP port: set the LDAP port here. The default port number is 389. • Server requires SSL: check this to enable SSL connection.
MAPI settings	The following options can be set via the MAPI settings pane: • Specified by user's default Outlook profile: allows you to use the default Outlook profile settings of the user. • Custom settings: allows you to specify an Exchange server, mail address, and mailbox ID to be used.
Exchange Web Services settings	The following option can be set via the Exchange Web Services settings: • Use the following service URL: allows you to enter a predefined service URL
WebDAV settings	The following options can be set via the WebDAV settings page: • Exchange server: The name or IP address of the Exchange server. • Server requires SSL for communication: communication with Exchange occurs via secure connection. • Use UPN Format for User Credentials (user@example.com): Uses UPN format for credentials instead of domain/username format. • Server uses forms-based authentication: Check this box when the Exchange server is configured to use Forms Based Authentication.

3. Configure fax format.
4. Review Summary.

31.2.2 - Protocol selector

Select the protocol combination to be used via this tab.

Field Name	Description
Protocol	Select the protocol composition you want to use.
User name	Enter the user name to be used.
Password	Enter the password to be used.
Domain	Enter the domain to be used.

Field Name	Description
Authentication	Select the authentication type: • Runtime: the client user is required to log on at the beginning of the workflow. • Login As: the provided credential is used for login at client side.
Search user names	Setting this combobox controls how the client side **Authentication** form manages the logon information: • Search while typing: The list of user names is queried as the user enters characters into the **User name** text box. • Search on demand: The query for the user names based on the entered few characters runs when the button with magnifier is pressed. • Disable search: The user is expected to enter the full user name, password and domain at client side. The Global Address book provider runs the query for the hints. The method of searching depends on the provider.
Testing the connection	Clicking the **Test** button tests the connector with the current settings.

31.2.3 - Protocol properties

The **Protocol properties** tab varies based on the selected protocol.

31.2.3.1 - LDAP Settings

Field Name	Description
Locate server at runtime	Click the **Find** button to locate the LDAP server during runtime.
Always use the following server	Specify the LDAP server manually.
Server requires SSL	Check if the server requires SSL connection. The default SSL port is 636.
LDAP port	Enter the port number to be used. The default is 389.
Credential type	Select the credential type: • Use the default credential: specified on the Protocol selector tab. • Connect anonymously • Use User defined credential: Specify the user DN and the password manually.
User DN	Only valid if **Use User defined credential** is specified.
Password	Only valid if **Use User defined credential** is specified.

Field Name	Description
LDAP search	Allows you to specify the attributes of the LDAP searches. The available settings are: • Base DN: Determines the LDAP search starts when typing in the LDAP authentication form or the Send form. Empty base DN prompts an error. • Search scope: Can be set to **All levels below starting point** or **One level below starting point**. • Search on: Allows defining the attributes to be searched on. • Max results: Sets the amount of results returned. The default value is 200.
Testing the connection	Clicking the **Test** button tests the connector with the current settings.

31.2.3.2 - WebDAV Settings

Field Name	Description
Exchange server	The name or IP address of the Exchange server.
Login URL	Specifies the ending of the Exchange WebDav URL used for the user login. It is set to "Exchange" by default for Exchange 2003 servers, and "owa" for Exchange 2007 servers. The edit field has a tooltip, which always shows the full Login URL, based on the current WebDav settings.
Defaults	Press this button to update the following fields of the dialog window with the default settings for Exchange 2003 or 2007 server: **Login URL**, **Form based authentication URL**, **Mail box URL**, **Enable mail box URL discovery**. Pressing the arrow on the right to switch between "Exchange 2003" and "Exchange 2007".
Server requires SSL for communication	When checked, all WebDAV communications with the Exchange store occur over HTTPS instead of HTTP.
Server uses nonstandard port	Allows the administrator to specify a nonstandard port for all WebDAV communication.
Server uses forms-based authentication	Check this box when the Exchange server is configured to use Forms Based Authentication (FBA). When FBA is configured on the Exchange server Outlook Web Access (OWA) presents users with a web page to enter credentials when instead of a dialog box.
Forms-based authentication URL	Specifies the ending of the Exchange WebDav URL used for the form-based authentication. It is set to `exchweb/bin/auth/owaauth.dll` by default for Exchange 2003 servers, and `owa/auth/owaauth.dll` for Exchange 2007 servers. The edit field has a tooltip, which always shows the full FBA URL, based on the current WebDav settings.

Field Name	Description
Mailbox URL	This setting is used if the mailbox URL could not be discovered by the connector. The connector composes the mail box URL based on the available information. You have the following choices: ▪ Default for Exchange 2003 This setting means that the mailbox URL is composed in the default way for Exchange 2003 servers (the Login URL followed by a slash and the exchange username). For example, if Login URL is `http://server/Exchange`, username is testuser, the composed mail box URL is `http://server/Exchange/testuser`. ▪ Default for Exchange 2007 This setting means that the mailbox URL is composed in the default way for Exchange 2007 servers,(the Login URL followed by a slash, then the exchange username, then the @ sign, followed by the domain). For example, if Login URL is `http://server/Exchange`, username is testuser, domain is testdomain, then the composed mail box URL is `http://server/Exchange/testuser@testdomain/`. ▪ Root URL, assuming redirect This setting means that the mailbox URL does not have to be composed, but simply the Login URL has to be used, as the Exchange server always redirects to the correct page. This works with Exchange 2007.
Use UPN Format for user credentials	This enables the connector to pass credentials in the User Principal Name format (user@domain.com) instead of the Domain\Username format. Some frontend servers can be configured to accept credentials only in the UPN format.
Enter the domain names that the user can select at the device	This option allows the user to specify a set of domains to be displayed to the user to pick from, as WebDAV/OWA queries do not return the Domain name for the users.
Testing the connection	Clicking the **Test** button tests the connector with the current settings.

31.2.3.3 - MAPI Settings

Field Name	Description
Exchange 2010 Client Access Server	You can specify if you want to use the Exchange Client Access Server (CAS). The following options are available: • Do not use CAS: select this option if you do not want to use CAS. • Use CAS: select this option if you want to use CAS. Choosing this option results in the **Service account properties** being displayed.
Server name	Specify the CAS server name (required if you use CAS).
Service account properties (Only visible if CAS is used)	The following options can be set: • Specified by user's default Outlook profile: allows you to use the default Outlook profile settings of the user. • Custom settings: allows you to specify an Exchange server, mail address, and mailbox ID to be used.
Test	Clicking the **Test** button tests the connector with the current settings.

31.2.4 - Web Services

Field Name	Description
Use the following service URL	Enter a valid full URL.
Autodiscover Service URL with usage of the email address below	Enter an email address to be used during the Autodiscovery process.
Redirection during discovery to these servers is allowed	Enter the URLs to which redirection is allowed.
Use EWS Impersonation	If checked, you can specify an account to be used for sending faxes when using this connector. This option is highly recommended when using **Bypass Session Logon (no authentication)** along with Cost Recovery or ID Services. The EWS Impersonation allows users to simply swipe their card when on the Session Logon screen, and the credentials entered under this option are used. Note that this function is only supported when using EWS protocol.
Testing the connection	Clicking the **Test** button tests the connector with the current settings.

31.2.5 - General settings

Allows you to set the generic settings of the Exchange connector.

Field Name	Description
Search recipients while typing	If checked, the hints appear at the client Send form as the user starts entering the recipient. If unchecked, the hints appear when the user presses the **Search** button next to the **To** or **Cc** field.
Enable user to manually enter fax number	The client is allowed to type the fax numbers manually.
Add message to Sent Items folder	If this feature is enabled, the message sent successfully is copied to the named folder.

31.2.6 - Sending options

This dialog tab provides control for the administrator over the default content of the mail – recipients, subject and note – and allows setting the express mode client workflow.

Field Name	Description
Display options	Manages the client side workflow.
Enable cover sheet	Enables the fax cover sheet.
Default cover sheet	Allows you to set the following cover sheet options: • Default Subject • Default Note: use the Manage Content button to specify a default note.
Default recipients	Allows you to manage the list of default recipients. The **Add** button allows you to add new members to the list, the **Edit** button allows you to modify the properties of the selected recipient, and the **Remove** button removes the selected recipient from the list. You can use the dropdown list to configure the data publishing behavior, selecting from the following options: • None: Default recipients • Data publishing • Default recipients and Data publishing For a practical example of configuring the Data Publishing with a connector, click here.

31.2.7 - Fax format settings

All settings in this table apply only to the eCopy Connector for Fax via Microsoft Exchange.

Section	Field Name	Description
Fax address format	Cover page / No cover page	Displays the fax format that you define in the Fax address format window.

Section	Field Name	Description
	Format	Opens the Fax Address Format window where you define the fax address format required by your fax server application or Internet fax service. Refer to the documentation for your fax application to obtain the correct format for the fax address. Since fax application vendors change these formatting schemes frequently, make certain you obtain the current format.
Valid characters in FAX number		The administrator can specify the valid characters accepted by the FAX server. The user is notified if invalid characters are entered on the client form. The defaults are: 01234567890()+-

31.3- Exchange connector profile settings

The Edit Profile window enables administrators who are more familiar with Exchange server environments to fine-tune the settings without relying on the Wizard. eCopy recommends that you use the Wizard to initially configure a connector profile. You can set the following:

- Protocol to be used
- Protocol properties
- Generic settings
- Sending options
- Fax format

31.4- Exchange Connector properties

The Properties window enables administrators who are more familiar with Exchange server environments to fine-tune the settings without relying on the Wizard. eCopy recommends that you use the Wizard to initially configure a connector profile. The **Properties** settings that are available depend on the connection protocols supported by your environment.

31.4.1 - Local address book

The **Local address book** tab enables you to configure the local address books that store Internet email addresses entered at the device, addresses that are not in the Global address list or in the Contacts folder. For

information about creating and configuring address books, see **Configuring support for Local address books**.

When you select the **Enable user to manually enter addresses when sending email** option on the **General settings** tab and you enable the **Internet address book** option on the **Local address book** tab, the system displays a **Save recipient** form, where you can save the email address. Saving the email address is not required; you can send the message without that.

32 - The eCopy Connector for Fax via Lotus Notes

The eCopy Connector for Fax via Lotus Notes enables users to scan and fax documents from an eCopy-enabled device through an email-to-fax gateway on the Lotus Notes server. To use this connector, you must have a network fax server and the appropriate Notes server plug-in.

The scanned document, along with sender and recipient information, is sent to the Notes server using the local Lotus Notes client.

Before faxing from a personal Lotus Notes account, you must first configure the eCopyMail pass-through database on a Domino HTTP server. Refer to the technical documentation in the following directory for further information and setup instructions: `<INSTALL_PATH>\Server\LNotes\` The default install path is `c:\program files\Nuance\ShareScan5`.

The connector provides access to the Lotus Notes address book as well as to the local Internet address book. When sending from a personal Lotus Notes account, a copy of the message is automatically delivered to the sender's Inbox folder.

Important!

You must install and configure the Lotus Notes client on the computer running the ShareScan Manager before you can install the Lotus Notes e-mail or fax connector. If you install the client after installing ShareScan, you must manually add the Lotus Notes client executable to the Path environment variable.

If the Lotus Notes client installation program 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. After the client installation program is finished, close it before configuring the connector in the Administration Console.

The recipient's fax number is included in the **To** field (on the ShareScan Client) in the format required by the fax server. The Notes server plug-in recognizes the recipient address as a fax number and hands the request off to the network fax server for delivery as a fax.

ShareScan typically uses the logon name specified in the Active ID file to access the Global Address List, while sending messages from the user's personal Lotus Notes account.

32.1- Configuring the connector

For the generic connector configuration options, click here.

32.1.1 - Fax format settings

Section	Field	Description
Fax address format	Cover page / No cover page	Displays the fax format that you define in the Fax Address Format window. Note that enabling the cover page via this option does not overrule the similar settings of the fax server.
	Format	Opens the Fax Address Format window where you define the fax address format required by your fax server application or Internet fax service. Refer to the documentation for your fax application to obtain the correct format for the fax address. Because fax application vendors change these formatting schemes frequently, make certain you obtain the current format.
	Embedded tags	Allows for embedding tags into the fax address.

32.1.2 - Lotus Notes configuration settings

Section	Field Name	Description
ShareScan User The account used to access the Global Address List.	Active ID file	The name of the Lotus Notes ID file installed on the local computer.
	User name	The user name associated with the Active ID file.
	Password	The password associated with the Active ID file.
	Test	Validates the logon information.
Send options	Send from personal account	Sends email from a personal Lotus Notes account, rather than from the ShareScan User account. This option is available only if the **Lotus Notes Address Book** option is enabled (on the **Address books** tab). If you select this option, you must configure a Domino HTTP/HTTPS server to use the eCopyMail pass-through database and specify the Domino Server, Mail Send Port, and encryption options.

Section	Field Name	Description
	Domino server	The name of the HTTP/HTTPS server where the eCopyMail pass-through database is installed: • For HTTP: Enter the server name, IP address, or fully qualified domain name, as appropriate, for your Domino environment. • For SSL/HTTPS: Enter the server name exactly as it appears in the SSL certificate. For example, if the name is “lsphere.ecopydocs.com”, enter this text in the field.
	Mail send port	The port number used to send mail (defaults are 80 for HTTP; 443 for SSL/HTTP).
	Use SSL/HTTPS	Encrypts communication with the HTTP server using SSL/HTTPS.

Note:
eCopy recommends that you create a generic Lotus Notes account for use by ShareScan.

32.1.3 - Content settings

Field Name	Description
Subjects	Displays a list of subjects appearing in the Subjects List of the client UI Send Form. Buttons are provided to **Add**, **Edit** and **Delete** subjects, as well as move a selected subject up or down in the list. Use of wildcards is allowed, the supported wildcards are: • `$$USER_NAME$$` - Sender. • `$$FILENAME$$` - File name.

32.1.4 - Address book

Section/Field Name	Description
Lotus Notes address book	If checked, enables the Lotus Notes address book. Use the **Address book** dropdown list to select a directory to be used, and the **Search on** dropdown list to set the search criterion.

Section/Field Name	Description
Fax address book	If checked, enables the Fax address book. Using the **Configure** button, you can access additional settings for the address book: • Setting database, address book, user, and search criteria • Managing the address book via the **Add**, **Delete**, **Import**, and **Export** options
Search while typing	If checked, enables the functionality.

32.1.5 - Express settings

Express mode allows the connector to function with a minimum of user input at the device. The subject, note, and recipient list are preconfigured on the **Express** tab so the user does not have to enter any of this information.

Field Name	Description
Enable	Enabling the Express function designates the profile you are creating as an Express profile.
Subject	Enter the subject to be used for messages.
Note	Enter the note you want to use.
Formatted fax email addresses	Use the **Add** and **Delete** buttons to manage the list of fax recipients.
Attach cover sheet	Send a cover sheet containing the Name, Fax number, and Note to the recipient with each faxed document. A cover sheet can only be sent with a fax if the **Use Cover Sheet** option is enabled in the RightFax FaxUtil client for the authenticated user (see your RightFax documentation).

33 - The eCopy Connector for Fax via Print

The eCopy Connector for Fax via Print is for use with MFPs or scanners that are connected to an eCopy ScanStation.

The connector enables users to scan and fax documents from an eCopy-enabled device through a third-party fax driver. The fax driver displays its own user interface, if any, on the ScanStation. Some fax drivers display an email client.

Note:

You can create Fax via Print connector profiles on any ShareScan Manager and publish them to any Manager that supports the ShareScan embedded software. However, you cannot run the Fax via Print connector on a device running the ShareScan embedded software.

You must configure the ScanStation Client to use the hard keyboard. This is because the soft keyboard does not support a third-party fax driver interface.

Before configuring a Fax via Print connector profile, install the fax driver on the ScanStation, or, if supported by the driver, on a network print server.

The connector supports the following Print/Fax drivers:

- Canon Fax
- RightFax
- Nortel CallPilot Fax

33.1- Configuring the connector

For the generic connector configuration options, click here.

Section/Field Name	Description
Print driver	A list of the available print drivers that you can use to fax scanned documents.
Authenticate user	Specifies the type of user authentication at the device: • None: The connector will not prompt the user for logon information. • Novell: The default Novell Netware tree. • Windows: The default Windows NT domain.

34 - The eCopy Connector for Fax via SMTP

The eCopy Connector for Fax via SMTP enables users to scan and fax documents from an eCopy-enabled device through an SMTP email-to-fax gateway. To use this connector, you must have a network fax server and the appropriate SMTP server plug-in.

The scanned document along with the sender and recipient information is sent to the SMTP server as a MIME-formatted mail message.

The recipient's fax number is included in the **To** field (on the ShareScan Client) in the format required by the fax server. The server plug-in recognizes the recipient address as a fax number and hands the request off to the network fax server for delivery as a fax.

34.1- Configuring the connector

For the generic connector configuration options, click here.

34.2- Connector properties

The **Properties** window enables administrators who are more familiar with LDAP to fine-tune the settings, without relying on the Wizard.

- Logon / SMTP settings
- LDAP settings
- Address book settings
- Sending options settings
- Fax format settings

34.2.1 - Logon / SMTP settings

Select the protocol combination to be used via this tab.

Field Name	Description
Authentication	Select the authentication type from the dropdown list: • Runtime: LDAP • None: Send from generic • None: Send from generic email address specified by Data Publishing For a practical example of configuring the Data Publishing with a connector, click here.
Allow user to modify	If checked, the user is able to customize the email field on each scan.
Generic email:	Allows the administrator to provide a generic email address to specify as the sender.
Server	IP or DNS name of the SMTP server.
Port	Port address of the SMTP server. Default is 25.
Test	Clicking the **Test** button tests the connector with the current settings.
Server requires SSL	Specifies if SSL is used for the SMTP communication.

Field Name	Description
Authentication	Define the type of authentication behavior for the SMTP server: • **Runtime: Prompt sender for a username and password**: the SMTP Authentication form is displayed to the user at runtime after the Send form. • **None**: When selected, the user is not prompted for a username and password. In addition the connector does not attempt any authentication with the SMTP server. The email send process may fail if the server requires authentication. • **Login as**: When selected the fields Username and Password will display below the Authentication combo in admin. Here the administrator can specify a set of credentials that will always be used when sending an email from the connector. • **Use senders LDAP userID attribute and runtime password**: When this option is selected and if the LDAP address book is enabled, the connector utilizes the LDAP userID attribute and password provided at the User Logon form to authenticate them against the SMTP server. If the LDAP address book is not enabled at the time of closing the properties dialog we will show an error to the user and tell them LDAP must be enabled or a different SMTP authentication type must be chosen.
Use specified domain if secure SMTP is enabled	If checked, the domain box is enabled and the user can input a domain. During the send process, the connector provides this domain along with username and password to the SMTP server.

34.2.2 - LDAP settings

Controls the various LDAP settings of the connector.

Field Name	Description
Enable LDAP address book	Click the **Find** button to locate the LDAP server during runtime.
Server	IP or DNS name of the LDAP server.
Port	Port number of the LDAP server for communication purposes. The default is 389.
Server requires SSL	Check if the server requires SSL connection.
User DN	User DN of the logged in user.
Password	Password of the logged in user.
Connect anonymously	Determines if the connector connects to the LDAP anonymously or if a UserDN and password are provided. Not all LDAP servers allow anonymous connections.

Field Name	Description
Advanced LDAP settings	Allows you to define what the actual attribute is called on the LDAP server itself and allows customization of LDAP attributes to return during your searches. The available settings are: • Person: Allows defining the actual ObjectClass to represent the “person” class during a recipient and sender search. • Group: Allows defining a second ObjectClass to represent the “Group” class during a recipient search only. • First name: Allows defining the actual attribute name to search for. • Last name: Allows defining the actual attribute name to search for. • Common name: Allows defining the actual attribute name to search for. • User ID: Allows defining the actual attribute name to search for. • Email: Allows defining the actual attribute name to search for. • Sender: Specifies custom attributes belonging to the class. Note that anything outside the square brackets is displayed as plain text.
LDAP search	Allows you to specify the attributes of the LDAP searches. The available settings are: • Base DN: Determines the LDAP search starts when typing in the LDAP authentication form or the Send form. Empty base DN prompts an error. • Search scope: Can be set to **All levels below starting point** or **One level below starting point**. • Search on: Allows defining the attributes to be searched on. • Search while typing • Max results: Sets the amount of results returned. The default value is 200.
Test	Clicking the **Test** button tests the connector with the current settings.

34.2.3 - Address book

Section/Field Name	Description
Enable Nuance address book	Enables the Nuance address book.
Database	Enables you to **Select** or **Create** a database. To create a database, you must provide the following data: • SQL server name: a valid SQL server name and instance • Database: the database name for the Nuance address book. • User ID: the identification of the user. • Password: the password required to access the database.

Section/Field Name	Description
Search on	Set the search parameters you want to use.
Address book	Shows the name of the selected address book.
User	Displays the name of the selected user.
Manage	Use the **Add**, **Delete**, **Import**, and **Export** buttons to manage the address data list.

34.2.4 - Sending options

You can set up the Express mode using the **Sending options** tab.

Section/Field Name	Description
Display options	Allows you to set the send form options: • Show • Show without CC field • Skip and send to default recipients • Skip and send to self
Default cover sheet	Allows you to set a default cover sheet.
Manage contents	Allows you to set the action taken.
Default recipients	Allows you to manage the default recipients. Using the **Add** button, you can select whether you want to add the recipients to the To, CC, or BCC fields.
Data publishing	Allows you to set the data publishing action: • Ignore Data Publishing values • Recipients are taken from Data Publishing only • Combine values with default recipients For a practical example of configuring the Data Publishing with a connector, click here.
Send copy to sender	Allows you to set the default message.
Manage content	Allows you to set the action taken.

34.2.5 - Fax Format settings

Section	Field	Description
Fax address format	Cover page / No cover page	Displays the fax format that you define in the Fax Address Format window.
	Format	Opens the Fax address format window where you define the fax address format required by your fax server application or Internet fax service. Refer to the documentation for your fax application to obtain the correct format for the fax address. Because fax application vendors change these formatting schemes frequently, make certain you obtain the current format.
	Embedded tags	Allows for embedding tags into the fax address.

34.2.6 - Connector Wizard settings

The Wizard enables administrators to initially configure the connector. Many windows contain a **Test** button that enables you to validate the logon information or test the server connection.

Wizard window	Field	Description
LDAP server type	Server type	The available server types: • None (disable LDAP address book) • Generic LDAP server • Windows Active Directory • Windows Active Directory (Untrusted) • Novell eDirectory • Netscape LDAP server • Open LDAP server • IBM Domino server If your server type is not on the list, select the **Generic LDAP server** option
	LDAP attributes	Enables you to set the attributes for the LDAP classes used by your server or to accept the defaults shown here.
Windows Active Directory server account	Account settings	Active Directory Server Account settings: • User name • Password • Domain The Wizard uses this information to set the user DN and server name. Available only if you select Active Directory as the server type.

Wizard window	Field	Description
LDAP server settings	Connect anonymously	Bypasses the Select LDAP User window and allows anonymous connection to the LDAP server, if the server supports anonymous authentication. Not available if you select Active Directory as the server type.
	LDAP server	LDAP server settings: • User DN • Password • Server • Port • Server requires SSL You must provide the full user DN if the server requires it. The Wizard assumes that the server is using the default port number (389). The Wizard resets the port back to 389 if it was changed in the **Properties** dialog box. Clicking the **Test** button checks your settings.
Search settings	Defines how the LDAP server searches the address book. Enables you to select a user from the LDAP tree in the Select LDAP User window. Not available if you select Active Directory as the server type.	
	Base DN	The node on the LDAP tree from which all searches should begin. If you do not know the node, click the **Browse** button and select the node from the tree structure in the selection window.
	Search scope	Select a search level: • All levels below search starting point: Allows expanded searching. • One level below search starting point: Optimizes LDAP queries and improves performance.
	Sender search	The search criterion that the server uses to find the sender: • First Name • Last Name • Common Name • User ID (default) The setting defines the information that the user sees on the Logon screen at the device.
	Search while typing	Enables or disables the **Search while typing** functionality for the related field at the device.
	Max results	The limit on the number of results to be returned by the LDAP search. The default value is 200.
SMTP settings	Select your SMTP server and the type of authentication that will be required of the user at the device.	

Wizard window	Field	Description
User login settings	Server	The SMTP server name
	Port	The SMTP port number.
	Authentication	The type of authentication to use on the SMTP server. Available only if SMTP Basic Authentication is enabled on the server.
	Generic e-mail	A generic email address that is used as the sender account for all email.
	User Modify	The user at the device can modify the sender's email address.
	Runtime: LDAP	Requires the user at the device to enter the user name and password specified for the LDAP server.
	Runtime: Windows	Enables users at the device to use their Windows logon information, via the SAMAccountName attribute, to log on. The **Domain** field specifies the Windows domain name, populated from the Account Settings window. This is required if you select the Windows option. Available only if you select Active Directory as the server type.
	Runtime: Novell	The Novell tree. This is required if you select the **Novell** option. Available only if you select eDirectory as the server type.
Fax address format	Cover page / No cover page	Displays the fax format that you define in the Fax Address Format window.
	Format	Opens the Fax address format window where you define the fax address format required by your fax server application or Internet fax service. Refer to the documentation for your fax application to obtain the correct format for the fax address. Since fax application vendors change these formatting schemes frequently, make certain you obtain the current format.
Settings summary	Enables you to review your settings. Use the **Back** button if you need to change any settings. Use the **Finish** button to apply your settings to the connector profile.	

34.2.7 - SMTP settings

Section	Field	Description
SMTP server	Server	The IP address or DNS name of the SMTP server to use for outgoing messages. If the server supports anonymous access, it must be disabled if you want to use SMTP authentication.
	Port	The SMTP port number (default is 25).
	Server requires SSL	Enables Secure Socket Layer (SSL) to be used for SMTP communication. If you select this option, you must install a valid SSL certificate on the same device as the connector.
Authentication	Runtime: Prompt Sender for a user name and password	Prompts the user at the device to enter a user name and password when the user presses the **Send** button on the Send screen. Available only if SMTP Basic Authentication is enabled on the server. **Note:** If Session Logon is enabled, and SSL is not enabled, eCopy recommends that you select “None” or “Login as”.
	None	Use if the SMTP server does not require authentication. The user at the device is not required to supply any credentials. If the server requires authentication, the email send process can fail.
	Login as	Enables the user at the device to connect to the SMTP server without being prompted for authentication information. The connector uses the user name and password set by the administrator.
	Use Sender’s User ID, LDAP attribute, and runtime password	Uses the sender’s LDAP authentication information to connect to the SMTP server. To use this option, you must enable the LDAP address book on the **LDAP settings** tab.

35 - The eCopy Connector for Lotus Notes

The eCopy Connector for Lotus Notes Mail enables users to send scanned documents from an eCopy-enabled device as email attachments from either a generic Lotus Notes account or from the user's personal Lotus Notes account. eCopy recommends that you create a generic Lotus Notes account for use by ShareScan.

Before email can be sent from a personal Lotus Notes account, you must first configure the eCopyMail pass-through database on a Domino HTTP server. Refer to the technical documentation in the following directory for further information and setup instructions: `<INSTALL_PATH>\Server\LNotes\` The default install path is `c:\program files\Nuance\ShareScan5.1`.

The connector provides access to the Lotus Notes address book as well as to the local Internet address book. When sending from a personal Lotus Notes account, a copy of the message is automatically delivered to the sender’s Inbox folder.

Important!

You must install and configure the Lotus Notes client on the computer running the ShareScan Manager before you can install the Lotus Notes email or fax connector. If you install the client after installing ShareScan, you must manually add the Lotus Notes client executable to the **Path environment** variable.

If the Lotus Notes client installation program 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. After the client installation program is finished, close it before configuring the connector in the Administration Console.

ShareScan typically uses the logon name specified in the Active ID file to access the Global Address List, while sending messages from the user's personal Lotus Notes account.

35.1- Configuring the connector

For the generic connector configuration options, click here.

Section	Field Name	Description
ShareScan User The account used to access the Global Address List.	Active ID file	The name of the Lotus Notes ID file installed on the local computer.
	User name	The user name associated with the Active ID file.
	Password	The password associated with the Active ID file.
	Test	Validates the logon information.
Send options	Send from personal account	Sends email from a personal Lotus Notes account, rather than from the ShareScan User account. This option is available only if the **Lotus Notes Address Book** option is enabled (on the **Address books** tab). If you select this option, you must configure a Domino HTTP/HTTPS server to use the eCopyMail pass-through database and specify the Domino Server, Mail Send Port, and encryption options.
	Domino server	The name of the HTTP/HTTPS server where the eCopyMail pass-through database is installed: • For HTTP: Enter the server name, IP address, or fully qualified domain name, as appropriate, for your Domino environment. • For SSL/HTTPS: Enter the server name exactly as it appears in the SSL certificate. For example, if the name is "lsphere.ecopydocs.com", enter this text in the field.
	Mail send port	The port number used to send mail (defaults are 80 for HTTP; 443 for SSL/HTTP).

Section	Field Name	Description
	Use SSL/HTTPS	Encrypts communication with the HTTP server using SSL/HTTPS.
Send to self		Disables the list of recipients and sends the scanned documents only to the logged on user. You can use the $$FILENAME$$ name variable on the Subject or Notes line to distinguish among scanned documents.
Enable user to Cc recipients when sending mail		Enables the user at the device to send a copy of a message to one or more recipients who are not the primary recipients.

Note:
eCopy recommends that you create a generic Lotus Notes account for use by ShareScan.

35.1.1 - Address book

Section/Field Name	Description
Lotus Notes address book	If checked, enables the Lotus Notes address book. Use the **Address book** dropdown list to select a directory to be used, and the **Search on** dropdown list to set the search criterion.
Internet address book	If checked, enables the Internet address book. Using the **Configure** button, you can access additional settings for the address book: • Setting database, address book, user, and search criteria • Managing the address book via the **Add**, **Delete**, **Import**, and **Export** options
Search while typing	If checked, enables the functionality.

35.1.2 - Content settings

Field Name	Description
Subjects	Displays a list of subjects appearing in the Subjects List of the client UI Send Form. Buttons are provided to **Add**, **Edit** and **Delete** subjects, as well as move a selected subject up or down in the list. Use of wildcards is allowed, the supported wildcards are: • `$$USER_NAME$$` - Sender. • `$$FILENAME$$` - File name.
Notes	Select this option of the dropdown menu to display a list of customized notes that appear on the Notes List of the client UI. Moving the cursor over a Note in the list displays an informational "bubble" with the entire contents of the Note. This allows the user to view an entire Note regardless of its length. Use of wildcards is allowed, the supported wildcards are: • `$$USER_NAME$$` - Sender • `$$RECIPIENTS$$` - Recipients • `$$FILENAME$$` - File name • `$$FILESIZE$$` - File size • `$$PAGECOUNT$$` - Page count
Email address format in message content	Set the email display format for the message.
Byline	Displays a customizable message in the body of the email.

35.1.3 - Express settings

Express mode allows the connector to function with a minimum of user input at the device. The subject, note, and recipient list are preconfigured on the **Express** tab so the user does not have to enter any of this information.

Field Name	Description
Enable	Enabling the Express function designates the profile you are creating as an Express profile.
Subject	Enter the subject to be used for messages.
Note	Enter the note you want to use.
To	Use the **Add** and **Delete** buttons to manage the recipients.
Cc	Use the **Add** and **Delete** buttons to manage the recipients.

36 - The eCopy Connector for Microsoft Exchange

The eCopy connector for Microsoft Exchange enables a user to send scanned documents from an eCopy-enabled device as email attachments from a generic Microsoft Exchange account or from the user's personal Microsoft Exchange account. eCopy recommends that you create a generic Microsoft Exchange account for use by ShareScan.

While ShareScan always uses the ShareScan user account information to log on to the Exchange server and retrieve the Global Address List, it sends scanned documents from this account only if the **Login As** authentication option is selected.

36.1- About Exchange Environment connection protocols

The connector supports six combinations of connection protocols that can be used to connect to your Exchange server, depending on your environment. The Wizard automatically selects the protocol based on the Exchange environment information that you supply.

Protocol con-figuration	Microsoft Outlook required?	Description	Suggested use
MAPI/MAPI	Yes	Requires Exchange 5.5 server or later.	Use it to access old Exchange versions (Exchange 2003 or even older). MAPI requires a Microsoft mail client on the machine running the ShareScan Manager. MAPI protocol does not support saving new contacts to the users' Personal Contact list; queries against Personal Contacts can be executed.
LDAP/MAPI	Yes	Requires that the specified Service Account has access to a Global catalog server in the forest where the ShareScan Manager is running. Requires Exchange Server 2003 or later.	MAPI along with LDAP is recommended when your organizational unit uses old Exchange versions, but Global Catalog servers are available for GAL queries. You can restrict LDAP queries with profile settings for the organizational unit which uses a particular scanning device; queries are executed faster, and the result lists are considerably shorter.

Protocol configuration	Microsoft Outlook required?	Description	Suggested use
LDAP/WEBDAV	No	Requires that the specified Service Account has access to a Global catalog server in the forest where the ShareScan Manager is running. Requires Exchange server 2003 or later.	WEBDAV along with LDAP is recommended when your company employs lot of people, uses Exchange 2007 or earlier Exchange servers, and needs simple firewall setups and communication over secured HTTPS. TCP ports 80 and 443 are supported (the latter for HTTPS communication). WEBDAV is not supported in Exchange versions above 2007, it was replaced by EWS in Exchange 2010.
WEBDAV/WEBDAV	No	Requires the front-end Exchange Server to be version 2003 or later.	WEBDAV is recommended when your company uses Exchange 2007 or earlier Exchange servers, and needs simple firewall setups and communication over HTTP/HTTPS. TCP ports 80 and 443 are supported (the latter for HTTPS communication). WEBDAV is not supported in Exchange versions above 2007, it was replaced by EWS in Exchange 2010.
LDAP/EWS	No	Requires Exchange Server 2007 with Service Pack 1 or later.	EWS along with LDAP is recommended when your company employs a number of people, uses multiple Exchange servers, and you want to take advantage of the service URL autodiscover feature (administrator do not need to reconfigure ShareScan when the Exchange infrastructure is changed). You can restrict LDAP queries with profile settings for the organizational unit which uses a particular scanning device; queries are executed faster, and result lists are considerably shorter. Our LDAP protocol implementation autodetects the Global Catalog server, and supports SSL communication as well. EWS also supports cross domain setups, so can be used when ShareScan and the target Exchange server exist within separate domains.

Protocol con-figuration	Microsoft Outlook required?	Description	Suggested use
EWS/EWS	No	Requires Exchange Server 2007 with Service Pack 1 or later.	Recommended when the ShareScan Manager works outside of Active Directory domains (can be used within the domain as well), and simple firewall setup is a requirement. Also the best choice when your Exchange server is hosted in a Datacenter, and you want to access that via HTTPS. EWS (Exchange Web Services) is based on SOAP/HTTPS, which transfers request and responses via TCP 443 port. EWS supports service URL autodiscovery, making it advantageous in environments where service endpoints change frequently. Limitations: supported versions are Exchange 2007 SP1 and above; **Search while typing** during login has limited functionality. Extras: Users can save new contacts into their Personal Contacts folder.

Notes:

When Microsoft Outlook is required, you must install it on the same computer as the ShareScan Manager so that the two applications can share common DLLs.

You must configure it as the default mail package. You must configure Microsoft Outlook 2000 to work with your Exchange server prior to using the ScanStation Client. eCopy also recommends that you configure Microsoft Outlook 2002, 2003, 2007, and 2010 to work with the Exchange server.

36.2- Configuring the connector

For the generic connector configuration options, click here.

36.2.1 - General settings

Allows you to set the generic settings of the Exchange connector.

Field Name	Description
Search Global Address List	Allows searching in the Global Address List.
Search Outlook contacts	Allows searching in the Outlook contacts.
Search recipients while typing	If checked, the hints appear at the client Send form as the user starts entering the recipient. If unchecked, the hints appear when the user presses the **Search** button next to the **To** or **Cc** field.
Enable user to manually enter email address	The client is allowed to enter email addresses manually.
Importance	Set the Importance of the mail message.
Delivery receipt	Set if you request a delivery receipt.
Sensitivity	Set the sensitivity of the message.
Read receipt	Set if you request a read receipt.
Add message to Sent Items folder	If this feature is enabled, the message sent successfully is copied to the named folder.

36.2.2 - Protocol selector

Select the protocol combination to be used via this tab.

Field Name	Description
Protocol	Select the protocol composition you want to use.
User name	Enter the user name to be used.
Password	Enter the password to be used.
Domain	Enter the domain to be used.
Authentication	Select the authentication type: • Runtime: the client user is required to log on at the beginning of the workflow. • Login As: the provided credential is used for login at client side.
Search user names	Setting this combobox controls how the client side **Authentication** form manages the logon information: • Search while typing: The list of user names is queried as the user enters characters into the **User name** text box. • Search on demand: The query for the user names based on the entered few characters runs when the button with magnifier is pressed. • Disable search: The user is expected to enter the full user name, password and domain at client side. The Global Address book provider runs the query for the hints. The method of searching depends on the provider.

Field Name	Description
Testing the connection	Clicking the **Test** button tests the connector with the current settings.

36.2.3 - Protocol properties

The **Protocol properties** tab varies based on the selected protocol.

LDAP settings

36.2.3.1 - LDAP Settings

Field Name	Description
Locate server at runtime	Click the **Find** button to locate the LDAP server during runtime.
Always use the following server	Specify the LDAP server manually.
Server requires SSL	Check if the server requires SSL connection. The default SSL port is 636.
LDAP port	Enter the port number to be used. The default is 389.
Credential type	Select the credential type: • Use the default credential: specified on the Protocol selector tab. • Connect anonymously • Use User defined credential: Specify the user DN and the password manually.
User DN	Only valid if **Use User defined credential** is specified.
Password	Only valid if **Use User defined credential** is specified.
LDAP search	Allows you to specify the attributes of the LDAP searches. The available settings are: • Base DN: Determines the LDAP search starts when typing in the LDAP authentication form or the Send form. Empty base DN prompts an error. • Search scope: Can be set to **All levels below starting point** or **One level below starting point**. • Search on: Allows defining the attributes to be searched on. • Max results: Sets the amount of results returned. The default value is 200.
Testing the connection	Clicking the **Test** button tests the connector with the current settings.

36.2.3.2 - WebDAV Settings

Field Name	Description
Exchange server	The name or IP address of the Exchange server.

Field Name	Description
Login URL	Specifies the ending of the Exchange WebDav URL used for the user login. It is set to "Exchange" by default for Exchange 2003 servers, and "owa" for Exchange 2007 servers. The edit field has a tooltip, which always shows the full Login URL, based on the current WebDav settings.
Defaults	Press this button to update the following fields of the dialog window with the default settings for Exchange 2003 or 2007 server: **Login URL**, **Form based authentication URL**, **Mail box URL**, **Enable mail box URL discovery**. Pressing the arrow on the right to switch between "Exchange 2003" and "Exchange 2007".
Server requires SSL for communication	When checked, all WebDAV communications with the Exchange store occur over HTTPS instead of HTTP.
Server uses nonstandard port	Allows the administrator to specify a nonstandard port for all WebDAV communication.
Server uses forms-based authentication	Check this box when the Exchange server is configured to use Forms Based Authentication (FBA). When FBA is configured on the Exchange server Outlook Web Access (OWA) presents users with a web page to enter credentials when instead of a dialog box.
Forms-based authentication URL	Specifies the ending of the Exchange WebDav URL used for the form-based authentication. It is set to `exchweb/bin/auth/owaauth.dll` by default for Exchange 2003 servers, and `owa/auth/owaauth.dll` for Exchange 2007 servers. The edit field has a tooltip, which always shows the full FBA URL, based on the current WebDav settings.

Field Name	Description
Mailbox URL	This setting is used if the mailbox URL could not be discovered by the connector. The connector composes the mail box URL based on the available information. You have the following choices: ▪ Default for Exchange 2003 This setting means that the mailbox URL is composed in the default way for Exchange 2003 servers (the Login URL followed by a slash and the exchange username). For example, if Login URL is `http://server/Exchange`, username is testuser, the composed mail box URL is `http://server/Exchange/testuser`. ▪ Default for Exchange 2007 This setting means that the mailbox URL is composed in the default way for Exchange 2007 servers,(the Login URL followed by a slash, then the exchange username, then the @ sign, followed by the domain). For example, if Login URL is `http://server/Exchange`, username is testuser, domain is testdomain, then the composed mail box URL is `http://server/Exchange/testuser@testdomain/`. ▪ Root URL, assuming redirect This setting means that the mailbox URL does not have to be composed, but simply the Login URL has to be used, as the Exchange server always redirects to the correct page. This works with Exchange 2007.
Use UPN Format for user credentials	This enables the connector to pass credentials in the User Principal Name format (user@domain.com) instead of the Domain\Username format. Some frontend servers can be configured to accept credentials only in the UPN format.
Enter the domain names that the user can select at the device	This option allows the user to specify a set of domains to be displayed to the user to pick from, as WebDAV/OWA queries do not return the Domain name for the users.
Testing the connection	Clicking the **Test** button tests the connector with the current settings.

36.2.3.3 - MAPI Settings

Field Name	Description
Exchange 2010 Client Access Server	You can specify if you want to use the Exchange Client Access Server (CAS). The following options are available: • Do not use CAS: select this option if you do not want to use CAS. • Use CAS: select this option if you want to use CAS. Choosing this option results in the **Service account properties** being displayed.
Server name	Specify the CAS server name (required if you use CAS).
Service account properties (Only visible if CAS is used)	The following options can be set: • Specified by user's default Outlook profile: allows you to use the default Outlook profile settings of the user. • Custom settings: allows you to specify an Exchange server, mail address, and mailbox ID to be used.
Test	Clicking the **Test** button tests the connector with the current settings.

36.2.4 - Web Services

Field Name	Description
Use the following service URL	Enter a valid full URL.
Autodiscover Service URL with usage of the email address below	Enter an email address to be used during the Autodiscovery process.
Redirection during discovery to these servers is allowed	Enter the URLs to which redirection is allowed.
Use EWS Impersonation	If checked, you can specify an account to be used for sending emails when using this connector. This option is highly recommended when using **Bypass Session Logon (no authentication)** along with Cost Recovery or ID Services. The EWS Impersonation allows users to simply swipe their card when on the Session Logon screen, and the credentials entered under this option are used. Note that this function is only supported when using EWS protocol.
Testing the connection	Clicking the **Test** button tests the connector with the current settings.

36.2.5 - Sending options

This dialog tab provides control for the administrator over the default content of the mail – recipients, subject and note – and allows setting the express mode client workflow.

Field Name	Description
Display options	Manages the client side workflow.
Default recipients	Allows you to specify default email recipients for a connector. Use the **Add** button to populate the list. Click the **Remove** button to delete the selected entry. You can use the dropdown list to configure the data publishing behavior, selecting from the following options: • None: Default recipients • Data publishing • Default recipients and Data publishing For a practical example of configuring the Data Publishing with a connector, click here.
Send copy to sender	Using this option, the recipient list can be extended with the logged on user dynamically.
Default message	Allows you to specify the default Subject and default note for the connector, by editing the relevant fields: • Default Subject • Default Note: use the **Manage Content** button to specify a default note. You can also define notes and subjects to be received from data publishing by using $$NOTE$$ and $$SUBJECT$$ in the **Note** and **Subject** fields.

36.3- Exchange connector profile settings

The **Edit Profile** window enables administrators who are more familiar with Exchange server environments to fine-tune the settings without relying on the Wizard. eCopy recommends that you use the Wizard to initially configure a connector profile. You can set the following:

- Protocol to be used
- Protocol properties
- Generic settings
- Sending options

36.4- Exchange Connector properties

The Properties window enables administrators who are more familiar with Exchange server environments to fine-tune the settings without relying on the Wizard. eCopy recommends that you use the Wizard to initially configure a connector profile. The **Properties** settings that are available depend on the connection protocols supported by your environment.

36.4.1 - Local address book

The **Local address book** tab enables you to configure the local address books that store Internet email addresses entered at the device, addresses that are not in the Global address list or in the Contacts folder. For information about creating and configuring address books, see Configuring support for Local address books.

When you select the **Enable user to manually enter addresses when sending email** option on the **General settings** tab and you enable the **Internet address book** option on the **Local address book** tab, the system displays a **Save recipient** form, where you can save the email address. Saving the email address is not required; you can send the message without that.

36.4.2 - Exchange Profile Wizard settings

The Profile wizard helps the administrator to setup a basic protocol composite containing one or two protocols. The additional settings are set up with their defaults; any further tuning of the setting can be done by editing Properties.

Configuring via the Wizard follows the steps below:

1. **Select protocol composite**

Field Name	Description
Protocol	Select the protocol combination to be used.
User name	Enter the user name.
Password	Enter the password.
Domain	Enter the selected domain name.
Authentication	Select the type of authentication to be used.
Search user names	Turn the **Search while typing** function on or off.

2. **Configure selected composite**

The components of this page differ according to the selected protocol combination.

Field Name	Description
LDAP settings	The following options can be set via the LDAP settings page: • Locate server at runtime: allows you to select an LDAP server during runtime. • Always use the following server: allows you to set an LDAP server to be used. • LDAP port: set the LDAP port here. The default port number is 389. • Server requires SSL: check this to enable SSL connection.
MAPI settings	The following options can be set via the MAPI settings pane: • Specified by user's default Outlook profile: allows you to use the default Outlook profile settings of the user. • Custom settings: allows you to specify an Exchange server, mail address, and mailbox ID to be used.
Exchange Web Services settings	The following option can be set via the Exchange Web Services settings: • Use the following service URL: allows you to enter a predefined service URL
WebDAV settings	The following options can be set via the WebDAV settings page: • Exchange server: The name or IP address of the Exchange server. • Server requires SSL for communication: communication with Exchange occurs via secure connection. • Use UPN Format for User Credentials (user@example.com): Uses UPN format for credentials instead of domain/username format. • Server uses forms-based authentication: Check this box when the Exchange server is configured to use Forms Based Authentication.

3. Review Summary.

37 - The eCopy Connector for Microsoft SharePoint

The eCopy Connector for Microsoft® SharePoint® enables users to scan documents directly into a SharePoint document management system using different, configurable workflows. When you install the SharePoint Connector and create and activate a connector profile on an eCopy-enabled device, a SharePoint button is added to the eCopy ShareScan Home screen.

The connector supports the selection of document destinations and the storage of documents in SharePoint sites, libraries, folders, and lists. Users can also store SharePoint column (metadata) information with their documents, as well as use the My Site feature of SharePoint.

The SharePoint connector provides support for batching Data Publishing values. For more information, click here.

Users can store documents in any eCopy-supported format (PDF, PDF/A, TIF Fax, TIF, JPG, DOC, DOCX, XPS, XLS and XLSX).

37.1- Configuring the connector

For the generic connector configuration options, click here.

37.1.1 - Defining a scanning destination

For a generic description of defining a scanning destination, click here.

If Content types are enabled for a location in which you want to store a document, users can select a content type for the document from the list at the device. The fields on the screen change according to the selected content type.

You can only add documents to the top level of a Discussion board. You cannot add documents in response to existing items.

37.1.2 - Destination settings: Authentication tab

Field Name	Description
Name	The alias you specify for the destination. This is the destination name seen by the user at the device.
Hyperlink	The URL of the SharePoint location in which you want to store documents. The address must not include any characters after the location. If you cut and paste an address from your browser into this field, you must remove any characters that appear after the location. For example: `http://sp2003/sites/pm/DocLibrary/`**`Forms/AllItems.aspx`** You must remove the characters shown in bold.

Field Name	Description
Enable Navigation	Select this setting if you want the user to be able to navigate the available storage locations of the selected destination, such as sub-sites or document libraries. If you choose a site as the destination of your documents, you must enable navigation so that the users can store documents in libraries, lists, and folders within the site. If users are allowed to navigate from the selected URL and down, they may not navigate above where the URL points. If the URL points to a location that can be stored to and does not have any items below it then this setting is ignored and the navigation form is skipped. The storage location can also come from Data Publishing, if configured. For more information about Data Publishing, see here.
Type	• Logon As: All documents scanned and stored to this destination use the credentials that you enter in the **User name** and **Password** fields. The user is not required to log on at the device. • Runtime: During each session at the device, prompts the user to provide logon credentials before storing the file. For Runtime authentication, the user name and password are used to retrieve the list of users from the SharePoint server.
Search while typing	Enables or disables the Search while typing functionality for the user name field at the device.
User name and Password	The user name and password required to use the connector. Since this connector uses Windows Authentication, you must specify the domain\user information to use for authentication. The connector also uses the user name and password to retrieve the user list from the SharePoint server. The **Search while typing** function uses the user list at the device If you change credential information on the SharePoint server, you must also change it for this connector profile.
Test	Verifies the authentication information. If the test is successful, you can enter information on the **Navigation** and **Columns** tabs.

37.1.3 - Destination settings: Navigation tab

You can configure the connector to filter the types of SharePoint locations that the user sees on the Navigation screen at the device. You can also define the way in which the locations are grouped and whether the user at the device can change any of the filter settings.

Field Name	Description
Default filter type	There are two types of filter: • Standard: All supported location types are shown at the device. • Custom: Only the location types selected in the custom filter section are shown at the device.
User modify	Enables the user to switch between the custom and standard filters at the device. If you select this setting, you must define a custom filter for the user to select.
Define custom filter	Enables the settings in the Custom filter section.
Custom filter	Custom filter settings: You can limit the SharePoint locations available to the user at the device to any combination of Sites, Document and Picture libraries, folders, and lists.
Grouping type	Defines how the locations are presented: • Alphabetical: Locations appear in alphabetical order. • By type: Locations are grouped by SharePoint location type.
Support My Site	This option can only be set if the login type is set to **Runtime**, as the 'My Site' location is tied to the user. The **My Site URL** is filled when the destination URL entered on the **Authentication** tab has been tested. If the test is succesful, the **My Site URL** is automatically filled with the port number according to the destination URL specified on the **Authentication** tab. If no value is specified in the **My Site URL**, the default relative location of the My Site locations on SharePoint 2007 (**personal**) are displayed. The destination can be changed to support those configurations where My Site is on a different server than the team site. In most cases, the automatically filled **My Site URL** requires no change, you only have to modify it when using SharePoint 2010 (as the default value of the relative location of My Site locations is different (**my/personal**) than in SharePoint 2007).

Field Name	Description
Auto-select location	Clicking on the key icon or on the text you can specify whether the location where the document is to be stored comes via data publishing or not. The name of the data published key follows this format: **SP_ <destination name>_AutoSelectLocation** The value of this published key can be a relative or an absolute URL. Absolute URLs must start with the URL specified as **Hyperlink** on the **Authentication** tab. A published value starting with **mysite:** has to be an URL relative to the configured **My Site** URL.

37.1.4 - Destination settings: Columns tab

This tab enables you to configure the SharePoint columns that are available to the user at the device. For Date/Time settings, use the **Settings** button on the ribbon bar of the Administration Console to set the format, which is picked up by the connector. If a user enters only the date, not the time, the system automatically formats the time to 0 hour, 0 minutes using the regional settings at the next change of input focus.

Field Name	Description
Show	Columns contain the document indexing information (metadata) that the connector sends to SharePoint to be stored with the document. You can control the information that the user enters at the device: • **None**: No metadata is required from the user. If you select this option, you must make certain that the destination does not include any required fields. • **All** (Default): All supported columns (metadata fields) are visible to the user. • **Required**: Only required fields are visible to the user. • **Autoindex**: This setting populates the column configuration grid with all columns associated with the current location defined in the hyperlink field on the **Authentication** tab. The user receives an error if the hyperlink and credentials have not been tested. The user can configure one or more columns to be available via document publishing or assign a custom default value. These can be configured by document content types. If the **Hyperlink** points to a site then columns can be configured by content types at every list/library under this site. Columns belonging to a list/library under configured My Site location cannot be configured. At runtime if the selected location points to a location under My Site, the connector tries to apply the column configurations which either belongs to the location itself specified in **Hyperlink** on **Authentication** tab if **Hyperlink** is a list, a library or a folder, or belongs to the list/library under the site specified in **Hyperlink** on **Authentication** tab which has the same relative path as the location under **My Site** selected at runtime. For example: The **Hyperlink** on **Authentication** tab is **http://server/site** Under this site is a **Marketing** site which has a **Plans** document library with **Document** content type and **Matter** column which is configured as **published** column. The relative URL (to **Hyperlink**) of this location is: Marketing/Plans. The absolute URL of this location is: http://server/site/Marketing/Plans. The My Site URL on Navigation tab: http://server/my/personal The published value of Matter column is only applied on a location under My Site selected at runtime if: • the relative url of the selected My Site location is 'Marketing/Plans' (the absolute url of this is in this form: http://server/my/personal/user/Marketing/Plans, and • this My Site location has a Document content type with Matter column.

Field Name	Description
Retrieve Content Type from Data Publishing	Clicking on the key icon or on the text you can specify whether the content type comes via data publishing or not. The name of the data published key follows this format: **SP_ <destination name>_ContentType**

Field Name	Description
Auto index	Here you can configure custom values of SharePoint columns by document content types: • **Content Type** Here, you can select which document content type columns will be shown in the grid to configure their custom values. If the **Hyperlink** points to a storable location (list, library, folder) you can select document content types of this location. If the **Hyperlink** points to a site then you can select a content type belonging to any list/library under the configured site. So it is possible to configure column settings for content types belonging to different lists/libraries under the site. In this case selecting a content type the relative path of the list/library which content type was selected is also displayed next to the **Content Type** label. • **Configuration grid** This displays all columns belonging to the selected document content type. Here you can specify the custom values of the columns by clicking on the **Default value** column of the SharePoint column in the grid and typing or choosing the value depending on the type of this SharePoint column. Clicking on the key icon in the first column of the SharePoint column row you can specify whether the custom value of this SharePoint column comes via data publishing or not. • **Update** If columns are configured to a SharePoint location and the hyperlink is changed on the **Authentication** tab then a warning message is displayed with an error message along the lines of **auto-index mapping is out-of date**. A similar warning message is displayed if the connector profile is migrated from a previous version of SharePoint connector. These warning messages indicate that the configured column values can be invalid for this new location because the new storable location can have different document content types and so different columns. This button updates content types and columns belonging to a list/library of the new storable location trying to preserve the configured column values. Every content type of every list/library and its configured column is investigated and if a column exists at the same content type of the same list/library regarding its relative path under the new location then set its value and data publishing state to the previously configured one. Otherwise the column configuration cannot be preserve. • **Reset** This reset the custom values of all SharePoint columns of any content types of the list/library which the selected content type belongs to setting their default values on the SharePoint server and turned off data publishing of the column regardless if the column is belonging to the selected content type or not.

37.2- Column information

When you configure your SharePoint columns in the ShareScan Administration Console, the user sees the settings on the Column information screen at the device. This screen enables users to enter metadata related to the documents they are scanning.

If your implementation of SharePoint includes the use of content types, this will be the first field on the screen. The other fields on the screen will change depending on the content type you select. When the screen first appears, only fields that are configured for the default content type are available. All available content types for the selected location are available from the Content type list.

The names of required fields are shown in yellow.

37.2.1 - SharePoint configuration considerations

Hidden columns: If a column in SharePoint is configured to be hidden for the location into which you want to store the scanned document, the field for that column will not appear on the Column Information screen.

Validation: All column information that the user enters into the connector at the device is entered as strings. When the user clicks the **Next** button, the connector may validate information in some fields, depending on the settings for the column in the SharePoint library. Validation includes the checking of numeric range and date formats.

37.2.2 - Supported SharePoint column types

If a SharePoint column has been configured to hold a type of information that the connector does not support, and if that field is set as required in the connector, the user will see a warning message. When the user clicks **OK** in the warning message dialog box, the connector returns the user to the Storage options window. The user can then select a destination where the unsupported column type is not required.

The connector supports the following column types:

SharePoint Column type	Description
Lookup (single select)	The user can select a single value from a list of values associated with the Lookup column in SharePoint. The eCopy SharePoint Web Services must be installed on the SharePoint server.
Single line of text	The user can enter a line of text. This can include punctuation but not line breaks.
Multiple lines of text	The user can enter multiple lines of text, but the connector determines how many lines are displayed in the column field, regardless of the Number of Lines to Display setting for the field on the SharePoint server.
Choice	The user can select from a list of values. The user can enter a value that is not on the list if the SharePoint server is configured to use the Allow Fill-in choices option.

SharePoint Column type	Description
Number	The user can enter only numeric characters. A percentage sign is added to the right of the field if the SharePoint server is configured to show a percentage.
Yes/No	The user can select either Yes or No as a value for the field.
Currency	The user can enter a currency amount. The connector does not validate the information.
Date and Time	The connector validates the values entered by the user against the values configured in the Administration Console Columns tab.
Hyperlink or Picture	The user must enter the Hyperlink type and the Hyperlink description type. The Hyperlink type defaults to http:// if no the SharePoint server does not provide a default value.
Managed metadata	You can enter multiple values separated by ;. The search while typing feature is used, and the search is performed on the label of the terms and on the label of the synonyms of the terms. You cannot enter a value not existing in the term set of the column except when the column is the Enterprise Keywords column. In this case the value you entered is automatically created storing the document on the SharePoint server
Person or Group	Allows the user to choose a group or person associated with the site the user is storing a document to. Only a single selection is allowed. The server configuration of a 'Person or Group' column allows various options such as showing only people or people and groups. This release of the connector does not support this option.

37.2.3 - Editing value of a date/time column

The value of date/time column is displayed in the same format specified in SharePoint. The column is set to editing mode by clicking on its value cell. In the value cell you can navigate with the horizontal arrow keys between parts of the date/time value (year, month, day, hour, minute, second) and value of a part is modified similarly using the vertical arrow keys. A value part can be also specified by typing itself but in the following way:

- to define a one-digit value click the digit once (for example, type 2 to set the value to 2)
- to define a two-digit value click the first digit twice and then the second digit (for example, type twice 1 and once 2 to set the value to 12 or three times 2 (twice 2 and once 2) to set the value to 22)

To define the value of the year part by typing you can define only the last two digits of the year in the same way mentioned above and the century is automatically filled.

The date part of the value can also be specified selecting a date from the calendar. This calendar can be opened by clicking on the down array at the right side of the cell where year, month and day can be selected.

38 - The eCopy Connector for Open Text Content Server

The eCopy Connector for Open Text Content Server enables users to scan documents directly into an Open Text document management system using different, configurable workflows. When you install, create and activate a connector profile on an eCopy-enabled device, a button is added to the eCopy ShareScan Home screen.

Users can store documents in any eCopy-supported format (PDF, PDF/A, TIF Fax, TIF, JPG, DOC, DOCX, XPS, XLS and XLSX).

38.1- Configuring the connector

For the generic connector configuration options, click here.

38.1.1 - Database & authentication settings

Field Name	Description
Name	The Livelink destination name; must be unique.
Livelink server	The Open Text Content Server-Enterprise Server name. The server must either be on the same local area network (LAN) as the Services Manager or must be connected to the Manager by a Virtual Public Network (VPN).
Database	The Livelink database name
Port	The port used by the server. The default is 2099.
Use default authentication	Use this if clients log in with the same username/password combination. The authentication form is not displayed on the client side.
Logon at runtime	Use this option if you want the clients to authenticate themselves during runtime.
Search while typing	Enabled only for **Logon at runtime**. The **User name** textbox of the Authentication form on the client side displays available Livelink usernames.
User name and Password	When you create libraries in Open Text Content Server, you set up credentials for users who have access to the information stored in each library. The user name and password that you enter here must provide access to the library referenced by this destination. The user name and password are also used to access the list of names used for the **Search while typing** function at the device. If you change this information on the Open Text Content Server, you must also change it for this connector profile.
Test	Test that the authentication information connects to the specified database.

38.1.2 - Navigation & Attributes settings

Field Name	Description
Store in specified folder / Allow user to navigate	Use these buttons to enable or disable the navigation form on the client side.
Default folder	Sets the default folder for document storage.
Document attributes of default folder	Document attributes associated with the default folder. Required ones are marked with an exclamation point.
Attribute options	• Show all attributes: Displays all attributes available in the Open Text Content Server database. • Show required attributes only: Limits the attributes displayed at the device to those designated as Required in the Open Text Content Server database. • Hide all and use preset attributes of the default folder.
Document naming	Set the document name.

If you use the Express Wizard to configure the connector profile, the user will press the connector button at the device and the document will be scanned to the destination you specify in the wizard without any further input from the user.

To use the Express Wizard:

1. In the Administration Console, select the **Connectors** tab.
2. Select the **Open Text Content Server** Connector.
3. To create a new Express profile, click **Save current profile as**, enter a name for the profile, and then click **Save**.
4. In the **Settings** pane, configure the **Display** settings and make sure that none of the other available settings is set to **User modify**.
5. In the **Configure connector** pane, click **Express Wizard**.

   The Express Wizard window opens.
6. Click **Next** and then enter the **Name** of the destination, the database and authentication settings, and then test the connection.
7. When the test is successful, click Next.
8. Configure the storage folder and attributes settings.

   You must specify default values for required attributes.
9. Click **Finish** to return to the **Configure** tab.
10. Click **Save current profile** to save the profile.

38.1.3 - Express settings

Express settings only work if the following criteria are met:

- Default login is allowed
- Folder navigation is disallowed (documents are saved into the default folder)
- All required attributes are set
- Document attributes form is set to be skipped
- Users are not allowed to change the document names.
- Default login is allowed
- Folder navigation is disallowed (documents are saved into the default folder)
- All required attributes are set
- Document attributes form is set to be skipped
- Users are not allowed to change the document names.

Field Name	Description
Enable Express mode	Clicking this button sets the connector parameters to meet the criteria above, if the user confirms the changes.

39 - eCopy Quick Connect

Quick Connect enables users to scan documents and deliver them to predetermined network locations, Web locations, databases, or to an SMTP server, with minimal data entry requirements. It is ideally suited to environments where large numbers of documents must be scanned quickly into automated or manual workflows.

39.1- Configuring the connector

For the generic connector configuration options, click here.

39.1.1 - Destination settings

Field/Button	Description
New	Adds a new destination.

Field/Button	Description
Edit	Edits an existing destination
Copy	Copies the selected destination.
Remove	Removes the selected destination.
Move up	Moves the selected destination up in the list.
Move down	Moves the selected destination down in the list.
Expression	Displays the Expression dialog.

39.1.1.1 - Generic Destination Settings

Field/Button	Description
Name	The name of the destination.
Type	The type of the destination. The following destination types are available: • Windows folder • Novell Netware folder • FTP folder • WebDAV folder • SMTP Message • Database • Destination List

39.1.1.2 - Folder Location Settings

Field/Button	Description
Folder location	Destination information for the scanned documents. • For Windows or Novell folders, click the **...** button and browse for an existing folder or create a new folder and select it. • For an FTP folder, enter the FTP location, such as “ftp://ftp01/scans”. • For a WebDAV folder, specify the root URL to a WebDAV folder, starting with either http:// or https://. Note that Quick Connect does not support long UNC paths, thus full path names are limited to 260 characters,
Secure connection (FTPS explicit)	Check this box to enable a secure connection. Only available for FTP folders.

Field/Button	Description
Enable subfolder navigation	Enables users to select a subfolder at the device.
Root path	Only valid for Windows folders. Clicking the key icon before this textbox allows ShareScan to retrieve the root path data from Data Publishing. When the icon is highlighted, the name of the data published key defining root path must to be specified in the textbox (for example, a barcode name). The root path (a UNC path) is retrieved from this data published key during runtime. If the key icon is not highlighted, the root path has to be specified in the textboxmanually. If the Data Publishing is used, subfolder routing and subfolder navigation works normally.
Maximum folder level	The number of folder levels down that users may navigate. The default is 3.
Subfolder creation	This button displays a dialog which configures subfolder names where documents are stored. The text box under **Folder Location** specifies the root folder of the destination. A user can navigate subfolders underneath this root folder. If subfolder navigation is enabled at the device, Quick Connect creates subfolder underneath the user-specified folder and stores documents in the created folder. If subfolder navigation is disabled, Quick Connect creates a subfolder underneath the root folder and stores documents in the created folder. The location where documents are stored is: `<Root folder>\<user navigated subfolders>\<subfolder to be created>\<document.pdf>` • The subfolder routing dialog consists of tree view and list view control. The tree view defines the hierarchy of subfolders while the list view defines folder naming rule for the selected subfolder. The text of tree node displays the names of field. • Field names must be unique across subfolders. • If a field is user modifiable, Quick Connect displays the Subfolders form at the device, between Folder Navigation and File Name form. • Alphanumeric, Numeric, List and Database fields publish a DP key, so administrators can map document services DP keys to these fields to retrieve runtime value.

39.1.1.3 - Authentication Settings

Field/Button	Description
Authenticate user	The options are: • None: Sends scanned documents to the destination without requiring user authentication. The Manager requires write access to the destination. • Logon As: All documents scanned and stored to this destination use the credentials that you enter in the **User name** and **Password** fields. The user is not required to log on at the device. Specify the domain/tree, user ID, and password to use for authentication. The specified account requires write access to the destination. • Runtime: During each session at the device, prompts the user to provide logon credentials before storing the file. You specify the domain or tree (for Novell Netware folders) to use for authentication.
User ID	All Authentication types require a user name and password if **Logon As** is selected as the user authentication method.
Password	Specifies the password for the **Logon as** user.
Domain	Select either **Logon as** or **RunTime** authentication mode to enable this combobox. • In **Logon as** mode, the combobox must specify the domain name for the Logon-as-user. • In **RunTime** mode, the combo box specifies the default domain name which is initially displayed on the Logon form but this is optional.
Tree	Only available for Novell Netware folders. Has the same function as the **Domain** combobox described directly above.

39.1.1.4 - SMTP Message Destination Settings

Field/Button	Description
Server	Specifies the SMTP server via name or IP address.
Port	Specifies the port number used. The default is 25.
Account	Sets the account to be used for authentication. The following options are available: • Generic account - None Authentication • Personal account - Windows Authentication • Personal account - Netware Authentication • Personal account - LDAP Authentication
Reply To:	Specifies the sender's email address. Available only for Generic account None Authentication.
Domain	Specifies the domain name used as initial value on the Logon form. Available only for Personal account - Windows Authentication.
Tree	Specifies the tree name used as initial value on the Logon form. Available only for Personal account - Netware Authentication.

Field/Button	Description
LDAP settings	Displays the LDAP server settings dialog. Available only for Personal account - LDAP Authentication.
Cc sender:	Checking this box sends a copy of each message to the sender.
To listbox	Use the **Add** button to add the SMTP addresses of the recipients.
Subject	Set the subject of the message.

39.1.1.5 - Database Destination Settings

For more information on database types and settings, see Database types and settings.

Field/Button	Description
DB type	The configured database types are displayed here. The available types are as follows: • Microsoft Access • Microsoft SQL • Oracle
Data source	Displays the data source.
Catalog	Displays the catalog name, if supported.
Table	Displays the table name with schema, if applicable.
Document data (BLOB)	Displays the column name for the document's data (BLOB).
Document name	Displays the column name for the document name.
Document extension	Displays the column name for the document extension.
Configure	Displays a situation-based dialog. If the administrator is defining a new Database destination, clicking this button displays the Configure Data Source dialog to define database connection. If a defined database connection exists, the **Select recent data source** dialog with previously used connections is displayed, thus the administrator can reuse existing connection setting or go to **Configure data source** dialog via the **New…** button. If an existing connection setting is selected or new connection setting has defined, the connector displays the **Map document destination** dialog to define data mapping.

39.1.1.6 - Destination List Settings

Field/Button	Description
Name Location, and Logon	Enables you to create a list of destinations to which the connector profile can send scanned documents. Clicking the **Add** button displays the **Add destination to ...** window, where you can set the attributes of the chosen destination. When you add a destination to the list, you specify the destination name, type, and location, as well as the authentication information. The **New destination** window then lists all the destinations.

Note:

To make sure that users have to log on, at most once, at the device, you cannot mix certain combinations of destination type and authentication in a destination list.

Example:

If you add a Windows Folder or Novell Netware Folder destination that uses **Runtime** authentication, and you then add an FTP Folder destination, the Authenticate User combo box without Runtime authentication mode is shown.

Invalid options will not be available in the Authenticate User list.

39.1.2 - LDAP server settings

Field/Button	Description
Server	The IP address, DNS name, or URL of the LDAP server associated with the directory you want to use.
Port	The LDAP server port number. The default is 389.
User ID	The ID of the administrator who logs on to the LDAP server. This administrator account is used to query e-mail address for runtime-log-on user from the LDAP server.
Password	The password associated with the server account.
Connect anonymously	Allows anonymous connection to the LDAP server, if the server supports anonymous authentication.
Base DN	The DN of the base or root of the directory in which to search. This varies depending on the server you are using and the portion of the directory you wish to search.
Test	Pressing this button checks the connection to the specified LDAP server. If the test succeeds, the **OK** button is enabled.

39.1.3 - Setting a database as a destination

Setting a database as a destination enables you to configure a connector profile so that users at the device can scan and index documents and store them in the specified database. You can configure the profile to store the index information in a file, in the same database as the scanned document, or in a different database.

To set a database as a destination:

1. On the **Configure** tab, click **New**.

   The **New destination** window opens.
2. In the **Name** field, enter a name for the destination.
3. In the **Type** list, select **Database**.
4. Under Destination, click **Configure** .

   The **Configure data source** window opens.
5. Configure a new data source.
   1. Select the database type and specify the settings.
   2. Click **Test connection**.
   3. When the system displays the "Test succeeded" message, click **OK** twice.

   Or

   Configure an existing data source
   - If the **Select recent data source** window opens, select the data source that you want to use.
   - Click **OK**.

   The data source is the database where the scanned documents will be stored.
6. Depending from the purpose, the following windows are displayed:
   1. Map document destination for database destinations.
   2. Choose fields dialog for database fields
   3. Map index fields dialog for index files.
   4. Click **OK**. The **New destination** window displays the database settings.
   5. Click **OK** to save the settings. The **Destinations** list displays the name and summary information for the database destination you created.

Note:

The **Index file** tab displays the mapped database column name in the **Table Column** in the Index File list view.

39.1.4 - Database types and settings

Database type	Settings
Microsoft Access	Specifies the path to the Access database (*.MDB), which can be on a local drive or on a Universal Naming Convention (UNC) path. If the database is on a local drive and does not require a user name and password, select the Blank Username and Password check box. If the database is on a UNC path, enter the appropriate credentials. The user must have permission to access the specified path.
Microsoft SQL	Specifies the SQL server, user name, and password used to access the SQL Server, and the Catalog/Database. • SQL Server: The SQL server that you want to use. If the Microsoft SQL Server Management Object component is installed on the computer, the system automatically fills the SQL Server list with the names of SQL servers on the local segment of the network and you can select the server from the list. If MDAO is not installed, you can type the server name in the field. • Username: SQL server user name. • Password: Password for the specified user. • Catalog/Database: The database where you want to start browsing tables. You can select the catalog or database from the list, if MDAO is installed, or you can type the catalog or database name in the field.
Oracle	Specifies the listener, user name, and password used to access the Oracle database. • TNS Name: Listener on the Oracle database server. • Username: Oracle user name for the integrated security user on the target database. • Password: Oracle password for the specified user.

39.1.5 - Map a document destination

When you set a database as a destination, you can use the **Map document destination** feature to map the name and file extension of the scanned document to STRING fields in a table in the database. This enables you, or a database administrator, to create associations between the scanned document and any index information that the user enters on the Index screen for the document, wherever that index information is stored.

Database type	Settings
Connection information	Displays current database connection information: • Data source: name of the data source. • Catalog: displays catalog name, or **N/A**, if none is available. • Table: table name with schema (if available). • Column: not used for document mapping. • Default value: not used for document mapping. Use the **Modify** button to edit the displayed information, and the **Refresh** button to clear table selection and field mapping.
Select Table Name	Displays available tables in the current data source. If a table is selected from the list, it gets bold and the **Map Fields** data grid view gets enabled.
Map Fields	Displays which fields are mapped to which database columns. The administrator selects a column name from dropdown list. The column for Document Data (BLOB) must be specified but Document Name and Document Extension is optional. If an already assigned column is reselected, the dialog shows an error message and clears column selection.

39.1.6 - Using a database as the source of field values

You can create a file name field or an index field that uses a database as the source of field values. Users at the device can then select from a list of available values for that field..

If the database administrator modifies, in a database, values that are associated with a Quick Connect field, users will have access to the changed values. You do not need to make any changes to the field in the Administration Console.

To use a database as the source of field values:

1. On the **File name** or the **Index file** tab, click **New**.

   The appropriate **Field editor** window opens (**File name field editor** or **Index file field editor**).
2. In the **Name** field, enter a name for the new field.
3. In the **Type** field, select **Database** as the type.
4. Check **User modify** if you want the user at the device to be able to alter this part of the file name.
5. Select the **Required** option if you want to require users at the device to specify a file name or index value.
6. Click **Configure**.

   If you have previously configured a data source, the **Select recent data source** window opens.

1. On the **File name** or the **Index file** tab, click **New**.

   The appropriate **Field editor** window opens (**File name field editor** or **Index file field editor**).
2. In the **Name** field, enter a name for the new field.
3. In the **Type** field, select **Database** as the type.
4. Check **User modify** if you want the user at the device to be able to alter this part of the file name.
5. Select the **Required** option if you want to require users at the device to specify a file name or index value.
6. Click **Configure**.

   If you have previously configured a data source, the **Select recent data source** window opens.

   - To use an existing data source, select it and then click **OK**.
   - If you do not want to use an existing data source, click **New**.

     The **Configure data source** window opens. Follow the instructions to configure a new data source.
   - If you have not previously configured a data source, the **Configure data source** window opens. Follow the instructions for configuring a new data source.

- After selecting or configuring a data source, the **Choose field** window opens.

6. Select a table, select a column in the table, and then select the default file name or index value from the list of available values. The user at the device can accept the default value for the field or select a value from the list.
7. Click **OK** to return to the **Field editor** window.

   The window displays the settings you have configured.
8. Click **OK** to save the settings and return to the **File name** or **Index file** tab.

   The tab displays the name and summary information for the Database field you created.

39.1.7 - Defining Expressions for destinations

You can define parameters, operators, and constant values via the Expression dialog. The parameters are published to the Data Mapping tool and mapped to published data from a document service. Document service publishes data as string and the connector converts the string to specific data type according to parameter type.

Field/Button	Description
New	Allows adding a new parameter via a dialog, where you can set the name and type of the new parameter. The available data types are the following: • String • Integer • Decimal
Edit	Edits the selected parameter.
Remove	Removes the selected parameter from the list view.
Operator	Select a parameter to display the available operators defining how to compare parameter and constant values. The set of operators varies according to parameter type.
Constant	Select a parameter to display the constant value which is compared to parameter value during runtime. The input text must be formatted properly to successfully process the equation.

39.1.8 - Defining file naming fields

The file name generated at the eCopy-enabled device is composed of one or more fields. Note that if file name is not published by document service, Quick Connect uses its file naming rule even if you check **Use Document Service** file name.

To define file naming fields:

1. Select the **File Name** tab.
2. Click **New**.
3. Use the **File name field editor** to specify a name for the field and set the default values.
4. Click **OK**.
5. Repeat this procedure for each new file naming field.

   Or

   Select **Use Document Service file name** to use the file name configured for the Document Service.
6. Click the **Save current profile** button.

   The system saves your settings as part of the connector profile.

Note:

If a scanned document already exists in a selected destination you are presented with a number of options.

39.1.9 - File name tab

Field/Button	Description
New	Adds a new entry via the File name field editor.
Edit	Edits an existing entry via the File name field editor.
Remove	Removes the selected entry from the list view.
Move up	Moves the selected entry up in the list view.
Move down	Moves the selected entry down in the list view.
Use Document service's file name	Checks published entry name by a document service. If the file name is published, the connector uses the published name as an output file name instead of the File naming form and constructing the file name according to file naming rule.
If file name already exists:	Set the method for resolving file name conflicts: • Create unique file name (.1,.2,etc): The connector creates a unique file name by appending a rolling number with a dot separator. • Overwrite always: Overwrite the existing file with the scanned document. • Return error: Show an error message at the device. The User has to specify a different name at the device or cancel the current job.

39.1.9.1 - File Name Field Editor

Field Type	Description
Name	Specifies a unique file name field name. Not case sensitive. If you increase the minimal length, this field becomes required.
Type	Specifies a type of field. Type-dependent settings change according to the field. For more information, see the Field types table below. • Alphanumeric • Numeric • Date • Time • List • Database • Batch-based index value • Batch number • Separator • Device name • Logged on user

Field Type	Description
Export to Index File	Specifies whether the entry name field value is exported to the index file. If checked, a field which has a name of *FileNameField.<field name>* is added to the Index File list view control in the **Index File** tab.

39.1.9.2 - Field Types

Field Type	Description
Alphanumeric	Inserts text into the file name. the text can contain any printable characters except those that are restricted from Windows file naming conventions or any characters that you define as separators. • Minimum/maximum length: The minimum and maximum number of characters allowed. • Remember: The number of previous entries to display when the user is prompted for the naming information. If set to zero, no previous values appear in the drop-down list.
Batch number	Inserts the current batch number into the file name. • Leading zeroes: Pads all values with leading zeroes to make their length equal to the maximum field size. For example, if you specify "3" in the Length field and you enable leading zeroes, batches are numbered “001”, “002”, … , “010”, “011”, … , “100”, “101”, … , “999”. If you do not enable leading zeroes, batches are numbered "1", "2", etc. • Length: The maximum number of digits allowed for the batch number, including leading zeroes.
Batch-based index value	You can only use batch-based index values if you have the eCopy Barcode Recognition Service. Batch-based indexing enables you to create index files with separate barcode values for each batch.
Database	Inserts a value from the database into the file name. Click the **Configure** button and configure a data source.
Date	Inserts the date on which the document was scanned into the file name. Format: The format in which you want the date to appear in the file name.
Device name	The name of the device from which the document is scanned. No additional settings.
Numeric	Inserts numeric characters into the file name. • Default: Only numeric characters can be entered in this field. • Field Size: The minimum and maximum number of digits allowed. • Leading zeroes: Pads all values with leading zeroes to make their length equal to the maximum field size. • Remember: The number of previous entries to display when the user is prompted for the naming information. If set to zero, no previous values appear in the drop-down list.

Field Type	Description
Separator	Character: The character that you want to use to separate the fields in the file name. The character that you select cannot be used in any other file name field.
List	Enables you to create a list of values from which the user can select a single value at the device. If you select the **Required** option, the user at the device must select a value from the list. If you do not select this option, the user at the device can leave the field blank. If you select the **Required** option and do not select the **User modify** option, you must set one of the list items as the default value.
Time	Inserts the time at which the document was scanned into the file name. Format: The format in which you want the time to appear in the file name.

39.1.10 - Defining index files

Setting up an index file enables the user at the device to enter indexing information for the scanned document in one or more fields. Quick Connect writes the field names that you create on the **Index file** tab to an index file, and creates data mapping information between field names and database columns. The default values that you associate with each index field, or the values entered for the field by the user at the device are also stored in the index file or database table.

The information describes the content of the document, such as a case ID, a client name, or a document type. Quick Connect saves the index information with the scanned document. This option is useful with back-end applications that can process the scanned documents (image files) and index files in the destination folder.

To configure an index file:

1. Select the **Index File** tab.
2. Click **New**.
3. Use the Index Field Editor to define an index field and its default values.
4. Click **OK**.
5. Repeat this procedure for each new index field.
6. In the **File format** area, select the format of the index file.
7. If the **Document splitting** option is enabled on the **Settings** pane and you want to create a single index file, select **Create single index file when Splitting is enabled**.
8. If you want to duplicate unchanging index values, select **Repeat unchanging index values**.
9. Click the **Save current profile** button.

   The system saves your settings as part of the connector profile.

39.1.11 - Index file tab

Field/Button	Description
New	Adds a new field via the Index file field editor.
Edit	Edits an existing file via the Index file field editor.
Remove	Removes the selected file from the list view.
Move up	Moves the selected file up in the list view.
Move down	Moves the selected file down in the list view.
Mapping	The Select Recent Data Source or Map Index Fields dialog is displayed directly, if no connection settings are stored to the registry. In the dialog you can assign Index fields to database columns. If at least one index field is configured and the **Database** button is clicked, this button gets enabled.
File format	The following file types are available: • XML • CSV • TSV • Database **Note**: When selecting the **Database** option, the **Mapping** button is enabled on the toolbar.
Convert XML file	Select XML index file format to enable this control. If this control is checked, the controls in XSLT group are enabled.
XSLT group	The following options are available via the XSLT group: • XSLT file: set the location of the XSLT file. • Extension: specifies an extension for the result file of the XSL transformation.
Create single index file when Batching is enabled	If checked, the connector creates a single index file per job. If unchecked, an index file per batch is created.
Repeat unchanging index values	Available only if **Create single index file when Batching is enabled** is checked. If checked, the connector records the system- or job-based index values for every batch. If unchecked, the connector records the system- or job-based index values only once and records batching-based index values for every batch.

39.1.11.1 - Index File Field Editor

Field Type	Description
Name	Specifies a unique file name. Not case sensitive.
Type	Specifies a type of field. Type-dependent settings change according to the field. For more information, see the Field Types table below. • Alphanumeric • Numeric • Date • Time • List • Database • Logged on user • Destination Path • File name • File size (KB) • Number of pages • Batch-based index value

39.1.11.2 - Field Types

Field Type	Description
Alphanumeric	Records the text which contains any printable character into the index file.
Batch-based index value	Pulls published value from DataPublishing based on current batch number and records into the index file.
Database	Records the selected value from the database into the index file.
Date	Records the formatted text of the date into the index file when the job was started
Destination path	Records the location where the document is sent into the index file. The location information differs according to destination type: • Windows Folder – A path to local or network folder • Novell Netware – A path to local or network folder • FTP Folder – An URL • WebDAV Folder – A URL • SMTP Message – Concatenated email addresses of recipients with semicolon • Database – <Data source> - <Catalog>.<Table>
Device name	Records the name of the device on which the client is running into the index file. The device name is retrieved when the connector starts.

Field Type	Description
File name	Records the file name of the document into the index file.
Logged on user	Records the logged on user's name into the index file. If the destination uses Runtime authentication, the connector records runtime-logon-user name (either Session Sign On user, CAC user or connector's log on user). If authentication mode is Logon as, it uses preconfigured user name. Otherwise it records empty string.
Number of pages	Records the number of pages in the document into the index file
Numeric	Records the text which contains only numeric characters into the index file.
File size (kB)	Records the file size of the document in kB into the index file.
List	Records the selected value from the list into the index file.
Time	Records the formatted text of the time into the index file when the job was started.

39.1.12 - Index file formats

The index file has the same name as the scanned document, but has a different file extension. The available formats of the index file are:

- XML
- CSV (comma-separated value)
- TSV (tab-separated value)
- Database

Example:

Click here to view file format examples:

CSV

filename,device,date,time,user-tag1<CRLF>

MyDocument.pdf,MEAP01,03052003,110534AM,value 1

TSV

filename<TAB>device<TAB>date<TAB>time<TAB>user-tag1<CRLF>

MyDocument.pdf<TAB>MEAP01<TAB>03052003<TAB>110534AM<TAB>value 1

XML

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<data>

<index id="filename">MyDocument.pdf</index>

<index id="device">MEAP01</index>

<index id="date">03052003</index>

```
<index id="time">110534AM</index>
<index id="user-tag1">value 1</index>
</data>
```

39.1.13 - Document splitting settings

When the **Document splitting** option is enabled on the **Settings** pane, you can configure Quick Connect to create a single index file that records the index values entered at the device for all scan jobs of a batch.

- The connector uses the file name that you create on the **File name** tab to create a name for the index file. If you do not configure a file name, the connector uses the default file naming rule.

  If the file name includes the **Batch number** field, the connector sets the current batch number in that field; otherwise, the connector adds an underscore (_) to the batching number, as in "document-20070131_1.pdf".

  If a file name already exists and the **Create unique file name** option is configured on the **File name** tab, the connector adds a period to the rolling number, as in "document-20070131_1.1.pdf".

- Index fields are divided into three types. The type of index value determines the frequency of changes to index values:

  - **System:** The index field retains the same index value when the user at the device starts a new scan job.

    Used with the following field type: Device Name.

  - **Scan Job:** The index values in index fields of this type are the same for the entire scan job.

    Used with the following field types: Alphanumeric, Numeric, Date, Time, List, Authenticated user, Destination path, Database.

  - **Splitting job:** A scan job can comprise multiple document splitting jobs. The index values in index fields of this type change for each document splitting job.

    Used with the following field types: File name, Number of pages, File size, and Batch-based index value.

- The **Repeat unchanging index values** option enables you to record the index values for a batch job each time the user enters the index values, even if the user at the device enters the same index values many times.

  - If you do not select this option, the connector records the system- and scan job-dependent index values only once.
  - Since batch job-dependent index values have different values based on the job, they will be recorded multiple times by default. However, if there is only a single batching job, the index values will be treated like system- and scan job-dependent values.

- If you select this option, batch job-dependent index values will be recorded in a different node (for an XML file) or a different row (for CSV and TSV files, and database tables). This does not apply when the connector is processing only one batch scanning job

39.1.14 - Mapping index fields to fields in a database

This feature enables you to specify a database that will store index values entered at an eCopy-enabled device. You can map any type of Quick Connect index field to fields in an SQL, Access, or Oracle database. When a user enters values in mapped index fields, the connector profile stores the values in the associated database fields.

Note:

The connector profile stores all mapped index values in the target database as STRING data, regardless of the type of index field.

If you store scanned documents in a database and you want to create a relationship between the database fields where the documents are stored and the database fields where the index values are stored, make sure that one of the mapped index fields is of the type "File name". Index fields of type "File name" automatically use the file name of the scanned document that is stored in the database destination.

Example:

Click here to see the example:

You configured a connector profile to scan insurance claims using the following file naming format:

```
eCopyClaims<Date><Time>
```

You configured the profile to store the scanned documents, named as shown below, in the target database:

```
eCopyClaims20060523123318.pdf
eCopyClaims20060523123319.pdf
eCopyClaims20060523123320.pdf
```

You created several Quick Connect index fields to capture account information and mapped them to fields in a database.

To associate the database record used to store the scanned documents with the database record used to store the scanned document's index values, you must have an index field of type "File name" that captures the file name during scanning.

To map index fields to fields in a database:

1. Select the **Index file** tab, click **New**, and then define each index field that you want to map.
2. Under **File format**, select **Database** and then click **Map Fields**.

   The **Configure data source** window opens.

3. If you have not yet configured a data source, configure it now.

   To use the current data source, proceed to step 4.

   If you do not want to use the current data source, click **Modify** to select a different data source. When the **Select recent data source** window opens, click **New** and follow the instructions for configuring a new data source.
4. If you previously configured a data source, the **Map index fields** window opens, displaying the connection information.
5. Via **Select table name**, select a table.
6. Under **Map fields**, which displays the index fields that you created, select the Quick Connect index field that you want to map to a database field. You do not have to map all the Quick Connect fields.

   In the **Database field** column, which only displays fields of STRING data type, select the target field. The index values that the user at the device enters in the index fields will be stored in the database fields after the document is scanned.
7. Click **OK** to save the settings and return to the **Index file** tab.

39.1.15 - Configuring batch-based indexing

If you have the eCopy Barcode Recognition Service, you can use batch-based index values. Batch-based indexing enables you to create index files with separate barcode values for each batch by assigning a base name (Publishing Name) to the position of the barcode.

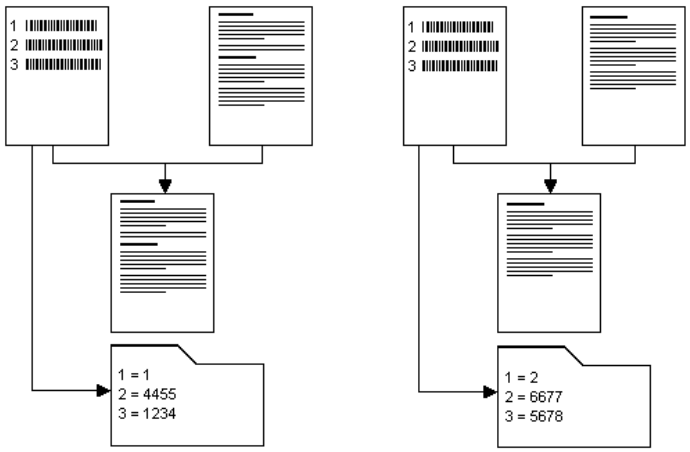
All Publishing Names also have batch information available for Quick Connect to use. Note that only the first value found per Publishing Name is published for the session.

For example, a document is divided into two batches. It begins with a page that contains three barcodes and is split by another page that also contains three barcodes. On both pages the barcodes follow the same sequence but have different values:

Table 4: Batch-based indexing example

Barcode Number	Batch-based index value - Publishing Name	Index value, page 1	Index value, page 2
1	Document Number	1	2
2	Locator	4455	6677
3	Extension	1234	5678

The following diagram shows the four page document and how, after processing, the scanned document is stored with the correct index information.



To configure batch based indexing in Quick Connect:

1. Select the **Index file** or **File name** tab.
2. Click **New**.

   The relevant **Field editor** opens.
3. Enter the Data Publishing name to receive the Published Key from the service. You can specify any name to the Name field. The Name field provides descriptive information for you.
4. Select **Batch-based index value** as the **Type**, and click **OK**.
5. Follow steps 2 through 4 above for each value that you want to use.
6. Save the connector profile with the values.

When you configure a device and select this connector profile, you must then select the corresponding Service profile that you set up in the Barcode Recognition Service.

39.1.16 - Quick Connect and Data Publishing

Quick Connect can read data published to a Data Publishing service by a connector. For example, a company can install a barcode recognition service and then use Quick Connect to access the barcode data that the service publishes.

The ShareScan administrator is responsible for the following tasks:

- Install and configure the Service on the same PC as the eCopy Manager. For more information see the Help topic for the Service in question.
- Work with the developer of the service, which may be available from eCopy or from a third party, to identify the data that the Service publishes and the names of the fields that will contain the published

data. For example, assume that the document to be scanned contains barcodes. The service extracts data from the following barcode fields and publishes the data to a COM object:

Barcode1, which contains a user name.

Barcode2, which contains a date.

Barcode3, which contains a company name.

Barcode4, which contains a city.

- Define Quick Connect index fields that reflect the names of the fields containing the published data. Using the example, the administrator must define index fields named Barcode1, Barcode2, Barcode3, and Barcode4.
- Configure the Quick Connect index file.

When a user scans a document at an eCopy-enabled device, the Manager starts the installed Service. The Service creates the COM object and publishes data from the scanned document to the COM object. The Manager passes the COM object to Quick Connect, which searches the COM object for the configured field names. If Quick Connect finds a match, for example, if it finds a field named "Barcode1", it reads the value in that field and writes the value over the default value in the "Barcode1" index field in the index file. Quick Connect then sends both the scanned image document and the index file to the target destination.

40 - eCopy Connector for Open Text Fax Server, RightFax Edition

The eCopy Connector for Open Text Fax Server, RightFax Edition enables users to scan and fax documents from the eCopy-enabled device through an existing Open Text Fax Server.

When configured appropriately, users can send files from their personal RightFax account and access their personal RightFax phone book for recipient selection. Delegation, cover pages, and billing codes are also supported when configured on the Open Text Fax Server.

40.1- Configuring the connector

For the generic connector configuration options, click here.

40.1.1 - Configuration settings

The following tables describe the settings on the **Configure** tab.

Table 5: RightFax Server configuration settings

Field Name	Description
Server	The name of your RightFax server.
User	The name of the user account used by the connector to log on to RightFax. The user account information is always used to log on to the RightFax server and retrieve the user list. If you plan to use Windows NT authentication, enter the user name for a Windows NT domain account.
Password	The account password.
Test	After you configure the settings in the fields of the RightFax server section, click to test the connection to the RightFax server. If the test fails, resolve the connection issue before proceeding. Verify that your spelling is correct and that the name of the RightFax server is accurate.
Send from personal account	Allows the user to log on to the RightFax server and then sends the fax from that user's personal RightFax account (or from a delegate account). If you do not select this option, the connector always sends the faxes from the user account specified in the User field.
Use delegation	If enabled, and an authenticated user is set up to send as someone else, the Send As button is shown on the UI.
Use Windows NT authentication	Available only for RightFax Server 8.7, 9.0, 9.3, and 9.4. If selected, all users must log on to the RightFax server using their Windows NT credentials. Note: Windows NT and RightFax UID authentication are mutually exclusive.

Table 6: Phone books configuration settings

Field Name	Description
Enable	Allows the user's personal phone book to be available for recipient selection.
Add new recipients	Allows users to add new recipients to their personal phone book using the Save Recipient option on the Send > Details screen at the device.
Limit to phone book recipients	Allows users to send faxes only to recipients already in the phone book.

Table 7: Cover sheet configuration settings

Field Name	Description
Yes/No	Specifies the default setting.
Hide buttons	If you select this option, the connector profile hides the cover sheet buttons from the user and uses your selected default setting (Yes or No) to determine whether to attach a cover sheet. In all cases, if the authenticated user's RightFax account has not been configured to send cover sheets, an error message appears when the user presses the Send button.

Important!

A cover sheet can only be sent with a fax if the **Use cover sheet** option is enabled in the RightFax FaxUtil client for the authenticated user (see your RightFax documentation).

40.1.2 - Billing codes settings

Field Name	Description
Fields 1, 2, and 3	Available billing codes are defined on the RightFax server and displayed in these fields. You can enable the fields for use with scanned documents. Each enabled field appears on the Billing Codes form at the device. (If you do not enable any fields, the Billing Codes form does not appear.) For each field, select the appropriate options.
Enable	Prompts the user to select or enter a billing code. If the field is defined as required on the RightFax server, it is highlighted in yellow on the Billing Codes form and the user must enter a value in the field. You must enable the first field in order to enable the second field, and the second field to enable the third field.
Verify	Validates the information entered by the user at the device against the list of billing codes defined on the RightFax server. You must enable verification for the first field in order to enable verification for the second field. There is no **Verify** option for the third field (the **Description** field).

Field Name	Description
Read billing codes from Cost Recovery	If your company uses the Cost Recovery Service, you can choose to obtain the billing codes directly from the service through eCopy Data Publishing. For a practical example of configuring the Data Publishing with a connector, click here. When the **Read billing codes from Cost Recovery** option is selected, the **Verify** option is disabled for all billing codes. For more information on Cost Recovery, see the relevant sections of the Help.
Billing codes form display options	Enables you to control the display of the Billing Codes form at the device: Hide Billing Codes form: The form does not appear at the device. Show Billing Codes form: The form at the device displays the fields that you enable on the **Billing codes** tab. Users can modify the contents of the fields. Show Billing Codes form read-only: The form at the device displays the fields that you enable on the **Billing codes** tab. Users cannot modify the contents of the fields.

40.1.3 - Content settings

The Cover sheet notes section on the **Content** tab enables you to create notes that the user at the device can add to the fax cover sheet.

When you add a new note to the list of notes available to the user at the device, you can use the following variables:

Variable	Description
`$$USER_NAME$$`	Replaces the variable with the sender name.
`$$RECIPIENTS$$`	Replaces the variable with the recipient name(s).
`$$FILESIZE$$`	Replaces the variable with the size of the file (in KB).
`$$FILENAME$$`	Replaces the variable with the name of the file.
`$$PAGECOUNT$$`	Replaces the variable with the number of pages in the document.

40.1.4 - Fax format

This tab allows you to specify valid characters for the Fax number. If the fax number contains characters other than these, the fax cannot be sent on the Send form or the recipient entry cannot be saved into the phone book on the Details dialog at the client side and an error message appears. If no character is specified as valid (the textbox is empty), then all characters are valid for fax number and there will be no validation on the client side.

Variable	Description
`Valid characters in fax number`	Enter the valid fax number characters here.

40.1.5 - Express Settings

A RightFax Express connector profile allows you to scan and fax the document by simply pressing the button on the main screen.

Field Name	Description
Enable	Enabling the Express function designates the profile you are creating as an Express profile. The information that you configure on this tab will be used for every document that you fax using this profile..
Billing codes 1 and 2 description	Enter the codes that you want to use for documents sent using this connector profile. When this information is pre-configured, the user at the device does not see the Billing codes screen.
Name	The name of the fax recipient.
Fax number	The fax number to which the scanned document is sent.
Note	The text included in the body of the fax to which the scanned document is attached.
Attach cover sheet	Send a cover sheet containing the Name, Fax number, and Note to the recipient with each faxed document. A cover sheet can only be sent with a fax if the **Use cover sheet** option is enabled in the RightFax FaxUtil client for the authenticated user (see your RightFax documentation).

Note:

If you use Express with a RightFax connector profile, you must save the connector profile with the RightFax server information before you test your Express configuration.

If you select the **Send from personal account** option on the **Configure** tab and then configure the connector profile to use Express, the connector will prompt the user at the device to enter authentication information.

40.1.6 - Send screen settings

Field/Option	Description
From	A read-only field populated with the name of the sender.
Search	Specifies the user ID of a recipient to search for in your RightFax phone book. When you move to the next field, the connector will fill in the recipient and fax number information from the RightFax phone book.
Recipient	The name of the recipient of the fax. If the recipient is in the RightFax phone book, this field is populated automatically when the user ID is selected in the **Search** field. If the recipient is not in the RightFax phone book, enter the recipient name and fax number or, click **Details** and use the Details window to enter the user information.
Fax number	The recipient's fax number (required).

Field/Option	Description
Notes	Notes to include in the message body (optional). Useful if you attach a cover sheet. The arrow button next to the text box displays a list of available, preconfigured messages.
Attach cover page	Specifies whether to attach a cover page to the fax. If you select Yes and your RightFax account is not configured to use a cover sheet, the connector ignores your selection. The connector profile can be configured to hide the cover page buttons.
Details	Displays information about the specified recipient. If the user exists in the RightFax phone book, you cannot change any of the information. Phone book entries can only be changed on the RightFax server. To add a new recipient to the RightFax phone book, click **Details** and then enter the recipient's name, user ID and any other user information in the blank fields in the Details window. Under **Save recipient**, select Yes and then press **OK**.
Send as	Allows the user to impersonate another RightFax user via the Delegation feature available in RightFax. The feature is only available if you have rights on the RightFax server to send faxes from another user's account and the feature is enabled for the connector. Press **Send as**. Select the RightFax user ID of the other user and then press **OK**.

41 - The eCopy Scan to Desktop connector

The Scan to Desktop connector enables ShareScan users at an eCopy-enabled device to scan documents and send them to recipients' scan inboxes or to network home directory folders, where the scanned documents can be retrieved by using eCopy PaperWorks, which was called eCopy Desktop in previous versions of ShareScan. For information about using eCopy PaperWorks, refer to the eCopy PaperWorks documentation or Help.

Depending on the configuration of the connector, the recipient may be the user scanning the document or any other eCopy PaperWorks user whose scan inbox is set up to receive scanned documents via the connector. The connector can also be configured to send scanned documents to storage destinations, specifically Windows, or Novell folders.

Notes:

- When a ShareScan user at an eCopy-enabled device chooses a recipient, the scanned document is delivered to the recipient's scan inbox or to the specified folder in the recipient's network home directory.
- You can configure the connector to secure the scan inboxes of recipients. Users must enter the network password associated with a recipient's scan inbox before the connector can send scanned documents to the scan inbox. The **Authenticate users** option is automatically selected when the inbox type is set to "Home Directories". Any user can send a scanned document to any user's scan inbox. However, only the owner can read from the scan inbox

- The list of available recipients that appears on the Specify Recipient screen (in the ShareScan Client) includes all users in the Windows Active Directory or Novell eDirectory, unless you restrict usage by choosing a base DN that limits the scope of the search.

41.1- Configuring the connector

For the generic connector configuration options, click here.

41.2- About scan inboxes and home directories

eCopy PaperWorks can use either scan inboxes or network home directories to store scanned documents received from the Scan to Desktop Connector:

- **Scan inboxes:** The connector creates scan inboxes when users first use the connector at a device. The connector creates scan inboxes in folders located beneath the Inbox root directory.

  When the connector creates scan inboxes, it assigns the permissions needed to ensure the appropriate level of scan inbox privacy. The connector uses the ShareScan Administrator group you designate in the Scan to Desktop Properties window to implement the required security.

- **Home Directories**: The network administrator must create these directories. If you configure the connector to use a network home directory to store scanned documents, the connector automatically uses the **Scan to Self** and **Authenticate Users** options. Network security ensures that only the Local Administrator, the ShareScan Administrator, and the local user can read from or write to the root of the network home directory or to the specified subdirectory. Scan to Desktop must connect to the specified folder as the owner of the home directory.

  Important!
  Network home directories configured through a logon script are not supported.

You configure a Scan to Desktop connector profile to scan to a single inbox type: scan inboxes or network home directories. You cannot configure the connector profile to scan to both types of inboxes. However, if you modify the inbox type in the connector profile, so that some users have scan inboxes while others have network home directories, both types of inboxes can coexist on the same system.

41.2.1 - Security settings for scan inboxes

System	Role	Permissions
Windows Active Directory	Administrators	Full control

System	Role	Permissions
Novell	Domain Administrators	Full control Not used in workgroups
	<*groupname*> (your designated ShareScan Administrator group)	Full control
	<*owner*>	Full control of the owner's individual inbox folder
	Admin	Full control
	<*groupname*> (your designated ShareScan Administrator group)	Full control
	<*owner*>	Full control

41.2.2 - Examples of scan inbox locations

System	User	Domain	Inbox Location
Windows Active Directory	User1	Using the Multiple domain mode option (only if required)	`\\Server\Inbox Root\xyz.com\<domain_ name>\User1`
Novell (NDS)	Cn=testuser, ou=engineering, 0=ecopy	When using the Use eDirectory hierarchy (only if required)	`\\Server\Inbox Root\eCopy\engineering\testuser`

41.3- About the Inbox root directory

The Inbox root directory, which was called "Inbox Management Directory" in previous versions of ShareScan, contains scan inboxes and a file named *userdirs.txt*. When users at a device use the connector for the first time, their names and the paths to their scan inboxes or network home directories are added to the *userdirs.txt* file.

The Inbox Agent uses the *userdirs.txt* file to provide eCopy PaperWorks with the path information that eCopy PaperWorks needs to connect to scan inboxes or network home directories.

Before you can use the Scan to Desktop Connector, you must configure the Inbox root directory.

The connector automatically assigns specific file and folder permissions to ensure inbox security depending on your network environment.

41.3.1 - Inbox root directory permissions (Windows)

Windows (NTFS)		
<inbox root directory>	Administrators	Full control: applied automatically
	<groupname> (your designated ShareScan Administrator group)	Full control: applied automatically
	Everyone	Read (List folder): applied automatically
userdirs.txt	Administrators	Full control: applied automatically
	<groupname> (your designated ShareScan Administrator group)	Full control: applied automatically
	Everyone	Read: applied automatically

41.3.2 - Inbox root directory permissions (Novell Netware [NDS])

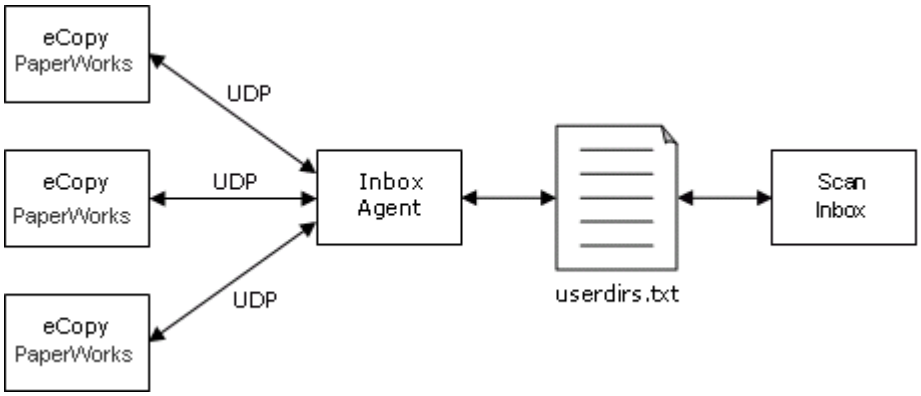
Novell Netware (NDS)		
<inbox root directory>	Administrators	Full control: applied automatically
	Domain Admins (not used in workgroups)	Full control: applied automatically
	<groupname> (your designated ShareScan Administrator group)	Full control: applied automatically
	Everyone	List folder: applied manually
userdirs.txt	Administrators	Full control: applied automatically
	Domain Admins (not used in workgroups)	Full control: applied automatically
	<groupname> (your designated ShareScan Administrator group)	Full control: applied automatically
	Everyone	None: applied manually

Supporting multiple Inbox root directories:

For information on the support of multiple Inbox root directories, refer to the Ask eCopy knowledge base, or contact eCopy Customer Support.

41.4- About the Inbox Agent

The eCopy Inbox Agent is a Windows Service that is installed with the ShareScan Manager. It uses the userdirs.txt file to provide eCopy PaperWorks with the path information that eCopy PaperWorks needs to connect to scan inboxes or network home directories. eCopy PaperWorks uses the UDP (User Datagram Protocol) to communicate with the Inbox Agent.



Important!

The default UDP server port is 9999 and the client port is 8888. The default multicast server and client IP address is 239.254.5.6. If you need to change these settings, contact Customer Support for assistance.

Example:

If you are logged on to your PC as <auser>, eCopy PaperWorks sends a UDP message to the Inbox Agent requesting the path to your scan inbox. The Inbox Agent looks up `<auser>` in the `userdirs.txt` file and returns the path to eCopy PaperWorks , which uses it to open `<auser>`'s scan inbox.

If you do not enable the Inbox Agent, each eCopy PaperWorks user must manually configure the path to the scan inbox. For more information about configuring eCopy PaperWorks, see the eCopy PaperWorks documentation or Help.

41.5- Pre-configuring the connector

Notes:

- If you are migrating from an earlier version of eCopy ShareScan and have already configured an Inbox root directory, you can use the existing location and settings. You can also import profiles from earlier versions of the connector using the **Import / Export** tool in the Administration Console. For more information, see the Administration Console Help.
- If you have a Novell network with multiple trees, you must set the **Preferred tree** field in the Novell client configuration so that the Inbox Agent and this connector will function properly.

Before you can configure Scan to Desktop, a network administrator must complete the following steps:

To pre-configure Scan to Desktop:

1. Create the Inbox root directory.

   If the directory is on a Microsoft or Novell network, you must share it.

2. Create a service account that will deliver scanned documents to scan inboxes or to network home directories.
3. Add the service account to a new or existing group in one of the following locations:
   - On the domain controller, for Windows domain-based networks.
   - On NDS, for Novell networks.
   - On the local machine, for workgroups.

Note:
ShareScan uses this group when assigning permissions to the Inbox root directory and scan inboxes.

4. Give the group Full Control access rights to the Inbox root directory.
5. For workgroup implementations only, on the PC where the scan inboxes are located, create a local account for each user of Scan to Desktop.

Note:
If multiple 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 Managers.

41.6- Scan Inbox settings

The environment settings depend on the environment type that you select in the Scan to Desktop Properties window. The General Settings are the same for all environments.

Field Name	Description
Environment type	Select the environment type from the dropdown list: • Windows Active Directory • Novell eDirectory • Local Computer (Workgroup)
Service account settings	The given credentials must be validated via the **Test** button, otherwise you cannot proceed. To access the advanced customization options, click the **Advanced** button.

Field Name	Description
ShareScan Administrator	Select a group you are part of. That group is used when creating files and applying permissions to them. The permissions allow members of the selected group to read the created files.
Inbox	Setup the destination path. For more customized settings, click the Advanced button.
If same file name already exists	The following options are available: • Overwrite always: overwrites the existing file with the new one. • Create unique file name (.1, .2): creates a new file with a number postponed to its end. • Return error: returns an error indicating the problem. The user will have to go back and do anything which is necessary to create a new filename

41.6.1 - Inbox settings

Field Name	Description
Root path	Determines where the files are created. A *userdirs.txt* file is created, to store the connector's accounting information. Note that if the user does not have a home directory, the root path is used as a fallback, and the system creates a folder for the user automatically to be used as a scan inbox.
Inbox type	Select from the following options: • ShareScan Inbox: a **$domain\$user** structure is created under the specified **Root path**. Files are moved to the appropriate user's directory. When selected, the user can choose to send it to multiple recipients by selecting **Recipient: Multiple**. • Home directory: a single recipient is allowed, and a subdirectory is needed. The connector puts the files under that directory. **Root path** is ignored in this case. If the subdirectory does not exist, it is created.
Subfolder	Name of the subfolder for the Home directory.

Field Name	Description
Use service account when user credentials are incompletely set by service	Only applicable if the **Environment type** is set to Windows Active Directory, and the **Inbox type** is Home directory. If checked, and a service providing any type of user credential is used (ID Service, Cost Recovery, Session Logon) but that service does not provide an user password, the connector uses the service account specified here to store the document of the **Home directory \ Subfolder** of the specified user. If unchecked, the document is stored under the **Root path**.

41.6.2 - Destination settings

Scan to Desktop enables you to scan to the following destination types:

- Windows Folder
- Novell Folder

For each type of folder, you must supply the folder location and authentication settings.

Section	Field	Description
If a scanned image file already exists		Specifies the action for the connector to take if the recipient's scan inbox already contains a scanned document with the same file name: • Overwrite always: Replaces an existing scanned document with the one the connector is currently saving. • Return error: Displays an error message prompting the user at the device to change the file name. • Create unique file name: Adds a unique number to the file name, for example `filename.1`, `filename.2`. The scanned document is saved to the location using a unique file name and the existing document is not overwritten.
Folder location	Path to the folder	Destination information for the scanned documents. Click the **Browse** button and then select a folder.
	Enable subfolder navigation	Enables users to select a subfolder at the device.
	Maximum folder levels	The number of folder levels down that users may navigate.

Section	Field	Description
Authentication	Authenticate user	The options are: • None: Sends scanned documents to the destination without requiring user authentication. The Services Manager requires write access to the destination. • Logon as: Sends scanned documents to the destination using the specified authentication information; the user does not need to enter authentication information at the device. Specify the domain/tree, user ID, and password to use for authentication. The specified account requires write access to the destination. • Runtime: Sends scanned documents to the destination after the user enters authentication information at the device and logs on to the destination. Specify a user ID, password and a domain or tree so that the connector can retrieve the user list at runtime and enable users to search the user list. Test the credentials to verify that the connector can retrieve the user list using the specified credentials.
	Advanced	Enables you to configure the Advanced account settings.

41.6.3 - Advanced account settings

Advanced account settings are used in the configuration of scan inboxes and destinations.

Windows Active Directory advanced settings

Field Name	Description
Global Catalog server	You can set the following options for the Global Catalog server: • Locate server at runtime: the connector checks for the Global Catalog during runtime. If it fails, the user cannot validate the service account. • Always use the following server: the validation uses the given server • LDAP port: LDAP port number of the Global Catalog server. The default is 3268. • Server requires SSL: check if the server requires communication via SSL.

Field Name	Description
Search	Allows you to specify the attributes of the searches. The available settings are: • Base DN: Determines the LDAP search starts when typing in the LDAP authentication form or the Send form. Empty base DN prompts an error. • Scope: Can be set to **All levels below starting point** or **One level below starting point**. • Search on: Allows defining the attributes to be searched on. • Search while typing
Domain controller settings	You can set the following options: • LDAP port • Server requires SSL

41.6.3.1 - Novell EDirectory Settings

Field Name	Description
eDirectory server	You can set the following options for the eDirectory server: • Locate server at runtime: the connector checks for the eDirectory server during client runtime. If it fails, the user cannot validate the service account. • Always use the following server: the validation uses the given server. • LDAP port: LDAP port number of the Global Catalog server. The default is 389. • Server requires SSL: check if the server requires communication via SSL. • Server allows Anonymous Bind
Search	Allows you to specify the attributes of the searches. The available settings are: • Base DN: Determines the LDAP search starts when typing in the LDAP authentication form or the Send form. Empty base DN prompts an error. • Scope: Can be set to **All levels below starting point** or **One level below starting point**. • Search on: Allows defining the attributes to be searched on. • Search while typing

41.6.3.2 - Local Computer (Workgroup) Settings

Field Name	Description
Search	Allows you to specify the attributes of the searches. The available settings are: • Search on: Allows defining the attributes to be searched on. • Search while typing

42 - eCopy Scan to File

Scan to File enables users to scan documents and deliver them to predetermined network locations, Web locations, or to an SMTP server, with minimal data entry requirements. It is ideally suited to environments where large numbers of documents must be scanned quickly into automated or manual workflows.

42.1- Configuring the connector

For the generic connector configuration options, click here.

42.1.1 - Destination settings

Field/Button	Description
New	Adds a new destination.
Edit	Edits an existing destination
Copy	Copies the selected destination.
Remove	Removes the selected destination.
Move up	Moves the selected destination up in the list.
Move down	Moves the selected destination down in the list.

42.1.1.1 - Generic Destination Settings

Field/Button	Description
Name	The name of the destination.

Field/Button	Description
Type	The type of the destination. The following destination types are available: • Windows folder • Novell Netware folder • FTP folder • WebDAV folder • SMTP Message

42.1.1.2 - Folder Location Settings

Field/Button	Description
Folder location	Destination information for the scanned documents. • For Windows or Novell folders, click the **...** button and browse for an existing folder or create a new folder and select it. • For an FTP folder, enter the FTP location, such as “ftp://ftp01/scans”. • For a WebDAV folder, specify the root URL to a WebDAV folder, starting with either http:// or https://. Note that Quick Connect does not support long UNC paths, thus full path names are limited to 260 characters,
Secure connection (FTPS explicit)	Check this box to enable a secure connection. Only available for FTP folders.
Enable subfolder navigation	Enables users to select a subfolder at the device.
Maximum folder level	The number of folder levels down that users may navigate. The default is 3.

42.1.1.3 - Authentication Settings

Field/Button	Description
Authenticate user	The options are: • None: Sends scanned documents to the destination without requiring user authentication. The Manager requires write access to the destination. • Logon As: All documents scanned and stored to this destination use the credentials that you enter in the **User name** and **Password** fields. The user is not required to log on at the device. Specify the domain/tree, user ID, and password to use for authentication. The specified account requires write access to the destination. • Runtime: During each session at the device, prompts the user to provide logon credentials before storing the file. You specify the domain/tree to use for authentication.
User ID	All Authentication types require a user name and password if Logon As is selected as the user authentication method.
Password	Specifies the password for the **Logon as** user.
Domain	Select either **Logon as** or **RunTime** authentication mode to enable this combobox. • In **Logon as** mode, the combobox must specify the domain name for the Logon-as-user. • In **RunTime** mode, the combo box specifies the default domain name which is initially displayed on the Logon form but this is optional.

42.1.1.4 - SMTP Message Destination Settings

Field/Button	Description
Name	Specifies the SMTP server via name or IP address.
Port	Specifies the port number used. The default is 25.
Account	Sets the account to be used for authentication. The following options are available: • Generic account and None Authentication • Personal account - Windows Authentication • Personal account - Netware Authentication • Personal account - LDAP Authentication
Reply To:	Specifies the sender's email address. Available only for Generic account None Authentication.
Domain	Specifies the domain name used as initial value on the Logon form. Available only for Personal account - Windows Authentication.
Tree	Specifies the tree name used as initial value on the Logon form. Available only for Personal account - Netware Authentication.
LDAP settings	Displays the LDAP server settings dialog. Available only for Personal account - LDAP Authentication.

Field/Button	Description
Cc sender:	Checking this box sends a copy of each message to the sender.
To listbox	Use the **Add** button to add the SMTP addresses of the recipients.
Subject	Set the subject of the message.

42.1.2 - File name tab

Field/Button	Description
New	Adds a new entry via the File name field editor.
Edit	Edits an existing entry via the File name field editor.
Remove	Removes the selected entry from the list view.
Move up	Moves the selected entry up in the list view.
Move down	Moves the selected entry down in the list view.
Use Document service's file name	Checks published file name by a document service. If the file name is published, the connector uses the published name as an output file name instead of the File naming form and constructing the file name according to file naming rule.
If file name already exists:	Set the method for resolving file name conflicts: • Create unique file name (.1,.2,etc): The connector creates a unique file name by appending a rolling number with a dot separator. • Overwrite always: Overwrite the existing file with the scanned document. • Return error: Show an error message at the device. The User has to specify a different name at the device or cancel the current job.

42.1.2.1 - File Name Field Editor

Field Type	Description
Name	Specifies a unique file name field name. Not case sensitive.

Field Type	Description
Type	Specifies a type of field. Type-dependent settings change according to the field. For more information, see the Field types table below. • Alphanumeric • Numeric • Date • Time • List • Batch-based index value • Batch Number • Separator • Device Name • Logged on user

42.1.2.2 - Field Types

Field Type	Description
Alphanumeric	Inserts text into the file name. the text can contain any printable characters except those that are restricted from Windows file naming conventions or any characters that you define as separators. • Minimum/maximum length: The minimum and maximum number of characters allowed. • Remember: The number of previous entries to display when the user is prompted for the naming information. If set to zero, no previous values appear in the drop-down list.
Batch number	Inserts the current batch number into the file name. • Leading zeroes: Pads all values with leading zeroes to make their length equal to the maximum field size. For example, if you specify "3" in the Length field and you enable leading zeroes, batches are numbered “001”, “002”, … , “010”, “011”, … , “100”, “101”, … , “999”. If you do not enable leading zeroes, batches are numbered "1", "2", etc. • Length: The maximum number of digits allowed for the batch number, including leading zeroes.
Batch-based index value	You can only use batch-based index values if you have the eCopyBarcode Recognition Service. Batch-based indexing enables you to create index files with separate barcode values for each batch.
Date	Inserts the date on which the document was scanned into the file name. Format: The format in which you want the date to appear in the file name.

Field Type	Description
Device name	The name of the device from which the document is scanned. No additional settings.
Numeric	Inserts numeric characters into the file name. • Default: Only numeric characters can be entered in this field. • Field Size: The minimum and maximum number of digits allowed. • Leading zeroes: Pads all values with leading zeroes to make their length equal to the maximum field size. • Remember: The number of previous entries to display when the user is prompted for the naming information. If set to zero, no previous values appear in the drop-down list.
Separator	Character: The character that you want to use to separate the fields in the file name. The character that you select cannot be used in any other file name field.
List	Enables you to create a list of values from which the user can select a single value at the device. If you select the **Required** option, the user at the device must select a value from the list. If you do not select this option, the user at the device can leave the field blank. If you select the **Required** option and do not select the **User modify** option, you must set one of the list items as the default value.
Time	Inserts the time at which the document was scanned into the file name. Format: The format in which you want the time to appear in the file name.

43 - Scan to Printer

The eCopy Scan to Printer Connector enables users at an eCopy-enabled device to scan and print documents to a network printer, regardless of its physical location. Users can select various printing and page layout options.

43.1- Configuring the connector

For the generic connector configuration options, click here.

43.2- Connector Document settings

Document settings enable you to specify default settings for options specific to a connector profile, including encryption, searchable text, and file format. They also enable you to specify whether users at the eCopy-enabled device can change the settings; user-modifiable options are available when the user presses the **Document settings** button on the Preview screen.

Note:
Each connector profile supports a unique group of settings. If a setting is not available for the connector you are configuring, it will be grayed out.

Option	Setting Description
File format	The connector supports only JPG format.
Color compression	Select High or Medium compression for color documents.

43.2.1 - Configure settings

Section/Field Name	Description
Enable QuickPrint	Does not display the settings screen to the user at the device. The scanned documents print directly to the default printer, using the default print settings from the connector.
Available printers	The printers that will be available at the device.
Set as Default printer	Enables you to specify the default printer. Indicated by a checkmark icon before the printer's name in the list.
Move up	Moves the selected printer up in the list. If you move a printer to the top of the list, you can confirm it as the default printer.
Move down	Moves the selected printer down in the list. Moving a printer from the top of the list sets the new topmost printer as default.
Refresh	Refreshes the printer list.
Printer information	Gives information on the location, model, and status of the selected printer.
Printer preferences	Informs you of the printing preferences (collation and duplex printing) for the selected device.

44 - Scan to USB

The eCopy Scan to USB Connector enables users at an eCopy-enabled device to scan documents to an USB device.

44.1- Configuring the connector

For the generic connector configuration options, click here.

44.1.1 - Configure settings

Section/Field Name	Description
If a scanned image file already exists then take this action	Allows you to set the action taken • Overwrite always • Return error • Create unique file name (.1, .2, etc.)

The eCopy Connector for SMTP via LDAP

The eCopy Connector for SMTP using LDAP enables users to send scanned documents from an eCopy-enabled device as email attachments using an SMTP server on the network. When a user sends email from a personal SMTP account (including a Gmail account), the system prompts users to log on to validate their identity. The Global Address List is provided by an LDAP server.

44.2- Configuring the connector

For the generic connector configuration options, click here.

44.3- Connector properties

The **Properties** window enables administrators who are more familiar with LDAP to fine-tune the settings, without relying on the Wizard.

- Logon / SMTP settings
- LDAP settings
- Address book settings
- Sending options settings

44.3.1 - Logon / SMTP settings

Select the protocol combination to be used via this tab.

Field Name	Description
Authentication	Select the authentication type from the dropdown list: • Runtime: LDAP • None: Send from generic • None: Send from generic email address specified by Data Publishing For a practical example of configuring the Data Publishing with a connector, click here.
Allow user to modify	If checked, the user is able to customize the email field on each scan.
Default generic email:	Allows the administrator to provide a default generic email address to specify as the sender.
Server	IP or DNS name of the SMTP server.
Port	Port address of the SMTP server. Default is 25, when an unencrypted communication channel is used. For encrypted SMTP communication, port 587 is selected.
Test	Clicking the **Test** button tests the connector with the current settings.
Server requires SSL	Specifies if SSL is used for the SMTP communication. Must be set to on (checked) when using Gmail.
Reset	Click this button to set the default values for setting Gmail or generic SMTP servers. For Gmail, the defaults are as follows: • **Hostname**: SMTP.GMAIL.COM • **Service port**: 587 • **Server requires SSL**: ON (checked) • **Server requires authentication** Searching your Gmail contacts is also enabled. The **Search while typing** feature can be configured on the **Address book** tab.

Field Name	Description
Authentication	Define the type of authentication behavior for the SMTP server: • **Runtime: Prompt sender for a username and password**: the SMTP Authentication form is displayed to the user at runtime after the Send form. • **None**: When selected, the user is not prompted for a username and password. In addition the connector does not attempt any authentication with the SMTP server. The email send process may fail if the server requires authentication. • **Login as**: When selected the fields Username and Password will display below the Authentication combo in admin. Here the administrator can specify a set of credentials that will always be used when sending an email from the connector. • **Use senders LDAP userID attribute and runtime password**: When this option is selected and if the LDAP address book is enabled, the connector utilizes the LDAP userID attribute and password provided at the User Logon form to authenticate them against the SMTP server. If the LDAP address book is not enabled at the time of closing the properties dialog we will show an error to the user and tell them LDAP must be enabled or a different SMTP authentication type must be chosen.
Use specified domain if secure SMTP is enabled	If checked, the domain box is enabled and the user can input a domain. During the send process, the connector provides this domain along with username and password to the SMTP server.

44.3.2 - LDAP settings

Controls the various LDAP settings of the connector.

Field Name	Description
Enable LDAP address book	Click the **Find** button to locate the LDAP server during runtime.
Server	IP or DNS name of the LDAP server.
Port	Port number of the LDAP server for communication purposes. The default is 389.
Server requires SSL	Check if the server requires SSL connection.
User DN	User DN of the logged in user.
Password	Password of the logged in user.
Connect anonymously	Determines if the connector connects to the LDAP anonymously or if a UserDN and password are provided. Not all LDAP servers allow anonymous connections.

Field Name	Description
Advanced LDAP settings	Allows you to define what the actual attribute is called on the LDAP server itself and allows customization of LDAP attributes to return during your searches. The available settings are: • Person: Allows defining the actual ObjectClass to represent the “person” class during a recipient and sender search. • Group: Allows defining a second ObjectClass to represent the “Group” class during a recipient search only. • First name: Allows defining the actual attribute name to search for. • Last name: Allows defining the actual attribute name to search for. • Common name: Allows defining the actual attribute name to search for. • User ID: Allows defining the actual attribute name to search for. • Email: Allows defining the actual attribute name to search for.
LDAP search	Allows you to specify the attributes of the LDAP searches. The available settings are: • Base DN: Determines the LDAP search starts when typing in the LDAP authentication form or the Send form. Empty base DN prompts an error. • Search scope: Can be set to **All levels below starting point** or **One level below starting point**. • Search on: Allows defining the attributes to be searched on. • Search while typing • Max results: Sets the amount of results returned. The default value is 200.
Test	Clicking the **Test** button tests the connector with the current settings.

44.3.3 - Address book

Section/Field Name	Description
Enable Nuance address book	Enables the Nuance address book.
Database	Enables you to **Select** or **Create** a database. To create a database, you must provide the following data: • SQL server name: a valid SQL server name and instance • Database: the database name for the Nuance address book. • User ID: the identification of the user. • Password: the password required to access the database.
Search on	Set the search parameters you want to use.
Address book	Shows the name of the selected address book.
User	Displays the name of the selected user.

Section/Field Name	Description
Manage	Use the **Add**, **Delete**, **Import**, and **Export** buttons to manage the address data list.
GMail	Check the **Enable using Gmail Contacts** checkbox to access the user's contacts list via the Gmail Contact API; this way, when the user enters recipients on the Send form of the connector, the Gmail contacts are visible and selectable along with, for example, the eCopy addressbook contacts. Use the **Search on** dropdown list to specify the search criterion.

44.3.4 - Sending options

You can set up the Express mode using the **Sending options** tab.

Section/Field Name	Description
Display options	Allows you to set the send form options: • Show • Show without CC field • Skip and send to default recipients • Skip and send to self
Default message	Allows you to set the default message.
Default recipients	Allows you to specify default email recipients for a connector. Use the **Add** button to populate the list. Click the **Remove** button to delete the selected entry. Also allows you to specify settings to retrieve recipient names from data publishing.
Data publishing	Allows you to set the data publishing action: • Ignore Data Publishing values • Recipients are taken from Data Publishing only • Combine values with default recipients For a practical example of configuring the Data Publishing with a connector, click here.
Send copy to sender	Sends you a copy of each message sent.
Manage content	Allows you to add /remove or reorder notes and subjects from the list. Also allows you to create bylines, which appear below the note in the email. You can also define notes and subjects to be received from data publishing by using $$NOTE$$ and $$SUBJECT$$ in the **Note** and **Subject** fields.

44.3.5 - Connector Wizard settings

The Wizard enables administrators to initially configure the connector. Many windows contain a **Test** button that enables you to validate the logon information or test the server connection.

Wizard window	Field	Description
LDAP server type	Server type	The available server types: • None (disable LDAP address book) • Generic LDAP server • Windows Active Directory • Windows Active Directory (Untrusted) • Novell eDirectory • Netscape LDAP server • Open LDAP server • IBM Domino server If your server type is not on the list, select the **Generic LDAP server** option
	LDAP attributes	Enables you to set the attributes for the LDAP classes used by your server or to accept the defaults shown here.
Windows Active Directory server account	Account settings	Active Directory Server Account settings: • User name • Password • Domain The Wizard uses this information to set the user DN and server name. Available only if you select Active Directory as the server type.
LDAP server settings	Connect anonymously	Bypasses the Select LDAP User window and allows anonymous connection to the LDAP server, if the server supports anonymous authentication. Not available if you select Active Directory as the server type.
	LDAP server	LDAP server settings: • User DN • Password • Server • Port • Server requires SSL You must provide the full user DN if the server requires it. The Wizard assumes that the server is using the default port number (389). The Wizard resets the port back to 389 if it was changed in the **Properties** dialog box. Clicking the **Test** button checks your settings.

Wizard window	Field	Description
Search settings	Defines how the LDAP server searches the address book. Enables you to select a user from the LDAP tree in the Select LDAP User window. Not available if you select Active Directory as the server type.	
	Base DN	The node on the LDAP tree from which all searches should begin. If you do not know the node, click the **Browse** button and select the node from the tree structure in the selection window.
	Search scope	Select a search level: • All levels below search starting point: Allows expanded searching. • One level below search starting point: Optimizes LDAP queries and improves performance.
	Sender search	The search criterion that the server uses to find the sender: • First Name • Last Name • Common Name • User ID (default) The setting defines the information that the user sees on the Logon screen at the device.
	Recipient search	The search criterion that the server uses to find the recipient: • Common Name (default) • First Name • Last Name • User ID The setting defines the information that the user sees on the Send screen at the device. **Tip**: If you are using an Active Directory server and want the list of recipients to display groups as well as individuals, eCopy recommends that you retain the default setting, Common Name. If you select any other search criterion, users who want to send documents to a group must enter the complete e-mail address of the group at the device.
	Search while typing	Enables or disables the **Search while typing** functionality for the related field at the device.
	Max results	The limit on the number of results to be returned by the LDAP search. The default value is 200.
SMTP settings	Select your SMTP server and the type of authentication that will be required of the user at the device.	
	Server	The SMTP server name
	Port	The SMTP port number.

Wizard window	Field	Description
User login settings	Authentication	The type of authentication to use on the SMTP server. Available only if SMTP Basic Authentication is enabled on the server.
	Generic email	A generic email address that is used as the sender account for all email.
	User Modify	The user at the device can modify the sender's email address.
	Runtime: LDAP	Requires the user at the device to enter the user name and password specified for the LDAP server.
	Runtime: Windows	Enables users at the device to use their Windows logon information, via the SAMAccountName attribute, to log on. The **Domain** field specifies the Windows domain name, populated from the Account Settings window. This is required if you select the Windows option. Available only if you select Active Directory as the server type.
	Runtime: Novell	The Novell tree. This is required if you select the **Novell** option. Available only if you select eDirectory as the server type.
Settings summary	Enables you to review your settings. Use the **Back** button if you need to change any settings. Use the **Finish** button to apply your settings to the connector profile.	

44.3.6 - SMTP settings

Section	Field	Description
SMTP server	Server	The IP address or DNS name of the SMTP server to use for outgoing messages. If the server supports anonymous access, it must be disabled if you want to use SMTP authentication.
	Port	The SMTP port number (default is 25).
	Server requires SSL	Enables Secure Socket Layer (SSL) to be used for SMTP communication. If you select this option, you must install a valid SSL certificate on the same device as the connector.

Section	Field	Description
Authentication	Runtime: Prompt Sender for a user name and password	Prompts the user at the device to enter a user name and password when the user presses the **Send** button on the Send screen. Available only if SMTP Basic Authentication is enabled on the server. **Note:** If Session Logon is enabled, and SSL is not enabled, eCopy recommends that you select "None" or "Login as".
	None	Use if the SMTP server does not require authentication. The user at the device is not required to supply any credentials. If the server requires authentication, the email send process can fail.
	Login as	Enables the user at the device to connect to the SMTP server without being prompted for authentication information. The connector uses the user name and password set by the administrator.
	Use Sender's User ID, LDAP attribute, and runtime password	Uses the sender's LDAP authentication information to connect to the SMTP server. To use this option, you must enable the LDAP address book on the **LDAP settings** tab.

45 - eCopy Connector for iManage WorkSite

The eCopy Connector for iManage WorkSite allows users to scan documents directly into the WorkSite library of an iManage WorkSite system from an eCopy-enabled device.

Users can store documents in any eCopy-supported format (PDF, PDF/A, TIF Fax, TIF, JPG, DOC, DOCX, XPS, XLS and XLSX).

45.1- Configuring the connector

For the generic connector configuration options, click here.

45.2- Defining a scanning destination

For a generic description of defining a scanning destination, click here.

If you select **Specify**, then you must specify a location, such as a folder or Document Worklist, that can hold documents.

Selecting the **Auto Index** option enables you to configure the index field values. The Document Profile screen does not appear at the device.

Selecting any of the other **Behavior** options disables the eCopy values table and displays the Document Profile screen at the device unless you also specify values for all of the default fields.

45.2.1 - Authentication settings

Field Name	Description
Name	Enter the display name of the destination.
User name	Enter the user name to be used. If **Login as** is selected, this user name is also used for authentication instead of prompting the scanning user for this information. If **Runtime** is selected, the scanning user is prompted for credentials at the scanning device.
Password	Enter the password to be used.
Server	Enter the server you want to connect to.
Type	Determines the authentication at the ScanStation. If **Login As** is selected, the authentication form is skipped and the credentials provided are used for login. If **Runtime** is selected, the authentication form is displayed at the scanning device.
Search while typing	Enables or disables the functionality.
Use trusted login	If checked, the trusted login settings are used when a user authenticates at the scanning device.
Trusted login settings	Set the following options: • Impersonation password: if login to the current domain/tree is successful, the connector logs the user in via the administrator password. • Windows/Novell: sets what to authenticate against.
Test	Clicking the **Test** button tests the connector with the current settings.

45.2.2 - Navigation settings

Field Name	Description
Behavior	Select the behavior you want to use: • Navigate workarea: if selected, the user is able to browse the entire Worksite server, and can choose any valid folder to store documents as a target. • Specify: select a valid folder as final scanning destination. The navigation form on the client side is skipped. • Specify and browse: select a valid folder as a default scanning destination. Users can browse for different folders, • Autoselect: the connector navigates a target automatically using the data publishing values. Three Data Publishing fields are used in this feature: `ECOPY_CLIENT_ID` (or `ECOPY_CUSTOM1`), `ECOPY_MATTER_NUMBER` (or `ECOPY_CUSTOM2`) and `WORKSITEFOLDER`. The first two are used to navigate to a workspace which relates to the client and matter. When a workspace is identified, the navigation to the folder can happen in two ways: the connector tries to find a folder with an administrator-defined name, or a folder with the name published via the `WORKSITEFOLDER` data publishing key. If the ellipsis button of the **Navigation** tab is pressed when this behavior is selected, the Search folder dialog is displayed, and the administrator can specify folder name source. Using the displayed dialog window, checking the **Create folder** option allows automatic folder creation with the provided name, if the workspace is identified succesfully, but the folder does not exist yet. Clicking the **Browse** button resets the content of the list control to the content before clicking on the **Search** button if the list contains search results. Otherwise it resets to the content which was in the list when the form was displayed.
Folder name	Displays the selected folder name. Use the **...** button to browse the folder structure.
Provide a storage confirmation screen	Enables or disables client-side displaying of the successfully stored document's Worksite document ID.
Provide autonavigation property screen as needed	Enabling allows the user to enter the Client ID and Matter number on a separate client form if these values are not received through data publishing. The connector performs workspace search based on the entered values and the document is stored at the found location. If disabled, the standard navigation form appears

45.2.3 - Attributes settings

Field Name	Description
Behavior	Select the behavior you want to use. The available options are: • Show selected fields: the connector displays all required fields and selected optional custom fields for the client, and prepopulate them from the source defined by the administrator. • Show required fields: the connector displays all required fields for the client, and prepopulates them from the source defined by the administrator. • Auto-index: the connector pre-populates attributes from the source defined by the administrator. When the automatic profile population creates a valid profile, the document attributes forms on the scanning device are skipped. If it fails, the document profile attributes form is displayed on the device screen, and the end user can correct the issue.
Select fields	Click this button to customize the visible fields.
eCopy values	Select an entry in the table and click the **Edit** button to configure the default value of the attribute. The following attributes can be configured: • Database: can be configured only if the target is the **Document worklist** and the Worksite server manages more than one database. • Description: always configurable. Can be populated from the `<FILENAME>` system variable as well. • Author: always configurable. Can be populated from the `<OPERATOR>` system variable as well. • Type, Class, Subclass, and custom fields: configurable via the Default value dialog. The Default value of <attribute> dialog provides a checkbox in order the enable/disable attribute value population from data publishing. The default value can be configured for folder default value, or administrator predefined value. Predefining is available if the target database is unambiguous, and works by either clicking the value on the displayed list, or entering it manually. The predefined value is validated against the target database, if it is possible. If not, a warning dialog is displayed, the validation process is skipped, and values are validated just before the document storing. When configuring a sub-attribute (a subcategory of a main attribute), the valid values list contains only those values which are real sub-categories of the already configured main category. The Category - Sub-Category pairs are: Class-SubClass, Custom1- Custom2 and Custom29-Custom30.

45.2.4 - Data Publishing keys

Published key	Mapped Worksite attribute	Note
ATTYPE_CLASS	Class	Used by the **Auto select** mode as well.
ATTYPE_SUBCLASS	Subclass	Used by the **Auto select** mode as well.

Published key	Mapped Worksite attribute	Note
ATTYPE_CUSTOM1	Custom1	When data are provided in both `ECOPY_CLIENT_ID` and `ATTYPE_CUSTOM1`, `ECOPY_CLIENT_ID` takes precedence.
ATTYPE_CUSTOM2	Custom2	When data are provided in both `ECOPY_MATTER_NUMBER` and `ATTYPE_CUSTOM2`, `ECOPY_MATTER_NUMBER` takes precedence.
ATTYPE_CUSTOM3	Custom3	
ATTYPE_CUSTOM4	Custom4	
ATTYPE_CUSTOM5	Custom5	
ATTYPE_CUSTOM6	Custom6	
ATTYPE_CUSTOM7	Custom7	
ATTYPE_CUSTOM8	Custom8	
ATTYPE_CUSTOM9	Custom9	
ATTYPE_CUSTOM10	Custom10	
ATTYPE_CUSTOM11	Custom11	
ATTYPE_CUSTOM12	Custom12	
ATTYPE_CUSTOM29	Custom29	
ATTYPE_CUSTOM30	Custom30	
WORKSITEFOLDER	-	Used by the **Auto select** mode as well.

For more information on Data Publishing, click here. The Worksite connector can also use batching when processing documents with the help of Data Publishing. For more information on batching and data publishing, click here.