XMedius

WWW.XMEDIUS.COM

XMediusFAX eCopy ShareScan Connector 5.0

Administration Guide

XMediusFAX eCopy ShareScan Connector

Version Number 5.0.0.52 – October 2017.

Patents

• Protected by US Patents 4,994,926; 5,291,302; 5,459,584; 6,643,034; 6,785,021; 7,283,270.

• Protected by Canadian Patents 1,329,852; 2,101,327; 2,417,202.

• Additional US, Europe and Japan patents pending.

Acknowledgments

This software includes several libraries and software owned by third parties and distributed under their respective license. For more information see the \3rd folder included in this distribution (when applicable).

• ShareScan: Copyright © Nuance Communications Inc.

Disclaimer

XMedius reserves the right to make changes and alterations to its software and documentation without prior notification.

Although every attempt has been made to accurately describe and document the product, XMedius does not guarantee that documentation is without error or omission. XMedius is not responsible for any loss of data that may occur during the operation of its software. Nor does XMedius recognize any liability that such losses may occasion.

No part of this publication may be reproduced or altered, by any means whatever, manual or electronic, without the prior written consent of XMedius.

All other trademarks, brand names, or product names are the property, trademarks, or registered trademarks of their rightful owners.

References to other products or software imply no warranty of the XMediusFAX eCopy ShareScan Connector software by the manufacturers of those products and software.

Copyright

Contact Information

• Web: www.xmedius.com
• Sales: sales@xmedius.com
• Licenses: license@xmedius.com

Americas, Asia and Oceania:

XMedius
3400 de Maisonneuve Blvd. West, Suite 1135
Montreal, Quebec H3Z 3B8 – CANADA - PO Box 48

• Telephone: +1 514-787-2100
• Tollfree North America: 1-888-766-1668
• Fax: +1 514-787-2111

Europe, Middle-East and Africa (EMEA):

XMedius
Building MB6 41 rue des 3 Fontanot
92000 Nanterre – France

• Telephone: +33 (0) 1 70 92 13 10
• Fax: +33 (0) 9 70 26 19 23

Technical Support

On-premises software:

• Web: support.xmediusfax.com
• Email: support.software@xmedius.com
• Tel. Americas: +1-866-615-3066 (North America only) | +1 514-787-2122
• Tel. EMEA: +33 (0) 1 70 92 13 12
• Tel. APAC: 0011-800-132-00000 (Australia only) | +1 514-787-2122

Cloud solution:

• Web: support.xmedius.com
• Email: support.cloud@xmedius.com
• Tel. North America: +1 855-867-5065
• Tel. Europe: +33 (0) 1 70 92 13 13

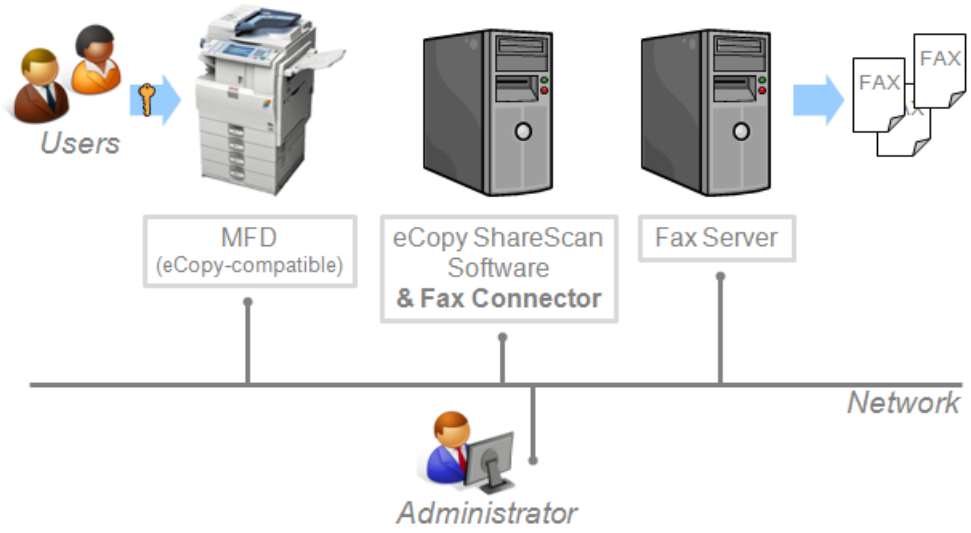
Table of Contents

Chapter 1 Introduction

The XMediusFAX eCopy ShareScan Connector

The XMediusFAX eCopy ShareScan Connector is a solution allowing Multi-Function Devices (MFDs) that are compatible with the eCopy ShareScan technology to fax documents by using XMediusFAX.

Here is an example of deployment including an MFD, the computer hosting the eCopy ShareScan Software (with XMediusFAX eCopy ShareScan Connector installed as a plug-in) and the Fax Server (XMediusFAX):



Note: More than one MFD connected to the network can benefit from the XMediusFAX eCopy ShareScan Connector.

From the MFD, users can benefit from many faxing features inherited from XMediusFAX, according to their faxing profile. They can also select recipients from the XMediusFAX phone books and add new entries to their personal contacts.

Many methods for authenticating the fax users can be configured in order to meet your needs.

Purpose of This Document

This document is intended for Administrators of XMediusFAX and MFDs and describes all steps to:

- Install the XMediusFAX eCopy ShareScan Connector on the machine hosting the eCopy ShareScan software.

- Configure the XMediusFAX eCopy ShareScan Connector within the eCopy ShareScan software.
- Configure MFDs to have the new faxing feature enabled.
- Optionally install a certificate from the XMediusFAX host for additional network security.

This document also gives information on all available fax user authentication methods and contexts in order to configure your faxing environment according to your needs.

Chapter 2 Installation Requirements

Installation Requirements

☞ **Important: Before you start**, please read this section carefully to verify if your current deployment is consistent with the system requirements.

XMediusFAX eCopy ShareScan Connector and eCopy ShareScan Software/Host

The eCopy ShareScan Fax Connector:

- Is only supported by eCopy ShareScan Software version 5.0 or above (the XMediusFAX eCopy ShareScan Connector version number actually follows the eCopy ShareScan SDK version used for its development).
- Must be installed on the computer where the eCopy ShareScan Software is installed and running.

☞ **Important:** This version of the XMediusFAX eCopy ShareScan Connector cannot be used to perform an upgrade from any of its previous versions.

The computer hosting the eCopy ShareScan Software must have network access to:

- The XMediusFAX host.
- All MFDs that are required to use the XMediusFAX eCopy ShareScan Connector

Multi-Function Devices (MFDs)

All MFDs that are required to use the XMediusFAX eCopy ShareScan Connector must:

- Be compatible with eCopy ShareScan Software version 5.0 or above.
- Have a panel screen with a minimum resolution of 640x190.
- Be registered on the computer hosting the eCopy ShareScan Software.

☞ **Note:** About fax users Authentication support on MFDs:

A fully operational authentication method specifically based on the XMediusFAX Internal User accounts is provided with the XMediusFAX eCopy ShareScan Connector.

However, the "Session Logon" integrated authentication method is also supported when configured and activated within the ShareScan software.

Fax Server (XMediusFAX)

The XMediusFAX eCopy ShareScan Connector is compatible with XMediusFAX 6.5.5 and above versions, as well as with the XMedius's cloud-based fax solution.

With cloud-based fax solution:

- You must have an active fax service account with XMedius.

With on-premises fax server deployment:

- XMediusFAX must be properly installed and running on a server accessible from the XMediusFAX eCopy ShareScan Connector host.
- The following minimum required hotfixes must be installed on your XMediusFAX, depending on your version:

XMediusFAX version	Component minimum version (hotfix) required
XMediusFAX 6.5.5	Config Manager (XMConfigManager.exe) 6.5.5.310
	Web Service (faxservice.war) 6.5.5.310
XMediusFAX 7.0.0	Config Manager (XMConfigManager.exe) 7.0.0.360
	Web Service (faxservice.war) 7.0.0.360
Higher versions of XMediusFAX	No specific hotfix required.

Note: All hotfixes are available for download at *support.xmediusfax.com*.

- Your XMediusFAX licence must include:
  - The Web Services feature.
  - The maximum number of MFDs that are allowed to use the XMediusFAX eCopy ShareScan Connector.

Note: For more details on XMediusFAX, please refer to its *Installation and Maintenance Guide* and its *Administration Guide*.

Chapter 3 Fax Connector Installation

Fax Connector Installation Overview

This chapter provides the steps to follow in order to:

- Install the XMediusFAX eCopy ShareScan Connector on the computer hosting the eCopy ShareScan software.
- Optionally install the certificate of the XMediusFAX host if you are planning to enable certificate validation for additional security.

Important: This version of the XMediusFAX eCopy ShareScan Connector cannot be used to perform an upgrade from any of its previous versions. It only applies to devices compatible with eCopy ShareScan Software version 5.0 or above.

Installing the XMediusFAX eCopy ShareScan Connector

Attention: This installation must be performed on the computer where the eCopy ShareScan software is installed.

To install the XMediusFAX eCopy ShareScan Connector:

1. Launch the XMediusFAX eCopy ShareScan Connector installer: `Setup.exe`.
2. Choose the language to use during the installation and click **OK**.
3. Simply follow the instructions of the installer.

The installation is now complete and you can configure the Connector and the MFDs directly from the eCopy ShareScan software interface (see: *Fax Connector and MFD Configurations – Overview* on page 7).

Installing the XMediusFAX Certificate (Optional)

The XMediusFAX eCopy ShareScan Connector uses by default the secured Web Services feature of XMediusFAX (with https).

If you wish to add more security for the Web Services connection, you can enable a validation of the server identity, via the Connector configuration interface (see *Configuring the XMediusFAX eCopy ShareScan Connector* on page 11). In that case, you must also ensure that the XMediusFAX certificate will be trusted on the computer hosting the XMediusFAX eCopy ShareScan Connector.

Note: A default keystore (certificate container) was automatically generated on the XMediusFAX host during its installation: `[tomcat_home]\conf\keystore.jks`. It is ready to be used without any changes and should work properly in your faxing environment. It includes the host name of XMediusFAX and its password is “changeit”.

However, if you wish to generate a new keystore to replace the default one (for example to adjust the Common Name or to change the password), see *Generating a New Certificate Container (If Required)* on page 19 before following the procedure below.

Important: This procedure is not required if the certificate is signed by a Trusted Certificate Authority.

To ensure that the XMediusFAX eCopy ShareScan Connector host will trust the XMediusFAX certificate:

1. Retrieve the certificate file from the XMediusFAX host:
   a) Open a Web browser and type the address: `https://` followed by the XMediusFAX host name.
   b) Continue despite the warning message (certificate not trusted yet).
   c) Locally save the certificate file (option **Copy to file** or **Export**, depending on your browser)
2. Add the certificate to the Trusted Root Certification Authorities store:
   a) Launch the Microsoft Management Console (search for `mmc.exe` from the **Start** menu).
   b) On the **File** menu, click **Add/Remove Snap-in**.
   c) Under **Available snap-ins**, click **Certificates**, and then click **Add**.
   d) Under **This snap-in will always manage certificates for**, click **Computer account**, and then click **Next**.
   e) Click **Local computer**, and click **Finish**.
   f) Click **OK**.
   g) In the console tree, double-click **Certificates**.
   h) Right-click the **Trusted Root Certification Authorities** store.
   i) Click **Import** to import the certificate (the file you saved at the previous main step) and follow the steps in the **Certificate Import Wizard**.

Chapter 4 Fax Connector and MFD Configurations

Fax Connector and MFD Configurations – Overview

Before being able to send faxes with MFDs using the XMediusFAX eCopy ShareScan Connector, you must configure the connector and each of the concerned MFDs.

This chapter covers the following subjects:

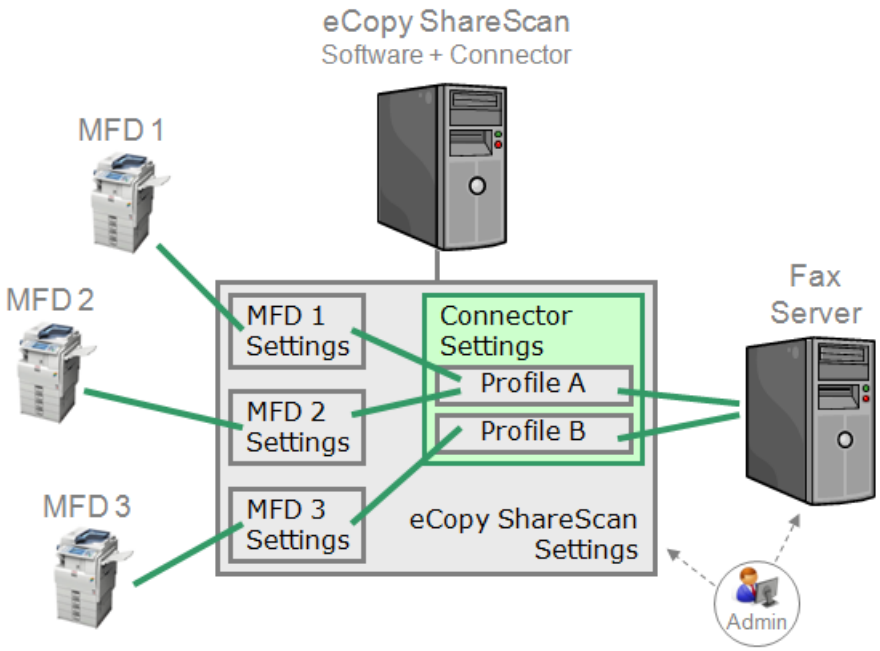
- Information on the way the faxing feature will be made available on your MFDs.
- Information on fax users authentication, with description of the various methods that can be used
- Some instructions to configure your faxing environment according to the authentication method that is used.
- The procedure to configure the XMediusFAX eCopy ShareScan Connector
- The procedure to configure MFDs to use the XMediusFAX eCopy ShareScan Connector.

👉 **Note:** Before starting, you must have first installed the XMediusFAX eCopy ShareScan Connector on the computer hosting the eCopy ShareScan software.

About XMediusFAX eCopy ShareScan Connector and MFD Configurations

The XMediusFAX eCopy ShareScan Connector is installed as a plug-in of the eCopy ShareScan software. Its configuration is performed via the eCopy ShareScan Administration Console.

To have the XMediusFAX eCopy ShareScan Connector enabled, each MFD must also be configured via the eCopy ShareScan Administration Console.



Connector Settings Profile

A settings profile of the XMediusFAX eCopy ShareScan Connector contains:

- All settings for connection and authentication of the connector with the server hosting XMediusFAX.
- Other settings for connector and user options that will be available on the MFD.

Note: You can decide to have different configuration settings (profiles) depending on the MFD that will use the XMediusFAX eCopy ShareScan Connector (e.g. if you want the fax users to be differently authenticated on each MFD).

MFD Settings

All MFDs available from the eCopy ShareScan Administration Console have separate settings where the XMediusFAX eCopy ShareScan Connector can be enabled among other connectors. The connector is enabled on one MFD when one of its available profiles is selected via these MFD settings.

Fax Users Authentication

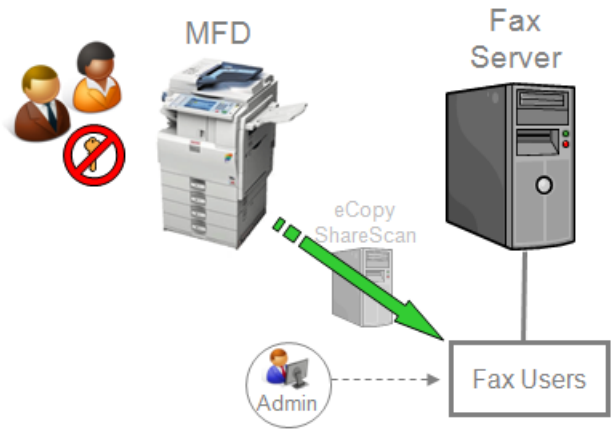
The way users will be authenticated in order to use the faxing feature are multiple and largely depend on your company architecture and policies.

Note: For technical reasons, this section should be preferably considered prior to configuring the XMediusFAX eCopy ShareScan Connector.

Several cases are developed in this section in order to help you make a choice and/or configuring the various devices of your faxing environment according to your needs:

- No authentication (using a default fax user account)
- XMediusFAX user authentication (specific authentication screen enabled on the faxing feature)
- Other authentication types (including single sign-on authentications), via the "Session Logon" feature of the the eCopy ShareScan software (which requires configuration in the related section of the eCopy ShareScan Administration Console).

Default User Configuration (No Authentication)



When no user authentication is required, all users will be allowed to fax, by sharing the same default fax sender properties and phone book.

For allowing this, you will create on XMediusFAX a default user account that will be referenced in the XMediusFAX eCopy ShareScan Connector configuration settings:

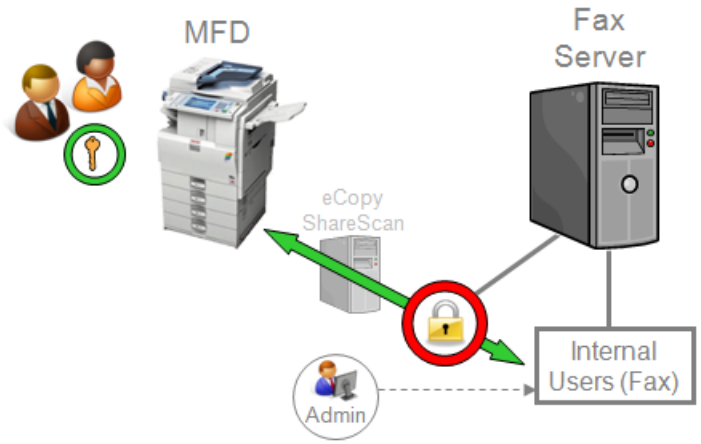
1. From the XMediusFAX administration interface, configure XMediusFAX to include a user that you will dedicate to the MFD.

   Note: This user can be either an **Internal User** or an external user retrieved by the **Directories Integration** (see the XMediusFAX *Administration Guide* for more information).

   For example, an **Internal User** identified with this **SMTP Address**: `mfd01@example.com`.

2. When you will configure the XMediusFAX eCopy ShareScan Connector, make sure to:
   a) Select `Default User` as **User Authentication Method** (no authentication).
   b) Enter in the **Username** field the SMTP address of the fax user account you previously created.
   In our example: `mfd01@example.com`.

XMediusFAX User Authentication Configuration



When user authentication is required at the XMediusFAX level, all users having an internal account on XMediusFAX will be able to fax, each using their own fax sender properties and their own phone book.

To allow this:

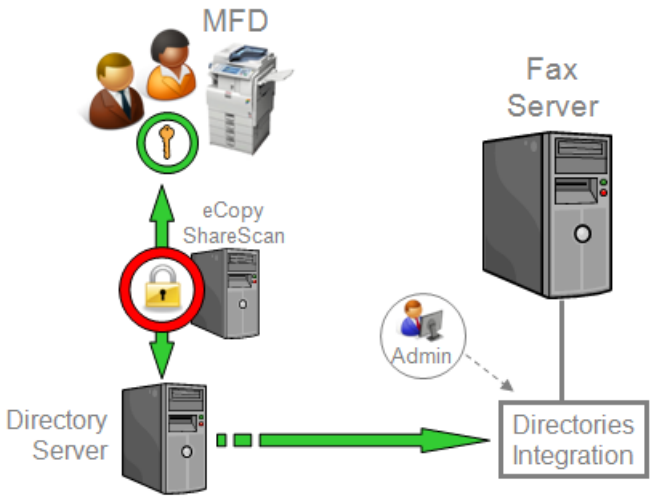
1. From the XMediusFAX administration interface, add all required fax user accounts to the list of **Internal Users**, according to the procedure given in the XMediusFAX *Administration Guide*.

   Tip: You also have the possibility to import Internal Users from an existing directory.

2. When you will configure the XMediusFAX eCopy ShareScan Connector, make sure to select `Fax Server` as **User Authentication Method**.

Remember: With this method, the authentication will be necessarily done by entering personal credentials, therefore the administrator will have to provide users these credentials, which are their fax user account name and password.

Other Authentication Configurations



Conceptually, any other authentication method can be supported for accessing the faxing feature on a MFD, as long as the method is supported by the "Session Logon" feature of the the eCopy ShareScan software (to push to XMediusFAX the information returned by the method).

Note: For more information, see the eCopy ShareScan Administration Console documentation.

Once those points have been verified, you must:

1. Configure the Session Logon feature within the eCopy ShareScan Administration Console.
2. Make sure to select `Session Logon` as **User Authentication Method** when you will configure the connector.

The attribute returned by the authentication method will always be the SMTP address of the authenticated user (directly or through some lookup). XMediusFAX will then be able to manage this attribute without requiring any other configuration – in addition to the ones you should have already performed for Directories Integration.

For more information, see the XMediusFAX *Administration Guide*.

Configuring the XMediusFAX eCopy ShareScan Connector

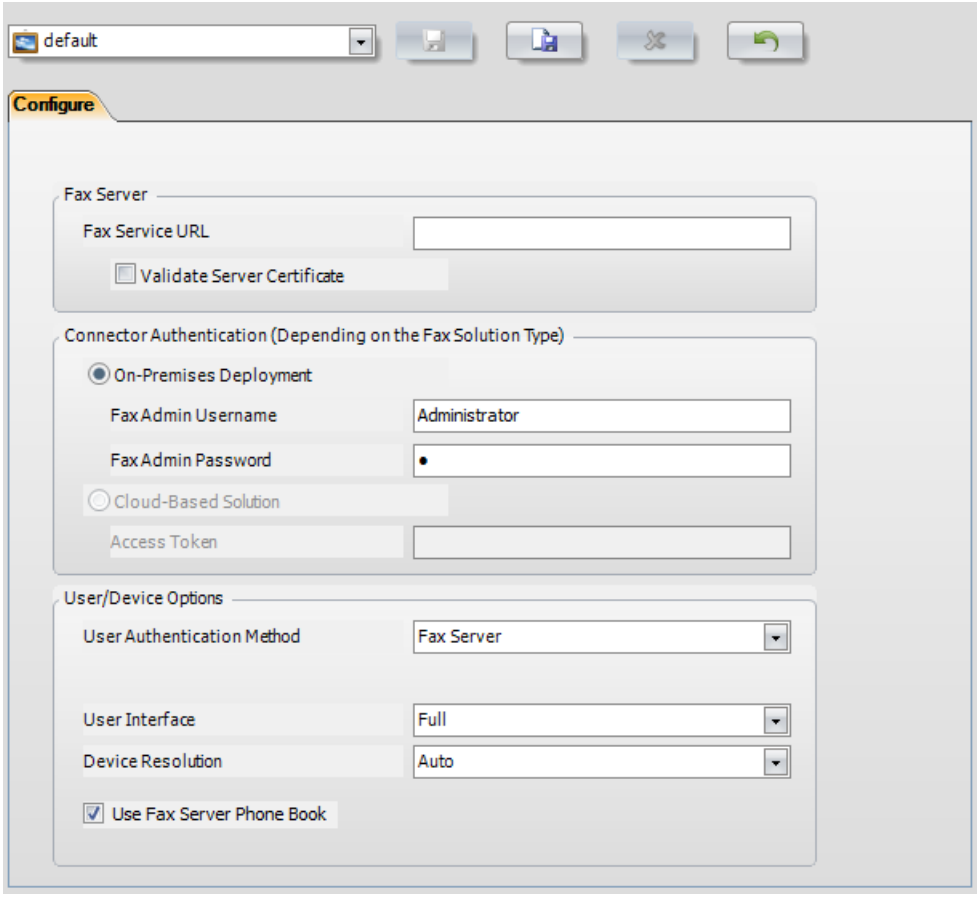
Important: Before starting, please be aware of all information you should have collected:

- XMediusFAX host connection settings (according to the fax solution type you are using).
- Fax users authentication method choice (see *Fax Users Authentication* on page 8).

To configure XMediusFAX eCopy ShareScan Connector (within the eCopy ShareScan software):

1. Launch the **eCopy ShareScan Administration Console**.
2. Select the **Connectors** tab at the bottom of the left pane.
3. Select **XMediusFAX** in the left pane.

   Note: You may first need to refresh the list of connectors (right-click in the list and select **Refresh Connectors**).



4. Enter the XMediusFAX eCopy ShareScan Connector configuration settings (for the settings profile selected at the top-left of the screen):

   Note: You can have several settings profiles (in addition to the "default" profile) if you are planning to use the XMediusFAX eCopy ShareScan Connector on several MFDs with different settings.

   a) **Fax Server**

Control	Description
Fax Service URL	• **For configuration with on-premises deployment:** The URL used to reach the on-premises XMediusFAX host, which must be entered in the form: `https://<ServerName_or_IP>:8443` • **For configuration with cloud-based solution:** The URL to connect to the cloud-based solution.
Validate Server Certificate (optional)	Enables an additional security for the Web Service connection to XMediusFAX, by validating the server identity. **Note:** This requires a certificate from the XMediusFAX host (see *Installing the XMediusFAX Certificate (Optional)* on page 5). **Important:** If you are using this option, the <*ServerName_or_IP*> in **Fax Service URL** field must match the Common Name (CN) of the certificate.

   b) **Connector Authentication (Depending on the Fax Solution Type)**

Note: The selection is automatically done according to the entered **Fax Service URL** (see above). Authentication parameters must be accordingly entered.

Control	Description
On-Premises Deployment	Connector authentication mode used for **on-premises deployment** only. Parameters: **Fax Admin Username**/**Fax Admin password** (the name and password of a valid administrator account of XMediusFAX).
Cloud-Based Solution	Connector authentication mode used for **cloud-based solution** only. Parameter: **Access Token**. **Note:** The **Access Token** must have the following permission types: • **Query user directory** • **Send and manage faxes** To create and retrieve such a token, go to **Access Tokens** from the navigation bar of your cloud faxing service portal.

c) **User/Device Options**

Control	Description
User Authentication Method	The authentication mode for fax users: • `Default User` (no authentication) – Forces the Connector to use a default fax user account as fax sender (rather than the currently logged user, if any). This requires to enter an existing **User ID** that will be used by all users of the MFD. • `Fax Server` – Enables an authentication method directly based on internal user accounts of XMediusFAX. • `Session Logon` (for other authentication method) – Relays the management of authentication methods to the eCopy ShareScan software (requires configuration in the related section of the eCopy ShareScan Administration Console – see its documentation). **Remember:** You may also need to adjust some settings on your XMediusFAX according to the choice you made here. For more details, see section: *Fax Users Authentication* on page 8.
User Interface	The type of user interface to be used by default on the MFD: `Full` (all composition fields) or `Basic` (fax number only).
Device Resolution	The resolution level of the MFD screen. Setting used to adjust the user interface display to fit the actual resolution of the MFD screen. Two ranges of resolutions are supported (`Auto` by default): • `Low`: less than 480 as screen height. • `High`: 480 and higher as screen height.
Use Fax Server Phone Book	Allows fax users to benefit from XMediusFAX phone book features when sending faxes on the MFD (enabled by default).

5. Save the settings for the selected profile.
6. Repeat the steps for additional profiles, if needed.

Important: After this configuration, you still need to enable the XMediusFAX eCopy ShareScan Connector on all MFDs that you have targeted to use it. See *Configuring a MFD to Use the XMediusFAX eCopy ShareScan Connector* on page 14.

Configuring a MFD to Use the XMediusFAX eCopy ShareScan Connector

At least one profile of settings for the XMediusFAX eCopy ShareScan Connector must have been previously configured within the **eCopy ShareScan Administration Console**. See *Configuring the XMediusFAX eCopy ShareScan Connector* on page 11.

To enable the XMediusFAX eCopy ShareScan Connector on a MFD:

1. Launch the **eCopy ShareScan Administration Console** (if not already done).
2. Select the **Devices** tab at the bottom of the left pane.
3. Select in the left pane the MFD you want to configure.
4. Locate the **XMediusFAX** connector in the list at the right and select a profile of settings according to the configurations previously done at the connector level.
5. Save the device settings.
6. Repeat all these steps for each MFD you want to configure.

The XMediusFAX faxing feature is now ready to be used on all concerned MFDs.

Chapter 5 Debugging

Debugging the XMediusFAX eCopy ShareScan Connector

If you encounter issues with the XMediusFAX eCopy ShareScan Connector, you can have access to some debugging information within the eCopy ShareScan software logs for troubleshooting purpose with XMediusFAX technical support.

Tracing with eCopy ShareScan

To setup the logs within the **eCopy ShareScan Administration Console**, select the **Services** tab at the bottom of the left pane, and then the **Tracing** node in the left pane.

👉 **Important:** The **Verbose** option must be enabled to have the XMediusFAX eCopy ShareScan Connector log entries written.

For more information on Tracing configuration and to know where the logs can be viewed, please refer to the eCopy ShareScan Administration Console documentation.

The XMediusFAX eCopy ShareScan Connector Traces

Within the logs, you can search for `XMediusFAX` to retrieve messages in relation with the XMediusFAX eCopy ShareScan Connector.

Chapter 6 Uninstallation

Uninstalling the XMediusFAX eCopy ShareScan Connector

To properly uninstall the XMediusFAX eCopy ShareScan Connector:

1. Exit the **eCopy ShareScan Administration Console** if it is open.
2. On the computer hosting the XMediusFAX eCopy ShareScan Connector, access the Add/Remove Programs feature.
3. Select **XMediusFAX eCopy ShareScan Connector** and click **Remove**.

Chapter 7 Appendix

Generating a New Certificate Container (If Required)

This procedure will allow you to generate a new valid certificate container (also called keystore) on the XMediusFAX host in order to install and trust it on the computer hosting the XMediusFAX eCopy ShareScan Connector. Follow this procedure only in case you would need to enable the certificate validation (for additional security) and you would not use the one generated by default during the XMediusFAX installation.

⚠ **Attention:** This operation must be performed on the XMediusFAX host and implies some configuration to be done on the XMediusFAX host itself in order for it to trust the newly generated certificate. Please follow carefully the procedure below.

👉 **Note:** The certificate that you are going to generate here is a self-signed certificate; however, you could decide to use a certificate signed by an official authority. In both cases, the `CN` parameter of the certificate must match the string that will be used from the client side (the XMediusFAX eCopy ShareScan Connector) to reach the XMediusFAX host.

On the XMediusFAX host:

1. Create a new keystore containing a single self-signed Certificate:

a) Execute the following command line:

```
[java_home]/bin/keytool -genkey -alias tomcat -keyalg RSA -validity 9125 -keystore
 keystore.jks
```

👉 **Note:** You can give the keystore another name than `keystore.jks`, as long as you respect the `.jks` extension and you adjust all the following steps in accordance with the name you entered in this command line.

b) As requested by the prompt, enter a `password` for the keystore.

👉 **Note:** Keep this password in mind, it will be required later in this procedure.

c) For `first and last name`, enter the *Common Name* (CN) of the XMediusFAX host.

👉 **Important:** This entry corresponds to the `CN` parameter of the certificate; it must imperatively match the string that will be used from the client side to reach XMediusFAX (the value will be checked at each connection attempt to the Web Services).

For example, if you enter here `myfaxserver`, ensure that the same string:

- is one of the names that will resolve to the IP address of the XMediusFAX host, and
- is the name that will be used to reach XMediusFAX from the client side.

d) Follow the prompt to enter the other general information:

- `Organizational unit`
- `Organization`
- `City`
- `State or province`
- `Two-letter country code`

After entering all this information, you will be prompted for confirming the entered values (`CN=`*`fax_server_common_name`*`, OU=`*`organizational_unit`*`, O=`*`organization`*`, L=`*`city`*`, ST=`*`state_or_province`*`, C=`*`country_code`*).

e) Enter a password for the key, which is the specific password for this Certificate (as opposed to any other Certificates stored in the same keystore file).

Important: You MUST use the same password here as was used for the keystore password itself (actually, the keytool prompt will tell you that pressing the ENTER key does this for you automatically).

Note: The `keystore.jks` is now generated. However, you must finish the current procedure in order for this keystore to be trusted by XMediusFAX.

2. Put a copy of the `keystore.jks` file in the *`[tomcat_home]`*`/conf` folder of the XMediusFAX host.
3. Edit the Tomcat configuration file:
   a) Open the `server.xml` file located in the *`[tomcat_home]`*`/conf` folder and search for the HTTPS connector definition tag:

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<Connector port="8443" maxHttpHeaderSize="8192"
           maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
           enableLookups="false" disableUploadTimeout="true"
           acceptCount="100" scheme="https" secure="true"
           clientAuth="false" sslProtocol="TLS"
           keystoreFile="conf/keystore.jks" keystorePass="changeit"/>
```

   b) Verify that the `keystoreFile` parameter contains the value `conf/keystore.jks`.
   This is the (relative) path to the keystore file you just created.
   c) Change the value of the `keystorePass` parameter for the password you entered during the creation of the keystore file.
   d) Save the file.
4. Restart the **Apache Tomcat** service to enable your changes.

The generated certificate container will now be trusted by XMediusFAX.

Remember: To install the certificate on the XMediusFAX eCopy ShareScan Connector host, see: *Installing the XMediusFAX Certificate (Optional)* on page 5.

Administration Guide
Noncontractual document

253566346

XMedius Solutions Inc.
3400, boul. de Maisonneuve Ouest - Bureau 1135
Montréal, Québec H3Z 3B8 - Canada
www.xmedius.com