XMedius

WWW.XMEDIUS.COM

XMediusFAX Ricoh ESA Connector 11.0.0

Administration Guide

XMediusFAX Ricoh ESA Connector

Version Number 11.0.0.42 – April 2016.

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).

• Ksoap2 and Kxml:
Copyright © 2006, James Seigel, Calgary, AB., Canada
Copyright © 2003,2004, Stefan Haustein, Oberhausen, Rhld., Germany

• Log4J:
Copyright © 2000-2002 The Apache Software Foundation

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.

References to other products or software imply no warranty of the XMediusFAX Ricoh ESA 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
31-33, rue des Beaux Soleils
95520 Osny – France

• Telephone: +33 (0) 1 57 61 30 54
• Fax: +33 (0) 9 70 26 19 22

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 30 17 90 43
• 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 57 61 30 20

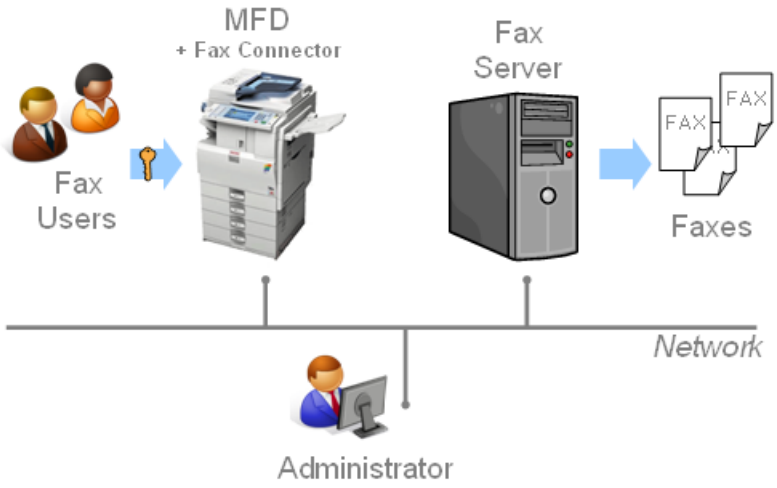
Table of Contents

Chapter 1 Introduction

The XMediusFAX Ricoh ESA Connector

The XMediusFAX Ricoh ESA Connector is a solution allowing Ricoh Multi-Function Devices (MFDs) that are compatible with the Ricoh ESA (Embedded Software Architecture) technology to fax documents through XMediusFAX.

Here is an example of deployment including an MFD (with the XMediusFAX Ricoh ESA Connector installed) and XMediusFAX:



Note: More than one MFD connected to the network can benefit from the XMediusFAX Ricoh ESA 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 Ricoh ESA Connector files (and all other required items) on a single computer (for later deployment on the MFDs).

- Configure and deploy the XMediusFAX Ricoh ESA Connector on MFDs in order for them to have the faxing feature enabled.

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.

Administrator's PC

The “administrator's PC” is the computer where the XMediusFAX Ricoh ESA Connector files will be installed for later deployment to one or several MFDs.

This computer must:

- Have the Java Runtime Environment 7 (JRE 7) installed.
- Have network access to communicate with your MFDs.

👉 **Note:** In case you need to access MFDs debugging information from this computer, a Remote Shell (rsh) client application must be installed – for example, the rsh.exe utility available for Microsoft Windows.

Multi-Function Devices (MFDs)

All MFDs on which you will deploy the XMediusFAX Ricoh ESA Connector must:

- Use Ricoh's Embedded Software Architecture (ESA), version 10.x, 11.x or 12.x.
- Have a panel screen with a resolution of µWVGA, WVGA or SVGA.
- Be reachable from the administrator's PC.
- Have network access to XMediusFAX.

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

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

However, If you wish to use other authentication methods (including single sign-on methods), your MFD can integrate with Ricoh's CAP or with AAA (using an appropriate AAA provider).

For more information about AAA integration and AAA providers, please contact your MFDs reseller.

👉 **Note:** Some Ricoh MFD models do not support auto-detection features (originals remaining on the exposure glass, original size auto-detection) used by default by the XMediusFAX Ricoh ESA Connector,

which makes the Connector unable to scan documents on these MFDs. This issue can however be solved via a workaround procedure: follow the instructions in KB Article #314106 (see *support.xmediusfax.com*).

Fax Server (XMediusFAX)

The XMediusFAX Ricoh ESA 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 your MFDs.
- Your XMediusFAX licence must include:
  - The Web Services feature.
  - The maximum number of MFDs that are allowed to use the XMediusFAX Ricoh ESA Connector.
- 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	Web Service (faxservice.war) 6.5.5.310
XMediusFAX 7.0.0	Web Service (faxservice.war) 7.0.0.360
XMediusFAX 7.5.0 and higher	No specific hotfix required.

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

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

Chapter 3 Deployment Tool Installation

Connector Deployment Tool Installation Overview

This chapter provides:

- The list of all items required to perform a full installation of the Connector.
- The steps to follow for installing the Connector files and Deployer on the administrator's PC (before configuring and deploying the Connector to the concerned MFDs – described in the next chapter).

Important: The XMediusFAX Ricoh ESA Connector has been designed for installation on MFDs using the deployment tool provided in the XMediusFAX Ricoh ESA Connector installation package. It is not recommended to use other methods to deploy the XMediusFAX Ricoh ESA Connector on MFDs. If however your environment requires the use of another method, you may contact our Professional Services team to help you find a solution.

Connector Installation Planning

To install the XMediusFAX Ricoh ESA Connector, the following items are required.

XMediusFAX Ricoh ESA Connector Files and Deployment Tool Installer

The XMediusFAX Ricoh ESA Connector package is composed of several files that will be installed – through a single installer – on the administrator's PC. It includes:

- A Deployer (utility software) that will be used to configure and deploy the Connector to the concerned MFDs.
- All Connector files required for the deployment.

XMediusFAX Web Services Certificate Container (Keystore) – Optional

The XMediusFAX Ricoh ESA 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. For this, a valid certificate container from the XMediusFAX host (keystore file with `.jks` extension) is required among the Connector files.

Note: A default keystore is available on the XMediusFAX host (generated during XMediusFAX installation): *[tomcat_home]*\conf\keystore.jks. It is ready to be used and should work properly in your faxing environment; it includes the XMediusFAX host name and its password is “changeit”.

However, if you wish to generate a new keystore to replace the default one (for example for adjusting the Common Name or for changing the password), a procedure is given in this guide (*Generating a New Certificate Container (If Required)* on page 25).

Installing the XMediusFAX Ricoh ESA Connector Files and Deployer

Attention: This installation must be performed on the administrator's PC from which the XMediusFAX Ricoh ESA Connector will be later deployed to the MFDs.

To install the XMediusFAX Ricoh ESA Connector (files and Deployer):

1. Launch the XMediusFAX Ricoh ESA Connector deployer installer: `Setup.exe`.

2. Simply follow the instructions of the installer.
   All files are installed by default in `C:\Program Files\XMediusFAX Ricoh ESA Connector\` (referenced as *[Connector_Install_Path]* in this document).
3. Install the Certificate (optional):
   a) Retrieve the Web Services certificate container from the XMediusFAX host (only if you need to enable a validation of the server identity):

      `keystore.jks`

      Note: For more information, see *Connector Installation Planning* on page 5.

   b) Copy and paste it to the following location on the administrator's PC:

      [Connector_Install_Path]\keystores

The installation is now complete and you can configure and deploy the Connector (see: *Fax Connector Configurations and Deployment – Overview* on page 9).

Upgrading the XMediusFAX Ricoh ESA Connector Deployer

Major Upgrades

To upgrade the XMediusFAX Ricoh ESA Connector Deployer from a previous major version (for example from version 10 to version 11), just launch the installation program of the new version (`Setup.exe`) and follow the on-screen instructions.

Attention: Please remember that the upgrade to the current version of the deployer can only be performed from version 10.0 minimum. Older versions of the deployer are not eligible for such an upgrade.

Minor Upgrades (Hotfixed Versions)

To upgrade the XMediusFAX Ricoh ESA Connector Deployer between two minor versions (for example from version 11.0.0.x to version 11.0.0.y), you need first to uninstall the current version (using Add/Remove Programs) and then install the new version (using its installation program).

Attention: Do not delete the remaining folders, they contain your current configurations (which will be used by the new version).

Connector Upgrade on MFDs

To be able to upgrade the XMediusFAX Ricoh ESA Connector on your MFDs, you must first upgrade the deployer by following the above instructions. Once done, you will need to redeploy the connector on all concerned MFDs (see *Managing the List of MFDs in the Deployer (Including Connector Upgrade)* on page 18).

Chapter 4 Fax Connector Configurations and Deployment

Fax Connector Configurations and Deployment – Overview

Before being able to send faxes with MFDs using the XMediusFAX Ricoh ESA Connector, you must configure and deploy the connector to each concerned MFD.

This chapter covers the following subjects:

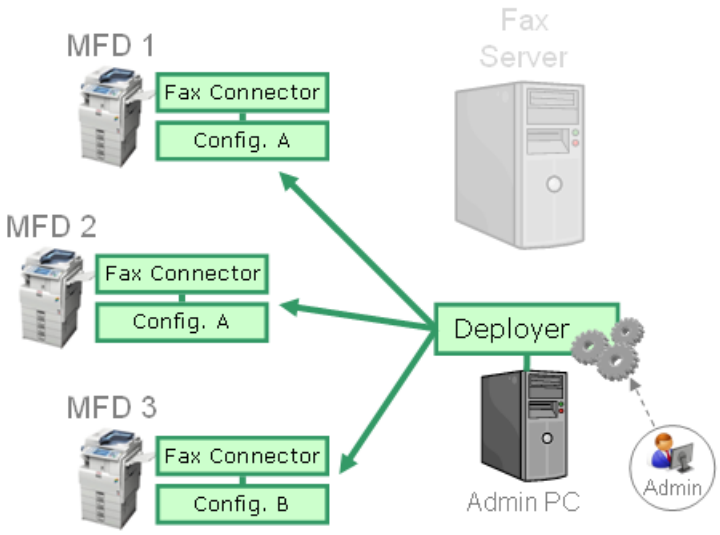
- Information on the way the faxing feature will be deployed on your MFDs.
- Information on fax users authentication, with description of the various methods that can be used
- The procedures to configure your faxing environment according to the authentication method that is used.
- The procedure to configure and deploy the XMediusFAX Ricoh ESA Connector to the concerned MFDs, using the provided Deployer.

Note: Before starting, you must have first installed the XMediusFAX Ricoh ESA Connector files and the Deployer on the administrator's PC (see *Installing the XMediusFAX Ricoh ESA Connector Files and Deployer* on page 6).

About XMediusFAX Ricoh ESA Connector Deployment

A Deployer (utility software) is available among the files that have been installed on the administrator's PC during the Connector installation.

This Deployer allows you to configure and install the XMediusFAX Ricoh ESA Connector simultaneously on all concerned MFDs.



Note: You can decide to have different configuration settings depending on the MFD where the connector will be installed. This can be justified depending on the way you would like the fax users to be authenticated on each MFD.

Fax Users Authentication

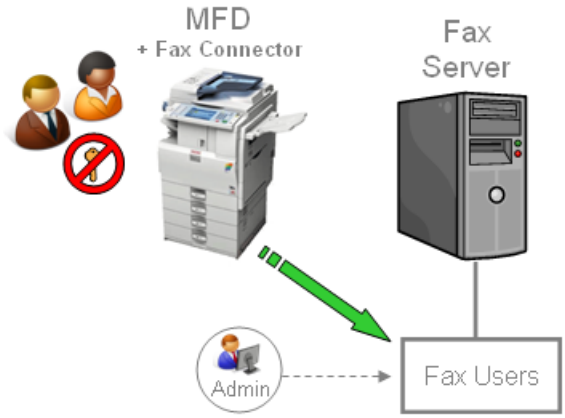
The way users will be authenticated in order to use the faxing feature are multiple and largely depend on your company architecture and policies.

Note: For technical reasons, this section should be preferably considered prior to deploying the XMediusFAX Ricoh ESA Connector on your MFDs.

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 such as Active Directory or other single sign-on authentications (implying use and configuration of the AAA software)

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 Ricoh ESA Connector configuration settings:

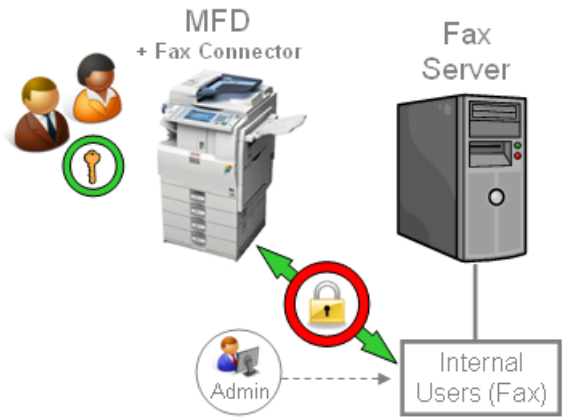
1. From the XMediusFAX administration interface, configure XMediusFAX to include a user that you will dedicate to the MFD.

   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 Ricoh ESA 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:

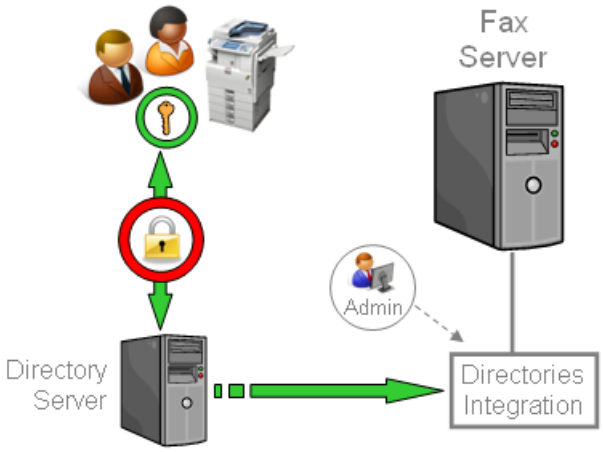
1. From the XMediusFAX administration interface, add all required fax user accounts to the list of **Internal Users**, according to the procedure given in the XMediusFAX *Administration Guide*.

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

2. When you will configure the XMediusFAX Ricoh ESA 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. More precisely, the XMediusFAX Ricoh ESA Connector can be configured to authenticate users:

- Through **Ricoh's Card Authentication Package (CAP)** – which requires to be previously configured (according to Ricoh's documentation), or
- Using any **AAA-compliant method** – which requires to be previously configured and deployed (AAA server and an appropriate AAA provider for the MFD to push to XMediusFAX the information returned by the method).

According to the solution used:

1. You must ensure to select the appropriate **User Authentication Method** (`CAP` or `AAA`) when you configure the connector before deploying it.
2. Depending on which type of attribute is returned by the authentication method (SMTP address, NT account or any other attribute), you may need to perform additional configurations on XMediusFAX (see below).

SMTP Address or NT Account Returned

If the authentication method returns an SMTP address for the authenticated user (directly or through some lookup), or a full NT Account (including the domain name), then XMediusFAX will 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 XMediusFAX *Administration Guide*.

Other Attribute Returned

If the authentication method returns an attribute that is neither an SMTP address nor a full NT account, XMediusFAX will consider it by default as an NT account.

In this case, you should adjust the way the Directories Integration is managed in XMediusFAX, in order to link the returned attribute with an actual user having faxing rights (example below).

Example: Single Sign-On with Card Reader (ID Number Returned)

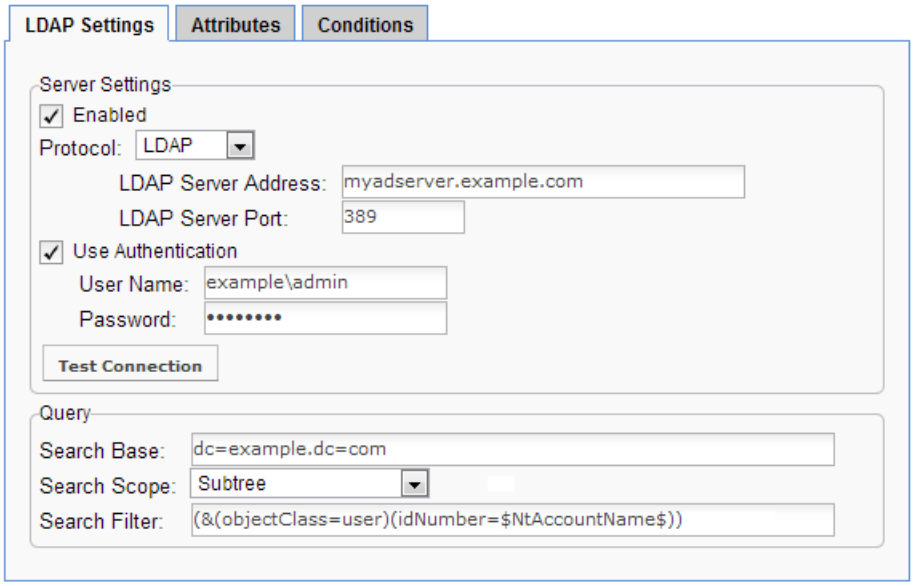
Let's consider the following scenario example:

- The MFD is configured to permit single sign-on.
- Users are accessing the MFD features using a personal card they scan with a card reader.
- The authentication method returns an ID number corresponding to the user.
- On the user directory side, this ID number is stored for each user under an attribute named `idNumber`.

In this precise case, you should create an additional **LDAP Directory** rule in the XMediusFAX **Directories Integration**, in order for the returned ID number (considered as an NT account) to match the `idNumber` attribute in your users directory. In this rule, the **Search Filter** of the **Query** can be for example:

```
(&(objectClass=user)(idNumber=$NtAccountName$))
```

In the XMediusFAX administration interface, the rule definition will look like this:



Remember: This rule – specifically used for resolving the ID number – should be created in addition to the existing Directories Integration rules, which will continue to fill their usual duties (please see XMediusFAX *Administration Guide* for more details on Directories Integration).

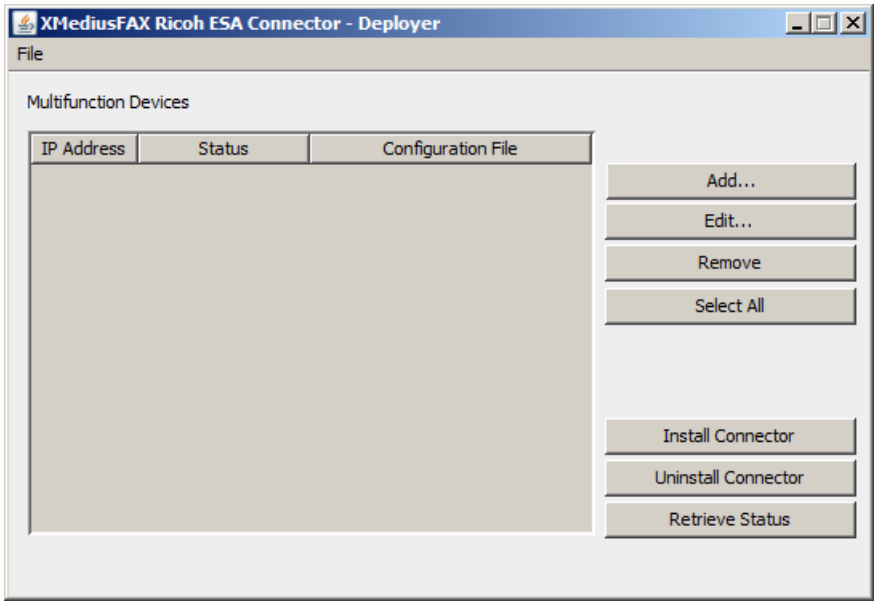
Configuring and Deploying the XMediusFAX Ricoh ESA Connector

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

- All IP addresses of the MFDs on which you are going to deploy the XMediusFAX Ricoh ESA Connector.
- Fax Server and Web Services connection settings (according to the computer hosting your XMediusFAX).
- Fax users authentication method choice (see *Fax Users Authentication* on page 10).

To configure and deploy the XMediusFAX Ricoh ESA Connector:

1. Launch the Deployer by selecting **XMediusFAX Ricoh ESA Connector ➤ Fax Connector Deployer** among your installed applications.

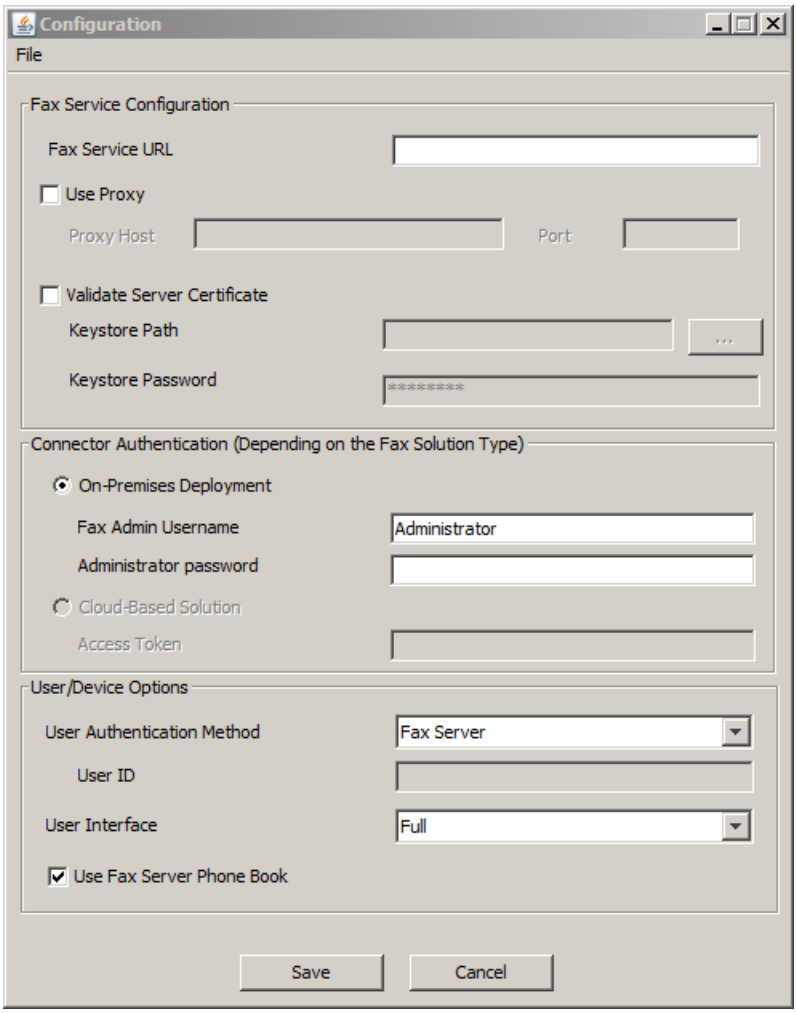


2. Create configuration files for the Connector:

   Note: These files will be applied later to one or several MFDs. You can have one single configuration file for all MFDs, or even have a different configuration file for each MFD, if needed.

   a) Select **File ➤ New Configuration**.

      Note: If you had previously saved a configuration file, you can edit it instead of starting from an empty one (**File ➤ Edit Configuration**).



b) **Fax Service Configuration**

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.
Use Proxy	Enables the use of a proxy to connect to the XMediusFAX server. Parameters: **Proxy Host/Port** (the hostname or IP address of the proxy and its port).
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 *Connector Installation Planning* 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.

Control	Description
	Parameters: **Keystore path**/**Keystore password** (the path and the password of the certificate container).

c) **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.

d) **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. • `CAP` – Enables authentication through Ricoh's Card Authentication Package (CAP). • `AAA` (for other authentication methods) – Relays the management of authentication methods to the MFD (requires configuration in the related section of the MFD settings – 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 10.
User Interface	The type of user interface to be used by default on the MFD: `Full` (all composition fields) or `Basic` (fax number only).
Use Fax Server Phone Book	Allows fax users to benefit from XMediusFAX phone book features when sending faxes on the MFD (enabled by default).

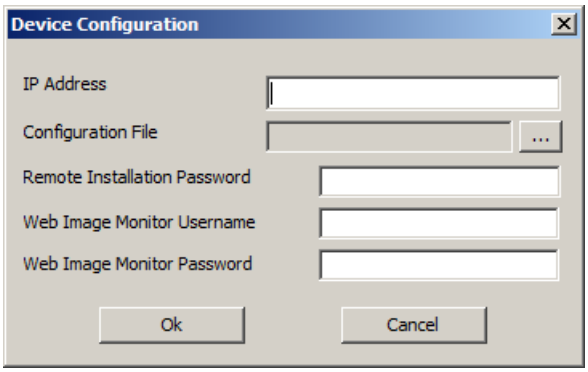
e) Click **Save**.

f) Give the configuration file an easily recognizable name (in case of multiple configurations) and save it.

> **Note:** If you cannot save the configuration file in the current directory (e.g. if permission is denied), you can still save it elsewhere, without any consequence for the deployment.

g) Repeat these substeps if you need to create other configuration files.

3. Add all concerned MFDs to the deployment list:
   a) Click **Add**.



   b) Enter the **IP address** of the MFD.
   c) Associate a **Configuration file** to this MFD (with the browse button).
   d) If required, adjust the authentication parameters according to your MFD settings:

Control	Description
Remote Installation Password	Fill-in this field only if your MFD is configured with a password to control remote installations. **Note:** This password may have been set via the **Web Image Monitor** of this MFD: **Device Management ➤ Configuration ➤ Extended Feature Settings ➤ Administrator Tools ➤ Web Service Settings**.
Web Image Monitor Username	Username and password of the account used to access the **Web Image Monitor** interface (Web page) of this MFD. **Note:** If you never changed the default login account of the Web Image Monitor for this MFD (username "admin" and blank password), you can leave these fields blank.
Web Image Monitor Password	

   e) Validate and repeat these substeps for each MFD.

> **Note:** The **Device Configuration** screen keeps in memory the last configuration file you selected; this will help you if you are going to associate the same configuration to several MFDs. However, you can still select another configuration file.

4. Verify and adjust (if needed) your list of MFDs before deployment:
   a) Select the MFDs to which you are going to deploy the Connector (this can be a partial selection, or a full selection with **Select All**).
   b) Click **Retrieve Status** for verifying the installation status and version of the connector on the selected MFDs.

> **Tip:** This will allow you to check if the MFDs are reachable with the entered IP addresses and if some of them have the Connector already installed from a previous installation.

   c) You can adjust the list and configuration of MFDs using the **Edit** or **Remove** buttons (on single or multiple selections).

5. Deploy the Connector:

a) Select the MFDs to which you are going to deploy the Connector.
b) Click **Install Connector** to deploy the configured Connector to the selected MFDs.

After the deployment, a summary displays the connector installation status (successful or not) for each MFD.

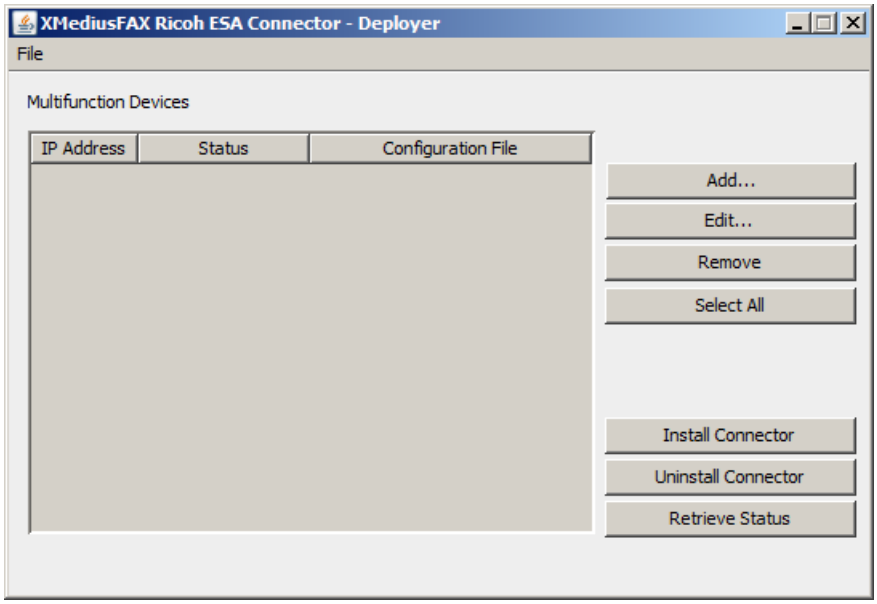
The faxing feature is now ready to be used on all concerned MFDs.

Note: The Deployer will remember the list of IP addresses and the configuration files associations after you close it, in case you would need to perform the deployment again (for example for configurations changes purpose).

Remember: You may need to adjust some settings on your XMediusFAX according to the choice you made for authenticating the users on each MFD (according to section: *Fax Users Authentication* on page 10).

Managing the List of MFDs in the Deployer (Including Connector Upgrade)

Launch the Deployer by selecting **XMediusFAX Ricoh ESA Connector ➤ Fax Connector Deployer** among your installed applications.



The main screen displays the list of all MFDs you already registered in the deployer, each with their main properties and their status regarding the XMediusFAX Ricoh ESA Connector installation. All the beside buttons allow you to manage the list: for example, to edit the settings of an MFD, to redeploy an updated version of the connector configuration file to an MFD, or to upgrade the version of the XMediusFAX Ricoh ESA Connector already installed on an MFD.

MFD List

Column	Description
IP Address	The IP address of the MFD.

Column	Description
Status	The XMediusFAX Ricoh ESA Connector version and installation status on this MFD. **Note:** To know the current status, you may need to use the **Retrieve Status** button.
Configuration File	The XMediusFAX Ricoh ESA Connector configuration file associated to this MFD (see *Configuring and Deploying the XMediusFAX Ricoh ESA Connector* on page 14 for more information on configuration file creation).

List Actions

All the actions described below are available for single or multiple MFD selection (except for adding a new MFD):

Button	Description
Add	To add a new MFD to the list (see *Configuring and Deploying the XMediusFAX Ricoh ESA Connector* on page 14 for more information on MFD settings).
Edit	To edit the settings of the selected MFD. **Note:** Multiple selection allows to quickly associate the same connector configuration file to several MFDs.
Remove	To remove the selected MFD.
Select All	Selects all the MFDs of the list.
Install Connector	Deploys the XMediusFAX Ricoh ESA Connector on the selected MFD with the configuration file associated to this MFD. **Note:** If a previous version of the XMediusFAX Ricoh ESA Connector is already installed, the deployer will automatically proceed to an upgrade to the current version. Remember that the versions of the XMediusFAX Ricoh ESA Connector older than 10.0 are not eligible for such an upgrade.
Uninstall Connector	Uninstalls the XMediusFAX Ricoh ESA Connector from the selected MFD (see *Uninstalling the XMediusFAX Ricoh ESA Connector* on page 23 for more general details about uninstallation).
Retrieve Status	Retrieves the XMediusFAX Ricoh ESA Connector version and installation status (**Status** column) for all listed MFDs.

Chapter 5 Debugging

Debugging the XMediusFAX Ricoh ESA Connector on MFDs

If you encounter issues with the XMediusFAX Ricoh ESA Connector on an MFD, you can have access to some debugging information for troubleshooting purpose with your XMediusFAX reseller's technical support.

There is no permanent logging of this information (no log file), however you can display it “live” using the Remote Shell (rsh) protocol. You will need an rsh-capable application, like the rsh.exe utility available for Microsoft Windows.

From the administrator's PC (for example), execute the following command line:

```
rsh [mfd_ip] mmesg_auto 125
```

👉 **Note:** This command lists output information from all applications that are installed on the MFD whose IP address *[mfd_ip]* has been entered.

Information lines about the XMediusFAX Ricoh ESA Connector can be easily identified as they all start with: `[stdout] [FaxServerXlet].`

👉 **Tip:** The on-screen view gives only access to a limited number of lines; if you wish to log information on a longer period, you can write it to a file instead of viewing it directly on the screen. For example:

```
rsh [mfd_ip] mmesg_auto 125 >> C:\mfd01-log.txt
```

Chapter 6 Uninstallation

Uninstalling the XMediusFAX Ricoh ESA Connector

To properly uninstall the XMediusFAX Ricoh ESA Connector:

1. Uninstall the XMediusFAX Ricoh ESA Connector from all concerned MFDs:
   a) Launch the Deployer by selecting **XMediusFAX Ricoh ESA Connector ➤ Fax Connector Deployer** among your installed applications.
   b) Select in the list the MFDs from which you need to remove the XMediusFAX Ricoh ESA Connector.
   c) Click **Uninstall Connector**.

   After the uninstallation, a summary displays the connector uninstallation status (successful or not) for each MFD.
2. Uninstall all Connector files and Deployer from the administrator's PC:

   Note: This step is optional and should be applied only if:

   - You uninstalled the XMediusFAX Ricoh ESA Connector from all your MFDs, and
   - You are not planning to deploy the XMediusFAX Ricoh ESA Connector on other MFDs.

   a) On the administrator's PC, access the Add/Remove Programs feature.
   b) Select **XMediusFAX Ricoh ESA 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) to be used on the MFDs by the XMediusFAX Ricoh ESA Connector, in case you would need to use a keystore (for additional security) and you would not use the one generated by default during XMediusFAX installation.

⚠ **Attention:** This operation must be performed on the XMediusFAX host and implies some configuration to be done on XMediusFAX 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 Fax Connector) to reach XMediusFAX.

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 and also for configuring the XMediusFAX Ricoh ESA Connector in the next chapter.

   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 generated `keystore.jks` file is the one you will need to complete the XMediusFAX Ricoh ESA Connector installation. However, you must finish the current procedure in order for this keystore to be trusted by the XMediusFAX host.

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.

You can now make a copy of the same `keystore.jks` file to make it available on the administrator's PC.

Administration Guide
Noncontractual document

253581806

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