XMedius

WWW.XMEDIUS.COM

XMediusFAX App 1.0

for Ricoh Smart Operation Panel enabled MFPs

Administration Guide

XMediusFAX App for Ricoh Smart Operation Panel enabled MFPs

Version Number 1.0.0.271 – May 2018.

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

Disclaimer

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 App for Ricoh Smart Operation Panel

The XMediusFAX App for Ricoh Smart Operation Panel is a solution allowing Ricoh Multi-Function Devices (MFDs) that are compatible with the Ricoh Smart Operation Panel technology to fax documents through XMediusFAX (On-Premises Server or Cloud Service).

XMediusFAX App Features

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

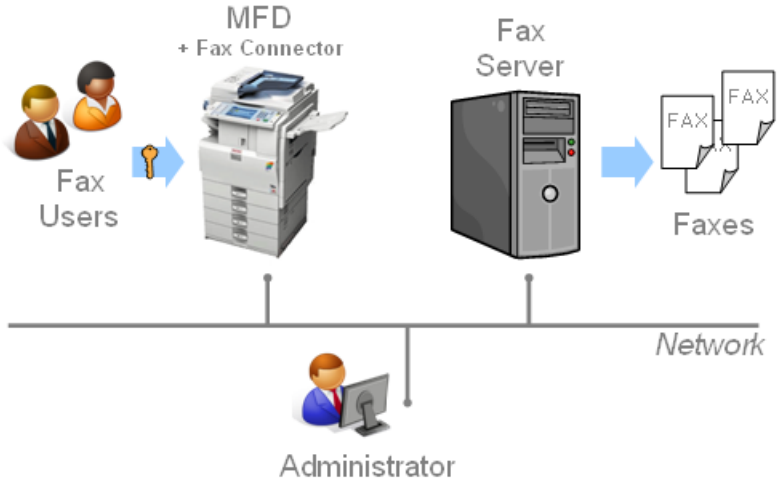
Several methods for authenticating the users of the XMediusFAX App on the MFDs can be configured in order to meet specific needs.

XMediusFAX App Environment Overview

The XMediusFAX App is designed to be installed (embedded) on the MFD, from which it will directly communicate with the XMediusFAX server (or cloud service).

To install the XMediusFAX App on MFDs, it is first needed to install a centralized deployment tool on a computer that has access to the MFDs through the network. This deployment tool allows to address multiple MFDs with different configurations of the same XMediusFAX App to fit heterogeneous needs across the MFD fleet.

Here is an example of on-premises deployment with one MFD:



Purpose of This Document

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

- Install the XMediusFAX App deployer on a centralized computer of the network, and
- Configure and deploy the XMediusFAX App on MFDs.

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

Additional Information and Documentation

XMediusFAX App User Instructions

A *User Instruction Sheet* is available within the XMediusFAX App distribution package, in all languages supported by the App.

It is intended for the end-users of the XMediusFAX App on the MFD and consists of a single printable page that describes all basic actions that a user can perform with the App.

Documentation Download

The User Instructions and the Administration Guide (this document) are available in several languages and their latest versions are downloadable from the XMedius Software Help Center:
https://support.xmediusfax.com/hc/en-us/articles/115005615766

XMedius Web Site

For more information about XMedius products and services including the XMediusFAX App, visit the site: *www.xmedius.com*.

Chapter 2 Installation Requirements

Installation Requirements

👉 **Important: Before you start**, please read this section carefully to verify if your current environment is consistent with the XMediusFAX App requirements.

Administrator's PC

The “administrator's PC” is the computer where the XMediusFAX App Deployer will be installed in order to further deploy the XMediusFAX App to one or several MFDs.

This computer must:

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

Multi-Function Devices (MFDs)

Any MFDs on which you will deploy the XMediusFAX App:

- Must be compliant with Ricoh Smart Operation Panel technology
- Must be reachable from the administrator's PC.
- Must have access to XMediusFAX:
  - Via the network for an On-Premises Server, or
  - Via Internet for the Cloud Service.

👉 **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 App.

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

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

Fax Server (XMediusFAX)

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

XMediusFAX Cloud Service

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

XMediusFAX On-Premises Server

- XMediusFAX must be properly installed and running on a server accessible from your MFDs.
- Your XMediusFAX license must include:
  - The Web Services feature.
  - The maximum number of MFDs that are allowed to use the XMediusFAX App.
- 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

Deployer Installation Overview

This chapter provides:

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

👉 **Important:** The XMediusFAX App has been designed for installation on MFDs using the deployment tool provided in the XMediusFAX App installation package. It is not recommended to use other methods to deploy the XMediusFAX App 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.

XMediusFAX App Installation Planning

To install the XMediusFAX App, the following items are required.

XMediusFAX App Deployment Tool Installer

The XMediusFAX App package includes a Deployer (utility software) that will be used to configure and deploy the XMediusFAX App to the concerned MFDs.

XMediusFAX Web Services Certificate Container (Keystore) – Optional

The XMediusFAX App 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.

If you are using the XMediusFAX On-Premises solution, a valid certificate is required on your XMediusFAX server. If this certificate is self-signed (i.e. not signed by a trusted certificate authority), you will need to configure your MFDs to trust this certificate. For more information on this specific subject, please refer to Ricoh.

👉 **Note:** If you are using the XMediusFAX Cloud service, the server identity validation can be (and must be) enabled without having to perform any further configuration (the XMediusFAX Cloud certificate is actually signed by a trusted authority).

Installing the XMediusFAX App Deployer

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

To install the XMediusFAX App Deployer:

1. Launch the XMediusFAX App deployer installer:
   `XMediusFAXRicohSmartApp_<version>.exe`
2. Simply follow the instructions of the installer.
   All files are installed by default in `C:\Program Files\XMediusFAX Ricoh Smart App\` (referenced as *[App_Install_Path]* in this document).

The installation is now complete and you can configure and deploy the XMediusFAX App (see: *XMediusFAX App Configurations and Deployment – Overview* on page 7).

Chapter 4 App Configuration and Deployment

XMediusFAX App Configurations and Deployment – Overview

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

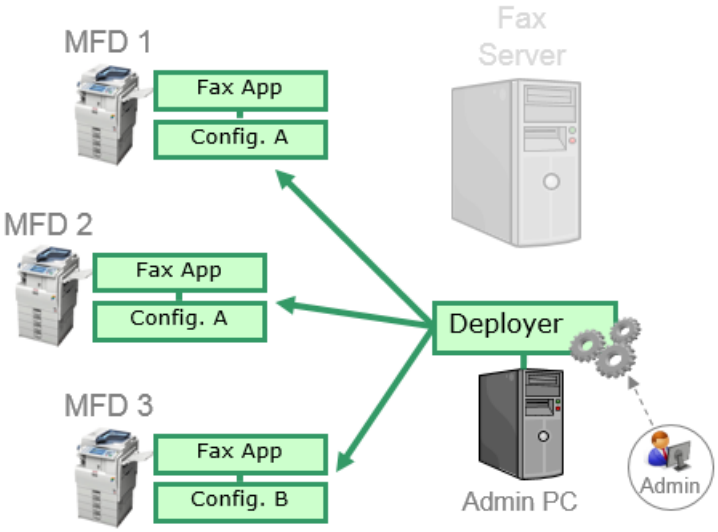
This chapter covers the following subjects:

- Information on the way the XMediusFAX App 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 App to the concerned MFDs using the provided Deployer.

Note: Before starting, you must have first installed the XMediusFAX App Deployer on the administrator's PC (see *Installing the XMediusFAX App Deployer* on page 6).

About XMediusFAX App Deployment

The Deployer allows you to configure and install the XMediusFAX App simultaneously on all concerned MFDs.



Note: You can decide to have different configuration settings depending on the MFD where the XMediusFAX App 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

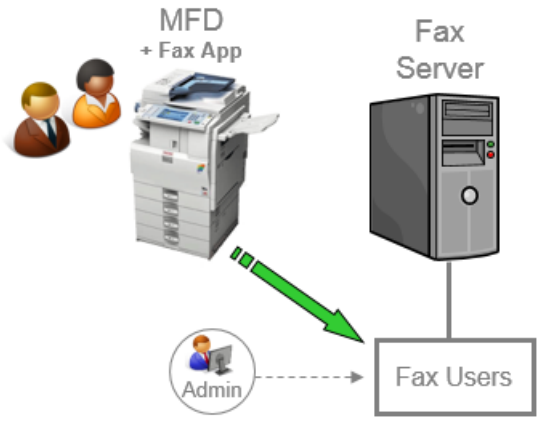
The way users will be authenticated in order to use the XMediusFAX App are multiple and largely depend on your company architecture and policies.

Note: For technical reasons, this section should be preferably considered prior to deploying the XMediusFAX App 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 XMediusFAX App)
- 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 App configuration settings:

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

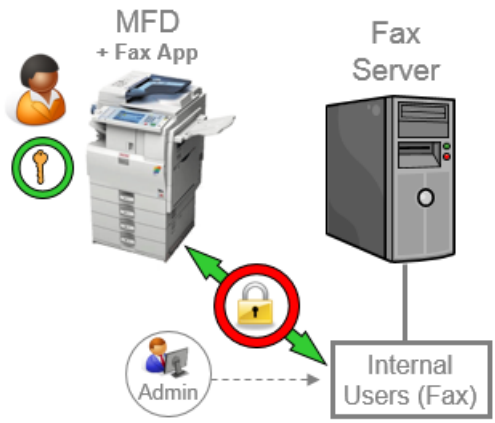
   Note: This user can be either an **Internal User** or an external user retrieved by the **Directories Integration** (see the XMediusFAX *Administration Guide* for more information).

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

2. When you will configure the XMediusFAX App, 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:

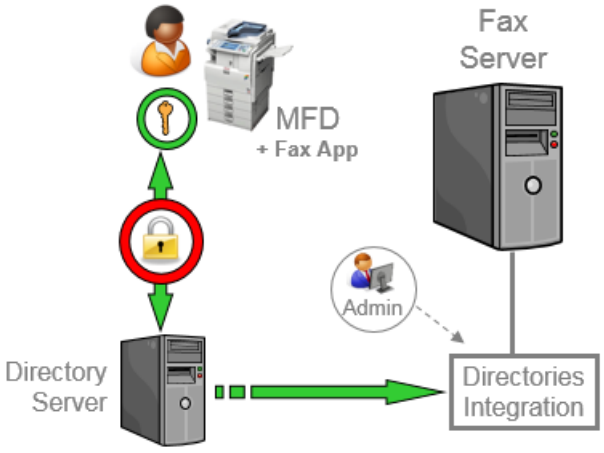
1. From the XMediusFAX administration interface, add all required fax user accounts to the list of **Internal Users**, according to the procedure given in the XMediusFAX *Administration Guide*.

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

2. When you will configure the XMediusFAX App, 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 XMediusFAX App on a MFD. More precisely, the XMediusFAX App can be configured to authenticate users 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** (`AAA`) when you configure the XMediusFAX App 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:

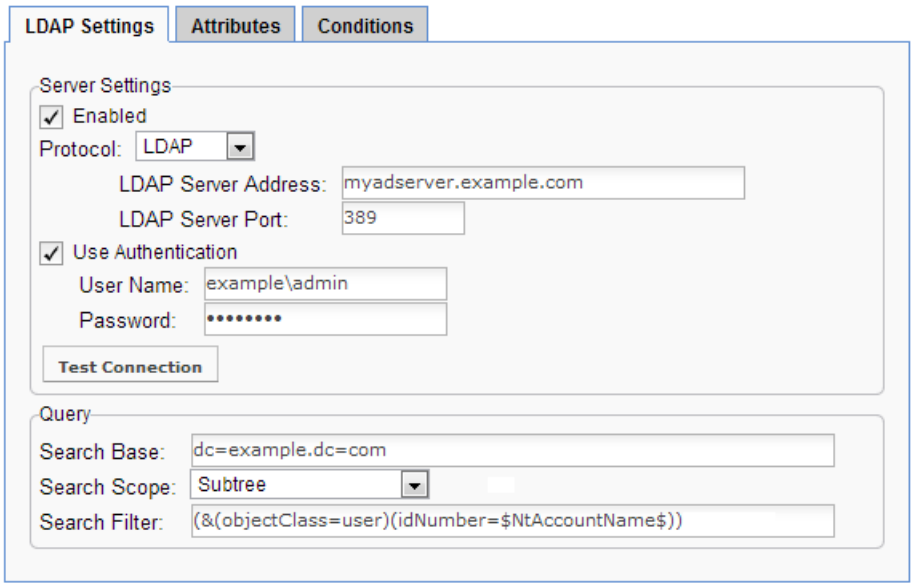
- The MFD is configured to permit single sign-on.
- Users are accessing the MFD features using a personal card they scan with a card reader.
- The authentication method returns an ID number corresponding to the user.

- 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).

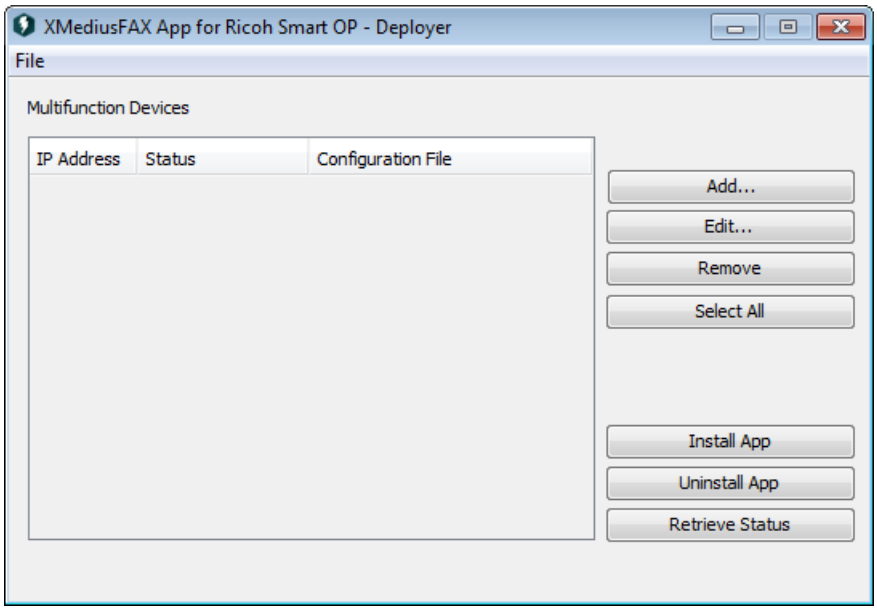
Configuring and Deploying the XMediusFAX App

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 App.
- 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 8).

To configure and deploy the XMediusFAX App:

1. Launch the Deployer by selecting **XMediusFAX App for Ricoh Smart OP ➤ Deployer of XMediusFAX App for Ricoh Smart OP** among your installed programs.

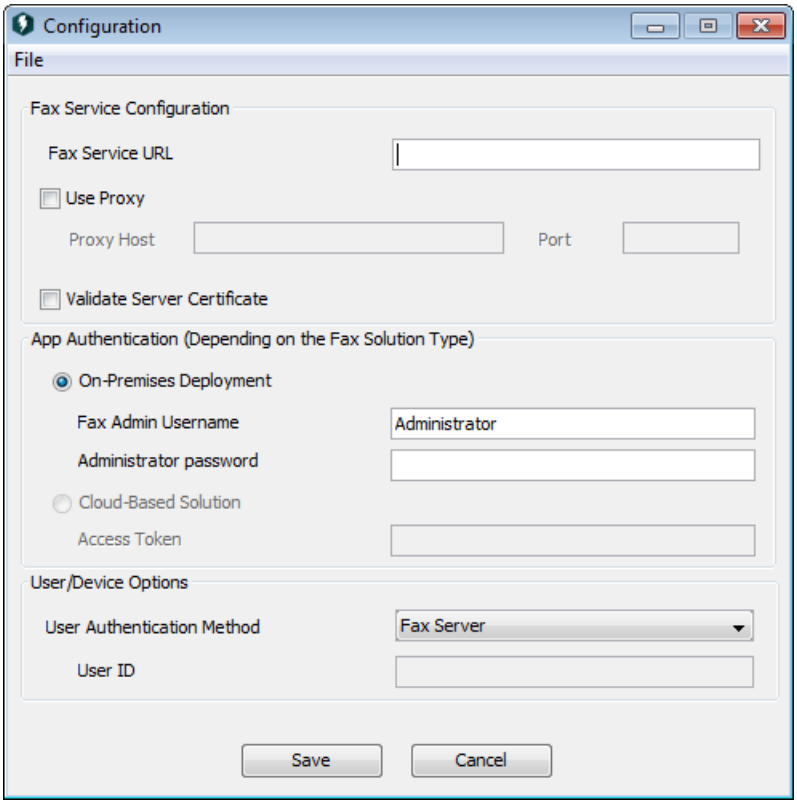


2. Create configuration files for the XMediusFAX App:

   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 but recommended)	Enables an additional security for the Web Service connection to XMediusFAX, by validating the server identity. **Attention:** Leaving this option disabled would represent a vulnerability that could be exploited by a malicious user to intercept and modify your fax traffic, as no server identity validation would be performed by the XMediusFAX App before sending fax data using the specified **Fax Service URL**. **Important:** If you are using the XMediusFAX Cloud service, you must enable this option. Note that the XMediusFAX Cloud certificate is signed by a trusted authority (no further configuration is required). If you are using the XMediusFAX On-Premises solution, enabling this option additionally requires: • To have a valid certificate from the XMediusFAX host (see *XMediusFAX App Installation Planning* on page 5), and • To ensure that the <*ServerName_or_IP*> specified in the **Fax Service URL** field matches the Common Name (CN) of the certificate.

c) **App 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	App 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	App 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 App 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. • `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 8.

e) Click **Save**.

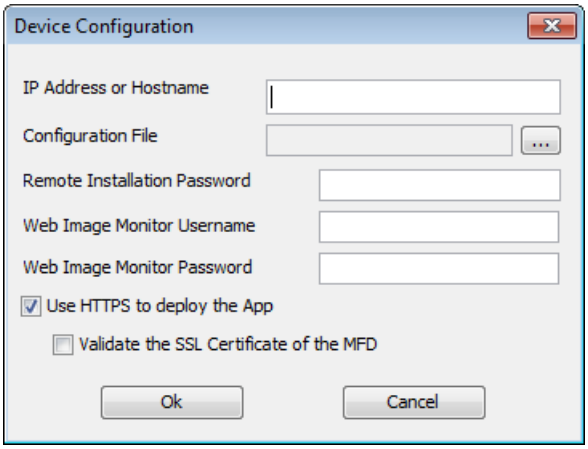
f) Give the configuration file an easily recognizable name (in case of multiple configurations) and save it.

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 or Hostname** of the MFD.

c) Associate a **Configuration file** to this MFD (with the browse button).

d) Optionally adjust the security 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**.

Control	Description
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	
Use HTTPS to deploy the App	Enables the use of HTTPS for the App deployment operation to the MFD (enabled by default).
Validate the SSL Certificate of the MFD (optional but recommended)	Enables an additional security while deploying the App to the MFD through HTTPS, by validating that the certificate of the MFD is signed by a trusted authority and is not expired. **Attention:** Leaving this option disabled would represent a vulnerability that could be exploited by a malicious user to intercept and modify your App configuration, as no MFD identity validation would be performed by the Deployer before deploying the App to the specified **IP address or Hostname**. **Important:** Using this option requires: • To have a valid SSL certificate (signed by a trusted authority) installed on the MFD, and • To ensure that the value specified in the **IP address or Hostname** field matches the Common Name (CN) of the certificate.

e) Click **OK** 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 App (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 App 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 App 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 App:
   a) Select the MFDs to which you are going to deploy the App.
   b) Click **Install App** to deploy the configured App to the selected MFDs.

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

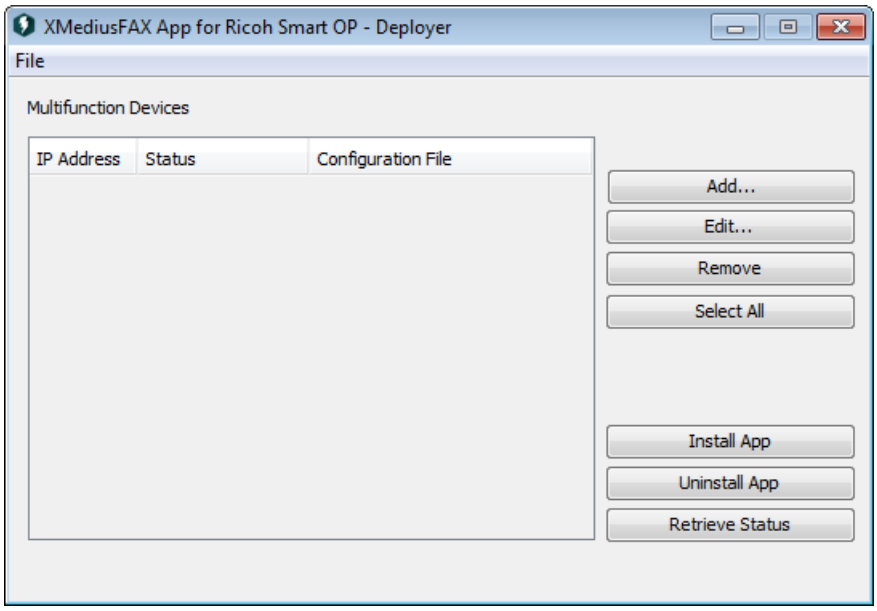
The XMediusFAX App is now ready to be used on all concerned MFDs.

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 8).

Managing the MFD List, Updating/Upgrading the App

Launch the Deployer by selecting **XMediusFAX App for Ricoh Smart OP ➤ Deployer of XMediusFAX App for Ricoh Smart OP** among your installed programs.



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 App 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 App configuration file to an MFD, or to upgrade the version of the XMediusFAX App already installed on an MFD.

MFD List

Column	Description
IP Address	The IP address of the MFD.
Status	The XMediusFAX App 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 App configuration file associated to this MFD (see *Configuring and Deploying the XMediusFAX App* on page 11 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 App* on page 11 for more information on MFD settings).

Button	Description
Edit	To edit the settings of the selected MFD. 👉 **Note:** Multiple selection allows to quickly associate the same App configuration file to several MFDs.
Remove	To remove the selected MFD.
Select All	Selects all the MFDs of the list.
Install App	Deploys the XMediusFAX App on the selected MFD with the configuration file associated to this MFD. 👉 **Note:** If a previous version of the XMediusFAX App is already installed, the deployer will automatically proceed to an upgrade to the current version.
Uninstall App	Uninstalls the XMediusFAX App from the selected MFD (see *Uninstalling the XMediusFAX App* on page 19 for more general details about uninstallation).
Retrieve Status	Retrieves the XMediusFAX App version and installation status (**Status** column) for all listed MFDs.

Chapter 5 Uninstallation

Uninstalling the XMediusFAX App

To properly uninstall the XMediusFAX App:

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

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

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

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

   a) On the administrator's PC, access the Add/Remove Programs feature.
   b) Select **XMediusFAX App for Ricoh Smart OP** and click **Remove**.

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