XMedius

WWW.XMEDIUS.COM

XMediusFAX Sharp OSA Connector 4.1.0

Administration Guide

XMediusFAX Sharp OSA Connector

Version Number 4.1.0.83 – February 2019.

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).

• OSA .NET: Copyright © 2005 - 2012 Sharp Corporation.
• log4net: Copyright © 2001-2003 Neoworks Limited (under Apache license). All Rights Reserved.

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 Sharp OSA 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

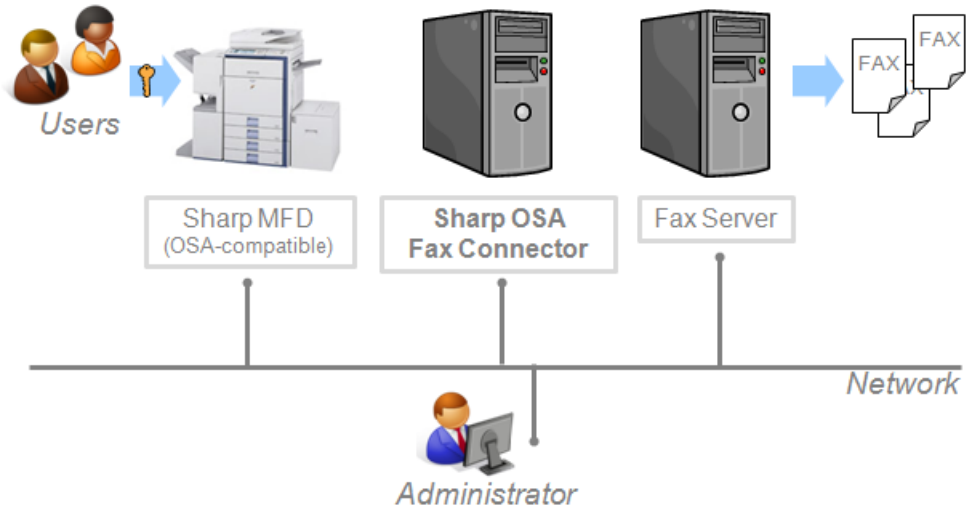
Table of Contents

Chapter 1 Introduction

The XMediusFAX Sharp OSA Connector

The XMediusFAX Sharp OSA Connector is a solution allowing Sharp Multi-Function Devices (MFDs) that are compatible with the OSA (Open Systems Architecture) technology to fax documents through XMediusFAX.

Here is an example of deployment including an MFD, a computer hosting the XMediusFAX Sharp OSA Connector and the Fax Server (XMediusFAX):



Note: In this example, the OSA Connector and the Fax Server are installed on separate machines; however, you could decide to install them on the same machine, if needed. Also, more than one MFD connected to the network can benefit from the XMediusFAX Sharp OSA 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 and configure the XMediusFAX Sharp OSA Connector.
- Configure Sharp 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 Sharp OSA Connector and its Host

Connector

The XMediusFAX Sharp OSA Connector can be installed either on the computer hosting XMediusFAX or on a separate computer (as long as both computers can communicate together on the network).

👉 **Important:** This version of the XMediusFAX Sharp OSA Connector cannot be used to perform an upgrade from any of its previous versions.

Connector Host

The computer hosting the XMediusFAX Sharp OSA Connector:

- Must have one of the following OS installed:
  - Windows Server 2008 / 2012
  - Windows 7 / 8
- Must have network access to communicate with:
  - The XMediusFAX host.
  - All MFDs that are required to use the XMediusFAX Sharp OSA Connector
- Must have the following components installed prior to installing the XMediusFAX Sharp OSA Connector:
  - .NET Framework 4.5 or greater
  - Internet Information Services 7 (IIS7) or greater

    👉 **Important:** You must configure IIS to have **ASP.NET** enabled. For example in Windows 2008:

    1. In **Server Manager** select the **Roles** node, expand the **Web Server (IIS)** heading and click on **Add Role Services**.
    2. On the **Select Role Services** page, under **Application Development**, select **ASP.NET**.
    3. If prompted, click **Add required role services**.
    4. Click **Next** and follow the instructions of the installer.

Multi-Function Devices (MFDs)

All MFDs that are required to use the XMediusFAX Sharp OSA Connector must:

- Be compatible with the Sharp OSA framework version 3.0 or above.
- Be compatible with the "HTML Browser" technology.
- Be on the network to communicate with the computer hosting the XMediusFAX Sharp OSA Connector.
- Have a panel screen with a resolution of WSVGA (1024x600), WVGA (800x480) or QVGA (480x272).

  Restriction: QVGA screens will only support the Basic interface of the XMediusFAX Sharp OSA Connector (fax number only).

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 Sharp OSA Connector.

However, the "External Account" integrated authentication method is also supported when configured and activated within the MFD.

Fax Server (XMediusFAX)

The XMediusFAX Sharp OSA 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 Sharp OSA 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 Sharp OSA 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 Sharp OSA Connector on the computer hosting XMediusFAX or on a separate computer on the network.
- 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 Sharp OSA Connector cannot be used to perform an upgrade from any of its previous versions. It only applies to devices compatible with the Sharp OSA framework version 3.0 or above. Previous versions of the XMediusFAX Sharp OSA Connector must be uninstalled before proceeding.

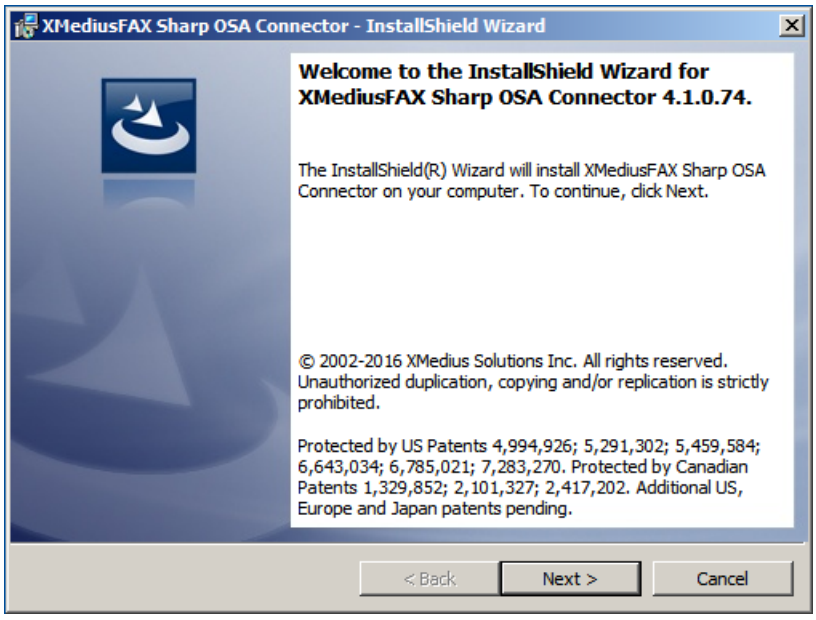
Installing the XMediusFAX Sharp OSA Connector

👉 **Note:** This installation can be performed either on the computer where XMediusFAX is installed or on a separate computer on the network.

👉 **Important:** Before you start the installation, read carefully the section: *Installation Requirements* on page 3. Some configuration are required on the computer that will host the XMediusFAX Sharp OSA Connector.

To install the XMediusFAX Sharp OSA Connector:

1. Launch `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 (see: *Fax Connector and MFD Configurations – Overview* on page 11).

Installing the XMediusFAX Certificate (Optional)

The XMediusFAX Sharp OSA Connector uses by default the secured Web Services feature of XMediusFAX (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 Sharp OSA Connector* on page 16). In that case, you must also ensure that the XMediusFAX certificate will be trusted on the computer hosting the XMediusFAX Sharp OSA 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 25 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 Sharp OSA 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 Sharp OSA Connector, you must configure the connector and each of the concerned MFDs.

This chapter covers the following subjects:

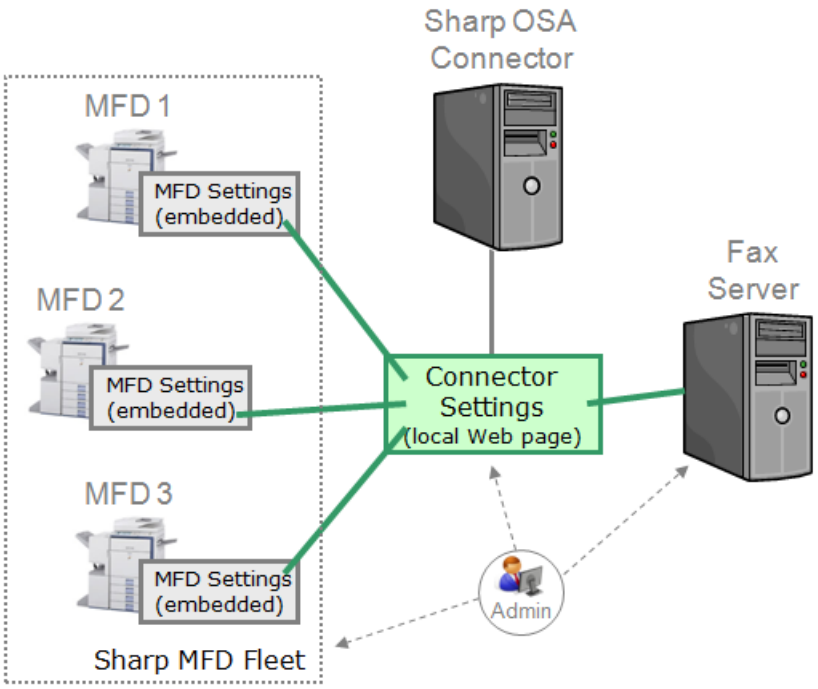
- Information on the way the faxing feature will be made available on your MFDs.
- Information on fax users authentication, with description of the various methods that can be used
- Some instructions to configure your faxing environment according to the authentication method that is used.
- The procedure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

👉 **Note:** Before starting, you must have first installed the XMediusFAX Sharp OSA Connector according to the requirements and procedure provided through this guide.

About XMediusFAX Sharp OSA Connector and MFD Configurations

The XMediusFAX Sharp OSA Connector is installed as a standalone application. Its configuration is performed via a local Web page on the computer where it is installed.

To have the XMediusFAX Sharp OSA Connector enabled, each MFD must also be configured separately via their embedded settings.



Connector Settings

The XMediusFAX Sharp OSA Connector settings contain:

- 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.

MFD Settings

Each MFD among your Sharp MFD fleet will require to be configured one by one to enable the XMediusFAX Sharp OSA Connector, by targeting the computer hosting the connector. All MFDs will then share the same XMediusFAX Sharp OSA Connector settings.

Fax Users Authentication

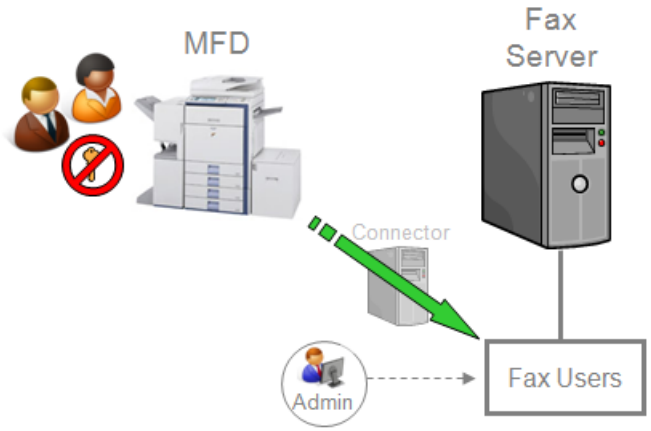
The way users will be authenticated in order to use the faxing feature are multiple and largely depend on your company architecture and policies.

Note: For technical reasons, this section should be preferably considered prior to configuring the XMediusFAX Sharp OSA 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 "External Account" feature of the Sharp MFD (which requires configuration in the related section of the MFD settings).

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 Sharp OSA Connector configuration settings:

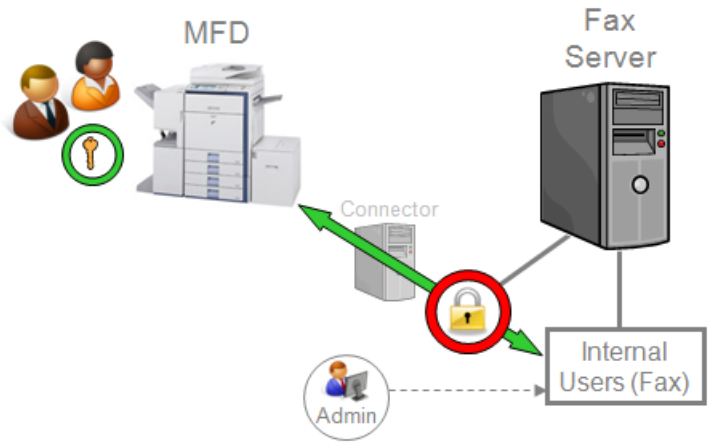
1. From the XMediusFAX administration interface, configure XMediusFAX to include a user that you will dedicate to the MFD.

   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 Sharp OSA 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:

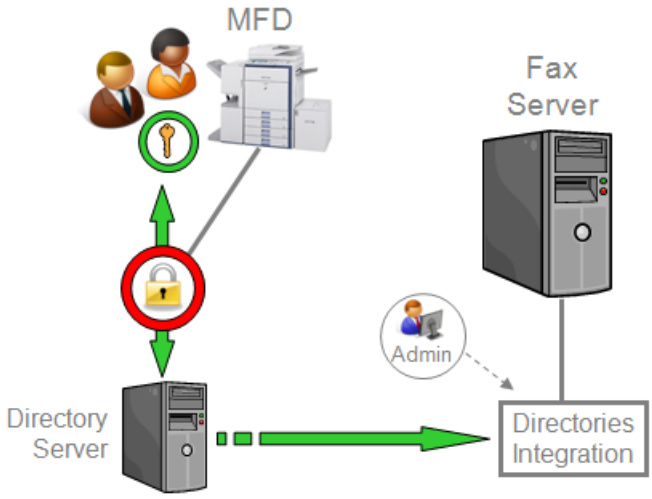
1. From the XMediusFAX administration interface, add all required fax user accounts to the list of **Internal Users**, according to the procedure given in the XMediusFAX *Administration Guide*.

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

2. When you will configure the XMediusFAX Sharp OSA 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 "External Account" feature of the MFD (to push to XMediusFAX the information returned by the method).

Note: For more information, see the MFD documentation.

Once those points have been verified:

1. Configure the External Account feature within the MFD.
2. Make sure to select `External Account` as **User Authentication Method** when you will configure the connector.

Depending on which type of attribute is returned by the External Account 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 the 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).

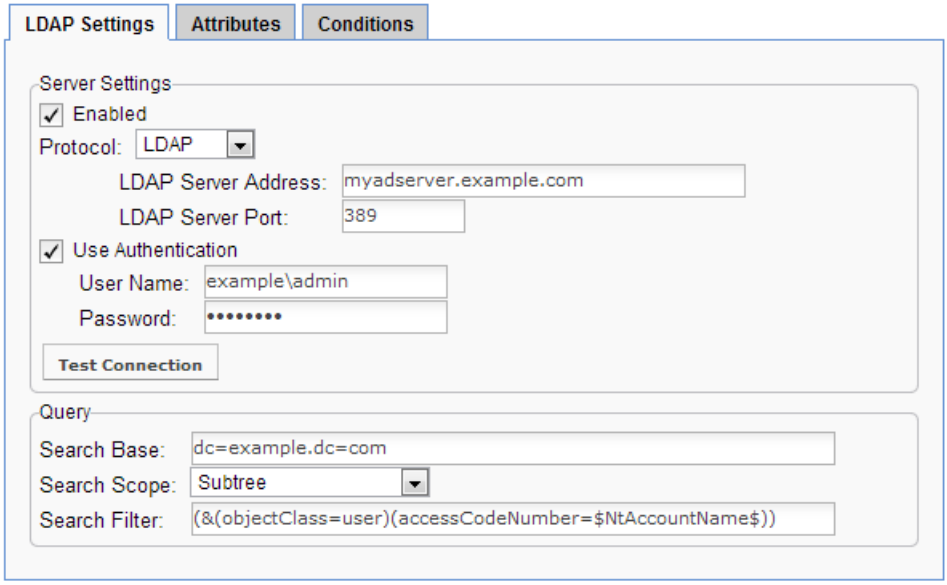
> **Example: Single Sign-On with Card Reader (Code Number Returned)**
>
> Let's consider the following scenario example:

- The MFD uses an authentication method that permits single sign-on (through the External Account feature).
- Users are accessing the MFD features using a personal card they scan with a card reader.
- The authentication method returns a code number corresponding to the user.
- On the user directory side, this code number is stored for each user under an attribute named `accessCodeNumber`.

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

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

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



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

Configuring the XMediusFAX Sharp OSA 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 12).

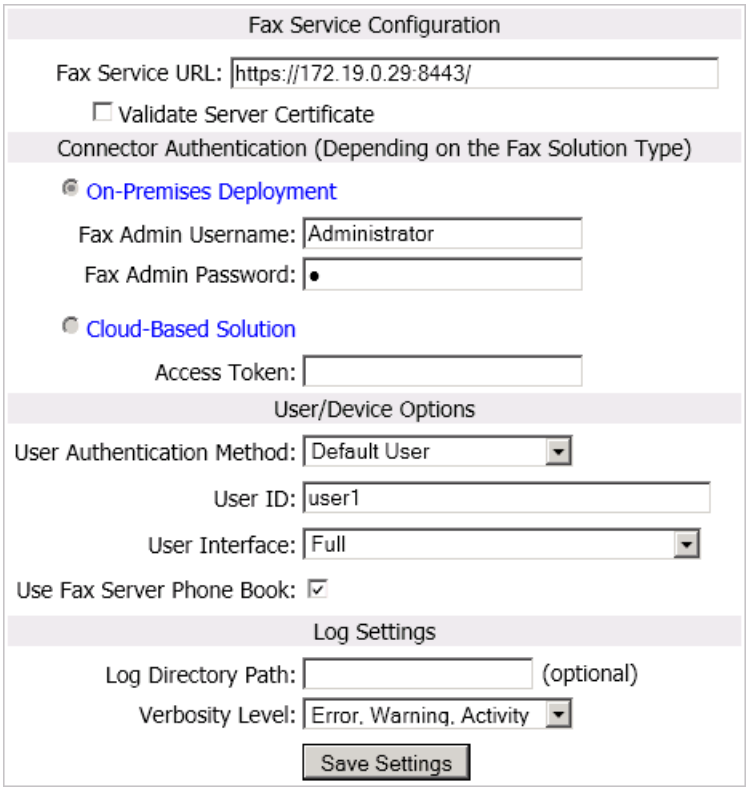
Important: This configuration must be performed from the computer hosting the XMediusFAX Sharp OSA Connector. The configuration page is not remotely available.

To configure XMediusFAX Sharp OSA Connector:

1. Using a Web browser, enter the following address: `http://localhost/OSAConnector/`

Note: The last "/" (slash) character is mandatory.

2. Enter the **User Name** and **Password**.
   By default, the values are `sharp` and `password`.



3. Enter the XMediusFAX Sharp OSA Connector configuration settings:
   a) **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.
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 8). **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. • `External Account` (for other authentication method) – 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 12.
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).

d) **Log Settings**

Control	Description
Log Directory Path	Path of the directory where the Log Files will be stored (see *Debugging the XMediusFAX Sharp OSA Connector* on page 21). **Note:** If you leave this field empty, the default path `C:\Inetpub\wwwroot\OSAConnector\LogFiles` will be used.
Verbosity Level	The depth of the information that will appear in the log files.

4. Save the settings.

Important: After this configuration, you still need to enable the XMediusFAX Sharp OSA Connector on all MFDs that you have targeted to use it. See *Configuring a Sharp MFD to Use the XMediusFAX Sharp OSA Connector* on page 19.

Configuring a Sharp MFD to Use the XMediusFAX Sharp OSA Connector

Note: The configuration steps provided below could be different depending on the Sharp MFD model you are using. For more details, please refer to the documentation of the MFD.

To enable the XMediusFAX Sharp OSA Connector on a Sharp MFD:

1. Using a Web browser, enter the IP address of the MFD and connect to its configuration page by using the Login Name and Password of the MFD.
2. Select **Application Settings ➤ External Applications Settings**, then click **Add**.
3. In **Application Name**, enter `XMediusFAX`.

   This will identify the XMediusFAX feature on the MFD screen.
4. Enter the **Address for Application UI**: `http://<Connector_Host_IP>/OSAConnector/`

   Note: <*Connector_Host_IP*> is the IP address of the computer hosting the XMediusFAX Sharp OSA Connector. The last "`/`" (slash) character is mandatory.
5. Add the icon that will visually identify the XMediusFAX feature on the MFD screen:

   Browse to the XMediusFAX Sharp OSA Connector installation package and select the file: `XMediusFAX.gif`.
6. Click **Submit** to save the settings.

   Note: For the most common implementation scenarios, it is not required to configure any other settings available through this page.

   The new application XMediusFAX appears on the list of applications.
7. 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 Sharp OSA Connector

If you encounter issues with the XMediusFAX Sharp OSA Connector, you can have access to some debugging information in log files, on the computer hosting the XMediusFAX Sharp OSA Connector, for troubleshooting purpose with XMediusFAX technical support.

By default, the log files can be found in the folder `C:\Inetpub\wwwroot\OSAConnector\LogFiles`.

A new log file is created every day (named with the date), and its contents depends on the verbosity level set via the XMediusFAX Sharp OSA Connector (see *Configuring the XMediusFAX Sharp OSA Connector* on page 16).

Chapter 6 Uninstallation

Uninstalling the XMediusFAX Sharp OSA Connector

To properly uninstall the XMediusFAX Sharp OSA Connector:

1. On the computer hosting the XMediusFAX Sharp OSA Connector, access the Add/Remove Programs feature.
2. Select **XMediusFAX Sharp OSA 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 Sharp OSA 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 Sharp OSA 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 Sharp OSA Connector host, see: *Installing the XMediusFAX Certificate (Optional)* on page 8.

Administration Guide
Noncontractual document

253566440

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