media5 corporation

Enabling Live Communications at the Edge of IP Networks

Configuration Notes 295

Auto-Provisioning Mediatrix units

June 22, 2011

Table of Contents

Introduction

This Configuration Note describes how to use the Mediatrix units' functionality that allows it to fetch the firmware and configuration files automatically from a provisioning server by using either TFTP or HTTP. This Configuration Note can be used to configure the Mediatrix 2102, Mediatrix 1100/1200 series and Mediatrix 4100 series (SIP v5.0 only).

Application Scenario

This Configuration Note will refer to the following scenario as an example throughout the document.

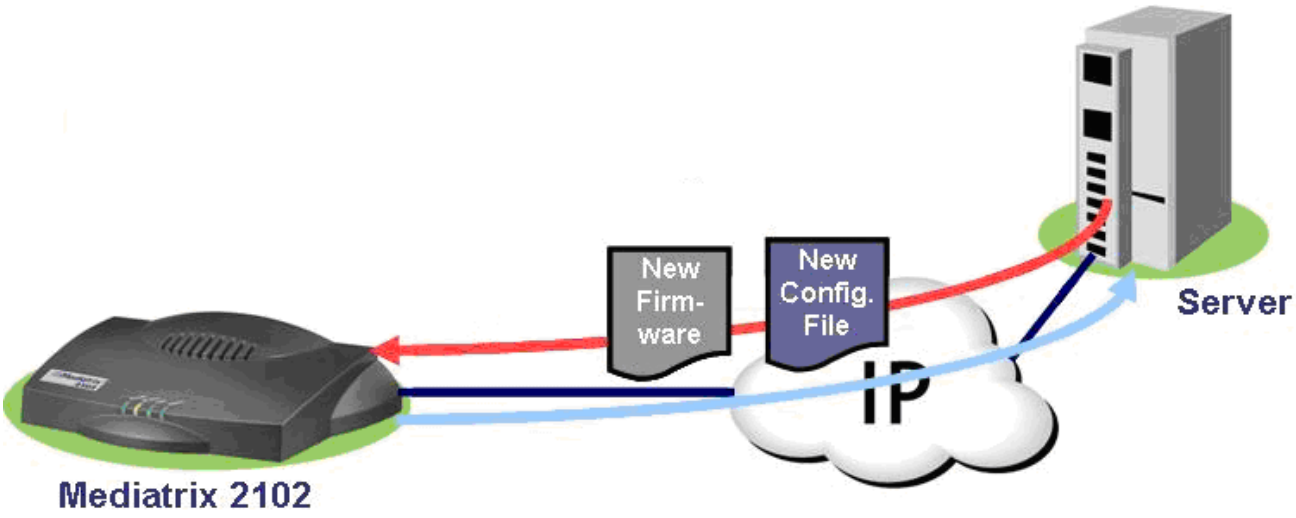


Figure 1. Network Diagram

In this document we will cover:

- Overview of the server setup
- Configuration required on the Mediatrix unit
- Preparation of the configuration files and firmware
- How to automatically configure your Mediatrix units

Server Configuration Overview

Preparing Windows Web Server for Auto-Provisioning

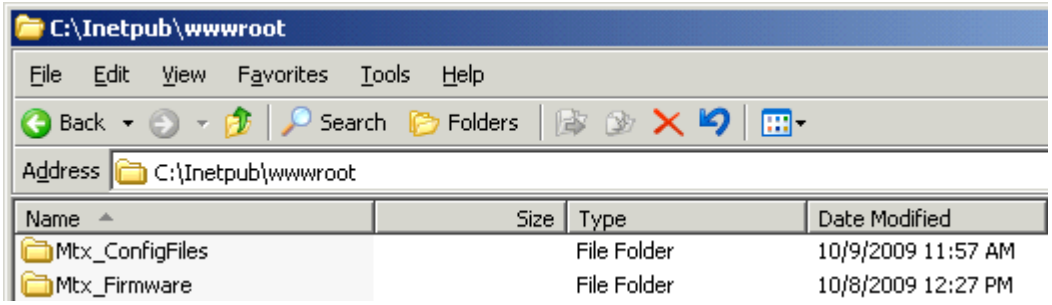
Ensure that the HTTP Server functionality is activated and that the configuration files and binaries are located under (IIS default):

C:\Inetpub\wwwroot

Media5 recommends that the administrator creates a subdirectory for the firmware and another subdirectory for the configuration files under the web server root directory:

For example:

- Configuration files are located under the *C:\Inetpub\wwwroot\Mtx_ConfigFiles* folder.
- Firmware files and folders are located under the *C:\Inetpub\wwwroot\Mtx_Firmware* folder.

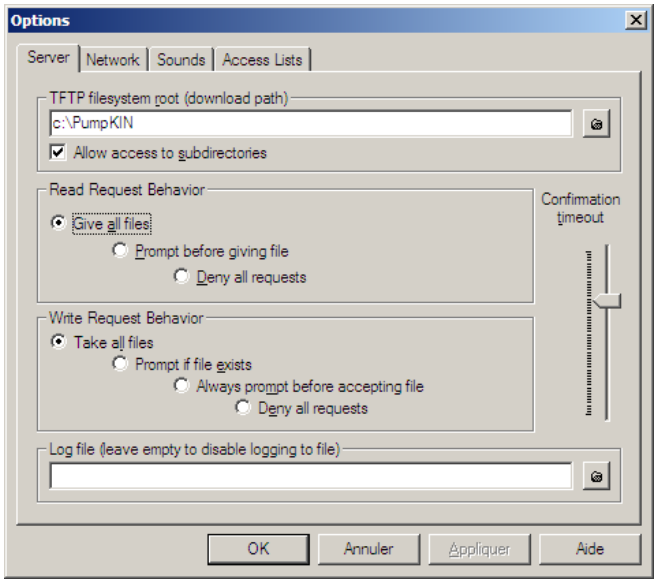


Preparing the TFTP Server for Auto-Provisioning

Ensure that the TFTP Server allows proper file or folder permission. For example, for the PumpKIN TFTP server, select the options as shown in the figure below. In the figure, the PumpKIN TFTP Server root directory is **C:\PumpKIN**. The TFTP root directory is where the firmware and configuration folders and binaries will be located. Media5 recommends that the administrator creates a subdirectory for the firmware and another subdirectory for the configuration files under the TFTP root.

For example:

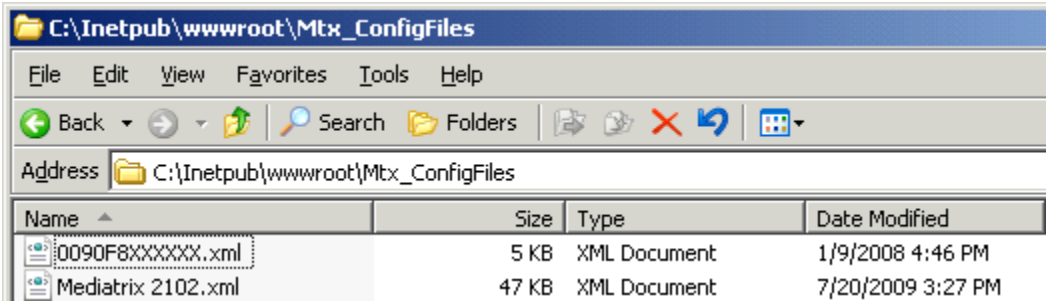
- Configuration files are located under *C:\PumpKIN\Mtx_ConfigFiles*
- Firmware files and folders are located under *C:\PumpKIN\Mtx_Firmware*



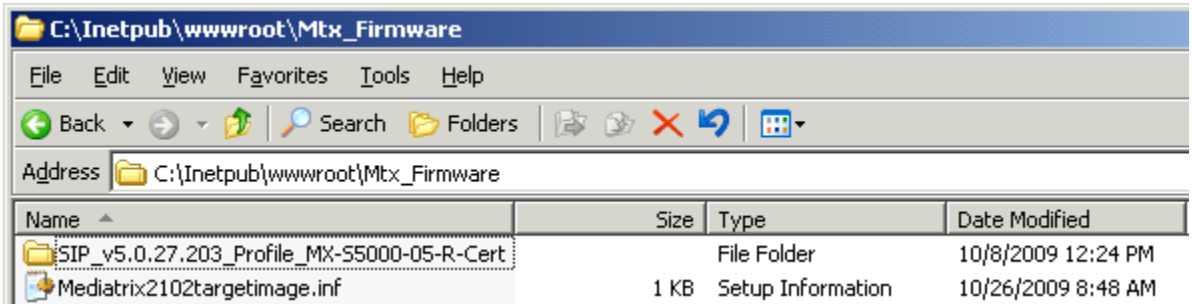
Example

For the example scenario, here is what each folder would look like:

<TFTP or Web root>\Mtx_ConfigFiles



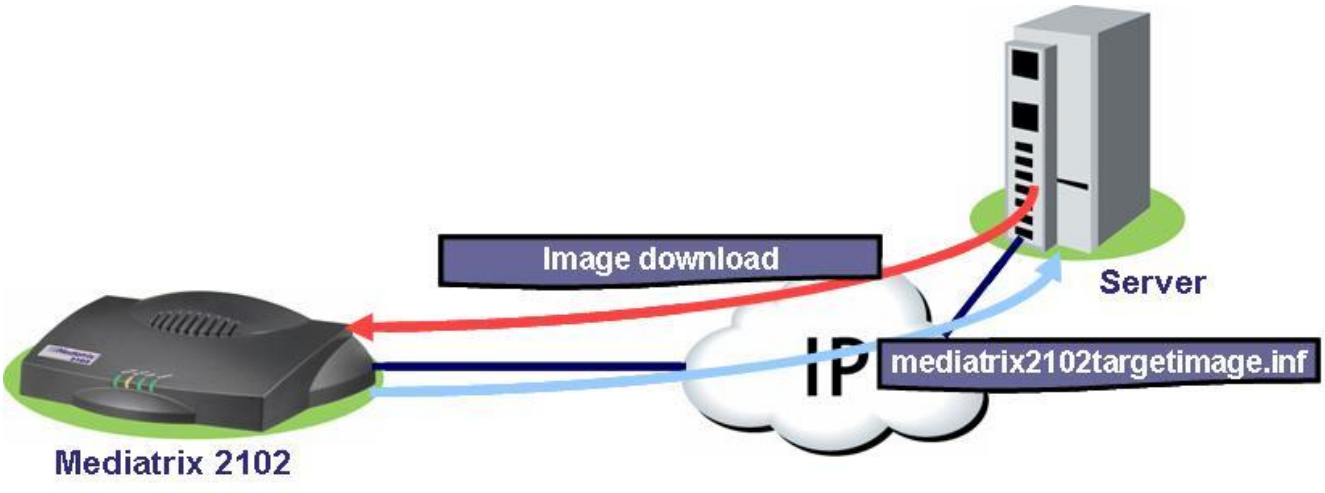
<TFTP or Web root>\Mtx_Firmware



We will explain the use of each file and folder later in this document.

Preparation of the Configuration Files and Firmware

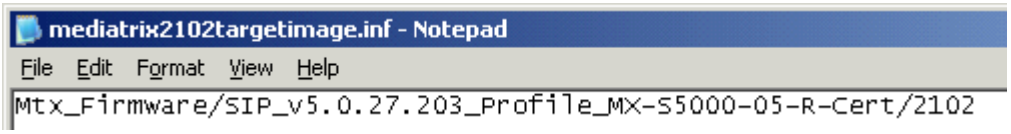
Firmware



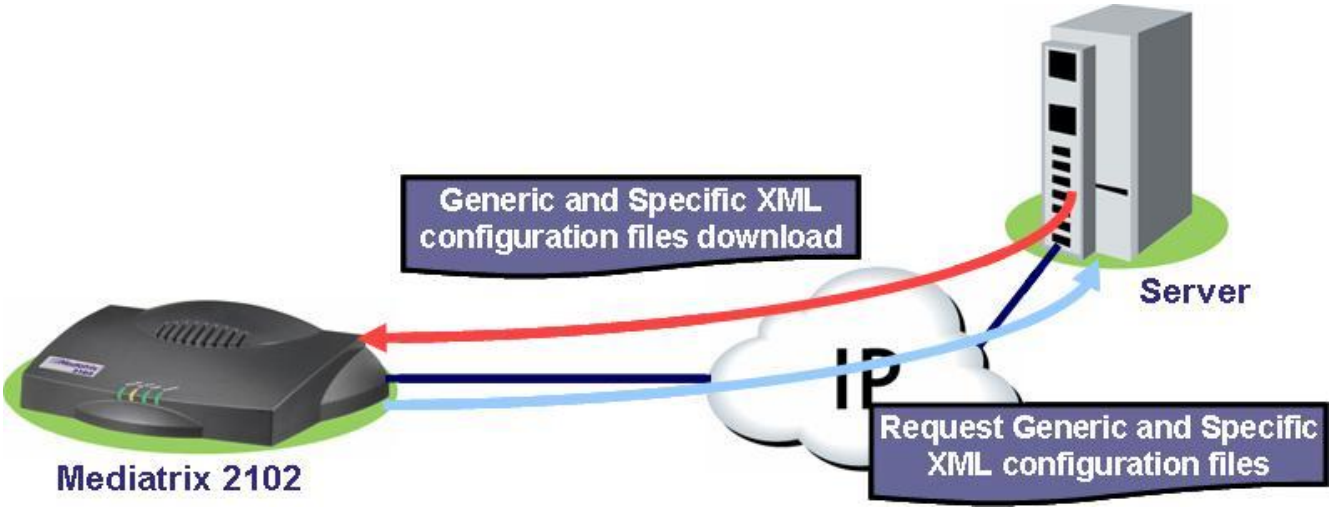
Media5 recommends using the file selection method for automatic image download. This method consists of fetching a file called *<product>targetimage.inf.* This file contains a single line outlining the directory where the binary files are located (see example below). When the Mediatrix unit downloads this file, it fetches the *Setup.inf* file located in the folder specified in the *<product>targetimage.inf* file. The Mediatrix unit then proceeds to check if its firmware on the system matches the name of the firmware specified in the *Setup.inf*. If there is no match, the Mediatrix unit proceeds with the complete download of the binary files. You must create this file and place it in the same directory as the folder containing the binaries.

For example:

- The binaries are located under **<TFTP or Web root>/Mtx_Firmware/SIP_v5.0.27.203_Profile_MX-S5000-05-R-Cert/2102**
- **2102** is the folder containing the binaries and the Setup.inf file.
- Place **mediatrix2102targetimage.inf** under **<TFTP or Web root>/Mtx_Firmware**



Configuration Files



The auto-provisioning feature on the Mediatrix units can fetch two types of files:

- Generic XML configuration file
- Specific XML configuration file

The Generic XML configuration file contains parameters that can be applied to all Mediatrix units in the field. For example, generic parameters such as SIP Proxy server address or voice codec can be specified in this file. This means that all Mediatrix units in the field will point to the same Service Provider SIP Proxy Server and use the same codec. To add flexibility, Media5 created a feature that allows the Mediatrix units to fetch the generic file with its product name as filename. The Mediatrix unit can be configured to fetch a generic file called: *%product%.xml* where *%product%* is a macro replaced by the product name of the unit.

The Specific XML configuration file contains parameters that are specific to each Mediatrix unit. For example, specific parameters are SIP username and SIP authentication parameters. To simplify the configuration of the specific XML file, Media5 created a feature that allows the Mediatrix unit to fetch the specific file with its MAC address as filename. The Mediatrix unit can be configured to fetch a specific file called: *%mac%.xml* where *%mac%* is a macro replaced by the MAC address of the unit.

For example:

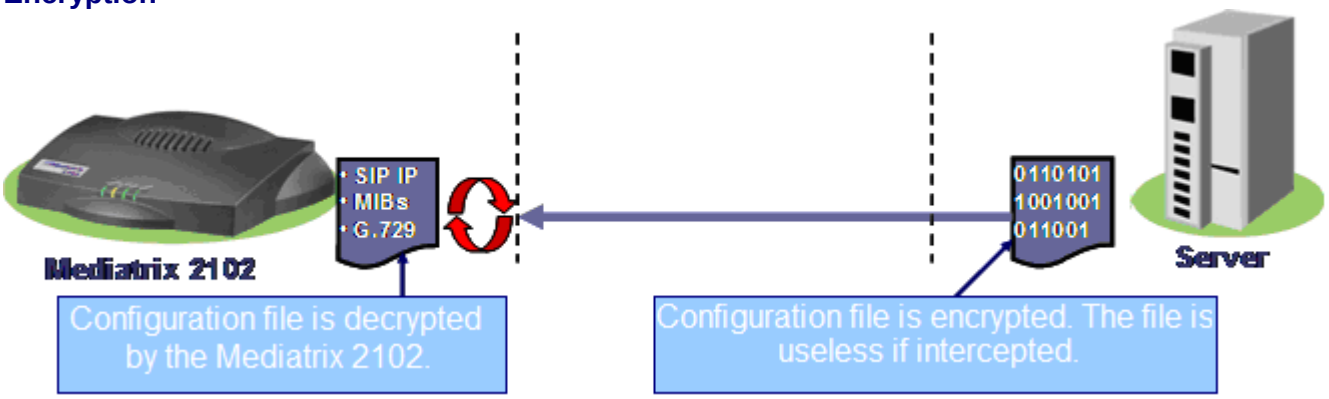
- The Mediatrix 2102 has the MAC address 0090F8XXXXXX.
- The generic XML configuration file on the server could be *Mediatrix 2102.xml*. (*%product%.xml)*
- The specific XML configuration file on the server could be *0090F8XXXXXX.xml. (%mac%.xml)*

Creating a Configuration File

To create a configuration file in XML format that can be used with the auto-provisioning feature, the Unit Manager Network (UMN) software is required.

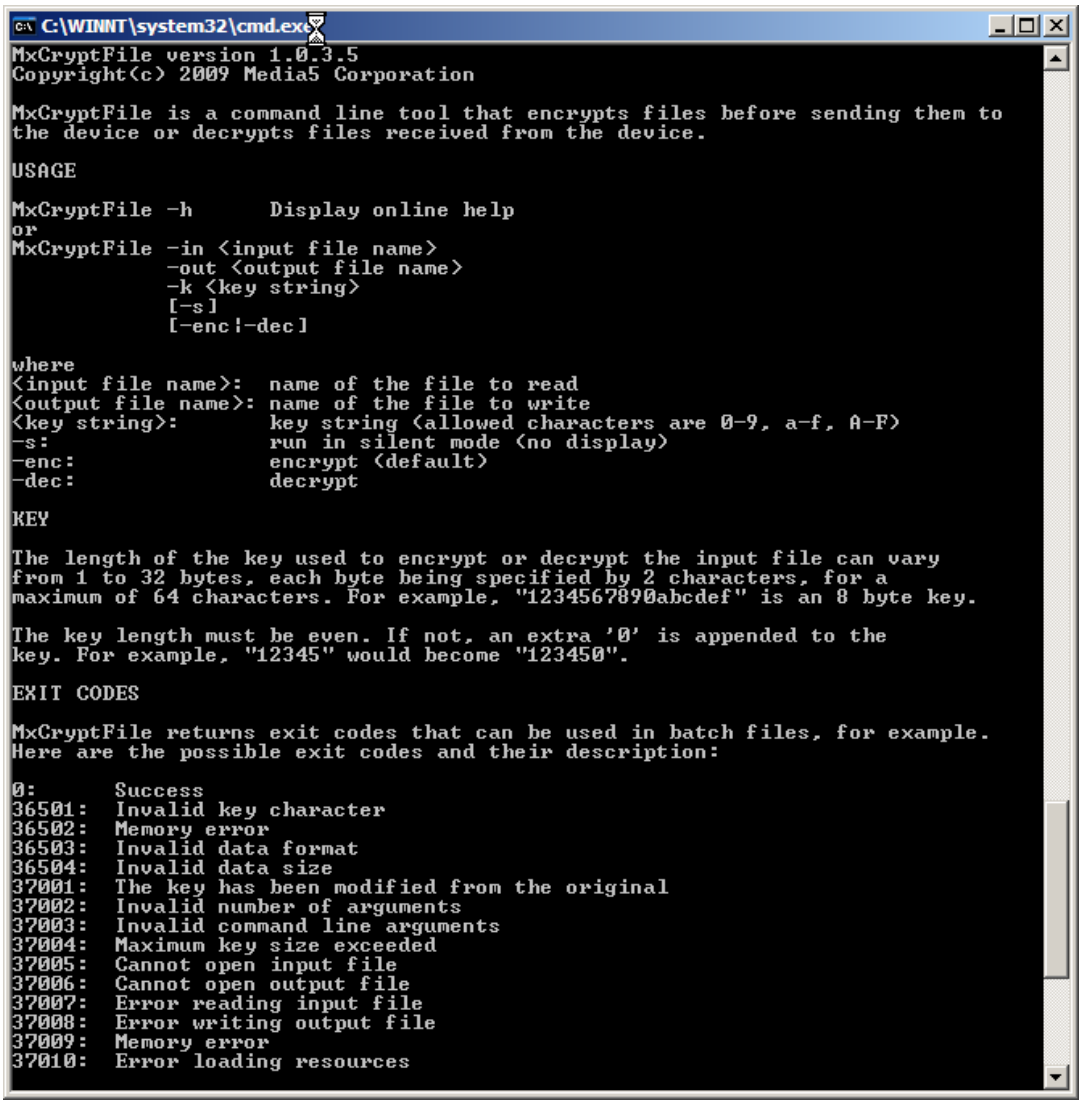
1. Once you have connected to the unit using the auto-detect feature of UMN, right-click the unit and select *Configuration File* and then *Save to XML…*
2. In the *Action Unit Selection* window, check the *Transfer configuration file from unit before proceeding* box and check the *Include SNMP specific settings in generated XML configuration file* if you intend to use SNMPv3 in your configuration files.
3. Wait for the operation to complete. It can take several seconds for the task to complete, especially on a slow network or when using SNMPv3.
4. At this point, UMN has created a CFG file and a XML file. To retrieve the XML file, browse to the default directory:
    - C:\Program Files\Unit Manager Network 3.2\UnitManager\CfgFile
5. The newly created file will have the name <mac address>.xml where <mac address> is the MAC address of the unit.

Encryption



Media5 provides an encryption tool to secure the XML configuration files on the server. Once the file is encrypted, the transfer of the information over the network is secure. The encryption tool uses symmetric block cipher to encrypt data. The encryption key supported by the tool can be up to 128-bits with increment of 8-bits. This encryption key must be configured on the Mediatrix units in order to decipher the information. The tool provided by Media5 can be used on Windows, Linux or Unix operating systems.

The following is an example of the tool running on Windows:



The following are some examples of MxCryptFile commands:

- MxCryptFile.exe –in "Mediatrix 2102_unencrypted.xml" –out "Mediatrix 2102.xml" –k 12345678
- MxCryptFile.exe –in 0090F8XXXXXX_unencrypted.xml –out 0090F8XXXXXX .xml –k 89bb6758ac895f56

Ensure that the Mediatrix unit is configured with the proper key in order to decipher the information. Without the proper key, the parameters in the encrypted XML file would not be applied to the Mediatrix unit.

Please refer to the *Technical Bulletin 0582 – Configuration Files Encryption Using MxCryptFile tool* or the MxCryptFile documentation for more details on the encryption tool.

Configuration of the Mediatrix Unit

You can configure the auto-provisioning in three ways:

1. Using the Administration web page
2. Using the Unit Manager Network
3. Using a MIB Browser

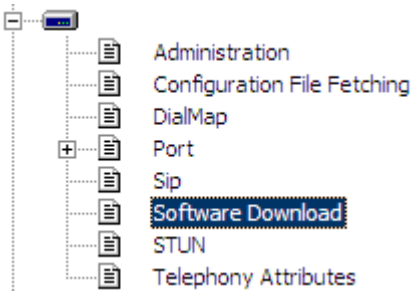
We will explain method one in length and present method two with screenshots throughout this section. If you wish to use method 3, use the variable names that are in parenthesis.

Firmware Download

1. Once you have gained access to the administration web page (Method 1) or connected (Method 2/3) to the unit, access the Firmware Download section:

Method 1:

Method 2:

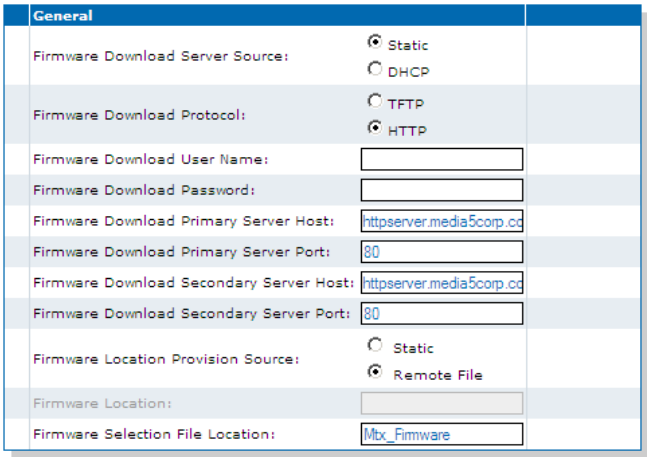


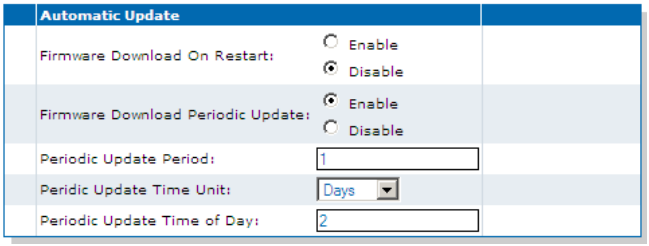
2. Server configuration
   - Configure the Download Server Source. You can configure the unit to request via DHCP the download servers. See the documentation for more details. (*imageSelectConfigSource*)
   - If you have set the Download Server Source to *Static*, configure the IP addresses or FQDN of the primary (*imageStaticPrimaryHost*) and secondary (*imageStaticSecondaryHost*) download server and their respective ports (*imageStaticPrimaryPort*/*imageStaticSecondaryPort*). By default, you can enter port *80* for a HTTP server and port *69* for a TFTP server.
3. Download configuration
   - Configure the Download Protocol (*imageTransferProtocol*).
   - When using HTTP, you can configure a username (*imageTransferUsername*) and password (*imageTransferPassword*) if your server requires basic or digest authentication.
   - Configure the Location Provision Source (*imageLocationProvisionSource*). Set to "Remote File" if you wish to use the feature described in the Section "Preparation of the configuration files and firmware" of this document.
   - If you have set the Location Provision Source to Remote file, configure the Selection File Location (*imageSelectionFileLocation*). This path should lead to the folder that contains the *<product>targetimage.inf* file.
   - If you have set the Location Provision Source to Static, configure the Firmware Location (*imageLocation*).

     In our example the Firmware Location would be set to: **Mtx_Firmware/ SIP_v5.0.27.203_Profile_MX-S5000-05-R-Cert/2102**

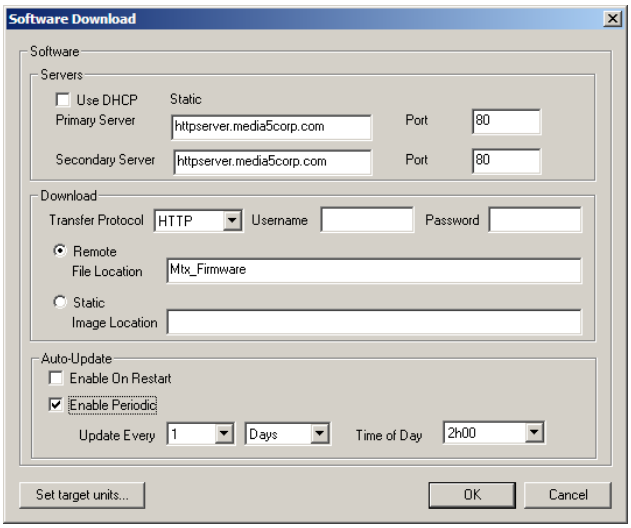
4. Automatic update configuration
   - Configure the Download On Restart (*imageAutoUpdateOnRestartEnable*) if you wish the unit to check for new firmware at each start.
   - Configure the Download Periodic Update (*imageAutoUpdatePeriodicEnable*) if you wish the unit to check for new firmware periodically.
   - If you have enabled the periodic update, you can configure the frequency with three parameters:
     - Period (*imageAutoUpdatePeriod*)
     - Time Unit (*imageAutoUpdateTimeUnit*)
     - Time of day (*imageAutoUpdateTimeOfDay*)
5. Here is what the configured interface would look like for Methods 1 and 2. In this example, the unit will check for a new firmware every day at 2h00 (24h format) on the HTTP server *httpserver.media5corp.com*. The unit will fetch the file *mediatrix2102targetimage.inf* in the Mtx_Firmware folder to verify if a new version is available.

Method 1:





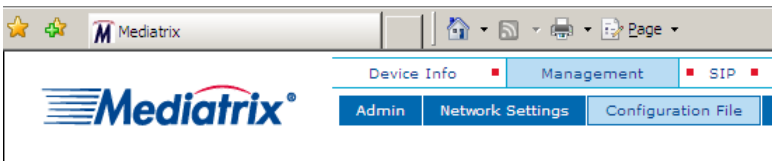
Method 2:



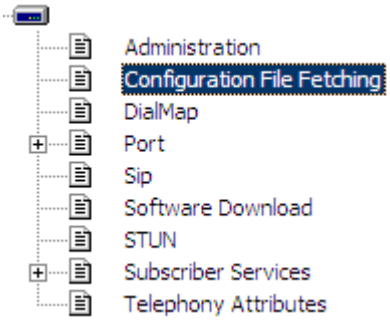
Configuration File Fetching

1. Once you have gained access to the administration web page (Method 1) or connected (Method 2/3) to the unit, access the Configuration file section :

Method 1



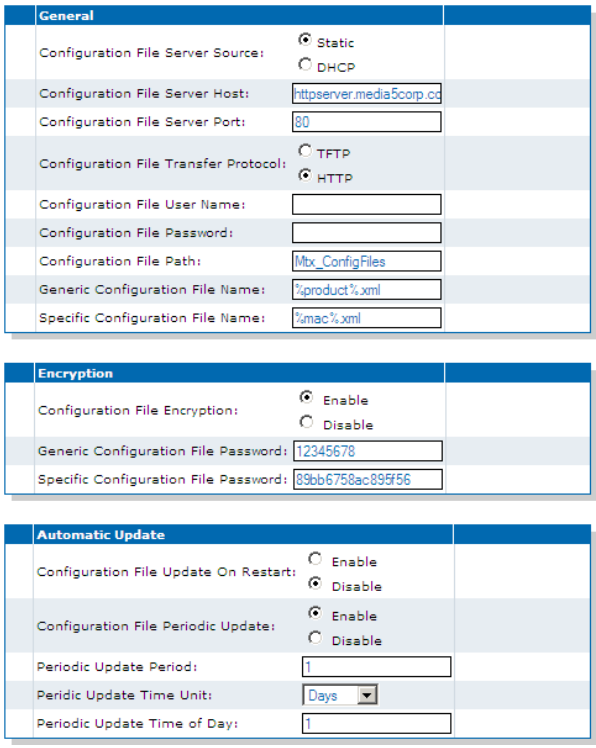
Method 2



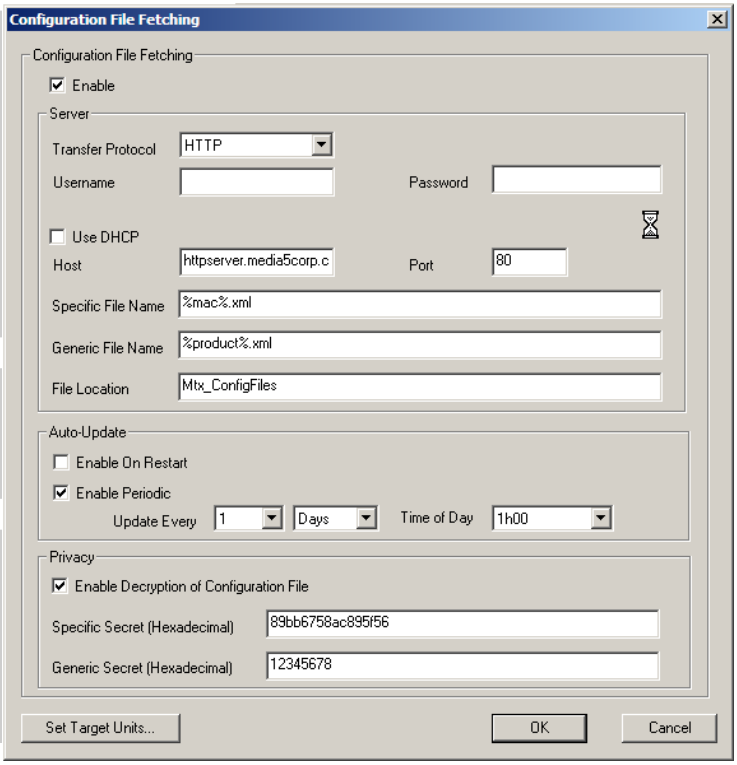
2. Server configuration
   - Configure the File Server Source. You can configure the unit to request via DHCP the configuration file server. See the documentation for more details. (*configFileFetchingSelectConfigSource*)
   - If you have set the File Server Source to *Static*, configure the IP address or FQDN of the file server (*configFileFetchingStaticHost*) and its port (*configFileFetchingStaticPort*). By default, you can enter port *80* for a HTTP server and port *69* for a TFTP server.
3. Download configuration
   - Configure the File Transfer Protocol (*configFileTransferProtocol*).
   - When using HTTP, you can configure a username (*configFileTransferUsername*) and password (*configFileTransferPassword*) if your server requires basic or digest authentication.
   - Configure the Configuration File Path (*configFileFetchingFileLocation*). This path should lead to the folder that contains the configuration files.
   - Configure the Generic Configuration File Name (*configFileFetchingFileName*). If you wish, you can use the macro %product% that will be replaced with the product name.
   - Configure the Specific Configuration File Name (*configFileFetchingSpecificFileName*). If you wish, you can use the macro %mac% that will be replaced with the MAC address of the unit.
4. Automatic update configuration
   - Configure the Download On Restart (*configFileAutoUpdateOnRestartEnable*) if you wish the unit to check for new firmware at each start.
   - Configure the Download Periodic Update (*configFileAutoUpdatePeriodicEnable*) if you wish the unit to check for new firmware periodically.
   - If you have enabled the periodic update, you can configure the frequency with three parameters:
     - Period (*confiFileAutoUpdatePeriod*)
     - Time Unit (*confiFileAutoUpdateTimeUnit*)
     - Time of day (*confiFileAutoUpdateTimeOfDay*)
5. Encryption
   - When using encryption, enable the Configuration File Encryption (*configFilePrivacyEnable*).
   - Configure the Generic Configuration File Password (*configFilePrivacyGenericSecret*) and the Specific Configuration File Password (*configFilePrivacySpecificSecret*).
6. Here is what the configured interface would look like for Methods 1 and 2. In this example, a Mediatrix 2102 with MAC address 0090F8XXXXXX will download two configuration files every day at 1h00 (24h format) on the HTTP server

httpserver.media5corp.com. The unit will fetch the files Mediatrix 2102.xml and 0090F8XXXXXX.xml in the Mtx_ConfigFiles folder. If the configuration has changed, the unit will reboot to apply the changes.

Method 1:



Method 2:



How to Automatically Configure your Mediatrix Units

With the auto-provisioning feature, it was explained how to configure the Mediatrix units to automatically fetch configuration files and firmware. However, as explained, this feature requires the Mediatrix units to be manually configured.

By using the Unit Manager Network (UMN) software, it is possible to have the Mediatrix units automatically configure themselves using pre-created configuration files.

Mediatrix units, by default, send DHCP requests to acquire an IP address. If the management server (UMN) vendor-encapsulated-option is found in the server's answer, the Mediatrix unit will contact the management server to acquire a configuration file.

DHCP Configuration

The value of the vendor-encapsulated-option (Option 43) needs to be formatted for the unit to understand the option.

- The prefix of the option is c8:04: (hexadecimal).
- The next value is the IP address encoded in hexadecimal format of the PC/server that hosts the UMN software. As example, if the UMN server has the IP address of 192.168.0.1, the encoded value would be: c0:a8:00:01.
- To get the final value of the vendor-encapsulated-option, concatenate the prefix and the IP address: c8:04:c0:a8:00:01

Please consult your DHCP server documentation for information on how to add vendor-encapsulated-options to DHCP answers. More details on the vendor-encapsulated-option can be found in your Mediatrix unit documentation.

UMN Configuration

When UMN receives a trap from a unit, the server will send a default configuration file. This configuration file needs to be modified with the correct settings to allow the Mediatrix unit to get its configuration.

- The default files are, by default, located in C:\Program Files\Unit Manager Network 3.2\UnitManager\DefaultCfgFile
- The files follow the following convention:

  DefaultConfigFile_[SoftwareVersion]_[ProductNumber][ProductType].cfg
- For example, the file sent to a Mediatrix 2102 with the firmware SIP v5.0 would be DefaultConfigFile_50_402FXS.cfg

The files need to be in CFG format. To create a sample CFG file, follow the instructions in the “Creating a configuration file” section.

Refer to the Unit Manager Network documentation for more detail.

Note: The Unit Manager Network server uses SNMP and TFTP to send the unit a configuration file. This automatic configuration technique is not recommended when either the units and/or the server are behind a NAT or a Firewall.