

Remote Firmware Update for FP Gateways Quick Guide



Version: 1.5.1

© 2018 -2021 FP InovoLabs GmbH

www.inovolabs.com

Publication date: 23/02/2021

This manual is protected by copyright. Any further dissemination is only permitted with permission from the issuer. This also applies to copies, microfilms, translations, and storing and processing in electronic systems.

Trade and brand names used in this manual are registered trademarks of the applicable companies even if they are not designated as such explicitly.

Table of contents

| | | |
|-----|--|---|
| 1 | INTRODUCTION | 3 |
| 2 | TIXML CONFIGURATION | 4 |
| 2.1 | Dynamic reconfiguration | 4 |
| 2.2 | References | 4 |
| 2.3 | Triggering the web update using the FwUpdate TiXML command | 4 |
| 3 | DETAILS ON THE PARAMETERS | 5 |
| 3.1 | Layout of the update.xml control file..... | 5 |
| 3.2 | TiXML configuration | 6 |
| 3.3 | Layout of the Tixi.Gate_FW.tar.gz.md5 checksum file | 7 |

1 Introduction

There is an ever increasing requirement to perform a firmware update on FP gateways in the field without having to be on site or enable certain ports on routers. The FP gateway should download the update from a web server and install it automatically.

The update should be usable on specific, targeted device groups:

- Device types
- Serial number ranges
- Firmware versions
- Customers or other ID options if the serial number is not known for certain.

Principle function

- Configure the remote FW update via TiXML
 - The remote FW update is switched off by default.
 - A TiXML database can be used to activate the remote FW update.
 - The update mechanism can be started automatically or using a TiXML command.
- **Collecting the control file from the web server**

The FP gateway collects an xml control file cyclically (e.g. 1x per day) from an update URL e.g. <http://www.tixi.com/fw-updates/update.xml>
- **Download the firmware**
- **Import the update**
- **Restart the system**

Example

The firmware for an FP S-ENGuard HE671 is to be updated. Customer web server:
<http://www.customer.de>

Device data:

| | |
|---------------------|---|
| Serial number: | 04223067 |
| Installed firmware: | 5.0.2.6 |
| Target firmware: | 5.0.3.8 |
| Download time: | daily at 23:00 |
| Update time: | immediately after downloading |
| Update server URL: | http://www.customer.de/fw-updates/5-0-3-8 |

File update.xml

The `update.xml` file must first be created in ASCII format.

```
<?xml version="1.0" encoding="UTF-8"?>
<firmware>
  <target firmware="5.0.2.6" serial="04223067" />
  <version _="5.0.3.8" />
  <type _="FW" />
  <url _="http://www.customer.de/fw-updates/5-0-3-8/Tixi.Gate_FW.tar.gz" />
</firmware>
```

Web server preparation

The `Tixi.Gate_FW.tar.gz`, `Tixi.Gate_FW.tar.gz.md5` and `update.xml` files must be stored in a director on the web server. In the example, we will use the directory `/fw-updates/5-0-3-8/`

It is best to use a web browser to check whether all three files can be downloaded.

2 TiXML configuration

The following database must be imported into the device using TICO.

```
[<SetConfig _="ISP" ver="y">
<TixiWebUpdate>
  <Enabled _="1" />
  <CheckForUpdates _="23.00" />
  <XmlPath _="http://www.customer.de/fw-updates/5-0-3-8/update.xml" />
  <RetryTimes _="2,5,10,30" />
</TixiWebUpdate>
</SetConfig>]
```

After implementing the TiXML configuration, the device must be restarted. The update mechanism is then activated.

In the example, the update mechanism downloads the `update.xml` file daily at 23:00 and checks whether new FW is available.

If the data in the `update.xml` file “matches”, the firmware is downloaded and installed.

The device is then restarted. The configuration and all log data are retained.

2.1 Dynamic reconfiguration

The process to control the update can be controlled dynamically. To do this, the process checks the settings for the **Enabled** and **CheckForUpdates**. If you change the settings for these parameters, the system saves the changes without restarting.

2.2 References

References can also be used for the **Enabled** and **CheckForUpdates** entries, e.g.:

```
<Enabled _="&#xae;/PARAM/Parameter/WebUpdate/Enabled;" />
<CheckForUpdates _="&#xae;/PARAM/Parameter/WebUpdate/CheckForUpdates;" />
```

The system then collects the configuration values from the referenced database (this is the database after the reference character `®`). This is generally the "PARAM" database.

2.3 Triggering the web update using the FwUpdate TiXML command

The `FwUpdate` TiXML command triggers a one-time download of the `update.xml` file.

The command can be called both directly (e.g. TICO) and in an `EventHandler`.

Syntax: `<FwUpdate/>` or `<FwUpdate _="XmlPath"/>`

The **XmlPath** is optional, the command can therefore be executed without specifying the **XmlPath**. In this case, the path is taken from the configuration database. If "XmlPath" is specified, the entire URL must always be specified!

The TiXML command can be triggered both manually (direct execution, e.g. via TICO) and using an event!

New time parameter for [CheckForUpdates](#)

The **CheckForUpdates** parameter should have an additional special value "Cmd":

```
<!-- only check the update if the "FwUpdate" command is executed -->
<CheckForUpdates _="Cmd" />
```

In this case, the update.xml file is not downloaded from the server cyclically but only when the FwUpdate TiXML command is called.

3 Details on the parameters

3.1 Layout of the update.xml control file

```
<?xml version="1.0" encoding="UTF-8"?>
<firmware>
  <title>Tixi FW Update for HE 671</title>
  <target hardware="HE671" firmware="5.0.0.56" serial="04221119"
    customPath="/LicenseRef/HW_Rev" customValue="H5-B600 V2.0" />

  <!-- Official new firmware 5.0.0.62 -->
  <version="5.0.0.62" />
  <build="00" />
  <type="FW" />
  <updatetime="2013/11/12,10:40:59" />
  <url="http://www.tixi.com/fw-updates/G6/Tixi.Gate_FW.tar.gz" />

  <!-- ... possibly further parameters /-->
</firmware>
```

Explanation of the elements

| | |
|---|--|
| <code><title>Title</title></code> | The title can be specified freely and is only of an informative nature |
| <code><target></code> | |
| <code>hardware</code> | Optional: Target hardware Must be compared with the value in <code>LicenseRef/ProdName</code> . The update is only performed if the values are identical. |
| <code>firmware</code> | Optional: Installed FW version The update is only performed if this FW is installed. |
| <code>serial</code> | Optional: Serial number (max. 8 characters) The update is only installed on devices with this SN Wildcards permitted: <code>serial="04221*"</code> : SNs starting with "04221" Wildcards are only permitted once. All characters following a wildcard are ignored: <code>serial="0421*12*"</code> is identical to <code>serial="0421*"</code> |
| <code>customPath</code> | Optional: Permits specifying any path within the System/Properties, e.g. <code>System/Properties/LicenseRef/Oem</code> |

| | |
|--------------|--|
| customValue | Optional value that the customPath must have for the update to be performed. Only makes sense in conjunction with customPath. e.g. /LicenseRef/HW_Rev _="H5-B600 V2.0" |
| <version> | Version number of the firmware that is to be installed |
| <build> | Optional: Build number of the firmware that is to be installed |
| <type> | Type of firmware that is to be installed. type="FW": Firmware or Firmware+Kernel type="Uboot": Uboot type="Kernel": Kernel only |
| <updatetime> | Optional: Date and time for installing the update that was downloaded |
| <url> | Download URL for the firmware and the *.md5 file |

3.2 TiXML configuration

The following parameters are defined in the TiXML configuration file:

```
[<SetConfig _="ISP" ver="y">
<!-- Definition of the update database -->
<TixiWebUpdate>
  <!-- 0 = disabled (default); 1 = enabled -->
  <Enabled _="1" />
  <!-- Time at which the device is to download the update.xml file -->
  <CheckForUpdates _="01.00" />
  <!-- XmlPath: Web server path, e.g. http://www.customer.de/update.xml: ) -->
  <!-- Optional: Path to the xml file (subdirectory on Tixi web server) -->
  <!-- XmlPath _="Customer" is expanded to:
  http://www.tixi.com/fw-updates/Customer/update.xml -->
  <XmlPath _="Customer" />
  <!-- Optional: Repeat after x minutes in the event of an error -->
  <RetryTimes _="2,5,10,30" />
</TixiWebUpdate>
</SetConfig>]
```

The **TixiWebUpdate** database can be queried via the following web server path:

[http://\[IP\]/System/Config/ISP/TixiWebUpdate](http://[IP]/System/Config/ISP/TixiWebUpdate)

Result as an example:

```
<TixiWebUpdate>
  <Enabled _="1" />
  <CheckForUpdates _="01.00" />
  <XmlPath _="Customer" />
  <RetryTimes _="2,5,10,30" />
</TixiWebUpdate>
```

3.3 Layout of the Tixi.Gate_FW.tar.gz.md5 checksum file

The update is only performed correctly if the checksum file matches the firmware.

FP InovoLabs delivers the `Tixi.Gate_FW.tar.gz.md5` file with each new firmware.

The `Tixi.Gate_FW.tar.gz.md5` file consists of one line only:

```
3d9b888eb3e6320181bceffcc3ce4a0d  /tmp/Tixi.Gate_FW.tar.gz
```

The line begins with the md5 checksum for the `Tixi.Gate_FW.tar.gz` file (32 characters).

There are then 2 spaces and the text `/tmp/Tixi.Gate_FW.tar.gz`