KB Name	eSync - Receiving data over HTTPS		
Type	How To		
Since revision	eSync 1.5		
KB Number	KB-0058-0	Build	24
Mod date	14. September 2014		

eSync - Receiving data over HTTPS

1 Introduction

Natively, the data transfer between eWON and eSync is done over an HTTP link. However when eSync is hosted on Internet, security must be taken in account and HTTP is not a secure protocol.

For security reason HTTPS is recommended more and more. The HTTPS protocol ensures encryption of data exchanges and the server identity.

This KB will show you how to configure your eSync server to listen for HTTPS requests and how to configure the eWON to send the data out using HTTPS.

2 HTTPS Keys and Certificates

HTTPS protocol is a HTTP protocol encrypted using OpenSSL technology.

OpenSSL uses certificates to identify Web Server and key files to encrypt data.

These certificates and keys can be generated from OpenSSL directly. However, to be trusted on Internet, your eSync certificate must be signed by trusted certificate authorities such as Thawte, VeriSign, etc.
Inside this document we use StartSSL (www.startssl.com). StartSSL delivers SSL certificates for free, which can be handy to test eSync/HTTPS setups.

Note

- A server certificate is associated to a domain name. Therefore you need to own a domain name (e.g : mydomain.com) and this domain name must be associated to the IP address of your eSync server.
- In case the eSync server does not have a fixed IP address and you use DynDNS, DynDNS.com can also issue server certificates.

3 eSync Configuration

eSync is running an Apache Web Server. All Apache related files are located in "...\eSync\Apache24" (Default eSync Root Directory is "C:\eSync\").

KB Name	eSync - Receiving data over HTTPS		
Type	How To		
Since revision	eSync 1.5		
KB Number	KB-0058-0	Build	24
Mod date	14. September 2014		

3.1 Apache Configuration

Open the file "***httpd.conf***" located in "...\eSync\Apache24\conf" and do the following operations :

- Replace "Listen 80" (80 = HTTP port) by "Listen 443" (443 Standard HTTPS port). To avoid port conflicts, it is recommended to check that the port 443 is not already used by a third party program (Using `netstat` command for example)

> **Note** HTTP and HTTPS can be both enabled on eSync. For this, use the configuration lines "Listen 80" **and** "Listen 443" (on 2 separate lines) in the file httpd.conf

- Uncomment the line `LoadModule ssl_module modules/mod_ssl.so` (remove the # in front of the line).
- Add the content :

```
<VirtualHost _default_:443>"
   ServerName mydomain.be
   ErrorLog "C:/eSync/Apache24/conf/error_log"
   TransferLog "C:/eSync/Apache24/conf/access_log"
   SSLEngine on
   SSLProtocol all -SSLv2
   SSLCipherSuite ALL:!ADH:!EXPORT:!SSLv2:RC4+RSA:+HIGH:+MEDIUM
   SSLCertificateFile "C:/eSync/Apache24/conf/mysite.crt"
   SSLCertificateKeyFile "C:/eSync/Apache24/conf/mysite.key"
   SSLCertificateChainFile "C:/eSync/Apache24/conf/ca.pem"
  CustomLog C:/eSync/Apache24/logs/ssl_request_log \
     "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
</VirtualHost>
```

and modify the value of the following parameters :

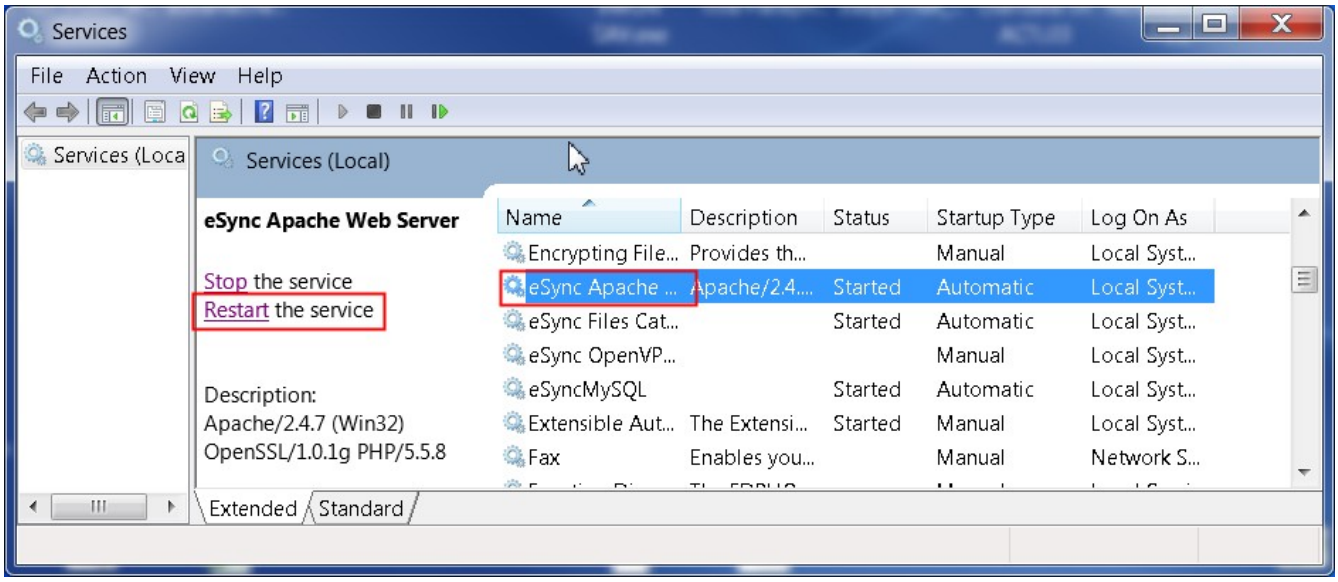
ServerName	type your domain name
SSLCertificateFile	type the path to your server certificate
SSLCertificateKeyFile	type the path to your server key
SSLCertificateChainFile	type the path to your CA certificate

KB Name	eSync - Receiving data over HTTPS		
Type	How To		
Since revision	eSync 1.5		
KB Number	KB-0058-0	Build	24
Mod date	14. September 2014		

Warning Check that all directory paths defined above exist on your system.

- Copy your certificates and key files in the right directory. See directories configured at point 3 for the parameters SSLCertificateFile, SSLCertificateKeyFile and SSLCertificateChainFile.

When everything is setup, you can then restart the service "eSync Apache Web Server" from the Windows services panel (Control Panel\Administrative Tools\Services)



3.2 Troubleshooting

In case the "eSync Apache" service does not restart, it probably means that there is a mistake in your configuration, certificate or key file.

Error logs can be retrieved from different locations :

- C:\eSync\Apache24\conf\ (File : error_log)
- C:\eSync\Apache24\logs (File : error.log)

For debugging purposes, you can also stop the Apache service and start the Apache server manually. For this, open a dos prompt and run "C:\eSync\Apache24\bin\httpd.exe".

The errors are directly returned in the DOS prompt.

Sometimes the process returns immediately but without any errors displayed. In this case, check the error file C:\eSync\Apache24\logs\error.log

3.2.1 Possible issues

- Private Key is protected by a pass-phrase.

  Apache Web Server does not support pass-phrase protection.
  To disable it, run the command : `C:\eSync\Apache24\bin\openssl.exe rsa -in server.key.org -out server.key`

  Rem : StartSSL provides pass-phrase protected Private Keys.

- Key does not match with Certificate

  In this case, you will see the following error in the log file "C:\eSync\Apache24\conf\error_log"

  ```
  [Wed May 07 11:27:17.093067 2014] [ssl:emerg] [pid 6796:tid 488] AH02238: Unable to configure RSA server private key
  [Wed May 07 11:27:17.093067 2014] [ssl:emerg] [pid 6796:tid 488] SSL Library Error: error:0B080074:x509 certificate routines:X509_check_private_key:key values mismatch
  ```

  To verify that, you must display the modulus of the key and the certificate and

then check that they match

```
OpenSSL> rsa -noout -modulus -in
"C:\eSync\Apache24\conf\ssl.key"
Modulus=AB78EAB0488FFA651FF108B3B60A110076D2C0CF35089665F4D5C4F0
1B30E21509629DE1A89D400445CD0FBFDC8C1B2063FE29B4DBE1A092238748A6
523B8774D63410A9F4C801F75997A546C4C704C0DC984051798DD381E785B0B7
BE41A46ACAF884C839990CEC4DBA6208E3ACB37AD070A7AEDB29DE658389337F
6042872ABA4F2F3D2F8998C67C359978B4D25965C6D59A6CFC1260F53296EF07
B77624276DB0C08C82D6AD58DAE81E4A898BAD511D85F878C0E5E79242214745
3096FD0D145FAA738A019384A06055132EA511081B76C6C7A93CBF65AB7F9841
B4D71684DAB8766D4CDBBA9C1905A716A8A505C8CFD25C4C0BEE46733232BEAE
21AF8C83
```

```
OpenSSL> x509 -noout -modulus -in
"C:\eSync\Apache24\conf\ssl.crt"
Modulus=BD60243340FD1ADA797C390944B8B9EF7D0977C96C0841D01A53F5EA
AAC66DF1CE38BED470B7500ED20078D0B1C976FE9F02774C7790747CCE060065
70A3242B14DB46CA95C8FDB7A98BBB4351714A7CCEB7CDD90DAA93A51073A589
2D7F99ED74A79FD08231FC57E835A4F8B78390AF9EE66AF3B68A6D6797A29615
83ACB9A516519F01B225D802952D51370E882DFC9FC706A21E26047904F79AD8
879EA3042E21E25D0D2CCD02175059B09ACEC8AAB01570F9F016261FEFC6C2DA
2A222A258B97D89C9C5C2B3D2C613AF518EB1F053A90ED371E7846E2F52DDE3A
B1FCC1FFCAE9C66CC5B97811047CC832508A8D55573C7B4F45289C25B4A1F226
A061EA39
```

If they do not match, reissue your certificates.

- Incorrect Server Name

  In this case, in C:\eSync\Apache24\conf\error_log, you get the log :
  ```
  [Wed May 07 11:16:05.559920 2014] [ssl:warn] [pid 7256:tid 488]
  AH01909: RSA certificate configured for LAP146.AD.ACTL.BE:443
  does NOT include an ID which matches the server name
  ```

  It means that the domain name used to create the certificate does not match with your web server domain name.

  Check the value of the parameter "ServerName" in httpd.conf.

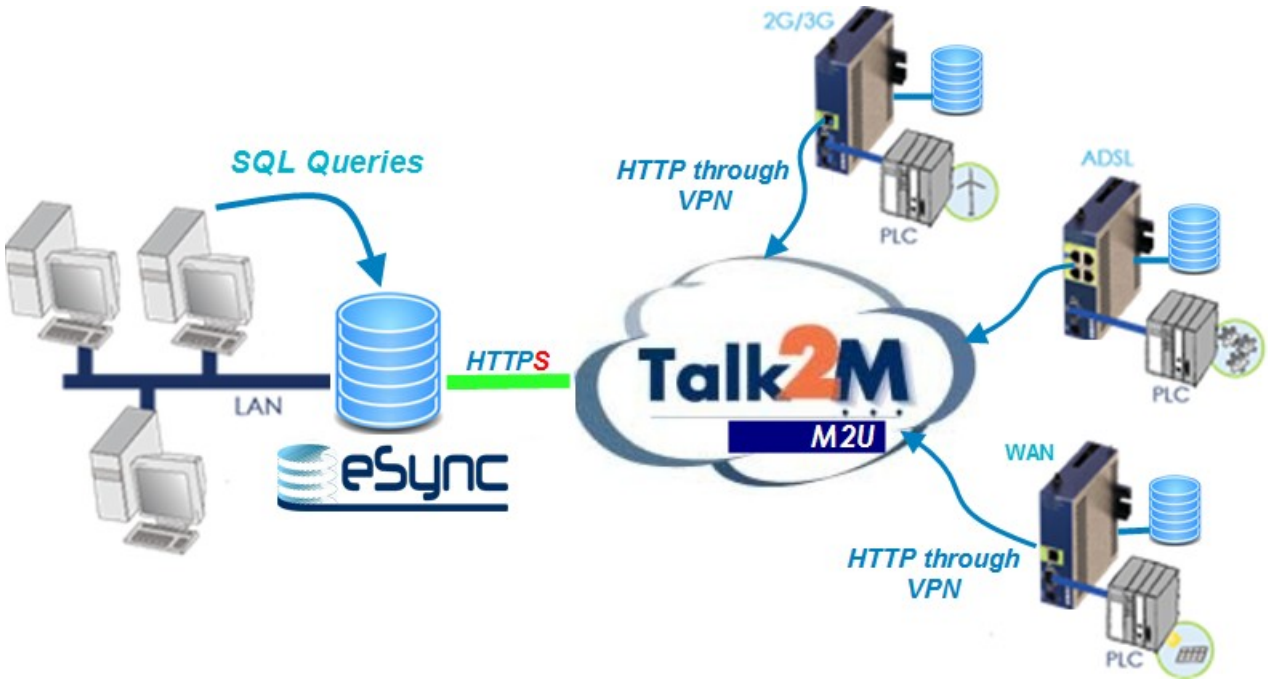
KB Name	eSync - Receiving data over HTTPS		
Type	How To		
Since revision	eSync 1.5		
KB Number	KB-0058-0	Build	24
Mod date	14. September 2014		

4 eWON Configuration

Natively eWON only supports HTTP. So eWON is not able to post data to eSync directly using HTTPS.

The solution is to use the M2U service of Talk2M (www.talk2m.com). M2U will act as a HTTP to HTTPS Gateway for the eWON.

The idea is to use the secured VPN connection established between the eWON and Talk2M server to send out the data using HTTP protocol. M2U receives these data and forward the data to eSync in HTTPS.



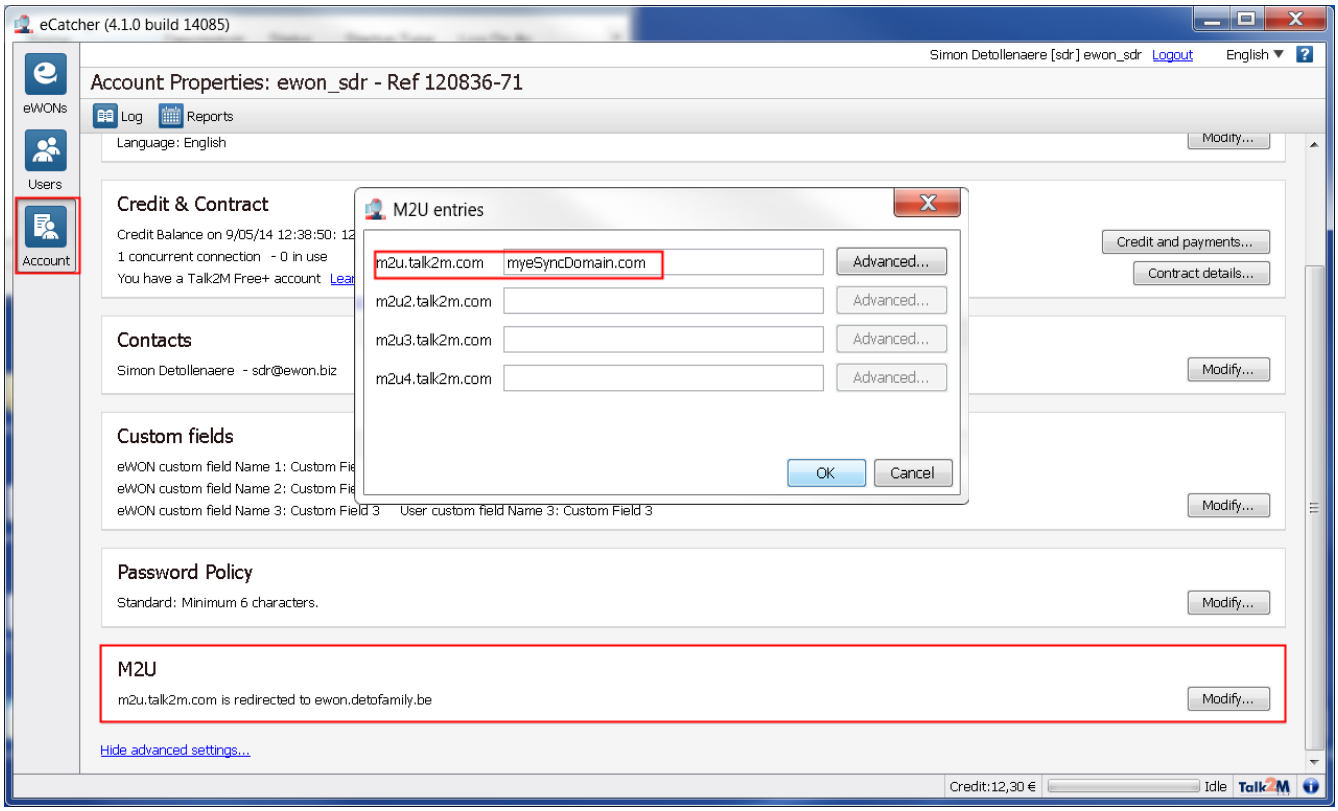
With this topology, you can see that the data are encrypted from the start to the end, either in VPN (between eWON and Talk2M/M2U) or in HTTPS (between Talk2M/M2U and eSync).

Note To configure your eWON on Talk2M, follow the guide Talk2M – Getting Started Free +.

KB Name	eSync - Receiving data over HTTPS		
Type	How To		
Since revision	eSync 1.5		
KB Number	KB-0058-0	**Build**	24
Mod date	14. September 2014		

To configure the M2U service to send the eWON data to your eSync server, you need to associate your eSync Domain Name to one of the 4 M2U URL links.

To do this, connect to your Talk2M account using eCatcher and open the menu Account > M2U :



Encode here the url of your eSync server.

On the eWON, inside the Data Management configuration window, you'll then need to encode **m2u.talk2m.com** for the Server URL.