

Ist es möglich den GridVis Dienst auf https (gesicherte Verbindung) umzustellen?

Hier die offizielle Beschreibung ab GridVis 8.1.25

HTTPS-Verschlüsselung

#ALT:

Frage:

Das Passwort für den Login wird im Klartext übertragen und kann mit Wireshark ausgelesen werden, anbei ein Screenshot. Jetzt unsere Frage, ist es möglich den Dienst anstatt auf http auf https laufen zu lassen, damit das Passwort verschlüsselt übertragen wird?

The screenshot shows a Wireshark capture of an HTTP request. The packet list pane shows a GET request to /energyservice/secure/info/version/all. The packet details pane shows the request body as a JSON object with a 'username' field containing the value 'admin' and a 'password' field containing '3m5t1tza'. The packet bytes pane shows the raw bytes of the request body, which are highlighted in red in the original image.

```
Frame 1321: 567 bytes on wire (4536 bits), 567 bytes captured (4536 bits) on interface 0  
Ethernet II, Src: RealtekUrb (0c8b35ca4ab7b), Dst: SophosXp-rt-01 (08:1a:8c:76:e4:01)  
Internet Protocol Version 4, Src: 192.168.1.215, Dst: 192.168.30.200  
Transmission Control Protocol, Src Port: 64807, Dst Port: 8080 (8080), Seq: 454, Ack: 824, Len: 513  
Source Port: 64807  
Destination Port: 8080  
[Stream index: 9]  
[TCP segment len= 513]  
Sequence number: 454 (relative sequence number)  
Next sequence number: 967 (relative sequence number)  
Acknowledgment number: 824 (relative ack number)  
Header length: 20 bytes  
Flags: 0x01 (PSH, ACK)  
Window size value: 251  
[calculated window size: 251]  
[window size scaling factor: -1 (unknown)]  
Checksum: 0xc118 (validation disabled)  
Urgent pointer: 0  
[SQ/ACK analysis]  
[Application Transfer Protocol]  
JavaScript Object Notation: application/json  
#json  
+ Header Key: "username"  
+ String value: admin  
+ Header Key: "password"  
+ String value: 3m5t1tza
```

Antwort:

Der Aufwand bei SSL liegt zu 95% beim Kunden. Dieser muss DNS und Zertifikat verwalten. Die Software kann das Zertifikat dann verwenden. Als Alternative schaltet der Kunde dafür einen eigenen SSL-Proxy-Server wie "apache" oder "nginx" davor, deswegen ist der Nutzen sehr gering, wenn er das direkt in der GridVis könnte. Anders sehe es aus, wenn die GridVis selbst Zertifikate erstellt. Dann ist die Verbindung zwar verschlüsselt, aber der Browser unterstützt das nicht.

Hier ein Beispiel:

<https://legacy.thomas-leister.de/apache-reverse-proxy-mit-ssl-support-einrichten/>

IIS Server:

<https://docs.microsoft.com/en-us/iis/extensions/url-rewrite-module/reverse-proxy-with-url-rewrite-v2-and-application-request-routing>