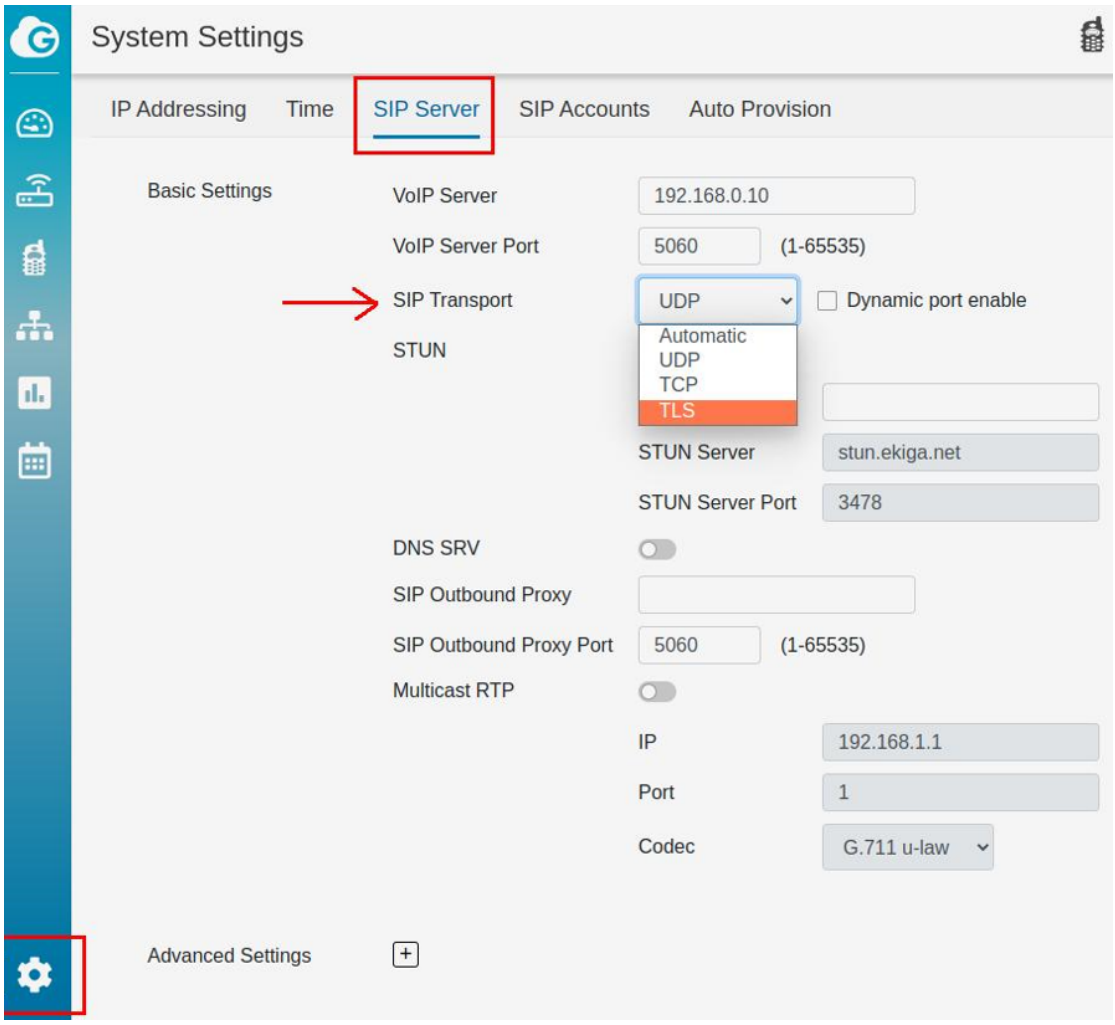
Release Note for TLS configuration in DuraFon-Roam

1. Overview

DuraFon-Roam supports TLS1.0, TLS 1.1 and TLS 1.2 and TLS1.3 for website GUI and SIP messaging.
For website GUI, as a TLS client role in DuraFon-Roam, it follows the TLS web server to specify the version of TLS.

For SIP messaging, you need to select “System Settings->SIP Transport” with TLS item as the photo.



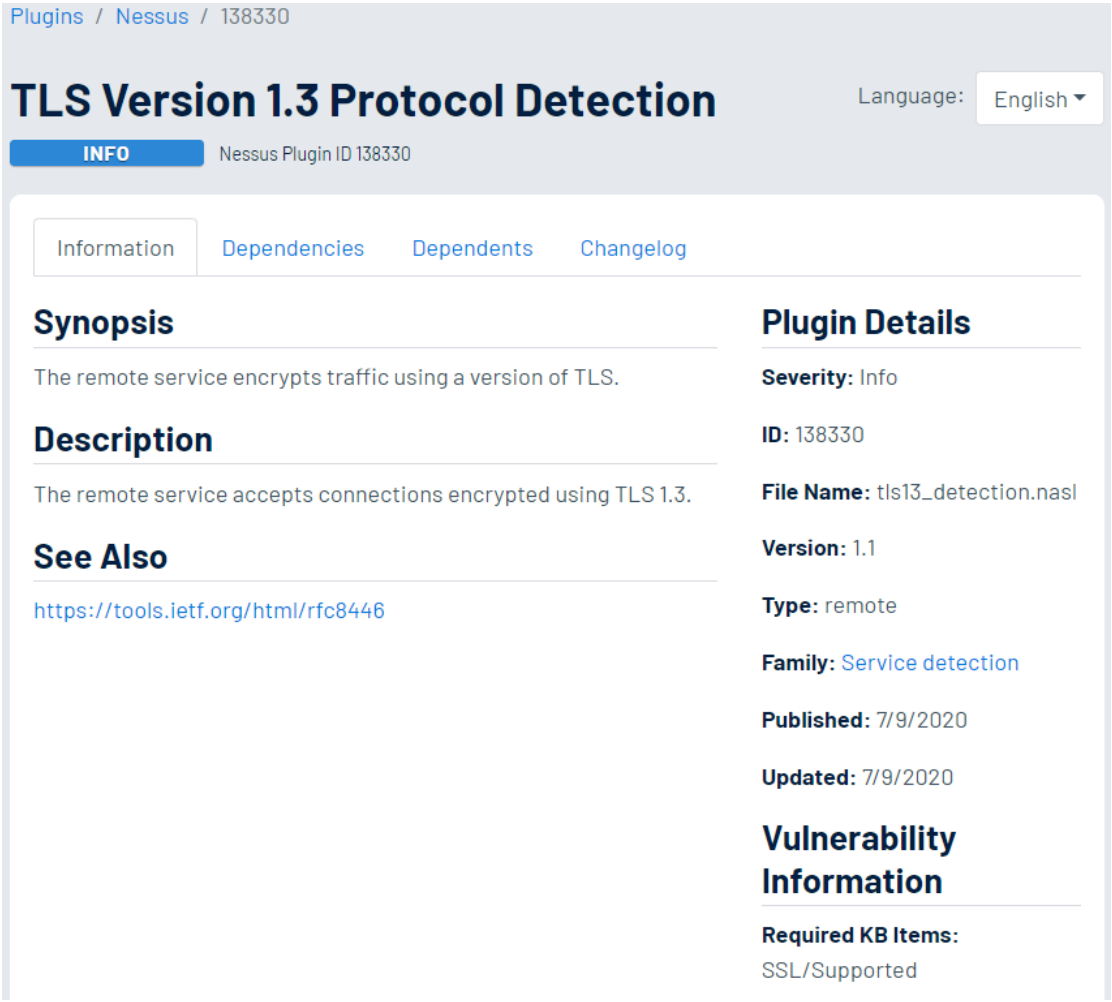
Once TLS is selected the phone will always negotiate the highest possible TLS version in the handshaking process. TLS 1.3, 1.2, 1.1 and 1.0 are supported.
Note that there are no other Certificates setting required.

2. Test Scan

Use Tenable Nessus to do Vulnerabilities by Host. According to the below item 37 in test cases, DuraFon-Roam supports TLS 1.3.

Item	Severity	CVSS v2.0	Plugin	Name
1	MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
2	MEDIUM	6.4	57582	SSL Self-Signed Certificate
3	MEDIUM	5.8	42263	Unencrypted Telnet Server
4	MEDIUM	4.3	85582	Web Application Potentially Vulnerable to Clickjacking
5	LOW	2.6	26194	Web Server Transmits Cleartext Credentials
6	INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
7	INFO	N/A	45590	Common Platform Enumeration (CPE)
8	INFO	N/A	11002	DNS Server Detection
9	INFO	N/A	54615	Device Type
10	INFO	N/A	35716	Ethernet Card Manufacturer Detection
11	INFO	N/A	86420	Ethernet MAC Addresses
12	INFO	N/A	84502	HSTS Missing From HTTPS Server
13	INFO	N/A	43111	HTTP Methods Allowed (per directory)
14	INFO	N/A	10107	HTTP Server Type and Version
15	INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
16	INFO	N/A	91634	HyperText Transfer Protocol (HTTP) Redirect Information
17	INFO	N/A	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
18	INFO	N/A	50345	Missing or Permissive X-Frame-Options HTTP Response Header
19	INFO	N/A	11219	Nessus SYN scanner
20	INFO	N/A	19506	Nessus Scan Information
21	INFO	N/A	11936	OS Identification
22	INFO	N/A	117886	OS Security Patch Assessment Not Available
23	INFO	N/A	70657	SSH Algorithms and Languages Supported
24	INFO	N/A	153588	SSH SHA-1 HMAC Algorithms Enabled
25	INFO	N/A	10267	SSH Server Type and Version Information
26	INFO	N/A	56984	SSL / TLS Versions Supported
27	INFO	N/A	10863	SSL Certificate Information

28	INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
29	INFO	N/A	21643	SSL Cipher Suites Supported
30	INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
31	INFO	N/A	94761	SSL Root Certification Authority Certificate Information
32	INFO	N/A	156899	SSL/TLS Recommended Cipher Suites
33	INFO	N/A	22964	Service Detection
34	INFO	N/A	21642	Session Initiation Protocol Detection
35	INFO	N/A	25220	TCP/IP Timestamps Supported
36	INFO	N/A	136318	TLS Version 1.2 Protocol Detection
37	INFO	N/A	138330	TLS Version 1.3 Protocol Detection
38	INFO	N/A	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
39	INFO	N/A	10281	Telnet Server Detection
40	INFO	N/A	10287	Traceroute Information
41	INFO	N/A	91815	Web Application Sitemap
42	INFO	N/A	11032	Web Server Directory Enumeration
43	INFO	N/A	10386	Web Server No 404 Error Code Check
44	INFO	N/A	10302	Web Server robots.txt Information Disclosure
45	INFO	N/A	10662	Web mirroring
46	INFO	N/A	106628	lighttpd HTTP Server Detection
47	INFO	N/A	66717	mDNS Detection (Local Network)



The detail information is referred to

Test_Scan_SP938 BSC_v1.0.1.3.html

~End of Documentation