Perfect Wireless Experience
完美无线体验

FIBOCOM_L610_AT_Commands_User_Manual_SSL

Version: V1.0.0

Date: 2019-01-26

Applicability Type

No.	Type	Note
1	L610	NA

Copyright

Attention

The document is subject to update from time to time owing to the product version upgrade or other reasons. Unless otherwise specified, the document only serves as the user guide. All the statements, information and suggestions contained in the document do not constitute any explicit or implicit guarantee.

Trademark

The trademark is registered and owned by Fibocom Wireless Inc.

Versions

Version	Author	Accessor	Approver	Date	Remarks
V1.0.0	sundaqing	longzhongyou	longzhongyou	2019-01-26	Initial version

Contents

1 SSL

1.1 +GTSSLFILE, Load certificates or keys

1.1.1 Description

This command is used to load the CA certificate of SSL, KEY, or the local certificate of trust.

1.1.2 Syntax

Command	Response/Action	Note
+GTSSLFILE=<file_type>,<file_len>	OK or ERROR	Set command sets the type and length of the loading certificate, CERTFILE and KEYFILE indicate which type of client public key certificate or key are loaded (generally for the situation of two-way authentication, when the client sends the public key certificate to the server, i.e., the server needs to validate the client's legitimacy). TRUSTFILE indicates that the trust certificate or root certificate is loaded into the machine, where the purpose of the certificate is to verify the validity of the server (both one-way authentication and bidirectional authentication may need to be validated (specifically by +GTSSLMODE chose)), Loading TRUSTFILE file support up to 40.
+GTSSLFILE?	+GTSSLFILE: <file_type>,<file_num> OK e.g. +GTSSLFILE: CERTFILE,0 +GTSSLFILE: KEYFILE,0	Read command queries whether the type of certificate has been loaded, where CERTFILE and KEYFILE can be at most 1,TRUSTFILE can be more than one. For example, there is no certificate file type of CERTFILE or KEYFILE; but have a TRUSTFILE certificate type ;

Command	Response/Action	Note
	+GTSSLFILE: TRUSTFILE,1	
+GTSSLFILE=?	+GTSSLFILE: ("CERTFILE,KEYFILE ,TRUSTFILE"),(list of supproted <file_len>s) OK	Test command can query the type and length of the loading certificate.

1.1.3Attributes

Pin Restricted	Persistent	Sync Mode	Effect Immediately	Time of duration
No	No	Yes	Yes	< 1s

1.1.4 Defined Values

<file_type>：Only use one type of file among "CERTFILE", "KEYFILE" and "TRUSTFILE"

<file_len>：length of certificate (which is the length of the file after encoding by Base64 format),range is 4-8192bytes

<file_num>：Represents the number of loaded certificates

Note:

If module power down, all certificates are lost. The CERTFILE and KEYFILE at module can only load one of them; TRUSTFILE, trust certificate, can load up to 40. At present, Command only can support to add (loading) and query certificates, but not support to delete and modify certificates. And most importantly, any type of file loaded into module must be encoded through base64 format. When module goes to ODM mode and appear ">", if module do not receive any data for more than 12 seconds, it will automatically exit ODM mode and return ERROR.

1.2 +GTSSLMODE, Set whether to verify the certificate of the server

1.2.1 Description

This command can set whether the client (module)verifies certificate downloaded from server or not, 1 indicates verify and 0 indicates not. If verify set, then there must be at least one trust certificate in the local trust client list, (i.e., we can get at least one file in the TRUSTFILE field of AT+GTSSLFILE?)

1.2.2 Syntax

Command	Response/Action
+GTSSLMODE=<checkmode>	OK or ERROR
+GTSSLMODE?	+GTSSLMODE: <checkmode> OK
+GTSSLMODE=?	+GTSSLMODE: (list of supported <checkmode>s) OK

1.2.3Attributes

Pin Restricted	Persistent	Sync Mode	Effect Immediately	Time of duration
No	No	Yes	Yes	< 1s

1.2.4 Defined Values

<checkmode>： integer type and range 0-1

0 indicates no verify (default setting)

1 indicates need to verify

1.3 +GTSSLERR, Get the SSL error code

1.3.1 Description

The function of this command is to query the error code generated by the last SSL error connection.

1.3.2 Syntax

Command	Response/Action	Note
+GTSSLERR	OK or +GTSSLERR: <err_code> OK	If SSL is no error in the connection, return OK, otherwise the error code returned from the last connection is returned.
+GTSSLERR?	OK or +GTSSLERR: <err_code> OK	If there are no error occurred in the SSL connection, then module will return OK, otherwise will return the error code occurred at the last connection.

1.3.3Attributes

Pin Restricted	Persistent	Sync Mode	Effect Immediately	Time of duration
No	No	Yes	Yes	< 1s

1.3.4 Defined Values

<err_code>:
-0: normal;
-1: indicates parameter error;
-2: indicates the SSL connection failed to execute;
-3: indicates file read error;
-4: indicates that the connection cannot be completed because socket cannot read or write effectively;
-5: indicates that the read and write operations cannot be completed because the socket cannot be read effectively;
-6: indicates that the read and write operations cannot be completed because the socket cannot be written effectively;
-7: indicates for SSL protocol error;
-8: indicates that the server did not respond to handshake the client initiated;
-9: indicates that the SSL connection is actively disconnected by the server;
-10: indicates an unknown error;
-11: indicates certificate validation failed (lack of TRUSTFILE, trust certificate or certificate expiration);
-12: indicates that the certificate length information does not match;
-13: indicates missing RSA encryption certificate;
-14: indicates missing RSA signature certificate;
-15: indicates that the public key information parameter cannot be found;
-16: indicates the unknown certificate type;
-17: indicates certificate file at the client error;

-18: indicates key file at the client error;
-19: indicates a trusted server certificate file error;
-20: indicates data timeout when the SSL session is received.

1.4 +GTSSLVER, Set and query the version of the SSL handshake protocol

1.4.1 Description

The command function is to set up or query the version of the SSL handshake protocol.

1.4.2 Syntax

Command	Response/Action
+GTSSLVER=<sslver>	OK or ERROR
+GTSSLVER?	+GTSSLVER: <sslver> OK
+GTSSLVER=?	+GTSSLVER: (list of supported <sslver>s) OK

1.4.3Attributes

Pin Restricted	Persistent	Sync Mode	Effect Immediately	Time of duration
No	No	Yes	Yes	< 1s

1.4.4 Defined Values

<sslver>: integer type and range 0-4
1: indicates the protocol version is SSL3.0;
2: indicates the protocol version is TLS1.0（Default）;
3: indicates the protocol version is TLS1.1;
4: indicates the protocol version is TLS1.2

1.5 +GTSSLCIPHER, Configure the encryption algorithm when establishing the connection

1.5.1 Description

The command function is to configure the encryption algorithm supported by the current product.

1.5.2 Syntax

Command	Response/Action
+GTSSLCIPHER=<cipalgID>,<cmd>	OK or ERROR
+GTSSLCIPHER?	+GTSSLCIPHER: (list of supported <cipalgID>s) OK list cipher algorithm ID that can be used or OK no cipher algorithm ID enabled, modem will load default cipher algorithms
+GTSSLCIPHER=?	+GTSSLCIPHER: (range of supported <cipalgID>s), (range of supported <cmd>s) OK

1.5.3Attributes

Pin Restricted	Persistent	Sync Mode	Effect Immediately	Time of duration
No	No	Yes	Yes	< 1s

1.5.4 Defined Values

<cipalgID>: integer type and range 1-31, each cipher algorithm ID is related with the corresponding

algorithm. Products on different platform have different correspondences between cipalgID and the related algorithm. The list of correspondences should been listed in single product manual.

Note:

if all of the algorithms are not configured, the device will load default algorithms, which should been informed in the product manual.

<cmd>: integer type, range 0, 1. cmd indicates whether to load the algorithm binded with the current cipher algorithm ID.

0 the algorithm mustn't be loaded when establishing the connection;

1 the algorithm should be loaded when establishing the connection;

cipalgID show below:

1 TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256

2 TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256

3 TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256

4 TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384

5 TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384

6 TLS-DHE-RSA-WITH-AES-256-GCM-SHA384

7 TLS-ECDHE-ECDSA-WITH-AES-256-CCM

8 TLS-DHE-RSA-WITH-AES-256-CCM

9 TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384

10 TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384

11 TLS-DHE-RSA-WITH-AES-256-CBC-SHA256

12 TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA

13 TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA

14 TLS-DHE-RSA-WITH-AES-256-CBC-SHA

15 TLS-ECDHE-ECDSA-WITH-AES-256-CCM-8

16 TLS-DHE-RSA-WITH-AES-256-CCM-8

17 TLS-ECDHE-ECDSA-WITH-CAMELLIA-256-GCM-SHA384

18 TLS-ECDHE-RSA-WITH-CAMELLIA-256-GCM-SHA384

19 TLS-DHE-RSA-WITH-CAMELLIA-256-GCM-SHA384

20 TLS-ECDHE-ECDSA-WITH-CAMELLIA-256-CBC-SHA384

21 TLS-ECDHE-RSA-WITH-CAMELLIA-256-CBC-SHA384

22 TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256

23 TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA

24 TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256

25 TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256

26 TLS-DHE-RSA-WITH-AES-128-GCM-SHA256
27 TLS-ECDHE-ECDSA-WITH-AES-128-CCM
28 TLS-DHE-RSA-WITH-AES-128-CCM
29 TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256
30 TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256
31 TLS-DHE-RSA-WITH-AES-128-CBC-SHA256

2 Example

Example1: Authentication certificate is not required, means MODE is 0

AT command ready

+SIM READY

at+gtsslfile?

+GTSSLFILE: CERTFILE,0

+GTSSLFILE: KEYFILE,0

+GTSSLFILE: TRUSTFILE,0

OK

at+gtsslmode?

+GTSSLMODE: 0// normal connection mode, do not need to verify the certificate

OK

at+mipcall=1,"cmnet"

OK

+MIPCALL: 10.79.220.142

at+mipopen=1,,"www.baidu.com",443,2

OK

+MIPOPEN: 1,1

at+mipclose=1

OK

+MIPCLOSE: 1,1

Example2: Setup needs authentication mode, but there is lack of trust certificates

at+gtsslmode=1

OK

at+gtsslmode?

+GTSSLMODE: 1

OK

at+mipopen=1,,"www.baidu.com",443,2

OK

+MIPOPEN 1,0 // connect fail

AT+GTSSLERR? // Query reason

+GTSSLERR: -11 //The certificate validation failed. First,

the reason may be that there is no TRUSTFILE certificate

at+gtsslfile? // query loading certificate Through the GTSSLFILE

+GTSSLFILE: CERTFILE,0

+GTSSLFILE: KEYFILE,0

+GTSSLFILE: TRUSTFILE,0 // lack of trust certificate ,means +GTSSLFILE:, TRUSTFILE, 0

OK

Example3: Setting requires authentication mode, system has a trusted certificate, but it does not connect because the time needs to be set. Because system will confirm whether the certificate has expired through to compare the current time to the time in the certificate.

at+gtsslmode=1 //Set to verify the desirable certificate mode

OK

at+gtsslmode?

+GTSSLMODE: 1

OK

AT+GTSSLFILE="TRUSTFILE",850 //Loading TRUSTFILE, trust certificate

>

....

OK

at+gtsslfile?

+GTSSLFILE: CERTFILE,0

+GTSSLFILE: KEYFILE,0

+GTSSLFILE: TRUSTFILE,1 //Not lack of trust certificate
OK

at+mipopen=1,,"114.255.225.39",20444,2

OK

+MIPOPEN 1,0 / / the connection failed

AT+GTSSLERR?

+GTSSLERR: -11/ / query error code, certificate verification failed, as certificate expired, but the above has been loaded to the certificate, Combining Example4

Example4: sets the current time based on the Example3 to facilitate verification of the certificate

AT+CCLK="15/01/23,15:30:36"//set time

OK

at+mipopen=1,,"114.255.225.39",20444,2

OK

+MIPOPEN: 1,1 //Connection success

AT+MIPCLOSE=1

OK

+MIPCLOSE: 1,1

Example5: one way of authentication: do not check server certificates

AT+GTSSLMODE?

+GTSSLMODE: 0

OK

AT+GTSSLFILE?

+GTSSLFILE: CERTFILE,0

+GTSSLFILE: KEYFILE,0

+GTSSLFILE: TRUSTFILE,0

OK

AT+GTSSLFILE=" CERTFILE",1334

>

….

OK

AT+GTSSLFILE="KEYFILE",1675

>

….

OK

AT+GTSSLFILE?

+GTSSLFILE: CERTFILE,1

+GTSSLFILE: KEYFILE,1

+GTSSLFILE: TRUSTFILE,0

OK

AT+MIPOPEN=1,,"188.93.19.231",5555,2

OK

+MIPOPEN: 1,1

+MIPRTCP:
1,201,350A576564204A616E2032312031353A35383A3034204D534B20323031350A576564204A
616E2032312031353A35383A3035204D534B20323031350A576564204A616E2032312031353A3
5383A3036204D534B20323031350A576564204A616E2032312031353A35383A3037204D534B20
323031350A576564204A616E2032312031353A35383A3038204D534B20323031350A576564204
A616E2032312031353A35383A3039204D534B20323031350A576564204A616E2032312031353A
35383A3130204D534B20323031350A576564204A616E2032312031353A35383A3131204D534B2
0323031350A576564204A616E2032312031353A35383A3132204D534B20323031350A576564204
A616E2032312031353A35383A3133204D534B20323031350A576564204A616E2032312031353A
35383A3134204D534B20323031350A576564204A616E2032312031353A35383A3135204D534B2
0323031350A576564204A616E2032312031353A35383A3136204D534B20323031350A576564204
A616E2032312031353A35383A3137204D534B20323031350A576564204A616E2032312031353A
35383A3138204D534B20323031350A576564204A616E2032312031353A35383A3139204D534B2
0323031350A576564204A616E2032312031353A35383A3230204D534B20323031350A576564204
A616E2032312031353A35383A3231204D534B20323031350A576564204A616E2032312031353A
35383A3232204D534B20323031350A576564204A616E2032312031353A35383A3233204D534B2
0323031350A576564204A616E2032312031353A35383A3234204D534B20323031350A576564204
A616E2032312031353A35383A3235204D534B20323031350A576564204A616E2032312031353A
35383A3236204D534B20323031350A576564204A616E2032312031353A35383A3237204D534B2
0323031350A576564204A616E2032312031353A35383A3238204D534B20323031350A576564204
A616E2032312031353A35383A3239204D534B20323031350A576564204A616E2032312031353A
35383A3330204D534B20323031350A576564204A616E2032312031353A35383A3331204D534B2
0323031350A576564204A616E2032312031353A35383A3332204D534B20323031350A576564204
A616E2032312031353A35383A3333204D534B20323031350A576564204A616E2032312031353A
35383A3334204D534B20323031350A576564204A616E2032312031353A35383A3335204D534B2
0323031350A576564204A616E2032312031353A35383A3336204D534B20323031350A576564204
A616E2032312031353A35383A3337204D534B20323031350A576564204A616E2032312031353A
35383A3338204D534B20323031350A576564204A616E2032312031353A35383A3339204D534B2
0323031350A576564204A616E2032312031353A35383A3430204D534B20323031350A576564204

A616E2032312031353A35383A3431204D534B20323031350A576564204A616E2032312031353A35383A3432204D534B20323031350A576564204A616E2032312031353A35383A3433204D534B20323031350A576564204A616E2032312031353A35383A3434204D534B20323031350A576564204A616E2032312031353A35383A3435204D534B20323031350A576564204A616E2032312031353A35383A3436204D534B20323031350A576564204A616E2032312031353A35383A3437204D534B20323031350A576564204A616E2032312031353A35383A3438204D534B20323031350A576564204A616E2032312031353A35383A3439204D534B20323031350A576564204A616E2032312031353A35383A3530204D534B20323031350A576564204A616E

+MIPRTCP: 1,201,2032312031353A35383A3531204D534B20323031350A576564204A61

Example6: Set current cipher algorithm to TLS_RSA_WITH_AES_256_CBC_SHA only

AT+COPS?
+COPS: 0,0,"CHINA MOBILE",7
OK

AT+MIPCALL=1,"CMNET"
OK

+MIPCALL: 10.109.197.168

AT+GTSSLCIPHER?
+GTSSLCIPHER: 1,2,3,4,5,6
OK

AT+GTSSLCIPHER=1,0
OK

AT+GTSSLCIPHER=2,0
OK

AT+GTSSLCIPHER=3,0

OK

AT+GTSSLCIPHER=4,0

OK

AT+GTSSLCIPHER=6,0

OK

AT+GTSSLCIPHER?

+GTSSLCIPHER: 5

OK

3 Appendix

CA certificate instance, note that this program supports only Base64 encoding format, as shown below:

-----BEGIN CERTIFICATE-----

MIIEUjCCA7ugAwIBAgIMaNRI/dS0fjCIWMzpMA0GCSqGSIb3DQEBBQUAMEExDTAL
BgNVBAYeBABDAE4xETAPBgNVBAseCABJAEMAQgBDMR0wGwYDVQQDHhQAcgBvAG8A
dABDAEEANwA4ADEAMDAeFw0wOTEyMDMxMTU3NTFaFw0zOTExMjYxMTU3NTFaMH4x
DTALBgNVBAYeBABDAE4xGzAZBgNVBAgeEgBHAHUAYQBuAGcAZABvAG4AZzENMAsG
A1UEBx4EAEcAWjERMA8GA1UECh4IAEIAYQBuAGsxETAPBgNVBAseCABJAEMAQgBD
MRswGQYDVQQDHhIAcwB1AGIAQwBBADcAOAAyADgwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBAJPVCgBKBJxImKAvTdJmnOJCN8xaO9to+mqKd0dIuyorMkBCBSsC
LNbveFTy4YzUQrwZKKbSYxOHFBpwSXMLWMzvQasU1QO6nM1pt6agDKFhyS0g07Md
eXurWZBPHjU5Kh6kNAtUgGCwCdwwy7kPqJU+hO6EhMEClzTxiTE0WIULAgMBAAGj
ggIQMIICDDAOBgNVHQ8BAQAEBAMCAIYwDwYDVR0TAQEABAUwAwEB/zCByQYDVR0f
AQEABIG+MIG7MIG4oIG1oIGyhoGvbGRhcDovLzEyMi4xMzYuNzguMTg6Mzg5L0NO
PXJvb3RDQTc4MTAsIENOPXJvb3RDQTc4MTAsIE9VPUNSTERpc3RyaWJ1dGVQb2lu
dHMsIERDPWI1Y2FkLCBEQz1pY2JjLCBEQz1jb20sIERDPWNuP2NlcnRpZmljYXRl
UmV2b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RjbGFzcz1jUkxEaXN0cmlidXRpb25Q
b2ludDAUBglghkgBhvhCAQEBAQAEBAMCAAQwIgYDVR0jAQEABBgwFoAU03ocnyxJ
tUIQ6aT51gu0K7uVgRgwgcAGCCsGAQUFBwEBAQEABIGwMIGtMIGqBggrBgEFBQcw
AoaBnWxkYXA6Ly8xMjIuMTM2Ljc4LjE4OjM4OS9DTj1yb290Q0E3ODEwLENOPXJv
b3RDQTc4MTAsT1U9Y0FDZXJ0aWZpY2F0ZXMsREM9aXVjYWQsIERDPWIjYmMsIERD
PWNvbSwgREM9Y24/Y0FDZXJ0aWZpY2F0ZT9iYXNlP29iamVjdENsYXNzPWNlcnRp

ZmljYXRpb25BdXRob3JpdHkwIAYDVR0OAQEABBYEFNzkkw+GM/atvbKrgpXzayzB
FrtiMA0GCSqGSIb3DQEBBQUAA4GBAGjfYnEvvYcoEpeHq+Uv/ZBA9lmcbCdUZ/9h
2QBw8SfR4Lv8LAB9Kp+23oOQTQeEsi5MNlQDxOGKxOUUsmt4DBCLNRevxBmWEpur
rUlM/Ar4xte+LXoItI1ZCVDSPjnvLXGopQfaUtS3IIlWYvU5XG9fpGgUX02cqAN2
d5TgyvLY

-----END CERTIFICATE-----