Fibocom
PERFECT WIRELESS EXPERIENCE

MTC

AT Commands User Manual_SSL

V1.4

Disclaimer

Any action you take in the course of using this document is at your own risk, and Fibocom shall not be liable for any damages or losses under any circumstances. Due to product version upgrade or other reasons, Fibocom reserves the right to modify any information in this document at any time without prior notice and any responsibility. Unless otherwise agreed, all statements, information and suggestions in this document do not constitute any express or implied guarantee.

This document may include the third-party information covering products, services, software, data, and so on. Fibocom does not control and assumes no responsibility for the third-party content, including but not limited to the accuracy, compatibility, reliability, availability, legitimacy, appropriateness, performance, non-infringement, and status update, unless otherwise specified in this document. Fibocom does not provide any guarantee or authorization for the third-party content mentioned or referenced in this document. If you need a third-party license, obtain it in an authorized or legal way, unless otherwise specified in this document.

Copyright Notice

Unless specially authorized by Fibocom, the recipient of the documents shall keep the documents and information received confidential, and shall not use them for any purpose other than the implementation and development of this project. Without the written permission of Fibocom, no unit or individual shall extract or copy part or all of the contents of this document without authorization, or transmit them in any form. Fibocom has the right to investigate legal liabilities for any offense and tort in connection with violation of confidentiality obligations, or unauthorized use or malicious use of the said documents and information in other illegal forms.

Trademark Statement

The trademark is registered and owned by Fibocom Wireless Inc.

Other trademarks, product names, service names and company names appearing in this document are owned by their respective owners.

Contact Information

Website: https://www.fibocom.com

Address: 10/F-14/F, Block A, Building 6, Shenzhen International Innovation Valley, Dashi First Road, Xili Community, Xili Subdistrict, Nanshan District, Shenzhen

Tel: 0755-26733555

Contents

Applicable Model

No.	Applicable Model	Description
1	MC66x series	NA
2	MG66x series	NA
3	L61x series	NA
4	LC61x series	NA
5	LG61x series	NA
6	MC61x series	NA
7	MG61x series	NA
8	LE13x series	NA
9	LE17x series	NA
10	LE23x series	NA
11	LE25x series	NA
12	LE27x series	NA
13	LE37x series	NA
14	FG132 series	NA
15	MA51x series	NA
16	NL668 series	NA

Change History

V1.4 (2025-03-12)	Expanded the **+GTSSLFILE** command to support setting **PSKKEY** and **PSKID**.
V1.3 (2024-11-06)	Modified the MA510x/NL668 series **+GTSSLFILE**, **+GTSSLVER**, and **+GTSSLCIPHER** command descriptions. Added FG132 series SSL error code list.
V1.2 (2024-10-23)	Modified applicable models and added LE23x and LE25x series products.
V1.1 (2024-08-30)	Modified the parameters of FG132 **+GTSSLCIPHER** and **+GTSSLVER** commands.
V1.0 (2024-07-15)	Initial version.

1 SSL

1.1 +GTSSLFILE, load certificate or key

Description

This command is used to load the CA certificate, key, local trust certificate, or PSK for SSL.

Format

Type	Command	Response
Setting command	AT+GTSSLFILE=<file_type>,<file_len>[,<socket_id>]	Response 1: OK Response 2: ERROR
Read current settings	AT+GTSSLFILE?	+GTSSLFILE: CERTFILE, <file_num> +GTSSLFILE: KEYFILE, <file_num> +GTSSLFILE: TRUSTFILE, <file_num> [+GTSSLFILE: PSKKEY,<file_num> +GTSSLFILE: PSKID,<file_num>] OK
Query command parameter range	AT+GTSSLFILE=?	+GTSSLFILE: ("CERTFILE,KEYFILE,TRUSTFILE,PSKKEY,PSKID"),(4-8192)[,(1-6)] OK
Query command	AT+GTSSLFILE	+GTSSLFILE: <socket_id>,<file_type>,<file_num> OK

Parameter

Name	Description	Value
file_type	Use only one type of file	Range: "CERTFILE", "KEYFILE", "TRUSTFILE","PSKKEY","PSKID". The setting command sets the type and length of the loaded certificate, and CERTFILE(CERTFILE_EXT) and KEYFILE(KEYFILE_EXT) indicate which type of client public key certificate or key to be loaded (typically used in the case of two-way authentication, when the client sends the public key certificate to the server, the server needs to verify the client's legitimacy). TRUSTFILE indicates that the trust certificate or root certificate is loaded into the computer, and if the purpose of the certificate is to verify the validity of the server (one-way authentication and two-way authentication may be required, through +GTSSLMODE), up to 40 trust files are loaded.
file_len	Certificate length or PSK length	Range: 4~8192 bits Length of file encoded in Base64 format
file_num	Indicates the number of loaded certificates or PSKs.	Range: Certificates :1 ~ 40 PSK:1~6
socket_id	socket id, the meaning is the same as <socket_id> parameters in AT commands such as +MIPOPEN, +MIPSEND, +MIPSTAT, etc. When this parameter is not carried, the configured certificate takes effect for all sockets.	Range: 1~6

If the module is powered down, all certificates will be lost. Only one group of the CERTFILE(CERTFILE_EXT) and KEYFILE(KEYFILE_EXT) in the module can be loaded; the TRUSTFILE can be loaded up to 40.

Currently, the command only supports adding (loading) and querying certificates, not deleting and modifying certificates. Most importantly, any type of file that is loaded into the module must be encoded in the base64 format.

When the module enters the ODM mode and ">" appears, if the module has not received any data for more than 12 seconds, it will automatically exit the ODM mode

and return an ERROR.

The query command returns the number of certificates loaded in sockets 1 to 6.

CERTFILE_EXT and KEYFILE_EXT only support in GMSSL. And GMSSL is only supported in some versions, specific versions need to be confirmed with Fibocom.

MA51x/NL668 series does not support query instruction AT+GTSSLFILE, please contact Fibocom for details.

PSKKEY and PSKID need to be set separately and they can be displayed only when they are configured.Note that the PSK setting or queying function is supported only by the Eigencomm platform.

Characteristic

Require SIM Card Normal	No	Require Network Registration	No
Require Data Connection	No	Async or Sync Command	Sync Command
Require Restart to Take Effect	No	Require Data Store at Power Down	No
Max Response Duration (ms)	1000	Max Result Returning Duration (ms)	1000

Example

```
AT+GTSSLFILE?
+GTSSLFILE: CERTFILE,0
+GTSSLFILE: KEYFILE,0
+GTSSLFILE: TRUSTFILE,0
[+GTSSLFILE: PSKKEY,1
+GTSSLFILE: PSKID,1]

OK

AT+GTSSLFILE=?
+GTSSLFILE: ("CERTFILE,KEYFILE,TRUSTFILE,PSKKEY,PSKID"),(4-8192)[,(1-6)]

OK

AT+GTSSLFILE="TRUSTFILE",850
>
```

```
...


OK

AT+GTSSLFILE
+GTSSLFILE: 1,CERTFILE,0
+GTSSLFILE: 1,KEYFILE,0
+GTSSLFILE: 1,TRUSTFILE,0
+GTSSLFILE: 2,CERTFILE,0
+GTSSLFILE: 2,KEYFILE,0
+GTSSLFILE: 2,TRUSTFILE,0
+GTSSLFILE: 3,CERTFILE,0
+GTSSLFILE: 3,KEYFILE,0
+GTSSLFILE: 3,TRUSTFILE,0
+GTSSLFILE: 4,CERTFILE,0
+GTSSLFILE: 4,KEYFILE,0
+GTSSLFILE: 4,TRUSTFILE,0
+GTSSLFILE: 5,CERTFILE,0
+GTSSLFILE: 5,KEYFILE,0
+GTSSLFILE: 5,TRUSTFILE,0
+GTSSLFILE: 6,CERTFILE,0
+GTSSLFILE: 6,KEYFILE,0
+GTSSLFILE: 6,TRUSTFILE,0

OK
```

1.2 +GTSSLMODE, set whether to authenticate the server certificate

Description

This command sets whether the client (module) authenticates the certificate downloaded by the server. If authentication is set, there must be at least one trust certificate in the local trusted client list.

Format

Type	Command	Response
Setting command	AT+GTSSLMODE=<checkmode>	Response 1: OK Response 2: ERROR
Read current settings	AT+GTSSLMODE?	+GTSSLMODE: <checkmode> OK
Query command parameter range	AT+GTSSLMODE=?	+GTSSLMODE: (list of supported <checkmode>s) OK

Parameter

Name	Description	Value
checkmode	checkmode value	Type: integer 0: no authentication (default value) 1: authentication is required

Characteristic

Require SIM Card Normal	No	Require Network Registration	No
Require Data Connection	No	Async or Sync Command	Sync command
Require Restart to Take Effect	No	Require Data Store at Power Down	No
Max Response Duration (ms)	1000	Max Result Returning Duration (ms)	1000

Example

```
AT+GTSSLMODE=?
+GTSSLMODE: (0,1)

OK
```

```
AT+GTSSLMODE?
+GTSSLMODE: 0

OK

AT+GTSSLMODE=1
OK
```

1.3 +GTSSLERR, obtain SSL error code

Description

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

Format

Type	Command	Response
Read current settings	AT+GTSSLERR	Response 1: OK Response 2: +GTSSLERR: <err_code> OK
Read current settings	AT+GTSSLERR?	Response 1: OK Response 2: ERROR
Query command parameter range	AT+GTSSLERR=?	Response 1: ERROR

Parameter

Name	Description	Value
err_code	Error code	0: normal -1: failed

Characteristic

Require SIM Card Normal	Yes	Require Network Registration	Yes
Require Data Connection	Yes	Async or Sync Command	Sync command
Require Restart to Take Effect	No	Require Data Store at Power Down	No
Max Response Duration (ms)	1000	Max Result Returning Duration (ms)	1000

err_code list:

FG132 series

```
0: normal
-1: The certificate validity has expired
-2: The certificate has been revoked (is on a CRL)
-3: The certificate Common Name (CN) does not match with the expected CN
-4: The certificate is not correctly signed by the trusted CA
-7: Certificate was missing
-9: Other reason (can be used by verify callback)
```

Example

```
AT+GTSSLERR?
+GTSSLERR: -1

OK

AT+GTSSLERR
OK
```

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

Description

This command is used to set and query the version of the SSL handshake protocol.

Format

Type	Command	Response
Setting command	AT+GTSSLVER=<sslver>	Response 1: OK Response 2: ERROR
Read current settings	AT+GTSSLVER?	+GTSSLVER: <sslver> OK
Query command parameter range	AT+GTSSLVER=?	+GTSSLVER: (list of supported < sslver >s) OK

Parameter

Name	Description	Value
sslver	SSL protocol version number	Type: integer a. 0: support ssl version 1-4 by default b. 1: indicates that the protocol version is SSL3.0. c. 2: indicates that the protocol version is TLS1.0. d. 3: indicates that the protocol version is TLS1.1. e. 4: indicates that the protocol version is TLS1.2. f. 5: indicates that the protocol version is GMSSL1.0.

GMSSL is only supported in some versions, specific versions need to be confirmed with Fibocom.

FG132 series sslver parameter 5: means the protocol version is TLS1.3. The specific versions need to be confirmed with Fibocom.

LE/MA51x/NL668 series sslver support list is 1-4. The specific list needs to be confirmed with Fibocom.

Characteristic

Require SIM Card Normal	No	Require Network Registration	No
Require Data Connection	No	Async or Sync Command	Sync Command
Require Restart to Take	No	Require Data Store at Power Down	No

Effect			
Max Response Duration (ms)	1000	Max Result Returning Duration (ms)	1000

Example

```
AT+GTSSLVER=?

+GTSSLVER: (0-5)


OK


AT+GTSSLVER?

+GTSSLVER: 0


OK


AT+GTSSLVER=1


OK
```

1.5 +GTSSLCIPHER, configure encryption algorithms

Description

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

Format

Type	Command	Response
Setting command	AT+GTSSLCIPHER=<cipalgID>,<cmd>	Response 1: OK Response 2: ERROR
Read current settings	AT+GTSSLCIPHER?	Response 1: + GTSSLCIPHER: (list of supported <cipalgID>s)

Type	Command	Response
		OK List the cryptographic algorithm IDs that can be used Response 2: OK The cipher algorithm ID is not enabled, the modem will load the default cipher algorithm.
Query command parameter range	AT+GTSSLCIPHER=?	+GTSSLCIPHER: (<cipalgID>, <cmd>) OK

Parameter

Name	Description	Value
cipalgID	If all algorithms are not configured, the device will load the default algorithm.	Type: integer Range: 1 to 138 Each cryptographic algorithm ID is associated with a corresponding algorithm. Products on different platforms have different correspondence between cipalgID and related algorithms.
cmd	The cmd indicates whether to load the algorithm bound to the current password algorithm ID.	Integer type. Range 0, 1. 0 Algorithms shall not be loaded when a connection is established; 1 Algorithm shall be loaded when establishing a connection;

cipalgID list is shown below, with the default algorithm being all algorithms enabled

Each cipher algorithm ID is related to the corresponding algorithm. Products on different platforms have different correspondences between cipalgID and related algorithms, subject to the actual query result of +GTSSLCIPHER or you can contact Fibocom support.

The cipalgID range of MA51x/NL668 series is 0-31,255, 0 for setting the default encryption

> suite, 11-31 for reserved ID,255 for setting all encryption suites, subject to the actual query result of +GTSSLCIPHER or you can contact Fibocom support.

Characteristic

Require SIM Card Normal	No	Require Network Registration	No
Require Data Connection	No	Async or Sync Command	Sync command
Require Restart to Take Effect	No	Require Data Store at Power Down	No
Max Response Duration (ms)	1000	Max Result Returning Duration (ms)	1000

List of supported algorithms:

LE series (except LE230-CN-1D2, LE270-CN-1D2, LE270-CN-1D21, LE370-CN-1D7 series)

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-AES-128-GCM-SHA256
18	TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256
19	TLS-DHE-RSA-WITH-AES-128-GCM-SHA256
20	TLS-ECDHE-ECDSA-WITH-AES-128-CCM
21	TLS-DHE-RSA-WITH-AES-128-CCM
22	TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256
23	TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256
24	TLS-DHE-RSA-WITH-AES-128-CBC-SHA256
25	TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA
26	TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA
27	TLS-DHE-RSA-WITH-AES-128-CBC-SHA
28	TLS-ECDHE-ECDSA-WITH-AES-128-CCM-8
29	TLS-DHE-RSA-WITH-AES-128-CCM-8
30	TLS-ECDHE-PSK-WITH-CHACHA20-POLY1305-SHA256
31	TLS-DHE-PSK-WITH-CHACHA20-POLY1305-SHA256
32	TLS-DHE-PSK-WITH-AES-256-GCM-SHA384
33	TLS-DHE-PSK-WITH-AES-256-CCM
34	TLS-ECDHE-PSK-WITH-AES-256-CBC-SHA384
35	TLS-DHE-PSK-WITH-AES-256-CBC-SHA384
36	TLS-ECDHE-PSK-WITH-AES-256-CBC-SHA
37	TLS-DHE-PSK-WITH-AES-256-CBC-SHA
38	TLS-DHE-PSK-WITH-AES-256-CCM-8
39	TLS-DHE-PSK-WITH-AES-128-GCM-SHA256
40	TLS-DHE-PSK-WITH-AES-128-CCM
41	TLS-ECDHE-PSK-WITH-AES-128-CBC-SHA256
42	TLS-DHE-PSK-WITH-AES-128-CBC-SHA256

43	TLS-ECDHE-PSK-WITH-AES-128-CBC-SHA
44	TLS-DHE-PSK-WITH-AES-128-CBC-SHA
45	TLS-DHE-PSK-WITH-AES-128-CCM-8
46	TLS-RSA-WITH-AES-256-GCM-SHA384
47	TLS-RSA-WITH-AES-256-CCM
48	TLS-RSA-WITH-AES-256-CBC-SHA256
49	TLS-RSA-WITH-AES-256-CBC-SHA
50	TLS-ECDH-RSA-WITH-AES-256-GCM-SHA384
51	TLS-ECDH-RSA-WITH-AES-256-CBC-SHA384
52	TLS-ECDH-RSA-WITH-AES-256-CBC-SHA
53	TLS-ECDH-ECDSA-WITH-AES-256-GCM-SHA384
54	TLS-ECDH-ECDSA-WITH-AES-256-CBC-SHA384
55	TLS-ECDH-ECDSA-WITH-AES-256-CBC-SHA
56	TLS-RSA-WITH-AES-256-CCM-8
57	TLS-RSA-WITH-AES-128-GCM-SHA256
58	TLS-RSA-WITH-AES-128-CCM
59	TLS-RSA-WITH-AES-128-CBC-SHA256
60	TLS-RSA-WITH-AES-128-CBC-SHA
61	TLS-ECDH-RSA-WITH-AES-128-GCM-SHA256
62	TLS-ECDH-RSA-WITH-AES-128-CBC-SHA256
63	TLS-ECDH-RSA-WITH-AES-128-CBC-SHA
64	TLS-ECDH-ECDSA-WITH-AES-128-GCM-SHA256
65	TLS-ECDH-ECDSA-WITH-AES-128-CBC-SHA256
66	TLS-ECDH-ECDSA-WITH-AES-128-CBC-SHA
67	TLS-RSA-WITH-AES-128-CCM-8
68	TLS-RSA-PSK-WITH-CHACHA20-POLY1305-SHA256
69	TLS-RSA-PSK-WITH-AES-256-GCM-SHA384
70	TLS-RSA-PSK-WITH-AES-256-CBC-SHA384

71	TLS-RSA-PSK-WITH-AES-256-CBC-SHA
72	TLS-RSA-PSK-WITH-AES-128-GCM-SHA256
73	TLS-RSA-PSK-WITH-AES-128-CBC-SHA256
74	TLS-RSA-PSK-WITH-AES-128-CBC-SHA
75	TLS-PSK-WITH-CHACHA20-POLY1305-SHA256
76	TLS-PSK-WITH-AES-256-GCM-SHA384
77	TLS-PSK-WITH-AES-256-CCM
78	TLS-PSK-WITH-AES-256-CBC-SHA384
79	TLS-PSK-WITH-AES-256-CBC-SHA
80	TLS-PSK-WITH-AES-256-CCM-8
81	TLS-PSK-WITH-AES-128-GCM-SHA256
82	TLS-PSK-WITH-AES-128-CCM
83	TLS-PSK-WITH-AES-128-CBC-SHA256
84	TLS-PSK-WITH-AES-128-CBC-SHA
85	TLS-PSK-WITH-AES-128-CCM-8
86	TLS-ECDHE-ECDSA-WITH-3DES-EDE-CBC-SHA
87	TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA
88	TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA
89	TLS-ECDHE-PSK-WITH-3DES-EDE-CBC-SHA
90	TLS-DHE-PSK-WITH-3DES-EDE-CBC-SHA
91	TLS-RSA-WITH-3DES-EDE-CBC-SHA
92	TLS-ECDH-RSA-WITH-3DES-EDE-CBC-SHA
93	TLS-ECDH-ECDSA-WITH-3DES-EDE-CBC-SHA
94	TLS-RSA-PSK-WITH-3DES-EDE-CBC-SHA
95	TLS-PSK-WITH-3DES-EDE-CBC-SHA

1	TLS-ECDHE-ECDSA-WITH-AES-256-CCM
2	TLS-DHE-RSA-WITH-AES-256-CCM
3	TLS-DHE-RSA-WITH-AES-256-CBC-SHA256
4	TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA
5	TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA
6	TLS-DHE-RSA-WITH-AES-256-CBC-SHA
7	TLS-ECDHE-ECDSA-WITH-AES-256-CCM-8
8	TLS-DHE-RSA-WITH-AES-256-CCM-8
9	TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256
10	TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256
11	TLS-DHE-RSA-WITH-AES-128-GCM-SHA256
12	TLS-ECDHE-ECDSA-WITH-AES-128-CCM
13	TLS-DHE-RSA-WITH-AES-128-CCM
14	TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256
15	TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256
16	TLS-DHE-RSA-WITH-AES-128-CBC-SHA256
17	TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA
18	TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA
19	TLS-DHE-RSA-WITH-AES-128-CBC-SHA
20	TLS-ECDHE-ECDSA-WITH-AES-128-CCM-8
21	TLS-DHE-RSA-WITH-AES-128-CCM-8
22	TLS-DHE-PSK-WITH-AES-256-CCM
23	TLS-ECDHE-PSK-WITH-AES-256-CBC-SHA
24	TLS-DHE-PSK-WITH-AES-256-CBC-SHA
25	TLS-DHE-PSK-WITH-AES-256-CCM-8
26	TLS-DHE-PSK-WITH-AES-128-GCM-SHA256
27	TLS-DHE-PSK-WITH-AES-128-CCM
28	TLS-ECDHE-PSK-WITH-AES-128-CBC-SHA256

29	TLS-DHE-PSK-WITH-AES-128-CBC-SHA256
30	TLS-ECDHE-PSK-WITH-AES-128-CBC-SHA
31	TLS-DHE-PSK-WITH-AES-128-CBC-SHA
32	TLS-DHE-PSK-WITH-AES-128-CCM-8
33	TLS-RSA-WITH-AES-256-CCM
34	TLS-RSA-WITH-AES-256-CBC-SHA256
35	TLS-RSA-WITH-AES-256-CBC-SHA
36	TLS-ECDH-RSA-WITH-AES-256-CBC-SHA
37	TLS-ECDH-ECDSA-WITH-AES-256-CBC-SHA
38	TLS-RSA-WITH-AES-256-CCM-8
39	TLS-RSA-WITH-AES-128-GCM-SHA256
40	TLS-RSA-WITH-AES-128-CCM
41	TLS-RSA-WITH-AES-128-CBC-SHA256
42	TLS-RSA-WITH-AES-128-CBC-SHA
43	TLS-ECDH-RSA-WITH-AES-128-GCM-SHA256
44	TLS-ECDH-RSA-WITH-AES-128-CBC-SHA256
45	TLS-ECDH-RSA-WITH-AES-128-CBC-SHA
46	TLS-ECDH-ECDSA-WITH-AES-128-GCM-SHA256
47	TLS-ECDH-ECDSA-WITH-AES-128-CBC-SHA256
48	TLS-ECDH-ECDSA-WITH-AES-128-CBC-SHA
49	TLS-RSA-WITH-AES-128-CCM-8
50	TLS-RSA-PSK-WITH-AES-256-CBC-SHA
51	TLS-RSA-PSK-WITH-AES-128-GCM-SHA256
52	TLS-RSA-PSK-WITH-AES-128-CBC-SHA256
53	TLS-RSA-PSK-WITH-AES-128-CBC-SHA
54	TLS-PSK-WITH-AES-256-CCM
55	TLS-PSK-WITH-AES-256-CBC-SHA
56	TLS-PSK-WITH-AES-256-CCM-8

57	TLS-PSK-WITH-AES-128-GCM-SHA256
58	TLS-PSK-WITH-AES-128-CCM
59	TLS-PSK-WITH-AES-128-CBC-SHA256
60	TLS-PSK-WITH-AES-128-CBC-SHA
61	TLS-PSK-WITH-AES-128-CCM-8
62	TLS-ECDHE-ECDSA-WITH-3DES-EDE-CBC-SHA
63	TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA
64	TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA
65	TLS-ECDHE-PSK-WITH-3DES-EDE-CBC-SHA
66	TLS-DHE-PSK-WITH-3DES-EDE-CBC-SHA
67	TLS-RSA-WITH-3DES-EDE-CBC-SHA
68	TLS-ECDH-RSA-WITH-3DES-EDE-CBC-SHA
69	TLS-ECDH-ECDSA-WITH-3DES-EDE-CBC-SHA
70	TLS-RSA-PSK-WITH-3DES-EDE-CBC-SHA
71	TLS-PSK-WITH-3DES-EDE-CBC-SHA

L61x/LC61x/LG61x/MC61x Series

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
32	TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA
33	TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA
34	TLS-DHE-RSA-WITH-AES-128-CBC-SHA
35	TLS-ECDHE-ECDSA-WITH-AES-128-CCM-8
36	TLS-DHE-RSA-WITH-AES-128-CCM-8
37	TLS-ECDHE-ECDSA-WITH-CAMELLIA-128-GCM-SHA256
38	TLS-ECDHE-RSA-WITH-CAMELLIA-128-GCM-SHA256
39	TLS-DHE-RSA-WITH-CAMELLIA-128-GCM-SHA256

40	TLS-ECDHE-ECDSA-WITH-CAMELLIA-128-CBC-SHA256
41	TLS-ECDHE-RSA-WITH-CAMELLIA-128-CBC-SHA256
42	TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256
43	TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA
44	TLS-ECDHE-ECDSA-WITH-3DES-EDE-CBC-SHA
45	TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA
46	TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA
47	TLS-ECDHE-PSK-WITH-CHACHA20-POLY1305-SHA256
48	TLS-DHE-PSK-WITH-CHACHA20-POLY1305-SHA256
49	TLS-DHE-PSK-WITH-AES-256-GCM-SHA384
50	TLS-DHE-PSK-WITH-AES-256-CCM
51	TLS-ECDHE-PSK-WITH-AES-256-CBC-SHA384
52	TLS-DHE-PSK-WITH-AES-256-CBC-SHA384
53	TLS-ECDHE-PSK-WITH-AES-256-CBC-SHA
54	TLS-DHE-PSK-WITH-AES-256-CBC-SHA
55	TLS-DHE-PSK-WITH-CAMELLIA-256-GCM-SHA384
56	TLS-ECDHE-PSK-WITH-CAMELLIA-256-CBC-SHA384
57	TLS-DHE-PSK-WITH-CAMELLIA-256-CBC-SHA384
58	TLS-DHE-PSK-WITH-AES-256-CCM-8
59	TLS-DHE-PSK-WITH-AES-128-GCM-SHA256
60	TLS-DHE-PSK-WITH-AES-128-CCM
61	TLS-ECDHE-PSK-WITH-AES-128-CBC-SHA256
62	TLS-DHE-PSK-WITH-AES-128-CBC-SHA256
63	TLS-ECDHE-PSK-WITH-AES-128-CBC-SHA
64	TLS-DHE-PSK-WITH-AES-128-CBC-SHA
65	TLS-DHE-PSK-WITH-CAMELLIA-128-GCM-SHA256
66	TLS-DHE-PSK-WITH-CAMELLIA-128-CBC-SHA256
67	TLS-ECDHE-PSK-WITH-CAMELLIA-128-CBC-SHA256

68	TLS-DHE-PSK-WITH-AES-128-CCM-8
69	TLS-ECDHE-PSK-WITH-3DES-EDE-CBC-SHA
70	TLS-DHE-PSK-WITH-3DES-EDE-CBC-SHA
71	TLS-RSA-WITH-AES-256-GCM-SHA384
72	TLS-RSA-WITH-AES-256-CCM
73	TLS-RSA-WITH-AES-256-CBC-SHA256
74	TLS-RSA-WITH-AES-256-CBC-SHA
75	TLS-ECDH-RSA-WITH-AES-256-GCM-SHA384
76	TLS-ECDH-RSA-WITH-AES-256-CBC-SHA384
77	TLS-ECDH-RSA-WITH-AES-256-CBC-SHA
78	TLS-ECDH-ECDSA-WITH-AES-256-GCM-SHA384
79	TLS-ECDH-ECDSA-WITH-AES-256-CBC-SHA384
80	TLS-ECDH-ECDSA-WITH-AES-256-CBC-SHA
81	TLS-RSA-WITH-AES-256-CCM-8
82	TLS-RSA-WITH-CAMELLIA-256-GCM-SHA384
83	TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256
84	TLS-RSA-WITH-CAMELLIA-256-CBC-SHA
85	TLS-ECDH-RSA-WITH-CAMELLIA-256-GCM-SHA384
86	TLS-ECDH-RSA-WITH-CAMELLIA-256-CBC-SHA384
87	TLS-ECDH-ECDSA-WITH-CAMELLIA-256-GCM-SHA384
88	TLS-ECDH-ECDSA-WITH-CAMELLIA-256-CBC-SHA384
89	TLS-RSA-WITH-AES-128-GCM-SHA256
90	TLS-RSA-WITH-AES-128-CCM
91	TLS-RSA-WITH-AES-128-CBC-SHA256
92	TLS-RSA-WITH-AES-128-CBC-SHA
93	TLS-ECDH-RSA-WITH-AES-128-GCM-SHA256
94	TLS-ECDH-RSA-WITH-AES-128-CBC-SHA256
95	TLS-ECDH-RSA-WITH-AES-128-CBC-SHA

96	TLS-ECDH-ECDSA-WITH-AES-128-GCM-SHA256
97	TLS-ECDH-ECDSA-WITH-AES-128-CBC-SHA256
98	TLS-ECDH-ECDSA-WITH-AES-128-CBC-SHA
99	TLS-RSA-WITH-AES-128-CCM-8
100	TLS-RSA-WITH-CAMELLIA-128-GCM-SHA256
101	TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256
102	TLS-RSA-WITH-CAMELLIA-128-CBC-SHA
103	TLS-ECDH-RSA-WITH-CAMELLIA-128-GCM-SHA256
104	TLS-ECDH-RSA-WITH-CAMELLIA-128-CBC-SHA256
105	TLS-ECDH-ECDSA-WITH-CAMELLIA-128-GCM-SHA256
106	TLS-ECDH-ECDSA-WITH-CAMELLIA-128-CBC-SHA256
107	TLS-RSA-WITH-3DES-EDE-CBC-SHA
108	TLS-ECDH-RSA-WITH-3DES-EDE-CBC-SHA
109	TLS-ECDH-ECDSA-WITH-3DES-EDE-CBC-SHA
110	TLS-RSA-PSK-WITH-CHACHA20-POLY1305-SHA256
111	TLS-RSA-PSK-WITH-AES-256-GCM-SHA384
112	TLS-RSA-PSK-WITH-AES-256-CBC-SHA384
113	TLS-RSA-PSK-WITH-AES-256-CBC-SHA
114	TLS-RSA-PSK-WITH-CAMELLIA-256-GCM-SHA384
115	TLS-RSA-PSK-WITH-CAMELLIA-256-CBC-SHA384
116	TLS-RSA-PSK-WITH-AES-128-GCM-SHA256
117	TLS-RSA-PSK-WITH-AES-128-CBC-SHA256
118	TLS-RSA-PSK-WITH-AES-128-CBC-SHA
119	TLS-RSA-PSK-WITH-CAMELLIA-128-GCM-SHA256
120	TLS-RSA-PSK-WITH-CAMELLIA-128-CBC-SHA256
121	TLS-RSA-PSK-WITH-3DES-EDE-CBC-SHA
122	TLS-PSK-WITH-CHACHA20-POLY1305-SHA256
123	TLS-PSK-WITH-AES-256-GCM-SHA384

124	TLS-PSK-WITH-AES-256-CCM
125	TLS-PSK-WITH-AES-256-CBC-SHA384
126	TLS-PSK-WITH-AES-256-CBC-SHA
127	TLS-PSK-WITH-CAMELLIA-256-GCM-SHA384
128	TLS-PSK-WITH-CAMELLIA-256-CBC-SHA384
129	TLS-PSK-WITH-AES-256-CCM-8
130	TLS-PSK-WITH-AES-128-GCM-SHA256
131	TLS-PSK-WITH-AES-128-CCM
132	TLS-PSK-WITH-AES-128-CBC-SHA256
133	TLS-PSK-WITH-AES-128-CBC-SHA
134	TLS-PSK-WITH-CAMELLIA-128-GCM-SHA256
135	TLS-PSK-WITH-CAMELLIA-128-CBC-SHA256
136	TLS-PSK-WITH-AES-128-CCM-8
137	TLS-PSK-WITH-3DES-EDE-CBC-SHA

MC66x/MG66x Series

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
32	TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA
33	TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA
34	TLS-DHE-RSA-WITH-AES-128-CBC-SHA
35	TLS-ECDHE-ECDSA-WITH-AES-128-CCM-8
36	TLS-DHE-RSA-WITH-AES-128-CCM-8
37	TLS-ECDHE-ECDSA-WITH-CAMELLIA-128-GCM-SHA256
38	TLS-ECDHE-RSA-WITH-CAMELLIA-128-GCM-SHA256
39	TLS-DHE-RSA-WITH-CAMELLIA-128-GCM-SHA256
40	TLS-ECDHE-ECDSA-WITH-CAMELLIA-128-CBC-SHA256

41	TLS-ECDHE-RSA-WITH-CAMELLIA-128-CBC-SHA256
42	TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256
43	TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA
44	TLS-ECDHE-PSK-WITH-CHACHA20-POLY1305-SHA256
45	TLS-DHE-PSK-WITH-CHACHA20-POLY1305-SHA256
46	TLS-DHE-PSK-WITH-AES-256-GCM-SHA384
47	TLS-DHE-PSK-WITH-AES-256-CCM
48	TLS-ECDHE-PSK-WITH-AES-256-CBC-SHA384
49	TLS-DHE-PSK-WITH-AES-256-CBC-SHA384
50	TLS-ECDHE-PSK-WITH-AES-256-CBC-SHA
51	TLS-DHE-PSK-WITH-AES-256-CBC-SHA
52	TLS-DHE-PSK-WITH-CAMELLIA-256-GCM-SHA384
53	TLS-ECDHE-PSK-WITH-CAMELLIA-256-CBC-SHA384
54	TLS-DHE-PSK-WITH-CAMELLIA-256-CBC-SHA384
55	TLS-DHE-PSK-WITH-AES-256-CCM-8
56	TLS-DHE-PSK-WITH-AES-128-GCM-SHA256
57	TLS-DHE-PSK-WITH-AES-128-CCM
58	TLS-ECDHE-PSK-WITH-AES-128-CBC-SHA256
59	TLS-DHE-PSK-WITH-AES-128-CBC-SHA256
60	TLS-ECDHE-PSK-WITH-AES-128-CBC-SHA
61	TLS-DHE-PSK-WITH-AES-128-CBC-SHA
62	TLS-DHE-PSK-WITH-CAMELLIA-128-GCM-SHA256
63	TLS-DHE-PSK-WITH-CAMELLIA-128-CBC-SHA256
64	TLS-ECDHE-PSK-WITH-CAMELLIA-128-CBC-SHA256
65	TLS-DHE-PSK-WITH-AES-128-CCM-8
66	TLS-RSA-WITH-AES-256-GCM-SHA384
67	TLS-RSA-WITH-AES-256-CCM
68	TLS-RSA-WITH-AES-256-CBC-SHA256

69	TLS-RSA-WITH-AES-256-CBC-SHA
70	TLS-ECDH-RSA-WITH-AES-256-GCM-SHA384
71	TLS-ECDH-RSA-WITH-AES-256-CBC-SHA384
72	TLS-ECDH-RSA-WITH-AES-256-CBC-SHA
73	TLS-ECDH-ECDSA-WITH-AES-256-GCM-SHA384
74	TLS-ECDH-ECDSA-WITH-AES-256-CBC-SHA384
75	TLS-ECDH-ECDSA-WITH-AES-256-CBC-SHA
76	TLS-RSA-WITH-AES-256-CCM-8
77	TLS-RSA-WITH-CAMELLIA-256-GCM-SHA384
78	TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256
79	TLS-RSA-WITH-CAMELLIA-256-CBC-SHA
80	TLS-ECDH-RSA-WITH-CAMELLIA-256-GCM-SHA384
81	TLS-ECDH-RSA-WITH-CAMELLIA-256-CBC-SHA384
82	TLS-ECDH-ECDSA-WITH-CAMELLIA-256-GCM-SHA384
83	TLS-ECDH-ECDSA-WITH-CAMELLIA-256-CBC-SHA384
84	TLS-RSA-WITH-AES-128-GCM-SHA256
85	TLS-RSA-WITH-AES-128-CCM
86	TLS-RSA-WITH-AES-128-CBC-SHA256
87	TLS-RSA-WITH-AES-128-CBC-SHA
88	TLS-ECDH-RSA-WITH-AES-128-GCM-SHA256
89	TLS-ECDH-RSA-WITH-AES-128-CBC-SHA256
90	TLS-ECDH-RSA-WITH-AES-128-CBC-SHA
91	TLS-ECDH-ECDSA-WITH-AES-128-GCM-SHA256
92	TLS-ECDH-ECDSA-WITH-AES-128-CBC-SHA256
93	TLS-ECDH-ECDSA-WITH-AES-128-CBC-SHA
94	TLS-RSA-WITH-AES-128-CCM-8
95	TLS-RSA-WITH-CAMELLIA-128-GCM-SHA256
96	TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256

97 TLS-RSA-WITH-CAMELLIA-128-CBC-SHA

98 TLS-ECDH-RSA-WITH-CAMELLIA-128-GCM-SHA256

99 TLS-ECDH-RSA-WITH-CAMELLIA-128-CBC-SHA256

100 TLS-ECDH-ECDSA-WITH-CAMELLIA-128-GCM-SHA256

101 TLS-ECDH-ECDSA-WITH-CAMELLIA-128-CBC-SHA256

102 TLS-RSA-PSK-WITH-CHACHA20-POLY1305-SHA256

103 TLS-RSA-PSK-WITH-AES-256-GCM-SHA384

104 TLS-RSA-PSK-WITH-AES-256-CBC-SHA384

105 TLS-RSA-PSK-WITH-AES-256-CBC-SHA

106 TLS-RSA-PSK-WITH-CAMELLIA-256-GCM-SHA384

107 TLS-RSA-PSK-WITH-CAMELLIA-256-CBC-SHA384

108 TLS-RSA-PSK-WITH-AES-128-GCM-SHA256

109 TLS-RSA-PSK-WITH-AES-128-CBC-SHA256

110 TLS-RSA-PSK-WITH-AES-128-CBC-SHA

111 TLS-RSA-PSK-WITH-CAMELLIA-128-GCM-SHA256

112 TLS-RSA-PSK-WITH-CAMELLIA-128-CBC-SHA256

113 TLS-PSK-WITH-CHACHA20-POLY1305-SHA256

114 TLS-PSK-WITH-AES-256-GCM-SHA384

115 TLS-PSK-WITH-AES-256-CCM

116 TLS-PSK-WITH-AES-256-CBC-SHA384

117 TLS-PSK-WITH-AES-256-CBC-SHA

118 TLS-PSK-WITH-CAMELLIA-256-GCM-SHA384

119 TLS-PSK-WITH-CAMELLIA-256-CBC-SHA384

120 TLS-PSK-WITH-AES-256-CCM-8

121 TLS-PSK-WITH-AES-128-GCM-SHA256

122 TLS-PSK-WITH-AES-128-CCM

123 TLS-PSK-WITH-AES-128-CBC-SHA256

124 TLS-PSK-WITH-AES-128-CBC-SHA

125	TLS-PSK-WITH-CAMELLIA-128-GCM-SHA256
126	TLS-PSK-WITH-CAMELLIA-128-CBC-SHA256
127	TLS-PSK-WITH-AES-128-CCM-8
128	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
129	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
130	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
131	TLS_ECDHE_PSK_WITH_3DES_EDE_CBC_SHA
132	TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA
133	TLS_RSA_WITH_3DES_EDE_CBC_SHA
134	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
135	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
136	TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA
137	TLS-PSK-WITH-3DES-EDE-CBC-SHA
138	GM-SM2-WITH-SM4-CBC-SM3

MA51x/NL668 Series

Old cipher suites:

1	TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA	(DEL)
2	TLS-DHE-RSA-WITH-AES-128-CBC-SHA	
3	TLS-RSA-WITH-AES-128-CBC-SHA	(DEL)
4	TLS-DHE-RSA-WITH-AES-128-CBC-SHA256	
5	TLS-DHE-RSA-WITH-AES-256-CBC-SHA	
6	TLS-RSA-WITH-3DES-EDE-CBC-SHA	(DEL)
7	TLS-DHE-RSA-WITH-AES-256-CBC-SHA256	
8	TLS-RSA-WITH-AES-128-CBC-SHA	
9	TLS-RSA-WITH-AES-128-CBC-SHA256	
10	TLS-RSA-WITH-AES-256-CBC-SHA256	

The new version will no longer support the encryption suite marked as (DEL). The initial encryption suite of the MA51x series has changed from 1, 2, and 3 (corresponding to the old encryption suite) to 1, 2, 3, 4, 5, 6, and 7 (corresponding to the new encryption suite).

There are differences in the initial encryption suites of the MA51x/NL668 series among different products. For specific information, refer to the product query results or contact the technical support of Fibocom.

New cipher suites:

1	TLS-DHE-RSA-WITH-AES-128-CBC-SHA
2	TLS-DHE-RSA-WITH-AES-128-CBC-SHA256
3	TLS-DHE-RSA-WITH-AES-256-CBC-SHA
4	TLS-DHE-RSA-WITH-AES-256-CBC-SHA256
5	TLS-RSA-WITH-AES-128-CBC-SHA
6	TLS-RSA-WITH-AES-128-CBC-SHA256
7	TLS-RSA-WITH-AES-256-CBC-SHA256

FG132 Series

1	TLS_CHACHA20_POLY1305_SHA256
2	TLS_AES_128_GCM_SHA256
3	TLS_AES_256_GCM_SHA384
4	TLS_AES_128_CCM_SHA256
5	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
6	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
7	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
8	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
9	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
10	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
11	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256

12 TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256
13 TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384
14 TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384
15 TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256
16 TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256
17 TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384
18 TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384
19 TLS_ECDHE_ECDSA_WITH_AES_128_CCM
20 TLS_ECDHE_ECDSA_WITH_AES_256_CCM
21 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
22 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
23 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
24 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
25 TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256
26 TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
27 TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384
28 TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
29 TLS_ECDHE_ECDSA_WITH_ARIA_128_CBC_SHA256
30 TLS_ECDHE_RSA_WITH_ARIA_128_CBC_SHA256
31 TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384
32 TLS_ECDHE_RSA_WITH_ARIA_256_CBC_SHA384
33 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
34 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
35 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
36 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
37 TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
38 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
39 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
40 TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256
41 TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384
42 TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256
43 TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384
44 TLS_DHE_RSA_WITH_AES_128_CCM

45 TLS_DHE_RSA_WITH_AES_256_CCM
46 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
47 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
48 TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
49 TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
50 TLS_DHE_RSA_WITH_ARIA_128_CBC_SHA256
51 TLS_DHE_RSA_WITH_ARIA_256_CBC_SHA384
52 TLS_DHE_RSA_WITH_AES_128_CBC_SHA
53 TLS_DHE_RSA_WITH_AES_256_CBC_SHA
54 TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
55 TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
56 TLS_DHE_RSA_WITH_SEED_CBC_SHA
57 TLS_RSA_WITH_AES_128_GCM_SHA256
58 TLS_RSA_WITH_AES_256_GCM_SHA384
59 TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256
60 TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384
61 TLS_RSA_WITH_ARIA_128_GCM_SHA256
62 TLS_RSA_WITH_ARIA_256_GCM_SHA384
63 TLS_RSA_WITH_AES_128_CCM
64 TLS_RSA_WITH_AES_256_CCM
65 TLS_RSA_WITH_AES_128_CBC_SHA256
66 TLS_RSA_WITH_AES_256_CBC_SHA256
67 TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
68 TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
69 TLS_RSA_WITH_ARIA_128_CBC_SHA256
70 TLS_RSA_WITH_ARIA_256_CBC_SHA384
71 TLS_RSA_WITH_AES_128_CBC_SHA
72 TLS_RSA_WITH_AES_256_CBC_SHA
73 TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
74 TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
75 TLS_RSA_WITH_SEED_CBC_SHA

Example

```
AT+GTSSLCIPHER=?

+GTSSLCIPHER: (1-138),(0-1)


OK

AT+GTSSLCIPHER?

+GTSSLCIPHER: 1,2,3,4,5,6,7,8,9,10……136,137,138


OK

AT+GTSSLCIPHER=1,0

OK
```