IbexOS Release Notes

Release 6.11.4-0

Westermo Network Technologies AB

June 27, 2024

Contents

1 General Information

Company
Westermo Network Technologies AB

Contact Support
www.westermo.com

Release Number
6.11.4-0

Software Build Number
0fd788aed9be625dd6383df55ec3c960e272fac4

Date of this build
June 27, 2024

2 Release Highlights

2.1 6.11.4-0

- Wireless: Add support for Dynamic VLAN
- Wireless: Add support for Inter-Carriage Link (ICL) on 802.11ax products (Ibex-1510, Ibex-3510)

3 Limitations

- When the device is reconfigured to Mesh with SAE as encryption, the device has to be rebooted after applying the configuration (802.11n products only)
- Multi-SSID with DFS channels does not work (802.11n products only)
- It is recommended to operate the wave 1 card (radio1) with a maximum of 60 active clients. (802.11ac products only)

4 Configuration Parameter Changes

The following configuration items have been added, changed, removed, deprecated or obsoleted:

- cfgWlan802dot1xDynamicVlan (added)
- cfgGnssDevDebugEnabled (added)
- cfgWlanDevQmrrString (changed)
- cfgWlanIfaceBitrates (changed)
- cfgWlanIfaceInactivityTimeout (changed)
- cfgWlan802dot1xCiphers (changed)
- cfgWlan802dot1xCaIds (changed)
- cfgRouteTableRoutingTables (changed)

- cfgRouteDhcpRoutingTables (changed)
- cfgDhcpDnsmasqDnsRebindDomainOk (changed)
- cfgHttpAdminPasswordHash (changed)
- cfgHttpMonitorPasswordHash (changed)
- cfgHttpTlsCiphers (changed)
- cfgLldpDescription (changed)
- cfgMdnsNetwork (changed)
- cfgCellDeviceOperatorSpn (changed)
- cfgScepCaIdentifier (changed)
- cfgScepChallengePassword (changed)
- cfgScepCsrC (changed)
- cfgScepCsrST (changed)
- cfgScepCsrL (changed)
- cfgScepCsrO (changed)
- cfgScepCsrOU (changed)
- cfgVpnOpenvpnAuth (changed)
- cfgVpnOpenvpnCipher (changed)
- cfgVpnOpenvpnVerifyX509String (changed)
- cfgVpnOpenvpnCaIds (changed)
- cfgVpnIpsecIke (changed)
- cfgVpnIpsecEsp (changed)
- cfgVpnIpsecPassword (changed)
- cfgVpnIpsecCaIds (changed)
- cfgVpnIpsecGlblCustomOptions (changed)

- cfgVpnWgPEndpoint (changed)
- cfgVpnWgPAllowedIps (changed)
- cfgLdapTlsCiphers (changed)
- cfgAfmRedundantName (changed)
- cfgAfmNeighbourName (changed)
- setWlanDevIndex (changed)
- setTlsCltTlsCiphers (changed)

5 Supported Cellular Firmware

This release supports and has been tested with the following cellular firmwares:

5.1 Ibex-RT-330, Ibex-RT-630

- EM12GPAR01A20M4G_01.003.01.003
- EM12GPAR01A21M4G_01.200.01.200

5.2 Ibex-RT-330-5G, Ibex-RT-630-5G

- RM520NGLAAR03A01M4G_01.202.01.202
- RM520NGLAAR03A03M4G_01.201.01.201

Other cellular firmware versions are not supported.

6 Changed Configuration Parameter Descriptions

6.1 MIB Reference: WESTERMO-SW6-MIB

6.1.1 cfgScepCsrC

C (Country) field for CSR

If set to ‘none’, C is not used for CSR.

Example:

- CH

Applies to STA.

Type	DisplayString
Range	1 - 4
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1002.2.1.13

6.1.2 cfgScepCsrST

ST (State) field for CSR

If set to ‘none’, ST is not used for CSR.

Example:

- Zurich

Applies to STA.

Type	DisplayString
Range	1 - 63
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1002.2.1.14

6.1.3 cfgScepCsrL

L (Locality) field for CSR

If set to ‘none’, L is not used for CSR.

Example:

- Bubikon

Applies to STA.

Type	DisplayString
Range	1 - 63
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1002.2.1.15

6.1.4 cfgScepCsrO

O (Organization) field for CSR

If set to ‘none’, O is not used for CSR.

Applies to STA.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1002.2.1.16

6.1.5 cfgScepCsrOU

OU (Organizational Unit) field for CSR

If set to ‘none’, OU is not used for CSR.

Applies to STA.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1002.2.1.17

6.1.6 cfgScepCaIdentifier

CA Identifier

Certification authority (CA) issuer identifier (if your SCEP server requires it). A CA Identifier is any string that is understood by the SCEP server (e.g. a domain name).

If set to 'none', CA Identifier is not used.

Applies to STA.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1002.2.1.3

6.1.7 cfgScepChallengePassword

SCEP Challenge Password

If set to 'none', Challenge Password is not used.

Applies to STA.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1002.2.1.5

6.1.8 cfgVpnOpenvpnVerifyX509String

X.509 Certificate Verification String

If a X.509 certificate verification method is enabled (see `cfgVpnOpenvpnVerifyX509Name`), this parameter defines the string to be compared by the verification method.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.1.1.1.22

6.1.9 cfgVpnOpenvpnCalds

OpenVPN CA ID(s)

This value contain the id(s) to reference the ca certificate in the certificate store.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.1.1.1.25

6.1.10 cfgVpnOpenvpnAuth

Packet Authentication

Authenticate packets with a Hash-based Message Authentication Code HMAC using the given message digest algorithm.

In static-key encryption mode, the HMAC key is included in the key file. In TLS mode, the HMAC key is dynamically generated and shared between peers via the TLS control channel.

Examples:

- **SHA256**
- **SHA3-512**
- **SHA1**: according to blank `auth` entry in ovpn config file
- **none**: to disable HMAC packet authentication

For a full list of supported algorithms please consult the user manual or execute **openvpn –show-digests** on a device.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.1.1.1.8

6.1.11 cfgVpnOpenvpnCipher

Data-Channel Encryption Cipher List

Colon separated list of ciphers to allow for the OpenVPN data-channel encryption.

Set to ‘none’ to disable packet encryption.

Examples:

- **AES-256-GCM:AES-128-GCM**
- **AES-256-CBC**
- **AES-256-GCM**
- **none**: to disable packet encryption

For a full list of supported algorithms please consult the user manual.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.1.1.1.9

6.1.12 cfgVpnIpsecIke

IKE/ISAKMP SA Encryption/Authentication Algorithms

Comma-separated list of IKE/ISAKMP SA encryption/authentication algorithms to be used, e.g. aes128-sha256-modp3072. The notation is encryption-integrity[-prf]-dhgroup. In IKEv2, multiple algorithms and proposals may be included, such as aes128-aes256-sha1-modp3072-modp2048,3des-sha1-md5-modp1024.

It is possible to configure a PRF algorithm different to that defined for integrity protection. If no PRF is configured, the algorithms defined for integrity are proposed as PRF. The prf keywords are the same as the integrity algorithms, but have a prf prefix (such as prfsha1, prfsha256 or prfaesxcbc).

Defaults to aes128-sha256-modp3072 (aes128-sha1-modp2048,3des-sha1-modp1536 before 5.4.0) for IKEv1. The daemon adds its extensive default proposal to this default or the configured value. To restrict it to the configured proposal an exclamation mark (!) can be added at the end.

Refer to IKEv1CipherSuites and IKEv2CipherSuites for a list of valid keywords.

Note: As a responder both daemons accept the first supported proposal received from the peer. In order to restrict a responder to only accept specific cipher suites, the strict flag (!, exclamation mark) can be used, e.g: aes256-sha512-modp4096!

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.2.1.1.104

6.1.13 cfgVpnIpsecEsp

ESP Encryption/Authentication Algorithms

Comma-separated list of ESP encryption/authentication algorithms to be used for the connection, e.g. aes128-sha256. The notation is encryption-integrity[-dhgroup][-esnmode]. For IKEv2, multiple algorithms (separated by -) of the same type can be included in a single proposal. IKEv1 only includes the first algorithm in a proposal. Only either the ah or the esp keyword may be used, AH+ESP bundles are not supported.

Defaults to aes128-sha256. The daemon adds its extensive default proposal to this default or the configured value. To restrict it to the configured proposal an exclamation mark (!) can be added at the end.

Note: As a responder, the daemon defaults to selecting the first configured proposal that's also supported by the peer. By disabling charon.prefer_configured_proposals in strongswan.conf this may be changed to selecting the first acceptable proposal sent by the peer instead. In order to restrict a responder to only accept specific cipher suites, the strict flag (!, exclamation mark) can be used, e.g: aes256-sha512-modp4096!

If dh-group is specified, CHILD_SA rekeying and initial negotiation include a separate Diffe-Hellman exchange (this also applies to IKEv1 Quick Mode). However, for IKEv2, the keys of the CHILD_SA created implicitly with the IKE_SA will always be derived from the IKE_SA's key material. So any DH group specified here will only apply when the CHILD_SA is later rekeyed or is created with a separate CREATE_CHILD_SA exchange. Therefore, a proposal mismatch might not immediately be noticed when the SA is established, but may later cause rekeying to fail.

Valid values for esnmode are esn and noesn. Specifying both negotiates extended sequence number support with the peer, the default is noesn.

Refer to IKEv1CipherSuites and IKEv2CipherSuites for a list of valid keywords.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.2.1.1.105

6.1.14 cfgVpnIpsecPassword

IPsec Password

When `cfgVpnIpsecRightAuth` is set to **psk**.

A preshared secret is most conveniently represented as a sequence of characters. The sequence

cannot contain newline or double-quote characters. Alternatively, preshared secrets can be represented as hexadecimal or Base64 encoded binary values. A character sequence beginning with 0x is interpreted as sequence hexadecimal digits. Similarly, a character sequence beginning with 0s is interpreted as Base64 encoded binary data.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.2.1.1.113

6.1.15 cfgVpnIpsecCalds

IPsec CA Certificate ID

This value contains the id(s) to reference the ca certificate in the certificate store.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.2.1.1.116

6.1.16 cfgVpnIpsecGlblCustomOptions

Custom Global IPsec Options

Set to `none` when no additional options shall be added.

When setting multiple options, separate them with a semicolon `;`.

Example to enable aggressive mode for PSK with IKEv1:

- `charon.i_dont_care_about_security_and_use_aggressive_mode_psk=yes`

For a full list of all available options, please see: https://wiki.strongswan.org/projects/strongswan/wiki/Strongswanco

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.2.2.2

6.1.17 cfgVpnWgPEndpoint

Wireguard Peer Endpoint

Specifies the remote end by IP and port.

Set to `0.0.0.0:0`, when the local peer accepts connections, but does not initiate by itself.

Examples:

- 192.168.1.20:51820
- 0.0.0.0:0

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.5.2.1.5

6.1.18 cfgVpnWgPAllowedIps

Wireguard Peer Allowed IPs

The Allowed IPs refers to the addresses inside the tunnel. It has two meanings:

In TX direction it acts as routing table. Frames with a destination matching the Allowed IPs are encrypted. All other frames that are routed to the interface but don't match the Allowed IPs are dropped.

In RX direction it acts as ACL. Only frames where the source matches the Allowed IPs are accepted. Everything else is dropped.

Multiple space and/or comma separated networks in CIDR notation may be specified.

When set to `none`, no frames will be sent nor received.

Examples:

- none
- 0.0.0.0/0
- 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.5.2.1.6

6.1.19 cfgLdapTlsCiphers

OpenSSL Cipher String for LDAP

Specify which OpenSSL ciphers to use for the LDAP connection.

Please read the user manual and the OpenSSL documentation for a list of available ciphers and used syntax.

Set to 'none' to disable restriction.

Examples:

- ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384
- none

Applies to AP and STA.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1005.17

6.1.20 cfgCellDeviceOperatorSpn

Operator Selection Service Provider Name (SPN)

Name of the operator if the selection mode `cfgCellDeviceOperatorMode` is set to **fix(1)** or **fixWithFallbackAuto(2)**.

Long format alphanumeric up to 16 characters. The string of the currently connected provider can be read from `swCellServiceName`.

Note: If the service provider name is not defined or is incorrect, the modem cannot connect to the mobile network and remote access is lost.

Applies to cellular products only.

Type	DisplayString
Range	1 - 16
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.101.7.1.5

6.1.21 cfgDhcpDnsmasqDnsRebindDomainOk

Allowed Domains for DNS Rebind Protection

This entry is active when `cfgDhcpDnsmasqDnsStopDnsRebind` is enabled.

Enter a space and/or comma separated list of domains which are allowed to resolve to private addresses (RFC1918).

No Domains are excepted when set to `none`.

Examples:

- example.com, example.net, example.org
- yourdomain.com anotherdomain.com

Note: Subdomains are included when excepting domains. e.g when domain.net is set, then subdomain1.domain.net and subdomain2.domain.net are excepted as well.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.13.2.1.9

6.1.22 cfgHttpMonitorPasswordHash

Monitor Password Hash

Used for configuration import/export only.

Use WebAPI or Web Interface to change the Password.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.15.11

6.1.23 cfgHttpTlsCiphers

OpenSSL Cipher and Ciphersuites String for HTTPS server

Specify which OpenSSL ciphers and ciphersuites to use for HTTPS connections.

Please read the user manual and the OpenSSL documentation for a list of available ciphers, ciphersuites and used syntax.

Up to TLSv1.2, OpenSSL uses ciphers, while with TLSv1.3 ciphersuites are used. The format for this parameter is as follows: [|], i.e. the pipe ('|') sign is used to separate the ciphers from the ciphersuites.

If ciphers or ciphersuites is left empty, no restrictions are applied and all of the related built-ins are available. If ciphers is set with the special string 'disable', the support for TLSv1.2 and below is disabled, while 'disable' given as cyphersuites disables TLSv1.3.

Set to 'none' to disable restriction.

Examples:

- **ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384**

  limit TLSv1.2 to the selected two ciphers, leave TLSv1.3 ciphersuites all enabled

- **DHE-RSA-AES256-GCM-SHA384|TLS_AES_256_GCM_SHA384**

  limit TLSv1.2 to one cipher and TLSv1.3 to one ciphersuite

- **DHE-RSA-AES256-GCM-SHA384|disable**

  limit TLSv1.2 to one cipher and disable TLSv1.3 support

- **disable|TLS_AES_256_GCM_SHA384**

  disable TLSv1.2 support and limit TLSv1.3 to one ciphersuite

- **|TLS_AES_256_GCM_SHA384**

  leave all TLSv1.2 enabled, limit TLSv1.3 to one ciphersuite

- **|disable**

  leave all TLSv1.2 ciphers enabled, disable TLSv1.3 support

- **disable|**

disable TLSv1.2 support, leave all TLSv1.3 ciphersuites enabled

- **none**

  no restrictions for TLSv1.2 and TLSv1.3

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.15.14

6.1.24 cfgHttpAdminPasswordHash

Admin Password Hash

Used for configuration import/export only.

Use WebAPI or Web Interface to change the Password.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.15.9

6.1.25 cfgLldpDescription

LLDP Description

Applies to AP and STA.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.16.2

6.1.26 cfgMdnsNetwork

mDNS Aware Network Interfaces

When set to the keywork `all` it will bind to all valid interfaces.

Multiple interfaces may be specified as a space and/or comma separated list.

Examples:

- br0.vlan0
- br0.vlan0, br0.vlan7, br0.vlan99
- br0.vlan0 br0.vlan66

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.17.2

6.1.27 cfgWlanDevQmrrString

A list of rate controller quadruples per queue.

Each quadruple consist of (mcs-rate [0-31], tries [0-15], rts_cts [0-1], sgi [0-1]) with 4 entries per queue.

16 values together are for a single queue.

The values are in the form: rate1, try1, rts_cts1, sgi1, rate2, . . . , rate4, try4, rts_cts4, sgi4.

The order of the queues is VO, VI, BE, BK.

QMRR override for a specific queue is disabled when its respective try1 value is 0.

When QMRR override is disabled, the normal minstrel or other configured overrides, are used.

Frames in the VO queue are never aggregated.

All characters other than numbers are ignored

Example:

[(7 1 0 0) (4 2 0 0) (2 3 0 0) (0 4 1 0)] [(7 1 0 0) (4 1 0 1) (2 1 0 1) (0 1 1 1)] [(7 1 0 0) (4 1 0 0) (0 0 0 0) (0 0 0 0)] [(7 1 0 0) (0 0 0 0) (0 0 0 0) (0 0 0 0)]

Applies to AP and STA. 802.11n products only.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.1.1.26

6.1.28 cfgWlan802dot1xCiphers

OpenSSL Cipher String for the RADIUS Client

This is an OpenSSL specific configuration option for configuring the default cipher.

Please read the documentation for a list of all available ciphers and used syntax.

Used only if `cfgWlanIfaceEncryption` is **eap(6)**, **eap2(10)** or **eap192(11)**.

Examples:

- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384
- none

Applies to STA.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.10.1.21

6.1.29 cfgWlan802dot1xCaIds

Certificate Authority (CA) IDs

Reference to the CA which should be used.

Multiple CAs may be referenced by writing the ids of the CAs as space and/or comma separated list. The order of the list is the order how the CAs will be concatenated.

Setting the CA ID to `-1` disables the CA verification.

Examples:

- `-1`
- `12`
- `1, 3, 4`
- `1 3 4`

Applies to STA.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.10.1.25

6.1.30 cfgWlan802dot1xDynamicVlan

Dynamic VLAN

This parameter is only active when the wlan interface is bridged using `cfgNetWlanBridge`. Dynamic VLAN can not be used together with 802.11r (`cfgWlan802dot11rEnabled`).

Allow the RADIUS authentication server to decide which VLAN is used for the stations. This information is parsed from following RADIUS attributes based on RFC 3580 and RFC 2868: Tunnel-Type (value 13 = VLAN), Tunnel-Medium-Type (value 6 = IEEE 802) Tunnel-Private-Group-ID (value VLANID as a string).

- **disabled(0)**: No dynamic VLANs are used
- **optional(1)**: Use default interface if the RADIUS server does not include a VLAN ID
- **required(2)**: Reject authentication if the RADIUS server does not include a VLAN ID

Applies to AP.

Enumeration	disabled (0), optional (1), required (2)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.10.1.28

6.1.31 cfgWlanIfaceBitrates

Fixed MCS Index For 802.11n Rates

Set to `-1` to not force an MCS index (auto-rate).

Allows multiple space and/or comma separated indices which are then used in auto rate.

This entry is only active when `cfgWlanDevModulation` is set to **ng(10)** or **na(12)**

Examples:

- -1
- 0 1 2 3 4 5 6 7
- 0, 4, 7, 8, 12, 15

Applies to AP and STA. 802.11n products only.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.2.1.11

6.1.32 cfgWlanIfaceInactivityTimeout

Allowed idle time before station is removed

If a station does not send anything in ap_max_inactivity seconds, an empty data frame is sent to it in order to verify whether it is still in range. If this frame is not ACKed, the station will be disassociated and then deauthenticated. This feature is used to clear the station table of old entries when the STAs move out of range.

Applies to AP. 802.11n products only.

Range	15 - 65535
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.2.1.23

6.1.33 cfgRouteTableRoutingTables

Routing Tables on Which Route are Created

This is a space and/or comma separated list of tables on which the route will be created.

Specify 254 to create routes on the `main` table.

Valid values are > 0 and < 2000000000. However in this range there are reserved values that may not be used:

- 128: prelocal
- 253: default
- 255: local

Use `cfgRouteRuleTable` to create policies which use the tables specified here.

Examples:

- 5000
- 254, 7000

- 100 254, 8000

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.4.2.1.11

6.1.34 cfgRouteDhcpRoutingTables

Routing Tables on Which Received Routes are Created

This is a space and/or comma separated list of tables on which the route will be created.

Specify 254 to create routes on the `main` table.

Valid values are > 0 and < 2000000000. However in this range there are reserved values that may not be used:

- 128: prelocal
- 253: default
- 255: local

Use `cfgRouteRuleTable` to create policies which use the table specified here.

Examples:

- 5000
- 254, 7000
- 100 254, 8000

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.4.5.1.5

6.1.35 setWlanDevIndex

Table Entry Index

Range	0 - 2
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.4.3.1.1.1

6.1.36 setTlsCltTlsCiphers

OpenSSL Cipher String for the TLS Client

This is an OpenSSL specific configuration option for configuring the cipher.

Please read the user manual and the OpenSSL documentation for a list of available ciphers and used syntax.

Set to 'none' to disable restriction.

Examples:

- ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384
- none

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.4.9.5

6.2 MIB Reference: WESTERMO-SW6-NWM-MIB

6.2.1 cfgAfmRedundantName

Name of the Redundant Area Frequency Manager

Applies to AP. 802.11n products only.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.3.1.7.10.2

6.2.2 cfgAfmNeighbourName

Name of the Neighbour (Adjacent) Area Frequency Manager

Applies to AP. 802.11n products only.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.3.1.7.20.1.3

6.3 MIB Reference: WESTERMO-SW6-GNSS-MIB

6.3.1 cfgGnssDevDebugEnabled

Disable or Enable Debug Messages

Applies to cellular products only.

Enumeration	disabled (0), enabled (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.10.1.1.2.4