Software 6 Release Notes

Release 6.10.0-2

Westermo Network Technologies AB

September 1, 2022

Contents

1 General Information

Company
Westermo Network Technologies AB

Contact Support
www.westermo.com

Release Number
6.10.0-2

Software Build Number
18f9ecd6f855fadf4599ed4b798ef463a3d76dfc

Date of this build
September 1, 2022

2 Release Highlights

2.1 6.10.0-0

- Certificate Management: New Certificate and Key Management System
- Certificate Management: Automatic Certificate Monitoring
- Certificate Management: CRL Auto-Download
- Certificate Management: Support for SCEP
- WebInterface/WebAPI/SNMP: Support for two Roles ’admin’ and ’monitor’
- WebInterface/WebAPI: Support LDAPS as Authentication Backend
- WebInterface: Configurable TLS Ciphers
- WebInterface/WebAPI: Add Security Log
- WebAPI: New endpoint: Status
- CLI: Add Session Timeout
- NLM: monitor types RSSI and LOGIC, per monitor traps
- 802.1X: Support for Daily Refresh of 802.1X
- 802.1X: Support for RADIUS Polling (RADIUS Redundancy)
- Wlan: Enable RX stall watchdog (802.11n products only)
- Cellular: Support for Multiple EPS Bearer
- Configuration: Extended Input Validation and Error Notification
- Configuration: Support for Encrypted Configuration Files
- Support: Support for Encrypted Support Files
- DHCP-Server: Support for DHCP-Relay
- Network: Support for Unicast VXLAN
- Firewall: Support for Mangle Operations (MSS and TTL)

2.2 6.10.0-1

- Wlan: Fix l2nat router autolearn mode
- Wlan: Fix roaming-decission in mixed HT20/HT40 (802.11n products only)
- Wlan: Fix keylifetime for SAEPSK to 68 years
- Cellular: Handle additional QMI disconnect reason
- Wireguard: Fix PSK
- NTP: Prevent y2k38 injection
- WebInterface: Prevent override of EAP settings in QuickSetup

2.3 6.10.0-2

- WebInterface/WebAPI/SNMP: Fix human readable uptime
- Cellular: Fix MTU handling of multiple default EPS bearer at 1500/1504 bytes
- Cellular: Detect and handle potential HW hang
- Upgrade: Fix custom config processing for upgrade through SNMP
- NLM: Fix NLM status during FQDN reresolve with unreachable DNS server
- CVE: Fix CVE-2022-36946

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 or marked as obsolete:

- cfgFwMangle (added)
- cfgFwMangleTable (added)
- cfgFwMangleTableEntry (added)
- cfgFwMnglIndex (added)
- cfgFwMnglEnabled (added)
- cfgFwMnglChain (added)
- cfgFwMnglAction (added)
- cfgFwMnglValue (added)
- cfgFwMnglInputInterface (added)
- cfgFwMnglOutputInterface (added)
- cfgFwMnglSourceAddress (added)
- cfgFwMnglDestinationAddress (added)
- cfgFwMnglComment (added)
- cfgNetEth802dot1xTable (added)
- cfgNetEth802dot1xTableEntry (added)
- cfgNetEth802dot1xIndex (added)
- cfgNetEth802dot1xName (added)
- cfgNetEth802dot1xEnabled (added)
- cfgNetEth802dot1xOwnIpAddr (added)
- cfgNetEth802dot1xAuthServerParameter (added)
- cfgNetEth802dot1xEapReauthPeriod (added)

- cfgWlan802dot1xRetryMax (added)
- cfgWlan802dot1xRetryTimeout (added)
- cfgWlan802dot1xPrimaryTestMode (added)
- cfgWlan802dot1xCrlExpiryExtension (added)
- cfgWlan802dot1xCaIds (added)
- cfgWlan802dot1xClientCertId (added)
- cfgLogRemoteType (added)
- cfgDhcpRelayTable (added)
- cfgDhcpRelayTableEntry (added)
- cfgDhcpRelayIndex (added)
- cfgDhcpRelayEnabled (added)
- cfgDhcpRelayInterface (added)
- cfgDhcpRelayLocalAddress (added)
- cfgDhcpRelayServerAddress (added)
- cfgDhcpRelayInterfaceToServer (added)
- cfgHttpTlsServerCertId (added)
- cfgHttpAdminPasswordHash (added)
- cfgHttpMonitorPasswordHash (added)
- cfgHttpSessionLimit (added)
- cfgHttpSessionTimeout (added)
- cfgHttpTlsCiphers (added)
- cfgNlmMonCountUp (added)
- cfgNlmMonRssi (added)
- cfgNlmMonLogic (added)

- cfgNlmMonLogicInput (added)
- cfgNlmMonTrap (added)
- cfgCliSshSessionTimeout (added)
- cfgCellSimSlotTable (added)
- cfgCellSimSlotTableEntry (added)
- cfgCellSimSlotIndex (added)
- cfgCellSimSlotName (added)
- cfgCellSimSlotEnabled (added)
- cfgCellSimSlotPinEnabled (added)
- cfgCellSimSlotPin (added)
- cfgCellSimSlotPriority (added)
- cfgCellSimSlotUnlockTimeout (added)
- cfgCellDefaultBearerTable (added)
- cfgCellDefaultBearerTableEntry (added)
- cfgCellDefaultBearerIndex (added)
- cfgCellDefaultBearerSimSlots (added)
- cfgCellDefaultBearerApn (added)
- cfgCellDefaultBearerUsername (added)
- cfgCellDefaultBearerPassword (added)
- cfgCellDefaultBearerAuthType (added)
- cfgCellDefaultBearerRoaming (added)
- cfgCertificate (added)
- cfgCrtCrlTable (added)
- cfgCrtCrlTableEntry (added)

- cfgCrtCrlIndex (added)
- cfgCrtCrlCaId (added)
- cfgCrtCrlEnabled (added)
- cfgCrtCrlUrl (added)
- cfgCrtCrlTimeBeforeExpire (added)
- cfgCrtCrlRetryPeriod (added)
- cfgCrtMonitoringTable (added)
- cfgCrtMonitoringTableEntry (added)
- cfgCrtMonIndex (added)
- cfgCrtMonEnabled (added)
- cfgCrtMonType (added)
- cfgCrtMonId (added)
- cfgCrtMonTimeBeforeExpire (added)
- cfgCrtMonRepeatPeriod (added)
- cfgCrtGlobal (added)
- cfgCrtGlblDailyRefreshEnabled (added)
- cfgCrtGlblDailyRefreshTime (added)
- cfgScep (added)
- cfgScepTable (added)
- cfgScepTableEntry (added)
- cfgScepIndex (added)
- cfgScepCaIdentifier (added)
- cfgScepChallengePassword (added)
- cfgScepPollingInterval (added)

- cfgScepPollingMaxTries (added)
- cfgScepAutoRenewEnabled (added)
- cfgScepAutoRenewTimeBeforeExpire (added)
- cfgScepAutoRenewRetryPeriod (added)
- cfgScepCsrCN (added)
- cfgScepServerUrl (added)
- cfgScepCsrC (added)
- cfgScepCsrST (added)
- cfgScepCsrL (added)
- cfgScepCsrO (added)
- cfgScepCsrOU (added)
- cfgScepCaId (added)
- cfgScepCertId (added)
- cfgVpnOpenvpnCaIds (added)
- cfgVpnOpenvpnCertId (added)
- cfgVpnOpenvpnStaticKeyId (added)
- cfgVpnIpsecCaIds (added)
- cfgVpnIpsecLeftCertId (added)
- cfgVpnIpsecRightCertId (added)
- cfgVpnIpsecLeftSigkeyId (added)
- cfgVpnIpsecRightSigkeyId (added)
- cfgVpnIpsecLeftKeyId (added)
- cfgVpnTepVnid (added)
- cfgVpnTepDestinationPort (added)

- cfgLdap (added)
- cfgLdapEnabled (added)
- cfgLdapUrl1 (added)
- cfgLdapUrl2 (added)
- cfgLdapCaIds (added)
- cfgLdapUserBaseDn (added)
- cfgLdapAccessDn (added)
- cfgLdapAccessPassword (added)
- cfgLdapAccessFilter (added)
- cfgLdapUserRoleAttribute (added)
- cfgLdapAdminRoleDn (added)
- cfgLdapMonitorRoleDn (added)
- cfgLdapRequestTimeout (added)
- cfgLdapCrlExpiryExtension (added)
- cfgLdapTlsControlParams (added)
- cfgLdapTlsCiphers (added)
- rpcCrtCrlTable (added)
- rpcCrtCrlTableEntry (added)
- rpcCrtCrlIndex (added)
- rpcCrtCrlGet (added)
- rpcCrtAttribute (added)
- rpcScep (added)
- rpcScepTable (added)
- rpcScepTableEntry (added)

- rpcScepIndex (added)
- rpcScepGetCaCrt (added)
- rpcScepEnroll (added)
- setCfgFileType (added)
- setCfgFilePassword (added)
- setCrtFileId (added)
- setCrtFileType (added)
- setCrtAttributeKey (added)
- setCrtAttributeValue (added)
- setCrtFilePassphrase (added)
- setSysSupportFile (added)
- setSysSfEncryptionEnabled (added)
- setSysSfEncryptionPassword (added)
- setTlsClient (added)
- setTlsCltCaIds (added)
- setTlsCltCrlExpiryExtension (added)
- setTlsCltTlsControlParams (added)
- setTlsCltTlsCiphers (added)
- swDrvCntWlanBeaconMiss (added)
- swDrvCntWlanBeaconRx (added)
- swDrvCntWlanApBeaconMiss (added)
- swDrvCntWlanPilotMiss (added)
- swDrvCntWlanPilotRx (added)
- swCertificate (added)

- swCrtExpirationTime (added)
- swCrtFingerprint (added)
- swCrtCertTable (added)
- swCrtCertTableEntry (added)
- swCrtCertTableIndex (added)
- swCrtCertId (added)
- swCrtCertLabel (added)
- swCrtCertExpirationTime (added)
- swCrtCertFingerprint (added)
- swCrtCrlTable (added)
- swCrtCrlTableEntry (added)
- swCrtCrlTableIndex (added)
- swCrtCrlId (added)
- swCrtCrlLabel (added)
- swCrtCrlExpirationTime (added)
- swCrtCrlFingerprint (added)
- swCellLteMode (added)
- swCellEarfcn (added)
- swCellCellId (added)
- swCellBandwidthUl (added)
- swCellBandwidthDl (added)
- cfgWlanBsteerMatchingWlan (added)
- cfgFwNatPrtFwdSourceAddress (changed)
- cfgFwNatPrtFwdDestinationAddress (changed)

- cfgFwNatOutSourceAddress (changed)
- cfgFwNatOutDestinationAddress (changed)
- cfgFwNatOneToOneSourceNet (changed)
- cfgFwNatOneToOneDestinationNet (changed)
- cfgFwNatOneToOneRewriteNet (changed)
- cfgFwL2IpFltrSource (changed)
- cfgFwL2IpFltrDestination (changed)
- cfgIclConnectionThreshold (changed)
- cfgIclInterfaceName (changed)
- cfgIclDisconnectionThreshold (changed)
- cfgSysHostname (changed)
- cfgSysNsType (changed)
- cfgSysNsDhcpInterface (changed)
- cfgNetVlanParent (changed)
- cfgNetIpInterface (changed)
- cfgNetCarpSyncInterface (changed)
- cfgNetMacVlanParent (changed)
- cfgNetWwanIndex (changed)
- cfgWlanDevPower (changed)
- cfgWlanAclWhiteInterface (changed)
- cfgWlanAclBlackInterface (changed)
- cfgWlanGlblConnectionStatusWlanInterface (changed)
- cfgWlan802dot1xTlsControlParams (changed)
- cfgRouteTableDestinationNetwork (changed)

- cfgRouteDhcpInterface (changed)
- cfgMRouteTableInput (changed)
- cfgMRouteTableSource (changed)
- cfgMRouteTableInput (changed)
- cfgMRouteTableOutput (changed)
- cfgRouteRuleFrom (changed)
- cfgRouteRuleTo (changed)
- cfgQosIpToTidMapSrcNet (changed)
- cfgQosIpToTidMapDestNet (changed)
- cfgQosIpToTidMapSrcPort (changed)
- cfgQosIpToTidMapDestPort (changed)
- cfgQosEthertypeToL2Ethertype (changed)
- cfgDhcpScopeInterface (changed)
- cfgDhcpHstOvrAddress (changed)
- cfgNlmMonType (changed)
- cfgNlmMonCount (changed)
- cfgNlmMonUpAction (changed)
- cfgNlmMonDownAction (changed)
- cfgNlmMonScanLoopInterval (changed)
- cfgVpnOpenvpnLocal (changed)
- cfgVpnTepSource (changed)
- cfgVpnTepDestination (changed)
- setCfgFileUrl (changed)
- setWlanDevFrequency (changed)

- setWlanDevPower (changed)
- setFwFileUrl (changed)
- setCrtFileUrl (changed)
- setCrtFilePkcs12Passphrase (changed)
- setSysTime (changed)
- swDrvConStatWlanIf (changed)
- swCellWwanName (changed)
- swCellSimSlot (changed)
- cfgWlan802dot1xClientKeyPassword (obsolete)
- cfgSnmpdComMaintainer (obsolete)
- cfgHttpUser (obsolete)
- cfgHttpPassword (obsolete)
- cfgCellSimTable (obsolete)
- cfgCellSimTableEntry (obsolete)
- cfgCellSimIndex (obsolete)
- cfgCellSimSlot1 (obsolete)
- cfgCellSimSlot2 (obsolete)
- cfgCellSimPrimarySlot (obsolete)
- cfgCellSimUnlockTimeout (obsolete)
- cfgCellSimProfileTable (obsolete)
- cfgCellSimProfileTableEntry (obsolete)
- cfgCellSimProfileIndex (obsolete)
- cfgCellSimProfileApn (obsolete)
- cfgCellSimProfileUsername (obsolete)

- cfgCellSimProfilePassword (obsolete)
- cfgCellSimProfilePinEnabled (obsolete)
- cfgCellSimProfilePin (obsolete)
- cfgCellSimProfileAuthType (obsolete)
- cfgCellSimProfileRoaming (obsolete)
- cfgVpnOpenvpnKeyPassword (obsolete)
- cfgVpnIpsecKeyPassword (obsolete)
- rpcCrtRefresh (obsolete)
- setCrtFileSelector (obsolete)
- cfgWlanBsteerMatchingSsid (obsolete)

5 Changed Configuration Parameter Descriptions

5.1 MIB Reference: WESTERMO-SW6-MIB

5.1.1 cfgSysHostname

The Hostname of the Device

Valid characters for hostnames are ASCII(7) letters from a to z, the digits from 0 to 9, and the hyphen (-). A hostname may not start or end with a hyphen.

Type	DisplayString
Range	1 - 63
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1.1

5.1.2 cfgSysNsType

Type of the Nameserver Entry

- **none(0):** Disables this entry

- **server(1):** Uses the address specified by `cfgSysNsServer`
- **dhcpinterface(2):** Uses nameservers provided by a DHCP-client referenced by `cfgSysNsDhcpInterface`
- **ignoreinterface(3):** Ignore nameservers provided by a DHCP-client referenced by `cfgSysNsDhcpInterfac`

Enumeration	none (0), server (1), dhcpinterface (2), ignoreinterface (3)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1.11.1.2

5.1.3 cfgSysNsDhcpInterface

DHCP Client Interface

This parameter is only used when `cfgSysNsType` is set to **dhcpinterface(2)** or **ignoreinterface(3)**.

Name of an interface on which a DHCP client is running. This may be a DHCP client defined by `cfgNetIpTable` or a wwan or ovpn interface which have their own means of handling DHCP.

Examples:

- wlan0
- ovpn0
- macvlan2
- wwan0
- br0.vlan7

Type	DisplayString
Range	1 - 15
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1.11.1.4

5.1.4 cfgCliSshSessionTimeout

SSH Session Timeout

Disconnect the session if no traffic is transmitted or received for 'session timeout' seconds.

Setting to 0 disables session timeout.

Range	0 - 86400
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.100.10

5.1.5 cfgCertificate

OID	1.3.6.1.4.1.16177.1.400.1.1.1001

5.1.6 cfgCrtCrlTable

Certificate Revocation List configuration table.

Range	0 - 15
OID	1.3.6.1.4.1.16177.1.400.1.1.1001.1

5.1.7 cfgCrtCrlTableEntry

Certificate Revocation List configuration table entry.

OID	1.3.6.1.4.1.16177.1.400.1.1.1001.1.1

5.1.8 cfgCrtCrlIndex

Table Entry Index

Range	0 - 15
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.1.1001.1.1.1

5.1.9 cfgCrtCrlCaId

Reference to the CA ID in the certificate store.

The received CRL will be stored to the CRL ID of the CRL associated to the configured CA ID.

Applies to AP and STA.

Type	Integer32
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1001.1.1.2

5.1.10 cfgCrtCrlEnabled

Enable automatic download of the CRL

The CRL must be in the DER format.

Applies to AP and STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1001.1.1.3

5.1.11 cfgCrtCrlUrl

CRL URL

This URL is used to download the new CRL. The CRL must be in the DER format.

Example:

- http://192.168.1.2/certs/example.crl

Applies to AP and STA.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1001.1.1.4

5.1.12 cfgCrtCrlTimeBeforeExpire

Time before the current CRL expire

The new CRL will be downloaded this number of days before the CRL expire.

Applies to AP and STA.

Range	0 - 365
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1001.1.1.5

5.1.13 cfgCrtCrlRetryPeriod

Retry period in minutes

If the download of a CRL failed the device will retry to download after this period.

Applies to AP and STA.

Range	1 - 1440
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1001.1.1.6

5.1.14 cfgCrtMonitoringTable

Certificate Monitoring configuration table.

Range	0 - 15
OID	1.3.6.1.4.1.16177.1.400.1.1.1001.2

5.1.15 cfgCrtMonitoringTableEntry

Certificate Monitoring configuration table entry.

OID	1.3.6.1.4.1.16177.1.400.1.1.1001.2.1

5.1.16 cfgCrtMonIndex

Table Entry Index

Range	0 - 15
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.1.1001.2.1.1

5.1.17 cfgCrtMonEnabled

Enable certificate/CRL expiry monitor

The monitor observes if a certificate/CRL is about to expire and informs via Trap/Syslog if this is the case.

Applies to AP and STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1001.2.1.2

5.1.18 cfgCrtMonType

Monitor type

Define the type to be monitored.

- **1**: CRL
- **2**: Certificate

Applies to AP and STA.

Enumeration	crl (1), cert (2)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1001.2.1.3

5.1.19 cfgCrtMonId

ID of the certificate to be monitored

Reference to the certificate ID in the certificate store.

In order to monitor CA and Client/Server certificates the corresponding ID needs to be specified and the `cfgCrtMonType` needs to set to **cert(2)**.

In order to monitor CRL the ID of the associated CA ID needs to be specified and the `cfgCrtMonType` needs to set to **crl(1)**.

Applies to AP and STA.

Type	Integer32
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1001.2.1.4

5.1.20 cfgCrtMonTimeBeforeExpire

Start alert this time before the current CA certificate expire

This value is in days before the CA certificate expire.

Applies to STA.

Range	0 - 365
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1001.2.1.5

5.1.21 cfgCrtMonRepeatPeriod

Repeat period for CA certificate expiration alert

Repeat the alert every X hours.

Applies to STA.

Range	1 - 24
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1001.2.1.6

5.1.22 cfgCrtGlobal

OID	1.3.6.1.4.1.16177.1.400.1.1.1001.3

5.1.23 cfgCrtGlblDailyRefreshEnabled

Enable Daily Certificate Refresh

Applies to AP and STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1001.3.1

5.1.24 cfgCrtGlblDailyRefreshTime

Daily Automatic Refresh time.

Define time (hour:minute) at which a certificate refresh is called (if `cfgCrtGlblDailyRefreshEnabled` is **enabled(1)**).

The time is referenced to the local time as define in `cfgSysTimezone`

Examples:

- 00:00 - force refresh each day at midnight
- 01:00 - force refresh each day at 01:00
- 23:05 - force refresh each day at 23:05

Applies to AP and STA.

Type	DisplayString
Range	5 - 5
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1001.3.2

5.1.25 cfgScep

OID	1.3.6.1.4.1.16177.1.400.1.1.1002

5.1.26 cfgScepTable

SCEP Table

Applies to STA.

Range	0 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.1002.2

5.1.27 cfgScepTableEntry

SCEP Table Entry

Applies to STA.

OID	1.3.6.1.4.1.16177.1.400.1.1.1002.2.1

5.1.28 cfgScepIndex

Index of the Table Entry

Applies to STA.

Range	0 - 255
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.1.1002.2.1.1

5.1.29 cfgScepAutoRenewRetryPeriod

SCEP Certificate Renew Period

SCEP re-enrollment retry interval in minutes.

Applies to STA.

Range	5 - 1440
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1002.2.1.10

5.1.30 cfgScepCsrCN

CN (Common Name) field for CSR

Example:

- example.com

Applies to STA.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1002.2.1.11

5.1.31 cfgScepServerUrl

URL of SCEP server

Example:

- http://192.168.1.2:8080/scep

Applies to STA.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1002.2.1.12

5.1.32 cfgScepCsrC

C (Country) field for CSR

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

Example:

- CH

Applies to STA.

Type	DisplayString
Range	0 - 4
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1002.2.1.13

5.1.33 cfgScepCsrST

ST (State) field for CSR

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

Example:

- Zurich

Applies to STA.

Type	DisplayString
Range	0 - 63
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1002.2.1.14

5.1.34 cfgScepCsrL

L (Locality) field for CSR

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

Example:

- Bubikon

Applies to STA.

Type	DisplayString
Range	0 - 63
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1002.2.1.15

5.1.35 cfgScepCsrO

O (Organization) field for CSR

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

Applies to STA.

Type	DisplayString
Range	0 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1002.2.1.16

5.1.36 cfgScepCsrOU

OU (Organizational Unit) field for CSR

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

Applies to STA.

Type	DisplayString
Range	0 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1002.2.1.17

5.1.37 cfgScepCaId

Reference ID for CA Certificate

Set to -1 if not using a CA certificate.

Applies to STA.

Range	-1 - 65535
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1002.2.1.18

5.1.38 cfgScepCertId

Reference ID for Client Certificate

Set to -1 if not using a client certificate.

Applies to STA.

Range	-1 - 65535
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1002.2.1.19

5.1.39 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	0 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1002.2.1.3

5.1.40 cfgScepChallengePassword

SCEP Challenge Password

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

Applies to STA.

Type	DisplayString
Range	0 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1002.2.1.5

5.1.41 cfgScepPollingInterval

SCEP Polling Interval in seconds

Applies to STA.

Range	1 - 86400
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1002.2.1.6

5.1.42 cfgScepPollingMaxTries

Max number of SCEP GetCertInitial requests

Applies to STA.

Type	Integer32
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1002.2.1.7

5.1.43 cfgScepAutoRenewEnabled

Enable/disable SCEP automatic re-enrollment

Applies to STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1002.2.1.8

5.1.44 cfgScepAutoRenewTimeBeforeExpire

SCEP Certificate Renew Days

Number of days before certificate expiration (i.e. automatic re-enrollment shall start these number of days before certificate expiration)

Applies to STA.

Type	Integer32
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1002.2.1.9

5.1.45 cfgVpnOpenvpnKeyPassword

****OBSOLETE:** Password to Unlock Private Key**

This parameter is obsolete and has been replaced with the Certificate Store.

Key material on the device is always encrypted. The password to import the file has to be specified once during import via `setCrtFilePassphrase`

Type	DisplayString
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.1.1.1.17

5.1.46 cfgVpnOpenvpnCaIds

OpenVPN CA ID(s)

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

Type	DisplayString
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.1.1.1.25

5.1.47 cfgVpnOpenvpnCertId

OpenVPN Certificate ID

This value contain the id to reference a certificate in the certificate store.

Type	Integer32
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.1.1.1.26

5.1.48 cfgVpnOpenvpnStaticKeyId

OpenVPN Static Key ID

This value contain the id to reference the static key in the certificate store.

Type	Integer32
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.1.1.1.27

5.1.49 cfgVpnOpenvpnLocal

Local IP Address

The OpenVPN instance binds to the given IP address only. Address 0.0.0.0 binds the OpenVPN instance to all interfaces.

Type	IpAddress
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.1.1.1.3

5.1.50 cfgVpnIpsecKeyPassword

****OBSOLETE:** Password to Unlock Private Key**

This parameter is obsolete and has been replaced with the Certificate Store.

Key material on the device is always encrypted. The password to import the file has to be specified once during import via `setCrtFilePassphrase`

Type	DisplayString
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.2.1.1.112

5.1.51 cfgVpnIpsecCalds

IPsec CA Certificate ID

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

Type	DisplayString
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.2.1.1.116

5.1.52 cfgVpnIpsecLeftCertId

IPsec Left Certificate ID

This value contains the id of the certificate in the certificate store used for the left side.

Type	Integer32
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.2.1.1.117

5.1.53 cfgVpnIpsecRightCertId

IPsec Right Certificate ID

This value contains the id of the certificate in the certificate store used for the right side.

Type	Integer32
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.2.1.1.118

5.1.54 cfgVpnIpsecLeftSigkeyId

IPsec Left Sig Key ID

This value contains the id of the sig key in the certificate store used for the left side.

Type	Integer32
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.2.1.1.119

5.1.55 cfgVpnIpsecRightSigkeyId

IPsec Right Sig Key ID

This value contains the id of the sig key in the certificate store used for the right side.

Type	Integer32
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.2.1.1.120

5.1.56 cfgVpnIpsecLeftKeyId

IPsec Left Key ID

This value contains the id of the private key in the certificate store used for the left side.

Type	Integer32
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.2.1.1.121

5.1.57 cfgVpnTepVnid

Virtual Network ID

This parameter is active when `cfgVpnTepTunnelType` is set to **vxlan(2)**.

Specify the vxlan network id.

Range	0 - 16777215
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.6.1.1.11

5.1.58 cfgVpnTepDestinationPort

Destination Port

This parameter is active when `cfgVpnTepTunnelType` is set to **vxlan(2)**.

Specify the destination UDP port. At the same time this parameter defines on which port the local tunnel endpoint is listening for inbound vxlan frames.

Range	1 - 65535
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.6.1.1.12

5.1.59 cfgVpnTepSource

Source Address of the Tunnel

Can be set to 0.0.0.0 to let the system select the appropriate address based on the routing table.

Type	IpAddress
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.6.1.1.4

5.1.60 cfgVpnTepDestination

Destination Address of the Tunnel

Encapsulated frames are sent to this address.

Type	IpAddress
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1003.6.1.1.5

5.1.61 cfgLdap

OID	1.3.6.1.4.1.16177.1.400.1.1.1005

5.1.62 cfgLdapEnabled

Disable or Enable LDAP Authentication

Applies to AP and STA.

Enumeration	disabled (0), enabled (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1005.1

5.1.63 cfgLdapAdminRoleDn

DN for Role Admin

Distinguished name for role admin.

Example:

- 'CN=net_admin,OU=Groups,OU=Company,DC=excompany,DC=ex'

Applies to AP and STA.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1005.10

5.1.64 cfgLdapMonitorRoleDn

DN for Role Monitor

Distinguished name for role monitor.

Example:

- 'CN=net_operator,OU=Groups,OU=Company,DC=excompany,DC=ex'

Applies to AP and STA.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1005.12

5.1.65 cfgLdapRequestTimeout

LDAP Request Timeout

Maximum time in seconds allowed for an LDAP request to take.

Applies to AP and STA.

Range	0 - 120
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1005.13

5.1.66 cfgLdapCrlExpiryExtension

CRL Validity Period Extension in Days

If set, the validity period of a CRL can be extended by the given amount of days.

- **0** no extension
- **1-1095** extension days
- **-1** extend to infinity => ignore CRL expiry

Applies to AP and STA.

Type	Integer32
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1005.15

5.1.67 cfgLdapTlsControlParams

Bitfield to Control TLS Behavior

- **0x0** all validity checks will be performed
- **0x1** ignore certificate validity time
- **0x2** ignore ca certificate
- **0x4** ignore CRLs

- **0x8** ignore missing CRLs

Applies to AP and STA.

Range	0 - 15
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1005.16

5.1.68 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
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1005.17

5.1.69 cfgLdapUrl1

LDAP Server 1

Primary LDAP server name, ignored if set to '0.0.0.0'.

Applies to AP and STA.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1005.2

5.1.70 cfgLdapUrl2

LDAP Server 2

Secondary LDAP server name, ignored if set to '0.0.0.0'.

Applies to AP and STA.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1005.3

5.1.71 cfgLdapCaIds

LDAP CA Certificate IDs

Select the CAs to be used for LDAP server certificate validation. Multiple CAs can be referenced by writing the ids of the CAs as space/comma-separated list.

Examples:

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

Applies to AP and STA.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1005.4

5.1.72 cfgLdapUserBaseDn

The Searchbase for LDAP User Base DN Retrieval

This is the starting point for the search in the LDAP database.

Using ldapsearch from openldap-utils, this corresponds to option '-b' (searchbase).

Example:

- 'dc=excompany, dc=ex'

Applies to AP and STA.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1005.5

5.1.73 cfgLdapAccessDn

The Bind-DN for LDAP User Search

This is the Distinguished Name (DN) to bind to the LDAP directory when searching for the user's DN.

Using ldapsearch from openldap-utils, this corresponds to option '-D'.

Example:

- 'cn=admin,ou=product accounts,dc=excompany,dc=ex'

Applies to AP and STA.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1005.6

5.1.74 cfgLdapAccessPassword

Simple Authentication Password for LDAP User Search

This is the password for simple authentication when searching for the user's DN.

Using ldapsearch from openldap-utils, this corresponds to option '-w'.

Applies to AP and STA.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1005.7

5.1.75 cfgLdapAccessFilter

Search Filter for LDAP User Search

Using ldapsearch from openldap-utils, this corresponds to argument 'filter'.

The string might have the following placeholder that is replaced with the according parameter: * '%USER%': username to retrieve role for

Example:

- `(sAMAccountName=%USER%)`

Applies to AP and STA.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1005.8

5.1.76 cfgLdapUserRoleAttribute

LDAP Attribute Name for User's Role Retrieval

Attribute name to be used to retrieve the user's role.

Example:

- `memberOf`

Applies to AP and STA.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1005.9

5.1.77 cfgCellSimTable

****OBSOLETE:** SIM Parameter Table**

This parameter is obsolete and has been replaced with `cfgCellSimSlotTable` and `cfgCellDefaultBearerTab`

Range	0 - 0
OID	1.3.6.1.4.1.16177.1.400.1.1.101.1

5.1.78 cfgCellSimTableEntry

****OBSOLETE:** SIM Parameter Table Entry**

This parameter is obsolete and has been replaced with `cfgCellSimSlotTable` and `cfgCellDefaultBearerTab`

OID	1.3.6.1.4.1.16177.1.400.1.1.101.1.1

5.1.79 cfgCellSimIndex

****OBSOLETE:** Table Entry Index**

This parameter is obsolete and has been replaced with `cfgCellSimSlotTable` and `cfgCellDefaultBearerTab`

Range	0 - 0
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.1.101.1.1.1

5.1.80 cfgCellSimSlot1

****OBSOLETE:** SIM Slot 1**

This parameter is obsolete and has been replaced with `cfgCellSimSlotTable` and `cfgCellDefaultBearerTab`

Range	-1 - -1
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.1.101.1.1.2

5.1.81 cfgCellSimSlot2

****OBSOLETE:** SIM Slot 2**

This parameter is obsolete and has been replaced with `cfgCellSimSlotTable` and `cfgCellDefaultBearerTab`

Range	-1 - -1
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.1.101.1.1.3

5.1.82 cfgCellSimPrimarySlot

****OBSOLETE:** Primary SIM Slot**

This parameter is obsolete and has been replaced with `cfgCellSimSlotTable` and `cfgCellDefaultBearerTab`

Enumeration	obsolete (-1)
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.1.101.1.1.4

5.1.83 cfgCellSimUnlockTimeout

****OBSOLETE:** SIM Unlock Timeout**

This parameter is obsolete and has been replaced with `cfgCellSimSlotTable` and `cfgCellDefaultBearerTab`

Range	-1 - -1
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.1.101.1.1.5

5.1.84 cfgCellSimProfileTable

****OBSOLETE:** SIM Profiles**

This parameter is obsolete and has been replaced with `cfgCellSimSlotTable` and `cfgCellDefaultBearerTab`

Range	0 - 9
OID	1.3.6.1.4.1.16177.1.400.1.1.101.2

5.1.85 cfgCellSimProfileTableEntry

****OBSOLETE:** SIM Profile**

This parameter is obsolete and has been replaced with `cfgCellSimSlotTable` and `cfgCellDefaultBearerTab`

OID	1.3.6.1.4.1.16177.1.400.1.1.101.2.1

5.1.86 cfgCellSimProfileIndex

****OBSOLETE:** Table Entry Index**

This parameter is obsolete and has been replaced with `cfgCellSimSlotTable` and `cfgCellDefaultBearerTab`

Range	0 - 9
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.1.101.2.1.1

5.1.87 cfgCellSimProfileApn

****OBSOLETE:** Access Point Name**

This parameter is obsolete and has been replaced with `cfgCellSimSlotTable` and `cfgCellDefaultBearerTab`

Type	DisplayString
Range	1 - 255
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.1.101.2.1.2

5.1.88 cfgCellSimProfileUsername

****OBSOLETE:** Username**

This parameter is obsolete and has been replaced with `cfgCellSimSlotTable` and `cfgCellDefaultBearerTab`

Type	DisplayString
Range	1 - 255
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.1.101.2.1.3

5.1.89 cfgCellSimProfilePassword

****OBSOLETE:** Password**

This parameter is obsolete and has been replaced with `cfgCellSimSlotTable` and `cfgCellDefaultBearerTab`

Type	DisplayString
Range	1 - 255
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.1.101.2.1.4

5.1.90 cfgCellSimProfilePinEnabled

****OBSOLETE:** PIN Authentication Disabled or Enabled**

This parameter is obsolete and has been replaced with `cfgCellSimSlotTable` and `cfgCellDefaultBearerTab`

Enumeration	obsolete (-1)
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.1.101.2.1.5

5.1.91 cfgCellSimProfilePin

****OBSOLETE:** PIN of the SIM Card**

This parameter is obsolete and has been replaced with `cfgCellSimSlotTable` and `cfgCellDefaultBearerTab`

Type	DisplayString
Range	1 - 255
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.1.101.2.1.6

5.1.92 cfgCellSimProfileAuthType

****OBSOLETE:** Authentication Type**

This parameter is obsolete and has been replaced with `cfgCellSimSlotTable` and `cfgCellDefaultBearerTab`

Enumeration	obsolete (-1)
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.1.101.2.1.7

5.1.93 cfgCellSimProfileRoaming

****OBSOLETE:** Roaming Disabled or Enabled**

This parameter is obsolete and has been replaced with `cfgCellSimSlotTable` and `cfgCellDefaultBearerTab`

Enumeration	obsolete (-1)
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.1.101.2.1.8

5.1.94 cfgCellSimSlotTable

SIM Slot Table

Applies to cellular products only.

Range	0 - 1
OID	1.3.6.1.4.1.16177.1.400.1.1.101.5

5.1.95 cfgCellSimSlotTableEntry

SIM Slot Entry

Applies to cellular products only.

OID	1.3.6.1.4.1.16177.1.400.1.1.101.5.1

5.1.96 cfgCellSimSlotIndex

Table Entry Index

Range	0 - 1
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.1.101.5.1.1

5.1.97 cfgCellSimSlotName

Name of the SIM Slot

The name of the pysical SIM slot. At least one SIM slot must be assigned to the default bearer configuration `cfgCellDefaultBearerSimSlots`.

Applies to cellular products only.

Type	DisplayString
Range	1 - 255
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.1.1.101.5.1.2

5.1.98 cfgCellSimSlotEnabled

Enable SIM Slot

Enable the physical SIM slot if a SIM card is inserted. SIM slots without SIM card should be disabled when SIM rotation `cfgCellConnMgmtSimRotationEnabled` is enabled.

Applies to cellular products only.

Enumeration	disabled (0), enabled (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.101.5.1.3

5.1.99 cfgCellSimSlotPinEnabled

PIN Authentication Disabled or Enabled

Set to **enabled(1)** if PIN authentication is required for the SIM card in the corresponding slot.

Applies to cellular products only.

Enumeration	disabled (0), enabled (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.101.5.1.4

5.1.100 cfgCellSimSlotPin

PIN of the SIM Card

The PIN is ignored, when PIN authentication is disabled, see `cfgCellSimSlotPinEnabled`.

Applies to cellular products only.

Type	DisplayString
Range	4 - 4
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.101.5.1.5

5.1.101 cfgCellSimSlotPriority

SIM Slot Priority

A lower value means a higher priority.

If two SIM slots have the same priority, the SIM slot with the lower index is preferred.

Applies to cellular products only.

Range	0 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.101.5.1.6

5.1.102 cfgCellSimSlotUnlockTimeout

SIM Unlock Timeout

The time in milliseconds how long the unlocking process waits until the SIM card is ready to be unlocked. Increase the timeout if older SIM cards cannot be unlocked. A high timeout affects the performance of SIM rotation.

Note: Changes become effective after restarting the device.

Applies to cellular products only.

Range	300 - 30000
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.101.5.1.7

5.1.103 cfgCellDefaultBearerTable

Default Bearer Table

Each cellular interface defined in `cfgNetWwanTable` enables a default bearer configuration.

Applies to cellular products only.

Range	0 - 7
OID	1.3.6.1.4.1.16177.1.400.1.1.101.6

5.1.104 cfgCellDefaultBearerTableEntry

Default Bearer Entry

Applies to cellular products only.

OID	1.3.6.1.4.1.16177.1.400.1.1.101.6.1

5.1.105 cfgCellDefaultBearerIndex

Table Entry Index

Range	0 - 7
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.1.101.6.1.1

5.1.106 cfgCellDefaultBearerSimSlots

Default Bearer SIM Slot Selection

A default bearer must refer to at least one physical SIM slot. The name of the SIM slot `cfgCellSimSlotName` is entered as a comma and/or space separated list.

Examples:

- slot1
- slot2
- slot1, slot2

Applies to cellular products only.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.101.6.1.2

5.1.107 cfgCellDefaultBearerApn

Default Bearer Access Point Name

auto No dedicated APN defined

If the APN is unknown, `auto` will establish a connection with the preferred default bearer of the cellular provider. This functionality must be supported by the cellular provider, who can also enforce a dedicated APN. Only one default bearer can be set to `auto` per SIM slot.

Dedicated APN defined

If the APN name is known or if more than one default bearer shall be defined per SIM slot, a dedicated APN must be entered. Multi default bearer functionality must be supported by the cellular provider.

Applies to cellular products only.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.101.6.1.3

5.1.108 cfgCellDefaultBearerUsername

Default Bearer Username

If the service provider requries authentication for the selected default bearer, the username shall be specified by this entry. If no authentication type is selected, see `cfgCellDefaultBearerAuthType`, this entry is ignored.

Applies to cellular products only.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.101.6.1.4

5.1.109 cfgCellDefaultBearerPassword

Default Bearer Password

Set the password for the user defined in `cfgCellDefaultBearerUsername`.

Applies to cellular products only.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.101.6.1.5

5.1.110 cfgCellDefaultBearerAuthType

Default Bearer Authentication Type

Select the authentication type for the selected default bearer. If no authentication is required, set this entry to its default value **none(0)**, otherwise choose one of the supported authentication types:

- **pap(1)**,
- **chap(2)**, or
- **both(3)**.

Applies to cellular products only.

Enumeration	none (0), pap (1), chap (2), both (3)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.101.6.1.6

5.1.111 cfgCellDefaultBearerRoaming

Default Bearer Roaming Disabled or Enabled

Set to **enabled(1)** to roam to other available cellular networks outside the range of the home network. The SIM card and network provider must support roaming.

Note: Activated roaming may incur additional costs!

Applies to cellular products only.

Enumeration	disabled (0), enabled (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.101.6.1.7

5.1.112 cfgLogRemoteType

Bitfield to Control Remote Syslog Type

- **0x00** - no remote syslog
- **0x01** - standard syslog
- **0x02** - security syslog
- **0x04** - commissioning syslog

Applies to AP and STA.

Range	0 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.11.2.1.1.7

5.1.113 cfgSnmpdComMaintainer

****OBSOLETE:** Password for the maintainer.**

Applies to AP and STA.

Type	DisplayString
Range	1 - 255
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.1.12.1.100.2

5.1.114 cfgDhcpScopeInterface

DHCP Server Listening Interface

Network interface on which the DHCP server listen for DHCP requests. The interface on which the server runs must have an address configured. The DHCP server offers lease addresses based on the assigned address, the `cfgDhcpScopeStart` offset and the `cfgDhcpScopeLimit`. If an interface has multiple addresses, then the first address in the order specified in the `cfgNetIpTable` is used.

Examples:

- eth1
- br0.vlan0
- macvlan0

Type	DisplayString
Range	1 - 15
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.13.3.1.3

5.1.115 cfgDhcpHstOvrAddress

Host Override Entry Address

IP Address to return.

This is the address which is returned when a query is received for the FQDN or name configured in `cfgDhcpHstOvrDomain`.

Type	IpAddress
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.13.5.1.5

5.1.116 cfgDhcpRelayTable

DHCP Relay Table

A DHCP Relay allows to forward DHCP requests to a remote DHCP server.

Range	0 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.13.6

5.1.117 cfgDhcpRelayTableEntry

DHCP Relay Table

OID	1.3.6.1.4.1.16177.1.400.1.1.13.6.1

5.1.118 cfgDhcpRelayIndex

Table Entry Index

Range	0 - 255
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.1.13.6.1.1

5.1.119 cfgDhcpRelayEnabled

Relay Disabled or Enabled

Enumeration	disabled (0), enabled (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.13.6.1.2

5.1.120 cfgDhcpRelayInterface

DHCP Relay Listening Interface

The interface on which the DHCP Relay listens for requests to forward.

A relay may not run on the same interface as a DHCP Server specified in `cfgDhcpScopeInterface`.

Examples:

- br1.vlan0
- wlan0

Type	DisplayString
Range	1 - 15
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.13.6.1.3

5.1.121 cfgDhcpRelayLocalAddress

Local Address to Use as Source to Server

The local address is an IP address residing on the interface specified in `cfgDhcpRelayInterface`. This address is used as Gateway IP Address (giaddr) for the relayed requests.

When set to `auto` the first address on the interface is used.

Examples:

- auto
- 192.168.100.1

Type	DisplayString
Range	4 - 15
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.13.6.1.4

5.1.122 cfgDhcpRelayServerAddress

DHCP Server Address

This is the address to which all DHCP requests arriving on the interface specified in `cfgDhcpRelayInterface` are relayed to.

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

When multiple servers are specified, the requests are concurrently forwarded to all of them.

Examples:

- 10.0.0.1
- 10.0.0.1, 10.0.0.2
- 10.0.0.1 10.0.0.2 10.0.0.3
- 10.0.0.1 10.0.0.2, 10.0.0.3 10.0.0.4

Type	DisplayString
Range	7 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.13.6.1.5

5.1.123 cfgDhcpRelayInterfaceToServer

Interface towards DHCP Server

This parameter defines on which interface DHCP replies from the server will be accepted. This is intended for configurations which have three or more interfaces: one being relayed from, a second connecting the DHCP server, and a third untrusted network, typically the internet. It avoids the possibility of spoof replies arriving via this third interface.

Set to `any` to accept replies from any interface.

Examples:

- any
- br0.vlan0
- eth0

Type	DisplayString
Range	3 - 15
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.13.6.1.6

5.1.124 cfgHttpUser

****OBSOLETE:** Web Administrator Username**

This parameter is obsolete and has no replacement.

There are two local users `admin` and `monitor`, that have the respective ‘admin’ and ‘monitor’ role.

Additional users with the ‘admin’ and ‘monitor’ role may be defined via LDAP. See `cfgLdapEnabled`.

Type	DisplayString
Range	1 - 255
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.1.15.1

5.1.125 cfgHttpMonitorPasswordHash

Monitor Password Hash

Type	DisplayString
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.15.11

5.1.126 cfgHttpSessionLimit

HTTP Access Session Limit

To restrict the maximum number of connected users. Set value <= 0 to disable session limitation.

Type	Integer32
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.15.12

5.1.127 cfgHttpSessionTimeout

HTTP Session Timeout

Timeout in seconds after a session is closed when there is no activity.

Range	10 - 18000
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.15.13

5.1.128 cfgHttpTlsCiphers

OpenSSL Cipher String for HTTPS server

Specify which OpenSSL ciphers to use for HTTPS connections.

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
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.15.14

5.1.129 cfgHttpPassword

****OBSOLETE:** Web Administrator Password**

This parameter is obsolete and has been replaced with `cfgHttpAdminPasswordHash` and `cfgHttpMonitorPass`

Additional users with their own password and role may be defined via LDAP. See `cfgLdapEnabled`.

Type	DisplayString
Range	1 - 255
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.1.15.2

5.1.130 cfgHttpTlsServerCertId

TLS Server Certificate ID

Reference ID of certificate in Cert-Store to be used as TLS Server Certificate.

Set to `-1` to use the default self signed server certificate.

Range	-1 - 1000
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.15.7

5.1.131 cfgHttpAdminPasswordHash

Admin Password Hash

Type	DisplayString
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.15.9

5.1.132 cfgNetEth802dot1xTable

Wired 802.1X

This table allows to configure authentication of clients connecting to the Ethernet ports.

The Ethernet port stays locked until the client has authenticated itself via 802.1X.

Depending on the value in `cfgNetEth802dot1xEapReauthPeriod`, client have to reauthenticate regularly.

A port is automatically locked when the link of the interface goes down (the cable is unplugged), and has to be authenticated again until it can be further used.

Range	0 - 9
OID	1.3.6.1.4.1.16177.1.400.1.1.2.10

5.1.133 cfgNetEth802dot1xTableEntry

Wired 802.1x Entry

OID	1.3.6.1.4.1.16177.1.400.1.1.2.10.1

5.1.134 cfgNetEth802dot1xIndex

Table Entry Index

Range	0 - 9
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.1.2.10.1.1

5.1.135 cfgNetEth802dot1xName

Name of the Ethernet Interface

Type	DisplayString
Range	1 - 255
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.1.1.2.10.1.2

5.1.136 cfgNetEth802dot1xEnabled

Wired Port Security Interface Disabled or Enabled

When this is enabled, connecting clients will not be admitted until they have authenticated against the configured RADIUS server.

Enumeration	disabled (0), enabled (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.2.10.1.3

5.1.137 cfgNetEth802dot1xOwnIpAddr

Own IP Address of the Authenticator

This field is used as NAS-IP-Address RADIUS attribute. Set this to the IP address with which the authenticator will communicate with the RADIUS server.

Type	IpAddress
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.2.10.1.4

5.1.138 cfgNetEth802dot1xAuthServerParameter

Reference ID to the RADIUS Auth Server Table

Uses all auth servers in the `cfgWlan802dot1xAuthServerTable` which have as `cfgWlan802dot1xAuthSrvId` the value set here.

Type	Integer32
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.2.10.1.5

5.1.139 cfgNetEth802dot1xEapReauthPeriod

EAP Reauthentication Period in Seconds

To disable reauthentication, set this value to `0`.

Type	Integer32
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.2.10.1.6

5.1.140 cfgNetWwanIndex

Table Entry Index

Applies to cellular products only.

Range	0 - 7
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.1.2.11.1.1

5.1.141 cfgNetVlanParent

VLAN Parent

Name of the physical parent interface on which the VLAN resides.

This entry is only active when the VLAN interface is not part of a bridge (`cfgNetVlanBridge` = -1).

Applies to AP and STA.

Type	DisplayString
Range	1 - 15
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.2.3.1.8

5.1.142 cfgNetIpInterface

Interface Name

The name of the network interface on which the specified IP address is created.

Type	DisplayString
Range	1 - 15
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.2.6.1.8

5.1.143 cfgNetCarpSyncInterface

Name of the CARP control interface.

This interface is used to transmit and receive CARP advertisements.

This interface is required to have its own unique IP address.

Applies to AP and STA.

Type	DisplayString
Range	1 - 15
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.2.7.1.19

5.1.144 cfgNetMacVlanParent

Name of the parent interface on which the MACVLAN resides.

Applies to AP and STA.

Type	DisplayString
Range	1 - 15
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.2.9.1.8

5.1.145 cfgWlanDevPower

TX Power Limit (EIRP)

Max. limit for wireless output power as effective isotropic radiated power (EIRP) in dBm including array gain and antenna gain.

Note: This parameter only limits the maximum output power. The effective output power might be lower (regulatory limits, rate depended limits).

EIRP (dBm) = antenna port power (dBm) + array gain (dB) + antenna gain (dBi)

- The antenna port power in dBm defines the power transmitted per antenna port (chain).
- The array gain in dB defines the gain which is achieved by the use of multiple antenna ports (chains). The number of active antenna ports (chains) is defined by `cfgWlanDevTxAntenna`. The array gain depends on number of active antenna ports (chains) as following:
  - One antenna port (chain) = 0 dB
  - Two antenna ports (chains) = 3 dB
  - Three antenna ports (chains) = 5 dB
  - Four antenna ports (chains) = 6 dB
- The antenna gain in dBi defines the gain which is achieved by the antenna. The antenna gain is configured by `cfgWlanDevAntennaGain`.

Applies to AP and STA.

Range	0 - 50
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.1.1.8

5.1.146 cfgWlan802dot1xClientKeyPassword

****OBSOLETE:** Password to Unlock the Private Key**

This parameter is obsolete and has been replaced with the Certificate Store.

Key material on the device is always encrypted. The password to import the file has to be specified once during import via `setCrtFilePassphrase`.

Type	DisplayString
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.1.3.10.1.17

5.1.147 cfgWlan802dot1xTlsControlParams

Bitfield to Control TLS Behaviour

- **0x0** all validity checks will be performed
- **0x1** ignore certificate validity time
- **0x2** ignore ca certificate
- **0x4** ignore CRLs
- **0x8** ignore missing CRLs

Applies to STA.

Range	0 - 15
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.10.1.18

5.1.148 cfgWlan802dot1xRetryMax

Number of Tries Before a RADIUS Server is Considered Down

Make sure that the product of `cfgWlan802dot1xRetryMax` and `cfgWlan802dot1xRetryTimeout` does not exceed the STA connection timeout of 2 seconds.

Applies to AP.

Range	1 - 10
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.10.1.19

5.1.149 cfgWlan802dot1xRetryTimeout

RADIUS Connection Timeout in Milliseconds

Make sure that the product of `cfgWlan802dot1xRetryMax` and `cfgWlan802dot1xRetryTimeout` does not exceed the STA connection timeout of 2 seconds.

Applies to AP.

Range	100 - 10000
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.10.1.20

5.1.150 cfgWlan802dot1xPrimaryTestMode

Primary RADIUS Authentication Server Test Mode

- **status(0)**: Send Status-Server messages (RADIUS message code 12)
- **access(1)**: Send Access-Request messages (RADIUS message code 1)

Note: Status-Server messages are experimental and might not be supported by all RADIUS authentication servers.

Applies to AP.

Enumeration	status (0), access (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.10.1.22

5.1.151 cfgWlan802dot1xCrlExpiryExtension

CRL Validity Period Extension in Days

If set, the validity period of a CRL can be extended by the given amount of days.

- **0**: no extension
- **1-1095**: number of extension days
- **-1**: extend to infinity => ignore CRL expiry

Applies to STA.

Range	-1 - 1095
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.10.1.24

5.1.152 cfgWlan802dot1xCalds

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/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
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.10.1.25

5.1.153 cfgWlan802dot1xClientCertId

Client Certificate ID

Reference to the Client Certificate which should be used.

Applies to STA.

Type	Integer32
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.10.1.27

5.1.154 cfgWlanAclWhiteInterface

Name of the Wireless Interface

The ACL entry is on this specified wireless interface active.

Applies to AP.

Type	DisplayString
Range	1 - 15
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.7.1.3

5.1.155 cfgWlanAclBlackInterface

Name of the Wireless Interface

The ACL entry is on this specified wireless interface active.

Applies to AP.

Type	DisplayString
Range	1 - 15
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.8.1.3

5.1.156 cfgWlanGlblConnectionStatusWlanInterface

Persistent Default of the Volatile Setting `swDrvConStatWlanIf`

The value set here is used to initialize `swDrvConStatWlanIf`. Initialisation happens on startup or configuration change.

Specify `all` to get the connection status of all wlan interfaces.

Applies to AP and STA.

Type	DisplayString
Range	3 - 17
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.9.4

5.1.157 cfgRouteTableDestinationNetwork

Destination Network in CIDR Notation

Set to `0.0.0.0/0` to match any destination. This is the equivalent to the default gateway in `cfgRouteDefGateway`.

Type	DisplayString
Range	5 - 50
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.4.2.1.3

5.1.158 cfgMRouteTableInput

Input Interface

The interface on which multicast traffic is received.

Type	DisplayString
Range	1 - 15
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.4.3.1.3

5.1.159 cfgMRouteTableSource

Unicast Source Address to Listen for

May be set to a specific address, or to a range in CIDR notation.

If it is set to `0.0.0.0` multicast traffic from all sources is forwarded.

Examples:

- 0.0.0.0
- 192.168.1.15
- 172.16.1.0/24

Type	DisplayString
Range	7 - 18
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.4.3.1.4

5.1.160 cfgMRouteTableOutput

Output Interface(s)

This is a space and/or comma separated list of interfaces from which the forwarded multicast traffic is sent.

Examples:

- br0.vlan0
- wlan0
- eth0, eth1, wlan1

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.4.3.1.6

5.1.161 cfgRouteRuleFrom

Source Network

This is an address or network in CIDR notation.

Set to `0.0.0.0/0` to match any source.

Type	DisplayString
Range	5 - 50
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.4.4.1.4

5.1.162 cfgRouteRuleTo

Destination Network

This is an address or network in CIDR notation.

Set to `0.0.0.0/0` to match any destination.

Type	DisplayString
Range	5 - 50
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.4.4.1.5

5.1.163 cfgRouteDhcpInterface

Interface of DHCP Client

The name of an interface on which a DHCP Client is running.

Examples:

- wlan0
- br0.vlan7

Type	DisplayString
Range	1 - 15
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.4.5.1.3

5.1.164 cfgNlmMonUpAction

NLM 'UP' State Monitor Action

The action is executed on a monitor-state transition to 'up'.

Set to `0` to disable (i.e. no action).

Supported actions are:

- **1xxx**: Offset: 1000, x: CARP group from 0 to 255. Un-demote CARP group defined by `cfgNetCarpLocalInterfaceGroup`.
- **20xx**: Offset: 2000, x: WLAN interface from 0 to 63. Enable Access Point operation on the wlan interface. Note: On 802.11n products all wlan interfaces on radio0 are enabled, regardless of the specified WLAN interface.
- **30xx**: Offset: 3000, x: Radio device from 0 to 63. Reset the chip of the specified radio device (802.11n products only).
- **4xxx**: Offset: 4000, x: Wireguard Peer Index from 0 to 255. Re-resolve the specified FQDN of the referenced peer.
- **8000**: Bring up all routes which reference to this NLM instance. References are defined via `cfgRouteTableMonitor` and `cfgRouteDhcpMonitor`.
- **8001**: Bring down all routes which reference to this NLM instance. References are defined via `cfgRouteTableMonitor` and `cfgRouteDhcpMonitor`.

Range	0 - 9999
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.40.2.1.10

5.1.165 cfgNlmMonDownAction

NLM 'DOWN' State Monitor Action

The action is executed on a monitor-state transition to 'down'.

Set to `0` to disable (i.e. no action).

Supported actions are:

- **1xxx**: Offset: 1000, x: CARP group from 0 to 255. Demote CARP group defined by `cfgNetCarpLocalInterfaceGroup`.
- **20xx**: Offset: 2000, x: wlan interface from 0 to 63. Disable Access Point operation on the wlan interface. Note: On 802.11n products all wireless interfaces on radio0 are disabled, regardless of the specified WLAN interface.
- **30xx**: Offset: 3000, x: Radio device from 0 to 63. Reset the chip of the specified radio device (802.11n products only).
- **4xxx**: Offset: 4000, x: Wireguard Peer Index from 0 to 255. Re-resolve the specified FQDN of the referenced peer.
- **8000**: Bring down all routes which reference to this NLM instance. References are defined via `cfgRouteTableMonitor` and `cfgRouteDhcpMonitor`.
- **8001**: Bring up all routes which reference to this NLM instance. References are defined via `cfgRouteTableMonitor` and `cfgRouteDhcpMonitor`.

Range	0 - 9999
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.40.2.1.11

5.1.166 cfgNlmMonScanLoopInterval

Scan Loop Debounce Interval In Milliseconds

This parameter is active when `cfgNlmMonType` is set to **wlan(2)**.

If set to non-zero it will mark interface 'down' after receiving scan loop trap 415 and mark it 'up' after scan loop interval if no other 415 events have been received.

Applies to STA. 802.11n products only.

Range	100 - 2147483647
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.40.2.1.12

5.1.167 cfgNlmMonCountUp

NLM Monitor Count for UP Transition

The number of times the measured criteria has to be up, until the monitor is reported as up.

This parameter is used for polling based monitor types only (see `cfgNlmMonType`).

Range	1 - 65535
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.40.2.1.13

5.1.168 cfgNlmMonRssi

NLM Monitor RSSI Threshold

This parameter is active when `cfgNlmMonType` is set to **rssi(4)**.

This defines the threshold where an RSSI monitor indicates a down condition if the current rssi value is below this number and up otherwise.

Range	0 - 127
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.40.2.1.14

5.1.169 cfgNlmMonLogic

NLM Logic Monitor Subtype

This parameter is active when `cfgNlmMonType` is set to **logic(5)**.

This parameter defines the logical operation on the input(s) defined in `cfgNlmMonLogicInput`.

Supported operations are:

- **none(0)**: Monitor is ignored
- **equal(1)**: The input defined is selected as is, this is essentially an alias to an existing monitor, allowing to define additional up/down actions
- **not(2)**: This is the inversion of equal(1), i.e. it references the configured monitor input, but with inverted state
- **or(3)**: The state is the OR combined state of referenced inputs, i.e. if one of them is UP, this monitor is UP

- **and(4)**: This is the AND equivalent for or(3), i.e. if one of the referenced inputs is DOWN, this monitor is DOWN
- **nor(5)**: The state is the NOR combined state of referenced inputs, i.e. if one of them is UP, this monitor is DOWN
- **nand(6)**: This is the NAND equivalent for nor(5), i.e. if one of the referenced inputs is DOWN, this monitor is UP

Enumeration	none (0), equal (1), not (2), or (3), and (4), nor (5), nand (6)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.40.2.1.15

5.1.170 cfgNlmMonLogicInput

NLM Input(s) for Logic Monitor

This parameter is active when `cfgNlmMonType` is set to **logic(5)**.

Specifies the monitor input(s) as space and/or comma-separated indices.

Examples:

- 1
- 2 3,4

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.40.2.1.16

5.1.171 cfgNlmMonTrap

NLM Trap Sending

This allows monitors to issue traps on state changes.

Supported operations are:

- **none(0)**: No traps are sent out
- **up(1)**: Trap 340 is sent out when monitor state gets UP
- **down(2)**: Trap 341 is sent out when monitor state gets DOWN
- **both(3)**: Both traps 340 and 341 are sent out

Enumeration	none (0), down (1), up (2), both (3)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.40.2.1.17

5.1.172 cfgNlmMonCount

NLM Monitor Count for DOWN Transition

The number of times the measured criteria has to be down, until the monitor is reported as down.

This parameter is used for polling based monitor types only (see `cfgNlmMonType`).

Range	1 - 65535
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.40.2.1.4

5.1.173 cfgNlmMonType

Objects That Can Be Monitored

- **phy(0)** monitor checks periodically the link status of the ethernet interfaces defined by `cfgNlmMonInterface`
  If at least one interface in the list specified is up the monitor is considered up. This is a polling based monitor.

- **icmp(1)** monitor pings periodically the destination defined by `cfgNlmMonDestination`. If the destination does reply to the ECHO request within the `cfgNlmMonInterval` the monitor is considered up. This is a polling based monitor.

- **wlan(2)** monitor listens to link status events of the wireless interface defined by `cfgNlmMonInterfaces`. This is an event based monitor.

  The wlan monitor consists of 3 components:

  Long Handoff Detector - Triggers when after disassociation no authorization event is detected within the configured time in `cfgNlmMonInterval`.

  Scan Loop Detector - Triggers immediately on trap 415. This happens if there is no AP or only a single AP which stays below/above the Handoff thresholds. This trap is only generated when `cfgWlanHoProfile` is set to 2 or higher.

  Handoff Loop Detector - Triggers if there have been `cfgNlmMonCount` number of Handoff events within `cfgNlmMonCount` * (`cfgNlmMonInterval` + `cfgNlmMonScanLoopInterval`).

The wlan monitor recovers:

Long Handoff Detector - Immediately after the next successful authorization.

Scan Loop Detector - After the time of the last 415 trap event + the configured `cfgNlmMonScanLoopInterv`
When down, this is checked regularly in `cfgNlmMonScanLoopInterval` intervals.

Handoff Loop Detector - When there are less than `cfgNlmMonCount` Handoff events within the time-window `cfgNlmMonCount` * (`cfgNlmMonInterval` + `cfgNlmMonScanLoopInterval`).
When down, this is checked regularly in `cfgNlmMonScanLoopInterval` intervals.

- **route(3)** monitor is the same as **icmp(1)**, but it binds the source interface statically, which is provided by a dhcp-client. This is set by referencing a monitor with `cfgRouteDhcpMonitor` in `cfgRouteDhcpTable`. It can only be used with actions `8000` and `8001` to bring up and tear down routes dynamically. When `cfgNlmMonDestination` is configured to `0.0.0.0`, this monitor is dynamically set to the default gateway received by the DHCP client. When a specific IP is set, this IP will be checked instead. This is only necessary when the gateway does not respond to ICMP requests. This is a polling based monitor.

- **rssi(4)** monitors the RSSI value of the wlan interface defined in `cfgNlmMonInterfaces`. A value below the threshold defined in `cfgNlmMonRssi` indicates a DOWN status. This is a polling based monitor.

- **logic(5)** monitors reference existing monitors and allow logical combinations of those. This type of monitor requires `cfgNlmMonLogic` to select the logical operation, along with `cfgNlmMonLogicInput` to define the monitors as input. This is an event based monitor.

Note: wlan(2) monitor is supported for 802.11n products only.

Enumeration	phy (0), icmp (1), wlan (2), route (3), rssi (4), logic (5)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.40.2.1.5

5.1.174 cfgQosIpToTidMapSrcNet

Source Network For IP Prioritization Rule

In CIDR format.

Applies to AP and STA. 802.11n products only.

Type	DisplayString
Range	5 - 50
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.6.4.1.2

5.1.175 cfgQosIpToTidMapDestNet

Destination Network For IP Prioritization Rule

In CIDR format.

Applies to AP and STA. 802.11n products only.

Type	DisplayString
Range	5 - 50
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.6.4.1.3

5.1.176 cfgQosIpToTidMapSrcPort

Source Port For IP Prioritization Rule

Use port -1 to match any port. This setting can only be used if the protocol is set to udp or tcp.

Applies to AP and STA. 802.11n products only.

Range	-1 - 65535
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.6.4.1.5

5.1.177 cfgQosIpToTidMapDestPort

Destination Port For IP Prioritization Rule

Use port -1 to match any port. This setting can only be used if the protocol is set to udp or tcp.

Applies to AP and STA. 802.11n products only.

Range	-1 - 65535
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.6.4.1.6

5.1.178 cfgQosEthertypeToL2Ethertype

Ethertype To Match

Some popular Ethertypes:

- 0800: IPv4
- 0806: ARP
- 0835: RARP
- 8100: VLAN
- 86DD: IPv6
- 8847: MPLS unicast
- 8848: MPLS multicast
- 8892: Profinet
- 9100: stacked VLAN

Applies to AP and STA. 802.11n products only.

Type	DisplayString
Range	4 - 4
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.6.6.1.3

5.1.179 rpcScep

OID	1.3.6.1.4.1.16177.1.400.1.3.100

5.1.180 rpcScepTable

SCEP RPCs

Range	0 - 255
OID	1.3.6.1.4.1.16177.1.400.1.3.100.1

5.1.181 rpcScepTableEntry

SCEP RPCs

OID	1.3.6.1.4.1.16177.1.400.1.3.100.1.1

5.1.182 rpcScepIndex

Table Entry Index

Range	0 - 255
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.3.100.1.1.1

5.1.183 rpcScepGetCaCrt

Start SCEP getca for SCEP entry in `cfgScepTable`

Enumeration	error (-1), done (0), start (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.3.100.1.1.2

5.1.184 rpcScepEnroll

SCEP enroll/re-enroll

Writing this value will:

- **start(1)** start SCEP enroll
- **reenroll(3)** start SCEP re-enroll
- **stop(2)** stop SCEP enroll or re-enroll

for corresponding SCEP entry in `cfgScepTable`.

Writing **reenroll(3)** to this value will start SCEP re-enroll process for corresponding SCEP entry in `cfgScepTable`.

Reading this value will return:

- **start(1)** as long as the enrollment is in process
- **reenroll(3)** as long as the re-enrollment is in process
- **done(0)** when enrollment or re-enrollment has finished
- **eerror(-1)** when enrollment failed
- **serror(-2)** when stopping enrollment or re-enrollment failed
- **reerror(-3)** when re-enrollment failed

Enumeration	reerror (-3), serror (-2), eerror (-1), done (0), start (1), stop (2), reenroll (3)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.3.100.1.1.3

5.1.185 rpcCrtRefresh

****OBSOLETE:** Refresh Certificates**

This parameter is obsolete and has been replaced with `rpcCfgApply`.

Range	-1 - -1
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.3.4.2

5.1.186 rpcCrtCrlTable

Certificate CRL RPCs

Range	0 - 15
OID	1.3.6.1.4.1.16177.1.400.1.3.4.3

5.1.187 rpcCrtCrlTableEntry

Certificate CRL RPCs entries

OID	1.3.6.1.4.1.16177.1.400.1.3.4.3.1

5.1.188 rpcCrtCrlIndex

Table Entry Index

Range	0 - 15
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.3.4.3.1.1

5.1.189 rpcCrtCrlGet

Import a CA CRL

- **importcrl(1)**: Import the CRL from `cfgCrtCrlUrl` and store it in certificate store to CRL ID corresponding to the `cfgCrtCrlCaId`.

Note: The CA CRL must be in the DER format.

Applies to AP and STA.

Enumeration	errorImportcrl (-1), nop (0), importcrl (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.3.4.3.1.2

5.1.190 rpcCrtAttribute

Read/Write a certificate attribute

To read an attribute the `setCrtFileId`, `setCrtFileType` and `setCrtAttributeKey` need to be set. After call this rpc the value is available in `setCrtAttributeValue`.

To write an attribute the `setCrtFileId`, `setCrtFileType`, `setCrtAttributeKey` and `setCrtAttributeValue` need to be set.

Applies to AP and STA.

Enumeration	writeerror (-2), readerror (-1), nop (0), read (1), write (2)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.3.4.4

5.1.191 setCfgFileUrl

Configuration File URL

The URL defines the location of the configuration file where it will be downloaded from or uploaded to when using `rpcCfgFile`.

For import files to the device the TFTP and HTTP/HTTPS protocols are supported. For export from the device to a server only the TFTP protocol is supported.

Allowed characters are [a-zA-Z0-9] and ._-~. Additionally the URL can contain spaces which will be encoded by the device. All other character need to be encoded by the user.

Examples:

- tftp://192.168.1.1/device.cfg

- http://192.168.1.1/device.cfg
- https://192.168.1.1/device.cfg

Note: If you use the HTTPS protocol it is highly recommended to install the TLS Client CA Certificate on the device. Otherwise the device will connect to any web server which use TLS, but the connection must be considered insecure. See `setTlsClient` for more information.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.4.1.1

5.1.192 setCfgFileType

Configuration File Type

This parameter specifies the type of the configuration file and how to handle the confguration file by the `rpcCfgFile`.

- **standard(0)** Plain text configuration file.
- **cyber(1)** Encrypted configuration file using `setCfgFilePassword`.

Enumeration	standard (0), cyber (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.4.1.5

5.1.193 setCfgFilePassword

Configuration File Password

This parameter is only needed for encrypted configuration files (when `setCfgFileType` is set to **cyber(1)**).

It specifies the password used to encrypt/decrypt the configuration file during import/export.

Type	DisplayString
Range	0 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.4.1.7

5.1.194 setWlanDevFrequency

Wireless Frequency in MHz

Set and get the operating frequency of the device (radio).

Set frequency is supported on 802.11n products only.

Applies to AP and STA.

Range	2300 - 6300
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.4.3.1.1.6

5.1.195 setWlanDevPower

Wireless Output Power

Output power as effective isotropic radiated power (EIRP) in dBm including antenna gain.

Applies to AP and STA. 802.11n products only.

Range	0 - 100
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.4.3.1.1.8

5.1.196 setFwFileUrl

Firmware File URL

The URL defines from which location the new firmware will be downloaded when using the `rpcFwFlash`.

Supported protocols are TFTP, HTTP/HTTPS.

Allowed characters are [a-zA-Z0-9] and ._-~. Additionally the URL can contain spaces which will be encoded by the device. All other character need to be encoded by the user itself.

Examples:

- tftp://192.168.1.1/firmware.img
- http://192.168.1.1/firmware.img
- https://192.168.1.1/firmware.img

Note: If you use the HTTPS protocol it is highly recommended to install the TLS Client CA Certificate on the device. Otherwise the device will connect to any web server which uses TLS, but the connection must be considered insecure. See `setTlsClient` for more information.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.4.5.1

5.1.197 setCrtFileUrl

Certificate File URL

The URL defines the location of the certificate file where it will be downloaded from or uploaded to.

Supported protocols are TFTP, HTTP/HTTPS. For export only the TFTP protocol is supported.

Examples:

- tftp://192.168.1.1/uttpd.crt
- http://192.168.1.1/uttpd.crt
- https://192.168.1.1/uttpd.crt

Note: If you use the HTTPS protocol is highly recommended to install the TLS Client CA Certificate on the device. Otherwise the device will connect to any web server which uses TLS, but the connection must be considered insecure. See `setTlsClient` for more information.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.4.6.1

5.1.198 setCrtFileSelector

****OBSOLETE:** Field to Select Which File Should be Imported/Exported** via `rpcCrtFile`

This parameter is obsolete and has been replaced with the Certificate Store.

See `setCrtFileId`, `setCrtFileType`, `setCrtAttributeKey`, `setCrtAttributeValue` and `setCrtFilePass`

Range	-1 - -1
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.4.6.2

5.1.199 setCrtFilePkcs12Passphrase

****OBSOLETE:** Set the PKCS#12 passphrase used to import with** `rpcCertFile`

This parameter is obsolete and has been replaced with `setCrtFilePassphrase`

Type	DisplayString
Range	0 - 255
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.4.6.4

5.1.200 setCrtFileId

Id of the Certificate

Define the id of the certificate processed by the `rpcCrtFile` for **export(2)** and **delete(3)**. During **import(1)** a new unique id is assigned to the certificate and therefore this parameter is ignored.

Every certificate will be stored with an id which is automatically assigned when the certificate is imported. This id is then used by the services to reference the desired certificate.

Range	0 - 1000
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.4.6.5

5.1.201 setCrtFileType

File type for the certificate action

Define the type of the certificate processed by the `rpcCrtFile`.

- **1**: CRL
- **2**: Certificate
- **3**: Private Key
- **4**: Static Key
- **5**: PKCS12
- **6**: Public Key

Enumeration	crl (1), cert (2), key (3), statickey (4), pkcs12 (5), pubkey (6)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.4.6.6

5.1.202 setCrtAttributeKey

Key of the attribute to read/write

Select the attribute which would be read/write by the `rpcCrtAttribute`.

- **0**: Label of a certificate

Enumeration	label (0)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.4.6.7

5.1.203 setCrtAttributeValue

Value of the attribute

This value will be written to the attribute defined by `setCrtFileId`, `setCrtFileType` and `setCrtAttributeKey` by using the `rpcCrtAttribute`.

The value read by using the `rpcCrtAttribute` will be available here.

Type	DisplayString
Range	0 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.4.6.8

5.1.204 setCrtFilePassphrase

Set the passphrase used to import with `rpcCertFile`

This passphrase will be used during the import to decrypt the PKCS#12 container data or the private key.

Type	DisplayString
Range	0 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.4.6.9

5.1.205 setSysTime

System time as epoch

Range	100000 - 2114384400
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.4.7.1

5.1.206 setSysSupportFile

OID	1.3.6.1.4.1.16177.1.400.1.4.7.11

5.1.207 setSysSfEncryptionEnabled

Disable or Enable Support File Encryption

If set to **enabled(1)**, the Technical Support File is encrypted using `setSysSfEncryptionPassword`.

Enumeration	disabled (0), enabled (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.4.7.11.1

5.1.208 setSysSfEncryptionPassword

Support File Encryption Password

Used to encrypt the Technical Support File if `setSysSfEncryptionEnabled` is **enabled(1)**.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.4.7.11.2

5.1.209 setTlsClient

OID	1.3.6.1.4.1.16177.1.400.1.4.9

5.1.210 setTlsCltCaIds

TLS Client CA Certificate IDs

Set to -1 to use TLS client without CA certificate. Multiple CAs may be referenced by writing the ids of the CAs as space/comma-separated list.

Examples:

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

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.4.9.1

5.1.211 setTlsCltCrlExpiryExtension

CRL Validity Period Extension in Days

If set, the validity period of a CRL can be extended by the given amount of days.

- **0** no extension
- **1-1095** extension days
- **-1** extend to infinity => ignore CRL expiry

Type	Integer32
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.4.9.3

5.1.212 setTlsCltTlsControlParams

Bitfield to Control the TLS Client Behavior

- **0x0** all validity checks will be performed
- **0x1** ignore certificate validity time
- **0x2** ignore ca certificate
- **0x4** ignore CRLs
- **0x8** ignore missing CRLs

Range	0 - 15
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.4.9.4

5.1.213 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
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.4.9.5

5.1.214 swDrvConStatWlanIf

Volatile Wlan Interface Selector for `swDrvConStatTable`

Changes made here will be lost upon reconfiguration or a reboot. Use `cfgWlanGlblConnectionStatusWlanInt` to set a persistent value which is used during initialisation.

Specify `all` to get the connection status of all wlan interfaces.

Applies to AP and STA.

Type	DisplayString
Range	3 - 17
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.6.5.7

5.1.215 swDrvCntWlanBeaconMiss

Number of Beacon Misses

Applies to STA.

Type	Counter32
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.1.6.5.9.1.40

5.1.216 swDrvCntWlanBeaconRx

Number of Beacons Received

Applies to STA.

Type	Counter32
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.1.6.5.9.1.41

5.1.217 swDrvCntWlanApBeaconMiss

Number of AP Missed Beacons

Applies to AP.

Type	Counter32
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.1.6.5.9.1.42

5.1.218 swDrvCntWlanPilotMiss

Number of Pilot Frame Misses

Applies to STA.

Type	Counter32
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.1.6.5.9.1.43

5.1.219 swDrvCntWlanPilotRx

Number of Pilot Frames Received

Applies to STA.

Type	Counter32
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.1.6.5.9.1.44

5.1.220 swCellLteMode

LTE Mode

LTE modulation mode FDD or TDD.

Applies to cellular products only.

Enumeration	unknown (0), tdd (1), fdd (2)
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.1.6.50.1.1.19

5.1.221 swCellWwanName

Name of the Cellular Network Interface

This is name of the corresponding network interface.

Applies to cellular products only.

Type	DisplayString
Range	1 - 255
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.1.6.50.1.1.2

5.1.222 swCellEarfcn

E-UTRA-ARFCN

The parameter determines the E-UTRA-ARFCN of the cell.

Applies to cellular products only.

Type	Integer32
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.1.6.50.1.1.20

5.1.223 swCellCellId

Cell ID

The parameter determines the 28-bit (WCDMA, LTE) or 36-bit (5G-NR) cell ID as a hexadecimal value.

Applies to cellular products only.

Type	DisplayString
Range	0 - 9
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.1.6.50.1.1.21

5.1.224 swCellBandwidthUl

Upload Bandwidth

- **bw1dot4(0)**: 1.4 MHz
- **bw3(1)**: 3 MHz
- **bw5(2)**: 5 MHz
- **bw10(3)**: 10 MHz
- **bw15(4)**: 15 MHz
- **bw20(5)**: 20 MHz

Applies to cellular products only.

Enumeration	bw1dot4 (0), bw3 (1), bw5 (2), bw10 (3), bw15 (4), bw20 (5)
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.1.6.50.1.1.22

5.1.225 swCellBandwidthDl

Download Bandwidth

- **bw1dot4(0)**: 1.4 MHz
- **bw3(1)**: 3 MHz
- **bw5(2)**: 5 MHz
- **bw10(3)**: 10 MHz
- **bw15(4)**: 15 MHz
- **bw20(5)**: 20 MHz

Applies to cellular products only.

Enumeration	bw1dot4 (0), bw3 (1), bw5 (2), bw10 (3), bw15 (4), bw20 (5)
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.1.6.50.1.1.23

5.1.226 swCellSimSlot

Active SIM Slot

- **none(0)**: No SIM slot is active
- **slot1(1)**: SIM slot 1 is active
- **slot2(2)**: SIM slot 2 is active

Applies to cellular products only.

Enumeration	none (0), slot1 (1), slot2 (2)
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.1.6.50.1.1.3

5.1.227 swCertificate

OID	1.3.6.1.4.1.16177.1.400.1.6.9

5.1.228 swCrtExpirationTime

Certificate expiration date/time (UTC).

Get the certificate expiration date/time for certificate type `setCrtFileType` at ID `setCrtFileId`

Example:

Oct 22 09:42:27 2018 GMT

Type	DisplayString
Range	1 - 255
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.1.6.9.1

5.1.229 swCrtFingerprint

SHA384 fingerprint of certificate

Get the certificate fingerprint for certificate type `setCrtFileType` at ID `setCrtFileId`

Example:

9C:A6:6D:7C:AD:93:A2:29:68:82:7F:50:AA:B0:5F:40:BB:82:D3:97:D5:97:28:A1:20:AE:A7:83:0C:7B:1A:CB:18:3A

Type	DisplayString
Range	1 - 255
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.1.6.9.2

5.1.230 swCrtCertTable

Certificate Table for Type CERT

Range	0 - 63
OID	1.3.6.1.4.1.16177.1.400.1.6.9.3

5.1.231 swCrtCertTableEntry

Certificate Table for Type CERT

OID	1.3.6.1.4.1.16177.1.400.1.6.9.3.1

5.1.232 swCrtCertTableIndex

Table Entry Index

Range	0 - 63
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.6.9.3.1.1

5.1.233 swCrtCertId

Certificate Id in the Certificate Store

Type	Integer32
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.1.6.9.3.1.2

5.1.234 swCrtCertLabel

Certificate Id Label in the Certificate Store

Type	DisplayString
Range	1 - 255
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.1.6.9.3.1.3

5.1.235 swCrtCertExpirationTime

Certificate Expiration Date/Time (UTC)

Example:

Oct 22 09:42:27 2018 GMT

Type	DisplayString
Range	1 - 255
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.1.6.9.3.1.4

5.1.236 swCrtCertFingerprint

SHA384 Fingerprint of Certificate

Example:

9C:A6:6D:7C:AD:93:A2:29:68:82:7F:50:AA:B0:5F:40:BB:82:D3:97:D5:97:28:A1:20:AE:A7:83:0C:7B:1A:CB:18:3A

Type	DisplayString
Range	1 - 255
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.1.6.9.3.1.5

5.1.237 swCrtCrlTable

Certificate Table for Type CERT

Range	0 - 63
OID	1.3.6.1.4.1.16177.1.400.1.6.9.4

5.1.238 swCrtCrlTableEntry

Certificate Table for Type CERT

OID	1.3.6.1.4.1.16177.1.400.1.6.9.4.1

5.1.239 swCrtCrlTableIndex

Table Entry Index

Range	0 - 63
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.1.6.9.4.1.1

5.1.240 swCrtCrlId

CRL Id in the Certificate Store

Type	Integer32
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.1.6.9.4.1.2

5.1.241 swCrtCrlLabel

CRL Id Label in the Certificate Store

Type	DisplayString
Range	1 - 255
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.1.6.9.4.1.3

5.1.242 swCrtCrlExpirationTime

CRL Expiration Date/Time (UTC)

Example:

Oct 22 09:42:27 2018 GMT

Type	DisplayString
Range	1 - 255
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.1.6.9.4.1.4

5.1.243 swCrtCrlFingerprint

SHA384 Fingerprint of CRL

Example:

9C:A6:6D:7C:AD:93:A2:29:68:82:7F:50:AA:B0:5F:40:BB:82:D3:97:D5:97:28:A1:20:AE:A7:83:0C:7B:1A:CB:18:3A

Type	DisplayString
Range	1 - 255
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.1.6.9.4.1.5

5.2 MIB Reference: WESTERMO-SW6-FIREWALL-MIB

5.2.1 cfgFwNatPrtFwdSourceAddress

Source Address to Match

This is a specific IP address or a range in CIDR notation.

An exclamation mark `!` before the address/network may be used to invert the sense of the rule, e.g `!192.168.0.0/24`.

Use this parameter to restrict the source of traffic on which the rule is applied.

Examples:

- 172.17.29.7/32: Match the specific source IP 172.17.29.7
- 0.0.0.0/0: Match all sources addresses
- 192.168.0.0/24: Match the specified source network
- !192.168.0.0/24: Match any source, except the specified network

Note: Usually this should be `0.0.0.0/0`.

Type	DisplayString
Range	7 - 19
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.1.1.5

5.2.2 cfgFwNatPrtFwdDestinationAddress

Destination Address to Redirect

This is a specific IP address or a range in CIDR notation.

Use this parameter to restrict the destination of traffic on which the rule is applied.

Set to `0.0.0.0/0` to match all destinations of inbound traffic on the interface specified in `cfgFwNatPrtFwdInterf`

An exclamation mark `!` before the destination may be used to invert the sense of the rule, e.g `!192.168.0.0/24`.

When using static IPs set this to the configured address of the respective interface or alias you want to forward.

Be aware, that setting `0.0.0.0/0` will redirect everything arriving on the configured interface, even if not sent to the device itself.

Examples:

- 172.17.29.7/32: Match the specific destination IP 172.17.29.7
- 0.0.0.0/0: Match all destination addresses

- 192.168.0.0/24: Match the specified destination network
- !192.168.0.0/24: Match any destination, except this network

Note: This should be `0.0.0.0/0` when using DHCP.

Type	DisplayString
Range	7 - 19
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.1.1.8

5.2.3 cfgFwNatOutSourceAddress

Source Address to Match

This is a specific IP address or a range in CIDR notation.

An exclamation mark `!` before the address/network may be used to invert the sense of the rule, e.g `!192.168.0.0/24`.

Use this parameter to restrict the source of traffic on which the rule is applied.

Examples:

- 172.17.29.7/32: Match the specific source IP 172.17.29.7
- 0.0.0.0/0: Match all sources addresses
- 192.168.0.0/24: Match the specified source network
- !192.168.0.0/24: Match any source, except the specified network

Note: Usually this should be `0.0.0.0/0`.

Type	DisplayString
Range	7 - 19
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.2.1.5

5.2.4 cfgFwNatOutDestinationAddress

Destination Address to Match

This is a specific IP address or a range in CIDR notation.

Use this parameter to restrict the destination of traffic on which the rule is applied.

Set to `0.0.0.0/0` to match all destinations of outbound traffic on the interface specified in `cfgFwNatOutInterfac`

An exclamation mark `!` before the destination may be used to invert the sense of the rule, e.g `!192.168.0.0/24`.

Examples:

- 172.17.29.7/32: Match the specific destination IP 172.17.29.7
- 0.0.0.0/0: Match all destination addresses
- 192.168.0.0/24: Match the specified destination network
- !192.168.0.0/24: Match any destination, except this network

Type	DisplayString
Range	7 - 19
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.2.1.8

5.2.5 cfgFwNatOneToOneSourceNet

Source Network

This is a source network in CIDR notation.

When `cfgFwNatOneToOneType` is set to **auto(0)** or **dnat(1)**, frames matched by this field are processed by this rule.

Set to `0.0.0.0/0` to match all inbound traffic.

When `cfgFwNatOneToOneType` is set to **snat(2)** the network specified here will be rewritten to the network specified in `cfgFwNatOneToOneRewriteNet`.

Type	DisplayString
Range	9 - 18
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.3.1.5

5.2.6 cfgFwNatOneToOneDestinationNet

Destination Network

This is a destination network in CIDR notation.

When cfgFwNatOneToOneType is set to **auto(0)** or **dnat(1)**, the network specified here will be rewritten to the network specified in cfgFwNatOneToOneRewriteNet.

When cfgFwNatOneToOneType is set to **snat(2)**, only frames matched by this field are processed by this rule.

Set to 0.0.0.0/0 to match all outbound traffic.

Type	DisplayString
Range	9 - 18
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.3.1.6

5.2.7 cfgFwNatOneToOneRewriteNet

Rewrite Network

This is the network in CIDR notation to/from which frames are rewritten.

Depending on the setting of cfgFwNatOneToOneType:

- **auto(0)**: For inbound traffic cfgFwNatOneToOneRewriteNet is the network to which the destination is rewritten to cfgFwNatOneToOneDestinationNet. For outbound traffic cfgFwNatOneToOneRewri is the network which matches the source that is rewritten to cfgFwNatOneToOneRewriteNet.
- **dnat(1)**: cfgFwNatOneToOneRewriteNet is the network to which the dest. net (cfgFwNatOneToOneDesti is rewritten to.
- **snat(2)**: cfgFwNatOneToOneRewriteNet is the network to which the source net (cfgFwNatOneToOneSour is rewritten to.

Type	DisplayString
Range	9 - 18
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.1.1.2.3.1.7

5.2.8 cfgFwL2IpFltrSource

Source Network/IP On Which The Rule Matches (CIDR Notation)

When cfgFwL2IpFilterMode is set to **full(1)**, then this field only has an effect when cfgFwL2IpFltrEthertype is set to 0800, 0806 or 8035.

When cfgFwL2IpFltrEthertype is set to 0800 this is an IP or network.

When cfgFwL2IpFltrEthertype is set to 0806 or 8035 it is the source address or a range of source addresses of an ARP/RARP frame (ARP_SPA).

Type	DisplayString
Range	7 - 18
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.1.1.3.3.1.6

5.2.9 cfgFwL2IpFltrDestination

Destination Network/IP On Which The Rule Matches (CIDR Notation)

When cfgFwL2IpFilterMode is set to **full(1)**, then this field only has an effect when cfgFwL2IpFltrEthertype is set to 0800, 0806 or 8035.

When cfgFwL2IpFltrEthertype is set to 0800 this is an IP or network.

When cfgFwL2IpFltrEthertype is set to 0806 or 8035 it is the target address or a range of target addresses of an ARP/RARP frame (ARP_TPA).

Type	DisplayString
Range	7 - 18
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.1.1.3.3.1.7

5.2.10 cfgFwMangle

OID	1.3.6.1.4.1.16177.1.400.2.1.1.5

5.2.11 cfgFwMangleTable

Firewall Mangle Table

Iptables mangle rules allow to modify frames that are received, transmitted or forwarded.

Range	0 - 255
OID	1.3.6.1.4.1.16177.1.400.2.1.1.5.1

5.2.12 cfgFwMangleTableEntry

Firewall Mangle Table

OID	1.3.6.1.4.1.16177.1.400.2.1.1.5.1.1

5.2.13 cfgFwMnglIndex

Table Entry Index

Range	0 - 255
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.2.1.1.5.1.1.1

5.2.14 cfgFwMnglComment

User Comment

This parameter has no operational function. It allows to store a comment about the use of this mangle rule.

Type	DisplayString
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.1.1.5.1.1.10

5.2.15 cfgFwMnglEnabled

Disable or Enable This Rule

Enumeration	disabled (0), enabled (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.1.1.5.1.1.2

5.2.16 cfgFwMnglChain

Chain on Which Mangle Action is Performed

Depending on the selected chain, `cfgFwMnglInputInterface` and/or `cfgFwMnglOutputInterface` may become active.

Enumeration	input (1), forward (2), output (3), prerouting (4), postrouting (5)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.1.1.5.1.1.3

5.2.17 cfgFwMnglAction

Action to be Performed

- **setmss(1)**: Sets the MSS to the value in `cfgFwMnglValue`.
- **ttlset(2)**: Sets the TTL to the value in `cfgFwMnglValue`.

Enumeration	setmss (1), ttlset (2)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.1.1.5.1.1.4

5.2.18 cfgFwMnglValue

Value to be Set

Depending on the mode of `cfgFwMnglAction` this value has a different meaning.

- **setmss(1)**: Set the MSS of TCP SYN frames to the specified value. This value should not be greater then the value of the MTU - 40. The value has a range of 28 to 8960.
- **ttlset(2)**: Set the TTL of frames to the specified value. The value has a range of 0 to 255. When a value of 0 is set, this frame can not be routed.

Type	Integer32
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.1.1.5.1.1.5

5.2.19 cfgFwMnglInputInterface

Name of the Input Interface to Match

This parameter may be used when `cfgFwMnglChain` is set to **input(1)**, **forward(2)** and **prerouting(4)**.

Groups of interfaces can be matched by adding the character '+' at the end. E.g. `eth+` to match the interfaces eth0, eth1 and eth2.

Set to `-1` to not use this parameter.

Type	DisplayString
Range	1 - 16
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.1.1.5.1.1.6

5.2.20 cfgFwMnglOutputInterface

Name of the Output Interface to Match

This parameter may be used when `cfgFwMnglChain` is set to **forward(2)**, **output(3)** and **postrouting(5)**.

Groups of interfaces can be matched by adding the character '+' at the end. E.g. `eth+` to match the interfaces eth0, eth1 and eth2.

Set to `-1` to not use this parameter.

Type	DisplayString
Range	1 - 16
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.1.1.5.1.1.7

5.2.21 cfgFwMnglSourceAddress

Source Address to Match

This can be a specific ip address or a range in CIDR notation. Set to `0.0.0.0/0` to match all sources. Set to `172.17.29.7/32` to match the specific IP 172.17.29.7. You may use ! to invert the sense of the rule, e.g. `!192.168.0.0/24`.

Type	DisplayString
Range	1 - 20
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.1.1.5.1.1.8

5.2.22 cfgFwMnglDestinationAddress

Destination Address to Match

This can be a specific ip address or a range in CIDR notation. Set to `0.0.0.0/0` to match all destinations. Set to `172.17.29.7/32` to match the specific IP 172.17.29.7. You may use ! to invert

the sense of the rule, e.g. `!192.168.0.0/24`.

Type	DisplayString
Range	1 - 20
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.1.1.5.1.1.9

5.3 MIB Reference: WESTERMO-SW6-ICL-MIB

5.3.1 cfgIclConnectionThreshold

This value defines the minimum signal level necessary for the ICL application to start evaluating a potential ICL partner.

Applies to AP. 802.11n products only.

Range	-99 - 99
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.5.1.1.3

5.3.2 cfgIclDisconnectionThreshold

This value defines the minimum signal level necessary for a ICL pair to stay connected. If the singal level drops below this level for longer than in cfgIclDisconnectionDelay specified, the ICL application will revert the device do access point and resume scans for a new partner.

Applies to AP. 802.11n products only.

Range	-99 - 99
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.5.1.1.5

5.3.3 cfgIclInterfaceName

This value describes the interface the ICL Application will use for its services.

Applies to AP. 802.11n products only.

Type	DisplayString
Range	1 - 15
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.5.1.1.6

5.4 MIB Reference: WESTERMO-SW6-PWN-MIB

5.4.1 cfgWlanBsteerMatchingSsid

****OBSOLETE:** List of Matching SSIDs**

This parameter is obsolete and has been replaced by `cfgWlanBsteerMatchingWlan`.

Type	DisplayString
Range	1 - 255
Access	noaccess
OID	1.3.6.1.4.1.16177.1.400.2.9.1.1.1.2

5.4.2 cfgWlanBsteerMatchingWlan

WLAN Interface Indices for Band Steering

Multiple indices in `cfgWlanInterfaceTable` may be referenced as a space and/or comma separated list.

All referenced wlan interfaces are used in band steering.

A value of `-1` implicitly disables bandsteering.

Examples:

- 0 1
- 1, 3
- 1,2 3,4

Applies to AP. 802.11ac products only.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.9.1.1.1.3