IbexOS Release Notes

Release 6.12.1-0

Westermo Network Technologies AB

August 12, 2026

Contents

1 General Information **3**

2 Release Highlights **4**
2.1 6.12.1-0 4

3 Limitations **4**

4 Configuration Parameter Changes **4**

5 Supported Cellular Firmware **6**
5.1 Ibex-RT-330, Ibex-RT-630 7
5.2 Ibex-RT-330-5G, Ibex-RT-630-5G 7

6 Changed Configuration Parameter Descriptions **7**
6.1 MIB Reference: WESTERMO-SW6-MIB 7
6.2 MIB Reference: WESTERMO-SW6-BLUETOOTH-MIB 22

1 General Information

Company
Westermo Network Technologies AB

Contact Support
www.westermo.com

Release Number
6.12.1-0

Software Build Number
d747d31b44fffb8d83b6464ef4a496d277f377da

Date of this build
August 12, 2026

2 Release Highlights

2.1 6.12.1-0

- Logging: Add support for RFC5425 Secure Syslog
- Network: Add TechPreview for sTunnel
- Wireless: Add TechPreview for Rogue Access Point Detection (RAPD)
- Bluetooth: Add TechPreview for Bluetooth scanner application

3 Limitations

- 802.11ac products no longer supported (Ibex-RT-610)
- ICL application is not yet supported on 802.11be products (Ibex-1520, Ibex-3520)
- 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)
- When encapsulating traffic in GRETAP, the inner DSCP tag is not inherited to the outer header.

4 Configuration Parameter Changes

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

- cfgWlanRogueApDetection (added)
- cfgWlanRapdServiceEnabled (added)
- cfgWlanRapdTable (added)
- cfgWlanRapdEnabled (added)
- cfgWlanRapdInterface (added)
- cfgWlanRapdCheckInterval (added)

- cfgWlanRapdScanFreqList (added)
- cfgWlanRapdAllowedMacParameter (added)
- cfgWlanRapdSsidParameter (added)
- cfgWlanRapdMacTable (added)
- cfgWlanRapdMacId (added)
- cfgWlanRapdMacEnabled (added)
- cfgWlanRapdMacAddr (added)
- cfgWlanRapdSsidTable (added)
- cfgWlanRapdSsidId (added)
- cfgWlanRapdSsidEnabled (added)
- cfgWlanRapdSsidSsid (added)
- cfgLogRemoteProtocol (changed)
- cfgLogRemotePort (changed)
- cfgLogRemoteCaIds (added)
- cfgLogRemoteCertId (added)
- cfgLogRemoteCrlExpiryExtension (added)
- cfgLogRemoteTlsControlParams (added)
- cfgLogRemoteCiphers (added)
- cfgDhcpDnsmasqScopeParameter (changed)
- cfgDhcpScopeId (changed)
- cfgCellDefaultBearerApn (changed)
- cfgScepRaId (added)
- cfgScepCaId (changed)
- cfgStunnelGlobalEnabled (added)

- cfgStunnelGlobalLogLevel (added)
- cfgStunnelInstanceTable (added)
- cfgStunnelInstEnabled (added)
- cfgStunnelInstMode (added)
- cfgStunnelInstListenAddress (added)
- cfgStunnelInstDestinationAddress (added)
- cfgStunnelInstTlsCertId (added)
- cfgStunnelInstTlsCaIds (added)
- cfgStunnelInstVerificationMode (added)
- cfgStunnelInstTlsTrustAnchorCerts (added)
- cfgStunnelInstTlsPeerIdentities (added)
- rpcSysFactoryReset (changed)
- swCellSupports5g (added)
- cfgBtScnWindow (added)
- cfgBtScnMacOutput (added)
- swBtScnMacCount (added)
- swBtScnMacAddress (added)
- swBtScnMacType (added)
- swBtScnName (added)

5 Supported Cellular Firmware

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

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

- EM12GPAR01A20M4G_01.003.01.003
- EM12GPAR01A21M4G_01.200.01.200
- EM12GPAR01A21M4G_01.204.01.204
- EM12GPAR01A21M4G_01.300.01.300 (preferred)

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

- RM520NGLAAR03A01M4G_01.202.01.202
- RM520NGLAAR03A03M4G_01.201.01.201
- RM520NGLAAR03A04M4G_01.204.01.204
- RM520NGLAAR03A04M4G_A0.301.A0.301
- RM520NGLAAR03A04M4G_A0.303.A0.303 (preferred)

Other cellular firmware versions are not supported.

6 Changed Configuration Parameter Descriptions

6.1 MIB Reference: WESTERMO-SW6-MIB

6.1.1 cfgScepCaId

Reference ID for CA Certificate

This certificate is used for the signing and optionally also for the encryption. If the SCEP server requires two separate certificates, the RA encryption certificate must be selected with the `cfgScepRaId` parameter.

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

6.1.2 cfgScepRaId

Reference ID for the RA Certificate

This is an optional RA encryption certificate. It is needed when the encryption is done with a separate certificate.

Set to -1 if not using a RA certificate.

Applies to STA.

Range	-1 - 65535
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1002.2.1.20

6.1.3 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. If more than one WWAN interfaces are enabled, explicit APN's must be defined. FOTA selects the cellular provider default APN to access the update server.

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. FOTA selects the APN of the first WWAN interface `wwan0` to access the update server.

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

6.1.4 cfgStunnelGlobalEnabled

TECHPREVIEW: Enable stunnel daemon

Enumeration	disabled (0), enabled (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1010.1.1

6.1.5 cfgStunnelGlobalLogLevel

TECHPREVIEW: Log level for stunnel daemon.

Default is `notice(5)`.

Enumeration	emerg (0), alert (1), crit (2), err (3), warning (4), notice (5), info (6), debug (7)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1010.1.4

6.1.6 cfgStunnelInstanceTable

Stunnel Instance Configuration

Range	0 - 7
OID	1.3.6.1.4.1.16177.1.400.1.1.1010.2

6.1.7 cfgStunnelInstListenAddress

TECHPREVIEW: Stunnel Instance Listen Address

If only port is supplied, the instance is accessible from all local IP addresses.

Corresponds to stunnel's `accept` config parameter.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1010.2.1.10

6.1.8 cfgStunnelInstDestinationAddress

TECHPREVIEW: Stunnel Instance Destination Address

Hostname/IP-address and/or port to which this stunnel instance connects.

If only port is supplied, the service to which stunnel connects needs to be running on localhost.

Corresponds to stunnel's `connect` config parameter.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1010.2.1.15

6.1.9 cfgStunnelInstEnabled

TECHPREVIEW: Enable this server

Enumeration	disabled (0), enabled (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1010.2.1.2

6.1.10 cfgStunnelInstTlsCertId

TECHPREVIEW: Stunnel Instance Certificate ID

Reference ID of certificate in Cert-Store to be used as TLS end-node/leaf certificate. Corresponds to certificate passed in stunnel's `cert` config parameter.

If `cfgStunnelInstMode` is `server(0)`, this param is required, otherwise, it is only needed if the server requires client authentication.

Depending on the client's configuration, the entire certificate chain must be available. Additionally required certificates can be passed via `cfgStunnelInstTlsCaIds`.

Type	Integer32
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1010.2.1.20

6.1.11 cfgStunnelInstTlsCaIds

TECHPREVIEW: Stunnel Instance CA Certificate IDs

Set to `-1` to use stunnel without CA certificate. Multiple certificates may be referenced by writing the ids of the certificates as space and/or comma separated list.

The configured CA certificates will be concatenated to `cfgStunnelInstTlsCertId` and passed to stunnel's `cert` config parameter.

Examples:

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

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1010.2.1.21

6.1.12 cfgStunnelInstVerificationMode

TECHPREVIEW: Stunnel Instance Verification Mode

Defines whether peers must authenticate themselves.

Default is `none(0)`. For all other values, the corresponding certificate(s) need to be specified in `cfgStunnelInstTlsCaIds`.

This parameter maps to the boolean `verifyPeer` and `verifyChain` in the stunnel config file.

- **none(0)** (default): Instance accepts all connections.
- **peer(1)**: The peer certificate must be in a locally installed certificate file.
- **chain(2)**: Verify the peer's certificate chain. I.e. peer's certificate needs to be signed by trusted root CA.
- **both(3)**: **peer(1)** and **chain(2)** apply at the same time.

Enumeration	none (0), peer (1), chain (2), both (3)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1010.2.1.22

6.1.13 cfgStunnelInstTlsTrustAnchorCerts

TECHPREVIEW: Stunnel Instance TLS Trust Anchor Certificates

Set to `-1` to use without trust anchor certificates. Multiple certificates may be referenced by writing the ids of the certificates as space and/or comma separated list.

Different certificates need to be supplied depending on the value of `cfgStunnelInstVerificationMode`:

- **none(0)**: No certificates are needed / loaded.
- **peer(1)**: Peer leaf certificate(s) must be supplied.
- **chain(2)**: Entire certificate chain of peer's signatory entity must be supplied (e.g. intermediate + root CA).
- **both(3)**: Both must be supplied.

The concatenated certificates will be passed in stunnel's `CAfile` configuration parameter.

Examples:

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

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1010.2.1.23

6.1.14 cfgStunnelInstTlsPeerIdentities

TECHPREVIEW: Stunnel Instance TLS Peer Identities

List of IP addresses and/or hostnames, which the peer certificate's CN or SAN must contain. Check is only performed if `cfgStunnelInstVerificationMode` is nonzero.

Set to `-1` to not verify peer identities. Multiple hostnames and/or IP addresses may be supplied by writing them as a space and/or comma separated list.

When configuring a client in a regular PKI setup, it is strongly recommended to supply the server host name and/or IP address corresponding to certificate CN or SAN.

Maps to stunnel's `checkHost` and `checkIP` configuration parameters.

Examples:

- `-1`
- `example.com`
- `192.168.1.55`
- `some.example.com 192.168.1.32`
- `192.168.1.32, example.com, westermo.com`

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1010.2.1.24

6.1.15 cfgStunnelInstMode

TECHPREVIEW: Stunnel Instance Mode

- **server(0)** Instance acts as TLS server, may accept connections from multiple clients.
- **client(1)** Instance acts as TLS client, may connect to one server at a time.

Enumeration	server (0), client (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.1010.2.1.3

6.1.16 cfgLogRemoteCrlExpiryExtension

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

Range	-1 - 1095
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.11.2.1.1.10

6.1.17 cfgLogRemoteTlsControlParams

Bitfield to Control TLS Behavior

When the upload server is to be accessed via certificates, this setting is used to control the TLS behaviour.

Supported bits:

- 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	1.3.6.1.4.1.16177.1.400.1.1.11.2.1.1.11

6.1.18 cfgLogRemoteCiphers

OpenSSL Cipher String for Remote Syslog

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

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

Used only if `cfgSyslogRemoteProtocol` is **tcptls(2)**.

Example:

- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384
- DEFAULT:!EXP:!LOW

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.11.2.1.1.12

6.1.19 cfgLogRemoteProtocol

Protocol to Send Log Messages

The udp(0) protocol complies with the syslog protocol according to RFC5424.

The tcptls(2) protocol complies with the secure syslog protocol according to RFC5425.

Enumeration	udp (0), tcp (1), tcptls (2)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.11.2.1.1.4

6.1.20 cfgLogRemotePort

Remote Port

The remote port to which syslog messages are sent.

When set to `-1` uses the assigned port according to the protocol that is selected in `cfgLogRemoteProtocol`:

udp(0) Port 514 **tcp(1)** Port 514 **tcptls(2)** Port 6514

Range	-1 - 65535
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.11.2.1.1.6

6.1.21 cfgLogRemoteCaIds

CA IDs

Reference to the CA IDs to be used.

Type	DisplayString
Range	1 - 255
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.11.2.1.1.8

6.1.22 cfgLogRemoteCertId

Certificate ID

Reference to the Certificate ID to be used.

Range	-1 - 1000
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.11.2.1.1.9

6.1.23 cfgDhcpDnsmasqScopeParameter

Parameter to Set Which Scope ID to use for the DHCP Server

This is used in conjunction with the scope ID parameter `cfgDhcpScopeId`.

Range	0 - 511
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.13.2.1.2

6.1.24 cfgDhcpScopeId

Scope ID

This is used in conjunction with the DHCP parameter `cfgDhcpDnsmasqScopeParameter`.

Range	0 - 511
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.13.3.1.2

6.1.25 cfgWlanRogueApDetection

OID	1.3.6.1.4.1.16177.1.400.1.1.3.30

6.1.26 cfgWlanRapdServiceEnabled

TECHPREVIEW: Enable Rogue AP Detection (RAPD)

This feature enables the rogue AP detection to monitor potential security issues. Rogue APs are defined as foreign ones which preted to provide one AP's own SSID.

This is a global enable flag that activates the detection service, while each interface to be monitored is defined in cfgWlanRapdTable and can be enabled individually.

The detection is available for 802.11ax and 802.11be APs.

Applies to AP.

Enumeration	disabled (0), enabled (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.30.1

6.1.27 cfgWlanRapdTable

RAPD Table

Range	0 - 15
OID	1.3.6.1.4.1.16177.1.400.1.1.3.30.10

6.1.28 cfgWlanRapdEnabled

TECHPREVIEW: Enable this Instance of RAPD Detection

Applies to AP.

Enumeration	disabled (0), enabled (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.30.10.1.2

6.1.29 cfgWlanRapdInterface

TECHPREVIEW: WLAN Interface Index for RAPD

An index in `cfgWlanInterfaceTable` may be referenced.

Applies to AP.

Range	0 - 63
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.30.10.1.3

6.1.30 cfgWlanRapdCheckInterval

TECHPREVIEW: Check Interval for RAPD Instance in Seconds

This defines the interval of the scan processes to look for potential rogue APs in seconds.

Note that scanning for RAPs comes at a cost, since the AP temporarily leaves its operating channel and during that time can't provide services to stations. Therefore, the check interval shall be chosen as a trade-off between a sufficient detection probability and an acceptable service degradation.

Applies to AP.

Range	1 - 86400
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.30.10.1.4

6.1.31 cfgWlanRapdScanFreqList

TECHPREVIEW: Scan frequency list to use for this RAPD instance

This is the index of the `cfgWlanFreqTable` that shall be used to scan for rogue APs. The chosen table is to be configured with the frequencies that should be monitored.

Setting the value to `-2` scans all frequencies possibly in the configured country code and allowed by the radio.

Setting the value to `-1` scans only the configured frequency on which the currently radio operates.

Note: scanning many frequencies increases service degradation, since the AP interrupts its operation for the scan process and the off-channel time is proportional to the amount of frequencies scanned. Therefore, a full scan of all available frequencies is not advised.

Applies to AP.

Range	-2 - 23
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.30.10.1.5

6.1.32 cfgWlanRapdAllowedMacParameter

TECHPREVIEW: MAC Addresses Ignored as Rogue APs

This is a reference ID to the `cfgWlanRapdMacTable`. Uses all referenced parameters which have as `cfgWlanRapdMacId` the value set here.

This allows to have an installation with multiple own APs providing the same SSID and allowing those. When no MAC addresses are referenced, any AP other using the own SSID will be detected as rogue.

A value of -1 means standlone mode.

Applies to AP.

Range	-1 - 63
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.30.10.1.6

6.1.33 cfgWlanRapdSsidParameter

TECHPREVIEW: SSIDs to Scan for Rogue APs

This is a reference ID to the cfgWlanRapdSsidTable. Uses all referenced parameters which have as cfgWlanRapdSsidId the value set here.

All referenced SSIDs are monitored for rogue APs. When this value is set to -1 the SSID to scan for is the interface's AP SSID.

Setting arbitrary SSIDs allows for one AP to do the detection work for a different AP. Assume an installation where a company has a public and a private wlan network, of which the private is not allowed to have service interruption. The AP providing the public network can be configured to scan for both SSIDs.

Applies to AP.

Range	-1 - 63
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.30.10.1.7

6.1.34 cfgWlanRapdMacTable

Rogue Access Point Detection Allowed MAC Addresses Table

Range	0 - 255
OID	1.3.6.1.4.1.16177.1.400.1.1.3.30.11

6.1.35 cfgWlanRapdMacId

TECHPREVIEW: ID of the RAPD MAC Address Table

The configuration item cfgWlanRapdAllowedMacParameter references to this ID.

Applies to AP.

Range	0 - 63
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.30.11.1.2

6.1.36 cfgWlanRapdMacEnabled

TECHPREVIEW: Disable or Enable This Entry in the MAC List

Applies to AP.

Enumeration	disabled (0), enabled (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.30.11.1.3

6.1.37 cfgWlanRapdMacAddr

TECHPREVIEW: MAC Address to be Allowed in RAPD

Format: `00:14:5a:09:01:23`

Applies to AP.

Type	DisplayString
Range	17 - 17
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.30.11.1.4

6.1.38 cfgWlanRapdSsidTable

Rogue Access Point Detection SSID Table

Range	0 - 63
OID	1.3.6.1.4.1.16177.1.400.1.1.3.30.12

6.1.39 cfgWlanRapdSsidId

TECHPREVIEW: ID of the RAPD SSID List

The configuration item `cfgWlanRapdSsidParameter` references to this ID.

Applies to AP.

Range	0 - 63
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.30.12.1.2

6.1.40 cfgWlanRapdSsidEnabled

TECHPREVIEW: Disable or Enable This Entry in the SSID List

Applies to AP.

Enumeration	disabled (0), enabled (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.30.12.1.3

6.1.41 cfgWlanRapdSsidSsid

TECHPREVIEW: Rogue SSID to Scan for

Applies to AP.

Type	DisplayString
Range	1 - 32
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.1.3.30.12.1.4

6.1.42 rpcSysFactoryReset

Factory Reset

Perform a factory reset and reboot the device. This will reset device configuration, including administrator password and certificates, to its default state.

Writing **reset(1)** the device will reboot after resetting.

Note: You will not be able to communicate with the device until the factory reset has finished and the device has been rebooted.

Writing **resetAndHalt(2)** will halt the device after resetting and shutting down.

Applies to AP and STA.

Enumeration	nop (0), reset (1), resetAndHalt (2)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.1.3.3.2

6.1.43 swCellSupports5g

Connected cellular network supports 5G

Indication if the currently connected cellular network supports 5G technology.

- **no(0)**
- **yes(1)**

Check `swCellSignalType` to get the exact signal type of the current connection. It can also be set to LTE if only the LTE cell is visible but the cellular network basically supports 5G. Some internet service provider enable carrier aggregation with a 5G-NSA cell only when the network load is heavy and fall back to LTE on idle.

Applies to 5G cellular products only.

Enumeration	no (0), yes (1)
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.1.6.50.1.1.28

6.2 MIB Reference: WESTERMO-SW6-BLUETOOTH-MIB

6.2.1 cfgBtScnWindow

TECHPREVIEW: Bluetooth Scanner Scan Window

Defines the scan window duration in seconds for the BLE scanner. Values -1 and 0 use the default scanner behavior.

Range	-1 - 7200
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.11.1.1.100.1

6.2.2 cfgBtScnMacOutput

TECHPREVIEW: Bluetooth Scanner MAC Output

Controls whether individual MAC addresses are printed on each scan window summary.

- **disabled(0)**: Only the MAC count is printed (default)
- **enabled(1)**: MAC addresses are printed along with the count

Enumeration	disabled (0), enabled (1)
Access	readwrite
OID	1.3.6.1.4.1.16177.1.400.2.11.1.1.100.2

6.2.3 swBtScnMacCount

TECHPREVIEW: Scanner MAC Count

Number of unique MAC addresses scanned during the last scan window.

Type	Integer32
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.2.11.2.1.100.1

6.2.4 swBtScnMacAddress

TECHPREVIEW: Scanned MAC address

Type	DisplayString
Range	0 - 17
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.2.11.2.1.100.100.1.2

6.2.5 swBtScnMacType

TECHPREVIEW: Scanned MAC address type

Type	DisplayString
Range	0 - 16
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.2.11.2.1.100.100.1.3

6.2.6 swBtScnName

TECHPREVIEW: Scanned Bluetooth name

Type	DisplayString
Range	0 - 255
Access	readonly
OID	1.3.6.1.4.1.16177.1.400.2.11.2.1.100.100.1.4