


# **Dell Networking W-Series Instant 6.4.0.2-4.1 MIB**



Reference Guide

## Copyright

© 2014 Aruba Networks, Inc. Aruba Networks trademarks include  Airwave, Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, and Aruba Mobility Management System®. Dell™, the DELL™ logo, and PowerConnect™ are trademarks of Dell Inc.

All rights reserved. Specifications in this manual are subject to change without notice.

Originated in the USA. All other trademarks are the property of their respective owners.

## Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. Includes software from Litech Systems Design. The IF-MAP client library copyright 2011 Infoblox, Inc. All rights reserved. This product includes software developed by Lars Fenneberg, et al. The Open Source code used can be found at this site:

[http://www.arubanetworks.com/open\\_source](http://www.arubanetworks.com/open_source)

## Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

---

<b>Contents</b> .....	<b>3</b>
<b>About this Guide</b> .....	<b>20</b>
Intended Audience .....	20
Related Documents .....	20
Conventions .....	20
What is New in this Release .....	21
Contacting Dell .....	21
<b>MIBs Overview</b> .....	<b>22</b>
MIBs .....	22
SNMP .....	23
<b>Using MIBs</b> .....	<b>25</b>
Downloading MIB Files .....	25
Reporting WLAN Health .....	25
SNMP Operations on W-IAPs .....	25
MIB Browsers .....	26
Reading MIB Files .....	26
Opening Line .....	27
Imports .....	27
Inheritance .....	27
Identity .....	28
MIB Modules .....	28
Group .....	28
Table .....	28
Entry .....	28
Closing Line .....	29
SNMP File .....	29
HP OpenView .....	29

<b>Instant MIBs</b> .....	<b>30</b>
aiInfoGroup .....	31
aiVirtualControllerKey .....	31
aiVirtualControllerName .....	32
aiVirtualControllerOrganization .....	32
aiVirtualControllerVersion .....	32
aiVirtualControllerIPAddress .....	32
aiMasterIPAddress .....	33
aiStateGroup .....	33
aiAccessPointTable .....	33
aiAccessPointEntry .....	34
aiAPMACAddress .....	34
aiAPName .....	34
aiAPIPAddress .....	34
aiAPSerialNum .....	34
aiAPModel .....	35
aiAPModelName .....	35
aiAPCPUUtilization .....	35
aiAPMemoryFree .....	35
aiAPUptime .....	35
aiAPTtotalMemory .....	36
aiAPStatus .....	36
aiRadioTable .....	36
aiRadioEntry .....	37
aiRadioAPMacAddress .....	37
aiRadioIndex .....	37
aiRadioMACAddress .....	37
aiRadioChannel .....	38
aiRadioTransmitPower .....	38
aiRadioNoiseFloor .....	38
aiRadioUtilization4 .....	38
aiRadioUtilization64 .....	38

aiRadioTxTotalFrames .....	39
aiRadioTxMgmtFrames .....	39
aiRadioTxDataFrames .....	39
aiRadioTxDataBytes .....	39
aiRadioTxDrops .....	39
aiRadioRxTotalFrames .....	40
aiRadioRxDataFrames .....	40
aiRadioRxDataBytes .....	40
aiRadioRxMgmtFrames .....	40
aiRadioRxBad .....	40
aiRadioPhyEvents .....	41
aiRadioStatus .....	41
<b>aiWlanTable .....</b>	<b>41</b>
aiWlanEntry .....	42
aiWlanAPMACAddress .....	42
aiWlanIndex .....	42
aiWlanESSID .....	42
aiWlanMACAddress .....	42
aiWlanTxTotalFrames .....	43
aiWlanTxDataFrames .....	43
aiWlanTxDataBytes .....	43
aiWlanRxTotalFrames .....	43
aiWlanRxDataFrames .....	43
aiWlanRxDataBytes .....	44
<b>aiClientTable .....</b>	<b>44</b>
aiClientEntry .....	45
aiClientMACAddress .....	45
aiClientWlanMACAddress .....	45
aiClientIPAddress .....	45
aiClientAPIPAddress .....	45
aiClientName .....	46
aiClientOperatingSystem .....	46

aiClientSNR .....	46
aiClientTxDataFrames .....	46
aiClientTxDataBytes .....	46
aiClientTxRetries .....	47
aiClientTxRate .....	47
aiClientRxDataFrames .....	47
aiClientRxDataBytes .....	47
aiClientRxRetries .....	47
aiClientRxRate .....	48
aiClientUptime .....	48
<b>Standard SNMP MIBs .....</b>	<b>49</b>
System MIB .....	49
sysDescr .....	50
sysObjectID .....	50
sysUpTime .....	50
sysName .....	50
sysLocation .....	51
sysServices .....	51
dot1qTpFdbTable .....	51
dot1qFdbId .....	51
dot1qTpFdbAddress .....	52
dot1qTpFdbPort .....	52
dot1qTpFdbStatus .....	52
ifTable .....	52
ifIndex .....	53
ifDescr .....	53
ifType .....	54
ifMtu .....	54
ifSpeed .....	54
ifPhysAddress .....	54
ifAdminStatus .....	55
ifOperStatus .....	55

ifInOctets .....	55
ifInUcastPkts .....	55
ifInNUcastPkts .....	56
ifInDiscards .....	56
ifInErrors .....	56
ifOutOctets .....	56
ifOutUcastPkts .....	57
ifOutDiscards .....	57
ifOutErrors .....	57
ifXTable .....	57
ifName .....	58
ifInMulticastPkts .....	58
ifInBroadcastPkts .....	58
ifOutMulticastPkts .....	59
ifOutBroadcastPkts .....	59
ifHCInOctets .....	59
ifHCInUcastPkts .....	59
ifHCInMulticastPkts .....	60
ifHCInBroadcastPkts .....	60
ifHCOctets .....	60
ifHCOUcastPkts .....	61
ifHCOMulticastPkts .....	61
ifHCOBroadcastPkts .....	61
ifLinkUpDownTrapEnable .....	62
ifPromiscuousMode .....	62
ifConnectorPresent .....	62
<b>Traps .....</b>	<b>63</b>
Trap Hierarchy .....	63
wlsxTrapAPMacAddress .....	68
wlsxTrapAPIpAddress .....	68
wlsxTrapAPBSSID .....	68
wlsxTrapEssid .....	69

---

wlsxTrapTargetAPBSSID .....	69
wlsxTrapTargetAPSSID .....	69
wlsxTrapTargetAPChannel .....	69
wlsxTrapNodeMac .....	70
wlsxTrapSourceMac .....	70
wlsxReceiverMac .....	70
wlsxTrapTransmitterMac .....	70
wlsxTrapReceiverMac .....	70
wlsxTrapSnr .....	71
wlsxTrapSignatureName .....	71
wlsxTrapFrameType .....	71
wlsxTrapAddressType .....	71
wlsxTrapAPLocation .....	71
wlsxTrapAPChannel .....	72
wlsxTrapAPTxPower .....	72
wlsxTrapMatchedMac .....	72
wlsxTrapMatchedIp .....	72
wlsxTrapRogueIpURL .....	72
wlsxTrapVLANId .....	73
wlsxTrapAdminStatus .....	73
wlsxTrapOperStatus .....	73
wlsxTrapAuthServerName .....	73
wlsxTrapAuthServerTimeout .....	73
wlsxTrapCardSlot .....	74
wlsxTrapTemperatureValue .....	74
wlsxTrapProcessName .....	74
wlsxTrapFanNumber .....	74
wlsxTrapVoltageType .....	74
wlsxTrapVoltageValue .....	75
wlsxTrapStationBlackListReason .....	75
wlsxTrapSpoofedIpAddress .....	75
wlsxTrapSpoofedOldPhyAddress .....	75



---

wlsxTrapSpoofedNewPhyAddress .....	75
wlsxTrapDBName .....	76
wlsxTrapDBUserName .....	76
wlsxTrapDBIpAddress .....	76
wlsxTrapDBType .....	76
wlsxTrapVrrpID .....	76
wlsxTrapVrrpMasterIp .....	77
wlsxTrapVrrpOperState .....	77
wlsxTrapESIServerGrpName .....	77
wlsxTrapESIServerName .....	77
wlsxTrapESIServerIpAddress .....	77
wlsxTrapLicenseDaysRemaining .....	78
wlsxTrapSwitchIp .....	78
wlsxTrapSwitchRole .....	78
wlsxTrapUserIpAddress .....	78
wlsxTrapUserPhyAddress .....	78
wlsxTrapUserName .....	79
wlsxTrapUserRole .....	79
wlsxTrapUserAuthenticationMethod .....	79
wlsxTrapAPRadioNumber .....	79
wlsxTrapRogueInfoURL .....	79
wlsxTrapInterferingAPIInfoURL .....	80
wlsxTrapPortNumber .....	80
wlsxTrapTime .....	80
wlsxTrapHostIp .....	80
wlsxTrapHostPort .....	80
wlsxTrapConfigurationId .....	81
wlsxTrapCTSURL .....	81
wlsxTrapCTSTransferType .....	81
wlsxTrapConfigurationState .....	81
wlsxTrapUpdateFailureReason .....	81
wlsxTrapUpdateFailedObj .....	82

---

wlsxTrapTableEntryChangeType .....	82
wlsxTrapGlobalConfigObj .....	82
wlsxTrapTableGenNumber .....	82
wlsxTrapLicenseld .....	82
wlsxTrapConfidenceLevel .....	83
wlsxTrapMissingLicenses .....	83
wlsxVoiceCurrentNumCdr .....	83
wlsxTrapTunnelId .....	83
wlsxTrapTunnelStatus .....	83
wlsxTrapTunnelUpReason .....	84
wlsxTrapTunnelDownReason .....	84
wlsxTrapApSerialNumber .....	84
wlsxTraptimeStr .....	84
wlsxTrapMasterIp .....	84
wlsxTrapLocalIp .....	85
wlsxTrapMasterName .....	85
wlsxTrapLocalName .....	85
wlsxTrapPrimaryControllerIp .....	85
wlsxTrapBackupControllerIp .....	85
wlsxTrapSpoofedFrameType .....	86
wlsxTrapAssociationType .....	86
wlsxTrapDeviceIpAddress .....	86
wlsxTrapDeviceMac .....	86
wlsxTrapVcIpAddress .....	86
wlsxTrapVcMacAddress .....	87
wlsxTrapAPName .....	87
wlsxTrapApMode .....	87
wlsxTrapAPPprevChannel .....	87
wlsxTrapAPPprevChannelSec .....	87
wlsxTrapAPPprevTxPower .....	88
wlsxTrapAPCurMode .....	88
wlsxTrapAPPprevMode .....	88

wlsxTrapAPARMChangeReason .....	88
wlsxTrapAPChannelSec .....	88
wlsxTrapUserAttributeChangeType .....	89
wlsxTrapAPControllerIp .....	89
wlsxTrapApMasterStatus .....	89
wlsxTrapCaName .....	89
wlsxTrapCrlName .....	89
wlsxTrapCount .....	90
wlsxTrapAPPreviousUplinkType .....	90
wlsxTrapAPPreviousUplinkActiveTime .....	90
wlsxTrapAPActiveUplinkType .....	90
wlsxTrapAPUplinkChangeReason .....	90
wlsxTrapAPManagedModeConfigFailure .....	91
ai Traps Objects Group .....	91
wlsxTrapAPMacAddress .....	95
wlsxTrapAPIpAddress .....	95
wlsxTrapAPBSSID .....	95
wlsxTrapEssid .....	96
wlsxTrapTargetAPBSSID .....	96
wlsxTrapTargetAPSSID .....	96
wlsxTrapTargetAPChannel .....	96
wlsxTrapNodeMac .....	97
wlsxTrapSourceMac .....	97
wlsxReceiverMac .....	97
wlsxTrapTransmitterMac .....	97
wlsxTrapReceiverMac .....	97
wlsxTrapSnr .....	98
wlsxTrapSignatureName .....	98
wlsxTrapFrameType .....	98
wlsxTrapAddressType .....	98
wlsxTrapAPLocation .....	98
wlsxTrapAPChannel .....	99

---

wlsxTrapAPTxPower .....	99
wlsxTrapMatchedMac .....	99
wlsxTrapMatchedIp .....	99
wlsxTrapRogueIfoURL .....	99
wlsxTrapVLANId .....	100
wlsxTrapAdminStatus .....	100
wlsxTrapOperStatus .....	100
wlsxTrapAuthServerName .....	100
wlsxTrapAuthServerTimeout .....	100
wlsxTrapCardSlot .....	101
wlsxTrapTemperatureValue .....	101
wlsxTrapProcessName .....	101
wlsxTrapFanNumber .....	101
wlsxTrapVoltageType .....	101
wlsxTrapVoltageValue .....	102
wlsxTrapStationBlackListReason .....	102
wlsxTrapSpoofedIpAddress .....	102
wlsxTrapSpoofedOldPhyAddress .....	102
wlsxTrapSpoofedNewPhyAddress .....	102
wlsxTrapDBName .....	103
wlsxTrapDBUserName .....	103
wlsxTrapDBIpAddress .....	103
wlsxTrapDBType .....	103
wlsxTrapVrrpID .....	103
wlsxTrapVrrpMasterIp .....	104
wlsxTrapVrrpOperState .....	104
wlsxTrapESIServerGrpName .....	104
wlsxTrapESIServerName .....	104
wlsxTrapESIServerIpAddress .....	104
wlsxTrapLicenseDaysRemaining .....	105
wlsxTrapSwitchIp .....	105
wlsxTrapSwitchRole .....	105

---

wlsxTrapUserIpAddress .....	105
wlsxTrapUserPhyAddress .....	105
wlsxTrapUserName .....	106
wlsxTrapUserRole .....	106
wlsxTrapUserAuthenticationMethod .....	106
wlsxTrapAPRadioNumber .....	106
wlsxTrapRogueInfoURL .....	106
wlsxTrapInterferingAPIInfoURL .....	107
wlsxTrapPortNumber .....	107
wlsxTrapTime .....	107
wlsxTrapHostIp .....	107
wlsxTrapHostPort .....	107
wlsxTrapConfigurationId .....	108
wlsxTrapCTSURL .....	108
wlsxTrapCTSTransferType .....	108
wlsxTrapConfigurationState .....	108
wlsxTrapUpdateFailureReason .....	108
wlsxTrapUpdateFailedObj .....	109
wlsxTrapTableEntryChangeType .....	109
wlsxTrapGlobalConfigObj .....	109
wlsxTrapTableGenNumber .....	109
wlsxTrapLicenseId .....	109
wlsxTrapConfidenceLevel .....	110
wlsxTrapMissingLicenses .....	110
wlsxVoiceCurrentNumCdr .....	110
wlsxTrapTunnelId .....	110
wlsxTrapTunnelStatus .....	110
wlsxTrapTunnelUpReason .....	111
wlsxTrapTunnelDownReason .....	111
wlsxTrapApSerialNumber .....	111
wlsxTraptimeStr .....	111
wlsxTrapMasterIp .....	111

---

wlsxTrapLocalIp .....	112
wlsxTrapMasterName .....	112
wlsxTrapLocalName .....	112
wlsxTrapPrimaryControllerIp .....	112
wlsxTrapBackupControllerIp .....	112
wlsxTrapSpoofedFrameType .....	113
wlsxTrapAssociationType .....	113
wlsxTrapDeviceIpAddress .....	113
wlsxTrapDeviceMac .....	113
wlsxTrapVcIpAddress .....	113
wlsxTrapVcMacAddress .....	114
wlsxTrapAPName .....	114
wlsxTrapApMode .....	114
wlsxTrapAPPrevChannel .....	114
wlsxTrapAPPrevChannelSec .....	114
wlsxTrapAPPrevTxPower .....	115
wlsxTrapAPCurMode .....	115
wlsxTrapAPPrevMode .....	115
wlsxTrapAPARMChangeReason .....	115
wlsxTrapAPChannelSec .....	115
wlsxTrapUserAttributeChangeType .....	116
wlsxTrapAPControllerIp .....	116
wlsxTrapApMasterStatus .....	116
wlsxTrapCaName .....	116
wlsxTrapCrlName .....	116
wlsxTrapCount .....	117
wlsxTrapAPPreviousUplinkType .....	117
wlsxTrapAPPreviousUplinkActiveTime .....	117
wlsxTrapAPActiveUplinkType .....	117
wlsxTrapAPUplinkChangeReason .....	117
wlsxTrapAPManagedModeConfigFailure .....	118
ai Traps Definitions Group .....	118

---

wlsxNUserEntryCreated .....	124
wlsxNUserEntryDeleted .....	124
wlsxNUserEntryAuthenticated .....	124
wlsxNUserEntryDeAuthenticated .....	124
wlsxNUserAuthenticationFailed .....	125
wlsxNAuthServerReqTimedOut .....	125
wlsxNAuthServerTimedOut .....	125
wlsxNAuthServerIsUp .....	125
wlsxNAccessPointIsUp .....	125
wlsxNChannelChanged .....	126
wlsxNStationAddedToBlackList .....	126
wlsxNStationRemovedFromBlackList .....	126
wlsxNRadioAttributesChanged .....	126
wlsxUnsecureAPDetected .....	126
wlsxUnsecureAPResolved .....	127
wlsxStalImpersonation .....	127
wlsxReservedChannelViolation .....	127
wlsxValidSSIDViolation .....	127
wlsxChannelMisconfiguration .....	127
wlsxOUIMisconfiguration .....	128
wlsxSSIDMisconfiguration .....	128
wlsxShortPreambleMisconfiguration .....	128
wlsxWPAMisconfiguration .....	128
wlsxAdhocNetworkDetected .....	128
wlsxAdhocNetworkRemoved .....	129
wlsxStaPolicyViolation .....	129
wlsxRepeatWEPIVViolation .....	129
wlsxWeakWEPIVViolation .....	129
wlsxChannelInterferenceDetected .....	129
wlsxChannelInterferenceCleared .....	130
wlsxAPIInterferenceDetected .....	130
wlsxAPIInterferenceCleared .....	130

---

wlsxStaInterferenceDetected .....	130
wlsxStaInterferenceCleared .....	130
wlsxFrameRetryRateExceeded .....	131
wlsxFrameReceiveErrorRateExceeded .....	131
wlsxFrameFragmentationRateExceeded .....	131
wlsxFrameBandWidthRateExceeded .....	131
wlsxFrameLowSpeedRateExceeded .....	131
wlsxFrameNonUnicastRateExceeded .....	132
wlsxLoadbalancingEnabled .....	132
wlsxLoadbalancingDisabled .....	132
wlsxChannelFrameRetryRateExceeded .....	132
wlsxChannelFrameFragmentationRateExceeded .....	132
wlsxChannelFrameErrorRateExceeded .....	133
wlsxSignatureMatchAP .....	133
wlsxSignatureMatchSta .....	133
wlsxChannelRateAnomaly .....	133
wlsxNodeRateAnomaly .....	133
wlsxNodeRateAnomalyAP .....	134
wlsxNodeRateAnomalySta .....	134
wlsxEAPRateAnomaly .....	134
wlsxSignalAnomaly .....	134
wlsxSequenceNumberAnomalyAP .....	135
wlsxSequenceNumberAnomalySta .....	135
wlsxDisconnectStationAttack .....	135
wlsxApFloodAttack .....	136
wlsxAdhocNetwork .....	136
wlsxWirelessBridge .....	136
wlsxInvalidMacOUIAP .....	136
wlsxInvalidMacOUISta .....	136
wlsxWEPMisconfiguration .....	137
wlsxStaRepeatWEPIVViolation .....	137
wlsxStaWeakWEPIVViolation .....	137



---

wlsxStaAssociatedToUnsecureAP .....	137
wlsxStaUnAssociatedFromUnsecureAP .....	137
wlsxAdhocNetworkBridgeDetected .....	138
wlsxInterferingApDetected .....	138
wlsxColdStart .....	138
wlsxWarmStart .....	138
wlsxAPImpersonation .....	138
wlsxNAuthServerIsDown .....	139
wlsxWindowsBridgeDetected .....	139
wlsxSignAPNetstumbler .....	139
wlsxSignStaNetstumbler .....	139
wlsxSignAPAsleep .....	139
wlsxSignStaAsleep .....	140
wlsxSignAPAirjack .....	140
wlsxSignStaAirjack .....	140
wlsxSignAPNullProbeResp .....	140
wlsxSignStaNullProbeResp .....	140
wlsxSignAPDeauthBcast .....	141
wlsxSignStaDeauthBcast .....	141
wlsxWindowsBridgeDetectedSta .....	141
wlsxAdhocNetworkBridgeDetectedAP .....	141
wlsxAdhocNetworkBridgeDetectedSta .....	142
wlsxHT40MHzIntoleranceSta .....	143
wlsxNAdhocNetwork .....	143
wlsxNAdhocNetworkBridgeDetectedAP .....	144
wlsxNStaUnAssociatedFromUnsecureAP .....	145
wlsxOmertaAttack .....	146
wlsxTKIPReplayAttack .....	146
wlsxChopChopAttack .....	146
wlsxFataJackAttack .....	146
wlsxInvalidAddressCombination .....	146
wlsxValidClientMisassociation .....	147

---

wlsxMalformedHTIEDetected .....	147
wlsxMalformedAssocReqDetected .....	147
wlsxOverflowIEDetected .....	147
wlsxOverflowEAPOLKeyDetected .....	148
wlsxMalformedFrameLargeDurationDetected .....	148
wlsxMalformedFrameWrongChannelDetected .....	148
wlsxMalformedAuthFrame .....	148
wlsxCTSRateAnomaly .....	148
wlsxRTSRateAnomaly .....	149
wlsxNRogueAPDetected .....	149
wlsxNRogueAPResolved .....	149
wlsxNeighborAPDetected .....	149
wlsxNInterferingAPDetected .....	149
wlsxNSuspectRogueAPDetected .....	150
wlsxNSuspectRogueAPResolved .....	150
wlsxBlockAckAttackDetected .....	150
wlsxHotspotterAttackDetected .....	150
wlsxNSignatureMatch .....	151
wlsxNSignatureMatchNetstumbler .....	151
wlsxNSignatureMatchAsleep .....	151
wlsxNSignatureMatchAirjack .....	151
wlsxNSignatureMatchNullProbeResp .....	152
wlsxNSignatureMatchDeathBcast .....	152
wlsxNSignatureMatchDisassocBcast .....	152
wlsxNSignatureMatchWellenreiter .....	153
wlsxAPDeathContainment .....	153
wlsxClientDeathContainment .....	153
wlsxAPWiredContainment .....	153
wlsxClientWiredContainment .....	153
wlsxAPTaggedWiredContainment .....	154
wlsxClientTaggedWiredContainment .....	154
wlsxTarpitContainment .....	154

---

wlsxAPChannelChange .....	154
wlsxAPPowerChange .....	154
wlsxAPModeChange .....	155
wlsxUserEntryAttributesChanged .....	155
wlsxNAPMasterStatusChange .....	155
wlsxNAdhocUsingValidSSID .....	155
wlsxMgmtUserAuthenticationFailed .....	156
SNMP Traps .....	156
linkDown .....	156
linkUp .....	156

This guide provides information on Management Information Base (MIBs) supported in Dell Networking W-Series Instant 6.4.0.2-4.1 software release.

## Intended Audience

This manual is intended for network administrators and operators responsible for managing the Dell Networking W-Series Instant Access Point (W-IAP).

## Related Documents

In addition to this document, the Dell W-IAP product documentation includes the following:

- *Dell Networking W-Series Instant Access Point Installation Guides*
- *Dell Networking W-Series Instant 6.4.0.2-4.1 User Guide*
- *Dell Networking W-Series Instant 6.4.0.2-4.1 CLI Reference Guide*
- *Dell Networking W-Series Instant 6.4.0.2-4.1 Quick Start Guide*
- *Dell Networking W-Series Instant 6.4.0.2-4.1 Syslog Messages Reference Guide*
- *Dell Networking W-Series Instant 6.4.0.2-4.1 Release Notes*

## Conventions

The following conventions are used throughout this manual to emphasize important concepts:

**Table 1:** *Typographical Conventions*

Type Style	Description
<i>Italics</i>	This style is used to emphasize important terms and to mark the titles of books.
System items	This fixed-width font depicts the following: <ul style="list-style-type: none"> <li>• Sample screen output</li> <li>• System prompts</li> <li>• Filenames, software devices, and specific commands when mentioned in the text</li> </ul>
<b>Commands</b>	In the command examples, this style depicts the keywords that must be typed exactly as shown.

Type Style	Description
<Arguments>	In the command examples, italicized text within angle brackets represents items that you should replace with information appropriate to your specific situation. For example: # <b>send</b> <text message> In this example, you would type “send” at the system prompt exactly as shown, followed by the text of the message you wish to send. Do not type the angle brackets.
[Optional]	Command examples enclosed in brackets are optional. Do not type the brackets.
{Item A   Item B}	In the command examples, items within curled braces and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the braces or bars.

The following informational icons are used throughout this guide:



Indicates helpful suggestions, pertinent information, and important things to remember.



Indicates a risk of damage to your hardware or loss of data.



Indicates a risk of personal injury or death.

## What is New in this Release

The version of the document contains the following updates:

**Table 2:** *New Features in Dell Networking W-Series Instant 6.4.0.2-4.1*

Feature	Description
Sourcing Virtual Controller traps from Virtual Controller IP address and sysObjectID enhancements	In the current release, if the Virtual Controller IP address is configured, the traps are generated with Virtual Controller IP as the source IP address. The <b>sysObjectID</b> of systemMIB returns results with <b>iapvc</b> when a query on the Virtual Controller IP is performed.

## Contacting Dell

**Table 3:** *Support Information*

Support	
Main Website	<b>dell.com</b>
Contact Information	<b>dell.com/contactdell</b>
Support Website	<b>dell.com/support</b>
Documentation Website	<b>dell.com/support/manuals</b>

This chapter provides information about Management Information Base (MIBs) supported in Dell Networking W-Series Instant 6.4.0.2-4.1 software release.

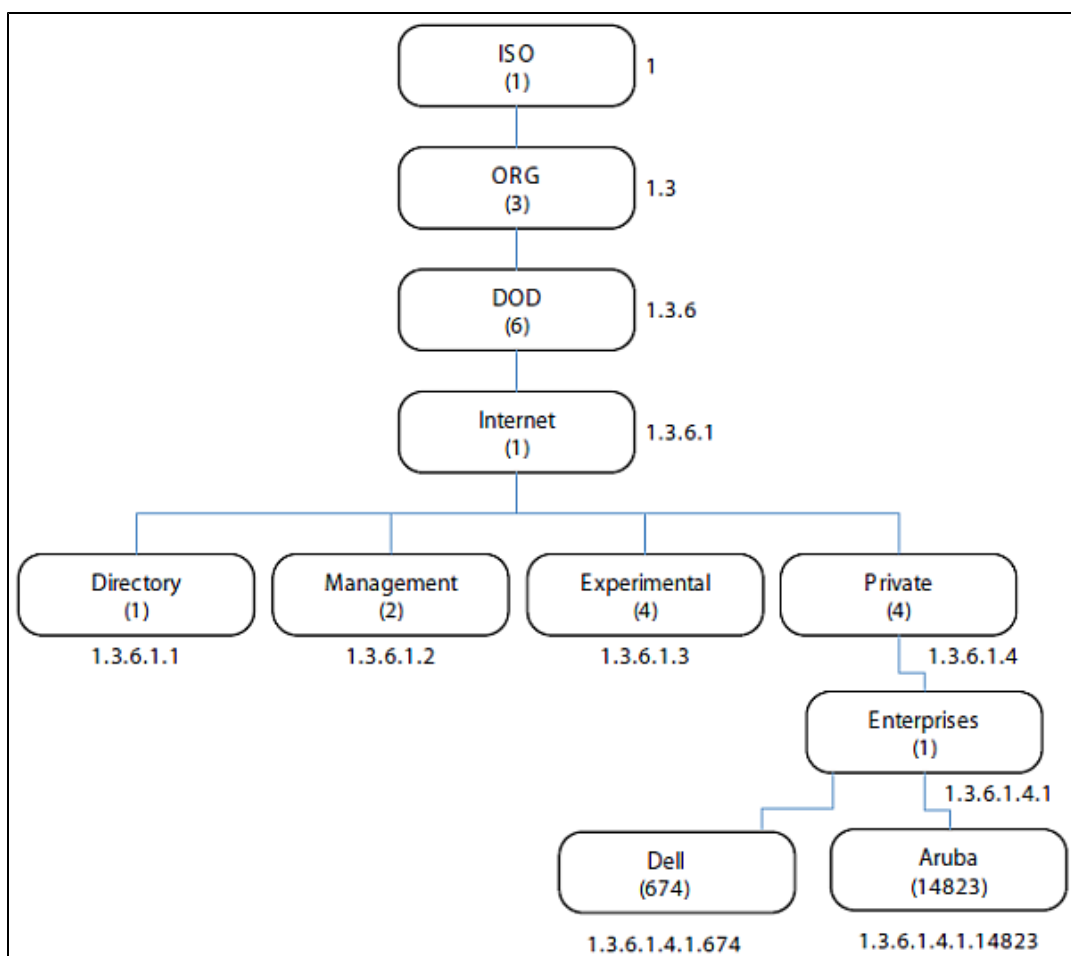
## MIBs

A MIB is a virtual database that contains information used for network management. Each managed device contains MIBs that define its properties. A separate MIB is provided for each defined property, such as the group of physical ports assigned to a VLAN or the statistical data of packets transferred at a specific rate.

MIB objects, such as a MIB table or a specific object in a MIB table, are identified with Object identifiers (OIDs). The OIDs are designated by text strings and integer sequences. For example, *Dell* and 1.3.6.1.4.1.674 both represent the private enterprise node *Dell*.

Figure 1 illustrates the high-level hierarchy of the Enterprise MIBs.

**Figure 1** High-Level MIB Hierarchy



The hardware MIBs are assigned under the Dell organization code, while all other MIBs are under the Aruba organization code.

Table 4 indicates the numerical string that lists the nodes of the enterprise MIB hierarchy.

**Table 4:** MIB Node Identification - Enterprise Nodes

		Name
1	1	OSI
3	1.3	ORG
6	1.3.6	DOD
1	1.3.6.1	Internet
4	1.3.6.1.4	Private
1	1.3.6.1.4.1	Enterprise
674	1.3.6.1.4.1.674	Dell

The information provided by a MIB is a file that describes network elements with numerical strings. This information is compiled into readable text by the SNMP manager. For information about reading MIB text files, see [Reading MIB Files on page 26](#).

## SNMP

MIB objects can be accessed through the Simple Network Management Protocol (SNMP). To deliver information between devices, every object referenced in an SNMP message must be listed in the MIB. A component of a device that is not described in a MIB cannot be recognized by SNMP as there is no information for SNMP managers and SNMP agents to exchange.

The significant elements of SNMP are Managers, Agents, and MIBs:

- SNMP Managers (software application) are used for communicating and managing the devices that support SNMP Agents. SNMP Managers can also be used for sending configuration updates or controlling requests to manage a network device.
- SNMP Agents (software application) provide information from the network devices to the SNMP Managers. Network devices include workstations, routers, microwave radios, and other network components.
- MIBs are used for communication between the Managers and the Agents. The OIDs of the MIBs enable the Managers and Agents to communicate specific data requests and data returns.



---

Instant MIBs support SNMPv1, SNMPv2, and SNMPv3. For information on configuring SNMP through the Instant UI, see *Dell Networking W-Series Instant Access Point 6.4.0.2-4.1 User Guide*.

---

To retrieve information from a MIB, the following information is required:

- SNMP version
- SNMP community name—*public* or *private*
- The IP Address of the virtual controller
- The OID of the MIB object

**Table 5: MIB Keywords**

Keyword	Description
<b>Sequence</b>	Refers to the sequence of objects of the MIB. This keyword is used with entry MIB objects to list the MIB objects that exchange information.
<b>Syntax</b>	Textual conventions, for example, <i>Integer32</i> .
<b>Max-Access</b>	Defines the object accessibility: <ul style="list-style-type: none"><li>• <i>read-only</i>: Can be retrieved but not modified</li><li>• <i>read-write</i>: Can be retrieved and modified</li><li>• <i>not-accessible</i>: Cannot be retrieved; it is for internal (device) use only</li><li>• <i>accessible-for-notify</i>: Can be retrieved when a trap message (notification) is sent</li></ul>
<b>Status</b>	Defines the status of the object: <ul style="list-style-type: none"><li>• <i>current</i>: Indicates that the object status is up-to-date and valid.</li><li>• <i>deprecated</i>: Indicates an obsolete definition. It permits new or continued implementation to maintain interoperability with existing implementations.</li><li>• <i>obsolete</i>: Obsolete. It should not be implemented and/or can be removed if previously implemented.</li></ul>
<b>Description</b>	A text string that describes the object.

In addition, MIB files can be placed in the appropriate disk location to assist the user in locating desired OID values for monitoring.

It is assumed that the workstation is connected to the Instant and a MIB browser is available. For most applications, the *root* of the MIB must be included in the OID—the OID begins with a decimal point as shown below.

```
.1.3.6.1.4.1.674.2.2.1.1.2.1
```

If you are using an application that is run through the Linux shell, you can use the following commands shown as examples:

- `snmpget -v1 -c <community name> <Instant IP address> <MIB OID/MIB name>`
- `snmpget -v2c -c <community name> <Instant IP address> <MIB OID/ MIB name>`
- `snmpget -v3 -c <community name> <Instant IP address> <MIB OID/ MIB name>`

The MIB objects can also be viewed from a MIB Browser GUI.



This chapter provides information on using MIBs.

- [Downloading MIB Files on page 25](#)
- [Reporting WLAN Health on page 25](#)
- [Reading MIB Files on page 26](#)
- [SNMP File on page 29](#)
- [HP OpenView on page 29](#)

## Downloading MIB Files

The latest Instant MIB files are available for registered customers at [download.dell-pcw.com](http://download.dell-pcw.com).

For assistance to set up an account and access files, contact customer service. See [Contacting Dell on page 21](#).

## Reporting WLAN Health

SNMP MIBs are frequently used for running health checks on Dell Networking W-Series Instant devices, through a MIB browser application.

To retrieve information from a MIB, the following information is required:

- SNMP version
- SNMP community name—*public* or *private*
- The IP Address of the Virtual Controller and the slave W-IAPs
- The OID of the MIB value you want to monitor

MIB files can be placed in the appropriate disk location to assist the user in locating desired OID values for monitoring. For most applications, the *root* of the MIB must be included in the OID—the OID begins with a decimal point as shown in the following example:

```
.1.3.6.1.4.1.674.2.2.1.1.2.1
```

## SNMP Operations on W-IAPs

Although the virtual controller address is configured on management station, the following MIBs are specific to a particular W-IAP and therefore cannot be accessed from the Virtual Controller.

- [ifTable](#)
- [ifXTable](#)
- [dot1qTpFdbTable](#)

To enable the management station to access the IF-MIB and Q-BRIDGE-MIB tables and W-IAPs to send traps, you must configure the IP address of each W-IAP on the management station. The management station can automatically configure the W-IAP details, by obtaining the IP address of each W-IAP from the AP MIB ([aiAccessPointTable](#)), which lists all the slave W-IAPs in a swarm and is implemented on a virtual controller.



---

You do not have to set the SNMP community string and security parameters on each W-IAP as this configuration is common to all W-IAPs and is inherited from virtual controller.

---

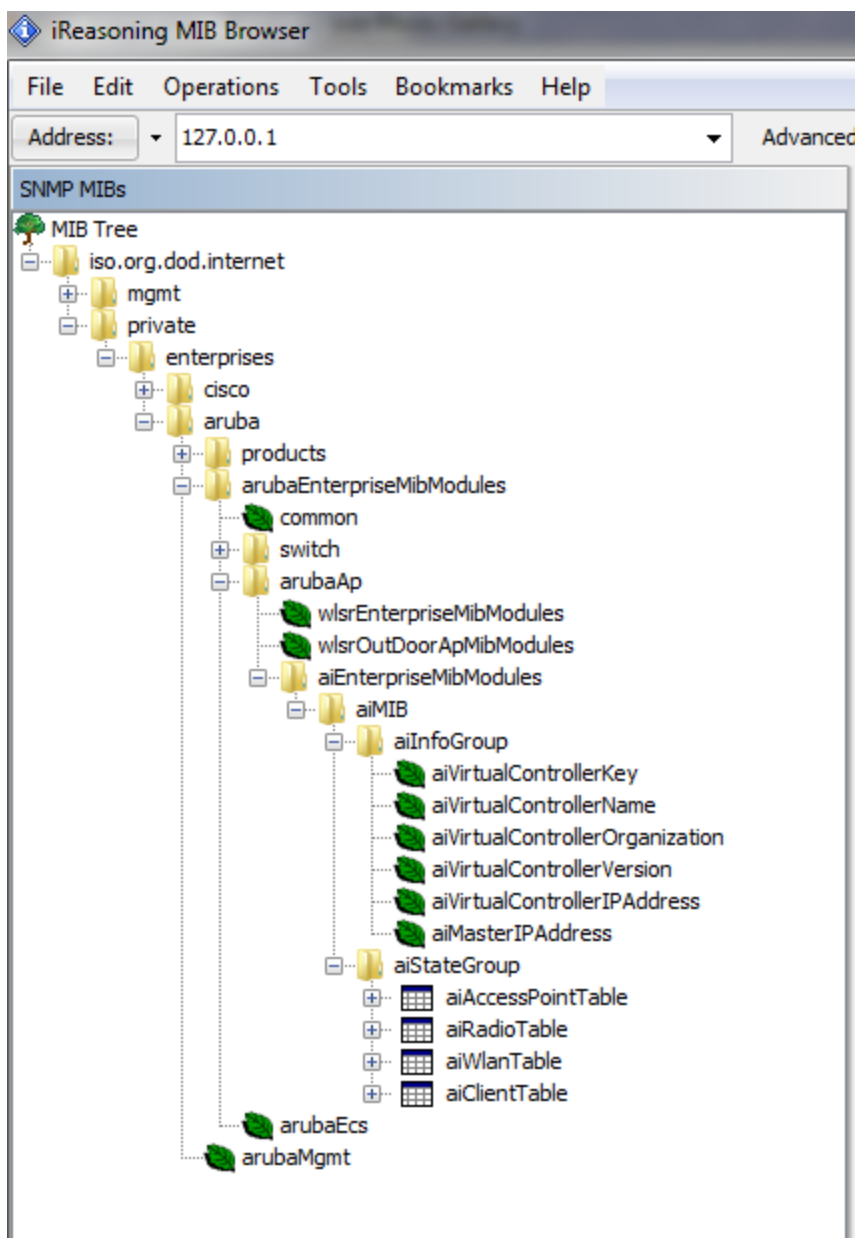
## MIB Browsers

The following is an example of `snmpget` command to obtain information.

```
[root@localhost ~]# snmpget -v 2c -c public 10.65.77.8 .1.3.6.1.4.1.14823.2.3.3.1.1.2.0
SNMPv2-SMI::enterprises.14823.2.3.3.1.1.2.0 = STRING: "Instant-CB:A5:52"
```

Figure 2 shows how information may be obtained through a graphical user interface (GUI). The user interface and the available features vary by application.

**Figure 2** *Graphical User Interface*



## Reading MIB Files

This section describes how to interpret the basic components of a MIB file. To determine the OIDs, view the file `snmp.h`. For more information, see [SNMP File](#) on page 29.

MIB files describe a specific component of a network device. The files are numerical strings that are converted to ASCII text by the compiler of the SNMP manager. A word processor or text editor can be used to open the ASCII file. The contents of an example Dell enterprise MIB file are as follows:

## Opening Line

Following is the opening line, the beginning of the MIB file.

```
AI-AP-MIB DEFINITIONS ::= BEGIN
```

## Imports

The *Imports* section lists the objects that are defined in external ASN.1 files and are used in the current MIB file.

```
IMPORTS
TEXTUAL-CONVENTION
FROM SNMPv2-TC

MODULE-IDENTITY,
OBJECT-TYPE,
snmpModules,
Integer32,
Counter32,
Counter64,
IpAddress,
NOTIFICATION-TYPE
FROM SNMPv2-SMI

DisplayString,
PhysAddress,
TimeInterval,
RowStatus,
StorageType,
TestAndIncr,
MacAddress,
TruthValue
FROM SNMPv2-TC

OBJECT-GROUP
FROM SNMPv2-CONF
aiEnterpriseMibModules
FROM ARUBA-MIB;
```

## Inheritance

This section shows the vendor of the MIB and the inheritance, and provides an overall description.

A significant part of inheritance is the OID. The entire OID is not listed for each MIB object—instead, the parent of the object is shown. The OID can be determined from the parent object as follows.

**aiEnterpriseMibModules** is the parent object—its OID is 1.3.6.1.4.1.14823.2.3.3.

**aiStateGroup OBJECT IDENTIFIER ::= { aiMIB 2 }**, the OID is 1.3.6.1.4.1.14823.2.3.3.1.2.

**aiVirtualControllerKey OBJECT-TYPE**, the OID is 1.3.6.1.4.1.14823.2.3.3.1.1.1.0.

All MIBs and their related OIDs are listed in the snmp file. For more information, see [SNMP File on page 29](#).

### aiEnterpriseMibModules

```
FROM ARUBA-MIB;
```

## Identity

Identity is the opening description of the MIB. The information includes contact information for the vendor and a general description of the MIB.

```
aiMIB MODULE-IDENTITY
    LAST-UPDATED "0804160206Z"
    ORGANIZATION "Aruba Wireless Networks"
    CONTACT-INFO
        "Postal: 1322 Crossman Avenue
        Sunnyvale, CA 94089
        E-mail: dl-support@arubanetworks.com
        Phone: +1 408 227 4500"
    DESCRIPTION
        "This MIB is for managing Dell Networking W-Series Instant WLAN"
    REVISION "0804160206Z"
    DESCRIPTION
        "The initial revision."
    ::= { aiEnterpriseMibModules 1 }
```

## MIB Modules

MIB objects can be placed in logical groups such as [Group](#) and [Table](#). A group typically contains at least one global-object or table. The table lists the MIB objects that contain the information exchanged.

The first object of a table is an [Entry](#). The OIDs of the subsequent objects of this table are appended increments of the Entry OID.

The keyword SEQUENCE lists the objects of the table that contain device information. Each subsequent object (Informative MIB Object) inherits the OID of the Entry, and contains information sorted by the Syntax, Access, Status, and Description keywords.

## Group

```
aiStateGroup OBJECT IDENTIFIER ::= { aiMIB 2 }
```

## Table

```
aiAccessPointTable OBJECT-TYPE
    SYNTAX SEQUENCE OF AiAccessPointEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "This contains all access points connected to the
        virtual controller. This table is empty on AP where
        virtual controller is not active"
    ::= { aiStateGroup 1 }
```

## Entry

```
aiAccessPointEntry OBJECT-TYPE
    SYNTAX AiAccessPointEntry
    MAX-ACCESS not-accessible
    STATUS current
```

```

DESCRIPTION
" "
INDEX { aiAPMACAddress }
 ::= { aiAccessPointTable 1 } AiAccessPointEntry ::=
SEQUENCE {
aiAPMACAddress MacAddress,
aiAPName DisplayString,
aiAPIPAddress IpAddress,
aiAPSerialNum DisplayString,
aiAPModel OBJECT IDENTIFIER,
aiAPModelName DisplayString,
aiAPCPUUtilization Integer32,
aiAPMemoryFree Integer32,
aiAPUptime TimeTicks

```

## Closing Line

Following is the closing line—the end of the MIBs file.

```
END
```

## SNMP File

The `snmp.h` file lists the OIDs of all MIBs. Following are sections from `snmp.h` that show the complete OID of each of the Controller Transport Service (CTS) MIB elements. The list starts from the ancestral parent *iso*.

The SNMP file with all Dell MIBs is listed in [Standard SNMP MIBs on page 49](#).

All Instant MIBs inherit their OIDs from the Dell MIB node. The following rows list the MIBs that precede CTS, starting from <i>iso</i> .	
{ "iso",	HASHNEXT ("1") },
{ "org",	HASHNEXT ("1.3") },
{ "dod",	HASHNEXT ("1.3.6") },
{ "internet",	HASHNEXT ("1.3.6.1") },
{ "private",	HASHNEXT ("1.3.6.1.4") },
{ "enterprises",	HASHNEXT ("1.3.6.1.4.1") },
{ "aruba",	HASHNEXT ("1.3.6.1.4.1.14823") },
{ "arubaEnterpriseMibModules",	HASHNEXT ("1.3.6.1.4.1.14823.2") },

## HP OpenView

To install the MIB module for HP OpenView, log in as the root user and execute the following script:

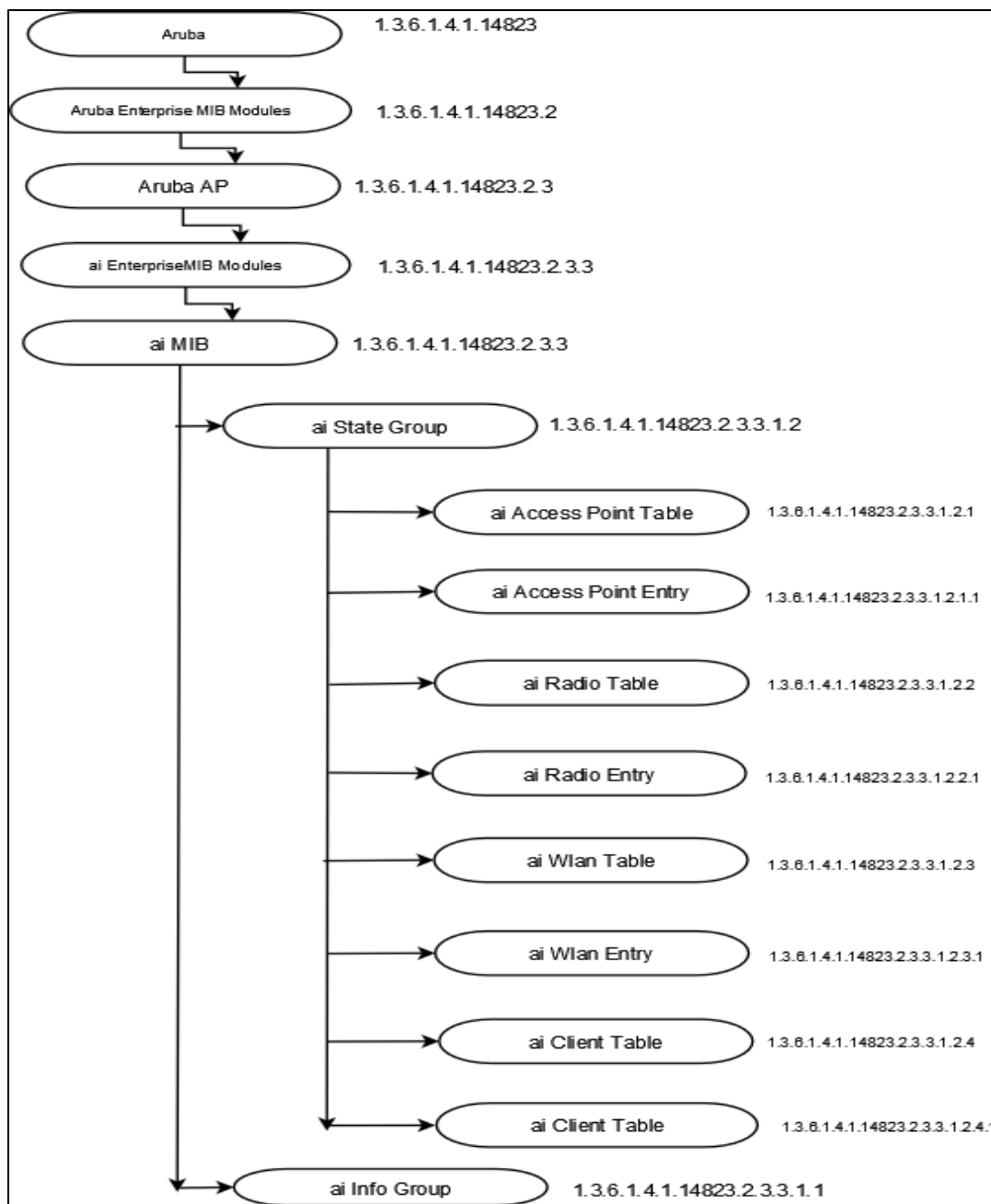
```
# $OV_CONTRIB/NNM/Aruba/install
```

This chapter provides information about the Instant MIB objects.

Figure 3 shows the architecture of the Instant MIB relative to 1.3.6.1.4.1.14823 (iso.org.dod.internet.private.enterprise.aruba).

The Instant MIB is listed in the file *aruba-instant.my*. For information about downloading the MIB file, see [Downloading MIB Files on page 25](#).

**Figure 3** MIB Hierarchy



The Instant MIB tree consists of the following MIB groups and tables.

**Table 6:** *Supported Instant MIBs and MIB Tables*

Group	Description
aiInfoGroup	Contains details of the virtual controller. For more information, see <a href="#">aiInfoGroup on page 31</a> .
aiStateGroup	<p>Contains information about status of the Access Point, Radio, WLAN, and Clients connected to a W-IAP. The following tables are available in the aiInfoGroup:</p> <ul style="list-style-type: none"> <li>● <b>aiAccessPointTable</b>—Contains all the access points connected to the virtual controller. This table is indexed by the MAC Address of the W-IAP.</li> <li>● <b>aiRadioTable</b>—Contains all the radios of the access points connected to the virtual controller. This table is indexed by the MAC Address and radio number.</li> <li>● <b>aiWlanTable</b>—Contains all the BSSIDs that are active on the virtual controller. This table is indexed by the MAC address and a WLAN Index of the W-IAP.</li> <li>● <b>aiClientTable</b>—Contains information about all the clients connected to the virtual controller. When a client roams from one access point to another, all the counters in this table are reset to 0.</li> </ul> <p>For more information, see <a href="#">aiStateGroup on page 33</a>.</p>
aiTrapGroup	Contains the details of traps that can be generated on a W-IAP. For more information, see <a href="#">Trap Hierarchy on page 63</a> .

## aiInfoGroup

The aiInfoGroup table provides information about the virtual controller:

- aiVirtualControllerKey
- aiVirtualControllerName
- aiVirtualControllerOrganization
- aiVirtualControllerVersion
- aiVirtualControllerIPAddress
- aiMasterIPAddress

### aiVirtualControllerKey

<b>Object ID</b>	1.3.6.1.4.1.14823.2.3.3.1.1.1
<b>Syntax</b>	DisplayString
<b>Max-Access</b>	Read-only
<b>Status</b>	Current
<b>Description</b>	Unique Virtual Controller key

## aiVirtualControllerName

<b>Object ID</b>	1.3.6.1.4.1.14823.2.3.3.1.1.2
<b>Syntax</b>	DisplayString
<b>Max-Access</b>	Read-only
<b>Status</b>	Current
<b>Description</b>	Name of the Virtual Controller

## aiVirtualControllerOrganization

<b>Object ID</b>	1.3.6.1.4.1.14823.2.3.3.1.1.3
<b>Syntax</b>	DisplayString
<b>Max-Access</b>	Read-only
<b>Status</b>	Current
<b>Description</b>	Virtual Controller organization

## aiVirtualControllerVersion

<b>Object ID</b>	1.3.6.1.4.1.14823.2.3.3.1.1.4
<b>Syntax</b>	DisplayString
<b>Max-Access</b>	Read-only
<b>Status</b>	Current
<b>Description</b>	Software version of the Virtual Controller

## aiVirtualControllerIPAddress

<b>Object ID</b>	1.3.6.1.4.1.14823.2.3.3.1.1.5
<b>Syntax</b>	IPAddress
<b>Max-Access</b>	Read-only
<b>Status</b>	Current
<b>Description</b>	IP address of the Virtual Controller. If this is not set, returns 0.0.0.0.



## aiMasterIPAddress

<b>Object ID</b>	1.3.6.1.4.1.14823.2.3.3.1.1.6
<b>Syntax</b>	IPAddress
<b>Max-Access</b>	Read-only
<b>Status</b>	Current
<b>Description</b>	IP address of the master W-IAP.

## aiStateGroup

The aiStateGroup contains the following tables:

- [aiAccessPointTable](#)
- [aiRadioTable](#)
- [aiWlanTable](#)
- [aiClientTable](#)

## aiAccessPointTable

The objects of the **aiAccessPointTable** provide information about all the W-IAPs connected to the virtual controller.

**Table 7:** *aiAccessPointTable OIDs*

Object	Object ID	Entry OID
<a href="#">aiAccessPointEntry</a>	1.3.6.1.4.1.14823.2.3.3.1.2.1.1	aiAccessPointTable 1
<a href="#">aiAPMACAddress</a>	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.1	aiAccessPointEntry 1
<a href="#">aiAPName</a>	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.2	aiAccessPointEntry 2
<a href="#">aiAPIPAddress</a>	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.3	aiAccessPointEntry 3
<a href="#">aiAPSerialNum</a>	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.4	aiAccessPointEntry 4
<a href="#">aiAPModel</a>	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.5	aiAccessPointEntry 5
<a href="#">aiAPModelName</a>	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.6	aiAccessPointEntry 6
<a href="#">aiAPCPUUtilization</a>	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.7	aiAccessPointEntry 7
<a href="#">aiAPMemoryFree</a>	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.8	aiAccessPointEntry 8
<a href="#">aiAPUptime</a>	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.9	aiAccessPointEntry 9
<a href="#">aiAPTtotalMemory</a>	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.10	aiAccessPointEntry 10
<a href="#">aiAPStatus</a>	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.11	aiAccessPointEntry 11

## aiAccessPointEntry

<b>Syntax</b>	aiAccessPointEntry
<b>Max-Access</b>	not-accessible
<b>Status</b>	current
<b>Description</b>	NA
<b>Index</b>	aiAPMACAddress

## aiAPMACAddress

<b>Syntax</b>	MacAddress (OCTET STRING). Hint: 1x:
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	MAC address of the Access Point.

## aiAPName

<b>Syntax</b>	DisplayString (SIZE(0..64))
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Name of the Access Point.

## aiAPIPAddress

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	IP address of the Access Point.

## aiAPSerialNum

<b>Syntax</b>	DisplayString (SIZE(0..64))
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Serial number of the Access Point.

## aiAPModel

<b>Syntax</b>	OBJECT IDENTIFIER
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	AP model

## aiAPModelName

<b>Syntax</b>	DisplayString (SIZE(0..32))
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Model name of the Access Point.

## aiAPCPUUtilization

<b>Syntax</b>	Integer32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	CPU utilization of the Access Point.

## aiAPMemoryFree

<b>Syntax</b>	Integer32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Amount of memory free in the access point in bytes.

## aiAPUptime

<b>Syntax</b>	TimeTicks
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Uptime of the Access Point.

## aiAPTtotalMemory

<b>Syntax</b>	Integer32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Total amount of memory available in the AP in bytes.

## aiAPStatus

<b>Syntax</b>	Integer {up(1), down(2)}
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Indicates the Access Point Status.

## aiRadioTable

The objects of the aiRadioTable provide information about all the radios and the related information of the Access Points.

**Table 8:** aiRadioTable OIDs

Object	Object ID	Entry OID
aiRadioEntry	1.3.6.1.4.1.14823.2.3.3.1.2.2.1	aiRadioTable 1
aiRadioAPMacAddress	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.1	aiRadioEntry 1
aiRadioIndex	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.2	aiRadioEntry 2
aiRadioMACAddress	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.3	aiRadioEntry 3
aiRadioChannel	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.4	aiRadioEntry 4
aiRadioTransmitPower	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.5	aiRadioEntry 5
aiRadioNoiseFloor	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.6	aiRadioEntry 6
aiRadioUtilization4	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.7	aiRadioEntry 7
aiRadioUtilization64	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.8	aiRadioEntry 8
aiRadioTxTotalFrames	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.9	aiRadioEntry 9
aiRadioTxMgmtFrames	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.10	aiRadioEntry 10
aiRadioTxDataFrames	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.11	aiRadioEntry 11
aiRadioTxDataBytes	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.12	aiRadioEntry 12
aiRadioTxDrops	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.13	aiRadioEntry 13

Object	Object ID	Entry OID
aiRadioTxTotalFrames	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.14	aiRadioEntry 14
aiRadioRxDataFrames	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.15	aiRadioEntry 15
aiRadioRxDataBytes	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.16	aiRadioEntry 16
aiRadioRxMgmtFrames	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.17	aiRadioEntry 17
aiRadioRxBad	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.18	aiRadioEntry 18
aiRadioPhyEvents	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.19	aiRadioEntry 19
aiRadioStatus	1.3.6.1.4.1.14823.2.3.3.1.2.2.1.20	aiRadioEntry 20

## aiRadioEntry

<b>Syntax</b>	aiRadioEntry
<b>Max-Access</b>	not-accessible
<b>Status</b>	current
<b>Description</b>	NA
<b>Index</b>	aiRadioAPMACAddress, aiRadioIndex

## aiRadioAPMacAddress

<b>Syntax</b>	MacAddress (OCTET STRING). Hint: 1x:
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	MAC Address of the Access Point where this radio is active.

## aiRadioIndex

<b>Syntax</b>	Integer32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Radio number of the Access Point.

## aiRadioMACAddress

<b>Syntax</b>	MacAddress
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Radio MAC address of the Access Point.

## aiRadioChannel

**Syntax** Integer32

**Max-Access** read-only

**Status** current

**Description** Radio channel. The first byte contains primary channel and first two bits of second byte contains indicator for the secondary channel. If first two bits of second byte are 0, it is a 20MHz channel. If first two bits of second byte are 01, the secondary channel is above primary channel, if first two bits of second byte are 10, the secondary channel is below the primary channel.

## aiRadioTransmitPower

**Syntax** Integer32

**Max-Access** read-only

**Status** current

**Description** Radio transmission power of the Access Point.

## aiRadioNoiseFloor

**Syntax** Integer32

**Max-Access** read-only

**Status** current

**Description** Radio noise of the Access Point in dBm.

## aiRadioUtilization4

**Syntax** Integer32

**Max-Access** read-only

**Status** current

**Description** Radio channel utilization 4 second average.

## aiRadioUtilization64

**Syntax** Integer32

**Max-Access** read-only

**Status** current

**Description** Radio channel utilization 64 second average.

### aiRadioTxTotalFrames

<b>Syntax</b>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Total number of frames transmitted.

### aiRadioTxMgmtFrames

<b>Syntax</b>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Total number of management frames transmitted.

### aiRadioTxDataFrames

<b>Syntax</b>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Total number of data frames transmitted.

### aiRadioTxDataBytes

<b>Syntax</b>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Total number of data bytes transmitted.

### aiRadioTxDrops

<b>Syntax</b>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Total number of frames dropped during transmission.

### aiRadioRxTotalFrames

<b>Syntax</b>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Total number of received frames.

### aiRadioRxDataFrames

<b>Syntax</b>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Total number of received data frames.

### aiRadioRxDataBytes

<b>Syntax</b>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Total number of received data bytes.

### aiRadioRxMgmtFrames

<b>Syntax</b>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Total number of received management frames.

### aiRadioRxBad

<b>Syntax</b>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Total number of frames received in error.



## aiRadioPhyEvents

<b>Syntax</b>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Number of physical layer events that indicates frames not received because of interference.

## aiRadioStatus

<b>Syntax</b>	Integer {up(1), down(2)}
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Indicates the radio status of the AP.

## aiWlanTable

The objects of the aiWlanTable provide information about all the BSSIDs active on the virtual controller.

**Table 9:** aiWlanTable OIDs

Object	Object ID	Entry OID
aiWlanEntry	1.3.6.1.4.1.14823.2.3.3.1.2.3.1	aiWlanTable 1
aiWlanAPMACAddress	1.3.6.1.4.1.14823.2.3.3.1.2.3.1.1	aiWlanEntry 1
aiWlanIndex	1.3.6.1.4.1.14823.2.3.3.1.2.3.1.2	aiWlanEntry 2
aiWlanESSID	1.3.6.1.4.1.14823.2.3.3.1.2.3.1.3	aiWlanEntry 3
aiWlanMACAddress	1.3.6.1.4.1.14823.2.3.3.1.2.3.1.4	aiWlanEntry 4
aiWlanTxTotalFrames	1.3.6.1.4.1.14823.2.3.3.1.2.3.1.5	aiWlanEntry 5
aiWlanTxDataFrames	1.3.6.1.4.1.14823.2.3.3.1.2.3.1.6	aiWlanEntry 6
aiWlanTxDataBytes	1.3.6.1.4.1.14823.2.3.3.1.2.3.1.7	aiWlanEntry 7
aiWlanRxTotalFrames	1.3.6.1.4.1.14823.2.3.3.1.2.3.1.8	aiWlanEntry 8
aiWlanRxDataFrames	1.3.6.1.4.1.14823.2.3.3.1.2.3.1.9	aiWlanEntry 9
aiWlanRxDataBytes	1.3.6.1.4.1.14823.2.3.3.1.2.3.1.10	aiWlanEntry 10

## aiWlanEntry

<b>Syntax</b>	AiWlanEntry
<b>Max-Access</b>	not-accessible
<b>Status</b>	current
<b>Description</b>	NA
<b>Index</b>	aiWlanAPMACAddress, aiWlanIndex

## aiWlanAPMACAddress

<b>Syntax</b>	MacAddress (OCTET STRING). Hint: 1x:
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	MAC Address of the Access Point where WLAN is active.

## aiWlanIndex

<b>Syntax</b>	Integer32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Index of the WLAN. This is a unique index assigned to the active WLAN on the Access Point.

## aiWlanESSID

<b>Syntax</b>	DisplayString
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	ESSID of the WLAN

## aiWlanMACAddress

<b>Syntax</b>	MacAddress (OCTET STRING). Hint: 1x:
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	BSSID of the WLAN

### aiWlanTxTotalFrames

<b>Syntax</b>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Total number of frames transmitted.

### aiWlanTxDataFrames

<b>Syntax</b>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Total number of data frames transmitted.

### aiWlanTxDataBytes

<b>Syntax</b>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Total number of data bytes transmitted.

### aiWlanRxTotalFrames

<b>Syntax</b>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Total number of received frames.

### aiWlanRxDataFrames

<b>Syntax</b>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Total number of received data frames.

## aiWlanRxDataBytes

<b>Syntax</b>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Total number of received data bytes.

## aiClientTable

The objects of the aiWlanTable provide information about all the clients connected to the virtual controller.

**Table 10:** aiClientTable OID

Object	Object ID	Entry OID
aiClientEntry	1.3.6.1.4.1.14823.2.3.3.1.2.4.1	aiClientTable 1
aiClientMACAddress	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.1	aiClientEntry 1
aiClientWlanMACAddress	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.2	aiClientEntry 2
aiClientIPAddress	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.3	aiClientEntry 3
aiClientAPIPAddress	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.4	aiClientEntry 4
aiClientName	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.5	aiClientEntry 5
aiClientOperatingSystem	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.6	aiClientEntry 6
aiClientSNR	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.7	aiClientEntry 7
aiClientTxDataFrames	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.8	aiClientEntry 8
aiClientTxDataBytes	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.9	aiClientEntry 9
aiClientTxRetries	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.10	aiClientEntry 10
aiClientTxRate	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.11	aiClientEntry 11
aiClientRxDataFrames	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.12	aiClientEntry 12
aiClientRxDataBytes	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.13	aiClientEntry 13
aiClientRxRetries	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.14	aiClientEntry 14
aiStateGroup	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.15	aiClientEntry 15
aiClientUptime	1.3.6.1.4.1.14823.2.3.3.1.2.4.1.16	aiClientEntry 16

## aiClientEntry

<b>Syntax</b>	aiClientEntry
<b>Max-Access</b>	not-accessible
<b>Status</b>	current
<b>Description</b>	NA
<b>Index</b>	aiClientMACAddress

## aiClientMACAddress

<b>Syntax</b>	MacAddress (OCTET STRING). Hint: 1x:
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	MAC Address of the client.

## aiClientWlanMACAddress

<b>Syntax</b>	MacAddress
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	BSSID of WLAN where client is associated.

## aiClientIPAddress

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	IP address of the client.

## aiClientAPIPAddress

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Radio channel. First byte contains primary channel and first two bits on second byte contains indicator for secondary channel. If first two bits of second byte is 0, it is a 20MHz channel. If first two bits of second byte is 01, secondary channel is above primary channel, if first two bits of second by is 10, secondary channel is below the primary channel.

## aiClientName

<b>Syntax</b>	
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Name of the user using the client.

## aiClientOperatingSystem

<b>Syntax</b>	
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Operating system of the client.

## aiClientSNR

<b>Syntax</b>	
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Signal to noise ratio of the client connected to the Access Point

## aiClientTxDataFrames

<b>Syntax</b>	
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Total number of frames transmitted by the client.

## aiClientTxDataBytes

<b>Syntax</b>	
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Total number of bytes transmitted by the client.

### aiClientTxRetries

<b>Syntax</b>	
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Total number of retry frames transmitted by the client.

### aiClientTxRate

<b>Syntax</b>	Integer32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Transmission rate of the client in mbps.

### aiClientRxDataFrames

<b>Syntax</b>	
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Total number of frames received by the client in mbps.

### aiClientRxDataBytes

<b>Syntax</b>	
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Total number of bytes received by the client in mbps.

### aiClientRxRetries

<b>Syntax</b>	
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Total number of retry frames received by the client.

## aiClientRxRate

<b>Syntax</b>	
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Receiving rate of the client in mbps.

## aiClientUptime

<b>Syntax</b>	TimeTicks
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Client uptime. On mobility event all counters are reset to 0 and uptime resets to 0.



This chapter provides information on the following standard MIBs modules and tables supported in this release of Instant.

- System MIB
- dot1qTpFdbTable
- ifTable
- ifXTable

## System MIB

The system MIB contains system-specific information about the W-IAP. The following system MIB objects are supported:

- **sysDescr**— Provides information on the W-IAP model and software version of the W-IAP.
- **sysObjectID**— Identifies the network management subsystem. The sysObjectID in the standard SNMP MIB can be used to retrieve OIDs for the W-IAPs. You can retrieve information on all node devices in the MIB file by extracting the sysObjectId for each device.

The sysObjectID returns OIDs for a specific model number of the device within the W-IAP product family. When an SNMP query is performed for this object on an AP IP address (either master W-IAP or slave W-IAP IP address), the AP type information is retrieved. However, if the query is performed on a Virtual Controller IP address, information on the W-IAP acting as the Virtual Controller is displayed.

For example, if a W-IAP135 is the master W-IAP, a query on this W-IAP returns the *iso.org.dod.internet.private.enterprise.aruba.products.apProducts.ap135* (1.3.6.1.4.1.14823.1.2.48) result. Similarly, a query on the Virtual Controller IP returns the OID details with **iapvc**.

- **sysUpTime**— Indicates the system up time since the W-IAP was initialized and actively connected to the network.
- **sysName**— Indicates the name of the W-IAP.
- **sysLocation**— Indicates the physical location of the W-IAP. To retrieve information on the AP location, the system location details for the W-IAP must be configured. For more information on configuring system location details, see Dell Networking W-Series Instant 6.4.0.2-4.1 *Access Point User Guide*.
- **sysServices**— Indicates the services offered by the W-IAP.

The following system MIB objects are not supported:

- sysContact
- sysORLastChange
- sysORTable

## sysDescr

<b>Object ID</b>	1.3.6.1.2.1.1.1
<b>Syntax</b>	DisplayString
<b>Max-Access</b>	read-only
<b>Status</b>	mandatory
<b>Description</b>	A textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software. It is mandatory that this only contains printable ASCII characters.

## sysObjectID

<b>Object ID</b>	1.3.6.1.2.1.1.2
<b>Syntax</b>	Object Identifier
<b>Max-Access</b>	read-only
<b>Status</b>	mandatory
<b>Description</b>	The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining 'what kind of box' is being managed.

## sysUpTime

<b>Object ID</b>	1.3.6.1.2.1.1.3
<b>Syntax</b>	TimeTicks
<b>Max-Access</b>	read-only
<b>Status</b>	mandatory
<b>Description</b>	The time (in hundredths of a second) since the network management portion of the system was last re-initialized.

## sysName

<b>Object ID</b>	1.3.6.1.2.1.1.5
<b>Syntax</b>	DisplayString
<b>Max-Access</b>	read-write
<b>Status</b>	mandatory
<b>Description</b>	An administrator-assigned fully-qualified domain name for the managed node.

## sysLocation

<b>Object ID</b>	1.3.6.1.2.1.1.6
<b>Syntax</b>	DisplayString
<b>Max-Access</b>	read-write
<b>Status</b>	mandatory
<b>Description</b>	System location of the W-IAP cluster

## sysServices

<b>Object ID</b>	1.3.6.1.2.1.1.7
<b>Syntax</b>	Integer
<b>Max-Access</b>	read-only
<b>Status</b>	mandatory
<b>Description</b>	A value which indicates the set of services that the AP primarily offers.

## dot1qTpFdbTable

This table contains information about the associated station MAC addresses, the corresponding port from the interface table, and status. The objects of the dot1qTpFdbTable provide information about the forwarding and filtering status of the clients connected to wired ports and wireless interfaces.

The dot1qTpFdbTable contains the following objects:

- [dot1qFdbId](#)
- [dot1qTpFdbAddress](#)
- [dot1qTpFdbPort](#)
- [dot1qTpFdbStatus](#)

## dot1qFdbId

<b>Object ID</b>	1.3.6.1.2.1.17.7.1.2.1.1.1
<b>Syntax</b>	UNSIGNED32
<b>Max-Access</b>	not-accessible
<b>Status</b>	current
<b>Description</b>	The identity of the filtering database such as VLAN ID of the AP.

## dot1qTpFdbAddress

<b>Object ID</b>	1.3.6.1.2.1.17.7.1.2.2.1.1
<b>Syntax</b>	MacAddress
<b>Max-Access</b>	not-accessible
<b>Status</b>	current
<b>Description</b>	MAC address for which the AP has forwarding or filtering information.

## dot1qTpFdbPort

<b>Object ID</b>	1.3.6.1.2.1.17.7.1.2.2.1.2
<b>Syntax</b>	Integer32 (0..65535)
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Port number on which a frame having a source address equal to the value of the corresponding instance of dot1qTpFdbAddress. The index value of ifTable is set as the port number field in this table. If the self MAC address is used, the index is 0.

## dot1qTpFdbStatus

<b>Object ID</b>	1.3.6.1.2.1.17.7.1.2.2.1.3
<b>Syntax</b>	INTEGER { other(1), invalid(2), learned(3), self(4), mgmt(5) }
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	The status of the bridge entry is set as learned to indicate that the value of the corresponding instance of dot1qTpFdbPort was learned and is being used. If self MAC address is used, the status is set as self to indicate that the value of the corresponding instance of dot1qTpFdbAddress represents one of the device's addresses. The corresponding instance of dot1qTpFdbPort indicates which of the device's ports has this address.

## ifTable

This table contains information about wired ports and wireless interfaces. The objects in this MIB provide information about the interfaces configured on a W-IAP. This table contains the following objects:

- [ifIndex](#)
- [ifDescr](#)
- [ifType](#)
- [ifMtu](#)
- [ifSpeed](#)
- [ifPhysAddress](#)

- ifAdminStatus
- ifOperStatus
- ifInOctets
- ifInUcastPkts
- ifInNUcastPkts
- ifInDiscards
- ifInErrors
- ifOutOctets
- ifOutUcastPkts
- ifInDiscards
- ifInErrors

The following ifTable objects are not supported:

- ifOutQLen
- ifSpecific
- ifInUnknownProtos
- ifLastChange

## ifIndex

<b>Object ID</b>	1.3.6.1.2.1.2.2.1.1
<b>Syntax</b>	Integer32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	<p>Value assigned to an interface.</p> <ul style="list-style-type: none"> <li>• Ethernet interface value range: 1–49</li> <li>• Radio 0 interface value range: 50–69.</li> <li>• Radio 1 interface range: 70–89.</li> <li>• GRE interface range: 90–09</li> <li>• PPP interface range: 110–129</li> <li>• VPN interface range: 130–150</li> <li>• Other interfaces: From 500 onwards</li> </ul>

## ifDescr

<b>Object ID</b>	1.3.6.1.2.1.2.2.1.2
<b>Syntax</b>	DisplayString (size (0..255))
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	<p>Description of the interface, for example eth for Ethernet, radio0_ssid_id2,aruba102 for Radio0 interface, and radioX_ssid_idY for Radio1 interface.</p>

## ifType

<b>Object ID</b>	1.3.6.1.2.1.2.2.1.3
<b>Syntax</b>	IANAifType
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Type of the interface. For example, Gigabit Ethernet interface or Fast Ethernet.

## ifMtu

<b>Object ID</b>	1.3.6.1.2.1.2.2.1.4
<b>Syntax</b>	Integer32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	The size of the largest packet which can be sent or received on interface.

## ifSpeed

<b>Object ID</b>	1.3.6.1.2.1.2.2.1.5
<b>Syntax</b>	Gauge32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	The current bandwidth of the interface in bits per second.

## ifPhysAddress

<b>Object ID</b>	1.3.6.1.2.1.2.2.1.6
<b>Syntax</b>	PhysAddress
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Indicates the MAC address of the client.

## ifAdminStatus

<b>Object ID</b>	1.3.6.1.2.1.2.2.1.7
<b>Syntax</b>	INTEGER
<b>Max-Access</b>	read-write
<b>Status</b>	current
<b>Description</b>	Administrative state of the interface.

## ifOperStatus

<b>Object ID</b>	1.3.6.1.2.1.2.2.1.8
<b>Syntax</b>	INTEGER
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Operational status of the interface.

## ifInOctets

<b>Object ID</b>	1.3.6.1.2.1.2.2.1.10
<b>Syntax</b>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Number of octets received on the interface.

## ifInUcastPkts

<b>Object ID</b>	1.3.6.1.2.1.2.2.1.11
<b>Syntax</b>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	The number of packets, delivered by this sub-layer to a higher sub-layer, which were not addressed to a multicast or broadcast address at this sub-layer.

## ifInNUcastPkts

<b>Object ID</b>	1.3.6.1.2.1.2.2.1.12
<b>Syntax</b>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	The number of packets, delivered by this sub-layer to a higher sub-layer, which were addressed to a multicast or broadcast address at this sub-layer.

## ifInDiscards

<b>Object ID</b>	1.3.6.1.2.1.2.2.1.13
<b>Syntax</b>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	The number of inbound packets discarded.

## ifInErrors

<b>Object ID</b>	1.3.6.1.2.1.2.2.1.14
<b>Syntax</b>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	The number of packets transmission units with errors.

## ifOutOctets

<b>Object ID</b>	1.3.6.1.2.1.2.2.1.16
<b>Syntax</b>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	The total number of octets transmitted out of the interface.



## ifOutUcastPkts

<b>Object ID</b>	1.3.6.1.2.1.2.2.1.17
<b>Syntax</b>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	The total number of packets that the higher-level protocols request for transmission, and the packets which are not addressed to a multicast or broadcast address at this sub-layer, including those that are discarded or not sent.

## ifOutDiscards

<b>Object ID</b>	1.3.6.1.2.1.2.2.1.19
<b>Syntax</b>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	The number of outbound packets discarded even though no errors that prevented the transmission were detected.

## ifOutErrors

<b>Object ID</b>	1.3.6.1.2.1.2.2.1.20
<b>Syntax</b>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	The number of outbound packets that could not be transmitted because of errors.

## ifXTable

The ifXTable table contains the following additional objects for the interface table.

- [ifName](#)
- [ifInMulticastPkts](#)
- [ifInBroadcastPkts](#)
- [ifOutMulticastPkts](#)
- [ifOutBroadcastPkts](#)
- [ifHCInOctets](#)
- [ifHCInUcastPkts](#)
- [ifHCInMulticastPkts](#)
- [ifHCInBroadcastPkts](#)

- ifHCOctets
- ifHCOUcastPkts
- ifHCOmulticastPkts
- ifHCObroadcastPkts
- ifLinkUpDownTrapEnable
- ifPromiscuousMode
- ifConnectorPresent

The following ifXTable objects are not supported:

- ifHighSpeed
- ifAlias
- ifCounterDiscontinuityTime

## ifName

<b>Object ID</b>	1.3.6.1.2.1.31.1.1.1.1
<b>Syntax</b>	DisplayString
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Name of the interface

## ifInMulticastPkts

<b>Object ID</b>	1.3.6.1.2.1.31.1.1.1.2
<b>Syntax</b>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	The number of packets, delivered by this sub-layer to a higher layer, which were addressed to a multicast or broadcast address at this sub-layer.

## ifInBroadcastPkts

<b>Object ID</b>	1.3.6.1.2.1.31.1.1.1.3
<b>Syntax</b>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	The number of packets, delivered by this sub-layer to a higher layer, which were addressed to a multicast or broadcast address at this sub-layer

## ifOutMulticastPkts

<b>Object ID</b>	1.3.6.1.2.1.31.1.1.1.4
<b>Syntax</b>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	The total number of packets that the higher-level protocols request for transmission, and which were addressed to a multicast or broadcast address at this sub-layer.

## ifOutBroadcastPkts

<b>Object ID</b>	1.3.6.1.2.1.31.1.1.1.5
<b>Syntax</b>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	The total number of packets that higher-level protocols requested for transmission, and the packets which were addressed to a multicast or broadcast address at this sub-layer.

## ifHCInOctets

<b>Object ID</b>	1.3.6.1.2.1.31.1.1.1.6
<b>Syntax</b>	Counter64
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	The total number of octets received on the interface, including framing characters. This object is a 64-bit version of ifInOctets.

## ifHCInUcastPkts

<b>Object ID</b>	1.3.6.1.2.1.31.1.1.1.7
<b>Syntax</b>	Counter64
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	The number of packets, delivered by this sub-layer to a higher sub-layer, which were not addressed to a multicast or broadcast address at this sub-layer.

## ifHCInMulticastPkts

<b>Object ID</b>	1.3.6.1.2.1.31.1.1.1.8
<b>Syntax</b>	Counter64
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	The number of packets, delivered by this sub-layer to a higher sub-layer, which were addressed to a multicast or broadcast address at this sub-layer.

## ifHCInBroadcastPkts

<b>Object ID</b>	1.3.6.1.2.1.31.1.1.1.9
<b>Syntax</b>	Counter64
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	The number of packets, delivered by this sub-layer to a higher sub-layer, which were addressed to a multicast or broadcast address at this sub-layer.

## ifHCOctets

<b>Object ID</b>	1.3.6.1.2.1.31.1.1.1.10
<b>Syntax</b>	Counter64
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	The total number of octets transmitted out of the interface, including framing characters.

## ifHCOUcastPkts

<b>Object ID</b>	1.3.6.1.2.1.31.1.1.1.11
<b>Syntax</b>	Counter64
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.

## ifHCOmulticastPkts

<b>Object ID</b>	1.3.6.1.2.1.31.1.1.1.12
<b>Syntax</b>	Counter64
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.

## ifHCObroadcastPkts

<b>Object ID</b>	1.3.6.1.2.1.31.1.1.1.13
<b>Syntax</b>	Counter64
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.

## ifLinkUpDownTrapEnable

<b>Object ID</b>	1.3.6.1.2.1.31.1.1.1.14
<b>Syntax</b>	Integer
<b>Max-Access</b>	read-write
<b>Status</b>	current
<b>Description</b>	Indicates whether linkUp or linkDown traps must be generated for this interface.

## ifPromiscuousMode

<b>Object ID</b>	1.3.6.1.2.1.31.1.1.1.16
<b>Syntax</b>	Integer
<b>Max-Access</b>	TruthValue
<b>Status</b>	current
<b>Description</b>	This object has true (1) and false(2) values.

## ifConnectorPresent

<b>Object ID</b>	1.3.6.1.2.1.31.1.1.1.17
<b>Syntax</b>	Integer
<b>Max-Access</b>	TruthValue
<b>Status</b>	current
<b>Description</b>	This object has True(1) value if there is any physical connector, else false (0) value.

This chapter defines the traps that can be generated by the W-IAP. Traps are MIB objects (variables) that transmit information to the SNMP Manager when an event occurs. Traps are included as varbinds (variable bindings) in the trap protocol data unit (PDU).

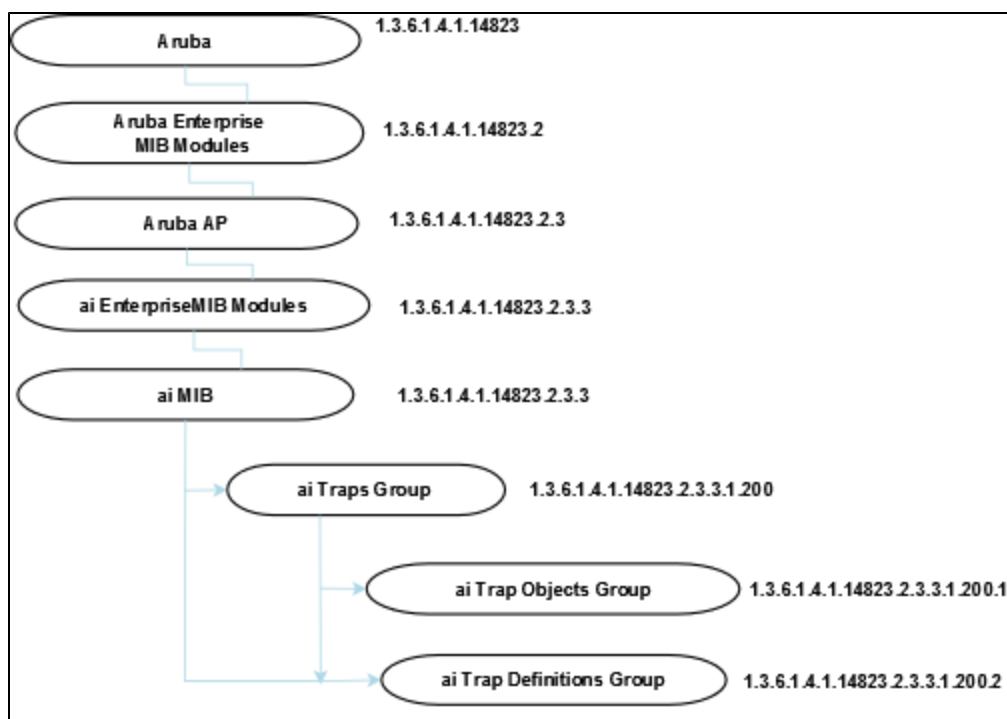


The traps for the W-IAP cluster are generated with the master W-IAP IP address as the source IP address. If the Virtual Controller IP is configured, the traps are generated from the Virtual Controller IP. However, the source IP address for the interface up and interface down traps is AP IP address.

Figure 4 shows the architecture of the Traps MIB relative to 1.3.6.1.4.1.14823 (iso.org.dod.internet.private.enterprise.aruba). The Traps are listed in the file *aruba-trap.my* MIB file. For information about downloading Instant MIB files, see [Downloading MIB Files on page 25](#).

## Trap Hierarchy

Figure 4 Trap Hierarchy



The following table lists the supported trap objects in this group:

**Table 11:** *aiTraps Objects Group OIDs*

Object	Object ID	
wlsxTrapAPMacAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.1	wlsxTrapObjectsGroup 1
wlsxTrapAPIpAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.2	wlsxTrapObjectsGroup 2
wlsxTrapAPBSSID	1.3.6.1.4.1.14823.2.3.3.1.200.1.3	wlsxTrapObjectsGroup 3
wlsxTrapEssid	1.3.6.1.4.1.14823.2.3.3.1.200.1.4	wlsxTrapObjectsGroup 4
wlsxTrapTargetAPBSSID	1.3.6.1.4.1.14823.2.3.3.1.200.1.5	wlsxTrapObjectsGroup 5
wlsxTrapTargetAPSSID	1.3.6.1.4.1.14823.2.3.3.1.200.1.6	wlsxTrapObjectsGroup 6
wlsxTrapTargetAPChannel	1.3.6.1.4.1.14823.2.3.3.1.200.1.7	wlsxTrapObjectsGroup 7
wlsxTrapNodeMac	1.3.6.1.4.1.14823.2.3.3.1.200.1.8	wlsxTrapObjectsGroup 8
wlsxTrapSourceMac	1.3.6.1.4.1.14823.2.3.3.1.200.1.9	wlsxTrapObjectsGroup 9
wlsxReceiverMac	1.3.6.1.4.1.14823.2.3.3.1.200.1.10	wlsxTrapObjectsGroup 10
wlsxTrapTransmitterMac	1.3.6.1.4.1.14823.2.3.3.1.200.1.11	wlsxTrapObjectsGroup 11
wlsxTrapReceiverMac	1.3.6.1.4.1.14823.2.3.3.1.200.1.12	wlsxTrapObjectsGroup 12
wlsxTrapSnr	1.3.6.1.4.1.14823.2.3.3.1.200.1.13	wlsxTrapObjectsGroup 13
wlsxTrapSignatureName	1.3.6.1.4.1.14823.2.3.3.1.200.1.14	wlsxTrapObjectsGroup 14
wlsxTrapFrameType	1.3.6.1.4.1.14823.2.3.3.1.200.1.15	wlsxTrapObjectsGroup 15
wlsxTrapAddressType	1.3.6.1.4.1.14823.2.3.3.1.200.1.16	wlsxTrapObjectsGroup 16
wlsxTrapAPLocation	1.3.6.1.4.1.14823.2.3.3.1.200.1.17	wlsxTrapObjectsGroup 17
wlsxTrapAPChannel	1.3.6.1.4.1.14823.2.3.3.1.200.1.18	wlsxTrapObjectsGroup 18
wlsxTrapAPTxFPower	1.3.6.1.4.1.14823.2.3.3.1.200.1.19	wlsxTrapObjectsGroup 19
wlsxTrapMatchedMac	1.3.6.1.4.1.14823.2.3.3.1.200.1.20	wlsxTrapObjectsGroup 20
wlsxTrapMatchedIp	1.3.6.1.4.1.14823.2.3.3.1.200.1.21	wlsxTrapObjectsGroup 21
wlsxTrapRogueIfoURL	1.3.6.1.4.1.14823.2.3.3.1.200.1.22	wlsxTrapObjectsGroup 22
wlsxTrapVLANId	1.3.6.1.4.1.14823.2.3.3.1.200.1.23	wlsxTrapObjectsGroup 23
wlsxTrapAdminStatus	1.3.6.1.4.1.14823.2.3.3.1.200.1.24	wlsxTrapObjectsGroup 24
wlsxTrapOperStatus	1.3.6.1.4.1.14823.2.3.3.1.200.1.25	wlsxTrapObjectsGroup 25
wlsxTrapAuthServerName	1.3.6.1.4.1.14823.2.3.3.1.200.1.26	wlsxTrapObjectsGroup 26
wlsxTrapAuthServerTimeout	1.3.6.1.4.1.14823.2.3.3.1.200.1.27	wlsxTrapObjectsGroup 27



**Table 11: aiTraps Objects Group OIDs**

Object	Object ID	
wlsxTrapCardSlot	1.3.6.1.4.1.14823.2.3.3.1.200.1.28	wlsxTrapObjectsGroup 28
wlsxTrapTemperatureValue	1.3.6.1.4.1.14823.2.3.3.1.200.1.29	wlsxTrapObjectsGroup 29
wlsxTrapProcessName	1.3.6.1.4.1.14823.2.3.3.1.200.1.30	wlsxTrapObjectsGroup 30
wlsxTrapFanNumber	1.3.6.1.4.1.14823.2.3.3.1.200.1.31	wlsxTrapObjectsGroup 31
wlsxTrapVoltageType	1.3.6.1.4.1.14823.2.3.3.1.200.1.32	wlsxTrapObjectsGroup 32
wlsxTrapVoltageValue	1.3.6.1.4.1.14823.2.3.3.1.200.1.33	wlsxTrapObjectsGroup 33
wlsxTrapStationBlackListReason	1.3.6.1.4.1.14823.2.3.3.1.200.1.34	wlsxTrapObjectsGroup 34
wlsxTrapSpoofedIpAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.35	wlsxTrapObjectsGroup 35
wlsxTrapSpoofedOldPhyAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.36	wlsxTrapObjectsGroup 36
wlsxTrapSpoofedNewPhyAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.37	wlsxTrapObjectsGroup 37
wlsxTrapDBName	1.3.6.1.4.1.14823.2.3.3.1.200.1.38	wlsxTrapObjectsGroup 38
wlsxTrapDBUserName	1.3.6.1.4.1.14823.2.3.3.1.200.1.39	wlsxTrapObjectsGroup 39
wlsxTrapDBIpAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.40	wlsxTrapObjectsGroup 40
wlsxTrapDBType	1.3.6.1.4.1.14823.2.3.3.1.200.1.41	wlsxTrapObjectsGroup 41
wlsxTrapVrrpID	1.3.6.1.4.1.14823.2.3.3.1.200.1.42	wlsxTrapObjectsGroup 42
wlsxTrapVrrpMasterIp	1.3.6.1.4.1.14823.2.3.3.1.200.1.43	wlsxTrapObjectsGroup 43
wlsxTrapVrrpOperState	1.3.6.1.4.1.14823.2.3.3.1.200.1.44	wlsxTrapObjectsGroup 44
wlsxTrapESIServerGrpName	1.3.6.1.4.1.14823.2.3.3.1.200.1.45	wlsxTrapObjectsGroup 45
wlsxTrapESIServerName	1.3.6.1.4.1.14823.2.3.3.1.200.1.46	wlsxTrapObjectsGroup 46
wlsxTrapESIServerIpAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.47	wlsxTrapObjectsGroup 47
wlsxTrapLicenseDaysRemaining	1.3.6.1.4.1.14823.2.3.3.1.200.1.48	wlsxTrapObjectsGroup 48
wlsxTrapSwitchIp	1.3.6.1.4.1.14823.2.3.3.1.200.1.49	wlsxTrapObjectsGroup 49
wlsxTrapSwitchRole	1.3.6.1.4.1.14823.2.3.3.1.200.1.50	wlsxTrapObjectsGroup 50
wlsxTrapUserIpAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.51	wlsxTrapObjectsGroup 51
wlsxTrapUserPhyAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.52	wlsxTrapObjectsGroup 52
wlsxTrapUserName	1.3.6.1.4.1.14823.2.3.3.1.200.1.53	wlsxTrapObjectsGroup 53
wlsxTrapUserRole	1.3.6.1.4.1.14823.2.3.3.1.200.1.54	wlsxTrapObjectsGroup 54

**Table 11: aiTraps Objects Group OIDs**

Object	Object ID	
wlsxTrapUserAuthenticationMethod	1.3.6.1.4.1.14823.2.3.3.1.200.1.55	wlsxTrapObjectsGroup 55
wlsxTrapAPRadioNumber	1.3.6.1.4.1.14823.2.3.3.1.200.1.56	wlsxTrapObjectsGroup 56
wlsxTrapRogueInfoURL	1.3.6.1.4.1.14823.2.3.3.1.200.1.57	wlsxTrapObjectsGroup 57
wlsxTrapInterferingAPInfoURL	1.3.6.1.4.1.14823.2.3.3.1.200.1.58	wlsxTrapObjectsGroup 58
wlsxTrapPortNumber	1.3.6.1.4.1.14823.2.3.3.1.200.1.59	wlsxTrapObjectsGroup 59
wlsxTrapTime	1.3.6.1.4.1.14823.2.3.3.1.200.1.60	wlsxTrapObjectsGroup 60
wlsxTrapHostIp	1.3.6.1.4.1.14823.2.3.3.1.200.1.61	wlsxTrapObjectsGroup 61
wlsxTrapHostPort	1.3.6.1.4.1.14823.2.3.3.1.200.1.63	wlsxTrapObjectsGroup 62
wlsxTrapConfigurationId	1.3.6.1.4.1.14823.2.3.3.1.200.1.63	wlsxTrapObjectsGroup 63
wlsxTrapCTSURL	1.3.6.1.4.1.14823.2.3.3.1.200.1.64	wlsxTrapObjectsGroup 64
wlsxTrapCTSTransferType	1.3.6.1.4.1.14823.2.3.3.1.200.1.65	wlsxTrapObjectsGroup 65
wlsxTrapConfigurationState	1.3.6.1.4.1.14823.2.3.3.1.200.1.66	wlsxTrapObjectsGroup 66
wlsxTrapUpdateFailureReason	1.3.6.1.4.1.14823.2.3.3.1.200.1.67	wlsxTrapObjectsGroup 67
wlsxTrapUpdateFailedObj	1.3.6.1.4.1.14823.2.3.3.1.200.1.68	wlsxTrapObjectsGroup 68
wlsxTrapTableEntryChangeType	1.3.6.1.4.1.14823.2.3.3.1.200.1.69	wlsxTrapObjectsGroup 69
wlsxTrapGlobalConfigObj	1.3.6.1.4.1.14823.2.3.3.1.200.1.70	wlsxTrapObjectsGroup 70
wlsxTrapTableGenNumber	1.3.6.1.4.1.14823.2.3.3.1.200.1.71	wlsxTrapObjectsGroup 71
wlsxTrapLicenseId	1.3.6.1.4.1.14823.2.3.3.1.200.1.72	wlsxTrapObjectsGroup 72
wlsxTrapConfidenceLevel	1.3.6.1.4.1.14823.2.3.3.1.200.1.73	wlsxTrapObjectsGroup 73
wlsxTrapMissingLicenses	1.3.6.1.4.1.14823.2.3.3.1.200.1.74	wlsxTrapObjectsGroup 74
wlsxVoiceCurrentNumCdr	1.3.6.1.4.1.14823.2.3.3.1.200.1.75	wlsxTrapObjectsGroup 75
wlsxTrapTunnelId	1.3.6.1.4.1.14823.2.3.3.1.200.1.76	wlsxTrapObjectsGroup 76
wlsxTrapTunnelStatus	1.3.6.1.4.1.14823.2.3.3.1.200.1.77	wlsxTrapObjectsGroup 77
wlsxTrapTunnelUpReason	1.3.6.1.4.1.14823.2.3.3.1.200.1.78	wlsxTrapObjectsGroup 78
wlsxTrapTunnelDownReason	1.3.6.1.4.1.14823.2.3.3.1.200.1.79	wlsxTrapObjectsGroup 79
wlsxTrapApSerialNumber	1.3.6.1.4.1.14823.2.3.3.1.200.1.80	wlsxTrapObjectsGroup 80
wlsxTrapTimeStr	1.3.6.1.4.1.14823.2.3.3.1.200.1.81	wlsxTrapObjectsGroup 81

**Table 11: aiTraps Objects Group OIDs**

Object	Object ID	
wlsxTrapMasterIrp	1.3.6.1.4.1.14823.2.3.3.1.200.1.82	wlsxTrapObjectsGroup 82
wlsxTrapLocalIrp	1.3.6.1.4.1.14823.2.3.3.1.200.1.83	wlsxTrapObjectsGroup 83
wlsxTrapMasterName	1.3.6.1.4.1.14823.2.3.3.1.200.1.84	wlsxTrapObjectsGroup 84
wlsxTrapLocalName	1.3.6.1.4.1.14823.2.3.3.1.200.1.85	wlsxTrapObjectsGroup 85
wlsxTrapPrimaryControllerIrp	1.3.6.1.4.1.14823.2.3.3.1.200.1.86	wlsxTrapObjectsGroup 86
wlsxTrapBackupControllerIrp	1.3.6.1.4.1.14823.2.3.3.1.200.1.87	wlsxTrapObjectsGroup 87
wlsxTrapSpoofedFrameType	1.3.6.1.4.1.14823.2.3.3.1.200.1.88	wlsxTrapObjectsGroup 88
wlsxTrapAssociationType	1.3.6.1.4.1.14823.2.3.3.1.200.1.89	wlsxTrapObjectsGroup 89
wlsxTrapDeviceIpAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.90	wlsxTrapObjectsGroup 90
wlsxTrapDeviceMac	1.3.6.1.4.1.14823.2.3.3.1.200.1.91	wlsxTrapObjectsGroup 91
wlsxTrapVcIpAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.92	wlsxTrapObjectsGroup 92
wlsxTrapVcMacAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.93	wlsxTrapObjectsGroup 93
wlsxTrapAPName	1.3.6.1.4.1.14823.2.3.3.1.200.1.94	wlsxTrapObjectsGroup 94
wlsxTrapApMode	1.3.6.1.4.1.14823.2.3.3.1.200.1.95	wlsxTrapObjectsGroup 95
wlsxTrapAPPrevChannel	1.3.6.1.4.1.14823.2.3.3.1.200.1.96	wlsxTrapObjectsGroup 96
wlsxTrapAPPrevChannelSec	1.3.6.1.4.1.14823.2.3.3.1.200.1.97	wlsxTrapObjectsGroup 97
wlsxTrapAPPrevTxPower	1.3.6.1.4.1.14823.2.3.3.1.200.1.98	wlsxTrapObjectsGroup 98
wlsxTrapAPCurMode	1.3.6.1.4.1.14823.2.3.3.1.200.1.99	wlsxTrapObjectsGroup 99
wlsxTrapAPPrevMode	1.3.6.1.4.1.14823.2.3.3.1.200.1.100	wlsxTrapObjectsGroup 100
wlsxTrapAPARMChangeReason	1.3.6.1.4.1.14823.2.3.3.1.200.1.101	wlsxTrapObjectsGroup 101
wlsxTrapAPChannelSec	1.3.6.1.4.1.14823.2.3.3.1.200.1.102	wlsxTrapObjectsGroup 102
wlsxTrapUserAttributeChangeType	1.3.6.1.4.1.14823.2.3.3.1.200.1.103	wlsxTrapObjectsGroup 103
wlsxTrapAPControllerIrp	1.3.6.1.4.1.14823.2.3.3.1.200.1.104	wlsxTrapObjectsGroup 104
wlsxTrapApMasterStatus	1.3.6.1.4.1.14823.2.3.3.1.200.1.105	wlsxTrapObjectsGroup 105
wlsxTrapCaName	1.3.6.1.4.1.14823.2.3.3.1.200.1.106	wlsxTrapObjectsGroup 106
wlsxTrapCrIName	1.3.6.1.4.1.14823.2.3.3.1.200.1.107	wlsxTrapObjectsGroup 107
wlsxTrapCount	1.3.6.1.4.1.14823.2.3.3.1.200.1.108	wlsxTrapObjectsGroup 108

**Table 11: aiTraps Objects Group OIDs**

Object	Object ID	
wlsxTrapAPPreviousUplinkType	1.3.6.1.4.1.14823.2.3.3.1.200.1.130	wlsxTrapObjectsGroup 130
wlsxTrapAPPreviousUplinkActiveTime	1.3.6.1.4.1.14823.2.3.3.1.200.1.131	wlsxTrapObjectsGroup 131
wlsxTrapAPActiveUplinkType	1.3.6.1.4.1.14823.2.3.3.1.200.1.132	wlsxTrapObjectsGroup 132
wlsxTrapAPUplinkChangeReason	1.3.6.1.4.1.14823.2.3.3.1.200.1.133	wlsxTrapObjectsGroup 133
wlsxTrapAPManagedModeConfigFailure	1.3.6.1.4.1.14823.2.3.3.1.200.1.134	wlsxTrapObjectsGroup 134

### wlsxTrapAPMacAddress

<b>Syntax</b>	MacAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the wired MAC address of an access point, for which the trap is being raised.

### wlsxTrapAPIpAddress

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the IP address of an access point for which for which the trap is being raised.

### wlsxTrapAPBSSID

<b>Syntax</b>	MacAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the BSSID of the access point for which we are raising the trap.

## wlsxTrapEssid

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the SSID of the access point, for which the trap is being raised.

## wlsxTrapTargetAPBSSID

<b>Syntax</b>	MacAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the BSSID of the access point, for which we are raising the trap. If an Air Monitor is sending the trap then this will indicate AP. If an access point is sending the trap, then it will point to itself.

## wlsxTrapTargetAPSSID

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the SSID of the access point, for which the trap is being raised. If an Air Monitor is sending the trap then this will indicate AP. If an access point is sending the trap, then it will point to itself.

## wlsxTrapTargetAPChannel

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the channel of the access point, for which the trap is being raised. If an wlsxr monitor is sending the trap then this will indicate AP. If an access point is sending the trap, then it will point to itself.

## wlsxTrapNodeMac

<b>Syntax</b>	MacAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the MAC address of a node.

## wlsxTrapSourceMac

<b>Syntax</b>	MacAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the MAC address of the source.

## wlsxReceiverMac

<b>Syntax</b>	MacAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the MAC address of the receiver.

## wlsxTrapTransmitterMac

<b>Syntax</b>	MacAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the MAC address of the transmitter.

## wlsxTrapReceiverMac

<b>Syntax</b>	MacAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the MAC address of the receiver.

## wlsxTrapSnr

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the signal-to-noise ratio.

## wlsxTrapSignatureName

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the signature name.

## wlsxTrapFrameType

<b>Syntax</b>	ArubaFrameType
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the frame type.

## wlsxTrapAddressType

<b>Syntax</b>	ArubaAddressType
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the address type.

## wlsxTrapAPLocation

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the location of the AP.

## wlsxTrapAPChannel

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the current channel.

## wlsxTrapAPTxFPower

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the AP transmit power.

## wlsxTrapMatchedMac

<b>Syntax</b>	MacAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the MAC address.

## wlsxTrapMatchedIp

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the IP address.

## wlsxTrapRogueIfURL

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used to point to the WEBUI Rogue AP information URL.



## wlsxTrapVLANId

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the VLAN ID.

## wlsxTrapAdminStatus

<b>Syntax</b>	ArubaEnableValue (INTEGER)
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the admin status of VLAN.

## wlsxTrapOperStatus

<b>Syntax</b>	ArubaOperStateValue
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the admin status of VLAN.

## wlsxTrapAuthServerName

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the authentication server used for authentication.

## wlsxTrapAuthServerTimeout

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the Authentication Server Timeout.

## wlsxTrapCardSlot

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the slot in which this card is present.

## wlsxTrapTemperatureValue

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the temperature value.

## wlsxTrapProcessName

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the process name.

## wlsxTrapFanNumber

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the fan number.

## wlsxTrapVoltageType

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the type of voltage.

## wlsxTrapVoltageValue

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the voltage value in float.

## wlsxTrapStationBlackListReason

<b>Syntax</b>	ArubaBlackListReason
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	The reason for which a station is black listed.

## wlsxTrapSpoofedIpAddress

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in a trap to identify a spoofed IP address.

## wlsxTrapSpoofedOldPhyAddress

<b>Syntax</b>	MacAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in a trap to identify an old MAC address.

## wlsxTrapSpoofedNewPhyAddress

<b>Syntax</b>	MacAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in a trap to identify a new MAC address.

## wlsxTrapDBName

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in a trap to identify the name of the database.

## wlsxTrapDBUserName

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in a trap to identify the name of the database user.

## wlsxTrapDBIpAddress

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in a trap to identify the IP address of the database.

## wlsxTrapDBType

<b>Syntax</b>	ArubaDBType
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in a trap to identify the port of the user.

## wlsxTrapVrrpID

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object contains the virtual router identifier.

## wlsxTrapVrrpMasterIp

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object contains the master IP address.

## wlsxTrapVrrpOperState

<b>Syntax</b>	ArubaVrrpState
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the VRRP operational state.

## wlsxTrapESIServerGrpName

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the External Services Interface (ESI) server group name.

## wlsxTrapESIServerName

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the External Services Interface (ESI) server name.

## wlsxTrapESIServerIpAddress

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the External Services Interface (ESI) server IP address.

## wlsxTrapLicenseDaysRemaining

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the number of days remaining prior to a license expiry.

## wlsxTrapSwitchIp

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the controller IP address.

## wlsxTrapSwitchRole

<b>Syntax</b>	ArubaSwitchRole
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the role of the controller.

## wlsxTrapUserIpAddress

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the IP address of the user.

## wlsxTrapUserPhyAddress

<b>Syntax</b>	MacAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the MAC address of the user.

## wlsxTrapUserName

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the user name.

## wlsxTrapUserRole

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the Authentication method of the user.

## wlsxTrapUserAuthenticationMethod

<b>Syntax</b>	ArubaAuthenticationMethods
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the Authentication method of the user.

## wlsxTrapAPRadioNumber

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the radio number.

## wlsxTrapRogueInfoURL

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used to point to the WEBGUI Rogue AP information URL.

## wlsxTrapInterferingAPIInfoURL

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used to point to the WEBGUI Rogue interfering access point information URL.

## wlsxTrapPortNumber

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the port number.

## wlsxTrapTime

<b>Syntax</b>	DateAndTime
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in all the enterprise traps to indicate the time when the trap is generated on the controller.

## wlsxTrapHostIp

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the trap host.

## wlsxTrapHostPort

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the trap host port.



## wlsxTrapConfigurationId

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	

## wlsxTrapCTSURL

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the URL from which the transfer should happen.

## wlsxTrapCTSTransferType

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the transfer type, upload or download.

## wlsxTrapConfigurationState

<b>Syntax</b>	ArubaConfigurationState (INTEGER)
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the state of the configuration transfer.

## wlsxTrapUpdateFailureReason

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the reason for the update failure.

## wlsxTrapUpdateFailedObj

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This variable represents the AMAPI object which is the reason for the update failure.

## wlsxTrapTableEntryChangeType

<b>Syntax</b>	ArubaConfigurationChangeType (INTEGER)
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the type of the configuration change.

## wlsxTrapGlobalConfigObj

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This variable represents the AMAPI object corresponding to the global configuration change.

## wlsxTrapTableGenNumber

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the generation number of a table. Used in the MMS to keep track of the table content changes.

## wlsxTrapLicenseId

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the license ID.

## wlsxTrapConfidenceLevel

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the confidence level as a percentage.

## wlsxTrapMissingLicenses

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This variable indicates any licenses that are not present during a configuration update.

## wlsxVoiceCurrentNumCdr

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the number of CDRs in buffer.

## wlsxTrapTunnelId

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the tunnel ID.

## wlsxTrapTunnelStatus

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the tunnel status.

## wlsxTrapTunnelUpReason

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the tunnel up reason.

## wlsxTrapTunnelDownReason

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the tunnel down reason.

## wlsxTrapApSerialNumber

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the AP serial number.

## wlsxTraptimeStr

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the Time in String format.

## wlsxTrapMasterIp

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the master IP address.

## wlsxTrapLocalIp

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the local IP address.

## wlsxTrapMasterName

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the master controller name.

## wlsxTrapLocalName

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the local controller name.

## wlsxTrapPrimaryControllerIp

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the IP address of the AP's primary controller.

## wlsxTrapBackupControllerIp

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the IP address of the AP's backup controller.

## wlsxTrapSpoofedFrameType

<b>Syntax</b>	DisplayString (SIZE(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the Spoofed Frame Type

## wlsxTrapAssociationType

<b>Syntax</b>	DisplayString (SIZE(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the type of association.

## wlsxTrapDeviceIpAddress

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the IP address of a device seen by an AP.

## wlsxTrapDeviceMac

<b>Syntax</b>	MacAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the MAC address of a device seen by an AP.

## wlsxTrapVcIpAddress

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the IP Address of a Voice client.

## wlsxTrapVcMacAddress

<b>Syntax</b>	MacAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the MAC address of a Voice client.

## wlsxTrapAPName

<b>Syntax</b>	DisplayString (SIZE(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the Name of the AP.

## wlsxTrapApMode

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	

## wlsxTrapAPPprevChannel

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the Previous Channel.

## wlsxTrapAPPprevChannelSec

<b>Syntax</b>	ArubaHTextChannel (INTEGER)
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the Previous Secondary Channel.

## wlsxTrapAPPprevTxPower

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate previous AP Transmit Power.

## wlsxTrapAPCurMode

<b>Syntax</b>	ArubaAccessPointMode (INTEGER)
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This Object represents the APs Current Mode.

## wlsxTrapAPPprevMode

<b>Syntax</b>	ArubaAccessPointMode (INTEGER)
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This Object represents the APs Previous Mode.

## wlsxTrapAPARMChangeReason

<b>Syntax</b>	ArubaARMChangeReason (INTEGER)
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This Object represents the APs Previous Mode.

## wlsxTrapAPChannelSec

<b>Syntax</b>	ArubaHTextChannel (INTEGER)
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the Current Secondary Channel.



## wlsxTrapUserAttributeChangeType

<b>Syntax</b>	ArubaConfigurationChangeType (INTEGER)
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents type of the configuration change.

## wlsxTrapAPControllerIp

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	

## wlsxTrapApMasterStatus

<b>Syntax</b>	ArubaAPMasterStatus (INTEGER)
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	Status of the AP as seen by the master when the status changes.

## wlsxTrapCaName

<b>Syntax</b>	DisplayString (SIZE(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	

## wlsxTrapCrlName

<b>Syntax</b>	DisplayString (SIZE(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the name of the CRL.

## wlsxTrapCount

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the number of occurrence of this trap.

## wlsxTrapAPPPreviousUplinkType

<b>Syntax</b>	ArubaAPUplinkType
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the previous uplink type of an AP.

## wlsxTrapAPPPreviousUplinkActiveTime

<b>Syntax</b>	TimeTicks
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the active time of the previous uplink of an AP.

## wlsxTrapAPActiveUplinkType

<b>Syntax</b>	ArubaAPUplinkType
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the active uplink type of an AP.

## wlsxTrapAPUplinkChangeReason

<b>Syntax</b>	ArubaAPUplinkChangeReason
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the uplink change reason.

## wlsxTrapAPManagedModeConfigFailure

<b>Syntax</b>	DisplayString (SIZE(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object indicates that the configuration application has failed on the AP.

## ai Traps Objects Group

The following table lists the supported trap objects in this group:

**Table 12:** aiTraps Objects Group OIDs

Object	Object ID	
wlsxTrapAPMacAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.1	wlsxTrapObjectsGroup 1
wlsxTrapAPIpAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.2	wlsxTrapObjectsGroup 2
wlsxTrapAPBSSID	1.3.6.1.4.1.14823.2.3.3.1.200.1.3	wlsxTrapObjectsGroup 3
wlsxTrapEssid	1.3.6.1.4.1.14823.2.3.3.1.200.1.4	wlsxTrapObjectsGroup 4
wlsxTrapTargetAPBSSID	1.3.6.1.4.1.14823.2.3.3.1.200.1.5	wlsxTrapObjectsGroup 5
wlsxTrapTargetAPSSID	1.3.6.1.4.1.14823.2.3.3.1.200.1.6	wlsxTrapObjectsGroup 6
wlsxTrapTargetAPChannel	1.3.6.1.4.1.14823.2.3.3.1.200.1.7	wlsxTrapObjectsGroup 7
wlsxTrapNodeMac	1.3.6.1.4.1.14823.2.3.3.1.200.1.8	wlsxTrapObjectsGroup 8
wlsxTrapSourceMac	1.3.6.1.4.1.14823.2.3.3.1.200.1.9	wlsxTrapObjectsGroup 9
wlsxReceiverMac	1.3.6.1.4.1.14823.2.3.3.1.200.1.10	wlsxTrapObjectsGroup 10
wlsxTrapTransmitterMac	1.3.6.1.4.1.14823.2.3.3.1.200.1.11	wlsxTrapObjectsGroup 11
wlsxTrapReceiverMac	1.3.6.1.4.1.14823.2.3.3.1.200.1.12	wlsxTrapObjectsGroup 12
wlsxTrapSnr	1.3.6.1.4.1.14823.2.3.3.1.200.1.13	wlsxTrapObjectsGroup 13
wlsxTrapSignatureName	1.3.6.1.4.1.14823.2.3.3.1.200.1.14	wlsxTrapObjectsGroup 14
wlsxTrapFrameType	1.3.6.1.4.1.14823.2.3.3.1.200.1.15	wlsxTrapObjectsGroup 15
wlsxTrapAddressType	1.3.6.1.4.1.14823.2.3.3.1.200.1.16	wlsxTrapObjectsGroup 16
wlsxTrapAPLocation	1.3.6.1.4.1.14823.2.3.3.1.200.1.17	wlsxTrapObjectsGroup 17
wlsxTrapAPChannel	1.3.6.1.4.1.14823.2.3.3.1.200.1.18	wlsxTrapObjectsGroup 18
wlsxTrapAPTxFPower	1.3.6.1.4.1.14823.2.3.3.1.200.1.19	wlsxTrapObjectsGroup 19
wlsxTrapMatchedMac	1.3.6.1.4.1.14823.2.3.3.1.200.1.20	wlsxTrapObjectsGroup 20

Object	Object ID	
wlsxTrapMatchedIp	1.3.6.1.4.1.14823.2.3.3.1.200.1.21	wlsxTrapObjectsGroup 21
wlsxTrapRogueIfoURL	1.3.6.1.4.1.14823.2.3.3.1.200.1.22	wlsxTrapObjectsGroup 22
wlsxTrapVLANId	1.3.6.1.4.1.14823.2.3.3.1.200.1.23	wlsxTrapObjectsGroup 23
wlsxTrapAdminStatus	1.3.6.1.4.1.14823.2.3.3.1.200.1.24	wlsxTrapObjectsGroup 24
wlsxTrapOperStatus	1.3.6.1.4.1.14823.2.3.3.1.200.1.25	wlsxTrapObjectsGroup 25
wlsxTrapAuthServerName	1.3.6.1.4.1.14823.2.3.3.1.200.1.26	wlsxTrapObjectsGroup 26
wlsxTrapAuthServerTimeout	1.3.6.1.4.1.14823.2.3.3.1.200.1.27	wlsxTrapObjectsGroup 27
wlsxTrapCardSlot	1.3.6.1.4.1.14823.2.3.3.1.200.1.28	wlsxTrapObjectsGroup 28
wlsxTrapTemperatureValue	1.3.6.1.4.1.14823.2.3.3.1.200.1.29	wlsxTrapObjectsGroup 29
wlsxTrapProcessName	1.3.6.1.4.1.14823.2.3.3.1.200.1.30	wlsxTrapObjectsGroup 30
wlsxTrapFanNumber	1.3.6.1.4.1.14823.2.3.3.1.200.1.31	wlsxTrapObjectsGroup 31
wlsxTrapVoltageType	1.3.6.1.4.1.14823.2.3.3.1.200.1.32	wlsxTrapObjectsGroup 32
wlsxTrapVoltageValue	1.3.6.1.4.1.14823.2.3.3.1.200.1.33	wlsxTrapObjectsGroup 33
wlsxTrapStationBlackListReason	1.3.6.1.4.1.14823.2.3.3.1.200.1.34	wlsxTrapObjectsGroup 34
wlsxTrapSpoofedIpAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.35	wlsxTrapObjectsGroup 35
wlsxTrapSpoofedOldPhyAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.36	wlsxTrapObjectsGroup 36
wlsxTrapSpoofedNewPhyAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.37	wlsxTrapObjectsGroup 37
wlsxTrapDBName	1.3.6.1.4.1.14823.2.3.3.1.200.1.38	wlsxTrapObjectsGroup 38
wlsxTrapDBUserName	1.3.6.1.4.1.14823.2.3.3.1.200.1.39	wlsxTrapObjectsGroup 39
wlsxTrapDBIpAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.40	wlsxTrapObjectsGroup 40
wlsxTrapDBType	1.3.6.1.4.1.14823.2.3.3.1.200.1.41	wlsxTrapObjectsGroup 41
wlsxTrapVrrpID	1.3.6.1.4.1.14823.2.3.3.1.200.1.42	wlsxTrapObjectsGroup 42
wlsxTrapVrrpMasterIp	1.3.6.1.4.1.14823.2.3.3.1.200.1.43	wlsxTrapObjectsGroup 43
wlsxTrapVrrpOperState	1.3.6.1.4.1.14823.2.3.3.1.200.1.44	wlsxTrapObjectsGroup 44
wlsxTrapESIServerGrpName	1.3.6.1.4.1.14823.2.3.3.1.200.1.45	wlsxTrapObjectsGroup 45
wlsxTrapESIServerName	1.3.6.1.4.1.14823.2.3.3.1.200.1.46	wlsxTrapObjectsGroup 46
wlsxTrapESIServerIpAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.47	wlsxTrapObjectsGroup 47
wlsxTrapLicenseDaysRemaining	1.3.6.1.4.1.14823.2.3.3.1.200.1.48	wlsxTrapObjectsGroup 48

Object	Object ID	
wlsxTrapSwitchIp	1.3.6.1.4.1.14823.2.3.3.1.200.1.49	wlsxTrapObjectsGroup 49
wlsxTrapSwitchRole	1.3.6.1.4.1.14823.2.3.3.1.200.1.50	wlsxTrapObjectsGroup 50
wlsxTrapUserIpAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.51	wlsxTrapObjectsGroup 51
wlsxTrapUserPhyAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.52	wlsxTrapObjectsGroup 52
wlsxTrapUserName	1.3.6.1.4.1.14823.2.3.3.1.200.1.53	wlsxTrapObjectsGroup 53
wlsxTrapUserRole	1.3.6.1.4.1.14823.2.3.3.1.200.1.54	wlsxTrapObjectsGroup 54
wlsxTrapUserAuthenticationMethod	1.3.6.1.4.1.14823.2.3.3.1.200.1.55	wlsxTrapObjectsGroup 55
wlsxTrapAPRadioNumber	1.3.6.1.4.1.14823.2.3.3.1.200.1.56	wlsxTrapObjectsGroup 56
wlsxTrapRogueInfoURL	1.3.6.1.4.1.14823.2.3.3.1.200.1.57	wlsxTrapObjectsGroup 57
wlsxTrapInterferingAPInfoURL	1.3.6.1.4.1.14823.2.3.3.1.200.1.58	wlsxTrapObjectsGroup 58
wlsxTrapPortNumber	1.3.6.1.4.1.14823.2.3.3.1.200.1.59	wlsxTrapObjectsGroup 59
wlsxTrapTime	1.3.6.1.4.1.14823.2.3.3.1.200.1.60	wlsxTrapObjectsGroup 60
wlsxTrapHostIp	1.3.6.1.4.1.14823.2.3.3.1.200.1.61	wlsxTrapObjectsGroup 61
wlsxTrapHostPort	1.3.6.1.4.1.14823.2.3.3.1.200.1.63	wlsxTrapObjectsGroup 62
wlsxTrapConfigurationId	1.3.6.1.4.1.14823.2.3.3.1.200.1.63	wlsxTrapObjectsGroup 63
wlsxTrapCTSURL	1.3.6.1.4.1.14823.2.3.3.1.200.1.64	wlsxTrapObjectsGroup 64
wlsxTrapCTSTransferType	1.3.6.1.4.1.14823.2.3.3.1.200.1.65	wlsxTrapObjectsGroup 65
wlsxTrapConfigurationState	1.3.6.1.4.1.14823.2.3.3.1.200.1.66	wlsxTrapObjectsGroup 66
wlsxTrapUpdateFailureReason	1.3.6.1.4.1.14823.2.3.3.1.200.1.67	wlsxTrapObjectsGroup 67
wlsxTrapUpdateFailedObj	1.3.6.1.4.1.14823.2.3.3.1.200.1.68	wlsxTrapObjectsGroup 68
wlsxTrapTableEntryChangeType	1.3.6.1.4.1.14823.2.3.3.1.200.1.69	wlsxTrapObjectsGroup 69
wlsxTrapGlobalConfigObj	1.3.6.1.4.1.14823.2.3.3.1.200.1.70	wlsxTrapObjectsGroup 70
wlsxTrapTableGenNumber	1.3.6.1.4.1.14823.2.3.3.1.200.1.71	wlsxTrapObjectsGroup 71
wlsxTrapLicenseId	1.3.6.1.4.1.14823.2.3.3.1.200.1.72	wlsxTrapObjectsGroup 72
wlsxTrapConfidenceLevel	1.3.6.1.4.1.14823.2.3.3.1.200.1.73	wlsxTrapObjectsGroup 73
wlsxTrapMissingLicenses	1.3.6.1.4.1.14823.2.3.3.1.200.1.74	wlsxTrapObjectsGroup 74
wlsxVoiceCurrentNumCdr	1.3.6.1.4.1.14823.2.3.3.1.200.1.75	wlsxTrapObjectsGroup 75
wlsxTrapTunnelId	1.3.6.1.4.1.14823.2.3.3.1.200.1.76	wlsxTrapObjectsGroup 76

Object	Object ID	
wlsxTrapTunnelStatus	1.3.6.1.4.1.14823.2.3.3.1.200.1.77	wlsxTrapObjectsGroup 77
wlsxTrapTunnelUpReason	1.3.6.1.4.1.14823.2.3.3.1.200.1.78	wlsxTrapObjectsGroup 78
wlsxTrapTunnelDownReason	1.3.6.1.4.1.14823.2.3.3.1.200.1.79	wlsxTrapObjectsGroup 79
wlsxTrapApSerialNumber	1.3.6.1.4.1.14823.2.3.3.1.200.1.80	wlsxTrapObjectsGroup 80
wlsxTraptimeStr	1.3.6.1.4.1.14823.2.3.3.1.200.1.81	wlsxTrapObjectsGroup 81
wlsxTrapMasterIrp	1.3.6.1.4.1.14823.2.3.3.1.200.1.82	wlsxTrapObjectsGroup 82
wlsxTrapLocalIrp	1.3.6.1.4.1.14823.2.3.3.1.200.1.83	wlsxTrapObjectsGroup 83
wlsxTrapMasterName	1.3.6.1.4.1.14823.2.3.3.1.200.1.84	wlsxTrapObjectsGroup 84
wlsxTrapLocalName	1.3.6.1.4.1.14823.2.3.3.1.200.1.85	wlsxTrapObjectsGroup 85
wlsxTrapPrimaryControllerIrp	1.3.6.1.4.1.14823.2.3.3.1.200.1.86	wlsxTrapObjectsGroup 86
wlsxTrapBackupControllerIrp	1.3.6.1.4.1.14823.2.3.3.1.200.1.87	wlsxTrapObjectsGroup 87
wlsxTrapSpoofedFrameType	1.3.6.1.4.1.14823.2.3.3.1.200.1.88	wlsxTrapObjectsGroup 88
wlsxTrapAssociationType	1.3.6.1.4.1.14823.2.3.3.1.200.1.89	wlsxTrapObjectsGroup 89
wlsxTrapDeviceIrpAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.90	wlsxTrapObjectsGroup 90
wlsxTrapDeviceMac	1.3.6.1.4.1.14823.2.3.3.1.200.1.91	wlsxTrapObjectsGroup 91
wlsxTrapVcIrpAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.92	wlsxTrapObjectsGroup 92
wlsxTrapVcMacAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.93	wlsxTrapObjectsGroup 93
wlsxTrapAPName	1.3.6.1.4.1.14823.2.3.3.1.200.1.94	wlsxTrapObjectsGroup 94
wlsxTrapApMode	1.3.6.1.4.1.14823.2.3.3.1.200.1.95	wlsxTrapObjectsGroup 95
wlsxTrapAPPrevChannel	1.3.6.1.4.1.14823.2.3.3.1.200.1.96	wlsxTrapObjectsGroup 96
wlsxTrapAPPrevChannelSec	1.3.6.1.4.1.14823.2.3.3.1.200.1.97	wlsxTrapObjectsGroup 97
wlsxTrapAPPrevTxPower	1.3.6.1.4.1.14823.2.3.3.1.200.1.98	wlsxTrapObjectsGroup 98
wlsxTrapAPCurMode	1.3.6.1.4.1.14823.2.3.3.1.200.1.99	wlsxTrapObjectsGroup 99
wlsxTrapAPPrevMode	1.3.6.1.4.1.14823.2.3.3.1.200.1.100	wlsxTrapObjectsGroup 100
wlsxTrapAPARMChangeReason	1.3.6.1.4.1.14823.2.3.3.1.200.1.101	wlsxTrapObjectsGroup 101
wlsxTrapAPChannelSec	1.3.6.1.4.1.14823.2.3.3.1.200.1.102	wlsxTrapObjectsGroup 102
wlsxTrapUserAttributeChangeType	1.3.6.1.4.1.14823.2.3.3.1.200.1.103	wlsxTrapObjectsGroup 103
wlsxTrapAPControllerIrp	1.3.6.1.4.1.14823.2.3.3.1.200.1.104	wlsxTrapObjectsGroup 104

Object	Object ID	
wlsxTrapApMasterStatus	1.3.6.1.4.1.14823.2.3.3.1.200.1.105	wlsxTrapObjectsGroup 105
wlsxTrapCaName	1.3.6.1.4.1.14823.2.3.3.1.200.1.106	wlsxTrapObjectsGroup 106
wlsxTrapCrlName	1.3.6.1.4.1.14823.2.3.3.1.200.1.107	wlsxTrapObjectsGroup 107
wlsxTrapCount	1.3.6.1.4.1.14823.2.3.3.1.200.1.108	wlsxTrapObjectsGroup 108
wlsxTrapAPPreviousUplinkType	1.3.6.1.4.1.14823.2.3.3.1.200.1.130	wlsxTrapObjectsGroup 130
wlsxTrapAPPreviousUplinkActiveTime	1.3.6.1.4.1.14823.2.3.3.1.200.1.131	wlsxTrapObjectsGroup 131
wlsxTrapAPActiveUplinkType	1.3.6.1.4.1.14823.2.3.3.1.200.1.132	wlsxTrapObjectsGroup 132
wlsxTrapAPUplinkChangeReason	1.3.6.1.4.1.14823.2.3.3.1.200.1.133	wlsxTrapObjectsGroup 133
wlsxTrapAPManagedModeConfigFailure	1.3.6.1.4.1.14823.2.3.3.1.200.1.134	wlsxTrapObjectsGroup 134

### wlsxTrapAPMacAddress

<b>Syntax</b>	MacAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the wired MAC address of an access point, for which the trap is being raised.

### wlsxTrapAPIpAddress

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the IP address of an access point for which for which the trap is being raised.

### wlsxTrapAPBSSID

<b>Syntax</b>	MacAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the BSSID of the access point for which we are raising the trap.

## wlsxTrapEssid

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the SSID of the access point, for which the trap is being raised.

## wlsxTrapTargetAPBSSID

<b>Syntax</b>	MacAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the BSSID of the access point, for which we are raising the trap. If an Air Monitor is sending the trap then this will indicate AP. If an access point is sending the trap, then it will point to itself.

## wlsxTrapTargetAPSSID

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the SSID of the access point, for which the trap is being raised. If an Air Monitor is sending the trap then this will indicate AP. If an access point is sending the trap, then it will point to itself.

## wlsxTrapTargetAPChannel

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the channel of the access point, for which the trap is being raised. If an wlsxr monitor is sending the trap then this will indicate AP. If an access point is sending the trap, then it will point to itself.



## wlsxTrapNodeMac

<b>Syntax</b>	MacAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the MAC address of a node.

## wlsxTrapSourceMac

<b>Syntax</b>	MacAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the MAC address of the source.

## wlsxReceiverMac

<b>Syntax</b>	MacAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the MAC address of the receiver.

## wlsxTrapTransmitterMac

<b>Syntax</b>	MacAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the MAC address of the transmitter.

## wlsxTrapReceiverMac

<b>Syntax</b>	MacAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the MAC address of the receiver.

## wlsxTrapSnr

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the signal-to-noise ratio.

## wlsxTrapSignatureName

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the signature name.

## wlsxTrapFrameType

<b>Syntax</b>	ArubaFrameType
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the frame type.

## wlsxTrapAddressType

<b>Syntax</b>	ArubaAddressType
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the address type.

## wlsxTrapAPLocation

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the location of the AP.

## wlsxTrapAPChannel

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the current channel.

## wlsxTrapAPTxPower

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the AP transmit power.

## wlsxTrapMatchedMac

<b>Syntax</b>	MacAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the MAC address.

## wlsxTrapMatchedIp

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the IP address.

## wlsxTrapRogueIfoURL

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used to point to the WEBUI Rogue AP information URL.

## wlsxTrapVLANId

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the VLAN ID.

## wlsxTrapAdminStatus

<b>Syntax</b>	ArubaEnableValue (INTEGER)
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the admin status of VLAN.

## wlsxTrapOperStatus

<b>Syntax</b>	ArubaOperStateValue
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the admin status of VLAN.

## wlsxTrapAuthServerName

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the authentication server used for authentication.

## wlsxTrapAuthServerTimeout

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the Authentication Server Timeout.

## wlsxTrapCardSlot

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the slot in which this card is present.

## wlsxTrapTemperatureValue

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the temperature value.

## wlsxTrapProcessName

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the process name.

## wlsxTrapFanNumber

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the fan number.

## wlsxTrapVoltageType

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the type of voltage.

## wlsxTrapVoltageValue

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the voltage value in float.

## wlsxTrapStationBlackListReason

<b>Syntax</b>	ArubaBlackListReason
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	The reason for which a station is black listed.

## wlsxTrapSpoofedIpAddress

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in a trap to identify a spoofed IP address.

## wlsxTrapSpoofedOldPhyAddress

<b>Syntax</b>	MacAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in a trap to identify an old MAC address.

## wlsxTrapSpoofedNewPhyAddress

<b>Syntax</b>	MacAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in a trap to identify a new MAC address.

## wlsxTrapDBName

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in a trap to identify the name of the database.

## wlsxTrapDBUserName

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in a trap to identify the name of the database user.

## wlsxTrapDBIpAddress

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in a trap to identify the IP address of the database.

## wlsxTrapDBType

<b>Syntax</b>	ArubaDBType
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in a trap to identify the port of the user.

## wlsxTrapVrrpID

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object contains the virtual router identifier.

## wlsxTrapVrrpMasterIp

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object contains the master IP address.

## wlsxTrapVrrpOperState

<b>Syntax</b>	ArubaVrrpState
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the VRRP operational state.

## wlsxTrapESIServerGrpName

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the External Services Interface (ESI) server group name.

## wlsxTrapESIServerName

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the External Services Interface (ESI) server name.

## wlsxTrapESIServerIpAddress

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the External Services Interface (ESI) server IP address.



## wlsxTrapLicenseDaysRemaining

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the number of days remaining prior to a license expiry.

## wlsxTrapSwitchIp

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the controller IP address.

## wlsxTrapSwitchRole

<b>Syntax</b>	ArubaSwitchRole
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the role of the controller.

## wlsxTrapUserIpAddress

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the IP address of the user.

## wlsxTrapUserPhyAddress

<b>Syntax</b>	MacAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the MAC address of the user.

## wlsxTrapUserName

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the user name.

## wlsxTrapUserRole

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the Authentication method of the user.

## wlsxTrapUserAuthenticationMethod

<b>Syntax</b>	ArubaAuthenticationMethods
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the Authentication method of the user.

## wlsxTrapAPRadioNumber

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the radio number.

## wlsxTrapRogueInfoURL

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used to point to the WEBGUI Rogue AP information URL.

## wlsxTrapInterferingAPIInfoURL

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used to point to the WEBGUI Rogue interfering access point information URL.

## wlsxTrapPortNumber

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the port number.

## wlsxTrapTime

<b>Syntax</b>	DateAndTime
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in all the enterprise traps to indicate the time when the trap is generated on the controller.

## wlsxTrapHostIp

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the trap host.

## wlsxTrapHostPort

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the trap host port.

## wlsxTrapConfigurationId

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	

## wlsxTrapCTSURL

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the URL from which the transfer should happen.

## wlsxTrapCTSTransferType

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the transfer type, upload or download.

## wlsxTrapConfigurationState

<b>Syntax</b>	ArubaConfigurationState (INTEGER)
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the state of the configuration transfer.

## wlsxTrapUpdateFailureReason

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the reason for the update failure.

## wlsxTrapUpdateFailedObj

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This variable represents the AMAPI object which is the reason for the update failure.

## wlsxTrapTableEntryChangeType

<b>Syntax</b>	ArubaConfigurationChangeType (INTEGER)
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the type of the configuration change.

## wlsxTrapGlobalConfigObj

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This variable represents the AMAPI object corresponding to the global configuration change.

## wlsxTrapTableGenNumber

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the generation number of a table. Used in the MMS to keep track of the table content changes.

## wlsxTrapLicenseId

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the license ID.

## wlsxTrapConfidenceLevel

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the confidence level as a percentage.

## wlsxTrapMissingLicenses

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This variable indicates any licenses that are not present during a configuration update.

## wlsxVoiceCurrentNumCdr

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the number of CDRs in buffer.

## wlsxTrapTunnelId

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the tunnel ID.

## wlsxTrapTunnelStatus

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the tunnel status.

## wlsxTrapTunnelUpReason

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the tunnel up reason.

## wlsxTrapTunnelDownReason

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the tunnel down reason.

## wlsxTrapApSerialNumber

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the AP serial number.

## wlsxTrapTimeStr

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the Time in String format.

## wlsxTrapMasterIp

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the master IP address.

## wlsxTrapLocalIp

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the local IP address.

## wlsxTrapMasterName

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the master controller name.

## wlsxTrapLocalName

<b>Syntax</b>	DisplayString(Size(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the local controller name.

## wlsxTrapPrimaryControllerIp

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the IP address of the AP's primary controller.

## wlsxTrapBackupControllerIp

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the IP address of the AP's backup controller.



## wlsxTrapSpoofedFrameType

<b>Syntax</b>	DisplayString (SIZE(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the Spoofed Frame Type

## wlsxTrapAssociationType

<b>Syntax</b>	DisplayString (SIZE(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the type of association.

## wlsxTrapDeviceIpAddress

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the IP address of a device seen by an AP.

## wlsxTrapDeviceMac

<b>Syntax</b>	MacAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the MAC address of a device seen by an AP.

## wlsxTrapVcIpAddress

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the IP Address of a Voice client.

## wlsxTrapVcMacAddress

<b>Syntax</b>	MacAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents the MAC address of a Voice client.

## wlsxTrapAPName

<b>Syntax</b>	DisplayString (SIZE(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the Name of the AP.

## wlsxTrapApMode

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	

## wlsxTrapAPPprevChannel

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the Previous Channel.

## wlsxTrapAPPprevChannelSec

<b>Syntax</b>	ArubaHTextChannel (INTEGER)
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the Previous Secondary Channel.

## wlsxTrapAPPprevTxPower

<b>Syntax</b>	Integer32
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate previous AP Transmit Power.

## wlsxTrapAPCurMode

<b>Syntax</b>	ArubaAccessPointMode (INTEGER)
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This Object represents the APs Current Mode.

## wlsxTrapAPPprevMode

<b>Syntax</b>	ArubaAccessPointMode (INTEGER)
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This Object represents the APs Previous Mode.

## wlsxTrapAPARMChangeReason

<b>Syntax</b>	ArubaARMChangeReason (INTEGER)
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This Object represents the APs Previous Mode.

## wlsxTrapAPChannelSec

<b>Syntax</b>	ArubaHTextChannel (INTEGER)
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the Current Secondary Channel.

## wlsxTrapUserAttributeChangeType

<b>Syntax</b>	ArubaConfigurationChangeType (INTEGER)
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object represents type of the configuration change.

## wlsxTrapAPControllerIp

<b>Syntax</b>	IpAddress
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	

## wlsxTrapApMasterStatus

<b>Syntax</b>	ArubaAPMasterStatus (INTEGER)
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	Status of the AP as seen by the master when the status changes.

## wlsxTrapCaName

<b>Syntax</b>	DisplayString (SIZE(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	

## wlsxTrapCrlName

<b>Syntax</b>	DisplayString (SIZE(0..64))
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This object is used in the traps to indicate the name of the CRL.

## wlsxTrapCount

**Syntax** Integer32

**Max-Access** accessible-for-notify

**Status** current

**Description**

## wlsxTrapAPPreviousUplinkType

**Syntax** ArubaAPUplinkType

**Max-Access** accessible-for-notify

**Status** current

**Description**

## wlsxTrapAPPreviousUplinkActiveTime

**Syntax** TimeTicks

**Max-Access** accessible-for-notify

**Status** current

**Description**

## wlsxTrapAPActiveUplinkType

**Syntax** ArubaAPUplinkType

**Max-Access** accessible-for-notify

**Status** current

**Description**

## wlsxTrapAPUplinkChangeReason

**Syntax** ArubaAPUplinkChangeReason

**Max-Access** accessible-for-notify

**Status** current

**Description**

## wlsxTrapAPManagedModeConfigFailure

**Syntax** DisplayString (SIZE(0..64))

**Max-Access** accessible-for-notify

**Status** current

**Description** This object indicates that the configuration application has failed on the AP.

## ai Traps Definitions Group

**Table 13:** ai Traps Definitions Group OIDs

Object	Object ID	Object ID
wlsxNUserEntryCreated	1.3.6.1.4.1.14823.2.3.3.1.200.2.1014	wlsxTrapDefinitionsGroup1014
wlsxNUserEntryDeleted	1.3.6.1.4.1.14823.2.3.3.1.200.2.1015	wlsxTrapDefinitionsGroup1015
wlsxNUserEntryAuthenticated	1.3.6.1.4.1.14823.2.3.3.1.200.2.1016	wlsxTrapDefinitionsGroup1016
wlsxNUserEntryDeAuthenticated	1.3.6.1.4.1.14823.2.3.3.1.200.2.1017	wlsxTrapDefinitionsGroup1017
wlsxNUserAuthenticationFailed	1.3.6.1.4.1.14823.2.3.3.1.200.2.1018	wlsxTrapDefinitionsGroup1018
wlsxNAuthServerReqTimedOut	1.3.6.1.4.1.14823.2.3.3.1.200.2.1019	wlsxTrapDefinitionsGroup1019
wlsxNAuthServerTimedOut	1.3.6.1.4.1.14823.2.3.3.1.200.2.1020	wlsxTrapDefinitionsGroup1020
wlsxNAuthServerIsUp	1.3.6.1.4.1.14823.2.3.3.1.200.2.1021	wlsxTrapDefinitionsGroup1021
wlsxNAccessPointsIsUp	1.3.6.1.4.1.14823.2.3.3.1.200.2.1040	wlsxTrapDefinitionsGroup1040
wlsxNAccessPointsIsDown	1.3.6.1.4.1.14823.2.3.3.1.200.2.1041	wlsxTrapDefinitionsGroup1041
wlsxNChannelChanged	1.3.6.1.4.1.14823.2.3.3.1.200.2.1043	wlsxTrapDefinitionsGroup1043
wlsxNStationAddedToBlackList	1.3.6.1.4.1.14823.2.3.3.1.200.2.1044	wlsxTrapDefinitionsGroup1044
wlsxNStationRemovedFromBlackList	1.3.6.1.4.1.14823.2.3.3.1.200.2.1045	wlsxTrapDefinitionsGroup1045
wlsxNRadioAttributesChanged	1.3.6.1.4.1.14823.2.3.3.1.200.2.1049	wlsxTrapDefinitionsGroup1049
wlsxUnsecureAPDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1053	wlsxTrapDefinitionsGroup1053
wlsxUnsecureAPResolved	1.3.6.1.4.1.14823.2.3.3.1.200.2.1054	wlsxTrapDefinitionsGroup1054
wlsxStalmpersonation	1.3.6.1.4.1.14823.2.3.3.1.200.2.1055	wlsxTrapDefinitionsGroup1055
wlsxReservedChannelViolation	1.3.6.1.4.1.14823.2.3.3.1.200.2.1056	wlsxTrapDefinitionsGroup1056
wlsxValidSSIDViolation	1.3.6.1.4.1.14823.2.3.3.1.200.2.1057	wlsxTrapDefinitionsGroup1057

Object	Object ID	Object ID
wlsxChannelMisconfiguration	1.3.6.1.4.1.14823.2.3.3.1.200.2.1058	wlsxTrapDefinitionsGroup1058
wlsxOUIMisconfiguration	1.3.6.1.4.1.14823.2.3.3.1.200.2.1059	wlsxTrapDefinitionsGroup1059
wlsxSSIDMisconfiguration	1.3.6.1.4.1.14823.2.3.3.1.200.2.1060	wlsxTrapDefinitionsGroup1060
wlsxShortPreamble Misconfiguration	1.3.6.1.4.1.14823.2.3.3.1.200.2.1061	wlsxTrapDefinitionsGroup1061
wlsxWPAMisconfiguration	1.3.6.1.4.1.14823.2.3.3.1.200.2.1062	wlsxTrapDefinitionsGroup1062
wlsxAdhocNetworkDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1063	wlsxTrapDefinitionsGroup1063
wlsxAdhocNetworkRemoved	1.3.6.1.4.1.14823.2.3.3.1.200.2.1064	wlsxTrapDefinitionsGroup1064
wlsxStaPolicyViolation	1.3.6.1.4.1.14823.2.3.3.1.200.2.1065	wlsxTrapDefinitionsGroup1065
wlsxRepeatWEPIVViolation	1.3.6.1.4.1.14823.2.3.3.1.200.2.1066	wlsxTrapDefinitionsGroup1066
wlsxWeakWEPIVViolation	1.3.6.1.4.1.14823.2.3.3.1.200.2.1067	wlsxTrapDefinitionsGroup1067
wlsxChannelInterference Detected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1068	wlsxTrapDefinitionsGroup1068
wlsxChannelInterference Cleared	1.3.6.1.4.1.14823.2.3.3.1.200.2.1069	wlsxTrapDefinitionsGroup1069
wlsxAPInterferenceDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1070	wlsxTrapDefinitionsGroup1070
wlsxAPInterferenceCleared	1.3.6.1.4.1.14823.2.3.3.1.200.2.1071	wlsxTrapDefinitionsGroup1071
wlsxStaInterferenceDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1072	wlsxTrapDefinitionsGroup1072
wlsxStaInterferenceCleared	1.3.6.1.4.1.14823.2.3.3.1.200.2.1073	wlsxTrapDefinitionsGroup1073
wlsxFrameRetryRateExceeded	1.3.6.1.4.1.14823.2.3.3.1.200.2.1074	wlsxTrapDefinitionsGroup1074
wlsxFrameReceiveErrorRate Exceeded	1.3.6.1.4.1.14823.2.3.3.1.200.2.1075	wlsxTrapDefinitionsGroup1075
wlsxFrameFragmentationRate Exceeded	1.3.6.1.4.1.14823.2.3.3.1.200.2.1076	wlsxTrapDefinitionsGroup1076
wlsxFrameBandWidthRate Exceeded	1.3.6.1.4.1.14823.2.3.3.1.200.2.1077	wlsxTrapDefinitionsGroup1077
wlsxFrameLowSpeedRate Exceeded	1.3.6.1.4.1.14823.2.3.3.1.200.2.1078	wlsxTrapDefinitionsGroup1078
wlsxFrameNonUnicastRate Exceeded	1.3.6.1.4.1.14823.2.3.3.1.200.2.1079	wlsxTrapDefinitionsGroup1079
wlsxLoadbalancingEnabled	1.3.6.1.4.1.14823.2.3.3.1.200.2.1080	wlsxTrapDefinitionsGroup1080
wlsxLoadbalancingDisabled	1.3.6.1.4.1.14823.2.3.3.1.200.2.1081	wlsxTrapDefinitionsGroup1081
wlsxChannelFrameRetryRate	1.3.6.1.4.1.14823.2.3.3.1.200.2.1082	wlsxTrapDefinitionsGroup1082

Object	Object ID	
Exceeded		
wlsxChannelFrame FragmentationRateExceeded	1.3.6.1.4.1.14823.2.3.3.1.200.2.1083	wlsxTrapDefinitionsGroup1083
wlsxChannelFrameErrorRate Exceeded	1.3.6.1.4.1.14823.2.3.3.1.200.2.1084	wlsxTrapDefinitionsGroup1084
wlsxSignatureMatchAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1085	wlsxTrapDefinitionsGroup1085
wlsxSignatureMatchSta	1.3.6.1.4.1.14823.2.3.3.1.200.2.1086	wlsxTrapDefinitionsGroup1086
wlsxChannelRateAnomaly	1.3.6.1.4.1.14823.2.3.3.1.200.2.1087	wlsxTrapDefinitionsGroup1087
wlsxNodeRateAnomaly	1.3.6.1.4.1.14823.2.3.3.1.200.2.1003	wlsxTrapDefinitionsGroup1003
wlsxNodeRateAnomalyAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1088	wlsxTrapDefinitionsGroup1088
wlsxNodeRateAnomalySta	1.3.6.1.4.1.14823.2.3.3.1.200.2.1089	wlsxTrapDefinitionsGroup1089
wlsxEAPRateAnomaly	1.3.6.1.4.1.14823.2.3.3.1.200.2.1090	wlsxTrapDefinitionsGroup1090
wlsxSignalAnomaly	1.3.6.1.4.1.14823.2.3.3.1.200.2.1091	wlsxTrapDefinitionsGroup1091
wlsxSequenceNumber AnomalyAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1092	wlsxTrapDefinitionsGroup1092
wlsxSequenceNumber AnomalySta	1.3.6.1.4.1.14823.2.3.3.1.200.2.1093	wlsxTrapDefinitionsGroup1093
wlsxDisconnectStationAttack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1094	wlsxTrapDefinitionsGroup1094
wlsxApFloodAttack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1095	wlsxTrapDefinitionsGroup1095
wlsxAdhocNetwork	1.3.6.1.4.1.14823.2.3.3.1.200.2.1096	wlsxTrapDefinitionsGroup1096
wlsxWirelessBridge	1.3.6.1.4.1.14823.2.3.3.1.200.2.1097	wlsxTrapDefinitionsGroup1097
wlsxInvalidMacOUIAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1098	wlsxTrapDefinitionsGroup1098
wlsxInvalidMacOUISta	1.3.6.1.4.1.14823.2.3.3.1.200.2.1099	wlsxTrapDefinitionsGroup1099
wlsxWEPMisconfiguration	1.3.6.1.4.1.14823.2.3.3.1.200.2.1100	wlsxTrapDefinitionsGroup1100
wlsxStaRepeatWEPIVViolation	1.3.6.1.4.1.14823.2.3.3.1.200.2.1101	wlsxTrapDefinitionsGroup1101
wlsxStaWeakWEPIVViolation	1.3.6.1.4.1.14823.2.3.3.1.200.2.1102	wlsxTrapDefinitionsGroup1102
wlsxStaAssociatedTo UnsecureAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1103	wlsxTrapDefinitionsGroup1103
wlsxStaUnAssociatedFrom UnsecureAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1104	wlsxTrapDefinitionsGroup1104
wlsxAdhocNetworkBridge Detected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1105	wlsxTrapDefinitionsGroup1105



Object	Object ID	Object ID
wlsxInterferingApDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1106	wlsxTrapDefinitionsGroup1106
wlsxColdStart	1.3.6.1.4.1.14823.2.3.3.1.200.2.1111	wlsxTrapDefinitionsGroup1111
wlsxWarmStart	1.3.6.1.4.1.14823.2.3.3.1.200.2.1112	wlsxTrapDefinitionsGroup1112
wlsxAPImpersonation	1.3.6.1.4.1.14823.2.3.3.1.200.2.1113	wlsxTrapDefinitionsGroup1113
wlsxNAAuthServerIsDown	1.3.6.1.4.1.14823.2.3.3.1.200.2.1115	wlsxTrapDefinitionsGroup1115
wlsxWindowsBridgeDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1129	wlsxTrapDefinitionsGroup1129
wlsxSignAPNetstumbler	1.3.6.1.4.1.14823.2.3.3.1.200.2.1134	wlsxTrapDefinitionsGroup1134
wlsxSignStaNetstumbler	1.3.6.1.4.1.14823.2.3.3.1.200.2.1135	wlsxTrapDefinitionsGroup1135
wlsxSignAPAsleep	1.3.6.1.4.1.14823.2.3.3.1.200.2.1136	wlsxTrapDefinitionsGroup1136
wlsxSignStaAsleep	1.3.6.1.4.1.14823.2.3.3.1.200.2.1137	wlsxTrapDefinitionsGroup1137
wlsxSignAPAirjack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1138	wlsxTrapDefinitionsGroup1138
wlsxSignStaAirjack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1139	wlsxTrapDefinitionsGroup1139
wlsxSignAPNullProbeResp	1.3.6.1.4.1.14823.2.3.3.1.200.2.1140	wlsxTrapDefinitionsGroup1140
wlsxSignStaNullProbeResp	1.3.6.1.4.1.14823.2.3.3.1.200.2.1141	wlsxTrapDefinitionsGroup1141
wlsxSignAPDeauthBcast	1.3.6.1.4.1.14823.2.3.3.1.200.2.1142	wlsxTrapDefinitionsGroup1142
wlsxSignStaDeauthBcast	1.3.6.1.4.1.14823.2.3.3.1.200.2.1143	wlsxTrapDefinitionsGroup1143
wlsxWindowsBridgeDetectedAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1144	wlsxTrapDefinitionsGroup1144
wlsxWindowsBridgeDetectedSta	1.3.6.1.4.1.14823.2.3.3.1.200.2.1145	wlsxTrapDefinitionsGroup1145
wlsxAdhocNetworkBridge DetectedAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1146	wlsxTrapDefinitionsGroup1146
wlsxAdhocNetworkBridge DetectedSta	1.3.6.1.4.1.14823.2.3.3.1.200.2.1147	wlsxTrapDefinitionsGroup1147
wlsxDisconnectStationAttackAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1148	wlsxTrapDefinitionsGroup1148
wlsxDisconnectStationAttackSta	1.3.6.1.4.1.14823.2.3.3.1.200.2.1149	wlsxTrapDefinitionsGroup1149
wlsxSuspectUnsecureAP Detected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1150	wlsxTrapDefinitionsGroup1150
wlsxSuspectUnsecureAP Resolved	1.3.6.1.4.1.14823.2.3.3.1.200.2.1151	wlsxTrapDefinitionsGroup1151
wlsxHtGreenfieldSupported	1.3.6.1.4.1.14823.2.3.3.1.200.2.1157	wlsxTrapDefinitionsGroup1157
wlsxHT40MHzIntoleranceAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1158	wlsxTrapDefinitionsGroup1158

Object	Object ID	Object ID
wlsxHT40MHzIntoleranceSta	1.3.6.1.4.1.14823.2.3.3.1.200.2.1159	wlsxTrapDefinitionsGroup1159
wlsxNAdhocNetwork	1.3.6.1.4.1.14823.2.3.3.1.200.2.1161	wlsxTrapDefinitionsGroup1161
wlsxNAdhocNetworkBridge DetectedAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1162	wlsxTrapDefinitionsGroup1162
wlsxNAdhocNetworkBridge DetectedSta	1.3.6.1.4.1.14823.2.3.3.1.200.2.1163	wlsxTrapDefinitionsGroup1163
wlsxClientFloodAttack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1170	wlsxTrapDefinitionsGroup1170
wlsxValidClientNotUsing Encryption	1.3.6.1.4.1.14823.2.3.3.1.200.2.1171	wlsxTrapDefinitionsGroup1171
wlsxAdhocUsingValidSSID	1.3.6.1.4.1.14823.2.3.3.1.200.2.1172	wlsxTrapDefinitionsGroup1172
wlsxAPSpooftingDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1173	wlsxTrapDefinitionsGroup1173
wlsxClientAssociatingOn WrongChannel	1.3.6.1.4.1.14823.2.3.3.1.200.2.1174	wlsxTrapDefinitionsGroup1174
wlsxNDisconnectStationAttack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1175	wlsxTrapDefinitionsGroup1175
wlsxNStaUnAssociatedFrom UnsecureAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1176	wlsxTrapDefinitionsGroup1176
wlsxOmertaAttack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1177	wlsxTrapDefinitionsGroup1177
wlsxTKIPReplayAttack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1178	wlsxTrapDefinitionsGroup1178
wlsxChopChopAttack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1179	wlsxTrapDefinitionsGroup1179
wlsxFataJackAttack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1180	wlsxTrapDefinitionsGroup1180
wlsxInvalidAddress Combination	1.3.6.1.4.1.14823.2.3.3.1.200.2.1181	wlsxTrapDefinitionsGroup1181
wlsxValidClientMisassociation	1.3.6.1.4.1.14823.2.3.3.1.200.2.1182	wlsxTrapDefinitionsGroup1182
wlsxMalformedHTIEDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1183	wlsxTrapDefinitionsGroup1183
wlsxMalformedAssocReq Detected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1184	wlsxTrapDefinitionsGroup1184
wlsxOverflowIEDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1185	wlsxTrapDefinitionsGroup1185
wlsxOverflowEAPOLKey Detected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1186	wlsxTrapDefinitionsGroup1186
wlsxMalformedFrameLarge DurationDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1187	wlsxTrapDefinitionsGroup1187
wlsxMalformedFrameWrong ChannelDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1188	wlsxTrapDefinitionsGroup1188

Object	Object ID	Object ID
wlsxMalformedAuthFrame	1.3.6.1.4.1.14823.2.3.3.1.200.2.1189	wlsxTrapDefinitionsGroup1189
wlsxCTSRateAnomaly	1.3.6.1.4.1.14823.2.3.3.1.200.2.1190	wlsxTrapDefinitionsGroup1190
wlsxRTSRateAnomaly	1.3.6.1.4.1.14823.2.3.3.1.200.2.1191	wlsxTrapDefinitionsGroup1191
wlsxNRogueAPDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1192	wlsxTrapDefinitionsGroup1192
wlsxNRogueAPResolved	1.3.6.1.4.1.14823.2.3.3.1.200.2.1193	wlsxTrapDefinitionsGroup1193
wlsxNeighborAPDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1194	wlsxTrapDefinitionsGroup1194
wlsxNInterferingAPDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1195	wlsxTrapDefinitionsGroup1195
wlsxNSuspectRogueAP Detected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1196	wlsxTrapDefinitionsGroup1196
wlsxNSuspectRogueAP Resolved	1.3.6.1.4.1.14823.2.3.3.1.200.2.1197	wlsxTrapDefinitionsGroup1197
wlsxBlockAckAttackDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1198	wlsxTrapDefinitionsGroup1198
wlsxHotspotterAttackDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1199	wlsxTrapDefinitionsGroup1199
wlsxNSignatureMatch	1.3.6.1.4.1.14823.2.3.3.1.200.2.1200	wlsxTrapDefinitionsGroup1200
wlsxNSignatureMatch Netstumbler	1.3.6.1.4.1.14823.2.3.3.1.200.2.1201	wlsxTrapDefinitionsGroup1201
wlsxNSignatureMatchAsleep	1.3.6.1.4.1.14823.2.3.3.1.200.2.1202	wlsxTrapDefinitionsGroup1202
wlsxNSignatureMatchAirjack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1203	wlsxTrapDefinitionsGroup1203
wlsxNSignatureMatchNull ProbeResp	1.3.6.1.4.1.14823.2.3.3.1.200.2.1204	wlsxTrapDefinitionsGroup1204
wlsxNSignatureMatchDeath Bcast	1.3.6.1.4.1.14823.2.3.3.1.200.2.1205	wlsxTrapDefinitionsGroup1205
wlsxNSignatureMatchDisassoc Bcast	1.3.6.1.4.1.14823.2.3.3.1.200.2.1206	wlsxTrapDefinitionsGroup1206
wlsxNSignatureMatch Wellenreiter	1.3.6.1.4.1.14823.2.3.3.1.200.2.1207	wlsxTrapDefinitionsGroup1207
wlsxAPDeathContainment	1.3.6.1.4.1.14823.2.3.3.1.200.2.1208	wlsxTrapDefinitionsGroup1208
wlsxClientDeathContainment	1.3.6.1.4.1.14823.2.3.3.1.200.2.1209	wlsxTrapDefinitionsGroup1209
wlsxAPWiredContainment	1.3.6.1.4.1.14823.2.3.3.1.200.2.1210	wlsxTrapDefinitionsGroup1210
wlsxClientWiredContainment	1.3.6.1.4.1.14823.2.3.3.1.200.2.1211	wlsxTrapDefinitionsGroup1211
wlsxAPTaggedWired Containment	1.3.6.1.4.1.14823.2.3.3.1.200.2.1212	wlsxTrapDefinitionsGroup1212
wlsxClientTaggedWired	1.3.6.1.4.1.14823.2.3.3.1.200.2.1213	wlsxTrapDefinitionsGroup1213

Object	Object ID	
Containment		
wlsxTarpitContainment	1.3.6.1.4.1.14823.2.3.3.1.200.2.1214	wlsxTrapDefinitionsGroup1214
wlsxAPChannelChange	1.3.6.1.4.1.14823.2.3.3.1.200.2.1216	wlsxTrapDefinitionsGroup1216
wlsxAPPowerChange	1.3.6.1.4.1.14823.2.3.3.1.200.2.1217	wlsxTrapDefinitionsGroup1217
wlsxAPModeChange	1.3.6.1.4.1.14823.2.3.3.1.200.2.1218	wlsxTrapDefinitionsGroup1218
wlsxUserEntryAttributes Changed	1.3.6.1.4.1.14823.2.3.3.1.200.2.1219	wlsxTrapDefinitionsGroup1219
wlsxPowerSaveDosAttack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1220	wlsxTrapDefinitionsGroup1220
wlsxNAPMasterStatusChange	1.3.6.1.4.1.14823.2.3.3.1.200.2.1221	wlsxTrapDefinitionsGroup1221
wlsxNAdhocUsingValidSSID	1.3.6.1.4.1.14823.2.3.3.1.200.2.1222	wlsxTrapDefinitionsGroup1222
wlsxMgmtUserAuthentication Failed	1.3.6.1.4.1.14823.2.3.3.1.200.2.1224	wlsxTrapDefinitionsGroup1224

### wlsxNUserEntryCreated

<b>Objects</b>	wlsxTrapTime, wlsxTrapUserIpAddress, wlsxTrapUserPhyAddress
<b>Status</b>	current
<b>Description</b>	This trap indicates that a new user was created.

### wlsxNUserEntryDeleted

<b>Objects</b>	wlsxTrapTime, wlsxTrapUserIpAddress, wlsxTrapUserPhyAddress
<b>Status</b>	current
<b>Description</b>	This trap indicates that a user was deleted.

### wlsxNUserEntryAuthenticated

<b>Objects</b>	wlsxTrapTime, wlsxTrapUserIpAddress, wlsxTrapUserPhyAddress, wlsxTrapUserName, wlsxTrapUserAuthentication Method, wlsxTrapUserRole
<b>Status</b>	current
<b>Description</b>	This trap indicates that a user is Authenticated.

### wlsxNUserEntryDeAuthenticated

<b>Objects</b>	wlsxTrapTime, wlsxTrapUserIpAddress, wlsxTrapUserPhyAddress
<b>Status</b>	current
<b>Description</b>	This trap indicates that a user is Deauthenticated.

## wlsxNUserAuthenticationFailed

<b>Objects</b>	wlsxTrapTime, wlsxTrapUserIpAddress, wlsxTrapUserPhyAddress
<b>Status</b>	current
<b>Description</b>	This trap indicates that a user authentication has failed.

## wlsxNAuthServerReqTimedOut

<b>Objects</b>	wlsxTrapTime, wlsxTrapAuthServerName
<b>Status</b>	current
<b>Description</b>	This trap indicates that the authentication server request timed out.

## wlsxNAuthServerTimedOut

<b>Objects</b>	wlsxTrapTime, wlsxTrapAuthServerName, wlsxTrapAuthServerTimeout
<b>Status</b>	current
<b>Description</b>	This trap indicates that the authentication server timed out.

## wlsxNAuthServerIsUp

<b>Objects</b>	wlsxTrapTime, wlsxTrapAuthServerName
<b>Status</b>	current
<b>Description</b>	This trap indicates that an authentication server is up.

## wlsxNAccessPointIsUp

<b>Objects</b>	wlsxTrapTime, wlsxTrapAPMacAddress
<b>Status</b>	current
<b>Description</b>	A Trap which indicates that an access point up.

## wlsxNAccessPointIsDown

<b>Objects</b>	wlsxTrapTime, wlsxTrapAPMacAddress
<b>Status</b>	current
<b>Description</b>	A Trap which indicates that an access point down.

## wlsxNChannelChanged

<b>Objects</b>	wlsxTrapTime, wlsxTrapAPBSSID, wlsxTrapAPLocation, wlsxTrapAPChannel
<b>Status</b>	current
<b>Description</b>	This trap indicates that an access point at Location wlsxTrapAPLocation has changed the channel.

## wlsxNStationAddedToBlackList

<b>Objects</b>	wlsxTrapTime, wlsxTrapNodeMac, wlsxTrapStationBlackListReason
<b>Status</b>	current
<b>Description</b>	This trap indicates that the station is black listed.

## wlsxNStationRemovedFromBlackList

<b>Objects</b>	wlsxTrapTime, wlsxTrapNodeMac
<b>Status</b>	current
<b>Description</b>	This trap indicates that the station is removed from the black list. the frame type.

## wlsxNRadioAttributesChanged

<b>Objects</b>	{wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPIpAddress, wlsxTrapAPChannel, wlsxTrapAPTxFPower }
<b>Status</b>	current
<b>Description</b>	A Trap which indicates changes in the Radio attributes of an access point.

## wlsxUnsecureAPDetected

<b>Objects</b>	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel, wlsxTrapMatchedMac, wlsxTrapMatchedIp, wlsxTrapRogueInfoURL}
<b>Status</b>	current
<b>Description</b>	This trap indicates that an unauthorized access point is connected to the wired network. The access point is declared Rogue because it was matched to a MAC address.

## wlsxUnsecureAPResolved

<b>Objects</b>	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	This trap indicates that a previously detected access point, classified as Rogue, is no longer present in the network.

## wlsxStalImpersonation

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapNodeMac, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AM detected Station Impersonation.

## wlsxReservedChannelViolation

<b>Objects</b>	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AM detected an access point which is violating the Reserved Channel configuration.

## wlsxValidSSIDViolation

<b>Objects</b>	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP has detected an access point is violating Valid SSID configuration by using an SSID that is reserved for use by a valid AP only.

## wlsxChannelMisconfiguration

<b>Objects</b>	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected an access point that has a channel misconfiguration because it is using a channel that is not valid.

## wlsxOUIMisconfiguration

<b>Objects</b>	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected an access point that has an OUI misconfiguration because it is using an OUI that is not valid.

## wlsxSSIDMisconfiguration

<b>Objects</b>	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected an access point that has an SSID misconfiguration because it is using an SSID that is not valid.

## wlsxShortPreambleMisconfiguration

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an access point has bad short preamble configuration.

## wlsxWPAMisconfiguration

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected an access point that is misconfigured because it is not using WPA.

## wlsxAdhocNetworkDetected

<b>Objects</b>	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AM has detected an adhoc network.



## wlsxAdhocNetworkRemoved

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	This trap indicates that a previously detected adhoc network is no longer present in the network.

## wlsxStaPolicyViolation

<b>Objects</b>	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapNodeMac, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	This trap indicates that Protection was enforced because a valid station's association to a non-valid access point violated Valid Station policy. For more information check <a href="http://www.wve.org/entries/show/WVE-2005-0008">http://www.wve.org/entries/show/WVE-2005-0008</a> and <a href="http://www.wve.org/entries/show/WVE-2005-0019">http://www.wve.org/entries/show/WVE-2005-0019</a> .

## wlsxRepeatWEPIVViolation

<b>Objects</b>	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected that a valid access point is using the same WEP initialization vector in consecutive packets.

## wlsxWeakWEPIVViolation

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel}
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected that a valid access point is using a Weak WEP initialization vector. For more information check <a href="http://www.wve.org/entries/show/WVE-2005-0021">http://www.wve.org/entries/show/WVE-2005-0021</a>

## wlsxChannelInterferenceDetected

<b>Objects</b>	{wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel}
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP has detected channel interference.

## wlsxChannelInterferenceCleared

<b>Objects</b>	{wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel}
<b>Status</b>	current
<b>Description</b>	This trap indicates that a previously detected channel interference is no longer present.

## wlsxAPIInterferenceDetected

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP has detected interference for an access point.

## wlsxAPIInterferenceCleared

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	This trap indicates that the previously detected interference for an access point is no longer present.

## wlsxStaInterferenceDetected

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapNodeMac, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP has detected interference for a station.

## wlsxStaInterferenceCleared

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapNodeMac, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	This trap indicates that the previously detected interference for a station is no longer present.

## wlsxFrameRetryRateExceeded

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected that an access point has exceeded the configured upper threshold for Frame Retry Rate.

## wlsxFrameReceiveErrorRateExceeded

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapTargetAPChannel, wlsxTrapAPLocation }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected that an access point has exceeded the configured upper threshold for Frame Receive Error Rate.

## wlsxFrameFragmentationRateExceeded

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapTargetAPChannel, wlsxTrapAPLocation }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected that an access point exceeded the configured upper threshold for Frame Fragmentation Rate.

## wlsxFrameBandWidthRateExceeded

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapNodeMac, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected that a station or access point has exceeded the configured upper threshold for Bandwidth rate.

## wlsxFrameLowSpeedRateExceeded

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapNodeMac, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected that a station has exceeded the configured upper threshold for Low speed rate.

## wlsxFrameNonUnicastRateExceeded

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapNodeMac, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel}
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected that station has exceeded the configured upper threshold for Non Unicast traffic rate.

## wlsxLoadbalancingEnabled

<b>Objects</b>	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	

## wlsxLoadbalancingDisabled

<b>Objects</b>	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AM is reporting that an AP has enabled Load balancing.

## wlsxChannelFrameRetryRateExceeded

<b>Objects</b>	{wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel}
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP has detected that the configured upper threshold for Frame Retry Rate was exceeded on a channel.

## wlsxChannelFrameFragmentationRateExceeded

<b>Objects</b>	{wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel}
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP has detected that the configured upper threshold for Frame Fragmentation Rate was exceeded on a channel.

## wlsxChannelFrameErrorRateExceeded

<b>Objects</b>	{wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel}
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP has detected that the configured upper threshold for Frame Receive Error Rate was exceeded on a channel.

## wlsxSignatureMatchAP

<b>Objects</b>	{wlsxTrapTime, wlsxTrapSignatureName, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation}
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a signature match in a frame from an access point.

## wlsxSignatureMatchSta

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapSignatureName, wlsxTrapSourceMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a signature match in a frame from a Station.

## wlsxChannelRateAnomaly

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapFrameType, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected frames on a channel which exceed the configured IDS rate threshold. For more information check: <a href="http://www.wve.org/entries/show/WVE-2005-0052">http://www.wve.org/entries/show/WVE-2005-0052</a> <a href="http://www.wve.org/entries/show/WVE-2005-0045">http://www.wve.org/entries/show/WVE-2005-0045</a> <a href="http://www.wve.org/entries/show/WVE-2005-0046">http://www.wve.org/entries/show/WVE-2005-0046</a> <a href="http://www.wve.org/entries/show/WVE-2005-0047">http://www.wve.org/entries/show/WVE-2005-0047</a> <a href="http://www.wve.org/entries/show/WVE-2005-0048">http://www.wve.org/entries/show/WVE-2005-0048</a>

## wlsxNodeRateAnomaly

<b>Objects</b>	wlsxTrapTime, wlsxTrapFrameType, wlsxTrapNodeMac, wlsxTrapSnr, wlsxTrapAPBSSID, wlsxTrapAPLocation
<b>Status</b>	current
<b>Description</b>	This trap indicates that a node is exceeding the threshold set for the frame type.

## wlsxNodeRateAnomalyAP

<b>Objects</b>	{wlsxTrapTime, wlsxTrapFrameType, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation}
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected frames transmitted or received by an access point, which exceed the configured IDS rate threshold. For more information check: <a href="http://www.wve.org/entries/show/WVE-2005-0052">http://www.wve.org/entries/show/WVE-2005-0052</a> <a href="http://www.wve.org/entries/show/WVE-2005-0045">http://www.wve.org/entries/show/WVE-2005-0045</a> <a href="http://www.wve.org/entries/show/WVE-2005-0046">http://www.wve.org/entries/show/WVE-2005-0046</a> <a href="http://www.wve.org/entries/show/WVE-2005-0047">http://www.wve.org/entries/show/WVE-2005-0047</a> <a href="http://www.wve.org/entries/show/WVE-2005-0048">http://www.wve.org/entries/show/WVE-2005-0048</a>

## wlsxNodeRateAnomalySta

<b>Objects</b>	{wlsxTrapTime, wlsxTrapFrameType, wlsxTrapNodeMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation}
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected frames transmitted or received by a node, which exceed the configured IDS rate threshold.

## wlsxEAPRateAnomaly

<b>Objects</b>	{wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel}
<b>Status</b>	current
<b>Description</b>	This trap indicates that the rate of EAP Handshake packets received by an AP has exceeded the configured IDS EAP Handshake rate threshold. For more information check <a href="http://www.wve.org/entries/show/WVE-2005-0049">http://www.wve.org/entries/show/WVE-2005-0049</a>

## wlsxSignalAnomaly

<b>Objects</b>	{wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AM detected a Signal Anomaly.

## wlsxSequenceNumberAnomalyAP

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation }
<b>Status</b>	current
<b>Description</b>	<p>This trap indicates that an AM received packets from an AP which exceeds the acceptable sequence number difference. The acceptable sequence number difference is an IDS configuration object.</p> <p>For more information check: <a href="http://www.wve.org/entries/show/WVE-2005-0061">http://www.wve.org/entries/show/WVE-2005-0061</a> <a href="http://www.wve.org/entries/show/WVE-2005-0019">http://www.wve.org/entries/show/WVE-2005-0019</a> <a href="http://www.wve.org/entries/show/WVE-2005-0008">http://www.wve.org/entries/show/WVE-2005-0008</a> <a href="http://www.wve.org/entries/show/WVE-2005-0045">http://www.wve.org/entries/show/WVE-2005-0045</a> <a href="http://www.wve.org/entries/show/WVE-2005-0046">http://www.wve.org/entries/show/WVE-2005-0046</a> <a href="http://www.wve.org/entries/show/WVE-2005-0047">http://www.wve.org/entries/show/WVE-2005-0047</a> <a href="http://www.wve.org/entries/show/WVE-2005-0048">http://www.wve.org/entries/show/WVE-2005-0048</a></p>

## wlsxSequenceNumberAnomalySta

<b>Objects</b>	wlsxTrapTime, wlsxTrapSourceMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation
<b>Status</b>	current
<b>Description</b>	<p>This trap indicates that an AM received packets from a Node which exceeds the acceptable sequence number difference. The acceptable sequence number difference is an IDS configuration object.</p> <p>For more information check: <a href="http://www.wve.org/entries/show/WVE-2005-0061">http://www.wve.org/entries/show/WVE-2005-0061</a> <a href="http://www.wve.org/entries/show/WVE-2005-0019">http://www.wve.org/entries/show/WVE-2005-0019</a> <a href="http://www.wve.org/entries/show/WVE-2005-0008">http://www.wve.org/entries/show/WVE-2005-0008</a> <a href="http://www.wve.org/entries/show/WVE-2005-0045">http://www.wve.org/entries/show/WVE-2005-0045</a> <a href="http://www.wve.org/entries/show/WVE-2005-0046">http://www.wve.org/entries/show/WVE-2005-0046</a> <a href="http://www.wve.org/entries/show/WVE-2005-0047">http://www.wve.org/entries/show/WVE-2005-0047</a> <a href="http://www.wve.org/entries/show/WVE-2005-0048">http://www.wve.org/entries/show/WVE-2005-0048</a></p>

## wlsxDisconnectStationAttack

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapFrameType, wlsxTrapSourceMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation }
<b>Status</b>	current
<b>Description</b>	<p>This trap indicates that an AM detected a station Disconnect attack.</p> <p>For more information check: <a href="http://www.wve.org/entries/show/WVE-2005-0045">http://www.wve.org/entries/show/WVE-2005-0045</a> <a href="http://www.wve.org/entries/show/WVE-2005-0046">http://www.wve.org/entries/show/WVE-2005-0046</a> <a href="http://www.wve.org/entries/show/WVE-2005-0048">http://www.wve.org/entries/show/WVE-2005-0048</a></p>

## wlsxApFloodAttack

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation}
<b>Status</b>	current
<b>Description</b>	This trap indicates that the number of potential fake APs detected by an AP has exceeded the configured IDS threshold. This is the total number of fake APs observed across all bands. For more information check <a href="http://www.wve.org/entries/show/WVE-2005-0056">http://www.wve.org/entries/show/WVE-2005-0056</a>

## wlsxAdhocNetwork

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapSourceMac, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AM detected an Adhoc Network. A station is connected to an adhoc AP.

## wlsxWirelessBridge

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapTransmitterMac, wlsxTrapReceiverMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation}
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a Wireless Bridge when a WDS frame was seen between the transmitter and receiver addresses.

## wlsxInvalidMacOUIAP

<b>Objects</b>	{wlsxTrapTime, wlsxTrapAddressType, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation}
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected an invalid MAC OUI in the BSSID of a frame. An invalid MAC OUI suggests that the frame may be spoofed.

## wlsxInvalidMacOUISta

<b>Objects</b>	{wlsxTrapTime, wlsxTrapAddressType, wlsxTrapNodeMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation}
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected an invalid MAC OUI in the SRC or DST address of a frame. An invalid MAC OUI suggests that the frame may be spoofed.



## wlsxWEPMisconfiguration

<b>Objects</b>	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel}
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected an access point that is misconfigured because it does not have Privacy enabled.

## wlsxStaRepeatWEPIVViolation

<b>Objects</b>	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapNodeMac, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel}
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected that a valid station is using the same WEP initialization vector in consecutive packets.

## wlsxStaWeakWEPIVViolation

<b>Objects</b>	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapNodeMac, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel}
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected that a valid station is using a Weak WEP initialization vector.

## wlsxStaAssociatedToUnsecureAP

<b>Objects</b>	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapNodeMac, wlsxTrapAPLocation, wlsxTrapAPChannel, wlsxTrapRogueInfoURL}
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AM detected a client associated with a Rogue access point.

## wlsxStaUnAssociatedFromUnsecureAP

<b>Objects</b>	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapNodeMac}
<b>Status</b>	current
<b>Description</b>	This trap indicates that a previously detected rogue access point association is no longer present.

## wlsxAdhocNetworkBridgeDetected

<b>Objects</b>	{wlsxTrapTime, wlsxTrapSourceMac, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AM has detected an Adhoc network that is bridging to a wired network.

## wlsxInterferingApDetected

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel, wlsxTrapInterferingAPIInfoURL }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected an access point classified as Interfering. The access point is declared Interfering because it is neither authorized nor classified as Rogue.

## wlsxColdStart

<b>Objects</b>	wlsxTrapTime
<b>Status</b>	current
<b>Description</b>	An enterprise version of cold start trap, which contains the controller time stamp.

## wlsxWarmStart

<b>Objects</b>	wlsxTrapTime
<b>Status</b>	current
<b>Description</b>	An enterprise version of warm start trap, which contains the controller time stamp.

## wlsxAPImpersonation

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected AP Impersonation because the number of beacons seen has exceeded the expected number by the configured percentage threshold. The expected number is calculated based on the Beacon Interval Field in the Beacon frame.

## wlsxNAuthServerIsDown

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapAuthServerName }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an authentication server is down.

## wlsxWindowsBridgeDetected

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapSourceMac, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AM has detected a station that is bridging from a wireless network to a wired network.

## wlsxSignAPNetstumbler

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapSignatureName, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a signature match for Netstumbler from an access point. For more information check <a href="http://www.wve.org/entries/show/WVE-2005-0025">http://www.wve.org/entries/show/WVE-2005-0025</a>

## wlsxSignStaNetstumbler

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapSignatureName, wlsxTrapSourceMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a signature match for Netstumbler from a Station. For more information check <a href="http://www.wve.org/entries/show/WVE-2005-0025">http://www.wve.org/entries/show/WVE-2005-0025</a> .

## wlsxSignAPAsleap

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapSignatureName, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a signature match for ASLEAP from an access point. For more information check <a href="http://www.wve.org/entries/show/WVE-2005-0027">http://www.wve.org/entries/show/WVE-2005-0027</a>

## wlsxSignStaAsleap

<b>Objects</b>	{wlsxTrapTime, wlsxTrapSignatureName, wlsxTrapSourceMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation}
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a signature match for ASLEAP from a Station. For more information check <a href="http://www.wve.org/entries/show/WVE-2005-0027">http://www.wve.org/entries/show/WVE-2005-0027</a>

## wlsxSignAPAirjack

<b>Objects</b>	{wlsxTrapTime, wlsxTrapSignatureName, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a signature match for AirJack from an access point. For more information check <a href="http://www.wve.org/entries/show/WVE-2005-0018">http://www.wve.org/entries/show/WVE-2005-0018</a>

## wlsxSignStaAirjack

<b>Objects</b>	{wlsxTrapTime, wlsxTrapSignatureName, wlsxTrapSourceMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation}
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a signature match for AirJack from a Station. For more information check <a href="http://www.wve.org/entries/show/WVE-2005-0018">http://www.wve.org/entries/show/WVE-2005-0018</a>

## wlsxSignAPNullProbeResp

<b>Objects</b>	{wlsxTrapTime, wlsxTrapSignatureName, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation}
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a signature match for Null-Probe-Response from an access point. For more information check <a href="http://www.wve.org/entries/show/WVE-2006-0064">http://www.wve.org/entries/show/WVE-2006-0064</a>

## wlsxSignStaNullProbeResp

<b>Objects</b>	{wlsxTrapTime, wlsxTrapSignatureName, wlsxTrapSourceMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation}
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a signature match for Null-Probe-Response from a Station. For more information check <a href="http://www.wve.org/entries/show/WVE-2006-0064">http://www.wve.org/entries/show/WVE-2006-0064</a>

## wlsxSignAPDeathBcast

<b>Objects</b>	{wlsxTrapTime, wlsxTrapSignatureName, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation}
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a signature match for Death-Broadcast from an access point. For more information check: <a href="http://www.wve.org/entries/show/WVE-2005-0019">http://www.wve.org/entries/show/WVE-2005-0019</a> <a href="http://www.wve.org/entries/show/WVE-2005-0045">http://www.wve.org/entries/show/WVE-2005-0045</a>

## wlsxSignStaDeathBcast

<b>Objects</b>	{wlsxTrapTime, wlsxTrapSignatureName, wlsxTrapSourceMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation}
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a signature match for Death-Broadcast from a Station. For more information check: <a href="http://www.wve.org/entries/show/WVE-2005-0019">http://www.wve.org/entries/show/WVE-2005-0019</a> <a href="http://www.wve.org/entries/show/WVE-2005-0045">http://www.wve.org/entries/show/WVE-2005-0045</a>

## wlsxWindowsBridgeDetectedAP

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP is detecting an access point that is bridging from a wireless network to a wired network.

## wlsxWindowsBridgeDetectedSta

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapSourceMac, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP is detecting a station that is bridging from a wireless network to a wired network.

## wlsxAdhocNetworkBridgeDetectedAP

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AM has detected an adhoc network that is bridging to a wired network

## wlsxAdhocNetworkBridgeDetectedSta

<b>Objects</b>	wlsxTrapTime, wlsxTrapSourceMac, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AM has detected an adhoc network that is bridging to a wired network

## wlsxDisconnectStationAttackAP

<b>Objects</b>	{wlsxTrapTime, wlsxTrapFrameType, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation}
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AM detected a station Disconnect attack. For more information check: <a href="http://www.wve.org/entries/show/WVE-2005-0045">http://www.wve.org/entries/show/WVE-2005-0045</a> <a href="http://www.wve.org/entries/show/WVE-2005-0046">http://www.wve.org/entries/show/WVE-2005-0046</a> <a href="http://www.wve.org/entries/show/WVE-2005-0048">http://www.wve.org/entries/show/WVE-2005-0048</a>

## wlsxDisconnectStationAttackSta

<b>Objects</b>	wlsxTrapTime, wlsxTrapFrameType, wlsxTrapSourceMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AM detected a station Disconnect attack. For more information check: <a href="http://www.wve.org/entries/show/WVE-2005-0045">http://www.wve.org/entries/show/WVE-2005-0045</a> <a href="http://www.wve.org/entries/show/WVE-2005-0046">http://www.wve.org/entries/show/WVE-2005-0046</a> <a href="http://www.wve.org/entries/show/WVE-2005-0048">http://www.wve.org/entries/show/WVE-2005-0048</a>

## wlsxSuspectUnsecureAPDetected

<b>Objects</b>	{wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPRadioNumber, wlsxTrapMatchedMac, wlsxTrapMatchedIp, wlsxTrapConfidenceLevel, wlsxTrapAPLocation, wlsxTrapRogueInfoURL}
<b>Status</b>	current
<b>Description</b>	This trap indicates that an access point, classified as Suspected Rogue, has been detected by a Controller. The AP is suspected to be rogue, with the supplied confidence level, because it was matched to the wired MAC address.

## wlsxSuspectUnsecureAPResolved

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPRadioNumber
<b>Status</b>	current
<b>Description</b>	This trap indicates that a previously detected access point, classified Suspected Rogue, is either no longer present in the network or has changed its state.

### wlsxHtGreenfieldSupported

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected an access point that supports HT Greenfield mode. For more information check <a href="http://www.wve.org/entries/show/WVE-2008-0005">http://www.wve.org/entries/show/WVE-2008-0005</a>

### wlsxHT40MHzIntoleranceAP

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP is detecting an access point with the HT 40MHz intolerance setting. For more information check <a href="http://www.wve.org/entries/show/WVE-2008-0004">http://www.wve.org/entries/show/WVE-2008-0004</a>

### wlsxHT40MHzIntoleranceSta

<b>Objects</b>	{wlsxTrapTime, wlsxTrapSourceMac, wlsxTrapSnr, wlsxTrapAPChannel, wlsxTrapFrameType, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation}
<b>Status</b>	current
<b>Description</b>	This trap indicates that the system is detecting an HT 40MHz Intolerance setting from a Station. For more information check <a href="http://www.wve.org/entries/show/WVE-2008-0004">http://www.wve.org/entries/show/WVE-2008-0004</a>

### wlsxNAdhocNetwork

<b>Objects</b>	{wlsxTrapTime, wlsxTrapSourceMac, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel}
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected an adhoc network where a station is connected to an adhoc access point.

## wlsxNAdhocNetworkBridgeDetectedAP

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel}
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected an adhoc network that is bridging to a wired network.

## wlsxNAdhocNetworkBridgeDetectedSta

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapSourceMac, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel}
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected an adhoc network that is bridging to a wired network.

## wlsxClietFloodAttack

<b>Objects</b>	wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation
<b>Status</b>	current
<b>Description</b>	This trap indicates that the number of potential fake clients detected by an AP has exceeded the configured IDS threshold. This is the total number of fake clients observed across all bands. For more information check <a href="http://www.wve.org/entries/show/WVE-2005-0056">http://www.wve.org/entries/show/WVE-2005-0056</a>

## wlsxValidClientNotUsingEncryption

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapSourceMac, wlsxTrapReceiverMac, wlsxTrapNodeMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected an unencrypted data frame between a valid client and an access point.

## wlsxAdhocUsingValidSSID

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected an adhoc network using a valid/protected SSID. For more information check <a href="http://www.wve.org/entries/show/WVE-2005-0008">http://www.wve.org/entries/show/WVE-2005-0008</a>



## wlsxAPspoofingDetected

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapSourceMac, wlsxTrapReceiverMac, wlsxTrapSpoofedFrameType, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected that one of its virtual APs is being spoofed using MAC spoofing. For more information check <a href="http://www.wve.org/entries/show/WVE-2005-0019">http://www.wve.org/entries/show/WVE-2005-0019</a>

## wlsxClientAssociatingOnWrongChannel

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapSourceMac, wlsxTrapReceiverMac, wlsxTrapSpoofedFrameType, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a client trying to associate to one of its BSSIDs on the wrong channel. This can be a sign that the BSSID is being spoofed in order to fool the client into thinking the AP is operating on another channel.

## wlsxNDisconnectStationAttack

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSourceMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP has determined that a client is under Disconnect Attack because the rate of Assoc/Reassoc Response packets received by that client exceeds the configured threshold. For more information check: <a href="http://www.wve.org/entries/show/WVE-2005-0045">http://www.wve.org/entries/show/WVE-2005-0045</a> <a href="http://www.wve.org/entries/show/WVE-2005-0046">http://www.wve.org/entries/show/WVE-2005-0046</a> <a href="http://www.wve.org/entries/show/WVE-2005-0048">http://www.wve.org/entries/show/WVE-2005-0048</a>

## wlsxNStaUnAssociatedFromUnsecureAP

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapNodeMac, wlsxTrapAPLocation, wlsxTrapAPChannel
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP that had previously detected a client association to a Rogue access point is no longer detecting that association.

## wlsxOmertaAttack

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapNodeMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected an Omerta attack. For more information check <a href="http://www.wve.org/entries/show/WVE-2005-0053">http://www.wve.org/entries/show/WVE-2005-0053</a>

## wlsxTKIPReplayAttack

<b>Objects</b>	wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapSourceMac, wlsxTrapReceiverMac, wlsxTrapTargetAPBSSID, wlsxTrapAPChannel, wlsxTrapSnr
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a TKIP replay attack. If successful this could be the precursor to more advanced attacks. For more information check <a href="http://www.wve.org/entries/show/WVE-2008-0013">http://www.wve.org/entries/show/WVE-2008-0013</a>

## wlsxChopChopAttack

<b>Objects</b>	wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapSourceMac, wlsxTrapReceiverMac, wlsxTrapTargetAPBSSID, wlsxTrapAPChannel, wlsxTrapSnr
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a ChopChop attack. For more information check <a href="http://www.wve.org/entries/show/WVE-2006-0038">http://www.wve.org/entries/show/WVE-2006-0038</a>

## wlsxFataJackAttack

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapNodeMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a FATA-Jack attack. For more information check <a href="http://www.wve.org/entries/show/WVE-2006-0057">http://www.wve.org/entries/show/WVE-2006-0057</a>

## wlsxInvalidAddressCombination

<b>Objects</b>	wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapSourceMac, wlsxTrapReceiverMac, wlsxTrapAPChannel, wlsxTrapSnr
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected an invalid source and destination combination. For more information check <a href="http://www.wve.org/entries/show/WVE-2008-0011">http://www.wve.org/entries/show/WVE-2008-0011</a>

## wlsxValidClientMisassociation

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapNodeMac, wlsxTrapAssociationType, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a misassociation between a valid client and an unsafe AP.

## wlsxMalformedHTIEDetected

<b>Objects</b>	wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapSourceMac, wlsxTrapReceiverMac, wlsxTrapTargetAPBSSID, wlsxTrapAPChannel, wlsxTrapSnr
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a malformed HT Information Element. This can be the result of a misbehaving wireless driver or it may be an indication of a new wireless attack.

## wlsxMalformedAssocReqDetected

<b>Objects</b>	wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapSourceMac, wlsxTrapReceiverMac, wlsxTrapTargetAPBSSID, wlsxTrapAPChannel, wlsxTrapSnr
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a malformed association request with a NULL SSID. For more information check <a href="http://www.wve.org/entries/show/WVE-2008-0010">http://www.wve.org/entries/show/WVE-2008-0010</a>

## wlsxOverflowIEDetected

<b>Objects</b>	wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapSourceMac, wlsxTrapReceiverMac, wlsxTrapTargetAPBSSID, wlsxTrapAPChannel, wlsxTrapSnr
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a management frame with a malformed information element. The declared length of the element is larger than the entire frame containing the element. This may be used to corrupt or crash wireless drivers. For more information check <a href="http://www.wve.org/entries/show/WVE-2008-0008">http://www.wve.org/entries/show/WVE-2008-0008</a>

## wlsxOverflowEAPOLKeyDetected

<b>Objects</b>	wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapSourceMac, wlsxTrapReceiverMac, wlsxTrapTargetAPBSSID, wlsxTrapAPChannel, wlsxTrapSnr
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a key in an EAPOL Key message with a specified length greater than the length of the entire message. For more information check <a href="http://www.wve.org/entries/show/WVE-2008-0009">http://www.wve.org/entries/show/WVE-2008-0009</a>

## wlsxMalformedFrameLargeDurationDetected

<b>Objects</b>	wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapSourceMac, wlsxTrapAPChannel, wlsxTrapSnr
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected an unusually large duration in a wireless frame. This may be an attempt to block other devices from transmitting. For more information check <a href="http://www.wve.org/entries/show/WVE-2005-0051">http://www.wve.org/entries/show/WVE-2005-0051</a>

## wlsxMalformedFrameWrongChannelDetected

<b>Objects</b>	wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapSourceMac, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPChannel, wlsxTrapAPChannel, wlsxTrapSnr
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a beacon on one channel advertising another channel. This could be an attempt to lure clients away from a valid AP. For more information check <a href="http://www.wve.org/entries/show/WVE-2006-0050">http://www.wve.org/entries/show/WVE-2006-0050</a>

## wlsxMalformedAuthFrame

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapNodeMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected an authentication frame with either a bad algorithm (similar to Fata-Jack) or a bad transaction. For more information check <a href="http://www.wve.org/entries/show/WVE-2006-0057">http://www.wve.org/entries/show/WVE-2006-0057</a>

## wlsxCTSRateAnomaly

<b>Objects</b>	wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
<b>Status</b>	current
<b>Description</b>	This trap indicates that the rate of CTS packets received by an AP exceeds the configured IDS threshold.

## wlsxRTSRateAnomaly

<b>Objects</b>	wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
<b>Status</b>	current
<b>Description</b>	This trap indicates that the rate of RTS packets received by an AP exceeds the configured IDS threshold.

## wlsxNRogueAPDetected

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPChannel
<b>Status</b>	current
<b>Description</b>	This trap indicates that an unauthorized access point is connected to the wired network. The access point is classified as Rogue by the system.

## wlsxNRogueAPResolved

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPChannel
<b>Status</b>	current
<b>Description</b>	This trap indicates that a previously detected access point, classified as Rogue, is either no longer present in the network or it changed its state.

## wlsxNeighborAPDetected

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPChannel
<b>Status</b>	current
<b>Description</b>	This trap indicates that an access point has been classified as a Neighbor by the system.

## wlsxNInterferingAPDetected

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPChannel
<b>Status</b>	current
<b>Description</b>	This trap indicates that an access point has been classified as Interfering by the system. The access point is declared Interfering because it is not authorized, nor has it been classified as a rogue.

## wlsxNSuspectRogueAPDetected

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPChannel, wlsxTrapConfidenceLevel
<b>Status</b>	current
<b>Description</b>	This trap indicates that an access point, classified as suspected rogue, is detected by the system. The AP is suspected to be rogue with the supplied confidence level.

## wlsxNSuspectRogueAPResolved

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapAPChannel
<b>Status</b>	current
<b>Description</b>	This trap indicates that a previously detected access point, classified as suspected rogue, is either no longer present in the network or has changed its state.

## wlsxBlockAckAttackDetected

<b>Objects</b>	wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapSourceMac, wlsxTrapReceiverMac, wlsxTrapTargetAPBSSID, wlsxTrapAPChannel, wlsxTrapSnr
<b>Status</b>	current
<b>Description</b>	This trap indicates that an attempt has been made to deny service to the source address by spoofing a block ACK add request that sets a sequence number window outside the currently used window. For more information check <a href="http://www.wve.org/entries/show/WVE-2008-0006">http://www.wve.org/entries/show/WVE-2008-0006</a>

## wlsxHotspotterAttackDetected

<b>Objects</b>	wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapNodeMac, wlsxTrapSourceMac, wlsxTrapTargetAPBSSID, wlsxTrapAPChannel, wlsxTrapSnr, wlsxTrapTargetAPSSID
<b>Status</b>	current
<b>Description</b>	This trap indicates that a new AP has appeared immediately following a client probe request. This is indicative of the Hotspotter tool or similar that attempts to trap clients with a fake hotspot or other wireless network. For more information check <a href="http://www.wve.org/entries/show/WVE-2005-0054">http://www.wve.org/entries/show/WVE-2005-0054</a>

## wlsxNSignatureMatch

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTransmitterMac, wlsxTrapReceiverMac, wlsxTrapSignatureName, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a signature match in a frame.

## wlsxNSignatureMatchNetstumbler

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTransmitterMac, wlsxTrapReceiverMac, wlsxTrapSignatureName, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a signature match for Netstumbler in a frame. For more information check <a href="http://www.wve.org/entries/show/WVE-2005-0025">http://www.wve.org/entries/show/WVE-2005-0025</a>

## wlsxNSignatureMatchAsleep

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTransmitterMac, wlsxTrapReceiverMac, wlsxTrapSignatureName, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a signature match for ASLEAP in a frame. For more information check <a href="http://www.wve.org/entries/show/WVE-2005-0027">http://www.wve.org/entries/show/WVE-2005-0027</a>

## wlsxNSignatureMatchAirjack

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTransmitterMac, wlsxTrapReceiverMac, wlsxTrapSignatureName, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a signature match for Airjack in a frame. For more information check <a href="http://www.wve.org/entries/show/WVE-2005-0018">http://www.wve.org/entries/show/WVE-2005-0018</a>

## wlsxNSignatureMatchNullProbeResp

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTransmitterMac, wlsxTrapReceiverMac, wlsxTrapSignatureName, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
<b>Max-Access</b>	
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a signature match for Null-Probe-Response in a frame. For more information check <a href="http://www.wve.org/entries/show/WVE-2006-0064">http://www.wve.org/entries/show/WVE-2006-0064</a>

## wlsxNSignatureMatchDeathBcast

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTransmitterMac, wlsxTrapReceiverMac, wlsxTrapSignatureName, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
<b>Max-Access</b>	
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a signature match for Death-Broadcast in a frame. For more information check: <a href="http://www.wve.org/entries/show/WVE-2005-0019">http://www.wve.org/entries/show/WVE-2005-0019</a> <a href="http://www.wve.org/entries/show/WVE-2005-0045">http://www.wve.org/entries/show/WVE-2005-0045</a>

## wlsxNSignatureMatchDisassocBcast

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTransmitterMac, wlsxTrapReceiverMac, wlsxTrapSignatureName, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
<b>Max-Access</b>	
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a signature match for Disassoc-Broadcast in a frame. For more information check: <a href="http://www.wve.org/entries/show/WVE-2005-0019">http://www.wve.org/entries/show/WVE-2005-0019</a> <a href="http://www.wve.org/entries/show/WVE-2005-0046">http://www.wve.org/entries/show/WVE-2005-0046</a>



## wlsxNSignatureMatchWellenreiter

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTransmitterMac, wlsxTrapReceiverMac, wlsxTrapSignatureName, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a signature match for Wellenreiter in a frame. For more information check <a href="http://www.wve.org/entries/show/WVE-2006-0058">http://www.wve.org/entries/show/WVE-2006-0058</a>

## wlsxAPDeathContainment

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapNodeMac, wlsxTrapAPChannel, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP has attempted to contain an access point by disconnecting its client.

## wlsxClientDeathContainment

<b>Objects</b>	wlsxTrapTime, wlsxTrapNodeMac, wlsxTrapTargetAPBSSID, wlsxTrapAPChannel, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP has attempted to contain a client by disconnecting it from the AP that it is associated with.

## wlsxAPWiredContainment

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapNodeMac, wlsxTrapDeviceIpAddress, wlsxTrapDeviceMac, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP has attempted to contain an access point by disrupting traffic to its client on the wired interface.

## wlsxClientWiredContainment

<b>Objects</b>	wlsxTrapTime, wlsxTrapNodeMac, wlsxTrapTargetAPBSSID, wlsxTrapDeviceIpAddress, wlsxTrapDeviceMac, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP has attempted to contain a client by disrupting traffic to it on the wired interface.

## wlsxAPTaggedWiredContainment

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapNodeMac, wlsxTrapDeviceIpAddress, wlsxTrapDeviceMac, wlsxTrapVlanId, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP has attempted to contain an access point by disrupting traffic to its client on the wired interface.

## wlsxClientTaggedWiredContainment

<b>Objects</b>	wlsxTrapTime, wlsxTrapNodeMac, wlsxTrapTargetAPBSSID, wlsxTrapDeviceIpAddress, wlsxTrapDeviceMac, wlsxTrapVlanId, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP has attempted to contain a client by disrupting traffic to it on the wired interface.

## wlsxTarpitContainment

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapNodeMac, wlsxTrapAPChannel, wlsxTrapTargetAPChannel, wlsxTrapSourceMac, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP has attempted to contain an access point by moving a client that is attempting to associate to it to a tarpit.

## wlsxAPChannelChange

<b>Objects</b>	wlsxTrapTime, wlsxTrapAPChannel, wlsxTrapAPChannelSec, wlsxTrapAPPprevChannel, wlsxTrapAPPprevChannelSec, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPARMChangeReason
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP changed its channel.

## wlsxAPPowerChange

<b>Objects</b>	wlsxTrapTime, wlsxTrapAPTxFPower, wlsxTrapAPPprevTxPower, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP changed its transmit power level.

## wlsxAPModeChange

<b>Objects</b>	wlsxTrapTime, wlsxTrapAPCurMode, wlsxTrapAPPrevMode, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP changed its mode from AP to AP Monitor or vice versa.

## wlsxUserEntryAttributesChanged

<b>Objects</b>	wlsxTrapTime, wlsxTrapUserIpAddress, wlsxTrapUserPhyAddress, wlsxTrapAPBSSID, wlsxTrapAPName, wlsxTrapCardSlot, wlsxTrapPortNumber, wlsxTrapUserAttributeChangeType
<b>Status</b>	current
<b>Description</b>	This trap indicates that the user entry attributes have changed.

## wlsxPowerSaveDosAttack

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapNodeMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a Power Save DoS attack.

## wlsxNAPMasterStatusChange

<b>Objects</b>	wlsxTrapTime, wlsxTrapAPMacAddress, wlsxTrapApControllerIp, wlsxTrapApMasterStatus
<b>Status</b>	current
<b>Description</b>	This trap indicates that the status of the AP as seen by the master controller has changed.

## wlsxNAdhocUsingValidSSID

<b>Objects</b>	wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSourceMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected an adhoc network node using a valid/protected SSID. For more information check <a href="http://www.wve.org/entries/show/WVE-2005-0008">http://www.wve.org/entries/show/WVE-2005-0008</a>

## wlsxMgmtUserAuthenticationFailed

<b>Objects</b>	wlsxTrapTime, wlsxTrapUserName, wlsxTrapUserIpAddress, wlsxTrapAuthServerName
<b>Status</b>	current
<b>Description</b>	

## SNMP Traps

SNMP Traps are MIB objects (variables) that transmit information to the SNMP Manager when an event occurs. Traps are included as varbinds (variable bindings) in the trap protocol data unit (PDU).

The following traps are supported for the ifTable objects:

- linkDown
- linkUp

These traps are sent when there is change on a specific interface such as GRE or Ethernet.

### linkDown

<b>Object ID</b>	1.3.6.1.6.3.1.1.5.3
<b>Syntax</b>	NA
<b>Max-Access</b>	Current
<b>Objects</b>	<ul style="list-style-type: none"><li>• ifIndex</li><li>• ifAdminStatus</li><li>• ifOperStatus</li></ul>
<b>Status</b>	current
<b>Description</b>	Indicates that change of state in communication link.

### linkUp

<b>Object ID</b>	1.3.6.1.6.3.1.1.5.4
<b>Syntax</b>	NA
<b>Max-Access</b>	Current
<b>Objects</b>	<ul style="list-style-type: none"><li>• ifIndex</li><li>• ifAdminStatus</li><li>• ifOperStatus</li></ul>
<b>Status</b>	current
<b>Description</b>	Indicates that change of state in communication link.