

# **Dell PowerConnect W-Series Instant Access Point MIB Reference Guide**



## Copyright

© 2012 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. 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.

# Contents

<b>Preface</b> .....	<b>15</b>
An Overview of This Manual .....	15
Contents .....	15
Related Documents .....	15
Frequently Used Acronyms.....	15
Website Contact .....	18
<b>Chapter 1</b> <b>MIBs Overview</b> .....	<b>19</b>
MIBs .....	19
SNMP .....	21
<b>Chapter 2</b> <b>Using MIBs</b> .....	<b>23</b>
Downloading MIB Files .....	23
Monitoring WLAN Health.....	23
MIB Browsers.....	23
Reading MIB Files .....	24
Opening Line.....	24
Imports .....	25
Inheritance .....	25
Identity .....	26
MIB Modules.....	26
Group.....	26
Table.....	26
Entry.....	27
Closing Line .....	27
SNMP File .....	27
HP OpenView .....	27
<b>Chapter 3</b> <b>Instant MIB</b> .....	<b>29</b>
aiAccessPointTable .....	30
aiAccessPointEntry.....	30
aiAPMACAddress.....	31
aiAPName.....	31
aiAPIPAddress.....	31
aiAPSerialNum.....	31
aiAPModel .....	31
aiAPModelName .....	32
aiAPCPUUtilization .....	32
aiAPMemoryFree.....	32
aiAPUptime.....	32
aiRadioTable.....	33
aiRadioEntry .....	33
aiRadioAPMacAddress .....	34
aiRadioIndex.....	34
aiRadioMACAddress.....	34
aiRadioChannel.....	34
aiRadioTransmitPower .....	34

aiRadioNoiseFloor .....	35
aiRadioUtilization4 .....	35
aiRadioUtilization64 .....	35
aiRadioTxTotalFrames .....	35
aiRadioTxMgmtFrames .....	35
aiRadioTxDataFrames .....	36
aiRadioTxDataBytes .....	36
aiRadioTxDrops .....	36
aiRadioRxTotalFrames .....	36
aiRadioRxDataFrames .....	36
aiRadioRxDataBytes .....	37
aiRadioRxMgmtFrames .....	37
aiRadioRxBad .....	37
aiRadioPhyEvents .....	37
aiWlanTable .....	38
aiWlanEntry .....	38
aiWlanAPMACAddress .....	38
aiWlanIndex .....	39
aiWlanESSID .....	39
aiWlanMACAddress .....	39
aiWlanTxTotalFrames .....	39
aiWlanTxDataFrames .....	39
aiWlanTxDataBytes .....	40
aiWlanRxTotalFrames .....	40
aiWlanRxDataFrames .....	40
aiWlanRxDataBytes .....	40
aiClientTable .....	41
aiClientTable Entry .....	41
aiClientMACAddress .....	41
aiClientWlanMACAddress .....	42
aiClientIPAddress .....	42
aiClientAPIPAddress .....	42
aiClientName .....	42
aiClientOperatingSystem .....	42
aiClientSNR .....	43
aiClientTxDataFrames .....	43
aiClientTxDataBytes .....	43
aiClientTxRetries .....	43
aiClientTxRate .....	43
aiClientRxDataFrames .....	44
aiClientRxDataBytes .....	44
aiClientRxRetries .....	44
aiClientRxRate .....	44
aiClientUptime .....	44
<b>Chapter 4      SNMP MIBs Reference .....</b>	<b>45</b>
<b>Chapter 5      Traps .....</b>	<b>47</b>
Trap Hierarchy .....	47
ai Traps Objects Group .....	48
wlsxTrapAPMacAddress .....	51
wlsxTrapAPIpAddress .....	51
wlsxTrapAPBSSID .....	51
wlsxTrapEssid .....	52
wlsxTrapTargetAPBSSID .....	52
wlsxTrapTargetAPSSID .....	52
wlsxTrapTargetAPChannel .....	52

wlsxTrapNodeMac.....	52
wlsxTrapSourceMac .....	53
wlsxReceiverMac.....	53
wlsxTrapTransmitterMac.....	53
wlsxTrapReceiverMac .....	53
wlsxTrapSnr .....	53
wlsxTrapSignatureName .....	53
wlsxTrapFrameType.....	54
wlsxTrapAddressType.....	54
wlsxTrapAPLocation.....	54
wlsxTrapAPChannel.....	54
wlsxTrapAPTxPower .....	54
wlsxTrapMatchedMac .....	54
wlsxTrapMatchedIp.....	55
wlsxTrapRogueIfoURL.....	55
wlsxTrapVLANId.....	55
wlsxTrapAdminStatus.....	55
wlsxTrapOperStatus .....	55
wlsxTrapAuthServerName .....	55
wlsxTrapAuthServerTimeout .....	56
wlsxTrapCardSlot.....	56
wlsxTrapTemperatureValue .....	56
wlsxTrapProcessName .....	56
wlsxTrapFanNumber.....	56
wlsxTrapVoltageType .....	56
wlsxTrapVoltageValue.....	57
wlsxTrapStationBlackListReason .....	57
wlsxTrapSpoofedIpAddress .....	57
wlsxTrapSpoofedOldPhyAddress .....	57
wlsxTrapSpoofedNewPhyAddress .....	57
wlsxTrapDBName .....	57
wlsxTrapDBUserName.....	58
wlsxTrapDBIpAddress.....	58
wlsxTrapDBType .....	58
wlsxTrapVrrpID.....	58
wlsxTrapVrrpMasterIp .....	58
wlsxTrapVrrpOperState.....	58
wlsxTrapESIServerGrpName .....	59
wlsxTrapESIServerName.....	59
wlsxTrapESIServerIpAddress .....	59
wlsxTrapLicenseDaysRemaining .....	59
wlsxTrapSwitchIp.....	59
wlsxTrapSwitchRole .....	59
wlsxTrapUserIpAddress.....	60
wlsxTrapUserPhyAddress .....	60
wlsxTrapUserName .....	60
wlsxTrapUserRole .....	60
wlsxTrapUserAuthenticationMethod .....	60
wlsxTrapAPRadioNumber .....	60
wlsxTrapRogueInfoURL.....	61
wlsxTrapInterferingAPInfoURL.....	61
wlsxTrapPortNumber.....	61
wlsxTrapTime .....	61
wlsxTrapHostIp.....	61
wlsxTrapHostPort.....	61
wlsxTrapConfigurationId.....	62
wlsxTrapCTSURL.....	62
wlsxTrapCTSTransferType .....	62

wlsxTrapConfigurationState.....	62
wlsxTrapUpdateFailureReason.....	62
wlsxTrapUpdateFailedObj.....	62
wlsxTrapTableEntryChangeType.....	63
wlsxTrapGlobalConfigObj.....	63
wlsxTrapTableGenNumber.....	63
wlsxTrapLicenseId.....	63
wlsxTrapConfidenceLevel.....	63
wlsxTrapMissingLicenses.....	63
wlsxVoiceCurrentNumCdr.....	64
wlsxTrapTunnelId.....	64
wlsxTrapTunnelStatus.....	64
wlsxTrapTunnelUpReason.....	64
wlsxTrapTunnelDownReason.....	64
wlsxTrapApSerialNumber.....	64
wlsxTraptimeStr.....	65
wlsxTrapMasterIp.....	65
wlsxTrapLocalIp.....	65
wlsxTrapMasterName.....	65
wlsxTrapLocalName.....	65
wlsxTrapPrimaryControllerIp.....	65
wlsxTrapBackupControllerIp.....	66
wlsxTrapSpoofedFrameType.....	66
wlsxTrapAssociationType.....	66
wlsxTrapDeviceIpAddress.....	66
wlsxTrapDeviceMac.....	66
wlsxTrapVcIpAddress.....	66
wlsxTrapVcMacAddress.....	67
wlsxTrapAPName.....	67
wlsxTrapApMode.....	67
wlsxTrapAPPrevChannel.....	67
wlsxTrapAPPrevChannelSec.....	67
wlsxTrapAPPrevTxPower.....	67
wlsxTrapAPCurMode.....	68
wlsxTrapAPPrevMode.....	68
wlsxTrapAPARMChangeReason.....	68
wlsxTrapAPChannelSec.....	68
wlsxTrapUserAttributeChangeType.....	68
wlsxTrapAPControllerIp.....	69
wlsxTrapApMasterStatus.....	69
wlsxTrapCaName.....	69
wlsxTrapCrIName.....	69
wlsxTrapCount.....	69
ai Traps Definitions Group.....	70
wlsxNodeRateAnomaly.....	77
wlsxNUserEntryCreated.....	77
wlsxNUserEntryDeleted.....	77
wlsxNUserEntryAuthenticated.....	77
wlsxNUserEntryDeAuthenticated.....	77
wlsxNUserAuthenticationFailed.....	78
wlsxNAuthServerReqTimedOut.....	78
wlsxNAuthServerTimedOut.....	78
wlsxNAuthServerIsUp.....	78
wlsxNAccessPointIsUp.....	78
wlsxNAccessPointIsDown.....	78
wlsxNChannelChanged.....	78
wlsxNStationAddedToBlackList.....	79
wlsxNStationRemovedFromBlackList.....	79

wlsxNRadioAttributesChanged.....	79
wlsxUnsecureAPDetected .....	79
wlsxUnsecureAPResolved.....	79
wlsxStalImpersonation.....	79
wlsxReservedChannelViolation .....	80
wlsxValidSSIDViolation .....	80
wlsxChannelMisconfiguration .....	80
wlsxOUIMisconfiguration .....	80
wlsxSSIDMisconfiguration .....	80
wlsxShortPreambleMisconfiguration .....	80
wlsxWPAMisconfiguration.....	81
wlsxAdhocNetworkDetected .....	81
wlsxAdhocNetworkRemoved .....	81
wlsxStaPolicyViolation .....	81
wlsxRepeatWEPIVViolation.....	81
wlsxWeakWEPIVViolation.....	81
wlsxChannelInterferenceDetected .....	82
wlsxChannelInterferenceCleared .....	82
wlsxAPInterferenceDetected .....	82
wlsxAPInterferenceCleared .....	82
wlsxStaInterferenceDetected.....	82
wlsxStaInterferenceCleared .....	82
wlsxFrameRetryRateExceeded .....	83
wlsxFrameReceiveErrorRateExceeded .....	83
wlsxFrameFragmentationRateExceeded .....	83
wlsxFrameBandWidthRateExceeded .....	83
wlsxFrameLowSpeedRateExceeded .....	83
wlsxFrameNonUnicastRateExceeded .....	84
wlsxLoadbalancingEnabled.....	84
wlsxLoadbalancingDisabled.....	84
wlsxChannelFrameRetryRateExceeded .....	84
wlsxChannelFrameFragmentationRateExceeded.....	84
wlsxChannelFrameErrorRateExceeded.....	84
wlsxSignatureMatchAP .....	85
wlsxSignatureMatchSta .....	85
wlsxChannelRateAnomaly.....	85
wlsxNodeRateAnomalyAP.....	85
wlsxNodeRateAnomalySta .....	85
wlsxEAPRateAnomaly .....	86
wlsxSignalAnomaly.....	86
wlsxSequenceNumberAnomalyAP .....	86
wlsxSequenceNumberAnomalySta .....	86
wlsxDisconnectStationAttack.....	87
wlsxApFloodAttack .....	87
wlsxAdhocNetwork.....	87
wlsxWirelessBridge.....	87
wlsxInvalidMacOUIAP.....	87
wlsxInvalidMacOUISta.....	88
wlsxWEPMisconfiguration .....	88
wlsxStaRepeatWEPIVViolation.....	88
wlsxStaWeakWEPIVViolation.....	88
wlsxStaAssociatedToUnsecureAP .....	88
wlsxStaUnAssociatedFromUnsecureAP .....	88
wlsxAdhocNetworkBridgeDetected .....	89
wlsxInterferingApDetected .....	89
wlsxColdStart.....	89
wlsxWarmStart.....	89
wlsxAPImpersonation.....	89

wlsxNAuthServerIsDown.....	89
wlsxWindowsBridgeDetected .....	90
wlsxSignAPNetstumbler .....	90
wlsxSignStaNetstumbler .....	90
wlsxSignAPAsleep .....	90
wlsxSignStaAsleep .....	90
wlsxSignAPAirjack.....	91
wlsxSignStaAirjack.....	91
wlsxSignAPNullProbeResp .....	91
wlsxSignStaNullProbeResp.....	91
wlsxSignAPDeauthBcast.....	91
wlsxSignStaDeauthBcast .....	92
wlsxWindowsBridgeDetectedAP .....	92
wlsxWindowsBridgeDetectedSta .....	92
wlsxAdhocNetworkBridgeDetectedAP.....	92
wlsxAdhocNetworkBridgeDetectedSta .....	92
wlsxDisconnectStationAttackAP .....	93
wlsxDisconnectStationAttackSta.....	93
wlsxSuspectUnsecureAPDetected.....	93
wlsxHT40MHzIntoleranceAP .....	93
wlsxHT40MHzIntoleranceSta .....	94
wlsxNAdhocNetwork.....	94
wlsxNAdhocNetworkBridgeDetectedAP.....	94
wlsxNAdhocNetworkBridgeDetectedSta .....	94
wlsxClientFloodAttack.....	94
wlsxValidClientNotUsingEncryption .....	95
wlsxAdhocUsingValidSSID .....	95
wlsxAPSpooftingDetected .....	95
wlsxClientAssociatingOnWrongChannel .....	95
wlsxNDisconnectStationAttack.....	96
wlsxNStaUnAssociatedFromUnsecureAP.....	96
wlsxOmertaAttack.....	96
wlsxTKIPReplayAttack .....	96
wlsxChopChopAttack.....	96
wlsxFataJackAttack.....	97
wlsxInvalidAddressCombination .....	97
wlsxValidClientMisassociation .....	97
wlsxMalformedHTIEDetected .....	97
wlsxMalformedAssocReqDetected .....	97
wlsxOverflowIEDetected.....	98
wlsxOverflowEAPOLKeyDetected .....	98
wlsxMalformedFrameLargeDurationDetected .....	98
wlsxMalformedFrameWrongChannelDetected .....	98
wlsxMalformedAuthFrame .....	98
wlsxCTSRateAnomaly.....	99
wlsxRTSRateAnomaly.....	99
wlsxNRogueAPDetected .....	99
wlsxNRogueAPResolved .....	99
wlsxNeighborAPDetected .....	99
wlsxNInterferingAPDetected .....	99
wlsxNSuspectRogueAPDetected.....	100
wlsxNSuspectRogueAPResolved.....	100
wlsxBlockAckAttackDetected .....	100
wlsxHotspotterAttackDetected .....	100
wlsxNSignatureMatch.....	100
wlsxNSignatureMatchNetstumbler .....	101
wlsxNSignatureMatchAsleep.....	101
wlsxNSignatureMatchAirjack.....	101



wlsxNSignatureMatchNullProbeResp .....	101
wlsxNSignatureMatchDeauthBcast.....	101
wlsxNSignatureMatchDisassocBcast .....	102
wlsxNSignatureMatchWellenreiter .....	102
wlsxAPDeauthContainment.....	102
wlsxClientDeauthContainment.....	102
wlsxAPWiredContainment.....	102
wlsxClientWiredContainment.....	103
wlsxAPTaggedWiredContainment .....	103
wlsxClientTaggedWiredContainment .....	103
wlsxTarpitContainment.....	103
wlsxAPChannelChange .....	103
wlsxAPPowerChange .....	104
wlsxAPModeChange .....	104
wlsxUserEntryAttributesChanged .....	104
wlsxPowerSaveDosAttack .....	104
wlsxNAPMasterStatusChange .....	104
wlsxNAdhocUsingValidSSID.....	104
wlsxMgmtUserAuthenticationFailed .....	105



# Figures

---

Figure 1	High-Level MIB Hierarchy .....	20
Figure 2	CLI Interface .....	23
Figure 3	Graphical User Interface.....	24
Figure 4	Instant MIB Hierarchy .....	29
Figure 5	Trap Hierarchy .....	47



# Tables

Table 1	Frequently Used Acronyms.....	15
Table 2	Website Support.....	18
Table 3	MIB Node Identification - Enterprise Nodes.....	19
Table 4	MIB Keywords .....	21
Table 5	Supported Instant MIB Tables .....	30
Table 6	aiAccessPointTable OIDs .....	30
Table 7	aiRadioTable OIDs.....	33
Table 8	aiWlanTable OIDs.....	38
Table 9	aiClientTable OID.....	41
Table 10	SNMP OIDs returned as sysObjectID for Dell Networks products.....	45
Table 11	SNMP OIDs returned as sysObjectID for Dell PowerConnect W-Series Instant Access products .....	45
Table 12	aiTraps Objects Group OIDs .....	48
Table 13	ai Traps Definitions Group OIDs.....	70



## An Overview of This Manual

This manual is for network administrators and operators responsible for managing the Dell PowerConnect W-Series Instant Access Points.

## Contents

This guide provides information about Dell PowerConnect Instant MIBs. Unless otherwise stated in the following table, each chapter provides information about the hierarchy, OIDs, and descriptions of the statistical information the MIBs provide.

Chapter	Contents
<a href="#">MIBs Overview</a>	Introductory information about Dell Instant MIBs.
<a href="#">Using MIBs</a>	Information and tips about Dell Instant MIB files.
<a href="#">Instant MIB</a>	Information about the supported Instant MIB tables.
<a href="#">SNMP MIBs Reference</a>	Reference—list of SNMP MIBs and associated OIDs.

## Related Documents

The complete documentation set for Dell Instant 6.1.2.3-2.0.0.0 software release are:

- *Dell PowerConnect W-Series Instant Access Point MIB Reference Guide (this guide)*
- *Dell PowerConnect W-Series Instant Access Point Quick Start Guide*
- *Dell PowerConnect W-Series Instant Access Point 6.1.2.3-2.0.0.0 User Guide*
- *Dell PowerConnect W-Series Instant Access Point 6.1.2.3-2.0.0.3 Release Notes*

## Frequently Used Acronyms

[Table 1](#) defines frequently used acronyms.

**Table 1** *Frequently Used Acronyms*

Acronym	Definition
3DES	Triple DES
ACL	Access Control List
AM	Air Monitor
AP	Access Point
ARM	Adaptive Radio Management
BSSID	Basic Service Set Identifier
CA	Certificate Authority

**Table 1** *Frequently Used Acronyms (Continued)*

<b>Acronym</b>	<b>Definition</b>
CAC	Call Admission Control
CHAP	Challenge Handshake Authentication Protocol
CLI	Command Line Interface
CRL	Certificate Revocation List
CSA	Channel Switch Announcement
CSR	Certificate Signing Request
CW	Contention Window
DA	Destination Address
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DOS	Denial of Service
DPD	Dead Peer Detection
DSS	Direct Spread Spectrum
EAP	Extensible Authentication Protocol
EDCA	Enhanced Distributed Channel Access
EIRP	Effective Isotropic Radiated Power
ESI	External Services Interface
ESSID	Extended Service Set Identifier
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
HAT	Home Agent Table
HT	High Throughput
IAS	Internet Authentication Service
IDS	Intrusion Detection System
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IV	Initialization Vectors
kB	Kilobyte
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LI	Listening Interval
MAC	Media Access Control



**Table 1** *Frequently Used Acronyms (Continued)*

<b>Acronym</b>	<b>Definition</b>
MB	Megabyte
MCHAP	Microsoft Challenge Handshake Authentication Protocol
MIB	Management Information Base
NAS	Network Address Server
NAT	Network Address Translation
NIC	Network Interface Card
NTP	Network Time Protocol
OFDM	Orthogonal Frequency Division Multiplexing
OID	Object Identifier
OUI	Organizational Unit Identifier
PAP	Password Authentication Protocol
PEAP	Protected EAP
PEF	Policy Enforcement Firewall
PIN	Personal Identification Number
PoE	Power over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PSK	Pre-Shared Key
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RAP	Remote Access Point
RF	Radio Frequency
RMON	Remote Monitor
RSA	Rivest-Shamir-Aldeman (encryption algorithm)
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSID	Service Set Identifier
TIM	Traffic Indication Map
TLS	Transport Layer Security
ToS	Type of Service
TSPEC	Traffic Specification
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network

**Table 1** *Frequently Used Acronyms (Continued)*

<b>Acronym</b>	<b>Definition</b>
VRRP	Virtual Router Redundancy Protocol
VSA	Vendor Specific Attributes
WEP	Wired Equivalent Protocol
WINS	Windows Internet Naming Service
WLAN	Wireless Local Area Network
WMM	Wireless MultiMedia / Wi-Fi Multimedia
WMS	WLAN Management System
WPA	Wi-Fi Protected Access

## Website Contact

**Table 2** *Website Support*

<b>Web Site Support</b>	
Main Website	<a href="http://dell.com">dell.com</a>
Support Website	<a href="http://support.dell.com">support.dell.com</a>
Documentation Website	<a href="http://support.dell.com/manuals">support.dell.com/manuals</a>

This chapter provides an overview of the ArubaOS Enterprise MIBs in the following sections:

- [MIBs](#)
- [SNMP](#)

### MIBs

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

MIB objects, such as a MIB table or a specific element of data in a MIB table, are identified with Object Identifiers (OIDs). The OIDs are designated by text strings and integer sequences.

The hardware MIBs are assigned under the Dell organization code, while all others are under the Aruba organization code. For example, *Dell* and *1.3.6.1.4.1.14823* both represent the private enterprise node *Aruba*, as shown in [Figure 1 on page 20](#).

*Dell* is the parent of the proprietary MIBs that are supported on Dell PowerConnect W-Series Mobility Controllers.

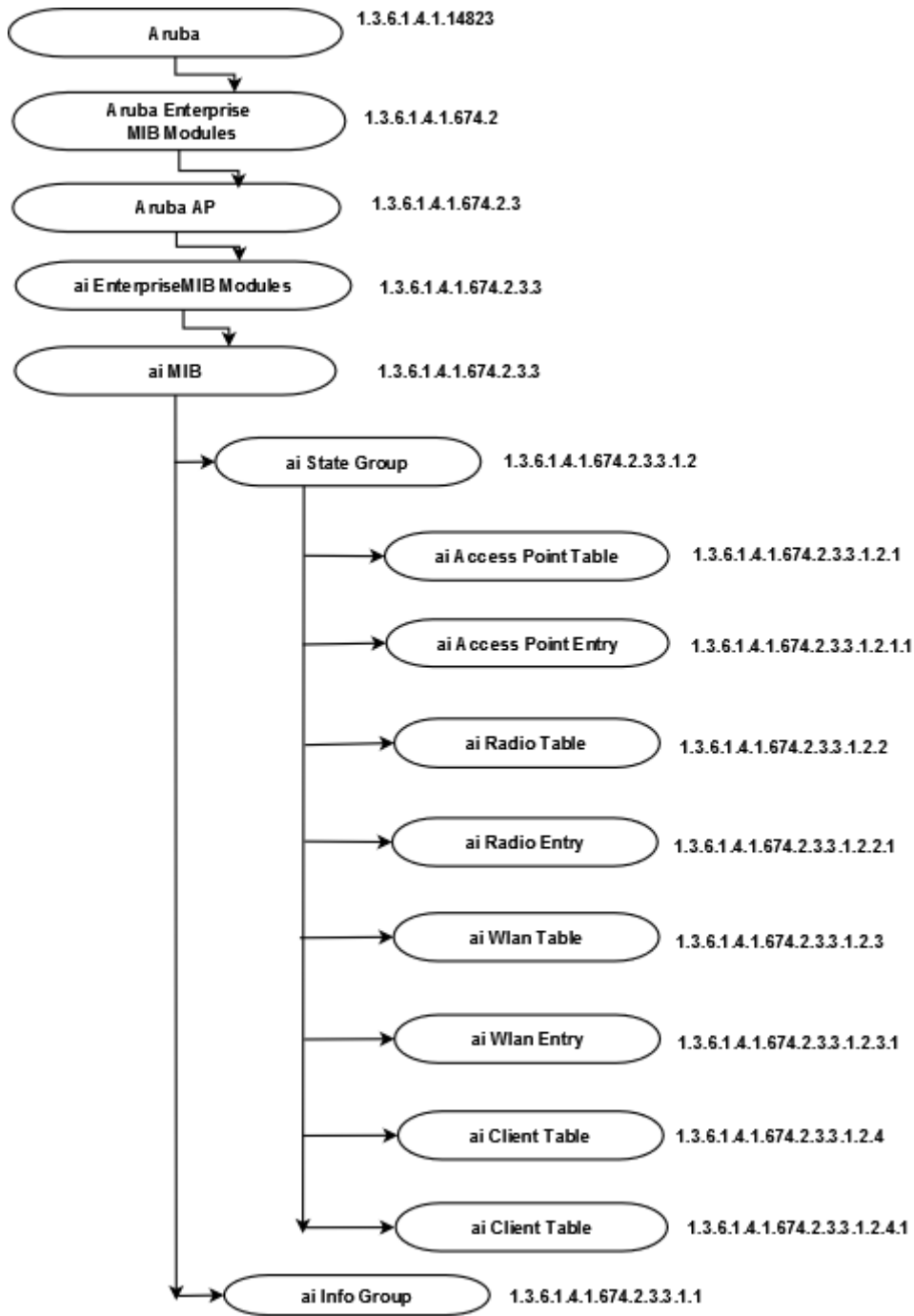
The numerical string lists the nodes of the enterprise MIB hierarchy, as shown in [Table 3](#).

**Table 3** MIB Node Identification - Enterprise Nodes

Integer	String	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

Figure 1 illustrates the high-level hierarchy of the MIBs. This document only covers the enterprise MIBs, objects designed to specifically support Dell devices. Standard MIBs are not covered.

**Figure 1** High-Level MIB Hierarchy



MIB is one of the elements of Simple Network Management Protocol (SNMP), which is used to manage network devices. To deliver information between devices, every object referred to in an SNMP message must be listed in the MIB. If a component of a device is not described in a MIB, that component cannot be recognized by SNMP—there is no information for SNMP managers and SNMP agents to exchange.

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 24](#).

# SNMP

Three significant elements of SNMP are Managers, Agents, and MIBs.

- Managers (software application) are consoles that are used to communicate with and manage devices that support SNMP Agents. Managers collect information by polling Agents. Managers can also be used to send configuration updates or send controlling requests to actively manage a network device.
- Agents (software application) provide information from the network devices to the Managers. Network devices include workstations, routers, microwave radios, and other network components. Agents are embedded in the Dell PowerConnect W-Series Mobility Controllers firmware, unlike some devices such as servers that require the agent to be installed separately.
- 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.
- To ensure functionality with SNMP, MIB objects must be defined with the proper *keywords*, as shown in [Table 4](#).

ArubaOS Enterprise MIBs support SNMPv1, SNMPv2, and SNMPv3.

**Table 4** MIB Keywords

Keyword	Description
<b>Sequence</b>	The sequence of objects of the MIB. This keyword is used mostly with entry MIB objects to list the MIB objects that exchange information.
<b>Syntax</b>	Textual conventions, such as <i>Integer32</i> .
<b>Max-Access</b>	Defines the object accessibility: <i>read-only</i> : can be retrieved but not modified <i>read-write</i> : can be retrieved and modified <i>not-accessible</i> : cannot be retrieved; it is for internal (device) use only <i>accessible-for-notify</i> : can be retrieved when a trap message (notification) is sent
<b>Status</b>	Defines the status of the object: <i>current</i> : up to date and valid. <i>deprecated</i> : indicates an obsolete definition. It permits new or continued implementation to maintain interoperability with existing implementations. <i>obsolete</i> : obsolete. It should not be implemented and/or can be removed if previously implemented.
<b>Description</b>	A text string that describes the object.



This chapter provides information on and examples of using MIBs.

- [Downloading MIB Files](#)
- [Monitoring WLAN Health](#)
- [Reading MIB Files](#)
- [SNMP File](#)
- [HP OpenView](#)

### Downloading MIB Files

The most recent Dell MIB files are available for registered customers at:

[support.dell.com](http://support.dell.com)

For assistance to set up an account and access files, please contact customer service. See “[Website Contact](#)” on [page 18](#).

### Monitoring WLAN Health

This section lists SNMP MIBs that are frequently used to run health checks on Dell Instant devices, which can be performed 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 Dell Instant
- The OID of the MIB value you want to monitor

In addition, MIB files can be placed in the appropriate disk location to assist the user in locating desired OID values for monitoring. If MIB files need to be acquired, see [Downloading MIB Files](#), above.

It is assumed that the workstation is connected to the Dell Instant and that 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.

```
.1.3.6.1.4.1.1674.2.2.1.1.2.1
```

### MIB Browsers

If using an application that is run through CLI (a *cmd* window), the command would resemble the following:

```
snmpget -v 2c -c <community name> <Instant IP address><MIB OID>
```

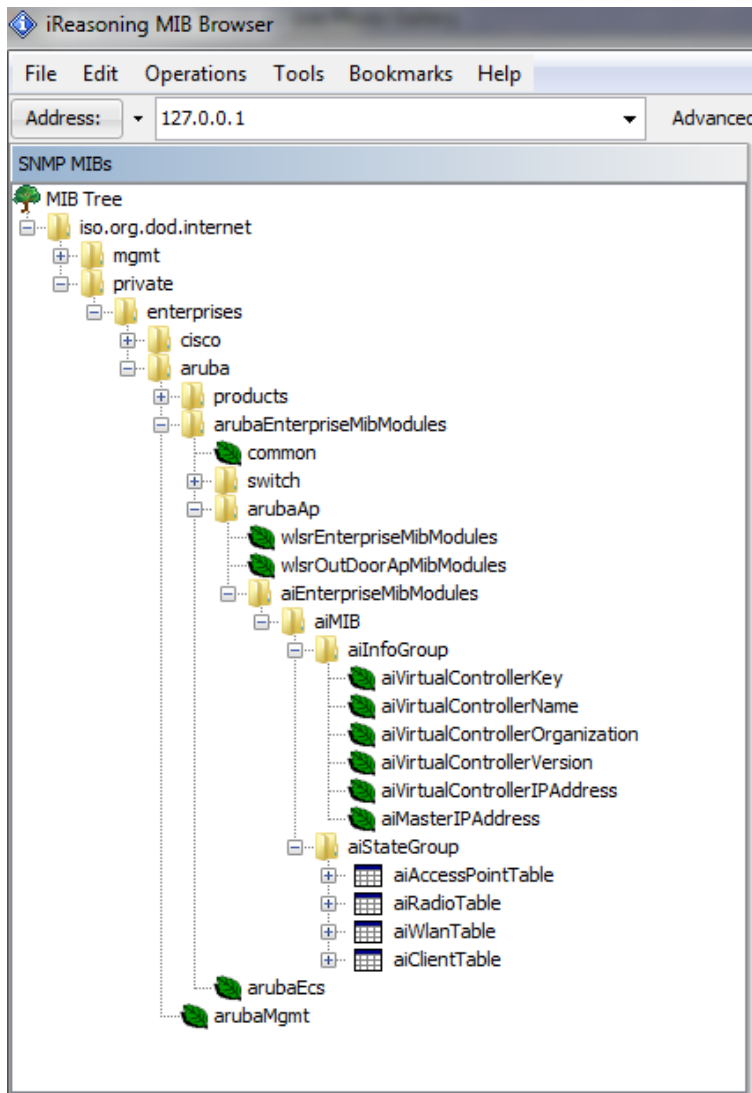
[Figure 2](#) shows an example of submitting a command to obtain information.

#### Figure 2 CLI Interface

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

**Figure 3** Graphical User Interface



## Reading MIB Files

This section describes how to interpret the basic components of a MIB file. To determine the OIDs, viewing the file `snmp.h` may be necessary, which is described in “SNMP File” on page 27. For additional information about MIB files, see “MIBs” on page 19. For a listing of SNMP MIB OIDs, see Chapter 4, “SNMP MIBs Reference” on page 45.

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 Instant enterprise MIB file, `aruba-cts.my`, are described below.

### 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 1.3.6.1.4.1.14823.2.3.3.1.1.0.

All MIBs and their related OIDs are listed in the `snmp` file of `Instant`. For more information, see [“SNMP File” on page 27](#).

`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 Aruba Instant WLAN"
        REVISION      "0804160206Z"
        DESCRIPTION
            "The initial revision."
 ::= { aiEnterpriseMibModules 1 }
```

## MIB Modules

MIB objects can be placed in logical groups, [Group](#) and [Table](#). One MIB file can consist of multiple groups. A group typically contains at least one table. The table lists the MIB objects that contain the information that is exchanged.

The first object of a table is an [Entry](#). 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 keywords: Syntax, Access, Status, Description. For details about keywords, see [“MIBs” on page 19](#).

The OID of the Entry is aiAccessPointEntry is aiAccessPointTable 1, which represents 1.3.6.1.4.1.14823.2.3.3.1.2.1.1. The OIDs of the subsequent objects of this table are appended increments of the Entry OID.

## 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 [Chapter 4, “SNMP MIBs Reference” on page 45](#).

All ArubaOS MIBs inherit their OIDs from the Dell MIB node. The following rows list the MIBs that precede CTS, starting from `iso`.

```
{ "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 Dell module for HP OpenView, log in as the root user and execute the following script:

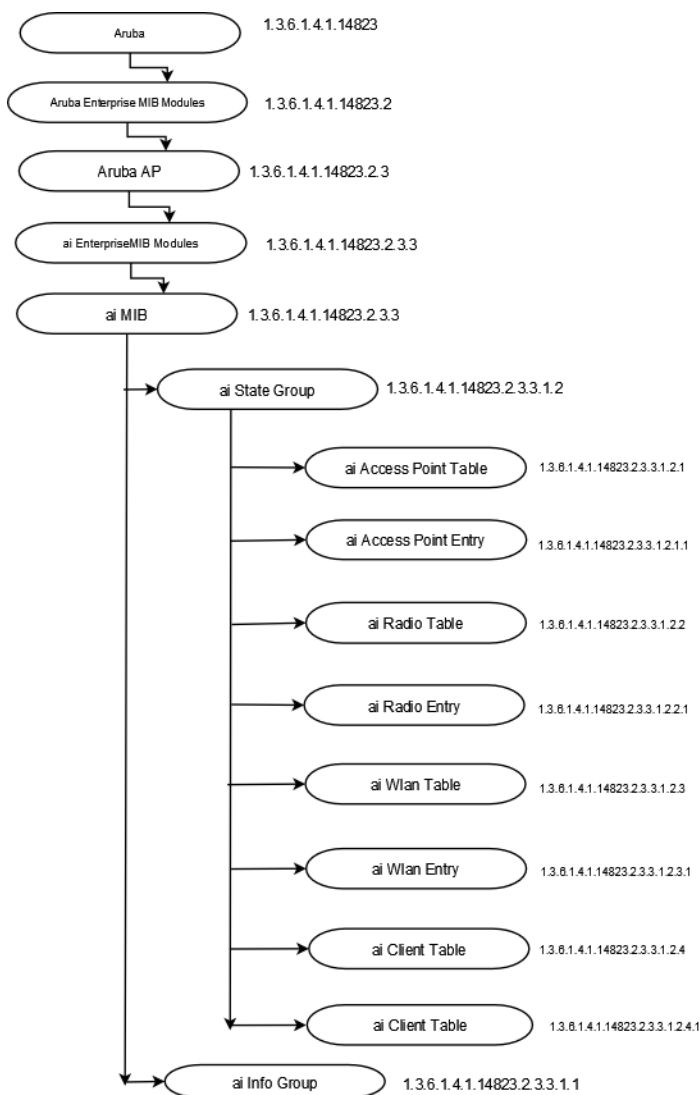
```
# $OV_CONTRIB/NNM/Dell/install
```



The chapter provides information about the Dell Instant MIB, as well as entities that are attempting to access the network.

Figure 4 shows the architecture of the Dell Instant MIB relative to 1.3.6.1.4.1.14823 (iso.org.dod.internet.private.enterprise.dell). The Instant MIB is listed in the file *aruba-instant.my*. For information about downloading Dell Instant MIB file, see “[Downloading MIB Files](#)” on page 23.

**Figure 4** Instant MIB Hierarchy



The supported tables in the Instant MIB are listed and summarized in [Table 5](#). The objects of the supported tables are described in the following sections.

The following table lists the supported tables in the Instant MIB:

**Table 5** *Supported Instant MIB Tables*

Group	Description
aiAccessPointTable	Contains all the access points connected to the virtual controller. This table is indexed by the MAC Address of the IAP.
aiRadioTable	Contains all the radios of the access points connected to the virtual controller. This table is indexed by the MAC Address and radio number.
aiWlanTable	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 IAP.
aiClientTable	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.

## aiAccessPointTable

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

**Table 6** *aiAccessPointTable OIDs*

Object	Object ID	
aiAccessPointEntry	1.3.6.1.4.1.14823.2.3.3.1.2.1.1	aiAccessPointTable 1
aiAPMACAddress	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.1	aiAccessPointEntry 1
aiAPName	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.2	aiAccessPointEntry 2
aiAPIPAddress	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.3	aiAccessPointEntry 3
aiAPSerialNum	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.4	aiAccessPointEntry 4
aiAPModel	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.5	aiAccessPointEntry 5
aiAPModelName	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.6	aiAccessPointEntry 6
aiAPCPUUtilization	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.7	aiAccessPointEntry 7
aiAPMemoryFree	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.8	aiAccessPointEntry 8
aiAPUptime	1.3.6.1.4.1.14823.2.3.3.1.2.1.1.9	aiAccessPointEntry 9

## aiAccessPointEntry

<b>Syntax</b>	aiAccessPointEntry
<b>Max-Access</b>	not-accessible
<b>Status</b>	current
<b>Description</b>	Server entry.
<b>Index</b>	{ authServerName }

## **aiAPMACAddress**

<b>Syntax</b>	MacAddress
<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>	Access Point System OID.

## **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.



## aiRadioTable

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

**Table 7** aiRadioTable OIDs

Object	Object ID	
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
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

## aiRadioEntry

<b>Syntax</b>	aiRadioEntry
<b>Max-Access</b>	not-accessible
<b>Status</b>	current
<b>Description</b>	Server entry.
<b>Index</b>	{ authServerName }

## **aiRadioAPMacAddress**

<b>Syntax</b>	MacAddress
<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**

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

## **aiRadioTransmitPower**

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

## **aiRadioNoiseFloor**

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

## **aiRadioUtilization4**

<b>Syntax</b>	Integer32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Radio channel utilization 4 second average.

## **aiRadioUtilization64**

<b>Syntax</b>	Integer32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	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.

# aiWlanTable

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

**Table 8** aiWlanTable OIDs

Object	Object ID	
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>	Server entry.
<b>Index</b>	{ authServerName }

## aiWlanAPMACAddress

<b>Syntax</b>	MacAddress
<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
<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 9** aiClientTable OID

Object	Object ID	
aiClientTable Entry	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
aiClientAPIAddress	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
aiClientRxDataFrames	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
aiClientRxRetries	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
aiClientRxRate	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

## aiClientTable Entry

<b>Syntax</b>	aiClientTable Entry
<b>Max-Access</b>	not-accessible
<b>Status</b>	current
<b>Description</b>	Server entry.
<b>Index</b>	{ authServerName }

## aiClientMACAddress

<b>Syntax</b>	MacAddress
<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>	IP Address of the associated Access Point.

## **aiClientName**

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

## **aiClientOperatingSystem**

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

## **aiClientSNR**

<b>Syntax</b>	Integer32
<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>	Counter32
<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>	Counter32
<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>	Counter32
<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>	Counter32
<b>Max-Access</b>	read-only
<b>Status</b>	current
<b>Description</b>	Transmission rate of the client in mbps.

## **aiClientRxDataFrames**

<b>Syntax</b>	Counter32
<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>	Counter32
<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>	Counter32
<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>	Integer32
<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.

**Table 10** *SNMP OIDs returned as sysObjectID for Dell Networks products*

SNMP MIB	OID
Dell	.1.3.6.1.4.1.674
PowerConnect products	.1.3.6.1.4.1.674.10895
Dell PowerConnect W-650 Controller	.1.3.6.1.4.1.674.10895.5001
Dell PowerConnect W-651 Controller	.1.3.6.1.4.1.674.10895.5002
Dell PowerConnect W-3200 Controller	.1.3.6.1.4.1.674.10895.5003
Dell PowerConnect W-3400 Controller	.1.3.6.1.4.1.674.10895.5004
Dell PowerConnect W-3600 Controller	.1.3.6.1.4.1.674.10895.5005
Dell PowerConnect W-AP92 Access Point	.1.3.6.1.4.1.674.10895.5006
Dell PowerConnect W-AP93 Access Point	.1.3.6.1.4.1.674.10895.5007
Dell PowerConnect W-AP105 Access Point	.1.3.6.1.4.1.674.10895.5008
Dell PowerConnect W-AP124 Access Point	.1.3.6.1.4.1.674.10895.5009
Dell PowerConnect W-AP125 Access Point	.1.3.6.1.4.1.674.10895.5010
Dell PowerConnect W-RAP5 Access Point	.1.3.6.1.4.1.674.10895.5011
Dell PowerConnect W-RAP5WN Access Point	.1.3.6.1.4.1.674.10895.5012
Dell PowerConnect W-RAP-2 Access Point	.1.3.6.1.4.1.674.10895.5013
Dell PowerConnect W-620 Controller	.1.3.6.1.4.1.674.10895.5014

This section provides lists of the SNMP MIB OIDs that are related to Dell Instant. The following table defines the sysObjectIds for Dell PowerConnect W-Series Instant products.

**Table 11** *SNMP OIDs returned as sysObjectID for Dell PowerConnect W-Series Instant Access products*

SNMP MIB	OID
Dell	.1.3.6.1.4.1.674
PowerConnect products	.1.3.6.1.4.1.674.10895
Dell PowerConnect W-650 Controller	.1.3.6.1.4.1.674.10895.5001
Dell PowerConnect W-651 Controller	.1.3.6.1.4.1.674.10895.5002
Dell PowerConnect W-3200 Controller	.1.3.6.1.4.1.674.10895.5003
Dell PowerConnect W-3400 Controller	.1.3.6.1.4.1.674.10895.5004
Dell PowerConnect W-3600 Controller	.1.3.6.1.4.1.674.10895.5005

**Table 11** *SNMP OIDs returned as sysObjectID for Dell PowerConnect W-Series Instant Access products (Continued)*

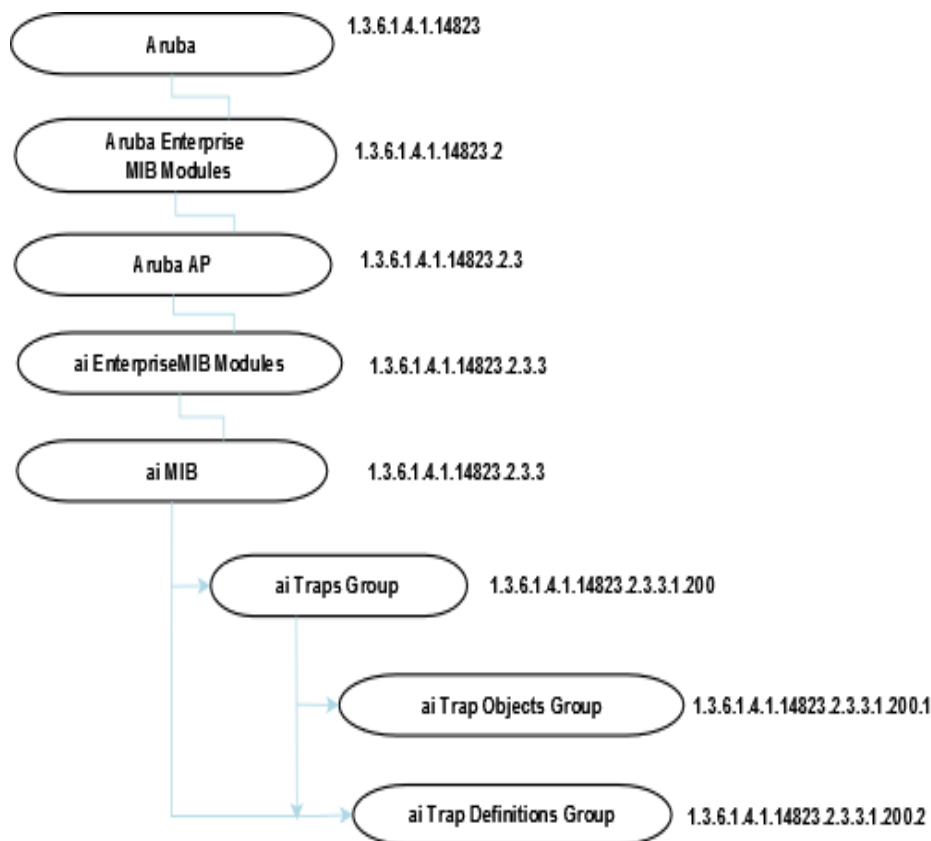
<b>SNMP MIB</b>	<b>OID</b>
Dell PowerConnect W-AP92 Access Point	.1.3.6.1.4.1.674.10895.5006
Dell PowerConnect W-AP93 Access Point	.1.3.6.1.4.1.674.10895.5007
Dell PowerConnect W-AP105 Access Point	.1.3.6.1.4.1.674.10895.5008
Dell PowerConnect W-AP124 Access Point	.1.3.6.1.4.1.674.10895.5009
Dell PowerConnect W-AP125 Access Point	.1.3.6.1.4.1.674.10895.5010
Dell PowerConnect W-RAP5 Access Point	.1.3.6.1.4.1.674.10895.5011
Dell PowerConnect W-RAP5WN Access Point	.1.3.6.1.4.1.674.10895.5012
Dell PowerConnect W-RAP-2 Access Point	.1.3.6.1.4.1.674.10895.5013
Dell PowerConnect W-620 Controller	.1.3.6.1.4.1.674.10895.5014

This module defines the traps that can be generated by the 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). Varbinds are defined in the *Description* section below.

Figure 5 shows the architecture of the Traps MIB relative to 1.3.6.1.4.1.14823 (iso.org.dod.internet.private.enterprise.dell). The Traps are listed in the file *aruba-trap.my* MIB file. For information about downloading Dell MIB files, see “[Downloading MIB Files](#)” on page 23.

### Trap Hierarchy

Figure 5 Trap Hierarchy



## ai Traps Objects Group

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

**Table 12** aiTraps Objects Group OIDs

Object	Object ID	
<a href="#">wlsxTrapAPMacAddress</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.1	wlsxTrapObjectsGroup 1
<a href="#">wlsxTrapAPIpAddress</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.2	wlsxTrapObjectsGroup 2
<a href="#">wlsxTrapAPBSSID</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.3	wlsxTrapObjectsGroup 3
<a href="#">wlsxTrapEssid</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.4	wlsxTrapObjectsGroup 4
<a href="#">wlsxTrapTargetAPBSSID</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.5	wlsxTrapObjectsGroup 5
<a href="#">wlsxTrapTargetAPSSID</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.6	wlsxTrapObjectsGroup 6
<a href="#">wlsxTrapTargetAPChannel</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.7	wlsxTrapObjectsGroup 7
<a href="#">wlsxTrapNodeMac</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.8	wlsxTrapObjectsGroup 8
<a href="#">wlsxTrapSourceMac</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.9	wlsxTrapObjectsGroup 9
<a href="#">wlsxReceiverMac</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.10	wlsxTrapObjectsGroup 10
<a href="#">wlsxTrapTransmitterMac</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.11	wlsxTrapObjectsGroup 11
<a href="#">wlsxTrapReceiverMac</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.12	wlsxTrapObjectsGroup 12
<a href="#">wlsxTrapSnr</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.13	wlsxTrapObjectsGroup 13
<a href="#">wlsxTrapSignatureName</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.14	wlsxTrapObjectsGroup 14
<a href="#">wlsxTrapFrameType</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.15	wlsxTrapObjectsGroup 15
<a href="#">wlsxTrapAddressType</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.16	wlsxTrapObjectsGroup 16
<a href="#">wlsxTrapAPLocation</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.17	wlsxTrapObjectsGroup 17
<a href="#">wlsxTrapAPChannel</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.18	wlsxTrapObjectsGroup 18
<a href="#">wlsxTrapAPTxPower</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.19	wlsxTrapObjectsGroup 19
<a href="#">wlsxTrapMatchedMac</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.20	wlsxTrapObjectsGroup 20
<a href="#">wlsxTrapMatchedIp</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.21	wlsxTrapObjectsGroup 21
<a href="#">wlsxTrapRogueIfoURL</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.22	wlsxTrapObjectsGroup 22
<a href="#">wlsxTrapVLANId</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.23	wlsxTrapObjectsGroup 23
<a href="#">wlsxTrapAdminStatus</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.24	wlsxTrapObjectsGroup 24
<a href="#">wlsxTrapOperStatus</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.25	wlsxTrapObjectsGroup 25
<a href="#">wlsxTrapAuthServerName</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.26	wlsxTrapObjectsGroup 26
<a href="#">wlsxTrapAuthServerTimeout</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.27	wlsxTrapObjectsGroup 27
<a href="#">wlsxTrapCardSlot</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.28	wlsxTrapObjectsGroup 28
<a href="#">wlsxTrapTemperatureValue</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.29	wlsxTrapObjectsGroup 29
<a href="#">wlsxTrapProcessName</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.30	wlsxTrapObjectsGroup 30
<a href="#">wlsxTrapFanNumber</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.31	wlsxTrapObjectsGroup 31
<a href="#">wlsxTrapVoltageType</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.32	wlsxTrapObjectsGroup 32



**Table 12** *aiTraps Objects Group OIDs (Continued)*

Object	Object ID	
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
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	1.3.6.1.4.1.14823.2.3.3.1.200.1.62	wlsxTrapObjectsGroup 62
wlsxTrapConfigurationId	1.3.6.1.4.1.14823.2.3.3.1.200.1.62	wlsxTrapObjectsGroup 63
wlsxTrapCTSURL	1.3.6.1.4.1.14823.2.3.3.1.200.1.63	wlsxTrapObjectsGroup 64
wlsxTrapCTSTransferType	1.3.6.1.4.1.14823.2.3.3.1.200.1.64	wlsxTrapObjectsGroup 65
wlsxTrapConfigurationState	1.3.6.1.4.1.14823.2.3.3.1.200.1.65	wlsxTrapObjectsGroup 66

**Table 12** *aiTraps Objects Group OIDs (Continued)*

Object	Object ID	
wlsxTrapUpdateFailureReason	1.3.6.1.4.1.14823.2.3.3.1.200.1.66	wlsxTrapObjectsGroup 67
wlsxTrapUpdateFailedObj	1.3.6.1.4.1.14823.2.3.3.1.200.1.67	wlsxTrapObjectsGroup 68
wlsxTrapTableEntryChangeType	1.3.6.1.4.1.14823.2.3.3.1.200.1.68	wlsxTrapObjectsGroup 69
wlsxTrapGlobalConfigObj	1.3.6.1.4.1.14823.2.3.3.1.200.1.69	wlsxTrapObjectsGroup 70
wlsxTrapTableGenNumber	1.3.6.1.4.1.14823.2.3.3.1.200.1.70	wlsxTrapObjectsGroup 71
wlsxTrapLicenseId	1.3.6.1.4.1.14823.2.3.3.1.200.1.71	wlsxTrapObjectsGroup 72
wlsxTrapConfidenceLevel	1.3.6.1.4.1.14823.2.3.3.1.200.1.72	wlsxTrapObjectsGroup 73
wlsxTrapMissingLicenses	1.3.6.1.4.1.14823.2.3.3.1.200.1.73	wlsxTrapObjectsGroup 74
wlsxVoiceCurrentNumCdr	1.3.6.1.4.1.14823.2.3.3.1.200.1.74	wlsxTrapObjectsGroup 75
wlsxTrapTunnelId	1.3.6.1.4.1.14823.2.3.3.1.200.1.75	wlsxTrapObjectsGroup 76
wlsxTrapTunnelStatus	1.3.6.1.4.1.14823.2.3.3.1.200.1.76	wlsxTrapObjectsGroup 77
wlsxTrapTunnelUpReason	1.3.6.1.4.1.14823.2.3.3.1.200.1.77	wlsxTrapObjectsGroup 78
wlsxTrapTunnelDownReason	1.3.6.1.4.1.14823.2.3.3.1.200.1.78	wlsxTrapObjectsGroup 79
wlsxTrapApSerialNumber	1.3.6.1.4.1.14823.2.3.3.1.200.1.79	wlsxTrapObjectsGroup 80
wlsxTraptimeStr	1.3.6.1.4.1.14823.2.3.3.1.200.1.80	wlsxTrapObjectsGroup 81
wlsxTrapMasterIp	1.3.6.1.4.1.14823.2.3.3.1.200.1.81	wlsxTrapObjectsGroup 82
wlsxTrapLocalIp	1.3.6.1.4.1.14823.2.3.3.1.200.1.82	wlsxTrapObjectsGroup 83
wlsxTrapMasterName	1.3.6.1.4.1.14823.2.3.3.1.200.1.83	wlsxTrapObjectsGroup 84
wlsxTrapLocalName	1.3.6.1.4.1.14823.2.3.3.1.200.1.84	wlsxTrapObjectsGroup 85
wlsxTrapPrimaryControllerIp	1.3.6.1.4.1.14823.2.3.3.1.200.1.85	wlsxTrapObjectsGroup 86
wlsxTrapBackupControllerIp	1.3.6.1.4.1.14823.2.3.3.1.200.1.86	wlsxTrapObjectsGroup 87
wlsxTrapSpoofedFrameType	1.3.6.1.4.1.14823.2.3.3.1.200.1.87	wlsxTrapObjectsGroup 88
wlsxTrapAssociationType	1.3.6.1.4.1.14823.2.3.3.1.200.1.88	wlsxTrapObjectsGroup 89
wlsxTrapDeviceIpAddress	1.3.6.1.4.1.14823.2.3.3.1.200.1.89	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

**Table 12** *aiTraps Objects Group OIDs (Continued)*

Object	Object ID	
<a href="#">wlsxTrapAPARMChangeReason</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.101	wlsxTrapObjectsGroup 101
<a href="#">wlsxTrapAPChannelSec</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.102	wlsxTrapObjectsGroup 102
<a href="#">wlsxTrapUserAttributeChangeType</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.103	wlsxTrapObjectsGroup 103
<a href="#">wlsxTrapAPControllerIp</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.104	wlsxTrapObjectsGroup 104
<a href="#">wlsxTrapApMasterStatus</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.105	wlsxTrapObjectsGroup 105
<a href="#">wlsxTrapCaName</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.106	wlsxTrapObjectsGroup 106
<a href="#">wlsxTrapCrlName</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.107	wlsxTrapObjectsGroup 107
<a href="#">wlsxTrapCount</a>	1.3.6.1.4.1.14823.2.3.3.1.200.1.108	wlsxTrapObjectsGroup 108

### **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>	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 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.

## **wlsxTrapInterferingAPInfoURL**

<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>	This object represents the ID of the configuration, to be used in traps.

## **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>	INTEGER{success(1),error(2)}
<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.
<b>History</b>	Added in ArubaOS 3.1.0.0.

## wlsxTrapTableEntryChangeType

<b>Syntax</b>	INTEGER {create(1),delete(2), modify(3)}
<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.

## 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.
<b>History</b>	Added in ArubaOS 3.1.0.0.

## **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.
<b>History</b>	Added in ArubaOS 3.4.1

## **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.

## **wlsxTrapVclpAddress**

<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>	This Object represents the AP Mode.

## **wlsxTrapAPPrevChannel**

<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.

## **wlsxTrapAPPrevChannelSec**

<b>Syntax</b>	INTEGER {none(1),above(2),below(3)}
<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.

## **wlsxTrapAPPrevTxPower**

<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>	INTEGER{airMonitor(1),accessPoint(2),accessPointAndMonitor(3),meshPortal(4),meshPoint(5),rfprotectSensor(6),spectrumSensor(7)}
<b>Max-Access</b>	accessible-for-notify
<b>Status</b>	current
<b>Description</b>	This Object represents the APs Current Mode.

## wlsxTrapAPPrevMode

<b>Syntax</b>	INTEGER{airMonitor(1),accessPoint(2),accessPointAndMonitor(3),meshPortal(4),meshPoint(5),rfprotectSensor(6),spectrumSensor(7)}
<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>	INTEGER{radarDetected(1),radarCleared(2),txHang(3),txHangClear(4),fortyMhzIntol(5),cancel40mhzIntol(6),fortyMhzAlign(7),armInterference(8),armInvalidCh(9),armErrorThresh(10),armNoiseThresh(11),armEmptyCh(12),armRogueCont(13),armDecreasePower(14),armIncreasePower(15),armTurnOffRadio(16),armTurnOnRadio(17)}
<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>	INTEGER {none(1),above(2),below(3)}
<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>	INTEGER {create(1),delete(2),modify(3)}
<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>	IP address of the controller to which the AP is (or was most recently) registered.

## **wlsxTrapApMasterStatus**

<b>Syntax</b>	INTEGER {create(1),delete(2),modify(3)}
<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>	This object is used in the traps to indicate the name of the trustpoint.

## **wlsxTrapCrIName**

<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.

## ai Traps Definitions Group

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

Object	Object ID	
wlsxNodeRateAnomaly	1.3.6.1.4.1.14823.2.3.3.1.200.2.1003	wlsxTrapDefinitionsGroup 1003
wlsxNUserEntryCreated	1.3.6.1.4.1.14823.2.3.3.1.200.2.1014	wlsxTrapDefinitionsGroup 1014
wlsxNUserEntryDeleted	1.3.6.1.4.1.14823.2.3.3.1.200.2.1015	wlsxTrapDefinitionsGroup 1015
wlsxNUserEntryAuthenticated	1.3.6.1.4.1.14823.2.3.3.1.200.2.1016	wlsxTrapDefinitionsGroup 1016
wlsxNUserEntryDeAuthenticated	1.3.6.1.4.1.14823.2.3.3.1.200.2.1017	wlsxTrapDefinitionsGroup 1017
wlsxNUserAuthenticationFailed	1.3.6.1.4.1.14823.2.3.3.1.200.2.1018	wlsxTrapDefinitionsGroup 1018
wlsxNAuthServerReqTimedOut	1.3.6.1.4.1.14823.2.3.3.1.200.2.1019	wlsxTrapDefinitionsGroup 1019
wlsxNAuthServerTimedOut	1.3.6.1.4.1.14823.2.3.3.1.200.2.1020	wlsxTrapDefinitionsGroup 1020
wlsxNAuthServerIsUp	1.3.6.1.4.1.14823.2.3.3.1.200.2.1021	wlsxTrapDefinitionsGroup 1021
wlsxNAccessPointsUp	1.3.6.1.4.1.14823.2.3.3.1.200.2.1040	wlsxTrapDefinitionsGroup 1040
wlsxNAccessPointsDown	1.3.6.1.4.1.14823.2.3.3.1.200.2.1041	wlsxTrapDefinitionsGroup 1041
wlsxNChannelChanged	1.3.6.1.4.1.14823.2.3.3.1.200.2.1043	wlsxTrapDefinitionsGroup 1043
wlsxNStationAddedToBlackList	1.3.6.1.4.1.14823.2.3.3.1.200.2.1044	wlsxTrapDefinitionsGroup 1044
wlsxNStationRemovedFromBlackList	1.3.6.1.4.1.14823.2.3.3.1.200.2.1045	wlsxTrapDefinitionsGroup 1045
wlsxNRadioAttributesChanged	1.3.6.1.4.1.14823.2.3.3.1.200.2.1049	wlsxTrapDefinitionsGroup 1049
wlsxUnsecureAPDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1053	wlsxTrapDefinitionsGroup 1053
wlsxUnsecureAPResolved	1.3.6.1.4.1.14823.2.3.3.1.200.2.1054	wlsxTrapDefinitionsGroup 1054
wlsxStalmpersonation	1.3.6.1.4.1.14823.2.3.3.1.200.2.1055	wlsxTrapDefinitionsGroup 1055
wlsxReservedChannelViolation	1.3.6.1.4.1.14823.2.3.3.1.200.2.1056	wlsxTrapDefinitionsGroup 1056
wlsxValidSSIDViolation	1.3.6.1.4.1.14823.2.3.3.1.200.2.1057	wlsxTrapDefinitionsGroup 1057

**Table 13** *ai Traps Definitions Group OIDs (Continued)*

<b>Object</b>	<b>Object ID</b>	
wlsxChannelMisconfiguration	1.3.6.1.4.1.14823.2.3.3.1.200.2.1058	wlsxTrapDefinitionsGroup 1058
wlsxOUIMisconfiguration	1.3.6.1.4.1.14823.2.3.3.1.200.2.1059	wlsxTrapDefinitionsGroup 1059
wlsxSSIDMisconfiguration	1.3.6.1.4.1.14823.2.3.3.1.200.2.1060	wlsxTrapDefinitionsGroup 1060
wlsxShortPreambleMisconfiguration	1.3.6.1.4.1.14823.2.3.3.1.200.2.1061	wlsxTrapDefinitionsGroup 1061
wlsxWPAMisconfiguration	1.3.6.1.4.1.14823.2.3.3.1.200.2.1062	wlsxTrapDefinitionsGroup 1062
wlsxAdhocNetworkDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1063	wlsxTrapDefinitionsGroup 1063
wlsxAdhocNetworkRemoved	1.3.6.1.4.1.14823.2.3.3.1.200.2.1064	wlsxTrapDefinitionsGroup 1064
wlsxStaPolicyViolation	1.3.6.1.4.1.14823.2.3.3.1.200.2.1065	wlsxTrapDefinitionsGroup 1065
wlsxRepeatWEPIVViolation	1.3.6.1.4.1.14823.2.3.3.1.200.2.1066	wlsxTrapDefinitionsGroup 1066
wlsxWeakWEPIVViolation	1.3.6.1.4.1.14823.2.3.3.1.200.2.1067	wlsxTrapDefinitionsGroup 1067
wlsxChannelInterferenceDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1068	wlsxTrapDefinitionsGroup 1068
wlsxChannelInterferenceCleared	1.3.6.1.4.1.14823.2.3.3.1.200.2.1069	wlsxTrapDefinitionsGroup 1069
wlsxAPIInterferenceDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1070	wlsxTrapDefinitionsGroup 1070
wlsxAPIInterferenceCleared	1.3.6.1.4.1.14823.2.3.3.1.200.2.1071	wlsxTrapDefinitionsGroup 1071
wlsxStaInterferenceDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1072	wlsxTrapDefinitionsGroup 1072
wlsxStaInterferenceCleared	1.3.6.1.4.1.14823.2.3.3.1.200.2.1073	wlsxTrapDefinitionsGroup 1073
wlsxFrameRetryRateExceeded	1.3.6.1.4.1.14823.2.3.3.1.200.2.1074	wlsxTrapDefinitionsGroup 1074
wlsxFrameReceiveErrorRateExceeded	1.3.6.1.4.1.14823.2.3.3.1.200.2.1075	wlsxTrapDefinitionsGroup 1075
wlsxFrameFragmentationRateExceeded	1.3.6.1.4.1.14823.2.3.3.1.200.2.1076	wlsxTrapDefinitionsGroup 1076
wlsxFrameBandWidthRateExceeded	1.3.6.1.4.1.14823.2.3.3.1.200.2.1077	wlsxTrapDefinitionsGroup 1077
wlsxFrameLowSpeedRateExceeded	1.3.6.1.4.1.14823.2.3.3.1.200.2.1078	wlsxTrapDefinitionsGroup 1078

**Table 13** *ai Traps Definitions Group OIDs (Continued)*

<b>Object</b>	<b>Object ID</b>	
wlsxFrameNonUnicastRateExceeded	1.3.6.1.4.1.14823.2.3.3.1.200.2.1079	wlsxTrapDefinitionsGroup 1079
wlsxLoadbalancingEnabled	1.3.6.1.4.1.14823.2.3.3.1.200.2.1080	wlsxTrapDefinitionsGroup 1080
wlsxLoadbalancingDisabled	1.3.6.1.4.1.14823.2.3.3.1.200.2.1081	wlsxTrapDefinitionsGroup 1081
wlsxChannelFrameRetryRateExceeded	1.3.6.1.4.1.14823.2.3.3.1.200.2.1082	wlsxTrapDefinitionsGroup 1082
wlsxChannelFrameFragmentationRateExceeded	1.3.6.1.4.1.14823.2.3.3.1.200.2.1083	wlsxTrapDefinitionsGroup 1083
wlsxChannelFrameErrorRateExceeded	1.3.6.1.4.1.14823.2.3.3.1.200.2.1084	wlsxTrapDefinitionsGroup 1084
wlsxSignatureMatchAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1085	wlsxTrapDefinitionsGroup 1085
wlsxSignatureMatchSta	1.3.6.1.4.1.14823.2.3.3.1.200.2.1086	wlsxTrapDefinitionsGroup 1086
wlsxChannelRateAnomaly	1.3.6.1.4.1.14823.2.3.3.1.200.2.1087	wlsxTrapDefinitionsGroup 1087
wlsxNodeRateAnomalyAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1088	wlsxTrapDefinitionsGroup 1088
wlsxNodeRateAnomalySta	1.3.6.1.4.1.14823.2.3.3.1.200.2.1089	wlsxTrapDefinitionsGroup 1089
wlsxEAPRateAnomaly	1.3.6.1.4.1.14823.2.3.3.1.200.2.1090	wlsxTrapDefinitionsGroup 1090
wlsxSignalAnomaly	1.3.6.1.4.1.14823.2.3.3.1.200.2.1091	wlsxTrapDefinitionsGroup 1091
wlsxSequenceNumberAnomalyAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1092	wlsxTrapDefinitionsGroup 1092
wlsxSequenceNumberAnomalySta	1.3.6.1.4.1.14823.2.3.3.1.200.2.1093	wlsxTrapDefinitionsGroup 1093
wlsxDisconnectStationAttack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1094	wlsxTrapDefinitionsGroup 1094
wlsxApFloodAttack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1095	wlsxTrapDefinitionsGroup 1095
wlsxAdhocNetwork	1.3.6.1.4.1.14823.2.3.3.1.200.2.1096	wlsxTrapDefinitionsGroup 1096
wlsxWirelessBridge	1.3.6.1.4.1.14823.2.3.3.1.200.2.1097	wlsxTrapDefinitionsGroup 1097
wlsxInvalidMacOUIAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1098	wlsxTrapDefinitionsGroup 1098
wlsxInvalidMacOUISta	1.3.6.1.4.1.14823.2.3.3.1.200.2.1099	wlsxTrapDefinitionsGroup 1099



**Table 13** *ai Traps Definitions Group OIDs (Continued)*

<b>Object</b>	<b>Object ID</b>	
wlsxWEPMisconfiguration	1.3.6.1.4.1.14823.2.3.3.1.200.2.1100	wlsxTrapDefinitionsGroup 1100
wlsxStaRepeatWEPIVViolation	1.3.6.1.4.1.14823.2.3.3.1.200.2.1101	wlsxTrapDefinitionsGroup 1101
wlsxStaWeakWEPIVViolation	1.3.6.1.4.1.14823.2.3.3.1.200.2.1102	wlsxTrapDefinitionsGroup 1102
wlsxStaAssociatedToUnsecureAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1103	wlsxTrapDefinitionsGroup 1103
wlsxStaUnAssociatedFromUnsecure AP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1104	wlsxTrapDefinitionsGroup 1104
wlsxAdhocNetworkBridgeDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1105	wlsxTrapDefinitionsGroup 1105
wlsxInterferingApDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1106	wlsxTrapDefinitionsGroup 1106
wlsxColdStart	1.3.6.1.4.1.14823.2.3.3.1.200.2.1111	wlsxTrapDefinitionsGroup 1111
wlsxWarmStart	1.3.6.1.4.1.14823.2.3.3.1.200.2.1112	wlsxTrapDefinitionsGroup 1112
wlsxAPImpersonation	1.3.6.1.4.1.14823.2.3.3.1.200.2.1113	wlsxTrapDefinitionsGroup 1113
wlsxNAuthServerIsDown	1.3.6.1.4.1.14823.2.3.3.1.200.2.1115	wlsxTrapDefinitionsGroup 1115
wlsxWindowsBridgeDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1129	wlsxTrapDefinitionsGroup 1129
wlsxSignAPNetstumbler	1.3.6.1.4.1.14823.2.3.3.1.200.2.1134	wlsxTrapDefinitionsGroup 1134
wlsxSignStaNetstumbler	1.3.6.1.4.1.14823.2.3.3.1.200.2.1135	wlsxTrapDefinitionsGroup 1135
wlsxSignAPAsleep	1.3.6.1.4.1.14823.2.3.3.1.200.2.1136	wlsxTrapDefinitionsGroup 1136
wlsxSignStaAsleep	1.3.6.1.4.1.14823.2.3.3.1.200.2.1137	wlsxTrapDefinitionsGroup 1137
wlsxSignAPAirjack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1138	wlsxTrapDefinitionsGroup 1138
wlsxSignStaAirjack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1139	wlsxTrapDefinitionsGroup 1139
wlsxSignAPNullProbeResp	1.3.6.1.4.1.14823.2.3.3.1.200.2.1140	wlsxTrapDefinitionsGroup 1140
wlsxSignStaNullProbeResp	1.3.6.1.4.1.14823.2.3.3.1.200.2.1141	wlsxTrapDefinitionsGroup 1141
wlsxSignAPDeathBcast	1.3.6.1.4.1.14823.2.3.3.1.200.2.1142	wlsxTrapDefinitionsGroup 1142

**Table 13** *ai Traps Definitions Group OIDs (Continued)*

<b>Object</b>	<b>Object ID</b>	
wlsxSignStaDeathBcast	1.3.6.1.4.1.14823.2.3.3.1.200.2.1143	wlsxTrapDefinitionsGroup 1143
wlsxWindowsBridgeDetectedAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1144	wlsxTrapDefinitionsGroup 1144
wlsxWindowsBridgeDetectedSta	1.3.6.1.4.1.14823.2.3.3.1.200.2.1145	wlsxTrapDefinitionsGroup 1145
wlsxAdhocNetworkBridgeDetectedAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1146	wlsxTrapDefinitionsGroup 1146
wlsxAdhocNetworkBridgeDetectedSta	1.3.6.1.4.1.14823.2.3.3.1.200.2.1147	wlsxTrapDefinitionsGroup 1147
wlsxDisconnectStationAttackAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1148	wlsxTrapDefinitionsGroup 1148
wlsxDisconnectStationAttackSta	1.3.6.1.4.1.14823.2.3.3.1.200.2.1149	wlsxTrapDefinitionsGroup 1149
wlsxSuspectUnsecureAPDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1150	wlsxTrapDefinitionsGroup 1150
wlsxSuspectUnsecureAPResolved	1.3.6.1.4.1.14823.2.3.3.1.200.2.1151	wlsxTrapDefinitionsGroup 1151
wlsxHtGreenfieldSupported	1.3.6.1.4.1.14823.2.3.3.1.200.2.1157	wlsxTrapDefinitionsGroup 1157
wlsxHT40MHzIntoleranceAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1158	wlsxTrapDefinitionsGroup 1158
wlsxHT40MHzIntoleranceSta	1.3.6.1.4.1.14823.2.3.3.1.200.2.1159	wlsxTrapDefinitionsGroup 1159
wlsxNAdhocNetwork	1.3.6.1.4.1.14823.2.3.3.1.200.2.1161	wlsxTrapDefinitionsGroup 1161
wlsxNAdhocNetworkBridgeDetectedAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1162	wlsxTrapDefinitionsGroup 1162
wlsxNAdhocNetworkBridgeDetectedSta	1.3.6.1.4.1.14823.2.3.3.1.200.2.1163	wlsxTrapDefinitionsGroup 1163
wlsxClientFloodAttack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1170	wlsxTrapDefinitionsGroup 1170
wlsxValidClientNotUsingEncryption	1.3.6.1.4.1.14823.2.3.3.1.200.2.1171	wlsxTrapDefinitionsGroup 1171
wlsxAdhocUsingValidSSID	1.3.6.1.4.1.14823.2.3.3.1.200.2.1172	wlsxTrapDefinitionsGroup 1172
wlsxAPspoofingDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1173	wlsxTrapDefinitionsGroup 1173
wlsxClientAssociatingOnWrongChannel	1.3.6.1.4.1.14823.2.3.3.1.200.2.1174	wlsxTrapDefinitionsGroup 1174
wlsxNDisconnectStationAttack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1175	wlsxTrapDefinitionsGroup 1175

**Table 13** *ai Traps Definitions Group OIDs (Continued)*

<b>Object</b>	<b>Object ID</b>	
wlsxNStaUnAssociatedFromUnsecur eAP	1.3.6.1.4.1.14823.2.3.3.1.200.2.1176	wlsxTrapDefinitionsGroup 1176
wlsxOmertaAttack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1177	wlsxTrapDefinitionsGroup 1177
wlsxTKIPReplayAttack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1178	wlsxTrapDefinitionsGroup 1178
wlsxChopChopAttack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1179	wlsxTrapDefinitionsGroup 1179
wlsxFataJackAttack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1180	wlsxTrapDefinitionsGroup 1180
wlsxInvalidAddressCombination	1.3.6.1.4.1.14823.2.3.3.1.200.2.1181	wlsxTrapDefinitionsGroup 1181
wlsxValidClientMisassociation	1.3.6.1.4.1.14823.2.3.3.1.200.2.1182	wlsxTrapDefinitionsGroup 1182
wlsxMalformedHTIEDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1183	wlsxTrapDefinitionsGroup 1183
wlsxMalformedAssocReqDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1184	wlsxTrapDefinitionsGroup 1184
wlsxOverflowIEDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1185	wlsxTrapDefinitionsGroup 1185
wlsxOverflowEAPOLKeyDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1186	wlsxTrapDefinitionsGroup 1186
wlsxMalformedFrameLargeDurationD etected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1187	wlsxTrapDefinitionsGroup 1187
wlsxMalformedFrameWrongChannel Detected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1188	wlsxTrapDefinitionsGroup 1188
wlsxMalformedAuthFrame	1.3.6.1.4.1.14823.2.3.3.1.200.2.1189	wlsxTrapDefinitionsGroup 1189
wlsxCTSRateAnomaly	1.3.6.1.4.1.14823.2.3.3.1.200.2.1190	wlsxTrapDefinitionsGroup 1190
wlsxRTSRateAnomaly	1.3.6.1.4.1.14823.2.3.3.1.200.2.1191	wlsxTrapDefinitionsGroup 1191
wlsxNRogueAPDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1192	wlsxTrapDefinitionsGroup 1192
wlsxNRogueAPResolved	1.3.6.1.4.1.14823.2.3.3.1.200.2.1193	wlsxTrapDefinitionsGroup 1193
wlsxNeighborAPDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1194	wlsxTrapDefinitionsGroup 1194
wlsxNInterferingAPDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1195	wlsxTrapDefinitionsGroup 1195
wlsxNSuspectRogueAPDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1196	wlsxTrapDefinitionsGroup 1196

**Table 13** *ai Traps Definitions Group OIDs (Continued)*

<b>Object</b>	<b>Object ID</b>	
wlsxNSuspectRogueAPResolved	1.3.6.1.4.1.14823.2.3.3.1.200.2.1197	wlsxTrapDefinitionsGroup 1197
wlsxBlockAckAttackDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1198	wlsxTrapDefinitionsGroup 1198
wlsxHotspotterAttackDetected	1.3.6.1.4.1.14823.2.3.3.1.200.2.1199	wlsxTrapDefinitionsGroup 1199
wlsxNSignatureMatch	1.3.6.1.4.1.14823.2.3.3.1.200.2.1200	wlsxTrapDefinitionsGroup 1200
wlsxNSignatureMatchNetstumbler	1.3.6.1.4.1.14823.2.3.3.1.200.2.1201	wlsxTrapDefinitionsGroup 1201
wlsxNSignatureMatchAsleep	1.3.6.1.4.1.14823.2.3.3.1.200.2.1202	wlsxTrapDefinitionsGroup 1202
wlsxNSignatureMatchAirjack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1203	wlsxTrapDefinitionsGroup 1203
wlsxNSignatureMatchNullProbeResp	1.3.6.1.4.1.14823.2.3.3.1.200.2.1204	wlsxTrapDefinitionsGroup 1204
wlsxNSignatureMatchDeathBcast	1.3.6.1.4.1.14823.2.3.3.1.200.2.1205	wlsxTrapDefinitionsGroup 1205
wlsxNSignatureMatchDisassocBcast	1.3.6.1.4.1.14823.2.3.3.1.200.2.1206	wlsxTrapDefinitionsGroup 1206
wlsxNSignatureMatchWellenreiter	1.3.6.1.4.1.14823.2.3.3.1.200.2.1207	wlsxTrapDefinitionsGroup 1207
wlsxAPDeathContainment	1.3.6.1.4.1.14823.2.3.3.1.200.2.1208	wlsxTrapDefinitionsGroup 1208
wlsxClientDeathContainment	1.3.6.1.4.1.14823.2.3.3.1.200.2.1209	wlsxTrapDefinitionsGroup 1209
wlsxAPWiredContainment	1.3.6.1.4.1.14823.2.3.3.1.200.2.1210	wlsxTrapDefinitionsGroup 1210
wlsxClientWiredContainment	1.3.6.1.4.1.14823.2.3.3.1.200.2.1211	wlsxTrapDefinitionsGroup 1211
wlsxAPTaggedWiredContainment	1.3.6.1.4.1.14823.2.3.3.1.200.2.1212	wlsxTrapDefinitionsGroup 1212
wlsxClientTaggedWiredContainment	1.3.6.1.4.1.14823.2.3.3.1.200.2.1213	wlsxTrapDefinitionsGroup 1213
wlsxTarpitContainment	1.3.6.1.4.1.14823.2.3.3.1.200.2.1214	wlsxTrapDefinitionsGroup 1214
wlsxAPChannelChange	1.3.6.1.4.1.14823.2.3.3.1.200.2.1216	wlsxTrapDefinitionsGroup 1216
wlsxAPPowerChange	1.3.6.1.4.1.14823.2.3.3.1.200.2.1217	wlsxTrapDefinitionsGroup 1217
wlsxAPModeChange	1.3.6.1.4.1.14823.2.3.3.1.200.2.1218	wlsxTrapDefinitionsGroup 1218

**Table 13** *ai Traps Definitions Group OIDs (Continued)*

Object	Object ID	
wlsxUserEntryAttributesChanged	1.3.6.1.4.1.14823.2.3.3.1.200.2.1219	wlsxTrapDefinitionsGroup 1219
wlsxPowerSaveDosAttack	1.3.6.1.4.1.14823.2.3.3.1.200.2.1220	wlsxTrapDefinitionsGroup 1220
wlsxNAPMasterStatusChange	1.3.6.1.4.1.14823.2.3.3.1.200.2.1221	wlsxTrapDefinitionsGroup 1221
wlsxNAdhocUsingValidSSID	1.3.6.1.4.1.14823.2.3.3.1.200.2.1022	wlsxTrapDefinitionsGroup 1222
wlsxMgmtUserAuthenticationFailed	1.3.6.1.4.1.14823.2.3.3.1.200.2.1024	wlsxTrapDefinitionsGroup 1224

**wlsxNodeRateAnomaly**

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapFrameType, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation }
<b>Status</b>	current
<b>Description</b>	This trap indicates that a node is exceeding the threshold set for the frame type.

**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, wlsxTrapUserAuthenticatio 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.

## **wlsxNAccessPointsUp**

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

## **wlsxNAccessPointsDown**

<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.

## **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.

## **wlsxStalmpersonation**

<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, wlsxTrap, TargetAPBSSID, 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 Ad hocnetwork.

## 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 Ad hoc 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 info check: <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-2005-0019">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 info 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.

## **wlsxStalInterferenceDetected**

<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.

## **wlsxStalInterferenceCleared**

<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>	This trap indicates that an AM is reporting that an AP has enabled Load balancing.

## **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 disabled 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 info 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>

## 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 info 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 info 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>	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. For more info 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>

## wlsxSequenceNumberAnomalySta

<b>Objects</b>	{ wlsxTrapTime, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation }
<b>Status</b>	current
<b>Description</b>	The acceptable sequence number difference is an IDS configuration object. For more info 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>

## wlsxDisconnectStationAttack

<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 info 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>

## 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 info 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 AdhocNetwork. An Station is connected to an ad hoc 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 Ad hoc 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 or 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 info 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 info check: <a href="http://www.wve.org/entries/show/WVE-2005-0025">http://www.wve.org/entries/show/WVE-2005-0025</a>

## wlsxSignAPAsleep

<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 info check: <a href="http://www.wve.org/entries/show/WVE-2005-0027">http://www.wve.org/entries/show/WVE-2005-0027</a>

## wlsxSignStaAsleep

<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 info 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 info 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 info 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 info 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 info check: <a href="http://www.wve.org/entries/show/WVE-2006-0064">http://www.wve.org/entries/show/WVE-2006-0064</a>

## wlsxSignAPDeauthBcast

<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 Deauth-Broadcast from an access point. For more info 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>

## wlsxSignStaDeauthBcast

<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 Deauth-Broadcast from a Station. For more info 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 Ad hoc network that is bridging to a wired network

## wlsxAdhocNetworkBridgeDetectedSta

<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 Ad hoc 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 info 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, wlsxTrapTargetAPBSSID, wlsxTrapTargetAPSSID, wlsxTrapSourceMac, wlsxTrapSnr, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation, wlsxTrapAPChannel }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AM detected a station Disconnect attack. For more info 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.

## 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 info 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 info 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 ad hoc network where a station is connected to an ad hoc 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 ad hoc 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 ad hoc network that is bridging to a wired network.

## wlsxClientFloodAttack

<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 info 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 ad hoc network using a valid/protected SSID. For more info check: <a href="http://www.wve.org/entries/show/WVE-2005-0008">http://www.wve.org/entries/show/WVE-2005-0008</a>

## wlsxAPSpooftingDetected

<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 info 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 info 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 info 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 info 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 info 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, wlsxTrapAPMacAddress, wlsxTrapBackupControllerIp, wlsxTrapPrimaryControllerIp }
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP detected a FATA-Jack attack. For more info 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 info 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 info 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 info 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 info 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 info 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, wlsxTrapTargetAPSSID, 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 info 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 info 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 info 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 info 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 info 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 info 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 info 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 info 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 info 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 info 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 info 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.

## wlsxClietWiredContainment

<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.

## wlsxClietTaggedWiredContainment

<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, wlsxTrapAPPrevChannel, wlsxTrapAPPrevChannelSec, 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, wlsxTrapAPTxPower, 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, wlsxTrapAPPprevMode, wlsxTrapAPMacAddress, wlsxTrapAPRadioNumber, wlsxTrapAPLocation
<b>Status</b>	current
<b>Description</b>	This trap indicates that an AP changed its mode from AP to APMonitor 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 ad hoc network node using a valid/protected SSID. For more info 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>	This trap indicates that a management user authentication has failed.



## A

Agents 21

## D

Description 21

## E

Entry 26

## G

group 26

## H

History

ArubaOS 3.1

lsxVoiceCurrentNumCdr 64

wlsxTrapConfidenceLevel 63

wlsxTrapConfigurationId 62

wlsxTrapConfigurationState 62

wlsxTrapCTSTransferType 62

wlsxTrapCTSURL 62

wlsxTrapGlobalConfigObj 63

wlsxTrapLicenseId 63

wlsxTrapMissingLicenses 63

wlsxTrapTableEntryChangeType 63

wlsxTrapTableGenNumber 63

wlsxTrapTunnelId 64

wlsxTrapTunnelStatus 64

wlsxTrapTunnelUpReason 64

wlsxTrapUpdateFailedObj 62

wlsxTrapUpdateFailureReason 62

ArubaOS 3.4

wlsxTrapAPSerialNumber 64

wlsxTraptimeStr 65

ArubaOS 3.4.1

wlsxTrapBackupControllerIp 66

wlsxTrapMasterIp 65

wlsxTrapMasterName 65

wlsxTrapPrimaryControllerIp 65

## M

Managers 21

Max-Access 21

MIB files 23

MIB objects 26

## P

pLocalName 65

## S

Sequence 21

Status 21

Syntax 21

## T

Traps

MIB hierarchy 47

## X

xTrapLocalIp 65

