Avaya WLAN - Security Switch 2300 Series Release Notes – Software Release 7.1

Avaya WLAN 2300

7.1

Document Status: **Standard**

Document Number: **NN47250-400**

Document Version: **05.02**

Notices
While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer
Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer
Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty
Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support
Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

Licenses
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright
Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components
Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks
The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Downloading documents
For the most current versions of documentation, see the Avaya Support. Web site: http://www.avaya.com/support

Contact Avaya Support
Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

Customer service 6
Navigation 6
Getting technical documentation 6
Getting product training 6
Getting help from a distributor or reseller 6
Getting technical support from the Avaya Web site 6

Regulatory information 8
Global changes in Release 6.0.7 8
Global changes in Release 6.0.5.1 9
Global changes in Release 6.0 10
Series 2332 Access Points Region Lock Mechanism 12
IEEE 802.11a/b/g Channel Designations: 14
2400 - 2483.5 MHz band 14
5.15 - 5.35 GHz bands 15
5.470 - 5.725 GHz bands 15
5.725 - 5.85 GHz bands 15
Series 2332 Access Points Country to Region Map 16
Global Changes in Release 7.0 17

Avaya WLAN - Security Switch 2300 Series Release Notes – Software Release 7.1 19
What's new in WSS Software version 7.1 20
Trapeze Virtual Controller Cluster Enhancements 21
SIP Awareness 21
LDAP Authentication Support 21
Version compatibility 22
WLAN Management System 22
Minimum WSS Software requirements for upgrade 22
Upgrading to WSS version 7.1 22
Preparing the WSS for the Upgrade 23
Upgrading an individual WSS using the CLI 23
Upgrade scenario 24

Installing Upgrade Activation Keys on a WSS 25
System parameter support 27
Best practices and common issues 31
Best practices when powering down a switch 31
System configuration best practices 31
Client and Web-based AAA best practices 31
Security best practices 38
VLANs 40
Web-based AAA best practices 41
Mobility Domain™ (Multiple WSSs) best practices 41
Distributed AP best practice when using STP 41
Use IGMP snooping effectively 42
User ACLs require explicit source and destination addresses 42
Rogue detection active scan interval is longer during a SpectraLink SVP call. (23317) 42
IPv6 support 43
VoIP devices vendor support 43
Interoperability 44
Wireless NICs tested with Avaya WSS Software 44
Known behaviors and issues 47
Mesh Services 49
System configuration issues 49
Switching and port issues 50
Access Point (AP) issues 50
Web-based AAA issues 50
Web View Issues 51
DAP to AP conversion during Upgrade from Release 5.0 to 6.0 51
Upgrading an individual switch using the CLI 52
Migrating your Web-based AAA and Last-Resort configurations from WSS Software version 5.*x* to WSS Software version 6.0 or later 53
WSS 2380, 2382, and MX-2800 supported AP license activation key upgrade . . 55
Issues resolved since version 7.1.5.4 56
Changes to Default Behaviors in WSS 57
Documentation Errata 57
Issues resolved since version 6.0.5.1 58
Issues resolved since version 6.0.4.6 59

Issues resolved since version 5.0.11.4 59
Issues resolved in version 5.0.9.4 66
Issues resolved since version 4.1.13 70

Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

Navigation

- "Getting technical documentation"
- "Getting product training"
- "Getting help from a distributor or reseller"
- "Getting technical support from the Avaya Web site"

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, you can access the Web site at www.avaya.com/support. From this Web site, you can locate the Training contacts link on the left-hand navigation pane.

Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.

Regulatory information

Global changes in Release 6.0.7

COUNTRY	GENERAL CHANGES
Global	- Added Outdoor support for the following 2332 models: A1, A2, A6, E1, E2, E3, E4, E6, E8, E9. This includes adding external antenna tabs for -OUT, -OUT-10, -OUT-25, -NEMA, -NEMA-10, -NEMA-25 for the following external antennas on each supported model: 24493, 24882, 24113, 24123, 24143 for all models; 5643, 5133, 5173, 5103 for all models except A6 and E9.
Global	- Removed support for the EU & EFTA countries for the 2330B for all antennas in both 2.4 GHz & 5.0 GHz bands.
COUNTRY	**ASIA PACIFIC**
China	- Disabled operation for all external antennas for China in the 2332-E8 model.
Japan	- Disabled operation on CH 14 for the 24553, 24883, 24123 & 24143 antennas per Japanese certification. - Added 24493, 24553 & 24123 antennas to the 2332-J1 model.
COUNTRY	**EU & Europe**
Israel	- Enabled DFS in the 5150 - 5250 MHz band.

Global changes in Release 6.0.5.1

COUNTRY	ASIA PACIFIC
Hong Kong	- Corrected regulatory settings for the Internal & Mixed antennas for the 5250 - 5350 MHz band. - Modified the 5150 - 5250 & 5250 - 5350 MHz bands to follow the ETSI test requirements. - Modified the 2.4 GHz band to follow the FCC settings for operation with no band-edge restrictions.
India	- Modified the 5150 - 5250 & 5250 - 5350 MHz bands to follow the ETSI test requirements. - Modified the 2.4 GHz band to follow the FCC settings for operation with no band-edge restrictions.
Malaysia	- Modified the 5250 - 5350 & 5725 - 5850 MHz bands to meet the correct regulatory EIRP limits.
Philippines	- Modified the 5150 - 5250 & 5250 - 5350 MHz bands to follow the ETSI test requirements. - Modified the 5470 - 5725 & 5725 - 5850 MHz bands to meet the correct regulatory EIRP limits.
Singapore	- Modified the 5150 - 5250 & 5250 - 5350 MHz bands to follow the ETSI test requirements.
Vietnam	- Modified the 5150 - 5250 & 5250 - 5350 MHz bands to follow the ETSI test requirements.
COUNTRY	**CALA**
Columbia	- Modified the 5470 - 5725 MHz band to follow the FCC test requirements.
Paraguay	- Modified the 5150 - 5250 & 5250 - 5350 MHz bands to follow the ETSI test requirements.
Peru	- Modified the 5150 - 5250 & 5250 - 5350 MHz bands to follow the ETSI test requirements.
Uruguay	- Modified the 5150 - 5250 & 5250 - 5350 MHz bands to follow the ETSI test requirements.
COUNTRY	**EU & Europe**
Croatia	-Disabled operation in the 5250 - 5350 & 5470 - 5725 MHz bands. Croatia follows the EU adoption dates for the ETSI standards. These bands were disabled because the access point will not meet the EN 301-893 v1.3.1 DFS standard, which goes into force on March 31, 2008.

COUNTRY	MIDDLE EAST & AFRICA
Kenya	- Modified the 5150 - 5250 & 5250 - 5350 MHz bands to follow the ETSI test requirements.
Saudi Arabia	- Modified the 2.4 GHz regulatory power settings to follow the ETSI requirements. This change was implemented across all access point models, including the 2330, 2330A & 2332-E3.

Global changes in Release 6.0

WSS/ WMS Global	The following countries are not supported by Avaya: • Belize (BZ) • Macedonia (MK) • Bosnia & Herzegovina (BA)
Outdoor 2330A	Created new outdoor antennas for the 2330A: 2.4 GHz band (24113-OUT, 24123-OUT, 24143-OUT, 24883-OUT, 24993-OUT) 5 GHz bands (5643-OUT, 5133-OUT).
Outdoor 2330A	Created new antennas for the 2.4 GHz & 5.0 GHz bands for the NEMA enclosure (-NEMA, -NEMA-10 & -NEMA-25).
2330A	Enabled operation for Greece, Italy, Latvia, Spain & France for the 24113 & 24123 antennas.
2330A	Disabled operation in the US for the 5250 - 5350 MHz band for the 5643 -OUT, -OUT-10, & -OUT-25 and 5133 -OUT, -OUT-10, & -OUT-25 antennas.
Series 2332	Added the (16) new regional locked APs: 2332-A1, 2332-A2, 2332-A3, 2332-A4, 2332-A5, 2332-A6, 2332-E1, 2332-E2, 2332-E3, 2332-E4, 2332-E5, 2332-E6, 2332-E7, 2332-E8, 2332-E9, and 2332-J1.
COUNTRY	**ASIA PACIFIC**
Hong Kong	Disabled DFS in the 5.25 - 5.35 GHz band. It is NOT required. Restricted operation in the 5.15 - 5.35 GHz band to indoors only per HK rules.
India	Enabled operation on the 5725 - 5850 MHz band per recent approval. Outdoor operation is limited to the 2.4 GHz band. All 5 GHz bands are indoor only operation.
Malaysia	Enabled operation on CH 165 for 2330/2330A.
Thailand	Limited operation in the 2.4 GHz band to indoors only per the rules.
Taiwan	Updated 24113 & 24123 operation for 802.11b & 802.11g to operate up through CH 11. It only used to work up to CH 7. Updated 5.25 GHz band to be indoors only per SRD rules.

Vietnam	Updated outdoor operation as follows: • Enabled operation for "indoors only" for the 5.15 to 5.25 GHz band. • Enabled operation in the 5.25 to 5.35 GHz and 5.725 to 5.85 GHz (5 CH) bands.
COUNTRY	**CALA**
Guam	Added Guam to 2332-A1. Follows FCC rules.
US Virgin Islands	Added US Virgin Islands to 2332-A1. Follows FCC rules.
COUNTRY	**EU & EUROPE**
EU & EFTA	Disabled 5250 - 5350 & 5470 - 5725 GHz bands on 2332-E1 to be compliant to EN 301-893 v1.3.1 by March 31, 2008.
Greece	Modified 802.11b/g settings for Outdoor Operation.
Spain	Modified 802.11b/g settings for Outdoor Operation.
Ukraine	Updated outdoor operation for 2.4 GHz and 5.0 GHz bands.
COUNTRY	**MIDDLE EAST & AFRICA**
Bahrain	Updated Outdoor parameters per country requirements. Enabled DFS for Bahrain in the 5.25 - 5.35 GHz band.
Egypt	Restricted operation in the 802.11b/g 2.4 GHz band to indoor only. Outdoor operation requires NTRA approval. Restricted use in 5725 -5850 MHz to "indoor only". Outdoor operation requires NTRA approval/license.
Jordan	Modified operation in the 2.4 GHz and 5.15 - 5.25 GHz bands for indoor operation only.
Kuwait	Enabled operation for 2.4 GHz based on EU. Operation is limited to indoor use only. Enabled 5 GHz operation in the 5150 - 5250 & 5250 -5350 MHz band for indoors only.
Lebanon	Enabled outdoor operation for 802.11b/g in the 2.4 GHz band. Enabled operation in the 5.725 - 5.85 GHz band for both indoor and outdoor. Added technical operating parameters for the 5.0 GHz band on all antenna tabs.
Mauritius	Added all 2.4 GHz and 5.0 GHz operating parameters on all antenna tabs. Follows the EN 300-328 & 301-893 ETSI standards. DFS is required in the 5.25 - 5.35 GHz & 5.470 - 5.725 GHz bands. Updated Outdoor operation per local rules.
Morocco	Enabled outdoor operation for 802.11b/g in the 2.4 GHz band for Channels 8 - 13. Operation on Channels 1 - 7 is allowed indoors only. Enabled operation in the 5.15 - 5.25 GHz band for indoor only.
Nigeria	Updated operation in the 2.4 GHz band to follow the EU rules. Operation is allowed in the 5725 - 5850 MHz band, but requires DFS so it is currently disabled.

Oman	Changed 2.4 GHz operation to allow for outdoor use. Restricted use on 5150 - 5350 MHz to "indoor only". DFS is required in the 5250 - 5350 & 5470 -5725 MHz bands. Disabled operation in the 5725 - 5850 MHz band because it is restricted to outdoor only operation and requires DFS.
Qatar	Changed 2.4 GHz operation from 13 to 11 channels and allowed outdoor use. DFS required for this country in the 5752 - 5850 MHz band (4 CHs). 5.0 GHz operation is currently disabled.

Series 2332 Access Points Region Lock Mechanism

A regional regulatory lock function has been implemented in the Series 2332 access points to manage the various worldwide operating channels and country approval requirements. The regional lock function contains sixteen (16) regions that are grouped by their operating frequency channels for both the 2.4 GHz and 5.0 GHz 802.11a/b/g bands for indoor operation. The following is a current list of the proposed regions:

Region Name	Regions	Operating Bands
[Models]		
US Based	**US Based**	**US Based**
2332-A4	11 : 1, 2, 4, 7	2.4 : 5.1, 5.2, 5.4, 5.7
2332-A3	11 : 1, 2, 7	2.4 : 5.1, 5.2, 5.7
2332-A1	11 : 1, 7	2.4 : 5.1, 5.7
2332-A2	11 : 2, 7	2.4 : 5.2, 5.7
2332-A5	11 : 7	2.4 : 5.7
2332-A6	11 : NO 5	2.4 : NO 5.0 GHz
EU Based	**EU Based**	**EU Based**
2332-E4	13 : 1, 2, 4, 7	2.4 : 5.1, 5.2, 5.4, 5.7
2332-E1	13 : 1, 2, 4	2.4 : 5.1, 5.2, 5.4
2332-E3	13 : 1, 2, 7	2.4 : 5.1, 5.2, 5.7
2332-E2	13 : 1, 2	2.4 : 5.1, 5.2
2332-E5	13 : 1, 7	2.4 : 5.1, 5.7
2332-E6	13 : 2, 7	2.4 : 5.2, 5.7
2332-E7	13 : 1	2.4 : 5.1
2332-E8	13 : 7	2.4 : 5.7
2332-E9	13 : NO 5	2.4 : NO 5.0 GHz

Region Name	Regions	Operating Bands
[Models]		
Specials	**Specials**	**Specials**
2332-J1	14 : 1, 2	2.4 : 5.1, 5.2

IEEE 802.11a/b/g Channel Designations:

2400 - 2483.5 MHz band

IEEE Mode	**11b/g**	**11b/g**	**11b/g**	**11b/g**	**11b/g**	**11b/g**	**11b/g**	**11b/g**	**11b/g**	**11b/g**	**11b/g**
Channel Number	1	2	3	4	5	6	7	8	9	10	11
Frequency [GHz]	2.412	2.417	2.422	2.427	2.432	2.437	2.442	2.447	2.452	2.457	2.462
IEEE Mode	11b/g	11b/g	11b/g								
Channel Number	12	13	14								
Frequency [GHz]	2.467	2.472	2.484								

Legend:

- 11: Channels 1 through 11, inclusive (US Based)
- 13: Channels 1 through 13, inclusive (EU Based)
- 14: Channels 1 through 14, inclusive (Japan Based)

5.15 - 5.35 GHz bands

IEEE Mode	11a	11a	11a	11a	11a	11a	11a	11a
Channel Number	36	40	44	48	52	56	60	64
Frequency [GHz]	5.180	5.200	5.220	5.240	5.260	5.280	5.300	5.320

5.470 - 5.725 GHz bands

IEEE Mode	11a	11a	11a	11a	11a	11a	11a	11a	11a	11a	11a
Channel Number	100	104	108	112	116	120	124	128	132	136	140
Frequency [GHz]	5.500	5.520	5.540	5.56	5.580	5.600	5.620	5.640	5.660	5.680	5.700

5.725 - 5.85 GHz bands

IEEE Mode	11a	11a	11a	11a	11a
Channel Number	149	153	157	161	165
Frequency [GHz]	5.745	5.765	5.785	5.805	5.825

Legend:

- 1: Channels 36, 40, 44 & 48
- 2: Channels 52, 56, 60 & 64
- 4: Channels 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
- 7: Channels 149, 153, 157, 161, 165
- All combinations, such as 1, 2, 7 represent all of the channels listed in the separate sections of 1, 2 and 7: 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165

The two base Series 2332 Access Points are the 2332-A1 and the 2332-E1. Their operating channels are listed below for reference:

2332-A1:	2.4 GHz band (802.11b/g):	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
	5.0 GHz bands (802.11a):	36, 40, 44, 48, 149, 153, 157, 161, 165
2332-E1:	2.4 GHz band (802.11b/g):	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13
	5.0 GHz bands (802.11a):	36, 40, 44, 48

Series 2332 Access Points Country to Region Map

Region Names	Order Number's	CC	Countries
2332-A1	DR4001086E6	CA	CANADA
		PR	PUERTO RICO
		US	USA
		GU	GUAM
		VI	US VIRGIN ISLANDS
2332-E1	DR4001087E6	AT	AUSTRIA
		BE	BELGIUM
		BW	BOTSWANA
		BG	BULGARIA
		HR	CROATIA
		CY	CYPRUS
		CZ	CZECH REPUBLIC
		DK	DENMARK
		EE	ESTONIA
		FI	FINLAND
		FR	FRANCE
		DE	GERMANY
		GR	GREECE
		HU	HUNGARY
		IS	ICELAND
		IE	IRELAND
		IT	ITALY
		LV	LATVIA
		LI	LICHTENSTEIN
		LT	LITHUANIA
		LU	LUXEMBOURG
		MT	MALTA
		MU	MAURITIUS
		NA	NAMIBIA
		NL	NETHERLANDS
		NO	NORWAY
		OM	OMAN
		PL	POLAND
		PT	PORTUGAL
		RO	ROMANIA
		SK	SLOVAKIA (Slovak Republic)
		SI	SLOVENIA
		ZA	SOUTH AFRICA
		ES	SPAIN
		SE	SWEDEN
		CH	SWITZERLAND
		TZ	TANZANIA
		GB	UNITED KINGDOM
		ZM	ZAMBIA
		ZW	ZIMBABWE
2332-J1	DR4001101E6	JP	JAPAN

Region Names	Order Number's	CC	Countries
2332-A2	DR4001088E6	TW	TAIWAN
2332-A3	DR4001089E6	DM	DOMINICA
		DO	DOMINICAN REPUBLIC
		GD	GRENADA
		JM	JAMAICA
		KN	ST KITTS AND NEVIS
		LC	ST LUCIA
		VC	ST VINCENT AND THE GRENADINES
2332-A4	DR4001090E6	TT	TRINIDAD AND TOBAGO
2332-A5	DR4001091E6	EC	ECUADOR
		QA	QATAR
2332-A6	DR4001092E6	CR	COSTA RICA
2332-E2	DR4001093E6	IL	ISRAEL
		TR	TURKEY
		KW	KUWAIT
		UA	UKRAINE
2332-E3	DR4001094E6	AI	ANGUILLA
		AU	AUSTRALIA
		BH	BAHRAIN
		KY	CAYMEN ISLANDS
		CL	CHILE
		EG	EGYPT
		SV	EL SALVADOR
		IN	INDIA
		MX	MEXICO
		MS	MONTSERRAT
		NZ	NEW ZEALAND
		NG	NIGERIA
		PA	PANAMA
		SA	SAUDI ARABIA
		SG	SINGAPORE
		VE	VENEZUELA
		VN	VIETNAM
2332-E4	DR4001095E6	CO	COLUMBIA
		HK	HONG KONG
		KE	KENYA
		PY	PARAGUAY
		PE	PERU
		PH	PHILIPPINES
		AE	UNITED ARAB EMIRATES
		UY	URUGUAY
2332-E5	DR4001096E6	KR	KOREA, REPUBLIC OF
2332-E6	DR4001097E6	AR	ARGENTINA
		MY	MALAYSIA
2332-E7	DR4001098E6	JO	JORDAN
		MA	MOROCCO
2332-E8	DR4001099E6	BR	BRAZIL
		CN	CHINA
		HN	HONDURAS
		LB	LEBANON
		PK	PAKISTAN
2332-E9	DR4001100E6	DZ	ALGERIA
		ID	INDONESIA
		RU	RUSSIAN FEDERATION
		TH	THAILAND

Global Changes in Release 7.0

COUNTRY	GENERAL CHANGES
Global	- Modified 2332-E1 outdoor operation for Greece, Italy, Latvia & Spain to match current regulations.
Global	- Added Outdoor support for the following 2332 models: A3, A4 & E5. This includes adding external antenna tabs for -OUT, -OUT-10, -OUT-25, -NEMA, -NEMA-10, -NEMA-25 for the following external antennas on each supported model: 24493, 24882, 24113, 24123, 24143 for all models; 5643, 5133, 5173, 5103 for all models.
COUNTRY	**ASIA PACIFIC**
Macau	- Model 2332-E8. Enabled operation in the 2.4 & 5.8 GHz bands.
COUNTRY	**CALA**
Antigua & Barbuda	- Model 2332-A1. Follows FCC rules. Requires DFS in 5250 & 5470 MHz bands, so it is disabled.
Bahamas	- Model 2332-A1. Follows FCC rules. Requires DFS in 5250 & 5470 MHz bands, so it is disabled.
Bermuda	- Model 2332-A1. Follows FCC rules. Requires DFS in 5250 & 5470 MHz bands, so it is disabled.
Guatemala	- Model 2332-A5. Follows FCC rules.
COUNTRY	**EU & EUROPE**
Curacao	- Model 2332-E1. Follows EU rules. Enabled DFS.
EU & EFTA Countries	- Enabled the 5.25 - 5.35 GHz and 5.470 - 5.725 GHz bands for the 2332-E1 per the EN 301-893 v1.3.1 rules. - Disabled channels 120, 124, 128 & 132 per weather radar rules implemented on July 1, 2008 in the 5600 - 5650 MHz band.
Kazakhstan	- Enabled operation in the 2.4 GHz band. No 5.0 GHz or outdoor operation allowed. (2332-E9).
Macedonia (FYR)	- Model 2332-E1. Follows EU rules. Enabled DFS.
Montenegro	- Model 2332-E1. Follows EU rules. Enabled DFS.
Serbia	- Model 2332-E1. Follows EU rules. Enabled DFS.

DEVIATION: In the 7.0 software release the 2332-E1 and related Series 2332 access points were tested to and are compliant with all of the technical specifications of EN 301-893 v1.4.1 for operation in the 5.0 GHz bands, **except** the DFS requirements in the 5600 – 5650 MHz band.

IEEE 802.11a operation in the 5250 to 5350 MHz and 5470 to 5725 MHz frequency bands is governed by ETSI EN 301-893 v1.4.1 and the R&TTE Directive 1999/5/EC. Effective July 1, 2008, EN 301-893 v1.4.1 was updated to require compliance with 0.8 ?second pulse widths and staggered PRF's in the 5470 – 5725 MHz band. The 2332-E1 access point meets compliance with these new mandates by disabling operation, via software, on channels 120, 124, 128 and 132 in the 5600 to 5650 MHz frequency band because it cannot meet the 0.8 ?second pulse width and staggered PRF DFS requirements as outlined in the updated EN 301-893v1.4.1 standard.

Operation in the 5.0 GHz frequency bands has been changed to the following:

2332-E1:	2.4 GHz band (802.11b/g):	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13
	5.0 GHz bands (802.11a):	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 136, 140

For more information on the 'Regulatory Information", go tothe Avaya website: http://www.avaya.com/support.

See the following:

- Approved Countries for the WLAN Security Switches 2300 Series and 2330-2330A-2330B Access Points.
- Approved Countries for the WLAN Security Switches 2300 Series and Series 2332 Access Points.
- Approved 5.0 GHz Antennas for the WLAN 2330/2330A/2330B Access Points.
- Approved 2.4 GHz Antennas for the WLAN 2330/2330A/2330B Access Points.
- Approved 5.0 GHz Antennas for the WLAN Series 2332 Access Points.
- Approved 2.4 GHz Antennas for the WLAN Series 2332 Access Points.

Avaya WLAN - Security Switch 2300 Series Release Notes – Software Release 7.1

What's new in WSS Software version 7.1 20
Version compatibility 22
Upgrading to WSS version 7.1 22
Installing Upgrade Activation Keys on a WSS 25
System parameter support 27
Best practices and common issues 31
Interoperability 44
Known behaviors and issues 47
WSS 2380, 2382, and MX-2800 supported AP license activation key upgrade 55

Avaya recommends that you familiarize yourself with the "Best practices and common issues" section in this document before installing WLAN Security Switch Software (WSS Software) Version 5.0.9. For additional product information, refer to the following manuals in addition to these release notes:

- Avaya WLAN Security Switch 2300 Series Quick Start Guide.
- Avaya WLAN Security Switch 2300 Series Installation and Basic Configuration Guide.
- Avaya WLAN Access Point 2330/2330A Installation Guide.
- Avaya WLAN Security Switch 2300 Series Configuration Guide.
- Avaya WLAN Security Switch 2300 Series Command Line Reference.
- Avaya WLAN Management System 2300 Series User Guide.
- Avaya WLAN Management System 2300 Series Reference Guide.

What's new in WSS Software version 7.1

WSS 7.0 version contains the following enhancements:

- Trapeze Virtual Controller Cluster Enhancements
  - AP Affinity
  - Hitless software upgrade
  - Licensing Changes
- SIP Awareness
- LDAP Authentication Support
- Licensing Changes
- Minor Enhancements
  - Security features
    - IPSec Client for secure RADIUS connections
    - Logging of RingMaster changes using Command Audit
    - Countermeasure support for Ad-hoc devices
    - Wired-auth session aging
    - Configurable RingMaster management port
    - Support for extended intermediate Certificate Authorities in Certificate path
    - SCP support for secure file copy operations
  - Supportability Features
    - Scheduled command execution
    - Embedded TFTP server support
    - Improvements to **show ap** output
  - AAA Features
    - Support for Web-portal clients in local switching mode
    - Per-User authentication of RingMaster changes
    - 'service-type' based access to privileged CLI mode
    - Configuration control for Acct-interim-update per SSID
  - Mesh and Bridging Enhancements
    - Mesh and Bridge services now support the use of "hidden" SSIDs for backhaul networks.
  - System Features
    - Configurable support for AP "lights out" mode
    - 512 AP support for MX-2800

Trapeze Virtual Controller Cluster Enhancements

WSS 7.1 continues to enhance the revolutionary Virtual Controller Cluster feature set. This release adds the following new functionality:

- AP Affinity

  AP Affinity allows a network operator to configure a preference for which controller APs connect to in non-failure scenarios. Groups are configured on each cluster member and are shared within the Cluster.

- Hitless software upgrade

  Network Resiliency enhancements in WSS 7.1 now allow you to optionally perform an in-service software upgrade. A coordinated upgrade of all controllers and APs in the cluster results in minimal service interruption for client devices.

- Licensing Changes

  The Virtual Controller Cluster feature is now part of the High Availability Add-on Module. When using the HA license with the Virtual Controller Cluster features, redundant AP licenses are automatically created on Cluster members (1:1 for licensed APs, up to the controller platform max).

SIP Awareness

Integrated stateful application awareness for the SIP protocol adds a new level of intelligence that allows granular and dynamic control of voice applications. Awareness of SIP call state allows for advanced QoS treatment, call-based Call Admission Control and Call Detail Record generation. The SIP Awareness feature set is enabled via the Advanced Voice Module software add-on.

LDAP Authentication Support

WSS 7.1 introduces native LDAP as an available method for user authentication. This allows for an operator to deploy wireless services without requiring a RADIUS backend. LDAP authentication is supported for Web-Portal, MAC, and Administrative authentications.

Licensing Changes

Starting in WSS 7.1 the current licensing model (AP licensing, FIPS licensing, etc) has been extended to support three new Feature License options. The following licenses are now available:

- High Availability Module - covers the Virtual Controller Cluster feature set.
- Advanced Voice Module - covers the SIP Awareness feature set including Dynamic CAC and Call Detail Records.
- Mesh and Bridging Module - covers APs in Mesh and Bridge applications

Version compatibility

WLAN Management System

This version of WLAN Security Switch Software (WSS Software) is intended for use with WLAN Management System Version 7.1 or higher.

Minimum WSS Software requirements for upgrade

Table 1 lists the minimum WSS Software version a WSS must be running when you upgrade the switch to WSS Software Version 5.0.9. If your switch is running an older WSS Software version, you can use the upgrade path to upgrade the switch to 5.0.9.

Table 1. Software Requirements for Upgrade to WSS Software Version 5.0.9

Product	Minimum WSS Software Version Required	Upgrade Path
2350	*5.x*	5.0.15.2 -> 6.0.7.2 ->*7.0.x.x*->*7.1.x.x*
2360/2361	*5.x*	5.0.15.2 -> 6.0.7.2 ->*7.0.x.x*->*7.1.x.x*
2380	*5.x*	5.0.15.2> 6.0.7.2 ->*7.0.x.x*->*7.1.x.x*
2382	*5.x*	5.0.15.2 -> 6.0.7.2 ->*7.0.x.x*->*7.1.x.x*
Trapeze MX-2800	7.0.3.6	*7.0.x.x*->*7.1.x.x*

Note. You must upgrade to WSS Release 7.0 or later before upgrading to WSS Release 7.1.

Upgrading to WSS version 7.1

Before upgrading, refer to "Version compatibility" on page 22. After verifying the WSS is running the minimum version required to upgrade to WSS Version 7.1, return to this section.

Warning! To avoid conflicts with the internal VLAN numbering scheme, it is strongly advised to use VLAN IDs less than 3520 on WSSs that are upgrading to WSS Version 7.1. Failure to do so may result in lost configuration data.

Note. WSS 7.1 includes changes to the storage location of system debug files. Debug information is now stored in persistent user-accessible storage for retrieval after a system restart.

Preparing the WSS for the Upgrade

Warning! Avaya recommends that you make a backup of the WSS configuration before installing the upgrade. If an error occurs during the upgrade, restore the WSS to a previous configuration.

Note. WSS 7.1 includes support for individual cipher configuration on both the WPA and RSN IEs. When downgrading from WSS 7.1 to an earlier version of WSS, changes to IE configuration will be lost.

You can use the following command to back up the configuration files:

backup system [tftp:*/ip-addr/*]filename [*all* | *critical*]

To restore a WSS that is backed up, use the following command:

restore system [tftp:*/ip-addr/*]filename [*all* | *critical*]

"Upgrade scenario" on page 24 shows an example of the **backup** command.

Upgrading an individual WSS using the CLI

Note. If configuration changes have been made but not saved, use the **save config** command to save the changes before you backup the WSS.

1. Back up the WSS, using the **backup system** command.
2. Copy the new system image onto a TFTP server.

   For example, log into http://www.avaya.com/support/ using a Web browser or your TFTP server and download the image onto the server.

3 Copy the new system image file from the TFTP server into a boot partition in the nonvolatile storage of the WSS. For example,

WSS# copy tftp://10.1.1.107/WSS071001.200 boot1:WSS071001.200

You can copy the image file only into the boot partition that was not used for the most recent restart. For example, if the currently running image was booted from partition 0, you can copy the new image only into partition 1.

4 Set the boot partition to the one with the upgrade image for the next restart.

To verify that the new image file is installed, type **show boot**.

5 Reboot the software.

To restart a WSS and reboot the software, type the following command: **reset system.**

When you restart the WSS, it boots using the new image. The WSS also sends the AP version of the new boot image to APs and restarts them. After an AP restarts, the version of the new AP boot image is checked to make sure the version is newer than the version currently installed on the AP. If the version is newer, the AP completes installation of the new boot image by copying the boot image into the flash memory, which takes about 30 seconds, then restarts again. The upgrade of the AP is complete after the second restart.

Upgrade scenario

Note. This example copies the image file into boot partition 1. On your WSS, copy the image file into the boot partition that was not used the last time the WSS was restarted. For example, if the WSS booted from boot partition 1, copy the new image into boot partition 0. To see boot partition information, type the **show boot** command.

To upgrade a WSS, use the following upgrade example.

WSS# save config success: configuration saved.

WSS# backup system tftp:/10.1.1.107/sysa_bak success: sent 28263 bytes in 0.324 seconds [87231 bytes/sec]

WSS# copy tftp://10.1.1.107/MX071001.200 boot1:WSS071001.200

.....

.....

.....success: received 10266629 bytes in 92.427 seconds [111078 bytes/sec]

WSS# set boot partition boot1

success: Boot partition set to boot1:WSS071001.200 (7.1.0.1).

WSS# show boot

Configured boot version:	**7.1.0.1**
Configured boot image:	**boot1:mx070001.200**
Configured boot configuration:	**file:configuration**

Backup boot configuration: **file:backup.cfg**

Booted version: **7.1.0.1**

Booted image: boot1: **WSS0701202.200**

Booted configuration: **file:configuration**

Product model: **WSS**

WSS# reset system

..... rebooting .....

Installing Upgrade Activation Keys on a WSS

WSS 7.1 includes support for AP upgrade licenses and 3 new feature license options:

- Advanced Voice Module
- High Availability Module
- Mesh/Bridging Module

These feature license keys are installed alongside AP upgrade licenses. Additional details of the features/functionality included with each license are available in the product data sheets. When installing AP based features licenses (e.g. Mesh/Bridging Module) the licenses should be installed on the WSS where the AP is configured. For Cluster environments, licenses should be installed on the Cluster seed.

AP licensing is supported on WSS platforms as shown in the following table.

Table 2. Licensing and Upgrade Increments for WSS Models

WSS Model	Base MP Support	Maximum MP Support	Upgrade Increment
WSS 2380	40	120	40
WSS 2382	32	192	32
MX-2800	64	512	64

Note. If you downgrade to a previous version of WSS that does not support the higher capacity licenses, the number of allowed APs is reduced to comply with the older software limitations and feature licenses are removed.

Feature licensing is supported on WSS platforms as show in the following table.

Table 3. WSS Feature Licensing Matrix

WSS Model	Advance Voice Module	High Availability Module	Mesh/Bridging Module
WSS 2350	Supported	Supported	Up to 4 MPs (16 MPs in Cluster mode)
WSS 2360/1	Supported	Supported	Up to 12 MPs (48 in Cluster mode)
WSS 2380	Not Supported	Not Supported	Up to 120 MPs (480 MPs in Cluster mode)
WSS 2382	Supported	Supported	Up to 192 MPs (768 in Cluster mode)
MX-2800	Supported	Supported	Up to 512 MPs (4096 in Cluster mode)

To upgrade an MX license:

1. Obtain a license coupon for the upgrade from Avaya or your reseller.
2. Establish a management session with the WSS to display the serial number. To display the serial number, type the following command:

   show license

   In the following example, the WSS serial number is 123456789:

   WSS> show license

   Serial Number 123456789

   Platform AP Count : 32 access points are supported

   Licensed AP Count : 96 additional access points

   128 access points are supported

   Additional Features:

   Feature Description Installed

   ----
3. Use a Web browser to access the Avaya license server at the following URL:

   http://www.trapezenetworks.com/support/product_licenses
4. Type your e-mail address in the E-mail and Confirm E-mail fields.
5. Select your WSS model and feature license (if applicable) from the Product Selection list.
6. Type or copy and paste the WSS serial number into the Product Serial Number field, and click OK.

   The Product Licensing page appears.

7. Type the coupon activation code(s) into the Coupon Code(s) fields and click OK. The Licensing Confirmation page appears, and displays the activation key (also called the license key).
8. Highlight and copy the entire activation key.
9. On the WSS, use the following command at the enable (configuration) level of the CLI to install the activation key:

   set license activation-key

   In the following example, an activation key for an additional 96 APs is installed on a WSS:

   WSS# set license 3B02-D821-6C19-CE8B-F20E

   success: license accepted
10. Verify installation of the new license by typing the following command:

    WSS# show licenses

    Serial Number 123456789

    Platform AP Count : 32 access points are supported

    Licensed AP Count : 96 aadditional access points

    128 access points are supported

    Additional Features:

    Feature Description Installed

Support for the additional APs begins immediately. You do not need to restart the MX to place the upgrade into effect.

System parameter support

The following tables list the recommended or maximum supported values for major system parameters.

Table 4. Mobility system parameters

Parameter	Supported Value
WSS switches in a single Network Domain	500
WSS switches in a single Mobility Domain	64
Roaming VLANs per WSS	• MX-2800: 256 total (256 configured) • WSS 2380: 256 total (128 configured) • WSS 2382: 256 total (128 configured) • WSS 2360/1: 256 total (128 configured) • WSS 2350: 256 total (128 configured)
VLANs per Mobility Domain	2048

Table 4. Mobility system parameters

Parameter	Supported Value
APs per WSS	• MX-2800: 4096 configured, 512 active • WSS 2380: 480 configured, 120 active • WSS 2382: 768 configured, 192 active • WSS 2360/1: 48 configured, 12 active • WSS 2350: 16 configured, 4 active Includes directly attached MPs and Distributed MPs. Inactive configurations are backups.
Minimum link speed between WSSs in a Mobility Domain	128 Kbps
Minimum link speed between an WSS and AP in a Mobility Domain	128 Kbps and 95ms round trip latency

Table 5. Network parameters

Parameter	Supported Value
Forwarding database entries	• MX-2800: 32768 • WSS 2380: 16383 • WSS 2382: 8192 • WSS 2360/1: 8192 • WSS 2350: 8192
Statically configured VLANs	• MX-2800: 256 configured • WSS 2380: 128 configured • WSS 2382: 128 configured • WSS 2360/1: 128 configured • WSS 2350: 128 configured
Spanning trees (STP/PVST+ instances)	64
ACLs	ACEs per WSS • 170 ACEs per ACL: • MX-2800: 256 • WSS 2380: 256 • WSS 2382: 256 • WSS 2360/1: 25 • WSS 2350: 25
Location Policies	Location Policies per MX: All models: 1 The Location Policy can have up to 150 rules.

Table 5. Network parameters

Parameter	Supported Value
IGMP streams	500 Replication of a stream on multiple VLANs counts as a separate stream on each VLAN.
Mesh Services and Bridging	• Mesh Depth - Mesh Links (Portal<->Mesh MP<->Mesh MP) • Mesh Fan Out - 6 APs • Maximum Supported Mesh Nodes per Mesh Portal - 6 • Bridge Links - 1:1

Table 6. Management parameters

Parameter	Supported Value
Maximum instances of RingMaster simultaneously managing a network	3
Telnet management sessions	• MX-2800: 8 • WSS 2380: 8 • WSS 2382: 8 • WSS 2360/1: 4 • WSS 2350: 4 The maximum combined number of management sessions for Telnet and SSH together is 8 for the WSS 2380, WSS 2382, or 4 for the WSS 2360/1 and WSS 2350, in any combination.
SSHv2 management sessions	• MX-2800: 8 • WSS 2380: 8 • WSS 2382: 8 • WSS 2360/1: 4 • WSS 2350: 4
Telnet client sessions (client for remote login)	• MX-2800: 8 • WSS 2380: 8 • WSS 2382: 8 • WSS 2360/1: 4 • WSS 2350: 4
NTP servers	3
SNMP trap receivers	8

Table 6. Management parameters

Parameter	Supported Value
Syslog servers	4
RADIUS and LDAP servers	• 40 configured on the WSS • 4 in a server group • 4 server groups in a AAA rule • A maximum of 40 servers in any combination of RADIUS and LDAP - for example, 30 RADIUS servers and 10 LDAP servers.

Table 7. Client and session parameters

Parameter	Supported Value
Authenticated and associated clients per radio	100 Clients who are authenticated but not yet associated are included in the total.
Active clients per radio	50 Total number of active clients simultaneously sending or receiving data
Active AAA sessions (clients trying to establish active connections) per WSS	• MX-2800: 12800 • WSS 2380: 2500 • WSS 2382: 4800 • WSS 2360/1: 300 • WSS 2350: 75
AAA users configured in local database	• MX-2800: 999 • WSS 2380: 999 • WSS 2382: 999 • WSS 2360/1: 250 • WSS 2350: 250

Best practices and common issues

Follow these best-practice recommendations during configuration and implementation to avoid or solve issues you might experience.

Best practices when powering down a switch

If a 2350 or 2360/2361 is connected to Power Sourcing Equipment (PSE), it is possible for the switch to remain powered on even when the power cord is unplugged. PSE can be a dedicated PoE injector or even another networking switch such as the WSS that is capable of supplying PoE. To ensure that the switch is powered off, unplug the power cord, then unplug all Ethernet cables that are connected to other PoE devices.

System configuration best practices

Avaya strongly recommends that you use WMS for archiving and version control of network-wide WSS configurations. Avaya also recommends that you archive the CLI-based configuration files of individual WSSs by copying the configurations to a server.

Client and Web-based AAA best practices

Follow these best-practice recommendations during configuration and implementation to avoid or solve issues you might experience.

Get clients and Web-based AAA working first

The greatest majority of installation issues are related to clients and web-based AAA server (authentication, authorization, and accounting) operation, due to their diverse nature. Avaya recommends first establishing a baseline of proper operation with a sampling of wireless clients and the web-based AAA server you plan to use. Working out client and web-based AAA configuration methods first provides valuable information as you scale the deployment.

The selection of client and web-based AAA server software will depend heavily on the requirements of your deployment. First, decide which EAP Protocol you will be using as that will restrict the available clients and servers. Each protocol has different advantages and disadvantages, which you will need to consider in your deployment. For most enterprise deployments, Avaya recommends using PEAP-MS-CHAP-V2 as the 802.1X protocol. Table 8 compares the EAP protocols.

Table 8. EAP Protocol Comparison

Protocol	Advantages	Disadvantages
PEAP-MS-CHAP-V2	• Does not require client certificates • Compatible with Avaya 802.1X Acceleration • Native support in Microsoft Windows XP and 2000 • Broad support in 802.1X clients	Username/password-based access might not be as strong as certificate-based access

Table 8. EAP Protocol Comparison (continued)

Protocol	Advantages	Disadvantages
EAP-TTLS	• Does not require client certificates • Broadest compatibility with user directories	• Requires third-party 802.1X client software • Username/password-based access might not be as strong as certificate-based access
EAP-TLS	• Strongest authentication using X.509 certificates. • Native support in Windows XP and 2000 • Broad support in all 802.1X clients	Client-side certificates require full PKI infrastructure and management overhead
PEAP-TLS	• Strongest authentication using X.509 certificates. • Native support in Windows XP and 2000 • Broad support in all 802.1X clients	• Client-side certificates require full PKI infrastructure and management overhead • Minimal advantage over EAP-TLS

Although LEAP uses the same ethertype as 802.1X (0x888e), the LEAP protocol is proprietary and does not conform to the IEEE 802.1X standard. Additionally, the LEAP protocol has serious security flaws. For example, LEAP-authenticated networks can be breached using a simple dictionary attack.

When testing and evaluating the Avaya WLAN 2300 Series System, enterprises using primarily Microsoft platforms are recommended to use Windows XP clients running PEAP-MS-CHAP-V2 with a Windows 2000 or 2003 server running Internet Authentication Service (IAS) as the RADIUS back end. This provides a test environment that is quick to set up and does not require additional third-party software.

Driver dependant behavior

- Some clients prefer a beaconed clear SSID to their configured SSIDs. If you configure WSS Software to beacon a clear SSID, some clients' adapters prefer this beaconed SSID over the SSIDs they are configured to use. Conversely, some adapters can associate only with a beaconed SSID. Determine whether to beacon the clear SSID based on the types of clients in the network.
- Standby mode can prevent some clients from reassociating. If a laptop PC whose wireless adapter is associated with an AP access point goes into standby (hibernate) mode, the operating system can either freeze or experience a Blue Screen of Death (BSOD) when the laptop comes out of standby mode and attempts to reassociate with the access point. To work around this behavior, disable standby mode. Alternatively, disable and reenable the wireless adapter after the client emerges from standby mode.
- If a client passes authentication but fails authorization, the client might indicate that authentication has succeeded but the AP access point nonetheless disassociates from the client. In this case, the client might indicate that the network is unavailable. For example, this situation can occur if the certificate exchange is valid but the requested VLAN or ACL filter is not available, or a Mobility Profile™ denies service to the client. Once the AP disassociates from the client, the network continues to be unavailable to the client through the AP for the duration of the 802.1X quiet-period timer, which defaults to 60 seconds. An error message indicating that a client has failed authorization appears in the WSS's system log.

802.1X clients

Properly preparing your clients for wireless connectivity is one of the most important things you can do to ensure an easy rollout. Here are some guidelines for preparing common 802.1X clients and platforms.

Windows XP

Windows XP is a popular platform for wireless clients because of its native support of 802.1X authentication and simplified configuration of wireless networks. If you choose to use the 802.1X client built-in to Windows XP, please note the following:

- Microsoft has extensive documentation on how to configure and use wireless 802.1X authentication in an Active Directory environment, published on their website. You can start with Microsoft's Wi-Fi center at:

  www.microsoft.com/windowsserver2003/technologies/networking/wifi/default.mspx

- Installing Windows XP Service Pack 2 is recommended for all wireless clients as it includes several important hotfixes.
- If you are not prepared to install Service Pack 2, Avaya strongly recommends that all wireless clients use Service Pack 1a with the following hotfixes installed:
  - KB826942—This is the WPA Hotfix Rollup and is available through Microsoft Update
  - KB834669—This corrects an 802.1X client issue which can cause system instability problems in Windows XP. You will need to contact Microsoft directly for this hotfix.
- If your network uses logon scripts, Active Directory group policies, or your users regularly share their laptops, you should enable computer authentication (also known as machine authentication) to achieve full functionality over your wireless connection.
- Download current drivers for your NICs from the NIC vendor(s).
- If your wireless NIC's driver includes the AEGIS protocol manager for WPA support, Avaya recommends against installing it. Some drivers install this automatically if you run the setup.exe utility to install the driver. Avaya strongly recommends that you update the driver manually using the driver properties in the Network control panel instead of installing the client manager.
- If you use computer authentication with different VLANs for the Computer and User accounts and do not have the WPA hotfix rollup (KB826942) or Service Pack 2, you need to install Microsoft hotfix KB822596. Otherwise, DHCP will not operate correctly after the user authenticates. You must contact Microsoft technical support for this hotfix. It is not available from their website. For more information on computer authentication, see "Computer authentication" on page 35.
- If MD5 challenge is configured on a Windows XP client for wired authentication, Avaya recommends that you set the quiet period to 5 to allow successful authentication. In addition, if the authentication is carried out manually, the timeout value must be set to no less than 30 seconds in order to allow the user ample time to enter their username and password. For example, to configure 802.1X on a WSS to allow these users time to log in, type the following commands:

  2380# **set dot1x quiet-period 5**
  2380# **set dot1x tx-period 30**

  The same recommendations for the quiet period and transmit period also apply to PEAP with manual entry of credentials.

Windows 2000

Many enterprises have a large installed base of Windows 2000 laptops, making this a common choice of platform. Windows 2000 Service Pack 4 includes a native 802.1X client. If you choose to use the 802.1X client built-in to Windows 2000, please note the following:

- Microsoft has extensive documentation on how to configure and use wireless 802.1X authentication in an Active Directory environment, published on their website. Most of this documentation is geared towards Windows XP, but both operating systems have many similarities in the client. You can start with Microsoft's Wi-Fi center at:

  www.microsoft.com/windowsserver2003/technologies/networking/wifi/default.mspx

- Installing Windows 2000 Service Pack 4 is required for all wireless clients.
- Some clients might experience system instability when using PEAP-MS-CHAP-V2 in an Active Directory environment. The primary symptom of this is a message displayed after login informing the user that the service svchost.exe has stopped unexpectedly. If you experience this problem, please contact Microsoft technical support and request hotfix KB833865.
- If your network uses logon scripts, Active Directory group policies, or your users regularly share their laptops, Avaya recommends that you enable computer authentication to achieve full functionality over your wireless connection.
- Download current drivers for your NICs from the NIC vendor(s).
- Windows 2000 does not include a full implementation of the Wireless Zero-Config service from Windows XP, so you will need to use the client manager software provided with your NIC to configure your SSID and enable WEP encryption. When using dynamic WEP in Windows 2000, select *static WEP 128bit* and enter any static WEP key as a placeholder. This temporary key configures the driver to use WEP to encrypt packets, and the Microsoft 802.1X client then overrides the static WEP key you entered with a dynamic key after you authenticate successfully.
- If your wireless NIC's driver includes the AEGIS protocol manager for WPA support, Avaya recommends against installing it. Some drivers install this automatically if you run the setup.exe utility to install the driver. If you are unable to install the client manager without the AEGIS component, contact the driver manufacturer or download an earlier version that does not contain the AEGIS component.
- 16-bit PCMCIA and built-in NICs (some 802.11b cards in Dell, Toshiba, and other manufacturers' laptop PCs) might require a registry setting to be changed before they will be able to associate with any SSID. Microsoft Knowledge Base article 327947 documents the changes necessary to resolve the problem. Multi-band cards (A/B or A/B/G) are generally 32-bit and do not experience this problem.
- If you use computer authentication with different VLANs for the Computer and User accounts, you need to install Microsoft hotfix KB822596. Otherwise, DHCP will not operate correctly after the user authenticates. You must contact Microsoft technical support for this hotfix. It is not available from their website. For more information on computer authentication, see "Computer authentication" on page 35.
- If you experience a delay in receiving your DHCP IP address wirelessly while using 802.1X authentication, you might need to install Microsoft hotfix KB829116. You must contact Microsoft technical support for this hotfix. It is not available from their website.

Funk Odyssey

The Funk Odyssey client is required when you require WPA support on Windows 2000, or when you need to authenticate to an LDAP backend database that does not support MS-CHAP-V2 over LDAP. If you choose to use this client, please note the following:

- Download the latest version from Juniper's website at: www.juniper.net
- Be sure to turn off Wireless Zero Config in Windows 2000 by disabling the service.
- If your wireless NIC's driver includes the AEGIS protocol manager for WPA support, Avaya recommends against installing it. Some drivers install this automatically if you run the setup.exe utility to install the driver. Avaya recommends that you update the driver manually using the driver properties in the Network control panel instead of installing the client manager.

Macintosh OS/X

OS/X Version 10.3, also known as Panther, includes an 802.1X client that supports Dynamic WEP and WPA/TKIP. If you choose to use this client, please note the following:

- The Panther client will only connect successfully to an SSID which is only dynamic WEP, or only WPA/TKIP. Any other configuration involving WEP with WPA enabled or AES is not supported by the current Panther client. If you need to run both WPA/TKIP and Dynamic WEP at the same time you must configured separate service profiles for each encryption type in order to maintain compatibility with Macintosh clients.
- The Panther client requires you to specify the inner and outer PEAP-MS-CHAP-V2 usernames in separate areas. Depending on your web-based AAA backend, both usernames might require a domain prefix in the form of *DOMAIN\username*.

Computer authentication

Windows clients support 802.1X authentication of the computer itself. This is called *computer authentication* (also known as *machine authentication*). Computer authentication is useful when you want your computer to be active on the domain even when no users are logged in to the computer. Some features of Windows XP Professional and Windows 2000 Professional work correctly only with an active network connection to the domain controller enabled before a user is logged on to the PC. Using computer authentication ensures that this network connection is established during the boot sequence, providing a wire-like infrastructure that allows you to use the following features on a wireless network. Table 9 lists Microsoft networking features that require computer authentication.

Table 9. Microsoft networking features that require computer authentication

Feature	Scenario Requiring Computer Authentication
Active Directory computer Group Policy	Computer–based Group Policy is applied during computer start up and at timed intervals—even when no on is logged in to windows.
Network logon scripts	Network logon scripts are run during initial user login.
Systems management agents	Systems management application agents such as those that come with Microsoft Systems Management Server (SMS) frequently need network access without user intervention.
Remote Desktop Connection	Computers are accessible from Windows Remote Desktop Connection when no one is logged in to windows.
Shared folders	Files and folders shared from a computer are still available, even when no user is logged in.

Configuring computer authentication on the client is simple, though it requires the use of the Microsoft 802.1X client built-in to Windows XP and Windows 2000. Keep the following information in mind when configuring computer authentication on Microsoft clients:

- To enable computer authentication, go to the **Authentication** tab where you normally select your 802.1X authentication method and enable the checkbox labeled **Authenticate as computer when computer information is available**.
- The authentication protocol that is configured for your user accounts will also be used for the computer account.
- If the EAP protocol you are using requires client certificates, you must use the Microsoft Enterprise Certificate Authority built-in to Windows 2000 Server and Windows Server 2003 to generate *Computer* certificates for PCs on your active directory domain. Microsoft Knowledgebase Article KB313407 explains how to enable the automatic distribution of computer certificates through Active Directory.
- If the user and machine accounts use different VLANs, you must install hotfixes on the client PCs to enable them to DHCP for a new IP address when the user authentications. Windows XP requires either the WPA Rollup Hotfix (KB826942) or Hotfix KB822596. Windows 2000 requires hotfix KB822596.
- Using PEAP-MS-CHAP-V2 with computer authentication will allow users who have never logged on to a PC authenticate wirelessly without having to login to the PC over a wired connection the first time. EAP-TLS still requires the user to connect to the network over a wired connection to generate a profile on the PC and a user certificate.

Enabling computer authentication also requires minor reconfiguration of Active Directory and IAS. Please note the following when configuring computer authentication on an active directory domain:

- You must grant dial-in access for the computer accounts in Active Directory that you wish to enable computer authentication on. If the tab to configure dial-in access does not appear, follow the directions in Microsoft Knowledgebase article KB306260.
- Review your remote access policies in IAS to insure that the computer accounts have appropriate group membership to allow them to match the proper policy.

Computer authentication also requires specific configuration considerations on the WSS:

- The username of a computer authentication connection will be in the form of host/*fully-qualified-domain-name*, for example host/bob-laptop.nrtl.com or host/tac1-laptop.support.nrtl.com. This username is the same regardless of the configured protocol (PEAP-MS-CHAP-V2 or EAP-TLS). An appropriate userglob would be *host/*.domain.com* where domain.com is the Active Directory domain name. Alternatively, in a smaller deployment you could use a userglob of ** and have both user and computer authentication go to the same RADIUS server.
- PEAP-MS-CHAP-V2 offload mode is not supported with computer authentication. You must use pass-through 802.1X authentication policies with computer authentication.

Web-based AAA

Table 10 lists the Web-based AAA servers and configurations that have been tested with WSS Software. Tests were performed to a local user database in most cases, and additionally to Microsoft Active Directory and LDAP with specific protocols as noted in the table. The tests were initially performed using Dynamic WEP, though subsequent testing has revealed no noticeable differences in RADIUS compatibility when using WPA.

A result of *Pass* indicates that the combination is supported by the Avaya WSS Software. A result of *Not Applicable* indicates that the RADIUS server tested does not support the feature. A result of *Fail* indicates that the RADIUS server does not interoperate with WSS Software for that feature. A result of *Not Tested* indicates that the feature was not tested.

Table 10. Web-based AAA servers tested with Avaya WSS Software

Configuration	RADIUS Servers Tested				
	Windows 2000 IAS	Windows 2003 IAS	Funk Steel Belted Radius	Cisco ACS	FreeRadius (Linux)
PEAP-MS-CHAP-V2	Pass	Pass	Pass	Pass	Pass
PEAP-MS-CHAP-V2 Offload	Pass	Pass	Pass	Pass	Pass
EAP-TLS	Pass	Pass	Pass	Not Tested	Pass
EAP-TTLS	Not Applicable	Not Applicable	Pass	Not Applicable	Not Tested
Single-Sign-On Active Directory & PEAP-MS-CHAP-V2	Pass	Pass	Pass	Pass	Not Applicable
Single-Sign-On LDAP & EAP-TTLS	Not Applicable	Not Applicable	Pass	Not Tested	Not Tested
Avaya VSAs	Pass	Pass	Pass	Pass	Pass
MAC-based authentication	Pass	Pass	Pass	Pass	Pass
Microsoft Active Directory computer authentication	Pass	Pass	Not Applicable	Pass	Not Applicable

Testing notes

- Single-Sign-On is defined as clients being able to use the same username and password for 802.1X authentication that they use to authenticate with network services and logon to their local PC.
- A *Pass* result for Avaya VSAs indicates that the VSAs were able to be added to the RADIUS server manually. Future versions of Steel Belted RADIUS and FreeRadius are planned to include standard definitions of the Avaya VSAs.
- Funk Steel Belted Radius version used for testing is 4.53
- Windows 2000 with Service Pack 4
- Cisco ACS 3.2 or later is required to support PEAP-MS-CHAP-V2

WPA

If you choose to use WPA to secure your wireless network, please note the following:

- CCMP (AES 802.11i draft support) is supported only when it is the only encryption type enabled on that SSID. Enabling TKIP or Dynamic WEP on the same SSID with CCMP can cause serious connectivity issues as most clients do not properly support this configuration. Avaya recommends that you create a separate service profile and SSID for WPA/CCMP.
- Enabling TKIP and Dynamic WEP on the same SSID is not recommended. This configuration forces the group key (multicast/broadcast key) to use the lowest common encryption type, in this case Dynamic WEP. Additionally, compatibility with wireless NICs is reduced.

- Downloading the latest drivers for your wireless NIC is strongly recommended. See "802.1X clients" on page 32 for specific information on installing drivers for your operating system.
- When a session key is changed, Microsoft WPA clients can sometimes incorrectly start using the new key before the end of the four-way handshake that is used to establish the key information. This issue can occur when the session timeout for the client session expires. As a result, the AP access point rejects the client's re-association attempt because the key information presented by the client is invalid. If you experience this issue, clear the Session-Timeout attribute on the affected users. The WSS will not force a reauthentication of WPA/TKIP and WPA/CCMP users periodically like it does with dynamic WEP users.
- Do not use the **set service-profile shared-key-auth** command in a WPA configuration. This command does not enable PSK authentication for WPA. To enable PSK for WPA, use the **set service-profile auth-psk** command.
- Use one WPA authentication method per SSID, either 802.1X authentication or preshared key (PSK) authentication, but not both.

Security—best practice when mixing encrypted access and clear access

It is possible to configure a RADIUS server or an WSS's local authentication database so that a user with encrypted access and a user with unencrypted access are authorized to join the same VLAN from different SSIDs. This configuration might allow a hacker to more quickly discover keys by listening to both the encrypted traffic and unencrypted traffic for comparisons. You can either use the Avaya SSID VSA or the encryption assignment VSA to prevent this problem.

If you only have one VLAN that each MAC-auth client should connect to, add the SSID VSA to the account for the MAC-address (either local or RADIUS). This will force the WSS to only allow that MAC address to connect to the specified SSID.

If you require the same MAC user to be able to connect to more than one SSID, you can use encryption assignment to enforce the type of encryption a user or group must have to access the network. When you assign the Encryption-Type attribute to a user or group, the encryption type or types are entered as an authorization attribute into the user or group record in the local WSS database or on the RADIUS server. Encryption-Type is a Avaya VSA. Clients who attempt to use an unauthorized encryption method are rejected. In this way, a client could connect to any WEP encrypted SSID, but not a clear SSID. (See the *Avaya WLAN 2300 Series System Software Configuration Guide* for more information.)

Security best practices

WSS Software and WLAN Management System provide robust options for securing management access, to WSSs and to the WLAN Management System client and WLAN Management System monitoring service. To optimize security for management access, use the following best practices.

Certificates

When anyone attempts to access a WSS, the switch authenticates itself by presenting a signed certificate to the management application that is requesting access. The switch's certificate can come from a certificate authority (CA) or it can be generated and signed by the switch itself. Avaya recommends that you use certificates assigned by a CA. Certificates from a trusted CA are more secure than self-signed certificates. Here are some trusted CAs:

- www.verisign.com
- www.entrust.com
- www.microsoft.com

If you use a self-signed certificate, configure the clients to not validate server certificates. If a client is configured to validate server certificates, the client will not be able to validate a self-signed certificate from the WSS.

Usernames

Avaya recommends that you do not create usernames that have the same spelling but use different case. For example, do not create both username *dang* and username *DANG*.

Passwords

The CLI, as well as WLAN Management System, can be secured using passwords. By default, the following access types do not have passwords configured. Each uses a separate password.

- Console access to the CLI. To secure console access, configure a username and password in the WSS's local database, using the **set user** command. After you configure at least one username and password, access to the CLI through the console requires a password. (Access through Telnet or SSH is not possible without a password, even on an unconfigured switch.)
- Access to the enable (configuration) level of the CLI, through the console, or through Telnet or SSH. To secure enable access, configure the enable password using the **set enablepass** command.
- Access to WLAN Management System client. To secure access, configure user accounts within WLAN Management System, on each machine on which the client is installed.
- Access to the WLAN Management System monitoring service. To secure access, configure user accounts within the monitoring service.

Do not use passwords that are easy to guess, such vehicle registration plates, family birthdays and names, or common words. Use combinations of uppercase and lowercase letters as well as numbers in all passwords.

SNMP

SNMP is disabled by default. Leave SNMP disabled unless you need it. If you do need to use SNMP, do not use the well-known community strings *public* (commonly used for read-only access) or *private* (commonly used for read-write access.) Likewise, if you are using SNMPv3, do not use a well-known or easy to guess string for the User Security Model (USM) username. By default, no SNMP community strings or USM users are configured. If you are using SNMPv1 or SNMPv2c, use it on an isolated management VLAN so that the clear text community strings are not visible on the public network. If you are using SNMPv3, set the security to a setting that is stronger than **unsecured**.

To disable SNMP (if not already disabled), use the **set ip snmp server disable** command.

CLI access

WSS Software allows CLI access through the console, through Telnet, and through SSH. Console and SSH access are enabled by default. Telnet is disabled by default.

Configure a username and password, so that WSS Software requires login even for console access. Usernames and their passwords are not specific to the type of management access. You can use the same username and password for access through the console, Telnet, or SSH.

Leave Telnet disabled unless you need it. Use SSH instead.

Web access

Web View uses HTTPS for encrypted communications and certificate-based server authentication, and requires use of the enable password.

Beginning in WSS Software Version 4.0, Web View access through HTTPS is disabled by default. Unless you need to use Web View, leave the HTTPS server on the WSS disabled. (Even though WLAN Management System also uses HTTPS, disabling the HTTPS server does not disable access by WLAN Management System.)

If you do need to use Web View, you can enable it using the **set ip https server enable** command. Use the following best practices to preserve or increase the security level related to Web access:

- Use an enable password that follows the password recommendations given above.
- Use a CA-signed certificate instead of a self-signed certificate on the WSS.

Note. If a user's wireless client does not trust the certificate, the user might experience an additional delay during login. To avoid the additional delay, use a certificate signed by your CA or an Internet CA.

WLAN Management System

By default, access to the WLAN Management System client and the WLAN Management System monitoring service do not require passwords. To secure access, configure user accounts within each instance of WLAN Management System client and within the monitoring service.

The monitoring service uses a signed certificate for authentication. The monitoring service has a self-signed certificate by default. For added security, used a certificate signed by a CA instead. To use a CA-signed certificate, install the certificate in a key store file on the machine where the monitoring service is installed, and change the name of the key store file used by the monitoring service from its default to the one where you installed the certificate signed by the CA.

Guest access (unencrypted SSIDs)

If you need to prevent all guest access (access to unencrypted SSIDs):

- Do not create any service profiles for SSID type clear.
- Delete any existing service profiles for a clear SSID.

VLANs

VLANs used for Web Portal must be separate from VLANs used for WSS System IP addresses. When configuring Web Portal users, ensure that users are assigned to VLANs different from those containing the System IP address of any WSS in the mobility domain.

Web-based AAA best practices

If you plan to use Web-based AAA, see the “Configuring Web-based AAA” section in the “Configuring Web-based AAA for Network Users” chapter of the *Avaya WLAN Security Switch Software Configuration Guide*. The section has configuration requirements and recommendations, in addition to an overview of the Web-based AAA process.

Mobility Domain™ (Multiple WSSs) best practices

Run the same WSS Software version on all WSSs in the Mobility Domain.

Avaya recommends that you run the same WSS Software version on all the WSSs in a Mobility Domain.

Helpful commands

Description Use the following commands to verify the proper operation of a Mobility Domain in support of features such as subnet roaming:

- **show mobility-domain**—In a functioning Mobility Domain, the output on every WSS displays every WSS in the Mobility Domain.
- **show roaming vlan**—In a functioning Mobility Domain, the output on every WSS displays the network-attached VLAN of every other WSS in the Mobility Domain.

Other useful commands, documented in the *Avaya WLAN Security Switch Software Command Reference*, include **show tunnel** and **show roaming station**.

Distributed AP best practice when using STP

A Distributed AP is a leaf device. You do not need to enable STP on the port that is directly connected to the AP.

If Spanning Tree Protocol (STP) is enabled on the port that is directly connected to a Distributed AP, you might need to change the STP configuration on the port, to allow the AP to boot.

Note. STP on a port directly connected to a Distributed AP can prevent the AP from booting.

Use IGMP snooping effectively

Using IGMP (11909, 12863, 12866)

Description WSS Software supports the Internet Engineering Task Force (IETF) draft *draft-ietf-magma-snoop* for controlling the forwarding of IP multicast traffic by a Layer 2 switch. The draft mandates the use of a 0.0.0.0 source IP address if no IP address is available on the switch for the subnet. However, some multicast routers and even other Layer 2 switches report errors in the presence of the 0.0.0.0 source IP address.

Workaround Apply the following methods to use IGMP snooping effectively:

- **Set IP addresses on all VLAN interfaces.** This straightforward workaround prevents most known issues. If querier functionality might be needed, ensure that the IP address of the WSS VLAN is higher than the address of any multicast router servicing the same subnet.
- **Consider disabling IGMP proxy reporting.** The IGMP proxy reporting function is enabled by default, but some multicast routers do not accept reports using a 0.0.0.0 source IP address. In this case, either assign an IP address to the VLAN interface on the WSS switch or disable IGMP proxy reporting. To disable proxy reporting, use the command **set igmp proxy-report disable**.

Note. Disabling proxy reporting can increase IGMP overhead traffic to the multicast router.

- **Enable the IGMP querier only if needed.** The IGMP pseudo-querier function is disabled by default. Enable it only if the source of a multicast stream is on a subnet the WSS switch is also connected to. If this is the case, you must assign an IP address to the VLAN interface. The IP address must be higher than the IP address of the querier multicast router on the same subnet. To enable the IGMP pseudo-querier, use the command **set igmp querier enable**.
- **Disable multicast router discovery.** This multicast router solicitation protocol (part of *draft-ietf-magma-snoop*) is known to cause error messages with other IGMP snooping switches and multicast routers. To disable the protocol, use the command **set igmp mrsol disable**. (The protocol is disabled by default in the current software version.)

User ACLs require explicit source and destination addresses

A user ACL is an ACL that is applied to a specific username. You can apply ACLs to a user's inbound or outbound wireless traffic. For a user ACL to take effect, you must explicitly set both the source and destination addresses in the ACL.

Rogue detection active scan interval is longer during a SpectraLink SVP call. (23317)

The active scan feature can be used during SVP calls. However, when a call is active, the interval at which active scan goes off-channel to look for rogues is increased from once a second to once every 60 seconds.

Due to the longer interval between active scans, it can take longer for WSS Software to detect a rogue AP when an SVP call is active. Generally, detection of a rogue while a call is active can take from 3.5 to around 7.5 minutes. To reduce the detection time, add more APs to the coverage area.

IPv6 support

WSS Software 5.0 can forward IPv6 traffic transparently, at Layer 2. IPv6 clients in the same subnet can communicate with one another through a WSS.

VoIP devices vendor support

These are the Avaya supported options:

- SpectraLink—Non-WMM SVP devices
- Vocera—Non-WMM Vocera devices

Interoperability

Wireless NICs tested with Avaya WSS Software

Manufacturer Model	Driver version	Driver Date	Dynamic WEP	Mixed WPA/TKIP with Dynamic WEP	WPA with TKIP	WPA with AES CCMP	WPA2 with TKIP	WPA2 with AES CCMP	11i Fast Roam	Web AAA	WSS Version Tested
3COM 3CRDAG675B PCI	2.0.0.1	2005-05-05	Pass	Pass	Pass	Pass	Pass	Pass	-	Pass	7.0.1.0.15
3COM 3CRPAG175B	v1.1.0.21/ 4.1.2.56	2005-07-14	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	7.0.0.0.87
ALPHA AFW-GC50 PCMCIA	3.1.1.7	2005-02-22	Pass	Pass	Pass	Pass	Pass	-	-	-	6.0.4.0.5
Apple iPhone	1.0.1 (1C25)	2007-07-31	-	-	Pass	-	-	Pass	-	-	6.0.3.2 REL
Apple MacBook Pro Atheros	-	-	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	-
Apple MacBook Pro	-	-	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	-
Cisco AIR-PI21AG PCI	3.5.0.44	2006-12-12	Pass	Pass	Pass	Pass	Pass	Pass	-	Pass	7.0.1.0.13
Cisco Air CB21AG-A-K9 PCMCIA	4.0.0.295	2008-01-04	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	7.0.0.0.78
Cisco Air CB21AG-E-K9 PCMCIA	v2.6	2006-03-28	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	5.0.8.0.8
Cisco Air CB21AG-W-K9 PCMCIA	23.0.0.104	2006-05-19	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	6.0.3.109
D-Link DWA-642	6.0.1.75	2006-08-28	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	6.0.3.0.56
D-Link DWA 160 USB	1.2.1.0	2008-07-30	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	7.0.6.0.3
D-LINK DWL-650+A Card	1.0.0.0	2005-03-23	Pass	-	Pass	Pass	Pass	Pass	Pass	Pass	6.0.4.0.5
D-Link DWL-AG530	3.00.51031 (v1.05)	2006-03-23	Pass	Pass	Pass	Pass	Pass	Pass	-	Pass	5.0.7.0.30

Manufacturer Model	Driver version	Driver Date	Dynamic WEP	Mixed WPA/TKIP with Dynamic WEP	WPA with TKIP	WPA with AES CCMP	WPA2 with TKIP	WPA2 with AES CCMP	11i Fast Roam	Web AAA	WSS Version Tested
D-link DWL-AG530 PCI	5.3.0.46	2007-05-28	Pass	Pass	Pass	Pass	Pass	Pass	-	Pass	7.0.1.0.15
D-Link DWL-AG660	4.1.2.72	2005-08-24	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	7.0.1.0.5
Dell 1470	4.100.15.5	2006-10-12	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	7.0.1.0.5
Dell 1505 MiniPCI	4.170.25.12	2007-09-20	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	7.0.6.0.010
Dell 2915	9.0.39	2005-09-12	Pass	Pass	Pass	-	Pass	Pass	-	Pass	4.2.0.2.11
Dlink DWA130	1.2	2007-10-07	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	-
Enrerasys RBTBJ AW	4.1.2.7116	2005-08-16	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	7.0.1.0.6
Intel 2200 miniPCI	9.0.4.37	2007-07-25	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	7.0.1.0.12
Intel 2915 miniPCI	v11.5.0.32 Device Driver: 9.0.4.37	2007-11-07	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	7.0.0.0.76
Intel 3945ABG miniPCI	11.5.0.32	2007-11-07	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	7.0.0.0.79
Intel 4965 MiniPCI	12.0.0.82	2008-07-08	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	7.0.6.0.010
Intel 5300 MiniPCI	12.0.0.82	2008-07-05	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	7.0.6.0.010
KINGNET W510C W510P PCMCIA	5.103.1020.2005	2005-10-20	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	6.0.4.0.5
LINKSYS Wireless-G WPC54G PCMCIA	3.100.64.0	2005-02-18	Pass	Pass	Pass	Pass	-	-	-	Pass	6.0.4.0.5
Linksys WPC 600N	4.150.31.0	2007-08-17	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	7.0.4.0.9
Linksys WUSB 600N	1.1.0.0	2007-12-14	Pass	Pass	Pass	-	Pass	-	Pass	-	7.0.4.0.9
Netgear WAG511U	4.0.0.7097	2006-09-28	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	7.0.0.0.89

Manufacturer Model	Driver version	Driver Date	Dynamic WEP	Mixed WPA/TKIP with Dynamic WEP	WPA with TKIP	WPA with AES CCMP	WPA2 with TKIP	WPA2 with AES CCMP	11i Fast Roam	Web AAA	WSS Version Tested
NetGear WG311T	Driver v4.1.2.130 Utility v4.3.16.306	2006-07-21	Pass	Pass	Pass	Pass	Pass	Pass	-	Pass	5.0.7.0.32
Netgear WG511T	4.2.2.14	2006-03-23	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	7.0.0.0.88
NETGEAR WG511 PCMCIA	3.1.1.7	2005-02-22	Pass	Pass	Pass	Pass	-	-	-	-	6.0.4.0.5
Netgear WN511T	4.1	2007-07-24	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	-
Netgear WNDA 3100	3.0.0.95	2008-01-17	Pass	-	Pass	Pass	Pass	Pass	-	Pass	7.0.4.0.9
Orinoco PC24E-11-FCR PCMCIA	7.64.1.316	2020-07-15	Pass	-	-	-	-	-	-	Pass	5.0.8.0.1
Planet WDL-U357	v1.10.25 / 3.1.3.115	2005-06-22	Pass	Pass	Pass	Pass	-	-	-	Pass	5.0.8.0.1
Proxim Orinoco 8480-FC PCMCIA	4.2.2.7	2006-01-20	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	7.0.1.0.6
Proxim Orinoco Gold PCI	3.0.1.6	2004-04-07	Pass	Pass	Pass	Pass	Pass	Pass	Pass	-	7.0.1.0.16
SMC 2802W	3.0.11.1	2006-3-23	Pass	Pass	Pass	Pass	-	-	-	Pass	5.0.8.0.7
TL-WN550G PCI	4.1.2.133	2006-12-21	Pass	Pass	Pass	Pass	Pass	Pass	-	Pass	6.0.4.0.5
TP-LINK TL-WN510G PCMCIA	4.1.2.133	2005-12-21	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	6.0.4.0.5

Note. Avaya does not guarantee interoperability with cards and configurations that are not tested.

Known behaviors and issues

In addition to the more common items indicated in "Best practices and common issues" on page 31, the current software version contains the following known behaviors and issues.

Upgrading from an earlier version of MSS 7.1 may invalidate the existing certificates on the MX. (64640)

Description After upgrading from WSS 7.1.4.2 to 7.1.5.3, the existing PKCS#12 certificates become invalid.

Workaround You must reinstall the certificates and generate the crypto keys to restore the certificates.

Auto-tune channel-config lockdown feature does not work in a cluster configuration. (62746)

Description When operating in Cluster mode, the auto-tune channel lockdown command is not available.

Workaround None. Auto-tune lockdown must be completed via alternate mechanisms. e.g. WMS or auto-tune lockdown while in a basic Mobility Domain configuration.

If AP has vlan-tagging enabled, it does not boot in bridging mode. (61935)

Description The static VLAN tag is not supported in mesh and bridging modes. It is not a valid configuration to enable both at the same time.

Workaround N/A

Some cluster configuration changes on the WSS are not accurately reflected by WMS. (59864)

Description When operating in Cluster mode, minor changes to mobility domain and load balancing configuration are not accurately reflected in WMS.

Workaround Restarting the WSS causes WMS to reread the WSS configuration and update accordingly.

The show ap verbose command incorrectly reports that the MP-82 has a second ethernet port. Port 1 is the only port available on the MP-82.

Workaround None.

Voice handsets can be sensitive to changes on an in-service SSID. (41603)

Description Particular voice handsets are sensitive to changes made to an in-service SSID. This can result in the handset operating with stale connection information.

Workaround When using affected handsets, disable the Service Profile prior to making any configuration changes.

802.11n adapter incompatible with Spectralink Voice Protocol (SVP) enabled service profiles. (55632)

Description Some 802.11n wireless adapters may experience packet loss on wireless services with the Spectralink Voice Protocol enabled. This problem only exists when using the Trapeze MP-432 with frame aggregation enabled.

Workaround When you use SVP on the Trapeze MP-432, disable the frame aggregation.

In Cluster, when Neighbor-list configuration is updated, the secondary seed and member seed fails to synchronize with primary seed. (55957)

Description After you setup Mobility Domain and configure the WSS on the Neighbor list, enable the Cluster. The synchoronize failure infomation is displayed.

Workaround You can follow the below steps :

1. Disable the Cluster.
2. Re-configure the 'Neighbor list' in all the WSSs.
3. Enable the Cluster.

Note: If deleting the ‘Neighbor-list’ do not solve the sync failure, re-add the ‘Neighbor-list’.

When the ACL is mapped to the port, the MAC Based Rules do not specify the Destination MAC in the ACL. (56038)

When calls are made to 6 phones (3 pairs), within 30 minutes, some calls get dropped, but phone will be still connected to AP.

Description Calls get dropped within 30 minutes, when calls are made to 6 phones (3 pairs). The problem only happens to the 61XX phones on 7.0.

The Trapeze MP-432 and Intel 2915 legacy 802.11g card have incompatibility issues. The problem is occurring on the HP laptops using the 2915 Intel NIC Card. The HP laptop that is using this NIC card at Avaya is NC6220. (55397)

Priority of Layer 2 ACL and static cos for the upstream traffic is not concurrent. (55074)

If you experience issues with Certificates or Private keys installed on WSS switches after upgrading to newer 5.0 and 6.0 releases. (32833)

Description Affected services may include SSH, Web-portal, PEAP-offload, WebView, and WMS administrative access and/or Domain Security. Error messages relating to this issue include the following:

- HTTPD Aug 14 16:32:13.648823 ERROR HTTPD: SSL connection failure (bad cert?).
- Admin client 145.36.245.51 EAP Aug 14 16:32:14.110502 ERROR EAP_STORE_ERR: No EAP key pair. Cannot do PEAP.

Workaround You can prevent this issue by generating new private keys and any related Certificates prior to upgrading to a newer version of WSS. Third party Certificates must be exempt from this issue provided a new private key was explicitly generated previous to the CSR request generation. If you are unsure whether a new private key was generated before the initial CSR the best course of action may be to request a replacement certificate from your provider using a new private key.

Auto AP command has no effect on Directly connected AP. It is meant for Distributed AP only. (39474)

If local changes are not deployed and WSS software is upgraded, local changes will be lost. (41914)

Uploading one WSS overwrites local switching configuration on other WSS. (38317)

Converting a mobility-domain member to a secondary-switch, the seed switch will see the secondary switch as a member. (39424)

Workaround Reboot the seed switch.

‘show rfdetect measures’ command may display wrong channel for AP while countermeasuring. (41235)

'show session output' is not updated when roaming between a 3rd party AP and an Avaya AP. (41124)

Ping from the Linux Controller to the wireless client didn't work after the user roamed from an AP with LS enabled to an AP without LS. (63582)

Hitless cluster upgrade fails - APs with sessions are being reset. (64946)

Config core on PS when disabling cluster. (64517)

Not all the APs had PAM and SAM. (64443)

IDS SSID spoof detection is broken. (62092)

The APs don't fail-over when disabling cluster on the switch. (60632)

Web logout does not work after roaming a LS web client from one WSS to another. (58471)

Mesh Services

The mesh AP attempts to connect to the AP with the lowest radio channel number.(40473)

System configuration issues

The default value for RADIUS "deadtime" shown in the CLI help is incorrect.

Workaround The correct default value is 0.

When upgrading systems with very large configurations, for example, hundreds of APs or hundreds of users, do the following. (41689)

Workaround It may be necessary to save the configuration to a backup file, generate a minimal configuration, perform the update, load the backup configuration from the command line, and then save the configuration.

The set ap <apnum> boot-configuration switch switch-ip cannot be set at the same time. set ap <apnum> boot-configuration switch name <switch-name> dns <ip addr>. The commands overwrite each other when used. (41330)

Time and date do not synchronize with an NTP server, if the switch's NTP client is enabled before the NTP service is started on the server. (20382)

Switching and port issues

Antenna sensing has been deprecated from system software. The antenna configuration is the authoritative source to enabling external antenna operation on the MP, even if the external antenna isn't actually connected.

Mixing Autonegotiation with full-duplex mode on a link causes slow throughput and can cause an WSS port to stop forwarding. (26276)

Description Avaya recommends that you do not configure the mode of an WSS port so that one side of the link is set to autonegotiation while the other side is set to full-duplex. Although WSS allows this configuration, it can result in slow throughput on the link. The slow throughput occurs because the side that is configured for autonegotiation falls back to half-duplex.

A stream of large packets sent to an WSS port in a certain configuration can cause forwarding on the link to stop.Router redundancy protocol on intermediary devices between WSS in a Mobility Domain can interfere with communication among the switches. (16910)

Description If the Mobility Domain contains intermediary switches or routers that use a router redundancy protocol, WSS switches communicating through those intermediary devices might lose communication with each other due to the way some router redundancy protocols handle MAC addresses. If this issue occurs, log messages appear periodically on the seed WSS indicating that member WSS switches are entering or leaving the Mobility Domain.

Workaround Set the FDB timer (default 300 seconds) and the ARP timer (default 1200 seconds) to the same values on the WSS switches. Avaya recommends using 300 seconds as the value for both timers. To set the FDB timer, use the set fdb agingtime command. To set the ARP timer, use the set arp agingtime command.

Access Point (AP) issues

Wireless clients connected to directly attached APs may not display as connected in the show system output information. (41792)

If a Series 2332 access point is configured with a transmission power less than 10, wireless clients cannot connect to the AP. (41018)

When connected to the network using an Intel 2100 wireless network card, large file transfers may cause the wireless client to disconnect. (40721)

A distributed AP may not successfully boot if Port 1 of the AP has an operational Ethernet link, but an WSS is unreachable via this data link. All other combinations of power and data connectivity are fully supported. (38807)

Web-based AAA issues

IPv6 clients cannot authenticate using Web Portal. (26291)

Description The web-portal ACL does not work on IPv6 traffic. IPv6 clients will not be able to authenticate using Web Portal unless the clients also run IPv4.

Workaround This issue affects Web-Portal authentication only. The other authentication types (802.1X, MAC, and Last Resort) can be used with IPv6 clients.

Web View Issues

If you are running Linux Redhat 9 and use Firefox 2.0 to open WebView, the browser may become unresponsive. This behavior is noted on the 2370 and 2380 (40676)

DAP to AP conversion during Upgrade from Release 5.0 to 6.0

The “DAP” configuration is changed to an “AP” configuration when you upgrade from Release 5.0 to 6.0.

For example:

Release 5.0 DAP configuration:

```
set dap 1 serial-id stp1111111 model 2330A
set dap 1 name AP-North
set dap 1 bias low
set dap 1 radio 1 radio-profile RadioProfile-1
set dap 1 radio 2 radio-profile RadioProfile-1 mode enable
```

Release 5.0 DAP configuration converted to Release 6.0 AP Configuration:

```
set ap 1 serial-id stp1111111 model 2330A
set ap 1 name AP-North
set ap 1 bias low
set ap 1 radio 1 radio-profile RadioProfile-1
set ap 1 radio 2 radio-profile RadioProfile-1 mode enable
```

To upgrade a mobility network with “dap” configurations, do the following:

When upgrading from Release 5.0 to 6.0, the “dap” configuration is updated to an “ap” configuration. When using the WMS to install the Release 6.0 image on the WSS, a backup configuration file is created on the WSS as “configuration-bak.5.0”. This backup file is the only way to go back to a “dap” configuration if the WSS software needs to be downgraded to Release 5.0 in future. It is highly recommended that another copy of the configuration is created on the WSS under a different file name. The administrator must store a copy on an external server. There is no method to convert an AP configuration to a DAP configuration when downgrading from Release 6.0 to 5.0 without a backup 5.0 configuration file. All associated AP configurations needs to be reconfigured if backup file is not available to use.

For more information on “Upgrading from WMS Version 5.0.8.1 or 5.0.11.3”, refer “*Avaya WLAN – Management Software 2300 Series Release Notes – Software Release 6.0.5.1*”.

Note. After the WSS reboots and is operational, go to WMS and "refresh devices". The WMS server indicates that there are network changes available. These changes are due to the “dap” configurations being converted to “ap” configurations. Accept the network change (**WMS, Devices, Networks Changes**).

Upgrading an individual switch using the CLI

Note. Always upgrade the "seed" switch first when upgrading a Mobility Domain. Verify that the "seed" switch is operating on the new software before proceeding to upgrade other members of the Mobility Domain.

1. Back up the switch, using the **backup system** command. (See "Preparing the WSS for the Upgrade" on page 23.)
2. Copy the new system image onto a TFTP server.

   For example, log in to http://www.avaya.com/support/ using a web browser on your TFTP server and download the image onto the server.
3. Copy the new system image file from the TFTP server into a boot partition in the switch's nonvolatile storage.

   You can copy the image file only into the boot partition that was *not* used for the most recent restart. For example, if the currently running image was booted from partition 0, you can copy the new image only into partition 1.
4. Set the boot partition to the one with the upgrade image for the next restart.

   To verify that the new image file is installed, type **show boot**.
5. Reboot the software.

   To restart a WSS and reboot the software, type the following command:

   reset system [**force**]

When you restart the WSS, the switch boots using the new WSS Software image. The switch also sends the AP version of the new boot image to APs and restarts the APs. After an AP restarts, it checks the version of the new AP boot image to make sure the boot image is newer than the boot image currently installed on the AP. If the boot image is newer, the AP completes installation of its new boot image by copying the boot image into the AP's flash memory, which takes about 30 seconds, then restarts again. The upgrade of the AP is complete after the second restart.

Upgrade scenario

To upgrade a 2360 switch, type commands such as the following.

Note. This example copies the image file into boot partition 1. On your switch, copy the image file into the boot partition that *was not* used the last time the switch was restarted. For example, if the switch booted from boot partition 1, copy the new image into boot partition 0. To see boot partition information, type the **show boot** command.

2360# **save configuration**
success: configuration saved.

2360# **backup system tftp:/10.1.1.107/sysa_bak**
success: sent 28263 bytes in 0.324 seconds [87231 bytes/sec]

2360# **copy tftp://10.1.1.107/N6060500.005 boot1: N6060500.005**
.....
.....
success: received 10266629 bytes in 92.427
seconds [111078 bytes/sec]2360# **set boot partition boot1**
success: Boot partition set to boot1:**N6060500.005**(6.0.5.0.5).
2360# **show boot**
Configured boot version: 6.0.5.0.5
Configured boot image: boot1:**N6060500.005**
Configured boot configuration: file:configuration
Backup boot configuration: file:backup.cfg
Booted version: 6.0.5.0.5
Booted image: boot1: **N6060500.005**
Booted configuration: file:configuration
Product model: 2360
2360# **reset system force**

To copy the saved running configuration to a backup file:

2382#**copy <running-filename><backup-file>**

Example: copy configuration configuration.bak

To tftp a copy of the configuation.bak file:

2382#**copy <backup-filename>tftp:<tftp server IP>/<backup-filename>**

Example: copy configuration.bak tftp:192.160.160.1/configuration.bak

Downgrade scenario

The WMS can be used to downgrade the WSS switches. After downgrading the WSS to Release 5.0, and that WSS comes back up and is operational, go to WMS and execute the refresh devices (**WMS, Devices, Refresh**). The WMS server will indicate that there are network changes. Undo these network changes and deploy the local changes. The local changes are related to the file "configuration-bak.5.0". The "ap" configurations in Release 6.0 will not be changed to "dap" configurations when WMS is used to deploy the local changes if the "configuration-bak.5.0" file does not exist upon downgrading. Another Release 5.0 backup configuration can be loaded after the WSS boots back up if there is no backup Release 5.0 configuration available on the WSS.

Migrating your Web-based AAA and Last-Resort configurations from WSS Software version 5.*x* to WSS Software version 6.0 or later

When you upgrade from 5.*x*, the Web-Portal and last-resort configuration is upgraded automatically. WSS Software makes the following configuration changes during upgrade.

The changes affect **web-portal-*ssid*** and **last-resort-*ssid*** users but they do not affect **web-portal-wired** or **last-resort-wired** users.

Web-Portal changes during upgrade

During upgrade, WSS Software automatically makes the following changes for each service profile whose fallthru type is set to **web-portal**.

- Copy the **vlan-name** attribute the **web-portal-*ssid*** user to the **vlan-name** attribute of the same SSID's service profile.
- Copy the **filter-id** *aclname***.in** attribute from the **web-portal-*ssid*** user to the **web-portal-acl** option of the SSID's service profile.
- Delete the **web-portal-*ssid*** user from the configuration.

Last-Resort changes during upgrade

During upgrade, WSS Software automatically makes the following changes for each service profile whose fallthru type is set to **last-resort**.

- Copy the **vlan-name** attribute and all other user attributes set on the **last-resort-*ssid*** user to the **vlan-name** attribute and other attributes of the same SSID's service profile. If an attribute is already configured on the service profile, the value is changed to the last-resort value for the same attribute, if set.
- Delete the **last-resort-*ssid*** user from the configuration.
- Delete the **set authentication last-resort** command from the configuration.

Considerations when using Third-Party APs (30061)

If you are using a third-party AP for Web-Portal and last-resort authentication, a service profile must exist on the WSS that provides authentication attributes for clients. The name of the service profile must match the name of the SSID configured for the third-party AP.

If your 5.*x* configuration already had a service profile with the same name as the SSID of the third-party AP, then the upgrade does not require any additional action. If your 4.*x* configuration did not have a service profile with the same name as the SSID of the third-party AP, then you must create one and set the authentication attributes. In release 6.0, last-resort authentication is always *local*.

Although it is possible to create multiple service profiles for a given SSID, Avaya recommends that you have only one service profile with the SSID of the third party AP.

If you need to downgrade from 5.0.9 to a 5.x release, the configuration will work properly if it had worked properly in 5.0.9

Considerations for configuring Mesh Services

WSS Version 6.0 supports five Mesh APs per Mesh Portal and a single Mesh Services link between the Mesh AP and the Mesh Portal. It is also recommended to configure local switching for the Mesh AP.

WSS 2380, 2382, and MX-2800 supported AP license activation key upgrade

A License Activation Key upgrade supports an additional 40 or 80 AP's up to the maximum of 120 AP's per WSS 2380.

A License Activation Key upgrade for an WSS 2382 supports an additional 32, 64 or 96 AP's up to the maximum of 128 AP's per WSS 2382

A License Certificate is used to provide a single software license and its associated License Activation Key. The number of supported Access Points beyond 40 for your Avaya WLAN WSS 2380 and beyond 32 for your Avaya WLAN WSS 2382 will depend on the upgrade License Activation Key that is installed and activated. To enable the additional support of Access Points, you must obtain a License Activation Key from Avaya.

To obtain the License Activation Key, follow the instructions on the License Certificate provided with either the WSS 2380 or 2382 supported AP License Upgrade Kits.

For 2382, to get maximum APs you will have to obtain multiple coupons. Each coupon needs to be activated against their 2382 Serial number. Only the last key is activated from the key activation Website and it will activate the max number of APs on the switch.

When the proper License Activation Key has been obtained, follow the instructions below to enable the WLAN WSS 2380 or 2382 features:

1 Use the following command at the enable (configuration) level of the CLI to install the activation key:

set license activation-key

2 Type in the entire activation key and press enter

In the following example, an activation key for additional AP’s is installed:

2380# set license 3B02-D821-6C19-CE8B-F20E
success: license accepted

3 Verify installation of the new license by typing the following command: show license Support for the additional AP’s begins immediately. The switch does not need to be restarted for the upgrade to be effective.

To upgrade an WSS license:

1 Obtain a license coupon for the upgrade from Avaya or your reseller.

2 Establish a management session with the WSS to display the serial number. To use the CLI to display the serial number, type the following command:

show version

In the following example, the switch serial number is 1234567890:

WSS> show version
Wireless Security Switch, Version: 6.0.3.0 QA 98
Copyright (c) 2010 Avaya, Inc. All rights reserved.
Build Information: <build#98> REL_6_0_branch 2007-05-15 14:21:00
Model: 2360

Hardware
Mainboard: version 1 ; revision 01 ; FPGA version 8
Serial number STP1W5002M
Flash: 1.0.0 - 0
Kernel: QNX-630
BootLoader: 4.3 / 6.0.7

3 Use a Web browser to access the Avaya license server at the following URLs:

For all Avaya-branded Switches: http://www.avayalicensing.com/

For Trapeze MX-2800 only: http://www.trapezenetworks.com/support/product_licenses/

4 Type your e-mail address in the E-mail and Confirm E-mail fields.

5 Select your WSS model from the Product Selection list.

6 Type or copy and paste the WSS serial number into the Product Serial Number field, and click OK. The Product Licensing page appears.

7 Type the coupon activation code(s) into the Coupon Code(s) fields and click OK. The Licensing Confirmation page appears, and displays the activation key (also called the license key).

8 Highlight and copy the entire activation key.

9 On the WSS, use the following command at the enable (configuration) level of the CLI to install the activation key:

set license activation-key

In the following example, an activation key for an additional 96 APs is installed:

WSS-2382# set license 3B02-D821-6C19-CE8B-F20E
success: license accepted

10 Verify installation of the new license by typing the following command:

WSS-2382# show licenses
Feature : 96 additional APs

11 Support for the additional APs begins immediately. You do not need to restart the WSS to place the upgrade into effect.

Issues resolved since version 7.1.5.4

- If a non-802.11n AP has a service profile configured with the option to require 11n, the AP does not beacon SSIDs over the network. (65362)
- Mesh APs were timing out on the network. (64302)
- The time on the WSS was drifting from the actual time on the network. (64156)
- When upgrading from an earlier version of WSS, CA certificates were deleted from the configuration. (63866)
- Some SSIDs were erroneously classified as rogue SSIDs on the network. (63829)

- The link up/down events on switch ports connected to the MP-82 were affecting connectivity to the network. (63144)

Changes to Default Behaviors in WSS

- The "dfs_channels" attribute in the radio profile of the Mesh AP backhaul radio must be enabled during pre-staging so that the backhaul link can be established on DFS channels. Please note that when there is no radio profile is specified, default radio profile is used. (63901)

Documentation Errata

- The ACL edit buffer is meant to be used for creating and editing one ACL at a time. If you need to create multiple ACLs, use 'commit security acl all' after each ACL. This is not fully documented in the WSS User's Guide. (61703)
- Starting with 7.0, the dot1x reauth-period works only on a dynamic WEP and WPA with WEP-40 or WEP-104 cipher. In case that both the dot1x reauth-period and session-timeout attribute (from the service profile or RADIUS) are set, the session-timeout attribute value is used.
- Additional LDAP Command - the following command was added to the LDAP feature: (64054)
  - **WSS# set ldap prefix-dn prefixdn**

    The attribute, prefixdn, can consist of up to 64 characters with a default value of *cn*. It is the first RDN attribute name to be used during simple-authentication.
- The WSS User's Guide omits the information that configuring 11n means that TKIP and WEP are no longer configurable as encryption methods.
- Although not explicitly stated in the WSS User's Guide, mesh configuration is supported for 802.11n products including the MP-432, MP-82, and the MP-632.

  In addition to configuring the AP LED mode for a single AP, you can also configure the mode for a range of APs and on auto APs. Use the following commands:

  WSS# set ap apnumrange led-mode {auto|static|off}

  WSS# set ap auto led-mode {auto|static|off}

  Trapeze APs and the equivalent OEM APs are supported, however, the MP-71, MP-620, and MP-622 are not supported.

  The **blink** command takes precedence over the **led-mode** command.

Issues resolved since version 6.0.5.1

A memory leak caused the WSS to become unresponsive. (49640)

The customer has to enter all the AP radio configurations (set ap <apnum> radio <radionum> antennatype <>,etc)before the Mesh AP configurations (set ap boot-configuration mesh ....) are entered in CLI. (49476)

When the command "show ap global" was run on a Mobility Domain with APs configured with redundancy, only the APs configured for High Bias on that WSS appeared. (48058)

The incoming port 80 and 443 connections were overriding the 16 max accepted connections. (46511)

The TXOP limit is sometimes included in AC Voice, and sometimes it does not appear (but the length of the WMS element is the same). Also, some management frames are two bytes smaller than what they specify because the radio driver appears to be stripping 2 bytes off of management frames in certain situations. (48572)

Under certain network conditions, WSS may send invalid responses to WMS requests. This event causes WMS to translate the error into "Empty or missing protocol" response. (48085)

Ascom phones report approximately 50% packet loss when using AES/CCMP with U-APSD power-save mode. (46468)

An AP may display erroneous settings when auto-tune is configured for the transmitted power. (46130)

The dot1x reauthorization timer overwrites the service profile or AAA session-timeout values. (44593)

An WSS may not respond when a large number of Spectralink phones attempt to connect at the same time. (44586)

The AP fails to send out buffered information to wireless phones after receiving a QoS-Null data frame with power bit ="0". (42764)

The first web-portal client through a network domain must wait (up to 5 minutes) to get access. (41625)

Issues resolved since version 6.0.4.6

Calling-station-id is not sent for RADIUS when using Web-portal. (46129)

Some wireless phones were unable to detect an SSID and connect to the network.(45832)

An ARP Request broadcasted packet with a tagged VLAN is re-broadcast to the Ethernet port to another AP.(45521)

The AP does not boot immediately when there are two DHCP servers in a same IP subnet because the AP records two IP addresses for one client in the ARP table. The AP will successfully boot up after a 5-10 minute delay.(42347)

When the WSS receives a TCP connection setup (SYN) packet on a listening TCP socket/port, (if that packet also has a connection termination flag (FIN) set) the WSS typically drops this packet. In normal conditions, SYN and FIN are not set on the same packet. Such a setting in a packet could be due to protocol error or DoS attacks. The fault caused WSS to close the listening socket incorrectly in addition to dropping the packet, and that is fixed now. (42015)

The client is reporting faulty behavior when sending different EAP packets with the same EAP ID and the WSS is not properly handling the scenario. The fix drops duplicate EAP packets.(41542)

The command “show arp" becomes illegal after a handover between other segment controllers. (37591)

Issues resolved since version 5.0.11.4

Downgrade WSS from V6 to V5 looses AP/DAP configuration. Deploy of local change failed because WSS response contains errors. "Verification" field does not contain error message. The only option left now is Undo local change, thus WSS looses all the dap configuration (43799).

FTP based ACLs which deny traffic will deny all the traffic when mapped to user or SSID (44179).

Workaround Use VLAN or port based ACLs.

DAP-Static-IP: When configuring the IP address on the DAP you cannot leave the gateway field empty. (32583)

Wireless clients connected to WLAN were unable to communicate with other wireless clients, but they could communicate with wired hosts. (41801)

Certain URLs that contain escape characters (of the form %HexHex) are not handled by Web Portal and may result in the client unable to fetch the login page or loss of Web connectivity. Such URLs are known to be generated by applications like Windows Live Messenger. It is recommended that clients do not run such applications before performing Web Authentication. (41477)

When configuring a mesh service profile, Avaya recommended increasing the service-profile retry limit. (40939)

In some instances, when traffic is roaming between WSS, the WSS may not send an accounting "interim" packet. (40743)

PoE compatibility with certain APs was improved.(40150)

In the show dhcp output, VLAN 0 is the subnet used for all APs configured as directly attached ports. (39775)

Static CoS configuration causes the following behavior: (39210)

Static CoS sets a fixed priority for client packets. When static-cos is not enabled, packets are classified and marked based on rules for flow-through CoS. In overlay mode, the WSS marks downstream packets in 802.1p and tunnel DSCP.In local-switching mode, the WSS is passive, and flow-through CoS rules affect downstream 802.1p.

Workaround Static CoS works in both modes on the AP to give wireless priority downstream and to mark packets upstream. In local-switching mode, packets are only marked in 802.1p.

A Mesh AP failed during a WPA 4-way handshake. (39216)

An AP was taking too long to reboot on the network. (38346)

After a power interruption, APs configured for Mesh Services could not reconnect to the network. (39241, 39216)

The WSS requires the CERTIFICATE header for PKCS7 PEM formatted certificates. (39207, 36658)

If the sensor image has been downloaded at least once to a distributed AP since the WSS booted, a new version is not used by the WSS until after reboot. (35084)

An AP would remain in the unconfigured state unless the ap <apnum> time-out setting was configured manually. (38346)

Loading a large configuration on an 2350 caused the WSS to become unresponsive. (37975)

On APs with the country code US, it is recommend to avoid configuring radio 2 for channels 52, 56, pr

60, and 64. Using these channels may cause periodic outages on the wireless network. This will be resolved in the next release of WSS Software. (37134)

A mobile client cannot associate with WSS Software configured for WEBAAA WPA/TKIP encryption and PSK authentication SSID if the PSK is provisioned by WMS 6.0.2.1.0. (37096)

An IP address of 0.0.0.0 was incorrectly processed by arp-request and arp-reply in WSS Software. (36438)

Configuring too many ACLs and ACEs caused the WSS to become unresponsive. (36261)

Rebooting the WSS via CLI command 'reset system' does not generate a 'warm start' trap on system reboot. Instead a 'cold start' trap is sent. (35357)

In WMS, the Disable Auto-Tune task at the Network plan level has confusing wording. (34058)

The views from a previously created floor plan appear in a new floor plan. (33041)

Load Balancing does not work well when a Load Balancing group has a mix of directly attached APs and DAPs. (32931)

On an untethered AP, the force-image-download flag should NOT be set. If it is set, clear it with the set ap <apnum> force-image-download disable command. (32341)

WSS Software sometimes reports that the CPU is idle more than 100% of the time. (32331). When accessing the Web Portal Login page, the SSL socket stays open until you submit the page or the browser closes. (31145)

A 'ping' initiated from a WMM client associated with an AP gets corrupted when the ping packet size is equal to or greater than 561 bytes. (30945)

The source-ip option of the ping command accepts an inappropriate IP address. (30289)

The clear trace command does not work when multiple tracing is enabled. You must use the command clear trace all to stop the process. (29473)

There are upgrade and downgrade issues with 3rd party APs for AAA. (29400)

Directly attached AP-352 stays in reboot loop when WSS Software is upgraded (29320)

After the SODA agent was downloaded by the client, the WSS produced a core file and restarted when a Web Portal session was cleared. (28356)

Attributes not present in “show sessions network verbose” command. (27886)

Login page is not served to Web-Portal client authenticated on tunneled VLAN. (27226)

On a tagged VLAN, reconfiguring a wired authentication port as a network port causes the switch to restart if the port is enabled. (27164)

Remediation ACL is not applied to a client after roaming back to a native WSS. (26547)

Remediation ACL does not work if the client browser has proxy enabled. (26478)

Using Autonegotiation with full-duplex mode on a link causes slow throughput and can cause an WSS port to stop forwarding. (26276)

If SODA is enabled but the enforce-check option is disabled, WSS Software does not download the agent to clients with browsers that have proxy enabled. (26213)

While virtual desktop is active, a reauthenticating Web Portal user cannot log in. (25754)

Occasionally a DAP/VLAN configuration is returned as a successful operation when it did not succeed. (25409)

Converting a Distributed AP with a static IP address into a directly connected AP results in harmless error message. (25563)

Port group names containing dashes prevent port groups from being listed by the show port-group command. (23874)

Client connection to an open SSID on an Auto-DAP can cause “Variable not implemented” message. (22467)

Deleting PEAP-MS-CHAP-V2 AAA methods in an 802.1X policy with WMS might not be reflected on the WSS. (14157)

In WSS 5.0.10.3, when a DAP updates the IP address, it takes longer to come up due to TAPA Announce timeout. (38693)

The AP crashed after receiving a UDP packet to port 1325. (38676)

When using WebView to monitor the network, the system page and the clients page did not match. (38414)

When using WebView to monitor the network and viewing more than 50 users, you could not click Next or Last. (38303)

The 802.1p QoS bits were not being properly set by the AP for traffic sent to the WSS. (37917)

The 'radio' value was missing from the 'ap/radio' field in the show sessions command. (37758, 37495)

Traces show MAC addresses with all 0's because the encapsulation buffer was not replicated when a packet was replicated, so tunnel encapsulated packets with no tunnel header were flooding the network.(38381)

With port-groups enabled or disabled, network traffic was looping on the network. (38247)

No broadcast flags were advertised on the network and certain clients could not communicate to each other on the same AP. (38114)

When configuring the Web portal and saving the default login page, remove everything between the quotes in the Action value.(38010)

To use PKCS#7 certificates on an WSS, you must enter the CERTIFICATE header for PKCS7 PEM formatted certificates.(37995)

ERROR AP 2 network: IP Checksum Error was occuring on the network when mesh services was enabled. (36650)

An invalid configuration file caused the WSS to become unresponsive and lose the core configuration. (36621)

CPU on the WSS spiked to 100% usage at a certain time of the day. (33320)

CPU utilization spikes on RBT systems were observed when 'rogue detection' polling is enabled. (32985)

An WSS stopped functioning when the session was terminated due to a corrupted data structure. (32340)

Problems getting DAPs to boot in an L3 environment using option 43. (32231)

Corrupt packets from an AP can cause the AP manage code inside netsys to crash. (32152)

It is possible that, even though the SODA agent has been downloaded and the virtual desktop started,

the browser is redirected to the login page. This could happen if the session was re-established after the SODA agent download. If this happens, exit out of the Virtual Desktop, open the browser and authenticate again. (25754)

An exception occurred when a DAP configured for 802.11a attempted to tune to a 802.11b radio channel. (37896)

Phantom DAP 0 entries showed up in the show dap connection and global commands.(37561)

On an WSS, static IP addresses had higher priority than IP addresses obtained through DHCP. (37326)

An invalid read operation caused the AP to cease responding. (37017)

Users are placed on the wrong VLAN after roaming to a different SSID.(36910)

The new D-Link DWA-642 pre-N adapter was not able to connect to the wireless network. (36694)

Client MAC address was not flushed from the forwarding database (FDB) after the DAP was disconnected. (36460)

DHCP renewal time of DAP was incorrect. (36336)

Multicast traffic was received from a source client, forwarded from an AP to an WSS but never forwarded back to the same AP. Other wireless clients associated to that AP cannot see the traffic.(36286)

An invalid configuration caused the WSS to cease responding. (36261)

STP was not working correctly when an WSS was connected to another WSS via tagged ports. (36072)

After upgrading to WSS 4.1.x, the user cannot enable 802.11a on a AP-252. (35973)

WebAAA tunneling a user to a VLAN on another WSS caused the WSS to cease responding. (35682)

The AP is broadcasting a DHCP REQUEST with every IP address renewal, thus, enabling another DHCP server to send a DHCP NAK which reboots the AP. (35632)

Unexpected errors occurred when a too long or too short packet is transmitted. (35614)

If an AP is powered using DC power, it will not re-establish an Ethernet link after the device it is plugged into is rebooted. (35472)

A DAP with clients on a low bias switch should not automatically move back to the high bias switch when available. (35143)

Rebooting the WSS via CLI command 'reset system' does not generate a 'warm start' trap on system reboot. Instead a 'cold start' trap is sent. (35357)

After executing the show session command, the WSS ceased to function. (35356)

A basic wireless frame header was not updating after decryption. (35321)

After a certain threshold of sessions on a very active VLAN, some users could not obtain IP addresses using DHCP.(35290)

If the sensor image has been downloaded at least once to a DAP since switch boot, a new version is not used by the switch until after reboot. (35084)

Cannot configure and enable a AP-620 in EMEA countries other than Netherlands. (34961)

A very high rate of error messages caused the WSS to become unresponsive. (34077)

A gno-broadcasth flag was applied to broadcasts sent on the wired network. (34470)

WSS was sending IGMP Membership Queries to the wired network when IGMP was disabled. (34429)

The config cores and WPA2 is configured on 2211 handset and does not work when the auto dap feature is enabled. (34436)

When attempting to boot 120 distributed APs, the WSS becomes unstable and causes an error message to be displayed. (34337)

Too many TCP connections caused the packet memory to degrade over time. (34231)

A MAC client needs to manually renew IP address when using DHCP restrict option. (34183)

Fast roaming between APs was not working. The key cache was not referenced by clients and, therefore the pmkid generated was incorrect and never matched any of the pmkids sent by the clients.(34077)

An WSS is unresponsive to telnet/http connections, and a ping command initiated from the WSS CLI fails with an "unable to allocate socket" error. (33881)

You have to reset the WSS to change the System IP Address and generate new Trap PDUs from this address. (33713)

A corrupt EAP instance causes an WSS to become unresponsive and must be rebooted. (33515)

Flooding of unknown destination unicasts to DAPs on the same VLAN seemed cause network problems. There was an issue where TAPA packets from one WSS to one of its DAPs were flooded to another WSS which then encapsulated the packet in another packet TAPA header and flooded it out to the rest of the DAPs. (33228)

Custom Web-AAA pages that worked in Release 4.0 and 4.1 no longer function in release 5.0. (34181)

When booting 120 DAPs, most APs are timing out when ~80Mbps of aggregate traffic is injected.

(34171, 34168)

Issues resolved in version 5.0.9.4

CPU on the WSS spiked to 100% usage at a certain time of the day. (33320)

Description The SSH CLI response became sluggish, and new sessions were difficult to establish causing the DAPs to reboot.

A core dump file caused by unknown reasons was located on a WSS. (32526)

Description Unspecified network events created a core dump file.

The auto blacklist counter in show rfdetect counters seems incorrect. (32510)

Description A configured blacklist client should not be counted for the automatic blacklist counter.

If a DNS query name is too long, it caused the WSS to stop functioning. (32418)

Description Two WSSs stopped functioning and user traffic ceased to flow when a DNS query name was used that had too many characters.

A WSS stopped functioning when the session was terminated due to a corrupted data structure. (32340)

Description The RADIUS server did not responding to access requests within the configured timeout period which triggers re-transmissions of requests. Or, the response (or responses) were received at the WSS after stations have moved to another AP or to another WSS.

The WSS sometimes reports that the CPU is idle more than 100% of the time. (32331)

Problems getting DAPs to boot in an L3 environment using option 43. (32231)

Description It appears that the comma character that designated the option 44 portion of the DHCP lease (ASCII character associated with 44 is the comma) caused the AP to interpret the option 44 data as continuing option 43 data. Since the format of the option 43 data now appeared to be invalid, the AP rejects the lease.

After configuring a DAP with a static IP number and then configuring it as a directly attached port, moving it back to a DAP port causes the DAP to become unresponsive. (31965)

Remediation ACL does not work if client's browser has proxy enabled. (26478)

Description A client whose browser has web proxy enabled was able to access the network despite failing the host integrity check.

The WSS produced a core file and restarted when a Web Portal session was cleared after the SODA agent was downloaded by the client. (28356)

When multiple ACLs were exercised at once, messages indicating an illegal memory access error appeared in the system log. (30943, 30560)

Invalid port or channel numbers reported from an AP resulted in a crash of the WSS. (31007)

Clearing an AP caused WSS Software to access an invalid memory location, resulting in a crash of the WSS. (31008)

Creating a policy in WMS caused Web-based AAA-related settings for a WSS to be overwritten. (31402)

An invalid access to a location in the EAP module caused the WSS to restart. (31808)

Enabling a DAP to use a WSS as its boot device caused the WSS to crash. (31993)

Corrupt packets generated by an AP caused the APs management software to crash. (32152)

An error message was displayed when attempting to read a value in the Avaya-AP-STATUS-MIB::nrtlApStatNumAps object. (32159)

APs deassociated from a WSS, at which time the WSS restarted and produced a core file. After the WSS restarted, it registered high CPU usage, and the APs could not associate with the WSS. (29110)

WSS crashed as a result of EAPOL deleting information cached by the RADIUS client to handle outstanding authentication requests. (29518)

The ID of the final EAP success message was incorrectly being incremented by 1 over the last EAP conversation. (29556)

2350 stays in boot loop following software upgrade. (29677)

Description After a new software image was loaded on an 2350, and the new image was set as the active boot partition, when the 2350 was restarted, it entered a loop in which it constantly rebooted. The boot prompt was not accessible while the 2350 was in this loop.

Authentication packets sent from the WSS's IP interface were being fragmented into segments larger than was allowable by remote routers. (29843)

When summertime was set to Eur-S, GMT was displayed as time zone. (30126)

Description Specifying a non-alphanumeric character (for example, a hyphen) as part of the time zone in the **set summertime** command was accepted by the CLI, but the time zone for the WSS was then set to GMT.

SNMP traps generated as a result of errors from a wireless client were reported as coming from "Radio 0", which is an invalid radio number for an AP. (30419)

The WSS crashed when accessing an invalid port number in the virtual port table. (30446)

WSSs created unicast "loop" when upgraded to 4.2. (30880)

Description A WSS that had been upgraded to a 4.2 release encountered a DHCP packet whose destination was not defined in its FDB. As a result, the WSS flooded the DHCP packet out all interfaces. When the DHCP packet reached another WSS also running a 4.2 release, it was similarly flooded out all interfaces. This caused a forwarding loop between the two WSSs.

Retrieving an invalid model name from an AP in a mobility domain was causing a WSS to crash and not reboot. (30928)

The WSS crashed when it encountered a packet with an invalid TAPA File Transfer packet type. (31154)

Description The WSS now logs an error message when this event occurs instead of restarting and producing a core file.

The WSS core dumps when an 802.1x client attempts to authenticate to a third-party AP. (33470)

Description The client associates and attempts to authenticate to a third-party AP. The WSS proxies the request to the RADIUS server. The RADIUS server sends an "Accept" message. The WSS core dumps and resets.

The following messages are displayed on the console. IP communication is completely lost (telnet, syslog) and you are unable to extract any debugs or traces from the WSS:

Example 1:

supervisor: 7526.894063 ERROR: process_sigchld: process netsys exited pid=823322 status=0x8b (0/139)

TELNET Oct 19 14:24:43.838097 ERROR TELNET_ERROR: can't accept the session, errno -3 supervisor: 7527.150328 ERROR: process_sigchld: process netsys. 823322 **core dumped**

Example 2:

No more recordssupervisor: 7899.107253 ERROR: process_sigchld: process netsys exited pid=913434 status=0x8b (0/139)

TELNET Oct 19 14:30:56.048672 ERROR TELNET_ERROR: can't accept the session, errno -3 supervisor: 7899.196630 ERROR: process_sigchld: process netsys. 913434 **core dumped**

WSS fails to recognize a broadcast deauthentication attack. Attached clients are deauthenticated by the attack. (28537)

AP will not reboot if it is changed from Directly Connected AP to DAP after booting. (32247)

Description If an AP was connected previously as Directly Connected and then reconnected as DAP it will not boot.

When "last-resort accounting" is configured using WMS it cannot be deleted using CLI. (33438)

Using CLI on the 2360 and executing the "show port mirror" command on port 8 of the switch does not show the settings. (33536)

DAPs could be disconnected from a WSS 2360, if the switch had been running at a very high bit rate >180Mbps for an extended period of time. (33643)

Workaround Reset the 2360

The command "set dap auto model (null) radiotype 11g" appears when executing the "set auto-dap" command using WMS. (33680)

Customized Web-based AAA pages from 4.0 and 4.1 configuration do not work properly in 5.0.9. (33708)

Description Customized Web-based AAA pages that worked in Release 4.0 and 4.1 no longer function in release 5.0.9. When enabled in 5.0.9 the client session is not captured and the client receives an HTTP 404 error message in the browser.

Quality of Service (QoS) Tx/Rx counters do not work properly. Using the CLI command *show ap qos-stat* shows incorrect information. (33971)

WSS logs show excessive "Recv Seq Cntr Failures" log entries. (33977)

The end user is able to see more CLI test commands than are supported for use on the switch. (34022)

Description Executing the "test simulate" command can cause the WSS to crash.

Workaround Do not use the "test simulate <device> operations" command.

Issues resolved since version 4.1.13

Web View did not require a username. (16799)

Web View did not display more than 32 service profiles. (18374)

Web View allowed configuration of duplicate SSID names in the same service profile. (18375)

Layer 2 traffic restrictions did not affect client-to-client traffic on the remote switch of a tunneled VLAN. (21700, 27117)

WSS Software could serve a login unsuccessful page to a Web-Portal client who had successfully logged on. (22881)

A successfully authenticated Web-Portal client could be redirected to a seemingly random web page. (22886)

The WSS crashed periodically in configurations where Web-based AAA Accounting was enabled. (24325)

Putty versions older than 0.58 and Tera Term Pro version 3.1 each reported fatal errors when SSH connection to a WSS was attempted. (24833)

In a service profile with WEP enabled, if a client was encrypting packets with key index 1, and the WSS had the same value configured for key index 2 (not key index 1), then the WSS was decrypting packets from the client using key index 2 and passing them on to the wired network. (24913)

WSS Software upgrades that included an upgrade to the AP boot loader could take a long time. (25229)

On a 2360/2361, internal buffers were occasionally not being freed, causing sporadic packet loss. (25394)

AP error message appeared too frequently in system log. (26007)

Description Error messages such as the following could occur too frequently in the log for similar but distinct errors:

AP Jan 09 09:33:52.577041 ERROR SYSLOG_DUP: last message repeated 1 time.
AP Jan 09 09:33:52.559474 ERROR DAP 80 ap_network: ip_fragment: fail, do clean up

Description In the current version, different messages are displayed depending on the error.

Distributed APs could restart around every two hours after running normally for 3 to 7 days. (26027)

VLAN ports on port group between WSS and Cisco device could be marked down on Cisco device even though the ports were up. (26047)

The Auto Tune function was setting the channel and power settings for an AP radio to values that were not permissible for the US country code (26146)

Invalid OID BER encoding packet sent to switch caused SNMP process to lockup, requiring a switch restart to restart SNMP. (26173)

RADIUS accounting could not be used for billing Web-Portal sessions. (26175)

Receiving an EAP packet 1750 bytes long or longer cause aWSS to restart. (26597)

CLI did not clearly indicate that STP was disabled on a port. (26668)

Corrupted EAP packet from a client could cause a WSS to restart. (26744)

Reconfiguring a wired authentication port as a network port in a tagged VLAN causes the switch to restart if the port is enabled. (27164)

> **Description** If you reconfigured a port from a wired authentication port to a network port in a tagged VLAN, without disabling the port before adding it the VLAN, the switch restarted.

Latency of 1 to 2 seconds occurred when a Vocera badge roamed, if the filter-id attribute was set for the badge (last-resort user). (27330)

An AP directly connected to a WSS on both the AP's Ethernet ports restarted if it received an ARP request on both ports. (27531)

Some PDA devices did not work with WPA using the Windows Mobile 5.0 supplicant. (27570)

Static WEP decryption errors were encountered on a WSS, apparently leading to loss of connectivity for some clients. (27593)

On a 2380, an ACL applied to the outbound direction of a virtual port (port plus tag value) did not take effect. (27656)

Distributed APs converted from Auto-DAPs into statically configured APs were always assigned to the default radio profile, even if another profile had been selected for them. (27692)

Empty identity response from a client could case a WSS to restart. (27999)

Transmission PM value was incorrectly set following CCMP keying. (28018)

Starting a Zebra wireless 802.11 printer could cause a WSS to restart. (28080)

SpectraLink handsets configured with static IP addresses took a long time to connect to a WPA2 SSID. (28268)

Intel 3945ABG wireless NICs could not connect to Avaya radios, or could not use the network once connected. (28863)