Avaya WLAN – Management Software 2300 Series Release Notes – Software Release 7.1.5.2

Avaya WLAN 2300

7.1.5.2

Document Status: **Standard**

Document Number: **NN47250-401**

Document Version: **05.03**

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

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 7.0.8.3

COUNTRY	GENERAL CHANGES
Global	- Created two new AP model domains (2332A-E1 and 2332A-E2) to enable compliance with the new DFS (Dynamic Frequency Selection) requirements that go into effect on April 1, 2009. As of April 1, 2009, WLAN equipment operating in the 5250 - 5350 and 5470 - 5725 MHz bands must be compliant to ETSI standard EN 301-893 v1.4.1 by having the ability to detect meteorological radars operating in these bands. As of April 1, 2009, the requirement to detect staggered or interleaved PRFs is extended to the bands 5250 - 5350 MHz and 5470 - 5725 MHz. As of the same date, equipment transmitting in the 5600 - 5650 MHz frequency bands must also be able to detect pulse widths down to 0.8 µs.
COUNTRY	**CALA**
Guadaloupe	- Added country to AP Model 2332-E1. It follows the EU rules and is governed as a French territory.
Martinique	- Added country to AP Model 2332-E1. It follows the EU rules and is governed as a French territory.
Nicaragua	- Added country to AP Model 2332-E3. It follows the EU & FCC rules. No DFS required.
COUNTRY	**EU & Europe**
2332A-E1	- This new model is required to be installed and operated in the following countries after April 1, 2009: AUSTRIA, BELGIUM, BULGARIA, CYPRUS, CZECH REPUBLIC, DENMARK, ESTONIA, FINLAND, FRANCE, GERMANY, GREECE, HUNGARY, IRELAND, ITALY, LATVIA, LITHUANIA, LUXEMBOURG, MALTA, NETHERLANDS, POLAND, PORTUGAL, ROMANIA, SLOVAKIA (Slovak Republic), SLOVENIA, SPAIN, SWEDEN, UNITED KINGDOM, ICELAND, LICHTENSTEIN, NORWAY, SWITZERLAND, ANDORRA, PRINCIPALITY OF, BOSNIA & HERZEGOVINA, CROATIA, GIBRALTAR, GREENLAND, MACEDONIA (FYR), MONACO, PRINCIPALITY OF, MONTENEGRO, SAN MARINO, REPUBLIC OF, SERBIA, VATICAN CITY STATE (HOLY SEE), REUNION, CURACAO, GUADELOUPE, MARTINIQUE
2332A-E2	This new model is required to be installed and operated in the following countries after April 1, 2009: TURKEY
Andorra, Principality of	- Added country to AP Model 2332-E1. It follows the EU rules. DFS is enabled in 5.25 & 5.47 GHz bands.
Bosnia & Herzegovina	- Added country to AP Model 2332-E1. It follows the EU rules. DFS is enabled in 5.25 & 5.47 GHz bands.

Gibraltar	- Added country to AP Model 2332-E1. It follows the EU rules. DFS is enabled in 5.25 & 5.47 GHz bands.
Greenland	- Added country to AP Model 2332-E1. It follows the EU rules. DFS is enabled in 5.25 & 5.47 GHz bands. 2.4 GHz band only allowed from 2450 - 2483.5 MHz (CHs 10 -13)
Monaco, Prinicipality of	- Added country to AP Model 2332-E1. It follows the EU rules. DFS is enabled in 5.25 & 5.47 GHz bands.
San Marino	- Added country to AP Model 2332-E1. It follows the EU rules. DFS is enabled in 5.25 & 5.47 GHz bands.
Vatican City State (Holy See)	- Added country to AP Model 2332-E1. It follows the EU rules. DFS is enabled in 5.25 & 5.47 GHz bands.
COUNTRY	**MIDDLE EAST & AFRICA**
Algeria	- Added country to AP Model 2332-E1. Follows rules similar to the EU rules. DFS is enabled in the 5.25 & 5.47 GHz band.
Reunion	- Added country to AP Model 2332-E1. It follows the EU rules. DFS is enabled in 5.25 & 5.47 GHz bands.
Tunisia	- Added country to AP Model 2332-E9. 2.4 GHz operation is limited to 10 dBm output power. No external antenna support for antenna models 24883, 24113, 24123 & 24143 and no outdoor operation is allowed.

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
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

For more information on the ‘Regulatory Information”, go to 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 – Management Software 2300 Series Release Notes – Software Release 7.1.5.2

Avaya recommends that you familiarize yourself with these release notes and the *Avaya WLAN Management Software 2300 Series User Guide* and *Avaya WLAN Management Software 2300 Series Reference Manual* before installation. For additional product information, refer to the following documents:

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

What's new in WMS version 7.1

WLAN Management System version 7.1 has the following enhancements:

- Access Control and Grouping
- WMS Audit Trail
- New Enhanced Reports including PCI Compliance Report
- WMS 7.1 Scaling (APs and Sessions)

Version compatibility

- This version of WMS has been verified against WSS Software Version 7.1.
- Network plans created with WMS 6.0, 6.1, 6.2, and 6.3 are compatible with this version of WMS. If you want to use network plans created with previous versions of WMS, make sure the option to delete the network plans directory is not checked when you uninstall.
- If you are installing for the first time, you will need to install and activate licenses before using WMS. If you are upgrading from a previous licensed version, you do not need to reinstall your licences.
- If you are upgrading from a version earlier than 6.0, Avaya recommends that you upgrade to 6.0 first, then upgrade from 6.0 to 7.0 and then to 7.1.

Supported platforms

- Microsoft Windows Server 2003, Microsoft Windows XP with Service Pack 1 or higher, Microsoft Windows 2000 with Service Pack 4, Microsoft Windows 2008, or Microsoft Vista Enterprise.
- SUSE Linux 10.2 and Red Hat WS ES5

Note. You must use the English version of the operating system you select. Operating system versions in other languages are not supported with WMS.

- Apple MacOS Version 10.4.x. with Java 1.5

VoIP devices vendor support

These are the Avaya supported options:

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

Upgrading from WMS version 6.0 to 7.1

You can install the new version of WMS on top of the previously installed one. You do not need to uninstall the previous version

Note. You must upgrade to 7.0 before upgrading to 7.1 if you are currently using a pre-7.0 version of the application

.

Note. Upgrading the WSS from 5.0 to 6.0 will convert from the “dap” to an “ap” configuration.
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)**.

For more information on "DAP to AP conversion during Upgrade from Release 5.0 to 6.0”, refer “*Avaya WLAN - Security Switch 2300 Series Release Notes – Software Release 6.0*”.

Upgrading from WMS version 4.0 or 4.1

If you are upgrading from WMS Version 4.0 or 4.1 and you have network plans created or saved in the version you are upgrading from, Avaya recommends that you archive the config-db directory (if 4.1 or 4.0) before you install the upgrade.

To install the upgrade:

1. Make an archive copy of the config-db directory.
2. Run install.exe (Windows) or install.bin (Linux).
3. The first time you run WMS, if you upgraded from 4.0, it might ask you what to do with the old network plans.
   - If WMS Version 6.0 has already been installed on another client, and the option to copy the network plans to the server was selected, then do not select the option to copy the plans to the server.

     Likewise, do not select the option to copy the plans to the server, if the plans have already been copied to the server manually.
   - If this is the first installation of WMS Version 6.0, then select the option to copy the plans to the server.

Downgrading to a previous WMS version

If you need to downgrade from a WMS 7.1.x version to a previous 7.0.*x* version, use the following procedure:

1. Back up the network plans, by copying the config-db directory to a location that is not in the WMS installation path.
2. Back up the services-db directory by copying it to a location that is not in the WMS installation path.
3. Uninstall the current WMS installation. Select to delete all but the license and the network plans.
4. Install the earlier WMS software version.
5. After installation, copy the folders in the backed up config-db directory to the one that is created by the installation in step 4.
6. After installation, copy the folders in the backed up services-db directory to the one that is created by the installation in step 4.

When you start the downgrade version of WMS, it opens the Default network plan.

If you need to downgrade the WSSs managed by WMS, you can do so before or after the WMS downgrade.

Note. Avaya recommends that you do not downgrade to previous WMS versions. Database files saved in WMS Version 7.1 cannot be used in earlier WMS Versions. In addition, WSS Software features that are new in WSS Software Version 7.1 are not supported in previous versions of WMS.

JRE 1.6 and WMS Java Web Start Client

If you are using Java Runtime Environment (JRE) 1.6.0_12 when trying to remotely connect to a server with WMS software, you may experience issues with the Java WebStart client failing to start due to the following Java bug:

http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=6522222.

http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=6808031

This issue potentially affects remote clients on all operating system with JRE 1.6.0_12 or higher. When starting the Java WebStart client from the desktop icon, an error message is displayed:

"Unable to start application" and a set of Java exceptions are thrown.

Customers that encounter this issue must downgrade the Java environment by uninstalling the JRE 1.6.0_12 and creating a fresh install of JRE 1.6.0_11. If you do not want to downgrade your JRE installation, you can click on the WMS icon on the WMS server page to launch the client.

Known issues

When using the WMS client to view Monitoring and then selecting a mesh AP, WMS does not respond to the request. (65991)

Workaround To resolve this issue, upgrade to the latest WMS release.

WMS does not import rotated text on a CAD drawing. (64663)

Description If text is rotated 90 degrees from horizontal, the text does not import with the CAD drawing. This appears to be a limitation with the CAD application and not WMS.

Workaround Select the text layer in the CAD drawing and rotate it so the text appears horizontally on the drawing.

A radio profile that requires CAC for voice traffic cannot be configured in WMS. (62885)

Description Starting in 7.0 WSS, you can configure a radio-profile with CAC which is used to configure WMM admission control. These settings are configured in the CLI with the set radio-profile profile cac commands but there are no options available in WMS. If you make network changes on the WSS, WMS does flag the changes but does not display the changes.

Workaround Configure CAC using WSS and accept the changes in WMS.

Enabling AAA access to a WSS using WMS and downgrading to 7.0 or earlier causes the authentication process to fail, and WMS can no longer access the WSS.

Description After upgrading to WMS 7.1 and enabling AAA for access to a WSS, if you downgrade to WSS 7.0 or earlier on the WSS, the WSS reverts to the enable password and WMS cannot access the WSS using AAA.

Workaround Disable the AAA feature in WMS before downgrading to an earlier software version.

MP licensing is not updating based on the number of MPs in the network. (61050)

Description If the serial number of an AP is changed, the change is not reflected in WMS and the serial number is deprecated from the license.

Workaround Restart the WMS server to reset the licensing.

Because of a limitation in Windows XP that allows no more than 10 half-open connections, running WMS services on Windows XP is not recommended if your network plan contains more than 10 devices. If 10 devices in your network plan were unreachable or not responding, Windows XP would exceed its half-open connection limit, and connection attempts to reachable devices might time out as a result.

Workaround If your network plan contains more than 10 devices, and you want to run WMS services on a Windows system, use a server OS, such as Windows 2000 or Windows 2003, instead of Windows XP.

Linux: The default browser is Firefox, which is not included with SuSE. (30491)

Description On SuSE, the default browser executable is Firefox. However, the Firefox browser is not included with the SuSE distribution; only the Konqueror browser is included. The Konqueror browser is not supported by WMS.

Workaround Install a different browser for accessing WMS online help. Preferred browsers for Linux are Firefox, Opera, Mozilla, and Netscape.

Daylight Savings Time or timezone changes are not automatically detected in WMS. (18422)

Description If a Daylight Savings Time or timezone change occurs on the host machine where WMS is running, displayed timestamps are not automatically updated in WMS.

This issue is actually a Java Virtual Machine (JVM) issue. The JVM does not detect date or time changes made at the OS level. See the following Web page:

bugs.sun.com/bugdatabase/view_bug.do?bug_id=4216582

Workaround Exit and restart WMS to place a date or time change made on the host machine that is running WMS into effect.

No Changes are returned when changing the order of dot1x authentication. (64609)

Incorrect time displayed in the monitor and reports areas (+5 hours). (64566)

"Find Clients" screen constantly expands groupings that the user has collapsed. (62959)

Issues Resolved Since Version 7.1.4.1

When switching plans in RingMaster, an error message was incorrectly displayed. (66096, 65705)

The "Clients by Time" report continuously reported 0 clients. (65241)

Issues Resolved Since Version 7.1.3.2

When configuring the SMTP server for e-mail notification, using a custom server setting caused the e-mail service to fail. (64492)

The RF Planning wizard did not display WSS option correctly for a Direct AP configuration. (64396)

Clicking Show Mesh Links did not display all of the connected links. (64328)

WSSs in a cluster configuration were not displayed in the Work Order report. (63233)

Enabling fault notification e-mail consolidation caused e-mail notification to fail on WMS. (61343)

Issues resolved since WMS version 7.0.8.3

APs disappeared from the network plan after enabling or disabling the cluster feature on a Mobility Domain. (59997,59784)

Accepting network changes for APs on two or more WSSs simultaneously corrupted the network plan. (59442)

The RM-200 was sending Alarm e-mails without the Fully Qualified Domain Name (FQDN). (60220)

Exporting client statistics was not working for any user sessions. (59655)

Antenna location did not update properly when changes were made to the AP configuration. (59623)

Client Load Report did not generate accurate information about the network. (59518)

The SSID list did not appear when using the MAC Network Access Wizard on a secondary seed WSS. (59465)

The RF Planning feature was missing the object, wiring closet, as part of the list of available objects to add to a plan. (59386)

All configured ACLs did not appear in the secondary seed configuration when using RingMaster. (59112)

Network changes did not synchronize properly in WMS. (59109)

The Monitor status did not match the data in the Client Load per AP report. (58441)

802.11n clients did not display properly in the Operational Rate report. (57952)

Upgrading from WMS 6.0.x to WMS 7.0.x caused the RADIUS server deadtime value to change from 5 to 0 which appears as a network change in WMS. (56185)

Issues resolved since WMS Version 7.0.7.3

Accepting autotune changes caused the WMS client to become unresponsive. (59046)

The Severity" of "Server Performance Alarm" was incorrectly displayed as a single alarm. (58767)

A VLAN name was randomly reset to an empty string for service profiles, MAC users, MAC user groups, named users, or named user groups. (58429)

Webview sessions were not released or timed out if the logout option was not used to close the session. (57417)

Issues resolved since WMS Version 7.0.6.7

The port up/down status was not correctly uptdated when the port number was greater than 10. (58173)

The Auto-Image Update feature did not work in WMS Version 7.0.6.7. (57165)

Using the “Save as” option to save network plans with a file size larger than 50 MB did not save the plan. (55694)

WMS incorrectly reports that the enable password for a WSS has changed when it has not. ((57300)

When generating a Customer Service Report, special characters and spaces were not allowed. (57221)

Out of date information caused certain country codes to be unsupported in WMS. (56922)

When using a Mac, the Alarms report would not print from the WMS. (55902)

Issues resolved since WMS Version 7.0.5.2

Some CAD objects were not read properly and required CAD clean-up before importing into WMS. (57318, 55979)

The "Client Errors by Time" chart in the Monitoring view displayed a value of 0, even if client errors occurred. The errors were available in the Alarms views and in the Client Error reports. (53963)

WMS Version 6.2 and higher incorrectly required that MSS be 6.2 or higher to support the MP-422A. The MP-422A is supported in MSS 5.0 and higher. (54133)

WMS did not display graphs on the Network Usage page under Monitoring. (56309)

Evaluation licenses would expire if the clock was changed on the server. (56058)

Placing an AP on a network plan caused WMS to lose data. (56023)

When MAC prefix is enabled, MAC users get the message “AUTHENTICATION PASSED BUT AUTHORIZATION FAILED”. (56013)

The WMS Planning wizard assigned the same channel to all APs on the network. (55980)

Copying and pasting configurations between WSSs did not work. (55900)

Clicking the Cancel button twice caused the transaction to cancel twice instead of one time. This caused an error in the software. (55821)

The country code for Singapore was not accepted by WMS. (55794)

Too many RF obstacles prevented the floor plan from importing into WMS. The recommended number of obstacles per floor is less than 1000. (55655)

After changing the severity of an alarm, WMS did not correctly display the new severity. (55575)

Floor plans did not import correctly into WMS. (54215)

Large floor plans caused WMS to use large amounts of server memory. (42374)

Issues resolved since WMS Version 7.0.4.5

After changing the monitoring settings in WMS, several reports were generated inadvertently. (55494)

message: WMS Services is not configured as an SNMPv1 trap receiver

hints: Create a Notification Target with the WMS services IP Address

Adding the AP fingerprint to a cluster configuration caused the configuration to fail on the network. (54841)

The e-mail "from address" domain that WMS uses to send alarm e-mails did not correctly initialize when the hostname was a domain longer than 2 segments. It used to default to "trapeze" when this occurred. (54688)

After configuring an ACL for a cluster configuration, the change appeared in the system change table rather than the cluster change table. (54614)

When command auditing is disabled, WMS did not automatically remove the related configuration. (54532)

The minor verification alarms "Low RSSI Threshold Alarm" & "Low SNR Threshold Alarm" were disabled by default. They should be enabled manually to help troubleshoot network connectivity issues. (54529)

Access Control Entries could not be deleted from an ACL policy. (54490)

Server group association was not deleted from WMS when clear accounting is entered on CLI. (54470)

When merging configurations in a cluster configuration, the primary seed WSS in a cluster configuration remained in the “executing” state. (54331)

A new feature was added to allow creating backups of monitoring database (services-db) to be an option in automatic and manual backups. (46005)

Issues resolved since WMS version 7.0.3.5

WMS could not add a location policy to an WSS configured in a cluster. (55017)

Using the optimal power feature in WMS did not adjust the transmit power of the APs appropriately. (54802)

When special characters were used in SSIDs, the configuration did not accept them. (54390)

If a configuration was reloaded from the CLI on an WSS, WMS did not detect the changes. (53593)

When restricted monitor users clicked on the "Alarms by Category" or "Alarms by Severity" pie slices or links, fewer alarms are displayed than expected. The user could query the entire database to get the accurate alarms for matching conditions. Reports were not affected by this issue. (53894)

Monitor users with restricted access may occasionally see a full user's view. (53812)

Issues resolved since WMS version 6.0.5.1

The RF Planning tools wizard to "Insert AP Placement Point" occasionally failed to complete with certain APs in some countries. (51062)

Some APs were incorrectly counted twice in the WMS licensing. (49635)

The use of the "Disable auto-tune" task to apply only power settings can cause the WMS client to become unresponsive. (46427)

Issues resolved since WMS Version 6.0.4.6

Upgrading switch models to 6.0 causes ports that support directly connected APs to lose PoE functionality and configured port names. (45914)

The use of the "Disable auto-tune" task to apply only power settings can cause the WMS client to become unresponsive. (46427)

When a redundantly configured AP radio has different radio profile settings on each WSS, the radio profile on any connection may silently change to the profile of the last redundant connection. This could happen while accepting network changes or when loading the plan. (45695)

Some characters in detected SSIDs could not be parsed or displayed correctly. (45477)

A screen refresh done after sorting APs by name removes all sorting. (45430)

Redundant DAPs may show old information in monitoring Status table. (44878)

Alarm notification sent via e-mail could cause the WMS server to cease responding when the mail server fails to send an SMTP response. (44539)

The distribution of certificates to WSSs via WMS could cause the WMS client to become unresponsive. (43820)

Changing radio profiles from x to y in a wireless service profile policy did not work as expected when applied to devices. The device would be configured with both x and y. The expected behavior has been restored. (42691)

If a number of WSS requests fail due to WSSs being unreachable, WMS may fail to synchronize network status and does not respond to a refresh on the Devices panel. This issue is seen when the configuration poll time is very low (1 minute) and a number of operations are issued against WSSs which are in the process of an image upgrade or reboot. (40990)

When new fault data arrives, the alarms table panel updates and forces the view back to the selected row. When updates are sent rapidly it is difficult or impossible to scroll the table. (40294)

The monitoring settings now allow consolidation restriction, which improves averages of some RF Traffic and Trending attributes during the specified hours. (38719)

Windows XP: Running WMS services on Windows XP is not recommended for network plans with more than 10 devices. (32095)

Radio statistics for Auto DAPs are not correct. (21644)

An error level log message is generated when IE requests for favicon.ico (41947)

Issues resolved since WMS Version 5.0.11.3

Modifying a SSID for an 802.1X configuration and saving the changes worked correctly, but did not deploy the new configuration on the network. (36453)

In RF planning, the coverage for APs using omnidirectional antennas was being shown as directional.(31671, 31033)

If you reordered authentication server groups, it did not create a local change that could be deployed.(31421)

Creating a policy caused AAA-related settings for an WSS to be overwritten. (31402)

In the Tasks View dialog, the device name disappeared from the list of entries when sorted. (31374)

Local change resulted in Network change that could not be accepted or undone. (31067)

This issue occured in the following scenario:

1. On an WSS, SNMP is enabled with the security type set to Encrypted and the protocol set to USM (SNMPv3).
2. The WSS is uploaded into WMS.
3. On the WSS, the command to disable USM is entered at the CLI.
4. The resulting network change is accepted in WMS.
5. On the WSS, the configuration is saved, and the WSS is rebooted.
6. After the WSS is rebooted, WMS indicates a network change that USM has been changed from enabled to disabled. However, this change cannot be accepted or undone; clicking Accept or Undo has no effect.

When a client roamed, its reported location was inaccurate. (29795)

License upgrade requires restarting WMS Services. (21342)

Disabled radio on operational AP does not turn red if the AP or WSS becomes unavailable. (18330)

An exception occurred when a last resort user was created in WMS, a last-resort user was created on an WSS using the CLI, and then the network change was deployed to the WSS. (29415)

WMS clients froze when multiple clients requested information at the same time. (29851)

Polling devices immediately after startup made it difficult to connect to the WMS services host.(29854)

Configure and connect a mesh AP to a portal AP accordingly on the a-radio. If "b/g" radio is enabled and "a" radio is disabled for the portal using WMS and the configuration is deployed, the switch console shows a coredump within a few seconds with forwarding processor data transmit errors. However, the switch recovers and is operational. (44272)

A web-portal user authentication works fine and the logout popup window appears. However when you click on "logout", the browser is redirected to an invalid page.(45740)

Some APs in different domains with same signature are reported as rogues in a period of 10 seconds to 3 minutes after "set rfdetect signature enable" command. After some time the APs eventually become "known"(41416).

Issues resolved since WMS Version 5.0.8.1

When the Alarms Panel was open, memory usage increased and caused WMS to become unresponsive. (37995, 35474)

When installing the Linux version of WMS software, the Client option was missing from the installation screen. (37986)

Occasionally in WMS, you could not save backup files. (37845)

Wording for the Autotune Wizard was misleading and confusing. (37829)

Incorrect session displayed for an WSS on the network. (37559)

The error message that occurred when a corrupted plan or monitoring history was displayed was unclear and ambiguous. (37080)

Lowered default severity level for several critical alarms to major or minor. This improves alarm usability by only making the most important service-affecting alarms critical.(36693)

Using a “&” character in a DAP name causes the reporting to fail. (36655)

Removed duplicate alarm that states "DAP with serial number (x) is not reporting a status" when a AP/DAP is down. Only one alarm is displayed now.(36534)

WMS was incorrectly marking WSS & APs as down and creating critical alarms due to incorrect flapping detection. (36098)

Clicking "print" from the "modify user" dialog now prints the plaintext (decrypted) password instead of the ciphertext.(35694)

Pressing the ESC (escape) key will now cancel or close the active dialog box or wizard. (34274)

The floor plan vanishes from Monitor Floor Viewer. (33739)

Solaris: It was not possible to start a browser to activate the Web interface to WMS Services. (30234)

When a client roamed, the reported location was inaccurate. (29795)

Open access rules folder does not appear for an WSS switch that was downgraded from release 5.0 to 4.0 (29790)

MacOS: WMS licenses were becoming invalid after the host running WMS Services is restarted. (29637)

MacOS: WMS services must be started manually. (28305)

Issues resolved in WMS version 5.0

Changes to radio-profile settings were not synchronized across all redundant APs. (31503)

Description Starting in this release, when a user changes the radio profile selection on one AP, WMS attempts to change the radio profile on all of its redundant connections, but if that radio profile does not exist on a redundant AP, it will be left alone (in some cases, this means that the radio-profile will be set to default).

MAC users disappeared from policy. (32072)

Description After creating an AAA policy that included a series of MAC addresses, then deploying the policy to a WSS, if you then restarted WMS, the specified MAC addresses no longer appeared in WMS, but were visible in the configuration on the WSS.

The "no auto-tune data available" message returned by the Disable Auto-Tune wizard was misleading. (32807)

Description When running the Disable Auto-Tune wizard against a WSS with configured DAPs not booted off the WSS (for example, low bias) the progress dialog displays "no auto-tune data available" for each configured DAP not actually booted from the WSS, which could lead users to think there is a problem when none exists.

Attempting to restore backup files larger than 25 Mb caused error messages to be displayed. (33461)

A network plan that included a floor layout with null characters in its layer names could not be imported into WMS**. (33935, 33241)**

Creating an SNMP Notification target caused an error to be displayed. (34101)

Linux: HTML generated in WMS reports incorrectly used uppercase letters to refer to .jpg files that had filenames with all lowercase letters. (34125)

Java errors when starting Web Client. (34138)

Description After installing the Web Client on a client machine, attempting to launch the Web Client displayed a message indicating certain files could not be located. WMS was looking for these files in the location they would be on the WMS server, but they would not necessarily be in that location on the client machine.

A large number of DeviceChange events being unnecessarily generated by the server caused WMS to become unresponsive. (34151)

It was not possible to launch the WMS Web client because the WMS .jar file and third-party .jar files were signed by different certificates. (34196)

Possible memory leak caused WMS services to be non-responsive. (34349)

When WMS was resolving verification rules, and a "Mobility Domain member is missing", verification message was displayed, clicking "Remove Member", caused WMS to crash. (34408)

The dot1X trace function incorrectly generated an error message due to an empty MAC address, and enabling traces using WMS did not cause them to be listed as local changes. (34418)

After creating one Distributed AP from the Alarms panel, an error message was displayed when attempting to create a second Distributed AP. (34446)

After making a configuration change in a network plan, the WMS screen constantly "refreshed", slowing down performance. (34718)

Filtering and sorting alerts for different areas and severities caused WMS to crash. (34752, 34455)

Deploying access rules from WMS to a WSS did not create them on the switch, and deleted access rules that were already on the switch. (34778)

An exception occurred when an access rule was created in WMS, an access rule was created on a WSS using the CLI, and then the network change was accepted by WMS. (29415)

WMS clients froze when multiple clients requested information at the same time. (29851)

Description When two (or more) WMS clients requested information from the WMS services host at the same time, one client retrieved the information, while the other client(s) waited. While waiting, the other client(s) were unable to do anything until the first client was finished with its request.

Polling devices immediately after startup made it difficult to connect to the WMS services host. (29854)

Description In a network plan with a large number (greater than 700) of WSSs, after WMS services finished starting, it attempted to poll all of the WSSs at the same time, causing high CPU usage and making it difficult to connect using the Web interface or a WMS client. In addition, polling all of the devices at once consumed all of the I/O threads, making it impossible for a second WMS client to connect. WMS now waits until the Web server and all services have been initialized before polling devices in the network plan.

Local change resulted in Network change that could not be accepted or undone. (31067)

Description This issue occurred in the following scenario:

1. On a WSS, SNMP is enabled with the security type set to Encrypted and the protocol set to USM (SNMPv3).
2. The WSS is uploaded into WMS.
3. On the WSS, the command to disable USM is entered at the CLI.
4. The resulting network change is accepted in WMS.
5. On the WSS, the configuration is saved, and the WSS is rebooted.
6. After the WSS is rebooted, WMS indicates a network change that USM has been changed from enabled to disabled. However, this change cannot be accepted or undone; clicking Accept or Undo has no effect.

In the Tasks View dialog, the device name disappeared from the list of entries when sorted. (31374)

Description If you displayed information in the Tasks View dialog (by selecting the Devices icon, then the View Operation Log task) the entries are initially sorted according to the Device column. If you then sorted the entries according to a different column, the names of the devices disappeared from the sorted list, making it impossible to sort the entries by device name again.

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

If you reordered authentication server groups, it did not create a local change that could be deployed. (31421)

In RF planning, the coverage for APs using omnidirectional antennas was being shown as directional. (31671, 31033)

The RF Monitor function did not display the correct list of WSSs configured for AP redundancy. (26858)

The RF Monitor function did not display user-defined names for DAPs. (27399)

Applied changes for ACLs in policies only took effect when the ACLs were deleted or created, but not when the ACLs were modified. (29416)

Description When you created an ACL using a policy, then applied the policy to a WSS, the ACL was correctly shown in the WSS's configuration. However, if you subsequently modified the ACL and deployed the changes to the WSS, WMS indicated that the changes deployed correctly, but the ACL changes did not actually appear in the WSS's configuration.

A policy containing Wireless Service Profiles and Radio Profiles could not be applied. (29659)

WMS crashed when saving RF obstacle data for a floor took longer than 15 minutes (29674)

Selecting a single WSS created by the RF Planning function and pressing Ctrl+D did not allow you to delete the WSS. (29676)

In a Network Plan consisting of multiple floors, the WMS Compute and Place function placed APs on the incorrect floor. (29679)

When configuring a Web Portal service profile, in the Authentication Server(s) dialog, the LOCAL option was not available in the Available RADIUS Server Groups list. (29685)

Message "Error: The server is currently unavailable due to critical errors encountered during startup." displayed when starting WMS. (29762)

Description Changing the model type for a switch in a network plan, then restarting the machine running WMS Services, resulted in an error message when you connected to the machine running WMS Services.

Deploying changes to an WSS caused the WSS to produce a core file. (29773)

Creating a Voice service on an Open Access SSID using the Wizard did not create the required Open Network Access Rule. (29785)

RF Detection resolution showed a blank screen. (29787)

Description If you added a MAC address to both the Rogue list and the Ignore list, an error message was displayed (correctly), but when you tried to view the details of the error message under the Verification tab, a blank screen was displayed.

Selecting a large number of WSSs (more than 10) and then accepting network changes for these WSSs took a long time. (29846)

Using certain IP address ranges generated Verification warnings. (29847)

Description If you tried to configure devices in WMS to use Class A IP addresses in a range higher than 126.0.0.0 (191.0.0.0 for Class B, 223.0.0.0 for Class C), WMS indicated that the IP address was not in any standard class (A, B, or C).

Device list data reverts to default sorting order after reviewing changes. (29848)

Description On the Devices Tab, if you clicked on a data column to sort the list of devices according to the data in that column, then clicked on Review to review local or network changes, when you closed the Review Changes dialog, the data in the device list reverted to the default sorting order.

WMS displayed a Warning message indicating an invalid slot number (0) was detected for an AP. (30331)

After clicking Objects to Place option, an Internal Application Error message was displayed. (30344)

The AP Redundancy dialog did not use max. configured AP count. (30553)

Description The Select Bias and Device(s) for Redundancy dialog, used in the Setup AP Redundancy wizard, displayed the number of APs that could be booted by the switch, instead of the maximum that could be configured on the switch.

New AutoCAD formats were not supported by WMS, and opening a floor plan with an unsupported AutoCAD format could cause an exception. (22542)

Attempting to copy and paste a service profile from one WSS to another WSS of a different model caused a Java exception. (25128)

Verification options did not allow changing the Default network plan's country code to match an uploadedWSS's, if the WSS's country code was not *US*. (27048)

WMS did not check for available space on a WSS's nonvolatile storage before attempting to download an image to the switch. (27521)

If you selected the Use System IP Address checkbox in the RADIUS configuration section, WMS did not see it as an available change. (28824)

Configuration parameters of an unmanaged switch that had the same configuration as a managed switch were listed as local configuration changes. (29121)

Access Control List (ACL) Setup Panel disappears when returning to setup panel screen from Device panel (33760)

Workaround Exit the ACL screen by selecting a feature on the Organizer panel (VLANs, QoS, etc.) and then return to the ACL screen.

WMS java client running on Windows XP or Windows Server 2003 reports an internal error of "failed connection to SQL database" (33890)

WMS Web client incorrectly shows switch connection settings as "WSS Connection Settings" it should show "WSS Connection Settings". (33958)

Submitting problem reports

WMS can send problem reports to the Avaya TAC team directly when it encounters a problem. You can also send a problem report at any time by selecting **Help > Report Problem** in WMS.

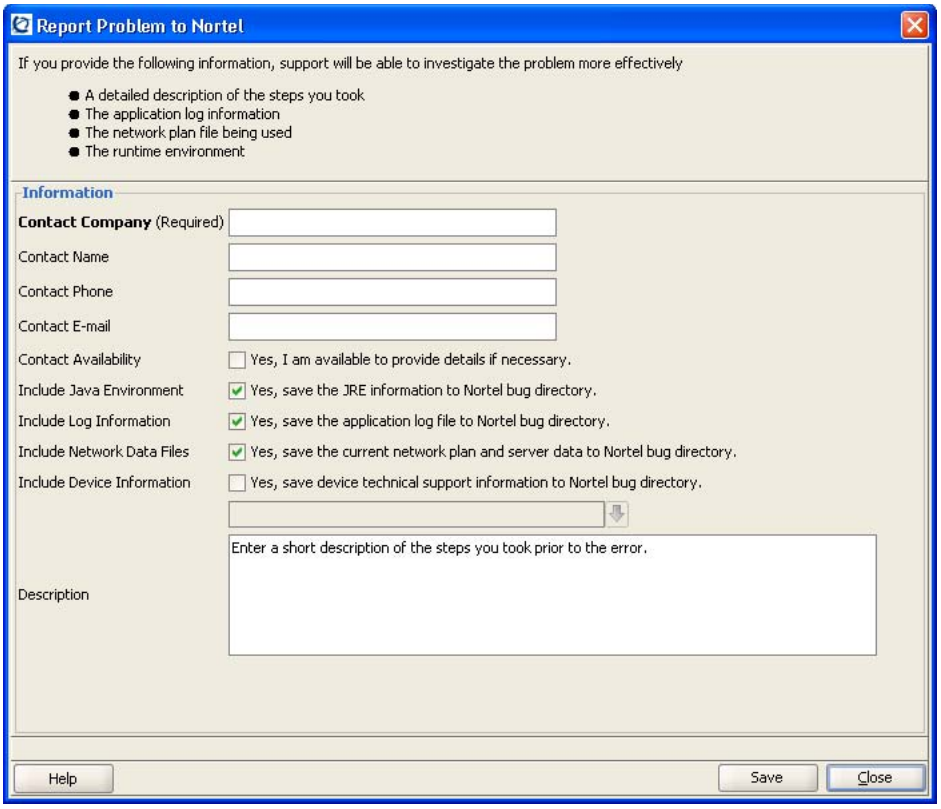
If a problem occurs, the Internal Application Error dialog box appears.

To submit a problem report:

1. Do one of the following:

- In the Internal Application Error dialog box, click **Report Problem**.
- The Report Problem to Avaya dialog box appears.

The Report Problem to Avaya dialog box appears.



2 Fill out the information in the dialog box.

Provide your name, and enter as much detail as possible about the task you were performing when the problem occurred. You must provide the name of your company.

3 Click Send Now.

4 If network access for the email report is not available from the WMS host, click Save to store the problem report on the WMS host.

The problem report is saved as a directory with a name containing the timestamp of the problem report (for example, Thu-Aug-19-13-04-11-PDT-2004). This directory is located in C:\Documents and Settings\user_home_directory\.avaya\bugs, where user_home_directory is the home directory of the user that is running WMS at the time the problem report is generated.

To send the problem report to Avaya, create a zip archive of the problem report directory and send the archive as an attachment to nms-support@Nortel.com.

Documentation Errata

With the release of WMS 7.0, the Import Layout task is no longer supported on the MacOS platform of WMS software. It is still supported on Windows and Linux platforms.