Part No. NN47250-401 (320667-F)
October 2007

4655 Great America Parkway
Santa Clara, CA 95054

Nortel WLAN – Management Software 2300 Series Release Notes – Software Release 6.0

NORTEL

Disclaimer

The network plan generated by the WMS planning tool uses a predictive RF model. This information is an estimate only of the amount, configuration, and placement of WLAN 2300 equipment and is intended to approximate project cost projections.

A Wireless LAN site survey service captures actual RF data to accurately model RF environments and is still the best method to determine correct location of APs, and therefore installation locations of cabling. A WMS network plan is an approximation only and does not substitute for a Wireless LAN site survey.

Contents

How to get help 5

Regulatory information 7
Global changes in Release 6.0 7
Series 2332 Access Points Region Lock Mechanism 9
IEEE 802.11a/b/g Channel Designations: 10
2400 - 2483.5 MHz band 10
5.15 - 5.35 GHz bands 11
5.470 - 5.725 GHz bands 11
5.725 - 5.85 GHz bands 11
Series 2332 Access Points Country to Region Map 12

Nortel WLAN – Management Software 2300 Series Release Notes – Software Release 6.0 15
What's new in WMS release 6.0 15
Support for WSS Software Version 6.0 Enhancements 16
RF Analysis 16
RF Link Testing 16
RF Visualizations 16
Reporting 16
RF Load Balancing 16
Mesh Services 17
Local Switching 17
Wireless Bridging 17
Licensing by Feature 17
Enforceable Beacon Data Rate Control 17
Logout for Web Authentication 17
WSS Seed Redundancy 17
Password Management 17
Nortel WSS 2382 Switch 18
Version compatibility 18
Supported platforms 18
VoIP devices vendor support 18

Upgrading from WMS Version 5.0.8.1 0r 5.0.11.3 19
Upgrading from WMS version 4.0 or 4.1 19
Downgrading to a previous WMS version 19
Issues resolved since WMS Version 5.0.11.3 20
Issues resolved since WMS Version 5.0.8.1 22
Issues resolved in WMS version 5.0 23
Known issues 27
Submitting problem reports 29

How to get help

This section explains how to get help for Nortel products and services.

Getting help from the Nortel web site

The best way to get technical support for Nortel products is from the Nortel Technical Support web site:

http://www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. More specifically, the site enables you to:

- download software, documentation, and product bulletins
- search the Technical Support web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the phone from a Nortel solutions center

If you do not find the information you require on the Nortel Technical Support web site, and you have a Nortel support contract, you can also receive help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following web site to obtain the phone number for your region:

http://www.nortel.com/callus

Getting help from a specialist by using an express routing code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

http://www.nortel.com/erc

Getting help through a Nortel distributor or reseller

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

Regulatory information

Global changes in Release 6.0

WSS/ WMS Global	The following countries are not supported by Nortel: • 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	5.60	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 nortel website: http://www.nortel.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.

Nortel WLAN – Management Software 2300 Series Release Notes – Software Release 6.0

What's new in WMS release 6.0 15
Version compatibility 18
Supported platforms 18
Upgrading from WMS Version 5.0.8.1 0r 5.0.11.3 19
Downgrading to a previous WMS version 19
Issues resolved since WMS Version 5.0.8.1 22
Known issues 27
Submitting problem reports 29

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

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

What's new in WMS release 6.0

Nortel WSS 2382 switch is introduced.

WMS 6.0 has the following enhancements.

- Local Switching Configuration Wizard
- Mesh Services Configuration Wizard
- AP Redundancy Wizard

- Mesh Services Monitoring
- Enhanced Monitoring Capabilities
  - RF Analysis
  - RF Link Testing
  - RF visualizations
  - Reporting
- Enhanced Password Management (FIPS-142 Compliant)

Support for WSS Software Version 6.0 Enhancements

WMS 6.0 supports configuration and management of the following WSS Software enhancements:

- RF Load Balancing
- Mesh Services
- Wireless Bridging
- Licensing by Feature
- Enforceable Beacon Data Rate Control
- Logout for Web Authentication
- WSS Seed Redundancy
- Password Management

RF Analysis

The RF analysis function analyzes key RF statistics and provides alerts based on the statistics.

RF Link Testing

RF Link Test helps you while troubleshooting a wireless client and determining the location of a client.

RF Visualizations

It allows you to find an AP on a floor, when selecting an AP from the Monitoring Equipment tree.

Reporting

Schedule reporting and r-mailing helps you to generate, store, and e-mail reports.

RF Load Balancing

RF load balancing is the ability to reduce network congestion over an area by distributing client sessions across the AP (access points) with overlapping coverage in the area.

Mesh Services

WLAN mesh services allows an AP to provide wireless services to clients, without a wired interface on the AP. Instead of a wired interface, there is a radio link to another AP with a wired interface.

Local Switching

It allows packets to be switched directly from the AP to the wired network.

Wireless Bridging

It allows you to use WLAN mesh services in a wireless bridge configuration, implementing APs as bridge endpoints in a transparent Layer 2 bridge.

Licensing by Feature

Installing license keys allows you to unlock WSS Software features on an as-needed basis.

Enforceable Beacon Data Rate Control

It helps you to completely prevent clients from transmitting at disabled data rates.

Logout for Web Authentication

Configure the Web Portal web-based AAA to allow a user to manually terminate the session. When this feature is enabled, the Web Portal web-based AAA user is successfully authenticated and redirected to the requested page, a window appears behind the user browser. The window has a button labeled “Logout”. When you click Logout, a URL appears and terminates the user session on the Mobility Domain.

WSS Seed Redundancy

on specifying a secondary seed in a Mobility Domain, it provides redundancy for the primary seed switch in the Mobility Domain. If the primary seed becomes unavailable, then the secondary seed assumes the role of the seed switch. This allows the Mobility Domain to continue functioning, if the primary seed becomes unavailable.

Password Management

It has control over handling passwords when users are authenticated on WSS.

For more information on above features see *Nortel WLAN - Security Switch 2300 Series Configuration Guide* and *Nortel WLAN – Management Software 2300 Series Reference Guide.*

Nortel WSS 2382 Switch

The 2382 switch provides high-bandwidth centralized control of many indirectly connected access points. It contains two gigabit Ethernet ports and has two 100-240V VAC autosensing AC power supplies.

Version compatibility

- This version of WMS has been verified against WSS Software Version 6.0.
- Network plans created with WMS 5.0.8.1 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.

  After you install the new software, WMS asks whether the old network plans are to be sent to the server (if you want to keep them) or deleted. If multiple clients are using the same server, then the old network plans need to be copied only once. Nortel recommends that you archive the xml/db directory before you delete any old plans.
- 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. (See "Support for WSS Software Version 6.0 Enhancements" (page 16).)
- If you are upgrading from a version earlier than 4.0, Nortel recommends that you upgrade to 4.0 first, then upgrade from 4.0 to 6.0.

Supported platforms

- Microsoft Windows Server 2003, Microsoft Windows XP with Service Pack 1 or higher, or Microsoft Windows 2000 with Service Pack 4
- SUSE Linux 9.1 and Red Hat WS 3

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

- Sun Solaris 8 and Solaris 9
- Apple MacOS Version 10.4.x.

VoIP devices vendor support

These are the Nortel supported options:

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

Upgrading from WMS Version 5.0.8.1 0r 5.0.11.3

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

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, Nortel 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 6.0 version to a previous 5.0.*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. Uninstall the current WMS installation. Select to delete all but the license and the network plans.
3. Install the earlier WMS software version.
4. After installation, copy the folders in the backed up config-db directory to the one that is created by the installation in step 3.
5. After installation, copy the folders in the backed up services-db directory to the one that is created by the installation in step 3.

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. Nortel recommends that you do not downgrade to previous WMS versions. Database files saved in WMS Version 5.0 cannot be used in earlier WMS Versions. In addition, WSS Software features that are new in WSS Software Version 5.0 are not supported in previous versions of WMS.

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)

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 "Modo 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)

Known issues

WMS has a feature called rflink in 6.0 and WSS has a feature called rfping in 6.0. Both features are the same. (40951)

When a switch was disconnected which was uploaded to WMS for more than 30 minutes , WMS has intermittent issues seeing the switch. (39251)

> **Workaround** Delete the switch and upload again.

WMS could not obtain lock for deployment intermittently. (41841)

> **Workaround** Re-start WMS service.

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

Bogus changes introduced when toggling software version in WMS (41919)

> **Description** The local changes can be seen by toggling the software version settings in WMS though real changes in configuration.

ACE can not be moved up/down in WMS. (41873)

When an image upgrade is performed in WMS for an WSS with pending local changes, the local changes are no longer flagged as changes after the image upgrade completes. Instead network changes are displayed with the reverse information. (41914)

Workaround To solve this, you can undo the network changes, and then deploy the resulting local changes.

A WMS Java Web Start (JWS) client did not work properly on Windows 2003 SP1. You must upgrade the system to SP2 for the client to work properly. (40997)

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)

Workaround To synchronize the WSS with the network, you can un-manage the WSS and then return it to the managed state. After this sequence, the refresh works as expected.

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)

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

Description 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.

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

Description The radio statistics for DAPs that are configured by the Distributed AP profile (Auto-DAP profile) are not correct. However, statistics for statically configured APs (Distributed and directly attached) are correct.

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

Description 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.

Roaming delay is high when SSID encryption is turned on with AP. (39623)

CLI does not have option to select AP 2332-E1. (41897)

Workaround You can use WMS to select 2332-E1.

802.11a radio active scan interval can not be displayed when country code is CN (China). (41876)

Local fallback authentication will not work with PEAP Offload for EAP type. (41868)

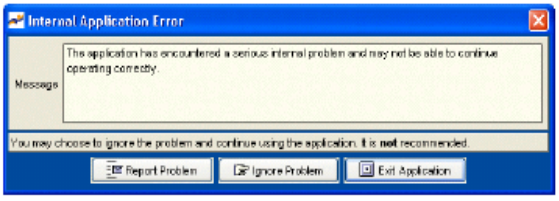
L2 restrict drop counter does not increment for all packets. (41653)

Known Performance issues with Cisco Aironet CB21AG NIC (41105)

Submitting problem reports

WMS can send problem reports to the Nortel 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.

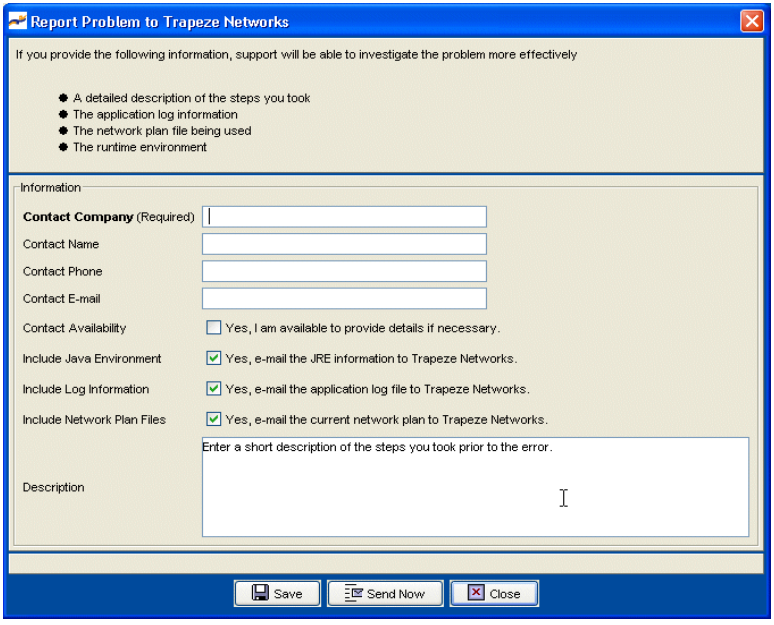


To submit a problem report:

1 Do one of the following:

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

The Report Problem to Nortel 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\.nortel\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 Nortel, create a zip archive of the problem report directory and send the archive as an attachment to nms-support@Nortel.com.

Nortel WLAN – Management System 2300 Series Release Notes – Software Release 6.0

WLAN 2300 Series

Release 6.0

Document Number: **NN47250-401**
Document Status: **Standard**
Document Version: **02.01**
Part Code: **320667-F**
Release Date: **October 2007**

To provide feedback, or to report a problem in this document, go to www.nortel.com/documentfeedback.

NORTEL