Avaya WLAN 8100 Release Notes

1.1.0.0
NN47251-400, 02.03
October 2011

Notice

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

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees 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 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 its Hardware and Software (“Product(s)”). 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://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya 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; 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 materials on this site, the Documentation, Software, or Hardware provided by Avaya. All content on this site, the documentation and the Product 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 unless expressly authorized by Avaya. 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 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 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, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: http://support.avaya.com.

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://support.avaya.com.

Contents

Chapter 1: Avaya WLAN 8100 Documentation Suite 5
Avaya WLAN 8100 documentation packaging 5
Roadmap 6
Product fundamentals 6
Installation and commissioning 6
Upgrades and patches 7
Operations 7
Fault and performance management 8
Chapter 2: New in this Release 9
Chapter 3: Changing WLAN 8100 software 11
Upgrading the WLAN Management System to Release 1.1.0 12
Upgrading the Wireless Controller image 13
Importing policies from the Wireless Controller into the WMS 15
Upgrading the Wireless Controller Diagnostics image to Release 1.1.0 15
Chapter 4: Resolved Issues 17
Chapter 5: Known Issues 23
Appendix A: Downgrading the Wireless Controller 31

Chapter 1: Avaya WLAN 8100 Documentation Suite

This section contains a description of the Avaya WLAN 8100 documentation suite. Refer to this section for an explanation of the documents, their use, and what information they contain.

Avaya WLAN 8100 documentation packaging

Avaya technical publications are organized according to a set of job functions. The following list outlines how the Avaya WLAN 8100 documentation suite is organized.

- Product fundamentals
  - *Avaya WLAN 8100 Regulatory Information (WC 8180)* (NN47251-101)
  - *Avaya WLAN 8100 Fundamentals* (NN47251-102)
  - *Avaya WLAN 8100 Regulatory Information (AP 8120)* (NN47251-104)
  - *Avaya WLAN 8100 WC 8180 CLI Reference* (NN47251-107)
  - *Avaya WLAN 8100 WC 8180 GUI Reference* (NN47251-108)
  - *Avaya WLAN 8100 Regulatory Information (AP 8120 with External Antenna)* (NN47251-109)
  - *Avaya WLAN 8100 Planning and Engineering* (NN47251-200)
- Installation and commissioning
  - *Avaya WLAN 8100 Quick Start Guide* (NN47251-106)
  - *Avaya WLAN 8100 Installation — AP 8120 and AP 8120 with External Antenna* (NN47251-302)
  - *Avaya WLAN 8100 Installation — WC 8180* (NN47251–303)
  - *Avaya WLAN 8100 Installation — SFPs and XFPs* (NN47251–306)
- Upgrades and patches

  Avaya WLAN 8100 Release Notes (NN47251-400)
- Operations

  Avaya WLAN 8100 Configuration (NN47251-305)
- Fault and performance management

  Avaya WLAN 8100 Troubleshooting (NN47251-700)

Roadmap

This section lists and describes the documentation available for the Avaya WLAN 8100 product suite.

Product fundamentals

Product fundamentals documentation includes overview and reference information about the product and product documentation. The following table lists the product fundamentals documents in the Avaya WLAN 8100 documentation suite.

Title	Description
Avaya WLAN 8100 Regulatory Information (WC 8180) (NN47251-101)	This document provides regulatory information for the Avaya WLAN 8100 WLAN Controller 8180.
Avaya WLAN 8100 Fundamentals (NN47251-102)	This document provides an overview of the technologies and products used in the Avaya WLAN 8100 product suite.
Avaya WLAN 8100 Regulatory Information (AP 8120) (NN47251-104)	This document provides regulatory information for the Avaya WLAN 8100 Access Point 8120.
Avaya WLAN 8100 WC 8180 CLI Reference (NN47251-107)	This document provides information and procedures for the configuration and management of the WLAN Controller 8180 using the command line interface (CLI).
Avaya WLAN 8100 WC 8180 GUI Reference (NN47251-108)	This document provides information and procedures for the configuration and management of the WLAN Controller 8180 using the WMS Management Software.
Avaya WLAN 8100 Regulatory Information (AP 8120 with External Antenna) (NN47251-109)	This document provides regulatory information for the Avaya WLAN 8100 AP 8120 with External Antenna
Avaya WLAN 8100 Planning and Engineering (NN47251-200)	This document provides information on network planning and integration.

Installation and commissioning

Installation and commissioning documentation describes the installation of Avaya WLAN 8100 hardware and how to perform initial configuration.

Title	Description
Avaya WLAN 8100 Quick Start Guide (NN47251-106)	This document provides the information and procedures necessary to quickly install the WC 8180 and AP 8120.
Avaya WLAN 8100 Installation - AP 8120 and AP 8120 with External Antenna (NN47251-302)	This document provides information and procedures for the physical installation of the AP 8120 and the AP8120 with External Antenna.
Avaya WLAN 8100 Installation - WC8180 (NN47251-303)	This document provides information and procedures for the physical installation of the WC 8180.
Avaya WLAN 8100 Installation -SPFs and XFPs (NN47251-306)	This document provides installation instructions and technical specifications for small form factor pluggable (SFP) transceivers and 10 gigabit SFP (XFP) transceivers.

Upgrades and patches

Upgrade and patch documentation describes the software upgrade process.

Title	Description
Avaya WLAN 8100 Release Notes (NN47251-400)	This document provides the latest information on the Avaya WLAN 8100 product and documentation suites as well as information on the installation of software upgrades.

Operations

Operations documentation describes the configuration and management of Avaya WLAN 8100 devices.

Title	Description
Avaya WLAN 8100 Configuration (NN47251-305)	This document provides workflows and procedures for the configuration and management of the WLAN Controller 8180 using the command line interface, WMS, and EDM interfaces.

Fault and performance management

Fault and performance management documentation describes fault and performance management techniques.

Title	Description
Avaya WLAN 8100 Troubleshooting (NN47251-700)	This document provides troubleshooting information and procedures for the WLAN Controller 8180 and Access Point 8120.

Chapter 2: New in this Release

The following sections detail what’s new in Avaya Wireless LAN (WLAN) 8100 for Release 1.1. The following list identifies the new features introduced in this release.

Hardware

- 8120 with External Antenna Access Point
- External Antenna for 8120 with External Antenna Access Point – 70 DEG and 180 DEG

Software

- Captive Portal Customization
- Captive Portal Redirect URL
- Captive Portal Interface
- Support for multiple countries per Domain
- AAA Acceleration
- RADIUS Load Balancing
- RADIUS Health check
- Access Point External Image Download
- Maximum User Scaling – 20K
- WLAN Management System (WMS) on VMWare
- WMS/ Site Manager Device (SMD) Changes for External Antennas

Chapter 3: Changing WLAN 8100 software

This chapter contains instructions on changing WLAN 8100 software including upgrading the Wireless LAN Management System (WMS), Wireless Controller, Access Points, and the Wireless Controller Diagnostics images.

Software Image Files Released with Release 1.1.0

Component	File Name	File Size (bytes)
WC8180 Image	wc8180_1.1.0.133s.img	49,513,064
WC8180 Diagnostics	wc8180_1.0.2.0_diag.bin	3,152,332
Access Point External Image	AP8120-Upgrade_1_1_0_133.tar	8,734,720
WMS Windows 32Bit	WLAN8100_WMS_1.1.0.133_Windows_32bit .exe	195,070,151
WMS Windows 64Bit	WLAN8100_WMS_1.1.0.133_Windows_64bit .exe	195,071,771
WMS Linux	WLAN8100_WMS_1.1.0.133_Linux.bin	230,525,556

Important:

You are required to upgrade the WC8180 Diagnostics Image to version 1.0.2.0 after upgrading the WC8180 to version 1.1.0 software.

Important:

You are required to upgrade the WMS to version 1.1.0 to manage WC8180 after upgrading to version 1.1.0 software.

Important:

Avaya recommends all upgrades to be performed in a scheduled maintenance window. The WLAN 8100 Release 1.1.0 supports upgrades from all 1.0.x (including 1.0.0, 1.0.1 and 1.0.2) code streams.

Upgrading the WLAN Management System to Release 1.1.0

About this task

You can use WLAN Management System (WMS) Release 1.1.0 to manage Mobility Domains with Wireless Controllers on Releases 1.0.0, 1.0.1, 1.0.2 and 1.1.0. WMS release 1.1.0 supports Wireless Controller Releases 1.0.0, 1.0.1, 1.0.2 and 1.1.0.

Important:

The WMS Releases 1.0.0, 1.0.1 and 1.0.2 do not support Wireless Controller Release 1.1.0. You are required to upgrade the WMS before upgrading any Wireless Controllers in any of the configured Mobility Domains to 1.1.0

Complete the following procedure to perform to upgrade the WMS to Release 1.1.0.

Procedure

1. **Uninstall the old WMS on the server**

   Important:

   You perform a WMS Backup during the uninstall process. The WMS database that is backed up through the WMS browser Administration section is only supported on the current installation and you cannot use it to restore the configuration after the upgrade.

   a. Launch the WMS Uninstaller, and choose one of the following:

      - In Windows, go to **Start**> **Programs** > **WMS** > **Uninstall WMS**
      - In Linux: **./ /opt/Avaya/WMS/uninstall_WMS/Uninstall WMS**

   b. Backup the WMS Database, Log, SMX, and License.

      Important:

      Choose a **default backup directory path** when you are asked to backup the database, Log, SMX and license. If you choose a different path, **do not** use the **WMS application default paths**: **C:\Program Files\Avaya\WMS** for Windows or **/opt/Avaya/WMS** for Linux. If you use the same location as the default WMS application path, the backup files are removed after the WMS is uninstalled

      The **default backup locations** from the WMS Un-install are as follows:

      - WIN 2008: C:\
      - WIN 2003: In Rel 1.0.x: C:\Documents and Settings\Administrator; In Rel 1.1: C:\

- Linux: /

The sub-directory is created appropriately i.e. C:\Log, C:\smx-repository, C:\Licenses. The SQL Database is placed under C:\

> **Note:**
>
> For Linux Installations, you are required to manually move the License file from the **wms/lsm** directory to a folder outside the WMS directory. The wms/lsm directory is removed during WMS uninstall of Releases 1.0.0, 1.0.1 or 1.0.2 . A manual backup is not required for Windows server deployments.

2. **Install the WMS 1.1.0 on the server**

   Double-click on the WMS executable file and follow the installation steps.

3. **Restore the WMS Database, SMX files, and License**

   During installation, select the Database, SMX files, and License file that you would like to restore when the option is presented.

4. **Verify the WMS Upgrade**

   a. Verify all the domains are visible and can be monitored through the WMS.

   b. Verify that License file is restored. In the WMS browser, the bottom bar should display the number of licenses installed —> Licensed to monitor [xx] APs.

   c. If **Site View** is setup, verify that the SMX files are restored. Click **Monitoring** > **Site Views** > **Site Model**. Highlight the SMX file to be activated, then click **Activate**.

Upgrading the Wireless Controller image

In a multiple controller domain environment, Avaya recommends to upgrade the AMDC , the BMDC, and then the Peer Controllers.

Complete the following procedure to perform an upgrade of the Wireless Controller image.

Procedure

1. **Backup the current configuration (Binary) to the TFTP server or USB drive**

   ```
   WC8180# copy config tftp address <tftp server address>
   filename <config file name to use>
   ```

   OR

   ```
   WC8180# copy config usb filename <config file name to use>
   ```

2. **Backup the ASCII configuration to the TFTP server or USB drive**

The ASCII configuration is required if the current configuration has to be restored on a the WC controller running version 1.1.0. The Binary configuration saved with Releases 1.0.0, 1.0.1 or 1.0.2 versions are not compatible with version 1.1.0.

```
WC8180# copy running-config tftp address <tftp server
address> filename <config file name to use>
```

OR

```
WC8180# copy running-config usb filename <config file name to
use>
```

3. **Download the 1.1.0 image to the Wireless Controller**

   ```
   WC8180# download address <tftp server address> secondary
   image <file name>
   ```

   The image download begins followed by Saving the Image to the system.

   The previous primary image is moved to secondary image and the new image is set as the primary image.

   The Wireless Controller resets after the image download is complete.

   If you use the no-reset option, the Wireless Controller will not reset to the new image.

   The total Download and Saving process can take about 15 to 20 minutes depending on the TFTP server and network.

4. **If you used the no-reset option during Step 3, reset the Controller to upgrade to the new image**

   `WC8180#show boot image` — Verify the new image is set to primary.

   ```
   WC8180# boot primary
   ```

   The Controller upgrades to the new image.

5. **Repeat Steps 1 to 4 for all the Wireless Controllers in the Mobility Domain**

6. **Verify that the Wireless Controller Image update is successful.**

   a. Verify Controller booted with the correct Image

      `WC8180# show sys-info` > Verify that the software version is correct.

   b. Verify the wireless functionality

      `WC8180# show wireless` > Verify that wireless is enabled.

      `WC8180# show wireless controller status` > Verify that on the AMDC, the Domain Role shows up as AMDC

      `WC8180# show wireless domain peer-controller status` > Verify that on AMDC, Peer Controller state is correct.

      `WC8180# show wireless ap status` > Verify that the APs that were managed prior to the upgrade are in a managed state.

The time that it takes to have all the APs managed depends on the total number of APs in the network.

Note: If it is observed that the configuration is not restored after the image upgrade is complete, please restore the configuration from the ASCII configuration saved during STEP 2.

7. **Upgrade the Access Point image**

   `WC8180# wireless domain ap image-update start`

   The download initiates on the new AP Image to the Access Points. After the image download is complete, the APs reset based on the configuration of the **`domain ap image-update reset-group-size`**.

8. **Verify that the AP Image upgrade is successful**

   `WC8180# show wireless ap status`> Verify that all the APs that were managed prior to the upgrade are in a managed state and the **Need Image Upgrade** flag is set to **No**.

   `WC8180# show wireless ap status detail`> Verify that the software version points to the new upgraded software image.

Importing policies from the Wireless Controller into the WMS

After the Wireless Controller upgrade is complete, you are required to Import Policies into the WMS from the AMDC in the Mobility Domain

Navigate to **WMS** > **Configuration** > **Mobility Domains** > **Import Policies** and enter the management IP of the AMDC.

Upgrading the Wireless Controller Diagnostics image to Release 1.1.0

Use the following procedure to upgrade the Wireless Controller Diagnostics image to a Release 1.1.0 image.

When using the Diagnostics menu to upgrade a Diagnostics image on Wireless Controllers running Releases 1.0.0, 1.0.1 or 1.0.2 code streams, refer to the instructions listed in the Diagnostics image upgrade document on the support portal.

Important:

You can upgrade the Diagnostics image using CLI only after the Wireless Controller is upgraded to the Release 1.1.0 image.

Procedure

1. **`WC8180# download address <tftp server address> diag <diagnostics image name>`**

   The new diagnostics image downloads to the controller and reset the controller.

2. After the controller boots up, verify that the diagnostics image upgrade is successful

   `WC8180# show sys-info` > The firmware version should display the new image.

Chapter 4: Resolved Issues

The following known issues are resolved in the current software release.

CR Number	Description
Wireless Controller	
wi00600410	WC8180 does not initialize correctly upon reset or when Wireless is disabled and re-enabled on the controller. When this happens the Controller does not join the domain and Aps cannot be managed by this controller. In order to recover from this situation, the administrator would have to either disable Wireless and re-enable Wireless or reboot the controller. This issue was not observed during normal switch operation."
wi00600450	When Peer Controllers are either reset to Factory Defaults or explicitly Leave the Wireless Domain, the stale controller on the AMDC has to be cleared via CLI cmd "wireless domain purge-stale-controllers" before the peer controller tries to join the domain again. If this step is not followed, CLI displays an Internal Error.
wi00600484	AMDC fails config sync to Peer Controllers in certain scenarios where Diffserv policies and the policies have empty classifier blocks or empty policies.
Access Point	
wi00600354	CLI command "show wireless ap upgrade-failed" shows the failed AP only until that AP becomes managed. The table is cleared once the AP becomes managed even though image upgrade has failed for that AP. Determined to be Working As Designed, as the AP can become managed via another controller in the domain. CLI Command "show wireless ap status" will show the correct status on the AMDC.
Wireless Clients	
wi00600803	Ekahau tags have a compatibility issue with Microsoft DHCP server 2008. The workaround is available for DHCP server 2003.
WMS	
wi00842909	WMS: New authentication profile for a WPA2 network profile cannot be pushed to A-MDC.
wi00575540	When SNMP v3 User is configured for Authentication Protocol=MD5 and Privacy Protocol = None; WMS gets stuck at Apply or Import Policies using this User Credentials. Using DES as the Privacy Protocol resolves this issue.

CR Number	Description
wi00576352	WMS does not allow to swap Mobility Vlan - Local Vlan mapping between two vlans. In order to swap the vlans mapped, both the mobility vlans have to be mapped to none, apply the settings, then change to new values.
wi00600324	WMS can get stuck during Importing Policies in SNMPv3 mode with 3DES encryption. On WC8180, it is recommended to use the AES encryption mode.
wi00600442	WMS does not display Client location view in the Client Dashboards when multiple APs report the client but the AP that reports the strongest signal is not present in the SMX Floor Plan. To avoid this issue, ensure that all the APs are added correctly to the Floor Plan.
wi00600504	WMS does not to consistency check when importing CSV File for Blacklist/ Whitelist Entries and incorrectly shows that Update is successful. However no entries are created in the database.
wi00600638	WMS fails to add a user in the Local User Database if a new user is created without specifying the password. WMS does not indicate any error and reports that the policy is applied successfully.
wi00600702	WMS will only refresh the Access Point and Client Views in real time every polling interval (10 min). For current state of an AP or a wireless client, right click on the AP/Client to open the dashboard. At this point WMS refreshes the data before displaying the dashboards.
wi00601101	When a new Language code is configured under WMS, Captive Portal; applying the configuration creates a new Captive Portal Profile on the controller. This is not observed when configured via CLI.:
wi00601113	Changes to the AP static channel and power settings via WMS are not applied to the controller.
wi00601372	WMS allows unsupported channels to be configured and applying the configuration returns a Success. However these channels are not applied to the controller.
wi00664708	WMS incorrectly prompts Auto-RF History Depth range as 0-24 instead of 0-10. However any values above 10 will not be accepted by WMS.
wi00664805	Changes to Rate Limiting configuration for the Radio Profile under the Data Rates Tab via WMS are not applied to the controller.
wi00672326	In some instances, changing the Auto-RF mode and applying the configuration via WMS resulted in certain APs changing their channel.
wi00673223	WMS incorrectly prompts Auto-RF History Depth range as 0-24 instead of 0-10. However any values above 10 will not be accepted by WMS. Duplicate of wi00664708.
wi00674985	WMS does not display the RF Scan Duration for WIDS-WIPS Radio Profiles. Information is available via CLI or on the Radio Profile Edit Screen in WMS.

CR Number	Description
wi00674990	Changes to the RF Scan band and RF Scan Duration for a WIDSWIPS Radio Profile via WMS are not applied to the controller.
wi00675071	Changes to the AP static channel and power settings via WMS are not applied to the controller. Duplicate of wi00601113
wi00685804	WMS does not allow admin to change the History Depth for Auto-RF in manual mode. The History Depth can be changed via CLI if required while in manual mode.
wi00685805	Auto-RF action is executed on the wrong radio when applied from WMS. The 2.4 and 5 GHz Radios are interchanged. Admin needs to select 5GHz to execute actions on the 2.4GHz Radio and vice versa.
wi00685809	Proposed Channels are not displayed correctly in WMS and different from values in CLI after running the Auto-RF Algorithm.
wi00686040	WMS Site Model Tab under Monitoring/Site Views gets stuck in loading when adding Site Model Files using Internet Explorer 8. The smx File gets added correctly, however this can only be viewed by closing and re-opening the browser. This issue is not observed while using Firefox.
wi00841408	In WMS: when using CLI to approve a discovered AP, the AP list and AP status list are not updated while the Discovered AP list is updated. Determined to be Working As Designed. If this configuration change needs to be reflected in WMS, User needs to Import Policies from the AMDC.
wi00842220	WMS: Channel and Power values are not pushed to A-MDC for configured domain. The workaround is to configure location field for AP.
wi00875828	WMS does not show the correct channels for 2.4GHz radio after importing policies from WC. CLI shows correctly for both 2.4GHz and 5GHz radios.
wi00878696	WMS: Assigning a radius-profile in a network-profile with Open user validation does not push the configuration to WC.
Captive Portal	
wi00600184	Captive Portal session information for a client connected to a peer controller is not displayed correctly on the controller that becomes AMDC after the original AMDC is shutdown. The Captive Portal Client remains connected to the network as expected and the session information can be obtained from the peer controller to which the client is connected to.
wi00600220	CLI command "show wireless captive-portal client status detail" does not display certain parameters on the AMDC when client connects to a peer controller on which the output is correct. Now if the CP client roams to a different controller, these values are not displayed on the AMDC as well as the controller where the client is connected. This does not impact the CP Client network connectivity.
wi00600313	Captive Portal Locale settings are not synchronized by the AMDC to the peer controllers. This will result in different portal page when users are connected to APs managed by different controllers. Workaround is to have the peer

CR Number	Description
	controllers Leave the wireless domain, apply the Captive Portal Locale settings on the standalone controllers, then join the domain.
wi00600616	Intermittently, "show wireless controller config-sync-status" shows that Captive Portal is out of sync. This is due to the mismatch in the ordering of the captive portal binary structures internally and should not impact system behavior.
wi00601711	Captive Portal users via Internet Explorer sometimes observe "Page Not Found" error after Logout. The user is logged out correctly.
wi00686032	When multiple Captive Portal Profiles are created, only the default Captive Portal profile customizations are operational. Even when a user connects to the non default Captive Portal profile, the login page displays customizations from the default Captive Portal profile.
wi00842178	Client QoS attributes are not retained when captive portal client roams.
Security	
wi00600133	When the Radius Profile has a high priority server offline, the WC continues to poll for the offline server intermittently. This could result in client authentication retries if the request came in when the system was polling for the offline server. Radius Health Check feature is implemented to resolve this issue.
wi00600498	WMS only accepts xx:xx:xx:xx:xx:xx for MAC format and does not accept xx-xx-xx-xx-xx-xx while configuring the MAC Database on the Controller. Issue is not reproducible in 1.1.
wi00601378	Cannot default the wids rogue-ap trap-interval, wired-detectioninterval, ageout adhoc-client.

Trap	
wi00575076	WC8180 does not generate Trap "ntWlanUnmanagedAPDiscovered" when a new AP is discovered on the network. Syslog reports the corresponding log message.
wi00600251	WC8180 fails to generate log messages as expected for Link Down event on the 10Gig Interfaces.
CLI	
wi00600228	Intermittently show wireless controller statistics' and 'show wireless controller tspec-statistics' do not increment properly.
wi00600314	CLI command ""show wireless radio-profile channels <profile>"" incorrectly displays multiple entries while the Radio Profile is configured for wids-wips.
wi00600489	CLI command "show wireless controller status" incorrectly displays the stored AP image versions as 0.0.0.0. This is a display issue and does not impact the image that is pushed to the APs on AP image upgrade.

wi00675045	CLI and EDM allow more than one Radius Accounting Profiles even though only one accounting profile is supported in release 1.0.0.0.
EDM	
wi00600139	EDM supports only 2 concurrent sessions in this release. Using more than 2 concurrent EDM sessions could degrade EDM & System performance.
wi00600696	EDM does not display all the supported channels when the Country Code is different than US. CLI & WMS will display the correct list of supported channels.
wi00601384	EDM/Wireless/Security/Widps/RogueAP & Client Controls tab does not display the correct configurable values for WiredNetworkDetectionInterval and DetectedTrapInterval. CLI displays the correct values.
wi00601386	EDM/Wireless/Security/Widps/KnownRogueAP tab does not provide all the configuration options available from CLI.
wi00601389	EDM/Wireless/Security/Widps/FailedAP tab does not provide all the configuration options available from CLI.
wi00601467	EDM/QoS Devices/Priority Q Assign - Range displayed incorrectly as 1-255. Correct Range is 1-8.
wi00878761	EDM cannot set auto-rf interval to 1 hour. The minimum value supported is 6 hours. The workaround is to use CLI or WMS to set interval to 1 hour.

Chapter 5: Known Issues

The following known issues are present in the current software release.

CR Number	Description
Wireless Controller	
wi00600170	802.1p Priority for non-IP Packets is not honored by the WC8180 and treats them similar to non prioritized traffic. This issue is not observed for IP Packets and the 802.1p Priority is honored as expected.
wi00882939	While WMS is running, Controller Host CPU spikes can be observed every 10 minutes (or WMS polling Interval). The CPU utilization will return to normal value once WMS poll is complete. CLI responses could be delayed during these spikes.
wi00898413	During External AP Image Upgrade, in some instances when the External Web Server is not responding correctly, the Wireless Controller fails to display an Error. Controller displays an Error when Web server is not reachable or the File is not available on the Web server.
wi00896183	Jumbo frames ingressing from a Wireless Client do not get forwarded out to the Wired Network by the Wireless Controller.
wi00909047	Doing configuration changes that would require config sync in a large scale setup with thousands of users connected could impact domain stability. It is recommended not to make configuration changes in a live environment with thousands of clients connected to the Wireless network.
wi00575545	Downloading the controller image from a USB will be very slow. **Workaround**: Avaya recommends to download the image from a TFTP server through the LAN interfaces.
wi00600595	IPFix functionality on the WC8180 allows monitoring of Wireless traffic with the Source/Destination Address of the Access Point. The traffic from the Wireless End Points is encapsulated by the Access Point, and IP Fix does not provide statistics for Individual Wireless End Points.
wi00671088	In some instances when Peer Controllers come up after a reboot, they display config out-of-sync, however they have the correct configuration and are operating as expected. This is expected to be due to the ordering of certain configuration. **Workaround**: Manually executing a config-sync from the AMDC will resolve the out-of-sync state.
wi00900158	Intermittently, MDC Controller Password is reset to "None". When this happens, the controller will not be able to join or leave the domain. Issue is not easily reproducible. Workaround is to reconfigure the password on the controller by issuing the command “no controller mdc-capable” and then

CR Number	Description
	“controller mdc-capable” this command will ask to create a password for the domain.
wi00909674	When the Wireless Controller is moved from one mobility domain to another, it is recommended to clean up the configuration on the Wireless Controller by doing defaulting the box configuration.
wi00904073	In some instances it was observed that the controller is stuck in Programming/Saving State during Image Download.
Mobility Domain	
wi00575533	Due the limited number of non overlapping channels available on the 2.4GHz Band using channel bonding (40MHz mode) could result in connectivity issues for some of the older adaptors. **Workaround**: Avaya recommends to use 40MHz Mode on the 5GHz Radio and use 20MHz Mode on the 2.4GHz Radio on the AP.
wi00928786	When auto-promote is enabled for the domain, the Domain AP Database could display the country-code as US (For North America) and DE (for Europe) even though the Domain Country Code is set to a non US country in NA (non DE country in Europe). This does not impact the AP functionality. The managed AP table (show wireless ap country-code in CLI or WMS Monitoring --> Access Points in WMS) shows the correct country code. This discrepancy in Domain AP Database (show wireless domain ap database in CLI or WMS->Configuration->Devices->APs in WMS) can be avoided if Access Points are manually added to the domain ap database.
wi00929515	AP Country Code consistency check with Default AP Profile Country Code while importing Domain AP Database entries from a CSV file.
Access Point	
wi00576644	While AP image update process is in-progress, executing image update for another AP via "wireless ap image-update <mac>" will result in error. **Workaround**: Please wait for the AP image update to complete before initiating image update for other APs.
wi00600511	The AP Link LED color does not always follow the specification. In some instances the LED was Green indicating 100 mbps link even though the link was operational at 1000 mbps and should have been Blue.
wi00900160	When the Wireless Controller is downgraded from 1.1 to 1.0.x, external antenna APs AP8120E are also downgraded. However these will be recognized by the controller as AP8120. When the controller is upgraded back to 1.1, this will result in the APs to be unmanaged. **Workaround**: Delete the corresponding AP Database entry for 8120E and add them back with the database as AP8120. Then the APs will get managed. At this time, the APs can be upgraded to 1.1. After the APs are upgraded to 1.1, the database entries should be reconfigured to 8120E for these APs.
Captive Portal	

CR Number	Description
wi00891828	When Captive Portal IP Interfaces are deleted and re-created multiple times, wpsProcessCpIpUpdates or wdpmCpInterfaceSet Error Messages can be observed intermittently and the operation fails. Retrying the operation will be successful.
wi00928771	Configuration with non-default values set for Captive Portal HTTPS port & Max-Bandwidth change after upgrading from ver 1.0.x to ver 1.1.0. These values have to be reconfigured after the upgrade.
wi00904833	Wireless Controller System IP can be exposed to the Captive Portal user if System IP is used as the Captive Portal IP. The Captive Portal IP should be different from the Wireless Controller System IP.
wi00891116	In scenarios where Captive Portal Message strings are customized with longer than 254 characters, show running-config and copy running-config commands do not display/copy the customized strings correctly. This could cause an issue when configurations are restored using the saved ASCII configuration files. This will not impact Captive Portal Customization functionality in run time. **Workarounds**: The following Workarounds are available: 1) In case of restoring configuration on the same software release, restore the configuration from binary configuration file. 2) The configuration can also be restored through WMS 3) If the above two workarounds are not acceptable, Captive Portal customization via the Downloaded Locale File is recommended.
wi00906368	In scenarios where the Captive Portal Client fails to download the Captive Portal HTML File correctly, the Captive Portal Page displays some garbage characters.
wi00576206	Captive Portal Client Associated with the AP continues to receive multicast traffic even after the Captive Portal session is closed.
wi00600710	While using https as the protocol for Captive Portal, Firefox complains about the certificate serial number and the issuer. **Workaround**: Please delete any previous certificate from the client browser store and re-launch the browser for Captive Portal to work.
wi00927481	While using CP IP Interface Feature, Captive Portal Session is not cleared on the controller hosting the CP IP correctly when the Captive Portal Client is associated to an AP managed by a different Wireless Controller and the client disconnects. The session is deleted after the CP Client Idle Time out or Session Time out expires.
wi00884585	Intermittently Captive Portal Sessions cannot be de-authenticated using the "wireless captive-portal client-deauthenticate captive-portal-profile <id>" command. Use "wireless captive-portal client-deauthenticate network-profile <id>" to de-authenticate clients.
wi00882613	Upon upgrading to 1.1.0.0 it is required to upgrade the APs as well before Captive Portal Clients can connect to the network. Not upgrading the APs will result in clients connecting to the Captive Portal SSID having Open access to the network.

CR Number	Description
Security	
wi00576447	Wildcard entries are not supported for MAC Entries in the MAC Database on the WC 8180.
wi00884023	In WMS mapping or un-mapping a certificate and applying policies only applies the configuration to the AMDS and does not push down to BMDC or Peers. **Workaround**: Force config sync by Right Clicking on Domain Name, Select Domain Actions and Click on Force ConfigSync.
wi00880664	When controller is not set up to with NTP Server, then Self signed certificates generated on the controller have a certificate validation date that is always starting from 2000/1/01. **Workaround**: Avaya recommends to configure the Wireless Controller with NTP Server.
wi00873112	Self Signed Certificate generation time on the WC8100 depends on the Key size and could take above 1 minute to generate a certificate. CLI/EDM configuration operation during this time could result in a Timeout.
WMS	
wi00576035	WMS takes about 3 minutes to update the MDC Capable Flags if the value is modified via CLI.
wi00600720	In scenarios where the JPEG file of the Floor Plan used in SMD has a lot of white space around the actual floor plan, importing that into WMS for RF Monitoring will result RF Views incorrectly mapped onto the Floor Plan. **Workaround**: Avaya recommends to crop additional white spaces around the Floor Plans within the JPEG before using it for RF Planning and Monitoring.
wi00600742	In some situations the AP Radio Power Levels displayed in the WMS RF Views is different from that displayed via "show wireless ap radio status" command in the CLI.
wi00664791	WMS with Internet Explorer 8 does not display policy names correctly in some instances as policy names appear to be overlapped.
wi00601329	Not able to monitor RF-Views in WMS when logging into WMS using the credentials for a Role - User.
wi00900592	WMS: Monitoring Clients in WMS does not work if http port on WC is non-default
wi00925454	Under WMS Monitoring Tabs, Sorting entries only sorts contents on the active page of the Tab instead of all the entries in the Tab.
wi00883059	Captive Portal Redirect URL configuration with "%" character is not accepted through WMS. **Workaround**: To configure URL with special characters use CLI or EDM.
wi00926746	WMS uninstall process removes the avaya/wms/backup folder and erases any backup files stored in that directory.

CR Number	Description
	Workaround : Avaya recommends to save the backup file to a folder outside avaya/wms folder to be able to restore WMS configuration after upgrade/re-installation.
wi00929392	**Workaround**: For Linux WMS installations: move the wms/lsm directory to a different location before installing the new version. The WMS installation process on Linux can fail if the wms/lsm directory is present during installation.
wi00664681	In WMS, when a new Radio Profile is created in bgn mode and channel bandwidth set to 40MHz, applying the configuration incorrectly applies the channel bandwidth as 20MHz to the controller. **Workaround**: Applying the configuration a second time pushes the 40MHz configuration to the controller.
wi00929502	In WMS, setting an Image Version as Active (set to "True" under Domain Name (Right Click) & Edit Settings/AP Image Download for active filename) is not always applied to the controller. **Workaround**: Retrying the Apply Policies, pushes the configuration to the controller.
wi00929519	Rel 1.1 WMS saves Alarms Data to the backup SQL File. If there are a lot of Traps in the database at the time of backup, the SQL File size can become large (above 750MB) and restoration can take a long time (above 30 minutes) or fail in some instances.
wi00908543	Using WMS version 1.1 to configure WC version 1.0.x could result in certain configuration parameters (Monitoring->wireless ap->select an ap and click Action to change power or channel) to fail due to limitations on the WC 8100 1.0.x software. **Workaround**: Use the CLI or EDM to do the configuration.
wi00897369	Site Model Designer may not work correctly in non-US/English localized Windows. **Workaround**: Use a US/English localized O/S to launch SMD.
wi00908763	WMS RF Views do not take Cable Length for External Antenna AP into account when displaying coverage area in the floor plans.
Diffserv Policies	
wi00600212	In some instances where diffserv policies are not applied to all the network profiles on a radio, then the CLI command ""show wireless diffserv statistics"" does not display client qos statistics. In this scenario, use ""show wireless client qos status"" displays the MAC addresses of all clients to which policies are applied. **Workaround**: Use the MAC address of a specific client and execute "show wireless diffserv statistics <mac>" to provide the correct statistics for a particular client. "
wi00686010	WMS Diffserv Classifers Table can be sorted either in Ascending or Descending order. If users do this, then the ordering of the classifers is modified and it cannot be modified to the required order unless all classifiers

CR Number	Description
	are deleted and recreated. However this is a display issue only and the configuration is not applied to the controller. **Workaround**: Avaya recommends not to sort the classifier table in WMS.
wi00925228	Intermittently Diffserv Policies applied to client via Radius Attributes are not applied correctly. **Workaround**: Diffserv policies created on the controller are applied as expected.
Traps/Syslog	
wi00576426	Trap message is not generated when a Wireless Client fails MAC Authentication.
wi00890955	The Wireless Controller fails to generate "avWlanAPDeniedAdmissionToMDNoLicense" and "avWlanAPUtilizationOverflow" trap as expected.
CLI	
wi00576289	The CLI command "show wireless managed-switch" can display incorrect information for the number of clients and number of managed aps on the peer switch in some instances. **Workaround**: Please user CLI commands "show wireless controller status" and "show wireless domain peer-controller status"
wi00575490	The command output for "show wireless ap vap status" is different on AMDC and BMDC. On the BMDC and Peer Controllers the output only displays the VAPs that are configured. On AMDC the total number of VAPs that are allowed on the system are displayed however only the VAPs that are configured have a SSID. This is a display issue and does not impact the system behavior.
wi00600554	On WC8180, "show wireless client status" displays client IP address as 0.0.0.0 in some instances. The controller learns the client IP Address via IP Packets received from the associated client. In instances where the client does not send any IP packets after association or after the client roams to a new AP, the controller will not learn the Client IP address and 0.0.0.0 is displayed in this table.
wi00600799	Intermittently APs managed by the Peer Controllers are not displayed by the AMDC after all the controllers in the domain are reset. WMS and the CLI on Peer controllers will display the complete list of managed APs in this situation.
wi00600411	Clearing domain / controller statistics does not clear the Wireless Diffserv statistics. Stats get cleared when a client either disconnects or roams.
wi00600206	In some instances the CLI output for "show wireless domain peer-controller status" on AMDC displays wrong number of APs managed by the peer controllers. CLI command "show wireless ap status" gives the correct number of APs managed in the domain on the AMDC and the command shows the number of APs managed by the switch on the peer controllers.

CR Number	Description
wi00600272	In some instances it is observed that CLI output for "show wireless security wids-wips rouge-ap-classification <mac>" gets stuck for about a minute before the display is complete and the command prompt is returned.
wi00876681	CLI: "show wireless client association controller" displays wrong info when client roams from AMDC to PWC .
wi00927048	In some instances BMDC & Peer Controllers do not show accurate information for the number of AP's for AP Database and Known AP Database. The actual entries in the database are accurate.
wi00928850	When you use the "Default" command in CLI to default the age-out parameters under "Security Wids" context, it sets the age-out value to 1440 mins instead of 24 mins.
wi00930198	CLI Command "show wireless captive-portal profile status" on AMDC displays incorrect "Auth User count" when CP clients are associated to Peer CP-IP address.
wi00930200	CLI: CP "Authenticated Users" count shows negative values
wi00928890	CLI: Inconsistent behaviour across CLI's for country code Case (lower & upper)
wi00898859	CLI Command "show wireless domain ap database country-code XX" can take a very long time based on the number of APs in the mobility domain - (about 7 min with 4K APs).
wi00896985	AMDC does not show ap-profile status as "Associated" if the AP assigned to that ap-profile is managed from Peer WC. Need to check "associated" status from Peer"
E911	
wi00839411	CPU spikes during E911 auditing.
wi00839405	E911: AP and client auditing did not finish within the configured interval (5 minutes) and could overlap. **Workaround**: Avaya recommends to configure the interval as 10 minutes or more.
wi00842513	E911 - Roaming traps are not sent to trap receiver during switch failure.
EDM	
wi00600593	EDM fails to create the network profile correctly when the WEP key entered shorter than the required length. Upon correcting the key length, EDM incorrectly creates a network profile with an empty WEP Key value. **Workaround**: Use the CLI to correct the configuration in this scenario.
wi00600121	Using EDM, users will not be able to clone existing Radio profiles. This is possible via CLI & WMS.
wi00600582	While monitoring Graphs for the 10Gig Interfaces, the counter values in some instances were observed to be very large numbers and in some instances negative numbers. In both the cases the value displayed by EDM is invalid.

CR Number	Description
wi00600583	While monitoring the Port/Device Graphs on EDM, clearing port statistics via CLI does not clear the statistics in EDM.
wi00600540	TACACS+ Configuration is not available via EDM. Please use CLI for TACACS+ Configuration on the Wireless Controller.
wi00600416	EDM cannot be used to reset or update APs managed by the Peer Wireless Controllers. **Workaround**: Avaya recommends to use either the CLI or WMS to perform domain wide operations.
wi00600204	EDM displays Error message while configuring Radius Profile with type = accounting while adding a server with priority 1. The server is added successfully but EDM does not indicate that.
wi00600241	EDM does not allow AP Campus Field Configuration. **Workaround**: Use the CLI/WMS to configure this value (if required).
wi00600384	EDM displays invalid error message "CommitFailed" when user tries to configure diffserv policies more than the supported limit. EDM should display correct error message similar to CLI
wi00653845	ASCII configuration download fails when initiated via EDM.
wi00601390	EDM/Wireless/NetworkProfile/Edit Profile/Security Tab/Security Mode=wepStatic - The help information for key length is incorrectly displayed as 13 for ASCII and 26 for HEX. **Workaround**: The correct key length is 5 for ASCII and 10 for HEX.
wi00601370	EDM/Wireless/Security/WIDPS/RF Scan AP Tab shows Avaya AP OIDs as Unknown.

Appendix A: Downgrading the Wireless Controller

Procedure

1. **Backup the current configuration (Binary) to the TFTP server or USB drive.**

   ```
   WC8180# copy config tftp address <tftp server address> filename
   <config file name>
   ```

   OR

   ```
   WC8180# copy config usb filename <config file name>
   ```

2. **Backup the ASCII Configuration to the TFTP server or USB drive**

   The ASCII configuration is required if the current configuration has to be restored on a WC controller running version 1.0.0, 1.0.1 or 1.0.2 software. The Binary configuration saved with 1.1.0 version will not be compatible with 1.0.0, 1.0.1 or 1.0.2 versions.

   ```
   WC8180# copy running-config tftp address <tftp server address>
   filename <config file name>
   ```

   OR

   ```
   WC8180# copy running-config usb filename <config file name>
   ```

3. **Reset the Wireless Controller to the default configuration**

   ```
   WC8180# boot default
   ```

   Ensure the partial default option is used to retain the management IP and Licenses on the controller.

4. **Download the 1.0.x image to the Wireless Controller if required**

   a. `WC8180# show boot image`

      Verify the 1.0.x image that is required for the downgrade is available on the controller. If it is not available, download the required image.

   b.
      ```
      WC8180# download address< tftp server address> secondary < image
      file name>
      ```

      The Wireless Controller resets to factory defaults after the controller boots up with the 1.0.x software image.

5. **Restore the configuration on the Wireless Controller**

   After the Controller is downgraded to the required software, connect to the controller and restore the configuration using the binary configuration file that was saved prior to upgrade to 1.1.0.

a. **Option 1: Using the Binary configuration file saved with the 1.0.x code stream**

   Loading the configuration from the USB:

   ```
   WC8180# copy usb config filename <file name>
   ```

   Loading the configuration from the TFTP server:

   Do the preliminary controller configuration to get connectivity to the TFTP server.

   Download the configuration from the TFTP server

   ```
   WC8180# copy tftp config address <TFTP Server IP> filename <file
   name>
   ```

b. **Option 2: Using the ASCII configuration file saved with the 1.1.0 code stream**

   Loading the configuration from the USB:

   ```
   WC8180# configure usb filename <file name>
   ```

   Loading the configuration from the TFTP server:

   ```
   WC8180# configure network address <TFTP Server IP> filename <file
   name>
   ```

6. **Restore the License file on the Wireless Controller**

   You must re-install the License file on the Wireless Controller after the image downgrade from software version 1.1.0 to 1.0.x . If the License file is not readily available, it can be downloaded from Avaya Licensing Portal.

   a. Loading the License file from the USB

      ```
      WC8180# copy usb license filename <License file name>
      ```

   b. Loading the License file from the TFTP server

      ```
      WC8180# copy tftp license address <TFTP Server IP> filename
      <License file name>
      ```

   c. Resetting the Wireless Controller after installing the License file.

      ```
      WC8180# boot
      ```

7. **Repeat Steps 1 to 5 for all the Wireless Controllers in the Mobility Domain**.

8. **Verify that the Wireless Controller image downgrade is successful**

   a. Verify that the Controller has the correct image

      `WC8180# show sys-info` > Verify that the software version is correct.

   b. Verify the wireless functionality

      `WC8180# show wireless` > Verify that wireless is enabled

      `WC8180# show wireless controller status` > Verify that on AMDC, the Domain Role shows up as AMDC

      `WC8180# show wireless domain peer-controller status` > Verify that on AMDC, the Peer Controller state is correct.

`WC8180# show wireless controller license-info` > Verify that the Licenses are loaded correctly.

`WC8180# show wireless ap status` > Verify that the APs that were managed prior to the downgrade are in managed state.

The time that takes to manage all the APs depends on the total number of APs in the network.

9. **Access Point image downgrade**

   ```
   WC8180# wireless domain ap image-update start
   ```

   This download initiates on the new AP Image to the Access Points. After the image download is complete, the APs will reset based on the of the **`domain ap image-update reset-group-size`** configuration.

10. **Verify that the AP image downgrade is successful**

    `WC8180# show wireless ap status` > Verify that all the APs that were managed prior to the image update are in a managed state and the **Need Image Upgrade** flag is set to **No**.

    `WC8180# show wireless ap status detail` > Verify that the software version points to the new software image.

11. **Import policies from the Wireless Controller into the WMS**

    After the Wireless Controller downgrade is complete, it is recommended to Import Policies into WMS from the AMDC in the Mobility Domain

    Navigate to **WMS** > **Configuration** > **Mobility Domains** > **Import Policies** and enter the management IP of the AMDC.