Infrastructure Management Compliance Audit

How-To Guide

Contents

Document Conventions

The following graphical alerts are used in this document to indicate notable situations:

✓ ***NOTE*** This symbol indicates something of special interest or importance to the reader. Failure to read the note will not result in physical harm to the reader, equipment or data.

⚠ ***CAUTION*** This symbol indicates that if this information is ignored, the possibility of data or material damage may occur.

⚠ ***WARNING!*** This symbol indicates that if this information is ignored the possibility that serious personal injury may occur.

1 Introduction

It is important for network operators to have the ability to monitor their WLAN network to ensure unauthorized configuration changes aren't being made. Unauthorized configuration changes can result in security risk or WLAN performance deterioration. The problem is compounded when large scale WLAN networks are deployed or a customer has a multi-vendor WLAN deployment.

The audit feature in Infrastructure Management allows operators to check for inconsistencies in device configurations and take corrective action.

2 Requirements

2.1 License Requirements

Devices that need to be audited require the WLAN Management license (AD-IMDV-P-X) and the service support license (SWS-AD-IMDV-X-Y).

2.2 Supported Devices

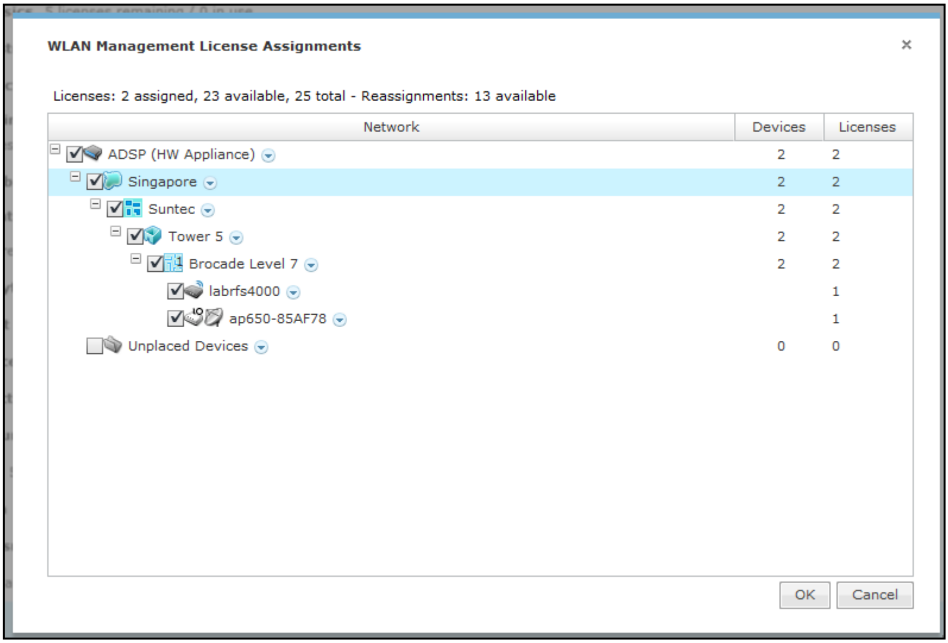
Please refer to the document *Motorola AirDefense Services Platform 9.0 Infrastructure Management Supported Devices* to see the list of supported vendors, models and firmware which can be managed by Air Defense.

Link to download the document:
http://support.symbol.com/support/search.do?cmd=displayKC&docType=kc&externalId=72E-148064-01InfrastructureManagementSupportedDevicesRevCpdf&sliceId=&dialogID=410618004&stateId=1%200%20410600757

3 Setup

The following steps walk you through the setup required to audit devices.

1. Apply the WLAN Management License:
   a. Go to **Configuration** > **Appliance Platform** > **Appliance Licensing**.
   b. Select **WLAN Management** and click on **License Assignments**.
   c. Select the device for which you wish to assign licenses. In Figure 1, a RFS4000 and an AP650 are selected.



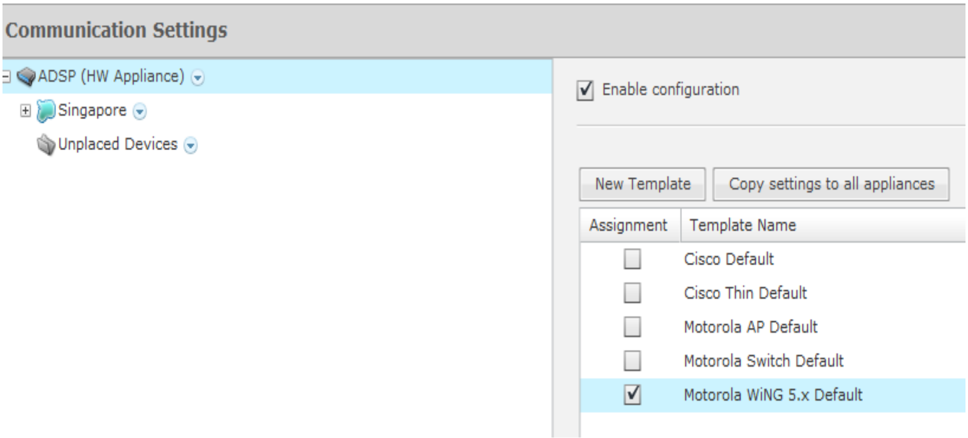
WLAN Management License Assignments

Licenses: 2 assigned, 23 available, 25 total - Reassignments: 13 available

Network	Devices	Licenses
☑ ADSP (HW Appliance)	2	2
☑ Singapore	2	2
☑ Suntec	2	2
☑ Tower 5	2	2
☑ Brocade Level 7	2	2
☑ labrfs4000		1
☑ ap650-85AF78		1
□ Unplaced Devices	0	0

Figure 1: WLAN Management License Applied to RFS4000 and AP650

2. Configure the Communication settings between ADSP and the managed device.
   a. Go to **Configuration** > **Communication Settings**.
   b. Select E**nable Configuration** for the required scope.
   c. Select an existing template or create a new one as required.
   d. If Motorola WiNG 5.x is to be managed, select **Motorola WiNG 5.x Default**.

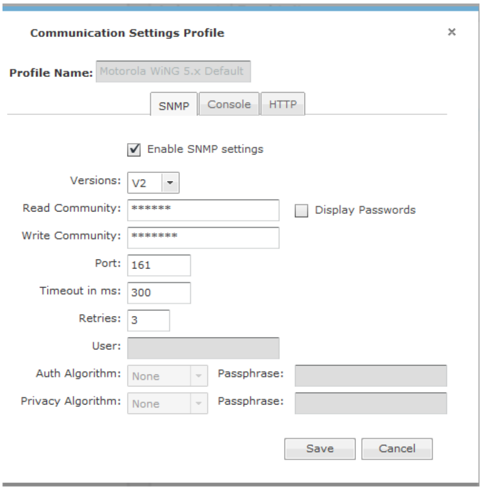


☑ Enable configuration

Assignment	Template Name
☐	Cisco Default
☐	Cisco Thin Default
☐	Motorola AP Default
☐	Motorola Switch Default
☑	Motorola WiNG 5.x Default

Figure 2: Assign the Motorola WiNG 5.x Default Template

e. Select the template to be used and click **Edit**.



Profile Name: Motorola WiNG 5.x Default

☑ Enable SNMP settings

Versions: V2

Read Community: ****** ☐ Display Passwords

Write Community: *******

Port: 161

Timeout in ms: 300

Retries: 3

User:

Auth Algorithm: None Passphrase:

Privacy Algorithm: None Passphrase:

f. Configure the SNMP and Console communication settings to match the SNMP and CLI settings on the device(s) to be managed.

⚠ ***CAUTION*** The SNMP and Console settings configured in ADSP must match the SNMP and Console settings on the managed device. For example, if ADSP is being used to manage a RFS controller and the RFS controller is using SNMP v2, then configure SNMP v2 in **Communication Settings** and enter the read/write community strings as defined in the RFS controller.

g. Click **Apply**.

3. Enable Device Configuration Management.

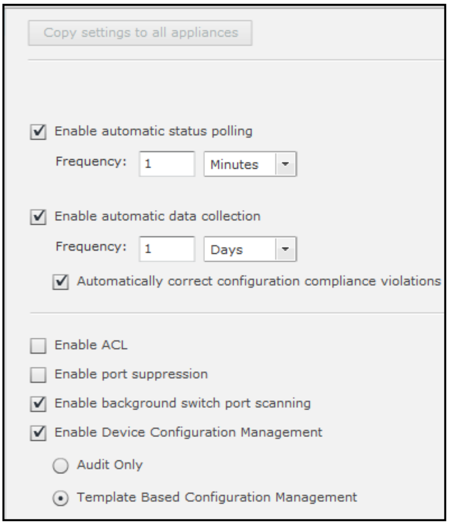
   a. Go to **Configuration** > **Appliance Platform** > **Polling**.

   b. Select **Automatically correct configuration compliance violations** if you want ADSP to push a compliant configuration whenever a non-compliant configuration is detected on a target device. ADSP will check for compliance violations whenever it performs data collection.

   c. Select **Enable Device Configuration Management**.

      i. Select **Audit Only** if configuration management is not required.

      ii. Select **Template Based Configuration Management** if configuration management is required.



☑ Enable automatic status polling
Frequency: 1 Minutes

☑ Enable automatic data collection
Frequency: 1 Days
☑ Automatically correct configuration compliance violations

□ Enable ACL
□ Enable port suppression
☑ Enable background switch port scanning
☑ Enable Device Configuration Management
○ Audit Only
● Template Based Configuration Management

Figure 3: Enable Device Configuration Management

✓ ***NOTE*** Select **Template Based Configuration Management** if you want ADSP to change the configuration of a device from a non-compliant configuration to a compliant configuration.

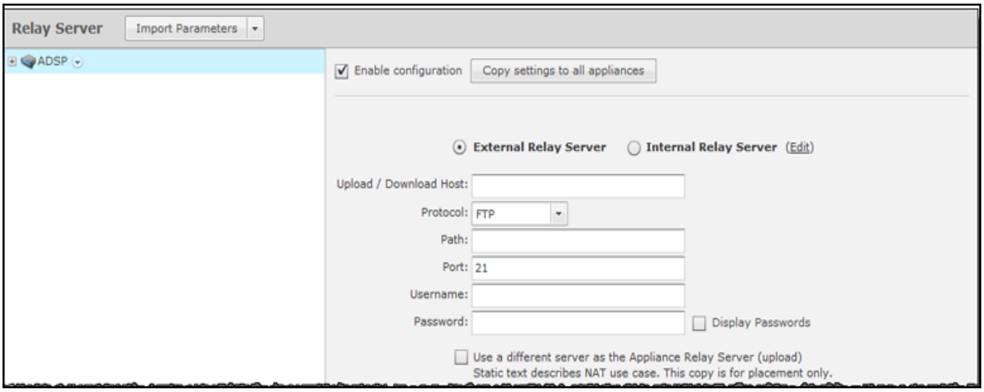
   d. Click **Apply**.

4. Enable a relay server.

   a. **Configuration** > **Appliance Platform** > **Relay Server**.

   b. Select **Enable Configuration**.

   c. Select **External Relay Server** if an external relay server is being used.



☑ Enable configuration

● External Relay Server ○ Internal Relay Server

Upload / Download Host:

Protocol: FTP

Path:

Port: 21

Username:

Password: □ Display Passwords

□ Use a different server as the Appliance Relay Server (upload)
Static text describes NAT use case. This copy is for placement only.

Figure 4: Configuring an External Relay Server

i. Enter the download host name of the relay server ADSP uses to access and fetch device configurations. Normally, this is the IP address of the relay server.

ii. Select a protocol from the dropdown menu (**FTP**, **TFTP**, **SFTP**, **SCP**, **HTTP**, or **HTTPS**).

iii. Specify the path ADSP uses to download information. You should either leave the path blank or use root (/).

iv. Define the port ADSP uses to connect to the relay server.

v. Enter the username needed to update the relay server used by ADSP.

vi. Enter the password required to update the relay server used by ADSP.

✓ ***NOTE*** In networks where NAT is utilized, the relay server address might be different when being accessed by a device and when it is accessed by ADSP. In this case, select **Use a different host address for ADSP connection to relay server** and enter the required information.

d. Select **Internal Relay Server** if the relay server in ADSP is being used.

4 Running an Audit

1. Select the device you want to audit.
   a. Go to **Network** > **Show** > **Network Device**.
   b. Select the device (s) which you want to audit.
   c. Right-click and select **Device Polling** >**Audit**.

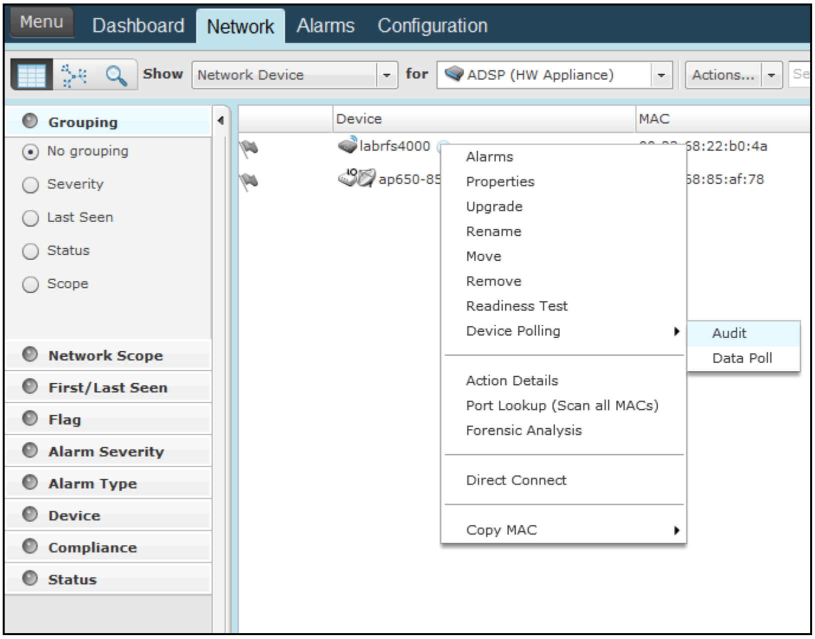
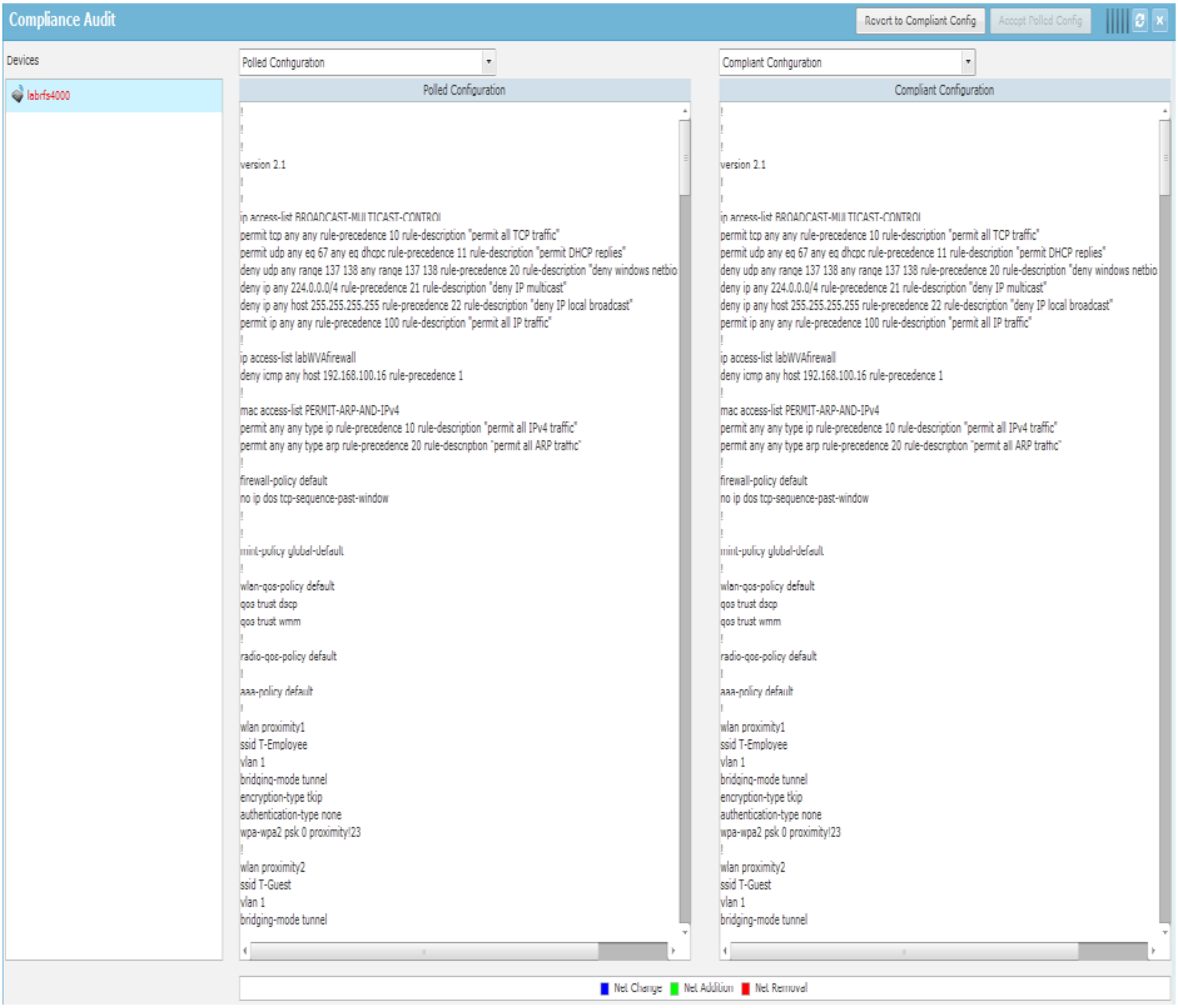


Figure 5: Running an Audit on a Single Device

   d. To run audit on multiple devices, select the devices and go to **Actions** > **Audit Devices**. The **Compliance Audit** screen is displayed. A description of the **Compliance Audit** display screen is given after Figure 6.



Polled Configuration

```
!
!
!
version 2.1
!
!
ip access-list BROADCAST-MULTICAST-CONTROL
permit tcp any any rule-precedence 10 rule-description "permit all TCP traffic"
permit udp any eq 67 any eq dhcpc rule-precedence 11 rule-description "permit DHCP replies"
deny udp any range 137 138 any range 137 138 rule-precedence 20 rule-description "deny windows netbio
deny ip any 224.0.0.0/4 rule-precedence 21 rule-description "deny IP multicast"
deny ip any host 255.255.255.255 rule-precedence 22 rule-description "deny IP local broadcast"
permit ip any any rule-precedence 100 rule-description "permit all IP traffic"
!
ip access-list labWVAfirewall
deny icmp any host 192.168.100.16 rule-precedence 1
!
mac access-list PERMIT-ARP-AND-IPv4
permit any any type ip rule-precedence 10 rule-description "permit all IPv4 traffic"
permit any any type arp rule-precedence 20 rule-description "permit all ARP traffic"
!
firewall-policy default
no ip dos tcp-sequence-past-window
!
!
mint-policy global-default
!
wlan-qos-policy default
qos trust dscp
qos trust wmm
!
radio-qos-policy default
!
aaa-policy default
!
wlan proximity1
ssid T-Employee
vlan 1
bridging-mode tunnel
encryption-type tkip
authentication-type none
wpa-wpa2 psk 0 proximity!23
!
wlan proximity2
ssid T-Guest
vlan 1
bridging-mode tunnel
```

Compliant Configuration

```
!
!
!
version 2.1
!
!
ip access-list BROADCAST-MULTICAST-CONTROL
permit tcp any any rule-precedence 10 rule-description "permit all TCP traffic"
permit udp any eq 67 any eq dhcpc rule-precedence 11 rule-description "permit DHCP replies"
deny udp any range 137 138 any range 137 138 rule-precedence 20 rule-description "deny windows netbio
deny ip any 224.0.0.0/4 rule-precedence 21 rule-description "deny IP multicast"
deny ip any host 255.255.255.255 rule-precedence 22 rule-description "deny IP local broadcast"
permit ip any any rule-precedence 100 rule-description "permit all IP traffic"
!
ip access-list labWVAfirewall
deny icmp any host 192.168.100.16 rule-precedence 1
!
mac access-list PERMIT-ARP-AND-IPv4
permit any any type ip rule-precedence 10 rule-description "permit all IPv4 traffic"
permit any any type arp rule-precedence 20 rule-description "permit all ARP traffic"
!
firewall-policy default
no ip dos tcp-sequence-past-window
!
!
mint-policy global-default
!
wlan-qos-policy default
qos trust dscp
qos trust wmm
!
radio-qos-policy default
!
aaa-policy default
!
wlan proximity1
ssid T-Employee
vlan 1
bridging-mode tunnel
encryption-type tkip
authentication-type none
wpa-wpa2 psk 0 proximity!23
!
wlan proximity2
ssid T-Guest
vlan 1
bridging-mode tunnel
```

Figure 6: Compliance Audit Display Screen

Description of the Compliance Audit Display Screen

Device Column: The first column in the Compliance Audit screen shows the devices on which the audit was run. Devices highlighted in red are devices whose polled configuration is different from the compliant configuration.

If you select the drop down box above column 2 or column 3, you will see two or four options depending on whether you enabled **Template Based Configuration Management.** Below is a description of the four options.

Polled Configuration: This is the configuration polled from the target device. It is the device's running-configuration.

Compliant Configuration: This is the compliant configuration for the target device. ADSP sets the compliant configuration as follows:

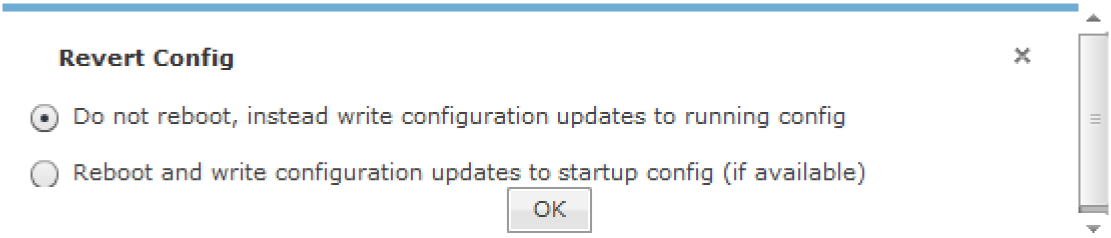
- When ADSP polls a device for the first time, the polled configuration is set to compliant configuration. Subsequently, you must manually **Accept Polled Configuration** as Compliant Configuration.
- When ADSP pushes a CLI Template configuration to a target device, this configuration is set to compliant configuration.

The next two options are seen only if **Template Based Configuration Management** is selected. Select these options if you have created a CLI Template for WLAN Management. (**Configuration** > **Infrastructure Management** >**CLI Configuration**)

Generated Configuration: This is the configuration generated by ADSP from the CLI Template created for the target device. The expansion/extraction variables in the CLI Template are replaced by corresponding CLI commands.

Configuration Template: This is the configuration template set in CLI Configuration for the target device. If expansion/extraction variables are used in the CLI template, they are not replaced by corresponding CLI commands and are displayed as is.

2. Inspect configuration differences as follows:
   a. Select one of the configurations from the drop down menu in column 2.
   b. Select one of the configurations from the drop down menu in column 3.
   c. Scroll down column 2 / column 3 to inspect differences between the 2 configurations selected. Usually, the polled configuration is compared to compliant configuration to check why a device is non-compliant.
3. Resolve configuration differences.
   a. Click on **Revert to Compliant Configuration** if you want to override the polled configuration and push the compliant configuration to the target device. You will see the following alert:


Revert Config

● Do not reboot, instead write configuration updates to running config

○ Reboot and write configuration updates to startup config (if available)

Figure 7: Revert Config Alert

- Select option 1 “Do no reboot…” if you want to overwrite the running-configuration. This will not reboot the target device.
- Select option 2 “Reboot and write …” if you want to overwrite the startup-configuration. This will reboot the target device.

b. Click on **Accept Polled Config** if you want do not want to make any change to the device configuration and want to set the polled configuration as the new compliant configuration.

5 Alarms

Below are the two alarms (related to Audit) that are raised by ADSP.

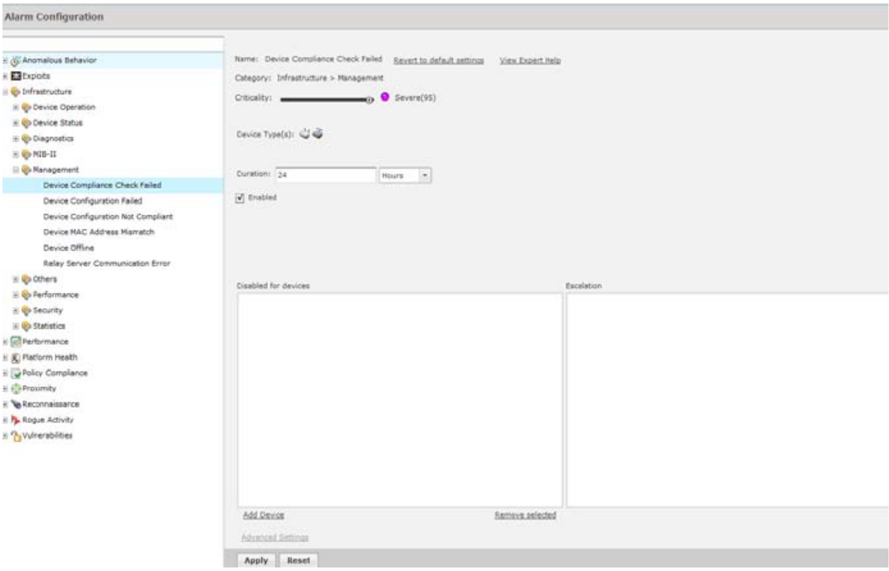
- **Device Compliance Check Failed:** Raised when ADSP is unable to run an audit on a device.
- **Device Configuration Not Compliant:** Raised when ADSP detects a non-compliant configuration on a device.

1. Alarm Configuration:

   a. Go to **Configuration** >**Operational Management** >**Alarm Configuration**.

   b. Expand **Infrastructure** >**Management**.

   c. Select one of the audit alarms.



Name: Device Compliance Check Failed

Category: Infrastructure > Management

Criticality: Severe(95)

Device Type(s):

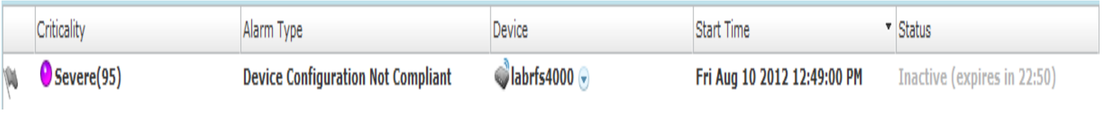
Duration: 24 Hours

☑ Enabled

Figure 8: “Device Compliance Check Failed” Alarm Configuration

2. Customize Alarm Configuration: For most customers, the default alarm configuration is acceptable. However, if you need to customize the alarm configuration follow these steps:
   a. Uncheck the **Enabled** box to disable the alarm.
   b. Change the criticality of the alarm as required.
   c. Change the **Duration** of the alarm as required. Duration refers to the amount of time the alarm will remain active in ADSP.
   d. Add the devices for which the alarm needs to be disabled.
   e. Click on **Revert to Default Settings** to reset the alarm configuration to default settings.
3. View Alarm in **Alarms** tab.

Below is a screenshot of the audit alarm as displayed in the **Alarms** tab:



	Criticality	Alarm Type	Device	Start Time	Status
	Severe(95)	Device Configuration Not Compliant	labrfs4000	Fri Aug 10 2012 12:49:00 PM	Inactive (expires in 22:50)

Figure 9: Example of an Audit Alarm

6 Reports

The WLAN Infrastructure Status report is an Infrastructure Management canned report which provides information related to device audits. To run the report:

1. Go to **Menu** > **Reports**.
2. Scroll down to **Infrastructure Management Reports**.
3. Click on **WLAN Infrastructure Status**.
4. Select the date range and scope for which the report should be run.
5. Enter an email address if the report is to be sent via email.
6. Click **Run Report**. You will see the generated report. The following audit related information is contained in the report:
   a. Configuration Compliance Failures
   b. Historical Switch Audit Compliance Failure Details
   c. Historical Compliance Audit Failures
   d. Top Occurrences of Infrastructure Alarms
   e. Top Criticalities Infrastructure Alarms

Motorola Solutions, Inc.
1301 E. Algonquin Rd.
Schaumburg, IL 60196-1078, U.S.A.
http://www.motorolasolutions.com

72E-171286-01 Rev A
December 2012