



ADSP Guest Network Tuning How-To Guide

MOTOROLA SOLUTIONS and the Stylized M Logo are registered in the US Patent & Trademark Office. © Motorola Solutions, Inc. 2012. All rights reserved.

Contents

| | | |
|----------|--|----------|
| 1 | Summary | 4 |
| 2 | Create Security Profile | 4 |
| 3 | Tune Alarm Settings | 6 |
| 4 | Setup Device Import Rules | 7 |

1 Summary

When the wireless infrastructure is hosting a guest Wi-Fi network, ADSP must be tuned so that it does not give false alarms. False alarms are generated because the guest network BSSs should be sanctioned, but you will not want every device that connects to the guest network to be sanctioned as well. This causes a situation that to ADSP it looks like you have a rogue client connecting to your network. This document walks through tuning ADSP for a guest network that is being hosted by the infrastructure.

2 Create Security Profile

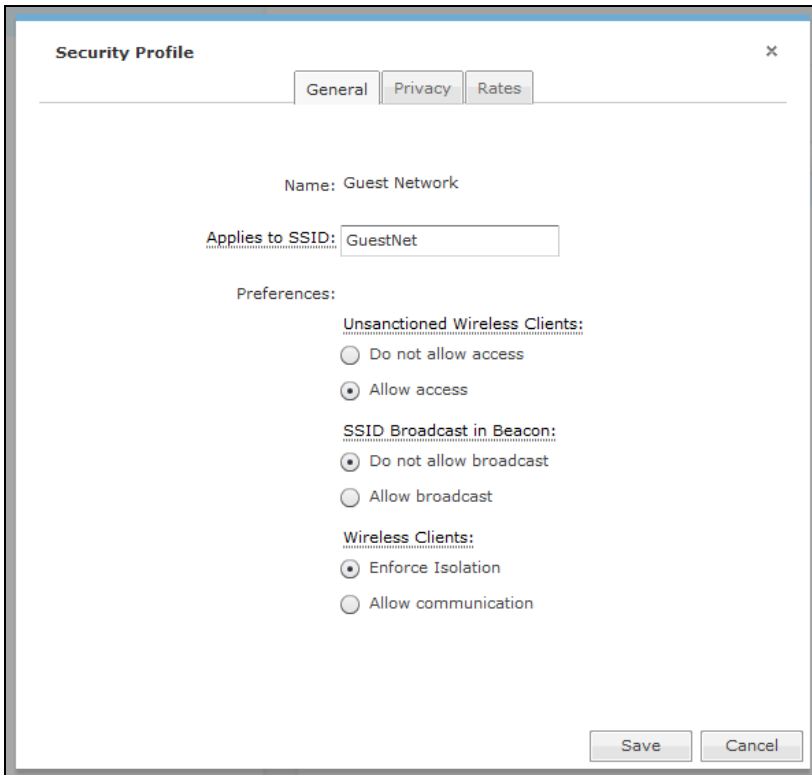
Create a Security Profile for the guest network and allow unsanctioned clients to connect to it. This will prevent the “Rogue Client” alarm from being generated for the guest network when an unknown client connects to it.



WARNING! Do not apply the security profile to any level of the network tree.

1. Go to **Configuration > Appliance Platform > Security Profiles**
2. Create a new security profile.
3. Enter the guest SSID into the Applies to SSID field.
4. Set **Unsanctioned Wireless Clients** to **Allow access**.
5. All other settings can be set as desired.

6. When complete, it should look like the below screen shot:



The screenshot shows a window titled "Security Profile" with a close button (X) in the top right corner. Below the title bar are three tabs: "General", "Privacy", and "Rates". The "General" tab is selected. The configuration details are as follows:

- Name: Guest Network
- Applies to SSID: GuestNet
- Preferences:
 - Unsanctioned Wireless Clients:**
 - Do not allow access
 - Allow access
 - SSID Broadcast in Beacon:**
 - Do not allow broadcast
 - Allow broadcast
 - Wireless Clients:**
 - Enforce Isolation
 - Allow communication

At the bottom right of the window are two buttons: "Save" and "Cancel".



WARNING! Do not apply the security profile to any level of the network tree.

3 Tune Alarm Settings

Tune the **Rogue Client on Sensor Segment** and **Rogue Client on Switch** alarms directly to prevent them from being triggered falsely for devices connected to the guest network.



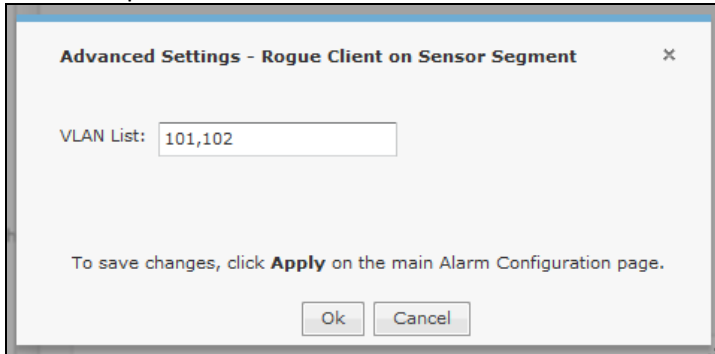
CAUTION There is an issue with WiNG4 devices sending VLAN information to ADSP in the wrong format, so these settings will not work with WiNG4 devices.

1. Go to **Configuration > Operational Management > Alarm Configuration**
2. Open the **Rogue Client on Sensor Segment** alarm.
3. Open the **Advanced Settings** located at the bottom of the alarm configuration window

The screenshot shows the 'Alarm Configuration' window for the 'Rogue Client on Sensor Segment' alarm. The left sidebar contains a tree view of alarm categories, with 'Rogue Client on Sensor Segment' selected. The main panel displays the following configuration details:

- Name: Rogue Client on Sensor Segment [Revert to default settings](#) [View Expert Help](#)
- Category: Rogue Activity > Rogue Exploit
- Criticality: Severe(90)
- Device Type(s): [Icon]
- Duration: 24 Hours
- Enabled
- Enabled for unsanctioned devices
- Enabled for neighboring devices
- Disabled for devices: [Empty list box]
- Escalation: [Empty list box]
- [Add Device](#) [Remove selected](#)
- [Advanced Settings](#) (circled in red)
- [Apply](#) [Reset](#)

- In the advanced settings window, enter all VLANs used by all guest Wi-Fi networks in a comma separated list.

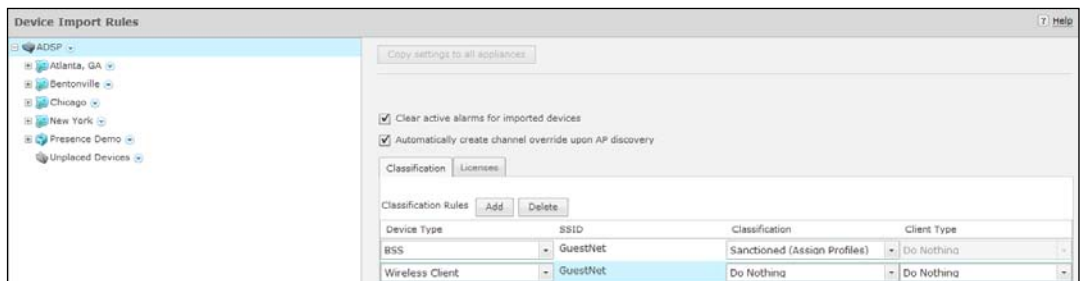


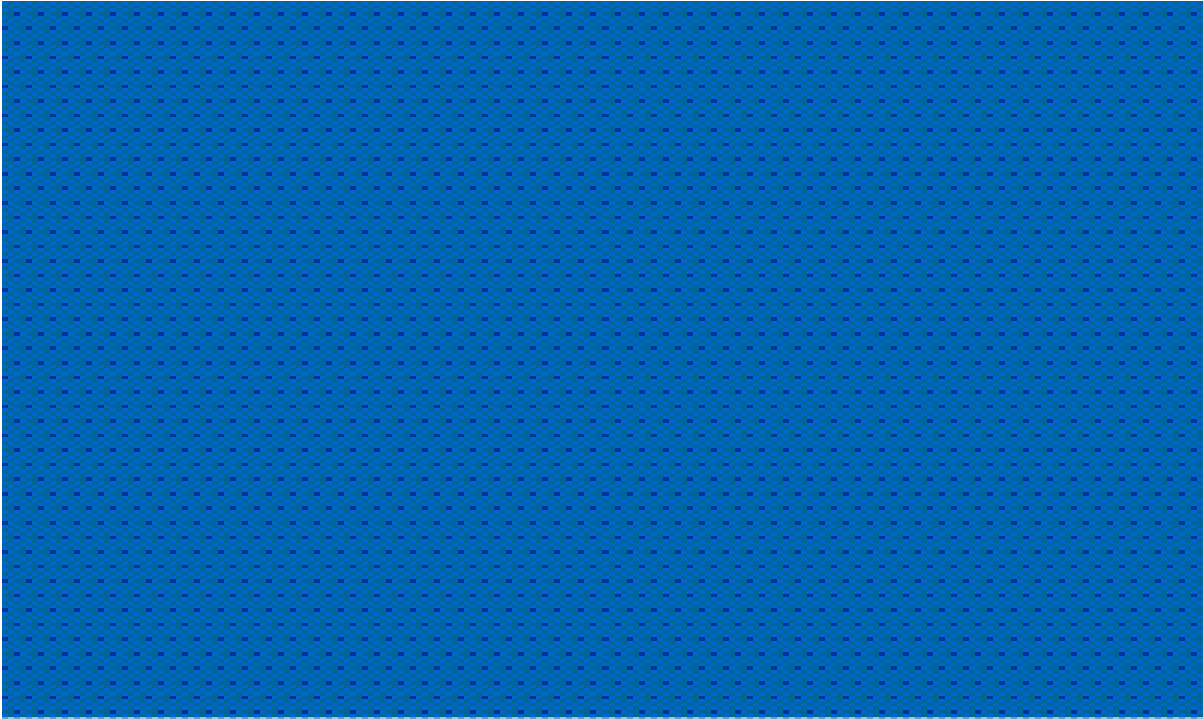
- Repeat the same settings for the “Rogue Client on Switch” alarm

4 Setup Device Import Rules

If data polls are being performed on the wireless infrastructure then device import rules must be setup so that the guest network BSSs and clients are configured correctly. This step will tell ADSP to apply the security profile that was defined earlier and not to assign any settings to the guest clients.

- Go to **Configuration > Appliance Platform > Device Import Rules**.
- Add a new classification rule for a BSS.
 - Set the **SSID** to **GuestNet**.
 - Set **Classification** to **Sanctioned (Assigned Profile)** This tells ADSP to assign the security profile to the BSS that matches the SSID.
- Add a new classification rule for a Wireless Client.
 - Set the **SSID** to **GuestNet**.
 - Set **Classification** to **Do Nothing**. When complete, the settings should look like the screenshot below:





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

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.
© 2012 Motorola Solutions, Inc. All Rights Reserved.

