ADSP Guest Network Tuning

How-To Guide

Zebra and the Zebra head graphic are registered trademarks of ZIH Corp. The Symbol logo is a registered trademark of Symbol Technologies, Inc., a Zebra Technologies company. © 2016 Symbol Technologies, Inc.

Contents

1 Summary 4
2 Create Security Profile 4
3 Tune Alarm Settings 6
4 Setup Device Import Rules 8

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.

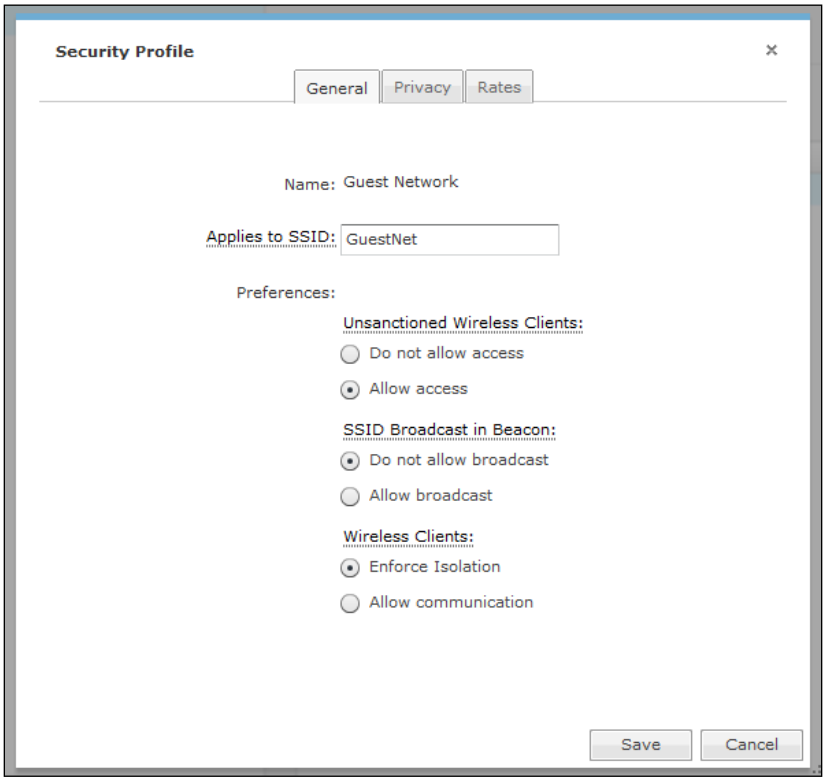
2 Create Security Profile

In order to allow unsanctioned clients to connect to the network, create a Security Profile for each the guest. This will prevent the “Rogue Client” alarm from being generated when an unknown client connects to the network.

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:



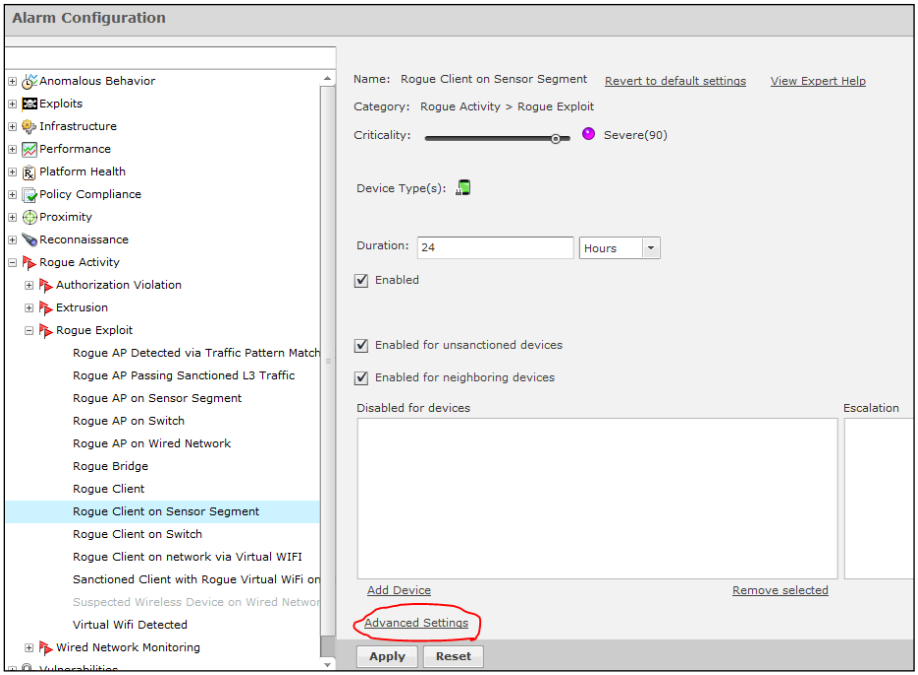
WARNING! Do not apply the security profile to any level of the network tree.

3 Tune Alarm Settings

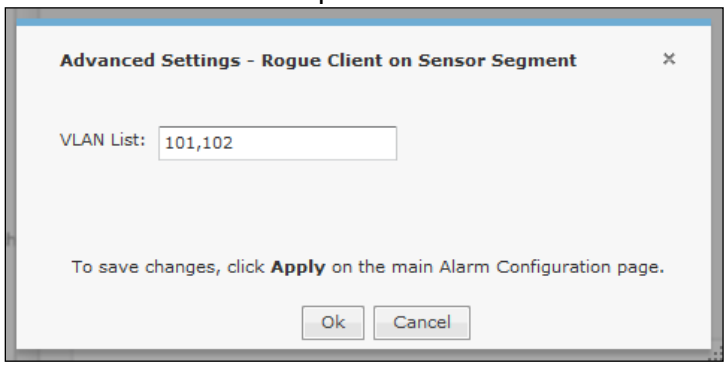
Tune the **Rogue Client on Sensor Segment** and **Rogue Client on Switch** alarms directly to prevent them from being triggered falsely for devices connected to the guest network.

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



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

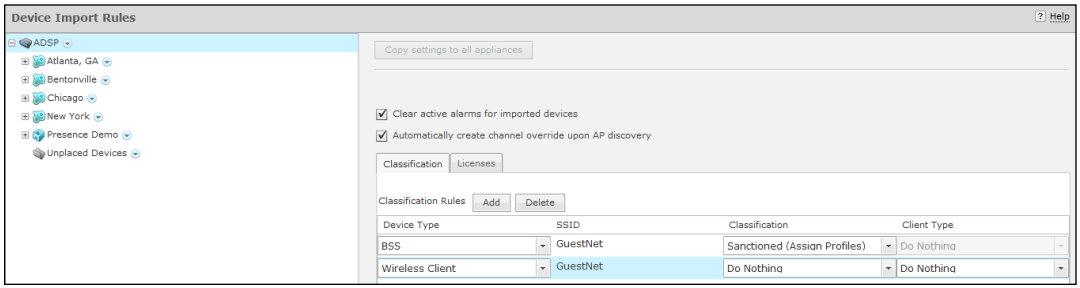


5. Repeat the same settings for the **Rogue Client on Switch** alarm

4 Set up 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.

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



Zebra Technologies Corporation.
Lincolnshire, IL 60069 USA

Zebra and the Zebra head graphic are registered trademarks of ZIH Corp.
The Symbol logo is a registered trademark of Symbol Technologies, Inc., a Zebra Technologies company.

©2016 Symbol Technologies, Inc.

MN-002713-01 Rev A, January 2016