在所有实验中，您应使用 ADSP 帮助菜单作为第一资源来解决可能产生的问题。该菜单将成为您实际部署时的主要资源，您必须熟悉此工具

概述：
此实验向您展示如何使用安全配置文件来定义无线 LAN 中经批准的无线设备的安全配置。

目标：
学员应能够执行以下操作：

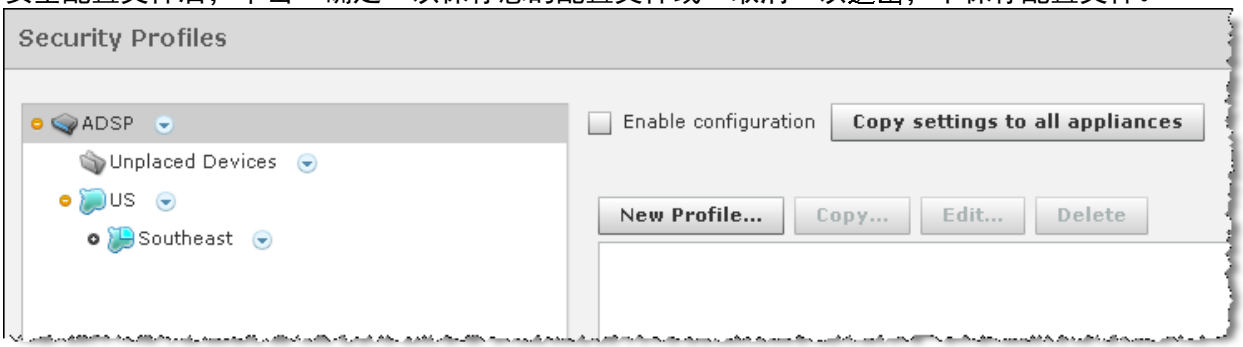
- 对设备进行分类
- 导入设备

策略和分类
安全配置文件

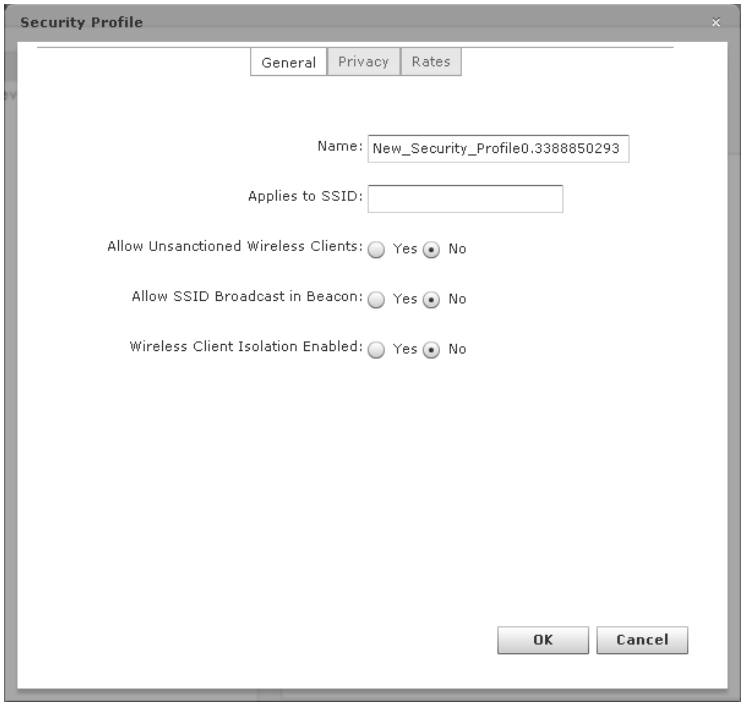
概述

安全配置文件定义了托管无线 LAN 基础设施设备的安全配置。当安全配置文件应用到您的系统时，如果设备操作不符合配置文件中定义的标准，则生成安全警报。安全配置文件提供独立的方法以无线方式监控 WLAN 基础设施配置，确保它符合为组织定义的安全标准。第二层安全保障为安全团队提供明确的方法以捕获管理配置错误或重置为出厂默认设置的设备（这可能允许对网络进行 身份验证和未加密的访问）。例如，对网络考虑需要 WPA2/EAP-TLS/AES 身份验证的企业 WLAN。进行更改时，管理员意外地从网络中删除所有加密和身份验证。这将在网络上产生一个漏洞，允许无意中闯入错误配置的 WLAN 的任何人访问该基础设施。由于更改是由管理员通过管理系统进行的，不会出现错误或警告，使该漏洞长时间不被注意。安全配置文件会快速捕获此策略合规性错误，并向安全团队提示错误配置。

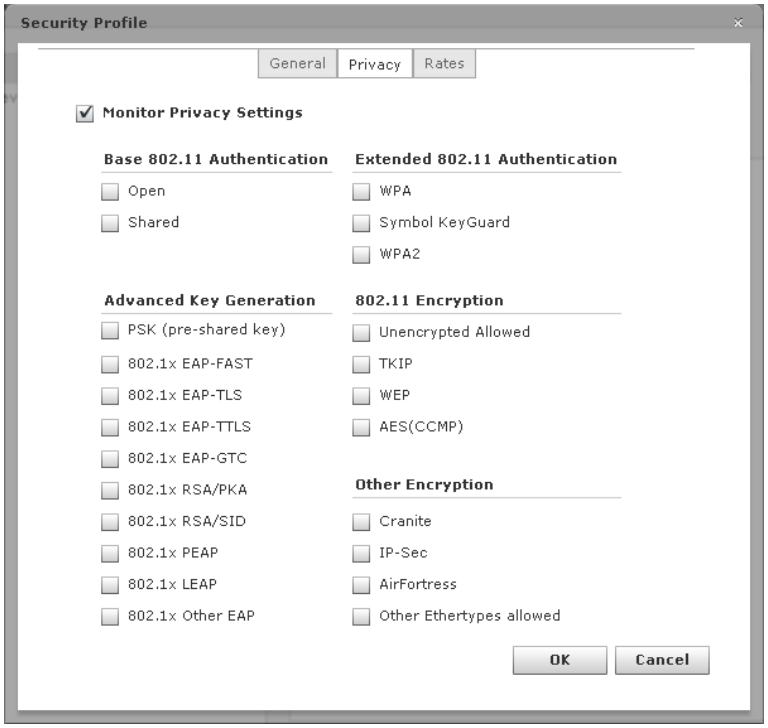
要访问安全配置文件，请转至**配置 > 安全性和合规性 > 安全配置文件**。然后单击“新建模板”按钮以添加新配置文件。再使用“常规”、“加密”和“速率”选项卡定义您的安全配置文件。定义您的安全配置文件后，单击“确定”以保存您的配置文件或“取消”以退出，不保存配置文件。



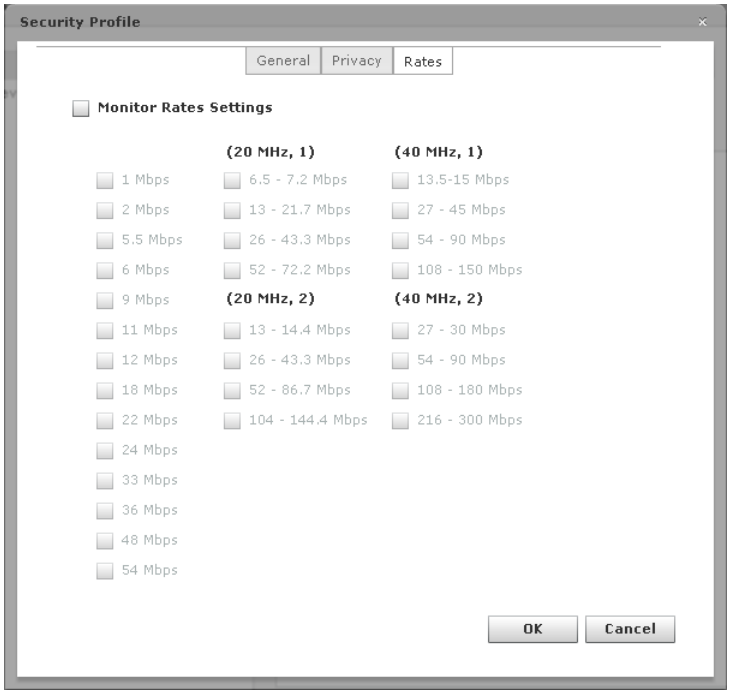
常规选项卡用于命名安全配置文件并指定是否要使用某些功能。



加密选项卡包含可用于输入有关传输加密的设置的选项。



速率选项卡用于选择供 BSS 使用的发射和接收数据速率。



实验设置和先决条件

使用在 AP 上预配置的两个网络。第一个网络为 WLAN_CORP，第二个网络为 Guest。以下为设置。

接入点 1

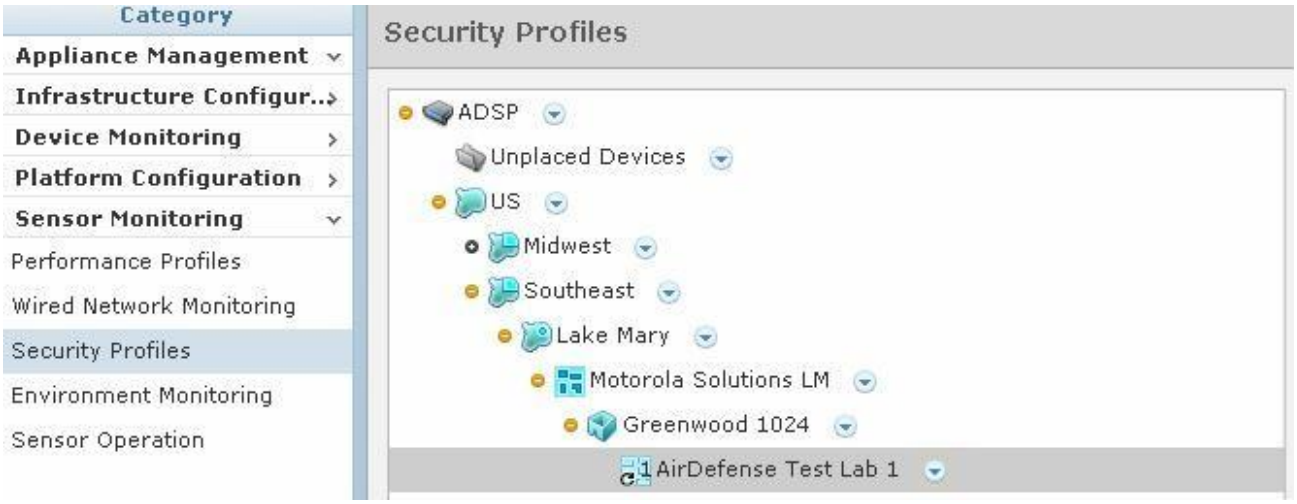
- SSID：WLAN_CORP
- 802.11a/n
- 身份验证：无
- 加密：WPA-PSK

接入点 2

- SSID：Guest
- 802.11a/n
- 身份验证：无
- 加密：无

实验

使用安全配置文件来定义无线 LAN 中经批准的无线设备的安全配置。
要访问安全配置文件，请转至**配置 > 安全性和合规性 > 安全配置文件**。



1. 现在，转至您的实验设备所在的子文件夹，然后继续定义分类规则。
2. 现在，选择“新建模板”，将出现“新建配置文件”屏幕。



以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：https://d.book118.com/938014134066006026