初始配置步骤FireSIGHT系统

目录

简介

在您再镜像FireSIGHT管理中心或FirePOWER设备后，您需要完成几个步骤使系统充分地运行和生成入侵事件的警报;例如，安装许可证，注册设备，应用卫生政策、系统策略、访问控制策略，入侵策略等。本文是补充对于FireSIGHT系统安装指南。

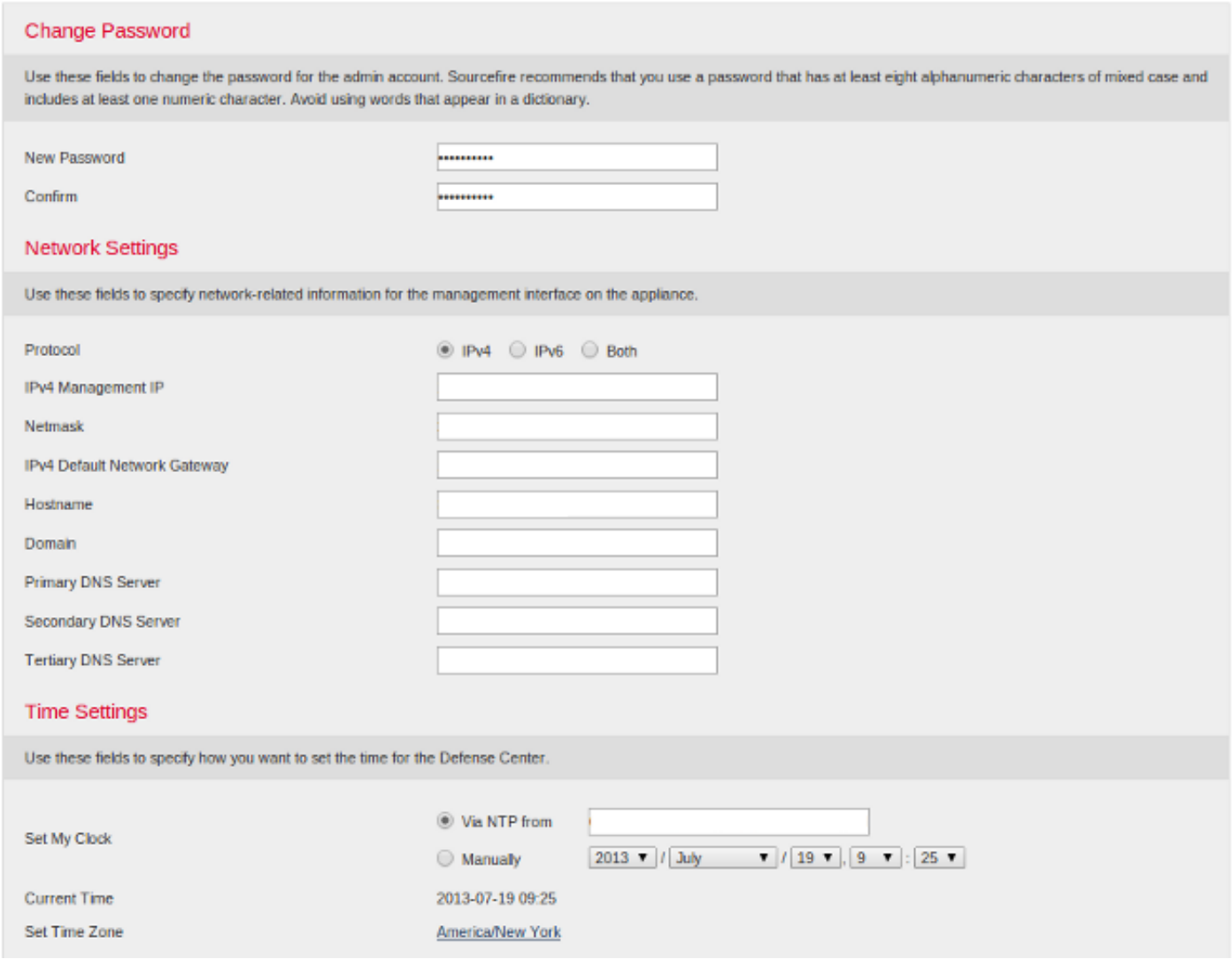
前提条件

此指南假设，您仔细阅读FireSIGHT系统安装指南。

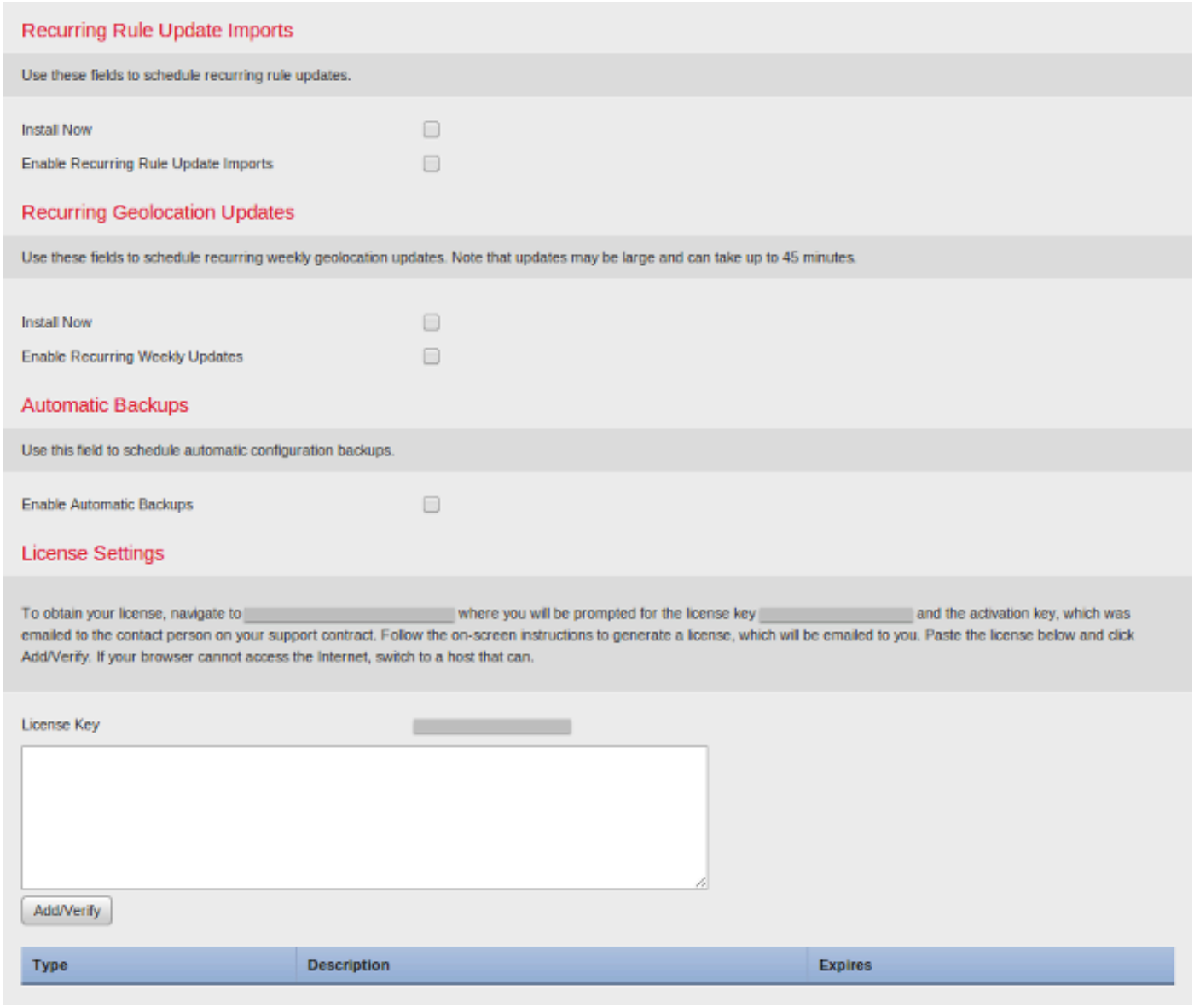
配置

步骤 1：初始设置

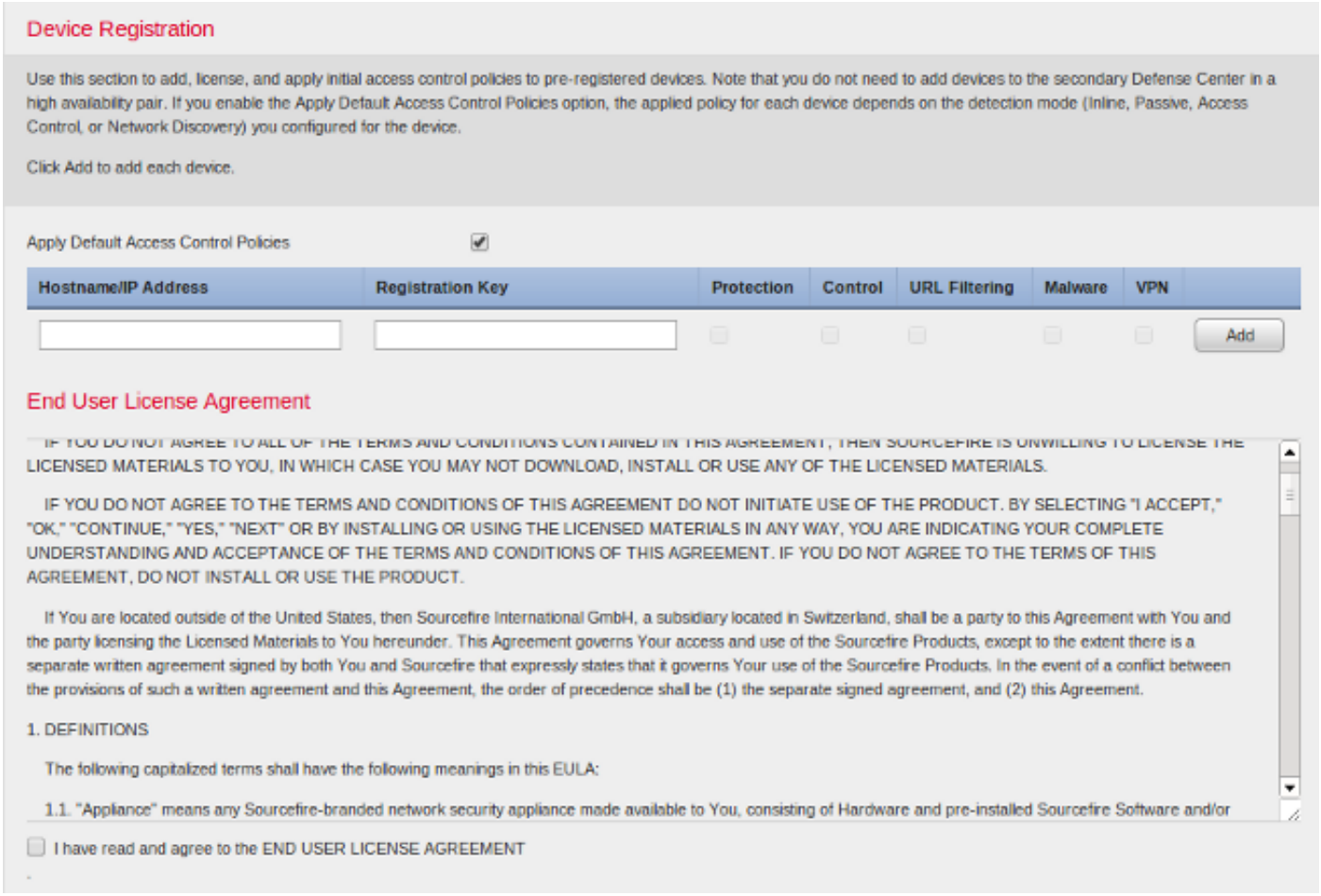
在您的FireSIGHT管理中心，您必须通过登录Web接口和指定在设置页的初始配置选项完成安装过程，如下所示。在此页，您必须更改管理员密码，并且能也指定网络设置例如域和DNS服务器和时间配置。



您能或者配置循环规则和geolocation更新以及自动备份。所有功能许可证可能这时也安装。



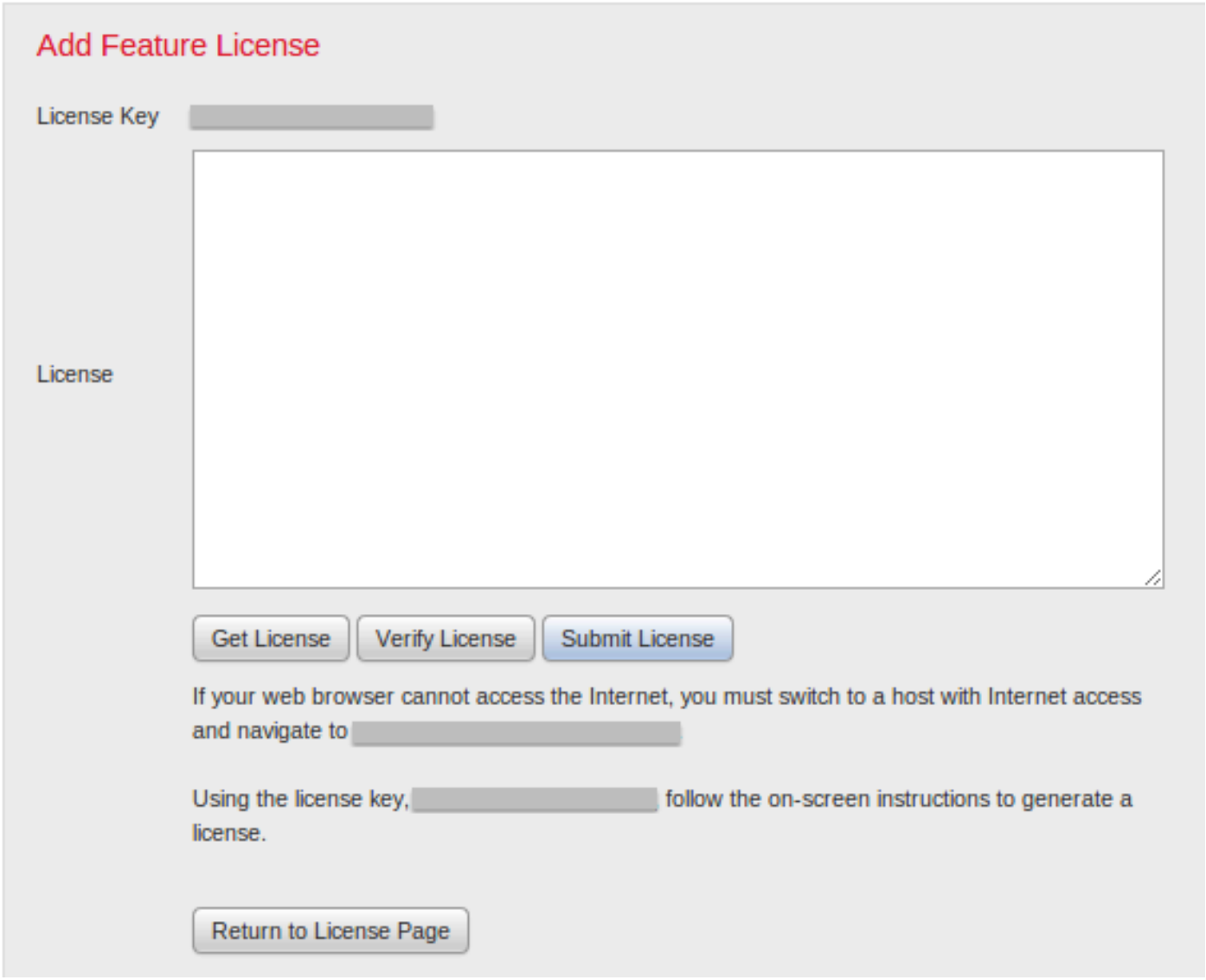
在此页，您能也注册设备到FireSIGHT管理中心和指定检测模式。您在注册时选择的检测模式和其它选项确定系统创建的默认接口、轴向集和区域，以及最初适用于受管理设备的策略。



步骤 2：安装许可证

在初始设置页期间，如果没有安装许可证，您能通过遵从这些步骤完成任务：

- 导航对以下页：**系统>许可证。**
- 单击**添加新的许可证。**



如果没有收到许可证，请与您的帐户联系销售代表。

步骤 3：运用系统策略

系统策略指定验证配置文件的在FireSIGHT管理中心和受管理设备之间的配置和时间同步。 要配置或运用系统策略请导航到**系统>本地>System策略**。 提供默认系统策略，但是需要应用到所有受管理设备。

步骤 4：运用卫生政策

卫生政策用于配置受管理设备如何他们的健康状态向FireSIGHT管理中心报告。 要配置或运用卫生政策请导航对**健康>卫生政策**。 提供默认卫生政策，但是需要应用到所有受管理设备。

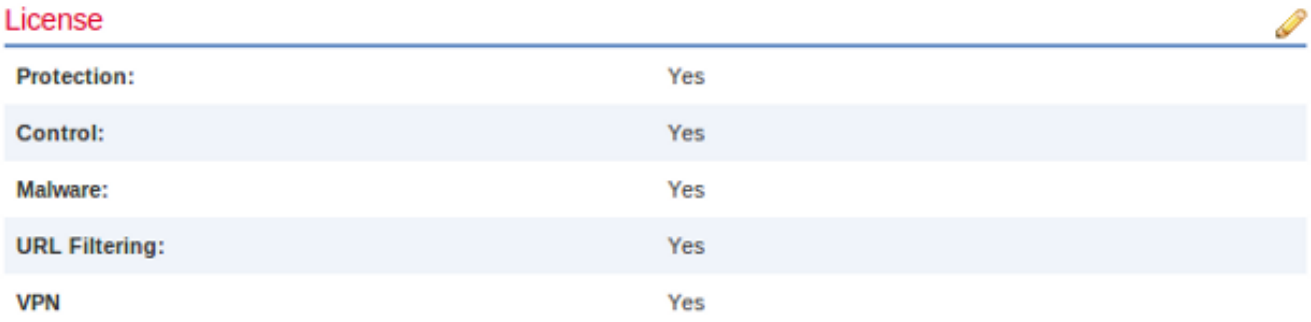
步骤 5：寄存器受管理设备

在初始设置页期间，如果没有注册设备，请读说明的本文关于怎样注册设备到FireSIGHT管理中心。

步骤 6：Enable (event)已安装许可证

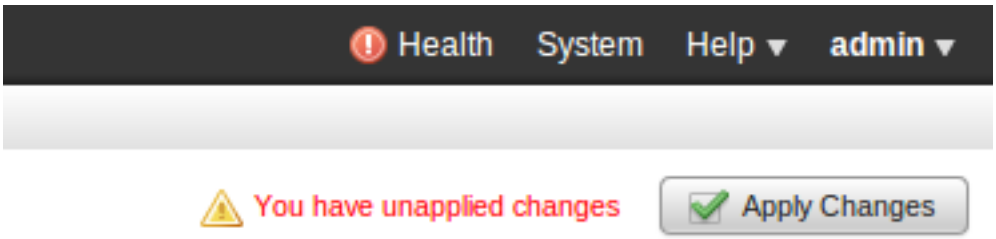
在您能使用在您的设备前的所有功能许可证，您需要为每受管理设备启用它。

1. 导航对以下页：**设备>设备管理**。
2. 点击您要启用许可证并且参与设备选项卡的设备。
3. 在许可证旁边单击**编辑**(*铅笔*图标)。



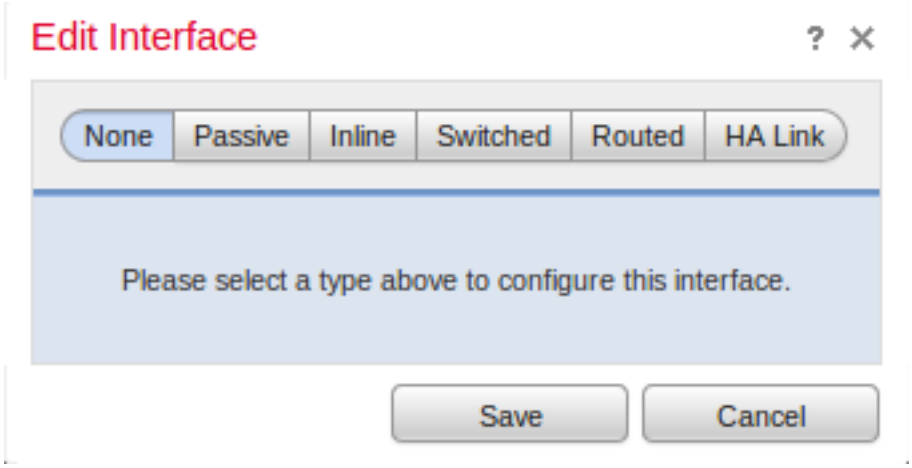
启用此设备的需要的许可证并且点击**"Save"**。

注意消息"*您有未应用的更改*"在右上角。此警告依然是活动，即使您导航远离设备管理页，直到您点击**应用更改**按钮。



步骤 7：配置感觉接口

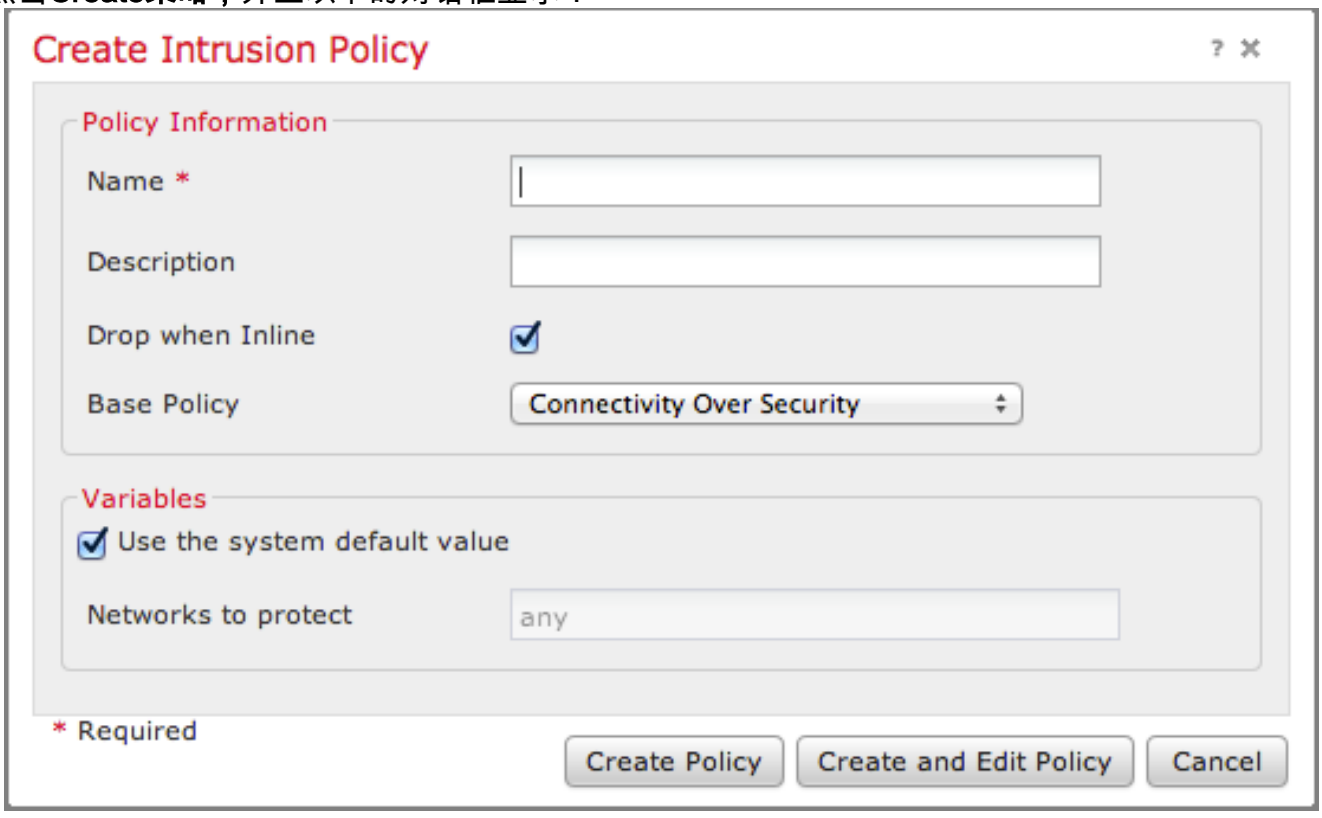
1. 导航对以下页**设备>设备管理**。
2. 点击您的选择传感器的**编辑**(铅笔)图标。
3. 在**接口下请**选中，点击**Edit图标**您的选择接口的。



选择一个被动或轴向接口配置。交换式和路由接口请是超出此条款的范围之外。

步骤 8:配置入侵策略

- 导航对以下页： **策略>入侵>入侵策略。**
- 点击**Create策略**，并且以下的对话框显示：



您必须分配名称和定义将使用的基本策略。根据您能的您的部署选择有选项**丢弃，当线型**启用。定义您要保护减少错误肯定和改进系统的性能的网络。

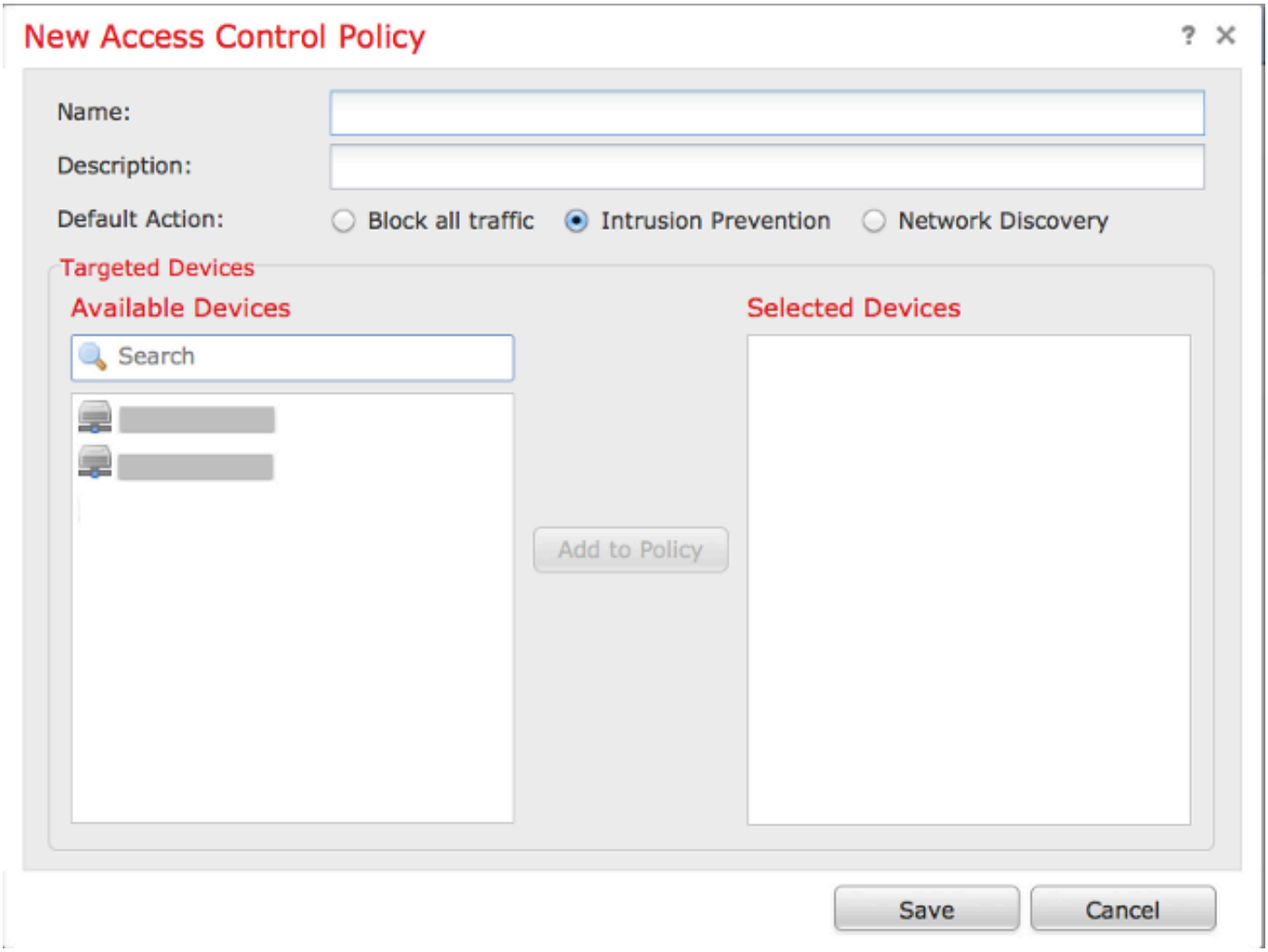
单击在**Create策略将**保存您的设置并且创建IPS策略。 如果要做对入侵策略的任何修改，您能选择**创建并且编辑策略**。

> **注意**：作为访问控制策略一部分，入侵策略应用。 在入侵策略应用后，所有修改可以应用，无需重新应用全部的访问控制策略通过单击**重新应用**按钮。

步骤 9：设定及适用访问控制策略

1. 导航到**策略>访问控制**。

2. 点击**新建的策略**。

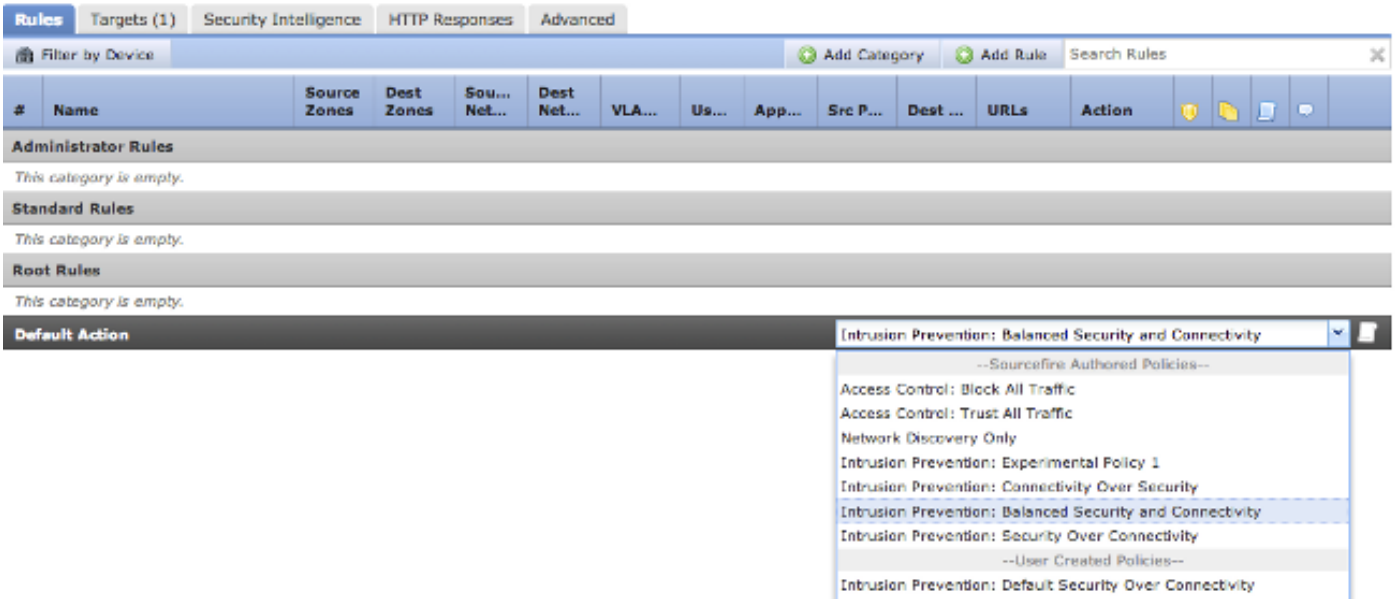


3. 为策略和**说明**提供一**名称**。

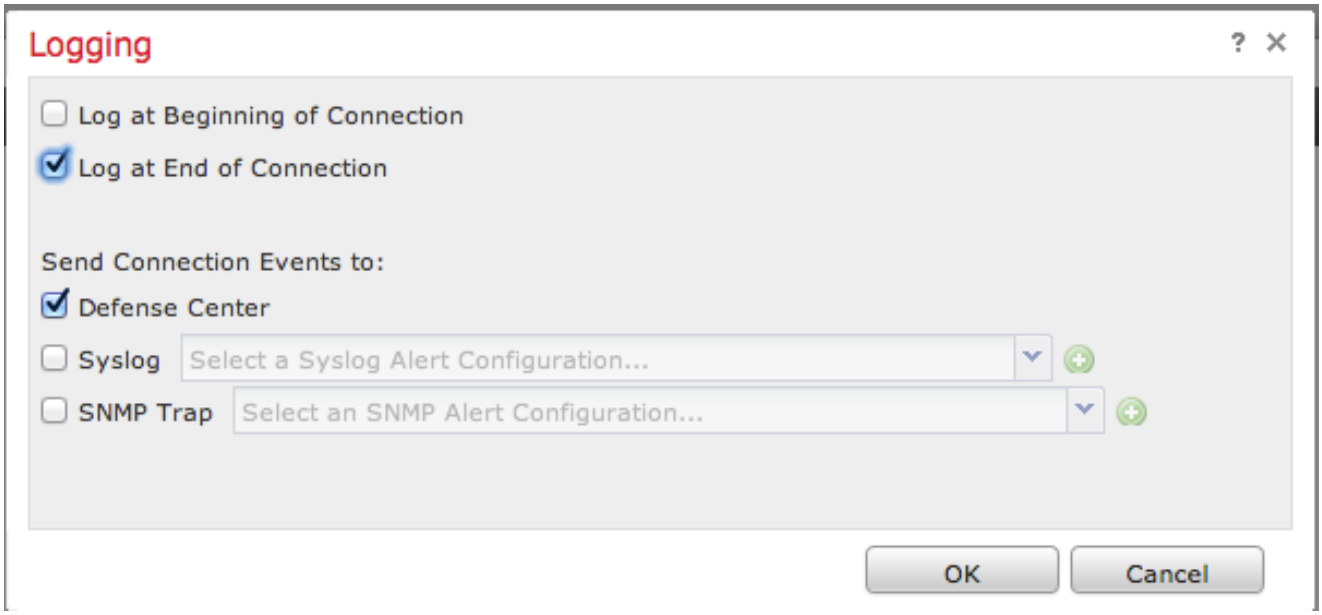
4. 选择**入侵防御**作为访问控制策略的**默认操作**。

5. 最终请选择您要适用于访问控制策略的**目标设备**，并且点击**“Save”**。

6. 选择您的默认操作的入侵策略。



7. 必须启用连接记录日志生成连接事件。单击是**默认操作的**权利的下拉菜单。



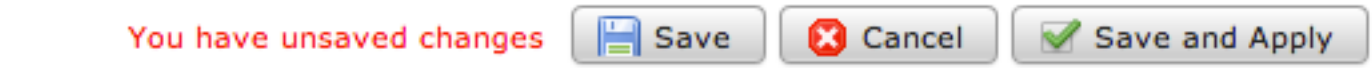
8. 选择记录连接在开始或连接的结束。事件可以被注册FireSIGHT管理中心，一个Syslog位置，或者通过SNMP。

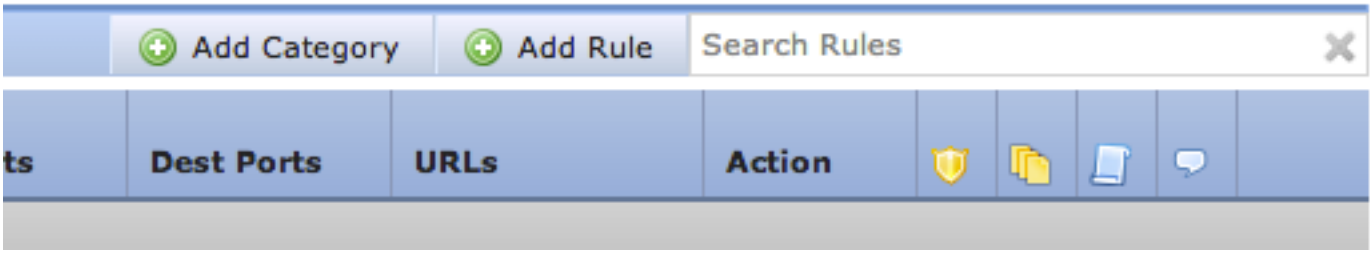
> **注意**：没有推荐记录在连接的两端，因为每连接(除了阻止连接)两次将被记录。首先记录为将阻塞的连接是有用的，并且在末端的记录日志为其他连接是有用的。

9. 单击 **Ok**。注意记录日志图标的颜色更改。

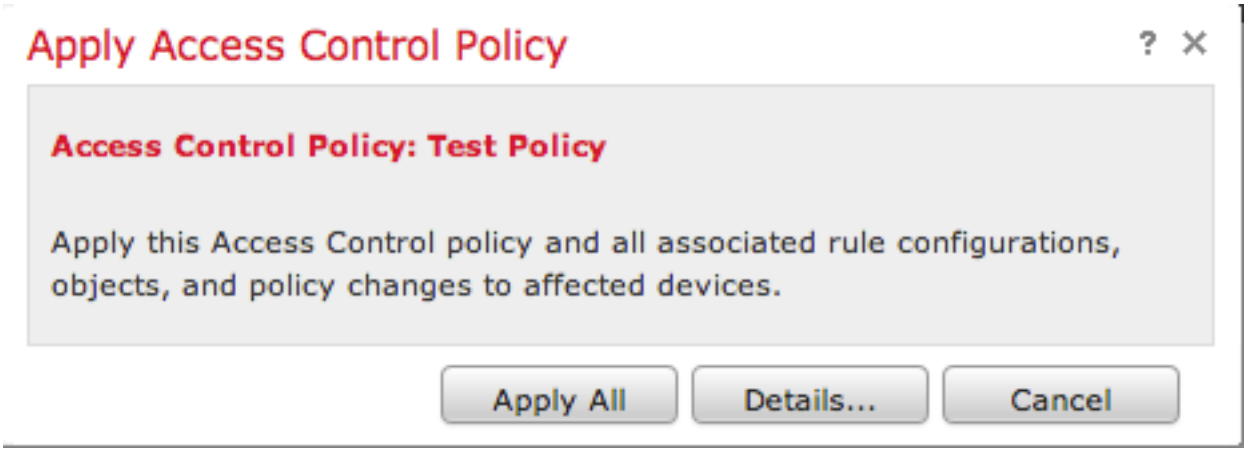
10. 您可以此时增加**访问控制规则**。您能使用的选项取决于您安装许可证的种类。

11. 当您完成时进行更改。点击**"Save"和应用按钮**。 您将注意消息指示您有在您的策略的未获救的更改在右上角，直到按钮点击。





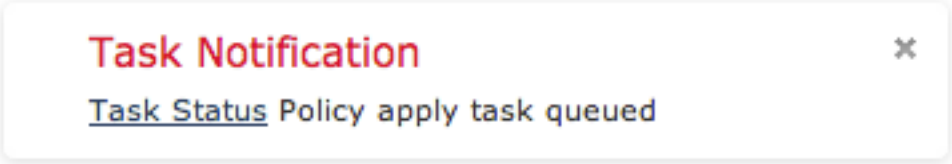
您能选择只**保存**更改或点击**"Save"和应用。** 如果选择后者，以下窗口将出现。



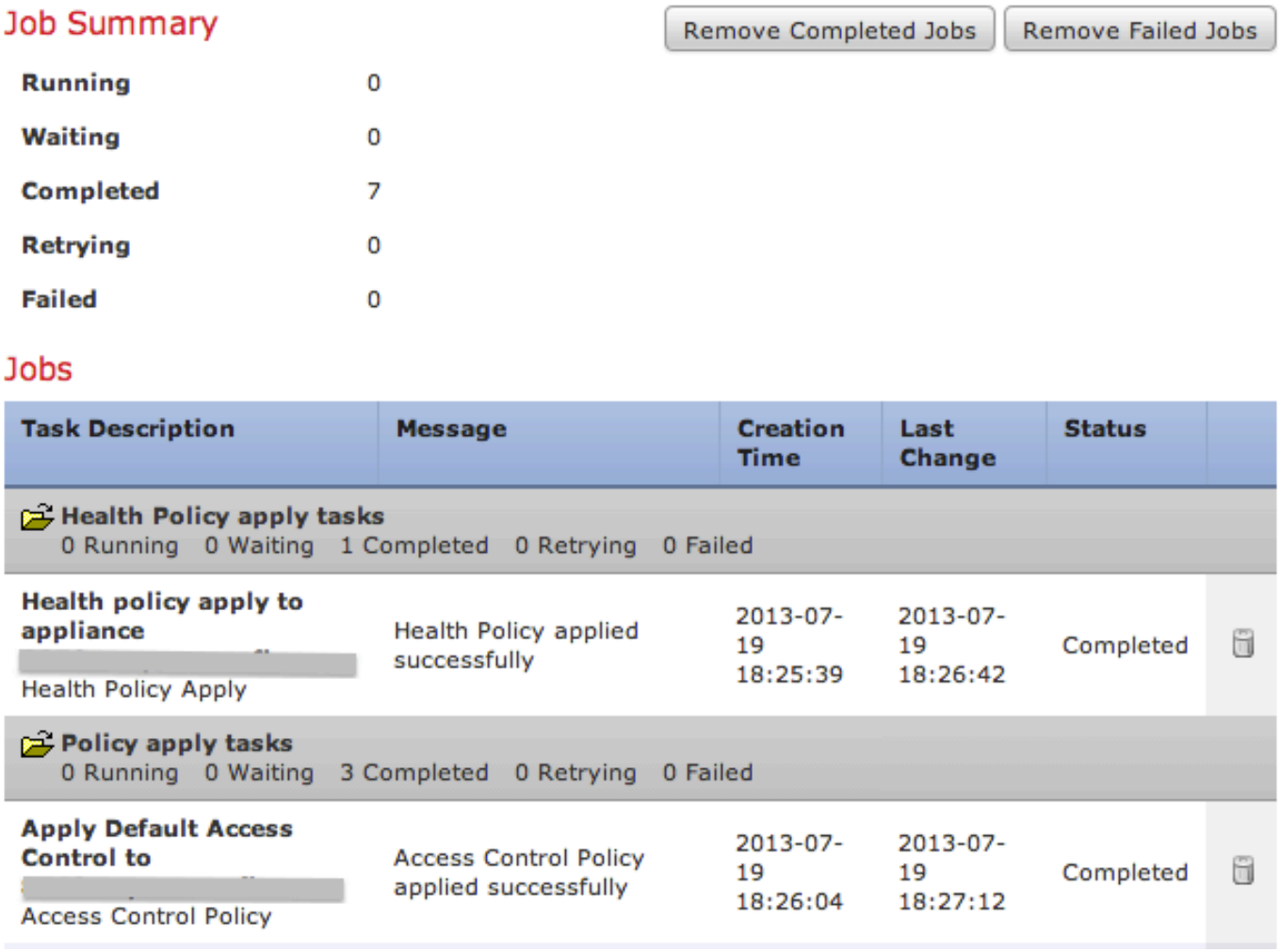
12. **运用所有将**适用于访问控制策略和所有相关的入侵策略目标设备。

注意：如果入侵策略第一次将应用，不可能取消选择。

13. 您能监控单击在导航显示的在页顶部，或者通知的**任务状态**链路的任务的状况对：**系统> Monitoring>任务状态**



14. 点击任务状态链路监控访问控制策略的进度应用。



步骤 10：如果FireSIGHT管理中心接收事件，请验证

在访问控制策略应用完成后，您应该根据流量入侵事件开始看到连接事件和。

其它建议

您能也配置在您的系统的以下其它功能。请参考用户指南关于实施细节。

- 定期备份
- 自动软件更新、SRU、VDB和GeoLocation下载/安装。
- 外部验证通过LDAP或RADIUS