FireSIGHT系统的初始配置步骤

目录

简介

重新映像FireSIGHT管理中心或FirePOWER设备后，需要完成几个步骤，使系统完全正常运行并生成入侵事件警报；例如，安装许可证、注册设备、应用运行状况策略、系统策略、访问控制策略、入侵策略等。本文档是对《FireSIGHT系统安装指南》的补充。

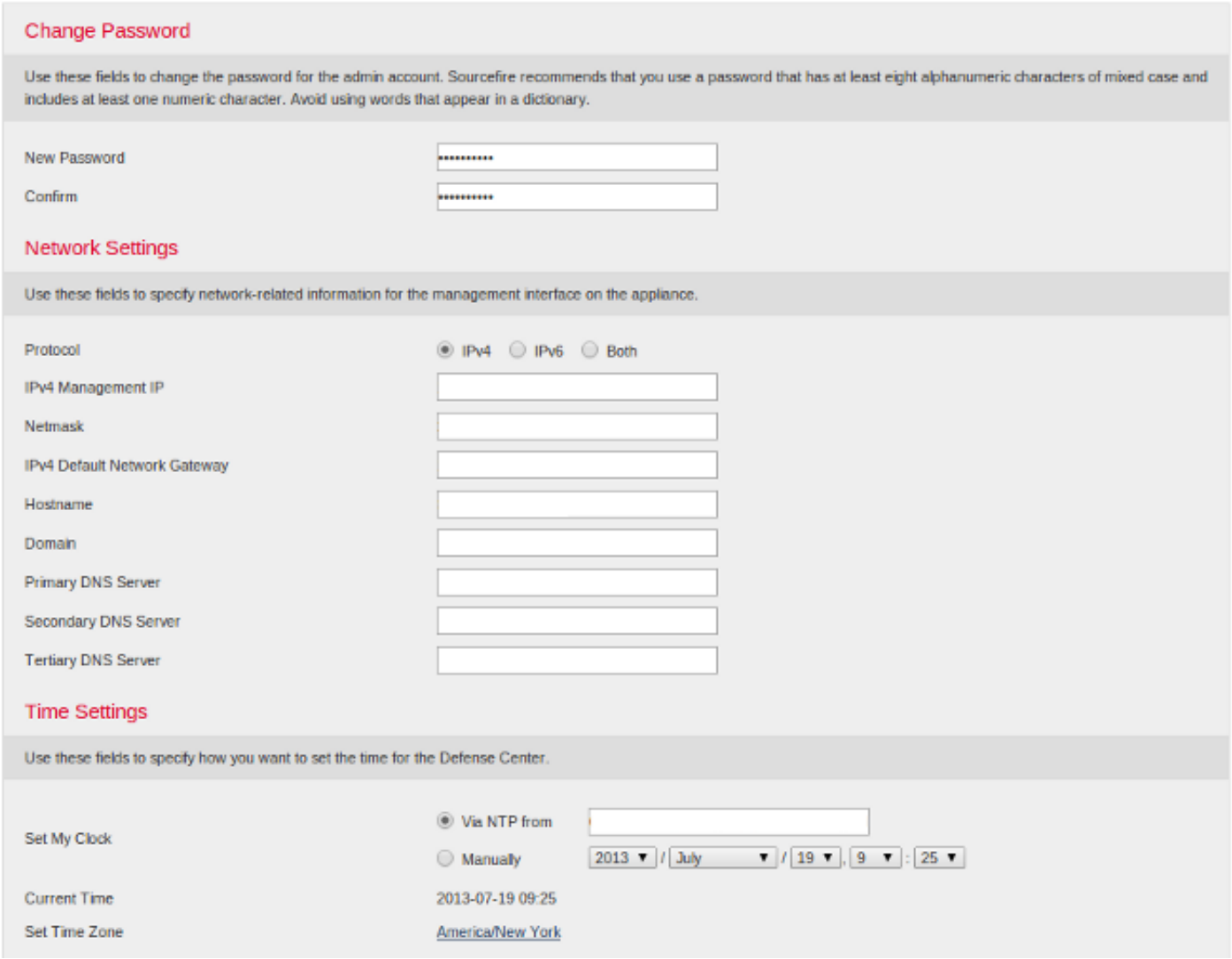
先决条件

本指南假定您已仔细阅读《FireSIGHT系统安装指南》。

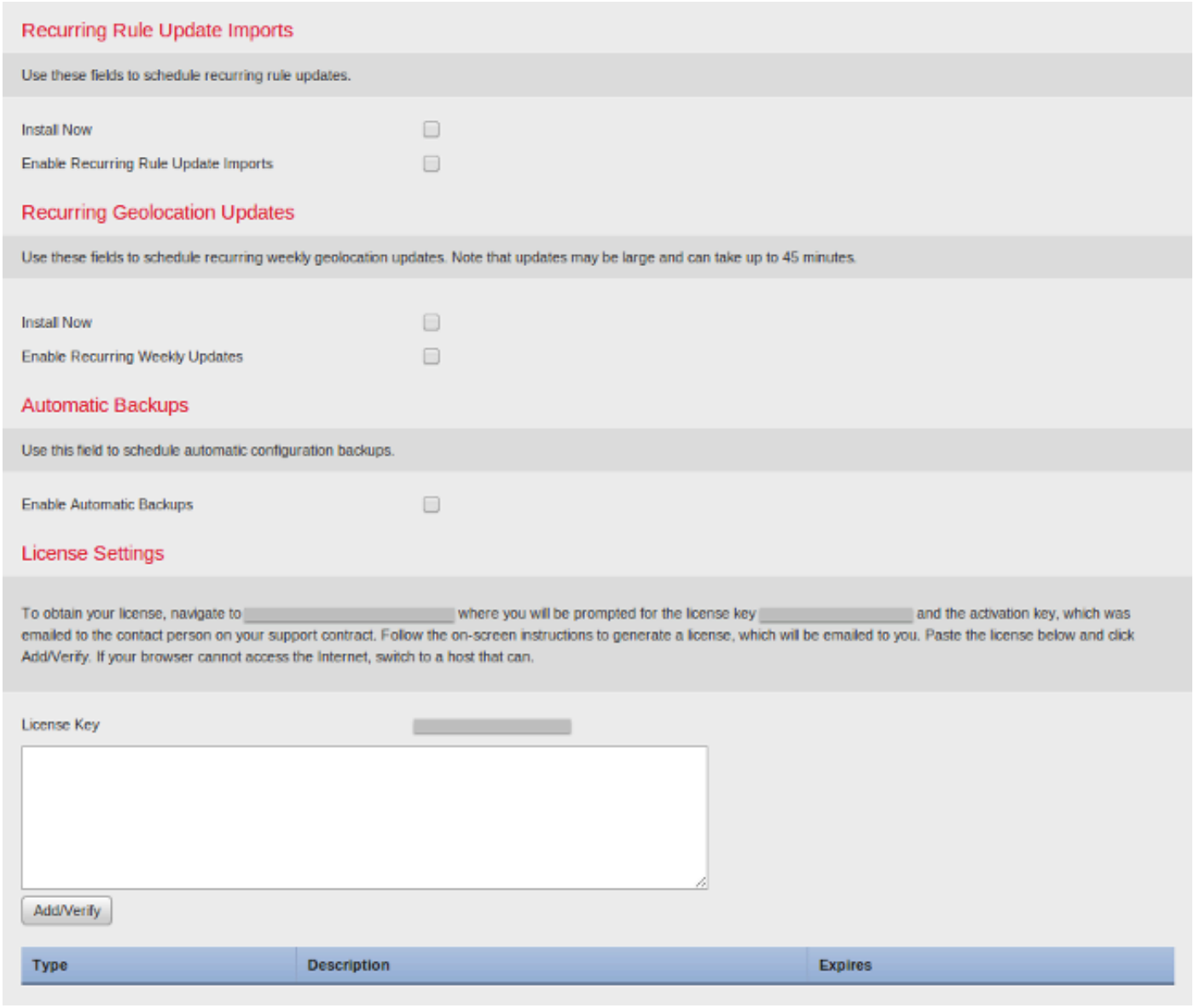
配置

步骤 1：初始设置

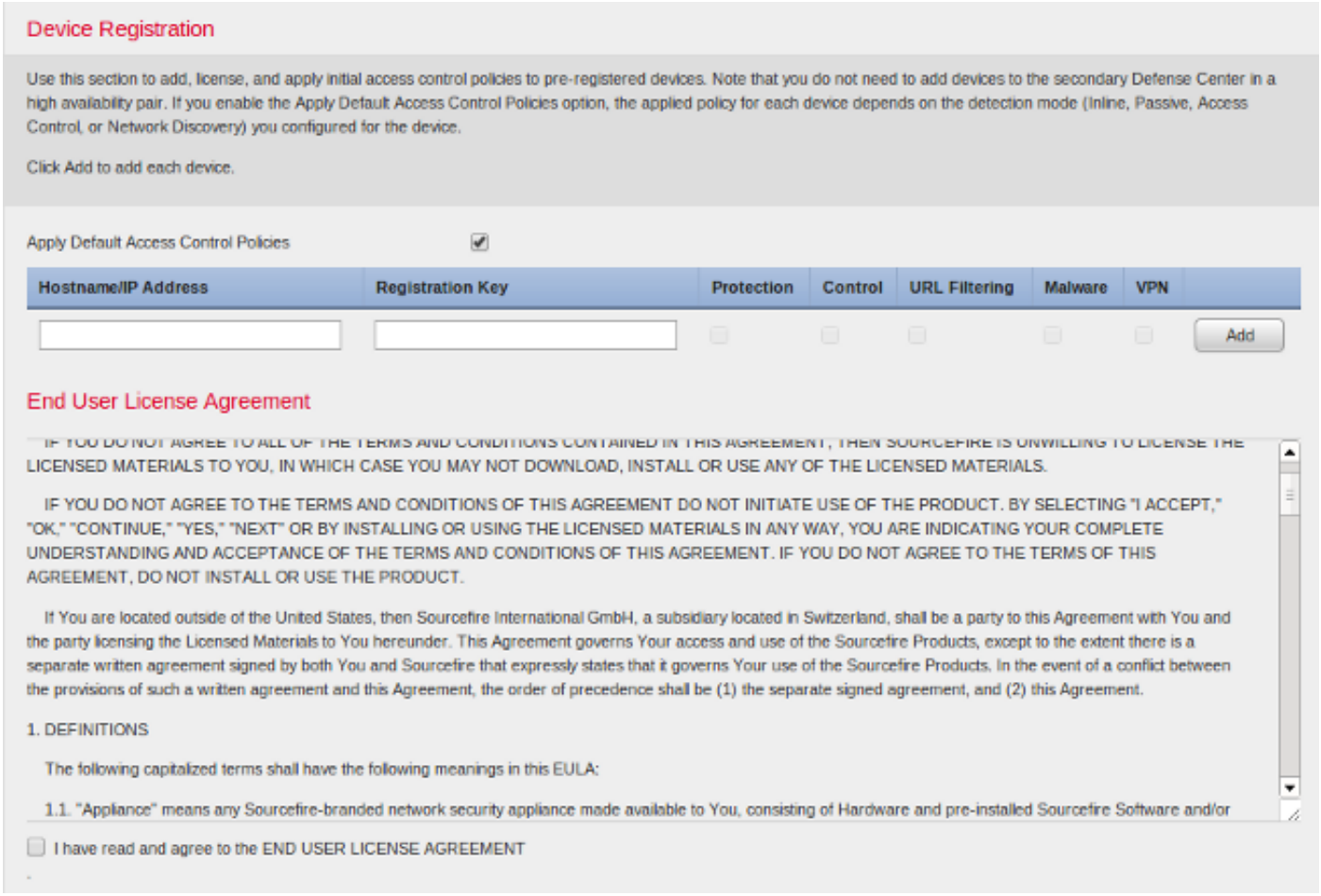
在FireSIGHT管理中心上，您必须通过登录网络界面并在设置页面上指定初始配置选项来完成设置过程，如下所示。在此页面上，您必须更改管理员密码，还可以指定网络设置（如域和DNS服务器）和时间配置。



您可以选择配置周期性规则和地理位置更新以及自动备份。此时也可以安装任何功能许可证。



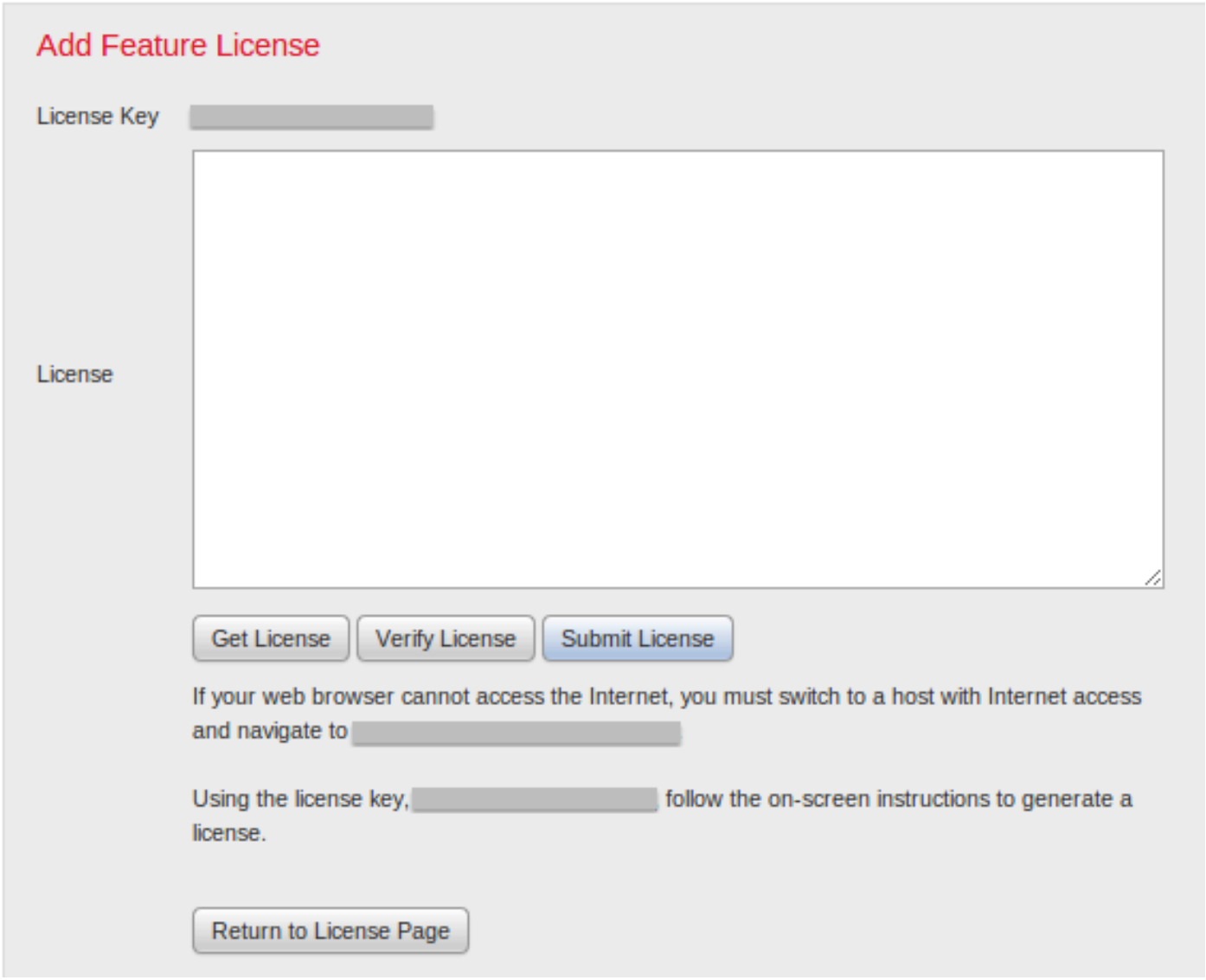
在此页上，您还可以将设备注册到FireSIGHT管理中心并指定检测模式。在注册期间选择的检测模式和其他选项决定系统创建的默认接口、内联集和区域，以及最初应用于受管设备的策略。



步骤 2：安装许可证

如果在初始设置页面中未安装许可证，可以按照以下步骤完成任务：

- 导航至以下页面：**系统>许可证**。
- 单击“添**加新许可证**”。



如果您未收到许可证，请联系您帐户的销售代表。

步骤 3：应用系统策略

系统策略指定FireSIGHT管理中心和受管设备之间的身份验证配置文件和时间同步的配置。 要配置或应用系统策略，请导航至**System > Local > System Policy**。 系统会提供默认系统策略，但需要应用于任何受管设备。

步骤 4：应用运行状况策略

运行状况策略用于配置受管设备向FireSIGHT管理中心报告其运行状况的方式。 要配置或应用运行状况策略，请导航至**运行状况>运行状况策略**。 提供默认运行状况策略，但需要应用于任何受管设备。

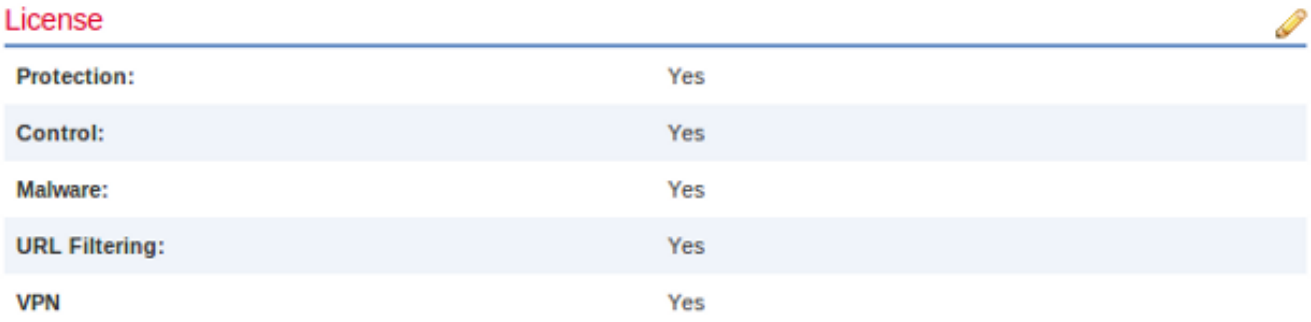
步骤 5：注册受管设备

如果在初始设置页面未注册设备，请阅读本文档，了解如何将设备注册到FireSIGHT管理中心。

步骤 6：启用已安装的许可证

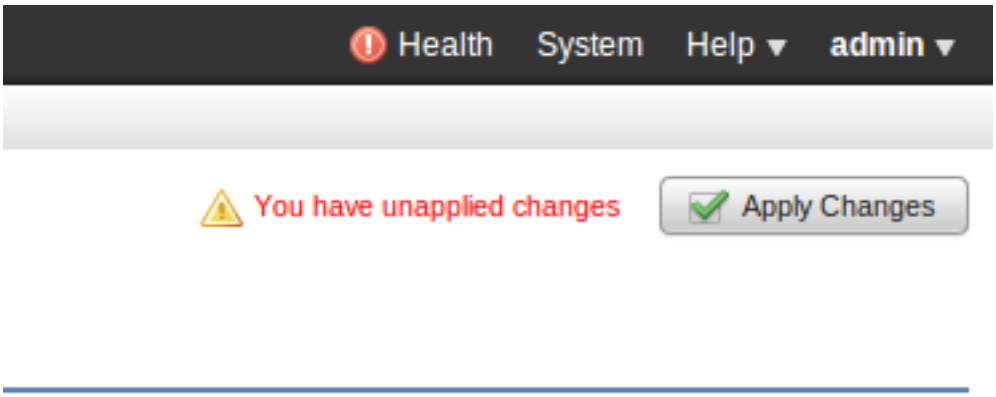
在设备上使用任何功能许可证之前，需要为每个受管设备启用该许可证。

1. 导航至以下页面：**Devices（设备）> Device Management(设备管理)**。
2. 点击要为其启用许可证的设备，然后输入设备选项卡。
3. 单击“License(许**可证)**”旁边的*Edit(*铅笔图标)。



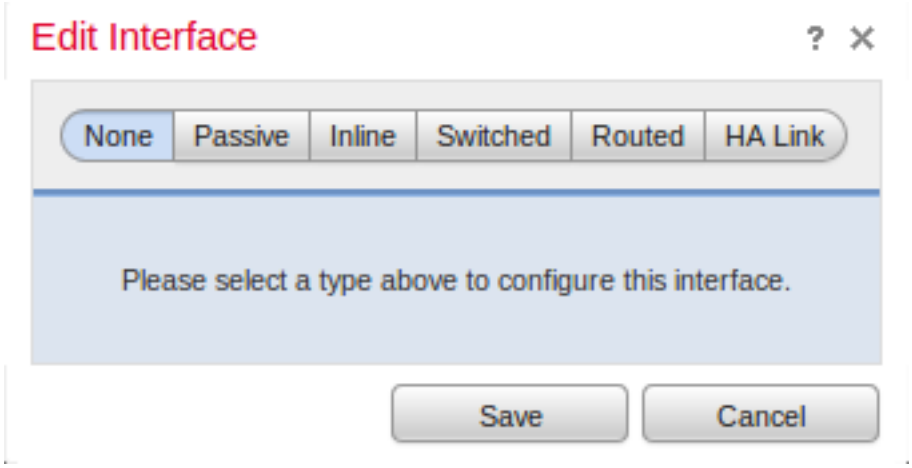
启用此设备所需的许可证，然后单击**Save**。

注意右上角*的消息*“You have unapplied changes”。此警告保持活动状态，即使您从设备管理页导航到单击“应用更改”**按钮**为止。



步骤 7：配置感应接口

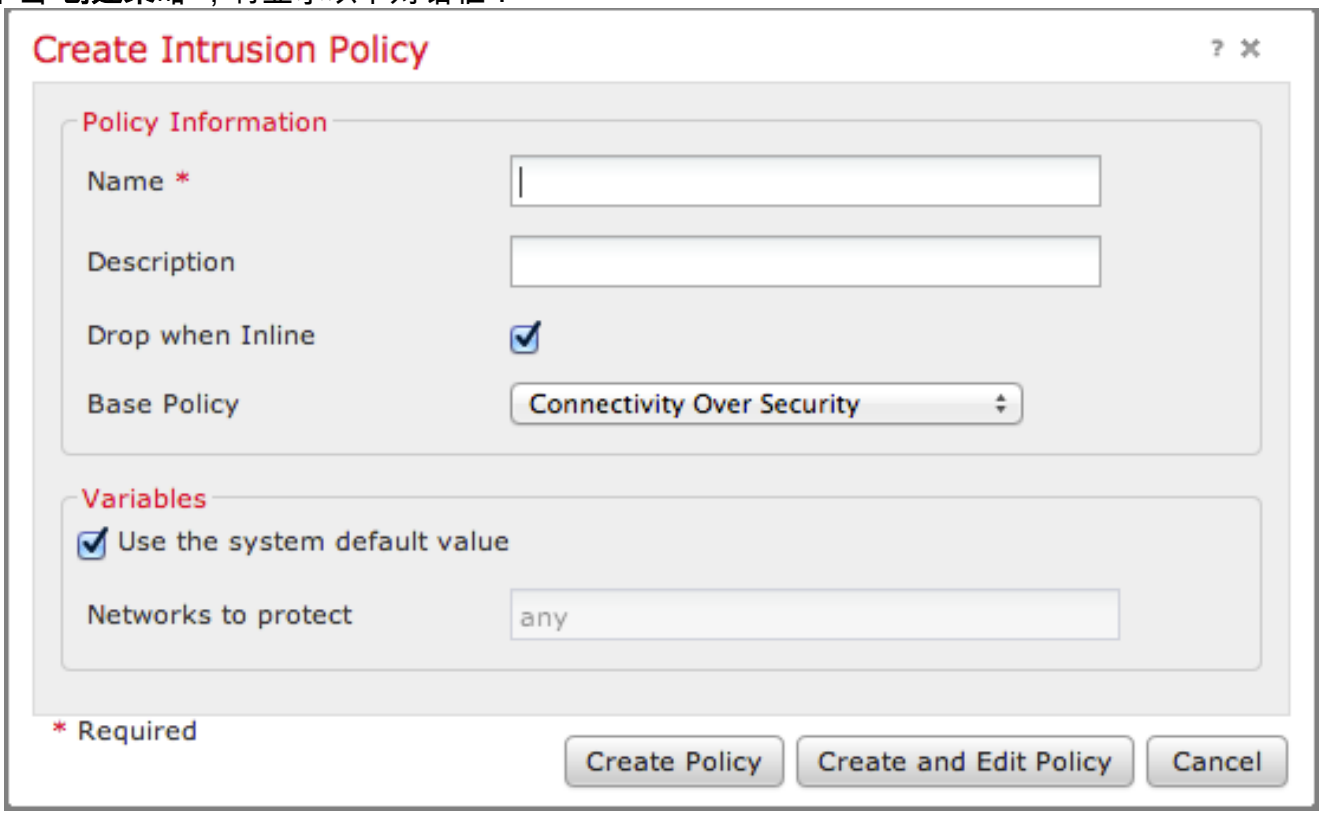
1. 导航至以下页**Devices > Device Management**。
2. 单击所选传感器的**编辑**（铅笔）图标。
3. 在“接口**”选**项卡下，单击**所**选接口的编辑图标。



选择被动或内联接口配置。交换接口和路由接口不在本文的讨论范围之内。

步骤 8::配置入侵策略

- 导航至以下页面：**Policies > Intrusion > Intrusion Policy。**
- 单击“**创建策**略”，将显示以下对话框：



您必须分配名称并定义要使用的基本策略。根据部署，您可以选择启用“内联时**丢弃”选**项。定义要保护的网络，以减少误报并提高系统性能。

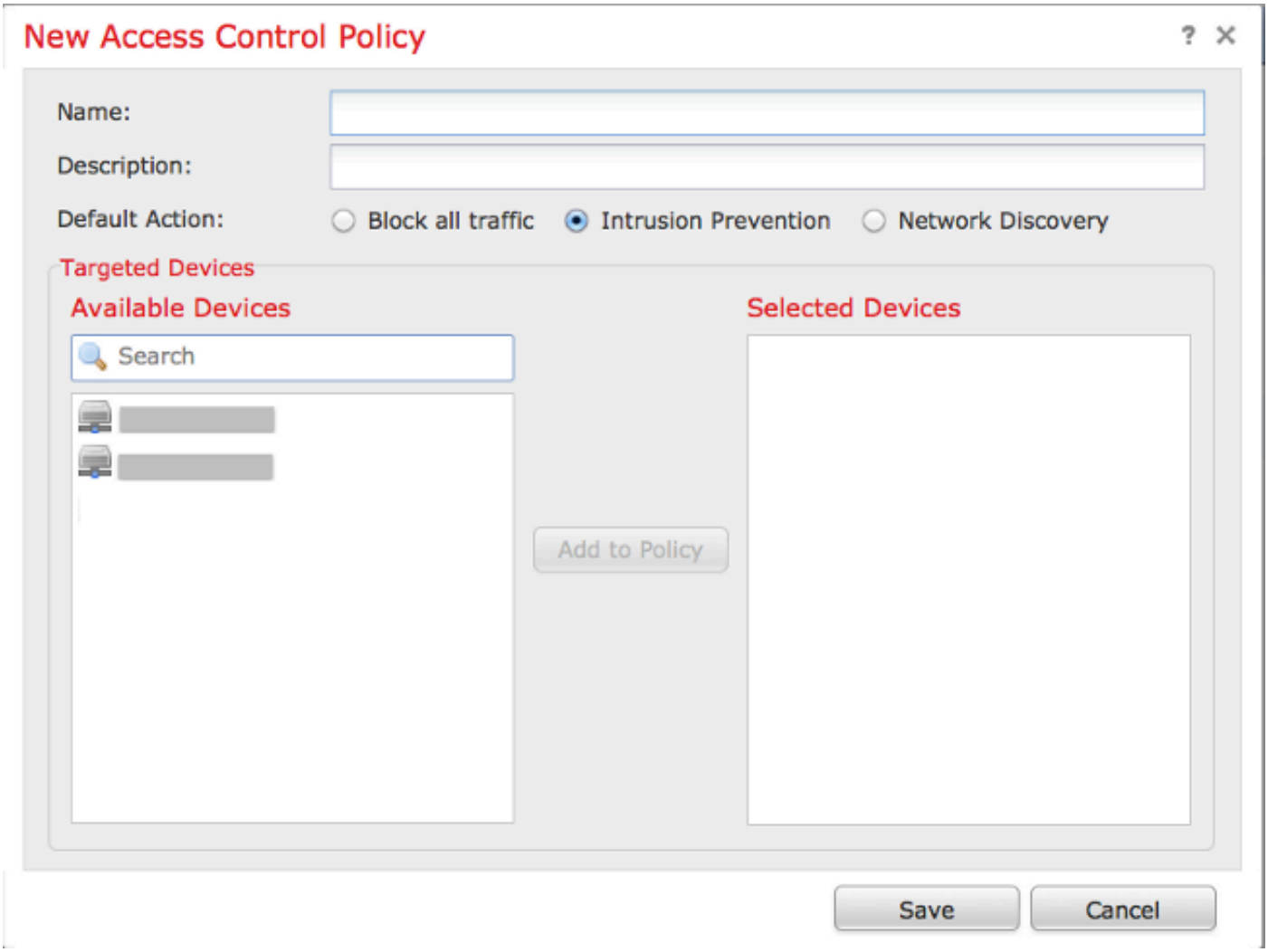
单击**创建**策略将保存设置并创建IPS策略。如果要对入侵策略进行任何修改，可以改**为创建和编**辑策略。

> **注意：**入侵策略作为访问控制策略的一部分应用。 应用入侵策略后，可以通过单击Reapply按钮应用任何修改，而无需重新应用整个访问控**制策**略。

步骤 9：配置并应用访问控制策略

1.导航至“策略”>“访问控制”。

2.单击“新策略”。

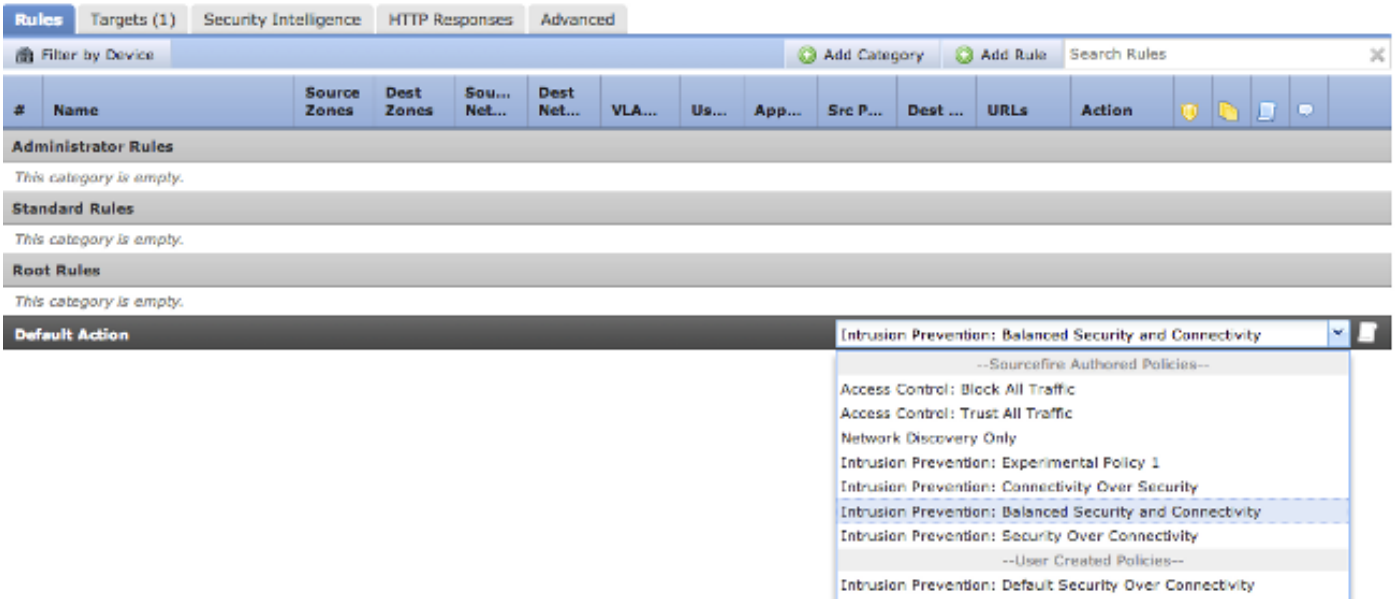


3.提供策略的名称和说明。

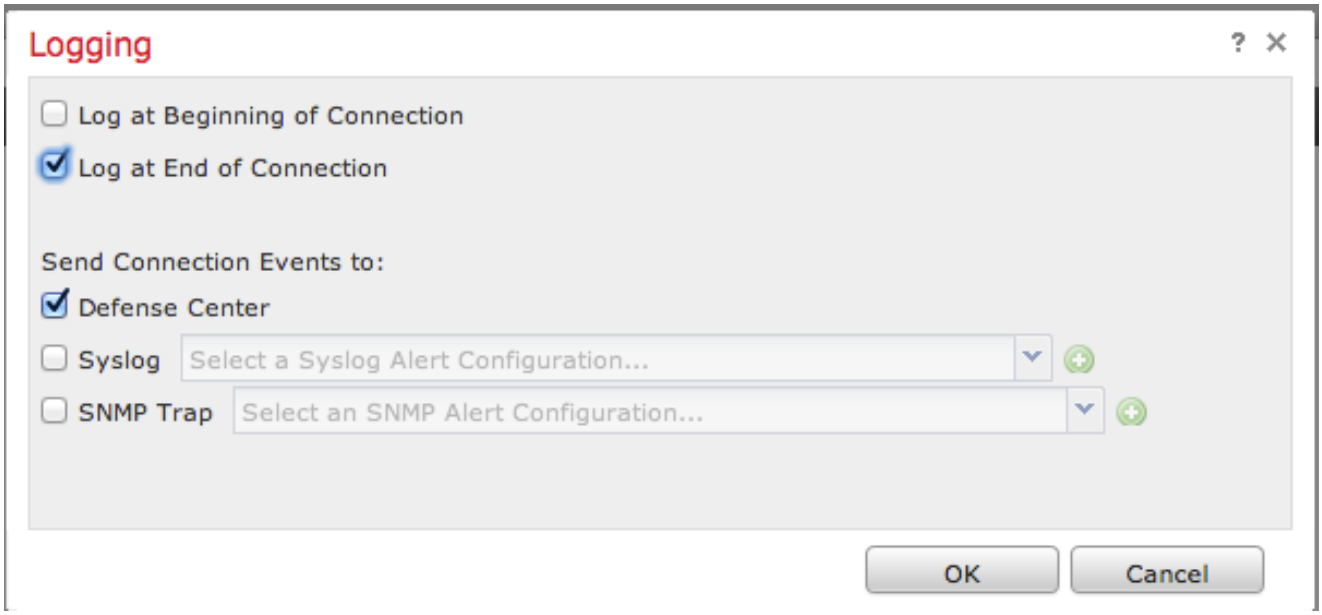
4.选择Intrusion Prevention作为Access Control策略的Default Action。

5.最后选择要应用访问控制策略的目标设备，然后单击保存。

6.为默认操作选择入侵策略。



7.必须启用连接日志记录才能生成连接事件。单击“默认操作”右侧的下**拉菜单**。



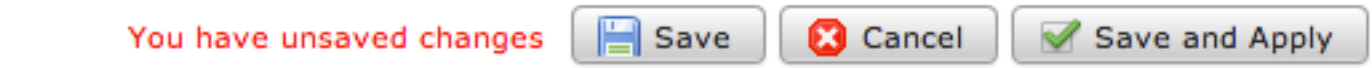
8.选择在连接开始或结束时记录连接。事件可以通过FireSIGHT管理中心、系统日志位置或SNMP进行记录。

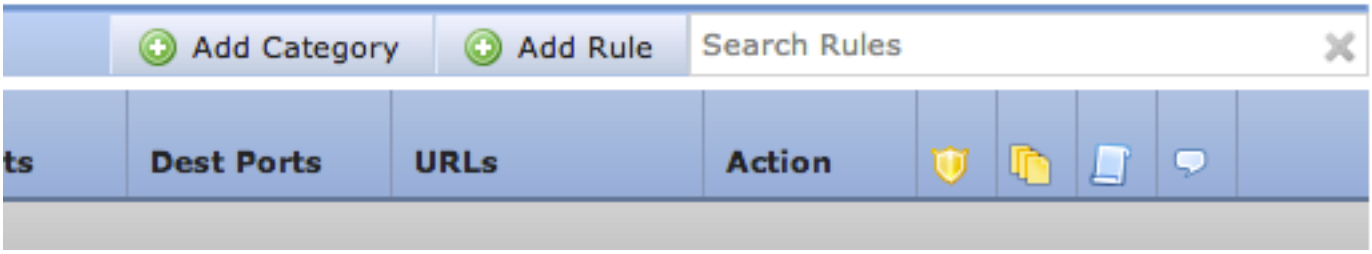
> **注意**：不建议在连接的两端记录，因为每个连接（阻塞的连接除外）将记录两次。在开始时记录对于将被阻止的连接非常有用，在结束时记录对于所有其他连接都有用。

9.单击“**确定**”。请注意，日志记录图标的颜色已更改。

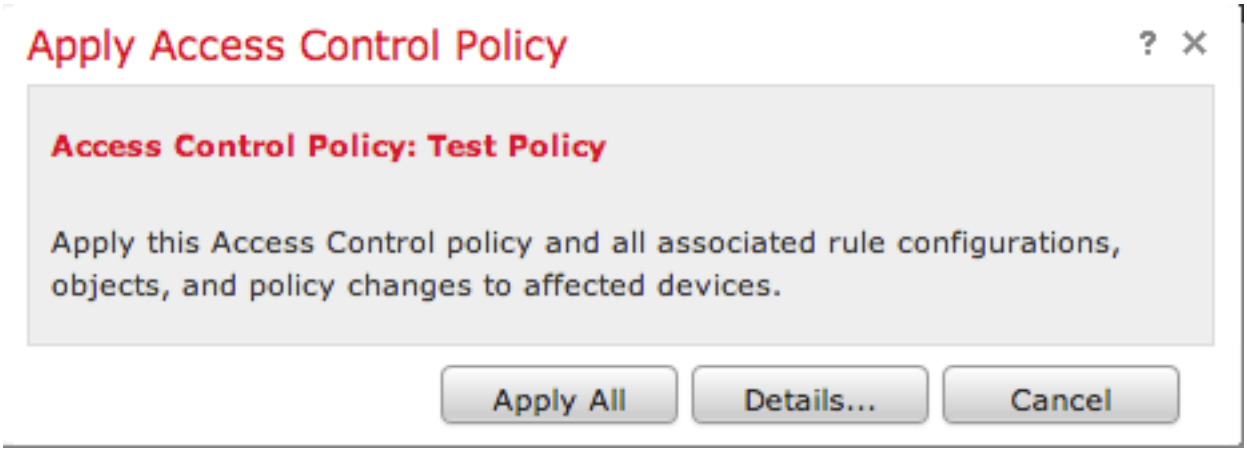
10.此时可以添**加访问**控制规则。可以使用的选项取决于您安装的许可证类型。

11.完成更改后。单击“保**存并应用**”按钮。 您会注意到一条消息，指示您在右上角有未保存的策略更改，直到单击该按钮。





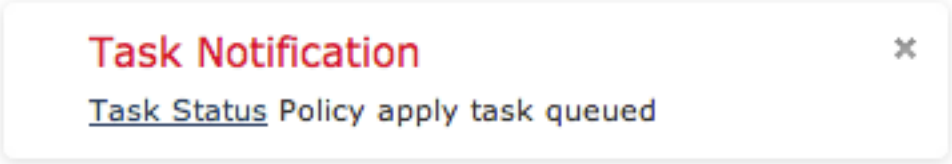
您可以选择仅保**存更**改或单击**保存并应**用。如果选择后者，将出现以下窗口。



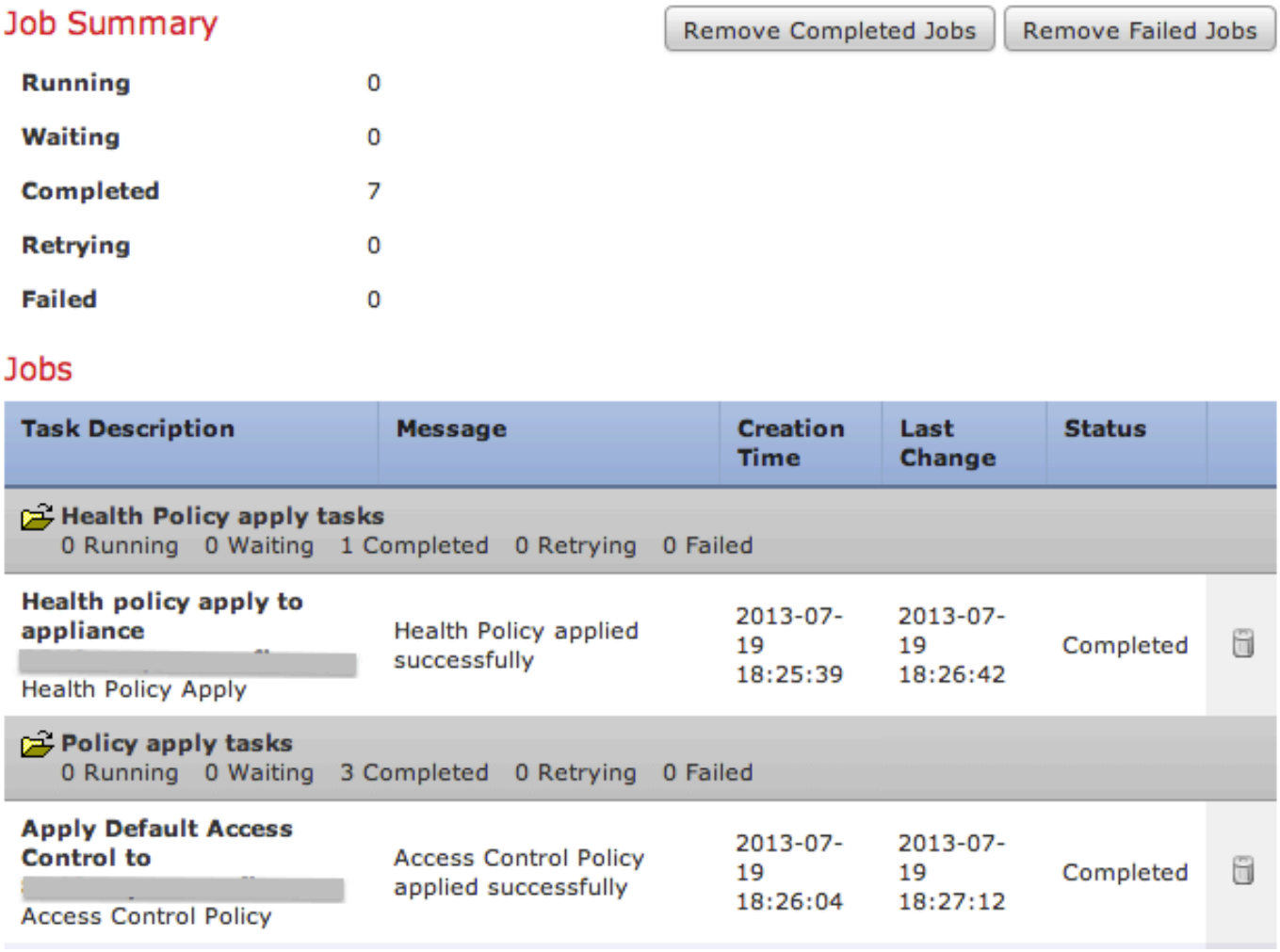
12. Apply All将将访问控制策略和任何关联的入侵策略应用到目标设备。

注意：如果入侵策略将首次应用，则无法取消选择。

13.单击页面顶部显示的通知上的“任务状态”链接，或导航到以下位置，可以监控任务的状态：**系统>监控>任务状态**



14.单击“任务状态”链接，监控应用访问控制策略的进度。



步骤 10：验证FireSIGHT管理中心是否收到事件

访问控制策略应用完成后，您应开始查看连接事件并根据流量入侵事件。

其他建议

您还可以在系统上配置以下附加功能。请参阅《用户指南》了解实施详细信息。

- 定时备份
- 自动软件更新、SRU、VDB和GeoLocation下载/安装。
- 通过LDAP或RADIUS进行外部身份验证