Шаги начальной конфигурации систем FireSIGHT

Содержание

Введение

После того, как вы повторно захватите образ Центр управления FireSIGHT или Устройство FirePOWER, необходимо выполнить несколько шагов, чтобы сделать систему полностью функциональной и генерировать предупреждения для событий проникновения; такой как, устанавливая лицензию, регистрируя устройства, применяя политику в области охраны здоровья, системную политику, политику контроля доступа, политика проникновения и т.д. Этот документ является дополнением к Руководству по установке системы FireSIGHT.

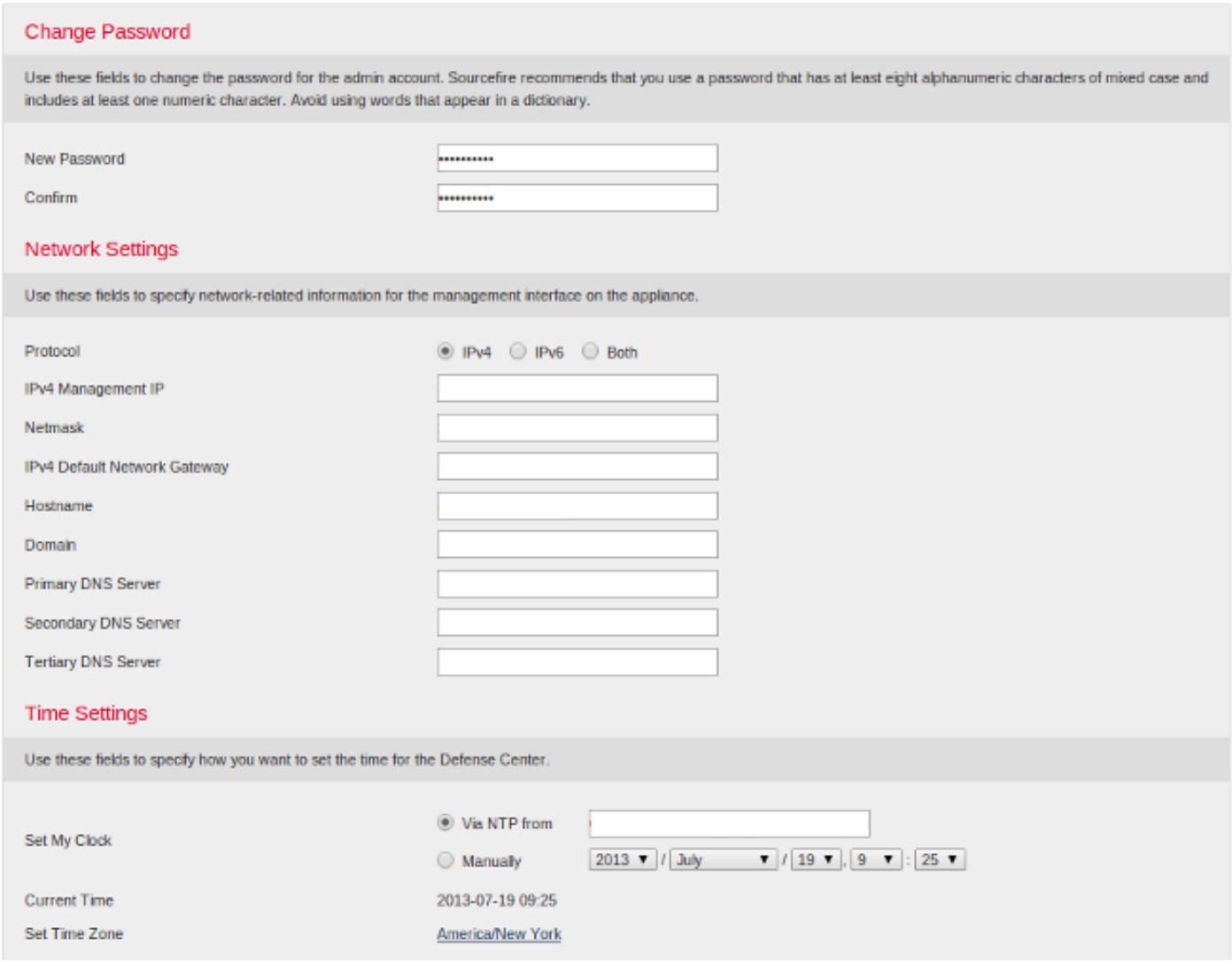
Предпосылка

Это руководство предполагает, что вы тщательно считали Руководство по установке системы FireSIGHT.

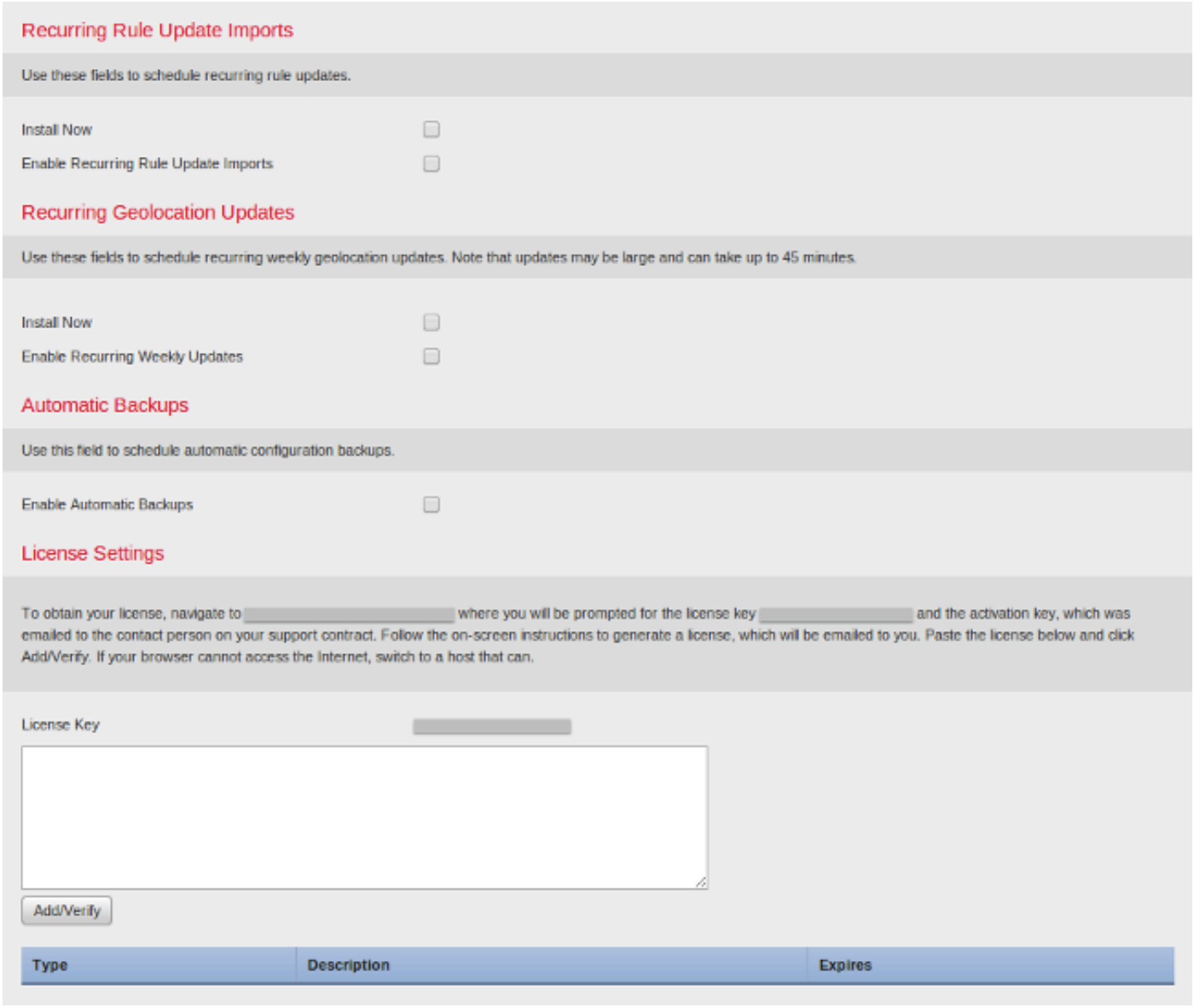
!--- конфигурацию

Шаг 1: Первоначальная конфигурация

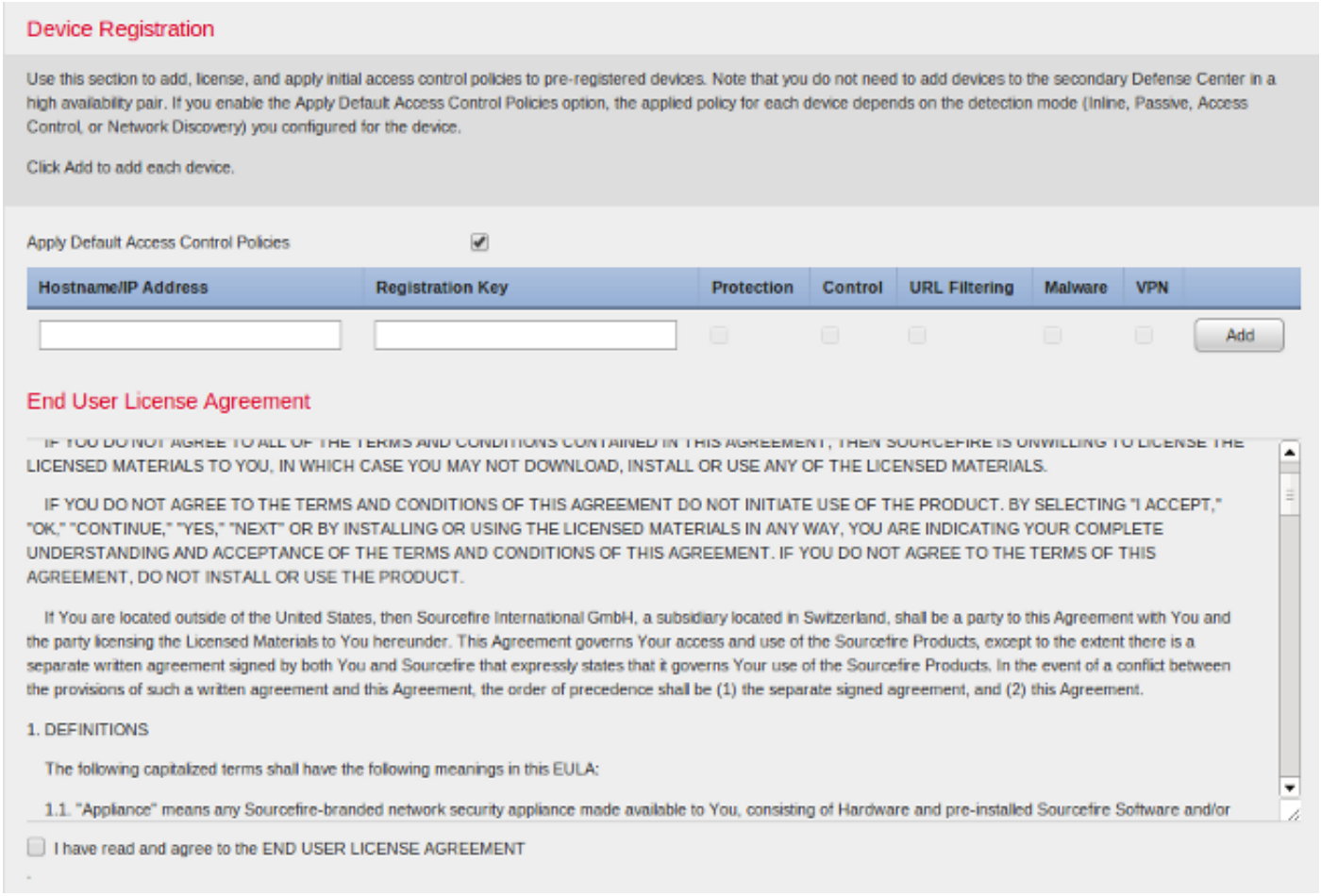
На вашем Центре управления FireSIGHT необходимо завершить процесс установки путем вхождения в веб-интерфейс и определения параметров начальной конфигурации на странице настройки, изображенной ниже. На этой странице вы должны изменить пароль администратора и можете также задать настройки сети, такие как Домен и серверы DNS и конфигурация времени.



Можно дополнительно настроить повторяющееся правило и обновления геолокации, а также автоматические резервные копии. Любые характеристики лицензирования могут также быть установлены на этом этапе.



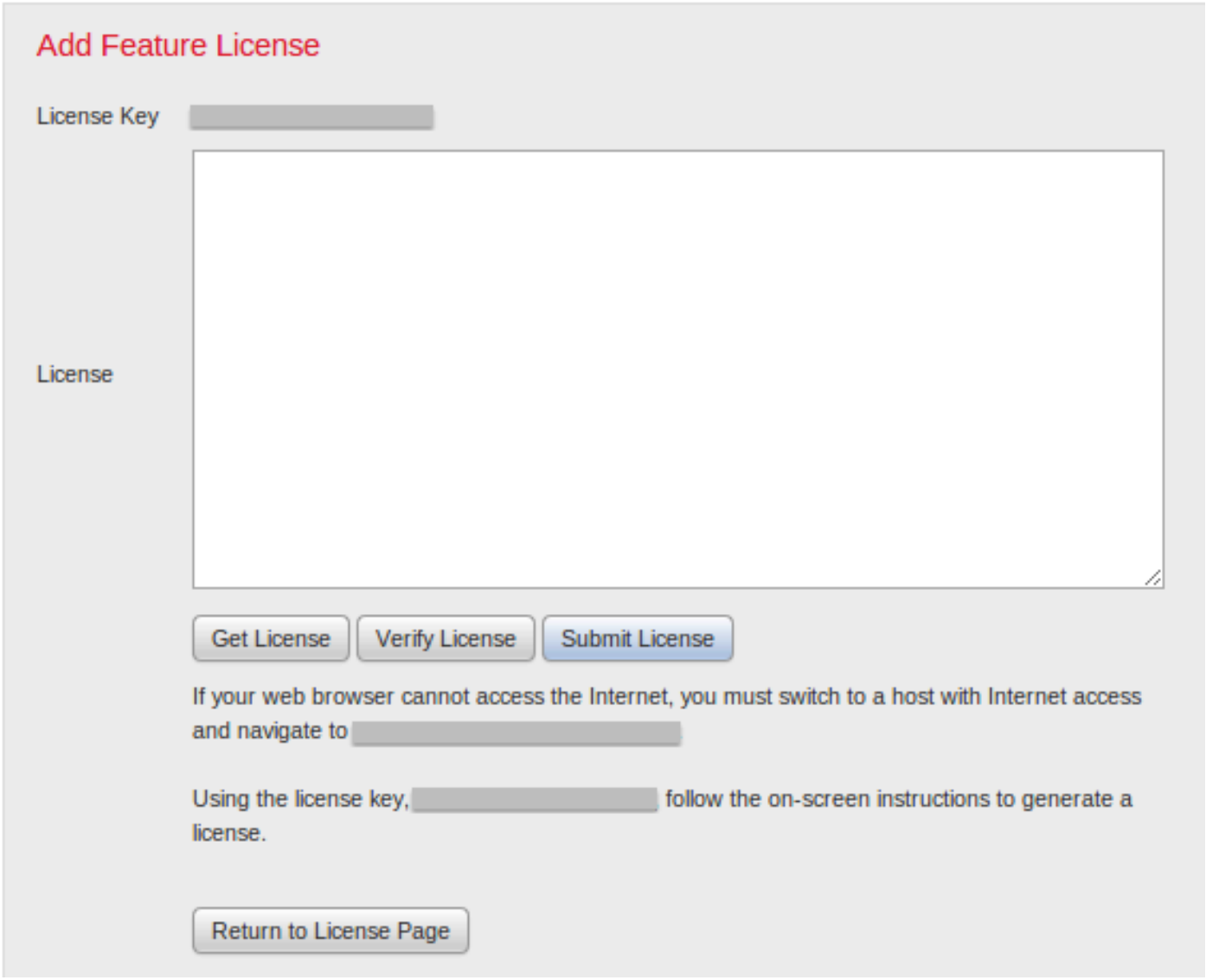
На этой странице можно также зарегистрировать устройство к Центру управления FireSIGHT и задать режим обнаружения. Режим обнаружения и другие опции, которые вы выбираете во время регистрации, определяют интерфейсы по умолчанию, встраивают наборы и зоны, которые система создает, а также политика, что это первоначально применяется к управляемым устройствам.



Шаг 2: Установите лицензии

Если вы не устанавливали лицензии во время страницы начальной настройки, можно выполнить задачу путем выполнения этих действий:

- Перейдите к следующей странице: **Система> Лицензии**.
- Щелкните **по Add New License**.



Если вы не получили лицензию, свяжитесь с Торговым представителем своей учетной записи.

Шаг 3: Примените системную политику

Системная политика задает конфигурацию для Опознавательных Профилей и Временной синхронизации между Центром управления FireSIGHT и управляемыми устройствами. Чтобы настроить или Применить Системную политику перешли к **Системе> Локальный> Системная политика**. Политика системы по умолчанию предоставлена, но должна быть применена к любым управляемым устройствам.

Шаг 4. : Примените политику в области охраны здоровья

Политика в области охраны здоровья используется, чтобы настроить, как управляемые устройства сообщают о своем состоянии здоровья Центру управления FireSIGHT. Чтобы настроить или Применить Политику в области охраны здоровья перешли к **состоянию> Политика в области охраны здоровья**. Политика в области охраны здоровья по умолчанию предоставлена, но должна быть применена к любым управляемым устройствам.

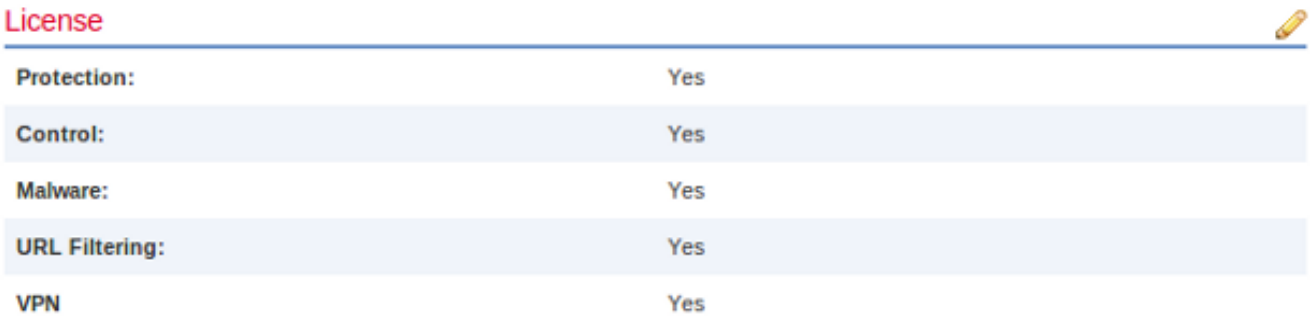
Шаг 5. : Зарегистрируйте управляемые устройства

Если вы не зарегистрировали устройства во время страницы начальной настройки, считайте этот документ для инструкций по тому, как зарегистрировать устройство к Центру управления FireSIGHT.

Шаг 6: Включите установленные лицензии

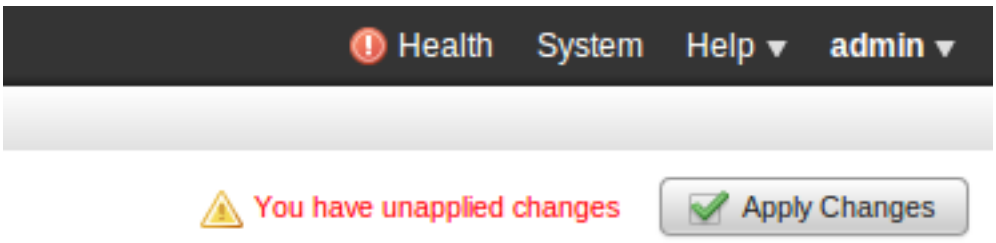
Прежде чем можно будет использовать любую характеристику лицензирования на устройстве, необходимо включить его для каждого управляемого устройства.

1. Перейдите к следующей странице: **Устройства> Управление устройствами**.
2. Щелкните по устройству, на которое вы хотите включить лицензии и ввести вкладку Device.
3. Нажмите **Edit** *(значок карандаша)*, следующий за Лицензией.



Включите необходимые лицензии для этого устройства и нажмите **Save**.

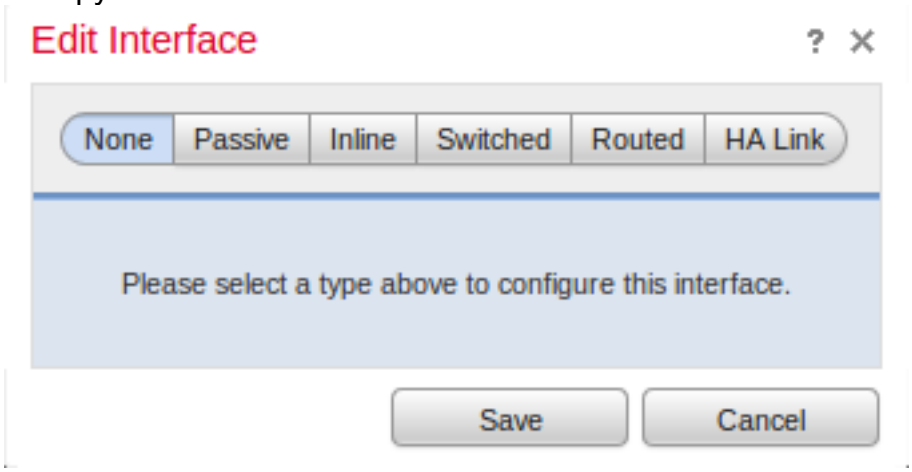
Заметьте сообщение, "*У вас есть остающиеся без применения изменения*" на правом верхнем угле. Это предупреждение остается активным, даже если вы перешли далеко от страницы управления устройствами, пока вы не нажимаете кнопку **Apply Changes**.



Шаг 7: Настройте интерфейсы считывания

1. Перейдите к следующей **странице Devices> Device Management**.

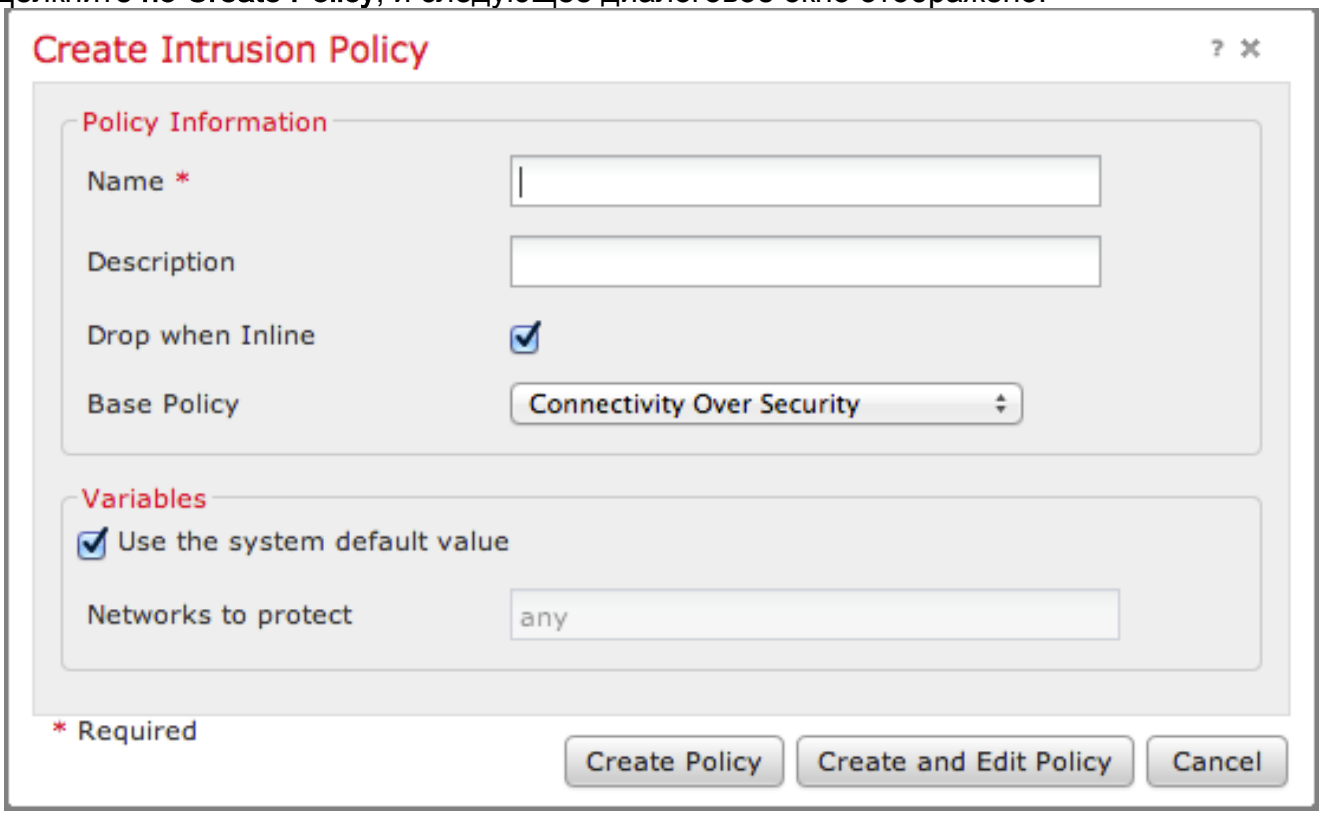
2. Нажмите **Edit** (карандаш) значок для датчика по Вашему выбору.
3. Под вкладкой **Interfaces** нажмите **Значок редактирования** для интерфейса по Вашему выбору.



Выберите Passive or Inline interface configuration. Коммутированный и Маршрутизируемые интерфейсы выходят за рамки этой статьи.

Шаг 8: Настройте политику проникновения

- Перейдите к следующей странице: **Политика> Проникновение> Политика Проникновения.**
- Щелкните **по Create Policy**, и следующее диалоговое окно отображено:



Необходимо назначить название и определить основную политику, которая будет использоваться. В зависимости от ваших развертываний вы можете, принял решение иметь **опцию Drop, когда Встроенный** включил. Определите сети, которые вы хотите защитить,

чтобы уменьшить ошибочные допуски и улучшить производительность системы.

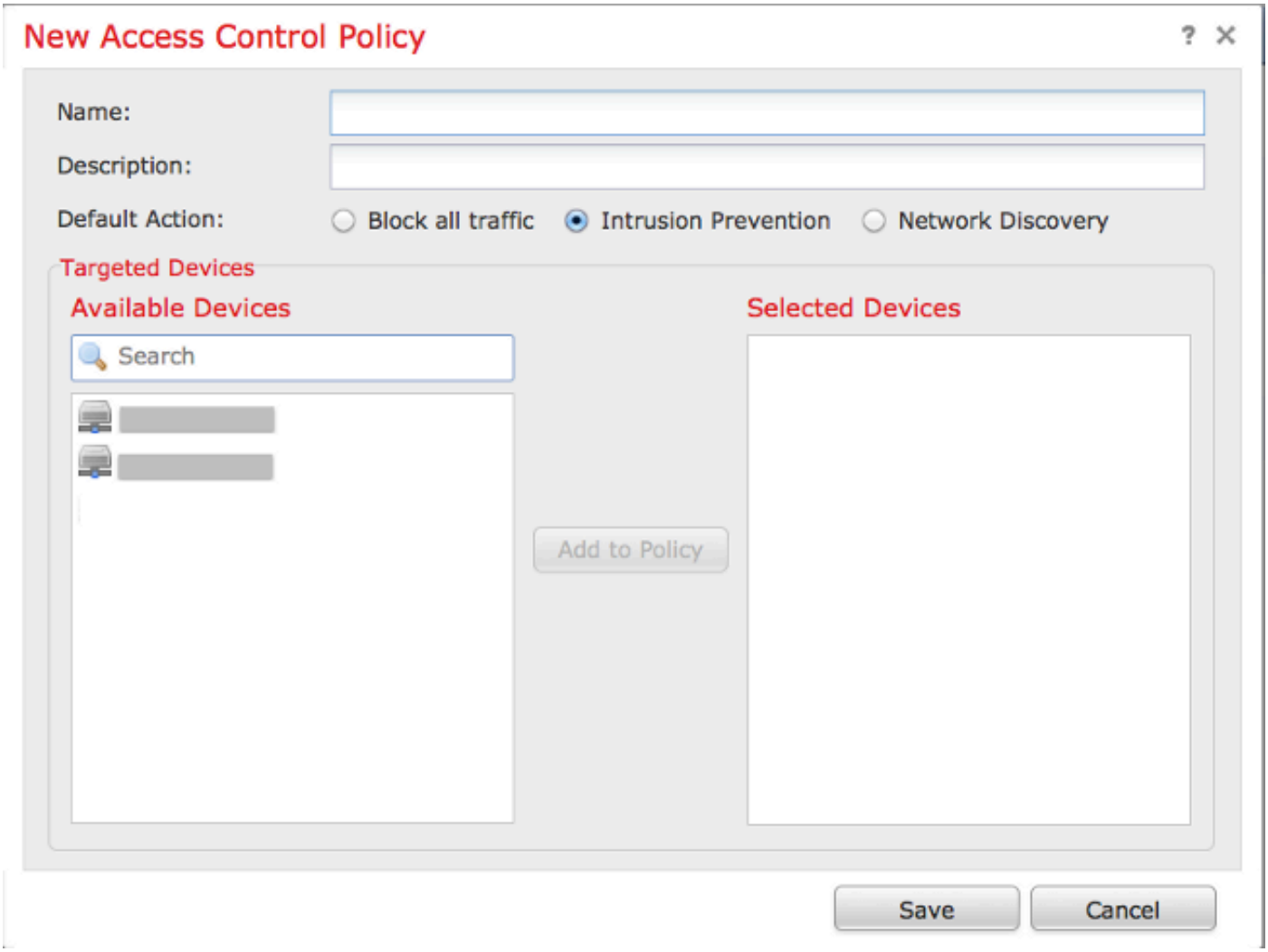
Щелчок **по Create Policy** сохранит ваши настройки и создаст политику IPS. Если вы хотите сделать какую-либо модификацию к политике проникновения, можно выбрать **Create и Edit Policy** вместо этого.

> **Примечание:** Политика проникновения применена как часть Политики контроля доступа. После того, как политика Проникновения применена, любые модификации могут быть применены, не повторно применяя целую Политику контроля доступа путем нажатия кнопки **Reapply**.

Шаг 9: Настройте и примените политику контроля доступа

1. Перейдите к **Политике> Управление доступом**.

2. Щелкните **по New Policy**.

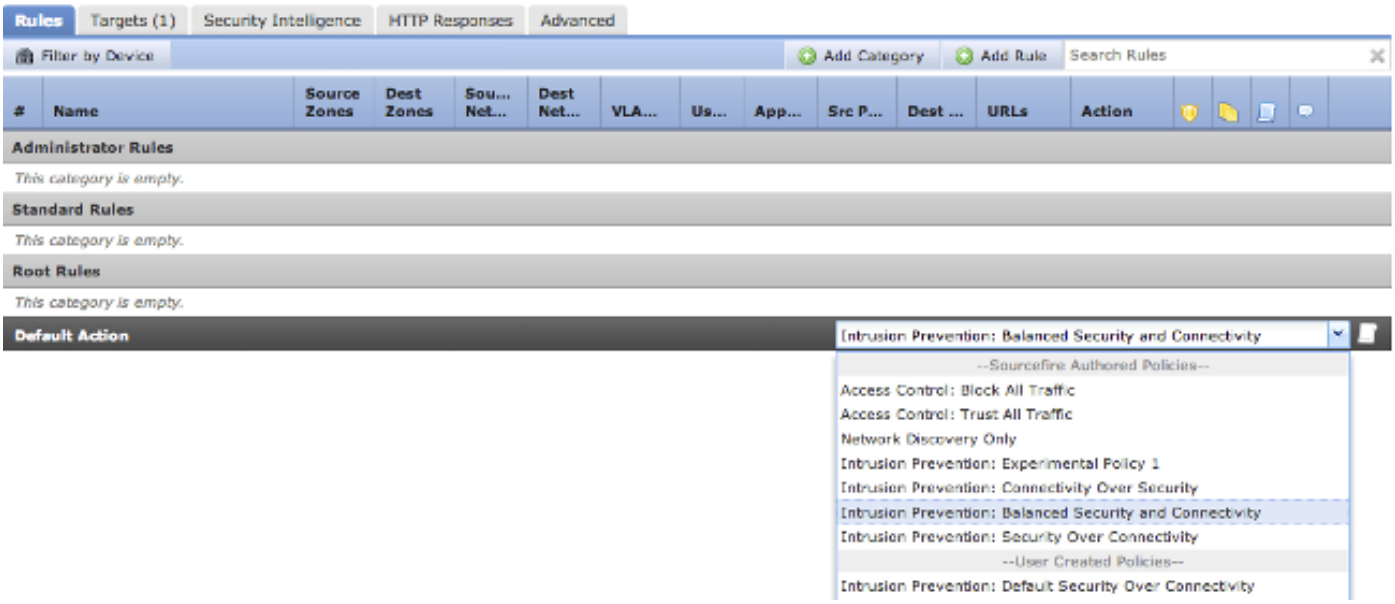


3. Предоставьте **Название** для политики и **Описания**.

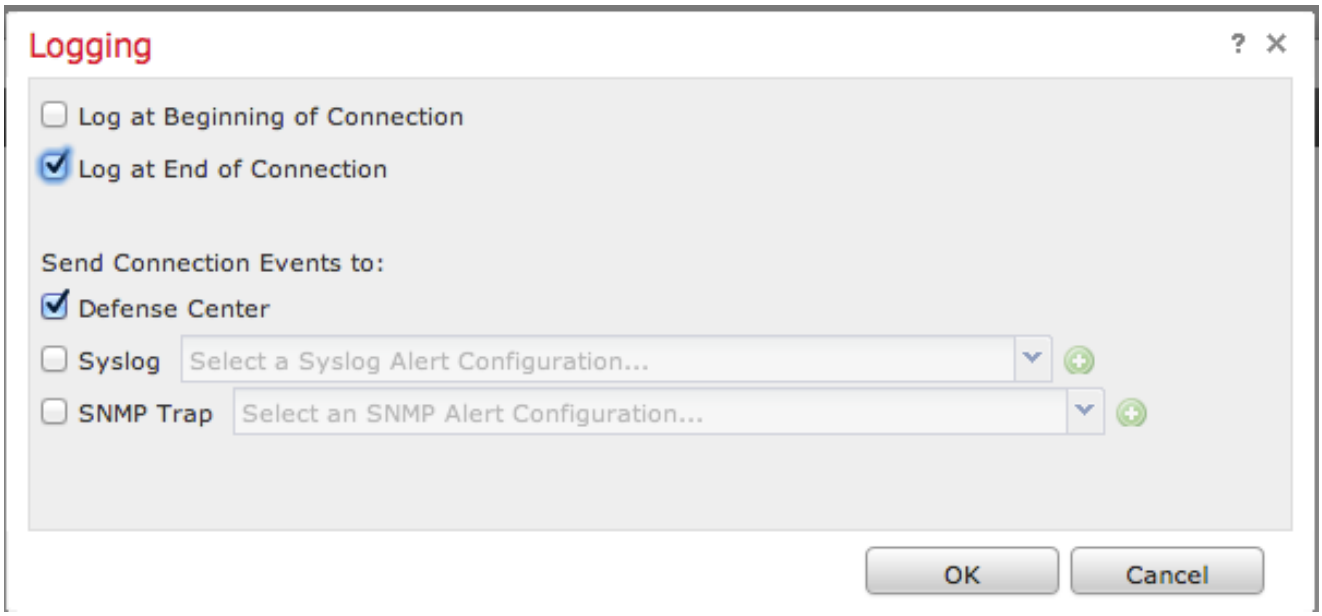
4. Выберите **Intrusion Prevention** как **Действие по умолчанию** Политики контроля доступа.

5. Наконец выберите **Targeted Devices**, к которому вы хотите применить политику контроля доступа и нажать **Save**.

6. Выберите свою политику Проникновения для действия по умолчанию.



7. Регистрации соединения нужно позволить генерировать события подключения. Нажмите выпадающее меню, которое является правильным из **Действия по умолчанию**.



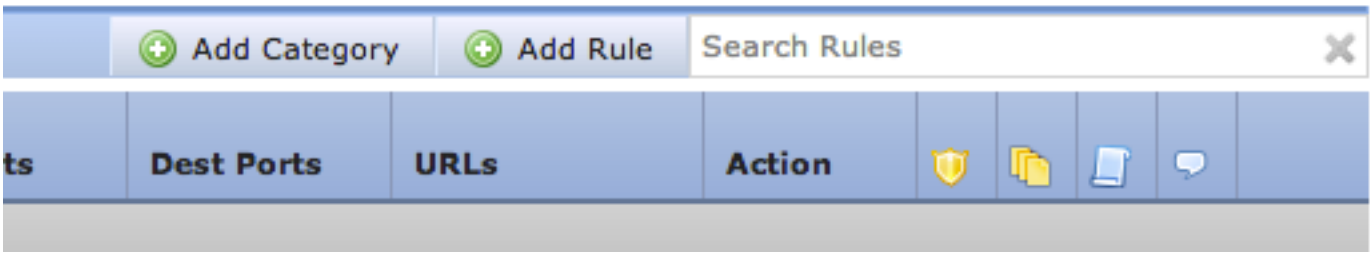
8. Примите решение регистрировать соединения или в начале или в конце соединения. События могут быть зарегистрированы на Центре управления FireSIGHT, местоположении системного журнала, или через SNMP.

> **Примечание:** Не рекомендуется регистрировать в обоих концах соединения, потому что каждое соединение (кроме заблокированных соединений) будет зарегистрировано дважды. Регистрация вначале полезна для соединений, которые будут заблокированы, и регистрирующий в конце полезно для всех других соединений.

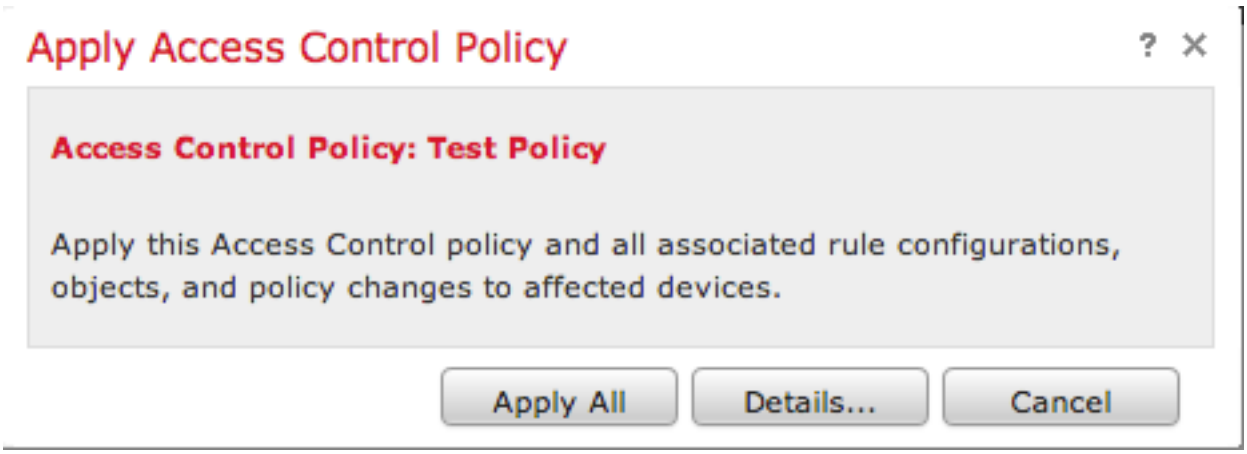
9. **Нажмите кнопку ОК**. Обратите внимание на то, что цвет значка регистрации изменился.

10. Можно добавить **Правило Управления доступом** в это время. Опции, которые можно использовать, зависят от типа лицензий, которые вы установили.

11. По окончании внеся изменения. нажмите кнопку **Save и Apply**. Вы заметите, что сообщение, указывающее на вас, не сохранило изменения на вашей политике по верхнему правому углу, пока не нажата кнопка.



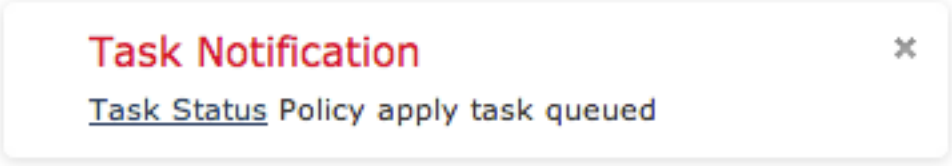
Можно принять решение только **Сохранить** изменения или щелкнуть **по Save и Apply**. Следующее окно появится при выборе последнего.



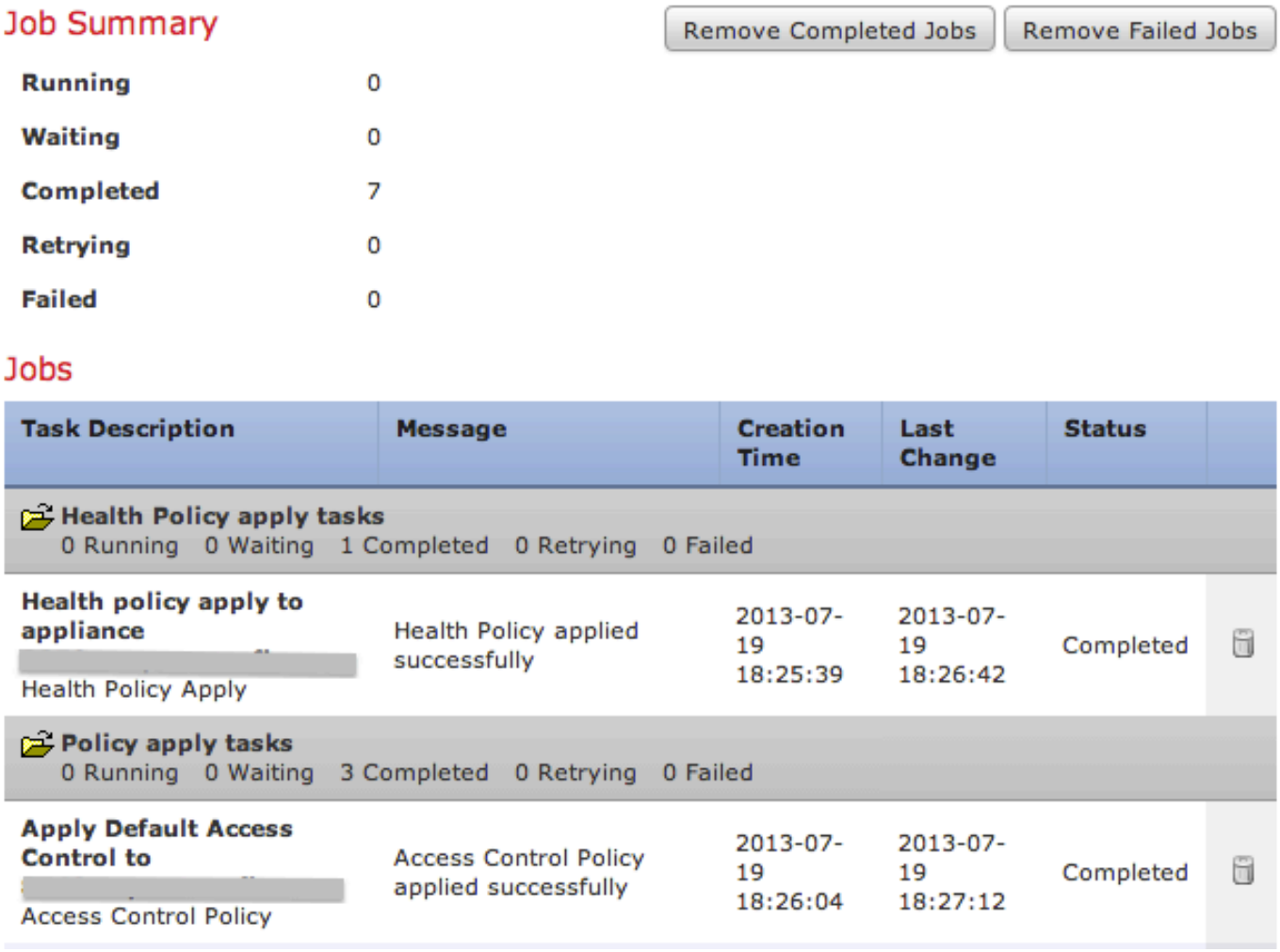
12. **Применитесь Все** применят Политику контроля доступа и любую связанную политику (политику) Проникновения к целевым устройствам.

> **Примечание:** Если политика проникновения будет применена впервые, она не может отменяться.

13. Можно контролировать статус задачи, нажимающей на ссылку **Статуса Задачи** на уведомлении, показанном в верхней части страницы, или путем навигации к: **Система> Контролирующий> Статус Задачи**



14. Щелкните по ссылке Статуса Задачи для мониторинга, выполнение Политики контроля доступа применяются.



Шаг 10: Проверьте если получения события центра управления FireSIGHT

После Политики контроля доступа применяются, завершил, необходимо начать видеть события соединений и в зависимости от событий проникновения трафика.

Дополнительная рекомендация

Можно также настроить следующие дополнительные характеристики в системе. См. Руководство пользователя для сведений о внедрении.

- Запланированные резервные копирования
- Автоматическое Обновление ПО, SRU, VDB и загрузки/установки GeoLocation.
- Внешняя проверка подлинности через LDAP или RADIUS