Инициируйте Запланированные Просмотры на FireAMP / AMP для Оконечных точек

Содержание

Введение

Можно выполнить Запланированные Просмотры на FireAMP ежедневно, еженедельно, или ежемесячно в зависимости от требований. При создании планируемых просмотров необходимо предоставить учетные данные административного пользователя для машин. Этот документ обращается к требуемым разрешениям учетной записи пользователя для успешных запланированных просмотров.

Предварительные условия

Требования

- Доступ к информационной панели FireAMP
- Учетные данные для Учетной записи администратора для Компьютеров с операционной системой Windows
- FireAMP 3.x для Windows XP или позже - Запланированные Просмотры
- FireAMP 4.x для Windows XP или позже - Запланированные Просмотры и Просмотры IOC Оконечной точки

Перед началом работы

Когда вы добавляете запланированный просмотр в политике FireAMP, это увеличивает серийное число политики. Оконечные точки, выпадающие новая политика, когда они передают биение. Использование предоставленных учетных данных, FireAMP создает

запланированную задачу в Windows, и позже выполняет задачу. Из-за этого дизайна мы должны удостовериться, что учетная запись, которую мы используем, имеет соответствующие разрешения.

Прежде чем мы настроим запланированное, просмотр, там два основных требования для учетной записи пользователя, чтобы вы запланировали использовать.

> **Примечание:** Эти разрешения также просят просмотры IOC Оконечной точки.

1. Учетная запись должна быть учетной записью администратора. Это могло или быть локальным администратором или администратором домена.
2. Учетная запись должна быть в состоянии **Войти в систему как группа**.

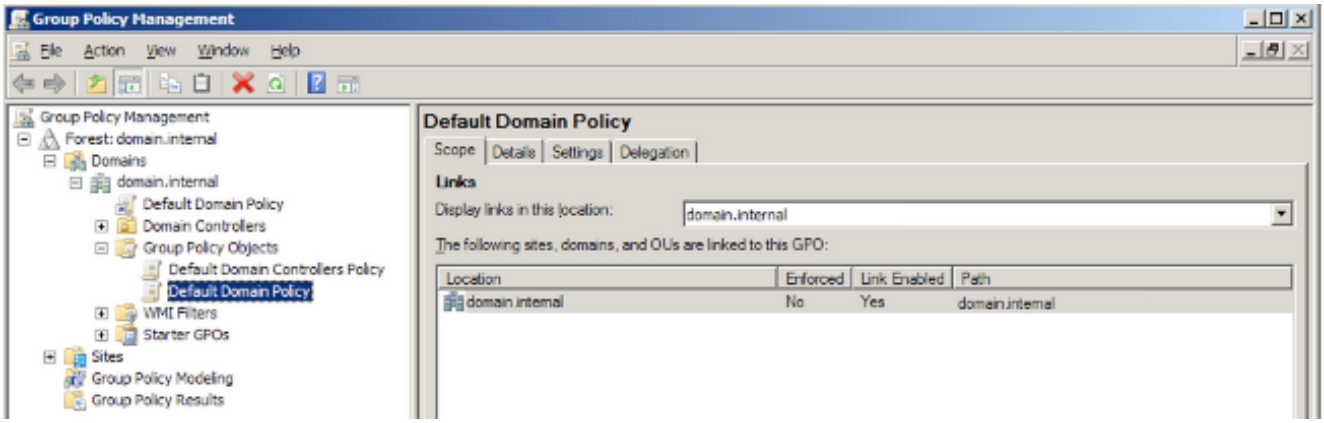
Вход в систему как пакетные разрешения настроен через групповую политику. Если это не настроено для вашего домена, то административные учетные записи по умолчанию должны быть в состоянии войти в систему как группа. Если это настроено для вашего домена, учетная запись должна принадлежать группе, определенной в Объекте групповой политики (GPO).

!--- конфигурацию

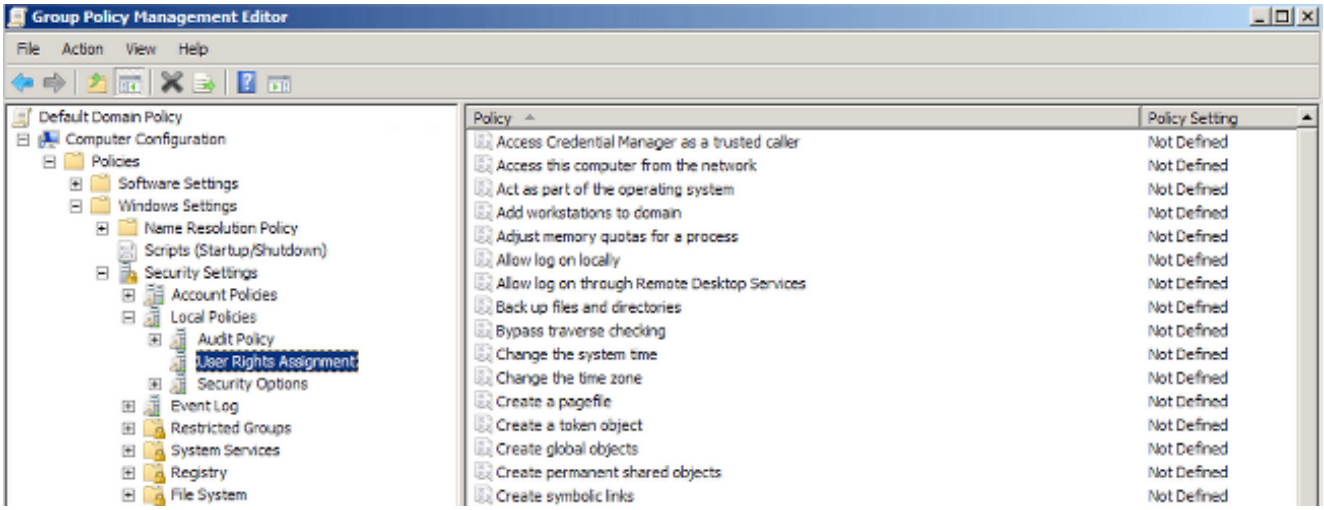
Следующие шаги применяются к Windows Server выполнения контроллера домена 2008 R2:

> **Внимание. :** Это - ваша обязанность гарантировать корректную конфигурацию групповой политики на Windows Server. Cisco не ответственна ни за какие проблемы, вызванные неправильными конфигурациями групповой политики.

1. Перейдите **к Пуску> Средства администрирования> менеджмент Групповой политики**.
2. Разверните **Лес> Домены>** *Your_Domain_Name*> **Объекты Групповой политики**.



3. Щелкните правой кнопкой по политике, вы хотите модифицировать и выбрать **"Edit"**.
4. Перейдите к **Конфигурации компьютера> Политика>> Security Windows Settings Параметры настройки> Локальная политика> Присвоение Прав пользователя**.



5. Двойной щелчок на **Входе в систему как пакетное задание**.

6. Выберите **Add User или Group**.

7. Нажмите **Browse**, затем введите требуемого пользователя или имя группы.

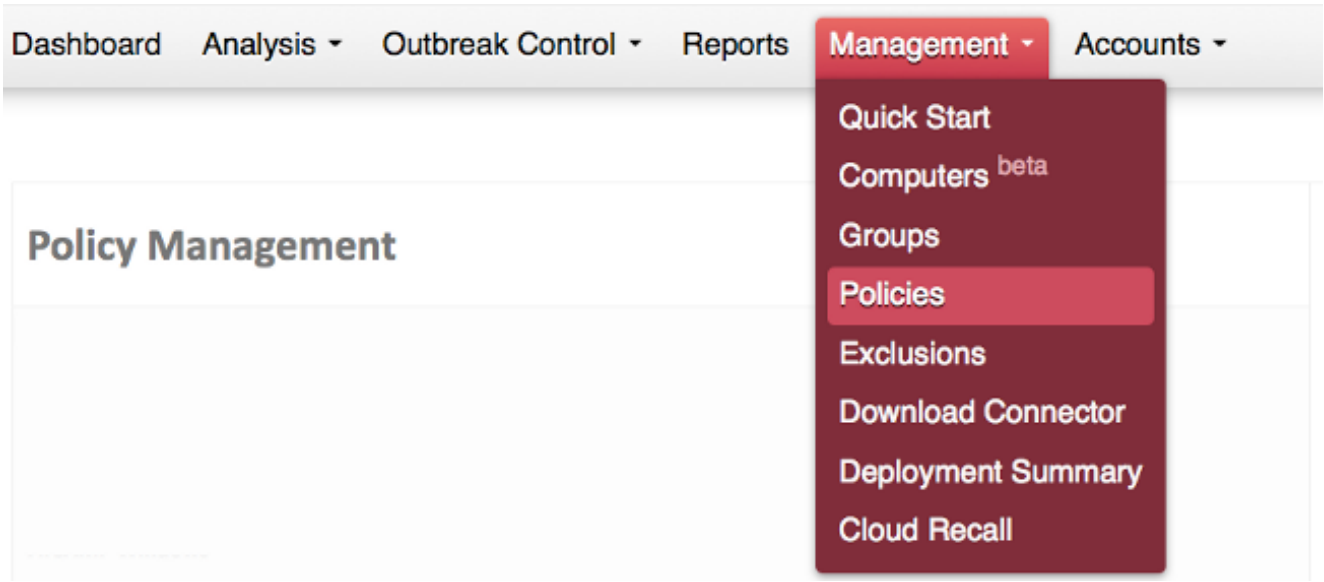
8. Нажмите **Check Name** для проверения его.

9. Щелкните **по OK**, пока вы не возвратитесь к **Редактору менеджмента Групповой политики**.

Примените групповую политику к своему домену или группе, если это уже не применено. Теперь, когда мы настроили учетную запись пользователя, мы настроим просмотр в информационной панели FireAMP.

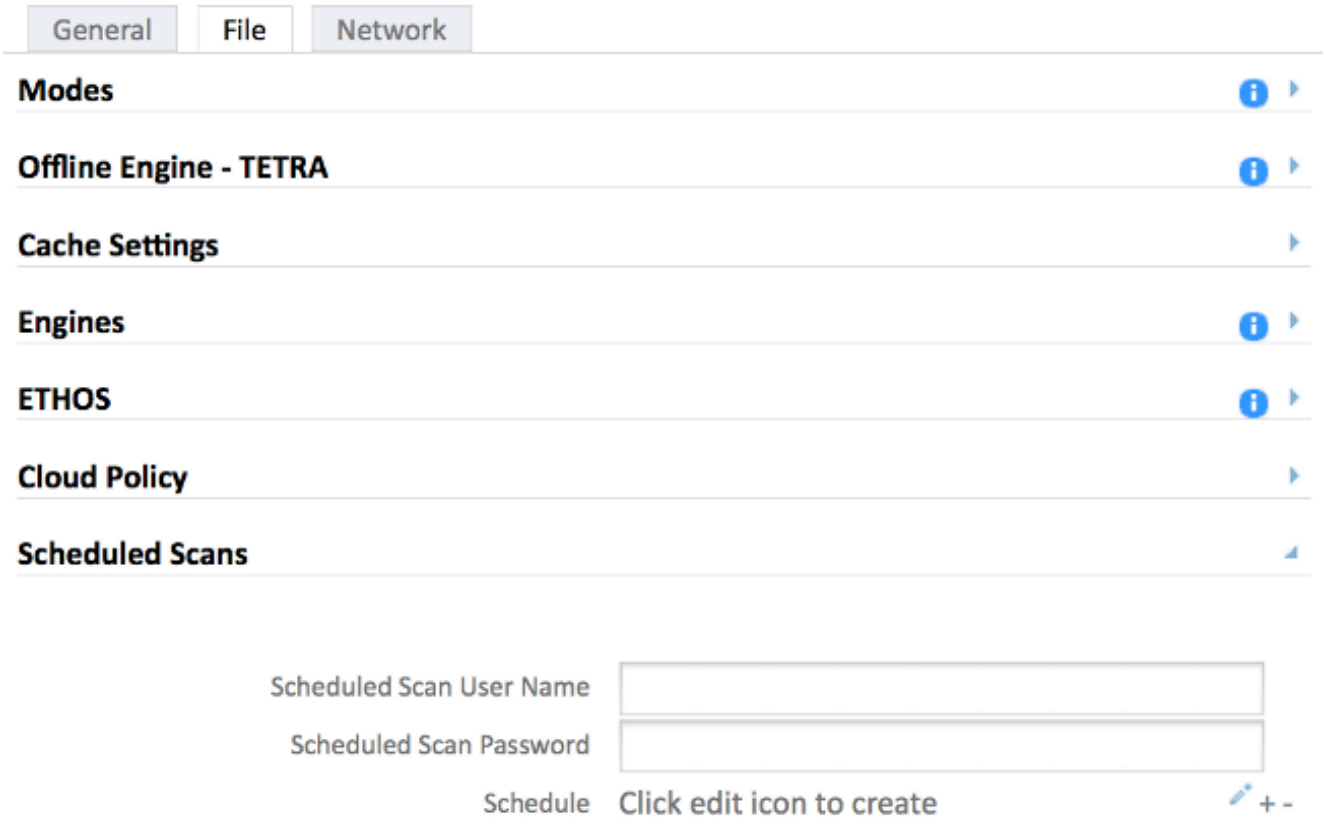
1. Войдите к информационной панели FireAMP.

2. Перейдите к **менеджменту> Политика**.



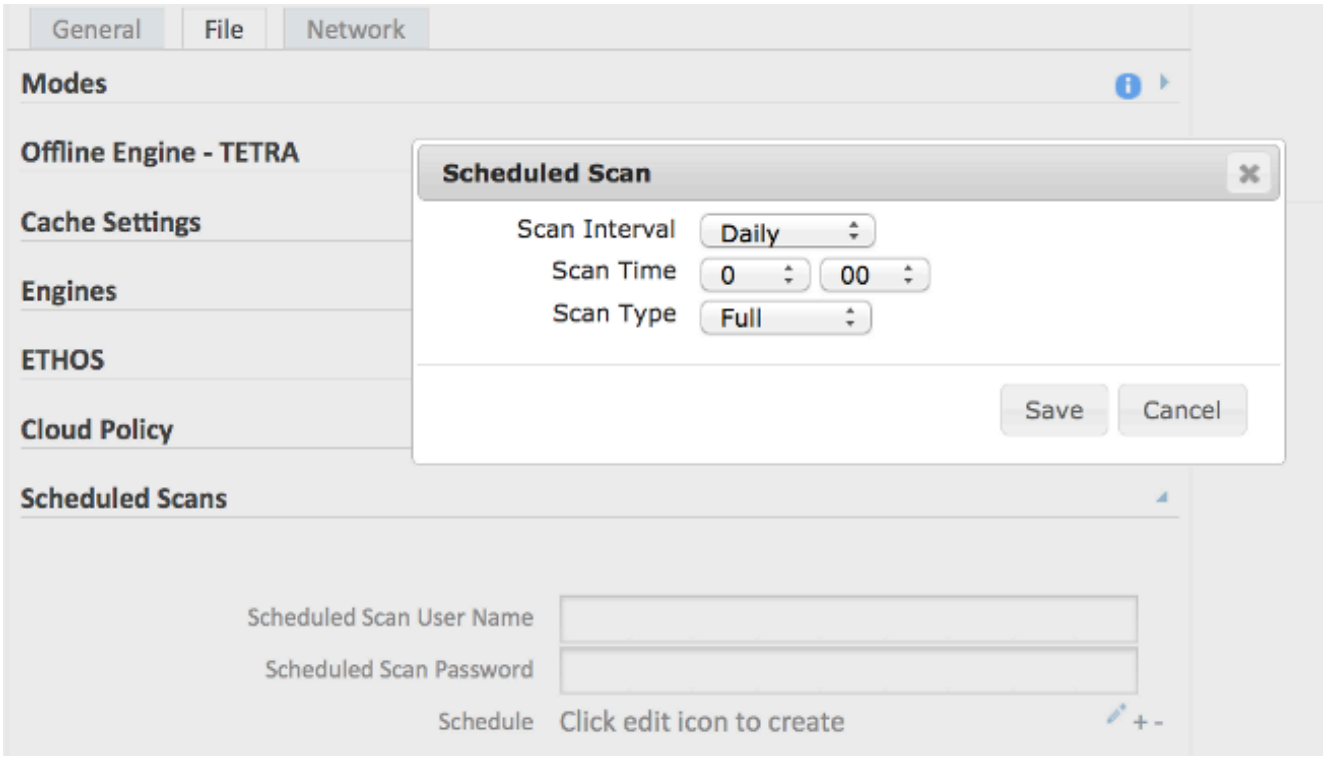
3. Отредактируйте желаемую политику.

4. Перейдите к вкладке **File> Запланированные Просмотры**. Введите имя пользователя и пароль.



Примечание: Имя пользователя должно быть в формате `domain\username`. Суффикс домена не необходим.

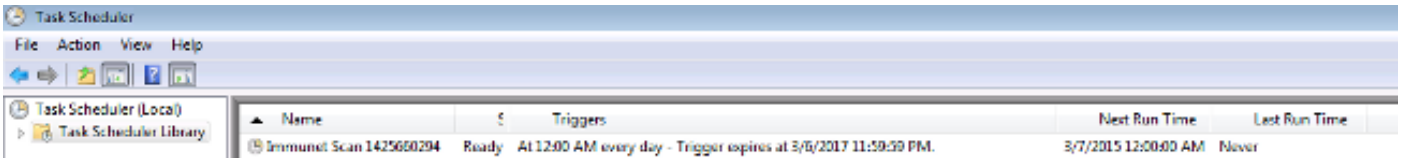
5. Настройте список. Используйте карандаш, плюс и минус значки для изменения, добавьте, удалите списки просмотра. Можно ввести множественные списки здесь. Можно выбрать Daily, Weekly или Monthly в дополнение к 24-часовому времени для инициирования просмотра. Можно также выбрать Scan Type (Flash или Full).



6. Выберите **Save**, тогда выбирают **Update** для фиксации изменений политики.

Проверка

После того, как политика обновлена на машинах, необходимо видеть одну или более задач в Windows Task Scheduler с названием **Immunet** как снимок экрана ниже:



Устранение неисправностей

Политика обновлена, но не найдена запланированная задача

Если ваша политика обновляет, но вы не видите запланированной задачи, это происходит, скорее всего, из-за учетной записи, вы использовали или наличие неправильного пароля или недостаток полномочий для создания задач (не администратор).

Задача создана, но не в состоянии работать

Если задача создана, но не в состоянии работать, учетная запись, скорее всего, не имеет способности **Войти в систему как группа**. Рассмотрите вышеупомянутые действия настройки, чтобы гарантировать, что ваша учетная запись настроена правильно.