Установка и конфигурация модуля AMP через AnyConnect 4.x и включатель AMP

Содержание

Введение

Этот документ описывает метод, чтобы установить и настроить модуль Усовершенствованной вредоносной защиты (AMP) в системе конечного пользователя с AnyConnect.

Включатель AMP AnyConnect используется в качестве среды для развертывания AMP для Оконечных точек. Это требует у AMP программное обеспечение Endpoints к подмножеству оконечных точек от сервера, размещенного локально в предприятии, и устанавливает сервисы AMP к его существующей пользовательской базе. Этот подход предоставляет администраторам пользовательской базы AnyConnect агента дополнительных мер безопасности, который обнаруживает потенциальные вредоносные угрозы, которые происходят в сети, удаляет те угрозы и защищает предприятие от компромисса. Это сохраняет пропускную способность и время, потраченное для загрузки, не требует никаких изменений на портала стороне и может быть сделано без учетных данных для аутентификации, передаваемых оконечным точкам.

Предварительные условия

Требования

- Версия 4 клиента Secure Mobility Client AnyConnect. x

- FireAMP / AMP для Оконечных точек
- AnyConnect Плюс / Лицензии Вершины
- Менеджер устройств адаптивной безопасности (ASDM) (ASDM) Версайон 7.3.2 или позже

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Устройство адаптивной защиты (ASA) 5525 с версией программного обеспечения 9.5.1
- Клиент Secure Mobility Client AnyConnect 4.2.00096 на Microsoft Windows 7 64-разрядных профессионалов
- Версия 7.5.1 (112) ASDM

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

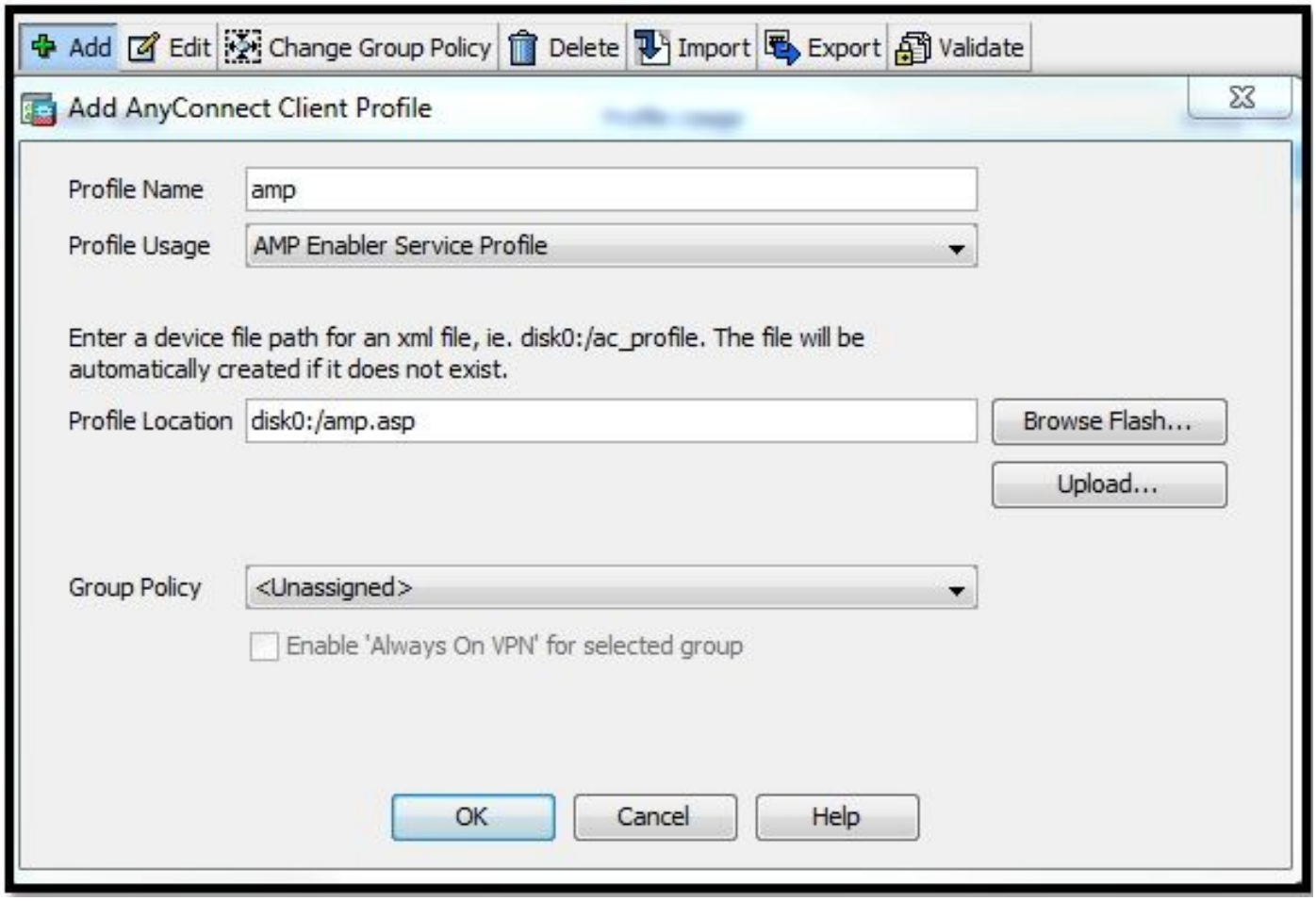
Развертывания AnyConnect для включателя AMP через ASA

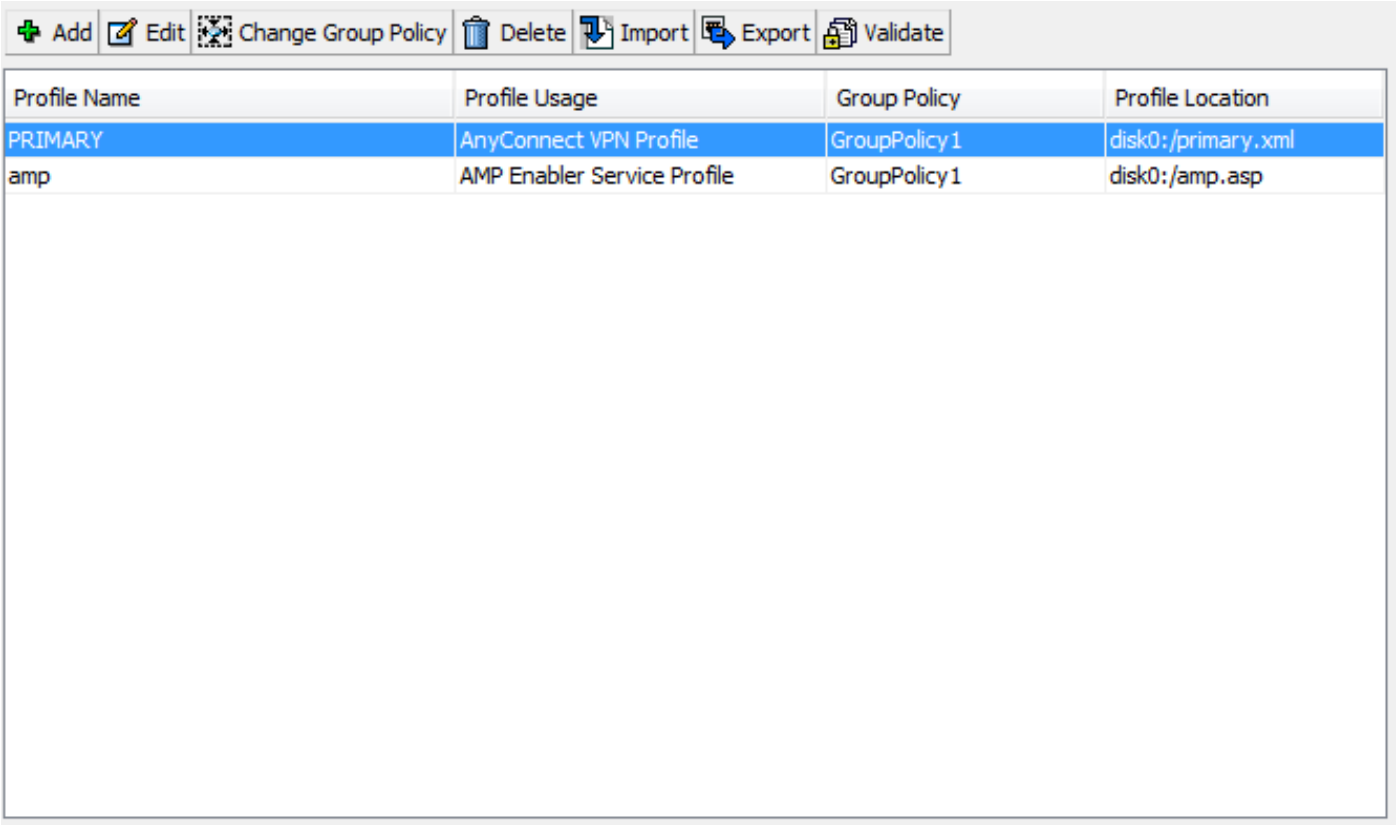
Шаги, вовлеченные в конфигурацию, следующие:

- Настройте профиль клиента включателя AMP AnyConnect.
- Отредактируйте политику группы VPN AnyConnect и загрузите Профиль сервиса включателя AMP.
- Измените Профиль AMP для получения конфигурации от Web-сервера.
- Проверьте установку на пользовательской машине.

Шаг 1: Настройте профиль клиента включателя AMP AnyConnect

- Перейдите к **Конфигурации> VPN для удаленного доступа> сетевой доступ (клиент)> Профиль Клиента AnyConnect**.
- Добавьте **профиль сервиса включателя AMP**.



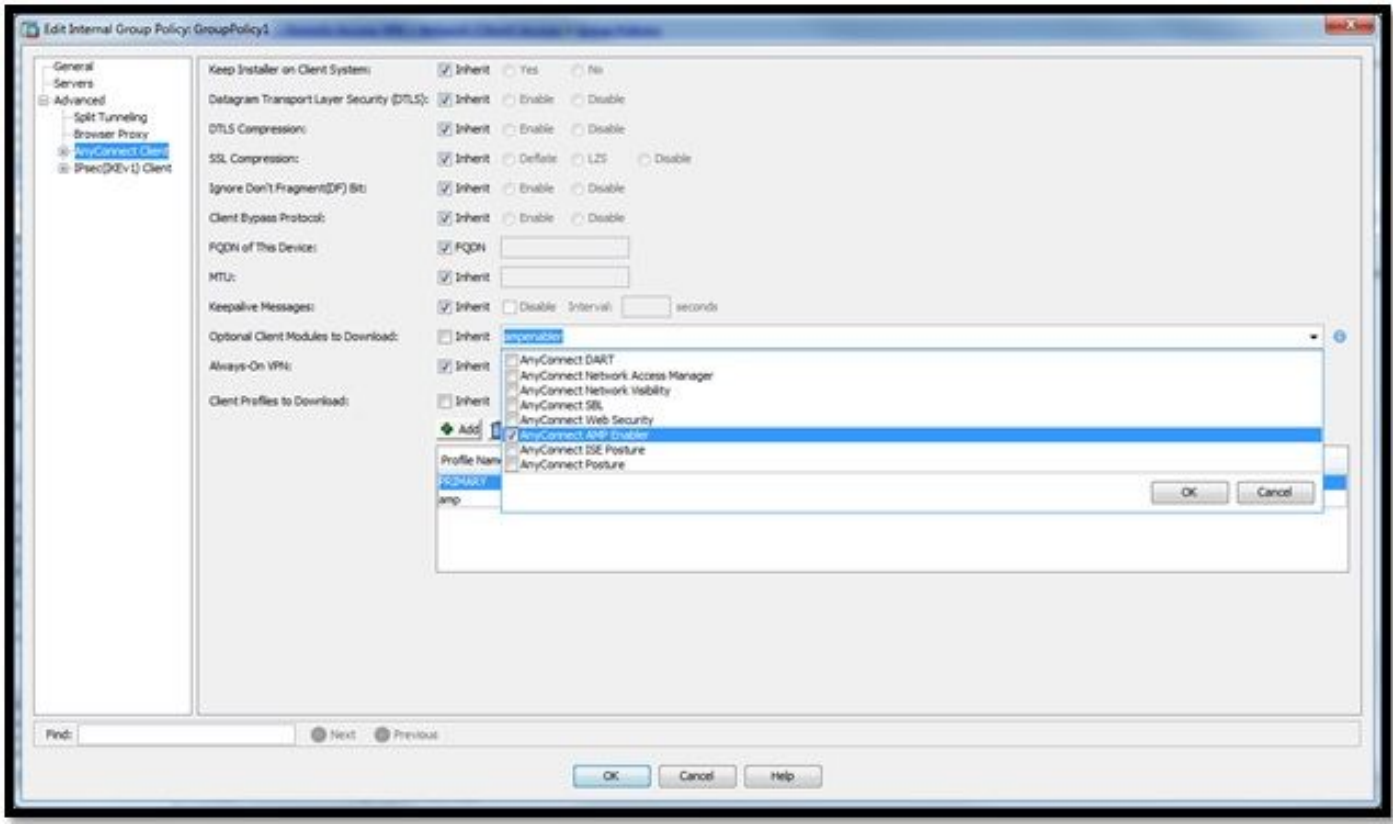


Шаг 2: Отредактируйте групповую политику для загрузки включателя AMP AnyConnect

- Перейдите к **Конфигурации>, Удаляют Доступ к VPN>, Групповые политики>**

Редактируют.

- Перейдите **Усовершенствованный> Клиент AnyConnect> Дополнительные Клиентские модули для Загрузки.**
- Выберите **AnyConnect AMP Enabler.**



Шаг 3: Загрузите политику FireAMP

> **Примечание:** Прежде чем вы продолжитесь, определите, удовлетворяет ли ваша система требования для AMP Windows Connector Оконечных точек.

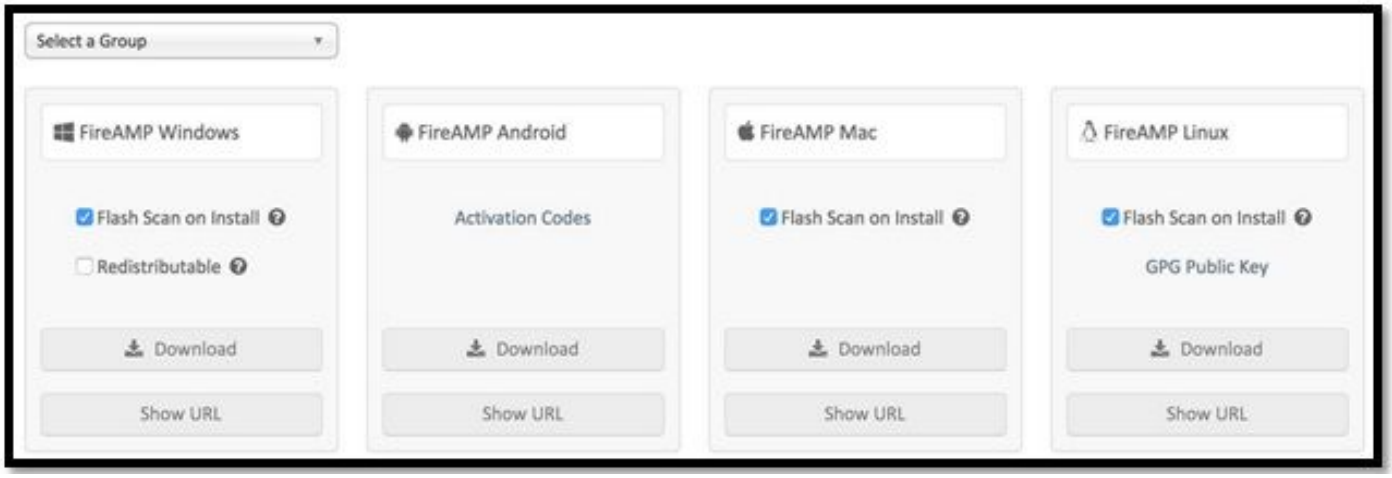
Системные требования для AMP для Windows Connector оконечных точек

Это минимальные системные требования для Разъёма FireAMP на основе операционной системы Windows. Разъём FireAMP поддерживает и 32-разрядные и 64-разрядные версии этих операционных систем.

ОПЕРАЦИОННАЯ СИСТЕМА	Процессор	Память	Дисковое пространство, Облако только режим	Дисковое пространство
Microsoft Windows XP с Пакетом обновления 3 или позже	500 МГц или быстрый процессор	ОЗУ НА 256 МБ	Доступное дисковое пространство на 150 МБ - режим Только для облака	Доступное дисковое пространство на 1 ГБ - TETRA
Microsoft Windows Vista с Пакетом обновления 2	1 ГГц или быстрый процессор	ОЗУ НА 512 МБ	Доступное дисковое пространство на 150 МБ - режим	Доступное дисковое пространство на 1 ГБ - TETRA

или позже			Только для облака	
Microsoft Windows 7	1 ГГц или быстрый процессор	ОЗУ НА 1 ГБ	Доступное дисковое пространство на 150 МБ - режим Только для облака	Доступное дисковое пространство на 1 ГБ - TETRA
Microsoft Windows 8 и 8.1 (требует Разъёма FireAMP 3.1.4 или позже),	1 ГГц или быстрый процессор	ОЗУ НА 512 МБ	Доступное дисковое пространство на 150 МБ - режим Только для облака	Доступное дисковое пространство на 1 ГБ – TETRA
Microsoft Windows Server 2003	1 ГГц или быстрый процессор	ОЗУ НА 512 МБ	Доступное дисковое пространство на 150 МБ - режим Только для облака	Доступное дисковое пространство на 1 ГБ - TETRA
Microsoft Windows server 2008	2 ГГц или быстрый процессор	ОЗУ НА 2 ГБ	Доступное дисковое пространство на 150 МБ – Облако только режим	Доступное дисковое пространство на 1 ГБ – TETRA
2012 Microsoft Windows server (требует Разъёма FireAMP 3.1.9 или позже),	2 ГГц или быстрый процессор	ОЗУ НА 2 ГБ	Доступное дисковое пространство на 150 МБ - Облако только режим	Доступное дисковое пространство на 1 ГБ – TETRA

Страница Download Connector позволяет вам или загружать пакеты установки для каждого типа разъёма FireAMP или копировать URL, где они могут быть загружены. Этот пакет может быть размещен в сетевой ресурс или распределен через программное обеспечение для управления. URL загрузки может быть послан по электронной почте пользователям, чтобы позволить им загружать и устанавливать его самим, который может быть загружен для удаленных пользователей.



Выберите группу

- **Аудит Только:** Используемый, когда вы все еще учитесь о продукте и хотите установить его без любого влияния к вашим существующим системам.
- **Защитите:** Используемый во время нормальной работы и вы хотите, чтобы FireAMP изолировал файл.
- **Медицинская сортировка:** Используемый, когда у вас есть известный или подозреваемый компьютер пораженный вирусом.
- **Сервер:** Используемый, когда вы устанавливаете разъём на сервере стандартных окон.
- **Domain controller:** Используемый, когда вы устанавливаете разъём на контроллере домена Windows.

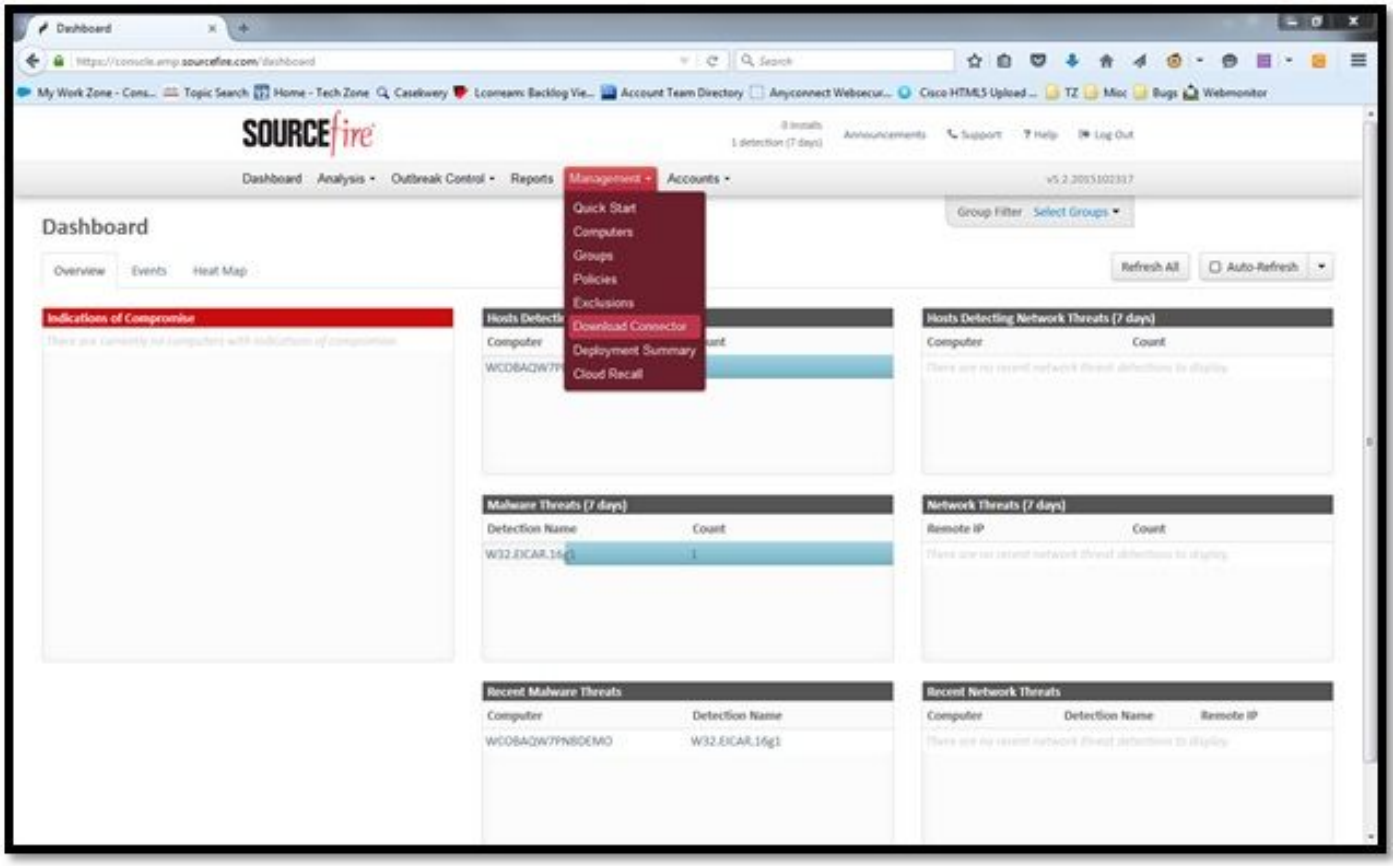
Функции

- **Просмотр Флэша на Установке:** процесс Просмотра выполняется во время установки. Этот просмотр является основанным на облачных вычислениях и требует сетевого подключения. Это относительно быстро для выполнения.
- **Распространяемый файл:** Эта опция загружает 32-разрядные и 64-разрядные установщики в одном одиночном пакете.

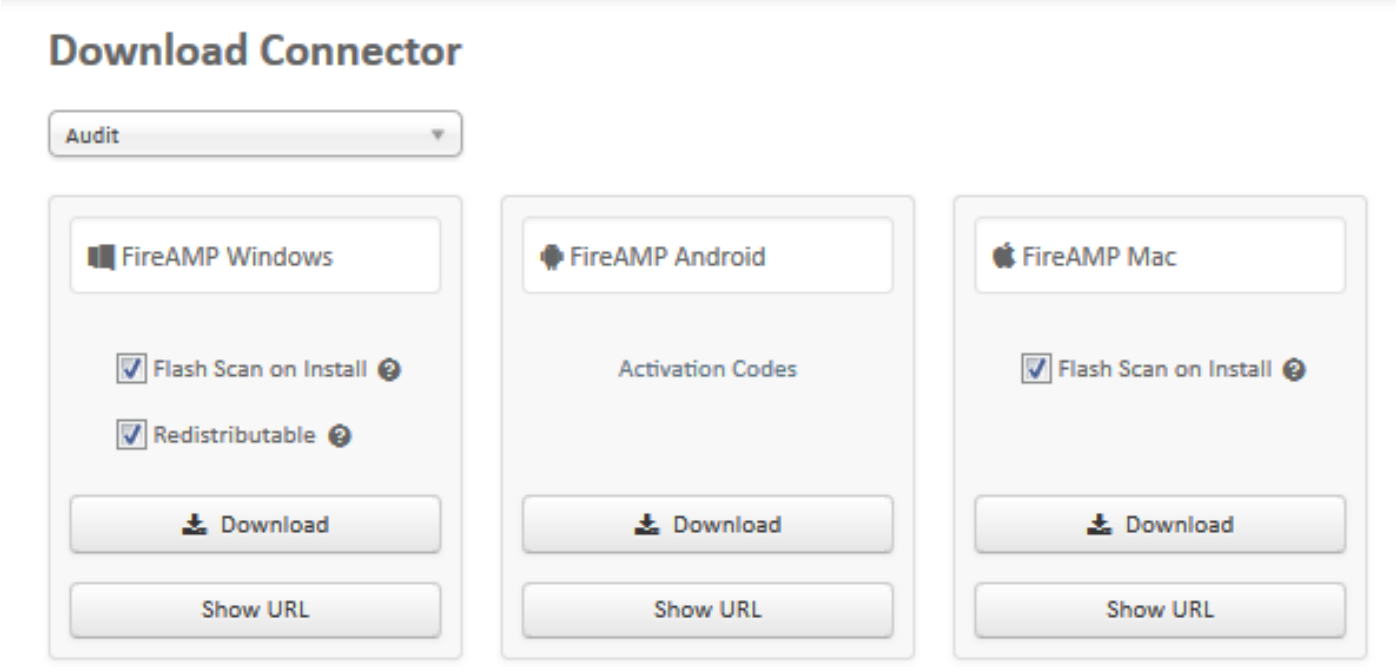
  Примечание: По умолчанию это загружает маленький файл загрузчика (на ~500 КБ) для установки Разъёма FireAMP. Этот исполняемый файл определяет, выполняет ли компьютер 32 или 64-разрядную операционную систему и загружает и устанавливает соответствующую версию Разъёма FireAMP.

  Однако в целях VPN, необходимо принять решение загрузить распространяемый установщик. Это - файл на 30 МБ, который содержит и 32 и 64-разрядные установщики. Этот файл может быть размещен в сетевой ресурс или выдвинут ко всем компьютерам в группе через программное средство как Системный Менеджер конфигурации Центра для установки Разъёма FireAMP на нескольких компьютеров. Загрузчик и распространяемый установщик также, оба содержат `policy.xml` файл, который используется в качестве файла конфигурации для установки.

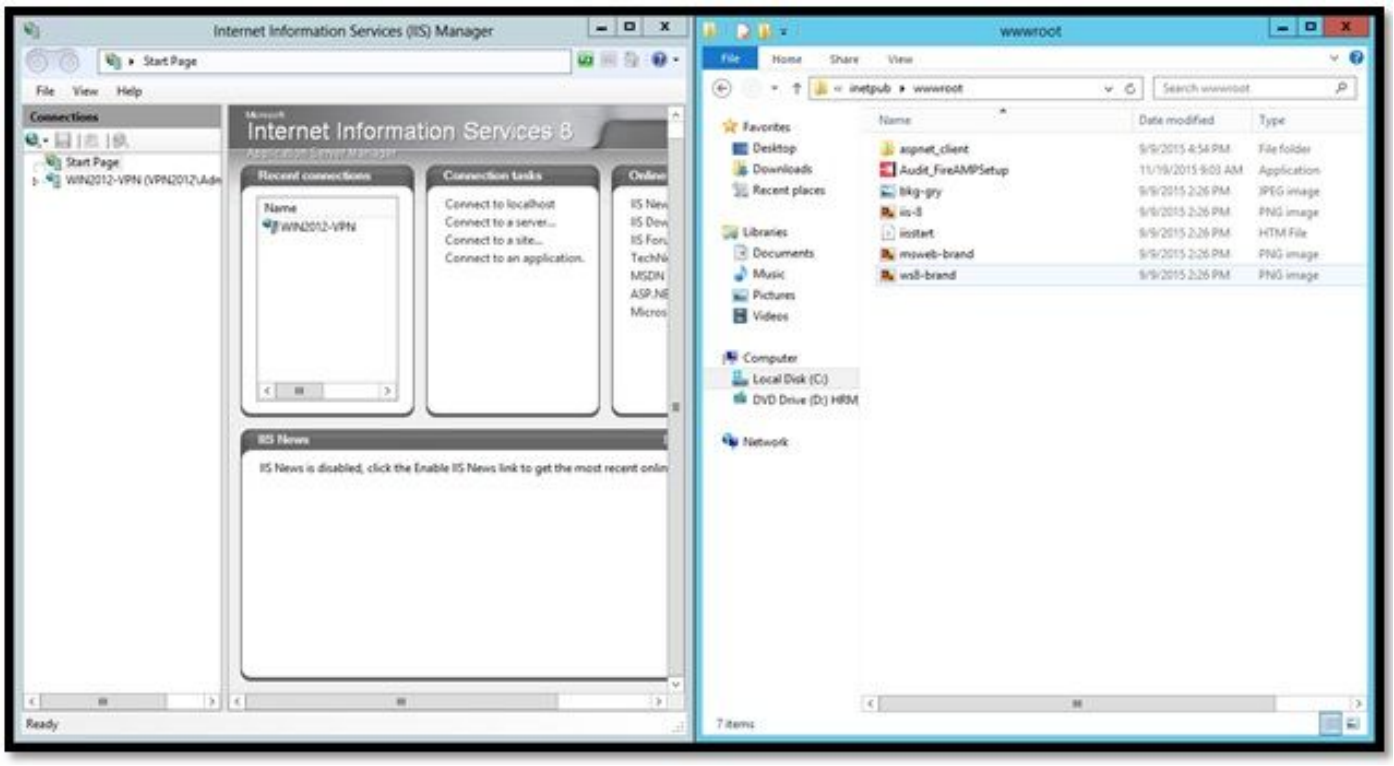
Для загрузки разъёма перейдите к **менеджменту> Разъём Загрузки**. Затем выберите тип и **Загрузку** FireAMP (Windows, Android, Mac, Linux).



В этом случае опция **Audit** для **Разъёма Загрузки** и установка для Windows Machine были выбраны.



Примечание: Когда этот файл загружен, он генерирует вызванный файл `.exe`, в этом случае, `Audit_FireAMPSetup.exe`. Этот файл передавался Web-серверу, чтобы быть доступным и загруженным от ASA, как только пользователь просит конфигурацию для AMP.

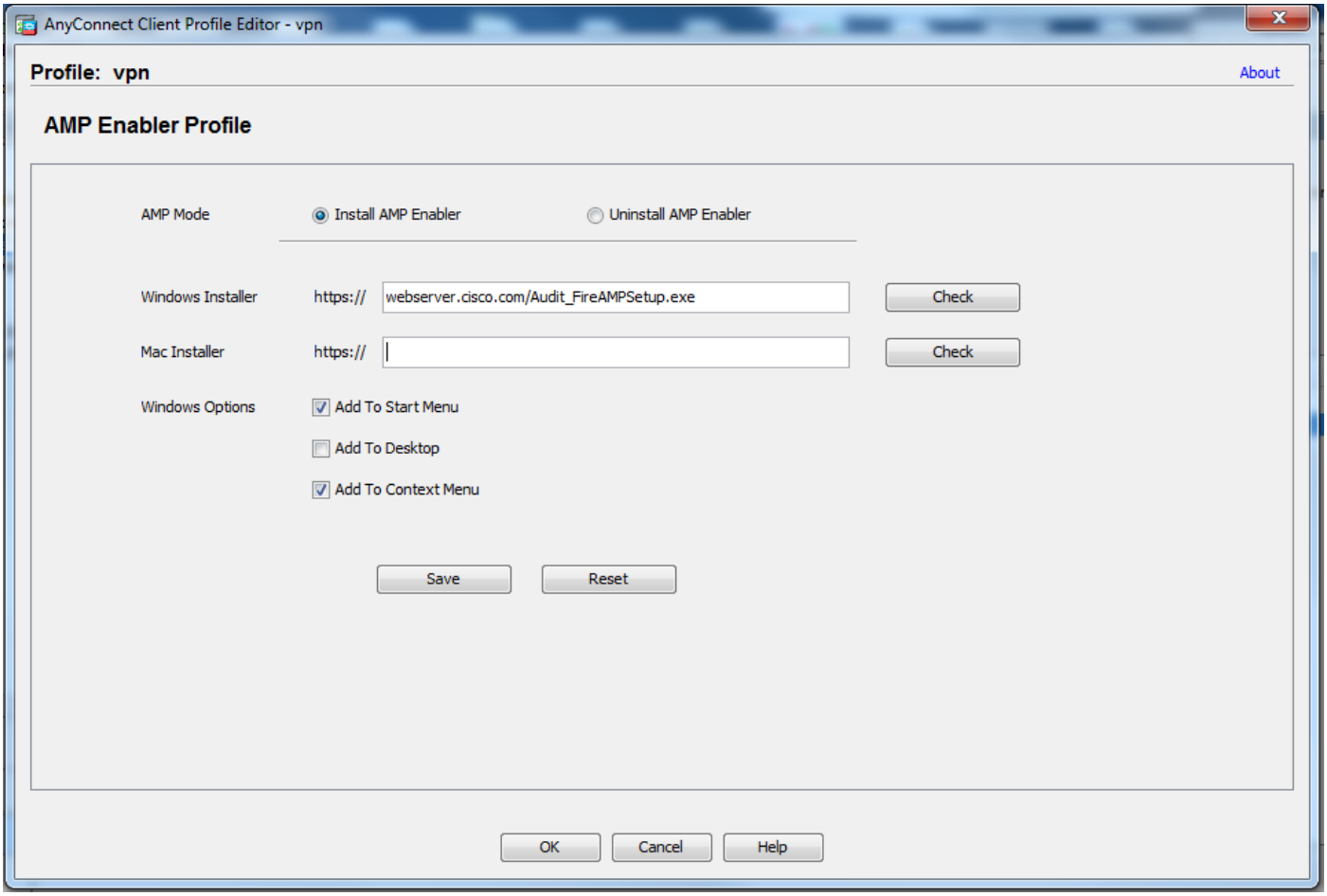


Шаг 4. : Загрузите веб-профиль клиента безопасности

Вернитесь к Профилю AMP, созданному прежде на ASA (Шаг 1), и измените **Профиль включателя AMP**:

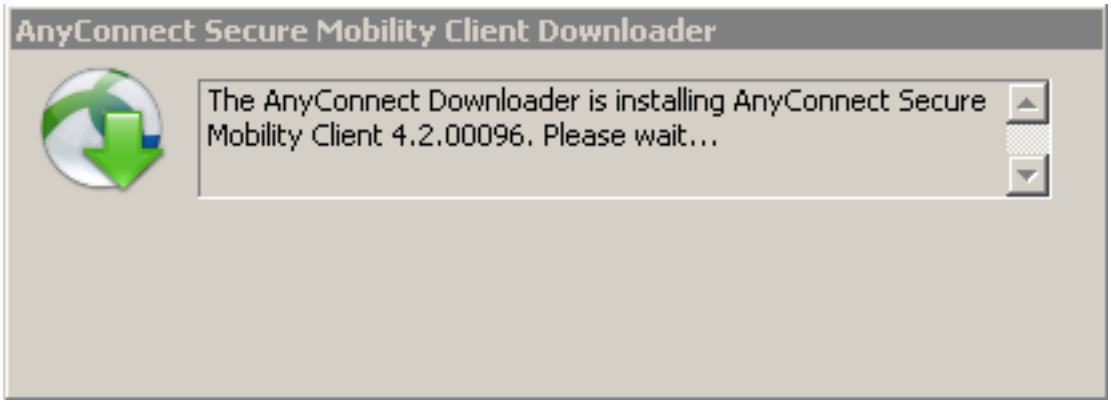
1. Для **Режима AMP** нажмите кнопку с зависимой фиксацией **Install AMP Enabler**.
2. В поле **Windows Installer** добавьте IP для Web-сервера и файл для FireAMP.
3. **Windows Options** являются дополнительными.

Нажмите **OK** и примените изменения.



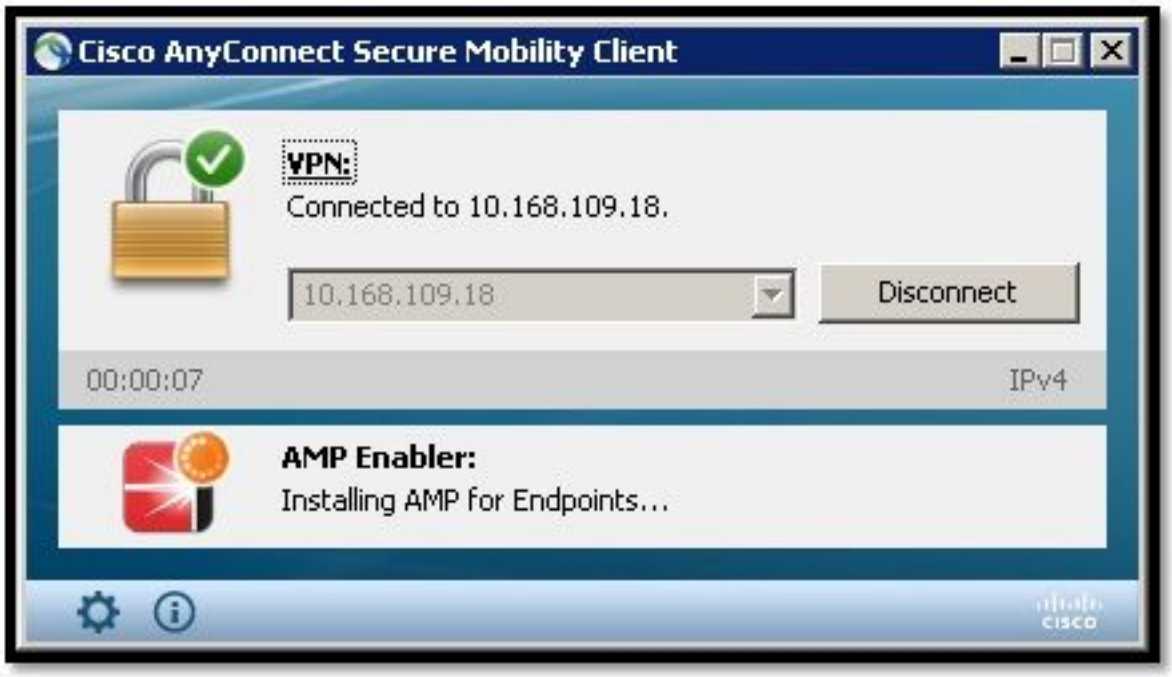
Шаг 5. : Подключение с AnyConnect и проверяет установку модуля

Когда пользователи VPN Anyconnect соединяются, ASA выдвигает модуль включателя AMP AnyConnect через VPN. Для уже вошел в пользователей, рекомендуется выйти из системы и затем войти назад для функциональности, которая будет включена.



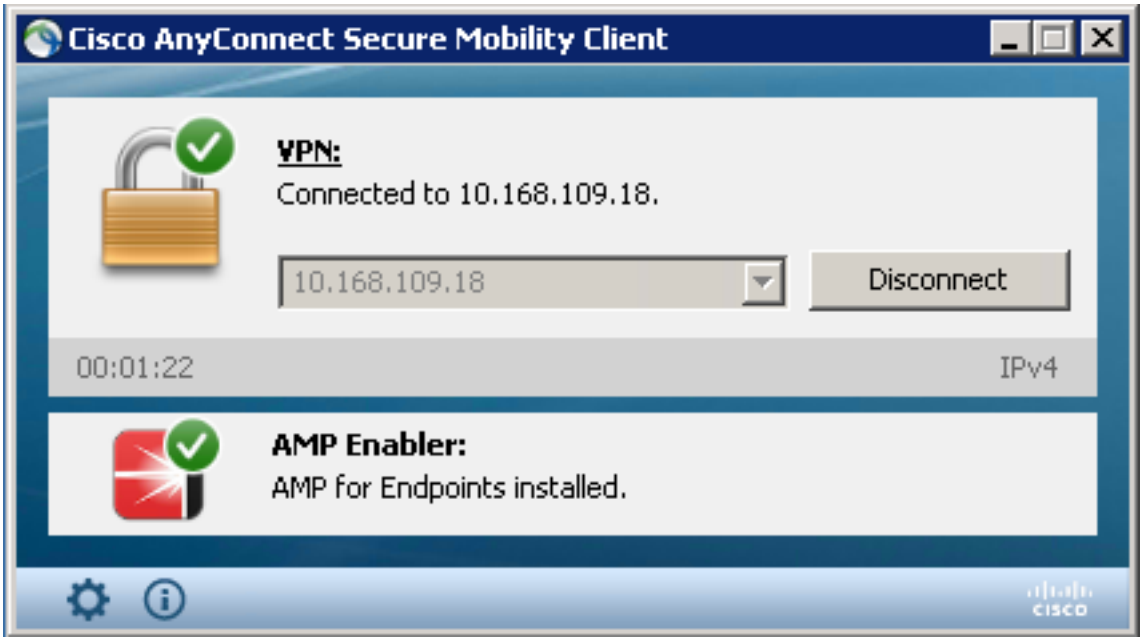
Шаг 6: Проверьте VPN-подключение и включатель AMP

Проверьте, связана ли VPN, и **включатель AMP** собирает конфигурацию от Web-сервера.



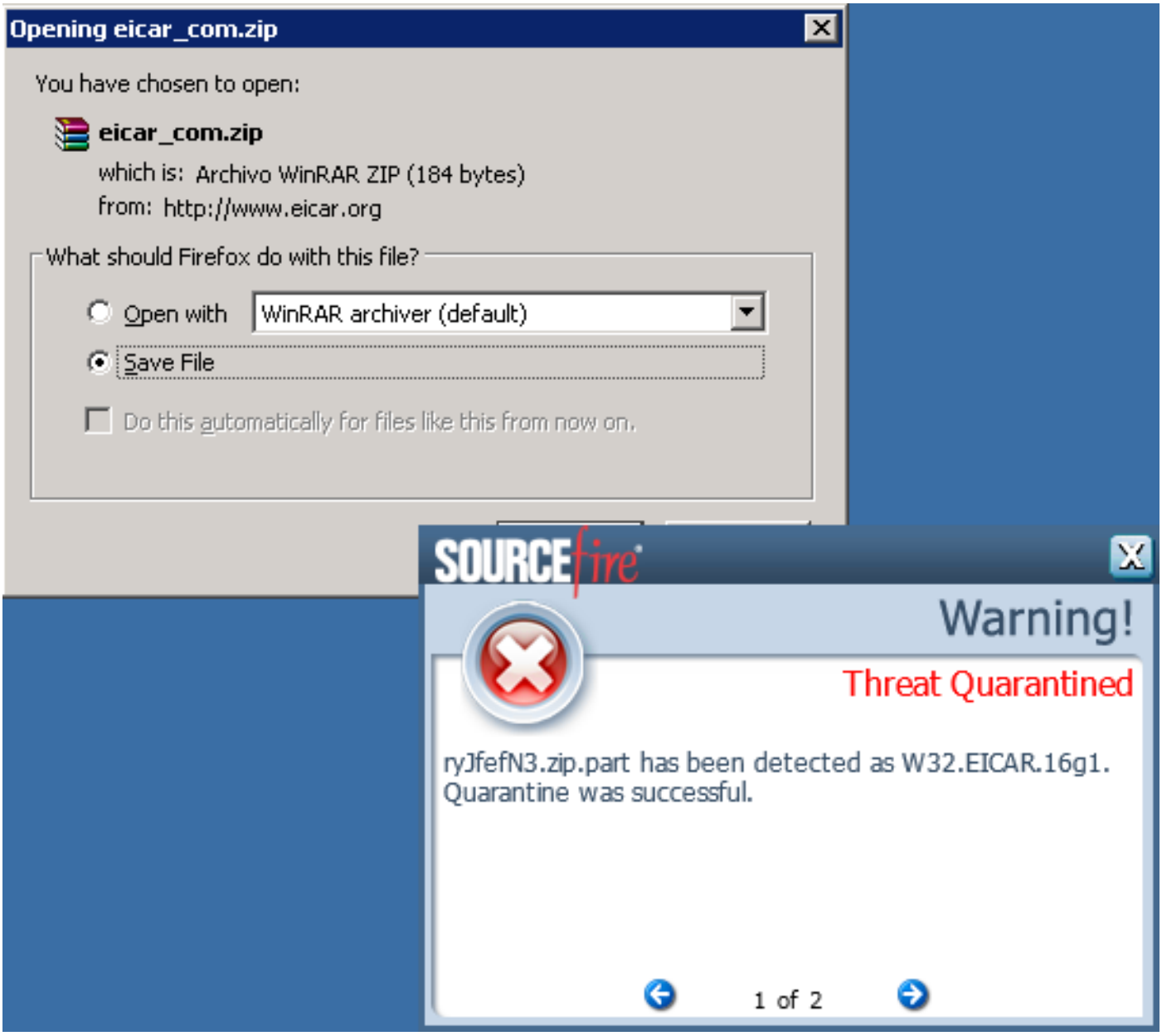
Шаг 7: Проверьте AnyConnect и Проверьте, Установлено ли Все

Как только VPN связана, и конфигурация Web-сервера установлена, проверьте AnyConnect и проверьте, что все установлено должным образом.



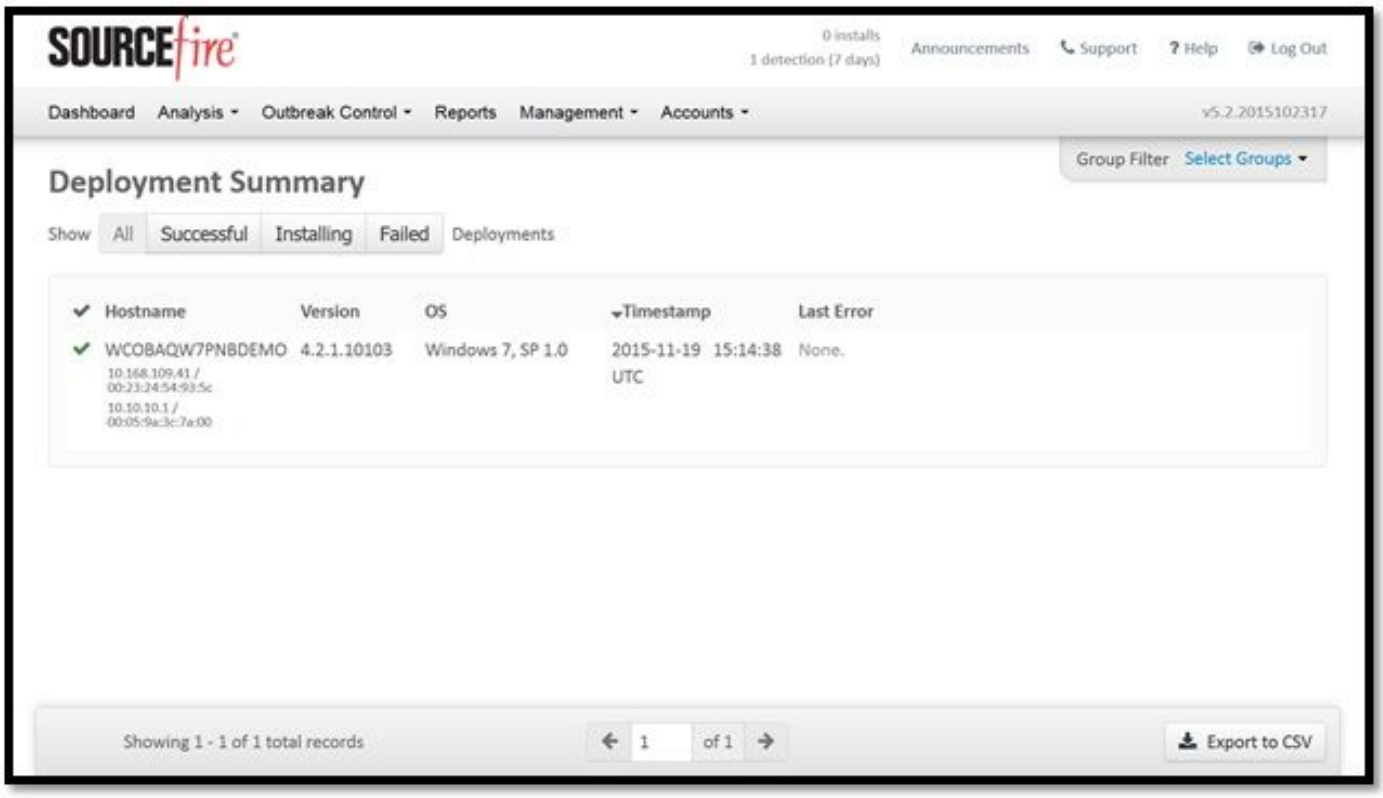
Шаг 8: Тест со строкой Eicar, содержавшейся в файле архива zip в компьютере

Тест со строкой Eicar, содержавшейся в файле архива zip в компьютере, чтобы проверить, работает ли все как ожидалось.



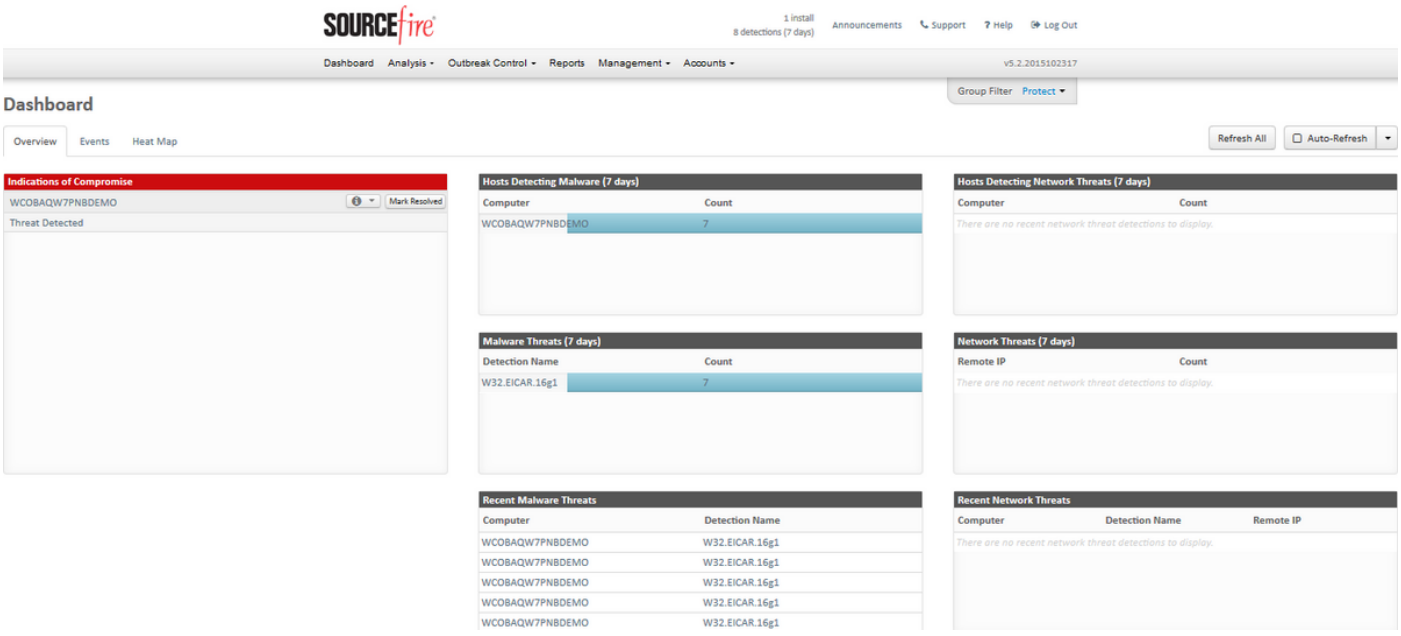
Шаг 9: Сводка развертываний

Эта страница показывает вам список успешных и отказавших установок разъёма FireAMP, а также в настоящее время происходящих. Можно перейти **к менеджменту> Сводка Развертываний**.



Шаг 10: Проверка обнаружения потока

Эта страница показывает вам список потоков, заблокированных разъёмом FireAMP и также машинами, на которые повлияли. Можно перейти **к Информационной панели**.



Дополнительные сведения

Несовместимое программное обеспечение для Windows Connector FireAMP:

- Зональный сигнал тревоги пунктом проверки
- Сажа
- Программное обеспечение Res AppGuard

Дополнительные сведения

- Настройте включатель AMP
- Cisco Systems – техническая поддержка и документация