NAC 4.5: Пример конфигурации импорта и экспорта политик

Содержание

Введение

Этот документ предоставляет пошаговые инструкции о том, как настроить функцию Импорта и экспорта политики (PIE) на Выпуске 4.5 NAC Cisco. Цель этой функции состоит в том, чтобы синхронизировать фильтры устройств, трафик и правила исправления и профили порта между Менеджерами NAC (Уберите Access Manager). Когда эта функция обсуждена, Менеджера NAC, где политика определена, называют **Ведущим устройством**, которое может выдвинуть или синхронизироваться, политика целых десяти Менеджеров NAC (Уберите Access Manager), названный **Приемниками**. Политика может синхронизироваться автоматически с предварительно установленным таймером или через ручное синхронизование.

Предварительные условия

Cisco рекомендует иметь знакомство с диспетчером Cisco NAC Manager (Уберите Access Manager), веб-интерфейс и политика, которая, как правило, настраивается. См. Комментарии к выпуску для Выпуска 4.5 NAC Cisco для получения информации о том, что поддерживается и не поддерживаемое с КРУГОМ.

Требования

Установите Менеджера (менеджеров) NAC и Сервер (серверы) по словам Руководства по установке и конфигурированию NAC Cisco. См. Рекомендации по оптимальному использованию для менеджера NAC Настройки Полики Импорт-Экспорта для определения, какой Менеджер должен использоваться в качестве Ведущего устройства и который как Получатель. Этот документ предполагает, что Менеджеры NAC Ведущего устройства и

Получателя определены, и рекомендации по оптимальному использованию используются.

Используемые компоненты

Сведения в этом документе основываются на программном обеспечении NAC Cisco 4.5.0.

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.

Условные обозначения

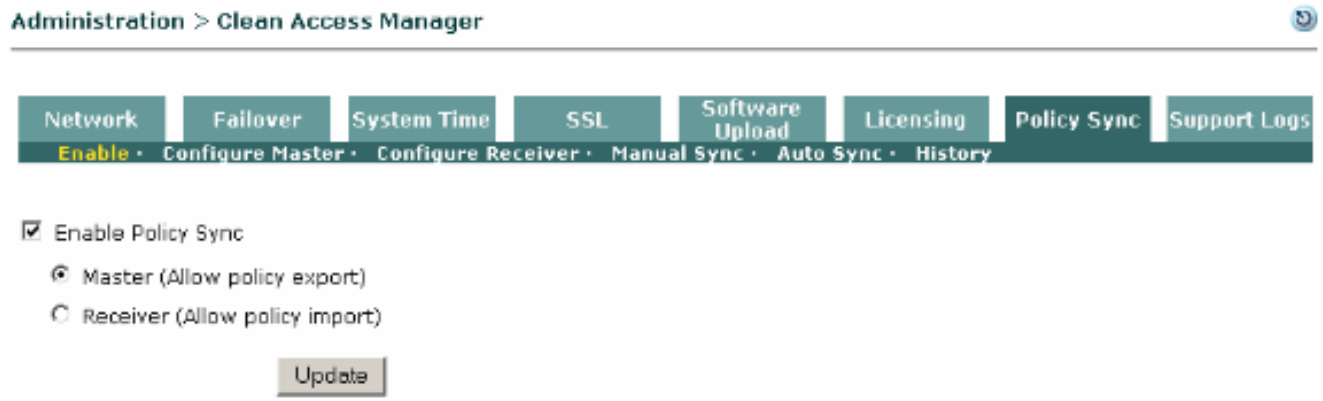
Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Примечание: Перед началом подтвердите, что Ведущее устройство и Получатель (получатели) выполняют те же самые версии. Кроме того, гарантируйте, что Ruleset Обновляют настройки под **Управлением устройствами> Чистый Доступ> Обновления>** соответствие **Обновления** на Ведущем устройстве и всех Приемниках.

NAC настраивает

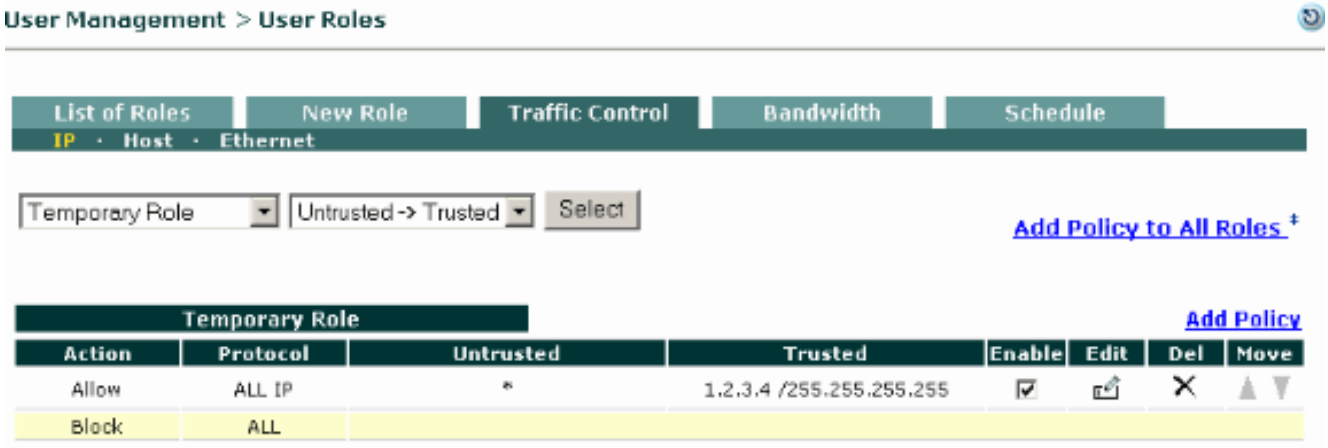
В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Выполните эти шаги для настройки Импорта/Экспорта Политики между Менеджерами NAC.

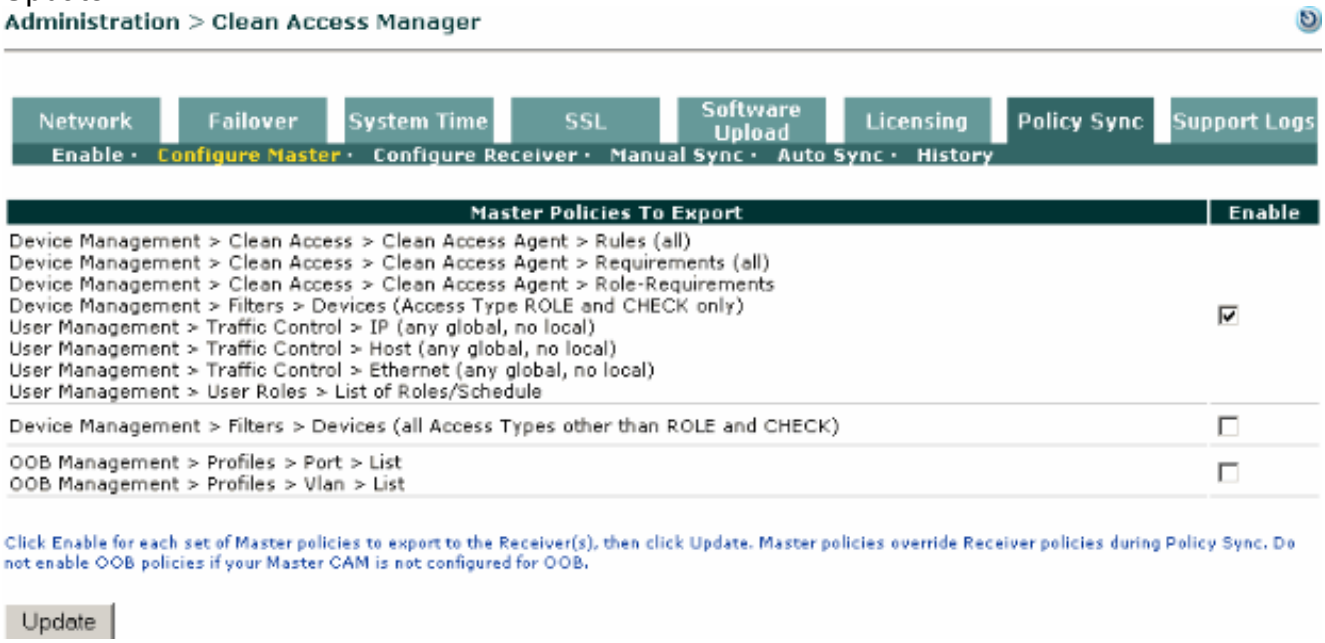
1. **Включите синхронизование политики на основном менеджере NAC:**На Основном Менеджере NAC перейдите к администрированию> Менеджер CCA>, Синхронизование Политики>
   Включает.
   

   Установите **Разрешать** флажок **Синхронизования Политики**. Выберите **Master (Экспорт политики Allow)** опция и нажмите **Update**.
2. **Определите политику, которая будет выдвинута:**В этом шаге вы определяете Политику, которая должна синхронизироваться между Основным CAM и Приемниками. Для данного примера цель состоит в том, чтобы синхронизировать политику Контроля за Глобальным трафиком между менеджерами. В этом случае Глобальная Политика Трафика на основывании IP должна быть выбрана под Ролями пользователя> Управление трафиком> IP (Выберите Временную Роль, Недоверяемую> Доверяемый

выпадающему, как показано. Нажмите Select. Это правило еще НЕ существует на получателе.

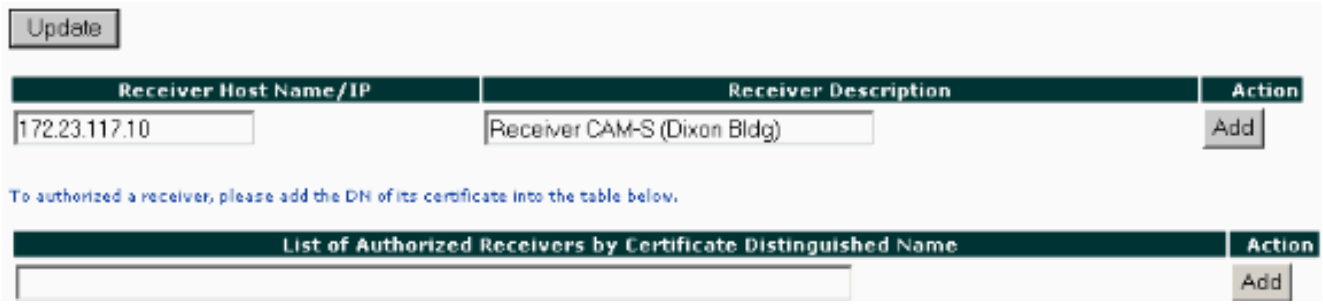


См. [Включают Глобальную Информационную политику Трафика на основывании IP](), как настроить Политику IP - трафика.Выберите Administration> Clean Access Manager> Policy Sync> Configure Master и проверьте флажок Enable как показано и нажмите Update.

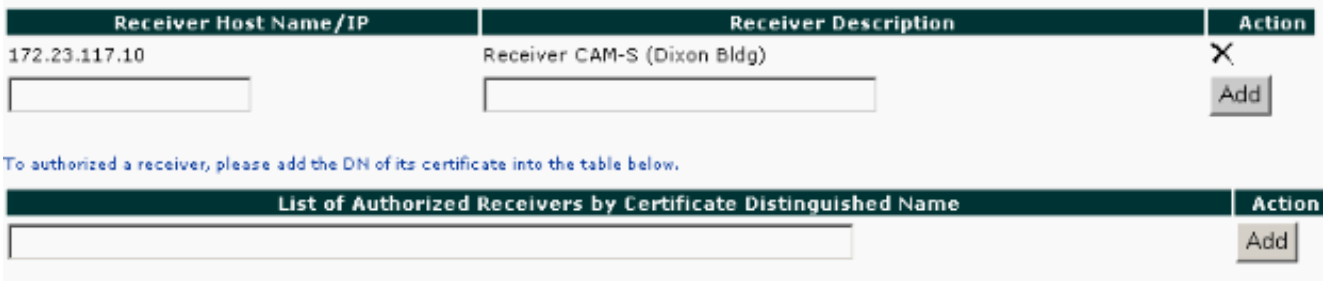


Примечание: Синхронизация Полицейских Трафика также требует синхронизирующихся Правил, Требований, Требования Роли, Фильтры устройств (РОЛЬ, ПРОВЕРЬТЕ типы), и Роли.

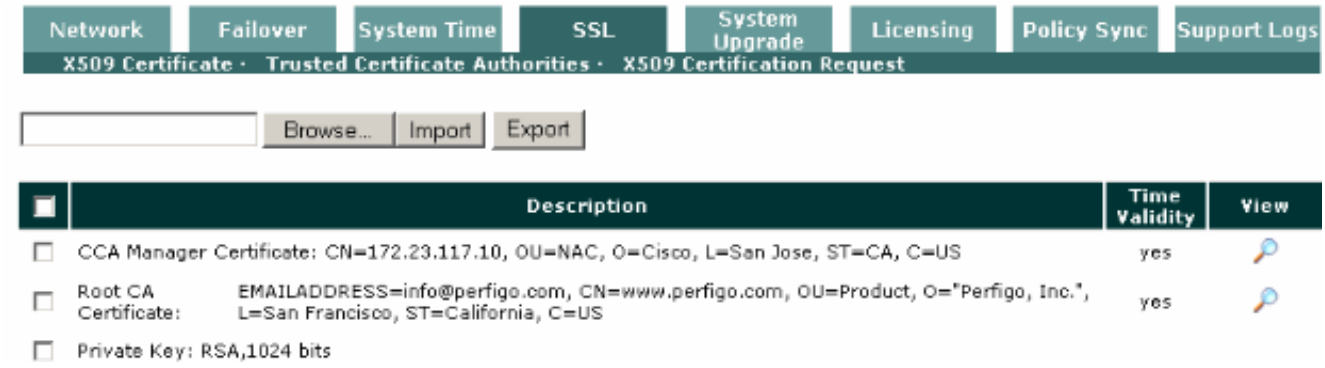
3. **Добавьте/Определите Получатель (получатели):**Можно составить в целом десять поддерживаемых Приемников Ведущему устройству. В данном примере вы добавляете один Получатель к Основному Менеджеру NAC.Выберите Administration> Clean Access Manager> Policy Sync> Configure Master. Под/IP Имени хоста Получателя добавьте Имя хоста (Основной Менеджер NAC должен быть в состоянии решить DNS для имени хоста), или IP-адрес Получателя. Добавьте дополнительное описание и нажмите Add.



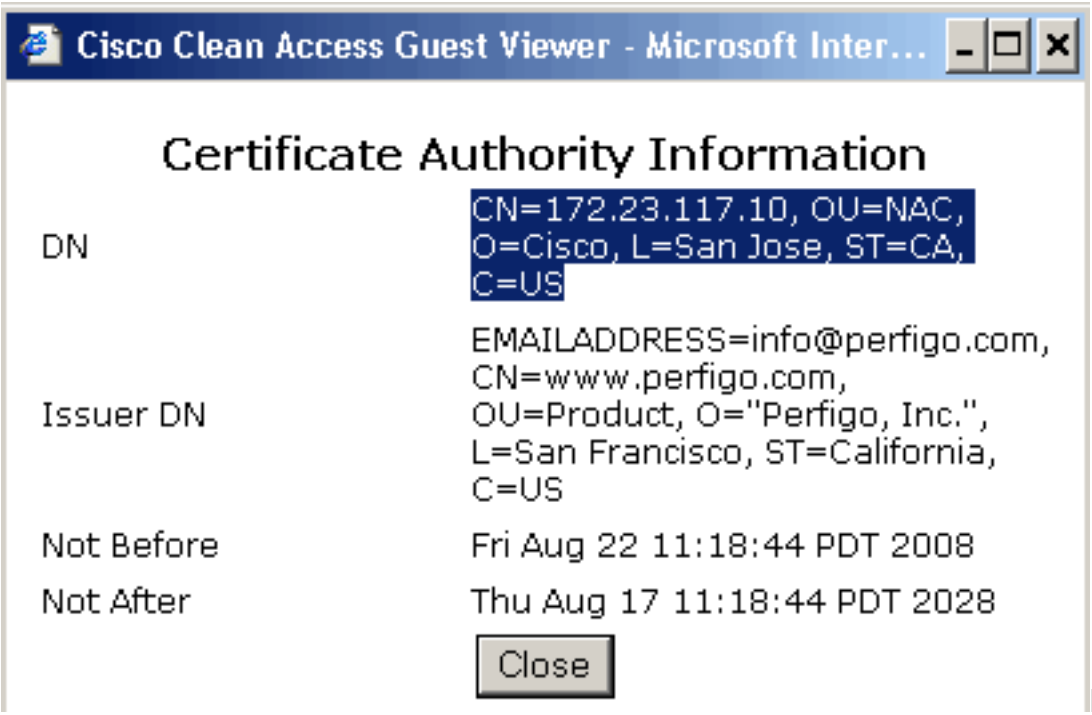
После того, как добавленный, новый Получатель появляется. Можно добавить несколька приемников (до десяти поддерживаемых) этот путь. В сценариях Высокой доступности (HA) необходимо добавить Действительное/Совместно используемое Имя хоста или Действительный/Совместно используемый IP-адрес Пары HA к списку.



4. **Авторизуйте получатель (получатели):**После добавления Получателя (получателей) важно защитить связь между Ведущим устройством и Получателем (получателями). Только Уполномоченное Ведущее устройство в состоянии выдвинуть политику к Получателю. Точно так же Ведущее устройство должно быть в состоянии связаться только с санкционированными Приемниками. Кроме того, доверие должно быть установлено для проверки, Ведущее устройство и Приемники - то, кем они утверждают, что были. SSL используется для этой цели. Мало того, что Ведущее устройство и Получатель должны определить друг друга через Данные DN в сертификате, но у них также должен быть свой сертификат идентификации от Доверяемых полномочий (CA). Короче говоря, Ведущее устройство и Получатель должны доверять сертификатам друг друга.Так как этот документ генерируется от лабораторной установки, подписанные сертификаты используются в данном примере. Однако обратите внимание, что необходимо использовать подписанный сертификат CA в производственной среде. См. Рекомендации по оптимальному использованию для менеджера NAC Настройки Полики Импорт-Экспорта для получения дополнительной информации.На Получателе выберите Administration> CCA Manager> SSL> X509 Certificate.

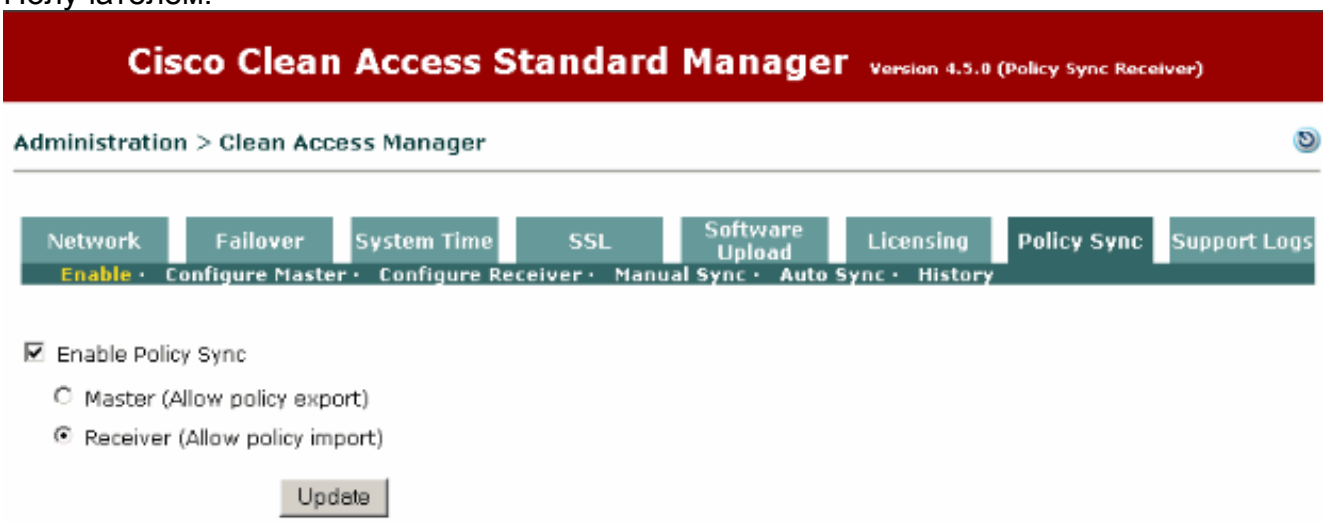


Определите менеджера CCA Сертификэйта и щелкните по значку при Представлении. В Окне, которое появляется, выберите и скопируйте (щелкните правой кнопкой мыши и скопируйте), Данные



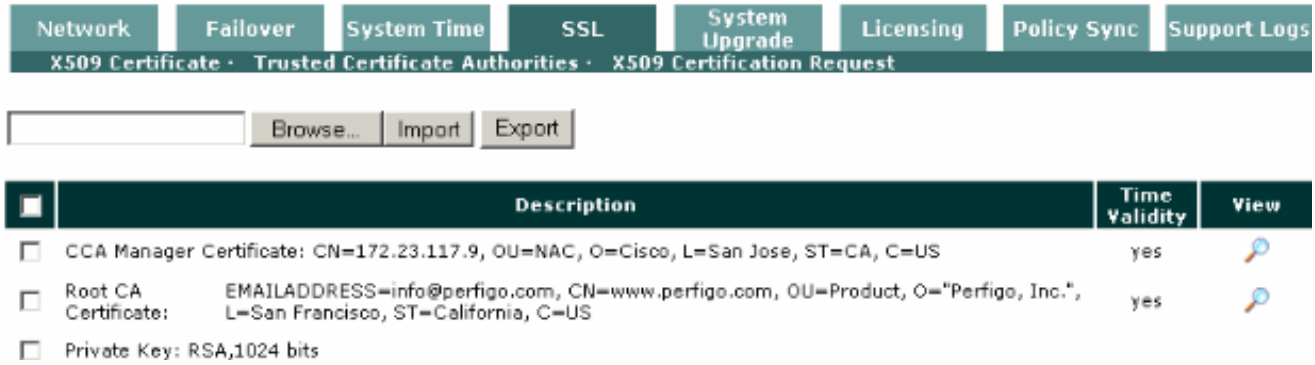
DN. Возвратитесь к Основному Менеджеру NAC при администрировании> Менеджер CCA>, Синхронизование Политики> Настраивает Ведущее устройство. В нижней части, под Списком Санкционированных Приемников Составным именем Сертификата, вставляют Данные DN сертификата, которые вы скопировали с Получателя в предыдущем шаге, и нажмите
Add.

5. **Включите синхронизование политики на менеджере NAC получателя:**На Менеджере NAC Получателя перейдите к администрированию> Менеджер CCA>, Синхронизование Политики> Включает.Установите **Разрешать** флажок **Синхронизования Политики**. Выберите **Receiver (Импорт политики Allow)** опция и нажмите **Update**.**Примечание:** Заметьте, что баннер на вершине покраснел, который указывает, что этот Менеджер NAC является включенным, чтобы быть Получателем.

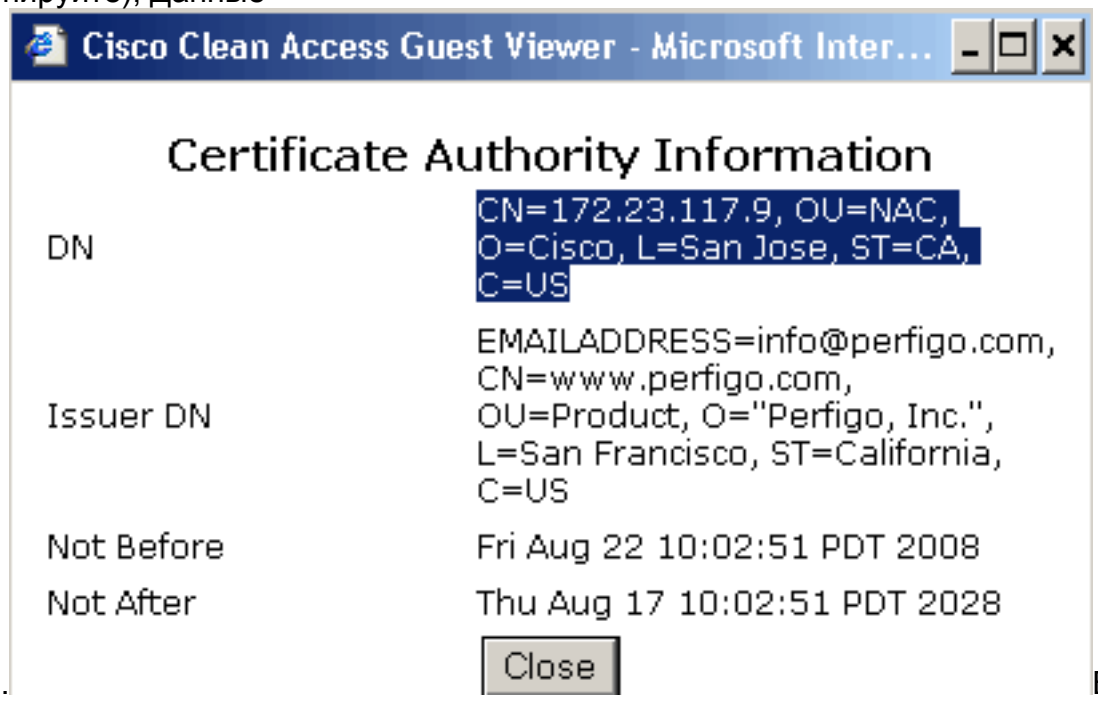


6. **Авторизуйте ведущее устройство:**На Ведущем устройстве выберите Administration>

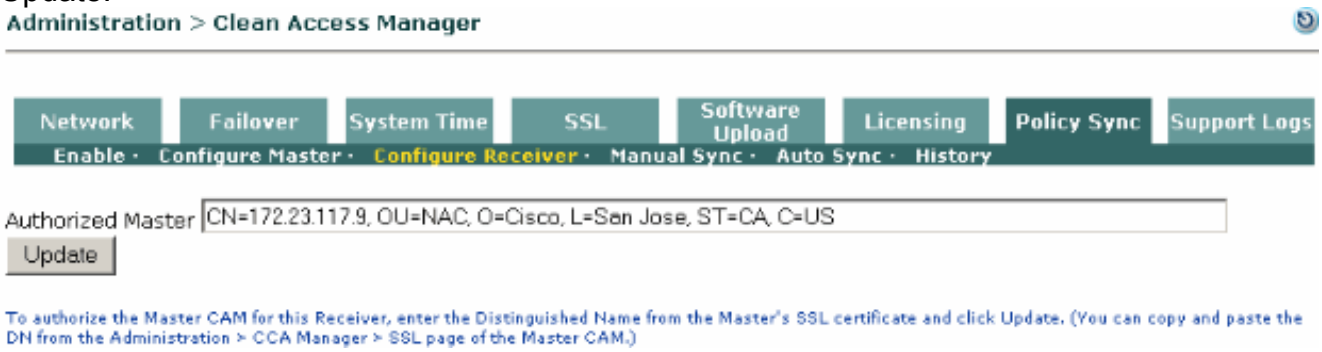
CCA Manager> SSL> X509
Certificate.



Определите менеджера CCA Сертификэйта и щелкните по значку при Представлении. В Окне, которое появляется, выберите и скопируйте (щелкните правой кнопкой мыши и скопируйте), Данные

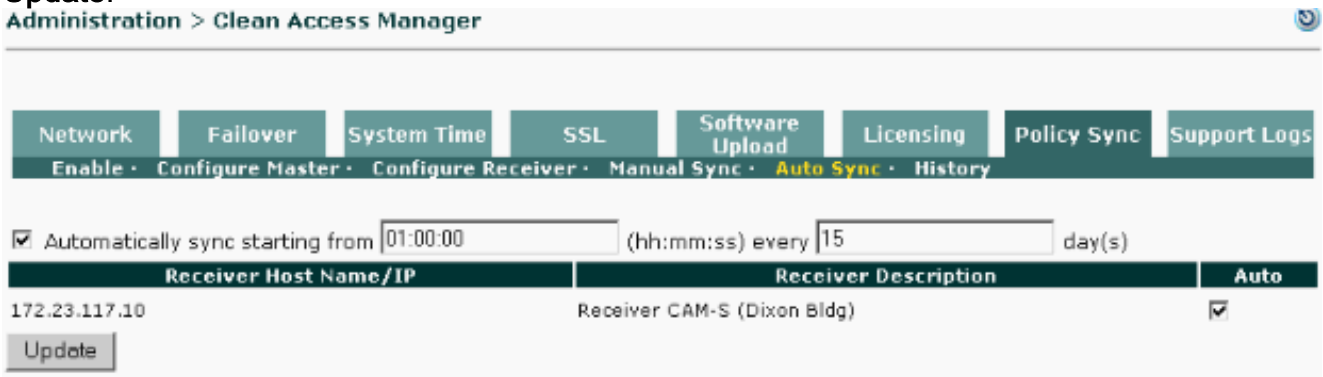


DN. Возвратитесь к Менеджеру NAC Получателя при администрировании> Менеджер CCA>, Синхронизование Политики> Настраивает Получатель. Рядом с Уполномоченным Ведущим устройством вставьте Данные DN сертификата, которые вы скопировали от Ведущего устройства в предыдущем шаге, и нажмите
Update.



7. **Настройте автоматическое синхронизование (Необязательно):**Синхронизование политики может быть ручным или автоматизировано. Ручное синхронизование может быть выполнено по мере необходимости, в то время как Автоматический Синхронизирующий Таймер может быть настройкой для автоматического выполнения синхронизования политики между Менеджерами NAC один раз в *x* число дней

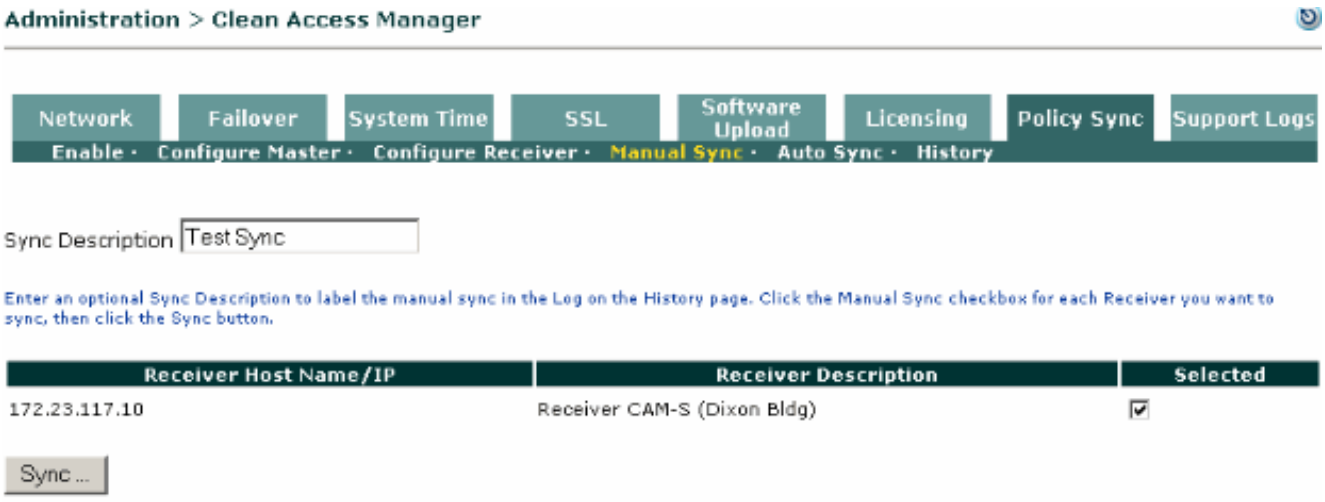
(минимум является одним днем) в предустановленное время. Cisco строго рекомендует, чтобы вы выполнили Ручное синхронизование и проверили, что синхронизование работает успешно перед включением Автоматического синхронизования между Менеджерами NAC. Посмотрите Устранение неполадок, чтобы понять, как можно использовать Ручное Синхронизование для решения проблем, отнесенных к КРУГУ.Для включения Автоматического синхронизования перейдите к администрированию> Менеджер CCA> Синхронизование Политики> Автоматическое Синхронизование на Основном Менеджере NAC.Проверьте **Автоматически синхронизирующее начало с ___ (hh:mm:ss) каждый ___ флажок дня (дней)**.Введите время синхронизования (1:00 в данном примере) и как часто (каждые 15 дней в данном примере), что вы хотите выполнить Автоматическое Синхронизование.Установите флажок под **Автоматическим** для выбора Receiver, которые автоматически получают политику по периодической основе и нажимают **Update**.



Проверка

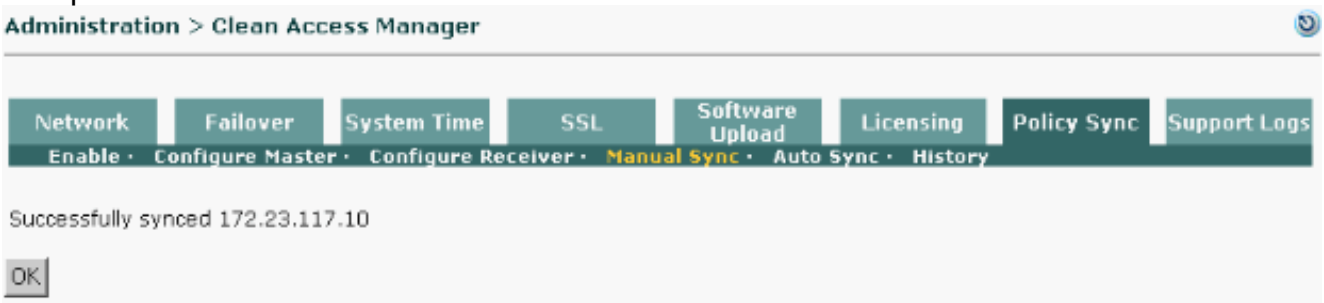
Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

1. Перейдите к администрированию> Менеджер CCA> Синхронизование Политики> Ручное Синхронизование на Ведущем устройстве.
2. Введите имя (дополнительное) для Синхронизации в соответствии с Синхронизирующим Описанием
3. Выберите Receiver, с которым вы хотите выполнить Синхронизирующее действие. Установите флажок под Выбранным, и нажмите **Sync**. В данном примере у вас есть только один Получатель, 172.23.117.10, таким образом, это выбрано.

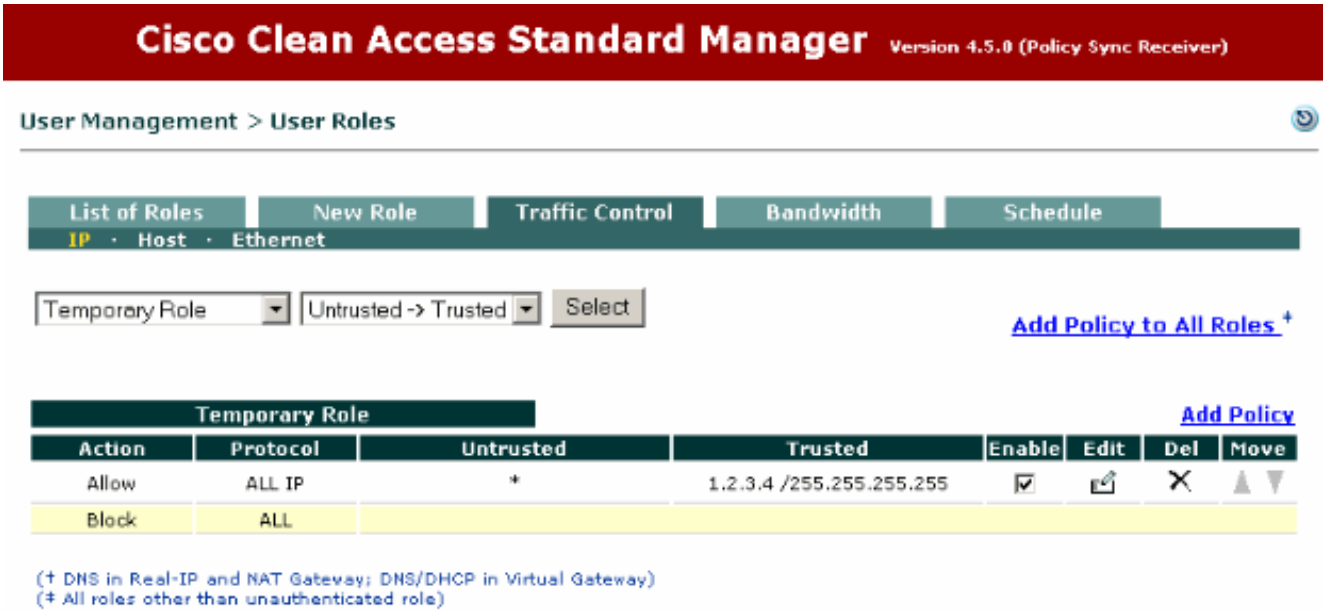


4. На этом этапе Ведущее устройство выполняет предсинхронизирующую проверку работоспособности против Получателя. Предсинхронизирующая проверка гарантирует, что менеджеры NAC Ведущего устройства и Получателя настроены правильно (чтобы Выдвинуть и Получить политику), и что сведения авторизации корректны и т.д. Если существует какая-либо конфигурация или ошибки Авторизации, предсинхронизирующие сбои проверки с соответствующими сообщениями об ошибках. Посмотрите раздел Устранения неполадок.
5. Если нет никакой конфигурации или проблем авторизации, Ведущее устройство отображает успешную предсинхронизирующую проверку.

6. Соответствие продолжает успешно завершать синхронизование.



7. Перейдите к Менеджеру NAC Получателя и проверьте, что синхронизируется Правило передачи трафика.



Устранение неполадок

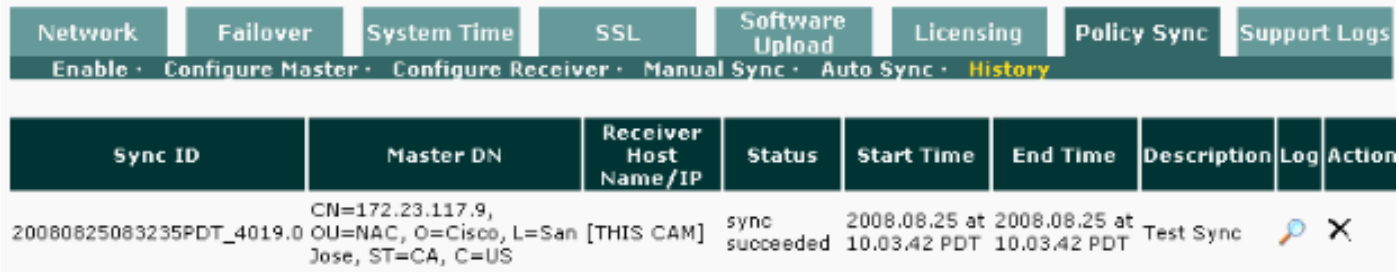
В этом разделе описывается процесс устранения неполадок конфигурации.

Регистрация

Синхронизирующая сводка зарегистрирована при Менеджере CCA> Синхронизование Политики> История на Ведущем устройстве и Получателе (получателях).

На основном менеджере NAC:

На менеджере NAC получателя:



Нажмите Magnifying Glass Icon под Журналом для просмотра подробных журналов транзакций:

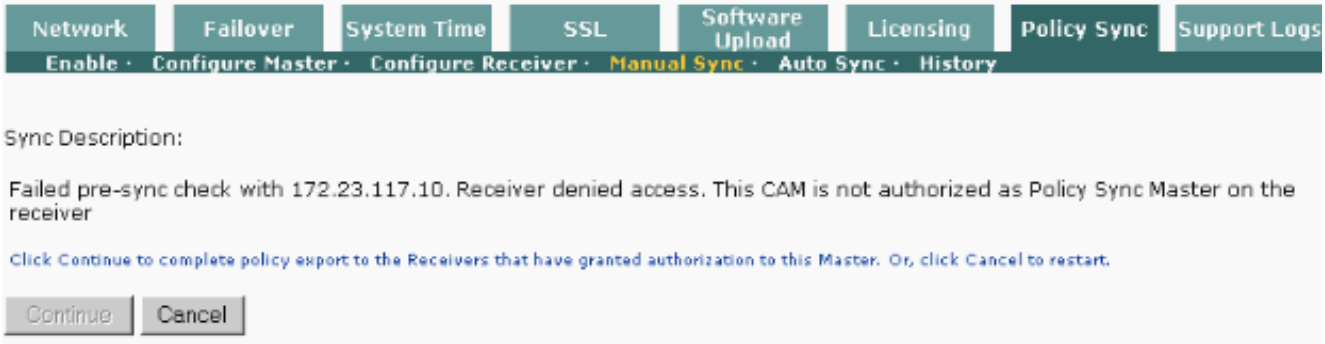
```
************** Master Log **************

Starting policy import/export on Policy Sync Master.
Created dump file for policy: User Management -> User Roles -> List of Roles/Schedule
Created dump file for policy: Device Management > Clean Access > Clean Access Agent > Role-
```

```
Requirements
Created dump file for policy: Device Management > Filters > Devices
Created dump file for policy: User Management->Traffic Control->IP
Created dump file for policy: User Management->Traffic Control->Host
Created dump file for policy: User Management->Traffic Control->Ethernet
Dump file creation is complete.
Created policy import/export dump file.
Created  policy import/export header file.
Created policy import/export tar file.


*************** Receiver Log ***************

Starting policy import on Policy Sync Receiver.
Hash value is a match.
Policy Sync Master and Receiver CAM versions match.
All SQL statements successfully executed
All requirements are valid.
All rules are valid.
Role tables integrity check is successful.
```

Импорт/экспорт политики успешно завершен на Получателе Синхронизования Политики.

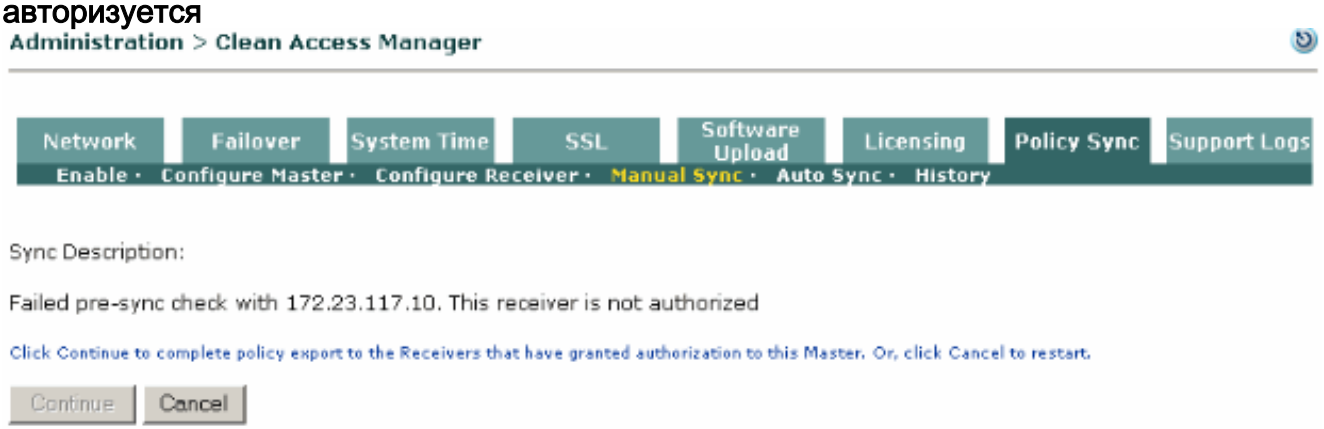
Проблемы

1. **Получатель запретил доступ. Этот CAM не авторизуется как Ведущее устройство Синхронизования Политики на получателе.**



   Эта ошибка, как правило, означает, что Получатель отклоняет синхронизование политики, потому что Основные Данные DN неправильно сконфигурированы на Менеджере NAC Получателя. Выберите Administration> CCA Manager> Policy Sync> Configure Receiver на Получателе и удостоверьтесь, что “Санкционированная Основная” информация настроена правильно.

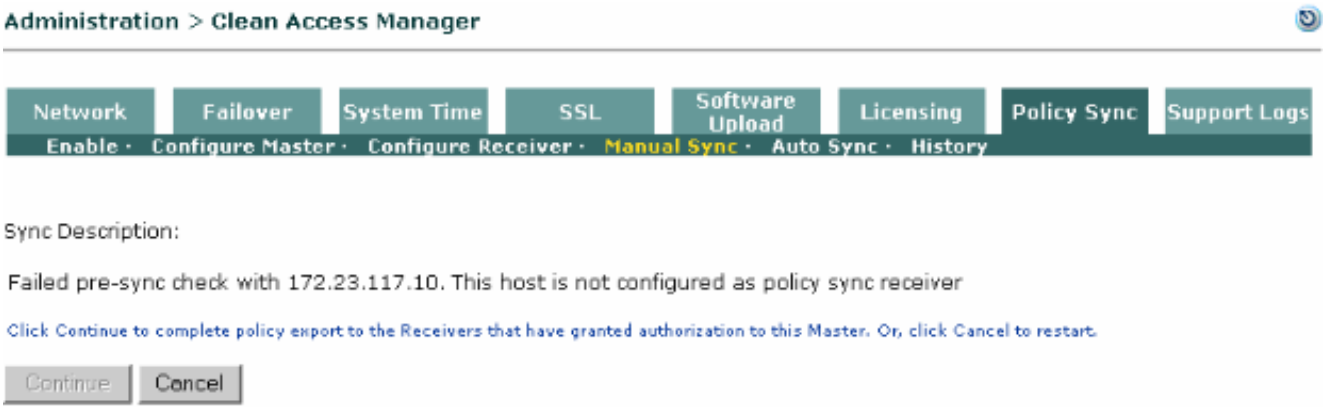
2. **Этот получатель не авторизуется**



   Это сообщение, как правило, означает, что Получатель не является настройкой для

Авторизации, или Параметры авторизации (Данные DN получателя) настроенный на Основном Менеджере NAC является неправильным. Выберите Administration> CCA Manager> Policy Sync> Configure Master на Ведущем устройстве и удостоверьтесь, что Данные DN сертификата Получателя существуют под Списком Санкционированных Приемников Составным именем Сертификата и настроены правильно.

3. **Этот хост не настроен как получатель синхронизования политики.**



Это сообщение, как правило, означает, что Ведущее устройство пытается синхронизировать к хосту, который или не включен для Синхронизования Политики, или это не настроено, чтобы быть Получателем. Выберите Administration> CCA Manager> Policy Sync> Settings на Менеджере NAC, который выбран, чтобы быть Получателем и гарантировать, что Включенный флажок Синхронизования Политики установлен и что Кнопка с зависимой фиксацией установлена в Получатель (Позвольте Импортировать Политику).

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация