Настройте и устраните неполадки внешних серверов tacacs на ISE

Содержание

Введение

Этот документ описывает функцию для использования Внешнего TACACS + Сервер в развертываниях с помощью Идентификационного механизма сервиса (ISE) в качестве прокси.

Предварительные условия

Требования

- Основное понимание Администрирования устройств на ISE.
- Этот документ основывается на Идентификационной версии 2.0 Механизма Сервиса, применимой на любой версии Идентификационной версии Механизма Сервиса выше, чем 2.0.

Используемые компоненты

> **Примечание:** Любая ссылка на ACS в этом документе может быть интерпретирована, чтобы быть ссылкой на любой Внешний TACACS + Сервер. Однако конфигурация на ACS и конфигурация на любом другом СЕРВЕРЕ TACACS могут варьироваться.

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

- Идентификационный механизм сервиса 2.0
- Система управления доступом (ACS) 5.7

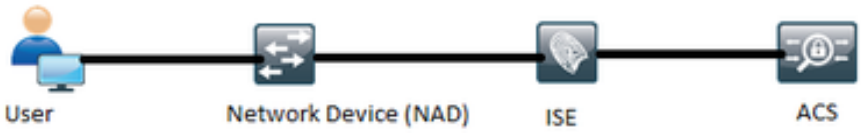
Сведения, представленные в этом документе, были получены от устройств, работающих в

специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. Если ваша сеть является оперативной, удостоверьтесь, что вы понимаете потенциальное воздействие любого изменения конфигурации.

Настройка

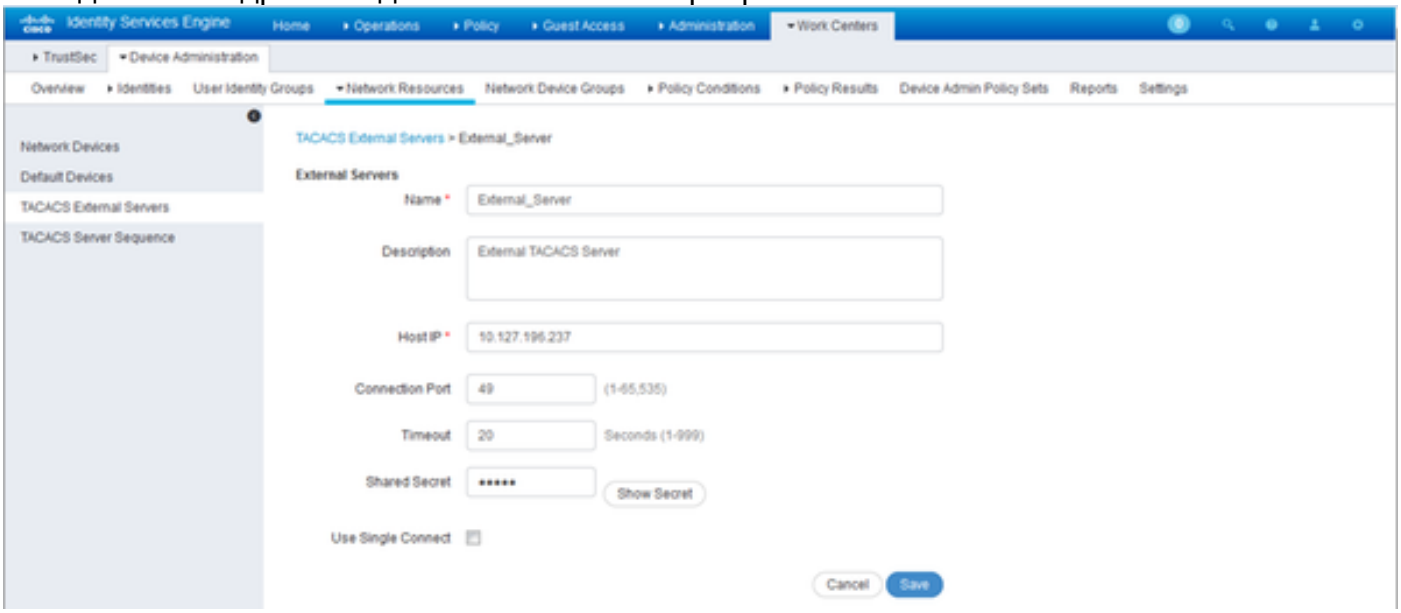
Этот раздел помогает настраивать ISE для проксирования TACACS +, запрашивает к ACS.

Схема сети



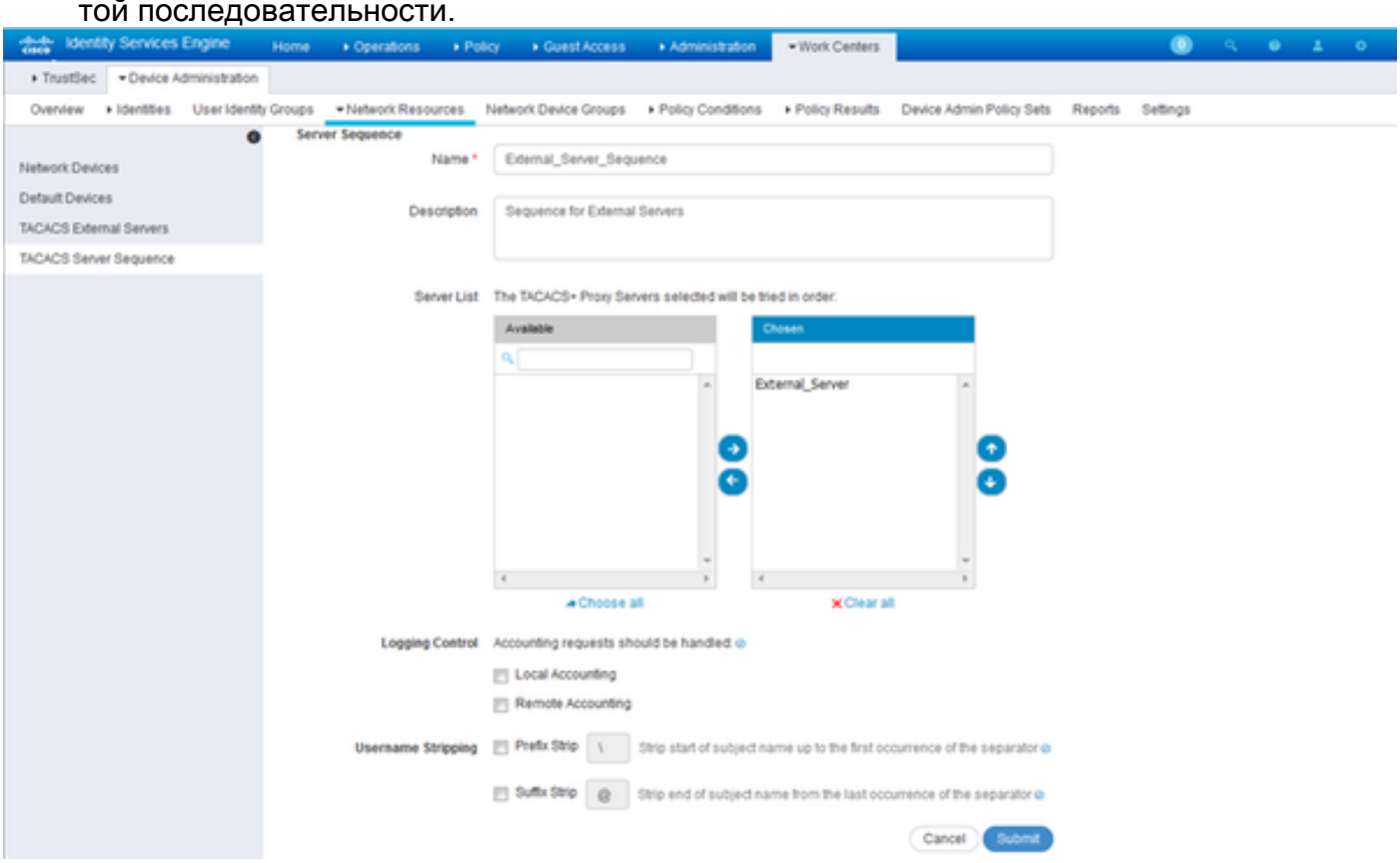
Настройте ISE

1. Множественные Внешние Серверы tacacs могут быть настроены на ISE и могут использоваться для аутентификации пользователей. Для настройки Внешнего TACACS + Сервер на ISE, перейдите для **Работы Центров> Администрирование устройств> Сетевые ресурсы> Внешние серверы TACACS. Нажмите Add** и заполните подробные данные Подробных данных Внешнего сервера.



Общий секретный ключ, предоставленный в этом разделе, должен быть той же тайной, используемой в ACS.

2. Для использования Внешнего настроенного СЕРВЕРА TACACS это должно быть добавленный в последовательности СЕРВЕРА TACACS, которая будет использоваться в наборах политики. Я упорядочиваю, чтобы настроить Последовательность СЕРВЕРА TACACS, перейти для **Работы Центров> Администрирование устройств> Сетевые ресурсы> Последовательность СЕРВЕРА TACACS. Нажмите Add,** заполните подробные данные и выберите серверы, которые необходимы, чтобы использоваться в той последовательности.

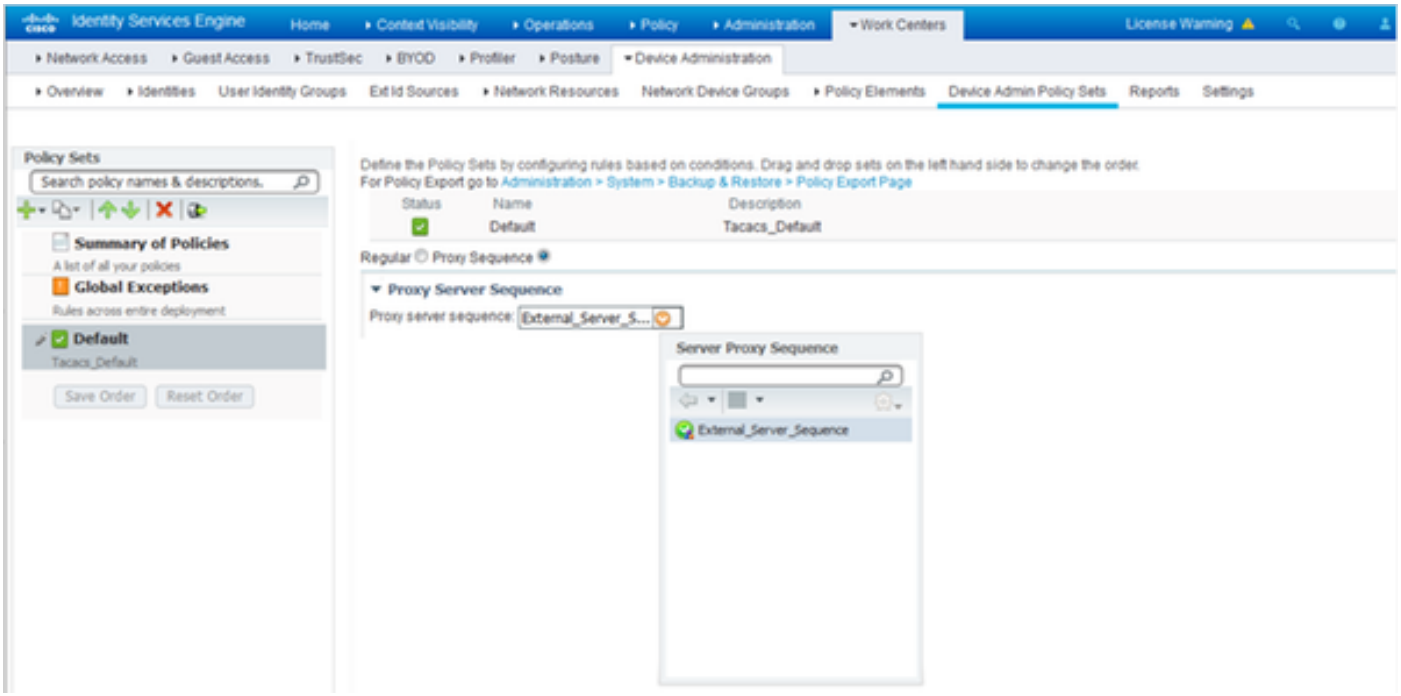


В дополнение к последовательности сервера были предоставлены две других возможности. Контроль за Регистрацией и Разделение Имени пользователя.

Контроль за Регистрацией дает опцию, чтобы или регистрировать бухгалтерские запросы локально на ISE или регистрировать бухгалтерские запросы к внешнему серверу, который обрабатывает аутентификацию также.

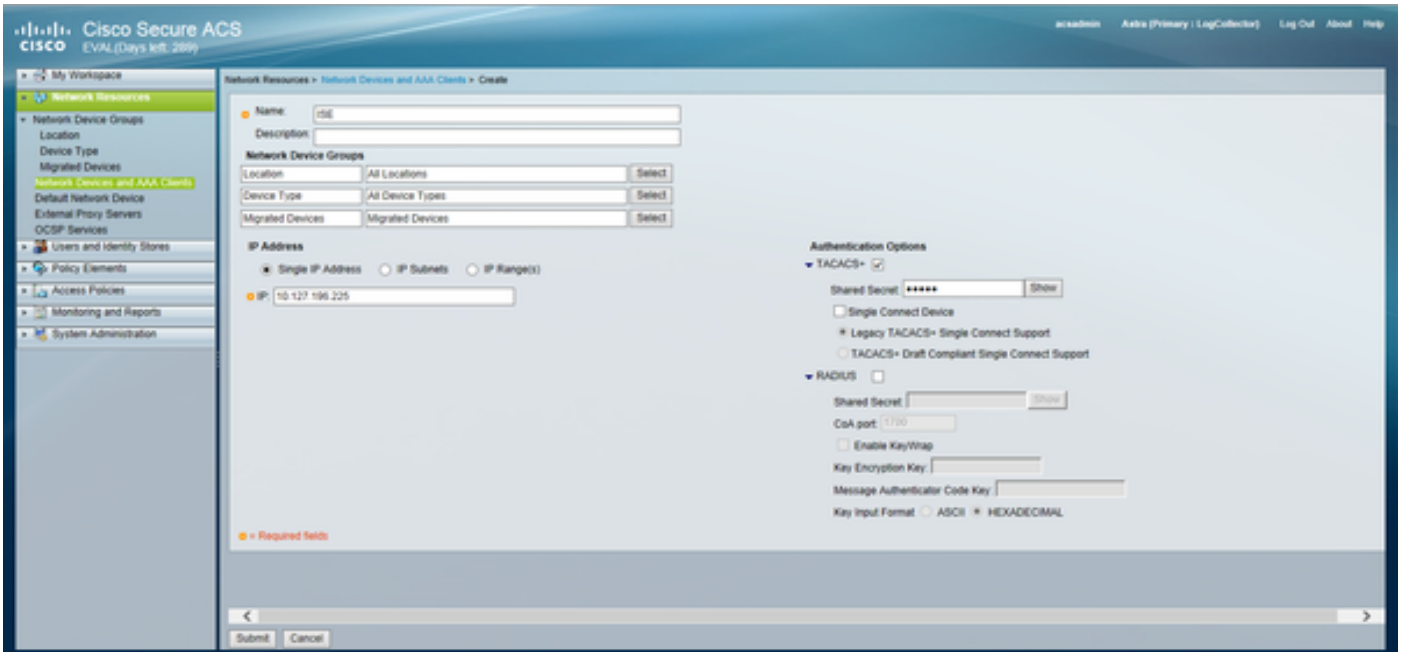
Разделение имени пользователя используется для разделения или Префикса или Суффикса sepcifying разделитель прежде, чем переслать запрос на Внешний СЕРВЕР TACACS.

3. Для использования Внешней настроенной Последовательности СЕРВЕРА TACACS наборы политики должны быть настроены для использования созданной последовательности. Для настройки наборов политики, чтобы использовать Последовательность Внешнего сервера, перейти для **Работы Центров> Администрирование устройств>, Наборы Политики Admin Устройства> [выбирают набор политики].** Переключите кнопку с зависимой фиксацией, которая говорит **Последовательность Прокси.** Выберите созданный External Server Sequence.

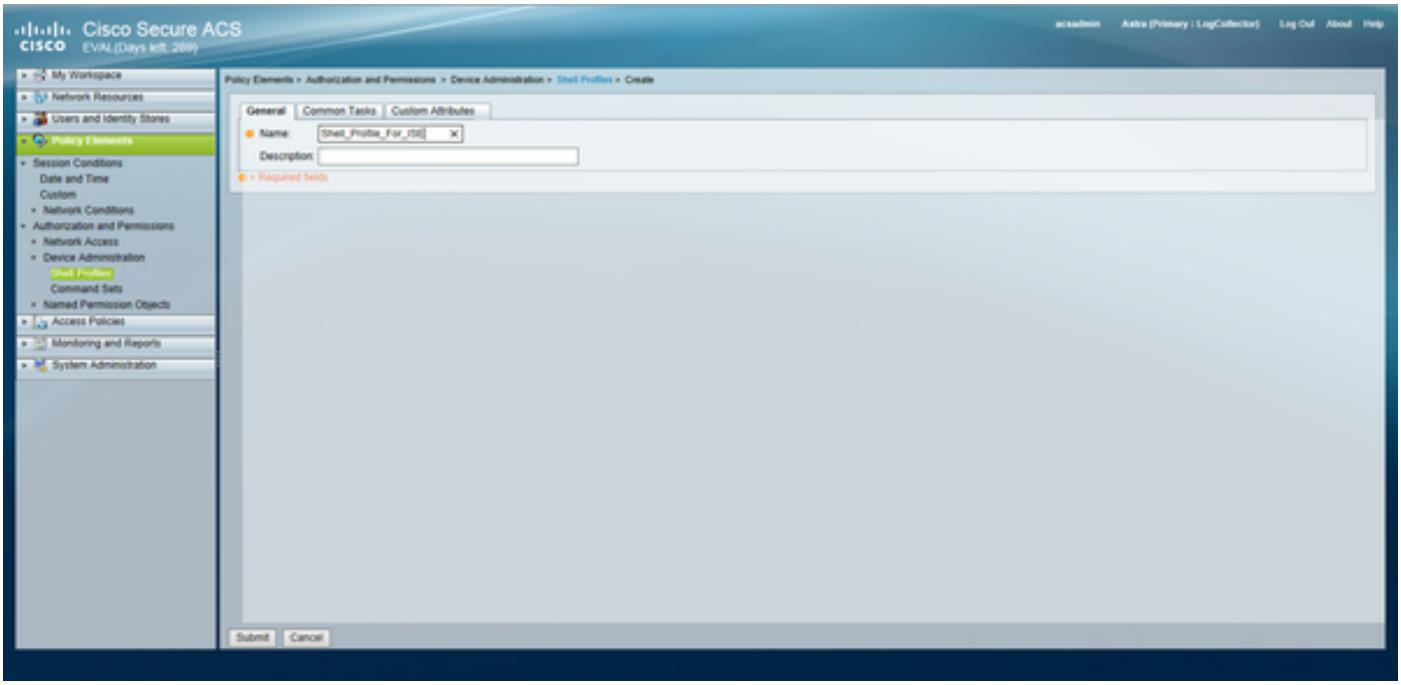


Настройте ACS

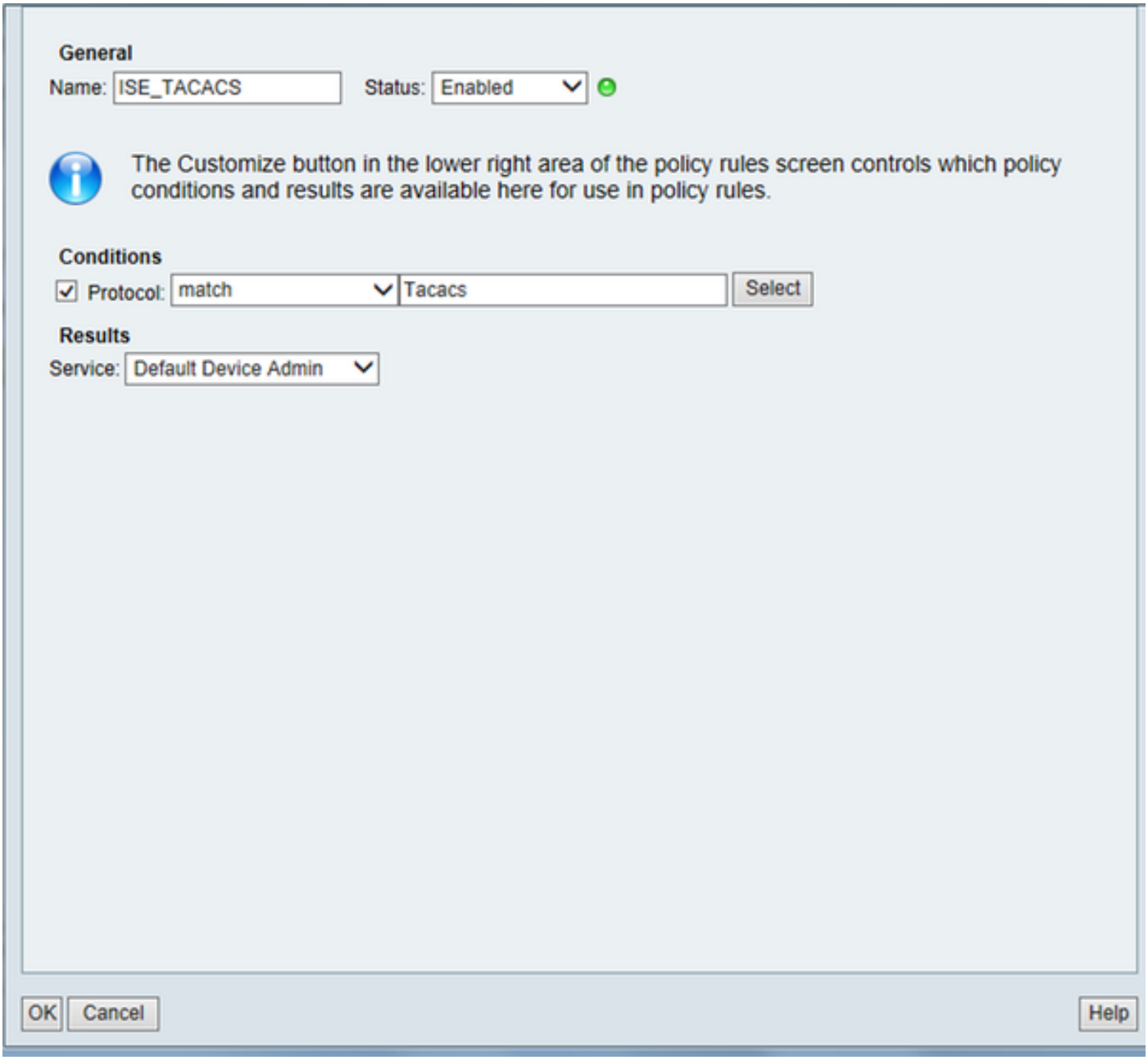
Для ACS ISE является просто другое Сетевое устройство, которое будет отправлять Запрос TACACS. Для настройки ISE как сетевого устройства в ACS перейдите к **Сетевым ресурсам> Сетевые устройства и Клиенты AAA.** Нажмите **Create** и заполните подробные данные Сервера ISE с помощью того же общего секретного ключа согласно конфигурации на ISE.



Настройте Параметры Администрирования устройств на ACS, которые являются, профили оболочки и наборы команд. Для настройки Профилей Shell перейдите к **Элементам Политики> Авторизация и Разрешения> Администрирование устройств> Профили Shell.** Нажмите **Create** и настройте название, Общие задачи и Настраиваемые атрибуты согласно требованию.



Чтобы к conofigure Наборам команд, перейдите к **Элементам Политики> Авторизация и Разрешения> Администрирование устройств> Наборы команд.** Нажмите **Create** и заполните подробные данные согласно требованию.



Настройте Службу доступа, Выбранную в Сервисном Правиле выбора согласно требованию. Для настройки Правил Службы доступа перейдите к **Политике доступа> Службы доступа> Администратор устройства по умолчанию> Идентичность**, где идентификационное хранилище, которое должно использоваться, может быть выбрано для аутентификации. Правила авторизации могут быть настроены путем навигации к **Политике доступа> Службы доступа> Администратор устройства по умолчанию> Авторизация.**

> **Примечание:** Конфигурация политики авторизации и оболочки profles для определенных устройств может варьироваться, и это вне области этого документа.

Проверка

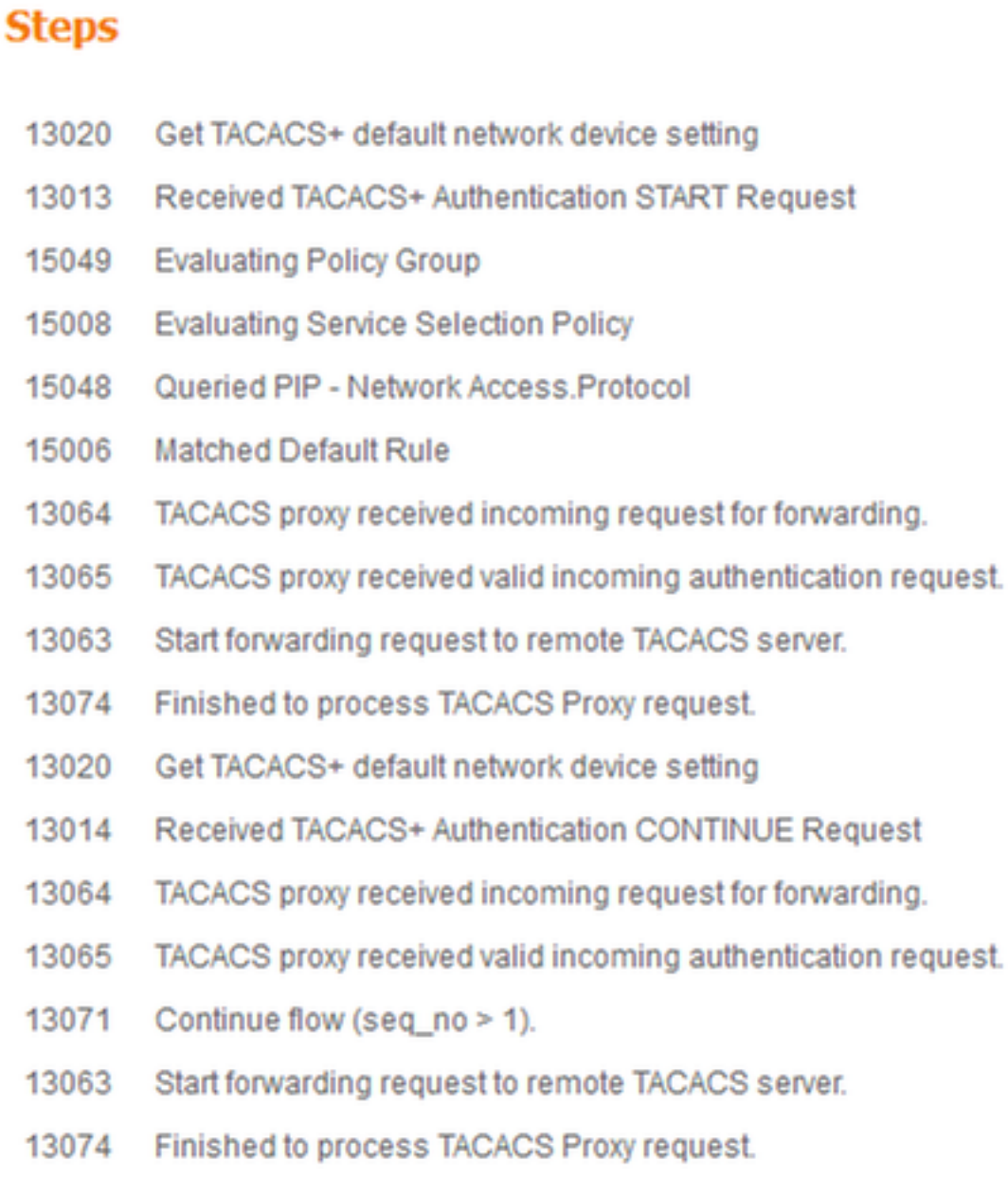
Используйте этот раздел, чтобы подтвердить, что конфигурация работает должным образом.

Проверка может быть сделана и на ISE и на ACS. Любая ошибка в конфигурации ISE или ACS приведет к ошибке проверки подлинности. ACS является основным сервером, который

обработает аутентификацию и запросы авторизации, ISE несет ответственность к и от сервера ACS и действия как прокси для запросов. Начиная с пакетных пересечений через обоих серверы, проверка аутентификации или запроса авторизации могут быть сделаны на обоих серверы.

Сетевые устройства настроены с ISE как Сервер tacacs а не ACS. Следовательно запрос достигает ISE, первого и основанного на настроенных правилах, ISE решает, должен ли запрос быть передан к внешнему серверу. Это может быть проверено в TACACS Оперативный вход в систему ISE.

Для просмотра оперативного входа в систему ISE перейдите к **Операциям> TACACS> Оперативные Журналы.** Репортажи с места события могут быть замечены на этой странице, и подробные данные определенного запроса могут быть проверены путем нажатия значка лупы, имеющего отношение к тому конкретному запросу, который представляет интерес.



Для просматривания опознавательных отчетов на ACS перейдите к **Отслеживанию и**

сообщению> Средство просмотра Отслеживающего и сообщающего Запуска> Отслеживающий и сообщающий> Отчёты> Протокол AAA (проверка подлинности, авторизация и учет)> Аутентификация TACACS. Как ISE, подробные данные определенного запроса могут быть проверены путем нажатия значка лупы, имеющего отношение к тому конкретному запросу, который представляет интерес

Устранение неполадок

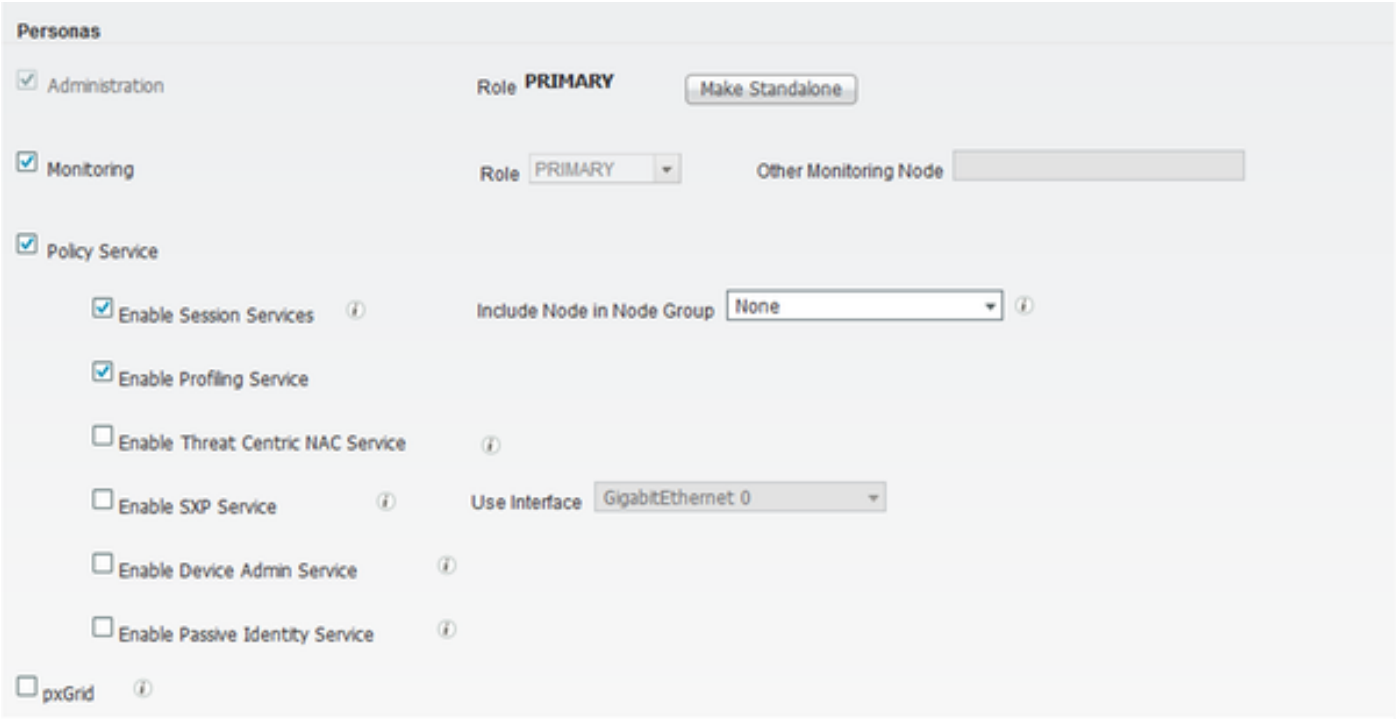
В этом разделе описывается процесс устранения неполадок конфигурации

1. Если подробные данные отчёта относительно ISE показывают сообщение об ошибках, показанное на рисунке, то это указывает на недопустимый общий секретный ключ, настроенный или на ISE или на Устройстве Netowrk (NAD).

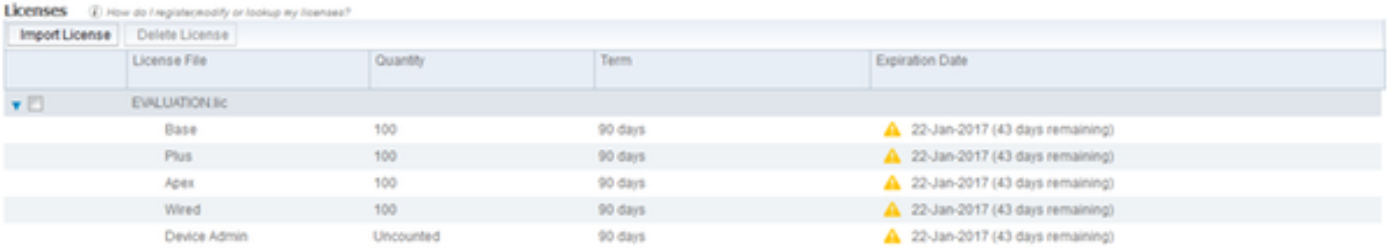
Message Text	TACACS: Invalid TACACS+ request packet - possibly mismatched Shared Secrets

2. Если нет никакого опознавательного отчёта для запроса на ISE, но доступ запрещается конечному пользователю к сетевому устройству, это обычно указывает на несколько вещей.

- Сам запрос сделал никакие не достигают сервера ISE.
- Если персона Администрирования устройств отключена на ISE, то любые TACACS + запрашивают к ISE, будет отброшен тихо. Никакие журналы, указывающие на то же, не покажут в отчётах или Оперативных Журналах. Для проверки этого перейдите к **администрированию> Система>, Развертывания> [выбирают узел].** Нажмите **Edit** и заметьте флажок **"Enable Device Admin Service"** под вкладкой **General Settings** как показано на рисунке. Тот флажок должен быть проверен для Администрирования устройств для работы на ISE.



- Если лицензия Администрирования устройств не присутствует с истекшим сроком, то все TACACS + запросы отброшены тихо. Никакие журналы не показывают в GUI для того же. Перейдите к **администрированию> Система> Лицензирование** для проверки лицензии администрирования устройств.

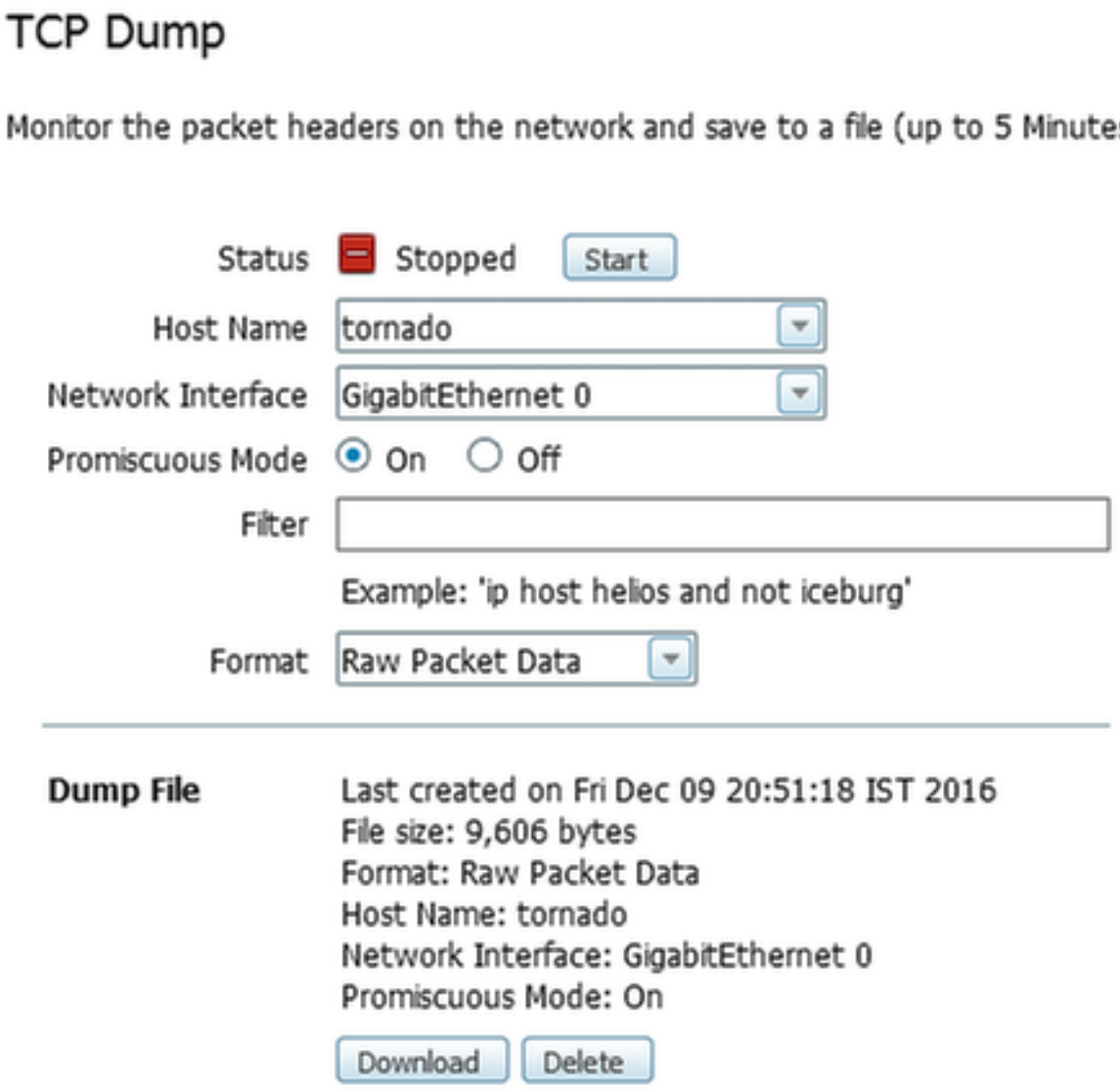


- Если сетевое устройство не будет настроено или если неправильный IP сетевого устройства будет настроен на ISE, то ISE тихо отбросит пакет. Никакой ответ не передают обратно клиенту, и никакие журналы не показывают в GUI. Это - изменение поведения в ISE для TACACS +, когда по сравнению с тем из ACS, который сообщает, что запрос вошел от unkown Сетевого устройства или Клиента AAA.

- Запрос достиг ACS, но ответ не возвратился к ISE. Этот сценарий может быть проверен из отчётов относительно ACS как показано на рисунке. Обычно это - becuase недопустимого общего секретного ключа или на ACS, настроенном для ISE или на ISE, настроенном для ACS.

- Ответ не будет передаваться, даже если ISE не будет настроен, или IP-адрес Интерфейса управления ISE не настроен на ACS в Конфигурации сетевого устройства. В таком secario сообщение на рисунке может наблюдаться относительно ACS.

- Если отчёт об успешной аутентификации замечен на ACS, но никакие отчёты не замечены на ISE, и пользователь отклоняется, то это могла очень хорошо быть проблема в сети. Это может быть проверено захватом пакета на ISE с необходимыми фильтрами. Для сбора захвата пакета на ISE перейдите к **Операциям> Устранение неполадок> Инструменты диагностики> Общие средства> Дамп TCP.**



3. Если отчёты могут быть замечены на ISE, но не на ACS, это могло бы или означать, что запрос не достиг ACS из-за неверной конфигурации Наборов Политики на ISE, который можно устранить неполадки на основе подробного отчета о ISE или из-за сетевой проблемы, которая может быть определена захватом пакета на ACS.

4. Если отчёты замечены и на ISE и на ACS, но пользователю все еще запрещают доступ, то это - чаще проблема в конфигурации Политики доступа на ACS, который можно устранить неполадки основанный на подробном отчете о ACS. Кроме того, ответный трафик с ISE на Устройство Netowork должен быть позволен.