Пример настройки Cisco Secure Services Client с PEAP/GTC WPA

Содержание

Введение

Этот документ описывает, как настроить Защищенный расширяемый протокол аутентификации (PEAP) / Карта с переменым паролем Общего назначения (GTC) Защищенный доступ по протоколу Wi-Fi (WAP) на Cisco Secure Services Client.

Предварительные условия

Используемые компоненты

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

- Версия 4.0 Cisco Secure Services ClientCisco Secure Services Client доступен для скачивания от Центра Программного обеспечения cisco.com (только зарегистрированные клиенты).
- Минимум Windows XP SP2 или 2000 SP 4

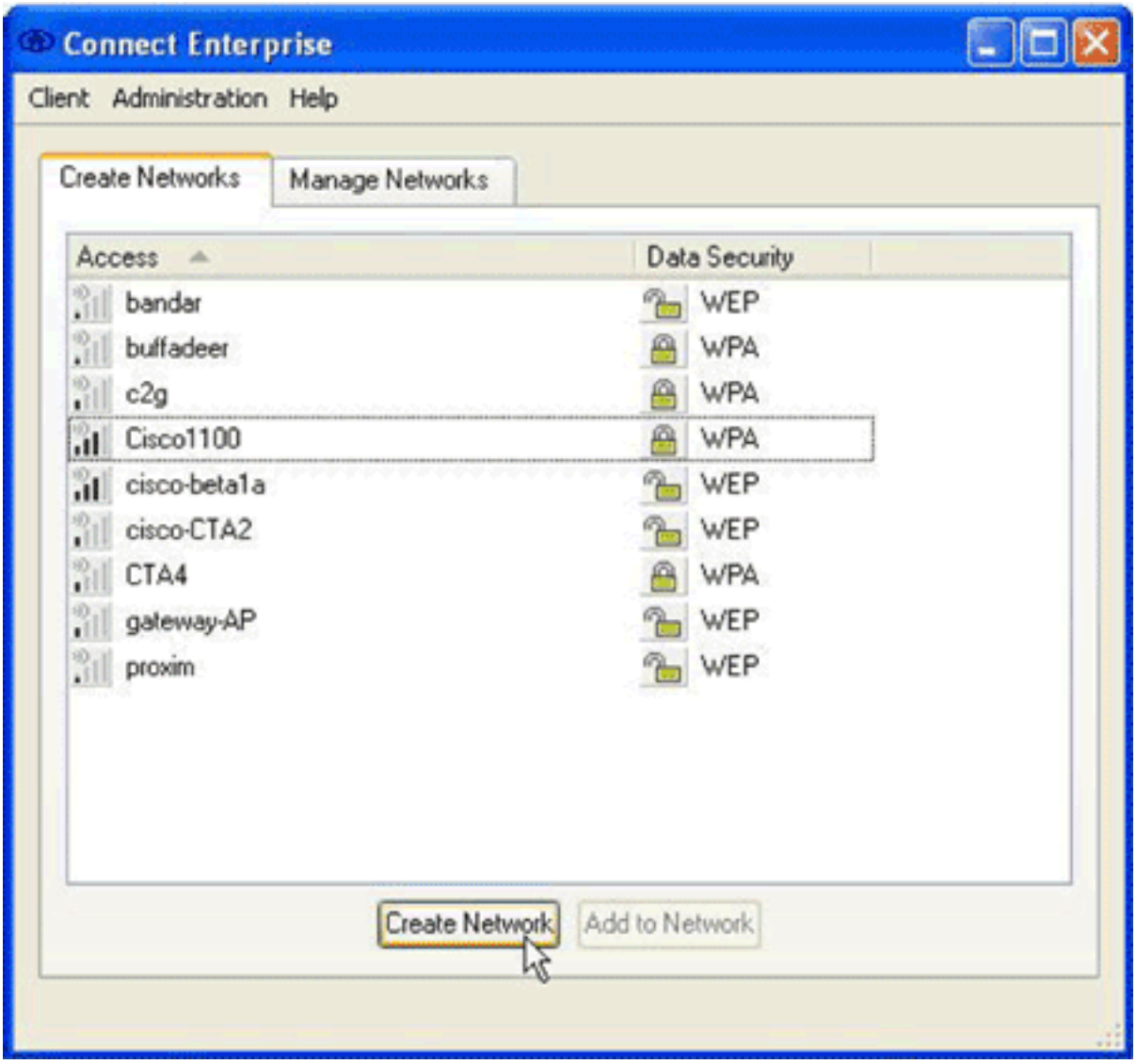
Условные обозначения

Для получения дополнительной информации об условных обозначениях в документации, обратитесь к Cisco Technical Tips Conventions.

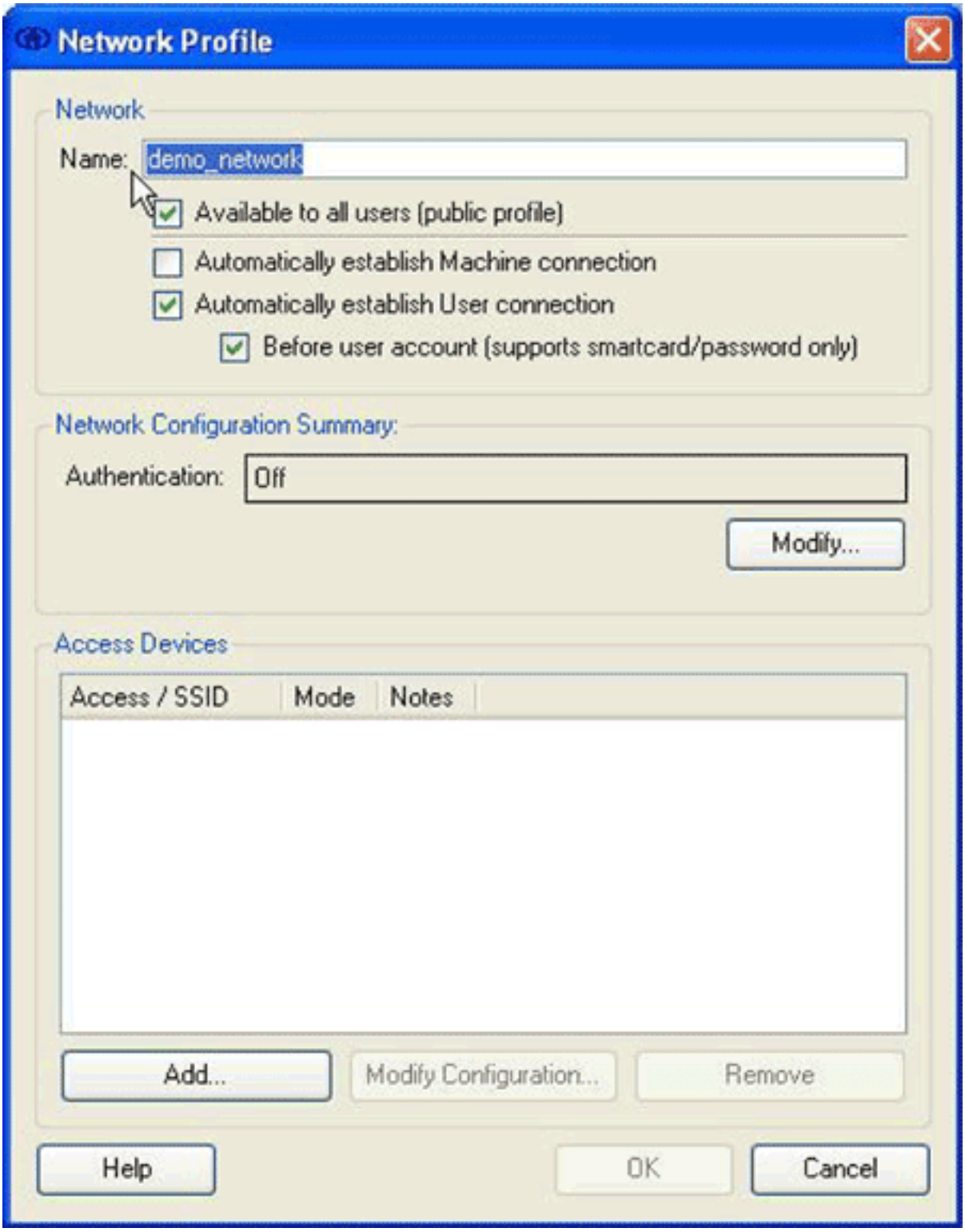
Настройте Cisco Secure Services Client с WPA PEAP / GTC WPA

Для настройки Cisco Secure Services Client с WPA PEAP / GTC WPA выполните эти шаги:

1. Щелкните правой кнопкой мыши значок на системном лотке Cisco Secure Services Client и выберите **Open**.**Примечание:** Если вы не связаны с сетью, ваш значок на системном лотке тускл.Диалоговое окно Connect Enterprise появляется.



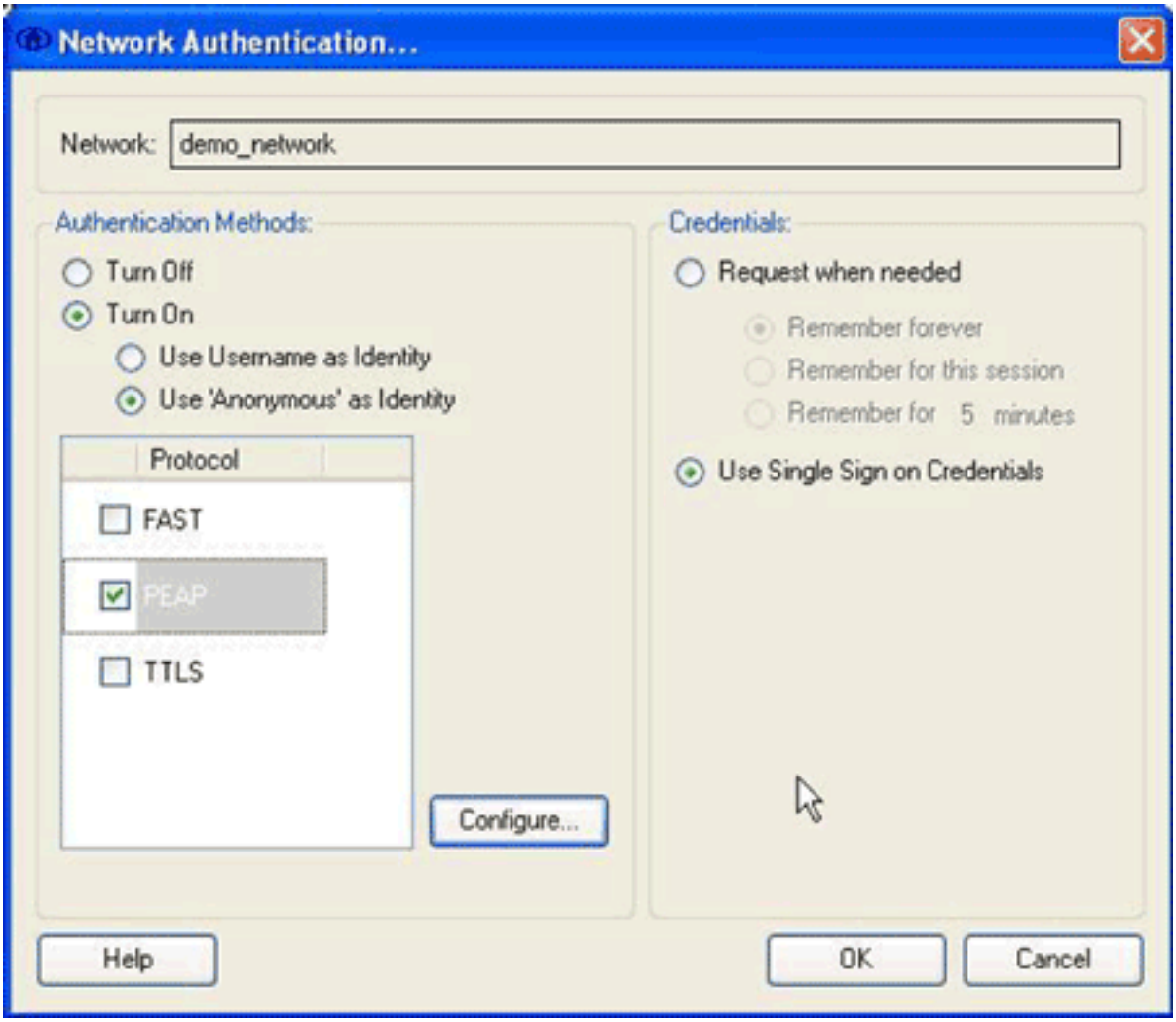
2. Нажмите вкладку **Create Networks**.Область Create Networks отображает сети, которые передавали их идентификатор набора сервисов (SSID).
3. Нажмите кнопку **Create Network**.Диалоговое окно Network Profile появляется.



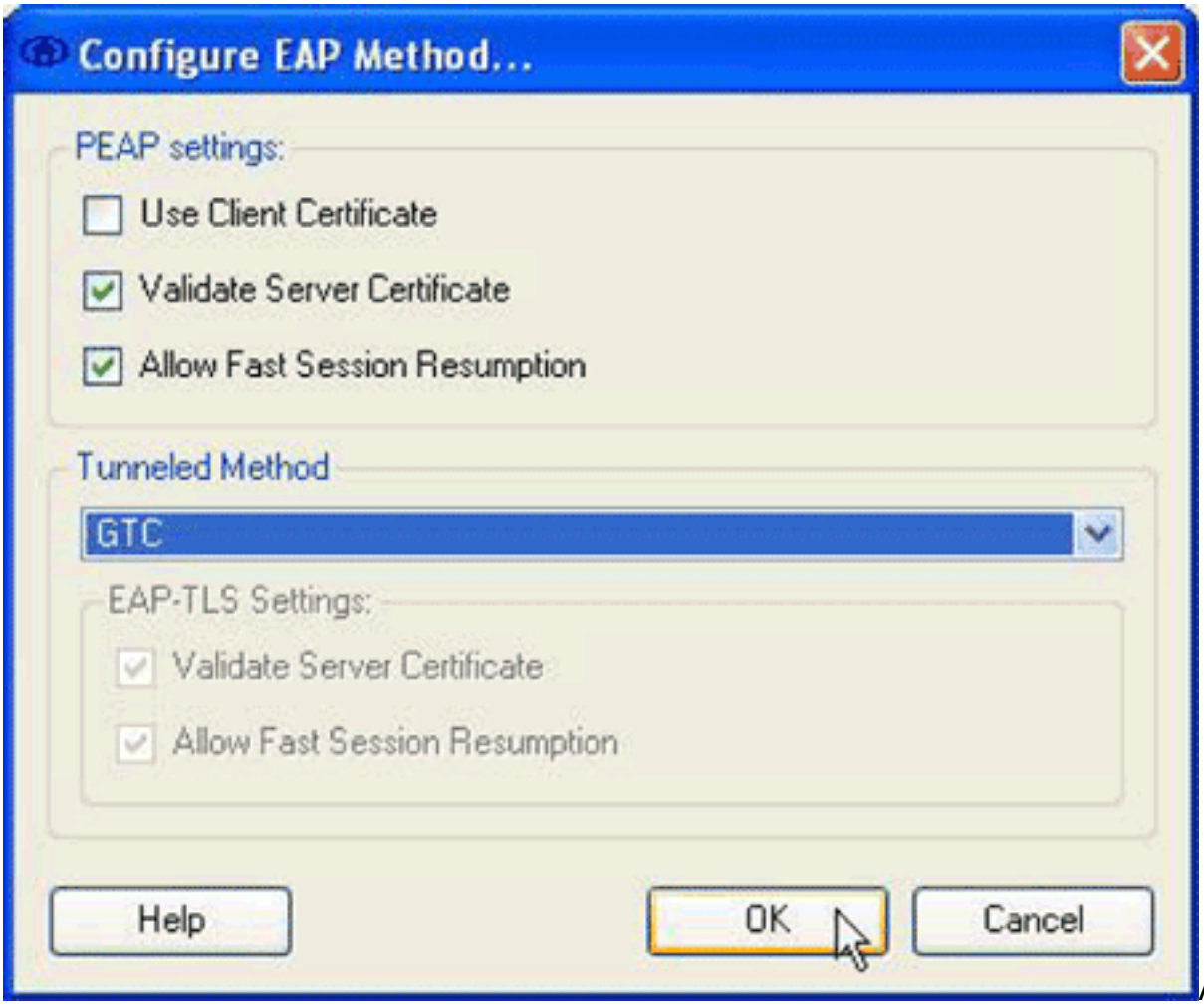
4. В Области сети настройте эти опции:В Поле имени введите имя для своей сети.Это название появляется как SSID для этой сети. Для данного примера название является *demo_network*.Проверьте **Доступное всем пользователям (общий профиль)** флажок.Проверьте**, Автоматически устанавливают** флажок **Подключения пользователя** и проверяют, Автоматически устанавливают флажок соединения Машины, не проверен.Проверьте **Перед учетной записью пользователя (поддерживает только смарт-карту/пароль)**, флажок.**Примечание:** Когда **Перед учетной записью пользователя (поддерживает только смарт-карту/пароль)** флажок проверен, аутентификация сразу продолжается после того, как учетные данные введены, но прежде чем происходит вход в домен. При использовании сертификатов пользователя не проверяйте **Перед учетной записью пользователя (поддерживает только смарт-карту/пароль)**, флажок. Поскольку они не доступны до входа в систему Windows, вы не можете использовать

сертификаты пользователя с входами в домен.

5. В области Network Configuration Summary нажмите кнопку **Modify**.Диалоговое окно Network Authentication
появляется.

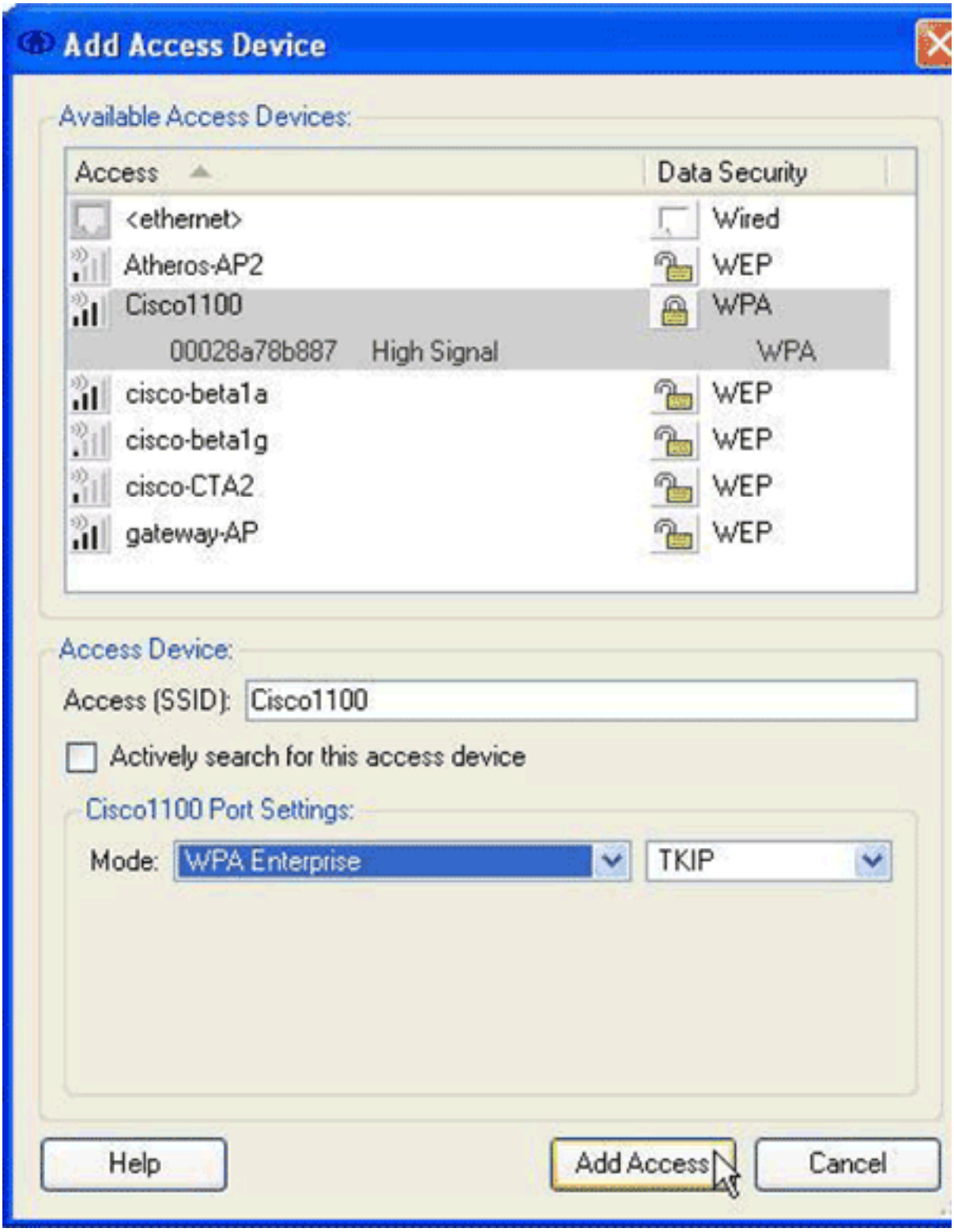


6. В диалоговом окне Network Authentication настройте эти опции:В области Credentials нажмите кнопку с зависимой фиксацией **Credentials Единой точки входа Использования**.В области Authentication Methods нажмите кнопку с зависимой фиксацией **Turn On**, и затем нажмите **Use, 'Анонимный' как Идентичность**.Кнопка с зависимой фиксацией Turn On заполняет список протокола, отображенный в области Authentication Methods. Использование, 'Анонимное' как кнопка с зависимой фиксацией Identity, ограничивает список только туннелируемыми протоколами аутентификации.Проверьте флажок **PEAP**, и затем нажмите **Configure**.Диалоговое окно Configure EAP Method
появляется.



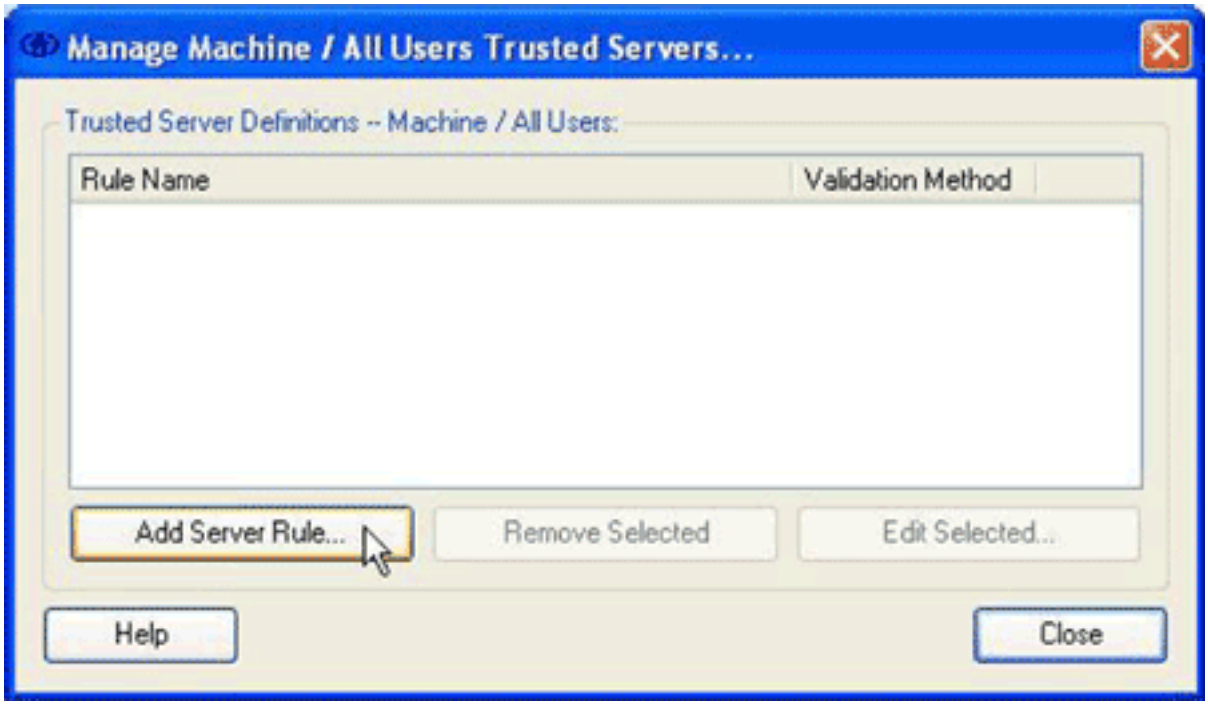
Анчек флажок **Use Client Certificate**.Проверьте флажки **Validate Server Certificate и Allow Fast Session Resumption**.От раскрывающегося меню Метода туннелирования выберите **GTC**.Нажмите **OK**, чтобы возвратиться к диалоговому окну Network Authentication, и затем нажать **OK** для возврата к диалоговому окну Network Profile.

7. В области Access Devices диалогового окна Network Profile **нажмите Add**.Диалоговое окно Add Access Device
появляется.

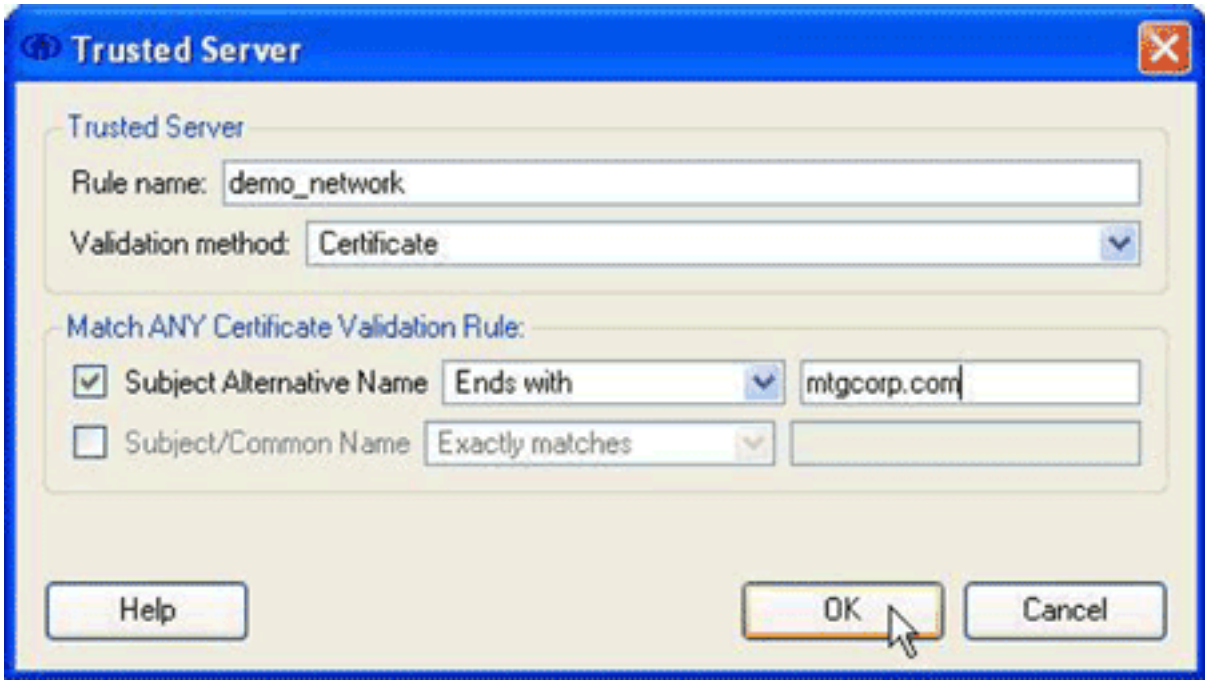


8. В диалоговом окне Add Access Devices выберите устройство, вы хотите настроить, и затем **нажмите Add Доступ.Примечание:** Если устройство, которое вы хотите настроить, в диапазоне, SSID для того устройства должен появиться в Доступном списке Устройств доступа. Если устройство не появляется, введите SSID для устройства в поле Access (SSID), введите параметры порта в область Port Settings Cisco 1100, и затем **нажмите Add Доступ**.
9. В диалоговом окне Network Profile нажмите **OK** для возврата к диалоговому окну Connect Enterprise.
10. В диалоговом окне Connect Enterprise выберите **Trusted Servers> Manage Machine / Все Пользователи доверяли серверам** из Меню клиента.Диалоговое окно Manage Machine / All Users Trusted Servers

появляется.



11. **Нажмите Add правило сервера**.Доверяемое диалоговое окно Server появляется.



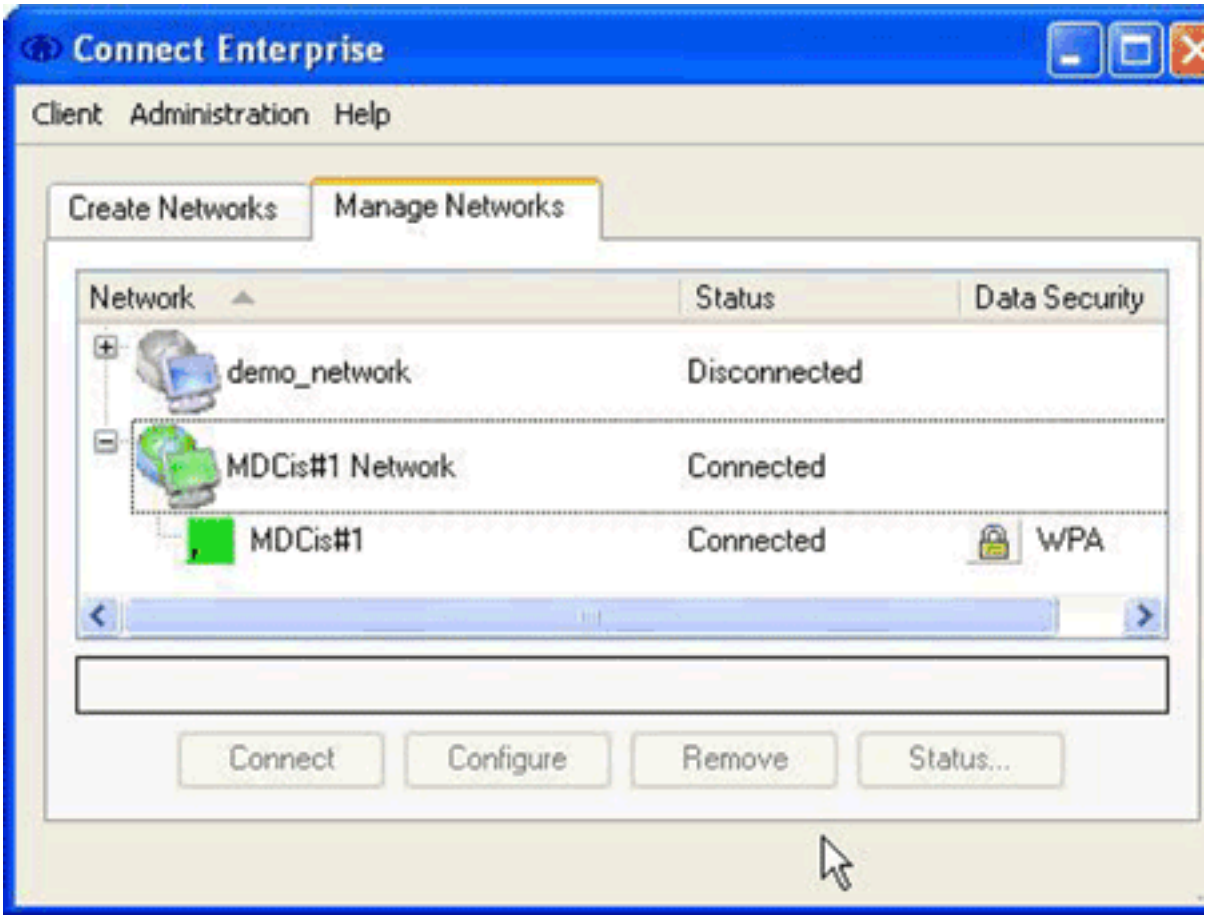
12. В Доверяемом диалоговом окне Server настройте эти опции:В поле Имени правила введите имя для правила.От раскрывающегося меню метода Проверки выберите **Certificate**.В совпадите с любым проверка сертификата управляют областью, опциями configure для правила.Для построения правила необходимо знать содержание серверного сертификата и ввести те значения в область правило проверки сертификата совпадите с любым. Например, если альтернативное имя субъекта содержит доменное имя сервера, *mtgcorpserver.mtgcorp.com*, выберите **Ends c** из раскрывающегося меню Альтернативного имени субъекта, и затем введите **mtgcorp.com** в текстовое поле.Нажмите **OK** для возврата к диалоговому окну Manage Machine / All Users Trusted Servers.
13. В диалоговом окне Manage Machine / All Users Trusted Servers нажмите**, Close to** возвращаются к диалоговому окну Connect Enterprise.

Конфигурация завершена, и можно соединиться с сетью.

Соединитесь с сетью

Для соединения с новой сетью выполните эти шаги:

1. В диалоговом окне Connect Enterprise нажмите вкладку **Manage Networks**.



2. Разъединение от любой сети, которая связана с адаптером, используемым вашей новой сетью.
3. От Списка сети выберите новый сетевой профиль и нажмите **Connect**.

На успешную конфигурацию и соединение, зеленые показы значка на системном лотке Cisco Secure Services Client.

Примечание: Если антивирусное ПО установлено на вашем компьютере, и это настроено для парсинга каталога журнала Cisco Secure Services Client, можно испытать циклы высокой загрузки CPU с аутентификацией Cisco Secure Services Client. Для улучшения производительности настройте антивирусное ПО для исключения каталога журнала Cisco Secure Services Client.

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация