Настройте 802.1x - PEAP с FreeRadius и WLC 8.3

Содержание

Введение

Эти документы объясняют, как установить WLAN (Wireless Local Area Network) с безопасностью 802.1x и PEAP (Защищенный Расширяемый протокол аутентификации) как EAP (Расширяемый протокол аутентификации). FreeRADIUS используется в качестве внешнего сервера Сервиса RADIUS.

Предварительные условия

Cisco рекомендует иметь базовые знания о Linux, Редакторе Vim и Контроллерах беспроводной локальной сети AireOS (WLC).

> **Примечание:** Этот документ предназначен, чтобы дать читателям пример на конфигурации, требуемой на freeRADIUS сервере для аутентификации PEAP-MS-CHAPv2. freeRADIUS конфигурация сервера, представленная в этом документе, была протестирована в лабораторной работе и, как находили, работала как ожидалось. Центр технической поддержки Cisco (TAC) не поддерживает freeRADIUS конфигурацию сервера.

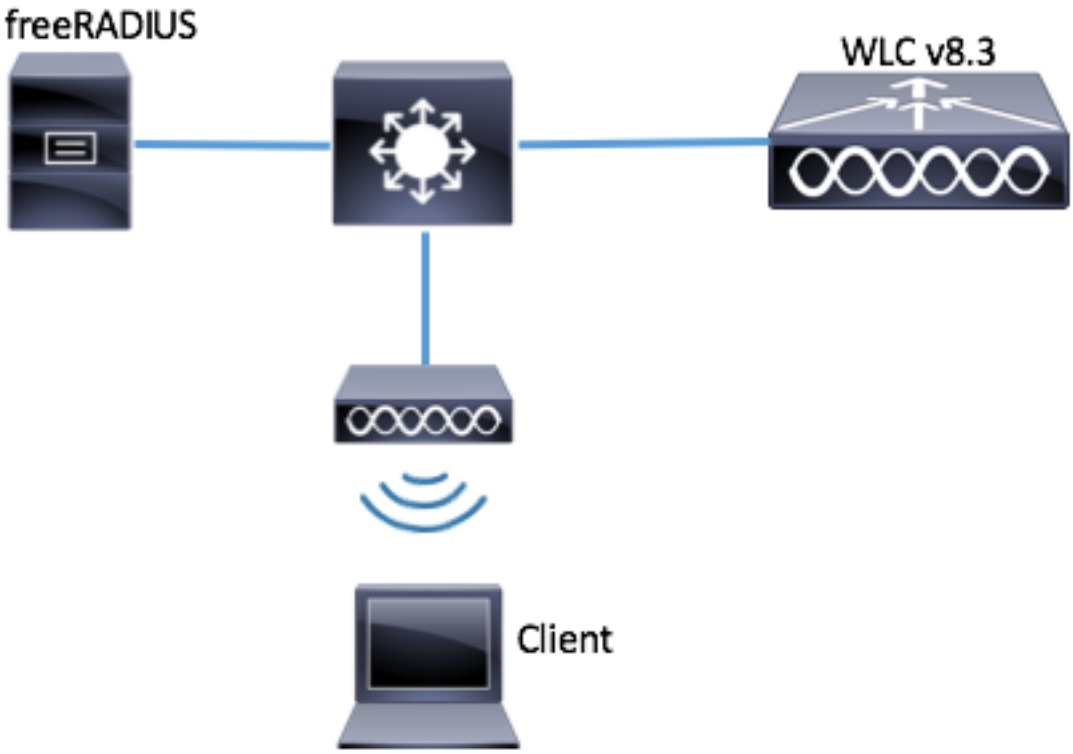
Используемые компоненты

- CentOS7 или Red Hat Enterprise Linux 7 (RHEL7) (Рекомендуемый ОЗУ на 1 ГБ и HDD на по крайней мере 20 ГБ)
- WLC 5508 v8.3
- MariaDB (MySQL)

- FreeRADIUS
- PHP 7

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.

Схема сети



!--- конфигурацию

Установите httpd Сервер и MariaDB

Шаг 1. Выполните эти команды для установки httpd сервера и MariaDB.

```
[root@tac-mxwireless ~]# yum -y update
[root@tac-mxwireless ~]# yum -y groupinstall "Development Tools"
[root@tac-mxwireless ~]# yum -y install httpd httpd-devel mariadb-server mariadb
```

Шаг 2. Запустите и включите httpd сервер MariaDB и (Apache).

```
[root@tac-mxwireless ~]# systemctl enable httpd
[root@tac-mxwireless ~]# systemctl start httpd
[root@tac-mxwireless ~]# systemctl start mariadb
[root@tac-mxwireless ~]# systemctl enable mariadb
```

Шаг 3. Настройте начальные параметры настройки MariaDB для обеспечения его.

```
[root@tac-mxwireless ~]#mysql_secure_installation

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB SERVERS IN PRODUCTION USE!
PLEASE READ EACH STEP CAREFULLY! In order to log into MariaDB to secure it, we'll need the
current password for the root user. If you've just installed MariaDB, and you haven't set the
root password yet, the password will be blank, so you should just press enter here. Enter
```

```
current password for root (enter for none): OK, successfully used password, moving on... Setting the root password ensures that nobody can log into the MariaDB root user without the proper authorisation. Set root password? [Y/n] Y New password: Re-enter new password: Password updated successfully! Reloading privilege tables.. ... Success! By default, a MariaDB installation has an anonymous user, allowing anyone to log into MariaDB without having to have a user account created for them. This is intended only for testing, and to make the installation go a bit smoother. You should remove them before moving into a production environment. Remove anonymous users? [Y/n] y ... Success! Normally, root should only be allowed to connect from 'localhost'. This ensures that someone cannot guess at the root password from the network. Disallow root login remotely? [Y/n] y ... Success! By default, MariaDB comes with a database named 'test' that anyone can access. This is also intended only for testing, and should be removed before moving into a production environment. Remove test database and access to it? [Y/n] y - Dropping test database... ... Success! - Removing privileges on test database... ... Success! Reloading the privilege tables will ensure that all changes made so far will take effect immediately. Reload privilege tables now? [Y/n] y ... Success! Cleaning up... All done! If you've completed all of the above steps, your MariaDB installation should now be secure. Thanks for using MariaDB!
```

Шаг 4. . Настройте Базу данных для freeRADIUS (используйте тот же пароль, настроенный в Шаге 3).

```
[root@tac-mxwireless ~]# mysql -u root -p -e "CREATE DATABASE radius"
[root@tac-mxwireless ~]# mysql -u root -p -e "show databases"
[root@tac-mxwireless ~]# mysql -u root -p
MariaDB [(none)]> GRANT ALL ON radius.* TO radius@localhost IDENTIFIED BY "radiuspassword";
MariaDB [(none)]> FLUSH PRIVILEGES; MariaDB [(none)]> \q
Bye
```

Установите PHP 7 на CentOS 7

Шаг 1. Выполните эти команды для установки PHP 7 на CentOS7.

```
[root@tac-mxwireless ~]# cd ~
[root@tac-mxwireless ~]# curl 'https://setup.ius.io/' -o setup-ius.sh
[root@tac-mxwireless ~]# sudo bash setup-ius.sh
[root@tac-mxwireless ~]# sudo yum remove php-cli mod_php php-common
[root@tac-mxwireless ~]# sudo yum -y install mod_php70u php70u-cli php70u-mysqlnd php70u-devel
php70u-gd php70u-mcrypt php70u-mbstring php70u-xml php70u-pear
[root@tac-mxwireless ~]# sudo apachectl restart
```

Установите FreeRADIUS

Шаг 1. Выполните эту команду для установки FreeRADIUS.

```
[root@tac-mxwireless ~]# yum -y install freeradius freeradius-utils freeradius-mysql freeradius-
sqlite
```

Шаг 2. Сделайте *radius.servicestart* после *mariadb.service.*

Выполните эту команду:

```
[root@tac-mxwireless ~]# vim /etc/systemd/system/multi-user.target.wants/radiusd.service
```

Включите линию **`[Unit]`** раздел:

```
After=mariadb.service
```

[Модуль] раздел должен быть похожим на это:

```
[Unit] Description=FreeRADIUS high performance RADIUS server. After=syslog.target network.target
After=mariadb.service
```

Шаг 3. Запустите и позвольте freeradius запуститься в, загружаются.

```
[root@tac-mxwireless ~]# systemctl start radiusd.service
```

```
[root@tac-mxwireless ~]# systemctl enable radiusd.service
```

Шаг 4. . Включите firewalld для безопасности.

```
[root@tac-mxwireless ~]# systemctl enable firewalld
[root@tac-mxwireless ~]# systemctl start firewalld
[root@tac-mxwireless ~]# systemctl status firewalld
```

Шаг 5. . Добавьте постоянные правила к зоне по умолчанию для разрешения http, https и сервисов RADIUS.

```
[root@tac-mxwireless ~]# firewall-cmd --get-services | egrep 'http|https|radius'
[root@tac-mxwireless ~]# firewall-cmd --add-service={http,https,radius} --permanent success
```

Шаг 6. Повторно загрузите firewalld для изменений для вступления в силу.

```
[root@tac-mxwireless ~]# firewall-cmd --reload
```

Настройте FreeRADIUS

Для настройки FreeRADIUS для использования MariaDB, выполните эти действия.

Шаг 1. Импортируйте схему RADIUSdatabase заполнить Базу данных RADIUS.

```
[root@tac-mxwireless ~]# mysql -u root -p radius < /etc/raddb/mods-
config/sql/main/mysql/schema.sql
```

Шаг 2. Создайте мягкую ссылку для SQL под*/etc/raddb/mods-enabled*

```
[root@tac-mxwireless ~]# ln -s /etc/raddb/mods-available/sql /etc/raddb/mods-enabled/
```

Шаг 3. Настройте модуль SQL*/raddb/mods-available/sql* и измените параметры соединения с базой данных на комплект ваша среда.

```
[root@tac-mxwireless ~]# vim /etc/raddb/mods-available/sql
```

Раздел SQL должен выглядеть подобным ниже.

```
sql {


driver = "rlm_sql_mysql"
dialect = "mysql"

# Connection info:

server = "localhost"

 port = 3306
login = "radius"
password = "radpass" # Database table configuration for everything except Oracle radius_db =
"radius" } # Set to ‘yes’ to read radius clients from the database (‘nas’ table) # Clients will
ONLY be read on server startup. read_clients = yes # Table to keep radius client info
client_table = “nas”
```

Шаг 4. . Право группы изменения на*/etc/raddb/mods-enabled/sql* к radiusd.

```
[root@tac-mxwireless ~]# chgrp -h radiusd /etc/raddb/mods-enabled/sql
```

Настройте WLC как клиента AAA на FreeRADIUS

Шаг 1. Отредактируйте*/etc/raddb/clients.conf* для установки общего ключа для WLC.

```
[root@tac-mxwireless ~]# vim /etc/raddb/clients.conf
```

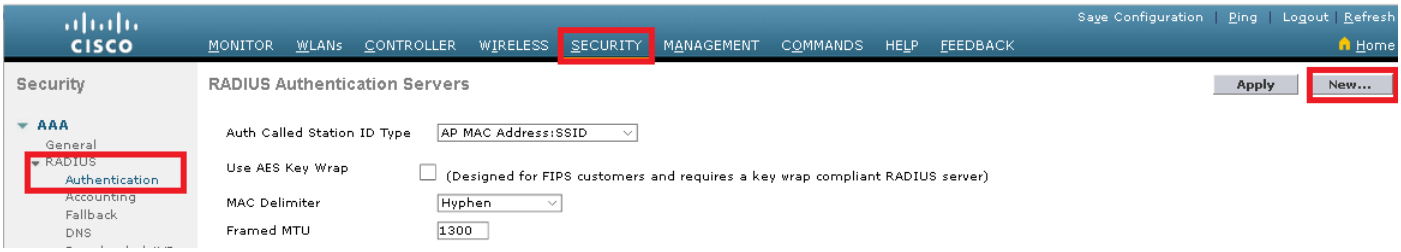
Шаг 2. В нижней части добавляют ваш IP-адрес контроллера и общий ключ.

```
client<WLC-ip-address> { secret = <shared-key> shortname = <WLC-name> }
```

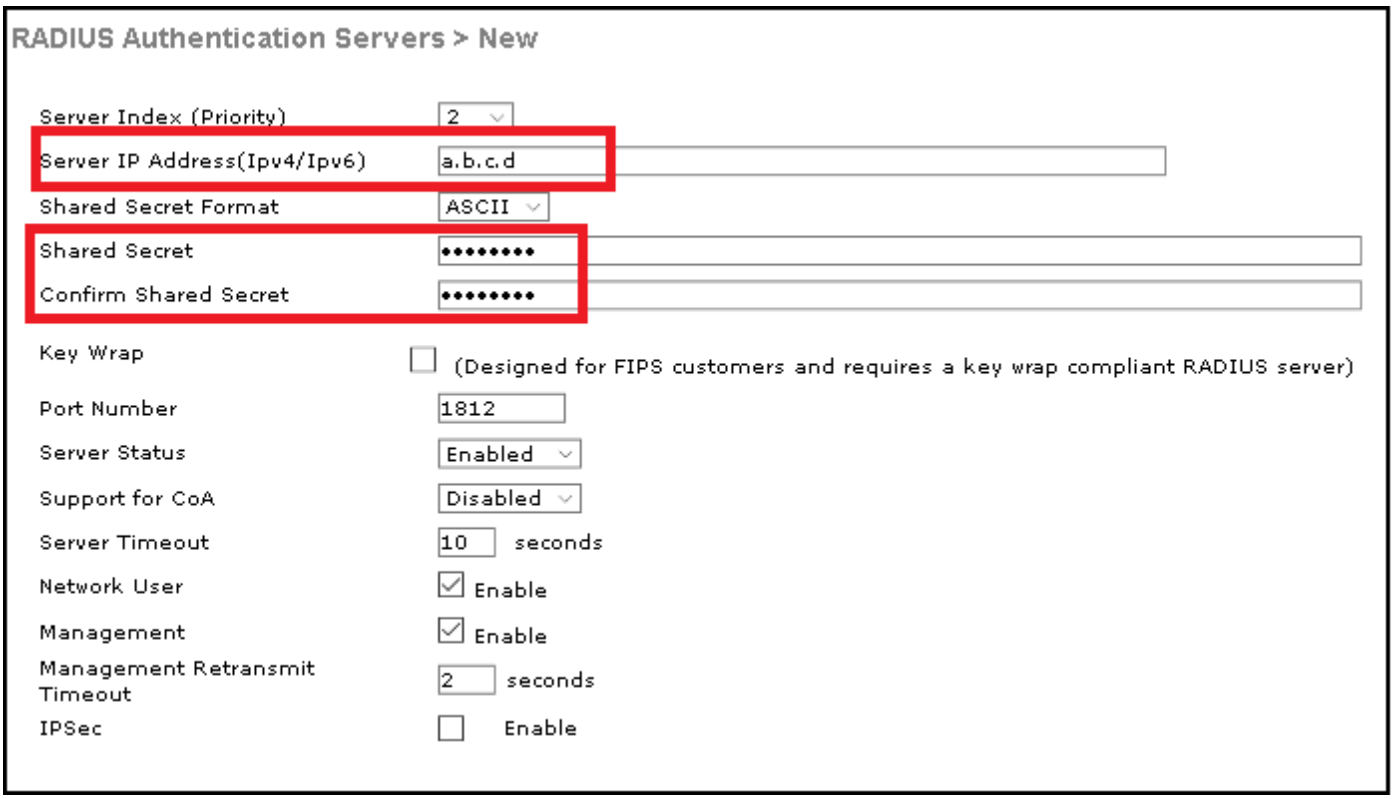
Настройте FreeRADIUS как сервер RADIUS на WLC

GUI:

Шаг 1. Откройте GUI WLC и перейдите к **БЕЗОПАСНОСТИ> RADIUS> Аутентификация> Новый.**



Шаг 2. Заполните информацию о сервере RADIUS.



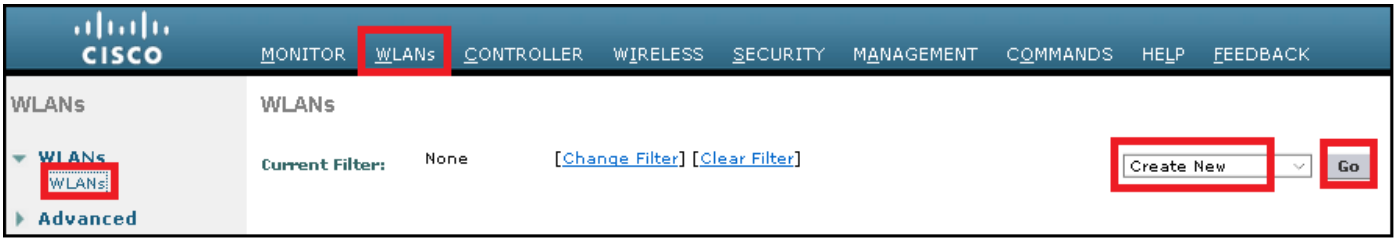
CLI:

```
> config radius auth add <index> <radius-ip-address> 1812 ascii <shared-key>
> config radius auth disable <index>
> config radius auth retransmit-timeout <index> <timeout-seconds>
> config radius auth enable <index>
```

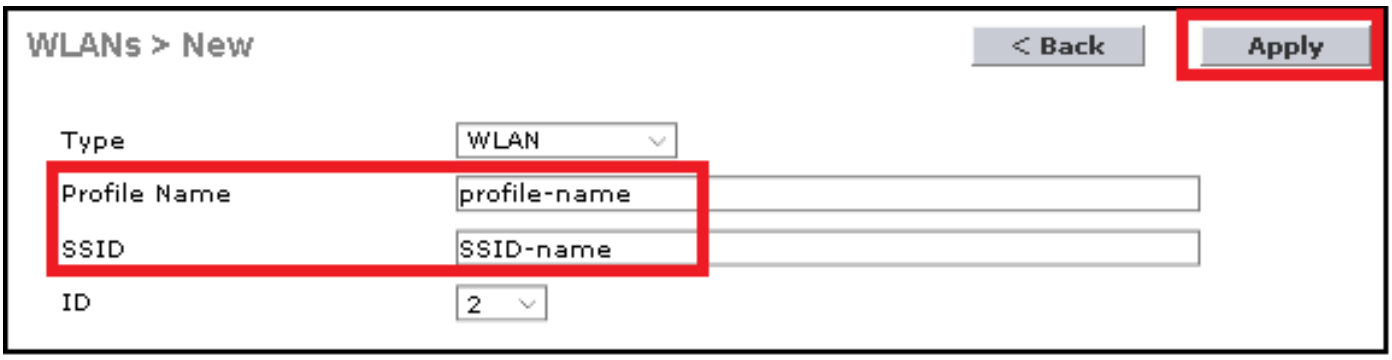
Настройте WLAN

GUI:

Шаг 1. Откройте GUI WLC и перейдите к **WLAN>, Создают Новый>, Идут.**



Шаг 2. Выберите название для SSID и профиля, затем нажмите **Apply.**



CLI:

```
> config wlan create <id> <profile-name> <ssid-name>
```

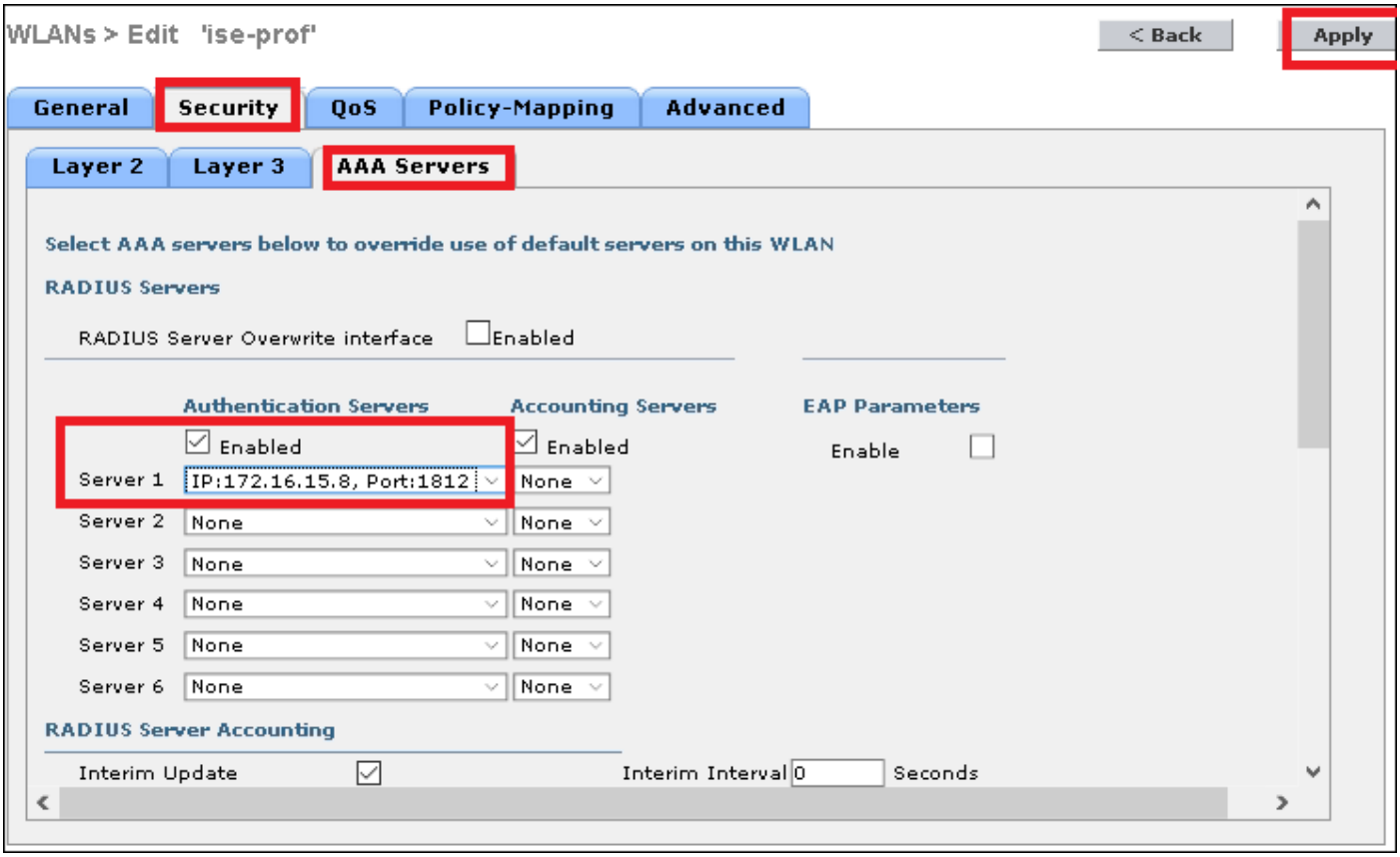
Шаг 3. Назначьте сервер RADIUS на WLAN.

CLI:

```
> config wlan radius_server auth add <wlan-id> <radius-index>
```

GUI:

Перейдите к **Безопасности> AAA-серверы** и выберите желаемый сервер RADIUS, тогда совершите нападки **, Применяются.**

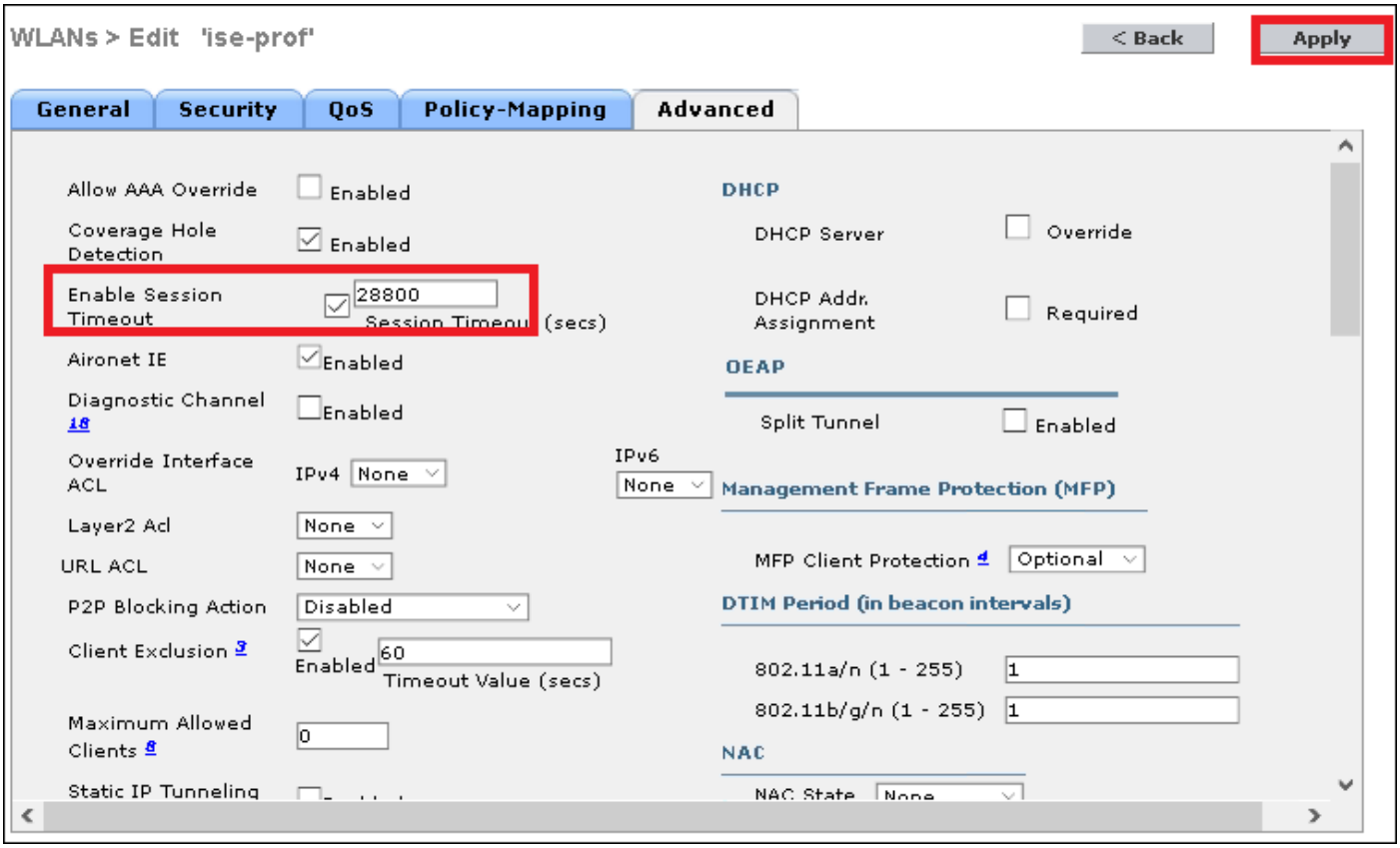


Шаг 4. . Дополнительно увеличьте превышение времени ожидания сеанса

CLI:

```
> config wlan session-timeout <wlan-id> <session-timeout-seconds>
```

GUI:

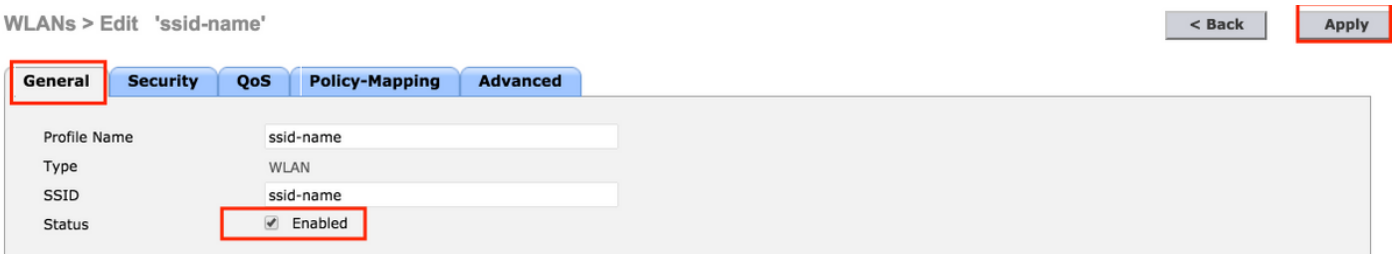


Шаг 5. . Включите WLAN

CLI:

```
> config wlan enable <wlan-id>
```

GUI:



Добавьте пользователей к freeRADIUS базе данных

Протоколами PEAP использования клиентов по умолчанию однако freeRadius поддерживают другие методы (не покрытый этим руководством).

Шаг 1. Отредактируйте файл*/etc/raddb/users*.

```
[root@tac-mxwireless ~]# nano /etc/raddb/users
```

Шаг 2. У основания файла добавляют информацию о пользователях. В данном примере *user1* является именем пользователя и *Cisco123* пароль.

```
user1        Cleartext-Password := "Cisco123"
```

Шаг 3. Перезапуск FreeRadius.

```
[root@tac-mxwireless ~]# systemctl restart radiusd.service
```

Сертификаты на freeRADIUS

FreeRADIUS идет с по умолчанию CA (Сертификация Authoritiy) сертификат и сертификат устройства, которые сохранены в пути */etc/raddb/certs.* Название этих сертификатов является *ca.pem* и *server.pem*. *сервер. pem* является сертификатом, который получат клиенты, в то время как они проходят процесс проверки подлинности. Если необходимо назначить другой сертификат для Аутентификации eap, можно просто удалить их и сохранить новые в том же пути с этим точным то же название.

Конфигурация конечного устройства

Настройте машину Windows портативного ПК для соединения с SSID с Аутентификацией 802.1x и PEAP/MS-CHAP (версия Microsoft Протокола аутентификации по квитированию вызова) версии 2.

Для создания профиля WLAN на машине окон существует две опции:

1. Установите подписанный сертификат на машине, чтобы проверить и доверять freeRADIUS серверу для завершения аутентификации
2. Обойдите проверку сервера RADIUS и положите, что любой сервер RADIUS использовал выполнять аутентификацию (не рекомендуемый, поскольку это может стать проблемой безопасности). Конфигурация для этих опций объяснена на конечной конфигурации устройства - Создают Профиль WLAN - xx Шага.

Конфигурация конечного устройства - Импорт freeRADIUS сертификат

При использовании сертификаты по умолчанию, установленные на freeRADIUS, выполняете эти действия для импорта сертификата EAP из freeRADIUS сервера в конечное устройство.

Шаг 1. Получите свидетельство от FreeRadius:

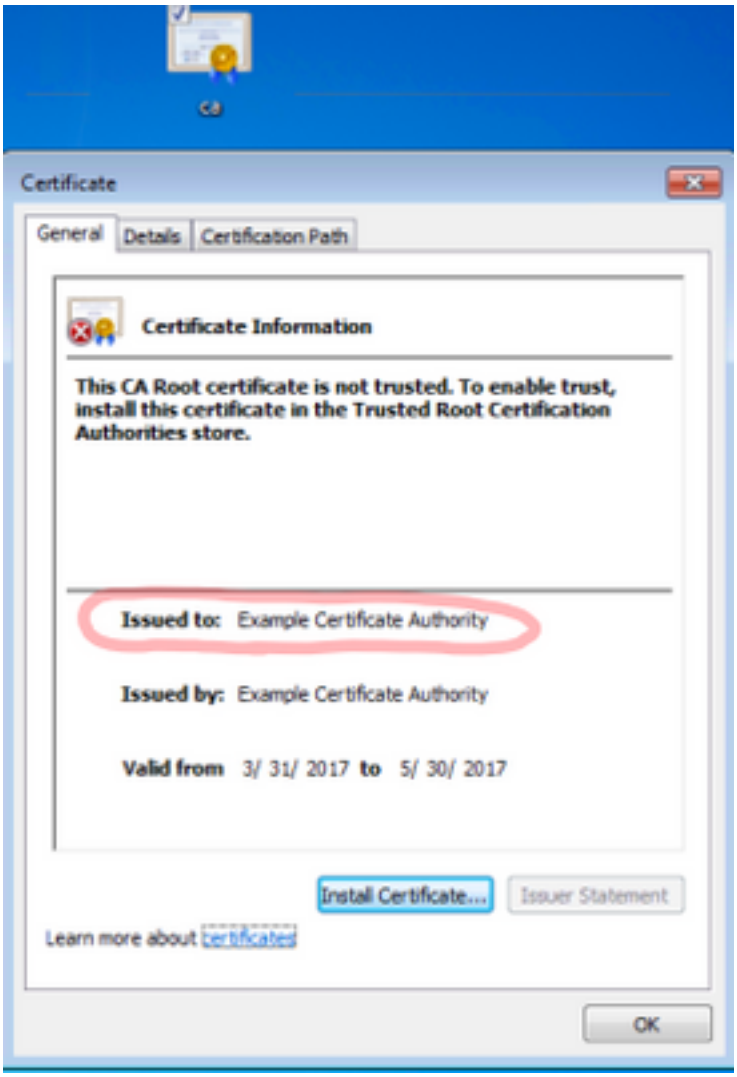
```
[root@tac-mxwireless ~]# cat /etc/raddb/certs/ca.pem

-----BEGIN CERTIFICATE-----
MIIE4TCCA8mgAwIBAgIJAKLmHn4eZLjBMA0GCSqGSIb3DQEBBQUAMIGTMQswCQYD
VQQGEwJGUjEPMA0GA1UECBMGUmFkaXVzMRIwEAYDVQQHEwlTb21ld2hlcmUxFTAT
BgNVBAoTDEV4YW1wbGUgSW5jLjEgMB4GCSqGSIb3DQEJARYRYWRtaW5AZXhhbXBs
ZS5jb20xJjAkBgNVBAMTHUV4YW1wbGUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4X
DTE3MDMzMTExMTIxNloXDTE3MDUzMDExMTIxNlowgZMxCzAJBgNVBAYTAkZSMQ8w
DQYDVQQIEwZSYWRpdXMxEjAQBgNVBAcTCVNvbWV3aGVyZTEVMBMGA1UEChMMRXhh
bXBsZSBJbmMuMSAwHgYJKoZIhvcNAQkBFhFhZG1pbkBleGFtcGxlLmNvbTEmMCQG
A1UEAxMdRXhhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQC0vJ53NN7J9vhpKhcB3B0OXLpeQFWjqolQOB9F
/8Lh2Hax2rzb9wxOi1MOyXR+kN22H7RNwUHET8VdyGUsA4OdZWuyzI8sKi5H42GU
Eu6GDw1YJvhHn4rVC36OZU/Nbaxj0eR8ZG0JGse4ftQKLfckkvCOS5QGn4X1elRS
oFe27HRF+pTDHd+nzbaDvhYWvFoe6iA27Od7AY/sDuo/tiIJWGdm9ocPz3+0IiFC
ay6dtG55YQOHxKaswH7/HJkLsKWhS4YmXLgJXCeeJqooqr+TEwyCDEaFaiX835Jp
gwNNZ7X5US0FcjuuOtpJJ3hfQ8K6uXjEWPOkDE0DAnqp4/n9AgMBAAGjggE0MIIB
MDAdBgNVHQ4EFgQUysFNRZKpAlcFCEgwdOPVGV0waLEwgcgGA1UdIwSBwDCBvYAU
ysFNRZKpAlcFCEgwdOPVGV0waLGhgZmkgZYwgZMxCzAJBgNVBAYTAkZSMQ8wDQYD
VQQIEwZSYWRpdXMxEjAQBgNVBAcTCVNvbWV3aGVyZTEVMBMGA1UEChMMRXhhbXBs
ZSBJbmMuMSAwHgYJKoZIhvcNAQkBFhFhZG1pbkBleGFtcGxlLmNvbTEmMCQGA1UE
AxMdRXhhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHmCCQCi5h5+HmS4wTAMBgNV
HRMEBTADAQH/MDYGA1UdHwQvMC0wK6ApoCeGJWh0dHA6Ly93d3cuZXhhbXBsZS5j
```

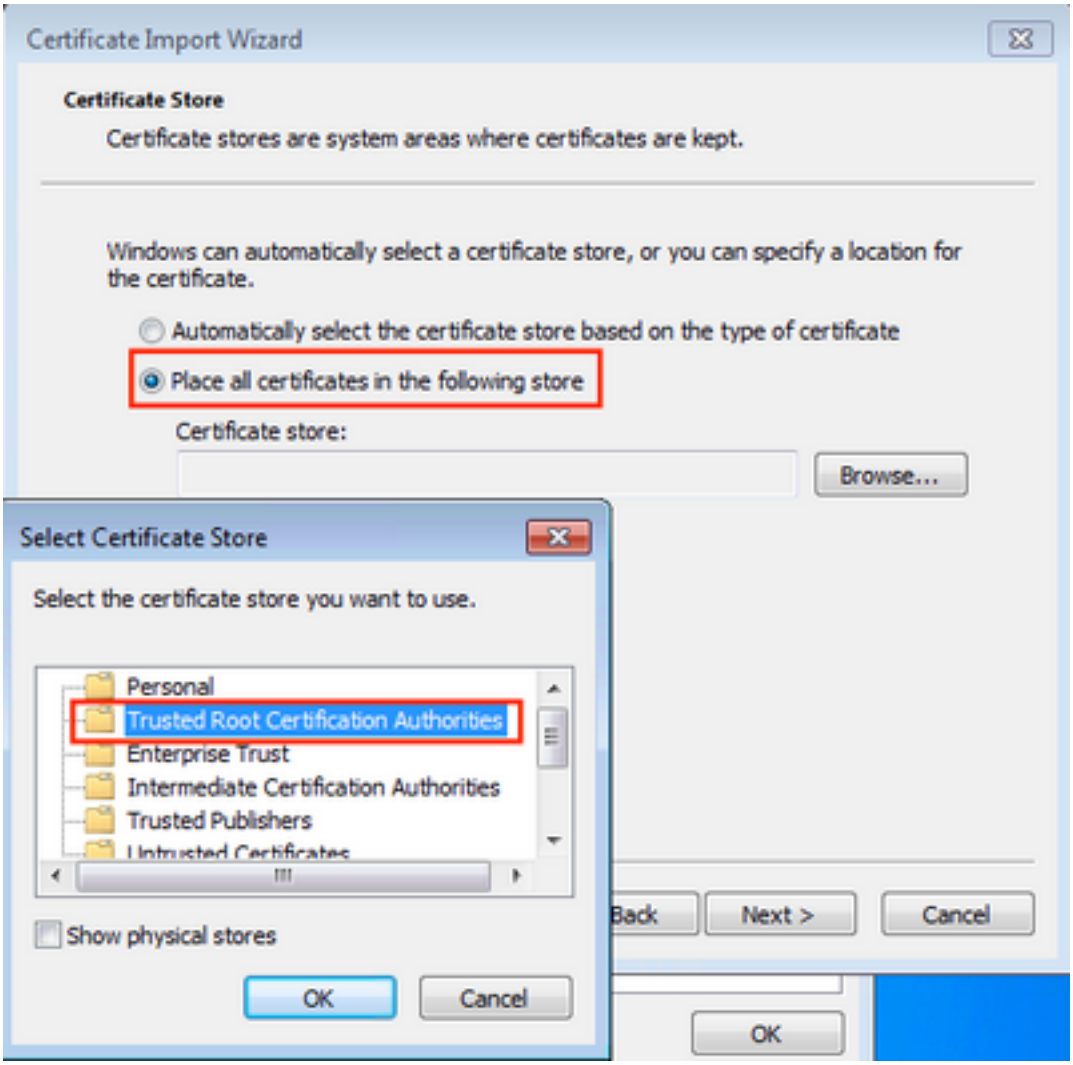
```
b20vZXhhbXBsZV9jYS5jcmwwDQYJKoZIhvcNAQEFBQADggEBACsPR2jiOFXnTsK4
1wnrrMylZZb12gDuqK+zKELox2mzlDMMK83tBsL8yjkv70KeZn821IzfTrTfvhzV
mjX6HgaWfYyMjYYYSw/iEu2JsAtQdpvC3di10nGwVPHlzbozPdov8cZtCb21ynfY
Z6cNjx8+aYQIcsRIyqA1IXMOBwIXo141TOmoODdgfX95lpoLwgktRLkvl7Y7owsz
ChYDO++H7IewsxX5pQfm56dA2cNrlTwWtMvViKyX7GlpwlbBOxgkLiFJ5+GFbfLh
a0HBHZWhTKvffbr62mkbfjCUfJU4T3xgY9zFwiwT+BetCJgAGy8CT/qmnO+NJERO
RUvDhfE=
-----END CERTIFICATE-----
```

Шаг 2. Скопируйте и вставьте выходные данные предыдущего шага в текстовый файл и измените расширение на .crt

Шаг 3. Двойной щелчок файл и выбирает **Install Certificate...**

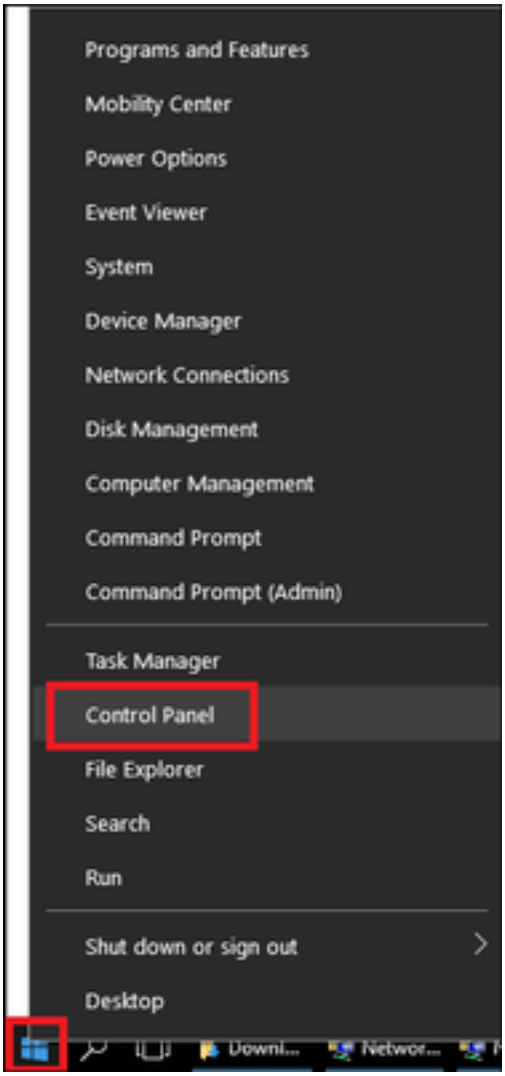


Шаг 4. . Установите сертификат в хранилище **Доверенных корневых центров сертификации**.

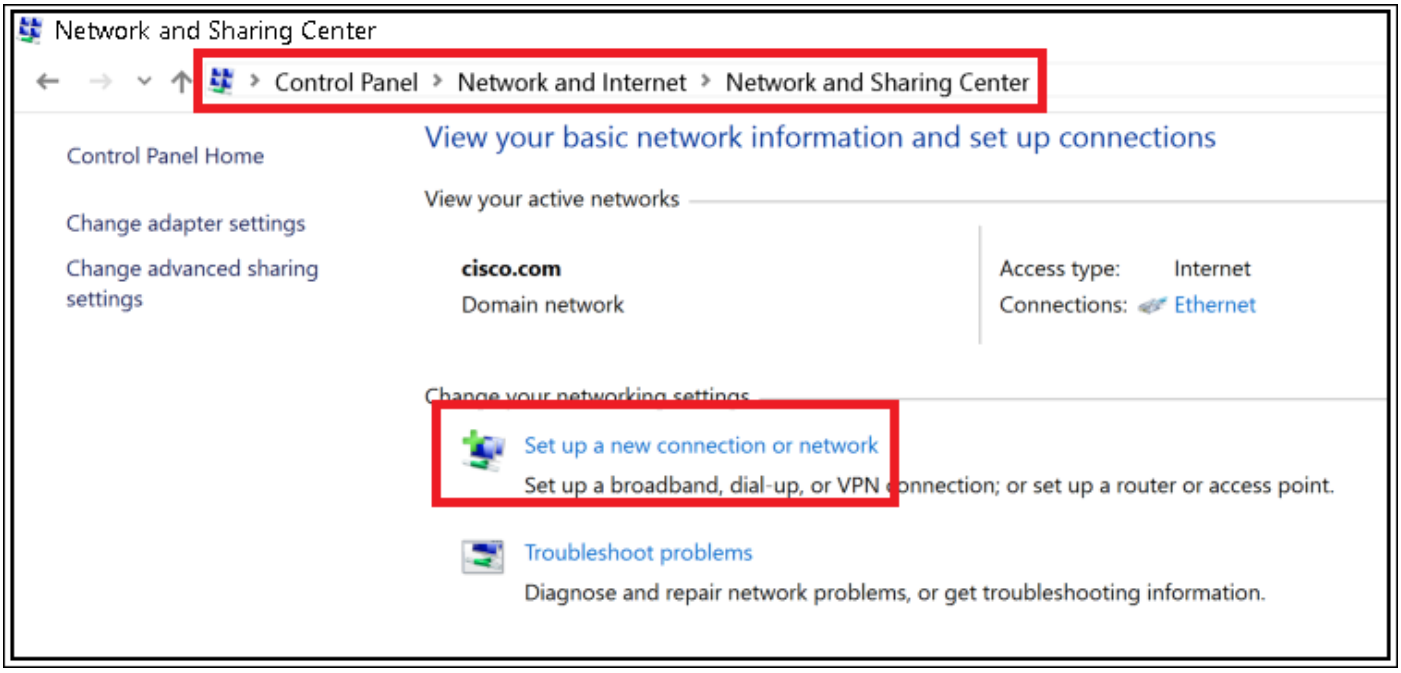


Конфигурация конечного устройства - Создает Профиль WLAN

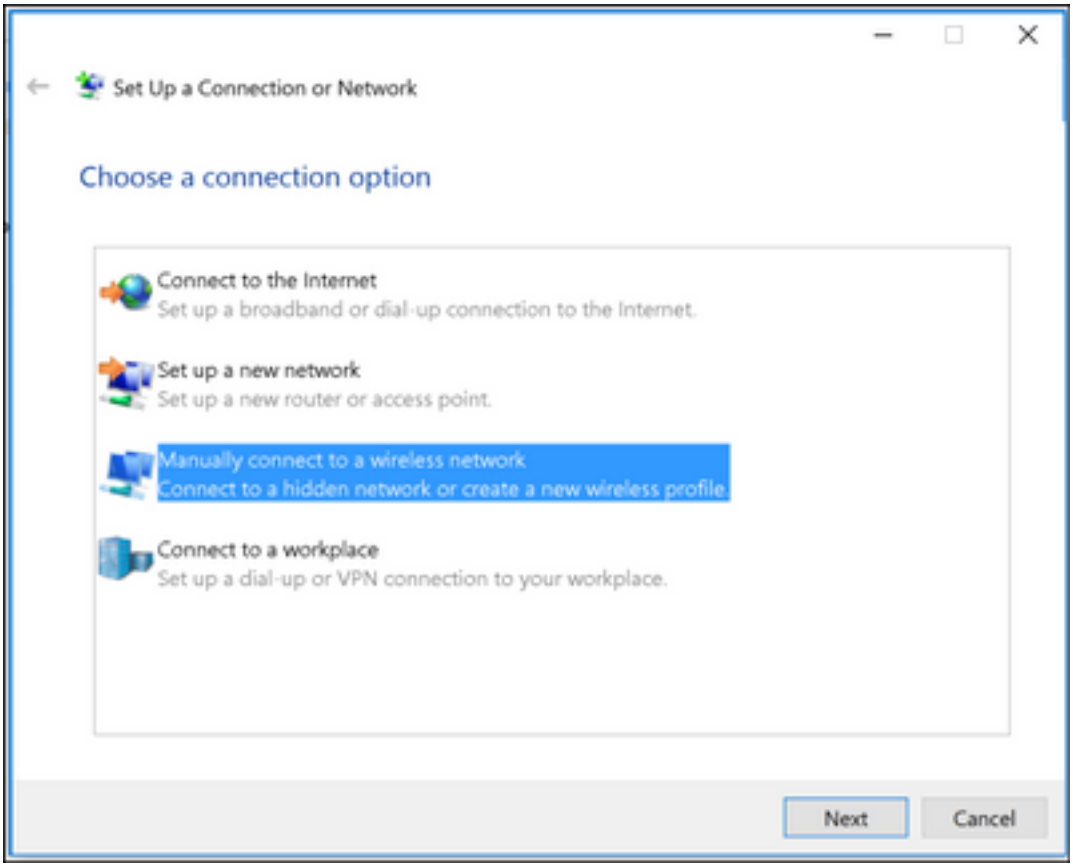
Шаг 1. Щелкните правой кнопкой по значку Start и выберите **Панель управления**.



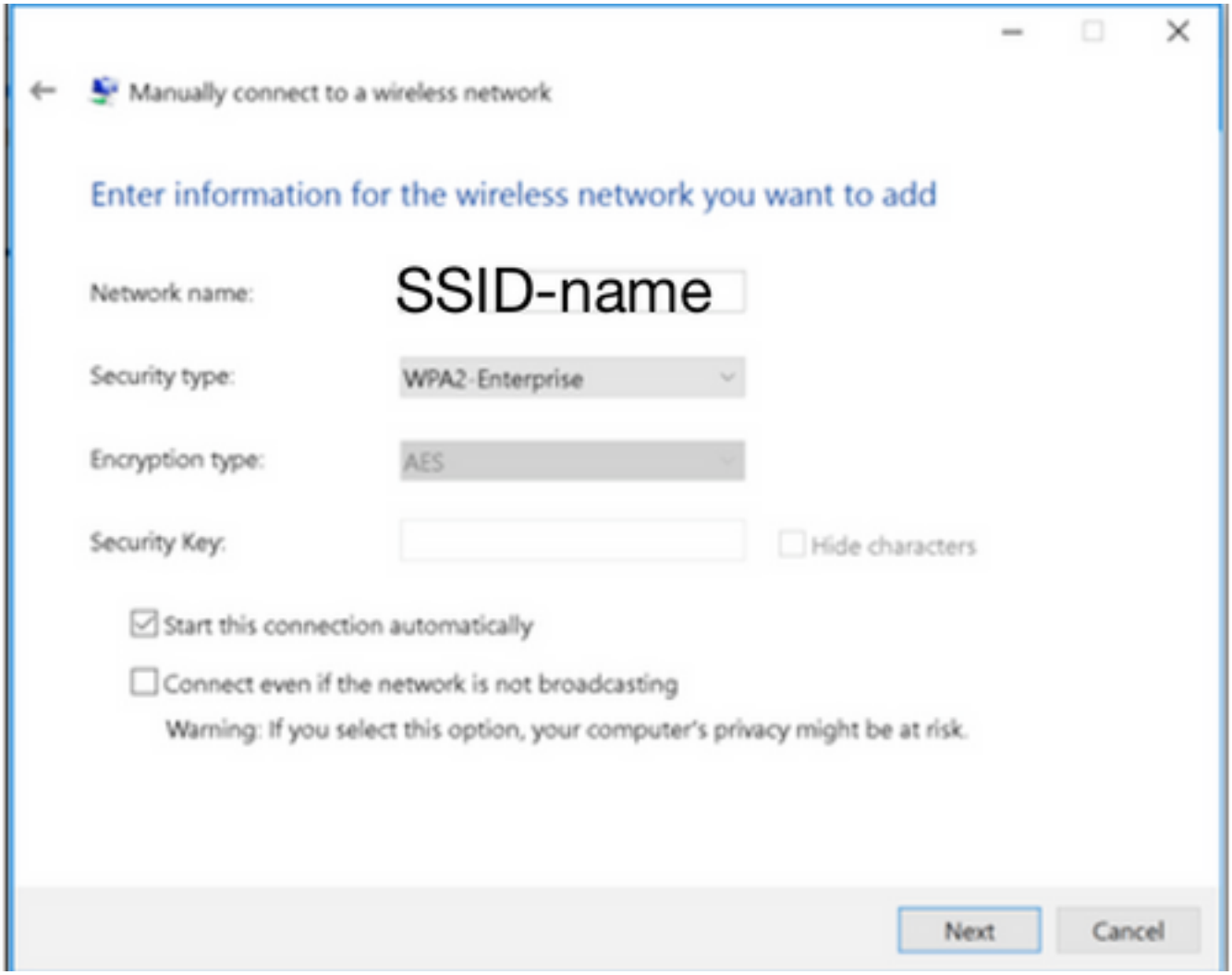
Шаг 2. Перейдите к **Сети и Интернету**, после этого перейдите к **Сети и Совместному использованию Центра** и щелкните **по Set up новое соединение или сеть.**



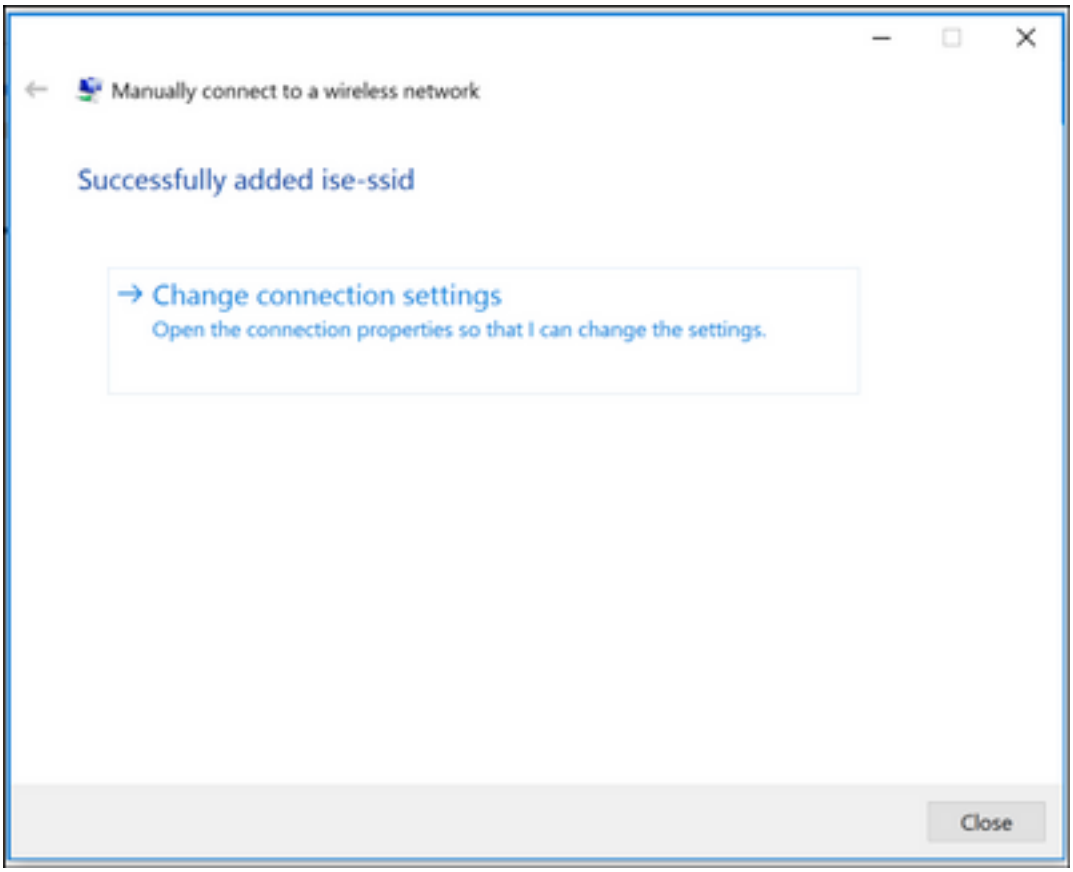
Шаг 3. Выберите **подключение Manually к беспроводной сети** и нажмите **Next.**



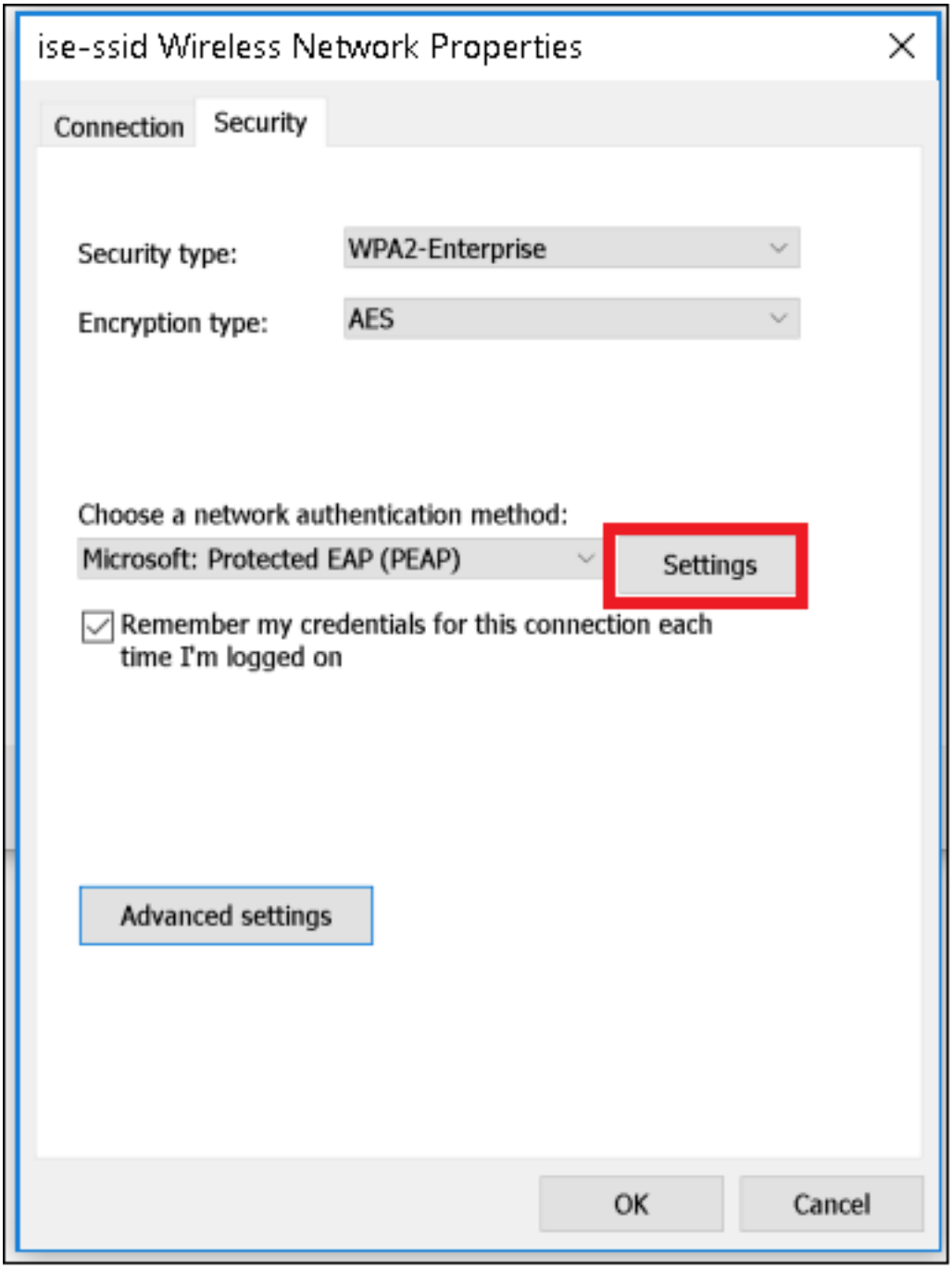
Шаг 4. . Введите информацию с названием SSID и Предприятия WPA2 типа безопасности и нажмите **Next.**



Шаг 5. . Выберите **настройки соединения Change** для настройки конфигурации профиля WLAN.



Шаг 6. Перейдите к **Вкладке Безопасность** и нажмите **Settings.**



Шаг 7. Выберите, если сервер RADIUS проверен или нет.

Если да, включите**, Проверяют идентичность сервера путем проверки сертификата** и от **Доверенных корневых центров сертификации:** список выбирает подписанный сертификат freeRADIUS.

После того, как это выбирает **Configure** и отключает**, Автоматически используют мое имя пользователя Windows и пароль... Затем нажмите кнопку OK**