Аутентификация 802.1x с PEAP, ISE 2.1 и WLC 8.3

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Настройка
Схема сети
Конфигурации
Объявите сервер RADIUS на WLC
Создайте SSID
Объявите WLC на ISE
Создайте нового пользователя на ISE
Создайте Опознавательное правило
Создайте профиль Авторизации
Создайте Правило авторизации
Конфигурация конечного устройства
Проверка
Процесс проверки подлинности на WLC
Процесс проверки подлинности на ISE

Введение

Эти документы объясняют, как установить WLAN (Wireless Local Area Network) с безопасностью 802.1x и VLAN (Виртуальная локальная сеть) замена с PEAP (Защищенный Расширяемый протокол аутентификации) как EAP (Расширяемый протокол аутентификации).

Предварительные условия

Cisco рекомендует иметь базовые знания о:

- 802.1x
- PEAP
- Центр сертификации (CA)
- Сертификаты

Требования

Используемые компоненты

WLC v8.3.102.0

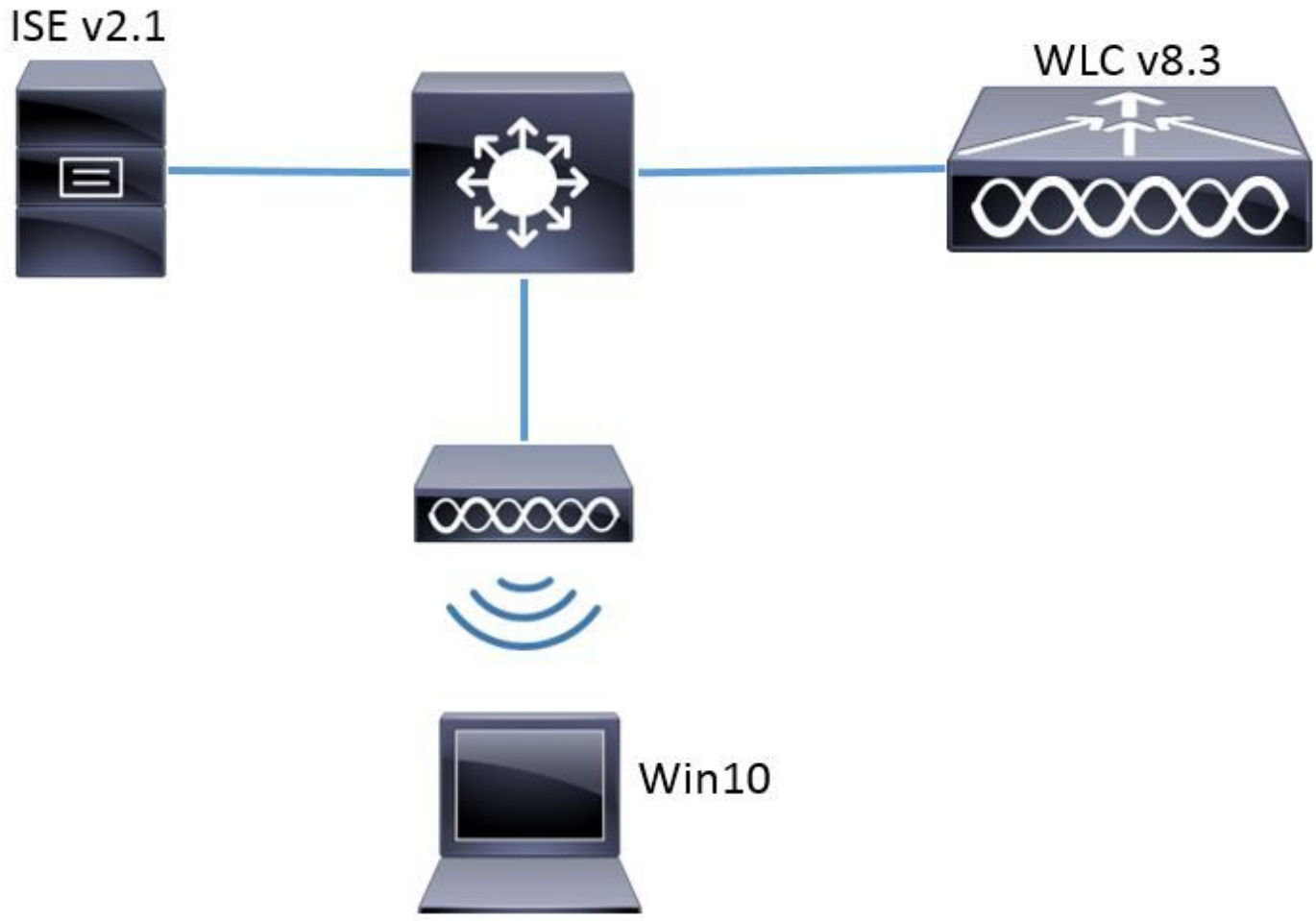
ISE v2.1

Windows 10 Laptop

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.

Настройка

Схема сети



Конфигурации

Общие действия:

1. Объявите сервер RADIUS (ISE в данном примере) на WLC и наоборот позволять связь друг с другом
2. Создайте SSID (идентификатор набора сервисов) в WLC
3. Создайте опознавательное правило о ISE
4. Создайте профиль авторизации на ISE

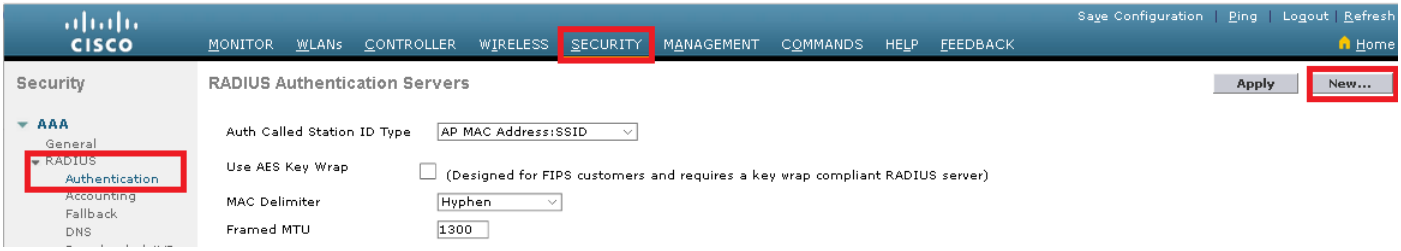
5. Создайте правило авторизации на ISE
6. Настройте оконечную точку

Объявите сервер RADIUS на WLC

Для разрешения связи между сервером RADIUS и WLC, необходимо зарегистрировать сервер RADIUS на WLC и наоборот.

GUI:

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



Шаг 2. Заполните информацию о сервере RADIUS.

CLI:

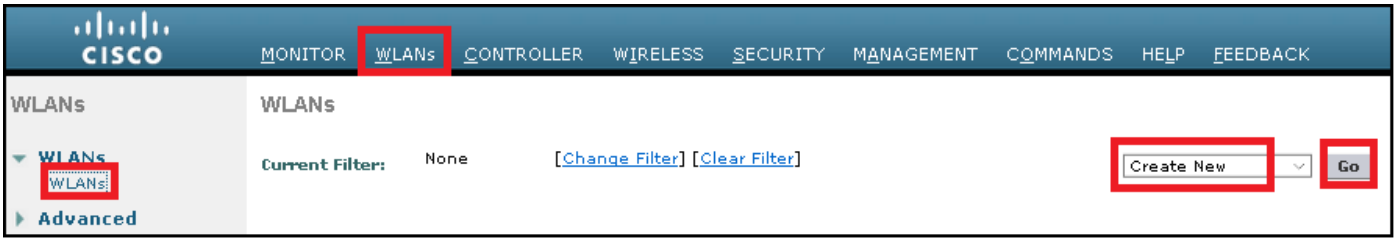
```
> config radius auth add <index> <a.b.c.d> 1812 ascii <shared-key>> config radius auth disable
<index>> config radius auth retransmit-timeout <index> <timeout-seconds>> config radius auth
enable <index>
```

<a.b. c . d> соответствует серверу RADIUS.

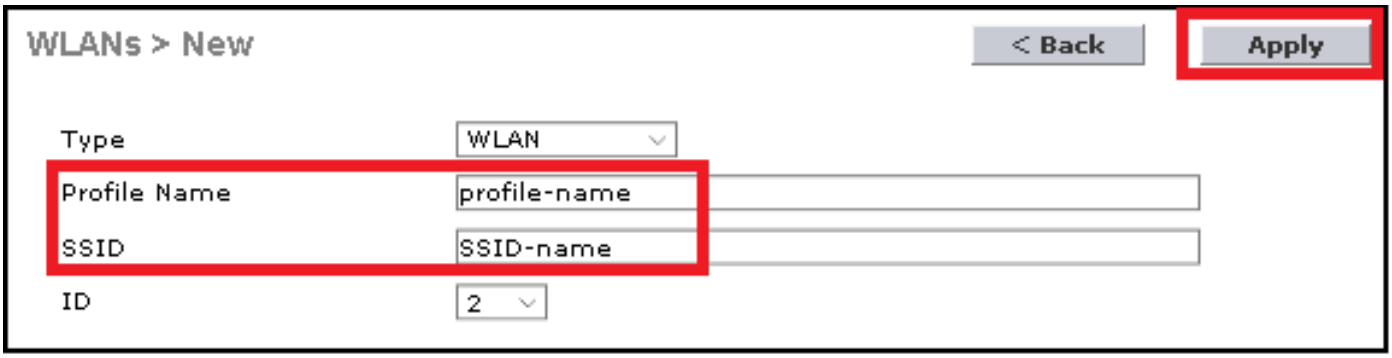
Создайте SSID

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>
```

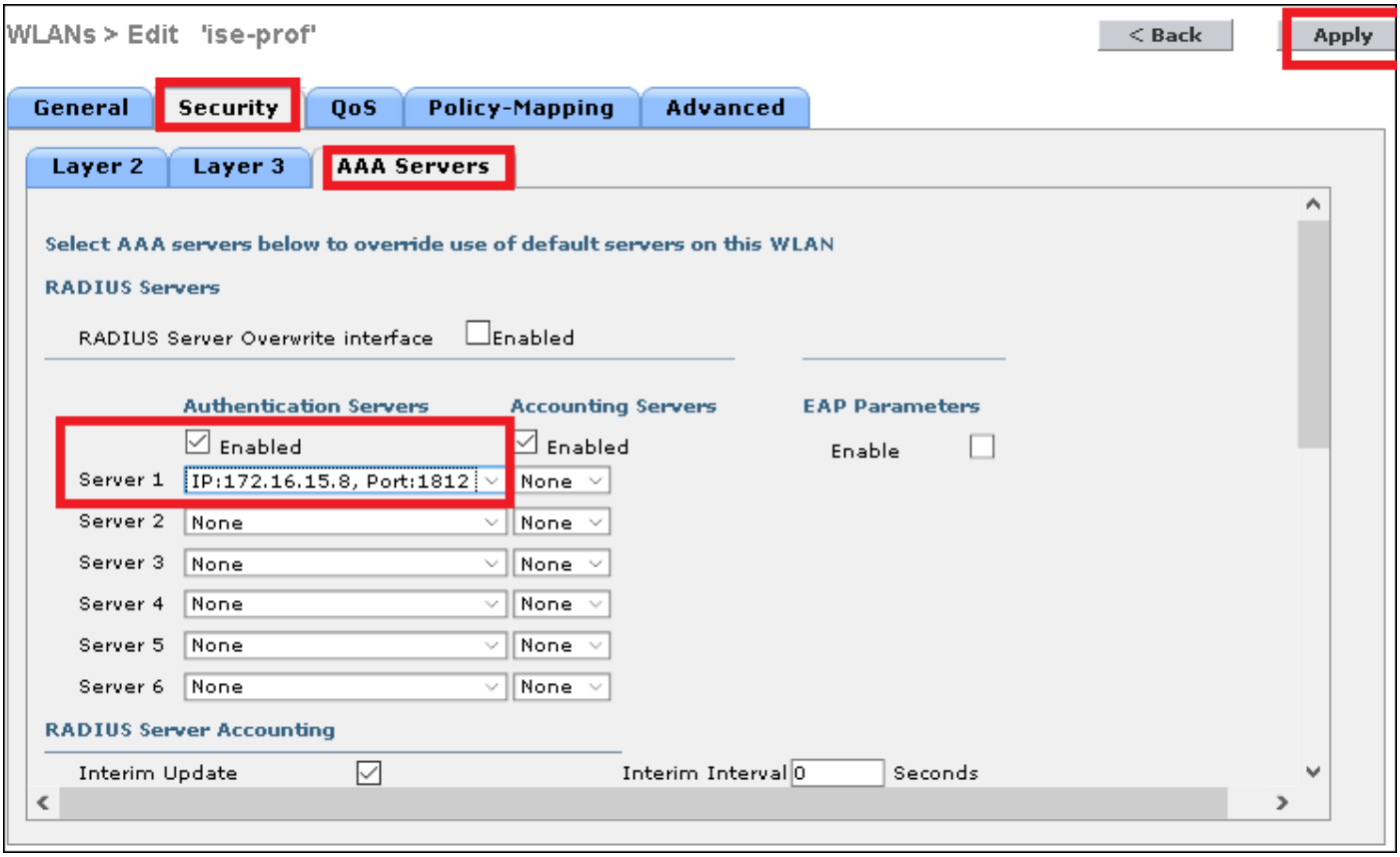
Шаг 3. Назначьте сервер RADIUS на WLAN.

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.**

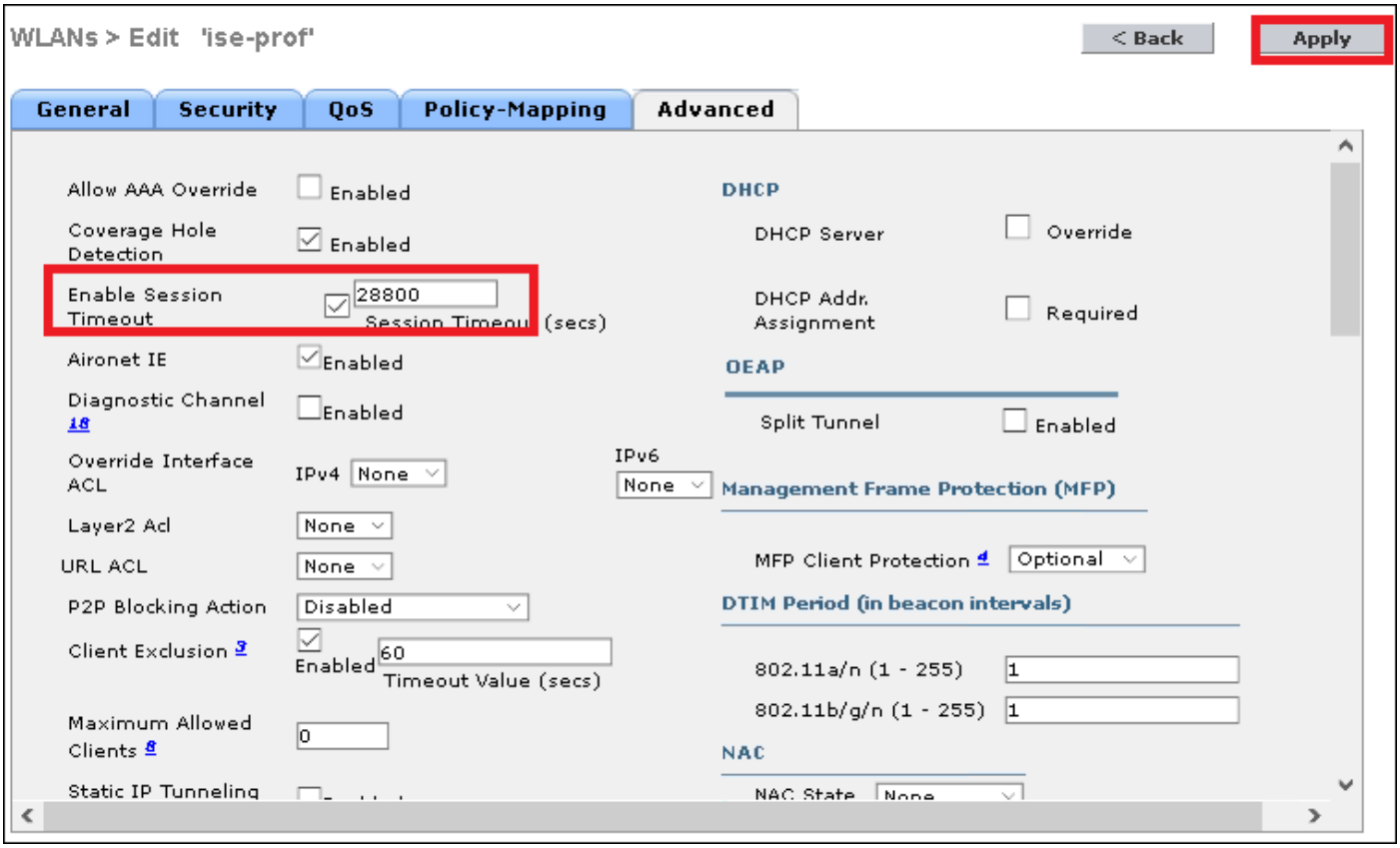


Шаг 4. . Дополнительно увеличьте превышение времени ожидания сеанса

CLI:

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

GUI:

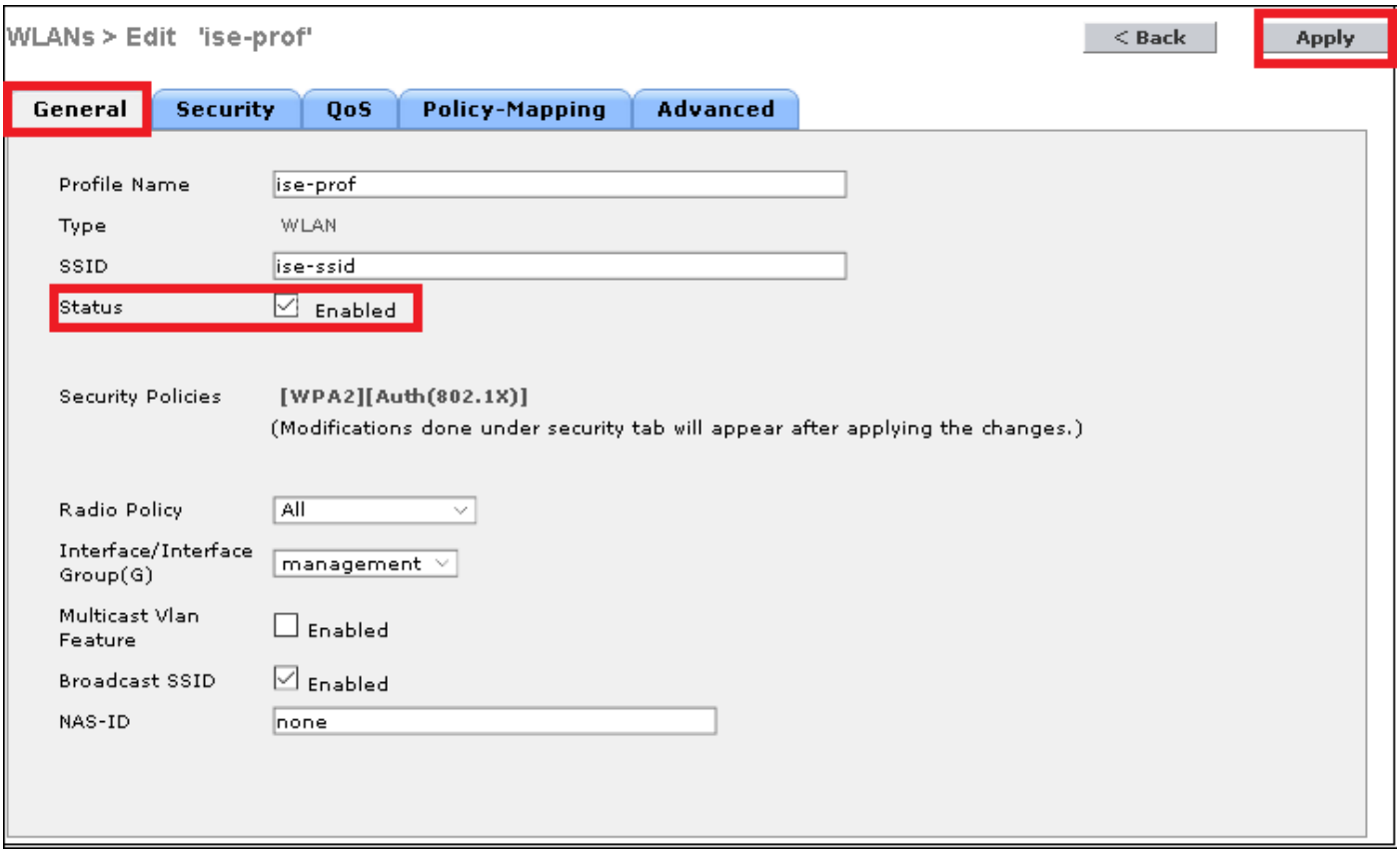


Шаг 5. . Включите WLAN

CLI:

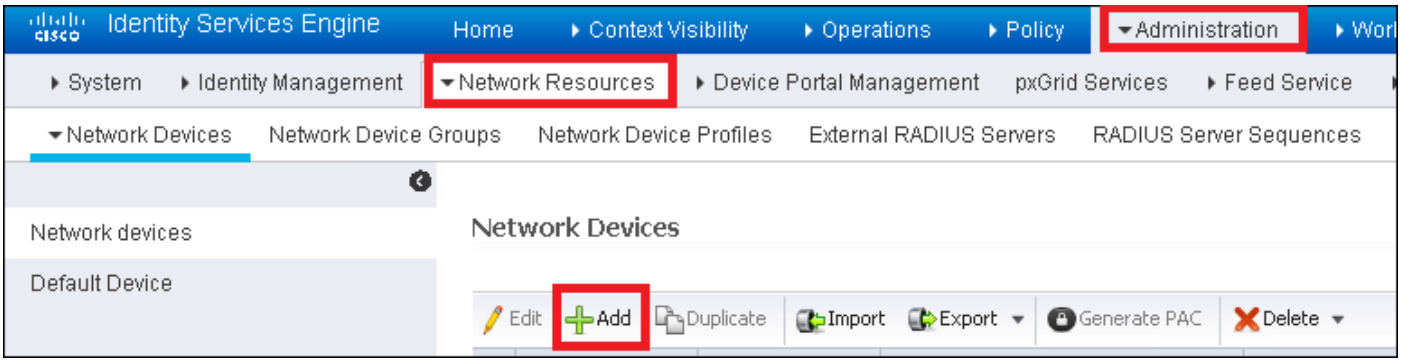
```
> config wlan enable <wlan-id>
```

GUI:



Объявите WLC на ISE

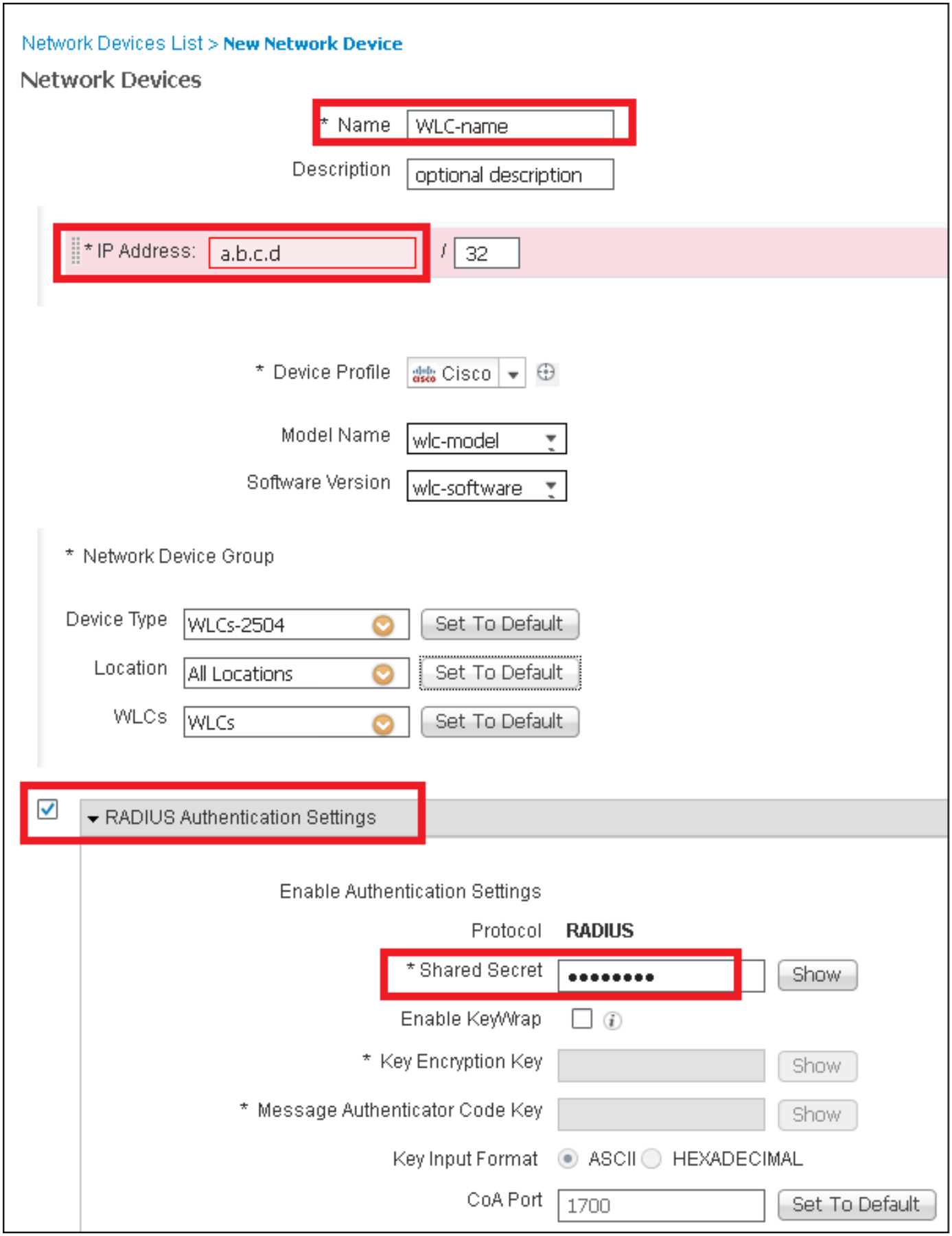
Шаг 1. Открытая консоль ISE и перешла к **администрированию> Сетевые ресурсы>, Сетевые устройства> Добавляют.**



Шаг 2. Заполните информацию

Дополнительно это может быть задано Имя модели, версия программного обеспечения, описание и назначить Группы сетевых устройств на основе типов устройства, местоположения или WLC.

o. b. c . d соответствуют интерфейсу WLC, который передает аутентификацию, которую запрашивают. По умолчанию это - интерфейс управления.

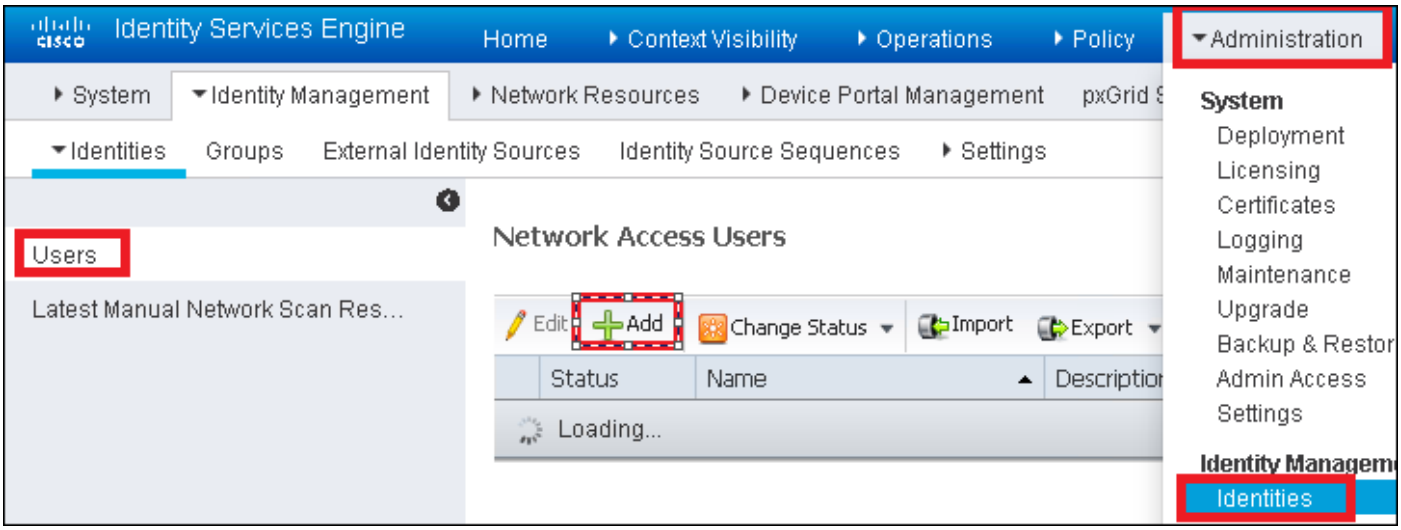


Для получения дополнительной информации о Группах сетевых устройств рассматривают эту ссылку:

[ISE - группы сетевых устройств]

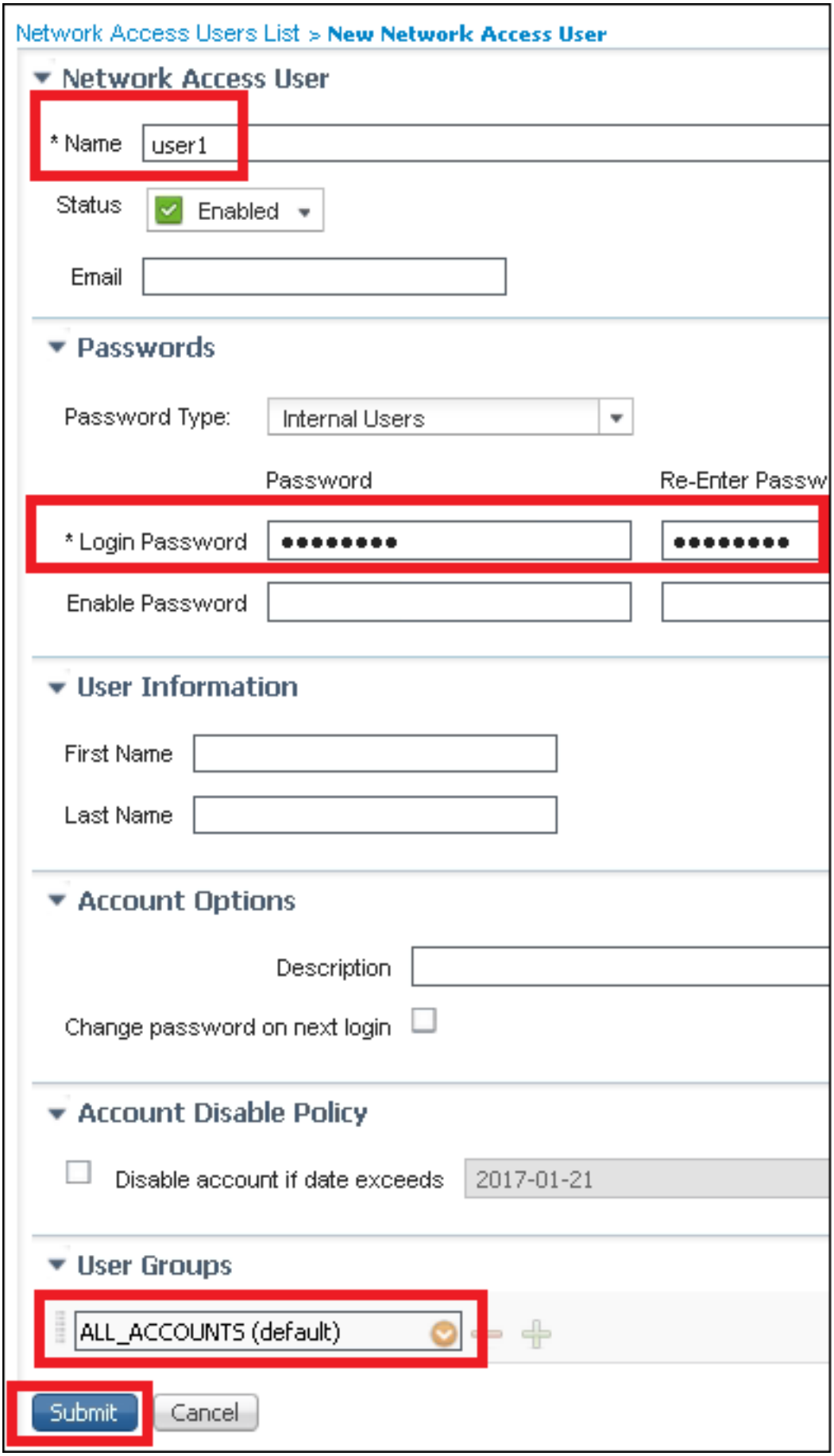
Создайте нового пользователя на ISE

Шаг 1. Перейдите к **администрированию> Управление идентификацией>, Идентификационный> Users> Добавляет**



Шаг 2. Заполните информацию

В данном примере этот пользователь принадлежит группе под названием ALL_ACCOUNTS, но это может быть отрегулировано по мере необходимости.

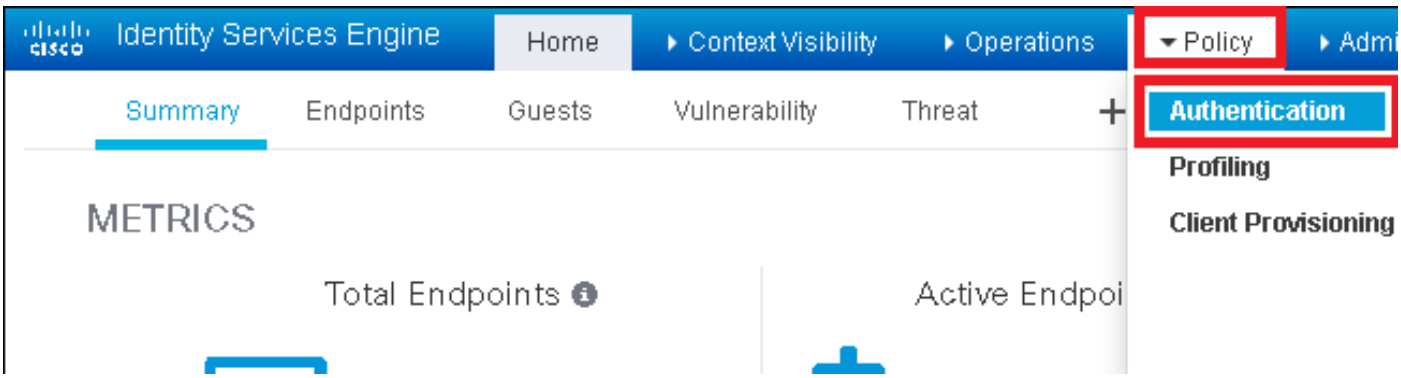


Создайте Опознавательное правило

Опознавательные правила используются, чтобы проверить, являются ли учетные данные пользователей правильными (Проверьте, является ли пользователь действительно то, кто

это говорит, что это), и ограничьте методы аутентификации , которым позволяют использоваться им.

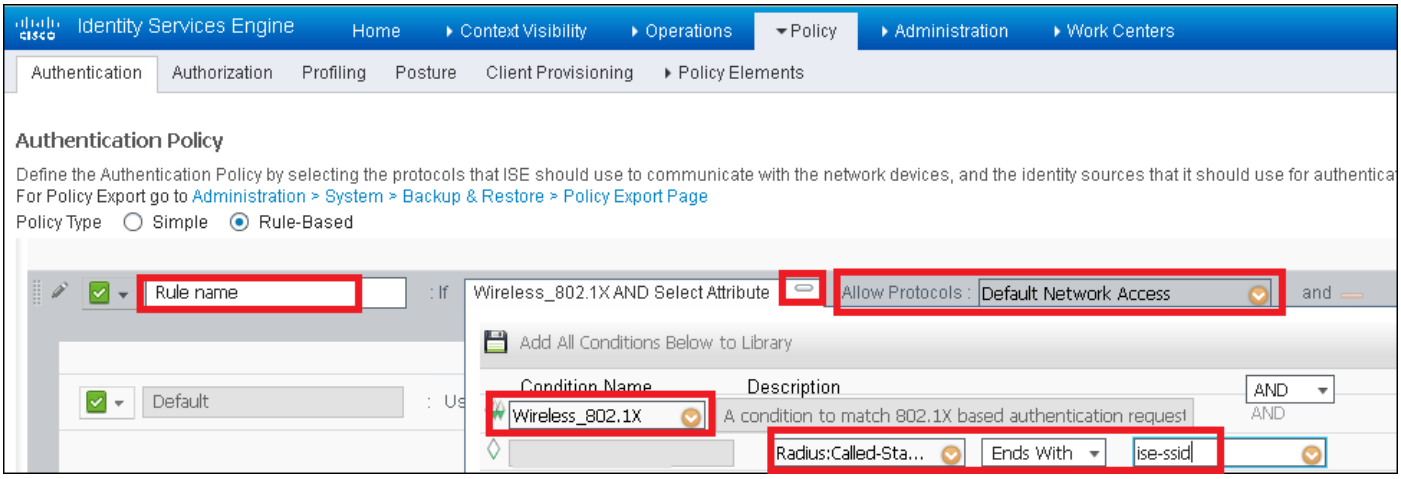
Шаг 1. Перейдите к **Политике> Аутентификация.**



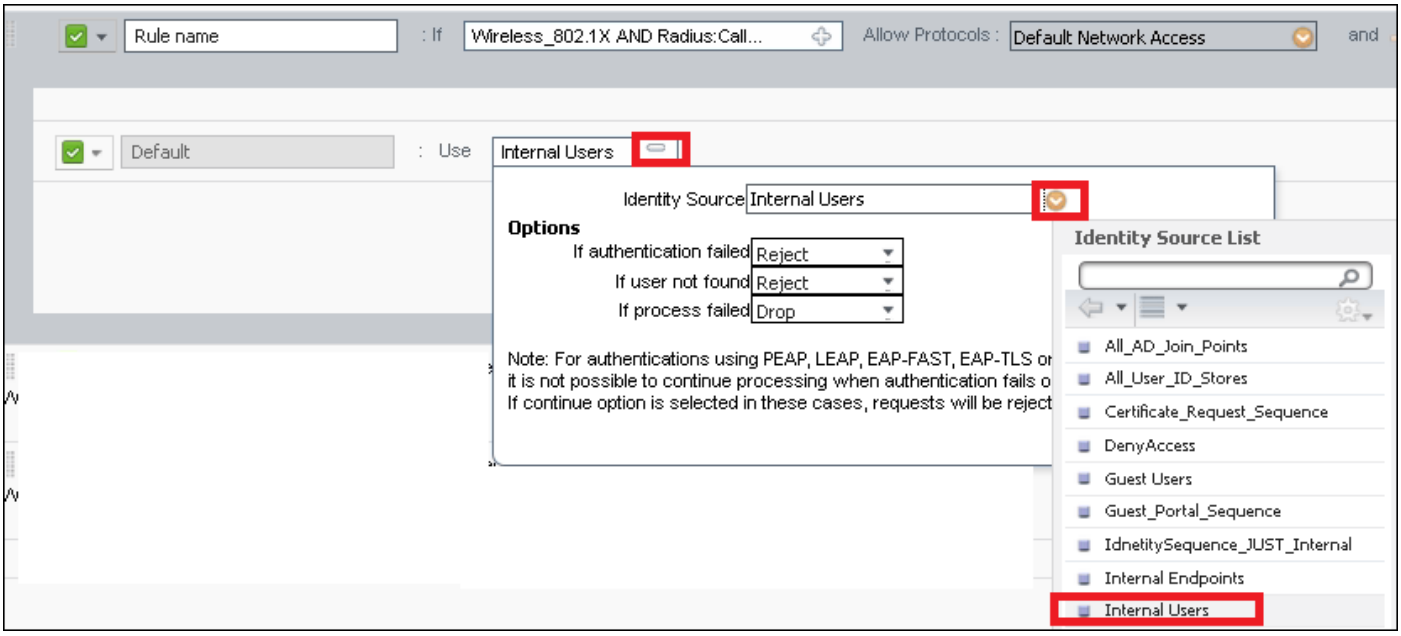
Шаг 2. Вставьте новое опознавательное правило.

Шаг 3. Введите значения.

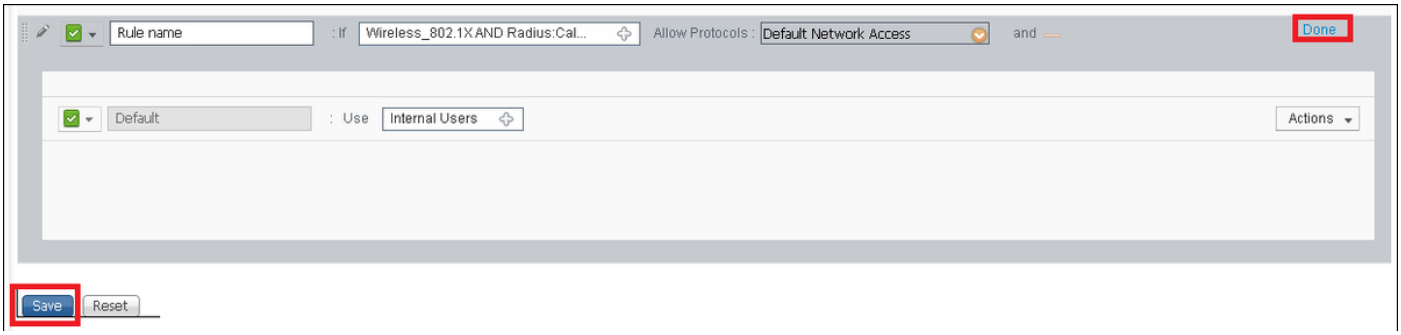
Это опознавательное правило позволяет все протоколы, перечисленные под списком **Доступа к сети по умолчанию**, это применяется к запросу аутентификации для беспроводных клиентов 802.1x и с Вызванным Station-ID и заканчивается **ssid ise**.



Также выберите Идентификационный источник для клиентов, который совпадает с этим опознавательным правилом, данный пример использует идентификационный список источников **Внутренних пользователей**



Как только Это закончено, нажимают **Done** и **Save**



Для получения дополнительной информации о Позволяют, что Политика Протоколов консультируется с этой ссылкой:

[Сервис разрешенных протоколов]

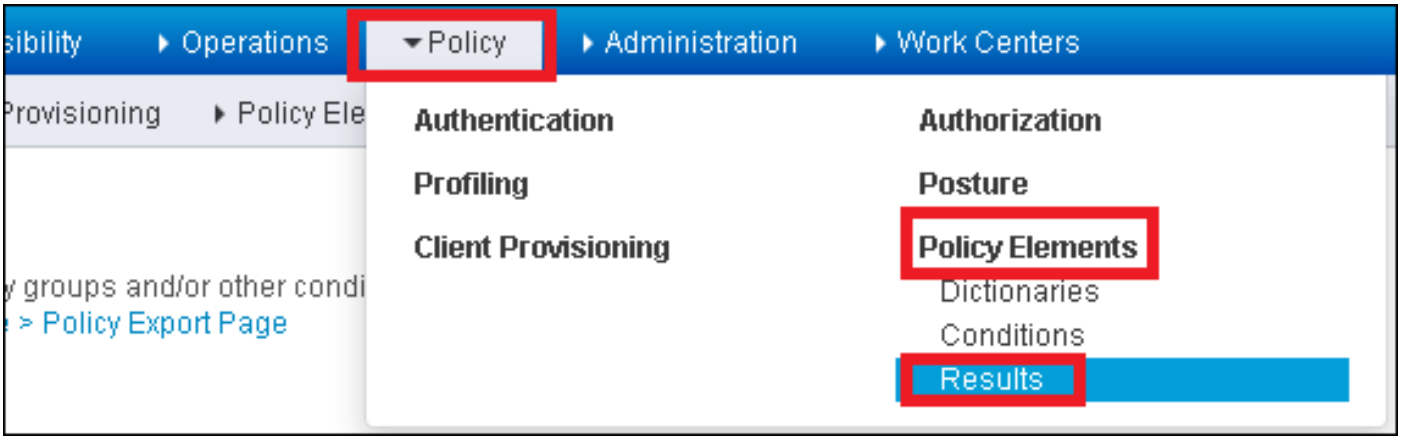
Для получения дополнительной информации об Идентичности источники консультируются с этой ссылкой:

[Создайте User Identity Group]

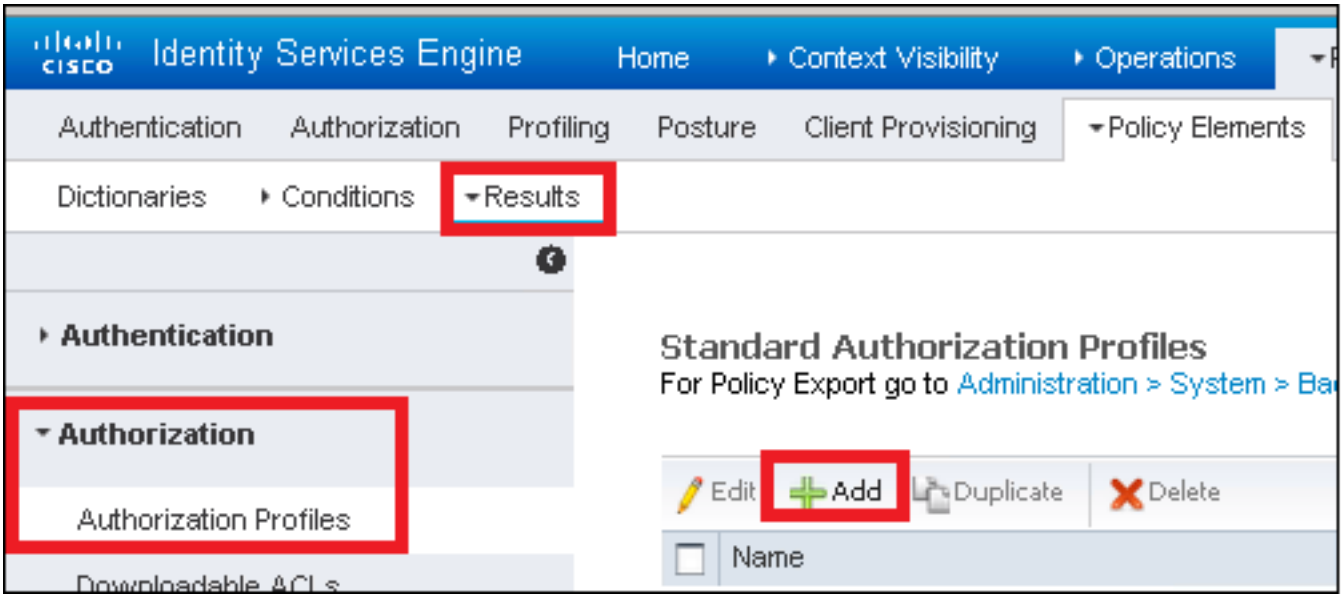
Создайте профиль Авторизации

Профиль авторизации определяет, есть ли у клиента доступ или не к сети, ACL толчка (списки контроля доступа), VLAN (Виртуальная локальная сеть) замена или какой-либо другой параметр. Профиль авторизации, показанный в данном примере, передает доступ, принимают для клиента, и назначает клиента на VLAN 2404.

Шаг 1. Перейдите к **Политике> Элементы Политики> Результаты**



Шаг 2. Добавьте новый профиль авторизации. Перейдите к **Авторизации>, Профили Авторизации> Добавляют**



Шаг 3. Заполните значения.