NAC (CCA): Настройка проверки подлинности Clean Access Manager (CAM) с помощью ACS

Содержание

Введение

Этот документ описывает, как настроить аутентификацию на Clean Access Manager (CAM) с сервером Cisco Secure Access Control Server (ACS). Для подобной конфигурации с помощью ACS 5.x и позже, обратитесь к NAC (CCA): Настройте Аутентификацию на Чистом Access Manager с ACS 5.x и Позже.

Предварительные условия

Требования

Эта конфигурация применима к версии 3.5 CAM и позже.

Используемые компоненты

Сведения в этом документе основываются на версии 4.1 CAM.

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.

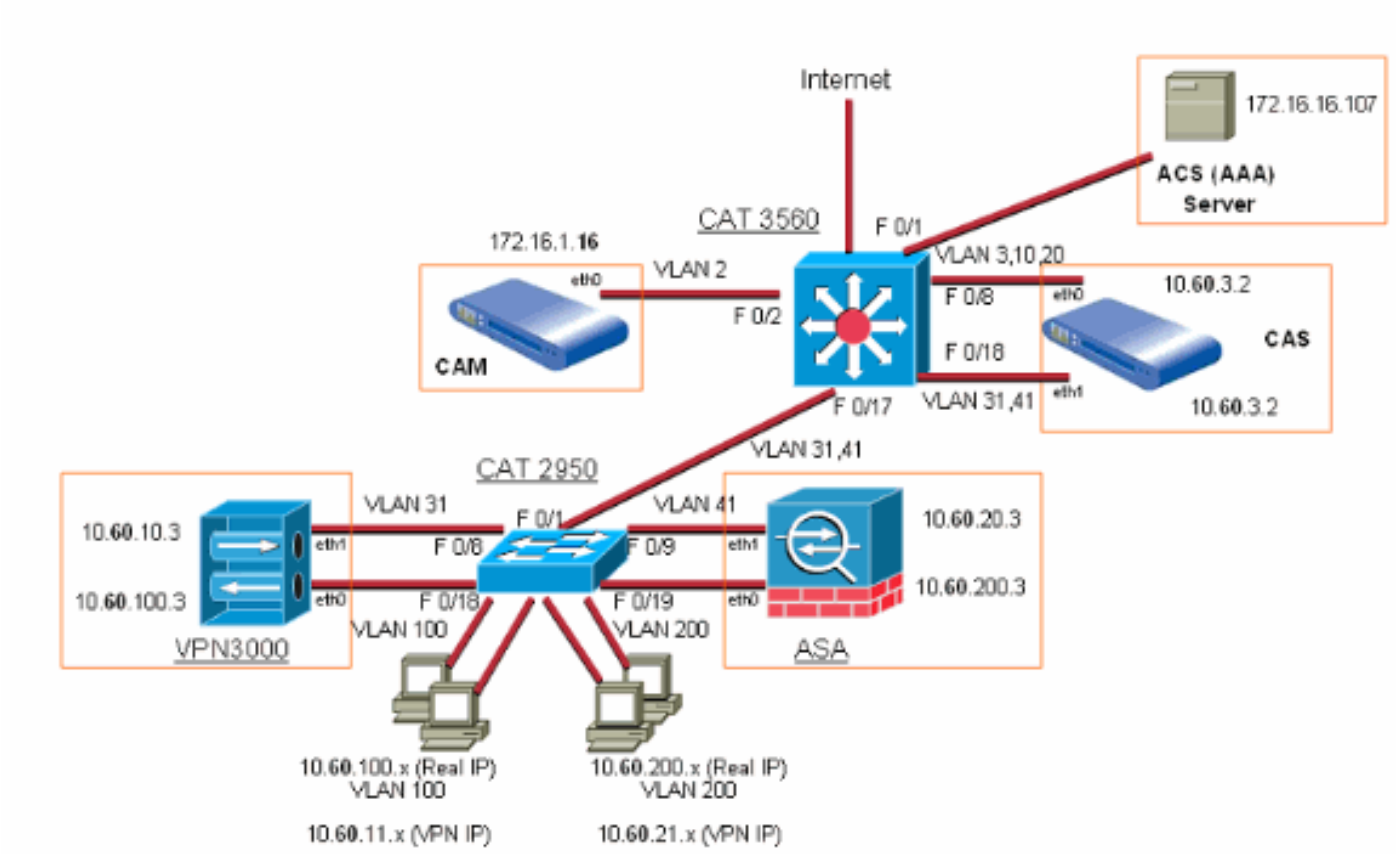
Настройка

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

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Схема сети

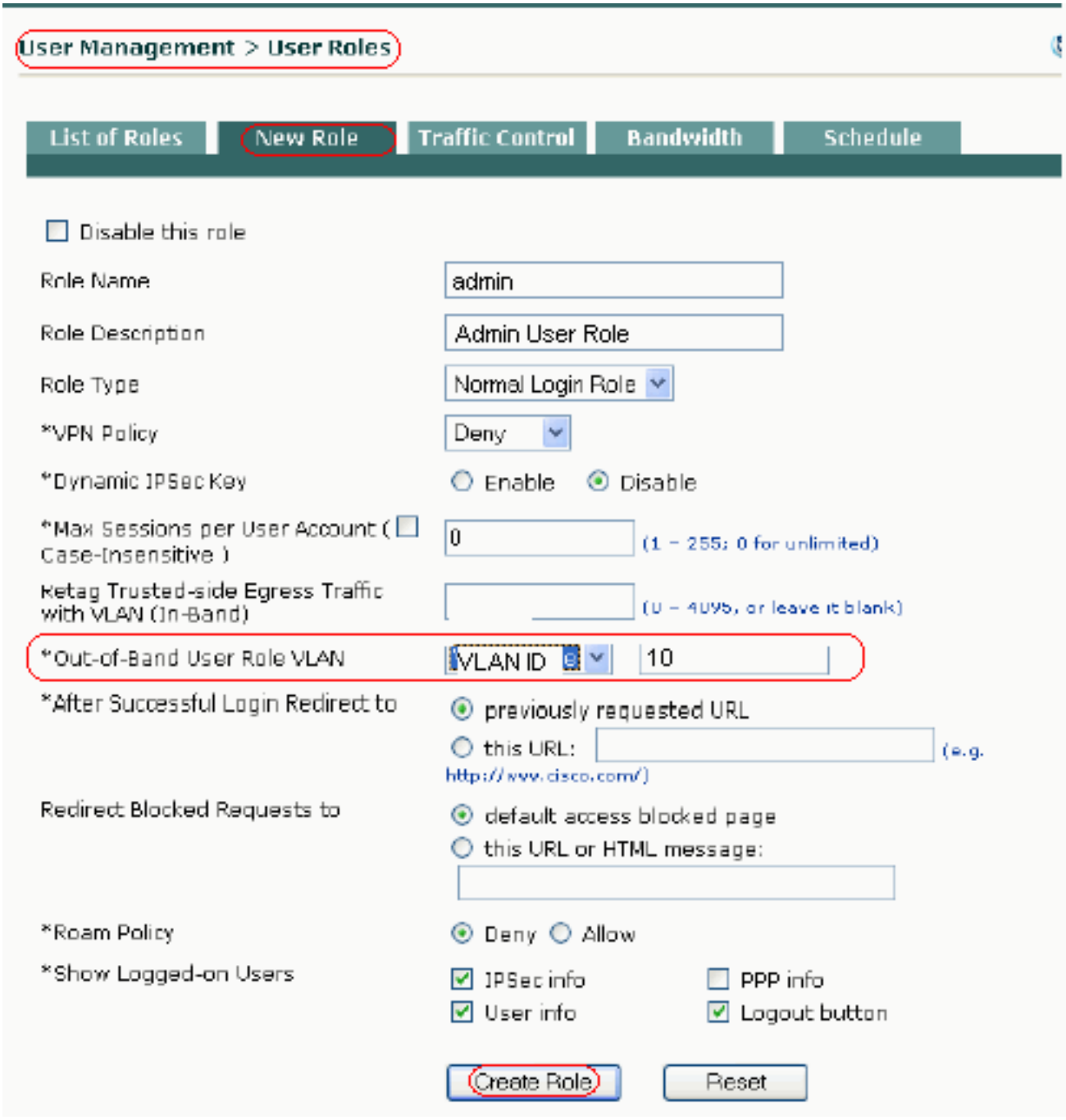
В настоящем документе используется следующая схема сети:



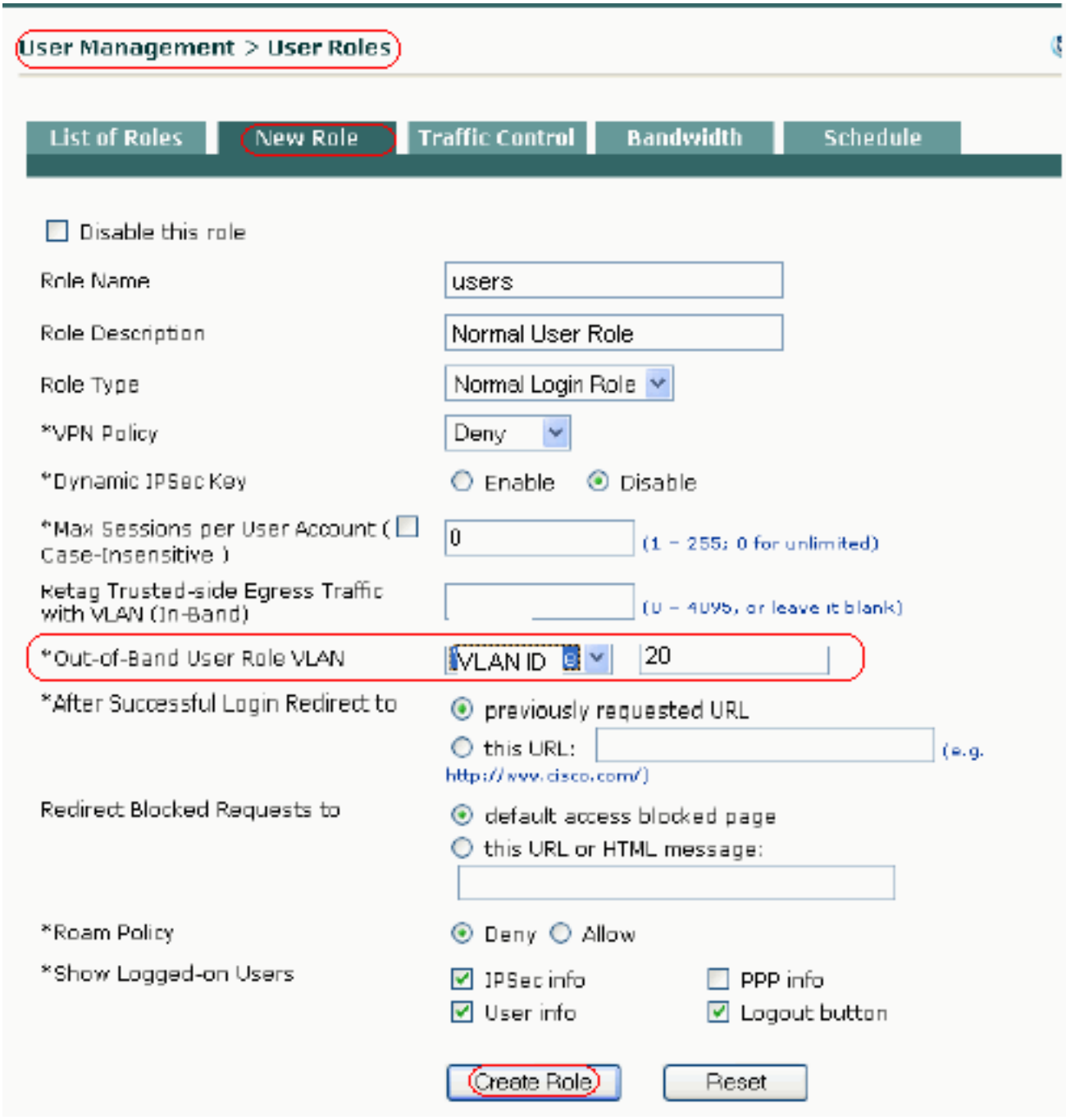
Шаги для Настройки аутентификации на CCA с ACS

Выполните следующие действия:

1. **Добавьте новые роли Создайте роль Admin**В CAM выберите **User Management> User Roles> New Role**.

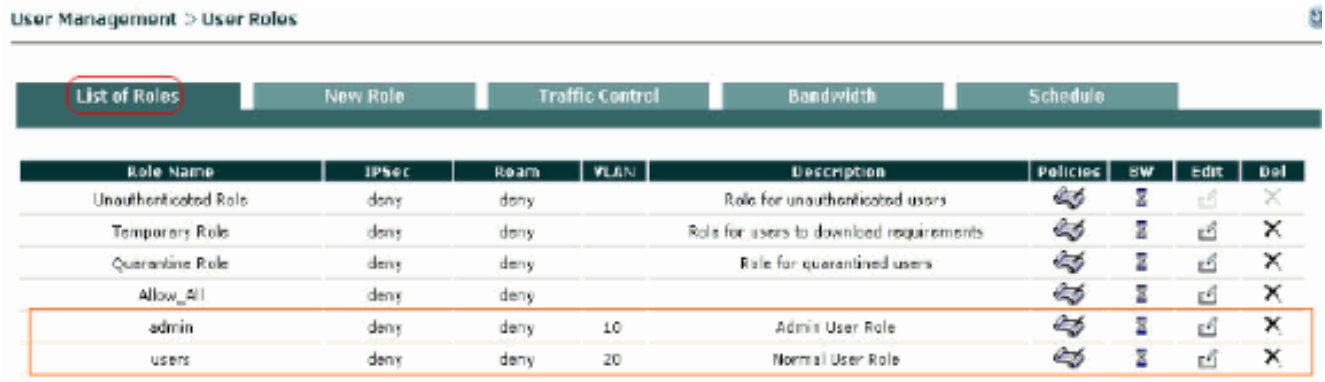


Введите уникальное имя, **admin**, для роли в поле Role Name.Введите **Роль пользователя Admin** как дополнительное Описание Роли.Выберите **Normal Login Role** в качестве типа роли.Настройте **Внеполосную (OOB)** VLAN роли пользователя с соответствующей VLAN. Например, выберите VLAN ID и задайте ID как 10.По окончании нажмите **Create Role**. Для восстановления свойств по умолчанию на форме нажмите **Reset**.Роль теперь появляется во вкладке List of Roles как показано в [VLAN Метки для Основанного на роли](#) раздела [сопоставлений OOB](#).**Создайте роль пользователя**В CAM выберите **User Management> User Roles> New Role**.

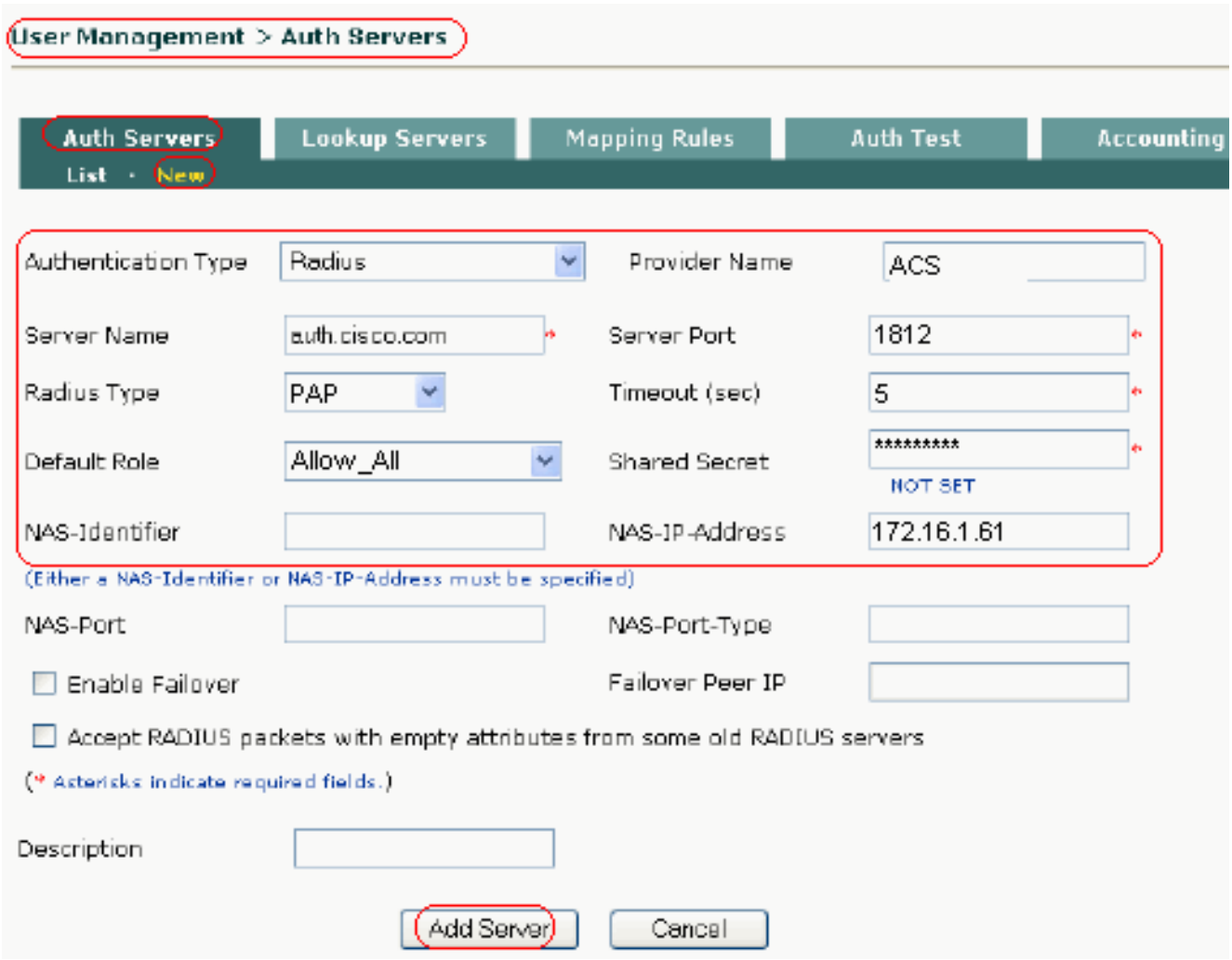


В ведите уникальное имя, **пользователей**, для роли в поле Role Name.Введите **Роль Обычного пользователя** как дополнительное Описание Роли.Настройте **Внеполосную (OOB)** VLAN роли пользователя с соответствующей VLAN. Например, выберите VLAN ID и задайте ID как 20.По окончании нажмите **Create Role**. Для восстановления свойств по умолчанию на форме нажмите **Reset**.Роль теперь появляется во вкладке List of Roles как показано в VLAN Метки для Основанного на роли раздела сопоставлений OOB.

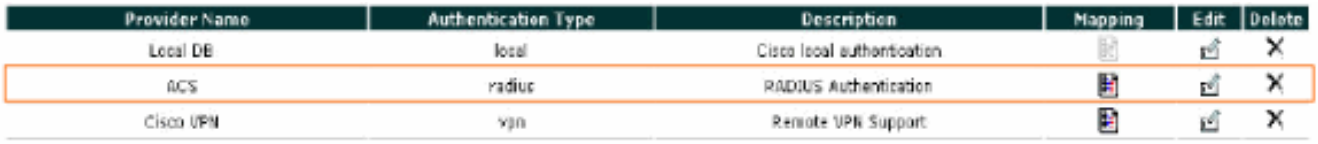
2. **VLAN метки для Основанных на роли сопоставлений OOB**В CAM выберите **User Management> User Roles> List of Roles** для наблюдения списка ролей до сих пор.



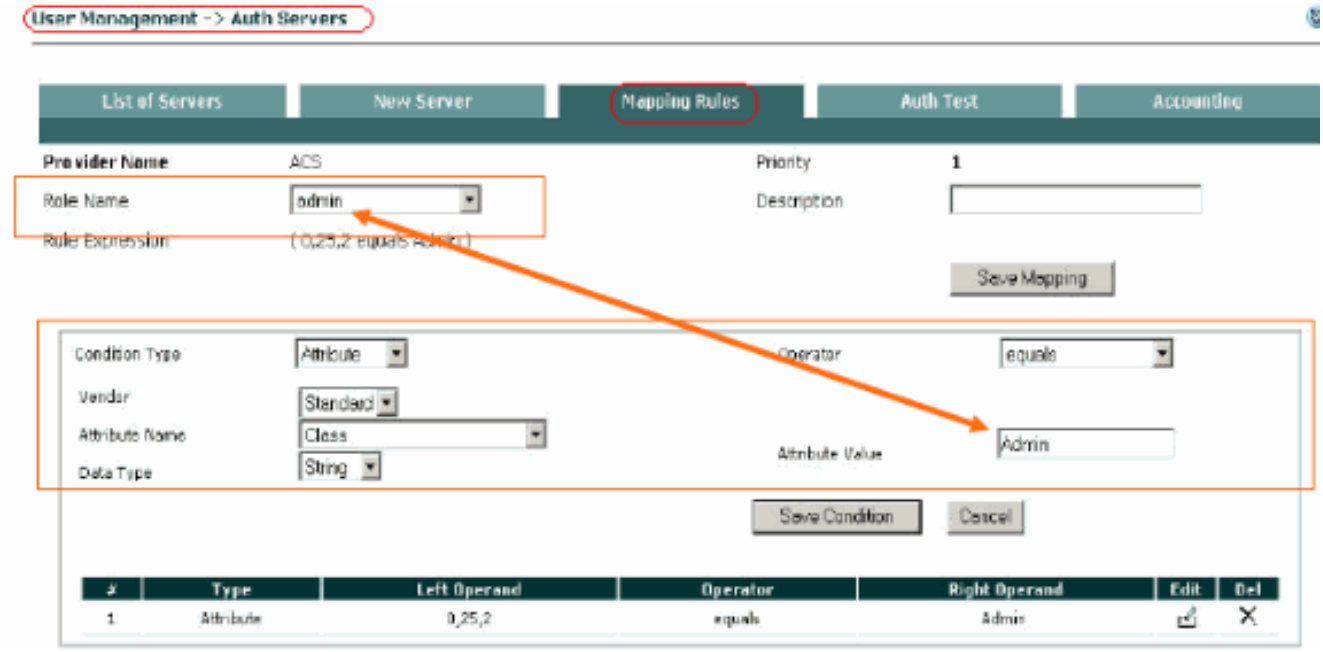
3. **Добавьте сервер проверки подлинности RADIUS (ACS)**Выберите **User Management> Auth Servers>**
New.



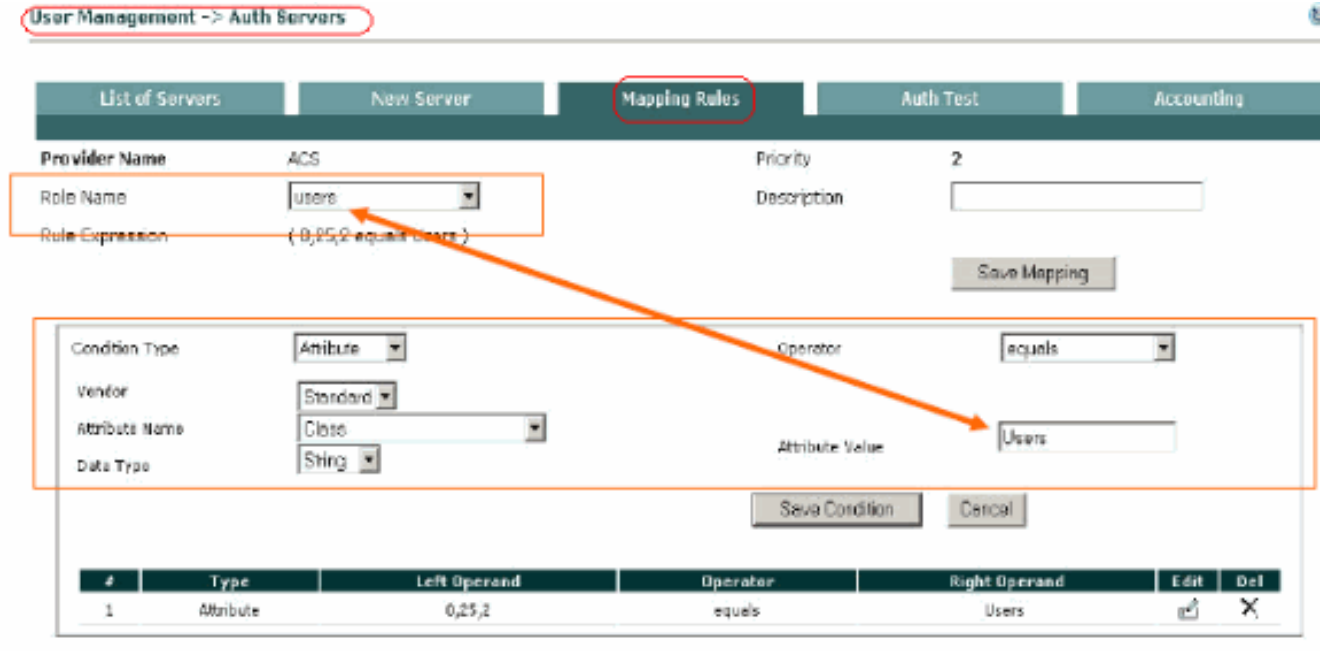
От раскрывающегося меню Типа проверки подлинности выберите **Radius**.Введите имя поставщика как **ACS**.Введите Имя сервера как **аутентификацию. cisco . com**.**Порт сервера** — номер порта **1812**, на котором слушает сервер RADIUS.**RADIUS Type. Метод аутентификации RADIUS.** Поддерживаемые методы включают EAPMD5, PAP, CHAP, MSCHAP и MSCHAP2.**Роль по умолчанию** используется, если сопоставление с ACS не определено или установлено правильно, или если атрибут RADIUS не определен или установлен правильно на ACS.**Общий секретный ключ** — общий секретный ключ RADIUS, связанный с IP-адресом указанного клиента.**Nas-ip-address** — Это значение, которое будет передаваться со всеми пакетами Проверки подлинности RADIUS.**Нажмите Add**
сервер.



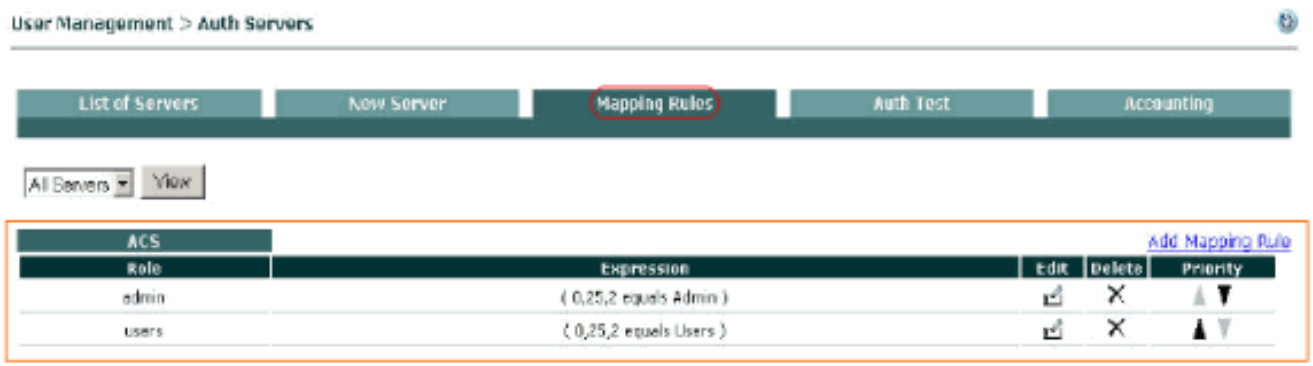
4. **Сопоставьте пользователей ACS с ролями пользователя CCA**Выберите **User Management> Auth Servers> Mapping Rules> Add Mapping Link** для сопоставления пользователя с правами администратора в ACS к роли пользователя с правами администратора
CCA.



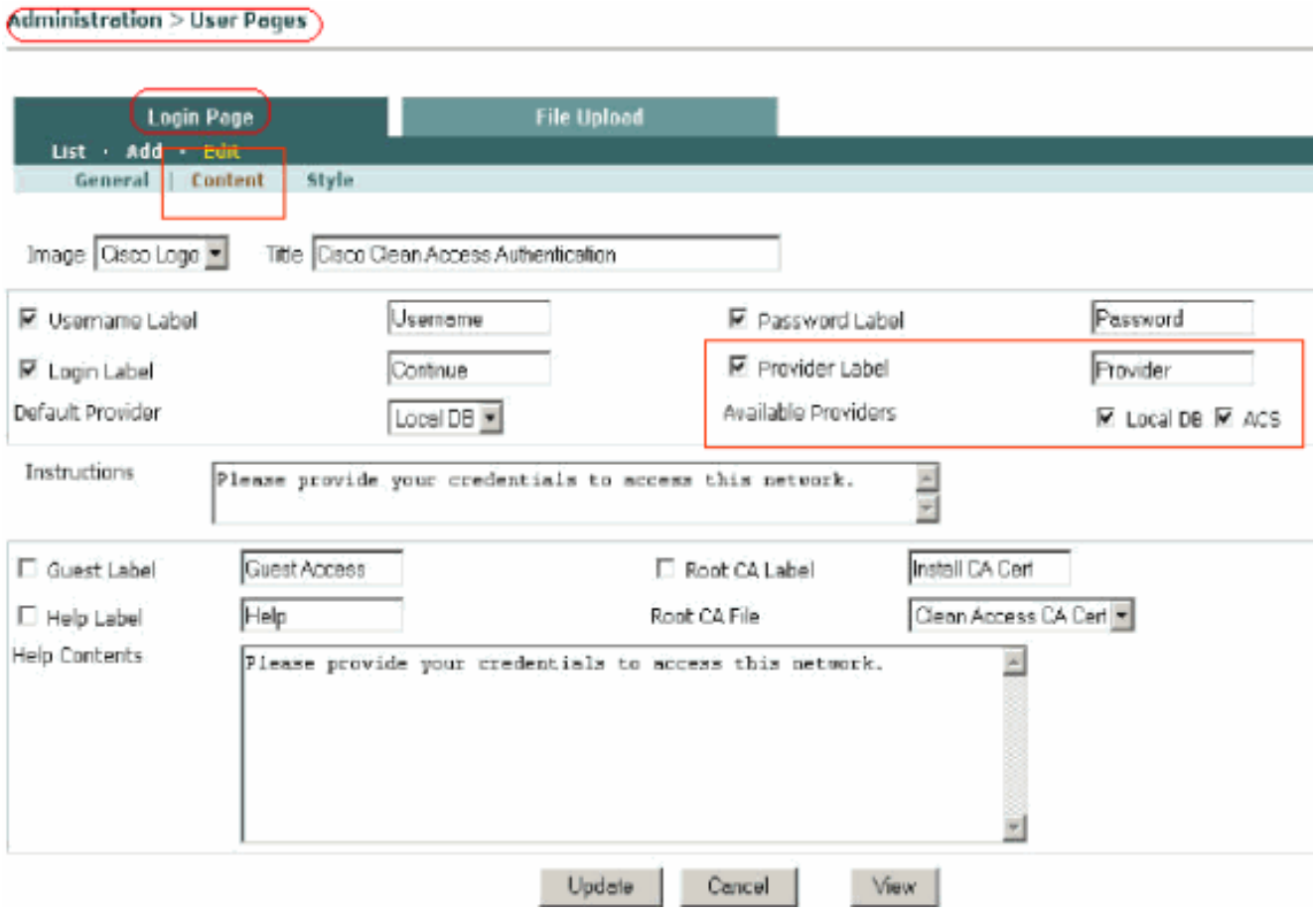
Выберите **User Management> Auth Servers> Mapping Rules> Add Mapping Link** для сопоставления обычного пользователя в ACS к роли пользователя
CCA.



Вот сводка сопоставления роли пользователя:

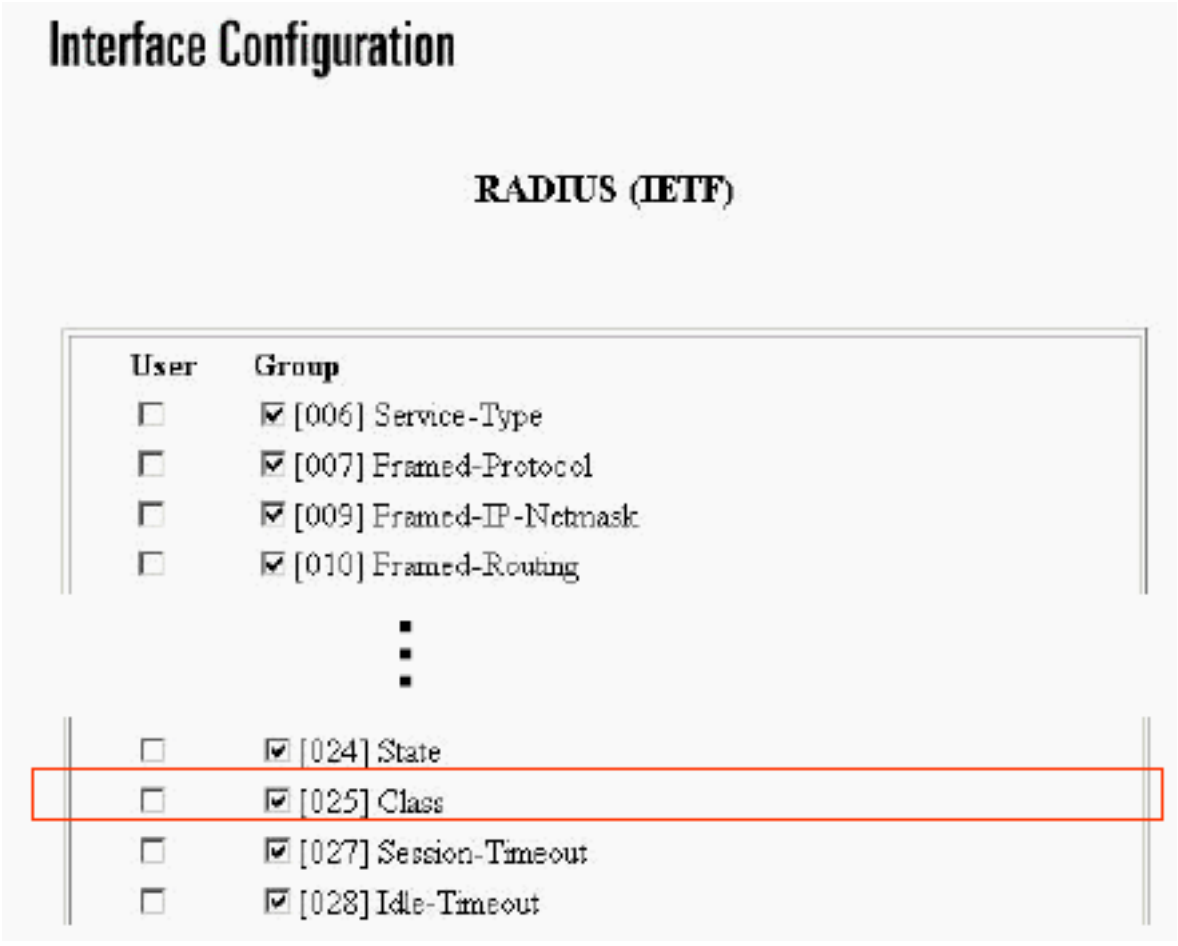


5. **Включите альтернативным поставщикам на странице пользователя**Выберите **Administration> User Pages> Login Page> Add> Content**, чтобы включить альтернативным поставщикам на странице регистрационной информации пользователя для
входа.



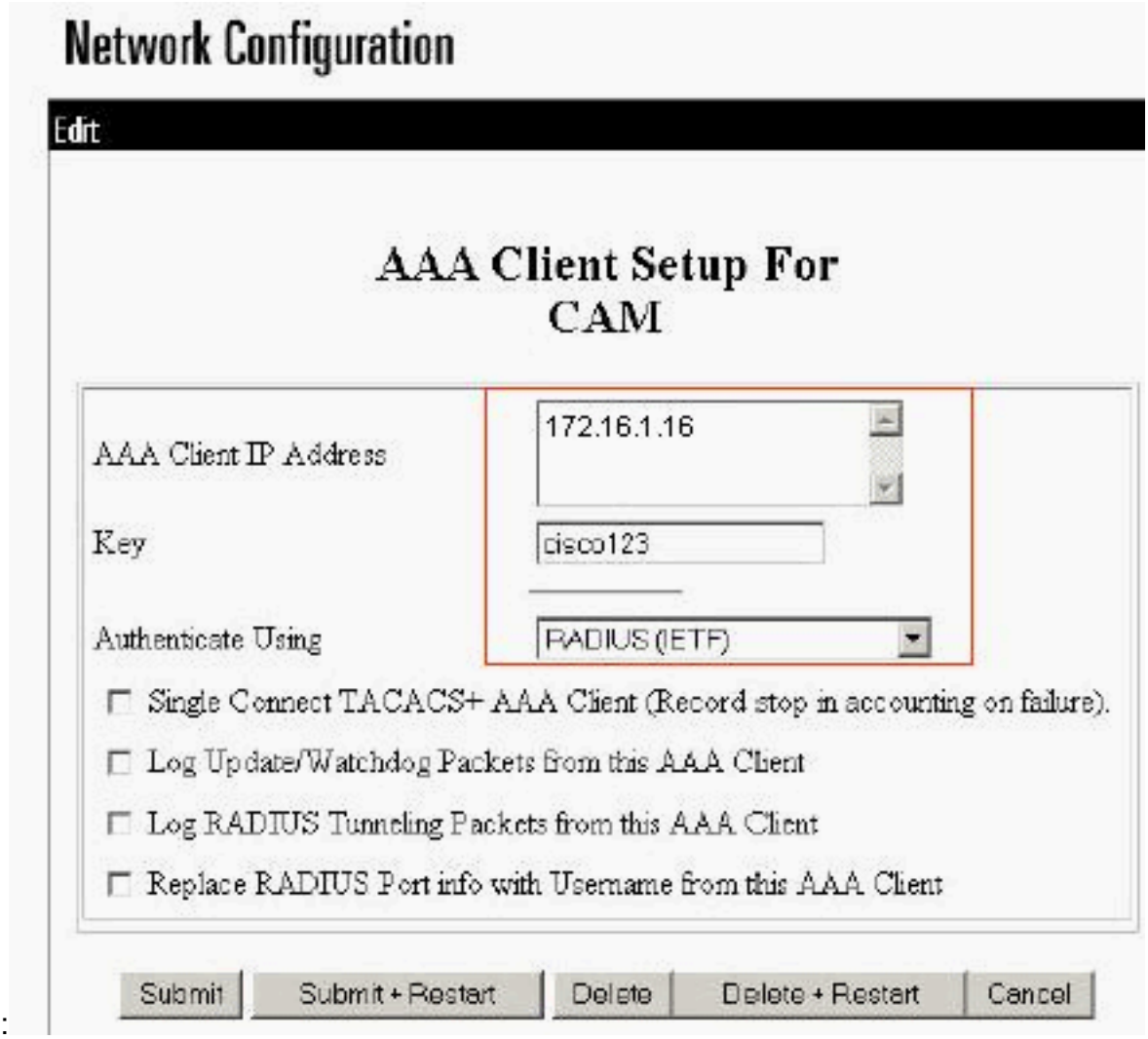
Конфигурация AcS

1. Выберите **Interface Configuration**, чтобы удостовериться, что включен RADIUS (IETF) Атрибут Class



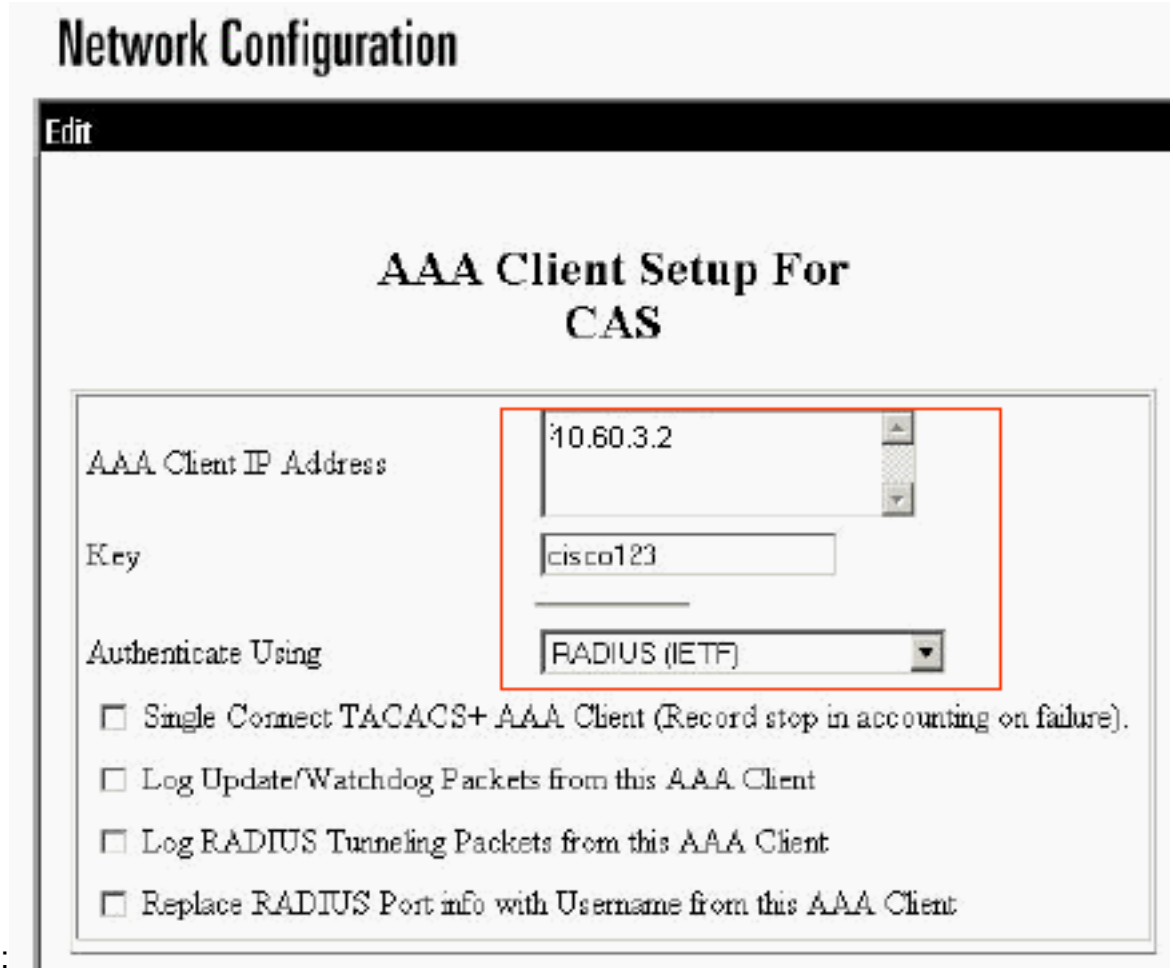
[025].

2. **Добавьте КЛИЕНТА RADIUS к серверу ACS**Выберите **Network Configuration** для добавления CAM клиента AAA как



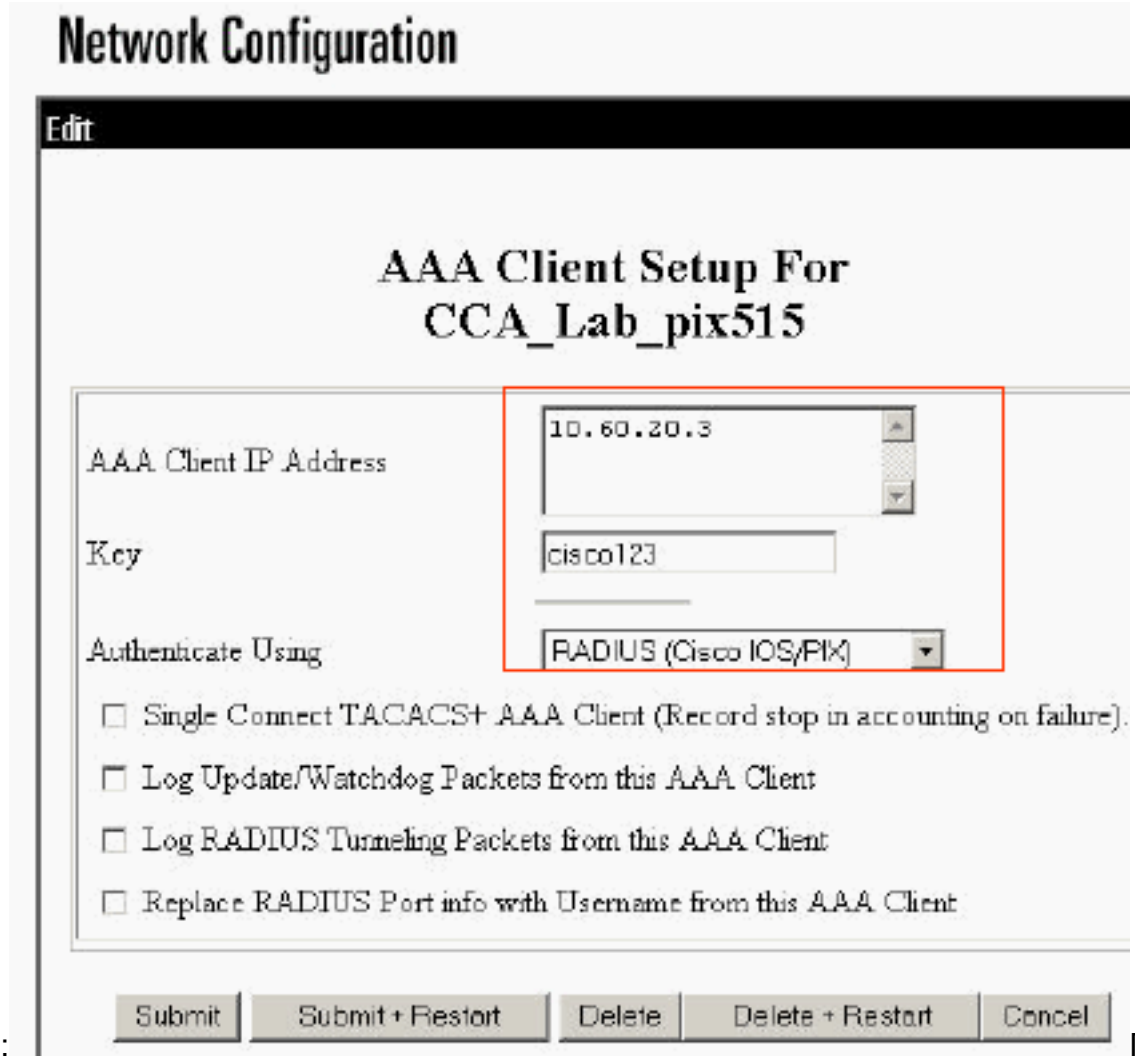
показано:

Нажмите Submit + Restart.Примечание: Удостоверьтесь, что ключ RADIUS совпадает с клиентом AAA и RADIUS использования (IETF).Выберите **Network Configuration** для добавления CAS клиента AAA как



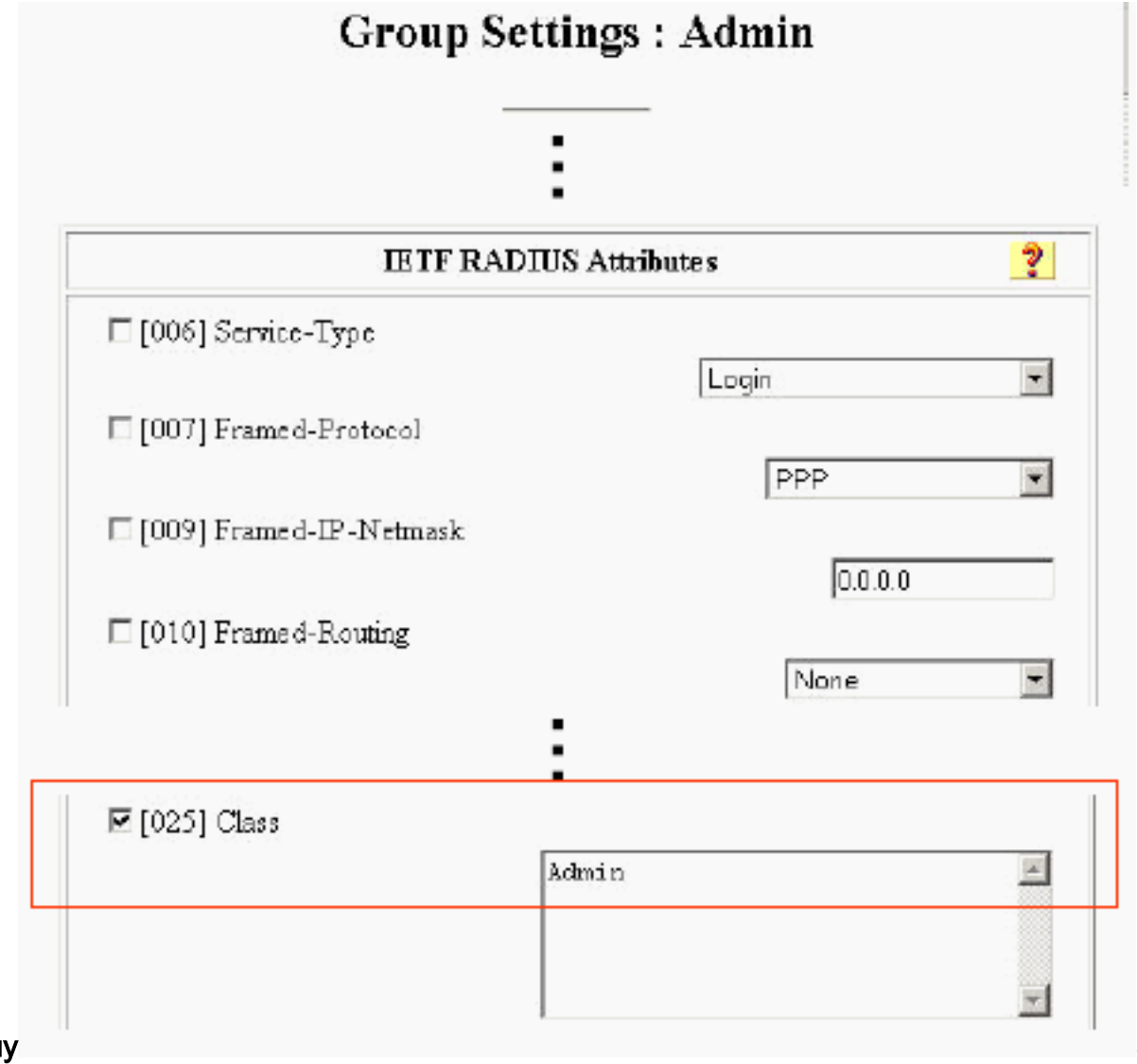
показано:

Нажмите Submit + Restart.Примечание: Для учета RADIUS Шлюза VPN политика CCA должна позволить пакетам учета RADIUS (UDP 1646/1813) от IP-адреса CAS проходить не прошедший поверку подлинности к IP-адресу сервера ACS.Выберите **Network Configuration** для добавления ASA клиента AAA как

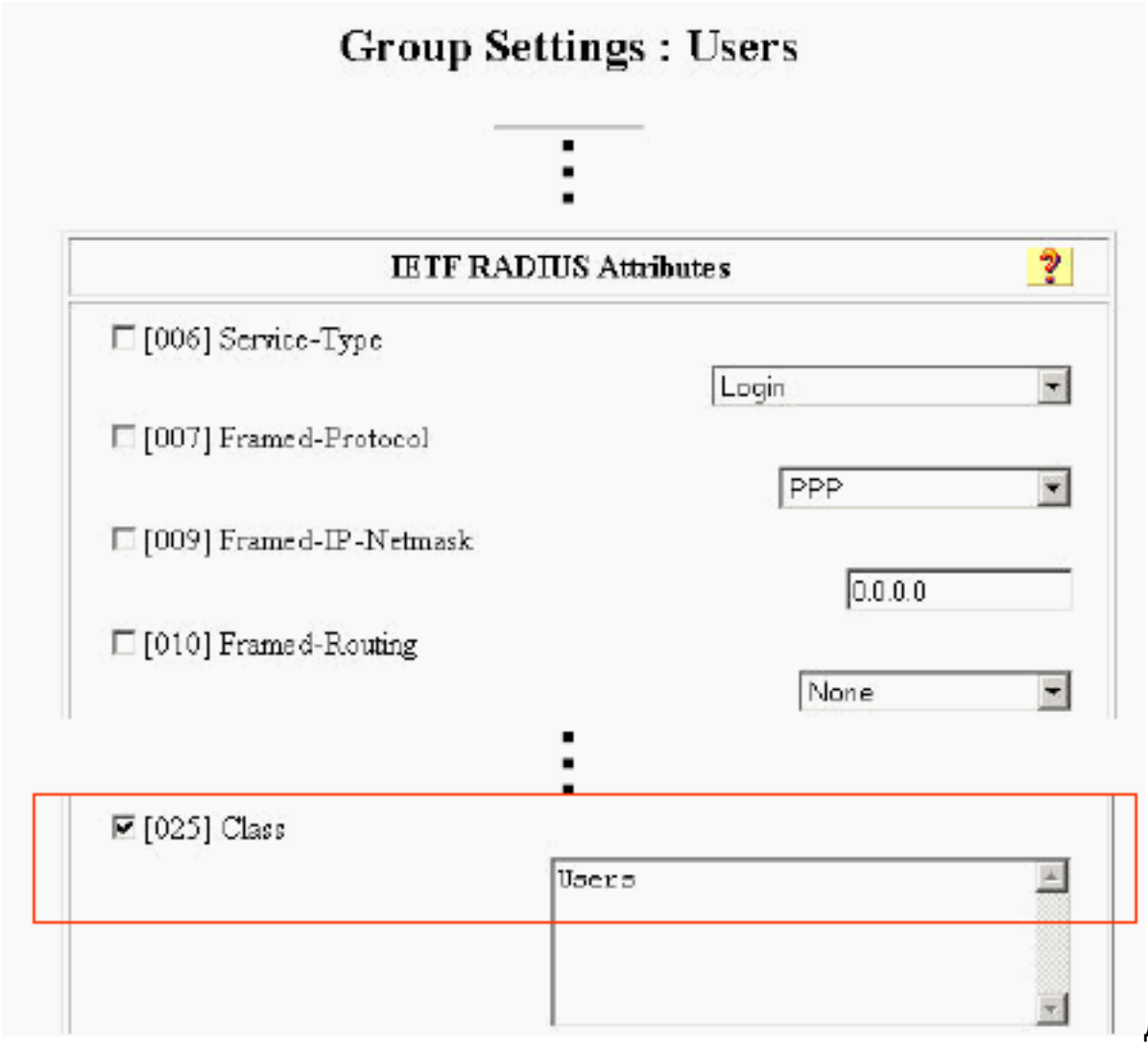


показано: По льзовательский PIX/ASA почти стороны взаимодействует адрес (как правило, внутренний интерфейс)Тип набора к RADIUS (Cisco IOS / PIX).

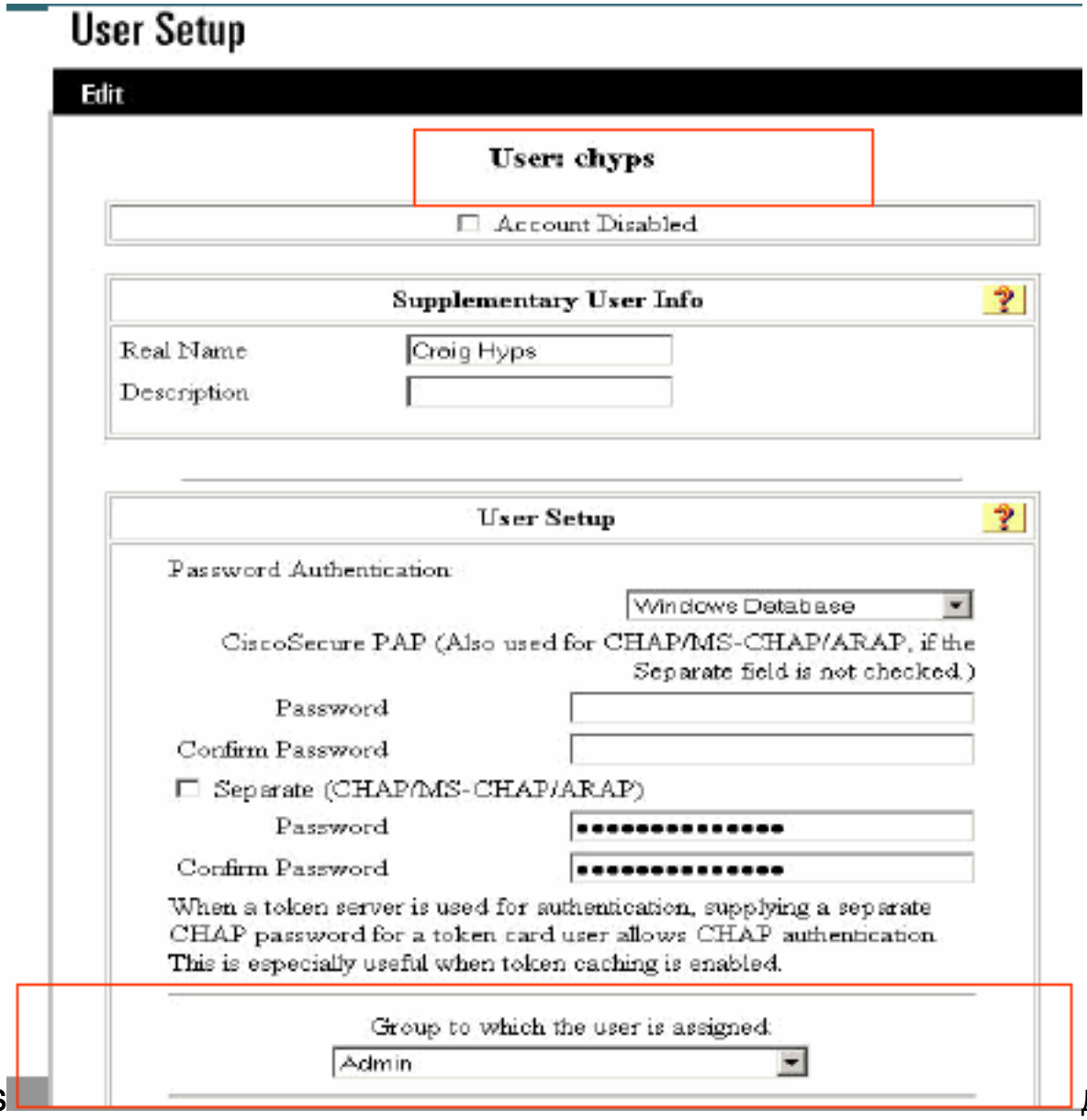
3. **Добавьте, что / Настраивают Группы на Сервере ACSСоздайте Административную**



группу За ставьте Атрибут Class РАДИУСА IETF [025] адаптировать групповое значение.Значение должно совпасть, который настроил на сопоставлении CAS.**Создайте Группу пользователей**



Добавьте/настройте группу для каждой Чистой Роли Пользователя доступа, которая будет сопоставлена.**Добавьте/Настройте Пользователей на Сервере**

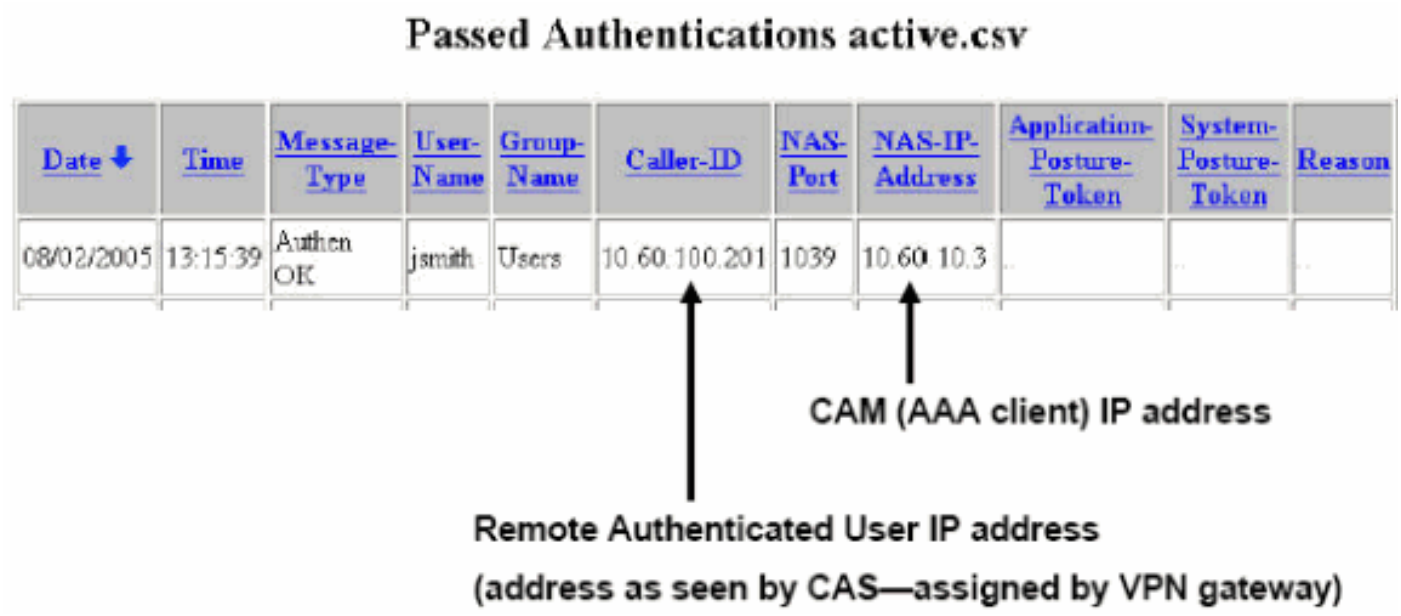


ACS Доба вьте/настройте пользователя ACS для каждого Чистого Пользователя доступа, чтобы аутентифицироваться ACS.Состав группы ACS набора.ACS также поддерживает проверку подлинности прокси-сервера к другим внешним серверам.

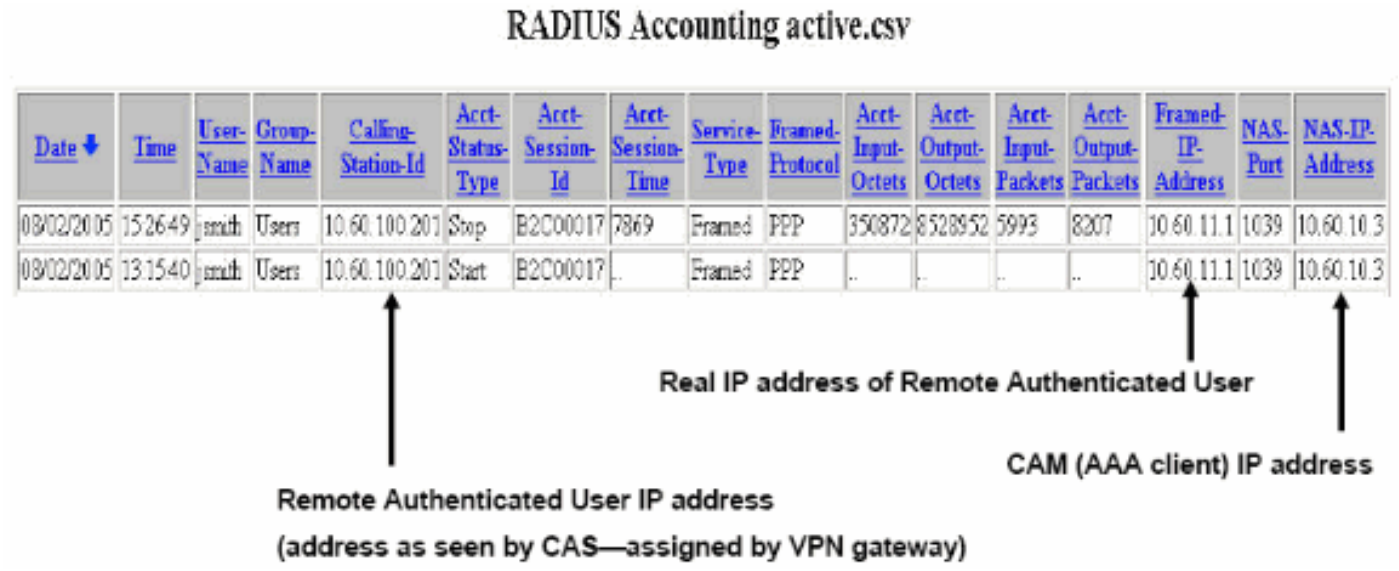
Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

В разделе мониторинга ACS вы видите информацию о переданных аутентификациях как показано:



Точно так же вы видите снимок экрана для учета RADIUS:



Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Страница технической поддержки устройства Cisco NAC
- Cisco Systems – техническая поддержка и документация