ACS 5.x и позже: Интеграция с Примером конфигурации Microsoft Active Directory

Содержание

Введение

В этом документе рассматривается пример настройки для интеграции Microsoft Active Directory с системой управления доступом Cisco Secure ACS 5.x и выше. ACS использует Microsoft Active Directory (AD) в качестве внешнего хранилища идентификационных данных для хранения информации о таких ресурсах, как пользователи, машины, группы и атрибуты. ACS выполняет аутентификацию этих ресурсов, сверяясь с AD.

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Windows Active Directory Domain, который будет использоваться потребности, которые будут полностью настроены, и в рабочем состоянии.
- Используйте Домен Microsoft Windows server 2003 года, Домен Microsoft Windows server 2008 года или Домен R2 Microsoft Windows server 2008 года, в то время как они поддерживаются ACS 5. x.**Примечание:** Интеграция Домена R2 Microsoft Windows server 2008 года с ACS поддерживается от ACS 5.2 и позже.

Используемые компоненты

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

- Cisco Secure ACS 5.3
- Домен Microsoft Windows server 2003 года

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.

Общие сведения

Windows Active Directory предоставляет много функций, которые использованы в ежедневном использовании сети. Интеграция ACS 5.x с AD позволяет использование существующих AD пользователей, машин и их сопоставления группы.

ACS 5.x интегрированный с AD предоставляет эти функции:

1. Аутентификация компьютера
2. Извлечение атрибута для авторизации
3. Извлечение сертификата для проверки подлинности EAP-TLS
4. Пользователь и ограничение учетной записи машины
5. Ограничения доступа машины
6. Проверка полномочий для удаленного доступа по телефонной линии
7. Параметры обратного вызова для Пользователей с наборным телефонным доступом
8. Атрибуты поддержки наборного (телефонный) доступа

!--- конфигурацию

Настройте ACS 5.x механизм установки приложений (ОС ADE)

Прежде чем вы интегрируете ACS 5.x к AD, гарантируете, что **TimeZone, Дата и Время** на ACS совпадают с этим на AD Primary Domain Controller. Кроме того, определите сервер DNS на ACS, чтобы быть в состоянии решить доменное имя от ACS 5. x. Выполните эти шаги для настройки ACS 5.x Механизм Установки приложений (ОС ADE):

1. SSH к прибору ACS и вводит учетные данные CLI.
2. Выполните **команду clock timezone** в режиме конфигурации как показано для настройки **ЧАСОВОГО ПОЯСА** на ACS для соответствия с этим на контроллере домена. `clock timezone Asia/Kolkata` **Примечание:** Азия/Калькутта является часовым поясом, используемым в этом документе. Можно найти определенный часовой пояс командой **show timezone** режима EXEC.
3. В случае, если ваш AD контроллер домена синхронизируется с сервером NTP, который

находится в вашей сети, он настоятельно рекомендован для использования того же сервера NTP на ACS. Если у вас нет сервера NTP, то пропустите к **шагу 4**. Это шаги для настройки сервера NTP:Сервер NTP может быть настроен с **командой ntp server <ip address of the NTP server>** в режиме конфигурации как показано.`ntp server 192.168.26.55`
`The NTP server was modified.`
`If this action resulted in a clock modification, you must restart ACS.`См. ACS 5. x: Синхронизация ACS Cisco с Примером конфигурации Сервера NTP для получения дополнительной информации о конфигурации NTP.

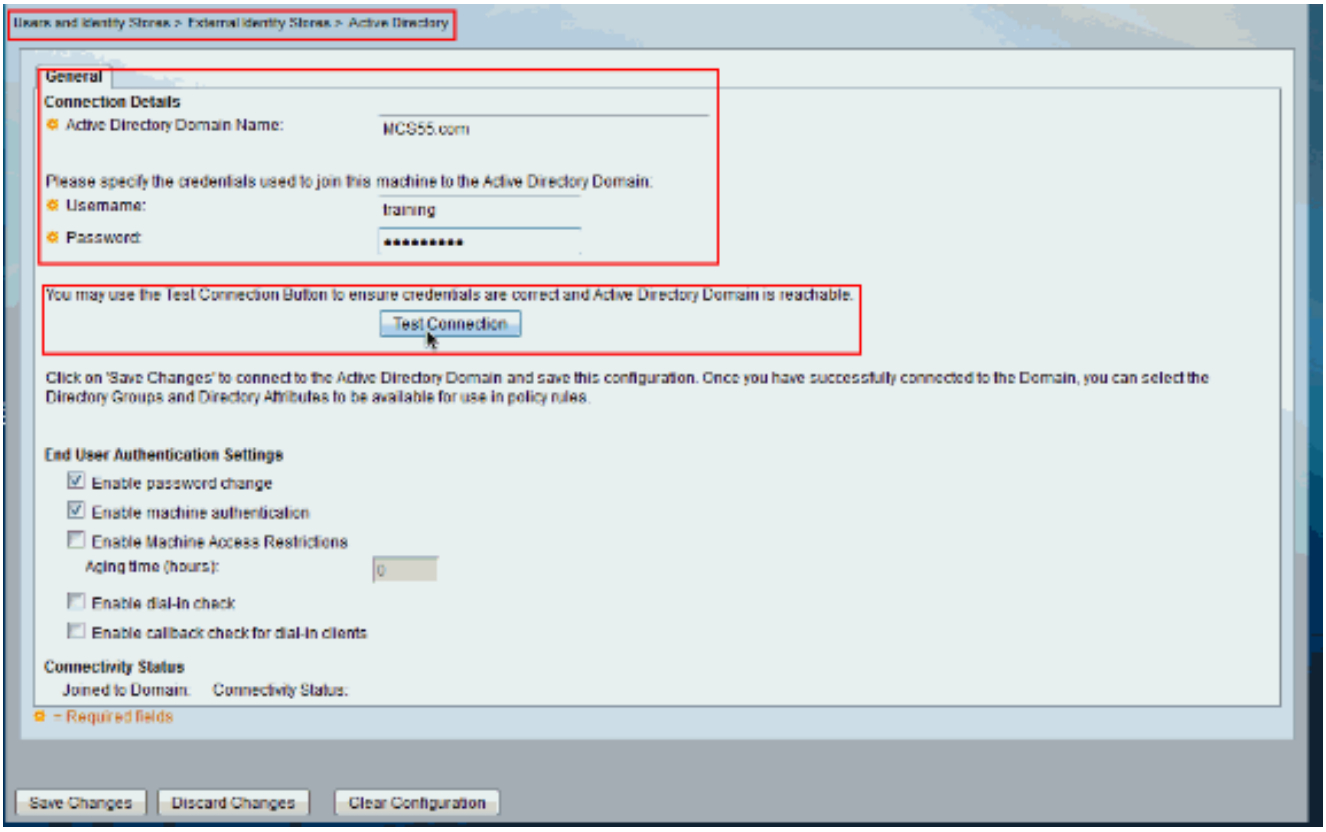
4. Для настройки даты и времени, вручную используют **команду clock set** в **режиме EXEC**. Пример выходных данных команды приводится ниже:
```
clock set Jun 8 10:36:00 2012
Clock was modified. You must restart ACS.
Do you want to restart ACS now? (yes/no) yes
Stopping ACS.
Stopping Management and View.....................
Stopping Runtime......
Stopping Database....
Cleanup.....
Starting ACS ....

To verify that ACS processes are running, use the
'show application status acs' command.
```
5. Теперь проверьте **Часовой пояс, Дата и время** с **командой show clock**. Выходные данные команды show clock показывают здесь:`acs51/admin# **show clock** Fri Jun 8 10:36:05 IST 2012`
6. Настройте DNS на ACS с **<**команда **<ip address of the DNS> ip name-server** в **режиме конфигурации** как показано здесь:`ip name-server 192.168.26.55`**Примечание:** IP-адрес DNS предоставлен вашим администратором Домена Windows.
7. Выполните **команду nslookup <domain name>** для проверки достижимости доменного имени как показано.`acs51/admin#**nslookup MCS55.com** Trying "MCS55.com" ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60485 ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1 ;; QUESTION SECTION: ;MCS55.com. IN ANY ;; ANSWER SECTION: MCS55.com. 600 IN A 192.168.26.55 MCS55.com. 3600 IN NS admin-zq2ttn9ux.MCS55.com. MCS55.com. 3600 IN SOA admin-zq2ttn9ux.MCS55.com. hostmaster.MCS55.com. 635 900 600 86400 3600 ;; ADDITIONAL SECTION: admin-zq2ttn9ux.MCS55.com. 3600 IN A 192.168.26.55 Received 136 bytes from 192.168.26.55#53 in 0 ms` **Примечание:** Если **ОТВЕТИТЬ РАЗДЕЛ** пуст, то свяжитесь со своим администратором домена Windows для обнаружения корректного сервера DNS для домена.
8. Выполните **команду ip domain-name <domain name>** для настройки **DOMAIN-NAME** на ACS как показано здесь:`ip domain-name MCS55.com`
9. Выполните **команду hostname <hostname>** для настройки **ИМЕНИ ХОСТА** на ACS как показано здесь:`hostname acs51`**Примечание:** Из-за ограничений NetBIOS, имена хоста ACS должны содержать меньше чем или равный 15 символам.
10. Выполните **Команду write memory** для сохранения конфигурации к ACS.

ACS соединения 5.x к AD

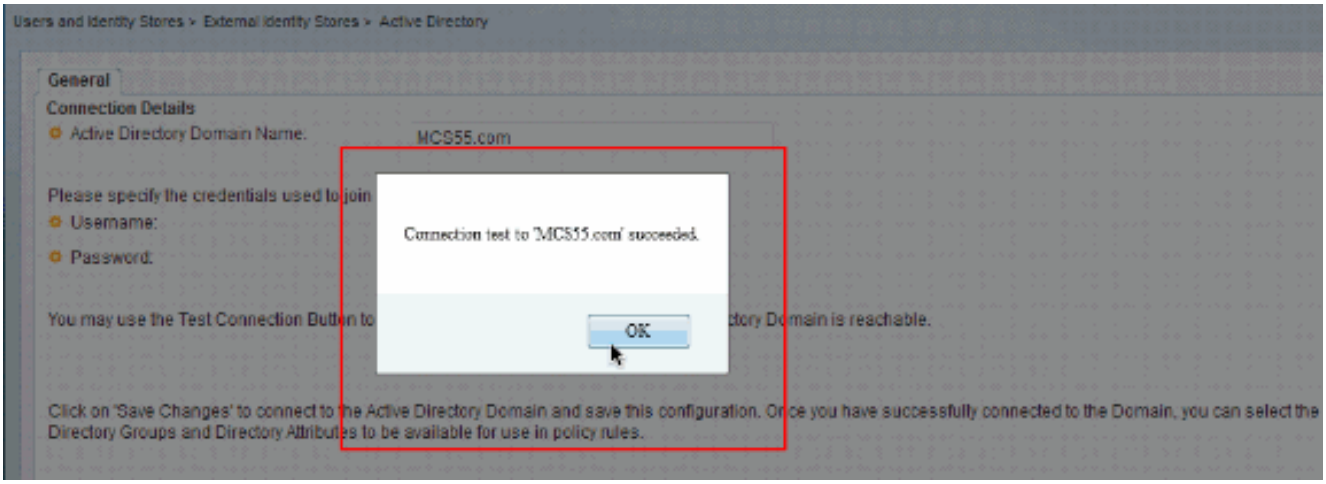
Выполните эти шаги для соединения ACS5.x с AD:

1. Выберите **Users и Identity Stores> External Identity Stores> Active Directory** и предоставьте Доменное имя, AD учетная запись (Имя пользователя) и его Пароль и щелкните **по Test Connection.Примечание:** AD учетная запись, требуемая для

доменного доступа в ACS, должна иметь любой из них:Добавьте рабочие станции к пользователю домена прямо в соответствующем домене.Создайте Компьютерные Объекты или Удалите Компьютерные разрешения Объектов на соответствующем компьютерном контейнере, где учетная запись машины ACS создана прежде, чем соединить машину ACS с доменом.**Примечание:** Cisco рекомендует, чтобы вы отключили политику локаута для учетной записи ACS и настроили AD инфраструктуру, чтобы передать предупреждения admin, если неправильный пароль используется для той учетной записи. Это вызвано тем, что при вводе неправильного пароля ACS не создает или модифицирует свою учетную запись машины, когда это необходимо, и поэтому возможно запретите все аутентификации.**Примечание:** Учетная запись Windows AD, которая соединяет ACS с AD доменом, может быть размещена в его собственное Подразделение (OU). Это находится в своем собственном OU или когда учетная запись создана или позже с ограничением, что название устройства должно совпасть с названием AD учетной
записи.

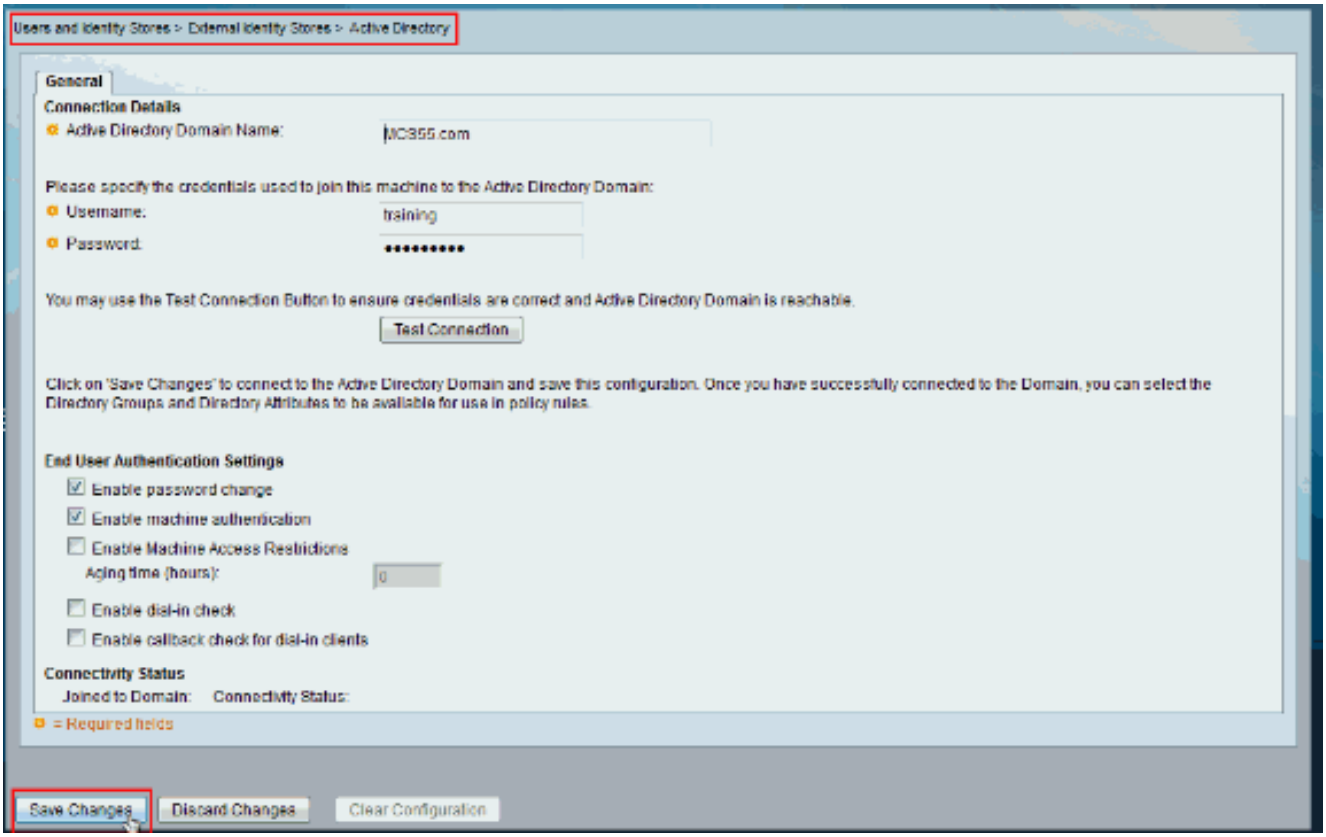


2. Этот снимок экрана показывает, что тестовое подключение к AD успешно. **Затем нажмите кнопку
ОК.**



Примечание: Когда существует медленный ответ от сервера при тестировании соединения ACS с AD доменом, на конфигурацию Centrify влияют и иногда разъединяют. Однако это хорошо работает с другими приложениями.

3. Нажмите **Save Changes** для ACS для присоединения к AD.



4. Как только ACS успешно присоединился к AD Домену, он показывает в статусе подключения.

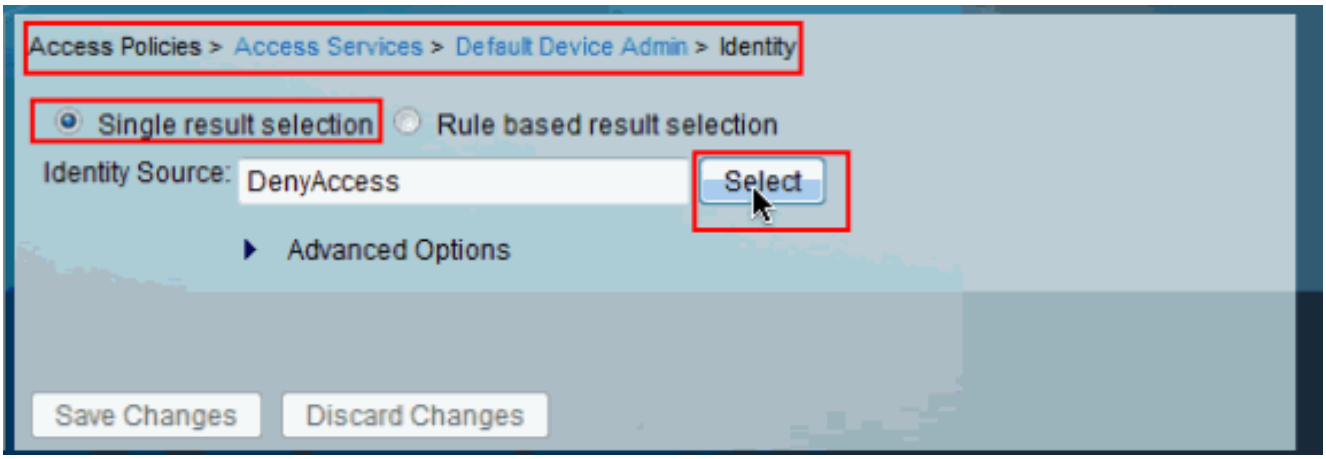
Примечание: При настройке AD идентификационного хранилища ACS также создает:Новый словарь для того хранилища с двумя атрибутами: ExternalGroups и другой атрибут для любого атрибута получены из страницы Directory Attributes.Новый атрибут, IdentityAccessRestricted. Можно вручную создать пользовательское условие для этого атрибута.Пользовательское условие для сопоставления группы от атрибута ExternalGroup; пользовательское название условия является AD1:ExternalGroups и

другим пользовательским условием для каждого атрибута, выбранного на странице Directory Attributes, например, AD1:cn.

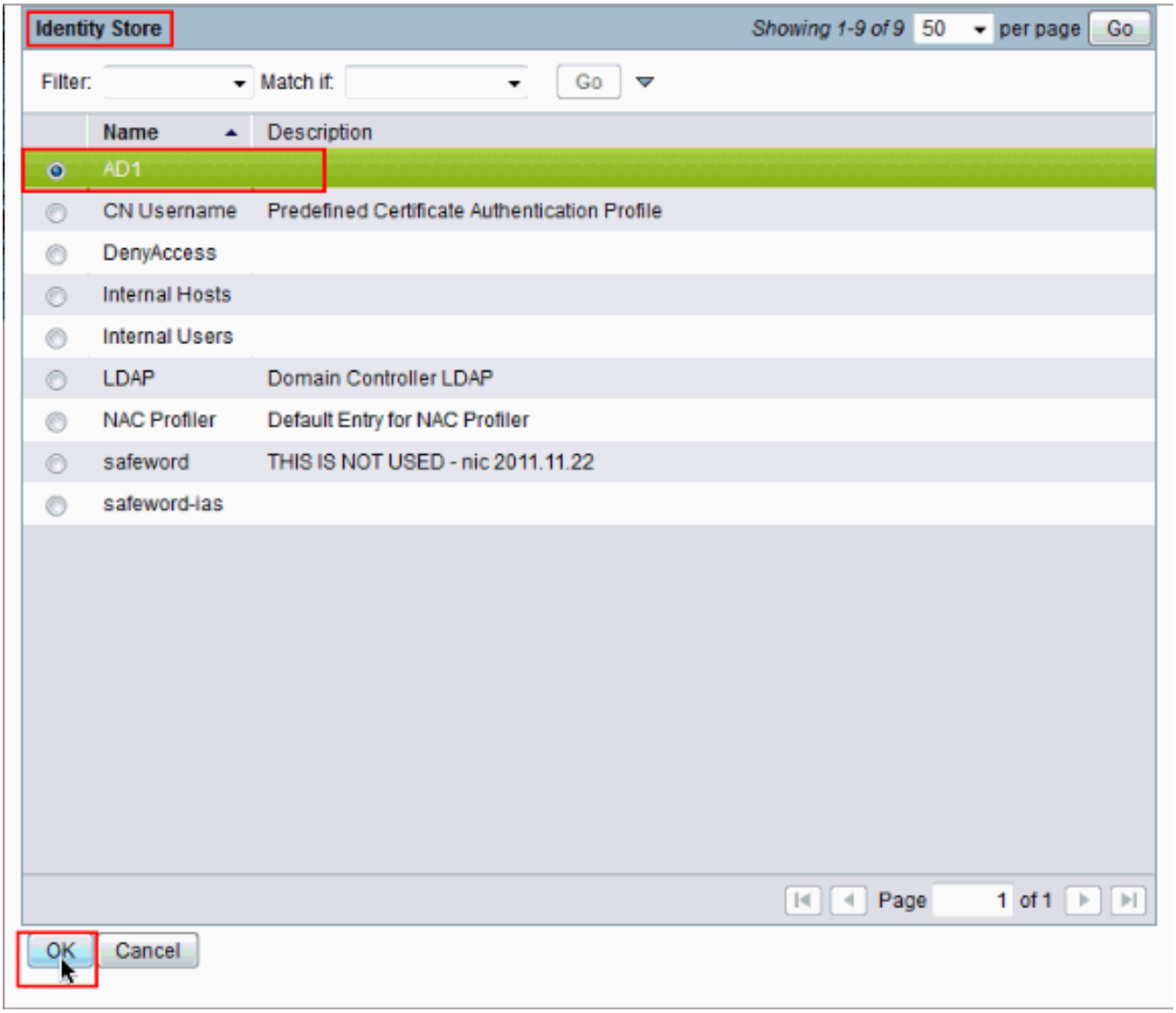
Настройте службу доступа

Выполните эти шаги для завершения конфигурации Службы доступа так, чтобы ACS мог использовать недавно настроенную AD Интеграцию.

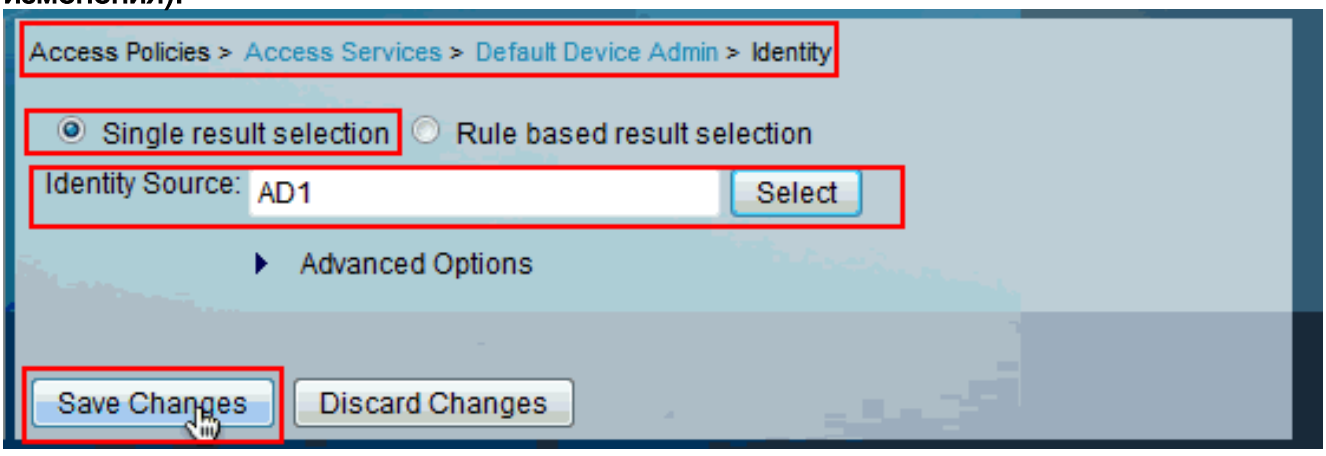
1. Выберите сервис из того, где вы хотели бы, чтобы пользователи аутентифицировались от AD, и щелкнули бы **по Identity**. Теперь нажмите **Select** рядом с полем Identity Source.



2. Выберите **AD1** и нажмите **OK**.



3. **Нажмите кнопку Save Changes (Сохранить изменения).**

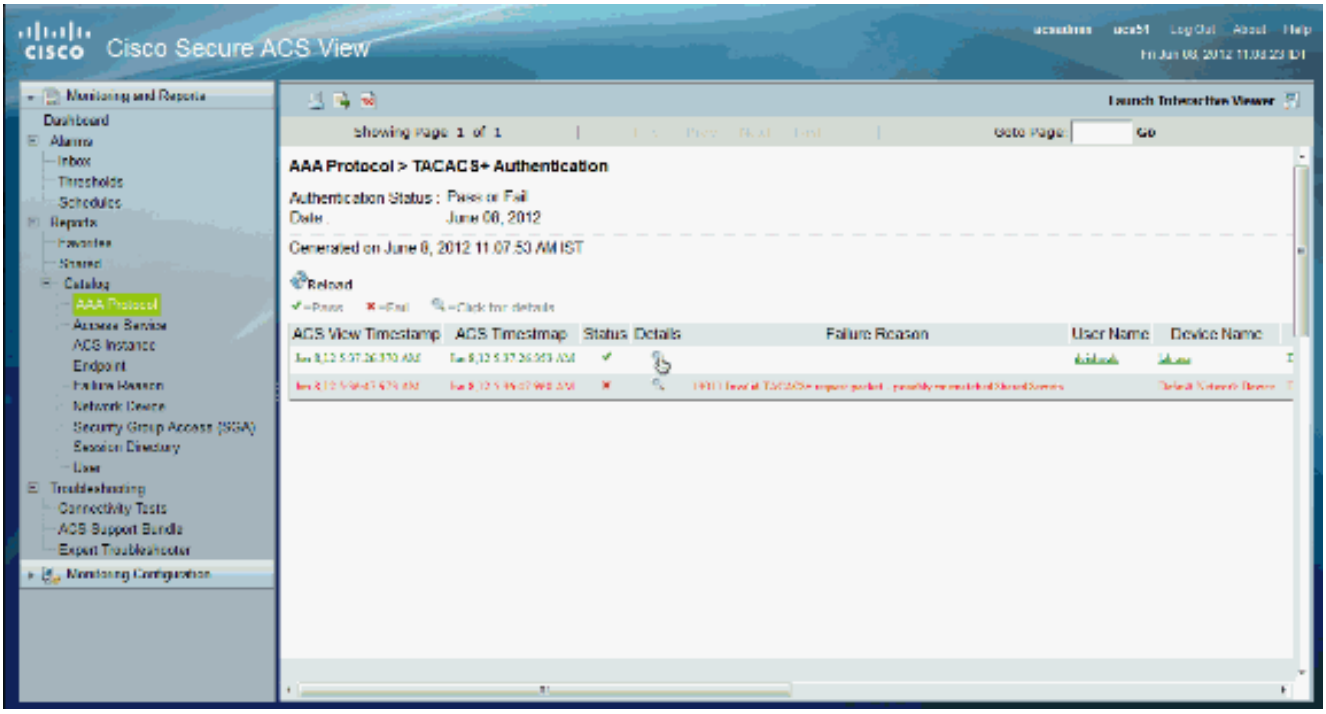


Проверка

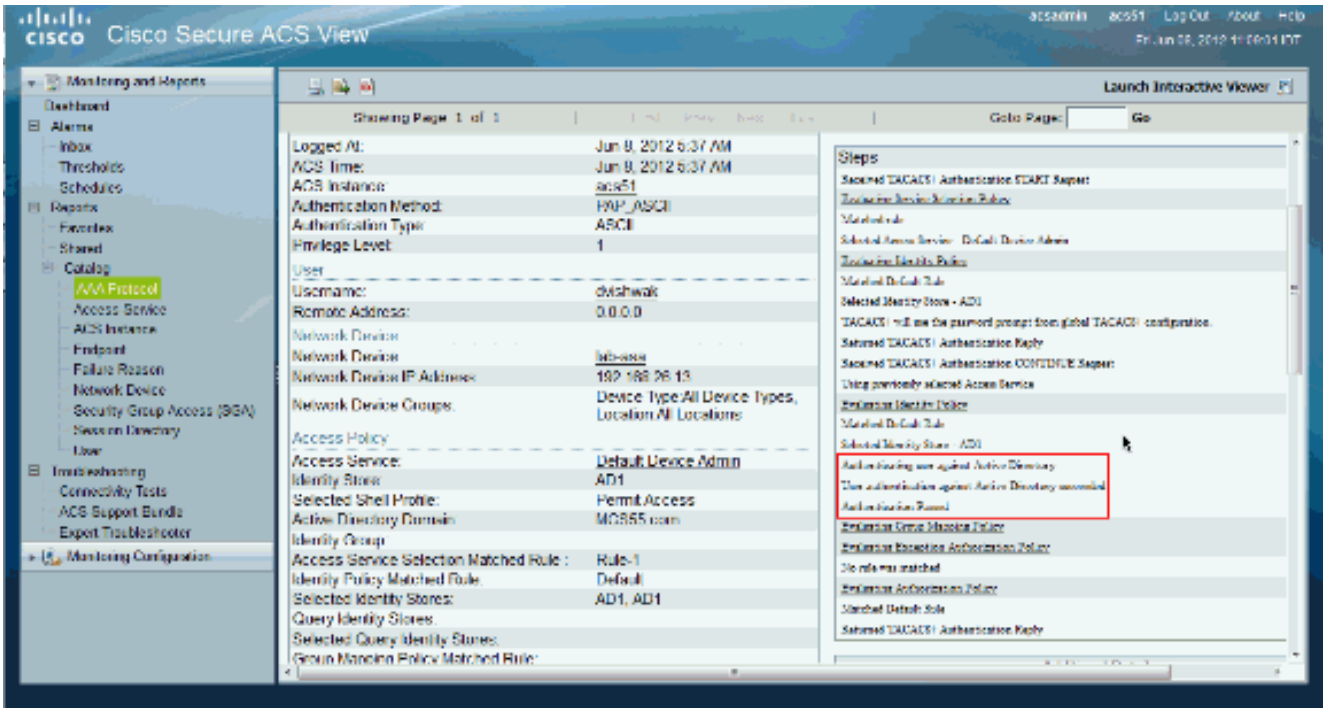
Для проверки AD аутентификации передайте запрос аутентификации от NAS с AD учетными данными. Гарантируйте, что NAS настроен на ACS, и запрос был бы обработан Службой доступа, настроенной в предыдущем разделе.

1. После успешной аутентификации от NAS входят в GUI ACS и выбирают **Monitoring and Reports> AAA Protocol> TACACS+Authentication**. Определите переданную

аутентификацию из списка и щелкните по символу **лупы** как показано.



2. Можно проверить от шагов, что ACS передал Запрос аутентификации к AD.



Дополнительные сведения

- Система управления доступом Cisco Secure Access Control System
- Cisco Systems – техническая поддержка и документация