NAC: Настройка LDAP Через SSL на Clean Access Manager (CAM)

Содержание

Введение

Этот документ описывает, как настроить Протокол LDAP через SSL на Clean Access Manager (CAM).

Предварительные условия

Требования

Эта конфигурация применима к версии 3.5 CAM и позже.

Используемые компоненты

Сведения в этом документе основываются на Чистой версии 4.1 Access Manager.

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

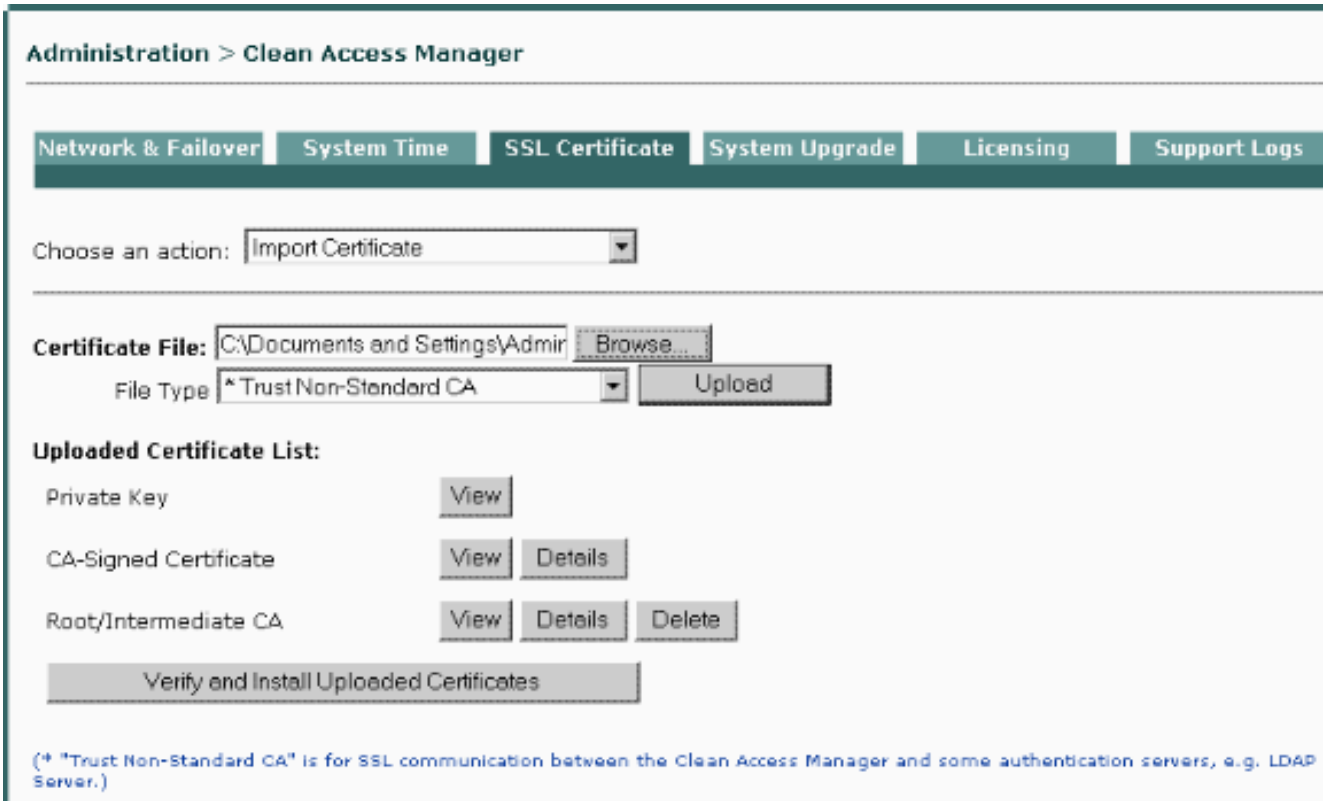
В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

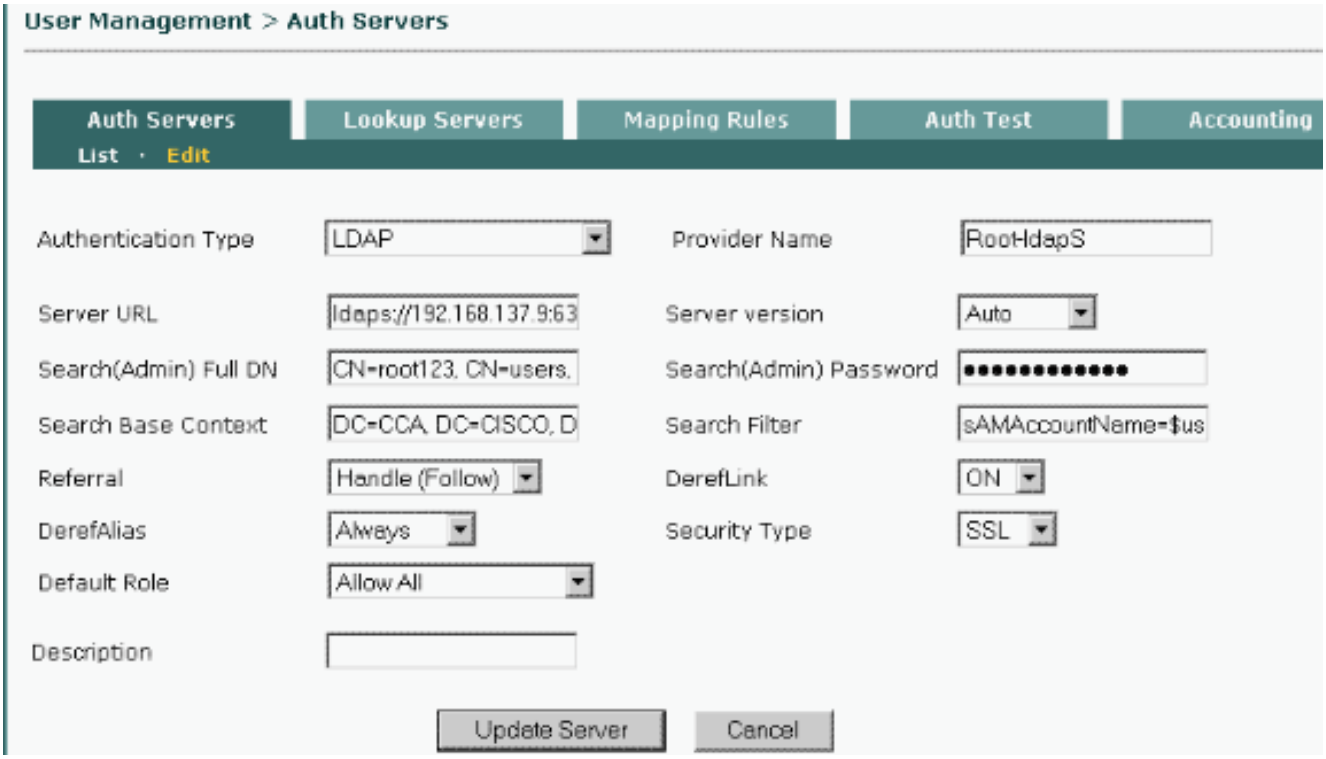
Шаги для Настройки LDAP через SSL на CAM

Выполните следующие действия:

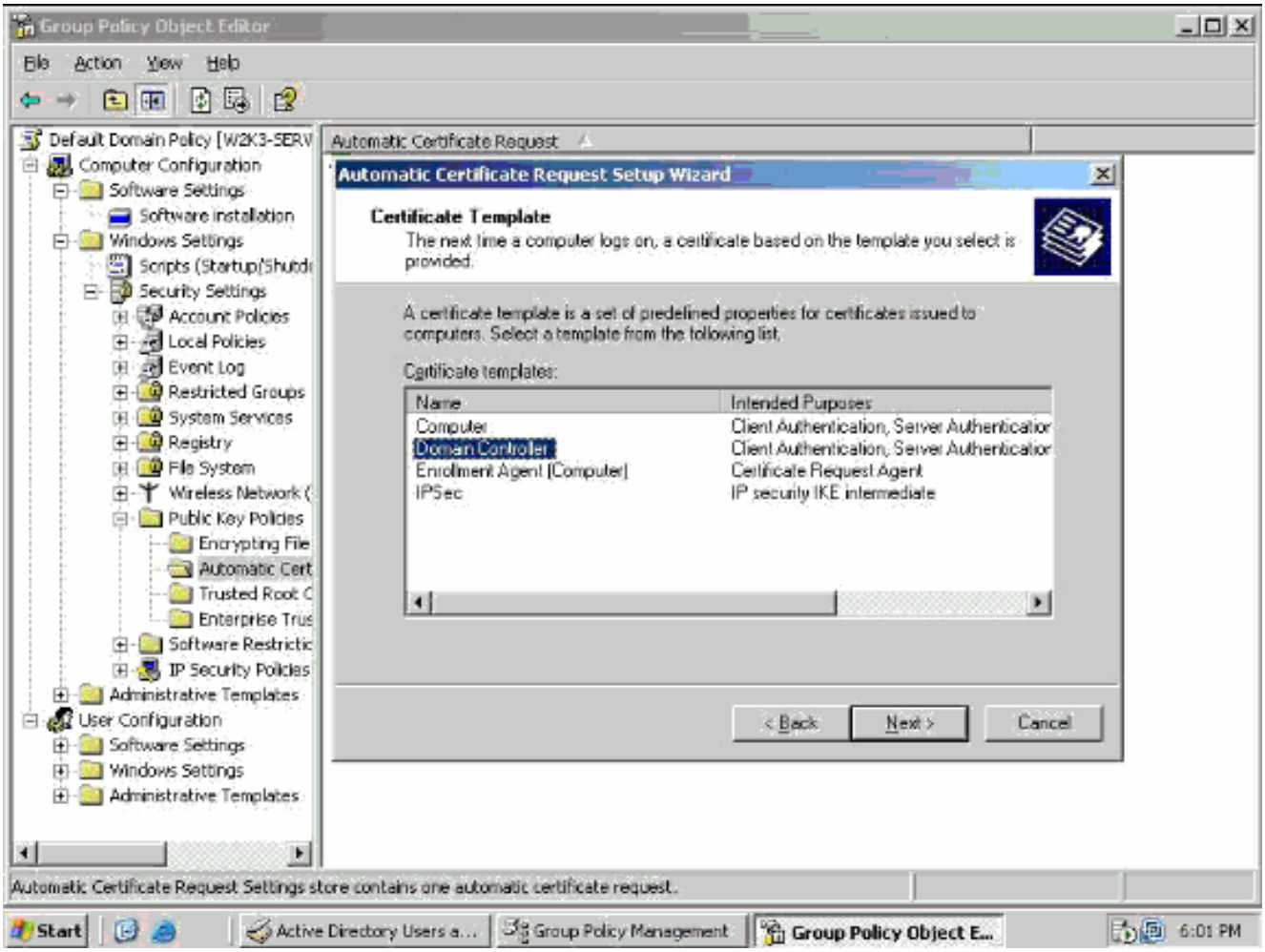
1. Получите корневой сертификат недоверяемого CA, который выполнил сертификат к Контроллеру домена и размещает его в ваш рабочий стол.Выберите **Administrator> CAM> сертификат SSL**, и затем просмотрите и загрузите Корневой сертификат CA как **Трастового Нестандартного CA.**



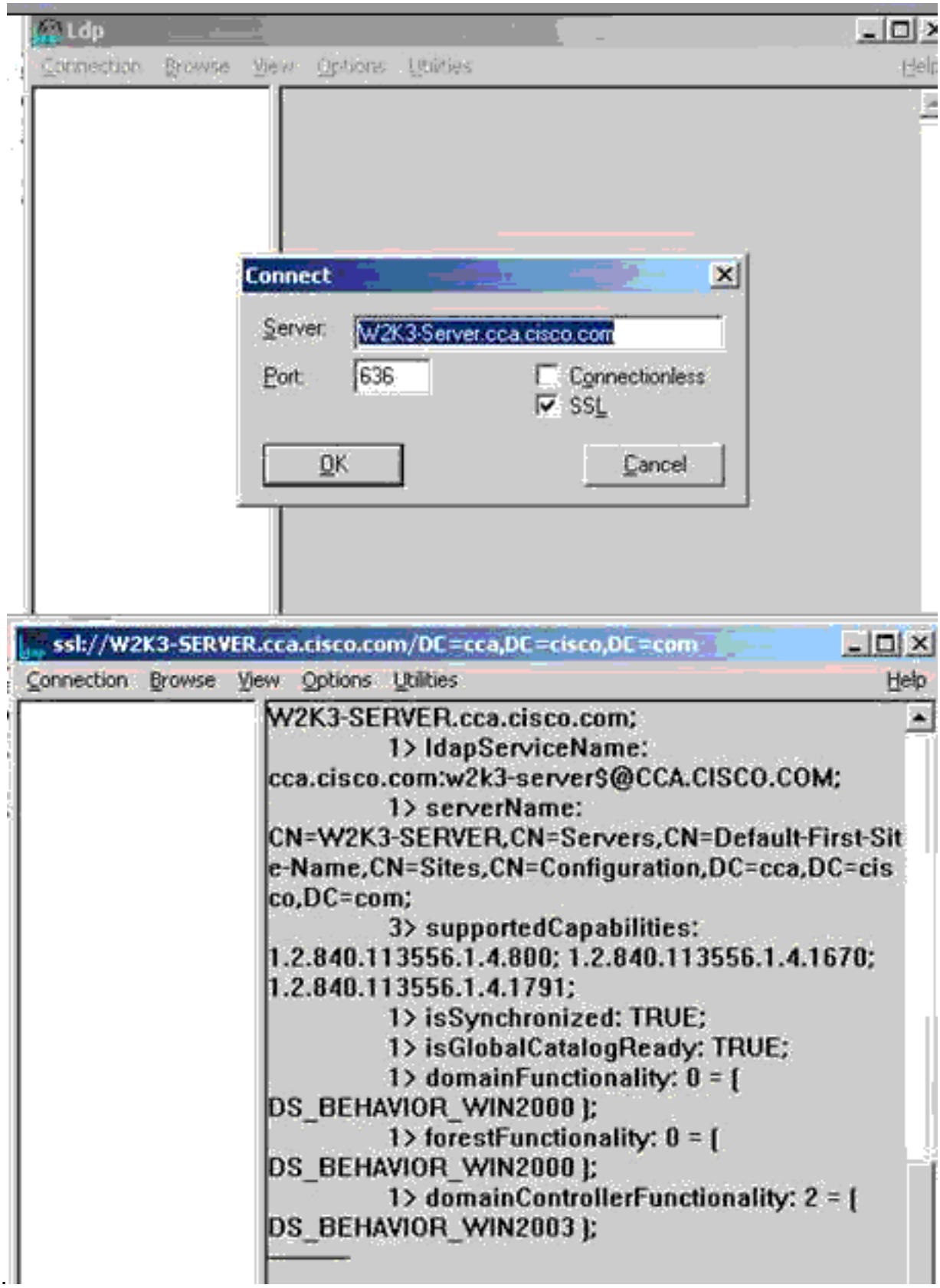
   Нажмите **Verify** и установите Корневой сертификат CA.
2. Настройте Сервер LDAP на CAM.Выберите **User Management> Auth Servers** и выберите **New**.Выберите **LDAP** в качестве Типа проверки подлинности.Выберите **ldaps://ip.address:636** в качестве URL Сервера.Выберите **SSL** в качестве типа безопасности.Выберите **Handle (Follow)!** как Рекомендация. Эта опция установлена для Среды Домена Разделения, например, Root и Дочерних доменов.Пользователь административной привилегии и пароль обязаны успешно связывать CAM (клиент ldap) к Серверу LDAP.



3. Получите сертификат на Контроллере домена (DC).При запросе сертификата на DC удостоверьтесь, что поместили CN как полное доменное имя Active Directory. Сертификат LDAP расположен в хранилище персонального сертификата локального компьютера. См. то, Как включить LDAP по SSL со сторонним центром сертификации для получения дополнительной информации.
4. Настройте контроллер домена для SSL.На вашем DC выберите **Start> All Programs> Administrative Tools> Active Directory Users и Computer**.В окне Active Directory Users and Computers щелкните правой кнопкой мыши на своем доменном имени и выберите **Properties**.В Доменном Диалоговом окне со свойствами выберите вкладку **Group Policy**.Выберите политику **Группы политик Домена по умолчанию** и затем нажмите **Edit**.Выберите **Computer Configuration> Windows Settings**.Выберите **Security Settings** и затем выберите **Public Key Policies**.Выберите **Automatic Certificate Request Settings**.Используйте мастера для добавления политики для Контроллеров домена как в данном
примере:

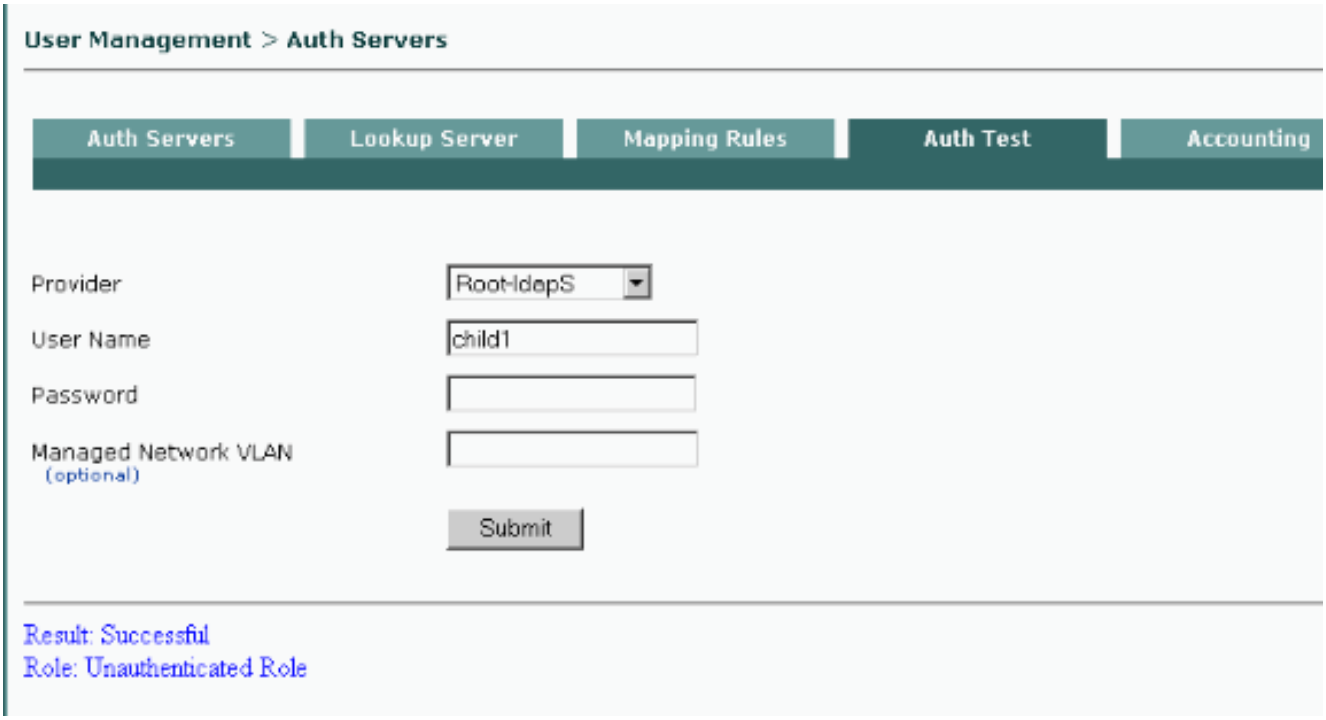


5. Проверьте контроллер домена для LDAP по SSL.На вашем DC выберите **Start> Run** и введите **ldp.exe**. Из Меню подключения нажмите **Connect** и заполните значения для сервера и порта. Это проверяет, что LDAP по SSL настроен правильно на



DC.

6. Выберите **вкладку User Management> Auth Servers> AUTH Test** для проверки конфигурации LDAP
   CAM.



Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

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