Телефон в Ижевске: +7 (3412) 72-11-00
Телефон в Москве: +7 (499) 277-1560
Сайт: www.directum.ru
E-mail: support@directum.ru

Инструкция по установке и настройке центра сертификации

Назначение документа

Для использования электронной подписи (ЭП) необходимо установить и настроить службу сертификации Active Directory. Службы сертификатов Active Directory можно использовать для создания одного или нескольких центров сертификации, которые будут получать запросы на сертификаты, проверять данные запросов, идентифицировать запрашивающую сторону, выдавать сертификаты, отзывать сертификаты и публиковать данные об отзывах сертификатов.

В документе описан порядок установки и пример настройки службы сертификации Active Directory и ее компонентов. Настраивайте службу сертификации Active Directory и ее компоненты с учетом специфики политики безопасности предприятия.

Перечень терминов и сокращений

Служба сертификации Active DIRECTORY

Служба для создания сертификатов открытых ключей и их управления, которые используются в системах безопасности программного обеспечения, где применяются технологии открытого ключа.

цифровой Сертификат

Выпущенный удостоверяющим центром электронный или печатный документ, подтверждающий принадлежность владельцу открытого ключа или каких-либо атрибутов.

Центр сертификации

Организация, которая выпускает сертификаты ключей электронной подписи.

Шаблон сертификатов

Набор правил и форматов для подачи заявок на цифровой сертификат, использования цифрового сертификата и управления им.

Установка и настройка службы сертификации Active Directory

1. Установите центр сертификации. Подробнее см. раздел по установке на Microsoft Windows Server 2008/2008 R2 или Microsoft Windows Server 2012/2012R2.
2. Настройте центр сертификации. Подробнее см. раздел по настройке на Microsoft Windows Server 2008/2008 R2 или Microsoft Windows Server 2012/2012 R2.
3. Зарегистрируйте сертификат центра сертификации на компьютерах с установленной клиентской частью системы DIRECTUM и серверах службы Workflow. Подробнее см. раздел «Установка сертификата центра сертификации».
4. При необходимости создайте и разверните шаблоны сертификатов. Подробнее см. разделы «Создание шаблона сертификата», «Добавление шаблона сертификата в центр сертификации».

Требования к оборудованию и программному обеспечению для установки службы сертификации Active Directory см. в документации Microsoft.

Время установки центра сертификации 30-60 мин.

После окончания срока действия центра сертификации все сертификаты нужно выдавать заново.

Центр сертификации на Microsoft Windows Server 2008/2008 R2

Установка центра сертификации

1. Войдите в Windows Server 2008/2008 R2 под именем пользователя, обладающего правами доменного администратора.
2. В меню **Пуск** последовательно выберите пункты **Все программы**, **Администрирование**, **Диспетчер сервера**.
3. В окне «Диспетчер сервера» в контекстном меню **Роли** выберите пункт **Добавить роли**.
4. В окне «Выбор ролей сервера» установите флажок **служба сертификации Active Directory**. Нажмите на кнопку **Далее>**.
5. В окне «Знакомство со службами сертификации Active Directory» нажмите на кнопку **Далее>**.
6. В окне «Выбор служб ролей» установите флажок **Центр сертификации** и **Служба регистрации в центре сертификации через Интернет** и нажмите на кнопку **Далее>**. Откроется сообщение: «Добавить службы ролей и компоненты, необходимые для компоненты «Служба регистрации в центре сертификации через Интернет?». Нажмите на кнопку **Добавить требуемые службы роли**.
7. Нажмите на кнопку **Далее>**.
8. В окне «Задание типа установки» выберите тип установки **Предприятие** и нажмите на кнопку **Далее>**.
9. В окне «Задание типа ЦС» выберите тип центра сертификации **Корневой ЦС** и нажмите на кнопку **Далее>**.

10. В окне «Установка закрытого ключа» выберите **Создать новый закрытый ключ** и нажмите на кнопку **Далее>**.
11. В окне «Настройка шифрования для ЦС» рекомендуется оставить все значения по умолчанию. Нажмите на кнопку **Далее>**.
12. В окне «Задание имени ЦС» в поле **Общее имя** укажите имя ЦС, которое будет отображаться во время создания запроса сертификата и нажмите на кнопку **Далее>**.
13. В окне «Установить срок действия» выберите срок действия сертификата, созданного для данного ЦС. Нажмите на кнопку **Далее>**.
14. В окне «Настройка базы данных сертификатов» оставьте все значения по умолчанию. Нажмите на кнопку **Далее>**.
15. В окне «Веб-сервер (IIS)» нажмите на кнопку **Далее>**.
16. В окне «Выбор служб ролей» оставьте все значения по умолчанию. Нажмите на кнопку **Далее>**.
17. В окне «Подтверждение» нажмите на кнопку **Установить**.
18. В окне «Результат установки» нажмите на кнопку **Закрыть**.

Настройка центра сертификации

Настройка центра сертификации состоит из нескольких этапов:

- настройка выдачи сертификатов
- настройка прав доступа к службам сертификации
- настройка доступа к веб-консоли служб сертификатов через SSL канал

Настройка выдачи сертификатов:

1. В меню **Пуск** последовательно выберите пункты **Программы**, **Администрирование**, **Центр сертификации**. Откроется консоль **Центр сертификации**.
2. Выберите установленный центр сертификации.
3. В меню **Действие** выберите пункт **Свойства**. В открывшемся окне:
   a) Выберите закладку «Модуль политики» и нажмите на кнопку **Свойства...**.
   b) Установите переключатель **Следовать параметрам, установленным в шаблоне сертификата, если они применимы, иначе автоматически выдавать сертификат**.
   c) Нажмите на кнопку **ОК**.

Настройка прав доступа к службам сертификации

1. В меню **Пуск** последовательно выберите пункты **Программы**, **Администрирование**, **Диспетчер служб IIS**. Откроется консоль **Диспетчер служб IIS**.
2. В дереве консоли IIS разверните **Веб-узел по умолчанию** и выделите **CertSrv**.
3. Нажмите на кнопку **Features View** и в режиме просмотра возможностей выберите **Authentication**.
4. В разделе «Проверка подлинности» проверьте, что включена только **Проверка подлинности Windows**. Для этого на панели **Действия** установите значение **Включить**.
5. В дереве консоли IIS выберите **CertSrv** и в контекстном меню выберите пункт **Редактировать разрешения**.

6. В окне «Свойства: CertSrv» на закладке «Безопасность» укажите пользователей и группы, которым будет обеспечен доступ к веб-консоли служб сертификатов.
7. Нажмите на кнопку **ОК**.

Настройка доступа к веб-консоли служб сертификатов через SSL канал

1. В меню **Пуск** последовательно выберите пункты **Программы**, **Администрирование**, **Диспетчер служб IIS**. Откроется консоль **Диспетчер служб IIS**.
2. В разделе «Подключения» выберите имя компьютера, на котором установлена служба сертификации.
3. Нажмите на кнопку **Сертификаты сервера**.
4. В окне «Сертификаты сервера» в меню **Действия** выберите пункт **Создать запрос сертификата**.
5. В окне «Свойства различающегося имени» заполните поля. В поле **Полное имя** введите имя сервера или имя центра сертификации. Нажмите на кнопку **Далее>**.
6. В окне «Свойства поставщика служб шифрования» рекомендуется оставить значения по умолчанию. Нажмите на кнопку **Далее>**.
7. В окне «Имя файла» выберите место хранения текста запроса получения сертификата и укажите имя файла запроса сертификата. Будет создан файл запроса сертификата. Нажмите на кнопку **Готово**.
8. Получите сертификат веб-сервера:
   - на сервере центра сертификации откройте сайт http:\\localhost\certsrv;
   - на странице «Добро пожаловать» выберите **Запрос сертификата**;
   - на странице «Запросить сертификат» выберите **Расширенный запрос сертификата**;
   - на странице «Расширенный запрос сертификата» выберите **Выдать запрос, используя base-64 шифрованный файл PKCS #10, или выдать запрос обновления, используя base-64 шифрованный файл PKCS #7**;
   - на странице «Выдача запроса на сертификат или на обновление сертификата», в поле **Сохраненный запрос** скопируйте текст файла запроса сертификата, созданного на шаге 8. Поле **Дополнительные атрибуты** оставьте пустым;
   - в поле **Шаблон сертификата** выберите значение **веб-сервер**. При этом пользователь должен иметь соответствующее разрешение на использование сертификата с данным шаблоном;
   - нажмите на кнопку **Выдать**;
   - на странице «Сертификат выдан» нажмите на кнопку **Загрузить сертификат**;
   - сохраните сертификат.
9. В меню **Пуск** последовательно выберите пункты **Программы**, **Администрирование**, **Диспетчер служб IIS**. Откроется консоль **Диспетчер служб IIS**.
10. В окне «Диспетчер служб IIS» на начальной странице нажмите на кнопку **Сертификаты сервера**.
11. В окне «Сертификаты сервера» в меню **Действия** выберите пункт **Запрос установки сертификатов**.
12. В окне «Ответ центра сертификации» выберите сертификат, который был создан на шаге 8 и напишите имя, которое будет отображаться в поле **Имя списка сертификатов сервера**. Нажмите на кнопку **ОК**.

Примечание

В поле **Имя списка сертификатов сервера** рекомендуется указывать имя сервера или имя центра сертификации.

13. В окне «Диспетчер служб IIS» выберите имя сервера и раздел «Узлы».
14. В дереве консоли IIS в контекстном меню **Default Web Site** выберите пункт **Изменить привязки**.
15. В окне «Привязки сайта» нажмите на кнопку **Добавить**.
16. В окне «Добавление привязки сайта» выберите тип **https** и выберите сертификат SSL из списка, который был установлен на шаге 12. Нажмите на кнопку **OK**.
17. В окне «Привязки сайта» нажмите на кнопку **Закрыть**.
18. В окне «Диспетчер служб IIS» выберите имя сервера и раздел «Узлы».
19. В дереве консоли IIS выберите **Default Web Site**. В контекстном меню **CertSrv** выберите пункт **Свойства**.
20. В окне «Начальная страница»/«CertSrv» нажмите на кнопку **Параметры SSL**.
21. В окне «Параметры SSL» установите флажок **Требовать SSL**.
22. Нажмите на кнопку **Применить**.

Центр сертификации на Microsoft Windows Server 2012/2012 R2

Установка центра сертификации

1. Войдите в Windows Server 2012/2012 R2 под именем пользователя, обладающего правами доменного администратора.
2. Запустите **Диспетчер Серверов**.
3. В окне «Диспетчер серверов» в меню **Управление** выберите пункт **Добавить роли и компоненты**. Откроется окно «Мастер добавления ролей и компонент».
4. В окне «Перед началом работы» нажмите на кнопку **Далее>**.
5. В окне «Выбор типа установки» установите переключатель **Установка ролей или компонентов** и нажмите на кнопку **Далее>**.
6. В окне «Выбор целевого сервера», установите переключатель **Выберите сервер из пула серверов** выберите текущий сервер из списка. Нажмите на кнопку **Далее>**.
7. В окне «Выбор ролей сервера» выберите **Службы сертификатов Active Directory**.
8. В окне «Добавить компоненты, необходимые для Службы сертификатов Active Directory?» нажмите на кнопку **Добавить компоненты**. Нажмите на кнопку **Далее>**.
9. В окне «Выбор компонентов» нажмите на кнопку **Далее>**.
10. В окне «Службы сертификатов Active Directory» ознакомьтесь с информацией и нажмите на кнопку **Далее>**.
11. В окне «Выбор служб ролей» установите флажки **Центр сертификации** и **Служба регистрации в центре сертификации через интернет**. Нажмите на кнопку **Далее>**.
12. В окне «Добавить компоненты, необходимые для Служба регистрации в центре сертификации через Интернет?» нажмите на кнопку **Добавить компоненты**. Нажмите на кнопку **Далее>**.

13. В окне «Подтверждение» нажмите на кнопку **Установить**. Откроется окно «Ход установки».
14. По окончании установки нажмите ссылку **Настроить службы сертификатов Active Directory на конечном сервере**.
15. В окне «Конфигурация службы сертификатов Active Directory» в разделе **Учетные данные** укажите учетные данные доменного администратора. Нажмите на кнопку **Далее>**.
16. В окне «Службы ролей» установите флажок **Центр сертификации** и **Служба регистрации в центре сертификации через интернет**. Нажмите кнопку **Далее>**.
17. В окне «Вариант установки» выберите **ЦС Предприятия**. Нажмите кнопку **Далее>**.
18. В окне «Тип ЦС» выберите тип центра сертификации **Корневой ЦС**. Нажмите на кнопку **Далее>**.
19. В окне «Закрытый ключ» выберите **Создать новый закрытый ключ**. Нажмите на кнопку **Далее>**.
20. В окне «Шифрование для ЦС» рекомендуется оставить все значения по умолчанию. Нажмите на кнопку **Далее>**.
21. В окне «Имя ЦС» в поле **Общее имя для этого ЦС** укажите имя ЦС, которое будет отображаться во время создания запроса сертификата. Нажмите на кнопку **Далее>**.
22. В окне «Срок действия» выберите срок действия сертификата, созданного для данного ЦС. Нажмите на кнопку **Далее>**.
23. В окне «База данных ЦС» оставьте все значения по умолчанию. Нажмите на кнопку **Далее>**.
24. В окне «Подтверждение» нажмите на кнопку **Настроить**. Откроется окно «Ход выполнения».
25. По завершении настройки откроется окно «Результаты». Ознакомьтесь с результатами и закройте окно.

Настройка центра сертификации

Порядок настройки центра сертификации на Microsoft Windows Server 2012/2012R2 аналогичен Microsoft Windows Server 2008/2008R2. Подробнее см. раздел «Настройка центра сертификации» для Microsoft Windows Server 2008/2008R2.

Установка сертификата центра сертификации

Для создания доверия к сертификатам пользователей, выданных центром сертификации, необходимо зарегистрировать сертификат центра сертификации на компьютерах пользователей системы.

Чтобы установить сертификат центра сертификации:

1. В сетевом окружении обратитесь к ресурсу \\<Сервер>\CertEnroll, где <Сервер> – это имя компьютера, на котором установлен центр сертификации.
2. Дважды щелкните мышью на файле с расширением «.CRT», например, «study1.domain1.comp.npo_NameCA.crt».
3. В окне «Сертификат» на закладке «Общие» нажмите на кнопку **Установить сертификат...**.

4. В окне «Мастер импорта сертификатов»:
   - нажмите на кнопку **Далее>**;
   - установите переключатель **Поместить все сертификаты в следующее хранилище**;
   - нажмите на кнопку **Обзор** и выберите хранилище сертификатов **Доверенные корневые центры сертификации**;
   - нажмите на кнопку **Далее>**;
   - нажмите на кнопку **Готово**;
   - нажмите на кнопку **ОК**;
   - в окне «Сертификат» нажмите на кнопку **ОК**.

Сертификат центра сертификации должны быть установлены на каждом компьютере с установленной клиентской частью системы DIRECTUM и серверах службы Workflow.

Шаблоны сертификатов центра сертификации Active Directory

Использование шаблонов сертификатов производится с учетом специфики политики безопасности Вашего предприятия. Настройка шаблонов является необязательной.

Шаблоны сертификатов упрощают задачу администрирования центра сертификации, позволяя администраторам выдавать сертификаты, предварительно настроенные для выбранных задач. Оснастка «Шаблоны сертификатов» устанавливается при установке центра сертификации и позволяет администратору выполнять задачи:

- просматривать свойства каждого шаблона сертификата;
- копировать и изменять шаблоны сертификатов;
- указывать пользователей и компьютеры, которые могут считывать шаблоны и регистрировать сертификаты;
- выполнять другие задачи администрирования, относящиеся к шаблонам сертификатов.

Примечание

Сертификаты, основанные на шаблонах сертификатов, могут выдаваться только центрами сертификации с типом «Предприятие».

Создание шаблона сертификата

Чтобы создать шаблон сертификата в Windows Server 2008/2008 R2:

1. В меню **Пуск** последовательно выберите пункты **Все программы**, **Администрирование**, **Панель управления**.
2. В окне «Диспетчер сервера» в меню **Роли** последовательно выберите пункты **Службы сертификации Active Directory**, **Шаблоны сертификатов**.
3. В окне «Шаблоны сертификатов**»** выберите пункт контекстного меню **Скопировать шаблон** шаблона «Пользователь».
4. В появившемся окне выберите версию шаблона: «Windows Server 2008/2008 R2, Enterprise Edition».

Примечание

Центры сертификации компании Microsoft поддерживают три типа шаблонов сертификатов: версия 1, версия 2 и версия 3. Подробнее см. в документации Microsoft. При переходе по ссылке откроется окно загрузки файла.

5. В окне «Свойства нового шаблона» на закладке «Общие»:
   - заполните поле **Отображаемое имя шаблона**. Отображается в оснастке **Шаблоны сертификатов**, а также во всех других компонентах используемых для выдачи сертификатов;
   - заполните поле **Имя шаблона**. Отображается только в свойствах самого сертификата;
   - задайте период действия шаблона в поле **Период действия**;
   - задайте период обновления шаблона сертификата в поле **Период обновления**;
   - установите флажок **Опубликовать в Active Directory**.
6. На закладке «Обработка запроса»:
   - в выпадающем списке **Цель сертификата** выберите значение **Подпись и шифрование**;
   - установите флажок **Включить симметричные алгоритмы, разрешенные субъектом**;
   - установите флажок **Разрешить экспортировать закрытый ключ**;
   - установите переключатель **Подавать заявку для субъекта, не требуя ввода данных**.
7. На закладке «Шифрование» заполните поля:
   - в выпадающем списке **Имя алгоритма выберите** значение **RSA**;
   - в поле **Минимальный размер ключа** укажите значение **512**;
   - установите переключатель **В запросах могут использоваться любые поставщики, доступные на компьютерах пользователя**;
   - в поле **Алгоритм хеширования** выберите значение **SHA1**.
8. На закладке «Имя субъекта» установите переключатель **Предоставляется в запросе**.
9. На закладке «Безопасность»:
   - для группы пользователей «Прошедшие проверки» установите флажок **Чтение**;
   - для группы пользователей «Administrator» установите флажки **Чтение**, **Запись**, **Заявка**;
   - для группы пользователей «Domain Admins» установите флажки **Чтение**, **Запись**, **Заявка**;
   - для группы пользователей «Domain Users» установите флажок **Заявка**;
   - для группы пользователей «Enterprise Admins» установите флажки **Чтение**, **Запись**, **Заявка**.
10. Нажмите на кнопку **ОК**.

Чтобы создать шаблон сертификата в Windows Server 2012:

1. В меню **Пуск** последовательно выберите пункты **Администрирование**, **Центр сертификации**.
2. В окне «Центр сертификации» выберите созданный центр сертификации в папке **Шаблоны сертификатов.** Выберите пункт контекстного меню **Управление**.

3. В окне «Консоль шаблонов сертификатов» выберите пункт контекстного меню **Скопировать шаблон** для шаблона «Пользователь».
4. В окне «Свойства нового шаблона» на закладке «Совместимость»:
   - в поле **Центр сертификации** укажите значение **Windows Server 2008 R2**;
   - в поле **Сертификат получателя** укажите значение **Windows 7 / Server 2008 R2**;
   - нажмите на кнопку **ОК**.
5. На закладке «Общие»:
   - заполните поле **Отображаемое имя шаблона**. Отображается в оснастке **Шаблоны сертификатов**, а также во всех других компонентах используемых для выдачи сертификатов;
   - заполните поле **Имя шаблона**. Отображается только в свойствах самого сертификата;
   - задайте период действия шаблона в поле **Период действия**;
   - задайте период обновления шаблона сертификата в поле **Период обновления**;
   - установите флажок **Опубликовать в Active Directory**.
6. На закладке «Обработка запроса»:
   - в выпадающем списке **Цель сертификата** выберите значение **Подпись и шифрование**;
   - установите флажок **Включить симметричные алгоритмы, разрешенные субъектом**;
   - установите флажок **Разрешить экспортировать закрытый ключ**;
   - установите переключатель **Подавать заявку для субъекта, не требуя ввода данных**.
7. На закладке «Шифрование» заполните поля:
   - в выпадающем списке **Категория поставщика** выберите **Поставщик хранилища ключей**;
   - в выпадающем списке **Имя алгоритма выберите** значение **RSA**;
   - в поле **Минимальный размер ключа** укажите значение **512**;
   - установите переключатель **В запросах могут использоваться любые поставщики, доступные на компьютерах пользователя**;
   - в поле **Хэш запроса** выберите значение **SHA1**.
8. На закладке «Имя субъекта» установите переключатель **Предоставляется в запросе**.
9. На закладке «Безопасность»:
   - для группы пользователей «Прошедшие проверки» установите флажок **Чтение**;
   - для группы пользователей «Administrator» установите флажки **Чтение, Запись, Заявка**;
   - для группы пользователей «Domain Admins» установите флажки **Чтение, Запись, Заявка**;
   - для группы пользователей «Domain Users» установите флажок **Заявка**;
   - для группы пользователей «Enterprise Admins» установите флажки **Чтение, Запись, Заявка**.
10. Нажмите на кнопку **ОК**.

Добавление шаблона сертификата в центр сертификации

При создании центра сертификации предприятия шаблоны сертификатов хранятся в доменных службах Active Directory. Их можно сделать доступными для всех центров сертификации предприятий в лесу доменов. Это упрощает репликацию, управление безопасностью и обновление шаблонов сертификатов при обновлении центра сертификации.

Примечание

Для развертывания шаблонов сертификатов группа администраторов корневого домена иметь полный доступ ко всем шаблонам сертификатов.

Шаблоны сертификатов автоматически реплицируются на все контроллеры домена в предприятии после создания. Репликация шаблонов занимает около восьми часов, поэтому создайте шаблон сертификата и завершите его репликацию до выдачи клиентам сертификатов, основанных на этом шаблоне. Настройка шаблонов и использование сертификатов до завершения репликации может иметь нежелательные последствия.

Чтобы центр сертификации выпускал сертификаты на основе разработанного шаблона сертификата, данный шаблон должен быть зарегистрирован в центре сертификации сразу после настройки. Подробнее см. документацию Microsoft.