

Инструкция по дополнительной настройке модуля синхронизации

ALD Pro

Exported on 09/19/2023

Table of Contents

1	Особенности работы Модуля синхронизации	4
2	Исходные настройки.....	5
2.1	Выгрузка сертификатов для контроллера домена MS AD.....	5
2.2	Выгрузка сертификатов для контроллера домена ALD Pro	10
3	Настройка синхронизации паролей AD → ALD	12
3.1	Развертывание	12
3.1.1	Уровни логирования	15
4	Синхронизация паролей ALD Pro → AD	16
4.1	Получение открытого ключа	16
4.2	Синхронизация паролей.....	16

В виду предотвращения конфликтных ситуаций при миграции и синхронизации данных из MS AD используется синхронная модель поведения синхронизации данных. В качестве ведущего сервера обработки информации выбран главный сервер в кластере серверов ALD Pro.

1 Особенности работы Модуля синхронизации

1. Нельзя производить переименование подразделений, добавленных в Сопоставление подразделений. Если возникла такая необходимость, корректно будет удалить сопоставление, произвести переименование и создать новое сопоставление подразделений.
2. Нельзя создавать сопоставления подразделений для дочерних подразделений подразделения, уже участвующего в синхронизации.
3. Атрибуты по умолчанию и соответствующие им сопоставления ограничены перечнем обязательных атрибутов для объектов ALD Pro
 - Пользователи: Логин, Пароль, Фамилия, Имя, Подразделение
 - Группы пользователей: Название группы, Подразделение
 - Подразделения: Наименование подразделения, Родительское подразделение Однако не все эти атрибуты явно указаны на карточке Атрибуты AD, Атрибуты ALD, так как их синхронизация происходит внутренними процессами Модуля синхронизации. Добавляя эти атрибуты в явном виде в Карте сопоставления вы рискуете нарушить логику работы Модуля синхронизации
4. Наименование подразделений, Наименования групп, логины пользователей не должны содержать специальных символов, за исключением ".", "-", "_".
5. Модуль синхронизации может быть установлен при первичной установке или в процессе обновления контроллера домена. Ограничением настоящей версии является установка модуля синхронизации только на первый контроллер домена. В случае отключения первого контроллера домена, синхронизация новых данных, добавленных после отключения первого контроллера домена, выполняться не будет. Ранее синхронизированные данные сохраняются и будут реплицироваться между контроллерами домена, для которых созданы соглашения о репликации.
6. Для успешной синхронизации необходимо учетную запись администратора, которая используется для подключения к контроллеру домена, добавить в группу admins.

2 Исходные настройки

Предполагается, что на момент настройки модуля синхронизации у нас имеются:

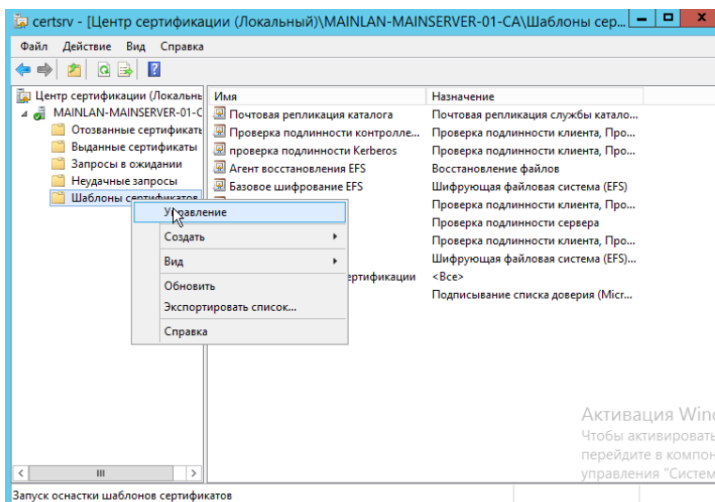
- Настроенный контроллер домена MS AD;
- Настроенный контроллер домена ALD Pro;
- Для сетей, в которых находятся контроллеры домена Microsoft AD и ALD Pro, настроено перенаправление DNS зон;
- В домене MS AD поднят центр сертификации и выдан сертификат для доступа по LDAPs (см. [Выгрузка сертификатов для контроллеров домена MS AD¹](#));
- Для учетной записи AD, под которой идет подключение модуля синхронизации к контроллерам домена AD, необходимо выдать права на контейнер "Deleted Object" через powershell:

```
//для выдачи прав на контейнер запускаем powershell от имени администратора
dscls "CN=Deleted Objects,DC=winad,DC=lan" /takeownership
dscls "CN=Deleted Objects,DC=winad,DC=lan" /g winad\aldagent:LCR
```

2.1 Выгрузка сертификатов для контроллера домена MS AD

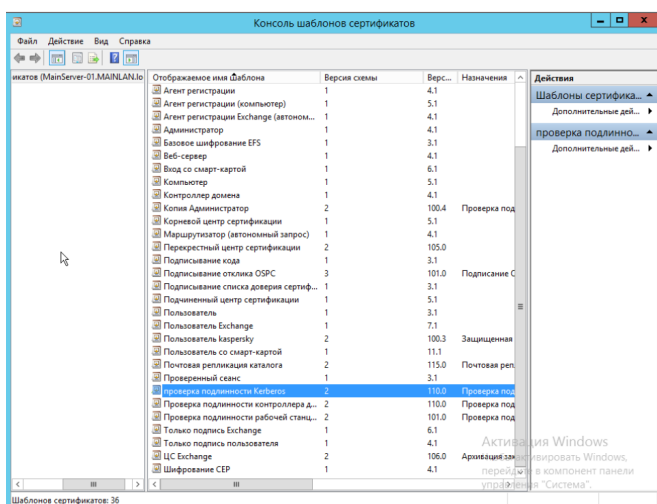
Для выгрузки сертификатов необходимо, чтобы в домене был настроен **Центр Сертификации**.

Запустить **Центр Сертификации** -> **Шаблоны Сертификатов** -> **Управление** на сервере с ролью **Центр Сертификации**:



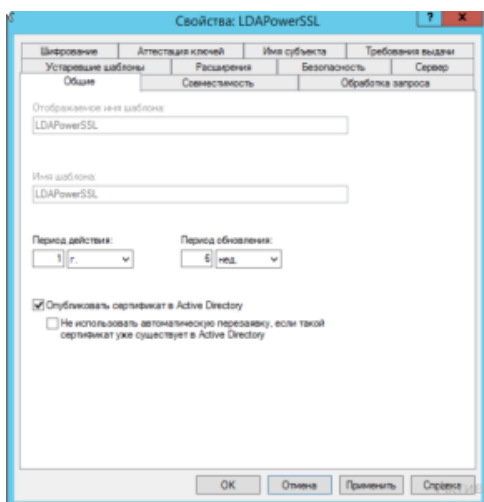
Создать копию шаблона **Проверка подлинности Kerberos**, выбрав пункт **Скопировать шаблон** контекстного меню:

¹ http://wiki.doc.aldpro-team.astralinux.ru/ad/help/api/instrukcii/instrukciya-po-dopolnitelnoj-nastrojke-syncer/#cert_ms_ad



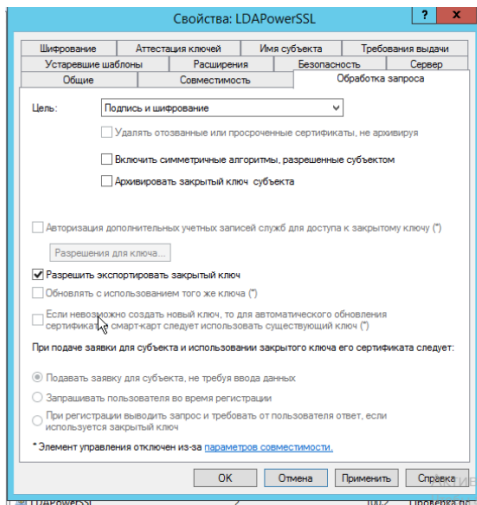
Настроить сертификат на вкладке **Общие**:

- имя сертификата **LDAPoverSSL**;
- период действия сертификата.

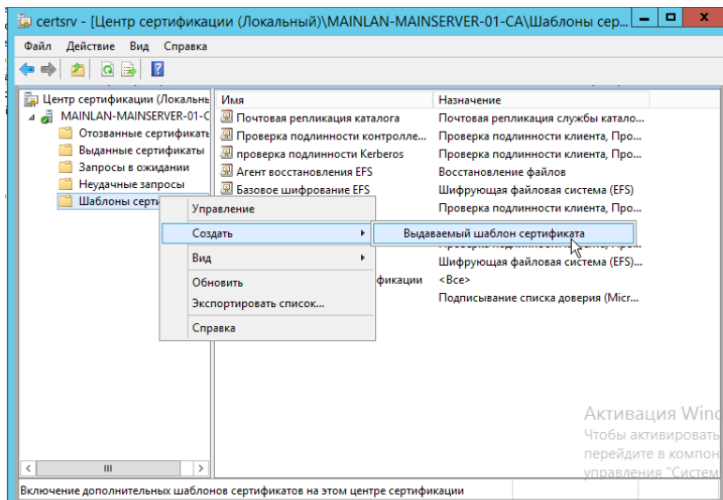


Опубликовать сертификат в MS AD.

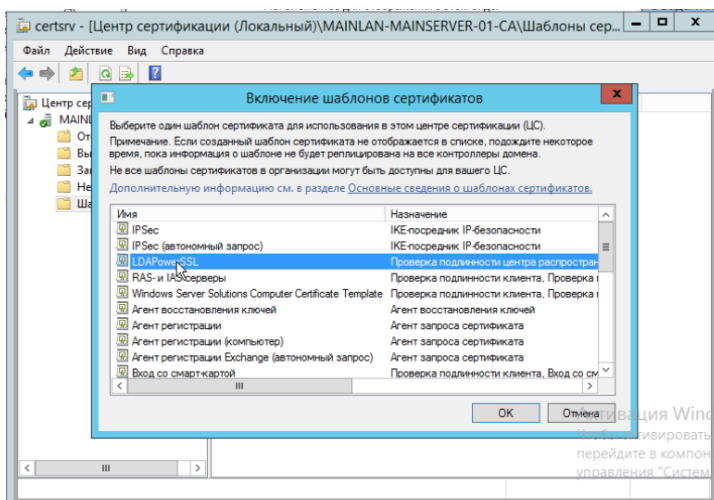
На вкладке **Обработка шаблона** установить чекбокс **Разрешить экспортировать закрытый ключ и сохранить как шаблон**.



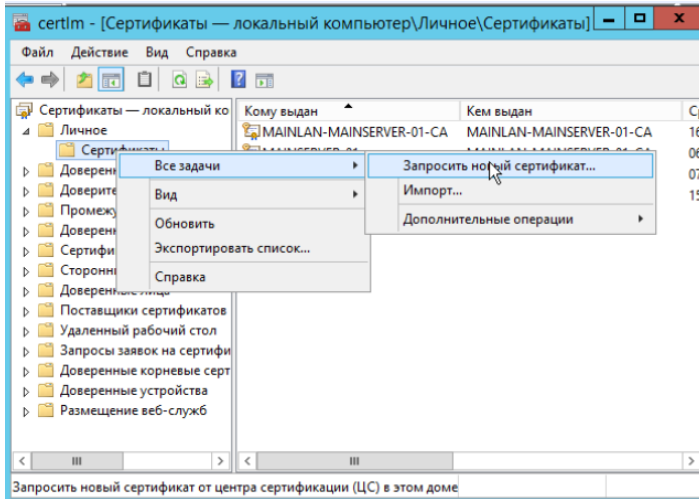
Опубликовать новый тип сертификата. Для этого в контекстном меню раздела **Шаблоны сертификатов** выбрать **Создать -> Выдаваемый шаблон сертификата**.



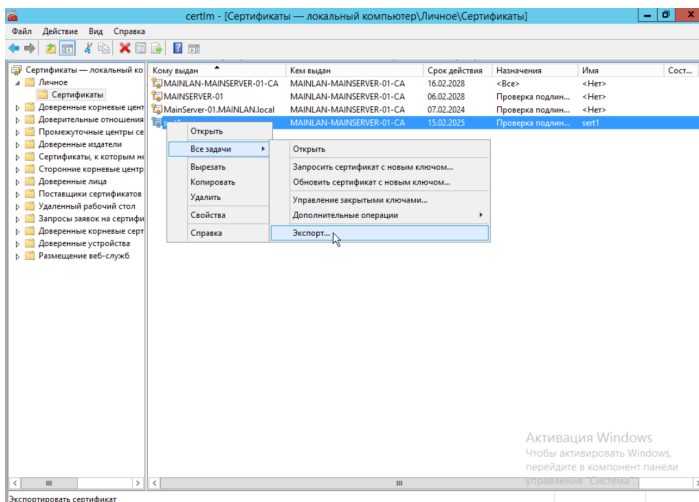
В списке доступных шаблонов выбрать созданный ранее:



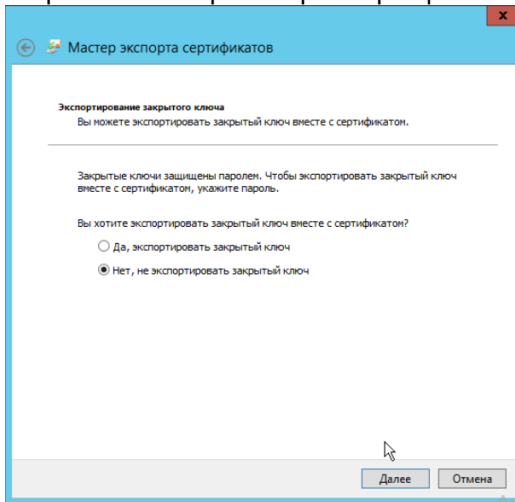
На контроллере домена, который будет задействован в процессе синхронизации данных со стороны MS AD, открыть оснастку **Управление сертификатами** компьютера. В дереве сертификатов перейти в папку **Личное** и в контекстном меню выбрать **Все задачи -> Запросить новый сертификат**:



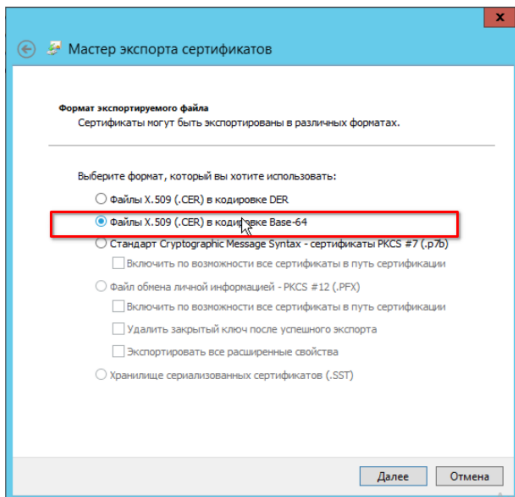
В списке доступных сертификатов выбрать созданный ранее, выпустить сертификат (кнопка **Выпустить сертификат**) и экспортировать (контекстное меню **Все задачи -> Экспорт**).



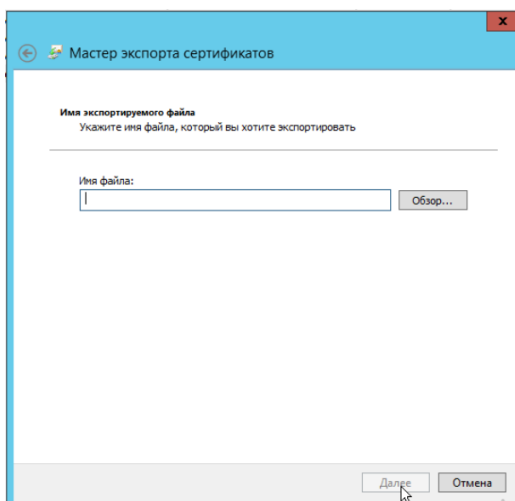
Откроется мастер экспорта сертификатов:



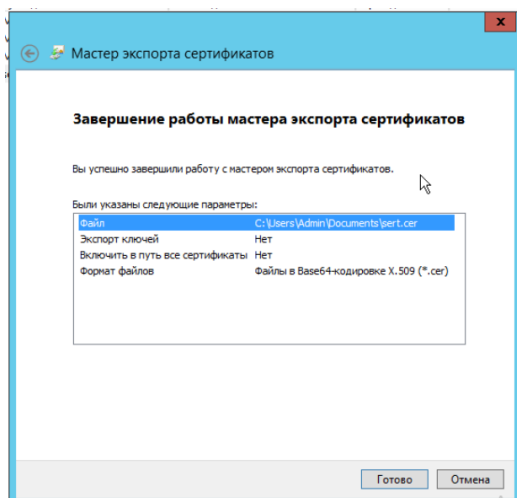
Выбрать кодировку base64 для файла сертификата:



Задать имя файла:



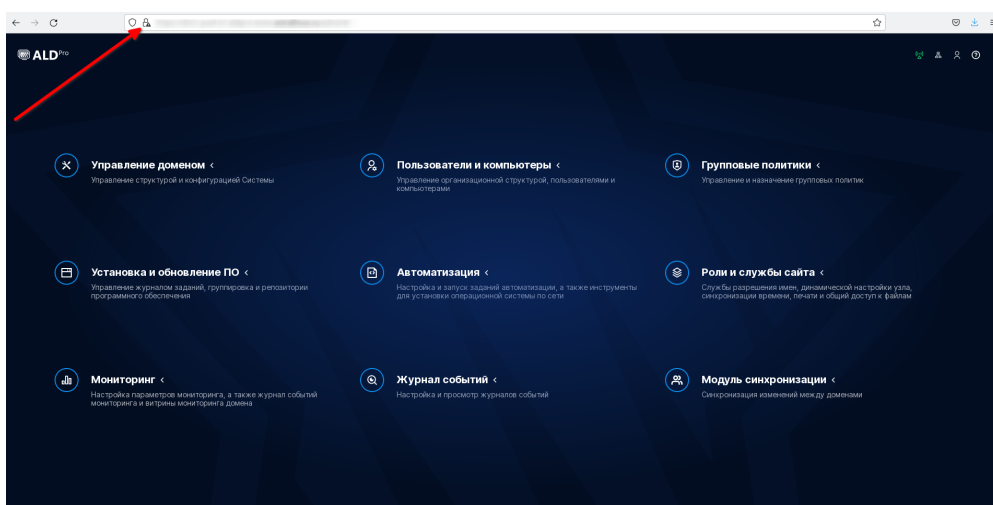
После нажатия кнопки **Готово** будет выгружен файл сертификата <имя_сертификата.cer>.



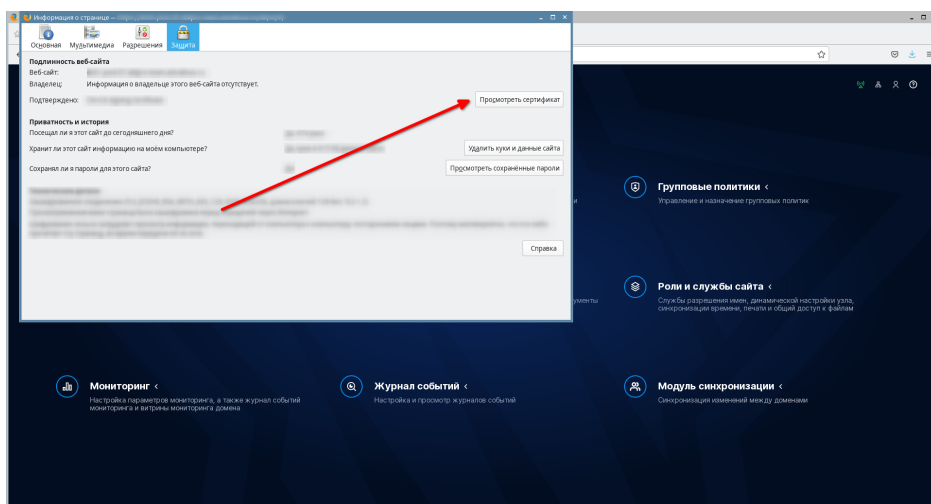
Необходимо изменить формат файла сертификата на *.pem, переименовав файл в <имя_сертификата.pem>.

2.2 Выгрузка сертификатов для контроллера домена ALD Pro

Для выгрузки сертификата необходимо зайти на портал управления ALD Pro, нажать на кнопку просмотра информации о сайте и выбрать **Незащищенное соединение -> Подробнее**:



Выбрать **Просмотреть сертификат**:



Откроется файл сертификата:

Сертификат

CA Signing Certificate	
Субъект	Общее имя
Издатель	Общее имя
Срок действия	Действителен с Действителен по
Дополнительное имя субъекта	Другое имя DNS-имя
Информация об открытом ключе	Алгоритм Размер ключа Экспонента Модуль

Открыть ссылку **PEM (сертификат)**:

Экспонента	Модуль
Разное	
Серийный номер	
Алгоритм подписи	
Версия	
Загрузить	PEM (сертификат) PEM (цепочка сертификатов)
Отличия	
SHA-256	
SHA-1	
Основные ограничения	
Центр сертификации	
Использование ключа	
Назначения	
Улучшенный ключ	
Назначения	

Сертификат сайта сохранен.

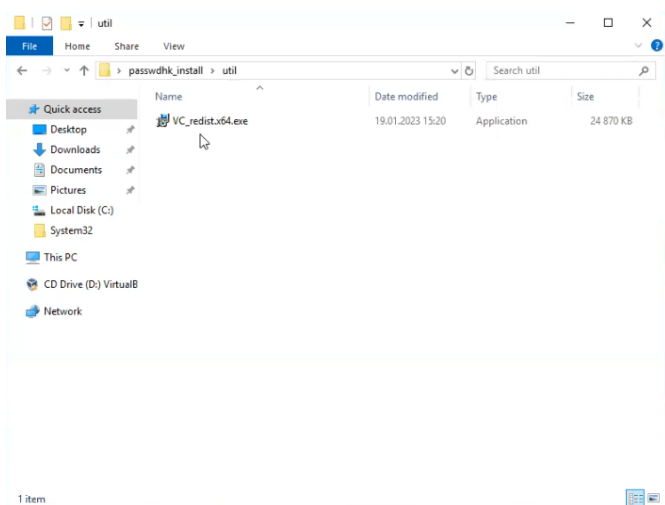
3 Настройка синхронизации паролей AD → ALD

3.1 Развертывание

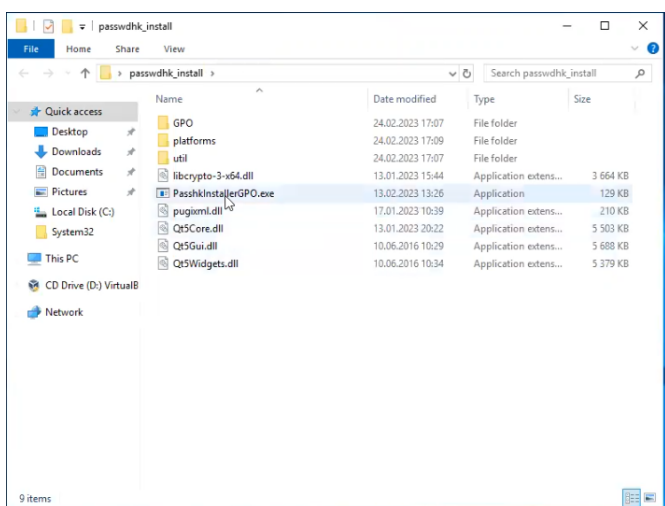
Для синхронизации паролей пользователей из домена Windows в домен ALD Pro на контроллере домена Windows необходимо настроить групповую политику фильтра паролей.

Для настройки потребуется файл **passwdhk_install.zip**, который можно скачать в личном кабинете пользователя Astra Linux <https://lk-new.astralinux.ru>

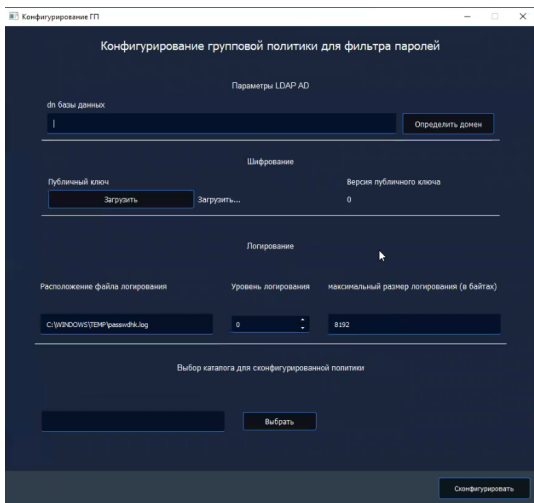
1. Для установки visual c++ sdk необходимо на всех контроллерах домена выполнить passwdhk_install/util/VC_redistx64.exe



2. На любом контроллере домена для настройки групповой политики фильтра паролей необходимо выполнить passwdhk_install/PasskhIntallerGPO.exe



3. Интерфейс приложения



Кнопка **Определить домен**: определяет домен, в котором развернут контроллер домена AD;

Публичный ключ → **Загрузить**: загружаем файл открытого ключа, скачанный при развертывании модуля синхронизации в ALD Pro;

Версия публичного ключа: подтягивается из файла открытого ключа;

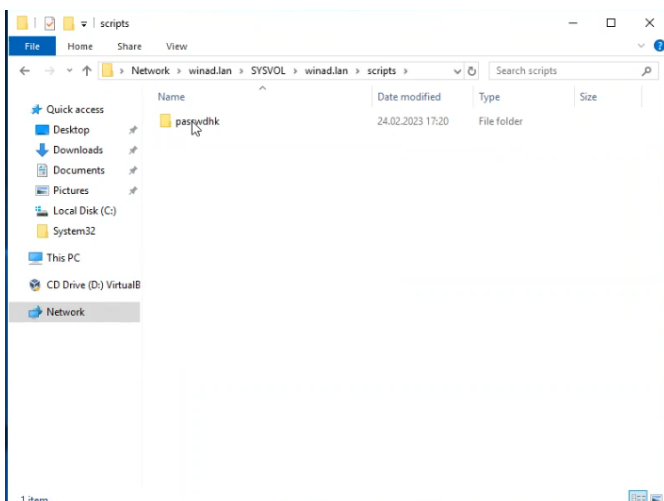
Расположение файла логирования: необходимо указать директорию и файл типа .log, куда будут записываться журналы;

Уровень логирования: указываем один из 4х уровней логирования (подробнее ниже);

Максимальный размер логирования (в байтах): максимальный размер файла логирования (по достижению максимального размера файлом логирования, он архивируется);

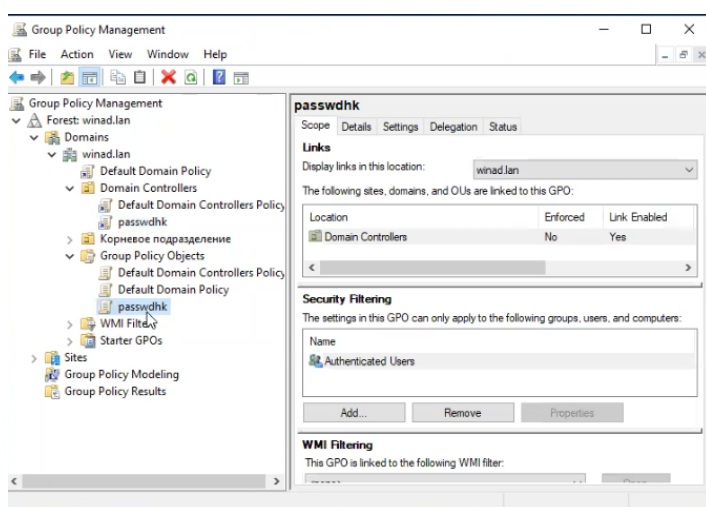
Выбор каталога для сконфигурированной политики: указываем директорию для хранения сконфигурированной политики.

4. В расположение \winad.lan\sysvol\winad.lan\scripts\ необходимо скопировать папку passwdhk из каталога для сконфигурированной политики, указанного на предыдущем шаге:

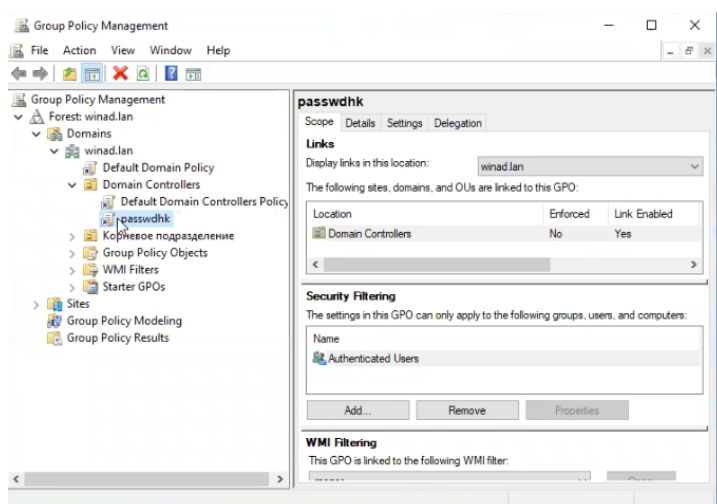


5. Следующим шагом необходимо запустить оствастку "Управление групповой политикой".

6. В папке "Объекты групповой политики" необходимо создать новую пустую групповую политику с названием passwdhk



7. Для созданной политики passwdhik выполнить импорт настроек.
8. На шаге с выбором расположения импорта настроек необходимо указать каталог Policies из каталога, указанного для сконфигурированной политики.
9. Групповую политику необходимо переместить в расположение "Контроллеры домена"

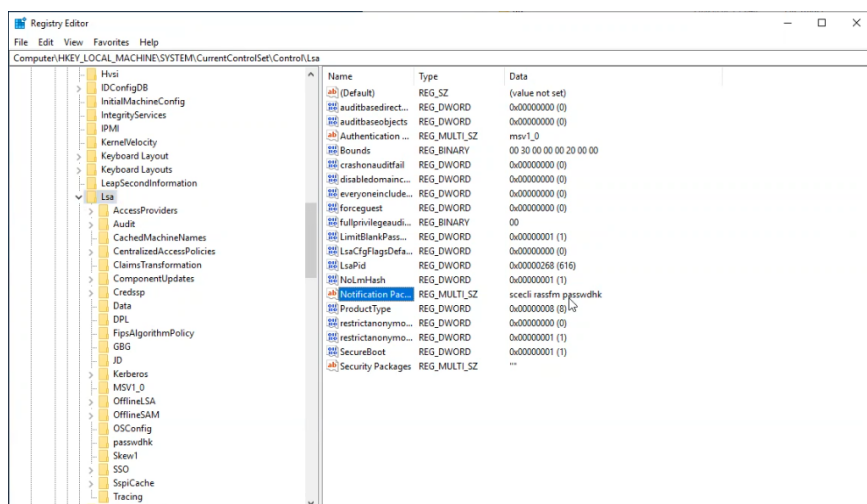


10. Для применения групповой политики в консоли powershell необходимо выполнить команду:

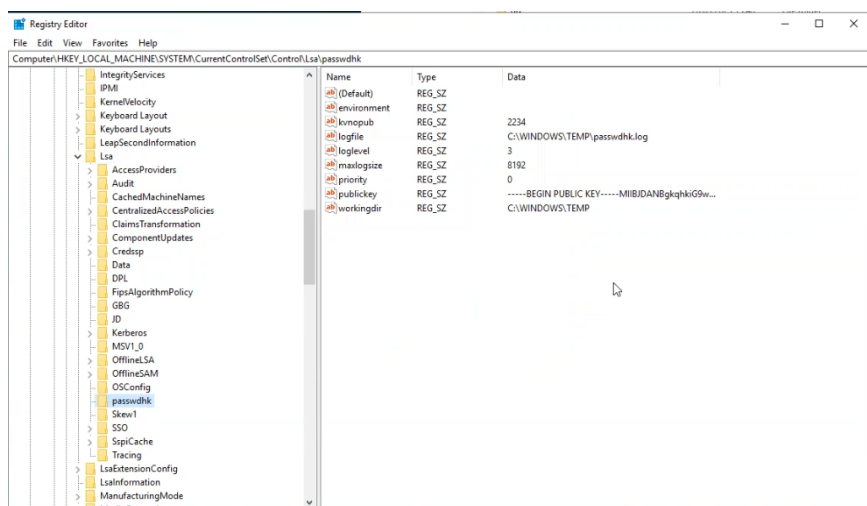
```
gp update force
```

11. Выполнить поочередную перезагрузку контроллеров домена.
12. Проверьте, что в реестре создались необходимые записи.

Первая:



вторая:



3.1.1 Уровни логирования

0 - отсутствие логирования

1 - в лог файл записываются только сообщения об ошибках

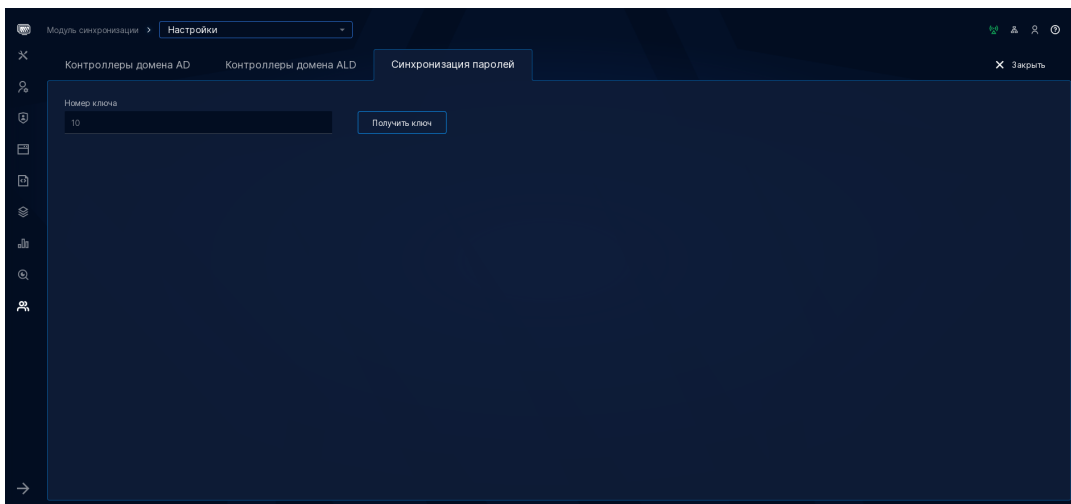
2 - в лог файл записываются сообщения об ошибках и информационные сообщения

3 - в лог файл записываются сообщения об ошибках, информационные сообщения + информация для отладки: все записи о процессе шифрования, какой ключ используется и т.д.

4 Синхронизация паролей ALD Pro → AD

4.1 Получение открытого ключа

В интерфейсе ALD Pro открыть **Модуль синхронизации** → **Конфигурации** → **Синхронизация паролей**



По нажатию кнопки **Получить ключ** скачивается файл открытого ключа и актуализируется порядковый номер ключа.

4.2 Синхронизация паролей

Скаченный файл открытого ключа необходимо сохранить в любую директорию, например, /tmp/. Следующим шагом файл открытого ключа необходимо скопировать в расположение /opt/rbta/aldpro/syncer/:

```
sudo cp /tmp/public.gpg /opt/rbta/aldpro/syncer/public.gpg
```

Перезагружаем контроллер домена:

```
sudo ipactl restart
```