

Настройка 2ФА на macOS в домене Windows с помощью Рутокен ЭЦП

Описание стенда

Сервер

ОС: Windows Server 2019

Доменное имя: test.rutoken.ru

IP: 172.16.113.102

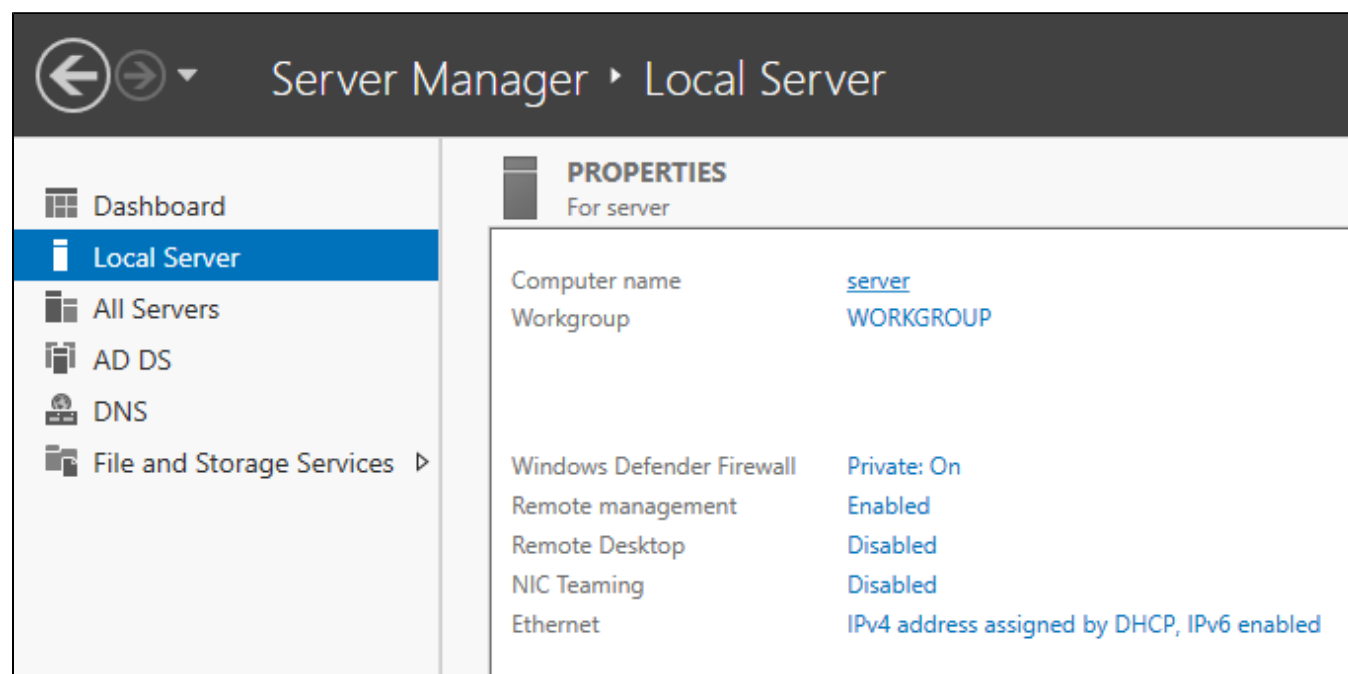
Клиент

ОС: macOS Ventura 13.2

Настройка сервера

Чтобы настроить сервер, установите сервис Active Directory.

До установки сервиса можно изменить имя сервера. Чтобы это сделать, задайте новое имя в окне менеджера сервера, в поле **Computer name**.



После этого начните процедуру установки Active Directory.

Установка сервиса Active Directory

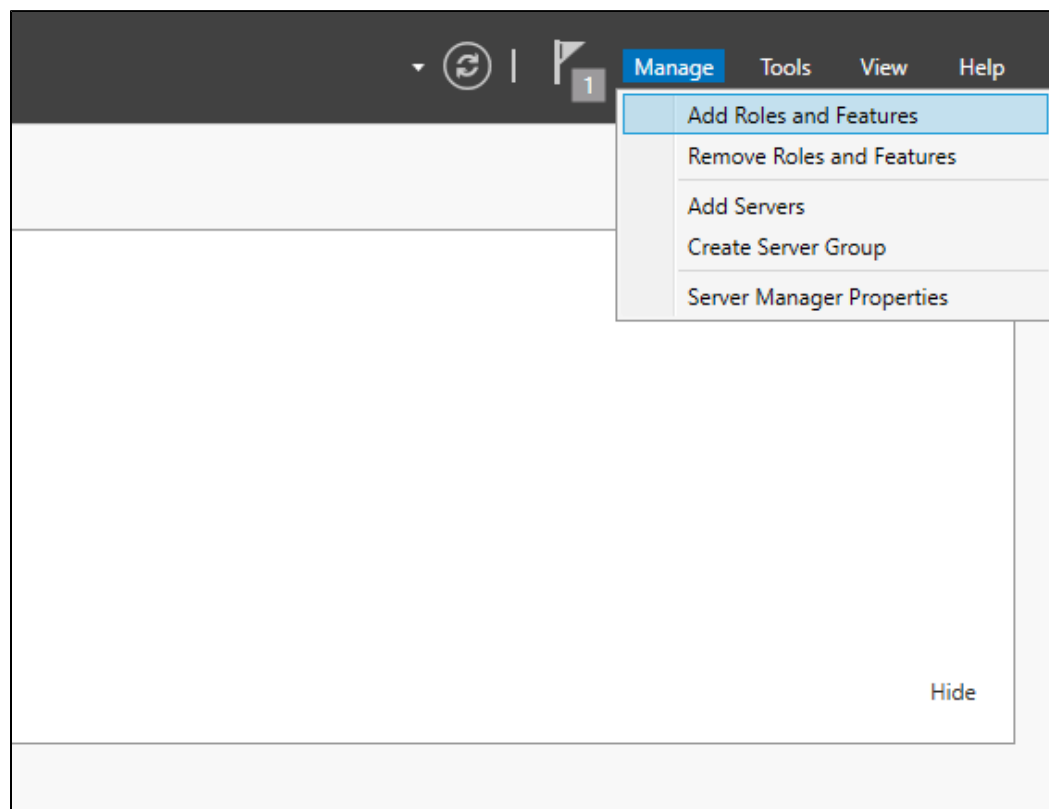
Процедура установки состоит из следующих шагов:

1. Добавление сервисов.
2. Настройка домена.
3. Добавление новых пользователей.
4. Установка центра сертификации Active Directory.

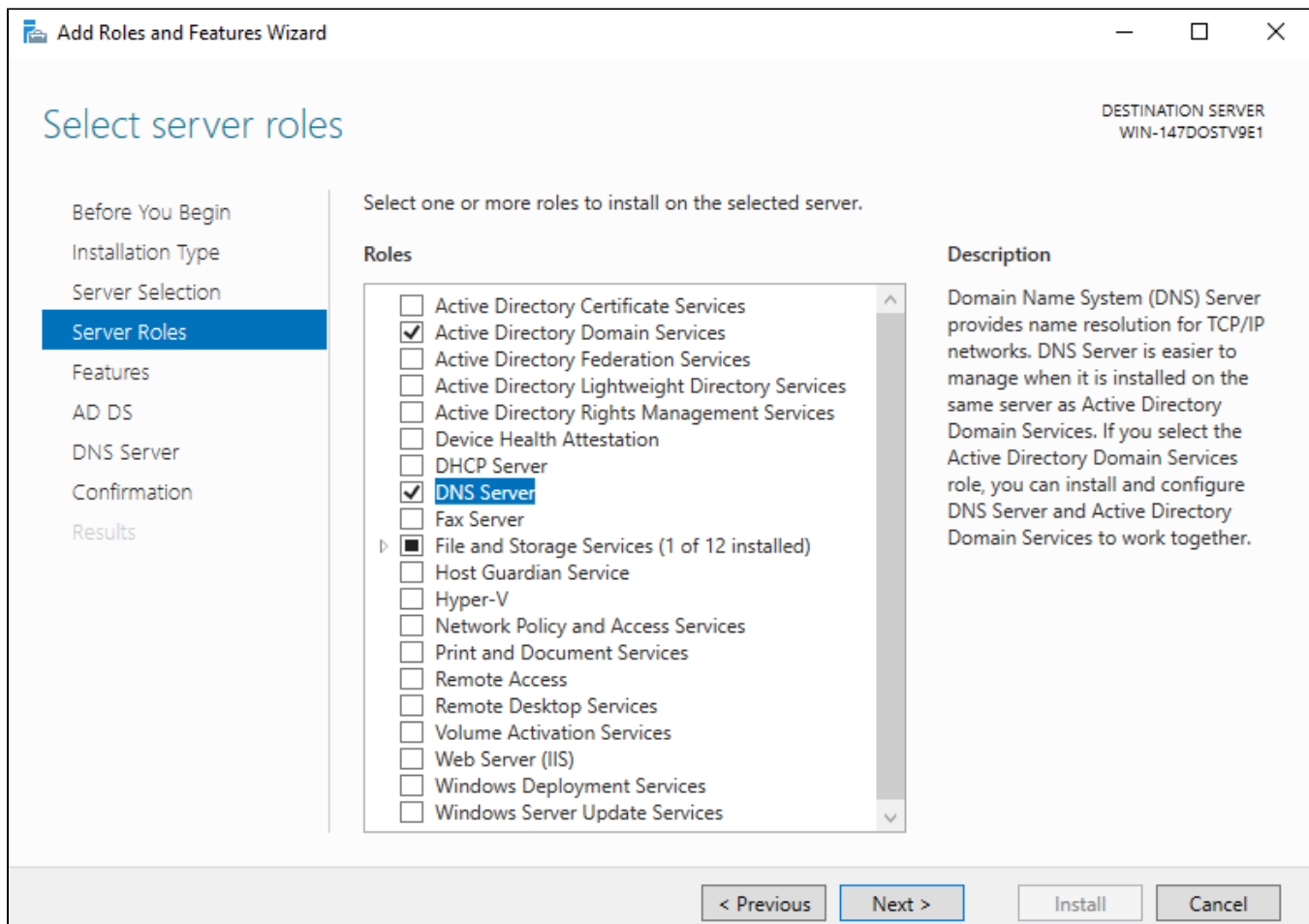
Шаг 1. Добавление необходимых сервисов

Добавьте на сервер сервисы **Active Directory** и **DNS**. Чтобы это сделать:

1. Откройте окно для добавления ролей в менеджере сервера.



2. В окне для выбора сервисов поставьте галочки **Active Directory Domain Services** и **DNS Server**.



3. Нажмите **Next**.

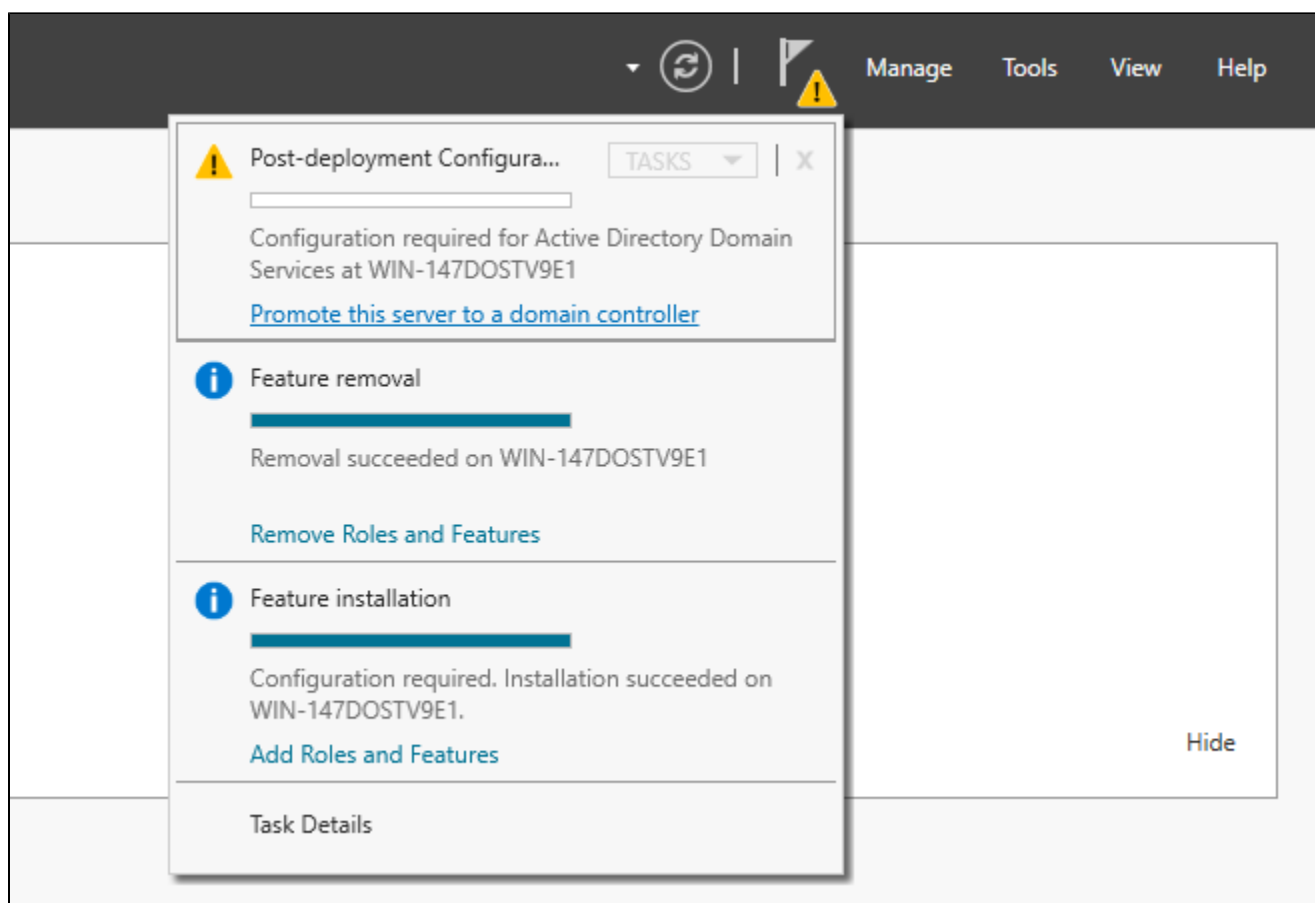
4. Далее дайте согласие на установку.

5. После завершения установки сервисов, перейдите к настройке домена.

Шаг 2. Настройка домена

Чтобы настроить домен:

1. Откройте меню уведомлений и щёлкните по ссылке **Promote this server to a domain controller**.



2. На вкладке **Deployment Configuration** выберите опцию для создания нового домена **Add a new forest** и в поле **Root domain name** укажите его название. Нажмите **Next**.

Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
server

Deployment Configuration

- Domain Controller Options
- Additional Options
- Paths
- Review Options
- Prerequisites Check
- Installation
- Results

Select the deployment operation

- ☐ Add a domain controller to an existing domain
- ☐ Add a new domain to an existing forest
- ☒ Add a new forest

Specify the domain information for this operation

Root domain name:

[More about deployment configurations](#)

< Previous Next > Install Cancel

3. На вкладке **Domain Controller Options** введите пароль сброса. Нажмите **Next**.

Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
server

Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2016

Domain functional level: Windows Server 2016

Specify domain controller capabilities

☒ Domain Name System (DNS) server
☒ Global Catalog (GC)
☐ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password:

Confirm password:

[More about domain controller options](#)

< Previous Next > Install Cancel

4. На вкладке **DNS Options** ничего не меняйте, т.к. сервер сам является DNS-сервером. Нажмите **Next**.

Active Directory Domain Services Configuration Wizard

DNS Options

TARGET SERVER
server

 A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found... [Show more](#) 

- Deployment Configuration
- Domain Controller Options
- DNS Options**
- Additional Options
- Paths
- Review Options
- Prerequisites Check
- Installation
- Results

Specify DNS delegation options

☐ Create DNS delegation

[More about DNS delegation](#)

< Previous

Next >

Install

Cancel

5. На следующих трёх вкладках тоже ничего не меняйте, просто нажимайте **Next**.

Additional Options

TARGET SERVER
server

Deployment Configuration

Domain Controller Options

DNS Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Verify the NetBIOS name assigned to the domain and change it if necessary

The NetBIOS domain name:

[More about additional options](#)

< Previous

Next >

Install

Cancel

Paths

TARGET SERVER
server

Deployment Configuration

Domain Controller Options

DNS Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Specify the location of the AD DS database, log files, and SYSVOL

Database folder:

C:\Windows\NTDS



Log files folder:

C:\Windows\NTDS



SYSVOL folder:

C:\Windows\SYSVOL

[More about Active Directory paths](#)

< Previous

Next >

Install

Cancel

Active Directory Domain Services Configuration Wizard

Review Options

TARGET SERVER
server

Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

Review your selections:

Configure this server as the first Active Directory domain controller in a new forest.

The new domain name is "astradomain.ad". This is also the name of the new forest.

The NetBIOS name of the domain: TEST

Forest Functional Level: Windows Server 2016

Domain Functional Level: Windows Server 2016

Additional Options:

Global catalog: Yes

DNS Server: Yes

Create DNS Delegation: No

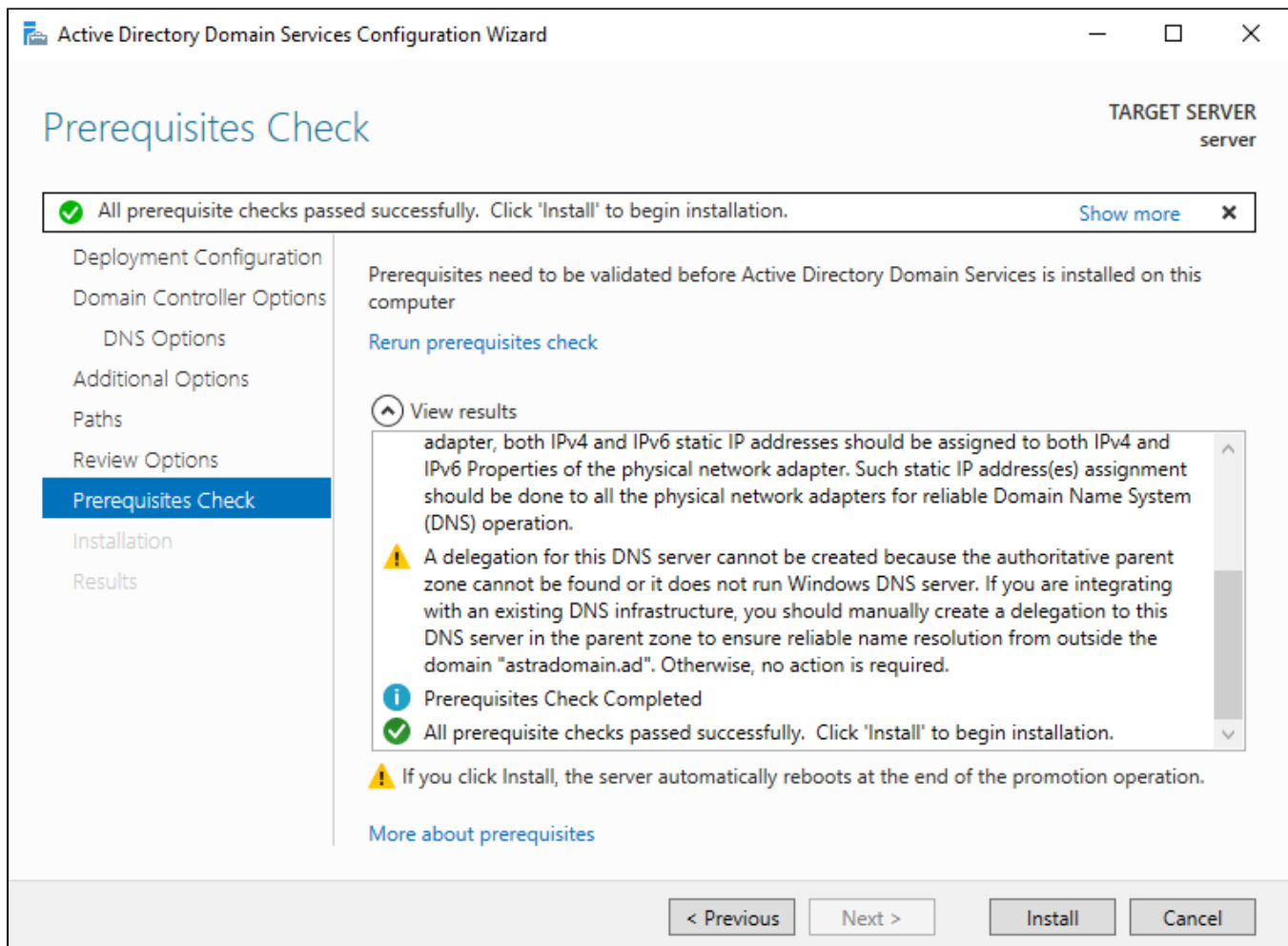
These settings can be exported to a Windows PowerShell script to automate additional installations

[View script](#)

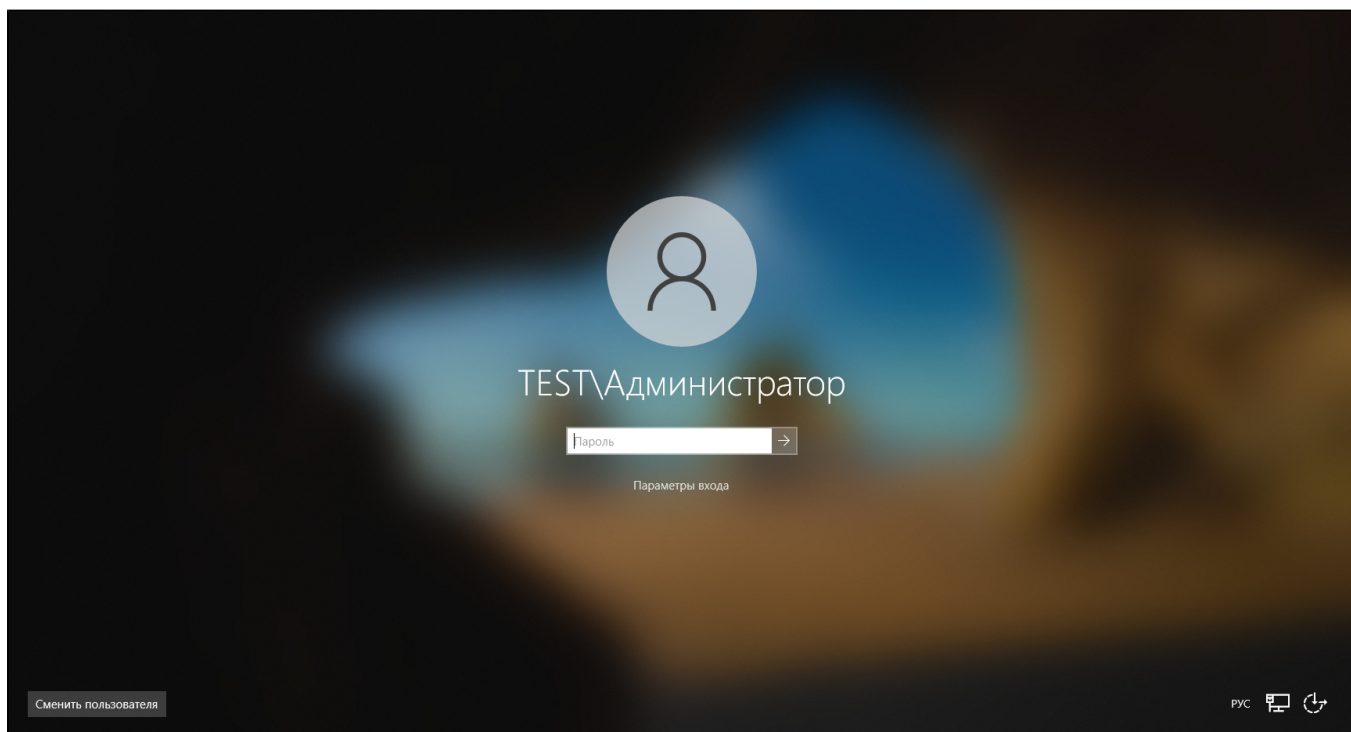
[More about installation options](#)

< Previous Next > Install Cancel

6. Перед запуском процесса установки ознакомьтесь с уведомлениями об ошибках. Если необходимо, устраните возникшие проблемы. В нашем примере уведомления не являются критичными.



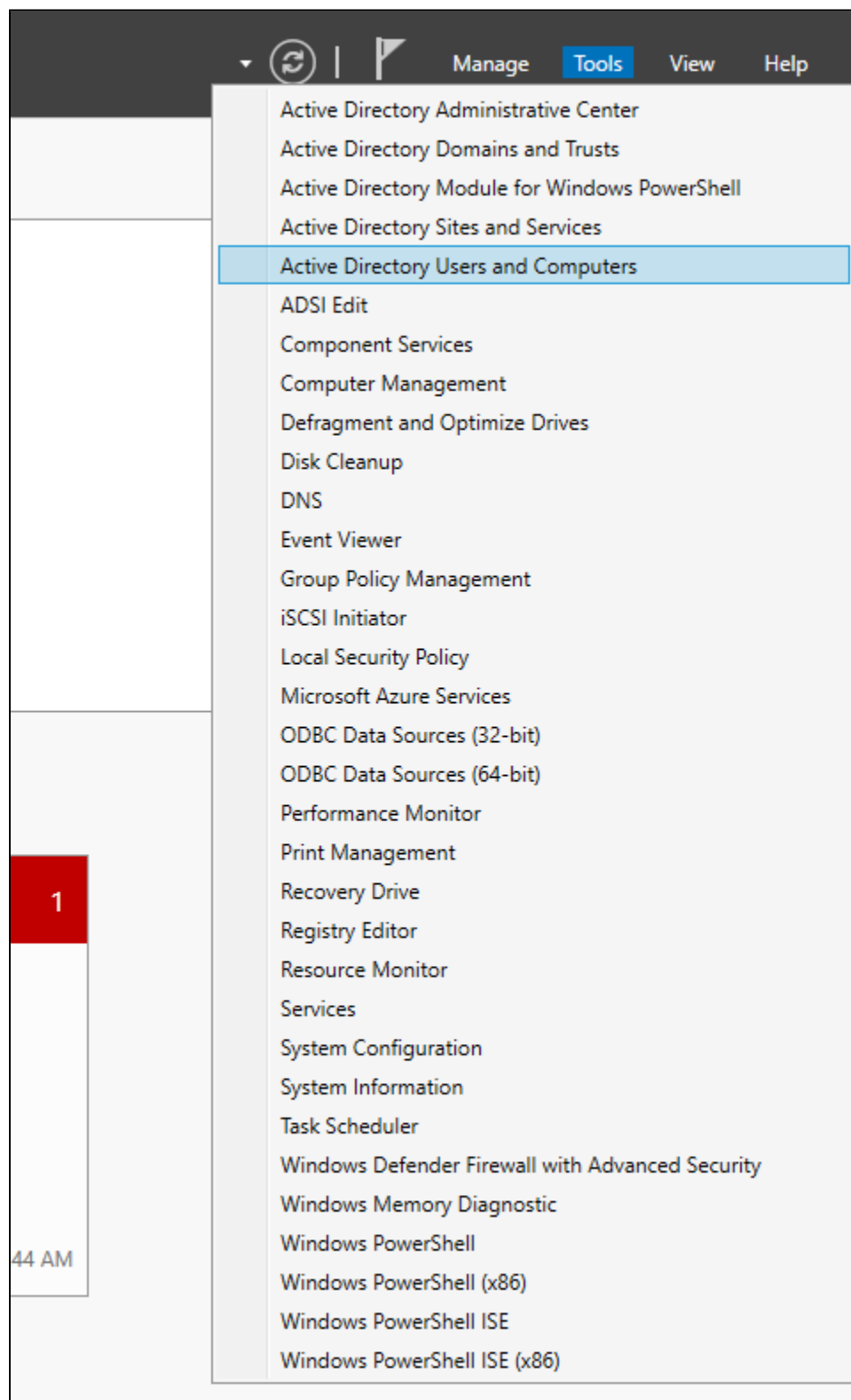
После установки Active Directory сервер перезагрузится. Если настройка прошла успешно, то на экране отобразится окно для входа в аккаунт доменного пользователя.



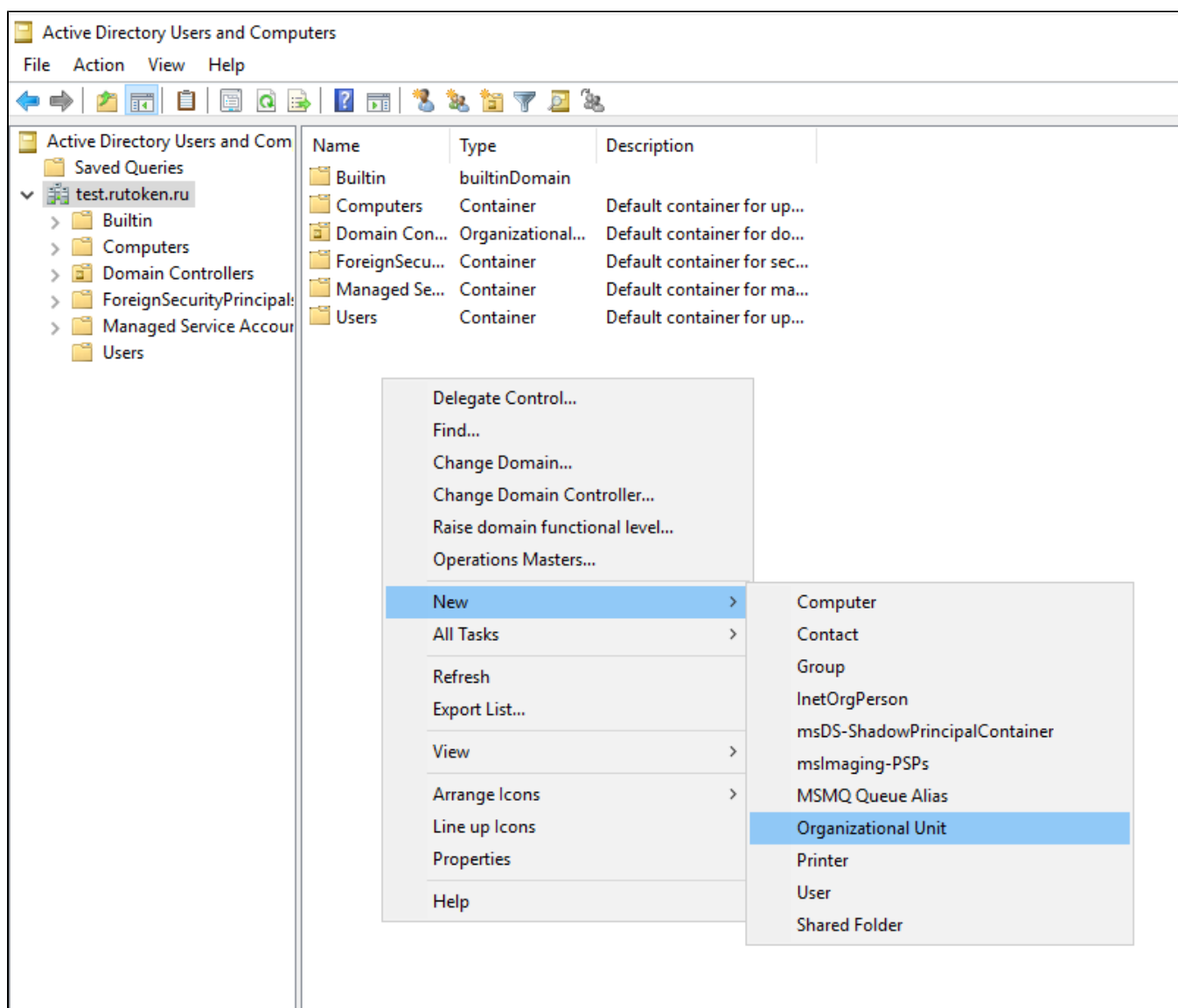
Шаг 3. Добавление новых пользователей

Чтобы добавить новых пользователей:

1. Откройте утилиту управления пользователями и компьютерами домена.



2. Для удобства создайте отдельную директорию Domain Users, в которой будете создавать доменных пользователей. В правой части окна щёлкните на пустом месте и выберите New → Organizational Unit.



В поле **Name** укажите имя директории **Domain Users**.

New Object - Organizational Unit

Create in: test.rutoken.ru/

Name:

☒ Protect container from accidental deletion

OK Cancel Help

3. Добавьте нового пользователя User. В правой части окна щёлкните на пустом месте и выберите New → User.

Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers

- Saved Queries
- test.rutoken.ru
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - Managed Service Accounts
 - Users
 - Domain Users

Name	Type	Description
Delegate Control... Move... Find... New > All Tasks > Refresh View > Arrange Icons > Line up Icons Properties Help		
		Computer Contact Group InetOrgPerson msDS-ShadowPrincipalContainer mslmaging-PSPs MSMQ Queue Alias Organizational Unit Printer User Shared Folder

Укажите данные пользователя.

New Object - User ✕

 Create in: test.rutoken.ru/Domain Users

First name: Initials:

Last name:

Full name:

User logon name:

User logon name (pre-Windows 2000):

New Object - User ✕

 Create in: test.rutoken.ru/Domain Users

Password:

Confirm password:

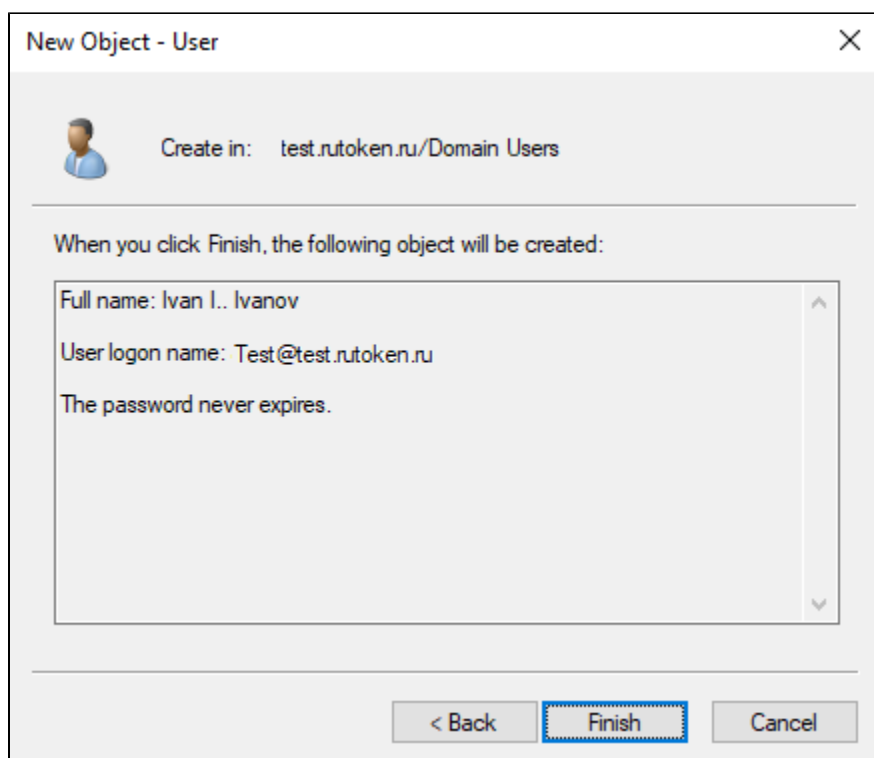
☐ User must change password at next logon

☐ User cannot change password

☒ Password never expires

☐ Account is disabled

Проверьте указанные данные и нажмите **Finish**.



4. Аналогичным образом добавьте остальных пользователей, которые должны быть в домене.

Шаг 4. Установка центра сертификации Active Directory

Перед процедурой установите на сервер драйверы для работы с устройствами Рутокен.

Ссылка на актуальную версию: <https://www.rutoken.ru/support/download/windows/>

После этого перейдите к настройке центра сертификации и выдаче сертификатов для пользователей. Это можно сделать по [данной инструкции](#).

Настройка клиента

Установка приложения "Рутокен для macOS"

Приложение **Рутокен для macOS** необходимо для настройки двухфакторной аутентификации в macOS с использованием сертификатов, записанных на устройствах Рутокен.

Чтобы установить **Рутокен для macOS**:

1. Перейдите на страницу:
<https://www.rutoken.ru/support/download/mac/>

2. На странице **Драйверы для macOS** нажмите **Рутокен для macOS**.

РУТОКЕН

О компании / Проекты / Партнеры / Пресс-центр / Форум / Контакты / World Wide

Продукты ▾ Решения ▾ Технологии ▾ Поддержка ▾ Заказ ▾

Центр загрузки ▾ [ДЛЯ РАЗРАБОТЧИКА](#)

[Главная](#) > [Поддержка](#) > [Центр загрузки](#) > Драйверы для macOS

Драйверы для macOS

ВОПРОС-ОТВЕТ

ЦЕНТР ЗАГРУЗКИ

- Драйверы для Windows
- Драйверы для ЕГАИС
- Драйверы для macOS**
- Драйверы для "nix"
- Рутокен Плагин
- Библиотека PKCS#11
- Рутокен Логон
- Рутокен Коннект
- ПО для Рутокен VPN
- Модули интеграции с OpenSSL
- Драйверы Рутокен Магистра
- Документация

Пользователям Рутокен ЭЦП

Драйверы для Рутокен ЭЦП в современных операционных системах macOS не требуются. Пользователям устаревших версий macOS X 10.6 Snow Leopard и более ранних может потребоваться внести изменения в конфигурационный файл в соответствии с инструкцией.

Если Рутокен используется в виртуальной среде Windows, запущенной на компьютере Mac через Parallels Desktop, VmWare Fusion или Oracle VirtualBox, то настраивать Рутокен в macOS не обязательно.

ИНСТРУКЦИИ

- [Рутокен ЭЦП в macOS](#)
- [Рутокен Lite в macOS](#)

ОБРАТИТЕ ВНИМАНИЕ

В современных macOS, начиная с версии 10.15 Catalina, устройства Рутокен не отображаются в приложении «Связка ключей» (KeyChain). Для отображения сертификатов в самих приложениях необходимо установить [Рутокен для macOS](#).

Рутокен для macOS

Версия: 1.1.0 от 24.08.2022

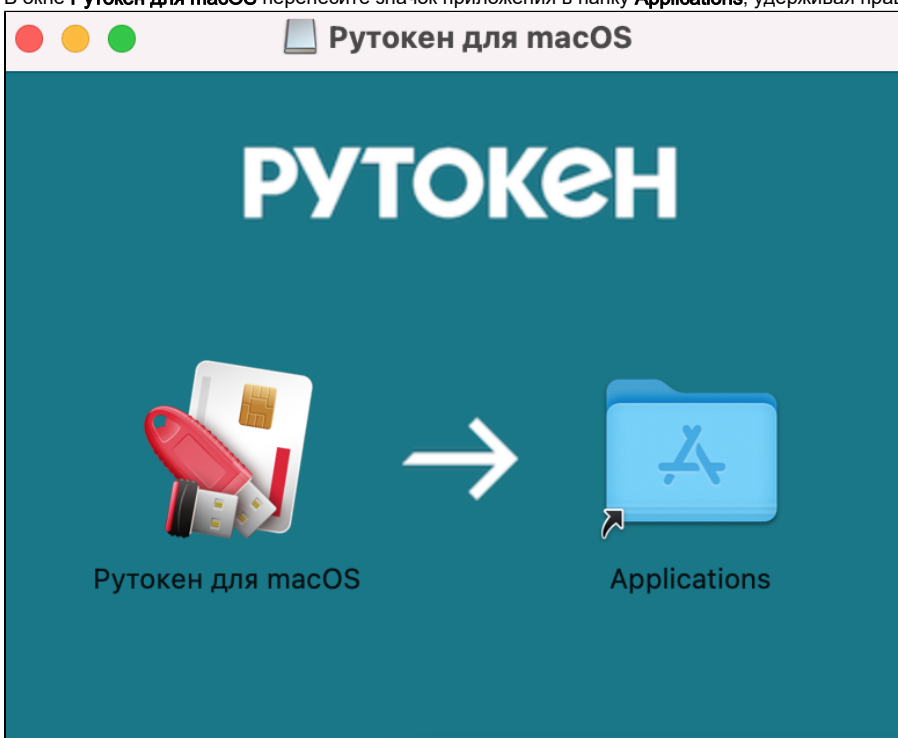
Поддерживаемые ОС: macOS 13/12/11/10.15

Специальное приложение для работы RSA-сертификатов на устройствах семейства Рутокен ЭЦП с использованием инструментов macOS.

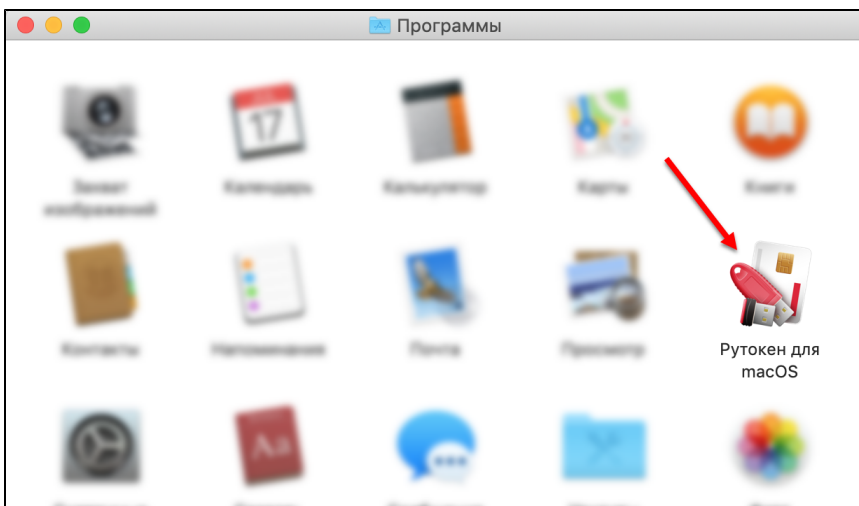
Поддержка KeyChain для macOS Mojave и более ранних

Версия: 2.0.0.0 от 23.10.2019

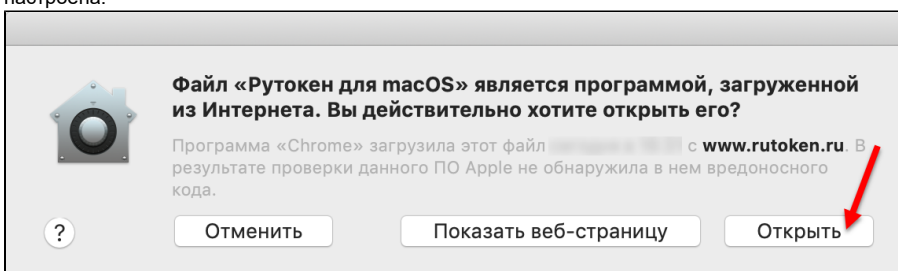
3. Загрузите программу установки.
4. Перейдите в папку **Загрузки** и запустите только что скачанную программу установки **Рутокен для macOS**.
5. В окне **Рутокен для macOS** перенесите значок приложения в папку **Applications**, удерживая правую кнопку мыши.



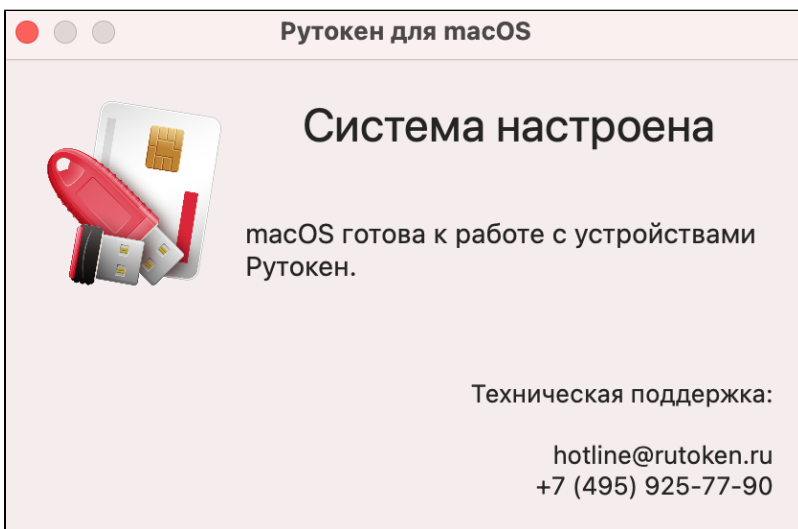
6. В окне **Рутокен для macOS** два раза щелкните по папке **Applications**. Откроется папка **Программы**. Найдите в этой папке приложение **Рутокен для macOS** и два раза щелкните по нему.



7. Чтобы подтвердить открытие приложения, нажмите **Открыть**. В результате на экране отобразится уведомление о том, что система настроена.



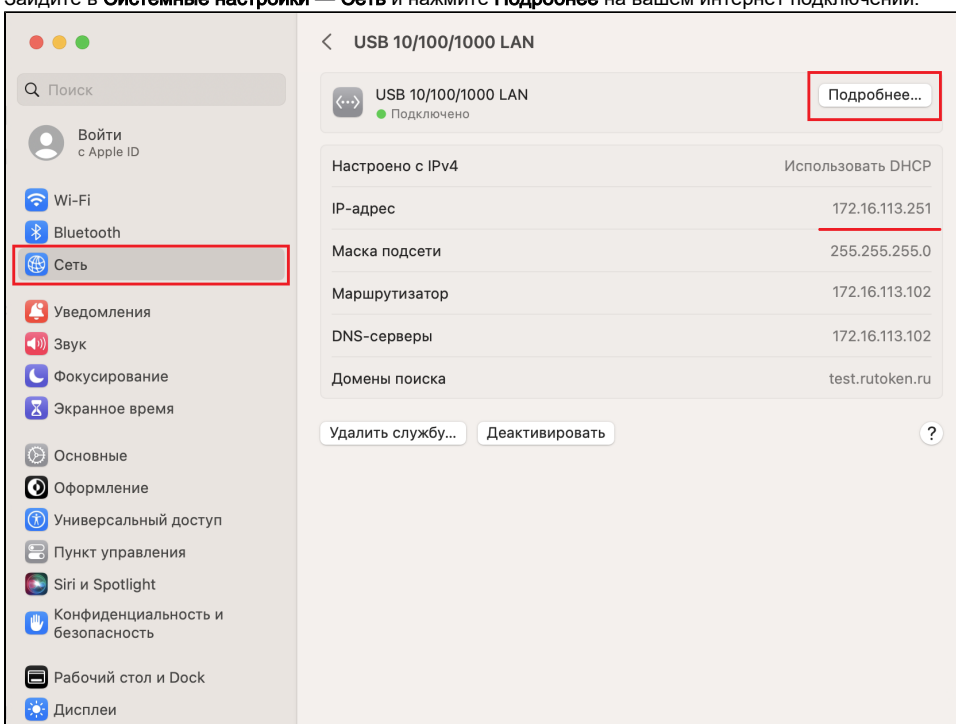
После установки приложения обязательно перезагрузите компьютер.



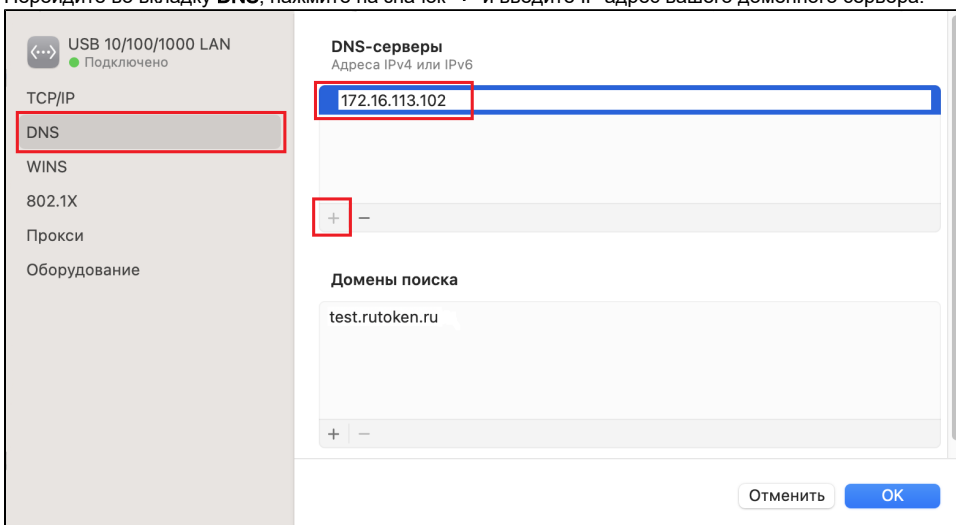
8. Закройте окно с уведомлением.

Настройка Сети

1. Зайдите в **Системные настройки** — **Сеть** и нажмите **Подробнее** на вашем интернет подключении.

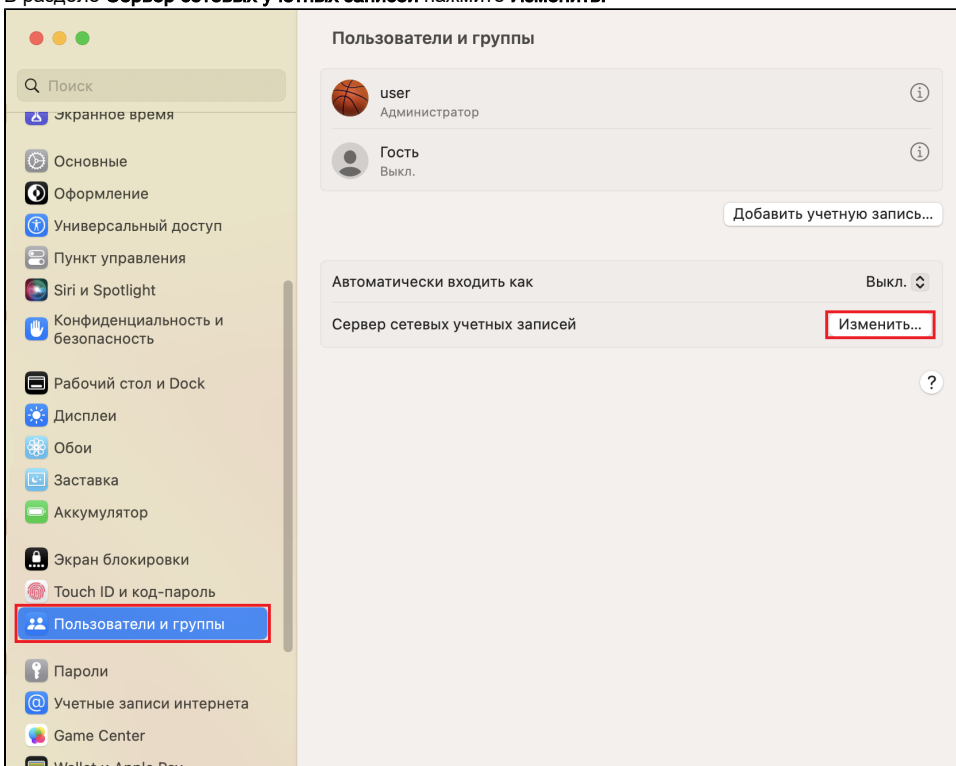


2. В открывшемся окне проверьте, чтобы ваш IP адрес находился в той же подсети, что и ваш доменный сервер.
3. Перейдите во вкладку **DNS**, нажмите на значок "+" и введите IP адрес вашего доменного сервера.

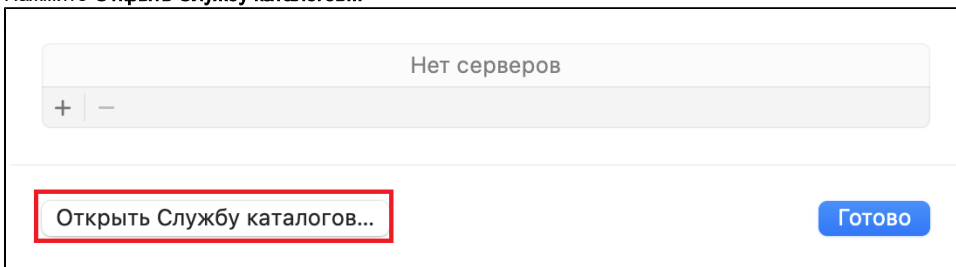


4. Перейдите в **Системные настройки** — **Пользователи и группы**.

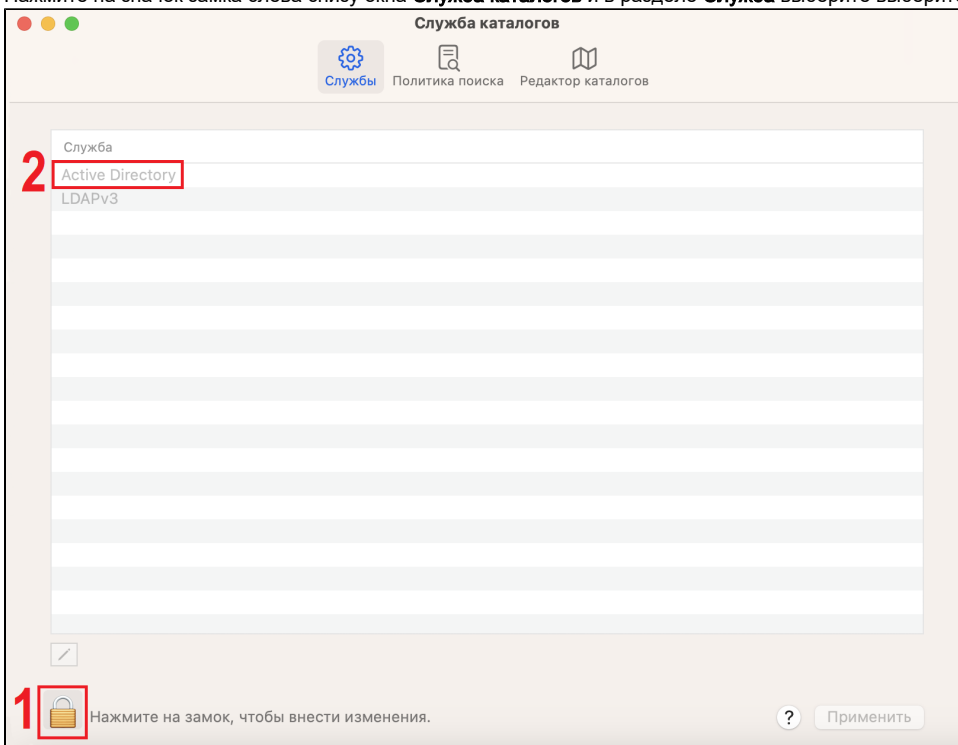
5. В разделе **Сервер сетевых учётных записей** нажмите **Изменить**.



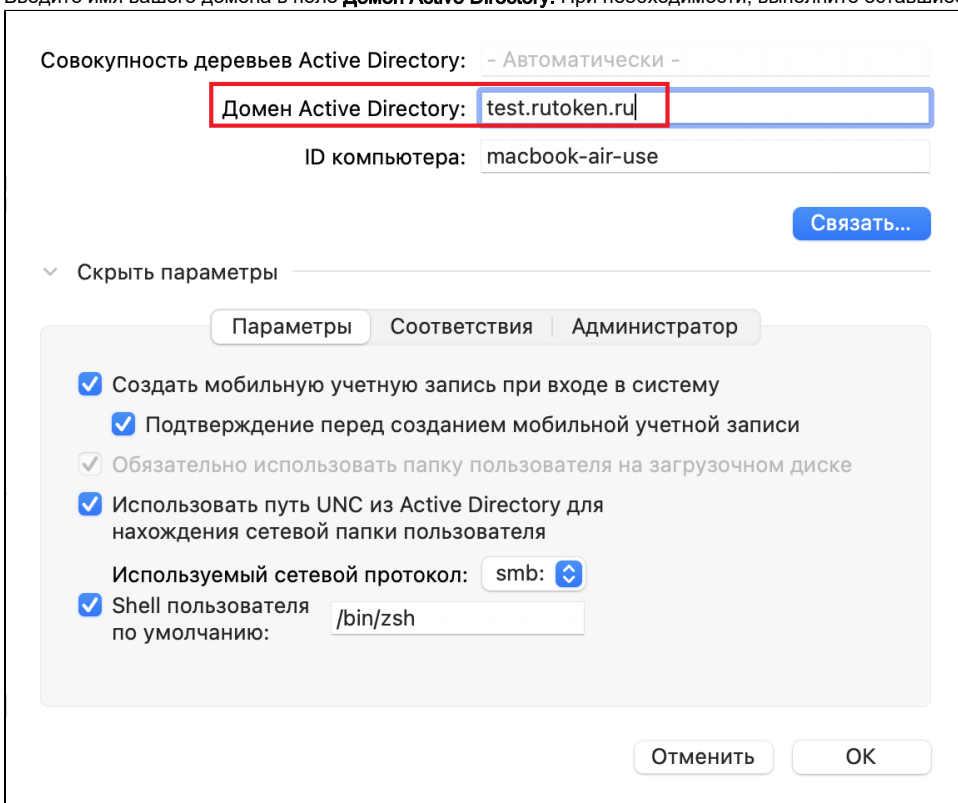
6. Нажмите **Открыть Службу каталогов...**



7. Нажмите на значок замка слева снизу окна **Служба каталогов** и в разделе **Служба** выберите **Active Directory**.



8. Введите имя вашего домена в поле **Домен Active Directory**. При необходимости, выполните оставшиеся настройки по своим параметрам.



9. После применения всех настроек, нажмите **Связать**. Потребуется ввести логин и пароль администратора домена.

Необходим администратор сети

Пользователь:

Пароль:

OU компьютера:

☒ Использовать для аутентификации

☒ Использовать для контактов

Настройка SmartcardLogin.plist

Чтобы использовать смарт-карту для авторизации доменного пользователя, необходимо создать и настроить конфигурационный файл SmartcardLogin.plist.

Чтобы создать и настроить SmartcardLogin.plist:

1. Откройте **Терминал** и введите следующую команду для отключения уведомления привязки токена к локальному пользователю:

```
sudo defaults write /Library/Preferences/com.apple.security.smartcard UserPairing -bool NO
```

2. Откройте и настройте конфигурационный файл **SmartcardLogin.plist**

```
sudo nano /private/etc/SmartcardLogin.plist
```

Пример настройки SmartcardLogin.plist:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>AttributeMapping</key>
<dict>
<key>fields</key>
<array>
<string>NT Principal Name</string>
</array>
<key>formatString</key>
<string>Kerberos:$1</string>
<key>dsAttributeString</key> <string>dsAttrTypeStandard:AltSecurityIdentities</string>
</dict>
</dict>
</plist>
```

3. Настройте права доступа к файлу.

```
sudo chown root:wheel /private/etc/SmartcardLogin.plist  
sudo chmod 644 /private/etc/SmartcardLogin.plist
```

4. Проверьте правильность конфигурационного файла. Следующая команда должна вывести **OK**.

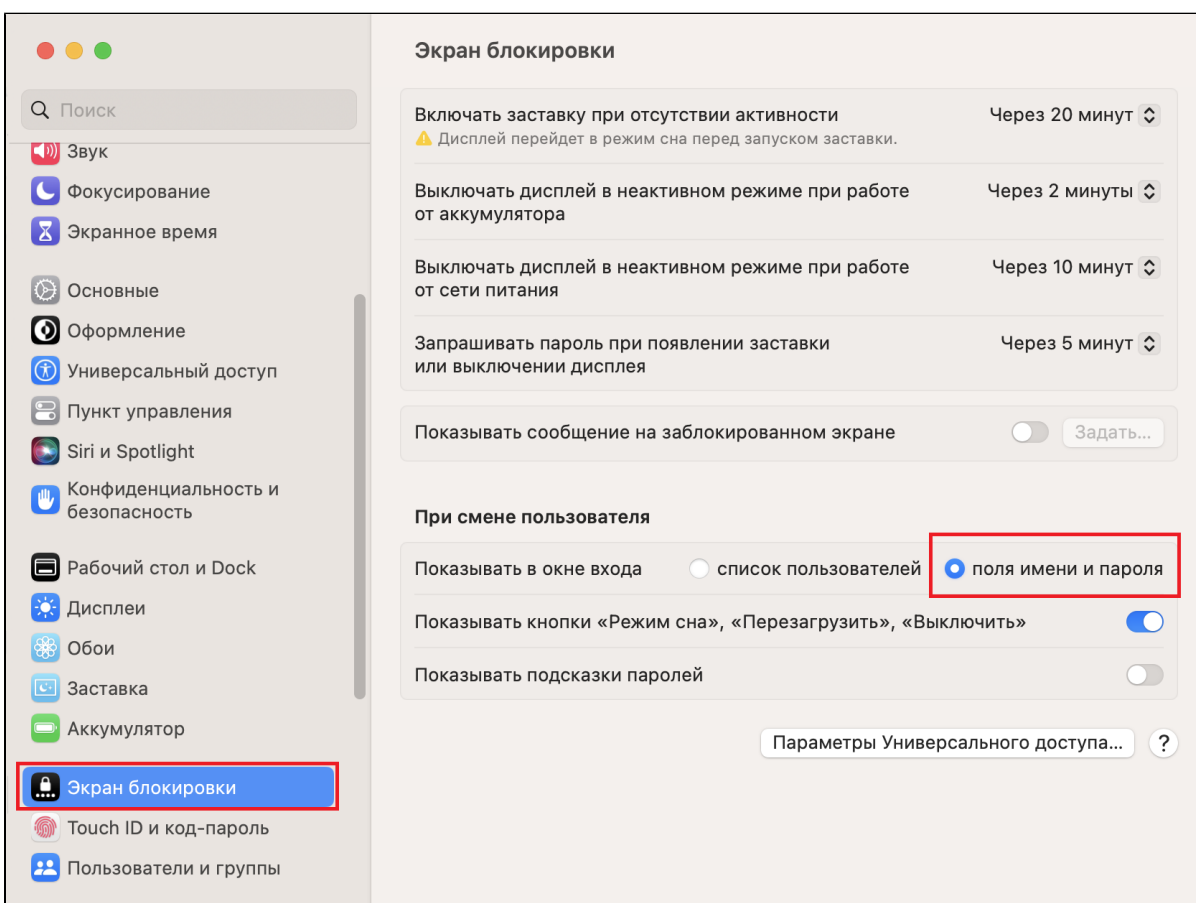
```
plutil -lint /private/etc/SmartcardLogin.plist  
/private/etc/SmartcardLogin.plist: OK
```

Подробнее про конфигурацию SmartcardLogin.plist можно прочитать на [странице техподдержки Apple](#).

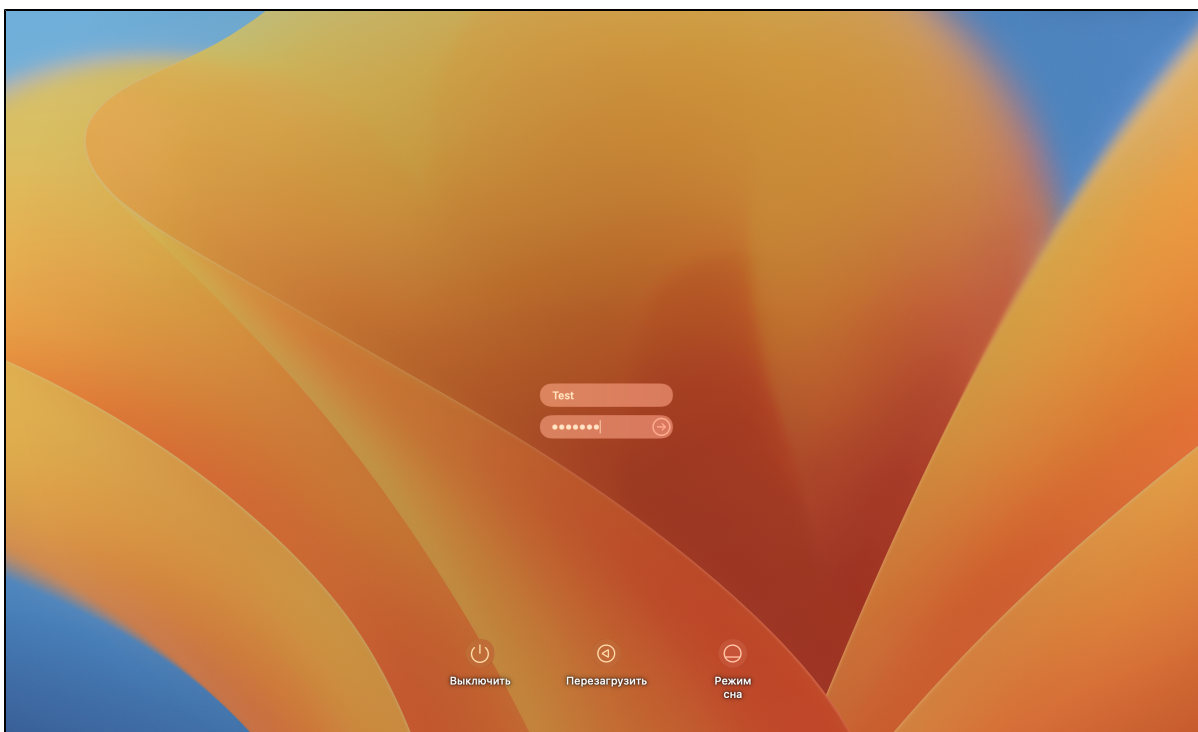
Настройка входа пользователя

Чтобы войти доменным пользователем:

1. В **Системных настройках** перейдите в **Экран блокировки**.
2. В разделе **При смене пользователя**, в строке **Показывать в окне входа**, выберите **поля имени и пароля**.



3. Перезагрузите компьютер. После перезагрузки вы сможете ввести логин и пароль доменного пользователя для входа.



4. После блокировки экрана или ухода компьютера в сон, потребуется PIN-код от Рутокен для возобновления сессии.

