



Инструкция по установке и настройке удалённого доступа к системе СА РАМ

Первое подключение

Перед первым подключением, с использованием системы удалённого доступа CA PAM, Вам необходимо проверить/выполнить следующие действия:

1. ИТ-заявка на удалённый доступ к системе согласована и исполнена
2. У Вас есть программный или аппаратный RSA ключ, генерирующий одноразовые пароли
3. Установлен и настроен VPN клиент (см. слайды 3-12)
4. Установлен и настроен CA PAM клиент (см. слайды 13-21)



Установка и настройка VPN клиента Check Point Endpoint Security VPN

Скачать дистрибутив можно по ссылке:

Для ОС Windows:

https://supportcenter.checkpoint.com/supportcenter/portal/role/supportcenterUser/page/default.psml/media-type/html?action=portlets.DCFileAction&eventSubmit_doGetdcdetails=&fileid=103038

Для ОС Mac OS:

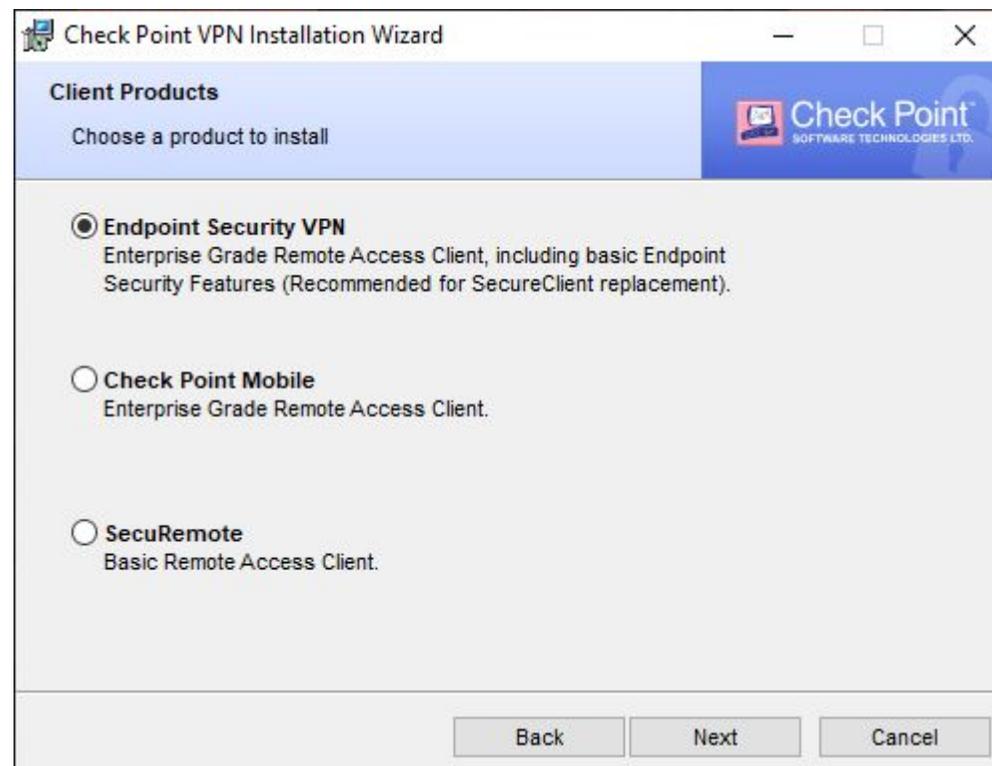
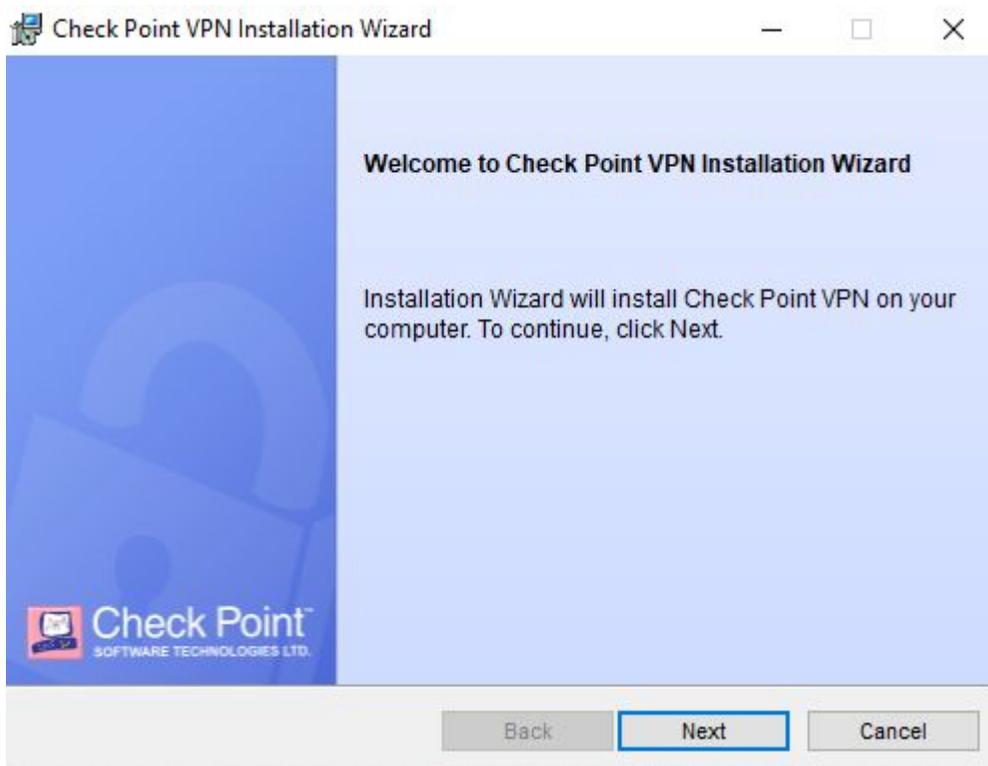
https://supportcenter.checkpoint.com/supportcenter/portal/user/anon/page/default.psml/media-type/html?action=portlets.DCFileAction&eventSubmit_doGetdcdetails=&fileid=96032

Установка VPN клиента

(выполняется единократно)



1. Запустите установку VPN клиента от имени администратора
2. Нажмите Next
3. Выберите Endpoint Security VPN и нажмите Next

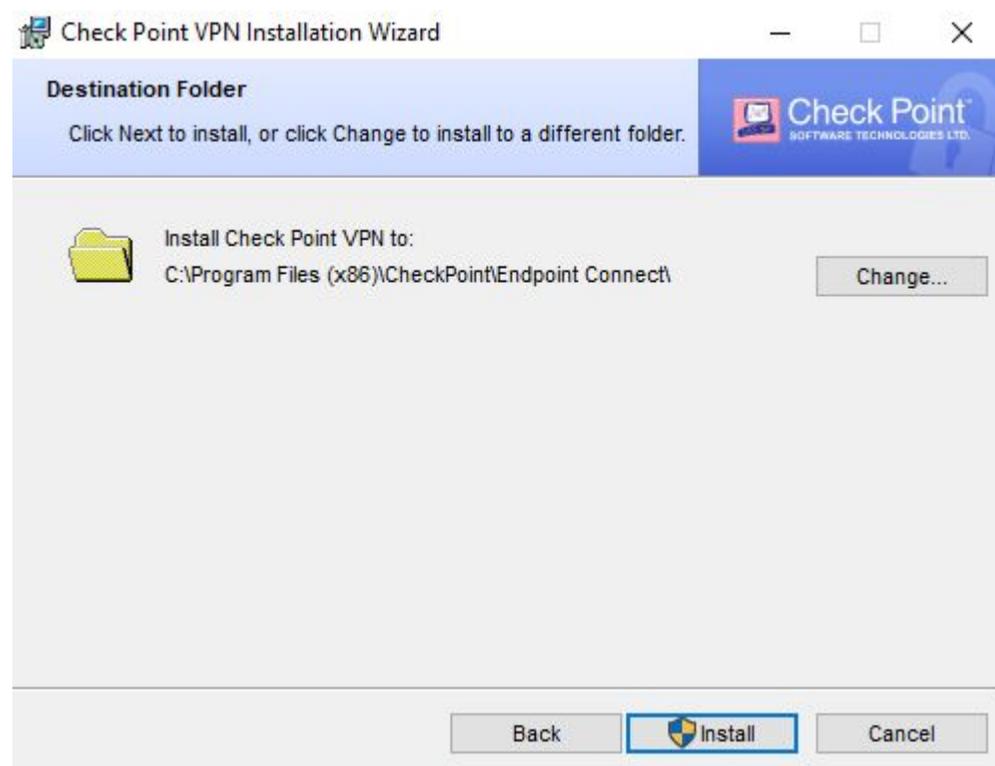
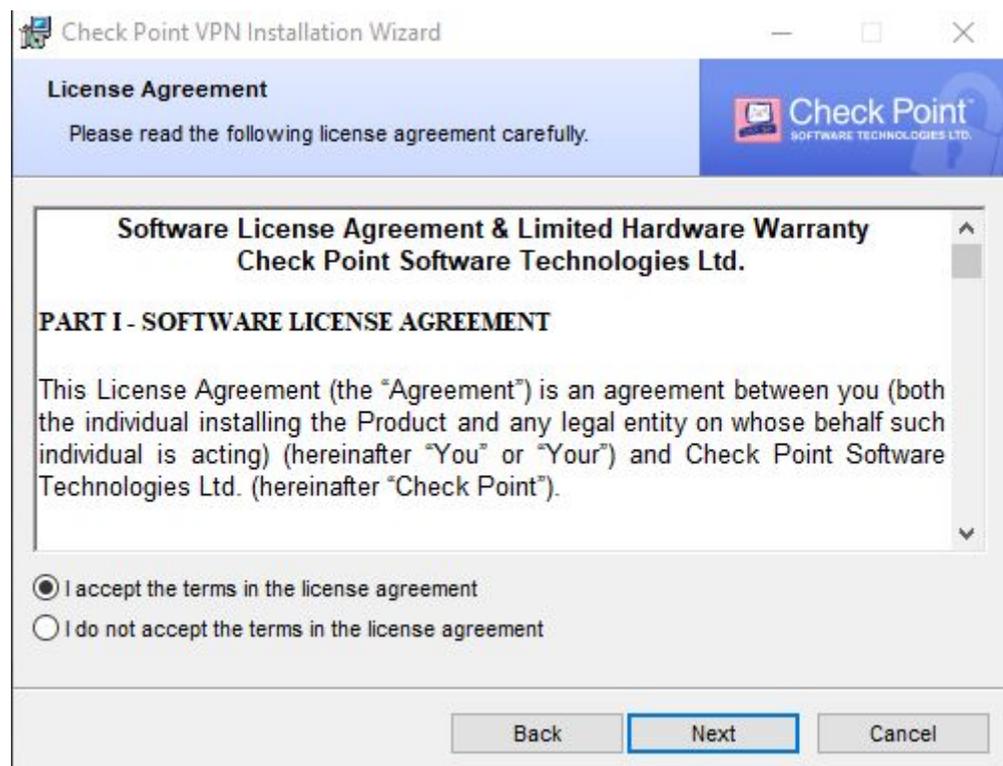


Установка VPN клиента

(выполняется единовременно)



4. Примите лицензионное соглашение
5. Выберите директорию для установки клиента
6. Нажмите Install и дождитесь окончания процесса установки

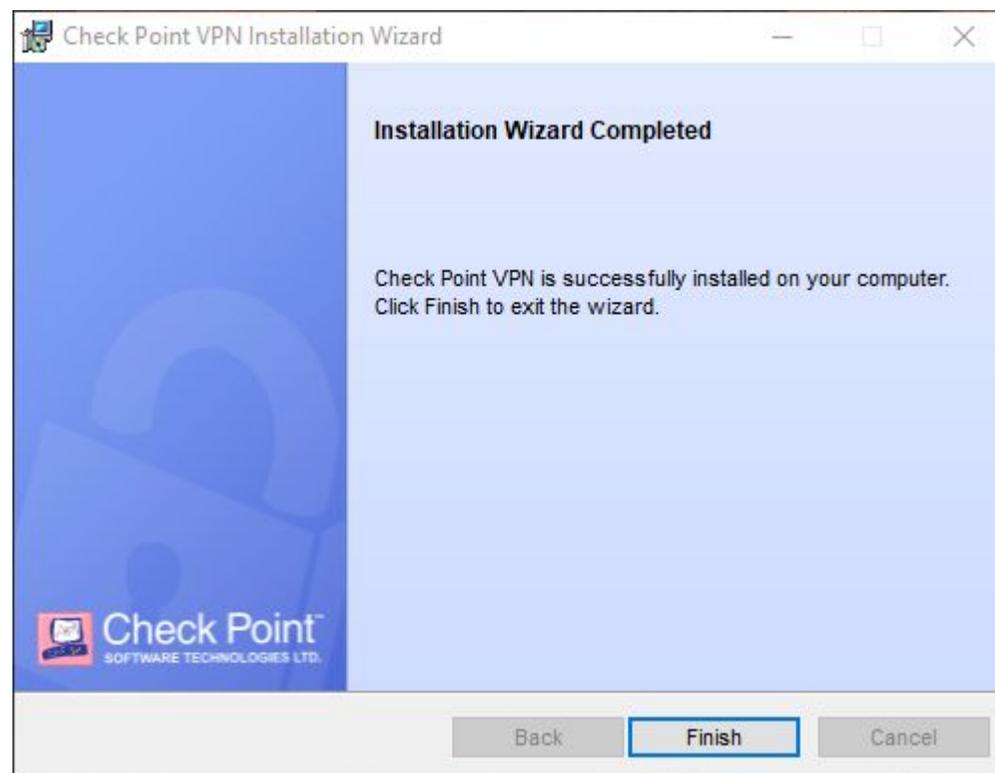
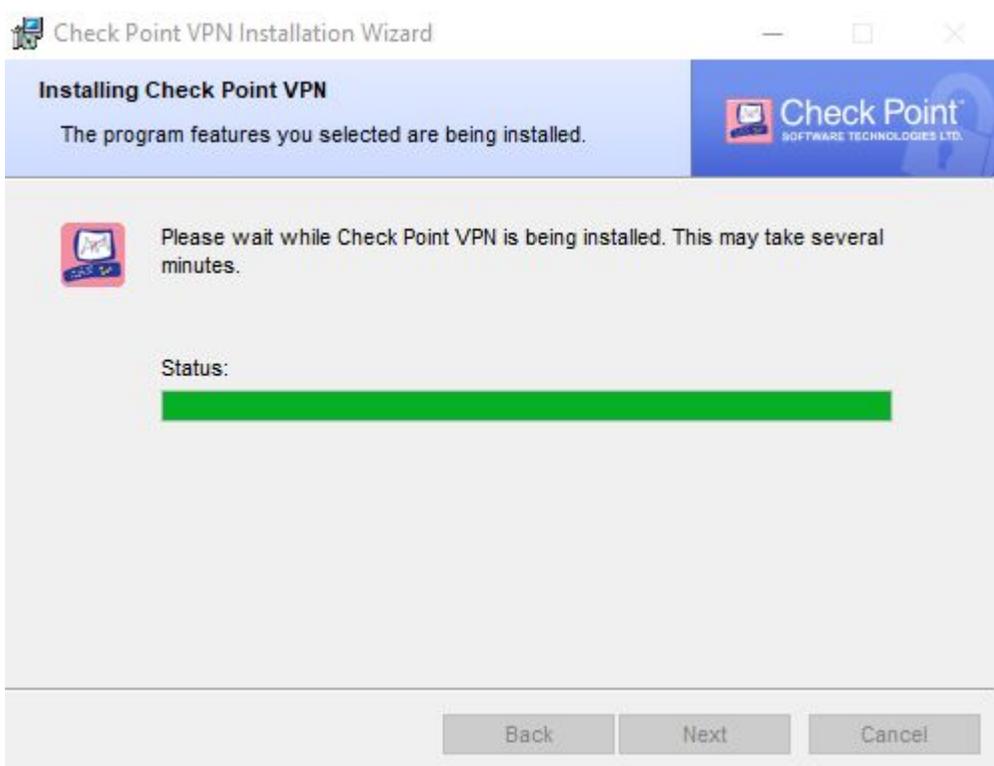


Установка VPN клиента

(выполняется единократно)



7. После завершения установки нажмите Finish и перезагрузите компьютер

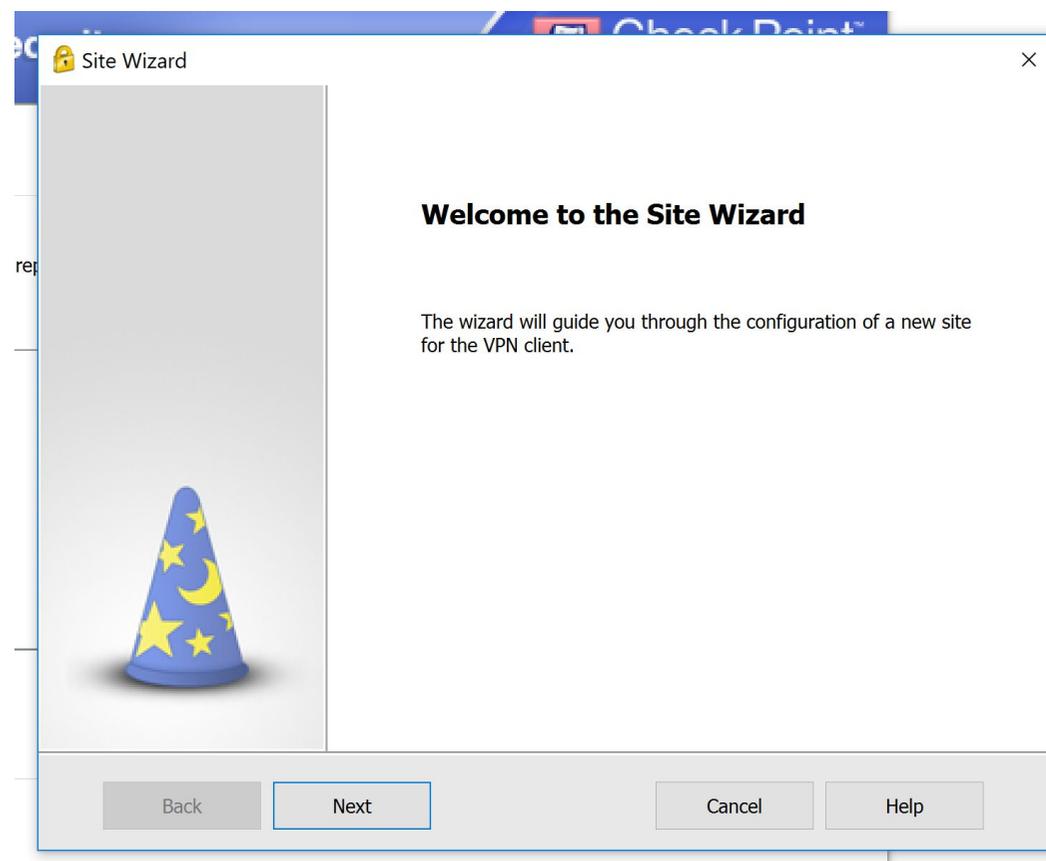
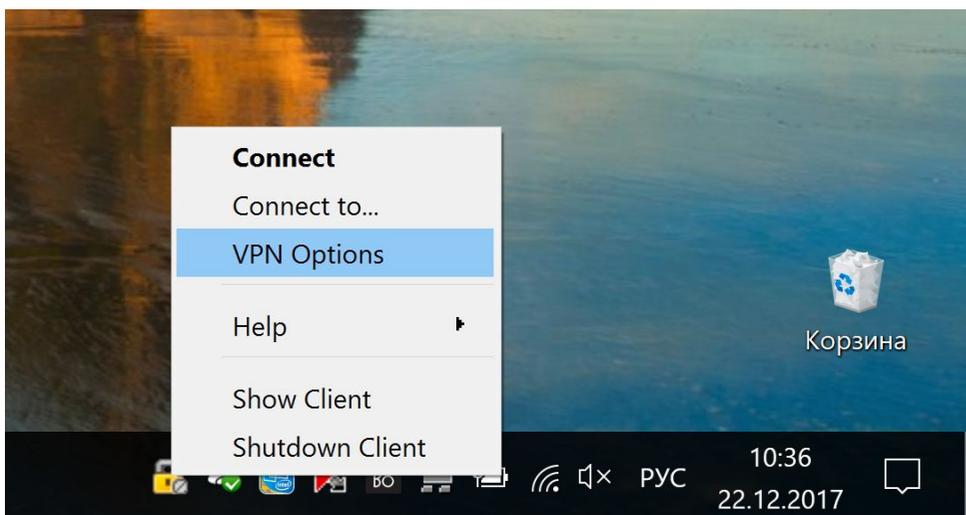


Настройка VPN клиента

(выполняется единоразово)



1. Запустите мастер настройки VPN из меню VPN Options
2. В открывшемся окне Sites нажмите New
3. В открывшемся окне Site Wizard нажмите Next



Настройка VPN клиента

(выполняется единократно)



4. Введите адрес шлюза: **217.12.96.114**
5. Введите название сайта в поле Display Name (опционально)
6. Нажмите Next

A screenshot of the 'Site Wizard' configuration window. The window title is 'Site Wizard'. It features a wizard icon and a lock icon. The main text reads 'Welcome to the Site Wizard' and 'A site is your gateway to network resources.' Below this, it says 'To continue, fill in the required information and click next.' There are two input fields: 'Server address or Name:' with the value '217.12.96.114' (highlighted by a red box) and 'Display name:' with the value 'CAPAM' (checked). At the bottom, there are four buttons: 'Back', 'Next', 'Cancel', and 'Help'.

Настройка VPN клиента

(выполняется единовременно)



7. Выберите Login Option – Standard (Default) и нажмите Next
8. Выберите SecurID Authentication – **Use Key FOB hard token**
9. Нажмите Next

Site Wizard

Login Option Selection
Select your login sequence choice from the options set by your administrator.

Please select your preferred login option from the following list

Standard (Default)

Back Next Cancel Help

Site Wizard

SecurID Authentication
Select your SecurID device type for authentication.

Use Key FOB hard token
This device connects easily to any key ring and fits into pocket or small carrying case.

Use PinPad card
Shaped as a credit card, the PinPad card contains a numeric keypad. The code displayed is a combination of the PIN and the current authenticator code.

Use SecurID software token
A software implementation of the SecurID authentication.

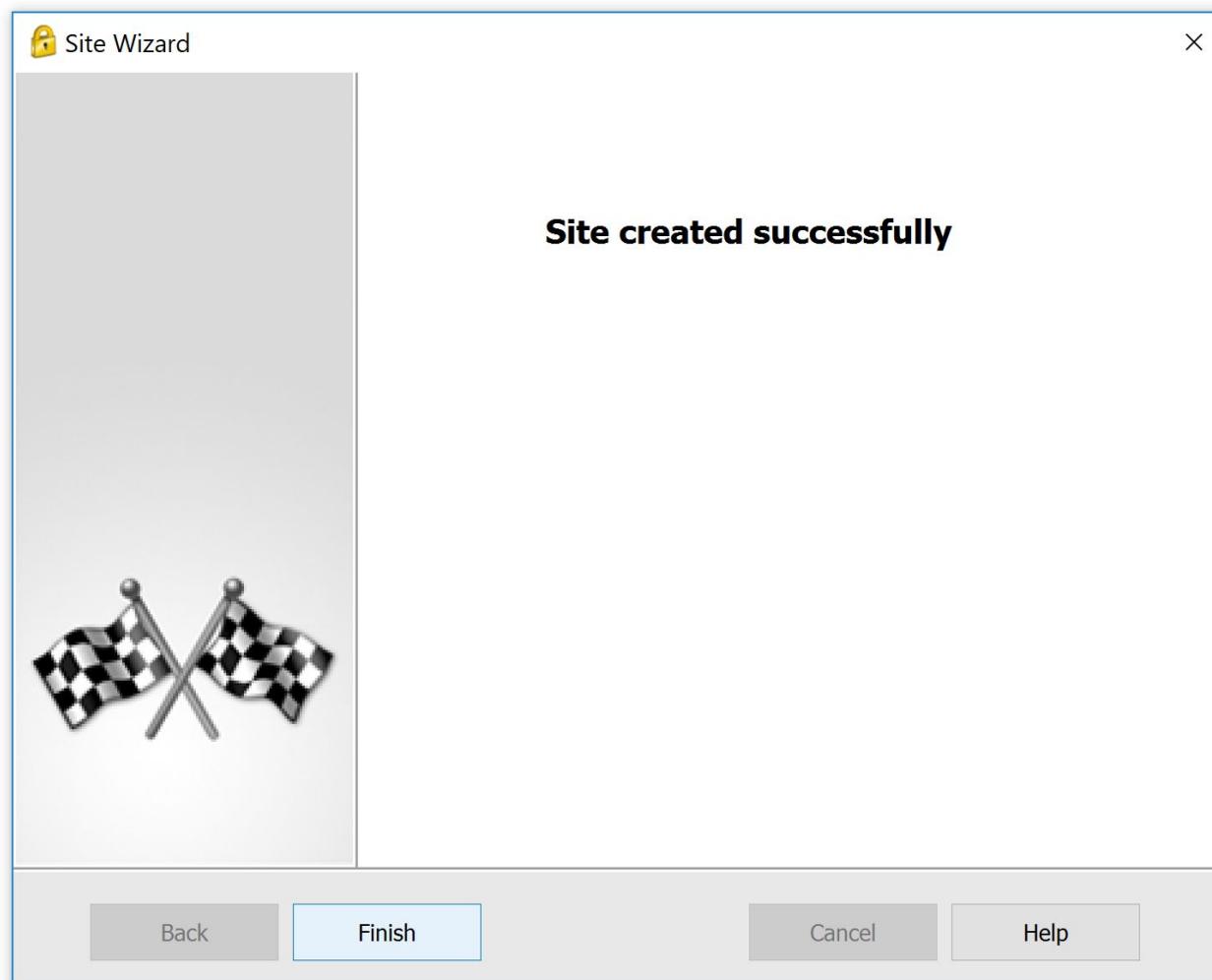
Back Next Cancel Help

Настройка VPN клиента

(выполняется единократно)



10. Нажмите Finish

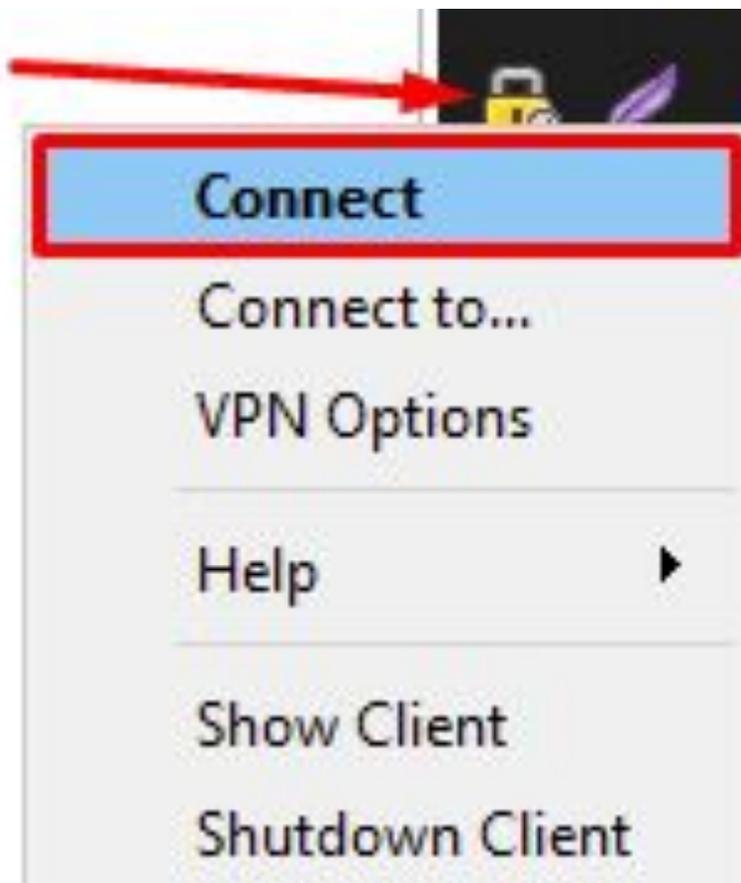


Установка VPN соединения

(выполняется при каждом подключении)



1. Откройте мастер подключения выбрав опцию Connect (значок клиента находится в трее)
2. Введите свои учетные данные и нажмите кнопку Connect



TrGUI

Endpoint Security

Check Point
SOFTWARE TECHNOLOGIES LTD.

Site: CAPAM

Authentication

Please enter your credentials:

Username: Ваша учетная запись в формате U_...

PIN: Пин-код, 4 цифры

Tokencode: Токен-код, 6 цифр

Connect Cancel Help

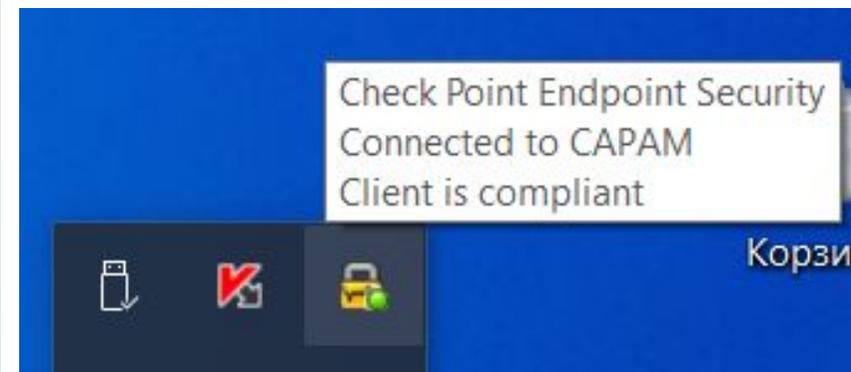
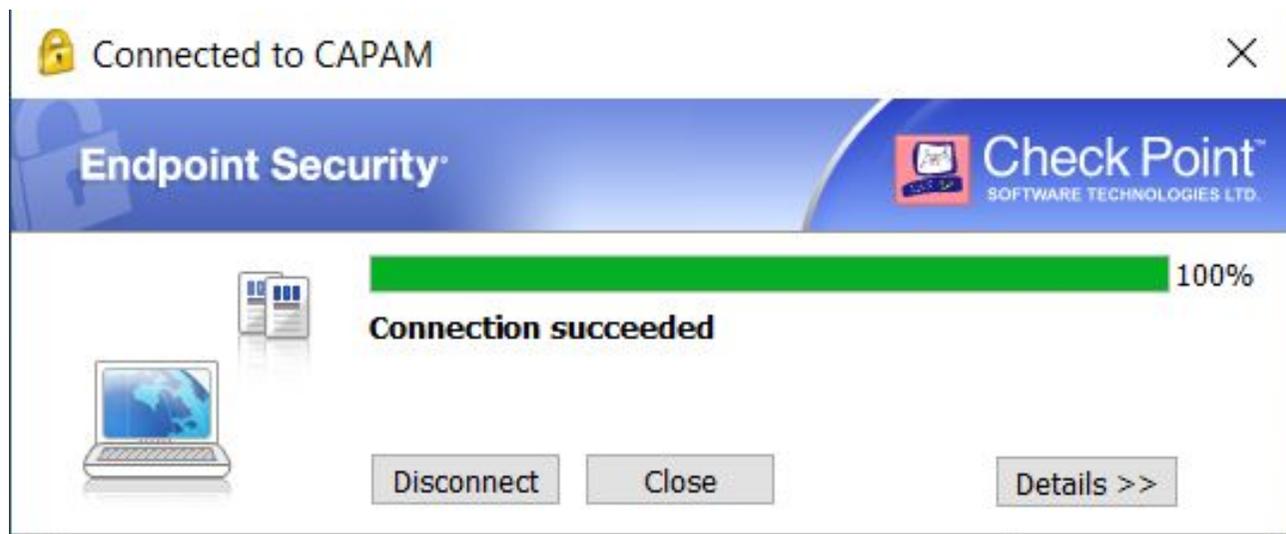
Selected Login Option: Standard [Change Login Option Settings](#)

Установка VPN соединения

(выполняется при каждом подключении)



3. Дождитесь успешного подключения в сеть Банка



Установка и настройка СА РАМ клиента

Скачать дистрибутив можно по ссылке:

Для ОС Windows:

https://d21oi5tjuccwe.cloudfront.net/ca-pam/install/win/CAPAMClientInstall_V2.8.0.exe

Для ОС Mac OS:

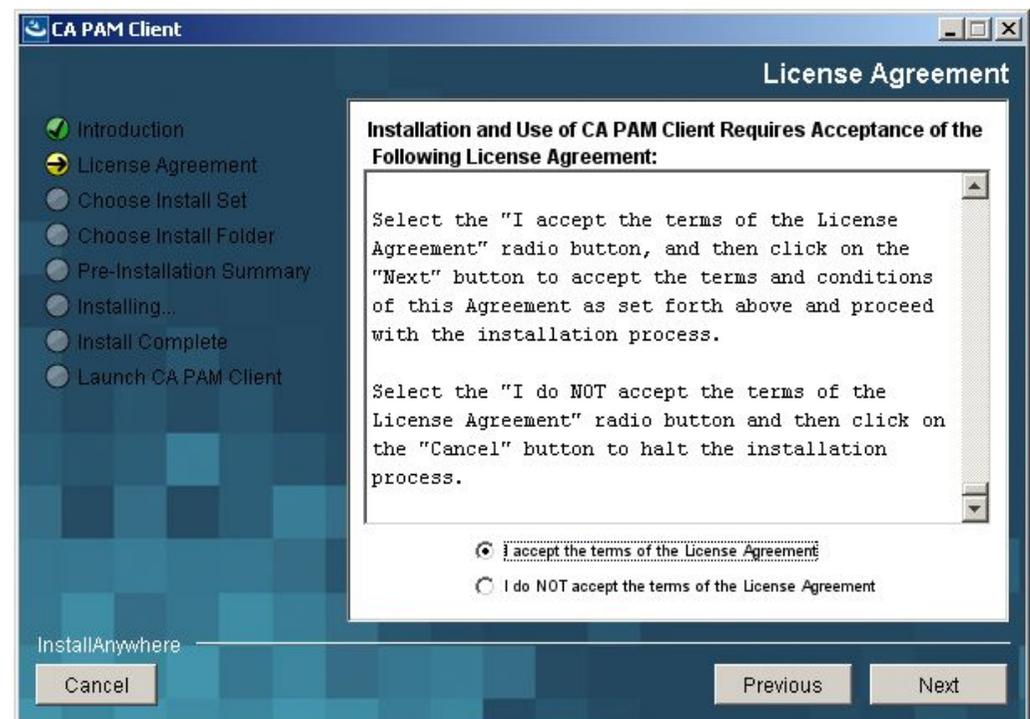
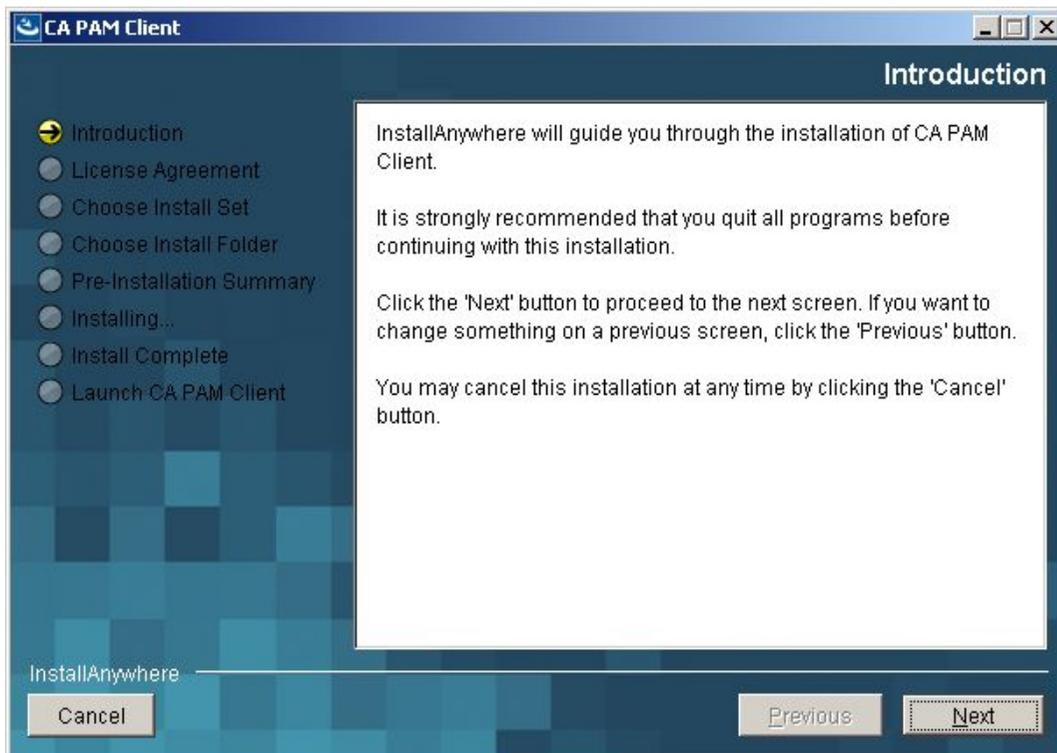
https://d21oi5tjuccwe.cloudfront.net/ca-pam/install/mac/CAPAMClientInstall_V2.8.0.zip

Установка СА РАМ клиента

(выполняется единократно)



1. Запустите установку СА РАМ клиента от имени администратора
2. Примите лицензионное соглашение, промотав текст в конец и нажмите Next



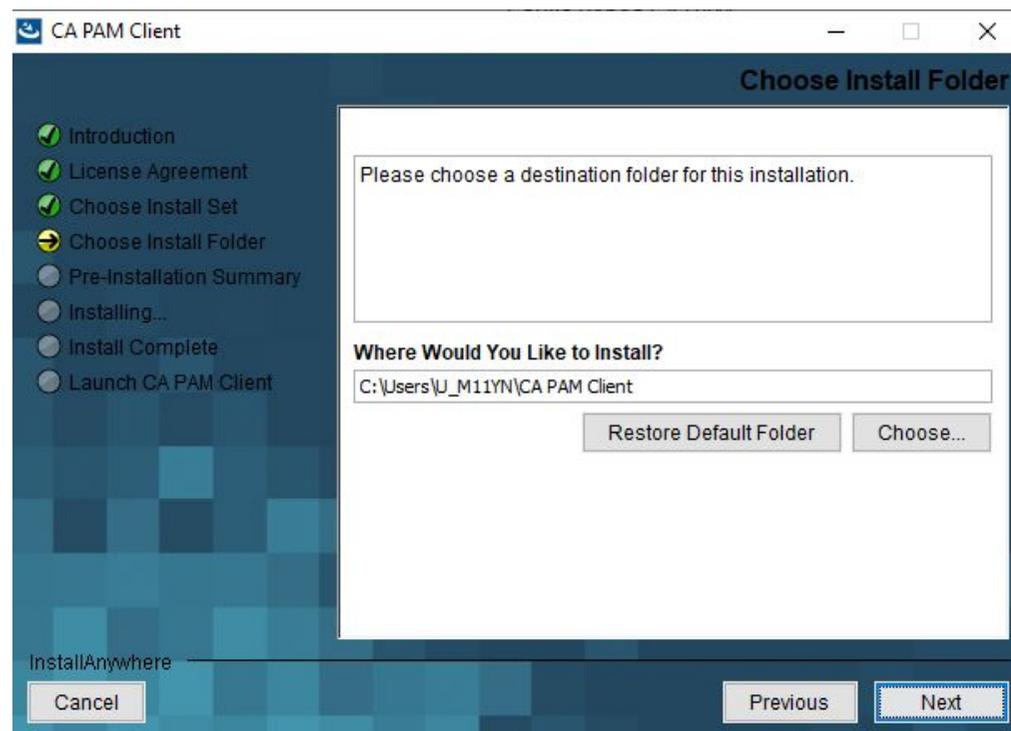
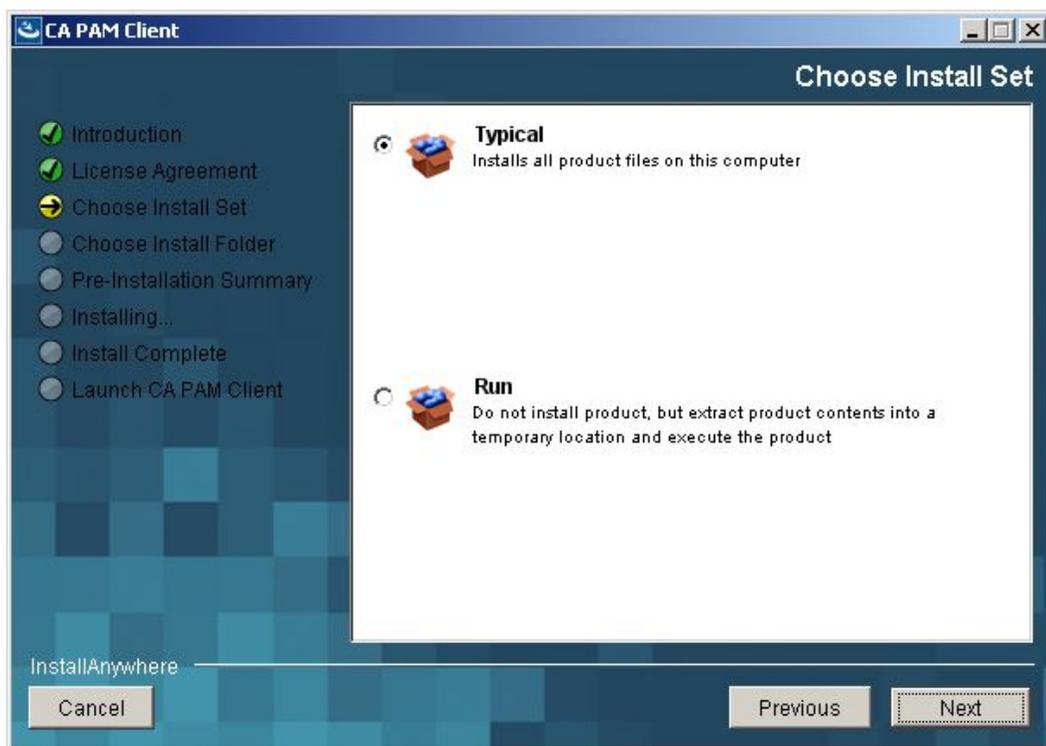
Установка CA PAM клиента

(выполняется единократно)



3. Выберите тип установки Typical

4. Укажите путь для установки CA PAM клиента
(рекомендуется оставить путь установки клиента по умолчанию)

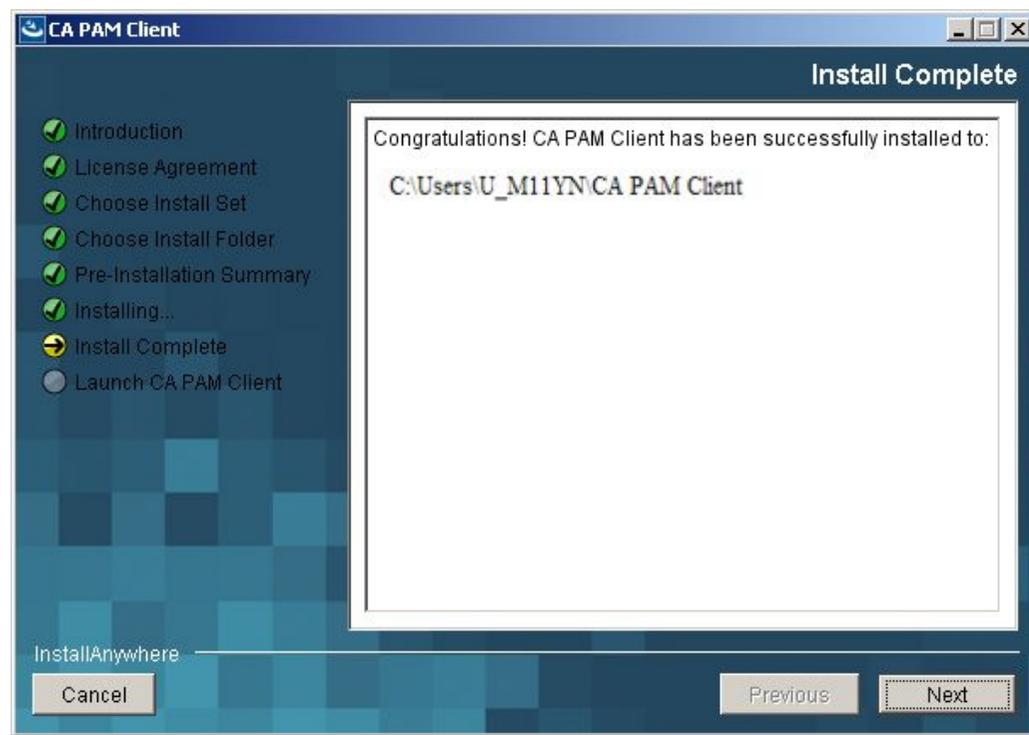
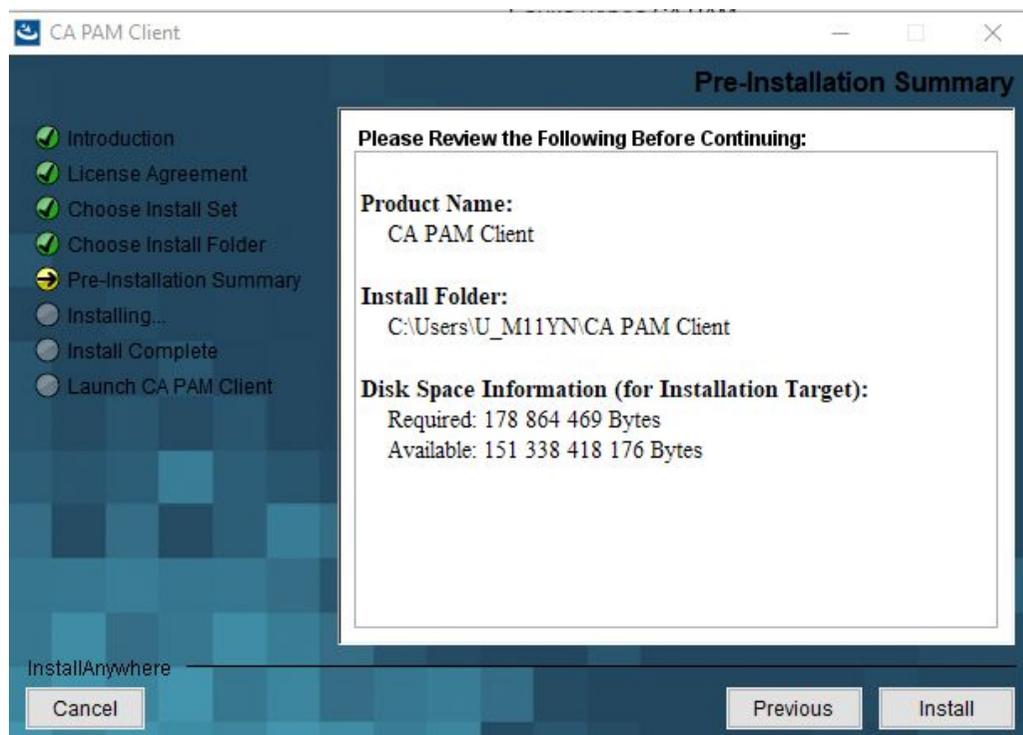


Установка CA PAM клиента

(выполняется единовременно)



5. Дождитесь завершения установки и убедитесь в том, что установка завершена успешно



Подключение к системе CA PAM

(выполняется при каждом подключении)

1. Запустите клиент CA PAM
2. Заполните данные подключения и нажмите Connect

Address: введите имя сервера CA PAM (**данная информация содержится в уведомлении об исполнении Вашей заявки от Service Manager**)

Имена серверов CA PAM:

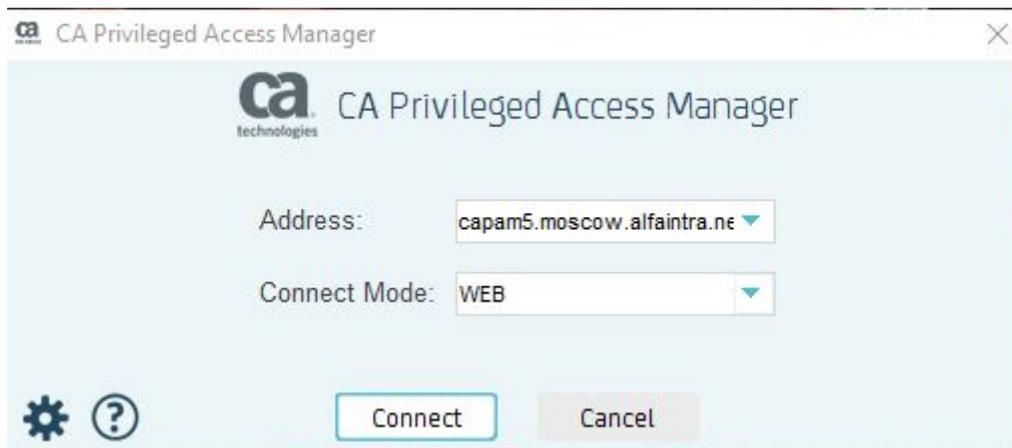
capam2.moscow.alfaintra.net

capam3.moscow.alfaintra.net

capam4.moscow.alfaintra.net

capam5.moscow.alfaintra.net

Connect Mode: выберите опцию WEB



Подключение к системе СА РАМ

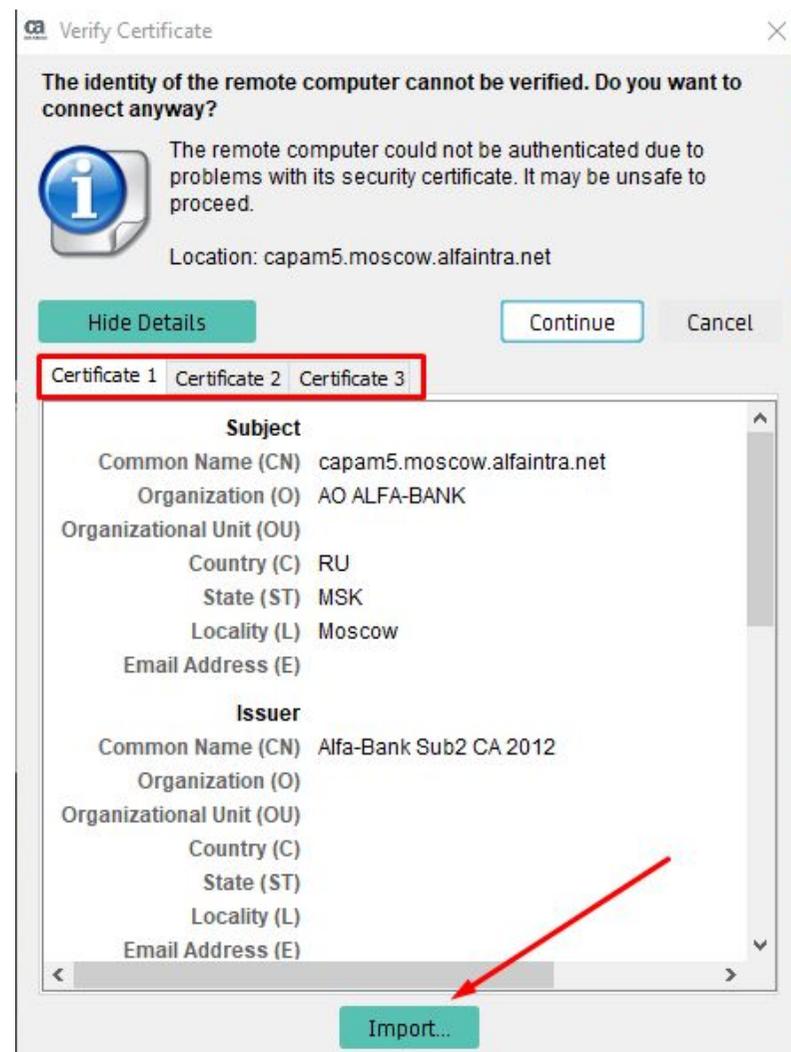
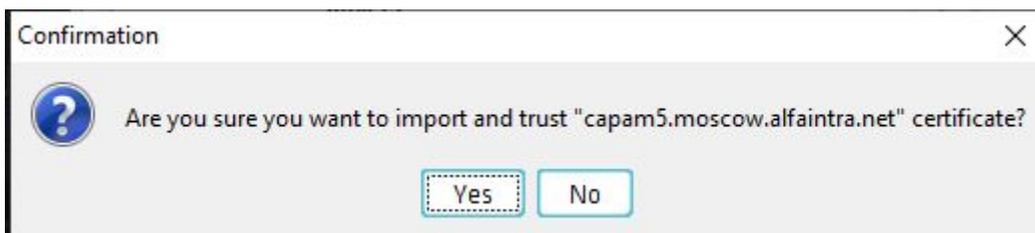
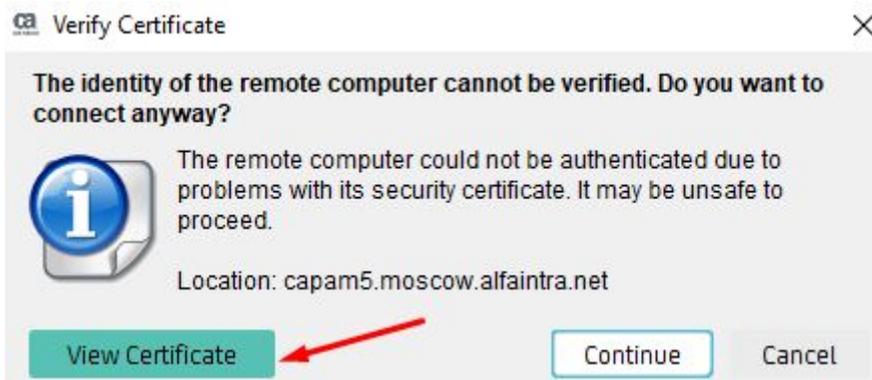
(выполняется при первом подключении)



3. Выполните импорт **всех** сертификатов, которые предлагаются клиентом

Для импорта сертификатов последовательно выполните следующие действия:

- нажмите кнопку View Certificate
- выберите вкладку Certificate 1 и нажмите Import, затем Yes
- выберите вкладку Certificate 2 и нажмите Import, затем Yes
- и так далее...
- нажмите кнопку Continue



Подключение к системе CA RAM

(выполняется при каждом подключении)

4. Обновите и перезапустите клиент



Подключение к системе CA PAM

(выполняется при каждом подключении)

4. Введите учётные данные и нажмите Login

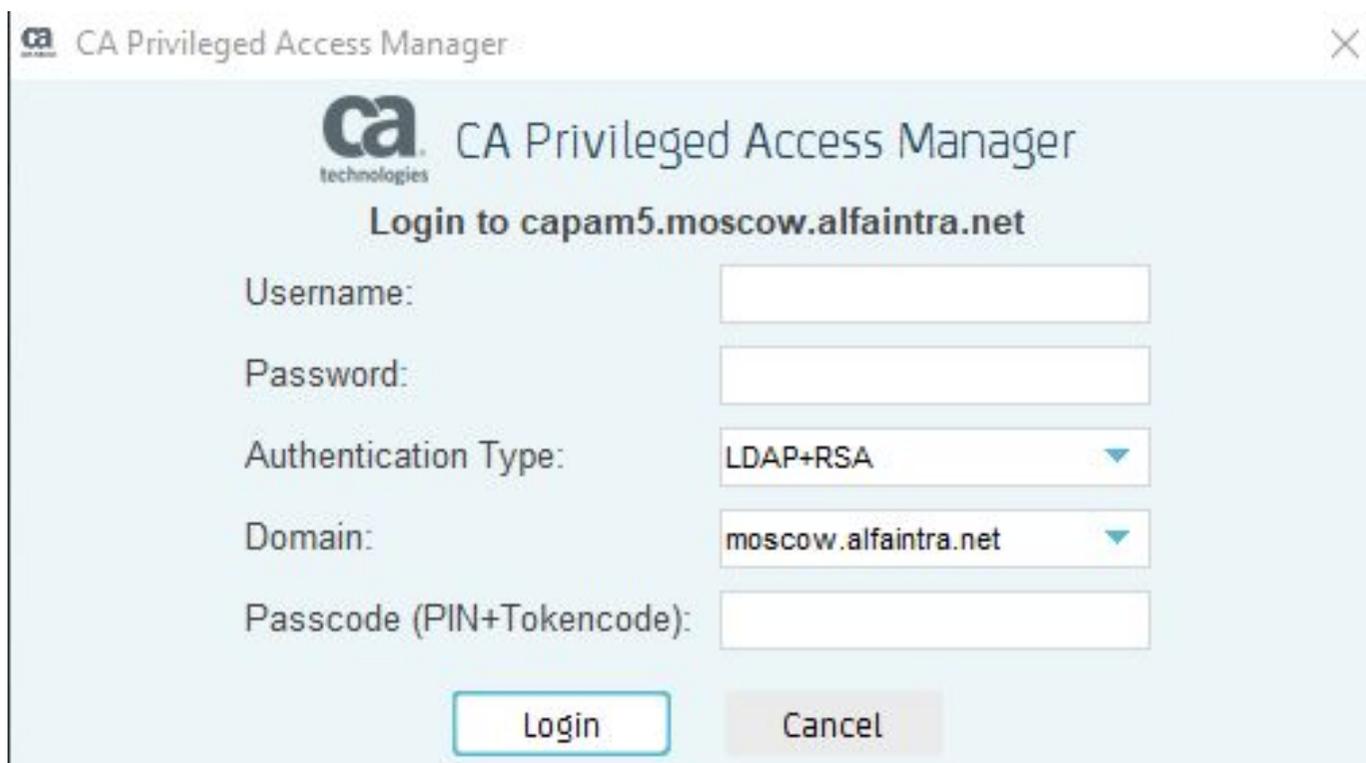
Username: введите общебанковскую учётную запись (u_...)

Password: введите общебанковский доменный пароль

Authentication Type: выберите опцию LDAP+RSA

Domain: выберите соответствующий вашей учётной записи домен

Passcode: введите в одном поле 4 цифры пин-кода и 6 цифр токена последовательно (отображаются в выданном Вам токене)



The screenshot shows a login dialog box for CA Privileged Access Manager. The window title is "CA Privileged Access Manager". The dialog contains the following fields and controls:

- CA logo and "CA Privileged Access Manager" text.
- Target URL: "Login to capam5.moscow.alfaintra.net"
- Username:
- Password:
- Authentication Type: (dropdown menu)
- Domain: (dropdown menu)
- Passcode (PIN+Tokencode):
- Buttons: "Login" and "Cancel"

Подключение к системе CA PAM

(выполняется при каждом подключении)



5. Убедитесь, что соединение успешно установлено и в списке присутствует Ваш рабочий ПК

6. Подключитесь к своему рабочему ПК

Для изменения размера окна необходимо задержать курсор на надписи rdp на 5 секунд, не нажимая кнопок мыши

