

Инструкция по получению удалённого доступа

- 1

Проверьте, что ваш компьютер соответствует необходимым требованиям
[Установка АВПО Касперский](#)

[Перейти к подробному описанию](#)
- 2

Установите сертификат с PKI
(если получили инструкцию не через портал <https://apps.sberbank.ru/>)

[Перейти к подробному описанию](#)
- 3

Сделайте заявку в ДРУГ на получение удалённого доступа

[Перейти к подробному описанию](#)
- 4

Установите приложение SberStore на мобильный телефон

[Перейти к подробному описанию](#)
- 5

Установите Cisco Anyconnect и Citrix Receiver

[Перейти к подробному описанию](#)
- 6

Подключите VPN с помощью Cisco Anyconnect и SberStore

[Перейти к подробному описанию](#)
- 7

Подключитесь к АРМ с помощью Citrix Receiver

[Перейти к подробному описанию](#)
- !

FAQ
Номер технической поддержки: **8-800-555-93-40**

[Перейти к подробному описанию](#)
- !

Ответственность пользователя при удалённом подключении

[Перейти к подробному описанию](#)

Данные шаги являются обязательными и последовательными для удалённой работы из дома.

Проверьте, что ваш компьютер соответствует необходимым требованиям

Личные устройства

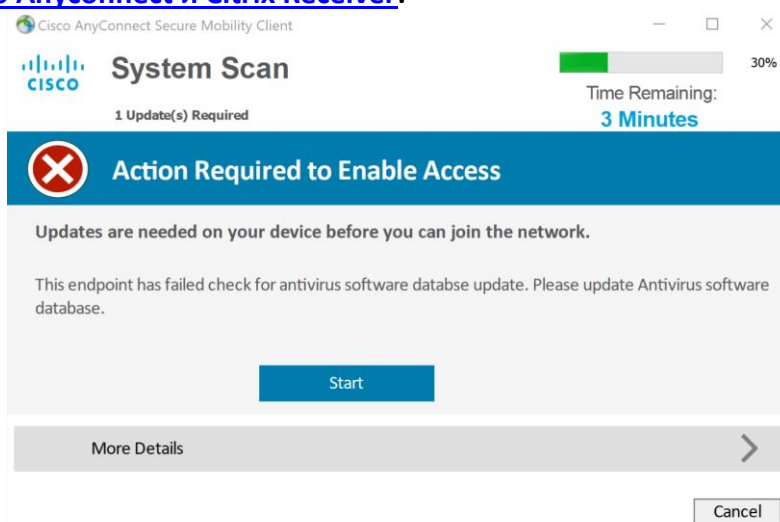
1. Компьютеры и ноутбуки под управлением ОС Windows

- Версия ОС Windows 7 и выше
- Наличие обновлений ОС
- Наличие АБПО следующих производителей:
 - Kaspersky Lab (либо установите корпоративный антивирус)
 - Agnitum Ltd. (Outpost)
 - AVAST Software a.s.
 - AVG Technologies CZ, s.r.o.
 - Avira GmbH
 - Bitdefender
 - Check Point Software Technologies
 - COMODO Security Solutions
 - Doctor Web, Ltd.
 - ESET
 - F-Secure Corporation
 - Lavasoft
 - Malwarebytes Corporation
 - Microsoft Corporation
 - Panda Security, S.L.
 - Sophos Limited
- Актуальность баз АБПО не более 3 дней
- Браузеры: Yandex, Chrome, IE11

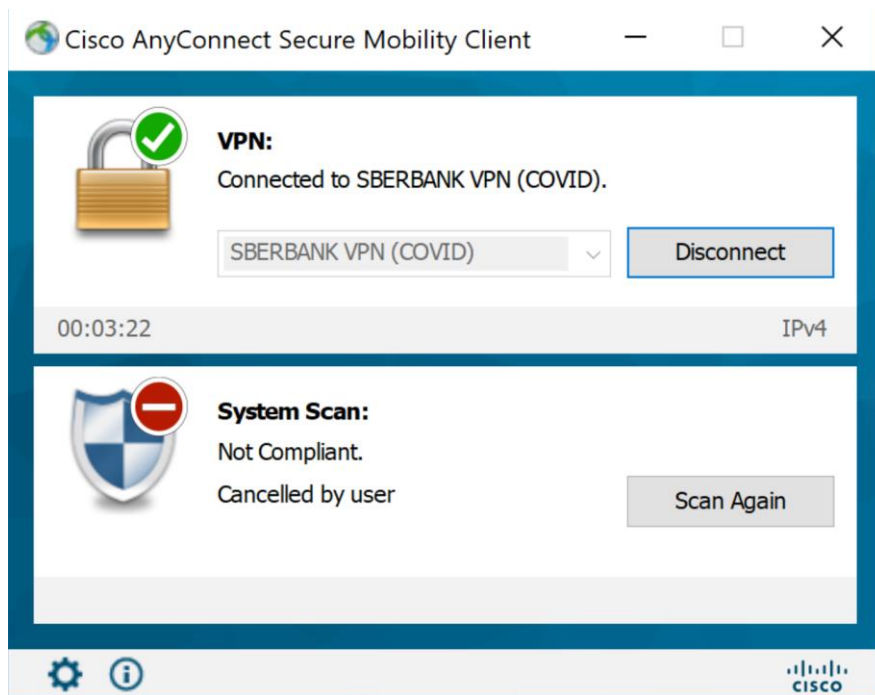
2. Устройства под управлением MacOS

- Версия ОС 10.13 (High Sierra) и выше

Если Ваш ПК НЕ соответствует требованиям безопасности, возникнет следующее сообщение при попытке установить [Cisco Anyconnect](#) и [Citrix Receiver](#):

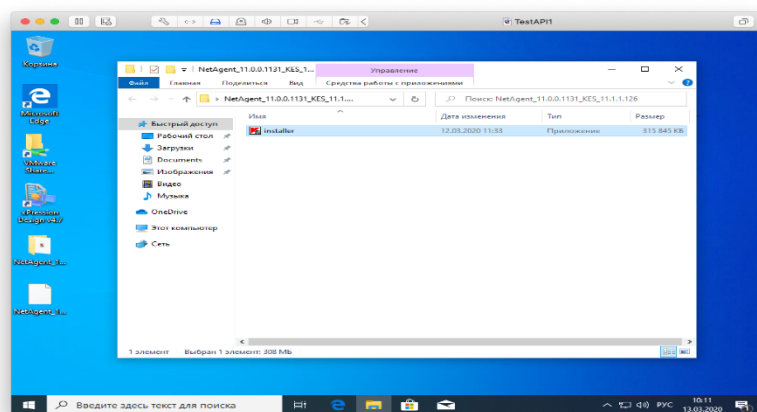


До приведения ПК в соответствие требованиям безопасности будет возникать такое сообщение:

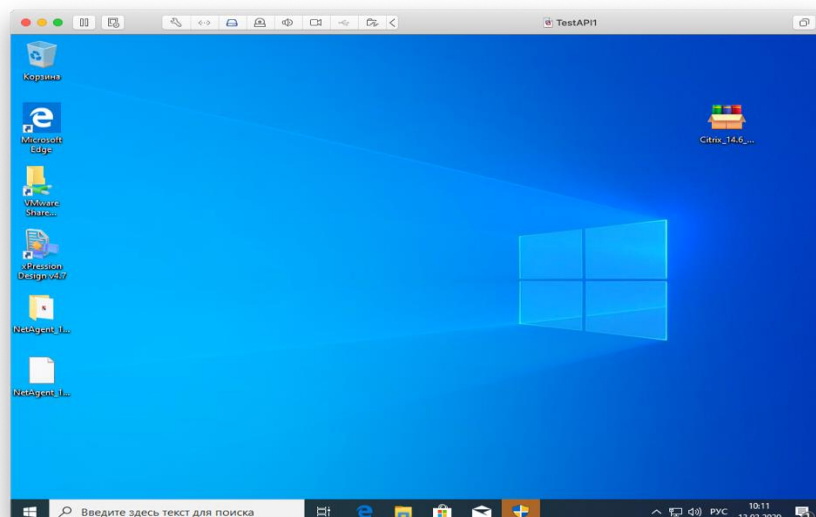


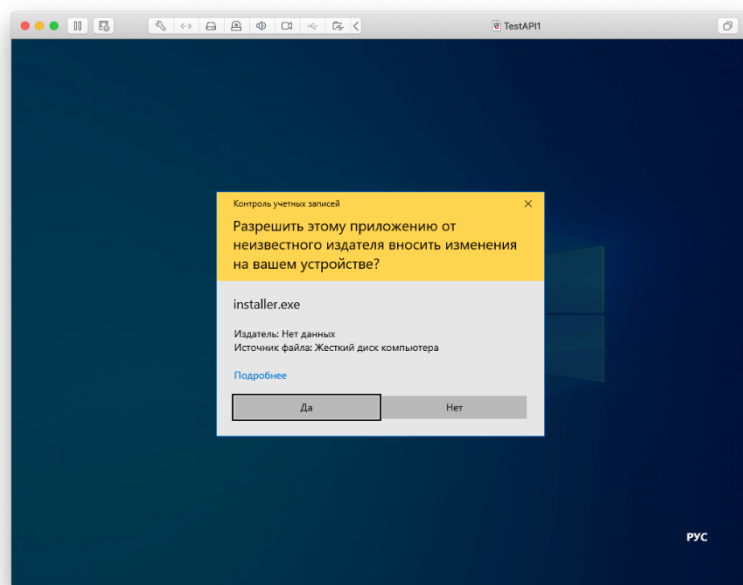
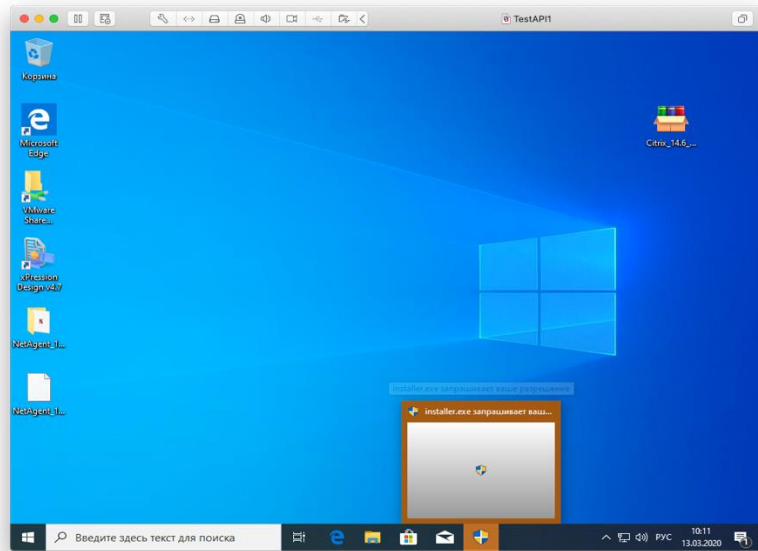
При необходимости, у Вас есть возможность воспользоваться корпоративным антивирусом на личном устройстве.

- Скачайте установочный пакет с АВПО Касперский по ссылке:
<https://files.apps.sberbank.ru/ci01528000-epromlg-sberstoreprod/portal/AVPO.exe>
- Запустите пакет с установкой АВПО Касперский

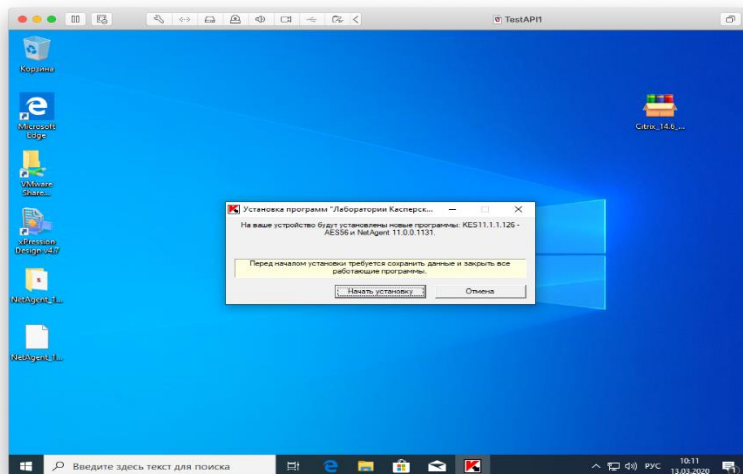


- В случае появления окна с подтверждением нажмите «Да»

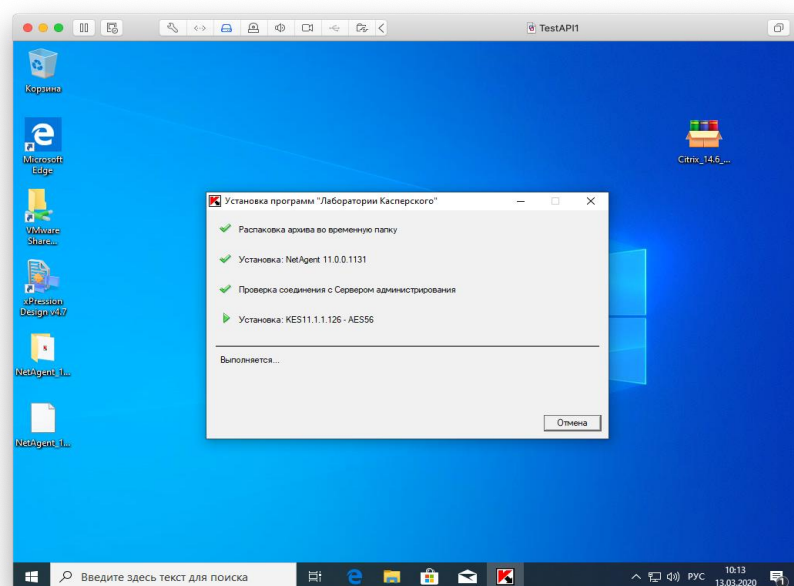
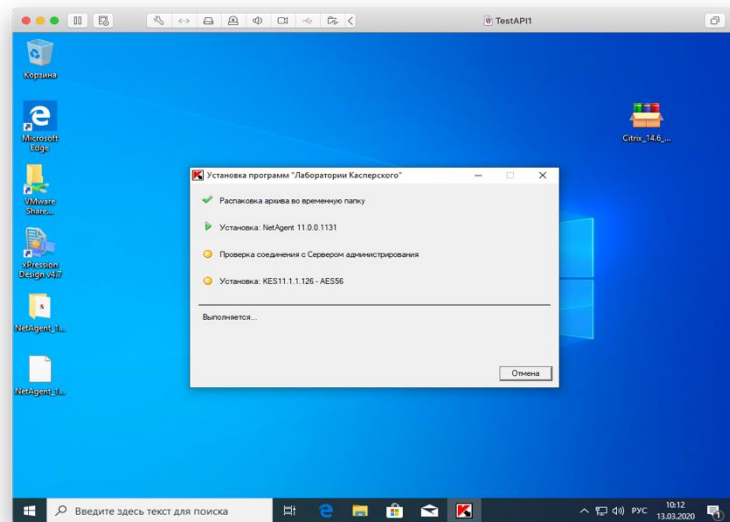
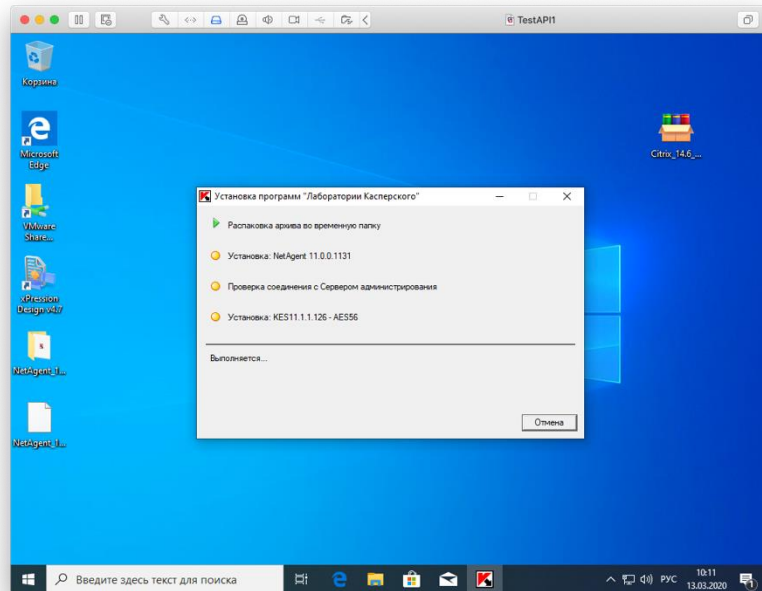


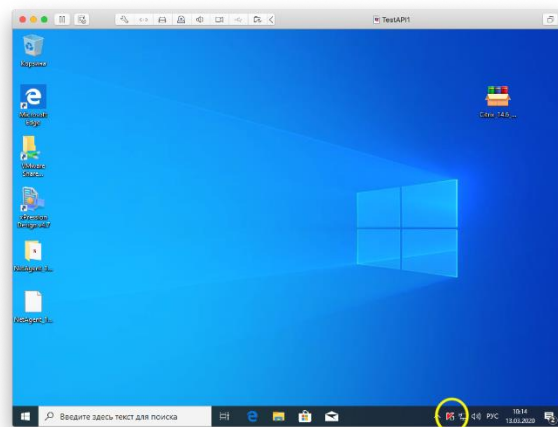
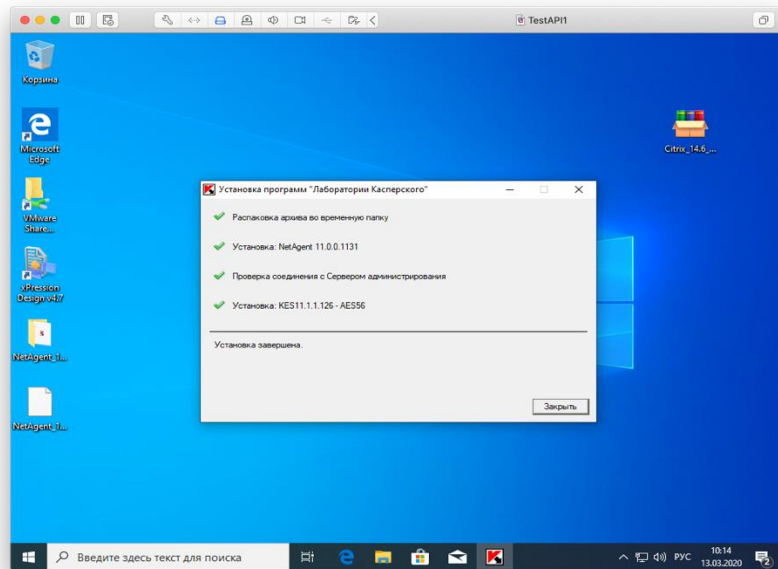


- Сохраните все свои файлы и нажмите «Начать установку»



- Наблюдайте





- Готово.

[Вернуться к Оглавлению.](#)

Установите сертификат с PKI

Данный шаг требуется выполнить, если вы получили инструкцию не через портал <https://apps.sberbank.ru/>.

Для обеспечения работы в режиме удалённого доступа вам необходимо установить на компьютер личный сертификат, подписанный удостоверяющим центром Сбербанка.

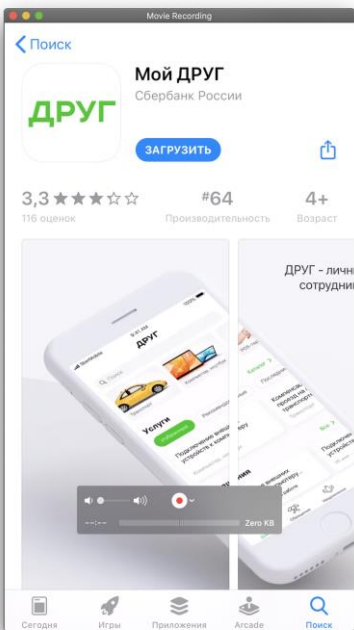
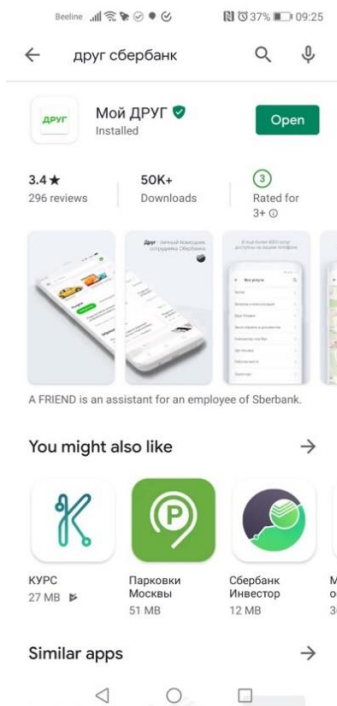
Для того, чтобы установить сертификат, перейдите на сайт <https://pki.sberbank.ru/> , и следуйте выложенным там инструкциям.

[Вернуться к Оглавлению.](#)

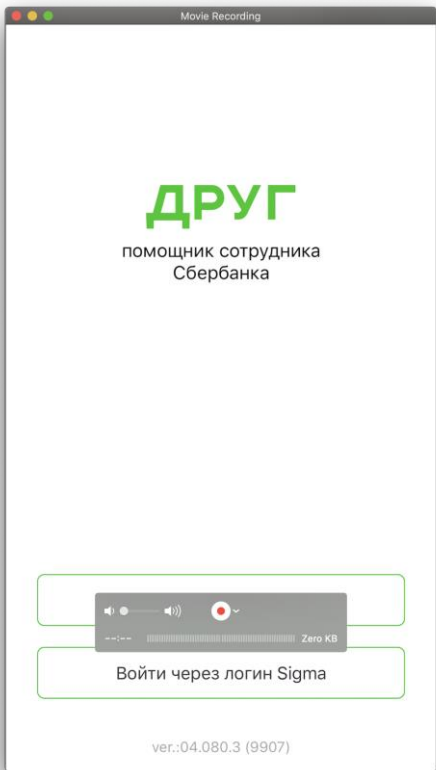
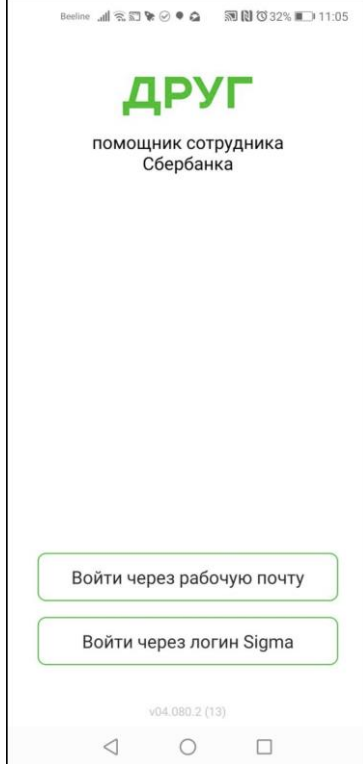
Сделайте заявку в ДРУГ на получение удалённого доступа

Данный шаг является обязательным для всех сотрудников, кому нужен удалённый доступ.

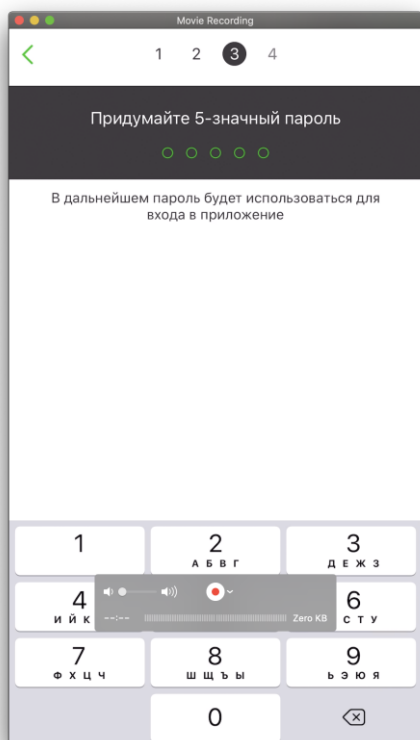
Для того, чтобы создать заявку на получение удаленного доступа из дома, установите приложение Мой ДРУГ на ваш мобильный телефон.

Для iOS	Для Android
https://apps.apple.com/ru/app/id1447496171	https://play.google.com/store/apps/details?id=ru.sberbank.sbfriend
	

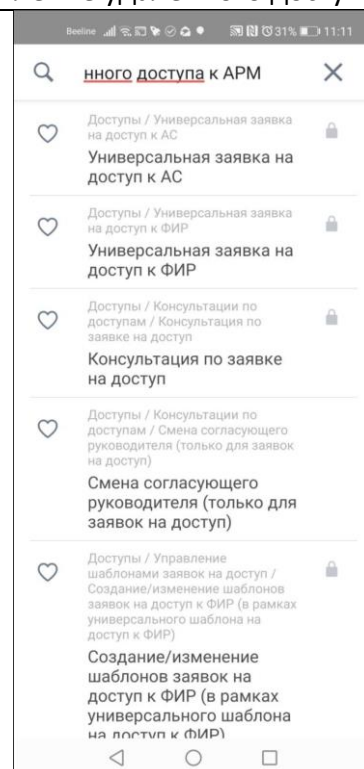
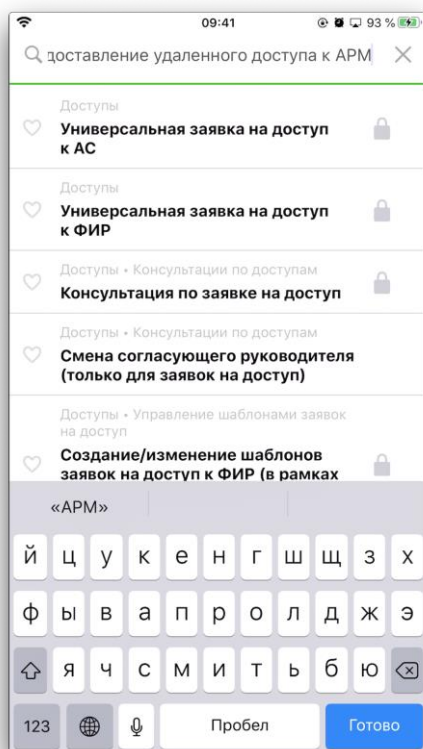
Авторизуйтесь в приложении при помощи вашей рабочей почты или логина Sigma.

	
---	--

Задайте пин-код и разрешите использование биометрических параметров для входа.



Воспользуйтесь поиском и найдите шаблон заявки «Предоставление удаленного доступа к АРМ».



Заполните поля в шаблоне, указав свои данные, куда требуется доступ и обоснование.

В поле «Логин сотрудника в выбранном домене» требуется всегда указывать логин Сигма.

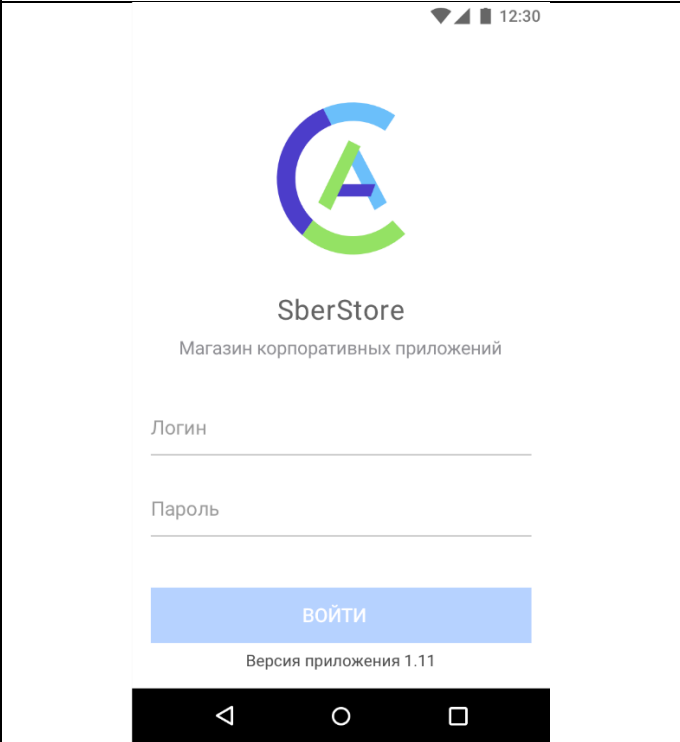
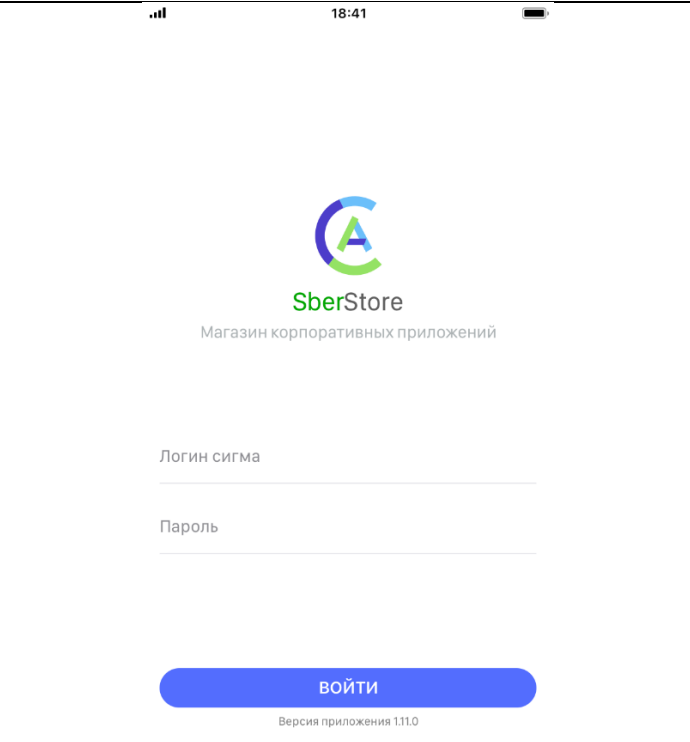
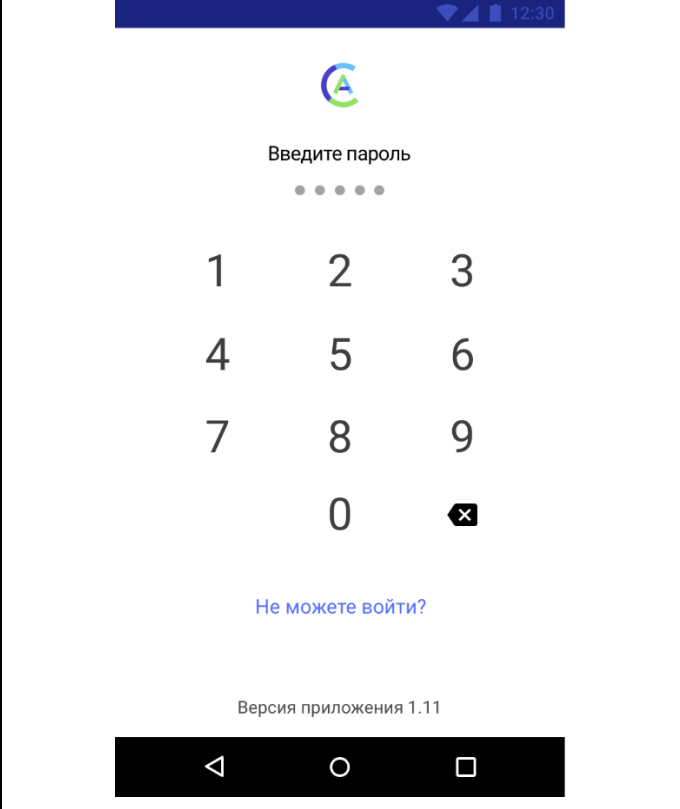
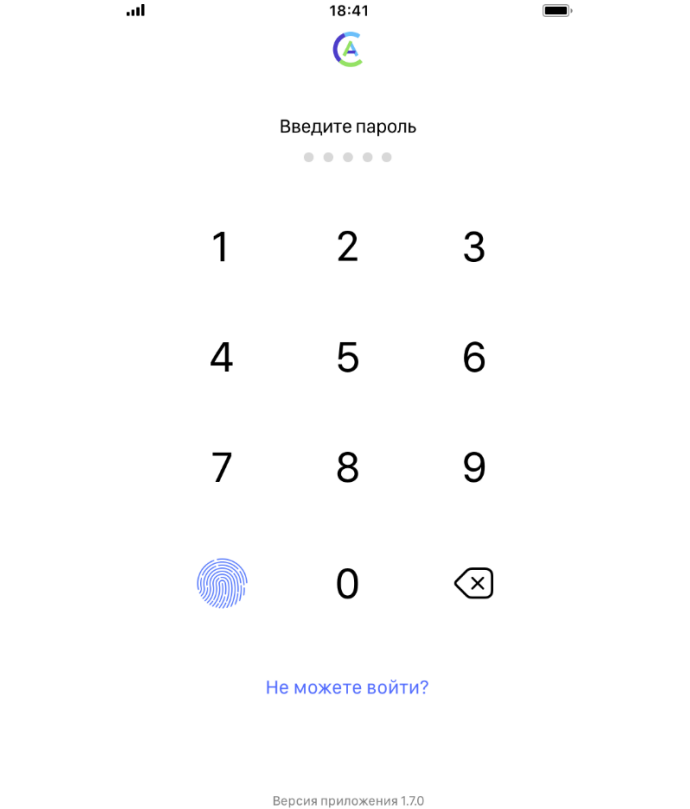
Нажмите кнопку «Создать обращение». Ваш запрос будет передан **на согласование непосредственному руководителю**, а затем на обработку.

По результатам выполнения запроса вам поступит уведомление на мобильный телефон.

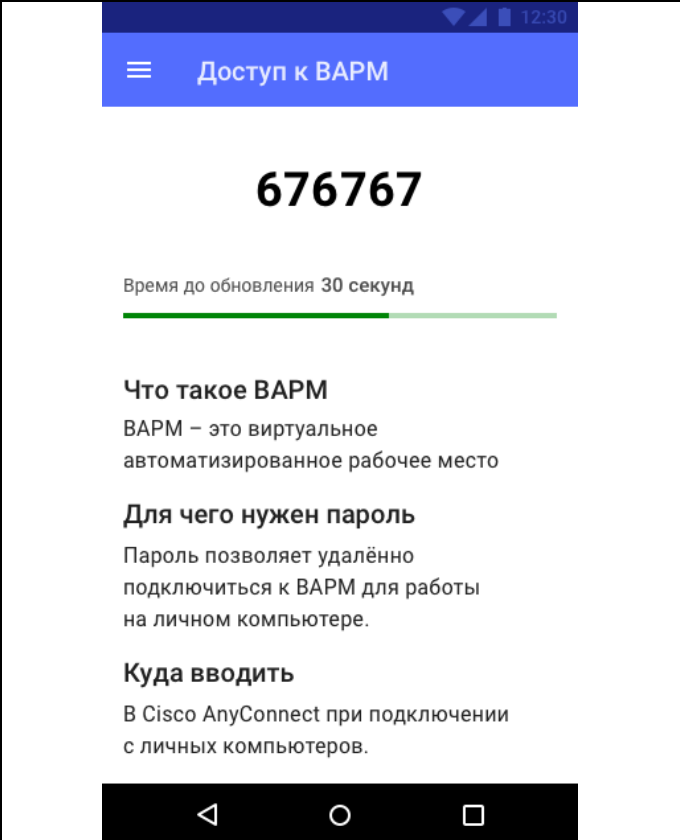
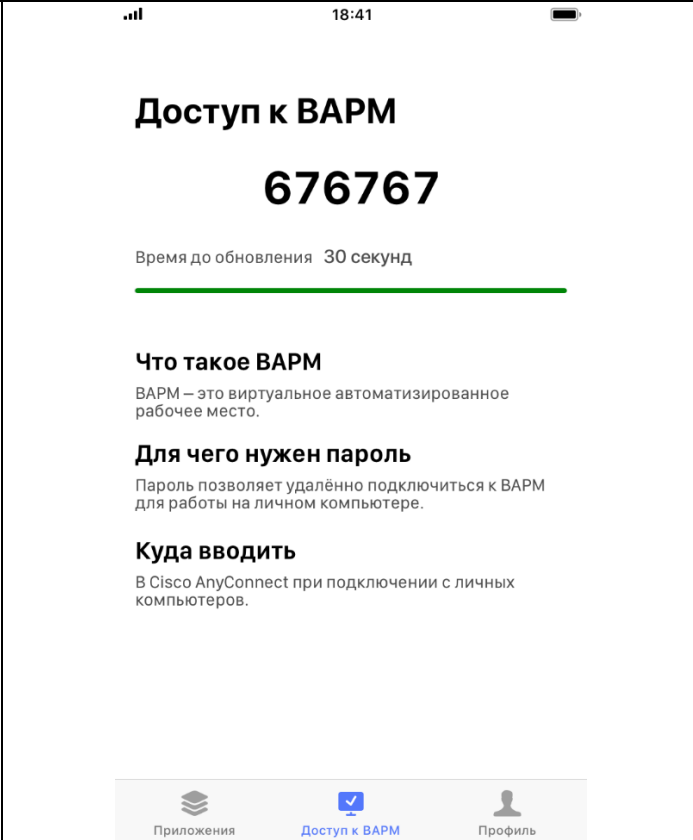
[Вернуться к Оглавлению.](#)

Установите приложение SberStore на мобильный телефон

Для получения одноразового пароля, необходимого при аутентификации при удалённом подключении, установите приложение SberStore на мобильный телефон.

Для Android для версии 5+	Для iOS для версии 11+
https://apps.sberbank.ru/instruction/android	https://apps.sberbank.ru/instruction/ios
При первом входе введите логин-пароль от вашей учётной записи Sigma.	
	
Установите и подтвердите пин-код для входа в приложение.	
	
Перейдите в меню слева и выберите «Доступ к ВАРМ».	Перейдите на вкладку "Доступ к ВАРМ", используя переключатели в нижней части экрана, и получите одноразовый пароль,

состоящий из шести цифр. Пароль, отображаемый на данном экране, потребуется вам для последующего подключения VPN с помощью Cisco Anyconnect.

	
---	---

[Вернуться к Оглавлению.](#)

Установите Cisco Anyconnect и Citrix Receiver

Вам необходимо установить программное обеспечение Cisco Anyconnect и Citrix Receiver самостоятельно, с помощью специально подготовленного комбо-пакета.

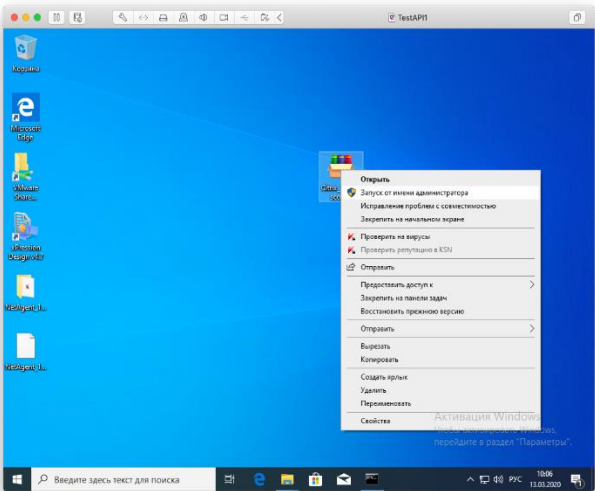
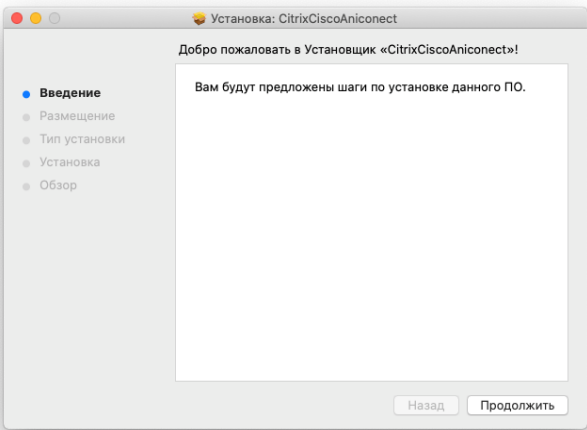
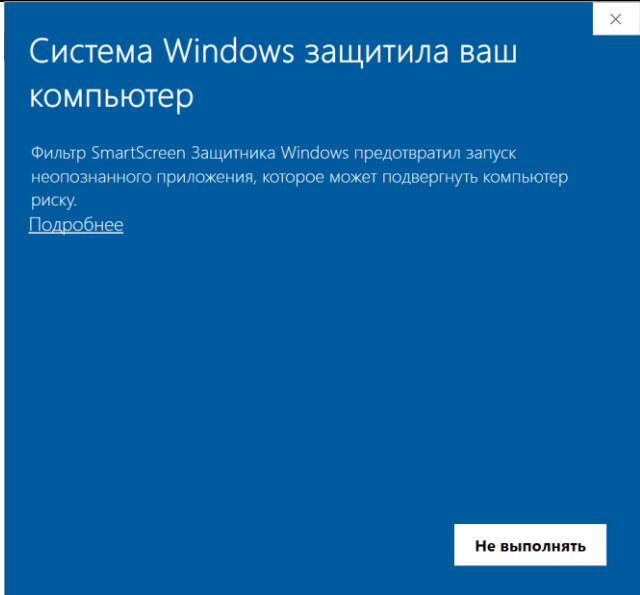
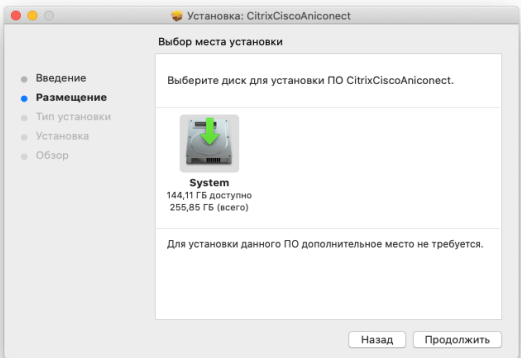
Данный шаг является обязательным для всех сотрудников, кому нужен удалённый доступ, даже если ранее на вашем компьютере была установлена одна из программ.

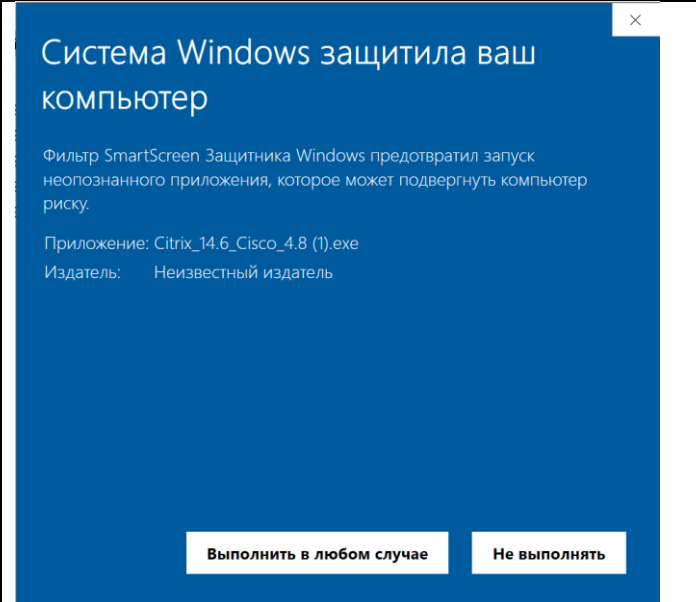
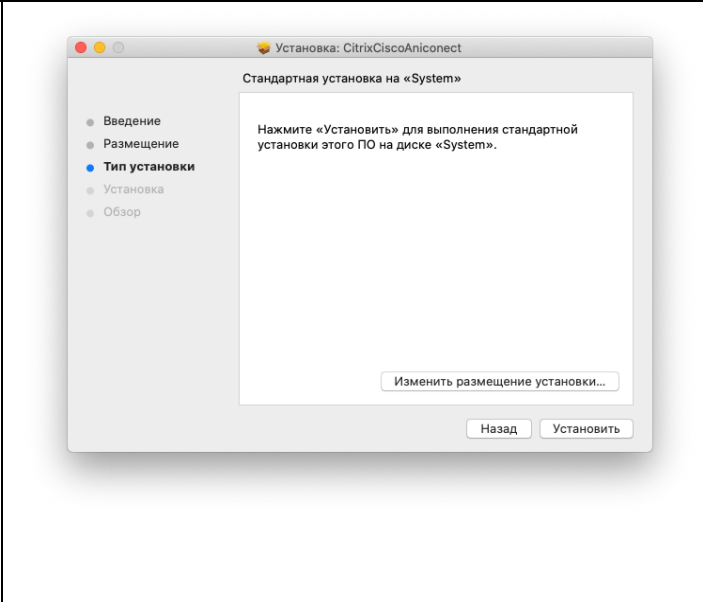
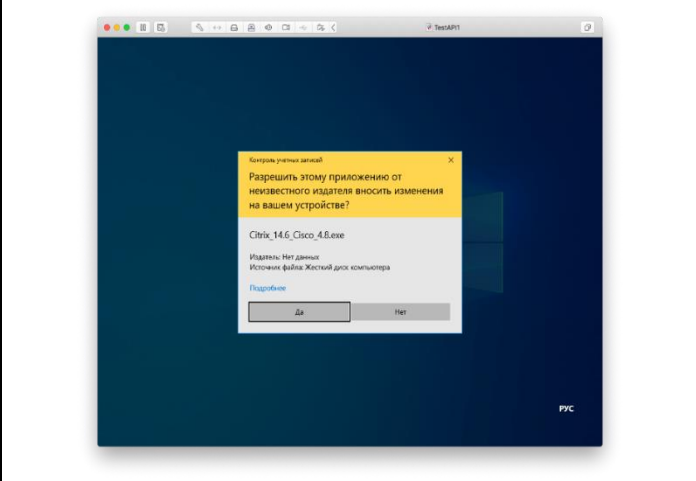
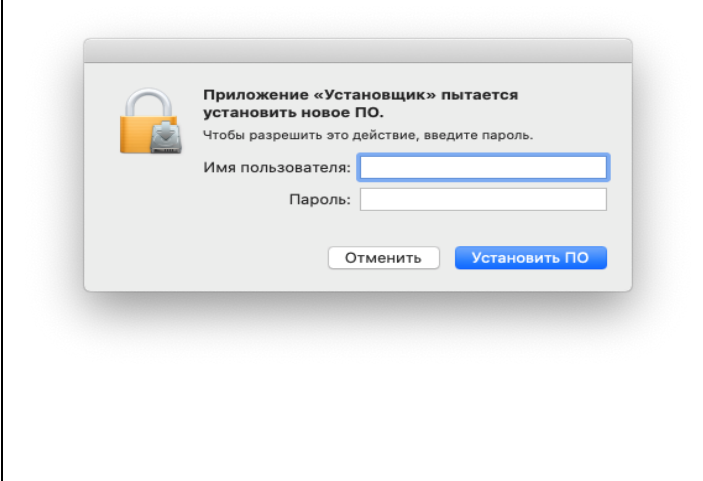
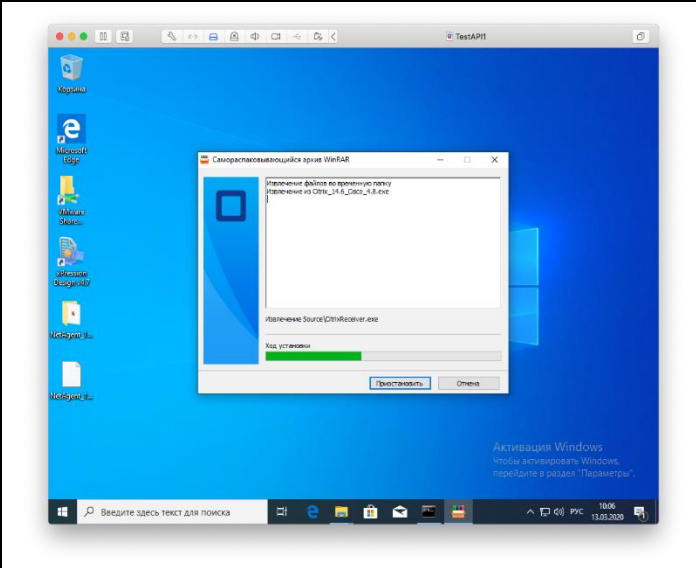
Ссылка на дистрибутив для Windows:

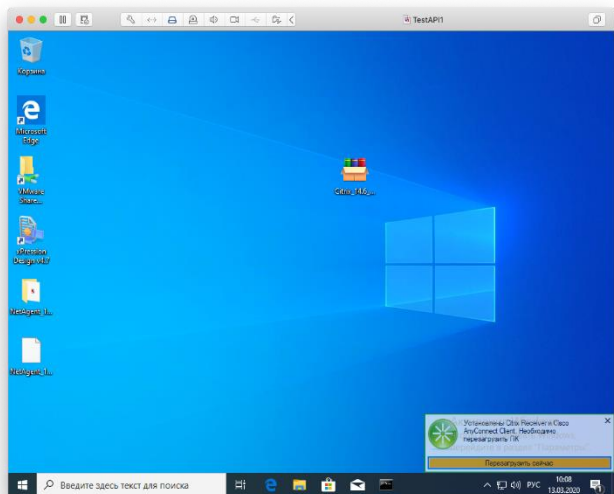
https://files.apps.sberbank.ru/ci01528000-epromlg-sberstoreprod/portal/Citrix_14.6_Cisco_4.8.exe

Ссылка на дистрибутив для Mac:

<https://files.apps.sberbank.ru/ci01528000-epromlg-sberstoreprod/portal/CitrixCiscoAniconect.pkg>

Для Windows	Для MacOS
Запустите пакет Citrix_14.6_Cisco_4.8 от имени администратора путем нажатия правой кнопкой мыши по пакету и выбрав пункт «Запуск от имени администратора».	Запустите пакет CitrixCiscoAniconect.pkg Появится следующее окно:
	
При запуске пакета установки может возникнуть следующее окно:	Нажмите «Продолжить».
	
Необходимо нажать «Подробнее», в появившемся окне нажать кнопку «Выполнить в любом случае»	Повторно нажмите «Продолжить».

 <p>Система Windows защитила ваш компьютер</p> <p>Фильтр SmartScreen Защитника Windows предотвратил запуск неопознанного приложения, которое может подвергнуть компьютер риску.</p> <p>Приложение: Citrix_14.6_Cisco_4.8 (1).exe Издатель: Неизвестный издатель</p> <p>Выполнить в любом случае Не выполнять</p>	 <p>Установка: CitrixCiscoAniconect</p> <p>Стандартная установка на «System»</p> <p>Нажмите «Установить» для выполнения стандартной установки этого ПО на диске «System».</p> <p>Изменить размещение установки...</p> <p>Назад Установить</p>
<p>В случае появления окна с подтверждением нажмите «Да».</p>	<p>Нажмите «Установить» В появившемся окне введите свои логин и пароль локального администратора macbook.</p>
 <p>Контроль учетных записей</p> <p>Разрешить этому приложению от неизвестного издателя вносить изменения на вашем устройстве?</p> <p>Citrix_14.6_Cisco_4.8.exe</p> <p>Издатель: Нет данных Источник файла: Жесткий диск компьютера</p> <p>Подробнее</p> <p>Да Нет</p>	 <p>Приложение «Установщик» пытается установить новое ПО.</p> <p>Чтобы разрешить это действие, введите пароль.</p> <p>Имя пользователя: <input type="text"/></p> <p>Пароль: <input type="password"/></p> <p>Отменить Установить ПО</p>
<p>Через некоторое время появится следующее окно.</p>	<p>Дождитесь завершения установки.</p>
 <p>Самостоятельно создающийся архив Windows</p> <p>Измененные файлы во временную папку скопированы из Citrix_14.6_Cisco_4.8.exe</p> <p>Ивлеченные Source(CitrixAniconect.exe)</p> <p>Ход установки</p> <p>Продолжить Отмена</p>	
<p>Дождитесь появления следующего окна.</p>	



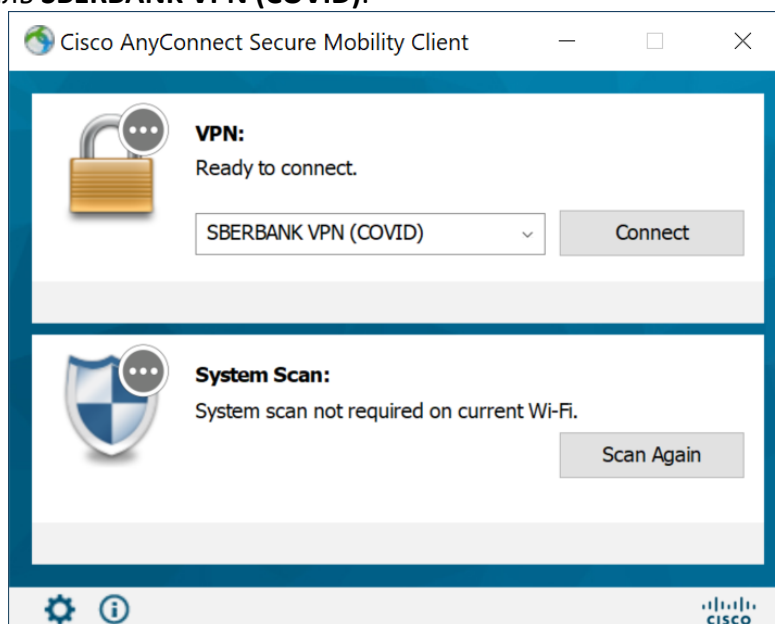
Перезагрузите компьютер.

[Вернуться к Оглавлению.](#)

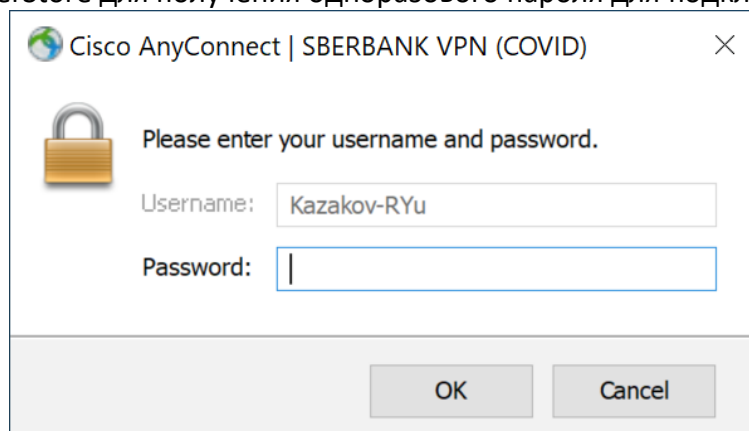
Подключите VPN с помощью Cisco Anyconnect и SberStore

Перед началом подключения убедитесь, что вашу заявку в ДРУГ «Предоставление удалённого доступа к АРМ» выполнили.

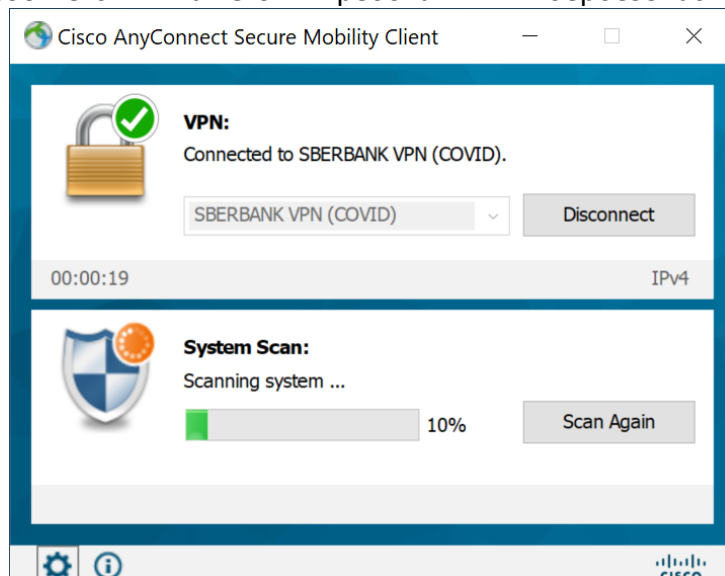
1. Для подключения к сети Банка запустите Cisco AnyConnect Secure Mobile Client.
2. Выберите профиль **SBERBANK VPN (COVID)**.



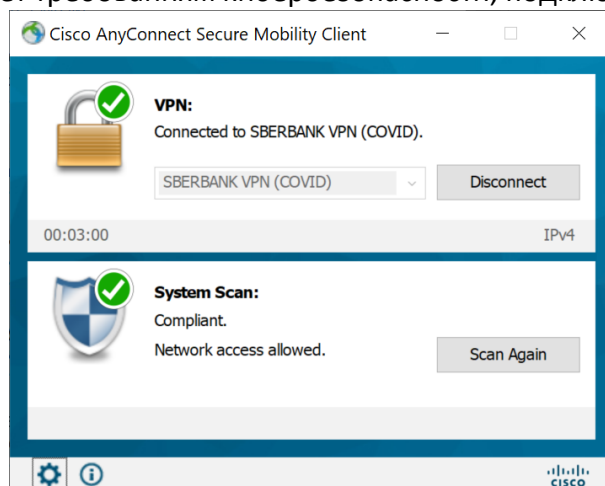
3. Нажмите кнопку **Connect**, ввести в поле **Password** цифры из SberStore, вкладка «Доступ к ВАРМ» (шаг «Установка SberStore для получения одноразового пароля для подключения VPN»).



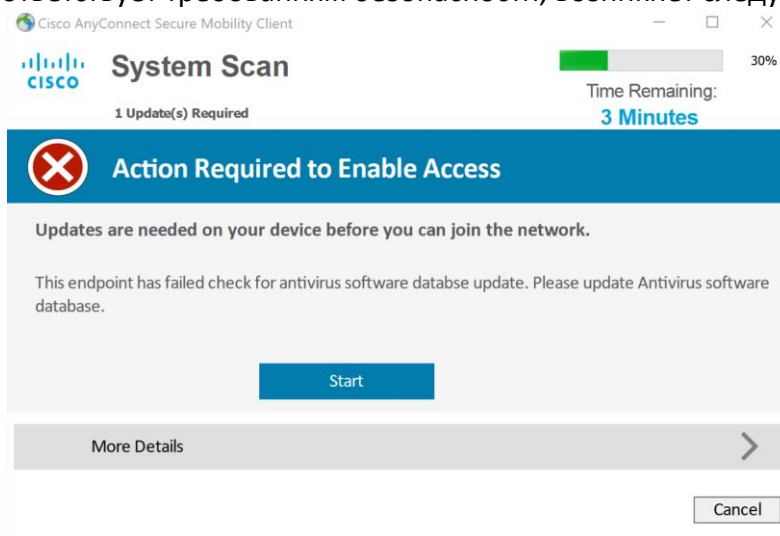
4. Начнётся проверка соответствия вашего ПК требованиям Кибербезопасности



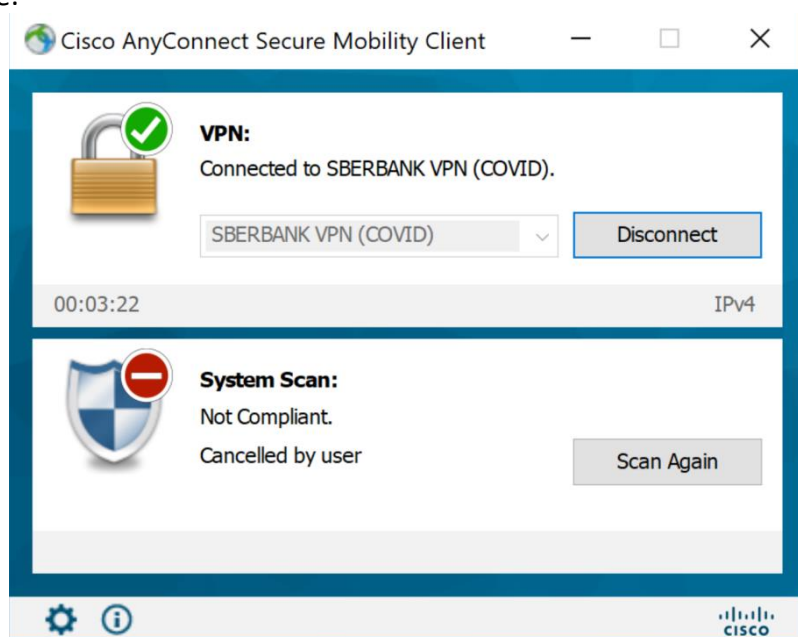
5. Если Ваш ПК соответствует требованиям кибербезопасности, подключение будет выполнено



6. Если Ваш ПК НЕ соответствует требованиям безопасности, возникнет следующее сообщение

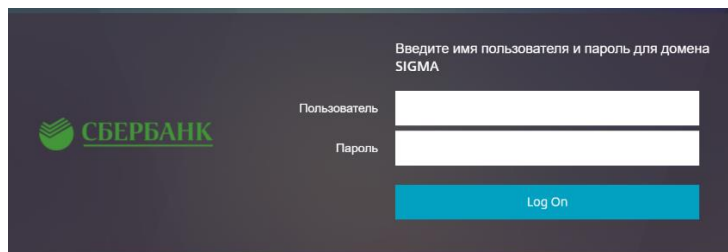


- Необходимо установить антивирус и обновить антивирусные базы, а также проверить требования к ОС на личном устройстве в разделе «Требования к используемой технике».
- До приведения ПК в соответствие требованиям безопасности будет возникать такое сообщение:

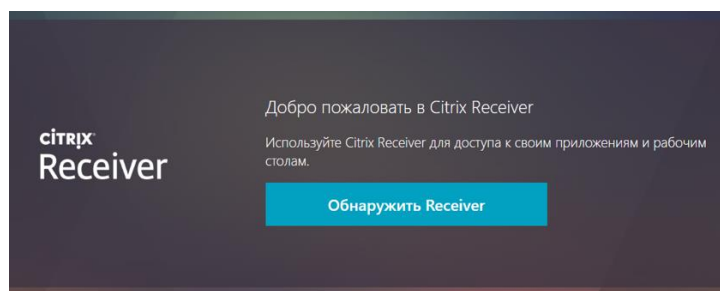


Подключитесь к АРМ с помощью Citrix Receiver

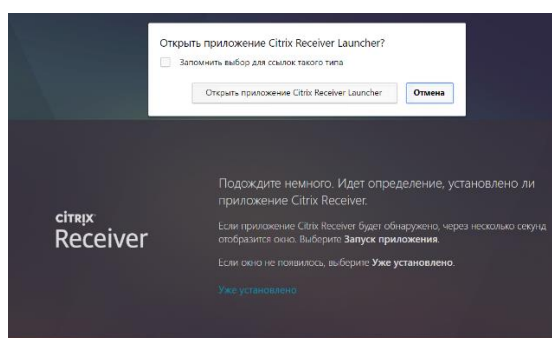
1. После успешного соединения откройте в браузере
 - Для подключения к АРМ Sigma: <https://s-gate.sigma.sbrf.ru>
 - Для подключения к АРМ Alpha: <https://asg.sigma.sbrf.ru>
 - Для подключения к ВАРМ Alpha-Sigma-CA: <https://asg.sigma.sbrf.ru>
2. Откроется окно идентификации пользователя



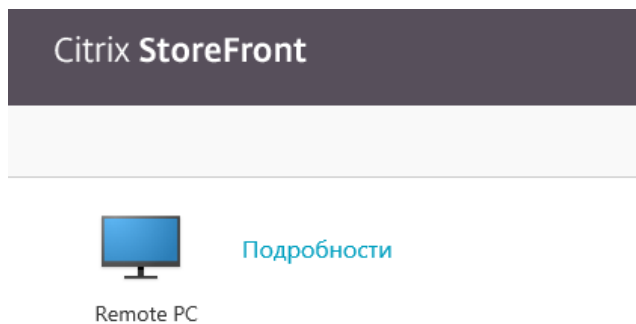
3. В полях **Пользователь** и **Пароль** укажите логин и пароль учетной записи в домене Sigma, либо Alpha.
4. Щёлкните **Log On**. Произойдёт подключение к Citrix Receiver.
5. При первом подключении появится окно приветствия, в котором щёлкните **Обнаружить Receiver**.



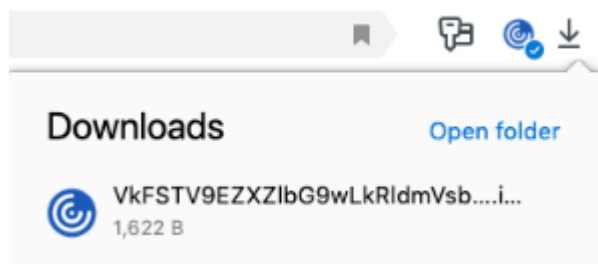
6. Если появилось окно запуска приложения, то запустите его.
7. Если окно запуска приложения не появилось, щёлкните **Уже установлено**.



8. Произойдёт переход на портал Citrix StoreFront. Откроется окно **Рабочие столы** с отображёнными в нем виртуальными АРМ, подключение к которым вы можете осуществить.



9. Щелкните иконку АРМ **Remote PC**. На ваш компьютер будет загружен ICA-файл.



10. Запустите загруженный ICA-файл, чтобы получить доступ к локальному АРМ.

[Вернуться к Оглавлению.](#)

FAQ

Для чего мне нужен удалённый доступ?

В случае, если вы направлены в карантин или самоизоляцию по согласованию с вашим руководством, вы можете осуществлять свою рабочую деятельность из дома. Для этого выполните действия, указанные в данной инструкции, и получите все необходимые вам для этого доступы.

Кто несёт ответственность за решение предоставить мне удалённый доступ для работы из дома?

Заявку на предоставление сотруднику удалённого доступа согласовывает непосредственный руководитель. Он несёт ответственность за это решение.

Я смогу получить доступ ко всем ресурсам банка?

Объем предоставляемых сотруднику доступов определяется вашим непосредственным руководителем. При необходимости сотруднику может быть предоставлен доступ к своему рабочему месту, находящемуся в офисе, к виртуальному рабочему месту (при его наличии).

А если у меня нет рабочего ноутбука, я не смогу работать из дома со своего личного компьютера?

Сможете. Удалённый доступ из дома возможен как с корпоративного ноутбука, так и с личного компьютера/ноутбука.

Я привык подключаться из дома через Cisco AnyConnect по ссылке <https://ssl.sberbank.ru>? Зачем мне все эти действия?

Привычный вам вариант подключения продолжает работать. И если имеющегося функционала вам достаточно – получать дополнительный удалённый доступ вам не требуется.

У меня возникли технические проблемы во время работы из дома. К кому мне обратиться за помощью?

В случае выявления аномальной активности устройства (блокировка экрана, самопроизвольный запуск приложений, самопроизвольный ввод текста, перемещение курсора и др.) или не работоспособности устройства (ноутбука, мобильного устройства), с которого осуществляется дистанционная работа, необходимо обратиться в службу поддержки МЦТП (бесплатный номер **8-800-555-93-40**).

[Вернуться к Оглавлению.](#)

Ответственность пользователя при удалённом подключении

1. Не производить копирование данных в обход средств защиты (видео, фото фиксация и скриншот экрана).
2. Обработку информации, составляющей банковскую тайну (сведения об операциях, о счетах и вкладах клиентов и корреспондентов Банка, данные платёжных карт), персональные данные клиентов и сотрудников Банка, а также информацию, составляющей коммерческую тайну, осуществлять только на период дистанционной работы в связи с угрозой распространения коронавирусной инфекции (2019-nCoV).
3. Исключить работу в публичных местах.
4. Исключить доступ к устройству, информации и АС Банка третьих лиц, в т.ч. членов семьи.
5. Не оставлять устройство без присмотра (независимо от характера дистанционной работы и продолжительности отсутствия), производить его блокировку (комбинацией Win+L для систем под управлением Windows или Command+Control+Q для систем с Mac OS).
6. В случае утраты (кражи, утери) устройства или носителя, содержащего информацию Банка, а также о ставших известными фактах (попытках) несанкционированного доступа к ним, немедленно информировать об этом своего непосредственного руководителя и департамент кибербезопасности (по телефону: **8-800-707-45-00** либо по адресу электронной почты: SCST@sberbank.ru).

[Вернуться к Оглавлению.](#)