kaspersky

Kaspersky Thin Client

Содержание

Справка Kaspersky Thin Client

	**Что нового** Узнайте, что нового в этой версии Kaspersky Thin Client.		**Аппаратные и программные требования** Проверьте требования к удаленным средам и подключаемым периферийным устройствам.
	**Обновление** Как обновить версию Kaspersky Thin Client.		**Сброс параметров и данных** Как выполнить сброс параметров и данных Kaspersky Thin Client.
	**Начало работы** Запуск тонкого клиента. Первоначальная настройка и соединение с Kaspersky Security Center. Назначение сертификатов.		**Настройка и подключение к удаленной среде** Доступные способы подключения. Подключение к удаленной среде. Настройка параметров Kaspersky Thin Client, а также параметров подключения к удаленным средам и Kaspersky Security Center. Настройка тонких клиентов через Kaspersky Security Center.
	**Дополнительные возможности** Управление сертификатами Kaspersky Thin Client. Управление политиками. Управление доступом к параметрам Kaspersky Thin Client.		**Мониторинг событий** Просмотр и отправка журналов событий и аудита на сервер журналирования. Просмотр событий Kaspersky Thin Client через Kaspersky Security Center Web Console.

О Kaspersky Thin Client

Kaspersky Thin Client версии 2.0 (далее также "Kaspersky Thin Client" и "система") представляет собой операционную систему для тонких клиентов на базе операционной системы KasperskyOS. Kaspersky Thin Client предназначена для предоставления пользователю доступа к удаленному рабочему столу и служит заменой локальной рабочей станции. Kaspersky Thin Client версии 2.0 устанавливается только на тонкие клиенты TONK TN1200 и Centerm F620.

Основные функции Kaspersky Thin Client:

- Подключение к удаленным и виртуальным рабочим столам под управлением операционных систем семейства Microsoft® Windows® по протоколу RDP, в том числе через брокер Microsoft Remote Desktop Connection Broker, с авторизацией с помощью имени пользователя и пароля.
- Подключение к терминальным серверам под управлением операционных систем семейства Microsoft Windows Server® по протоколу RDP, в том числе через брокер Microsoft Remote Desktop Connection Broker, с авторизацией с помощью имени пользователя и пароля.
- Подключение к удаленным и виртуальным рабочим столам под управлением операционных систем семейства Linux® по протоколу RDP с авторизацией с помощью имени пользователя и пароля.
- Подключение к виртуальным приложениям по протоколу RDP через брокер Microsoft Remote Desktop Connection Broker с авторизацией с помощью имени пользователя и пароля.
- Подключение к виртуальным рабочим столам, развернутым в инфраструктуре виртуальных рабочих столов Базис.WorkPlace, с авторизацией с помощью имени пользователя и пароля.
- Подключение к виртуальным рабочим столам, развернутым в инфраструктурах Citrix Workspace и VMware Horizon™, в приложении Web Access.
- Передача изображения экрана удаленного рабочего стола на монитор, подключенный к Kaspersky Thin Client.
- Перенаправление клавиатуры и мыши, подключенных к Kaspersky Thin Client, в удаленную среду.
- Перенаправление USB-накопителей, смарт-карт, USB-токенов, принтеров, микрофона и устройств воспроизведения звука, подключенных к Kaspersky Thin Client, в удаленную среду.
- Централизованное управление, обновление и контроль Kaspersky Thin Client через Kaspersky Security Center Web Console версии 14.2. Для связи Kaspersky Thin Client и Kaspersky Security Center используется веб-плагин Kaspersky Security Management Suite.

Комплект поставки

Kaspersky Thin Client поставляется в одном из следующих форматов:

- Образ Kaspersky Thin Client без поставки аппаратной платформы (тонкого клиента).
- Аппаратная платформа с предустановленным Kaspersky Thin Client, поставляемая партнером.

В комплект поставки Kaspersky Thin Client без аппаратной платформы входят следующие файлы:

- Архив с установочным образом Kaspersky Thin Client: Kaspersky_Thin_Client_<номер версии>.tar.gz.

- Загрузочный пакет KTC_uboot_<номер версии>.tar.gz.
- Скрипт для установки на тонкий клиент hw_install.sh.
- Текстовый файл с информацией о стороннем коде: KTC_LegalNotices_en.txt.
- Текстовые файлы с описанием новых функций и известных ограничений:
  - ReleaseNotes_Kaspersky_Thin_Client_<номер версии>_EN.txt.
  - ReleaseNotes_Kaspersky_Thin_Client_<номер версии>_ES.txt.
  - ReleaseNotes_Kaspersky_Thin_Client_<номер версии>_PT_BR.txt.
  - ReleaseNotes_Kaspersky_Thin_Client_<номер версии>_RU.txt.
- Файлы Лицензионного соглашения Kaspersky Thin Client:
  - eula_en_ktc_<номер версии>.txt.
  - eula_es_ktc_<номер версии>.txt.
  - eula_pt_ktc_<номер версии>.txt.
  - eula_ru_ktc_<номер версии>.txt.

В комплект поставки Kaspersky Security Management Suite версии 2.0 входят перечисленные ниже составляющие.

Если вы распаковываете архив с помощью средств автоматизации (например, скрипта), вы должны ознакомиться с текстом Лицензионного соглашения и начать использовать Kaspersky Security Management Suite только после ознакомления и принятия положений и условий Лицензионного соглашения.

- Архивы для Microsoft Windows с установочными образами и файлами подписи веб-плагина для Kaspersky Security Center Web Console:
  - Web_Plugin_Kaspersky_Security_Management_Suite_<номер версии плагина>_en.exe.
  - Web_Plugin_Kaspersky_Security_Management_Suite_<номер версии плагина>_es.exe.
  - Web_Plugin_Kaspersky_Security_Management_Suite_<номер версии плагина>_pt_br.exe.
  - Web_Plugin_Kaspersky_Security_Management_Suite_<номер версии плагина>_ru.exe.
- Архивы для Linux с установочными образами и файлами подписи веб-плагина для Kaspersky Security Center Web Console:
  - Web_Plugin_Kaspersky_Security_Management_Suite_<номер версии плагина>_en.sh.
  - Web_Plugin_Kaspersky_Security_Management_Suite_<номер версии плагина>_es.sh.
  - Web_Plugin_Kaspersky_Security_Management_Suite_<номер версии плагина>_pt_br.sh.
  - Web_Plugin_Kaspersky_Security_Management_Suite_<номер версии плагина>_ru.sh.

- Текстовый файл с информацией о стороннем коде для Kaspersky Security Management Suite: KSMS_LegalNotices_en.txt.
- Файлы Лицензионного соглашения Kaspersky Security Management Suite:
  - eula_en_ksms_<номер версии>.txt.
  - eula_es_ksms_<номер версии>.txt.
  - eula_pt_ksms_<номер версии>.txt.
  - eula_ru_ksms_<номер версии>.txt.

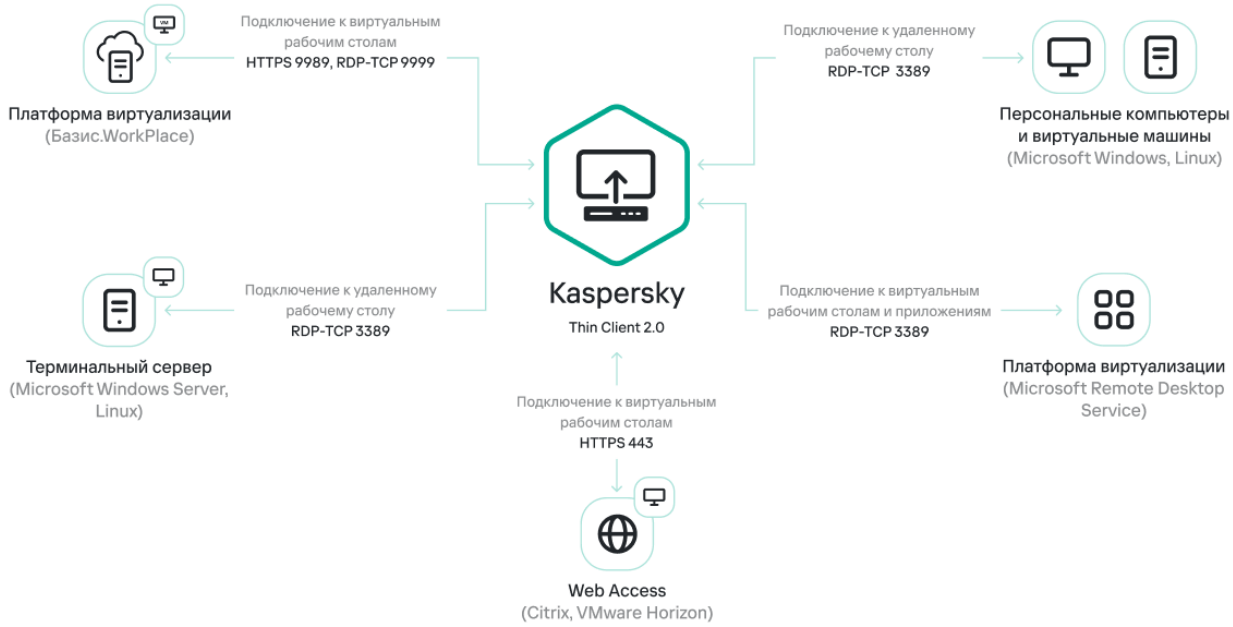
Принцип работы Kaspersky Thin Client

Типовая схема работы Kaspersky Thin Client (см. рис ниже) предполагает следующее:

- Kaspersky Thin Client, установленный на аппаратную платформу, получает параметры сети от DHCP-сервера, либо администратор настраивает параметры вручную.
- Администратор подключает и настраивает взаимодействие между Kaspersky Thin Client и Kaspersky Security Center.
- Kaspersky Thin Client получает параметры подключения к удаленному рабочему столу или к виртуальному приложению (далее также сессия подключения), обновлений, доверенных сертификатов, а также дату и время с политикой от Kaspersky Security Center.
- Пользователь подключается к удаленному рабочему столу или виртуальному приложению по протоколу RDP.
- Пользователь подключается к удаленному рабочему столу через платформу виртуализации Базис.WorkPlace
- Пользователь подключается к удаленной среде в Web Access.
- Пользователь в интерфейсе Kaspersky Thin Client отправляет журналы событий и аудита на сторонний сервер журналирования.
- Kaspersky Thin Client получает обновление программного обеспечения от сервера обновлений "Лаборатории Касперского" с помощью Kaspersky Security Center.

Типовая схема работы Kaspersky Thin Client

На рисунке ниже приведена схема взаимодействия Kaspersky Thin Client с платформами виртуализации.



Взаимодействие Kaspersky Thin Client с платформами виртуализации

Аппаратные и программные требования

В этом разделе описаны аппаратные и программные требования к Kaspersky Thin Client.

Требования к мониторам, подключаемым к Kaspersky Thin Client

Kaspersky Thin Client поддерживает подключение двух мониторов.

Kaspersky Thin Client поддерживает следующие разрешения мониторов:

- 1024x768.
- 1280x800.
- 1280x1024.
- 1366x768.
- 1440x900.
- 1600x900.
- 1680x1050.
- 1920x1080.
- 1920x1200. При подключении монитора с этим разрешением фактическое отображение разрешения будет не более 1920x1080.

Kaspersky Thin Client поддерживает следующие интерфейсы подключения:

- HDMI.
- Display Port.

Kaspersky Thin Client поддерживает глубину цвета монитора только TrueColor.

Требования к периферийным устройствам, подключаемым к Kaspersky Thin Client

Kaspersky Thin Client поддерживает работу со следующими периферийными устройствами:

- Стандартные, проводные клавиатуры и мыши без мультимедийных функций, которые подключаются через USB-порты.
- USB-накопители, а также смарт-карты и токены, подключаемые через USB-порты.
- Принтеры, подключаемые через USB-порты. В удаленной среде должен быть установлен драйвер для принтера, который подключен к тонкому клиенту.
- Проводные устройства записи и воспроизведения звука, которые подключаются через разъемы mini-jack.

Требования к удаленным рабочим столам

Вы можете подключаться к удаленным компьютерам, виртуальным машинам и терминальным серверам, на которых установлена одна из следующих операционных систем:

- Microsoft Windows 7.

- Microsoft Windows 10.
- Microsoft Windows 11.
- Microsoft Windows Server 2016.
- Microsoft Windows Server 2019.
- Microsoft Windows Server 2022.
- Astra Linux Common Edition 2.12 (xRDP 0.9.21.1).
- Astra Linux Special Edition 1.7 (xRDP 0.9.21.1).
- ALT Linux 10 (xRDP 0.9.24).
- РЕД ОС® 7.3 (xRDP 0.9.23.1).

Требования к удаленным рабочим столам Базис.WorkPlace

Kaspersky Thin Client поддерживает работу с платформой виртуализации Базис.WorkPlace версии 1.96. Через брокер Базис.WorkPlace вы можете подключаться к удаленным рабочим столам под управлением одной из следующих операционных систем:

- Microsoft Windows 10.
- Microsoft Windows 11.
- Microsoft Windows Server 2016.
- Microsoft Windows Server 2019.
- Microsoft Windows Server 2022.
- Astra Linux Common Edition 2.12 (xRDP 0.9.21.1).
- Astra Linux Special Edition 1.7 (xRDP 0.9.21.1).
- ALT Linux 10 (xRDP 0.9.24).
- РЕД ОС 7.3 (xRDP 0.9.23.1).

Требования к сети

Скорость сети должна составлять не менее 50 Мбит/с.

Требования к Kaspersky Security Center и Kaspersky Security Center Web Console

Система Kaspersky Thin Client совместима с Kaspersky Security Center версии 14.2. Системные и программные требования к серверу, на котором разворачивается Kaspersky Security Center, приведены в онлайн-справке Kaspersky Security Center.

Требования к серверам для отправки журналов событий

Сервер журналирования, на который будут отправляться журналы событий и аудита Kaspersky Thin Client, разворачивается в инфраструктуре вашего предприятия специалистами заказчика.

К серверу журналирования предъявляются следующие требования:

- Подключение Kaspersky Thin Client к серверу журналирования осуществляется по протоколу HTTPS (по умолчанию используется порт 443).
- Подключение Kaspersky Thin Client к серверу журналирования осуществляется только по сертификату безопасности.
- Kaspersky Thin Client отправляет журналы событий и аудита на сторонний сервер журналирования методом PUT.

Способы подключения к удаленным средам

Этот раздел содержит информацию о технологиях и средах удаленного доступа, поддерживаемых Kaspersky Thin Client, а также о способах подключения к таким средам. В разделе представлены данные о том, какие из устройств, подключенных к Kaspersky Thin Client, могут быть перенаправлены в удаленную среду.

Подключение по протоколу RDP

В Kaspersky Thin Client вы можете подключиться по протоколу RDP к удаленной среде, в том числе развернутой в инфраструктуре Microsoft Remote Desktop Services (далее также MS RDS). В таблице ниже описаны доступные способы подключения и периферийные устройства для операционных систем Windows и Linux.

Для перенаправления периферийных устройств на удаленный рабочий стол под управлением Linux необходимо установить расширение Kaspersky USB Redirector для xRDP-сервера на гостевой операционной системе. Kaspersky USB Redirector не входит в комплект поставки. Вы можете запросить это расширение у специалистов "Лаборатории Касперского".

Перед подключением к удаленному рабочему столу под управлением Linux с использованием xRDP-сервера, на котором не установлено расширение Kaspersky USB Redirector, уточните версию поддерживаемого xRDP-сервера в отдельной статье.

Инструкции по подключению к удаленной среде приведены в отдельной статье.

RDP: поддерживаемые операционные системы, способы подключения и периферийные устройства

	Windows Server 2016/2019/2022 в MS RDS	Windows 7	Windows 10/11	Windows Server 2016/2019/2022	ALT Linux 10 РЕД ОС 7.3 Astra Linux CE 2.12	Astra L SE 1.
Подключение к виртуальному приложению	✓	–	✓ Примечание	✓	–	–
Подключение к удаленному рабочему столу						
Прямое подключение	–	✓	✓	✓	✓	✓
Подключение с помощью VDI	✓	–	–	–	–	–
Терминальное подключение	✓	–	–	✓	✓	✓
Периферийные устройства						
USB-токены	✓	–	✓	✓	✓ Примечание	–
Смарт-карты (USB)	✓	–	✓	✓	✓ Примечание	–
USB-накопители	✓	–	✓	✓	✓	–

					Примечание	
Принтеры (USB)	✓	–	✓	✓ Примечание	✓ Примечание	–
Микрофон (mini-jack)	✓	–	✓	✓ Примечание	✓ Примечание	✓ Примеч
Устройство воспроизведения звука	✓	✓	✓	✓	✓ Примечание	✓ Примеч

Подключение при помощи Базис.WorkPlace

В Kaspersky Thin Client вы можете подключиться к удаленной среде, развернутой в инфраструктуре Базис.WorkPlace. В таблице ниже описаны доступные способы подключения и периферийные устройства для операционных систем Windows и Linux.

Для перенаправления периферийных устройств на удаленный рабочий стол под управлением Linux необходимо установить расширение Kaspersky USB Redirector для xRDP-сервера на гостевой операционной системе. Kaspersky USB Redirector не входит в комплект поставки. Вы можете запросить это расширение у специалистов "Лаборатории Касперского".

Перед подключением к удаленному рабочему столу под управлением Linux с использованием xRDP-сервера, на котором не установлено расширение Kaspersky USB Redirector, уточните версию поддерживаемого xRDP-сервера в отдельной статье.

Инструкции по подключению к удаленной среде приведены в отдельной статье.

Базис.WorkPlace: поддерживаемые операционные системы, способы подключения и периферийные устройства

	Windows 10/11	Windows Server 2016/2019/2022	РЕД ОС 7.3 ALT Linux 10 Astra Linux CE 2.12 Astra Linux SE 1.7
Подключение к удаленному рабочему столу			
Прямое подключение	–	–	–
Подключение с помощью VDI	✓	✓	✓
Терминальное подключение	–	✓	–
Периферийные устройства			
USB-токены	✓	✓	–
Смарт-карты (USB)	✓	✓	–
USB-накопители	✓	✓	–
Принтеры (USB)	✓	✓ Примечание	–
Микрофон (mini-jack)	✓	✓	✓

Устройство воспроизведения звука	✓	✓	✓

Подключение в приложении Web Access

В приложении Web Access вы можете подключиться к удаленной среде, развернутой в инфраструктурах Citrix Workspace и VMware Horizon, с помощью технологии HTML5. При подключении используется браузер Chromium™. В таблице ниже описаны доступные способы подключения и периферийные устройства для операционных систем Windows.

Инструкции по подключению приведены в отдельной статье.

Web Access: поддерживаемые операционные системы, способы подключения и периферийные устройства

	Microsoft Windows 10/11	Microsoft Windows Server 2016/2019/2022
Подключение к удаленному рабочему столу		
Прямое подключение	–	–
Подключение с помощью VDI	✓	✓
Терминальное подключение	–	✓
Периферийные устройства		
USB-токены	–	–
Смарт-карты (USB)	–	–
USB-накопители	–	–
Принтеры (USB)	–	–
Микрофон (mini-jack)	✓	✓
Устройство воспроизведения звука	✓	✓

В текущей версии Kaspersky Thin Client в приложении Web Access не поддерживается подключение к удаленным рабочим столам под управлением Linux, а также к виртуальным приложениям.

Что нового

В Kaspersky Thin Client версии 2.0 появились следующие возможности и доработки:

- Подключение к удаленным рабочим столам и приложениям, развернутым в инфраструктуре Microsoft Remote Desktop Services, – добавлена возможность подключения к удаленным рабочим столам и виртуальным приложениям под управлением операционных систем семейства Microsoft Windows через брокер Microsoft Remote Desktop Connection Broker.

- Добавлена возможность подключения к виртуальным рабочим столам, развернутым в инфраструктуре Citrix и VMware Horizon, по HTML5.

- Перенаправление устройств записи и воспроизведения звука, подключенных к тонкому клиенту через разъем mini-jack, в удаленную среду.

- Перенаправление смарт-карт, USB-накопителей и принтеров на удаленный рабочий стол под управлением операционных систем Linux (Astra Linux CE/SE, ALT Linux или РЕД ОС). Для перенаправления периферийных устройств необходимо установить расширение Kaspersky USB Redirector для xRDP-сервера на гостевой ОС, в том числе в инфраструктуре Базис.WorkPlace.

- Добавлена поддержка тонкого клиента Centerm F620.

- Автоматическое подключение при разрыве соединения – добавлена функция автоматического подключения к удаленному рабочему столу по протоколу RDP при разрыве соединения.

- Расширена поддержка гостевых операционных систем – добавлена возможность подключаться к удаленным рабочим столам под управлением операционных систем Microsoft Windows 11 и Microsoft Windows Server 2022.

- Перенаправление принтеров в удаленную среду – добавлена функция печати документов из гостевой операционной системы (при подключении по протоколу RDP, в том числе в инфраструктуре виртуальных рабочих столов Базис.WorkPlace) на принтере, который подключен к тонкому клиенту.

- Поддержка новой конфигурации TONK TN1200 – добавлена функциональность, обеспечивающая запуск и работу Kaspersky Thin Client на устройствах TONK TN1200 с жестким диском типа mSATA.

- Улучшение производительности Kaspersky Thin Client:

  - Увеличена скорость доставки удаленного рабочего стола и виртуальных приложений на тонкий клиент.

  - Увеличена скорость загрузки тонкого клиента при включении.

  - Увеличена скорость подключения к удаленным рабочим столам по доменному имени.

- Повышение стабильности работы тонких клиентов, управляемых через Kaspersky Security Center.

- Добавлена поддержка испанского и бразильского португальского языков в интерфейсе и в качестве языка ввода.

- Обновлен дизайн и текст интерфейса пользователя Kaspersky Thin Client, в том числе:

  - Переработана панель подключения в удаленной среде.

  - Добавлена интерактивная панель уведомлений.

Установка и обновление Kaspersky Thin Client

Процедура установки Kaspersky Thin Client зависит от формата поставки:

- Партнер поставляет аппаратную платформу с предустановленным Kaspersky Thin Client. В этом случае установку Kaspersky Thin Client на аппаратную платформу выполняют специалисты ООО "Группа Компаний ТОНК".
- Поставляется образ Kaspersky Thin Client без поставки аппаратной платформы (тонкого клиента). В этом случае программная платформа устанавливается по инструкции, приведенной в этом разделе.

Подготовка к установке

Перед установкой Kaspersky Thin Client выполните следующие действия:

1. Подготовьте загрузочный USB-накопитель с операционной системой Linux Ubuntu (рекомендованная версия: Ubuntu 20.04).
2. Скопируйте в отдельный раздел на загрузочном USB-накопителе или на отдельный USB-накопитель файлы установки Kaspersky Thin Client, полученные в комплекте поставки:
   - KTC_uboot_<номер версии>.tar.gz – загрузочный пакет.
   - Kaspersky_Thin_Client_<номер версии>.tar.gz – установочный образ.
   - hw_install.sh – скрипт для установки Kaspersky Thin Client.

Для обеспечения безопасности перед установкой Kaspersky Thin Client также рекомендуется обновить BIOS на тонком клиенте до последней версии, установить пароль на изменение параметров BIOS и настроить возможность загрузки только с локального SSD-устройства. Принятые меры помогут предотвратить вероятные риски безопасности, такие как подмена операционной системы, подмена или удаление сертификатов подключения к удаленным серверам и получение несанкционированного доступа к настройкам операционной системы.

Установка Kaspersky Thin Client

Чтобы установить Kaspersky Thin Client на тонком клиенте:

1. Вставьте подготовленный загрузочный USB-накопитель в соответствующий разъем на тонком клиенте.
2. Включите тонкий клиент и загрузите образ Ubuntu с загрузочного USB-накопителя, не устанавливая систему на жесткий диск тонкого клиента.
3. В запущенной операционной системе перейдите в директорию с файлами установки Kaspersky Thin Client.
4. Выполните следующую команду от имени пользователя с root-правами:

   ```
   sudo ./hw_install.sh -b KTC_uboot_<номер версии>.tar.gz -u
   Kaspersky_Thin_Client_<номер версии>.tar.gz
   ```

где:

- `./hw_install.sh` – путь к скрипту установки.
- `KTC_uboot_<номер версии>.tar.gz` – загрузочный пакет.
- `Kaspersky_Thin_Client_<номер версии>.tar.gz` – установочный образ.

После успешного завершения установки отобразится сообщение *Installed OK! Remove USB drive and reboot*.

5. Выключите тонкий клиент и извлеките загрузочный USB-накопитель.

При следующем включении тонкого клиента загрузится установленная система Kaspersky Thin Client.

Проверить номер текущей версии операционной системы вы можете в интерфейсе Kaspersky Thin Client.

Обновление Kaspersky Thin Client

Для обновления Kaspersky Thin Client на версию 2.0 необходимо получить архив с базами обновлений у специалистов "Лаборатории Касперского". Полученный архив необходимо загрузить в Kaspersky Security Center Web Console (далее также Web Console), затем создать, настроить и запустить задачу загрузки обновлений в хранилище Сервера администрирования Kaspersky Security Center (далее также Сервер) в интерфейсе Web Console.

Обновление Kaspersky Thin Client возможно, только если тонкий клиент подключен к Kaspersky Security Center.

На одном Сервере администрирования Kaspersky Security Center может быть только одна активная задача обновления с одним приоритетным источником обновлений. В связи с этим рекомендуется использовать отдельный Сервер для управления тонкими клиентами, чтобы получать важные исправления безопасности от серверов обновлений "Лаборатории Касперского".

Чтобы обновить Kaspersky Thin Client на тонком клиенте через Kaspersky Security Center Web Console:

1. На Сервере Kaspersky Security Center распакуйте архив с базами обновлений, полученный от специалистов "Лаборатории Касперского".
2. Предоставьте всем пользователям системы полные права доступа к распакованной папке, выполнив следующие действия:
   a. Нажмите на распакованную папку правой кнопкой мыши и выберите **Свойства**.
   b. В открывшемся меню выберите вкладку **Безопасность** и нажмите **Изменить**.
   c. В открывшемся окне нажмите **Добавить**, затем выберите **Дополнительно** и в открывшемся окне нажмите на кнопку **Поиск**.
   d. В отобразившемся списке выберите группу **Все** и нажмите **ОК**, затем еще раз нажмите **ОК** в открывшемся окне.

      Отобразится вкладка **Безопасность**, группа **Все** отобразится в списке **Группы или пользователи**.

e. В блоке **Разрешения для группы Все** установите флажки для всех параметров в колонке **Разрешить**.

f. Нажмите **OK**, затем еще раз нажмите **OK** в открывшемся окне.

3. Запустите Web Console и выберите раздел **Устройства**, затем перейдите на вкладку **Задачи**.

4. Если задача **Загрузка обновлений в хранилище Сервера администрирования** есть в списке, перейдите к следующему шагу инструкции. Если нет – добавьте ее, выполнив следующие действия:

   a. На вкладке **Задачи** нажмите **Добавить**.

   b. В открывшемся окне в раскрывающемся списке **Тип задачи** выберите **Загрузка обновлений в хранилище Сервера администрирования** и нажмите **Далее**.

   c. Нажмите **Готово**, чтобы завершить создание задачи.

5. Выберите задачу **Загрузка обновлений в хранилище Сервера администрирования** и в открывшемся окне перейдите на вкладку **Параметры программы**.

6. В блоке параметров **Источники обновлений** установите флажок напротив источника **Серверы обновлений "Лаборатории Касперского"** и нажмите на кнопку **Удалить**.

7. В этом же блоке параметров нажмите **Добавить**, затем в отобразившемся списке выберите **Локальная или сетевая папка** и укажите полный путь до папки с файлами обновлений.

8. Нажмите **Сохранить**, чтобы завершить замену источника обновлений.

9. Перейдите на вкладку **Расписание**, затем в раскрывающемся списке **Запуск по расписанию** выберите необходимое значение.

   Настройте другие параметры на этой вкладке, если требуется.

10. Нажмите **Сохранить**, чтобы завершить настройку задачи.

11. В списке задач установите флажок напротив задачи **Загрузка обновлений в хранилище Сервера администрирования** и нажмите **Запустить**.

    Задача будет запущена. Вы можете отслеживать прогресс ее выполнения в списке задач в столбце **Статус**.

12. Если требуется посмотреть результат выполнения задачи для отдельных устройств, выполните следующие действия:

    a. В списке задач выберите **Загрузка обновлений в хранилище Сервера администрирования** и в открывшемся окне перейдите на вкладку **Результаты**.

    b. Если требуется посмотреть подробную информацию о выполнении задачи на устройстве, установите флажок напротив необходимого устройства и нажмите **История устройства**.

13. По завершении задачи загрузки обновлений примите Лицензионное соглашение и подтвердите загрузку обновлений на тонкие клиенты, выполнив следующие действия:

    a. В Web Console перейдите в раздел **Операции → Программы "Лаборатории Касперского"** и в раскрывающемся списке выберите **Обновления**.

    b. В отобразившемся списке обновлений нажмите **Вы должны принять Лицензионное соглашение** напротив необходимого обновления, затем в открывшемся окне ознакомьтесь с текстом Лицензионного соглашения.

c. Если вы согласны с условиями соглашения, примите его, установив флажок **Положения и условия настоящего Лицензионного соглашения** и подтвердив свой выбор. Если вы не согласны с условиями Лицензионного соглашения и не примете их, вы не сможете загрузить обновления на тонкие клиенты.

d. В списке обновлений нажмите на имя необходимого обновления, затем в отобразившемся окне в блоке параметров **Статус одобрения обновления** выберите **Одобрено** и подтвердите свой выбор.

   Подробную информацию о подтверждении загрузки обновлений см. в разделе *Одобрение и отклонение обновлений программного обеспечения* в онлайн-справке Kaspersky Security Center.

Запрос на загрузку обновлений будет подтвержден.

После подтверждения запроса обновления будут загружены на подключенные к Kaspersky Security Center тонкие клиенты, в том числе не входящие в группы администрирования или управляемые группы.

Подробная информации о том, как принимать и устанавливать обновления на тонких клиентах, приведена в отдельной статье.

Интерфейс Kaspersky Thin Client

Интерфейс Kaspersky Thin Client содержит следующие элементы:

- Главное окно Kaspersky Thin Client.

  В центральной части главного окна вы можете выбрать вариант подключения к удаленной среде:

  - **RDP**: подключение к удаленным рабочим столам или виртуальным приложениям по протоколу RDP.
  - **Базис.WorkPlace**: подключение к виртуальным рабочим столам, развернутым в инфраструктуре Базис.WorkPlace.
  - **Web Access**: подключение к удаленной среде, развернутой в инфраструктуре Citrix Workspace и VMware Horizon.

  В окне подключения вы можете настроить параметры подключения по протоколу RDP или параметры подключения через Базис.WorkPlace.

- Панель управления Kaspersky Thin Client. Содержит следующие элементы:

  - – кнопка вызова меню завершения работы. В этом меню вы можете выключить или перезагрузить Kaspersky Thin Client.
  - – кнопка перехода к разделам **Параметры** и **Инструменты**:

    В разделе **Параметры** вы можете настроить Kaspersky Thin Client.

    В разделе **Инструменты** вы можете выполнять следующие действия:

    - Просматривать информацию о Kaspersky Thin Client.
    - Просматривать информацию о состоянии сети.
    - Просматривать и отправлять журнал событий Kaspersky Thin Client.
    - Обновлять Kaspersky Thin Client.
    - Просматривать действующее Лицензионное соглашение.
    - Просматривать информацию о стороннем коде.
    - Управлять доступом к параметрам Kaspersky Thin Client.
  - Если Kaspersky Thin Client входит в группу администрирования и в общих параметрах группы указаны контактные данные администратора, в панели управления также отображаются контакты администратора Kaspersky Security Center.
  - Информация о состоянии подключения Kaspersky Thin Client к сети.
  - Информация о новых уведомлениях Kaspersky Thin Client. Вы можете просматривать полученные уведомления.
  - Кнопка переключения языка ввода текста с клавиатуры.
  - Дата и время системы.

- Панель подключения.

Отображается во время сессии подключения к удаленной среде.

Во время подключения к удаленному рабочему столу в панели подключения отображаются следующие элементы:

- Имя подключения.
- Статус подключения.
- Кнопка **Завершить сессию**.
- Контакты администратора, если они были указаны при развертывании системы.
- Значок состояния сети.

Во время подключения к виртуальному приложению в панели подключения дополнительно отображаются следующие элементы:

- Значок приложения.
- Текущая дата, установленная на тонком клиенте.
- Текущее время, установленное на тонком клиенте.
- Язык, установленный на тонком клиенте.

Лицензирование Kaspersky Thin Client

Условия использования Kaspersky Thin Client изложены в Лицензионном соглашении или подобном документе, на основании которого используется система.

Лицензионное соглашение – это юридическое соглашение между вами и АО "Лаборатория Касперского", в котором указано, на каких условиях вы можете использовать Kaspersky Thin Client.

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с Kaspersky Thin Client.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения при первом запуске. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать запуск и не должны использовать Kaspersky Thin Client. При обновлении Kaspersky Thin Client условия Лицензионного соглашения, если они изменились для новой версии Kaspersky Thin Client, принимает администратор Kaspersky Security Center.

При необходимости вы можете просмотреть текст Лицензионного соглашения в интерфейсе Kaspersky Thin Client.

Чтобы просмотреть текст Лицензионного соглашения,

в панели управления Kaspersky Thin Client нажмите на кнопку  и в открывшемся меню выберите **Инструменты → Лицензионное соглашение**.

Откроется окно, в котором отображается текст Лицензионного соглашения для текущей версии Kaspersky Thin Client.

Предоставление данных

Kaspersky Thin Client не передает никаких данных в "Лабораторию Касперского". Данные обрабатываются на тонких клиентах, на которых установлена система Kaspersky Thin Client, а также на серверах локальной инфраструктуры, с которыми взаимодействует Kaspersky Thin Client.

Kaspersky Thin Client сохраняет на тонком клиенте следующую информацию:

- Журнал событий, содержащий технические сведения о работе системы и события, которые Kaspersky Thin Client отправляет на Сервер администрирования Kaspersky Security Center.
- Журнал аудита, содержащий данные о сертификатах, загруженных в Kaspersky Thin Client, и информацию о фактах включения и выключения управления тонкими клиентами с помощью Kaspersky Security Center.
- Параметры тонкого клиента:
  - Дата и время установки Kaspersky Thin Client на тонком клиенте.
  - Имя тонкого клиента.
  - Текущая установленная версия Kaspersky Thin Client.
  - Язык интерфейса Kaspersky Thin Client.
  - Список языков, доступных для ввода текста с клавиатуры.
  - Информация о том, какой из мониторов является основным, а какой – дополнительным.
  - Идентификатор основного монитора.
  - Месторасположение (координаты) панели подключения.
  - Время последнего использования сертификатов для проверки подлинности подключения к следующим узлам: брокерам; удаленным рабочим столам или виртуальным приложениям по протоколу RDP; виртуальным рабочим столам, развернутым в инфраструктуре Базис.WorkPlace; удаленной среде через приложение Web Access; серверу журналирования.
- Параметры взаимодействия с Kaspersky Security Center:
  - Адрес (имя или IP-адрес и порт) Сервера администрирования Kaspersky Security Center.
  - Способ подключения Kaspersky Security Center (вручную или по DHCP).
  - Набор идентификаторов Kaspersky Thin Client для подключения к Kaspersky Security Center.
  - Период синхронизации Kaspersky Thin Client с Kaspersky Security Center в минутах.
  - Количество сертификатов, полученных от Kaspersky Security Center для проверки подлинности подключения Kaspersky Thin Client к следующим узлам: брокерам; удаленным рабочим столам или виртуальным приложениям по протоколу RDP; виртуальным рабочим столам, развернутым в инфраструктуре Базис.WorkPlace; удаленной среде через приложение Web Access; серверу журналирования.
  - Отпечаток текущего сертификата для проверки подлинности подключения Kaspersky Thin Client к Kaspersky Security Center.

- Параметры именования тонкого клиента, заданные администратором Kaspersky Security Center (имя, идентификатор тонкого клиента и дополнительная информация).
- Набор секретов для подтверждения действия пользователя в интерфейсе Kaspersky Thin Client: сброс параметров и данных, отключение тонкого клиента от Kaspersky Security Center и изменение сертификата для подключения тонкого клиента к Kaspersky Security Center.
- Контактные данные Службы технической поддержки.
- Файлы сертификатов для проверки подлинности подключения Kaspersky Thin Client к Kaspersky Security Center.

- Параметры подключения в приложении Web Access:
  - Веб-адрес сервера.
  - Файлы сертификатов для проверки подлинности подключения.
  - Данные, необходимые для работы в удаленной среде, включая файлы cookies.
- Параметры подключения к инфраструктуре Базис.WorkPlace:
  - Адрес (имя или IP-адрес и порт) диспетчера подключений Базис.WorkPlace.
  - Имя пользователя для подключения к диспетчеру подключений Базис.WorkPlace.
  - Файлы сертификатов для проверки подлинности брокера при подключении к удаленному рабочему столу под управлением Базис.WorkPlace.
  - Идентификатор Kaspersky Thin Client.
  - Количество попыток повторного подключения.
  - Профиль соединения Kaspersky Thin Client с брокером Базис.WorkPlace.
  - Параметры перенаправления на удаленный рабочий стол периферийных устройств: разрешено ли перенаправление USB-накопителей и смарт-карт.
  - Включено ли использование двух мониторов.
- Параметры подключения к RDP-серверу:
  - Адрес (имя или IP-адрес и порт) сервера Remote Desktop Connection Broker.
  - Домен и имя пользователя для подключения к серверу Remote Desktop Connection Broker.
  - Идентификатор коллекции Remote Desktop Connection Broker.
  - Псевдоним приложения.
  - Файлы сертификатов для проверки подлинности сервера Remote Desktop Connection Broker при подключении к удаленному рабочему столу или виртуальному приложению по протоколу RDP.
  - Параметры перенаправления на удаленный рабочий стол периферийных устройств:
    - Разрешено ли перенаправление USB-накопителей.

        - Разрешено ли перенаправление смарт-карт.
        - Разрешено ли перенаправление принтеров.
        - Разрешено ли перенаправление устройств воспроизведения звука.
        - Разрешено ли перенаправление устройств записи звука.
    - Включено ли использование двух мониторов.
    - Включено ли автоматическое подключение к удаленному рабочему столу или виртуальному приложению при разрыве соединения.
    - Параметры внешнего вида окон:
        - Включено ли сглаживание шрифтов.
        - Включена ли анимация меню.
        - Включено ли отображение фона рабочего стола.
        - Включено ли отображение содержимого окна при перемещении.
        - Включено ли использование тем в Microsoft Windows.
- Параметры сети:
    - Включена ли автоматическая настройка сети по DHCP.
    - IP-адрес тонкого клиента.
    - Маска подсети.
    - Список IP-адресов DNS-серверов.
    - IP-адрес сетевого шлюза.
- Параметры энергосбережения: количество минут до выключения монитора и количество минут до выключения тонкого клиента при бездействии Kaspersky Thin Client.
- Параметры подключения к серверу журналирования:
    - Адрес (имя или IP-адрес и порт) сервера журналирования для отправки журналов событий и аудита.
    - Файлы сертификатов для проверки подлинности сервера журналирования при подключении Kaspersky Thin Client к этому серверу.
- Параметры даты и времени:
    - Дата и время, полученные от Сервера администрирования при последней синхронизации с Kaspersky Security Center.
    - Часовой пояс.
- Информация о доступных и скачанных обновлениях Kaspersky Thin Client:

- Статус доступности обновления.
- Статус установки обновления.
- Статус доставки обновления.
- Данные доступного обновления: версия Kaspersky Thin Client, название, дата и время выпуска, важность.
- Время последней успешной проверки обновления.
- Время успешной установки обновления.

- Информация о Лицензионных соглашениях Kaspersky Thin Client:
  - Идентификаторы Лицензионных соглашений.
  - Тексты Лицензионных соглашений на русском, английском, испанском и бразильском португальском языках.
  - Информация о факте принятия Лицензионных соглашений.
  - Информация о датах выпуска Лицензионных соглашений.

Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского". Данные передаются по зашифрованным каналам связи.

Включение и выключение Kaspersky Thin Client

Перед началом работы с Kaspersky Thin Client требуется подключить к тонкому клиенту мышь, клавиатуру и монитор/мониторы, используя соответствующие разъемы на задней панели устройства. Для начала работы с Kaspersky Thin Client нужно включить тонкий клиент.

Kaspersky Thin Client позволяет подключить к тонкому клиенту мышь, клавиатуру и монитор во время работы системы. При подключении второго монитора отобразится уведомление с предложением настроить взаимное расположение мониторов.

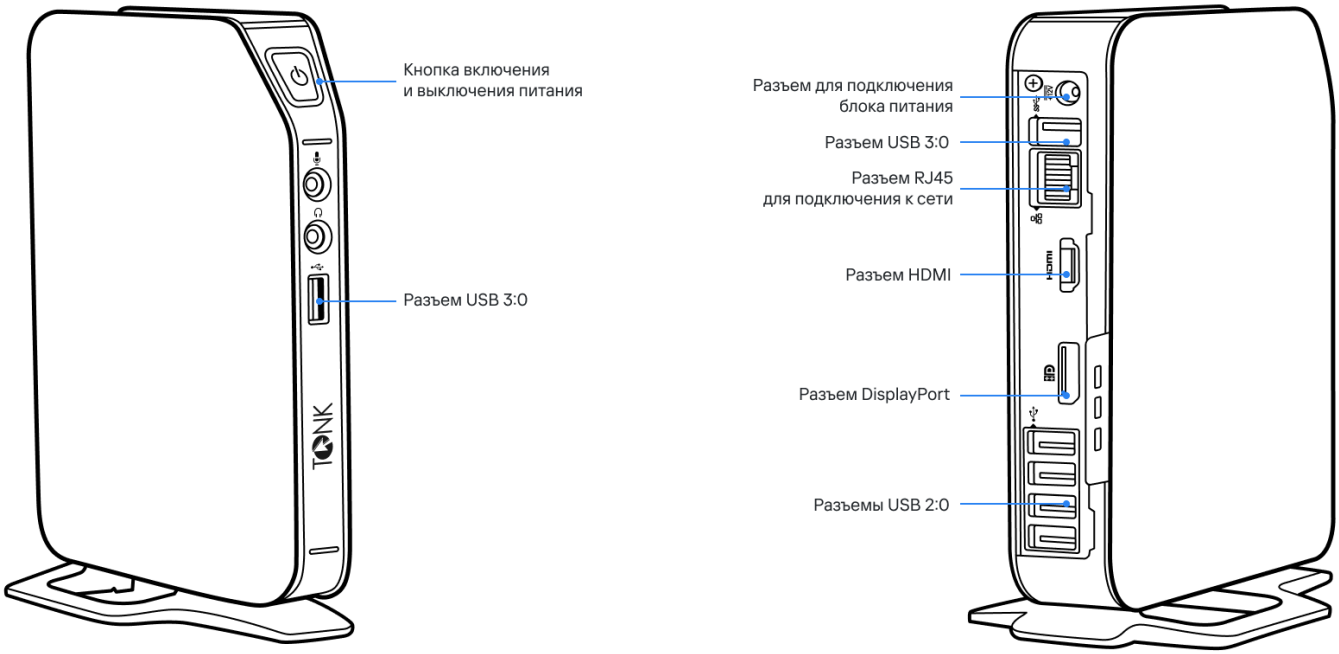
Чтобы включить Kaspersky Thin Client,

нажмите кнопку включения / выключения питания в верхней части лицевой панели тонкого клиента.

В результате на тонком клиенте начнет запускаться Kaspersky Thin Client.

В процессе запуска Kaspersky Thin Client на подключенном к тонкому клиенту мониторе последовательно отображаются заставка производителя тонкого клиента, приветствие загрузчика, журнал загрузчика и динамическая заставка загрузки Kaspersky Thin Client. Появление на экране основного окна Kaspersky Thin Client означает, что система включилась.

При первом запуске Kaspersky Thin Client отобразится окно принятия Лицензионного соглашения. Для продолжения работы с Kaspersky Thin Client нужно принять Лицензионное соглашение, предварительно с ним ознакомившись.



Лицевая и задняя панели тонкого клиента TONK TN1200

После завершения работы с Kaspersky Thin Client требуется его выключить.

Чтобы выключить Kaspersky Thin Client:

1. В главном окне Kaspersky Thin Client нажмите на кнопку завершения работы в панели управления .
2. В открывшемся меню выберите **Выключить**.

Kaspersky Thin Client будет выключен.

Перезагрузка Kaspersky Thin Client

Вы можете перезагрузить Kaspersky Thin Client, например если требуется применить выбранный язык интерфейса Kaspersky Thin Client.

Чтобы перезагрузить Kaspersky Thin Client:

1. В главном окне Kaspersky Thin Client нажмите на кнопку завершения работы в панели управления .
2. В открывшемся меню выберите пункт **Перезагрузить**.

Kaspersky Thin Client будет перезагружен.

Использование сертификатов в Kaspersky Thin Client

Криптографический протокол TLS обеспечивает безопасность передачи данных между клиентом и сервером с использованием сертификатов SSL-соединений. *Сертификат SSL-соединения* (далее SSL-сертификат или сертификат) – это блок данных, содержащий информацию о владельце сертификата, открытом ключе владельца, датах начала и окончания действия сертификата.

В Kaspersky Thin Client сертификаты используются в следующих целях:

- Подключение тонкого клиента к Kaspersky Security Center.
- Подключение к удаленной среде:
  - Проверка подлинности сервера Remote Desktop Connection Broker при подключении к удаленному рабочему столу или виртуальному приложению.
  - Проверка подлинности брокера при подключении к удаленному рабочему столу под управлением Базис.WorkPlace.
  - Проверка подлинности веб-адреса сервера при подключении к удаленной среде в Web Access.
- Подключение к серверу журналирования.

Если тонкий клиент не подключен к Kaspersky Security Center и администратор не назначал для него сертификаты в Web Console, при подключении к удаленной среде или к серверу журналирования пользователь тонкого клиента может самостоятельно принять или отклонить сертификат в интерфейсе Kaspersky Thin Client. Все принятые сертификаты будут сохраняться в хранилище тонкого клиента. В такой ситуации пользователь может подключаться в том числе к тем узлам и использовать те сертификаты, которые не контролирует администратор.

Рекомендуется настроить подключение Kaspersky Thin Client к серверу журналирования и к удаленной среде только с применением сертификатов, назначенных администратором в Web Console. При этом все сертификаты, принятые пользователем ранее, будут удалены из хранилища тонкого клиента. Такие меры помогут предотвратить подключение Kaspersky Thin Client к недоверенным узлам.

Рекомендуется обновлять назначенные сертификаты в следующих случаях:

- текущие сертификаты скомпрометированы;
- закончился срок действия сертификатов;
- нужно выполнить регулярное обновление сертификатов в соответствии с требованиями информационной безопасности вашей организации.

Kaspersky Thin Client не проверяет, находится ли сертификат в списке отозванных сертификатов (Certificate Revocation List).

Настройка Kaspersky Thin Client

Этот раздел содержит информацию о настройке Kaspersky Thin Client.

Сценарий: быстрый старт для администратора

В этом разделе приводится последовательность действий, которые требуется выполнить администратору, чтобы настроить Kaspersky Thin Client и Kaspersky Security Center, а также установить между ними соединение.

Инструкции по установке Kaspersky Thin Client на тонкий клиент приведены в отдельной статье.

Перед установкой Kaspersky Thin Client или перед первым включением тонкого клиента, на котором предустановлена система Kaspersky Thin Client, рекомендуется обновить BIOS на тонком клиенте до последней версии, установить пароль на изменение параметров BIOS и настроить возможность загрузки только с локального SSD-устройства. Принятые меры помогут предотвратить вероятные риски безопасности, такие как подмена операционной системы, подмена или удаление сертификатов подключения к удаленным серверам и получение несанкционированного доступа к настройкам операционной системы.

Сценарий первоначальной настройки Kaspersky Thin Client и Kaspersky Security Center, а также установки соединения между ними, состоит из следующих этапов:

1. **Установка Kaspersky Security Center**

   Загрузите дистрибутив Kaspersky Security Center и установите полную версию Kaspersky Security Center на сервере. Дистрибутив полной версии Kaspersky Security Center включает Kaspersky Security Center Web Console. При установке рекомендуется выбрать стандартную установку. Подробную информацию об установке Kaspersky Security Center см. в разделе *Установка Kaspersky Security Center* в онлайн-справке Kaspersky Security Center.

2. **Настройка правил межсетевого экрана**

   Если для подключения тонкого клиента к Kaspersky Security Center планируется использовать порт по умолчанию, для межсетевого экрана операционной системы сервера, на котором установлен Kaspersky Security Center, настройте правила, разрешающие подключение по протоколу TCP через порт 13292. Если планируется использовать порт отличный от 13292, настройте разрешение для нужного порта. Подробную информацию о настройке правил межсетевого экрана вы можете получить в руководстве используемой операционной системы.

3. **Установка веб-плагина управления Kaspersky Security Management Suite**

   В Kaspersky Security Center Web Console установите веб-плагин управления Kaspersky Security Management Suite.

4. **Подготовка портов**

   Kaspersky Thin Client использует для подключения к Kaspersky Security Center мобильный протокол. На Сервере администрирования Kaspersky Security Center включите использование по протоколу TCP порта, доступ к которому вы настроили на шаге 2 этого сценария. Подробную информацию о включении на Сервере администрирования Kaspersky Security Center порта по протоколу TCP вы можете получить в разделе онлайн-справки Kaspersky Security Center *Изменение параметров управления мобильными устройствами*.

5. **Включение Kaspersky Thin Client**

Включите Kaspersky Thin Client и дождитесь загрузки системы. Ознакомьтесь с условиями Лицензионного соглашения и примите его.

6. **Настройка параметров Kaspersky Thin Client**

   После включения и принятия лицензионного соглашения Kaspersky Thin Client настройте общие параметры и параметры подключения к сети.

7. **Настройка подключения Kaspersky Thin Client к Kaspersky Security Center**

   В интерфейсе Kaspersky Thin Client настройте подключение к Kaspersky Security Center.

8. **Добавление Kaspersky Thin Client в список управляемых устройств**

   Подключитесь к Kaspersky Security Center Web Console и добавьте Kaspersky Thin Client в список управляемых устройств Kaspersky Security Center. Политики в Kaspersky Security Center Web Console действуют только для управляемых устройств.

9. **Создание активной политики Kaspersky Security Center для Kaspersky Thin Client**

   Если требуется управление группой устройств создайте активную политику для Kaspersky Thin Client.

10. **Назначение сертификатов для группы устройств**

    Назначьте сертификаты для подключения к удаленной среде и к серверу журналирования для группы устройств. Также рекомендуется добавить сертификат для подключения Kaspersky Thin Client к Kaspersky Security Center.

В результате выполнения этих действий система Kaspersky Thin Client будет готова к работе, и вы сможете управлять Kaspersky Thin Client через интерфейс Kaspersky Thin Client или через Kaspersky Security Center Web Console, а также осуществлять мониторинг событий Kaspersky Thin Client.

Сценарий: назначение сертификатов для группы тонких клиентов

При назначении сертификатов для группы администрирования в Kaspersky Security Center Web Console пользователь тонкого клиента, входящего в такую группу, сможет подключаться только к серверам, для которых были добавлены сертификаты в Web Console.

Предварительно требуется установить и настроить Kaspersky Security Center.

Сценарий назначения сертификатов для группы тонких клиентов состоит из следующих этапов:

1. **Настройка подключения к Kaspersky Security Center**

   В интерфейсе Kaspersky Thin Client настройте подключение Kaspersky Security Center.

2. **Добавление тонких клиентов в управляемые устройства**

   В интерфейсе Web Console добавьте тонкий клиент в группу управляемых устройств, если он находится в нераспределенных устройствах.

3. **Создание активной политики Kaspersky Security Center для Kaspersky Thin Client**

   В интерфейсе Web Console создайте активную политику для необходимой группы устройств.

4. **Добавление сертификатов для подключения к удаленной среде и к серверу журналирования**

В интерфейсе Kaspersky Security Center Web Console добавьте необходимые сертификаты и переведите переключатель в правой части страницы в положение **Принудительно**. Дождитесь выполнения синхронизации Kaspersky Thin Client и Kaspersky Security Center. Вы можете установить период синхронизации при настройке Kaspersky Thin Client через Kaspersky Security Center Web Console. После синхронизации устройства получат сертификаты Сервера администрирования Kaspersky Security Center.

Если вы удалите все сертификаты, назначенные группе устройств, пользователи тонких клиентов из такой группы смогут подключаться к любым серверам, в том числе к тем, для которых не были назначены сертификаты.

Сценарий: миграция тонких клиентов на новый Сервер Kaspersky Security Center

В этом разделе приводится последовательность действий, которые требуется выполнить администратору при подключении устройств с Kaspersky Thin Client к управлению через новый Сервер администрирования Kaspersky Security Center (далее также Сервер), если управление этой группой ранее осуществлялось через другой Kaspersky Security Center.

Сценарий настройки управления Kaspersky Thin Client при миграции тонких клиентов на новый Сервер Kaspersky Security Center состоит из следующих этапов:

1. **Установка нового Сервера администрирования Kaspersky Security Center**

   Загрузите дистрибутив Kaspersky Security Center и установите полную версию Kaspersky Security Center на сервере. Дистрибутив полной версии Kaspersky Security Center включает Kaspersky Security Center Web Console. При установке рекомендуется выбрать стандартную установку. Подробную информацию об установке Kaspersky Security Center см. в разделе *Установка Kaspersky Security Center* в онлайн-справке Kaspersky Security Center.

2. **Настройка правил межсетевого экрана**

   Если для подключения тонкого клиента к Kaspersky Security Center планируется использовать порт по умолчанию, для межсетевого экрана операционной системы сервера, на котором установлен Kaspersky Security Center, настройте правила, разрешающие подключение по протоколу TCP через порт 13292. Если планируется использовать порт отличный от 13292, настройте разрешение для нужного порта. Подробную информацию о настройке правил межсетевого экрана вы можете получить в руководстве используемой операционной системы.

3. **Установка веб-плагина управления Kaspersky Security Management Suite**

   В Web Console для нового Сервера администрирования Kaspersky Security Center установите веб-плагин управления Kaspersky Security Management Suite.

4. **Подготовка портов**

   Kaspersky Thin Client использует для подключения к Kaspersky Security Center мобильный протокол. На Сервере администрирования Kaspersky Security Center включите использование по протоколу TCP порта, доступ к которому вы настроили на шаге 2 этого сценария. Подробную информацию о включении на Сервере администрирования Kaspersky Security Center порта по протоколу TCP вы можете получить в разделе онлайн-справки Kaspersky Security Center *Изменение параметров Управления мобильными устройствами*.

5. **Включение Kaspersky Thin Client**

   Включите Kaspersky Thin Client и дождитесь загрузки системы.

6. **Создание активной политики Kaspersky Security Center для Kaspersky Thin Client**

В используемой ранее Web Console создайте активную политику для группы устройств, управление которыми планируется осуществлять через новый Kaspersky Security Center.

7. **Обновление сертификата безопасности для подключения к Kaspersky Security Center**

   Выпустите сертификат, который будет сохранен на текущем Сервере администрирования Kaspersky Security Center как резервный и затем будет использован на новом Сервере как основной.

8. **Настройка подключения Kaspersky Thin Client к новому Серверу Kaspersky Security Center**

   Если в инфраструктуре вашего предприятия развернут сервер DHCP и получение параметров подключения Kaspersky Thin Client и Kaspersky Security Center происходит автоматически, задайте в опции 224 IP-адрес или доменное имя нового Сервера администрирования Kaspersky Security Center и дождитесь выполнения синхронизации всех устройств с Kaspersky Thin Client и Kaspersky Security Center.

   Если в инфраструктуре вашего предприятия не развернут сервер DHCP, в интерфейсе Kaspersky Thin Client настройте подключение к новому Kaspersky Security Center вручную.

Группы администрирования тонких клиентов будут подключены к новому Серверу Kaspersky Security Center, и вы сможете управлять ими через интерфейс Web Console.

Настройка общих параметров

В интерфейсе Kaspersky Thin Client вы можете настроить общие параметры тонкого клиента. Например, вы можете указать имя тонкого клиента, которое будет отображаться в панели задач Kaspersky Thin Client и в Kaspersky Security Center Web Console, а также выбрать язык интерфейса Kaspersky Thin Client.

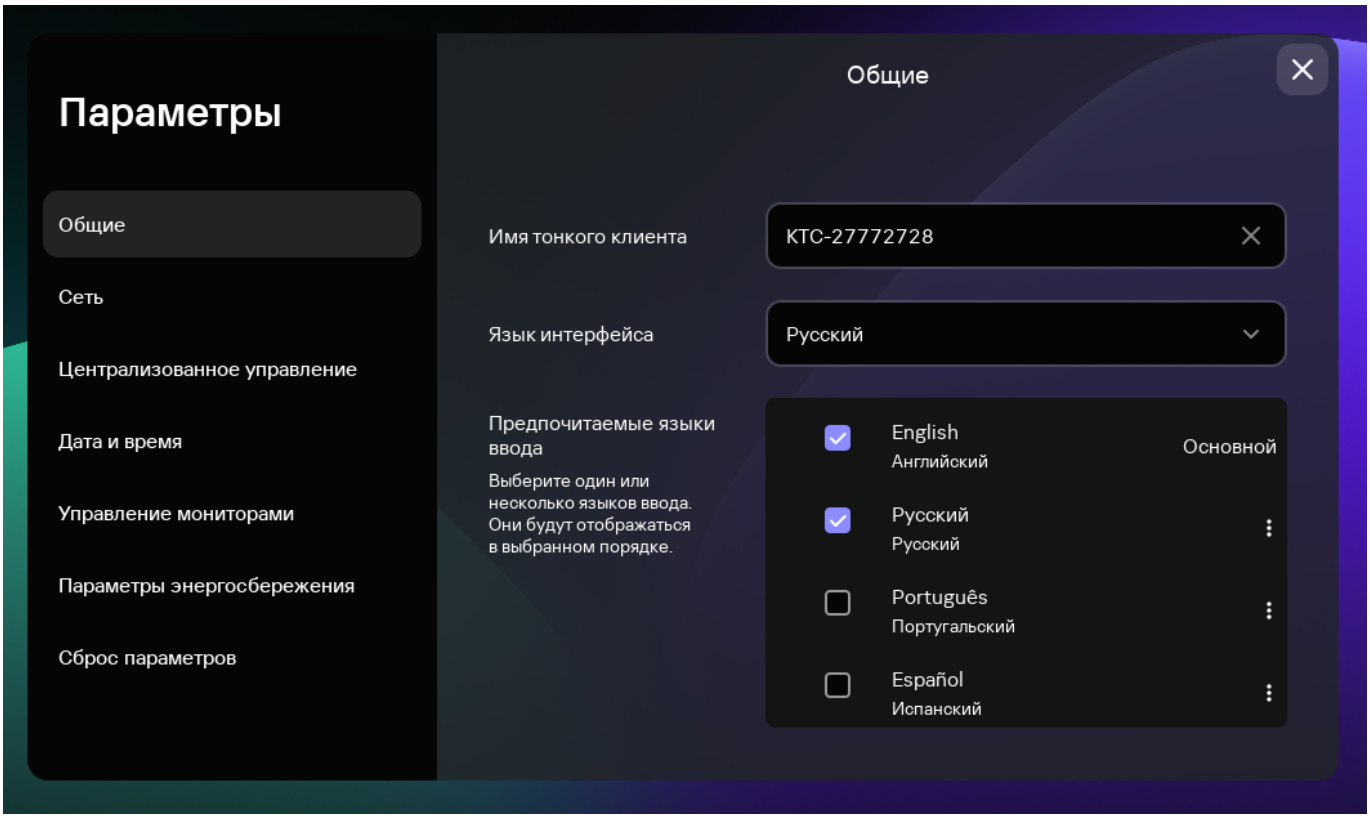
Если тонкий клиент входит в группу администрирования, значения параметров, указанных в этой статье, могут быть принудительно заданы через Web Console. В этом случае настройка данных параметров в интерфейсе Kaspersky Thin Client будет недоступна.

Указанные в этой статье параметры также могут быть скрыты на тонком клиенте.

Чтобы настроить общие параметры Kaspersky Thin Client:

1. В панели управления Kaspersky Thin Client нажмите на кнопку и в открывшемся меню выберите **Параметры**.

2. В открывшемся окне выберите раздел **Общие** (см. рис. ниже).



Параметры. Раздел **Общие**

3. В поле **Имя тонкого клиента** введите имя, под которым Kaspersky Thin Client будет отображаться в Web Console. Допускается использовать прописные и строчные латинские и русские буквы, цифры и дефис. Длина имени тонкого клиента не должна превышать 30 символов.

4. В раскрывающемся списке **Язык интерфейса** выберите язык интерфейса. Kaspersky Thin Client поддерживает русский, английский, испанский и бразильский португальский языки интерфейса.

5. В раскрывающемся списке **Предпочитаемые языки ввода** выберите один или несколько языков. Kaspersky Thin Client поддерживает русский, английский, испанский и бразильский португальский языки ввода. Выбранные языки будут отображаться в панели управления Kaspersky Thin Client в том порядке, в котором вы их выбрали, и будут доступны для переключения языка ввода текста с клавиатуры.

Изменения вступят в силу после перезагрузки тонкого клиента.

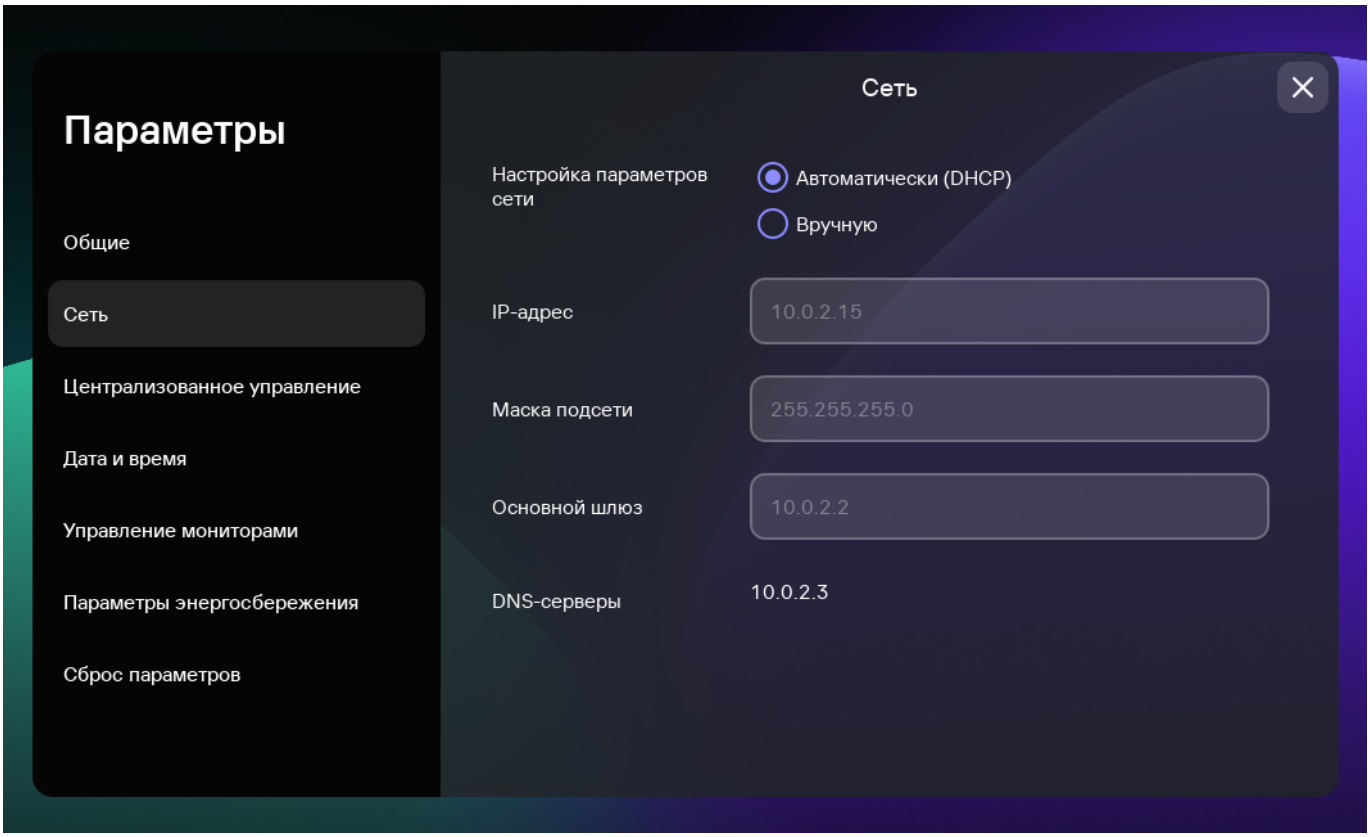
Настройка параметров сети

В разделе **Параметры** → **Сеть** вы можете настроить параметры сети для подключения Kaspersky Thin Client к сети.

Чтобы настроить параметры сети:

1. В панели управления Kaspersky Thin Client нажмите на кнопку и в открывшемся меню выберите **Параметры**.

2. В открывшемся окне выберите раздел **Сеть** (см. рис. ниже).



Параметры. Раздел Сеть

3. Настройте параметры подключения Kaspersky Thin Client к сети:

   - Если требуется получать параметры сети автоматически по протоколу DHCP, для параметра **Настройка параметров сети** выберите **Автоматически (DHCP)**. В этом режиме поля **IP-адрес**, **Маска подсети**, **Основной шлюз** и **DNS-серверы** недоступны для заполнения.

   - Если требуется указать параметры сети вручную, для параметра **Настройка параметров сети** выберите **Вручную** и выполните следующие действия:

     - В поле **IP-адрес** введите IP-адрес Kaspersky Thin Client в формате IPv4.

     - В поле **Маска подсети** введите маску подсети.

     - В поле **Основной шлюз** введите адрес сетевого шлюза.

     - В поле **DNS-серверы** введите адреса DNS-серверов. Вы можете указать не более двух адресов. Это поле не является обязательным для заполнения.

4. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить изменения.

Настройка параметров подключения Kaspersky Thin Client к Kaspersky Security Center

Для управления тонким клиентом через Web Console необходимо настроить параметры подключения Kaspersky Thin Client к Серверу администрирования Kaspersky Security Center.

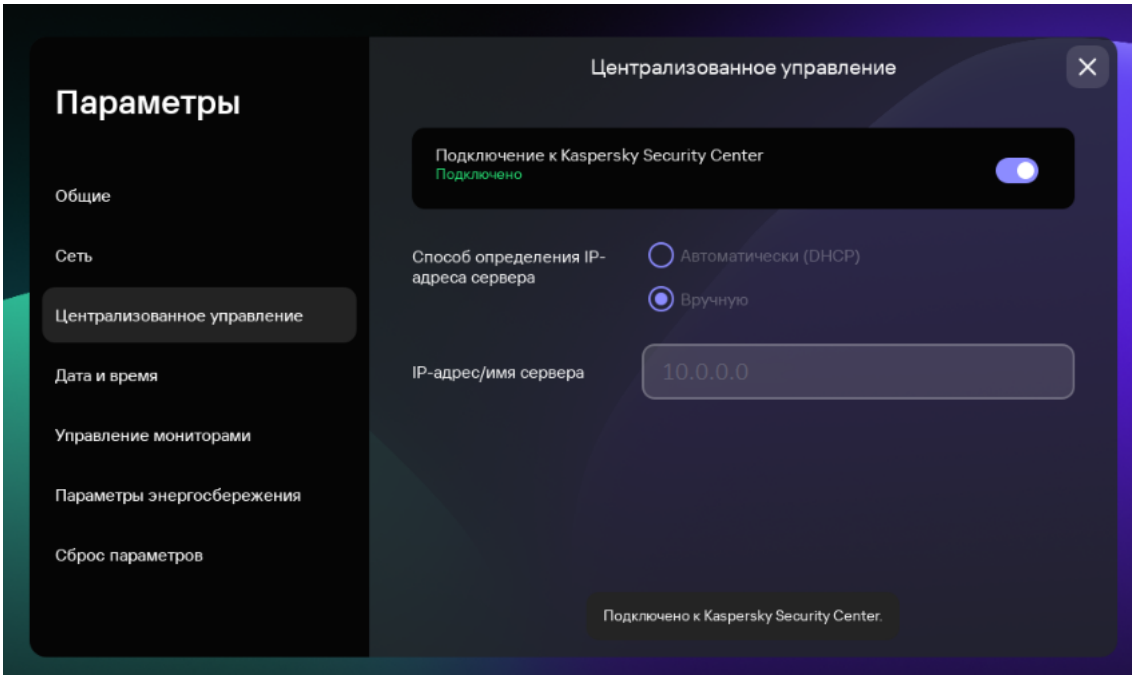
Подключение Kaspersky Thin Client к Серверу Kaspersky Security Center необходимо осуществлять в безопасном сегменте сети. Рекомендуется настраивать подключение при помощи квалифицированного специалиста из вашей организации, который сможет удостовериться в подлинности принимаемого сертификата.

Рекомендуется использовать отдельный Сервер администрирования Kaspersky Security Center для управления тонкими клиентами, чтобы получать важные обновления безопасности от серверов обновлений "Лаборатории Касперского". Это связано с тем, что на одном Сервере администрирования Kaspersky Security Center может быть только одна активная задача обновления с одним приоритетным источником обновлений.

Чтобы настроить параметры подключения Kaspersky Thin Client к Серверу администрирования Kaspersky Security Center:

1. В панели управления Kaspersky Thin Client нажмите на кнопку и в открывшемся меню выберите **Параметры**.

2. В открывшемся окне выберите раздел **Централизованное управление** (см. рис. ниже).



Параметры. Раздел **Централизованное управление**

3. В открывшемся окне **Централизованное управление** настройте следующие параметры подключения Kaspersky Thin Client к Kaspersky Security Center:

   - Если вы хотите получать параметры подключения Kaspersky Thin Client к Kaspersky Security Center автоматически по протоколу DHCP, в блоке **Способ определения IP-адреса сервера** выберите **Автоматически (DHCP)**. В этом режиме поле **IP-адрес/имя сервера** недоступно для изменения.

     Для использования этого варианта подключения требуется развернуть в инфраструктуре предприятия сервер DHCP и задать на нем в опции 224 IP-адрес или доменное имя Сервера администрирования Kaspersky Security Center, к которому планируется подключение Kaspersky Thin Client. Kaspersky Thin Client принимает в опции 224 значения в формате `IP-адрес:Порт` или `Имя сервера:Порт` (тип значения – строка). Например, `192.168.2.4` или `ksc.example.com:12345`. Порт требуется указывать, только если для подключения используется порт отличный от 13292.

     По умолчанию включено автоматическое получение параметров подключения Kaspersky Thin Client к Kaspersky Security Center по протоколу DHCP.

- Если вы хотите указать параметры подключения Kaspersky Thin Client к Kaspersky Security Center вручную, в блоке **Способ определения IP-адреса сервера** выберите **Вручную** и в поле **IP-адрес/имя сервера** введите IP-адрес или имя Сервера администрирования Kaspersky Security Center. Если вы используете порт, отличный от 13292, укажите его в формате `IP-адрес:Порт` или `Имя сервера:Порт`.

4. Переведите переключатель **Подключение к Kaspersky Security Center** в положение включено.

5. Если вы подключаетесь к Kaspersky Security Center впервые, в открывшемся окне **Добавление сертификата** проверьте параметры сертификата для подключения Kaspersky Thin Client к Kaspersky Security Center и нажмите на кнопку **Добавить сертификат**. При последующих подключениях тонкого клиента к Kaspersky Security Center будет использоваться добавленный сертификат.

   Если в Kaspersky Security Center изменился сертификат для подключения Kaspersky Thin Client к Kaspersky Security Center для продолжения настройки параметров подключения требуется подтвердить изменение сертификата.

Будет выполнена попытка подключения Kaspersky Thin Client к Kaspersky Security Center. После успешного подключения к Kaspersky Security Center отобразится статус **Подключено к Kaspersky Security Center**.

Изменение параметров подключения Kaspersky Thin Client к Kaspersky Security Center

Если тонкий клиент входит в группу администрирования, значения параметров, указанных в этой статье, могут быть принудительно заданы через Web Console. В этом случае настройка данных параметров в интерфейсе Kaspersky Thin Client будет недоступна.

Указанные в этой статье параметры также могут быть скрыты на тонком клиенте.

Чтобы изменить параметры подключения Kaspersky Thin Client к Kaspersky Security Center:

1. В панели управления Kaspersky Thin Client нажмите на кнопку и в открывшемся меню выберите **Параметры**.

2. В открывшемся окне выберите раздел **Централизованное управление**.

3. Переведите переключатель **Подключение к Kaspersky Security Center** в положение выключено.

4. В открывшемся окне **Подтверждение отключения** посмотрите и запомните код подтверждения для отключения Kaspersky Thin Client от Kaspersky Security Center, сообщите его администратору Kaspersky Security Center. Контакты администратора указаны в окне **Подтверждение отключения**. Администратор в ответ должен сообщить код подтверждения.

5. Нажмите на кнопку **Далее**.

6. В открывшемся окне **Код подтверждения** введите код, который сообщил вам администратор Kaspersky Security Center и нажмите на кнопку **Подтвердить**.

   Kaspersky Thin Client будет отключен от управления через Kaspersky Security Center.

7. В окне **Централизованное управление** вручную настройте параметры подключения к Kaspersky Security Center.

8. Переведите переключатель **Подключение к Kaspersky Security Center** в положение включено.

Будет выполнена попытка подключения тонкого клиента к Kaspersky Security Center. После успешного подключения к Kaspersky Security Center отобразится статус **Подключено к Kaspersky Security Center**.

Настройка параметров подключения к удаленной среде по протоколу RDP

Kaspersky Thin Client позволяет настроить параметры подключения к виртуальному приложению или удаленному рабочему столу по протоколу RDP.

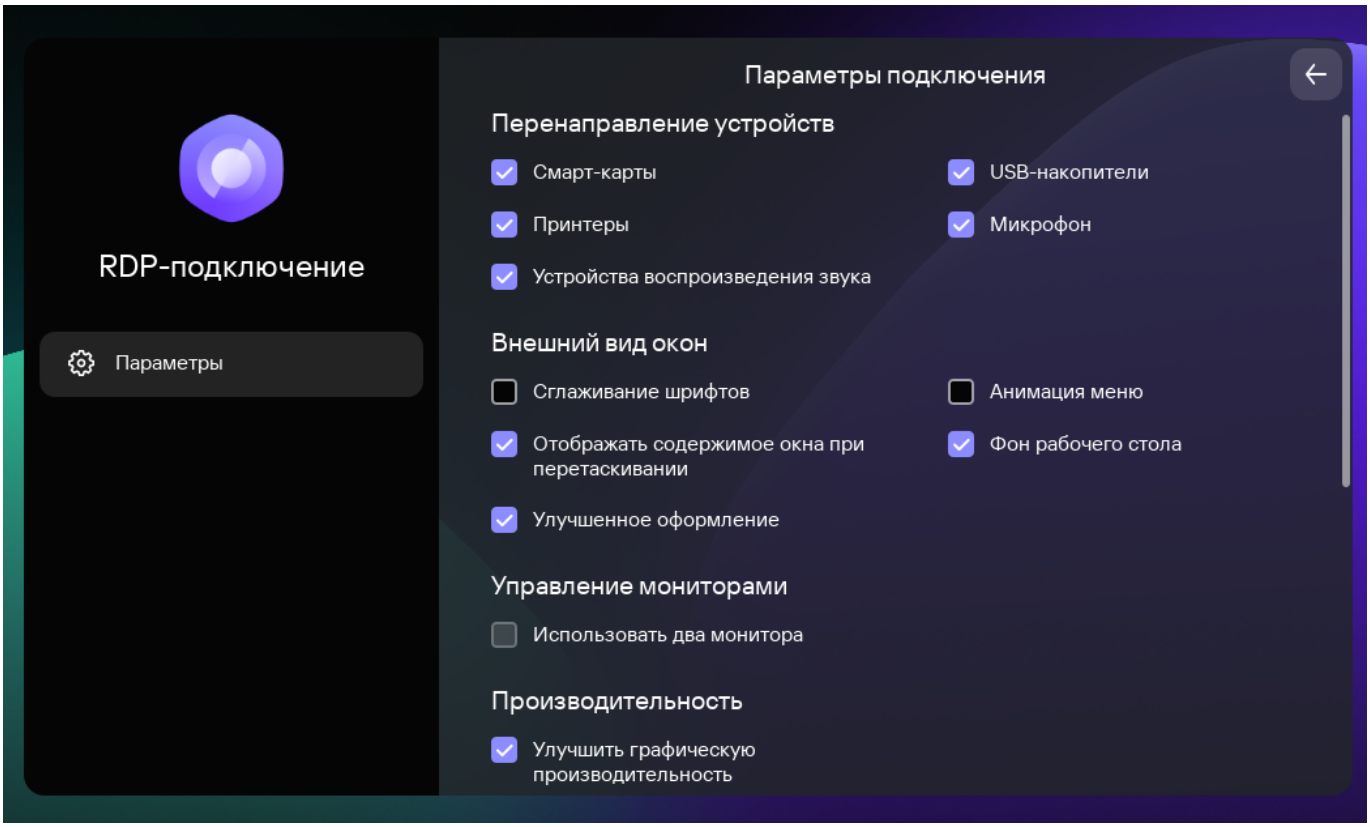
Информация об устройствах, перенаправляемых в удаленную среду, приведена в отдельной статье.

Для корректного перенаправления USB-устройств на удаленный рабочий стол в операционной системе Microsoft Windows 10 требуется включить службу Microsoft Remote Desktop Services и разрешить перенаправление устройств Plug and Play в параметрах Remote Desktop Services. Для операционных систем Microsoft Windows Server 2016 и Microsoft Windows Server 2019 также требуется разрешить удаленное подключение с использованием службы Remote Desktop Services и разрешить установку правил удаленного управления для сессий подключения в службе Microsoft Remote Desktop Services.

Чтобы настроить параметры подключения к удаленному рабочему столу или виртуальному приложению по протоколу RDP:

1. В главном окне Kaspersky Thin Client нажмите на кнопку **RDP**.
2. В открывшемся окне подключения нажмите **Параметры** в левой части окна.

   Откроется окно настройки параметров подключения к удаленному рабочему столу (см. рис. ниже).



Окно настройки параметров подключения к удаленному рабочему столу по протоколу RDP

3. В блоке параметров **Перенаправление устройств** напротив необходимых устройств установите следующие флажки:

- **Смарт-карты**, если хотите включить перенаправление смарт-карт и токенов.
- **USB-накопители**, если хотите включить перенаправление USB-накопителей.
- **Принтеры**, если хотите включить перенаправление принтеров.

  На удаленном компьютере должен быть установлен драйвер для принтера, который подключен к тонкому клиенту.
- **Микрофон**, если хотите включить перенаправление устройств записи звука.

  Управление громкостью и другими параметрами выполняется на удаленном компьютере.
- **Устройства воспроизведения звука**, если хотите включить перенаправление наушников или колонок.

  Kaspersky Thin Client поддерживает воспроизведение в моно и стерео форматах. Управление громкостью и другими параметрами выполняется в удаленной среде.

4. В блоке **Внешний вид окон** установите флажки напротив графических параметров удаленного рабочего стола, которые требуется использовать:
   - **Сглаживание шрифтов**.
   - **Анимация меню**.
   - **Фон рабочего стола**.
   - **Отображать содержимое окна при перетаскивании**.
   - **Улучшенное оформление**.

   Включение параметров отображения удаленного рабочего стола может замедлить скорость работы Kaspersky Thin Client.

5. Если на вашем рабочем месте установлено два монитора и вы хотите, чтобы изображение удаленного рабочего стола выводилось на оба монитора, в блоке **Управление мониторами** установите флажок **Использовать два монитора**. Если требуется, вы можете настроить расположения мониторов.

6. Если требуется улучшить отображение и плавность графических элементов при подключении к удаленной среде, в блоке **Производительность** установите флажок **Улучшить графическую производительность**.

   Если требуется подключиться к удаленному рабочему столу под управлением операционной системы Microsoft Windows 7, снимите флажок **Улучшить графическую производительность**. Эта функциональность не поддерживается при подключении к удаленным рабочим столам под управлением Microsoft Windows 7.

7. Если для подключения к удаленному рабочему столу требуется использовать брокер Microsoft Remote Desktop Connection Broker в поле **Идентификатор коллекции Remote Desktop Connection Broker** укажите идентификатор коллекции, в формате `tsv://MS Terminal Services Plugin.1.collection_id`, где `collection_id` – идентификатор коллекции.

   Для подключения к виртуальному приложению необходимо указать идентификатор коллекции Remote Desktop Connection Broker.

8. Если требуется запустить виртуальное приложение, в поле **Псевдоним приложения** укажите псевдоним приложения.

9. Если вы хотите, чтобы подключение к удаленному рабочему столу восстанавливалось автоматически после разрыва соединения, установите флажок **Подключаться повторно, если соединение прервано**.

10. Нажмите на стрелку назад в верхнем правом углу окна для возврата к сессии подключения.

Настройка параметров подключения к удаленной среде в инфраструктуре Базис.WorkPlace

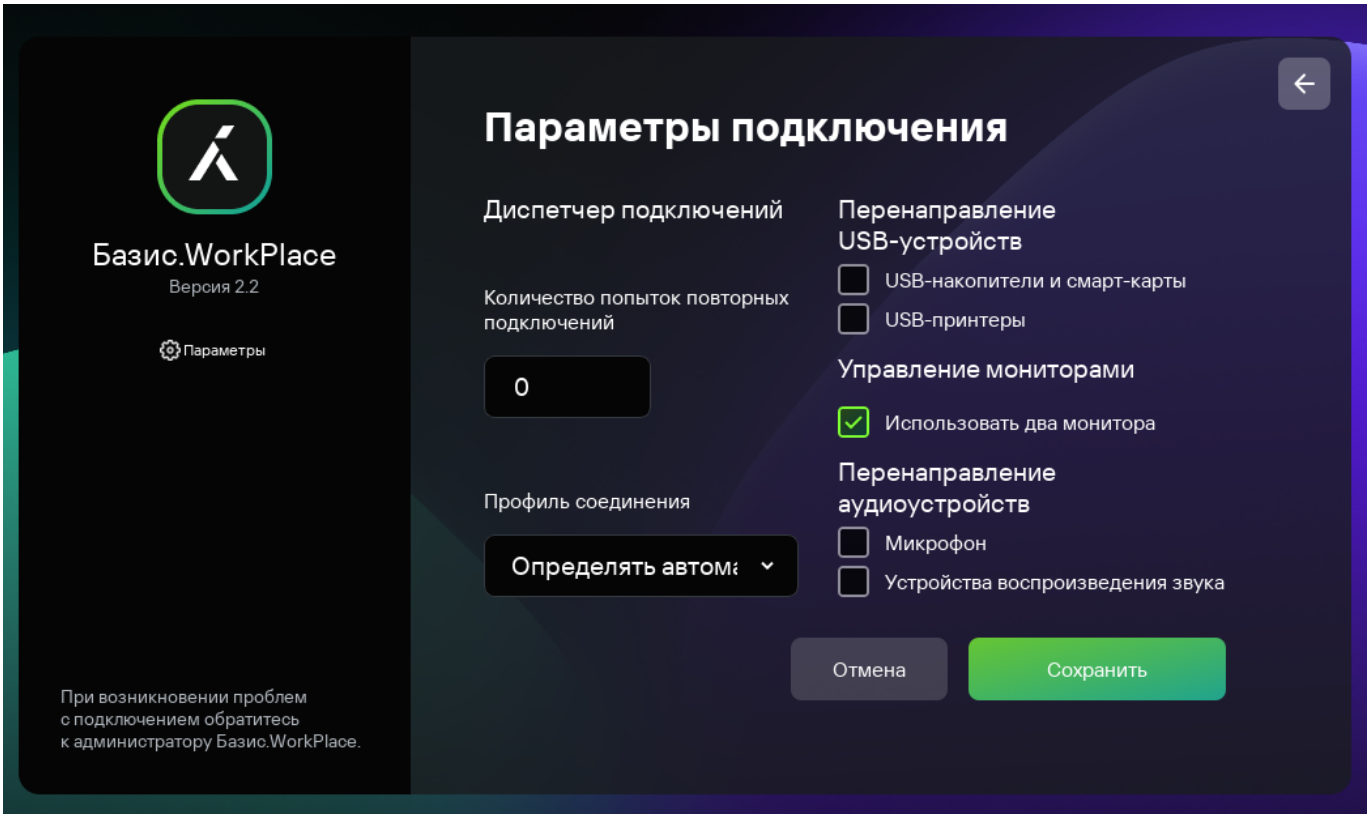
Kaspersky Thin Client позволяет настроить параметры подключения к удаленной среде в инфраструктуре Базис.WorkPlace.

Информация об устройствах, перенаправляемых в удаленную среду, приведена в отдельной статье.

Чтобы настроить параметры подключения к удаленной среде в инфраструктуре Базис.WorkPlace:

1. В главном окне Kaspersky Thin Client нажмите на кнопку **Базис.WorkPlace**.

2. В открывшемся окне подключения к удаленному рабочему столу нажмите **Параметры** в левой части окна.
   Откроется окно настройки параметров подключения к удаленному рабочему столу (см. рис. ниже).



Окно настройки параметров подключения к удаленному рабочему столу под управлением Базис.WorkPlace

3. Если требуется включить или выключить перенаправление устройств в удаленную среду, в блоке **Перенаправление USB-устройств** установите или снимите необходимые флажки.

> Перенаправление USB-устройства на удаленный рабочий стол под управлением Базис.WorkPlace может быть заблокировано администратором Базис.WorkPlace.

4. В поле **Количество попыток повторных подключений** введите количество попыток для повторного подключения к брокеру Базис.WorkPlace, которое должен выполнить Kaspersky Thin Client при разрыве соединения. Вы можете указать не более пяти попыток для повторного подключения.

5. В раскрывающемся списке **Профиль соединения** выберите тип соединения Kaspersky Thin Client с брокером Базис.WorkPlace. Тип соединения зависит от скорости соединения. Для выбора доступны следующие значения:

   - **Определять автоматически**.
   - **Модем**.
   - **Низкоскоростное широкополосное**.
   - **Спутник**.
   - **Высокоскоростное широкополосное**.
   - **Глобальная сеть**.
   - **Локальная сеть**.

6. Если на вашем рабочем месте установлено два монитора и вы хотите, чтобы изображение удаленного рабочего стола выводилось на оба монитора, в блоке **Управление мониторами** установите флажок **Использовать два монитора**. Если требуется, вы можете настроить расположения мониторов.

7. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить изменения.

8. Нажмите на стрелку назад в верхнем правом углу окна для возврата к окну подключения к удаленному рабочему столу.

Настройка параметров энергосбережения

> Если тонкий клиент входит в группу администрирования, значения параметров, указанных в этой статье, могут быть принудительно заданы через Web Console. В этом случае настройка данных параметров в интерфейсе Kaspersky Thin Client будет недоступна.

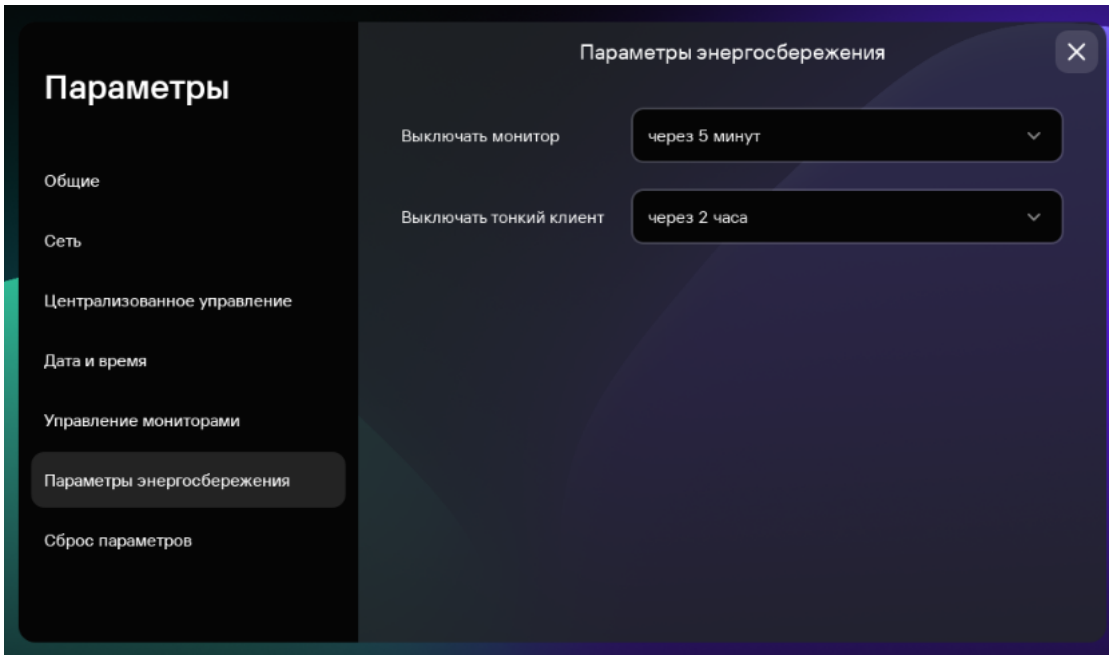
> Указанные в этой статье параметры также могут быть скрыты на тонком клиенте.

Вы можете настроить время выключения монитора. При нажатии клавиши мыши или клавиатуры или при перемещении мыши монитор включится автоматически. Также вы можете настроить время выключения тонкого клиента при бездействии Kaspersky Thin Client. Для возобновления работы тонкого клиента потребуется его включить.

Чтобы настроить параметры энергосбережения:

1. В панели управления Kaspersky Thin Client нажмите на кнопку и в открывшемся меню выберите **Параметры**.

2. В открывшемся окне выберите раздел **Параметры энергосбережения** (см. рис. ниже).



Параметры. Раздел **Параметры энергосбережения**

3. В раскрывающемся списке **Выключать монитор** выберите время бездействия системы, по истечении которого монитор будет выключен.

4. В раскрывающемся списке **Выключать тонкий клиент** выберите время бездействия системы, по истечении которого тонкий клиент будет выключен.

Также вы можете настроить параметры энергосбережения через интерфейс Kaspersky Security Center Web Console.

Настройка расположения мониторов

Если на вашем рабочем месте установлено два монитора, вы можете выбрать какой из мониторов будет использоваться как основной, а какой как дополнительный при выводе изображения удаленного рабочего стола. На основном мониторе во время подключения к удаленному рабочему столу в верхней части экрана отображается панель подключения.

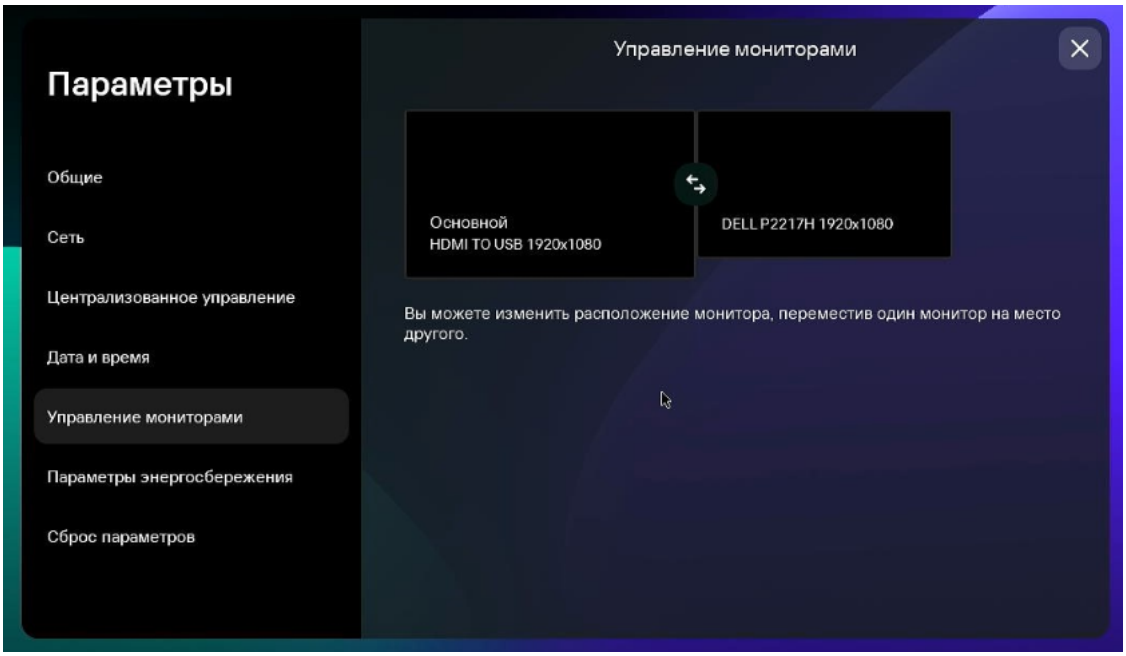
Предварительно требуется включить использование двух мониторов в параметрах подключения к удаленному рабочему столу по протоколу RDP или под управлением Базис.WorkPlace.

Чтобы изменить расположение мониторов для отображения удаленного рабочего стола:

1. В панели управления Kaspersky Thin Client нажмите на кнопку и в открывшемся меню выберите **Параметры**.

2. В открывшемся окне выберите раздел **Управление мониторами** (см. рис. ниже).

   В открывшемся окне схематично отображается расположение мониторов. Основной монитор всегда расположен слева и подписан.



Параметры. Раздел **Управление мониторами**

3. Измените расположение мониторов, нажав на кнопку , которая расположена между мониторами на схеме.

Расположение мониторов для отображения удаленного рабочего стола будет изменено.

Управление доступом к параметрам Kaspersky Thin Client

Вы можете выключить или включить отображение в интерфейсе Kaspersky Thin Client параметров, которые настраиваются однократно и в дальнейшем не используются в ключевых сценариях работы тонкого клиента.

Если тонкий клиент входит в группу администрирования, значения параметров могут быть заданы принудительно через Web Console. Такие параметры будут заблокированы для изменения в интерфейсе Kaspersky Thin Client и включение или выключение их отображения будет недоступно.

Чтобы выключить или включить отображение параметров Kaspersky Thin Client:

1. В панели управления Kaspersky Thin Client нажмите на кнопку и в открывшемся меню выберите **Инструменты**.

2. В открывшемся окне выберите раздел **Доступ к параметрам** (см. рис. ниже) и выполните одно из следующих действий:

   - Если требуется скрывать параметры, переведите переключатель в положение **Доступ закрыт**.

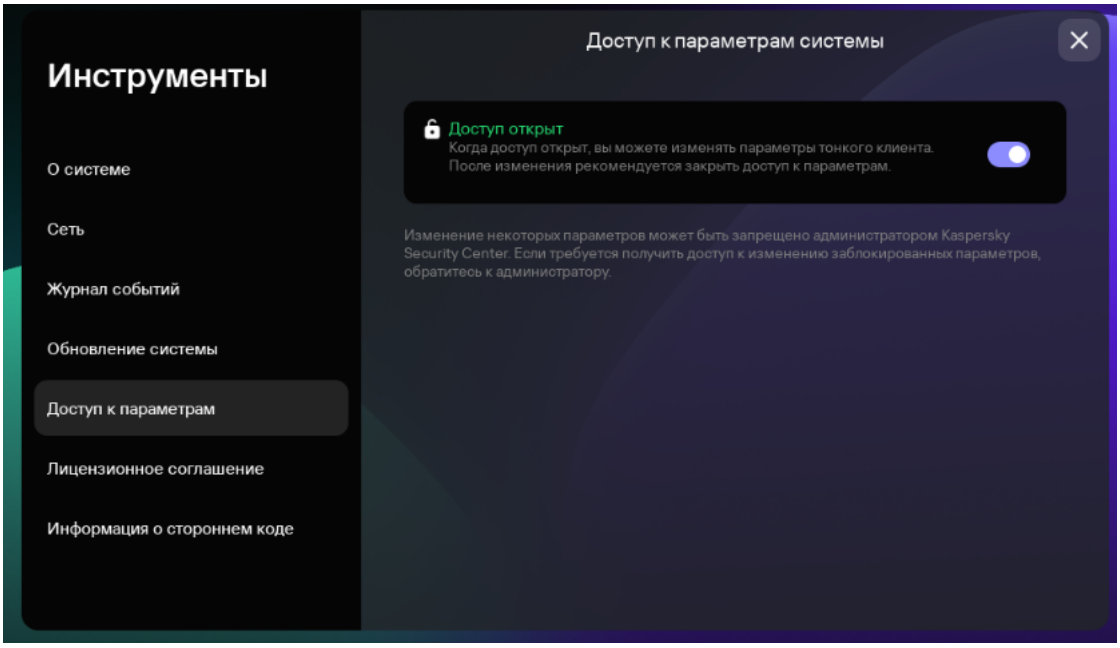
     В интерфейсе тонкого клиента будут скрыты все следующие параметры:

     - Параметры подключения по протоколу RDP.
     - Параметры подключения к Базис.WorkPlace.
     - Общие параметры.
     - Параметры сети.

- Параметры подключения к Kaspersky Security Center.
- Дата и время.
- Настройка параметров энергосбережения.
- Настройка расположения мониторов.
- Сброс параметров Kaspersky Thin Client.

- Если требуется показывать параметры, переведите переключатель в положение **Доступ открыт**.

  Параметры будут отображены. Вы сможете установить для них новые значения.



Инструменты. Раздел **Доступ к параметрам**

Настройка даты и времени

Тонкий клиент, подключенный к Kaspersky Security Center, получает дату и время от Сервера администрирования Kaspersky Security Center. Вы можете вручную изменить дату и время Kaspersky Thin Client, только если система не управляется через Kaspersky Security Center.

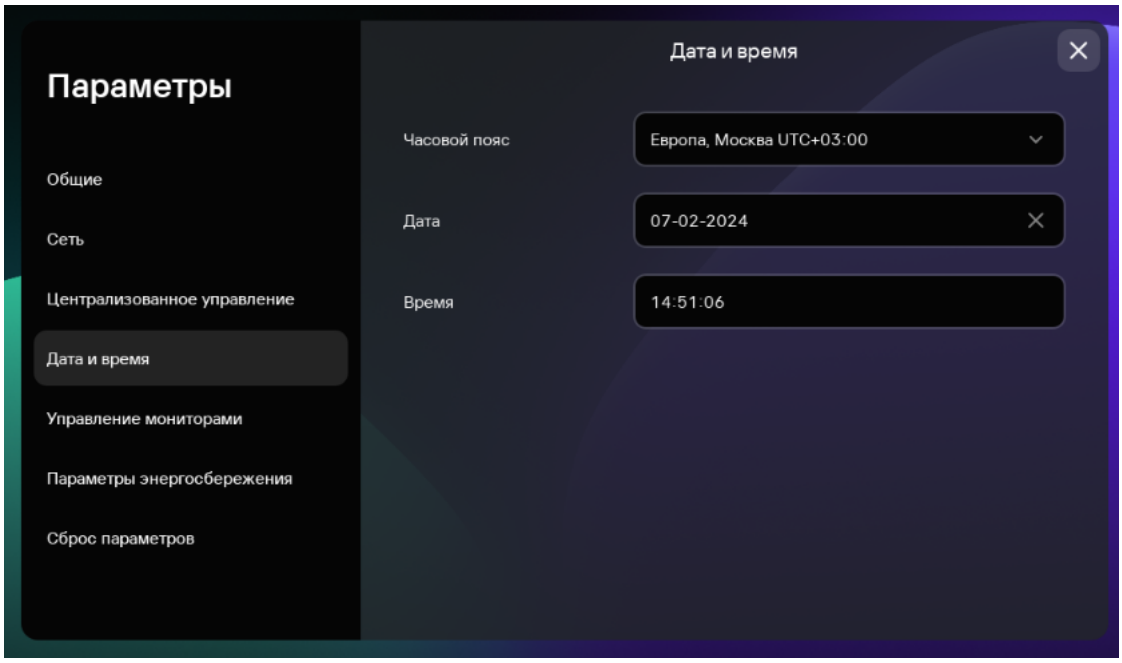
Если тонкий клиент входит в группу администрирования, значения параметров, указанных в этой статье, могут быть принудительно заданы через Web Console. В этом случае настройка данных параметров в интерфейсе Kaspersky Thin Client будет недоступна.

Указанные в этой статье параметры также могут быть скрыты на тонком клиенте.

Чтобы изменить дату и время Kaspersky Thin Client:

1. В панели управления Kaspersky Thin Client нажмите на кнопку и в открывшемся меню выберите **Параметры**.

2. В открывшемся окне выберите раздел **Дата и время** (см. рис. ниже).



Параметры. Раздел Дата и время

3. Настройте параметры даты и времени:

   - В раскрывающемся списке **Часовой пояс** выберите нужный часовой пояс.
   - В поле **Дата** введите текущую дату в формате `ДД-ММ-ГГГГ`.
   - В поле **Время** введите текущее время в формате `ЧЧ:ММ:СС`.

4. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить изменения.

Сброс параметров Kaspersky Thin Client

Сброс параметров приведет к потере всех установленных значений параметров и всех данных Kaspersky Thin Client (кроме журнала аудита и даты системы), а также к разрыву связи между устройством и Kaspersky Security Center. Рекомендуется выполнять сброс только по согласованию с администратором вашей организации.

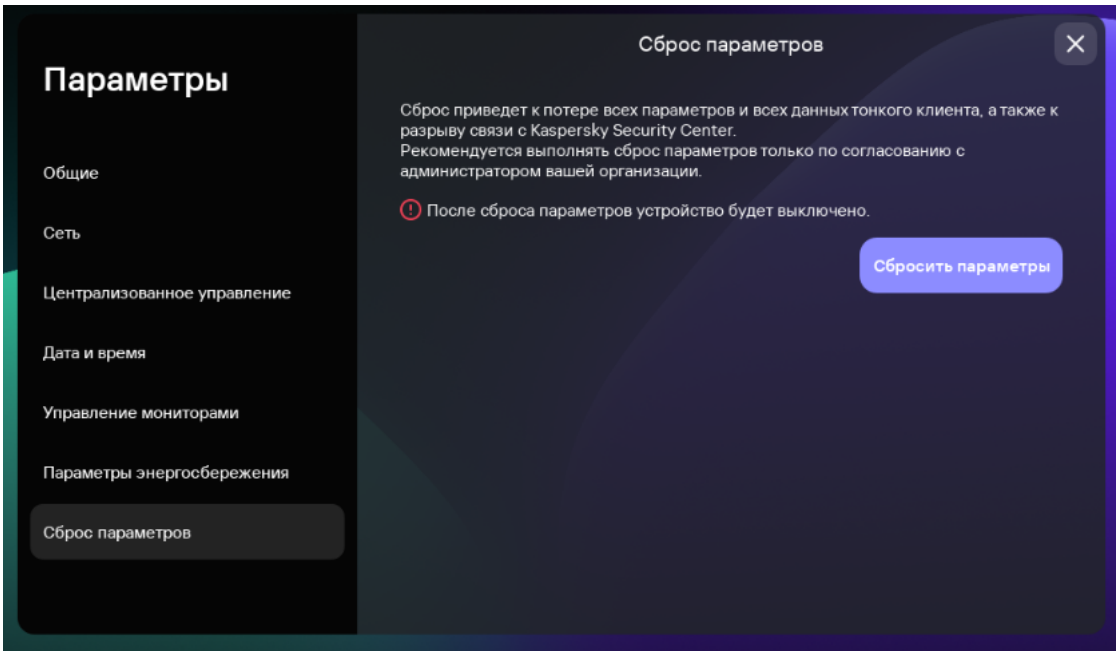
Если тонкий клиент входит в группу администрирования, значения параметров, указанных в этой статье, могут быть принудительно заданы через Web Console. В этом случае настройка данных параметров в интерфейсе Kaspersky Thin Client будет недоступна.

Указанные в этой статье параметры также могут быть скрыты на тонком клиенте.

Чтобы выполнить сброс параметров тонкого клиента, который не входит в группу администрирования:

1. В панели управления Kaspersky Thin Client нажмите на кнопку и в открывшемся меню выберите **Параметры**.

2. В открывшемся окне выберите раздел **Сброс параметров** (см. рис. ниже).



Параметры. Раздел **Сброс параметров**

В результате все установленные параметры Kaspersky Thin Client будут возвращены к первоначальным значениям (по умолчанию), а так же будут удалены все данные на устройстве (кроме журнала аудита и системной даты) и разорвано соединение между Kaspersky Thin Client и Kaspersky Security Center. После выполнения сброса тонкий клиент выключится.

Чтобы выполнить сброс параметров тонкого клиента, который входит в группу администрирования:

1. В панели управления Kaspersky Thin Client нажмите на кнопку и в открывшемся меню выберите **Параметры**.
2. В открывшемся окне выберите раздел **Сброс параметров**.
3. В открывшемся окне нажмите на кнопку **Сбросить параметры**.

   Откроется окно **Подтверждение сброса**, в котором отображается код подтверждения.
4. Сообщите администратору Kaspersky Security Center код подтверждения. Контакты администратора указаны в окне **Подтверждение сброса**. В ответ администратор Kaspersky Security Center сообщит вам код подтверждения.
5. Нажмите на кнопку **Далее**.
6. В открывшемся окне **Код подтверждения** введите код, который сообщил вам администратор Kaspersky Security Center, и нажмите на кнопку **Подтвердить**.

В результате все установленные параметры Kaspersky Thin Client будут возвращены к первоначальным значениям (по умолчанию), а так же будут удалены все данные на устройстве (кроме журнала аудита и системной даты) и разорвано соединение между Kaspersky Thin Client и Kaspersky Security Center. После выполнения сброса тонкий клиент выключится.

Управление Kaspersky Thin Client в интерфейсе тонкого клиента

В этом разделе описан основной сценарий работы с Kaspersky Thin Client и приведены инструкции по использованию Kaspersky Thin Client.

Основной сценарий работы с Kaspersky Thin Client состоит из следующих этапов:

1. **Подготовка Kaspersky Thin Client к включению**

   Подключите к тонкому клиенту периферийные устройства перед первым включением.

2. **Запуск Kaspersky Thin Client**

   Включите тонкий клиент для начала работы.

3. **Сессия подключения**

   Подключитесь к удаленной среде и начните работу.

4. **Блокирование рабочего стола и возобновление работы**

   Если требуется временно покинуть рабочее место, заблокируйте удаленный рабочий стол. По возвращении на рабочее место возобновите работу. Подробную информацию о блокировании удаленного рабочего стола и возобновлении работы см. в руководстве операционной системы, к которой вы подключаетесь удаленно.

5. **Завершение сессии подключения**

   Завершите сессию подключения к удаленной среде по завершении работы.

6. **Остановка Kaspersky Thin Client**

   Выключите тонкий клиент в конце рабочего дня.

Подключение к удаленной среде

С помощью Kaspersky Thin Client вы можете выполнить следующие действия:

- **Подключиться к удаленному рабочему столу по протоколу RDP**

Чтобы подключиться к удаленному рабочему столу по протоколу RDP:

1. Включите Kaspersky Thin Client.
2. В главном окне Kaspersky Thin Client нажмите на кнопку **RDP**.
3. В открывшемся окне укажите параметры подключения:
   a. В поле **Сервер** укажите IP-адрес или имя сервера брокера Microsoft Remote Desktop Connection Broker.

      Kaspersky Thin Client сохраняет последний введенный адрес сервера, к которому было совершено успешное подключение, и вам не нужно вводить его при повторном подключении.

   b. В поле **Имя пользователя** введите локальное или доменное имя пользователя. Вы можете указать доменное имя пользователя в формате `Домен\Имя пользователя` или в формате `Имя пользователя`.

      Kaspersky Thin Client сохраняет последнее введенное имя пользователя, который успешно подключался к серверу, и вам не нужно вводить его при повторном подключении.

   c. В поле **Пароль** введите пароль пользователя.

      Пароль пользователя не сохраняется, при следующем подключении необходимо ввести пароль снова.
4. Если требуется настроить параметры подключения к удаленному рабочему столу, нажмите **Параметры** в левой части окна.
5. Нажмите на клавишу **ENTER** или на кнопку **Подключиться**.

   Если вы в первый раз подключаетесь к удаленному рабочему столу и при этом Kaspersky Thin Client не входит в группу администрирования, в открывшемся окне **Добавление сертификата** проверьте параметры добавляемого сертификата и нажмите на кнопку **Добавить сертификат**.

   Если Kaspersky Thin Client ранее был добавлен в группу администрирования, управляется через Kaspersky Security Center Web Console, для этой группы администрирования администратор Kaspersky Security Center добавил сертификат для проверки подлинности сервера, то подключение произойдет автоматически.

   Сертификат для проверки подлинности сервера будет добавлен в системное хранилище сертификатов Kaspersky Thin Client и будет использоваться при следующих подключениях.
6. Если при настройке подключения к удаленному рабочему столу вы указали идентификатор коллекции Remote Desktop Connection Broker и вам доступно несколько рабочих столов, в открывшемся окне выбора удаленного рабочего стола нажмите на кнопку с названием рабочего стола, к которому вы хотите подключиться.

   Отобразится окно удаленного рабочего стола, начнется сессия подключения.

- Подключиться к виртуальному приложению по протоколу RDP

Чтобы подключиться к виртуальному приложению по протоколу RDP:

1. Включите Kaspersky Thin Client.
2. В главном окне Kaspersky Thin Client нажмите на кнопку **RDP**.
3. В открывшемся окне укажите параметры подключения:
   a. В поле **Сервер** укажите IP-адрес или имя сервера брокера Microsoft Remote Desktop Connection Broker.

      Kaspersky Thin Client сохраняет последний введенный адрес сервера, к которому было совершено успешное подключение, и вам не нужно вводить его при повторном подключении.

   b. В поле **Имя пользователя** введите локальное или доменное имя пользователя. Вы можете указать доменное имя пользователя в формате `Домен\Имя пользователя` или в формате `Имя пользователя`.

      Kaspersky Thin Client сохраняет последнее введенное имя пользователя, который успешно подключался к серверу, и вам не нужно вводить его при повторном подключении.

   c. В поле **Пароль** введите пароль пользователя.

      Пароль пользователя не сохраняется, при следующем подключении необходимо ввести пароль снова.
4. Нажмите **Параметры** в левой части окна.
5. В поле **Идентификатор коллекции Remote Desktop Connection Broker** укажите идентификатор коллекции в формате `tsv://MS Terminal Services Plugin.1.collection_id`, где `collection_id` – идентификатор коллекции.
6. В поле **Псевдоним приложения** укажите псевдоним виртуального приложения, которое требуется открыть.

   Kaspersky Thin Client сохраняет псевдоним, который вы вводили в последний раз, и вам не нужно вводить его при повторном подключении.
7. Нажмите на стрелку назад в верхнем правом углу окна для возврата к окну подключения.
8. В окне подключения нажмите на клавишу **ENTER** или на кнопку **Подключиться**.

   Если вы впервые подключаетесь к выбранному виртуальному приложению и при этом Kaspersky Thin Client не входит в группу администрирования, в открывшемся окне **Добавление сертификата** проверьте параметры добавляемого сертификата и нажмите на кнопку **Добавить сертификат**.

   Сертификат будет добавлен в системное хранилище сертификатов Kaspersky Thin Client и будет использоваться при следующих подключениях.

   Если администратор Kaspersky Security Center уже добавил Kaspersky Thin Client в группу администрирования и добавил для этой группы сертификат для проверки подлинности сервера, то подключение произойдет автоматически.

   Отобразится окно запущенного виртуального приложения, начнется сессия подключения.

Чтобы переключиться на другое окно запущенного виртуального приложения,

наведите курсор мыши на значок приложения в панели подключения в верхней части экрана и выберите нужное окно в раскрывающемся списке.

- Подключиться к удаленному рабочему столу под управлением Базис.WorkPlace

Чтобы подключиться к удаленному рабочему столу под управлением Базис.WorkPlace:

1. Включите Kaspersky Thin Client.
2. В главном окне Kaspersky Thin Client нажмите на кнопку **Базис.WorkPlace**.
3. В открывшемся окне подключения укажите параметры подключения к Базис.WorkPlace:
   a. В поле **Сервер** укажите IP-адрес или имя сервера диспетчера подключений Базис.WorkPlace.

      Kaspersky Thin Client сохраняет адрес диспетчера подключений Базис.WorkPlace, к которому было совершено успешное подключение, и вам не нужно вводить его при повторном подключении.

   b. В поле **Домен** введите имя домена.
   c. В поле **Имя пользователя** введите имя пользователя.

      Kaspersky Thin Client сохраняет имя пользователя, который последний раз успешно подключался к Базис.WorkPlace, и вам не нужно вводить его при повторном подключении.

   d. В поле **Пароль** введите пароль пользователя.

      Пароль пользователя не сохраняется: при следующем подключении необходимо ввести пароль снова.

      При превышении количества попыток неправильного ввода пароля, учетная запись пользователя будет заблокирована. Сообщение об этом отобразится в окне подключения к удаленному рабочему столу. Количество попыток ввода пароля определяется действующей политикой безопасности, установленной администратором Базис.WorkPlace.

4. Нажмите на кнопку **Подключиться**.

   Если вы в первый раз подключаетесь к удаленному рабочему столу под управлением Базис.WorkPlace и при этом Kaspersky Thin Client не входит в группу администрирования, в открывшемся окне **Добавление сертификата** проверьте параметры добавляемого сертификата и нажмите на кнопку **Добавить сертификат**.

   Если Kaspersky Thin Client ранее был добавлен в группу администрирования, управляется через Kaspersky Security Center Web Console, а для этой группы администрирования администратор Kaspersky Security Center добавил сертификат для проверки подлинности брокера Базис.WorkPlace, то подключение к удаленному рабочему столу под управлением Базис.WorkPlace произойдет автоматически.

   Сертификат для проверки подлинности брокера Базис.WorkPlace будет добавлен в системное хранилище сертификатов Kaspersky Thin Client и будет использоваться при следующих подключениях.

   Откроется окно выбора удаленного рабочего стола, в котором отображаются все доступные для подключения рабочие столы.

5. Если требуется обновить список рабочих столов, нажмите на кнопку **Обновить**.
6. Нажмите на кнопку с названием рабочего стола, к которому вы хотите подключиться.

Через несколько секунд на мониторе отобразится удаленный рабочий стол, к которому вы подключились.

Также в окне подключения к рабочим столам под управлением Базис.WorkPlace вы можете настроить параметры подключения, нажав **Параметры**.

Администратор Базис.WorkPlace может ограничить доступ к рабочим столам под управлением Базис.WorkPlace. Например, он может заблокировать вашу учетную запись или запретить доступ к удаленным рабочим столам под управлением Базис.WorkPlace, которые ранее были доступны для вашей учетной записи. При возникновении проблем с подключением к удаленному рабочему столу рекомендуется обратиться к администратору Базис.WorkPlace.

- **Подключиться к удаленной среде в приложении Web Access**

В приложении Web Access вы можете подключиться к удаленной среде, развернутой в инфраструктурах Citrix Workspace и VMware Horizon, с помощью технологии HTML5. При подключении используется браузер Chromium™.

Чтобы подключиться к удаленной среде в приложении Web Access:

1. Включите Kaspersky Thin Client.
2. В главном окне Kaspersky Thin Client нажмите на кнопку **Web Access**.
3. В открывшемся окне подключения в поле **Сервер** укажите веб-адрес сервера необходимой удаленной среды.
4. Нажмите на кнопку **Подключиться**.

   Если вы в первый раз подключаетесь к указанной удаленной среде и при этом Kaspersky Thin Client не входит в группу администрирования, в открывшемся окне **Добавление сертификата** проверьте параметры добавляемого сертификата и нажмите на кнопку **Добавить сертификат**.

   Если Kaspersky Thin Client ранее был добавлен в группу администрирования, управляется через Kaspersky Security Center Web Console, а для этой группы администрирования администратор Kaspersky Security Center добавил сертификат для проверки подлинности веб-адреса сервера, то подключение к удаленной среде произойдет автоматически.

   Сертификат для проверки подлинности веб-адреса сервера будет добавлен в системное хранилище сертификатов Kaspersky Thin Client и будет использоваться при следующих подключениях.

   Если вам доступен только один рабочий стол для подключения, на мониторе отобразится удаленный рабочий стол, к которому вы подключились. Если вам доступно несколько удаленных рабочих столов, откроется окно выбора, в котором отображаются все доступные для подключения рабочие столы.

   Данные, необходимые для работы в удаленной среде, включая файлы cookies, будут сохраняться на тонком клиенте до завершения удаленного подключения. Затем эти данные будут удалены.

5. Если требуется обновить список удаленных рабочих столов, нажмите на кнопку **Обновить**.
6. Нажмите на кнопку с названием удаленного рабочего стола, к которому вы хотите подключиться.

Через несколько секунд на мониторе отобразится удаленный рабочий стол, к которому вы подключились.

Одновременный запуск нескольких сессий подключения не поддерживается.

Kaspersky Thin Client использует шифрование по протоколу TLS для защиты всех сессий подключения, а также для защиты данных от перехвата или подмены.

Работа с панелью подключения

Панель подключения отображается в верхней части экрана после успешного подключения к удаленной среде и используется для управления активной сессией подключения.

Чтобы управлять сессией подключения к удаленной среде в панели подключения:

1. Если требуется завершить сессию подключения к удаленной среде, нажмите на кнопку **Завершить сессию**.
2. Если требуется изменить язык интерфейса тонкого клиента, нажмите на сокращенное название текущего языка и выберите необходимый язык в раскрывающемся списке.
3. Если требуется посмотреть информацию о технической поддержке, нажмите на значок .

Панель подключения автоматически переходит в свернутое состояние при перемещении фокуса клавиатуры или курсора мыши с панели.

Чтобы переключиться на другое окно запущенного виртуального приложения,

нажмите на значок приложения в панели подключения и выберите нужное окно в раскрывающемся списке.

Чтобы свернуть или развернуть панель подключения:

1. Если требуется восстановить панель подключения, нажмите на свернутую панель подключения с помощью мыши или нажмите комбинацию клавиш **Ctrl+Alt+Home**.
2. Если требуется свернуть панель подключения, на которой находится фокус клавиатуры, нажмите **Esc**.
3. Если требуется свернуть панель подключения, не перемещая фокус с окна удаленной сессии, нажмите комбинацию клавиш **Ctrl+Alt+Home**.

Вы также можете перемещать свернутую панель подключения по горизонтали вправо или влево.

Чтобы изменить положение панели подключения,

нажмите на панель подключения в области, где нет кнопок, и перетащите ее мышью.

Положение панели подключения на экране сохраняется при последующих подключениях, в том числе после перезагрузки или выключения тонкого клиента.

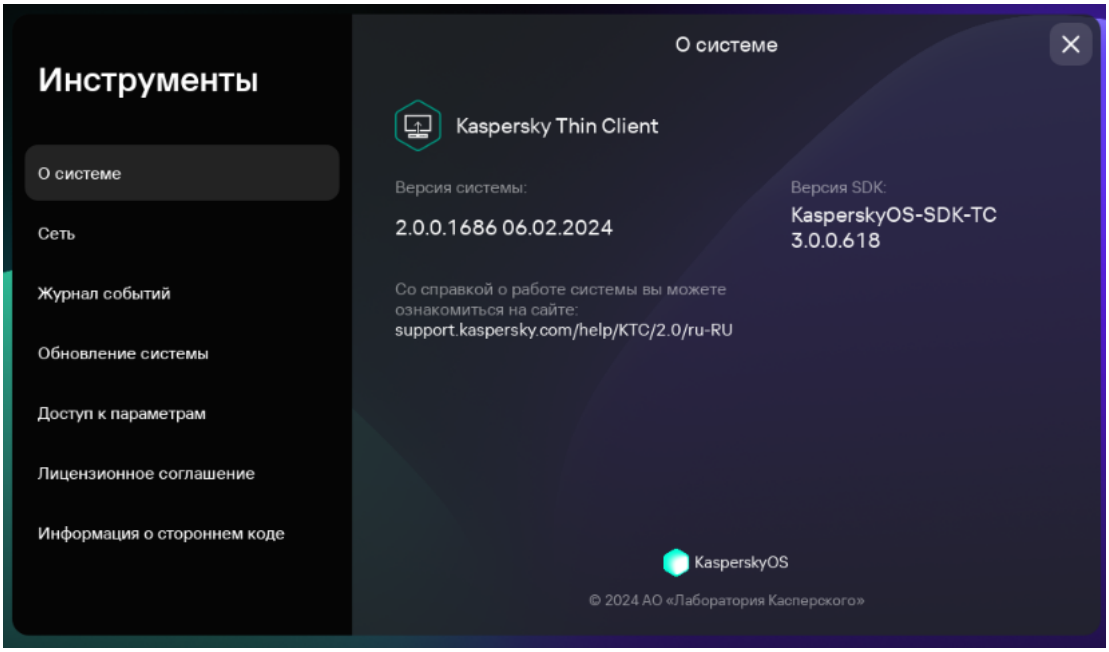
Вы также можете управлять панелью подключения и сессией подключения к удаленной среде при помощи горячих клавиш.

Просмотр информации о Kaspersky Thin Client

Вы можете просматривать информацию о Kaspersky Thin Client в разделе **Инструменты** → **О системе**.

В разделе **О системе** (см. рис. ниже) отображаются следующие данные:

- Номер версии Kaspersky Thin Client.
- Номер версии KasperskyOS.
- Ссылка на онлайн-справку Kaspersky Thin Client.



Инструменты. Раздел **О системе**

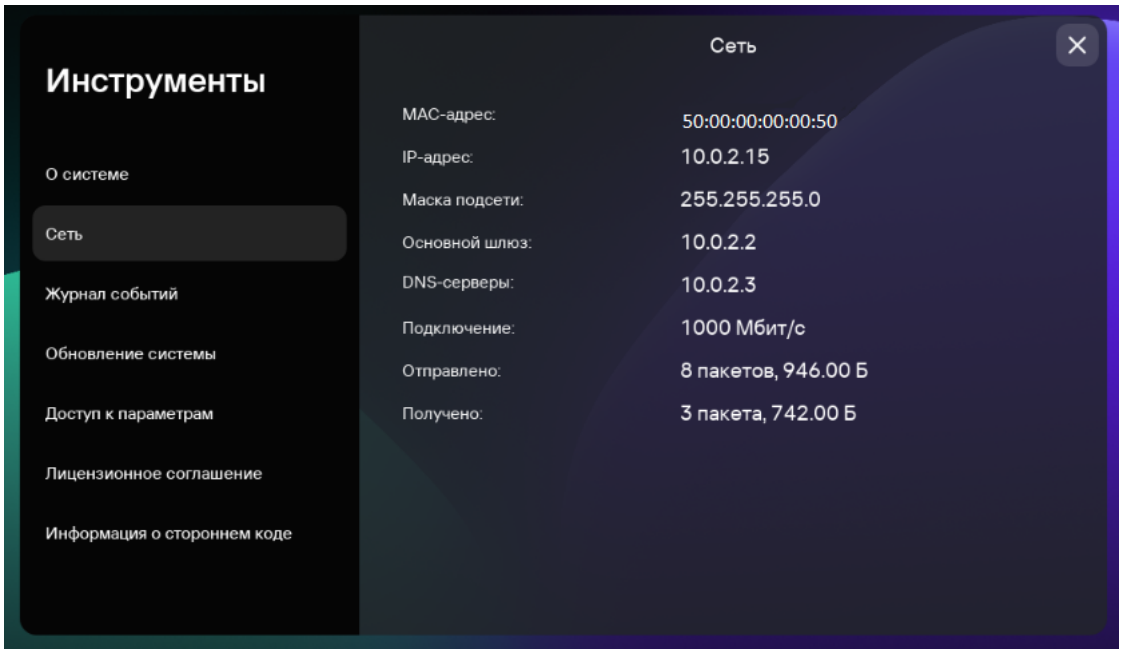
Просмотр информации о состоянии сети

Вы можете просматривать параметры подключения Kaspersky Thin Client к сети и состояние сети в разделе **Инструменты** → **Сеть**. Информация о параметрах подключения Kaspersky Thin Client к сети обновляется автоматически не реже одного раза в секунду.

В разделе **Сеть** отображается следующая информация о параметрах подключения Kaspersky Thin Client к сети (см. рис. ниже):

- **MAC-адрес** – MAC-адрес устройства, на котором установлен Kaspersky Thin Client.
- **IP-адрес** – IP-адрес устройства, на котором установлен Kaspersky Thin Client.
- **Маска подсети** – маска подсети, к которой относится IP-адрес устройства.
- **Основной шлюз** – адрес сетевого шлюза.
- **DNS-серверы** – адреса DNS-серверов. Для просмотра всех адресов (если их больше трех) требуется навести курсор мыши на значение параметра.
- **Подключение** – статус подключения Kaspersky Thin Client к сети и скорость подключения.
- **Отправлено** – количество и общий размер оправленных от Kaspersky Thin Client сетевых пакетов.

- **Получено** – количество и общий размер полученных Kaspersky Thin Client сетевых пакетов.



Инструменты. Раздел **Сеть**

Просмотр уведомлений Kaspersky Thin Client

В интерфейсе Kaspersky Thin Client отображаются уведомления следующих типов:

- Уведомление, требующее выбрать определенное действие с помощью нажатия на соответствующую кнопку, например, применить обновление немедленно или отложить его. Если вы закрыли уведомление-действие, не выбрав действие, через некоторое время Kaspersky Thin Client снова отобразит это уведомление. Уведомление считается обработанным после выбора действия.

- Уведомление, предлагающее перейти в другой раздел Kaspersky Thin Client для дополнительной настройки параметров. Например, при подключении второго монитора система предлагает настроить взаимное расположение мониторов. Вы можете перейти в другой раздел системы, нажав на соответствующую кнопку, или закрыть уведомление.

- Уведомление информационного характера. Такие уведомления не требуют дополнительных действий, вы можете только закрыть уведомление после ознакомления.

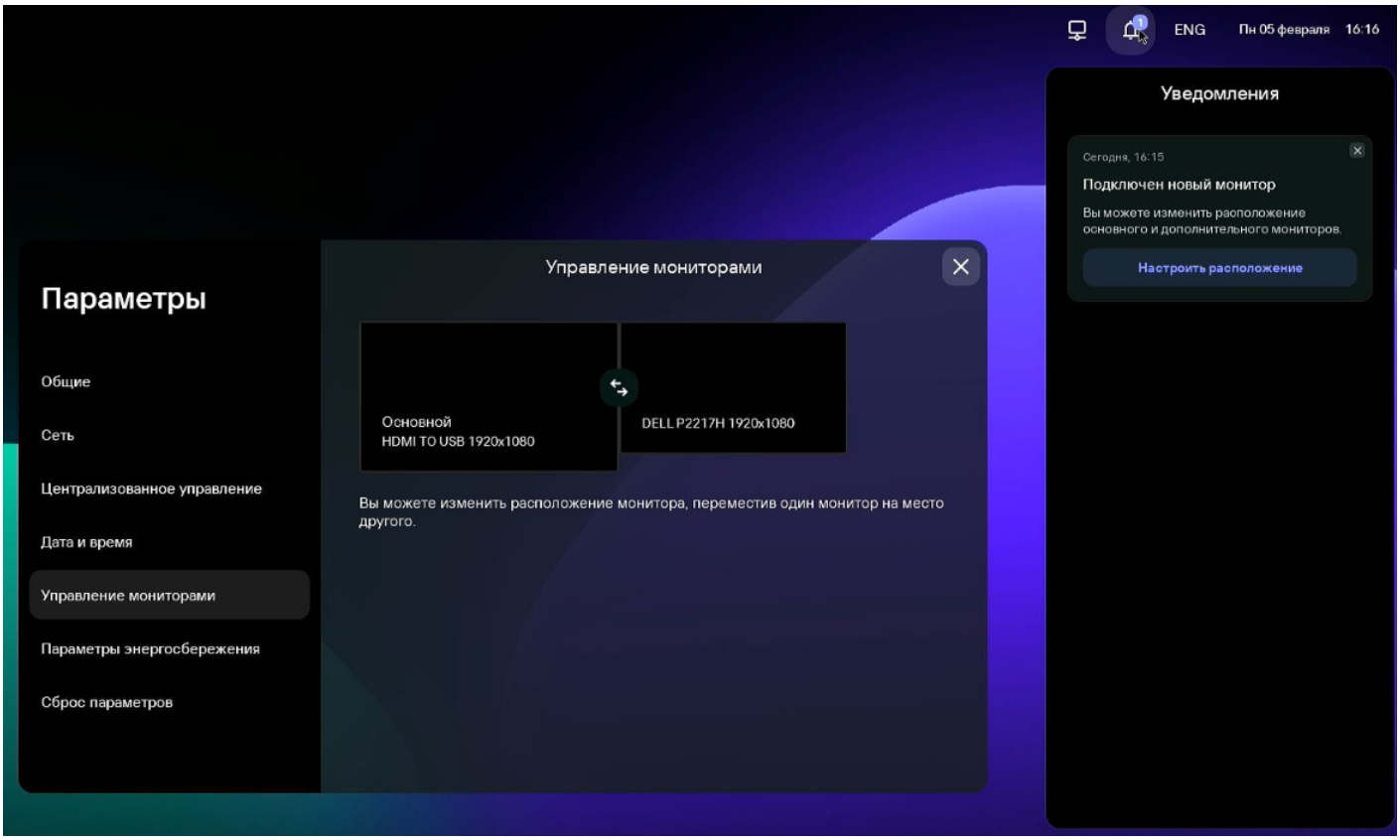
Необработанные и непрочитанные (при отсутствии курсора мыши или фокуса на зоне уведомления) уведомления скрываются, а в панели управления счетчик отображает количество необработанных уведомлений.

> В сессии подключения уведомления об обновлениях не скрываются автоматически: вы можете закрыть такие уведомления вручную или выбрать требуемое действие, после чего уведомление закроется.

Чтобы просмотреть список всех уведомлений Kaspersky Thin Client,

в панели управления Kaspersky Thin Client нажмите на значок .

Если новые уведомления есть, отобразится список уведомлений (см. рис. ниже).



Панель уведомлений Kaspersky Thin Client

Управление сертификатами в интерфейсе тонкого клиента

Kaspersky Thin Client не проверяет, находится ли сертификат в списке отозванных сертификатов (Certificate Revocation List).

О сертификатах для подключения к Kaspersky Security Center

При замене администратором Kaspersky Security Center сертификата для подключения к Kaspersky Security Center в некоторых случаях может потребоваться подтверждение замены сертификата. Например, если тонкий клиент длительное время был выключен, не синхронизировался с Kaspersky Security Center, а срок действия используемого ранее сертификата для подключения к Kaspersky Security Center закончился.

Чтобы подтвердить замену мобильного сертификата для подключения к Kaspersky Security Center:

1. Включите Kaspersky Thin Client.
2. В открывшемся окне **Требуется замена сертификата** посмотрите и запомните код подтверждения, сообщите его администратору Kaspersky Security Center. Контакты администратора указаны в окне **Требуется замена сертификата**. В ответ администратор Kaspersky Security Center сообщит вам код замены сертификата.
3. Нажмите на кнопку **Далее**.
4. В открывшемся окне **Код замены сертификата** введите код, который сообщил вам администратор Kaspersky Security Center и нажмите на кнопку **Подтвердить**.

В результате новый сертификат для подключения к Kaspersky Security Center будет сохранен в хранилище сертификатов Kaspersky Thin Client и в дальнейшем будет использоваться для подключения к Kaspersky Security Center.

О сертификатах для подключения к удаленной среде и к серверу журналирования

Если тонкий клиент не подключен к Kaspersky Security Center и администратор не назначал для него сертификаты в Web Console, пользователь может подключаться в том числе к тем узлам и использовать те сертификаты, которые не контролирует администратор. Рекомендуется настроить подключение группы тонких клиентов к серверу журналирования и к удаленной среде только с применением сертификатов, назначенных администратором в Web Console. Такие меры помогут предотвратить подключение Kaspersky Thin Client к недоверенным узлам.

Вы можете применить или отклонить сертификат в интерфейсе Kaspersky Thin Client в следующих случаях:

- при первом подключении Kaspersky Thin Client к Kaspersky Security Center;
- при первом подключении к удаленной среде;
- при первом подключении к серверу журналирования.

Принятые сертификаты сохраняются в системном хранилище Kaspersky Thin Client.

Если тонкий клиент входит в группу администрирования и для этой группы уже были назначены сертификаты в Web Console, вы не сможете управлять сертификатами в интерфейсе Kaspersky Thin Client.

Завершение сессии подключения

Чтобы завершить сессию подключения к удаленной среде:

разверните панель подключения и в отобразившейся панели нажмите на кнопку **Завершить сессию**.

Сессия подключения будет завершена, отобразится окно подключения.

Управление Kaspersky Thin Client с помощью горячих клавиш

Вы можете использовать специальные горячие клавиши и сочетания клавиш во время работы с Kaspersky Thin Client и во время сессии подключения. В таблице ниже приведены все доступные специальные клавиши и сочетания клавиш.

Специальные клавиши и сочетания клавиш Kaspersky Thin Client

Клавиши и сочетания клавиш	Действия
Win	Открыть или закрыть меню завершения работы.

→ ←	Переключиться между доступными вариантами подключений (**RDP**, **Базис.WorkPlace**, **Web Access**) в главном окне Kaspersky Thin Client.
↑ ↓	• Переключиться между элементами раскрывающегося списка. • Прокрутить содержимое страницы вверх или вниз.
Tab	Переключиться *слева направо* или *сверху вниз* между следующими элементами: • варианты подключений; • последовательность полей, например, в окне **Параметры**; • кнопки в панели подключения. При переключении элементы, недоступные для взаимодействия (например, поле, которое заблокировано для изменения), а также неактивные элементы пропускаются.
Shift+Tab	Переключиться *справа налево* или *снизу вверх* между следующими элементами: • варианты подключений; • последовательность полей, например, в окне **Параметры**; • кнопки в панели подключения. При переключении элементы, недоступные для взаимодействия (например, поле, которое заблокировано для изменения), а также неактивные элементы пропускаются.
Space или **Enter**	• Нажать на кнопку, на которой находится фокус клавиатуры. • Открыть или закрыть раскрывающийся список, на котором находится фокус клавиатуры. При переключении элементы, недоступные для взаимодействия (например, поле, которое заблокировано для изменения), а также неактивные элементы пропускаются.
Esc	• Закрыть активное окно. • Свернуть панель подключения, если на ней находится фокус клавиатуры.
Alt+Shift	Сменить язык раскладки клавиатуры.
Alt+Page down **Alt+Page up**	Переместиться в следующий или предыдущий раздел окна **Параметры** или **Инструменты**. При переключении между разделами их состояние и элемент, находящийся в фокусе, сохраняются. Например, в окне **Параметры** при переходе из раздела **Основные** в раздел **Сеть** фокус в разделе **Основные** останется на том же поле, в котором он был, когда вы переключились на другой раздел.
Ctrl+Alt+Home	Свернуть или развернуть панель подключения.
Ctrl+D	Завершить сессию подключения. Комбинация работает только если панель подключения развернута.
Win+I	Открыть раздел **Параметры**, находясь в главном окне Kaspersky Thin Client, если

	доступ к параметрам открыт.
Win+U	Открыть раздел **Инструменты**, находясь в главном окне Kaspersky Thin Client.
Win+Esc	Выключить Kaspersky Thin Client, находясь в главном окне Kaspersky Thin Client.
Win+F12 или **Win+End**	Перезагрузить Kaspersky Thin Client, находясь в главном окне Kaspersky Thin Client.
Win+A или **Win+N**	Открыть панель уведомлений, находясь в главном окне Kaspersky Thin Client.
Win+↓ **Win+↑**	Свернуть или восстановить свернутое окно во время подключения к виртуальному приложению.
Win+M	Свернуть все окна во время подключения к виртуальному приложению.
Win+Shift+M	Восстановить все окна во время подключения к виртуальному приложению.

Обновление Kaspersky Thin Client в интерфейсе тонкого клиента

Обновление Kaspersky Thin Client возможно, только если тонкий клиент подключен к Kaspersky Security Center.

После загрузки обновлений на устройство в интерфейсе Kaspersky Thin Client отображается уведомление о времени применения обновления.

Вы можете установить обновление одним из следующих способов:

- **Из уведомления о доступном обновлении**

  - Если вы хотите установить обновления прямо сейчас, в окне уведомления о доступном обновлении нажмите на кнопку **Перезагрузить сейчас**.

    Обновления будут установлены и Kaspersky Thin Client перезагрузится.

  - Если вы хотите установить обновления позже, в окне уведомления о доступном обновлении нажмите на кнопку **Позже**. Уведомление о доступном обновлении содержит информацию о времени отложенного запуска обновления. Время отложенного запуска обновления устанавливает администратор.

    Перезагрузка и обновление системы будут отложены.

    Если вы несколько раз закроете или проигнорируете уведомление об обновлении Kaspersky Thin Client, установка обновления будет выполнена автоматически.

- **При перезагрузке или выключении тонкого клиента**

1. В панели управления Kaspersky Thin Client нажмите на кнопку завершения работы .
2. В зависимости от того, планируете вы завершить или продолжить работу с Kaspersky Thin Client после обновления, выполните одно из следующих действий:
   - Если вы хотите продолжить работу, в открывшемся меню выберите пункт **Обновить и перезагрузить**.

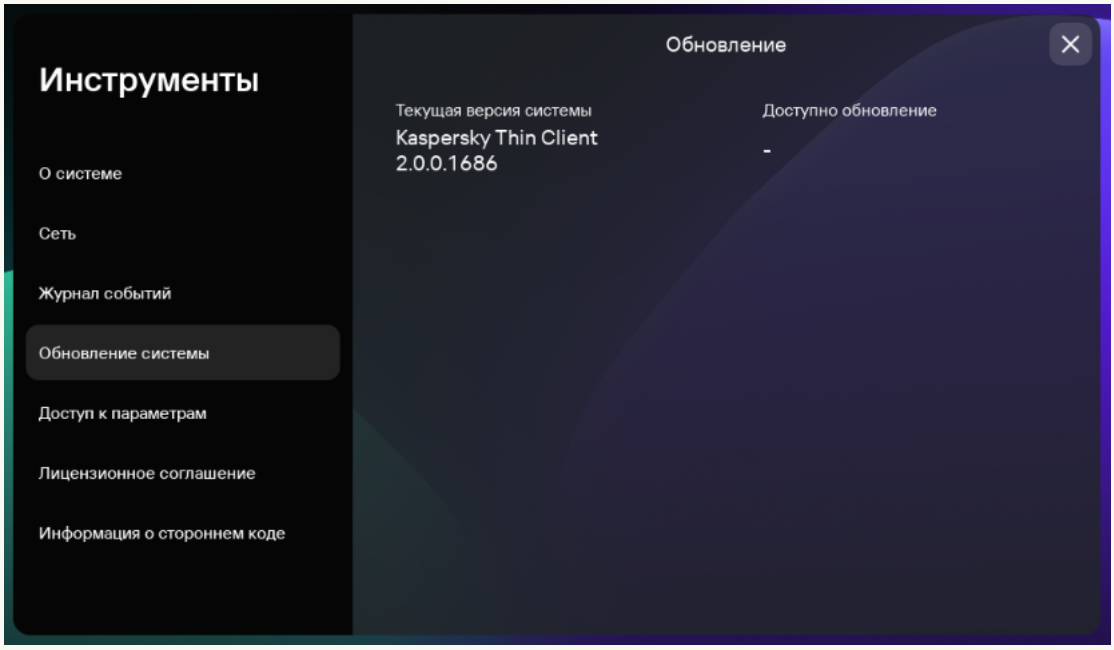
     Обновления будут установлены и Kaspersky Thin Client перезагрузится.
   - Если вы хотите завершить работу, в открывшемся меню выберите пункт **Обновить и выключить**.

     Обновления будут установлены и Kaspersky Thin Client выключится.

- В разделе Обновление системы

1. В панели управления Kaspersky Thin Client нажмите на кнопку и в открывшемся меню выберите **Инструменты**.
2. Выберите раздел **Обновление системы**.

   Откроется окно, в котором отображается информация о текущей версии системы и загруженных обновлениях (см. рис. ниже).



Инструменты. Раздел **Обновление системы**

3. Нажмите на кнопку **Установить и перезагрузить**. Если нет доступных обновлений, то кнопка не отображается.

Обновления будут установлены, и Kaspersky Thin Client перезагрузится.

Если обновление Kaspersky Thin Client было загружено, но вы не выполнили перезагрузку, то при следующей перезагрузке или при следующем включении устройства установка обновления будет выполнена автоматически.

Подробная информация о централизованном обновлении тонких клиентов через Web Console приведена в отдельной статье.

Управление Kaspersky Thin Client через Kaspersky Security Center Web Console

Kaspersky Security Center Web Console (далее также Web Console) представляет собой программу (веб-приложение), предназначенную для централизованного решения основных задач по управлению и обслуживанию системы защиты сети организации. Web Console является компонентом Kaspersky Security Center, предоставляющим пользовательский интерфейс. Подробную информацию о Kaspersky Security Center Web Console см. в онлайн-справке Kaspersky Security Center Web Console.

О веб-плагине управления Kaspersky Security Management Suite

Веб-плагин управления Kaspersky Security Management Suite (далее также веб-плагин) – специальный компонент, предоставляющий возможность управления работой Kaspersky Thin Client через Kaspersky Security Center Web Console.

Веб-плагин позволяет централизованно выполнять следующие действия:

- Управлять параметрами Kaspersky Thin Client.
- Настраивать получение и просматривать события Kaspersky Thin Client.
- Управлять сертификатами безопасности Kaspersky Thin Client.

Для взаимодействия Kaspersky Thin Client и Kaspersky Security Center требуется выполнить следующие условия:

- При настройке Kaspersky Thin Client требуется указать параметры подключения к Kaspersky Security Center.
- В Kaspersky Security Center Web Console требуется установить веб-плагин управления Kaspersky Security Management Suite.

Установка веб-плагина управления Kaspersky Security Management Suite

Kaspersky Security Management Suite, Kaspersky Security Center и Kaspersky Security Center Web Console не входят в комплект поставки Kaspersky Thin Client, их требуется установить отдельно.

Вы можете просмотреть список установленных веб-плагинов в интерфейсе Web Console (**Параметры Консоли** → **Веб-плагины**).

Функции веб-плагина доступны всем администраторам, у которых есть доступ к Web Console в браузере. Если требуется, вы можете разграничить доступ к функциям Kaspersky Security Management Suite.

Если для подключения тонкого клиента к Kaspersky Security Center планируется использовать порт по умолчанию, на Сервере администрирования Kaspersky Security Center должен быть доступен порт 13292. Если планируется использовать порт отличный от 13292, требуется настроить разрешение для нужного порта. Подробную информацию о включении порта на Сервере администрирования Kaspersky Security Center вы можете получить в разделе онлайн-справки Kaspersky Security Center *Изменение параметров управления мобильными устройствами*.

Чтобы установить веб-плагин в Web Console:

1. Откройте необходимый архив с установочными образами и файлами подписи веб-плагина, входящий в комплект поставки Kaspersky Thin Client.

   Отобразится текст Лицензионного соглашения.

2. Ознакомьтесь с Лицензионным соглашением и примите его, если согласны с его условиями.

   Архив с установочными образами и файлами подписи веб-плагина будет распакован автоматически после принятия соглашения.

3. В меню Web Console выберите **Параметры консоли** → **Веб-плагины**.

   Отобразится список доступных плагинов управления Web Console.

4. Нажмите на кнопку **Добавить из файла**.

5. В открывшейся панели добавьте файлы из распакованного архива с установочными образами и файлами подписи веб-плагина:

   - ZIP-архив с дистрибутивом веб-плагина (plugin.zip), нажав на кнопку **Загрузить файл формата ZIP**;
   - файл подписи (signature.txt), нажав на кнопку **Загрузить подпись**.

6. Нажмите на кнопку **Добавить**.

7. После завершения установки веб-плагина нажмите на кнопку **OK**.

Веб-плагин управления Kaspersky Security Management Suite будет загружен с параметрами по умолчанию и отобразится в списке плагинов управления Web Console.

Обновление веб-плагина управления Kaspersky Security Management Suite

Чтобы обновить Kaspersky Security Management Suite, вам требуется получить архив с пакетом установки веб-плагина и цифровую подпись архива от специалистов "Лаборатории Касперского".

Чтобы обновить веб-плагин в Web Console:

1. Откройте архив с установочными образами и файлами подписи веб-плагина, полученный от специалистов "Лаборатории Касперского".

   Отобразится текст Лицензионного соглашения.

2. Ознакомьтесь с Лицензионным соглашением и примите его, если согласны с его условиями.

Архив с установочными образами и файлами подписи веб-плагина будет распакован автоматически после принятия соглашения.

3. В меню Web Console выберите **Параметры Консоли** → **Веб-плагины**.
4. В отобразившемся списке плагинов Web Console найдите Kaspersky Security Management Suite и нажмите на него.
5. В открывшемся окне нажмите на кнопку **Обновить из файла**.
6. В открывшейся панели добавьте файлы из распакованного архива с установочными образами и файлами подписи веб-плагина:
   - ZIP-архив с дистрибутивом веб-плагина (plugin.zip), нажав на кнопку **Загрузить файл формата ZIP**;
   - файл подписи (signature.txt), нажав на кнопку **Загрузить подпись**.
7. Нажмите на кнопку **Обновление**.
8. После завершения обновления в окне сообщения об успешной установке нажмите на кнопку **OK**.

Веб-плагин Kaspersky Security Management Suite будет обновлен, и в таблице плагинов в Web Console отобразится информация о его версии и времени обновления.

Удаление веб-плагина управления Kaspersky Security Management Suite

Вы можете удалить веб-плагин управления Kaspersky Security Management Suite в Web Console. После удаления веб-плагина управление Kaspersky Thin Client через интерфейс Web Console будет недоступно.

Перед удалением веб-плагина удалите устройство из группы управляемых устройств.

Чтобы удалить веб-плагин управления Kaspersky Security Management Suite из Web Console:

1. В меню интерфейса Web Console выберите **Параметры консоли** → **Веб-плагины**.

   Отобразится список доступных плагинов управления Web Console.
2. В списке плагинов управления установите флажок около веб-плагина управления Kaspersky Security Management Suite.
3. Нажмите на кнопку **Удалить**.
4. В открывшемся окне подтверждения удаления плагина, выполните одно из следующих действий:
   - Если требуется сохранить резервную копию плагина, нажмите на кнопку **OK**.

     Резервная копия плагина будет создана. Веб-плагин управления Kaspersky Security Management Suite будет удален из Web Console.
   - Если не требуется сохранять резервную копию плагина, нажмите на кнопку **Пропустить резервное копирование данных**.

     Веб-плагин управления Kaspersky Security Management Suite будет удален из Web Console.
5. В появившемся окне с информацией об удалении плагина нажмите на кнопку **OK**.

Разделение доступа к функциям веб-плагина управления Kaspersky Security Management Suite

Если для пользователя Kaspersky Security Center не настроены права доступа к функциям программы или не назначена типовая роль Kaspersky Security Center, то пользователь не сможет работать в Kaspersky Security Center Web Console.

Вы можете настраивать для пользователей Kaspersky Security Center права доступа к функциям Kaspersky Security Center одним из следующих способов:

- настраивать права каждого пользователя или группы пользователей индивидуально;
- создавать типовые роли Kaspersky Security Center с заранее настроенным набором прав и присваивать эти роли пользователям в зависимости от их служебных обязанностей.

Роль – это заранее определенный набор прав доступа к функциям Kaspersky Security Management Suite, который вы можете назначить пользователю. Рекомендуется настраивать права доступа в роли в соответствии с типовыми задачами и служебными обязанностями пользователей. Если пользователю назначена роль, пользователь получает доступ к функциям, которые требуются для выполнения служебных обязанностей.

Подробную информацию о настройке доступа в зависимости от роли см. в разделе *Настройка прав доступа к функциям программы. Управление доступом на основе ролей* в онлайн-справке Kaspersky Security Center.

Также в дополнение к типовым ролям Kaspersky Security Center вы можете назначить пользователю следующие типовые роли для управления функциями Kaspersky Thin Client:

- *Офицер безопасности*. Для этой роли разрешен просмотр всех разделов Kaspersky Security Management Suite и разрешено управление сертификатами Kaspersky Thin Client. Вы можете назначить эту роль сотруднику, который отвечает за информационную безопасность в вашей организации.
- *Администратор*. Для этой роли разрешен просмотр всех разделов Kaspersky Security Management Suite, разрешено управление параметрами подключения к удаленным рабочим столам, общим и системным параметрами, а также управление данными Kaspersky Thin Client. Вы можете назначить эту роль сотруднику, который отвечает за поддержку и администрирование информационных систем в вашей организации.
- *Расширенный администратор*. Для этой роли разрешен просмотр и управление всеми разделами Kaspersky Security Management Suite, управление сертификатами, параметрами подключения к удаленным рабочим столам, общими и системными параметрами, а также управление данными Kaspersky Thin Client. Вы можете назначить эту роль сотруднику, который отвечает за поддержку и администрирование информационных систем, а также информационную безопасность в вашей организации.

В таблице ниже описаны функции, которые доступны пользователю в зависимости от назначенной роли для управления Kaspersky Thin Client. Для функций, отмеченных значком ✓, доступно изменение параметров Kaspersky Thin Client через Web Console. Просмотр параметров Kaspersky Thin Client через Web Console для всех функций доступен для всех ролей.

Функции управления Kaspersky Thin Client через Web Console в зависимости от роли пользователя

Функция	Офицер безопасности	Администратор	Расширенный администратор

Управление сертификатами в политике Kaspersky Security Management Suite	✓	–	✓
Настройка параметров подключения к удаленным рабочим столам в политике Kaspersky Security Management Suite	–	✓	✓
Настройка общих параметров в политике Kaspersky Security Management Suite	–	✓	✓
Управление системными параметрами в политике Kaspersky Security Management Suite	–	✓	✓
Управление данными Kaspersky Thin Client в политике Kaspersky Security Management Suite	–	✓	✓

Вход и выход из Web Console

Для входа в Web Console требуется получить у администратора Web Console веб-адрес Сервера администрирования Kaspersky Security Center и номер порта, указанные во время установки (по умолчанию используется порт 8080). Также требуется включить JavaScript в браузере.

Чтобы войти в Web Console:

1. В браузере перейдите по адресу `https://<Адрес Сервера администрирования>:<Номер порта>`. Требования к браузеру, который используется для работы с Web Console см. в разделе *Аппаратные и программные требования* в онлайн-справке Kaspersky Security Center Web Console.

   Откроется страница входа.

2. Войдите с использованием имени пользователя и пароля локального администратора.

   Если Сервер администрирования не отвечает или вы указали неверные учетные данные, отобразится сообщение об ошибке.

После входа отобразится информационная панель с последним используемым языком и темой. Если вы вошли в Web Console впервые, запустится мастер первоначальной настройки. Дополнительная информация о работе Kaspersky Security Center Web Console приведена в онлайн-справке Kaspersky Security Center Web Console.

Чтобы выйти из Web Console:

1. В левом нижнем углу экрана нажмите на имя пользователя.

2. В открывшемся меню выберите пункт **Выход**.

Web Console закроется и отобразится страница входа.

Добавление тонкого клиента в группу управляемых устройств

В Web Console вы можете централизованно управлять тонкими клиентами, подключенными к Kaspersky Security Center: например, объединять их в группы администрирования и применять необходимые политики. Для централизованного управления тонким клиентом требуется переместить его в группу управляемых устройств.

Чтобы добавить тонкий клиент в группу управляемых устройств:

1. В главном окне Web Console выберите **Обнаружение устройств и развертывание → Нераспределенные устройства**.

   Отобразится список всех обнаруженных нераспределенных устройств.

2. Установите флажок рядом с именем устройства, которое вы хотите добавить в группу управляемых устройств.

3. Нажмите на кнопку **Переместить в группу**.

   Справа появится панель **Переместить в группу**. Установите флажок рядом с группой администрирования **Управляемые устройства**.

4. Нажмите на кнопку **Переместить**.

Тонкий клиент будет добавлен в группу управляемых устройств.

Управление политиками

Политика – это набор параметров работы Kaspersky Thin Client, определенный для группы администрирования. Для одного устройства можно настроить несколько политик с различными значениями. Для разных групп администрирования параметры работы программы могут быть различными. В каждой группе администрирования может быть создана собственная политика для программы. Более подробную информацию о концепции управления программой с помощью политик Kaspersky Security Center вы можете прочитать в разделе *Политики и профили политик* в онлайн-справке Kaspersky Security Center.

Параметры политики настраиваются в Kaspersky Security Center Web Console с помощью веб-плагина и передаются в Kaspersky Thin Client при синхронизации программы и Kaspersky Security Center. Время синхронизации можно изменить в параметрах политики.

Активная и неактивная политика

Политика предназначена для группы управляемых устройств и может быть активной или неактивной. Параметры активной политики во время синхронизации сохраняются на клиентских устройствах. К одному устройству нельзя одновременно применить несколько политик, поэтому в каждой группе активной может быть только одна политика.

Вы можете создать неограниченное количество неактивных политик. Неактивная политика не влияет на параметры программы на устройствах в сети. Неактивные политики предназначены для подготовки к нештатным ситуациям, например в случае вирусной атаки. В случае атаки через USB-накопители, вы можете активировать политику, блокирующую доступ к USB-накопителям. При этом активная политика автоматически становится неактивной.

Наследование параметров

Политики, как и группы администрирования, имеют иерархию. По умолчанию дочерняя политика наследует параметры родительской политики. *Дочерняя политика* – политика вложенного уровня иерархии, то есть политика для вложенных групп администрирования и подчиненных Серверов администрирования. Вы можете выключить наследование параметров из родительской политики.

Каждый параметр, представленный в политике, имеет атрибут , который показывает наложен ли запрет на изменение параметров в политиках и локальных параметрах программы. В зависимости от статуса этого атрибута рядом с параметром отображается одно из следующих значений:

- Не определено **Не определено**. Если рядом с параметром отображается значок открытого замка и переключатель выключен, параметр не указан в политике. Пользователь может изменить эти параметры в локальном интерфейсе программы "Лаборатории Касперского". Такие параметры называются разблокированными.

- Принудительно **Принудительно**. Если рядом с параметром отображается закрытый значок замка и переключатель включен, параметр применяется к устройствам, на которых применяется политика. Пользователь не может изменять значения этих параметров в локальном интерфейсе программы "Лаборатории Касперского". Такие параметры называются заблокированными.

Для дочерней политики атрибут работает только, если в дочерней политике включено наследование параметров из родительской политики.

Создание политики

Для управления группой устройств с Kaspersky Thin Client через Web Console требуется создать политику.

Чтобы создать политику для группы устройств:

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне в списке программ выберите Kaspersky Security Management Suite и нажмите на кнопку **Далее**.
4. В окне настройки новой политики на вкладке **Общие** укажите следующие параметры:
   - В поле **Имя** введите имя политики. По умолчанию в поле отображается имя веб-плагина управления Kaspersky Thin Client – Kaspersky Security Management Suite.
   - В блоке **Состояние политики** выберите один из статусов: *Активна*, *Неактивна*, *Для автономных пользователей*. По умолчанию выбран статус *Активна*.
   - Если требуется настроить наследование параметров политики, настройте следующие параметры в блоке **Наследование параметров**:
     - Включите или выключите параметр **Наследовать параметры родительской политики**.
     - Включите или выключите параметр **Обеспечить принудительное наследование параметров для дочерних политик**.
5. Нажмите на кнопку **Сохранить** в нижней части страницы.

Политика будет создана и появится в списке политик Web Console.

Изменение политики

Вы можете изменять созданную ранее политику для группы устройств с Kaspersky Thin Client.

Чтобы изменить политику:

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Выберите политику, которую требуется изменить.
3. В открывшемся окне настройки политики на вкладке **Общие** укажите следующие параметры:
   - Если требуется, в поле **Имя** введите новое имя политики.
   - Если требуется изменить статус политики, в блоке **Состояние политики** выберите один из статусов: *Активна*, *Неактивна*, *Для автономных пользователей*.
   - Если требуется настроить наследование параметров политики, настройте следующие параметры в блоке **Наследование параметров**:
     - Включите или выключите параметр **Наследовать параметры родительской политики**.
     - Включите или выключите параметр **Обеспечить принудительное наследование параметров для дочерних политик**.
4. Нажмите на кнопку **Сохранить** в нижней части страницы.

Изменения в политике будут сохранены и отобразятся в свойствах политики в разделе **История ревизий**.

Настройка параметров Kaspersky Thin Client через Web Console

Этот раздел содержит информацию о настройке параметров Kaspersky Thin Client через Web Console.

Настройка основных параметров Kaspersky Thin Client через Web Console

В Web Console вы можете настроить общие параметры для одного устройства или для группы устройств с Kaspersky Thin Client.

Как настроить основные параметры для одного устройства

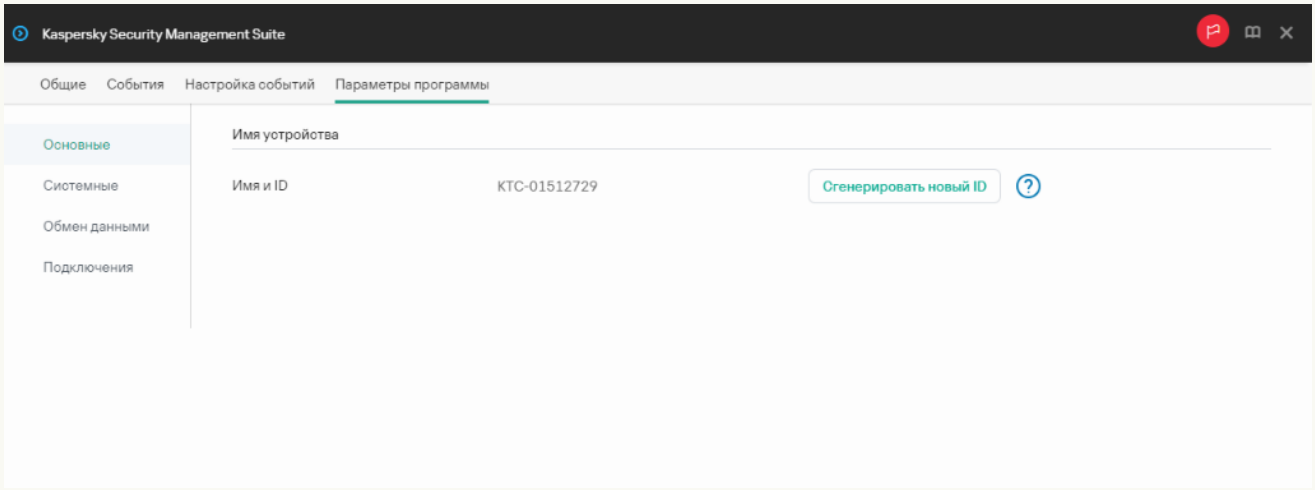
1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя тонкого клиента, на котором запущен Kaspersky Thin Client. Вы можете просмотреть имя устройства в интерфейсе Kaspersky Thin Client. Если имя тонкого клиента отсутствует в списке, добавьте его в группу **Управляемые устройства**.

   Если управляемое устройство добавлено в группу администрирования и для параметров группы настроена принудительная политика, настроенные для этого устройства значения параметров не будут применяться.

3. В открывшемся окне выберите вкладку **Программы**.
4. Нажмите на название веб-плагина управления Kaspersky Security Management Suite.

   Откроется окно, содержащее информацию о Kaspersky Thin Client.

5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Основные** (см. рис. ниже).



Окно настройки общих параметров через Web Console для одного устройства

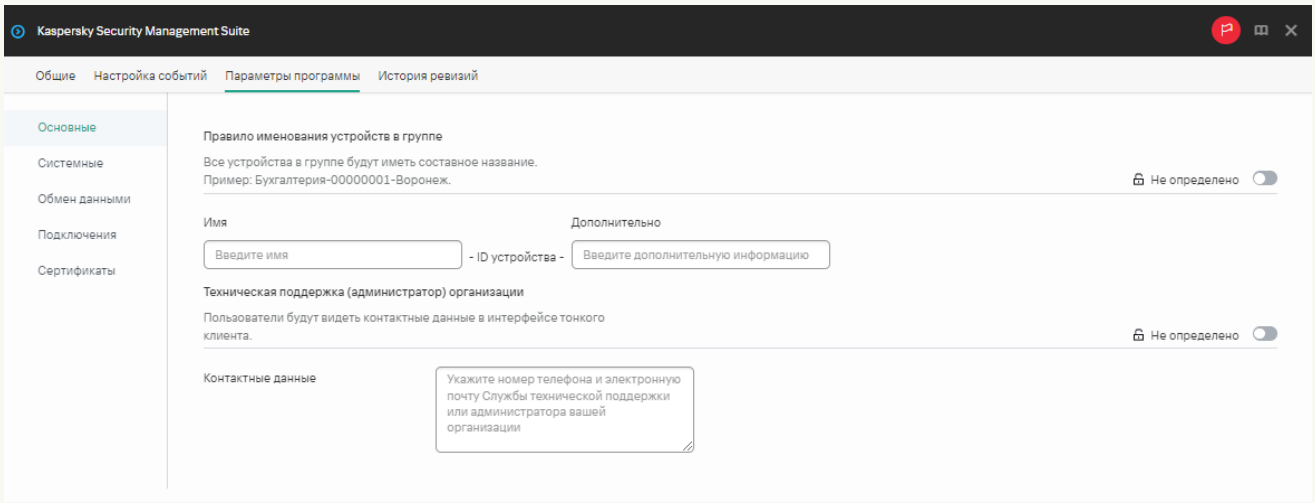
7. Если требуется изменить идентификатор в имени тонкого клиента, в блоке **Имя устройства** нажмите на кнопку **Сгенерировать новый ID**. Управляемое устройство, для которого вы хотите сгенерировать новый идентификатор, должно быть добавлено в группу администрирования и для этой группы должна быть настроена принудительная политика для правила именования устройств в группе.

   Новый идентификатор в имени тонкого клиента будет создан после синхронизации устройства и Kaspersky Security Center.

8. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить изменения.

Как настроить основные параметры для группы устройств

1. В главном окне Web Console выберите **Устройства → Политики и профили политик**.
2. Нажмите на имя политики для веб-плагина управления Kaspersky Security Management Suite.
3. В открывшемся окне выберите вкладку **Параметры программы**.
4. Выберите раздел **Основные** (см. рис. ниже).



Окно настройки общих параметров через Web Console для группы устройств

5. Если требуется указать новый формат имени для устройств группы администрирования, в блоке **Правило именования устройств в группе** укажите новое имя группы и дополнительную информацию, используя прописные и срочные латинские и русские буквы, а также спецсимволы. Уникальный идентификатор (восемь символов) для каждого устройства группы будет сформирован автоматически. Количество символов в имени устройства не должно превышать 30 символов.
6. Переведите переключатель, расположенный справа в блоке **Правило именования устройств в группе**, в положение **Принудительно**.

   Если переключатель напротив названия группы параметров находится в положении **Принудительно** (Принудительно), то установленные значения параметров применяются к устройствам, на которые распространяется политика, изменение этих параметров заблокировано в интерфейсе Kaspersky Thin Client. Если переключатель напротив названия группы параметров в положении **Не определено** (Не определено), то установленные значения параметров не применяются к устройствам, на которых распространяется политика, изменение этих параметров разрешено в интерфейсе Kaspersky Thin Client и для управляемых устройств в разделе **Устройства → Управляемые устройства**.

7. Добавьте контактные данные администратора Kaspersky Security Center в поле **Контактные данные**. Вы можете указать фамилию, имя, номер телефона и адрес электронной почты администратора. Количество символов в поле не должно быть более 80.

   Контактные данные администратора Kaspersky Security Center отображаются пользователю в главном окне Kaspersky Thin Client, в окнах подтверждения сброса параметров и данных Kaspersky Thin Client и подтверждения изменения параметров подключения к Kaspersky Security Center, а также при замене сертификата для подключения к Kaspersky Security Center.

8. Переведите переключатель, расположенный справа в блоке **Техническая поддержка (администратор) организации**, в положение **Принудительно**.
9. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить изменения.

Настройка подключения к удаленной среде под управлением Базис.WorkPlace через Web Console

Вы можете настроить параметры подключения к удаленной среде, развернутой в инфраструктуре Базис.WorkPlace, для одного устройства или группы устройств с Kaspersky Thin Client через Web Console.

Инструкции по подключению к удаленной среде приведены в отдельной статье.

Как настроить параметры подключения к удаленной среде под управлением Базис.WorkPlace для одного устройства

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя тонкого клиента, на котором запущен Kaspersky Thin Client. Вы можете просмотреть имя устройства в интерфейсе Kaspersky Thin Client. Если имя тонкого клиента отсутствует в списке, добавьте его в группу **Управляемые устройства**.

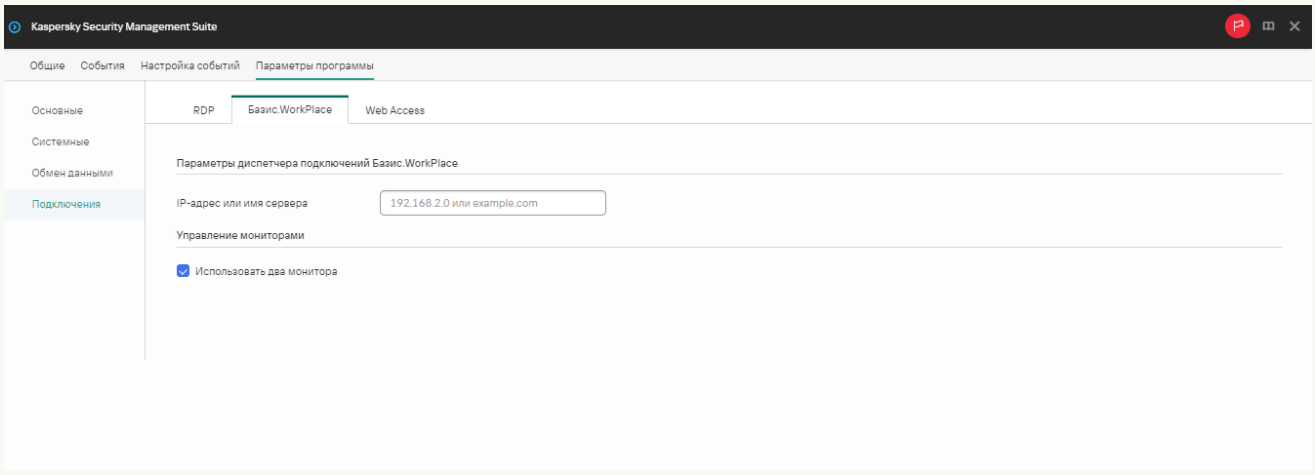
   Если управляемое устройство добавлено в группу администрирования и для параметров группы настроена принудительная политика, настроенные для этого устройства значения параметров не будут применяться.

3. В открывшемся окне выберите вкладку **Программы**.
4. Нажмите на название веб-плагина управления Kaspersky Security Management Suite.

   Откроется окно, содержащее информацию о Kaspersky Thin Client.

5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Подключения** → **Базис.WorkPlace**.

   Откроется окно настройки параметров подключения к удаленной среде, развернутой в инфраструктуре Базис.WorkPlace (см. рис. ниже).



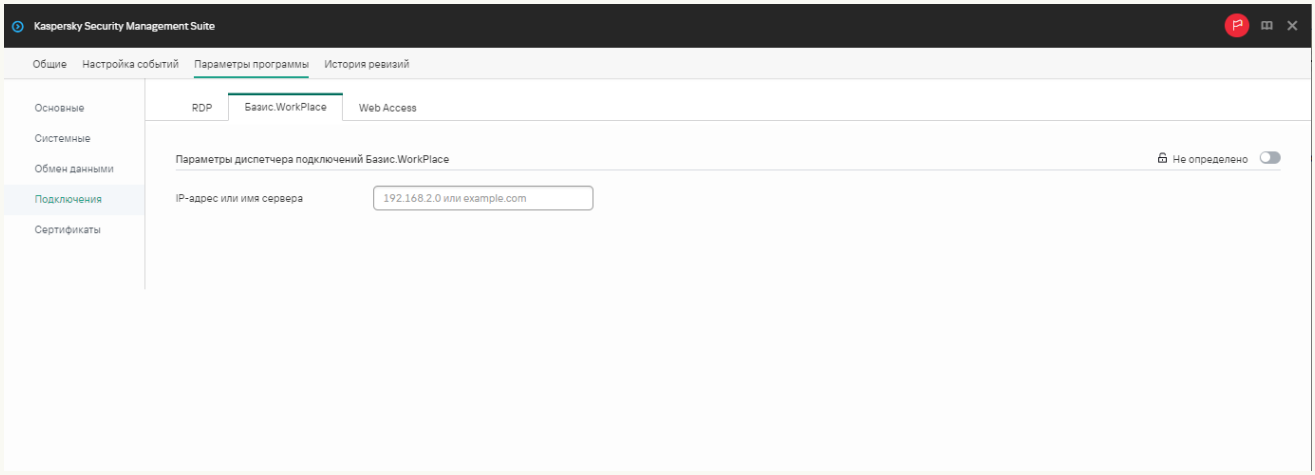
Окно настройки параметров подключения к удаленному рабочему столу под управлением Базис.WorkPlace через Web Console для одного устройства

7. В поле **IP-адрес или имя сервера** введите IP-адрес или имя сервера, к которому необходимо подключиться.
8. Если на вашем рабочем месте установлено два монитора и вы хотите, чтобы изображение удаленного рабочего стола выводилось на оба монитора, в блоке **Управление мониторами** установите флажок **Использовать два монитора**.
9. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить изменения.

Как настроить параметры подключения к удаленной среде под управлением Базис.WorkPlace для группы устройств

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на имя политики для веб-плагина управления Kaspersky Security Management Suite.
3. В открывшемся окне выберите вкладку **Параметры программы**.
4. Выберите раздел **Подключения** → **Базис.WorkPlace**.

   Откроется окно настройки параметров подключения к удаленному рабочему столу под управлением Базис.WorkPlace (см. рис. ниже).



Окно настройки параметров подключения к удаленному рабочему столу под управлением Базис.WorkPlace через Web Console для группы устройств

5. В поле **IP-адрес или имя сервера** введите IP-адрес или имя сервера, к которому необходимо подключиться.
6. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить изменения.

Если переключатель напротив названия группы параметров находится в положении **Принудительно** (Принудительно), то установленные значения параметров применяются к устройствам, на которые распространяется политика, изменение этих параметров заблокировано в интерфейсе Kaspersky Thin Client. Если переключатель напротив названия группы параметров в положении **Не определено** (Не определено), то установленные значения параметров не применяются к устройствам, на которых распространяется политика, изменение этих параметров разрешено в интерфейсе Kaspersky Thin Client и для управляемых устройств в разделе **Устройства** → **Управляемые устройства**.

Существуют следующие ограничения при работе Kaspersky Thin Client через Базис.WorkPlace:

- Не поддерживается авторизация пользователей по смарт-картам в диспетчере подключений Базис.WorkPlace.
- Не поддерживается смена пароля пользователя, инициированная пользователем, через Kaspersky Thin Client.
- Не поддерживается одновременное подключение к нескольким удаленным рабочим столам под управлением Базис.WorkPlace.

Настройка подключения к удаленной среде по протоколу RDP через Web Console

Вы можете настроить параметры подключения к удаленному рабочему столу или виртуальному приложению по протоколу RDP для одного устройства или группы устройств с Kaspersky Thin Client через Web Console.

Инструкции по подключению к удаленной среде приведены в отдельной статье.

Как настроить параметры подключения к удаленной среде по протоколу RDP для одного устройства

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.

2. Нажмите на имя тонкого клиента, на котором запущен Kaspersky Thin Client. Вы можете просмотреть имя устройства в интерфейсе Kaspersky Thin Client. Если имя тонкого клиента отсутствует в списке, добавьте его в группу **Управляемые устройства**.

   Если управляемое устройство добавлено в группу администрирования и для параметров группы настроена принудительная политика, настроенные для этого устройства значения параметров не будут применяться.

3. В открывшемся окне выберите вкладку **Программы**.

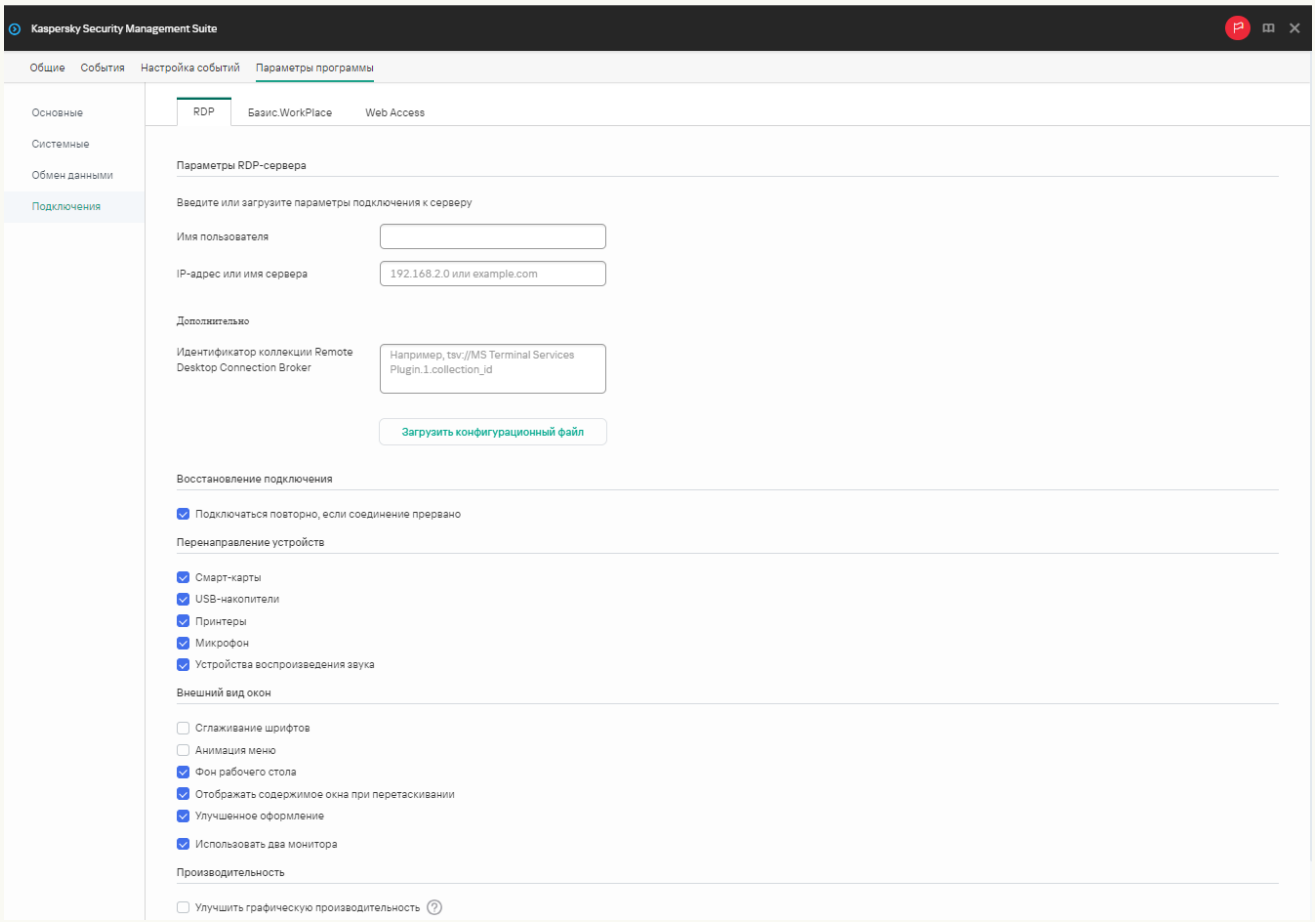
4. Нажмите на название веб-плагина управления Kaspersky Security Management Suite.

   Откроется окно, содержащее информацию о Kaspersky Thin Client.

5. Выберите вкладку **Параметры программы**.

6. Выберите раздел **Подключения** → **RDP**.

   Откроется окно настройки параметров подключения к удаленному рабочему столу или виртуальному приложению по протоколу RDP (см. рис. ниже).



Окно настройки параметров подключения к удаленному рабочему столу по протоколу RDP через Web Console для одного устройства

7. В поле **Сервер** введите IP-адрес или имя сервера брокера Microsoft Remote Desktop Connection Broker.

8. В поле **Имя пользователя** введите имя учетной записи, которая будет использоваться для подключения.

9. Если для подключения к удаленному рабочему столу требуется использовать брокер Microsoft Remote Desktop Connection Broker в поле **Идентификатор коллекции Remote Desktop Connection Broker** укажите идентификатор коллекции, в формате `tsv://MS Terminal Services Plugin.1.collection_id`, где `collection_id` – идентификатор коллекции.

   Для подключения к виртуальному приложению необходимо указать идентификатор коллекции Remote Desktop Connection Broker.

10. Если требуется запустить виртуальное приложение, в поле **Псевдоним приложения** укажите псевдоним приложения.

    Для подключения к виртуальному приложению требуется указать идентификатор коллекции Remote Desktop Connection Broker.

    Если у вас есть конфигурационный файл с параметрами подключения к Microsoft Remote Desktop Connection Broker и, при необходимости, именем приложения, которое нужно открыть, загрузите этот файл, нажав на кнопку **Загрузить конфигурационный файл**. При этом заполнять поля **Идентификатор коллекции Remote Desktop Connection Broker** и **Приложение** не нужно.

11. Если вы хотите, чтобы подключение к удаленному рабочему столу восстанавливалось автоматически после разрыва соединения, установите флажок **Подключаться повторно, если соединение прервано**.

12. В блоке параметров **Перенаправление устройств** напротив необходимых устройств установите следующие флажки:

    - **Смарт-карты**, если хотите включить перенаправление смарт-карт и токенов.
    - **USB-накопители**, если хотите включить перенаправление USB-накопителей.
    - **Принтеры**, если хотите включить перенаправление принтеров.

      На удаленном компьютере должен быть установлен драйвер для принтера, который подключен к тонкому клиенту.

    - **Микрофон**, если хотите включить перенаправление устройств записи звука.

      Управление громкостью и другими параметрами выполняется на удаленном компьютере.

    - **Устройства воспроизведения звука**, если хотите включить перенаправление наушников или колонок.

      Kaspersky Thin Client поддерживает воспроизведение в моно и стерео форматах. Управление громкостью и другими параметрами выполняется в удаленной среде.

13. В блоке **Внешний вид окон** установите флажки напротив графических параметров удаленного рабочего стола, которые требуется использовать:

    - **Сглаживание шрифтов**.
    - **Анимация меню**.
    - **Фон рабочего стола**.
    - **Отображать содержимое окна при перетаскивании**.
    - **Улучшенное оформление**.

Включение параметров отображения удаленного рабочего стола может замедлить скорость работы Kaspersky Thin Client.

14. Если на вашем рабочем месте установлено два монитора и вы хотите, чтобы изображение удаленного рабочего стола выводилось на оба монитора, в блоке **Управление мониторами** установите флажок **Использовать два монитора**.

15. Если вы хотите улучшить производительность при подключении к удаленным рабочим столам или приложениям, в блоке **Производительность** установите флажок **Улучшить графическую производительность**.

    Если пользователю требуется подключиться к удаленному рабочему столу под управлением операционной системы Microsoft Windows 7, снимите флажок **Улучшить графическую производительность**. Эта функциональность не поддерживается при подключении к удаленным рабочим столам под управлением Microsoft Windows 7.

16. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить изменения.

Как настроить параметры подключения к удаленной среде по протоколу RDP для группы устройств

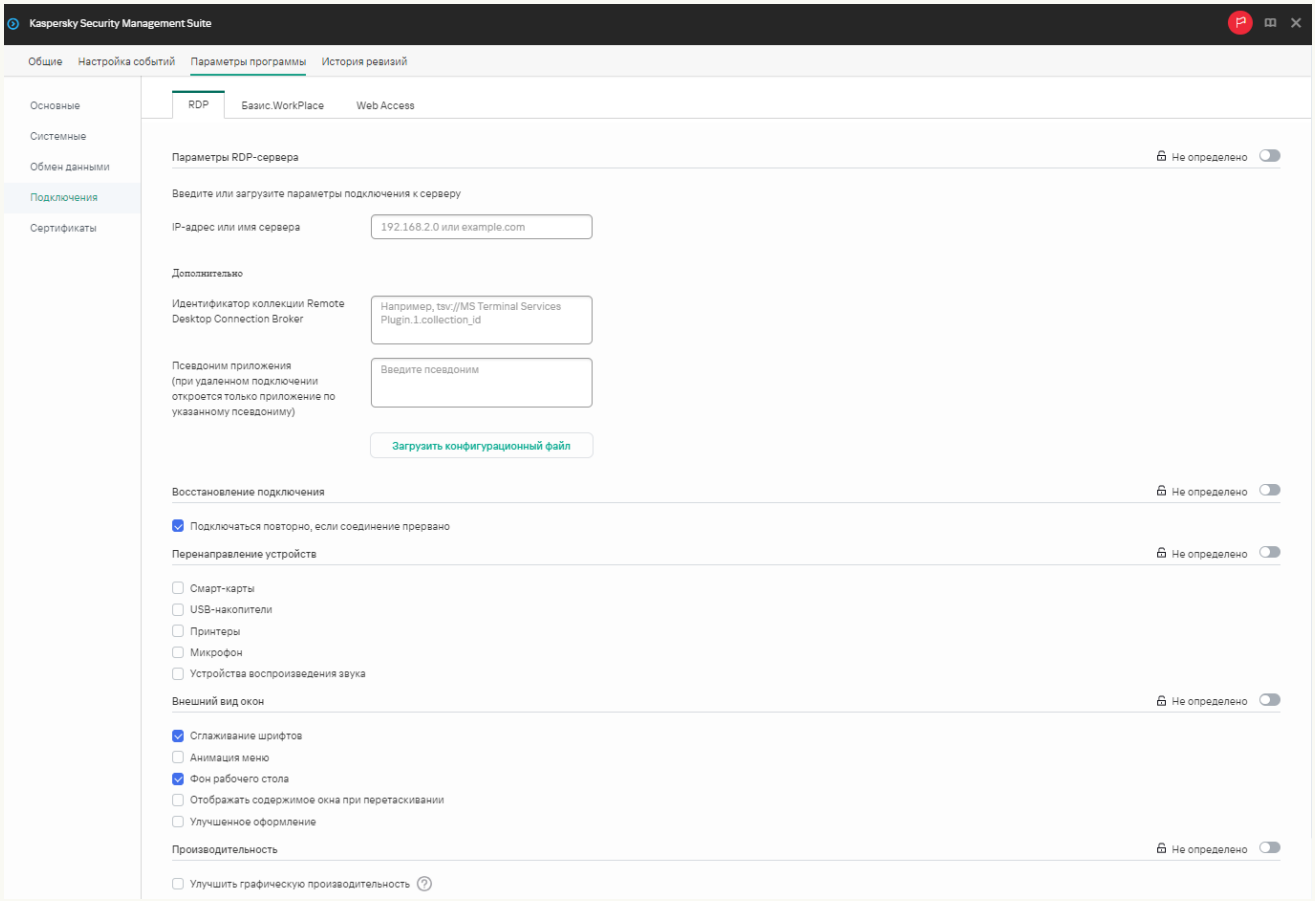
1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.

2. Нажмите на имя политики для веб-плагина управления Kaspersky Security Management Suite.

3. В открывшемся окне выберите вкладку **Параметры программы**.

4. Выберите раздел **Подключения** → **RDP**.

   Откроется окно настройки параметров подключения к удаленному рабочему столу по протоколу RDP (см. рис. ниже).



Окно настройки параметров подключения к удаленному рабочему столу по протоколу RDP через Web Console для группы устройств

5. В поле **Сервер** введите IP-адрес или имя сервера для подключения к удаленному рабочему столу по протоколу RDP.

6. В поле **Имя пользователя** введите имя учетной записи, которая будет использоваться для подключения к удаленному рабочему столу по протоколу RDP.

7. Если для подключения к удаленному рабочему столу требуется использовать брокер Microsoft Remote Desktop Connection Broker в поле **Идентификатор коллекции Remote Desktop Connection Broker** укажите идентификатор коллекции, в формате `tsv://MS Terminal Services Plugin.1.collection_id`, где `collection_id` – идентификатор коллекции.

   Для подключения к виртуальному приложению необходимо указать идентификатор коллекции Remote Desktop Connection Broker.

8. Если требуется запустить виртуальное приложение, в поле **Псевдоним приложения** укажите псевдоним приложения.

Для подключения к удаленному приложению требуется указать идентификатор коллекции Remote Desktop Connection Broker.

Если у вас есть конфигурационный файл с параметрами подключения к Microsoft Remote Desktop Connection Broker и, при необходимости, именем приложения, которое нужно открыть, загрузите этот файл, нажав на кнопку **Загрузить конфигурационный файл**. При этом заполнять поля **Идентификатор коллекции Remote Desktop Connection Broker** и **Приложение** не нужно.

9. Если вы хотите, чтобы подключение к удаленному рабочему столу восстанавливалось автоматически после разрыва соединения, установите флажок **Подключаться повторно, если соединение прервано**.

10. В блоке параметров **Перенаправление устройств** напротив необходимых устройств установите следующие флажки:

    - **Смарт-карты**, если хотите включить перенаправление смарт-карт и токенов.
    - **USB-накопители**, если хотите включить перенаправление USB-накопителей.
    - **Принтеры**, если хотите включить перенаправление принтеров.

      На удаленном компьютере должен быть установлен драйвер для принтера, который подключен к тонкому клиенту.
    - **Микрофон**, если хотите включить перенаправление устройств записи звука.

      Управление громкостью и другими параметрами выполняется на удаленном компьютере.
    - **Устройства воспроизведения звука**, если хотите включить перенаправление наушников или колонок.

      Kaspersky Thin Client поддерживает воспроизведение в моно и стерео форматах. Управление громкостью и другими параметрами выполняется в удаленной среде.

11. В блоке **Внешний вид окон** установите флажки напротив графических параметров удаленного рабочего стола, которые требуется использовать:

    - **Сглаживание шрифтов**.
    - **Анимация меню**.
    - **Фон рабочего стола**.
    - **Отображать содержимое окна при перетаскивании**.
    - **Улучшенное оформление**.

    Включение параметров отображения удаленного рабочего стола может замедлить скорость работы Kaspersky Thin Client.

12. Если вы хотите улучшить производительность при подключении к удаленным рабочим столам или приложениям, в блоке **Производительность** установите флажок **Улучшить графическую производительность**.

Если пользователю требуется подключиться к удаленному рабочему столу под управлением операционной системы Microsoft Windows 7, снимите флажок **Улучшить графическую производительность**. Этот функционал не поддерживается при подключении к удаленным рабочим столам под управлением Microsoft Windows 7.

13. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить изменения.

Если переключатель напротив названия группы параметров находится в положении **Принудительно** (Принудительно), то установленные значения параметров применяются к устройствам, на которые распространяется политика, изменение этих параметров заблокировано в интерфейсе Kaspersky Thin Client. Если переключатель напротив названия группы параметров в положении **Не определено** (Не определено), то установленные значения параметров не применяются к устройствам, на которых распространяется политика, изменение этих параметров разрешено в интерфейсе Kaspersky Thin Client и для управляемых устройств в разделе **Устройства** → **Управляемые устройства**.

Настройка подключения к удаленной среде в Web Access через Web Console

Вы можете настроить параметры подключения к удаленной среде в приложении Web Access для одного устройства или группы устройств с Kaspersky Thin Client через Web Console.

В приложении Web Access вы можете подключиться к удаленной среде, развернутой в инфраструктурах Citrix Workspace и VMware Horizon, с помощью технологии HTML5. При подключении используется браузер Chromium™.

Инструкции по подключению к удаленной среде приведены в отдельной статье.

Как настроить параметры подключения к удаленной среде в Web Access для одного устройства

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя тонкого клиента, на котором запущен Kaspersky Thin Client. Вы можете просмотреть имя устройства в интерфейсе Kaspersky Thin Client. Если имя тонкого клиента отсутствует в списке, добавьте его в группу **Управляемые устройства**.

   Если управляемое устройство добавлено в группу администрирования и для параметров группы настроена принудительная политика, настроенные для этого устройства значения параметров не будут применяться.

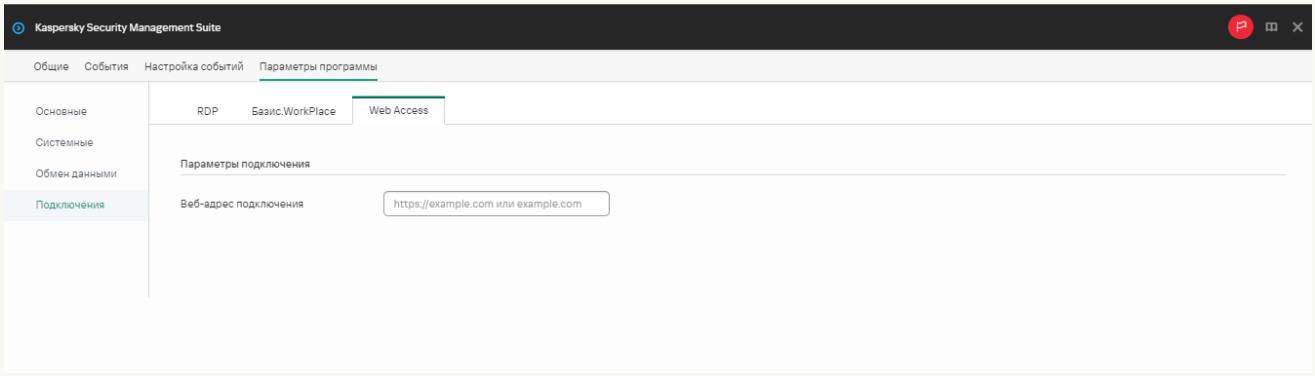
3. В открывшемся окне выберите вкладку **Программы**.
4. Нажмите на название веб-плагина управления Kaspersky Security Management Suite.

   Откроется окно, содержащее информацию о Kaspersky Thin Client.

5. Выберите вкладку **Параметры программы**.

   Выберите раздел **Подключения** → **Web Access**.

   Откроется окно настройки параметров подключения (см. рис. ниже).



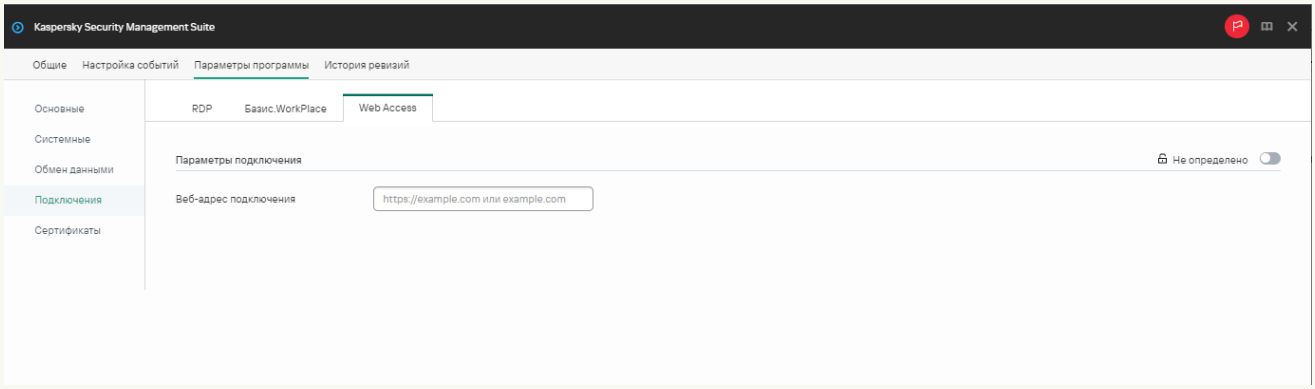
Окно настройки параметров подключения к среде в приложении Web Access через Web Console

6. В поле **Веб-адрес подключения** введите веб-адрес сервера для подключения к необходимой удаленной среде.
7. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить изменения.

Как настроить параметры подключения к удаленной среде в Web Access для группы устройств

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на имя политики для веб-плагина управления Kaspersky Security Management Suite.
3. В открывшемся окне выберите вкладку **Параметры программы**.
4. Выберите раздел **Подключения** → **Web Access**.

   Откроется окно настройки параметров подключения (см. рис. ниже).



Окно настройки параметров подключения к удаленной среде в приложении Web Access через Web Console

5. В поле **Веб-адрес подключения** введите веб-адрес сервера для подключения к необходимой удаленной среде.
6. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить изменения.

Существуют следующие ограничения при работе Kaspersky Thin Client с удаленными рабочими столами под управлением Citrix Workspace:

- Не поддерживается обмен файлами между тонким клиентом и удаленным рабочим столом.
- Не поддерживается буфер обмена между тонким клиентом и удаленным рабочим столом.
- Не поддерживается перенаправление USB-накопителей, смарт-карт, USB-токенов.

Настройка параметров энергосбережения Kaspersky Thin Client через Web Console

В Web Console вы можете настроить параметры энергосбережения для одного устройства или для группы устройств с Kaspersky Thin Client.

Как настроить параметры энергосбережения для одного устройства

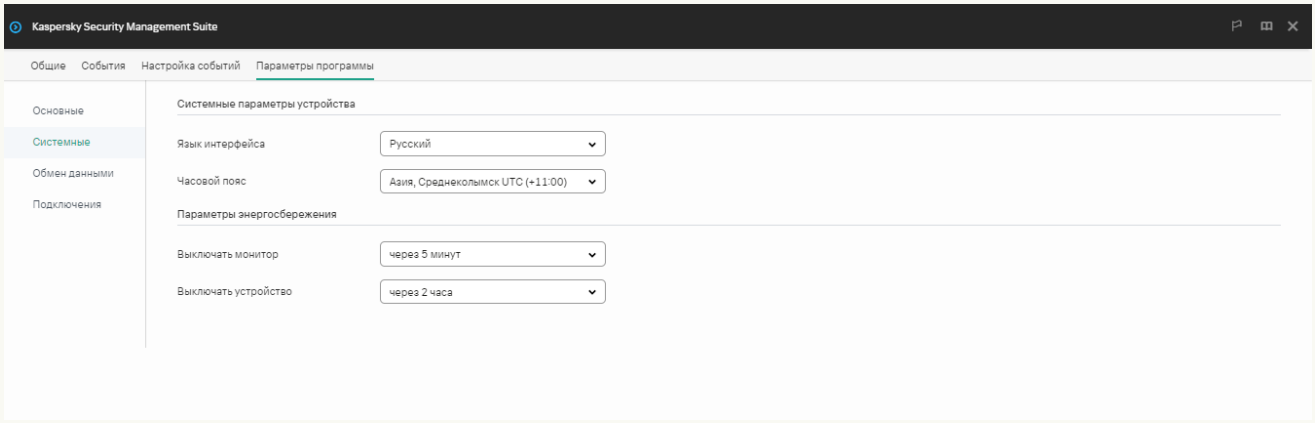
1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя тонкого клиента, на котором запущен Kaspersky Thin Client. Вы можете просмотреть имя устройства в интерфейсе Kaspersky Thin Client. Если имя тонкого клиента отсутствует в списке, добавьте его в группу **Управляемые устройства**.

   Если управляемое устройство добавлено в группу администрирования и для параметров группы настроена принудительная политика, настроенные для этого устройства значения параметров не будут применяться.

3. В открывшемся окне выберите вкладку **Программы**.
4. Нажмите на название веб-плагина управления Kaspersky Security Management Suite.

   Откроется окно, содержащее информацию о Kaspersky Thin Client.

5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Системные** (см. рис. ниже).



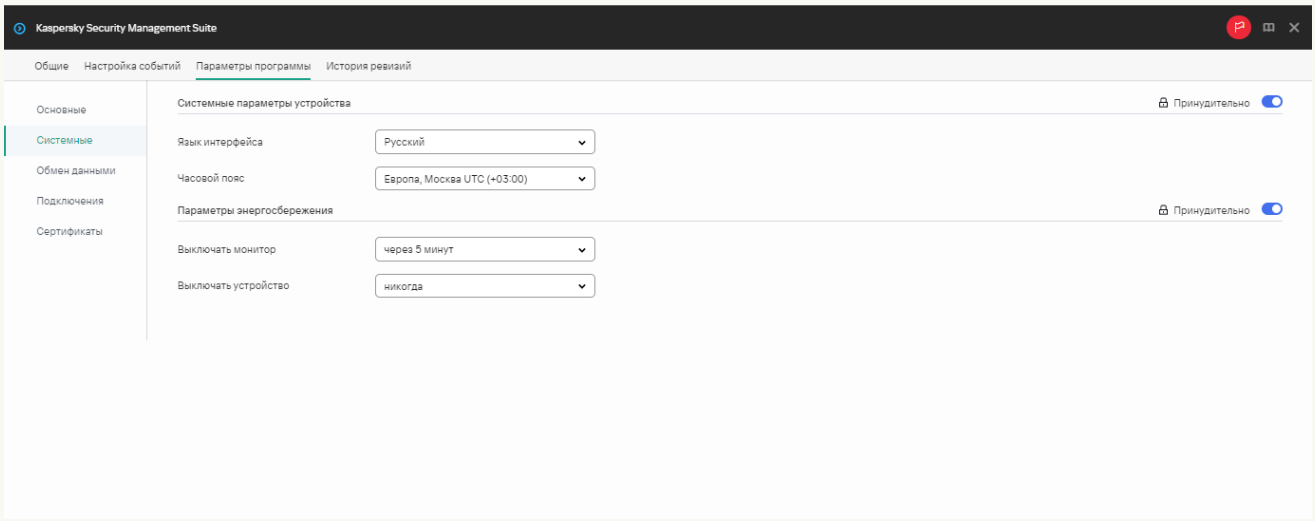
Окно настройки параметров энергосбережения через Web Console для одного устройства

7. В блоке **Параметры энергосбережения** настройте следующие параметры:
   - В раскрывающемся списке **Выключать монитор** выберите время бездействия системы, по истечении которого монитор будет выключен.
   - В раскрывающемся списке **Выключать устройство** выберите время бездействия системы, по истечении которого тонкий клиент будет выключен.
8. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить изменения.

После синхронизации Kaspersky Thin Client и Kaspersky Security Center параметры энергосбережения будут применены к Kaspersky Thin Client.

Как настроить параметры энергосбережения для группы устройств

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на имя политики для веб-плагина управления Kaspersky Security Management Suite.
3. В открывшемся окне выберите вкладку **Параметры программы**.
4. Выберите раздел **Системные** (см. рис. ниже).



Окно настройки параметров энергосбережения через Web Console для группы устройств

5. В блоке **Параметры энергосбережения** настройте следующие параметры:
   - В раскрывающемся списке **Выключать монитор** выберите время бездействия системы, по истечении которого монитор будет выключен.
   - В раскрывающемся списке **Выключать устройство** выберите время бездействия системы, по истечении которого тонкий клиент будет выключен.
6. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить изменения.

После синхронизации всех устройств группы администрирования и Kaspersky Security Center параметры энергосбережения будут применены ко всем Kaspersky Thin Client, которые входят в эту группу.

Если переключатель напротив названия группы параметров находится в положении **Принудительно** (Принудительно), то установленные значения параметров применяются к устройствам, на которые распространяется политика, изменение этих параметров заблокировано в интерфейсе Kaspersky Thin Client. Если переключатель напротив названия группы параметров в положении **Не определено** (Не определено), то установленные значения параметров не применяются к устройствам, на которых распространяется политика, изменение этих параметров разрешено в интерфейсе Kaspersky Thin Client и для управляемых устройств в разделе **Устройства** → **Управляемые устройства**.

Настройка языка интерфейса и часового пояса Kaspersky Thin Client через Web Console

В Web Console вы можете настроить язык интерфейса и часовой пояс для одного устройства или для группы устройств с Kaspersky Thin Client.

Как настроить язык интерфейса и часовой пояс для одного устройства

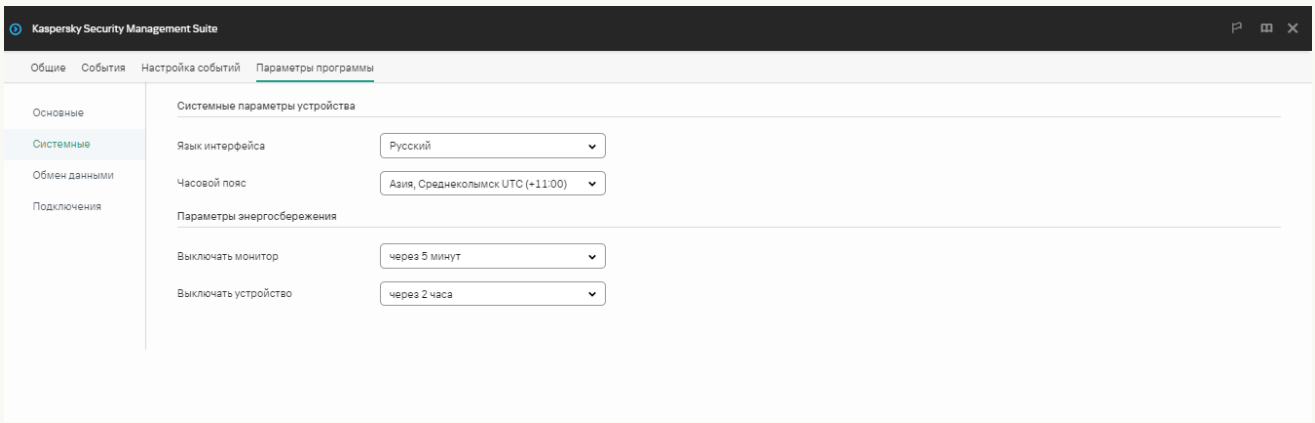
1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя тонкого клиента, на котором запущен Kaspersky Thin Client. Вы можете просмотреть имя устройства в интерфейсе Kaspersky Thin Client. Если имя тонкого клиента отсутствует в списке, добавьте его в группу **Управляемые устройства**.

   Если управляемое устройство добавлено в группу администрирования и для параметров группы настроена принудительная политика, настроенные для этого устройства значения параметров не будут применяться.

3. В открывшемся окне выберите вкладку **Программы**.
4. Нажмите на название веб-плагина управления Kaspersky Security Management Suite.

   Откроется окно, содержащее информацию о Kaspersky Thin Client.

5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Системные** (см. рис. ниже).

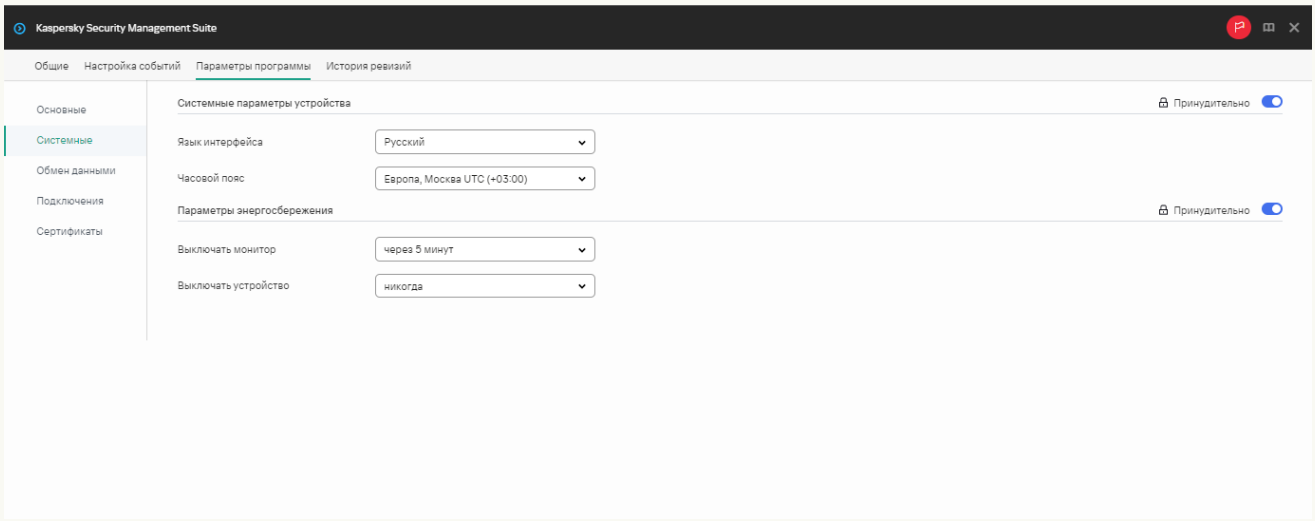


Окно настройки языка интерфейса и часового пояса через Web Console для одного устройства

7. В блоке **Системные параметры устройства** в раскрывающихся списках **Язык интерфейса** и **Часовой пояс** выберите нужные значения.
8. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить изменения.

Как настроить язык интерфейса и часовой пояс для группы устройств

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на имя политики для веб-плагина управления Kaspersky Security Management Suite.
3. В открывшемся окне выберите вкладку **Параметры программы**.
4. Выберите раздел **Системные** (см. рис. ниже).



Окно настройки языка интерфейса и часового пояса через Web Console для группы устройств

5. В блоке **Системные параметры устройства** в раскрывающихся списках **Язык интерфейса** и **Часовой пояс** выберите нужные значения.
6. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить изменения.

Если переключатель напротив названия группы параметров находится в положении **Принудительно** (Принудительно), то установленные значения параметров применяются к устройствам, на которые распространяется политика, изменение этих параметров заблокировано в интерфейсе Kaspersky Thin Client. Если переключатель напротив названия группы параметров в положении **Не определено** (Не определено), то установленные значения параметров не применяются к устройствам, на которых распространяется политика, изменение этих параметров разрешено в интерфейсе Kaspersky Thin Client и для управляемых устройств в разделе **Устройства** → **Управляемые устройства**.

Настройка синхронизации Kaspersky Thin Client и Kaspersky Security Center

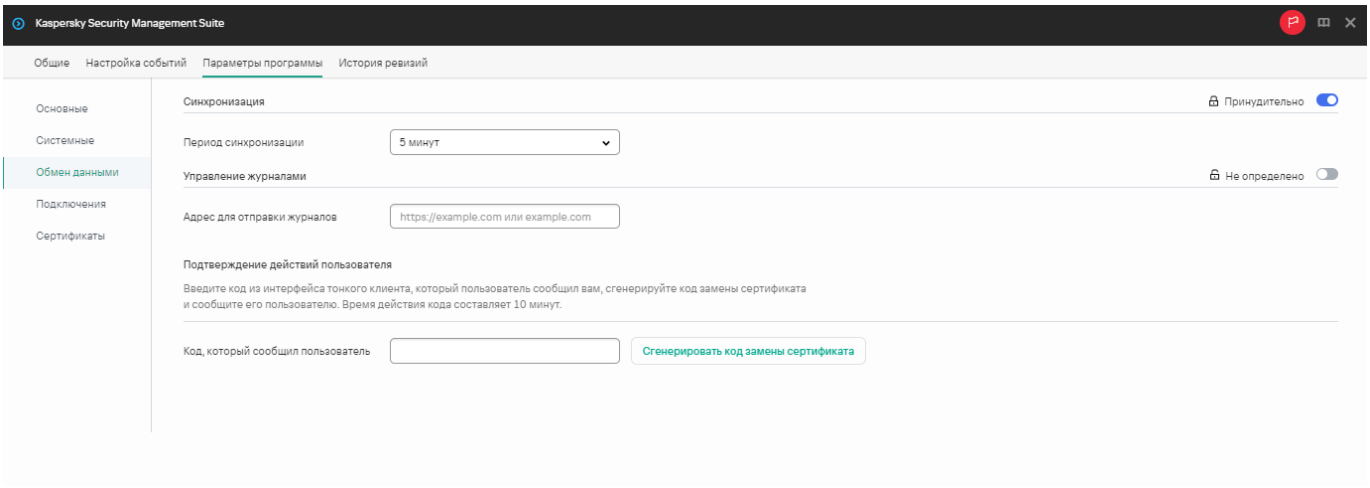
В Web Console вы можете настроить синхронизацию с Kaspersky Security Center только для группы устройств с Kaspersky Thin Client.

Чтобы настроить синхронизацию Kaspersky Thin Client и Kaspersky Security Center:

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на имя политики для веб-плагина управления Kaspersky Security Management Suite.

3. В открывшемся окне выберите вкладку **Параметры программы**.

4. Выберите раздел **Обмен данными** (см. рис. ниже).



Окно настройки синхронизации Kaspersky Thin Client и Kaspersky Security Center

5. В поле **Период синхронизации** укажите время, через которое будет выполняться синхронизация Kaspersky Thin Client с Kaspersky Security Center.

6. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить изменения.

Если переключатель напротив названия группы параметров находится в положении **Принудительно** (Принудительно), то установленные значения параметров применяются к устройствам, на которые распространяется политика, изменение этих параметров заблокировано в интерфейсе Kaspersky Thin Client. Если переключатель напротив названия группы параметров в положении **Не определено** (Не определено), то установленные значения параметров не применяются к устройствам, на которых распространяется политика, изменение этих параметров разрешено в интерфейсе Kaspersky Thin Client и для управляемых устройств в разделе **Устройства** → **Управляемые устройства**.

Настройка отправки журналов Kaspersky Thin Client на сервер журналирования

В Web Console вы можете настроить отправку журналов Kaspersky Thin Client на сервер журналирования для одного устройства или для группы устройств с Kaspersky Thin Client.

Как настроить отправку журналов для одного устройства

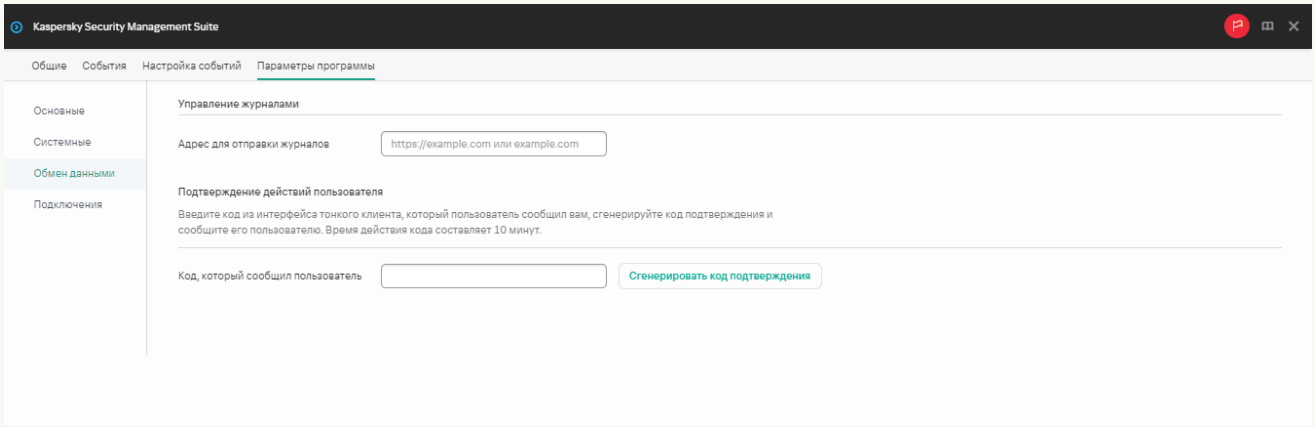
1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя тонкого клиента, на котором запущен Kaspersky Thin Client. Вы можете просмотреть имя устройства в интерфейсе Kaspersky Thin Client. Если имя тонкого клиента отсутствует в списке, добавьте его в группу **Управляемые устройства**.

   Если управляемое устройство добавлено в группу администрирования и для параметров группы настроена принудительная политика, настроенные для этого устройства значения параметров не будут применяться.

3. В открывшемся окне выберите вкладку **Программы**.
4. Нажмите на название веб-плагина управления Kaspersky Security Management Suite.

   Откроется окно, содержащее информацию о Kaspersky Thin Client.

5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Обмен данными** (см. рис. ниже).

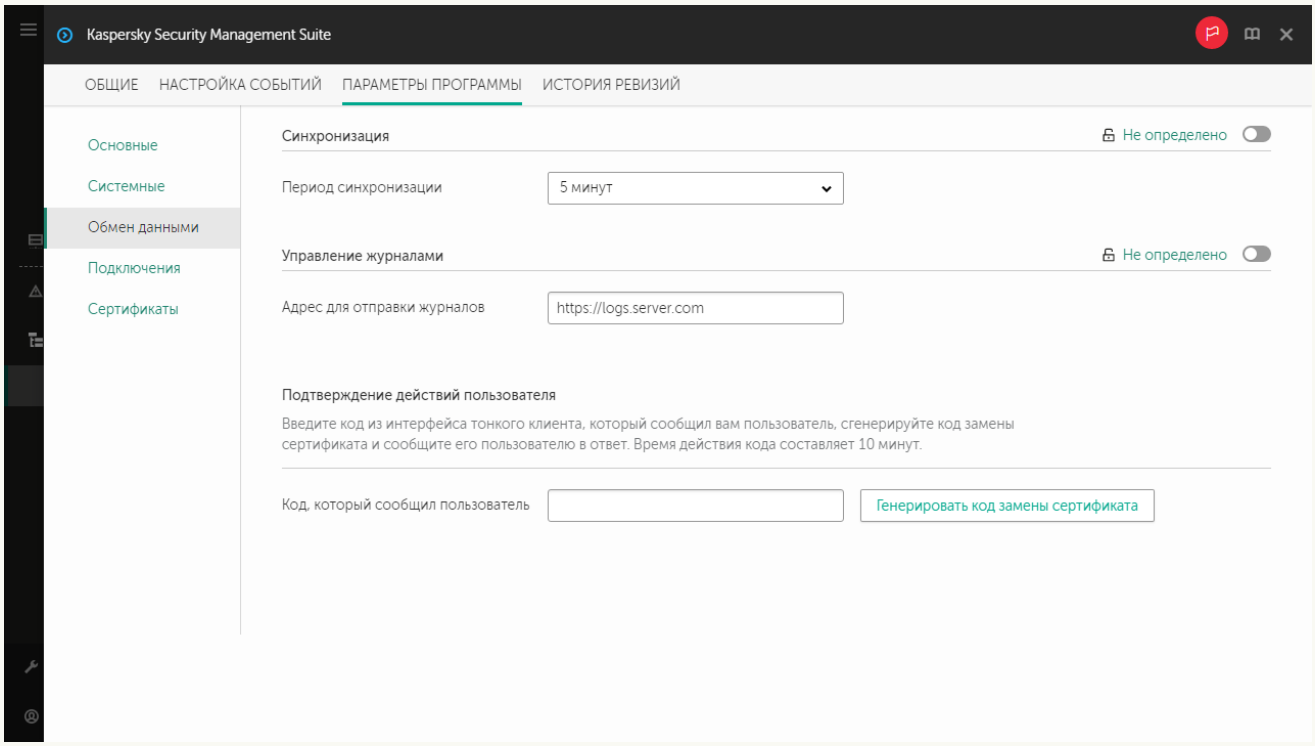


Окно настройки отправки журналов Kaspersky Thin Client через Web Console для одного устройства

7. В поле **Адрес для отправки журналов** введите адрес сервера журналирования, на который будут отправляться журналы, в формате https://<адрес сервера>. Предварительно требуется убедиться, что в инфраструктуре предприятия развернут сервер журналирования с учетом требований.
8. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить изменения.

Как настроить отправку журналов для группы устройств

1. В главном окне Web Console выберите **Устройства → Политики и профили политик**.
2. Нажмите на имя политики для веб-плагина управления Kaspersky Security Management Suite.
3. В открывшемся окне выберите вкладку **Параметры программы**.
4. Выберите раздел **Обмен данными** (см. рис. ниже).



Окно настройки отправки журналов Kaspersky Thin Client через Web Console для группы устройств

5. В поле **Адрес для отправки журналов** введите адрес сервера журналирования, на который будут отправляться журналы, в формате https://<адрес сервера>. Предварительно требуется убедиться, что в инфраструктуре предприятия развернут сервер журналирования с учетом требований.
6. Нажмите на кнопку **Сохранить** в нижней части окна, чтобы сохранить изменения.

Подтверждение действий пользователя Kaspersky Thin Client

Следующие действия пользователя требуют подтверждения со стороны администратора Kaspersky Security Center:

- изменение параметров подключения к Kaspersky Security Center;
- изменение сертификата для подключения к Kaspersky Security Center;
- сброс всех параметров и данных тонкого клиента.

Если тонкий клиент с Kaspersky Thin Client не подключен к Kaspersky Security Center или подключен, но не входит в группу управляемых устройств, от такого тонкого клиента администратору не будут приходить запросы на подтверждение перечисленных выше действий. Добавьте тонкий клиент в группу управляемых устройств, чтобы получать запросы на подтверждение действий пользователя.

Чтобы подтвердить изменение параметров подключения к Kaspersky Security Center или сброс всех параметров тонкого клиента:

1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя тонкого клиента, на котором запущен Kaspersky Thin Client. Вы можете просмотреть имя устройства в интерфейсе Kaspersky Thin Client. Если имя тонкого клиента отсутствует в списке, добавьте его в группу **Управляемые устройства**.

   Если управляемое устройство добавлено в группу администрирования и для параметров группы настроена принудительная политика, настроенные для этого устройства значения параметров не будут применяться.

3. В открывшемся окне выберите вкладку **Программы**.
4. Нажмите на название веб-плагина управления Kaspersky Security Management Suite.

   Откроется окно, содержащее информацию о Kaspersky Thin Client.

5. Выберите вкладку **Параметры программы**.
6. Выберите раздел **Обмен данными**.
7. В блоке **Подтверждение действий пользователя** введите код из интерфейса Kaspersky Thin Client, который сообщил вам пользователь, и нажмите на кнопку **Сгенерировать код подтверждения**.

   Код подтверждения будет создан и отобразится в блоке **Подтверждение действий пользователя**.

8. Сообщите код подтверждения пользователю Kaspersky Thin Client.

Чтобы подтвердить изменение сертификата для подключения к Kaspersky Security Center:

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на имя политики для веб-плагина управления Kaspersky Security Management Suite.
3. В открывшемся окне выберите вкладку **Параметры программы**.
4. Выберите раздел **Обмен данными**.
5. В блоке **Подтверждение действий пользователя** введите код из интерфейса Kaspersky Thin Client, который сообщил вам пользователь, и нажмите на кнопку **Сгенерировать код замены сертификата**.

   Код замены сертификата будет создан и отобразится в блоке **Подтверждение действий пользователя**.

6. Сообщите код замены сертификата пользователю Kaspersky Thin Client.

Управление сертификатами Kaspersky Thin Client через Web Console

В Kaspersky Security Center доступны функции управления сертификатами для подключения тонких клиентов к серверу журналирования и к удаленной среде. В интерфейсе Kaspersky Security Center Web Console вы можете просматривать, добавлять или удалять такие сертификаты.

Рекомендуется настроить подключение группы тонких клиентов к серверу журналирования и к удаленной среде и только с применением сертификатов, назначенных администратором в Web Console. Это поможет предотвратить подключение Kaspersky Thin Client к недоверенным узлам.

В этом разделе также приведены инструкции по управлению сертификатами для подключения Kaspersky Thin Client к Kaspersky Security Center.

О сертификате для подключения Kaspersky Thin Client к Kaspersky Security Center

Kaspersky Thin Client использует для подключения к Kaspersky Security Center *пользовательский мобильный сертификат* (далее также: сертификат). Подробную информацию об этом и других типах сертификатов, используемых Kaspersky Security Center, см. в разделе *О сертификатах* онлайн-справки Kaspersky Security Center.

Сертификат создается с помощью *Мастера первоначальной настройки Сервера администрирования* после установки Kaspersky Security Center. По умолчанию срок действия выпущенного сертификата составляет один год.

Пользовательские мобильные сертификаты не перевыпускаются автоматически.

Вы можете перевыпустить сертификат в Web Console или создать новый сертификат вручную и загрузить его в Web Console.

При миграции на новый Сервер администрирования Kaspersky Security Center также необходимо создать новый сертификат вручную, чтобы затем загрузить его на текущий Сервер как резервный и на новый Сервер как основной.

Перевыпуск сертификата для подключения Kaspersky Thin Client к Kaspersky Security Center в Web Console

Kaspersky Thin Client использует для подключения к Kaspersky Security Center пользовательский мобильный сертификат. Данный тип сертификатов не перевыпускается автоматически.

Чтобы перевыпустить сертификат для подключения Kaspersky Thin Client к Kaspersky Security Center в интерфейсе Web Console:

1. В меню Kaspersky Security Center Web Console нажмите на значок рядом с именем Сервера администрирования Kaspersky Security Center.

   Откроется окно **Свойства Сервера администрирования**.

2. В списке подразделов выберите подраздел **Сертификаты**.

3. В открывшемся окне в блоке **Аутентификация Сервера администрирования мобильными устройствами** выберите необходимый сертификат и нажмите **Перевыпустить**.

4. В открывшемся окне задайте адрес Сервера и укажите, когда требуется активировать сертификат, затем подтвердите свой выбор.

5. Нажмите **Сохранить** в открывшемся окне.

Сертификат для подключения Kaspersky Thin Client к Kaspersky Security Center будет перевыпущен.

Управляемые устройства и устройства, входящие в группу администрирования, получат перевыпущенный сертификат для подключения к Kaspersky Security Center после синхронизации Kaspersky Thin Client и Kaspersky Security Center. Перевыпущенный сертификат сохраняется в хранилище сертификатов Kaspersky Thin Client и может быть использован в качестве резервного для подключения тонких клиентов к Kaspersky Security Center, когда закончится срок действия текущего используемого сертификата.

Вы также можете вручную выпустить новый сертификат для подключения Kaspersky Thin Client к Kaspersky Security Center.

Создание сертификата для подключения Kaspersky Thin Client к Kaspersky Security Center

Вы можете вручную создать сертификат для подключения Kaspersky Thin Client к Kaspersky Security Center. Созданный сертификат может быть использован в качестве основного или резервного (например, при миграции на новый Сервер администрирования Kaspersky Security Center.

Предварительно рекомендуется ознакомиться с требованиями, которые предъявляются к сертификатам Kaspersky Security Center, в разделе *Требования к пользовательским сертификатам, используемым в Kaspersky Security Center* в онлайн-справке Kaspersky Security Center.

Созданный сертификат необходимо загрузить в Web Console.

Чтобы создать сертификат для подключения Kaspersky Thin Client к Kaspersky Security Center с помощью утилиты OpenSSL:

1. Запустите консоль и перейдите в директорию, в которой вы хотите создать сертификат.

2. В консоли запустите утилиту OpenSSL и выполните следующую команду:

   ```
   openssl req -x509 -newkey rsa:2048 -keyout key.pem -out server.pem -days 397 -subj
   '/CN=mydomain.ru/C=RU/L=Moscow/O=My Organization Name/OU=My Organization Unit Name' -
   addext "keyUsage = digitalSignature, keyEncipherment, dataEncipherment, cRLSign,
   keyCertSign" -addext "extendedKeyUsage = serverAuth, clientAuth"
   ```

   где:

   - `-keyout key.pem` – имя файла, в котором будет сохранен закрытый ключ созданного сертификата.
   - `-out server.pem` – имя файла, в котором будет сохранен созданный сертификат.
   - `-days` – параметр, определяющий срок действия созданного сертификата в днях. Рекомендуется указывать срок действия сертификата не более 397 дней.
   - `-subj '/CN=mydomain.ru/C=RU/L=Moscow/O=My Organization Name/OU=My Organization Unit Name'` – данные вашей организации: доменное имя, месторасположение, название.

3. Введите и повторите пароль для закрытого ключа сертификата. Этот пароль потребуется ввести при загрузке пользовательского сертификата в Web Console в качестве мобильного сертификата. Минимальная длина пароля – 8 символов.

В результате в директории, в которой вы запустили команду, будет создано два файла:

- server.pem – файл сертификата для подключения Kaspersky Thin Client к Kaspersky Security Center;
- key.pem – закрытый ключ сертификата для подключения Kaspersky Thin Client к Kaspersky Security Center.

При необходимости вы можете конвертировать файл сертификата из формата PEM в формат DER.

Загрузка сертификата для подключения Kaspersky Thin Client к Kaspersky Security Center в Web Console

Если вы создали сертификат для подключения Kaspersky Thin Client к Kaspersky Security Center, необходимо загрузить такой сертификат в Web Console для передачи на управляемые тонкие клиенты.

Предварительно рекомендуется ознакомиться с требованиями, которые предъявляются к сертификатам Kaspersky Security Center, в разделе *Требования к пользовательским сертификатам, используемым в Kaspersky Security Center* в онлайн-справке Kaspersky Security Center.

Чтобы загрузить в Web Console сертификат для подключения Kaspersky Thin Client к Kaspersky Security Center:

1. В меню Kaspersky Security Center Web Console нажмите на значок рядом с именем Сервера администрирования Kaspersky Security Center.

   Откроется окно **Свойства Сервера администрирования**.

2. В списке подразделов выберите подраздел **Сертификаты**.

3. В открывшемся окне в блоке **Аутентификация Сервера администрирования мобильными устройствами** выберите **Другой сертификат** и нажмите на кнопку **Управление сертификатом**.

4. В открывшейся справа панели нажмите **Обзор** и выполните следующие действия:

   a. В раскрывающемся списке **Тип сертификата** выберите **X.509-сертификат**.

   b. Введите пароль, если пользовательский сертификат защищен паролем.

   c. Выберите файл пользовательского сертификата, нажав на кнопку **Обзор** в блоке **Сертификат**.

   d. Выберите закрытый ключ для пользовательского сертификата, нажав на кнопку **Обзор** в блоке **Приватный ключ**.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить добавление сертификата.

6. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения в подразделе **Сертификаты**.

Сертификат для подключения Kaspersky Thin Client к Kaspersky Security Center будет загружен в Web Console. Управляемые устройства и устройства, входящие в группу администрирования, получат новый сертификат после синхронизации Kaspersky Thin Client и Kaspersky Security Center.

Добавление новых сертификатов в Web Console

Для тонких клиентов, которые входят в группу администрирования, вы можете добавлять в Web Console сертификаты для подключения к удаленной среде или к серверу журналирования.

После добавления сертификата для тонкого клиента в Web Console все сертификаты, принятые пользователем ранее, будут удалены из хранилища устройства.

Чтобы добавить новые сертификаты через Web Console:

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на имя политики для веб-плагина управления Kaspersky Security Management Suite.
3. В открывшемся окне выберите вкладку **Параметры программы**.
4. Выберите раздел **Сертификаты**.
5. В таблице **Действительные сертификаты** нажмите на кнопку **Добавить** в верхней части таблицы сертификатов.
6. В открывшейся справа панели выберите все сертификаты, которые были загружены ранее и новые сертификаты. Общий размер загружаемых файлов не должен превышать 1 МБ. Вы можете загрузить сертификаты только в формате DER. Файл сертификата должен содержать только один сертификат. Если требуется, вы можете предварительно конвертировать сертификат из формата PEM в формат DER.
7. Нажмите на кнопку **OK**, для подтверждения загрузки выбранных сертификатов.

   Выбранные сертификаты загрузятся и информация о них отобразится в таблице **Действительные сертификаты**.

Если добавленный сертификат является корневым (root), то подключение будет осуществляться только по доменному имени сервера.

Удаление сертификатов в Web Console

В Web Console вы можете удалять сертификаты для тонких клиентов, которые входят в группу администрирования.

При удалении всех сертификатов, назначенных группе тонких клиентов, устройства из такой группы смогут быть подключены к любым серверам, в том числе к тем, для которых не были назначены сертификаты.

Чтобы удалить сертификаты:

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на имя политики для веб-плагина управления Kaspersky Security Management Suite.
3. В открывшемся окне выберите вкладку **Параметры программы**.
4. Выберите раздел **Сертификаты**.

5. В таблице **Действительные сертификаты** установите флажки около тех сертификатов, которые требуется удалить.

6. Нажмите на кнопку **Удалить** и подтвердите свои действия.

Выбранные сертификаты будут удалены.

Конвертация сертификата из формата PEM в формат DER

Kaspersky Security Management Suite поддерживает загрузку сертификатов только в формате DER. Вы можете выполнить конвертацию файла сертификата из формата PEM в формат DER.

Для выполнения инструкции на локальном компьютере требуется наличие утилиты OpenSSL.

Чтобы конвертировать файл сертификата из формата PEM в формат DER:

1. На локальном компьютере запустите консоль.

2. Перейдите в директорию, в которой расположен файл сертификата в формате PEM и выполните команду конвертации файла:

   ```
   openssl x509 -outform der -in <имя файла сертификата>.pem -out <имя файла сертификата>.der
   ```

   где:

   - <имя файла сертификата>.pem – название исходного файла сертификата в формате PEM.
   - <имя файла сертификата>.der – название конвертированного файла сертификата в формате DER.

Новый файл сертификата в формате DER будет располагаться в той же директории.

Обновление сертификата при миграции на новый Сервер Kaspersky Security Center

Для миграции тонких клиентов на новый Сервер администрирования Kaspersky Security Center необходимо выпустить сертификат, который будет сохранен на текущем Сервере Kaspersky Security Center как резервный и затем будет использован на новом Сервере как основной.

Чтобы выпустить и подготовить новый сертификат:

1. Запустите консоль и перейдите в папку, в которой вы хотите создать сертификат.

2. Запустите утилиту OpenSSL и выпустите сертификат с помощью следующей команды:

   ```
   openssl req -x509 -sha256 -nodes -days 397 -newkey rsa:2048 -keyout <название файла ключа>.key -out <название файла сертификата>.crt
   ```

   Созданные файлы сертификата и ключа будут сохранены локально.

3. Упакуйте сертификат и ключ в контейнер с помощью следующей команды:

   ```
   openssl pkcs12 -export -out -<название контейнера>.pfx -inkey <название файла ключа>.key -in <название файла сертификата>.crt
   ```

4. Введите и повторите пароль от контейнера. Этот пароль потребуется ввести при загрузке сертификата на серверы.

В результате файл контейнера в формате PFX будет сохранен локально.

Чтобы загрузить сертификат на текущий Сервер Kaspersky Security Center в качестве резервного:

1. Перейдите в папку с установленной программой Kaspersky Security Center и запустите консоль.
2. Запустите утилиту klsetsrvcert и введите следующую команду:

```
klsetsrvcert -t MR -i <путь к контейнеру> -p <пароль от контейнера> -o NoCA
```

> Вам не нужно загружать утилиту klsetsrvcert. Утилита входит в состав комплекта поставки Kaspersky Security Center.

После выполнения команды произойдет перезагрузка Kaspersky Security Center.

Резервный сертификат будет загружен в Web Console.

Чтобы загрузить сертификат на новый Сервер Kaspersky Security Center в качестве основного:

в консоли запустите утилиту klsetsrvcert и выполните следующую команду:

```
klsetsrvcert -t M -i <путь к контейнеру> -p <пароль от контейнера> -o NoCA
```

В результате выполнения инструкций, приведенных выше, сертификат для подключения к новому Серверу администрирования Kaspersky Security Center будет обновлен.

Мониторинг событий Kaspersky Thin Client через Kaspersky Security Center Web Console

Этот раздел содержит инструкции по мониторингу событий, зарегистрированных в Kaspersky Thin Client, через Kaspersky Security Center Web Console

Настройка регистрации уведомлений о событиях Kaspersky Thin Client в Kaspersky Security Center Web Console

Kaspersky Security Center позволяет получать информацию о событиях, произошедших во время работы Kaspersky Thin Client. В интерфейсе Kaspersky Security Center Web Console вы можете настроить уведомление о регистрации таких событий. Каждое событие в Kaspersky Security Center имеет собственный уровень важности. В зависимости от условий возникновения, событию может быть присвоен один из следующих уровней важности:

- *Критическое событие* – событие, указывающее на возникновение критической проблемы, которая может привести к потере данных, сбою в работе или критической ошибке.
- *Отказ функционирования* – событие, указывающее на возникновение серьезной проблемы, ошибки или сбоя, произошедшего во время работы программы или выполнения процедуры.

- *Предупреждение* – событие, на которое нужно обратить внимание, поскольку оно отражает важные ситуации в работе Kaspersky Thin Client и может указывать на возможную проблему в будущем. Чаще всего события относятся к Предупреждениям, если после их возникновения работа программы может быть восстановлена без потери данных или функциональных возможностей.

- *Информационное сообщение* – событие, информирующее об успешном выполнении операции, корректной работе программы или завершении процедуры.

Вы можете настроить уведомления о событиях Kaspersky Thin Client в Kaspersky Security Center Web Console для одного устройства или для группы устройств.

Как настроить уведомления о событиях для одного устройства

1. В главном окне Kaspersky Security Center Web Console выполните одно из следующих действий:

   - Если тонкий клиент входит в группу администрирования, выберите **Устройства** → **Управляемые устройства**.
   - Если тонкий клиент не добавлен в группу администрирования, выберите **Обнаружение устройств и развертывание** → **Нераспределенные устройства**.

2. Нажмите на имя устройства, на котором запущен Kaspersky Thin Client. Вы можете просмотреть имя устройства в интерфейсе Kaspersky Thin Client.

3. В открывшемся окне выберите вкладку **Программы**.

4. Нажмите на название веб-плагина управления Kaspersky Security Management Suite.

   Откроется окно, содержащее информацию о Kaspersky Thin Client.

5. Выберите закладку **Настройка событий**.

6. Выберите уровень важности событий, информацию о которых вы хотите получать:

   - **Критическое**.
   - **Отказ функционирования**.
   - **Предупреждение**.
   - **Информационное сообщение**.

   Отобразится таблица событий для выбранного уровня важности.

7. Нажмите на кнопку **Добавить событие** и в открывшемся окне установите флажок около тех типов событий, которые вы хотите добавить.

8. Нажмите на кнопку **ОК**.

9. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Kaspersky Thin Client будет отправлять на Сервер администрирования Kaspersky Security Center выбранные типы событий с указанным уровнем важности. По умолчанию срок хранения событий составляет 30 дней.

Как настроить уведомления о событиях для группы устройств

1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.
2. Нажмите на имя политики для веб-плагина управления Kaspersky Security Management Suite.
3. В открывшемся окне выберите вкладку **Настройка событий**.
4. Выберите уровень важности событий, информацию о которых вы хотите получать:
   - **Критическое**.
   - **Отказ функционирования**.
   - **Предупреждение**.
   - **Информационное сообщение**.

   Отобразится таблица событий для выбранного уровня важности.
5. Нажмите на кнопку **Добавить событие** и в открывшемся окне установите флажок около тех типов событий, которые вы хотите добавить.
6. Нажмите на кнопку **ОК**.
7. Нажмите на кнопку **Сохранить**, чтобы сохранить внесенные изменения.

Если переключатель **Принудительно** выключен, то параметры не будут применены к устройствам с Kaspersky Thin Client, которые входят в группу администрирования и на которые распространяется текущая политика безопасности.

Kaspersky Thin Client будет отправлять на Сервер администрирования Kaspersky Security Center выбранные типы событий с указанным уровнем важности. По умолчанию срок хранения событий составляет 30 дней.

Подробную информацию о настройке оповещений при регистрации событий в Kaspersky Security Center Web Console см. в разделе онлайн-справки Kaspersky Security Center *Настройка параметров доставки уведомлений*.

Просмотр событий Kaspersky Thin Client через Web Console

Вы можете просматривать события, зарегистрированные Kaspersky Thin Client, через Web Console.

Чтобы просмотреть события, зарегистрированные Kaspersky Thin Client, через Web Console:

1. В главном окне Kaspersky Security Center Web Console выполните одно из следующих действий:
   - Если тонкий клиент входит в группу администрирования, выберите **Устройства** → **Управляемые устройства**.
   - Если тонкий клиент не добавлен в группу администрирования, выберите **Обнаружение устройств и развертывание** → **Нераспределенные устройства**.

2. Нажмите на имя требуемого устройства. Имя устройства указано в интерфейсе Kaspersky Thin Client.

3. В открывшемся окне выберите закладку **События**.

Откроется окно, в котором отображается таблица зарегистрированных событий. Для каждого события отображается следующая информация:

- **Время** – дата и время, когда событие, зарегистрированное на устройстве, было получено в Web Console.
- **Событие** – тип события.
- **Описание** – краткое описание зарегистрированного события.
- **Программа** – название программы, для которой событие было получено в Web Console.
- **Номер версии** – версия программы, для которой событие было получено в Web Console.
- **Уровень критичности** – уровень критичности события (*Критическое*, *Отказ функционирования*, *Предупреждение* или *Информационное сообщение*).
- **Задача** – имя задачи, запускаемой при регистрации события.
- **Зарегистрировано** – дата и время, когда событие было зарегистрированное на устройстве.

Устранение неисправностей

При возникновении ошибки требуется убедиться в следующем:

1. Тонкий клиент включен.
2. Тонкий клиент подключен к сети.
3. При подключении к удаленному рабочему столу были введены верные IP-адрес или имя сервера, имя пользователя и пароль.

Если устранить ошибку не удается, обратитесь в Службу технической поддержки. При необходимости специалисты Службы технической поддержки могут запросить у вас сведения о системе и / или журнал событий.

Разрыв соединения с удаленным рабочим столом

При возникновении ошибки, приводящей к разрыву соединения Kaspersky Thin Client с удаленным рабочим столом, выполнится автоматическое подключение, если такой параметр включен в настройках подключения к удаленной среде.

Если при повторном подключении не было восстановлено соединение или если автоматическое подключение было отключено, экран удаленной сессии закрывается и отображается сообщение с указанием причины сбоя.

Чтобы возобновить работу на удаленном рабочем столе:

1. Закройте сообщение об ошибке.
2. Попробуйте подключиться к удаленному рабочему столу.
3. Если подключение установить не удалось, перезагрузите тонкий клиент, а затем снова попробуйте подключиться к удаленному рабочему столу.
4. Если подключение установить не удалось, обратитесь к администратору вашего предприятия, чтобы устранить физические причины, приводящие к разрыву соединения Kaspersky Thin Client с удаленным рабочим столом.
5. Если установлено прямое подключение, но по-прежнему не удается подключиться к удаленному рабочему столу, обратитесь в Службу технической поддержки.

Проверка подключения к сети

Чтобы проверить, подключен ли тонкий клиент к сети,

просмотрите информацию о состоянии подключения Kaspersky Thin Client к сети в панели управления Kaspersky Thin Client.

Обращение в Службу технической поддержки

При возникновении неисправностей в работе Kaspersky Thin Client, которые не удается решить самостоятельно, обратитесь в Службу технической поддержки "Лаборатории Касперского".

Прежде чем обратиться в Службу технической поддержки, пожалуйста, ознакомьтесь с правилами оказания технической поддержки.

При обращении в Службу технической поддержки специалисты могут запросить у вас журналы событий и аудита. В интерфейсе Kaspersky Thin Client вы можете отправить журналы на сервер журналирования, развернутый в инфраструктуре вашей организации, откуда их смогут загрузить специалисты "Лаборатории Касперского".

О журналах Kaspersky Thin Client

Kaspersky Thin Client ведет два типа журналов:

- Журнал событий. В этом журнале хранятся все события, регистрируемые компонентами Kaspersky Thin Client. Вы можете просмотреть журнал событий через интерфейс Kaspersky Thin Client, а также отправить его на сервер журналирования.
- Журнал аудита. В этом журнале хранятся данные о сертификатах, загруженных в Kaspersky Thin Client, а также информация о фактах включения и выключения управления тонкими клиентами с помощью Kaspersky Security Center. Журнал аудита недоступен для просмотра через интерфейс Kaspersky Thin Client. Вы можете отправить файл журнала аудита на сервер журналирования.

Журнал событий Kaspersky Thin Client содержит следующую информацию:

- Дата и время возникновения события.
- Наименование компонента Kaspersky Thin Client, который зафиксировал событие.
- Важность события. Возможны следующие значения:
  - *Trace* – все возможные сообщения и предупреждения, возникающие при работе программы.
  - *Debug* – отладочные сообщения и все информационные и важные сообщения, а также все предупреждения и сообщения об обычных и критических ошибках.
  - *Info* – информационные сообщения, важные сообщения и все предупреждения, а так же сообщения об обычных и критических ошибках.
  - *Warn* – все предупреждения и сообщения об обычных и критических ошибках.
  - *Error* – сообщения об ошибках и критических ошибках в работе программы.
  - *Fatal* – сообщения о критических ошибках в работе программы.
- Отладочная информация в формате <File>:<Line Number>,<Function>, где:
  - *File* – имя файла.
  - *Line Number* – номер строки в файле.

- *Function* – отладочная информация.

- Идентификатор процесса и идентификатор потока.

- Идентификатор версии продукта.

Журнал аудита Kaspersky Thin Client содержит следующую информацию:

- Дата и время загрузки сертификата для подключения Kaspersky Thin Client к Kaspersky Security Center.

- Адрес Сервера администрирования Kaspersky Security Center (IP-адрес и/или доменное имя сервера).

- Номер порта Сервера администрирования Kaspersky Security Center.

- Список атрибутов сертификата: имя издателя, имя субъекта, отпечаток сертификата, дата и время начала действия, дата и время окончания действия, идентификатор тонкого клиента.

- Информацию о фактах включения и выключения управления Kaspersky Thin Client через Kaspersky Security Center Web Console.

Отправка журналов

При обращении в Службу технической поддержки специалисты "Лаборатории Касперского" могут запросить у вас журналы событий и аудита. В интерфейсе Kaspersky Thin Client вы можете отправить журналы на сервер журналирования, откуда их смогут загрузить специалисты.

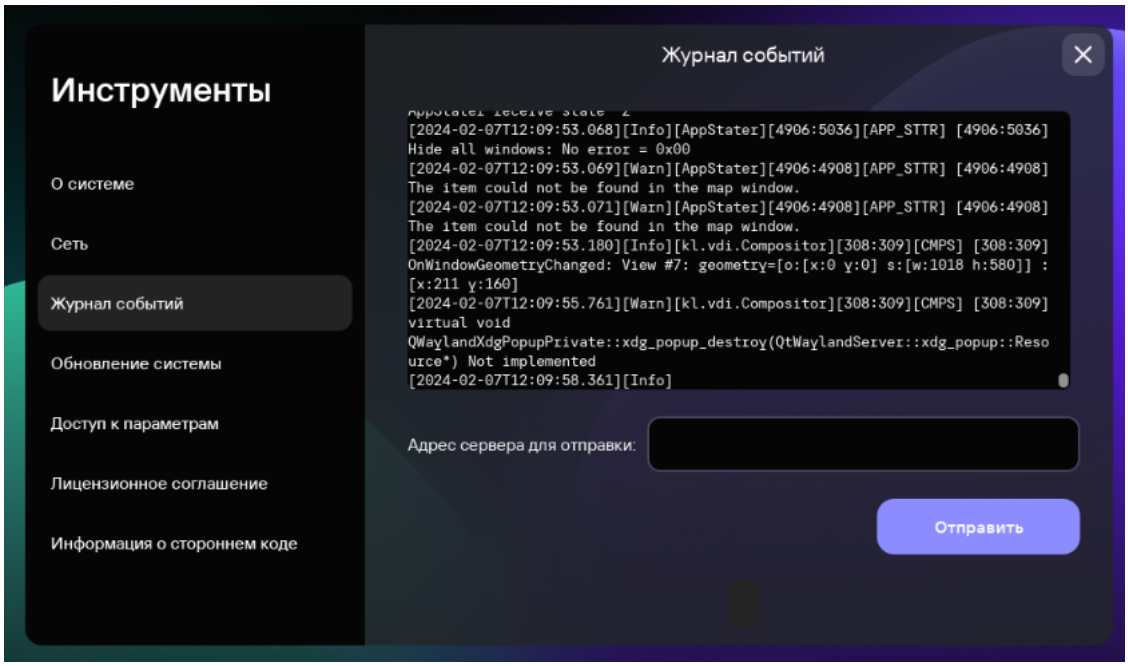
Необходимо предварительно развернуть сервер журналирования в инфраструктуре вашей организации. Подробную информацию о развертывании сервера см. в руководстве администратора к этому серверу.

Максимальный размер файлов журнала событий и журнала аудита составляет 150 МБ и 512 МБ соответственно. Когда размер файлов журнала событий и журнала аудита достигает максимального значения, Kaspersky Thin Client удаляет существующие записи событий и аудита и начинает запись новых. При каждом обновлении журналов событий и аудита в начале журнала фиксируется текущая версия Kaspersky Thin Client.

Чтобы отправить журналы событий и аудита Kaspersky Thin Client:

1. В панели управления Kaspersky Thin Client нажмите на кнопку  и в открывшемся меню выберите **Инструменты**.

2. В открывшемся окне выберите раздел **Журнал событий** (см. рис. ниже).



Инструменты. Раздел Журнал событий

Отобразится информация о зарегистрированных событиях Kaspersky Thin Client.

3. В поле **Адрес сервера для отправки** введите адрес сервера, на который вы хотите отправить журналы событий и аудита и нажмите на кнопку **Отправить**.

   Если Kaspersky Thin Client входит в группу администрирования и управляется централизовано через Web Console и включена функция **Принудительно**, поле **Адрес сервера для отправки** содержит значение, установленное администратором Kaspersky Security Center и недоступно для изменения.

   Рекомендуется проверить правильность адреса сервера, на который вы отправляете журналы. Если указан неверный адрес, журналы будут отправлены и могут попасть к третьим лицам. Конфиденциальность содержащихся в них данных может быть нарушена.

4. В открывшемся окне подтвердите отправку журналов событий и аудита.

   Если Kaspersky Thin Client не входит в группу администрирования, и вы в первый раз выполняете отправку журналов событий и аудита на сервер журналирования, в открывшемся окне **Добавление сертификата** проверьте параметры добавляемого сертификата и нажмите на кнопку **Добавить сертификат**. Сертификат будет добавлен в системное хранилище сертификатов Kaspersky Thin Client и будет использоваться при следующих подключениях.

Журналы событий и аудита Kaspersky Thin Client будут отправлены на указанный сервер.

Глоссарий

TLS

Безопасный протокол передачи данных в локальных сетях и в интернете с использованием шифрования.

Web Access

Приложение для подключения к удаленной среде с помощью технологии HTML5. В текущей версии Kaspersky Thin Client в Web Access поддерживается подключение к виртуальным рабочим столам, развернутым в инфраструктуре Citrix Workspace и VMware Horizon.

Администратор Kaspersky Security Center

Лицо, управляющее работой тонкого клиента через систему удаленного централизованного администрирования Kaspersky Security Center.

Брокер

Сервис, контролирующий доступ и подключение к удаленным рабочим столам и приложениям (например, Microsoft Remote Desktop Connection Broker).

Виртуальное приложение

Приложение, развернутое на удаленном сервере, подключение к которому осуществляется с помощью технологий удаленного доступа.

Группа администрирования

Набор устройств, объединенных в соответствии с выполняемыми функциями. Устройства группируются для удобства управления ими как единым целым. В состав группы могут входить другие группы. Для каждого тонкого клиента, добавленного в группу, могут быть созданы групповые политики.

Обновление

Процедура замены / добавления новых файлов (баз или модулей Kaspersky Thin Client), получаемых с серверов обновлений "Лаборатории Касперского".

Плагин управления Kaspersky Security Management Suite

Специализированный компонент, предоставляющий интерфейс для управления параметрами Kaspersky Thin Client через Консоль администрирования Kaspersky Security Center.

Политика

Политика определяет параметры работы Kaspersky Thin Client и доступ к настройке параметров Kaspersky Thin Client, установленной на устройствах группы администрирования. Вы можете создать неограниченное количество различных политик для Kaspersky Thin Client, установленных на устройствах в каждой группе администрирования, но в пределах группы администрирования только одна политика может применяться единовременно к каждому устройству с Kaspersky Thin Client.

Сервер администрирования

Компонент приложения Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации приложениях "Лаборатории Касперского" и управления ими.

Серверы обновлений "Лаборатории Касперского"

HTTP-серверы "Лаборатории Касперского", с которых приложение "Лаборатории Касперского" получает обновления баз и программных модулей.

Событие

Запись, содержащая информацию об изменении состояния или конфигурации тонкого клиента, или произошедших ошибках, требующих внимания системного администратора.

Тонкий клиент

Компактный персональный компьютер, используемый для удаленного соединения через сеть с удаленными серверами, на которых установлены все необходимые для работы приложения и хранятся данные. К тонкому клиенту подключаются периферийные устройства (например, монитор, клавиатура и мышь).

Удаленный рабочий стол

Операционная система, установленная на машине или развернутая в виртуальной среде. Подключение к такой операционной системе осуществляется с помощью технологий удаленного доступа.

Управляемые устройства

Устройства сети организации, включенные в одну из групп администрирования.

Информация о стороннем коде

Информация о стороннем коде содержится в файле LegalNotices_en.txt, который входит в комплект поставки.

Также вы можете просмотреть информацию о стороннем коде в интерфейсе Kaspersky Thin Client.

Чтобы просмотреть информацию о стороннем коде,

в панели управления Kaspersky Thin Client нажмите на кнопку и в открывшемся меню выберите **Инструменты → Информация о стороннем коде**.

Откроется окно, в котором отображается текст, содержащий информацию об использовании стороннего кода в текущей версии Kaspersky Thin Client.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Ubuntu является зарегистрированным товарным знаком Canonical Ltd.

Citrix, Citrix Workspace являются зарегистрированными товарными знаками или товарными знаками Cloud Software Group, Inc. и/или дочерних компаний в США и/или других странах.

Chromium – товарный знак Google LLC.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft, RemoteFX, Windows и Windows Server являются товарными знаками группы компаний Microsoft.

OpenSSL является товарным знаком правообладателя OpenSSL Software Foundation.

JavaScript – зарегистрированный товарный знак компании Oracle и/или аффилированных компаний.

VMware Horizon – товарный знак VMware, Inc. или зарегистрированный в США или других юрисдикциях товарный знак VMware, Inc.