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 рабочим столам 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** Как настроить параметры Kaspersky Thin Client. Как перевести Kaspersky Thin Client в доверенный режим работы. Как подключиться к удаленному рабочему столу.		**Дополнительные возможности** Управление сертификатами Kaspersky Thin Client. Управление политиками. Управление режимом энергосбережения. Управление доступом к параметрам Kaspersky Thin Client.
	**Мониторинг событий** Как отправить журналы событий и аудита на сервер журналирования. Как просматривать события Kaspersky Thin Client через Kaspersky Security Center Web Console.		**Лицензирование** Узнайте, как осуществляется лицензирование Kaspersky Thin Client.

О Kaspersky Thin Client

Kaspersky Thin Client версии 1.6.1 beta (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 1.6.1 beta устанавливается только на тонкий клиент TONK TN1200.

Kaspersky Thin Client версии 1.6.1 beta распространяется исключительно с целью проведения тестирования в практических условиях информационно-коммуникационной среды юридического лица.

Основные функции Kaspersky Thin Client:

- Подключение к физическим и виртуальным рабочим столам под управлением операционных систем семейства Microsoft® Windows® по протоколу RDP, в том числе через брокер подключений 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 подключений Microsoft Remote Desktop Connection Broker, с авторизацией с помощью имени пользователя и пароля.
- Подключение к физическим и виртуальным рабочим столам под управлением операционных систем семейства Linux® по протоколу RDP с авторизацией с помощью имени пользователя и пароля.
- Подключение к виртуальным рабочим столам, развернутым в инфраструктуре виртуальных рабочих мест Базис.WorkPlace, с авторизацией с помощью имени пользователя и пароля.
- Передача изображения экрана удаленного рабочего места на монитор, подключенный к Kaspersky Thin Client.
- Передача событий от клавиатуры и мыши, подключенных к Kaspersky Thin Client, на удаленный рабочий стол.
- Передача флеш-накопителей, смарт-карт, USB-токенов и принтеров, подключенных к Kaspersky Thin Client, на удаленный рабочий стол.
- Централизованное управление, обновление и контроль Kaspersky Thin Client через Kaspersky Security Center Web Console версии 13.2 и 14.

Kaspersky Thin Client входит в состав комплексного продуктового решения Kaspersky Secure Remote Workspace. Также в состав этого решения входит Kaspersky Security Center Web Console, предназначенная для централизованного администрирования и мониторинга тонких клиентов с Kaspersky Thin Client. Управление тонкими клиентами через Kaspersky Security Center Web Console осуществляется с помощью веб-плагина Kaspersky Security Management Suite (входит в комплект поставки).

Комплект поставки

В комплект поставки Kaspersky Thin Client входят следующие составляющие:

- Архив с установочным образом Kaspersky Thin Client: Kaspersky_Thin_Client_<номер версии>.tar.gz.
- Текстовый файл с информацией о стороннем коде: LegalNotices_en.txt.

- Текстовые файлы с описанием нового функционала и известных ограничений ReleaseNotes_Kaspersky_Thin_Client_<номер версии>_RU.txt, ReleaseNotes_Kaspersky_Thin_Client_<номер версии>_EN.txt.

- Файлы Лицензионного соглашения Kaspersky Thin Client: eula_ru_ktc_<номер версии>.txt, eula_en_ktc_<номер версии>.txt.

В комплект поставки Kaspersky Security Management Suite входят следующие составляющие:

- Архив с установочным образом и файлом подписи веб-плагина для Kaspersky Security Center Web Console: Web_Plugin_Kaspersky_Security_Management_Suite_<номер версии плагина>_ru.exe.

- Архив с установочным образом и файлом подписи веб-плагина для Kaspersky Security Center Web Console: Web_Plugin_Kaspersky_Security_Management_Suite_<номер версии плагина>_en.exe.

- Текстовый файл с информацией о стороннем коде: KSMS_LegalNotices_en.txt.

- Текстовые файлы с описанием нового функционала и известных ограничений ReleaseNotes_Kaspersky_Thin_Client_<номер версии>_RU.txt, ReleaseNotes_Kaspersky_Thin_Client_<номер версии>_EN.txt.

- Файлы Лицензионного соглашения Kaspersky Security Management Suite: eula_ru_ksms_<номер версии>.rtf, eula_en_ksms_<номер версии>.rtf.

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.

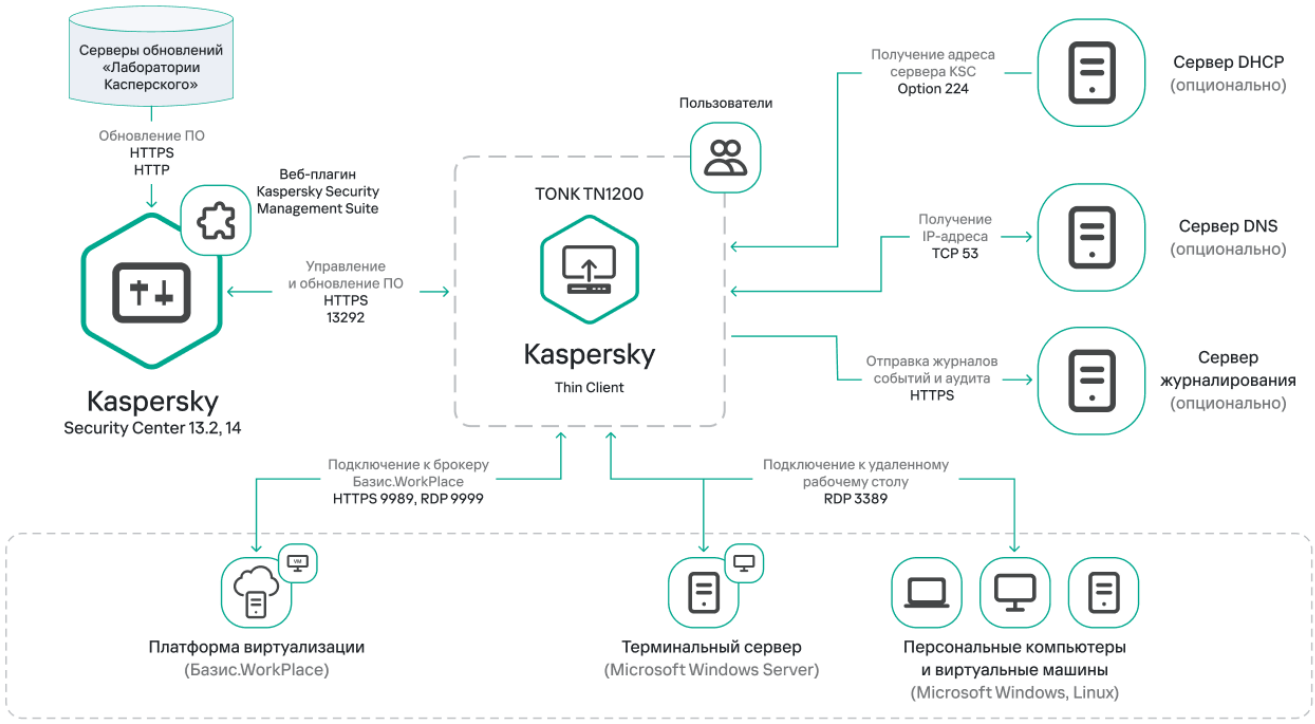
- Администратор подключает и настраивает взаимодействие между Kaspersky Thin Client и Kaspersky Security Center.

- Kaspersky Thin Client получает параметры подключения к удаленному рабочему столу, обновлений, доверенных сертификатов, а также дату и время с политикой от Kaspersky Security Center.

- Пользователь подключается к удаленному рабочему столу по протоколу RDP либо через платформу виртуализации Базис.WorkPlace.

- 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

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 стандартными, проводными клавиатурой и мышью без мультимедийных функций, которые подключаются через USB-порты. При необходимости вы можете подключать и/или отключать клавиатуру и/или мышь через USB-порты во время работы Kaspersky Thin Client. Вы можете переключать раскладку клавиатуры только с помощью комбинации клавиш ALT+SHIFT (изменение комбинации клавиш для смены раскладки не поддерживается). Kaspersky Thin Client поддерживает работу с принтерами, которые подключаются через USB-порты. На удаленном компьютере должен быть установлен драйвер для принтера, который подключен к тонкому клиенту.

Требования к удаленным рабочим столам

Вы можете подключаться к физическим 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 2.12.43.
- Astra Linux Special Edition 1.7.
- ALT Linux 10.
- РЕД ОС® 7.3.

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 виртуальным 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 2.12.43.
- Astra Linux Special Edition 1.7.
- ALT Linux 10.
- РЕД ОС 7.3.

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 версий 13.2 и 14. 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.
- Приемка журналов Kaspersky Thin Client осуществляется методом PUT.

Что нового

В Kaspersky Thin Client версии 1.6.1 beta появились следующие возможности и доработки:

- Подключение через Microsoft Remote Desktop Connection Broker – добавлена функциональность, позволяющая подключаться к удаленным рабочим столам под управлением операционных систем семейства Microsoft Windows через брокер подключений Microsoft Remote Desktop Connection Broker.

- Автоматическое подключение при разрыве соединения – добавлена функциональность, позволяющая использовать автоматическое подключение к удаленному рабочему столу по протоколу RDP при разрыве соединения.

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

- Перенаправление принтера на удаленный рабочий стол – добавлена возможность печати документов из гостевой операционной системы (при подключении по протоколу RDP) 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 подключения к удаленным рабочим столам по доменному имени.

- Улучшение работы тонкого клиента – улучшена стабильность работы тонкого клиента, подключенного к Kaspersky Security Center.

Установка Kaspersky Thin Client

Установку Kaspersky Thin Client на аппаратную платформу выполняют специалисты ООО "Группа Компаний ТОНК".

Интерфейс Kaspersky Thin Client

Интерфейс Kaspersky Thin Client содержит следующие элементы:

- Главное окно Kaspersky Thin Client. В главном окне вы можете выбрать подключение к удаленному рабочему столу по протоколу RDP напрямую или подключение к удаленным рабочим столам под управлением Базис.WorkPlace. В окне подключения вы можете настроить параметры подключения по протоколу RDP или параметры подключения к Базис.WorkPlace. Если Kaspersky Thin Client входит в группу администрирования и в общих параметрах группы указаны контактные данные администратора, в главном окне также отображаются контакты администратора Kaspersky Security Center.

- Панель управления Kaspersky Thin Client. Содержит следующие элементы:

  - – кнопка завершения работы. Позволяет 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.

  - Область уведомлений, в которой отображается:

    - Информация о состоянии подключения Kaspersky Thin Client к сети и к Kaspersky Security Center.
    - Информация о новых уведомлениях Kaspersky Thin Client.

  - Кнопка переключения языка ввода текста с клавиатуры.

  - Дата и время системы.

После подключения и во время сессии подключения к удаленному рабочему столу в верхней части экрана отображается панель подключения. В панели подключения отображается название удаленного рабочего стола и имя подключенного пользователя. Когда вы подключаетесь к удаленному рабочему столу панель подключения свернута и ее кнопки скрыты. Вы можете перемещать панель подключения по горизонтали вправо или влево, нажав на нее левой клавишей мыши и дождавшись появления стрелки.

Панель подключения можно развернуть одним из следующих способов:

- Нажать на панель подключения левой клавишей мыши.

- Нажать комбинацию клавиш **CTRL+ALT+HOME**.

В развернутой панели подключения отображается кнопка **Завершить сессию**, которая завершает сессию подключения к удаленному рабочему столу. Также вы можете завершить сессию подключения, нажав комбинацию клавиш **CTRL+D**.

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 устройствах, на которых установлена система Kaspersky Thin Client, а также на серверах локальной инфраструктуры, с которыми взаимодействует Kaspersky Thin Client.

Kaspersky Thin Client сохраняет на устройстве следующую информацию:

- Журнал событий, содержащий технические сведения о работе системы и события, которые Kaspersky Thin Client отправляет на Сервер 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 устройстве.
  - 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 или дополнительным.
  - Идентификатор основного монитора.
  - Месторасположение (координаты) панели подключения.
  - Время последнего использования сертификатов для проверки подлинности подключения: к Kaspersky Security Center, к удаленным рабочим столам по протоколу RDP или через Базис.WorkPlace и к серверу журналирования.
- Параметры работы 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 удаленным рабочим столам, диспетчеру подключений Базис.WorkPlace и серверу журналирования.
  - Отпечаток текущего сертификата для проверки подлинности подключения Kaspersky Thin Client к Kaspersky Security Center.
  - Параметры именования Kaspersky Thin Client, заданные администратором Kaspersky Security Center (имя, идентификатор устройства 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 к 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 соединения при подключении к удаленному рабочему столу под управлением Базис.WorkPlace.
  - Количество попыток повторного подключения.
  - Тип соединения Kaspersky Thin Client с брокером подключений Базис.WorkPlace.
  - Параметры перенаправления на удаленный рабочий стол локальных 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) RDP-сервера.
  - Домен и имя пользователя для подключения к RDP-серверу.
  - Идентификатор коллекции Remote Desktop Connection Broker.
  - Файлы сертификатов для проверки подлинности RDP-сервера при подключении к удаленному рабочему столу по протоколу RDP.
  - Параметры перенаправления на удаленный рабочий стол локальных устройств:
    - Разрешено ли перенаправление USB-накопителей.
    - Разрешено ли перенаправление смарт-карт.
    - Разрешено ли перенаправление принтеров.
  - Включено ли использование двух мониторов.
  - Включено ли автоматическое подключение к удаленному рабочему столу 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 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 режима 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 и английском языках.

- Информация о факте принятия Лицензионных соглашений.
- Информация о датах выпуска Лицензионных соглашений.

Система виртуализации Базис.WorkPlace сохраняет в базе данных следующую информацию:

- Имя пользователя.
- IP-адрес Kaspersky Thin Client.
- Идентификатор Kaspersky Thin Client.
- События установления сессии.
- События завершения сессии.

Имя или IP-адрес RDP-сервера и диспетчера подключений Базис.WorkPlace перезаписываются при каждом успешном подключении.

Имя пользователя перезаписывается при каждом успешном подключении к RDP-серверу или диспетчеру подключений Базис.WorkPlace.

Адрес сервера журналирования для отправки журнала событий и аудита перезаписывается при каждой успешной отправке событий системы на сервер журналирования. При отправке журнала событий и аудита на сервер журналирования отправляются все события системы, сохраненные на тонком клиенте.

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.

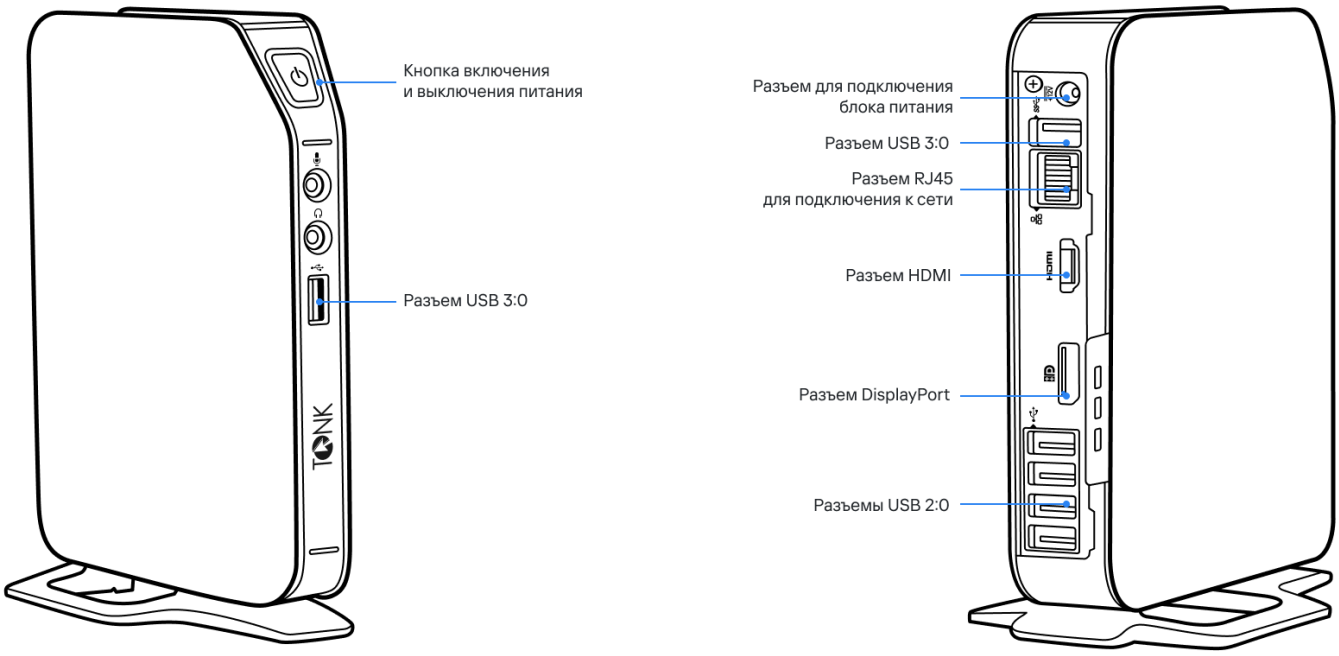
Чтобы включить Kaspersky Thin Client,

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, логи 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.

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 установить и настроить Kaspersky Thin Client, Kaspersky Security Center, а также установить между ними соединение.

Сценарий установки Kaspersky Thin Client, Kaspersky Security Center и настройки между ними соединения 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. ZIP-архив с дистрибутивом веб-плагина входит в комплект поставки.

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. **Включение доверенного режима работы для группы устройств**

    Переведите устройства, которые входят в группу администрирования, в доверенный режим работы. Также рекомендуется добавить резервный сертификат для подключения Kaspersky Thin Client к Kaspersky Security Center.

В результате выполнения этих действий Kaspersky Thin Client будет готов 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: Миграция управления Kaspersky Thin Client на новый Сервер Kaspersky Security Center

В этом разделе приводится последовательность действий, которые требуется выполнить администратору при подключении группы устройств с Kaspersky Thin Client к управлению новым Сервером администрирования Kaspersky Security Center, если управление этой группой осуществлялось ранее через другой Kaspersky Security Center.

Сценарий настройки управления Kaspersky Thin Client при миграции на новый 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. ZIP-архив с дистрибутивом веб-плагина входит в комплект поставки.

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. **Сохранение мобильного сертификата нового Сервера администрирования Kaspersky Security Center**

   Сохраните локально мобильный сертификат нового Сервера администрирования Kaspersky Security Center.

8. **Загрузка резервного сертификата в используемой Kaspersky Security Center Web Console**

   Загрузите мобильный сертификат нового Сервера администрирования Kaspersky Security Center в качестве резервного сертификата в используемой ранее Kaspersky Security Center Web Console. При необходимости вы можете в качестве резервного сертификата загрузить пользовательский сертификат для подключения Kaspersky Thin Client к Kaspersky Security Center. Для этого предварительно требуется создать и загрузить в Kaspersky Security Center Web Console пользовательский сертификат.

   Дождитесь выполнения синхронизации Kaspersky Thin Client и Kaspersky Security Center. Период синхронизации устанавливается при настройке Kaspersky Thin Client через Kaspersky Security Center Web Console. После синхронизации устройства, входящие в группу администрирования, получат мобильные сертификаты нового Сервера администрирования Kaspersky Security Center.

9. **Настройка подключения Kaspersky Thin Client к новому 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.

   Устройства, входящие в группу администрирования, будут подключены к новому Серверу администрирования Kaspersky Security Center, и вы сможете управлять ими через интерфейс Web Console.

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

Сценарий: Переход Kaspersky Thin Client в доверенный режим работы

Доверенный режим работы – это режим работы Kaspersky Thin Client, при котором тонкий клиент подключен и управляется через Kaspersky Security Center. Предварительно требуется установить и настроить Kaspersky Security Center.

Сценарий включения доверенного режима работы Kaspersky Thin Client состоит из следующих этапов:

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

   В интерфейсе Kaspersky Thin Client настройте подключение Kaspersky Security Center.

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

В интерфейсе Kaspersky Security Center Web Console создайте активную политику для группы устройств, для которых требуется включить централизованное управление через Kaspersky Security Center.

3. **Добавление сертификатов для безопасного подключения к удаленным рабочим столам**

   В интерфейсе Kaspersky Security Center Web Console добавьте сертификаты для безопасного подключения к удаленным рабочим столам (по RDP или под управлением Базис.WorkPlace) и переведите переключатель в правой части страницы в положение **Принудительно**. Дождитесь выполнения синхронизации Kaspersky Thin Client и Kaspersky Security Center. Период синхронизации устанавливается при настройке Kaspersky Thin Client через Kaspersky Security Center Web Console. После синхронизации устройства получат сертификаты Сервера администрирования Kaspersky Security Center.

В результате выполнения этих действий Kaspersky Thin Client перейдет в доверенный режим работы.

В некоторых случаях, например при переходе на новый Сервер администрирования Kaspersky Security Center, вы можете вывести устройство с Kaspersky Thin Client из доверенного режима работы, удалив сертификаты безопасности и отключив управление группой через Kaspersky Security Center.

Настройка общих параметров

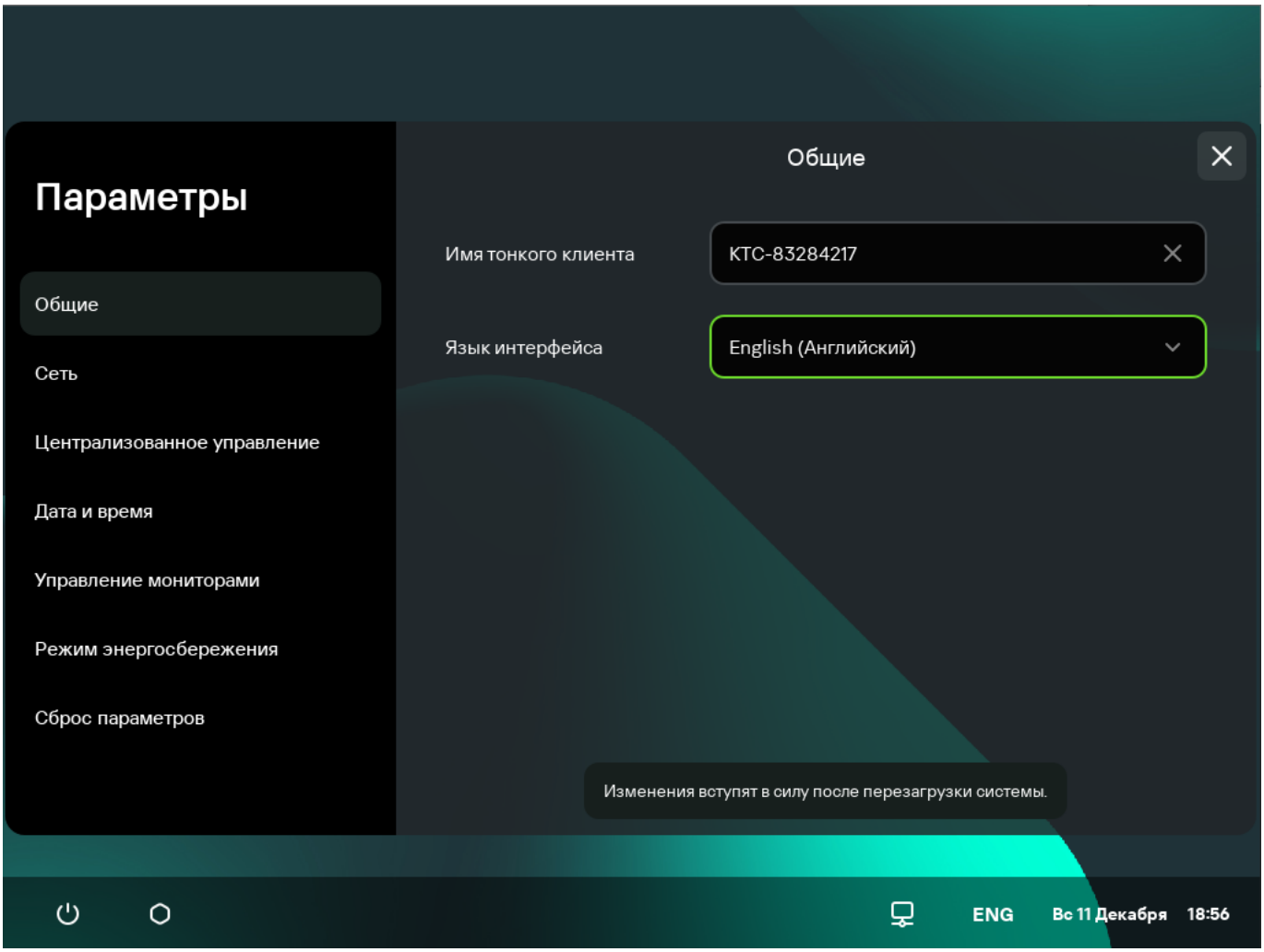
В интерфейсе Kaspersky Thin Client вы можете настроить общие параметры тонкого клиента. Например, вы можете указать имя тонкого клиента, которое будет отображаться в панели задач Kaspersky Thin Client и в Kaspersky Security Center Web Console, а также выбрать язык интерфейса Kaspersky Thin Client.

Если Kaspersky Thin Client входит в группу администрирования и управляется централизовано через Web Console, имя устройства задает администратор Kaspersky Security Center. При включенной функции **Принудительно** поле **Имя тонкого клиента** в интерфейсе Kaspersky Thin Client недоступно для изменения.

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.

Изменения вступят в силу после перезагрузки системы.

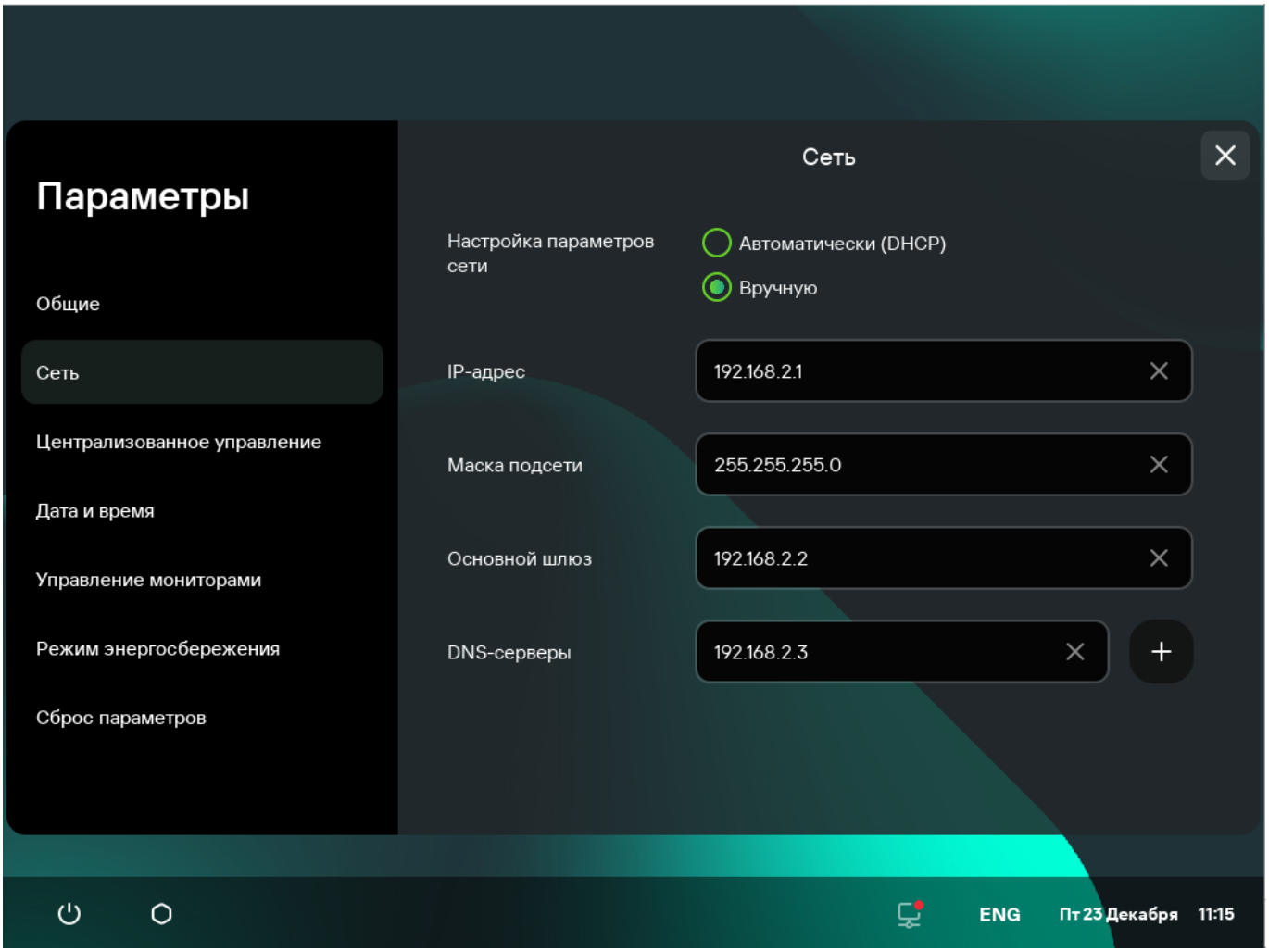
Настройка параметров сети

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

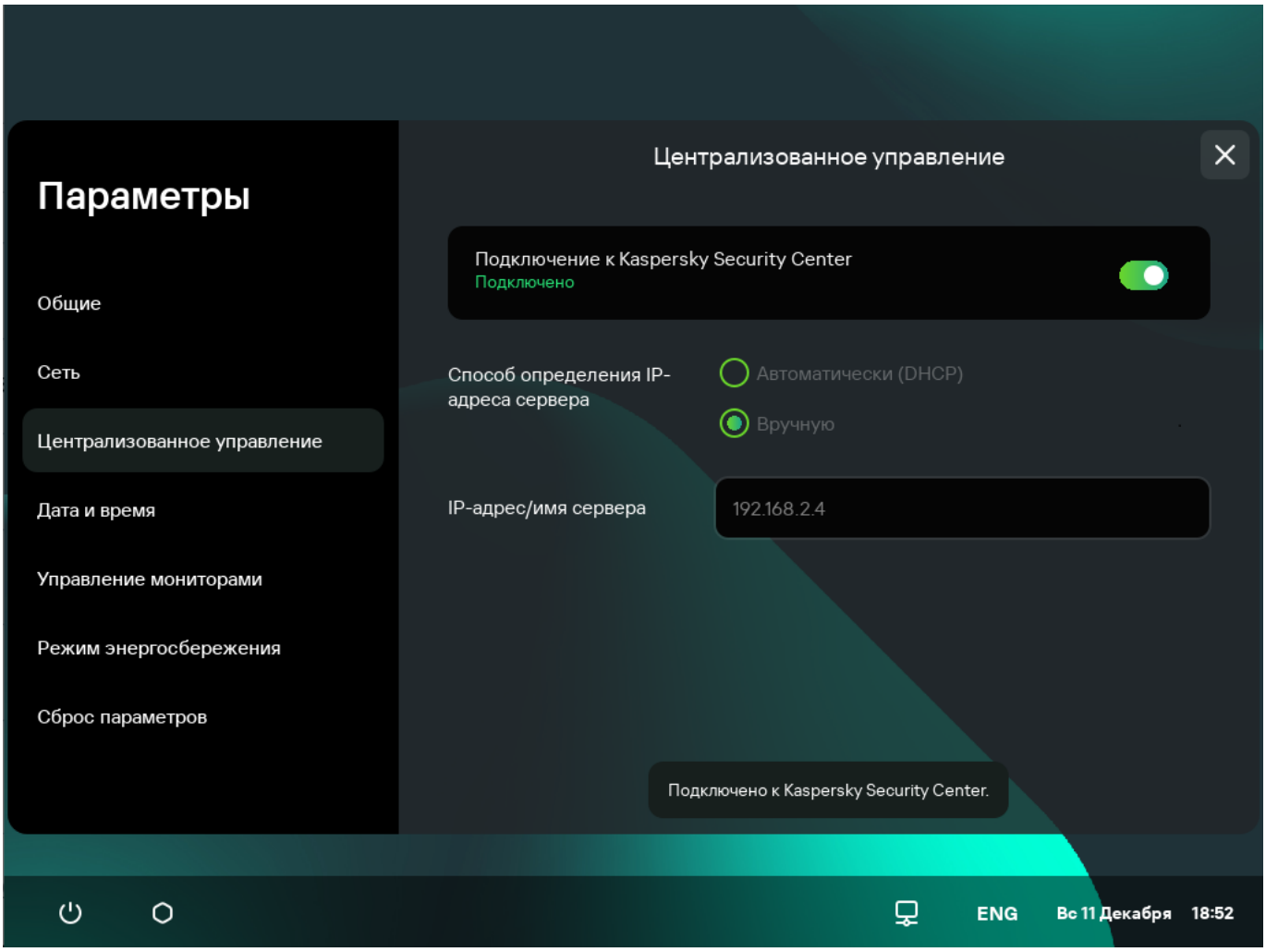
Для управления тонким клиентом через Web Console требуется настроить параметры подключения Kaspersky Thin Client к Серверу администрирования Kaspersky Security Center.

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.

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.

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 Kaspersky Thin Client входит в группу администрирования и управляется централизовано через Web Console, изменение параметров подключения Kaspersky Thin Client к Kaspersky Security Center недоступно.

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**.

Управление сертификатами Kaspersky Thin Client

Криптографический протокол TLS обеспечивает безопасность передачи данных 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.

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

В Kaspersky Thin Client используются следующие сертификаты:

- Сертификат для подключения Kaspersky Thin Client к Kaspersky Security Center.
- Сертификат для проверки подлинности RDP-сервера при подключении к удаленному рабочему столу.
- Сертификат для проверки подлинности брокера соединения при подключении к удаленному рабочему столу под управлением Базис.WorkPlace.
- Сертификат для подключения к серверу журналирования.

Рекомендуется обновлять 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 использует мобильный сертификат для подключения к Kaspersky Security Center. Мобильный сертификат создается автоматически при установке Kaspersky Security Center. Подробную информацию о том, как перевыпустить мобильный сертификат см. в разделе *Перевыпуск сертификата Веб-сервера* в онлайн-справке Kaspersky Security Center.

Для безопасного подключения Kaspersky Thin Client к удаленному рабочему столу по протоколу RDP или к брокеру соединения с удаленными рабочими столами под управлением Базис.WorkPlace, а также к серверу журналирования требуется добавить соответствующий сертификат безопасности. Все добавленные сертификаты сохраняются в системном хранилище Kaspersky Thin Client.

Для Kaspersky Thin Client, который не входит в группу администрирования и не управляется из Kaspersky Security Center Web Console, вы можете добавить сертификат в интерфейсе Kaspersky Thin Client самостоятельно в следующих случаях:

- при первом подключении Kaspersky Thin Client к Kaspersky Security Center;
- при первом подключении к удаленному рабочему столу по протоколу RDP или под управлением Базис.WorkPlace;

- при первом подключении к серверу журналирования.

Для Kaspersky Thin Client, который добавлен в группу администрирования и управляется из Kaspersky Security Center Web Console, администратор Kaspersky Security Center добавляет сертификаты через интерфейс Kaspersky Security Center Web Console. В этом случае вы сможете подключаться только к тем серверам, для которых администратор добавил сертификат. Если добавленный в политике сертификат является корневым (root), то подключение осуществляется только по доменному имени сервера.

При замене администратором Kaspersky Security Center сертификата для подключения к Kaspersky Security Center в некоторых случаях может потребоваться подтверждение замены сертификата для подключения к Kaspersky Security Center. 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 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.

Настройка параметров подключения к удаленному рабочему столу по протоколу RDP

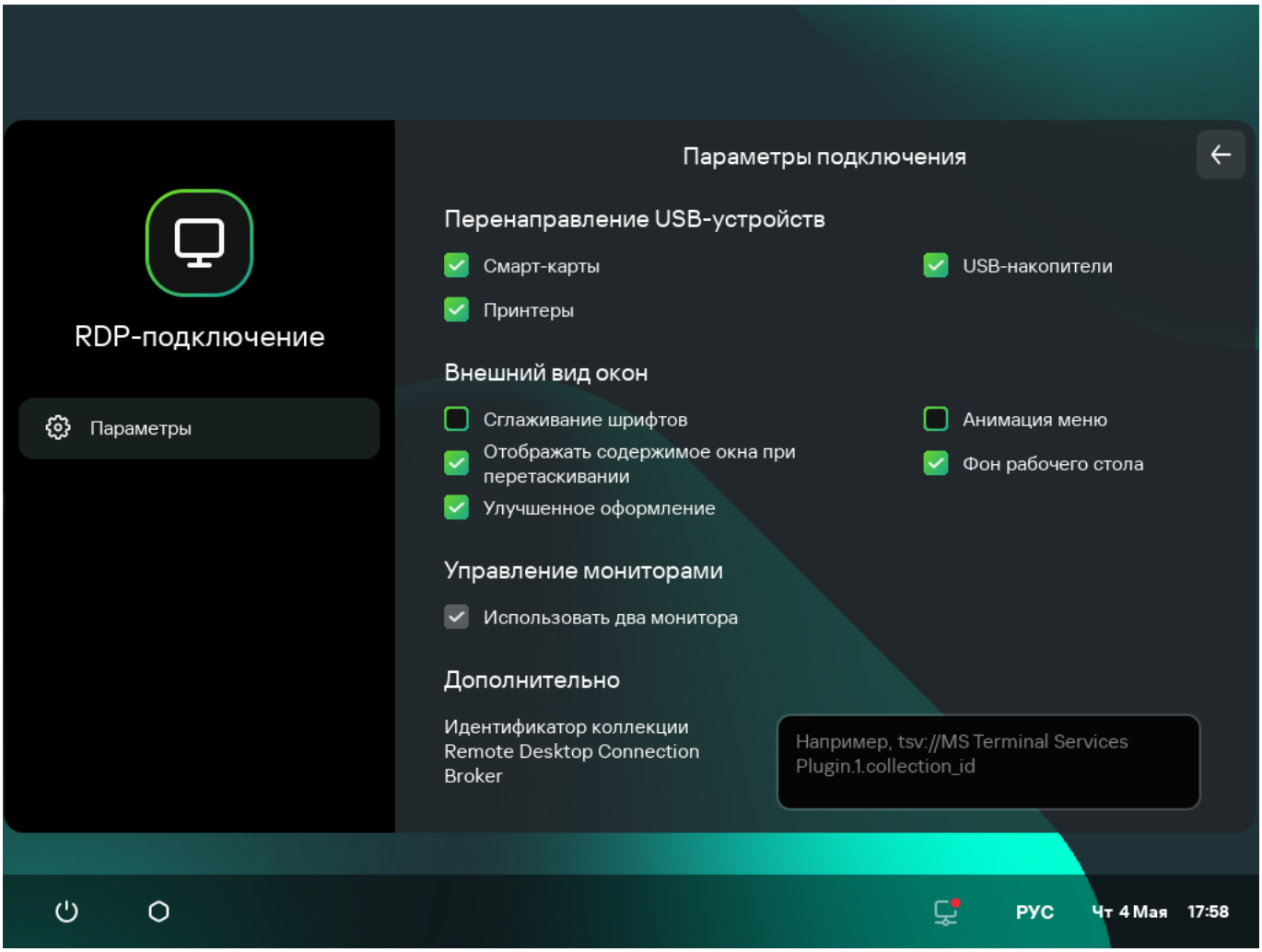
Kaspersky Thin Client позволяет настроить перенаправление USB-устройств на удаленный рабочий стол, а также параметры подключения к удаленному рабочему столу по протоколу RDP.

Для корректного перенаправления USB-устройств на удаленный рабочий стол в операционной системе Microsoft Windows 10 требуется включить службу 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 пользовательских сеансов в службе Remote Desktop Services. Перенаправление смарт-карт, флеш-накопителей и токенов на удаленный рабочий стол под управлением операционной системы Microsoft Windows 7 не поддерживается.

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

1. В главном окне Kaspersky Thin Client нажмите на кнопку **RDP**.
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 по протоколу RDP

3. В блоке параметров **Перенаправление USB-устройств** напротив подключенных через USB к тонкому клиенту устройств, которые нужно пробрасывать на удаленный рабочий стол, 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.

     По умолчанию все флажки сняты.

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 для подключения к удаленному рабочему столу вы хотите использовать брокер подключений 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.

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

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

Настройка параметров подключения к удаленным рабочим столам Базис.WorkPlace

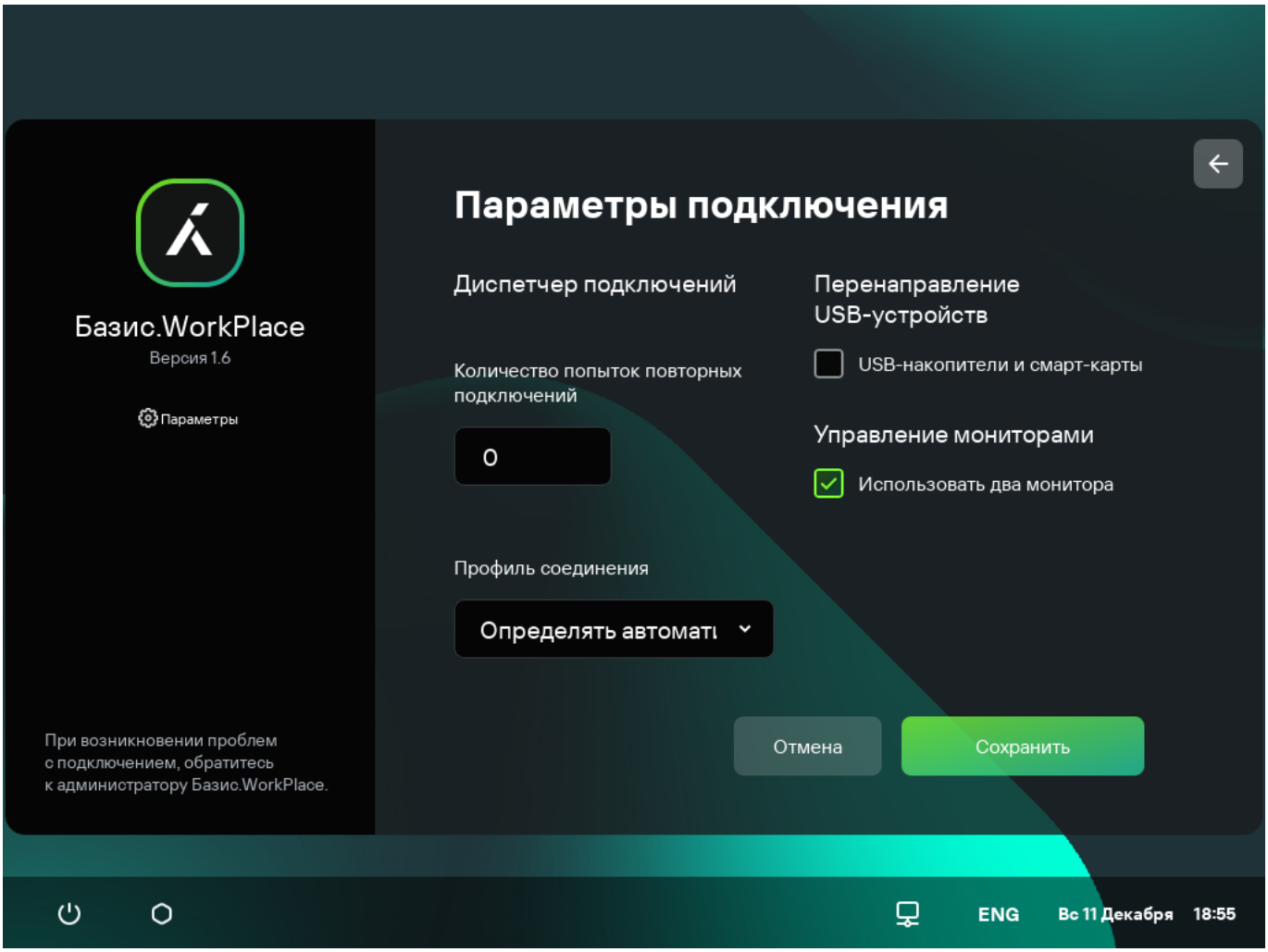
Kaspersky Thin Client позволяет настроить параметры подключения к удаленным рабочим столам под управлением Базис.WorkPlace.

Чтобы настроить параметры подключения к удаленным рабочим столам под управлением 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 USB-устройств на удаленный рабочий стол, в блоке **Перенаправление USB-устройств** установите или снимите флажок **USB-накопители и смарт-карты**.

   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 подключений 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 подключений Базис.WorkPlace. Тип соединения зависит от скорости соединения. Для выбора доступны следующие значения:

   - **Определять автоматически**.
   - **Модем**.
   - **Низкоскоростное широкополосное подключение**.
   - **Спутник**.
   - **Высокоскоростное широкополосное подключение**.

- **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.

Управление режимом энергосбережения

Режим энергосбережения – режим пониженного потребления электроэнергии. В этом режиме Kaspersky Thin Client продолжает работать в стандартном режиме с сохранением активного подключения к удаленному рабочему столу.

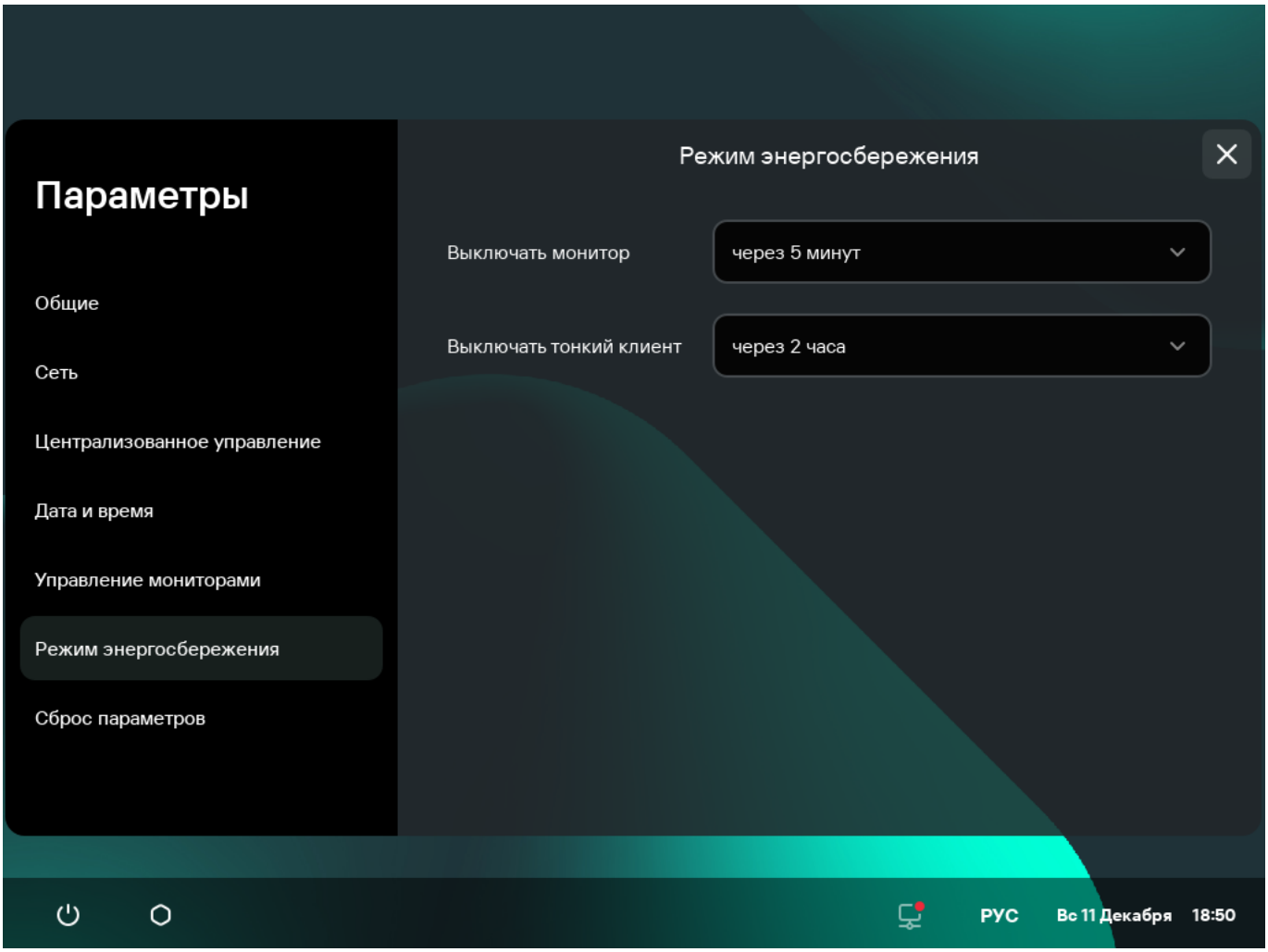
> Если Kaspersky Thin Client входит в группу администрирования и управляется централизовано через Web Console, а также включена функция **Принудительно,** управление режимом энергосбережения недоступно в интерфейсе Kaspersky Thin Client.

Вы можете настроить время перехода в режим энергосбережения для 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 режим энергосбережения:

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

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



Параметры. Раздел Режим энергосбережения

3. В раскрывающемся списке **Выключать монитор** выберите время бездействия системы, по истечении которого монитор будет переведен в режим энергосбережения.

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

Также вы можете настроить режим 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.

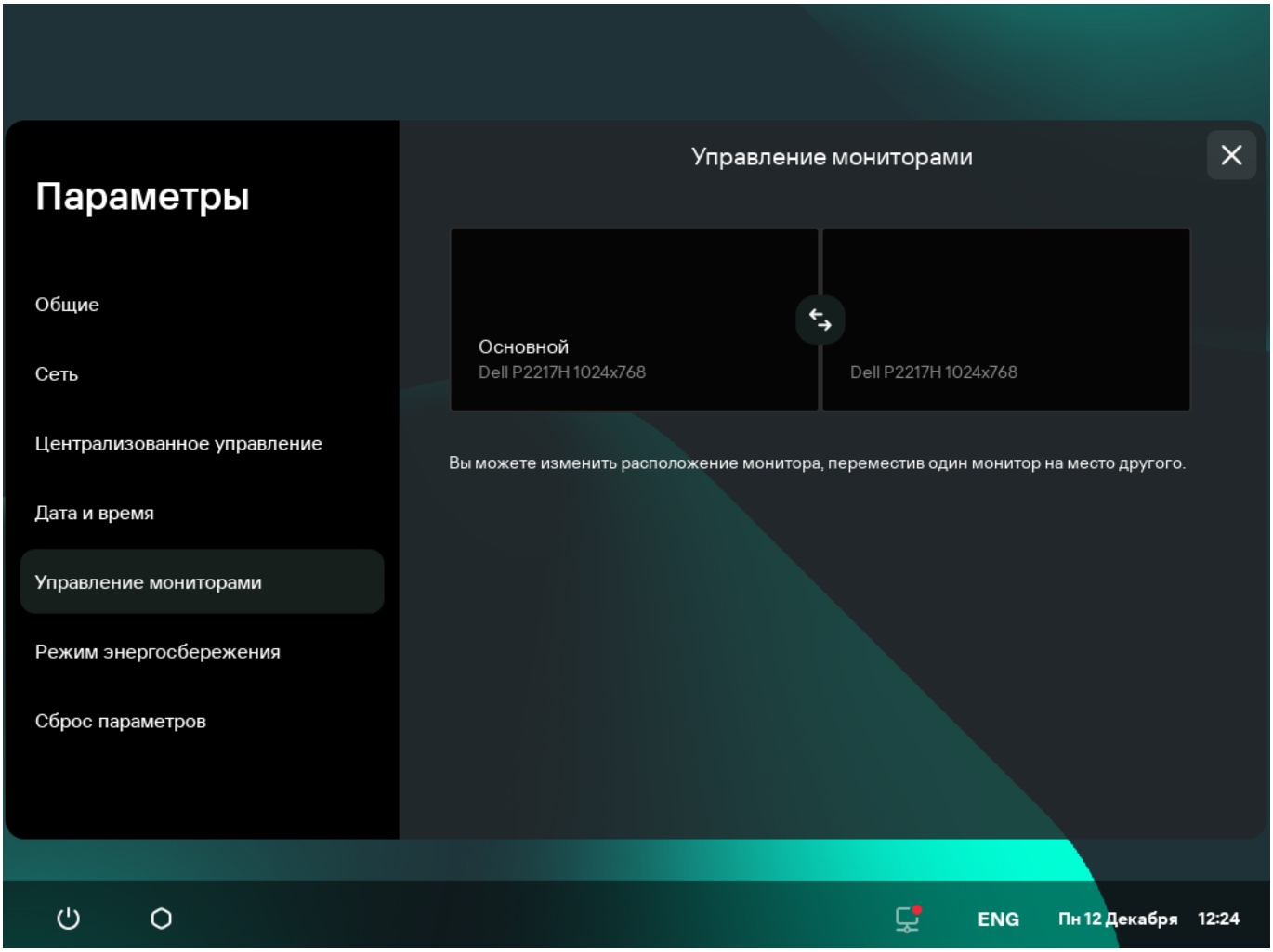
Предварительно требуется включить использование двух мониторов в параметрах подключения к удаленному рабочему столу по протоколу RDP или под управлением Базис.WorkPlace.

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 параметров в интерфейсе Kaspersky Thin Client, которые настраиваются однократно и в дальнейшем не используются в ключевых сценариях работы тонкого клиента.

Kaspersky Thin Client позволяет одновременно скрыть следующие параметры системы:

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

- Дата и время.
- Управление режимом энергосбережения.
- Настройка расположения мониторов.
- Сброс параметров Kaspersky Thin Client.

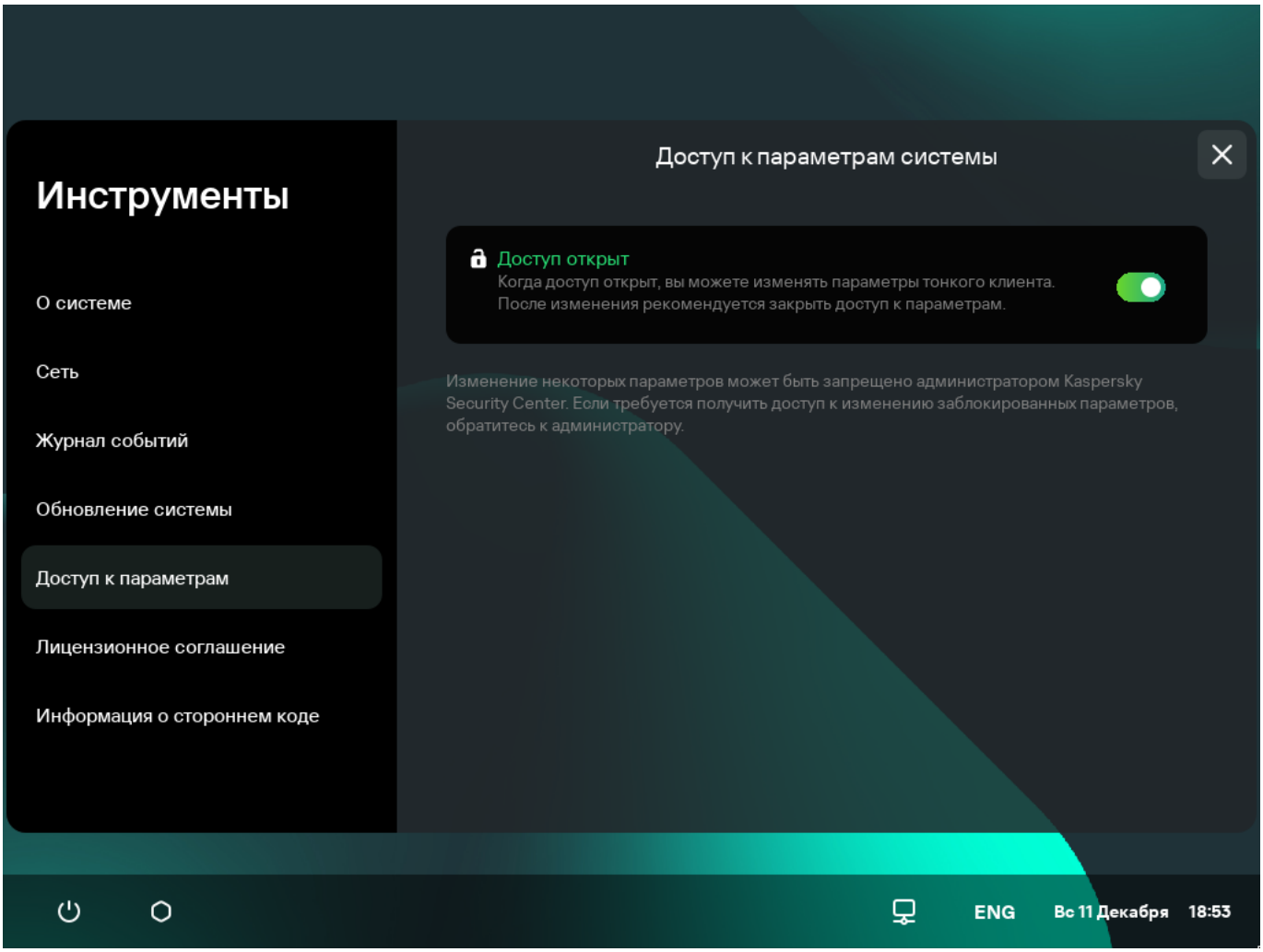
Если Kaspersky Thin Client входит в группу администрирования и управляется централизовано через Web Console, перечисленные выше параметры скрыты в интерфейсе Kaspersky Thin Client.

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**.

     Параметры будут скрыты.
   - 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

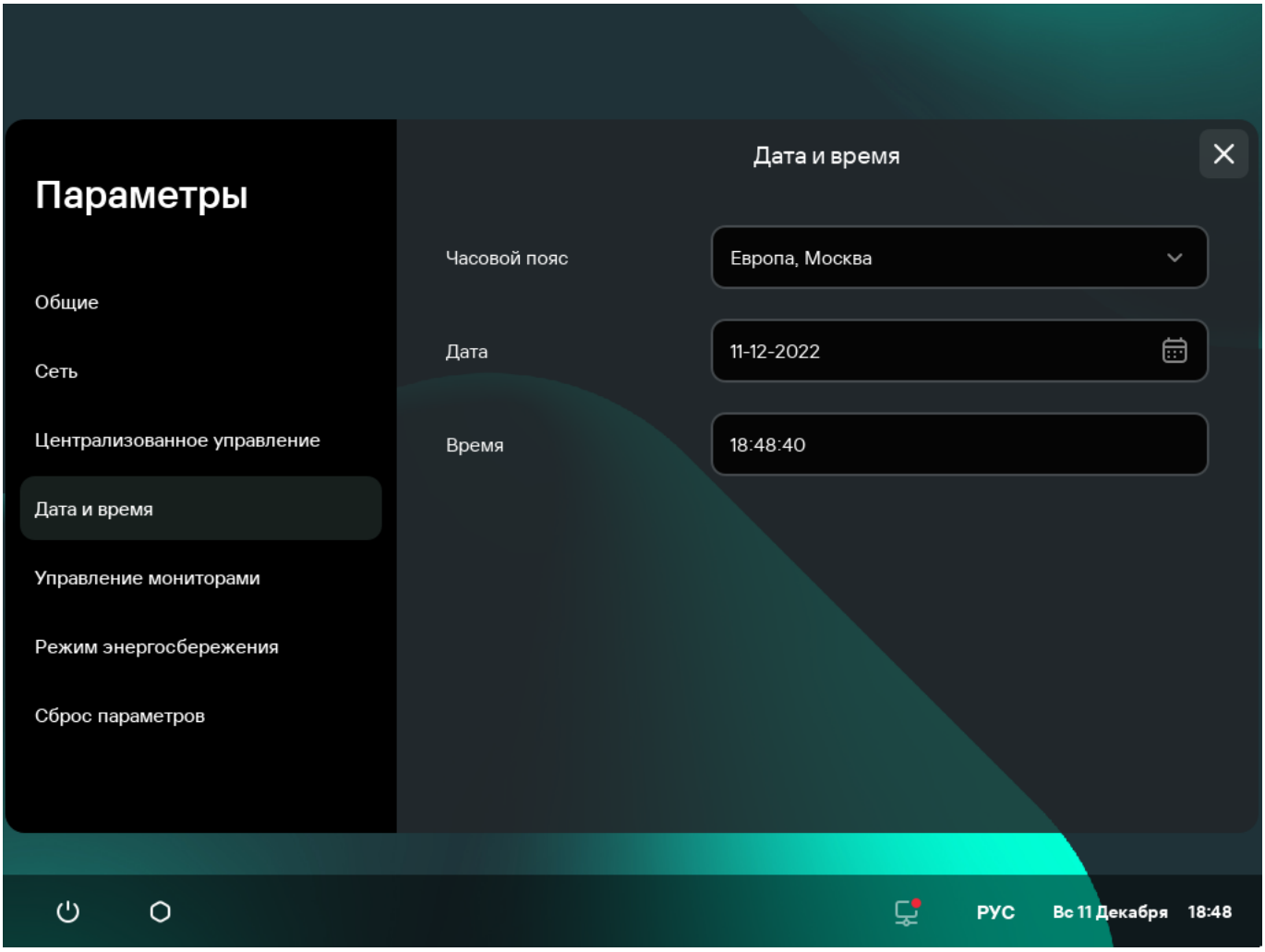
Настройка даты и времени

Kaspersky Thin Client, 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.

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.

   - Нажмите на поле **Дата** и в открывшейся форме с помощью мыши или клавиатуры выберите дату. Для перемещения между датами в календаре с помощью клавиатуры используйте следующие клавиши:

     - **TAB** – позволяет переместиться в календаре на один месяц вперед.

     - **SHIFT+TAB** – позволяет переместиться в календаре на один месяц назад.

- Стрелка вправо (→) – позволяет переместиться в календаре на один день вперед.
- Стрелка влево (←) – позволяет переместиться в календаре на один день назад.

- В поле **Время** введите текущее время в формате `ЧЧ:MM:CC`.

  Если Kaspersky Thin Client входит в группу администрирования и управляется централизовано через Web Console, поля **Дата** и **Время** недоступны для изменения.

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

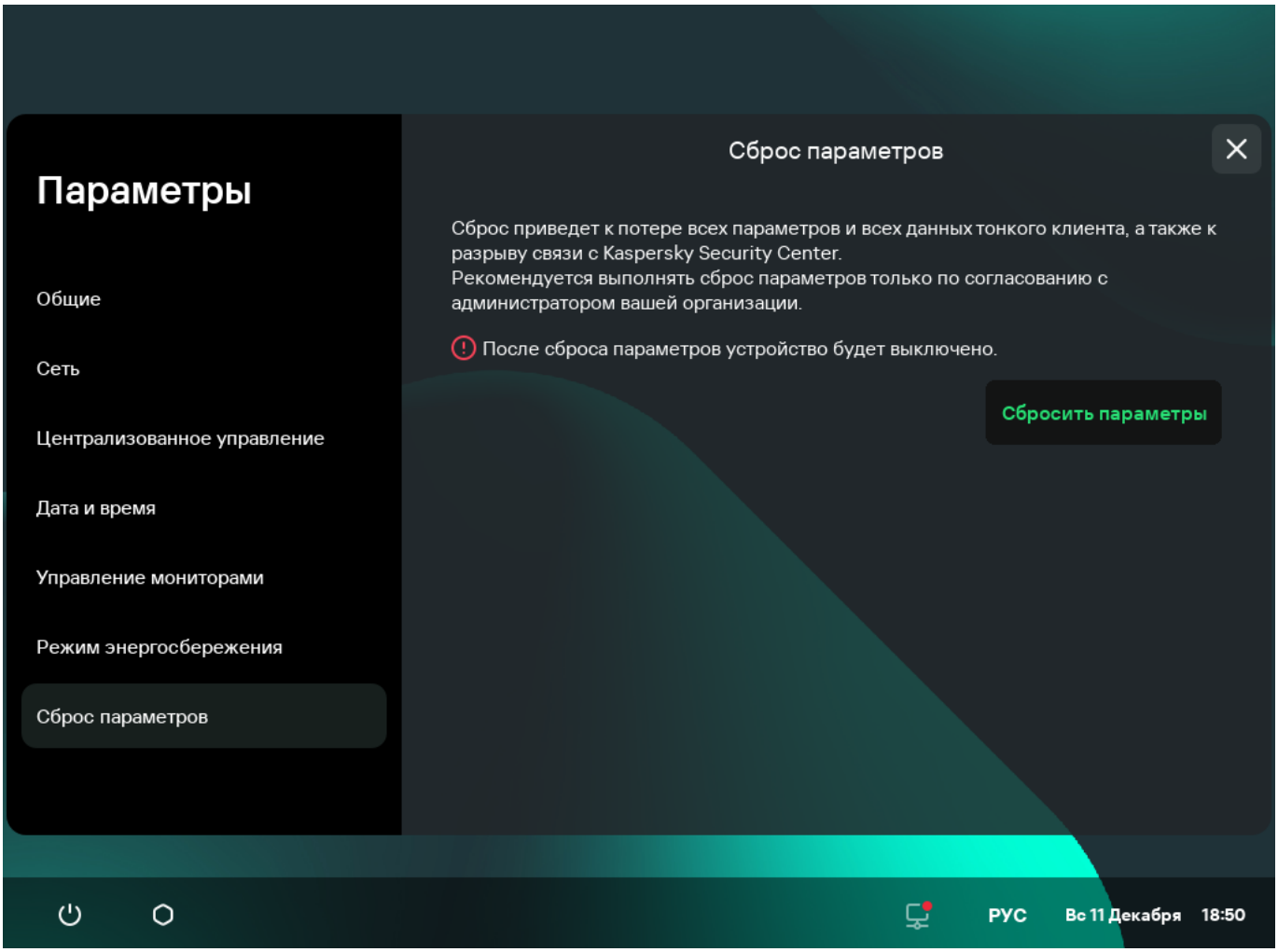
Сброс параметров Kaspersky Thin Client

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.

Чтобы выполнить сброс параметров 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 **Сброс параметров** (см. рис. ниже).



Параметры. 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.

Работа с Kaspersky Thin Client

Основной сценарий работы с Kaspersky Thin Client предполагает подготовку системы к запуску, включение системы и подключение к удаленному рабочему столу. По завершении работы с удаленным рабочим столом предполагается завершение сеанса подключения и выключение системы. Все остальное время вы проводите в привычном для себя программном окружении и непосредственное взаимодействие с интерфейсом Kaspersky Thin Client не требуется.

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

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

   Подключите к устройству монитор, клавиатуру, мышь перед первым включением. При необходимости вы можете также подключить USB-накопители и/или USB-токены.

2. **Запуск Kaspersky Thin Client**

   Включите тонкий клиент для начала работы.

3. **Подключение к удаленному рабочему столу**

   Подключитесь к удаленному рабочему столу 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 сеанса подключения**

   Завершите сеанс подключения к удаленному рабочему столу по завершении работы.

6. **Остановка Kaspersky Thin Client**

   Выключите тонкий клиент в конце рабочего дня.

Подключение к удаленному рабочему столу

Kaspersky Thin Client позволяет выбрать подключение к удаленному рабочему столу по протоколу RDP напрямую или подключение к удаленным рабочим столам под управлением Базис.WorkPlace. В зависимости от инфраструктуры в вашей организации вы можете выбрать один из следующих вариантов:

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

Существуют следующие особенности, которые нужно учитывать при подключении к удаленному рабочему столу по протоколу RDP:

- При подключении к удаленному рабочему столу под управлением операционной системы Astra Linux (CE или SE), использующей реализацию протокола xRDP, пользовательский пароль, срок действия которого закончился, принимается, но подключение не происходит. Схожая ситуация возникает при вводе некорректного имени пользователя. Также при таком подключении отсутствует механизм изменения пароля.

- Невозможно подключиться к удаленному рабочему столу под управлением операционной системы семейства Microsoft Windows с включенной проверкой подлинности сетевого уровня (NLA), если срок действия пароля закончился. Также невозможно самостоятельно сменить пароль при таком подключении.

  Для решения таких проблем рекомендуется обратиться к администратору вашей организации.

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 подключения укажите параметры подключения к удаленному рабочему столу:

   a. В поле **Сервер** укажите IP-адрес или имя RDP-сервера, к которому вы хотите подключиться.

   > Если в инфраструктуре вашей организации развернута система контроля доступа привилегированных пользователей Wallix Bastion, вы можете подключаться к удаленным рабочим столам, через эту систему, указав ее IP-адрес или имя сервера в поле **Сервер**.

   Kaspersky Thin Client сохраняет адрес последнего RDP-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. Если вы указываете доменное имя пользователя, название домена указывать не обязательно, но вы можете это сделать в формате `Домен\Имя пользователя`.

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

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

   Пароль пользователя сбрасывается каждый раз, когда вы выходите из окна подключения к удаленному рабочему столу.

4. 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 RDP-сервера, то подключение произойдет автоматически.

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

5. 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.

   Через несколько секунд на мониторе отобразится удаленный рабочий стол компьютера, к которому вы подключились по протоколу RDP.

Также вы можете настроить параметры подключения к рабочему столу по протоколу RDP, нажав **Параметры**.

- **Подключение к удаленному рабочему столу под управлением Базис.WorkPlace**

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.

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.

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 сбрасывается каждый раз, когда вы выходите из окна подключения к рабочим столам под управлением Базис.WorkPlace.

      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 соединения Базис.WorkPlace, то подключение к удаленному рабочему столу под управлением Базис.WorkPlace произойдет автоматически.

Сертификат для проверки подлинности брокера соединения 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**.

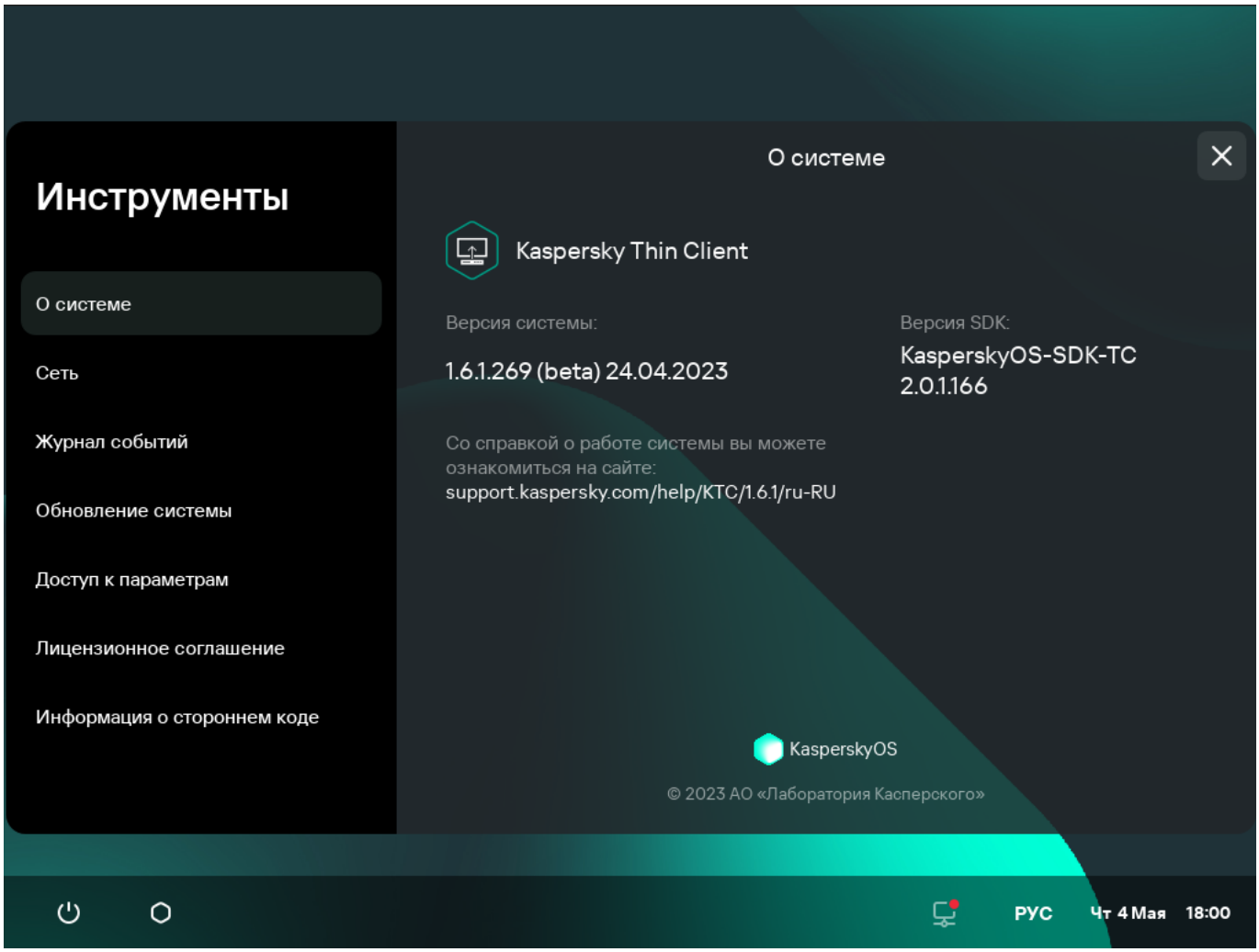
При подключении к удаленному рабочему столу Kaspersky Thin Client использует шифрование по протоколу TLS для защиты сеанса подключения, а также защиты данных от перехвата или подделки.

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**

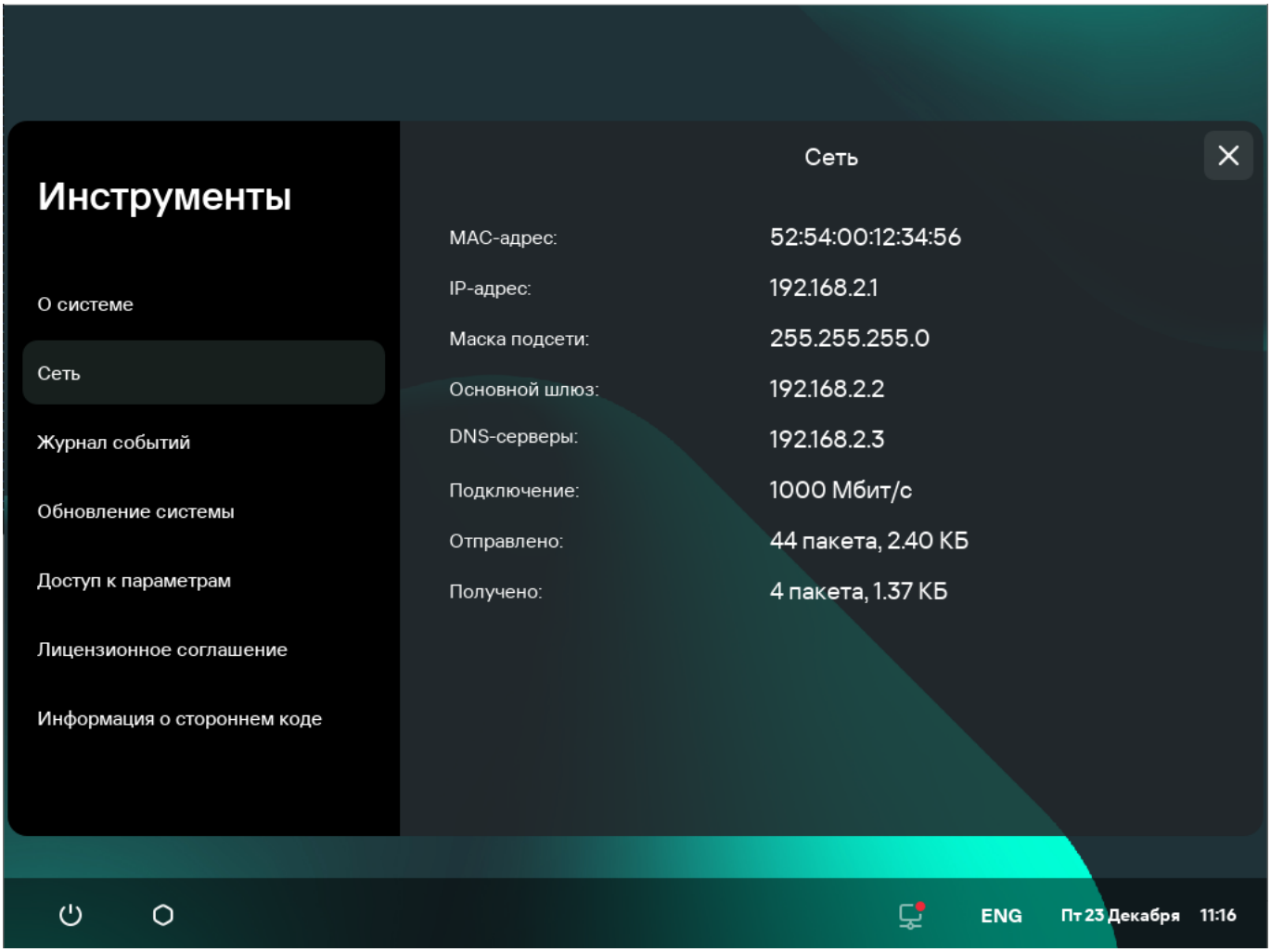
Просмотр информации о состоянии сети

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**

Работа с журналами Kaspersky Thin Client

Этот раздел содержит информацию о работе с журналами Kaspersky Thin Client.

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 событий и аудита

Вы можете просматривать журнал событий Kaspersky Thin Client через интерфейс Kaspersky Thin Client в разделе **Инструменты → Журнал событий**. Также вы можете отправить журнал событий на сервер журналирования. Вместе с журналом событий на сервер автоматически отправляется журнал аудита.

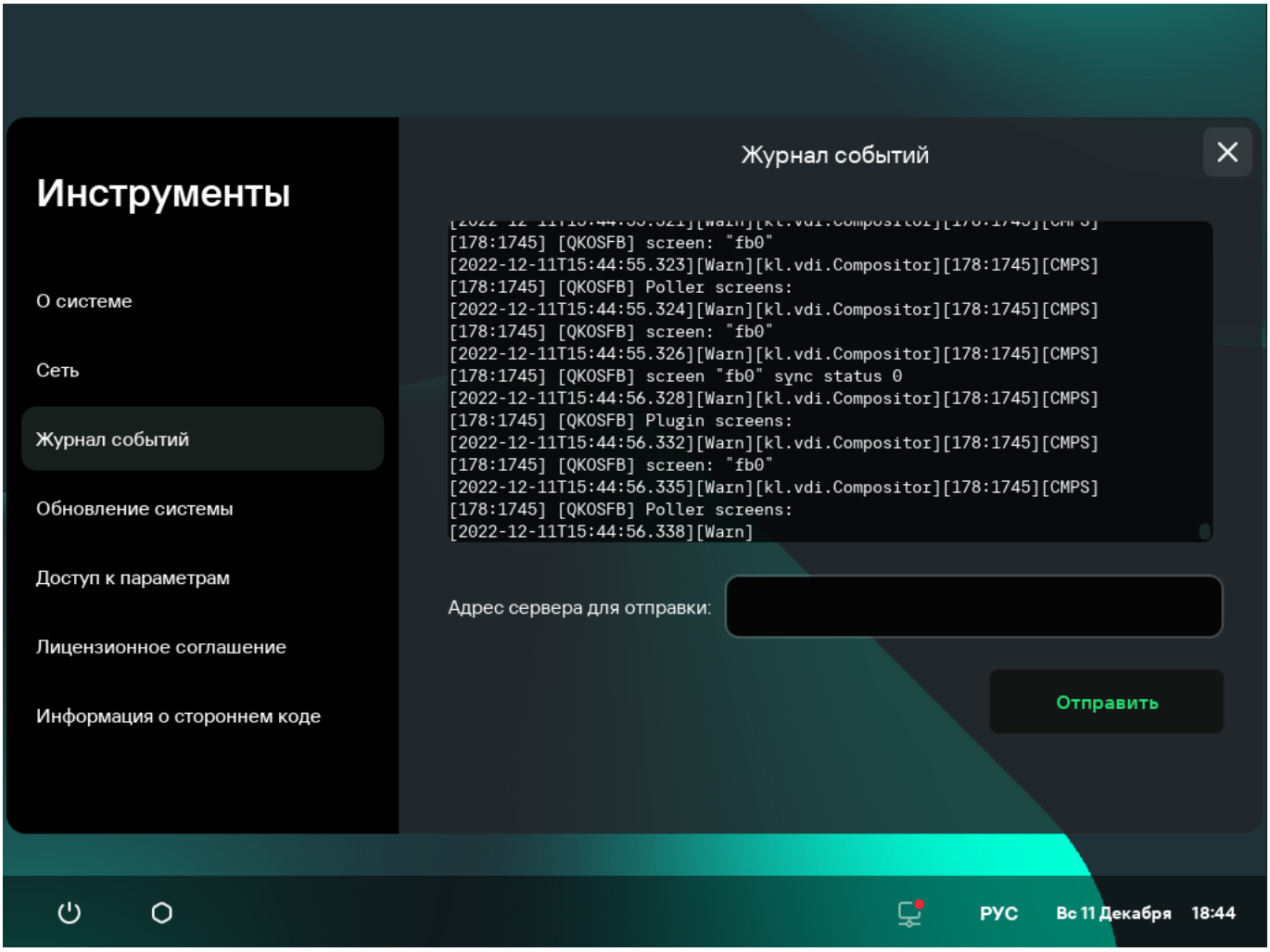
Для отправки журнала событий и журнала аудита Kaspersky Thin Client на сервер требуется предварительно развернуть сервер журналирования в инфраструктуре вашей организации. Подробную информацию о развертывании сервера см. в руководстве администратора к этому серверу.

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.

Обновление Kaspersky Thin Client

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

Kaspersky Thin Client не поддерживает обновление с версии 1.5/1.6 до версии 1.6.1 beta.

Доступные обновления загружаются на тонкий клиент с Сервера администрирования Kaspersky Security Center или с серверов обновлений "Лаборатории Касперского" только после того, как администратор Kaspersky Security Center подтвердил эти обновления в интерфейсе Web Console. Если для новой версии Kaspersky Thin Client было сформировано новое Лицензионное соглашение, администратор Kaspersky Security Center принимает его в интерфейсе Kaspersky Security Center Web Console. Подробную информацию о подтверждении обновлений администратором см. в разделе *Одобрение и отклонение обновлений программного обеспечения* в онлайн-справке Kaspersky Security Center. Дополнительно администратор Kaspersky Security Center может настроить регулярную проверку обновлений Kaspersky Thin Client (подробнее см. в разделе *Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского"* в онлайн-справке 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**.

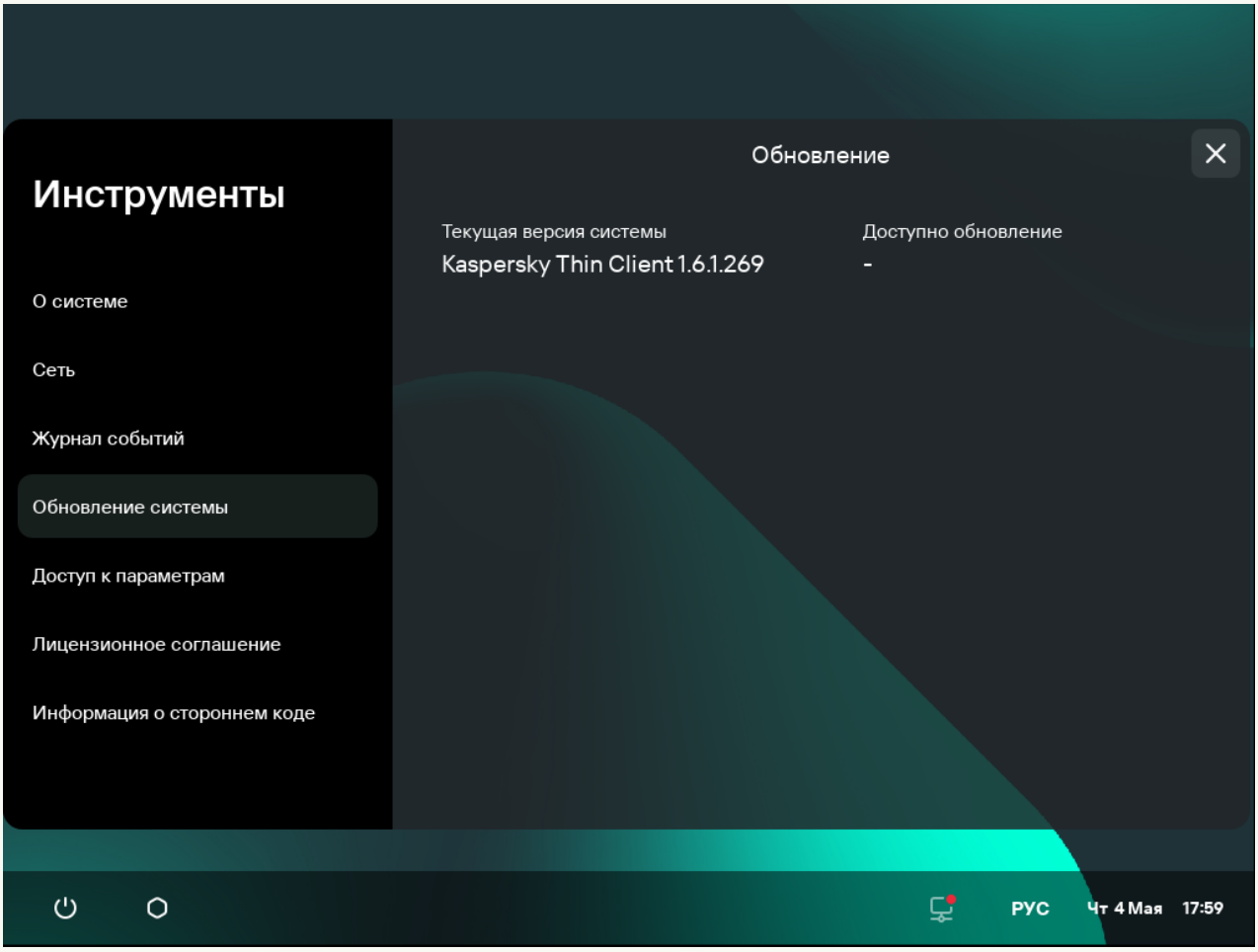
       Обновления будут установлены и Kaspersky Thin Client выключится.

- **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.

Завершение сессии подключения

Чтобы завершить сессию подключения к удаленному рабочему столу:

1. Нажмите на панель подключения Kaspersky Thin Client в центре верхней части удаленного рабочего стола.

2. В раскрывшейся панели подключения нажмите на кнопку **Завершить сессию**.

В результате сессия подключения к рабочему столу будет завершена и на мониторе отобразится окно подключения к удаленному рабочему столу.

Если администратор Базис.WorkPlace установил время бездействия Kaspersky Thin Client, по окончании которого завершается сессия подключения к удаленному рабочему столу под управлением Базис.WorkPlace, то по истечении периода бездействия подключение будет завершено автоматически.

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 при подключении к удаленному рабочему столу. В таблице ниже приведены все доступные специальные клавиши и сочетания клавиш.

Специальные клавиши и сочетания клавиш Kaspersky Thin Client

Клавиши и сочетания клавиш	Действие	Область применения
`Win`	Открыть или закрыть меню завершения работы.	Любое окно интерфейса Kaspersky Thin Client, в котором отображается панель управления.
→ ←	Переключиться между доступными вариантами подключения к удаленному рабочему столу: **RDP**, **Базис.Workplace**.	Главное окно Kaspersky Thin Client.
↑ ↓	• Переключиться между элементами раскрывающегося списка. • Прокрутить содержимое страницы вверх или вниз.	Любое окно интерфейса Kaspersky Thin Client, которое содержит поле с раскрывающимся списком или содержимое которого больше размера окна и есть возможность прокрутки.
`Tab`	Переключиться между следующими элементами: • варианты подключения к удаленному рабочему столу: **RDP**, **Базис.Workplace**; • последовательность полей, например, в окне **Параметры**. Вы можете переключаться между элементами в направлении *слева направо* и *сверху вниз*.	• Главное окно Kaspersky Thin Client. • Любое окно интерфейса Kaspersky Thin Client, содержащее несколько полей. При переключении элементы, недоступные для взаимодействия (например, поле, которое заблокировано для редактирования), а также неактивные элементы пропускаются.
`Shift+Tab`	Переключиться между следующими элементами: • варианты подключения к	• Главное окно Kaspersky Thin Client. • Любое окно интерфейса Kaspersky Thin Client, содержащее несколько полей.

	удаленному рабочему столу: **RDP**, **Базис.Workplace**; • последовательность полей, например, в окне **Параметры**. Вы можете переключаться между элементами в направлении *справа налево* и *снизу вверх*.	При переключении элементы, недоступные для взаимодействия (например, поле, которое заблокировано для редактирования), а также неактивные элементы пропускаются.
Space или **Enter**	Нажать на кнопку.	Кнопка.
Space или **Enter**	Открыть или закрыть раскрывающийся список.	Раскрывающийся список. При переключении элементы списка, недоступные для взаимодействия, а также неактивные элементы пропускаются.
Esc	Закрыть окно.	Любое окно, которое можно закрыть.
Esc	Свернуть панель подключения.	Во время подключения к удаленному рабочему столу при наведении курсора мыши на панель подключения.
Alt+Shift	Сменить язык раскладки клавиатуры.	Любое окно интерфейса Kaspersky Thin Client.
Alt+Page down	Переместиться в следующий раздел окна **Параметры** или **Инструменты**.	Окно **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.
Alt+Page up	Переместиться в предыдущий раздел окна **Параметры** или **Инструменты**.	Окно **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 восстановить панель	Во время подключения к удаленному рабочему столу.

	подключения.	
Ctrl+D	Завершить подключение к удаленному рабочему столу.	Во время подключения к удаленному столу при наведении курсора мыши на панель подключения.
Win+I	Открыть **Параметры**, если доступ к параметрам открыт.	Любое окно интерфейса Kaspersky Thin Client.
Win+U	Открыть **Инструменты**.	Любое окно интерфейса Kaspersky Thin Client.
Win+Esc	Выключить Kaspersky Thin Client.	Любое окно интерфейса Kaspersky Thin Client.
Win+F12 или **Win+End**	Перезагрузить Kaspersky Thin Client.	Любое окно интерфейса Kaspersky Thin Client.

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 входит в состав комплекта поставки Kaspersky Thin Client и обеспечивает взаимодействие Kaspersky Thin Client с Kaspersky Security Center.

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

Веб-плагин управления Kaspersky Security Management Suite по умолчанию не установлен в Web Console. Веб-плагин входит в комплект поставки Kaspersky Thin Client и его требуется установить на компьютер с установленной программой Kaspersky Security Center Web Console. 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, вы можете разграничить доступ к функция 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*.

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

Чтобы установить веб-плагин в Web Console:

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

   Отобразится список доступных плагинов управления Web Console.

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

3. В открывшейся справа панели добавьте следующие файлы:

   - ZIP-архив с дистрибутивом веб-плагина (plugin.zip), полученный в комплекте поставки Kaspersky Thin Client, нажав на кнопку **Загрузить файл формата ZIP**;

   - файл подписи (signature.txt), полученный в комплекте поставки Kaspersky Thin Client, нажав на кнопку **Загрузить подпись**.

4. Нажмите на кнопку **Добавить**.

5. Внимательно ознакомьтесь с Лицензионным соглашением и примите его.

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

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

Обновление веб-плагина управления Kaspersky Security Management Suite

Обновить веб-плагин управления Kaspersky Security Management Suite можно только до более новой версии.

Предварительно требуется получить ZIP-архив с дистрибутивом новой версии веб-плагина и цифровую подпись архива у специалистов "Лаборатории Касперского".

Чтобы обновить веб-плагин в Web Console:

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

2. В отобразившемся списке плагинов Web Console найдите Kaspersky Security Management Suite и нажмите на него.

3. В открывшемся окне нажмите на кнопку **Обновить из файла**.

4. В открывшейся справа панели добавьте следующие файлы:

   - ZIP-архив с дистрибутивом плагина, нажав на кнопку **Загрузить файл формата ZIP**;

- файл цифровой подписи, нажав на кнопку **Загрузить подпись**.

5. Нажмите на кнопку **Обновление**.

6. Если для новой версии плагина было сформировано новое Лицензионное соглашение, внимательно ознакомьтесь с ним и примите новое Лицензионное соглашение.

7. 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.

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 Kaspersky Thin Client в группу управляемых устройств

При первом подключении Kaspersky Thin Client к Web Console требуется переместить его в группу управляемых устройств.

Чтобы добавить Kaspersky Thin Client 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**.

Kaspersky Thin Client будет добавлен в группу управляемых устройств Web Console.

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 флеш-накопители, вы можете активировать политику, блокирующую доступ к флеш-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 общих 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 общие параметры для одного устройства

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

2. Нажмите на имя устройства, на котором запущен Kaspersky Thin Client. Вы можете просмотреть имя устройства в панели управления в интерфейсе Kaspersky Thin Client. Если имя компьютера отсутствует в списке, добавьте его в группу **Управляемые устройства**. Также вы можете управлять устройствами, которые еще не добавлены в управляемые, в разделе **Обнаружение устройств и развертывание** → **Нераспределенные устройства**.

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

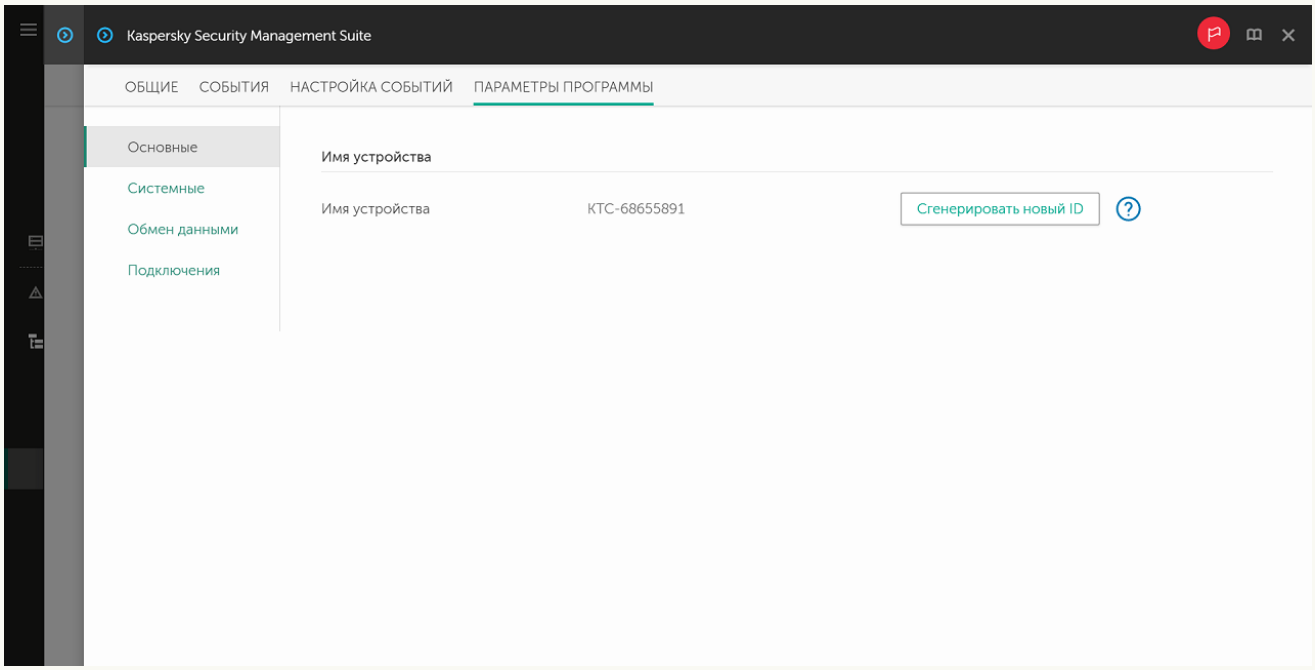
3. В открывшемся окне выберите вкладку **Программы**.

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.

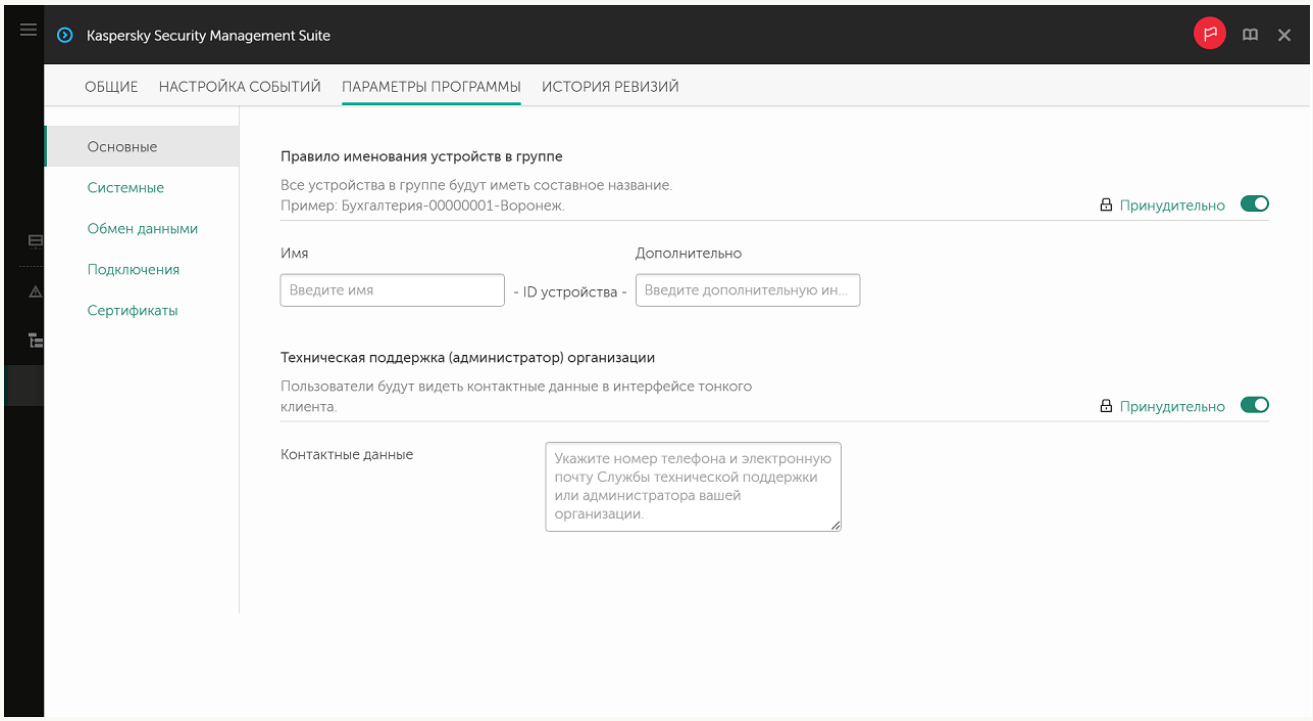
Как настроить общие параметры для группы устройств

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 параметров подключения к удаленному рабочему столу по протоколу RDP через Web Console

Вы можете настроить параметры подключения к удаленным рабочим столам по протоколу RDP для одного устройства или группы устройств с Kaspersky Thin Client через Web Console.

Как настроить параметры подключения к удаленным рабочим столам по протоколу RDP для одного устройства

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

2. Нажмите на имя устройства, на котором запущен Kaspersky Thin Client. Вы можете просмотреть имя устройства в панели управления в интерфейсе Kaspersky Thin Client. Если имя компьютера отсутствует в списке, добавьте его в группу **Управляемые устройства**. Также вы можете управлять устройствами, которые еще не добавлены в управляемые, в разделе **Обнаружение устройств и развертывание** → **Нераспределенные 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**.

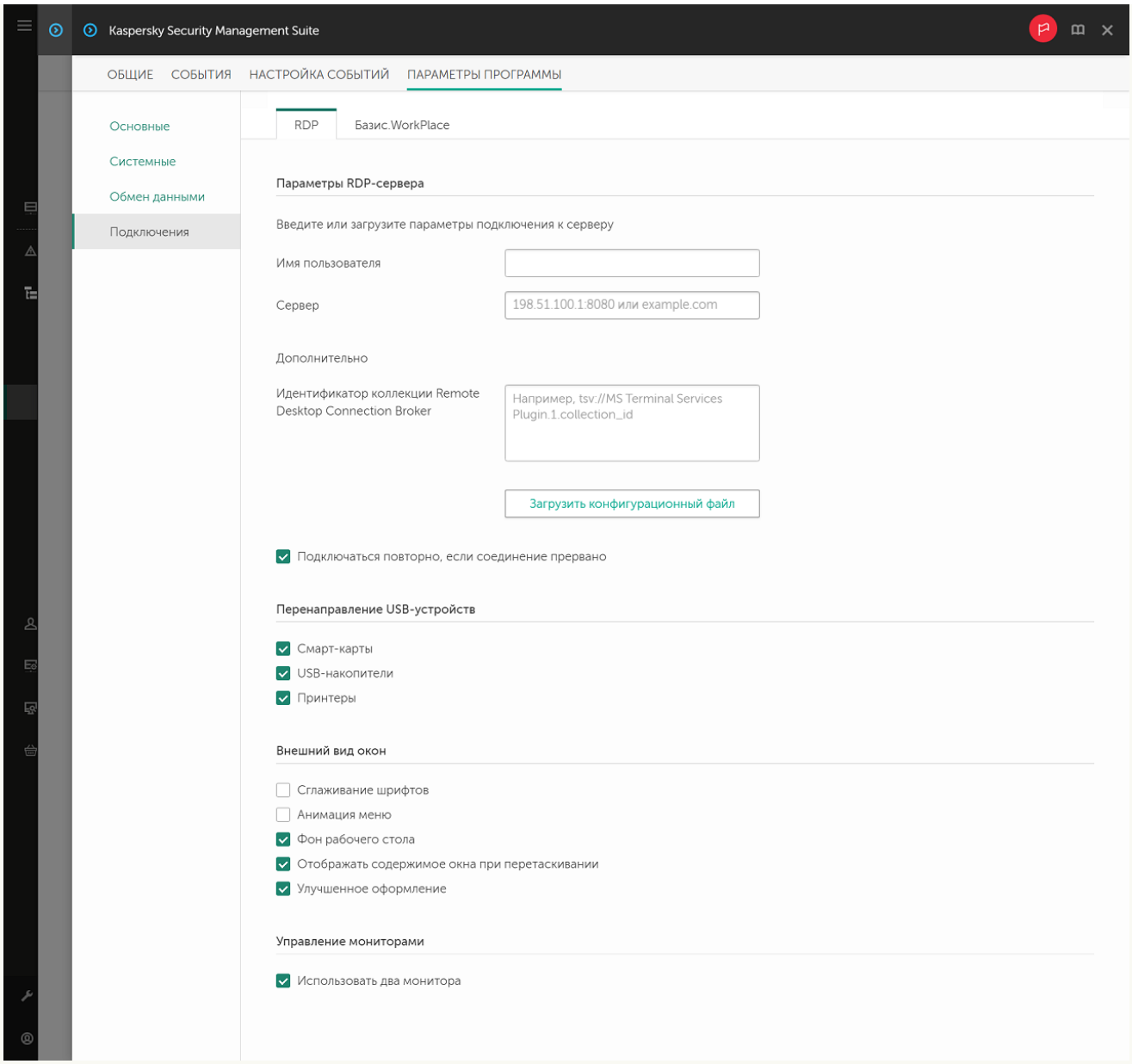
4. Нажмите на название веб-плагина управления Kaspersky Security Management Suite.

   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 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 для подключения к удаленному рабочему столу по протоколу RDP.

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

9. Если для подключения к удаленному рабочему столу вы хотите использовать брокер подключений 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.

   Если у вас есть конфигурационный файл с параметрами подключения к Microsoft Remote Desktop Connection Broker, загрузите его, нажав на кнопку **Загрузить конфигурационный файл**. При этом заполнять поле **Идентификатор коллекции Remote Desktop Connection Broker** не нужно.

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

11. В блоке параметров **Перенаправление USB-устройств** напротив подключенных через USB к тонкому клиенту устройств, которые нужно пробрасывать на удаленный рабочий стол, 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.

  По умолчанию все флажки сняты.

12. 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.

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

[Как настроить параметры подключения к удаленным рабочим столам по протоколу RDP для группы устройств]

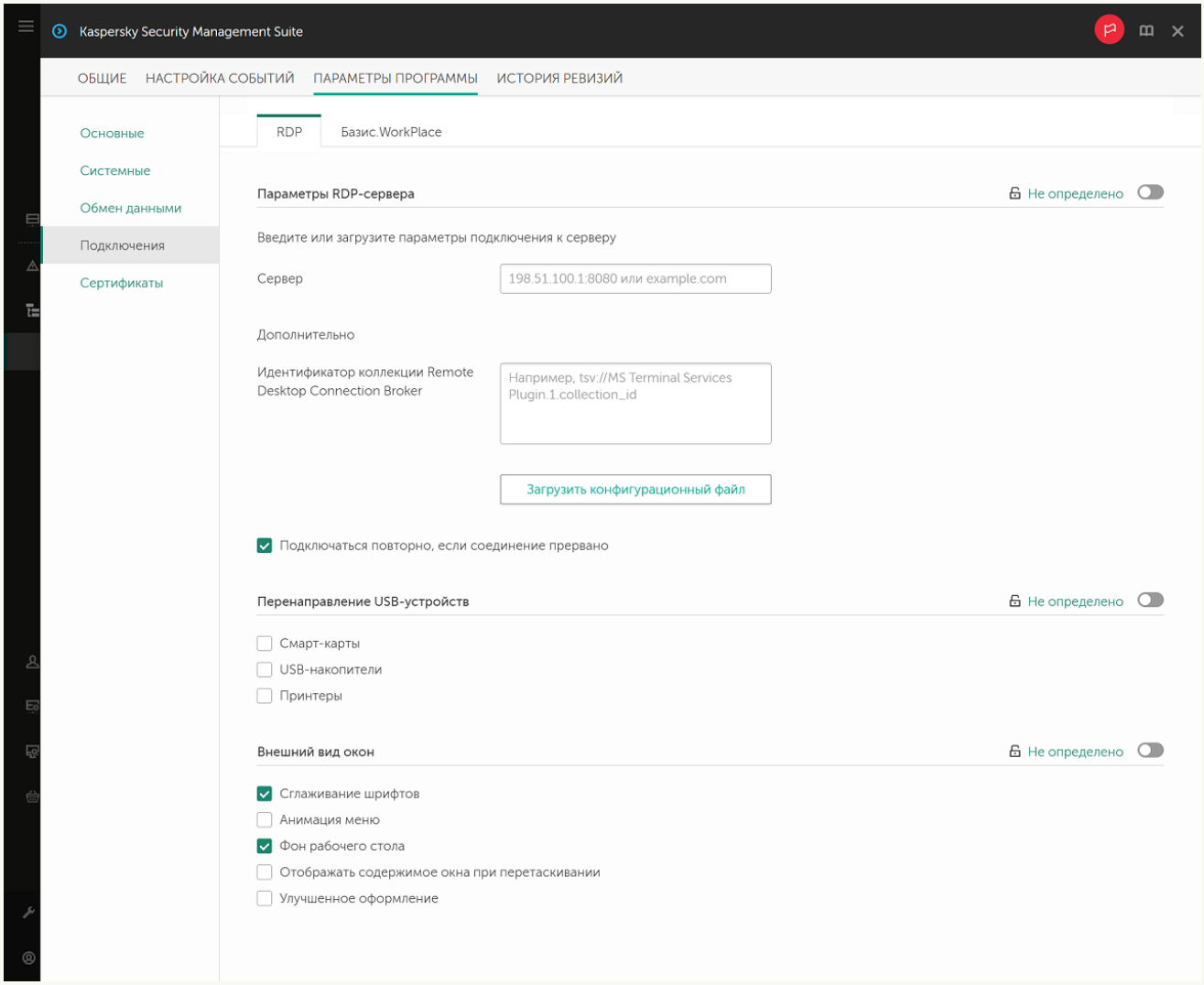
1. В главном окне Web Console выберите **Устройства** → **Политики и профили политик**.

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 вы хотите использовать брокер подключений 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.

   Если у вас есть конфигурационный файл с параметрами подключения к Microsoft Remote Desktop Connection Broker, загрузите его, нажав на кнопку **Загрузить конфигурационный файл**. При этом заполнять поле **Идентификатор коллекции Remote Desktop Connection Broker** не нужно.

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

9. В блоке параметров **Перенаправление USB-устройств** напротив подключенных через USB к тонкому клиенту устройств, которые нужно пробрасывать на удаленный рабочий стол, 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.

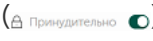
     По умолчанию все флажки сняты.

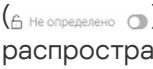
10. В блоке **Внешний вид окон** установите флажки напротив графических параметров удаленного рабочего стола, которые требуется использовать:

    - **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.

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

Если переключатель напротив названия группы параметров находится в положении **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** (

), 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 параметров подключения к удаленному рабочему столу под управлением Базис.WorkPlace через Web Console

Вы можете настроить параметры подключения к удаленному рабочему столу под управлением Базис.WorkPlace для одного устройства или группы устройств с Kaspersky Thin Client через Web Console.

Как настроить параметры подключения к удаленному рабочему столу под управлением Базис.WorkPlace для одного устройства

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

2. Нажмите на имя устройства, на котором запущен Kaspersky Thin Client. Вы можете просмотреть имя устройства в панели управления в интерфейсе Kaspersky Thin Client. Если имя компьютера отсутствует в списке, добавьте его в группу **Управляемые устройства**. Также вы можете управлять устройствами, которые еще не добавлены в управляемые, в разделе **Обнаружение устройств и развертывание** → **Нераспределенные 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**.

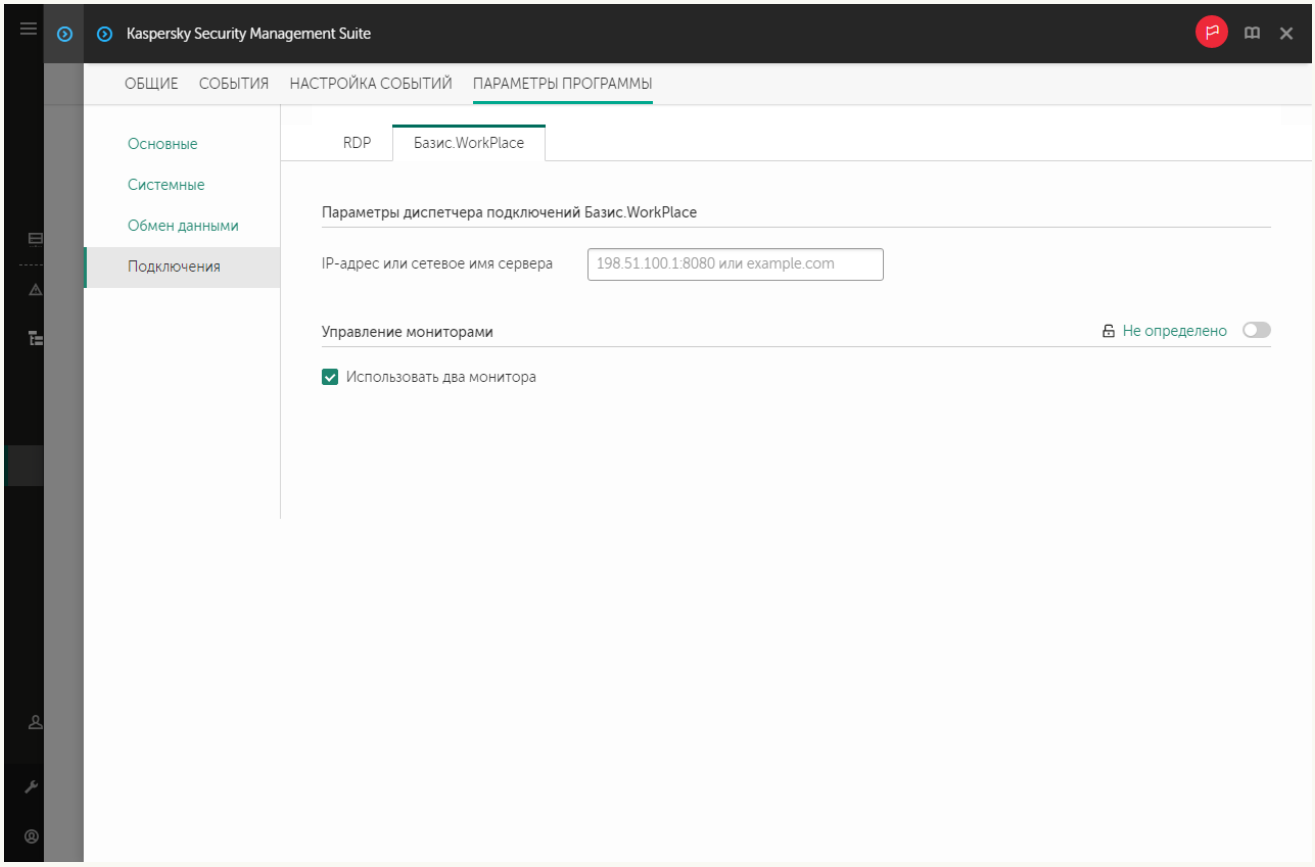
4. Нажмите на название веб-плагина управления Kaspersky Security Management Suite.

   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 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 одного устройства

7. В поле **IP-адрес или сетевое имя сервера** введите IP-адрес или имя сервера для подключения к удаленному рабочему столу под управлением Базис.WorkPlace.

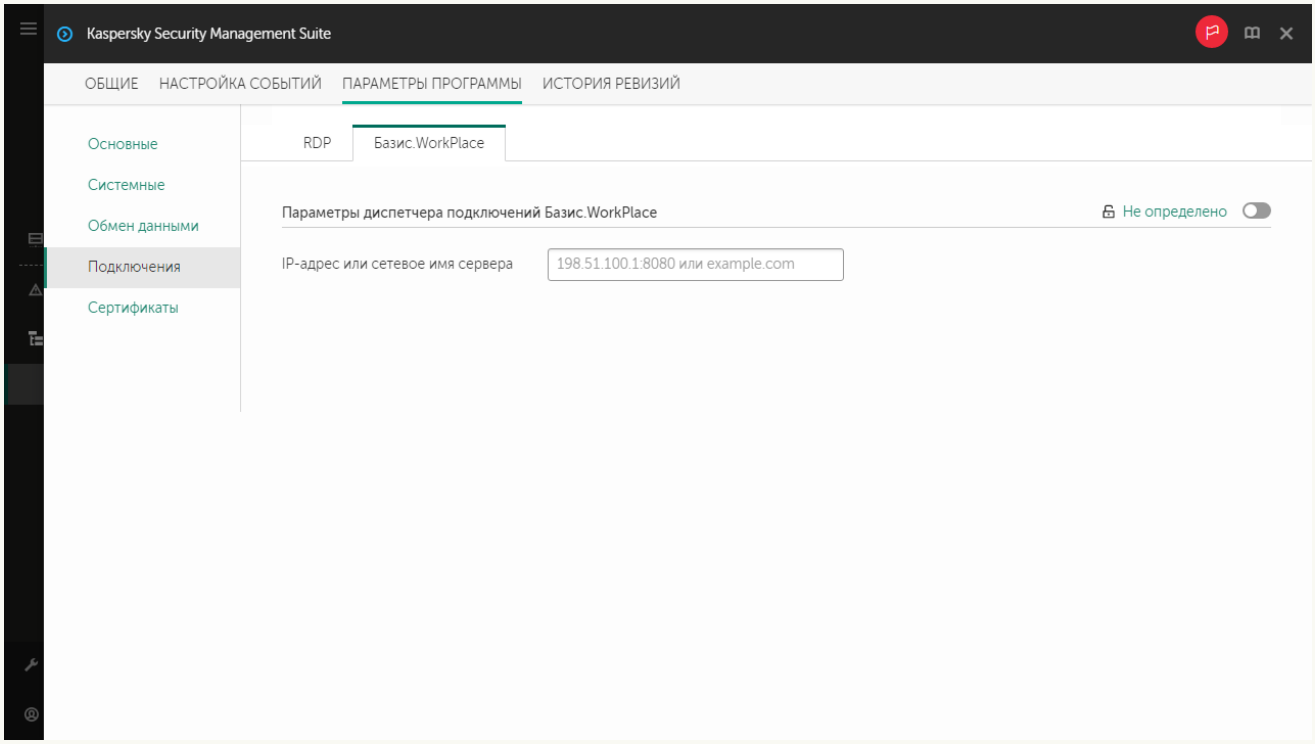
8. Если на вашем рабочем месте установлено два монитора и вы хотите, чтобы изображение удаленного рабочего стола выводилось на оба монитора, в блоке **Управление мониторами** установите флажок **Использовать два монитора**.

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

[Как настроить параметры подключения к удаленному рабочему столу 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 сетевое имя сервера** введите IP-адрес или имя сервера для подключения к удаленному рабочему столу под управлением Базис.WorkPlace.
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**.

Управление режимом энергосбережения Kaspersky Thin Client через Web Console

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

Как настроить режим энергосбережения для одного устройства

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

2. Нажмите на имя устройства, на котором запущен Kaspersky Thin Client. Вы можете просмотреть имя устройства в панели управления в интерфейсе Kaspersky Thin Client. Если имя компьютера отсутствует в списке, добавьте его в группу **Управляемые устройства**. Также вы можете управлять устройствами, которые еще не добавлены в управляемые, в разделе **Обнаружение устройств и развертывание** → **Нераспределенные устройства**.

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

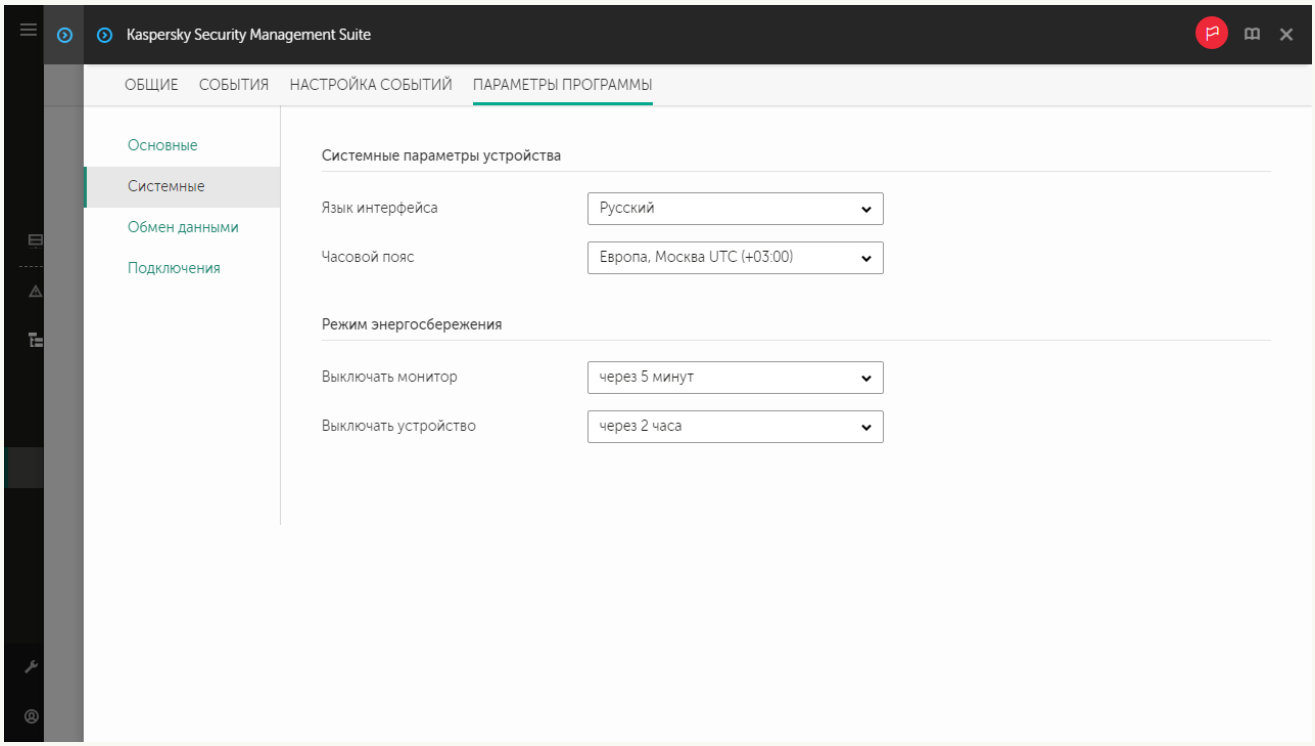
3. В открывшемся окне выберите вкладку **Программы**.

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 режима энергосбережения через Web Console для одного устройства

7. В блоке **Режим энергосбережения** настройте следующие параметры:

   - В раскрывающемся списке **Выключать монитор** выберите время бездействия системы, по истечении которого монитор будет переведен в режим энергосбережения.
   - 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 режима энергосбережения будут применены к Kaspersky Thin Client.

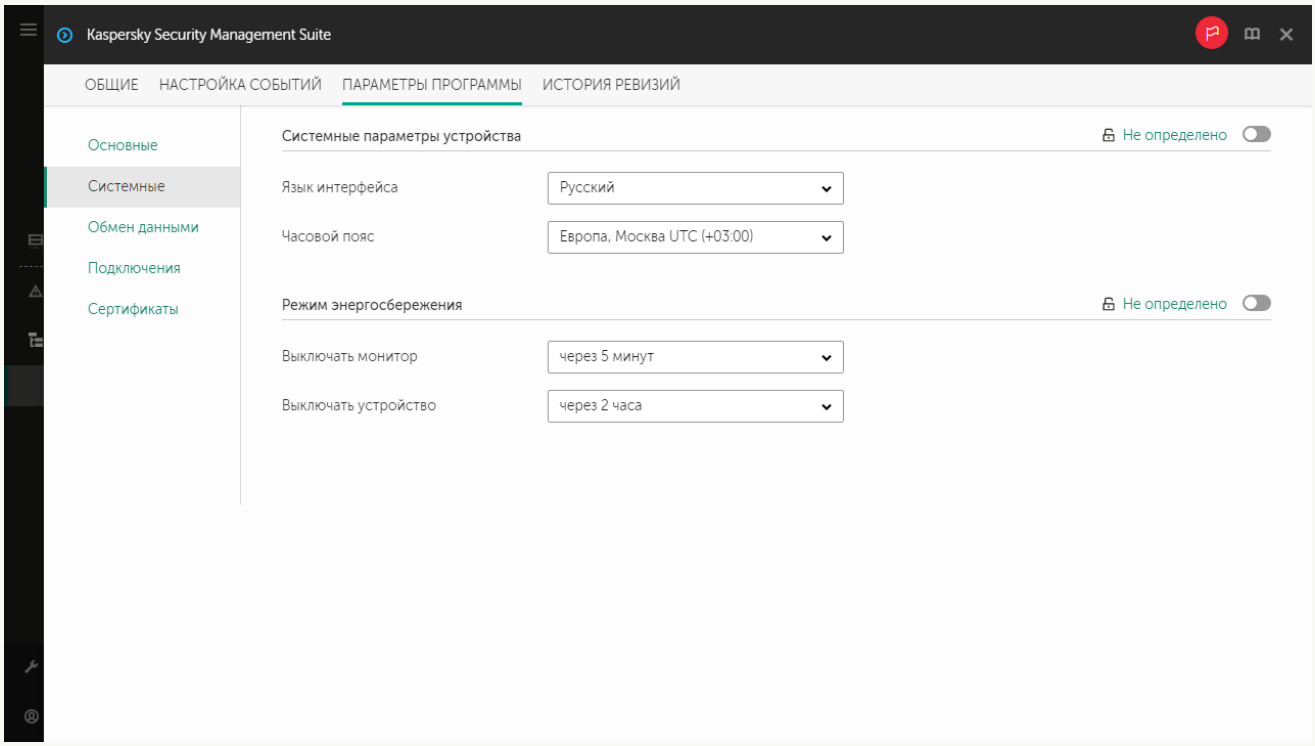
[Как настроить режим энергосбережения для группы устройств](#)

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 режима энергосбережения через Web Console для группы устройств

5. В блоке **Режим энергосбережения** настройте следующие параметры:

   - В раскрывающемся списке **Выключать монитор** выберите время бездействия системы, по истечении которого монитор будет переведен в режим энергосбережения.

   - 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 режима 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 устройства, на котором запущен Kaspersky Thin Client. Вы можете просмотреть имя устройства в панели управления в интерфейсе Kaspersky Thin Client. Если имя компьютера отсутствует в списке, добавьте его в группу **Управляемые устройства**. Также вы можете управлять устройствами, которые еще не добавлены в управляемые, в разделе **Обнаружение устройств и развертывание** → **Нераспределенные устройства**.

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

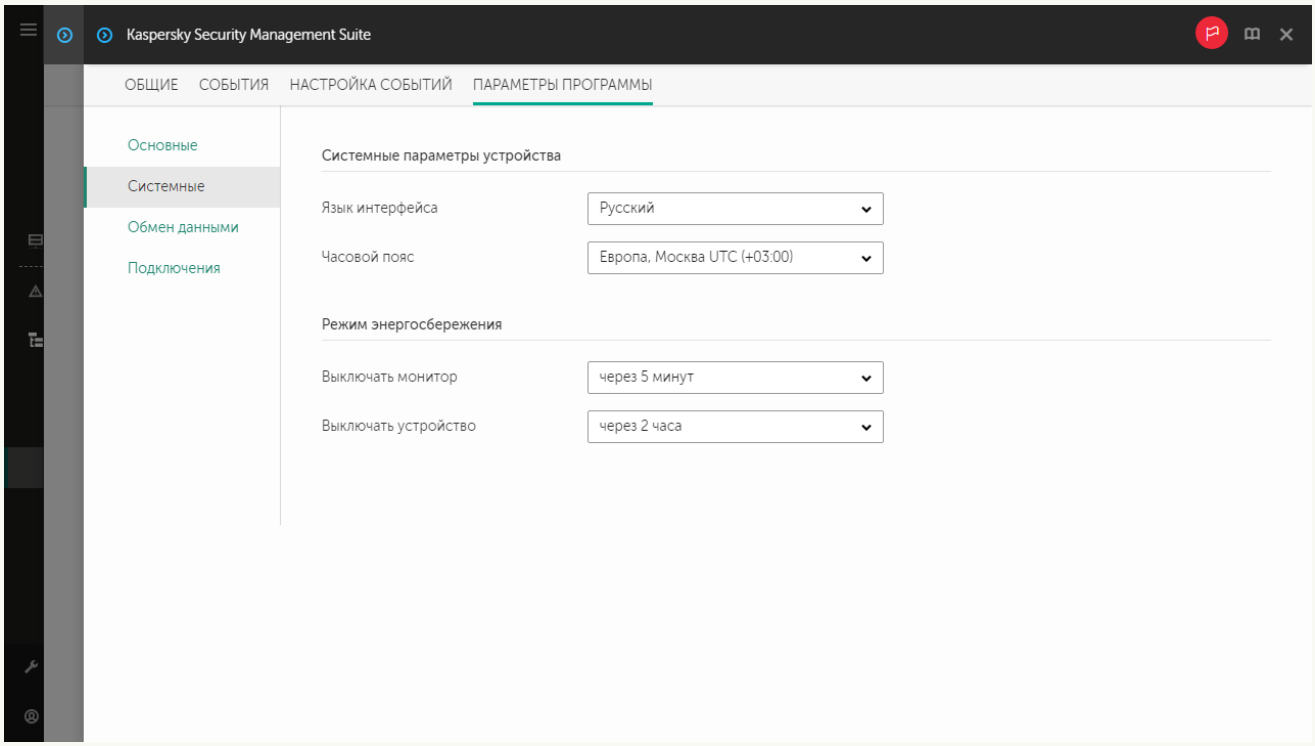
3. В открывшемся окне выберите вкладку **Программы**.

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).



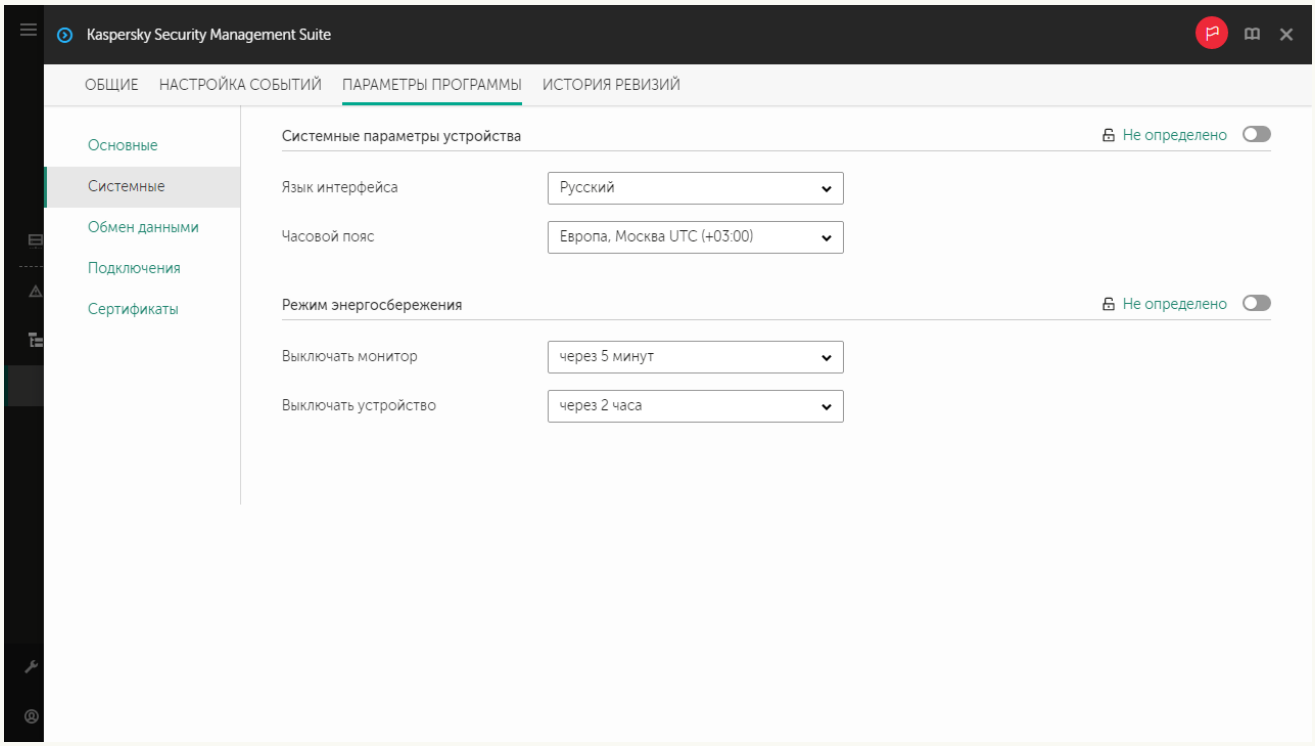
Окно настройки языка интерфейса и часового пояса через Web Console для одного устройства

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.

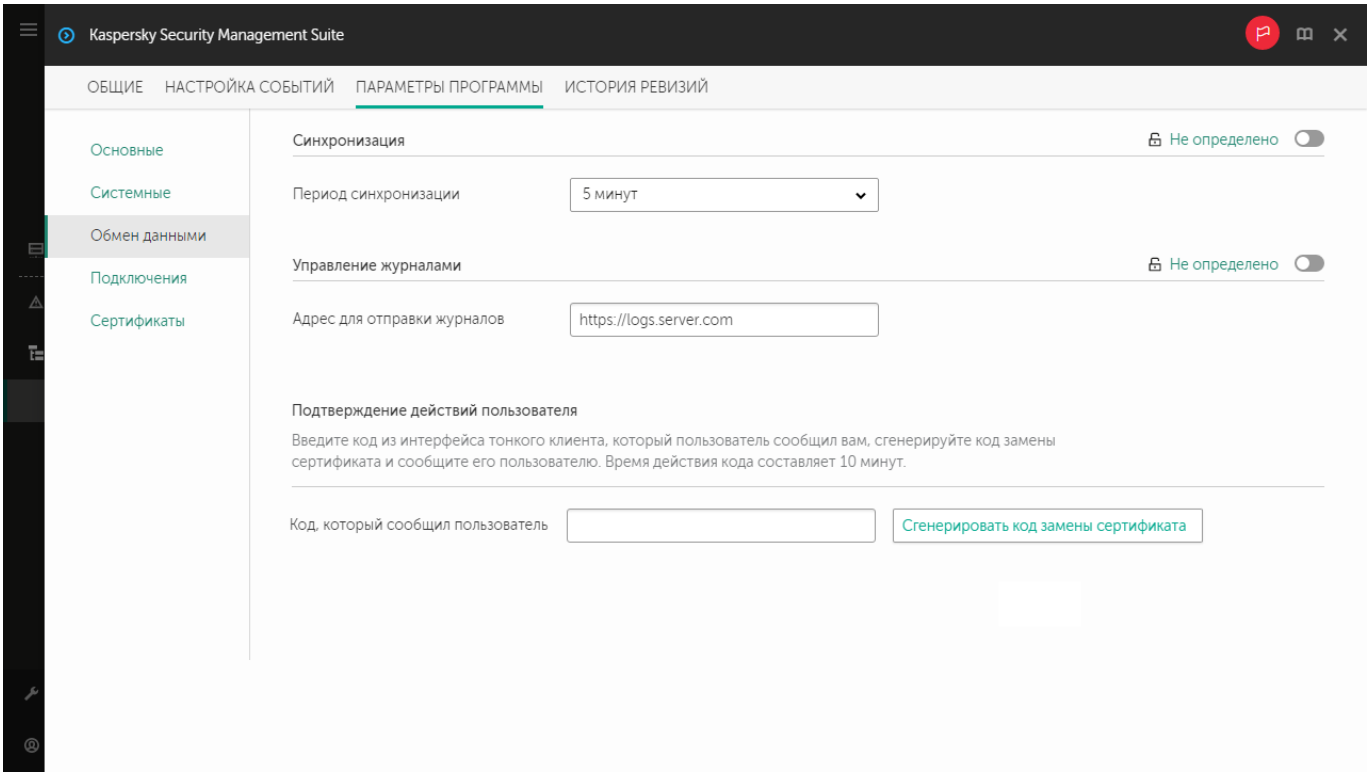
Если переключатель напротив названия группы параметров находится в положении **Принудительно** (Принудительно), то установленные значения параметров применяются к устройствам, на которые распространяется политика, изменение этих параметров заблокировано в интерфейсе Kaspersky Thin Client. Если переключатель 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

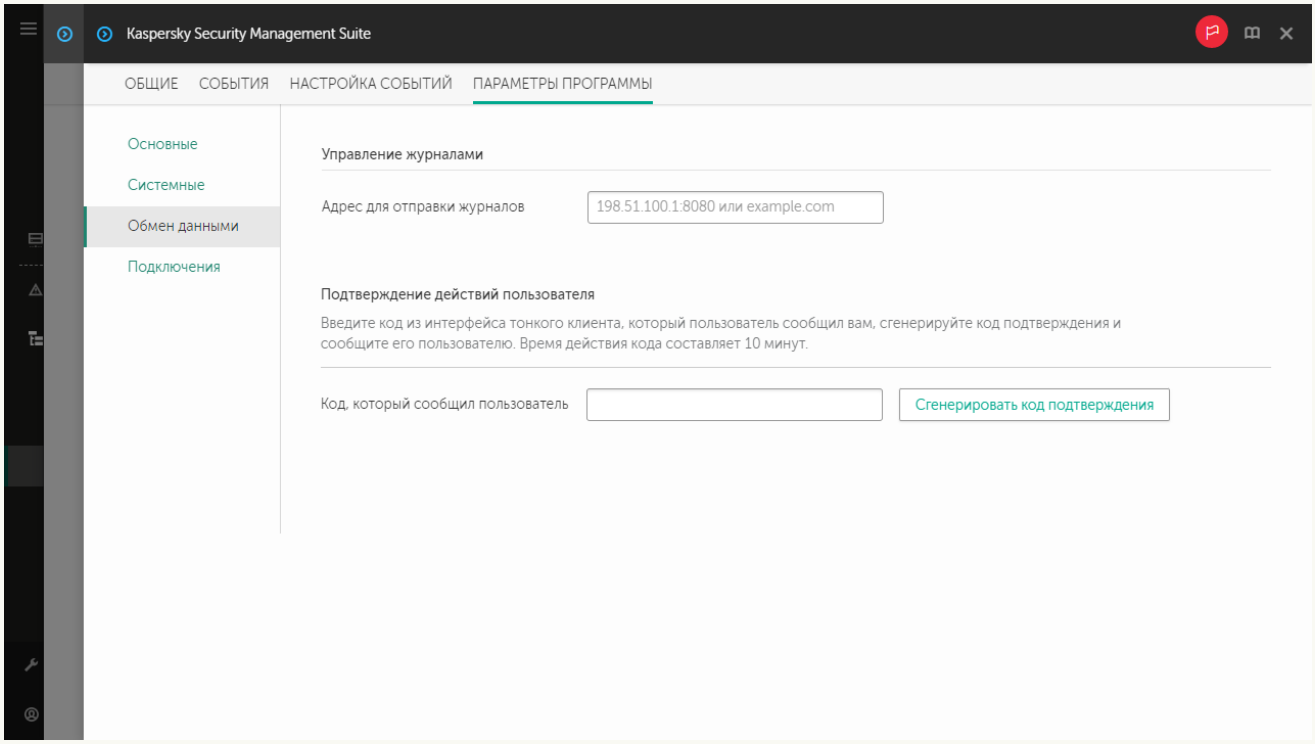
1. В главном окне Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства, на котором запущен Kaspersky Thin Client. Вы можете просмотреть имя устройства в панели управления в интерфейсе Kaspersky Thin Client. Если имя компьютера отсутствует в списке, добавьте его в группу **Управляемые устройства**. Также вы можете управлять устройствами, которые еще не добавлены в управляемые, в разделе **Обнаружение устройств и развертывание** → **Нераспределенные 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).

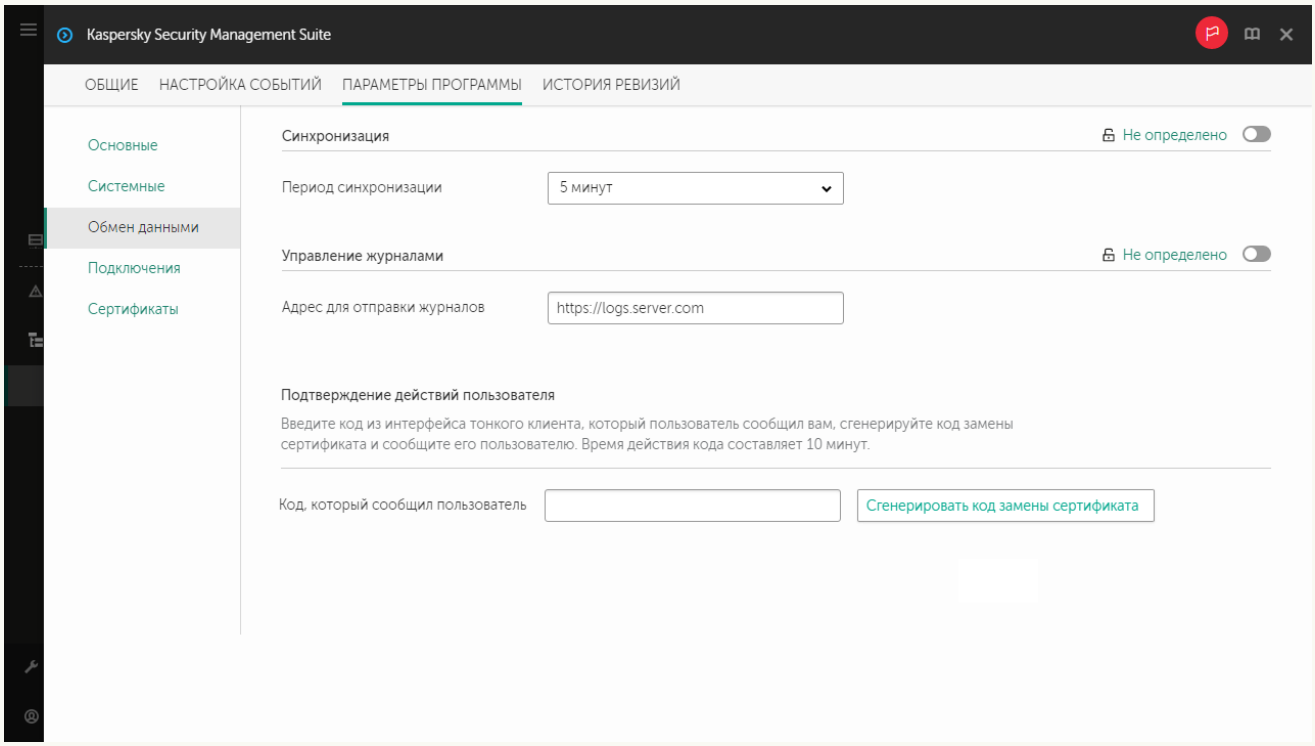


Окно настройки отправки журналов Kaspersky Thin Client через Web Console для одного устройства

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.

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 устройства, на котором запущен Kaspersky Thin Client. Вы можете просмотреть имя устройства в панели управления в интерфейсе Kaspersky Thin Client. Если имя компьютера отсутствует в списке, добавьте его в группу **Управляемые устройства**. Также вы можете управлять устройствами, которые еще не добавлены в управляемые, в разделе **Обнаружение устройств и развертывание → Нераспределенные устройства**.

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

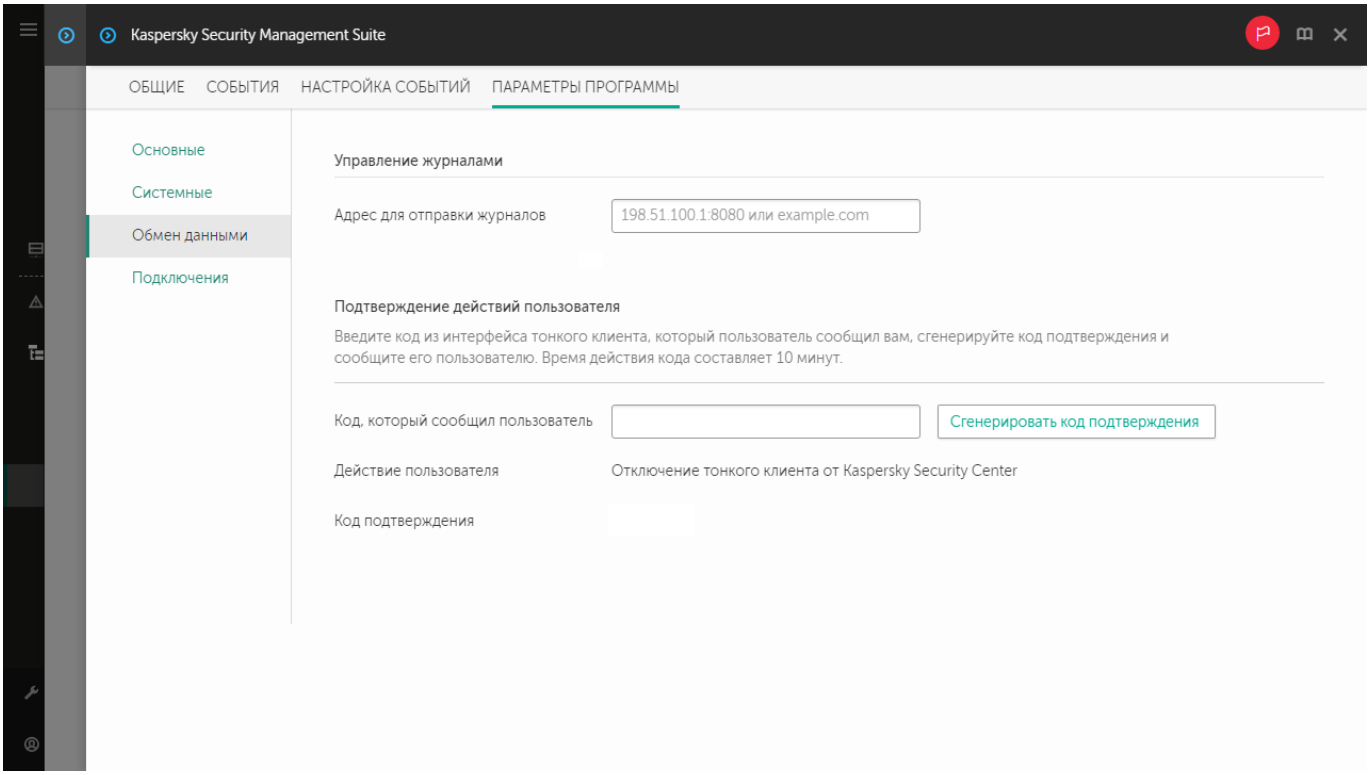
3. В открывшемся окне выберите вкладку **Программы**.

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 подтверждения изменения параметров подключения к Kaspersky Security Center

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.

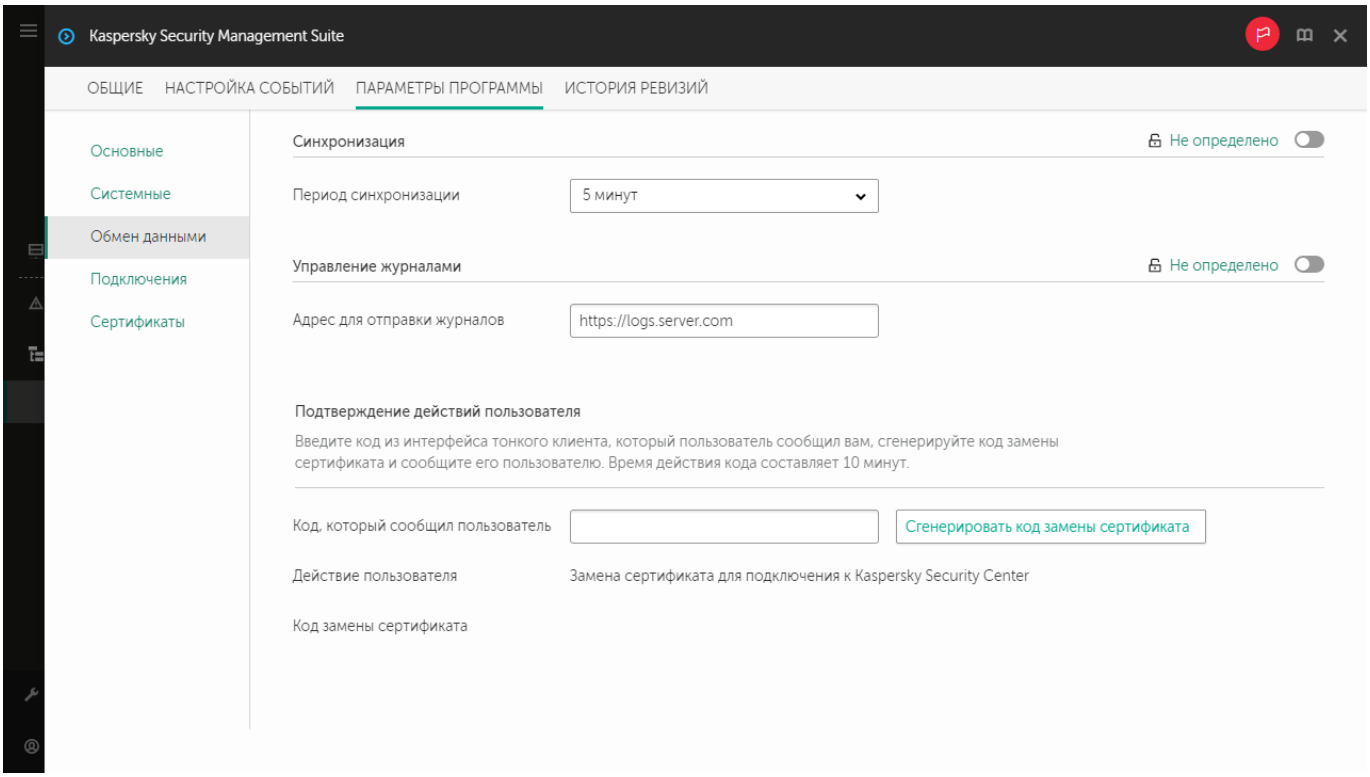
Чтобы подтвердить изменение сертификата для подключения к Kaspersky Security Center:

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** (см. рис. ниже).



Окно подтверждения изменения сертификата для подключения к Kaspersky Security Center

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 безопасности Kaspersky Thin Client через Web Console

Через Web Console вы можете управлять сертификатами безопасности для группы устройств с установленной операционной системой Kaspersky Thin Client. Вы можете просматривать действительные сертификаты, добавлять или удалять сертификаты.

После добавления в Kaspersky Security Center Web Console сертификатов для безопасного подключения к удаленным рабочим столам или к серверу журналирования тонкие клиенты, которые входят в группу администрирования, переходят в доверенный режим работы. При этом вы не сможете добавлять сертификаты через интерфейс Kaspersky Thin Client.

В разделе **Сертификаты** для каждого сертификата отображается следующая информация:

- **Имя файла** – имя файла сертификата и его формат.
- **Издатель** – информация об организации, выпустившей сертификат.
- **Субъект** – информация о программе, для которой выпущен сертификат.

- **Начало действия** – дата начала действия сертификата.
- **Окончание действия** – дата окончания действия сертификата.
- **Отпечаток сертификата** – хеш сертификата, вычисляемый по всем данным сертификата и его подпись.

Вы можете сортировать список сертификатов по дате начала или дате окончания действия сертификата, а также по издателю и субъекту.

О резервном сертификате для подключения Kaspersky Thin Client к Kaspersky Security Center

Kaspersky Thin Client использует для подключения к Kaspersky Security Center мобильный сертификат Сервера администрирования Kaspersky Security Center, который создается с помощью *Мастера первоначальной настройки Сервера администрирования* после установки Kaspersky Security Center. По умолчанию срок действия выпущенного сертификата составляет один год. При подключении к Kaspersky Security Center Kaspersky Thin Client проверяет действительность сертификата. Если требуется, вы можете выпустить новый (резервный) мобильный сертификат или настроить правило для выпуска сертификатов. Подробную информацию о создании нового мобильного сертификата Сервера администрирования Kaspersky Security Center см. в разделе *Работа с сертификатами для мобильных устройств*, а также в разделе *Перевыпуск сертификата Веб-сервера* онлайн-справки Kaspersky Security Center. Подробную информацию о настройке правил для выпуска сертификатов см. в разделе *Настройка правил выпуска сертификатов* онлайн-справки Kaspersky Security Center.

Управляемые устройства и устройства, входящие в группу администрирования получат новый (резервный) сертификат для подключения Kaspersky Thin Client к Kaspersky Security Center после синхронизации Kaspersky Thin Client и Kaspersky Security Center. Новый (резервный) сертификат будет сохранен в хранилище сертификатов Kaspersky Thin Client и будет использован для подключения тонких клиентов к Kaspersky Security Center, когда закончится срок действия текущего используемого сертификата.

Также вы можете выпустить пользовательский сертификат для подключения Kaspersky Thin Client к Kaspersky Security Center. При этом потребуется загрузить в Web Console созданный пользовательский сертификат в качестве мобильного сертификата. Подробную информацию о требованиях, которые предъявляются к пользовательским сертификатами Kaspersky Security Center, см. в разделе *Требования к пользовательским сертификатам, используемым в Kaspersky Security Center* в онлайн-справке Kaspersky Security Center.

Создание пользовательского сертификата для подключения Kaspersky Thin Client к Kaspersky Security Center

Вы можете использовать пользовательский сертификат для подключения Kaspersky Thin Client к Kaspersky Security Center. Подробную информацию о требованиях, которые предъявляются к сертификатам Kaspersky Security Center, см. в разделе *Требования к пользовательским сертификатам, используемым в Kaspersky Security Center* в онлайн-справке Kaspersky Security Center. Рекомендуется использовать пользовательский сертификат при миграции на новый Сервер администрирования Kaspersky Security Center группы устройств с установленной Kaspersky Thin Client. После создания пользовательский сертификат требуется загрузить в Web Console в качестве мобильного сертификата. Вы можете создать пользовательский сертификат с помощью утилиты OpenSSL.

Чтобы создать пользовательский 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 729 -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 729 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. Специальные требования к паролю не предъявляются.

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 в Web Console резервного и пользовательского сертификата для подключения Kaspersky Thin Client к Kaspersky Security Center

Если вы создали пользовательский сертификат или резервный сертификат для подключения Kaspersky Thin Client к Kaspersky Security Center, требуется загрузить созданный сертификат в Web Console в качестве мобильного сертификата.

Предварительно рекомендуется проверить соответствие пользовательского сертификата требованиям Kaspersky Security Center. Подробную информацию о требованиях, которые предъявляются к сертификатам Kaspersky Security Center, см. 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 в качестве мобильного сертификата.

Добавление новых сертификатов в Web Console

Для тонких клиентов, которые входят в группу администрирования вы можете добавлять в Web Console новые сертификаты для безопасного подключения к удаленным рабочим столам (по протоколу RDP и под управлением Базис.WorkPlace) или к серверу журналирования.

После добавления в Web Console сертификатов для безопасного подключения к удаленным рабочим столам или к серверу журналирования устройства, которые входят в группу администрирования, переходят в доверенный режим работы. При этом вы не сможете добавлять сертификаты через интерфейс Kaspersky Thin Client.

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 **ОК**, для подтверждения загрузки выбранных сертификатов.

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

Удаление сертификатов в Web Console

Для тонких клиентов, которые входят в группу администрирования вы можете удалять в Web Console сертификаты для безопасного подключения к удаленным рабочим столам (по протоколу RDP и под управлением Базис.WorkPlace) или к серверу журналирования.

При удалении сертификата вы больше не сможете выполнять безопасное подключение из интерфейса Kaspersky Thin Client к серверам, на которых установлен этот сертификат или подписанные им сертификаты.

После удаления в Web Console сертификатов для безопасного подключения к удаленным рабочим столам или к серверу журналирования устройства, которые входят в группу администрирования, выходят из доверенного режима работы. При этом для подключения к удаленным рабочим столам или к серверу журналирования потребуется добавление сертификатов в интерфейсе Kaspersky Thin Client.

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.

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 выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя устройства, на котором запущен Kaspersky Thin Client. Вы можете просмотреть имя устройства в панели управления в интерфейсе Kaspersky Thin Client. Если имя компьютера отсутствует в списке, добавьте его в группу **Управляемые устройства**.
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 Web Console выберите **Устройства** → **Управляемые устройства**.
2. Нажмите на имя тонкого клиента, на котором запущен 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, экран рабочего стола 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 физическое подключение есть, но по-прежнему не удается подключиться к удаленному рабочему столу, обратитесь в Службу технической поддержки.

Некорректно введенные данные

Перед инициацией подключения к удаленному рабочему столу Kaspersky Thin Client проверяет корректность следующих введенных пользователем данных:

- IP-адреса или имени сервера;
- имени пользователя;
- пароля пользователя.

Если формат указанных сведений отличается от ожидаемого системой, в нижней части окна подключения к удаленному рабочему столу отображается сообщение о некорректности данных.

Ошибок может быть несколько: требуется навести курсор на сообщение в нижней части окна подключения к удаленному рабочему столу, чтобы в окне подсказки просмотреть их полный список.

Чтобы подключиться к удаленному рабочему столу:

1. Укажите верные IP-адрес или имя сервера, имя пользователя и пароль.

2. Если вы уверены, что правильно ввели имя пользователя и пароль, но при попытке подключиться все равно отображается ошибка, убедитесь, что указываете правильное имя или IP-адрес сервера, к которому хотите подключиться.

Проверка подключения к сети

Чтобы проверить, подключен ли тонкий клиент к сети,

просмотрите информацию о состоянии подключения Kaspersky Thin Client к сети и к Kaspersky Security Center 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 к специалистам Службы технической поддержки ООО "Группа Компаний ТОНК".

При обращении в Службу технической поддержки специалисты могут запросить у вас журналы событий и аудита Kaspersky Thin Client. Эти журналы располагаются на устройстве с установленной системой Kaspersky Thin Client. Вы можете просмотреть журналы событий, используя интерфейс Kaspersky Thin Client, в разделе **Инструменты** → **Журнал событий**. Также вы можете отправить журналы событий и аудита на сервер журналирования, развернутый в инфраструктуре вашей организации.

Глоссарий

TLS

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

Администратор Kaspersky Security Center

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

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 монитор, клавиатура и мышь.

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.

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

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

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