

The Kaspersky logo, consisting of the word "kaspersky" in a lowercase, bold, sans-serif font. The background of the slide is a vibrant green with a white, irregular, rounded shape in the center where the text is placed.

kaspersky

Kaspersky Thin Client

© 2026 АО "Лаборатория Касперского"

Содержание

[Справка Kaspersky Thin Client](#)

[О Kaspersky Thin Client](#)

[Комплект поставки](#)

[Принцип работы Kaspersky Thin Client](#)

[Аппаратные и программные требования](#)

[Способы подключения к удаленным средам](#)

[Подключение с помощью приложения RDP](#)

[Подключение с помощью приложения Базис.WorkPlace](#)

[Подключение с помощью приложения Web Access](#)

[Что нового](#)

[Установка и обновление Kaspersky Thin Client](#)

[Установка Kaspersky Thin Client](#)

[Обновление Kaspersky Thin Client](#)

[Интерфейс Kaspersky Thin Client](#)

[Лицензирование Kaspersky Thin Client](#)

[Предоставление данных](#)

[Включение и первый запуск Kaspersky Thin Client](#)

[Перезагрузка и выключение Kaspersky Thin Client](#)

[Использование сертификатов в Kaspersky Thin Client](#)

[Настройка Kaspersky Thin Client](#)

[Сценарий: быстрый старт для администратора](#)

[Сценарий: назначение сертификатов для группы тонких клиентов](#)

[Сценарий: миграция тонких клиентов на новый Сервер Kaspersky Security Center](#)

[Настройка общих параметров](#)

[Настройка параметров сети](#)

[Управление устройствами воспроизведения и записи звука](#)

[Настройка параметров подключения Kaspersky Thin Client к Kaspersky Security Center](#)

[Изменение параметров подключения Kaspersky Thin Client к Kaspersky Security Center](#)

[Настройка даты и времени](#)

[Настройка автоматического запуска и отображения приложений](#)

[Настройка мониторов и экранов](#)

[Настройка параметров энергосбережения](#)

[Настройка параметров удаленного управления тонким клиентом в интерфейсе Kaspersky Thin Client](#)

[Изменение типа нераспознанных USB-устройств](#)

[Сброс параметров Kaspersky Thin Client](#)

[Настройка параметров подключения к удаленной среде с помощью приложения RDP](#)

[Настройка параметров подключения к удаленной среде с помощью приложения Базис.WorkPlace](#)

[Управление доступом к параметрам Kaspersky Thin Client](#)

[Управление Kaspersky Thin Client, установленной на тонком клиенте](#)

[Сценарий: работа в Kaspersky Thin Client на тонком клиенте](#)

[Подключение к удаленной среде](#)

[Подключение к удаленной среде с помощью приложения RDP](#)

[Подключение к удаленной среде с помощью приложения Базис.WorkPlace](#)

[Подключение к удаленной среде с помощью приложения Web Access](#)

[Управление удаленной сессией](#)

[Работа с панелью подключения](#)

[Блокировка и разблокировка удаленной сессии](#)

[Завершение удаленной сессии](#)

[Управление устройствами воспроизведения и записи звука в панели подключения](#)

[Управление окнами виртуального приложения](#)

[Web Access: перенаправление USB-устройств в удаленную среду](#)

[Просмотр информации о Kaspersky Thin Client и тонком клиенте](#)

[Просмотр информации о состоянии сети](#)

[Просмотр уведомлений Kaspersky Thin Client](#)

[Управление сертификатами в интерфейсе Kaspersky Thin Client](#)

[Управление Kaspersky Thin Client с помощью горячих клавиш](#)

[Управление доступом к удаленному управлению и экрану удаленной среды](#)

[Удаленное подключение к тонкому клиенту](#)

[Управление Kaspersky Thin Client через Kaspersky Security Center Web Console](#)

[О веб-плагине управления Kaspersky Security Management Suite](#)

[Установка веб-плагина управления Kaspersky Security Management Suite](#)

[Обновление веб-плагина управления Kaspersky Security Management Suite](#)

[Удаление веб-плагина управления Kaspersky Security Management Suite](#)

[Разделение доступа к функциям веб-плагина управления Kaspersky Security Management Suite](#)

[Вход и выход из Web Console](#)

[Управление политиками и группами администрирования](#)

[Создание группы администрирования](#)

[Добавление тонких клиентов в группу администрирования](#)

[Создание политики](#)

[Изменение политики](#)

[Блокировка параметров в политике](#)

[Настройка параметров Kaspersky Thin Client через Web Console для одного устройства](#)

[Изменение идентификатора тонкого клиента через Web Console: одно устройство](#)

[Настройка подключения к удаленной среде с помощью приложения RDP через Web Console: одно устройство](#)

[Настройка подключения к удаленной среде с помощью приложения Базис.WorkPlace через Web Console: одно устройство](#)

[Настройка подключения к удаленной среде с помощью приложения Web Access через Web Console: одно устройство](#)

[Настройка мониторов и экранов через Web Console: одно устройство](#)

[Настройка системных параметров Kaspersky Thin Client через Web Console: одно устройство](#)

[Настройка отправки журналов Kaspersky Thin Client на сервер журналирования: одно устройство](#)

[Настройка параметров персонализации Kaspersky Thin Client: одно устройство](#)

[Настройка параметров удаленного подключения к тонкому клиенту через Web Console: одно устройство](#)

[Настройка автоматического запуска и отображения приложений: одно устройство](#)

[Настройка параметров Kaspersky Thin Client через Web Console для группы администрирования](#)

[Настройка основных параметров Kaspersky Thin Client через Web Console: группа администрирования](#)

[Настройка подключения к удаленной среде с помощью приложения RDP через Web Console: группа администрирования](#)

[Настройка подключения к удаленной среде с помощью приложения Базис.WorkPlace через Web Console: группа администрирования](#)

[Настройка подключения к удаленной среде с помощью приложения Web Access через Web Console: группа администрирования](#)

[Настройка мониторов и экранов через Web Console: группа администрирования](#)

[Настройка системных параметров Kaspersky Thin Client через Web Console: группа администрирования](#)

[Настройка отправки журналов Kaspersky Thin Client на сервер журналирования: группа администрирования](#)

[Настройка параметров персонализации Kaspersky Thin Client: группа администрирования](#)

[Настройка параметров удаленного подключения к тонкому клиенту через Web Console: группа администрирования](#)

[Настройка автоматического запуска и отображения приложений: группа администрирования](#)

[Настройка синхронизации Kaspersky Thin Client и Kaspersky Security Center](#)

[Подтверждение действий пользователя Kaspersky Thin Client](#)

[Управление сертификатами Kaspersky Thin Client через Web Console](#)

[О сертификате для подключения Kaspersky Thin Client к Kaspersky Security Center](#)

[Перевыпуск сертификата для подключения Kaspersky Thin Client к Kaspersky Security Center в Web Console](#)

[Создание сертификата для подключения Kaspersky Thin Client к Kaspersky Security Center](#)

[Загрузка сертификата для подключения Kaspersky Thin Client к Kaspersky Security Center в Web Console](#)

[Добавление новых сертификатов в Web Console](#)

[Удаление сертификатов в Web Console](#)

[Конвертация сертификата из формата PEM в формат DER](#)

[Обновление сертификата при миграции на новый Сервер Kaspersky Security Center](#)

[Мониторинг событий Kaspersky Thin Client через Kaspersky Security Center Web Console](#)

[Настройка регистрации уведомлений о событиях Kaspersky Thin Client через Kaspersky Security Center Web Console](#)

[Просмотр событий Kaspersky Thin Client через Web Console](#)

[Устранение неисправностей](#)

[Разрыв соединения с удаленной средой](#)

[Проблемы с разделением доступа к функциям веб-плагина управления Kaspersky Security Management Suite](#)

[Обращение в Службу технической поддержки](#)

[О журналах Kaspersky Thin Client](#)

[Отправка журналов](#)

[Глоссарий](#)

[TLS](#)

[Администратор Kaspersky Security Center](#)

[Брокер](#)

[Виртуальное приложение](#)

[Группа администрирования](#)

[Плагин управления Kaspersky Security Management Suite](#)

[Политика](#)

[Сервер администрирования](#)

[Сервер журналирования](#)

[Событие](#)

[Тонкий клиент](#)

[Удаленная сессия](#)

[Удаленная среда](#)

[Удаленный рабочий стол](#)

[Информация о стороннем коде](#)

[Уведомления о товарных знаках](#)

Справка Kaspersky Thin Client

	Что нового Узнайте, что нового в этой версии Kaspersky Thin Client.		Аппаратные и программные требования Поддерживаемые удаленные среды и периферийные устройства.
	Установка и обновление Как установить Kaspersky Thin Client на тонкий клиент. Как обновить версию Kaspersky Thin Client.		Начало работы Запуск тонкого клиента. Первоначальная настройка и соединение с Kaspersky Security Center. Назначение сертификатов.
	Подключение к удаленной среде Доступные способы подключения к удаленной среде. Как подключаться к удаленной среде. Настройка параметров подключения.		Централизованное управление через Kaspersky Security Center Web Console Управление политиками и группами администрирования. Настройка тонких клиентов с Kaspersky Thin Client.
	Дополнительные возможности Управление сертификатами Kaspersky Thin Client. Управление доступом к параметрам Kaspersky Thin Client.		Мониторинг Просмотр и отправка журналов событий и аудита на сервер журналирования. Просмотр событий Kaspersky Thin Client через Kaspersky Security Center Web Console.
	Удаленное управление Как дистанционно подключиться к тонкому клиенту со своего устройства.		Сброс параметров и данных Как выполнить сброс параметров и данных Kaspersky Thin Client.

О Kaspersky Thin Client

Kaspersky Thin Client версии 2.3 (далее также "система") представляет собой кибериммунную микроядерную операционную систему для [тонких клиентов](#) на базе KasperskyOS. Kaspersky Thin Client предназначена для подключения к удаленной среде и работы в удаленной среде, в том числе с использованием периферийных устройств, подключенных к тонкому клиенту. Kaspersky Thin Client версии 2.3 устанавливается на тонкие клиенты [Dell™ Wyse 3040](#), [Centerm F620](#) и [TONK TN1200](#).

Обзор аппаратных компонентов тонких клиентов (в том числе элементов управления и разъемов) не приводится в этом документе, поскольку содержится в документации производителя устройства, на которое устанавливается Kaspersky Thin Client.

Основные функции Kaspersky Thin Client:

- Подключение к удаленной среде:
 - подключение к удаленным и виртуальным рабочим столам под управлением операционных систем семейства [Microsoft® Windows®](#) по протоколу RDP, в том числе через брокер Microsoft Remote Desktop Connection Broker;
 - подключение к терминальным серверам под управлением операционных систем семейства [Microsoft Windows Server®](#) по протоколу RDP, в том числе через брокер Microsoft Remote Desktop Connection Broker;
 - подключение к удаленным и виртуальным рабочим столам под управлением операционных систем семейства [Linux®](#) по протоколу RDP;
 - подключение к виртуальным приложениям, в том числе развернутым в инфраструктуре Microsoft Remote Desktop Services, или находящимся под управлением операционных [Microsoft® Windows®](#), по протоколу RDP;
 - подключение к виртуальным рабочим столам, развернутым в инфраструктуре [Базис.WorkPlace](#);
 - подключение к виртуальным рабочим столам, развернутым в инфраструктуре [Citrix Workspace™](#).
- Передача изображения удаленной среды на мониторы, подключенные к тонкому клиенту.
- Перенаправление в удаленную среду следующих [устройств, подключенных к тонкому клиенту](#):
 - проводной и беспроводной клавиатуры и мыши;
 - USB-накопителей;
 - устройств воспроизведения и записи звука (USB-гарнитур);
 - веб-камер;
 - смарт-карт и токенов;
 - устройств печати и сканирования: принтеров, сканеров (в том числе QR- и штрихкодов).

- Централизованное управление, обновление и контроль Kaspersky Thin Client через [Kaspersky Security Center Web Console](#). Для связи Kaspersky Thin Client и Kaspersky Security Center используется [веб-плагин Kaspersky Security Management Suite](#).

Kaspersky Thin Client 2.3 поддерживает Kaspersky Security Center Linux версии 15.3 и Kaspersky Security Center Web Console версии 15.3.

Kaspersky Thin Client 2.3 поддерживает следующие языки интерфейса: русский, английский (США), испанский (Мексика) и португальский (Бразилия).

Комплект поставки

Kaspersky Thin Client 2.3 поставляется в одном из следующих форматов:

- образ Kaspersky Thin Client без поставки аппаратной платформы (тонкого клиента);
- аппаратная платформа с предустановленным Kaspersky Thin Client, поставляемая партнером.

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

- `Kaspersky_Thin_Client_2.3.0.<техническая версия сборки>_Wyse3040.tar.gz` – архив с установочным образом Kaspersky Thin Client для платформы Dell Wyse 3040.
- `Kaspersky_Thin_Client_2.3.0.<техническая версия сборки>_TN1200.tar.gz` – архив с установочным образом Kaspersky Thin Client для платформы TONK TN1200 и Centerm F620.
- `hw_install.sh` – скрипт для установки на тонкий клиент.
- Скрипты для обновления с коммерческой версии 2.0 и 2.0.1 на версию 2.3:
 - `hw_update.sh`;
 - `save_files.sh`;
 - `restore_files.sh`.
- `KTC_LegalNotices_en.txt` – текстовый файл с информацией о стороннем коде.
- Текстовые файлы с описанием новых функций и известных ограничений:
 - `ReleaseNotes_Kaspersky_Thin_Client_2.3.0.<техническая версия сборки>_EN.txt`;
 - `ReleaseNotes_Kaspersky_Thin_Client_2.3.0.<техническая версия сборки>_ES.txt`;
 - `ReleaseNotes_Kaspersky_Thin_Client_2.3.0.<техническая версия сборки>_PT_BR.txt`;
 - `ReleaseNotes_Kaspersky_Thin_Client_2.3.0.<техническая версия сборки>_RU.txt`.
- Файлы Лицензионного соглашения Kaspersky Thin Client:
 - `eula_en_ktc_00008.txt`;
 - `eula_es_ktc_00008.txt`;

- eula_pt_ktc_00008.txt;
- eula_ru_ktc_00008.txt.

В комплект поставки Kaspersky Security Management Suite версии 2.3 входят перечисленные ниже составляющие.

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

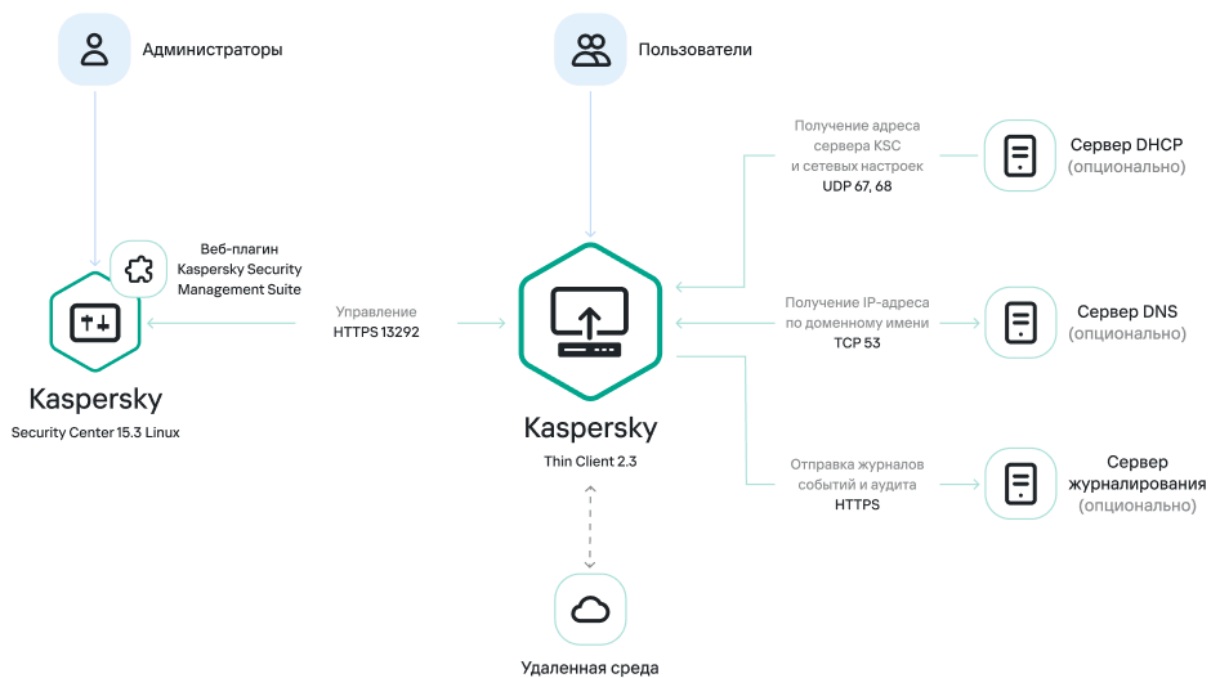
- Архивы для операционных систем семейства Linux с установочными образами и файлами подписи веб-плагина для Kaspersky Security Center:
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<техническая версия сборки>_en.sh;
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<техническая версия сборки>_es.sh;
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<техническая версия сборки>_pt_br.sh;
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<техническая версия сборки>_ru.sh.
- Архивы для операционных систем семейства Microsoft Windows с установочными образами и файлами подписи веб-плагина для Kaspersky Security Center:
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<техническая версия сборки>_ru.exe;
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<техническая версия сборки>_en.exe;
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<техническая версия сборки>_es.exe;
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<техническая версия сборки>_pt_br.exe.
- KSMS_2_3_0_0.conf – конфигурационный файл RBAC.
- KSMS_LegalNotices_en.txt – текстовый файл с информацией о стороннем коде для Kaspersky Security Management Suite.
- Файлы Лицензионного соглашения Kaspersky Security Management Suite:
 - eula_en_ksms_2.3.rtf;
 - eula_es_ksms_2.3.rtf;

- eula_pt_ksms_2.3.rtf;
- eula_ru_ksms_2.3.rtf.

Принцип работы Kaspersky Thin Client

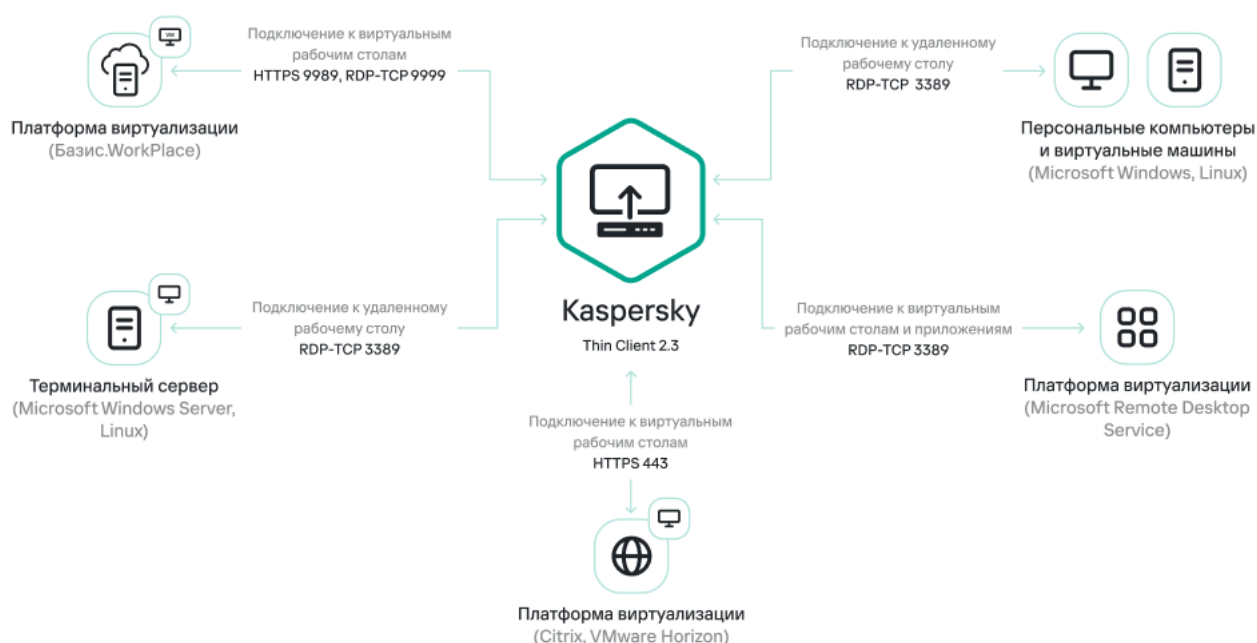
Типовая схема работы Kaspersky Thin Client (см. рис ниже) предполагает следующее:

- Система Kaspersky Thin Client, установленная на тонком клиенте, получает параметры сети от DHCP-сервера, либо администратор настраивает параметры вручную.
- Администратор подключает и настраивает взаимодействие между Kaspersky Thin Client и Kaspersky Security Center, а также [устанавливает веб-плагин управления](#) Kaspersky Security Management Suite.
- Kaspersky Thin Client получает доверенные сертификаты, параметры подключения к удаленной среде, дату и время и другие основные параметры с помощью [политики](#) [?](#), созданной через Kaspersky Security Center Web Console.
- Пользователь подключается к [удаленной среде](#) [?](#).
- В случае возникновения неполадок пользователь в интерфейсе Kaspersky Thin Client отправляет [журналы событий и аудита](#) на [сервер журналирования](#) [?](#), развернутый в инфраструктуре вашей организации.
- Администратор [выполняет обновление Kaspersky Thin Client](#).



Типовая схема работы Kaspersky Thin Client

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



Взаимодействие Kaspersky Thin Client с платформами виртуализации и удаленными средами

Аппаратные и программные требования

В этом разделе описаны аппаратные и программные требования к Kaspersky Thin Client 2.3.

Обзор аппаратных компонентов тонких клиентов (в том числе элементов управления и разъемов) не приводится в этом документе, поскольку содержится в документации производителя устройства, на которое устанавливается Kaspersky Thin Client.

Требования к мониторам

Kaspersky Thin Client поддерживает подключение двух мониторов.

В зависимости от настроек ориентации экрана Kaspersky Thin Client поддерживает следующие разрешения мониторов:

- Если настроена горизонтальная или перевернутая горизонтальная ориентация экрана:
 - 1024x768 (XGA);
 - 1280x720 (HD);
 - 1280x1024 (SXGA);
 - 1280x768 (WXGA);

- 1440x900 (WXGA+);
 - 1400x1050 (SXGA+);
 - 1920x1080 (Full HD).
- Если настроена вертикальная или перевернутая вертикальная ориентация экрана:
- 1280x1024 (SXGA);
 - 1400x1050 (SXGA+);
 - 1920x1080 (Full HD).

Kaspersky Thin Client поддерживает следующие интерфейсы подключения:

- HDMI;
- Display Port.

Kaspersky Thin Client поддерживает глубину цвета монитора только TrueColor.

Требования к периферийным устройствам, подключаемым к Kaspersky Thin Client

Kaspersky Thin Client поддерживает работу со следующими периферийными устройствами:

- Проводные клавиатуры и мыши без мультимедийных функций, подключаемые через USB-порт, а также беспроводные клавиатуры и мыши (радиосигнал).
- USB-накопители.
- Смарт-карты и токены, подключаемые через USB-порт.
- Устройства печати и сканирования, подключаемые через USB-порт: принтеры, сканеры (в том числе QR- и штрихкодов).

В удаленной среде должен быть установлен драйвер для устройства, которое подключено к тонкому клиенту.

- Проводные устройства записи и воспроизведения звука, подключаемые в разъем mini-jack и через USB-порт, а также беспроводные USB-гарнитуры (радиосигнал).
- Веб-камеры, подключаемые через USB-порт.

Требования к системам виртуализации и удаленного доступа

Kaspersky Thin Client поддерживает работу с системами виртуализации и удаленного доступа следующих версий:

- Базис.WorkPlace 2.4.1.
- Citrix Virtual Apps and Desktops 2402 cu1.
Клиент: Citrix Workspace app for HTML5 24.11.0.51.

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 15.3 Linux. Системные и программные требования к серверу, на котором разворачивается Kaspersky Security Center, приведены в [онлайн-справке Kaspersky Security Center](#).

Требования к серверу журналирования

К [серверу журналирования](#) предъявляются следующие требования:

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

Инструкции по установке и настройке сервера журналирования см. в [Базе знаний](#).

Способы подключения к удаленным средам

Этот раздел содержит информацию о технологиях удаленного подключения и [удаленных средах](#) поддерживаемых Kaspersky Thin Client, а также о способах подключения к таким средам с помощью приложений Kaspersky Thin Client.

В Kaspersky Thin Client предустановлены следующие приложения:

- **RDP** – приложение для подключения к удаленным рабочим столам или виртуальным приложениям по протоколу RDP.
- **Базис.WorkPlace** – приложение для подключения к виртуальным рабочим столам, развернутым в инфраструктуре Базис.WorkPlace.
- **Web Access** – приложение для подключения к удаленной среде, развернутой в инфраструктуре Citrix Workspace.

В этом разделе также представлены данные о том, какие из подключенных к Kaspersky Thin Client устройств могут быть перенаправлены в удаленную среду.

Подключение с помощью приложения RDP

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

Начиная с версии 2.3.4, Kaspersky Thin Client обеспечивает горячее подключение USB-токенов, USB-накопителей и принтеров (USB) во время активной сессии удаленного подключения.

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

Инструкции по подключению к удаленной среде приведены в [отдельной статье](#).

RDP: поддерживаемые операционные системы, способы подключения и периферийные устройства

	Windows Server 2016/2019/2022 в MS RDS	Windows 10/11	Windows Server 2016/2019/2022	ALT Linux 11 РЕД ОС 8	Astra Linux SE 1.8.1
Подключение к виртуальному приложению	✓	✓	✓	—	—
Подключение к удаленному рабочему столу					
Прямое подключение ?	—	✓	✓	✓	✓
Подключение с помощью VDI ?	✓	—	—	—	—
Терминальное подключение ?	✓	—	✓	✓	✓
Периферийные устройства					

USB-токены	✓	✓	✓	✓ Примечание ?	—
Смарт-карты (USB)	✓	✓	✓	✓ Примечание ?	—
USB-накопители	✓	✓	✓	✓ Примечание ?	—
Принтеры (USB)	✓	✓	✓ Примечание ?	✓ Примечание ?	—
Сканеры (USB)	✓	✓	✓ Примечание ?	✓ Примечание ?	—
Сканеры QR- и штрихкодов (USB)	✓	✓	✓	✓	✓
Микрофоны (mini-jack, USB) Примечание ?	✓	✓	✓ Примечание ?	✓ Примечание ?	✓ Примечание ?
Устройства воспроизведения звука (mini-jack, USB) Примечание ?	✓	✓	✓ Примечание ?	✓ Примечание ?	✓ Примечание ?
Веб-камера (видео, USB)	✓	✓	✓	—	—

Подключение с помощью приложения Базис.WorkPlace

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

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

Инструкции по подключению к удаленной среде приведены в [отдельной статье](#).

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

	Windows 10/11	Windows Server 2016/2019/2022	РЕД ОС 8 ALT Linux 11 Astra Linux SE 1.8.1
Подключение к удаленному рабочему столу			
Прямое подключение ?	—	—	—
Подключение с помощью VDI ?	✓	✓	✓
Терминальное подключение ?	—	✓	—
Периферийные устройства			
USB-токены	✓	✓	—
Смарт-карты (USB)	✓	✓	—
USB-накопители	✓	✓	—

Принтеры (USB)	✓	✓ Примечание 2	—
Сканеры (USB)	✓	✓	—
Сканеры QR- и штрихкодов (USB)	✓	✓	—
Микрофоны (mini-jack, USB) Примечание 2	✓	✓	✓
Устройства воспроизведения звука (mini-jack, USB) Примечание 2	✓	✓	✓
Веб-камера (видео, USB)	—	—	—

Подключение с помощью приложения Web Access

С помощью приложения Web Access вы можете подключаться к удаленной среде, развернутой в инфраструктуре Citrix Workspace. Web Access поддерживает HTML5 и обеспечивает безопасное соединение HTTPS при подключении. В таблице ниже описаны доступные способы подключения и периферийные устройства для операционных систем Windows.

Инструкции по подключению приведены в [отдельной статье](#).

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

	Microsoft Windows 10/11	Microsoft Windows Server 2016/2019/2022
Подключение к удаленному рабочему столу		
Прямое подключение 2	—	—
Подключение с помощью VDI 2	✓	✓
Терминальное подключение 2	—	✓
Периферийные устройства (Citrix Workspace)		
USB-токены	—	—
Смарт-карты (USB)	—	—
USB-накопители (FAT16 и FAT32, до 128 ГБ)	✓	✓
Принтеры (USB)	✓	✓
Сканеры (USB)	✓	✓
Сканеры QR- и штрихкодов (USB)	✓	✓
Микрофоны (mini-jack, USB) Примечание 2	✓	✓
Устройства воспроизведения звука (mini-jack, USB) Примечание 2	✓	✓
Веб-камера (видео, USB)	✓	✓

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

При подключении к удаленной среде, развернутой в инфраструктуре Citrix Workspace, не поддерживается перенаправление более двух USB-устройств одновременно.

Что нового

В Kaspersky Thin Client версии 2.3 появились следующие возможности и доработки:

- Перенаправление в виртуальную среду Citrix через приложение Web Access следующих устройств:
 - USB-накопителей (с использованием технологии Client Drive Mapping);
 - USB-гарнитур;
 - веб-камер;
 - устройств печати и сканирования: принтеров, сканеров (в том числе штрих- и QR-кодов).
- Перенаправление в удаленную среду по протоколу RDP следующих устройств:
 - USB-гарнитур;
 - веб-камер;
 - устройств печати и сканирования: принтеров, сканеров (в том числе штрих- и QR-кодов).
- Добавлена возможность в удаленной сессии выбирать устройство воспроизведения и записи звука в панели подключения.
- Добавлена возможность настраивать следующие параметры подключения к удаленному рабочему столу тонкого клиента по протоколу RDP:
 - подключение администратора к удаленному рабочему столу тонкого клиента (автоматически, с подтверждением пользователя или запрещено);
 - отображение администратору окна запущенной удаленной сессии пользователя (автоматически, с подтверждением пользователя или запрещено).
- Поддержано удаленное подключение к тонкому клиенту по протоколу RDP с авторизацией по имени устройства и паролю.
- Поддержана блокировка экрана тонкого клиента из активной удаленной сессии.
- Добавлена поддержка тонкого клиента Dell Wyse 3040.
- Поддержана прошивка UEFI, которая увеличивает скорость загрузки тонкого клиента и поддерживает большие объемы памяти.
- Добавлена возможность отображать на рабочем столе тонкого клиента только те приложения, которые пользователь выбрал в настройках (RDP, Базис.WorkPlace, Web Access).
- Добавлена возможность автоматически запускать одно из приложений (RDP, Базис.WorkPlace, Web Access), выбранное пользователем, после запуска тонкого клиента.
- Добавлена возможность автоматически подключаться к удаленной среде после запуска приложения RDP.
- Добавлен мастер выбора языка при первом старте Kaspersky Thin Client.

- Добавлена возможность установки персонализированных обоев на рабочий стол Kaspersky Thin Client через Kaspersky Security Center Web Console.
- Добавлена возможность установки персонализированной заставки на экран блокировки Kaspersky Thin Client через Kaspersky Security Center Web Console.
- Добавлена возможность централизованной настройки мониторов через Kaspersky Security Center Web Console, включая следующие параметры:
 - разрешение и ориентация экрана;
 - режим отображения (дублирование или расширение) неосновного экрана.
- Добавлена возможность вручную определять тип подключенного устройства, нераспознанного системой.
- Поддержано перенаправление в удаленную среду беспроводной USB-гарнитуры, клавиатуры и мыши (радиосигнал).
- Добавлена поддержка следующих языков ввода: немецкий (de-DE), франко-швейцарский (fr-CH), немецко-швейцарский (de-CH).
- Добавлена возможность закрепить или полностью скрыть панель подключения в удаленной среде.
- Добавлена возможность [перенаправлять](#) на удаленный рабочий стол РЕД ОС 8.0 и затем на удаленный рабочий стол Windows 10 (если между этими рабочими столами установлен еще один сеанс удаленного рабочего стола) по протоколу RDP следующие токены:
 - Рутокен Lite;
 - JaCarta-2 PKI/ГОСТ.
- Поддержана новая версия [Kaspersky Security Center Web Console](#): 15.3.
- Улучшен дизайн и текст интерфейса пользователя Kaspersky Thin Client и [Kaspersky Security Management Suite](#).

Установка и обновление Kaspersky Thin Client

Процедура установки Kaspersky Thin Client зависит от [формата поставки](#):

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

Установка Kaspersky Thin Client

Перед установкой Kaspersky Thin Client выполните следующие действия:

1. Подготовьте загрузочный USB-накопитель с операционной системой Linux Ubuntu (рекомендованная версия: Ubuntu 20.04).
2. Скопируйте в отдельный раздел на загрузочном USB-накопителе или на отдельный USB-накопитель файлы установки Kaspersky Thin Client, полученные в [комплекте поставки](#):
 - Kaspersky_Thin_Client_<номер версии>_Wyse3040.tar.gz или Kaspersky_Thin_Client_<номер версии>_TN1200.tar.gz – установочный образ;
 - hw_install.sh – скрипт для установки Kaspersky Thin Client.

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

Kaspersky Thin Client поддерживает технологию Secure Boot, которая позволяет UEFI проверять подлинность загружаемых компонентов. Если вы хотите настроить Secure Boot, вы можете получить необходимые ключи у специалистов "Лаборатории Касперского" и воспользоваться инструкцией из [Базы знаний](#) .

Чтобы установить Kaspersky Thin Client на тонком клиенте:

1. Вставьте подготовленный загрузочный USB-накопитель в [соответствующий разъем](#) на тонком клиенте.
2. [Включите тонкий клиент](#) и загрузите образ Ubuntu с загрузочного USB-накопителя, не устанавливая систему на жесткий диск тонкого клиента.

3. В запущенной операционной системе перейдите в директорию с файлами установки Kaspersky Thin Client.

4. Выполните следующую команду:

```
sudo bash ./hw_install.sh -u Kaspersky_Thin_Client_<номер версии>_<название платформы>.tar.gz
```

где:

- ./hw_install.sh – путь к скрипту установки.
- Kaspersky_Thin_Client_<номер версии>_<название платформы>.tar.gz – установочный образ.

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

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

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

Проверить номер текущей версии операционной системы вы можете в [интерфейсе Kaspersky Thin Client](#).

Обновление Kaspersky Thin Client

Вы можете обновить Kaspersky Thin Client с версии 2.0 или 2.0.1 до версии 2.3.

Перед обновлением Kaspersky Thin Client выполните следующие действия:

1. Подготовьте загрузочный USB-накопитель с дистрибутивом Linux. Мы рекомендуем использовать Linux Ubuntu (рекомендованная версия: Ubuntu 20.04).

2. Убедитесь, что в системе установлена утилита OpenSSL. Если нет, установите ее с помощью команды:

```
sudo apt install openssl
```

3. Скопируйте в одну директорию на USB-накопителе следующие файлы из комплекта поставки Kaspersky Thin Client 2.3:

- Архив с установочным образом Kaspersky_Thin_Client_<номер версии>_TN1200.tar.gz.
- Скрипты для установки и обновления:
 - hw_install.sh;
 - hw_update.sh;
 - save_files.sh;
 - restore_files.sh.

Чтобы обновить *Kaspersky Thin Client* на тонком клиенте:

1. Вставьте подготовленный загрузочный USB-накопитель в соответствующий разъем на тонком клиенте.
2. [Включите тонкий клиент](#) и запустите образ Ubuntu с загрузочного USB-накопителя, не устанавливая систему на жесткий диск тонкого клиента. Для этого выберите опцию *Try without installation*.
3. В запущенной операционной системе перейдите в директорию со скриптами и установочным образом Kaspersky Thin Client 2.3.
4. Выполните скрипт обновления с помощью следующей команды:

```
sudo bash ./hw_update.sh -u <путь к архиву с установочным образом Kaspersky Thin Client>
```

Если скрипт обновления завершился успешно, отобразится сообщение *Updated OK!*.

Если во время выполнения скрипта произошла ошибка, [обратитесь в Службу технической поддержки](#).
5. Выключите тонкий клиент и извлеките загрузочный USB-накопитель.

Обновление будет завершено. При следующем включении устройства вы сможете пользоваться функциями Kaspersky Thin Client 2.3.

Интерфейс Kaspersky Thin Client

Интерфейс Kaspersky Thin Client содержит следующие элементы:

- рабочий стол с приложениями;
- панель управления в верхней части окна;
- панель подключения, которая отображается во время удаленной сессии.

Рабочий стол

В центральной части рабочего стола Kaspersky Thin Client отображаются приложения, с помощью которых вы можете подключиться к [удаленной среде](#) 

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

Панель управления

Панель управления Kaspersky Thin Client содержит следующие элементы:

-  – кнопка вызова меню завершения работы.
В этом меню вы можете [выключить](#) или [перезагрузить](#) Kaspersky Thin Client.
-  – кнопка перехода к разделам **Параметры** и **Инструменты**.
В разделе **Параметры** вы можете [настраивать 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](#);
 - просматривать информацию об обновлениях Kaspersky Thin Client;
 - [просматривать действующее Лицензионное соглашение](#);
 - [просматривать информацию о стороннем коде](#);
 - [управлять доступом к параметрам Kaspersky Thin Client](#).
-  – кнопка вызова окна с [информацией о тонком клиенте и контактами технической поддержки](#).
- Информация о [состоянии подключения Kaspersky Thin Client к сети](#) 

-  – кнопка вызова [панели уведомлений](#).
- Кнопка [переключения языка ввода](#) текста с клавиатуры.
- [Дата и время системы](#).
-  – кнопка вызова меню [удаленного управления Kaspersky Thin Client](#).

Панель подключения

[Панель подключения](#) отображается во время [удаленной сессии](#) .

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

-  – кнопка [завершения удаленной сессии](#).
- Имя подключения.
- Статус подключения.
-  – кнопка вызова окна с [информацией о тонком клиенте и контактами технической поддержки](#).
-  – кнопка [блокировки удаленной сессии](#).
-  – кнопка вызова [панели уведомлений](#).
- Значок состояния сети.
-  – кнопка вызова окна [управления устройствами воспроизведения и записи звука](#).
Кнопка отображается, если к тонкому клиенту подключено два или более устройств такого типа.
-  – кнопка вызова окна [управления перенаправленными USB-устройствами](#).
Кнопка отображается [при подключении к удаленной среде, развернутой в инфраструктуре Citrix Workspace](#).

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

- значок приложения;
- текущая дата, установленная в Kaspersky Thin Client;
- текущее время, установленное в Kaspersky Thin Client;
- язык интерфейса Kaspersky Thin Client.

Лицензирование Kaspersky Thin Client

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

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

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

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

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

Чтобы просмотреть текст Лицензионного соглашения,

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

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

Предоставление данных

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

Kaspersky Thin Client сохраняет на тонком клиенте следующую информацию:

- [Журнал событий](#), содержащий технические сведения о работе системы и события, которые Kaspersky Thin Client отправляет на Сервер администрирования Kaspersky Security Center.
- [Журнал аудита](#), содержащий следующие события и данные о них:
 - добавление, замена и переключение сертификата для подключения к Kaspersky Security Center в интерфейсе Kaspersky Thin Client;
 - сброс параметров Kaspersky Thin Client;
 - принятие удаленного подключения к тонкому клиенту;
 - создание нового файла журнала аудита в случае ротации;
 - сохранение и удаление пароля пользователя для автоматического подключения к удаленной среде;
 - включение (вручную и автоматически) и выключение управления Kaspersky Thin Client через Kaspersky Security Center.
- Параметры системы:
 - Дата и время установки Kaspersky Thin Client на тонком клиенте.
 - Имя тонкого клиента.
 - Текущая установленная версия Kaspersky Thin Client.
 - Язык интерфейса Kaspersky Thin Client.
 - Список языков, доступных для ввода текста с клавиатуры.
 - Месторасположение (координаты) панели подключения.
 - Время последнего использования сертификатов для проверки подлинности подключения к следующим узлам: брокерам; удаленным рабочим столам или виртуальным приложениям по протоколу RDP; виртуальным рабочим столам, развернутым в инфраструктуре Базис.WorkPlace; удаленной среде через приложение Web Access; серверу журналирования.
 - Устройство записи и воспроизведения звука, выбранное как основное.
 - Список приложений, которые отображаются на рабочем столе Kaspersky Thin Client.
 - Приложение, выбранное для автоматического запуска.
 - Список нераспознанных USB-устройств, тип которых определен вручную.

- Файлы обоев рабочего стола и экрана блокировки, установленных на тонком клиенте, и их метаданные.
- Параметры подключенных мониторов:
 - информация о том, какой из мониторов является основным, а какой – дополнительным;
 - идентификатор основного и дополнительного монитора;
 - разрешение основного и дополнительного монитора;
 - ориентация основного и дополнительного монитора;
 - режим отображения для дополнительного монитора.
- Параметры взаимодействия с Kaspersky Security Center:
 - адрес (имя или IP-адрес и порт) Сервера администрирования Kaspersky Security Center;
 - способ подключения Kaspersky Security Center (вручную или по DHCP);
 - набор идентификаторов Kaspersky Thin Client для подключения к Kaspersky Security Center;
 - период синхронизации Kaspersky Thin Client с Kaspersky Security Center в минутах;
 - количество сертификатов, полученных от Kaspersky Security Center для проверки подлинности подключения Kaspersky Thin Client к следующим узлам: брокерам; удаленным рабочим столам или виртуальным приложениям по протоколу RDP; виртуальным рабочим столам, развернутым в инфраструктуре Базис.WorkPlace; удаленной среде через приложение Web Access; серверу журналирования;
 - отпечаток текущего сертификата для проверки подлинности подключения Kaspersky Thin Client к Kaspersky Security Center;
 - параметры именования тонкого клиента, заданные администратором Kaspersky Security Center (имя, идентификатор тонкого клиента и дополнительная информация);
 - набор секретов для подтверждения действия пользователя в интерфейсе Kaspersky Thin Client: сброс параметров и данных, отключение тонкого клиента от Kaspersky Security Center и изменение сертификата для подключения тонкого клиента к Kaspersky Security Center;
 - контактные данные Службы технической поддержки;
 - файлы сертификатов для проверки подлинности подключения Kaspersky Thin Client к Kaspersky Security Center.
- Параметры подключения в приложении Web Access:
 - веб-адрес сервера;
 - файлы сертификатов для проверки подлинности подключения;
 - данные, необходимые для работы в удаленной среде (например, файлы cookies).

- Параметры подключения к инфраструктуре Базис.WorkPlace:
 - адрес (имя или IP-адрес и порт) диспетчера подключений Базис.WorkPlace;
 - имя пользователя для подключения к диспетчеру подключений Базис.WorkPlace;
 - файлы сертификатов для проверки подлинности брокера при подключении к удаленному рабочему столу под управлением Базис.WorkPlace;
 - идентификатор Kaspersky Thin Client;
 - количество попыток повторного подключения;
 - профиль соединения Kaspersky Thin Client с брокером Базис.WorkPlace;
 - параметры перенаправления на удаленный рабочий стол периферийных устройств: разрешено ли перенаправление USB-накопителей и смарт-карт;
 - включено ли использование двух мониторов;
 - список адресов (имя или IP-адрес и порт) диспетчеров подключений геораспределенной инсталляции под управлением Базис.WorkPlace.
- Параметры подключения к RDP-серверу:
 - Адрес (имя или IP-адрес и порт) сервера Remote Desktop Connection Broker.
 - Домен и имя пользователя для подключения к серверу Remote Desktop Connection Broker.
 - Идентификатор коллекции Remote Desktop Connection Broker.
 - Псевдоним приложения.
 - Файлы сертификатов для проверки подлинности сервера Remote Desktop Connection Broker при подключении к удаленному рабочему столу или виртуальному приложению по протоколу RDP.
 - Параметры перенаправления на удаленный рабочий стол периферийных устройств:
 - разрешено ли перенаправление USB-накопителей;
 - разрешено ли перенаправление смарт-карт;
 - разрешено ли перенаправление принтеров;
 - разрешено ли перенаправление устройств воспроизведения звука;
 - разрешено ли перенаправление устройств записи звука;
 - разрешено ли перенаправление видеопотока от веб-камеры;
 - разрешено ли перенаправление устройств сканирования.
 - Включено ли использование двух мониторов.

- Включено ли автоматическое подключение к удаленному рабочему столу или виртуальному приложению при разрыве соединения.
- Параметры внешнего вида окон:
 - включено ли сглаживание шрифтов;
 - включена ли анимация меню;
 - включено ли отображение фона рабочего стола;
 - включено ли отображение содержимого окна при перемещении;
 - включено ли использование тем в Microsoft Windows.
- Включено ли автоматическое подключение к удаленному рабочему столу:
 - пароль для подключения к удаленному рабочему столу, только если выбрана опция автоматического подключения.
- Параметры подключения к удаленному рабочему столу тонкого клиента по протоколу RDP:
 - сертификат RDP-сервера;
 - секрет для подключения;
 - режим подключения к удаленному рабочему столу тонкого клиента (автоматически, с подтверждением пользователя или запрещено);
 - режим отображения содержания удаленной среды пользователя (автоматически, с подтверждением пользователя или запрещено).
- Параметры сети:
 - включена ли автоматическая настройка сети по DHCP;
 - IP-адрес тонкого клиента;
 - маска подсети;
 - список IP-адресов DNS-серверов;
 - IP-адрес сетевого шлюза.
- Параметры энергосбережения: количество минут до выключения монитора и количество минут до выключения тонкого клиента при бездействии Kaspersky Thin Client.
- Параметры подключения к серверу журналирования:
 - адрес (имя или IP-адрес и порт) сервера журналирования для отправки журналов событий и аудита;
 - файлы сертификатов для проверки подлинности сервера журналирования при подключении Kaspersky Thin Client к этому серверу.

- Параметры даты и времени:
 - дата и время, полученные от Сервера администрирования при последней синхронизации с Kaspersky Security Center;
 - часовой пояс.
- Информация о доступных и скачанных обновлениях Kaspersky Thin Client:
 - статус доступности обновления;
 - статус установки обновления;
 - статус доставки обновления;
 - данные доступного обновления: версия Kaspersky Thin Client, название, дата и время выпуска, важность;
 - время последней успешной проверки обновления;
 - время успешной установки обновления.
- Информация о Лицензионных соглашениях Kaspersky Thin Client:
 - идентификаторы Лицензионных соглашений;
 - тексты Лицензионных соглашений на русском, английском, испанском и бразильском португальском языках;
 - информация о факте принятия Лицензионных соглашений;
 - информация о датах выпуска Лицензионных соглашений.

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

Включение и первый запуск Kaspersky Thin Client

Перед началом работы с Kaspersky Thin Client требуется подключить к тонкому клиенту мышь, клавиатуру и монитор/мониторы, используя соответствующие разъемы. Kaspersky Thin Client также поддерживает подключение [периферийных устройств](#) во время работы системы.

Обзор аппаратных компонентов тонкого клиента (в том числе элементов управления и разъемов) не приводится в этом документе, поскольку содержится в документации производителя устройства. Модели тонких клиентов, на которые устанавливается Kaspersky Thin Client, см. в [разделе с основной информацией о Kaspersky Thin Client](#).

Для начала работы с Kaspersky Thin Client необходимо включить тонкий клиент.

Чтобы включить Kaspersky Thin Client и пройти процедуру первого запуска:

1. Нажмите кнопку включения / выключения питания на тонком клиенте.

На устройстве начнет загружаться Kaspersky Thin Client. После загрузки системы отобразится окно выбора языка интерфейса.

2. Выберите необходимый язык интерфейса и нажмите на кнопку **Далее**.

Отобразится окно с текстом [Лицензионного соглашения](#) на выбранном языке.

3. Ознакомьтесь с текстом Лицензионного соглашения и нажмите на кнопку **Принять**.

Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать запуск и не должны использовать Kaspersky Thin Client.

Процедура первого запуска будет завершена, отобразится [рабочий стол](#) Kaspersky Thin Client.

При последующих включениях тонкого клиента после загрузки системы будет отображаться рабочий стол.

Перезагрузка и выключение Kaspersky Thin Client

По завершении работы в Kaspersky Thin Client необходимо выключать тонкий клиент.

Чтобы выключить Kaspersky Thin Client:

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

Kaspersky Thin Client будет выключена.

Вы можете перезагрузить Kaspersky Thin Client, например если требуется применить выбранный язык интерфейса Kaspersky Thin Client или установить обновления системы.

Чтобы перезагрузить Kaspersky Thin Client:

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

Kaspersky Thin Client будет перезагружена.

Использование сертификатов в Kaspersky Thin Client

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

В Kaspersky Thin Client сертификаты используются в следующих целях:

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

Пользователь может самостоятельно [принять или отклонить сертификат в интерфейсе Kaspersky Thin Client](#), если соблюдаются следующие условия:

- пользователь впервые подключается к [удаленной среде](#) или к [серверу журналирования](#) в интерфейсе Kaspersky Thin Client;
- тонкий клиент находится в одном из следующих состояний:
 - не подключен к Kaspersky Security Center;
 - не добавлен в группу администрирования;
 - для группы администрирования, в которой состоит тонкий клиент, не [добавлены сертификаты для подключения к удаленной среде](#).

Все принятые сертификаты будут сохраняться в хранилище тонкого клиента. В такой ситуации пользователь может подключаться в том числе к тем узлам и использовать те сертификаты, которые не контролирует администратор.

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

Рекомендуется обновлять назначенные сертификаты в следующих случаях:

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

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

Настройка Kaspersky Thin Client

Этот раздел содержит информацию о настройке Kaspersky Thin Client.

Сценарий: быстрый старт для администратора

В этом разделе приводится последовательность действий, которые требуется выполнить, чтобы настроить Kaspersky Thin Client и Kaspersky Security Center, а также установить между ними соединение. Эти действия необходимо выполнить администратору или другому квалифицированному специалисту из вашей организации, который сможет удостовериться в подлинности принимаемого сертификата подключения к Kaspersky Security Center.

Инструкции по установке Kaspersky Thin Client на тонкий клиент приведены в [отдельной статье](#).

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

Kaspersky Thin Client поддерживает технологию Secure Boot, которая позволяет UEFI проверять подлинность загружаемых компонентов. Если вы хотите настроить Secure Boot, вы можете получить необходимые ключи у специалистов "Лаборатории Касперского" и воспользоваться инструкцией из [Базы знаний](#).

Для ознакомления с функциональностью вы можете просмотреть обучающее видео (см. ниже).



<https://rutube.ru/video/private/9c5c830b7745d541b6a1ea4d44fb312c/?p=5Kj7Jttqgt1em4SRiQnmEw>

Kaspersky Thin Client: быстрый старт

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

1 Установка Kaspersky Security Center

Загрузите дистрибутив Kaspersky Security Center и установите полную версию Kaspersky Security Center на сервере. Дистрибутив полной версии Kaspersky Security Center включает Kaspersky Security Center Web Console. При установке рекомендуется выбрать стандартную установку. Подробную информацию об установке Kaspersky Security Center см. в [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-плагинов управления Kaspersky Security Management Suite

В Kaspersky Security Center Web Console установите [веб-плагин управления Kaspersky Security Management Suite](#).

4 Подготовка портов

Kaspersky Thin Client использует для подключения к Kaspersky Security Center мобильный протокол. На Сервере администрирования Kaspersky Security Center включите использование по протоколу TCP порта, доступ к которому вы настроили на шаге 2 этого сценария. Подробнее о включении на Сервере администрирования Kaspersky Security Center порта по протоколу TCP см. в [онлайн-справке Kaspersky Security Center](#).

5 Включение Kaspersky Thin Client

[Включите Kaspersky Thin Client](#) и дождитесь загрузки системы. Выберите язык 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 тонкого клиента с Kaspersky Thin Client в группу администрирования

В Web Console [добавьте тонкий клиент в группу администрирования](#) вручную или настройте автоматизированное перемещение устройств.

9 Создание активной политики в Kaspersky Security Center

В Web Console [создайте активную политику](#) для группы администрирования.

10 Назначение сертификатов для группы администрирования

[Назначьте сертификаты](#) для подключения к удаленной среде и к серверу журналирования для группы администрирования. Также рекомендуется [добавить сертификат](#) для подключения Kaspersky Thin Client к Kaspersky Security Center.

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

Сценарий: назначение сертификатов для группы тонких клиентов

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

Предварительно требуется [установить и настроить Kaspersky Security Center](#).

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

1 Настройка подключения к Kaspersky Security Center

В интерфейсе Kaspersky Thin Client [настройте подключение к Kaspersky Security Center](#).

2 Добавление тонких клиентов в группу администрирования

В интерфейсе Web Console [добавьте тонкий клиент в группу администрирования](#), если он находится в нераспределенных устройствах.

3 Создание активной политики Kaspersky Security Center для Kaspersky Thin Client

В интерфейсе Web Console [создайте активную политику](#) для необходимой группы администрирования.

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

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

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

Сценарий: миграция тонких клиентов на новый Сервер Kaspersky Security Center

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

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

1 Установка нового Сервера администрирования Kaspersky Security Center

Загрузите дистрибутив Kaspersky Security Center и установите полную версию Kaspersky Security Center на сервере. Дистрибутив полной версии Kaspersky Security Center включает Kaspersky Security Center Web Console. При установке рекомендуется выбрать стандартную установку. Подробную информацию об установке Kaspersky Security Center см. в [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-плагинов управления Kaspersky Security Management Suite

В Web Console для нового Сервера администрирования Kaspersky Security Center установите [веб-плагин управления Kaspersky Security Management Suite](#).

4 Подготовка портов

Kaspersky Thin Client использует для подключения к Kaspersky Security Center мобильный протокол. На Сервере администрирования Kaspersky Security Center включите использование по протоколу TCP порта, доступ к которому вы настроили на шаге 2 этого сценария. Подробнее о включении на Сервере администрирования Kaspersky Security Center порта по протоколу TCP см. в [онлайн-справке Kaspersky Security Center](#).

5 Включение Kaspersky Thin Client

[Включите Kaspersky Thin Client](#) и дождитесь загрузки системы.

6 Создание активной политики Kaspersky Security Center для Kaspersky Thin Client

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

7 Обновление сертификата безопасности для подключения к Kaspersky Security Center

[Выпустите сертификат](#), который необходимо сохранить на текущем Сервере администрирования Kaspersky Security Center как резервный и затем использовать на новом Сервере как основной.

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

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

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

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

Настройка общих параметров

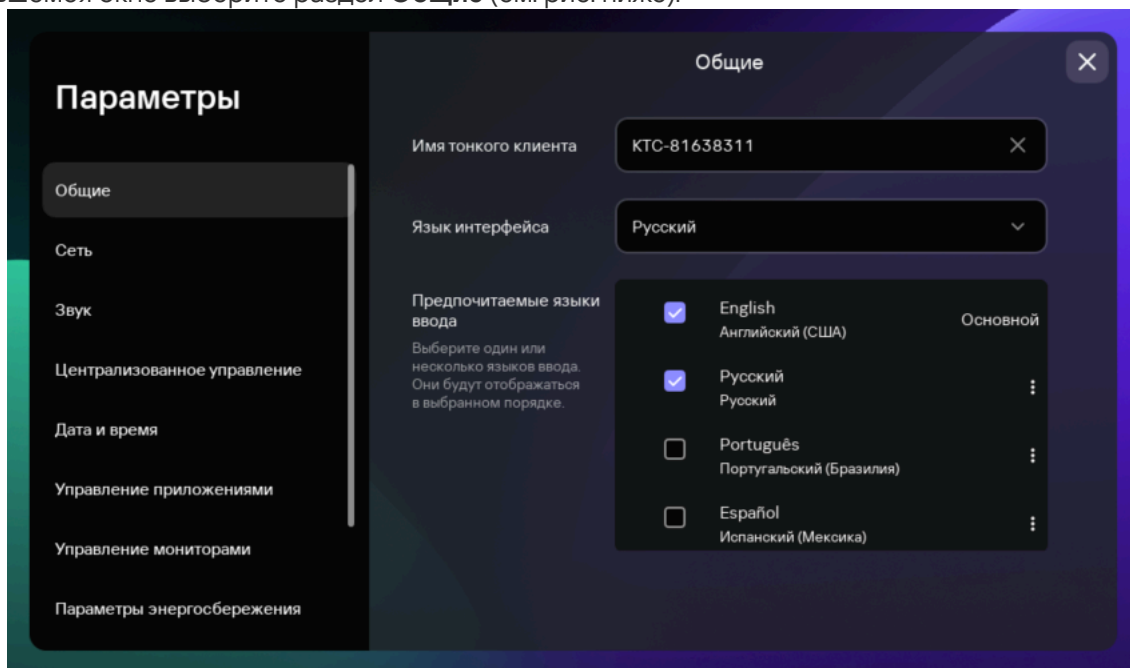
В интерфейсе Kaspersky Thin Client вы можете настроить общие параметры тонкого клиента. Например, вы можете указать имя тонкого клиента, которое будет отображаться в панели задач Kaspersky Thin Client и в Kaspersky Security Center Web Console, а также выбрать язык интерфейса Kaspersky Thin Client.

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

Указанные в этой статье параметры также могут быть [скрыты в Kaspersky Thin Client](#).

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 2.3 поддерживает следующие языки интерфейса: русский, английский (США), испанский (Мексика) и португальский (Бразилия).
5. В раскрывающемся списке **Предпочитаемые языки ввода** выберите один или несколько языков. Kaspersky Thin Client поддерживает следующие языки ввода: русский, английский (США), испанский (Мексика), немецкий (стандартный и Швейцария), португальский (Бразилия), французский (Швейцария). Выбранные языки будут отображаться в панели управления Kaspersky Thin Client в том порядке, в котором вы их выбрали, и будут доступны для переключения языка ввода текста с клавиатуры.

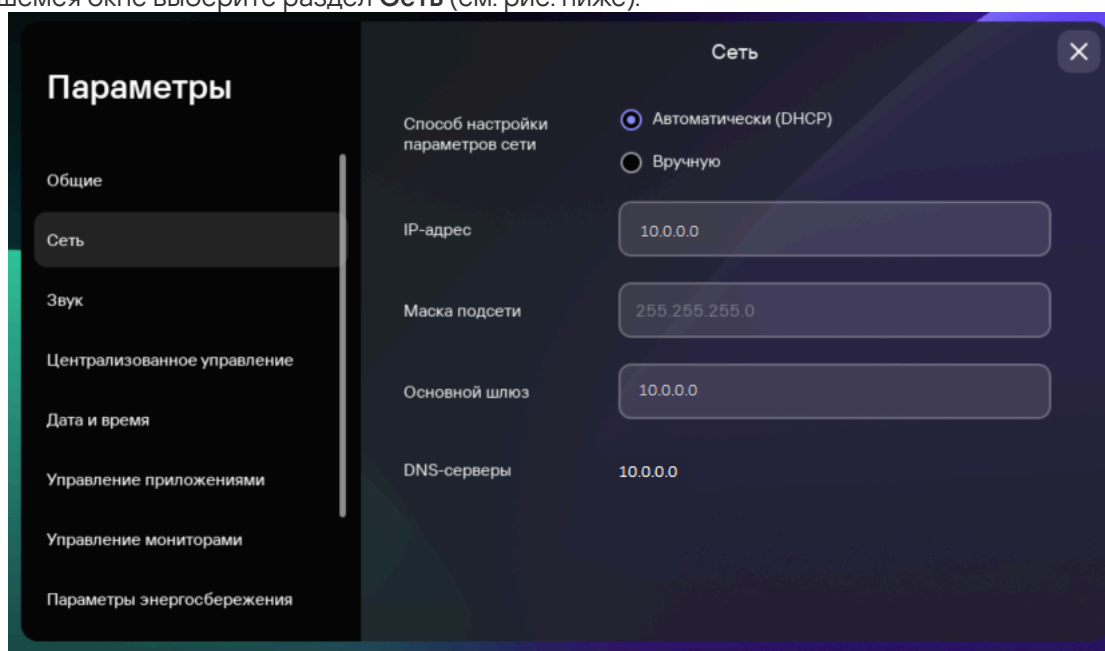
Изменения вступят в силу после [перезагрузки тонкого клиента](#).

Настройка параметров сети

Вы интерфейсе Kaspersky Thin Client вы можете настроить параметры 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 **Способ настройки 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 **Способ настройки 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.

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

Управление устройствами воспроизведения и записи звука

Вы можете подключить к тонкому клиенту с Kaspersky Thin Client несколько устройств воспроизведения и записи звука через разъем mini-jack или USB, чтобы перенаправить их в удаленную среду. В интерфейсе Kaspersky Thin Client вы можете [переключаться между подключенными устройствами](#).

Управление громкостью и другими параметрами звука и видео выполняется в удаленной среде.

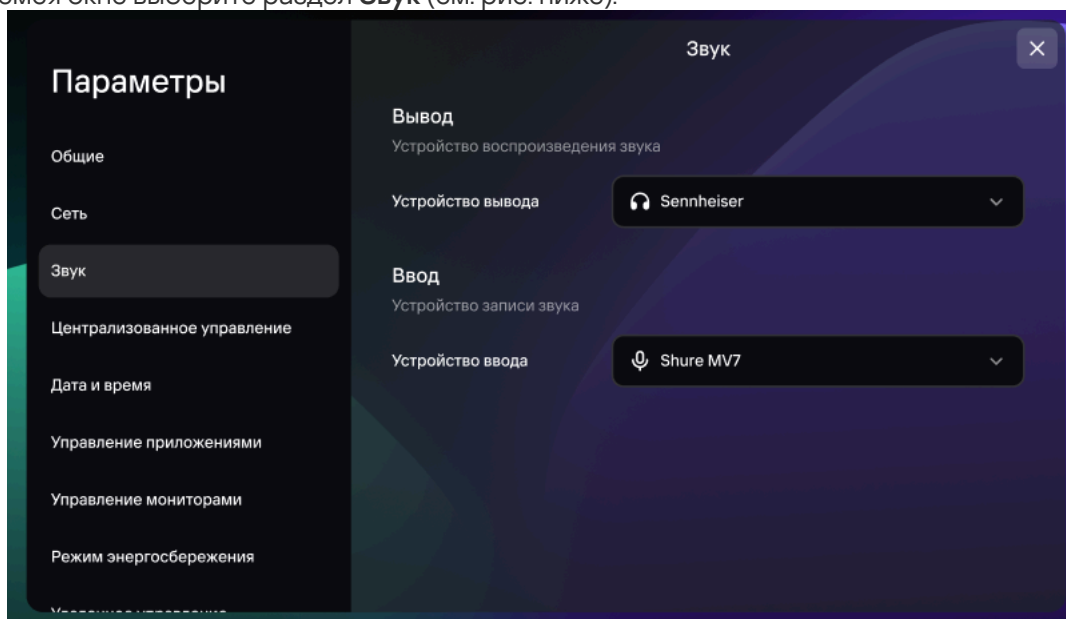
Подключение через mini-jack не поддерживается на тонких клиентах модели Dell Wyse 3040.

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

Указанные в этой статье параметры также могут быть [скрыты в Kaspersky Thin Client](#).

Чтобы выбрать устройства воспроизведения и записи звука в 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 **Звук** (см. рис. ниже).



Параметры. Раздел Звук

3. В раскрывающемся списке **Устройство вывода** выберите устройство воспроизведения звука.
4. В раскрывающемся списке **Устройство ввода** выберите устройство записи звука.

Вы также можете использовать устройства воспроизведения и записи звука в удаленной среде и [переключаться между ними в панели подключения](#).

Настройка параметров подключения Kaspersky Thin Client к Kaspersky Security Center

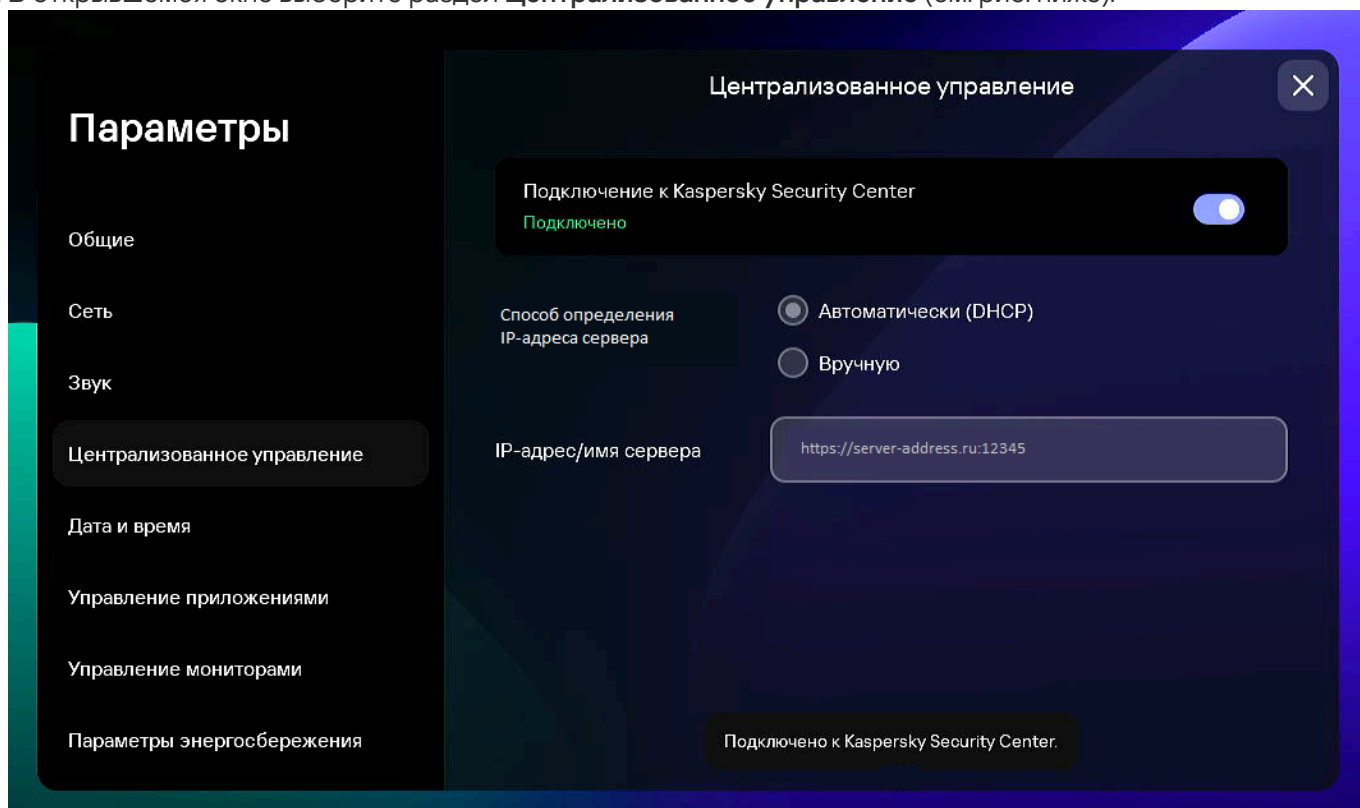
Для управления тонким клиентом через Web Console необходимо настроить параметры подключения Kaspersky Thin Client к Серверу администрирования Kaspersky Security Center (далее также Kaspersky Security Center).

Рекомендуется настраивать подключение Kaspersky Thin Client к Kaspersky Security Center при помощи квалифицированного специалиста из вашей организации, который сможет удостовериться в подлинности принимаемого сертификата.

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

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

1. В панели управления Kaspersky Thin Client нажмите на кнопку  и в открывшемся меню выберите **Параметры**.
2. В открывшемся окне выберите раздел **Централизованное управление** (см. рис. ниже).



Параметры. Раздел Централизованное управление

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

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

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

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

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

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

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

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

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

Изменение параметров подключения Kaspersky Thin Client к Kaspersky Security Center

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

Указанные в этой статье параметры также могут быть [скрыты в Kaspersky Thin Client](#).

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

1. В панели управления Kaspersky Thin Client нажмите на кнопку  и в открывшемся меню выберите **Параметры**.
2. В открывшемся окне выберите раздел **Централизованное управление**.
3. Переведите переключатель **Подключение к Kaspersky Security Center** в положение выключено.
4. В открывшемся окне **Подтверждение отключения** посмотрите и запомните код подтверждения для отключения Kaspersky Thin Client от Kaspersky Security Center, сообщите его администратору Kaspersky Security Center. Контакты администратора указаны в окне **Подтверждение отключения**. Администратор в ответ должен сообщить код подтверждения.
5. Нажмите на кнопку **Далее**.
6. В открывшемся окне **Код подтверждения** введите код, который сообщил вам администратор Kaspersky Security Center и нажмите на кнопку **Подтвердить**.
Kaspersky Thin Client будет отключен от управления через Kaspersky Security Center.
7. В окне **Централизованное управление** вручную [настройте параметры подключения к Kaspersky Security Center](#).
8. Переведите переключатель **Подключение к Kaspersky Security Center** в положение включено.

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

Настройка даты и времени

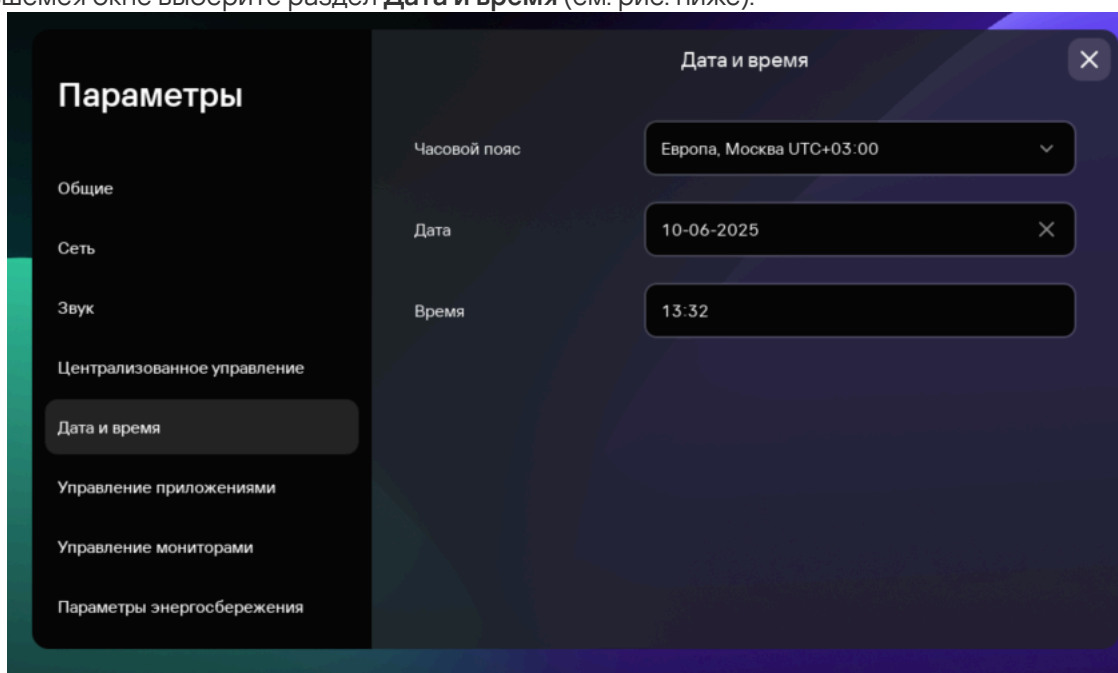
Тонкий клиент, подключенный к Kaspersky Security Center, получает дату и время от Сервера администрирования Kaspersky Security Center. Вы можете вручную изменить дату и время Kaspersky Thin Client только если система не управляется через Kaspersky Security Center.

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

Указанные в этой статье параметры также могут быть [скрыты в Kaspersky Thin Client](#).

Чтобы изменить дату и время Kaspersky Thin Client:

1. В панели управления Kaspersky Thin Client нажмите на кнопку  и в открывшемся меню выберите **Параметры**.
2. В открывшемся окне выберите раздел **Дата и время** (см. рис. ниже).



Параметры. Раздел Дата и время

3. Настройте параметры даты и времени:

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

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

Настройка автоматического запуска и отображения приложений

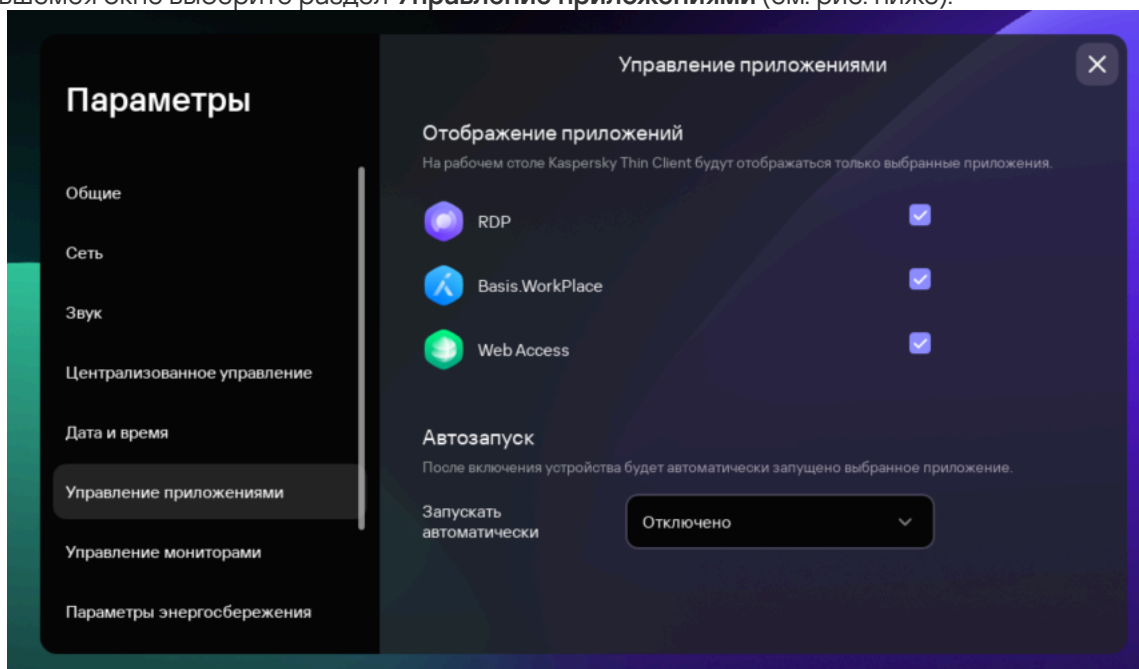
Вы можете выбрать [приложение](#), которое будет автоматически запускаться после включения устройства и загрузки системы, а также указать, какие приложения будут отображаться на рабочем столе Kaspersky Thin Client.

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

Указанные в этой статье параметры также могут быть [скрыты в Kaspersky Thin Client](#).

Чтобы настроить автоматический запуск и отображение приложений:

1. В панели управления Kaspersky Thin Client нажмите на кнопку  и в открывшемся меню выберите **Параметры**.
2. В открывшемся окне выберите раздел **Управление приложениями** (см. рис. ниже).



Параметры. Раздел Управление приложениями

3. В блоке **Отображение приложений** установите флажки напротив приложений, которые будут отображаться на рабочем столе Kaspersky Thin Client.
4. В раскрывающемся списке **Запускать автоматически** выберите приложение, которое будет автоматически запускаться после включения устройства и загрузки системы. При выборе значения **Отключено** автоматический запуск будет выключен.

Изменения будут сохранены и применены.

Вы также можете [настроить автоматическое подключение к удаленной среде в приложении RDP](#), чтобы после загрузки Kaspersky Thin Client запускалась удаленная сессия.

Настройка мониторов и экранов

Kaspersky Thin Client поддерживает подключение двух мониторов.

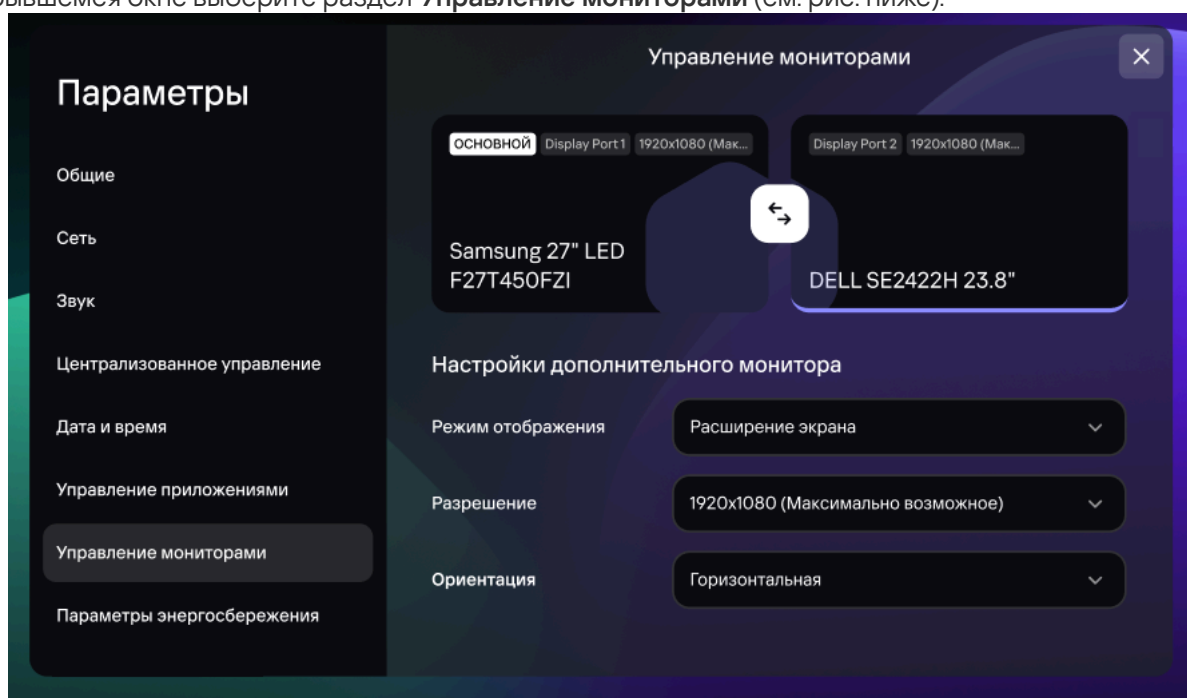
При подключении двух мониторов система считает один из них основным, другой – дополнительным. На экране основного монитора отображается панель подключения во время [удаленной сессии](#) . Экран дополнительного монитора расширяет или дублирует изображение основного. В интерфейсе Kaspersky Thin Client вы можете выбрать, какой монитор будет считаться основным (далее также "изменить взаимное расположение мониторов").

Если вы хотите, чтобы экран удаленной сессии отображался на обоих мониторах, включите их использование в параметрах подключения к удаленной среде в приложении [RDP](#) или [Базис.WorkPlace](#).

В интерфейсе Kaspersky Thin Client вы можете посмотреть информацию о подключенных к тонкому клиенту мониторах, а также изменить режим отображения экранов или настроить параметры каждого из них отдельно.

Чтобы настроить мониторы и экраны:

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).



Параметры. Раздел Управление мониторами

3. Если к вашему тонкому клиенту подключено два монитора, вы можете изменить их взаимное расположение. Для этого нажмите на кнопку .

4. Если вы хотите настроить экран определенного монитора, выберите его. Для этого нажмите на его схематичное изображение.

Чтобы выделить настраиваемый монитор, наведите курсор мыши на схематичное изображение. На экране соответствующего монитора отобразится красная рамка.

5. Настройте необходимые параметры:

- В раскрывающемся списке **Режим отображения** выберите способ вывода изображения на экраны мониторов:
 - **Расширение экрана** – изображение распределяется между двумя мониторами.
 - **Дублирование экрана** – изображение экрана основного монитора дублируется на дополнительном. Если выбран этот параметр, настройки, перечисленные ниже, будут недоступны для дополнительного экрана.

Параметр отображается только если к тонкому клиенту подключено два монитора.

- В раскрывающемся списке **Разрешение** выберите необходимое разрешение для выбранного экрана. Поддерживаемые разрешения перечислены в [разделе с аппаратными и программными требованиями](#). Если выбрано значение **Максимально возможное**, будет установлено наибольшее значение параметра, поддерживаемое монитором и Kaspersky Thin Client.
- В раскрывающемся списке **Ориентация** выберите положение экрана на мониторе:
 - **Горизонтальная** – стандартное положение экрана.
 - **Перевернутая горизонтальная** – экран повернут на 180°.
 - **Вертикальная** – экран повернут на 90°.
 - **Перевернутая вертикальная** – экран повернут на 270°.

При изменении каждого параметра будет отображаться окно с обратным отсчетом.

6. В отобразившемся окне подтвердите изменения, нажав **Сохранить**. Если вы хотите отменить изменения и вернуться к настройке параметров, нажмите **Отмена**.

Изменения будут сохранены.

Настройка параметров энергосбережения

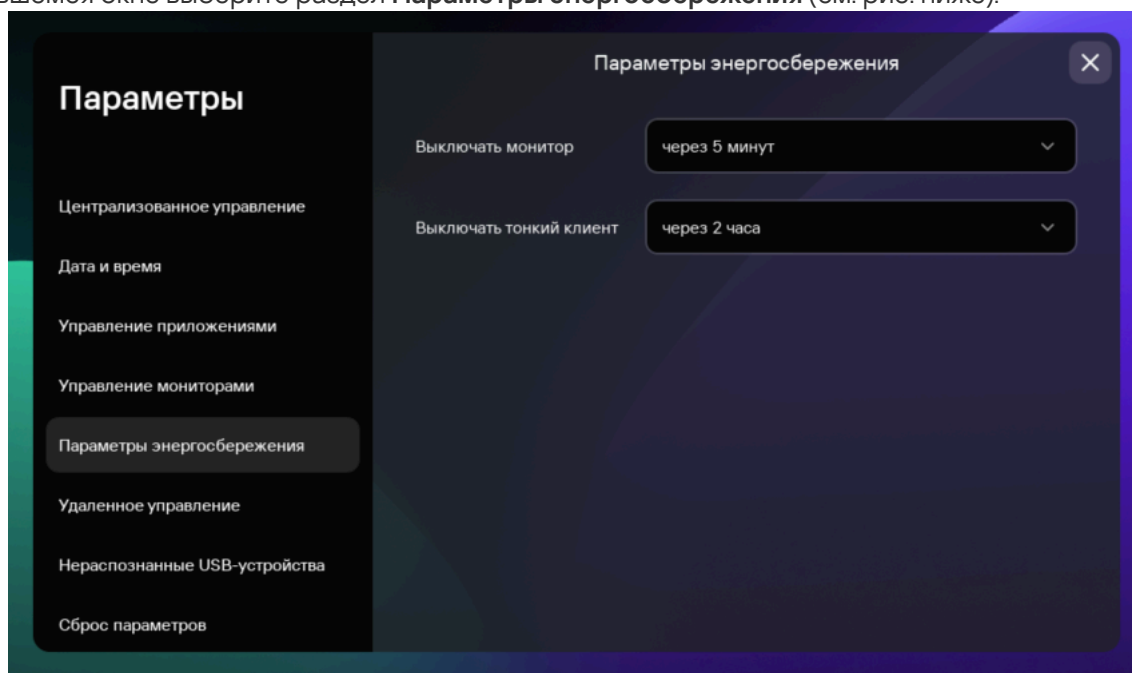
Если тонкий клиент входит в [группу администрирования](#), значения параметров, указанных в этой статье, могут быть принудительно заданы через Web Console. В этом случае настройка данных параметров в интерфейсе Kaspersky Thin Client будет недоступна.

Указанные в этой статье параметры также могут быть [скрыты в Kaspersky Thin Client](#).

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

Чтобы настроить параметры энергосбережения:

1. В панели управления Kaspersky Thin Client нажмите на кнопку  и в открывшемся меню выберите **Параметры**.
2. В открывшемся окне выберите раздел **Параметры энергосбережения** (см. рис. ниже).



Параметры. Раздел Параметры энергосбережения

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

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

Настройка параметров удаленного управления тонким клиентом в интерфейсе Kaspersky Thin Client

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

Указанные в этой статье параметры также могут быть [скрыты в Kaspersky Thin Client](#).

В интерфейсе Kaspersky Thin Client вы можете настроить следующие параметры [удаленного управления](#):

- Режим доступа к удаленному управлению.

Определяет условия и порядок подключения к тонкому клиенту.

- Режим доступа к удаленной сессии, запущенной на тонком клиенте в момент подключения к нему (далее также "экран удаленной среды").

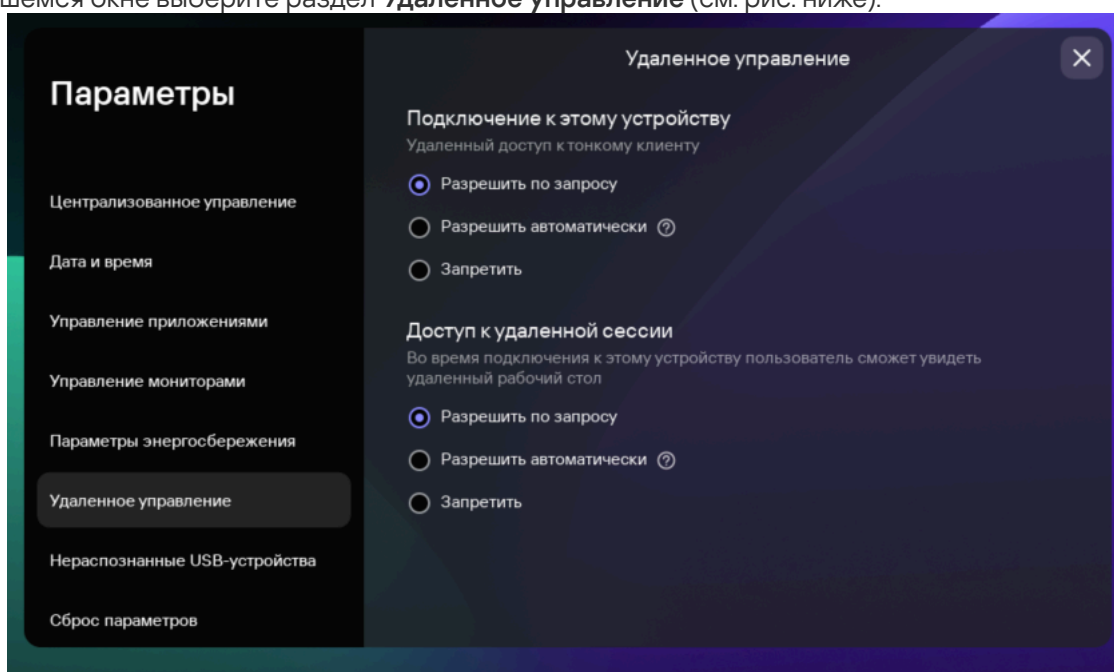
Ограничение доступа к экрану удаленной среды может понадобиться, если пользователь тонкого клиента работает с чувствительными или конфиденциальными данными.

Чтобы настроить параметры удаленного управления тонким клиентом:

1. [Включите тонкий клиент](#).

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

3. В открывшемся окне выберите раздел **Удаленное управление** (см. рис. ниже).



Параметры. Раздел Удаленное управление

4. В блоке параметров **Подключение к этому устройству** выберите режим доступа к удаленному управлению тонким клиентом:

- **Разрешить автоматически**

В этом режиме администратор сможет удаленно подключиться к тонкому клиенту после того, как пользователь [примет запрос на удаленное управление в интерфейсе Kaspersky Thin Client](#). Если пользователь отклонит запрос, подключение завершится. Если в течение 30 секунд ответа не последует, подключение установится автоматически.

Используйте этот режим только если тонкий клиент подключен к Kaspersky Security Center для обеспечения безопасности устройства.

- **Разрешить по запросу**

В этом режиме администратор сможет удаленно подключиться к тонкому клиенту только после того, как пользователь [примет запрос на удаленное управление в интерфейсе Kaspersky Thin Client](#). Если пользователь отклонит запрос, подключение завершится.

- **Запретить**

В этом режиме администратор не сможет удаленно подключаться к тонкому клиенту.

Если вы установили режим **Разрешить автоматически** или **Разрешить по запросу**, отобразится блок параметров **Доступ к удаленной сессии**.

5. В блоке параметров **Доступ к удаленной сессии** выберите режим доступа к экрану удаленной среды:

- **Разрешить автоматически**

В этом режиме после подключения к тонкому клиенту администратор сможет получать доступ к экрану удаленной среды без подтверждения пользователя.

- **Разрешить по запросу**

В этом режиме после подключения к тонкому клиенту администратор сможет получать доступ к экрану удаленной среды только после того, как пользователь [подтвердит запрос на этот доступ в интерфейсе Kaspersky Thin Client](#).

- **Запретить**

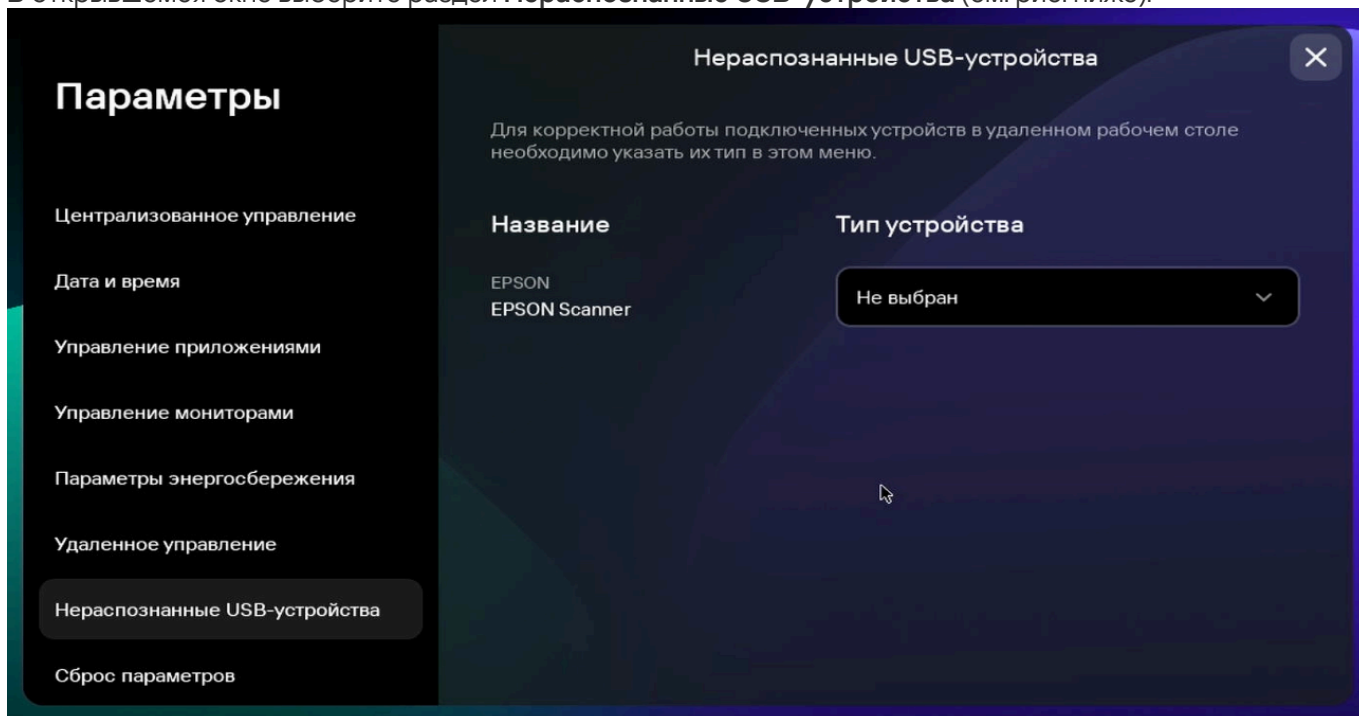
В этом режиме администратор не сможет перейти к удаленному управлению тонким клиентом, пока пользователь самостоятельно не [завершит удаленную сессию](#).

Изменение типа нераспознанных USB-устройств

По умолчанию Kaspersky Thin Client автоматически определяет тип [поддерживаемого USB-устройства](#), подключенного к тонкому клиенту. Если системе не удалось определить тип подключенного устройства (далее также "нераспознанное устройство"), для его корректной работы необходимо выбрать тип вручную в интерфейсе Kaspersky Thin Client.

Чтобы вручную изменить тип нераспознанного USB-устройства:

1. В панели управления Kaspersky Thin Client нажмите на кнопку  и в открывшемся меню выберите **Параметры**.
2. В открывшемся окне выберите раздел **Нераспознанные USB-устройства** (см. рис. ниже).



Параметры. Раздел Нераспознанные USB-устройства

Отобразится список USB-устройств, тип которых система не смогла определить. Для каждого устройства отображается название модели и производитель, если системе удалось получить эту информацию.

Если нераспознанные устройства не обнаружены, список будет пуст.

3. В раскрывающемся списке напротив названия необходимого устройства выберите его тип.

В текущей версии Kaspersky Thin Client доступен только следующий тип USB-устройства: сканер.

Тип нераспознанного устройства будет изменен и сохранен в системе. Вы сможете [перенаправлять устройство в удаленную среду](#).

Сброс параметров Kaspersky Thin Client

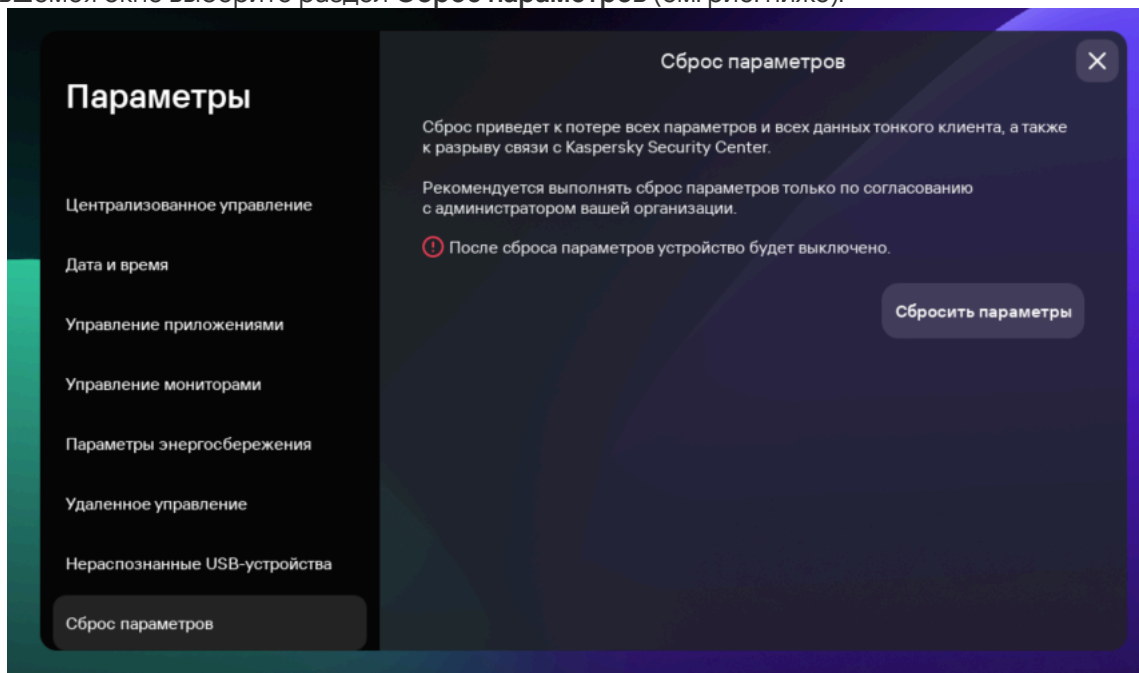
Сброс параметров приведет к потере всех установленных значений параметров и всех данных Kaspersky Thin Client (кроме [журнала аудита](#) и даты системы), а также к разрыву связи между устройством и Kaspersky Security Center. Рекомендуется выполнять сброс только по согласованию с администратором вашей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

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

Указанные в этой статье параметры также могут быть [скрыты в Kaspersky Thin Client](#).

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

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

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

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

Откроется окно **Подтверждение сброса**, в котором отображается код подтверждения.

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

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

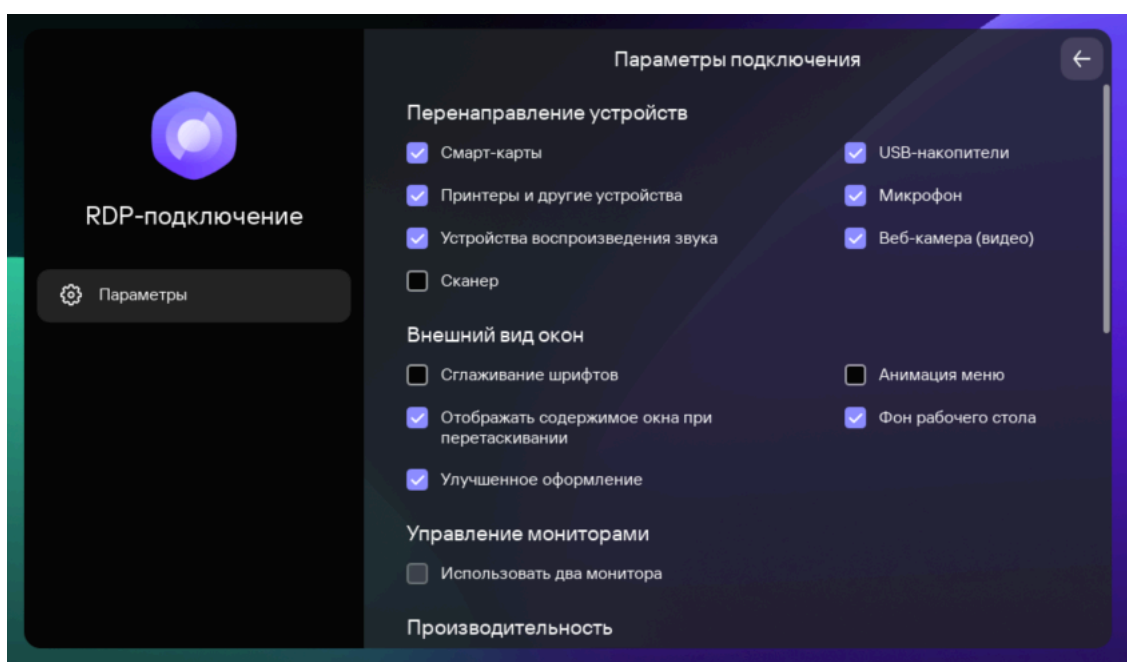
Настройка параметров подключения к удаленной среде с помощью приложения RDP

В приложении RDP вы можете настроить параметры [подключения к виртуальному приложению или удаленному рабочему столу](#) по протоколу RDP, в том числе автоматическое подключение к удаленной среде.

Чтобы настроить параметры подключения к удаленной среде в приложении RDP:

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

Откроется окно настройки параметров подключения к удаленной среде (см. рис. ниже).



Окно настройки параметров подключения к удаленной среде в приложении RDP

3. В блоке параметров **Перенаправление устройств** выберите устройства, которые необходимо перенаправить в удаленную среду: **Смарт-карты**, **USB-накопители**, **Принтеры и другие устройства**, **Микрофон**, **Устройства воспроизведения звука**, **Веб-камера (видео)**, **Сканер**.

Управление громкостью и другими параметрами звука и видео выполняется в удаленной среде.

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

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 удаленной среды выводилось на оба монитора, в блоке **Управление мониторами** установите флажок **Использовать два монитора**.
6. Если требуется улучшить производительность при подключении к удаленным рабочим столам или приложениям, в блоке **Производительность** установите флажок **Улучшить графическую производительность**.
7. Для автоматического [подключения к удаленному рабочему столу или виртуальному приложению](#) при запуске приложения RDP, в блоке **Автоподключение** установите флажок **Подключаться автоматически**.
- Для активации функции необходимо однократно подключиться к удаленной среде вручную и отключиться от нее. При этом в хранилище тонкого клиента будут сохранены следующие данные для подключения к RDP-серверу: имя пользователя, адрес сервера и пароль. При следующем запуске приложения RDP автоматически начнется подключение к удаленной среде с использованием этих данных. При выключении функции автоматического подключения сохраненный пароль будет удален из хранилища устройства.
- Для автоматического подключения к удаленной среде в приложении RDP сразу после загрузки Kaspersky Thin Client, [настройте автоматический запуск приложения](#) в разделе **Параметры**.
8. Если для подключения к удаленному рабочему столу требуется использовать брокер Microsoft Remote Desktop Connection Broker, в поле **Идентификатор коллекции Remote Desktop Connection Broker** укажите идентификатор коллекции в формате `tsv://MS_Terminal_Services_Plugin.1.collection_id`, где `collection_id` – идентификатор коллекции.
- Если требуется запустить виртуальное приложение, в поле **Псевдоним приложения** укажите псевдоним приложения.
9. Если вы хотите, чтобы подключение к удаленному рабочему столу восстанавливалось автоматически после разрыва соединения, установите флажок **Подключаться повторно, если соединение прервано**.
10. Нажмите на стрелку назад в верхнем правом углу окна для возврата к окну подключения.

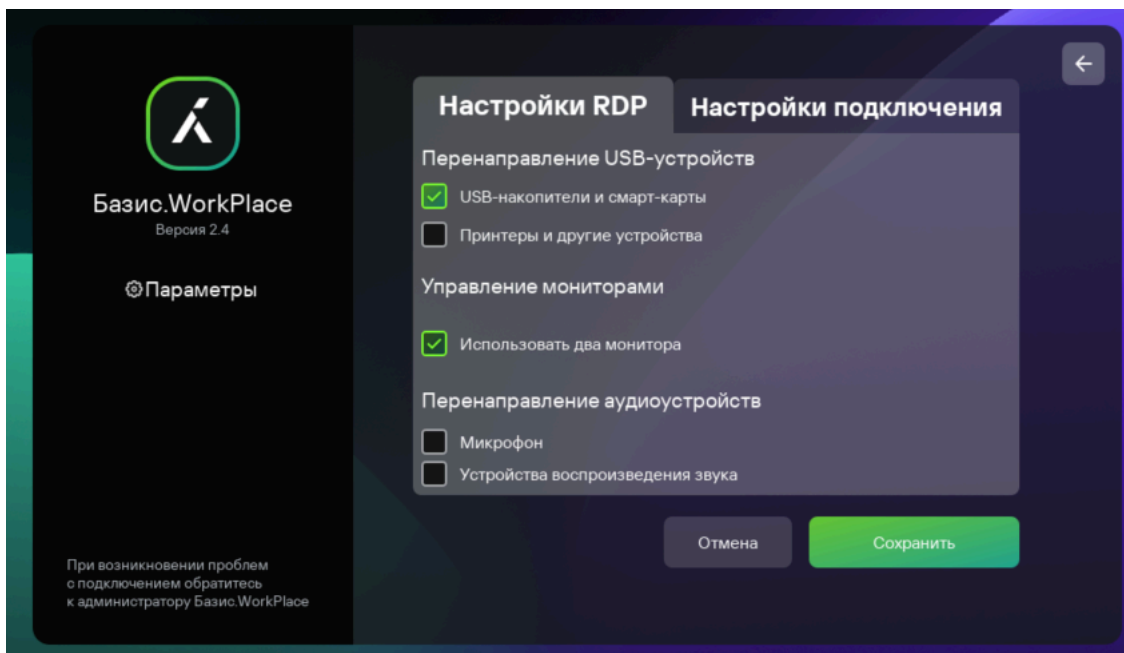
Настройка параметров подключения к удаленной среде с помощью приложения Базис.WorkPlace

С помощью приложения Базис.WorkPlace вы можете настроить параметры подключения к удаленной среде, развернутой в инфраструктуре Базис.WorkPlace.

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

1. На рабочем столе 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 перенаправления устройств в удаленную среду (см. рис. ниже).



Окно настройки параметров перенаправления устройств в удаленную среду, развернутую в инфраструктуре Базис.WorkPlace

3. Чтобы настроить параметры перенаправления устройств в удаленную среду:

- a. В блоке параметров **Перенаправление USB-устройств** выберите устройства, которые необходимо перенаправить в удаленную среду: **USB-накопители и смарт-карты**, **Принтеры и другие устройства**.
- b. Если на вашем рабочем месте установлено два монитора и вы хотите, чтобы изображение удаленной среды выводилось на оба монитора, в блоке **Управление мониторами** установите флажок **Использовать два монитора**.
- c. В блоке параметров **Перенаправление аудиоустройств** выберите устройства, которые необходимо перенаправить в удаленную среду: **Устройства воспроизведения звука**, **Микрофон**.
- d. Управление громкостью и другими параметрами звука и видео выполняется в удаленной среде.

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

4. Чтобы настроить параметры подключения к геораспределенной удаленной среде, перейдите на вкладку **Настройки подключения** (см. рис. ниже).

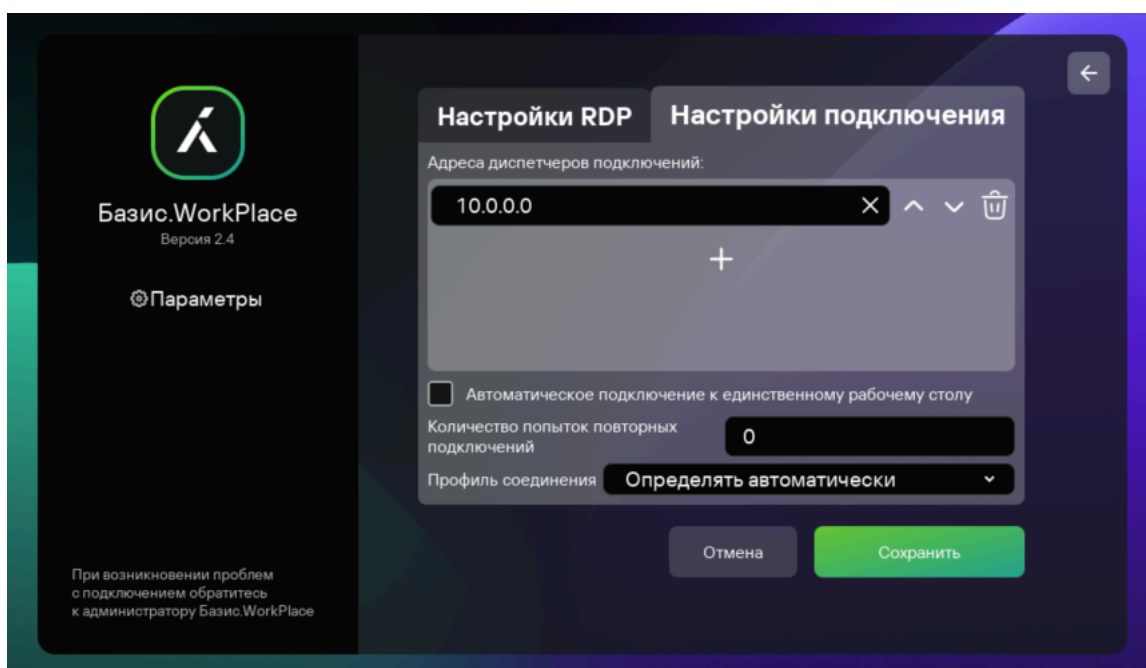
Подробное описание параметров этой вкладки см. в [руководстве по построению геораспределенной инсталляции](#) на сайте Базис.WorkPlace.

Выполните следующие действия на выбранной вкладке:

- a. В блоке **Адреса диспетчеров подключений** нажмите + и в отобразившемся поле укажите IP-адрес [брокера](#) Базис.WorkPlace. Вы можете добавить не более четырех IP-адресов.
- b. В поле **Количество попыток повторных подключений** введите количество попыток для повторного подключения к брокеру Базис.WorkPlace, которое необходимо выполнить Kaspersky Thin Client при разрыве соединения. Вы можете указать не более пяти попыток для повторного подключения.

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

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



Окно настройки параметров подключения к геораспределенной удаленной среде, развернутой в инфраструктуре Базис.WorkPlace

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

6. Нажмите на стрелку назад в верхнем правом углу окна для возврата к окну подключения к удаленной среде.

Управление доступом к параметрам Kaspersky Thin Client

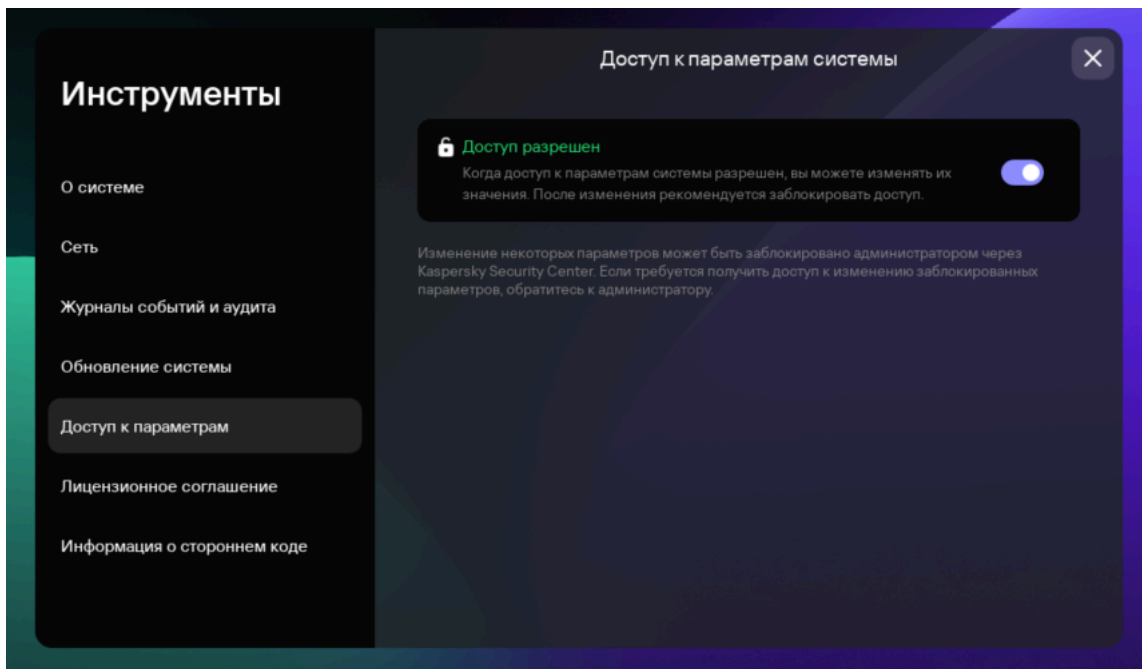
Вы можете выключить или включить отображение в интерфейсе Kaspersky Thin Client параметров, которые настраиваются однократно и в дальнейшем не используются в ключевых сценариях работы тонкого клиента.

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

Чтобы выключить или включить отображение параметров Kaspersky Thin Client:

1. В панели управления Kaspersky Thin Client нажмите на кнопку  и в открывшемся меню выберите **Инструменты**.
2. В открывшемся окне выберите раздел **Доступ к параметрам** (см. рис. ниже) и выполните одно из следующих действий:
 - Если требуется скрывать параметры, переведите переключатель в положение **Доступ заблокирован**.
В интерфейсе тонкого клиента будут скрыты все следующие параметры:
 - [Параметры подключения по протоколу RDP](#).
 - [Параметры подключения к Базис.WorkPlace](#).
 - [Общие параметры](#).
 - [Параметры сети](#).
 - [Параметры подключения к Kaspersky Security Center](#).
 - [Дата и время](#).
 - [Настройка параметров энергосбережения](#).
 - [Настройка расположения мониторов](#).
 - [Сброс параметров Kaspersky Thin Client](#).

- Если требуется показывать параметры, переведите переключатель в положение **Доступ разрешен**.
Параметры будут отображены. Вы сможете установить для них новые значения.



Инструменты. Раздел Доступ к параметрам

Управление Kaspersky Thin Client, установленной на тонком клиенте

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

Сценарий: работа в Kaspersky Thin Client на тонком клиенте

Основной сценарий работы в Kaspersky Thin Client, установленной на [тонком клиенте](#) ⁷ состоит из следующих этапов:

1 Подготовка Kaspersky Thin Client к включению

Подключите к тонкому клиенту [периферийные устройства](#) перед первым включением.

2 Запуск Kaspersky Thin Client

[Включите](#) тонкий клиент для начала работы.

3 Начало работы в удаленной сессии

[Подключитесь к удаленной среде](#) и начните работу в удаленной сессии.

4 Блокировка и разблокировка удаленной сессии

Если требуется временно покинуть рабочее место, [заблокируйте удаленную сессию](#). По возвращении возобновите работу.

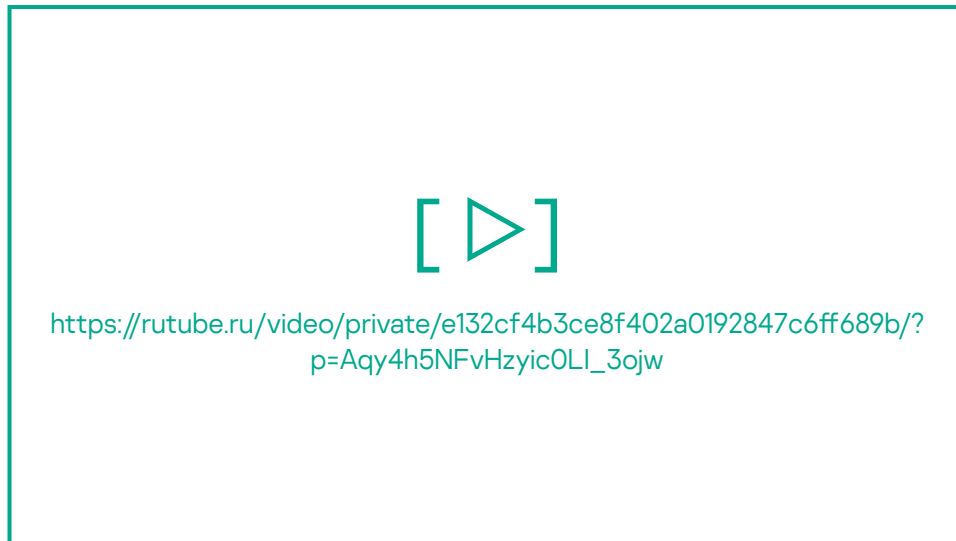
5 Завершение подключения к удаленной среде

[Завершите удаленную сессию](#) по окончании работы.

6 Остановка Kaspersky Thin Client

Выключите тонкий клиент в конце рабочего дня.

Для ознакомления с функциональностью вы можете посмотреть обучающее видео (см. ниже).



Kaspersky Thin Client для пользователя

Подключение к удаленной среде

В этом разделе приведена информация о том, как подключаться к [удаленной среде](#) с помощью приложений Kaspersky Thin Client и начинать работу в [удаленной сессии](#).

Существуют следующие ограничения при подключении к удаленной среде в Kaspersky Thin Client:

- Не поддерживается обмен файлами между Kaspersky Thin Client и удаленной средой.
- Не поддерживается буфер обмена между Kaspersky Thin Client и удаленной средой.
- Не поддерживается одновременный запуск нескольких удаленных сессий, а также одновременное подключение к нескольким удаленным средам в рамках одной удаленной сессии.

Kaspersky Thin Client использует шифрование по протоколу [TLS](#) (версии 1.2, 1.3) для защиты всех удаленных сессий, а также для защиты данных от перехвата или подмены.

Для подключения к удаленным средам под управлением Microsoft Windows Kaspersky Thin Client поддерживает следующие наборы шифров:

- Для TLS 1.2:
 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 = {0xC0, 0x30}.
 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 = {0xC0, 0x2F}.
 - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 = {0xC0, 0x2B}.
 - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 = {0xC0, 0x2C}.
 - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 = {0xCC, 0xA8}.

- TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 = {0xCC, 0xAA}.
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 = {0x00, 0x9F}.
- Для TLS 1.3:
 - TLS_AES_128_GCM_SHA256 = {0x13, 0x01}.
 - TLS_AES_256_GCM_SHA384 = {0x13, 0x02}.
 - TLS_CHACHA20_POLY1305_SHA256 = {0x13, 0x03}.
 - TLS_AES_128_CCM_SHA256 = {0x13, 0x04}.

Подключение к удаленной среде с помощью приложения RDP

В приложении RDP вы можете подключаться к [удаленным рабочим столам](#) и [виртуальным приложениям](#) по протоколу RDP.

Подключение к удаленному рабочему столу

Чтобы подключиться к удаленному рабочему столу в приложении RDP:

1. [Включите Kaspersky Thin Client.](#)
2. На рабочем столе Kaspersky Thin Client нажмите на кнопку **RDP**.
3. В открывшемся окне укажите параметры подключения:
 - a. В поле **Сервер** укажите IP-адрес или имя сервера брокера Microsoft Remote Desktop Connection Broker.
Kaspersky Thin Client сохраняет последний введенный адрес сервера, к которому было совершено успешное подключение, и вам не нужно вводить его при повторном подключении.
 - b. В поле **Имя пользователя** введите локальное или доменное имя пользователя. Вы можете указать доменное имя пользователя в формате Домен\Имя пользователя или в формате Имя пользователя.
Kaspersky Thin Client сохраняет последнее введенное имя пользователя, который успешно подключался к серверу, и вам не нужно вводить его при повторном подключении.
 - c. В поле **Пароль** введите пароль пользователя.
Если вы не [активировали функцию автоматического подключения](#), пароль не сохранится, и при следующем подключении будет необходимо ввести его снова.
4. Если требуется [настроить параметры](#) подключения к удаленному рабочему столу, нажмите **Параметры** в левой части окна.
5. Нажмите на клавишу **Enter** или на кнопку **Подключиться**.

Отобразится окно с предложением добавить сертификат для подключения к удаленной среде, если соблюдаются следующие условия:

- вы в первый раз подключаетесь к удаленной среде в интерфейсе Kaspersky Thin Client;
- тонкий клиент находится в одном из следующих состояний:
 - не подключен к Kaspersky Security Center;
 - не добавлен в [группу администрирования](#) 
 - для группы администрирования, в которой состоит тонкий клиент, [не добавлены сертификаты](#) для подключения к удаленной среде.

Проверьте параметры сертификата и нажмите на кнопку **Добавить сертификат**. Сертификат будет добавлен в системное хранилище сертификатов Kaspersky Thin Client и будет использоваться при следующих подключениях.

6. Если при [настройке подключения к удаленному рабочему столу](#) вы указали идентификатор коллекции Remote Desktop Connection Broker и вам доступно несколько рабочих столов, в открывшемся окне выбора удаленного рабочего стола нажмите на кнопку с названием рабочего стола, к которому вы хотите подключиться.

Отобразится окно удаленного рабочего стола, начнется удаленная сессия.

Подключение к виртуальному приложению

Чтобы подключиться к [виртуальному приложению](#)  в приложении RDP:

1. [Включите Kaspersky Thin Client](#).
2. На рабочем столе Kaspersky Thin Client нажмите на кнопку **RDP**.
3. В открывшемся окне укажите параметры подключения:
 - a. В поле **Сервер** укажите IP-адрес или имя сервера брокера Microsoft Remote Desktop Connection Broker.

Kaspersky Thin Client сохраняет последний введенный адрес сервера, к которому было совершено успешное подключение, и вам не нужно вводить его при повторном подключении.
 - b. В поле **Имя пользователя** введите локальное или доменное имя пользователя. Вы можете указать доменное имя пользователя в формате Домен\Имя пользователя или в формате Имя пользователя.

Kaspersky Thin Client сохраняет последнее введенное имя пользователя, который успешно подключался к серверу, и вам не нужно вводить его при повторном подключении.
 - c. В поле **Пароль** введите пароль пользователя.

Если вы не [активировали функцию автоматического подключения](#), пароль не сохранится, и при следующем подключении будет необходимо ввести его снова.
4. Нажмите **Параметры** в левой части окна.
5. В поле **Идентификатор коллекции Remote Desktop Connection Broker** укажите идентификатор коллекции в формате tsv://MS Terminal Services Plugin.1.collection_id, где collection_id – идентификатор коллекции.

6. В поле **Псевдоним приложения** укажите псевдоним виртуального приложения, которое требуется открыть.

Kaspersky Thin Client сохраняет псевдоним, который вы вводили в последний раз, и вам не нужно вводить его при повторном подключении.

7. Нажмите на стрелку назад в верхнем правом углу окна для возврата к окну подключения.

8. В окне подключения нажмите на клавишу **Enter** или на кнопку **Подключиться**.

Отобразится окно с предложением добавить сертификат для подключения к удаленной среде, если соблюдаются следующие условия:

- вы в первый раз подключаетесь к удаленной среде в интерфейсе Kaspersky Thin Client;
- тонкий клиент находится в одном из следующих состояний:
 - не подключен к Kaspersky Security Center;
 - не добавлен в [группу администрирования](#) 
 - для группы администрирования, в которой состоит тонкий клиент, [не добавлены сертификаты](#) для подключения к удаленной среде.

Проверьте параметры сертификата и нажмите на кнопку **Добавить сертификат**. Сертификат будет добавлен в системное хранилище сертификатов Kaspersky Thin Client и будет использоваться при следующих подключениях.

Отобразится окно запущенного виртуального приложения, начнется удаленная сессия.

Чтобы переключиться на другое окно запущенного виртуального приложения,

наведите курсор мыши на значок приложения в [панели подключения](#) в верхней части экрана и выберите нужное окно в раскрывающемся списке.

Подключение к удаленной среде с помощью приложения Базис.WorkPlace

В приложении Базис.WorkPlace вы можете подключаться к виртуальным рабочим столам, развернутым в инфраструктуре Базис.WorkPlace.

Не поддерживается смена пароля пользователя, инициированная пользователем, через Kaspersky Thin Client.

Чтобы подключиться к виртуальному рабочему столу в приложении Базис.WorkPlace:

1. [Включите Kaspersky Thin Client](#).
2. На рабочем столе Kaspersky Thin Client нажмите на кнопку **Базис.WorkPlace**.
3. В открывшемся окне подключения укажите параметры подключения к Базис.WorkPlace:
 - а. В поле **Сервер** укажите IP-адрес или имя сервера [брокера](#)  Базис.WorkPlace.

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

b. В поле **Домен** введите имя домена.

c. В поле **Имя пользователя** введите имя пользователя.

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

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

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

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

4. Нажмите на клавишу **ENTER** или на кнопку **Подключиться**.

Отобразится окно с предложением добавить сертификат для подключения к удаленной среде, если соблюдаются следующие условия:

- вы в первый раз подключаетесь к удаленной среде в интерфейсе Kaspersky Thin Client;
- тонкий клиент находится в одном из следующих состояний:
 - не подключен к Kaspersky Security Center;
 - не добавлен в [группу администрирования](#) 
 - для группы администрирования, в которой состоит тонкий клиент, [не добавлены сертификаты](#) для подключения к удаленной среде.

Проверьте параметры сертификата и нажмите на кнопку **Добавить сертификат**. Сертификат будет добавлен в системное хранилище сертификатов Kaspersky Thin Client и будет использоваться при следующих подключениях.

Откроется окно инфраструктуры Базис.WorkPlace с доступными виртуальными рабочими столами.

5. Если требуется обновить список виртуальных рабочих столов, нажмите на кнопку **Обновить**.

6. Нажмите на кнопку с названием виртуального рабочего стола, к которому хотите подключиться.

Отобразится окно виртуального рабочего стола. Начнется удаленная сессия.

Администратор может ограничить доступ к Базис.WorkPlace. Например, он может заблокировать вашу учетную запись или запретить доступ к виртуальным рабочим столам, которые ранее были доступны для вашей учетной записи. При возникновении проблем с подключением к удаленной среде обратитесь к администратору вашей организации.

Подключение к удаленной среде с помощью приложения Web Access

С помощью приложения Web Access вы можете подключаться к удаленной среде, развернутой в инфраструктуре Citrix Workspace. Web Access поддерживает HTML5 и обеспечивает безопасное соединение HTTPS при подключении.

Данные, необходимые для работы в удаленной среде (например, файлы cookies), будут сохраняться на тонком клиенте до завершения удаленной сессии. Затем эти данные будут удалены.

Чтобы подключиться к удаленной среде с помощью приложения Web Access:

1. [Включите Kaspersky Thin Client](#).
2. На рабочем столе Kaspersky Thin Client нажмите на кнопку **Web Access**.
3. В открывшемся окне подключения в поле **Сервер** укажите веб-адрес сервера необходимой удаленной среды.
4. Нажмите на клавишу **Enter** или на кнопку **Подключиться**.

Отобразится окно с предложением добавить сертификат для подключения к удаленной среде, если соблюдаются следующие условия:

- вы в первый раз подключаетесь к удаленной среде в интерфейсе Kaspersky Thin Client;
- тонкий клиент находится в одном из следующих состояний:
 - не подключен к Kaspersky Security Center;
 - не добавлен в [группу администрирования](#) 
 - для группы администрирования, в которой состоит тонкий клиент, [не добавлены сертификаты](#) для подключения к удаленной среде.

Проверьте параметры сертификата и нажмите на кнопку **Добавить сертификат**. Сертификат будет добавлен в системное хранилище сертификатов Kaspersky Thin Client и будет использоваться при следующих подключениях.

Отобразится окно ввода данных для подключения.

5. Введите имя пользователя и пароль для подключения к удаленной среде.

Система не сохраняет данные для подключения к удаленной среде, развернутой в инфраструктуре Citrix Workspace: необходимо вводить их при каждом запуске удаленной сессии.

Если вам доступен один удаленный рабочий стол, он отобразится на экране и вы сможете начать работу в удаленной среде. Если вам доступно несколько удаленных рабочих столов, отобразится окно с их списком.

6. Чтобы обновить список удаленных рабочих столов, нажмите на кнопку **Обновить**.

7. Нажмите на кнопку с названием удаленного рабочего стола, к которому вы хотите подключиться.

Отобразится окно удаленной среды, к которой вы подключились. Начнется [удаленная сессия](#).

Управление удаленной сессией

Этот раздел содержит информацию о том, как в интерфейсе Kaspersky Thin Client управлять [удаленной сессией](#) с помощью панели подключения и [горячих клавиш](#).

Работа с панелью подключения

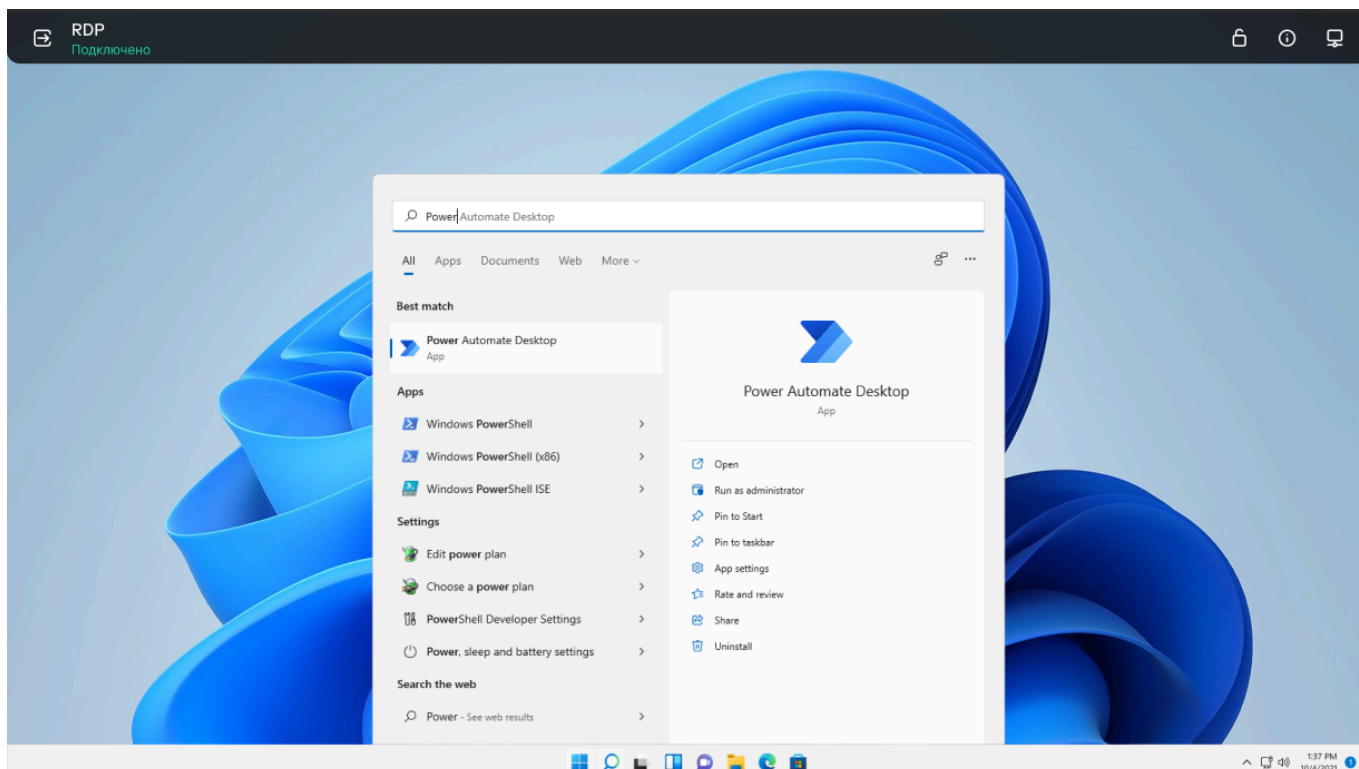
Панель подключения (далее также панель) отображается в верхней части экрана после успешного подключения к удаленной среде и используется для управления [удаленной сессией](#).

Состояния панели подключения

Панель подключения может находиться в одном из следующих состояний:

- Развернута.

Панель полностью отображается в верхней части экрана удаленной сессии (см. рис. ниже).



Окно запущенной удаленной сессии с развернутой панелью подключения

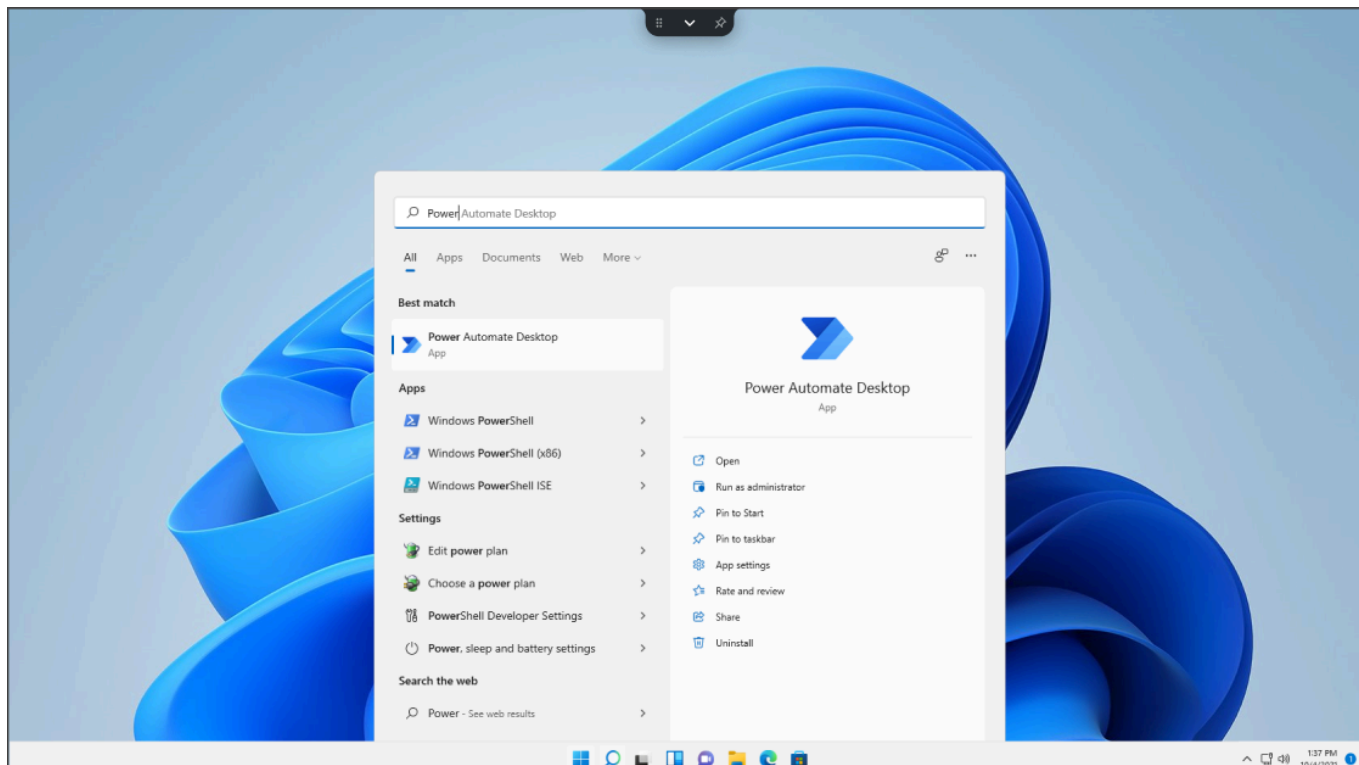
- Скрыта.

Панель не отображается на экране.

Если панель не закреплена, она автоматически переходит в это состояние при перемещении фокуса клавиатуры или курсора мыши с панели.

- Свернута.

Элементы управления панелью подключения отображаются при наведении курсора на верхнюю часть экрана (см. рис. ниже).



Окно запущенной удаленной сессии со свернутой панелью подключения

Изменение состояния панели подключения

В интерфейсе Kaspersky Thin Client вы можете менять состояние панели подключения, а также перемещать свернутую панель по горизонтали и закреплять ее в нужной области экрана.

Вы можете изменить состояние панели подключения следующими способами:

- Если требуется полностью скрыть развернутую панель подключения, выполните одно из следующих действий:
 - нажмите комбинацию клавиш **Ctrl+Alt+Home** или **Esc**;
 - нажмите на любую область экрана вне панели.
- Если требуется отобразить свернутую панель подключения, наведите курсор на верхнюю часть экрана. Отобразятся элементы управления панелью.
- Если требуется развернуть панель подключения, выполните одно из следующих действий:
 - нажмите комбинацию клавиш **Ctrl+Alt+Home**;
 - вызовите свернутую панель подключения и нажмите на кнопку .

Чтобы управлять свернутой панелью подключения, выполните одно из следующих действий:

- Если требуется изменить положение панели, нажмите на кнопку  и, удерживая ее, переместите панель вправо или влево.
- Если требуется закрепить свернутую панель в текущем положении, нажмите на кнопку .
Панель подключения будет отображаться в верхней части экрана в свернутом состоянии, пока вы не скроете ее или не открепите.
- Если требуется открепить панель, нажмите на кнопку .

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

Блокировка и разблокировка удаленной сессии

Запущенная удаленная сессия блокируется автоматически, когда экран тонкого клиента выключается спустя время бездействия, [заданное в настройках Kaspersky Thin Client](#). Вы также можете заблокировать и затем разблокировать удаленную сессию вручную.

Чтобы заблокировать запущенную удаленную сессию,

используйте комбинацию клавиш **Win+L** или [разверните панель подключения](#) и нажмите на кнопку .

Удаленная сессия будет заблокирована. Отобразится экран блокировки.

Чтобы завершить заблокированную удаленную сессию:

1. Подвиньте мышь или нажмите любую клавишу на клавиатуре.
2. На отобразившемся экране нажмите **Завершить удаленную сессию**.

Удаленная сессия будет завершена, отобразится окно приложения, в котором вы запускали удаленную сессию.

Чтобы разблокировать удаленную сессию:

1. Подвиньте мышь или нажмите любую клавишу на клавиатуре.
2. На отобразившемся экране введите пароль, который использовался при текущем подключении к удаленной среде.

Если вы сначала проходили авторизацию в [брокере](#) или в другой службе удаленного подключения, необходимо ввести пароль, который использовался при подключении к этой службе.

3. Нажмите **Разблокировать**.

Удаленная сессия будет разблокирована. Отобразится экран удаленной среды.

Завершение удаленной сессии

Чтобы завершить удаленную сессию,

[разверните панель подключения](#) и в отобразившейся панели нажмите на кнопку  или нажмите комбинацию клавиш **Ctrl+D**.

Удаленная сессия будет завершена, отобразится окно подключения.

Управление устройствами воспроизведения и записи звука в панели подключения

Вы можете подключить к тонкому клиенту с Kaspersky Thin Client несколько устройств воспроизведения и записи звука через разъем mini-jack или USB, чтобы перенаправить их в удаленную среду. В интерфейсе Kaspersky Thin Client вы можете [переключаться между подключенными устройствами](#).

Управление громкостью и другими параметрами звука и видео выполняется в удаленной среде.

При подключении к удаленной среде, развернутой в инфраструктуре Citrix Workspace, не поддерживается перенаправление более двух USB-устройств одновременно.

Подключение через mini-jack не поддерживается на тонких клиентах модели Dell Wyse 3040.

Чтобы выбрать устройства воспроизведения и записи звука в удаленной сессии:

1. [Разверните панель подключения](#) и в отобразившейся панели нажмите на кнопку .
2. В открывшемся окне в списке **Вывод** выберите устройство воспроизведения звука, а в списке **Ввод** выберите устройство записи звука.

Если необходимое устройство не отображается в списке, проверьте настройки перенаправления в приложении, в котором вы подключались к удаленной среде, или обратитесь к администратору вашей организации.

Управление окнами виртуального приложения

При подключении к [виртуальному приложению](#)  вы можете переключаться между его окнами в панели подключения Kaspersky Thin Client.

Чтобы переключиться на другое окно запущенного виртуального приложения:

1. Разверните панель подключения.

2. Нажмите на значок приложения.

Отобразится список открытых окон приложения.

3. Нажмите на необходимое окно.

Отобразится выбранное окно виртуального приложения.

Web Access: перенаправление USB-устройств в удаленную среду

Вы можете перенаправлять принтеры, сканеры, веб-камеру и USB-накопители в удаленную среду, развернутую в инфраструктуре Citrix Workspace. Для перенаправления веб-камеры не требуется дополнительная настройка в удаленной среде.

Поддерживается перенаправление не более двух [USB-устройств](#) одновременно.

Перенаправление принтера или сканера в удаленную среду

Чтобы перенаправить принтер или сканер в удаленную среду:

1. Подключите устройство к тонкому клиенту через разъем USB.

2. Если вы подключаете сканер, [укажите тип устройства вручную](#) в разделе **Параметры** -> **Нераспознанные USB-устройства**.

3. [Подключитесь к удаленной среде в приложении Web Access](#).

4. Разверните панель управления Citrix Workspace в верхней части окна и нажмите на кнопку **USB Devices**.

Отобразится окно с предложением перенаправить USB-устройство.

5. Нажмите **Добавить**.

Отобразится окно со списком устройств, доступных для перенаправления.

6. Если необходимое устройство не отображается в списке, попробуйте перезапустить удаленную сессию, не извлекая USB-устройство.

7. Выберите необходимое устройство в списке и нажмите **Подключить**.

Устройство будет перенаправлено в удаленную среду. Вы сможете пользоваться им в удаленном рабочем столе.

Если требуется перенаправить несколько устройств, повторите шаги 4-6 этой инструкции для каждого из них.

Подробнее о перенаправлении USB-устройств см. в [документации к продуктам Citrix Workspace](#).

Перенаправление USB-накопителей в удаленную среду

Вы также можете перенаправлять в удаленную среду USB-накопители и затем безопасно извлекать их. При перенаправлении используется технология Client Drive Mapping, подробнее см. в [документации к продуктам Citrix Workspace](#) ².

Чтобы перенаправить USB-накопители в удаленную среду, развернутую в инфраструктуре Citrix Workspace:

1. Подключите устройство к тонкому клиенту через разъем USB.
2. [Подключитесь к удаленной среде в приложении Web Access](#).
3. Разверните панель управления Citrix Workspace в верхней части окна и нажмите на кнопку **Map a drive**.
Отобразится окно выбора директории монтирования.
4. Нажмите **Browse**.
Отобразится окно подтверждения.
5. Нажмите **Перенаправить**, чтобы подтвердить перенаправление всех USB-накопителей, подключенных к тонкому клиенту.
Отобразится окно выбора директории монтирования.
6. Нажмите **Add**, чтобы подтвердить перенаправление.
7. Завершите удаленную сессию и подключитесь к удаленной среде снова, чтобы завершить перенаправление.

USB-накопители будут перенаправлены в удаленную среду. В файловой системе удаленной среды отобразится диск, внутри которого находятся папки с названиями перенаправленных USB-накопителей.

Безопасное извлечение USB-накопителей в удаленной сессии

Kaspersky Thin Client поддерживает безопасное извлечение USB-накопителей в удаленной сессии. Чтобы избежать повреждения данных, хранящихся на устройстве, извлекайте его по инструкции ниже.

Чтобы безопасно извлечь USB-накопитель в удаленной сессии:

1. [Подключитесь к удаленной среде в приложении Web Access](#).
2. [Разверните панель подключения](#) и нажмите на кнопку .
- Отобразится список USB-устройств, перенаправленных в удаленную среду.
3. Выберите необходимое устройство или нажмите **Извлечь все USB-накопители**.
4. Если при безопасном извлечении произошли неполадки, отобразится сообщение об ошибке. Закройте все окна на удаленном рабочем столе и завершите процессы копирования, затем попробуйте еще раз.

Устройство будет готово к безопасному извлечению и вы сможете физически отключить его от тонкого клиента.

Просмотр информации о Kaspersky Thin Client и тонком клиенте

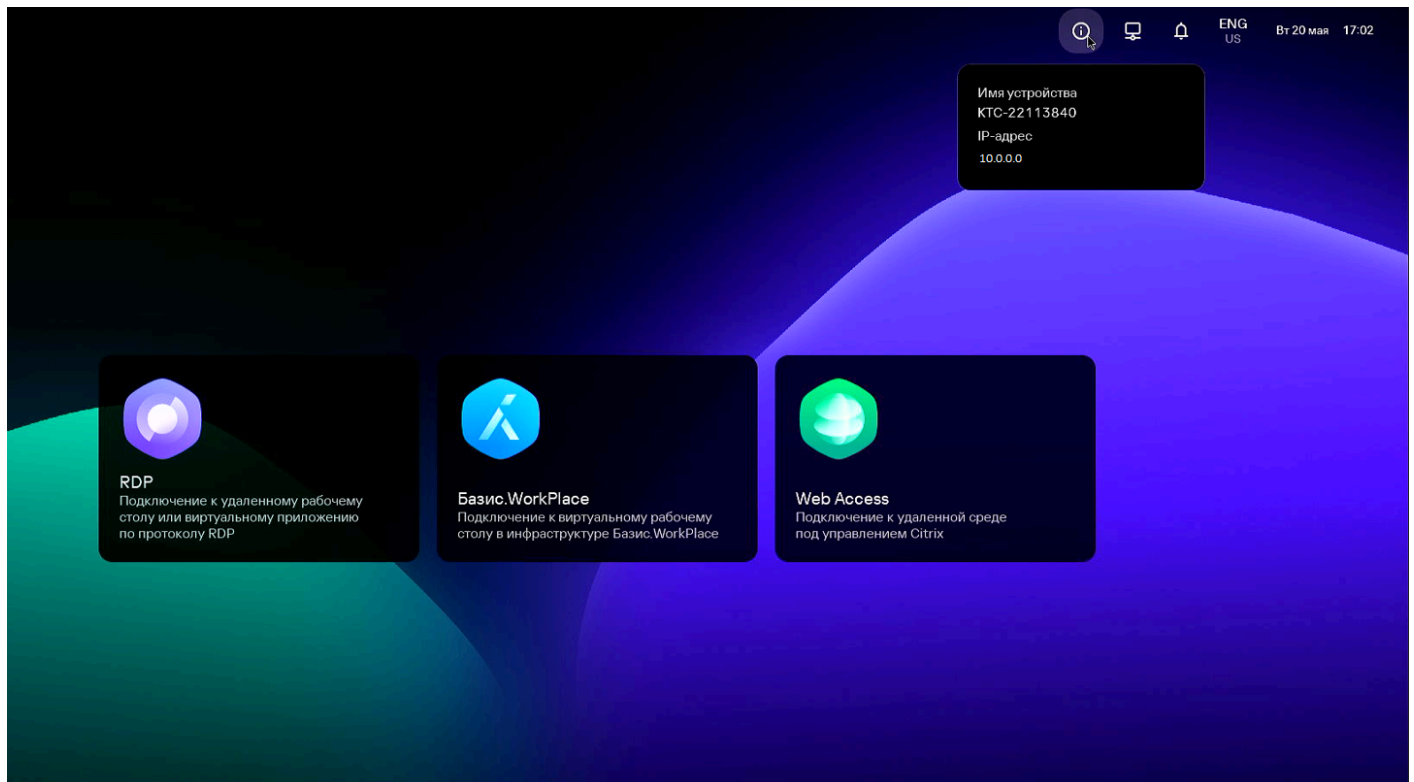
В интерфейсе Kaspersky Thin Client вы можете посмотреть текущую версию операционной системы и дату ее выпуска, а также версию SDK. Также в интерфейсе отображается IP-адрес и имя тонкого клиента.

Чтобы посмотреть информацию о тонком клиенте,

в панели управления Kaspersky Thin Client нажмите на кнопку .

Отобразится окно с информацией о тонком клиенте.

В этом окне также будут отображаться контакты службы технической поддержки или администратора вашей организации, если тонкий клиент добавлен в [группу администрирования](#) и если эти данные были [указаны в политике через Web Console](#).

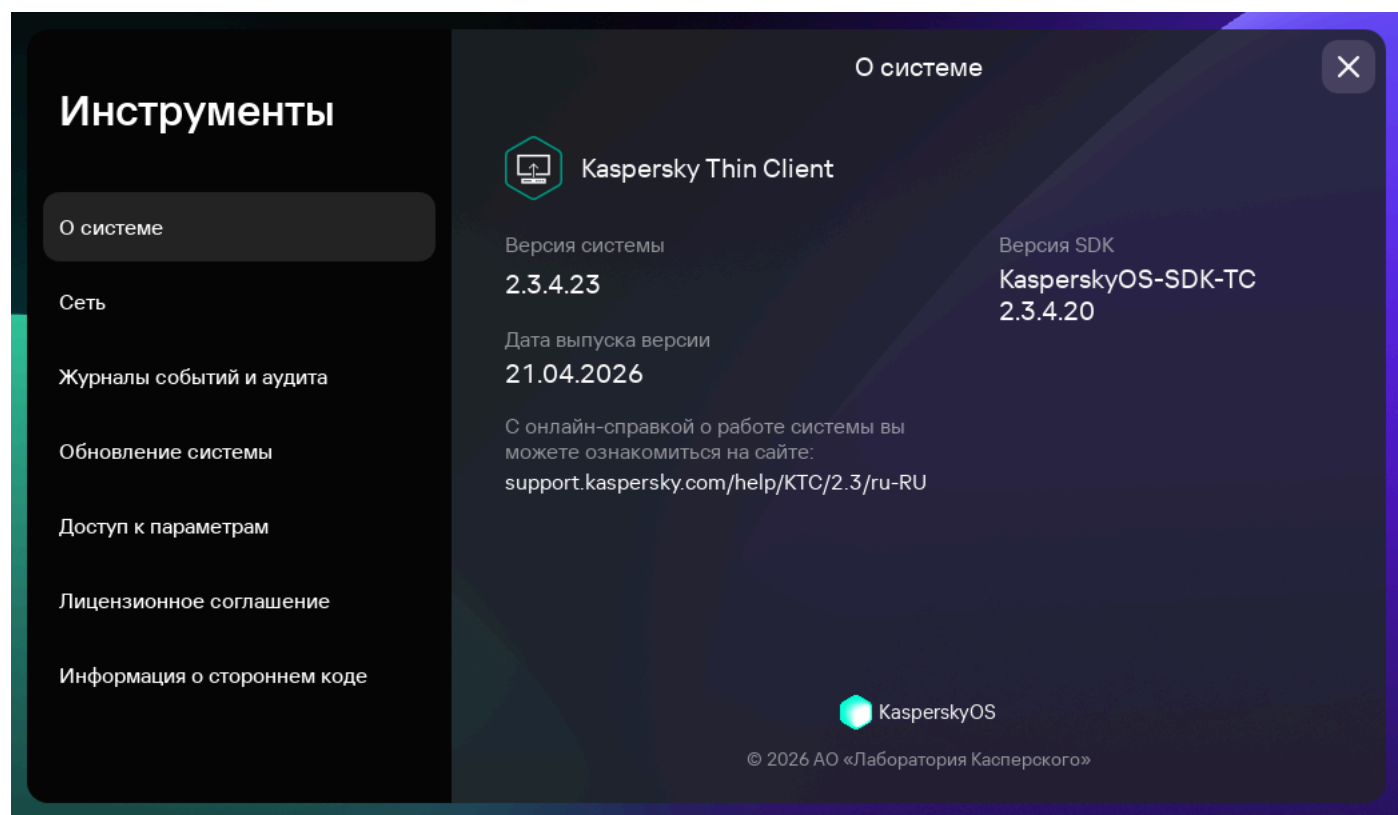


Окно с информацией о тонком клиенте

Чтобы посмотреть информацию о Kaspersky Thin Client,

в панели управления Kaspersky Thin Client нажмите на кнопку  и в открывшемся меню выберите **Инструменты** → **О системе** (см. рис. ниже).

Отобразится окно с информацией о Kaspersky Thin Client.



Инструменты. Раздел О системе

Просмотр информации о состоянии сети

В интерфейсе Kaspersky Thin Client вы можете просматривать параметры подключения системы к сети и информацию о состоянии подключения к сети. Информация о параметрах подключения Kaspersky Thin Client к сети обновляется автоматически не реже одного раза в секунду.

Чтобы посмотреть информацию о состоянии подключения к сети,

в панели управления Kaspersky Thin Client наведите курсор на значок .

Отобразится окно с информацией о состоянии подключения к сети.

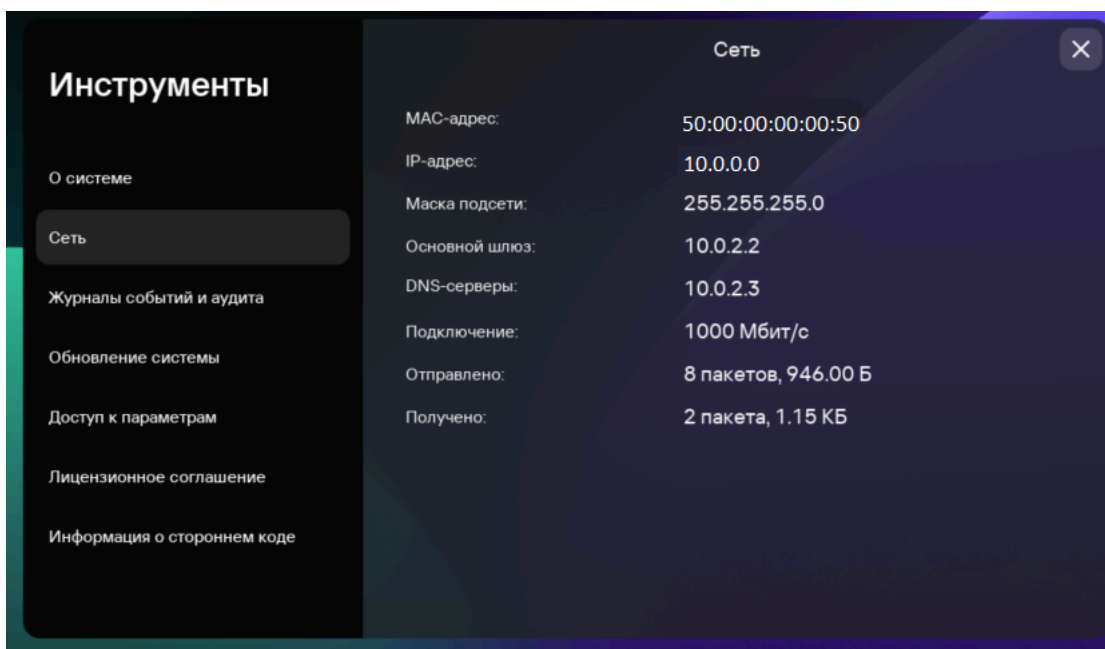
Чтобы посмотреть параметры подключения к сети,

в панели управления Kaspersky Thin Client нажмите на кнопку  и в открывшемся меню выберите **Инструменты** → **Сеть** (см. рис. ниже).

Отобразится окно с параметрами 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 отправленных от Kaspersky Thin Client сетевых пакетов.
- **Получено** – количество и общий размер полученных Kaspersky Thin Client сетевых пакетов.



Инструменты. Раздел Сеть

Просмотр уведомлений Kaspersky Thin Client

В интерфейсе Kaspersky Thin Client отображаются уведомления следующих типов:

- Уведомление, требующее выбрать определенное действие с помощью нажатия на соответствующую кнопку, например, применить обновление немедленно или отложить его. Если вы закрыли уведомление-действие, не выбрав действие, через некоторое время Kaspersky Thin Client снова отобразит это уведомление. Уведомление считается обработанным после выбора действия.
- Уведомление, предлагающее перейти в другой раздел Kaspersky Thin Client для дополнительной настройки параметров. Например, при подключении второго монитора система предлагает настроить взаимное расположение мониторов. Вы можете перейти в другой раздел системы, нажав на соответствующую кнопку, или закрыть уведомление.
- Уведомление информационного характера. Такие уведомления не требуют дополнительных действий, вы можете только закрыть уведомление после ознакомления.

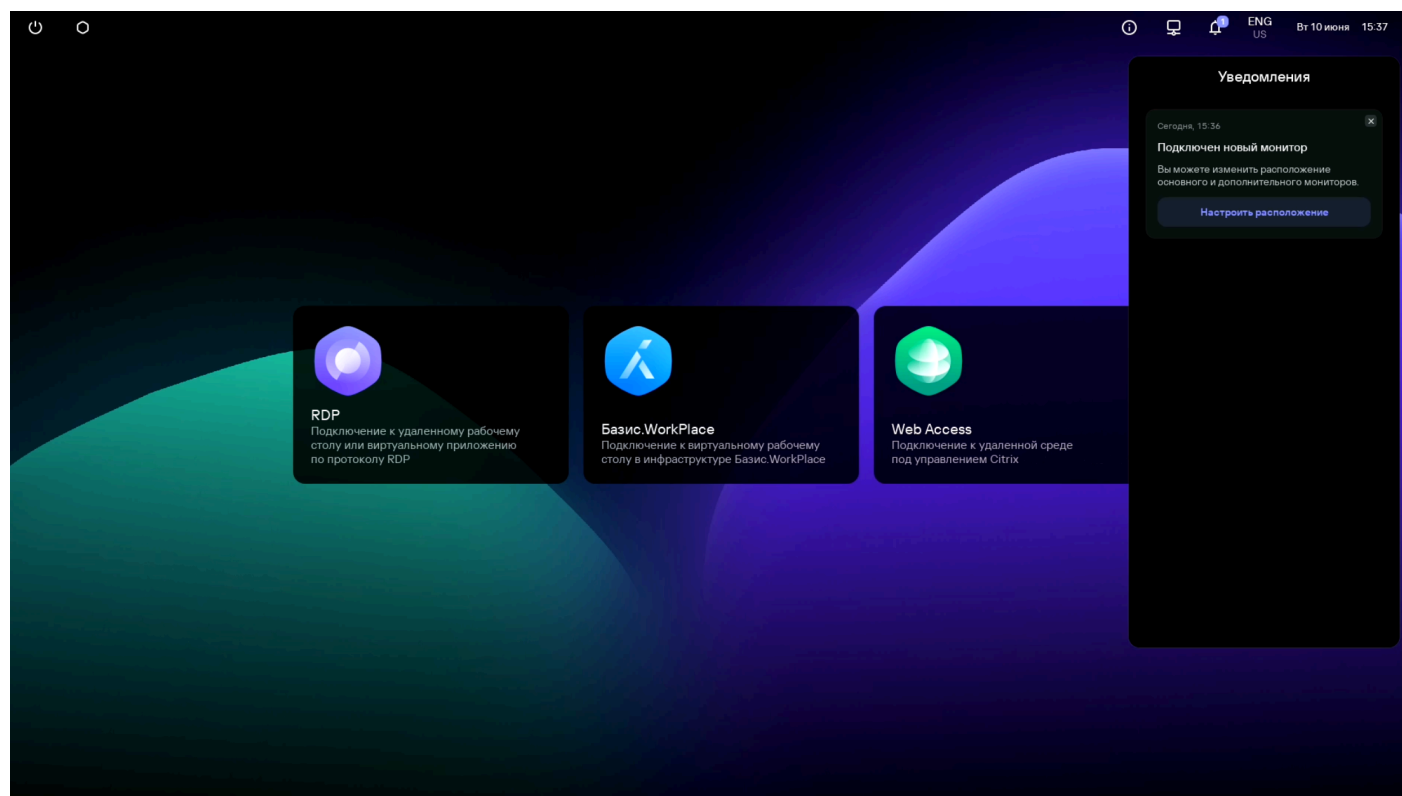
Необработанные и непрочитанные (при отсутствии курсора мыши или фокуса на зоне уведомления) уведомления скрываются, а в панели управления счетчик отображает количество необработанных уведомлений.

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

Чтобы просмотреть список всех уведомлений Kaspersky Thin Client,

в [панели управления](#) Kaspersky Thin Client нажмите на кнопку .

Отобразится панель уведомлений. Если у вас есть новые уведомления, они отобразятся в ней (см. рис. ниже).



Панель уведомлений Kaspersky Thin Client

Управление сертификатами в интерфейсе Kaspersky Thin Client

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

О сертификатах для подключения к Kaspersky Security Center

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

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

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

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

О сертификатах для подключения к удаленной среде и к серверу журналирования

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

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

- [при первом подключении Kaspersky Thin Client к Kaspersky Security Center](#);
- при первом подключении к удаленной среде;
- [при первом подключении к серверу журналирования](#).

Принятые сертификаты сохраняются в системном хранилище Kaspersky Thin Client.

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

Управление Kaspersky Thin Client с помощью горячих клавиш

Вы можете использовать специальные горячие клавиши и сочетания клавиш во время работы с Kaspersky Thin Client и во время [удаленной сессии](#). В таблице ниже приведены все доступные специальные клавиши и сочетания клавиш.

Специальные клавиши и сочетания клавиш Kaspersky Thin Client

Клавиши и сочетания клавиш	Действия
Win	Открыть или закрыть меню завершения работы .
→ ←	Переключиться между приложениями (RDP, Базис.WorkPlace, Web Access) на рабочем столе Kaspersky Thin Client.
↑ ↓	• Переключиться между элементами раскрывающегося списка. • Прокрутить содержимое страницы вверх или вниз.
Tab	Переключиться <i>слева направо</i> или <i>сверху вниз</i> между следующими элементами: • варианты подключений; • последовательность полей, например, в окне Параметры; • кнопки в панели подключения. При переключении элементы, недоступные для взаимодействия (например, поле, которое заблокировано для изменения), а также неактивные элементы пропускаются.
Shift+Tab	Переключиться <i>справа налево</i> или <i>снизу вверх</i> между следующими элементами: • варианты подключений; • последовательность полей, например, в окне Параметры; • кнопки в панели подключения. При переключении элементы, недоступные для взаимодействия (например, поле, которое заблокировано для изменения), а также неактивные элементы пропускаются.
Space или Enter	• Нажать на кнопку, на которой находится фокус клавиатуры. • Открыть или закрыть раскрывающийся список, на котором находится фокус клавиатуры. При переключении элементы, недоступные для взаимодействия (например, поле, которое заблокировано для изменения), а также неактивные элементы пропускаются.
Esc	• Закрыть активное окно. • Свернуть панель подключения, если на ней находится фокус клавиатуры.
Alt+Shift	Сменить язык раскладки клавиатуры.
Alt+Page down Alt+Page up	Переместиться в следующий или предыдущий раздел окна Параметры или Инструменты . При переключении между разделами их состояние и элемент, находящийся в фокусе, сохраняются. Например, в окне Параметры при переходе из раздела Основные в раздел Сеть фокус в разделе Основные останется на том же поле, в котором он был, когда вы переключились на другой раздел.
Ctrl+Alt+Home	Свернуть или развернуть панель подключения .
Ctrl+D	Завершить удаленную сессию. Комбинация работает только если панель подключения развернута.
Win+I	Открыть раздел Параметры , находясь на рабочем столе Kaspersky Thin Client, если доступ к параметрам открыт .
Win+U	Открыть раздел Инструменты , находясь на рабочем столе Kaspersky Thin Client.
Win+L	Заблокировать запущенную удаленную сессию.
Win+Esc	Выключить Kaspersky Thin Client , находясь на рабочем столе Kaspersky Thin Client.
Win+F12 или Win+End	Перезагрузить Kaspersky Thin Client , находясь на рабочем столе Kaspersky Thin Client.
Win+A или Win+N	Открыть панель уведомлений , находясь на рабочем столе Kaspersky Thin Client.
Win+↓ Win+↑	Свернуть или восстановить свернутое окно во время подключения к виртуальному приложению.

Клавиши и сочетания клавиш	Действия
Win+M	Свернуть все окна во время подключения к виртуальному приложению.
Win+Shift+M	Восстановить все окна во время подключения к виртуальному приложению.

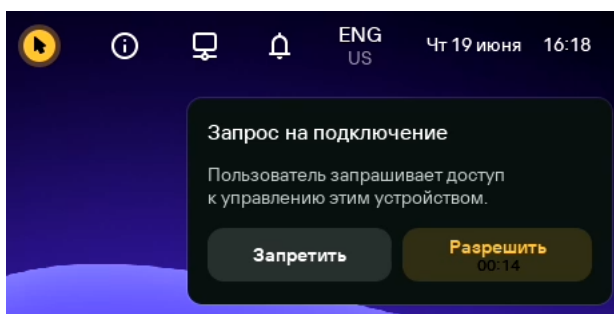
Управление доступом к удаленному управлению и экрану удаленной среды

В Kaspersky Thin Client вы можете принимать и отклонять запросы на доступ к удаленному управлению тонким клиентом и на доступ к экрану [удаленной сессии](#) ² запущенной на нем (далее также "экран удаленной среды").

Чтобы принять или отклонить запрос на доступ к удаленному управлению устройством и экрану удаленной среды:

1. [Включите тонкий клиент](#) и убедитесь, что [устройство подключено к сети](#).

При попытке подключения к Kaspersky Thin Client в панели управления отобразится значок . На рабочем столе отобразится уведомление с запросом на подключение (см. рис. ниже).



Уведомление с запросом на доступ к удаленному управлению тонким клиентом на рабочем столе Kaspersky Thin Client

2. Выполните одно из следующих действий:

- Нажмите **Запретить**, чтобы не предоставлять доступ к удаленному управлению Kaspersky Thin Client.
- Нажмите **Разрешить**, чтобы разрешить администратору просматривать экран Kaspersky Thin Client и управлять настройками системы.

Принимайте запрос только если вы уверены, что к Kaspersky Thin Client подключается администратор вашей организации.

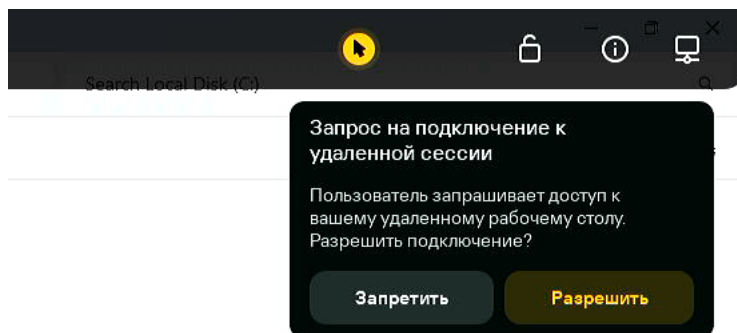
Управление Kaspersky Thin Client будет передано администратору.

Если в [параметрах Kaspersky Thin Client](#) или в настройках дистанционного управления в Web Console для [устройства](#) или [его группы администрирования](#) установлен режим **Разрешить автоматически**, при отсутствии реакции на запрос в течение 30 секунд управление Kaspersky Thin Client автоматически перейдет администратору.

3. Если на момент удаленного подключения в Kaspersky Thin Client запущена [удаленная сессия](#) или если ее запустит администратор во время дистанционного управления устройством, доступ к экрану такой удаленной сессии регулируется следующим образом:

- Если в [параметрах Kaspersky Thin Client](#) или в настройках дистанционного управления в Web Console для [устройства](#) или [его группы администрирования](#) разрешено автоматическое подключение к экрану удаленной среды, администратор автоматически получит доступ к экрану запущенной удаленной сессии.
- Если в параметрах Kaspersky Thin Client или в настройках дистанционного управления в Web Console установлен режим доступа к экрану удаленной среды **Разрешить по запросу**, в интерфейсе Kaspersky Thin Client отобразится уведомление с запросом на подключение к удаленной сессии (см. рис. ниже).

Управление Kaspersky Thin Client будет автоматически передано пользователю.



Уведомление с запросом на подключение к удаленной сессии

4. Выполните одно из следующих действий:

- Нажмите **Запретить**, не предоставлять администратору доступ к экрану удаленной среды.
Если требуется снова передать администратору управление тонким клиентом без доступа к экрану удаленной среды, [завершите удаленную сессию](#).
- Нажмите **Разрешить**, чтобы разрешить администратору просматривать экран удаленной среды и управлять удаленной сессией.

Управление Kaspersky Thin Client будет передано администратору.

Удаленное подключение к тонкому клиенту

Администратор может дистанционно (далее также удаленно) подключаться со своего устройства к тонкому клиенту для удаленного управления им с помощью RDP-клиента, если необходимо исправить неполадки или помочь пользователю настроить Kaspersky Thin Client.

Для удаленного управления тонкий клиент должен быть [включен](#) и [подключен к сети](#). В [параметрах Kaspersky Thin Client](#) или в параметрах дистанционного управления в Web Console для [тонкого клиента](#) или его [группы администрирования](#) должен быть установлен один из следующих режимов доступа к удаленному управлению: **Разрешить автоматически**, **Разрешить по запросу**.

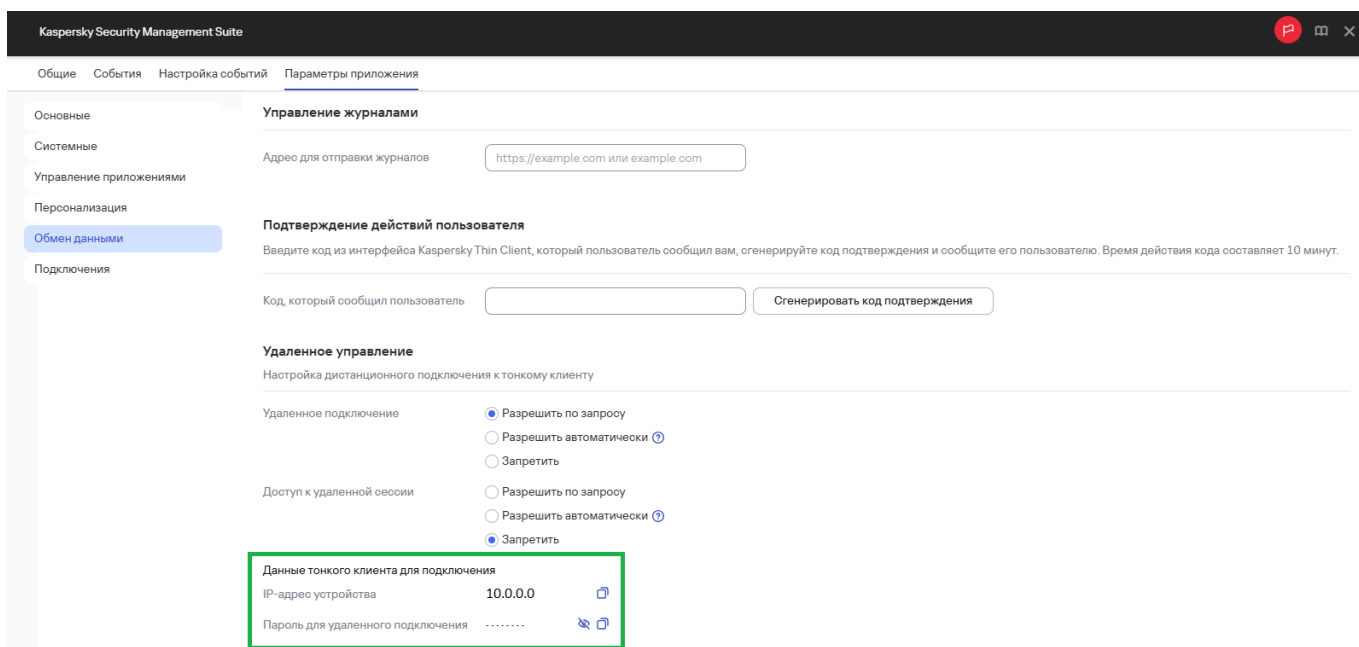
Для дистанционного управления необходимы IP-адрес тонкого клиента и пароль для удаленного подключения (далее также учетные данные).

Чтобы подключиться к тонкому клиенту для удаленного управления:

1. Откройте RDP-клиент на устройстве, с которого вы будете подключаться к тонкому клиенту.
2. Получите учетные данные для удаленного подключения одним из следующих способов:
 - Если тонкий клиент [подключен к Kaspersky Security Center](#), скопируйте учетные данные в интерфейсе Web Console:
 - a. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**, если хотите подключиться к устройству из группы администрирования, или **Обнаружение устройств и развертывание** → **Нераспределенные устройства**, если хотите подключиться к устройству, которое не входит ни в одну из групп администрирования.
 - b. В открывшемся списке нажмите на [имя тонкого клиента](#), к которому хотите подключиться.
 - c. В открывшемся окне выберите вкладку **Приложения**.
 - d. Нажмите на название веб-плагина управления Kaspersky Security Management Suite.
 - e. В открывшемся окне выберите вкладку **Параметры приложения**.
 - f. Перейдите в раздел **Обмен данными**.

г. В блоке **Данные тонкого клиента для подключения** скопируйте учетные данные для удаленного подключения, нажав на кнопку  напротив них (см. рис. ниже).

Пароль для удаленного подключения в Web Console обновляется один раз в сутки, а также после каждой перезагрузки тонкого клиента.



Окно настройки удаленного управления тонким клиентом в Web Console

- Если тонкий клиент не подключен к Kaspersky Security Center, запросите стандартный пароль в [Службе технической поддержки](#) и [получите IP-адрес устройства в интерфейсе Kaspersky Thin Client](#).

Стандартный пароль предназначен для временного использования: используйте его, только если тонкий клиент еще не подключен к Kaspersky Security Center.

3. В RDP-клиенте, установленном на вашем устройстве, введите полученные учетные данные и начните подключение к тонкому клиенту.
4. Для подключения к тонкому клиенту в зависимости от режима доступа к удаленному управлению, установленного в [параметрах Kaspersky Thin Client](#) или в параметрах дистанционного управления в Web Console для [устройства](#) или его [группы администрирования](#), выполните одно из следующих действий:

- Если установлен режим **Разрешить автоматически**, дождитесь подключения к тонкому клиенту. Пользователь может принять или отклонить ваш запрос в течение 30 секунд. Если пользователь не предпримет никаких действий в течение этого времени, подключение начнется автоматически.
- Если установлен режим **Разрешить по запросу**, дождитесь, пока пользователь [примет запрос на удаленное управление в интерфейсе Kaspersky Thin Client](#).

Если вы успешно подключились к тонкому клиенту, отобразится окно доступа к экрану удаленной среды.

5. Для получения доступа к экрану удаленной среды в зависимости от режима, установленного в [параметрах Kaspersky Thin Client](#) или в параметрах дистанционного управления в Web Console для [устройства](#) или его [группы администрирования](#), выполните одно из следующих действий:

- Если установлен режим **Разрешить автоматически**, дождитесь подключения к тонкому клиенту.
- Если установлен режим **Разрешить по запросу**, дождитесь, пока пользователь примет запрос на подключение в интерфейсе Kaspersky Thin Client или [завершит удаленную сессию](#).
- Если установлен режим **Запретить**, дождитесь, пока пользователь завершит удаленную сессию.

Отобразится интерфейс Kaspersky Thin Client. Вы получите доступ к удаленному управлению Kaspersky Thin Client.

Чтобы завершить удаленное управление тонким клиентом в интерфейсе Kaspersky Thin Client,

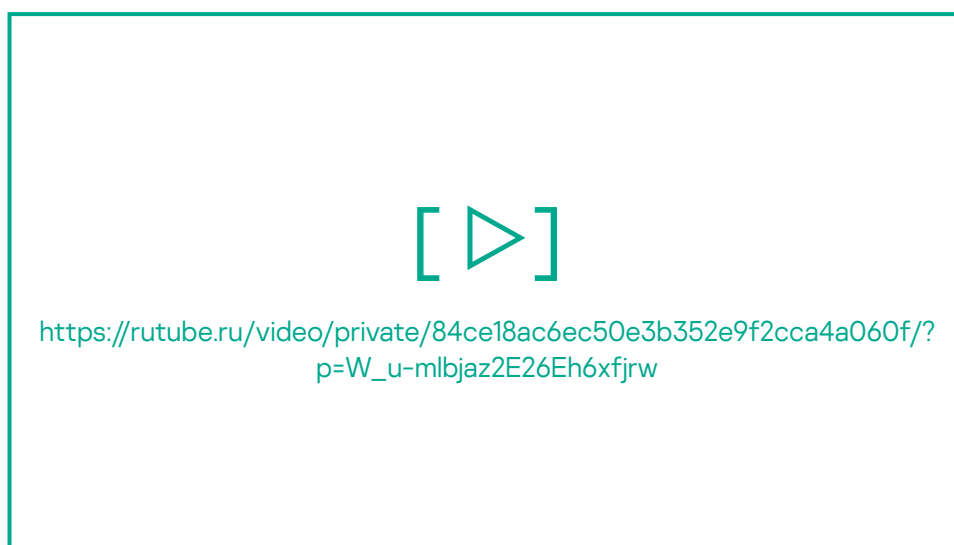
на [панели подключения](#) нажмите на кнопку , затем в открывшемся окне нажмите **Завершить**.

Управление Kaspersky Thin Client через Kaspersky Security Center Web Console

Kaspersky Security Center Web Console (далее также Web Console) – веб-приложение для централизованного решения основных задач по управлению устройствами и обслуживанию системы защиты сети организации. Web Console – компонент Kaspersky Security Center, предоставляющий пользовательский интерфейс. Подробную информацию о Kaspersky Security Center Web Console см. в [онлайн-справке Kaspersky Security Center](#).

Kaspersky Thin Client 2.3 поддерживает Kaspersky Security Center Linux версии 15.3 и Kaspersky Security Center Web Console версии 15.3.

Для ознакомления с функциональностью вы можете посмотреть обучающее видео (см. ниже).



Kaspersky Thin Client для администратора

О веб-плагине управления Kaspersky Security Management Suite

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

Веб-плагин позволяет централизованно выполнять следующие действия:

- управлять параметрами Kaspersky Thin Client для [одного](#) или [для нескольких тонких клиентов](#) в [группе администрирования](#);
- [настраивать получение событий Kaspersky Thin Client и просматривать их](#);
- [управлять сертификатами безопасности Kaspersky Thin Client](#).

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

- [указать параметры подключения к Kaspersky Security Center](#) при настройке Kaspersky Thin Client;
- [установить веб-плагин управления Kaspersky Security Management Suite](#) в Kaspersky Security Center.

Для стабильной работы функций системы и доступа ко всем ее возможностям мажорные версии веб-плагина управления Kaspersky Security Management Suite и Kaspersky Thin Client должны совпадать.

Установка веб-плагина управления Kaspersky Security Management Suite

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

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

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

Если для подключения тонкого клиента к Kaspersky Security Center планируется использовать порт по умолчанию, на Сервере администрирования Kaspersky Security Center должен быть доступен порт 13292. Если планируется использовать порт отличный от 13292, требуется настроить разрешение для нужного порта. Подробнее о включении порта на Сервере администрирования Kaspersky Security Center см. в [онлайн-справке Kaspersky Security Center](#).

Для стабильной работы функций системы и доступа ко всем ее возможностям мажорные версии веб-плагина управления Kaspersky Security Management Suite и Kaspersky Thin Client должны совпадать.

Чтобы установить веб-плагин в Web Console:

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

Отобразится текст Лицензионного соглашения.

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

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

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

Отобразится список доступных веб-плагинов управления Web Console.

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

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

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

6. Нажмите на кнопку **Добавить**.

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

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

Обновление веб-плагина управления Kaspersky Security Management Suite

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

Чтобы обновить веб-плагин в Web Console:

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

Отобразится текст Лицензионного соглашения.

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

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

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

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

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

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

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

7. Нажмите на кнопку **Обновление**.

8. После завершения обновления в окне сообщения об успешной установке нажмите на кнопку **ОК**.

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

Удаление веб-плагина управления Kaspersky Security Management Suite

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

Перед удалением веб-плагина удалите управляемые устройства из [групп администрирования](#).

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 веб-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 **ОК**.
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 **ОК**.

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 [онлайн-справке Kaspersky Security Center](#).

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 разрешено только [управление сертификатами](#). Вы можете назначить эту роль сотруднику, который отвечает за информационную безопасность в вашей организации.
- **Администратор.** Для этой роли разрешен доступ ко всем функциям управления Kaspersky Thin Client через Web Console, кроме управления сертификатами.
- **Расширенный администратор.** Для этой роли разрешен доступ ко всем функциям управления Kaspersky Thin Client через Web Console. Вы можете назначить эту роль сотруднику, который отвечает за поддержку и администрирование информационных систем, а также информационную безопасность в вашей организации.

В таблице ниже перечислены функции управления Kaspersky Thin Client, которые доступны пользователю в зависимости от назначенной роли. 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 удаленной среде 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	–	✓	✓
Управление приложениями Kaspersky Thin Client в политике Kaspersky Security Management Suite	–	✓	✓
Настройка параметров персонализации в политике Kaspersky Security Management Suite	–	✓	✓

Вход и выход из Web Console

Для входа в Web Console потребуется 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. Требования к браузеру, который используется для работы с Web Console см. в разделе [Аппаратные и программные требования](#) онлайн-справки Kaspersky Security Center.

Чтобы войти в Web Console:

1. В браузере перейдите по адресу <https://<Адрес Сервера администрирования>:<Номер порта>>.
Откроется страница входа.
2. Войдите с использованием имени и пароля доменного пользователя.

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. Вы можете перемещаться по Web Console и использовать ее для работы с Kaspersky Security Center.

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.

Управление политиками и группами администрирования

В Web Console вы можете добавлять подключенные к Kaspersky Security Center тонкие клиенты с Kaspersky Thin Client в [группу администрирования](#) , чтобы [централизованно настраивать параметры системы](#) с помощью [политик](#) .

По умолчанию сразу после установки Kaspersky Security Center в иерархии групп администрирования есть одна группа – **Управляемые устройства**. Любые создаваемые вами группы будут дочерними по отношению к ней. В политике, созданной для группы **Управляемые устройства**, вы можете настраивать параметры устройств во всех группах администрирования. Такую политику рекомендуется использовать, например, для централизованного [добавления сертификатов](#). Подробнее об иерархии групп и политик см. в [онлайн-справке Kaspersky Security Center](#) .

В этом разделе приведены инструкции по созданию групп администрирования и добавлению в них тонких клиентов, а также по созданию или изменению политик. Более подробную информацию см. в разделах о [политиках](#)  и об [управлении устройствами](#) справки Kaspersky Security Center.

Создание группы администрирования

В Web Console вы можете создавать [группы администрирования](#) , чтобы добавлять в них подключенные к Kaspersky Security Center тонкие клиенты с Kaspersky Thin Client и [централизованно настраивать параметры устройств](#) с помощью [политик](#) .

Чтобы создать группу администрирования:

1. В главном окне Web Console перейдите в раздел **Активы (Устройства)** → **Иерархия групп**.
2. Установите флажок напротив группы администрирования, в состав которой должна входить новая группа.
Если вы еще не создавали группы администрирования, выберите группу **Управляемые устройства**.
3. Нажмите на кнопку **Добавить**.
4. В открывшейся панели введите имя группы администрирования и нажмите на кнопку **Добавить**.

Имя группы администрирования должно быть уникальным на уровне своей иерархии.

Новая группа отобразится в списке групп администрирования.

Добавление тонких клиентов в группу администрирования

Вы можете добавлять тонкие клиенты с Kaspersky Thin Client в [созданную вами группу администрирования](#) или в группу **Управляемые устройства**.

Чтобы добавить устройства в группу администрирования:

1. В главном окне Web Console выберите **Обнаружение устройств и развертывание** → **Нераспределенные устройства**.
Отобразится список всех устройств, которые подключены к Kaspersky Security Center, но не добавлены ни в одну из групп администрирования.
2. Установите флажки напротив устройств, которые вы хотите добавить в группу.
3. Нажмите на кнопку **Переместить**.
4. В отобразившейся панели выберите необходимую группу администрирования.
5. Нажмите на кнопку **Переместить**.

Устройства будут добавлены в выбранную группу администрирования.

Вы также можете автоматизировать перемещение тонких клиентов в группы администрирования. Подробнее см. в [онлайн-справке Kaspersky Security Center](#).

Создание политики

Для настройки Kaspersky Thin Client, установленной на тонких клиентах из [группы администрирования](#) ², необходимо создать [политику](#) ² для этой группы в Web Console.

По умолчанию сразу после установки Kaspersky Security Center в иерархии групп администрирования есть одна группа – **Управляемые устройства**. Любые создаваемые вами группы будут дочерними по отношению к ней. В политике, созданной для группы **Управляемые устройства**, вы можете настраивать параметры устройств во всех группах администрирования. Такую политику рекомендуется использовать, например, для централизованного [добавления сертификатов](#). Подробнее об иерархии групп и политик см. в [онлайн-справке Kaspersky Security Center](#) ².

Чтобы создать политику:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Политики и профили политик**.
2. Выберите нужную группу администрирования. Для этого нажмите на ссылку текущего пути в верхней части окна и в открывшейся панели нажмите на необходимую группу администрирования.
3. Нажмите на кнопку **Добавить**.
4. В открывшемся окне в списке приложений выберите веб-плагин управления Kaspersky Thin Client и нажмите на кнопку **Далее**.
5. В окне настройки новой политики на вкладке **Общие** настройте следующие параметры:
 - В поле **Имя** введите имя политики.
 - В блоке **Состояние политики** выберите один из следующих статусов:
 - **Активна**
Политика, которая в настоящее время применяется к устройствам в группе администрирования. Если выбран этот вариант, при следующей синхронизации Kaspersky Thin Client и Kaspersky Security Center эта политика станет активной. В каждой группе администрирования может быть только одна активная политика.
Этот статус выбран по умолчанию.
 - **Неактивна**
Политика, которая в настоящее время не применяется к устройствам в группе администрирования. Если выбран этот вариант, политика становится неактивной, но сохраняется в списке политик. Позже вы можете активировать неактивную политику.
 - **Для автономных пользователей**
Политика активируется, когда устройство покидает периметр сети организации.
 - Включите или выключите переключатели в блоке **Наследование параметров**:
 - **Наследовать параметры родительской политики**
Если переключатель включен, значения параметров политики наследуются из политики для группы верхнего уровня иерархии и недоступны для изменения.

По умолчанию параметр включен.

- **Обеспечить принудительное наследование параметров для дочерних политик**

Значения параметров политики будут распространены на политики вложенных групп администрирования (дочерние политики), а в блоке **Наследование параметров** раздела **Общие** окна свойств каждой дочерней политики будет автоматически включен параметр **Наследовать параметры родительской политики**.

Когда параметр включен, значения параметров дочерних политик недоступны для изменения.

По умолчанию параметр выключен.

Подробнее об иерархии групп и политик см. в [онлайн-справке Kaspersky Security Center](#) .

6. Если вы хотите [настроить другие параметры](#), выберите вкладку **Параметры приложения** и внесите необходимые изменения.

7. Нажмите на кнопку **Сохранить** в нижней части экрана.

Политика будет создана и отобразится в списке политик.

Изменение политики

В Web Console вы можете изменять [созданную политику](#).

Чтобы изменить политику:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Политики и профили политик**.
2. Выберите политику, которую требуется изменить.
3. В открывшемся окне настройки политики на вкладке **Общие** настройте [необходимые параметры](#).
4. Нажмите на кнопку **Сохранить** в нижней части страницы.

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

Блокировка параметров в политике

В каждой [политике](#)  у настраиваемых параметров есть переключатель блокировки параметра со значком замка. Возможные положения переключателя описаны в таблице ниже.

Положения переключателя блокировки параметра

Состояние	Описание
 Не определено 	Заданные для параметра значения не применяются к устройствам, на которые действует политика. Пользователь может изменить такой параметр в интерфейсе Kaspersky Thin Client.
 Принудительно 	Заданные для параметра значения применяются к устройствам, на которые действует политика. Пользователь не сможет изменить такой параметр в интерфейсе Kaspersky Thin Client.

Настройка параметров Kaspersky Thin Client через Web Console для одного устройства

В Web Console вы можете настраивать параметры Kaspersky Thin Client, установленной на тонком клиенте. Устройство должно быть подключено к Kaspersky Security Center и [добавлено в группу администрирования](#).

Изменение идентификатора тонкого клиента через Web Console: одно устройство

В Kaspersky Security Center Web Console можно изменить идентификатор тонкого клиента, [добавленного в группу администрирования](#), если устройство с таким именем уже есть в этой группе администрирования.

Имена устройств в группе администрирования вы можете настраивать с помощью [политики](#).

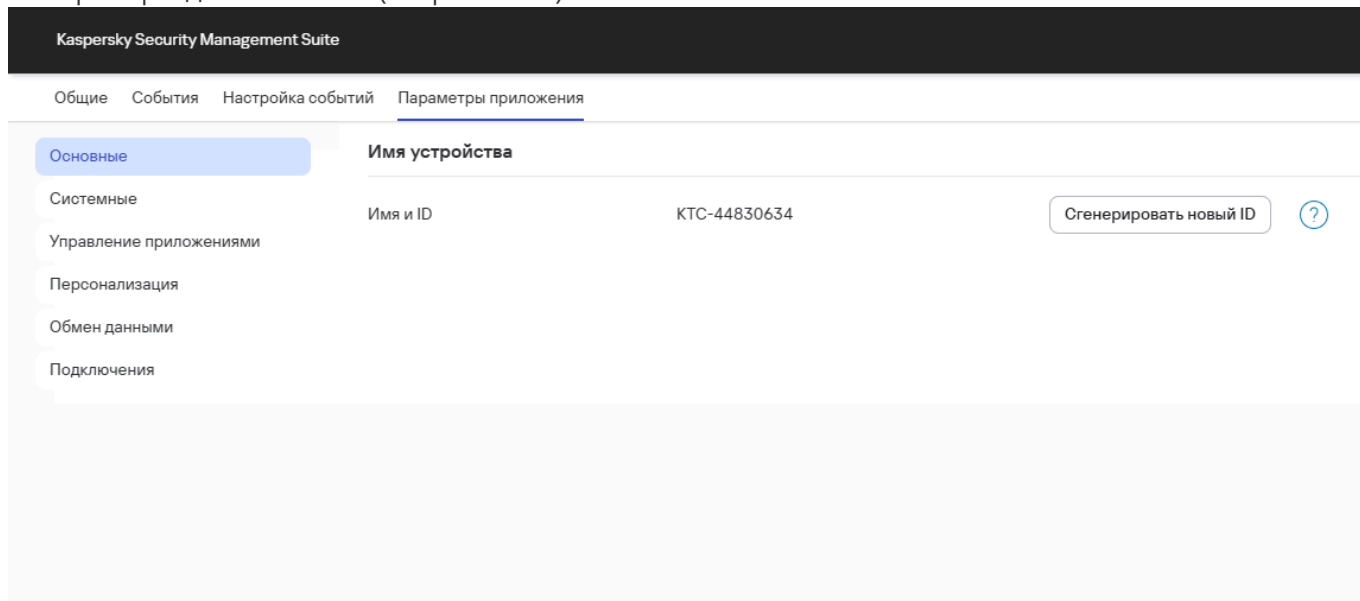
Чтобы изменить идентификатор тонкого клиента через Web Console:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.
2. В отобразившемся списке нажмите на имя нужного тонкого клиента. Вы можете просмотреть имя устройства в [интерфейсе Kaspersky Thin Client](#). Если имя тонкого клиента отсутствует в списке, [добавьте его в группу администрирования](#).

Если настраиваемый параметр заблокирован в [политике, созданной для группы администрирования](#), такой параметр невозможно изменить при настройке отдельного устройства. [Измените](#) или [разблокируйте](#) этот параметр в политике.

3. В открывшемся окне выберите вкладку **Приложения**.
4. Нажмите на название веб-плагина управления Kaspersky Security Management Suite.
Откроется окно с информацией о Kaspersky Thin Client.
5. Выберите вкладку **Параметры приложения**.

6. Выберите раздел **Основные** (см. рис. ниже).



Изменение идентификатора тонкого клиента через Web Console

7. В блоке **Имя устройства** нажмите на кнопку **Сгенерировать новый ID**.

Начнется процесс создания нового идентификатора. Он обновится в интерфейсе Web Console после синхронизации тонкого клиента и Kaspersky Security Center.

8. Нажмите на кнопку **Сохранить** в нижней части окна.

Изменения будут сохранены и применены в Kaspersky Thin Client, установленной на тонком клиенте, после синхронизации Kaspersky Thin Client и Kaspersky Security Center.

Настройка подключения к удаленной среде с помощью приложения RDP через Web Console: одно устройство

В Web Console вы можете настраивать параметры [подключения к удаленной среде с помощью приложения RDP](#).

Чтобы настроить параметры подключения к удаленной среде с помощью приложения RDP:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.
2. В отобразившемся списке нажмите на имя нужного тонкого клиента. Вы можете просмотреть имя устройства в [интерфейсе Kaspersky Thin Client](#). Если имя тонкого клиента отсутствует в списке, [добавьте его в группу администрирования](#).

Если настраиваемый параметр заблокирован в [политике, созданной для группы администрирования](#), такой параметр невозможно изменить при настройке отдельного устройства. [Измените](#) или [разблокируйте](#) этот параметр в политике.

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

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

Откроется окно с информацией о Kaspersky Thin Client.

5. Выберите вкладку **Параметры приложения**.

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

Откроется окно настройки параметров подключения к удаленной среде (см. рис. ниже).

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

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

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

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

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

Если у вас есть конфигурационный файл с параметрами подключения к Microsoft Remote Desktop Connection Broker и при необходимости именем приложения, которое нужно открыть, загрузите этот файл, нажав на кнопку **Загрузить конфигурационный файл**. При этом заполнять поля **Идентификатор коллекции Remote Desktop Connection Broker** и **Псевдоним приложения** 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 устройств** выберите устройства, которые необходимо перенаправить в удаленную среду: **Смарт-карты, USB-накопители, Принтеры и другие устройства, Микрофон, Устройства воспроизведения звука, Веб-камера (видео), Сканер**.

Управление громкостью и другими параметрами звука и видео выполняется в удаленной среде.

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

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 удаленной среды выводилось на оба монитора, в блоке **Управление мониторами** установите флажок **Использовать два монитора**.
14. Если требуется улучшить производительность при подключении к удаленным рабочим столам или приложениям, в блоке **Производительность** установите флажок **Улучшить графическую производительность**.
15. Если требуется автоматически подключаться к удаленному рабочему столу или виртуальному приложению при запуске приложения RDP, в блоке **Автоподключение** установите флажок **Подключаться автоматически**.

Для активации функции пользователю необходимо однократно подключиться к удаленной среде вручную и отключиться от нее. При этом в хранилище тонкого клиента будут сохранены следующие данные для подключения к RDP-серверу: имя пользователя, адрес сервера и пароль. При следующем запуске приложения RDP автоматически начнется подключение к удаленной среде с использованием этих данных. При выключении функции автоматического подключения сохраненный пароль будет удален из хранилища устройства.

В Web Console не поддерживается задание пароля для подключения к удаленной среде.

Для автоматического подключения к удаленной среде в приложении RDP сразу после загрузки Kaspersky Thin Client, [настройте автоматический запуск приложения](#).

16. Нажмите на кнопку **Сохранить** в нижней части окна.

Изменения будут сохранены и применены в Kaspersky Thin Client, установленной на тонком клиенте, после синхронизации Kaspersky Thin Client и Kaspersky Security Center.

Настройка подключения к удаленной среде с помощью приложения Базис.WorkPlace через Web Console: одно устройство

В Web Console вы можете настраивать параметры подключения к удаленной среде, развернутой в инфраструктуре Базис.WorkPlace.

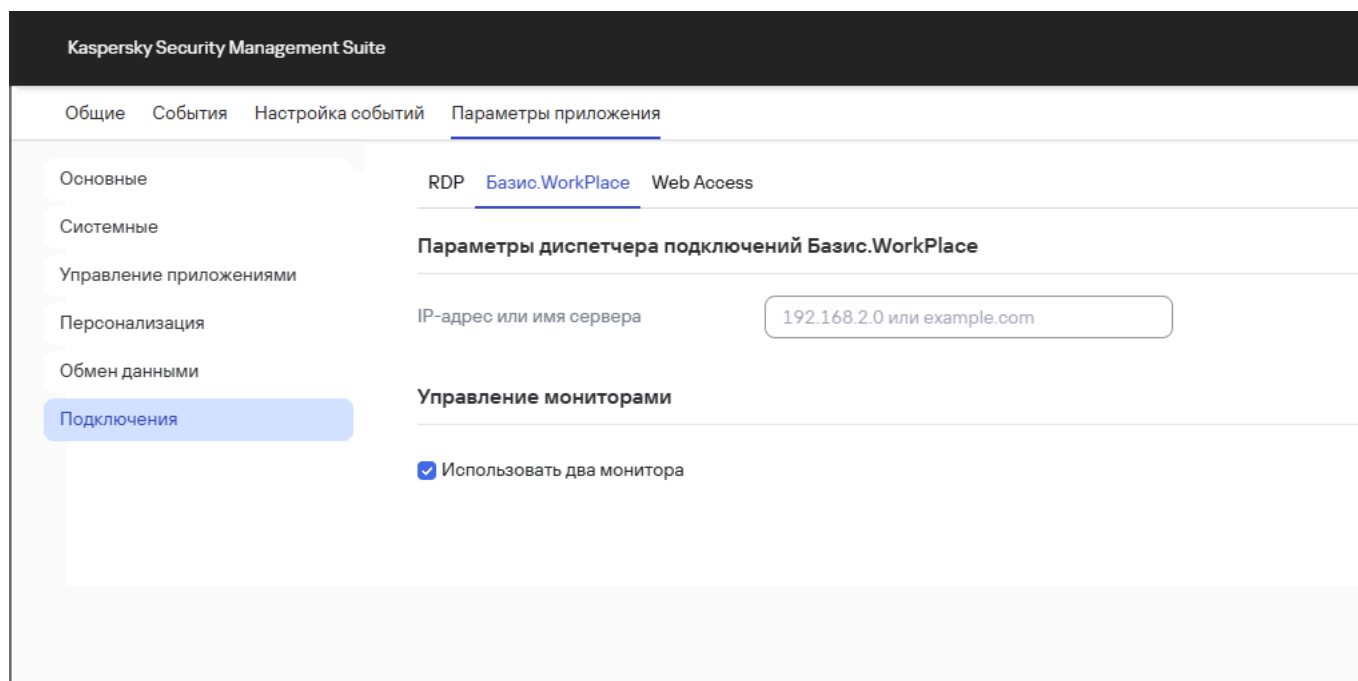
Не поддерживается смена пароля пользователя, инициированная пользователем, через Kaspersky Thin Client.

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

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.
2. В отобразившемся списке нажмите на имя нужного тонкого клиента. Вы можете просмотреть имя устройства в [интерфейсе Kaspersky Thin Client](#). Если имя тонкого клиента отсутствует в списке, [добавьте его в группу администрирования](#).

Если настраиваемый параметр заблокирован в [политике, созданной для группы администрирования](#), такой параметр невозможно изменить при настройке отдельного устройства. [Измените](#) или [разблокируйте](#) этот параметр в политике.

3. В открывшемся окне выберите вкладку **Приложения**.
4. Нажмите на название веб-плагина управления Kaspersky Security Management Suite.
Откроется окно с информацией о Kaspersky Thin Client.
5. Выберите вкладку **Параметры приложения**.
6. Выберите раздел **Подключения** → **Базис.WorkPlace**.
Откроется окно настройки параметров подключения к удаленной среде (см. рис. ниже).



Окно настройки параметров подключения к удаленной среде, развернутой в инфраструктуре Базис.WorkPlace, через Web Console

7. В поле **IP-адрес или имя сервера** введите IP-адрес или имя сервера, к которому необходимо подключиться.

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

9. Нажмите на кнопку **Сохранить** в нижней части окна.

Изменения будут сохранены и применены в Kaspersky Thin Client, установленной на тонком клиенте, после синхронизации Kaspersky Thin Client и Kaspersky Security Center.

Настройка подключения к удаленной среде с помощью приложения Web Access через Web Console: одно устройство

В Web Console вы можете настраивать параметры [подключения к удаленной среде с помощью приложения Web Access](#).

С помощью приложения Web Access вы можете подключаться к удаленной среде, развернутой в инфраструктуре Citrix Workspace. Web Access поддерживает HTML5 и обеспечивает безопасное соединение HTTPS при подключении.

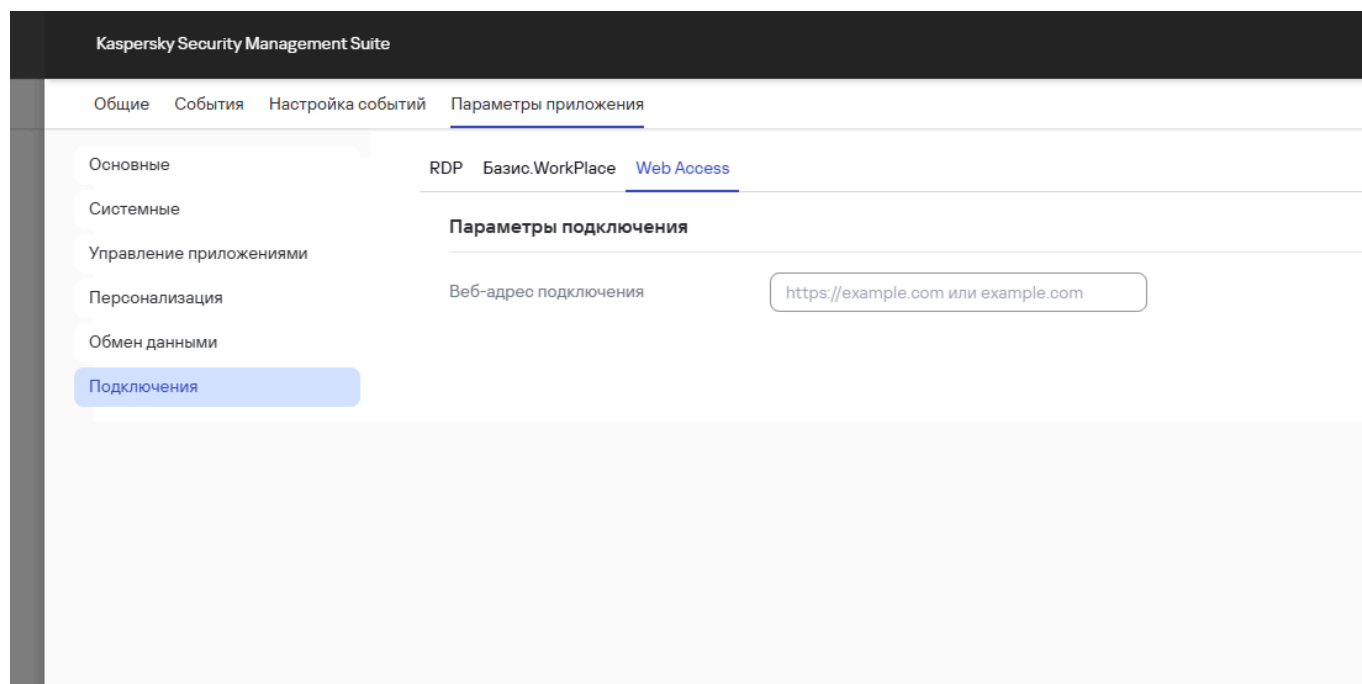
Чтобы настроить параметры подключения к удаленной среде с помощью приложения Web Access:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.
2. В отобразившемся списке нажмите на имя нужного тонкого клиента. Вы можете просмотреть имя устройства в [интерфейсе Kaspersky Thin Client](#). Если имя тонкого клиента отсутствует в списке, [добавьте его в группу администрирования](#).

Если настраиваемый параметр заблокирован в [политике, созданной для группы администрирования](#), такой параметр невозможно изменить при настройке отдельного устройства. [Измените](#) или [разблокируйте](#) этот параметр в политике.

3. В открывшемся окне выберите вкладку **Приложения**.
4. Нажмите на название веб-плагина управления Kaspersky Security Management Suite.
Откроется окно с информацией о Kaspersky Thin Client.
5. Выберите вкладку **Параметры приложения**.
6. Выберите раздел **Подключения** → **Web Access**.

Откроется окно настройки параметров подключения к удаленной среде (см. рис. ниже).



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

7. В поле **Веб-адрес подключения** введите веб-адрес сервера для подключения к [необходимой удаленной среде](#).

8. Нажмите на кнопку **Сохранить** в нижней части окна.

Изменения будут сохранены и применены в Kaspersky Thin Client, установленной на тонком клиенте, после синхронизации Kaspersky Thin Client и Kaspersky Security Center.

Настройка мониторов и экранов через Web Console: одно устройство

В Web Console вы можете настраивать мониторы, подключенные к тонкому клиенту в [группе администрирования](#) [?](#), и параметры их экранов.

Kaspersky Thin Client поддерживает подключение двух мониторов. Система считает один из мониторов основным, другой – дополнительным. На экране основного монитора отображается панель подключения во время [удаленной сессии](#) [?](#). Экран дополнительного монитора расширяет или дублирует изображение основного. В Web Console вы можете выбрать, какой монитор будет считаться основным (далее также "изменить взаимное расположение мониторов").

В интерфейсе Web Console мониторы пронумерованы. Система определяет номер монитора по разъему, через который он подключен к тонкому клиенту: монитор 1 – в ближайшем к питанию, монитор 2 – в следующем. Расположение разъемов на [поддерживаемых моделях тонких клиентов](#) вы можете посмотреть в документации производителей устройств.

В Web Console не отображается информация о том, сколько мониторов подключено к определенному тонкому клиенту.

Если вы хотите, чтобы экран удаленной сессии отображался на обоих мониторах, включите их использование в параметрах подключения к удаленной среде в приложении [RDP](#) или [Базис.WorkPlace](#).

Чтобы настроить мониторы и экраны через Web Console:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.
2. В отобразившемся списке нажмите на имя нужного тонкого клиента. Вы можете просмотреть имя устройства в [интерфейсе Kaspersky Thin Client](#). Если имя тонкого клиента отсутствует в списке, [добавьте его в группу администрирования](#).

Если настраиваемый параметр заблокирован в [политике, созданной для группы администрирования](#), такой параметр невозможно изменить при настройке отдельного устройства. [Измените](#) или [разблокируйте](#) этот параметр в политике.

3. В открывшемся окне выберите вкладку **Приложения**.
4. Нажмите на название веб-плагина управления Kaspersky Security Management Suite.
Откроется окно с информацией о Kaspersky Thin Client.
5. Выберите вкладку **Параметры приложения**.
6. Выберите раздел **Системные** (см. рис. ниже).

The screenshot displays the 'Kaspersky Security Management Suite' interface. The top navigation bar includes 'Общие', 'События', 'Настройка событий', and 'Параметры приложения'. The left sidebar shows a tree structure with 'Основные' expanded, containing 'Системные' (selected), 'Управление приложениями', 'Персонализация', 'Обмен данными', and 'Подключения'. The main content area is titled 'Системные параметры устройства' and contains several sections: 'Системные параметры устройства' with 'Язык интерфейса' (Russian) and 'Часовой пояс' (Europe, Moscow UTC (+03:00)); 'Параметры энергосбережения' with 'Выключать монитор' (every 25 minutes) and 'Выключать устройство' (every 2 hours); 'Управление мониторами' with a descriptive note and settings for 'Основной монитор' (Monitor 1) and 'Режим отображения' (Extended display); and individual settings for 'Монитор 1' and 'Монитор 2', each with 'Разрешение монитора' (1920x1080) and 'Ориентация' (Horizontal).

Окно настройки мониторов и экранов через Web Console

7. В блоке **Управление мониторами** настройте необходимые параметры:

- В раскрывающемся списке **Основной монитор** выберите, какой монитор система должна считать основным.

Если к тонкому клиенту подключен только один монитор, к нему будут применены настройки монитора, который выбран основным в Web Console.

- В раскрывающемся списке **Режим отображения** выберите способ вывода изображения на экраны мониторов:
 - **Расширение экрана** – изображение распределяется между двумя мониторами.
 - **Дублирование экрана** – изображение экрана основного монитора дублируется на дополнительном.
- В раскрывающемся списке **Разрешение монитора** выберите необходимое разрешение для выбранного экрана.

Поддерживаемые разрешения перечислены в [разделе с аппаратными и программными требованиями](#).

Если выбрано значение **Максимально возможное**, будет установлено наибольшее значение параметра, поддерживаемое монитором и Kaspersky Thin Client.

- В раскрывающемся списке **Ориентация** выберите положение экрана на мониторе:
 - **Горизонтальная** – стандартное положение экрана.
 - **Перевернутая горизонтальная** – экран повернут на 180°.
 - **Вертикальная** – экран повернут на 90°.
 - **Перевернутая вертикальная** – экран повернут на 270°.

8. Нажмите на кнопку **Сохранить** в нижней части окна.

Изменения будут сохранены и применены в Kaspersky Thin Client, установленной на тонком клиенте, после синхронизации Kaspersky Thin Client и Kaspersky Security Center.

Настройка системных параметров Kaspersky Thin Client через Web Console: одно устройство

В Web Console вы можете настраивать язык интерфейса и часовой пояс Kaspersky Thin Client, а также время выключения тонкого клиента и мониторов, подключенных к нему.

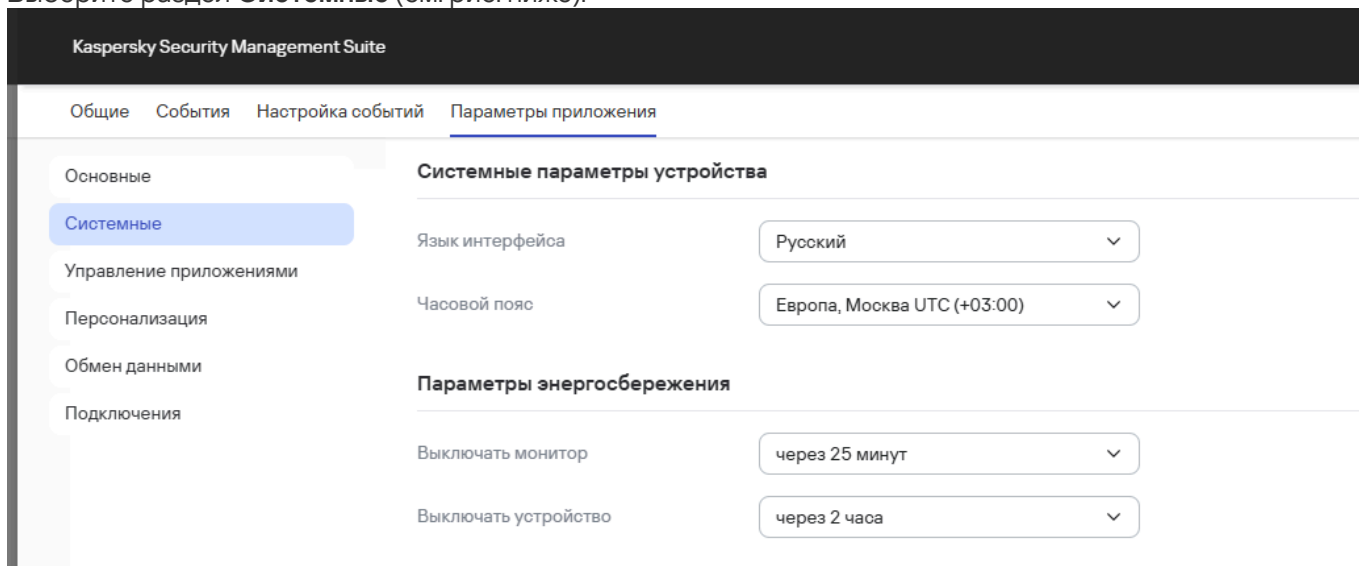
Kaspersky Thin Client 2.3 поддерживает следующие языки интерфейса: русский, английский (США), испанский (Мексика) и португальский (Бразилия).

Чтобы настроить системные параметры Kaspersky Thin Client через Web Console:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.
2. В отобразившемся списке нажмите на имя нужного тонкого клиента. Вы можете просмотреть имя устройства в [интерфейсе Kaspersky Thin Client](#). Если имя тонкого клиента отсутствует в списке, [добавьте его в группу администрирования](#).

Если настраиваемый параметр заблокирован в [политике, созданной для группы администрирования](#), такой параметр невозможно изменить при настройке отдельного устройства. [Измените](#) или [разблокируйте](#) этот параметр в политике.

3. В открывшемся окне выберите вкладку **Приложения**.
4. Нажмите на название веб-плагина управления Kaspersky Security Management Suite.
Откроется окно с информацией о Kaspersky Thin Client.
5. Выберите вкладку **Параметры приложения**.
6. Выберите раздел **Системные** (см. рис. ниже).



Окно настройки системных параметров Kaspersky Thin Client через Web Console

7. В блоке **Системные параметры устройства** в раскрывающихся списках **Язык интерфейса** и **Часовой пояс** выберите необходимые значения.
8. В блоке **Параметры энергосбережения** настройте следующее:
 - В раскрывающемся списке **Выключать монитор** выберите время бездействия системы, по истечении которого монитор будет выключен.
 - В раскрывающемся списке **Выключать устройство** выберите время бездействия системы, по истечении которого тонкий клиент будет выключен.
9. Нажмите на кнопку **Сохранить** в нижней части окна.

Изменения будут сохранены и применены в Kaspersky Thin Client, установленной на тонком клиенте, после синхронизации Kaspersky Thin Client и Kaspersky Security Center.

Настройка отправки журналов Kaspersky Thin Client на сервер журналирования: одно устройство

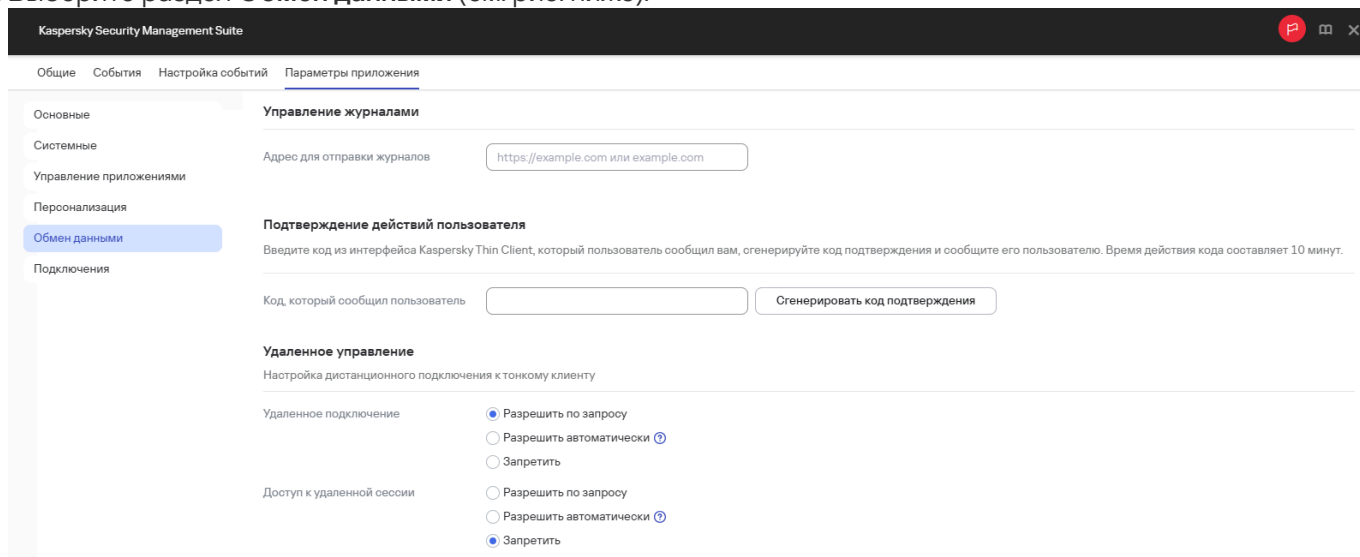
В Web Console вы можете менять адрес [сервера журналирования](#) ² на который отправляются [журналы событий и аудита](#) Kaspersky Thin Client.

Чтобы настроить отставку журналов Kaspersky Thin Client на сервер журналирования через Web Console:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.
2. В отобразившемся списке нажмите на имя нужного тонкого клиента. Вы можете просмотреть имя устройства в [интерфейсе Kaspersky Thin Client](#). Если имя тонкого клиента отсутствует в списке, [добавьте его в группу администрирования](#).

Если настраиваемый параметр заблокирован в [политике, созданной для группы администрирования](#), такой параметр невозможно изменить при настройке отдельного устройства. [Измените](#) или [разблокируйте](#) этот параметр в политике.

3. В открывшемся окне выберите вкладку **Приложения**.
4. Нажмите на название веб-плагина управления Kaspersky Security Management Suite.
Откроется окно с информацией о Kaspersky Thin Client.
5. Выберите вкладку **Параметры приложения**.
6. Выберите раздел **Обмен данными** (см. рис. ниже).



Окно настройки отправки журналов Kaspersky Thin Client через Web Console

7. В поле **Адрес для отправки журналов** введите адрес сервера журналирования, на который будут отправляться журналы, в формате `https://<адрес сервера>`.

Для получения журналов событий и аудита из Kaspersky Thin Client в инфраструктуре вашей организации должен быть развернут сервер журналирования с учетом [аппаратных и программных требований](#).

8. Нажмите на кнопку **Сохранить** в нижней части окна.

Изменения будут сохранены и применены в Kaspersky Thin Client, установленной на тонком клиенте, после синхронизации Kaspersky Thin Client и Kaspersky Security Center.

Настройка параметров персонализации Kaspersky Thin Client: одно устройство

В Web Console вы можете загружать свои изображения и устанавливать их в качестве фона рабочего стола или экрана блокировки Kaspersky Thin Client. Поддерживаются файлы следующих форматов: JPEG, PNG, JPG. Максимальный размер файла: 15 МБ. Вы также можете удалять загруженные изображения из Web Console.

По умолчанию на рабочем столе и экране блокировки Kaspersky Thin Client установлен стандартный фон. Если вы устанавливали другой фон, вы можете сбросить настройки персонализации, чтобы снова установить стандартный.

Изменение фона в интерфейсе Kaspersky Thin Client не поддерживается – вы можете изменять фон экранов только через Web Console. Также изображение, установленное через Web Console, меняется на стандартный фон при [сбросе параметров системы](#).

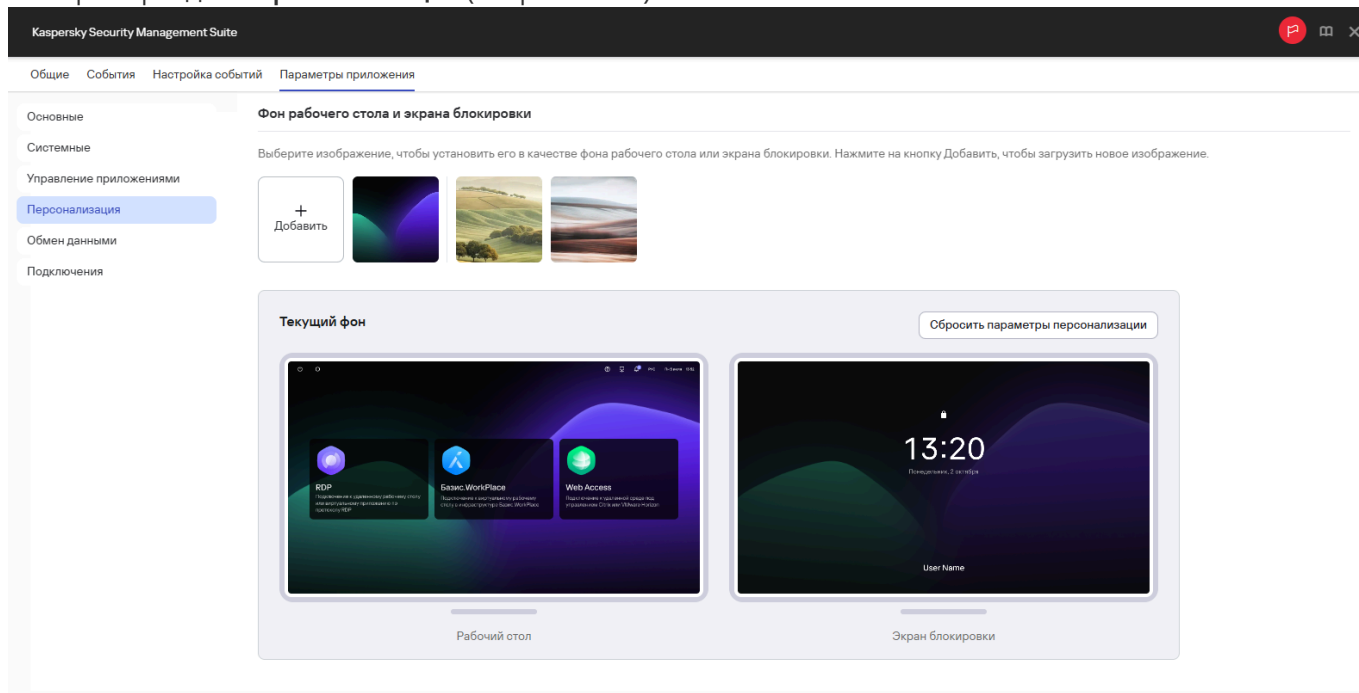
Чтобы изменить фон экрана блокировки или рабочего стола Kaspersky Thin Client:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.
2. В отобразившемся списке нажмите на имя нужного тонкого клиента. Вы можете просмотреть имя устройства в [интерфейсе Kaspersky Thin Client](#). Если имя тонкого клиента отсутствует в списке, [добавьте его в группу администрирования](#).

Если настраиваемый параметр заблокирован в [политике, созданной для группы администрирования](#), такой параметр невозможно изменить при настройке отдельного устройства. [Измените](#) или [разблокируйте](#) этот параметр в политике.

3. В открывшемся окне выберите вкладку **Приложения**.
4. Нажмите на название веб-плагина управления Kaspersky Security Management Suite.
Откроется окно с информацией о Kaspersky Thin Client.
5. Выберите вкладку **Параметры приложения**.

6. Выберите раздел **Персонализация** (см. рис. ниже).



Окно настройки параметров персонализации Kaspersky Thin Client через Web Console

7. Чтобы изменить фон рабочего стола или экрана блокировки, выполните следующие действия:

а. Выберите необходимое изображение.

- Если вы хотите загрузить новое изображение в Web Console, нажмите на кнопку **Добавить**.
В открывшемся окне перетащите нужное изображение в область загрузки или нажмите **Загрузить файл или перетащить его сюда**, затем в открывшемся окне выберите нужное изображение.
- Если вы хотите установить уже загруженное в Web Console изображение, нажмите на его миниатюру.

Отобразится окно предпросмотра выбранного изображения на экранах Kaspersky Thin Client.

Если вы хотите сохранить изображение в Web Console, не устанавливая его в качестве фона, перейдите к шагу с. этой инструкции.

б. Установите флажки напротив экранов, на которых нужно установить изображение в качестве фона:

- **Рабочий стол** – изображение будет установлено в качестве [фона рабочего стола Kaspersky Thin Client](#).
- **Экран блокировки** – изображение будет установлено в качестве [фона экрана блокировки](#).

с. Нажмите **Сохранить** в окне предпросмотра.

Отобразится основной экран раздела **Персонализация**. На выбранных экранах будет установлен выбранный вами фон.

8. Чтобы удалить загруженное в Web Console изображение, наведите курсор на его миниатюру, затем нажмите на отобразившуюся кнопку **✕**.

Подтвердите свои действия в отобразившемся окне.

Изображение будет безвозвратно удалено из Web Console. Если изображение было выбрано в качестве фона на каком-либо экране, вместо него будет установлен стандартный фон.

9. Чтобы установить стандартный фон на все экраны, нажмите **Сбросить параметры персонализации** и подтвердите свои действия в открывшемся окне.

На рабочем столе и экране блокировки Kaspersky Thin Client будет установлен стандартный фон.

10. Нажмите на кнопку **Сохранить** в нижней части окна раздела **Персонализация**.

Изменения будут сохранены и применены на тонком клиенте в течение часа после синхронизации Kaspersky Thin Client и Kaspersky Security Center.

Настройка параметров удаленного подключения к тонкому клиенту через Web Console: одно устройство

В Web Console вы можете настроить следующие параметры удаленного подключения к устройству:

- Режим доступа к удаленному управлению – определяет условия и порядок подключения к тонкому клиенту.
- Режим доступа к удаленной сессии, запущенной на тонком клиенте в момент подключения к нему (далее также "экран удаленной среды").

Ограничение доступа к экрану удаленной среды может понадобиться, если пользователь тонкого клиента работает с чувствительными или конфиденциальными данными.

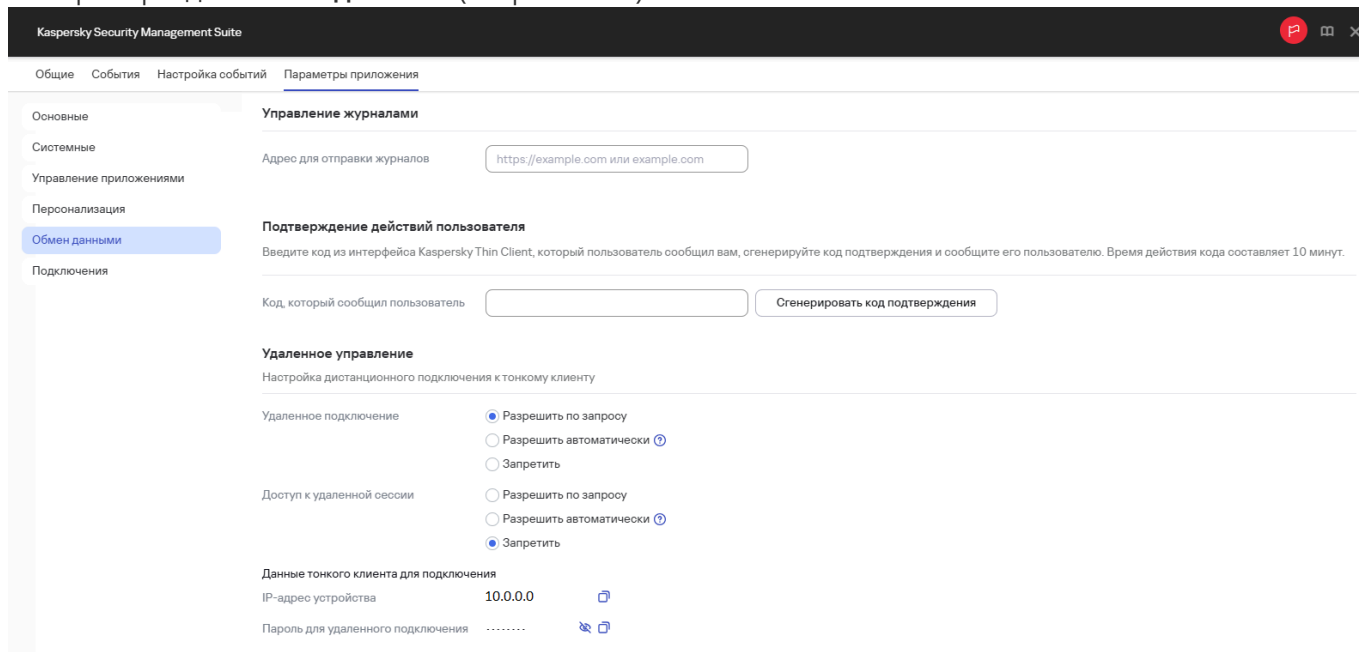
Чтобы настроить параметры удаленного подключения к тонкому клиенту:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.
2. В отобразившемся списке нажмите на имя нужного тонкого клиента. Вы можете просмотреть имя устройства в [интерфейсе Kaspersky Thin Client](#). Если имя тонкого клиента отсутствует в списке, [добавьте его в группу администрирования](#).

Если настраиваемый параметр заблокирован в [политике, созданной для группы администрирования](#), такой параметр невозможно изменить при настройке отдельного устройства. [Измените](#) или [разблокируйте](#) этот параметр в политике.

3. В открывшемся окне выберите вкладку **Приложения**.
4. Нажмите на название веб-плагина управления Kaspersky Security Management Suite.
Откроется окно с информацией о Kaspersky Thin Client.
5. Выберите вкладку **Параметры приложения**.

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



Окно настройки параметров удаленного управления тонким клиентом через Web Console

7. В разделе **Удаленное управление** выберите режим доступа к удаленному управлению тонким клиентом:

- **Разрешить автоматически**

В этом режиме администратор сможет удаленно подключиться к тонкому клиенту после того, как пользователь [примет запрос на удаленное управление в интерфейсе Kaspersky Thin Client](#). Если пользователь отклонит запрос, подключение завершится. Если в течение 30 секунд ответа не последует, подключение установится автоматически.

- **Разрешить по запросу**

В этом режиме администратор сможет удаленно подключиться к тонкому клиенту только после того, как пользователь [примет запрос на удаленное управление в интерфейсе Kaspersky Thin Client](#). Если пользователь отклонит запрос, подключение завершится.

- **Запретить**

В этом режиме администратор не сможет подключаться к тонкому клиенту удаленно.

Если вы установили режим **Разрешить автоматически** или **Разрешить по запросу**, блок параметров **Доступ к удаленной сессии** будет разблокирован.

8. В блоке параметров **Доступ к удаленной сессии** выберите режим доступа к экрану удаленной среды:

- **Разрешить автоматически**

В этом режиме после подключения к тонкому клиенту администратор сможет получать доступ к экрану удаленной среды без подтверждения пользователя.

- **Разрешить по запросу**

В этом режиме после подключения к тонкому клиенту администратор сможет получать доступ к экрану удаленной среды только после того, как пользователь [примет запрос на этот доступ в интерфейсе Kaspersky Thin Client](#).

- **Запретить**

В этом режиме администратор не сможет перейти к удаленному управлению тонким клиентом, пока пользователь самостоятельно не завершит удаленную сессию.

9. Нажмите на кнопку **Сохранить** в нижней части окна.

Изменения будут сохранены и применены в Kaspersky Thin Client, установленной на тонком клиенте, после синхронизации Kaspersky Thin Client и Kaspersky Security Center.

Настройка автоматического запуска и отображения приложений: одно устройство

В Web Console вы можете выбрать [приложение](#), которое будет автоматически запускаться после включения тонкого клиента и загрузки системы, а также указать, какие приложения будут отображаться на рабочем столе Kaspersky Thin Client.

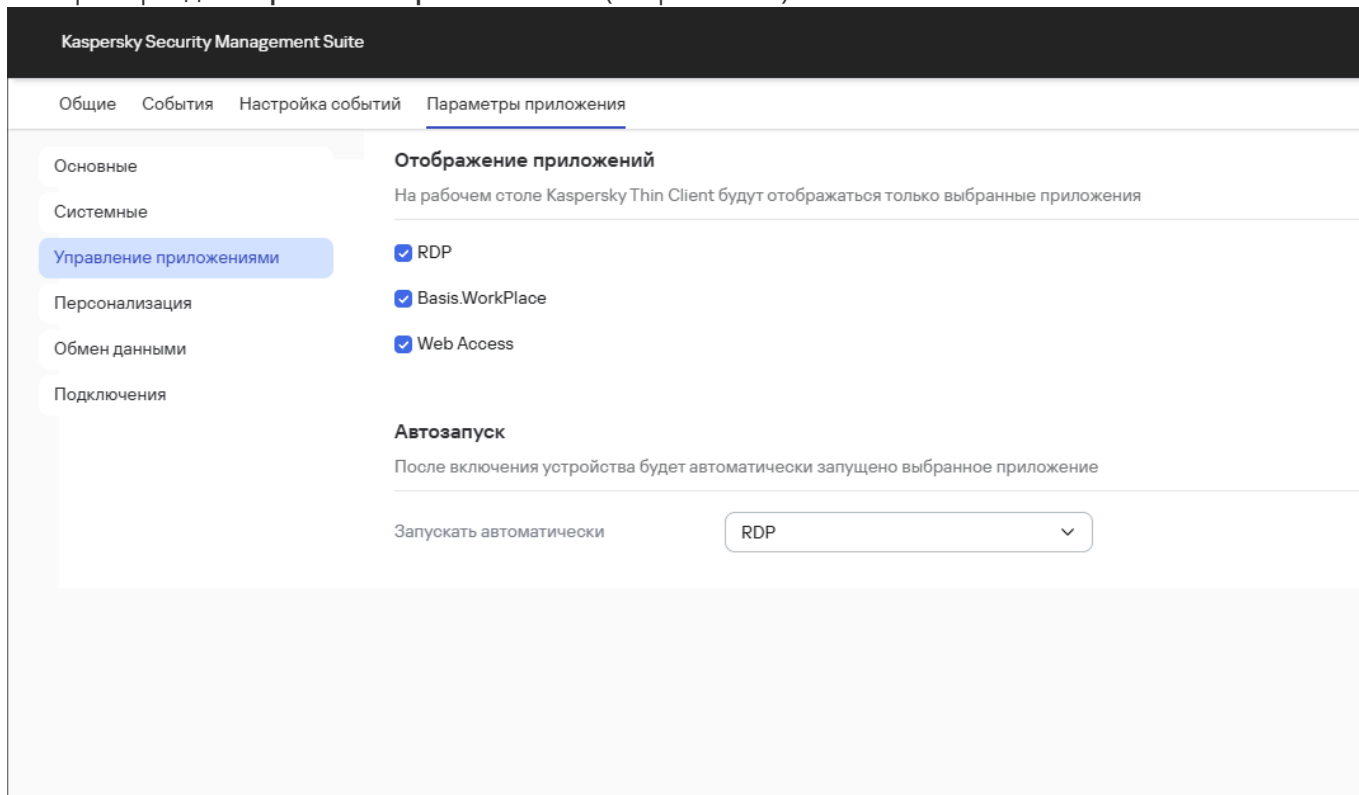
Чтобы настроить автоматический запуск и отображение приложений:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.
2. В отобразившемся списке нажмите на имя нужного тонкого клиента. Вы можете просмотреть имя устройства в [интерфейсе Kaspersky Thin Client](#). Если имя тонкого клиента отсутствует в списке, [добавьте его в группу администрирования](#).

Если настраиваемый параметр заблокирован в [политике, созданной для группы администрирования](#), такой параметр невозможно изменить при настройке отдельного устройства. [Измените](#) или [разблокируйте](#) этот параметр в политике.

3. В открывшемся окне выберите вкладку **Приложения**.
4. Нажмите на название веб-плагина управления Kaspersky Security Management Suite.
Откроется окно с информацией о Kaspersky Thin Client.
5. Выберите вкладку **Параметры приложения**.

6. Выберите раздел **Управление приложениями** (см. рис. ниже).



Окно настройки автоматического запуска и отображения приложений через Web Console

7. В блоке **Отображение приложений** установите флажки напротив приложений, которые будут отображаться на рабочем столе Kaspersky Thin Client.

В раскрывающемся списке **Запускать автоматически** выберите приложение, которое будет автоматически запускаться после включения устройства и загрузки системы. При выборе значения **Отключено** автоматический запуск будет выключен.

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

Изменения будут сохранены и применены в Kaspersky Thin Client, установленной на тонком клиенте, после синхронизации Kaspersky Thin Client и Kaspersky Security Center.

Настройка параметров Kaspersky Thin Client через Web Console для группы администрирования

В Web Console вы можете с помощью [политик](#) настраивать параметры Kaspersky Thin Client, установленной на тонких клиентах, которые подключены к Kaspersky Security Center и добавлены в [группу администрирования](#).

Настройка основных параметров Kaspersky Thin Client через Web Console: группа администрирования

В Web Console вы можете с помощью [политик](#) присваивать имена тонким клиентам в [группе администрирования](#) и задавать контактные данные администратора, которые будут отображаться в интерфейсе Kaspersky Thin Client, установленной на этих устройствах.

Чтобы настроить основные параметры Kaspersky Thin Client через Web Console:

1. В главном окне Web Console выберите **Активы (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 приложения**.
4. Выберите раздел **Основные** (см. рис. ниже).

The screenshot displays the 'Kaspersky Security Management Suite' interface. At the top, there's a navigation bar with tabs: 'Общие', 'Настройка событий', 'Параметры приложения' (which is active), and 'История ревизий'. Below this, on the left, is a sidebar with a list of settings categories: 'Основные' (highlighted in blue), 'Системные', 'Управление приложениями', 'Персонализация', 'Обмен данными', 'Подключения', and 'Сертификаты'. The main content area is titled 'Правило именования устройств в группе'. It contains a description: 'Все устройства в группе будут иметь составное название. Пример: Бухгалтерия-00000001-Воронеж.' Below this, there are two input fields: 'Имя' with a placeholder 'Введите имя' and 'Дополнительно' with a placeholder 'Введите дополнительную информацию'. Between these fields is a separator '- ID устройства -'. At the bottom of the main area, there's a section titled 'Контакты технической поддержки' with the text 'Пользователи будут видеть указанные здесь данные в интерфейсе Kaspersky Thin Client.' and a text area for 'Контактные данные' with a placeholder 'Укажите номер телефона и электронную почту Службы технической поддержки или администратора вашей организации'.

Окно настройки основных параметров Kaspersky Thin Client, установленной на тонких клиентах в группе администрирования, через Web Console

5. Настройте необходимые параметры:

- В блоке **Правило именования устройств в группе** введите имя и дополнительную информацию в соответствующих полях. Эти данные будут отображаться в названии каждого тонкого клиента, добавленного в группу администрирования. Вы можете ввести прописные и строчные буквы на кириллице или латинице, а также спецсимволы. Максимальная длина каждого поля – 10 символов.

В названии тонких клиентов также присутствует идентификатор (ID). Это уникальный набор из восьми символов, который автоматически формируется для каждого устройства, добавленного в группу администрирования. Вы можете [изменить идентификатор отдельного тонкого клиента](#).

- В блоке **Контакты технической поддержки** в поле **Контактные данные** введите номер телефона и имя администратора или, например, адрес электронной почты вашей службы технической поддержки. Количество символов в поле не должно быть более 80.

Введенная информация будет отображаться для тонких клиентов, добавленных в группу администрирования, в интерфейсе Kaspersky Thin Client: в панели управления, 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](#).

6. Если вы хотите, чтобы настроенные параметры применились в Kaspersky Thin Client, установленной на тонких клиентах в дочерних группах администрирования, и были недоступны для изменения в Kaspersky Thin Client на тонких клиентах в текущей группе администрирования, переведите [переключатели рядом с необходимыми блоками параметров](#) в положение **Принудительно**.

7. Нажмите на кнопку **Сохранить** в нижней части окна.

Изменения будут сохранены и применены в Kaspersky Thin Client, установленной на тонких клиентах, добавленных в группу администрирования, после синхронизации Kaspersky Security Center и Kaspersky Thin Client.

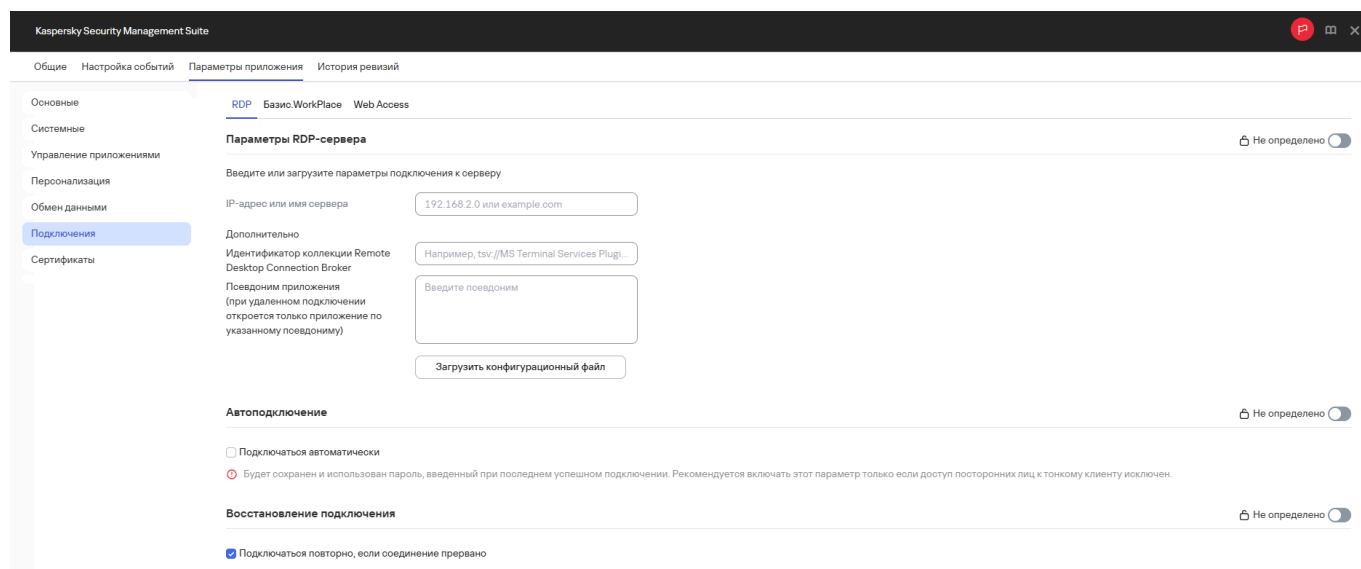
Настройка подключения к удаленной среде с помощью приложения RDP через Web Console: группа администрирования

В Web Console вы можете с помощью [политик](#) настраивать параметры [подключения к удаленной среде с помощью приложения RDP](#).

Чтобы настроить параметры подключения к удаленной среде с помощью приложения RDP:

1. В главном окне Web Console выберите **Активы (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 приложения**.
4. Выберите раздел **Подключения** → **RDP**.

Откроется окно настройки параметров подключения к удаленной среде (см. рис. ниже).



Окно настройки параметров подключения к удаленной среде в приложении RDP через Web Console: группа администрирования

- В поле **IP-адрес или имя сервера** введите соответствующие данные сервера для подключения к удаленной среде по протоколу RDP.
- Если для подключения к удаленному рабочему столу требуется использовать брокер Microsoft Remote Desktop Connection Broker, в поле **Идентификатор коллекции Remote Desktop Connection Broker** укажите идентификатор коллекции в формате `tsv://MS Terminal Services Plugin.1.collection_id`, где `collection_id` – идентификатор коллекции.

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

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

- Если вы хотите, чтобы подключение к удаленному рабочему столу восстанавливалось автоматически после разрыва соединения, установите флажок **Подключаться повторно, если соединение прервано**.
- В блоке параметров **Перенаправление устройств** выберите устройства, которые необходимо перенаправить в удаленную среду: **Смарт-карты, USB-накопители, Принтеры и другие устройства, Микрофон, Устройства воспроизведения звука, Веб-камера (видео), Сканер**.

Управление громкостью и другими параметрами звука и видео выполняется в удаленной среде.

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

9. 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.

10. Если на вашем рабочем месте установлено два монитора и вы хотите, чтобы изображение удаленной среды выводилось на оба монитора, в блоке **Управление мониторами** установите флажок **Использовать два монитора**.
11. Если требуется улучшить производительность при подключении к удаленным рабочим столам или приложениям, в блоке **Производительность** установите флажок **Улучшить графическую производительность**.

12. Если требуется автоматически подключаться к удаленному рабочему столу или виртуальному приложению при запуске приложения RDP, в блоке **Автоподключение** установите флажок **Подключаться автоматически**.

Для активации функции пользователю необходимо однократно подключиться к удаленной среде вручную и отключиться от нее. При этом в хранилище тонкого клиента будут сохранены следующие данные для подключения к RDP-серверу: имя пользователя, адрес сервера и пароль. При следующем запуске приложения RDP автоматически начнется подключение к удаленной среде с использованием этих данных. При выключении функции автоматического подключения сохраненный пароль будет удален из хранилища устройства.

В Web Console не поддерживается задание пароля для подключения к удаленной среде.

Для автоматического подключения к удаленной среде в приложении RDP сразу после загрузки Kaspersky Thin Client, [настройте автоматический запуск приложения](#).

13. Если вы хотите, чтобы настроенные параметры применились в Kaspersky Thin Client, установленной на тонких клиентах в дочерних группах администрирования, и были недоступны для изменения в Kaspersky Thin Client на тонких клиентах в текущей группе администрирования, переведите [переключатели рядом с необходимыми блоками параметров](#) в положение **Принудительно**.

14. Нажмите на кнопку **Сохранить** в нижней части окна.

Изменения будут сохранены и применены в Kaspersky Thin Client, установленной на тонких клиентах, добавленных в группу администрирования, после синхронизации Kaspersky Security Center и Kaspersky Thin Client.

Настройка подключения к удаленной среде с помощью приложения Базис.WorkPlace через Web Console: группа администрирования

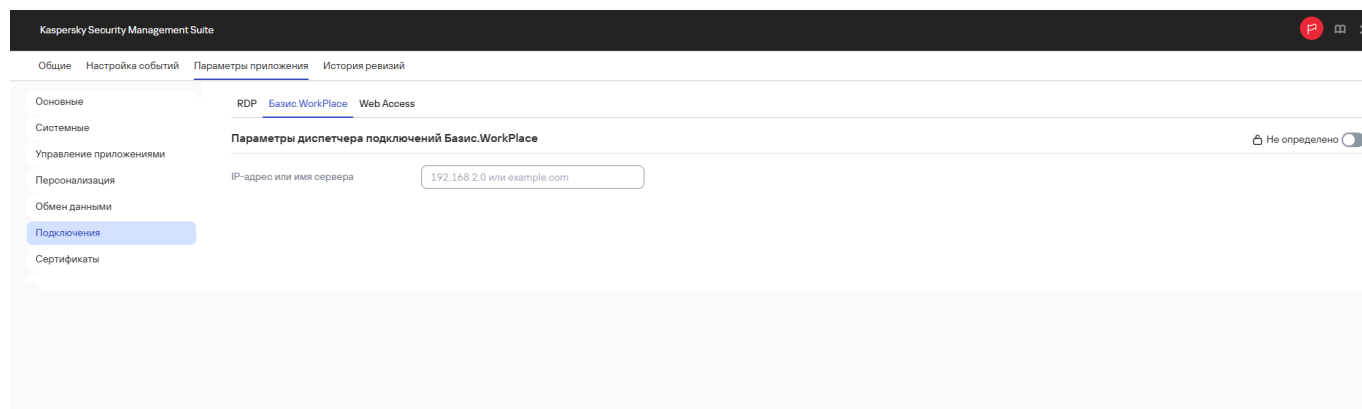
В Web Console вы можете с помощью [политик](#)  настраивать параметры [подключения к удаленной среде, развернутой в инфраструктуре Базис.WorkPlace](#).

Не поддерживается смена пароля пользователя, инициированная пользователем, через Kaspersky Thin Client.

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

1. В главном окне Web Console выберите **Активы (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 приложения**.
4. Выберите раздел **Подключения** → **Базис.WorkPlace**.

Откроется окно настройки параметров подключения к удаленной среде (см. рис. ниже).



Окно настройки параметров подключения к удаленной среде, развернутой в инфраструктуре Базис.WorkPlace, через Web Console: группа администрирования

5. В поле **IP-адрес или имя сервера** введите IP-адрес или имя сервера, к которому необходимо подключиться.
6. Если вы хотите, чтобы настроенные параметры применились в Kaspersky Thin Client, установленной на тонких клиентах в дочерних группах администрирования, и были недоступны для изменения в Kaspersky Thin Client на тонких клиентах в текущей группе администрирования, переведите [переключатели рядом с необходимыми блоками параметров](#) в положение **Принудительно**.
7. Нажмите на кнопку **Сохранить** в нижней части окна.

Изменения будут сохранены и применены в Kaspersky Thin Client, установленной на тонких клиентах, добавленных в группу администрирования, после синхронизации Kaspersky Security Center и Kaspersky Thin Client.

Настройка подключения к удаленной среде с помощью приложения Web Access через Web Console: группа администрирования

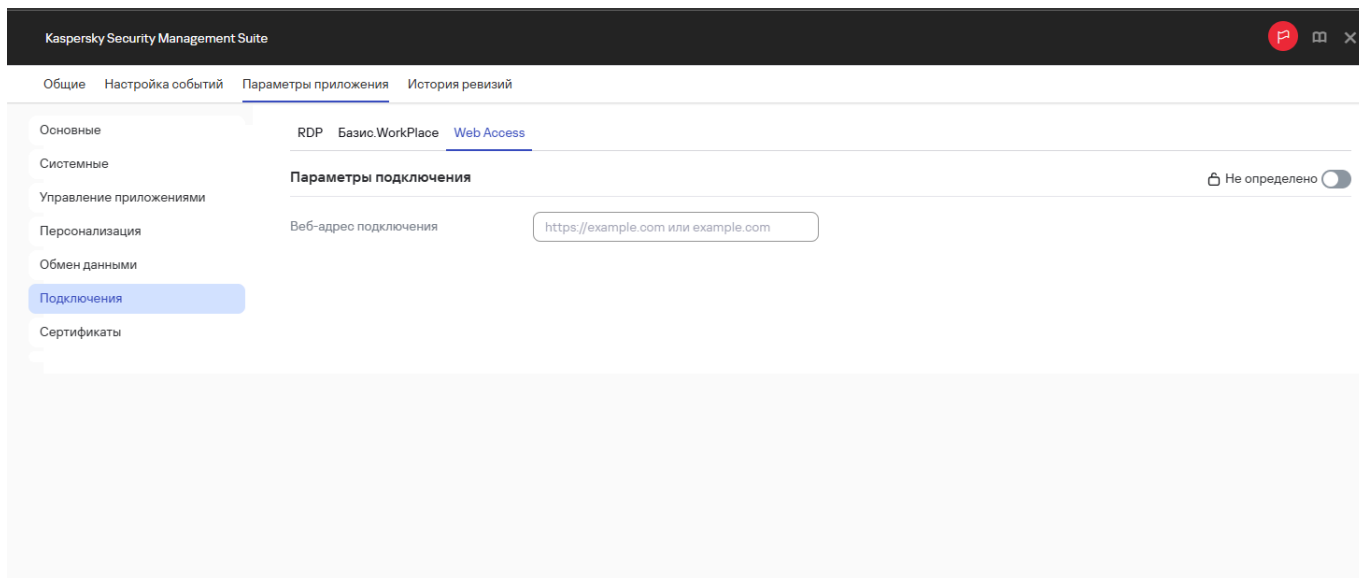
В Web Console вы можете с помощью [политик](#)  настраивать параметры [подключения к удаленной среде с помощью приложения Web Access](#).

С помощью приложения Web Access вы можете подключаться к удаленной среде, развернутой в инфраструктуре Citrix Workspace. Web Access поддерживает HTML5 и обеспечивает безопасное соединение HTTPS при подключении.

Чтобы настроить параметры подключения к удаленной среде с помощью приложения Web Access:

1. В главном окне Web Console выберите **Активы (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 приложения**.
4. Выберите раздел **Подключения** → **Web Access**.

Откроется окно настройки параметров подключения к удаленной среде (см. рис. ниже).



Окно настройки параметров подключения к удаленной среде с помощью приложения Web Access через Web Console: группа администрирования

5. В поле **Веб-адрес подключения** введите веб-адрес сервера для подключения к необходимой удаленной среде.
6. Если вы хотите, чтобы настроенные параметры применились в Kaspersky Thin Client, установленной на тонких клиентах в дочерних группах администрирования, и были недоступны для изменения в Kaspersky Thin Client на тонких клиентах в текущей группе администрирования, переведите [переключатели рядом с необходимыми блоками параметров](#) в положение **Принудительно**.
7. Нажмите на кнопку **Сохранить** в нижней части окна.

Изменения будут сохранены и применены в Kaspersky Thin Client, установленной на тонких клиентах, добавленных в группу администрирования, после синхронизации Kaspersky Security Center и Kaspersky Thin Client.

Настройка мониторов и экранов через Web Console: группа администрирования

В Web Console вы можете с помощью [политик](#)  настраивать мониторы, подключенные к тонким клиентам, и параметры экранов Kaspersky Thin Client.

Kaspersky Thin Client поддерживает подключение двух мониторов. Система считает один из мониторов основным, другой – дополнительным. На экране основного монитора отображается панель подключения во время [удаленной сессии](#) [?]. Экран дополнительного монитора расширяет или дублирует изображение основного. В Web Console вы можете выбрать, какой монитор будет считаться основным (далее также "изменить взаимное расположение мониторов").

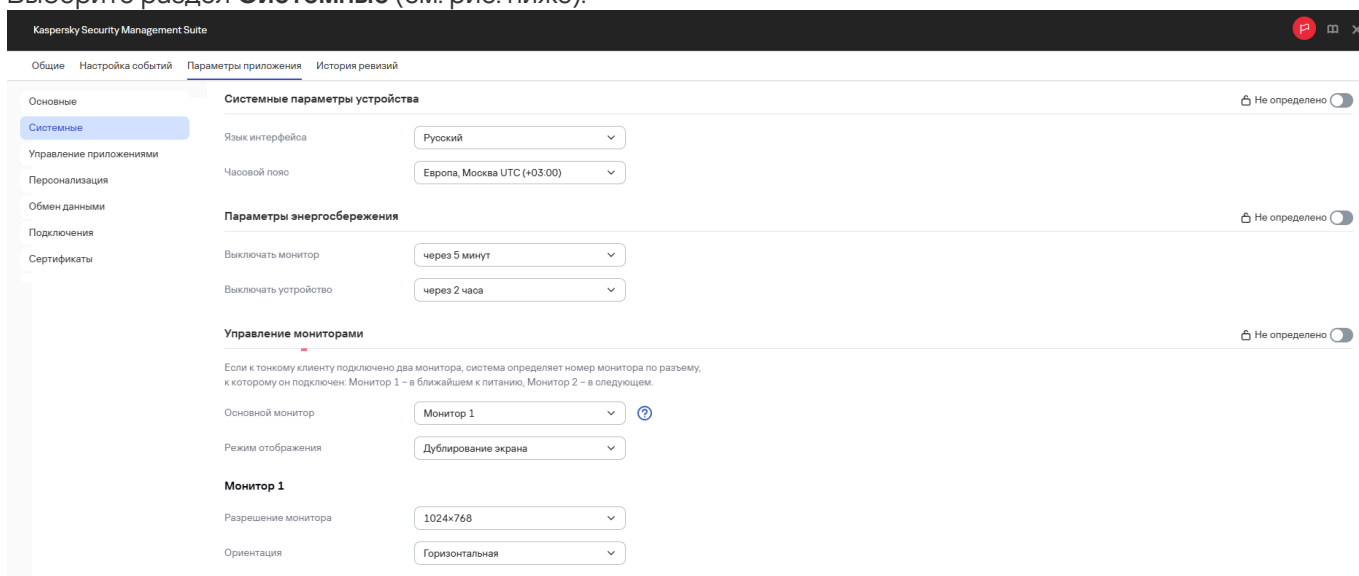
В интерфейсе Web Console мониторы пронумерованы. Система определяет номер монитора по разъему, через который он подключен к тонкому клиенту: монитор 1 – в ближайшем к питанию, монитор 2 – в следующем. Расположение разъемов на [поддерживаемых моделях тонких клиентов](#) вы можете посмотреть в документации производителей устройств.

В Web Console не отображается информация о том, сколько мониторов подключено к определенному тонкому клиенту.

Если вы хотите, чтобы экран удаленной сессии отображался на обоих мониторах, включите их использование в параметрах подключения к удаленной среде в приложении [RDP](#) или [Базис.WorkPlace](#).

Чтобы настроить мониторы и экраны через Web Console:

1. В главном окне Web Console выберите **Активы (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 приложения**.
4. Выберите раздел **Системные** (см. рис. ниже).



Окно настройки мониторов и экранов через Web Console: группа администрирования

5. В блоке **Управление мониторами** настройте необходимые параметры:

- В раскрывающемся списке **Основной монитор** выберите, какой монитор система должна считать основным.

Если к одному из тонких клиентов в группе администрирования подключен только один монитор, к нему будут применены настройки монитора, который выбран основным в Web Console.

- В раскрывающемся списке **Режим отображения** выберите способ вывода изображения на экраны мониторов:

- **Расширение экрана** – изображение распределяется между двумя мониторами.
- **Дублирование экрана** – изображение экрана основного монитора дублируется на дополнительном.

- В раскрывающемся списке **Разрешение монитора** выберите необходимое разрешение для выбранного экрана.

Поддерживаемые разрешения перечислены в [разделе с аппаратными и программными требованиями](#).

Если выбрано значение **Максимально возможное**, будет установлено наибольшее значение параметра, поддерживаемое монитором и Kaspersky Thin Client.

- В раскрывающемся списке **Ориентация** выберите положение экрана на мониторе:

- **Горизонтальная** – стандартное положение экрана.
- **Перевернутая горизонтальная** – экран повернут на 180°.
- **Вертикальная** – экран повернут на 90°.
- **Перевернутая вертикальная** – экран повернут на 270°.

6. Если вы хотите, чтобы настроенные параметры применились в Kaspersky Thin Client, установленной на тонких клиентах в дочерних группах администрирования, и были недоступны для изменения в Kaspersky Thin Client на тонких клиентах в текущей группе администрирования, переведите [переключатели рядом с необходимыми блоками параметров](#) в положение **Принудительно**.

7. Нажмите на кнопку **Сохранить** в нижней части окна.

Изменения будут сохранены и применены в Kaspersky Thin Client, установленной на тонких клиентах, добавленных в группу администрирования, после синхронизации Kaspersky Security Center и Kaspersky Thin Client.

Настройка системных параметров Kaspersky Thin Client через Web Console: группа администрирования

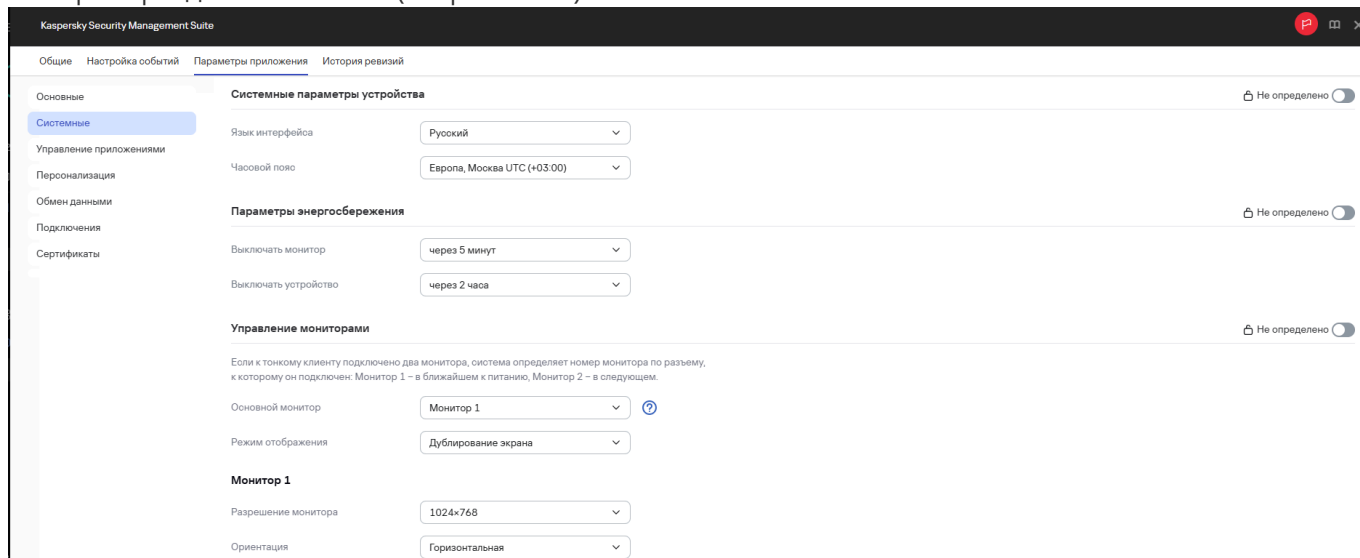
В Web Console вы можете с помощью [политик](#)  настраивать язык интерфейса и часовой пояс Kaspersky Thin Client, а также время выключения тонких клиентов и мониторов, подключенных к ним.

Kaspersky Thin Client 2.3 поддерживает следующие языки интерфейса: русский, английский (США), испанский (Мексика) и португальский (Бразилия).

Чтобы настроить системные параметры Kaspersky Thin Client через Web Console:

1. В главном окне Web Console выберите **Активы (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 приложения**.

4. Выберите раздел **Системные** (см. рис. ниже).



Окно настройки системных параметров через Web Console: группа администрирования

5. В блоке **Системные параметры устройства** в раскрывающихся списках **Язык интерфейса** и **Часовой пояс** выберите необходимые значения.

6. В блоке **Параметры энергосбережения** настройте следующее:

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

7. Если вы хотите, чтобы настроенные параметры применились в Kaspersky Thin Client, установленной на тонких клиентах в дочерних группах администрирования, и были недоступны для изменения в Kaspersky Thin Client на тонких клиентах в текущей группе администрирования, переведите [переключатели рядом с необходимыми блоками параметров](#) в положение **Принудительно**.

8. Нажмите на кнопку **Сохранить** в нижней части окна.

Изменения будут сохранены и применены в Kaspersky Thin Client, установленной на тонких клиентах, добавленных в группу администрирования, после синхронизации Kaspersky Security Center и Kaspersky Thin Client.

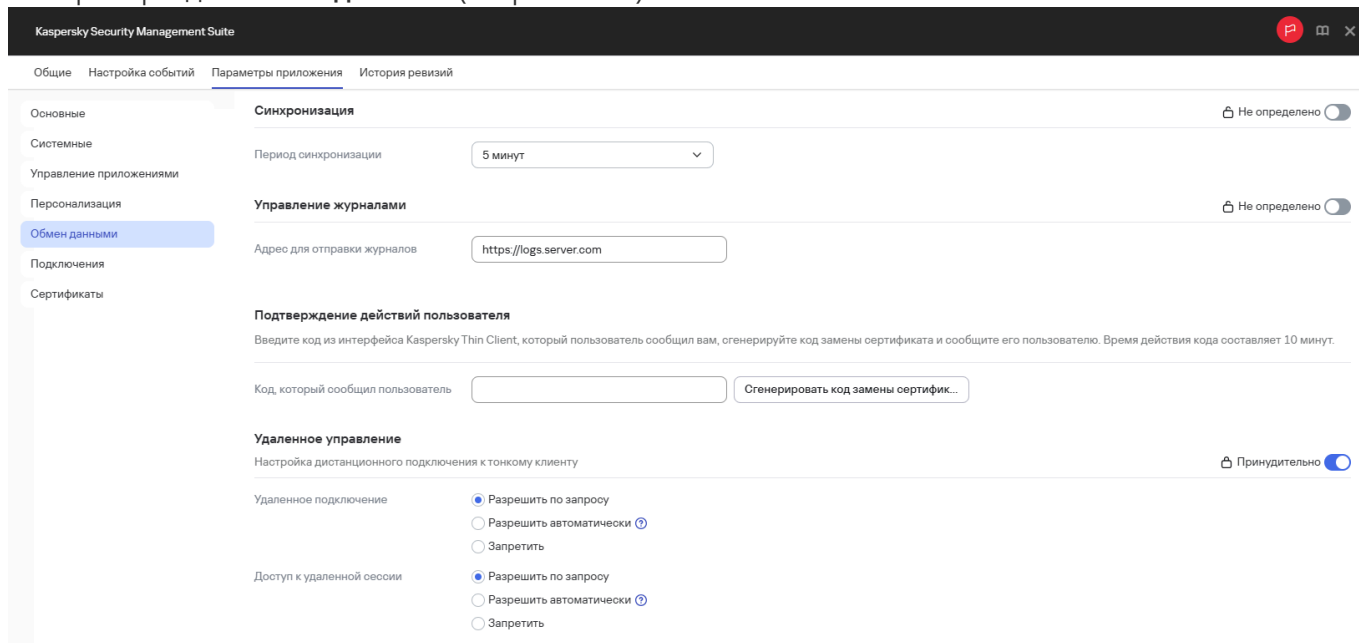
Настройка отправки журналов Kaspersky Thin Client на сервер журналирования: группа администрирования

В Web Console вы можете с помощью [политик](#) менять адрес [сервера журналирования](#) ^[?] на который отправляются [журналы событий и аудита](#) Kaspersky Thin Client.

Чтобы настроить отправку журналов событий и аудита на сервер журналирования через Web Console:

1. В главном окне Web Console выберите **Активы (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 приложения**.

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



Окно настройки отправки журналов Kaspersky Thin Client через Web Console: группа администрирования

5. В поле **Адрес для отправки журналов** введите адрес сервера журналирования, на который будут отправляться журналы, в формате `https://<адрес сервера>`.

Для получения журналов событий и аудита из Kaspersky Thin Client в инфраструктуре вашей организации должен быть развернут сервер журналирования с учетом [аппаратных и программных требований](#).

6. Если вы хотите, чтобы настроенные параметры применились в Kaspersky Thin Client, установленной на тонких клиентах в дочерних группах администрирования, и были недоступны для изменения в Kaspersky Thin Client на тонких клиентах в текущей группе администрирования, переведите [переключатели рядом с необходимыми блоками параметров](#) в положение **Принудительно**.

7. Нажмите на кнопку **Сохранить** в нижней части окна.

Изменения будут сохранены и применены в Kaspersky Thin Client, установленной на тонких клиентах, добавленных в группу администрирования, после синхронизации Kaspersky Security Center и Kaspersky Thin Client.

Настройка параметров персонализации Kaspersky Thin Client: группа администрирования

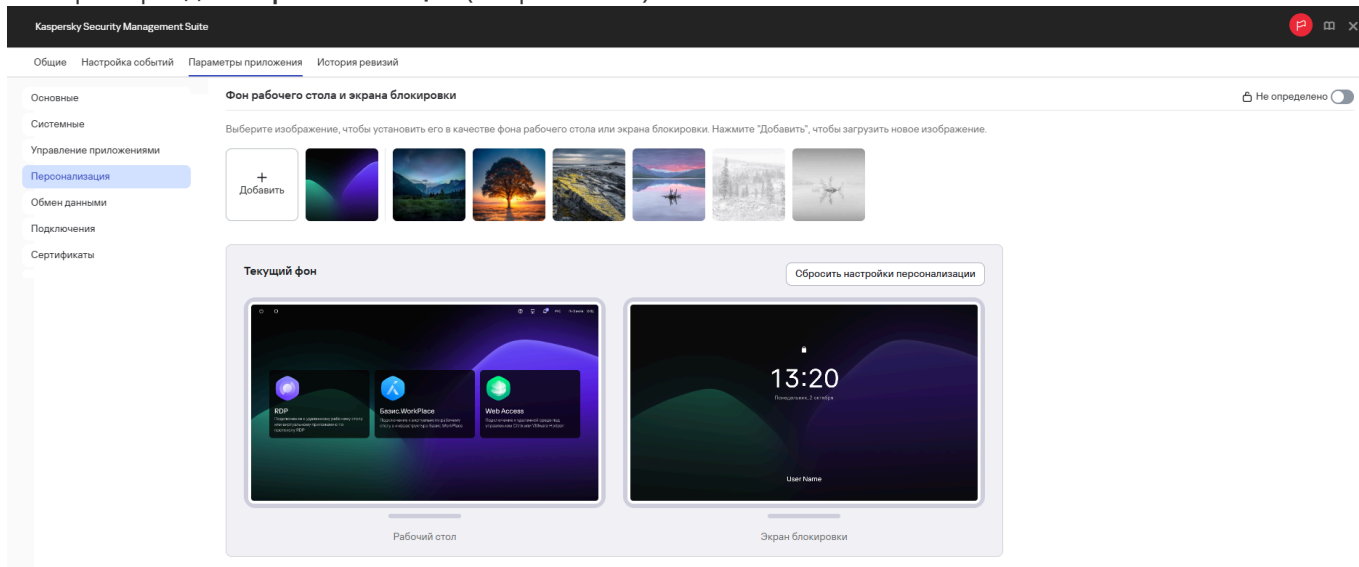
В Web Console вы можете с помощью [политик](#) загружать свои изображения и устанавливать их в качестве фона рабочего стола или экрана блокировки Kaspersky Thin Client. Поддерживаются файлы следующих форматов: JPEG, PNG, JPG. Максимальный размер файла: 15 МБ. Вы также можете удалять загруженные изображения из Web Console.

По умолчанию на рабочем столе и экране блокировки Kaspersky Thin Client установлен стандартный фон. Если вы устанавливали другой фон, вы можете сбросить настройки персонализации, чтобы снова установить стандартный.

Изменение фона в интерфейсе Kaspersky Thin Client не поддерживается – вы можете изменять фон экранов только через Web Console. Также изображение, установленное через Web Console, меняется на стандартный фон при [сбросе параметров системы](#).

Чтобы изменить фон экрана блокировки или рабочего стола Kaspersky Thin Client через Web Console:

1. В главном окне Web Console выберите **Активы (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 приложения**.
4. Выберите раздел **Персонализация** (см. рис. ниже).



Окно настройки параметров персонализации Kaspersky Thin Client через Web Console: группа администрирования

5. Чтобы изменить фон рабочего стола или экрана блокировки, выполните следующие действия:

а. Выберите необходимое изображение.

- Если вы хотите загрузить новое изображение в Web Console, нажмите на кнопку **Добавить**.
В открывшемся окне перетащите нужное изображение в область загрузки или нажмите **Загрузить файл или перетащить его сюда**, затем в открывшемся окне выберите нужное изображение.
- Если вы хотите установить уже загруженное в Web Console изображение, нажмите на его миниатюру.

Отобразится окно предпросмотра выбранного изображения на экранах Kaspersky Thin Client.

Если вы хотите сохранить изображение в Web Console, не устанавливая его в качестве фона, перейдите к шагу с этой инструкции.

б. Установите флажки напротив экранов, на которых нужно установить изображение в качестве фона:

- **Рабочий стол** – изображение будет установлено в качестве [фона рабочего стола Kaspersky Thin Client](#).
- **Экран блокировки** – изображение будет установлено в качестве [фона экрана блокировки](#).

с. Нажмите **Сохранить** в окне предпросмотра.

Отобразится основной экран раздела **Персонализация**. На выбранных экранах будет установлен выбранный вами фон.

6. Чтобы удалить загруженное в Web Console изображение, наведите курсор на его миниатюру, затем нажмите на отобразившуюся кнопку .

Подтвердите свои действия в отобразившемся окне.

Изображение будет безвозвратно удалено из Web Console. Если изображение было выбрано в качестве фона на каком-либо экране, вместо него будет установлен стандартный фон.

7. Чтобы установить стандартный фон на все экраны, нажмите **Сбросить параметры персонализации** и подтвердите свои действия в открывшемся окне.
8. На рабочем столе и экране блокировки Kaspersky Thin Client будет установлен стандартный фон.
9. Если вы хотите, чтобы настроенные параметры применились в Kaspersky Thin Client, установленной на тонких клиентах в дочерних группах администрирования, и были недоступны для изменения в Kaspersky Thin Client на тонких клиентах в текущей группе администрирования, переведите [переключатели рядом с необходимыми блоками параметров](#) в положение **Принудительно**.
10. Нажмите на кнопку **Сохранить** в нижней части окна раздела **Персонализация**.

Изменения будут сохранены и применены на тонких клиентах, добавленных в группу администрирования, в течение часа после синхронизации Kaspersky Security Center и Kaspersky Thin Client.

Настройка параметров удаленного подключения к тонкому клиенту через Web Console: группа администрирования

В Web Console вы можете с помощью [политик](#)  настраивать следующие параметры удаленного подключения к устройству:

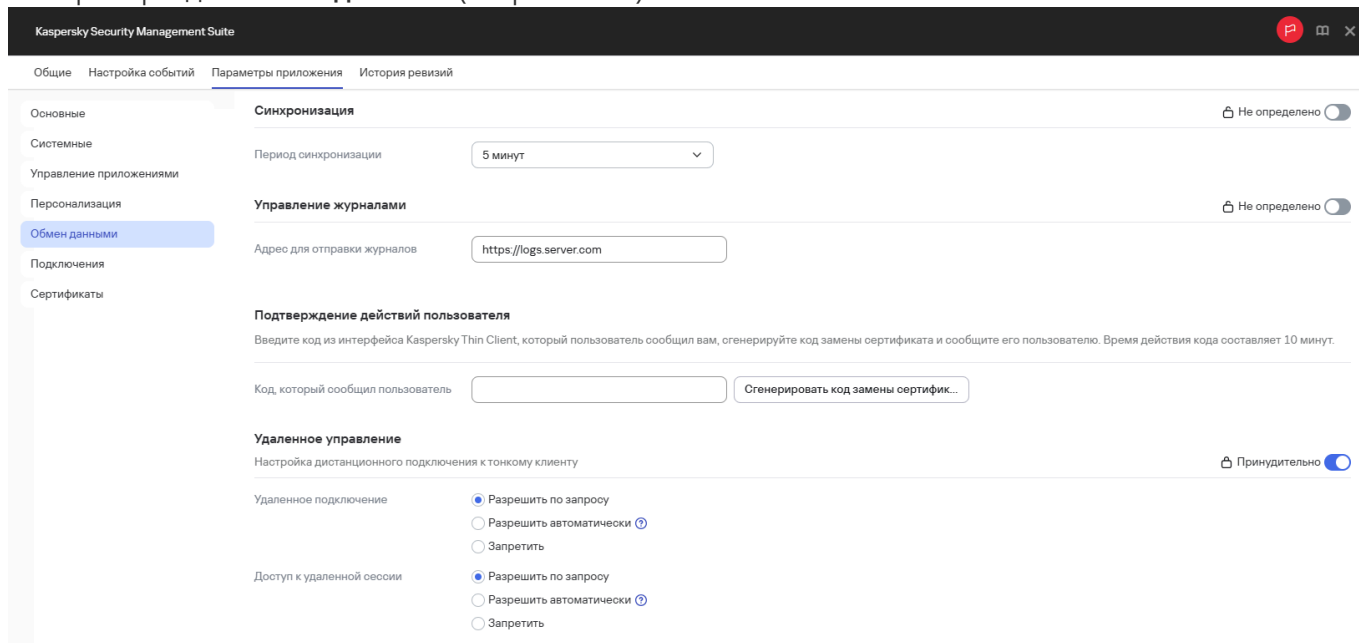
- Режим доступа к удаленному управлению – определяет условия и порядок подключения к тонкому клиенту.
- Режим доступа к удаленной сессии, запущенной на тонком клиенте в момент подключения к нему (далее также "экран удаленной среды").

Ограничение доступа к экрану удаленной среды может понадобиться, если пользователь тонкого клиента работает с чувствительными или конфиденциальными данными.

Чтобы настроить параметры удаленного подключения к тонкому клиенту:

1. В главном окне Web Console выберите **Активы (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 приложения**.

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



Окно настройки параметров удаленного подключения к тонкому клиенту через Web Console: группа администрирования

5. В разделе **Удаленное управление** выберите режим доступа к удаленному управлению тонким клиентом:

- **Разрешить автоматически**

В этом режиме администратор сможет удаленно подключиться к тонкому клиенту после того, как пользователь [примет запрос на удаленное управление в интерфейсе Kaspersky Thin Client](#). Если пользователь отклонит запрос, подключение завершится. Если в течение 30 секунд ответа не последует, подключение установится автоматически.

- **Разрешить по запросу**

В этом режиме администратор сможет удаленно подключиться к тонкому клиенту только после того, как пользователь [примет запрос на удаленное управление в интерфейсе Kaspersky Thin Client](#). Если пользователь отклонит запрос, подключение завершится.

- **Запретить**

В этом режиме администратор не сможет подключаться к тонкому клиенту удаленно.

Если вы установили режим **Разрешить автоматически** или **Разрешить по запросу**, блок параметров **Доступ к удаленной сессии** будет разблокирован.

6. В блоке параметров **Доступ к удаленной сессии** выберите режим доступа к экрану удаленной среды:

- **Разрешить автоматически**

В этом режиме после подключения к тонкому клиенту администратор сможет получать доступ к экрану удаленной среды без подтверждения пользователя.

- **Разрешить по запросу**

В этом режиме после подключения к тонкому клиенту администратор сможет получать доступ к экрану удаленной среды только после того, как пользователь [примет запрос на этот доступ в интерфейсе Kaspersky Thin Client](#).

- **Запретить**

В этом режиме администратор не сможет перейти к удаленному управлению тонким клиентом, пока пользователь самостоятельно не завершит удаленную сессию.

7. Если вы хотите, чтобы настроенные параметры применились в Kaspersky Thin Client, установленной на тонких клиентах в дочерних группах администрирования, и были недоступны для изменения в Kaspersky Thin Client на тонких клиентах в текущей группе администрирования, переведите [переключатели рядом с необходимыми блоками параметров](#) в положение **Принудительно**.

8. Нажмите на кнопку **Сохранить** в нижней части окна.

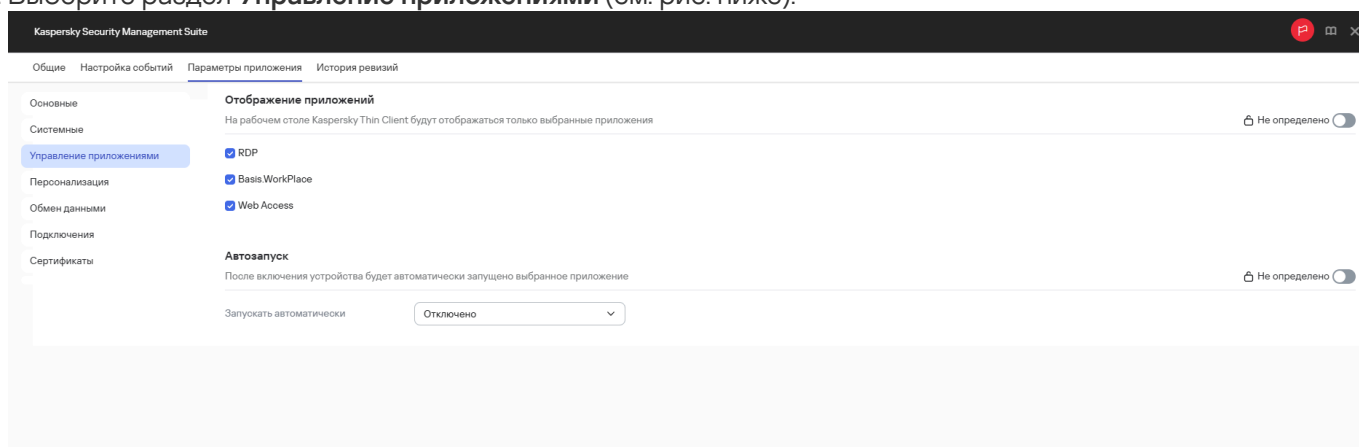
Изменения будут сохранены и применены в Kaspersky Thin Client, установленной на тонких клиентах, добавленных в группу администрирования, после синхронизации Kaspersky Security Center и Kaspersky Thin Client.

Настройка автоматического запуска и отображения приложений: группа администрирования

В Web Console вы можете с помощью [политик](#) выбрать [приложение](#), которое будет автоматически запускаться после включения устройства и загрузки системы, а также указать, какие приложения будут отображаться на рабочем столе Kaspersky Thin Client.

Чтобы настроить автоматический запуск и отображение приложений:

1. В главном окне Web Console выберите **Активы (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 приложения**.
4. Выберите раздел **Управление приложениями** (см. рис. ниже).



Окно настройки автоматического запуска и отображения приложений через Web Console: группа администрирования

5. В блоке **Отображение приложений** установите флажки напротив приложений, которые будут отображаться на рабочем столе Kaspersky Thin Client.

В раскрывающемся списке **Запускать автоматически** выберите приложение, которое будет автоматически запускаться после включения устройства и загрузки системы. При выборе значения **Отключено** автоматический запуск будет выключен.

6. Если вы хотите, чтобы настроенные параметры применились в Kaspersky Thin Client, установленной на тонких клиентах в дочерних группах администрирования, и были недоступны для изменения в Kaspersky Thin Client на тонких клиентах в текущей группе администрирования, переведите [переключатели рядом с необходимыми блоками параметров](#) в положение **Принудительно**.

7. Нажмите на кнопку **Сохранить** в нижней части окна.

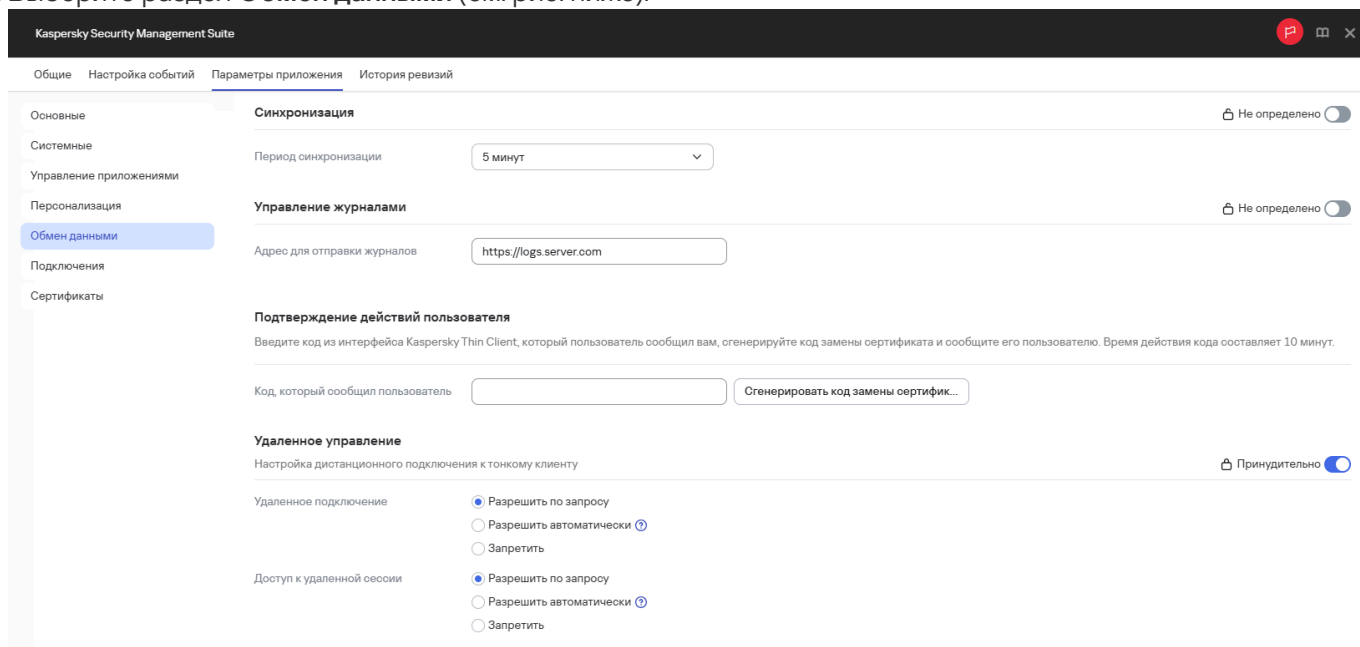
Изменения будут сохранены и применены в Kaspersky Thin Client, установленной на тонких клиентах, добавленных в группу администрирования, после синхронизации Kaspersky Security Center и Kaspersky Thin Client.

Настройка синхронизации Kaspersky Thin Client и Kaspersky Security Center

В Web Console вы можете настроить период синхронизации Kaspersky Thin Client и Kaspersky Security Center только с помощью [ПОЛИТИК ?](#).

Чтобы настроить синхронизацию Kaspersky Thin Client и Kaspersky Security Center:

1. В главном окне Web Console выберите **Активы (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 приложения**.
4. Выберите раздел **Обмен данными** (см. рис. ниже).



Окно настройки синхронизации Kaspersky Thin Client и Kaspersky Security Center

5. В раскрывающемся списке **Период синхронизации** выберите время, через которое будет выполняться синхронизация Kaspersky Thin Client и Kaspersky Security Center.

6. Если вы хотите, чтобы настроенные параметры применились в Kaspersky Thin Client, установленной на тонких клиентах в дочерних группах администрирования, и были недоступны для изменения в Kaspersky Thin Client на тонких клиентах в текущей группе администрирования, переведите [переключатели рядом с необходимыми блоками параметров](#) в положение **Принудительно**.

7. Нажмите на кнопку **Сохранить** в нижней части окна.

Изменения будут сохранены и применены в Kaspersky Thin Client, установленной на тонких клиентах, добавленных в группу администрирования, после синхронизации Kaspersky Security Center и Kaspersky Thin Client.

Подтверждение действий пользователя Kaspersky Thin Client

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

- [изменение параметров подключения к Kaspersky Security Center](#);
- [изменение сертификата для подключения к Kaspersky Security Center](#);
- [сброс всех параметров и данных тонкого клиента](#).

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

Чтобы подтвердить изменение параметров подключения к Kaspersky Security Center или сброс параметров Kaspersky Thin Client:

1. В главном окне Web Console выберите **Активы (Устройства)** → **Управляемые устройства**.
2. В отобразившемся списке нажмите на имя нужного тонкого клиента. Вы можете просмотреть имя устройства в [интерфейсе Kaspersky Thin Client](#). Если имя тонкого клиента отсутствует в списке, [добавьте его в группу администрирования](#).

Если настраиваемый параметр заблокирован в [политике, созданной для группы администрирования](#), такой параметр невозможно изменить при настройке отдельного устройства. [Измените](#) или [разблокируйте](#) этот параметр в политике.

3. В открывшемся окне выберите вкладку **Приложения**.
4. Нажмите на название веб-плагина управления Kaspersky Security Management Suite.
Откроется окно с информацией о Kaspersky Thin Client.
5. Выберите вкладку **Параметры приложения**.
6. Выберите раздел **Обмен данными**.

7. В блоке **Подтверждение действий пользователя** введите код из интерфейса Kaspersky Thin Client, который сообщил вам пользователь, и нажмите на кнопку **Сгенерировать код подтверждения**.

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

8. Сообщите код подтверждения пользователю Kaspersky Thin Client.

Чтобы подтвердить изменение сертификата для подключения к Kaspersky Security Center:

1. В главном окне Web Console выберите **Активы (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 приложения**.

4. Выберите раздел **Обмен данными**.

5. В блоке **Подтверждение действий пользователя** введите код из интерфейса Kaspersky Thin Client, который сообщил вам пользователь, и нажмите на кнопку **Сгенерировать код замены сертификата**.

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

6. Сообщите код замены сертификата пользователю Kaspersky Thin Client.

Управление сертификатами Kaspersky Thin Client через Web Console

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

Рекомендуется настроить [подключение тонких клиентов в группе администрирования](#) к серверу журналирования и к удаленной среде только с применением сертификатов, назначенных администратором в Web Console. Это поможет предотвратить подключение Kaspersky Thin Client к недоверенным узлам.

В этом разделе также приведены [инструкции по управлению сертификатами для подключения Kaspersky Thin Client к Kaspersky Security Center](#).

О сертификате для подключения Kaspersky Thin Client к Kaspersky Security Center

Kaspersky Thin Client использует для подключения к Kaspersky Security Center *пользовательский мобильный сертификат* (далее также: сертификат). Подробную информацию об этом и других типах сертификатов, используемых Kaspersky Security Center, см. в [онлайн-справке Kaspersky Security Center](#) ¹².

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

Пользовательские мобильные сертификаты не перевыпускаются автоматически.

Вы можете [перевыпустить сертификат в Web Console](#) или [создать новый сертификат](#) вручную и [загрузить его в Web Console](#).

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

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

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

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

1. В меню Kaspersky Security Center Web Console нажмите на кнопку  рядом с именем Сервера администрирования Kaspersky Security Center.
Откроется окно **Свойства Сервера администрирования**.
2. Выберите подраздел **Сертификаты**.
3. В открывшемся окне в блоке **Аутентификация Сервера администрирования мобильными устройствами** выберите необходимый сертификат и нажмите **Перевыпустить**.
4. В открывшемся окне задайте адрес Сервера и укажите, когда требуется активировать сертификат, затем подтвердите свой выбор.
5. Нажмите **Сохранить** в открывшемся окне.

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

Устройства, входящие в [группу администрирования](#) , получают перевыпущенный сертификат для подключения к Kaspersky Security Center после синхронизации Kaspersky Thin Client и Kaspersky Security Center. Перевыпущенный сертификат сохраняется в хранилище сертификатов Kaspersky Thin Client и может быть использован в качестве резервного для подключения тонких клиентов к Kaspersky Security Center, когда закончится срок действия текущего сертификата.

Вы также можете [вручную выпустить новый сертификат](#) для подключения Kaspersky Thin Client к Kaspersky Security Center.

Создание сертификата для подключения Kaspersky Thin Client к Kaspersky Security Center

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

Предварительно рекомендуется ознакомиться с требованиями, которые предъявляются к сертификатам Kaspersky Security Center, в [онлайн-справке Kaspersky Security Center](#).

Созданный сертификат необходимо [загрузить в Web Console](#).

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

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

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

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

где:

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

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

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

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

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

Если вы [создали сертификат](#) для подключения Kaspersky Thin Client к Kaspersky Security Center, необходимо загрузить такой сертификат в Web Console для передачи на тонкие клиенты, добавленные в [группу администрирования](#) [?](#).

Предварительно рекомендуется ознакомиться с требованиями, которые предъявляются к сертификатам 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 кнопку  рядом с именем Сервера администрирования Kaspersky Security Center.
Откроется окно **Свойства Сервера администрирования**.
2. 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:
5. В раскрывающемся списке **Тип сертификата** выберите **X.509-сертификат**:
 - a. Введите пароль, если пользовательский сертификат защищен паролем.
 - b. Выберите файл пользовательского сертификата, нажав на кнопку **Обзор** в блоке **Сертификат**.
 - c. Выберите закрытый ключ для пользовательского сертификата, нажав на кнопку **Обзор** в блоке **Приватный ключ**.
6. Нажмите на кнопку **Сохранить**, чтобы сохранить добавление сертификата.
7. 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. Устройства, входящие в группу администрирования, получат новый сертификат после синхронизации Kaspersky Thin Client и Kaspersky Security Center.

Добавление новых сертификатов в Web Console

В Web Console вы можете добавлять [сертификаты](#) для подключения к удаленной среде или к серверу журналирования. Для этого тонкий клиент должен быть [добавлен в группу администрирования](#).

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

Чтобы добавить новые сертификаты через Web Console:

1. В главном окне Web Console выберите **Активы (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 приложения**.
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**.

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

Удаление сертификатов в Web Console

В Web Console вы можете удалять сертификаты, назначенные тонким клиентам в [группе администрирования](#) .

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

Чтобы удалить сертификаты:

1. В главном окне Web Console выберите **Активы (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 приложения**.
4. Выберите раздел **Сертификаты**.
5. В таблице **Действительные сертификаты** установите флажки около тех сертификатов, которые требуется удалить.
6. Нажмите на кнопку **Удалить** и подтвердите свои действия.

Выбранные сертификаты будут удалены.

Конвертация сертификата из формата PEM в формат DER

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

Для выполнения инструкции на локальном компьютере требуется наличие утилиты OpenSSL.

Чтобы конвертировать файл сертификата из формата PEM в формат DER:

1. На локальном компьютере запустите консоль.
2. Перейдите в директорию, в которой расположен файл сертификата в формате PEM и выполните команду конвертации файла:

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

где:

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

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

Обновление сертификата при миграции на новый Сервер Kaspersky Security Center

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

Чтобы выпустить и подготовить новый сертификат:

1. Запустите консоль и перейдите в директорию, в которой вы хотите создать сертификат.
2. Запустите утилиту OpenSSL и выпустите сертификат с помощью следующей команды:

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

Созданные файлы сертификата и ключа будут сохранены локально.

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

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

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

В результате файл контейнера в формате PFX будет сохранен локально.

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

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

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

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

После выполнения команды произойдет перезагрузка Kaspersky Security Center.

[Резервный сертификат](#) будет загружен в Web Console.

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

в консоли запустите утилиту klsetsrvcert и выполните следующую команду:

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

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

Мониторинг событий Kaspersky Thin Client через Kaspersky Security Center Web Console

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

Настройка регистрации уведомлений о событиях Kaspersky Thin Client через 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:

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

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

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

Как настроить уведомления о событиях для одного устройства

1. В главном окне Kaspersky Security Center Web Console выполните одно из следующих действий:
 - Если тонкий клиент входит в группу администрирования, выберите **Активы (Устройства)** → **Управляемые устройства**.
 - Если тонкий клиент не добавлен в группу администрирования, выберите **Обнаружение устройств и развертывание** → **Нераспределенные устройства**.
 2. Нажмите на имя устройства, на котором запущен Kaspersky Thin Client. Вы можете просмотреть имя устройства [в интерфейсе Kaspersky Thin Client](#).
 3. В открывшемся окне выберите вкладку **Приложения**.
 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 устройств в группе администрирования

1. В главном окне Web Console выберите **Активы (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 [онлайн-справке Kaspersky Security Center](#).

Просмотр событий Kaspersky Thin Client через Web Console

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

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

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

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

2. Нажмите на имя требуемого устройства. Имя устройства указано в [интерфейсе Kaspersky Thin Client](#).

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

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

- **Время** – дата и время, когда событие, зарегистрированное Kaspersky Thin Client, было получено в Web Console.
- **Событие** – тип события.
- **Описание** – краткое описание зарегистрированного события.
- **Приложение** – название приложения, для которого событие было получено в Web Console.
- **Номер версии** – версия приложения, для которого событие было получено в Web Console.
- **Уровень важности** – уровень критичности события.
- **Задача** – имя задачи, запускаемой при регистрации события.
- **Зарегистрировано** – дата и время, когда событие было зарегистрировано Kaspersky Thin Client.

Устранение неисправностей

При возникновении ошибки требуется убедиться в следующем:

1. [Тонкий клиент включен](#).
2. [Тонкий клиент подключен к сети](#).
3. [При подключении к удаленной среде были введены верные IP-адрес или имя сервера, имя пользователя и пароль](#).

Если устранить ошибку не удастся, обратитесь в [Службу технической поддержки](#). При необходимости специалисты Службы технической поддержки могут запросить у вас сведения о системе или [журналы событий и аудита](#).

Разрыв соединения с удаленной средой

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

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

Чтобы возобновить работу в удаленной сессии:

1. Закройте сообщение об ошибке.
2. Попробуйте подключиться к удаленной среде.
3. Если подключение установить не удалось, обратитесь к администратору вашей организации, чтобы устранить физические причины, приводящие к разрыву соединения Kaspersky Thin Client с удаленным рабочим столом.
4. Если установлено прямое подключение, но по-прежнему не удастся подключиться к удаленному рабочему столу, обратитесь в [Службу технической поддержки](#).

Проблемы с разделением доступа к функциям веб-плагина управления Kaspersky Security Management Suite

После [установки](#) или [обновления](#) веб-плагина управления Kaspersky Security Management Suite у [пользователей с полным набором прав](#) может не быть доступа к некоторым функциям программы.

Чтобы исправить проблемы с разделением доступа к функциям веб-плагина:

1. Поместите файл RBAC из [комплекта поставки веб-плагина](#) в следующие директории на [Сервере администрирования](#) ^[?]:

a. <директория установки Kaspersky Security Center>/rbac

b. /var/opt/kaspersky/klnagent_srv/1093/dat/rbac

2. Перезагрузите Сервер администрирования.

Пользователи должны получить права на доступ к функциям веб-плагина в соответствии со своими ролями.

Если устранить проблему не удалось, обратитесь в [Службу технической поддержки](#).

Обращение в Службу технической поддержки

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

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

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

О журналах Kaspersky Thin Client

Kaspersky Thin Client ведет два типа журналов:

- Журнал событий. В этом журнале хранятся все события, регистрируемые компонентами Kaspersky Thin Client. Вы можете просмотреть журнал событий через интерфейс Kaspersky Thin Client, а также отправить его на сервер журналирования.
- Журнал аудита. В этом журнале хранятся ключевые события работы тонкого клиента, например: взаимодействие с сертификатами для подключения к Kaspersky Security Center; сведения о Сервере администрирования и факты подключения или отключения от него; сброс параметров устройства. Журнал аудита недоступен для просмотра через интерфейс Kaspersky Thin Client. Вы можете отправить файл журнала аудита на сервер журналирования.

Журнал событий

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

Журнал аудита Kaspersky Thin Client содержит следующие события и данные о них:

- Добавление, замена и переключение сертификата для подключения к Kaspersky Security Center в интерфейсе Kaspersky Thin Client:
 - дата и время события;
 - IP-адрес и/или доменное имя Сервера администрирования Kaspersky Security Center;
 - номер порта Сервера администрирования Kaspersky Security Center;
 - идентификатор тонкого клиента;
 - список атрибутов сертификата: имя издателя, имя субъекта, отпечаток сертификата, дата и время начала действия, дата и время окончания действия.
- Включение (вручную и автоматически) и выключение управления Kaspersky Thin Client через Kaspersky Security Center:
 - дата и время события;
 - IP-адрес и/или доменное имя Сервера администрирования Kaspersky Security Center;
 - номер порта Сервера администрирования Kaspersky Security Center;
 - идентификатор тонкого клиента.
- Сброс параметров Kaspersky Thin Client:
 - дата и время события;
 - идентификатор тонкого клиента.

- Принятие удаленного подключения к тонкому клиенту:
 - дата и время события;
 - IP-адрес и\или доменное имя пользователя, который подключался к тонкому клиенту;
 - имя пользователя, который подключался к тонкому клиенту.
- Создание нового файла журнала аудита в случае ротации:
 - дата и время события;
 - идентификатор тонкого клиента;
 - версия Kaspersky Thin Client.
- Сохранение и удаление пароля пользователя для автоматического подключения к удаленной среде:
 - дата и время события;
 - имя пользователя, используемое для подключения к удаленной среде.

Отправка журналов

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

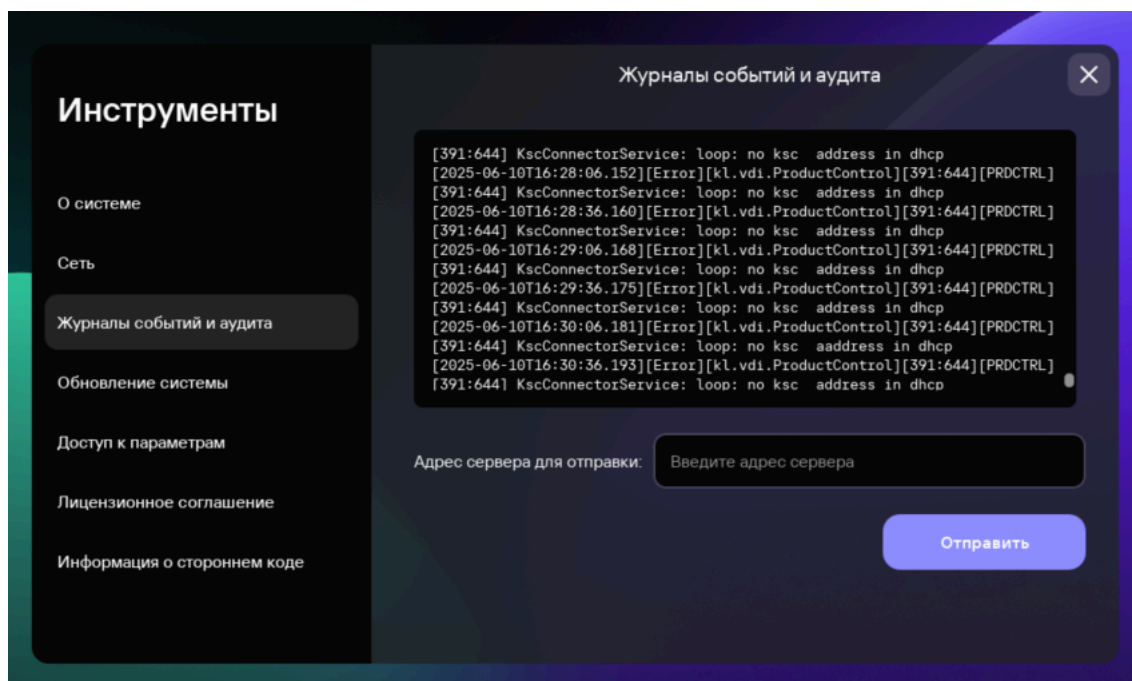
Необходимо предварительно развернуть [сервер журналирования](#) в инфраструктуре вашей организации. Подробную информацию о развертывании сервера см. в руководстве администратора к этому серверу.

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

Чтобы отправить журналы событий и аудита Kaspersky Thin Client:

1. В панели управления Kaspersky Thin Client нажмите на кнопку  и в открывшемся меню выберите **Инструменты**.
2. В открывшемся окне выберите раздел **Журналы событий и аудита** (см. рис. ниже).

В этом разделе отображаются записи журнала событий. Записи журнала аудита не отображаются в интерфейсе Kaspersky Thin Client.



Инструменты. Раздел Журналы событий и аудита

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 тонкий клиент входит в [группу администрирования](#), адрес сервера журналирования может быть [принудительно задан через Web Console](#). В этом случае его изменение в интерфейсе Kaspersky Thin Client будет недоступно.

Рекомендуется проверить правильность адреса сервера, на который вы отправляете журналы. Если указан неверный адрес, журналы могут попасть к третьим лицам.

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

Если устройство не входит в [группу администрирования](#), и вы в первый раз выполняете отправку журналов событий и аудита на сервер журналирования, отобразится окно с предложением добавить [сертификат для подключения к серверу журналирования](#).

Проверьте параметры добавляемого сертификата и нажмите на кнопку **Добавить сертификат**. Сертификат будет добавлен в системное хранилище сертификатов Kaspersky Thin Client и будет использоваться при следующих подключениях.

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

Глоссарий

TLS

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

Администратор Kaspersky Security Center

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

Брокер

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

Виртуальное приложение

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

Группа администрирования

Набор устройств под управлением Kaspersky Security Center, объединенных в соответствии с выполняемыми функциями. Устройства группируются для удобства управления ими как единым целым. В состав группы могут входить другие группы. Для каждого добавленного в группу устройства могут быть созданы групповые политики и сформированы групповые задачи.

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 системы Kaspersky Thin Client, установленной на устройствах группы администрирования. Вы можете создать неограниченное количество различных политик для Kaspersky Thin Client, установленной на устройствах в каждой группе администрирования, но в пределах группы администрирования только одна политика может применяться одновременно 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.

Сервер журналирования

Сервер, на который будут отправляться [журналы событий и аудита](#) Kaspersky Thin Client. Разворачивается в инфраструктуре вашей организации.

Событие

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

Тонкий клиент

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

Удаленная сессия

Сеанс работы в удаленной среде, к которой пользователь подключился через интерфейс тонкого клиента.

Удаленная среда

Любой поддерживаемый удаленный ресурс (например, удаленный рабочий стол или виртуальное приложение), к которому пользователь тонкого клиента может подключиться с помощью технологий удаленного доступа для выполнения рабочих задач.

Удаленный рабочий стол

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

Информация о стороннем коде

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

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

Чтобы просмотреть информацию о стороннем коде,

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

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

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Ubuntu является зарегистрированным товарным знаком Canonical Ltd.

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

Dell и другие товарные знаки являются товарными знаками компании Dell Inc или её дочерних компаний.

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

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

OpenSSL является товарным знаком правообладателя OpenSSL Software Foundation.

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