



Kaspersky Thin Client

Kaspersky Thin Client — защищенная на уровне архитектуры операционная система для тонких клиентов на базе KasperskyOS. Такие тонкие клиенты предназначены для предоставления пользователю доступа к удаленному рабочему столу и служат заменой локальной рабочей станции.

Для централизованного и безопасного управления инфраструктурой тонких клиентов с Kaspersky Thin Client используется единая консоль **Kaspersky Security Center**. Также она применяется для управления и другими продуктами «Лаборатории Касперского». Для подключения тонких клиентов к консоли предусмотрен модуль расширения **Kaspersky Security Management Suite**.



Гибкое управление тонкими клиентами

| | |
|--|---|
| Централизованная система управления | С помощью консоли Kaspersky Security Center выполняется: <ul style="list-style-type: none"> • настройка тонких клиентов; • обновление ПО тонких клиентов; • сбор системных событий с тонких клиентов для аудита и исправления неполадок. |
| Автоматическая настройка | Быстрая интеграция тонких клиентов в инфраструктуру благодаря автоматическому подключению и получению настроек от Kaspersky Security Center. |
| Удаленный доступ и управление | Подключение к тонкому клиенту по протоколу RDP с возможностью авторизации. |
| Разграничение прав доступа к настройкам администрирования | Каждый администратор может обращаться только к тем настройкам управления тонкими клиентами, которые имеют отношение к его служебным обязанностям. |
| Гибкая система отчетности | <ul style="list-style-type: none"> • Настраиваемые отчеты с динамической фильтрацией и сортировкой по любому полю. • Информативный дашборд, позволяющий быстро получить все необходимые сведения. |
| Управление настройками тонкого клиента | <ul style="list-style-type: none"> • Откат настроек тонкого клиента к заводским значениям. • Управление доступом пользователя к настройкам тонкого клиента. • Централизованное управление настройками монитора, включая изменение фона рабочего стола и экрана блокировки тонкого клиента. |
| Совместимость с Kaspersky Security Center | Поддерживается Kaspersky Security Center Linux версии: 15.2. |

Защита тонких клиентов от кибератак

| | |
|--|---|
| Исходная безопасность (Security by Design) | Заложенный в архитектуру Kaspersky Thin Client принцип Security by Design и разработка решения с использованием кибериммунной методологии исключают возможность эксплуатации широкого набора уязвимостей, присущих тонким клиентам других производителей. |
| Безопасная передача данных | Обеспечение целостности данных, передаваемых между пользователями, удаленным рабочим столом, сервером централизованного управления, серверами инфраструктуры удаленных рабочих столов и журналирования. Отсутствие необходимости в наложенных средствах защиты. |
| Безопасное обновление | Централизованное автоматическое получение обновлений от сервера обновлений «Лаборатории Касперского» с помощью Kaspersky Security Center. Администратору доступно централизованное ознакомление и принятие условий EULA для новых версий KTC и управление доставкой обновлений на тонкие клиенты. |
| Контроль сетевых подключений | С помощью сертификатов контролируется: <ul style="list-style-type: none"> • подключение пользователей к удаленным рабочим столам и брокерам подключений; • подключение тонких клиентов к системе централизованного управления и серверу журналирования. |
| Резервные сертификаты для Kaspersky Security Center | Автоматическая и прозрачная для администратора Kaspersky Security Center доставка резервного сертификата Kaspersky Security Center в системное хранилище сертификатов Kaspersky Thin Client. |
| Безопасная миграция на новый сервер Kaspersky Security Center | Безопасное подключение тонкого клиента к Kaspersky Security Center с сертификатом, отличным от текущего. |

Аппаратные платформы

| | |
|-----------------------|---|
| TONK TN1200 | Производительный тонкий клиент для организации удаленного рабочего места пользователя. Особенности: ремонтпригодность, установка на подставку или за монитор (VESA-крепление). TONK TN1200 внесен в реестр Минпромторга РФ на основании заключения № 40608/11. Номер реестровой записи — 1018\1\2023. |
| Dell Wyse 3040 | Компактный и энергоэффективный тонкий клиент для организации удаленного рабочего места пользователя. Особенности: потребляемая мощность менее 5 Вт. |

Сценарии подключения

| | |
|--|--|
| Терминальные серверы и гостевые операционные системы | Подключение по протоколу RDP к гостевым операционным системам: <ul style="list-style-type: none">• Microsoft Windows 10/11• Microsoft Windows Server 2016/2019/2022• Astra Linux 1.8• Alt Linux 10• РЕД ОС 8.0 |
| Поддерживаемые инфраструктуры удаленных рабочих столов и способы подключения | Microsoft Remote Desktop Services: <ul style="list-style-type: none">• Windows Server 2016/2019/2022 Базис.WorkPlace: <ul style="list-style-type: none">• Windows 10/11• Windows Server 2016/2019/2022• Astra Linux 1.8, ALT Linux 10 и РЕД ОС 8.0 Citrix и VMware Horizon (по HTML5): <ul style="list-style-type: none">• Windows 10/11• Windows Server 2016/2019/2022 Терминальное подключение: <ul style="list-style-type: none">• Windows Server 2016/2019/2022 (в том числе в MS RDS)• Astra Linux 1.8, ALT Linux, РЕД ОС 8.0 Прямое подключение: <ul style="list-style-type: none">• Windows 10/11• Windows Server 2016/2019/2022• Astra Linux 1.8, ALT Linux 10, РЕД ОС 8.0 |
| Виртуальные приложения | Поддерживается подключение к отдельным бизнес-приложениям: <ul style="list-style-type: none">• развернутым в инфраструктуре Microsoft Remote Desktop Services (Windows Server 2016/2019/2022);• развернутым на терминальных серверах Windows Server 2016/2019/2022;• работающим под управлением Windows 10/11. |

Периферийные устройства

| | |
|---|---|
| Мониторы | Подключение до двух мониторов (HDMI + DisplayPort или DisplayPort + DisplayPort). Разрешение изображения удаленного рабочего стола — до FullHD (1920x1080). |
| USB-устройства | Перенаправление в удаленную среду по протоколу RDP и HTML5 следующих устройств: <ul style="list-style-type: none">• USB-накопители (в том числе с использованием Client Drive Mapping);• веб-камеры;• USB-гарнитуры;• устройства печати и сканирования (принтеры, сканеры, сканеры штрих-кодов);• USB-носители ключевой информации — токены и смарт-карты (только по протоколу RDP)*. <p>* 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) следующие токены: Рутокен Lite, JaCarta-2 PKI/ГОСТ.</p> |
| Беспроводные устройства ввода (USB-интерфейс) | Подключение устройств с передачей данных по радиоканалу: <ul style="list-style-type: none">• клавиатуры;• мыши. |

Мультимедийные возможности

| | |
|------------------|--|
| Аудио | Воспроизведение и передача звука с аудиоустройств, подключенных к тонкому клиенту, в удаленный рабочий стол. |
| Видео | Перенаправление видеопотока от веб-камеры, подключенной к тонкому клиенту, в удаленный рабочий стол. |
| Аудиоконференции | Поддерживаются аудиоконференции в решениях VideoMost, IVA Technologies и SPIRIT DSP. |

Дополнительные функции

| | |
|--|---|
| Интерфейс и возможности для пользователя | <ul style="list-style-type: none">• Настраиваемая панель управления Kaspersky Thin Client, не перекрывающая важные элементы удаленного рабочего стола.• Настройки интерфейса в соответствии с индивидуальными предпочтениями.• Мастер первоначальной настройки операционной системы Kaspersky Thin Client.• Расширенная система уведомлений. Например, система опрашивает пользователя об удобном времени перезагрузки.• Детализированные сообщения об ошибках с советами по их устранению.• Автоматическое переподключение к удаленному рабочему столу в случае разрыва соединения. |
| Локализация пользовательского интерфейса | Настройка только необходимых пользователю языков ввода. Доступен выбор следующих раскладок клавиатуры: <ul style="list-style-type: none">• русской;• английской;• мексиканской испанской;• бразильской португальской;• немецкой;• немецко-швейцарской;• франко-швейцарской. |
| Контроль со стороны администратора | Администратор может гибко управлять настройками пользователя, например, запретить использование микрофона, наушников или второго монитора. |
| Экран блокировки | Возможность блокирования пользователем экрана удаленной сессии и интерфейса тонкого клиента. |
| Избранные подключения | Возможность отображения на рабочем столе тонкого клиента только тех приложений, которые выбраны в настройках (RDP, Базис.WorkPlace, Web Access). |
| Автозапуск приложений | Возможность автоматического запуска одного из приложений (RDP, Базис.WorkPlace, Web Access), выбранного пользователем, после запуска тонкого клиента. |
| Автоматическое подключение | Автоматическое подключение к удаленному рабочему столу после запуска приложения RDP. |
| Настройка параметров энергосбережения | Настройка выключения питания монитора и тонкого клиента при бездействии Kaspersky Thin Client. |
| Отложенная установка обновлений | Возможность для пользователя отложить установку обновления Kaspersky Thin Client на фиксированное количество времени. |