



Kaspersky Secure Remote Workspace

Характеристики решения

Kaspersky Secure Remote Workspace — решение для создания кибериммунной и функциональной инфраструктуры тонких клиентов с удобным централизованным управлением.

Kaspersky Secure Remote Workspace состоит из трех компонентов:

- **Kaspersky Thin Client** — программный продукт на базе операционной системы KasperskyOS, устанавливаемый на аппаратную платформу.
- **Kaspersky Security Center** — единая консоль, предоставляющая удобный централизованный мониторинг и администрирование всех событий Kaspersky Thin Client и других продуктов «Лаборатории Касперского».
- **Kaspersky Security Management Suite** — модуль расширения для связи программного обеспечения тонких клиентов с Kaspersky Security Center.



Гибкое управление тонкими клиентами

Централизованная система управления

С помощью консоли Kaspersky Security Center выполняется:

- настройка тонких клиентов;
- проверка наличия обновлений и обновление ПО тонких клиентов;
- сбор системных событий с тонких клиентов для аудита и исправления неполадок.

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

Настраиваемые отчеты с динамической фильтрацией и сортировкой по любому полю. Информативный дашборд, позволяющий быстро получить все необходимые сведения.

Управление настройками тонкого клиента

- Откат настроек тонкого клиента к заводским значениям.
- Отключение доступа пользователя к настройкам тонкого клиента.

Совместимость с Kaspersky Security Center

Поддерживается Kaspersky Security Center версий: 13.2, 14.0.

Защита тонких клиентов от кибератак

Исходная безопасность (Security by Design)

Заложенный в архитектуру KasperskyOS 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, виртуальным рабочим столом, сервером централизованного управления, серверами брокеров соединения 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 КТС и управление доставкой обновлений на тонкие клиенты.

Контроль сетевых подключений	<p>С помощью сертификатов контролируется:</p> <ul style="list-style-type: none"> • подключение пользователей к удаленным рабочим столам и брокерам; • 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 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.

Аппаратная платформа

TONK TN 1200

Компактный и производительный тонкий клиент для организации удаленного рабочего места пользователя. Особенности: пассивное охлаждение, ремонтпригодность, установка на подставке или за монитор (VESA-крепление).

TONK TN1200 внесен в реестр Минпромторга РФ на основании заключения № 40608/11. Номер реестровой записи — 1018\1\2023.

Подключение

Операционные системы

Подключение по протоколу RDP к гостевым операционным системам:

- Microsoft Windows 7
- Microsoft Windows 10
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Astra Linux Common Edition 2.12.43 (Орел)
- Astra Linux Special Edition 1.7 (Смоленск)
- Alt Linux 10
- РЕД ОС 7.3

Поддерживаемые разрешения мониторов

Возможность вывода изображения удаленного рабочего стола на экраны двух мониторов, подключенных к тонкому клиенту.

Подключение по HDMI и DisplayPort. Поддерживаемые разрешения:

- 1920x1080
- 1366x768
- 1280x1024
- 1600x900
- 1024x768
- 1680x1050
- 1920x1200 (при подключении монитора с этим разрешением фактическое отображение разрешения будет не более 1920x1080)

USB-устройства

Передача флеш-накопителей, смарт-карт и токенов, подключенных к тонкому клиенту, на виртуальный рабочий стол под управлением Windows.

VDI-доступ

Подключение к удаленным виртуальным рабочим столам, созданным на VDI-платформе Basis.Workplace.

Терминальный доступ

Подключение к удаленным рабочим столам на Windows Server.

Режим энергосбережения

Настройка выключения питания монитора и тонкого клиента при бездействии Kaspersky Thin Client.

Возможности интерфейса для пользователя

Удобный и интуитивно понятный интерфейс

- Возможность перемещения панели подключения Kaspersky Thin Client по горизонтали в виртуальном рабочем столе.
- Детализированные сообщения об ошибках.

Отложенная установка обновлений

Возможность для пользователя отложить установку обновления Kaspersky Thin Client на фиксированное количество времени.

os.kaspersky.ru
www.kaspersky.ru

© 2023 АО «Лаборатория Касперского»
Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

