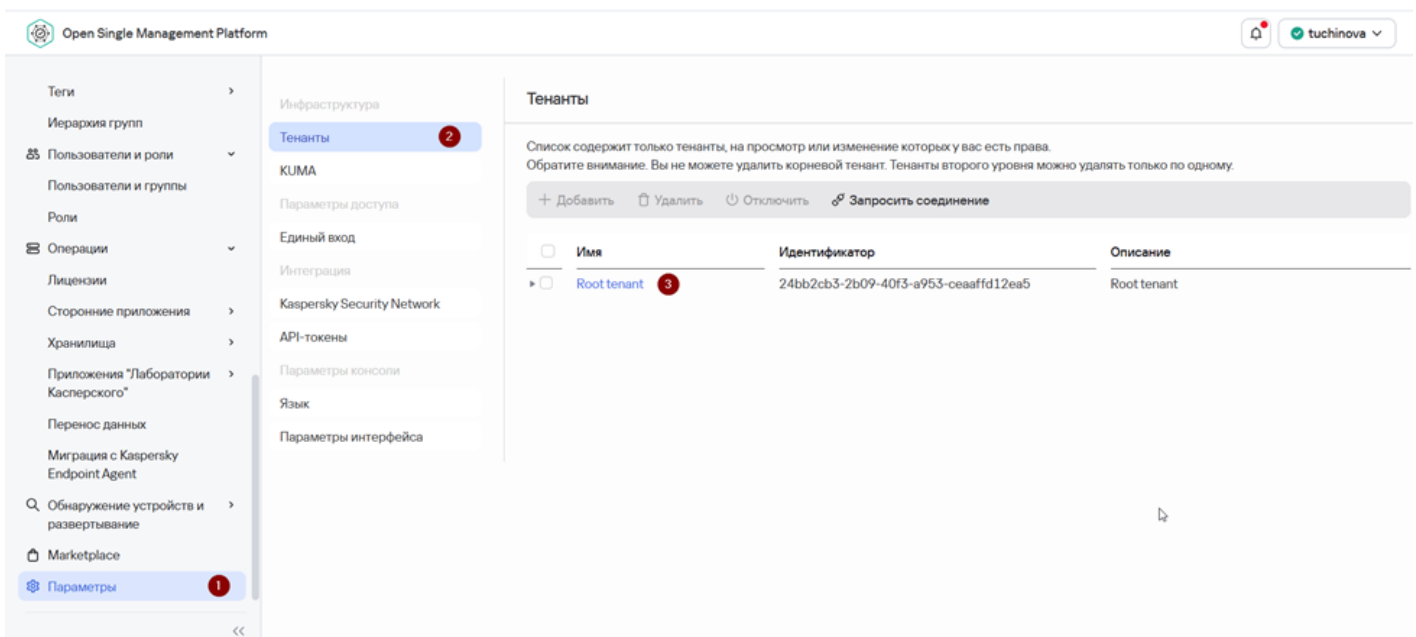


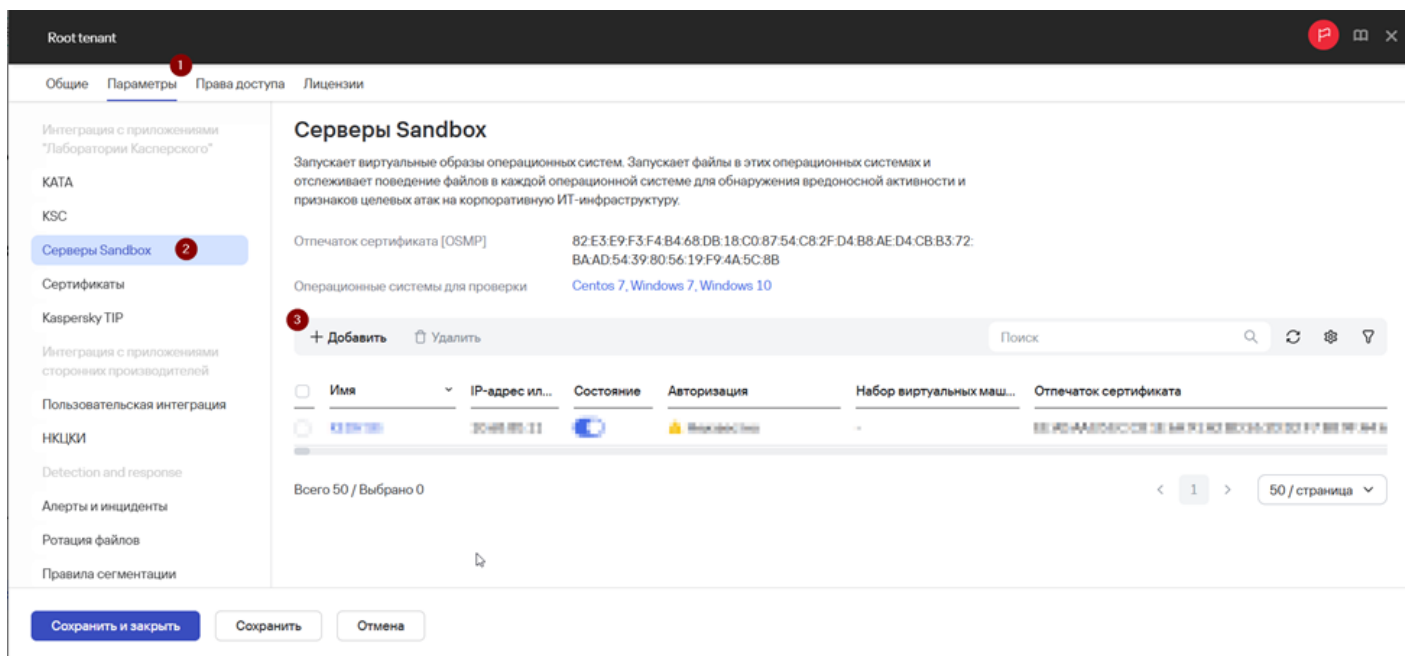
Интеграция с Sandbox

Интеграция с KATA Sandbox

1. Настройки интеграции с KATA Sandbox можно задавать отдельно для каждого тенанта SMP. Для этого откройте **Веб-консоль → Параметры → Расширенный RootTenant → Выбрать** и выберите один из тенантов (в этом сценарии — Root).



2. Перейдите в **Параметры** тенанта **Root** → **Серверы Sandbox** → **Добавить**



3. В новом окне **Добавление сервера Sandbox**:

- Укажите **IP - адрес** сервера KATA Sandbox.
- Нажмите **Получить отпечаток сертификата**
- Задайте имя **Sandbox**.

Добавление сервера Sandbox



1. Введите IP-адрес сервера и нажмите на кнопку, чтобы получить отпечаток сертификата.

IP-адрес*

Получить отпечаток сертификата

2

2. Сравните отпечатки в интерфейсе Sandbox и подтвердите подключение. Не подтверждайте подключение, если отпечатки не совпадают.

Отпечаток сертификата

56:5D:32:AA:38:77:8D:0A:6E:10:65:8B:DE:5E:69:D3:BF:EA:71:E3:B3:FA:C9:DD:90:88:F9:F9:19:93:5D:0D

3. Укажите имя сервера, которое будет отображаться в таблице.

Имя сервера Sandbox*

Добавить

Заккрыть

3. Теперь статус авторизации должен измениться на **Запрос отправлен**. Нажмите **Сохранить и Заккрыть**

Серверы Sandbox

Запускает виртуальные образы операционных систем. Запускает файлы в этих операционных системах и отслеживает поведение файлов в каждой операционной системе для обнаружения вредоносной активности и признаков целевых атак на корпоративную ИТ-инфраструктуру.

Отпечаток сертификата [OSMP] 82E3E9F3F4B468DB18C08754C82FD4B8AE04CB372BAAD5439805619F94A5C8B

Операционные системы для проверки Windows 7, Windows 10

+ Добавить		Удалить		Поиск			
Имя	IP-адрес ил...	Состояние	Авторизация	Набор виртуальных маш...	Отпечаток сертификата		
sandbox	156		Запрос отправлен	-	52E583A54FC76C26AAC35D15BD23E0ED730864AD36C5255D6CB4FD7198BD308A		

4. Войдите в интерфейс KATA Sandbox. Откройте меню **KATA - авторизация** и нажмите **Принять**. Затем нажмите **Применить** и сохраните изменения. После обновления статус должен измениться с **Ожидается** на **Принят**.

Авторизация

Запрос на подключение к компоненту Sandbox требуется отправить с каждого сервера OSMP, который вы хотите подключить к компоненту. Подробнее о том, как создать запрос на подключение, см. в онлайн-справке Kaspersky Endpoint Detection and Response Expert (on-premise).

Sandbox IP  156

Отпечаток сертификата 52.E5.83.A5.4F.C7.6C.26.AA.C3.5D.15.BD.23.E0.ED.73.08.64.AD.36.C5.25.5D.6C.B4.FD.71.98.BD.30.8A

Запросы на подключение

IP	Отпечаток сертификата	Состояние	
 21	82.E3.E9.F3.F4.B4.68.DB.18.C0.87.54.C8.2F.D4.B8.AE.D4.CB.B3.72.BA.AD.54.39.80.56.19.F9.4A.5C.8B	Принят	<button>Отозвать</button>

ОтменитьПрименить

5. Вернитесь в веб-интерфейс XDR и откройте **параметры** тенанта **Root** (или ранее выбранный тенант в вашей среде). Обновите страницу со списком серверов Sandbox — статус должен быть **Подтверждено**. Теперь можно настроить интеграцию с Sandbox.

Root tenant

Общие

Параметры

Права доступа

Лицензии

Интеграция с приложениями "Лаборатория Касперского"

KATA

KSC

Серверы Sandbox

Сертификаты

Kaspersky TIP

Интеграция с приложениями сторонних производителей

Пользовательская интеграция

НКЦКИ

Detection and response

Алерты и инциденты

Ротация файлов

Правила сегментации

Правила агрегации

Управление инцидентами

Аудит активов

Подключение к почтовому серверу

Управление учетными данными

Шаблоны электронных писем

Параметры активов

Серверы Sandbox

Запускает виртуальные образы операционных систем. Запускает файлы в этих операционных системах и отслеживает поведение файлов в каждой операционной системе для обнаружения вредоносной активности и признаков целевых атак на корпоративную ИТ-инфраструктуру.

Отпечаток сертификата [OSMP] 82.E3.E9.F3.F4.B4.68.DB.18.C0.87.54.C8.2F.D4.B8.AE.D4.CB.B3.72.BA.AD.54.39.80.56.19.F9.4A.5C.8B

Операционные системы для проверки Windows 7, Windows 10

+ Добавить

Удалить

Поиск

Имя	IP-адрес ил...	Состояние	Авторизация	Набор виртуальных маш...	Отпечаток сертификата
☐ sandbox	 156		 Подтверждено	-	52.E5.83.A5.4F.C7.6C.26.AA.C3.5D.15.BD.23.E0.ED.73.08.64.AD.36.C5.25.5D.6C.B4.FD.71.98.BD.30.8A

Всего 50 / Выбрано 0

< 1 >

50 / страница

Сохранить и закрыть

Сохранить

Отмена

6. Откройте **Сетевое сканирование** в **параметрах** тенанта и включите одну или все необходимые настройки сканирования:

- **Автоматически отправлять файлы в Sandbox**
- **Отправлять файлы с устройства для анализа в Sandbox**

Root tenant

Общие

Параметры

Права доступа

Лицензии

Интеграция с приложениями "Лаборатории Касперского"

КАТА

KSC

Серверы Sandbox

Сертификаты

Kaspersky TIP

Интеграция с приложениями сторонних производителей

Пользовательская интеграция

НКЦКИ

Detection and response

Алерты и инциденты

Ротация файлов

Правила сегментации

Правила агрегации

Управление инцидентами

Аудит активов

Подключение к почтовому серверу

Управление учетными данными

Шаблоны электронных писем

Параметры сканирования

Параметры активов

Репутационная база KPSN

Параметры сканирования

Sandbox

Расписание IOC-проверки

Обновление баз

Архивы

⚠

Интеграция с Sandbox не настроена. Параметры вступят в силу после настройки интеграции.

[Перейти к серверам Sandbox](#)

Автоматически отправлять файлы в Sandbox

Настройте автоматическую отправку файлов на проверку компонентом Sandbox в соответствии с правилами TAA (IOA) "Лаборатории Касперского".

☒

Отправить файлы

2

Отправлять файлы с устройств для анализа в Sandbox

Настройте отправку файлов в Sandbox с устройств с установленным Endpoint Agent. Вы можете настроить отправку файлов вручную или автоматически.

☒

Отправлять файлы вручную

3

☐

Отправлять файлы автоматически

Сохранить и закрыть

Сохранить

Отмена

Revision #6

Created 2026-08-05 07:30:08 UTC by Koala

Updated 2026-08-19 11:46:47 UTC by Ierat