Политика KES для Windows 12.8 - Standard

Название политики:

Политика KES 12.8 - Рабочие станции Windows (Standard)

Применение:

- Группа устройств: Рабочие станции пользователей (Windows)
- Тип ОС: Windows

Для кого эта политика:

- Для всех сотрудников

Компоненты

Компонент	Статус	Описание
Kaspersky Security Network	**Включен**	Проверка по облачной базе Kaspersky
Поведенческий анализ	**Включен**	Анализ поведения приложений для обнаружения сложных угроз
Защита от эксплойтов	**Включен**	Защита от приложений, эксплуатирующих уязвимости в ПО
Предотвращение вторжений	**Включен**	Регулятор активности, совершаемую приложениями в системе
Откат вредоносных действий	**Включен**	Сбор информации о подозрительных действиях ПО, в рамках текущей и предыдущих сессий. Для возможности отмены совершенных приложением действий
Файловый антивирус	**Включен**	Проверка файловой системы
Веб Антивирус	**Включен**	Проверка HTTP/HTTPS-трафика
Почтовый антивирус	**Включен**	Анализ почтового трафика

Сетевой экран	**Включен**	Firewall
Защита от сетевых угроз	**Включен**	Защита от подозрительной сетевой активности
Защита от атак BadUSB	**Выключен**	Защита от использования USB-устройств, имитирующих поведение клавиатур
AMSI-защита	**Включен**	Antimalware Scan Interface от Microsoft (проверка скриптов PS и макросов MS Office)
Endpoint Detection and Response (KATA)	**Выключен**	EDR
Контроль приложений	**Включен**	Контроль запускаемых приложений (черный и белый списки)
Контроль устройств	**Включен**	Контроль подключенных и внешних устройств
Веб-контроль	**Включен**	Контроль доступа пользователей к веб-ресурсам
Контроль аномалий	**Включен**	Контроль действий, не характерных для компьютеров в сети на основе типичных сценариев вредоносной активности
Контроль целостности системы	**Включен**	Контроль изменений файлов в системе, реестра и подключения к компьютеру внешних устройств
Шифрование данных	**Выключен**	Общие настройки шифрования, полное шифрование дисков, внешних устройств и файлов
Интеграция с KUMA	**Выключен**	Интеграция с SIEM системой
Режим легкого агента	**Выключен**	Серверный вариант использования, с выносом активных компонентов на SVM сервер
Профили политики	**Обсуждаемое**	Привязка политики к компьютерам в соответствии с группами в AD

Общие

- Состояние политики: Активная
- Наследование параметров: Наследовать параметры родительской политики - **снять галку**

Настройка событий

- Регистрация событий
  - Хранить в базе данных Сервера администрирования в течении (сут) - до 30
  - Экспортировать в SIEM-систему по протоколу Syslog - **выключить**

- События политики

Тип события	Время хранения на KSC	Отправка в SIEM
:drop_of_blood: Критические события		Да :tick: / Нет :cross:
Нарушено лицензионное соглашение	30 дней	:cross:
Срок действия лицензии почти истек	Не хранить	:cross:
Базы повреждены или отсутствуют	Не хранить	:cross:
Базы сильно устарели	Не хранить	:cross:
Авто запуск приложения выключен	30 дней	:cross:
Ошибка активации	30 дней	:cross:
Обнаружена активная угроза. Требуется запуск процедуры лечения активного заражения.	30 дней	:cross:
Серверы KSN недоступны	30 дней	:cross:
Недостаточно места в хранилище карантина	30 дней	:cross:
Объект не восстановлен из карантина	30 дней	:cross:
Объект не удален из карантина	30 дней	:cross:
Приложение установило соединение с сайтом с недоверенным сертификатом	30 дней	:cross:
Возникла ошибка проверки зашифрованного соединения. Домен добавлен в список исключений	30 дней	:cross:
Достигнуто ограничение на количество событий, отправляемых в Kaspersky Security Center	15 дней	:cross:
Обнаружен вредоносный объект (локальные базы)	30 дней	:cross:
Обнаружен вредоносный объект (KSN)	30 дней	:cross:

Лечение невозможно	30 дней	:cross:
Невозможно удалить	30 дней	:cross:
Ошибка обработки	Не хранить	:cross:
Процесс завершен	30 дней	:cross:
Невозможно завершить процесс	Не хранить	:cross:
Остановлен переход на сайт	30 дней	:cross:
Открыта опасная ссылка	30 дней	:cross:
Обнаружена ранее открытая опасная ссылка	30 дней	:cross:
Действие процесса заблокировано	30 дней	:cross:
Адаптивный контроль аномалий: отключено срабатывание правил для учетных записей с неустановленным идентификатором безопасности (SID)	30 дней	:cross:
Клавиатура не авторизована	5 дней	:cross:
AMSI-запрос заблокирован	30 дней	:cross:
Сетевая активность запрещена	30 дней	:cross:
Обнаружена сетевая атака	30 дней	:cross:
Запуск приложения запрещен	30 дней	:cross:
Запрещенный процесс был запущен до старта KES	30 дней	:cross:
Контроль приложений: отключено срабатывание правил для учетных записей с неустановленным идентификатором безопасности (SID)	30 дней	:cross:
Доступ запрещен (локальные базы)	30 дней	:cross:
Доступ запрещен (KSN)	30 дней	:cross:
Веб-контроль: отключено срабатывание правил для учетных записей с неустановленным идентификатором безопасности (SID)	30 дней	:cross:
Операция с устройством запрещена	30 дней	:cross:
Сетевое соединение заблокировано	30 дней	:cross:
Контроль устройств: отключено срабатывание правил для учетных записей с неустановленным идентификатором безопасности (SID)	30 дней	:cross:

Ошибка обновления компонента	Не хранить	:cross:
Ошибка копирования обновлений компонента	Не хранить	:cross:
Локальная ошибка обновлений	Не хранить	:cross:
Сетевая ошибка обновлений	Не хранить	:cross:
Невозможен запуск двух задач одновременно	5 дней	:cross:
Ошибка проверки баз и модулей приложения	30 дней	:cross:
Ошибка взаимодействия с Kaspersky Security Center	30 дней	:cross:
Обновлены не все компоненты	30 дней	:cross:
Обновление завершено успешно, а копирование обновлений закончено с ошибкой	Не хранить	:cross:
Внутренняя ошибка задачи	Не хранить	:cross:
Ошибка установки патча	30 дней	:cross:
Ошибка отката патча	30 дней	:cross:
Ошибка применения правил шифрования / расшифровки файлов	Не хранить	:cross:
Ошибка шифрования / расшифровки файлов	Не хранить	:cross:
Заблокирован доступ к файлу	Не хранить	:cross:
Ошибка активации портативного режима	30 дней	:cross:
Ошибка деактивации портативного режима	30 дней	:cross:
Ошибка создания зашифрованного архива	30 дней	:cross:
Ошибка шифрования / расшифровки устройства	Не хранить	:cross:
Не удалось загрузить модуль шифрования	Не хранить	:cross:
Задача управления учетными записями Агента аутентификации завершилась с ошибкой	30 дней	:cross:
Политика не может быть применена	30 дней	:cross:
Обновление функциональности шифрования завершено с ошибкой	Не хранить	:cross:

Откат обновления функциональности шифрования завершен с ошибкой	Не хранить	:cross:
Сервер Kaspersky Anti Targeted Attack Platform недоступен	Не хранить	:cross:
Ошибка удаления объекта	30 дней	:cross:
Объект не помещен на карантин (Sandbox)	Не хранить	:cross:
Возникла внутренняя ошибка	30 дней	:cross:
Ошибка отправки задачи проверки в Sandbox пользователем	Не хранить	:cross:
Сертификат сервера Sandbox не действителен	Не хранить	:cross:
Узел Sandbox не доступен	Не хранить	:cross:
Обработка объекта в Sandbox завершилась ошибкой	Не хранить	:cross:
Превышена допустимая нагрузка на Sandbox	Не хранить	:cross:
IOC обнаружен	Не хранить	:cross:
Возникла ошибка при проверке лицензии Sandbox	Не хранить	:cross:
Ошибка создания задачи Sandbox	Не хранить	:cross:
Сертификат клиента Sandbox не действителен	Не хранить	:cross:
Не удалось сконвертировать сертификат клиента Sandbox	Не хранить	:cross:
Запрещен запуск объекта	30 дней	:cross:
Объект не заблокирован	30 дней	:cross:
Запуск объекта не заблокирован	30 дней	:cross:
Запуск процесса не заблокирован	30 дней	:cross:
Выполнение скрипта не заблокировано	30 дней	:cross:
Объект не помещен на карантин (EDR)	Не хранить	:cross:
Обнаружена возможная попытка взлома пароля с помощью подбора	30 дней	:cross:
Обнаружены признаки компрометации журналов Windows	30 дней	:cross:
Обнаружена подозрительная активность со стороны новой установленной службы	30 дней	:cross:

Обнаружена подозрительная аутентификация с явным указанием учетных записей	30 дней	:cross:
Обнаружены признаки атаки Kerberos forged PAC (MS14-068)	30 дней	:cross:
Обнаружены подозрительные изменения привилегированной группы Администраторы	30 дней	:cross:
Обнаружена подозрительная активность во время сетевого сеанса входа	30 дней	:cross:
Сработало правило Анализа журналов	30 дней	:cross:
Подозрительное событие повторяется слишком часто. Запущено формирование агрегированных событий.	30 дней	:cross:
Отчет о подозрительном событии за период агрегации	30 дней	:cross:
Анализ журналов: отключено срабатывание правил для учетных записей с неустановленным идентификатором безопасности (SID)	30 дней	:cross:
Ошибка подключения к серверу Kaspersky Anti Targeted Attack Platform	Не хранить	:cross:
Некорректный сертификат сервера Kaspersky Anti Targeted Attack Platform	Не хранить	:cross:
Некорректный сертификат агента на сервере Kaspersky Anti Targeted Attack Platform	Не хранить	:cross:
Обнаружено изменение файла или папки	30 дней	:cross:
Объект изменяется слишком часто. Запущено формирование агрегированных событий	30 дней	:cross:
Отчет об изменениях объекта за период агрегации	30 дней	:cross:
Область мониторинга содержит некорректные объекты	30 дней	:cross:
Попыток выполнения запрещенных действий с объектом слишком много. Запущено формирование агрегированных событий	30 дней	:cross:

Контроль целостности системы: отключено срабатывание правил для учетных записей с неустановленным идентификатором безопасности (SID)	30 дней	:cross:
Ошибка подключения к серверу NDR	Не хранить	:cross:
Некорректный сертификат сервера NDR	Не хранить	:cross:
Некорректный сертификат агента на сервере NDR	Не хранить	:cross:
Не удалось получить данные о проекте ПЛК	Не хранить	:cross:
Не удалось сравнить проект ПЛК с эталонным	Не хранить	:cross:
Отсутствуют доступные для подключения SVM	Не хранить	:cross:
Обнаружен вредоносный объект. Требуется запуск процедуры лечения активного заражения на шаблоне виртуальной машины	30 дней	:cross:
Ошибка подключения к серверу KUMA	Не хранить	:cross:
Некорректный сертификат сервера KUMA	Не хранить	:cross:
Некорректный сертификат агента на сервере KUMA	Не хранить	:cross:
Ваше устройство подключено к недоверенному Серверу администрирования. Обратитесь к администратору вашей организации	30 дней	:cross:
:cross: Отказ функционирования		**Да :tick: / Нет :cross:**
Не удалось выполнить задачу	Не хранить	:cross:
Ошибка в настройках задачи. Настройки задачи не применены	30 дней	:cross:
Ошибка обработки (Контроль целостности системы)	30 дней	:cross:
:warning: Предупреждение		**Да :tick: / Нет :cross:**
Срок действия лицензии скоро истекает	Не хранить	:cross:
Базы устарели	Не хранить	:cross:
Автоматическое обновление выключено	30 дней	:cross:
Самозащита приложения выключена	30 дней	:cross:

Компоненты защиты выключены	Не хранить	:cross:
Компьютер работает в безопасном режиме	Не хранить	:cross:
Есть необработанные файлы	Не хранить	:cross:
Применена групповая политика	Не хранить	:cross:
Задача остановлена	Не хранить	:cross:
Для завершения обновления необходимо перезапустить приложение	30 дней	:cross:
Необходима перезагрузка компьютера	30 дней	:cross:
Установлены не все компоненты приложения, которые позволяет использовать лицензия	10 дней	:cross:
Запущена процедура лечения активного заражения	30 дней	:cross:
Процедура лечения активного заражения завершена	30 дней	:cross:
Некорректный резервный ключ	10 дней	:cross:
Подписка скоро истекает	10 дней	:cross:
Объект не восстановлен из резервного хранилища	10 дней	:cross:
Обнаружена подозрительная сетевая активность	30 дней	:cross:
Защищенное соединение разорвано	10 дней	:cross:
Установлено соединение с сайтом с недоверенным сертификатом по решению пользователя	30 дней	:cross:
Участие в KSN выключено	30 дней	:cross:
Обработка приложением некоторых функций ОС отключена	30 дней	:cross:
В хранилище карантина скоро закончится место	30 дней	:cross:
Соединение разблокировано	10 дней	:cross:
Ошибка при удалении предыдущей версии приложения	10 дней	:cross:
Настройки операционной системы не позволяют контролировать доступ к сетям Wi-Fi	10 дней	:cross:
Не удалось установить обновление приложения	30 дней	:cross:

Невозможно создать резервную копию объекта	10 дней	:cross:
Объект не обработан	30 дней	:cross:
Объект зашифрован	30 дней	:cross:
Объект поврежден	30 дней	:cross:
Обнаружено легальное приложение, которое может быть использовано злоумышленниками для нанесения вреда компьютеру или данным пользователям (локальная база)	30 дней	:cross:
Обнаружено легальное приложение, которое может быть использовано злоумышленниками для нанесения вреда компьютеру или данным пользователям (KSN)	30 дней	:cross:
Объект удален	30 дней	:cross:
Объект вылечен	30 дней	:cross:
Откат выполнен	30 дней	:cross:
Запрещено	30 дней	:cross:
Ошибка авторизации клавиатуры	30 дней	:cross:
:information: Информационное сообщение		**Да :tick: / Нет :cross:**
Самозащита ограничила доступ к защищаемому ресурсу	Не хранить	:cross:
Отчет очищен	Не хранить	:cross:
Групповая политика деактивированна	Не хранить	:cross:
Изменены настройки приложения	Не хранить	:cross:
Задача запущена	Не хранить	:cross:
Задача приостановлена	Не хранить	:cross:
Задача завершена	Не хранить	:cross:
Все компоненты приложения, которые допускает лицензия, установлены и работают в нормальном режиме	Не хранить	:cross:
Параметры подписки были изменены	Не хранить	:cross:
Подписка была продлена	Не хранить	:cross:
Объект восстановлен из резервного хранилища	Не хранить	:cross:
Ввод имени пользователя и пароля	Не хранить	:cross:

Получен доступ к защищаемой области	Не хранить	:cross:
Участие в KSN включено	Не хранить	:cross:
Серверы KSN недоступны	10 дней	:cross:
Приложение работает и обрабатывает данные в соответствии с местным законодательством и использует локальную инфраструктуру	Не хранить	:cross:
Объект восстановлен из карантина	10 дней	:cross:
Объект удален из карантина	10 дней	:cross:
Создана резервная копия объекта	10 дней	:cross:
Объект перезаписан вылеченной ранее копией	10 дней	:cross:
Обнаружен защищенный паролем архив	10 дней	:cross:
Информация об обнаруженном объекте	Не хранить	:cross:
Объект находится в списке разрешенных в Kaspersky Private Security Network	Не хранить	:cross:
Объект переименован	Не хранить	:cross:
Ссылка находится в списке разрешенных в Kaspersky Private Security Network	Не хранить	:cross:
Приложение помещено в группу доверенных приложений	10 дней	:cross:
Приложение помещено в группу с ограничениями	10 дней	:cross:
Сработал компонент Предотвращение вторжений	30 дней	:cross:
Файл восстановлен	10 дней	:cross:
Значение реестра восстановлено	10 дней	:cross:
Значение реестра удалено	10 дней	:cross:
Действие процесса пропущено	10 дней	:cross:
Клавиатура авторизована	Не хранить	:cross:
Сетевая активность разрешена	Не хранить	:cross:
Запуск приложения запрещен в тестовом режиме	Не хранить	:cross:
Запуск приложения разрешен в тестовом режиме	Не хранить	:cross:

Открыта разрешенная страница	Не хранить	:cross:
Операция с устройством разрешена	Не хранить	:cross:
Выполнена операция с файлом	Не хранить	:cross:
Выбран источник обновления	Не хранить	:cross:
Нет доступных обновлений	Не хранить	:cross:
Копирование обновлений успешно завершено	Не хранить	:cross:
Началось применение правил шифрования / расшифровки файлов	Не хранить	:cross:
Завершено применение правил шифрования / расшифровки файлов	Не хранить	:cross:
Загружен модуль шифрования	Не хранить	:cross:
Создана новая учетная запись Агента утентификации	Не хранить	:cross:
Удалена учетная запись Агента аутентификации	Не хранить	:cross:
Изменен пароль для учетной записи Агента аутентификации	Не хранить	:cross:
Успешная аутентификация в Агенте аутентификации	Не хранить	:cross:
Аутентификация в Агенте аутентификации завершилась с ошибкой	Не хранить	:cross:
Получен доступ к жесткому диску с помощью процедуры запроса доступа к зашифрованным устройствам	Не хранить	:cross:
Попытка получения доступа к жесткому диску с помощью процедуры запроса доступа к зашифрованным устройствам завершилась с ошибкой	Не хранить	:cross:
Учетная запись не добавлена. Такая учетная запись уже существует	Не хранить	:cross:
Учетная запись не изменена. Такая учетная запись не существует	Не хранить	:cross:
Учетная запись не удалена. Такая учетная запись не существует	Не хранить	:cross:
Обновление функциональности шифрования завершено успешно	Не хранить	:cross:
Откат обновления функциональности шифрования завершен успешно	Не хранить	:cross:

Не удалось удалить драйверы для компонента Шифрование диска Kaspersky из образа среды восстановления Windows	Не хранить	:cross:
Ключ восстановления для BitLocker изменен	Не хранить	:cross:
Пароль / PIN-код для BitLocker изменен	Не хранить	:cross:
Ключ восстановления BitLocker был сохранен на съемный диск	Не хранить	:cross:
Задачи с сервера Kaspersky Anti Targeted Attack Platform не обрабатываются	Не хранить	:cross:
Компонент Endpoint Sensor подключен к серверу	Не хранить	:cross:
Связь с сервером Kaspersky Anti Targeted Attack Platform восстановлена	Не хранить	:cross:
Задачи с сервера Kaspersky Anti Targeted Attack Platform обрабатываются	Не хранить	:cross:
Запуск клиентского приложения облачной службы разрешен	10 дней	:cross:
Доступ к облачной службе разрешен	10 дней	:cross:
Объект удален	30 дней	:cross:
Статистика задачи удаления	10 дней	:cross:
Объект помещен на карантин (Sandbox)	Не хранить	:cross:
Объект удален (Sandbox)	Не хранить	:cross:
Задача проверки успешно отправлена в Sandbox пользователем	Не хранить	:cross:
Запущен поиск IOC	Не хранить	:cross:
Завершен поиск IOC	Не хранить	:cross:
Объект помещен на карантин (Endpoint Detection and Response)	Не хранить	:cross:
Объект удален (Endpoint Detection and Response)	Не хранить	:cross:
Успешное подключение к серверу Kaspersky Anti Targeted Attack Platform	Не хранить	:cross:
Обнаружено изменение файла или папки	Не хранить	:cross:

Объект изменяется слишком часто. Запущено формирование агрегированных событий	15 дней	:cross:
Отчет об изменениях объекта за период агрегации	15 дней	:cross:
Область мониторинга содержит некорректные объекты	15 дней	:cross:
Снимок состояния системы создан	10 дней	:cross:
Снимок состояния системы обновлен	10 дней	:cross:
Успешное подключение к серверу NDR	Не хранить	:cross:
Подключение к Серверу интеграции было восстановлено	10 дней	:cross:
Соединение с SVM установлено	Не хранить	:cross:
Успешное подключение к серверу KUMA	10 дней	:cross:
Сервер администрирования, к которому подключено ваше устройство, стал доверенным	10 дней	:cross:
Ваше устройство подключено к новому доверенному Серверу Администрирования	10 дней	:cross:
Сервер администрирования, к которому подключено ваше устройство, перестал быть доверенным	10 дней	:cross:
Состав приложения успешно изменен	Не хранить	:cross:
Асинхронное обнаружение Sandbox	Не хранить	:cross:
Отчет о событиях облачной службы за период агрегации	10 дней	:cross:
Устройство подключено	Не хранить	:cross:
Устройство отключено	Не хранить	:cross:

Продвинутая защита

Kaspersky Security Network

Описание: Репутационная облачная база Лаборатории Касперского. В базе содержится информация о репутации файлов, интернет ресурсов, ПО.

- Kaspersky Security Network - **включено**
- Расширенный режим KSM - **включено**

Настройка KSN:

- Включить облачный режим - **включено**
- Статус компьютера при недоступности серверов KSN - **Предупреждение**
- При выключенном облачном режиме: **Предупреждение**

Настройки KSN Proxy

- Использовать Сервер администрирования как прокси-сервер KSN - **включено**
- Использовать серверы Kaspersky Securoty Network, если прокси-сервер KSN недоступен - **включено**

Анализ поведения

Описание: Анализ поведения приложений, и обнаружение сложных угроз, таких как приложения-вымогатели.

Действие при обнаружении вредоносной активности: Удалить

Защита папок общего доступа от внешнего шифрования:

- Защита папки общего доступа - **включено**
- Блокировать соединение - **60 мин.**

Области защиты:

- Папки общего доступа - **Все общие сетевые папки защищаемого устройства**
- Исключения по имени или IP адресу - **по необходимости**
- Исключения по маске - **по необходимости**

Защита от эксплойтов

Описание: Блокировка действий вредоносных приложений, которые используют уязвимости ПО

Защита от эксплойтов - **включено**

При обнаружении эксплойта

- Блокировать

Защита памяти системных процессов

- Включить защиту памяти системных процессов - **включено**

Предотвращение вторжений

Описание: Регистрация активности, совершаемой приложениями в системе, и регулировка деятельности приложений в зависимости от их статуса.

Предотвращение вторжений - **включено**

Права приложений и защищаемые ресурсы

Настройка прав приложений для политики (по умолчанию)

Приложение	Ограничения
Доверенные	Файлы и системный реестр - **разрешено все** Права доступа к процессам и изменению системы - **разрешено все** Сетевые правила - **разрешено все**
Слабые ограничения	Файлы и системный реестр - **разрешено все** Права: (запрещено) • Изменение системных модулей (KnownDlls) • Доступ к камере • Доступ к устройству аудиозаписи Сетевые правила - **разрешено все**

<table>
<tr>
<td>Сильные ограничения</td>
<td>Файлы и системный реестр:
<table>
<tr><th>Ресурс</th><th>Чтение</th><th>Запись</th><th>Удаление</th><th>Создание</th></tr>
<tr><td>Операционная система</td><td>:tick:</td><td>:cross:</td><td>:cross:</td><td>:cross:</td></tr>
<tr><td>Системные файлы</td><td>:tick:</td><td>:cross:</td><td>:cross:</td><td>:cross:</td></tr>
<tr><td>Настройки безопасности</td><td>:tick:</td><td>:cross:</td><td>:cross:</td><td>:cross:</td></tr>
<tr><td>Системные службы</td><td>:tick:</td><td>:cross:</td><td>:cross:</td><td>:cross:</td></tr>
<tr><td>Персональные данные</td><td>:tick:</td><td>:tick:</td><td>:tick:</td><td>:tick:</td></tr>
<tr><td>Файлы пользователя</td><td>:tick:</td><td>:tick:</td><td>:tick:</td><td>:tick:</td></tr>
<tr><td>Настройки приложений</td><td>:tick:</td><td>:tick:</td><td>:tick:</td><td>:tick:</td></tr>
</table>
Запрещены права:

Приостановка других процессов и потоков
Запуск драйвера
Внедрение кода
Изменение системных модулей (KnownDlls)
Низкоуровневый доступ к диску
Низкоуровневый доступ к файловой системе
Управление драйверами принтера
Создание службы
Открытие службы с правами на запись
Изменение конфигурации службы
Управление службой
Запуск службы
Удаление службы
Доступ к хранилищу паролей
Завершение работы Microsoft Windows
Доступ к камере
Доступ к устройствам аудиозаписи
Установка прав отладчика
Использование программных интерфейсов браузера
Использование программных интерфейсов системы (DNS)
Использование программных интерфейсов системы

Сетевые правила: Запрещено все</td>
</tr>
<tr>
<td>Не доверенные</td>
<td>Файлы и системный реестр - запрещено все
Права доступа к процессам и изменению системы - запрещено все
Сетевые правила - запрещено все</td>
</tr>
</table>

Защищаемые ресурсы

По умолчанию

Правила обработки приложений:

- Обновлять правила для ранее неизвестных приложений из базы KSN - **включено**
- Доверять приложениям, имеющим цифровую подпись - **включено**
- Удалять правила приложений, не запускавшихся более 60 дней - **включено**
- Группа доверия для приложений, которые не удалось распределить по другим группам - **Слабые ограничения**

Откат вредоносных действий: **включено**

Базовая защита

Защита от файловых угроз

Описание: Проверка всех открываемых, запускаемых и сохраняемых файлов

- Уровень безопасности: **Рекомендуемый**
  - Машинное обучение и сигнатурный анализ - **включено**
  - Эвристический анализ - **включено** (Поверхностный)
  - Оптимизация - Проверять только новые и измененные файлы - **включено**
  - Проверка составных файлов
    - Распаковывать составные файлы в фоновом режиме - **выключено**
    - Не распаковывать составные файлы большего размера - **8 Мб**
      - Проверять архивы - **выключено**
      - Проверять дистрибутивы - **выключено**
      - Проверять файлы офисных форматов - **включено**
      - Проверять файлы почтовых форматов - **включено**
      - Дополнительно:
  - Дополнительно
    - По расписанию - **выключено**
    - При запуске приложений - **выключено**
    - Останавливать контейнеры, если лечение невозможно - **выключено**
    - Не проверять файловые операции, исполняемые в контейнерах Windows - **выключено**
      - Режим проверки: Интеллектуальный
      - Технологии проверки: iSwift - **включено**
      - Технологии проверки: iChecker - **включено**
      - Приостановка защиты от файловых угроз

    - Проверка файловых операций, исполняемых в контейнерах Windows

  - Общие - **Файлы, проверяемые по формату**
  - Области защиты - **все диски**
  - Производительность

- Лечить. Удалять, если лечение невозможно

Защита от веб-угроз

Описание: Проверяет входящий веб-трафик и предотвращает запуск опасных скриптов

  -

  - Уроверь безопасности: **Рекомендуемый**
  - Общие - Проверять веб-адрес по базе вредоносных веб-адресов - **включено**
  - Общие - Использовать эвристический анализ - **включено** (средний)
  - Анти-Фишинг - Проверять веб-адреса по базе фишинговых веб-адресов - **включено**
  - Анти-Фишинг - Использовать эвристический анализ - **включено**
  - Доверенные веб-адреса:
    - Не проверять веб-трафик с доверенных веб-адресов: ***.serbsky.lan , *.serbsky.ru**

- Действия при обнаружении угрозы: **Блокировать**

Защита от почтовых угроз

Описание: Проверка почты на наличие опасных объектов

- Уровень безопасности: **Рекомендуемый**
  - Проверять трафик POP3, SMTP, NNTP, IMAP - **включено**
  - Подключать расширение для Microsoft Outlook - **включено**
  - Проверять вложенные архивы - **включено**
  - Проверять вложенные файлы офисных форматов - **включено**
  - Не проверять архивы размером более - **8Мб**
  - **Переименовывать вложения указанных типов**
    - ***.cmd**
    - ***.com**
    - ***.exe**
    - ***.js**

    - ***.jse**
    - ***.msi**
    - ***.scr**
    - ***.vbe**
    - ***.vbs**

  - Эвристический анализ - **включено** (средний)
    - Общие - Область защиты - **Входящие и исходящие сообщения**
    - Общие - Встраивание в систему
    - Проверка составных файлов
    - Фильтр вложений
    - Дополнительно

- Действия при обнаружении угрозы: **Лечить. Удалять, если лечение невозможно.**

Сетевой экран

Описание: Компонент фильтрует всю сетевую активность в соответствии с правилами

- **Сетевые правила приложений** (по умолчанию)

Приложение	Сеть	Группа	Разрешения
Доверенные	:tick:	Доверенные	Файлы и системный реестр - **разрешено все** Права доступа к процессам и изменению системы - **разрешено все** Сетевые правила - **разрешено все**
Слабые ограничения	:tick:	Слабые ограничения	Файлы и системный реестр - **разрешено все** Права: (запрещено) • Изменение системных модулей (KnownDlls) • Доступ к камере • Доступ к устройству аудиозаписи Сетевые правила - **разрешено все**

Сильные ограничения	:cross:	Сильные ограничения	Файлы и системный реестр: **Ресурс** / **Чтение** / **Запись** / **Удаление** / **Создание** Операционная система — :tick: / :cross: / :cross: / :cross: Системные файлы — :tick: / :cross: / :cross: / :cross: Настройки безопасности — :tick: / :cross: / :cross: / :cross: Системные службы — :tick: / :cross: / :cross: / :cross: Персональные данные — :tick: / :tick: / :tick: / :tick: Файлы пользователя — :tick: / :tick: / :tick: / :tick: Настройки приложений — :tick: / :tick: / :tick: / :tick: Запрещены права: • Приостановка других процессов и потоков • Запуск драйвера • Внедрение кода • Изменение системных модулей (KnownDlls) • Низкоуровневый доступ к диску • Низкоуровневый доступ к файловой системе

Не доверенные	:cross:	Не доверенные	Файлы и системный реестр - **запрещено все** Права доступа к процессам и изменению системы - **запрещено все** Сетевые правила - **запрещено все**

- **Сетевые пакетные правила**

Включено	Сетевая служба	Настройки	Разрешение	Адрес
Включено	Запросы к серверу DNS по TCP	Исходящее TCP/53	:tick:	Любые
Включено	Запросы к серверу DNS по UDP	Исходящее UDP/53	:tick:	Любые
Включено	Отправка электронных писем	Исходящие TCP/25,465,143,993	:tick:	Любые
Включено	Любая сетевая активность	any	:tick:	Локальные сети
Включено	Любая сетевая активность	any	:tick:	Доверенные сети
Включено	Сетевая активность для работы технологии удаленного рабочего стола	Входящие TCP/3389	:tick:	Доверенные сети
Включено	Соединения по протоколу TCP через локальные порты	Входящие TCP/135, 137, 138, 139, 445, 1110, 2869, 19780	:cross:	Любые
Включено	Соединения по протоколу UDP через локальные порты	Входящие UDP/123, 135, 137, 138, 139, 445	:cross:	Любые
Включено	Входящая активность по протоколу TCP	Входящие TCP	:tick:	Любые
Включено	Входящая активность по протоколу UDP	Входящие UDP	:tick:	Любые
Включено	Входящие ответы ICMP Destination Unreachable	Входящие ICMP	:tick:	Любые
Включено	Входящие пакеты ICMP Echo Reply	Входящие ICMP	:tick:	Любые
Включено	Входящие ответы ICMP Time Exceeded	Входящие ICMP	:tick:	Любые

Включено	Входящая активность по протоколу ICMP	Входящие ICMP	:cross:	Любые
Включено	Входящие пакеты ICMPv6 Echo Request	Входящие ICMPv6	:cross:	Любые
Включено	Входящие подключения на 445 SMB	Входящее TCP/445	:cross:	Любые
Включено	Входящие подключения на 445 SMB	Входящее UDP/445	:cross:	Любые

- **Сети**

Важно заполнить!

Название	Статус	IP-адрес/Сеть
	Локальная сеть	
	Публичная сеть	
	Доверенная сеть	

Защита от сетевых угроз

Описание: Защита от опасной сетевой активности

- Настройка защиты от сетевых угроз
  - Считать атаками сканирование портов и интенсивные сетевые запросы - **выключить**
  - Блокировать атакующие устройства на 60 мин - **включить**
  - Исключения - **RedCheck**
- Режим защиты от MAC-спуффинга: **Не отслеживать MAC-спуфинг**

Защита от атак BadUSB

Выключить

AMSI-защита

Описание: Проверка других приложений, таких как макросы Microsoft Office или скрипты PowerShell через интерфейс AMSI

- Проверка составных файлов
  - Проверять архивы - **выключить**
  - Проверять дистрибутивы - **выключить**
  - Проверять файлы офисных форматов - **включить**
  - Не распаковывать составные файлы большого размера - **включить**
  - Максимальный размер файла: **8 Мб**

Detection And Response

Endpoint Sensor

Выключено

Managed Detection and Response

Выключено

Endpoint Detection and Response (KATA)

Выключено

Network Detection and Response (KATA)

Выключено

Контроль безопасности

Анализ журналов

Описание: Мониторинг журналов Windows на предмет подозрительной активности

- Предустановленные правила: **включить все**
- Пользовательские правила:
  - Application popup detection 26
  - Служба была установлена в системе 7045

    - Создана задача в планировщике событий 4696, 602
    - Создание новой учетной записи 4720
    - Добавление пользователя в привилегированную группу 4728
    - Добавление в локальную группу 4732
    - Изменение имени учетной записи 4781
    - Очистка журнала событий 1102

Контроль приложений - Нужен список

- Режим контроля: **Список запрещенных**
    -
    - Действие: **Тестировать правила**
- Использовать строгую проверку цифровой подписи - **включить**

Создать сетевую шару, исключительно для доступа KSC

Создать категорию приложений. Выбрать вариант "**Категория, в которую входят исполняемые файлы приложений, копируемых в указанную папку, обрабатываются автоматически, и их метрики заносятся в категорию**"

Указать это "Хранилище"

- Включать в категорию динамически подключаемые библиотеки DLL - **выключить**
- Включать в категорию данные о скриптах - **выключить**
- Вычислять SHA256 для файлов категории - **включить**
- Вычислять MD5 для файлов категории - **выключить**
- Принудительно проверять папку на наличие изменений - **12ч.**

Положить в папку ПО :

- **AnyDesk**
- **TeamViewer**
- **Ammyy Admin**
- **UltraVNC**
- **AeroAdmin**
- **Radmin Server**
- **uTorrent**
- **qBittorrent**
- **BitTorrent**
- **DC++**
- **Cheat Engine**
- **KMSpico**
- **RatiborusKMS**

- **KMSAuto**
- **Discord**
- **Steam**

Контроль устройств

Устройство	Доступ
Жесткие диски	:tick:
Съемные диски	:tick:
Локальные принтеры	:tick:
Дискеты	:cross:
CD/DVD-приводы	:cross:
Модемы	:cross:
Стримеры	:cross:
Многофункциональные устройства	:tick:
Устройства чтения смарт-карт	:tick:
Widows CE USB ActiveSync устройства	:cross:
Wi-Fi	:tick:
Внешние сетевые адаптеры	:tick:
Портативные устройства MTP	:tick:
Bluetooth	:tick:
Камеры и сканеры	:tick:
Сетевые принтеры	:tick:
Шины подключения	
Инфракрасный порт	:cross:
Последовательный порт	:tick:
Параллельный порт	:tick:
USB (Кроме мышей и клавиатур)	:tick:
FireWire	:cross:
PCMCIA	:cross:

- Разрешить запрашивать временный доступ - **включить**
- Анти-Бриджинг - **выключить**

Веб-Контроль

- Настройки веб-контроля
  - Криптовалюты, майнинг
  - Торренты
  - Для взрослых
  - Запрещено законодательством Российской Федерации
    - Фильтр по категориям: **запретить**

Адаптивный контроль аномалий:

Включить

Контроль целостности системы

- Режим работы блокирующих правил: **Информировать**
- Контролировать целостность системы в режиме реального времени - **включить**
  - Мониторинг файла hosts
    - Следить за устройствами - **включить**
    - Уровень важности событий: **Предупреждение** (надо смотреть логи после включения)
    - Следить за файлами и реестром - **включить**
    - Как пример:

Шифрование данных

Не используется

Локальные задачи

Управление задачами

- Разрешить использование локальных задач - **включено**
- Разрешить отображение групповых задач - **включено**
- Разрешить управление групповыми задачами - **выключено**

Проверка из контекстного меню

- Уровень безопасности: **Рекомендуемый**
  - Типы файлов: **Файлы, проверяемые по формату**
  - Проверять только новые и измененные файлы - **включить**
  - Пропускать файлы, если их проверка длится более - **30с**
  - Проверять все архивы - **включить**
  - Проверять все дистрибутивы - **выключено**
  - Проверять все файлы офисных форматов - **включить**
  - Проверять файлы почтовых форматов - **включить**
  - Проверять архивы, защищенные паролем - **выключено**
  - Дополнительно - Не распаковывать составные файлы большого размера - **100МБ**

- Дополнительно
  - Эвристический анализ: **средний**
  - Технология проверки iSwift - **включить**
  - Технология проверки iChecker - **включить**

- Действие при обнаружении угроз: **Лечить. Удалят, если лечение невозможно**

Проверка съемных дисков

- Действие при подключении съемного диска: **Быстрая проверка**
- Максимальный размер съемного диска: **16384**
- Отображать ход проверки - **включить**
- Запретить остановку задачи проверки - **выключено**

Фоновая проверка

- Включить фоновую проверку - **включить**

Режим легкого агента

Не используется

Интеграция с KUMA

Выключить

Общие настройки

Настройки приложения

- Общие
  - Запускать приложение при включении компьютера - **включить**
  - Применять технологию лечения активного заражения - **выключить**
  - Использовать Kaspersky Security Center в качестве прокси-сервера для активации - **выключить**

- Самозащита
  - Включить самозащиту - **включить**
  - Блокировать внешнее управление службами приложения - **включить**

- Производительность
  - Откладывать задачи по расписанию при работе от аккумулятора - **включить**
  - Уступать ресурсы другим приложениям - **включить**
  - Ограничить потребление ресурсов процессора для задачи проверки - **выключить**

- Отладочная информация
  - Включить запись дампов - **включить**
  - Включить защиту файлов дампов и файлов трассировки - **включить**

- Статус компьютера при применении настроек
  - При ошибке применения политики: **Критический**
  - При ошибке выполнения задачи: **Предупреждение**

- Дополнительные настройки
  - Устанавливать обновления приложения без перезагрузки - **включить**

- Настройки совместимости
  - Совместимость с приложениями для удаленного администрирования - **выключить**

Настройки сети

- Прокси сервер: **по умолчанию**
- Контролируемые порты: **Контролировать только выбранные сетевые порты**
- Проверка защищенных соединений:

    - Проверять защищенные соединения - **включить**
    - Проверять защищенные соединения по запросу компонентов защиты - **включить**

- Ограничивать трафик при лимитном подключении - **включить**
- Внедрять в трафик скрипт взаимодействия с веб-страницами - **выключить**

- Доверенные адреса
    - ***.serbsky.lan, *.serbsky.ru***

- Доверенные приложения
    - Пока пусто

- Дополнительные настройки
    - Переход на домен с не доверенным сертификатом - **Разрешать**
    - Переход на домен с ошибкой проверки защищенного соединения - **Разрешать и добавлять домен в исключения**
    - Блокировать соединения по протоколу SSL 2.0 - **включить**
    - Блокировать соединения по протоколу TLS 1.0 - **включить**
    - Расшифровывать защищенное соединение с сайтом, использующим EV-сертификат - **выключить**

Исключения и типы объектов

- Типы обнаруживаемых объектов - **включить**
    - Вирусы и черви - **включить**
    - Троянские приложения - **включить**
    - Вредоносные утилиты - **включить**
    - Рекламные приложения - **включить**
    - Приложения автодозвона - **включить**
    - Упакованные объекты, способ упаковки которых может использоваться для защиты вредоносного кода - **включить**
    - Многократно упакованные объекты - **включить**
    - Легальные приложения, которые могут быть использованы злоумышленниками - **выключить**

- Исключения из проверки и доверенные приложения - **пока нет списка**

Отчеты и хранилище

- Отчеты
    - Хранить отчеты не более **30 дней**

    - Ограничить размер файла отчетов до **1024 МБ**

- Резервное хранилище
    - Хранить объекты не более **30 дней**
    - Ограничить размер хранилища до **- выключить**

- Карантин
    - Ограничить размер карантина до **200 МБ**
    - Уведомлять при заполнении карантина на **90%**

- Передача данных на Сервер администрирования
    - **Включить все**

Интерфейс

- Взаимодействие с пользователем
    - Скрыть раздел Мониторинг активности - **выключить**
    - Отправлять уведомления "Базы устарели", если базы не обновлялись **3 дня**
    - Отправлять уведомление "Базы сильно устарели", если базы не обновлялись **7 дней**
        - Отображать пользовательский интерфейс - **включить**
        - Уведомления (**надо разбираться с Полиной**)
        - Статусы: **Включить все**
        - Уведомления о состоянии локальных антивирусных баз
        - Защита паролем: **Включить** (настроить на группу в AD)
        - Поддержка пользователей: **"В случае возникновения проблем с работой антивируса, просьба обратиться в сервис деск по адресу https://help.serbsky.ru или по телефону xxxx)**

Профили политик

Нужно обсудить, будем-ли мы мапить группы AD на политики касперского, или просто будем пользоваться структурой Касперского.

Revision #2
Created 18 June 2025 18:51:24 by admin_mf
Updated 18 June 2025 18:54:15 by admin_mf