

Table of Contents

Table of Contents	1
UserGate SIEM 7.x Руководство администратора	5
Введение	6
Архитектура UserGate SIEM	7
Лицензирование	9
Лицензирование UserGate SIEM	10
Первоначальная настройка	12
Общие сведения	13
Развертывание образа UserGate SIEM в виртуальной среде	14
Подключение к устройству	15
Офлайн-операции с узлом	16
Настройка устройства	17
Настройка общих параметров	18
Управление устройством	19
Администраторы	21
Управление сертификатами	24
Серверы аутентификации	25
Профили аутентификации	26
Роли и ролевые разрешения пользователей	27
Каталоги пользователей	31
Расширение системного раздела	32
Кластеризация и отказоустойчивость	33
Настройка сети	37
Настройка сетевых зон	38
Настройка интерфейсов	39
Настройка шлюзов	41
Маршруты	42
Сенсоры	43
Общие сведения	44
Сенсоры UserGate	45
Сенсоры SNMP	46
Управление SNMP MIB	47
Сенсоры WMI	48
Конечные устройства	49
Коннекторы	50
Сборщик логов	51
Общие сведения	52
Настройка параметров syslog-сервера	53
Настройка фильтрации syslog	54
Библиотеки	55
IP-адреса	56
Useragent браузеров	58
Типы контента	60
Списки URL	62
Категории URL	64
Текстовые списки	65
Почтовые адреса	67
Номера телефонов	68
Команды	69
Правила аналитики	70

Правила нормализации логов	71
Профили оповещений	72
Категории срабатываний	73
Внешние сервисы обогащений	74
Приложения syslog	75
Диагностика и мониторинг	76
Маршруты	77
Ping	78
Traceroute	79
Запрос DNS	80
Оповещения	81
Правила оповещений	82
SNMP	83
Параметры SNMP	89
Профили безопасности SNMP	90
Журналы и отчеты	91
Журналы	92
Общие сведения	93
Журнал событий	94
Журнал веб-доступа	95
Журнал DNS	96
Журнал трафика	97
Журнал COB	98
Журнал АСУ ТП	99
Журнал инспектирования SSH	100
История поиска	101
Журналы конечных устройств	102
Журнал syslog	103
Журнал защиты почтового трафика	104
Журнал UserID	105
Журнал RADIUS	106
Экспорт журналов	107
Пользовательская нормализация логов	109
Поиск и фильтрация данных	116
Описание форматов журналов	117
Экспорт журналов в формате CEF	118
Экспорт журналов в формате JSON	135
Отчеты	145
Общие сведения	146
Шаблоны	147
Создание пользовательских шаблонов отчетов	148
Правила отчетов	149
Созданные отчеты	150
Отчеты инцидентов	151
Общие сведения	152
Шаблоны отчетов инцидентов	153
Правила отчетов инцидентов	154
Созданные отчеты инцидентов	155
Аналитика	156
Общие сведения	157
Управление правилами аналитики	158
Поиск событий	160

Управление действиями реагирования	163
Управление срабатываниями правил аналитики	166
Просмотр подробной информации о срабатывании	167
Просмотр списка процессов конечных устройств	168
Использование списков из библиотек в поисковых запросах	169
Отправка нотификаций UserGate SIEM через Telegram	171
Инциденты	173
Общие сведения	174
Настройки инцидентов	175
Дашборд по инцидентам	176
Журнал инцидентов	177
Создание инцидентов безопасности	178
Подробности инцидента	179
Передача отчётов об инцидентах информационной безопасности в ГосСОПКА	180
Интерфейс командной строки	182
Общие положения	183
Общие положения (описание)	184
Команды, доступные до первичной инициализации узла	185
Команды, доступные до первичной инициализации узла (описание)	186
Первоначальная инициализация	187
Первоначальная инициализация (описание)	188
Режим конфигурации	189
Режим конфигурации (описание)	190
Настройка устройства	193
Настройка устройства (описание)	194
Настройка управления доступом к консоли устройства	197
Настройка сертификатов	200
Настройка серверов аутентификации	201
Настройка профилей аутентификации	203
Роли пользователей	204
Каталоги пользователей	205
Настройка сети	206
Зоны	207
Интерфейсы	209
Шлюзы	213
Настройка маршрутизации	214
DNS-настройки	215
Настройка библиотек	216
Настройка библиотек (Описание)	217
Настройка сенсоров	223
Настройка сенсоров (описание)	224
Настройка мониторинга	227
Настройка параметров мониторинга устройства	228
Настройка инцидентов	230
Настройка инцидентов (описание)	231
Настройка аналитики	232
Настройка аналитики (описание)	233
Дашборд	236
Дашборд (описание)	237
Техническая поддержка	238
Раздел технической поддержки	239
Аварийные ситуации	240

Admin	241
Admin (описание)	242
Избранные	243
Избранные (описание)	244
Приложения	245
Требования к сетевому окружению	246
Синтаксис языка запросов	247

Архитектура UserGate SIEM

Documentation: ☒
Product: SIEM
Version: 7.x
Technology: SIEM

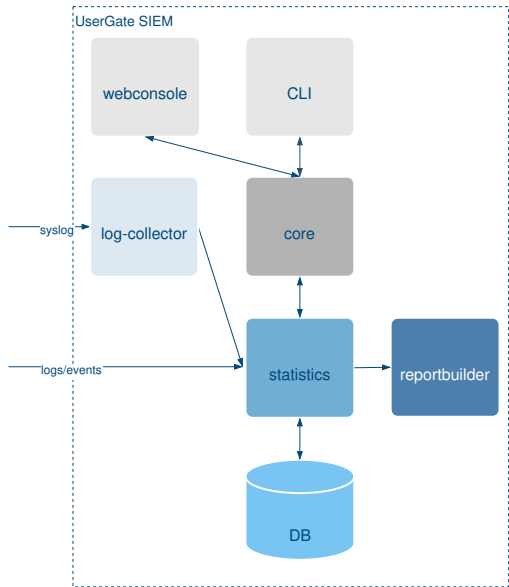
UserGate SIEM — система управления событиями информационной безопасности, которая собирает системные журналы и данные о событиях с различных устройств в подконтрольной сетевой инфраструктуре. Данные подвергаются обработке и анализу, в результате которого могут быть выявлены подозрительные действия или признаки известных сетевых угроз. В зависимости от степени опасности выявленных угроз могут быть произведены определенные действия реагирования, включающие в себя оповещения, создание инцидентов безопасности для дальнейшего расследования или отправка команд на определенные устройства сети с целью предотвращения угрозы.

Результаты обработки данных отображаются в едином веб-интерфейсе, а также предоставляются в виде файлов с отчетами для изучения характерных особенностей инцидентов безопасности. Для проведения расследований инцидентов кибербезопасности используется встроенная в UserGate SIEM система IRP. IRP — это платформа управления процессами реагирования на инциденты информационной безопасности. Она позволяет настроить процесс расследования инцидентов индивидуально под нужды конкретной компании.

UserGate SIEM поставляется в виде образа виртуальной машины, предназначенного для развертывания в виртуальной среде.

Архитектура решения

В основе решения UserGate SIEM лежат следующие программные модули:

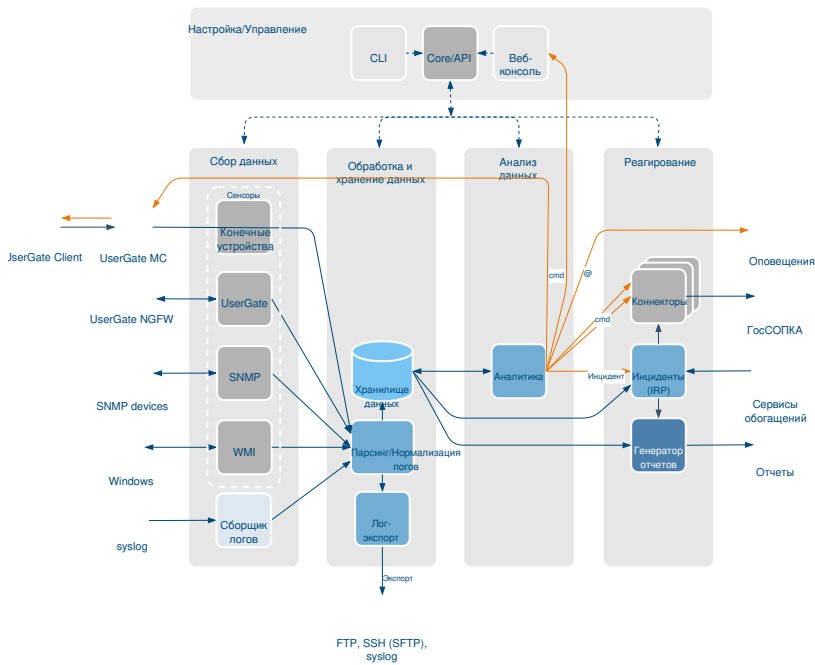


- core — модуль ядра системы, реализующий функции настройки, управления, API, хранения конфигурации.
- statistics — основной функциональный модуль системы, реализующий функции приема, обработки, анализа, хранения данных, создания инцидентов безопасности, управления процессами реагирования, экспорта данных и создания отчетов.
- log-collector — модуль сбора событий от сетевых устройств по протоколу syslog.
- DB — хранилище данных.
- webconsole — модуль веб-консоли управления системой.
- CLI — модуль интерфейса командной строки для управления системой.
- reportbuilder — модуль генерации отчетов в форматах HTML и PDF.

Функциональная модель

Функциональную модель UserGate SIEM можно описать с помощью следующих основных блоков:

- Блок сбора данных.
- Блок обработки данных.
- Блок анализа данных.
- Блок реагирования.
- Блок настройки и управления системой.



Сбор данных

UserGate SIEM собирает данные с внешних источников с помощью сборщика логов (модуль log-collector) и с помощью сенсоров (настраиваются и хранятся в модуле core).

Сборщик логов предназначен для сбора событий от сетевых устройств по протоколу syslog. Настраиваемые правила syslog позволяют осуществлять фильтрацию записей событий по времени, критичности событий, объектам, названию устройств, приложениям, упрощая поиск необходимой информации.

Сенсоры позволяют собирать данные с межсетевых экранов UserGate (сенсор UserGate), конечных устройств с установленным ПО UserGate Client (сенсор конечных устройств), компьютеров под управлением ОС Windows (сенсор WMI), а также с любых других сетевых устройств, способных передавать данные по протоколу SNMP (сенсор SNMP).

При интеграции с межсетевым экраном UserGate NGFW устройство UserGate SIEM сначала подключается к UserGate NGFW с помощью параметров, настроенных в сенсоре UserGate, и передает в UserGate NGFW настройки для подключения. Далее UserGate NGFW собирает свои данные в локальном кэше и периодически передает их в модуль statistics в UserGate SIEM по таймеру.

С помощью сенсора SNMP можно подключить SNMP-совместимое сетевое устройство к UserGate SIEM для сбора и анализа его метрик. SIEM может отображать любые метрики, полученные с помощью запросов SNMP. Для настройки сенсора SNMP необходимо иметь базы MIB на управляемое устройство. Базы MIB устройств сторонних производителей могут импортироваться в систему SIEM.

С помощью сенсора WMI можно подключить WMI-совместимое сетевое устройство (компьютер под управлением ОС Windows) к UserGate SIEM для сбора и анализа его данных. В настройках сенсора WMI указываются адрес устройства, атрибуты входа в устройство, пространство имен и параметры event-лога Windows, которые будут контролироваться системой SIEM.

Конечные устройства с установленным ПО UserGate Client подключаются к UserGate SIEM не напрямую, а через UserGate Management Center. При интеграции UserGate SIEM с UserGate MC между ними устанавливается SSH-туннель, по которому параметры настройки и данные статистики с интегрированных в MC конечных устройств передаются на UserGate SIEM.

Обработка и хранение данных

Собираемые данные поступают в модуль statistics, где они подвергаются предварительному анализу и нормализации. В процессе нормализации записи журналов, полученные из различных источников, приводятся к единому виду, пригодному для записи в стандартные поля базы данных UserGate SIEM. Далее нормализованные записи передаются в сервис лог-экспорта и в хранилище данных.

Сервис лог-экспорта с помощью настраиваемых правил позволяет экспортировать журналы (в формате CEF или JSON) на внешние серверы FTP, SSH (SFTP) и syslog. Отправка на серверы SSH и FTP проводится по указанному в настройках правил расписанию или разово. Отправка на серверы syslog происходит сразу же при добавлении записи в журнал.

В таблицах хранилища данных содержатся все собранные записи журналов как самого устройства UserGate SIEM, так и подключенных к нему устройств. Также в таблицах хранилища данных содержатся созданные инциденты и оповещения.

Данные устройств в таблицах хранятся по ключу, который содержит в себе ClusterID. Например, при регистрации UserGate NGFW в UserGate SIEM в модуле statistics для него создается аккаунт, в котором ему прописывается ClusterID и токен. Токен возвращается в UserGate NGFW и используется для авторизации.

Журналы в хранилище данных циклически перезаписываются, обеспечивая необходимое для работы свободное дисковое пространство. Ротация записей журналов (всех, кроме журнала событий) происходит автоматически по критерию свободного пространства на данном разделе. Записи о ротации базы данных отображаются в журнале событий UserGate SIEM. Ротация записей журнала событий не производится.

Анализ данных

Сервис аналитики работает также в модуле statistics. С его помощью производится анализ журналов событий безопасности, полученных с настроенных сенсоров. В процессе анализа данных сервис аналитики производит агрегацию повторяющихся событий и их корреляцию, используя условия правил аналитики, написанные с помощью SQL-подобного синтаксиса. В случае срабатывания правила будет выполнено действие реагирования, настроенное для данного правила.

Реагирование

В качестве мер реагирования на выявленные в результате анализа данных аномалии и угрозы безопасности могут использоваться следующие действия:

- Визуализация срабатываний системы анализа данных в консоли управления системой.
- Оповещение персонала служб информационной безопасности.
- Создание инцидента информационной безопасности для дальнейшего расследования.
- Создание отчетов об инцидентах информационной безопасности.
- Отправка команд на определенные сетевые устройства с целью снижения угрозы.

В правилах аналитики UserGate SIEM задаются действия реагирования, которые должны выполняться в случае их срабатывания. В качестве таких действий могут быть использованы оповещения по email или SMS, отображение информации на специальной веб-странице (webhook), отправка команд для выполнения на сетевом устройстве, создание инцидента. Создание инцидента как действие реагирования позволяет автоматизировать процесс создания инцидентов информационной безопасности. Информация о срабатывании правил аналитики и о созданных инцидентах безопасности выводится в режиме онлайн на информационных экранах и дашбордах в веб-консоли администратора UserGate SIEM.

Расследование инцидентов информационной безопасности производится с помощью платформы управления процессами реагирования — IRP (Incident Response Platform). Сервис IRP интегрирован с сервисом аналитики и необходим для управления процессами реагирования на инциденты информационной безопасности. При расследовании инцидентов сервис IRP использует внешние ресурсы для сбора дополнительной информации — внешние сервисы обогащения. В случае, если в качестве улик к инциденту прикреплены записи журнала, то IRP автоматически извлекает сведения об индикаторах компрометации (IP-адресе, URL, домене, названии файла, хэш) для работы с внешними сервисами обогащения.

С помощью модуля генерации отчетов могут создаваться отчеты по инцидентам безопасности в формате PDF или HTML, которые доступны для скачивания или отправки на электронную почту.

С помощью настраиваемых программных коннекторов возможна организация подключения системы UserGate SIEM к различным средствам защиты или службам обмена данными об инцидентах информационной безопасности. Через коннектор с типом сервера SSH возможна передача команд на подключаемое устройство в качестве реакции на срабатывание правила аналитики. По умолчанию в системе создан коннектор Gossorka, предназначенный для автоматизации обмена информацией об инцидентах информационной безопасности с ГосСОПКА (Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак).

Настройка и управление

Модуль веб-консоли взаимодействует с большинством модулей UserGate SIEM и выполняет функции управления и представления данных. Модуль позволяет формировать и просматривать отчеты и журналы, использовать графическое представление данных с помощью виджетов дашборда, производить настройки в веб-интерфейсе управления (общие настройки SIEM, настройки правил аналитики, управление инцидентами безопасности и т. д.).

Запросы из веб-консоли приходят сначала в модуль core в специальный сервис Web Console Proxy, затем запросы на чтение данных напрямую (не попадая в API) перебрасываются в модуль statistics. Statistics обрабатывает эти запросы, формирует корректные SQL-запросы к базе данных и возвращает данные обратно по прямому туннелю в веб-консоль.

Настройка UserGate SIEM также может выполняться с использованием интерфейса командной строки посредством модуля CLI. Команды интерфейса CLI реализованы с помощью API.

Лицензирование UserGate SIEM

Documentation: ☒
Product: SIEM
Version: 7.x
Technology: SIEM

Для использования UserGate SIEM необходима [базовая лицензия](#), которая предоставляет доступ к основным функциям устройства. Чтобы получать обновления UserGate SIEM и использовать его расширенные функции, нужны [дополнительные лицензии](#).

В веб-консоли UserGate SIEM вы можете активировать и обновить лицензию, а также проверить срок ее действия [в онлайн-режиме](#). Если доступ к серверу лицензирования отсутствует, возможна [активация лицензии офлайн](#).

Базовая лицензия

Базовая лицензия UserGate SIEM является бессрочной. В нее включена годовая подписка Security Updates, которая обеспечивает обновления программного обеспечения и библиотеки правил нормализации в течение первого года. По истечении этого срока подписку необходимо продлить для продолжения получения обновлений.

Кроме того, базовая лицензия UserGate SIEM позволяет подключать любое количество сенсоров. При отсутствии базовой лицензии подключение сенсоров к устройству невозможно.

Лицензирование UserGate SIEM версий 7.3.0 и выше осуществляется по параметрам производительности платформы.

При активации базовой лицензии проверяются следующие параметры:

- **Тип аппаратной платформы.** Для устройства, поставляемого в виде программно-аппаратного комплекса, тип аппаратной платформы должен совпадать с указанным в лицензии.
- **Количество ядер виртуальной машины** . Для устройства, поставляемого в виде виртуального образа, количество поддерживаемых ядер процессора должно быть меньше или равно количеству ядер, разрешенному лицензией.

В случае несоответствия параметров устройства указанным в лицензии процесс активации будет завершен с ошибкой. Кроме того, если после активации лицензии в виртуальную машину будет добавлено больше ядер, чем предусмотрено базовой лицензией, устройство будет использовать только разрешенное количество ядер. Начиная с версии 7.4.0 в разделе **Дашборды** в виджете с лицензией вы можете просматривать информацию об ограничениях на количество ядер процессора.

Дополнительные лицензии

Для расширения функциональности доступны следующие подписки и модули UserGate SIEM.

Подписки и модули	Описание
Security Updates (SU)	Подписка предоставляет доступ к сервису обновления UserGate SIEM и дает право на получение обновлений: • программного обеспечения (ПО); • библиотеки правил нормализации. Срок действия подписки — 1 год. По окончании этого срока: • последняя установленная версия ПО устройства остается работоспособной без возможности обновления; • обновление библиотеки правил нормализации прекращается
Cluster	Модуль обеспечивает возможность работы устройств UserGate SIEM в режиме кластера. Срок действия лицензии на модуль не ограничен
SIEM Expert	Модуль предоставляет право на поддержку и обновление экспертизы UserGate: • библиотеки правил аналитики; • библиотеки команд удаленного управления устройствами UserGate. Модуль поставляется на срок от 1 до 5 лет. По истечении этого срока скачанные библиотеки остаются работоспособными, но их обновление становится недоступным. Для возобновления обновлений необходимо продлить лицензию. Продление доступно только при наличии действующей подписки SU

Онлайн-лицензирование

При активации, проверке и обновлении лицензии UserGate SIEM подключается к серверу лицензирования <https://reg2.usergate.com> и передает номер версии ПО, лицензионный ключ, название и модель устройства. В ответ UserGate SIEM получает данные о сроке действия лицензии и поддерживаемых модулях.

Активация лицензии

Чтобы активировать лицензию:

1. В разделе **Дашборды** в виджете **Лицензия** нажмите **Нет лицензии**.
2. В поле **ПИН-код** введите лицензионный ключ и нажмите **Далее**.

Если UserGate SIEM установлен в изолированной сети (без доступа в интернет), вы можете активировать лицензию с использованием прокси-сервера. Для этого выберите **Использовать прокси-сервер для активации и апдейтов** и укажите параметры вышестоящего прокси-сервера.

3. Следуйте указаниям мастера активации устройства.

Проверка лицензии

Автоматическая проверка срока действия лицензии выполняется раз в сутки, ее результаты отображаются в журнале событий UserGate SIEM. По окончании проверки отключаются те модули, срок поддержки которых истек, и подключаются вновь доступные.

Если во время проверки не удалось получить доступ к серверу лицензирования, выполняется 14 попыток подключения к серверу с интервалом в 2 минуты. При неуспешных попытках проверка приостанавливается на сутки, после чего попытки повторяются. Если за это время истечет срок действия лицензии на один из модулей, модуль будет отключен.

Вы также можете запускать проверку срока действия лицензии вручную. Действие доступно в разделе **Дашборды** в виджете **Лицензия** по ссылке **Проверить лицензию**.

Обновление лицензии

Чтобы обновить лицензию:

1. В разделе **Дашборды** в виджете **Лицензия** нажмите **Зарегистрированная версия**.
2. В поле **ПИН-код** введите лицензионный ключ и нажмите **Далее**.

Если UserGate SIEM установлен в изолированной сети (без доступа в интернет), вы можете обновить лицензию с использованием прокси-сервера. Для этого выберите **Использовать прокси-сервер для активации и апдейтов** и укажите параметры вышестоящего прокси-сервера.

3. Следуйте указаниям мастера активации устройства.

Офлайн-активация лицензии

Вы можете активировать лицензию устройства в офлайн-режиме. Это нужно в том случае, если UserGate SIEM установлен в изолированной сети (без доступа в интернет) и нет возможности использовать прокси-сервер для активации.

Чтобы активировать лицензию офлайн:

1. Войдите в веб-консоль UserGate SIEM по ссылке <https://<IP-адрес веб-консоли>:8001?features=offline-reg>.
2. В разделе **Дашборды** в виджете **Лицензия** нажмите **Нет лицензии**.
3. Нажмите **Начать активацию в автономном режиме**.
4. В поле **ПИН-код** введите лицензионный ключ и нажмите **Далее**.
Будет сгенерирован файл с запросом на активацию лицензии (далее также — файл запроса).
5. Сохраните файл запроса на съемный носитель.

6. Закройте окно по кнопке **Отмена**.

7. Получите файл активации запроса через сервис офлайн-активации лицензий poa.usergate.com.

Подробнее об активации запроса — в разделе «[Офлайн-активация лицензий](#)».

Примечание Для выполнения действий требуется подключение к интернету и учетная запись для авторизации в сервисе офлайн-активации. Получить учетную запись можно зарегистрировавшись в Едином центре авторизации id.usergate.com.

8. Повторите шаг 2 инструкции.

9. Нажмите **Завершить активацию в автономном режиме**.

10. Загрузите файл активации запроса и нажмите **Далее**.

11. Следуйте указаниям мастера активации устройства.

Общие сведения

Documentation: 
Product: SIEM
Version: 7.x

UserGate SIEM поставляется в виде образа виртуальной машины (virtual appliance) с четырьмя Ethernet-интерфейсами, предназначенного для развертывания в виртуальной среде.

Развертывание образа UserGate SIEM в виртуальной среде

Documentation: ☒

Product: SIEM

Version: 7.x

Для установки UserGate SIEM в виртуальной среде потребуется образ виртуальной машины и гипервизор для импорта этого образа. Поддерживаются такие системы виртуализации, как VMware, Oracle VirtualBox, Microsoft Hyper-V и KVM.

Гипервизор для импорта образа виртуальной машины с UserGate SIEM должен поддерживать работу 64-битных операционных систем.

Если требуется обеспечить большой объем хранения данных, рекомендуется создать выделенный диск (например, объемом 20 ТБ) и добавить его после импорта образа, до первого запуска виртуальной машины. Добавление диска в уже работающий продукт не позволит увеличить объем хранилища.

Примечание При установке UserGate SIEM на диск объемом более 16 ТБ часть дискового пространства не используется. Это связано с параметрами файловой системы, которые применяются по умолчанию. Например, после добавления диска объемом 20 ТБ для записи событий доступно 16 ТБ, так как часть дискового пространства резервируется под системные требования.

Для развертывания виртуального образа с UserGate SIEM:

1. Скачайте образ виртуальной машины в личном кабинете клиента на официальном сайте usergate.com и распакуйте этот образ.
2. Импортируйте образ виртуальной машины в гипервизор согласно инструкции, размещенной на сайте производителя используемой системы виртуализации.
- Важно!** Для Microsoft Hyper-V и KVM требуется создать виртуальную машину и указать в качестве диска скачанный образ. После этого в параметрах виртуальной машины необходимо отключить службы интеграции.
3. Если в свойствах виртуальной машины объем ОЗУ и размер диска ниже значений, указанных в минимальных аппаратных требованиях, увеличьте значения этих параметров.
4. Подключите сетевые интерфейсы к виртуальным коммутаторам.

По умолчанию в UserGate SIEM предусмотрены два интерфейса — port0 и port1, назначенные для зон Management и Trusted соответственно. При необходимости вы можете добавить дополнительные сетевые интерфейсы.

5. Если для хранения данных нужен диск объемом 20 ТБ и более, добавьте его до запуска виртуальной машины.

6. Запустите виртуальную машину.

При первом запуске выполняется сброс параметров виртуальной машины до значений по умолчанию и применение настроенной конфигурации.

Подключение к устройству

Documentation: ☒
Product: SIEM
Version: 7.x

Интерфейс port0 настроен на получение IP-адреса в автоматическом режиме (DHCP) и назначен в зону **Management**. Первоначальная настройка осуществляется через подключение администратора к веб-консоли через интерфейс port0.

Если нет возможности назначить адрес для Management-интерфейса в автоматическом режиме с помощью DHCP, то его можно явно задать, используя CLI (Command Line Interface). Более подробно об использовании CLI смотрите в главе [Интерфейс командной строки \(CLI\)](#).

Примечание Если устройство не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя *Admin*, в качестве пароля — *usergate*.

Остальные интерфейсы отключены и требуют последующей настройки.

Первоначальная настройка требует выполнения следующих шагов:

Наименование	Описание
Шаг 1. Подключиться к интерфейсу управления	При наличии DHCP-сервера. Подключить интерфейс port0 в сеть предприятия с работающим DHCP-сервером. Включить устройство. После загрузки устройство укажет IP-адрес, на который необходимо подключиться для дальнейшей активации продукта. Статический IP-адрес. Включить устройство. Используя CLI (Command Line Interface), назначить необходимый IP-адрес на интерфейс port0. Детали использования CLI смотрите в главе Интерфейс командной строки (CLI). Подключиться к веб-консоли UserGate SIEM по указанному адресу, он должен выглядеть примерно следующим образом: <code>https://SIEM_IP_address:8010</code>.
Шаг 2. Выбрать язык	Выбрать язык, на котором будет продолжена первоначальная настройка.
Шаг 3. Задать пароль	Задать логин и пароль для входа в веб-интерфейс управления.
Шаг 4. Зарегистрировать систему	Ввести ПИН-код для активации продукта и заполнить регистрационную форму. Для активации системы необходим доступ устройства в Интернет. Если на данном этапе выполнить регистрацию не удается, то ее следует повторить после настройки сетевых интерфейсов на шаге 8.
Шаг 5. Настроить зоны, IP-адреса интерфейсов, подключить UserGate SIEM в сеть предприятия	В разделе Интерфейсы включить необходимые интерфейсы, установить корректные IP-адреса, соответствующие вашим сетям, и назначить интерфейсы соответствующим зонам. Подробно об управлении интерфейсами читайте в главе Настройка интерфейсов. Система поставляется с предопределенными зонами: - Зона Management (сеть управления), интерфейс port0. - Зона Trusted (LAN). Предполагается, что через зону Trusted UserGate SIEM будет подключен в сеть, через которую шлюзы UserGate будут отсылать на него журналы, а также через которую UserGate SIEM получит доступ в интернет. Для работы UserGate SIEM достаточно одного настроенного интерфейса. Разделение функций управления устройством и сбора данных на разные сетевые интерфейсы рекомендовано для обеспечения безопасности, но не является жестким требованием.
Шаг 6. Настроить шлюз в Интернет	В разделе Шлюзы указать IP-адрес шлюза в Интернет на интерфейсе, имеющим доступ в Интернет, как правило, это зона Trusted . Подробно о настройке шлюзов в Интернет читайте в главе Настройка шлюзов .
Шаг 7. Указать системные DNS-серверы	В разделе DNS укажите IP-адреса серверов DNS, вашего провайдера или серверов, используемых в вашей организации. Подробно об управлении DNS читайте в главе Раздел настройки .
Шаг 8. Зарегистрировать продукт (если не был зарегистрирован на шаге 4)	Зарегистрировать продукт с помощью ПИН-кода. Для успешной регистрации необходимо подключение к Интернету и выполнение предыдущих шагов. Более подробно о лицензировании продукта читайте в главе Лицензирование UserGate SIEM .
Шаг 9. Создать дополнительных администраторов (опционально)	В разделе Администраторы создать дополнительных администраторов системы, наделить их необходимыми полномочиями (ролями).

После выполнения вышеперечисленных действий UserGate SIEM готов к работе. Для более детальной настройки обратитесь к необходимым главам справочного руководства.

Офлайн-операции с узлом

Documentation: ☒
Product: SIEM
Version: 7.x

Некоторые операции с узлом проводятся, когда узел не выполняет свою функцию и находится в офлайн-режиме. Для выполнения таких операций необходимо во время загрузки узла выбрать раздел меню **Support menu** и затем одну из требуемых операций. Для получения доступа к этому меню необходимо подключить монитор к разъему VGA(HDMI), клавиатуру к разъему USB (при наличии соответствующих разъемов на устройстве) или используя специальный кабель для последовательного порта или переходник USB-Serial, подключить свой компьютер к UserGate SIEM. Запустить терминал, позволяющий подключение через последовательный порт, например, Putty для Windows. Установить подключение через последовательный порт, указав параметры подключения 115200 8n1.

Во время загрузки администратор может выбрать один из нескольких пунктов загрузки в boot-меню:

Наименование	Описание
UGOS SIEM	Загрузка узла UserGate SIEM с выводом диагностической информации о загрузке в последовательный порт.
UGOS SIEM (failsafe)	Загрузка узла UserGate SIEM в упрощённом видео режиме.
Support menu	Войти в раздел системных утилит с выводом информации в консоль tty1 (монитор).
Restore previous version	Раздел доступен после обновления или создания резервной копии.

Раздел системных утилит (Support menu) позволяет выполнить следующие действия:

Наименование	Описание
Check filesystems	Запуск проверки файловой системы устройства на наличие ошибок и их автоматическое исправление.
Expand data partition	Увеличение раздела для хранения данных на весь выделенный диск. Эта операция обычно используется после увеличения дискового пространства, выделенного гипервизором для виртуальной машины узла UserGate. Данные и настройки узла UserGate не сбрасываются.
Create backup	Создать полную копию диска узла UserGate на внешний USB-носитель. Все данные на внешнем носителе будут удалены.
Restore from backup	Восстановление узла UserGate с внешнего USB-носителя.
Factory reset	Сброс состояния узла UserGate к первоначальному состоянию системы. Все данные и настройки будут утеряны.
Exit	Выход и перезагрузка устройства.

Настройка общих параметров

Documentation: ☒
Version: 7.x
Product: SIEM

В этом разделе описаны общие параметры UserGate SIEM, а также приведены рекомендации по настройке этих параметров.

Блок параметров	Параметр	Описание
Настройки интерфейса	Часовой пояс	Часовой пояс, соответствующий вашему местоположению. Используется для работы расписаний, настроенных в правилах, а также для корректного отображения времени и даты, например в отчетах или в журналах
	Язык интерфейса по умолчанию	Язык, используемый в веб-консоли устройства по умолчанию
	Таймер автоматического закрытия сессии (мин.)	Для настройки таймера необходимо указать, по истечении скольких минут бездействия администратора в веб-консоли должна завершаться его сессия
Настройка времени сервера	Использовать NTP	При включенном параметре для синхронизации времени на устройстве будут использоваться серверы NTP из указанного списка
	Основной сервер NTP	Адрес основного сервера точного времени. Значение по умолчанию — pool.ntp.org
	Запасной сервер NTP	Адрес запасного сервера точного времени
	Время на сервере (UTC)	Время на сервере в часовом поясе UTC
Обновления ПО (в версиях 7.1.x, 7.2.x, 7.3.x доступен общий блок параметров с обновлениями — Центр обновлений)	Канал обновлений	Настройка канала для получения обновлений программного обеспечения UserGate (UGOS) из репозитория UserGate. Вы можете выбрать Стабильные (стабильные версии ПО) или Бета (версии ПО для бета-тестирования). Если настроена интеграция с UserGate Management Center, параметр примет значение Management Center и будет недоступен для изменения
	Обновления	Проверка наличия обновлений UGOS в репозитории UserGate. После проверки вы можете вручную загрузить и установить доступные обновления. В процессе установки обновления UGOS вы можете создать точку восстановления. Это позволит восстановить предыдущую версию UGOS при возникновении проблем. Действие будет доступно в стартовом меню после установки обновления UGOS
	Офлайн-обновление	Загрузка файла обновления UGOS офлайн
Обновления библиотек (в версиях 7.1.x, 7.2.x, 7.3.x доступен общий блок параметров с обновлениями — Центр обновлений)	Обновления	Проверка наличия обновлений системных библиотек, предоставляемых по подписке, в репозитории UserGate. После проверки вы можете вручную обновить необходимые библиотеки
	Расписание автоматических обновлений	Настройка расписания автоматического обновления библиотек. При настройке расписания вы можете выбрать одно из предустановленных значений или указать время вручную в cron-формате: <минуты: 0-59> <часы: 0-23> <дни месяца: 1-31> <месяцы: 1-12> <дни недели: 0-6, где 0 — воскресенье>. Для ручного ввода вы можете использовать следующие символы: - Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что резервное копирование должно выполняться каждый час. - Дефис (-) — для указания диапазона значений. - Запятая (,) — в качестве разделителя значений. - Косая черта (/) — для указания шага между значениями. При установке флажка Единое расписание для всех обновлений расписание выбранной библиотеки будет применено ко всем библиотекам в списке
Учет изменений	Настройка учета изменений	Для настройки учета изменений в веб-консоли устройства необходимо включить параметр и добавить типы изменений (например, распоряжение, приказ или регламентные работы). Учет изменений предполагает, что при внесении какого-либо изменения через веб-консоль администратору необходимо указать тип и причину этого изменения
Системные DNS-серверы		Для настройки DNS-серверов необходимо указать их IP-адреса
Состояние базы данных журналов	Состояние	Состояние модуля статистики
	Версия устройства	Версия ПО UserGate SIEM
	Метрики	Количество событий, которые получает модуль статистики (среднее значение за последние 5 секунд)
Состояние сборщика логов	Состояние	Состояние модуля сбора событий syslog
	Метрики	Количество событий, которые получает модуль сбора событий syslog (среднее значение за последние 5 секунд)
Агент UserGate Management Center	Настройка агента	Настройка интеграции с UserGate Management Center (UGMC). Для настройки доступны следующие параметры: Включено — управление состоянием подключения UserGate SIEM к UGMC. Адрес UserGate Management Center — адрес сервера UGMC в формате IPv4-адреса или FQDN (возможно использование IDN-адреса). Код устройства — идентификатор UserGate SIEM для подключения к UGMC

Управление устройством

Version: 7.x
Product: SIEM
Documentation: 

В разделе **Настройки** → **UserGate** → **Управление устройством** вы можете настраивать следующие параметры устройства:

- кластеры отказоустойчивости;
- кластер конфигурации;
- диагностика;
- операции с сервером;
- резервное копирование;
- экспорт и импорт настроек.

Информация о настройке кластеров приведена в разделе «[Кластеризация и отказоустойчивость](#)».

Диагностика

В этом блоке вы можете управлять параметрами диагностики, необходимыми службе технической поддержки UserGate для решения возможных проблем в работе устройства.

Параметр	Описание
Детализация диагностики	Доступны следующие уровни журналирования: • Off — ведение журналов диагностики отключено. • Error — журналировать только ошибки в работе SIEM-системы. • Warning — журналировать только ошибки и предупреждения. • Info — журналировать только ошибки, предупреждения и дополнительную информацию. • Debug — журналировать все возможные события. При журналировании уровней Warning , Info и Debug может снижаться производительность SIEM-системы, поэтому рекомендуется устанавливать уровни Error или Off , если технической поддержкой UserGate не было предложено иное
Журналы диагностики	Вы можете: • Скачать журналы — скачать диагностические журналы для их передачи в службу технической поддержки UserGate. Для скачивания доступны журналы веб-консоли и системные журналы. Скачать выбранные журналы можно только после их архивирования по кнопке Начать архивирование журналов. • Очистить файлы логов — удалить архивные (неактивные в настоящий момент) журналы
Удаленный помощник	Удаленный помощник позволяет специалисту технической поддержки UserGate безопасно подключаться к серверу UserGate SIEM для диагностики и решения проблем. Для активации удаленного помощника устройство должно иметь доступ к серверу удаленного помощника по протоколу SSH. При включенном удаленном помощнике отображаются его идентификатор и токен, которые необходимо сообщить специалисту технической поддержки UserGate

Операции с сервером

В этом блоке вы можете перезагрузить или выключить сервер UserGate SIEM, а также настроить вышестоящий прокси-сервер для получения лицензий и обновлений устройства.

Наименование	Описание
Операции с сервером	Доступны следующие действия: • Перезагрузить — перезагрузка сервера UserGate SIEM. • Выключить — выключение сервера UserGate SIEM
Настройки вышестоящего прокси для проверки лицензий и обновлений	Настройка параметров вышестоящего HTTP или HTTPS прокси-сервера, используемого для получения лицензий и обновлений устройства. Вы можете настроить IP-адрес и порт вышестоящего прокси-сервера, а также логин и пароль, если необходима аутентификация на этом прокси-сервере

UserGate поставляет обновления в рамках лицензии на модуль Security Update (см. раздел «[Лицензирование UserGate SIEM](#)»). При наличии обновлений в блоке **Операции с сервером** отобразится соответствующее оповещение. Установка обновлений может занять длительное время, поэтому рекомендуется планировать этот процесс с учетом возможного времени простоя UserGate SIEM.

Перед установкой обновлений рекомендуется создать резервную копию UserGate SIEM. Это позволит восстановить предыдущее состояние устройства, если возникнут проблемы, связанные с применением обновлений.

Управление резервным копированием

В этом блоке вы можете:

- [создавать резервные копии;](#)
- [восстанавливать состояние устройства из резервной копии;](#)
- [настраивать расписание экспорта резервных копий на удаленный сервер;](#)
- [настраивать SSH-ключи.](#)

Чтобы создать резервную копию устройства:

В разделе **Настройки** → **UserGate** → **Управление устройством** → **Управление резервным копированием** нажмите **Создание резервной копии**.

Начнется создание резервной копии. Вы можете прервать процесс по кнопке **Остановить**.

По окончании процесса резервная копия UserGate SIEM будет сохранена в файле backup_PRODUCT_NODENAME_DATE.gpg, где:

- PRODUCT — тип устройства: SIEM;
- NODENAME — имя узла устройства;
- DATE — дата и время создания резервной копии в формате YYYY-MM-DD-HH-MM (в часовом поясе UTC+0).

Запись о создании резервной копии отобразится в журнале событий устройства.

Чтобы восстановить состояние устройства из резервной копии:

1. В разделе **Настройки** → **UserGate** → **Управление устройством** → **Управление резервным копированием** нажмите **Восстановление резервной копии** и подтвердите восстановление.
2. Укажите путь к файлу с резервной копией UserGate SIEM.
Восстановление будет предложено в консоли TTY при перезагрузке сервера UserGate SIEM.

Администраторы могут создавать правила экспорта, по которым резервные копии будут выгружаться на удаленные серверы по расписанию.

Чтобы создать правило экспорта резервной копии устройства:

1. В разделе **Настройки** → **UserGate** → **Управление устройством** → **Управление резервным копированием** нажмите **Добавить**.
2. На вкладке **Общие** укажите имя правила.
3. На вкладке **Удаленный сервер** укажите параметры удаленного сервера:
 - тип — FTP или SSH;
 - адрес;

- порт для подключения;
- логин и пароль учетной записи;
- путь к существующей папке для сохранения файлов экспорта.

Внимание! Если вы создаете правило для SSH-сервера, необходимо [предварительно настроить SSH-ключи](#). Кроме того, необходимо проверить соединение с SSH-сервером по кнопке «Проверить соединение». Во время проверки устанавливается первичное соединение, при котором отпечаток открытого ключа автоматически добавляется на удаленный сервер. Это обеспечивает безопасность последующих соединений.

4. На вкладке **Расписание** укажите время экспорта резервной копии.

Вы можете выбрать одно из предустановленных значений или указать время вручную в cron-формате: <минуты: 0—59> <часы: 0—23> <дни месяца: 1—31> <месяцы: 1—12> <дни недели: 0—6, где 0 — воскресенье>.

При ручном вводе также можно использовать следующие символы:

- Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что резервное копирование должно выполняться каждый час.
- Дефис (-) — для указания диапазона значений.
- Запятая (,) — в качестве разделителя значений.
- Косая черта (/) — для указания шага между значениями.

5. Нажмите **Сохранить**.

Перед подключением к удаленному SSH-серверу, необходимо настроить SSH-ключи, используемые для авторизации на этом сервере.

Чтобы настроить SSH-ключи:

1. В разделе **Настройки** → **UserGate** → **Управление устройством** → **Управление резервным копированием** нажмите **Настроить SSH-ключ**.
2. Нажмите **Сгенерировать новый ключ**.

Будет сгенерирована пара SSH-ключей (закрытый и открытый). Открытый ключ отобразится в окне настройки, закрытый ключ будет автоматически сохранен на сервере UserGate SIEM.

Примечание! Если у вас уже есть пара SSH-ключей, вы можете добавить закрытый ключ на сервер UserGate SIEM вручную по кнопке «Загрузить ключ».

3. Добавьте открытый SSH-ключ на удаленный сервер.

По умолчанию SSH-ключи хранятся в папке /home/user/.ssh/ в файле authorized_keys.

Экспорт и импорт настроек

В этом блоке вы можете экспортировать текущие параметры UserGate SIEM в виде файлов экспорта в формате BIN. Впоследствии такие файлы могут понадобиться [для восстановления параметров устройства](#), а также для импорта в другие системы SIEM.

Экспорт может выполняться [вручную](#) или [по расписанию](#). Вы можете экспортировать **все текущие параметры** или **только сетевые**. К сетевым относятся параметры зон, интерфейсов, шлюзов, маршрутов. Сетевые параметры настраиваются в разделе **Настройки** → **Сеть**.

Чтобы экспортировать все параметры устройства:

В разделе **Настройки** → **UserGate** → **Управление устройством** → **Экспорт и импорт настроек** нажмите **Экспорт** → **Экспортировать все настройки**.

Параметры будут сохранены в файле siem_core-siem_core@NODENAME_VERSION_DATE.bin, где:

- NODENAME — имя узла устройства;
- VERSION — версия UGOS;
- DATE — дата и время выгрузки параметров в формате YYYYMMDD_HHMMSS (в часовом поясе UTC+0).

Чтобы экспортировать только сетевые параметры устройства:

В разделе **Настройки** → **UserGate** → **Управление устройством** → **Экспорт и импорт настроек** нажмите **Экспорт** → **Экспортировать сетевые настройки**.

Параметры будут сохранены в файле network-siem_core-siem_core@NODENAME_VERSION_DATE.bin, где:

- NODENAME — имя узла устройства;
- VERSION — версия UGOS;
- DATE — дата и время выгрузки параметров в формате YYYYMMDD_HHMMSS (в часовом поясе UTC+0).

Администраторы могут создавать правила экспорта, по которым параметры устройства будут выгружаться на удаленные серверы по расписанию. Если узлы устройства объединены в кластер, то при создании правила экспорта на одном из узлов это правило будет распространяться на все узлы кластера. Параметры каждого узла при экспорте будут сохраняться в отдельном файле.

Чтобы создать правило экспорта параметров устройства:

1. В разделе **Настройки** → **UserGate** → **Управление устройством** → **Экспорт и импорт настроек** нажмите **Добавить**.

2. На вкладке **Общие** укажите имя правила.

3. На вкладке **Удаленный сервер** укажите параметры удаленного сервера:

- тип — FTP или SSH;
- адрес;
- порт для подключения;
- логин и пароль учетной записи;
- путь к существующей папке для сохранения файлов экспорта.

Примечание! Для авторизации на удаленном SSH-сервере вы можете использовать SSH-ключи. Для этого их нужно [предварительно настроить](#).

Внимание! Если вы создаете правило для SSH-сервера с авторизацией по SSH-ключам, вам необходимо проверить соединение с этим сервером по кнопке «Проверить соединение». Во время проверки устанавливается первичное соединение, при котором отпечаток открытого ключа автоматически добавляется на удаленный сервер. Это обеспечивает безопасность последующих соединений.

4. На вкладке **Расписание** укажите время экспорта параметров.

Вы можете выбрать одно из предустановленных значений или указать время вручную в cron-формате: <минуты: 0—59> <часы: 0—23> <дни месяца: 1—31> <месяцы: 1—12> <дни недели: 0—6, где 0 — воскресенье>.

При ручном вводе также можно использовать следующие символы:

- Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что резервное копирование должно выполняться каждый час.
- Дефис (-) — для указания диапазона значений.
- Запятая (,) — в качестве разделителя значений.
- Косая черта (/) — для указания шага между значениями.

5. Нажмите **Сохранить**.

Вы можете восстанавливать параметры устройства из файлов экспорта. Эти файлы не содержат данные о кластерах и лицензии, поэтому после восстановления параметров вам потребуется повторно активировать лицензию и настроить кластеры. Кроме того, если для входа в UserGate SIEM вы используете многофакторную аутентификацию через TOTP, после восстановления необходимо повторно добавить ключи инициализации.

Чтобы восстановить параметры устройства из файла экспорта:

1. В разделе **Настройки** → **UserGate** → **Управление устройством** → **Экспорт и импорт настроек** нажмите **Импорт**.
2. Выберите файл экспорта.
3. В окне **Импортировать настройки** выберите тип импорта (все параметры или только сетевые).
4. Нажмите **Старт**.

Начнется восстановление параметров. По окончании процесса сервер UserGate SIEM будет перезагружен.

Администраторы

Version: 7.x
Product: SIEM
Documentation: 

Доступ к веб-консоли UserGate SIEM регулируется с помощью создания дополнительных учетных записей администраторов, назначения им профилей доступа, создания политики управления паролями администраторов и настройки доступа к веб-консоли на уровне разрешения сервиса в свойствах зоны сети.

Примечание! При первоначальной настройке UserGate SIEM создается локальный суперпользователь Admin.

Для создания дополнительных учетных записей администраторов устройства необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать профиль доступа администратора	В разделе Администраторы → Профили администраторов нажать кнопку Добавить и указать необходимые настройки.
Шаг 2. Создать учетную запись администратора и назначить ей один из созданных ранее профилей администратора	В разделе Администраторы нажать кнопку Добавить и выбрать необходимый вариант: Добавить локального администратора — создать локального пользователя, задать ему пароль доступа и назначить созданный ранее профиль доступа. Добавить пользователя LDAP — добавить пользователя из существующего домена. Для этого должен быть корректно настроен LDAP-коннектор в разделе Серверы аутентификации. При входе в консоль администрирования необходимо указывать имя пользователя в формате user @domain. Назначить созданный ранее профиль. Добавить группу LDAP — добавить группу пользователей из существующего домена. Для этого должен быть корректно настроен LDAP-коннектор в разделе Серверы аутентификации. При входе в консоль администрирования необходимо указывать имя пользователя в формате user @domain. Назначить созданный ранее профиль. Добавить администратора с профилем аутентификации — создать пользователя, назначить созданный ранее профиль администратора и профиль аутентификации (необходимо корректно настроенные серверы аутентификации).

При создании профиля доступа администратора необходимо указать следующие параметры:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Права доступа	Список объектов дерева веб-консоли, доступных для делегирования. В качестве доступа можно указать: - Нет доступа; - Чтение; - Чтение и запись.
Роли пользователей	Определяет роли пользователя для действия над инцидентами и правилами аналитики, назначаемые администраторам данного профиля. По умолчанию в системе определены следующие роли: - Administrator; - Supervisor; - Investigator; - Analyst. Описание разрешений ролей, определенных в системе по умолчанию указано в таблице ниже.

Рольевые разрешения для ролей, созданных в системе по умолчанию:

Рольевое разрешение	Описание	Administrator	Supervisor	Investigator	Analyst
Назначаемый пользователь	Пользователь с этим разрешением может быть назначен на инцидент при создании или редактировании инцидента.		+	+	+
Назначение инцидентов	Возможность назначать пользователей на инциденты при создании или редактировании инцидента.		+	+	+
Закрытие инцидента	Возможность закрыть инцидент.		+	+	+
Создание инцидентов	Возможность создавать инциденты.		+	+	+
Изменение инцидента	Возможность изменять инциденты.		+	+	+
Переоткрытие инцидента	Возможность переоткрывать инциденты.		+	+	+
Редактирование наблюдателей	Возможность добавлять и удалять наблюдателей.		+	+	+
Оставление комментариев	Возможность комментировать инциденты.		+	+	+
Удаление любых комментариев	Возможность удалять любые комментарии к инцидентам.		+		
Удаление собственных комментариев	Возможность удалять собственные комментарии к инцидентам.		+	+	+
Редактирование любых комментариев	Возможность редактировать любые комментарии к инцидентам.		+		
Редактирование своих комментариев	Возможность редактировать свои комментарии к инцидентам.		+	+	+
Создание вложений	Возможность добавлять вложения к инцидентам.		+	+	+
Удаление любых вложений	Возможность удалять любые вложения.		+	+	
Удаление своих вложений	Возможность удалять свои вложения.		+	+	+
Редактирование улик	Возможность создания и редактирования улик.		+	+	+
Обновление обогачений	Возможность обновлять/запрашивать обогачения улик.		+	+	

Рольное разрешение	Описание	Administrator	Supervisor	Investigator	Analyst
Создание отчёта	Возможность создавать, загружать и посылать отчёты инцидентов.		+	+	+
Добавление журналов к инциденту	Возможность добавлять журналы к инциденту.		+	+	+
Удалить все срабатывания/журналы из инцидента	Возможность удаления всех срабатываний/журналов из инцидента.		+	+	
Удаление собственных срабатываний, журналов к инцидентам	Возможность удалять собственные срабатывания/журналы к инцидентам.		+	+	+
Создание схемы инцидента	Возможность создавать схемы инцидентов.		+		
Редактирование схемы инцидента	Возможность редактировать схемы инцидентов.		+		
Удаление схемы инцидента	Возможность удалять схемы инцидентов.		+		
Установка схемы инцидентов по умолчанию	Возможность установки схем инцидентов по умолчанию.		+		
Создание состояния инцидента	Возможность создавать состояния инцидентов.	+	+		
Редактирование состояния инцидента	Возможность редактировать состояния инцидентов.	+	+		
Удаление состояния инцидента	Возможность удалять состояния инцидентов.	+	+		
Создание типа инцидента	Возможность создавать типы инцидентов.	+	+		
Редактирование типа инцидента	Возможность редактировать типы инцидентов.	+	+		
Удаление типа инцидента	Возможность удалять типы инцидентов.	+	+		
Создание решения инцидента	Возможность создавать решения инцидентов.	+	+		
Редактирование решения инцидента	Возможность редактировать решения инцидентов.	+	+		
Удаление решения инцидентов	Возможность удалять решения инцидентов.	+	+		
Создание правила аналитики	Возможность создавать правила аналитики.		+	+	
Удаление правила аналитики	Возможность удалять правила аналитики.		+		
Редактирование правила аналитики	Возможность редактировать правила аналитики.		+	+	
Включение/выключение правила аналитики	Возможность включать/выключать правила аналитики.		+	+	
Запуск правила аналитики	Возможность запустить правило аналитики не в режиме реального времени.		+		
Создание действия реагирования	Возможность создавать действия реагирования.		+	+	
Редактирование действия реагирования	Возможность редактировать действия реагирования.		+	+	
Удаление действия реагирования	Возможность удалять действия реагирования.		+	+	
Включение/выключение действия реагирования	Возможность включать/выключать действия реагирования.		+	+	
Создание сенсора UserGate	Возможность создавать сенсоры UserGate.	+	+		
Редактирование сенсора UserGate	Возможность редактировать сенсоры UserGate.	+	+		
Включение/выключение сенсора UserGate	Возможность включать/выключать сенсоры UserGate.	+	+		
Удаление сенсора UserGate	Возможность удалять сенсоры UserGate.	+	+		
Создание сенсора SNMP	Возможность создавать сенсоры SNMP.	+	+		
Редактирование сенсора SNMP	Возможность редактировать сенсоры SNMP.	+	+		
Включение/выключение сенсора SNMP	Возможность включать/выключать сенсоры SNMP.	+	+		
Удаление сенсора SNMP	Возможность удалять сенсоры SNMP.	+	+		
Создание сенсора WMI	Возможность создавать сенсоры WMI.	+	+		
Редактирование сенсора WMI	Возможность редактировать сенсоры WMI.	+	+		
Включение/выключение сенсора WMI	Возможность включать/выключать сенсоры WMI.	+	+		
Удаление сенсора WMI	Возможность удалять сенсоры WMI.	+	+		
Добавление SNMP MIB файла	Возможность добавлять SNMP MIB файлы.	+	+		
Удаление SNMP MIB файла	Возможность удалять SNMP MIB файлы.	+	+		
Создание коннекторов	Возможность создавать коннекторы.	+	+		

Ролевое разрешение	Описание	Administrator	Supervisor	Investigator	Analyst
Редактирование коннекторов	Возможность редактирования коннекторов.	+	+		
Удаление коннекторов	Возможность удалять коннекторы.	+	+		
Создание правила Syslog	Возможность создавать правила Syslog.	+	+		
Удаление правила Syslog	Возможность удалять правила Syslog.	+	+		
Редактирование правил и коннектора Syslog	Возможность редактировать правила Syslog и настраивать Syslog.	+	+		
Включение/выключение правила Syslog	Возможность включать/выключать правила Syslog.	+	+		
Создание группы email	Возможность создавать почтовые адреса/почтовые группы.	+	+		
Редактирование группы email	Возможность редактировать почтовые адреса/почтовые группы.	+	+		
Удаление группы email	Возможность удалять почтовые адреса/почтовые группы.	+	+		
Создание группы номеров телефонов	Возможность создавать номера телефонов/группы телефонных номеров.	+	+		
Редактирование группы номеров телефонов	Возможность редактировать номера телефонов/группы телефонных номеров.	+	+		
Удаление группы номеров телефонов	Возможность удалять номера телефонов/группы телефонных номеров.	+	+		
Создание команд.	Возможность создавать команды к коннекторам.	+	+		
Редактирование команд.	Возможность редактировать команды к коннекторам.	+	+		
Удаление команд.	Возможность удалять команды к коннекторам.	+	+		
Создание профиля оповещения	Возможность создавать профиль оповещения.	+	+		
Редактирование профиля оповещения	Возможность редактировать профиль оповещения.	+	+		
Удаление профиля оповещения	Возможность редактировать профиль оповещения.	+	+		
Создание категории срабатывания	Возможность создавать категории срабатывания.	+	+		
Редактирование категории срабатывания	Возможность редактировать категории срабатывания.	+	+		
Удаление категории срабатывания	Возможность удалять категории срабатывания.	+	+		
Редактирование настройки обогащения	Возможность редактировать настройки обогащений.	+	+		
Включение/выключение сервиса обогащения	Возможность включать/выключать сервисы обогащений.	+	+		
Создание правила нормализации	Возможность создавать правила нормализации журналов.	+	+		
Редактирование правила нормализации	Возможность редактировать правила нормализации журналов.	+	+		
Удаление правила нормализации	Возможность удалять правила нормализации журналов.	+	+		
Включение/выключение правила нормализации	Возможность включать/выключать правила нормализации журналов.	+	+		

Более подробно о ролевых разрешениях смотрите в разделе [Роли и ролевые разрешения пользователей](#).

Примечание Не следует путать роли и ролевые разрешения с правами доступа на определенные объекты в консоли управления. Права доступа дают возможность просматривать или изменять определенные объекты, например, инциденты, а роли и ролевые разрешения позволяют пользователю производить определенные действия с элементами объектов, например, создать инцидент, назначить ему исполнителя и т.п. Для полноценной работы пользователя в системе, как правило, требуется делегирование ему прав доступа и определенных ролевых разрешений.

Администратор может настроить дополнительные параметры защиты учетных записей администраторов, такие, как сложность пароля и блокировку учетной записи на определенное время при превышении количества неудачных попыток авторизации.

Для настройки этих параметров необходимо:

Наименование	Описание
Шаг 1. Настроить политику паролей	В разделе Администраторы → Администраторы нажать кнопку Настроить .
Шаг 2. Заполнить необходимые поля	Указать значения следующих полей: Сложный пароль — включает дополнительные параметры сложности пароля, задаваемые ниже, такие как — минимальная длина, минимальное число символов в верхнем регистре, минимальное число символов в нижнем регистре, минимальное число цифр, минимальное число специальных символов, максимальная длина блока из одного и того же символа. Число неверных попыток аутентификации — количество неудачных попыток аутентификации администратора, после которых учетная запись заблокируется на Время блокировки. Время блокировки — время, на которое блокируется учетная запись.

ПримечаниеДополнительные параметры защиты учетной записи администратора применимы только к локальным учетным записям. Если в качестве администратора устройства выбирается учетная запись из внешнего каталога (например, LDAP), то параметры защиты для такой учетной записи определяются этим внешним каталогом.

В разделе **Администраторы → Сессии администраторов** отображаются все администраторы, выполнившие вход в веб-консоль администрирования UserGate SIEM. При необходимости любую из сессий администраторов можно закрыть (сбросить).

Администратор может указать зоны, с которых будет возможен доступ к сервису веб-консоли (порт TCP 8010).

ПримечаниеНе рекомендуется разрешать доступ к веб-консоли для зон, подключенных к неконтролируемым сетям, например, к сети Интернет.

Для разрешения сервиса веб-консоли для определенной зоны необходимо в свойствах зоны в разделе контроль доступа разрешить доступ к сервису **Консоль администрирования**. Более подробно о настройке контроля доступа к зонам можно прочитать в разделе [Настройка зон](#).

Управление сертификатами

Version: 7.x
Product: SIEM
Documentation: 

UserGate SIEM использует защищенный протокол HTTPS для управления устройством. Для выполнения данной функции UserGate SIEM использует сертификат типа **SSL веб-консоли**.

Для того чтобы создать новый сертификат, необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать сертификат	Нажать на кнопку Создать в разделе Сертификаты .
Шаг 2. Заполнить необходимые поля	Указать значения следующих полей: • Название — название сертификата, под которым он будет отображен в списке сертификатов. • Описание — описание сертификата. • Страна — страна, в которой выписывается сертификат. • Область или штат — область или штат, в котором выписывается сертификат. • Город — город, в котором выписывается сертификат. • Название организации — название организации, для которой выписывается сертификат. • Common name — имя сертификата. Рекомендуется использовать только символы латинского алфавита для совместимости с большинством браузеров. • E-mail — email вашей компании.
Шаг 3. Указать, для чего будет использован данный сертификат	После создания сертификата необходимо указать его роль в UserGate SIEM. Для этого необходимо выделить необходимый сертификат в списке сертификатов, нажать на кнопку Редактировать и указать тип сертификата — SSL веб-консоли. После этого UserGate SIEM перезагрузит сервис веб-консоли и предложит вам подключиться уже с использованием нового сертификата.

UserGate SIEM позволяет экспортировать созданные сертификаты и импортировать сертификаты, созданные на других системах, например, сертификат, выписанный доверенным удостоверяющим центром вашей организации.

Для экспорта сертификата необходимо:

Наименование	Описание
Шаг 1. Выбрать сертификат для экспорта	Выделить необходимый сертификат в списке сертификатов.
Шаг 2. Экспортировать сертификат	Выбрать тип экспорта: • Экспорт сертификата — экспортирует данные сертификата в der-формате без экспортирования приватного ключа сертификата. Используйте файл, полученный в результате экспорта сертификата для инспектирования SSL, для установки его в качестве локального удостоверяющего центра на компьютеры пользователей. • Экспорт CSR — экспортирует CSR сертификата, например, для подписи его удостоверяющим центром.

ПримечаниеРекомендуется сохранять сертификат для возможности его последующего восстановления.

ПримечаниеВ целях безопасности UserGate SIEM не разрешает экспорт приватных ключей сертификатов.

Для импорта сертификата необходимо иметь файлы сертификата и — опционально — приватного ключа сертификата и выполнить следующие действия:

Наименование	Описание
Шаг 1. Начать импорт	Нажать на кнопку Импорт .
Шаг 2. Заполнить необходимые поля	Указать значения следующих полей: • Название — название сертификата, под которым он будет отображен в списке сертификатов. • Описание — описание сертификата. • Файл сертификата: файл, содержащий данные сертификата. • Приватный ключ: файл, содержащий приватный ключ сертификата. • Пароль для приватного ключа, если таковой требуется. • Цепочка сертификатов — файл, содержащий сертификаты вышестоящих центров сертификации, которые участвовали в создании сертификата (необязательное поле).

Серверы аутентификации

Version: 7.x
Product: SIEM
Documentation: 

Серверы аутентификации — это внешние источники учетных записей пользователей для авторизации в веб-консоли управления UserGate SIEM. Устройство поддерживает следующие серверы аутентификации: LDAP-коннектор, RADIUS и TACACS+.

LDAP-коннектор

LDAP-коннектор позволяет:

- Получать информацию о пользователях и группах Active Directory или других LDAP-серверов. Поддерживается работа с LDAP-сервером FreeIPA.
- Осуществлять авторизацию администраторов UserGate SIEM через домены Active Directory/FreeIPA.

Для создания LDAP-коннектора необходимо нажать на кнопку **Добавить**, выбрать **Добавить LDAP-коннектор** и указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данного сервера аутентификации.
Название	Название сервера аутентификации.
SSL	Определяет, требуется ли SSL-соединение для подключения к LDAP-серверу.
Доменное имя LDAP или IP-адрес	IP-адрес контроллера домена, FQDN контроллера домена или FQDN домена (например, test.local). Если указан FQDN, то UserGate получит адрес контроллера домена с помощью DNS-запроса. Если указан FQDN домена, то при отключении основного контроллера домена, UserGate будет использовать резервный.
Bind DN («login»)	Имя пользователя, которое необходимо использовать для подключения к серверу LDAP. Имя необходимо использовать в формате DOMAIN\username или username @domain. Данный пользователь уже должен быть заведен в домене
Пароль	Пароль пользователя для подключения к домену.
Домены LDAP	Список доменов, которые обслуживаются указанным контроллером домена, например, в случае дерева доменов или леса доменов Active Directory. Здесь же можно указать короткое netbios имя домена.
Пути поиска	Список путей в сервере LDAP, начиная с которых система будет осуществлять поиск пользователей и групп. Необходимо указывать полное имя, например, ou=Office,dc=example,dc=com.

После создания сервера необходимо проверить корректность параметров, нажав на кнопку **Проверить соединение**. Если параметры указаны верно, система сообщит об этом либо укажет на причину невозможности соединения.

Настройка LDAP-коннектора завершена. Для входа в консоль пользователям LDAP необходимо указывать имя в формате:

domain\user/system или user@domain/system

Сервер аутентификации RADIUS

Сервер аутентификации RADIUS позволяет производить авторизацию пользователей в веб-консоли UserGate, который выступает в роли RADIUS-клиента. При авторизации через RADIUS-сервер UserGate посылает на серверы RADIUS информацию с именем и паролем пользователя, а RADIUS-сервер отвечает, успешно прошла аутентификация или нет.

Для добавления сервера аутентификации RADIUS необходимо нажать **Добавить**, выбрать **Добавить RADIUS-сервер** и указать следующие параметры:

Наименование	Описание
Включено	Включение/отключение использования данного сервера аутентификации.
Название	Название сервера аутентификации RADIUS.
Описание	Описание сервера (опционально).
Секрет	Общий ключ, используемый протоколом RADIUS для аутентификации.
Адреса	Указание IP-адреса сервера и UDP-порта, на котором сервер RADIUS слушает запросы на аутентификацию (по умолчанию, 1812).

Для авторизации пользователей в веб-интерфейсе UserGate с помощью сервера RADIUS необходимо настроить профиль аутентификации. Подробнее о создании и настройке профилей читайте в разделе [Профили аутентификации](#).

Сервер аутентификации TACACS+

Сервер TACACS+ позволяет производить авторизацию пользователей в консоли администрирования UserGate. При использовании сервера UserGate передаёт на серверы аутентификации информацию с именем и паролем пользователя, после чего серверы TACACS+ отвечают, успешно прошла аутентификация или нет.

Для добавления сервера аутентификации TACACS+ необходимо нажать **Добавить**, выбрать **Добавить TACACS+ сервер** и указать следующие параметры:

Наименование	Описание
Включено	Включение/отключение использования данного сервера аутентификации.
Название	Название сервера аутентификации TACACS+.
Описание	Описание сервера (опционально).
Секретный ключ	Общий ключ, используемый протоколом TACACS+ для аутентификации.
Адрес	IP-адрес сервера TACACS+.
Порт	UDP-порт, на котором сервер TACACS+ слушает запросы на аутентификацию.
Использовать одно TCP-соединение	Использовать одно TCP-соединение для работы с сервером TACACS+.
Таймаут (сек)	Время ожидания сервера TACACS+ для получения аутентификации. По умолчанию 4 секунды.

Для авторизации пользователей в веб-интерфейсе UserGate с помощью сервера TACACS+ необходимо настроить профиль аутентификации. Подробнее о создании и настройке профилей читайте в разделе [Профили аутентификации](#).

Профили аутентификации

Documentation: ☒
Version: 7.x
Product: SIEM

Профиль позволяет определить набор способов авторизации пользователей в консоли администрирования UserGate SIEM. При создании или настройке профиля достаточно указать:

Наименование	Описание
Название	Название профиля аутентификации.
Описание	Описание профиля (опционально).
Методы аутентификации	Методы аутентификации пользователей, настроенные ранее: LDAP-коннектор, серверы аутентификации RADIUS, TACACS+.

Роли и ролевые разрешения пользователей

Version: 7.x
Product: SIEM
Documentation: 

Роль пользователя — это набор ролевых разрешений. Ролевое разрешение — это возможность администратору совершать определенные действия, например, добавлять или удалять вложение из созданного инцидента, создавать правило срабатывания, создать или закрыть инцидент и т.д. Роли назначаются профилям администраторов, которые присваиваются администраторам. Подробно о создании администраторов и их профилей смотрите в разделе [Администраторы](#).

Чтобы создать роль и назначить ей определенные разрешения необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать роль	В разделе Роли пользователей нажать на кнопку Добавить , дать название и описание создаваемой роли.
Шаг 2. Добавить в созданную роль необходимые разрешения	В разделе Ролевые разрешения выбрать необходимое разрешение и с помощью кнопки Добавить добавить в него созданную ранее роль.

Для пользователей могут быть указаны следующие ролевые разрешения.

Наименование	Описание
Назначаемый пользователь	Пользователь с этим разрешением может быть назначен на инцидент. Ответственный за инцидент может быть указан при создании или редактировании инцидента.
Назначение инцидентов	Возможность назначать пользователей на инциденты. Указать ответственного можно при создании или редактировании инцидента.
Закрытие инцидента	Возможность закрыть инцидент. Часто бывает полезно, когда разработчики разрешают инциденты, а тестировщики закрывают их. Закрыть инцидент можно во вкладке Инциденты → <INC-N:Название инцидента> (где N — порядковый номер инцидента). Закрытие инцидента возможно только из состояний, для которых в схеме инцидента настроен переход в состояние Закрыт. Подробнее читайте в Настройках инцидентов .
Создание инцидентов	Возможность создавать инциденты. Инциденты могут быть созданы во вкладке Инциденты → Журнал инцидентов или автоматически при срабатывании правила аналитики. О создании инцидентов подробнее читайте в разделе Создание инцидентов безопасности .
Изменение инцидента	Возможность изменять инциденты. Редактирование инцидентов доступно во вкладке Инциденты → <INC-N:Название инцидента> (где N — порядковый номер инцидента). Подробнее читайте в разделе Подобности инцидента .
Переоткрытие инцидента	Возможность переоткрывать инциденты. Заново открыть инцидент можно во вкладке Инциденты → <INC-N:Название инцидента> (где N — порядковый номер инцидента).
Редактирование наблюдателей	Возможность добавлять и удалять наблюдателей. Пользователи для наблюдения за инцидентом могут быть указаны при создании или редактировании инцидента.
Оставление комментариев	Возможность комментировать инциденты. Комментирование инцидентов возможно во вкладке Инциденты → <INC-N:Название инцидента> (где N — порядковый номер инцидента) в разделе Активность .
Удаление любых комментариев	Возможность удалять любые комментарии к инцидентам. Комментарии к инциденту можно посмотреть во вкладке Инциденты → <INC-N:Название инцидента> (где N — порядковый номер инцидента) в разделе Активность .
Удаление собственных комментариев	Возможность удалять собственные комментарии к инцидентам. Комментарии к инциденту можно посмотреть во вкладке Инциденты → <INC-N:Название инцидента> (где N — порядковый номер инцидента) в разделе Активность .
Редактирование любых комментариев	Возможность редактировать любые комментарии к инцидентам. Комментарии к инциденту можно посмотреть во вкладке Инциденты → <INC-N:Название инцидента> (где N — порядковый номер инцидента) в разделе Активность .
Редактирование своих комментариев	Возможность редактировать свои комментарии к инцидентам. Комментарии к инциденту можно посмотреть во вкладке Инциденты → <INC-N:Название инцидента> (где N — порядковый номер инцидента) в разделе Активность .
Создание вложений	Возможность добавлять вложения к инцидентам. Вложения к инциденту можно добавить во вкладке Инциденты при создании инцидента или его редактировании. Вложения отображены во вкладке Инциденты → <INC-N:Название инцидента> (где N — порядковый номер инцидента) в разделе Вложения .
Удаление любых вложений	Возможность удалять любые вложения. Вложения к инциденту отображены во вкладке Инциденты → <INC-N:Название инцидента> (где N — порядковый номер инцидента) в разделе Вложения .
Удаление своих вложений	Возможность удалять свои вложения. Вложения к инциденту отображены во вкладке Инциденты → <INC-N:Название инцидента> (где N — порядковый номер инцидента) в разделе Вложения .
Редактирование улик	Возможность создания и редактирования улик. Улики могут быть добавлены во вкладке Инциденты → <INC-N:Название инцидента> (где N — порядковый номер инцидента) в разделе Улики . Подробнее об уликах читайте в разделе Подобности инцидента .
Обновление обогащений	Возможность обновлять/запрашивать обогащения улик. Список внешних сервисов обогащений доступен во вкладке Настройки в разделе Библиотеки → Внешние сервисы обогащений . Подробнее о внешних сервисах обогащений читайте в разделе Внешние сервисы обогащений .
Создание отчёта	Возможность создавать, загружать и посылать отчёты инцидентов. Создание отчётов инцидентов доступно во вкладке Инциденты → INC-N:Название инцидента (где N — порядковый номер инцидента). Подробнее читайте в разделе Подобности инцидента .
Добавление журналов к инциденту	Возможность добавлять журналы к инциденту. Журналы могут быть добавлены во вкладке Инциденты → <INC-N:Название инцидента> (где N — порядковый номер инцидента) в разделе Журналы . Подробнее о журналах читайте в разделе Поиск ; о срабатываниях — в разделе Срабатывания .

[illegible]

[illegible]

Наименование	Описание
Создание команд	Возможность создавать команды к коннекторам. Команды к коннекторам могут быть созданы во вкладке Настройки в разделе Библиотеки → Команды . Подробнее читайте в разделе Команды .
Редактирование команд	Возможность редактировать команды к коннекторам. Команды к коннекторам доступны во вкладке Настройки в разделе Библиотеки → Команды . Подробнее читайте в разделе Команды .
Удаление команд	Возможность удалять команды к коннекторам. Команды к коннекторам доступны во вкладке Настройки в разделе Библиотеки → Команды . Подробнее читайте в разделе Команды .
Создание профиля оповещения	Возможность создавать профиль оповещения. Во вкладке Настройки в разделе Библиотеки → Профили оповещений могут быть созданы два типа профилей: SMPP и SMTP. Подробнее о профилях оповещений читайте в разделе Профили оповещений .
Редактирование профиля оповещения	Возможность редактировать профиль оповещения. Список профилей доступен во вкладке Настройки в разделе Библиотеки → Профили оповещений . Подробнее о профилях оповещений читайте в разделе Профили оповещений .
Удаление профиля оповещения	Возможность редактировать профиль оповещения. Список профилей доступен во вкладке Настройки в разделе Библиотеки → Профили оповещений . Подробнее о профилях оповещений читайте в разделе Профили оповещений .
Создание категории сбрасывания	Возможность создавать категории сбрасывания. Категории сбрасываний могут быть созданы во вкладке Настройки в разделе Библиотеки → Категории сбрасываний . Подробнее о категориях сбрасываний читайте в разделе Категории сбрасываний .
Редактирование категории сбрасывания	Возможность редактировать категории сбрасывания. Список категорий сбрасываний доступен во вкладке Настройки в разделе Библиотеки → Категории сбрасываний . Подробнее о категориях сбрасываний читайте в разделе Категории сбрасываний .
Удаление категории сбрасывания	Возможность удалять категории сбрасывания. Список категорий сбрасываний доступен во вкладке Настройки в разделе Библиотеки → Категории сбрасываний . Подробнее о категориях сбрасываний читайте в разделе Категории сбрасываний .
Редактирование настройки обогащения	Возможность редактировать настройки обогащений. Список внешних сервисов обогащения доступен во вкладке Настройки в разделе Библиотеки → Внешние сервисы обогащений . Подробнее о внешних сервисах обогащений читайте в разделе Внешние сервисы обогащений .
Включение/выключение сервиса обогащения	Возможность включать/выключать сервисы обогащений. Список внешних сервисов обогащения доступен во вкладке Настройки в разделе Библиотеки → Внешние сервисы обогащений . Подробнее о внешних сервисах обогащений читайте в разделе Внешние сервисы обогащений .
Создание правила нормализации	Возможность создавать правила нормализации. Правила нормализации могут быть созданы во вкладке Журналы и отчеты в разделе Журналы → Пользовательская нормализация логов . Подробнее о категориях сбрасываний читайте в разделе Пользовательская нормализация логов .
Редактирование правила нормализации	Возможность редактировать правила нормализации. Правила нормализации доступны во вкладке Журналы и отчеты в разделе Журналы → Пользовательская нормализация логов . Подробнее о категориях сбрасываний читайте в разделе Пользовательская нормализация логов .
Удаление правила нормализации	Возможность удалять правила нормализации. Правила нормализации доступны во вкладке Журналы и отчеты в разделе Журналы → Пользовательская нормализация логов . Подробнее о категориях сбрасываний читайте в разделе Пользовательская нормализация логов .
Включение/выключение правила нормализации	Возможность включать/выключать правила нормализации. Правила нормализации доступны во вкладке Журналы и отчеты в разделе Журналы → Пользовательская нормализация логов . Подробнее о категориях сбрасываний читайте в разделе Пользовательская нормализация логов .

После создания роли, она может быть использована для назначения в профили администраторов.

Каталоги пользователей

Version: 7.x
Product: SIEM
Documentation: 

В разделе **Каталоги пользователей** можно добавить LDAP-коннектор для организации доступа серверов UserGate SIEM к серверу AD. Доступ к AD позволяет при необходимости обновить информацию об имени пользователя в журналах, импортированных из различных сенсоров.

Для создания LDAP-коннектора необходимо нажать на кнопку **Добавить** и указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данного LDAP-коннектора.
Название	Название LDAP-коннектора.
Описание	Описание LDAP-коннектора.
SSL	Определяет, требуется ли SSL-соединение для подключения к LDAP-серверу.
Доменное имя LDAP или IP-адрес	IP-адрес контроллера домена, FQDN контроллера домена или FQDN домена (например, test.local). Если указан FQDN, то UserGate получит адрес контроллера домена с помощью DNS-запроса. Если указан FQDN домена, то при отключении основного контроллера домена, UserGate будет использовать резервный.
Bind DN («login»)	Имя пользователя, которое необходимо использовать для подключения к серверу LDAP. Имя необходимо использовать в формате DOMAIN\username или username @domain. Данный пользователь уже должен быть заведен в домене.
Пароль	Пароль пользователя для подключения к домену.
Домены LDAP	Список доменов, которые обслуживаются указанным контроллером домена, например, в случае дерева доменов или леса доменов Active Directory.
Пути поиска	Список путей на сервере LDAP, начиная с которых система будет осуществлять поиск пользователей и групп. Необходимо указывать полное имя, например, ou=Office,dc=example,dc=com.

После заполнения параметров LDAP-коннектора можно проверить корректность конфигурации, нажав на кнопку **Проверить соединение**. Если параметры указаны верно, система сообщит об этом либо укажет на причину невозможности соединения.

Расширение системного раздела

Version: 7.x
Product: SIEM
Documentation: 

Для расширения системного раздела с сохранением конфигурации и данных узла UserGate SIEM необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Добавить дополнительный виртуальный диск.	Средствами гипервизора добавить новый диск необходимого размера в свойствах виртуальной машины UserGate SIEM.
Шаг 2. Расширить размер раздела в системных утилитах.	В меню загрузки узла UserGate SIEM войти в раздел Support menu . В открывшемся разделе выбрать Expand data partition и запустить процесс расширения раздела.
Шаг 3. Проверить размер системного раздела.	После завершения процесса расширения загрузить узел и в разделе Дашборд → Диски проверить размер системного раздела.

Примечание Расширение системного раздела путем увеличения размера имеющегося диска виртуальной машины возможно только при сбросе узла до заводских настроек, т. е. при выполнении операции factory reset.

Technology: Clustering and HA
Version: 7.x
Product: SIEM
Documentation: 

Общие принципы

Для построения отказоустойчивого решения UserGate SIEM необходимо настроить два типа кластеров — кластер конфигурации и кластер отказоустойчивости.

Кластер конфигурации — это объединение нескольких узлов в одну общую схему. Входящие в кластер конфигурации узлы «видят» друг друга и синхронизируют свою конфигурацию. При этом часть настроек для каждого из узлов кластера уникальна, например, настройки сетевых интерфейсов, шлюзов, маршрутов, настройки диагностики.

Кластер отказоустойчивости обеспечивает работу сетевых операций на узлах, входящих в кластер конфигурации, например, переключаемый виртуальный IP, который по определённым правилам мигрирует с одного узла на другой.

Кластер отказоустойчивости и кластер конфигурации работают на разных протоколах и в разных окружениях. При этом информация о статусе кластера отказоустойчивости распространяется между узлами через кластер конфигурации. Речь идёт именно об информации о статусе, а не о данных, которыми кластер отказоустойчивости поддерживает свою работу. Статус узлов кластера отображается в веб-консоли.

Минимальный состав отказоустойчивого решения UserGate SIEM состоит из двух узлов UserGate SIEM и узла-арбитра.

Максимальное количество узлов в кластере — 4, один из которых является арбитром.

Узел-арбитр предназначен для определения кворума в конфигурации для обеспечения консистентности данных. Он не несёт в себе функции полноценного UserGate SIEM (сбор, хранение, обработка данных), но участвует в процедуре определения большинства согласно алгоритму распределённого консенсуса для согласования операций в отказоустойчивом кластере.

На данном этапе отказоустойчивым кластером UserGate SIEM поддерживается режим работы **Актив-Пассив**. В режиме Актив-Пассив один из узлов выступает в роли мастер-узла, обрабатывающего трафик, а другой — в качестве резервного. Для кластера указывается один или более виртуальных IP-адресов. Переключение виртуальных адресов с главного на один из запасных узлов происходит при следующих событиях:

- Запасной узел не получает подтверждения о том, что главный узел в сети, например, если он выключен или отсутствует сетевая доступность узлов.
- Изменение приоритета мастер-узла. Например, приоритет мастер-узла уменьшается при отключении одного или нескольких сетевых интерфейсов, на которых назначены виртуальные IP-адреса. Также приоритет узла может быть изменен явным образом через смену мастера в веб-консоли устройства.
- Сбой в работе ПО.

Создание отказоустойчивого кластера UserGate SIEM

Для создания отказоустойчивого кластера UserGate SIEM необходимо сначала настроить кластер конфигурации, объединив в него необходимые узлы, затем настроить кластер отказоустойчивости.

Настройка кластера конфигурации

Для создания кластера конфигурации необходимо выполнить следующие шаги:

- Выполнить первоначальную настройку на первом узле. Подробнее читайте в главе [Первоначальная настройка](#).
- Настроить на первом узле зону, через интерфейс которой будет выполняться репликация кластера.

В разделе **Зоны** создать выделенную зону для репликации настроек кластера. В настройках доступа зоны разрешить следующие сервисы:

- Консоль администрирования
- Кластер

Важно! Не следует использовать для репликации зоны, интерфейс которых подключены к недоверенным сетям, например, к интернету.

- В разделе **Кластер конфигурации** указать IP-адрес, который будет использоваться для связи с другими узлами кластера.

- Сгенерировать секретный код на первом узле, нажав одноимённую кнопку в разделе **Кластер конфигурации**. Полученный код скопировать в буфер обмена. Данный секретный код необходим для одноразовой авторизации следующего узла при добавлении его в кластер.

- Подключить второй узел в кластер.

В процессе первоначальной установки второго узла подключиться к его веб-консоли, выбрать язык установки.

Указать интерфейс, который будет использован для подключения к первому узлу кластера и назначить ему IP-адрес. Оба узла кластера должны находиться в одной подсети. В противном случае необходимо указать IP-адрес шлюза, через который будет доступен первый узел кластера.

Указать IP-адрес первого узла, настроенный на шаге 3, вставить секретный код и нажать на кнопку **Подключить**:

Если IP-адреса кластера, настроенные на шаге 2, назначены корректно, то второй узел будет добавлен в кластер и настройки первого узла кластера реплицируются на второй.

Состояние узлов кластера конфигурации отображается в разделе **Кластер конфигурации**:

6. Назначить зоны интерфейсам второго узла. В веб-консоли второго узла кластера в разделе **Сеть → Интерфейсы** необходимо назначить каждому интерфейсу корректную зону. Зоны и их настройки получены в результате репликации данных с первого узла кластера.

7. Подключить в кластер узел, который будет в дальнейшем исполнять роль арбитра.

Сгенерировать секретный код на первом узле, нажав одноимённую кнопку в разделе **Кластер конфигурации**. Полученный код скопировать в буфер обмена. Данный код необходим для одноразовой авторизации нового узла при добавлении его в кластер.

В процессе первоначальной установки третьего узла подключиться к его веб-консоли, выбрать язык установки.

Указать интерфейс, который будет использован для подключения к первому узлу кластера и назначить ему IP-адрес. Оба узла кластера должны находиться в одной подсети. В противном случае необходимо указать IP-адрес шлюза, через который будет доступен первый узел кластера. Поставить флажок **Перевести ноду в режим арбитра**.

Указать IP-адрес первого узла, настроенный на шаге 3, вставить секретный код и нажать на кнопку **Подключить**:

Если IP-адреса кластера, настроенные на шаге 2, назначены корректно, то второй узел будет добавлен в кластер и настройки первого узла кластера реплицируются на новый узел.

Состояние узлов кластера конфигурации отображается в разделе **Кластер конфигурации**. Узел-арбитр помечается в списке узлов кластера соответствующей иконкой:

8. Настроить параметры, индивидуальные для каждого узла кластера (опционально). Настроить шлюзы, маршруты, параметры OSPF, BGP, индивидуальные для каждого из узлов.

Настройка кластера отказоустойчивости

Узлы кластера конфигурации можно объединить в отказоустойчивый кластер. В настоящий момент поддерживается режим кластера отказоустойчивости **Актив-Пассив**.

В режиме Актив-Пассив один из узлов UserGate SIEM выступает в роли мастер-узла, принимающего трафик, а другой — в качестве резервного. На каждом из узлов кластера выбираются сетевые интерфейсы, у которых обязательно должны быть определены IP-адреса.

Администратор назначает виртуальные IP-адреса. Между этими интерфейсами передаются VRRP-объявления (ADVERTISEMENT) — сообщения, с помощью которых узлы обмениваются информацией о своём состоянии.

Для создания кластера отказоустойчивости необходимо в разделе **Кластеры отказоустойчивости** нажать иконку "+" :

В открывшемся окне свойств кластера отказоустойчивости произвести следующие настройки:

На вкладке **Общие**:

- Указать название кластера отказоустойчивости.
- Задать значение идентификатора виртуального маршрутизатора. VRID должен быть уникален для каждого VRRP-кластера в локальной сети.
- Поставить флажок **Включено** для активации кластера.

На вкладке **Узлы** выбрать узлы кластера конфигурации, которые войдут в создаваемый кластер отказоустойчивости.

На вкладке **Виртуальные IP** указать виртуальный IP-адрес и маску сети кластера отказоустойчивости, выбрать основные узлы и порты, на которых будет работать VRRP.

Отображение состояния кластера отказоустойчивости

Состояние и роль входящих в кластер узлов можно увидеть в разделе **Кластеры отказоустойчивости**. Роли узлов отмечены соответствующими иконками: звёздочкой отмечен активный мастер-узел, свистком — узел-арбитр.

При успешном создании кластера его состояние отображается следующим образом:

В случае недоступности мастер-узла кластера его роль перейдёт к резервному узлу. В веб-консоли второго узла поменяется статус состояния кластера и недоступного узла. При наведении на иконку статуса кластера указателя мыши отображается подсказка о причине изменения состояния кластера:

В журнале событий отобразится соответствующая запись:

В случае неконсистентного состояния кластера отказоустойчивости его статус помечается соответствующей иконкой. При наведении на иконку указателя мыши отображается подсказка о причине данного состояния кластера:

Настройка сетевых зон

Documentation: ☒
Product: SIEM
Version: 7.x

Под сетевой зоной в UserGate SIEM понимается логическое объединение сетевых интерфейсов. Рекомендуется объединять интерфейсы в зоне на основе их функционального назначения, например можно создать зону для локальной сети (LAN) или зону интерфейсов управления (Management).

По умолчанию в UserGate SIEM предусмотрены следующие сетевые зоны:

- **Management** — для доверенных сетей, из которых разрешено администрирование устройства.
- **Trusted** — для внутренних доверенных сегментов сети (например, LAN). Вы можете использовать эту зону для подключения к устройству сенсоров UserGate, а также для доступа в интернет.

Вы можете изменять параметры этих сетевых зон, а также [добавлять новые зоны](#) (не больше 255 зон). Кроме того, вы можете управлять доступом к сервисам устройства для подключенных к зоне клиентов.

В свойствах зоны можно управлять доступом к следующим сервисам UserGate SIEM.

Сервис	Назначение
Ping	Проверка доступности UserGate SIEM с помощью утилиты ping
SNMP	Доступ к UserGate SIEM по SNMP-протоколу (порт UDP 161)
Консоль администрирования	Доступ к веб-консоли UserGate SIEM (порт TCP 8010)
API XML RPC поверх HTTP	Доступ к API UserGate SIEM по протоколу HTTP (порт TCP 4041)
API XML RPC поверх HTTPS (доступен начиная с версии 7.4.0)	Доступ к API UserGate SIEM по протоколу HTTPS (порт TCP 4443)
Кластер	Объединение нескольких узлов UserGate SIEM в кластер конфигурации
VRRP	Объединение нескольких узлов UserGate SIEM в кластер отказоустойчивости
CLI по SSH	Доступ к интерфейсу командной строки UserGate SIEM (порт TCP 2200)
База данных журналов	Интеграция UserGate SIEM с сенсорами UserGate . Исходящие подключения — порты TCP 9713 и TCP 2023. Входящие подключения — порт TCP 22711 либо порт 22699 (для сенсоров UserGate с ПО версии 6.1.9 и ниже)
Сборщик логов	Получение событий от syslog-источников (по умолчанию — порт TCP 514)

Для работы сервисов необходимо разрешить соответствующие порты и протоколы в сетевой инфраструктуре организации. Подробнее — в разделе « [Требования к сетевому окружению](#) ».

Вы также можете включать защиту от DoS-атак и защиту от IP-спуфинга для каждой зоны. Кроме того, в свойствах зоны вы можете ограничить количество активных сессий для одного IP-адреса. Это позволит снизить нагрузку на инфраструктуру организации при DDoS-атаках, предотвратить злоупотребление ресурсами и обеспечить их доступность для всех пользователей.

Чтобы добавить сетевую зону:

1. В разделе **Настройки** → **Сеть** → **Зоны** нажмите **Добавить**.
2. На вкладке **Общие** выполните следующие действия:
 - Укажите название и при необходимости описание зоны.
 - При необходимости укажите параметры защиты сетевой зоны от DoS-атак для протоколов TCP (SYN-флуд), UDP, ICMP соответственно:
 - Установите флажок **Включено** для включения защиты.
 - При необходимости установите флажок **Агрегировать** для суммарного подсчета всех входящих пакетов. Если флажок не установлен, пакеты учитываются отдельно для каждого IP-адреса.
 - В поле **Порог уведомления** укажите количество запросов с одного IP-адреса, при превышении которого в системном журнале будет сгенерирована запись о событии.
Рекомендованное значение — 3000 пакетов/сек.
 - В поле **Порог отбрасывания пакетов** укажите количество запросов с одного IP-адреса, при превышении которого будут отброшены пакеты, поступившие с этого IP-адреса, с регистрацией события в системном журнале.
Рекомендованное значение — 6000 пакетов/сек. Для протокола UDP необходимо увеличить это значение, если через интерфейсы зоны проходит трафик таких сервисов, как IP-телефония или L2TP VPN.
 - При необходимости в блоке параметров **Исключения защиты от DoS** добавьте IP-адреса узлов, к которым не следует применять ограничения. Это может понадобиться, например, для серверов IP-телефонии, генерирующих интенсивный поток UDP-пакетов.
 - **Примечание**Рекомендуется включать защиту от DoS-атак для каждой сетевой зоны.
3. При необходимости на вкладке **Контроль доступа** укажите сервисы, которые будут доступны подключенным к зоне клиентам.
Важно!Не рекомендуется разрешать доступ к сервисам для зон, подключенных к недоверенным сетям (например, к интернету).
ПримечаниеВы можете дополнительно ограничить доступ к каждому сервису, указав разрешенные диапазоны IP-адресов или географические регионы (GeoIP).
4. При необходимости на вкладке **Защита от IP-спуфинга** включите защиту и укажите для зоны разрешенные диапазоны IP-адресов или географические регионы (GeoIP). Сетевые пакеты, поступающие с IP-адресов, не входящих в разрешенный список, будут отброшены.
При включении инвертирования (соответствует логическому отрицанию) указанные диапазоны IP-адресов будут запрещены для сетевой зоны.
ПримечаниеНапример, можно указать диапазоны «серых» IP-адресов (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) и установить флажок «Инвертировать».
5. При необходимости на вкладке **Ограничение сессий** включите ограничение и укажите максимальное количество активных сессий для одного IP-адреса.
ПримечаниеВ блоке параметров «Исключения» вы можете добавить список IP-адресов, для которых ограничение не будет действовать.
6. Нажмите **Сохранить**.

Настройка интерфейсов

Documentation: ☒
Product: SIEM
Version: 7.x

Раздел **Интерфейсы** отображает все физические и виртуальные интерфейсы, имеющиеся в системе, позволяет менять их настройки и добавлять VLAN и бонд-интерфейсы.

ПримечаниеДля работы UserGate SIEM достаточно одного настроенного интерфейса. Разделение функций управления устройством и сбора данных на разные сетевые интерфейсы рекомендовано для обеспечения безопасности, но не является жестким требованием.

Кнопка **Редактировать** позволяет изменять параметры сетевого интерфейса:

- Включить или отключить интерфейс.
- Указать тип интерфейса — Layer 3.
- Назначить зону интерфейсу.
- Изменить физические параметры интерфейса — MAC-адрес, размер MTU, размер MSS.
- Выбрать тип присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP.

Кнопка **Добавить** позволяет добавить следующие типы логических интерфейсов:

- VLAN.
- Бонд.

Создание интерфейса VLAN

С помощью кнопки **Добавить VLAN** администратор может создавать сабинтерфейсы. При создании VLAN необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает VLAN.
Название	Название VLAN. Название присваивается автоматически на основе имени физического порта и тега VLAN.
Описание	Опциональное описание интерфейса.
Тип интерфейса	Указать тип интерфейса — Layer 3 или Mirror.
Тег VLAN	Номер сабинтерфейса. Допускается создание до 4094 интерфейсов.
Имя узла	Имя узла в кластере, на котором создается данный VLAN.
Интерфейс	Физический интерфейс, на котором создается VLAN.
Зона	Зона, которой принадлежит VLAN.
Алиас/Псевдоним	Альтернативное имя интерфейса, заданное администратором. Параметр является опциональным и используется для работы с SNMP. Значение параметра — строка длиной не более 64-х символов. Важно! Значение параметра не может содержать символы кириллицы.
Сеть	Способ присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Возможность изменить MAC-адрес, размер MTU, размер MSS (доступно в версии ПО 7.3.0 и выше).

Объединение интерфейсов в бонд

С помощью кнопки **Добавить бонд-интерфейс** администратор может объединить несколько физических интерфейсов в один логический агрегированный интерфейс для повышения пропускной способности или для отказоустойчивости канала. При создании бонда необходимо указать следующие параметры:

Наименование	Описание
Вкл	Включает бонд.
Название	Название бонда.
Зона	Зона, к которой принадлежит бонд.
Интерфейсы	Один или более интерфейсов, которые будут использованы для построения бонда.
Режим	Режим работы бонда должен совпадать с режимом работы на том устройстве, куда подключается бонд. Может быть: • Round robin. Пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. Эта политика применяется для балансировки нагрузки и отказоустойчивости. • Active backup. Только один сетевой интерфейс из объединенных будет активным. Другой интерфейс может стать активным только в том случае, когда упадет текущий активный интерфейс. При такой политике MAC-адрес бонд-интерфейса виден снаружи только через один сетевой порт, во избежание появления проблем с коммутатором. Эта политика применяется для отказоустойчивости. • XOR. Передача распределяется между сетевыми картами используя формулу: [(«MAC-адрес источника» XOR «MAC-адрес назначения») по модулю «число интерфейсов»]. Получается, одна и та же сетевая карта передает пакеты одним и тем же получателям. Опционально распределение передачи может быть основано и на политике «xmit_hash». Политика XOR применяется для балансировки нагрузки и отказоустойчивости. • Broadcast. Передает все на все сетевые интерфейсы. Эта политика применяется для отказоустойчивости. • IEEE 802.3ad — режим работы, установленный по умолчанию, поддерживается большинством сетевых коммутаторов. Создаются агрегированные группы сетевых карт с одинаковой скоростью и дуплексом. При таком объединении передача задействует все каналы в активной агрегации согласно стандарту IEEE 802.3ad. Выбор, через какой интерфейс отправлять пакет, определяется политикой; по умолчанию используется XOR-политика, можно также использовать «xmit_hash» политику. • Adaptive transmit load balancing. Исходящий трафик распределяется в зависимости от загрузки каждой сетевой карты (определяется скоростью загрузки). Не требует дополнительной настройки на коммутаторе. Входящий трафик приходит на текущую сетевую карту. Если она выходит из строя, то другая сетевая карта берет себе MAC-адрес вышедшей из строя карты. • Adaptive load balancing. Включает в себя предыдущую политику плюс осуществляет балансировку входящего трафика. Не требует дополнительной настройки на коммутаторе. Балансировка входящего трафика достигается путем ARP-переговоров. Драйвер перехватывает ARP-ответы, отправляемые с локальных сетевых карт наружу, и переписывает MAC-адрес источника на один из уникальных MAC-адресов сетевой карты, участвующей в объединении. Таким образом, различные пиры используют различные MAC-адреса сервера. Балансировка входящего трафика распределяется последовательно (round-robin) между интерфейсами.
MII monitoring period (мсек)	Устанавливает периодичность MII-мониторинга в миллисекундах. Определяет, как часто будет проверяться состояние линии на наличие отказов. Значение по умолчанию — 0 — отключает MII-мониторинг.
Down delay (мсек)	Определяет время (в миллисекундах) задержки перед отключением интерфейса, если произошел сбой соединения. Эта опция действительна только для мониторинга MII (miimon). Значение параметра должно быть кратным значениям miimon. Если оно не кратно, то округлится до ближайшего кратного значения. Значение по умолчанию 0.
Up delay (мсек)	Задает время задержки в миллисекундах, перед тем как поднять канал при обнаружении его восстановления. Этот параметр возможен только при MII-мониторинге (miimon). Значение параметра должно быть кратным значениям miimon. Если оно не кратно, то округлится до ближайшего кратного значения. Значение по умолчанию 0.

Наименование	Описание
LACP rate	Определяет, с каким интервалом будут передаваться партнером LACPDU-пакеты в режиме 802.3ad. Возможные значения: • Slow — запрос партнера на передачу LACPDU-пакетов каждые 30 секунд. • Fast — запрос партнера на передачу LACPDU-пакетов каждую 1 секунду.
Failover MAC	Определяет, как будут прописываться MAC-адреса на объединенных интерфейсах в режиме active-backup при переключении интерфейсов. Обычным поведением является одинаковый MAC-адрес на всех интерфейсах. Возможные значения: • Отключено — устанавливает одинаковый MAC-адрес на всех интерфейсах во время переключения. • Active — MAC-адрес на бонд-интерфейсе будет всегда таким же, как на текущем активном интерфейсе. MAC-адреса на резервных интерфейсах не изменяются. MAC-адрес на бонд-интерфейсе меняется во время обработки отказа. • Follow — MAC-адрес на бонд-интерфейсе будет таким же, как на первом интерфейсе, добавленном в объединение. На втором и последующем интерфейсе этот MAC не устанавливается, пока они в резервном режиме. MAC-адрес прописывается во время обработки отказа, когда резервный интерфейс становится активным, он принимает новый MAC (тот, что на бонд-интерфейсе), а старому активному интерфейсу прописывается MAC, который был на текущем активном.
Xmit hash policy	Определяет хэш-политику передачи пакетов через объединенные интерфейсы в режиме XOR или IEEE 802.3ad. Возможные значения: • Layer 2 — использует только MAC-адреса для генерации хэша. При этом алгоритме трафик для конкретного сетевого хоста будет отправляться всегда через один и тот же интерфейс. Алгоритм совместим с IEEE 802.3ad. • Layer 2+3 — использует как MAC-адреса, так и IP-адреса для генерации хэша. Алгоритм совместим с IEEE 802.3ad. • Layer 3+4 — используются IP-адреса и протоколы транспортного уровня (TCP или UDP) для генерации хэша. Алгоритм не всегда совместим с IEEE 802.3ad, так как в пределах одного и того же TCP- или UDP-взаимодействия могут передаваться как фрагментированные, так и нефрагментированные пакеты. Во фрагментированных пакетах порт источника и порт назначения отсутствуют. В результате в рамках одной сессии пакеты могут дойти до получателя не в том порядке, так как отправляются через разные интерфейсы.
Сеть	Способ присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Возможность изменить MAC-адрес, размер MTU, размер MSS (доступно в версии ПО 7.3.0 и выше).

Настройка шлюзов

Documentation: 
Product: SIEM
Version: 7.x

Для подключения UserGate SIEM к интернету необходимо указать IP-адрес одного или нескольких шлюзов.

Можно указать несколько шлюзов, если для подключения к интернету используется несколько провайдеров. Пример настройки сети с двумя провайдерами:

- Интерфейс port1 с IP-адресом 192.168.11.2 подключен к интернет-провайдеру 1. Для выхода в Интернет с этого провайдера необходимо добавить шлюз с IP-адресом 192.168.11.1
- Интерфейс port2 с IP-адресом 192.168.12.2 подключен к интернет-провайдеру 2. Для выхода в Интернет с этого провайдера необходимо добавить шлюз с IP-адресом 192.168.12.1

При наличии двух или более шлюзов возможны 2 варианта работы:

Наименование	Описание
Балансировка трафика между шлюзами	Установить флажок Балансировка и указать Вес каждого шлюза. В этом случае весь трафик в интернет будет распределен между шлюзами в соответствии с указанными весами (чем больше вес, тем большая доля трафика идет через шлюз).
Основной шлюз с переключением на запасной	Выбрать один из шлюзов в качестве основного и настроить Проверку сети , нажав на одноименную кнопку в интерфейсе. Проверка сети проверяет доступность хоста в интернет с указанной в настройках периодичностью, и в случае, если хост перестает быть доступен, переводит весь трафик на запасные шлюзы в порядке их расположения в консоли.

По умолчанию проверка доступности сети настроена на работу с публичным DNS-сервером Google (8.8.8.8), но может быть изменена на любой другой хост по желанию администратора.

Маршруты

Documentation: ☒
Product: SIEM
Version: 7.x

Данный раздел позволяет указать маршрут в сеть, доступную за определенным маршрутизатором. Например, в локальной сети может быть маршрутизатор, который объединяет несколько IP-подсетей.

Для добавления маршрута необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Задать название и описание данного маршрута	В разделе Сеть выберите в меню Маршруты , нажмите кнопку Добавить . Укажите имя для данного маршрута. Опционально можно задать описание маршрута.
Шаг 2. Указать адрес назначения	Задайте подсеть, куда будет указывать маршрут, например, 172.16.20.0/24 или 172.16.20.5/32.
Шаг 3. Указать шлюз	Задайте IP-адрес шлюза, через который указанная подсеть будет доступна. Этот IP-адрес должен быть доступен с сервера UserGate SIEM.
Шаг 4. Указать интерфейс	Выберите интерфейс, через который будет добавлен маршрут. Если оставить значение Автоматически , UserGate SIEM сам определит интерфейс, исходя из настроек IP-адресации сетевых интерфейсов.
Шаг 5. Указать метрику	Задайте метрику маршрута. Чем меньше метрика, тем приоритетней маршрут в данную сеть, если маршрутов несколько.

Общие сведения

Documentation: ☒
Version: 7.x
Product: SIEM

Для сбора информации с различных устройств и последующего ее анализа UserGate SIEM использует сенсоры. Сенсор — это совместимое с UserGate SIEM устройство, которое может передавать определенные данные на UserGate SIEM. Сенсорами могут выступать UserGate NGFW, конечные устройства UserGate Client, компьютеры под управлением ОС Windows, а также любые другие сетевые устройства, способные передавать данные по протоколу SNMP.

Сенсоры UserGate

Version: 7.x
Product: SIEM
Documentation: 

Вы можете настраивать интеграцию UserGate SIEM с межсетевыми экранами UserGate NGFW (далее также — сенсоры UserGate). Для подключенных сенсоров это позволяет использовать UserGate SIEM в качестве базы данных журналов, в которой выполняется их хранение, последующая обработка и анализ.

При первоначальном сетевом взаимодействии UserGate SIEM обменивается с сенсорами UserGate ключами шифрования и устанавливает канал управления (порты TCP 9713 и TCP 2023). Далее сенсоры передают данные журналов на сервер UserGate SIEM (порт TCP 22711) и данные о своем состоянии по протоколу SNMP (порт UDP 161). Для SNMP-мониторинга на каждом сенсоре UserGate автоматически создается соответствующее правило. Подробная информация о сетевом взаимодействии устройств приведена в разделе «[Требования к сетевому окружению](#)».

В разделе **Настройки** → **Сенсоры** → **Сенсоры UserGate** вы можете [управлять подключенными сенсорами UserGate](#), а также отслеживать состояние этих устройств (например, объем используемой памяти и время непрерывной работы). Кроме того, в разделе **Дашборды** вы можете добавлять виджеты сенсоров UserGate и просматривать на них информацию о состоянии устройств в графическом представлении.

Данные о событиях, полученные от сенсоров UserGate, отображаются в разделе **Журналы и отчеты** в виде записей [в соответствующих журналах](#). Вы можете управлять этими данными: фильтровать их, скачивать в CSV-формате, а также экспортировать на внешние серверы и создавать сводные отчеты. Кроме того, в разделе **Аналитика** доступен [анализ данных](#).

Настройка интеграции с UserGate NGFW

Для настройки интеграции UserGate SIEM с UserGate NGFW необходимо:

- В веб-консоли UserGate NGFW в свойствах зоны для подключения UserGate SIEM разрешить использование сервисов **Log Analyzer/SIEM** и **SNMP**. Подробнее — в Руководстве администратора UserGate NGFW в разделе «Настройка зон».
- В веб-консоли UserGate NGFW [получить уникальный код устройства](#) и передать его администратору UserGate SIEM.
- В веб-консоли UserGate SIEM [в свойствах зоны](#) для подключения UserGate NGFW разрешить использование сервиса **База данных журналов**.
- [Подключить UserGate NGFW к UserGate SIEM в качестве сенсора](#).

Получение кода устройства UserGate NGFW

ПримечаниеИнструкция ниже выполняется в веб-консоли UserGate NGFW.

Чтобы получить код устройства:

В разделе **Настройки** → **Консоль администратора** → **Настройки** в блоке **Состояние базы данных журналов** → **Код устройства** нажмите **Показать**.

Полученный код необходимо скопировать в буфер обмена и передать его администратору UserGate SIEM.

Подключение UserGate NGFW в качестве сенсора

ПримечаниеИнструкция ниже выполняется в веб-консоли UserGate SIEM.

Чтобы подключить UserGate NGFW к UserGate SIEM в качестве сенсора:

- В разделе **Настройки** → **Сенсоры** → **Сенсоры UserGate** нажмите **Добавить**.
- В окне свойств сенсора выполните следующие действия:
 - установите флажок **Включено** для активации соединения с сервером UserGate NGFW;
 - укажите название и при необходимости описание сенсора;
 - укажите IP-адрес или доменное имя сервера UserGate NGFW (например, 198.51.100.22);
 - в поле **SIEM адрес** выберите IP-адрес UserGate SIEM;
 - укажите код устройства, полученный от администратора UserGate NGFW.
- Нажмите **Сохранить**.

Подключенный сенсор отобразится в таблице **Сенсоры UserGate**.

Управление сенсорами UserGate

В разделе **Настройки** → **Сенсоры** → **Сенсоры UserGate** отображается список устройств UserGate NGFW, подключенных к UserGate SIEM в качестве сенсоров.

В таблице вы можете отслеживать статус подключения каждого сенсора к UserGate SIEM с помощью следующих цветовых индикаторов:

- Зеленый — соединение между серверами сенсора UserGate и UserGate SIEM установлено.
- Красный — соединение между серверами сенсора UserGate и UserGate SIEM не установлено, сенсор отключен или недоступен.

Вы можете управлять подключенными сенсорами:

- Включать и отключать сенсоры от UserGate SIEM по кнопкам **Включить** и **Отключить** соответственно.

ПримечаниеПри выборе нескольких сенсоров в таблице с помощью клавиши Ctrl или Shift доступно их одновременное включение или отключение.

- Удалять сенсор по кнопке **Удалить**.
- Изменять параметры сенсора по кнопке **Редактировать**.

При редактировании в окне свойств сенсора доступна кнопка **Перенастроить**, по нажатию которой выполняется переподключение сенсора к UserGate SIEM. Это может понадобиться, например, при изменении IP-адреса или кода устройства UserGate.

Кроме того, вы можете настраивать отображение сенсоров в таблице с помощью следующих фильтров:

- Все** — все сенсоры (фильтр по умолчанию).
- Включенные** и **Выключенные** — сенсоры в выбранном состоянии.
- Онлайн** — сенсоры, для которых установлено соединение с сервером UserGate SIEM.
- Офлайн** — сенсоры, для которых не установлено соединение с сервером UserGate SIEM.

По умолчанию для сенсора в таблице отображаются следующие данные:

- название;
- IP-адрес или доменное имя;
- название и модель устройства;
- версия ПО;
- информация о лицензии;
- время непрерывной работы;
- параметры мониторинга состояния сенсора, включая объем используемой оперативной памяти и загрузженность центрального процессора.

Сенсоры SNMP

Version: 7.x
Product: SIEM
Documentation: 

С помощью сенсора SNMP администратор может подключить SNMP-совместимое сетевое устройство к серверу UserGate SIEM для сбора и анализа его метрик. UserGate SIEM может отображать любые счетчики, полученные по SNMP с помощью запросов SNMP. Для настройки сенсора SNMP необходимо иметь базы MIB (Management Information Base) на управляемое устройство. Подробнее об управлении базами MIB смотрите раздел данного руководства [Управление SNMP MIB](#).

Для настройки сенсора SNMP необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Загрузите базу MIB того устройства, которое хотите добавить для мониторинга.	На сервере UserGate SIEM в разделе Сенсоры → Управление SNMP MIB загрузите файл с MIB.
Шаг 2. Создайте сенсор SNMP	На сервере UserGate SIEM в разделе Сенсоры → Сенсоры SNMP нажмите кнопку Добавить и заполните необходимые поля.

При создании сенсора SNMP необходимо заполнить следующие поля:

Наименование	Описание
Включено	Включает или выключает данный сенсор SNMP.
Название	Название сенсора SNMP.
Описание	Опциональное описание сенсора SNMP.
Адрес сервера	IP-адрес сенсора SNMP.
Порт	Порт сенсора SNMP. Обычно для запросов данных по протоколу SNMP используется порт TCP 161.
Версия	Указывает версию протокола SNMP, которая будет использоваться в данном сенсоре. Возможны варианты SNMP v2 и SNMP v3.
Community	SNMP community — строка для идентификации сервера UserGate SIEM и сетевого устройства для версии SNMP v2. Используйте только латинские буквы и цифры.
Интервал опроса (сек)	Интервал, через который сервер UserGate SIEM будет инициировать получение данных с сетевого устройства.
Пользователь	Только для SNMP v3. Имя пользователя для аутентификации на сетевом устройстве.
Тип аутентификации	Выбор режима аутентификации. Возможны варианты: - Без аутентификации, без шифрования (noAuthNoPriv). - С аутентификацией, без шифрования (authNoPriv). - С аутентификацией, с шифрованием (authPriv). Наиболее безопасным считается режим работы authPriv.
Алгоритм аутентификации	Алгоритм, используемый для аутентификации.
Пароль аутентификации	Пароль, используемый для аутентификации.
Алгоритм шифрования	Алгоритм, используемый для шифрования. Возможно использовать DES и AES.
Пароль шифрования	Пароль, используемый для шифрования.
Счётчики	Укажите здесь все требуемые данные, которые UserGate SIEM будет запрашивать на сетевом устройстве. Счетчики выбираются из баз MIB, которые загружены на устройство. Выберите в дереве SNMP необходимый раздел и добавьте соответствующий счетчик либо укажите в строке SNMP OID счетчика и его тип.

После успешного добавления сенсора в разделе **Дашборд** появится возможность добавить виджет с графиками данных SNMP, полученными с данного сенсора.

Управление SNMP MIB

Product: SIEM

Version: 7.x

Documentation: 

В этом разделе администратор может добавлять и удалять базы MIB (Management Information Base) UserGate SIEM.

Для получения специфических MIB обратитесь к производителю вашего устройства. UserGate SIEM уже содержит наиболее популярные базы сетевых устройств.

Сенсоры WMI

Version: 7.x
Product: SIEM
Documentation: 

С помощью сенсора WMI администратор может подключить WMI-совместимое сетевое устройство (компьютер под управлением ОС Windows) к UserGate SIEM для сбора и анализа его метрик.

Для создания сенсора WMI необходимо перейти в раздел **Сенсоры → WMI сенсоры**, нажать кнопку **Добавить** и заполнить необходимые поля:

Наименование	Описание
Включено	Включает или выключает данный сенсор WMI.
Название	Название сенсора WMI.
Описание	Опциональное описание сенсора.
Адрес сервера	IP-адрес устройства WMI.
Namespace	Пространство имен идентификаторов на устройстве WMI.
Интервал опроса (сек)	Интервал, через который сенсор WMI будет инициировать получение данных с сетевого устройства.
Пользователь	Имя пользователя для аутентификации на сетевом устройстве.
Пароль	Пароль, используемый для аутентификации.
Счётчики	Указать параметры Windows event log, которые UserGate SIEM будет мониторить на сетевом устройстве.

Конечные устройства

Version: 7.x

Product: SIEM

Documentation: 

Этот раздел содержит список конечных устройств с установленным программным обеспечением UserGate Client.

Примечание Конечное устройство будет отображено при выборе на UGMC данного устройства UserGate SIEM в качестве сервера для передачи информации о событиях, соответственно, UserGate SIEM должен быть предварительно зарегистрирован на UGMC.

Отображена следующая информация:

- Название конечного устройства, заданное на UGMC.
- Версия ПО UserGate Client, установленная на устройстве.
- Время последнего подключения к устройству.
- IP-адрес устройства.
- Netbios имя.
- Версия операционной системы (ОС) устройства.
- Телеметрическая информация.

В UserGate SIEM реализована возможность удаленного управления устройствами UserGate Client. Для этого нажмите **Послать команду** и выберите необходимое действие:

- Отключить от сети.
- Разрешить передачу данных по сети.
- Завершить процесс. При выборе данного действия необходимо указать идентификатор процесса.
- Запустить/остановить службу. Для выполнения данных действий необходимо указать название службы.

Коннекторы

Version: 7.x
Product: SIEM
Documentation: 

Коннекторы используются для возможности подключения устройства UserGate SIEM к различным средствам защиты или службам обмена данными об инцидентах информационной безопасности.

Для добавления коннектора необходимо указать следующие данные:

Наименование	Описание
Имя	Название коннектора.
Описание	Описание коннектора (опционально).
Тип сервера	Выбор типа сервера: • SSH; • HTTP; • HTTPS; (в текущей версии реализован только для интеграции с ГосСОПКА) .
Адрес сервера	Тип: • IP; • FQDN.
IP-адрес	IP-адрес сервера; указывается в случае выбора адреса сервера типа IP .
Порт	Порт сервера; указывается в случае выбора адреса сервера типа IP .
FQDN	FQDN сервера; указывается в случае выбора адреса сервера типа FQDN .
URL-путь	Используется при управлении устройством по API.
Логин	Логин пользователя для авторизации на коннекторе.
Пароль	Пароль учётной записи пользователя, необходимый для авторизации на коннекторе.
Группа команд	Указание группы команд доступно только для SSH-сервера, подробнее читайте в разделе Команды .
HTTP заголовки	Указание заголовков доступно только для серверов HTTP и HTTPS.

Кнопка **Тест** предназначена для проверки корректности настройки коннектора с типом сервера SSH. После нажатия **Тест** будет предложено выбрать команду из указанной группы для отправки на коннектор; в случае наличия в команде переменных, будут отображены дополнительные поля, в которых необходимо указать их значения.

В UserGate SIEM, по умолчанию, создан коннектор Gossopka, предназначенный для автоматизации обмена информацией об инцидентах информационной безопасности с ГосСОПКА (Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак). Подробнее читайте в разделе [Передача отчётов об инцидентах информационной безопасности в ГосСОПКА](#).

Общие сведения

Documentation: 

Product: SIEM

Version: 7.x

UserGate SIEM журналирует данные о событиях Unix-систем и других сетевых устройств, использующих стандарт syslog, с помощью [модуля log-collector](#). Эти данные содержат сведения о работе системы, ее состоянии, наличии ошибок, сбоях в работе, а также о событиях безопасности.

Модуль log-collector выполняет предварительную обработку и фильтрацию собранных данных, что позволяет UserGate SIEM использовать только необходимую информацию для обработки и [последующего анализа](#). В веб-консоли UserGate SIEM вы можете [настраивать параметры модуля log-collector](#), используемого в качестве syslog-сервера для сетевых устройств, а именно выбирать транспортный протокол (TCP или UDP) и порт подключения, а также настраивать TLS-шифрование для протокола TCP. Кроме того, вы можете [настраивать правила syslog](#) для фильтрации данных о событиях по нужным параметрам (например, по уровню важности событий).

В ходе обработки данных, полученных от модуля log-collector, UserGate SIEM записывает их в единое хранилище. Поддерживаются такие стандарты журналирования событий, как RFC 3164 и RFC 5424. Для стандарта RFC 5424 расширенные данные записываются в поле data хранилища. Вы можете просматривать все записи о событиях стандарта syslog в веб-консоли UserGate SIEM в разделе **Журналы и отчеты** → **Журналы** → **Syslog** (см. раздел «[Журнал syslog](#)»).

Настройка параметров syslog-сервера

Documentation: 

Product: SIEM

Version: 7.x

Для сбора событий стандарта syslog от сетевых устройств необходимо:

- активировать сервис **Сборщик логов** [для зон](#), в которых находятся сетевые устройства;
- настроить параметры syslog-сервера, роль которого выполняет модуль log-collector.

Чтобы настроить параметры syslog-сервера:

1. В разделе **Настройки** → **Сборщик логов** → **Syslog** нажмите **Настроить сервер**.

2. В блоке параметров **TCP** выполните следующие действия:

- включите прием событий syslog по протоколу TCP;
- укажите порт подключения к syslog-серверу (по умолчанию — 514);
- укажите максимальное количество одновременных сессий между syslog-сервером и сетевыми устройствами, от которых этот сервер получает данные.

Если требуется, включите TLS-шифрование передаваемых данных. Для этого установите флажок **Безопасное соединение** и [выберите необходимые сертификаты](#). При необходимости в блоке параметров **Разрешенные соседи** вы можете указать IP-адреса и доменные имена сетевых устройств, данные о событиях которых будет разрешено передавать на syslog-сервер.

3. В блоке параметров **UDP** выполните следующие действия:

- включите прием событий syslog по протоколу UDP;
- укажите порт подключения к syslog-серверу (по умолчанию — 514).

4. Нажмите **Сохранить и перезапустить** для применения новых параметров к syslog-серверу.

Настройка фильтрации syslog

Documentation: ☒

Product: SIEM

Version: 7.x

Вы можете настроить правила syslog для фильтрации данных, которые модуль log-collector будет передавать в UserGate SIEM для дальнейшей обработки и анализа.

Правила syslog отображаются в таблице раздела **Настройки → Сборщик логов → Syslog**. Вы можете управлять правилами syslog: изменять, удалять, а также включать и отключать их. Для этого используются соответствующие кнопки в панели инструментов. Также вы можете фильтровать правила в таблице по состоянию. Так, например, можно просмотреть только правила во включенном состоянии, применив фильтр **Показать включенные**.

Порядок расположения правил syslog в таблице соответствует порядку их применения к записям журналов событий по стандарту syslog. При необходимости вы можете изменять порядок с помощью кнопок **Наверх**, **Выше**, **Ниже**, **Вниз**.

Чтобы настроить правило syslog:

- В разделе **Настройки → Сборщик логов → Syslog** нажмите **Добавить**.
- На вкладке **Общие** выполните следующие действия:
 - Включите правило syslog.
 - Укажите название и при необходимости описание правила syslog.
 - Выберите действие по срабатыванию правила syslog (**Разрешить** — отправлять запись в UserGate SIEM, **Запретить** — не отправлять запись в UserGate SIEM).
 - Укажите часовой пояс правила syslog относительно UTC в секундах (по умолчанию — UTC+0). Указанный часовой пояс будет использоваться для отображения времени событий в UserGate SIEM.
 - Выберите расположение правила в таблице правил syslog.
- На соответствующих вкладках укажите необходимые параметры фильтрации записей:
 - На вкладке **Критичность** по кнопке **Добавить** выберите уровни важности событий, записи о которых следует отправлять в UserGate SIEM. При установке флажка **Инвертировать** (соответствует логическому отрицанию) выбранные уровни важности будут исключены из условий срабатывания правила syslog.
 - На вкладке **Объект** по кнопке **Добавить** выберите подсистемы, службы и сервисы, записи которых следует отправлять в UserGate SIEM. При установке флажка **Инвертировать** (соответствует логическому отрицанию) выбранные объекты будут исключены из условий срабатывания правила syslog.
 - На вкладке **Имя хоста** по кнопке **Добавить** укажите IP-адреса и доменные имена сетевых устройств, записи которых следует отправлять в UserGate SIEM.
 - На вкладке **Название приложения** укажите системные приложения, записи которых следует отправлять в UserGate SIEM. Вы можете выбрать эти приложения по кнопке **Добавить из библиотеки приложений syslog** или добавить новые приложения по кнопке **Создать и добавить новый объект**.
- Нажмите **Сохранить**.

IP-адреса

Product: SIEM
Version: 7.x
Documentation: 

Раздел **IP-адреса** содержит списки диапазонов IP-адресов, которые могут использоваться в поисковых запросах.

Списки IP-адресов создаются на панели **Группы**. Они могут быть **локальными** и **обновляемыми**.

Локальные списки создаются и хранятся на самом устройстве.

Если список предполагается использовать в поисковых запросах, необходимо в свойствах создаваемого списка поставить соответствующий флажок.

IP-адреса в эти списки добавляются администратором вручную на панели **Адреса из выбранной группы**:

IP-адреса добавляются в виде: IP-адрес, IP-адрес/маска сети или диапазон IP-адресов, например: 192.168.1.5, 192.168.1.0/24 или 192.168.1.5-192.168.2.100.

Обновляемые списки получают информацию об IP-адресах с внешних серверов по указанному в свойствах списка URL обновления:

Если список предполагается использовать в поисковых запросах, необходимо в свойствах создаваемого списка поставить соответствующий флажок.

На вкладке **Настройка расписания автоматических обновлений** настраивается расписание обновления этого списка:

Администратор имеет возможность создавать свои обновляемые списки IP-адресов. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми IP-адресами.	Создать файл list.txt со списком адресов. Список адресов записывается в обычный текстовый файл, где адреса прописываются в столбик без знаков препинания. Например: x.x.x.x y.y.y.y z.z.z.z
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip .
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.

Наименование	Описание
Шаг 5. Создать список IP-адресов и указать URL для обновления.	На каждом устройстве создать список IP-адресов. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. Устройство будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. ПримечаниеURL списка задается в формате: <code>http://х.х.х.х/</code> или <code>ftp://х.х.х.х/</code>. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать sgmlab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение ""/2" в поле "часы" будет означать "каждые два часа".

Useragent браузеров

Documentation: ☒
Product: SIEM
Version: 7.x

Списки Useragent браузеров создаются в веб-консоли администратора в разделе **Библиотеки → Useragent браузеров → Категории**. Они содержат информацию о типах браузеров у пользователей.

Списки могут быть **локальными** и **обновляемыми**.

Локальные списки создаются и хранятся на самом устройстве.

Если список предполагается использовать в поисковых запросах, необходимо в свойствах создаваемого списка поставить соответствующий флажок.

Данные в эти списки добавляются администратором вручную на панели **Шаблоны useragent**. Исчерпывающий список строк Useragent представлен на этом ресурсе: <http://www.useragentstring.com/pages/useragentstring.php>.

Обновляемые списки получают информацию с внешних серверов по указанному в свойствах списка URL обновления:

Если список предполагается использовать в поисковых запросах, необходимо в свойствах создаваемого списка поставить соответствующий флажок.

На вкладке **Настройка расписания автоматических обновлений** настраивается расписание обновления этого списка:

Администратор имеет возможность создавать свои обновляемые списки Useragent и централизованно распространять их на все свои устройства. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми Useragent.	Создать файл list.txt со списком Useragent .
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip .
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.

Наименование	Описание
Шаг 5. Создать список Useragent и указать URL для обновления.	На каждом устройстве создать список Useragent. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. Устройство будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: - Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. - Ежедневно. - Еженедельно. - Ежемесячно. - Каждые ... часов. - Каждые ... минут. - Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: - Звездочка (*) — обозначает весь диапазон (от первого до последнего). - Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. - Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". - Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение " */2" в поле "часы" будет означать "каждые два часа".

Типы контента

Documentation: ☒
Product: SIEM
Version: 7.x

Раздел **Типы контента** содержит список типов контента, которые могут использоваться в поисковых запросах.

Списки Типов контента создаются на панели **Категории**. Они могут быть **локальными** и **обновляемыми**.

Локальные списки создаются и хранятся на самом устройстве.

Если список предполагается использовать в поисковых запросах, необходимо в свойствах создаваемого списка поставить соответствующий флажок.

Данные в формате MIME в эти списки добавляются администратором вручную на панели **Типы контента**. Различные типы контента и их описание доступны по ссылке <https://www.iana.org/assignments/media-types/media-types.xhtml>.

Обновляемые списки получают данные с внешних серверов по указанному в свойствах списка URL обновления:

Если список предполагается использовать в поисковых запросах, необходимо в свойствах создаваемого списка поставить соответствующий флажок.

На вкладке **Настройка расписания автоматических обновлений** настраивается расписание обновления этого списка:

Администратор имеет возможность создавать свои списки типов контента и централизованно распространять их на все свои управляемые устройства. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми типами контента.	Создать файл list.txt со списком типов контента.
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip .
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.

Наименование	Описание
Шаг 5. Создать список типа контента и указать URL для обновления.	На каждом устройстве создать список типа контента. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. Устройство будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать cronTab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение " */2" в поле "часы" будет означать "каждые два часа".

Списки URL

Version: 7.x
Documentation: 
Product: SIEM

Раздел **Списки URL** содержит списки URL-адресов, которые могут использоваться в поисковых запросах.

Списки URL создаются на панели **Списки URL**. Они могут быть **локальными** и **обновляемыми**.

Локальные списки создаются и хранятся на самом устройстве.

Необходимо установить категорию создаваемого списка в поле **Чувствительность к регистру**:

- Чувствительный к регистру** — список URL адресов, чувствительных к регистру букв в адресе.
- Нечувствительный к регистру** — список URL адресов, нечувствительных к регистру букв в адресе. Использование списка этой категории исключает необходимость перебора вариантов написания одного и того же выражения с буквами в различных регистрах.
- Домен** — список адресов доменов для использования в правилах DNS-фильтрации.

Категория списка задается при его создании. Изменить категорию после создания списка нельзя.

Если список предполагается использовать в поисковых запросах, необходимо в свойствах создаваемого списка поставить соответствующий флажок.

Данные в эти списки добавляются администратором вручную на панели **URL**:

В списках можно использовать специальные символы «^», «\$» и «*»:

«*» — любое количество любых символов

«^» — начало строки

«\$» — конец строки

Символы «?» и «#» не могут быть использованы.

Если URL-запись начинается с http://, «https://», «ftp://» или содержит один или более символов «/», то это считается URL и применяется только для HTTP(S) фильтрации, к DNS-фильтрации такая запись не применяется. В противном случае строка рассматривается как имя домена и применяется для DNS-фильтрации и HTTP(S)-фильтрации.

Для фильтрации точного адреса используйте символы «^» и «\$»:

`^http://domain.com/exacturl$`

Для фильтрации точного URL всех дочерних папок используйте символ «^»:

`^http://domain.com/exacturl/`

Для фильтрации домена со всеми возможными URL используйте запись такого вида:

`domain.com`

Пример интерпретации URL-записей:

Пример записи	Обработка DNS- запросов	Обработка HTTP-запросов
yahoo.com или *yahoo.com*	Фильтруется весь домен и домены более высоких (3,4 и т.д.) уровней, например: sport.yahoo.com mail.yahoo.com а также: qweryahoo.com	Фильтруется весь домен и все URL этого домена, а также домены более высоких (3,4 и т.д.) уровней, например: http://sport.yahoo.com http://mail.yahoo.com https://mail.yahoo.com http://sport.yahoo.com/123 http://qwertyyahoo.com/
^mail.yahoo.com\$	Отфильтрован только mail.yahoo.com	Отфильтрованы только: http://mail.yahoo.com https://mail.yahoo.com
^mail.yahoo.com/\$	Ничего не отфильтровано	Ничего не отфильтровано, так как последний символ слэш определяет URL, но не указаны «https» или «http»
^http://finance.yahoo.com/personal-finance/\$	Ничего не отфильтровано	Отфильтрован только: http://finance.yahoo.com/personal-finance/
^yahoo.com/12345/	Ничего не отфильтровано	Отфильтрованы: http://yahoo.com/12345/whatever/ https://yahoo.com/12345/whatever/

Обновляемые списки получают данные с внешних серверов по указанному в свойствах списка URL обновления:

Необходимо установить категорию создаваемого списка в поле **Чувствительность к регистру** (описание поля см. [ранее](#)).

Если список предполагается использовать в поисковых запросах, необходимо в свойствах создаваемого списка поставить соответствующий флажок.

На вкладке **Настройка расписания автоматических обновлений** настраивается расписание обновления этого списка:

Администратор имеет возможность создавать собственные списки и централизованно распространять их на все свои устройства. Для создания таких списков необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимым списком URL.	Создать текстовый файл list.txt со списком URL в следующем формате: www.site1.com/url1 www.site2.com/url2 ... www.siteend.com/urlN
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip .
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.
Шаг 5. Создать список и указать URL для обновления.	На каждом устройстве создать список URL. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. Устройство будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. ПримечаниеURL списка задается в формате: http://х.х.х.х/ или ftp://х.х.х.х/. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать sgmlab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение ""/2" в поле "часы" будет означать "каждые два часа".

Категории URL

Documentation: ☒
Product: SIEM
Version: 7.x

Раздел **Категории URL** содержит группы категорий, которые могут использоваться в поисковых запросах.
Группы категорий создаются на панели **Группы URL категорий**. Категории в группу категорий URL добавляются на панели **Категории**.

Если список предполагается использовать в поисковых запросах, необходимо в свойствах создаваемого списка поставить соответствующий флажок.

Текстовые списки

Documentation: ☒
Product: SIEM
Version: 7.x

Раздел **Текстовые списки** содержит произвольные строковые списки, которые могут использоваться в поисковых запросах. Примеры данных, которые могут содержаться в этих списках — значение хэшей, MAC-адреса итд.

Списки создаются на панели **Текстовые списки**. Они могут быть **локальными** и **обновляемыми**.

Локальные списки создаются и хранятся на самом устройстве.

Если список предполагается использовать в поисковых запросах, необходимо в свойствах создаваемого списка поставить соответствующий флажок.

Данные в эти списки добавляются администратором вручную на панели **Строки**:

Обновляемые списки получают данные с внешних серверов по указанному в свойствах списка URL обновления:

Если список предполагается использовать в поисковых запросах, необходимо в свойствах создаваемого списка поставить соответствующий флажок.

На вкладке **Настройка расписания автоматических обновлений** настраивается расписание обновления этого списка:

Администратор имеет возможность создавать собственные списки и централизованно распространять их на все свои устройства. Для создания таких списков необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимым списком.	Создать текстовый файл list.txt со списком.
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip .
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии списка, например, 4. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.

Наименование	Описание
Шаг 5. Создать список и указать URL для обновления.	На каждом устройстве создать текстовый список. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. Устройство будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. ПримечаниеURL списка задается в формате: <code>http://х.х.х.х/</code> или <code>ftp://х.х.х.х/</code>. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: - Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. - Ежедневно. - Еженедельно. - Ежемесячно. - Каждые ... часов. - Каждые ... минут. - Задать вручную. При задании вручную необходимо использовать столб-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: - Звездочка (*) — обозначает весь диапазон (от первого до последнего). - Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. - Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". - Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение ""/2" в поле "часы" будет означать "каждые два часа".

Почтовые адреса

Documentation: ☒
Product: SIEM
Version: 7.x

Элемент библиотеки **Почтовые адреса** позволяет создать группы почтовых адресов, которые впоследствии можно использовать в правилах фильтрации почтового трафика и для использования в оповещениях.

Для добавления новой группы почтовых адресов необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать группу почтовых адресов	В панели Группы почтовых адресов нажать на кнопку Добавить , дать название группе.
Шаг 2. Добавить почтовые адреса в группу	Выделить созданную группу, нажать на кнопку Добавить на панели Почтовые адреса и добавить необходимые почтовые адреса.

Администратор имеет возможность создавать обновляемые списки почтовых адресов и централизованно распространять их на устройства UserGate. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми списком почтовых адресов.	Создать файл list.txt со списком почтовых адресов.
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip .
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.
Шаг 5. Создать список почтовых адресов и указать URL для обновления.	На каждом UserGate создать список адресов. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. UserGate будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: - Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. - Ежедневно. - Еженедельно. - Ежемесячно. - Каждые ... часов. - Каждые ... минут. - Задать вручную. При задании вручную необходимо использовать cronTab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: - Звездочка (*) — обозначает весь диапазон (от первого до последнего). - Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7. - Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". - Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

Администратор может экспортировать и импортировать списки почтовых адресов используя соответствующие кнопки **Экспорт/Импорт**.

Номера телефонов

Version: 7.x
Product: SIEM
Documentation: 

Элемент библиотеки **Номера телефонов** позволяет создать группы номеров, которые впоследствии можно использовать в правилах оповещения SMPP.

Для добавления новой группы телефонных номеров необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать группу телефонных номеров	В панели Группы телефонных номеров нажать на кнопку Добавить , дать название группе.
Шаг 2. Добавить номера телефонов в группу	Выделить созданную группу, нажать на кнопку Добавить на панели Группа телефонных номеров и добавить необходимые номера.

Администратор имеет возможность создавать обновляемые списки телефонных номеров и централизованно распространять их на устройства UserGate. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми списком номеров.	Создать файл list.txt со списком номеров.
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip .
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.
Шаг 5. Создать список телефонных номеров и указать URL для обновления.	На каждом UserGate создать список номеров. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. UserGate будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: - Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. - Ежедневно. - Еженедельно. - Ежемесячно. - Каждые ... часов. - Каждые ... минут. - Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: - Звездочка (*) — обозначает весь диапазон (от первого до последнего). - Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. - Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". - Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "/"2" в поле "часы" будет означать "каждые два часа".

Администратор может экспортировать и импортировать списки телефонных номеров используя соответствующие кнопки **Экспорт/Импорт**.

Команды

Documentation: ☒
Product: SIEM
Version: 7.x

Данный раздел позволяет создавать группы команд, предназначенных для отправки на коннекторы.

Для создания группы команд необходимо указать следующие параметры:

Наименование	Описание
Шаг 1. Создать список команд.	На панели Группы команд нажать на кнопку Добавить , задать название списка, описание и тип списка.
Шаг 2. Указать адрес обновления списка (не обязательно).	В случае создания обновляемого списка указать адрес сервера обновления. Более подробно об обновляемых списках смотрите далее в этой главе.
Шаг 3. Добавить команды в группу.	На панели Команды нажать на кнопку Добавить и указать название и текст команды. Для определения переменных необходимо использовать фигурные скобки ({}). Далее переменные будут использованы для подстановки актуальных значений.

Администратор имеет возможность создавать обновляемые списки команд и централизованно распространять их на устройства UserGate. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми списком команд.	Создать файл list.txt со списком команд.
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip .
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.
Шаг 5. Создать список команд и указать URL для обновления.	На каждом UserGate создать список. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. UserGate будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: - Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. - Ежедневно. - Еженедельно. - Ежемесячно. - Каждые ... часов. - Каждые ... минут. - Задать вручную. При задании вручную необходимо использовать cronTab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: - Звездочка (*) — обозначает весь диапазон (от первого до последнего). - Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. - Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". - Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение ""/2" в поле "часы" будет означать "каждые два часа".

Администратор может экспортировать и импортировать списки команды используя соответствующие кнопки **Экспорт**/**Импорт**. При импорте необходимо создать файл, содержащий список команд, заданных в следующем формате: ИМЯ_КОМАНДЫ:ТЕКСТ_КОМАНДЫ (для определения переменных используйте фигурные скобки).

Правила аналитики

Documentation: 
Product: SIEM
Version: 7.x

В данной библиотеке находятся правила аналитики, созданные разработчиками UserGate. Библиотека обновляется при наличии модуля Security update в лицензии на решение UserGate SIEM.

Наличие такой библиотеки призвано упростить процесс создания правил аналитики для пользователей UserGate SIEM. Предусмотренные правила из библиотеки могут быть использованы в качестве примера для написания собственных правил аналитики. Для этого пользователи могут импортировать правила из библиотеки в свой рабочий набор правил аналитики следующим образом:

- 1. Выбрать в библиотеке правил аналитики группу аналитики, далее в области **Правила аналитики** выбрать необходимое правило.
- 2. Нажать кнопку **Добавить в аналитику** на панели правил аналитики:



Диалоговое окно предложит выбрать категорию срабатывания и Часовой пояс для импорта правила:

- 3. После импорта правила из библиотеки оно появится на вкладке **Правила аналитики** в разделе **Аналитика**:



- 4. Настройки импортированного правила могут редактироваться пользователями. Для этого необходимо выбрать правило и нажать кнопку **Редактировать** в панели инструментов:

Правила нормализации логов

Documentation: ☒
Product: SIEM
Version: 7.x

В данной библиотеке находятся правила нормализации логов, созданные разработчиками UserGate. Библиотека обновляется при наличии модуля Security update в лицензии на решение UserGate SIEM.

Наличие такой библиотеки призвано упростить процесс создания правил корреляции данных для пользователей UserGate SIEM. Предусмотренные правила из библиотеки могут быть использованы в качестве примера для написания собственных правил нормализации. Для этого пользователи могут импортировать правила из библиотеки в свой рабочий набор правил нормализации следующим образом:

- 1. Выбрать в библиотеке правил нормализации логов группу нормализации, далее в области **Правила нормализации логов** выбрать необходимое правило.
- 2. Нажать кнопку **Добавить в пользовательскую нормализацию логов** на панели правил нормализации:



- 3. После импорта правила из библиотеки оно появится в разделе пользовательской нормализации логов:



- 4. Настройки импортированного правила могут редактироваться пользователями. Для этого необходимо выбрать правило и нажать кнопку **Редактировать** в панели инструментов:

Профили оповещений

Documentation: ☒
Product: SIEM
Version: 7.x

Профиль оповещения указывает транспорт, с помощью которого оповещения могут быть доставлены получателям. Поддерживается 2 типа транспорта:

- SMTP, доставка сообщений с помощью email
- SMPP, доставка сообщений с помощью SMS практически через любого оператора сотовой связи или через большое количество SMS-центров рассылки

Для создания профиля сообщений SMTP необходимо нажать на кнопку **Добавить** в разделе **Профили оповещений**, выбрать вариант **Добавить профиль оповещения SMTP** и заполнить необходимые поля:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Хост	IP-адрес сервера SMTP, который будет использоваться для отсылки почтовых сообщений.
Порт	Порт TCP, используемый сервером SMTP. Обычно для протокола SMTP используется порт 25, для SMTP с использованием SSL - 465. Уточните данное значение у администратора почтового сервера.
Безопасность	Варианты безопасности отправки почты, возможны варианты: Нет, STARTTLS, SSL.
Аутентификация	Включает аутентификацию при подключении к SMTP-серверу.
Логин	Имя учетной записи для подключения к SMTP-серверу.
Пароль	Пароль учетной записи для подключения к SMTP-серверу.

Для создания профиля сообщений SMPP необходимо нажать на кнопку **Добавить** в разделе **Профили оповещений**, выбрать вариант **Добавить профиль оповещения SMPP** и заполнить необходимые поля:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Хост	IP-адрес сервера SMPP, который будет использоваться для отсылки SMS сообщений.
Порт	Порт TCP, используемый сервером SMPP. Обычно для протокола SMPP используется порт 2775, для SMPP с использованием SSL - 3550.
SSL	Использовать или нет шифрацию с помощью SSL.
Логин	Имя учетной записи для подключения к SMPP-серверу.
Пароль	Пароль учетной записи для подключения к SMPP-серверу.
Правила трансляции номеров	В некоторых случаях SMPP-провайдер ожидает номер телефона в определенном формате, например, в виде 89123456789. Для соответствия требованиям провайдера можно указать замену первых символов номеров с одних на другие. Например, заменить все номера, начинающиеся на +7, на 8.

Категории срабатываний

Documentation: 
Product: SIEM
Version: 7.x

Элемент библиотеки **Категории срабатываний** позволяет создать категории, по которым можно группировать определенные срабатывания правил аналитики, применяемые к событиям. Более подробно о правилах аналитики смотрите в разделе [Аналитика](#). По умолчанию создаются категории:

- **Availability** — правила аналитики, определяющие инциденты, приводящие к ухудшению доступности информационных систем.
- **Performance** — правила аналитики, определяющие инциденты, приводящие к ухудшению производительности информационных систем.
- **Security** — правила аналитики, определяющие инциденты, приводящие к ухудшению безопасности информационных систем.

Внешние сервисы обогащений

Product: SIEM
Documentation: 
Version: 7.x

В данном элементе библиотеки представлены ресурсы, с помощью которых происходит дополнительный сбор информации об угрозах. С данных источников приходят фиды — структурированные проанализированные данные об IP-адресах и доменах, с которых происходит распространение вредоносных файлов, их примеры и хэши; списки фишинговых сайтов, почтовые адреса отправителей фишинговых писем; адреса, с которых происходит сканирование сетей с целью обнаружения уязвимостей; IP-адреса, с которых проводятся атаки типа брутфорс; сигнатуры для обнаружения вредоносного программного обеспечения.

Чтобы использовать сервисы обогащения, необходимо их включить. Некоторые сервисы требуют прохождения регистрации с предоставлением ключа доступа.

Наименование	Описание
dnsgoogle	Интернет-сервис компании Google, представляющий собой общедоступные DNS-серверы. Подробнее: https://dns.google . Предназначен для типов улик: IP.
urlihaus	Проект abuse.ch. Целью проекта является сбор, отслеживание и обмен URL-адресами вредоносных программ. Подробнее: https://urlihaus.abuse.ch/ . Предназначен для типов улик: Домен, Хэш, Имя хоста, IP, URL.
dshield	Система корреляции журналов межсетевого экрана для совместной работы. Система получает журналы от добровольцев со всего мира и использует их для анализа тенденций атак. Подробнее: https://www.dshield.org/xml.html . Предназначен для типов улик: Домен, FQDN, IP.
cybercrime	Сервис предоставляет информацию об уровнях угрозы разных объектов. Подробнее: http://cybercrime-tracker.net . Предназначен для типов улик: Домен, FQDN, IP, URL, Другое.
cyberprotect	Сервис предоставляет информацию об уровнях угрозы разных объектов. Подробнее: https://console.threatscore.cyberprotect.cloud/ . Предназначен для типов улик: Домен, Хэш, IP, URL, Агент пользователя.
unshorten	Сервис предоставляет возможности предварительного просмотра целевого URL для любого короткого URL и проверки безопасности на вредоносные ссылки. Сервис не использует внешний ресурс; анализирует ответ на запрос по тестируемому URL. Предназначен для типов улик: URL.
ipwhois	Сервис позволяет получить информацию об IP-адресах. Подробнее: https://ipwhois.io/ . Предназначен для типов улик: IP.
ipinfo	Инструмент для определения владельца, Интернет-провайдера и местонахождения веб-сайта, домена или IP-адреса. Подробнее: https://ipinfo.io/ . Предназначен для типов улик: IP. Для использования сервиса необходимо ввести реквизиты.
hashdd	Сервис предоставляет базу вредоносных хэшей файлов и различные проверки для получения полного представления об угрозе. Подробнее: https://hashdd.com/ . Предназначен для типов улик: Хэш. Для использования сервиса необходимо ввести реквизиты.
urlscan	Сервис для получения информации о подозрительных, вредоносных и фишинговых URL. Подробнее: https://urlscan.io/ . Предназначен для типов улик: Домен, FQDN, Хэш, IP, URL. Для использования сервиса необходимо ввести реквизиты.
emailrep	Система, которая собирает данные об адресах электронной почты, доменах и пользователях. Подробнее: https://emailrep.io/ . Предназначен для типов улик: Почта. Для использования сервиса необходимо ввести реквизиты.
greynoise	Компания занимается анализом фонового шума Интернета (пакеты данных, адресованные IP-адресам или портам, где нет сетевого устройства, настроенного для их приёма). Благодаря такой фильтрации снижается количество ложных срабатываний. Подробнее: https://www.greynoise.io/ . Предназначен для типов улик: IP. Для использования сервиса необходимо ввести реквизиты.
abuseip	Проект, который занимается борьбой со злоумышленной деятельностью. Подробнее: https://www.abuseipdb.com/ . Предназначен для типов улик: IP. Для использования сервиса необходимо ввести реквизиты.
hybridanalysis	Сервис проверки файлов на вредоносность. Подробнее: https://www.hybrid-analysis.com/ . Предназначен для типов улик: Хэш. Для использования сервиса необходимо ввести реквизиты.

Documentation: ☒
Product: SIEM
Version: 7.x

Данный раздел содержит приложения, которые могут быть использованы в правилах syslog для сбора информации.

Чтобы добавить приложение необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать приложение.	Нажать кнопку Добавить и указать название и описание приложения.
Шаг 2. Указать приложение.	Указать название приложения, для которого будут применены правила syslog.

Маршруты

Documentation: 

Product: SIEM

Version: 7.x

Раздел **Маршруты** позволяет получить список всех маршрутов, указанных на определенном узле UserGate SIEM. Для просмотра маршрутов необходимо нажать на кнопку **Фильтр** и указать типы маршрутов, которые необходимо отобразить. Возможно указать следующие типы маршрутов:

- **Подключенные к интерфейсам** — маршруты к сетям, которые подключены непосредственно к интерфейсам UserGate SIEM. Данные маршруты будут помечены символом **С** в списке маршрутов.
- **Заданные статически** — маршруты, заданные статически в разделе **Сеть → Маршруты**. Данные маршруты будут помечены символом **К** в списке маршрутов.
- **OSPF** — маршруты, полученные по протоколу OSPF. Данные маршруты будут помечены символом **О** в списке маршрутов.
- **BGP** — маршруты, полученные по протоколу BGP. Данные маршруты будут помечены символом **В** в списке маршрутов.

Отображаемый список маршрутов можно скачать в виде текстового файла с помощью кнопки **Скачать все маршруты**.

Documentation: ☒
Product: SIEM
Version: 7.x

С помощью утилиты ping можно диагностировать доступность сетевых ресурсов. Параметры команды ping:

Наименование	Описание
Ping host	Хост, который необходимо проверить.
TTL	Максимальное количество промежуточных хостов, которое разрешено пройти на пути к проверяемому хосту.
Интерфейс	Адрес выбранного интерфейса будет использоваться в качестве адреса источника для выполнения ping, а интерфейс отправки пакета будет выбран согласно таблице маршрутизации.
Счетчик	Количество повторов.
Показывать timestamp	Добавляет timestamp в вывод команды.
Не резолвить имена	Оперировать IP-адресами, не преобразовывая их в доменные имена.

Traceroute

Documentation: ☒
Product: SIEM
Version: 7.x

С помощью утилиты traceroute можно проверить путь следования сетевых пакетов к определенному хосту. Параметры команды traceroute:

Наименование	Описание
Traceroute host	Хост, который необходимо проверить.
Использовать ICMP	Использовать протокол ICMP для выполнения команды traceroute. Если не указано, то используется протокол UDP.
Интерфейс	С какого сетевого интерфейса выполнять команду.
Не резолвить имена	Оперировать IP-адресами, не преобразовывая их в доменные имена.

Запрос DNS

Documentation: ☒
Product: SIEM
Version: 7.x

Используя запрос DNS, администратор может проверить работу DNS-серверов.

Наименование	Описание
DNS-запрос (хост)	DNS имя для проверки.
IP источника запроса	Один из IP-адресов, назначенных UserGate.
DNS сервер	DNS сервер, куда посылать запрос.
Порт	UDP порт, используемый для запроса.
Тип DNS-запроса	Тип запроса.

Documentation: ☒
Product: SIEM
Version: 7.x

Данный раздел позволяет определить правила оповещений, которые в дальнейшем можно использовать для отсылки оповещений о различных типах событий, например, высокой загрузке CPU или отправке пароля пользователю по SMS. Для создания правила оповещений необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать один или несколько профилей оповещений.	Смотрите раздел Профили оповещений.
Шаг 2. Создать группы получателей оповещений.	Смотрите разделы Почтовые адреса и Номера телефонов.
Шаг 3. Создать правило оповещения.	Во вкладке Диагностика и мониторинг в разделе Оповещения → Правила оповещений добавить правило.

При добавлении правила необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает данное правило.
Название	Название правила.
Описание	Описание правила.
Профиль оповещения	Созданный ранее профиль оповещения. Для профилей SMPP появится закладка для указания адресатов в виде телефонных номеров, для SMTP появится закладка для указания адресатов в виде email-адресов.
От	От кого будет приходить оповещение.
Тема	Тема оповещения.
Таймаут перед повторной отправкой, секунд	Укажите таймаут, в течение которого сервер не будет отправлять сообщение при повторном срабатывании данного правила. Данная настройка позволяет предотвратить шторм сообщений при частом срабатывании правила оповещения.
События	Укажите события, для которых необходимо получать оповещения.
Телефоны	Для SMPP-профиля. Укажите группы номеров телефонов, куда отправлять SMS-оповещения.
Emails	Для SMTP-профиля. Укажите группы адресов email, на которые будут отправляться почтовые оповещения.

Documentation: ☒
Product: SIEM
Version: 7.x

UserGate поддерживает мониторинг с помощью протоколов SNMP v2c и SNMP v3. Поддерживается управление как с помощью запросов (SNMP queries), так и с помощью отсылки оповещений (SNMP traps). Это позволяет наблюдать за критическими параметрами UserGate с помощью программного обеспечения SMNP-управления, используемого в компании.

Для настройки мониторинга с помощью SNMP необходимо:

1. В свойствах зоны интерфейса, к которому будет осуществляться подключение по протоколу SNMP, во вкладке **Контроль доступа** разрешить сервис **SNMP**.
2. Создать правило SNMP

Для настройки мониторинга с помощью SNMP необходимо создать правила SNMP. Для создания правила SNMP необходимо в разделе **SNMP** нажать на кнопку **Добавить** и указать следующие параметры:

Наименование	Описание
Название правила	Название правила.
IP-адрес сервера для трапов	IP-адрес сервера для трапов и порт, на котором сервер слушает оповещения. Обычно это порт UDP 162. Данная настройка необходима только в случае, если необходимо отправлять трапы на сервер оповещений.
Комьюнити	SNMP community - строка для идентификации сервера UserGate и сервера управления SNMP для версии SNMP v2c. Используйте только латинские буквы и цифры.
Контекст	Необязательный параметр, определяющий SNMP context. Можно использовать только латинские буквы и цифры. На некоторых устройствах может быть несколько копий полного поддерева MIB. Например, на устройстве может быть создано несколько виртуальных маршрутизаторов. Каждый такой виртуальный маршрутизатор будет иметь полное поддерево MIB. В этом случае каждый виртуальный маршрутизатор может быть указан как контекст на сервере SNMP. Контекст определяется по имени. Когда клиент отправляет запрос, он может указать имя контекста. Если имя контекста не указано, будет запрошен контекст по умолчанию.
Версия	Указывает версию протокола SNMP, которая будет использоваться в данном правиле. Возможны варианты SNMP v2c и SNMP v3.
Разрешить SNMP-запросы	При включении разрешает получение и обработку SNMP-запросов от SNMP-менеджера.
Разрешить SNMP-трапы	При включении разрешает отправку SNMP-трапов на сервер, настроенный для приема оповещений.
Название профиля безопасности SNMP	Только для SNMP v3. Подробнее — в разделе Профили безопасности SNMP .
События	Выбор типов параметров, доступных для мониторинга по правилу.

Примечание:настройки аутентификации для SNMP v2c (community) и для SNMP v3 (пользователь, тип аутентификации, алгоритм аутентификации, пароль аутентификации, алгоритм шифрования, пароль шифрования — в профиле безопасности SNMP) на SNMP-менеджере должны совпадать с настройками SNMP в UserGate.

Информацию по настройке параметров аутентификации для вашего SNMP-менеджера смотрите в руководстве по настройке выбранного вами программного обеспечения для управления SNMP.

UserGate выделен уникальный идентификатор **SNMP PEN** (Private Enterprise Number) **45741**.

Актуальные mib-файлы UserGate с параметрами мониторинга можно скачать из консоли администратора устройства. Для этого необходимо перейти на вкладку **Диагностика и мониторинг**, далее в разделе **Оповещения** → **SNMP** нажать **Скачать MIB**.

Для скачивания доступны следующие MIB-файлы:

- UTM-TRAPS-MIB.
- UTM-TRAPS-BINDINGS-MIB.
- UTM-MIB.
- UTM-INTERFACES-MIB.
- UTM-TEMPERATURE-MIB.

UTM-TRAPS-MIB

Наименование	Описание
trapCoreCrush	Сбой ядра.
trapStatDown	Сервис статистики (UserGate Log Analyzer) недоступен.
trapCoreBootstrapEnd	Загрузка сервера завершена успешно.
trapDefaultGatewayChanged	Изменение шлюза по умолчанию.
trapHighSessionsCounter	Таблица сессий заполнена на 90%.
trapHighUsersCounter	Количество активных пользователей достигло 90% от порога лицензии.
trapDataPartitionFSStatus	Статус файловой системы. Состояние файловой системы изменилось на "not_clean".
trapStatusChanged	Изменение статуса узла отказоустойчивого кластера.
trapMemberUp	Статус узла отказоустойчивого кластера изменился на «Подключен».
trapMemberDown	Узел отказоустойчивого кластера отключен.
trapAttackDetected	Обнаружение атаки системой COB.
trapChecksumFailed	Нарушение целостности бинарных файлов.
trapHighCPUUsage	Высокая загрузка центрального процессора (95%).
trapLowMemory	Высокая загрузка памяти (95%).

Наименование	Описание
trapLowLogdiskSpace	Недостаточно места на диске для хранения журналов.
trapRaidStatus	Изменение статуса RAID.
trapPowerSupply	Первый источник питания отключен.
trapCableStatus	Кабель был подключен или отключен от интерфейса.
trapHighDiskIOutilization	Высокая нагрузка диска. Оповещение отправляется при загрузке >=95% за 5 минут хотя бы на одном из дисковых устройств.
trapTrafficDrop	Срабатывание запрещающего правила межсетевого экрана.
trapLDAPServerDown	Сервер LDAP недоступен.
trapCriticalTemperature	Критическая температура на одном из сенсоров. Оповещение отправляется при пересечении одного из пределов рабочей температуры (нижнего или верхнего). Нижний предел рабочей температуры обычно равен 0°C (для устройств серии X -40°C), верхний предел равен 85°C.

UTM-TRAPS-BINDINGS-MIB

Наименование	Тип данных	Описание
utmSessions	integer	Текущее количество активных сессий.
utmSessionsMax	integer	Максимальное количество активных сессий.
utmUsers	integer	Количество активных пользователей на данный момент.
utmUsersMax	integer	Максимальное количество активных пользователей.
utmDataPartionFSStatus	integer	Состояние файловой системы. 0 — clean. 1 — not clean.
utmHASStatus	integer	Текущий статус узла кластера отказоустойчивости: 0 — master-узел. 1 — slave-узел. 3 — fault.
utmHASStatusReason	integer	Причина изменения статуса узла отказоустойчивого кластера: 1 — связь с узлом потеряна. 2 — HTTP прокси-сервер недоступен. 3 — ни один из шлюзов недоступен. 4 — DNS-сервер недоступен. 5 — узел UserGate Management Center недоступен.
utmCPUUsage	integer	Загруженность центрального процессора (%).
utmMemory	integer	Использование оперативной памяти (%).
utmLogdiskSpace	integer	Пространство на диске, используемое под журналы (%).
utmAdaptecRaidStatus	integer	Текущий статус RAID (Redundant Array of Independent Disks), построенного на контроллере Adaptec: - no_raid. 0 — optimal — массив в оптимальном состоянии. 1 — degraded — полный или частичный выход из строя одного из дисков. 2 — rebuild — восстановление массива.
utmBroadcomRaidStatus	integer	Текущий статус RAID (Redundant Array of Independent Disks), построенного на контроллере Broadcom: - no_raid 0 — optimal — массив в оптимальном состоянии. 1 — degraded — полный или частичный выход из строя одного из дисков. Переход в данный статус произойдёт при выходе из строя 2-х дисков. 2 — partialDegraded — полный или частичный выход из строя одного из дисков. 3 — failed — не работает из-за наличия ошибки. 4 — offline — диск не доступен для RAID-контроллера.
utmPowerSupply	integer	Количество источников питания: 1 — один блок питания. 2 — два блока питания.
utmPowerSupplyStatus	integer	Состояние источника питания: - no_power_supplies. 0 — off. 1 — on.
utmCSCIfName	string	Название интерфейса.

Наименование	Тип данных	Описание
utmCSCStatus	integer	Статус сетевого адаптера: 1 — кабель подключен. 2 — кабель не подключен.
utmDiskIOUtilization	integer	Текущая утилизация диска (%).
utmLDAPServerName	string	Название LDAP-сервера.
utmLDAPServerAddress	string	IP-адрес LDAP-сервера.
utmThermSensor	string	Название температурного сенсора.
utmThermValue	integer	Значение температуры, измеренное сенсором.

UTM-MIB

Наименование	Тип данных	Описание
vcpuCount	integer	Количество виртуальных процессоров в системе.
vcpuUsage	integer	Загруженность виртуальных процессоров системы; отображается фактическое число загруженных виртуальных процессоров.
usersCounter	integer	Количество активных пользователей на текущий момент времени. (*)
sessionsCounter	integer	Количество активных сессий на текущий момент времени. (*)
tcpsessionsCounter	integer	Количество активных TCP сессий на текущий момент времени. (*)
udpsessionsCounter	integer	Количество активных UDP сессий на текущий момент времени. (*)
icmpsessionsCounter	integer	Количество активных ICMP сессий на текущий момент времени. (*)
sessionsRate10	integer	Количество новых сессий в секунду. Среднее значение за последние 10 секунд. (*)
sessionsRate60	integer	Количество новых сессий в секунду. Среднее значение за последние 60 секунд. (*)
sessionsRate300	integer	Количество новых сессий в секунду. Среднее значение за последние 300 секунд. (*)
tcpsessionsRate10	integer	Количество новых TCP сессий в секунду. Среднее значение за последние 10 секунд. (*)
tcpsessionsRate60	integer	Количество новых TCP сессий в секунду. Среднее значение за последние 60 секунд. (*)
tcpsessionsRate300	integer	Количество новых TCP сессий в секунду. Среднее значение за последние 300 секунд. (*)
udpsessionsRate10	integer	Количество новых UDP сессий в секунду. Среднее значение за последние 10 секунд. (*)
udpsessionsRate60	integer	Количество новых UDP сессий в секунду. Среднее значение за последние 60 секунд. (*)
udpsessionsRate300	integer	Количество новых UDP сессий в секунду. Среднее значение за последние 300 секунд. (*)
icmpsessionsRate10	integer	Количество новых ICMP сессий в секунду. Среднее значение за последние 10 секунд. (*)
icmpsessionsRate60	integer	Количество новых ICMP сессий в секунду. Среднее значение за последние 60 секунд. (*)
icmpsessionsRate300	integer	Количество новых ICMP сессий в секунду. Среднее значение за последние 300 секунд. (*)
dnsRequestCounter	integer	Общее количество DNS запросов. (*)
dnsBlockedRequestCounter	integer	Количество заблокированных DNS запросов. (*)
dnsRequestRate	integer	Количество DNS запросов в секунду. (*)
httpRequestCounter	integer	Общее количество HTTP запросов. (*)
httpBlockedRequestCounter	integer	Количество заблокированных HTTP запросов. (*)
httpRequestRate	integer	Количество HTTP запросов в секунду. (*)
dataPartitionFSStatus	string	Состояние файловой системы.
haStatus	integer	Текущее состояние узла кластера.
cpuLoad	integer	Загруженность центрального процессора системы; отображается в %.
memoryUsed	integer	Использование оперативной памяти; отображается в %.
logDiskSpace	integer	Пространство на диске, используемое под журналы; отображается в %.
powerSupply1Status	string	Состояние первого источника питания: - no_power_supplies. - on. - off.

Наименование	Тип данных	Описание
powerSupply2Status	string	Состояние второго источника питания: • no_power_supplies. • on. • off.
raidType	string	Тип RAID массива.
raidStatus	string	Текущий статус RAID (Redundant Array of Independent Disks): • no_raid. • 0 — optimal — массив в оптимальном состоянии. • 1 — degraded — полный или частичный выход из строя одного из дисков. • 2 — rebuild — восстановление массива.
diskIOUtilization	integer	Текущая утилизация диска (%).
diskIOUtilization60	integer	Утилизация диска (%). Среднее значение за последние 60 секунд.
diskIOUtilization300	integer	Утилизация диска (%). Среднее значение за последние 300 секунд.

ПримечаниеМетрики, отмеченные в описании символом (*) не актуальны для *UGMC* и *LogAn/SIEM*. Значения метрик для этих устройств будут всегда равны нулю.

UTM-INTERFACES-MIB

Наименование	Тип данных	Описание
ifNumber	integer	Количество сетевых интерфейсов.
ifIndex	integer	Значение уникально для каждого интерфейса и может принимать значения от 1 до ifNumber.
ifDescr	string	Информация об интерфейсе, которая может включать в себя название производителя, имя продукта, аппаратную версию интерфейса.
ifType	integer	Тип интерфейса, определённый в соответствии с протоколом физического/канального уровней: • 1 — other — неизвестный тип. • 2 — regular1822 — определён в BBN Report 1822. • 3 — hdh1822 — определён в BBN Report 1822. • 4 — ddn-x25 — определён в BBN Report 1822. • 5 — определён в стандарте канального уровня сетевой модели OSI X.25. • 6 — ethernet-csmacd — сетевой интерфейс типа Ethernet, независимо от скорости (определён в RFC 3635). • 7 — iso88023-csmacd — определён в IEEE 802.3. • 8 — iso88024-tokenBus — определён в стандарте IEEE 8802.4. • 9 — iso88025-tokenRing — сетевой интерфейс использует подключение Token Ring; определяется в стандарте IEEE 802.5. • 10 — iso88026-man — определён в стандарте ISO 88026 "MAN". • 11 — starLan — определён в стандарте IEEE 802.3e. • 12 — proteon-10Mbit — Proteon 10 Mbit • 13 — proteon-80Mbit — Proteon 80 Mbit. • 14 — hyperchannel — высокоскоростной канал, используемы в сети ISDN. • 15 — fddi — сетевой интерфейс использует подключение FDDI (Fiber Distributed Data Interface). FDDI — это набор стандартов передачи данных по оптоволоконным линиям в локальной сети. • 16 — lapb — протокол канального уровня, используемым для передачи пакетов стандарта X.25. • 17 — sdlc — протокол канального уровня для системной сетевой архитектуры IBM. • 18 — ds1 — способен обрабатывать 24 одновременных соединения на общей скорости 1,544 Мбит/с; также называется T1 • 19 — e1 — европейский аналог T1. • 20 — basicISDN — для связи аппаратуры абонента и ISDN-станции. • 21 — primaryISDN — используется для подключения к широкополосным магистралям, связывающим местные и центральные АТС или сетевые коммутаторы. • 22 — propPointToPointSerial — определён в стандарте RFC1213. • 23 — ppp — сетевой интерфейс использует подключение PPP (Point-To-Point Protocol). • 24 — softwareLoopback — сетевой интерфейс является петлевым адаптером. Такие интерфейсы часто используются для тестирования; они не отправляют трафик в сеть. • 25 — eon — ConnectionLess Network Protocol (CLNP) over Internet Protocol (IP); определён в ISO/IEC 8473-1. • 26 — ethernet-3Mbit — сетевой интерфейс использует подключение Ethernet со скоростью 3 Мбит/с. Эта версия Ethernet определяется в стандарте IETF RFC 895. • 27 — nsip — XNS over IP — предназначен для использования в разнообразных средах передачи данных. • 28 — slip — сетевой интерфейс использует подключение SLIP (Serial Line Internet Protocol). SLIP определяется в стандарте IETF RFC 1055. • 29 — ultra — ULTRA Technologies. • 30 — ds3 — высокоскоростной интерфейс передачи данных, сформированный мультиплексированием сигналов DS1 и DS2; также называется T3. • 31 — sip — сетевой интерфейс использует подключение SLIP (Serial Line Internet Protocol). SLIP определяется в стандарте IETF RFC 1055. • 32 — frame-relay — обеспечивает возможность передачи данных с коммутацией пакетов через интерфейс между устройствами пользователя и оборудованием сети.
ifMtu	integer	Максимальный размер пакета сетевого уровня, который можно послать через этот интерфейс.
ifSpeed	gauge32	Пропускная способность интерфейса в битах в секунду.
ifPhysAddress	string	Физический адрес интерфейса (MAC-адрес).

Наименование	Тип данных	Описание
ifAdminStatus	integer	Состояние интерфейса, назначаемое администратором: 1 — up — готов для передачи пакетов. 2 — down — не работает. 3 — testing — в режиме тестирования; рабочие пакеты не могут быть переданы.
ifOperStatus	integer	Текущий статус работы интерфейса: 1 — up — интерфейс готов для передачи пакетов. 2 — down — интерфейс не может передавать пакеты данных. 3 — testing — выполняется тестирование сетевого интерфейса; рабочие пакеты не могут быть переданы. 4 — unknown — интерфейс находится в неизвестном состоянии. 5 — dormant — сетевой интерфейс не может передавать пакеты данных, он ожидает внешнее событие. 6 — notPresente — сетевой интерфейс не может передавать пакеты данных из-за отсутствующего компонента, обычно аппаратного. 7 — lowerLayerDown — сетевой интерфейс не может передавать пакеты данных, потому что он работает поверх одного или нескольких других интерфейсов, и не менее одного из этих интерфейсов "нижнего уровня" не работает.
ifLastChange	timeticks	Значение SysUpTime, когда интерфейс оказался в данном состоянии.
ifInOctets	counter32	Количество байтов, принятое данным интерфейсом, включая служебные.
ifInUcastPkts	counter32	Количество доставленных пакетов одноадресной рассылки.
ifInNUcastPkts	counter32	Количество доставленных многоадресных и широковещательных пакетов.
ifInDiscards	counter32	Количество входящих пакетов, которые были отброшены, даже если не было обнаружено ошибок, препятствующих их доставке. Одна из возможных причин отбрасывания: освобождение буферного пространства.
ifInErrors	counter32	Количество входящих пакетов, которые содержат ошибки, препятствующие их доставке.
ifInUnknownProtos	counter32	Количество пакетов, которые были получены через этот интерфейс и отброшены из-за использования неизвестного или неподдерживаемого протокола.
ifOutOctets	counter32	Количество байтов, переданное данным интерфейсом, включая служебные.
ifOutUcastPkts	counter32	Количество отправленных пакетов одноадресной рассылки, включая пакеты, которые были отброшены или не отправлены.
ifOutNUcastPkts	counter32	Количество отправленных многоадресных и широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены.
ifOutDiscards	counter32	Количество исходящих пакетов, которые были отброшены, даже если не было обнаружено ошибок, препятствующих их передаче. Одна из возможных причин отбрасывания: освобождение буферного пространства.
ifOutErrors	counter32	Количество исходящих пакетов, передача которых невозможна вследствие наличия ошибок.
ifOutQLen	gauge32	Длина выходной очереди (в пакетах).
ifInMulticastPkts	counter32	Количество доставленных пакетов многоадресной рассылки.
ifInBroadcastPkts	counter32	Количество доставленных широковещательных пакетов.
ifOutMulticastPkts	counter32	Количество отправленных пакетов многоадресной рассылки, включая пакеты, которые были отброшены или не отправлены.
ifOutBroadcastPkts	counter32	Количество отправленных широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены.
ifHCInOctets	counter64	Смысл одинаков со смыслом объекта ifInOctets — количество байтов, принятое данным интерфейсом, включая служебные; используется счётчик большей ёмкости.
ifHCInUcastPkts	counter64	Смысл одинаков со смыслом объекта ifInUcastPkts — количество доставленных пакетов одноадресной рассылки; используется счётчик большей ёмкости.
ifHCInMulticastPkts	counter64	Смысл одинаков со смыслом объекта ifInMulticastPkts — количество доставленных пакетов многоадресной рассылки; используется счётчик большей ёмкости.
ifHCInBroadcastPkts	counter64	Смысл одинаков со смыслом объекта ifInBroadcastPkts — количество доставленных широковещательных пакетов; используется счётчик большей ёмкости.
ifHCOctets	counter64	Смысл одинаков со смыслом объекта ifOutOctets — количество байтов, переданное данным интерфейсом, включая служебные; используется счётчик большей ёмкости.
ifHCOutUcastPkts	counter64	Смысл одинаков со смыслом объекта ifOutUcastPkts — количество отправленных пакетов одноадресной рассылки, включая пакеты, которые были отброшены или не отправлены; используется счётчик большей ёмкости.
ifHCOutMulticastPkts	counter64	Смысл одинаков со смыслом объекта ifOutMulticastPkts — количество отправленных пакетов многоадресной рассылки, включая пакеты, которые были отброшены или не отправлены; используется счётчик большей ёмкости.
ifHCOutBroadcastPkts	counter64	Смысл одинаков со смыслом объекта ifOutBroadcastPkts — количество отправленных широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены; используется счётчик большей ёмкости.
ifLinkUpDownTrapEnable	integer	Указывает, должен ли создаваться трап при изменении статуса соединения: 1 — enabled — включено. 2 — disabled — отключено.
ifHighSpeed	gauge32	Оценка текущей полосы пропускания интерфейса; указывается в бит/с, кбит/с, Мбит/с, Гбит/с.
ifPromiscuousMode	integer	"Неразборчивый" режим. Может принимать значения: 1 — true — станция принимает все пакеты/кадры независимо от того, кому они адресованы. 2 — false — интерфейс принимает только пакеты/кадры, адресованные этой станции. Значение объекта не влияет на приём широковещательных и многоадресных пакетов/кадров.

Наименование	Тип данных	Описание
ifAlias	string	Название интерфейса, заданное администратором при настройке интерфейса.
ifCounterDiscontinuityTime	timeticks	Значение SysUpTime, когда произошло событие, ставшее причиной сбоя работы одного или более счётчиков интерфейса.

UTM-TEMPERATURE-MIB

Наименование	Тип данных	Описание
termNumber	integer	Количество температурных сенсоров на данной платформе.
thermLowerThreshold	integer	Нижний предел рабочей температуры.
thermUpperThreshold	integer	Верхний предел рабочей температуры.
thermTable	sequence	Таблица температурных сенсоров с показаниями (thermEntry).
thermEntry	sequence	Информация о конкретном сенсоре: - thermName (string) — название сенсора. - thermValue (integer) — показание сенсора. - thermUnit (string) — единица измерения показаний сенсора.

Примечание Данные температурных сенсоров будут отображаться только для поддерживаемых аппаратных платформ. В настоящий момент поддерживаются устройства UserGate C150, C151, FG, X10. Для неподдерживаемых платформ или виртуальных решений таблица сенсоров будет пустой, а значения количества сенсоров и пределы рабочих температур будут равны нулю.

Примечание Если с сенсора не удалось снять показание температуры, он не будет передан в таблице, при этом параметр thermNumber подсчитывает общее количество температурных сенсоров, даже с учётом неработающих. В таком случае количество сенсоров в таблице и значение thermNumber могут не совпадать.

Параметры SNMP

Documentation: ☒
Product: SIEM
Version: 7.x

Данный раздел используется для задания настроек по выдаче информации SNMP-агентом по протоколу SNMP. Параметры SNMP задаются для каждого узла индивидуально.

Наименование	Описание
SNMP имя системы	Название системы, используемое подсистемой управления SNMP.
SNMP локация системы	Информация о физическом расположении SNMP-агента.
SNMP описание системы	Описание системы.
Engine ID	Каждое устройство UserGate SIEM имеет уникальный идентификатор SNMPv3 Engine ID. По умолчанию Engine ID генерируется на основании имени узла UserGate SIEM. При редактировании Engine ID необходимо указать длину, тип и значение идентификатора. Длина может быть определена как фиксированная (не более 8 байт) или динамическая (не более 27 байт). Фиксированная длина идентификатора применима только для типа text. Engine ID может быть сформирован в формате: - IPv4 (ip4). - IPv6 (ipv6). - MAC-адрес (mac). - Текст (text). - Океты (jctets).

Documentation: 
Product: SIEM
Version: 7.x

В данном разделе производится настройка профилей безопасности для аутентификации SNMPv3-менеджера.

Примечание Настройки аутентификации для SNMP v3 (имя пользователя, пароль, тип и алгоритм аутентификации, алгоритм и пароль шифрования) на SNMP-менеджере должны совпадать с настройками SNMP в UserGate SIEM.

Наименование	Описание
Название	Название профиля безопасности SNMP
Описание	Описание профиля безопасности SNMP
Пользователь	Имя пользователя для аутентификации SNMP-менеджера.
Тип аутентификации	Выбор режима аутентификации SNMP-менеджера. Возможны варианты: - Без аутентификации, без шифрования (noAuthNoPriv). - C аутентификацией, без шифрования (authNoPriv). - C аутентификацией, с шифрованием (authPriv). Наиболее безопасным считается режим работы authPriv.
Алгоритм аутентификации	Алгоритм, используемый для аутентификации. Возможно использовать: - SHA1; - MD5; - SHA224; - SHA256; - SHA384; - SHA512.
Пароль аутентификации	Пароль, используемый для аутентификации.
Алгоритм шифрования	Алгоритм, используемый для шифрования. Возможно использовать DES и AES.
Пароль шифрования	Пароль, используемый для шифрования.

Product: SIEM
Version: 7.x
Documentation: 

UserGate SIEM журналирует все события, которые происходят во время его работы и работы подключенных к нему серверов, и записывает их в следующие журналы:

- **Журнал событий** — содержит события, связанные с изменением настроек серверов, подключенных к UserGate SIEM, авторизацией пользователей, администраторов, обновлениями различных списков и т.п.
- **Журнал веб-доступа** — подробный журнал всех веб-запросов, обработанных UserGate SIEM.
- **Журнал DNS** — содержит события, связанные с DNS трафиком.
- **Журнал трафика** — подробный журнал срабатываний правил межсетевого экрана, NAT, DNAT, Port forwarding, Policy-based routing. Для регистрации данных событий необходимо включить журналирование в необходимых правилах межсетевого экрана, NAT, DNAT, Port forwarding, Policy-based routing.
- **Журнал COB** — содержит события, регистрируемые системой обнаружения и предотвращения вторжений.
- **Журнал ACU ТП** — содержит события, регистрируемые правилами контроля ACU ТП.
- **Журнал инспектирования SSH** — журнал срабатывания правил инспектирования SSH. Для регистрации данных событий необходимо включить журналирование.
- **История поиска** — содержит поисковые запросы пользователей в популярных поисковых системах.
- **Журнал событий конечных устройств** — отображает события, получаемые от контролируемых с помощью программного обеспечения UserGate Endpoint конечных устройств, а также события, полученные из контроллера домена AD по WMI.
- **Журнал правил конечных устройств** — события срабатывания правил межсетевого экрана конечных устройств, в настройках которых включено журналирование.
- **Приложения конечных устройств** — отображает приложения, которые когда-либо запускались на конечных устройствах.
- **Аппаратура конечных устройств** — содержит информацию об устройствах, подключённых к конечным устройствам.
- **Журнал syslog** — отображены записи сообщений о событиях удалённых Unix-систем, полученные по протоколу syslog.
- **Журнал защиты почтового трафика** — содержит события срабатывания правил защиты почтового трафика, в настройках которых включено журналирование.
- **Журнал UserID** — содержит описание событий отражающие результат работы UserID агента.
- **Журнал RADIUS** — содержит события, собранные агентом UserID из данных RADIUS accounting.
- **Журнал событий SIEM** — содержит события, связанные с изменением настроек сервера UserGate SIEM, авторизацией пользователей, администраторов, обновлениями различных списков и т.п.

Управление журналами автоматизировано: журналы циклически перезаписываются, обеспечивая необходимое для работы свободное дисковое пространство.

Ротация записей журналов (всех, кроме журнала событий) происходит автоматически по критерию свободного пространства на данном разделе. Записи о ротации базы данных будут отображены в журнале событий UserGate SIEM.

Ротация записей журнала событий не производится.

Documentation: 
Product: SIEM
Version: 7.x

Журнал событий отображает события, связанные с изменением параметров сервера UserGate SIEM, например, добавление, удаление или изменение данных учетной записи, правила или любого другого элемента. Здесь же отображаются все события входа в веб-консоль, авторизации пользователей через Captive-портал и другие.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как диапазон дат, компоненте, важности, типу события.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Documentation: ☒
Product: SIEM
Version: 7.x

Журнал веб-доступа отображает все запросы пользователей в Интернет по протоколам HTTP и HTTPS. Отображается следующая информация:

- Узел UserGate, на котором произошло событие.
- Время события.
- Пользователь.
- Действия.
- Правило.
- Причины (при блокировке сайта).
- URL назначения.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- IP назначения.
- Порт назначения.
- Категории.
- Протокол (HTTP).
- Метод (HTTP).
- Код ответа (HTTP).
- MIME (если присутствует).
- Байт передано/получено.
- Пакетов отправлено.
- Реферер (при наличии).
- Операционная система.
- Useragent Браузера.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как учетная запись пользователя, правило, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Documentation: 
Product: SIEM
Version: 7.x

Журнал DNS отображает события, связанные с DNS трафиком. Для логирования событий DNS на UserGate NGFW должна быть включена DNS-фильтрация в настройках DNS-прокси и разрешено журналирование в правилах контентной фильтрации, в которые будет попадать DNS трафик.

Отображается следующая информация:

- Узел.
- Время.
- Пользователь.
- Правило.
- Причины.
- Имя домена.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- MAC-адрес источника.
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.
- Сетевой протокол.
- Категория URL.
- Информация.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как протокол, диапазон дат, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Product: SIEM
Documentation: 
Version: 7.x

Журнал трафика отображает события срабатывания правил межсетевого экрана или правил NAT, в настройках которых включено журналирование. Отображается следующая информация:

- Узел UserGate, на котором произошло событие.
- Время события.
- Пользователь.
- Действие.
- Правило.
- Приложение.
- Протокол.
- Зона источника.
- Адрес источника.
- Порт источника.
- IP-назначения.
- Порт назначения.
- NAT IP-источника (если это правило NAT).
- NAT порт источника (если это правило NAT).
- NAT IP назначения (если это правило NAT).
- NAT порт назначения (если это правило NAT).
- Байт отправлено/получено.
- Пакетов.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как учетная запись пользователя, правило, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Documentation: 
Product: SIEM
Version: 7.x

Журнал системы обнаружения вторжений отображает сработавшие сигнатуры COB, для которых установлено действие журналировать или блокировать. Отображается следующая информация:

- Файлы Pcap.
- Узел UserGate NGFW, на котором произошло событие.
- Время.
- Содержание события.
- Пользователь.
- Действие.
- Правило.
- Сигнатуры.
- Приложение.
- Сетевой протокол.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- MAC источника.
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.
- MAC назначения.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как протокол, диапазон дат, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Documentation: 
Product: SIEM
Version: 7.x

Журнал АСУ ТП отображает срабатывания правил автоматизированной системы управления технологическим процессом, для которых включена функция журналирования. Отображается следующая информация:

- Узел UserGate NGFW, на котором произошло событие.
- Время.
- Действие.
- Правило.
- Зона источника.
- IP-адрес источника.
- IP-адрес назначения.
- Порт назначения.
- Протокол АСУ ТП.
- Команда АСУ ТП.
- Адрес регистра.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как протокол, диапазон дат, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Documentation: 
Product: SIEM
Version: 7.x

Журнал инспектирования SSH отображает сработавшие правила инспектирования SSH. Отображается следующая информация:

- Узел UserGate, на котором произошло событие.
- Время.
- Пользователь.
- Действие.
- Правило.
- Команда.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- MAC-адрес источника.
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов и в появившемся контекстном меню оставить отмеченными только те столбцы, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как протокол, диапазон дат, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Version: 7.x

Documentation: 

Product: SIEM

В разделе **История поиска** отображаются все поисковые запросы пользователей, для которых настроено журналирование в политиках веб-безопасности. Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как пользователи, диапазон дат, поисковые системы и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Documentation: 
Product: SIEM
Version: 7.x

Журналы конечных устройств отображают информацию, получаемую от контролируемых с помощью программного обеспечения UserGate Client конечных устройств.

В UserGate SIEM имеются следующие журналы:

- **Журнал событий конечных устройств** — отображает события, получаемые от конечных устройств.
- **Журнал правил конечных устройств** — события срабатывания правил межсетевого экрана конечных устройств, в настройках которых включено журналирование.
- **Приложения конечных устройств** — отображает приложения, которые когда-либо запускались на конечных устройствах.
- **Аппаратура конечных устройств** — содержит информацию об устройствах, подключённых к конечным устройствам.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как диапазон дат, важности, типу события и так далее.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Documentation: ☒
Product: SIEM
Version: 7.x

Журнал syslog отображает события, собранные агентом UserID с серверов syslog. В журнале отображаются события входа пользователей в систему и завершение их сеанса работы. Отобрана следующая информация:

Наименование	Описание
Узел	Узел UserGate, на котором зафиксировано событие.
Время	Время произошедшего события.
Запись журнала syslog	Ссылка на событие.
Правило	Правило под которое попало syslog-сообщение.
Критичность	Уровень события syslog.
Объект	Представление процесса, вызвавшего сообщение (kernel messages,user-level messages,security/authentication и тд)
Имя компьютера	Имя компьютера на котором произошло событие.
Приложение	Приложение вызвавшее событие.
Идентификатор процесса	PID процесса вызвавшего событие.
Данные	Описание события.

Documentation: 
Product: SIEM
Version: 7.x

Журнал защиты почтового трафика отображает события срабатывания правил защиты почтового трафика, в настройках которых включено журналирование. Отображается следующая информация:

- Узел UserGate, на котором произошло событие.
- Время срабатывания.
- Пользователь.
- Отправитель.
- Получатель
- Правило.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.
- Приложение.
- Протокол прикладного уровня.
- Байт отправлено/получено.
- Пакетов отправлено/получено.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как протокол, диапазон дат, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Documentation: ☒
Product: SIEM
Version: 7.x

Журнал UserID содержит описание событий отражающие результат работы UserID агента. Отображена следующая информация:

Наименование	Описание
Узел	Узел UserGate, на котором зафиксировано событие
Время	Время произошедшего события
Действие	Действие, примененное к событию
Источник логов	Источник полученного события
Пользователь	Пользователь UG, который вызвал событие
IP-адрес	IP-адрес узла, на котором произошло событие
Информация	Описание события

Documentation: ☒
Product: SIEM
Version: 7.x

Журнал RADIUS отображает события, собранные агентом UserID из данных RADIUS accounting. В журнале отображаются события входа пользователей в систему и завершение их сеанса работы. Отображена следующая информация:

Наименование	Описание
Узел	Узел UserGate, на котором зафиксировано событие
Время	Время произошедшего события
Идентификатор правила	Идентификатор правила, срабатывание которого создало событие
Пользователь	Пользователь, который вызвал событие
Группы	Строка групп, в которых состоит пользователь
Статус соединения	Текущий статус соединения
IP источника	IP-адрес источника, откуда пришло сообщение
IP адрес NAS	IP-адрес NAS, авторизовавшего пользователя
IP-адрес пользователя	IP-адрес пользователя (framed ip address)

Documentation: ☒
Product: SIEM
Version: 7.x

Функция экспортирования журналов UserGate SIEM позволяет выгружать информацию на внешние серверы для последующего анализа или для обработки.

UserGate SIEM поддерживает выгрузку следующих журналов:

- Журнал DNS.
- Журнал событий.
- Журнал веб-доступа.
- Журнал COB.
- Журнал АСУ ТП.
- Журнал инспектирования SSH.
- Журнал трафика.
- Журнал событий конечных устройств.
- Журнал правил конечных устройств.
- Приложения конечных устройств.
- Аппаратура конечных устройств.

Поддерживается отправка журналов на серверы SSH (SFTP), FTP и syslog. Отправка на серверы SSH и FTP проводится по указанному в конфигурации расписанию или разово (кнопка **Послать разово**). Отправка на серверы syslog происходит сразу же при добавлении записи в журнал.

Для отправки журналов необходимо создать конфигурации экспорта журналов в разделе **Экспорт журналов**.

При создании конфигурации требуется указать следующие параметры:

Наименование	Описание
Название правила	Название правила экспорта журналов.
Описание	Оptionальное поле для описания правила.
Параметры разового экспорта	Выбор диапазона экспорта журналов.
Журналы для экспорта	Выбор файлов журналов, которые необходимо экспортировать: • Журнал DNS. • Журнал событий. • Журнал веб-доступа. • Журнал COB. • Журнал АСУ ТП. • Журнал инспектирования SSH. • Журнал трафика. • Журнал событий конечных устройств. • Журнал правил конечных устройств. • Приложения конечных устройств. • Аппаратура конечных устройств. Для каждого из журналов возможно указать синтаксис выгрузки: • CEF — Common Event Format (ArcSight). • JSON — JSON format. • @CEE: JSON — CEE Log Syntax (CLS) Encoding JSON. Обратитесь к документации на используемую систему SIEM для выбора необходимого формата выгрузки журналов. Подробное описание форматов журналов читайте в приложении Описание форматов журналов.
Тип сервера	SSH (SFTP), FTP, syslog.
Адрес сервера	IP-адрес или доменное имя сервера.
Транспорт	Только для типа серверов syslog — TCP или UDP.
Порт	Порт сервера, на который следует отправлять данные.
Протокол	Только для типа серверов syslog — RFC5424 или BSD syslog RFC 3164. Выберите протокол, совместимый с используемой системой SIEM.
Критичность	Только для типа серверов syslog. Необязательное поле, проконсультируйтесь с документацией на используемую систему SIEM. Возможны следующие значения: • Тревога: состояние, требующее незамедлительного вмешательства. • Критическая: состояние, требующее незамедлительного вмешательства либо предупреждающее о сбое в системе. • Ошибки: в системе возникли ошибки. • Предупреждения: предупреждения о возможном возникновении ошибок, если не будут предприняты никакие действия. • Уведомительная: события, которые относятся к необычному поведению системы, но не являются ошибками. • Информативная: информационные сообщения.

Наименование	Описание
Объект	Только для типа серверов syslog. Необязательное поле, проконсультируйтесь с документацией на используемую систему SIEM. Возможны следующие значения: • Сообщения пользовательские. • Системный сервис. • Безопасность/авторизация. • Аудит. • Тревога. • Local 0. • Local 1. • Local 2. • Local 3. • Local 4. • Local 5. • Local 6. • Local 7.
Имя хоста	Только для типа серверов syslog. Уникальное имя хоста, идентифицирующее сервер, отправляющий данные на сервер syslog, в формате Fully Qualified Domain Name (FQDN).
App-Name	Только для типа серверов syslog. Уникальное имя приложения, которое отправляет данные на сервер syslog.
Логин	Имя учетной записи для подключения к удаленному серверу. Не применяется к методу отправки syslog.
Пароль	Пароль учетной записи для подключения к удаленному серверу. Не применяется к методу отправки syslog.
Повторите пароль	Подтверждение пароля учетной записи для подключения к удаленному серверу. Не применяется к методу отправки syslog.
Путь на сервере	Каталог на сервере для копирования файлов журналов. Не применяется к методу отправки syslog.
Расписание	Выбор расписания для отправки логов. Не применяется к методу отправки syslog. Возможны варианты: • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать cronTab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "/" в поле "часы" будет означать "каждые два часа".

Documentation: ☒
Product: SIEM
Version: 7.x
Technology: SIEM

Правила нормализации логов позволяют приводить к единому виду данные, полученные UserGate SIEM с различных источников (сенсоров).

Логи, поступающие с различных сенсоров в UserGate SIEM, могут обрабатываться с помощью регулярных выражений, указанных в правилах пользовательской нормализации. В результате данные, найденные в логах, будут записаны в стандартные поля базы данных UserGate SIEM.

Порядок выполнения правил нормализации задается администратором в разделе **Журналы и отчеты → Журналы → Пользовательская нормализация логов**. Последующие правила могут перезаписать значения, нормализованные и записанные предыдущими. Менять расположение правила можно перетаскиванием правила с помощью мыши, или с помощью кнопок меню: **Вниз**, **Наверх**, **Выше**, **Ниже**.

Источники логов и их поля, которые можно дополнительно нормализовать:

Журнал событий конечных устройств	Syslog
Конечное устройство (sensorName)	Правило (ruleName)
Данные (data)	Имя компьютера (computerName)
Статус (status)	Приложение (applicationName)
Источник журнала событий (sourceName)	Идентификатор процесса (processId)
Категория инцидента (logCategoryString)	Данные (data)
Имя компьютера (computerName)	
Пользователь (userName)	
Строка вставки (insertionString)	
Файл журнала лог (logFile)	

Список полей базы данных UserGate SIEM, в которые можно сохранять найденные данные (т.е. использовать эти названия полей в регулярных выражениях в правилах нормализации):

Название	Тип
node	string
userId	guid
user	string
ruleId	guid
rule	string
ipSource	ip
ipDest	ip
portSource	integer16
portDest	integer16
macSource	mac
macDest	mac
natIpSource	ip
natIpDest	ip
natPortSource	integer16
natPortDest	integer16
applicationName	string
bytesSent	integer64
bytesRecv	integer64
packetsSent	integer64
packetsRecv	integer64
mime	string
httpMethod	string

Название	Тип
referer	url
url	url
statusCode	integer16
userAgent	string
sensor	string
sensorId	guid
processId	string
networkProtocol	ip protocol
status	string
error	integer
counterId	guid
logCategory	integer16
taskCategory	string
computerName	string
logEventCode	integer16
logEventId	integer16
logEventType	integer16
logFile	string
severity	severity
module	string
component	string
event	string
syslogFacility	integer8
syslogSeverity	integer8
image	string
cmdLine	string
originalFileName	string
parentProcessId	integer64
parentImage	string
parentCommandLine	string
targetObject	string
targetFilename	string
scriptBlockText	string
queryName	string
queryResults	string
workstationName	string
logonId	string
imageLoaded	string
sourceImage	string
targetImage	string
customString1	string
...	string

Название	Тип
customString15	string
customNumber1	string
...	string
customNumber5	string
customIp1	ip
customIp2	ip
customDate1	date
customDate2	date

Типы полей:

Тип	Значение по умолчанию	Описание
string	""	Строка любой длины.
guid	00000000-0000-0000-0000-000000000000	Строка вида XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX, где X - шестнадцатиричная цифра (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f, A, B, C, D, E, F).
ip	0.0.0.0	Строка вида X.X.X.X, где X = 0..255; или X:X:X:X:X:X:X, где X = 4-значное шестнадцатиричное число.
integer	0	Любое целое неотрицательное число.
url	""	Строка URL, формат в RFC1738.
ip protocol	255	Число 0 .. 255 или строка из списка протоколов ниже.
severity	unknown	Строки: unknown, critical, error, info, warning.
integer8	0	Целое число в интервале [0, 255].
integer16	0	Целое число в интервале [0, 65535].
integer64	0	Целое число в интервале [0, 2^64-1].
date	1970-01-01T00:00:00	2024-03-06T10:30:00.

Список протоколов, допустимых для поля networkProtocol (буквы могут быть в любом регистре):

Название	Значение
IP	0
ICMP	1
IGMP	2
GGP	3
IP-ENCAP	4
ST	5
TCP	6
CBT	7
EGP	8
IGP	9
BBN-RCC-MON	10
NVP-II	11
PUP	12
ARGUS	13
EMCON	14
XNET	15
CHAOS	16
UDP	17
MUX	18

Название	Значение
DCN-MEAS	19
HMP	20
PRM	21
XNS-IDP	22
TRUNK-1	23
TRUNK-2	24
LEAF-1	25
LEAF-2	26
RDP	27
IRTP	28
ISO-TP4	29
NETBLT	30
MFE-NSP	31
MERIT-INP	32
DCCP	33
3PC	34
IDPR	35
XTP	36
DDP	37
IDPR-CMTP	38
TP++	39
IL	40
IPV6	41
SDRP	42
IPV6-ROUTE	43
IPV6-FRAG	44
IDRP	45
RSVP	46
GRE	47
DSR	48
BNA	49
IPSEC-ESP	50
IPSEC-AH	51
I-NLSP	52
SWIPE	53
NARP	54
MOBILE	55
TLSP	56
SKIP	57
IPV6-ICMP	58
IPV6-NONXT	59
IPV6-OPTS	60

Название	Значение
ANY HOST INTERNAL PROTOCOL	61
CFTP	62
ANY LOCAL NETWORK	63
SAT-EXPAK	64
KRYPTOLAN	65
RVD	66
IPPC	67
ANY DISTRIBUTED FILE SYSTEM	68
SAT-MON	69
VISA	70
IPCU	71
CPNX	72
CPHB	73
WSN	74
PVP	75
BR-SAT-MON	76
SUN-ND	77
WB-MON	78
WB-EXPAK	79
ISO-IP	80
VMTP	81
SECURE-VMTP	82
VINES	83
IPTM	84
NSFNET-IGP	85
DGP	86
TCF	87
EIGRP	88
OSPFIGP	89
SPRITE-RPC	90
LARP	91
MTP	92
AX.25	93
IPIP	94
MICP	95
SCC-SP	96
ETHERIP	97
ENCAP	98
ANY PRIVATE ENCRYPTION SCHEME	99
GMTP	100
IFMP	101
PNNI	102

Название	Значение
PIM	103
ARIS	104
SCPS	105
QNX	106
A/N	107
IPCOMP	108
SNP	109
COMPAQ-PEER	110
IPX-IN-IP	111
VRRP	112
PGM	113
ANY 0-HOP PROTOCOL	114
L2TP	115
DDX	116
IATP	117
STP	118
SRP	119
UTI	120
SMP	121
SM	122
PTP	123
IS-IS OVER IPV4	124
FIRE	125
CRTP	126
CRUDP	127
SSCOPMCE	128
IPLT	129
SPS	130
PIPE	131
SCTP	132
FC	133
RSVP-E2E-IGNORE	134
MOBILITY HEADER	135
UDPLITE	136
MPLS-IN-IP	137
MANET	138
HIP	139
SHIM6	140
WESP	141
ROHC	142
USE FOR EXPERIMENTATION AND TESTING	254
RESERVED	255

Для создания правила нормализации необходимо в разделе **Журналы и отчеты → Журналы → Пользовательская нормализация логов** нажать **Добавить** и в открывшемся окне заполнить следующие поля:

Наименование	Описание
Включено	Включение/выключение правила пользовательской нормализации логов.
Название	Название правила пользовательской нормализации логов.
Описание	Описание правила пользовательской нормализации логов.
Категория	Выбор категории (типа) логов, для которых применяется данное правило: - Журнал событий конечных устройств; - Syslog.
Столбец с данными	Выбор столбца, из которого будут извлекаться данные.
Регулярное выражение	Строка регулярного выражения с группами, названия которых совпадают со столбцами, куда будут записываться значения.

Пример создания правила, которое обрабатывает логи категории syslog, извлекает из них имя пользователя, ip, port и записывает их в соответствующие поля базы данных UserGate SIEM:

Свойства правила пользовательской нормализации логов

Включено:

☒

Название:

Syslog1

Описание:

Категория:

Syslog

Столбец с данными:

Данные

Регулярное выражение:

.+Accepted.+for\s(?:<user>[A-Za-z0-9]+\)\sfrom\s(?:<ipSource>[0-9]+\)\sport\s(?:<portSource>[0-9]+\)

Сохранить

Отмена

Правила пользовательской нормализации могут быть экспортированы в бинарный файл, или импортированы в систему с помощью кнопок **Экспорт/Импорт** в меню инструментов раздела **Журналы и отчеты → Журналы → Пользовательская нормализация логов** (доступно в версии ПО 7.4.0 и выше):

В UserGate SIEM имеется встроенная библиотека правил нормализации логов, которая содержит созданные разработчиками UserGate референсные правила нормализации. Правила из библиотеки могут быть импортированы в раздел пользовательской нормализации логов и использованы для создания собственных правил. Подробнее о библиотеке правил — в разделе [Правила нормализации логов](#).

Documentation: 

Product: SIEM

Version: 7.x

Количество записей, регистрируемых в журналах, как правило, очень велико, и UserGate SIEM предоставляет удобные способы поиска и фильтрации необходимой информации. Администратор может использовать простой и расширенный поиск по содержанию журналов.

При использовании простого поиска администратор использует графический интерфейс, чтобы задать фильтрацию по значениям требуемых полей журналов, отфильтровывая таким образом ненужную информацию. Например, администратор может задать интересующий его диапазон времени, список пользователей, категорий и т.п. Задание критериев поиска интуитивно понятно и не требует специальных знаний.

Построение более сложных фильтров возможно в режиме расширенного поиска с использованием специального языка запросов. В режиме расширенного поиска можно строить запросы с использованием полей журналов, которые недоступны в базовом режиме. Для формирования запросов используются названия полей, значения полей, ключевые слова и операторы. Значения полей могут быть введены с использованием одинарных или двойных кавычек, или без них, если значения не содержат пробелов. Для группировки нескольких условий можно использовать круглые скобки. Подробнее — в приложении [«Синтаксис языка запросов»](#).

Documentation: ☒
Product: SIEM
Version: 7.x

Формат журнала событий

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	events
	Origin	Модуль, в котором произошло событие.	admin_console
	Severity	Важность события.	Может принимать значения: • 1 — информационные. • 4 — предупреждения. • 7 — ошибки. • 10 — критичные.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	act	Тип события.	login_successful
	suser	Имя пользователя.	Admin
	src	IPv4-адрес источника.	192.168.117.254
	cat	Компонент, в котором произошло событие.	console_auth
	cs1Label	Поле используется для указания деталей события.	Attributes
	cs1	Детали события в формате JSON.	{"name":"MIME_BUILTIN_COMPOSITE","module":"nlist_import"}

Формат журнала веб-доступа

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	webaccess
	Name	Тип источника.	log
	Threat Level	Уровень угрозы категории URL.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	captive
	reason	Причина, по которой было создано событие, например, причина блокировки сайта.	{"id":39,"name":"Social Networking","threat_level":3}
	proto	Используемый протокол 4-го уровня.	TCP.
	app	Протокол прикладного уровня и его версия.	HTTP/1.1
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	requestMethod	Метод, используемый для доступа к URL-адресу (POST, GET и т.п.).	GET

Тип поля	Название поля	Описание	Пример значения
	request	В случае HTTP-запроса поле содержит URL-адрес запрашиваемого ресурса с указанием используемого протокола.	http://www.secure.com
	requestContext	URL источника запроса (реферер HTTP).	https://www.google.com/
	requestClientApplication	Useragent пользовательского браузера.	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	40
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Default Allow
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)
	cs6Label	Поле указывает было ли содержимое расшифровано.	Decrypted
	cs6	Расшифровано или нет.	true, false
	flexString1Label	Поле указывает на тип контента.	Media type
	flexString1	Тип контента.	text/html
	flexString2Label	Поле указывает на категорию запрашиваемого URL-адреса.	URL Categories
	flexString2	Категория URL.	Computers & Technology
	cn1Label	Поле используется для указания количества переданных пакетов в направлении источник — назначение.	Packets sent
	cn1	Количество переданных пакетов в направлении источник — назначение.	3
	cn2Label	Поле используется для указания количества переданных пакетов в направлении назначение — источник.	Packets received
	cn2	Количество переданных пакетов в направлении назначение — источник.	1
	cn3Label	Поле указывает исходный ответ сервера.	Response
	cn3	Код ответа HTTP.	302

Формат журнала веб-доступа **CEF Compact**:

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	webaccess
	Name	Тип источника.	log
	Threat Level	Уровень угрозы категории URL.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknowп, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	captive
	reason	Причина, по которой было создано событие, например, причина блокировки сайта.	{"id":39,"name":"Social Networking","threat_level":3}

Тип поля	Название поля	Описание	Пример значения
	proto	Используемый протокол 4-го уровня.	TCP.
	app	Протокол прикладного уровня и его версия.	HTTP/1.1
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	requestMethod	Метод, используемый для доступа к URL-адресу (POST, GET и т.н.).	GET
	request	В случае HTTP-запроса поле содержит URL-адрес запрашиваемого ресурса с указанием используемого протокола.	http://www.secure.com
	requestContext	URL источника запроса (реферер HTTP).	https://www.google.com/
	requestClientApplication	Useragent пользовательского браузера.	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	40
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Default Allow
	cs2Label	Поле используется для индикации зоны источника.	SrcZone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для индикации зоны назначения.	DstZone
	cs3	Название зоны назначения.	Untrusted
	flexString1Label	Поле указывает на категорию запрашиваемого URL-адреса.	URLCats
	flexString1	Категория URL.	Computers & Technology
	cn1Label	Поле указывает исходный ответ сервера.	Response
	cn1	Код ответа HTTP.	302

ПримечаниеОбщее правило для компактного формата — значения некоторых полей обрезаются по длине до 80 символов. Например, список url-категорий, url, имя пользователя, имя правила, имя зоны, и т.д.

Формат журнала DNS

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	dns
	Name	Тип источника.	log
	Threat Level	Уровень угрозы категории URL.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1701085036026
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorereaeda
	act	Действие, принятое устройством в соответствии с настроенными политиками.	block
	reason	Причина, по которой было создано событие, например, url категория, на которых сработало правило.	{"url_cats":[{"id":"37","name":"Search Engines & Portals","threat_level":1}]}
	proto	Используемый протокол 4-го уровня.	UDP
	dhost	Имя хоста назначения, адрес которого определяется с помощью DNS сервера.	google.com
	app	Протокол прикладного уровня.	DNS
	suser	Имя пользователя.	user1 (Unknown, если пользователь неизвестен)

Тип поля	Название поля	Описание	Пример значения
	src	IPv4 источника трафика.	10.10.0.11
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	smac	MAC-адрес источника.	FA:16:3E:65:1C:B4
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535. Для DNS обычно используется порт 53.
	cs1Label	Поле используется для указания сработавшего правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Rule1
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)
	cs6Label	Поле используется для указания передаваемых данных.	Data
	cs6	Передаваемые данные.	{"question":{"domain":"google.com","type":"A","class":"IN"}, "answer":{"domain":"google.com","type":"TXT","class":"IN","ttl":5,"data":"Blocked"}, {"domain":"google.com","type":"A","class":"IN","ttl":5,"data":"10.10.0.1"}}
	flexString1Label	Поле указывает на категорию запрашиваемого URL-адреса.	URL Categories
	flexString1	Категория URL.	Search Engines & Portals

Формат журнала DNS CEF Compact:

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	dns
	Name	Тип источника.	log
	Threat Level	Уровень угрозы категории URL.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1701085036026
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorereaeda
	act	Действие, принятое устройством в соответствии с настроенными политиками.	block
	reason	Причина, по которой было создано событие, например, url категория, на которых сработало правило.	{"url_cats":{"id":37,"name":"Search Engines & Portals","threat_level":1}}
	proto	Используемый протокол 4-го уровня.	UDP
	dhost	Имя хоста назначения, адрес которого определяется с помощью DNS сервера.	google.com
	app	Протокол прикладного уровня.	DNS
	suser	Имя пользователя.	user1 (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.0.11
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	smac	MAC-адрес источника.	FA:16:3E:65:1C:B4
	dst	IPv4 адрес назначения трафика.	194.226.127.130

Тип поля	Название поля	Описание	Пример значения
	dpt	Порт назначения.	Может принимать значения от 0 до 65535. Для DNS обычно используется порт 53.
	cs1Label	Поле используется для указания сработавшего правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Rule 1
	cs2Label	Поле используется для индикации зоны источника.	SrcZone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для индикации зоны назначения.	DstZone
	cs3	Название зоны назначения.	Untrusted
	cs4Label	Поле используется для указания передаваемых данных.	Data
	cs4	Передаваемые данные.	{"question":{"domain":"google.com","type":"A","class":"IN"}, "answer":{"domain":"google.com","type":"TXT","class":"IN","ttl":5,"data":"Blocked"}, {"domain":"google.com","type":"A","class":"IN","ttl":5,"data":"10.10.0.1"}}
	flexString1Label	Поле указывает на категорию запрашиваемого URL-адреса.	URLCats
	flexString1	Категория URL.	Search Engines & Portals

Формат журнала трафика

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	traffic
	Rule Type	Тип правила, срабатывание которого вызвало событие.	firewall
	Threat Level	Уровень угрозы приложения.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	proto	Используемый протокол 4-го уровня.	TCP или UDP
	app	Имя сработавшего приложения	my_app
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	smac	MAC-адрес источника.	00:50:56:80:28:08
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	dmac	MAC-адрес назначения.	00:50:56:80:7D:21
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	40
	sourceTranslatedAddress	Адрес источника после переназначения (если настроены правила NAT).	192.168.174.134 (0.0.0.0 — если нет)
	sourceTranslatedPort	Порт источника после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (0 — если нет)
	destinationTranslatedAddress	Адрес назначения после переназначения (если настроены правила NAT).	192.226.127.130 (0.0.0.0 — если нет)
	destinationTranslatedPort	Порт назначения после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (0 — если нет)
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Allow trusted to untrusted

Тип поля	Название поля	Описание	Пример значения
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)
	cn1Label	Поле используется для указания количества переданных пакетов в направлении источник — назначение.	Packets sent
	cn1	Количество переданных пакетов в направлении источник — назначение.	3
	cn2Label	Поле используется для указания количества пакетов, переданных в направлении назначение — источник.	Packets received
	cn2	Количество пакетов, переданных в направлении назначение — источник.	1

Формат журнала трафика CEF Compact:

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	traffic
	Rule Type	Тип правила, срабатывание которого вызвало событие.	firewall
	Threat Level	Уровень угрозы приложения.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	proto	Используемый протокол 4-го уровня.	TCP или UDP
	app	Имя сработавшего приложения	my_app
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	smac	MAC-адрес источника.	00:50:56:80:28:08
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	dmac	MAC-адрес назначения.	00:50:56:80:7D:21
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	40
	sourceTranslatedAddress	Адрес источника после переназначения (если настроены правила NAT).	192.168.174.134 (0.0.0.0 — если нет)
	sourceTranslatedPort	Порт источника после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (0 — если нет)
	destinationTranslatedAddress	Адрес назначения после переназначения (если настроены правила NAT).	192.226.127.130 (0.0.0.0 — если нет)
	destinationTranslatedPort	Порт назначения после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (0 — если нет)
	cs1Label	Поле используется для указания срабатывания правила.	Rule

Тип поля	Название поля	Описание	Пример значения
	cs1	Название правила, срабатывание которого вызвало событие.	Allow trusted to untrusted
	cs2Label	Поле используется для индикации зоны источника.	SrcZone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для индикации зоны назначения.	DstZone
	cs3	Название зоны назначения.	Untrusted

Формат журнала COB

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	idps
	Signature	Название сработавшей сигнатуры COB.	BlackSun Test
	Threat Level	Уровень угрозы сигнатуры.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	proto	Используемый протокол 4-го уровня.	TCP или UDP
	app	Протокол прикладного уровня.	HTTP
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	40
	msg	Уровень угрозы сигнатуры и её название.	[2] BlackSun
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	IDPS Rule Example
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)

Формат журнала COB CEF Compact:

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate

Тип поля	Название поля	Описание	Пример значения
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	idps
	Signature	Название сработавшей сигнатуры COB.	BlackSun Test
	Threat Level	Уровень угрозы сигнатуры.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	proto	Используемый протокол 4-го уровня.	TCP или UDP
	app	Протокол прикладного уровня.	HTTP
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	40
	msg	Уровень угрозы сигнатуры и её название.	[2] BlackSun
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	IDPS Rule Example

Формат журнала АСУ ТП

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	scada
	Name	Тип источника.	log
	PDU Severity	Критичность АСУ ТП.	Может принимать значения: 1 — очень низкий. 2 — низкий. 3 — средний. 4 — высокий. 5 — очень высокий.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	app	Протокол прикладного уровня.	Modbus
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.

Тип поля	Название поля	Описание	Пример значения
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Scada Rule Example
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)
	cs6Label	Поле указывает на информацию об устройстве.	PDU Details
	cs6	Информация об устройстве в формате JSON.	{"protocol":"modbus","pdu_severity":0,"pdu_func":"3","pdu_address":0,"mb_value":0,"mb_quantity":0,"mb_payload":"AAIAAA==", "mb_message":"response","mb_addr":0}

Формат журнала инспектирования SSH

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	ssh
	Name	Тип источника.	log
	Threat Level	Уровень угрозы приложения.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unkown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	app	Протокол прикладного уровня.	SSH или SFTP
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	smac	MAC-адрес источника.	FA:16:3E:65:1C:B4
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	SSH inspection rule
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)

Тип поля	Название поля	Описание	Пример значения
	cs6Label	Указание на команду, передаваемую по SSH.	Command
	cs6	Команда, передаваемая по SSH, в формате JSON.	whoami

Формат журнала инспектирования SSH CEF Compact:

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	ssh
	Name	Тип источника.	log
	Threat Level	Уровень угрозы приложения.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	app	Протокол прикладного уровня.	SSH или SFTP
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	smac	MAC-адрес источника.	FA:16:3E:65:1C:B4
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	SSH inspection rule
	cs2Label	Поле используется для индикации зоны источника.	SrcZone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для индикации зоны назначения.	DstZone
	cs3	Название зоны назначения.	Untrusted
	cs4Label	Указание на команду, передаваемую по SSH.	Command
	cs4	Команда, передаваемая по SSH, в формате JSON.	whoami

Формат журнала защиты почтового трафика

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	mailsecurity
	Name	Тип источника.	log
	Threat Level	Уровень угрозы приложения.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@einsonstal
	act	Действие, выполненное устройством в соответствии с настроенными политиками.	mark

Тип поля	Название поля	Описание	Пример значения
	app	Протокол прикладного уровня.	SMTP
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4-адрес источника.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	dst	IPv4-адрес назначения.	10.10.10.10
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	10
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	10
	cs1Label	Поле используется для указания названия правила.	Rule
	cs1	Название правила защиты почтового трафика.	Mail security rule
	cs2Label	Поле используется для указания зоны источника.	Source Zone
	cs2	Зона источника.	Untrusted
	cs3Label	Поле используется для индикации страны источника трафика.	Source Country
	cs3	Страна источника трафика.	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для указания зоны назначения трафика.	Destination Zone
	cs4	Название зоны назначения трафика.	Untrusted
	cs5Label	Поле используется для индикации страны назначения трафика.	Destination Country
	cs5	Страна назначения.	RU (отображается двухбуквенный код страны)
	cs6Label	Поле используется для указания почтового адреса получателя.	To
	cs6	Email получателя.	receiver@example.com
	flexString1Label	Поле используется для указания почтового адреса отправителя.	From
	flexString1	Email отправителя.	sender@example.com
	cn1Label	Поле используется для указания количества переданных пакетов в направлении источник — назначение.	Packets sent
	cn1	Количество переданных пакетов в направлении источник — назначение.	3
	cn2Label	Поле используется для указания количества переданных пакетов в направлении назначение — источник.	Packets received
	cn2	Количество переданных пакетов в направлении назначение — источник.	1

Формат журнала защиты почтового трафика **CEF Compact**:

Тип поля	Название поля	Описание	Пример значения
CEF заголовков	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	mailsecurity
	Name	Тип источника.	log
	Threat Level	Уровень угрозы приложения.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@einsonstal
	act	Действие, выполненное устройством в соответствии с настроенными политиками.	mark
	app	Протокол прикладного уровня.	SMTP

Тип поля	Название поля	Описание	Пример значения
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4-адрес источника.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	dst	IPv4-адрес назначения.	10.10.10.10
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	10
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	10
	cs1Label	Поле используется для указания названия правила.	Rule
	cs1	Название правила защиты почтового трафика.	Mail security rule
	cs2Label	Поле используется для указания зоны источника.	SrcZone
	cs2	Зона источника.	Untrusted
	cs4Label	Поле используется для указания зоны назначения трафика.	DstZone
	cs4	Название зоны назначения трафика.	Untrusted
	cs5Label	Поле используется для указания почтового адреса отправителя.	From
	cs5	Email отправителя.	sender@example.com
	cs6Label	Поле используется для указания почтового адреса получателя.	To
	cs6	Email получателя.	receiver@example.com

Формат журнала событий конечных устройств

Тип поля	Название поля	Описание	Пример значения
CEF заголовков	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	endpoint_log
	Name	Тип источника.	log
	Severity	Важность события.	Может принимать значения: 1 — error; 2 — warning; 3 — info; 4 — audit success; 5 — audit failure.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Идентификатор устройства, сгенерировавшего это событие.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	msg	Подробная информация о событии.	Состояние Windows Defender успешно изменено на SECURITY_PRODUCT_STATE_ON.
	suser	Имя пользователя.	Admin
	cs1Label	Поле используется для указания идентификатора конечного устройства.	endpointId
	cs1	Идентификатор конечного устройства или сенсора.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	cs2Label	Поле используется для индикации имени конечного устройства или сенсора.	endpointName
	cs2	Имя конечного устройства или сенсора.	DESKTOP-0731NFQ
	cs3Label	Поле используется для указания на тип события.	logLevel
	cs3	Тип события.	Аудит успеха, Предупреждение, Сведения, Аудит отказа, Ошибка
	cs4Label	Поле используется для указания категории события.	logCategoryString
	cs4	Категория события.	Special Logon

Тип поля	Название поля	Описание	Пример значения
	cs5Label	Поле используется для индикации типа журнала.	logFile
	cs5	Тип журнала, содержащего важную информацию о программных и аппаратных событиях.	Security (файл журнала безопасности), Application (файл журнала приложений), System (файл системного журнала), Windows PowerShell
	cs6Label	Поле используется для указания на источник журнала событий.	sourceName
	cs6	Источник журнала событий.	Microsoft-Windows-Security-Auditing
	cn1Label	Поле используется для индикации кода события журнала.	logEventCode
	cn1	Код события журнала.	1154
	cn2Label	Поле используется для указания на идентификатор события.	logEventId
	cn2	Идентификатор события.	10016
	cn3Label	Поле используется для индикации типа события лога.	logEventType
	cn3	Тип события лога.	1 (error), 2 (warning), 3 (information), 4 (audit success), 5 (audit failure).
	flexString1Label	Поле используется для индикации строки вставки.	insertionString
	flexString1	Строка вставки - данные блока eventData события Windows.	Windows DefenderSECURITY_PRODUCT_STATE_ON

Формат журнала правил конечных устройств

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	endpoint_log
	Name	Тип источника.	log
	Threat Level	Уровень угрозы категории URL.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Идентификатор устройства, сгенерировавшего это событие.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	proto	Используемый протокол 4-го уровня.	TCP
	shost	Имя хоста.	www.google.com
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	filePath	Приложение, к которому было применено правило межсетевого экрана.	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
	cs1Label	Поле используется для указания идентификатора конечного устройства.	endpointId
	cs1	Идентификатор конечного устройства или сенсора.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	cs2Label	Поле используется для указания на имя NetBIOS конечного устройства.	endpointName
	cs2	Имя NetBIOS конечного устройства.	DESKTOP-0731NFQ
	cs3Label	Поле используется для указания правила, срабатывание которого создало запись в журнале.	Rule
	cs3	Название правила.	Test rule name
	flexString1Label	Поле указывает на тип контента.	Media type
	flexString1	Тип контента.	text/html
	flexString2Label	Поле указывает на категорию запрашиваемого URL-адреса.	Categories
	flexString2	Категория URL.	Computers & Technology

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	endpoint_log
	Name	Тип источника.	log
	Threat Level	Уровень угрозы категории URL.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	165234423822
	deviceExternalId	Идентификатор устройства, сгенерировавшего это событие.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	proto	Используемый протокол 4-го уровня.	TCP
	shost	Имя хоста.	www.google.com
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	filePath	Приложение, к которому было применено правило межсетевого экрана.	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
	cs1Label	Поле используется для указания идентификатора конечного устройства.	endpointId
	cs1	Идентификатор конечного устройства или сенсора.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	cs2Label	Поле используется для указания на имя NetBIOS конечного устройства.	endpointName
	cs2	Имя NetBIOS конечного устройства.	DESKTOP-0731NFQ
	cs3Label	Поле используется для указания правила, срабатывание которого создало запись в журнале.	Rule
	cs3	Название правила.	Test rule name

Формат журнала приложений конечных устройств

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	endpoint_applications
	Name	Тип источника.	log
	Threat Level	Значение по умолчанию.	0
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	165234423822
	deviceExternalId	Идентификатор устройства, сгенерировавшего это событие.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	act	Действие (запуск или остановка приложения).	start, stop
	suser	Пользователь.	DESKTOP-0731NFQ\User
	filePath	Расположение файла.	C:\Windows\system32\cmd.exe
	spid	Идентификатор процесса.	3860
	fileHash	Хэш приложения.	B4979A9F970029889713D756C3F123643DDE73DA
	cs1Label	Поле используется для указания идентификатора конечного устройства.	endpointId
	cs1	Идентификатор конечного устройства.	35fb5820-74db-4eac-b05b-d01bc284c4e8

Тип поля	Название поля	Описание	Пример значения
	cs2Label	Поле используется для указания на имя NetBIOS конечного устройства.	endpointName
	cs2	Имя NetBIOS конечного устройства.	DESKTOP-0731NFQ
	cs3Label	Поле используется для индикации командной строки.	cmdLine
	cs3	Запрос командной строки.	C:\\Windows\\system32\\sc.exe start w32time task_started
	cs4Label	Поле используется для указания идентификатора сессии.	sessionId
	cs4	Идентификатор сессии.	1656395717

Формат журнала аппаратуры конечных устройств

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	endpoint_hardware
	Name	Тип источника.	log
	Threat Level	Значение по умолчанию.	0
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Идентификатор устройства, сгенерировавшего это событие.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	act	Действие (подключение или извлечение устройства).	add_device, remove_device
	sourceServiceName	Драйвер Windows, обеспечивающий взаимодействие компьютера с оборудованием/устройством.	USBHUB3
	cs1Label	Поле используется для указания идентификатора конечного устройства.	endpointId
	cs1	Идентификатор конечного устройства.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	cs2Label	Поле используется для указания на имя NetBIOS конечного устройства.	endpointName
	cs2	Имя NetBIOS конечного устройства.	DESKTOP-0731NFQ
	cs3Label	Поле используется для указания идентификатора подключаемого/извлекаемого устройства.	deviceId
	cs3	Идентификатор устройства.	USB\\VID_0E0F&PID_0002\\6&201153C1&0&8
	cs4Label	Поле используется для индикации имени устройства.	deviceName
	cs4	Название устройства.	Kingston DataTraveler 2.0 USB Device

Формат журнала syslog

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	syslog
	Name	Тип источника.	log
	Threat Level	Уровень угрозы.	Может принимать значения: 0 — emergencies; 1 — alerts; 2 — critical; 3 — errors; 4 — warnings; 5 — notifications; 6 — informational; 7 — debugging.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1701085036026

Тип поля	Название поля	Описание	Пример значения
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorereaeda
	msg	Описание события.	[3603:3603:1128/175000.938565.ERROR:CONSOLE(6)] "console.assert", source: devtools://devtools/bundled/devtools-frontend/front_end/panels/console/console.js (6)
	cn1Label	Поле используется для указания типа источника событий syslog. Подробнее о значениях syslog facility смотрите в RFC 5424 .	Facility
	cn1	Тип источника событий syslog. Например, user-level messages.	1
	cs1Label	Поле используется для указания имени устройства, на котором произошло событие.	Hostname
	cs1	Имя компьютера, на котором произошло событие.	node1
	cs2Label	Поле используется для указания приложения, вызвавшего событие.	Tag
	cs2	Приложение, вызвавшее событие.	org.gnome.Shell.desktop
	cs3Label	Поле используется для указания идентификатора процесса события.	ProcessID
	cs3	PID процесса вызвавшего событие.	3036
	cs4Label	Поле используется для указания срабатывания правила.	Rule
	cs4	Название правила, срабатывание которого вызвало событие.	Example — Allow user-level messages

Формат журнала RADIUS

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	radius
	Name	Тип источника.	log
	Threat Level	Уровень угрозы.	Может принимать значения: 0 — emergencies; 1 — alerts; 2 — critical; 3 — errors; 4 — warnings; 5 — notifications; 6 — informational; 7 — debugging.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1701085036026
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorereaeda
	act	Статус пользователя (acct_status_type).	start, stop, interim update, accounting-on, accounting-off
	suser	Имя пользователя.	Unknown, если пользователь неизвестен.
	src_ip	IP-адрес источника, откуда пришло сообщение.	192.168.57.4
	dst	IP-адрес NAS, авторизовавшего пользователя.	172.16.1.4
	dvc	IP-адрес пользователя (framed ip address).	192.168.57.29
	cs1Label	Поле используется для указания группы, в которой состоит пользователь.	user groups
	cs1	Строка групп в которых состоит пользователь.	test_group

Формат журнала UserID

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW

Тип поля	Название поля	Описание	Пример значения
	Device Version	Версия продукта.	7
	Source	Название журнала.	userid
	Name	Тип источника.	log
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1701085036026
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorereaeda
	act	Действие, принятое устройством в соответствии с настроенными политиками.	login
	reason	Причина, по которой было создано событие.	{"user_groups_sids":["S-1-5-21-3795870133-5220325-2125745684-513","S-1-5-21-3795870133-5220325-2125745684-512"], "user_sid":"S-1-5-21-3795870133-5220325-2125745684-1103","login":"user1","domain":"DEV","event_id":4624}
	suser	Имя пользователя.	user1 (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.0.11
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	dev.local

Documentation: ☒
Product: SIEM
Version: 7.x

Описание журнала событий

Название поля	Описание	Пример значения
timestamp	Время получения события в формате: yyyy-mm-ddTth:mm:ssZ.	2022-05-12T08:11:46.15869Z
node	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
ip_address	IPv4-адрес источника события.	192.168.174.134
attributes	Детали события в формате JSON.	{"rule":{"logrotate":12,"attributes":{"timezone":"Asia/Novosibirsk"},"id":"66f9de9f-d698-4bec-b3b0-ba65b46d3608","name":"Example log export ftp"}}
event_type	Тип события.	logexport_rule_updated
event_severity	Важность события.	info (информационные), warning (предупреждения), error (ошибки), critical (критичные).
event_origin	Модуль, в котором произошло событие.	core
event_component	Компонент, в котором произошло событие.	console_auth
user	Имя пользователя.	{"guid":"37333739-3733-3734-3635-366400000000","name":"System","groups":[]}}

Описание журнала веб-доступа

Название поля		Описание	Пример значения
timestamp		Время получения события в формате: yyyy-mm-ddTth:mm:ssZ.	2022-05-12T08:11:46.15869Z
session		Идентификатор сессии.	a7a3cd49-8232-4f1a-962a-3659af89e96f (если System: 00000000-0000-0000-0000-000000000000)
node		Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
reasons		Причина, по которой было создано событие, например, причина блокировки сайта.	"url_cats":[{"id":39,"name":"Social Networking","threat_level":3}]
proto		Используемый протокол 4-го уровня.	TCP
host		Имя хоста.	www.google.com
action		Действие, принятое устройством в соответствии с настроенными политиками.	block
bytes_sent		Количество байтов, переданных в направлении источник — назначение.	52
bytes_recv		Количество пакетов, переданных в направлении назначение — источник.	100
packets_sent		Количество пакетов, переданных в направлении источник — назначение.	2
packets_recv		Количество байтов, переданных в направлении назначение — источник.	5
request_method		Метод, используемый для доступа к URL-адресу (POST, GET и т.п.).	GET
url		Поле содержит URL-адрес запрашиваемого ресурса с указанием используемого протокола.	http://www.secure.com
media_type		Тип контента.	application/json
status_code		Код ответа HTTP.	302
http_referer		URL источника запроса (реферер HTTP).	https://www.google.com/
decrypted		Поле указывает было ли содержимое расшифровано.	true, false
useragent		Useragent пользовательского браузера.	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
application	id	Идентификатор приложения.	20
	name	Название приложения.	Youtube
	threat_level	Уровень угрозы приложения.	0
	app_protocol	Протокол прикладного уровня и его версия.	HTTPV1.1"
url_categories	id	Идентификатор категории, к которой относится URL.	39
	threat_level	Уровень угрозы категории URL.	Может принимать значения: 1 — очень низкий. 2 — низкий. 3 — средний. 4 — высокий. 5 — очень высокий.

Название поля			Описание	Пример значения
	name		Название категории, к которой относится URL.	Social Networking
source	zone	guid	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника.	Trusted
	country		Страна источника трафика.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника.	10.10.10.10
	port		Порт источника.	Может принимать значения от 0 до 65535.
	mac		MAC-адрес источника	01:23:45:67:89:AB
destination	zone	guid	Уникальный идентификатор зоны назначения трафика.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика.	Untrusted
	country		Страна назначения.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес назначения.	192.168.174.134
	port		Порт назначения.	Может принимать значения от 0 до 65535.
	mac		MAC-адрес назначения.	01:23:45:67:89:AB
rule	guid		Уникальный идентификатор правила, срабатывание которого вызвало создание события.	f93da24d-74f9-4f8c-9e9b-8e6d02346fb4
	name		Название правила.	Default allow
	type		Тип сработавшего правила.	
user	guid		Уникальный идентификатор пользователя.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name		Имя пользователя	user_name
	groups	guid	Уникальный идентификатор группы, в которой состоит пользователь.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Название группы, в которой состоит пользователь.	Default Group

Описание журнала DNS

Название поля			Описание	Пример значения
timestamp			Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
session			Идентификатор сессии.	00000000-0000-0000-0000-000000000000
node			Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorereaeda
reasons			Причина, по которой было создано событие, например, url категория, на которых сработало правило.	{ "url_cats": [{"id": 37, "name": "Search Engines & Portals", "threat_level": 1}] }
proto			Используемый протокол 4-го уровня.	UDP
host			Имя хоста.	google.com
data			Поле используется для указания передаваемых данных.	{ "question": [{"domain": "google.com", "type": "A", "class": "IN"}], "answer": [{"domain": "google.com", "type": "TXT", "class": "IN", "ttl": 5, "data": "Blocked"}, {"domain": "google.com", "type": "A", "class": "IN", "ttl": 5, "data": "10.10.0.1"}] }
url_categories	id	Идентификатор сработавшей URL-категории.		37
	threat_level	Уровень угрозы сработавшей категории.		Может принимать значения: 1 — очень низкий. 2 — низкий. 3 — средний. 4 — высокий. 5 — очень высокий.
	name	Название сработавшей категории.		Search Engines & Portals
action			Действие, принятое устройством в соответствии с настроенными политиками.	block
application	id	Идентификатор приложения.		5
	name	Название приложения.		
	threat_level	Уровень угрозы приложения.		0
	app_protocol	Протокол прикладного уровня.		DNS
source	zone	guid	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47

Название поля			Описание	Пример значения
		name	Название зоны источника трафика.	Trusted
	country		Название страны источника.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика.	10.10.10.10
	port		Порт источника.	Может принимать значения от 0 до 65535.
	mac		MAC-адрес источника.	01:23:45:67:89:AB
destination	zone	guid	Уникальный идентификатор зоны назначения трафика.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика.	Untrusted
	country		Название страны назначения.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес назначения трафика.	104.19.197.151
	port		Порт назначения	Может принимать значения от 0 до 65535. Для DNS обычно используется порт 53.
	mac		MAC-адрес назначения	01:23:45:67:89:AB
rule	guid		Уникальный идентификатор правила, срабатывание которого создало событие.	59e38e06-533a-4771-9664-031c3e8b2e1f
	name		Название правила, срабатывание которого вызвало событие.	Rule1
	Type		Тип сработавшего правила.	
user	guid		Уникальный идентификатор пользователя. Если пользователь типа Unknown, то идентификатор: 00000000-0000-0000-0000-000000000000.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name		Имя пользователя.	user1
	groups	guid	Уникальный идентификатор группы, в которых состоит пользователь.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Название группы, в которой состоит пользователь.	Default Group

Описание журнала трафика

Название поля			Описание	Пример значения
timestamp			Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
session			Идентификатор сессии.	a7a3cd49-8232-4f1a-962a-3659af89e96f (если System: 00000000-0000-0000-0000-000000000000)
node			Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
proto			Используемый протокол 4-го уровня.	TCP или UDP
action			Действие, принятое устройством в соответствии с настроенными политиками.	accept
bytes_sent			Количество байтов, переданных в направлении источник — назначение.	100
bytes_recv			Количество байтов, переданных в направлении назначение — источник.	6
packets_recv			Количество пакетов, переданных в направлении назначение — источник.	1
packets_sent			Количество пакетов, переданных в направлении источник — назначение.	1
json_data			Дополнительные данные.	null
application	id		Идентификатор приложения.	195
	threat_level		Уровень угрозы приложения.	Может принимать значения: 1 — очень низкий. 2 — низкий. 3 — средний. 4 — высокий. 5 — очень высокий.
	app_protocol		Протокол прикладного уровня.	HTTP
	name		Название приложения.	Youtube
source	zone	guid	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника трафика.	Trusted
	country		Название страны источника.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика.	10.10.10.10

Название поля			Описание	Пример значения
	port		Порт источника.	Может принимать значения от 0 до 65535.
destination	zone	guid	Уникальный идентификатор зоны назначения трафика.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика.	Untrusted
	country		Название страны назначения.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес назначения трафика.	104.19.197.151
	port		Порт назначения	Может принимать значения от 0 до 65535.
nat	source	ip	Адрес источника после переназначения (если настроены правила NAT).	192.168.117.85 (если NAT не настроен, то: "nat":null)
		port	Порт источника после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (если NAT не настроен, то: "nat":null)
	destination	ip	Адрес назначения после переназначения (если настроены правила NAT).	64.233.164.198 (если NAT не настроен, то: "nat":null)
		port	Порт источника после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (если NAT не настроен, то: "nat":null)
rule	guid		Уникальный идентификатор правила, срабатывание которого создало событие.	59e38e06-533a-4771-9664-031c3e8b2e1f
	type		Тип правила.	firewall
	name		Название правила, срабатывание которого вызвало событие.	Allow trusted to untrusted
user	guid		Уникальный идентификатор пользователя. Если пользователь типа Unknown, то идентификатор: 00000000-0000-0000-0000-000000000000.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name		Имя пользователя.	Admin
	groups	guid	Уникальный идентификатор группы, в которых состоит пользователь.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Название группы, в которой состоит пользователь.	Default Group

Описание журнала COB

Название поля			Описание	Пример значения
timestamp			Время получения события в формате: yyyy-mm-ddTTh:mm:ssZ.	2022-05-12T08:11:46.15869Z
session			Идентификатор сессии.	a7a3cd49-8232-4f1a-962a-3659af89e96f (если System: 00000000-0000-0000-0000-000000000000)
node			Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
proto			Используемый протокол 4-го уровня.	TCP или UDP
action			Действие, принятое устройством в соответствии с настроенными политиками.	accept
bytes_sent			Количество байтов, переданных в направлении источник — назначение.	100
bytes_recv			Количество байтов, переданных в направлении назначение — источник.	6
packets_sent			Количество пакетов, переданных в направлении источник — назначение.	1
packets_recv			Количество пакетов, переданных в направлении назначение — источник.	1
json_data			Дополнительные данные.	null
application	id		Идентификатор приложения.	195
	threat_level		Уровень угрозы приложения.	Может принимать значения: 1 — очень низкий. 2 — низкий. 3 — средний. 4 — высокий. 5 — очень высокий.
	name		Название приложения.	Youtube
	app_protocol		Протокол прикладного уровня.	HTTP
user	guid		Уникальный идентификатор пользователя. Если пользователь типа Unknown, то идентификатор: 00000000-0000-0000-0000-000000000000.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name		Имя пользователя.	Admin
	groups	guid	Уникальный идентификатор группы, в которых состоит пользователь.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Название группы, в которой состоит пользователь.	Default Group
rule	guid		Уникальный идентификатор правила, срабатывание которого создало событие.	59e38e06-533a-4771-9664-031c3e8b2e1f

Название поля			Описание	Пример значения
	name		Название правила, срабатывание которого вызвало событие.	Allow trusted to untrusted
	type		Тип сработавшего правила	idps
signatures	id		Идентификатор сработавшей сигнатуры.	999999
	threat_level		Уровень угрозы сработавшей сигнатуры.	Может принимать значения: 1 — очень низкий. 2 — низкий. 3 — средний. 4 — высокий. 5 — очень высокий.
	name		Название сработавшей сигнатуры.	BlackSun Test
source	zone	guid	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника трафика.	Trusted
	country		Название страны источника.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика.	10.10.10.10
	port		Порт источника.	Может принимать значения от 0 до 65535.
	mac		MAC-адрес источника.	01:23:45:67:89:AB
destination	zone	guid	Уникальный идентификатор зоны назначения трафика.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика.	Untrusted
	country		Название страны назначения.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес назначения трафика.	104.19.197.151
	port		Порт назначения.	Может принимать значения от 0 до 65535.
	mac		MAC-адрес назначения.	01:23:45:67:89:AB

Описание журнала АСУ ТП

Название поля		Описание	Пример значения
timestamp		Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
pdu_severity		Критичность АСУ ТП.	1
pdu_func		Код функции (говорит ведомому устройству, какие данные или выполнение какого действия требует от него ведущее устройство).	12
pdu_address		Адрес регистра, с которым необходимо провести операцию.	3154
node		Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
details	pdu_varname	Имя переменной. Параметр, в основном, используется для обмена данными в режиме реального времени. Параметр относится к протоколу MMS.	VAR
	pdu_device	Адрес устройства, используемый в протоколах MMS и OPCUA.	DEV
	mb_write_quantity	Количество значений для записи (команда Read Write Register).	998
	mb_write_addr	Начальный адрес регистра для записи (команда Read Write Register).	776
	mb_value	Записываемое значение (для команд Write Single Coil, Write Single Register).	322
	mb_unit_id	Адрес устройства.	186
	mb_read_quantity	Количество значений для чтения (команда Read Write Register).	658
	mb_read_addr	Начальный адрес регистра для чтения (команда Read Write Register).	122
	mb_quantity	Количество значений для чтения.	875
	mb_payload	Значения регистров (для команд Read Coil, Read Holding Registers, Read Input Registers, Read/Write Multiple registers, Write Multiple Coil).	75be5ecdс24f9883
	mb_or_mask	Значение маски OR команды Mask Write Register.	1024
	mb_message	Сообщение Modbus.	exception
	mb_exception_code	Код ошибки. Актуален для типа сообщения error_response.	255
	mb_and_mask	Значение маски AND команды Mask Write Register.	121
	mb_addr	Адрес регистра.	3154

Название поля			Описание	Пример значения
	iec104_msgtype		Тип запроса.	request, response, error_response
	iec104_ioa		Адрес объекта информации, который позволяет однозначно идентифицировать приёмной стороной тип события.	23
	iec104_cot		Причина передачи протокольного блока данных прикладного уровня (Application Protocol Data Unit, APDU).	6
	iec104_asdu		Адрес ASDU (COA — Common Object Address). Параметр относится к протоколу IEC-104.	123
	app_protocol			Протокол прикладного уровня.
action			Действие, принятое устройством в соответствии с настроенными политиками.	pass
source	zone	guid	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника трафика.	Trusted
	country		Название страны источника.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика.	10.10.10.10
	port		Порт источника.	Может принимать значения от 0 до 65535.
	destination	zone	guid	Уникальный идентификатор зоны назначения трафика.
name			Название зоны назначения трафика.	Untrusted
country		Название страны назначения.	RU (отображается двухбуквенный код страны)	
ip		IPv4-адрес назначения трафика.	104.19.197.151	
port		Порт назначения	Может принимать значения от 0 до 65535.	
rule		guid		Уникальный идентификатор правила, срабатывание которого создало событие.
	name		Название правила, срабатывание которого вызвало событие.	SCADA Sample Rule

Описание журнала инспектирования SSH

Название поля			Описание	Пример значения
timestamp			Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node			Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
command			Команда, передаваемая по SSH.	whoami
action			Действие, принятое устройством в соответствии с настроенными политиками.	block
application	id	name	Идентификатор приложения.	195
		threat_level	Название приложения.	
			Уровень угрозы приложения.	Может принимать значения от 2 до 10 (установленный уровень угрозы приложения, умноженный на 2).
	app_protocol		Протокол прикладного уровня.	SSH или SFTP
source	zone	guid	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника трафика.	Trusted
	country		Название страны источника.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика.	10.10.10.10
	port		Порт источника.	Может принимать значения от 0 до 65535.
	mac		MAC-адрес источника.	FA:16:3E:65:1C:B4
destination	zone	guid	Уникальный идентификатор зоны назначения трафика.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика.	Untrusted
	country		Название страны назначения.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес назначения трафика.	104.19.197.151
	port		Порт назначения.	Может принимать значения от 0 до 65535.
	mac		MAC-адрес назначения.	01:23:45:67:89:AB
rule	guid		Уникальный идентификатор правила, срабатывание которого создало событие.	59e38e06-533a-4771-9664-031c3e8b2e1f
	name		Название правила, срабатывание которого вызвало событие.	SSH Rule Example

Название поля		Описание	Пример значения
	type	Тип сработавшего правила.	ssh
user	guid	Уникальный идентификатор пользователя. Если пользователь типа Unknown, то идентификатор: 00000000-0000-0000-0000-000000000000.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name	Имя пользователя.	Admin
	groups	Уникальный идентификатор группы, в которых состоит пользователь.	919878b2-e882-49ed-3331-8ec72c3c79cb
	name		Default Group

Описание журнала защиты почтового трафика

Название поля			Описание	Пример значения
timestamp			Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node			Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
action			Действие, принятое устройством в соответствии с настроенными политиками.	mark
bytes_sent			Количество байтов, переданных в направлении источник — назначение.	0
bytes_rcv			Количество байтов, переданных в направлении назначение — источник.	0
packets_sent			Количество пакетов, переданных в направлении источник — назначение.	0
packets_rcv			Количество пакетов, переданных в направлении назначение — источник.	0
decrypted			Поле указывает было ли содержимое расшифровано.	true, false
from			Почтовый адрес отправителя.	sender@example.com
to			Почтовый адрес получателя.	receiver@example.com
application		id	Идентификатор приложения.	9
		name	Название приложения.	
		threat_level	Уровень угрозы приложения.	Может принимать значения от 2 до 10 (установленный уровень угрозы приложения, умноженный на 2).
		app_protocol	Сетевой протокол прикладного уровня.	SMTP
source	zone	guid	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника трафика.	Trusted
	country		Название страны источника.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика.	10.10.10.10
	port		Порт источника.	Может принимать значения от 0 до 65535.
	mac		MAC-адрес источника.	01:23:45:67:89:AB
	destination	zone	guid	Уникальный идентификатор зоны назначения трафика.
name			Название зоны назначения трафика.	Untrusted
country		Название страны назначения.	RU (отображается двухбуквенный код страны)	
ip		IPv4-адрес назначения трафика.	10.10.10.10	
port		Порт назначения.	Может принимать значения от 0 до 65535.	
port		MAC-адрес назначения.	01:23:45:67:89:AB	
rule		guid		Уникальный идентификатор правила, срабатывание которого создало событие.
	name		Название правила, срабатывание которого вызвало событие.	Mail security rule
	type		Тип сработавшего правила.	Mail security rule
user	guid		Уникальный идентификатор пользователя.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name		Имя пользователя.	user_name
	groups	guid	Уникальный идентификатор группы, в которой состоит пользователь.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Название группы, в которой состоит пользователь.	Default Group

Описание журнала событий конечных устройств

Название поля	Описание	Пример значения

Название поля	Описание	Пример значения
user_name	Имя пользователя.	DESKTOP-0731NFQ\\Username
timestamp	Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
status	Результат выполнения WMI или SNMP запроса.	OK, Error
source_name	Источник журнала событий.	Microsoft-Windows-Security-Auditing
endpoint_name	Название конечного устройства или сенсора.	DESKTOP-0731NFQ
endpoint_id	Идентификатор конечного устройства или сенсора.	35fb5820-74db-4eac-b05b-d01bc284c4e8
node	Идентификатор конечного устройства или узла, на котором запущен сенсор.	35fb5820-74db-4eac-b05b-d01bc284c4e8
log_level	Тип события.	Аудит успеха, Предупреждение, Сведения, Аудит отказа, Ошибка
log_file	Тип журнала, содержащего важную информацию о программных и аппаратных событиях.	Security (файл журнала безопасности), Application (файл журнала приложений), System (файл системного журнала), Windows PowerShell
log_event_type	Тип события лога.	1 (error), 2 (warning), 3 (information), 4 (audit success), 5 (audit failure).
log_event_id	Идентификатор события.	4672
log_event_code	Код события журнала.	14056
log_category_string	Категория события.	Special Logon
insertion_string	Строка вставки - данные блока eventData события Windows.	Windows DefenderSECURITY_PRODUCT_STATE_ON
error	Ошибка WMI или SNMP, возникшая в результате выполнения запроса.	0
data	Подробная информация о событии.	Тип запуска службы "Установщик модулей Windows" был изменен с "Автоматически" на "Вручную".
counter_id	Идентификатор счётчика, добавленного в WMI или SNMP сенсор.	35fb5820-74db-4eac-b05b-d01bc284c4e8
computer_name	Имя компьютера.	DESKTOP-0731NFQ

Описание журнала правил конечных устройств

Название поля		Описание	Пример значения
timestamp		Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
session		Идентификатор сессии.	00000006-0000-0000-f04d-14bdad0f01bb
proto		Используемый протокол 4-го уровня.	TCP
host		Имя хоста.	www.google.com
action		Действие, принятое устройством в соответствии с настроенными политиками.	drop, accept, nat
endpoint_name		Имя конечного устройства.	DESKTOP-0731NFQ
endpoint_id		Идентификатор конечного устройства.	35fb5820-74db-4eac-b05b-d01bc284c4e8
media_type		Тип контента.	application/json
app_name		Приложение, к которому было применено правило межсетевого экрана.	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
source	ip	IPv4-адрес источника.	10.10.10.10
	port	Порт источника.	Может принимать значения от 0 до 65535.
destination	ip	IPv4-адрес назначения.	104.19.197.151
	port	Порт назначения	Может принимать значения от 0 до 65535.
rule	guid	Уникальный идентификатор правила, срабатывание которого создало событие.	f93da24d-7419-4f8c-9e9b-8e6d02346fb4
	name	Название правила, срабатывание которого вызвало событие.	Default allow
	type	Тип сработавшего правила.	
url_categories	id	Идентификатор категории, к которой относится URL.	39
	threat_level	Уровень угрозы категории URL.	Может принимать значения: 1 — очень низкий. 2 — низкий. 3 — средний. 4 — высокий. 5 — очень высокий.
	name	Название категории, к которой относится URL.	Social Networking

Описание журнала приложений конечных устройств

Название поля	Описание	Пример значения
user_name	Имя пользователя, под учётной записью которого выполнен вход на конечном устройстве.	DESKTOP-0731NFQ\\User
timestamp	Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
endpoint_name	Название конечного устройства или сенсора.	DESKTOP-0731NFQ
endpoint_id	Идентификатор конечного устройства или сенсора.	35fb5820-74db-4eac-b05b-d01bc284c4e8
process_id	Идентификатор процесса.	3916
hash	Хэш приложения.	B4CE5C3495FEA0A4FDBAC8ABDCD199F7E4CA8C1F
app_name	Приложение, которое было запущено/остановлено.	C:\\Program Files (x86)\\Microsoft\\Edge\\Application\\msedge.exe
action	Действие (запуск или остановка приложения).	start, stop
version	Версия приложения.	6.2.19041.746
subject	Субъект подписи.	Microsoft Corporation
issuer	Издатель сертификата для приложения.	Microsoft Windows Production PCA 2011
cmd_line	Запрос командной строки.	C:\\Windows\\system32\\svchost.exe -k wsappx -p -s AppXSvc
session_id	Идентификатор сессии.	1656038456

Описание журнала аппаратуры конечных устройств

Название поля	Описание	Пример значения
timestamp	Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
endpoint_name	Название конечного устройства или сенсора.	DESKTOP-0731NFQ
endpoint_id	Идентификатор конечного устройства или сенсора.	35fb5820-74db-4eac-b05b-d01bc284c4e8
action	Действие (подключение/извлечение устройства).	add_device, remove_device
device_name	Название устройства, которое было подключено/извлечено.	Generic USB Hub
device_id	Идентификатор устройства.	USB\\VID_0E0F&PID_0002\\6&201153C1&0&7
service	Драйвер Windows, обеспечивающий взаимодействие компьютера с оборудованием/устройством.	USBHUB3

Описание журнала syslog

Название поля		Описание	Пример значения
timestamp		Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node		Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorereaeda
syslog_facility		Тип источника события syslog. Например, user-level messages. Подробнее о значениях syslog facility смотрите в RFC 5424 .	1
syslog_severity		Уровень важности события syslog. Например, warning. Подробнее о значениях syslog severity смотрите в RFC 5424 .	4
computer_name		Имя устройства, на котором произошло событие.	node1
app_name		Приложение, вызвавшее событие.	org.gnome.Shell.desktop
process_id		PID процесса, вызвавшего событие.	3036
data		Описание события.	[3603:3603:1130/125201.838651:ERROR:CONSOLE(6)] \"console.assert()\", source: devtools://devtools/bundled/devtools-frontend/front_end/panels/console/console.js (6)
rule	guid	Уникальный идентификатор правила, срабатывание которого создало событие.	16535060-5a1a-4e92-8331-239406ec34da
	name	Название правила, срабатывание которого вызвало событие.	Example — Allow user-level messages
	type	Тип сработавшего правила.	

Описание журнала RADIUS

Название поля	Описание	Пример значения
timestamp	Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorereaeda

Название поля		Описание	Пример значения	
event_type		Статус пользователя (acct_status_type).	start, stop, interim update, accounting-on, accounting-off	
action		Действие, принятое устройством в соответствии с настроенными политиками.	login	
src_ip		IP-адрес источника, откуда пришло сообщение.	192.168.57.4	
nas_ip		IP-адрес NAS, авторизовавшего пользователя.	172.16.1.4	
framed_ip		IP-адрес пользователя.	192.168.57.29	
rule	guid	Уникальный идентификатор правила, срабатывание которого создало событие.	16535060-5a1a-4e92-8331-239406ec34da	
user	guid	Уникальный идентификатор пользователя. Если пользователь типа Unknown, то идентификатор: 00000000-0000-0000-0000-000000000000.	745591c3-9d21-092d-8db4-5b9b0000044f	
	name	Имя пользователя.	user_name	
	groups	guid	Уникальный идентификатор группы, в которой состоит пользователь.	aa218609-8716-9252-df20-88c43a0d0bf6
		name	Название группы, в которой состоит пользователь.	test_group

Описание журнала UserID

Название поля		Описание	Пример значения	
timestamp		Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z	
node		Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntooreaeada	
reasons		Причина, по которой было создано событие.	{\"user_groups_sids\":[\"S-1-5-21-3795870133-5220325-2125745684-513\", \"S-1-5-21-3795870133-5220325-2125745684-512\", \"S-1-5-21-3795870133-5220325-2125745684-572\"], \"user_sid\": \"S-1-5-21-3795870133-5220325-2125745684-1103\", \"login\": \"user1\", \"domain\": \"DEV\", \"event_id\": 4624}	
action		Действие, принятое устройством в соответствии с настроенными политиками.	login	
src_ip		IPv4 источника события.	10.10.0.11	
rule	guid	Уникальный идентификатор правила, срабатывание которого создало событие.	16535060-5a1a-4e92-8331-239406ec34da	
	name	Название правила, срабатывание которого вызвало событие.	dev.local	
	type	Тип сработавшего правила.	syslog	
user	guid	Уникальный идентификатор пользователя. Если пользователь типа Unknown, то идентификатор: 00000000-0000-0000-0000-000000000000.	745591c3-9d21-092d-8db4-5b9b0000044f	
	name	Имя пользователя.	user1	
	groups	guid	Уникальный идентификатор группы, в которых состоит пользователь.	aa218609-8716-9252-df20-88c43a0d0bf6
		name	Название группы, в которой состоит пользователь.	CN=Domain Users,CN=Users,DC=dev,DC=local

Documentation: 
Product: SIEM
Version: 7.x

С помощью отчетов администратор может предоставить различные срезы данных о событиях безопасности, конфигурирования или действиях пользователей. Отчеты могут создаваться по созданным ранее правилам и шаблонам в автоматическом режиме и отправляться адресатам по электронной почте.

Раздел **Отчеты** состоит из четырех подразделов — **Шаблоны**, **Пользовательские шаблоны**, **Правила отчетов** и **Созданные отчеты**. Чтобы создать отчет необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать правило создания отчета	Создать правило создания отчета, в котором указать необходимые параметры создания отчета.
Шаг 2. Запустить отчет	Запустить отчет в ручном режиме или дождаться времени, когда он запустится в автоматическом режиме по указанному в правиле расписанию.
Шаг 3. Получить отчет	Получить отчет по почте, если в правиле была настроена отправка отчета по почте, или скачать полученный отчет в разделе Созданные отчеты .

ПримечаниеПроцесс создания отчета может продолжаться достаточно длительное время и может потреблять большое количество вычислительных ресурсов.

Documentation: 
Product: SIEM
Version: 7.x

Шаблон определяет внешний вид и поля, которые будут использоваться в отчете. Шаблоны отчетов предоставляются компанией разработчиком UserGate.

Список возможных шаблонов отчетов, сгруппированных по категориям:

- **Пользовательский** — группа шаблонов по обобщенной статистике срабатывания правил отчетов.
- **Captive-портал** — группа шаблонов по событиям, авторизации пользователей с помощью Captive-портала.
- **Приложения конечных устройств** — группа шаблонов со списками приложений, которые когда-либо запускались на конечных устройствах.
- **Журнал правил конечных устройств** — группа шаблонов по событиям срабатывания правил межсетевого экрана конечных устройств.
- **Журнал событий конечных устройств** — группа шаблонов по событиям, полученным от контролируемых с помощью программного обеспечения UserGate Endpoint конечных устройств.
- **События** — группа шаблонов по событиям, регистрируемым в журнале событий.
- **СОВ** — группа шаблонов по событиям, регистрируемым в журнале СОВ.
- **Защита почтового трафика** — группа шаблонов по событиям, регистрируемым в журнале защиты почтового трафика.
- **Сетевая активность** — группа шаблонов по событиям, регистрируемым в журнале трафика.
- **Веб-портал** — группа шаблонов авторизации через SSL VPN.
- **Трафик** — группа шаблонов по событиям, регистрируемым в журнале трафика и относящимся к объему потребленного трафика пользователями, приложениями и т.п.
- **UserID** — группа шаблонов для создания отчетов по работе UserID агента.
- **VPN** — группа шаблонов по событиям, относящимся к VPN.
- **Веб-активность** — группа шаблонов по событиям, регистрируемым в журнале веб-доступа.

Каждый шаблон содержит название, описание отчета и тип отображения отчета (таблица, гистограмма, пирог).

Documentation: 

Product: SIEM

Version: 7.x

Если в системных шаблонах отсутствуют параметры, необходимые для отчета, вы можете создать собственный шаблон и использовать его в правилах генерации этого отчета.

Чтобы создать шаблон:

1. В разделе **Журналы и отчеты** → **Отчеты** → **Пользовательские шаблоны** нажмите **Добавить**.

2. В окне настройки шаблона выполните следующее:

- Укажите название и при необходимости описание шаблона.
- Укажите источник, данные которого требуется использовать для создания отчета. Вы можете выбрать [один из журналов](#) или [список срабатываний правил аналитики](#).
- При необходимости введите [выражение на языке запросов](#), по которому будут отфильтрованы данные при создании отчета.
- При необходимости укажите параметр, по которому будут отсортированы записи отчета, а также направление сортировки (по возрастанию или по убыванию значений параметра).
Выбор параметра для сортировки недоступен, если указан параметр для группировки записей. В этом случае сортировка выполняется по количеству записей в каждой группе в порядке убывания.
- При необходимости укажите параметр, по которому будут сгруппированы записи отчета.
Выбор параметра для группировки недоступен, если указан параметр для сортировки записей.
- В блоке **Столбцы** → **Доступно** двойным щелчком мыши выберите параметры, значения которых необходимо отображать в отчете.
Примечание Чтобы запись отчета, содержащая массив в качестве значения параметра, была преобразована в несколько записей (по одной для каждого элемента массива), установите флажок «Разъединять записи».

3. Нажмите **Сохранить**.

Созданный шаблон отобразится в таблице **Пользовательские шаблоны**. Для использования шаблона необходимо добавить его [в правило генерации отчетов](#).

Documentation: 
Product: SIEM
Version: 7.x

Правило отчета задает параметры создаваемого отчета, а также расписание запуска отчетов и способы доставки отчета пользователям. При создании правила отчета администратор указывает следующие параметры:

Наименование	Описание
Включено	Включение/отключение отчета.
Название	Название правила.
Описание	Оptionальное поле для описания правила.
Язык отчета	Выбор языка, который будет использован в отчете.
Диапазон	Диапазон времени, за который необходимо подготовить отчет.
Формат отчета	Формат отчета (PDF, HTML, XML, CSV), в котором будет создаваться данный отчет. Важно! Создание отчета в формате PDF создает высокую нагрузку на процессор и память. Чем объемнее отчет, тем более высокая нагрузка. Не используйте формат отчета PDF для пользовательских шаблонов. Для шаблонов Подробный список всех посещенных URL и Подробный список всех посещенных сайтов автоматически используется формат CSV, независимо от выбранного формата.
Количество записей	Задание ограничения числа записей, которые будут выводиться в отчетах, в которых присутствует ограничение по количеству топ записей, например, топ 20 пользователей с ошибочной авторизацией в веб-консоль.
Количество в группировке (если применимо)	Задание ограничения числа записей, которые будут выводиться в отчетах, в которых присутствует ограничение по количеству сгруппированных записей, например, топ 10 пользователей по категориям — для каждой категории будет указано не более 10 пользователей. Данное ограничение применимо только для тех шаблонов отчетов, которые содержат группирование.
Пользователи	Задаёт пользователей или группы пользователей, для которых будет создаваться отчет. Если оставить поле пустым, то отчет будет создаваться для всех пользователей.
Шаблоны	Список шаблонов, которые будут использоваться для построения отчета. Обязательно необходимо добавить хотя бы один шаблон.
Расписание	Выбор расписания для создания отчетов. Возможны варианты: - Ежедневно. - Еженедельно. - Ежемесячно. - Каждые ... часов. - Каждые ... минут. - Задать вручную. При задании вручную необходимо использовать cronTab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 0-31) (месяц: 0-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: - Звездочка (*) — обозначает весь диапазон (от первого до последнего). - Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. - Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". - Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".
Доставка	Возможность задать опциональную отправку созданного отчета получателям по протоколу SMTP. Необходимо задать: - Профиль SMTP, который будет использован для отправки отчетов. Подробно о настройке профилей SMTP смотрите в главе Профили оповещений. - От — имя отправителя письма. - Тема письма — тема письма (subject). - Тело письма — содержимое письма. - Получатели — список получателей письма. Получатели должны быть добавлены в списки библиотеки Почтовые адреса.

ПримечаниеПроцесс создания отчета может продолжаться достаточно длительное время и может потреблять большое количество вычислительных ресурсов. Особенно важно учитывать загрузку ресурсов при запуске отчетов за большой диапазон времени.

ПримечаниеДля того, чтобы запустить правило отчета не обязательно включать его и указывать время запуска правила. В ручном режиме можно запустить любой, в том числе отключенный отчет, для этого в списке правил необходимо выбрать требуемое правило и нажать на кнопку Запустить сейчас. Готовый отчет после создания будет доступен в разделе Созданные отчеты.

Созданные отчеты

Documentation: 
Product: SIEM
Version: 7.x

В разделе **Созданные отчеты** хранятся все полученные отчеты. Отчеты создаются в формате pdf или csv. Для каждого отчета указывается название отчета, которое совпадает с названием правила отчета, которое было использовано для создания данного отчета, время создания отчета и размер отчета.

Для скачивания отчета необходимо использовать кнопку **Скачать**, для удаления — **Удалить**.

Время хранения готовых отчетов (ротация) настраивается по нажатию на кнопку **Настроить**. Значение по умолчанию — 60 дней.

Documentation: ☒
Product: SIEM
Version: 7.x

В данном разделе администратор может формировать отчёты об инцидентах информационной безопасности. Отчеты могут создаваться в соответствии с созданными правилами и шаблонам; отчёт доступен для скачивания или передачи на коннектор.

Раздел состоит из трех подразделов - **Шаблоны отчетов инцидентов**, **Правила отчетов инцидентов** и **Созданные отчеты инцидентов**. Чтобы создать отчет, необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать правило создания отчета.	Создать правило создания отчета, в котором указать необходимые параметры создания отчета.
Шаг 2. Запустить отчет.	Выбрать инцидент и сгенерировать отчет.
Шаг 3. Получить отчет.	Записи о создании отчетов доступны в разделе Созданные отчеты инцидентов .

Documentation: 
Product: SIEM
Version: 7.x

Шаблон определяет внешний вид и поля, которые будут использоваться в отчете. Шаблоны отчетов инцидентов делятся на 2 категории:

- **Форма ключ-заключение** — шаблоны, позволяющие настроить поля, которые необходимо отобразить в отчёте. Шаблоны данного типа пользователь может создавать самостоятельно.
- **Инциденты** — группа шаблонов для создания отчётов по инцидентам. Шаблоны предоставляются компанией UserGate.

Каждый шаблон содержит название, описание отчета и тип отображения отчета (таблица, гистограмма, пирог).

Documentation: 
Product: SIEM
Version: 7.x

Правило отчета задает параметры создаваемого отчета, а также способы доставки отчета пользователям. При создании правила отчета администратор указывает следующие параметры:

Наименование	Описание
Название	Название правила.
Описание	Опциональное поле для описания правила.
Язык отчёта	Выбор языка, который будет использован в отчете.
Часовой пояс	Часовой пояс, который будет использоваться при формировании отчёта.
Формат отчёта	Формат (PDF, HTML), в котором будет создаваться данный отчет.
Коннектор	Коннектор, на который необходимо отправить отчёт (необязательно).
Шаблоны	Список шаблонов, которые будут использоваться для построения отчета. Обязательно необходимо добавить хотя бы один шаблон.

ПримечаниеПроцесс создания отчета может продолжаться достаточно длительное время и может потреблять большое количество вычислительных ресурсов. Особенно важно учитывать загрузку ресурсов при запуске отчетов за большой диапазон времени.
После создания правила пользователь может запустить создание отчёта по выбранному инциденту. После формирования отчёт доступен для скачивания локально или передачи на выбранный коннектор.

Созданные отчеты инцидентов

Documentation: 
Product: SIEM
Version: 7.x

В разделе **Созданные отчеты инцидентов** хранятся все сформированные отчеты. Отчеты создаются в формате pdf или html. Для каждого отчета указывается название отчета, которое совпадает с названием правила отчета, использованного для создания данного отчета, время создания отчета и файл отчета с указанием его размера. Все отчеты доступны для скачивания и удаления.

Время хранения готовых отчетов (ротация) настраивается по нажатию на кнопку **Настроить**.

Общие сведения

Documentation: 

Product: SIEM

Version: 7.x

Technology: SIEM

UserGate SIEM получает данные журналов событий безопасности [от модуля log-collector](#) и [от подключенных сенсоров](#) и записывает эти данные в единое хранилище для последующего анализа.

Администраторы могут управлять полученными событиями безопасности в разделе **Аналитика**. Для этого на соответствующих вкладках раздела вы можете:

- [настраивать правила аналитики](#);
- [выполнять поиск событий по заданным параметрам](#);
- [создавать действия реагирования для срабатываний правил аналитики](#);
- [управлять срабатываниями правил аналитики](#);
- [просматривать подробную информацию о срабатываниях правил аналитики](#);
- [просматривать список процессов конечных устройств](#).

Version: 7.x
Documentation: 
Product: SIEM
Technology: SIEM

События в UserGate SIEM хранятся в виде записей. Каждое событие (например, попытка входа в систему, изменение файла или сетевая активность) представляет собой отдельную запись. Для выявления взаимосвязи между событиями выполняется их корреляция на основе правил аналитики. Это позволяет обнаружить инциденты ИБ, которые могут быть пропущены при анализе каждого события в отдельности.

Правило аналитики содержит набор критериев и условий, по которым UserGate SIEM обнаруживает последовательности событий (корреляцию) в исторических данных из хранилища, а также в потоке данных реального времени, и генерирует [записи о срабатываниях](#) для оповещения администраторов об инцидентах ИБ. Правило аналитики также может определять [действия реагирования](#), которые следует выполнить UserGate SIEM при срабатывании этого правила, например, отправить уведомления по выбранному каналу связи или зарегистрировать инцидент безопасности для последующего анализа и расследования администратором.

По способу создания правила аналитики в UserGate SIEM делятся [на пользовательские правила](#), создаваемые администраторами в веб-консоли устройства, [и системные правила](#), которые вы можете импортировать из библиотеки правил аналитики для дальнейшего использования.

Работа с правилами аналитики

Список всех доступных правил аналитики отображается в разделе **Аналитика → Правила аналитики**.

Для каждого правила в таблице отображаются следующие параметры.

Параметр	Описание
Уровень угрозы	Уровень опасности угрозы (от 1 до 5, где 1 — очень низкий уровень), который определяет степень потенциального ущерба ИТ-инфраструктуре при срабатывании правила аналитики. Этот уровень также определяет интервал запуска правила
Название	Название, указанное при создании правила
Приоритет	Приоритет срабатывания правила аналитики: - Низкий — имеет низкий уровень важности и не требует незамедлительного реагирования; - Нормальный — требует обратить внимание и при необходимости принять соответствующие меры; - Важный — требует обратить внимание и принять соответствующие меры; - Критический — требует незамедлительного реагирования.
Категория срабатывания	Тип инцидента ИБ, на который указывает срабатывание правила аналитики. По умолчанию доступны следующие категории: - Security — инциденты, приводящие к ослаблению безопасности информационных систем; - Availability — инциденты, приводящие к ухудшению доступности информационных систем; - Performance — инциденты, приводящие к снижению производительности информационных систем. Примечание Вы можете создавать дополнительные категории срабатываний правил аналитики в разделе «Настройки» → «Библиотеки» → «Категории срабатываний».
Условия	Условия срабатывания правила аналитики
Действия реагирования	Действия, которые выполняются при срабатывании правила аналитики

Вы можете управлять правилами аналитики в таблице: включать и отключать их состояние, а также удалять эти правила. Для этого необходимо выбрать нужные правила, удерживая клавишу Ctrl или Shift, и нажать соответствующую кнопку в панели инструментов.

Для дальнейшего анализа вы можете экспортировать данные о выбранных правилах и срабатываниях этих правил в файл формата BIN (по кнопке **Экспорт**). Кроме того, вы можете загружать правила аналитики в UserGate SIEM в виде файлов формата BIN или YAML (по кнопке **Импорт → Бинарный** или по кнопке **Импорт → YAML** соответственно).

Также вы можете фильтровать правила в таблице по состоянию. Так, например, можно просмотреть только правила во включенном состоянии, применив фильтр **Показать включенные**.

Для выбранного правила в таблице доступны следующие действия:

- изменение параметров правила по кнопке **Редактировать**;
- создание копии правила по кнопке **Копировать**;
- [просмотр списка срабатываний правила](#) по кнопке **Показать срабатывания**.

Все правила аналитики, находящиеся в таблице во включенном состоянии, используются для обработки данных, поступающих в UserGate SIEM в режиме реального времени. Запуск каждого правила выполняется с интервалом, соответствующим уровню опасности угрозы по срабатыванию этого правила (очень низкий, низкий, средний, высокий или очень высокий). Вы можете изменять интервалы запуска правил аналитики в окне конфигурации, доступном по кнопке **Настроить** в панели инструментов.

Конфигурация правил аналитики

Интервалы работы правил в режиме реального времени, мин

3 очень высокий:

2

4 высокий:

6

3 средний:

8

2 низкий:

14

1 очень низкий:

18

Сохранить

Отмена

Кроме того, вы можете запускать выбранное в таблице правило аналитики для обработки исторических данных по кнопке **Запустить сейчас**. В параметрах запуска правила необходимо указать период получения данных для обработки. Если требуется выполнить анализ всех данных из хранилища, необходимо снять флажок **Указать диапазон времени**. Для проверки работы правила вы можете установить флажок **Тестовый запуск**, при этом записи о срабатывании правила генерироваться не будут.

Создание правила аналитики

Чтобы создать правило аналитики:

1. В разделе **Аналитика** → **Правила аналитики** нажмите **Добавить**.
2. На вкладке **Общие** выполните следующие действия:
 - Включите правило аналитики. Включенное правило используется для обработки данных, поступающих в режиме реального времени.
 - Укажите название и при необходимости описание правила аналитики.
 - Выберите уровень опасности угрозы по срабатыванию правила аналитики (от 1 до 5, где 1 — очень низкий уровень угрозы).
 - Выберите приоритет срабатывания правила аналитики.
 - Выберите категорию срабатываний правила аналитики.
 - Выберите часовой пояс правила аналитики (по умолчанию — UTC+0).
 - Если требуется, чтобы для срабатывания правила аналитики все условия выполнялись в течение определенного времени, установите флажок **Ограничить общее время условий** и в поле **Общее время условий** укажите время в секундах.

3. На вкладке **Условия** нажмите **Добавить** и выполните следующие действия:
- Укажите название и при необходимости описание условия срабатывания правила аналитики.
 - Если требуется, чтобы для срабатывания правила аналитики условие выполнялось в течение определенного времени, установите флажок **Ограничить время выполнения условия** и в поле **Время выполнения условия** укажите время в секундах.
 - Если требуется, чтобы количество выполнений условия для срабатывания правила аналитики обнулялось по указанному запросу, установите флажок **Использовать запрос остановки** и в поле **Запрос остановки** введите выражение [на языке запросов](#). Для формирования запроса вы можете использовать доступные параметры и их значения, а также логические операторы и операторы сравнения.

В поле **Запрос фильтра** введите условие срабатывания правила аналитики [с помощью языка запросов](#). В запросе вы можете указывать доступные параметры и их значения, а также логические операторы и операторы сравнения. Ниже в этом разделе приведены [примеры запросов для условий срабатывания правил](#).

Для формирования запроса вы также можете использовать оператор MATCH и синтаксис регулярных выражений библиотеки RE2. Описание библиотеки см. на сайте [github.com](#) в разделе компании Google.

Например, для обработки данных журнала событий конечных устройств можно ввести следующее условие:

source = 'wmi log' and logFile = 'Microsoft-Windows-Sysmon/Operational' and logEventId = 1 and data MATCH 'ParentCommandLine:(.*)cmd.exe' and data ~ 'CertReq -Post -config'

Будет выполнен поиск событий из журнала Microsoft-Windows-Sysmon/Operational, связанных с запуском в командной строке Windows утилиты certreq.exe для отправки запроса на выпуск сертификата. Эти события могут указывать на попытки кражи или подделки сертификатов аутентификации злоумышленником.

- При необходимости укажите параметры, по которым будут сгруппированы срабатывания правила аналитики.
- В поле **Повторений шаблона** укажите количество выполнений условия для срабатывания правила аналитики.

ПримечаниеЕсли поле не отображается, необходимо увеличить размер окна свойств.

- Нажмите **Сохранить**.

Условие срабатывания правила аналитики отобразится в таблице на вкладке **Условия**. При необходимости вы можете добавить дополнительные условия срабатывания правила, повторив шаг 3 инструкции.

Порядок расположения условий в таблице соответствует порядку их применения в правиле аналитики при обработке событий. При необходимости вы можете изменять порядок с помощью кнопок **Наверх**, **Выше**, **Ниже**, **Вниз**.

4. При необходимости на вкладке **Действия реагирования** выберите действия, которые следует выполнять при срабатывании правила аналитики.

Вы можете выбирать действия из списка по кнопке **Добавить** [или создавать новые](#) по кнопке **Создать и добавить новый объект**.

5. При необходимости по кнопке **Запустить сейчас** запустите правило аналитики для обработки исторических данных из хранилища.

6. Нажмите **Сохранить**.

Примеры запросов для условий срабатывания правил

Ниже приведены примеры запросов, которые можно использовать при добавлении условий срабатывания правил аналитики, для выявления инцидентов ИБ в инфраструктуре организации.

Обнаружение брутфорса

Подбор множества паролей к одной учетной записи (брутфорс) можно обнаружить с помощью анализа событий, связанных с аутентификацией пользователей в системе. Для этого в условиях срабатывания правил аналитики вы можете использовать запросы следующего типа.

Пример запроса:

source = 'endpoint events log' AND logEventId = 4625 AND data MATCH 'Failure Reason:(\s*)Unknown user name or bad password.'

В журнале событий конечных устройств будет выполнен поиск записей о неудачной аутентификации в системе Windows по причине ввода неправильного логина или пароля. В качестве идентификатора события используется значение 4625, подробнее — [в документации Microsoft](#).

Пример запроса:

source = 'endpoint events log' AND logEventId = 4672

В журнале событий конечных устройств будет выполнен поиск записей, указывающих на вход в систему Windows пользователей с особыми (административными) привилегиями. В качестве идентификатора события используется значение 4672, подробнее — [в документации Microsoft](#).

Пример запроса:

source = 'endpoint events log' AND logEventId = 4624

В журнале событий конечных устройств будет выполнен поиск записей об успешном входе в систему Windows. В качестве идентификатора события используется значение 4624, подробнее — [в документации Microsoft](#).

Обнаружение изменения владельца файла

Для обнаружения подозрительной активности, связанной с изменением прав доступа к файлам в Unix-системах, вы можете использовать следующий запрос в условии срабатывания правила аналитики:

source = 'syslog' AND data ~ 'COMMAND=/bin/chown root' AND applicationName = 'sudo'

Среди данных, полученных от syslog-сервера, выполняется поиск записей об изменении владельца файла на пользователя root.

Поиск событий

Documentation: ☒
Product: SIEM
Version: 7.x
Technology: SIEM

В разделе **Аналитика → Поиск** отображаются записи о событиях безопасности, полученные из собственных журналов UserGate SIEM, а также из журналов [подключенных сенсоров](#).

В таблице событий вы можете:

- изменять набор столбцов в контекстном меню **Столбцы**, доступном по нажатию справа от заголовка столбца;
- изменять ширину столбцов;
- изменять порядок следования столбцов, перемещая заголовок столбца;
- сортировать данные по нажатию на заголовки столбцов (не все столбцы поддерживают функцию сортировки);
- просматривать подробную информацию о событии (по нажатию на иконку записи журнала);
- изменять формат отображения данных по кнопкам **Переключить в текстовый вид** и **Переключить в табличный вид** внизу таблицы.

Фильтрация данных о событиях

По умолчанию в таблице отображаются данные о событиях, полученные за все время. Вы можете изменить период отображения данных с помощью предустановленных значений. Для этого в раскрывающемся списке, доступном по кнопке **Все время** в панели инструментов, необходимо выбрать один из периодов.

Данные в таблице событий можно фильтровать с помощью специальных выражений [на языке запросов](#). Для формирования запроса вы можете использовать доступные параметры и их значения, а также логические операторы и операторы сравнения. Кроме того, вы можете добавлять запросы по ссылкам в таблице событий. Так, например, по нажатию на значение IP-адреса источника в строку фильтрации добавляется соответствующий запрос с IP-адресом источника взаимодействия (например, `ipSource = '203.0.113.1'`).

Также в запросе вы можете использовать оператор `MATCH` и синтаксис регулярных выражений библиотеки `RE2`. Описание библиотеки см. на сайте [github.com](#) в разделе компании Google.

Вы можете использовать запросы в строке фильтрации в качестве условий срабатывания новых правил аналитики. Для этого необходимо ввести запрос и в панели инструментов нажать кнопку **Добавить правило**. Дальнейшие действия аналогичны [созданию правила аналитики](#). Также вы можете добавлять запросы для условий срабатывания правил аналитики, созданных ранее. Для этого необходимо ввести запрос и в панели инструментов нажать кнопку **Добавить условие**.

Кроме того, вы можете сохранять примененные фильтры по кнопке **Сохранить как**. Список сохраненных фильтров доступен по кнопке **Популярные фильтры**. Также для дальнейшего анализа вы можете скачать отфильтрованные данные таблицы в виде CSV-файла по кнопке **Экспортировать в CSV**.

Просмотр записи о событии

Запись о событии в таблице может содержать данные, приведенные в таблице ниже. Наличие того или иного параметра зависит от журнала, из которого получено событие.

Параметр	Описание
Узел	Имя устройства
Время	Дата события
Время первого события	Дата и время первого срабатывания правила
Время последнего события	Дата и время последнего срабатывания правила
Источник	Журнал, из которого получено событие
Важность	Присвоенная событию степень важности. Могут быть указаны следующие значения: • Критичные; • Ошибки; • Предупреждения; • Информационные
Компонент	Компонент устройства
Тип события	Тип события
Пользователь	Имя пользователя
Модуль	Модуль устройства
Учет изменений	Тип изменений
Данные	Описание события
Информация	Детали события
Правило	Название правила
Действие	Действие при срабатывании правила
Приложение	Название приложения в системной библиотеке
Угроза приложения	Уровень опасности приложения
Сетевой протокол	Сетевой протокол
Протокол прикладного уровня	Протокол прикладного уровня и его версия
Категории сайтов	Категория URL
Угроза URL-категории	Уровень опасности категории URL
Причины	Причины, указанные в журнале веб-доступа (например, причина блокировки)
HTTP-метод	Метод HTTP-запроса

Параметр	Описание
Код ответа HTTP	Код HTTP-ответа
Тип контента	MIME-тип запроса
URL	URL-адрес ресурса
Реферер	Заголовок Referer в запросе
Операционная система	Тип ОС источника запроса
User-agent	User-Agent браузера
Сигнатуры COB	Название сигнатуры COB
Угроза сигнатуры	Уровень угрозы сигнатуры COB
Зона источника	Название сетевой зона источника
IP-источника	IP-адрес источника
Порт источника	Номер порта источника
MAC-источника	MAC-адрес источника
Зона назначения	Название сетевой зоны назначения
IP-назначения	IP-адрес назначения
Порт назначения	Номер порта назначения
MAC-назначения	MAC-адрес назначения
NAT-адрес источника	IP-адрес источника после NAT-трансляции
NAT-порт источника	Порт источника после NAT-трансляции
NAT-адрес назначения	IP-адрес назначения после NAT-трансляции
NAT-порт назначения	Порт назначения после NAT-трансляции
Байт отправлено/получено	Количество отправленных и полученных байтов соответственно
Пакетов отправлено/получено	Количество отправленных и полученных пакетов соответственно
Конечное устройство/сенсор	ID сенсора
Счетчик	Имя счетчика
Объект SNMP	Идентификатор SNMP-объекта (SNMP OID)
Тип SNMP-объекта	Тип SNMP-объекта
Статус	Статус выполнения запроса к сенсору WMI или SNMP
Ошибка	Код ошибки при выполнении запроса к сенсору WMI или SNMP
Протокол АСУ ТП	Протокол прикладного уровня АСУ ТП
Уровень лога	Уровень важности события Windows. Могут быть указаны следующие значения: • Error — события, указывающие на существенные проблемы, которые могут привести к потере функциональности или данных; • Warning — события, указывающие на проблемы, которые не требуют немедленного реагирования, но могут привести к ошибкам в будущем; • Information — информирующие события, которые не требуют немедленного реагирования; • Audit Success — события при успешном обращении к ресурсам; • Audit Failure — события при неуспешном обращении к ресурсам
Источник журнала событий	Источник события Windows
Категория лога	Категория события Windows
Категория задачи	Категория задачи Windows
Имя компьютера	Имя источника события
Код события лога	Код события Windows
Идентификатор события лога	ID события Windows

Параметр	Описание
Тип события лога	Тип события Windows, которому соответствует определенный уровень важности события (см. параметр Уровень лога). Параметр относится к записям журнала событий конечных устройств. Могут быть указаны следующие значения: 1 — ошибка; 2 — предупреждение; 3 — сведения; 4 — аудит успеха; 5 — аудит отказа
Строка вставки	Данные события Windows после обработки
Файл журнала лога	Журнал Windows. Могут быть указаны следующие значения: Application — журнал приложений, содержащий события приложений и служб; Security — журнал безопасности, содержащий события системы аудита; System — системный журнал, содержащий события драйверов устройств; CustomLog — пользовательский журнал событий, содержащий события, зарегистрированные определенными приложениями
Команда	Код функции ACU ТП
Адрес регистра	Адрес регистра ACU ТП
Номер ASDU	Адрес ASDU (COA) для протокола IEC-104
Идентификатор устройства	ID устройства из базы данных OPC-сервера для протокола OPC UA
Имя переменной	Имя переменной для обмена данными в режиме реального времени по протоколу MMS
Хэш	Хеш-сумма приложения
Объект	Категория события syslog
Критичность	Уровень важности события syslog
Идентификатор процесса	ID процесса

Technology: SIEM

Version: 7.x

Documentation: 

Product: SIEM

В разделе **Аналитика → Действия реагирования** отображается список действий, которые выполняет UserGate SIEM при срабатывании того или иного правила аналитики. Действия реагирования назначаются каждому правилу аналитики при его создании.

Вы можете управлять действиями реагирования в списке: создавать, изменять, копировать и удалять действия реагирования, а также включать и отключать их. Для этого используются соответствующие кнопки в панели инструментов. Также вы можете фильтровать действия реагирования в списке по их состоянию. Так, например, можно просмотреть только включенные действия реагирования, применив фильтр **Показать включенные**.

При создании действия реагирования для выбора доступны следующие действия:

- отправка уведомлений по каналу связи:
 - [на электронную почту](#);
 - [номер телефона](#);
 - [URL-адрес](#) (с помощью механизма webhook);
- [регистрация инцидента](#);
- [отправка команды на коннектор](#);
- [отправка команды на конечное устройство](#).

Создание действия реагирования

Чтобы создать действие реагирования:

1. В разделе **Аналитика → Действия реагирования** нажмите **Добавить**.

Откроется окно создания действия реагирования.

2. На вкладке **Общие** выполните следующее:

- Включите действие реагирования.
- Укажите название и при необходимости описание действия реагирования.
- Выберите действие, которое следует выполнять при срабатываниях правила аналитики:
 - отправлять уведомления о срабатывании на указанные адреса электронной почты;
 - отправлять уведомления о срабатывании на указанные номера телефонов;
 - отправлять уведомления о срабатывании с помощью механизма webhook на указанный URL;
 - регистрировать инцидент;
 - отправлять команду на выбранный коннектор;
 - отправлять команду на конечное устройство.
- Если требуется журналировать данные действия реагирования, установите флажок **Записывать в журнал правил**. Записи о выполнении действия реагирования будут отображаться в журнале событий UserGate SIEM в разделе **Журналы и отчеты → Журналы**.
- Если требуется выполнять действие реагирования для группы срабатываний, настройте группировку срабатываний правила аналитики по одному из следующих параметров:
 - **Никогда**. По умолчанию группировка отключена.
 - **За период времени**. Действие реагирования будет выполнено, если в течение указанного времени правило аналитики работает хотя бы один раз.
 - **По количеству срабатываний**. Действие реагирования будет выполнено после указанного количества срабатываний правила аналитики.
 - **В существующий инцидент**. Параметр доступен только при выборе действия **Создать инцидент**. По первому срабатыванию правила аналитики будет зарегистрирован инцидент, а все последующие срабатывания правила будут добавляться в этот инцидент в виде новых записей в блоке **Срабатывания**.

3. На вкладке **Действие** укажите параметры, соответствующие действию, выбранному на шаге 2. Ниже приведены параметры для каждого действия.

Для отправки уведомлений на электронную почту укажите следующие параметры:

- [Профиль оповещения SMTP](#), который будет использоваться для отправки уведомлений.
- Адрес электронной почты отправителя.
- Тему уведомлений.
- Группы адресов электронной почты получателей уведомлений. По кнопке **Добавить** вы можете выбрать [группы адресов](#), созданные в разделе **Настройки → Библиотеки → Почтовые адреса**. Также вы можете создать новые группы адресов по кнопке **Создать и добавить новый объект**.

Для отправки уведомлений на номер телефона укажите следующие параметры:

- [Профиль оповещения SMPP](#), который будет использоваться для отправки уведомлений.
- Имя отправителя уведомлений.
- Группы номеров телефонов получателей уведомлений. По кнопке **Добавить** вы можете выбрать [группы номеров телефонов](#), созданные в разделе **Настройки → Библиотеки → Номера телефонов**. Также вы можете создавать новые группы номеров телефонов по кнопке **Создать и добавить новый объект**.

Для отправки уведомлений на URL с помощью webhook:

Укажите URL-адрес веб-ресурса, на который будут отправляться уведомления.

Примечание Вы можете протестировать отправку уведомлений с помощью сервиса [webhook.site](#). Для этого в качестве URL необходимо указать адрес, сгенерированный сервисом, например <https://webhook.site/7e8d2095-02d0-41aa-atc9-588552c515d1>. Кроме того, для отправки уведомлений вы можете [настроить интеграцию UserGate SIEM с Telegram](#).

Для регистрации инцидента укажите следующие параметры:

- Название инцидента.
- Тип инцидента.
- Приоритет инцидента.
- Ответственного за расследование инцидента.

- Наблюдателей за состоянием инцидента.
Если в инцидент требуется добавлять последующие срабатывания правила аналитики, установите флажок **Добавлять срабатывания**.
Если к инциденту требуется прикрепить PCAP-файл, сгенерированный по срабатыванию правила аналитики, установите флажок **Приложить файлы PCAP**.

Для отправки команды на коннектор укажите следующие параметры:

- Устройства, на которые будет отправляться команда. С помощью кнопки **Добавить** вы можете выбрать [коннекторы](#), добавленные в разделе **Настройки → Сенсоры → Коннекторы**. Следует выбирать только коннекторы с одинаковой группой команд.
- Команду для устройств. В раскрывающемся списке выберите [команду из группы](#), указанной для коннекторов. Если команда [содержит переменные](#), укажите их значения в отобразившихся полях.

Для отправки команды на конечное устройство выберите одну из следующих команд:

- **Отключить от сети**. Ограничение доступа конечного устройства в интернет.
- **Завершить процесс**. Завершение на конечном устройстве процесса по его идентификатору, полученному после выполнения [запроса правила аналитики](#).

4. На вкладке **Шаблон** введите описание шаблона, который будет использоваться для уведомлений по выбранному каналу связи, а также для описания инцидента.

ПримечаниеЭтот шаг инструкции следует выполнять, если в качестве действия на шаге 2 вы выбрали регистрацию инцидента или отправку уведомлений по электронной почте, номеру телефона или URL-адресу (с помощью webhook).

В описании шаблона вы можете указывать переменные, относящиеся к срабатыванию правила аналитики, их необходимо вводить прописными буквами в формате {имя переменной>}, например {ANALYTICS_RULE_NAME}. [В таблице ниже](#) приведены переменные, которые вы можете использовать.

5. Нажмите **Сохранить**.
Созданное действие реагирования отобразится в списке действий раздела.

Переменные в командах и в шаблонах уведомлений

Если в запросе правила аналитики указаны переменные, вы можете использовать их в командах и в шаблонах уведомлений [при создании действия реагирования](#). Такие переменные перечислены в таблице ниже.

Переменная	Описание
{ANALYTICS_RULE_NAME}	Название правила аналитики
{ANALYTICS_RULE_DESCRIPTION}	Описание правила аналитики
{NAME}	Название срабатывания правила аналитики
{TIME}	Время срабатывания правила аналитики
{TRIGGERED_ALERTS_NUMBER}	Количество срабатываний правила аналитики
{FIRST_TRIGGERED_ALERT_TIME}	Время первого срабатывания правила аналитики
{LAST_TRIGGERED_ALERT_TIME}	Время последнего срабатывания правила аналитики
{TRIGGERED_ALERTS_NAMES}	Список названий срабатываний правила аналитики, если срабатывания сгруппированы по параметру
{FIRST_EVENT_TIME}	Время первого события, на которое сработало правило аналитики
{LAST_EVENT_TIME}	Время последнего события, на которое сработало правило аналитики
{THREAT_LEVEL}	Уровень опасности угрозы по срабатыванию правила аналитики
{CATEGORY}	Категория срабатывания правила аналитики
{PRIORITY}	Приоритет срабатывания правила аналитики
{ADMINISTRATOR_NAME}	Администратор, создавший правило аналитики
{USER_NAME}	Имя пользователя, под учетной записью которого сработало правило аналитики
{SOURCE_ZONE}	Зона источника подключения
{DESTINATION_ZONE}	Зона назначения подключения
{SOURCE_COUNTRY}	Страна источника подключения
{DESTINATION_COUNTRY}	Страна назначения подключения
{SOURCE_IP}	IP-адрес источника подключения
{SOURCE_PORT}	Порт источника подключения
{DESTINATION_IP}	IP-адрес назначения подключения

Переменная	Описание
{DESTINATION_PORT}	Порт назначения подключения
{SOURCE_ZONE_ALL}	Зоны источников событий, на которые сработало правило аналитики
{DESTINATION_ZONE_ALL}	Зоны назначения событий, на которые сработало правило аналитики
{SOURCE_COUNTRY_ALL}	Страны источников событий, на которые сработало правило аналитики
{DESTINATION_COUNTRY_ALL}	Страны назначения событий, на которые сработало правило аналитики
{SOURCE_IP_ALL}	IP-адреса источников событий, на которые сработало правило аналитики
{SOURCE_PORT_ALL}	Порты источников событий, на которые сработало правило аналитики
{DESTINATION_IP_ALL}	IP-адреса назначения событий, на которые сработало правило аналитики
{DESTINATION_PORT_ALL}	Порты назначения событий, на которые сработало правило аналитики

Documentation: ☒
Product: SIEM
Version: 7.x
Technology: SIEM

В разделе **Аналитика → Срабатывания** отображаются срабатывания правил аналитики.

В таблице срабатываний вы можете:

- изменять набор столбцов в контекстном меню **Столбцы**, доступном по нажатию справа от заголовка столбца;
- изменять ширину столбцов;
- изменять порядок следования столбцов, перемещая заголовок столбца;
- сортировать данные по нажатию на заголовки столбцов (не все столбцы поддерживают функцию сортировки).

Фильтрация данных о срабатываниях

Вы можете фильтровать данные в таблице, выбрав один из следующих режимов:

- **Простой** — фильтрация с помощью доступных параметров. Например, по дате и времени срабатывания, идентификатору срабатывания, сработавшему правилу аналитики, а также приоритету этого правила. Для выбора параметров используются соответствующие кнопки в панели инструментов. В раскрывающемся по кнопке **Еще** списке вы также можете выбирать дополнительные параметры фильтрации, устанавливая соответствующие флажки.
- **Расширенный** — фильтрация с помощью специальных выражений [на языке запросов](#). Для формирования запроса вы можете использовать доступные параметры и их значения, а также логические операторы и операторы сравнения.

Кроме того, вы можете сохранять примененные фильтры по кнопке **Сохранить как**. Список сохраненных фильтров доступен по кнопке **Популярные фильтры**. Также для дальнейшего анализа вы можете скачать отфильтрованные данные таблицы в виде CSV-файла по кнопке **Экспортировать в CSV**. Для сброса примененных фильтров доступна кнопка **Сброс**.

Просмотр записи о срабатывании

Запись о срабатывании в таблице содержит следующие данные.

Параметр	Описание
Узел	Имя устройства
Время	Время срабатывания правила
Идентификатор срабатывания	Идентификатор срабатывания правила
Время первого события	Дата и время первого срабатывания правила
Время последнего события	Дата и время последнего срабатывания правила
Количество событий	Количество всех событий, на которые сработало правило
Правило	Название правила аналитики
Категория срабатывания	По умолчанию для срабатываний доступны следующие категории: • Security — срабатывания категории указывают на инциденты, приводящие к ослаблению безопасности информационных систем; • Availability — срабатывания категории указывают на инциденты, приводящие к ухудшению доступности информационных систем; • Performance — срабатывания категории указывают на инциденты, приводящие к снижению производительности информационных систем Вы можете создавать дополнительные категории срабатываний правил аналитики в разделе Настройки → Библиотеки → Категории срабатываний
Приоритет	Приоритет срабатывания, указанный при создании правила аналитики: • Низкий — имеет низкий уровень важности и не требует незамедлительного реагирования; • Нормальный — требует обратить внимание и при необходимости принять соответствующие меры; • Важный — требует обратить внимание и принять соответствующие меры; • Критический — требует незамедлительного реагирования
Конечное устройство/сенсор	ID сенсора
Имя компьютера	Имя источника события
Пользователь	Имя пользователя
Сигнатуры COB	Название сигнатуры COB
Зона источника	Название сетевой зона источника
IP-источника	IP-адрес источника
Порт источника	Номер порта источника
Зона назначения	Название сетевой зоны назначения
IP-назначения	IP-адрес назначения
Порт назначения	Номер порта назначения

Вы также можете просматривать основную информацию о срабатывании в его карточке, которая открывается по нажатию на иконку срабатывания.

Действия со срабатыванием

С выбранным срабатыванием в таблице вы можете выполнять следующие действия:

- Добавлять срабатывание в зарегистрированный ранее инцидент (по кнопке **Добавить в инцидент**).
- Просматривать основную информацию о срабатывании в его карточке (по кнопке **Показать**).
- Просматривать подробную информацию о срабатывании на отдельной вкладке раздела **Аналитика** (по кнопке **Показать подробно**). При выборе инцидента в списке вам также доступна регистрация нового инцидента по кнопке **Создать новый инцидент**.

Просмотр подробной информации о срабатывании

Technology: SIEM
Documentation: 
Product: SIEM
Version: 7.x

В разделе **Аналитика → Подробности срабатывания** вы можете просматривать подробную информацию о каждом срабатывании правила аналитики. Для этого в блоке **Срабатывание** из выпадающего списка выберите идентификатор нужного срабатывания. Информация о срабатывании отобразится в таблице и в соответствующих блоках.

Вы можете управлять выбранным срабатыванием:

- Просматривать основную информацию о срабатывании в его карточке (по кнопке **Показать**).
- Просматривать срабатывание в таблице всех срабатываний (по кнопке **Показать срабатывания**).
- Добавлять срабатывание в зарегистрированный ранее инцидент (по кнопке **Добавить в инцидент**). При выборе инцидента в списке вам также доступна [регистрация нового инцидента](#) по кнопке **Создать новый инцидент**.

Просмотр списка процессов конечных устройств

Documentation: ☒
Product: SIEM
Version: 7.x
Technology: SIEM

В разделе **Аналитика → Процессы конечных устройств** отображается информация о процессах устройств с установленным ПО UserGate Client. Например, информация о процессах запущенных приложений, о фоновых процессах устройств, а также о системных процессах Windows. Вы можете просматривать параметры запуска этих процессов, а также отслеживать цепочки их вызовов.

В левой части страницы в блоке **Лог процессов** отображается таблица процессов, в которой вы можете:

- изменять набор столбцов в контекстном меню **Столбцы**, доступном по нажатию справа от заголовка столбца;
- изменять ширину столбцов;
- изменять порядок следования столбцов, перемещая заголовок столбца;
- сортировать данные по нажатию на заголовки столбцов (не все столбцы поддерживают функцию сортировки).

Также вы можете фильтровать данные в таблице процессов, выбрав один из следующих режимов:

- **Простой** — фильтрация с помощью доступных параметров. Например, по дате и времени запуска процесса, конечному устройству, на котором запущен процесс, а также по названию запущенного приложения. Для выбора параметров используются соответствующие кнопки в панели инструментов.
- **Расширенный** — фильтрация с помощью специальных выражений [на языке запросов](#). Для ввода выражений используется строка запросов.

Запись о процессе в таблице содержит следующие данные:

- дату и время запуска процесса;
- название конечного устройства, на котором запущен процесс;
- название запущенного приложения;
- идентификатор процесса.

Для выбранной записи в таблице вы можете просматривать подробную информацию о процессе, а также его дерево процессов. Действия доступны в правой части страницы в блоке **Процесс** на вкладках **Информация о процессе** и **Дерево процессов** соответственно.

Использование списков из библиотек в поисковых запросах

Product: SIEM
Version: 7.x
Technology: SIEM

В UserGate SIEM можно использовать списки из библиотек в поисковых запросах везде, где они есть: в правилах аналитики, в поиске, в журналах, в дашбордах, в пользовательских отчетах.

Данные в списки заносятся либо вручную (для локальных списков), либо пополняются через указанный в настройках внешний URL обновления (для обновляемых списков). Если в правилах аналитики в фильтрах условий срабатывания используются списки, то новые элементы поиска будут добавляться в правила динамически по мере их добавления в списки.

Функция поддерживается для следующих видов списков:

Тип списка	Поле в запросе
IP-адреса	ipSource, ipDest, natIpSource, natIpDest
Списки URL	url
Типы контента	mime
Useragent браузеров	userAgent
Категории URL	urlCategory
Текстовые списки	user, rule, zoneSource, zoneDest, macSource, macDest, applicationName, httpProtocol, httpMethod, referer, sensor, computerName, logFile, data, hash, cmdLine, device, service, image, originalFilename, parentImage, parentCommandLine, targetObject, targetFilename, scriptBlockText, queryName, queryResult, workstationName, logonId, imageLoaded, sourceImage, targetImage, customString1.. customString15

Для использования списка в запросах необходимо:

1. Создать список с включенной опцией **Использовать в поисковых запросах**.
2. Добавить в него элементы списка.
3. Добавить список в поисковый запрос.

Подробнее о поддерживаемых видах и типах списков читайте в разделе [Библиотеки](#). При активации в свойствах списка опции **Использовать в поисковых запросах** создается внутренний словарь БД с содержимым этого списка и обработчик событий изменения списка.

В поисковых запросах списки могут использоваться с операторами **IN** и **NOT IN**. Синтаксис: <field name> **IN** <list name>. При получении запросов значения из запроса сравниваются со значениями из словаря.

Для IP-листов запрос вида: *ipSource IN list_1* проверяет, находится ли ipSource в каком-либо из диапазонов IP-адресов из списка list_1.

Для useragent браузеров, типов контента, списков URL, категорий URL, текстовых списков запросы *userAgent IN list_1, mime IN list_2, url IN list_3, urlCategory IN games, signatureName IN list1* проверяют, равно ли значение поля какому-либо значению из списка.

Пример:

1. Создадим список вида IP-адреса со следующим содержимым:

2. Создадим список вида Useragent браузеров со следующим содержимым:

3. Добавим созданные списки в фильтр условия правила аналитики:

В результате работы правила произойдет срабатывание на основании выбранных фильтров со списками в условии срабатывания правила:

--	--

Отправка уведомлений UserGate SIEM через Telegram

Version: 7.x
Technology: SIEM
Product: SIEM

UserGate SIEM может быть интегрирован с Telegram для отправки уведомлений событий информационной безопасности.

Для такой интеграции понадобятся несколько компонентов:

- Заранее созданный чат-бот и Telegram-канал, в который чат-бот будет отправлять уведомления из UserGate SIEM.
- Веб-сервер, который будет выступать связующим звеном между UserGate SIEM и Telegram.
- Созданное в UserGate SIEM действие реагирования, использующее метод webhook в качестве механизма отправки событий информационной безопасности, генерируемых в SIEM.

UserGate SIEM инициирует действие webhook, отправляя на веб-сервер данные, которые должны быть переданы в Telegram. Веб-сервер обрабатывает полученные данные и посредством чат-бота отправляет в Telegram-канал данные из UserGate SIEM.

1. Инструкцию по созданию чат-бота можно найти на сайте Telegram (<https://core.telegram.org/bots/tutorial>) или на других ресурсах в Интернете. Дополнительно нужно создать Telegram-канал и разрешить чат-боту минимальные привилегии - постить сообщения.

Результатом этого подготовительного шага должны быть:

- Токен чат-бота. Он будет передан в диалоге с BotFather при создании бота.
- Токен канала. Его можно получить, добавив в целевой канал специального бота @username_to_id_bot, либо в адресной строке браузера, например: `https://web.telegram.org/a/#-xxxxxxxxxxxxx`, где "-xxxxxxxxxxxxx" — токен канала.

2. Необходимо запустить веб-сервер, который будет обрабатывать данные из UserGate SIEM. Пример кода на FastAPI: <https://gitflic.ru/project/cisecs/telegram-bot-and-webhooks/>.

3. В UserGate SIEM на странице **Действия реагирования** в разделе **Аналитика** необходимо создать действие реагирования типа webhook:

На вкладке **Действие** прописать URL созданного веб-сервера, например:

На вкладке **Шаблон** создать шаблон сообщения, например:

Добавить созданное действие реагирования в правило аналитики:

Общие сведения

Documentation: ☒

Technology: IRP

Version: 7.x

Product: SIEM

Раздел **Инциденты** предоставляет функциональность встроенной в UserGate SIEM системы IRP — платформы управления процессами реагирования на инциденты информационной безопасности. Инцидентом считается событие или набор событий информационной безопасности, которые подлежат расследованию. UserGate SIEM позволяет настроить процесс расследования инцидентов индивидуально под нужды конкретной компании (подробнее читайте разделе [Настройки инцидентов](#)).

IRP система плотно интегрирована с UserGate SIEM, функциональность которой представлена разделом [Аналитика](#). Раздел **Аналитика** позволяет задать создание инцидента в качестве действия реагирования, тем самым автоматизируя процесс создания инцидентов информационной безопасности (подробнее о настройке действий реагирования читайте в разделе [Действия реагирования](#)).

Также, помимо автоматического создания, инциденты могут быть созданы вручную инженером информационной безопасности (подробнее читайте в разделе [Создание инцидентов безопасности](#)).

Настройки инцидентов

Technology: IRP
Version: 7.x
Product: SIEM
Documentation: 

Процесс расследования инцидента проходит в несколько этапов, на каждом из которых инциденту присваивается определенный статус или **Состояние**, например, **Открыт → Сбор данных → В работе → Закрыт**. Переход между состояниями возможен по определенным правилам, определяемыми администратором, например, нельзя перейти из состояния **Открыт** сразу в состояние **Закрыт**. Возможные переходы между состояниями инцидентов описываются в **Схеме инцидентов**.

По окончании расследования каждому инциденту присваивается **Решение**, например, ложная атака, подтвержденная атака, выполнено и т.п.

Тип инцидента выбирается на этапе создания инцидента и определяет назначение инцидента. Например, типом инцидента может быть Инцидент безопасности, Задача и т.п.

Схема инцидента связывает воедино состояния, возможные переходы между состояниями, решения и типы инцидентов, формируя процесс расследования инцидента информационной безопасности.

UserGate SIEM позволяет настроить процесс расследования инцидентов индивидуально под нужды конкретной компании. После первоначальной установки решения создается схема расследования по умолчанию с названием **Incident**. Администратор системы может изменить существующую схему или создать свою собственную схему. Можно создать несколько схем расследования инцидентов, но использоваться может только одна схема, которая является активной.

Чтобы создать свою собственную схему расследования инцидентов необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создайте необходимые решения инцидентов	В разделе Настройки инцидентов → Решения инцидентов нажмите добавить, укажите название и описание создаваемого решения и нажмите кнопку Сохранить .
Шаг 2. Создайте типы инцидентов	В разделе Настройки инцидентов → Типы инцидентов нажмите добавить, укажите название и описание создаваемого типа и нажмите кнопку Сохранить .
Шаг 3. Создайте состояния инцидентов	В разделе Настройки инцидентов → Состояния инцидентов нажмите добавить, укажите название, описание и группу создаваемого состояния. Группа состояние определяет положение данного состояние в схеме состояний. Возможно 3 варианта: • Открыто — данная группа назначается состояниям инцидентов, по которым еще не начата работа или она приостановлена. Как правило, это начальные состояния инцидентов, например Создан. Все состояния данной группы помечаются синим цветом в веб-консоли. • В работе — данная группа назначается состояниям инцидентов, по которым ведется, но еще не завершена работа. Это промежуточные состояния инцидентов, например, В работе, Расследование. Все состояния данной группы помечаются желтым цветом в веб-консоли. • Закрыто — данная группа назначается состояниям инцидентов, по которым завершена работа. Это конечные состояния инцидентов, например, Завершено, Закрыто. При переходе в состояние этой группы необходимо обязательно указать решение инцидента, например, Ложная атака, Подтвержденная атака, Выполнено. Все состояния данной группы помечаются зеленым цветом в веб-консоли. После определения всех полей нажмите кнопку Сохранить.
Шаг 4. Создайте схему инцидентов	В разделе Настройки инцидентов → Схемы инцидентов нажмите добавить и укажите следующие параметры: • Сделать активной — делает данную схему активной. Только одна схема может быть активной, если была активна другая схема, то данное действие делает ее не активной, и все новые и существующие инциденты перейдут на работу по новой схеме. • Схема — название схемы. • Префикс — префикс, который будет использован при назначении идентификаторов создаваемым инцидентам. Идентификатор будет иметь вид Префикс — порядковый номер, например INC-99. • Описание — необязательное описание данной схемы. • Состояния рабочего процесса — описывает все состояния, которые может принимать инцидент в своем жизненном цикле. Добавьте сюда все состояния инцидентов, созданные на предыдущем шаге. • Начальное состояние — указывает начальное состояние, которое принимает инцидент при его создании. • Переходы — необходимо указать все возможные переходы между состояниями и дать им названия. Например, создать переход под названием Взять в работу для перехода из состояния Открыто в состояние В работе. Перевод инцидента между состояниями возможен только для тех состояний, между которыми определены переходы. • Решения инцидентов — указывает список возможных решений инцидентов. Решение является обязательным при завершении работы по расследованию тикета, то есть при переводе его в состояние, относящееся к группе закрыто. Выберите все необходимые решения, которые были созданы ранее. • Типы инцидентов — укажите типы инцидентов, которые могут быть использованы в этой схеме.
Шаг 5. Активируйте схему инцидентов	После создания схемы инцидентов ее необходимо активировать. Для этого активируйте чекбокс Сделать активной в настройках схемы инцидентов.

Дашборд по инцидентам

Technology: IRP
Version: 7.x
Product: SIEM
Documentation: 

В данной вкладке можно просмотреть текущее состояние инцидентов информационной безопасности, созданных на UserGate SIEM. Отчеты представлены в виде виджетов, которые могут быть настроены администратором системы в соответствии с его требованиями. Виджеты можно добавлять, удалять, изменять расположение и размер на странице Дашборд.

Некоторые виджеты позволяют настроить отображение, указать фильтрацию данных и настроить прочие параметры. Для настройки виджета необходимо кликнуть по символу шестеренки в правом верхнем углу. Не все параметры, перечисленные ниже, доступны для каждого типа виджетов.

Наименование	Описание
Название	Название виджета, которое будет отображено в Дашборд.
Диаграмма	Тип представления данных: - Число. - Вертикальная гистограмма. - Таблица.
Запрос фильтра	SQL-подобная строка запроса, позволяющая ограничить объем информации, используемой при построении виджета.
Описание	Описание виджета.
Количество записей	Максимальное количество записей для отображения.

Журнал инцидентов

Version: 7.x
Technology: IRP
Product: SIEM
Documentation:

Во вкладке **Журнал инцидентов** представлен список созданных инцидентов информационной безопасности. В таблице отражена следующая информация об инцидентах.

Наименование в базе данных	Наименование в поисковом запросе	Описание
Создан	date	Дата и время создания инцидента.
Изменён	updateDate	Дата и время последнего изменения.
Индекс	incidentPrefix	Префикс инцидента (INC-N, где N — порядковый номер инцидента; нумерация начинается с 0).
Имя	incidentName	Название инцидента.
Правило	rule	Название правила аналитики, в результате срабатывания которого автоматически был создан инцидент, т.е. при настройке правила аналитики было задано действие реагирования Создать инцидент .
Статус	status	Статус инцидента. Существует 3 группы состояний, которые определяют положение данного состояние в схеме состояний: • Открыто — данная группа назначается состояниям инцидентов, по которым еще не начата работа или она приостановлена. Как правило, это начальные состояния инцидентов, например Создан. Все состояния данной группы помечаются синим цветом в веб-консоли. • В работе — данная группа назначается состояниям инцидентов, по которым ведется, но еще не завершена работа. Это промежуточные состояния инцидентов, например, В работе, Расследование. Все состояния данной группы помечаются желтым цветом в веб-консоли. • Закрыто — данная группа назначается состояниям инцидентов, по которым завершена работа. Это конечные состояния инцидентов, например, Завершено, Закрыто. При переходе в состояние этой группы необходимо обязательно указать решение инцидента, например, Ложная атака, Подтвержденная атака, Выполнено. Все состояния данной группы помечаются зеленым цветом в веб-консоли. По умолчанию в UserGate создана схема Incident, которая содержит переходы между всеми состояниями. Схемы инцидентов можно добавить в разделе Настройки → Настройка инцидентов → Схема инцидентов. Дополнительные состояния инцидентов можно задать во вкладке Настройки → Настройка инцидентов → Состояния инцидентов. Подробнее читайте в разделе Настройки инцидентов.
Решение	resolution	Решение инцидента. По умолчанию созданы: • False positive: ложная атака. • True positive: подтвержденная атака. • Duplicate: проблема повторяет другую проблему. • Won't do: задача не выполнима. • Done: проблема решена. Дополнительные решения инцидентов можно создать во вкладке Настройки → Настройка инцидентов → Решения инцидентов. Подробнее читайте в разделе Настройки инцидентов.
Тип	type	Тип инцидента. По умолчанию доступны 2 типа: инцидент безопасности и задача. Дополнительно типы инцидентов можно создать в разделе Настройки → Настройка инцидентов → Типы инцидентов . Подробнее читайте в разделе Настройки инцидентов .
Приоритет	priority	Приоритет инцидента: • Низкий. • Нормальный. • Важный. • Критический.
Инициатор	reporter	Имя администратора, который создал инцидент.
Последнее изменение	lastChangeBy	Имя администратора, который внёс последнее изменение.
Назначен	assignee	Имя администратора, назначенного на инцидент.
Активность		Количество комментариев, срабатываний правил аналитики и журналов событий, добавленных в инцидент.

Администратор может выбрать для показа только те столбцы, которые ему необходимы. Для этого необходимо навести указатель мыши на название любого столбца, нажать на появившуюся справа от названия столбца стрелку, выбрать **Столбцы** и в появившемся контекстном меню выбрать необходимые параметры.

Возможно производить фильтрацию инцидентов по параметрам, представленным в таблице. Фильтрация доступна в двух режимах: простой и расширенный (подробнее о синтаксисе расширенного поиска читайте в разделе [Поиск и фильтрация данных](#)).

Настроенные фильтры можно сохранять, нажав кнопку **Сохранить как**. Сохранённые фильтры можно просмотреть с использованием кнопки **Популярные фильтры**.

Нажатием кнопки **Экспортировать в CSV** администратор может скачать отфильтрованный список инцидентов в csv-файл для дальнейшего анализа.

Создание инцидентов безопасности

Technology: IRP
Version: 7.x
Product: SIEM
Documentation: 

Во вкладке **Журнал инцидентов** также можно создавать инциденты информационной безопасности. Для создания и работы с инцидентами информационной безопасности пользователь должен обладать определёнными ролевыми разрешениями (подробнее читайте в разделе [Роли и ролевые разрешения пользователей](#)).

Инциденты создаются нажатием кнопки **Создать инцидент**. Далее необходимо указать следующие параметры.

Наименование	Описание
Имя	Указать название инцидента информационной безопасности.
Тип	Указать тип инцидента. По умолчанию созданы 2 типа инцидентов: инцидент безопасности и задача. Дополнительно типы инцидентов могут быть созданы в разделе Настройки → Настройка инцидентов → Типы инцидентов . Подробнее читайте в разделе Настройки инцидентов .
Приоритет	Назначить приоритет - Низкий. - Нормальный. - Важный. - Критический.
Назначен	Назначить ответственного на инцидент.
Наблюдатели	Указать список сотрудников для наблюдения за инцидентом. При любых изменениях инцидента они будут получать уведомление.
Вложения	Прикрепить файлы, относящиеся к инциденту.
Описание	Ввести описание инцидента.

Подробности инцидента

Technology: IRP
 Version: 7.x
 Product: SIEM
 Documentation: 

Выбор инцидента и нажатие кнопки **Показать** произведет перевод на новую вкладку (название вкладки формируется из индекса и заданного имени инцидента), где будет отображена подробная информация о выбранном инциденте. На данной вкладке также можно редактировать (кнопка **Редактировать**) и комментировать (кнопка **Комментировать**) инцидент, изменять ответственного за инцидент (кнопка **Назначить**), и статус рабочего процесса (кнопка **Рабочий процесс**). Помимо информации об инциденте, отображённой во вкладке **Журнал инцидентов** (подробнее читайте в разделе [Журнал инцидентов](#)), можно увидеть следующую информацию.

В разделе **Срабатывания** отражена информация о срабатываниях правил аналитики, добавленных в инцидент. Подробнее читайте в разделе [Срабатывания](#). Добавить срабатывания в инцидент можно нажатием кнопки **Добавить срабатывания**. Далее необходимо выбрать срабатывания, которые необходимо добавить в инцидент. Чтобы просмотреть подробности срабатывания выделите нужное срабатывание правила аналитики и нажмите кнопку **Показать подробно**. Также можно просмотреть краткую информацию о срабатывании нажав на кнопку **Показать**. Нажатием на кнопку **Удалить из инцидента** можно удалить запись о срабатывании правила аналитики из инцидента. Список срабатываний правил аналитики, добавленный в инциденты, можно скачать в csv-файл для дальнейшего анализа нажатием кнопки **Экспортировать в CSV**.

В разделе **Журналы** отображена подробная информация о событиях всех журналов (подробнее о записях журналов читайте в разделе [Поиск](#)). Чтобы добавить события в инцидент нажмите **Добавить в инцидент** и выберите события для добавления. Нажатие кнопки **Удалить из инцидента** позволяет удалить ненужные события.

В разделе **Улики** отображены записи о наблюдениях за объектами, указанными при настройке. Улики необходимы для упрощения анализа инцидента информационной безопасности, принятия верного решения и уменьшения затраченного на инцидент времени. Для получения информации используются ресурсы для обогащения (подробнее читайте в разделе [Внешние сервисы обогащений](#)). Подробную информацию, предоставленную сервисом, можно увидеть в настройках обогащения, нажав на обогащение.

Улики можно создать нажатием кнопки **Добавить**. Далее необходимо указать параметры, которые будут отражены в таблице раздела.

Наименование	Описание
Тип улики	Возможен выбор одного из следующих типов улик: Автономная система: система IP-сетей и маршрутизаторов, находящихся под единым управлением. Домен: имя сайта в Интернете. Файл: файл, о котором необходимо собрать информацию. Имя файла: название файла, о котором необходимо собрать информацию. FQDN: полное доменное имя. Хэш: хэш какого-либо файла, например, добавленного в инцидент. Имя хоста: метка устройства, подключённого к компьютерной сети и использующаяся для идентификации устройства. IP: уникальный адрес, идентифицирующий устройство в компьютерной сети. Почта: адрес электронной почты. Тема письма: часть письма, указанная в поле subject. Реестр: ключ реестра Microsoft Windows — каталог, в котором хранятся настройки и параметры операционной системы. Путь URI: последовательность символов, идентифицирующая абстрактный или физический ресурс. URL: индивидуальный адрес ресурса в сети Интернет. Агент пользователя: буквенно-цифровая строка, идентифицирующая программу, которая отправляет запрос на сервер и одновременно запрашивает доступ к web-сайту. Другое.
Значение	Необходимо указать объект, с которым будет производиться работа: IP-адрес, домен, и т.п.
Тип атаки	Для указания доступны следующие типы атаки: Ботнет — сеть заражённых компьютеров, удалённо управляемых преступниками. Фишинг — вид Интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Вредоносное ПО — любое программное обеспечение, которое пытается заразить компьютер или мобильное устройство. DDoS — способ заблокировать работу сайта путем подачи большого количества запросов, превышающих пропускную способность сети. Угон трафика — злоумышленное перенаправление трафика. Сетевое сканирование — сканирование узлов сети для определения уязвимостей. Брутфорс — метод взлома учётных записей путём подбора паролей к ним. Компроментация — факт несанкционированного доступа к защищенной информации, а также подозрение осуществления такого доступа. Спам — массовая рассылка с использованием специальных программ, коммерческой, политической и иной рекламы или иного вида сообщений людям, не выразившим желания их получать. Другое.
TLP	Отображена маркировка конфиденциальной информации (Traffic Light Protocol). Возможны следующие маркировки: RED: информация является крайне конфиденциальной. AMBER: информацией можно поделиться в рамках своей организации, при условии, что этой информацией нужно поделиться. GREEN: информация может быть широко распространена в пределах определённого сообщества. WHITE: информация в свободном распространении, но не нарушает авторские права.
Индикатор компроментации?	Чекбокс необходимо отметить, если объект является потенциальным индикатором компроментации.
Сервисы	Отображён список сервисов, которые используются для получения дополнительной информации об объектах наблюдения. Список сервисов отображается автоматически после выбора типа улики. Список сервисов доступен в разделе Настройки → Библиотеки → Внешние сервисы обогащений . Подробнее читайте в разделе Внешние сервисы обогащений.
Обновлено	Показаны дата и время последнего обновления сервиса.

С использованием соответствующих кнопок **Редактировать** и **Удалить** улики можно редактировать или удалять.

В разделе **Активность** можно просмотреть комментарии по инциденту и историю внесения изменений (добавление наблюдателей, изменение статуса рабочего процесса и т.д.).

С использованием кнопки **Создать отчёт** можно создать отчёт об инциденте:

- Incident report**: пользовательский отчёт, который может быть создан на английском или русском языках в формате PDF или HTML. При создании отчёта возможно использование шаблонов, список которых доступен в разделе **Журналы и отчёты → Отчёты инцидентов → Правила отчётов инцидентов** .
- GOSSOPKA report**: для создание отчёта используется шаблон **Форма для ГОССОПКА**, который соответствует требованиям к отчётам ГОССОПКА. Отчёт можно просто скачать (кнопка **Создать файл**) или сразу сформировать в требуемом формате и отправить в систему личных кабинетов ГОССОПКА (кнопка **Послать через сеть**). Для автоматической отправки отчёта пользователю необходимо предоставить учётную запись для входа в личный кабинет на сайте ГОССОПКА и защищённый канал передачи. Подробнее читайте в разделе [Передача отчётов об инцидентах информационной безопасности в ГосСОПКА](#).

Передача отчётов об инцидентах информационной безопасности в ГосСОПКА

Technology: IRP
Version: 7.x
Product: SIEM
Documentation:

ГосСОПКА — Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Целью создания ГосСОПКА является защита критической информационной инфраструктуры (КИИ), владельцы объектов которой должны подключиться к ГосСОПКА. Также к ГосСОПКА можно подключиться и на добровольной основе для обеспечения более высокого уровня информационной безопасности и улучшения методов выявления и реагирования на инциденты.

В UserGate SIEM реализована возможность передачи отчётов о компьютерных атаках, инцидентах и уязвимостях в стандартизированном формате через личный кабинет ГосСОПКА.

Для отправки отчётов необходимо:

- 1. Самостоятельно подключиться к системе личных кабинетов ГосСОПКА.

Подключение необходимо для взаимодействия и автоматизации обмена информацией о зафиксированных инцидентах информационной безопасности и методах их предотвращения с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак.

- 2. Добавить криптографический шлюз для организации межсетевого взаимодействия с сетью НКЦКИ (Национальный координационный центр по компьютерным инцидентам; главный центр ГосСОПКА).

Для самостоятельного подключения к ГосСОПКА используются аппаратно-программные комплексы компаний Инфотекс (ViPNet), Код безопасности (Континент), С-Терра (С-Терра Шлюз).

ПримечаниеНе указывайте криптографический шлюз в качестве шлюза по умолчанию.

- 3. Добавить DNS-серверы для определения адреса системы личных кабинетов ГосСОПКА.

Для определения адреса системы личных кабинетов ГосСОПКА необходимо добавить серверы с адресами 10.0.100.49 и 10.0.100.50.

ПримечаниеВ список системных DNS-серверов можно добавить не более трёх серверов. Серверы ГосСОПКА не могут быть использованы для преобразования доменных имён в сети Интернет.

- 4. Настроить статический маршрут в сеть ГосСОПКА для обеспечения доступности DNS-серверов, указанных в пункте 3.

Для обеспечения доступности серверов ГосСОПКА необходимо добавить статический маршрут с адресом назначения: 10.0.100.0/24. Подробнее о настройке маршрутов читайте в разделе [Маршруты](#).

- 5. Настроить подключение к личному кабинету ГосСОПКА с UserGate SIEM для возможности отправки отчёта.

В UserGate SIEM по умолчанию создан коннектор **Gossopka**, предназначенный для взаимодействия с ГосСОПКА.

Для настройки коннектора перейдите во вкладку **Настройки** в раздел **Сенсоры → Коннектор**. Используйте коннектор **Gossopka**, созданный в UserGate SIEM по умолчанию; необходимо указать: FQDN личного кабинета, вместо указанного по умолчанию (значение по умолчанию отображает формат, в котором должно быть указано значение поля), логин/пароль и ключ API, который добавляется в поле HTTP заголовки.

- 6. Настроить шаблон отчёта.

По умолчанию создан шаблон **Форма для ГОССОПКА**, соответствующий требованиям ГосСОПКА к отчётам. Заполните поля формы; данная форма будет использоваться при формировании отчёта.

Наименование	Описание
Организация	Название организации.
Категория	Категория уведомления: - Уведомление о компьютерном инциденте. - Уведомление о компьютерной атаке. - Уведомление о наличии уязвимости.
Тип события ИБ	Тип события информационной безопасности: - Вовлечение контролируемого ресурса в инфраструктуру ВПО. - Замедление работы ресурса в результате DDoS-атаки. - Заражение ВПО. - Захват сетевого трафика. - Использование контролируемого ресурса для фишинга. - Компрометация учётной записи. - Несанкционированное изменение информации. - Несанкционированное разглашение информации. - Публикация на ресурсе запрещённой законодательством РФ информации. - Рассылка спам-сообщений с контролируемого ресурса. - Успешная эксплуатация уязвимости.
Статус реагирования на инцидент	Статус реагирования на инцидент: - Меры приняты. - Проводятся мероприятия по реагированию. - Возобновлены мероприятия по реагированию.
Необходимость привлечения сил ГосСОПКА	Отметьте чекбокс в случае необходимости привлечения сил ГосСОПКА.
Краткое описание события ИБ	Описание события информационной безопасности.
Сведения о средстве или способе выявления инцидента	Информация о способе и устройстве/ПО, посредством которого был выявлен инцидент.
Дата и время выявления инцидента	Дата и время выявления инцидента заполняются автоматически.
Дата и время завершения инцидента	Дата и время завершения инцидента заполняются автоматически.
Ограничительный маркер TLP	Маркировка конфиденциальной информации (Traffic Light Protocol). Возможны следующие маркировки: RED: информация является крайне конфиденциальной. AMBER: информацией можно поделиться в рамках своей организации, при условии, что этой информацией нужно поделиться. GREEN: информация может быть широко распространена в пределах определённого сообщества. WHITE: информация в свободном распространении, но не нарушает авторские права.
Влияние на доступность	Потенциальное влияние на доступность информационных ресурсов: - Отсутствует. - Низкое. - Высокое.

Наименование	Описание
Влияние на целостность	Потенциальное влияние на целостность ресурсов информационной системы: - Отсутствует. - Низкое. - Высокое.
Влияние на конфиденциальность	Потенциальное влияние на конфиденциальность (ограничение доступа к информационным ресурсам, разрешения доступа к системе только авторизованным пользователям, предотвращение раскрытия информации неуполномоченным лицам): - Отсутствует. - Низкое. - Высокое.
Краткое описание иной формы последствий компьютерного инцидента	Описание последствий инцидента, кроме тех, что были указаны ранее.
Наименование контролируемого ресурса, на котором был выявлен компьютерный инцидент	Наименование контролируемого информационного ресурса объекта КИИ, на котором выявлен компьютерный инцидент, компьютерная атака или уязвимость.
Информация о категорировании ОКИИ	Присвоенная объекту КИИ категория значимости: - Информационный ресурс не является объектом КИИ. - Объект КИИ без категории значимости (объект признан незначимым). - Объект КИИ третьей категории значимости (самая низкая). - Объект КИИ второй категории значимости. - Объект КИИ первой категории значимости (самая высокая).
Сфера функционирования субъекта	Сфера функционирования объекта КИИ (например, банковская сфера, здравоохранение и т.п.).
Наличие подключения к сети Интернет	Наличие подключения к сети Интернет: - Да. - Нет.
Страна/регион	Код в соответствии с ISO-3166-2 .
Населенный пункт или геокоординаты	Название населённого пункта или его географические координаты. Географические координаты указываются в формате: <i>широта</i> — С.Ш, <i>долгота</i> — В.Д.

7. Сформировать и отправить отчёт об инциденте информационной безопасности.

Формирование отчёта доступно во вкладке с подробностями об инциденте нажатием кнопки **Создать отчёт → GOSSOPKA report**. Для отправки отчёта необходимо указать коннектор, настроенный ранее и нажать **Послать через сеть**.

Далее нужно заполнить необходимые поля формы (большинство поле заполнено в соответствии с шаблоном **Форма для ГОССОПКА**) и нажать **ОК**. В случае успешного соединения сервер UserGate SIEM отправит отчёт на коннектор (в систему личных кабинетов ГосСОПКА).

Запись об отправке отчёта будет отображена в журнале событий UserGate SIEM.

Documentation: 
Product: SIEM
Version: 7.x

UserGate SIEM поддерживает интерфейс командной строки CLI (Command Line Interface), с помощью которого можно производить настройку устройства.

CLI полезно использовать для диагностики сетевых проблем или в случае, когда доступ к веб-консоли утерян, например некорректно указан IP-адрес интерфейса или ошибочно установлены параметры контроля доступа для зоны, запрещающие подключение к веб-интерфейсу.

Подключение к CLI можно выполнить с помощью протокола SSH по сети.

Примечание Если устройство не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin, в качестве пароля — usergate.

Для подключения к CLI выполните следующие шаги:

1. В разделе **Настройки** → **Сеть** → **Зоны** для зоны, к которой вы собираетесь подключаться для управления с помощью CLI, разрешите доступ для протокола CLI по SSH. Будет открыт порт TCP 2200.
2. Запустите у себя на компьютере SSH-терминал, например SSH для Linux или Putty для Windows. Укажите адрес устройства UserGate SIEM, в качестве порта подключения — 2200, в качестве имени пользователя — имя пользователя с правами корневого администратора (по умолчанию Admin с паролем usergate). Для Linux команда на подключение должна выглядеть так:

```
ssh Admin@<IP-SIEM> -p 2200
```

После успешной аутентификации в CLI появится строка ожидания ввода команды (режим диагностики). Для просмотра текущих возможных значений или автодополнения команды используйте клавишу «Tab». В режиме диагностики доступны следующие команды:

- **configure** — переход в режим конфигурации.
- **date** — просмотр текущих даты и времени на устройстве.
- **dig** — проверка записи DNS-домена.
- **exit** — выход из командной строки.
- **netcheck** — проверка доступности стороннего HTTP/HTTPS-сервера.
- **show** — просмотр сетевых настроек, версии ПО, статистики активных сессий.
- **clear** — очистка данных статистики по активным сессиям и сетевым интерфейсам.
- **ping** — выполнение ping определённого хоста.
- **reboot** — перезагрузка устройства.
- **shutdown** — выключение устройства.
- **traceroute** — трассировка соединения до определённого хоста.

Эти команды доступны также в режиме конфигурации. Подробнее — в разделе [«Команды execute»](#).

Для отмены ввода текущей команды используйте сочетание клавиш «Ctrl + C»; для просмотра истории команд — клавиши клавиатуры «↑» и «↓».

Все команды интерфейса командной строки имеют следующую структуру:

<action> <level> <filter> <configuration_info>

Где:

<action> — действие, которое необходимо выполнить.

<level> — уровень конфигурации; уровни соответствуют разделам веб-интерфейса NGFW.

<filter> — идентификатор объекта, к которому происходит обращение.

<configuration_info> — значение параметров, которые необходимо применить к объекту <filter>.

Команды, доступные до первичной инициализации узла (описание)

Documentation: 
Product: SIEM
Version: 7.x

Если устройство не прошло первоначальную инициализацию, то в CLI доступны команды диагностики и мониторинга, а в режиме конфигурации — только команды настройки сети, т.е. настройка зон, интерфейсов, шлюзов и виртуальных маршрутизаторов, а также включение/отключение удалённого доступа к серверу `radmin-emergency`.

Первоначальная инициализация (описание)

Documentation: 
Product: SIEM
Version: 7.x

Первоначальная инициализация устройства с использованием интерфейса командной строки.

Для настройки устройства используется команда:

Admin@nodename# execute install master

Необходимо указать параметры:

Параметр	Описание
login	Задать логин администратора.
password	Задать пароль учётной записи администратора. Указание пароля также доступно при нажатии Enter после указания логина администратора; необходимо дважды ввести пароль учётной записи.

Documentation: 
Product: SIEM
Version: 7.x

Для перехода в режим конфигурации используется команда:

Admin@nodename> configure

После перехода в режим конфигурации командная строка будет выглядеть следующим образом:

Admin@nodename#

Для просмотра подсказки о текущих возможных значениях или для автодополнения команд необходимо нажать клавишу **Tab**. В подсказке могут использоваться следующие вспомогательные символы:

- * — обязательное поле в командах create и ряде других команд;
- + — необязательное/вариативное поле;
- > — вложенное поле, после его введения предыдущий список полей становится недоступным, появляется новый список полей, которые можно ввести.

Например:

```
Admin/system@nodename# set network zone Trusted
* name          Name
+ antispoof-enable  Enable/Disable IP spoofing protection
+ antispoof-negate  Enable/Disable Negate ip-spoof addresses
+ description      Description
+ enabled-services  Services list to enable
+ geoip            IP spoofing protection by geo IP code
+ ip-list           IP spoofing protection by IP list
> dos-protection-icmp  Configure DoS protection per IP for ICMP packets
> dos-protection-syn   Configure DoS protection per IP for SYN packets
> dos-protection-udp   Configure DoS protection per IP for UDP packets
> service-addresses   Access control service addresses
```

Общая структура команд в режиме конфигурации

Команды интерфейса командной строки имеют следующую структуру:

<action> <level> <filter> <configuration_info>

где:

- <action> — действие, которое необходимо выполнить.
- <level> — уровень конфигурации; уровни соответствуют разделам веб-консоли UserGate SIEM.
- <filter> — идентификатор объекта, к которому происходит обращение.
- <configuration_info> — значение параметров, которые необходимо применить к объекту <filter>.

Наименование	Описание
<action>	В режиме конфигурации доступны следующие действия: execute — выполнение команд, которые не относятся к конфигурации UserGate (ping, date, traceroute и т.п.) Команда доступна независимо от уровня конфигурации (<level>). set — редактирование всех объектов, а также включение различных параметров, например, admin. end — переход на один уровень выше. show — отображение текущих значений. Можно использовать на любом уровне конфигурации — будет отображено всё, что находится глубже текущего уровня. edit — переход на какой-либо уровень конфигурации. Уровень конфигурации будет отображён под командной строкой. top — возврат на самый верхний уровень конфигурации. exit — выход из режима конфигурации. export — экспорт конфигурации. import — импорт конфигурации. create — создание новых объектов. delete — удаление объекта или параметра из списка параметров. Например, для просмотра информации о всех интерфейсах необходимо выполнить команду: <pre>Admin@nodename# show network interface</pre> С использованием следующей команды производится переход на уровень network interface. Текущий уровень будет отображён под командной строкой: <pre>Admin@nodename# edit network interface Admin@nodename# Level: network interface</pre> После перехода на уровень network interface для отображения всех интерфейсов используется команда show без указания уровня: <pre>Admin@nodename# show</pre> adapter: <pre>port0 type : adapter interface-name : port0 node-name : node zone : Management enabled : on ip-addresses : 192.168.56.3/24 iface-mode : dhcp Level: network interface</pre> Для возвращения с уровня network interface обратно на общий уровень режима конфигурации необходимо набрать команду end: <pre>Admin@nodename# end Level: network interface Admin@nodename# end Level: network Admin@nodename#</pre>

Наименование	Описание
<level>	Уровни в командной строке повторяют веб-интерфейс системной консоли UserGate SIEM: • network — соответствует разделу веб-интерфейса Сеть. • settings — соответствует разделу веб-интерфейса UserGate. • users — соответствует разделу веб-интерфейса Пользователи и устройства. • libraries — соответствует разделу веб-интерфейса Библиотеки. • monitoring — соответствует разделу веб-интерфейса Диагностика и мониторинг. • sensors — соответствует разделу веб-интерфейса Сенсоры. • analytics — соответствует разделу веб-интерфейса Аналитика. • incident — соответствует разделу веб-интерфейса Инциденты.
<filter>	Идентификатор объекта, к которому происходит обращение. Идентификация происходит по имени объекта. Если имеются объекты с одинаковыми именами или удобнее идентифицировать объект по другому параметру, то используются круглые скобки, в которых необходимо указать <configuration_info>. В результате будет найден объект, для которого совпали все поля, указанные в круглых скобках.
<configuration_info>	Набор пар: параметр-аргумент. Параметр — имя поля, для которого нужно установить аргумент. Аргумент может быть одиночным или множественным. Одиночный аргумент — значение, соответствующее параметру. Если строка содержит пробелы, то необходимо использовать кавычки. Например, необходимо создать профиль аутентификации с именем New profile: Admin@nodename# create users auth-profile name "New profile" Множественные аргументы используются для установки множества значений какого-либо параметра; записываются в квадратных скобках и разделяются пробелами. Например, необходимо создать список IP-адресов в библиотеке элементов и добавить в него два IP-адреса 10.10.0.1 и 10.10.0.2: Admin@nodename# create libraries ip-list name testlist ips [10.10.0.1 10.10.0.2] Важно! Квадратные скобки должны быть отделены пробелами с обеих сторон.

Команды execute

Команды имеет следующую структуру:

Admin@nodename# execute <command-name>

Доступны следующие команды:

Параметр	Описание
traceroute	Трассировка соединения до определённого хоста. Доступны параметры: • hostname <ip-or-domain> — IP-адрес или имя домена, для которого производится трассировка. • interface <iface-name> — интерфейс, с которого будут отправляться пакеты. • not-map-ip — не искать hostname для IP-адреса при отображении. • use-icmp-echo — использовать ICMP echo. • port — указать порт вместо порта по умолчанию (1 — 65535). • min-interval — минимальный интервал между пакетами. Admin@nodename# execute traceroute hostname <hostname>
termination	Закрытие сессий администраторов. Подробнее читайте в разделе Управление сессиями администраторов .
ping	Выполнение ping определенного хоста. Можно задать следующие параметры: • hostname — IP-адрес или доменное имя хоста. • count — количество отправляемых echo-запросов. Если параметр не задан, то отправка пакетов будет происходить, пока соединение не будет прервано пользователем (чтобы прервать отправку: Ctrl+C). • numeric — не резолвить имена. • timestamp — отображение временных меток. • interval — интервал времени, через который будет производиться отправка пакетов; указывается в секундах. • ttl — время жизни пакета. • interface — адрес выбранного интерфейса будет использоваться в качестве адреса источника для выполнения ping. • mtu — размер mtu отправляемых пакетов. • virtual-router — имя виртуального маршрутизатора. Admin@nodename# execute ping hostname <hostname> count <number>
reboot	Перезагрузка устройства.
date	Просмотр текущих даты и времени на сервере.
shutdown	Выключение устройства.
netcheck	Проверка доступности стороннего HTTP/HTTPS-сервера. Могут быть использованы следующие параметры: • address — доменное имя хоста для проверки доступности по TCP или URL для HTTP. • dns-ip — IP-адрес сервера DNS. • dns-tcp — использование TCP вместо UDP для DNS-запроса. • check-cert — проверка SSL-сертификата • type — проверка доступности по: ◦ http. ◦ tcp (если порт не указан, то используется порт 80). • data — запрос содержимого сайта. По умолчанию запрашиваются только заголовки. • timeout — максимальный таймаут ожидания ответа от веб-сервера. • user-agent — параметр для указания типа браузера (useragent). На некоторых сайтах может быть разрешен доступ только с определенных браузеров. Значение параметра указывается в двойных кавычках. Admin@nodename# execute netcheck type tcp address <host-domain-name> data on Admin@nodename# execute netcheck address <host-domain-name>

Параметр	Описание
dig	Проверка записи DNS домена. • hostname — доменное имя хоста или IP-адрес для реверсивного поиска. • reverse-lookup — получение хоста по IP-адресу. • dns — указание IP-адреса DNS-сервера. • tcp — использование протокола TCP вместо UDP. Admin@nodename# execute dig hostname <host-domain-name> Admin@nodename# execute dig hostname <IP-address> reverse-lookup on
license	Команда регистрации продукта имеет следующую структуру: Admin@nodename# execute license activate <pin-code> Укажите код активации продукта вместо <pin-code>.

Часть представленных выше команд также доступны в режиме диагностики и мониторинга. Для их выполнения используется команда:

Admin@nodename> <command-name>

Documentation: 
Version: 7.x
Product: SIEM

Общие настройки устройства

Общие настройки устройства задаются на уровне **settings general**. Структура команды для настройки одного из разделов (<settings-module>):

Admin@nodename# set settings general <settings-module>

Доступна настройка следующих разделов:

Параметр	Описание
admin-console	Настройки интерфейса (уровень settings general admin-console): timezone: часовой пояс, соответствующий вашему местоположению. Часовой пояс используется в расписаниях, применяемых в правилах, а также для корректного отображения времени и даты в отчетах, журналах и т.п. language: язык интерфейса: ru — русский. en — английский. api-session-lifetime: время ожидания сеанса администратора в секундах.
server-time	Настройка параметров установки точного времени (уровень settings general server-time): ntp-enabled: включение/отключение использования NTP-серверов: on. off. primary-ntp-server: указание основного ntp-сервера. second-ntp-server: указание запасного ntp-сервера. time: установка времени на сервере; время указывается в часовом поясе UTC в формате yyyy-mm-ddThh:mm:ss (например, 2022-02-15T12:00:00)
change-tracker	Настройка учёта изменений (уровень settings general change-tracker): enabled: включение/отключение учёта изменений. on. off. event-tracker-types: типы изменений задаются администратором. Для удаления типа изменения используется команда: Admin/system@nodename# delete settings general change-tracker event-tracker-types [type1 ...]
management-center	Настройка агента UserGate Management Center (уровень settings general management-center): enabled: включение/отключение агента UserGate Management Center. on. off. mc-address: адрес сервера UserGate Management Center. device-code: уникальный код устройства для подключения устройства к UserGate Management Center.
updates-schedule	Настройка расписания скачивания обновлений программного обеспечения и библиотек (уровень settings general updates-schedule). Для расписания обновления программного обеспечения UserGate: Admin/system@nodename# set settings general updates-schedule software schedule <schedule/disabled> Расписание скачивания обновлений библиотек может быть единым: Admin/system@nodename# set settings general updates-schedule all-libraries schedule <schedule/disabled> или может быть настроено отдельно для каждого элемента: Admin/system@nodename# set settings general updates-schedule libraries [lib-module ...] schedule <schedule/disabled> Время задаётся в cronlab-формате: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: - Звездочка (*) — обозначает весь диапазон (от первого до последнего). - Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. - Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". - Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "'/2" в поле "часы" будет означать "каждые два часа". Команда для просмотра расписания обновлений: Admin/system@nodename# show settings general updates-schedule

Настройка управления устройством

Настройка Radmin-emergency

Для активации удаленного помощника при возникновении проблемы с программным ядром устройства администратор может зайти в CLI под учетной записью корневого администратора, которая была создана при инициализации узла. Обычно это учетная запись Admin, хотя может быть и другой. Для входа необходимо указать имя в виде Admin@emergency, в качестве пароля — пароль корневого администратора. Команда включения/отключения удалённого доступа к серверу для технической поддержки в таких случаях:

Adminm@emergency@SIEM# set radmin-emergency enabled <on | off>

Параметр	Описание
interface	Название интерфейса.
ip-addr	IP-адрес и маска интерфейса.
gateway-address	IP-адрес шлюза.

Настройка операций с сервером

Следующая команда позволяет определить канал обновлений:

Admin@nodename# set settings device-mgmt updates-channel <stable | beta>

Для просмотра наличия обновлений и выбранного канал обновления используется команда:

Admin@nodename# show settings device-mgmt updates-channel

Для настройки активации лицензии и обновления ПО устройства через внешний прокси-сервер используется команда:

Admin@nodename# set settings device-mgmt licensing-upstream-proxy <parameters>

В качестве дополнительных параметров указываются:

Параметр	Описание
enabled	Включение/выключение режима активации лицензии и обновления ПО через внешний прокси-сервер: - on — включено. - off — выключено.
ip	IP-адрес внешнего прокси-сервера.
port	Порт внешнего прокси-сервера.
auth	Аутентификация на внешнем прокси-сервере: - on — включена. - off — выключена.
name	Логин на внешнем прокси-сервере.
password	Пароль на внешнем прокси-сервере.

Для просмотра созданных настроек активации лицензии и обновления ПО устройства через внешний прокси-сервер используется команда:

Admin@nodename# show settings device-mgmt licensing-upstream-proxy

Управление резервным копированием

Создание резервной копии устройства осуществляется на уровне **settings device-mgmt**. Для создания правила резервного копирования и выгрузки файлов на внешние серверы (FTP/SSH) используется следующая команда:

Admin@nodename# create settings device-mgmt settings-backup <parameters>

Для настройки доступны следующие параметры:

Параметр	Описание
enabled	Включение/отключение правила создания резервной копии устройства.
name	Название правила резервного копирования.
description	Описание правила резервного копирования.
type	Выбор удалённого сервера для экспорта файлов: - ssh. - ftp.
address	IP-адрес удалённого сервера.
port	Порт сервера.
login	Учётная запись на удалённом сервере.
password	Пароль учётной записи.
path	Путь на сервере, куда будут выгружены файлы.
schedule	Расписание экспорта файлов резервных копий. Время задаётся в Crontab-формате: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: - Звездочка (*) — обозначает весь диапазон (от первого до последнего). - Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. - Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". - Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение ""/2" в поле "часы" будет означать "каждые два часа".

Редактирование существующего правила резервного копирования устройства производится с использованием следующей команды:

Admin@nodename# set settings device-mgmt settings-backup <rule-name>

Список параметров, доступных для изменения аналогичен списку параметров, доступных при создании правила.

Команда для удаления правила резервного копирования:

Admin@nodename# delete settings device-mgmt settings-backup <rule-name>

Команда для отображения правила резервного копирования:

Admin@nodename# show settings device-mgmt settings-backup <rule-name>

Также, для команд редактирования, удаления или отображения правил в качестве <filter> возможно использование не только названия правила, но и заданные в существующем правиле параметры (удобно, например, при наличии нескольких правил с одинаковым названием). Параметры, с использованием которых можно произвести идентификацию правила экспорта, аналогичны параметрам команды **set**.

Экспорт настроек

Создание и настройка правил экспорта настроек происходит на уровне **settings device-mgmt settings-export**.

Для создания правила экспорта настроек:

Admin@nodename# create settings device-mgmt settings-export (<parameters>)

Доступны параметры:

Параметр	Описание
enabled	Включение/отключение правила экспорта настроек сервера UserGate.

Параметр	Описание
name	Название правила экспорта.
description	Описание правила экспорта.
type	Выбор удалённого сервера для экспорта настроек: - ssh. - ftp.
address	IP-адрес удалённого сервера.
port	Порт сервера.
login	Учётная запись на удалённом сервере.
password	Пароль учётной записи.
path	Путь на сервере, куда будут выгружены настройки.
schedule	Расписание экспорта настроек. Время задаётся в Crontab-формате: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: - Звездочка (*) — обозначает весь диапазон (от первого до последнего). - Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. - Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". - Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

Обновление существующего правила экспорта настроек устройства производится с использованием следующей команды:

```
Admin@nodename# set settings device-mgmt settings-export <rule-name>
```

Список параметров, доступных для изменения аналогичен списку параметров, доступных при создании правила.

Команда для удаления правила экспорта настроек:

```
Admin@nodename# delete settings device-mgmt settings-export <rule-name>
```

Команда для отображения правила экспорта настроек:

```
Admin@nodename# show settings device-mgmt settings-export <rule-name>
```

Также, для команд обновления, удаления или отображения правил в качестве <filter> возможно использование не только названия правила, но и заданные в существующем правиле параметры (удобно, например, при наличии нескольких правил с одинаковым названием). Параметры, с использованием которых можно произвести идентификацию правила экспорта, аналогичны параметрам команды **set**.

Version: 7.x
Product: SIEM
Documentation: 

Настройка данного раздела производится на уровне **settings administrators**. В разделе описаны настройка параметров защиты учётных записей, настройка администраторов и их профилей.

Общие настройки доступа

Данный раздел позволяет настроить дополнительные параметры защиты учётных записей администраторов. Настройка производится на уровне **settings administrators general**.

Для изменения параметров используется следующая команда:

Admin@nodename# set settings administrators general

Параметры, доступные для редактирования:

Параметр	Описание
password	Изменить пароля текущего администратора.
unblock	Разблокировать администратора.
strong-password	Использовать сложный пароль: - on. - off.
num-auth-attempts	Установить максимальное количество неверных попыток аутентификации.
block-time	Указать время блокировки учётной записи в случае достижения администратором максимального количества попыток аутентификации; указывается в секундах (максимальное значение: 3600 секунд).
min-length	Определить минимальную длину пароля (максимальное значение: 100 символов).
min-uppercase	Определить минимальное количество символов в верхнем регистре (максимальное значение: 100 символов).
min-lowercase	Определить минимальное количество символов в нижнем регистре (максимальное значение: 100 символов).
min-digits	Определить минимальное количество цифр (максимальное значение: 100 символов).
spec-characters	Определить минимальное количество специальных символов (максимальное значение: 100 символов).
char-repetition	Указать максимальную длину блока из одного и того же символа (максимальное значение: 100 символов).

Пример редактирования параметров учетных записей:

Admin@nodename# set settings administrators general block-time 400

Для просмотра текущих параметров защиты учётных записей администраторов используется следующая команда:

Admin@nodename# show settings administrators general

strong-password : off
block-time : 400
min-length : 7
min-uppercase : 1
min-lowercase : 1
min-digits : 1
spec-characters : 1
char-repetition : 2
num-auth-attempts : 10

Настройка учётных записей администраторов

Настройка учётных записей администраторов производится на уровне **settings administrators administrators**.

Для создания учётной записи администратора используется следующая команда:

Admin@nodename# create settings administrators administrators

Далее необходимо указать тип учётной записи администратора (локальный, пользователь LDAP, группа LDAP, с профилем аутентификации) и установить соответствующие параметры:

Параметр	Описание
local	Добавить локального администратора: enabled: включение/отключение учётной записи администратора: - on. - off. login: логин администратора. display-name: отображаемое имя администратора. description: описание учётной записи администратора. admin-profile: профиль администратора. Создание профилей администраторов рассмотрено далее. password: пароль администратора.
ldap-user	Добавить пользователя из существующего домена (необходим корректно настроенный LDAP-коннектор; подробнее читайте в разделе Настройка LDAP-коннектора): enabled: включение/отключение учётной записи администратора: - on. - off. login: логин администратора в формате domainuser. Структура команды при указании данного параметра: display-name: отображаемое имя администратора. connector: название сконфигурированного ранее LDAP-коннектора. description: описание учётной записи администратора. admin-profile: профиль администратора. Создание профилей администраторов рассмотрено далее. Admin@nodename# create settings administrators administrators ldap-user admin-profile "test profile 1" connector "LDAP connector" description "Admin as domain user" login testd.localuser1 enabled on

Параметр	Описание
ldap-group	Добавить группу пользователей из существующего домена (необходим корректно настроенный LDAP-коннектор; подробнее читайте в разделе Настройка LDAP-коннектора): enabled: включение/отключение учётной записи администратора: on. off. login: логин администратора display-name: отображаемое имя администратора. connector: название используемого LDAP-коннектора. description: описание учётной записи администратора. admin-profile: профиль администратора. Создание профилей администраторов рассмотрено далее. Admin@nodename# create settings administrators administrators ldap-group admin-profile "test profile 1" connector "LDAP connector" description "Domain admin group" login testd.local\users enabled on
admin-auth-profile	Добавить администратора с профилем аутентификации (необходимы корректно настроенные серверы аутентификации; подробнее читайте в разделе Настройка серверов аутентификации): enabled: включение/отключение учётной записи администратора: on. off. login: логин администратора. display-name: отображаемое имя администратора. description: описание учётной записи администратора. admin-profile: профиль администратора. Создание профилей администраторов рассмотрено далее. auth-profile: выбор профиля аутентификации из созданных ранее; подробнее о профилях аутентификации читайте в разделе Настройка профилей аутентификации.

Для редактирования параметров профиля используется команда:

```
Admin@nodename# set settings administrators administrators <admin-type> <admin-login>
```

Параметры для редактирования аналогичны параметрам создания профиля администратора.

Для отображения информации о всех учётных записях администраторов:

```
Admin@nodename# show settings administrators administrators
```

Для отображения информации об определённой учётной записи администратора:

```
Admin@nodename# show settings administrators administrators <admin-type> <admin-login>
```

Пример выполнения команды:

```
Admin@nodename# show settings administrators administrators ldap-user testd.local\user1
```

```
login      : testd.local\user1
enabled    : on
type       : ldap_user
locked     : off
admin-profile : test profile 1
```

Для удаления учётной записи используется команда:

```
Admin@nodename# delete settings administrators administrators <admin-type> <admin-login>
```

Пример команды:

```
Admin@nodename# delete settings administrators administrators ldap-user testd.local\user1
```

Настройка прав доступа профилей администраторов

Настройка прав доступа профилей администраторов производится на уровне **settings administrators profiles**.

Для создания профиля администратора используется следующая команда:

```
Admin@nodename# create settings administrators profiles
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля администратора.
description	Описание профиля администратора.
roles	Выбор роли для профиля администратора. Подробнее о ролях читайте в разделе Роли и ролевые разрешения пользователей .
permissions	Права доступа: no-access: нет доступа. read: только чтение. write: чтение и запись.

Для редактирования профиля используется команда:

```
Admin@nodename# set settings administrators profiles <profile-name> <parameter>
```

Параметры для редактирования аналогичны параметрам создания профиля администратора.

Для просмотра информации о всех профилях администраторов:

```
Admin@nodename# show settings administrators profiles
```

Для отображения информации об определённом профиле:

```
Admin@nodename# show settings administrators profiles <profile-name>
```

Чтобы удалить профиль администратора:

```
Admin@nodename# delete settings administrators profiles <profile-name>
```

Управление сессиями администраторов

С использованием следующих команд возможен просмотр активных сессий администраторов, прошедших аутентификацию в веб-консоли или CLI, и закрытие сессий (уровень: **settings administrators admin-sessions**).

Просмотр сессий администраторов устройства (возможен просмотр сессии отдельного администратора: необходимо из предложенного списка выбрать IP-адрес, с которого была произведена аутентификация):

```
Admin@nodename# show settings administrators admin-sessions
```

Для отображения сессий доступно использование фильтра:

- ip**: IP-адрес, с которого вошел администратор.

- **source:** где была произведена аутентификация: CLI (**cli**), веб-консоль (**web**) или подключение по SSH (**ssh**).
- **admin-login:** имя администратора.

Admin@nodename# show settings administrators admin-sessions (node <node-name> ip <session-ip> source <cli | web | ssh> admin-login <administrator-login>)

Команда для закрытия сессии администратора; необходимо из предложенного списка выбрать IP-адрес, с которого была произведена аутентификация:

Admin@nodename# execute termination admin-sessions <IP-address/connection type>

Пример выполнения команд:

Admin@nodename# show settings administrators admin-sessions

```
admin-login      : Admin
source           : ssh
session_start_date : 2023-08-10T11:33:47Z
ip               : 127.0.0.1
node             : <node-name>
```

```
admin-login      : Admin
source           : web
session_start_date : 2023-08-10T11:33:10Z
ip               : 10.0.2.2
node             : <node-name>
```

Admin@nodename# execute termination admin-sessions 10.0.2.2/web

Admin@nodename# show settings administrators admin-sessions

```
admin-login      : Admin
source           : ssh
session_start_date : 2023-08-10T11:33:47Z
ip               : 127.0.0.1
node             : <node-name>
```

При закрытии сессии администраторов возможно использование фильтра (<filter>). Параметры фильтрации аналогичны параметрам команды **show**.

Admin@nodename# execute termination admin-sessions (node <node-name> ip <session-ip> source <cli | web | ssh> admin-login <administrator-login>)

Version: 7.x
Product: SIEM
Documentation: 

Раздел **Сертификаты** находится на уровне **settings certificates**.

Для импорта сертификатов предназначена команда:

```
Admin@nodename# import settings certificates
```

Далее необходимо указать параметры:

Параметр	Описание
name	Название сертификата, под которым он будет отображен в списке сертификатов.
description	Описание сертификата.
certificate-data	Данные сертификата в формате PEM.
private-key	Приватный ключ сертификата в формате PEM.
passphrase	Пароль для приватного ключа, если таковой требуется.
certificate-chain	Цепочка сертификатов вышестоящих центров сертификации, которые участвовали в создании сертификата, в формате PEM.

Для экспорта доступны сертификаты, вся цепочка сертификатов:

```
Admin@nodename# export settings certificates <certificate-name>
Admin@nodename# export settings certificates <certificate-name> with-chain on
```

С использованием командной строки возможно создание сертификата и CSR:

```
Admin@nodename# create settings certificates type <certificate | csr>
```

Далее необходимо указание следующих параметров:

Параметр	Описание
name	Название сертификата.
description	Описание сертификата.
country	Страна, в которой выписывается сертификат.
state	Область/штат, в котором выписывается сертификат.
locality	Город, в котором выписывается сертификат.
organization	Название организации, для которой выписывается сертификат.
common-name	Имя сертификата. Рекомендуется использовать только символы латинского алфавита для совместимости с большинством браузеров.
email	Email компании.

Команда для управления сертификатом:

```
Admin@nodename# set settings certificates <certificate-name>
```

Доступны параметры:

Параметр	Описание
name	Название сертификата.
description	Описание сертификата.
role	Тип сертификата: web-cert-chain: цепочка сертификатов веб-консоли. web-ssl: сертификат, использующийся для создания безопасного HTTPS-подключения администратора к веб-консоли UserGate. none.
certificate-chain	Цепочка сертификатов в формате PEM.

Для удаления сертификата:

```
Admin@nodename# delete settings certificates <certificate-name>
```

Команды для просмотра информации об определённом сертификате или о всех сертификатах:

```
Admin@nodename# show settings certificates
Admin@nodename# show settings certificates <certificate-name>
```

Version: 7.x
Product: SIEM
Documentation: 

Раздел Серверы аутентификации позволяет произвести настройку LDAP-коннектора, серверов RADIUS, TACACS+. Настройка серверов аутентификации производится на уровне **users auth-server** и будет рассмотрена далее в соответствующих разделах.

Настройка LDAP-коннектора

Настройка LDAP-коннектора производится на уровне **users auth-server ldap**.

Для создания LDAP-коннектора используется команда:

Admin@nodename# create users auth-server ldap <parameter>

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя LDAP-коннектора.
enabled	Включение/отключение сервера аутентификации.
description	Описание LDAP-коннектора.
ssl	Определяет: - on — использование SSL-соединения для подключения к LDAP-серверу. - off — подключение к LDAP-серверу без использования SSL-соединения.
address	IP-адрес контроллера или название домена LDAP.
bind-dn	Имя пользователя, которое будет использоваться для подключения к серверу; указывается в формате DOMAIN\username или username @domain. Пользователь должен быть заведён в домене.
password	Пароль пользователя для подключения к домену.
domains	Список доменов, которые обслуживаются указанным контроллером домена.
search-roots	Список путей в сервере LDAP, начиная с которых система будет осуществлять поиск пользователей и групп. Необходимо указывать полное имя, например, ou=Office,dc=example,dc=com. Если пути поиска не указаны, то поиск производится по всему каталогу, начиная от корня.

Для редактирования информации о существующем LDAP-коннекторе используется команда:

Admin@nodename# set users auth-server ldap <ldap-server-name> <parameter>

Параметры, доступные для обновления, аналогичны параметрам создания LDAP-коннектора.

Команда для отображения информации о LDAP-коннекторе:

Admin@nodename# show users auth-server ldap <ldap-server-name>

Примеры команд создания и редактирования LDAP-коннектора:

Admin@nodename# create users auth-server ldap name "New LDAP connector" ssl on address 10.10.0.10 bind-dn ug@testd.local password 12345 domains [testd.local] search-roots [dc=testd,dc=local] enabled on
Admin@nodename# show users auth-server ldap "New LDAP connector"

```
name      : New LDAP connector
enabled   : on
ssl       : on
address   : 10.10.0.10
bind-dn   : ug@testd.local
domains   : testd.local
search-roots : dc=testd,dc=local
keytab_exists : off
Admin@nodename# set users auth-server ldap "New LDAP connector" description "New LDAP connector description"
Admin@nodename# show users auth-server ldap "New LDAP connector"
```

```
name      : New LDAP connector
description : New LDAP connector description
enabled   : on
ssl       : on
address   : 10.10.0.10
bind-dn   : ug@testd.local
domains   : testd.local
search-roots : dc=testd,dc=local
keytab_exists : off
```

Для удаления LDAP-коннектора используется команда:

Admin@nodename# delete users auth-server ldap <ldap-server-name> <parameter>

Также возможно удаления отдельных параметров LDAP-коннектора. Для удаления доступны следующие параметры:

- domains.
- search-roots.

Настройка RADIUS-сервера

Настройка RADIUS-сервера производится на уровне **users auth-server radius**.

Для создания сервера аутентификации RADIUS используется команда со следующей структурой:

Admin@nodename# create users auth-server radius <parameter>

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя RADIUS-сервера.
enabled	Включение/отключение сервера аутентификации.
description	Описание сервера аутентификации.
secret	Общий ключ, используемый протоколом RADIUS для аутентификации.
addresses	IP-адрес и UDP-порт, на котором сервер RADIUS слушает запросы (по умолчанию порт 1812); указывается в формате <ip:port>.

Команда для обновления информации о сервере RADIUS:

```
Admin@nodename# set users auth-server radius <radius-server-name> <parameter>
```

Параметры, которые могут быть обновлены, соответствуют параметрам, указание которых возможно при создании сервера аутентификации.

Команда для отображения информации о RADIUS-сервере:

```
Admin@nodename# show users auth-server radius <radius-server-name>
```

Примеры команд создания и редактирования RADIUS-сервера:

```
Admin@nodename# create users auth-server radius name "New RADIUS server" addresses [ 10.10.0.9:1812 ] secret 12345 enabled on
Admin@nodename# show users auth-server radius "New RADIUS server"
```

```
name      : New RADIUS server
enabled   : on
addresses :
  host    : 10.10.0.9
  port    : 1812
Admin@nodename# set users auth-server radius "New RADIUS server" description "New RADIUS server description"
Admin@nodename# show users auth-server radius "New RADIUS server"
```

```
name      : New RADIUS server
description : New RADIUS server description
enabled   : on
addresses :
  host    : 10.10.0.9
  port    : 1812
```

Для удаления сервера:

```
Admin@nodename# delete users auth-server radius <radius-server-name> <parameter>
```

Также возможно удаления отдельных параметров RADIUS-сервера. Для удаления доступны следующие параметры:

- **addresses.**

Настройка сервера TACACS+

Настройка сервера TACACS+ производится на уровне **users auth-server tacacs**.

Для создания сервера аутентификации TACACS+ используется команда со следующей структурой:

```
Admin@nodename# create users auth-server tacacs <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя сервера TACACS+.
enabled	Включение/отключение сервера.
description	Описание сервера аутентификации.
secret	Общий ключ, используемый протоколом TACACS+ для аутентификации.
address	IP-адрес сервера TACACS+.
port	UDP-порт, на котором сервер TACACS+ слушает запросы на аутентификацию. По умолчанию это порт UDP 1812.
single-connection	Использовать одно TCP-соединение для работы с сервером TACACS+.
timeout	Время ожидания сервера TACACS+ для получения аутентификации. По умолчанию 4 секунды.

Команда для редактирования информации о сервере TACACS+:

```
Admin@nodename# set users auth-server tacacs <tacacs-server-name> <parameter>
```

Параметры, которые могут быть обновлены, соответствуют параметрам, указание которых возможно при создании сервера аутентификации.

Команда для отображения информации о сервере TACACS+:

```
Admin@nodename# show users auth-server tacacs <tacacs-server-name>
```

Примеры команд для создания и редактирования сервера TACACS+:

```
Admin@nodename# create users auth-server tacacs address 10.10.0.11 name "New TACACS+ server" port 1812 secret 12345 enabled on
Admin@nodename# show users auth-server tacacs "New TACACS+ server"
```

```
name      : New TACACS+ server
enabled   : on
address   : 10.10.0.11
port      : 1812
single-connection : off
timeout   : 4
Admin@nodename# set users auth-server tacacs "New TACACS+ server" description "New TACACS+ server description"
Admin@nodename# show users auth-server tacacs "New TACACS+ server"
```

```
name      : New TACACS+ server
description : New TACACS+ server description
enabled   : on
address   : 10.10.0.11
port      : 1812
single-connection : off
timeout   : 4
```

Для удаления сервера:

```
Admin@nodename# delete users auth-server tacacs <tacacs-server-name>
```

Настройка профилей аутентификации

Technology: Identification and Authentication
Version: 7.x
Product: SIEM
Documentation: ☒

Настройка профилей аутентификации производится на уровне **users auth-profile**.

Для создания профиля аутентификации используется следующая команда:

Admin@nodename# create users auth-profile <parameter>

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля.
description	Описание профиля.
idle-time	Время бездействия до отключения; указывается в секундах. Через указанный промежуток времени при отсутствии активности пользователь перейдёт в статус Unknown user.
expiration-time	Время жизни аутентифицированного пользователя; указывается в секундах. Через указанный промежуток времени пользователь перейдёт в статус Unknown user; необходима повторная аутентификация пользователя.
max-attempts	Число неудачных попыток аутентификации до блокировки учётной записи пользователя.
lockout-time	Время, на которое блокируется учетная запись пользователя при достижении указанного числа неудачных попыток аутентификации; указывается в секундах.
auth-methods	Метод аутентификации: • ldap: аутентификация с использованием LDAP-коннектора. • radius: аутентификация с использованием RADIUS-сервера. • tacacs: аутентификация с использованием сервера TACACS+.

Команда для редактирования настроек профилей аутентификации:

Admin@nodename# set users auth-profile <auth-profile-name> <parameter>

Для обновления доступен список параметров, аналогичный списку параметров команды **create**.

Пример создания и редактирования профиля аутентификации пользователя:

Admin@nodename# create users auth-profile name "New LDAP auth profile" auth-methods ldap ["New LDAP connector"]
Admin@nodename# show users auth-profile "New LDAP auth profile"

name : New LDAP auth profile
max-attempts : 5
idle-time : 900
expiration-time : 86400
lockout-time : 300
mfa : none
auth-methods :
 http-basic : off
 local-user-auth : off
 policy-accept : off
Admin@nodename# set users auth-profile "New LDAP auth profile" description "New LDAP auth profile description"
Admin@nodename# show users auth-profile "New LDAP auth profile"

name : New LDAP auth profile
description : New LDAP auth profile description
max-attempts : 5
idle-time : 900
expiration-time : 86400
lockout-time : 300
mfa : none
auth-methods :
 http-basic : off
 local-user-auth : off
 policy-accept : off
 ldap : New LDAP connector

Через интерфейс командной строки возможно удаления всего профиля или отдельных способов аутентификации, заданных в профиле. Для этого используются следующие команды.

Для удаления профиля аутентификации:

Admin@nodename# delete users auth-profile <auth-profile-name>

Для удаления методов аутентификации, заданных в профиле, необходимо указать метод аутентификации (доступные методы авторизации перечислены в таблице выше):

Admin@nodename# delete users auth-profile <auth-profile-name> auth-methods <auth-method>

Version: 7.x

Product: SIEM

Documentation: 

Роль пользователя — это набор ролевых разрешений. Ролевое разрешение — это возможность администратору совершать определенные действия, например, добавлять или удалять вложение из созданного инцидента, создавать правило срабатывания, создать или закрыть инцидент и т.д. Роли назначаются профилям администраторов, которые присваиваются администраторам.

Создание и настройка ролей пользователей производится на уровне **users roles**.

Для создания ролей и назначения ролевых разрешений используется команда:

```
Admin@nodename# create users roles <role-name> description <role-description> permissions [ <permissions> ]
```

Подробнее о ролях и списке имеющихся ролевых разрешений читайте в разделе [Роли и ролевые разрешения пользователей](#) Руководства администратора UserGate SIEM.

Для редактирования созданных ранее ролей и ролевых ограничений используется команда:

```
Admin@nodename# set users roles <role-name> description <role-description> permissions [ <permissions> ]
```

Для удаления ранее созданных ролей или отдельных ролевых разрешений в ранее созданных ролях используется команда:

```
Admin@nodename# delete users roles <role-name> permissions [ <permissions> ]
```

Version: 7.x
Product: SIEM
Documentation: 

Для работы с каталогами пользователей необходим корректно настроенный LDAP-коннектор, который позволяет получать информацию о пользователях и группах Active Directory или других LDAP-серверов. Пользователи и группы могут быть использованы при настройке политик, применяемых к управляемым устройствам.

Создание и настройка каталога пользователей производится на уровне **users catalogs ldap**.

Для создания каталога используется команда:

```
Admin@nodename# create users catalogs ldap <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя LDAP-коннектора.
enabled	Включение/отключение сервера аутентификации.
description	Описание LDAP-коннектора.
ssl	Определяет: • on — использование SSL-соединения для подключения к LDAP-серверу. • off — подключение к LDAP-серверу без использования SSL-соединения.
address	IP-адрес контроллера или название домена LDAP.
bind-dn	Имя пользователя, которое будет использоваться для подключения к серверу; указывается в формате DOMAIN\username или username@domain. Пользователь должен быть заведён в домене.
password	Пароль пользователя для подключения к домену.
domains	Список доменов, которые обслуживаются указанным контроллером домена.
search-roots	Список путей в сервере LDAP, начиная с которых система будет осуществлять поиск пользователей и групп. Необходимо указывать полное имя, например, ou=Office,dc=example,dc=com. Если пути поиска не указаны, то поиск производится по всему каталогу, начиная от корня.

Для редактирования информации о существующем каталоге используется команда:

```
Admin@nodename# set users catalogs ldap <ldap-server-name> <parameter>
```

Параметры, доступные для обновления, аналогичны параметрам создания каталога.

Команда для отображения информации о каталоге пользователей:

```
Admin@nodename# show users catalogs ldap <ldap-server-name>
```

Для удаления каталога используется команда:

```
Admin@nodename# delete users catalogs ldap <ldap-server-name> <parameter>
```

Также возможно удаления отдельных параметров LDAP-коннектора. Для удаления доступны следующие параметры:

- **domains**.
- **search-roots**.

Documentation: ☒
Product: SIEM
Version: 7.x

Данный раздел находится на уровне **network zone**. Команда для создания новой зоны:

Admin@nodename# create network zone

Далее необходимо указать параметры зоны:

Параметр	Описание
name	Название зоны.
description	Описание зоны.
dos-protection-syn	Защита зоны от сетевого флуда для протокола TCP (SYN-flood): • enabled: включение/отключение защиты. ◦ on. ◦ off. • aggregate: ◦ on — считаются все пакеты, входящие в интерфейсы данной зоны. ◦ off — пакеты считаются отдельно для каждого IP-адреса. • alert-threshold: порог уведомления; если количество запросов превышает данный порог, то происходит запись события в системный журнал. • drop-threshold: порог отбрасывания пакетов; если количество запросов превышает указанное значение, то UserGate отбрасывает пакеты и записывает данное событие в системный журнал. • excluded-ips: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-udp	Защита зоны от сетевого флуда для протокола UDP: • enabled: включение/отключение защиты. ◦ on. ◦ off. • aggregate: ◦ on — считаются все пакеты, входящие в интерфейсы данной зоны. ◦ off — пакеты считаются отдельно для каждого IP-адреса. • alert-threshold: порог уведомления; если количество запросов превышает данный порог, то происходит запись события в системный журнал. • drop-threshold: порог отбрасывания пакетов; если количество запросов превышает указанное значение, то UserGate отбрасывает пакеты и записывает данное событие в системный журнал. • excluded-ips: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-icmp	Защита зоны от сетевого флуда для протокола ICMP: • enabled: включение/отключение защиты. ◦ on. ◦ off. • aggregate: ◦ on — считаются все пакеты, входящие в интерфейсы данной зоны. ◦ off — пакеты считаются отдельно для каждого IP-адреса. • alert-threshold: порог уведомления; если количество запросов превышает данный порог, то происходит запись события в системный журнал. • drop-threshold: порог отбрасывания пакетов; если количество запросов превышает указанное значение, то UserGate отбрасывает пакеты и записывает данное событие в системный журнал. • excluded-ips: список IP-адресов серверов, которые необходимо исключить из защиты.
enabled-services	Параметры контроля доступа зоны: • "Any ICMP": разрешение использования команды ping адреса UserGate. • SNMP: доступ к UserGate по протоколу SNMP (UDP 161). • rpc: XML-RPC для управления - позволяет управлять продуктом по API (TCP 4040). • VRP: сервис, необходимый для объединения нескольких узлов UserGate в отказоустойчивый кластер (IP протокол 112). • "CLI over SSH": доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200. • Cluster: сервис, необходимый для объединения нескольких узлов UserGate в кластер (TCP 4369, TCP 9000-9100). • "Admin Console": доступ к веб-консоли управления (TCP 8001).
service-addresses	Указание разрешённых IP-адресов для сервисов: • service: выбор сервисов (список соответствует enabled-services). • allowed-addresses: разрешённые IP-адреса: ◦ geoip — код GeoIP. ◦ ip-list — заранее созданный в библиотеке элементов список IP-адресов.
antispoof-enable	Включение/отключение защиты от IP-спуфинга: • on. • off.
antispoof-negate	Возможные значения: • on. • off. При antispoof-negate on адреса источников, указанные в значении ip-spoofing-networks, будут являться адресами, которые не могут быть получены на интерфейсах данной зоны. В этом случае будут отброшены пакеты с указанными IP-адресами источников.
sessions-limit-enabled	Включение ограничения количества одновременных сессий с одного IP-адреса: • on. • off.

Параметр	Описание
sessions-limit-exclusions	Добавление списка IP-адресов, для которых ограничение на количество одновременных сессий не будет действовать.
sessions-limit-threshold	Максимально возможное количество одновременных сессий с одного IP-адреса.
geoip	Коды GeoIP, которые используются в защите от IP-спуфинга.
ip-list	Список IP-адресов, которые используются в защите от IP-спуфинга.

Пример создания новой зоны:

```
Admin@nodename# create network zone name Test_zone description "Test_zone description" antispoof-enable on enabled-services [ "Any ICMP" DNS ] dos-protection-icmp enabled on
```

Для редактирования параметров зоны:

```
Admin@nodename# set network zone <zone-name>
```

Пример редактирования параметров зоны:

```
Admin@nodename# set network zone Test_zone dos-protection-syn enabled on
```

Команда удаления зоны или её параметров:

```
Admin@nodename# delete network zone <zone-name>
```

Параметры, доступные для удаления:

Параметр	Описание
dos-protection-syn	Защита зоны от сетевого флуда для протокола TCP (SYN-flood): excluded-ips: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-udp	Защита зоны от сетевого флуда для протокола UDP: excluded-ips: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-icmp	Защита зоны от сетевого флуда для протокола ICMP: excluded-ips: список IP-адресов серверов, которые необходимо исключить из защиты.
enabled-services	Установленные ранее параметры контроля доступа в данной зоне
geoip	Коды GeoIP, которые используются в защите от IP-спуфинга.
ip-list	Список IP-адресов, которые используются в защите от IP-спуфинга.

Команда для просмотра настроек зоны:

```
Admin@nodename# show network zone <zone-name>
```

Documentation: 
Product: SIEM
Version: 7.x

Настройка интерфейсов производится на уровне **network interface**:

Настройка adapter

Сетевые адаптеры настраиваются на уровне **network interface adapter**.

Создать сетевой адаптер нельзя. Для обновления существующего сетевого адаптера используется команда:

Admin@nodename# set network interface adapter <adapter_name>

Далее необходимо указать параметры сетевого адаптера:

Параметр	Описание
enabled	Включение/отключение сетевого интерфейса: - on. - off.
description	Описание сетевого интерфейса.
alias	Алиас/псевдоним интерфейса.
iface-type	Тип интерфейса: - I3: интерфейс, работающий в режиме Layer 3 (можно назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах, это стандартный режим работы интерфейса). - mirror: интерфейс, работающий в режиме Mirror (может получать трафик со SPAN-порта сетевого оборудования для его анализа).
iface-mode	Режим назначения IP-адреса: - dhcp: получение динамического IP-адреса по DHCP. - manual: без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса.
zone	Зона, которой будет принадлежать интерфейс.
link-info	Настройка параметров сетевого интерфейса: - bc_forwarding: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. - proxy_arp, proxy_arp_vlan: механизм Proxy ARP. Параметр proxy_arp — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; proxy_arp_vlan — UserGate будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: Admin@nodename# create network interface <iface-type> ... link-info [key/value] где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. Важно! Удаление заданных параметров недоступно.
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся в следующем виде: [<ip_address/mask>] или [<ip_address/mask> <ip_address/mask>], если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел); маска подсети задаётся в десятичном виде. Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса.
mtu	Указание размера MTU.
mss	Указание размера MSS (доступно в версии ПО 7.3.0 и выше): 0, или от 4 до введённого значения MTU минус 40.

Команда удаления адаптера или его параметров:

Admin@nodename# delete network interface adapter <adapter-name>

Параметры, доступные для удаления:

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay server-address	IP-адрес сервера DHCP.

Команда для отображения информации о всех сетевых адаптерах:

Admin@nodename# show network interface adapter

Для отображения информации об адаптере:

Admin@nodename# show network interface adapter <adapter-name>

Настройка VLAN

Интерфейсы VLAN настраиваются на уровне **network interface vlan**.

Команда для добавления нового VLAN-интерфейса:

Admin@nodename# create network interface vlan

Далее необходимо указать параметры:

Параметр	Описание
----------	----------

Параметр	Описание
enabled	Включение/отключение VLAN-интерфейса: - on. - off.
description	Описание интерфейса.
alias	Алиас/псевдоним интерфейса.
iface-type	Тип интерфейса: - l3: Layer 3 (можно назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах, это стандартный режим работы интерфейса). - mirror: интерфейс, работающий в режиме Mirror (может получать трафик со SPAN-порта сетевого оборудования для его анализа).
iface-mode	Режим назначения IP-адреса: - dhcp: получение динамического IP-адреса по DHCP. - manual: без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса.
tag	Тег VLAN. Допускается создание до 4094 интерфейсов.
node-name	Имя узла кластера, на котором создаётся VLAN.
interface	Физический интерфейс, на котором создается VLAN.
zone	Зона, которой будет принадлежать интерфейс.
link-info	Настройка параметров сетевого интерфейса: - bc_forwarding: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. - proxy_arp, proxy_arp_vlan: механизм Proxy ARP. Параметр proxy_arp — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; proxy_arp_vlan — UserGate будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: Admin@nodename# create network interface <iface-type> ... link-info [key/value] где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. Важно! Удаление заданных параметров недоступно.
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся в следующем виде: [<ip_address/mask>] или [<ip_address/mask> <ip_address/mask>], если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел); маска подсети задаётся в десятичном виде. Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса.
mtu	Указание размера MTU.
mss	Указание размера MSS (доступно в версии ПО 7.3.0 и выше): 0, или от 4 до введённого значения MTU минус 40.
dhcp-relay	Настройка работы DHCP-релея на интерфейсе. Необходимо указать: - enabled: включение/отключения релея: - on. - off. - utm-address: IP-адрес интерфейса UserGate, на который добавляется функция релея. - server-address: адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Редактирование существующего VLAN:

```
Admin@nodename# set network interface vlan <vlan-name>
```

Параметры, доступные для обновления, аналогичны параметрам создания VLAN, кроме **tag**, **node-name**, **interface** (изменение значений этих параметров недоступно).

Команда удаления VLAN-интерфейса или его параметров:

```
Admin@nodename# delete network interface vlan <vlan-name>
```

Параметры, доступные для удаления:

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay server-address	IP-адрес сервера DHCP.

Чтобы отобразить информацию о всех интерфейсах VLAN:

```
Admin@nodename# show network interface vlan
```

или об определённом интерфейсе:

```
Admin@nodename# show network interface vlan <vlan-name>
```

Настройка bond-интерфейса

Настройка бонд-интерфейса производится на уровне **network interface bond**.

Команда для создания бонд-интерфейса:

```
Admin@nodename# create network interface bond
```

Параметры, которые необходимо указать:

Параметр	Описание
enabled	Включение/отключение интерфейса: - on. - off.
interface-name	Необходимо ввести номер, который будет отображён в имени интерфейса (например 1, тогда название созданного интерфейса будет bond1).
description	Описание интерфейса.
alias	Алиас/псевдоним интерфейса.
node-name	Узел кластера, на котором будет создан бонд-интерфейс.
zone	Зона, которой будет принадлежать бонд.
link-info	Настройка параметров сетевого интерфейса: - bc_forwarding: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. - proxy_arp, proxy_arp_vlan: механизм Proxy ARP. Параметр proxy_arp — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; proxy_arp_vlan — UserGate будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: Admin@nodename# create network interface <iface-type> ... link-info [key/value] где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. Важно! Удаление заданных параметров недоступно.
bonding	Дополнительные параметры бонд-интерфейса: - mode — режим работы бонда: - round-robin: режим Round robin (пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. Эта политика применяется для балансировки нагрузки и отказоустойчивости). - active-backup: режим Active backup (только один сетевой интерфейс из объединенных будет активным. Другой интерфейс может стать активным только в том случае, когда упадет текущий активный интерфейс. При такой политике MAC-адрес бонд-интерфейса виден снаружи только через один сетевой порт, во избежание появления проблем с коммутатором. Данная политика применяется для обеспечения отказоустойчивости). - xor: режим XOR (передача распределяется между сетевыми картами используя формулу: [(«MAC-адрес источника» XOR «MAC-адрес назначения») по модулю «число интерфейсов»]. Получается, одна и та же сетевая карта передает пакеты одним и тем же получателям. Опционально распределение передачи может быть основано и на политике «xmit_hash». Политика XOR применяется для балансировки нагрузки и обеспечения отказоустойчивости). - broadcast: режим Broadcast (передает все на все сетевые интерфейсы. Эта политика применяется для отказоустойчивости). 802.3ad: режим IEEE 802.3ad (режим работы, установленный по умолчанию, поддерживается большинством сетевых коммутаторов. Создаются агрегированные группы сетевых карт с одинаковой скоростью и дуплексом. При таком объединении передача задействует все каналы в активной агрегации согласно стандарту IEEE 802.3ad. Выбор, через какой интерфейс отправлять пакет, определяется политикой; по умолчанию используется XOR-политика, можно также использовать «xmit_hash» политику). - transmit: режим Adaptive transmit load balancing (исходящий трафик распределяется в зависимости от загруженности каждой сетевой карты (определяется скоростью загрузки). Не требует дополнительной настройки на коммутаторе. Входящий трафик приходит на текущую сетевую карту. Если она выходит из строя, то другая сетевая карта берет себе MAC-адрес вышедшей из строя карты). - load: режим Adaptive load balancing. Включает в себя предыдущую политику плюс осуществляет балансировку входящего трафика. Не требует дополнительной настройки на коммутаторе. Балансировка входящего трафика достигается путем ARP-переговоров. Драйвер перехватывает ARP-ответы, отправляемые с локальных сетевых карт наружу, и переписывает MAC-адрес источника на один из уникальных MAC-адресов сетевой карты, участвующей в объединении. Таким образом, различные пиры используют различные MAC-адреса сервера. Балансировка входящего трафика распределяется последовательно (round-robin) между интерфейсами. - mii-monitoring: периодичность MII-мониторинга в миллисекундах. Определяет, как часто будет проверяться состояние линии на наличие отказов. - down-delay: время (в миллисекундах) задержки перед отключением интерфейса, если произошел сбой соединения. Эта опция действительна только для мониторинга MII (miimon). Значение параметра должно быть кратным значениям miimon. - up-delay: время задержки в миллисекундах, перед тем как поднять канал при обнаружении его восстановления. Этот параметр возможен только при MII-мониторинге (miimon). Значение параметра должно быть кратным значениям miimon. - lacp-rate: интервал, с которым будут передаваться партнером LACPDU-пакеты в режиме 802.3ad. Возможные значения: - slow: запрос партнера на передачу LACPDU-пакетов каждые 30 секунд. - fast: запрос партнера на передачу LACPDU-пакетов каждую секунду. - failover-mac: определение способа назначения MAC-адресов на объединенные интерфейсы в режиме Active backup при переключении интерфейсов. Возможные значения: - disabled: устанавливает одинаковый MAC-адрес на всех интерфейсах во время переключения. - active: MAC-адрес на бонд-интерфейсе будет всегда таким же, как на текущем активном интерфейсе. MAC-адреса на резервных интерфейсах не изменяются. MAC-адрес на бонд-интерфейсе меняется во время обработки отказа. - follow: MAC-адрес на бонд-интерфейсе будет таким же, как на первом интерфейсе, добавленном в объединение. На втором и последующем интерфейсе этот MAC не устанавливается, пока они в резервном режиме. MAC-адрес прописывается во время обработки отказа, когда резервный интерфейс становится активным, он принимает новый MAC (тот, что на бонд-интерфейсе), а старому активному интерфейсу прописывается MAC, который был на текущем активном. - xmit-hash: определение хэш-политики передачи пакетов через объединенные интерфейсы в режиме XOR или IEEE 802.3ad. Возможные значения: - I2: использует только MAC-адреса для генерации хэша. При этом алгоритме трафик для конкретного сетевого хоста будет отправляться всегда через один и тот же интерфейс. Алгоритм совместим с IEEE 802.3ad. - I2-3: использует как MAC-адреса, так и IP-адреса для генерации хэша. Алгоритм совместим с IEEE 802.3ad. - I3-4: используются IP-адреса и протоколы транспортного уровня (TCP или UDP) для генерации хэша. Алгоритм не всегда совместим с IEEE 802.3ad, так как в пределах одного и того же TCP- или UDP-взаимодействия могут передаваться как фрагментированные, так и нефрагментированные пакеты. Во фрагментированных пакетах порт источника и порт назначения отсутствуют. В результате в рамках одной сессии пакеты могут прийти до получателя не в том порядке, так как отправляются через разные интерфейсы. - interface: интерфейсы, которые будут объединены в бонд.
iface-mode	Режим назначения IP-адреса: - dhcp: получение динамического IP-адреса по DHCP. - manual: без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса.
iface-type	Тип создаваемого интерфейса: - I3 — Layer 3 интерфейс. - mirror — интерфейс зеркалирования трафика.

Параметр	Описание
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся в следующем виде: [<ip_address/mask>] или [<ip_address/mask> <ip_address/mask>], если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел); маска подсети задаётся в десятичном виде. Важно! Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса.
mtu	Указание размер MTU.
mss	Указание размера MSS (доступно в версии ПО 7.3.0 и выше): 0, или от 4 до введённого значения MTU минус 40.

Обновление существующего бонд-интерфейса:

```
Admin@nodename# set network interface bond <bond-name>
```

Параметры, доступные для обновления, аналогичны параметрам создания бонд-интерфейс, кроме **interface-name**, **node-name** (изменение значений этих параметров недоступно).

Команда удаления бонд-интерфейса или его параметров:

```
Admin@nodename# delete network interface bond <bond-name>
```

Параметры, доступные для удаления:

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay server-address	IP-адрес сервера DHCP.
bonding interface	Интерфейсы, объединённые в бонд.

Чтобы отобразить информацию о всех бонд-интерфейсах:

```
Admin@nodename# show network interface bond
```

или об определённом интерфейсе:

```
Admin@nodename# show network interface bond <bond-name>
```

Documentation: 
Product: SIEM
Version: 7.x

Данный раздел находится на уровне **network gateway**.

Для добавления нового шлюза используется команда:

Admin@nodename# create network gateway

Доступные параметры:

Параметр	Описание
enabled	Включение/отключение шлюза: - on. - off.
name	Название шлюза.
description	Описание шлюза.
interface	Интерфейс, использующийся для выхода в Интернет: - Выбор конкретного порта (port0, port1, port2 итд.); auto — после выбора этого параметра порт определится автоматически.
ip	IP-адрес шлюза.
node-name	Выбор узла кластера, для которого настраивается шлюз.
weight	Вес шлюза (чем больше вес, тем большая доля трафика идет через шлюз).
balancing	Режим балансировки - весь трафик в интернет будет распределен между шлюзами в соответствии с указанными весами: - on. - off.
default	Использование данного шлюза в качестве шлюза по умолчанию: - on. - off.

Обновление параметров шлюза:

Admin@nodename# set network gateway <gateway-name>

Список параметров, доступных для изменения, аналогичен списку, доступному при создании шлюза.

Команда для удаления шлюза:

Admin@nodename# delete network gateway <gateway-name>

Чтобы отобразить информацию о всех шлюзах:

Admin@nodename# show network gateway

или об определённом шлюзе:

Admin@nodename# show network gateway <gateway-name>

Documentation: ☒
Product: SIEM
Version: 7.x
Technology: Routing

В данном разделе описана настройка маршрутизации с использованием интерфейса командной строки. Настройка производится на уровне **network routes**.

Для добавления нового статического маршрута используется команда:

```
Admin@nodename# create network routes <parameters>
```

Далее указываются параметры:

Параметр	Описание
enabled	Включение/отключение использования статического маршрута: • on. • off.
name	Имя маршрута.
description	Описание маршрута.
node-name	Выбор узла кластера для настройки маршрутизации.
type	Тип маршрута: • unicast — стандартный тип маршрута. Пересылает трафик, адресованный на адреса назначения, через заданный шлюз. • unreachable — трафик отбрасывается. Источнику отправляется ICMP сообщение host unreachable (type 3 code 1). • prohibit — трафик отбрасывается. Источнику отправляется ICMP сообщение host unreachable (type 3 code 13). • blackhole — трафик отбрасывается (теряется), не сообщая источнику о том, что данные не достигли адресата.
destination-ip	IP-адрес подсети назначения; указывается в формате <ip/mask>.
gateway	IP-адрес шлюза, через который будет доступна указанная подсеть; этот IP-адрес должен быть доступен с устройства.
interface	Интерфейс, через который будет добавлен маршрут.
metric	Метрика маршрута. Если маршрутов в данную сеть несколько: чем меньше метрика, тем более приоритетен маршрут.

Пример добавления статического маршрута:

```
Admin@nodename# create network routes name test_route description "Test static route" destination-ip 192.168.200.0/24 gateway 192.168.100.100 interface port1 type unicast metric 1 enabled on
Admin@nodename#
```

```
Admin@nodename# show network routes test_route
```

```
name      : test_route
description : Test static route
enabled   : on
node-name : testnode1
interface : port1
type      : unicast
destination-ip : 192.168.200.0/24
gateway   : 192.168.100.100
metric    : 1
```

Чтобы изменить параметры созданного ранее статического маршрута, используйте команду:

```
Admin@nodename# set network routes <route-name>
```

Параметры, доступные для изменения, представлены в таблице выше.

Используйте следующую команду для удаления статического маршрута:

```
Admin@nodename# delete network routes <route-name>
```

Пример удаления статического маршрута:

```
Admin@nodename# delete network routes test_route
```

Для отображения статических маршрутов:

```
Admin@nodename# show network routes
```

Documentation: 

Product: SIEM

Version: 7.x

Настройка системных серверов DNS производится на уровне **network dns system-dns-servers**.

Для добавления новых DNS-серверов или обновления существующего списка используются следующие команды:

```
Admin@nodename# set network dns system-dns-servers ip [ <ip> <ip> ... ]
```

Для удаления всего списка адресов серверов DNS:

```
Admin@nodename# delete network dns system-dns-servers
```

Для удаления определённых серверов:

```
Admin@nodename# delete network dns system-dns-servers ip [ <ip> <ip> ... ]
```

Для отображения списка системных DNS-серверов используется команда:

```
Admin@nodename# show network dns
```


Documentation: 
Product: SIEM
Version: 7.x

Настройка IP-адресов

Данный раздел находится на уровне **libraries ip-list**.

Для создания группы IP-адресов используется следующая команда:

```
Admin@nodename# create libraries ip-list <parameters>
```

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название списка адресов.
description	Описание списка.
threat-lvl	Уровень угрозы: very-low — очень низкий уровень угрозы. low — низкий уровень угрозы. medium — средний уровень угрозы. high — высокий уровень угрозы. very-high — высокий уровень угрозы.
type	Тип списка: local — локальный. updateable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром shedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: - Звездочка (*) — обозначает весь диапазон (от первого до последнего). - Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. - Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". - Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".
lists	Выбор существующих IP-листов для добавления в создаваемый лист.
ips	IP-адреса или диапазон IP-адресов, которые необходимо включить в список. Указывается в формате: <ip>, <ip/mask> или <ip_range_start-ip_range_end>.
use-in-search-queries	Должен ли использоваться данный список в поисковых запросах: on; off.

Для редактирования списка (список параметров, доступных для обновления, аналогичен списку параметров команды создания списка):

```
Admin@nodename# set libraries ip-list <ip-list-name> <parameters>
```

Чтобы добавить в список новые адреса:

```
Admin@nodename# set libraries ip-list <ip-list-name> [ <ip1> <ip2> ... ]
```

Следующие команды используются для удаления всего списка адресов или IP-адресов, содержащихся в нём:

```
Admin@nodename# delete libraries ip-list <ip-list-name>
Admin@nodename# delete libraries ip-list <ip-list-name> ips [ <ip1> <ip2>... ]
```

Команда отображения информации о всех имеющихся списках:

```
Admin@nodename# show libraries ip-list
```

Чтобы отобразить информацию об определённом списке, необходимо указать название интересующего списка IP-адресов:

```
Admin@nodename# show libraries ip-list <ip-list-name>
```

Также доступен просмотр содержимого списка IP-адресов:

```
Admin@nodename# show libraries ip-list <ip-list-name> items
```

Настройка useragent браузеров

Данный раздел находится на уровне **libraries useragents**.

Для создания списка useragent браузеров используется следующая команда:

```
Admin@nodename# create libraries useragents <parameters>
```

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название списка.
description	Описание списка.
patterns	Строка описания useragent. Исчерпывающий список строк aseragent представлен на этом ресурсе: http://www.useragentstring.com/pages/useragentstring.php .

Параметр	Описание
type	Тип списка: • local — локальный. • updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром shedule в формате cronlab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение ""/2" в поле "часы" будет означать "каждые два часа".
use-in-search-queries	Должен ли использоваться данный список в поисковых запросах: • on; • off.

Для редактирования списка (список параметров, доступных для обновления, аналогичен списку параметров команды создания списка):

Admin@nodename# set libraries useragents <list-name> <parameters>

Следующие команды используются для удаления всего списка или отдельных useragent из списка по их паттернам:

Admin@nodename# delete libraries useragents <list-name>
Admin@nodename# delete libraries useragents <list-name> <patterns>

Команда отображения информации о всех имеющихся списках:

Admin@nodename# show libraries useragents

Чтобы отобразить информацию об определённом списке, необходимо указать название интересующего списка:

Admin@nodename# show libraries useragents <list-name>

Также доступен просмотр содержимого конкретного списка useragents:

Admin@nodename# show libraries useragents <list-name> patterns

Настройка типов контента

Данный раздел находится на уровне **libraries content-types**.

Для создания списка типов контента используется следующая команда:

Admin@nodename# create libraries content-types <parameters>

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название списка.
description	Описание списка.
mime	Данные в формате MIME. Различные типы контента и их описание доступны по ссылке https://www.iana.org/assignments/media-types/media-types.xhtml .
type	Тип списка: • local — локальный. • updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром shedule в формате cronlab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение ""/2" в поле "часы" будет означать "каждые два часа".
use-in-search-queries	Должен ли использоваться данный список в поисковых запросах: • on; • off.

Для редактирования списка (список параметров, доступных для обновления, аналогичен списку параметров команды создания списка):

Admin@nodename# set libraries content-types <list-name> <parameters>

Следующие команды используются для удаления всего списка или отдельных типов контента, содержащихся в нём:

Admin@nodename# delete libraries content-types <list-name>
Admin@nodename# delete libraries content-types <list-name> mime [<mime1> <mime2>...]

Команда отображения информации о всех имеющихся списках:

Admin@nodename# show libraries content-types

Чтобы отобразить информацию об определённом списке, необходимо указать название интересующего списка:

Admin@nodename# show libraries content-types <list-name>

Также доступен просмотр содержимого списка типов контента:

Admin@nodename# show libraries content-types <list-name> mime

Настройка списков URL

Данный раздел находится на уровне **libraries url-list**.

Для создания списка URL-адресов используется следующая команда:

Admin@nodename# create libraries url-list <parameters>

Далее необходимо задать следующие параметры:

Параметр	Описание
----------	----------

Параметр	Описание
name	Название списка.
description	Описание списка.
case-sensitivity	Чувствительность к регистру в написании адреса URL: sensitive — чувствительно к регистру букв в адресе. insensitive — нечувствительно к регистру букв в адресе. domain — список адресов доменов.
urls	URL, которые необходимо добавить в список.
type	Тип списка: local — локальный. updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром shedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: - Звездочка (*) — обозначает весь диапазон (от первого до последнего). - Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. - Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". - Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение ""/2" в поле "часы" будет означать "каждые два часа".
use-in-search-queries	Должен ли использоваться данный список в поисковых запросах: on; off.

Для редактирования списка (список параметров, доступных для обновления, аналогичен списку параметров команды создания списка):

Admin@nodename# set libraries url-list <list-name> <parameters>

Следующие команды используются для удаления всего списка или отдельных URL-адресов, содержащихся в нём:

Admin@nodename# delete libraries url-list <list-name>
Admin@nodename# delete libraries url-list <list-name> urls [<url1> <url2>...]

Команда отображения информации о всех имеющихся списках:

Admin@nodename# show libraries url-list

Чтобы отобразить информацию об определённом списке, необходимо указать название интересующего списка:

Admin@nodename# show libraries url-list <list-name>

Также доступен просмотр содержимого списка URL-адресов:

Admin@nodename# show libraries url-list <list-name> urls

Настройка почтовых адресов

Раздел находится на уровне **libraries email-list**.

Чтобы добавить новую группу почтовых адресов используется следующая команда:

Admin@nodename#& create libraries email-list <parameter>

Далее указываются параметры:

Параметр	Описание
name	Название группы почтовых адресов.
description	Описание группы почтовых адресов.
type	Тип списка: local — локальный. updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром shedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: - Звездочка (*) — обозначает весь диапазон (от первого до последнего). - Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. - Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". - Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение ""/2" в поле "часы" будет означать "каждые два часа".
emails	Почтовые адреса, которые необходимо добавить в данную группу.

Команда, предназначенная для редактирования информации о группе почтовых адресов:

Admin@nodename# set libraries email-list <email-list-name> <parameter>

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании группы почтовых адресов.

Для удаления группы или почтовых адресов из неё используются следующие команды:

Admin@nodename# delete libraries email-list <email-list-name>
Admin@nodename# delete libraries email-list <email-list-name> emails [<email> ...]

Следующие команды используются для просмотра информации о всех созданных группах, об определённых группах или для просмотра почтовых адресов, входящих в группу:

Admin@nodename# show libraries email-list
Admin@nodename# show libraries email-list <email-list-name>
Admin@nodename# show libraries email-list <email-list-name> emails

Настройка номеров телефонов

Настройка раздела **Номера телефонов** производится на уровне **libraries phone-list**.

Для создания группы телефонных номеров:

Admin@nodename# create libraries phone-list <parameter>

Далее необходимо указать следующие данные:

Параметр	Описание
name	Название группы телефонных номеров.
description	Описание группы телефонных номеров.
type	Тип списка: • local — локальный. • updatable — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (url). Периодичность обновления списка указывается параметром shedule в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".
phones	Номера телефонов, которые необходимо добавить в данную группу.

Для редактирования информации о группе телефонных номеров используется команда:

```
Admin@nodename# set libraries phone-list <phone-list-name> <parameter>
```

Параметры, доступные для обновления, представлены в таблице выше.

Для удаления группы или номеров телефонов из неё используются следующие команды:

```
Admin@nodename# delete libraries phone-list <phone-list-name>
Admin@nodename# delete libraries phone-list <phone-list-name> phones [ <phone> ... ]
```

Следующие команды используются для просмотра информации о всех созданных группах:

```
Admin@nodename# show libraries phone-list
```

или об определённых группах телефонных номеров:

```
Admin@nodename# show libraries phone-list <phone-list-name>
```

Для просмотра номеров, содержащихся в группе, используется команда:

```
Admin@nodename# show libraries phone-list <phone-list-name> phones
```

Настройка команд

Данный раздел позволяет создавать группы команд, предназначенных для отправки на коннекторы.

Для создания списка команд используется команда:

```
Admin@nodename# create libraries commands-list name <command-list-name> type <local | updatable> commands new <command-string>
```

Для редактирования созданного ранее списка команд используется команда:

```
Admin@nodename# set libraries commands-list <command-list-name> commands <command-string>
```

Для просмотра созданного ранее списка команд используется команда:

```
Admin@nodename# show libraries commands-list <command-list-name>
```

Для удаления созданного ранее списка команд или отдельных команд из списка используется команда:

```
Admin@nodename# delete libraries commands-list <command-list-name>
```

```
Admin@nodename# delete libraries commands-list <command-list-name> commands <command-string>
```

Настройка профилей оповещений

Профили оповещений SMTP (no email) и SMPP (no SMS) настраиваются на уровне **libraries notification-profiles**.

Для добавления нового профиля оповещения SMTP:

```
Admin@nodename# create libraries notification-profiles smtp <parameter>
```

Далее необходимо указать:

Параметр	Описание
name	Название профиля.
description	Описание профиля.
host	IP-адрес или FQDN сервера SMTP, который будет использоваться для отсылки почтовых сообщений.
port	Порт TCP, используемый сервером SMTP. Обычно для протокола SMTP используется порт 25, для SMTP с использованием SSL — 465. Уточните данное значение у администратора почтового сервера.
connection-security	Варианты безопасности отправки почты; возможны варианты: • none. • starttls. • ssl.
authentication	Включение/отключение авторизации при подключении к серверу SMTP: • on. • off.
login	Имя учётной записи для подключения к SMTP-серверу.
password	Пароль учётной записи для подключения к SMTP-серверу.

Для создания профиля оповещения по SMS (SMPP):

```
Admin@nodename# create libraries notification-profiles smpp <parameter>
```

Далее необходимо указать значения следующих параметров:

Параметр	Описание
----------	----------

Параметр	Описание
name	Название профиля.
description	Описание профиля.
host	IP-адрес или FQDN сервера SMPP, который будет использоваться для отсылки SMS.
port	Порт TCP, который используется для подключения к серверу SMPP. Обычно для протокола SMPP используется порт 2775; при использовании SSL — 3550.
ssl	Включение/отключение шифрования SSL: • on. • off.
login	Имя учётной записи для подключения к SMPP-серверу.
password	Пароль учётной записи для подключения к SMPP-серверу.
phone-translation-rules	Правила трансляции телефонных номеров. Правила используются для соответствия требованиям провайдера. Например, если необходимо заменить все номера, начинающиеся на +7, на 8: Admin@nodename# set libraries notification-profiles smpp <profile-name> phone-translation-rules + [+7;8]
source-ton	Тип номера (Type of Number) для источника сообщения: • 0 — Unknown (Неизвестный). • 1 — International (Международный). • 2 — National (Государственный). • 3 — Network Specific (Сетевой Специальный). • 4 — Subscriber Number (Номер абонента). • 5 — Alphanumeric (Алфавитно-цифровой). • 6 — Abbreviated (Сокращённый).
dest-ton	Тип номера (Type of Number) для адресата: • 0 — Unknown (Неизвестный). • 1 — International (Международный). • 2 — National (Государственный). • 3 — Network Specific (Сетевой Специальный). • 4 — Subscriber Number (Номер абонента). • 5 — Alphanumeric (Алфавитно-цифровой). • 6 — Abbreviated (Сокращённый).
source-npi	Индикатор схемы присвоения номеров (Numbering Plan Indicator) для источника: • 0 — Unknown. • 1 — ISDN/telephone numbering plan (E.163/E.164). • 3 — Data numbering plan (X.121). • 4 — Telex numbering plan (F.69). • 6 — Land Mobile (E.212). • 8 — National numbering plan. • 9 — Private numbering plan. • 10 — ERMES numbering plan (ETSI DE/PS 3 01-3). • 13 — Internet (IP). • 18 — WAP Client Id (to be defined by WAP Forum).
dest-npi	Индикатор схемы присвоения номеров (Numbering Plan Indicator) для адресата: • 0 — Unknown. • 1 — ISDN/telephone numbering plan (E.163/E.164). • 3 — Data numbering plan (X.121). • 4 — Telex numbering plan (F.69). • 6 — Land Mobile (E.212). • 8 — National numbering plan. • 9 — Private numbering plan. • 10 — ERMES numbering plan (ETSI DE/PS 3 01-3). • 13 — Internet (IP). • 18 — WAP Client Id (to be defined by WAP Forum).

Для редактирования профиля оповещения используется команда:

Admin@nodename# set libraries notification-profiles <smtp | smpp> <profile-name> <parameter>

Параметры профилей SMTP и SMPP, доступные для изменения, представлены в соответствующих таблицах выше.

Для удаления профиля:

Admin@nodename# delete libraries notification-profiles <smtp | smpp> <profile-name>

Также для профилей оповещений SMPP доступно удаление правил трансляции номеров:

Admin@nodename# delete libraries notification-profiles smpp <profile-name> phone-translation-rules [phone1|phone2]

Следующие команды предназначены для отображения информации о всех имеющихся профилях оповещений:

Admin@nodename# show libraries notification-profiles

о всех профилях одного типа:

Admin@nodename# show libraries notification-profiles <smtp | smpp>

об определённом профиле оповещения:

Admin@nodename#show libraries notification-profiles <smtp | smpp> <profile-name>

Настройка категорий срабатывания

Элемент библиотеки **Категории срабатываний** позволяет создать категории, по которым можно группировать определенные срабатывания правил аналитики, применяемые к событиям. Более подробно о правилах аналитики смотрите в разделе [Аналитика](#). По умолчанию создаются категории:

- **Availability** — правила аналитики, определяющие инциденты, приводящие к ухудшению доступности информационных систем.
- **Performance** — правила аналитики, определяющие инциденты, приводящие к ухудшению производительности информационных систем.
- **Security** — правила аналитики, определяющие инциденты, приводящие к ухудшению безопасности информационных систем.

Для создания категорий срабатывания используется команда:

```
Admin@nodename# create libraries alert-categories name <category-name> key <category-key>
```

Для редактирования категорий срабатывания используется команда:

```
Admin@nodename# set libraries alert-categories name <category-name> key <category-key>
```

Для просмотра созданных ранее категорий срабатывания используется команда:

```
Admin@nodename# show libraries alert-categories name <category-name>
```

Для удаления созданных ранее категорий срабатывания используется команда:

```
Admin@nodename# delete libraries alert-categories name <category-name>
```

Настройка внешних сервисов обогащений

В данном элементе библиотеки представлены ресурсы, с помощью которых происходит дополнительный сбор информации об угрозах. С данных источников приходят фиды — структурированные проанализированные данные об IP-адресах и доменах, с которых происходит распространение вредоносных файлов, их сэмплы и хэши; списки фишинговых сайтов, почтовые адреса отправителей фишинговых писем; адреса, с которых происходит сканирование сетей с целью обнаружения уязвимостей; IP-адреса, с которых проводятся атаки типа брутфорс; сигнатуры для обнаружения вредоносного программного обеспечения. Подробнее о доступных сервисах читайте в разделе [Внешние сервисы обогащений](#) Руководства администратора UserGate SIEM.

Чтобы использовать сервисы обогащения их необходимо включить. Для использования некоторых сервисов обогащения необходимо прохождение регистрации и предоставление ключа доступа.

Для редактирования сервисов обогащений используется команда:

```
Admin@nodename# set libraries enrichment-services <service-name>
```

Для просмотра сервисов обогащений используется команда:

```
Admin@nodename# show libraries enrichment-services <service-name>
```

Настройка syslog-фильтров

Создание и настройка syslog-фильтров производятся на уровне **libraries syslog-filters**.

Команда для создания syslog-фильтра:

```
Admin@nodename# create libraries syslog-filters <parameter>
```

Далее представлены параметры, которые необходимо указать:

Параметр	Описание
name	Название фильтра.
description	Описание фильтра.
login-address	Строка для поиска IP-адреса пользователя в syslog-сообщении.
login-event	Строка для поиска события входа пользователя в syslog-сообщении.
login-username	Строка для поиска имени пользователя в syslog-сообщении.
logout-address	Строка для поиска IP-адреса пользователя в syslog-сообщении.
logout-event	Строка для поиска события выхода пользователя в syslog-сообщении.
logout-username	Строка для поиска имени пользователя в syslog-сообщении.

Следующая команда предназначена для редактирования информации о syslog-фильтре:

```
Admin@nodename# set libraries syslog-filters <filter-name> <parameter>
```

Параметры, доступные для обновления, аналогичны параметрам, указываемым при создании фильтра.

Чтобы отобразить информацию о syslog-фильтрах:

```
Admin@nodename# show libraries syslog-filters <filter-name>
```

Пользователь может удалить syslog-фильтр, используя следующую команду:

```
Admin@nodename# delete libraries syslog-filters <filter-name>
```

Настройка приложений syslog

Создание и настройка приложений syslog производятся на уровне **libraries syslog-application**.

Команда для создания приложений syslog:

```
Admin@nodename# create libraries syslog-application <parameter>
```

Далее представлены параметры, которые необходимо указать:

Параметр	Описание
name	Название приложения.
description	Описание приложения.
app-name	Название приложения, отображаемое в журналах.

Documentation: 
Product: SIEM
Version: 7.x

Для сбора информации с различных устройств и последующего ее анализа UserGate SIEM использует сенсоры. Сенсор — это совместимое с UserGate SIEM устройство, которое может передавать определенные данные на сервер SIEM. Сенсорами могут выступать устройства UserGate NGFW, конечные устройства UserGate Client, а также любые другие сетевые устройства, способные передавать данные по протоколу SNMP.

Сенсоры UserGate

Сенсор UserGate подключает одно устройство типа межсетевого экрана UserGate к UserGate SIEM. Для подключения сенсора UserGate необходимо выполнить следующие шаги:

1. На **NGFW** разрешить сервисы **Log Analyzer** и **SNMP** в настройках требуемой зоны:

Admin@ngfw-nodename# set network zone <zone-name> enabled-services [SNMP "Log Analyzer"]

2. На **NGFW** получить токен устройства:

Admin@ngfw-nodename# show settings general log-analyzer

state : ready
logan-server : 127.0.0.1
logan-version : 7.1.0.
device-version : 7.1.0.
device-code : 9R4FCVET

3. В UserGate SIEM разрешить сервис **База данных журналов** в свойствах требуемой зоны:

Admin@nodename# set network zone <zone-name> enabled-services ["Log Analyzer"]

4. Создать сенсор UserGate.

Для создания сенсора UserGate используется команда:

Admin@ndeformedo# create sensors ug-sensors <parameters>

Необходимо добавить следующие параметры:

Параметр	Описание
enabled	Включает или выключает данный сенсор UserGate.
name	Название сенсора UserGate.
description	Оptionальное описание сенсора UserGate.
address	IP-адрес узла UserGate, для которого создается данный сенсор.
SIEM-address	IP-адрес сервера UserGate SIEM, который будет использоваться на узле UserGate, в качестве назначения для отсылки журналов. Для выбора отображаются только те адреса, на интерфейсах зон которых разрешен сервис Log Analyzer.
device-code	Токен, полученный на узле UserGate.

После создания сенсора, узел UserGate начинает отсылать данные в UserGate SIEM.

Для просмотра сенсоров UserGate используется команда:

Admin@nodename# show sensors ug-sensors

Сенсоры SNMP

С помощью сенсора SNMP администратор может подключить SNMP-совместимое сетевое устройство к серверу UserGate SIEM для сбора и анализа его метрик. UserGate SIEM может отображать любые счетчики, полученные по SNMP с помощью запросов SNMP. Для настройки сенсора SNMP необходимо иметь базы MIB (Management Information Base) на управляемое устройство.

Для настройки сенсора SNMP необходимо выполнить следующие шаги:

1. Загрузить базу MIB того устройства, которое требуется добавить для мониторинга.

2. Создать сенсор SNMP:

Admin@nodename# create sensors snmp-sensors <parameters>

Далее указать следующие параметры.:

Наименование	Описание
enabled	Включает или выключает данный сенсор SNMP.
name	Название сенсора SNMP.
description	Оptionальное описание сенсора SNMP.
ip	IP-адрес сенсора SNMP.
port	Порт сенсора SNMP. Обычно для запросов данных по протоколу SNMP используется порт TCP 161.
version	Указывает версию протокола SNMP, которая будет использоваться в данном сенсоре. Возможны варианты SNMP v2 (2) и SNMP v3 (3).
community	SNMP community — строка для идентификации сервера UserGate SIEM и сетевого устройства для версии SNMP v2. Используйте только латинские буквы и цифры.
interval	Интервал в секундах, через который сервер UserGate SIEM будет инициировать получение данных с сетевого устройства.
username	Только для SNMP v3. Имя пользователя для аутентификации сетевом устройстве.
auth-type	Выбор режима аутентификации. Возможны варианты: - Без аутентификации, без шифрования (none). - С аутентификацией, без шифрования (no-encrypt). - С аутентификацией, с шифрованием (encrypt).

Наименование	Описание
auth-alg	Алгоритм, используемый для аутентификации: • md5; • sha; • sha224; • sha256; • sha284; • sha512.
auth-password	Пароль, используемый для аутентификации.
encrypt-alg	Алгоритм, используемый для шифрования. Возможно использовать DES и AES.
encrypt-password	Пароль, используемый для шифрования.
counters	Укажите здесь все требуемые данные, которые UserGate SIEM будет запрашивать на сетевом устройстве. Счетчики выбираются из баз MIB, которые загружены на устройство. Укажите в скобках [] SNMP OID счетчика.

Для просмотра сенсоров SNMP используется команда:
Admin@nodename# show sensors snmp-sensors

Сенсоры WMI

С помощью сенсора WMI администратор может подключить WMI-совместимое сетевое устройство (компьютер под управлением ОС Windows) к UserGate SIEM для сбора и анализа его метрик.
Для создания сенсора WMI используется команда:
Admin@nodename# create sensors wmi-sensors <parameters>
Далее указать следующие параметры::

Наименование	Описание
enabled	Включает или выключает данный сенсор.
name	Название сенсора.
description	Опциональное описание сенсора.
ip	IP-адрес сенсора.
login	Имя пользователя для подключения к устройству.
password	Пароль пользователя для подключения к устройству.
namespace	Пространство имен идентификаторов.
polling-interval	Интервал опроса в секундах.
counters	Указать данные, которые UserGate SIEM будет мониторить на сетевом устройстве: • name — название счетчика. • type — тип счетчика (windows-event-logs). • filter-query — WQL запрос (например, Logfile='Security').

Для просмотра сенсоров WMI используется команда:
Admin@nodename# show sensors wmi-sensors

Конечные устройства

Конечное устройство с установленным программным обеспечением UserGate Client будет отображено при выборе на UGMC данного устройства UserGate SIEM в качестве сервера для передачи информации о событиях, при этом UserGate SIEM должен быть предварительно зарегистрирован на UGMC (подробнее читайте в разделе [Управление устройствами LogAn](#)).
Для просмотра данных конечных устройств используется команда:
Admin@nodename# show sensors endpoint-devices

Коннекторы

Коннекторы используются для возможности подключения устройства UserGate SIEM к различным средствам защиты с целью сбора информации.
Для добавления коннектора предназначена команда:
Admin@nodename# create sensors connectors <parameters>
Необходимо указать следующие данные:

Параметр	Описание
name	Название коннектора.
description	Описание коннектора (опционально).
server-type	Выбор типа сервера: • SSH; • HTTP; • HTTPS (в текущей версии реализован только для интеграции с ГосСОПКА) .
address-format	Тип: • ip. • fqdn.

Параметр	Описание
ip	IP-адрес сервера; указывается в случае выбора адреса сервера типа IP .
port	Порт сервера; указывается в случае выбора адреса сервера типа IP .
fqdn	FQDN сервера; указывается в случае выбора адреса сервера типа FQDN .
url-path	Используется при управлении устройством по API.
login	Логин пользователя для авторизации на коннекторе.
password	Пароль учётной записи пользователя, необходимый для авторизации на коннекторе.
connamd-group	Указание группы команд доступно только для SSH-сервера, подробнее читайте в разделе Команды .
headers	Указание заголовков доступно только для серверов HTTP и HTTPS.

Для редактирования созданного ранее коннектора используется команда:

```
Admin@nodename# create sensors connectors <connector-name> <parameters>
```

Для просмотра параметров созданных ранее коннекторов используется команда:

```
Admin@nodename# show sensors connectors <connector-name>
```

Для удаления созданных ранее коннекторов используется команда:

```
Admin@nodename# delete sensors connectors <connector-name>
```


Documentation: ☒
Product: SIEM
Version: 7.x

Настройка параметров мониторинга устройства в интерфейсе CLI производится в режиме конфигурации на уровне **monitoring**. Команды этого уровня позволяют управлять настройкой параметров SNMP устройства, правил мониторинга по SNMP, профилей безопасности для аутентификации SNMP-менеджеров, правилами оповещений. Подробнее о правилах мониторинга и оповещений читайте в разделе [Оповещения](#).

Настройка параметров SNMP устройства

Для настройки параметров SNMP устройства используются команды на уровне **monitoring smnp-parameter**:

Admin@nodename# edit monitoring smnp-parameter <parameters>

Для редактирования доступны следующие параметры:

Параметр	Описание
agent-name	Название системы, используемое подсистемой управления SNMP.
location	Информация о физическом расположении SNMP-агента.
description	Описание системы.
Engine ID	Каждое устройство UserGate имеет уникальный идентификатор SNMPv3 Engine ID. По умолчанию Engine ID генерируется на основании имени узла UserGate. При редактировании Engine ID необходимо указать длину (length), тип и значение идентификатора. Длина может быть определена как фиксированная (не более 8 байт) или динамическая (не более 27 байт). Фиксированная длина идентификатора применима только для типа text . Engine ID может быть сформирован в формате: ip4 — IPv4. ipv6 — IPv6. mac — MAC-адрес. text — Текст. octets — Октеты.

Подробнее о параметрах SNMP устройства UserGate читайте в разделе [SNMP](#).

Настройка правил мониторинга по SNMP

Для настройки правил мониторинга устройства по SNMP используются команды на уровне **monitoring smnp**:

Admin@nodename# edit monitoring smnp <parameters>

Для редактирования доступны следующие параметры:

Параметр	Описание
name	Название правила.
enabled	Включение/отключение правила
community	SNMP community — строка для идентификации устройства UserGate и сервера управления SNMP для версии SNMP v2c. Используйте только латинские буквы и цифры.
context	Необязательный параметр, определяющий SNMP context. Можно использовать только латинские буквы и цифры. На некоторых устройствах может быть несколько копий полного поддерева MIB. Например, на устройстве может быть создано несколько виртуальных маршрутизаторов. Каждый такой виртуальный маршрутизатор будет иметь полное поддерево MIB. В этом случае каждый виртуальный маршрутизатор может быть указан как контекст на сервере SNMP. Контекст определяется по имени. Когда клиент отправляет запрос, он может указать имя контекста. Если имя контекста не указано, будет запрошен контекст по умолчанию.
version	Указывает версию протокола SNMP, которая будет использоваться в данном правиле. Возможны варианты SNMP v2c и SNMP v3.
query	При включении разрешает получение и обработку SNMP-запросов от SNMP-менеджера.
trap	При включении разрешает отправку SNMP-трапов на сервер, настроенный для приема оповещений.
trap-host	IP-адрес сервера для трапов. Данная настройка необходима только в случае, если необходимо отправлять трапы на сервер оповещений.
trap-port	Порт, на котором сервер слушает оповещения. Обычно это порт UDP 162. Данная настройка необходима только в случае, если необходимо отправлять трапы на сервер оповещений.
security-profile	Только для SNMP v3. Подробнее — в разделе Профили безопасности SNMP .
events	Выбор типов параметров, доступных для мониторинга по правилу.

Для работы SNMP-менеджера с устройством UserGate необходимо в свойствах зоны интерфейса, к которому будет осуществляться подключение по протоколу SNMP, разрешить сервис **SNMP** в настройках контроля доступа. Подробнее о настройке зон в CLI читайте в разделе [Настройки сети](#).

Настройка профилей безопасности SNMP

Для настройки профилей безопасности для аутентификации SNMP-менеджеров используются команды на уровне **monitoring smnp-security-profile**:

Admin@nodename# edit monitoring smnp-security-profile <parameters>

Для редактирования доступны следующие параметры:

Параметр	Описание
name	Название профиля безопасности SNMP
description	Описание профиля безопасности SNMP
username	Имя пользователя для аутентификации SNMP-менеджера.

Параметр	Описание
auth-type	Выбор режима аутентификации SNMP-менеджера. Возможны варианты: • none — без аутентификации, без шифрования. • no-encrypt — с аутентификацией, без шифрования. • encrypt — с аутентификацией, с шифрованием. Наиболее безопасным считается режим работы authPriv.
auth-alg	Алгоритм, используемый для аутентификации. Возможно использовать: • sha; • md5; • sha224; • sha256; • sha384; • sha512.
auth-password	Пароль, используемый для аутентификации.
encrypt-alg	Алгоритм, используемый для шифрования. Возможно использовать DES и AES.
encrypt-password	Пароль, используемый для шифрования.

Настройка правил оповещений

Для настройки правил оповещений используются команды на уровне **monitoring alert-rules**:

Admin@nodename# edit monitoring alert-rules <parameters>

Для редактирования доступны следующие параметры:

Параметр	Описание
enabled	Включает/отключает данное правило.
name	Название правила.
description	Описание правила.
notification-profile	Созданный ранее профиль оповещения.
sender	От кого будет приходить оповещение.
subject	Тема оповещения.
timeout	Тайм-аут, в течение которого сервер не будет отправлять сообщение при повторном срабатывании данного правила. Данная настройка позволяет предотвратить шторм сообщений при частом срабатывании правила оповещения.
events	События, для которых необходимо получать оповещения.
phones	Для SMPP-профиля. Группы номеров телефонов, куда отправлять SMS-оповещения.
emails	Для SMTP-профиля. Группы адресов email, на которые будут отправляться почтовые оповещения.

Documentation: ☒
Product: SIEM
Version: 7.x

Раздел **Инциденты** предоставляет функциональность встроенной в UserGate SIEM системы IRP — платформы управления процессами реагирования на инциденты информационной безопасности. Инцидентом считается событие или набор событий информационной безопасности, которые подлежат расследованию. UserGate SIEM позволяет настроить процесс расследования инцидентов индивидуально под нужды конкретной компании.

Подробнее о функциональности системы IRP читайте в разделе [Инциденты](#) в Руководстве администратора UserGate SIEM.

Настройки инцидентов в интерфейсе CLI производятся на уровне **incident**.

Для создания собственной схемы расследования инцидентов необходимо:

1. Создать необходимые решения инцидентов.
2. Создать типы инцидентов.
3. Создать состояния инцидентов.
4. Создать схему инцидентов.
5. Активировать схему инцидентов.

Для создания решения инцидентов используется команда:

```
Admin@nodename# create incident resolutions name <incident-name> description <incident-description>
```

Для создания типов инцидентов используется команда:

```
Admin@nodename# create incident types name <incident-type-name> description <incident-type-description>
```

Для создания состояния инцидентов используется команда:

```
Admin@nodename# create incident states name <incident-state-name> description <incident-state-description> group <open|closed|progress>
```

Для создания схемы инцидентов используется команда:

```
Admin@nodename# create incident schema <parameters>
```

Для редактирования доступны следующие параметры схемы инцидентов:

Параметр	Описание
name	Название схемы.
description	Описание схемы
prefix	Префикс, который будет использован при назначении идентификаторов создаваемым инцидентам. Идентификатор будет иметь вид: префикс — порядковый номер, например INC-99.
initial-state	Начальное состояние, которое принимает инцидент при его создании.
workflow-states	Состояния рабочего процесса — описывает все состояния, которые может принимать инцидент в своем жизненном цикле.
incidents-resolutions	Решения инцидентов — указывает список возможных решений инцидентов.
incidents-types	Типы инцидентов, которые могут быть использованы в этой схеме.
transition	Все возможные переходы между состояниями.

Для всех этапов создания схемы инцидентов также доступны команды **set** (редактирование), **show** (просмотр) и **delete** (удаление).

Documentation: ☒
Product: SIEM
Version: 7.x

UserGate SIEM позволяет проводить анализ журналов событий безопасности, получаемых с настроенных сенсоров. Все данные хранятся в одной базе данных, что даёт возможность осуществлять сложный поиск, корреляцию повторяющихся событий, их агрегацию, создавая инциденты безопасности, и упростить процесс изучения особенностей инцидентов. Подробнее об архитектуре и принципах работы функциональности UserGate SIEM — в разделе [Аналитика](#) Руководства администратора UserGate SIEM.

В интерфейсе CLI возможно создавать и настраивать правила аналитики и действия реагирования. С помощью правил аналитики инженер безопасности может автоматизировать процесс корреляции событий и создание срабатываний, а также назначить определенные действия реагирования (реакцию) системы на создаваемые срабатывания. Все это позволяет облегчить процесс изучения регистрируемых событий и сократить время между обнаружением проблемы и ее решением.

Правила аналитики и действия реагирования в CLI создаются и настраиваются на уровне **analytics**.

Правила аналитики

С помощью правил аналитики происходит обработка событий журналов. Настройка правил аналитики позволяет производить сложный поиск среди событий информационной безопасности. Срабатывание правила происходит при выявлении корреляции событий с разных источников.

Для создания правила аналитики предназначена команда:

Admin@nodename# create analytics analytics-rules <parameters>

Далее необходимо указать следующие параметры:

Параметр	Описание
enabled	on/off — Включение/отключение правила аналитики для работы в режиме реального времени.
name	Название правила аналитики.
description	Описание правила аналитики.
threat-level	Уровень угрозы, который будет отображаться при срабатывании правила. informational: события, сформировавшие срабатывание правила аналитики, представляют очень низкий уровень угрозы, и администратор может не предпринимать никаких действий. low: события, сформировавшие срабатывание правила аналитики, представляют низкий уровень угрозы, и администратор может не предпринимать никаких действий. medium: необходимо обратить внимание на события, попавшие под срабатывание правила аналитики. high: события, требующие исследования и принятия мер. critical: события, требующие исследования и срочного принятия мер.
priority	Показывает приоритет, установленный для срабатывания правила аналитики: low: срабатывания данных правил обладают низким приоритетом реагирования. normal: на срабатывания данных правил необходимо обратить внимание и, возможно, предпринять меры. important: на срабатывания данных правил необходимо обратить внимание и предпринять меры. critical: срабатывания данных правил требуют незамедлительного реагирования. При срабатывании правила установленный приоритет будет указывать на важность срабатывания правила аналитики.
alert-category	Отображает категорию, к которой относится срабатывание. По умолчанию для выбора доступны следующие категории: security: правила данной категории определяют инциденты, приводящие к ухудшению безопасности информационных систем. availability: правила данной категории определяют инциденты, которые приводят к ухудшению доступности информационных систем. performance: правила данной категории определяют инциденты, которые приводят к ухудшению производительности информационных систем. Дополнительные категории срабатываний могут быть созданы в библиотеке Категории срабатывания . Подробнее читайте в разделе Настройка категорий срабатывания .
timezone	Указывает на часовой пояс, во времени которого будут работать правила аналитики, т.к. сервер может собирать данные с источников, находящихся в различных часовых поясах.
response-actions	Выбор действий реагирования, которые будут выполнены автоматически при срабатывании правила аналитики. Подробнее о создании действий реагирования и их настройке читайте в разделе Действия реагирования .
conditions	Указание условий срабатывания правила.

Условия срабатывания, которые указываются при создании правила аналитики, имеют следующие параметры настройки:

Параметр	Описание
name	Название условия правила аналитики.
description	Описание условия правила аналитики.
condition-time-enabled	Включить/отключить ограничение времени выполнения условия. При включении ограничения времени правило аналитики работает, только в том случае, когда за указанный отрезок времени условие выполнится заданное количество раз.
condition-time	Указывает на отрезок времени, за который условие должно выполниться заданное количество раз, чтобы произошло срабатывание правила аналитики. Время указывается в секундах. Указание времени выполнения условия доступно при активированном параметре condition-time-enabled .
break-query-enabled	Включить/отключить использование запроса остановки в правиле аналитики.
break-query	SQL-подобный поисковый запрос остановки выполняется вместе с запросом условия. Для формирования запроса используются названия полей, значения полей, ключевые слова и операторы (задаётся аналогично запросу фильтра). Если при выполнении анализа найдётся хотя бы одна запись, соответствующая заданному запросу остановки, до того, как будет найдено заданное количество событий, соответствующих условию правила аналитики, то правило аналитики не работает, а счётчик количества записей, найденных до выполнения запроса остановки, будет обнулён.
filter-query	Отображает SQL-подобный поисковый запрос условия, который пишется по базе журналов. Для формирования запроса используются названия полей, значения полей, ключевые слова и операторы. Синтаксис написания запроса можно посмотреть в разделе Поиск и фильтрация данных . Запрос также может быть написан с использованием синтаксиса Google/RE2 в операторе MATCH. Подробнее о синтаксисе Google/RE2 в операторе MATCH: https://github.com/google/re2/wiki/Syntax .

Параметр	Описание
group-by	Отображает список параметров, по которым могут быть сгруппированы правила в результате срабатывания. Поля будут отображены при просмотре карточки срабатывания. О параметрах, по которым возможна группировка, читайте в разделе Поиск . При указании категорий для группировки правило аналитики сработает только в том случае, если условие выполнится именно для выбранной категории заданное количество раз, указанное в поле параметра pattern-repeats .
pattern-repeats	Показывает количество выполнений условия, необходимое для срабатывания правила. Данный параметр может быть использован вместе с параметром condition-time-enabled или без него.

Для правил аналитики также доступны команды **set** (редактирование), **show** (просмотр) и **delete** (удаление).

Действия реагирования

Действия реагирования позволяют определить методы реагирования при срабатывании правил аналитики информационной безопасности. UserGate SIEM позволяет гибко настраивать правила, используя переменные, относящиеся к категориям срабатывания правил аналитики.

Для создания действия реагирования предназначена команда:

```
Admin@nodename# create analytics response-actions <parameters>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
enabled	on/off — Включение/отключение правила реагирования.
name	Название правила реагирования.
description	Описание правила реагирования.
action	Показывает действие, выбранное для исполнения в случае срабатывания правила аналитики. Действие реагирования выполнится, если оно указано в свойствах правила аналитики. Для выбора доступны следующие виды реагирования: send-email: отправка письма на выбранные почтовые адреса. Настройка действия Отправить email будет рассмотрена далее в разделе Действие типа send-email. send-message: отправка сообщения на указанные номера телефонов. Настройка действия Отправить сообщение будет рассмотрена далее в разделе Действие типа send-message. webhook: получение уведомления о срабатывании правила на веб-странице, адрес которой был указан при настройке действия. Настройка действия Webhook будет рассмотрена далее в разделе Действие типа webhook. create-incident: автоматическое создание инцидента в результате срабатывания правил аналитики. О настройке действия Создать инцидент читайте в разделе Настройки инцидентов. send-command-to-connector: отправка команды на выбранный коннектор. Настройка действия Послать команду на коннектор будет рассмотрена далее в разделе Действие типа send-command-to-connector. send-command-to-endpoint: отправка команды на конечное устройство с установленным ПО UserGate Client. Подробнее читайте в раздел Действие типа send-command-to-endpoint.
enable-logging	Включает/отключает журналирование данных о срабатывании действия реагирования. Данные записываются в журнал событий UserGate SIEM.
grouping	Для удобства при настройке действий реагирования возможно использование функции группировки срабатываний. Группировка возможна по следующим параметрам: never — никогда. period — при настройке группировки срабатываний правила аналитики за период времени действие реагирования выполнится, если в течение указанного времени произошло хотя бы одно срабатывание. number — при настройке группировки по количеству срабатываний правила аналитики действие реагирования выполнится только после указанного количества срабатываний.
time-period	Отображает период группировки в минутах. Задание параметра возможно только при выборе группировки похожих срабатываний за период времени.
alerts-number	Отображает заданное количество срабатываний. Задание параметра возможно только при выборе группировки похожих срабатываний по их количеству.

Для действий реагирования также доступны команды **set** (редактирование), **show** (просмотр) и **delete** (удаление).

Действие типа send-email

Если в качестве действия реагирования была выбрана отправка email, то в свойствах правила реагирования необходимо указать следующие параметры.

Наименование	Описание
notification-profile	Профиль оповещения SMTP, который будет использован для отправки email. Подробнее о настройке профилей SMTP читайте в главе Настройка профилей оповещений .
sender	Имя отправителя письма.
subject	Тема письма.
emails	Список почтовых адресов получателей. Получатели должны быть добавлены в списки в библиотеке элементов. О добавлении почтовых адресов читайте в разделе Настройка почтовых адресов .
template	Шаблон письма уведомления с возможностью передачи значений различных переменных, относящихся к срабатыванию. Подробнее читайте в разделе Шаблон уведомлений и Переменные для уведомлений и команд .

Действие типа send-message

Если в качестве действия реагирования была выбрана отправка сообщения, то в свойствах правила реагирования необходимо указать следующие параметры.

Наименование	Описание
notification-profile	Профиль оповещения SMPP, который будет использован для отправки сообщения. Подробнее о настройке профилей SMPP читайте в главе Настройка профилей оповещений .
sender	Имя отправителя письма.
phones	Список номеров телефонов получателей. Получатели должны быть добавлены в библиотеку элементов. О добавлении телефонных номеров читайте в разделе Настройка номеров телефонов .
template	Шаблон сообщения с возможностью передачи значений различных переменных, относящихся к срабатыванию. Подробнее читайте в разделе Шаблон уведомлений и Переменные для уведомлений и команд .

Действие типа webhook

Для настройки webhook в свойствах правила реагирования необходимо указать следующие параметры.

Наименование	Описание
url	Адрес веб-сайта, на котором будут отображаться оповещения о срабатывании правила.
template	Шаблон уведомления с возможностью передачи значений различных переменных, относящихся к срабатыванию. Подробнее читайте в разделе Шаблон уведомлений и Переменные для уведомлений и команд .

Для тестирования webhook можно воспользоваться сервисом <https://webhook.site>. Для этого необходимо перейти на сайт [Webhook.site](#) и скопировать созданную ссылку. Далее её необходимо указать в свойствах правила реагирования в поле url параметра **action**.

Действие типа send-command-to-connector

В качестве одного из действий реагирования может быть настроена отправка команды на коннектор.

Если в качестве действия реагирования настроена передача команды для исполнения на коннекторе, то необходимо указать следующие параметры:

Наименование	Описание
connectors	Выбор устройств, на которые необходимо отправить команду в случае срабатывания правила аналитики. Коннектор должен быть заранее добавлен и настроен. Подробнее читайте в разделе Коннекторы . Важно! Могут выбраны только коннекторы с одинаковой группой команд.
command	Определение команды, которая будет передана на коннектор для выполнения; представлены команды группы, указанной для выбранных коннекторов. В случае наличия в команде переменных, будут отображены дополнительные поля для указания их значений. Подробнее о командах читайте в разделе Настройка команд .

Действие типа send-command-to-endpoint

В качестве одного из действий реагирования может быть настроена отправка команды на конечное устройство с установленным ПО UserGate Client. Доступны следующие команды:

- block** — блокировка доступа к сети Интернет.
- kill** — завершение указанного в запросе фильтра процесса.

Шаблон уведомлений

В параметре **template** необходимо указать текст уведомления. Можно передавать не только фиксированный текст, но и данные, относящиеся к срабатыванию или его записям в журнале.

Чтобы передать данные, относящиеся к срабатыванию, необходимо в поле **template** ввести название одного из параметров, представленных в таблице. Например, если ввести **{ANALYTICS_RULE_NAME}**, то в тексте уведомления, настроенном как отправка email, SMS или webhook, будет отражено название правила аналитики, которое сработало. Если заполнить шаблон при настройке действия **create incident**, то текст будет отображён в описании инцидента.

Дашборд (описание)

Documentation: ☒
Product: SIEM
Version: 7.x

Данный раздел позволяет посмотреть текущее состояние сервера и серверов, которые подключены к нему для отправки логов, их загрузку, статус лицензии и так далее.

Отчеты предоставлены в виде виджетов, которые могут быть настроены администратором системы в соответствии с его требованиями. Виджеты можно добавлять, удалять, изменять расположение и размер на странице **Дашборд**. По умолчанию созданы страницы с виджетами UserGate SIEM (отображение состояния сервера UserGate SIEM), NOC (Network Operation Center) и SOC (Security Operation Center), Срабатывания (срабатывания правил аналитики).

Некоторые виджеты позволяют настроить отображение, указать фильтрацию данных и настроить прочие параметры. Для настройки виджета необходимо кликнуть по символу шестеренки в правом верхнем углу. Не все параметры, перечисленные ниже, доступны для каждого типа виджетов.

Наименование	Описание
Название	Название виджета, которое будет отображаться в Дашборд.
Описание	Опциональное описание виджета.
Количество записей	Максимальное количество записей для отображения.
Группировать по	Поле данных, по которому будут сгруппированы данные в виджете.
Диаграмма	Выбор типа представления данных. Доступны значения: - Число - Круговая диаграмма - Вертикальная гистограмма - Горизонтальная гистограмма - Таблица - График - Карта мира
Запрос фильтра	SQL-подобная строка запроса, позволяющая ограничить объем информации, используемой при построении виджета. Для формирования запросов используются названия полей, значения полей, ключевые слова и операторы. Ключевые слова и операторы, а также примеры их использования можно посмотреть в разделе документации Поиск и фильтрация данных .
Сенсор	Сенсор, данные с которого используются для данного виджета.

Раздел технической поддержки

Documentation: ☒
Product: SIEM
Version: 7.x

Раздел технической поддержки [на сайте компании](#) содержит дополнительную информацию по настройке устройства. Здесь же вы можете оставить заявку на решение возникшей проблемы с оборудованием.

Аварийные ситуации

Product: SIEM

Version: 7.x

Сбои в работе устройства могут возникнуть при некорректной установке обновлений программного обеспечения.

Для профилактики аварийных ситуаций:

1. Перед установкой обновления сделайте резервную копию устройства. Подробнее — в разделе « [Управление резервным копированием](#)».
2. Во время установки обновления создайте [точку восстановления системы](#). Это позволит оперативно вернуть систему в рабочее состояние.

В случае возникновения аварийной ситуации при обновлении устройства:

1. Восстановите предыдущую стабильную версию ПО. Подробнее — в разделе « [Обновление ПО](#)».
2. Обратитесь в службу технической поддержки в зависимости от уровня вашего сервисного контракта:
 - Premium-поддержка: позвоните по выделенному телефону для экстренной помощи.
 - Brilliant-поддержка: свяжитесь с вашим выделенным техническим специалистом.
 - Базовая поддержка: обратитесь за квалифицированной помощью [на странице поддержки](#).

Admin (описание)

Documentation: ☒
Product: SIEM
Version: 7.x

Данный раздел позволяет зарегистрированному администратору сменить свой пароль, изменить некоторые настройки профиля и выйти из системы.

Наименование	Описание
Сменить пароль	Для смены пароля необходимо указать свой текущий пароль и два раза указать новый пароль.
Предпочтения	- Количество элементов на странице — устанавливает количество строк, отображаемых в одном диалоговом окне, например, список правил межсетевого экрана. - Ночной режим — устанавливает черный цвет темы графического интерфейса UGOS. - Популярные фильтры — изменение названия или удаление фильтров различных журналов, созданных данным пользователем.
Выход	Завершение сеанса работы в веб-консоли устройства.

Избранные (описание)

Documentation: 
Product: SIEM
Version: 7.x

В веб-интерфейсе имеется возможность фильтрации отображаемых разделов путем их добавления в избранное и поиск разделов по их названию. Фильтрация позволяет скрыть неиспользуемые разделы. Отображение только избранных разделов не влияет на функциональность или конфигурацию устройств. Чтобы добавить раздел в избранные, необходимо отметить символ звездочки напротив названия раздела; для настройки отображения используйте переключатель **Только избранные**, расположенный в нижней части панели.

Требования к сетевому окружению

Documentation: ☒
Product: SIEM
Version: 7.x

Сервис	Протокол	Порт	Исходящий/Входящий	Функция
Веб-консоль	TCP	8010	Входящий (к веб-консоли UserGate SIEM)	Доступ к веб-интерфейсу управления устройством.
CLI по SSH	TCP	2200	Входящий (к CLI по SSH)	Доступ к интерфейсу командной строки (CLI) UserGate по протоколу SSH.
XML-RPC	TCP	4041	Входящий (к UserGate по API)	Управление устройством UserGate по API.
XML-RPC поверх HTTPS	TCP	4443	Входящий (к UserGate по API)	Доступ к API поверх HTTPS.
Удалённый помощник	TCP	22	Исходящий (до серверов технической поддержки)	Удалённый доступ к серверу технической поддержки. Доступ к серверам: 93.91.171.46; 178.154.221.222; - ra.entensys.com.
NTP	UDP	123	Исходящий (до сервера точного времени)	Синхронизация времени.
DNS	UDP	53	Исходящий (до DNS-серверов)	Сервис получения информации (IP-адрес) о доменах.
Регистрация сервера UserGate	TCP	443	Исходящий (до сервера регистрации)	Доступ до сервера регистрации продуктов UserGate reg2.usergate.com.
Обновление ПО и библиотек	TCP	443	Исходящий (до серверов обновления)	Обновление программного обеспечения и элементов библиотек: доступ до сервера updates.usergate.com.
Связь с UGMC	TCP	9712	Исходящий (от UserGate SIEM к UGMC)	Первоначальная установка связи и обмен ключами шифрования с сервером UGMC.
		2022	Исходящий (от UserGate SIEM к UGMC)	Построение SSH-туннеля для обмена данными с помощью полученных ключей.
Сервис SIEM	TCP	9713	Исходящий (от UserGate SIEM к NGFW)	Первоначальная установка связи и обмен ключами шифрования с сервером NGFW.
		2023	Исходящий (от UserGate SIEM к UserGate NGFW)	Построение SSH-туннеля для обмена данными с помощью полученных ключей.
	TCP	22699 (приём данных от NGFW 6.x.x), 22711 (приём данных от NGFW 7.x.x, использующих SSL)	Входящий (от UserGate NGFW к UserGate SIEM)	Сервис сбора журналов UserGate SIEM.
SNMP	UDP	161	Входящий (к UserGate SIEM)	Доступ к серверу UserGate SIEM по протоколу SNMP.
Сборщик логов	TCP/UDP	514	Входящий (к UserGate SIEM)	Сервис сбора информации от удаленных устройств по стандарту syslog.
SMTP	TCP	25	Исходящий (к почтовому серверу)	Отправка уведомлений на электронную почту.
DHCP	UDP	67, 68	Исходящий (запрос на получение адреса от UserGate SIEM на сервер DHCP)	Сервис службы DHCP.
LDAP	TCP	389, 636	Исходящий (к LDAP-коннектору)	Выполнение запросов LDAP (389 — для LDAP и 636 — для LDAP over SSL).
RADIUS	UDP	1812	Исходящий (к серверу аутентификации RADIUS)	Аутентификация пользователей по протоколу RADIUS.
TACACS+	TCP	49	Исходящий (к серверу аутентификации TACACS+)	Аутентификация пользователей по протоколу TACACS+.
FTP (экспорт журналов)	TCP	21	Исходящий (к серверу FTP)	Экспорт журналов на сервер FTP.
SSH (экспорт журналов)	TCP	22	Исходящий (к серверу SSH)	Экспорт журналов на сервер SSH.
Syslog (экспорт журналов)	TCP/UDP	514	Исходящий (к syslog-серверу)	Экспорт журналов на syslog-сервер.

Синтаксис языка запросов

Product: UserGate SIEM
Version: 7.x

В этом приложении приводится справочная информация об SQL-подобном языке запросов UserGate. Вы можете использовать выражения на языке запросов для поиска и фильтрации данных, а также для формирования условий срабатывания правил аналитики.

Для ввода выражений используется строка запросов, которая отображается в следующих разделах веб-консоли UserGate SIEM:

- в разделе **Журналы и отчеты** → **Журналы** [при выборе соответствующего журнала](#) (в режиме **Расширенный**);
- в разделе **Журналы и отчеты** → **Отчеты** → **Пользовательские шаблоны** [при создании пользовательских шаблонов](#);
- в разделе **Аналитика** → **Правила аналитики** [в свойствах условия срабатывания правила аналитики](#);
- в разделе **Аналитика** → **Поиск**;
- в разделе **Аналитика** → **Срабатывания** (в режиме **Расширенный**).
- в разделе **Аналитика** → **Процессы конечных устройств** → **Лог процессов** (в режиме **Расширенный**);
- в разделе **Инциденты** → **Журнал инцидентов** (в режиме **Расширенный**).

При составлении запросов используются доступные параметры, значения этих параметров, а также логические операторы и операторы сравнения.

Структура запроса

Запрос состоит из одного или нескольких условий, каждое из которых имеет вид:

<параметр запроса> <оператор> <значение параметра запроса>

ПримечаниеПри вводе запросов вы можете заключать значения параметров в кавычки. Если значение параметра содержит пробелы, использование кавычек обязательно (например, 'значение 1' или "значение 2"). Для группировки нескольких условий в запросе допускается использовать круглые скобки.

Операторы в запросах

При составлении запросов вы можете использовать логические операторы и операторы сравнения.

Оператор	Значение	Пример запроса	Примечания
Логические операторы			
AND	И (выполняются все условия)	ipSource = 198.51.100.13 AND action = deny	—
OR	Или (выполняется одно из условий)	severity = info OR severity = warning	—
Операторы сравнения			
=	Равно (полностью совпадает)	ipSource = 192.0.2.53	—
!=	Не равно (не совпадает)	ipSource != 192.0.2.55	—
<	Меньше	statusCode < 404	Оператор применим к параметрам, поддерживающим сравнение значений (например, date, portSource, portDest или statusCode)
>	Больше	statusCode > 200	
<=	Меньше либо равно	date <= 2019-03-28T20:59:59	
>=	Больше либо равно	date >= 2019-03-13T21:00:00	
IN	Равно одному из перечисленных в скобках значений	category IN (botnets, compromised, 'illegal software', 'phishing and fraud','reputation high risk','unknown category')	В качестве значений параметров ipSource и ipDest можно указывать адреса подсетей в формате CIDR
NOT IN	Не равно перечисленным в скобках значениям	ipDest NOT IN (203.0.113.0/24)	
~	Содержит подстроку	ipSource ~ 203.0.113	Оператор применим к параметрам, имеющим строковые значения, без учета регистра
!~	Не содержит подстроку	browser !~ Mozilla/5.0	
MATCH	Совпадает с регулярным выражением	details MATCH NAT	Оператор использует синтаксис регулярных выражений библиотеки RE2. Описание библиотеки см. на сайте github.com в разделе компании Google
NOT MATCH	Не совпадает с регулярным выражением	details NOT MATCH NAT	
Прочие операторы			
GROUP BY	Группировка выводимых результатов по указанному параметру	GROUP BY ipSource	Оператор доступен только для запросов в разделе Аналитика → Поиск
LIMIT	Ограничение количества выводимых результатов	LIMIT 100	

Параметры запросов

Вы можете просматривать список всех параметров запросов, доступных в выбранном разделе веб-консоли устройства, используя в строке запроса символ `{ }` (запятая).

Кроме того, для каждого параметра вы можете просматривать список доступных операторов. Для этого после ввода параметра в строке запроса необходимо нажать клавишу Space.

Также вы можете просматривать возможные значения некоторых параметров запросов. Для этого в строке запроса необходимо ввести параметр и оператор, а затем нажать клавишу Space.

Далее приведены параметры запросов и примеры их использования в различных разделах веб-консоли устройства.

Параметры запросов в журналах событий

В таблице ниже приведены параметры запросов, доступные [в журнале событий UserGate SIEM](#), а также в журнале событий подключенных к UserGate SIEM устройств.

Параметр	Значение	Пример запроса
changeTracker	Тип изменений (при учете изменений)	changeTracker = update
component	Компонент устройства	component = vpn
date	Дата события	date = 2025-04-18
dayOfMonth	День месяца (число)	dayOfMonth = 16
dayOfWeek	День недели	dayOfWeek = monday
details	Детали события	details MATCH NAT
event	Тип события	event = 'vpn client connected'
hourOfDay	Час суток	hourOfDay = 12
ipSource	IP-адрес источника	ipSource = 203.0.113.14
module	Модуль устройства	module = 'vpn server'
monthOfYear	Месяц	monthOfYear = march
node	Имя устройства	node = utmcore@nodename
severity	Степень важности события	severity = critical
time	Время события	time > 00:00:00
trackerReason	Причина изменений (при учете изменений)	trackerReason = fix
user	Имя пользователя	user = Admin
userId	ID пользователя	userId = 37333739-3733-3734-3635-366400000000

Параметры запросов в журнале веб-доступа

В таблице ниже приведены параметры запросов, доступные [в журнале веб-доступа](#).

Параметр	Значение	Пример запроса
action	Действие при срабатывании правила	action = 'allow webaccess'
application	Название приложения в системной библиотеке	application = 1 C
applicationCategory	Категория приложения	applicationCategory = Business

Параметр	Значение	Пример запроса
applicationId	ID приложения	applicationId = c93af622-0da7-4133-851d-c0e062772ef3
applicationName	Название приложения	applicationName MATCH Testapp1
applicationTechnology	Технология приложения	applicationTechnology = Client-server
applicationThreat	Уровень опасности приложения	applicationThreat = medium
bytesRecv	Количество полученных байтов	bytesRecv > 1000
bytesSent	Количество переданных байтов	bytesSent > 2000
date	Дата события	date = 2025-04-17
dayOfMonth	День месяца	dayOfMonth = 17
dayOfWeek	День недели	dayOfWeek = thursday
details	Детали события	details MATCH error
domain	Доменное имя ресурса	domain ~ example.com
group	Название группы пользователей	group ~ group1
groupId	ID группы пользователей	groupId = 919878b2-e882-49ed-3331-8ec72c3c79cb
hourOfDay	Час суток	hourOfDay = 14
httpMethod	Метод HTTP-запроса	httpMethod = CONNECT
httpProtocol	Протокол прикладного уровня и его версия	httpProtocol = HTTP/1.1
ipDest	IP-адрес назначения	ipDest = 198.51.100.201
ipSource	IP-адрес источника	ipSource = 198.51.100.206
mime	MIME-тип запроса	mime = text
monthOfYear	Месяц	monthOfYear = march
node	Имя устройства	node = utmcore@nodename
operatingSystem	Тип ОС источника запроса	operatingSystem = Windows
packetsRecv	Количество полученных пакетов	packetsRecv > 1000
packetsSent	Количество переданных пакетов	packetsSent > 2000
portDest	Порт назначения	portDest = 1110
portSource	Порт источника	portSource = 1111
referer	Заголовок Referer в запросе	referer = https://www.example.com
rule	Название правила	rule = Rule1
ruleId	ID правила	ruleId = f93da24d-74f9-4f8c-9e9b-8e6d02346fb4
statusCode	Код HTTP-ответа	statusCode = 302
time	Время события	time > 00:00:00
url	URL-адрес ресурса	url = https://www.example.com
urlCategory	Категория URL	urlCategory = chat
urlCategoryThreat	Уровень опасности категории URL	urlCategoryThreat = medium
user	Имя пользователя	user = Admin
userAgent	User-Agent браузера	userAgent MATCH Mozilla/5.0
userId	ID пользователя	userId = 37333739-3733-3734-3635-366400000000
zoneDest	Зона назначения	zoneDest = Untrusted
zoneSource	Зона источника	zoneSource = Trusted

Параметры запросов в журнале DNS

В таблице ниже приведены параметры запросов, доступные [в журнале DNS](#).

Параметр	Значение	Пример запроса
----------	----------	----------------

actionПараметр	Действие при срабатывании правила	action = 'allow web browser запроса
application	Название приложения в системной библиотеке	application = DNS
applicationCategory	Категория приложения	applicationCategory = 'Web browsing'
applicationId	ID приложения	applicationId = c93af622-0da7-4133-851d-c0e062772ef3
applicationName	Название приложения	applicationName MATCH Testapp1
applicationTechnology	Технология приложения	applicationTechnology = Browser-based
applicationThreat	Уровень опасности приложения	applicationThreat = low
countryDest	Страна назначения	countryDest = 'Russian Federation'
countrySource	Страна источника	countrySource = 'Russian Federation'
date	Дата события	date = 2025-04-17
dayOfMonth	День месяца	dayOfMonth = 17
dayOfWeek	День недели	dayOfWeek = thursday
details	Детали события	details MATCH error
domain	Доменное имя ресурса	domain ~ example.com
group	Название группы пользователей	group ~ group1
groupId	ID группы пользователей	groupId = 919878b2-e882-49ed-3331-8ec72c3c79cb
hourOfDay	Час суток	hourOfDay = 17
ipDest	IP-адрес назначения	ipDest = 192.0.2.11
ipSource	IP-адрес источника	ipSource = 192.0.2.12
monthOfYear	Месяц	monthOfYear = march
networkProtocol	Сетевой протокол	networkProtocol = UDP
node	Имя устройства	node = utmcore@nodename
portDest	Порт назначения	portDest = 1110
portSource	Порт источника	portSource = 1111
rule	Название правила	rule = Rule1
ruleId	ID правила	ruleId = f93da24d-74f9-4f8c-9e9b-8e6d02346fb4
time	Время события	time > 00:00:00
urlCategory	Категория URL	urlCategory = chat
urlCategoryThreat	Уровень опасности категории URL	urlCategoryThreat = low
user	Имя пользователя	user = Admin
userId	ID пользователя	userId = 37333739-3733-3734-3635-366400000000
zoneDest	Зона назначения	zoneDest = Untrusted
zoneSource	Зона источника	zoneSource = Trusted

Параметры запросов в журнале трафика

В таблице ниже приведены параметры запросов, доступные [в журнале трафика](#).

Параметр	Значение	Пример запроса
action	Действие при срабатывании правила	action = allow
application	Название приложения в системной библиотеке	application = 1C
applicationCategory	Категория приложения	applicationCategory = Business
applicationId	ID приложения	applicationId = c93af622-0da7-4133-851d-c0e062772ef3
applicationName	Название приложения	applicationName MATCH Testapp1
applicationProtocol	Протокол приложения	applicationProtocol = HTTP
applicationTechnology	Технология приложения	applicationTechnology = Browser-based

Параметр	Значение	Пример запроса
applicationThreat	Уровень опасности приложения	applicationThreat = low
bytesRecv	Количество полученных байтов	bytesRecv > 1000000
bytesSent	Количество переданных байтов	bytesSent > 100
countryDest	Страна назначения	countryDest = 'Russian Federation'
countrySource	Страна источника	countrySource = 'Russian Federation'
date	Дата события	date = 2025-04-17
dayOfMonth	День месяца	dayOfMonth = 17
dayOfWeek	День недели	dayOfWeek = thursday
group	Название группы пользователей	group ~ group1
groupId	ID группы пользователей	groupId = 919878b2-e882-49ed-3331-8ec72c3c79cb
hourOfDay	Час суток	hourOfDay = 17
ipDest	IP-адрес назначения	ipDest = 192.0.2.10
ipSource	IP-адрес источника	ipSource = 192.0.2.12
macDest	MAC-адрес назначения	macDest = 00:00:5E:00:53:11
macSource	MAC-адрес источника	macSource = 00:00:5E:00:53:2B
monthOfYear	Месяц	monthOfYear = march
natIpDest	IP-адрес назначения после NAT-трансляции	natIpDest = 198.51.100.10
natIpSource	IP-адрес источника после NAT-трансляции	natIpSource = 198.51.100.100
natPortDest	Порт назначения после NAT-трансляции	natPortDest = 1111
natPortSource	Порт источника после NAT-трансляции	natPortSource = 1111
networkProtocol	Сетевой протокол	networkProtocol = ICMP
node	Имя устройства	node = utlcore@nodename
packetsRecv	Количество полученных пакетов	packetsRecv > 1000
packetsSent	Количество переданных пакетов	packetsSent > 100
portDest	Порт назначения	portDest = 1110
portSource	Порт источника	portSource = 1111
rule	Название правила	rule = Rule1
ruleId	ID правила	ruleId = f93da24d-74f9-4f8c-9e9b-8e6d02346fb4
time	Время события	time > 00:00:00
type	Тип правила	type = firewall
user	Имя пользователя	user = Admin
userId	ID пользователя	userId = 37333739-3733-3734-3635-366400000000
zoneDest	Зона назначения	zoneDest = Untrusted
zoneSource	Зона источника	zoneSource = Trusted

Параметры запросов в журнале COB

В таблице ниже приведены параметры запросов, доступные [в журнале COB](#).

Параметр	Значение	Пример запроса
action	Действие при срабатывании правила	action = pass
application	Название приложения в системной библиотеке	application = 1C
applicationCategory	Категория приложения	applicationCategory = Business

Параметр	Значение	Пример запроса
applicationId	ID приложения	applicationId = c93af622-0da7-4133-851d-c0e062772ef3
applicationName	Название приложения	applicationName MATCH Testapp1
applicationProtocol	Протокол прикладного уровня	applicationProtocol = HTTP
applicationTechnology	Технология приложения	applicationTechnology = Client-Server
applicationThreat	Уровень опасности приложения	applicationThreat = high
countryDest	Страна назначения	countryDest = 'Russian Federation'
countrySource	Страна источника	countrySource = 'Russian Federation'
date	Дата события	date = 2025-04-18
dayOfMonth	День месяца	dayOfMonth = 16
dayOfWeek	День недели	dayOfWeek = monday
group	Название группы пользователей	group ~ group1
groupId	ID группы пользователей	groupId = 919878b2-e882-49ed-3331-8ec72c3c79cb
hourOfDay	Час суток	hourOfDay = 14
ipDest	IP-адрес назначения	ipDest = 198.51.100.10
ipSource	IP-адрес источника	ipSource = 192.0.2.12
macDest	MAC-адрес назначения	macDest = 00:00:5E:00:53:11
macSource	MAC-адрес источника	macSource = 00:00:5E:00:53:2B
monthOfYear	Месяц	monthOfYear = march
networkProtocol	Сетевой протокол	networkProtocol = IGMP
node	Имя устройства	node = utlcore@nodename
portDest	Порт назначения	portDest = 1110
portSource	Порт источника	portSource = 1111
rule	Название правила	rule = Rule1
ruleId	ID правила	ruleId = f93da24d-74f9-4f8c-9e9b-8e6d02346fb4
signatureCategory	Категория сигнатуры COB	signatureCategory = exploit
signatureClass	Класс сигнатуры COB	signatureClass = attempted-dos
signatureId	ID сигнатуры COB	signatureId = 999999
signatureName	Название сигнатуры COB	signatureName = 'BlackSun Test'
signatureOS	ОС сигнатуры COB	signatureOS = Linux
signatureThreat	Уровень опасности сигнатуры	signatureThreat = high
time	Время события	time > 00:00:00
user	Имя пользователя	user = Admin
userId	ID пользователя	userId = 37333739-3733-3734-3635-366400000000
zoneDest	Зона назначения	zoneDest = Untrusted
zoneSource	Зона источника	zoneSource = Trusted

Параметры запросов в журнале АСУ ТП

В таблице ниже приведены параметры запросов, доступные [в журнале АСУ ТП](#) (автоматизированных систем управления технологическим процессом).

Параметр	Значение	Пример запроса
action	Действие при срабатывании правила	action = drop
countryDest	Страна назначения	countryDest = 'Russian Federation'
countrySource	Страна источника	countrySource = 'Russian Federation'
date	Дата события	date = 2025-05-26

Параметр	Значение	Пример запроса
dayOfMonth	День месяца	dayOfMonth = 26
dayOfWeek	День недели	dayOfWeek = monday
hourOfDay	Час суток	hourOfDay = 14
ipDest	IP-адрес назначения	ipDest = 198.51.100.2
ipSource	IP-адрес источника	ipSource = 198.51.100.10
monthOfYear	Месяц	monthOfYear = march
node	Имя устройства	node = utmcore@nodename
portDest	Порт назначения	portDest = 1110
portSource	Порт источника	portSource = 1111
rule	Название правила	rule = Rule1
scadaAddress	Адрес регистра АСУ ТП	scadaAddress = 3154
scadaCommand	Код функции АСУ ТП	scadaCommand = 12
scadaProtocol	Протокол прикладного уровня АСУ ТП	scadaProtocol = modbus
scadaSeverity	Уровень опасности события АСУ ТП	scadaSeverity = 1
time	Время события	time > 00:00:00
zoneDest	Зона назначения	zoneDest = Untrusted
zoneSource	Зона источника	zoneSource = Trusted

Параметры запросов в журнале инспектирования SSH

В таблице ниже приведены параметры запросов, доступные [в журнале инспектирования SSH](#).

Параметр	Значение	Пример запроса
action	Действие при срабатывании правила	action = drop
command	Команда SSH	command = whoami
countryDest	Страна назначения	countryDest = 'Russian Federation'
countrySource	Страна источника	countrySource = 'Russian Federation'
date	Дата события	date = 2025-04-17
dayOfMonth	День месяца	dayOfMonth = 17
dayOfWeek	День недели	dayOfWeek = thursday
group	Название группы пользователей	group ~ group1
groupId	ID группы пользователей	groupId = 919878b2-e882-49ed-3331-8ec72c3c79cb
hourOfDay	Час суток	hourOfDay = 17
ipDest	IP-адрес назначения	ipDest = 192.0.2.153
ipSource	IP-адрес источника	ipSource = 192.0.2.195
macSource	MAC-адрес источника	macSource = 00:00:5E:00:53:11
monthOfYear	Месяц	monthOfYear = march
node	Имя устройства	node = utmcore@nodename
portDest	Порт назначения	portDest = 1110
portSource	Порт источника	portSource = 1111
rule	Название правила	rule = Rule1
ruleId	ID правила	ruleId = f93da24d-74f9-4f8c-9e9b-8e6d02346fb4
time	Время события	time > 00:00:00
user	Имя пользователя	user = Admin

Параметр	Значение	Пример запроса
userId	ID пользователя	userId = 37333739-3733-3734-3635-366400000000
zoneDest	Зона назначения	zoneDest = Untrusted
zoneSource	Зона источника	zoneSource = Trusted

Параметры запросов в журнале истории поиска

В таблице ниже приведены параметры запросов, доступные [в журнале истории поиска](#).

Параметр	Значение	Пример запроса
countrySource	Страна источника	countrySource = 'Russian Federation'
date	Дата события	date = 2025-04-17
dayOfMonth	День месяца	dayOfMonth = 17
dayOfWeek	День недели	dayOfWeek = thursday
group	Название группы пользователей	group ~ group1
groupId	ID группы пользователей	groupId = 919878b2-e882-49ed-3331-8ec72c3c79cb
hourOfDay	Час суток	hourOfDay = 17
ipSource	IP-адрес источника	ipSource = 192.0.2.3
monthOfYear	Месяц	monthOfYear = march
node	Имя устройства	node = utmcore@nodename
query	Поисковый запрос	query = 'example search'
searchEngine	Поисковая система	searchEngine = Yandex
time	Время события	time > 00:00:00
user	Имя пользователя	user = Admin
userId	ID пользователя	userId = 37333739-3733-3734-3635-366400000000

Параметры запросов в журнале событий конечных устройств

В таблице ниже приведены параметры запросов, доступные [в журнале событий конечных устройств](#).

Параметр	Значение	Пример запроса
computerName	Имя источника события	computerName = node1
counter	Имя счетчика	counter = login_logout
data	Описание события	data ~ console.example
date	Дата события	date = 2025-04-17
dayOfMonth	День месяца	dayOfMonth = 17
dayOfWeek	День недели	dayOfWeek = thursday
endpoint	Имя конечного устройства	endpoint ~ example.local
endpointId	ID конечного устройства	endpointId = 16535060-5a1a-4e92-8331-239406ec34da
error	Код ошибки при выполнении запроса к сенсору WMI или SNMP	error ~ 0
hourOfDay	Час суток	hourOfDay = 17
insertionString	Данные события Windows после обработки	insertionString MATCH user1
logCategory	Категория события Windows	logCategory = 'Group Membership'
logEventCode	Код события Windows	logEventCode = 4627
logEventId	ID события Windows	logEventId = 4627
logEventSource	Источник события Windows	logEventSource = Microsoft-Windows-Security-Auditing
logEventType	Тип события Windows	logEventType = 4
logFile	Журнал Windows	logFile = Security
logLevel	Уровень важности события Windows	logLevel MATCH Audit

Параметр	Значение	Пример запроса
monthOfYear	Месяц	monthOfYear = march
node	Имя устройства	node = utmcore@nodename
status	Статус выполнения запроса к сенсору WMI или SNMP	status ~ error
taskCategory	Категория задачи Windows	taskCategory = Logon
time	Время события	time > 00:00:00
user	Имя пользователя	user = Admin

Параметры запросов в журнале правил конечных устройств

В таблице ниже приведены параметры запросов, доступные [в журнале правил конечных устройств](#).

Параметр	Значение	Пример запроса
action	Действие при срабатывании правила	action = allow
applicationName	Название приложения	applicationName MATCH Testapp1
date	Дата события	date = 2025-04-17
dayOfMonth	День месяца	dayOfMonth = 17
dayOfWeek	День недели	dayOfWeek = thursday
domain	Доменное имя ресурса	domain ~ example.com
endpoint	Имя конечного устройства	endpoint = desktop-0731nfq
endpointId	ID конечного устройства	endpointId = 35fb5820-74db-4eac-b05b-d01bc284c4e8
hourOfDay	Час суток	hourOfDay = 17
ipDest	IP-адрес назначения	ipDest = 192.0.2.156
ipSource	IP-адрес источника	ipSource = 192.0.2.127
mime	MIME-тип запроса	mime ~ text
monthOfYear	Месяц	monthOfYear = march
networkProtocol	Сетевой протокол	networkProtocol = ICMP
node	Имя устройства	node = utmcore@nodename
portDest	Порт назначения	portDest = 1110
portSource	Порт источника	portSource = 1111
rule	Название правила	rule = Rule1
ruleId	ID правила	ruleId = f93da24d-74f9-4f8c-9e9b-8e6d02346fb4
time	Время события	time > 00:00:00
uriCategory	Категория URL	uriCategory = chat

Параметры запросов в журнале приложений конечных устройств

В таблице ниже приведены параметры запросов, доступные [в журнале приложений конечных устройств](#).

Параметр	Значение	Пример запроса
action	Действие при срабатывании правила	action = start
applicationName	Название приложения	applicationName MATCH Testapp1
cmdLine	Команда запуска приложения	cmdLine ~ sc.exe
date	Дата события	date = 2025-04-17
dayOfMonth	День месяца	dayOfMonth = 17
dayOfWeek	День недели	dayOfWeek = thursday
endpoint	Имя конечного устройства	endpoint = desktop-0731nfq
endpointId	ID конечного устройства	endpointId = 35fb5820-74db-4eac-b05b-d01bc284c4e8
hash	Хеш-сумма приложения	hash = B4CE5C3495FEA0A4FDBAC8ABDCD199F7E4CA8C1F

Параметр	Значение	Пример запроса
hourOfDay	Час суток	hourOfDay = 17
issuer	Издатель сертификата	issuer ~ microsoft
monthOfYear	Месяц	monthOfYear = march
node	Имя устройства	node = utmcore@nodename
parentPid	ID родительского процесса	parentPid > 0
processId	ID процесса	processId = 3916
sessionId	ID пользовательской сессии	sessionId = 1656038456
subject	Владелец сертификата	subject ~ microsoft
time	Время события	time > 00:00:00
version	Версия приложения	version > 6

Параметры запросов в журнале оборудования конечных устройств

В таблице ниже приведены параметры запросов, доступные [в журнале оборудования конечных устройств](#).

Параметр	Значение	Пример запроса
action	Действие при срабатывании правила	action = add_device
date	Дата события	date = 2025-04-17
dayOfMonth	День месяца	dayOfMonth = 17
dayOfWeek	День недели	dayOfWeek = thursday
device	Имя оборудования	device ~ 'USB Hub'
deviceId	ID оборудования	deviceId ~ USB
endpoint	Имя конечного устройства	endpoint = desktop-0731nfq
endpointId	ID конечного устройства	endpointId = 35fb5820-74db-4eac-b05b-d01bc284c4e8
hourOfDay	Час суток	hourOfDay = 17
monthOfYear	Месяц	monthOfYear = march
node	Имя устройства	node = utmcore@nodename
service	Драйвер оборудования	service ~ USBHUB3
time	Время события	time > 00:00:00

Параметры запросов в журнале syslog

В таблице ниже приведены параметры запросов, доступные [в журнале syslog](#).

Параметр	Значение	Пример запроса
applicationName	Название приложения	applicationName = org.gnome.Shell.desktop
computerName	Имя источника события	computerName = node1
data	Описание события	data MATCH Authentication
date	Дата события	date = 2025-04-17
dayOfMonth	День месяца	dayOfMonth = 17
dayOfWeek	День недели	dayOfWeek = thursday
facility	Категория события syslog	facility = authorization
hourOfDay	Час суток	hourOfDay = 17
monthOfYear	Месяц	monthOfYear = march
node	Имя устройства	node = utmcore@nodename
processId	ID процесса	processId = 3036
rule	Название правила	rule = Rule1
ruleId	ID правила	ruleId = f93da24d-74f9-4f8c-9e9b-8e6d02346fb4

Параметр	Значение	Пример запроса
syslogSeverity	Уровень важности события syslog	syslogSeverity = critical
time	Время события	time > 00:00:00

Параметры запросов в журнале защиты почтового трафика

В таблице ниже приведены параметры запросов, доступные [в журнале защиты почтового трафика](#).

Параметр	Значение	Пример запроса
action	Действие при срабатывании правила	action = mark
application	Название приложения в системной библиотеке	application = Gmail
applicationCategory	Категория приложения	applicationCategory = Email
applicationId	ID приложения	applicationId = c93af622-0da7-4133-851d-c0e062772ef3
applicationName	Название приложения	applicationName MATCH Testapp1
applicationTechnology	Технология приложения	applicationTechnology = Browser-based
applicationThreat	Уровень опасности приложения	applicationThreat = high
bytesRecv	Количество полученных байтов	bytesRecv > 1000000
bytesSent	Количество переданных байтов	bytesSent > 1000000
countryDest	Страна назначения	countryDest = 'Russian Federation'
countrySource	Страна источника	countrySource = 'Russian Federation'
date	Дата события	date = 2025-04-17
dayOfMonth	День месяца	dayOfMonth = 17
dayOfWeek	День недели	dayOfWeek = thursday
from	Электронный адрес отправителя	from = sender@example.com
group	Название группы пользователей	group = 111
groupId	ID группы пользователей	groupId = 919878b2-e882-49ed-3331-8ec72c3c79cb
hourOfDay	Час суток	hourOfDay = 17
httpProtocol	Протокол прикладного уровня	httpProtocol = SMTP
ipDest	IP-адрес назначения	ipDest = 192.0.2.10
ipSource	IP-адрес источника	ipSource = 192.0.2.12
monthOfYear	Месяц	monthOfYear = march
node	Имя устройства	node = utlcore@nodename
packetsRecv	Количество полученных пакетов	packetsRecv > 1000
packetsSent	Количество переданных пакетов	packetsSent > 100
portDest	Порт назначения	portDest = 1110
portSource	Порт источника	portSource = 1111
rule	Название правила	rule = Rule1
ruleId	ID правила	ruleId = f93da24d-74f9-4f8c-9e9b-8e6d02346fb4
time	Время события	time > 00:00:00
to	Электронный адрес получателя	to = receiver@example.com
user	Имя пользователя	user = Admin
userId	ID пользователя	userId = 37333739-3733-3734-3635-366400000000
zoneDest	Зона назначения	zoneDest = Untrusted
zoneSource	Зона источника	zoneSource = Trusted

Параметры запросов в журнале событий аутентификации агента UserID

В таблице ниже приведены параметры запросов, доступные [в журнале событий аутентификации агента UserID](#).

Параметр	Значение	Пример запроса
action	Действие пользователя	action = login
date	Дата события	date = 2025-04-17
dayOfMonth	День месяца	dayOfMonth = 17
dayOfWeek	День недели	dayOfWeek = thursday
details	Детали события	details MATCH error
group	Название группы пользователя	group MATCH users
groupId	ID группы пользователя	groupId = 919878b2-e882-49ed-3331-8ec72c3c79cb
hourOfDay	Час суток	hourOfDay = 17
ipSource	IP-адрес источника	ipSource = 192.0.2.111
logSource	Имя источника UserID	logSource = DC01
logSourceId	ID источника UserID	logSourceId = 123e4567-e89b-12d3-a456-426614174000
monthOfYear	Месяц года	monthOfYear = march
node	Имя устройства	node = utmcore@nodename
time	Время события	time > 00:00:00
user	Имя пользователя	user = Admin
userId	ID пользователя	userId = 745591c3-9d21-092d-8db4-5b9b0000044f

Параметры запросов в журнале RADIUS-сервера агента UserID

В таблице ниже приведены параметры запросов, доступные [в журнале RADIUS-сервера агента UserID](#).

Параметр	Значение	Пример запроса
date	Дата события	date = 2025-04-17
event	Статус пользователя	event = start
ipSource	IP-адрес источника	ipSource = 192.0.2.12
node	Имя устройства	node = utmcore@nodename
rule	Название правила	rule = Rule1
ruleId	ID правила	ruleId = f93da24d-74f9-4f8c-9e9b-8e6d02346fb4
time	Время события	time > 00:00:00
user	Имя пользователя	user = Admin

Параметры запросов в разделе «Аналитика»

В таблице ниже приведены параметры запросов, доступные в разделе **Аналитика** [при поиске событий](#), на вкладке **Поиск**, а также [при формировании условий срабатывания правил аналитики](#).

Возможность использования того или иного параметра зависит от журнала, из которого получено событие.

Параметр	Значение	Журнал	Пример запроса
action	Действие при срабатывании правила	Событий, веб-доступа, DNS, трафика, COB, ACY ТП, инспектирования SSH, правил конечных устройств, приложений конечных устройств, оборудования конечных устройств, защиты почтового трафика, аутентификации UserID-агента	action = deny
application	Название приложения в системной библиотеке	Веб-доступа, DNS, трафика, COB, защиты почтового трафика	application = DNS
applicationCategory	Категория приложения	Веб-доступа, DNS, трафика, COB, защиты почтового трафика	applicationCategory = Email
applicationId	ID приложения	Веб-доступа, DNS, трафика, COB, защиты почтового трафика	applicationId = c93af622-0da7-4133-851d-c0e062772ef3
applicationName	Название приложения	Веб-доступа, DNS, трафика, COB, правил конечных устройств, приложений конечных устройств, защиты почтового трафика	applicationName MATCH Testapp1
applicationTechnology	Технология приложения	Веб-доступа, DNS, трафика, COB, защиты почтового трафика	applicationTechnology = Browser-based
applicationThreat	Уровень опасности приложения	Веб-доступа, DNS, трафика, COB, защиты почтового трафика	applicationThreat = high
bytesRecv	Количество полученных байтов	Веб-доступа, трафика, защиты почтового трафика	bytesRecv > 1000
bytesSent	Количество отправленных байтов	Веб-доступа, трафика, защиты почтового трафика	bytesSent > 2000
changeTracker	Тип изменений	Событий	changeTracker = update

Параметр	Значение	Журнал	Пример запроса
cmdLine	Команда запуска приложения	Приложений конечных устройств	cmdLine ~ sc.exe
component	Компонент устройства	Событий	component = vpn
computerName	Имя источника события	Событий конечных устройств, syslog	computerName = node1
counter	Имя счетчика	Событий конечных устройств	counter = login_logout
countryDest	Страна назначения	DNS, трафика, COB, ACY ТП, инспектирования SSH, защиты почтового трафика	countryDest = 'Russian Federation'
countrySource	Страна источника	DNS, трафика, COB, ACY ТП, инспектирования SSH, истории поиска, защиты почтового трафика	countryDest = 'Russian Federation'
data	Описание события	Событий конечных устройств, syslog	data ~ powershell
date	Дата события	Все	date = 2025-04-17
dayOfMonth	День месяца	Все	dayOfMonth = 17
dayOfWeek	День недели	Все	dayOfWeek = thursday
details	Детали события	Событий, веб-доступа, DNS, аутентификации UserID-агента	details MATCH error
device	Имя оборудования	Оборудования конечных устройств	device ~ 'USB Hub'
deviceId	ID оборудования	Оборудования конечных устройств	deviceId ~ USB
domain	Доменное имя ресурса	Веб-доступа, DNS, правил конечных устройств	domain ~ example.com
error	Код ошибки при выполнении запроса к сенсору WMI или SNMP	Событий конечных устройств	error ~ 0
event	Тип события	Событий, RADIUS-сервера агента UserID	event = 'vpn client connected'
facility	Категория события syslog	Syslog	facility = authorization
from	Электронный адрес отправителя	Защиты почтового трафика	from = sender@example.com
group	Название группы пользователей	Веб-доступа, DNS, трафика, COB, инспектирования SSH, истории поиска, защиты почтового трафика, аутентификации UserID-агента	group ~ users
groupId	ID группы пользователей	Веб-доступа, DNS, трафика, COB, инспектирования SSH, истории поиска, защиты почтового трафика, аутентификации UserID-агента	groupId = 919878b2-e882-49ed-3331-8ec72c3c79cb
hash	Хеш-сумма приложения	Приложений конечных устройств	hash = B4CE5C3495FEA0A4FDBAC8ABDCD199F7E4CA8C1F
hourOfDay	Час суток	Все	hourOfDay = 17
httpMethod	Метод HTTP-запроса	Веб-доступа	httpMethod = CONNECT
httpProtocol	Протокол прикладного уровня и его версия	Веб-доступа, защиты почтового трафика	httpProtocol = HTTP/1.1
image	Путь к исполняемому файлу процесса в ОС Windows	Событий конечных устройств	image ~ cmd.exe
imageLoaded	Путь к загруженному модулю процесса в ОС Windows	Событий конечных устройств	imageLoaded = C:\\Windows\\System32\\kernel32.dll
insertionString	Данные события Windows после обработки	Событий конечных устройств	insertionString MATCH services.exe
ipDest	IP-адрес назначения	Веб-доступа, DNS, трафика, COB, ACY ТП, инспектирования SSH, правил конечных устройств, защиты почтового трафика	ipDest = 203.0.113.10
ipSource	IP-адрес источника	Событий, веб-доступа, DNS, трафика, COB, ACY ТП, инспектирования SSH, истории поиска, правил конечных устройств, защиты почтового трафика, аутентификации UserID-агента, RADIUS-сервера агента UserID	ipSource = 192.0.2.12
logCategory	Категория события Windows	Событий конечных устройств	logCategory = 'Group Membership'
logEventCode	Код события Windows	Событий конечных устройств	logEventCode = 4625
logEventId	ID события Windows	Событий конечных устройств	logEventId = 4624
logEventSource	Служба Windows, зарегистрировавшая событие	Событий конечных устройств	logEventSource = Microsoft-Windows-Security-Auditing
logEventType	Тип события Windows	Событий конечных устройств	logEventType = 4
logFile	Журнал Windows	Событий конечных устройств	logFile = Security
logLevel	Уровень важности события Windows	Событий конечных устройств	logLevel = Error
logonId	Идентификатор входа в ОС Windows	Событий конечных устройств	logonId ~ 0x3E7
macDest	MAC-адрес назначения	Трафика, COB	macDest = 00:00:5E:00:53:11

Параметр	Значение	Журнал	Пример запроса
macSource	MAC-адрес источника	Трафика, COB, инспектирования SSH	macSource = 00:00:5E:00:53:2B
mime	MIME-тип запроса	Веб-доступа	mime = text/html
module	Модуль устройства	Событий	module = 'vpn server'
monthOfYear	Месяц	Все	monthOfYear = march
natIpDest	IP-адрес назначения после NAT-трансляции	Трафика	natIpDest = 198.51.100.1
natIpSource	IP-адрес источника после NAT-трансляции	Трафика	natIpSource = 198.51.100.100
natPortDest	Порт назначения после NAT-трансляции	Трафика	natPortDest = 1110
natPortSource	Порт источника после NAT-трансляции	Трафика	natPortSource = 1111
networkProtocol	Сетевой протокол	DNS, трафика, COB, правил конечных устройств	networkProtocol = TCP
node	Имя устройства	Все	node = utmcore@nodename
operatingSystem	Тип ОС источника запроса	Веб-доступа, COB	operatingSystem = Windows
originalFilename	Исходное имя файла в ОС Windows	Событий конечных устройств	originalFilename = malware.exe
packetsRecv	Количество полученных пакетов	Веб-доступа, трафика, защиты почтового трафика	packetsRecv > 1000
packetsSent	Количество отправленных пакетов	Веб-доступа, трафика, защиты почтового трафика	packetsSent > 100
parentCommandLine	Команда запуска родительского процесса в ОС Windows	Событий конечных устройств	parentCommandLine ~ cmd.exe
parentImage	Путь к исполняемому файлу родительского процесса в ОС Windows	Событий конечных устройств	parentImage = C:\\Windows\\System32\\cmd.exe
parentPid	ID родительского процесса в ОС Windows	Событий конечных устройств	parentPid = 1234
portDest	Порт назначения	Веб-доступа, DNS, трафика, COB, АСУ ТП, инспектирования SSH, правил конечных устройств, защиты почтового трафика	portDest = 1110
portSource	Порт источника	Веб-доступа, DNS, трафика, COB, АСУ ТП, инспектирования SSH, правил конечных устройств, защиты почтового трафика	portSource = 1111
processId	ID процесса	Приложений конечных устройств, syslog	processId = 3036
queryName	Имя DNS-запроса	Событий конечных устройств	queryName ~ example.com
queryResult	Результат DNS-запроса	Событий конечных устройств	queryResult = 192.0.2.1
referer	Заголовок Referer в запросе	Веб-доступа	referer = https://www.example.com
rule	Название правила	Веб-доступа, DNS, трафика, COB, АСУ ТП, инспектирования SSH, правил конечных устройств, syslog, защиты почтового трафика, RADIUS-сервера агента UserID	rule = Rule1
ruleId	ID правила	Веб-доступа, DNS, трафика, COB, инспектирования SSH, правил конечных устройств, syslog, защиты почтового трафика, RADIUS-сервера агента UserID	ruleId = f93da24d-74f9-4f8c-9e9b-8e6d02346fb4
ruleType	Тип правила	Событий	ruleType = nat
scadaAddress	Адрес регистра АСУ ТП	АСУ ТП	scadaAddress = 3154
scadaCommand	Код функции АСУ ТП	АСУ ТП	scadaCommand = 12
scadaProtocol	Протокол прикладного уровня АСУ ТП	АСУ ТП	scadaProtocol = modbus
scriptBlockText	Текст выполненного скрипта PowerShell	Событий конечных устройств	scriptBlockText ~ DownloadFile
sensor	Имя сенсора	Событий конечных устройств	sensor = DESKTOP-NAME
sensorId	ID сенсора	Событий конечных устройств	sensorId = 12345
service	Драйвер оборудования	Оборудования конечных устройств	service ~ USBHUB3
session	Идентификатор сессии запуска правила аналитики (GUID)	Срабатываний	session = 550e8400-e29b-41d4-a716-446655440000
sessionId	ID пользовательской сессии	Приложений конечных устройств	sessionId > 1
severity	Степень важности события	Событий	severity = critical
signatureCategory	Категория сигнатуры COB	COB	signatureCategory = exploit
signatureClass	Класс сигнатуры COB	COB	signatureClass = attempted-dos

Параметр	Значение	Журнал	Пример запроса
signatureId	ID сигнатуры COB	COB	signatureId = 999999
signatureName	Название сигнатуры COB	COB	signatureName = Example
signatureOS	OC сигнатуры COB	COB	signatureOS = Linux
signatureThreat	Уровень опасности сигнатуры	COB	signatureThreat = high
snmpData	Данные SNMP	Событий конечных устройств	snmpData = 0
snmpObject	Идентификатор SNMP-объекта (SNMP OID)	Событий конечных устройств	snmpObject = 1.3.6.1.2.1.1.3.0
snmpObjectType	Тип SNMP-объекта	Событий конечных устройств	snmpObjectType = counter
source	Журнал, из которого получено событие	Все	source = mailsecurity
sourceImage	Путь к исполняемому файлу	Событий конечных устройств	sourceImage = C:\\Windows\\System32\\cmd.exe
status	Статус выполнения запроса к сенсору WMI или SNMP	Событий конечных устройств	status ~ error
statusCode	Код HTTP-ответа	Веб-доступа	statusCode = 302
syslogSeverity	Уровень важности события syslog	syslog	syslogSeverity = critical
targetFilename	Имя целевого файла	Событий конечных устройств	targetFilename ~ malware.exe
targetImage	Путь к целевому исполняемому файлу	Событий конечных устройств	targetImage = C:\\Users\\Admin\\Desktop\\malware.exe
targetObject	Целевой объект	Событий конечных устройств	targetObject ~ Run
taskCategory	Категория задачи Windows	Событий конечных устройств	taskCategory = 'User Account Management'
time	Время события	Все	time > 00:00:00
to	Электронный адрес получателя	Защиты почтового трафика	to = receiver@example.com
triggeredAlert	Идентификатор срабатывания правила	Срабатываний	triggeredAlert = AVL-11638
triggeredAlertFirstEventDate	Дата и время первого срабатывания правила	Срабатываний	triggeredAlertFirstEventDate >= 2026-06-29
triggeredAlertLastEventDate	Дата и время последнего срабатывания правила	Срабатываний	triggeredAlertLastEventDate >= 2026-06-29T00:00:00
url	URL-адрес ресурса	Веб-доступа	url = https://www.example.com
urlCategory	Категория URL	Веб-доступа, DNS, правил конечных устройств	urlCategory = chat
urlCategoryThreat	Уровень опасности категории URL	Веб-доступа, DNS	urlCategoryThreat = medium
user	Имя пользователя	Событий, веб-доступа, DNS, трафика, COB, инспектирования SSH, истории поиска, защиты почтового трафика, аутентификации UserID-агента, RADIUS-сервера агента UserID	user = Admin
userAgent	User-Agent браузера	Веб-доступа	userAgent MATCH Mozilla
userId	ID пользователя	Событий, веб-доступа, DNS, трафика, COB, инспектирования SSH, истории поиска, защиты почтового трафика, аутентификации UserID-агента	userId = 37333739-3733-3734-3635-366400000000
workstationName	Имя рабочей станции	Событий конечных устройств, аутентификации UserID-агента	workstationName ~ 'DESKTOP'
zoneDest	Зона назначения	Веб-доступа, DNS, трафика, COB, АСУ ТП, инспектирования SSH, защиты почтового трафика	zoneDest = Untrusted
zoneSource	Зона источника	Веб-доступа, DNS, трафика, COB, АСУ ТП, инспектирования SSH, защиты почтового трафика	zoneSource = Trusted

Параметры запросов в журнале срабатываний правил аналитики

В таблице ниже приведены параметры запросов, доступные [в журнале срабатываний правил аналитики](#). Журнал отображается в разделе **Аналитика → Срабатывания**.

Параметр	Значение	Пример запроса
countryDest	Страна назначения	countryDest = 'Russian Federation'
countrySource	Страна источника	countrySource = 'Russian Federation'
date	Дата события	date = 2025-04-18
dayOfMonth	День месяца	dayOfMonth = 16
dayOfWeek	День недели	dayOfWeek = monday
group	Название группы пользователей	group ~ group1

Параметр	Значение	Пример запроса
groupId	ID группы пользователей	groupId = 919878b2-e882-49ed-3331-8ec72c3c79cb
hourOfDay	Час суток	hourOfDay = 14
ipDest	IP-адрес назначения	ipDest = 198.51.100.10
ipSource	IP-адрес источника	ipSource = 192.0.2.12
monthOfYear	Месяц	monthOfYear = march
node	Имя устройства	node = utmcore@nodename
portDest	Порт назначения	portDest = 1110
portSource	Порт источника	portSource = 1111
rule	Название правила	rule = Rule1
ruleId	ID правила	ruleId = f93da24d-74f9-4f8c-9e9b-8e6d02346fb4
signatureCategory	Категория сигнатуры COB	signatureCategory = exploit
signatureClass	Класс сигнатуры COB	signatureClass = attempted-dos
signatureId	ID сигнатуры COB	signatureId = 999999
signatureName	Название сигнатуры COB	signatureName = 'BlackSun Test'
signatureOS	ОС сигнатуры COB	signatureOS = Linux
threat	Уровень опасности срабатывания	threat = 5
time	Время события	time > 00:00:00
triggeredAlert	Идентификатор срабатывания правила	triggeredAlert = AVL-11638
triggeredAlertCategory	Категория срабатывания	triggeredAlertCategory = Security
triggeredAlertCategoryId	ID категории срабатывания	triggeredAlertCategoryId = 1
triggeredAlertFirstEventDate	Дата и время первого срабатывания правила	triggeredAlertFirstEventDate >= 2026-06-29
triggeredAlertLastEventDate	Дата и время последнего срабатывания правила	triggeredAlertLastEventDate >= 2026-06-29T00:00:00
user	Имя пользователя	user = Admin
userId	ID пользователя	userId = 37333739-3733-3734-3635-366400000000
zoneSource	Зона источника	zoneSource = Trusted
zoneDest	Зона назначения	zoneDest = Untrusted

Параметры запросов в журнале процессов конечных устройств

Параметры запросов, доступные [в журнале процессов конечных устройств](#), совпадают с параметрами запросов журнала приложений конечных устройств. Журнал процессов конечных устройств отображается в разделе **Аналитика** → **Процессы конечных устройств** → **Лог процессов**.

Параметры запросов в журнале инцидентов

В таблице ниже приведены параметры запросов, доступные [в журнале инцидентов](#), зарегистрированных по срабатыванию правил аналитики. Журнал отображается в разделе **Инциденты** → **Журнал инцидентов**.

Параметр	Значение	Пример запроса
alerts	Количество срабатываний, связанных с инцидентом	alerts = 5
alertsID	ID срабатываний, связанных с инцидентом	alertsID = AVL-130
assignee	Имя пользователя, ответственного за расследование инцидента	assignee = admin
assigneeId	ID пользователя, ответственного за расследование инцидента	assigneeId = 37333739-3733-3734-3635-366400000000
date	Дата регистрации инцидента	date >= 2025-04-17
incidentId	ID инцидента	incidentId = 1
incidentName	Название инцидента	incidentName = 'BruteForce Attack'
incidentPrefix	Индекс инцидента	incidentPrefix = INC-1
lastChangeBy	Имя пользователя, внесшего последние изменения в инцидент	lastChangeBy = admin
lastChangeById	ID пользователя, внесшего последние изменения в инцидент	lastChangeById = 37333739-3733-3734-3635-366400000000

Параметр	Значение	Пример запроса
priority	Уровень важности инцидента	priority = critical
reporter	Имя пользователя, зарегистрировавшего инцидент	reporter = admin
reporterId	ID пользователя, зарегистрировавшего инцидент	reporterId = 37333739-3733-3734-3635-366400000000
resolution	Решение по инциденту (при закрытии)	resolution = Resolved
resolutionId	ID решения по инциденту	resolutionId = 1
rule	Название правила аналитики, по которому создан инцидент	rule = BruteForce_Detection
ruleId	ID правила аналитики	ruleId = f93da24d-74f9-4f8c-9e9b-8e6d02346fb4
schema	Схема расследования инцидента	schema = Incident
schemald	ID схемы расследования инцидента	schemald = 1
status	Статус расследования инцидента	status = Opened
statusId	ID статуса расследования инцидента	statusId = 28202bc1-ca44-47d7-918f-f5e6296c0498
type	Тип инцидента	type = Task
typeId	ID типа инцидента	typeId = c14a175f-6513-4545-9b8a-a6beb17a6b67
updateDate	Дата последнего обновления инцидента	updateDate >= 2025-04-17
watchers	Количество наблюдателей за расследованием инцидента	watchers = 2
watchersId	ID пользователей-наблюдателей	watchersId = 37333739-3733-3734-3635-366400000000

Примеры запросов для поиска и фильтрации данных

В таблице ниже приведены примеры выражений на языке запросов UserGate SIEM для поиска и фильтрации событий по заданным критериям.

Критерий	Пример запроса	Результат
Дата и время событий	date >= 2025-04-17 AND time > 12:00:00 AND time < 18:00:00	Записи о событиях, зарегистрированных 17 апреля 2025 года в период с 12:00 до 18:00
Заблокированный трафик	action = deny AND ipSource = 192.0.2.100	Записи о трафике, заблокированном для источника с IP-адресом 192.0.2.100
Код HTTP-ответа	statusCode >= 400 AND statusCode < 500	Записи о событиях веб-доступа с кодами HTTP-ответа, указывающими на ошибки клиента или сервера
Неудачные попытки авторизации администраторов	event = 'administrator login failed'	Записи о неудачных попытках авторизации администраторов
Совпадение с подстрокой	data ~ powershell	Записи о событиях, в теле которых содержится подстрока powershell
IP-адрес с использованием подсети	ipSource IN (192.0.2.0/24, 198.51.100.0/24)	Записи о событиях, в которых IP-адрес источника принадлежит одной из указанных подсетей
Комбинация нескольких условий	(action = deny OR action = drop) AND ipSource = 203.0.113.10	Записи о заблокированном или отброшенном трафике от источника с IP-адресом 203.0.113.10

