Table of Contents

Table of Contents 1
Журналы 2
- Описание 3
- Журнал событий 4
- Журнал веб-доступа 5
- Журнал DNS 6
- Журнал трафика 7
- История поиска 8
- UserID-агент 9
- Поиск и фильтрация данных 12
- Экспорт журналов 14
- Описание форматов журналов 17

Журналы

Описание

Version: 7.5.x
Product: SWG

UserGate SWG регистрирует события, возникающие в процессе его функционирования, и сохраняет их в следующих журналах:

- **Журнал событий** — содержит события, связанные с изменением параметров UserGate SWG, авторизацией пользователей, обновлениями различных списков и т. п.
- **Журнал веб-доступа** — подробный журнал всех веб-запросов, обработанных UserGate SWG.
- **Журнал DNS** — содержит события, связанные с DNS-трафиком.
- **Журнал трафика** — подробный журнал срабатывания правил межсетевого экрана, NAT, DNAT, правил подмены портов и правил маршрутизации на основе политик (PBR). Для регистрации этих событий необходимо включить функцию журналирования в соответствующих правилах.
- **История поиска** — содержит сведения о поисковых запросах пользователей в популярных поисковых системах.
- **Агент UserID** — содержит описание событий, отражающих результат работы UserID-агента.

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 отображаются в журнале событий. В случае, если узел интегрирован с UserGate Log Analyzer, записи будут отображаться в журнале событий UserGate Log Analyzer. Ротация записей журнала событий никогда не производится.

Журнал событий

Version: 7.5.x

Product: SWG

Журнал событий отображает события, связанные с изменением настроек UserGate SWG, например, добавление/удаление/изменение данных учетной записи, правила или любого другого элемента. Здесь же отображаются все события входа в веб-консоль, авторизации пользователей через Captive-портал, старта, выключения, перезагрузки сервера и т. п.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например по диапазону дат, компоненту, важности, типу события.

Вы можете выбрать для отображения только те столбцы, которые вам необходимы. Для этого нажмите указателем мыши на любом из столбцов, и в появившемся контекстном меню оставьте галочки только для тех столбцов, которые необходимо отображать.

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

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

Журнал веб-доступа

Version: 7.5.x
Product: SWG

Журнал веб-доступа отображает все запросы пользователей в интернет по протоколам HTTP и HTTPS. Выводятся события срабатывания правил фильтрации контента, инспектирования SSL, Веб-безопасности, Captive-портала в настройках которых включено журналирование. Отображается следующая информация:

- Узел, на котором произошло событие.
- Время события.
- Содержание события.
- Пользователь.
- Действие.
- Правило.
- Причины (при блокировке сайта).
- URL назначения.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.
- Категории сайтов.
- Приложение.
- Протокол прикладного уровня.
- HTTP метод.
- Код ответа HTTP.
- Тип контента (если присутствует).
- Информация.
- Байт отправлено/получено.
- Пакетов отправлено/получено.
- Реферер (при наличии).
- Операционная система.
- User agent браузера.

ПримечаниеВ столбцах трафика (Байт отправлено/получено, Пакетов отправлено/получено) указывается трафик после срабатывания всех правил на этом запросе.
Если правила требуют анализа ответа от веб-сервера, то трафик ответа также будет подсчитан и учтён одинаковый, в том числе у первого сработавшего на этом запросе правила (bypass captive, decrypt). Таким образом, учитывается весь прошедший трафик и указывается одно и то же значение каждому правилу, сработавшему на этом запросе.
Если анализ ответа от веб-сервера для правил не требуется, то весь остальной трафик не учитывается.

Вы можете выбрать только те столбцы для показа, которые вам необходимы. Для этого нажмите указателем мыши на любом из столбцов, и в появившемся контекстном меню оставьте 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** выр можете скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

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

Журнал DNS

Version: 7.5.x
Product: SWG

Журнал DNS отображает события, связанные с DNS трафиком. Для журналирования событий DNS на UserGate SWG 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.

Вы можете выбрать только те столбцы для показа, которые вам необходимы. Для этого нажмите указателем мыши на любом из столбцов, и в появившемся контекстном меню оставьте 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** вы можете скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

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

Журнал трафика

Version: 7.5.x
Product: SWG

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

- Узел, на котором произошло событие.
- Время события.
- Содержание события.
- Пользователь.
- Действие.
- Правило.
- Приложение.
- Сетевой протокол.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- MAC-адрес источника
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.
- MAC-адрес назначения.
- NAT IP-адрес источника (если это правило NAT).
- NAT порт источника (если это правило NAT).
- NAT IP-адрес назначения (если это правило NAT).
- NAT порт назначения (если это правило NAT).
- Байт отправлено/получено.
- Пакетов отправлено/получено.

ПримечаниеВ столбцах трафика (Байт отправлено/получено, Пакетов отправлено/получено) указывается трафик, учтенный в момент срабатывания журналирующего правила.
Если в настройках журналирования в правиле выбрано: "Журналировать каждый пакет", то значения учтенного трафика в журнале будут кумулятивно нарастать в течение сессии.
Если в настройках журналирования в правиле выбрано: "Журналировать начало сессии", будет учтен всего один или несколько пакетов, необходимых для срабатывания этого правила.

Вы можете выбрать только те столбцы для показа, которые вам необходимы. Для этого нажмите указателем мыши на любом из столбцов, и в появившемся контекстном меню оставьте 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** вы можете скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

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

История поиска

Version: 7.5.x

Product: SWG

В разделе **История поиска** отображаются все поисковые запросы пользователей, для которых настроено журналирование в политиках веб-безопасности.

Вы можете выбрать только те столбцы для показа, которые вам необходимы. Для этого нажмите указателем мыши на любом из столбцов, и в появившемся контекстном меню оставьте 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** вы можете скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

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

Technology: Identification and Authentication
Version: 7.5.x
Product: SWG

Журнал Windows Active Directory

Журнал Windows Active Directory отображает события, собранные UserID-агентом с помощью коннектора «Microsoft Active Directory» с серверов AD. В журнале отображаются события с успешным входом в систему (идентификатор события 4624), события Kerberos (события с номерами: 4768, 4769, 4770) и события членства в группах (идентификатор события 4627).

Параметр	Описание
Узел	Узел UserGate, которым зафиксировано событие
Время	Время произошедшего события
Запись журнала событий конечных устройств	Ссылка на событие
Конечное устройство\сенсор	Коннектор UserID
Уровень лога	Поле «Keywords» из журнала AD
Данные	Содержание события из журнала AD
Источник журнала событий	Поле «Источник» из журнала AD
Категория журнала	Код категории инцидента (12554 Group Membership, 12544 Logon, 14337 Kerberos Service Ticket Operations и т. д)
Категория инцидента	Поле «Тип задачи» из журнала AD
Имя компьютера	Узел Windows, на котором произошло событие
Пользователь	Поле «Пользователь» из журнала AD
Код события лога	Поле «Код события» из журнала AD (EventCode)
Идентификатор события лога	Поле «Идентификатор события» из журнала AD (EventID)
Тип события лога	Тип событий журнала Windows (Система\Безопасность\Приложение и т. д.)
Файл журнала лога	файл журнала Windows

Syslog (Журнал)

Журнал syslog отображает события, собранные UserID-агентом с помощью коннектора «Отправитель syslog» с серверов-источников данных syslog. В журнале отображаются события входа пользователей в систему и завершения сеанса работы.

Параметр	Описание
Узел	Узел UserGate, на котором зафиксировано событие
Время	Время произошедшего события

Параметр	Описание
Запись журнала syslog	Ссылка на событие
Правило	Правило, под которое попало syslog-сообщение
Критичность	Уровень критичности события syslog
Объект	Тип процесса, вызвавшего сообщение (kernel messages,user-level messages,security/authentication и т. д)
Имя компьютера	Имя компьютера, на котором произошло событие
Приложение	Приложение, вызвавшее событие
Идентификатор процесса	PID процесса, вызвавшего событие
Данные	Описание события

UserID (Журнал)

Журнал UserID содержит описания событий, отражающие результат работы UserID-агента.

Параметр	Описание
Узел	Узел UserGate, на котором зафиксировано событие
Время	Время произошедшего события
Содержание события	Открыть подробное описание события
Действие	Действие, примененное к событию
Источник логов	Источник полученного события
Пользователь	Пользователь, который вызвал событие
IP-адрес	IP-адрес узла, на котором произошло событие
Информация	Описание события

RADIUS (Журнал)

Журнал RADIUS отображает события, собранные UserID-агентом с помощью коннектора «RADIUS» из данных RADIUS accounting. В журнале отображаются события входа пользователей в систему и завершения сеанса работы.

Параметр	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

Параметр	Описание
Группы	Строка групп, в которых состоит пользователь
Статус	Статус пользователя
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)

Поиск и фильтрация данных

Version: 7.5.x
Product: SWG

Объем данных, регистрируемых в журналах, как правило, значителен, поэтому в стандартном режиме просмотра отображается лишь часть доступных полей. Для быстрого доступа к необходимой информации в UserGate SWG предусмотрены средства поиска и фильтрации журналов. Поиск может выполняться как в простом, так и в расширенном режиме.

В режиме простого поиска фильтрация записей осуществляется с помощью графического интерфейса. Настройка условий поиска выполняется в удобной форме и не требует знания специальных команд или синтаксиса.

Для создания более сложных условий отбора предназначен режим расширенного поиска, использующий специализированный язык запросов. В этом режиме доступны поля журналов, которые не отображаются и не могут использоваться в стандартном режиме поиска. Запросы формируются с использованием имен полей, их значений, ключевых слов и логических операторов. Значения, содержащие пробелы, необходимо заключать в одинарные (' ') или двойные (" ") кавычки. Для значений без пробелов кавычки не требуются. Для объединения и группировки нескольких условий в запросе можно использовать круглые скобки.

Ключевые слова отделяются пробелами и могут быть следующими:

Ключевые поля	**Значение**
AND или and	Логическое «И», требует выполнение всех условий, заданных в запросе
OR или or	Логическое «ИЛИ», требует выполнение одного из условий запроса

Операторы определяют условия фильтра и могут быть следующими:

Оператор	**Значение**
=	Равно — требует полного совпадения значения поля с указанным значением. Пример: ip = 172.16.31.1 . Будут отображены все записи журнала, в которых поле ip будет точно соответствовать значению 172.16.31.1
!=	Не равно — значение поля не должно совпадать с указанным значением. Пример: ip != 172.16.31 . Будут отображены все записи журнала, в которых поле ip не будет равно значению 172.16.31.1
<=	Меньше либо равно — значение поля должно быть меньше или равно указанному в запросе значению. Оператор применим для полей, поддерживающих сравнение. Например, поля даты, portSource, portDest, statusCode и т. п. Пример: date <= '2019-03-28T20:59:59' AND statusCode = 303
>=	Больше либо равно — значение поля должно быть больше или равно указанному в запросе значению. Оператор применим для полей, поддерживающих сравнение. Например, поля даты, portSource, portDest, statusCode и т. п. Пример: date >= "2019-03-13T21:00:00" AND statusCode = 200
<	Меньше — значение поля должно быть меньше указанного в запросе значения. Оператор применим для полей, поддерживающих сравнение. Например, поля даты, portSource, portDest, statusCode и т. п. Пример: date < '2019-03-28T20:59:59' AND statusCode = 404
>	Больше — значение поля должно быть больше указанного в запросе значения. Оператор применим для полей, поддерживающих сравнение. Например, поля даты, portSource, portDest, statusCode и т. п. Пример: (statusCode > 200 AND statusCode < 300) OR (statusCode = 404)
IN	Позволяет указать в запросе несколько значений поля. Список значений необходимо заключать в круглые скобки. Пример: category IN (botnets, compromised, 'illegal software', 'phishing and fraud',' reputation high risk', 'unknown category')

Оператор	Значение
NOT IN	Позволяет указать в запросе несколько значений поля. Будут отображены записи, в которых значение поля не совпадает ни с одним из указанных. Список значений необходимо заключать в круглые скобки. Пример: category NOT IN (botnets, compromised, 'illegal software', 'phishing and fraud', 'reputation high risk', 'unknown category')
~	Содержит — позволяет указать подстроку, которая должна присутствовать в значении выбранного поля. Поиск выполняется без учета регистра. Пример: browser ~ "Mozilla/5.0". Оператор применяется только к полям, содержащим строковые значения
!~	Не содержит — позволяет указать подстроку, которая не должна присутствовать в значении выбранного поля. Поиск выполняется без учета регистра. Пример: browser !~ "Mozilla/5.0". Оператор применяется только к полям, содержащим строковые значения
MATCH	Поиск по полю с помощью регулярного выражения. Будут показаны только те записи, в которых значение поля соответствует заданному шаблону. Пример: details MATCH NAT — будут отфильтрованы все записи журнала, в которых в проверяемом поле details найдется слово «NAT»
NOT MATCH	Поиск записей, в которых значение поля не совпадает с заданным регулярным выражением. Будут показаны только те записи, в которых значение поля не соответствует заданному шаблону. Пример: details NOT MATCH NAT — будут отфильтрованы все записи журнала, в которых в проверяемом поле details не найдется слово «NAT»

При формировании запроса в режиме расширенного поиска UserGate SWG предлагает варианты названий полей, допустимых операторов и возможных значений. Это упрощает создание сложных поисковых выражений и снижает вероятность ошибок при вводе. Набор доступных полей и перечень допустимых значений зависят от типа просматриваемого журнала.

При переходе из режима простого поиска в режим расширенного поиска UserGate SWG автоматически преобразует заданные параметры фильтрации в строку запроса, соответствующую условиям, указанным в базовом режиме. Вы можете продолжить формирование строки поиска с использованием расширенных возможностей языка запросов без необходимости повторного ввода критериев отбора.

Экспорт журналов

Version: 7.5.x
Product: SWG
Documentation:

С помощью функции экспорта журналов вы можете выгружать информацию о работе системы на внешние серверы для последующего анализа или для обработки в системах SIEM (Security information and event management).

UserGate SWG поддерживает выгрузку следующих журналов:

- Журнал событий.
- Журнал веб-доступа.
- Журнал трафика.
- Журнал DNS.
- Журнал UserID.

Поддерживается отправка журналов на серверы SSH (SFTP), FTP и Syslog. Отправка на серверы SSH и FTP выполняется по указанному в конфигурации расписанию. Отправка на серверы Syslog происходит сразу же при добавлении записи в журнал.

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

ПримечаниеЕсли в параметрах UserGate SWG указан Log Analyzer, то обработка и экспорт журналов, создание отчётов и обработка других статистических данных производятся сервером UserGate Log Analyzer.

При создании правила укажите необходимые параметры для экспорта журналов.

Параметр	Описание
Название правила	Название правила экспорта журналов
Описание	Опциональное поле для описания правила
Параметры разового экспорта	Выбор диапазона экспорта журналов
Журналы для экспорта	Выбор файлов журналов, которые необходимо экспортировать: • Журнал событий. • Журнал веб-доступа. • Журнал трафика. • Журнал DNS. • UserID. Для каждого из журналов возможно указать синтаксис выгрузки: • CEF — Common Event Format (ArcSight). • CEF Compact. • JSON — JSON format. • @CEE: JSON — CEE Log Syntax (CLS) Encoding JSON. Обратитесь к документации на используемую у вас 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

Параметр	Описание
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 у вас системой SIEM
Критичность	Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас 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
Facility	Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас 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
Путь на сервере	Каталог на сервере для копирования файлов журналов. Не применяется к методу отправки Syslog

Параметр	Описание
Расписание	Выбор расписания для отправки журналов. Не применяется к методу отправки Syslog. Вы можете выбрать одно из предустановленных значений расписания 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 экспорт журналов должен выполняться каждый час. • Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений. • Косая черта (/) — для указания шага между значениями
Управление журналами	Управление временными файлами журналов, подготавливаемых для отправки на удаленные серверы ssh и ftp. При отправке журналов на сервера ssh и ftp UserGate сохраняет данные для отправки во временные файлы. По указанному расписанию все созданные для отправки файлы копируются на удаленный сервер, при этом файлы не очищаются и не удаляются. Данная настройка позволяет указать период ротации временных файлов (в днях) или удалить любой из временных файлов вручную. Ротация файлов происходит один раз в сутки. Всего хранятся N архивов журналов за предыдущие дни (по количеству дней ротации) и один журнал за текущий день

Product: SWG
Version: 7.5.x

Экспорт журналов в формате CEF

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.	SWG
	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

Тип поля	Название поля	Описание	Пример значения
	Device Product	Тип продукта.	SWG
	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
	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

Тип поля	Название поля	Описание	Пример значения
	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

Тип поля	Название поля	Описание	Пример значения
	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.	SWG
	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.
	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.

Тип поля	Название поля	Описание	Пример значения
CEF [расширение]	**requestMethod**	Метод, используемый для доступа к URL-адресу (POST, GET и т.п.).	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.	SWG

Тип поля	Название поля	Описание	Пример значения
	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
	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

Тип поля	Название поля	Описание	Пример значения
	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.	SWG
	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

Тип поля	Название поля	Описание	Пример значения
	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
	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.	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

Тип поля	Название поля	Описание	Пример значения
	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.	SWG
	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

Тип поля	Название поля	Описание	Пример значения
	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
	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

Тип поля	Название поля	Описание	Пример значения
	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.	SWG
	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

Тип поля	Название поля	Описание	Пример значения
	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
	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 Windows Active Directory

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	SWG
	Device Version	Версия продукта.	7
	Source	Название журнала.	endpoint_log
	Name	Тип источника.	log
	Threat Level	Уровень угрозы.	Может принимать значения от 1 до 10 (указанный уровень угрозы, умноженный на 2).

Тип поля	Название поля	Описание	Пример значения
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
	suser	Имя пользователя.	user1.dep.local
	msg	Описание события в журнале AD.	Group membership information Subject: Security ID: S-1-0-0 Account Name: — Account Domain: — Logon ID: 0x0 Logon Type: 3 New Logon: Security ID: S-1-5-21-3795870133-5220325-2125745684-1103 Account Name: user1 Account Domain: DEP Logon ID: 0xA57A446 Event in sequence: 1 of 1 Group Membership: %{S-1-5-21-3795870133-5220325-2125745684-513} %{S-1-1-0} %{S-1-5-32-544} %{S-1-5-32-555} %{S-1-5-32-545} %{S-1-5-32-554} %{S-1-5-2} %{S-1-5-11} %{S-1-5-15} %{S-1-5-21-3795870133-5220325-2125745684-512} %{S-1-5-21-3795870133-5220325-2125745684-572} %{S-1-5-64-10} %{S-1-16-12288} The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. This event is generated when the Audit Group Membership subcategory is configured. The Logon ID field can be used to correlate this event with the corresponding user logon event as well as to any other security audit events generated during this logon session.
	cn1Label	Поле используется для указания кода события из журнала AD.	logEventCode
	cn1	Код события.	4627
	cn2Label	Поле используется для указания номера идентификатора события из журнала AD.	logEventId
	cn2	Идентификатор события.	4627
	cn3Label	Поле используется для указания типа события журнала Windows (Система\Безопасность\Приложение и т. д.).	logEventType
	cn3	Тип события журнала Windows.	4
	cs1Label	Поле используется для указания идентификатора конечного устройства — источника события.	endpointId
	cs1	Идентификатор конечного устройства.	16535060-5a1a-4e92-8331-239406ec34da
	cs2Label	Поле используется для указания имени конечного устройства — источника события (UserGate клиента, сенсора WMI итд.).	endpointName

Тип поля	Название поля	Описание	Пример значения
	cs2	Имя конечного устройства.	dep.local
	cs3Label	Поле используется для указания уровня важности события в журнале AD.	logLevel
	cs3	Уровень важности события.	Audit Success
	cs4Label	Поле используется для указания кода категории события (12554 Group Membership, 12544 Logon, 14337 Kerberos Service Ticket Operations и тд)	logCategoryString
	cs4	Категория события.	Group Membership
	cs5Label	Поле используется для указания файла журнала Windows.	logFile
	cs5	Файл журнала Windows	Security
	cs6Label	Поле используется для указания источника из журнала AD.	sourceName
	cs6	Источник из журнала AD.	Microsoft-Windows-Security-Auditing
	flexString1Label	Поле используется для указания содержания события из журнала AD.	insertionString
	flexString1	Параметры события из журнала AD после парсинга сообщения.	['S-1-0-0', '-', '-', '0x0', 'S-1-5-21-3795870133-5220325-2125745684-1103', 'user1', 'DEP', '0x7a25a21', '3', '1', '1', '\\r\\n\\t\\t% {S-1-5-21-3795870133-5220325-2125745684-513}\\r\\n\\t\\t%{S-1-1-0}\\r\\n\\t\\t%{S-1-5-32-544}\\r\\n\\t\\t%{S-1-5-32-555}\\r\\n\\t\\t%{S-1-5-32-545}\\r\\n\\t\\t%{S-1-5-32-554}\\r\\n\\t\\t%{S-1-5-2}\\r\\n\\t\\t%{S-1-5-11} \\r\\n\\t\\t%{S-1-5-15}\\r\\n\\t\\t%{S-1-5-21-3795870133-5220325-2125745684-512}\\r\\n\\t\\t%{S-1-5-21-3795870133-5220325-2125745684-572}\\r\\n\\t\\t%{S-1-5-64-10}\\r\\n\\t\\t%{S-1-16-12288}']

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.	SWG
	Device Version	Версия продукта.	7
	Source	Название журнала.	syslog
	Name	Тип источника.	log

Тип поля	Название поля	Описание	Пример значения
	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
	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.	SWG
	Device Version	Версия продукта.	7
	Source	Название журнала.	radius
	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	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.	SWG
	Device Version	Версия продукта.	7
	Source	Название журнала.	userid
	Name	Тип источника.	log

Тип поля	Название поля	Описание	Пример значения
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

Экспорт журналов в формате JSON

Описание журнала событий

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
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-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
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

Название поля			Описание	Пример значения
		app_protocol	Протокол прикладного уровня и его версия.	HTTP\/1.1"
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.
	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

Название поля			Описание	Пример значения
	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.	

Название поля			Описание	Пример значения
		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
		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

Название поля			Описание	Пример значения
		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

Название поля			Описание	Пример значения
	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.	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 Windows Active Directory

Название поля	Описание	Пример значения
timestamp	Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z

Название поля	Описание	Пример значения
node_name	Имя, которое однозначно идентифицирует устройство UserGate, генерирующее это событие.	utmcore@ntoorereaeda
endpoint_id	Идентификатор конечного устройства — источника события.	16535060-5a1a-4e92-8331-239406ec34da
endpoint_name	Имя конечного устройства — источника события (UserGate клиента, сенсора WMI итд.).	dep.local
user_name	Поле «Пользователь» из журнала AD.	user1.dep.local
log_level	Поле «Keywords» из журнала AD.	Audit Success
log_category_string	Код категории события из журнала AD.	Group Membership
log_file	Файл журнала Windows.	Security
source_name	Поле «Источник» из журнала AD.	Microsoft-Windows-Security-Auditing
data	Описание события в журнале AD.	Group membership information.\r\n\r\nSubject:\r\n\tSecurity ID:\t\tS-1-0-0\r\n\tAccount Name:\t\t-\r\n\tAccount Domain:\t\t-\r\n\tLogon ID:\t\t0x0\r\n\r\nLogon Type:\t\t\t3\r\n\r\nNew Logon:\r\n\tSecurity ID:\t\tS-1-5-21-3795870133-5220325-2125745684-1103\r\n\tAccount Name:\t\tuser1\r\n\tAccount Domain:\t\tDEP\r\n\tLogon ID:\t\t0x7A25A21\r\n\r\nEvent in sequence:\t\t1 of 1\r\n\r\nGroup Membership:\t\t\t\r\n\t\t%{S-1-5-21-3795870133-5220325-2125745684-513}\r\n\t\t%{S-1-1-0}\r\n\t\t%{S-1-5-32-544}\r\n\t\t%{S-1-5-32-555}\r\n\t\t%{S-1-5-32-545}\r\n\t\t%{S-1-5-32-554}\r\n\t\t%{S-1-5-2}\r\n\t\t%{S-1-5-11}\r\n\t\t%{S-1-5-15}\r\n\t\t%{S-1-5-21-3795870133-5220325-2125745684-512}\r\n\t\t%{S-1-5-21-3795870133-5220325-2125745684-572}\r\n\t\t%{S-1-5-64-10}\r\n\t\t%{S-1-16-12288}\r\n\r\nThe subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.\r\n\r\nThe logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).\r\n\r\nThe New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.\r\n\r\nThis event is generated when the Audit Group Membership subcategory is configured. The Logon ID field can be used to correlate this event with the corresponding user logon event as well as to any other security audit events generated during this logon session.
computer_name	Узел Windows из журнала AD, на котором произошло событие.	DC1.dep.local
insertion_string	Параметры события из журнала AD после парсинга сообщения.	['S-1-0-0', '-', '-', '0x0', 'S-1-5-21-3795870133-5220325-2125745684-1103', 'user1', 'DEP', '0x7a25a21', '3', '1', '1', '\\r\\n\\t\\t% {S-1-5-21-3795870133-5220325-2125745684-513}\\r\\n\\t\\t%{S-1-1-0}\\r\\n\\t\\t%{S-1-5-32-544}\\r\\n\\t\\t%{S-1-5-32-555}\\r\\n\\t\\t%{S-1-5-32-545}\\r\\n\\t\\t%{S-1-5-32-554}\\r\\n\\t\\t%{S-1-5-2}\\r\\n\\t\\t%{S-1-5-11} \\r\\n\\t\\t%{S-1-5-15}\\r\\n\\t\\t%{S-1-5-21-3795870133-5220325-2125745684-512}\\r\\n\\t\\t%{S-1-5-21-3795870133-5220325-2125745684-572}\\r\\n\\t\\t%{S-1-5-64-10}\\r\\n\\t\\t%{S-1-16-12288}']
error	Код ошибки из журнала AD, которая произошла при получении данных.	0
status	Описание ошибки из журнала AD, которая произошла при получении данных.	

Название поля	Описание	Пример значения
counter_id	Идентификатор счетчика WMI сенсора.	login_logout
log_event_code	Поле «Код события» из журнала AD.	4627
log_event_id	Поле «Идентификатор события» из журнала AD.	4627
log_event_type	Тип событий журнала Windows (Система\Безопасность\Приложение и т. д.).	4

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

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
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	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@ntoorereaeda
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

Название поля			Описание	Пример значения
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 которой состоит пользователь.	aa218609-8716-9252-df20-88c43a0d0bf6
		name	Название группы, в которой состоит пользователь.	CN=Domain Users,CN=Users,DC=dev,DC=local