

Table of Contents

Table of Contents	1
Приложения	2
Требования к сетевому окружению	3
Синтаксис языка запросов	5

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.

Сервис	Протокол	Порт	Исходящий/Входящий	Функция
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.

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	Оператор применим к параметрам, поддерживающим сравнение значений (например, date, portSource, portDest или statusCode)
!=	Не равно (не совпадает)	ipSource != 192.0.2.55	
<	Меньше	statusCode < 404	
>	Больше	statusCode > 200	
<=	Меньше либо равно	date <= 2019-03-28T20:59:59	
>=	Больше либо равно	date >= 2019-03-13T21:00:00	

Оператор	Значение	Пример запроса	Примечания
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

Параметр	Значение	Пример запроса
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 = 1C
applicationCategory	Категория приложения	applicationCategory = Business
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

Параметр	Значение	Пример запроса
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

Параметр	Значение	Пример запроса
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
action	Действие при срабатывании правила	action = 'allow webaccess'
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

Параметр	Значение	Пример запроса
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

Параметр	Значение	Пример запроса
applicationProtocol	Протокол приложения	applicationProtocol = HTTP
applicationTechnology	Технология приложения	applicationTechnology = Browser-based
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 = utmcore@nodename
packetsRecv	Количество полученных пакетов	packetsRecv > 1000

Параметр	Значение	Пример запроса
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
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

Параметр	Значение	Пример запроса
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 = 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
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

Параметр	Значение	Пример запроса
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
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

Параметр	Значение	Пример запроса
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

Параметр	Значение	Пример запроса
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
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

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
urlCategory	Категория URL	urlCategory = 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

Параметр	Значение	Пример запроса
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
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'

Параметр	Значение	Пример запроса
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

Параметр	Значение	Пример запроса
ipSource	IP-адрес источника	ipSource = 192.0.2.12
monthOfYear	Месяц	monthOfYear = march
node	Имя устройства	node = utmcore@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

Параметр	Значение	Пример запроса
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

Параметр	Значение	Журнал	Пример запроса
action	Действие при срабатывании правила	Событий, веб-доступа, DNS, трафика, COB, ACU 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
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

Параметр	Значение	Журнал	Пример запроса
countryDest	Страна назначения	DNS, трафика, COB, ACU ТП, инспектирования SSH, защиты почтового трафика	countryDest = 'Russian Federation'
countrySource	Страна источника	DNS, трафика, COB, ACU 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

Параметр	Значение	Журнал	Пример запроса
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, АСУ ТП, инспектирования SSH, правил конечных устройств, защиты почтового трафика	ipDest = 203.0.113.10
ipSource	IP-адрес источника	Событий, веб-доступа, DNS, трафика, COB, АСУ 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

Параметр	Значение	Журнал	Пример запроса
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
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

Параметр	Значение	Журнал	Пример запроса
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

Параметр	Значение	Журнал	Пример запроса
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
signatureId	ID сигнатуры COB	COB	signatureId = 999999
signatureName	Название сигнатуры COB	COB	signatureName = Example
signatureOS	ОС 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

Параметр	Значение	Журнал	Пример запроса
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

Параметр	Значение	Журнал	Пример запроса
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
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

Параметр	Значение	Пример запроса
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

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
assigneeld	ID пользователя, ответственного за расследование инцидента	assigneeld = 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
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

Параметр	Значение	Пример запроса
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

