UserGate

UserGate SIEM 7.1.x Руководство администратора

Оглавление

ВВЕДЕНИЕ

Введение (описание)

UserGate SIEM (SIEM) — это система управления информацией о безопасности и событиями информационной безопасности. SIEM собирает в себе данные, получаемые из различных источников — сенсоров. Примерами таких сенсоров могут быть межсетевые экраны UserGate, системы управления и контроля конечных устройств UserGate, сенсоры SNMP, сенсоры WMI, конечные устройства с установленным ПО UserGate Client. Результаты обработки данных предоставляются в едином интерфейсе, что способствует изучению характерных особенностей инцидентов безопасности. На основе полученных данных SIEM в реальном времени с помощью правил аналитики осуществляет агрегацию и корреляцию повторяющихся событий, идентифицируя инциденты кибербезопасности. Правила реагирования позволяют автоматически определить методы реагирования на инциденты информационной безопасности.

Для проведения расследований инцидентов кибербезопасности используется встроенная в SIEM система IRP. IRP — это платформа управления процессами реагирования на инциденты информационной безопасности. SIEM позволяет настроить процесс расследования инцидентов индивидуально под нужды конкретной компании.

SIEM поставляется в виде программно-аппаратного комплекса (ПАК, appliance) либо в виде образа виртуальной машины (virtual appliance), предназначенного для развертывания в виртуальной среде.

ЛИЦЕНЗИРОВАНИЕ SIEM

Лицензирование SIEM (описание)

Для лицензирования SIEM необходима лицензия с базовой функциональностью LogAn и дополнительными модулями, открывающими функциональность SIEM.

Базовая функциональность LogAn лицензируется по количеству настроенных сенсоров, с которых он собирает информацию. В качестве сенсора может выступать шлюз UserGate либо любое другое устройство, которое может отправлять информацию по протоколу SNMP на сервер SIEM.

Лицензия на LogAn дает право бессрочного пользования продуктом.

> **Примечание**
>
> **При добавлении модуля SIEM в лицензию LogAn, администратору отображается предупреждение о смене роли сервера. Роль сервера будет изменена автоматически.**

Дополнительно лицензируются следующие модули:

Наименование	Описание
Модуль Security Update (SU)	Модуль SU дает право на получение обновлений ПО LogAn. Модуль выписывается на 1 год, по истечении данного срока для получения обновлений ПО необходимо приобрести продление лицензии.
Сенсоры	Данный модуль определяет количество сенсоров, с которых LogAn может собирать информацию. Данный модуль выписывается сроком на 1 год и требует ежегодного продления.
Модуль Функциональность SIEM	Модуль предоставляет возможность использования функциональности систем SIEM и IRP: создание и настройка правил аналитики, а также определения методов реагирования на их срабатывания. Модуль дает право на бессрочное использование функциональности SIEM.
Модуль Подписка на экспертизу SIEM	Дополнительный модуль к модулю лицензирования Функциональность SIEM. Данный модуль дает право на получение экспертизы UserGate: • обновление библиотеки правил аналитики; • обновление библиотеки команд удалённого управления устройствами UserGate.

Наименование	Описание
	Данный модуль выписывается сроком на 1 год. По истечении данного срока скачанные на момент наличия лицензии библиотеки продолжают работу, а их обновление становится недоступным; для получения обновлений необходимо продлить лицензию.

Для регистрации продукта необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Перейти в Дашборд	Нажать на пиктограмму **Дашборд** в правом верхнем углу.
Шаг 2. В разделе **Лицензия** зарегистрировать продукт	В разделе **Лицензия** нажать на ссылку **Нет лицензии**, ввести ПИН-код и заполнить регистрационную форму. При нахождении узла UserGate в закрытом контуре без прямого доступа в интернет возможна активация/обновление лицензии через прокси-сервер. Для этого необходимо выбрать режим **Использовать прокси сервер для активации и апдейтов**. Далее указать IP-адрес и порт вышестоящего прокси сервера. При необходимости указать логин и пароль для аутентификации на прокси-сервере.

Посмотреть статус установленной лицензии можно в разделе **Дашборд** в виджете **Лицензия**.

ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА

Описание

LogAn(SIEM) поставляется в виде программно-аппаратного комплекса (ПАК, appliance) либо в виде образа виртуальной машины (virtual appliance), предназначенного для развертывания в виртуальной среде. В случае виртуальной машины LogAn(SIEM) поставляется с четырьмя Ethernet-интерфейсами. В случае поставки в виде ПАК LogAn(SIEM) может содержать 8 или более Ethernet-портов.

Развертывание программно-аппаратного комплекса

В случае поставки решения в виде ПАК, программное обеспечение уже загружено и готово к первоначальной настройке. Перейдите к главе Подключение к устройству для дальнейшей настройки.

Развертывание виртуального образа

LogAn Virtual Appliance позволяет быстро развернуть виртуальную машину, с уже настроенными компонентами. Образ предоставляется в формате OVF (Open Virtualization Format), который поддерживают такие вендоры как VMWare, Oracle VirtualBox. Для Microsoft Hyper-v и KVM поставляются образы дисков виртуальной машины.

> **Примечание**
>
> **Для корректной работы виртуальной машины рекомендуется использовать минимум 8 Гб оперативной памяти и 2-ядерный виртуальный процессор. Гипервизор должен поддерживать работу 64-битных операционных систем.**

Для начала работы с виртуальным образом, выполните следующие шаги:

Наименование	Описание
Шаг 1. Скачайте образ и распакуйте	Скачайте последнюю версию виртуального образа с официального сайта https://www.usergate.com/ru.
Шаг 2. Импортируйте образ в свою систему виртуализации	Инструкцию по импорту образа вы можете посмотреть на сайтах VirtualBox и VMWare. Для Microsoft Hyper-v и KVM необходимо создать виртуальную машину и указать в качестве диска скачанный образ, **после чего отключить службы интеграции** в настройках созданной виртуальной машины.
Шаг 3. Настройте параметры виртуальной машины	Увеличьте размер оперативной памяти виртуальной машины. Используя свойства виртуальной машины, установите минимум 8Gb.
Шаг 4. Важно! Увеличьте размер диска виртуальной машины	Размер диска по умолчанию составляет 100Gb, что обычно недостаточно для хранения всех журналов и настроек. Используя свойства виртуальной машины, установите

Наименование	Описание
	размер диска в 300Gb или более. Рекомендованный размер - 1000Gb или более.
Шаг 5. Настройте виртуальные сети	UserGate LogAn поставляется с двумя интерфейсами, назначенными в зоны: • **Management** — первый интерфейс виртуальной машины. • **Trusted** — второй интерфейс виртуальной машины.
Шаг 6. Выполните сброс к заводским настройкам	Запустите виртуальную машину LogAn. Во время загрузки выберите **Support Menu** и выполните **Factory reset**. **Этот шаг крайне важен**. Во время этого шага настраивает сетевые адаптеры и увеличивает размер раздела на жестком диске до полного размера диска, увеличенного в 4-м пункте.

Подключение к устройству

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

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

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

Остальные интерфейсы отключены и требуют последующей настройки.

Первоначальная настройка требует выполнения следующих шагов:

Наименование	Описание
Шаг 1. Подключиться к интерфейсу управления	**При наличии DHCP-сервера** Подключить интерфейс port0 в сеть предприятия с работающим DHCP-сервером. Включить LogAn. После загрузки LogAn укажет IP-адрес, на который необходимо подключиться для дальнейшей активации продукта. **Статический IP-адрес** Включить LogAn. Используя CLI (Command Line Interface), назначить необходимый IP-адрес на интерфейс port0. Детали использования CLI смотрите в главе Интерфейс командной строки (CLI). Подключиться к веб-консоли LogAn по указанному адресу, он должен выглядеть примерно следующим образом: https://LogAn_IP_address:8010.
Шаг 2. Выбрать язык	Выбрать язык, на котором будет продолжена первоначальная настройка.
Шаг 3. Задать пароль	Задать логин и пароль для входа в веб-интерфейс управления.
Шаг 4. Зарегистрировать систему	Ввести ПИН-код для активации продукта и заполнить регистрационную форму. Для активации системы необходим доступ LogAn в Интернет. Если на данном этапе выполнить регистрацию не удается, то ее следует повторить после настройки сетевых интерфейсов на шаге 8.
Шаг 5. Настроить зоны, IP-адреса интерфейсов, подключить UserGate LogAn в сеть предприятия	В разделе **Интерфейсы** включить необходимые интерфейсы, установить корректные IP-адреса, соответствующие вашим сетям, и назначить интерфейсы соответствующим зонам. Подробно об управлении интерфейсами читайте в главе Настройка интерфейсов. Система поставляется с предопределенными зонами: • Зона Management (сеть управления), интерфейс port0. • Зона Trusted (LAN). Предполагается, что через зону Trusted LogAn будет подключен в сеть, через которую шлюзы UserGate будут отсылать на него журналы, а также через которую LogAn получит доступ в Интернет. Для работы LogAn достаточно одного настроенного интерфейса. Разделение функций управления устройством и сбора данных на разные сетевые интерфейсы рекомендовано для обеспечения безопасности, но не является жестким требованием.
Шаг 6. Настроить шлюз в Интернет	В разделе **Шлюзы** указать IP-адрес шлюза в Интернет на интерфейсе, имеющим доступ в Интернет, как правило, это зона **Trusted**. Подробно о настройке шлюзов в Интернет читайте в главе Настройка шлюзов.

Наименование	Описание
Шаг 7. Указать системные DNS-серверы	В разделе **DNS** укажите IP-адреса серверов DNS, вашего провайдера или серверов, используемых в вашей организации. Подробно об управлении DNS читайте в главе Раздел настройки.
Шаг 8. Зарегистрировать продукт (если не был зарегистрирован на шаге 4)	Зарегистрировать продукт с помощью ПИН-кода. Для успешной регистрации необходимо подключение к Интернету и выполнение предыдущих шагов. Более подробно о лицензировании продукта читайте в главе Лицензирование SIEM.
Шаг 9. Создать дополнительных администраторов (опционально)	В разделе **Администраторы** создать дополнительных администраторов системы, наделить их необходимыми полномочиями (ролями).

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

ОФЛАЙН ОПЕРАЦИИ С СЕРВЕРОМ

Офлайн операции с сервером (описание)

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

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

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

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

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

НАСТРОЙКА SIEM

Раздел настройки

Раздел **Настройки** определяет базовые установки LogAn:

Наименование	Описание
Настройки интерфейса	Настройки интерфейса LogAn: • **Часовой пояс**, соответствующий вашему местоположению. Часовой пояс используется в расписаниях, применяемых в правилах, а также для корректного отображения времени и даты в отчетах, журналах и т.п. • **Язык интерфейса по умолчанию** — язык, который будет использоваться по умолчанию в консоли.
Настройка времени сервера	Настройка параметров установки точного времени: • **Использовать NTP** — использовать сервера NTP из указанного списка для синхронизации времени. • **Основной сервер NTP** — адрес основного сервера точного времени. Значение по умолчанию — pool.ntp.org • **Запасной сервер NTP** — адрес запасного сервера точного времени. • **Время на сервере** — позволяет установить время на сервере. Время должно быть указано в часовом поясе UTC.
Системные DNS-серверы	Укажите корректные IP-адреса серверов DNS в настройках.
Расписание скачивания обновлений	Настройка расписания скачивания обновлений ПО и библиотек. Также возможно проверить наличие обновлений вручную нажатием на **Проверка обновлений**.
Состояние сборщика логов	Отображается текущее состояние сервера LogAn: • **Состояние** — показывает текущее состояние сервиса статистики. • **Версия устройства** — версия LogAn.
Агент UserGate Management Center	Настройки для подключения устройства к центральной консоли управления, позволяющей управлять парком устройств LogAn из одной точки. • **Включен/Выключен** — включение или отключение управления с помощью UGMC. • **Адрес UserGate Management Center** — адрес сервера в формате IPv4-адреса, FQDN (допускается использование IDN-адреса). • **Код устройства** — токен, требуемый для подключения к UGMC.

Управление устройством

Раздел **Управление устройством** определяет следующие установки LogAn:

- Диагностика.
- Операции с сервером.
- Резервное копирование.
- Экспорт и импорт настроек.

Диагностика

В данном разделе задаются параметры диагностики сервера, необходимые службе технической поддержки LogAn при решении возможных проблем.

Наименование	Описание
Детализация диагностики	• **Off** — ведение журналов диагностики отключено. • **Error** — журналировать только ошибки работы сервера. • **Warning** — журналировать только ошибки и предупреждения. • **Info** — журналировать только ошибки, предупреждения и дополнительную информацию. • **Debug** — максимум детализации. Рекомендуется установить значение параметра **Детализация диагностики** в **Error** (только ошибки) или **Off** (Отключено), если техническая поддержка UserGate не попросила вас установить иные значения. Любые значения, отличные от Error (только ошибки) или Off (Отключено), негативно влияют на производительность LogAn.
Журналы диагностики	• **Скачать журналы** — скачать диагностические журналы для передачи их в службу поддержки UserGate. • **Очистить журналы** — удалить содержимое папки крэш-логов.
Удаленный помощник	

Наименование	Описание
	• **Включено/Отключено** — включение/отключение режима удаленного помощника. Удаленный помощник позволяет инженеру технической поддержки UserGate, зная значения идентификатора и токена удаленного помощника, произвести безопасное подключение к серверу LogAn для диагностики и решения проблем. Для успешной активации удаленного помощника LogAn должен иметь доступ к серверу удаленного помощника компании UserGate по протоколу SSH. • **Идентификатор удаленного помощника** — полученное случайным образом значение. Уникально для каждого включения удаленного помощника. • **Токен удаленного помощника** — полученное случайным образом значение токена. Уникально для каждого включения удаленного помощника.

Операции с сервером

Данный раздел позволяет произвести следующие операции с сервером:

Наименование	Описание
Операции с сервером	• **Перезагрузить** — перезагрузка сервера LogAn. • **Выключить** — выключение сервера LogAn.
Обновления	Выбор канала обновлений ПО LogAn: • **Стабильные** — проверка наличия стабильных обновлений ПО. • **Бета** — проверка наличия экспериментальных обновлений.
Обновления сервера	Индикация имеющихся обновлений сервера UserGate. Запуск процесса обновления сервера с возможностью создания точки восстановления. Просмотр списка изменений ПО в обновлении.
Офлайн обновления	Загрузка файла для офлайн обновления.
Настройки вышестоящего прокси для проверки лицензий и обновлений	Настройка параметров вышестоящего HTTP(S) прокси-сервера для обновления лицензии и обновления ПО сервера UserGate.

Наименование	Описание
	Необходимо указать IP-адрес и порт вышестоящего прокси сервера. При необходимости указать логин и пароль для аутентификации на вышестоящем прокси-сервере.

Компания UserGate постоянно работает над улучшением качества своего программного обеспечения и предлагает обновления продукта LogAn в рамках подписки на модуль лицензии Security Update (подробно о лицензировании смотрите в разделе Лицензирование SIEM). При наличии обновлений в разделе **Управление устройством** отобразится соответствующее оповещение. Обновление продукта может занять довольно длительное время, рекомендуется планировать установку обновлений с учетом возможного времени простоя LogAn.

Для установки обновлений необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл резервного копирования	Создать резервную копию состояния LogAn, как это описано в разделе Системные утилиты. Данный шаг рекомендуется всегда выполнять перед применением обновлений, поскольку он позволит восстановить предыдущее состояние устройства в случае возникновения каких-либо проблем во время применения обновлений.
Шаг 2. Установить обновления	В разделе **Управление устройством** при наличии оповещения **Доступны новые обновления** нажать на ссылку **Установить сейчас**. Система установит скачанные обновления, по окончании установки LogAn будет перезагружен.

Управление резервным копированием

Данный раздел позволяет управлять резервным копированием UserGate: настройка правил экспорта конфигурации, создание резервной копии, восстановление устройства UserGate.

Для создания резервной копии необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать резервную копию	В разделе **Управление устройством → Управление резервным копированием** нажать **Создание резервной копии**. Система сохранит текущие настройки сервера под следующим именем: backup_PRODUCT_NODE-NAME_DATE.gpg, где *PRODUCT* — тип продукта: NGFW, LogAn, MC;

Наименование	Описание
	NODE-NAME — имя узла UserGate; *DATE* — дата и время создания резервной копии в формате YYYY-MM-DD-HH-MM; время указывается в часовом поясе UTC. Процесс создания резервной копии может быть прерван нажатием кнопки **Остановить**. Запись о создании резервной копии отобразится в журнале событий устройства.

Для восстановления состояния устройства необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Восстановить состояние устройства	В разделе **Управление устройством → Управление резервным копированием** нажать **Восстановление из резервной копии** и указать путь к ранее созданному файлу настроек для его загрузки на сервер. Восстановление будет предложено в консоли tty при перезагрузке устройства.

Дополнительно администратор может настроить сохранение файлов на внешние серверы (FTP, SSH) по расписанию. Для создания расписания выгрузки настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать правило экспорта конфигурации	В разделе **Управление устройством → Управление резервным копированием** нажать кнопку **Добавить**, указать имя и описание правила.
Шаг 2. Указать параметры удаленного сервера	Во вкладке правила **Удаленный сервер** указать параметры удаленного сервера: • **Тип сервера** — FTP или SSH. • **Адрес сервера** — IP-адрес сервера. • **Порт** — порт сервера. • **Логин** — учетная запись на удаленном сервере. • **Пароль**/**Повторите пароль** — пароль учетной записи. • **Путь на сервере** — путь на сервере, куда будут выгружены настройки. В случае использование SSH-сервера возможно использование авторизации по ключу. Для импорта или генерации ключа необходимо выбрать **Настроить SSH-ключ** и указать **Сгенерировать ключи** или **Импортировать ключ**. **Важно!** При повторном создании ключа существующий SSH-ключ будет удален. Публичный ключ должен

Наименование	Описание
	находиться на SSH-сервере в директории пользовательских ключей **/home/user/.ssh/** в файле **authorized_keys**. При первоначальной настройке правила экспорта резервного копирования по SSH обязательна проверка соединения (кнопка **Проверить соединение**); при проверке соединения fingerprint помещается в known_hosts, без проверки файлы не будут отправляться. **Важно!** Если сменить сервер SSH или его переустановить, то файлы резервного копирования будут недоступны, так как fingerprint изменится - это защита от спуфинга.
Шаг 3. Выбрать расписание выгрузки	Во вкладке правила **Расписание** указать необходимое время отправки настроек. В случае задания времени в crontab-формате, задайте его в следующем виде: (минуты:0-59) (часы:0-23) (дни месяца:1-31) (месяц:1-12) (день недели:0-6, 0-воскресенье) Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка и тире используются для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

Экспорт и импорт настроек

Администратор имеет возможность сохранить текущие настройки LogAn в файл и впоследствии восстановить эти настройки на этом же или другом сервере LogAn. В отличие от резервного копирования, экспорт/импорт настроек не сохраняет текущее состояние всех компонентов комплекса, сохраняются только текущие настройки.

Примечание

Экспорт/импорт настроек не восстанавливает состояние интерфейсов и информацию о лицензии. После окончания процедуры импорта необходимо повторно зарегистрировать LogAn с помощью имеющегося ПИН-кода и настроить интерфейсы.

Для экспорта настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Экспорт настроек	В разделе **Управление устройством → Экспорт и импорт настроек** нажмите **Экспорт** и выберите **Экспортировать все настройки** или **Экспортировать сетевые настройки**. Система сохранит: • текущие настройки сервера под именем: logan_core-logan_core@nodename_version_YYYYMMDD_HHMMSS.bin • сетевые настройки под именем: network-logan_core-logan_core@nodename_version_YYYYMMDD_HHMMSS.bin nodename — имя узла LogAn. version — версия LogAn. YYYYMMDD_HHMMSS — дата и время выгрузки настроек в часовом поясе UTC. Например, logan_core-logan_core@ranreahattha_6.2.0.13494RS-1_20211227_091350.bin или network-logan_core-logan_core@ranreahattha_6.2.0.13494RS-1_20211227_091407.bin.

Для применения созданных ранее настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Импорт настроек	В разделе **Управление устройством → Экспорт и импорт настроек** нажать **Импорт** и указать путь к ранее созданному файлу настроек. Указанные настройки применятся к серверу, после чего сервер будет перезагружен

Дополнительно администратор может настроить сохранение настроек на внешние серверы (FTP, SSH) по расписанию. Для создания расписания выгрузки настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать правило экспорта	В разделе **Управление устройством → Экспорт и импорт настроек** нажать кнопку **Добавить**, указать имя и описание правила.
Шаг 2. Указать параметры удаленного сервера	Во вкладке правила **Удаленный сервер** указать параметры удаленного сервера: • **Тип сервера** — FTP или SSH. • **Адрес сервера** — IP-адрес сервера. • **Порт** — порт сервера. • **Логин** — учетная запись на удаленном сервере. • **Пароль/Повторите пароль** — пароль учетной записи. • **Путь на сервере** — путь на сервере, куда будут выгружены настройки.
Шаг 3. Выбрать расписание выгрузки	Во вкладке правила **Расписание** указать необходимое время отправки настроек. В случае задания времени в CRONTAB-формате, задайте его в следующем виде: (минуты:0-59) (часы:0-23) (дни месяца:1-31) (месяц:1-12) (день недели:0-6, 0-воскресенье) Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка и тире используются для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа."

Администраторы

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

> **Примечание**
>
> **При первоначальной настройке LogAn создается локальный суперпользователь Admin.**

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

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

При создании профиля доступа администратора необходимо указать следующие параметры:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.

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

Ролевые разрешения для ролей, созданных в системе по умолчанию:

Более подробно о ролевых разрешениях смотрите в разделе Роли и ролевые разрешения пользователей.

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

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

Для настройки этих параметров необходимо:

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

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

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

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

> **Примечание**
> **Не рекомендуется разрешать доступ к веб-консоли для зон, подключенных к неконтролируемым сетям, например, к сети Интернет.**

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

Управление сертификатами

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

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

Наименование	Описание
Шаг 1. Создать сертификат	Нажать на кнопку **Создать** в разделе **Сертификаты**.
Шаг 2. Заполнить необходимые поля	Указать значения следующих полей: • **Название** — название сертификата, под которым он будет отображен в списке сертификатов.

Наименование	Описание
	• **Описание** — описание сертификата. • **Страна** — страна, в которой выписывается сертификат. • **Область или штат** — область или штат, в котором выписывается сертификат. • **Город** — город, в котором выписывается сертификат. • **Название организации** — название организации, для которой выписывается сертификат. • **Common name** — имя сертификата. Рекомендуется использовать только символы латинского алфавита для совместимости с большинством браузеров. • **E-mail** — email вашей компании.
Шаг 3. Указать, для чего будет использован данный сертификат	После создания сертификата необходимо указать его роль в LogAn. Для этого необходимо выделить необходимый сертификат в списке сертификатов, нажать на кнопку **Редактировать** и указать тип сертификата — SSL веб-консоли. После этого LogAn перезагрузит сервис веб-консоли и предложит вам подключиться уже с использованием нового сертификата.

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

Для экспорта сертификата необходимо:

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

> **Примечание**
>
> **Рекомендуется сохранять сертификат для возможности его последующего восстановления.**

> **Примечание**
>
> **В целях безопасности LogAn не разрешает экспорт приватных ключей сертификатов.**

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

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

Серверы аутентификации

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

LDAP-коннектор

LDAP-коннектор позволяет:

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

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

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

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

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

domain\user/system или *user@domain/system*

Сервер аутентификации RADIUS

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

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

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

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

Сервер аутентификации TACACS+

Сервер TACACS+ позволяет производить авторизацию пользователей в консоли администрирования UserGate. При использовании сервера UserGate передаёт на серверы аутентификации информацию с именем и паролем пользователя,

после чего серверы TACACS+ отвечают, успешно прошла аутентификация или нет.

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

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

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

Профили аутентификации

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

Наименование	Описание
Название	Название профиля аутентификации.
Описание	Описание профиля (опционально).

Наименование	Описание
Методы аутентификации	Методы аутентификации пользователей, настроенные ранее: LDAP-коннектор, серверы аутентификации RADIUS, TACACS+.

Роли и ролевые разрешения пользователей

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

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

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

Для пользователей могут быть указаны следующие ролевые разрешения.

Наименование	Описание
Назначаемый пользователь	Пользователь с этим разрешением может быть назначен на инцидент. Ответственный за инцидент может быть указан при создании или редактировании инцидента.
Назначение инцидентов	Возможность назначать пользователей на инциденты. Указать ответственного можно при создании или редактировании инцидента.
Закрытие инцидента	Возможность закрыть инцидент. Часто бывает полезно, когда разработчики разрешают инциденты, а тестировщики закрывают их. Закрыть инцидент можно во вкладке **Инциденты → <INC-N:Название инцидента>** (где N — порядковый номер

Наименование	Описание
	инцидента). Закрытие инцидента возможно только из состояний, для которых в схеме инцидента настроен переход в состояние Закрыт. Подробнее читайте в Настройки инцидентов.
Создание инцидентов	Возможность создавать инциденты. Инциденты могут быть созданы во вкладке **Инциденты → Журнал инцидентов** или автоматически при срабатывании правила аналитики. О создании инцидентов подробнее читайте в разделе Создание инцидентов безопасности.
Изменение инцидента	Возможность изменять инциденты. Редактирование инцидентов доступно во вкладке **Инциденты → <INC-N:Название инцидента>** (где N — порядковый номер инцидента). Подробнее читайте в разделе Подробности инцидента.
Переоткрытие инцидента	Возможность переоткрывать инциденты. Заново открыть инцидент можно во вкладке **Инциденты → <INC-N:Название инцидента>** (где N — порядковый номер инцидента).
Редактирование наблюдателей	Возможность добавлять и удалять наблюдателей. Пользователи для наблюдения за инцидентом могут быть указаны при создании или редактировании инцидента.
Оставление комментариев	Возможность комментировать инциденты. Комментирование инцидентов возможно во вкладке **Инциденты → <INC-N:Название инцидента>** (где N — порядковый номер инцидента) в разделе **Активность**.
Удаление любых комментариев	Возможность удалять любые комментарии к инцидентам. Комментарии к инциденту можно посмотреть во вкладке **Инциденты → <INC-N:Название инцидента>** (где N — порядковый номер инцидента) в разделе **Активность**.
Удаление собственных комментариев	Возможность удалять собственные комментарии к инцидентам. Комментарии к инциденту можно посмотреть во вкладке **Инциденты → <INC-N:Название инцидента>** (где N — порядковый номер инцидента) в разделе **Активность**.

Наименование	Описание
Редактирование любых комментариев	Возможность редактировать любые комментарии к инцидентам. Комментарии к инциденту можно посмотреть во вкладке **Инциденты → <INC-N:Название инцидента>** (где N — порядковый номер инцидента) в разделе **Активность**.
Редактирование своих комментариев	Возможность редактировать свои комментарии к инцидентам. Комментарии к инциденту можно посмотреть во вкладке **Инциденты → <INC-N:Название инцидента>** (где N — порядковый номер инцидента) в разделе **Активность**.
Создание вложений	Возможность добавлять вложения к инцидентам. Вложения к инциденту можно добавить во вкладке **Инциденты** при создании инцидента или его редактировании. Вложения отображены во вкладке **Инциденты → <INC-N:Название инцидента>** (где N — порядковый номер инцидента) в разделе **Вложения**.
Удаление любых вложений	Возможность удалять любые вложения. Вложения к инциденту отображены во вкладке **Инциденты → <INC-N:Название инцидента>** (где N — порядковый номер инцидента) в разделе **Вложения**.
Удаление своих вложений	Возможность удалять свои вложения. Вложения к инциденту отображены во вкладке **Инциденты → <INC-N:Название инцидента>** (где N — порядковый номер инцидента) в разделе **Вложения**.
Редактирование улик	Возможность создания и редактирования улик. Улики могут быть добавлены во вкладке **Инциденты → <INC-N:Название инцидента>** (где N — порядковый номер инцидента) в разделе **Улики**. Подробнее об уликах читайте в разделе Подробности инцидента.
Обновление обогащений	Возможность обновлять/запрашивать обогащения улик. Список внешних сервисов обогащений доступен во вкладке **Настройки** в разделе **Библиотеки → Внешние сервисы обогащений**. Подробнее о внешних сервисах обогащений читайте в разделе Внешние сервисы обогащений.

Наименование	Описание
Создание отчёта	Возможность создавать, загружать и посылать отчёты инцидентов. Создание отчётов инцидентов доступно во вкладке **Инциденты → INC-N:Название инцидента** (где N — порядковый номер инцидента). Подробнее читайте в разделе Подробности инцидента.
Добавление журналов к инциденту	Возможность добавлять журналы к инциденту. Журналы могут быть добавлены во вкладке **Инциденты → <INC-N:Название инцидента>** (где N — порядковый номер инцидента) в разделе **Журналы**. Подробнее о журналах читайте в разделе Поиск; о срабатываниях — в разделе Срабатывания.
Удалить все срабатывания/журналы из инцидента	Возможность удаления всех срабатываний/журналов из инцидента. Срабатывания и журналы отображены во вкладке **Инциденты → <INC-N:Название инцидента>** (где N — порядковый номер инцидента) в соответствующих разделах **Срабатывания** и **Журналы**. Подробнее о журналах читайте в разделе Поиск; о срабатываниях — в разделе Срабатывания.
Удаление собственных срабатываний, журналов к инцидентам	Возможность удалять собственные срабатывания/журналы к инцидентам. Срабатывания и журналы отображены во вкладке **Инциденты → <INC-N:Название инцидента>** (где N — порядковый номер инцидента) в соответствующих разделах **Срабатывания** и **Журналы**. Подробнее о журналах читайте в разделе Поиск; о срабатываниях — в разделе Срабатывания.
Создание схемы инцидента	Возможность создавать схемы инцидентов. Схемы инцидентов доступны во вкладке **Настройки** в разделе **Настройка инцидентов → Схема инцидентов**. Подробнее читайте в разделе Настройки инцидентов.
Редактирование схемы инцидента	Возможность редактировать схемы инцидентов. Схемы инцидентов доступны во вкладке **Настройки** в разделе **Настройка инцидентов → Схема инцидентов**. Подробнее читайте в разделе Настройки инцидентов.
Удаление схемы инцидента	Возможность удалять схемы инцидентов. Схемы инцидентов доступны во вкладке **Настройки** в разделе **Настройка инцидентов → Схема инцидентов**. Подробнее читайте в разделе Настройки инцидентов.
	Возможность установки схем инцидентов по умолчанию.

Наименование	Описание
Установка схемы инцидентов по умолчанию	В UserGate LogAn создана одна схема инцидента по умолчанию; доступна во вкладке **Настройки** в разделе **Настройка инцидентов → Схема инцидентов**. Подробнее читайте в разделе Настройки инцидентов.
Создание состояния инцидента	Возможность создавать состояния инцидентов. Список состояний инцидентов отображён во вкладке **Настройки** в разделе **Настройка инцидентов → Состояния инцидентов**. Подробнее читайте в разделе Настройки инцидентов.
Редактирование состояния инцидента	Возможность редактировать состояния инцидентов. Список состояний инцидентов отображён во вкладке **Настройки** в разделе **Настройка инцидентов → Состояния инцидентов**. Подробнее читайте в разделе Настройки инцидентов.
Удаление состояния инцидента	Возможность удалять состояния инцидентов. Список состояний инцидентов отображён во вкладке **Настройки** в разделе **Настройка инцидентов → Состояния инцидентов**. Подробнее читайте в разделе Настройки инцидентов.
Создание типа инцидента	Возможность создавать типы инцидентов. Типы инцидентов доступны во вкладке **Настройки** в разделе **Настройка инцидентов → Типы инцидентов**. Подробнее читайте в разделе Настройки инцидентов.
Редактирование типа инцидента	Возможность редактировать типы инцидентов. Типы инцидентов доступны во вкладке **Настройки** в разделе **Настройка инцидентов → Типы инцидентов**. Подробнее читайте в разделе Настройки инцидентов.
Удаление типа инцидента	Возможность удалять типы инцидентов. Типы инцидентов доступны во вкладке **Настройки** в разделе **Настройка инцидентов → Типы инцидентов**. Подробнее читайте в разделе Настройки инцидентов.
Создание решения инцидента	Возможность создавать решения инцидентов. Список решений инцидентов отображён во вкладке **Настройки** в разделе **Настройка инцидентов → Решения инцидентов**. Подробнее читайте в разделе Настройки инцидентов.

Наименование	Описание
Редактирование решения инцидента	Возможность редактировать решения инцидентов. Список решений инцидентов отображён во вкладке **Настройки** в разделе **Настройка инцидентов → Решения инцидентов**. Подробнее читайте в разделе Настройки инцидентов.
Удаление решения инцидентов	Возможность удалять решения инцидентов. Список решений инцидентов отображён во вкладке **Настройки** в разделе **Настройка инцидентов → Решения инцидентов**. Подробнее читайте в разделе Настройки инцидентов.
Создание правила аналитики	Возможность создавать правила аналитики. Правила аналитики могут быть созданы во вкладке **Аналитика → Правила аналитики**. Подробнее читайте в разделе Аналитика.
Удаление правила аналитики	Возможность удалять правила аналитики. Правила аналитики отображены во вкладке **Аналитика → Правила аналитики**. Подробнее читайте в разделе Аналитика.
Редактирование правила аналитики	Возможность редактировать правила аналитики. Правила аналитики отображены во вкладке **Аналитика → Правила аналитики**. Подробнее читайте в разделе Аналитика.
Включение/выключение правила аналитики	Возможность включать/выключать правила аналитики. Правила аналитики отображены во вкладке **Аналитика → Правила аналитики**. Подробнее читайте в разделе Аналитика.
Запуск правила аналитики	Возможность запустить правило аналитики не в режиме реального времени. Правила аналитики отображены во вкладке **Аналитика → Правила аналитики**. Подробнее читайте в разделе Аналитика.
Создание действия реагирования	Возможность создавать действия реагирования. Действия реагирования могут быть созданы во вкладке **Аналитика → Действия реагирования**. Подробнее читайте в разделе Действия реагирования.
Редактирование действия реагирования	Возможность редактировать действия реагирования.

Наименование	Описание
	Действия реагирования отображены во вкладке **Аналитика → Действия реагирования**. Подробнее читайте в разделе Действия реагирования.
Удаление действия реагирования	Возможность удалять действия реагирования. Действия реагирования отображены во вкладке **Аналитика → Действия реагирования**. Подробнее читайте в разделе Действия реагирования.
Включение/выключение действия реагирования	Возможность включать/выключать действия реагирования. Действия реагирования отображены во вкладке **Аналитика → Действия реагирования**. Подробнее читайте в разделе Действия реагирования.
Создание сенсора UserGate	Возможность создавать сенсоры UserGate. Сенсоры UserGate могут быть созданы во вкладке **Настройки** в разделе **Сенсоры → Сенсоры UserGate**. Подробнее читайте в разделе Сенсоры UserGate.
Редактирование сенсора UserGate	Возможность редактировать сенсоры UserGate. Сенсоры UserGate, доступны во вкладке **Настройки** в разделе **Сенсоры → Сенсоры UserGate**. Подробнее читайте в разделе Сенсоры UserGate.
Включение/выключение сенсора UserGate	Возможность включать/выключать сенсоры UserGate. Сенсоры UserGate доступны во вкладке **Настройки** в разделе **Сенсоры → Сенсоры UserGate**. Подробнее читайте в разделе Сенсоры UserGate.
Удаление сенсора UserGate	Возможность удалять сенсоры UserGate. Сенсоры UserGate доступны во вкладке **Настройки** в разделе **Сенсоры → Сенсоры UserGate**. Подробнее читайте в разделе Сенсоры UserGate.
Создание сенсора SNMP	Возможность создавать сенсоры SNMP. Сенсоры SNMP могут быть созданы во вкладке **Настройки** в разделе **Сенсоры → Сенсоры SNMP**. Подробнее читайте в разделе Сенсоры SNMP.
Редактирование сенсора SNMP	Возможность редактировать сенсоры SNMP. Сенсоры SNMP доступны во вкладке **Настройки** в разделе **Сенсоры → Сенсоры SNMP**. Подробнее читайте в разделе Сенсоры SNMP.
Включение/выключение сенсора SNMP	Возможность включать/выключать сенсоры SNMP.

Наименование	Описание
	Сенсоры SNMP доступны во вкладке **Настройки** в разделе **Сенсоры → Сенсоры SNMP**. Подробнее читайте в разделе Сенсоры SNMP.
Удаление сенсора SNMP	Возможность удалять сенсоры SNMP. Сенсоры SNMP доступны во вкладке **Настройки** в разделе **Сенсоры → Сенсоры SNMP**. Подробнее читайте в разделе Сенсоры SNMP.
Создание сенсора WMI	Возможность создавать сенсоры WMI. Сенсоры WMI могут быть созданы во вкладке **Настройки** в разделе **Сенсоры → Сенсоры WMI**. Подробнее читайте в разделе Сенсоры WMI.
Редактирование сенсора WMI	Возможность редактировать сенсоры WMI. Сенсоры WMI доступны во вкладке **Настройки** в разделе **Сенсоры → Сенсоры WMI**. Подробнее читайте в разделе Сенсоры WMI.
Включение/выключение сенсора WMI	Возможность включать/выключать сенсоры WMI. Сенсоры WMI доступны во вкладке **Настройки** в разделе **Сенсоры → Сенсоры WMI**. Подробнее читайте в разделе Сенсоры WMI.
Удаление сенсора WMI	Возможность удалять сенсоры WMI. Сенсоры WMI доступны во вкладке **Настройки** в разделе **Сенсоры → Сенсоры WMI**. Подробнее читайте в разделе Сенсоры WMI.
Добавление SNMP MIB файла	Возможность добавлять SNMP MIB файлы. MIB файлы могут быть добавлены во вкладке **Настройки** в разделе **Сенсоры → Управление SNMP MIB**. Подробнее читайте в разделе Управление SNMP MIB.
Удаление SNMP MIB файла	Возможность удалять SNMP MIB файлы. MIB файлы отображены во вкладке **Настройки** в разделе **Сенсоры → Управление SNMP MIB**. Подробнее читайте в разделе Управление SNMP MIB.
Создание коннекторов	Возможность создавать коннекторы. Коннекторы могут быть созданы во вкладке **Настройки** в разделе **Сенсоры → Коннекторы**. Подробнее читайте в разделе Коннекторы.
Редактирование коннекторов	Возможность редактировать коннекторы.

Наименование	Описание
	Коннекторы доступны во вкладке **Настройки** в разделе **Сенсоры → Коннекторы**. Подробнее читайте в разделе Коннекторы.
Удаление коннекторов	Возможность удалять коннекторы. Коннекторы доступны во вкладке **Настройки** в разделе **Сенсоры → Коннекторы**. Подробнее читайте в разделе Коннекторы.
Создание правила Syslog	Возможность создавать правила Syslog. Правила Syslog могут быть созданы во вкладке **Настройки** в разделе **Сборщик логов → Syslog**.
Удаление правила Syslog	Возможность удалять правила Syslog. Правила Syslog отображены во вкладке **Настройки** в разделе **Сборщик логов → Syslog**.
Редактирование правил и коннектора Syslog	Возможность редактировать правила Syslog и настраивать Syslog. Созданные правила Syslog доступны во вкладке **Настройки** в разделе **Сборщик логов → Syslog**.
Включение/выключение правила Syslog	Возможность включать/выключать правила Syslog. Правила Syslog доступны во вкладке **Настройки** в разделе **Сборщик логов → Syslog**.
Создание группы email	Возможность создавать почтовые адреса/почтовые группы. Почтовые адреса и группы почтовых адресов могут быть созданы во вкладке **Настройки** в разделе **Библиотеки → Почтовые адреса**. Подробнее читайте в разделе Почтовые адреса.
Редактирование группы email	Возможность редактировать почтовые адреса/почтовые группы. Почтовые адреса и группы почтовых адресов доступны во вкладке **Настройки** в разделе **Библиотеки → Почтовые адреса**. Подробнее читайте в разделе Почтовые адреса.
Удаление группы email	Возможность удалять почтовые адреса/почтовые группы. Почтовые адреса и группы почтовых адресов доступны во вкладке **Настройки** в разделе **Библиотеки → Почтовые адреса**. Подробнее читайте в разделе Почтовые адреса.
Создание группы номеров телефонов	Возможность создавать номера телефонов/группы телефонных номеров.

Наименование	Описание
	Номера телефонов и группы телефонных адресов могут быть созданы во вкладке **Настройки** в разделе **Библиотеки → Почтовые адреса**. Подробнее читайте в разделе Почтовые адреса.
Редактирование группы номеров телефонов	Возможность редактировать номера телефонов/группы телефонных номеров. Номера телефонов и группы телефонных адресов могут доступны во вкладке **Настройки** в разделе **Библиотеки → Почтовые адреса**. Подробнее читайте в разделе Почтовые адреса.
Удаление группы номеров телефонов	Возможность удалять номера телефонов/группы телефонных номеров. Номера телефонов и группы телефонных адресов могут доступны во вкладке **Настройки** в разделе **Библиотеки → Почтовые адреса**. Подробнее читайте в разделе Почтовые адреса.
Создание команд	Возможность создавать команды к коннекторам. Команды к коннекторам могут быть созданы во вкладке **Настройки** в разделе **Библиотеки → Команды**. Подробнее читайте в разделе Команды.
Редактирование команд	Возможность редактировать команды к коннекторам. Команды к коннекторам доступны во вкладке **Настройки** в разделе **Библиотеки → Команды**. Подробнее читайте в разделе Команды.
Удаление команд	Возможность удалять команды к коннекторам. Команды к коннекторам доступны во вкладке **Настройки** в разделе **Библиотеки → Команды**. Подробнее читайте в разделе Команды.
Создание профиля оповещения	Возможность создавать профиль оповещения. Во вкладке **Настройки** в разделе **Библиотеки → Профили оповещений** могут быть созданы два типа профилей: SMPP и SMTP. Подробнее о профилях оповещений читайте в разделе Профили оповещений.
Редактирование профиля оповещения	Возможность редактировать профиль оповещения. Список профилей доступен во вкладке **Настройки** в разделе **Библиотеки → Профили оповещений**. Подробнее о профилях оповещений читайте в разделе Профили оповещений.
	Возможность редактировать профиль оповещения.

Наименование	Описание
Удаление профиля оповещения	Список профилей доступен во вкладке **Настройки** в разделе **Библиотеки → Профили оповещений**. Подробнее о профилях оповещений читайте в разделе Профили оповещений.
Создание категории срабатывания	Возможность создавать категории срабатывания. Категории срабатываний могут быть созданы во вкладке **Настройки** в разделе **Библиотеки → Категории срабатываний**. Подробнее о категориях срабатываний читайте в разделе Категории срабатываний.
Редактирование категории срабатывания	Возможность редактировать категории срабатывания. Список категорий срабатываний доступен во вкладке **Настройки** в разделе **Библиотеки → Категории срабатываний**. Подробнее о категориях срабатываний читайте в разделе Категории срабатываний.
Удаление категории срабатывания	Возможность удалять категории срабатывания. Список категорий срабатываний доступен во вкладке **Настройки** в разделе **Библиотеки → Категории срабатываний**. Подробнее о категориях срабатываний читайте в разделе Категории срабатываний.
Редактирование настройки обогащения	Возможность редактировать настройки обогащений. Список внешних сервисов обогащения доступен во вкладке **Настройки** в разделе **Библиотеки → Внешние сервисы обогащений**. Подробнее о внешних сервисах обогащений читайте в разделе Внешние сервисы обогащений.
Включение/выключение сервиса обогащения	Возможность включать/выключать сервисы обогащений. Список внешних сервисов обогащения доступен во вкладке **Настройки** в разделе **Библиотеки → Внешние сервисы обогащений**. Подробнее о внешних сервисах обогащений читайте в разделе Внешние сервисы обогащений.
Создание правила нормализации	Возможность создавать правила нормализации. Правила нормализации могут быть созданы во вкладке **Журналы и отчеты** в разделе **Журналы → Пользовательская нормализация логов**. Подробнее о категориях срабатываний читайте в разделе Пользовательская нормализация логов.
Редактирование правила нормализации	Возможность редактировать правила нормализации. Правила нормализации доступны во вкладке **Журналы и отчеты** в разделе **Журналы → Пользовательская нормализация логов**. Подробнее о категориях

Наименование	Описание
	срабатываний читайте в разделе Пользовательская нормализация логов.
Удаление правила нормализации	Возможность удалять правила нормализации. Правила нормализации доступны во вкладке **Журналы и отчеты** в разделе **Журналы → Пользовательская нормализация логов**. Подробнее о категориях срабатываний читайте в разделе Пользовательская нормализация логов.
Включение/выключение правила нормализации	Возможность включать/выключать правила нормализации. Правила нормализации доступны во вкладке **Журналы и отчеты** в разделе **Журналы → Пользовательская нормализация логов**. Подробнее о категориях срабатываний читайте в разделе Пользовательская нормализация логов.

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

Каталоги пользователей

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

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

Наименование	Описание
Включено	Включает или отключает использование данного LDAP-коннектора.
Название	Название LDAP-коннектора.
Описание	Описание LDAP-коннектора.
SSL	Определяет, требуется ли SSL-соединение для подключения к LDAP-серверу.
Доменное имя LDAP или IP-адрес	IP-адрес контроллера домена, FQDN контроллера домена или FQDN домена (например, test.local). Если указан FQDN,

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

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

Расширение системного раздела

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

Наименование	Описание
Шаг 1. Добавить дополнительный виртуальный диск.	Средствами гипервизора добавить **новый** диск необходимого размера в свойствах виртуальной машины UserGate.
Шаг 2. Расширить размер раздела в системных утилитах.	В меню загрузки узла UserGate войти в раздел **Support menu**. В открывшемся разделе выбрать **Expand data partition** и запустить процесс расширения раздела.

Наименование	Описание
Шаг 3. Проверить размер системного раздела.	После завершения процесса расширения загрузить узел и в разделе **Дашборд → Диски** проверить размер системного раздела.

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

НАСТРОЙКА СЕТИ

Настройка зон

Зона в LogAn — это логическое объединение сетевых интерфейсов. Политики безопасности LogAn используют зоны интерфейсов, а не непосредственно интерфейсы.

Рекомендуется объединять интерфейсы в зоне на основе их функционального назначения, например, зона LAN-интерфейсов, зона Интернет-интерфейсов, зона интерфейсов управления.

По умолчанию UserGate LogAn поставляется со следующими зонами:

Наименование	Описание
Management	Зона для подключения доверенных сетей, из которых разрешено управление LogAn.
Trusted	Зона для подключения доверенных сетей, например, LAN-сетей. Предполагается, что через зону Trusted LogAn будет подключен в сеть, через которую межсетевые экраны UserGate будут отсылать на него журналы, а также через которую LogAn получит доступ в Интернет.

Для работы LogAn достаточно одного настроенного интерфейса. Разделение функций управления устройством и сбора данных на разные сетевые

интерфейсы рекомендовано для обеспечения безопасности, но не является жестким требованием.

Администраторы LogAn могут изменять настройки зон, созданных по умолчанию, а также создавать дополнительные зоны.

> **Примечание**
>
> **Можно создать не более 255 зон.**

Для создания зоны необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать зону	Нажать на кнопку **Добавить** и дать название зоне.
Шаг 2. Настроить параметры защиты зоны от DoS (опционально)	Указать параметры защиты зоны от сетевого флуда для протоколов TCP (SYN-flood), UDP, ICMP: • **Порог уведомления** — при превышении количества запросов с одного IP-адреса над указанным значением происходит запись события в системный журнал. • **Порог отбрасывания пакетов** — при превышении количества запросов с одного IP-адреса над указанным значением LogAn начинает отбрасывать пакеты, поступившие с этого IP-адреса, и записывает данное событие в системный журнал. Рекомендованные значения для порога уведомления — 300 запросов в секунду, для порога отбрасывания пакетов — 600 запросов в секунду. **Исключения защиты от DoS** — позволяет указать список IP-адресов серверов, которые необходимо исключить из защиты. Это может быть полезно, например, для шлюзов UserGate, которые могут слать большой объем данных на сервера LogAn.
Шаг 3. Настроить параметры контроля доступа зоны (опционально)	Указать предоставляемые LogAn сервисы, которые будут доступны клиентам, подключенным к данной зоне. Для зон, подключенных к неконтролируемым сетям, таким, как Интернет, рекомендуется отключить все сервисы. Сервисы: • **Ping** — позволяет пинговать LogAn. • **SNMP** — доступ LogAn по протоколу SNMP (UDP 161). • **XML-RPC для управления** — позволяет управлять продуктом по API (TCP 4040).

Наименование	Описание
	• **Консоль администрирования** — доступ к веб-консоли управления (TCP 8010). • **CLI по SSH** — доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200. • **Log Analyzer** — сервис анализатора журналов Log Analyzer. Необходимо разрешить на зонах, с которых LogAn будет получать данные от серверов UserGate (TCP 1269). • **Сборщик логов** — сервис для разрешения получения информации с удалённых устройств по протоколу Syslog (по умолчанию используется порт TCP 514). Подробнее о требованиях сетевой доступности читайте в приложении Требования к сетевому окружению.
Шаг 4. Настроить параметры защиты от IP-спуфинг атак (опционально)	Атаки на основе IP-спуфинга позволяют передать пакет из одной сети, например, из **Trusted**, в другую, например, в **Management**. Для этого атакующий подменяет IP-адрес источника на предполагаемый адрес необходимой сети. В таком случае ответы на этот пакет будут пересылаться на внутренний адрес. Для защиты от подобных атак администратор может указать диапазоны IP-адресов, адреса источников которых допустимы в выбранной зоне. Сетевые пакеты с адресами источников отличных от указанных будут отброшены. С помощью флага **Инвертировать** администратор может указать адреса источников, которые не могут быть получены на интерфейсах данной зоны. В этом случае будут отброшены пакеты с указанными диапазонами IP-адресов источников. Например, можно указать диапазоны "серых" IP-адресов 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0./16 и включить опцию **Инвертировать**.

Настройка интерфейсов

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

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

- Включить или отключить интерфейс.
- Указать тип интерфейса — Layer 3.

Назначить зону интерфейсу.

- Изменить физические параметры интерфейса — MAC-адрес и размер MTU.
- Выбрать тип присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP.

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

- VLAN.
- Бонд.

Объединение интерфейсов в бонд

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

Наименование	Описание
Вкл	Включает бонд.
Название	Название бонда.
Зона	Зона, к которой принадлежит бонд.
Интерфейсы	Один или более интерфейсов, которые будут использованы для построения бонда.
Режим	Режим работы бонда должен совпадать с режимом работы на том устройстве, куда подключается бонд. Может быть: • **Round robin**. Пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. Эта политика применяется для балансировки нагрузки и отказоустойчивости. • **Active backup**. Только один сетевой интерфейс из объединенных будет активным. Другой интерфейс может стать активным только в том случае, когда упадет текущий активный интерфейс. При такой политике MAC-адрес бонд-интерфейса виден снаружи только через один сетевой порт, во избежание появления проблем с коммутатором. Эта политика применяется для отказоустойчивости.

Наименование	Описание
	• **XOR**. Передача распределяется между сетевыми картами используя формулу: [(«MAC-адрес источника» XOR «MAC-адрес назначения») по модулю «число интерфейсов»]. Получается, одна и та же сетевая карта передает пакеты одним и тем же получателям. Опционально распределение передачи может быть основано и на политике «xmit_hash». Политика XOR применяется для балансировки нагрузки и отказоустойчивости. • **Broadcast**. Передает все на все сетевые интерфейсы. Эта политика применяется для отказоустойчивости. • **IEEE 802.3ad** — режим работы, установленный по умолчанию, поддерживается большинством сетевых коммутаторов. Создаются агрегированные группы сетевых карт с одинаковой скоростью и дуплексом. При таком объединении передача задействует все каналы в активной агрегации согласно стандарту IEEE 802.3ad. Выбор, через какой интерфейс отправлять пакет, определяется политикой; по умолчанию используется XOR-политика, можно также использовать «xmit_hash» политику. • **Adaptive transmit load balancing**. Исходящий трафик распределяется в зависимости от загруженности каждой сетевой карты (определяется скоростью загрузки). Не требует дополнительной настройки на коммутаторе. Входящий трафик приходит на текущую сетевую карту. Если она выходит из строя, то другая сетевая карта берет себе MAC-адрес вышедшей из строя карты. • **Adaptive load balancing**. Включает в себя предыдущую политику плюс осуществляет балансировку входящего трафика. Не требует дополнительной настройки на коммутаторе. Балансировка входящего трафика достигается путем ARP-переговоров. Драйвер перехватывает ARP-ответы, отправляемые с локальных сетевых карт наружу, и переписывает MAC-адрес источника на один из уникальных MAC-адресов сетевой карты, участвующей в объединении. Таким образом, различные пиры используют различные MAC-адреса сервера. Балансировка входящего трафика распределяется последовательно (round-robin) между интерфейсами.
MII monitoring period (мсек)	Устанавливает периодичность MII-мониторинга в миллисекундах. Определяет, как часто будет проверяться состояние линии на наличие отказов. Значение по умолчанию — 0 — отключает MII-мониторинг.

Наименование	Описание
Down delay (мсек)	Определяет время (в миллисекундах) задержки перед отключением интерфейса, если произошел сбой соединения. Эта опция действительна только для мониторинга MII (miimon). Значение параметра должно быть кратным значениям miimon. Если оно не кратно, то округлится до ближайшего кратного значения. Значение по умолчанию 0.
Up delay (мсек)	Задает время задержки в миллисекундах, перед тем как поднять канал при обнаружении его восстановления. Этот параметр возможен только при MII-мониторинге (miimon). Значение параметра должно быть кратным значениям miimon. Если оно не кратно, то округлится до ближайшего кратного значения. Значение по умолчанию 0.
LACP rate	Определяет, с каким интервалом будут передаваться партнером LACPDU-пакеты в режиме 802.3ad. Возможные значения: • **Slow** — запрос партнера на передачу LACPDU-пакетов каждые 30 секунд. • **Fast** — запрос партнера на передачу LACPDU-пакетов каждую 1 секунду.
Failover MAC	Определяет, как будут прописываться MAC-адреса на объединенных интерфейсах в режиме active-backup при переключении интерфейсов. Обычным поведением является одинаковый MAC-адрес на всех интерфейсах. Возможные значения: • **Отключено** — устанавливает одинаковый MAC-адрес на всех интерфейсах во время переключения. • **Active** — MAC-адрес на бонд-интерфейсе будет всегда таким же, как на текущем активном интерфейсе. MAC-адреса на резервных интерфейсах не изменяются. MAC-адрес на бонд-интерфейсе меняется во время обработки отказа. • **Follow** — MAC-адрес на бонд-интерфейсе будет таким же, как на первом интерфейсе, добавленном в объединение. На втором и последующем интерфейсе этот MAC не устанавливается, пока они в резервном режиме. MAC-адрес прописывается во время обработки отказа, когда резервный интерфейс становится активным, он принимает новый MAC (тот, что на бонд-интерфейсе), а старому активному интерфейсу прописывается MAC, который был на текущем активном.

Наименование	Описание
Xmit hash policy	Определяет хэш-политику передачи пакетов через объединенные интерфейсы в режиме XOR или IEEE 802.3ad. Возможные значения: • **Layer 2** — использует только MAC-адреса для генерации хэша. При этом алгоритме трафик для конкретного сетевого хоста будет отправляться всегда через один и тот же интерфейс. Алгоритм совместим с IEEE 802.3ad. • **Layer 2+3** — использует как MAC-адреса, так и IP-адреса для генерации хэша. Алгоритм совместим с IEEE 802.3ad. • **Layer 3+4** — используются IP-адреса и протоколы транспортного уровня (TCP или UDP) для генерации хэша. Алгоритм не всегда совместим с IEEE 802.3ad, так как в пределах одного и того же TCP- или UDP-взаимодействия могут передаваться как фрагментированные, так и нефрагментированные пакеты. Во фрагментированных пакетах порт источника и порт назначения отсутствуют. В результате в рамках одной сессии пакеты могут дойти до получателя не в том порядке, так как отправляются через разные интерфейсы.
Сеть	Способ присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP.

Настройка шлюзов

Для подключения LogAn к Интернету необходимо указать IP-адрес одного или нескольких шлюзов.

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

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

При наличии двух или более шлюзов возможны 2 варианта работы:

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

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

Маршруты

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

Для добавления маршрута необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Задать название и описание данного маршрута	В разделе **Сеть** выберите в меню **Маршруты**, нажмите кнопку **Добавить**. Укажите имя для данного маршрута. Опционально можно задать описание маршрута.
Шаг 2. Указать адрес назначения	Задайте подсеть, куда будет указывать маршрут, например, 172.16.20.0/24 или 172.16.20.5/32.
Шаг 3. Указать шлюз	Задайте IP-адрес шлюза, через который указанная подсеть будет доступна. Этот IP-адрес должен быть доступен с сервера LogAn.

Наименование	Описание
Шаг 4. Указать интерфейс	Выберите интерфейс, через который будет добавлен маршрут. Если оставить значение **Автоматически**, то LogAn сам определит интерфейс, исходя из настроек IP-адресации сетевых интерфейсов.
Шаг 5. Указать метрику	Задайте метрику маршрута. Чем меньше метрика, тем приоритетней маршрут в данную сеть, если маршрутов несколько.

ПОЛЬЗОВАТЕЛИ И УСТРОЙСТВА

UserID агент

Описание

UserID агент предназначен для осуществления прозрачной аутентификации на выбранных устройствах UserGate. В качестве источника данных аутентификации используются журналы Microsoft Active Directory (посредством протокола WMI) и Syslog (посредством стандартизированного протокола syslog RFC 3164, RFC 5424, RFC 6587).

Схема работы

UserID агент периодически делает запрос в базу данных для поиска событий входов/выходов пользователей. Поиск происходит только среди записей, полученных при помощи источников UserID, то есть другие записи (полученные через WMI сенсоры, конечные устройства, сборщики логов) игнорируются. По полученным данным происходит поиск пользователя в каталогах пользователей источника логов. Если пользователь найден, то данные для авторизации пользователя отправляются на все устройства NGFW, указанные в профиле редистрибуции источника. Таким образом производится авторизация пользователя на всех указанных устройствах. В случае выхода пользователя ситуация аналогична (за исключением Microsoft Active Directory, где данные о выходе пользователя на данный момент не обрабатываются). Информация о входе/выходе/ошибке сохраняется в журнал UserID.

> **Примечание**
>
> **События, полученные с источников, будут отображены в журналах UserID на рабочем столе Журналы и отчёты.**

Настройка

В общем случае для настройки сбора информации с источников необходимо выполнить следующее:

Наименование	Описание
Шаг 1. Настроить параметры агента UserID.	Настройка осуществляется в разделе **Пользователи и устройства → UserID агент**, кнопка **Настроить агент**.
Шаг 2. Настроить источник событий.	В качестве источников могут быть использованы Microsoft Active Directory или Syslog.

При настройке агента необходимо заполнить следующие поля:

Наименование	Описание
Интервал опроса (сек.)	Период опроса серверов Active Directory. Значение по умолчанию – 120 секунд.
Время жизни аутентифицированного пользователя (сек.)	Период времени, по истечении которого сессия пользователя будет завершена принудительно. Значение по умолчанию – 2700 секунд (45 минут).
Интервал мониторинга syslog (сек.)	Период опроса базы данных для поиска событий начала/завершения сеанса пользователей syslog-источников.
Ignore network list	Списки IP-адресов, события от которых будут проигнорированы агентом UserID. Запись об игнорировании источника появится в журнале **Агент UserID**. Список может быть создан в разделе **Библиотеки → IP-адреса** или при настройке агента (кнопка **Создать и добавить новый объект**). Подробнее о создании и настройке списков IP-адресов читайте в разделе IP-адреса. Данная настройка является глобальной и относится ко всем источникам.
Ignore user list	Имена пользователей, события от которых будут проигнорированы агентом UserID. Поиск производится по Common Name (CN) пользователя AD. Данная настройка является глобальной и относится ко всем источникам. Запись об игнорировании пользователя появится в журнале UserID.

Наименование	Описание
	Важно! При задании имени допустимо использовать символ астериск (*), но только в конце строки.

> **Примечание**
> **При подключении NGFW к Log Analyzer возможна одновременная работа агентов UserID, настроенных на обоих устройствах. Агенты устройств будут работать независимо друг от друга. События журналов агента UserID, полученные NGFW, как и события других журналов, будут переданы на LogAn.**

Microsoft Active Directory

В случае, если в качестве источника информации выступает Microsoft Active Directory необходимо:

Наименование	Описание
Шаг 1. Настроить параметры агента UserID для мониторинга Microsoft AD.	Параметры агента UserID были рассмотрены ранее.
Шаг 2. Настроить источник событий.	Настроить Microsoft Active Directory в качестве источника. Подробнее о параметрах источника читайте далее.

При использовании серверов AD в качестве источников событий UserGate выполняет WMI-запросы для поиска событий, связанных с успешным входом в систему (идентификатор события 4624), событий Kerberos (события с номерами: 4768, 4769, 4770) и события членства в группах (идентификатор события 4627). Периодичность выполнения запросов регулируется настройками агента UserID (параметр **Интервал опроса**). Найденные события отображаются на рабочем столе **Журналы и отчёты**, в разделе **Журналы → Конечные устройства → Журнал событий**.

При добавлении источника событий типа Microsoft Active Directory необходимо указать следующие данные:

Наименование	Описание
Включено	Включение/отключение получения журналов с источника.
Название	Название источника.

Наименование	Описание
Описание	Описание источника (опционально).
Адрес сервера	Адрес Microsoft Active Directory.
Протокол	Протокол доступа к AD (WMI).
Имя	Имя пользователя для подключения к AD.
Пароль	Пароль пользователя для подключения к AD.
Профиль редистрибуции	Профиль редистрибуции, который описывает круг устройств UserGate на который будет отправлена информация о найденных пользователях. Подробнее смотрите раздел Профиль редистрибуции.
Каталоги пользователей	Предназначена для выбора LDAP-коннектора, который используется для поиска информации о пользователях, найденных в журналах агентом UserID. Можно выбрать настроенный ранее каталог или добавить новый.

Syslog

> **Примечание**
> **Для корректной работы сборщика логов UserID, необходимо настроить сервер Syslog для отправки журналов на адрес агента UserID. Подробнее см. документацию Syslog.**

Для настройки источника событий необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Разрешить сбор информации с удалённых устройств по протоколу syslog.	В разделе **Сеть → Зоны** разрешить сервис **Сборщик логов** д ля зоны, в которой находятся сервера Syslog.
Шаг 2. Настроить параметры агента UserID для мониторинга сервера syslog.	Параметры агента UserID были рассмотрены ранее.

Наименование	Описание
Шаг 3. Настроить источник событий.	Настроить сервер Syslog в качестве источника. Подробнее о параметрах источника читайте далее.

При добавлении источника событий типа Syslog необходимо указать следующие параметры:

Наименование	Описание
Включено	Включение/отключение получения журналов с источника.
Название	Название источника.
Описание	Описание источника.
Адрес сервера	Адрес хоста, с которого UserGate будет получать события по протоколу syslog.
Домен по умолчанию	Название домена, который используется для поиска найденных в журналах syslog пользователей.
Часовой пояс	Часовой пояс, установленный на источнике.
Профиль редистрибуции	Профиль редистрибуции который описывает круг устройств UserGate на который будет отправлена информация о найденных пользователях. Подробнее смотрите раздел Профиль редистрибуции.
Фильтры	Фильтры для поиска необходимых записей журнала. Фильтры создаются и настраиваются в разделе **Библиотеки → Syslog фильтры UserID агента.** Подробнее читайте в разделе Syslog фильтры UserID агента.
Каталоги пользователей	Предназначена для выбора LDAP коннектора, который используется для поиска информации о пользователях, найденных в журналах агентом UserID. Можно выбрать настроенный ранее каталог или добавить новый.

Найденные события отображаются на рабочем столе **Журналы и отчёты**, в разделе **Журналы → Агент UserID → Syslog**.

Профили редистрибуции

Описание

Предназначены для определения круга устройств UserGate, на которые отправляется информация о найденных агентом UserID пользователях. Для добавления профиля необходимо нажать кнопку **Добавить и настроить профиль.**

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля (опционально).
Сенсоры UserGate	Список устройств UserGate, на которые будет отправлена информация о найденных пользователях. Добавление сенсоров доступно разделе **Сенсоры → Сенсоры UserGate** рабочего стола **Настройки**.

Примечание

По умолчанию создан профиль *Share with all UserGate sensors*, при выборе которого информация о пользователях будет отправлена на все сенсоры LogAn.

СЕНСОРЫ

Общие сведения

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

Сенсоры UserGate

Сенсор UserGate подключает одно устройство типа межсетевого экрана UserGate к LogAn. Для подключения сенсора UserGate необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. На узле UserGate разрешить сервисы **Log Analyzer** и **SNMP** на требуемой зоне	На узле UserGate, который вы хотите добавить в качестве сенсора, в разделе **Сеть → Зоны** выберите зону, через интерфейсы которой будет происходить сетевой обмен с сервером LogAn, и разрешите сервисы **Log Analyzer** и **SNMP**.
Шаг 2. На узле UserGate скопируйте токен в буфер обмена	На узле UserGate, который вы хотите добавить в качестве сенсора, в разделе **Настройки → Log Analyzer** скопируйте значение токена в буфер обмена. Он понадобится на шаге 4.
Шаг 3. На LogAn разрешить сервис Log Analyzer на требуемой зоне	На LogAn в разделе **Сеть → Зоны** выберите зону, через интерфейсы которой будет происходить сетевой обмен с узлом UserGate, и разрешите сервис Log Analyzer.
Шаг 4. Создайте сенсор UserGate	На сервере LogAn в разделе **Сенсоры → Сенсоры UserGate** нажмите кнопку **Добавить** и заполните необходимые поля.

При создании сенсора UserGate необходимо заполнить следующие поля:

Наименование	Описание
Включено	Включает или выключает данный сенсор UserGate.
Название	Название сенсора UserGate.
Описание	Опциональное описание сенсора UserGate.
Адрес сервера	IP-адрес узла UserGate, для которого создается данный сенсор.
Log Analyzer адрес	IP-адрес сервера LogAn, который будет использоваться на узле UserGate, в качестве назначения для отсылки журналов. Для выбора отображаются только те адреса, на интерфейсах зон которых разрешен сервис Log Analyzer.
Токен	Токен, полученный на узле UserGate.

После создания сенсора, узел UserGate начинает отсылать данные на LogAn.

> **Примечание**
> **После подключения LogAn обработка и экспорт журналов, создание отчётов и обработка других статистических данных сенсора UserGate производятся сервером LogAn.**

На узле UserGate произошли следующие изменения конфигурации:

- В разделе **Настройки → Log Analyzer** изменился адрес сервера Log Analyzer на адрес, указанный при создании сенсора UserGate.
- В разделе **Диагностика и мониторинг → Оповещения → SNMP** добавилось правило SNMP, разрешающее LogAn получать информацию по протоколу SNMP.

На LogAn добавились следующие элементы:

- В разделе **Журналы и отчеты → Журналы** появились записи с созданного сенсора UserGate.
- В **Дашборде** появилась возможность добавить новый виджет — **График сенсора UserGate**, содержащий информацию, полученную с сенсора UserGate.

> **Примечание**
> **В случае изменения администратором правила SNMP на узле UserGate, LogAn вернет настройки или пересоздаст правило при включении/отключении сенсора на сервере LogAn.**

Сенсоры SNMP

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

Для настройки сенсора SNMP необходимо выполнить следующие шаги:

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

При создании сенсора SNMP необходимо заполнить следующие поля:

Наименование	Описание
Включено	Включает или выключает данный сенсор SNMP.
Название	Название сенсора SNMP.
Описание	Опциональное описание сенсора SNMP.
Адрес сервера	IP-адрес сенсора SNMP.
Порт	Порт сенсора SNMP. Обычно для запросов данных по протоколу SNMP используется порт TCP 161.
Версия	Указывает версию протокола SNMP, которая будет использоваться в данном сенсоре. Возможны варианты SNMP v2 и SNMP v3.
Community	SNMP community — строка для идентификации сервера LogAn и сетевого устройства для версии SNMP v2. Используйте только латинские буквы и цифры.
Интервал опроса (сек)	Интервал, через который сервер LogAn будет инициировать получение данных с сетевого устройства.
Пользователь	Только для SNMP v3. Имя пользователя для аутентификации на сетевом устройстве.
Тип аутентификации	Выбор режима аутентификации. Возможны варианты: • Без аутентификации, без шифрования (noAuthNoPriv). • С аутентификацией, без шифрования (authNoPriv). • С аутентификацией, с шифрованием (authPriv). Наиболее безопасным считается режим работы authPriv.

Наименование	Описание
Алгоритм аутентификации	Алгоритм, используемый для аутентификации.
Пароль аутентификации	Пароль, используемый для аутентификации.
Алгоритм шифрования	Алгоритм, используемый для шифрования. Возможно использовать DES и AES.
Пароль шифрования	Пароль, используемый для шифрования.
Счётчики	Укажите здесь все требуемые данные, которые LogAn будет запрашивать на сетевом устройстве. Счетчики выбираются из баз MIB, которые загружены на устройство. Выберите в дереве SNMP необходимый раздел и добавьте соответствующий счетчик либо укажите в строке SNMP OID счетчика и его тип.

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

Управление SNMP MIB

В данном разделе администратор может добавлять и удалять базы MIB (Management Information Base) на LogAn.

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

Сенсоры WMI

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

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

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

Конечные устройства

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

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

Отображена следующая информация:

- Название конечного устройства, заданное на UGMC.
- Версия ПО UserGate Client, установленная на устройстве.
- Время последнего подключения к устройству.

- IP-адрес устройства.
- Netbios имя.
- Версия операционной системы (ОС) устройства.
- Телеметрическая информация.

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

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

Коннекторы

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

Для добавления коннектора необходимо указать следующие данные:

Наименование	Описание
Имя	Название коннектора.
Описание	Описание коннектора (опционально).
Тип сервера	Выбор типа сервера: • **SSH**. • **HTTP**. • **HTTPS** (в текущей версии реализован только для интеграции с ГосСОПКА).
Адрес сервера	

Наименование	Описание
	Тип: • **IP**. • **FQDN**.
IP-адрес	IP-адрес сервера; указывается в случае выбора адреса сервера типа **IP**.
Порт	Порт сервера; указывается в случае выбора адреса сервера типа **IP**.
FQDN	FQDN сервера; указывается в случае выбора адреса сервера типа **FQDN**.
URL-путь	Используется при управлении устройством по API.
Логин	Логин пользователя для авторизации на коннекторе.
Пароль	Пароль учётной записи пользователя, необходимый для авторизации на коннекторе.
Группа команд	Указание группы команд доступно только для SSH-сервера, подробнее читайте в разделе Команды.
HTTP заголовки	Указание заголовков доступно только для серверов HTTP и HTTPS.

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

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

СБОРЩИК ЛОГОВ

Описание

Сборщик логов предназначен для централизованного сбора информации с сетевых устройств, что помогает облегчить мониторинг сети, виртуальных машин, серверов, пользовательских устройств, приложений.

Syslog

В данном разделе настраиваются правила сбора событий системных журналов Unix-систем (syslog), которые содержат информацию о работе системы, её состоянии и безопасности, наличии ошибок, сбоях в работе. Правила syslog позволяют осуществлять фильтрацию записей событий (по времени, критичности событий, объектам, названию устройств, приложениям), упрощая поиск необходимой информации.

Для работы сборщика логов необходимо настроить сервер, с которого будет происходить сбор информации, и правила syslog.

Для настройки сервера необходимо в веб-консоли администратора перейти в раздел **Сборщик логов → Syslog**, нажать кнопку **Настроить сервер** и указать следующие данные в открывшемся окне **Настройки syslog**:

Наименование	Описание
Включено	Включение/отключение приёма syslog событий.
Протокол	Сетевой протокол, использующийся для сбора информации: • TCP. • UDP.
Порт	Номер порта, использующегося для сбора syslog событий. По умолчанию — порт 514.
Максимальное количество сессий	Максимальное количество устройств, подключённых одновременно с целью отправки сообщений.
Безопасное соединение	Включение/отключение шифрования потока данных. Подробнее об использовании TLS в Syslog читайте в соответствующей документации.

Наименование	Описание
Файл сертификата УЦ	Сертификат удостоверяющего центра (центра сертификации), который используется для установления безопасного соединения.
Файл сертификата	Сертификат, сгенерированный пользователем и подписанный центром сертификации (ЦС); необходимо указать при настройке безопасного соединения.
Разрешённые соседи	Список устройств, с которых LogAn будет получать информацию в случае использования безопасного соединения.

Для настройки правил фильтрации записей событий syslog необходимо указать следующие данные:

Наименование	Описание
Включено	Включение/отключение правила syslog.
Название	Название правила syslog.
Описание	Описание правила syslog (опционально).
Действие	Действие: • **Разрешить** — разрешение приёма сообщений, подходящих под условия правила. • **Запретить** — блокировка приёма сообщений, подходящих под условия правила.
Часовой пояс	Часовой пояс, настроенный на удалённых устройствах. Приём сообщений будет разрешён или запрещён с устройств, у которых сохранение записей происходит в указанном часовом поясе.
Вставить	Место вставки создаваемого правила в списке правил: наверх, вниз или выше выбранного существующего правила.
Критичность	Критичность событий syslog: • **Экстренная**: критическое состояние, которое сказывается на работоспособности системы. • **Тревога**: состояние, требующее незамедлительного вмешательства.

Наименование	Описание
	• **Критическая**: состояние, требующее незамедлительного вмешательства либо предупреждающее о сбое в системе. • **Ошибки**: сообщения о сбоях в системе. • **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 уведомления. • **Отладочная**: информация, полезная разработчикам для отладки приложений.
Объект	Категория события: • **Сообщения ядра**. • **Сообщения пользовательские**. • **Почтовая система**. • **Системный сервис**. • **Безопасность/авторизация**. • **Сообщения syslog**. • **Система печати LPR**. • **Система сетевых новостей**. • **Подсистема UUCP**. • **Сервис времени**. • **Безопасность/аутентификация**. • **FTP сервис**. • **Система NTP**. • **Аудит**. • **Тревога**. • **Сервис времени 2**. • **Local 0 — Local 7**.
Имя хоста	Название устройства.
Название приложения	Название приложения, сбор информации о котором необходимо разрешить/запретить. Подробнее читайте в разделе Приложения syslog.

Записи событий будут отображены в журнале **Syslog**, подробнее читайте в разделе Системный журнал.

БИБЛИОТЕКИ

IP-адреса

Раздел **IP-адреса** содержит список диапазонов IP-адресов, которые используются в настройках зон и UserID. Для добавления нового списка адресов необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать список.	На панели **Группы** нажать на кнопку **Добавить**, дать название списку IP-адресов.
Шаг 2. Указать адрес обновления списка (не обязательно).	Указать адрес сервера, где находится обновляемый список. Более подробно об обновляемых списках смотрите далее в этой главе.
Шаг 3. Добавить IP-адреса.	На панели **Адреса из выбранной группы** нажать на кнопку **Добавить** и ввести адреса. IP-адреса вводятся в виде IP-адрес, IP-адрес/маска сети или диапазон IP-адресов, например: 192.168.1.5, 192.168.1.0/24 или 192.168.1.5-192.168.2.100.

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

Наименование	Описание

Шаг 1. Создать файл с необходимыми IP-адресами.	Создать файл **list.txt** со списком адресов.
	Список адресов записывается в обычный текстовый файл, где адреса прописываются в столбик без знаков препинания. Например:
	`x.x.x.x`
	`y.y.y.y`
	`z.z.z.z`

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

Наименование	Описание
	• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

Почтовые адреса

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

Для добавления новой группы почтовых адресов необходимо выполнить следующие шаги:

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

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

Наименование	Описание
Шаг 1. Создать файл с необходимыми списком почтовых адресов.	Создать файл **list.txt** со списком почтовых адресов.
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем **list.zip**.
Шаг 3. Создать файл с версией списка.	Создать файл **version.txt**, внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.

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

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

Номера телефонов

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

Для добавления новой группы телефонных номеров необходимо выполнить следующие шаги:

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

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

Наименование	Описание
Шаг 1. Создать файл с необходимыми списком номеров.	Создать файл **list.txt** со списком номеров.
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем **list.zip**.
Шаг 3. Создать файл с версией списка.	Создать файл **version.txt**, внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте **list.zip** и **version.txt**, чтобы они были доступны для скачивания.
Шаг 5. Создать список телефонных номеров и указать URL для обновления.	На каждом UserGate создать список номеров. При создании указать тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. UserGate будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно.

Наименование	Описание
	• Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

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

Команды

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

Для создания группы команд необходимо указать следующие параметры:

Наименование	Описание
Шаг 1. Создать список команд.	На панели **Группы команд** нажать на кнопку **Добавить**, задать название списка, описание и тип списка.
Шаг 2. Указать адрес обновления списка (не обязательно).	В случае создания обновляемого списка указать адрес сервера обновления. Более подробно об обновляемых списках смотрите далее в этой главе.

Наименование	Описание
Шаг 3. Добавить команды в группу.	На панели **Команды** нажать на кнопку **Добавить** и указать название и текст команды. Для определения переменных необходимо использовать фигурные скобки ({}). Далее переменные будут использованы для подстановки актуальных значений.

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

Наименование	Описание
Шаг 1. Создать файл с необходимыми списком команд.	Создать файл **list.txt** со списком команд.
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем **list.zip**.
Шаг 3. Создать файл с версией списка.	Создать файл **version.txt**, внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте **list.zip** и **version.txt**, чтобы они были доступны для скачивания.
Шаг 5. Создать список команд и указать URL для обновления.	На каждом UserGate создать список. При создании указать тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. UserGate будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца:

Наименование	Описание
	1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

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

Профили оповещений

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

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

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

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.

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

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

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

Категории срабатываний

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

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

Внешние сервисы обогащений

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

Чтобы использовать сервисы обогащения их необходимо включить. Для использования некоторых сервисов обогащения необходимо прохождение регистрации и предоставление ключа доступа.

Наименование	Описание
dnsgoogle	Интернет-сервис компании Google, представляющий собой общедоступные DNS-серверы. Подробнее: https://dns.google. Предназначен для типов улик: IP.
urlhaus	

Наименование	Описание
	Проект abuse.ch. Целью проекта является сбор, отслеживание и обмен URL-адресами вредоносных программ. Подробнее: https://urlhaus.abuse.ch/. Предназначен для типов улик: Домен, Хэш, Имя хоста, IP, URL.
dshield	Система корреляции журналов межсетевого экрана для совместной работы. Система получает журналы от добровольцев со всего мира и использует их для анализа тенденций атак. Подробнее: https://www.dshield.org/xml.html. Предназначен для типов улик: Домен, FQDN, IP.
cybercrime	Сервис предоставляет информацию об уровнях угрозы разных объектов. Подробнее: http://cybercrime-tracker.net. Предназначен для типов улик: Домен, FQDN, IP, URL, Другое.
cyberprotect	Сервис предоставляет информацию об уровнях угрозы разных объектов. Подробнее: https://console.threatscore.cyberprotect.cloud/. Предназначен для типов улик: Домен, Хэш, IP, URL, Агент пользователя.
unshorten	Сервис предоставляет возможности предварительного просмотра целевого URL для любого короткого URL и проверки безопасности на вредоносные ссылки. Сервис не использует внешний ресурс; анализирует ответ на запрос по тестируемому URL. Предназначен для типов улик: URL.
ipwhois	Сервис позволяет получить информацию об IP-адресах. Подробнее: https://ipwhois.io/. Предназначен для типов улик: IP.
ipinfo	Инструмент для определения владельца, Интернет-провайдера и местонахождения веб-сайта, домена или IP-адреса. Подробнее: https://ipinfo.io/. Предназначен для типов улик: IP. Для использования сервиса необходимо ввести реквизиты.
hashdd	

Наименование	Описание
	Сервис предоставляет базу вредоносных хэшей файлов и различные проверки для получения полного представления об угрозе. Подробнее: https://hashdd.com/. Предназначен для типов улик: Хэш. Для использования сервиса необходимо ввести реквизиты.
urlscan	Сервис для получения информации о подозрительных, вредоносных и фишинговых URL. Подробнее: https://urlscan.io/. Предназначен для типов улик: Домен, FQDN, Хэш, IP, URL. Для использования сервиса необходимо ввести реквизиты.
emailrep	Система, которая собирает данные об адресах электронной почты, доменах и пользователях. Подробнее: https://emailrep.io/. Предназначен для типов улик: Почта. Для использования сервиса необходимо ввести реквизиты.
greynoise	Компания занимается анализом фонового шума Интернета (пакеты данных, адресованные IP-адресам или портам, где нет сетевого устройства, настроенного для их приёма). Благодаря такой фильтрации снижается количество ложных срабатываний. Подробнее: https://www.greynoise.io/. Предназначен для типов улик: IP. Для использования сервиса необходимо ввести реквизиты.
abuseip	Проект, который занимается борьбой со злоумышленной деятельностью. Подробнее: https://www.abuseipdb.com/. Предназначен для типов улик: IP. Для использования сервиса необходимо ввести реквизиты.
hybridanalysis	Сервис проверки файлов на вредоносность. Подробнее: https://www.hybrid-analysis.com/. Предназначен для типов улик: Хэш. Для использования сервиса необходимо ввести реквизиты.

Приложения syslog

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

Чтобы добавить приложение необходимо выполнить следующие действия:

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

Syslog фильтры UserID агента

При использовании Syslog в качестве источников событий UserGate производит фильтрацию событий в соответствии с указанными Syslog фильтрами UserID агента. Фильтры Syslog представляют из себя стандартные Regexp выражения, которые пользователь может писать и сам. В стандартной поставке представлены два вида фильтров:

Наименование	Описание
SSH Authentication	Фильтр предназначенный для отслеживания событий входа/выхода пользователей по протоколу SSH в журналах syslog.
Unix PAM Authentication	Фильтр предназначенный для отслеживания событий входа/выхода пользователей посредством технологии **Pluggable Authentication Modules** (PAM) в журналах syslog.
Unix PAM Authentication	Фильтр предназначенный для отслеживания событий входа/выхода пользователей посредством технологии **Pluggable Authentication Modules** (PAM) в журналах syslog.

Примечание

Используя правила Regexp, возможно написание дополнительных правил. Таким образом фильтры Syslog представляют из себя универсальный инструмент, который можно использовать практически в любых случаях.

Найденные события отображаются во вкладке **Журналы и отчёты**, в разделе **Журналы → Агент UserID → Syslog**.

ДИАГНОСТИКА И МОНИТОРИНГ

Маршруты

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

- **Подключенные к интерфейсам** — маршруты к сетям, которые подключены непосредственно к интерфейсам UserGate. Данные маршруты будут помечены символом **C** в списке маршрутов.
- **Заданные статически** — маршруты, заданные статически в разделе **Сеть → Маршруты**. Данные маршруты будут помечены символом **S** в списке маршрутов.
- **OSPF** — маршруты, полученные по протоколу OSPF. Данные маршруты будут помечены символом **O** в списке маршрутов.
- **BGP** — маршруты, полученные по протоколу BGP. Данные маршруты будут помечены символом **B** в списке маршрутов.

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

Ping

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

Наименование	Описание
Ping host	Хост, который необходимо проверить.

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

Traceroute

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

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

Запрос DNS

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

Наименование	Описание
DNS-запрос (хост)	DNS имя для проверки.
IP источника запроса	Один из IP-адресов, назначенных UserGate.

Наименование	Описание
DNS сервер	DNS сервер, куда посылать запрос.
Порт	UDP порт, используемый для запроса.
Тип DNS-запроса	Тип запроса.

ОПОВЕЩЕНИЯ

Правила оповещений

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

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

При добавлении правила необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает данное правило.
Название	Название правила.
Описание	Описание правила.

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

SNMP

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

Для настройки мониторинга с помощью SNMP необходимо:

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

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

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

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

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

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

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

Для скачивания доступны следующие MIB-файлы:

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

UTM-TRAPS-MIB

Наименование	Описание
trapCoreCrush	Сбой ядра.
trapStatDown	Сервис статистики (UserGate Log Analyzer) недоступен.
trapCoreBootstrapEnd	Загрузка сервера завершена успешно.
trapDefaultGatewayChanged	Изменение шлюза по умолчанию.
trapHighSessionsCounter	Таблица сессий заполнена на 90%.

Наименование	Описание
trapHighUsersCounter	Количество активных пользователей достигло 90% от порога лицензии.
trapDataPartitionFSStatus	Стутус файловой системы. Состояние файловой системы изменилось на "not_clean".
trapStatusChanged	Изменение статуса узла отказоустойчивого кластера.
trapMemberUp	Статус узла отказоустойчивого кластера изменился на «Подключен».
trapMemberDown	Узел отказоустойчивого кластера отключен.
trapAttackDetected	Обнаружение атаки системой СОВ.
trapChecksumFailed	Нарушение целостности бинарных файлов.
trapHighCPUUsage	Высокая загрузка центрального процессора.
trapLowMemory	Высокая загрузка памяти.
trapLowLogdiskSpace	Недостаточно места на диске для хранения журналов.
trapRaidStatus	Изменение статуса RAID.
trapPowerSupply	Первый источник питания отключен.
trapCableStatus	Кабель был подключен или отключен от интерфейса.
trapHighDiskIOUtilization	Высокая загрузка диска. Оповещение отправляется при загруженности >=95% за 5 минут хотя бы на одном из дисковых устройств.
trapTrafficDrop	Срабатывание запрещающего правила межсетевого экрана.
trapLDAPServerDown	Сервер LDAP недоступен.
trapCriticalTemperature	Критическая температура на одном из сенсоров. Оповещение отправляется при пересечении одного из пределов рабочей температуры (нижнего или верхнего). Нижний предел рабочей температуры обычно равен 0°C (для устройств серии X -40°C), верхний предел равен 85°C.

UTM-TRAPS-BINDINGS-MIB

Наименование	Тип данных	Описание
utmSessions	integer	Текущее количество активных сессий.
utmSessionsMax	integer	Максимальное количество активных сессий.
utmUsers	integer	Количество активных пользователей на данный момент.
utmUsersMax	integer	Максимальное количество активных пользователей.
utmDataPartionFSStatus	integer	Состояние файловой системы. • **0** — clean. • **1** — not clean.
utmHAStatus	integer	Текущий статус узла кластера отказоустойчивости: • **0** — master-узел. • **1** — slave-узел. • **3** — fault.
utmHAStatusReason	integer	Причина изменения статуса узла отказоустойчивого кластера: • **1** — связь с узлом потеряна. • **2** — HTTP прокси-сервер недоступен. • **3** — ни один из шлюзов недоступен. • **4** — DNS-сервер недоступен. • **5** — узел UserGate Management Center недоступен.
utmCPUUsage	integer	Загруженность центрального процессора (%).

Наименование	Тип данных	Описание
utmMemory	integer	Использование оперативной памяти (%).
utmLogdiskSpace	integer	Пространство на диске, используемое под журналы (%).
utmAdaptecRaidStatus	integer	Текущий статус RAID (Redundant Array of Independent Disks), построенного на контроллере Adaptec: • **no_raid**. • **0** — optimal — массив в оптимальном состоянии. • **1** — degraded — полный или частичный выход из строя одного из дисков. • **2** — rebuild — восстановление массива.
utmBroadcomRaidStatus	integer	Текущий статус RAID (Redundant Array of Independent Disks), построенного на контроллере Broadcom: • **no_raid** • **0** — optimal — массив в оптимальном состоянии. • **1** — degraded — полный или частичный выход из строя одного из дисков. Переход в данный статус произойдёт при выходе из строя 2-х дисков. • **2** — partialDegraded — полный или частичный выход из

Наименование	Тип данных	Описание
		строя одного из дисков. • **3** — failed — не работает из-за наличия ошибки. • **4** — offline — диск не доступен для RAID-контроллера.
utmPowerSupply	integer	Количество источников питания: • **1** — один блок питания. • **2** — два блока питания.
utmPowerSupplyStatus	integer	Состояние источника питания: • **no_power_supplies**. • **0** — off. • **1** — on.
utmCSCIfName	string	Название интерфейса.
utmCSCStatus	integer	Статус сетевого адаптера: • **1** — кабель подключен. • **2** — кабель не подключен.
utmDiskIOUtilization	integer	Текущая утилизация диска (%).
utmLDAPServerName	string	Название LDAP-сервера.
utmLDAPServerAddress	string	IP-адрес LDAP-сервера.
utmThermSensor	string	Название температурного сенсора.
utmThermValue	integer	Значение температуры, измеренное сенсором.

UTM-MIB

Наименование	Тип данных	Описание
vcpuCount	integer	Количество виртуальных процессоров в системе.
vcpuUsage	integer	Загруженность виртуальных процессоров системы; отображается в %.
usersCounter	integer	Количество активных пользователей на текущий момент времени. (*)
sessionsCounter	integer	Количество активных сессий на текущий момент времени. (*)
tcpsessionsCounter	integer	Количество активных TCP сессий на текущий момент времени. (*)
udpsessionsCounter	integer	Количество активных UPD сессий на текущий момент времени. (*)
icmpsessionsCounter	integer	Количество активных ICMP сессий на текущий момент времени. (*)
sessionsRate10	integer	Количество новых сессий в секунду. Среднее значение за последние 10 секунд. (*)
sessionsRate60	integer	Количество новых сессий в секунду. Среднее значение за последние 60 секунд. (*)
sessionsRate300	integer	Количество новых сессий в секунду. Среднее значение за последние 300 секунд. (*)
tcpsessionsRate10	integer	Количество новых TCP сессий в секунду. Среднее значение за последние 10 секунд. (*)
tcpsessionsRate60	integer	Количество новых TCP сессий в секунду. Среднее значение за последние 60 секунд. (*)

Наименование	Тип данных	Описание
tcpsessionsRate300	integer	Количество новых TCP сессий в секунду. Среднее значение за последние 300 секунд. (*)
udpsessionsRate10	integer	Количество новых UPD сессий в секунду. Среднее значение за последние 10 секунд. (*)
udpsessionsRate60	integer	Количество новых UPD сессий в секунду. Среднее значение за последние 60 секунд. (*)
udpsessionsRate300	integer	Количество новых UPD сессий в секунду. Среднее значение за последние 300 секунд. (*)
icmpsessionsRate10	integer	Количество новых ICMP сессий в секунду. Среднее значение за последние 10 секунд. (*)
icmpsessionsRate60	integer	Количество новых ICMP сессий в секунду. Среднее значение за последние 60 секунд. (*)
icmpsessionsRate300	integer	Количество новых ICMP сессий в секунду. Среднее значение за последние 300 секунд. (*)
dnsRequestCounter	integer	Общее количество DNS запросов. (*)
dnsBlockedRequestCounter	integer	Количество заблокированных DNS запросов. (*)
dnsRequestRate	integer	Количество DNS запросов в секунду. (*)
httpRequestCounter	integer	Общее количество HTTP запросов. (*)

Наименование	Тип данных	Описание
httpBlockedRequestCounter	integer	Количество заблокированных HTTP запросов. (*)
httpRequestRate	integer	Количество HTTP запросов в секунду. (*)
dataPartitionFSStatus	string	Состояние файловой системы.
haStatus	integer	Текущее состояние узла кластера.
cpuLoad	integer	Загруженность центрального процессора системы; отображается в %.
memoryUsed	integer	Использование оперативной памяти; отображается в %.
logDiskSpace	integer	Пространство на диске, используемое под журналы; отображается в %.
powerSupply1Status	string	Состояние первого источника питания: • **no_power_supplies**. • **on**. • **off**.
powerSupply2Status	string	Состояние второго источника питания: • **no_power_supplies**. • **on**. • **off**.
raidType	string	Тип RAID массива.
raidStatus	string	Текущий статус RAID (Redundant Array of Independent Disks): • **no_raid**.

Наименование	Тип данных	Описание
		• **0** — optimal — массив в оптимальном состоянии. • **1** — degraded — полный или частичный выход из строя одного из дисков. • **2** — rebuild — восстановление массива.
diskIOUtilization	integer	Текущая утилизация диска (%).
diskIOUtilization60	integer	Утилизация диска (%). Среднее значение за последние 60 секунд.
diskIOUtilization300	integer	Утилизация диска (%). Среднее значение за последние 300 секунд.

Примечание

Метрики, отмеченные в описании символом (*) не актуальны для *UGMC* и *LogAn*.

Значения метрик для этих устройств будут всегда равны нулю.

UTM-INTERFACES-MIB

Наименование	Тип данных	Описание
ifNumber	integer	Количество сетевых интерфейсов.
ifIndex	integer	Значение уникально для каждого интерфейса и может принимать значения от 1 до ifNumber.
ifDescr	string	Описание интерфейса.
ifType	integer	Тип интерфейса, определённый в соответствии с протоколом

Наименование	Тип данных	Описание
		физического/канального уровней: • **1** — other — неизвестный тип. • **2** — regular1822 — определён в BBN Report 1822. • **3** — hdh1822 — определён в BBN Report 1822. • **4** — ddn-x25 — определён в BBN Report 1822. • **5** — определён в стандарте канального уровня сетевой модели OSI X.25. • **6** — ethernet-csmacd — сетевой интерфейс типа Ethernet, независимо от скорости (определён в RFC 3635). • **7** — iso88023-csmacd — определён в IEEE 802.3. • **8** — iso88024-tokenBus — определён в стандарте IEEE 8802.4. • **9** — iso88025-tokenRing — сетевой интерфейс использует подключение Token Ring; определяется в стандарте IEEE 802.5. • **10** — iso88026-man — определён в стандарте ISO 88026 "MAN". • **11** — starLan — определён в стандарте IEEE 802.3e. • **12** — proteon-10Mbit — Proteon 10 Mbit • **13** — proteon-80Mbit — Proteon 80 Mbit.

Наименование	Тип данных	Описание
		• **14** — hyperchannel — высокоскоростной канал, используемы в сети ISDN. • **15** — fddi — сетевой интерфейс использует подключение FDDI (Fiber Distributed Data Interface). FDDI — это набор стандартов передачи данных по оптоволоконным линиям в локальной сети. • **16** — lapb — протокол канального уровня, используемым для передачи пакетов стандарта X.25. • **17** — sdlc — протокол канального уровня для системной сетевой архитектуры IBM. • **18** — ds1 — способен обрабатывать 24 одновременных соединения на общей скорости 1,544 Мбит/с; также называется T1 • **19** — e1 — европейский аналог T1. • **20** — basicISDN — для связи аппаратуры абонента и ISDN-станции. • **21** — primaryISDN — используется для подключения к широкополосным магистралям, связывающим местные и центральные АТС или сетевые коммутаторы. • **22** — propPointToPointSeri

Наименование	Тип данных	Описание
		al — определён в стандарте RFC1213. • **23** — ppp — сетевой интерфейс использует подключение PPP (Point-To-Point Protocol). • **24** — softwareLoopback — сетевой интерфейс является петлевым адаптером. Такие интерфейсы часто используются для тестирования; они не отправляют трафик в сеть. • **25** — eon — ConnectionLess Network Protocol (CLNP) over Internet Protocol (IP); определён в ISO/IEC 8473-1. • **26** — ethernet-3Mbit — сетевой интерфейс использует подключение Ethernet со скоростью 3 Мбит/с. Эта версия Ethernet определяется в стандарте IETF RFC 895. • **27** — nsip — XNS over IP — предназначен для использования в разнообразных средах передачи данных. • **28** — slip — сетевой интерфейс использует подключение SLIP (Serial Line Internet Protocol). SLIP определяется в стандарте IETF RFC 1055. • **29** — ultra — ULTRA Technologies.

Наименование	Тип данных	Описание
		• **30** — ds3 — высокоскоростной интерфейс передачи данных, сформированный мультиплексированием сигналов DS1 и DS2; также называется T3. • **31** — sip — сетевой интерфейс использует подключение SLIP (Serial Line Internet Protocol). SLIP определяется в стандарте IETF RFC 1055. • **32** — frame-relay — обеспечивает возможность передачи данных с коммутацией пакетов через интерфейс между устройствами пользователя и оборудованием сети.
ifMtu	integer	Максимальный размер пакета сетевого уровня, который можно послать через этот интерфейс.
ifSpeed	gauge32	Пропускная способность интерфейса в битах в секунду.
ifPhysAddress	string	Физический адрес интерфейса (MAC-адрес).
ifAdminStatus	integer	Состояние интерфейса, назначаемое администратором: • **1** — up — готов для передачи пакетов. • **2** — down — не работает. • **3** — testing — в режиме тестирования;

Наименование	Тип данных	Описание
		рабочие пакеты не могут быть переданы.
ifOperStatus	integer	Текущий статус работы интерфейса: • **1** — up — интерфейс готов для передачи пакетов. • **2** — down — интерфейс не может передавать пакеты данных. • **3** — testing — выполняется тестирование сетевого интерфейса; рабочие пакеты не могут быть переданы. • **4** — unknown — интерфейс находится в неизвестном состоянии. • **5** — dormant — сетевой интерфейс не может передавать пакеты данных, он ожидает внешнее событие. • **6** — notPresente — сетевой интерфейс не может передавать пакеты данных из-за отсутствующего компонента, обычно аппаратного. • **7** — lowerLayerDown — сетевой интерфейс не может передавать пакеты данных, потому что он работает поверх одного или нескольких других интерфейсов, и не менее одного из этих интерфейсов "нижнего уровня" не работает.

Наименование	Тип данных	Описание
ifLastChange	timeticks	Значение SysUpTime, когда интерфейс оказался в данном состоянии.
ifInOctets	counter32	Количество байтов, принятое данным интерфейсом, включая служебные.
ifInUcastPkts	counter32	Количество доставленных пакетов одноадресной рассылки.
fInNUcastPkts	counter32	Количество доставленных многоадресных и широковещательных пакетов.
ifInDiscards	counter32	Количество входящих пакетов, которые были отброшены, даже если не было обнаружено ошибок, препятствующих их доставке. Одна из возможных причин отбрасывания: освобождение буферного пространства.
ifInErrors	counter32	Количество входящих пакетов, которые содержат ошибки, препятствующие их доставке.
ifInUnknownProtos	counter32	Количество пакетов, которые были получены через этот интерфейс и отброшены из-за использования неизвестного или неподдерживаемого протокола.
ifOutOctets	counter32	Количество байтов, переданное данным интерфейсом, включая служебные.
ifOutUcastPkts	counter32	Количество отправленных пакетов одноадресной

Наименование	Тип данных	Описание
		рассылки, включая пакеты, которые были отброшены или не отправлены.
ifOutNUcastPkts	counter32	Количество отправленных многоадресных и широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены.
ifOutDiscards	counter32	Количество исходящих пакетов, которые были отброшены, даже если не было обнаружено ошибок, препятствующих их передачи. Одна из возможных причин отбрасывания: освобождение буферного пространства.
ifOutErrors	counter32	Количество исходящих пакетов, передача которых невозможна вследствие наличия ошибок.
ifOutQLen	gauge32	Длина выходной очереди (в пакетах).
ifInMulticastPkts	counter32	Количество доставленных пакетов многоадресной рассылки.
ifInBroadcastPkts	counter32	Количество доставленных широковещательных пакетов.
ifOutMulticastPkts	counter32	Количество отправленных пакетов многоадресной рассылки, включая пакеты, которые были отброшены или не отправлены.
ifOutBroadcastPkts	counter32	Количество отправленных широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены.

Наименование	Тип данных	Описание
ifHCInOctets	counter64	Смысл одинаков со смыслом объекта **ifInOctets** — количество байтов, принятое данным интерфейсом, включая служебные; используется счётчик большей ёмкости.
ifHCInUcastPkts	counter64	Смысл одинаков со смыслом объекта **ifInUcastPkts** — количество доставленных пакетов одноадресной рассылки; используется счётчик большей ёмкости.
ifHCInMulticastPkts	counter64	Смысл одинаков со смыслом объекта **ifInMulticastPkts** — количество доставленных пакетов многоадресной рассылки; используется счётчик большей ёмкости.
ifHCInBroadcastPkts	counter64	Смысл одинаков со смыслом объекта **ifInBroadcastPkts** — количество доставленных широковещательных пакетов; используется счётчик большей ёмкости.
ifHCOutOctets	counter64	Смысл одинаков со смыслом объекта **ifOutOctets** — количество байтов, переданное данным интерфейсом, включая служебные; используется счётчик большей ёмкости.
ifHCOutUcastPkts	counter64	Смысл одинаков со смыслом объекта **ifOutUcastPkts** — количество отправленных пакетов одноадресной рассылки, включая пакеты, которые были отброшены или не отправлены; используется счётчик большей ёмкости.
ifHCOutMulticastPkts	counter64	Смысл одинаков со смыслом объекта **ifOutMulticastPkts**

Наименование	Тип данных	Описание
		— количество отправленных пакетов многоадресной рассылки, включая пакеты, которые были отброшены или не отправлены; используется счётчик большей ёмкости.
ifHCOutBroadcastPkts	counter64	Смысл одинаков со смыслом объекта **ifOutBroadcastPkts** — количество отправленных широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены; используется счётчик большей ёмкости.
ifLinkUpDownTrapEnable	integer	Указывает, должен ли создаваться трап при изменении статуса соединения: • **1** — enabled — включено. • **2** — disabled — отключено.
ifHighSpeed	gauge32	Оценка текущей полосы пропускания интерфейса; указывается в бит/с, кбит/с, Мбит/с, Гбит/с.
ifPromiscuousMode	integer	"Неразборчивый" режим. Может принимать значения: • **1** — true — станция принимает все пакеты/кадры независимо от того, кому они адресованы. • **2** — false — интерфейс принимает только пакеты/кадры, адресованные этой станции. Значение объекта не влияет на приём широковещательных и

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

UTM-TEMPERATURE-MIB

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

Примечание

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

Примечание

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

Параметры SNMP

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

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

Наименование	Описание
	• MAC-адрес (mac). • Текст (text). • Октеты (jctets).

Профили безопасности SNMP

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

Примечание

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

Наименование	Описание
Название	Название профиля безопасности SNMP
Описание	Описание профиля безопасности SNMP
Пользователь	Имя пользователя для аутентификации SNMP-менеджера.
Тип аутентификации	Выбор режима аутентификации SNMP-менеджера. Возможны варианты: • Без аутентификации, без шифрования (noAuthNoPriv). • С аутентификацией, без шифрования (authNoPriv). • С аутентификацией, с шифрованием (authPriv). Наиболее безопасным считается режим работы authPriv.

Наименование	Описание
Алгоритм аутентификации	Алгоритм, используемый для аутентификации. Возможно использовать: • SHA1; • MD5; • SHA224; • SHA256; • SHA384; • SHA512.
Пароль аутентификации	Пароль, используемый для аутентификации.
Алгоритм шифрования	Алгоритм, используемый для шифрования. Возможно использовать DES и AES.
Пароль шифрования	Пароль, используемый для шифрования.

ЖУРНАЛЫ И ОТЧЕТЫ

ЖУРНАЛЫ

Описание

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

- **Журнал событий** — содержит события, связанные с изменением настроек сервера LogAn, авторизацией пользователей, администраторов, обновлениями различных списков и т.п.
- **Журнал веб-доступа** — подробный журнал всех веб-запросов, обработанных LogAn.
- **Журнал DNS** — содержит события, связанные с DNS трафиком.
- **Журнал трафика** — подробный журнал срабатываний правил межсетевого экрана, NAT, DNAT, Port forwarding, Policy-based routing. Для регистрации

данных событий необходимо включить журналирование в необходимых правилах межсетевого экрана, NAT, DNAT, Port forwarding, Policy-based routing.

- **Журнал СОВ** — содержит события, регистрируемые системой обнаружения и предотвращения вторжений.
- **Журнал АСУ ТП** — содержит события, регистрируемые правилами контроля АСУ ТП.
- **Журнал инспектирования SSH** — журнал срабатывания правил инспектирования SSH. Для регистрации данных событий необходимо включить журналирование.
- **История поиска** — содержит поисковые запросы пользователей в популярных поисковых системах.
- **Журнал событий конечных устройств** — отображает события, получаемые от контролируемых с помощью программного обеспечения UserGate Endpoint конечных устройств.
- **Журнал правил конечных устройств** — события срабатывания правил межсетевого экрана конечных устройств, в настройках которых включено журналирование.
- **Приложения конечных устройств** — отображает приложения, которые когда-либо запускались на конечных устройствах.
- **Аппаратура конечных устройств** — содержит информацию об устройствах, подключённых к конечным устройствам.
- **Системный журнал** (**Syslog**) — отображены записи сообщений о событиях удалённых Unix-систем, полученные по протоколу Syslog.
- **Журнал защиты почтового трафика** — содержит события срабатывания правил защиты почтового трафика, в настройках которых включено журналирование.
- **Журнал UserID** — содержит описание событий отражающие результат работы UserID агента.

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

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

Ротация записей журнала событий не производится.

Журнал событий

Журнал событий отображает события, связанные с изменением настроек сервера LogAn, 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 и другие.

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

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

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

Журнал веб-доступа

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

- Узел UserGate, на котором произошло событие.
- Время события.
- Пользователь.
- Действия.
- Правило.

- Причины (при блокировке сайта).
- URL назначения.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- IP назначения.
- Порт назначения.
- Категории.
- Протокол (HTTP).
- Метод (HTTP).
- Код ответа (HTTP).
- MIME (если присутствует).
- Байт передано/получено.
- Пакетов отправлено.
- Реферер (при наличии).
- Операционная система.
- Useragent Браузера.

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

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

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

Журнал DNS

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

Отображается следующая информация:

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

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

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

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

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

Журнал трафика

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

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

- Байт отправлено/получено.
- Пакетов.

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

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

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

Журнал СОВ

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

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

- Порт источника.
- MAC источника.
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.
- MAC назначения.

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

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

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

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

Журнал АСУ ТП

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

- Узел NGFW, на котором произошло событие.
- Время.
- Действие.
- Правило.
- Зона источника.
- IP-адрес источника.
- IP-адрес назначения.

- Порт назначения.
- Протокол АСУ ТП.
- Команда АСУ ТП.
- Адрес регистра.

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

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

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

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

Журнал инспектирования SSH

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

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

- Зона назначения.
- IP-адрес назначения.
- Порт назначения.

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

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

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

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

История поиска

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

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

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

Журналы конечных устройств

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

В UserGate имеются следующие журналы:

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

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

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

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

Журнал Syslog

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

Наименование	Описание
Узел	Узел UserGate, на котором зафиксировано событие.
Время	Время произошедшего события.
Запись журнала syslog	Ссылка на событие.
Правило	Правило под которое попало Syslog сообщение.
Критичность	Уровень события Syslog.

Наименование	Описание
Объект	Представление процесса, вызвавшего сообщение (kernel messages,user-level messages,security/authentication и тд)
Имя компьютера	Имя компьютера на котором произошло событие.
Приложение	Приложение вызвавшее событие.
Идентификатор процесса	PID процесса вызвавшего событие.
Данные	Описание события.

Журнал защиты почтового трафика

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

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

Байт отправлено/получено.

- Пакетов отправлено/получено.

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

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

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

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

Журнал UserID

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

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

Журнал Windows Active Directory

Журнал Windows Active Directory отображает события, собранные агентом UserID с серверов AD. В журнале отображаются события с успешным входом в систему (идентификатор события 4624), событий Kerberos (события с номерами: 4768, 4769, 4770) и события членства в группах (идентификатор события 4627). В журнале отображена следующая информация:

Наименование	Описание
Узел	Узел UserGate, которым зафиксировано событие.
Время	Время произошедшего события.
Запись журнала событий конечных устройств	Ссылка на событие.
Конечное устройство\сенсор	UserID конектор.
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 тд)
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.

Экспорт журналов

Функция экспортирования журналов LogAn позволяет выгружать информацию на внешние серверы для последующего анализа или для обработки в системах SIEM (Security Information and Event Management).

UserGate LogAn поддерживает выгрузку следующих журналов:

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

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

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

При создании конфигурации требуется указать следующие параметры:

Наименование	Описание
Название правила	Название правила экспорта журналов.
Описание	Опциональное поле для описания правила.
Журналы для экспорта	

Наименование	Описание
	Выбор файлов журналов, которые необходимо экспортировать: • Журнал DNS. • Журнал событий. • Журнал веб-доступа. • Журнал СОВ. • Журнал АСУ ТП. • Журнал инспектирования SSH. • Журнал трафика. • Журнал событий конечных устройств. • Журнал правил конечных устройств. • Приложения конечных устройств. • Аппаратура конечных устройств. Для каждого из журналов возможно указать синтаксис выгрузки: • CEF — Common Event Format (ArcSight). • JSON — JSON format. • @CEE: JSON — CEE Log Syntax (CLS) Encoding JSON. Обратитесь к документации на используемую 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.
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.

Наименование	Описание
	• **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.
Объект	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.

Наименование	Описание
Повторите пароль	Подтверждение пароля учетной записи для подключения к удаленному серверу. Не применяется к методу отправки Syslog.
Путь на сервере	Каталог на сервере для копирования файлов журналов. Не применяется к методу отправки Syslog.
Расписание	Выбор расписания для отправки логов. Не применяется к методу отправки Syslog. Возможны варианты: • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа."

Пользовательская нормализация логов

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

Логи, поступающие с различных сенсоров на SIEM, могут обрабатываться с помощью регулярных выражений, указанных в правилах пользовательской

нормализации. В результате данные, найденные в логах, будут записаны в стандартные поля базы данных SIEM.

Источники логов и их поля, которые можно дополнительно нормализовать:

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

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

Название	Тип
node	string
userId	guid
user	string
ruleId	guid

Название	Тип
rule	string
ipSource	ip
portSource	integer16
portDest	integer16
macSource	mac
macDest	mac
natIpSource	ip
natIpDest	ip
natPortSource	integer16
natPortDest	integer16
applicationName	string
bytesSent	integer64
bytesRecv	integer64
packetsSent	integer64
packetsRecv	integer64
mime	string
httpMethod	string
referer	url
url	url
statusCode	integer16
userAgent	string
sensor	string
sensorId	guid

Название	Тип
processId	string
networkProtocol	ip protocol
status	string
error	integer
counterId	guid
logCategory	integer16
taskCategory	string
computerName	string
logEventCode	integer16
logEventId	integer16
logEventType	integer16
logFile	string
severity	severity
module	string
component	string
event	string
syslogFacility	integer8
syslogSeverity	integer8
image	string
cmdLine	string
originalFileName	string
parentProcessId	integer64
parentImage	string

Название	Тип
parentCommandLine	string
targetObject	string
targetFilename	string
scriptBlockText	string
queryName	string
queryResults	string
workstationName	string
logonId	string
imageLoaded	string
sourceImage	string
targetImage	string
customString1	string
...	string
customString15	string
customNumber1	string
...	string
customNumber5	string
customIp1	ip
customIp2	ip
customDate1	date
customDate2	date

Типы полей:

Тип	Значение по умолчанию	Описание
string	""	Строка любой длины.
guid	00000000-0000-0000-0000-00000000000	Строка вида XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX, где X - шестнадцатиричная цифра (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f, A, B, C, D, E, F).
ip	0.0.0.0	Строка вида X.X.X.X, где X = 0..255; или X:X:X:X:X:X:X:X, где X = 4-значное шестнадцатиричное число.
integer	0	Любое целое неотрицательное число.
url	""	Строка URL, формат в RFC1738.
ip protocol	255	Число 0 .. 255 или строка из списка протоколов ниже.
severity	unknown	Строки: unknown, critical, error, info, warning.
integer8	0	Целое число в интервале [0, 255].
integer16	0	Целое число в интервале [0, 65535].
integer64	0	Целое число в интервале [0, 2^64-1].
date	1970-01-01T00:00:00	2024-03-06T10:30:00.

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

Название	Значение
IP	0
ICMP	1
IGMP	2

Название	Значение
GGP	3
IP-ENCAP	4
ST	5
TCP	6
CBT	7
EGP	8
IGP	9
BBN-RCC-MON	10
NVP-II	11
PUP	12
ARGUS	13
EMCON	14
XNET	15
CHAOS	16
UDP	17
MUX	18
DCN-MEAS	19
HMP	20
PRM	21
XNS-IDP	22
TRUNK-1	23
TRUNK-2	24
LEAF-1	25

Название	Значение
LEAF-2	26
RDP	27
IRTP	28
ISO-TP4	29
NETBLT	30
MFE-NSP	31
MERIT-INP	32
DCCP	33
3PC	34
IDPR	35
XTP	36
DDP	37
IDPR-CMTP	38
TP++	39
IL	40
IPV6	41
SDRP	42
IPV6-ROUTE	43
IPV6-FRAG	44
IDRP	45
RSVP	46
GRE	47
DSR	48

Название	Значение
BNA	49
IPSEC-ESP	50
IPSEC-AH	51
I-NLSP	52
SWIPE	53
NARP	54
MOBILE	55
TLSP	56
SKIP	57
IPV6-ICMP	58
IPV6-NONXT	59
IPV6-OPTS	60
ANY HOST INTERNAL PROTOCOL	61
CFTP	62
ANY LOCAL NETWORK	63
SAT-EXPAK	64
KRYPTOLAN	65
RVD	66
IPPC	67
ANY DISTRIBUTED FILE SYSTEM	68
SAT-MON	69
VISA	70

Название	Значение
IPCU	71
CPNX	72
CPHB	73
WSN	74
PVP	75
BR-SAT-MON	76
SUN-ND	77
WB-MON	78
WB-EXPAK	79
ISO-IP	80
VMTP	81
SECURE-VMTP	82
VINES	83
IPTM	84
NSFNET-IGP	85
DGP	86
TCF	87
EIGRP	88
OSPFIGP	89
SPRITE-RPC	90
LARP	91
MTP	92
AX.25	93

Название	Значение
IPIP	94
MICP	95
SCC-SP	96
ETHERIP	97
ENCAP	98
ANY PRIVATE ENCRYPTION SCHEME	99
GMTP	100
IFMP	101
PNNI	102
PIM	103
ARIS	104
SCPS	105
QNX	106
A/N	107
IPCOMP	108
SNP	109
COMPAQ-PEER	110
IPX-IN-IP	111
VRRP	112
PGM	113
ANY 0-HOP PROTOCOL	114
L2TP	115
DDX	116

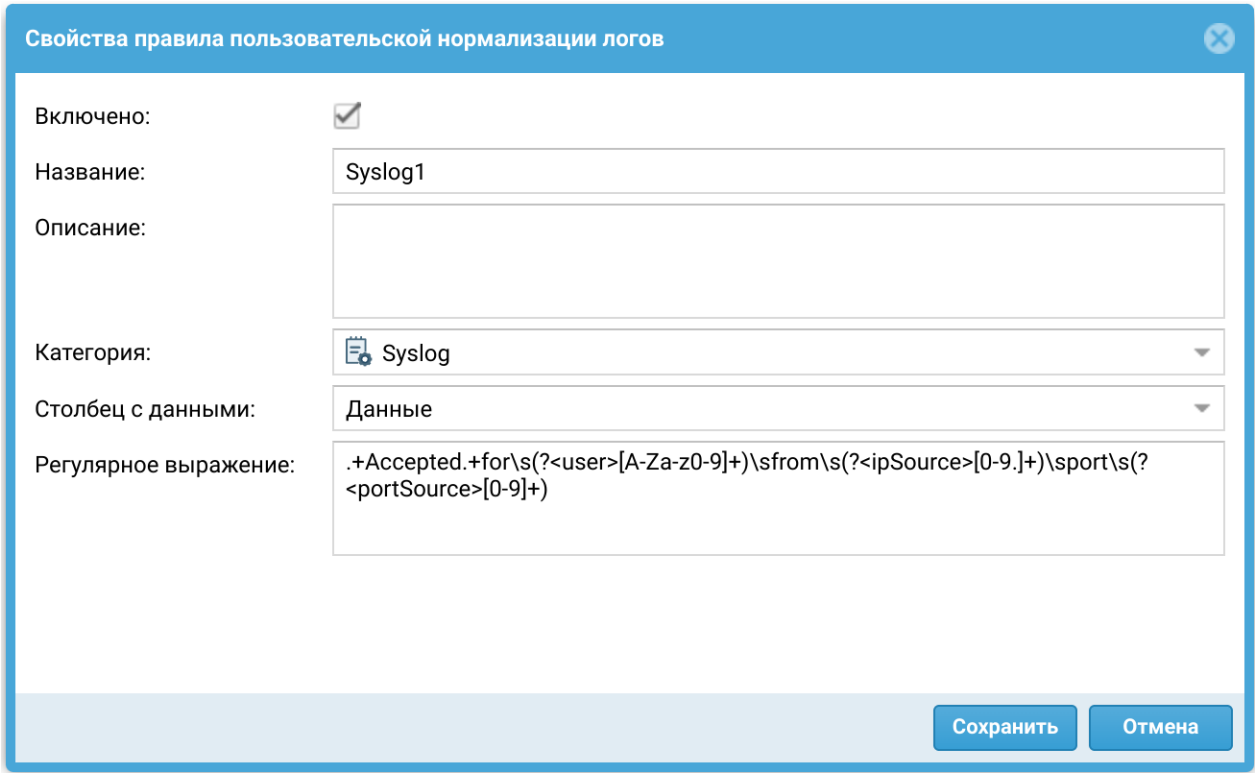
Название	Значение
IATP	117
STP	118
SRP	119
UTI	120
SMP	121
SM	122
PTP	123
IS-IS OVER IPV4	124
FIRE	125
CRTP	126
CRUDP	127
SSCOPMCE	128
IPLT	129
SPS	130
PIPE	131
SCTP	132
FC	133
RSVP-E2E-IGNORE	134
MOBILITY HEADER	135
UDPLITE	136
MPLS-IN-IP	137
MANET	138
HIP	139

Название	Значение
SHIM6	140
WESP	141
ROHC	142
USE FOR EXPERIMENTATION AND TESTING	254
RESERVED	255

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

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

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



Поиск и фильтрация данных

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

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

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

Ключевые слова отделяются пробелами и могут быть следующими:

Наименование	Описание
AND или and	Логическое И, требует выполнения всех условий, заданных в запросе.
OR или or	Логическое ИЛИ, достаточно выполнения одного из условий запроса.

Операторы определяют условия фильтра и могут быть следующими:

Наименование	Описание
=	Равно. Требует полного совпадения значения поля указанному значению, например, *ip=172.16.31.1* будут отображены все записи журнала, в котором поле IP будет точно соответствовать значению 172.16.31.1.
!=	Не равно. Значение указанного поля не должно совпадать с указанным значением, например, *ip!=172.16.31* будут отображены все записи журнала, в котором поле IP не будет равно значению 172.16.31.1.
<=	Меньше либо равно. Значение поля должно быть меньше либо равны указанному в запросе значению. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, *date <= '2019-03-28T20:59:59' AND statusCode=303*.
>=	Больше либо равно. Значение поля должно быть больше либо равны указанному в запросе значению. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, *date >= "2019-03-13T21:00:00" AND statusCode=200*.
<	Меньше. Значение поля должно быть меньше указанного в запросе значения. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, *date < '2019-03-28T20:59:59' AND statusCode=404*.
>	Больше. Значение поля должно быть больше указанного в запросе значения. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, *(statusCode>200 AND statusCode <300) OR (statusCode=404)*.
IN	Позволяет указать несколько значений поля в запросе. Список значений необходимо указывать в круглых скобках,

Наименование	Описание
	например, например, *category IN (botnets, compromised, 'illegal software', 'phishing and fraud','reputation high risk','unknown category')*.
NOT IN	Позволяет указать несколько значений поля в запросе; будут отображены записи, не содержащие указанные значения. Список значений необходимо указывать в круглых скобках, например, *category NOT IN (botnets, compromised, 'illegal software', 'phishing and fraud','reputation high risk','unknown category')*.
~	Содержит. Позволяет указать подстроку, которая должна находиться в указанном поле, например, *browser ~ "Mozilla/5.0"* Данный оператор может быть применен только к полям, в которых хранятся строковые данные.
!~	Не содержит. Позволяет указать подстроку, которая не должна присутствовать в указанном поле, например, *browse r !~ "Mozilla/5.0"* Данный оператор может быть применен только к полям, в которых хранятся строковые данные.
MATCH	При использовании оператора MATCH подстрока, которая должна присутствовать в указанном поле, задаётся в формате JSON и с использованием одинарных кавычек, например, details MATCH '\"module\":\"threats\"' Синтаксис запросов с использованием данного оператора соответствует стандарту RE2. Подробнее о синтаксисе Google/RE2: https://github.com/google/re2/wiki/Syntax.
NOT MATCH	При использовании оператора NOT MATCH подстрока, которая не должна присутствовать в указанном поле, задаётся в формате JSON и с использованием одинарных кавычек, например, details NOT MATCH '\"module\":\"threats\"' Синтаксис запросов с использованием данного оператора соответствует стандарту RE2. Подробнее о синтаксисе Google/RE2: https://github.com/google/re2/wiki/Syntax.

При составлении расширенного запроса LogAn показывает возможные варианты названия полей, применимых к ним операторов и возможных значений, облегчая оператору системы формирование сложных запросов. При переключении режима поиска с основного на расширенный LogAn автоматически формирует строку с поисковым запросом, которая соответствует фильтру, указанному в основном режиме поиска.

ОТЧЕТЫ

Шаблоны

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

Список возможных шаблонов отчетов, сгруппированных по категориям:

- **Пользовательский** — группа шаблонов по обобщенной статистике срабатывания правил отчетов.
- **Captive-портал** — группа шаблонов по событиям, авторизации пользователей с помощью Captive-портала.
- **Приложения конечных устройств** — группа шаблонов со списками приложений, которые когда-либо запускались на конечных устройствах.
- **Журнал правил конечных устройств** — группа шаблонов по событиям срабатывания правил межсетевого экрана конечных устройств.
- **Журнал событий конечных устройств** — группа шаблонов по событиям, полученным от контролируемых с помощью программного обеспечения UserGate Endpoint конечных устройств
- **События** — группа шаблонов по событиям, регистрируемым в журнале событий.
- **СОВ** — группа шаблонов по событиям, регистрируемым в журнале СОВ.
- **Защита почтового трафика** — группа шаблонов по событиям, регистрируемым в журнале защиты почтового трафика.
- **Сетевая активность** — группа шаблонов по событиям, регистрируемым в журнале трафика.
- **Веб-портал** — группа шаблонов авторизации через SSL VPN.

- **Трафик** — группа шаблонов по событиям, регистрируемым в журнале трафика и относящимся к объему потребленного трафика пользователями, приложениями и т.п.
- **UserID** — группа шаблонов для создания отчетов по работе UserID агента.
- **VPN** — группа шаблонов по событиям, относящимся к VPN.
- **Веб-активность** — группа шаблонов по событиям, регистрируемым в журнале веб-доступа.

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

Пользовательские шаблоны

В отличии от обычных шаблонов, предоставляемых производителем решения, пользовательские шаблоны позволяют создать отчет по тем критериям, которые необходимо пользователю. Администратор может выбрать необходимые поля для отображения, задать условия и возможные группировки. Созданные пользовательские отчеты могут быть использованы в правилах построения отчетов наряду с обычными предопределенными отчетами. Для создания пользовательского шаблона необходимо в разделе **Отчеты → Пользовательские отчеты** нажать на кнопку **Добавить** и заполнить следующие параметры:

Наименование	Описание
Название	Название пользовательского шаблона.
Описание	Опциональное поле для описания пользовательского шаблона.
Категория	Выбор источника данных для данного шаблона. Доступны значения: • Журнал событий. • Журнал трафика. • Журнал веб-доступа. • Журнал СОВ. • Журнал инспектирования SSH. • Срабатывания. • Журнал событий конечных устройств.

Наименование	Описание
	• Журнал правил конечных устройств. • Приложения конечных устройств.
Запрос фильтра	SQL-подобная строка запроса, позволяющая ограничить объем информации, используемой при построении отчета по данному шаблону. Для формирования запросов используются названия полей, значения полей, ключевые слова и операторы. В качестве полей данных можно использовать столбцы, перечисленные ниже в поле **Столбцы.** Ключевые слова и операторы, а также примеры их использования можно посмотреть в разделе документации Поиск и фильтрация данных.
Сортировать по	Укажите поле данных, по которому будут отсортированы данные в отчете. Сортировку можно указать по возрастанию и по убыванию.
Группировать по	Укажите поле данных, по которому будут сгруппированы данные в отчете.
Столбцы	Список столбцов, доступных для конкретного источника данных.
Выбранные	Список столбцов, выбранных для отображения в отчете.

Общие сведения

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

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

Наименование	Описание
Шаг 1. Создать правило создания отчета	Создать правило создания отчета, в котором указать необходимые параметры создания отчета.
Шаг 2. Запустить отчет	

Наименование	Описание
	Запустить отчет в ручном режиме или дождаться времени, когда он запустится в автоматическом режиме по указанному в правиле расписанию.
Шаг 3. Получить отчет	Получить отчет по почте, если в правиле была настроена отправка отчета по почте, или скачать полученный отчет в разделе **Созданные отчеты.**

Примечание

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

Правила отчетов

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

Наименование	Описание
Включено	Включение/отключения отчета.
Название	Название правила.
Описание	Опциональное поле для описания правила.
Язык отчета	Выбор языка, который будет использован в отчете.
Диапазон	Диапазон времени, за который необходимо подготовить отчет.
Формат отчета	Формат отчета (PDF, HTML, XML, CSV), в котором будет создаваться данный отчет. **Важно!** Создание отчета в формате PDF создает высокую нагрузку на процессор и память. Чем объемнее отчет, тем более высокая нагрузка. Не используйте формат отчета PDF для пользовательских шаблонов. Для шаблонов **Подробный список всех посещенных URL** и **Подробный список всех посещенных сайтов** автоматически используется формат CSV, независимо от выбранного формата.

Наименование	Описание
Количество записей	Задание ограничения числа записей, которые будут выводиться в отчетах, в которых присутствует ограничение по количеству топ записей, например, топ 20 пользователей с ошибочной авторизацией в веб-консоль.
Количество в группировке (если применимо)	Задание ограничения числа записей, которые будут выводиться в отчетах, в которых присутствует ограничение по количеству сгруппированных записей, например, топ 10 пользователей по категориям — для каждой категории будет указано не более 10 пользователей. Данное ограничение применимо только для тех шаблонов отчетов, которые содержат группирование.
Пользователи	Задает пользователей или группы пользователей, для которых будет создаваться отчет. Если оставить поле пустым, то отчет будет создаваться для всех пользователей.
Шаблоны	Список шаблонов, которые будут использоваться для построения отчета. Обязательно необходимо добавить хотя бы один шаблон.
Расписание	Выбор расписания для создания отчетов. Возможны варианты: • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 0-31) (месяц: 0-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а

Наименование	Описание
	выражение "*/2" в поле "часы" будет означать "каждые два часа.
Доставка	Возможность задать опциональную отправку созданного отчета получателям по протоколу SMTP. Необходимо задать: • Профиль SMTP, который будет использован для отправки отчетов. Подробно о настройке профилей SMTP смотрите в главе Профили оповещений. • От — имя отправителя письма. • Тема письма — тема письма (subject). • Тело письма — содержимое письма. • Получатели — список получателей письма. Получатели должны быть добавлены в списки библиотеки **Почтовые адреса.**

Примечание

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

Примечание

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

Созданные отчеты

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

использовано для создания данного отчета, время создания отчета и размер отчета.

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

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

ОТЧЕТЫ ИНЦИДЕНТОВ

Шаблоны отчетов инцидентов

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

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

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

Общие сведения

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

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

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

Правила отчетов инцидентов

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

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

Примечание

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

После создания правила пользователь может запустить создание отчёта по выбранному инциденту. После формирования отчёт доступен для скачивания локально или передачи на выбранный коннектор.

Созданные отчеты инцидентов

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

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

АНАЛИТИКА

Общие сведения

Раздел **Аналитика** предоставляет функциональность SIEM — системы управления информацией о безопасности и событиями информационной безопасности. UserGate SIEM позволяет проводить анализ журналов событий безопасности, получаемых с настроенных сенсоров, таких как МЭ UserGate, конечные устройства UserGate Client, сторонние сетевые устройства, поддерживающие передачу данных по протоколу SNMP, сенсоры WMI. Все данные хранятся в одной базе данных, что даёт возможность осуществлять сложный поиск, корреляцию повторяющихся событий, их агрегацию, создавая инциденты безопасности, и упростить процесс изучения особенностей инцидентов.

Первоначальной единицей информации, которая поступает в UserGate SIEM, является событие. **Событие** — это одна запись в журнале, например, единичное срабатывание правила СОВ на МЭ UserGate, блокировка доступа к запрещенному ресурсу (срабатывание блокирующего правила контентной фильтрации), успешная или неуспешная попытка доступа в консоль управления и другие подобные события, которые регистрируются на устройствах,

подключенных к UserGate SIEM. Отдельное событие может не нести достаточно информации об угрозе ИБ, но несколько однотипных событий (например, неуспешных попыток доступа в консоль управления) или разных событий, зарегистрированных в определенной последовательности и поступивших из разных источников, могут представлять ценность в идентификации угрозы. Этот процесс называется корреляция событий. Группа событий, объединенная правилом аналитики (корреляции), представляет собой **Срабатывание**. Инженер безопасности проводит анализ срабатывания, изучает входящие в срабатывание события и при необходимости может создавать **Инцидент** компьютерной безопасности на основе одного или нескольких срабатываний.

С помощью правил аналитики инженер безопасности может автоматизировать процесс корреляции событий и создание срабатываний, а также назначить определенные **Действия реагирования** (реакцию) системы на создаваемые срабатывания. Все это позволяет облегчить процесс изучения регистрируемых событий и сократить время между обнаружением проблемы и ее решением.

Настройка данной функции доступна во вкладке **Аналитика**, где можно настроить правила аналитики, создать действия реагирования, просмотреть журнал срабатываний правил и подробности срабатывания.

Данные функции будут рассмотрены далее в соответствующих разделах: Действия реагирования, Срабатывания и Подробности срабатывания.

Во вкладке **Правила аналитики** можно создавать правила обработки событий журналов. Настройка правил аналитики позволяет производить сложный поиск среди событий информационной безопасности. Срабатывание правила происходит при выявлении корреляции событий с разных источников. Правила могут работать в двух режимах: исторический режим (анализ событий за выбранный период) и режим реального времени.

Правила создаются нажатием кнопки **Добавить**. Далее во вкладке **Общие** необходимо указать свойства правила.

Наименование	Описание
Включено	Включает/отключает правило аналитики для работы в режиме реального времени.
Название	Отображает название правила аналитики.
Описание	Описывает правила аналитики. Данное поле необязательно для заполнения.
Уровень угрозы	Показывает уровень угрозы, который будет отображаться при срабатывании правила.

Наименование	Описание
	Для выбора доступны следующие уровни: • **Очень низкий**: события, сформировавшие срабатывание правила аналитики, представляют очень низкий уровень угрозы, и администратор может не предпринимать никаких действий. • **Низкий**: события, сформировавшие срабатывание правила аналитики, представляют низкий уровень угрозы, и администратор может не предпринимать никаких действий. • **Средний**: необходимо обратить внимание на события, попавшие под срабатывание правила аналитики. • **Высокий**: события, требующие исследования и принятия мер. • **Очень высокий**: события, требующие исследования и срочного принятия мер.
Приоритет	Показывает приоритет, установленный для срабатывания правила аналитики: • **Низкий**: срабатывания данных правил обладают низким приоритетом реагирования. • **Нормальный**: на срабатывания данных правил необходимо обратить внимание и, возможно, предпринять меры. • **Важный**: на срабатывания данных правил необходимо обратить внимание и предпринять меры. • **Критический**: срабатывания данных правил требуют незамедлительного реагирования. При срабатывании правила установленный приоритет будет указывать на важность срабатывания правила аналитики.
Категория	Отображает категорию, к которой относится срабатывание. По умолчанию для выбора доступны следующие категории: • **Security**: правила данной категории определяют инциденты, приводящие к ухудшению безопасности информационных систем. • **Availability**: правила данной категории определяют инциденты, которые приводят к ухудшению доступности информационных систем. • **Performance**: правила данной категории определяют инциденты, которые приводят к ухудшению производительности информационных систем.

Наименование	Описание
	Дополнительные категории срабатываний могут быть созданы во вкладке **Настройки** в разделе **Библиотеки → Категории срабатываний**.
Часовой пояс	Указывает на часовой пояс, по времени которого будут работать правила аналитики, т.к. сервер может собирать данные с источников, находящихся в различных часовых поясах.
Ограничить общее время условий	Включить/отключить ограничение времени выполнения всех условий в правиле. При включении ограничения общего времени правило аналитики сработает только в том случае, когда за указанный отрезок времени все условия, настроенные в правиле, выполнятся заданное количество раз.
Общее время условий, сек	Указывает на отрезок времени, за который все условия, указанные в правиле, должны выполнится заданное количество раз, чтобы произошло срабатывание правила аналитики. Время указывается в секундах. Указание общего времени выполнения условий доступно при поставленном флажке **Ограничить общее время условий**.

Во вкладке **Условия** необходимо указать условие/условия срабатывания правила. Если условий несколько, то они связаны между собой логическим «И» и выполняются сверху вниз. Т.е. правило сработает только в том случае, если будут выполнены все условия. Условие можно создать нажатием кнопки **Добавить**. Далее необходимо указать следующие параметры.

Наименование	Описание
Название	Отображает название условия правила аналитики.
Описание	Описывает условие правила аналитики. Данное поле необязательно для заполнения.
Ограничить время выполнения условия	Включить/отключить ограничение времени выполнения условия. При включении ограничения времени правило аналитики сработает, только в том случае, когда за указанный отрезок времени условие выполнится заданное количество раз.
Время выполнения условия	Указывает на отрезок времени, за который условие должно выполнится заданное количество раз, чтобы произошло срабатывание правила аналитики. Время указывается в секундах.

Наименование	Описание
	Указание времени выполнения условия доступно при поставленном флажке **Ограничить время выполнения условия**.
Использовать запрос остановки	Включить/отключить использование запроса остановки в правиле аналитики.
Запрос остановки	SQL-подобный поисковый запрос остановки выполняется вместе с запросом условия. Для формирования запроса используются названия полей, значения полей, ключевые слова и операторы (задаётся аналогично запросу фильтра). Если при выполнении анализа найдётся хотя бы одна запись, соответствующая заданному запросу остановки, до того, как будет найдено заданное количество событий, соответствующих условию правила аналитики, то правило аналитики не сработает, а счётчик количества записей, найденных до выполнения запроса остановки, будет обнулён.
Запрос фильтра	Отображает SQL-подобный поисковый запрос условия, который пишется по базе журналов. Для формирования запроса используются названия полей, значения полей, ключевые слова и операторы. Синтаксис написания запроса можно просмотреть в разделе Поиск и фильтрация данных. Запрос также может быть написан с использованием синтаксиса Google/RE2 в операторе MATCH. **Например**. Поисковый запрос: source = 'wmi log' and logFile = 'Microsoft-Windows-Sysmon/Operational' and logEventId = 1 and data MATCH 'ParentCommandLine:(.*)cmd.exe' and data ~ 'CertReq -Post -config'. Данный запрос производит поиск в журнале событий конечных устройств, который берёт данные из журнала Microsoft-Windows-Sysmon/Operational. При нахождении события, которое соответствует созданию нового процесса, запускается поиск родительского процесса (т.е. процесса, который вызвал создание нового процесса) и поиск вызова команды certreq с параметрами. Часть запроса с оператором MATCH позволяет определить, что certreq запустили из cmd (командной строки). Таким образом определяется то, что у текущего процесса родительским был cmd.exe. Подробнее о синтаксисе Google/RE2 в операторе MATCH: https://github.com/google/re2/wiki/Syntax.
Группировать по	

Наименование	Описание
	Отображает список параметров, по которым могут быть сгруппированы правила в результате срабатывания. Поля будут отображены при просмотре карточки срабатывания. О параметрах, по которым возможна группировка, читайте в разделе Поиск. При указании категорий для группировки правило аналитики сработает только в том случае, если условие выполнится именно для выбранной категории заданное количество раз, указанное в поле параметра **Повторений шаблона**.
Повторений шаблона	Показывает количество выполнений условия, необходимое для срабатывания правила. Данный параметр может быть использован вместе с параметром **Ограничить время выполнения условия** или без него.
Запустить сейчас	Производит запуск анализа событий за определённый период времени (работа в историческом режиме). Далее необходимо задать временной диапазон. Если флажок **Указать диапазон времени** не поставлен, то анализ по созданному правилу аналитики проводится по всей базе событий за всё время. После завершения анализа, нажав кнопку **Показать срабатывания** в окне **Запуск правила аналитики**, можно перейти в журнал срабатываний и просмотреть информацию о срабатывании этого правила. Также правило можно запустить без записи в журнал срабатываний, т.е. для проверки работоспособности правила или просмотра количества срабатываний. Для этого необходимо поставить флажок **Тестовый запуск**.

Во вкладке **Действия реагирования** могут быть добавлены действия, которые будут выполнены автоматически при срабатывании правила аналитики. Действия реагирования могут быть созданы нажатием кнопки **Создать и добавить новый объект** или добавлены из списка существующих действий. Подробнее о действиях реагирования и их настройке читайте в разделе Действия реагирования.

Чтобы запустить правило в режиме реального времени необходимо нажать кнопку **Включить**. Кнопка **Отключить** завершает выполнение выбранного правила аналитики.

Созданные правила можно редактировать, удалять и копировать. Кнопка **Показать срабатывания** отобразит журнал с краткой информацией о всех срабатываниях выбранного правила. Также можно настроить отображение списка правил: отображать все правила, только включённые/выключенные правила.

Для правил аналитики также доступны функции экспорта и импорта. Импорт правил производится в бинарном формате или формате YAML. Экспортировать правила можно только в бинарном формате; экспортируются выделенные правила или все созданные, если правила не были выбраны.

При настройке условий правил аналитики возможно производить группировку событий по параметрам, представленным в записях журналов SIEM, NGFW и конечных устройств. Список параметров, по которым возможна группировка событий, смотрите в таблице раздела Поиск.

Примеры настройки правила аналитики

Рассмотрим несколько примеров настройки правил аналитики.

Пример 1. Поиск попыток брутфорса

Брутфорс (Brute force) — метод взлома учётных записей путём подбора паролей к ним. Суть подхода заключается в последовательном автоматизированном переборе всех возможных комбинаций символов с целью определения правильной.

После задания общих настроек, таких как название правила, описание, уровень угрозы, приоритет, категория срабатывания и часовой пояс, были заданы несколько условий.

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

В соответствии с условием производится поиск в журнале событий конечных устройств по идентификатору события 4625. Данный идентификатор события соответствует неудачной попытке авторизации учётной записи. Часть условия с оператором MATCH позволяет определить причину отказа в авторизации: неправильный логин или пароль.

Подробнее о событии 4625 читайте в соответствующей документации: https://docs.microsoft.com/ru-ru/windows/security/threat-protection/auditing/event-4625.

```
source = 'endpoint events log' AND logEventId = 4672
```

В соответствии с условием производится поиск в журнале событий конечных устройств по идентификатору события 4672. Данный идентификатор события соответствует успешной авторизации с назначением специальных привилегий текущему сеансу.

Подробнее о событии 4672 читайте в соответствующей документации: https://docs.microsoft.com/ru-ru/windows/security/threat-protection/auditing/event-4672.

```
source ='endpoint events log' AND logEventId = 4624
```

В соответствии с условием производится поиск в журнале событий конечных устройств по идентификатору события 4624. Данный идентификатор события соответствует успешному входу пользователя в систему.

Подробнее о событии 4624 читайте в соответствующей документации: https://docs.microsoft.com/ru-ru/windows/security/threat-protection/auditing/event-4624.

Пример 2. Обнаружение изменения владельца файла

В данном примере рассматривается написание правила аналитики с использованием источника событий syslog. Правило обнаруживает изменение владельца файла на root с помощью утилиты chown. Условие задается следующей строкой:

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

Поиск

Во вкладке **Поиск** отражён список всех событий журналов подключённых сенсоров и событий журналов UserGate SIEM. С использованием строки поиска можно производить поиск нужных событий. Строка поиска использует SQL-подобный поисковый запрос. Для формирования запроса используются названия полей, значения полей, ключевые слова и операторы. Синтаксис написания запроса можно просмотреть в разделе Поиск и фильтрация данных.

Запрос также может быть написан с использованием синтаксиса Google/RE2 в операторе MATCH.

С использованием кнопки **Добавить правило**, можно добавить новое правило аналитики, в котором в качестве запроса фильтра будет указан введённый поисковый запрос. Подробнее о правилах аналитики смотрите в разделе Аналитика.

Также, нажатием кнопки **Добавить условие**, по введённому поисковому запросу можно сформировать условие и добавить его в созданное ранее правило аналитики. При добавлении необходимо указать правило аналитики и имя условия.

Выбранное событие можно добавить в инцидент нажатием кнопки **Добавить в инцидент**. Подробнее об инцидентах читайте в главе Настройки инцидентов.

Существует 2 режима представления данных о событиях: табличный вид и текстовый вид. Для перехода в выбранный режим используются кнопки **Переключить в текстовый вид** или **Переключить в табличный вид**.

Во вкладке **Поиск** можно увидеть следующую информацию о событиях.

Наименование в базе данных	Наименование в поисковом запросе	Описание
Узел	node	Показано имя узла устройства NGFW или SIEM.
Время	date	Указано время события или срабатывания правила аналитики. Отображается в часовом поясе, настроенном на UserGate SIEM.
Время первого события	triggeredAlertFirstEventDate	Для журнала срабатываний: отображено время первого события, попавшего под срабатывание правила аналитики.
Время последнего события	triggeredAlertLastEventDate	Для журнала срабатываний: отображено время последнего события, попавшего под срабатывание правила аналитики.
Источник	source	Показан журнал, в который записано событие: журналы

Наименование в базе данных	Наименование в поисковом запросе	Описание
		SIEM, NGFW, конечных устройств, срабатываний.
Важность	severity	Отражена категория события журналов событий NGFW, SIEM: • **Информационные**: как правило, не требуют внимания администратора. • **Предупреждение**: предупреждают о возможных проблемах. • **Ошибка**: сообщают об ошибках. • **Критические**: сообщают о серьёзных ошибках, которые могут повлиять на функциональность.
Компонент	component	Отражён компонент, в котором произошло событие (например: обновления, настройки, консольная авторизация, аналитика и т.п.). Относится к записям журнала событий NGFW и SIEM.
Тип события	event	Отображён тип события из журнала событий NGFW, SIEM (например: проверка, скачивание, установка обновлений, успешная/ неуспешная авторизация, поиск параметров и т.п.).
Пользователь	user	Показано имя пользователя, с учётной записи которого был совершён вход в систему NGFW, SIEM, конечного устройства. Относится к записям журналов событий NGFW,

Наименование в базе данных	Наименование в поисковом запросе	Описание
		SIEM и конечных устройств, веб доступа, трафика, СОВ, срабатываний.
Модуль	module	Указан модуль, в котором произошло событие (например: Web console, Core, VPN сервер и т.п.). Относится к записям журнала событий NGFW, SIEM.
Учёт изменений	changeTracker	Указан тип изменений (журнал событий SIEM, NGFW). Возможные типы изменений пользователь может задать самостоятельно.
Данные	data	Представлена подробная информация о событии. Относится к записям журналов событий конечных устройств и Syslog.
Информация	details	Представлена подробная информация о событии из журнала событий SIEM и NGFW.
Правило	rule	Отображено название правила аналитики, межсетевого экрана, контентной фильтрации, АСУ ТП или СОВ.
Действие	action	Отображено действие, настроенное в правилах межсетевого экрана, контентной фильтрации, АСУ ТП или СОВ: • **Разрешить** (allow/pass/allow_webaccess): действие, настроенное в правилах межсетевого экрана, СОВ или

Наименование в базе данных	Наименование в поисковом запросе	Описание
		контентной фильтрации. • **Безопасный поиск** ('safe browsing'). • **Captive-портал** ('captive portal'). • **Предупредить** (warning): действие, настроенное в правилах контентной фильтрации. • **Уведомление** (alert): относится к DoS защите на зоне. • **NAT** (nat). • **DNAT** (dnat). • **Порт-форвардинг** ('port forwarding'). • **Policy-based routing** ('policy based routing'). • **Network mapping** ('network mapping'). • **Запретить** (deny/drop/deny_webaccess): действие, настроенное в правилах межсетевого экрана, СОВ или контентной фильтрации. • **Расшифровать** (decrypt): действие, настроенное в правилах инспектирования. • **Журналировать** (log): действие, настроенное в правилах СОВ. • **Пропускать** (pass): действие, настроенное в правилах АСУ ТП. • **Блокировать** (drop): действие,

Наименование в базе данных	Наименование в поисковом запросе	Описание
		настроенное в правилах АСУ ТП.
Приложение	application	Название приложения. Относится к записям журнала трафика, СОВ, Syslog, журналов правил и приложений конечных устройств.
Угроза приложения	applicationThreat	Уровень угрозы приложения. Относится к записям журнала веб-доступа, трафика и СОВ.
Сетевой протокол	networkProtocol	Показан транспортный протокол подключения, использующийся для доступа к ресурсу. Относится к записям журналов трафика, СОВ, журнала правил конечных устройств.
Протокол прикладного уровня	httpProtocol	Указана версия HTTP протокола. Относится к записям журнала веб-доступа.
Категории сайтов	urlCategory	Отображены категории, к которым относится сайт. Относится к записям журнала веб-доступа и журнала правил конечных устройств.
Угроза URL-категории	urlCategoryThreat	Уровень угрозы категории URL. Параметр относится к записям журнала веб-доступа.
Причины		Отображены причины из журнала веб-доступа (например: причина блокировки).
HTTP метод	httpMethod	

Наименование в базе данных	Наименование в поисковом запросе	Описание
		Отображен метод HTTP (основная операция над ресурсом). • **OPTIONS**: используется для определения возможностей веб-сервера или параметров соединения для конкретного ресурса. • **GET**: используется для запроса содержимого указанного ресурса. • **HEAD**: аналогичен методу GET, за исключением того, что в ответе сервера отсутствует тело. • **POST**: применяется для передачи пользовательских данных заданному ресурсу. • **PUT**: используется для загрузки содержимого запроса на указанный в запросе URI. • **PATCH**: аналогично PUT, но применяется только к фрагменту ресурса. • **DELETE**: удаляет указанный ресурс. • **TRACE**: возвращает полученный запрос так, что клиент может увидеть, какую информацию промежуточные серверы добавляют или изменяют в запросе. • **CONNECT**: преобразует соединение запроса в

Наименование в базе данных	Наименование в поисковом запросе	Описание
		прозрачный TCP/IP-туннель. Относится к записям журнала веб-доступа.
Код ответа HTTP	statusCode	Отображён код состояния, являющийся частью первой строки ответа от сервера при запросах по протоколу HTTP. Относится к записям журнала веб-доступа.
Тип контента	mime	Показан тип контента. Является записью журнала веб-доступа и журнала правил конечных устройств.
URL	url	Показан URL-адрес ресурса, к которому было выполнено обращение. Относится к записям журнала веб-доступа.
Реферер	referer	Отображён URL-адрес предыдущей страницы (если есть). Относится к записям журнала веб-доступа.
Операционная система	operatingSystem	Отображён тип операционной системы устройства пользователя. Относится к записям журнала веб-доступа и СОВ.
User-agent	userAgent	Указан Useragent пользовательского браузера. Относится к записям журнала веб-доступа.
Сигнатуры	signature	Отображено имя сработавшей сигнатуры системы обнаружения вторжений (СОВ). Является параметром журнала СОВ.
Угроза сигнатуры	signatureThreat	

Наименование в базе данных	Наименование в поисковом запросе	Описание
		Уровень угрозы сигнатуры. Относится к записям журнала СОВ.
Зона источника	zoneSource	Указана зона источника. Относится к записям журналов веб-доступа, трафика, АСУ ТП, СОВ.
IP источника	ipSource	Показан IP-адрес источника трафика. Относится к записям журналов веб-доступа, трафика, АСУ ТП, СОВ, журнала правил конечных устройств.
Порт источника	portSource	Отображён номер порта источника, через который осуществляется подключение. Относится к записям журналов веб-доступа, трафика, СОВ, журнала правил конечных устройств.
MAC источника	macSource	Показан MAC-адрес источника. Относится к записям журналов трафика и СОВ.
Зона назначения	zoneDest	Отображена зона назначения. Относится к записям журналов веб-доступа, трафика, СОВ, журнала правил конечных устройств.
IP назначения	ipDest	Показан IP-адрес назначения трафика. Относится к записям журналов веб-доступа, трафика, АСУ ТП, СОВ, журнала правил конечных устройств.
Порт назначения	portDest	Указан номер порта назначения, используемый транспортным протоколом.

Наименование в базе данных	Наименование в поисковом запросе	Описание
		Относится к записям журналов веб-доступа, трафика, АСУ ТП, СОВ, журнала правил конечных устройств.
MAC назначения	macDest	Показан MAC-адрес назначения. Относится к записям журналов трафика и СОВ.
NAT адрес источника	natIpSource	Отображён NAT IP-адрес источника (если настроены правила NAT). Относится к записям журнала трафика.
NAT порт источника	natPortSource	Отображён NAT порт источника (если настроены правила NAT). Относится к записям журнала трафика.
NAT адрес назначения	natIpDest	Отображён NAT IP-адрес назначения (если настроены правила NAT). Относится к записям журнала трафика.
NAT порт назначения	natPortDest	Отображён NAT порт назначения (если настроены правила NAT). Относится к записям журнала трафика.
Байт отправлено/ получено	bytesSent/bytesRecv	Отображён отправленный/ полученный объём информации. Относится к записям журналов трафика и веб-доступа.
Пакетов отправлено/ получено	packetSent/packetRecv	Показано количество отправленных/полученных пакетов. Относится к записям журналов трафика и веб-доступа.
Конечное устройство/ сенсор	sensor	Отображено имя конечного устройства/сенсора. Относится к записям журнала событий конечных устройств.

Наименование в базе данных	Наименование в поисковом запросе	Описание
Счётчик	counter	Название счётчика, добавленного в WMI и SNMP сенсор. Относится к записям журнала событий конечных устройств.
Объект SNMP	snmpObject	Указан идентификатор SNMP объекта (SNMP OID). Относится к записям журнала событий конечных устройств.
Тип SNMP объекта	snmpObjectType	Указан тип SNMP объекта. Относится к записям журнала событий конечных устройств.
Статус	status	Отображён результат выполнения WMI или SNMP запроса (OK или Error). Относится к записям журнала событий конечных устройств.
Ошибка	error	Показана ошибка WMI или SNMP, возникшая в результате выполнения запроса. Относится к записям журнала событий конечных устройств.
Протокол АСУТП	scadaProtocol	Указан протокол SCADA (Supervisory Control And Data Acquisition - диспетчерское управление и сбор данных). • **IEC 104** (ГОСТ Р МЭК 60870-5-104). • **Modbus**. • **DNP3** (Distributed Network Protocol). • **MMS** (Manufacturing Message Specification). • **OPC UA** (Open Platform Communications Unified Architecture).

Наименование в базе данных	Наименование в поисковом запросе	Описание
		Относится к записям журнала АСУ ТП.
Уровень лога	logLevel	Указан тип события: • **Audit Success** (успешный аудит): событие журнала безопасности, которое происходит при успешном обращении к аудируемым ресурсам. • **Audit Failure** (неуспешный аудит): событие журнала безопасности, которое происходит при неуспешном обращении к аудируемым ресурсам. • **Error** (ошибка): событие указывает на существенные проблемы, которые могут стать причиной потери функциональности или данных. • **Information** (сведения): информационные события, которые, как правило, не требуют внимания администратора. • **Warning** (предупреждение): события указывают на проблемы, которые не требуют немедленного исправления, однако могут привести к ошибкам в будущем. Относится к записям журнала событий конечных устройств.

Наименование в базе данных	Наименование в поисковом запросе	Описание
Источник журнала событий	logEventSource	Отображено название программного обеспечения, которое сформировало запись события в журнал. Относится к записям журнала событий конечных устройств.
Категория лога	logCategory	Указана категория лога, необходимая для упорядочивания событий. Данные берутся из Windows EventLog. Каждый источник может определять свои идентификаторы категорий. Относится к записям журнала событий конечных устройств.
Категория задачи	taskCategory	Показана категория задачи. Является записью журнала событий конечных устройств.
Имя компьютера	computerName	Представлено полное имя конечного устройства. Относится к записям журналов событий конечных устройств, Syslog.
Код события лога	logEventCode	Отображён код события лога, соответствующий определённому событию. Является записью журнала событий конечных устройств.
Идентификатор события лога	logEventId	Показан идентификатор события лога, который определяет первичный идентификатор события. Относится к записям журнала событий конечных устройств.
Тип события лога	logEventType	Отображён тип события лога. Он представлен параметрами, каждый из

Наименование в базе данных	Наименование в поисковом запросе	Описание
		которых соответствует уровню лога: • 1 — уровень лога: error. • 2 — уровень лога: warning. • 3 — уровень лога: information. • 4 — уровень лога: audit success. • 5 — уровень лога: audit failure. Относится к записям журнала событий конечных устройств.
Строка вставки	insertionString	Отображены данные блока EventData события Windows. Относится к записям журнала событий конечных устройств.
Файл журнала лога	logFile	Показана информация из журнала событий конечных устройств, т.е. информация о важных программных и аппаратных событиях. Типы журналов: • **Application** (файл журнала приложений): для событий приложений и служб. • **Security** (файл журнала безопасности): для событий системы аудита. • **System** (файл системного журнала): для событий драйверов устройств. • **CustomLog**: журнал содержит события, регистрируемые приложениями, которые создают

Наименование в базе данных	Наименование в поисковом запросе	Описание
		пользовательский журнал. Использование пользовательского журнала позволяет приложению управлять размером журнала или присоединять списки управления доступом в целях безопасности, не затрагивая другие приложения. Относится к записям журнала событий конечных устройств.
Команда	scadaCommand	Отображена команда управления АСУ ТП (например: чтение или запись). Относится к записям журнала АСУ ТП.
Адрес регистра	scadaAddress	Представлен адрес регистра, с которым необходимо провести операцию (запись или чтение). Относится к записям журнала АСУ ТП.
Номер ASDU	scadaAsdu	Показан адрес ASDU (COA - Common Object Address). Параметр относится к протоколу IEC-104. Относится к записям журнала АСУ ТП.
Идентификатор устройства	scadaDevice	Указан уникальный номер устройства, содержащийся в базе данных OPC-сервера. Параметр относится к протоколу OPC UA. Относится к записям журнала АСУ ТП.
Имя переменной	scadaVarname	Отображено имя переменной. Параметр, в основном, используется для

Наименование в базе данных	Наименование в поисковом запросе	Описание
		обмена данными в режиме реального времени. Параметр относится к протоколу MMS. Относится к записям журнала АСУ ТП.
Хэш	hash	Показан хэш приложения. Является параметром журнала приложений конечных устройств.
Объект	facility	Отображена категория события. Относится к записям журнала Syslog. Возможны следующие значения: • Сообщения ядра. • Сообщения пользовательские. • Почтовая система. • Системный сервис. • Безопасность/ авторизация. • Сообщения syslog. • Система печати LPR. • Система сетевых новостей. • Подсистема UUCP. • Сервис времени. • Безопасность/ аутентификация. • FTP сервис. • Система NTP. • Аудит. • Тревога. • Сервис времени 2. • Local 0 - Local7.
Критичность	syslogSeverity	Указана критичность событий журнала Syslog. • **Экстренная**: критическое

Наименование в базе данных	Наименование в поисковом запросе	Описание
		состояние, которое сказывается на работоспособности системы. • **Тревога**: состояние, требующее незамедлительного вмешательства. • **Критическая**: состояние, требующее незамедлительного вмешательства либо предупреждающее о сбое в системе. • **Ошибки**: несрочные сбои в системе. • **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 уведомления. • **Отладочная**: информация, полезная разработчикам для отладки приложений.
Идентификатор процесса	processId	Указан идентификатор процесса. Относится к записям журнала Syslog.

Администратор может выбрать для показа только те столбцы, которые ему необходимы. Для этого необходимо навести указатель мыши на название любого столбца, нажать на появившуюся справа от названия столбца стрелку,

выбрать **Столбцы** и в появившемся контекстном меню выбрать необходимые параметры.

Действия реагирования

Действия реагирования позволяют определить методы реагирования при срабатывании правил аналитики информационной безопасности. UserGate SIEM позволяет гибко настраивать правила, используя переменные, относящиеся к категориям срабатывания правил аналитики.

Действия могут быть созданы во вкладке **Аналитика → Действия реагирования**. При добавлении действия необходимо указать следующие параметры.

Наименование	Описание
Включено	Включает/отключает правило реагирования.
Название	Отображает название правила реагирования.
Описание	Описывает правила реагирования. Данное поле необязательно для заполнения.
Действие	Показывает действие, выбранное для исполнения в случае срабатывания правила аналитики. Действие реагирования выполнится, если оно указано в свойствах правила аналитики. Для выбора доступны следующие виды реагирования: • **Отправить email**: отправка письма на выбранные почтовые адреса. Настройка действия **Отправить email** будет рассмотрена далее в разделе Действие типа отправить email. • **Отправить сообщение**: отправка сообщения на указанные номера телефонов. Настройка действия **Отправить сообщение** будет рассмотрена далее в разделе Действие типа отправить сообщение. • **Webhook**: получение уведомления о срабатывании правила на веб-странице, адрес которой был указан при настройке действия. Настройка действия **Webhook** будет рассмотрена далее в разделе Действие типа webhook. • **Создать инцидент**: автоматическое создание инцидента в результате срабатывания правил аналитики. О настройке действия **Создать инцидент** читайте в разделе Настройки инцидентов.

Наименование	Описание
	• **Послать команду на коннектор** – отправка команды на выбранный коннектор. Настройка действия Послать команду на коннектор будет рассмотрена далее в разделе Действие типа послать команду на коннектор. • **Послать команду на эндпоинт** – отправка команды на конечное устройство с установленным ПО UserGate Client. Подробнее читайте в раздел Действие типа послать команду на эндпоинт.
Записывать в журнал правил	Включает/отключает журналирование данных о срабатывании действия реагирования. Данные записываются в журнал событий SIEM, который можно просмотреть во вкладке **Журналы и отчёты → Журналы → Журнал событий**.
Группировать похожие срабатывания	Для удобства при настройке действий реагирования возможно использование функции группировки срабатываний. Группировка возможна по следующим параметрам: • **Никогда**. • **За период времени**. При настройке группировки срабатываний правила аналитики за период времени действие реагирования выполнится, если в течение указанного времени произошло хотя бы одно срабатывание. • **По количеству срабатываний**. При настройке группировки по количеству срабатываний правила аналитики действие реагирования выполнится только после указанного количества срабатываний.
Период группировки	Отображает период группировки в минутах. Задание параметра возможно только при выборе группировки похожих срабатываний за период времени.
Количество срабатываний	Отображает заданное количество срабатываний. Задание параметра возможно только при выборе группировки похожих срабатываний по их количеству.

Созданные действия реагирования можно редактировать, удалять, копировать, включать, отключать. Также в списке действий реагирования можно отображать все действия, только включённые или только выключенные.

Действие типа отправить email

Если в качестве действия реагирования была выбрана отправка email, то в свойствах правила реагирования необходимо указать следующие параметры.

Наименование	Описание
Профиль оповещения	Профиль оповещения SMTP, который будет использован для отправки email. Подробнее о настройке профилей SMTP читайте в главе Профили оповещений.
От	Имя отправителя письма.
Тема	Тема письма.
Почтовые адреса	Список почтовых адресов получателей. Получатели должны быть добавлены в списки в разделе **Настройки → Библиотеки → Почтовые адреса**. О добавлении почтовых адресов читайте в разделе Почтовые адреса.
Шаблон	Шаблон письма уведомления с возможностью передачи значений различных переменных, относящихся к срабатыванию. Подробнее читайте в разделе Шаблон уведомлений и Переменные для уведомлений и команд.

Действие типа отправить сообщение

Если в качестве действия реагирования была выбрана отправка сообщения, то в свойствах правила реагирования необходимо указать следующие параметры.

Наименование	Описание
Профиль оповещения	Профиль оповещения SMPP, который будет использован для отправки сообщения. Подробнее о настройке профилей SMPP читайте в главе Профили оповещений.
От	Имя отправителя письма.
Номера телефонов	Список номеров телефонов получателей. Получатели должны быть добавлены в списки в разделе **Настройки → Библиотеки → Номера телефонов**. О добавлении телефонных номеров читайте в разделе Номера телефонов.
Шаблон	Шаблон сообщения с возможностью передачи значений различных переменных, относящихся к срабатыванию.

Наименование	Описание
	Подробнее читайте в разделе Шаблон уведомлений и Переменные для уведомлений и команд.

Действие типа webhook

Для настройки webhook в свойствах правила реагирования необходимо указать следующие параметры.

Наименование	Описание
URL	Адрес веб-сайта, на котором будут отображаться оповещения о срабатывании правила.
Шаблон	Шаблон уведомления с возможностью передачи значений различных переменных, относящихся к срабатыванию. Подробнее читайте в разделе Шаблон уведомлений и Переменные для уведомлений и команд.

Для тестирования webhook можно воспользоваться сервисом https://webhook.site. Для этого необходимо перейти на сайт Webhook.site и скопировать сгенерированную ссылку. Далее её необходимо указать в свойствах правила реагирования в поле **URL** во вкладке **Действия**.

Действие типа послать команду на коннектор

В качестве одного из действий реагирования может быть настроена отправка команды на коннектор.

Если в качестве действия реагирования настроена передача команды для исполнения на коннекторе, то необходимо указать следующие параметры:

Наименование	Описание
Коннекторы	Выбор устройств, на которые необходимо отправить команду в случае срабатывания правила аналитики. Коннектор должен быть заранее добавлен и настроен в разделе **Сенсоры --> Коннекторы** вкладки **Настройки** веб-интерфейса управления UserGate SIEM (для более подробной информации обратитесь к разделу Коннекторы). **Важно!** Могут выбраны только коннекторы с одинаковой группой команд.
Команда	Определение команды, которая будет передана на коннектор для выполнения; представлены команды группы, указанной для выбранных коннекторов.

Наименование	Описание
	В случае наличия в команде переменных, будут отображены дополнительные поля для указания их значений. Подробнее о командах читайте в разделе Команды.

Действие типа послать команду на эндпоинт

В качестве одного из действий реагирования может быть настроена отправка команды на конечное устройство с установленным ПО UserGate Client. Доступны следующие команды:

- **Отключить от сети** – блокировка доступа к сети Интернет.
- **Завершить процесс** – завершение указанного в запросе фильтра процесса.

Шаблон уведомлений

Во вкладке **Шаблон** необходимо указать текст уведомления. Можно передавать не только фиксированный текст, но и данные, относящиеся к срабатыванию или его записям в журнале.

Чтобы передать данные, относящиеся к срабатыванию, необходимо в поле во вкладке **Шаблон** ввести название одного из параметров, представленных в таблице. Например, если ввести **{ANALYTICS_RULE_NAME}**, то в тексте уведомления, настроенном как отправка email, SMS или webhook, будет отражено название правила аналитики, которое сработало. Если заполнить шаблон при настройке действия **Создать инцидент**, то текст будет отображён в описании инцидента.

Переменные для уведомлений и команд

Примечание

Поле чувствительно к регистру букв. Название переменных необходимо вводить прописными буквами в фигурных скобках (как представлено в таблице).

Примечание

Использование переменных в командах и уведомлениях возможно в случае, если они были выбраны в разделе *Аналитика → Правила аналитики → Условия для группировки событий.*

Наименование	Описание
{ANALYTICS_RULE_NAME}	Название правила аналитики.
{ANALYTICS_RULE_DESCRIPTION}	Описание правила аналитики.
{NAME}	Название определённого срабатывания.
{TIME}	Время срабатывания правила аналитики.
{TRIGGERED_ALERTS_NUMBER}	Количество срабатываний.
{FIRST_TRIGGERED_ALERT_TIME}	Время первого срабатывания.
{LAST_TRIGGERED_ALERT_TIME}	Время последнего срабатывания.
{TRIGGERED_ALERTS_NAMES}	Список названий срабатываний, если используется группировка.
{FIRST_EVENT_TIME}	Время первого события, попавшего под срабатывание правила аналитики.
{LAST_EVENT_TIME}	Время последнего события, попавшего под срабатывания правила аналитики.
{THREAT_LEVEL}	Указанный уровень угрозы.
{CATEGORY}	Категория, к которой относится срабатывание.
{PRIORITY}	Приоритет срабатывания правила аналитики.
{ADMINISTRATOR_NAME}	Имя администратора, которым было создано правило аналитики.
{USER_NAME}	Имя пользователя.
{SOURCE_ZONE}	Зона источника.
{DESTINATION_ZONE}	Зона назначения.
{SOURCE_COUNTRY}	Страна источника.
{DESTINATION_COUNTRY}	Страна назначения.
{SOURCE_IP}	IP-адрес источника.

Наименование	Описание
{SOURCE_PORT}	Порт источника.
{DESTINATION_IP}	IP-адрес назначения.
{DESTINATION_PORT}	Порт назначения.
{SOURCE_ZONE_ALL}	Зоны источников всех событий, сформировавших срабатывание.
{DESTINATION_ZONE_ALL}	Зоны назначения всех событий, сформировавших срабатывание.
{SOURCE_COUNTRY_ALL}	Страны источников всех событий, сформировавших срабатывание.
{DESTINATION_COUNTRY_ALL}	Страны назначения всех событий, сформировавших срабатывание.
{SOURCE_IP_ALL}	IP-адреса источников всех событий, сформировавших срабатывание.
{SOURCE_PORT_ALL}	Порты источников всех событий, сформировавших срабатывание.
{DESTINATION_IP_ALL}	IP-адреса назначения всех событий, сформировавших срабатывание.
{DESTINATION_PORT_ALL}	Порты назначения всех событий, сформировавших срабатывание.

Срабатывания

Во вкладке **Срабатывания** показан список срабатываний правил аналитики и отображена краткая информация о них. Срабатывание — это набор событий, объединенных правилом аналитики.

Можно увидеть следующую информацию о срабатываниях.

Наименование	Описание
Узел	Показан уникальный код, соответствующий устройству.
Время	Указаны дата и время срабатывания правила аналитики.

Наименование	Описание
ID	Отображен идентификатор срабатывания.
Время первого события	Показано время первого события, попавшего под срабатывание правила аналитики.
Время последнего события	Показано время последнего события, попавшего под срабатывание правила аналитики.
Количество событий	Показано количество событий, попавших под срабатывание правила аналитики.
Правило	Отображено название правила аналитики, которое сработало.
Категория	Отображена категория, к которой относится срабатывание. По умолчанию для выбора доступны следующие категории: • **Security**: правила данной категории определяют инциденты, приводящие к ухудшению безопасности информационных систем. • **Availability**: правила данной категории определяют инциденты, которые приводят к ухудшению доступности информационных систем. • **Performance**: правила данной категории определяют инциденты, которые приводят к ухудшению производительности информационных систем. Дополнительные категории срабатываний правил аналитики могут быть созданы во вкладке **Настройки** в разделе **Библиотеки → Категории срабатываний**.
Приоритет	Показан приоритет срабатывания, указанный при настройке правила аналитики: • **Низкий**: данные правила обладают низким приоритетом реагирования. • **Нормальный**: на данные правила необходимо обратить внимание и, возможно, предпринять меры. • **Важный**: на данные правила необходимо обратить внимание и предпринять меры. • **Критический**: данные правила требуют незамедлительного реагирования. Установленный приоритет указывает на важность срабатывания.
Пользователь	Указано имя пользователя.

Наименование	Описание
Сигнатуры	Отображено имя сработавшей сигнатуры СОВ.
Зона источника	Отображена зона, из которой происходит подключение.
IP источника	Показан IP-адрес источника.
Порт источника	Указан порт источника.
Зона назначения	Отображена зона назначения.
IP назначения	Показан IP-адрес назначения.
Порт назначения	Указан порт назначения.

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

Доступны два режима поиска: простой и расширенный. Простой режим использует графический интерфейс; расширенный поиск предназначен для формирования более сложных фильтров поиска с использованием специального языка запросов, о синтаксисе которого написано в разделе Поиск и фильтрация данных.

Нажатием кнопки **Сохранить как** можно сохранить настроенный фильтр. Список сохранённых фильтров поиска можно просмотреть, нажав на кнопку **Популярные фильтры**.

Чтобы посмотреть карточку срабатывания (краткую информацию о выбранном срабатывании), необходимо нажать кнопку **Показать**.

Нажатие кнопки **Показать подробно** произведёт перевод на вкладку Подробности срабатывания, где отображена подробная информации о выбранном срабатывании. О вкладке **Подробности срабатывания** читайте в соответствующей главе Подробности срабатывания.

Выбранное срабатывание правила аналитики можно добавить в инцидент нажатием одноимённой кнопки **Добавить в инцидент**.

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

Подробности срабатывания

На данной вкладке отображена подробная информация о срабатывании правила аналитики и отображаются все события, попавшие в данное срабатывание.

Данные могут быть представлены в табличном или текстовом виде. Переключение между режимами осуществляется нажатием кнопок **Переключить в текстовый вид** или **Переключить в табличный вид**, находящихся внизу экрана.

Представлена следующая информация о срабатывании.

Наименование	Описание
Срабатывание	Показан идентификатор срабатывания.
Время	Указано время срабатывания правила аналитики. Отображается в часовом поясе, настроенном на UserGate SIEM.
Приоритет	Отображён установленный при настройке приоритет срабатывания. • **Низкий**: данные правила обладают низким приоритетом реагирования. • **Нормальный**: на данные правила необходимо обратить внимание и, возможно, предпринять меры. • **Важный**: на данные правила необходимо обратить внимание и предпринять меры. • **Критический**: данные правила требуют незамедлительного реагирования.
Правило	Показано название правила аналитики, которое сработало.
Поиск инцидента	Нажатие данной кнопки производит поиск инцидента, в котором используется данное срабатывание.
Список событий	Показаны события, которые попали в данное срабатывание.

Нажатие кнопки **Показать срабатывания** произведёт перевод на вкладку **Срабатывания**, где будет отображён список срабатываний выбранного правила аналитики.

Процессы конечных устройств

Во вкладке **Процессы конечных устройств** отображён список процессов устройств с установленным ПО UserGate Client. Она позволяет отследить цепочку вызова процессов, а также разобраться в параметрах запуска и просмотреть полезную информацию о файле. Вкладка представлена двумя панелями: **Лог процессов** и **Процесс**.

На панели **Лог процессов** отображён список процессов конечных устройств (процессы запущенных приложений, фоновые процессы, процессы Windows), передающих информацию на SIEM. Для просмотра доступна следующая информация:

- Дата и время запуска.
- Название конечного устройства.
- Приложение.
- Идентификатор процесса.

Для удобства записи могут быть отфильтрованы по различным критериям, например, таким, как диапазон дат, название приложения, идентификатор процесса и т.п. Фильтрация также возможна с использованием расширенного поиска для формирования сложных фильтров; в режиме расширенного поиска используется специальный язык запросов, синтаксис которого рассмотрен далее в разделе Поиск и фильтрация данных.

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

Выделив процесс можно просмотреть дерево процесса и подробную информацию о нём. Дерево процесса и подробная информация будут отображены на панели **Процесс**.

ИНЦИДЕНТЫ

Общие сведения

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

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

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

Настройки инцидентов

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

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

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

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

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

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

Наименование	Описание
Шаг 1. Создайте необходимые решения инцидентов	В разделе **Настройки инцидентов → Решения инцидентов** н ажмите добавить, укажите название и описание создаваемого решения и нажмите кнопку **Сохранить**.
Шаг 2. Создайте типы инцидентов	В разделе **Настройки инцидентов → Типы инцидентов** нажм ите добавить, укажите название и описание создаваемого типа и нажмите кнопку **Сохранить**.
Шаг 3. Создайте состояния инцидентов	В разделе **Настройки инцидентов → Состояния инцидентов** нажмите добавить, укажите название, описание и группу создаваемого состояния. Группа состояние определяет положение данного состояние в схеме состояний. Возможно 3 варианта: • **Открыто** — данная группа назначается состояниям инцидентов, по которым еще не начата работа или она приостановлена. Как правило, это начальные состояния инцидентов, например Создан. Все состояния данной группы помечаются синим цветом в веб-консоли. • **В работе** — данная группа назначается состояниям инцидентов, по которым ведется, но еще не завершена работа. Это промежуточные состояния инцидентов, например, В работе, Расследование. Все состояния данной группы помечаются желтым цветом в веб-консоли. • **Закрыто** — данная группа назначается состояниям инцидентов, по которым завершена работа. Это конечные состояния инцидентов, например, Завершено, Закрыто. При переходе в состояние этой группы необходимо обязательно указать решение инцидента, например, Ложная атака, Подтвержденная атака, Выполнено. Все состояния данной группы помечаются зеленым цветом в веб-консоли. После определения всех полей нажмите кнопку **Сохранить**.

Наименование	Описание
Шаг 4. Создайте схему инцидентов	В разделе **Настройки инцидентов → Схемы инцидентов** нажмите добавить и укажите следующие параметры: • Сделать активной — делает данную схему активной. Только одна схема может быть активной, если была активна другая схема, то данное действие сделает ее не активной, и все новые и существующие инциденты перейдут на работу по новой схеме. • Схема — название схемы. • Префикс — префикс, который будет использован при назначении идентификаторов создаваемым инцидентам. Идентификатор будет иметь вид Префикс — порядковый номер, например INC-99. • Описание — необязательное описание данной схемы. • Состояния рабочего процесса — описывает все состояния, которые может принимать инцидент в своем жизненном цикле. Добавьте сюда все состояния инцидентов, созданные на предыдущем шаге. • Начальное состояние — указывает начальное состояние, которое принимает инцидент при его создании. • Переходы — необходимо указать все возможные переходы между состояниями и дать им названия. Например, создать переход под названием **Взять в работу** для перехода из состояния **Открыто** в состояние **В работе**. Перевод инцидента между состояниями возможен только для тех состояний, между которыми определены переходы. • Решения инцидентов — указывает список возможных решений инцидентов. Решение является обязательным при завершении работы по расследованию тикета, то есть при переводе его в состояние, относящееся к группе **закрыто**. Выберите все необходимые решения, которые были созданы ранее. • Типы инцидентов — укажите типы инцидентов, которые могут быть использованы в этой схеме.
Шаг 5. Активируйте схему инцидентов	После создания схемы инцидентов ее необходимо активировать. Для этого активируйте чекбокс **Сделать активной** в настройках схемы инцидентов.

Дашборд по инцидентам

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

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

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

Журнал инцидентов

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

Наименование в базе данных	Наименование в поисковом запросе	Описание
Создан	date	Дата и время создания инцидента.
Изменён	updateDate	

Наименование в базе данных	Наименование в поисковом запросе	Описание
		Дата и время последнего изменения.
Индекс	incidentPrefix	Префикс инцидента (INC-N, где N — порядковый номер инцидента; нумерация начинается с 0).
Имя	incidentName	Название инцидента.
Правило	rule	Название правила аналитики, в результате срабатывания которого автоматически был создан инцидент, т.е. при настройке правила аналитики было задано действие реагирования **Создать инцидент**.
Статус	status	Статус инцидента. Существует 3 группы состояний, которые определяют положение данного состояние в схеме состояний: • **Открыто** — данная группа назначается состояниям инцидентов, по которым еще не начата работа или она приостановлена. Как правило, это начальные состояния инцидентов, например Создан. Все состояния данной группы помечаются синим цветом в веб-консоли. • **В работе** — данная группа назначается состояниям инцидентов, по которым ведется, но еще не завершена работа. Это

Наименование в базе данных	Наименование в поисковом запросе	Описание
		промежуточные состояния инцидентов, например, В работе, Расследование. Все состояния данной группы помечаются желтым цветом в веб-консоли. • **Закрыто** — данная группа назначается состояниям инцидентов, по которым завершена работа. Это конечные состояния инцидентов, например, Завершено, Закрыто. При переходе в состояние этой группы необходимо обязательно указать решение инцидента, например, Ложная атака, Подтвержденная атака, Выполнено. Все состояния данной группы помечаются зеленым цветом в веб-консоли. По умолчанию в UserGate создана схема Incident, которая содержит переходы между всеми состояниями. Схемы инцидентов можно добавить в разделе **Настройки → Настройка инцидентов → Схема инцидентов**. Дополнительные состояния инцидентов можно задать во вкладке **Настройки → Настройка инцидентов → Состояния инцидентов**. Подробнее читайте в разделе Настройки инцидентов.
Решение	resolution	

Наименование в базе данных	Наименование в поисковом запросе	Описание
		Решение инцидента. По умолчанию созданы: • **False positive**: ложная атака. • **True positive**: подтверждённая атака. • **Duplicate**: проблема повторяет другую проблему. • **Won't do**: задача не выполнима. • **Done**: проблема решена. Дополнительные решения инцидентов можно создать во вкладке **Настройки → Настройка инцидентов → Решения инцидентов**. Подробнее читайте в разделе Настройки инцидентов.
Тип	type	Тип инцидента. По умолчанию доступны 2 типа: инцидент безопасности и задача. Дополнительно типы инцидентов можно создать в разделе **Настройки → Настройка инцидентов → Типы инцидентов**. Подробнее читайте в разделе Настройки инцидентов.
Приоритет	priority	Приоритет инцидента: • Низкий. • Нормальный. • Важный. • Критический.
Инициатор	reporter	Имя администратора, который создал инцидент.

Наименование в базе данных	Наименование в поисковом запросе	Описание
Последнее изменение	lastChangeBy	Имя администратора, который внёс последнее изменение.
Назначен	assignee	Имя администратора, назначенного на инцидент.
Активность		Количество комментариев, срабатываний правил аналитики и журналов событий, добавленных в инцидент.

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

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

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

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

Создание инцидентов безопасности

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

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

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

Подробности инцидента

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

В разделе **Срабатывания** отражена информация о срабатываниях правил аналитики, добавленных в инцидент. Подробнее читайте в разделе Срабатывания. Добавить срабатывания в инцидент можно нажатием

кнопки **Добавить срабатывания**. Далее необходимо выбрать срабатывания, которые необходимо добавить в инцидент. Чтобы просмотреть подробности срабатывания выделите нужное срабатывание правила аналитики и нажмите кнопку **Показать подробно**. Также можно просмотреть краткую информацию о срабатывании нажав на кнопку **Показать**. Нажатием на кнопку **Удалить из инцидента** можно удалить запись о срабатывании правила аналитики из инцидента. Список срабатываний правил аналитики, добавленный в инциденты, можно скачать в csv-файл для дальнейшего анализа нажатием кнопки **Экспортировать в CSV**.

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

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

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

Наименование	Описание
Тип улики	Возможен выбор одного из следующих типов улик: • **Автономная система**: система IP-сетей и маршрутизаторов, находящихся под единым управлением. • **Домен**: имя сайта в Интернете. • **Файл**: файл, о котором необходимо собрать информацию. • **Имя файла**: название файла, о котором необходимо собрать информацию. • **FQDN**: полное доменное имя. • **Хэш**: хэш какого-либо файла, например, добавленного в инцидент. • **Имя хоста**: метка устройства, подключённого к компьютерной сети и использующаяся для идентификации устройства.

Наименование	Описание
	• **IP**: уникальный адрес, идентифицирующий устройство в компьютерной сети. • **Почта**: адрес электронной почты. • **Тема письма**: часть письма, указанная в поле subject. • **Реестр**: ключ реестра Microsoft Windows — каталог, в котором хранятся настройки и параметры операционной системы. • **Путь URI**: последовательность символов, идентифицирующая абстрактный или физический ресурс. • **URL**: индивидуальный адрес ресурса в сети Интернет. • **Агент пользователя**: буквенно-цифровая строка, идентифицирующая программу, которая отправляет запрос на сервер и одновременно запрашивает доступ к web-сайту. • **Другое**.
Значение	Необходимо указать объект, с которым будет производиться работа: IP-адрес, домен, и т.п.
Тип атаки	Для указания доступны следующие типы атаки: • **Ботнет** — сеть заражённых компьютеров, удалённо управляемых преступниками. • **Фишинг** — вид Интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. • **Вредоносное ПО** — любое программное обеспечение, которое пытается заразить компьютер или мобильное устройство. • **DDoS** — способ заблокировать работу сайта путем подачи большого количества запросов, превышающих пропускную способность сети. • **Угон трафика** — злоумышленное перенаправление трафика. • **Сетевое сканирование** — сканирование узлов сети для определения уязвимостей. • **Брутфорс** — метод взлома учётных записей путём подбора паролей к ним. • **Компроментация** — факт несанкционированного доступа к защищенной информации, а также подозрение осуществления такого доступа. • **Спам** — массовая рассылка с использованием специальных программ, коммерческой, политической

Наименование	Описание
	и иной рекламы или иного вида сообщений людям, не выразившим желания их получать. • **Другое**.
TLP	Отображена маркировка конфиденциальной информации (Traffic Light Protocol). Возможны следующие маркировки: • **RED**: информация является крайне конфиденциальной. • **AMBER**: информацией можно поделиться в рамках своей организации, при условии, что этой информацией нужно поделиться. • **GREEN**: информация может быть широко распространена в пределах определённого сообщества. • **WHITE**: информация в свободном распространении, но не нарушает авторские права.
Индикатор компроментации?	Чекбокс необходимо отметить, если объект является потенциальным индикатором компроментации.
Сервисы	Отображён список сервисов, которые используются для получения дополнительной информации об объектах наблюдения. Список сервисов отображается автоматически после выбора типа улики. Список сервисов доступен в разделе **Настройки → Библиотеки → Внешние сервисы обогащений**. Подробнее читайте в разделе Внешние сервисы обогащений.
Обновлено	Показаны дата и время последнего обновления сервиса.

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

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

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

- **Incident report**: пользовательский отчёт, который может быть создан на английском или русском языках в формате PDF или HTML. При создании отчёта возможно использование шаблонов, список которых доступен в разделе **Журналы и отчёты → Отчёты инцидентов → Правила отчётов инцидентов**.

- **GOSSOPKA report**: для создание отчёта используется шаблон **Форма для ГОССОПКА**, который соответствует требованиям к отчётам ГОССОПКА. Отчёт можно просто скачать (кнопка **Создать файл**) или сразу сформировать в требуемом формате и отправить в систему личных кабинетов ГОССОПКА (кнопка **Послать через сеть**). Для автоматической отправки отчёта пользователю необходимо предоставить учётную запись для входа в личный кабинет на сайте ГОССОПКА и защищённый канал передачи. Подробнее читайте в разделе Передача отчётов об инцидентах информационной безопасности в ГосСОПКА.

Передача отчётов об инцидентах информационной безопасности в ГосСОПКА

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

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

Для отправки отчётов необходимо:

1. Самостоятельно подключиться к системе личных кабинетов ГосСОПКА.

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

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

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

> **Примечание**
> **Не указывайте криптографический шлюз в качестве шлюза по умолчанию.**

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

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

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

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

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

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

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

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

6. Настроить шаблон отчёта.

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

Наименование	Описание
Организация	Название организации.
Категория	Категория уведомления: • Уведомление о компьютерном инциденте. • Уведомление о компьютерной атаке. • Уведомление о наличии уязвимости.
Тип события ИБ	Тип события информационной безопасности: • Вовлечение контролируемого ресурса в инфраструктуру ВПО. • Замедление работы ресурса в результате DDoS-атаки. • Заражение ВПО. • Захват сетевого трафика. • Использование контролируемого ресурса для фишинга. • Компрометация учётной записи. • Несанкционированное изменение информации. • Несанкционированное разглашение информации. • Публикация на ресурсе запрещённой законодательством РФ информации. • Рассылка спам-сообщений с контролируемого ресурса. • Успешная эксплуатация уязвимости.
Статус реагирования на инцидент	Статус реагирования на инцидент: • Меры приняты. • Проводятся мероприятия по реагированию. • Возобновлены мероприятия по реагированию.
Необходимость привлечения сил ГосСОПКА	Отметьте чекбокс в случае необходимости привлечения сил ГосСОПКА.
Краткое описание события ИБ	Описание события информационной безопасности.
Сведения о средстве или способе выявления инцидента	Информация о способе и устройстве/ПО, посредством которого был выявлен инцидент.

Наименование	Описание
Дата и время выявления инцидента	Дата и время выявления инцидента заполняются автоматически.
Дата и время завершения инцидента	Дата и время завершения инцидента заполняются автоматически.
Ограничительный маркер TLP	Маркировка конфиденциальной информации (Traffic Light Protocol). Возможны следующие маркировки: • **RED**: информация является крайне конфиденциальной. • **AMBER**: информацией можно поделиться в рамках своей организации, при условии, что этой информацией нужно поделиться. • **GREEN**: информация может быть широко распространена в пределах определённого сообщества. • **WHITE**: информация в свободном распространении, но не нарушает авторские права.
Влияние на доступность	Потенциальное влияние на доступность информационных ресурсов: • Отсутствует. • Низкое. • Высокое.
Влияние на целостность	Потенциальное влияние на целостность ресурсов информационной системы: • Отсутствует. • Низкое. • Высокое.
Влияние на конфиденциальность	Потенциальное влияние на конфиденциальность (ограничение доступа к информационным ресурсам, разрешения доступа к системе только авторизованным пользователям, предотвращение раскрытия информации неуполномоченным лицам): • Отсутствует. • Низкое. • Высокое.
Краткое описание иной формы последствий	Описание последствий инцидента, кроме тех, что были указаны ранее.

Наименование	Описание
компьютерного инцидента	
Наименование контролируемого ресурса, на котором был выявлен компьютерный инцидент	Наименование контролируемого информационного ресурса объекта КИИ, на котором выявлен компьютерный инцидент, компьютерная атака или уязвимость.
Информация о категорировании ОКИИ	Присвоенная объекту КИИ категория значимости: • Информационный ресурс не является объектом КИИ. • Объект КИИ без категории значимости (объект признан незначимым). • Объект КИИ третьей категории значимости (самая низкая). • Объект КИИ второй категории значимости. • Объект КИИ первой категории значимости (самая высокая).
Сфера функционирования субъекта	Сфера функционирования объекта КИИ (например, банковская сфера, здравоохранение и т.п.).
Наличие подключения к сети Интернет	Наличие подключения к сети Интернет: • **Да**. • **Нет**.
Страна/регион	Код в соответствии с ISO-3166-2.
Населенный пункт или геокоординаты	Название населённого пункта или его географические координаты. Географические координаты указываются в формате: *широта* — С.Ш, *долгота* — В.Д.

7. Сформировать и отправить отчёт об инциденте информационной безопасности.

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

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

Запись об отправке отчёта будет отображена в журнале событий SIEM.

ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ (CLI)

ОБЩИЕ ПОЛОЖЕНИЯ

Общие положения (описание)

В UserGate SIEM имеется возможность производить настройку устройства с помощью интерфейса командной строки CLI (Command Line Interface).

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

Подключение к CLI можно выполнить через стандартные порты VGA/клавиатуры (при наличии таких портов на оборудовании SIEM), через последовательный порт или с помощью SSH по сети.

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

Для подключения к CLI с использованием монитора и клавиатуры необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Подключить монитор и клавиатуру к устройству	Подключить монитор к разъему VGA(HDMI), клавиатуру к разъему USB.
Шаг 2. Войти в CLI	Войти в CLI, используя имя и пароль пользователя с правами корневого администратора (по умолчанию Admin).

Для подключения к CLI с использованием последовательного порта необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Подключиться к устройству	Используя специальный кабель для последовательного порта или переходник USB-Serial, подключить свой компьютер к устройству.
Шаг 2. Запустить терминал	Запустить терминал, позволяющий подключение через последовательный порт, например, Putty для Windows или minicom для Linux. Установить подключение через последовательный порт, указав параметры подключения 115200 8n1.
Шаг 3. Войти в CLI	Войти в CLI, используя имя и пароль пользователя с правами корневого администратора (по умолчанию Admin).

Для подключения к CLI по сети с использованием протокола SSH необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Разрешить доступ к CLI (SSH) для выбранной зоны	Разрешить доступ для протокола CLI по SSH в настройках зоны, к которой вы собираетесь подключаться для управления с помощью CLI. Будет открыт порт TCP 2200.
Шаг 2. Запустить SSH-терминал	Запустить у себя на компьютере SSH-терминал, например, SSH для Linux или Putty для Windows. Указать в качестве адреса адрес устройства SIEM, в качестве порта подключения — 2200, в качестве имени пользователя — имя пользователя с правами корневого администрвтора (по умолчанию Admin). Для Linux команда на подключение должна выглядеть так: *ssh Admin@IPSIEM -p 2200*
Шаг 3. Войти в CLI	Войти в CLI, используя пароль пользователя, указанного на предыдущем шаге.

После успешной аутентификации в CLI появится строка ожидагия ввода команды (режим диагностики). Для просмотра текущих возможных значений или автодополнения необходимо использовать клавишу **Tab**. Доступны:

- **configure** — переход в режим конфигурации.
- **date** — просмотр текущих даты и времени на устройстве.
- **dig** — проверка записи DNS-домена.
- **exit** — выход из командной строки.
- **netcheck** — проверка доступности стороннего HTTP/HTTPS-сервера.
- **show** — просмотр сетевых настроек, версии ПО, статистики активных сессий.
- **clear** — очистка данных статистики по активным сессиям и сетевым интерфейсам.
- **ping** — выполнение ping определённого хоста.
- **reboot** — перезагрузка устройства.
- **shutdown** — выключение устройства.
- **traceroute** — трассировка соединения до определённого хоста.

Данные команды доступны в режиме конфигурации; подробнее читайте в разделе Команды execute.

Для отмены ввода текущей команды используется сочетание **Ctrl + C**; для просмотра истории команд — ↑, ↓.

Все команды интерфейса командной строки имеют следующую структуру:

```
<action> <level> <filter> <configuration_info>
```

где:

<action>: действие, которое необходимо выполнить.

<level>: уровень конфигурации; уровни соответствуют разделам веб-интерфейса NGFW.

<filter>: идентификатор объекта, к которому происходит обращение.

<configuration_info>: значение параметров, которые необходимо применить к объекту <filter>.

КОМАНДЫ, ДОСТУПНЫЕ ДО ПЕРВИЧНОЙ ИНИЦИАЛИЗАЦИИ УЗЛА

Команды, доступные до первичной инициализации узла (описание)

Если устройство не прошло первоначальную инициализацию, то в CLI доступны команды диагностики и мониторинга, а в режиме конфигурации — только команды настройки сети, т.е. настройка зон, интерфейсов, шлюзов и виртуальных маршрутизаторов, а также включение/отключение удалённого доступа к серверу radmin-emergency.

ПЕРВОНАЧАЛЬНАЯ ИНИЦИАЛИЗАЦИЯ

Первоначальная инициализация (описание)

Первоначальная инициализация устройства с использованием интерфейса командной строки.

Для настройки устройства используется команда:

```
Admin@nodename# execute install master
```

Необходимо указать параметры:

Параметр	Описание
login	Задать логин администратора.

Параметр	Описание
password	Задать пароль учётной записи администратора. Указание пароля также доступно при нажатии **Enter** после указания логина администратора; необходимо дважды ввести пароль учётной записи.

РЕЖИМ КОНФИГУРАЦИИ

Режим конфигурации (описание)

Для перехода в режим конфигурации используется команда:

```
Admin@nodename> configure
```

После перехода в режим конфигурации командная строка будет выглядеть следующим образом:

```
Admin@nodename#
```

Для просмотра подсказки о текущих возможных значениях или для автодополнения команд необходимо нажать клавишу **Tab**. В подсказке могут использоваться следующие вспомогательные символы:

***** — обязательное поле в командах create и ряде других команд;

+ — необязательное/вариативное поле;

> — вложенное поле, после его введения предыдущий список полей становится недоступным, появляется новый список полей, которые можно ввести.

Например:

```
Admin/system@nodename# set network zone Trusted
* name                    Name
+ antispoof-enable        Enable/Disable IP spoofing protection
+ antispoof-negate        Enable/Disable Negate ip-spoof addresses
```

```
+ description              Description
+ enabled-services         Services list to enable
+ geoip                    IP spoofing protection by geo IP code
+ ip-list                  IP spoofing protection by IP list
> dos-protection-icmp      Confugure DoS protection per IP for ICMP
packets
> dos-protection-syn       Confugure DoS protection per IP for SYN
packets
> dos-protection-udp       Confugure DoS protection per IP for UDP
packets
> service-addresses        Access control service addresses
```

Общая структура команд в режиме конфигурации

Команды интерфейса командной строки имеют следующую структуру:

```
<action> <level> <filter> <configuration_info>
```

где:

<action> — действие, которое необходимо выполнить.

<level> — уровень конфигурации; уровни соответствуют разделам веб-интерфейса LogAn.

<filter> — идентификатор объекта, к которому происходит обращение.

<configuration_info> — значение параметров, которые необходимо применить к объекту <filter>.

Наименование	Описание
<action>	В режиме конфигурации доступны следующие действия: • **execute** — выполнение команд, которые не относятся к конфигурации UserGate (ping, date, traceroute и т.п.) Команда доступна независимо от уровня конфигурации (<level>). • **set** — редактирование всех объектов, а также включение различных параметров, например, radmin. • **end** — переход на один уровень выше.

Наименование	Описание

	• **show** — отображение текущих значений. Можно использовать на любом уровне конфигурации — будет отображено всё, что находится глубже текущего уровня.
	• **edit** — переход на какой-либо уровень конфигурации. Уровень конфигурации будет отображён под командной строкой.
	• **top** — возврат на самый верхний уровень конфигурации.
	• **exit** — выход из режима конфигурации.
	• **export** — экспорт конфигурации.
	• **import** — импорт конфигурации.
	• **create** — создание новых объектов.
	• **delete** — удаление объекта или параметра из списка параметров.
	
	Например, для просмотра информации о всех интерфейсах необходимо выполнить команду:
	
	`Admin@nodename# show network interface`
	
	С использованием следующей команды производится переход на уровень **network interface.** Текущий уровень будет отображён под командной строкой:
	
	`Admin@nodename# edit network interface`
	`Admin@nodename#`
	`Level: network interface`
	
	После перехода на уровень **network interface** для отображения всех интерфейсов используется команда show без указания уровня:
	
	`Admin@nodename# show`
	
	`adapter:`
	`port0`
	`type : adapter`
	`interface-name : port0`
	`node-name : node`

Наименование	Описание
	zone : Management enabled : on ip-addresses : 192.168.56.3/24 iface-mode : dhcp ... ... Level: network interface Для возвращения с уровня **network interface** обратно на общий уровень режима конфигурации необходимо набрать команду **end**: Admin@nodename# end Level: network interface Admin@nodename# end Level: network Admin@nodename#
<level>	Уровни в командной строке повторяют веб-интерфейс системной консоли LogAn: • **network** — соответствует разделу веб-интерфейса **Сеть**. • **settings** — соответствует разделу веб-интерфейса **UserGate**. • **users** — соответствует разделу веб-интерфейса **Пользователи и устройства**. • **libraries** — соответствует разделу веб-интерфейса **Библиотеки**. • **monitoring** — соответствует разделу веб-интерфейса **Диагностика и мониторинг**. • **sensors** — соответствует разделу веб-интерфейса **Сенсоры**. • **analytics** — соответствует разделу веб-интерфейса **Аналитика**. • **incident** — соответствует разделу веб-интерфейса **Инциденты**.
<filter>	Идентификатор объекта, к которому происходит обращение. Идентификация происходит по имени объекта.

Наименование	Описание
	Если имеются объекты с одинаковыми именами или удобнее идентифицировать объект по другому параметру, то используются круглые скобки, в которых необходимо указать <configuration_info>. В результате будет найден объект, для которого совпали все поля, указанные в круглых скобках.

<configuration_info>	Набор пар: параметр-аргумент. Параметр — имя поля, для которого нужно установить аргумент. Аргумент может быть одиночным или множественным.
	Одиночный аргумент — значение, соответствующее параметру. Если строка содержит пробелы, то необходимо использовать кавычки.
	Например, необходимо создать профиль аутентификации с именем New profile:
	`Admin@nodename# create users auth-profile name "New profile"`
	Множественные аргументы используются для установки множества значений какого-либо параметра; записываются в квадратных скобках и разделяются пробелами.
	Например, необходимо создать список IP-адресов в библиотеке элементов и добавить в него два IP-адреса 10.10.0.1 и 10.10.0.2:
	`Admin@nodename# create libraries ip-list name testlist ips [ 10.10.0.1 10.10.0.2 ]`
	Важно! Квадратные скобки должны быть отделены пробелами с обеих сторон.

Команды execute

Команды имеет следующую структуру:

```
Admin@nodename# execute <command-name>
```

Доступны следующие команды:

Параметр	Описание
traceroute	

Параметр	Описание
	Трассировка соединения до определённого хоста. Доступны параметры: • **hostname <ip-or-domain>** — IP-адрс или имя домена, для которого производится трассировка. • **interface <iface-name>** — интерфейс, с которого будут отправляться пакеты. • **not-map-ip** — не искать hostname для IP-адреса при отображении. • **use-icmp-echo** — использовать ICMP echo. • **port** — указать порт вместо порта по умолчанию (1 — 65535). • **min-interval** — минимальный интервал между пакетами. `Admin@nodename# execute traceroute hostname <hostname>`
termination	Закрытие сессий администраторов. Подробнее читайте в разделе Управление сессиями администраторов.

Параметр	Описание
ping	Выполнение ping определенного хоста. Можно задать следующие параметры: • **hostname** — IP-адрес или доменное имя хоста. • **count** — количество отправляемых echo-запросов. Если параметр не задан, то отправка пакетов будет происходить, пока соединение не будет прервано пользователем (чтобы прервать отправку: Ctrl+C). • **numeric** — не резолвить имена. • **timestamp** — отображение временных меток. • **interval** — интервал времени, через который будет производиться отправка пакетов; указывается в секундах. • **ttl** — время жизни пакета. • **interface** — адрес выбранного интерфейса будет использоваться в качестве адреса источника для выполнения ping. • **mtu** — размер mtu отправляемых пакетов. • **virtual-router** — имя виртуального маршрутизатора. `Admin@nodename# execute ping hostname <hostname> count <number>`
reboot	Перезагрузка устройства.
date	Просмотр текущих даты и времени на сервере.
shutdown	Выключение устройства.
netcheck	Проверка доступности стороннего HTTP/HTTPS-сервера. Могут быть использованы следующие параметры: • **address** — доменное имя хоста для проверки доступности по TCP или URL для HTTP. • **dns-ip** — IP-адрес сервера DNS. • **dns-tcp** — использование TCP вместо UDP для DNS-запроса. • **check-cert** — проверка SSL-сертификата • **type** — проверка доступности по: ◦ **http**. ◦ **tcp** (если порт не указан, то используется порт 80).

Параметр	Описание

	• **data** — запрос содержимого сайта. По умолчанию запрашиваются только заголовки.
	• **timeout** — максимальный таймаут ожидания ответа от веб-сервера.
	• **user-agent** — параметр для указания типа браузера (useragent). На некоторых сайтах может быть разрешен доступ только с определенных браузеров. Значение параметра указывается в двойных кавычках.
	
	`Admin@nodename# execute netcheck type tcp address <host-domain-name> data on`
	`Admin@nodename# execute netcheck address <host-domain-name>`

dig	Проверка записи DNS домена.
	• **hostname** — доменное имя хоста или IP-адрес для реверсивного поиска.
	• **reverse-lookup** — получение хоста по IP-адресу.
	• **dns** — указание IP-адреса DNS-сервера.
	• **tcp** — использование протокола TCP вместо UDP.
	
	`Admin@nodename# execute dig hostname <host-domain-name>`
	`Admin@nodename# execute dig hostname <IP-address> reverse-lookup on`

license	Команда регистрации продукта имеет следующую структуру: `Admin@nodename# execute license activate <pin-code>` Укажите код активации продукта вместо <pin-code>.

Часть представленных выше команд также доступны в режиме диагностики и мониторинга. Для их выполнения используется команда:

```
Admin@nodename> <command-name>
```

НАСТРОЙКА УСТРОЙСТВА

Настройка устройства (описание)

Общие настройки устройства

Общие настройки устройства задаются на уровне **settings general**. Структура команды для настройки одного из разделов (<settings-module>):

```
Admin@nodename# set settings general <settings-module>
```

Доступна настройка следующих разделов:

Параметр	Описание
admin-console	Настройки интерфейса (уровень **settings general admin-console**): • **timezone**: часовой пояс, соответствующий вашему местоположению. Часовой пояс используется в расписаниях, применяемых в правилах, а также для корректного отображения времени и даты в отчетах, журналах и т.п. • **language**: язык интерфейса: ◦ **ru** — русский. ◦ **en** — английский. • **api-session-lifetime**: время ожидания сеанса администратора в секундах.
server-time	Настройка параметров установки точного времени (уровень **settings general server-time**): • **ntp-enabled**: включение/отключение использования NTP-серверов: ◦ **on**. ◦ **off**.

Параметр	Описание
	• **primary-ntp-server**: указание основного ntp-сервера. • **second-ntp-server**: указание запасного ntp-сервера. • **time**: установка времени на сервере; время указывается в часовом поясе UTC в формате yyyy-mm-ddThh:mm:ss (например, 2022-02-15T12:00:00)
change-tracker	Настройка учёта изменений (уровень **settings general change-tracker**): • **enabled**: включение/отключение учёта изменений. ◦ **on**. ◦ **off**. • **event-tracker-types**: типы изменений задаются администратором. Для удаления типа изменения используется команда: `Admin/system@nodename# delete settings general change-tracker event-tracker-types [ type1 ... ]`
management-center	Настройка агента UserGate Management Center (уровень **settings general management-center**): • **enabled**: включение/отключение агента UserGate Management Center. ◦ **on**. ◦ **off**. • **mc-address**: адрес сервера UserGate Management Center. • **device-code**: уникальный код устройства для подключения устройства к UserGate Management Center.
updates-schedule	Настройка расписания скачивания обновлений программного обеспечения и библиотек (уровень **settings general updates-schedule**). Для расписания обновления программного обеспечения UserGate: `Admin/system@nodename# set settings general updates-schedule software schedule <schedule/disabled>`

Параметр	Описание

	Расписание скачивания обновлений библиотек может быть единым:
	`Admin/system@nodename# set settings general updates-schedule all-libraries schedule <schedule/disabled>`
	или может быть настроено отдельно для каждого элемента:
	`Admin/system@nodename# set settings general updates-schedule libraries [ lib-module ... ] schedule <schedule/disabled>`
	Время задаётся в crontab-формате: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом:
	• Звездочка (*) — обозначает весь диапазон (от первого до последнего).
	• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.
	• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".
	• Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".
	Команда для просмотра расписания обновлений:
	`Admin/system@nodename# show settings general updates-schedule`

Настройка управления устройством

Настройка Radmin-emergency

Для активации удаленного помощника при возникновении проблемы с программным ядром устройства администратор может зайти в CLI под учетной записью корневого администратора, которая была создана при инициализации узла. Обычно это учетная запись Admin, хотя может быть и другой. Для входа

необходимо указать имя в виде Admin@emergency, в качестве пароля — пароль корневого администратора. Команда включения/отключения удалённого доступа к серверу для технической поддержки в таких случаях:

```
Adminm@emergency@LogAn# set radmin-emergency enabled <on | off>
```

Параметр	Описание
interface	Название интерфейса.
ip-addr	IP-адрес и маска интерфейса.
gateway-address	IP-адрес шлюза.

Настройка операций с сервером

Следующая команда позволяет определить канал обновлений:

```
Admin@nodename# set settings device-mgmt updates-channel <stable |
beta>
```

Для просмотра наличия обновлений и выбранного канал обновления используется команда:

```
Admin@nodename# show settings device-mgmt updates-channel
```

Для настройки активации лицензии и обновления ПО устройства через внешний прокси-сервер используется команда:

```
Admin@UGOS# set settings device-mgmt licensing-upstream-proxy
<parameters>
```

В качестве дополнительных параметров указываются:

Параметр	Описание
enabled	Включение/выключение режима активации лицензии и обновления ПО через внешний прокси-сервер: • **on** — включено. • **off** — выключено.
ip	IP-адрес внешнего прокси-сервера.
port	Порт внешнего прокси-сервера.
auth	Аутентификация на внешнем прокси-сервере: • **on** — включена. • **off** — выключена.
name	Логин на внешнем прокси-сервере.
password	Пароль на внешнем прокси-сервере.

Для просмотра созданных настроек активации лицензии и обновления ПО устройства через внешний прокси-сервер используется команда:

```
Admin@UGOS# show settings device-mgmt licensing-upstream-proxy
```

Управление резервным копированием

Создание резервной копии устройства осуществляется на уровне **settings device-mgmt**. Для создания правила резервного копирования и выгрузки файлов на внешние серверы (FTP/SSH) используется следующая команда:

```
Admin@nodename# create settings device-mgmt settings-backup
<parameters>
```

Для настройки доступны следующие параметры:

Параметр	Описание
enabled	Включение/отключение правила создания резервной копии устройства.
name	Название правила резервного копирования.

Параметр	Описание
description	Описание правила резервного копирования.
type	Выбор удалённого сервера для экспорта файлов: • **ssh**. • **ftp**.
address	IP-адрес удалённого сервера.
port	Порт сервера.
login	Учётная запись на удалённом сервере.
password	Пароль учётной записи.
path	Путь на сервере, куда будут выгружены файлы.
schedule	Расписание экспорта файлов резервных копий. Время задаётся в Crontab-формате: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

Редактирование существующего правила резервного копирования устройства производится с использованием следующей команды:

```
Admin@nodename# set settings device-mgmt settings-backup <rule-name>
```

Список параметров, доступных для изменения аналогичен списку параметров, доступных при создании правила.

Команда для удаления правила резервного копирования:

```
Admin@nodename# delete settings device-mgmt settings-backup <rule-name>
```

Команда для отображения правила резервного копирования:

```
Admin@nodename# show settings device-mgmt settings-backup <rule-name>
```

Также, для команд редактирования, удаления или отображения правил в качестве <filter> возможно использование не только названия правила, но и заданные в существующем правиле параметры (удобно, например, при наличии нескольких правил с одинаковым названием). Параметры, с использованием которых можно произвести идентификацию правила экспорта, аналогичны параметрам команды **set**.

Экспорт настроек

Создание и настройка правил экспорта настроек происходит на уровне **settings device-mgmt settings-export**.

Для создания правила экспорта настроек:

```
Admin@nodename# create settings device-mgmt settings-export
( <parameters> )
```

Доступны параметры:

Параметр	Описание
enabled	Включение/отключение правила экспорта настроек сервера UserGate.
name	Название правила экспорта.
description	Описание правила экспорта.
type	Выбор удалённого сервера для экспорта настроек: • **ssh**. • **ftp**.
address	IP-адрес удалённого сервера.
port	Порт сервера.

Параметр	Описание
login	Учётная запись на удалённом сервере.
password	Пароль учётной записи.
path	Путь на сервере, куда будут выгружены настройки.
schedule	Расписание экспорта настроек. Время задаётся в Crontab-формате: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

Обновление существующего правила экспорта настроек устройства производится с использованием следующей команды:

```
Admin@nodename# set settings device-mgmt settings-export <rule-name>
```

Список параметров, доступных для изменения аналогичен списку параметров, доступных при создании правила.

Команда для удаления правила экспорта настроек:

```
Admin@nodename# delete settings device-mgmt settings-export <rule-name>
```

Команда для отображения правила экспорта настроек:

```
Admin@nodename# show settings device-mgmt settings-export <rule-name>
```

Также, для команд обновления, удаления или отображения правил в качестве <filter> возможно использование не только названия правила, но и заданные в существующем правиле параметры (удобно, например, при наличии нескольких правил с одинаковым названием). Параметры, с использованием которых можно произвести идентификацию правила экспорта, аналогичны параметрам команды **set**.

Настройка управления доступом к консоли устройства

Настройка данного раздела производится на уровне **settings administrators**. В разделе описаны настройка параметров защиты учётных записей, настройка администраторов и их профилей.

Общие настройки доступа

Данный раздел позволяет настроить дополнительные параметры защиты учётных записей администраторов. Настройка производится на уровне **settings administrators general**.

Для изменения параметров используется следующая команда:

```
Admin@nodename# set settings administrators general
```

Параметры, доступные для редактирования:

Параметр	Описание
password	Изменить пароля текущего администратора.
unblock	Разблокировать администратора.
strong-password	Использовать сложный пароль: • **on**. • **off**.
num-auth-attempts	Установить максимальное количество неверных попыток аутентификации.

Параметр	Описание
block-time	Указать время блокировки учётной записи в случае достижения администратором максимального количества попыток аутентификации; указывается в секундах (максимальное значение: 3600 секунд).
min-length	Определить минимальную длину пароля (максимальное значение: 100 символов).
min-uppercase	Определить минимальное количество символов в верхнем регистре (максимальное значение: 100 символов).
min-lowercase	Определить минимальное количество символов в нижнем регистре (максимальное значение: 100 символов).
min-digits	Определить минимальное количество цифр (максимальное значение: 100 символов).
spec-characters	Определить минимальное количество специальных символов (максимальное значение: 100 символов).
char-repetition	Указать максимальную длину блока из одного и того же символа (максимальное значение: 100 символов).

Пример редактирования параметров учетных записей:

```
Admin@nodename# set settings administrators general block-time 400
```

Для просмотра текущих параметров защиты учётных записей администраторов используется следующая команда:

```
Admin@nodename# show settings administrators general

strong-password      : off
block-time           : 400
min-length           : 7
min-uppercase        : 1
min-lowercase        : 1
min-digits           : 1
spec-characters      : 1
char-repetition      : 2
num-auth-attempts    : 10
```

Настройка учётных записей администраторов

Настройка учётных записей администраторов производится на уровне **settings administrators administrators**.

Для создания учётной записи администратора используется следующая команда:

```
Admin@nodename# create settings administrators administrators
```

Далее необходимо указать тип учётной записи администратора (локальный, пользователь LDAP, группа LDAP, с профилем аутентификации) и установить соответствующие параметры:

Параметр	Описание
local	Добавить локального администратора: • **enabled**: включение/отключение учётной записи администратора: ◦ **on**. ◦ **off**. • **login**: логин администратора. • **display-name**: отображаемое имя администратора. • **description**: описание учётной записи администратора. • **admin-profile**: профиль администратора. Создание профилей администраторов рассмотрено далее. • **password**: пароль администратора.
ldap-user	Добавить пользователя из существующего домена (необходим корректно настроенный LDAP-коннектор; подробнее читайте в разделе Настройка LDAP-коннектора): • **enabled**: включение/отключение учётной записи администратора: ◦ **on**. ◦ **off**. • **login**: логин администратора в формате **domain\user**. Структура команды при указании данного параметра: • **display-name**: отображаемое имя администратора. • **connector**: название сконфигурированного ранее LDAP-коннектора.

Параметр	Описание
	• **description**: описание учётной записи администратора. • **admin-profile**: профиль администратора. Создание профилей администраторов рассмотрено далее. `Admin@nodename# create settings administrators administrators ldap-user admin-profile "test profile 1" connector "LDAP connector" description "Admin as domain user" login testd.local\user1 enabled on`
ldap-group	Добавить группу пользователей из существующего домена (необходим корректно настроенный LDAP-коннектор; подробнее читайте в разделе Настройка LDAP-коннектора): • **enabled**: включение/отключение учётной записи администратора: ◦ **on**. ◦ **off**. • **login**: логин администратора • **display-name**: отображаемое имя администратора. • **connector**: название используемого LDAP-коннектора. • **description**: описание учётной записи администратора. • **admin-profile**: профиль администратора. Создание профилей администраторов рассмотрено далее. `Admin@nodename# create settings administrators administrators ldap-group admin-profile "test profile 1" connector "LDAP connector" description "Domain admin group" login testd.local\users enabled on`
admin-auth-profile	Добавить администратора с профилем аутентификации (необходимы корректно настроенные серверы аутентификации; подробнее читайте в разделе Настройка серверов аутентификации): • **enabled**: включение/отключение учётной записи администратора: ◦ **on**. ◦ **off**.

Параметр	Описание
	• **login**: логин администратора. • **display-name**: отображаемое имя администратора. • **description**: описание учётной записи администратора. • **admin-profile**: профиль администратора. Создание профилей администраторов рассмотрено далее. • **auth-profile**: выбор профиля аутентификации из созданных ранее; подробнее о профилях аутентификации читайте в разделе Настройка профилей аутентификации.

Для редактирования параметров профиля используется команда:

```
Admin@nodename# set settings administrators administrators <admin-type>
<admin-login>
```

Параметры для редактирования аналогичны параметрам создания профиля администратора.

Для отображения информации о всех учётных записях администраторов:

```
Admin@nodename# show settings administrators administrators
```

Для отображения информации об определённой учётной записи администратора:

```
Admin@nodename# show settings administrators administrators <admin-
type> <admin-login>
```

Пример выполнения команды:

```
Admin@nodename# show settings administrators administrators ldap-user
testd.local\user1

login            : testd.local\user1
enabled          : on
type             : ldap_user
```

```
locked           : off
admin-profile    : test profile 1
```

Для удаления учётной записи используется команда:

```
Admin@nodename# delete settings administrators administrators <admin-type> <admin-login>
```

Пример команды:

```
Admin@nodename# delete settings administrators administrators ldap-user testd.local\user1
```

Настройка прав доступа профилей администраторов

Настройка прав доступа профилей администраторов производится на уровне **settings administrators profiles**.

Для создания профиля администратора используется следующая команда:

```
Admin@nodename# create settings administrators profiles
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля администратора.
description	Описание профиля администратора.
roles	Выбор роли для профиля администратора. Подробнее о ролях читайте в разделе Роли и ролевые разрешения пользователей.
permissions	Права доступа: • **no-access**: нет доступа. • **read**: только чтение. • **write**: чтение и запись.

Для редактирования профиля используется команда:

```
Admin@nodename# set settings administrators profiles <profile-name>
<parameter>
```

Параметры для редактирования аналогичны параметрам создания профиля администратора.

Для просмотра информации о всех профилях администраторов:

```
Admin@nodename# show settings administrators profiles
```

Для отображения информации об определённом профиле:

```
Admin@nodename# show settings administrators profiles <profile-name>
```

Чтобы удалить профиль администратора:

```
Admin@nodename# delete settings administrators profiles <profile-name>
```

Управление сессиями администраторов

С использованием следующих команд возможен просмотр активных сессий администраторов, прошедших аутентификацию в веб-консоли или CLI, и закрытие сессий (уровень: **settings administrators admin-sessions**).

Просмотр сессий администраторов устройства (возможен просмотр сессии отдельного администратора: необходимо из предложенного списка выбрать IP-адрес, с которого была произведена аутентификация):

```
Admin@nodename# show settings administrators admin-sessions
```

Для отображения сессий доступно использование фильтра:

- **ip**: IP-адрес, с которого вошел администратор.
- **source**: где была произведена аутентификация: CLI (**cli**), веб-консоль (**web**) или подключение по SSH (**ssh**).

- **admin-login**: имя администратора.

```
Admin@nodename# show settings administrators admin-sessions ( node
<node-name> ip <session-ip> source <cli | web | ssh> admin-login
<administrator-login> )
```

Команда для закрытия сессии администратора; необходимо из предложенного списка выбрать IP-адрес, с которого была произведена аутентификация:

```
Admin@nodename# execute termination admin-sessions <IP-address/
connection type>
```

Пример выполнения команд:

```
Admin@nodename# show settings administrators admin-sessions

admin-login           : Admin
source                : ssh
session_start_date    : 2023-08-10T11:33:47Z
ip                    : 127.0.0.1
node                  : <node-name>

admin-login           : Admin
source                : web
session_start_date    : 2023-08-10T11:33:10Z
ip                    : 10.0.2.2
node                  : <node-name>

Admin@nodename# execute termination admin-sessions 10.0.2.2/web

Admin@nodename# show settings administrators admin-sessions

admin-login           : Admin
source                : ssh
session_start_date    : 2023-08-10T11:33:47Z
ip                    : 127.0.0.1
node                  : <node-name>
```

При закрытии сессии администраторов возможно использование фильтра (<filter>). Параметры фильтрации аналогичны параметрам команды **show**.

```
Admin@nodename# execute termination admin-sessions ( node <node-name>
ip <session-ip> source <cli | web | ssh> admin-login <administrator-
login> )
```

Настройка сертификатов

Раздел **Сертификаты** находится на уровне **settings certificates**.

Для импорта сертификатов предназначена команда:

```
Admin@nodename# import settings certificates
```

Далее необходимо указать параметры:

Параметр	Описание
name	Название сертификата, под которым он будет отображен в списке сертификатов.
description	Описание сертификата.
certificate-data	Данные сертификата в формате PEM.
private-key	Приватный ключ сертификата в формате PEM.
passphrase	Пароль для приватного ключа, если таковой требуется.
certificate-chain	Цепочка сертификатов вышестоящих центров сертификации, которые участвовали в создании сертификата, в формате PEM.

Для экспорта доступны сертификаты, вся цепочка сертификатов:

```
Admin@nodename# export settings certificates <certificate-name>
Admin@nodename# export settings certificates <certificate-name> with-chain on
```

С использованием командной строки возможно создание сертификата и CSR:

```
Admin@nodename# create settings certificates type <certificate | csr>
```

Далее необходимо указание следующих параметров:

Параметр	Описание
name	Название сертификата.
description	Описание сертификата.
country	Страна, в которой выписывается сертификат.
state	Область/штат, в котором выписывается сертификат.
locality	Город, в котором выписывается сертификат.
organization	Название организации, для которой выписывается сертификат.
common-name	Имя сертификата. Рекомендуется использовать только символы латинского алфавита для совместимости с большинством браузеров.
email	Email компании.

Команда для управления сертификатом:

```
Admin@nodename# set settings certificates <certificate-name>
```

Доступны параметры:

Параметр	Описание
name	Название сертификата.
description	Описание сертификата.

Параметр	Описание
role	Тип сертификата: • **web-cert-chain**: цепочка сертификатов веб-консоли. • **web-ssl**: сертификат, использующийся для создания безопасного HTTPS-подключения администратора к веб-консоли UserGate. • **none**.
certificate-chain	Цепочка сертификатов в формате PEM.

Для удаления сертификата:

```
Admin@nodename# delete settings certificates <certificate-name>
```

Команды для просмотра информации об определённом сертификате или о всех сертификатах:

```
Admin@nodename# show settings certificates
Admin@nodename# show settings certificates <certificate-name>
```

Настройка серверов аутентификации

Раздел Серверы аутентификации позволяет произвести настройку LDAP-коннектора, серверов RADIUS, TACACS+. Настройка серверов аутентификации производится на уровне **users auth-server** и будет рассмотрена далее в соответствующих разделах.

Настройка LDAP-коннектора

Настройка LDAP-коннектора производится на уровне **users auth-server ldap**.

Для создания LDAP-коннектора используется команда:

```
Admin@nodename# create users auth-server ldap <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя LDAP-коннектора.
enabled	Включение/отключение сервера аутентификации.
description	Описание LDAP-коннектора.
ssl	Определяет: • **on** — использование SSL-соединения для подключения к LDAP-серверу. • **off** — подключение к LDAP-серверу без использования SSL-соединения.
address	IP-адрес контроллера или название домена LDAP.
bind-dn	Имя пользователя, которое будет использоваться для подключения к серверу; указывается в формате DOMAIN\username или username@domain. Пользователь должен быть заведён в домене.
password	Пароль пользователя для подключения к домену.
domains	Список доменов, которые обслуживаются указанным контроллером домена.
search-roots	Список путей в сервере LDAP, начиная с которых система будет осуществлять поиск пользователей и групп. Необходимо указывать полное имя, например, ou=Office,dc=example,dc=com. Если пути поиска не указаны, то поиск производится по всему каталогу, начиная от корня.

Для редактирования информации о существующем LDAP-коннекторе используется команда:

```
Admin@nodename# set users auth-server ldap <ldap-server-name>
<parameter>
```

Параметры, доступные для обновления, аналогичны параметрам создания LDAP-коннектора.

Команда для отображения информации о LDAP-коннекторе:

```
Admin@nodename# show users auth-server ldap <ldap-server-name>
```

Примеры команд создания и редактирования LDAP-коннектора:

```
Admin@nodename# create users auth-server ldap name "New LDAP connector"
ssl on address 10.10.0.10 bind-dn ug@testd.local password 12345 domains
[ testd.local ] search-roots [ dc=testd,dc=local ] enabled on
Admin@nodename# show users auth-server ldap "New LDAP connector"

name             : New LDAP connector
enabled          : on
ssl              : on
address          : 10.10.0.10
bind-dn          : ug@testd.local
domains          : testd.local
search-roots     : dc=testd,dc=local
keytab_exists    : off
Admin@nodename# set users auth-server ldap "New LDAP connector"
description "New LDAP connector description"
Admin@nodename# show users auth-server ldap "New LDAP connector"

name             : New LDAP connector
description      : New LDAP connector description
enabled          : on
ssl              : on
address          : 10.10.0.10
bind-dn          : ug@testd.local
domains          : testd.local
search-roots     : dc=testd,dc=local
keytab_exists    : off
```

Для удаления LDAP-коннектора используется команда:

```
Admin@nodename# delete users auth-server ldap <ldap-server-name>
<parameter>
```

Также возможно удаления отдельных параметров LDAP-коннектора. Для удаления доступны следующие параметры:

- **domains**.

- **search-roots**.

Настройка RADIUS-сервера

Настройка RADIUS-сервера производится на уровне **users auth-server radius**.

Для создания сервера аутентификации RADIUS используется команда со следующей структурой:

```
Admin@nodename# create users auth-server radius <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя RADIUS-сервера.
enabled	Включение/отключение сервера аутентификации.
description	Описание сервера аутентификации.
secret	Общий ключ, используемый протоколом RADIUS для аутентификации.
addresses	IP-адрес и UDP-порт, на котором сервер RADIUS слушает запросы (по умолчанию порт 1812); указывается в формате <ip:port>.

Команда для обновления информации о сервере RADIUS:

```
Admin@nodename# set users auth-server radius <radius-server-name>
<parameter>
```

Параметры, которые могут быть обновлены, соответствуют параметрам, указание которых возможно при создании сервера аутентификации.

Команда для отображения информации о RADIUS-сервере:

```
Admin@nodename# show users auth-server radius <radius-server-name>
```

Примеры команд создания и редактирования RADIUS-сервера:

```
Admin@nodename# create users auth-server radius name "New RADIUS
server" addresses [ 10.10.0.9:1812 ] secret 12345 enabled on
Admin@nodename# show users auth-server radius "New RADIUS server"

name           : New RADIUS server
enabled        : on
addresses      :
    host    : 10.10.0.9
    port    : 1812
Admin@nodename# set users auth-server radius "New RADIUS server"
description "New RADIUS server description"
Admin@nodename# show users auth-server radius "New RADIUS server"

name           : New RADIUS server
description    : New RADIUS server description
enabled        : on
addresses      :
    host    : 10.10.0.9
    port    : 1812
```

Для удаления сервера:

```
Admin@nodename# delete users auth-server radius <radius-server-name>
<parameter>
```

Также возможно удаления отдельных параметров RADIUS-сервера. Для удаления доступны следующие параметры:

- **addresses**.

Настройка сервера TACACS+

Настройка сервера TACACS+ производится на уровне **users auth-server tacacs**.

Для создания сервера аутентификации TACACS+ используется команда со следующей структурой:

```
Admin@nodename# create users auth-server tacacs <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя сервера TACACS+.
enabled	Включение/отключение сервера.
description	Описание сервера аутентификации.
secret	Общий ключ, используемый протоколом TACACS+ для аутентификации.
address	IP-адрес сервера TACACS+.
port	UDP-порт, на котором сервер TACACS+ слушает запросы на аутентификацию. По умолчанию это порт UDP 1812.
single-connection	Использовать одно TCP-соединение для работы с сервером TACACS+.
timeout	Время ожидания сервера TACACS+ для получения аутентификации. По умолчанию 4 секунды.

Команда для редактирования информации о сервере TACACS+:

```
Admin@nodename# set users auth-server tacacs <tacacs-server-name>
<parameter>
```

Параметры, которые могут быть обновлены, соответствуют параметрам, указание которых возможно при создании сервера аутентификации.

Команда для отображения информации о сервере TACACS+:

```
Admin@nodename# show users auth-server tacacs <tacacs-server-name>
```

Примеры команд для создания и редактирования сервера TACACS+:

```
Admin@nodename# create users auth-server tacacs address 10.10.0.11 name
"New TACACS+ server" port 1812 secret 12345 enabled on
Admin@nodename# show users auth-server tacacs "New TACACS+ server"

name                 : New TACACS+ server
```

```
enabled              : on
address              : 10.10.0.11
port                 : 1812
single-connection    : off
timeout              : 4
Admin@nodename# set users auth-server tacacs "New TACACS+ server"
description "New TACACS+ server description"
Admin@nodename# show users auth-server tacacs "New TACACS+ server"

name                 : New TACACS+ server
description          : New TACACS+ server description
enabled              : on
address              : 10.10.0.11
port                 : 1812
single-connection    : off
timeout              : 4
```

Для удаления сервера:

```
Admin@nodename# delete users auth-server tacacs <tacacs-server-name>
```

Настройка профилей аутентификации

Настройка профилей аутентификации производится на уровне **users auth-profile**.

Для создания профиля аутентификации используется следующая команда:

```
Admi@nodename# create users auth-profile <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля.

Параметр	Описание
description	Описание профиля.
idle-time	Время бездействия до отключения; указывается в секундах. Через указанный промежуток времени при отсутствии активности пользователь перейдёт в статус Unknown user.
expiration-time	Время жизни аутентифицированного пользователя; указывается в секундах. Через указанный промежуток времени пользователь перейдёт в статус Unknown user; необходима повторная аутентификация пользователя.
max-attempts	Число неудачных попыток аутентификации до блокировки учётной записи пользователя.
lockout-time	Время, на которое блокируется учетная запись пользователя при достижении указанного числа неудачных попыток аутентификации; указывается в секундах.
auth-methods	Метод аутентификации: • **ldap**: аутентификация с использованием LDAP-коннектора. • **radius**: аутентификация с использованием RADIUS-сервера. • **tacacs**: аутентификация с использованием сервера TACACS+.

Команда для редактирования настроек профилей аутентификации:

```
Admin@nodename# set users auth-profile <auth-profile-name> <parameter>
```

Для обновления доступен список параметров, аналогичный списку параметров команды **create**.

Пример создания и редактирования профиля аутентификации пользователя:

```
Admin@nodename# create users auth-profile name "New LDAP auth profile"
auth-methods ldap [ "New LDAP connector" ]
Admin@nodename# show users auth-profile "New LDAP auth profile"

name               : New LDAP auth profile
max-attempts       : 5
```

```
idle-time          : 900
expiration-time    : 86400
lockout-time       : 300
mfa                : none
auth-methods       :
    http-basic         : off
    local-user-auth    : off
    policy-accept      : off
Admin@nodename# set users auth-profile "New LDAP auth profile"
description "New LDAP auth profile description"
Admin@nodename# show users auth-profile "New LDAP auth profile"

name               : New LDAP auth profile
description        : New LDAP auth profile description
max-attempts       : 5
idle-time          : 900
expiration-time    : 86400
lockout-time       : 300
mfa                : none
auth-methods       :
    http-basic         : off
    local-user-auth    : off
    policy-accept      : off
    ldap               : New LDAP connector
```

Через интерфейс командной строки возможно удаления всего профиля или отдельных способов аутентификации, заданных в профиле. Для этого используются следующие команды.

Для удаления профиля аутентификации:

```
Admin@nodename# delete users auth-profile <auth-profile-name>
```

Для удаления методов аутентификации, заданных в профиле, необходимо указать метод аутентификации (доступные методы авторизации перечислены в таблице выше):

```
Admin@nodename# delete users auth-profile <auth-profile-name> auth-
methods <auth-metod>
```

Роли пользователей

Роль пользователя — это набор ролевых разрешений. Ролевое разрешение — это возможность администратору совершать определенные действия, например, добавлять или удалять вложение из созданного инцидента, создавать правило срабатывания, создать или закрыть инцидент и т.д. Роли назначаются профилям администраторов, которые присваиваются администраторам.

Создание и настройка ролей пользователей производится на уровне **users roles**.

Для создания ролей и назначения ролевых разрешений используется команда:

```
Admin@nodename# create users roles <role-name> description <role-
description> permissions [ <permissions> ]
```

Подробнее о ролях и списке имеющихся ролевых разрешений читайте в разделе Роли и ролевые разрешения пользователей Руководства администратора SIEM.

Для редактирования созданных ранее ролей и ролевых ограничений используется команда:

```
Admin@nodename# set users roles <role-name> description <role-
description> permissions [ <permissions> ]
```

Для удаления ранее созданных ролей или отдельных ролевых разрешений в ранее созданных ролях используется команда:

```
Admin@nodename# delete users roles <role-name> permissions
[ <permissions> ]
```

Каталоги пользователей

Для работы с каталогами пользователей необходим корректно настроенный LDAP-коннектор, который позволяет получать информацию о пользователях и группах Active Directory или других LDAP-серверов. Пользователи и группы могут быть использованы при настройке политик, применяемых к управляемым устройствам.

Создание и настройка каталога пользователей производится на уровне **users catalogs ldap**.

Для создания каталога используется команда:

```
Admin@nodename# create users catalogs ldap <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя LDAP-коннектора.
enabled	Включение/отключение сервера аутентификации.
description	Описание LDAP-коннектора.
ssl	Определяет: • **on** — использование SSL-соединения для подключения к LDAP-серверу. • **off** — подключение к LDAP-серверу без использования SSL-соединения.
address	IP-адрес контроллера или название домена LDAP.
bind-dn	Имя пользователя, которое будет использоваться для подключения к серверу; указывается в формате DOMAIN\username или username@domain. Пользователь должен быть заведён в домене.
password	Пароль пользователя для подключения к домену.
domains	Список доменов, которые обслуживаются указанным контроллером домена.
search-roots	Список путей в сервере LDAP, начиная с которых система будет осуществлять поиск пользователей и групп.

Параметр	Описание
	Необходимо указывать полное имя, например, ou=Office,dc=example,dc=com. Если пути поиска не указаны, то поиск производится по всему каталогу, начиная от корня.

Для редактирования информации о существующем каталоге используется команда:

```
Admin@nodename# set users catalogs ldap <ldap-server-name> <parameter>
```

Параметры, доступные для обновления, аналогичны параметрам создания каталога.

Команда для отображения информации о каталоге пользователей:

```
Admin@nodename# show users catalogs ldap <ldap-server-name>
```

Для удаления каталога используется команда:

```
Admin@nodename# delete users catalogs ldap <ldap-server-name>
<parameter>
```

Также возможно удаления отдельных параметров LDAP-коннектора. Для удаления доступны следующие параметры:

- **domains**.
- **search-roots**.

НАСТРОЙКА СЕТИ

Зоны

Данный раздел находится на уровне **network zone**. Команда для создания новой зоны:

```
Admin@nodename# create network zone
```

Далее необходимо указать параметры зоны:

Параметр	Описание
name	Название зоны.
description	Описание зоны.
dos-protection-syn	Защита зоны от сетевого флуда для протокола TCP (SYN-flood): • **enabled**: включение/отключение защиты. ◦ **on**. ◦ **off**. • **aggregate**: ◦ **on** — считаются все пакеты, входящие в интерфейсы данной зоны. ◦ **off** — пакеты считаются отдельно для каждого IP-адреса. • **alert-threshold**: порог уведомления; если количество запросов превышает данный порог, то происходит запись события в системный журнал. • **drop-threshold**: порог отбрасывания пакетов; если количество запросов превышает указанное значение, то UserGate отбрасывает пакеты и записывает данное событие в системный журнал. • **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-udp	Защита зоны от сетевого флуда для протокола UDP: • **enabled**: включение/отключение защиты. ◦ **on**. ◦ **off**. • **aggregate**: ◦ **on** — считаются все пакеты, входящие в интерфейсы данной зоны. ◦ **off** — пакеты считаются отдельно для каждого IP-адреса. • **alert-threshold**: порог уведомления; если количество запросов превышает данный порог, то происходит запись события в системный журнал.

Параметр	Описание
	• **drop-threshold**: порог отбрасывания пакетов; если количество запросов превышает указанное значение, то UserGate отбрасывает пакеты и записывает данное событие в системный журнал. • **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-icmp	Защита зоны от сетевого флуда для протокола ICMP: • **enabled**: включение/отключение защиты. ◦ **on**. ◦ **off**. • **aggregate**: ◦ **on** — считаются все пакеты, входящие в интерфейсы данной зоны. ◦ **off** — пакеты считаются отдельно для каждого IP-адреса. • **alert-threshold**: порог уведомления; если количество запросов превышает данный порог, то происходит запись события в системный журнал. • **drop-threshold**: порог отбрасывания пакетов; если количество запросов превышает указанное значение, то UserGate отбрасывает пакеты и записывает данное событие в системный журнал. • **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты.
enabled-services	Параметры контроля доступа зоны: • **"Any ICMP"**: разрешение использования команды ping адреса UserGate. • **SNMP**: доступ к UserGate по протоколу SNMP (UDP 161). • **rpc**: XML-RPC для управления - позволяет управлять продуктом по API (TCP 4040). • **VRRP**: сервис, необходимый для объединения нескольких узлов UserGate в отказоустойчивый кластер (IP протокол 112). • **"CLI over SSH"**: доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200. • **Cluster**: сервис, необходимый для объединения нескольких узлов UserGate в кластер (TCP 4369, TCP 9000-9100). • **"Admin Console"**: доступ к веб-консоли управления (TCP 8001).

Параметр	Описание
service-addresses	Указание разрешённых IP-адресов для сервисов: • **service**: выбор сервисов (список соответствует **enabled-services**). • **allowed-addresses**: разрешённые IP-адреса: ◦ **geoip** — код GeoIP. ◦ **ip-list** — заранее созданный в библиотеке элементов список IP-адресов.
antispoof-enable	Включение/отключение защиты от IP-спуфинга: • **on**. • **off**.
antispoof-negate	Возможные значения: • **on**. • **off**. При **antispoof-negate on** адреса источников, указанные в значении **ip-spoofing-networks**, будут являться адресами, которые не могут быть получены на интерфейсах данной зоны. В этом случае будут отброшены пакеты с указанными IP-адресами источников.
sessions-limit-enabled	Включение ограничения количества одновременных сессий с одного IP-адреса: • **on**. • **off**.
sessions-limit-exclusions	Добавление списка IP-адресов, для которых ограничение на количество одновременных сессий не будет действовать.
sessions-limit-threshold	Максимально возможное количество одновременных сессий с одного IP-адреса.
geoip	Коды GeoIP, которые используются в защите от IP-спуфинга.
ip-list	Список IP-адресов, которые используются в защите от IP-спуфинга.

Пример создания новой зоны:

```
Admin@nodename# create network zone name Test_zone description
"Test_zone description" antispoof-enable on enabled-services [ "Any
ICMP" DNS ] dos-protection-icmp enabled on
```

Для редактирования параметров зоны:

```
Admin@nodename# set network zone <zone-name>
```

Пример редактирования параметров зоны:

```
Admin@nodename# set network zone Test_zone dos-protection-syn enabled
on
```

Команда удаления зоны или её параметров:

```
Admin@nodename# delete network zone <zone-name>
```

Параметры, доступные для удаления:

Параметр	Описание
dos-protection-syn	Защита зоны от сетевого флуда для протокола TCP (SYN-flood): • **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-udp	Защита зоны от сетевого флуда для протокола UDP: • **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-icmp	Защита зоны от сетевого флуда для протокола ICMP: • **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты.
enabled-services	Установленные ранее параметры контроля доступа в данной зоне
geoip	Коды GeoIP, которые используются в защите от IP-спуфинга.

Параметр	Описание
ip-list	Список IP-адресов, которые используются в защите от IP-спуфинга.

Команда для просмотра настроек зоны:

```
Admin@nodename# show network zone <zone-name>
```

Интерфейсы

Настройка интерфейсов производится на уровне **network interface:**

Настройка adapter

Сетевые адаптеры настраиваются на уровне **network interface adapter**.

Создать сетевой адаптер нельзя. Для обновления существующего сетевого адаптера используется команда:

```
Admin@nodename# set network interface adapter <adapter_name>
```

Далее необходимо указать параметры сетевого адаптера:

Параметр	Описание
enabled	Включение/отключение сетевого интерфейса: • **on**. • **off**.
description	Описание сетевого интерфейса.
alias	Алиас/псевдоним интерфейса.
iface-type	Тип интерфейса: • **l3**: интерфейс, работающий в режиме Layer 3 (можно назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах, это стандартный режим работы интерфейса).

Параметр	Описание
	• **mirror**: интерфейс, работающий в режиме Mirror (может получать трафик со SPAN-порта сетевого оборудования для его анализа).
iface-mode	Режим назначения IP-адреса: • **dhcp**: получение динамического IP-адреса по DHCP. • **manual**: без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса.
zone	Зона, которой будет принадлежать интерфейс.
link-info	Настройка параметров сетевого интерфейса: • **bc_forwarding**: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • **proxy_arp**, **proxy_arp_vlan**: механизм Proxy ARP. Параметр **proxy_arp** — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; **proxy_arp_vlan** — UserGate будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: `Admin@nodename# create network interface <iface-type> … link-info [ key/value ]` где **key** — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). **value** — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. **Важно!** Удаление заданных параметров недоступно.
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся в следующем виде: **[<ip_address/mask>]** или **[<ip_address/mask> <ip_address/mask>]**, если необходимо назначить несколько IP-адресов (адреса

Параметр	Описание
	перечисляются через пробел); маска подсети задаётся в десятичном виде. **Важно!** Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса.
mtu	Указание размера MTU.

Команда удаления адаптера или его параметров:

```
Admin@nodename# delete network interface adapter <adapter-name>
```

Параметры, доступные для удаления:

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay server-address	IP-адрес сервера DHCP.

Команда для отображения информации о всех сетевых адаптерах:

```
Admin@nodename# show network interface adapter
```

Для отображения информации об адаптере:

```
Admin@nodename# show network interface adapter <adapter-name>
```

Настройка VLAN

Интерфейсы VLAN настраиваются на уровне **network interface vlan**.

Команда для добавления нового VLAN-интерфейса:

```
Admin@nodename# create network interface vlan
```

Далее необходимо указать параметры:

Параметр	Описание
enabled	Включение/отключение VLAN-интерфейса: • **on**. • **off**.
description	Описание интерфейса.
alias	Алиас/псевдоним интерфейса.
iface-type	Тип интерфейса: • **l3**: Layer 3 (можно назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах, это стандартный режим работы интерфейса). • **mirror**: интерфейс, работающий в режиме Mirror (может получать трафик со SPAN-порта сетевого оборудования для его анализа).
iface-mode	Режим назначения IP-адреса: • **dhcp**: получение динамического IP-адреса по DHCP. • **manual**: без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса.
tag	Тег VLAN. Допускается создание до 4094 интерфейсов.
node-name	Имя узла кластера, на котором создаётся VLAN.
interface	Физический интерфейс, на котором создается VLAN.
zone	Зона, которой будет принадлежать интерфейс.
link-info	Настройка параметров сетевого интерфейса: • **bc_forwarding**: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • **proxy_arp**, **proxy_arp_vlan**: механизм Proxy ARP. Параметр **proxy_arp** — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; **proxy_arp_vlan** — UserGate будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате:

Параметр	Описание
	`Admin@nodename# create network interface <iface-type> … link-info [ key/value ]` где **key** — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). **value** — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. **Важно!** Удаление заданных параметров недоступно.
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся в следующем виде: **[<ip_address/mask>]** или **[<ip_address/mask> <ip_address/mask>]**, если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел); маска подсети задаётся в десятичном виде. **Важно!** Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса.
mtu	Указание размера MTU.

dhcp-relay	Настройка работы DHCP-релея на интерфейсе. Необходимо указать:
	
	• **enabled**: включение/отключения релея:
	  ◦ **on**.
	  ◦ **off**.
	• **utm-address**: IP-адрес интерфейса UserGate, на который добавляется функция релея.
	• **server-address**: адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Редактирование существующего VLAN:

```
Admin@nodename# set network interface vlan <vlan-name>
```

Параметры, доступные для обновления, аналогичны параметрам создания VLAN, кроме **tag**, **node-name**, **interface** (изменение значений этих параметров недоступно).

Команда удаления VLAN-интерфейса или его параметров:

```
Admin@nodename# delete network interface vlan <vlan-name>
```

Параметры, доступные для удаления:

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay server-address	IP-адрес сервера DHCP.

Чтобы отобразить информацию о всех интерфейсах VLAN:

```
Admin@nodename# show network interface vlan
```

или об определённом интерфейсе:

```
Admin@nodename# show network interface vlan <vlan-name>
```

Настройка bond-интерфейса

Настройка бонд-интерфейса производится на уровне **network interface bond**.

Команда для создания бонд-интерфейса:

```
Admin@nodename# create network interface bond
```

Параметры, которые необходимо указать:

Параметр	Описание
enabled	Включение/отключение интерфейса: • **on**. • **off**.

Параметр	Описание
interface-name	Необходимо ввести номер, который будет отображён в имени интерфейса (например 1, тогда название созданного интерфейса будет bond1).
description	Описание интерфейса.
alias	Алиас/псевдоним интерфейса.
node-name	Узел кластера, на котором будет создан бонд-интерфейс.
zone	Зона, которой будет принадлежать бонд.
link-info	Настройка параметров сетевого интерфейса: • **bc_forwarding**: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • **proxy_arp**, **proxy_arp_vlan**: механизм Proxy ARP. Параметр **proxy_arp** — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; **proxy_arp_vlan** — UserGate будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: `Admin@nodename# create network interface <iface-type> … link-info [ key/value ]` где **key** — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). **value** — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. **Важно!** Удаление заданных параметров недоступно.
bonding	Дополнительные параметры бонд-интерфейса: • **mode** — режим работы бонда: ◦ **round-robin**: режим Round robin (пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая

Параметр	Описание
	последним. Эта политика применяется для балансировки нагрузки и отказоустойчивости). ◦ **active-backup**: режим Active backup (только один сетевой интерфейс из объединенных будет активным. Другой интерфейс может стать активным только в том случае, когда упадет текущий активный интерфейс. При такой политике MAC-адрес бонд-интерфейса виден снаружи только через один сетевой порт, во избежание появления проблем с коммутатором. Данная политика применяется для обеспечения отказоустойчивости). ◦ **xor**: режим XOR (передача распределяется между сетевыми картами используя формулу: [(«MAC-адрес источника» XOR «MAC-адрес назначения») по модулю «число интерфейсов»]. Получается, одна и та же сетевая карта передает пакеты одним и тем же получателям. Опционально распределение передачи может быть основано и на политике «xmit_hash». Политика XOR применяется для балансировки нагрузки и обеспечения отказоустойчивости). ◦ **broadcast**: режим Broadcast (передает все на все сетевые интерфейсы. Эта политика применяется для отказоустойчивости). ◦ **802.3ad**: режим IEEE 802.3ad (режим работы, установленный по умолчанию, поддерживается большинством сетевых коммутаторов. Создаются агрегированные группы сетевых карт с одинаковой скоростью и дуплексом. При таком объединении передача задействует все каналы в активной агрегации согласно стандарту IEEE 802.3ad. Выбор, через какой интерфейс отправлять пакет, определяется политикой; по умолчанию используется XOR-политика, можно также использовать «xmit_hash» политику). ◦ **transmit**: режим Adaptive transmit load balancing (исходящий трафик распределяется в зависимости от загруженности каждой сетевой карты (определяется скоростью загрузки). Не требует дополнительной настройки на коммутаторе. Входящий трафик приходит на текущую сетевую карту. Если она выходит из строя, то другая сетевая карта берет себе MAC-адрес вышедшей из строя карты). ◦ **load**: режим Adaptive load balancing. Включает в себя предыдущую политику плюс осуществляет балансировку входящего трафика. Не требует

Параметр	Описание
	дополнительной настройки на коммутаторе. Балансировка входящего трафика достигается путем ARP-переговоров. Драйвер перехватывает ARP-ответы, отправляемые с локальных сетевых карт наружу, и переписывает MAC-адрес источника на один из уникальных MAC-адресов сетевой карты, участвующей в объединении. Таким образом, различные пиры используют различные MAC-адреса сервера. Балансировка входящего трафика распределяется последовательно (round-robin) между интерфейсами. • **mii-monitoring**: периодичность MII-мониторинга в миллисекундах. Определяет, как часто будет проверяться состояние линии на наличие отказов. • **down-delay**: время (в миллисекундах) задержки перед отключением интерфейса, если произошел сбой соединения. Эта опция действительна только для мониторинга MII (miimon). Значение параметра должно быть кратным значениям miimon. • **up-delay**: время задержки в миллисекундах, перед тем как поднять канал при обнаружении его восстановления. Этот параметр возможен только при MII-мониторинге (miimon). Значение параметра должно быть кратным значениям miimon. • **lacp-rate**: интервал, с которым будут передаваться партнером LACPDU-пакеты в режиме 802.3ad. Возможные значения: ◦ **slow**: запрос партнера на передачу LACPDU-пакетов каждые 30 секунд. ◦ **fast**: запрос партнера на передачу LACPDU-пакетов каждую секунду. • **failover-mac**: определение способа назначения MAC-адресов на объединенные интерфейсы в режиме Active backup при переключении интерфейсов. Возможные значения: ◦ **disabled**: устанавливает одинаковый MAC-адрес на всех интерфейсах во время переключения. ◦ **active**: MAC-адрес на бонд-интерфейсе будет всегда таким же, как на текущем активном интерфейсе. MAC-адреса на резервных интерфейсах не изменяются. MAC-адрес на бонд-интерфейсе меняется во время обработки отказа. ◦ **follow**: MAC-адрес на бонд-интерфейсе будет таким же, как на первом интерфейсе, добавленном в объединение. На втором и последующем интерфейсе этот MAC не

Параметр	Описание
	устанавливается, пока они в резервном режиме. MAC-адрес прописывается во время обработки отказа, когда резервный интерфейс становится активным, он принимает новый MAC (тот, что на бонд-интерфейсе), а старому активному интерфейсу прописывается MAC, который был на текущем активном. • **xmit-hash**: определение хэш-политики передачи пакетов через объединенные интерфейсы в режиме XOR или IEEE 802.3ad. Возможные значения: ◦ **l2**: использует только MAC-адреса для генерации хэша. При этом алгоритме трафик для конкретного сетевого хоста будет отправляться всегда через один и тот же интерфейс. Алгоритм совместим с IEEE 802.3ad. ◦ **l2-3**: использует как MAC-адреса, так и IP-адреса для генерации хэша. Алгоритм совместим с IEEE 802.3ad. ◦ **l3-4**: используются IP-адреса и протоколы транспортного уровня (TCP или UDP) для генерации хэша. Алгоритм не всегда совместим с IEEE 802.3ad, так как в пределах одного и того же TCP- или UDP-взаимодействия могут передаваться как фрагментированные, так и нефрагментированные пакеты. Во фрагментированных пакетах порт источника и порт назначения отсутствуют. В результате в рамках одной сессии пакеты могут дойти до получателя не в том порядке, так как отправляются через разные интерфейсы. • **interface**: интерфейсы, которые будут объединены в бонд.
iface-mode	Режим назначения IP-адреса: • **dhcp**: получение динамического IP-адреса по DHCP. • **manual**: без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса.
iface-type	Тип создаваемого интерфейса: • **l3** — Layer 3 интерфейс. • **mirror** — интерфейс зеркалирования трафика.
ip-addresses	Назначение интерфейсу IP-адреса.

Параметр	Описание
	Адрес задаётся в следующем виде: **[<ip_address/mask>]** или **[<ip_address/mask> <ip_address/mask>]**, если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел); маска подсети задаётся в десятичном виде. **Важно!** Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса.
mtu	Указание размер MTU.

Обновление существующего бонд-интерфейса:

```
Admin@nodename# set network interface bond <bond-name>
```

Параметры, доступные для обновления, аналогичны параметрам создания бонд-интерфейс, кроме **interface-name**, **node-name** (изменение значений этих параметров недоступно).

Команда удаления бонд-интерфейса или его параметров:

```
Admin@nodename# delete network interface bond <bond-name>
```

Параметры, доступные для удаления:

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay server-address	IP-адрес сервера DHCP.
bonding interface	Интерфейсы, объединённые в бонд.

Чтобы отобразить информацию о всех бонд-интерфейсах:

```
Admin@nodename# show network interface bond
```

или об определённом интерфейсе:

```
Admin@nodename# show network interface bond <bond-name>
```

Шлюзы

Данный раздел находится на уровне **network gateway**.

Для добавления нового шлюза используется команда:

```
Admin@nodename# create network gateway
```

Доступные параметры:

Параметр	Описание
enabled	Включение/отключение шлюза: • **on**. • **off**.
name	Название шлюза.
description	Описание шлюза.
interface	Интерфейс, использующийся для выхода в Интернет.
ip	IP-адрес шлюза.
node-name	Выбор узла кластера, для которого настраивается шлюз.
weight	Вес шлюза (чем больше вес, тем большая доля трафика идет через шлюз).
balancing	Режим балансировки - весь трафик в интернет будет распределен между шлюзами в соответствии с указанными весами: • **on**. • **off**.
default	

Параметр	Описание
	Использование данного шлюза в качестве шлюза по умолчанию: • **on**. • **off**.

Обновление параметров шлюза:

```
Admin@nodename# set network gateway <gateway-name>
```

Список параметров, доступных для изменения, аналогичен списку, доступному при создании шлюза.

Команда для удаления шлюза:

```
Admin@nodename# delete network gateway <gateway-name>
```

Чтобы отобразить информацию о всех шлюзах:

```
Admin@nodename# show network gateway
```

или об определённом шлюзе:

```
Admin@nodename# show network gateway <gateway-name>
```

Настройка маршрутизации

В данном разделе описана настройка маршрутизации с использованием интерфейса командной строки. Настройка производится на уровне **network routes**.

Для добавления нового статического маршрута используется команда:

```
Admin@nodename# create network routes <parameters>
```

Далее указываются параметры:

Параметр	Описание
enabled	Включение/отключение использования статического маршрута: • **on**. • **off**.
name	Имя маршрута.
description	Описание маршрута.
node-name	Выбор узла кластера для настройки маршрутизации.
type	Тип маршрута: • **unicast** — стандартный тип маршрута. Пересылает трафик, адресованный на адреса назначения, через заданный шлюз. • **unreachable** — трафик отбрасывается. Источнику отправляется ICMP сообщение host unreachable (type 3 code 1). • **prohibit** — трафик отбрасывается. Источнику отправляется ICMP сообщение host unreachable (type 3 code 13). • **blackhole** — трафик отбрасывается (теряется), не сообщая источнику о том, что данные не достигли адресата.
destination-ip	IP-адрес подсети назначения; указывается в формате <ip/mask>.
gateway	IP-адрес шлюза, через который будет доступна указанная подсеть; этот IP-адрес должен быть доступен с устройства.
interface	Интерфейс, через который будет добавлен маршрут.
metric	Метрика маршрута. Если маршрутов в данную сеть несколько: чем меньше метрика, тем более приоритетен маршрут.

Пример добавления статического маршрута:

```
Admin@nodename# create network routes name test_route description "Test
static route" destination-ip 192.168.200.0/2
```

```
4 gateway 192.168.100.100 interface port1 type unicast metric 1 enabled
on
Admin@nodename#

Admin@nodename# show network routes test_route

name              : test_route
description       : Test static route
enabled           : on
node-name         : testnode1
interface         : port1
type              : unicast
destination-ip    : 192.168.200.0/24
gateway           : 192.168.100.100
metric            : 1
```

Чтобы изменить параметры созданного ранее статического маршрута, используйте команду:

```
Admin@nodename# set network routes <route-name>
```

Параметры, доступные для изменения, представлены в таблице выше.

Используйте следующую команду для удаления статического маршрута:

```
Admin@nodename# delete network routes <route-name>
```

Пример удаления статического маршрута:

```
Admin@nodename# delete network routes test_route
```

Для отображения статических маршрутов:

```
Admin@nodename# show network routes
```

DNS-настройки

Настройка системных серверов DNS производится на уровне **network dns system-dns-servers**.

Для добавления новых DNS-серверов или обновления существующего списка используются следующие команды:

```
Admin@nodename# set network dns system-dns-servers ip [ <ip> <ip> ... ]
```

Для удаления всего списка адресов серверов DNS:

```
Admin@nodename# delete network dns system-dns-servers
```

Для удаления определённых серверов:

```
Admin@nodename# delete network dns system-dns-servers ip [ <ip>
<ip> ... ]
```

Для отображения списка системных DNS-серверов используется команда:

```
Admin@nodename# show network dns
```

НАСТРОЙКА БИБЛИОТЕК

Настройка библиотек (Описание)

Настройка IP-адресов

Данный раздел находится на уровне **libraries ip-list**.

Для создания группы IP-адресов используется следующая команда:

```
Admin@nodename# create libraries ip-list <parameter>
```

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название списка адресов.
description	Описание списка.
threat-lvl	Уровень угрозы: • **very-low** — очень низкий уровень угрозы. • **low** — низкий уровень угрозы. • **medium** — средний уровень угрозы. • **high** — высокий уровень угрозы. • **very-high** — высокий уровень угрозы.
type	Тип списка: • **local** — локальный. • **updatable** — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (**url**). Периодичность обновления списка указывается параметром **shedule** в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".
lists	Выбор существующих IP-листов для добавления в создаваемый лист.

Параметр	Описание
ips	IP-адреса или диапазон IP-адресов, которые необходимо включить в список. Указывается в формате: <ip>, <ip/mask> или <ip_range_start-ip_range_end>.

Для редактирования списка (список параметров, доступных для обновления, аналогичен списку параметров команды создания списка):

```
Admin@nodename# set libraries ip-list <ip-list-name> <parameter>
```

Чтобы добавить в список новые адреса:

```
Admin@nodename# set libraries ip-list <ip-list-name> [ <ip1>
<ip2> ... ]
```

Следующие команды используются для удаления всего списка адресов или IP-адресов, содержащихся в нём:

```
Admin@nodename# delete libraries ip-list <ip-list-name>
Admin@nodename# delete libraries ip-list <ip-list-name> ips [ <ip1>
<ip2>... ]
```

Команда отображения информации о всех имеющихся списках:

```
Admin@nodename# show libraries ip-list
```

Чтобы отобразить информацию об определённом списке, необходимо указать название интересующего списка IP-адресов:

```
Admin@nodename# show libraries ip-list <ip-list-name>
```

Также доступен просмотр содержимого списка IP-адресов:

```
Admin@nodename# show libraries ip-list <ip-list-name> items
```

Настройка почтовых адресов

Раздел находится на уровне **libraries email-list**.

Чтобы добавить новую группу почтовых адресов используется следующая команда:

```
Admin@nodename#& create libraries email-list <parameter>
```

Далее указываются параметры:

Параметр	Описание
name	Название группы почтовых адресов.
description	Описание группы почтовых адресов.
type	Тип списка: • **local** — локальный. • **updatable** — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (**url**). Периодичность обновления списка указывается параметром **shedule** в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".
emails	Почтовые адреса, которые необходимо добавить в данную группу.

Команда, предназначенная для редактирования информации о группе почтовых адресов:

```
Admin@nodename# set libraries email-list <email-list-name> <parameter>
```

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании группы почтовых адресов.

Для удаления группы или почтовых адресов из неё используются следующие команды:

```
Admin@nodename# delete libraries email-list <email-list-name>
Admin@nodename# delete libraries email-list <email-list-name> emails
[ <email> ... ]
```

Следующие команды используются для просмотра информации о всех созданных группах, об определённых группах или для просмотра почтовых адресов, входящих в группу:

```
Admin@nodename# show libraries email-list
Admin@nodename# show libraries email-list <email-list-name>
Admin@nodename# show libraries email-list <email-list-name> emails
```

Настройка номеров телефонов

Настройка раздела **Номера телефонов** производится на уровне **libraries phone-list**.

Для создания группы телефонных номеров:

```
Admin@nodename# create libraries phone-list <parameter>
```

Далее необходимо указать следующие данные:

Параметр	Описание
name	Название группы телефонных номеров.

Параметр	Описание
description	Описание группы телефонных номеров.
type	Тип списка: • **local** — локальный. • **updatable** — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (**url**). Периодичность обновления списка указывается параметром **shedule** в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".
phones	Номера телефонов, которые необходимо добавить в данную группу.

Для редактирования информации о группе телефонных номеров используется команда:

```
Admin@nodename# set libraries phone-list <phone-list-name> <parameter>
```

Параметры, доступные для обновления, представлены в таблице выше.

Для удаления группы или номеров телефонов из неё используются следующие команды:

```
Admin@nodename# delete libraries phone-list <phone-list-name>
Admin@nodename# delete libraries phone-list <phone-list-name> phones
[ <phone> ... ]
```

Следующие команды используются для просмотра информации о всех созданных группах:

```
Admin@nodename# show libraries phone-list
```

или об определённых группах телефонных номеров:

```
Admin@nodename# show libraries phone-list <phone-list-name>
```

Для просмотра номеров, содержащихся в группе, используется команда:

```
Admin@nodename# show libraries phone-list <phone-list-name> phones
```

Настройка команд

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

Для создания списка команд используется команда:

```
Admin@nodename# create libraries commands-list name <command-list-name>
type <local | updatable> commands new <command-string>
```

Для редактирования созданного ранее списка команд используется команда:

```
Admin@nodename# set libraries commands-list <command-list-name>
commands <command-string>
```

Для просмотра созданного ранее списка команд используется команда:

```
Admin@nodename# show libraries commands-list <command-list-name>
```

Для удаления созданного ранее списка команд или отдельных команд из списка используется команда:

```
Admin@nodename# delete libraries commands-list <command-list-name>
```

```
Admin@nodename# delete libraries commands-list <command-list-name>
commands <command-string>
```

Настройка профилей оповещений

Профили оповещений SMTP (по email) и SMPP (по SMS) настраиваются на уровне **libraries notification-profiles**.

Для добавления нового профиля оповещения SMTP:

```
Admin@nodename# create libraries notification-profiles smtp <parameter>
```

Далее необходимо указать:

Параметр	Описание
name	Название профиля.
description	Описание профиля.
host	IP-адрес или FQDN сервера SMTP, который будет использоваться для отсылки почтовых сообщений.
port	Порт TCP, используемый сервером SMTP. Обычно для протокола SMTP используется порт 25, для SMTP с использованием SSL — 465. Уточните данное значение у администратора почтового сервера.
connection-security	Варианты безопасности отправки почты; возможны варианты: • **none**. • **starttls**. • **ssl**.
authentication	Включение/отключение авторизации при подключении к серверу SMTP: • **on**. • **off**.

Параметр	Описание
login	Имя учётной записи для подключения к SMTP-серверу.
password	Пароль учётной записи для подключения к SMTP-серверу.

Для создания профиля оповещения по SMS (SMPP):

```
Admin@nodename# create libraries notification-profiles smpp <parameter>
```

Далее необходимо указать значения следующих параметров:

Параметр	Описание
name	Название профиля.
description	Описание профиля.
host	IP-адрес или FQDN сервера SMPP, который будет использоваться для отсылки SMS.
port	Порт TCP, который используется для подключения к серверу SMPP. Обычно для протокола SMPP используется порт 2775; при использовании SSL — 3550.
ssl	Включение/отключение шифрования SSL: • **on**. • **off**.
login	Имя учётной записи для подключения к SMPP-серверу.
password	Пароль учётной записи для подключения к SMPP-серверу.
phone-translation-rules	Правила трансляции телефонных номеров. Правила используются для соответствия требованиям провайдера. Например, если необходимо заменить все номера, начинающиеся на +7, на 8: `Admin@nodename# set libraries notification-profiles smpp <profile-name> phone-translation-rules + [ +7¦8 ]`
source-ton	

Параметр	Описание
	Тип номера (Type of Number) для источника сообщения: • **0** — Unknown (Неизвестный). • **1** — International (Международный). • **2** — National (Государственный). • **3** — Network Specific (Сетевой Специальный). • **4** — Subscriber Number (Номер абонента). • **5** — Alphanumeric (Алфавитно-цифровой). • **6** — Abbreviated (Сокращённый).
dest-ton	Тип номера (Type of Number) для адресата: • **0** — Unknown (Неизвестный). • **1** — International (Международный). • **2** — National (Государственный). • **3** — Network Specific (Сетевой Специальный). • **4** — Subscriber Number (Номер абонента). • **5** — Alphanumeric (Алфавитно-цифровой). • **6** — Abbreviated (Сокращённый).
source-npi	Индикатор схемы присвоения номеров (Numbering Plan Indicator) для источника: • **0** — Unknown. • **1** — ISDN/telephone numbering plan (E.163/E.164). • **3** — Data numbering plan (X.121). • **4** — Telex numbering plan (F.69). • **6** — Land Mobile (E.212). • **8** — National numbering plan. • **9** — Private numbering plan. • **10** — ERMES numbering plan (ETSI DE/PS 3 01-3). • **13** — Internet (IP). • **18** — WAP Client Id (to be defined by WAP Forum).
dest-npi	Индикатор схемы присвоения номеров (Numbering Plan Indicator) для адресата: • **0** — Unknown. • **1** — ISDN/telephone numbering plan (E.163/E.164). • **3** — Data numbering plan (X.121). • **4** — Telex numbering plan (F.69).

Параметр	Описание
	• **6** — Land Mobile (E.212). • **8** — National numbering plan. • **9** — Private numbering plan. • **10** — ERMES numbering plan (ETSI DE/PS 3 01-3). • **13** — Internet (IP). • **18** — WAP Client Id (to be defined by WAP Forum).

Для редактирования профиля оповещения используется команда:

```
Admin@nodename# set libraries notification-profiles <smtp | smpp>
<profile-name> <parameter>
```

Параметры профилей SMTP и SMPP, доступные для изменения, представлены в соответствующих таблицах выше.

Для удаления профиля:

```
Admin@nodename# delete libraries notification-profiles <smtp | smpp>
<profile-name>
```

Также для профилей оповещений SMPP доступно удаления правил трансляции номеров:

```
Admin@nodename# delete libraries notification-profiles smpp <profile-
name> phone-translation-rules [ phone1¦phone2 ]
```

Следующие команды предназначены для отображения информации о всех имеющихся профилях оповещений:

```
Admin@nodename# show libraries notification-profiles
```

о всех профилях одного типа:

```
Admin@nodename# show libraries notification-profiles <smtp | smpp>
```

об определённом профиле оповещения:

```
Admin@nodename#show libraries notification-profiles <smtp | smpp>
<profile-name>
```

Настройка категорий срабатывания

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

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

Для создания категорий срабатывания используется команда:

```
Admin@nodename# create libraries alert-categories name <category-name>
key <category-key>
```

Для редактирования категорий срабатывания используется команда:

```
Admin@nodename# set libraries alert-categories name <category-name> key
<category-key>
```

Для просмотра созданных ранее категорий срабатывания используется команда:

```
Admin@nodename# show libraries alert-categories name <category-name>
```

Для удаления созданных ранее категорий срабатывания используется команда:

```
Admin@nodename# delete libraries alert-categories name <category-name>
```

Настройка внешних сервисов обогащений

В данном элементе библиотеки представлены ресурсы, с помощью которых происходит дополнительный сбор информации об угрозах. С данных источников приходят фиды — структурированные проанализированные данные об IP-адресах и доменах, с которых происходит распространение вредоносных файлов, их сэмплы и хэши; списки фишинговых сайтов, почтовые адреса отправителей фишинговых писем; адреса, с которых происходит сканирование сетей с целью обнаружения уязвимостей; IP-адреса, с которых проводятся атаки типа брутфорс; сигнатуры для обнаружения вредоносного программного обеспечения. Подробнее о доступных сервисах читайте в разделе Внешние сервисы обогащений Руководства администратора SIEM.

Чтобы использовать сервисы обогащения их необходимо включить. Для использования некоторых сервисов обогащения необходимо прохождение регистрации и предоставление ключа доступа.

Для редактирования сервисов обогащений используется команда:

```
Admin@nodename# set libraries enrichment-services <service-name>
```

Для просмотра сервисов обогащений используется команда:

```
Admin@nodename# show libraries enrichment-services <service-name>
```

Настройка syslog-фильтров

Создание и настройка syslog-фильтров производятся на уровне **libraries syslog-filters**.

Команда для создания syslog-фильтра:

```
Admin@nodename# create libraries syslog-filters <parameter>
```

Далее представлены параметры, которые необходимо указать:

Параметр	Описание
name	Название фильтра.
description	Описание фильтра.
login-address	Строка для поиска IP-адреса пользователя в syslog-сообщении.
login-event	Строка для поиска события входа пользователя в syslog-сообщении.
login-username	Строка для поиска имени пользователя в syslog-сообщении.
logout-address	Строка для поиска IP-адреса пользователя в syslog-сообщении.
logout-event	Строка для поиска события выхода пользователя в syslog-сообщении.
logout-username	Строка для поиска имени пользователя в syslog-сообщении.

Следующая команда предназначена для редактирования информации о syslog-фильтре:

```
Admin@nodename# set libraries syslog-filters <filter-name> <parameter>
```

Параметры, доступные для обновления, аналогичны параметрам, указываемым при создании фильтра.

Чтобы отобразить информацию о syslog-фильтрах:

```
Admin@nodename# show libraries syslog-filters <filter-name>
```

Пользователь может удалить syslog-фильтр, используя следующую команду:

```
Admin@nodename# delete libraries syslog-filters <filter-name>
```

Настройка приложений syslog

Создание и настройка приложений syslog производятся на уровне **libraries syslog-application**.

Команда для создания приложений syslog:

```
Admin@nodename# create libraries syslog-application <parameter>
```

Далее представлены параметры, которые необходимо указать:

Параметр	Описание
name	Название приложения.
description	Описание приложения.
app-name	Название приложения, отображаемое в журналах.

НАСТРОЙКА РАЗДЕЛА ПОЛЬЗОВАТЕЛИ И УСТРОЙСТВА

Настройка UserID агента

UserID агент предназначен для осуществления прозрачной аутентификации на выбранных устройствах UserGate. В качестве источника данных аутентификации используются журналы Microsoft Active Directory (посредством протокола WMI) и Syslog (посредством стандартизированного протокола syslog RFC 3164, RFC 5424, RFC 6587). Подробнее о схеме работы UserID агента читайте в разделе Пользователи и устройства Руководства администратора LogAn.

Настройка UserID в CLI производится на уровне **users userid-agent**.

Настройка параметров UserID агента

Общие параметры UserID агента настраиваются с помощью команды:

```
Admin@nodename# set users userid-agent configurate-agent <parameters>
```

При настройке необходимо установить следующие параметры:

Параметр	Описание
polling-interval	Период опроса серверов Active Directory. Значение по умолчанию – 120 секунд.
expiration-time	Период времени, по истечении которого сессия пользователя будет завершена принудительно. Значение по умолчанию – 2700 секунд (45 минут).
syslog-monitoring-interval	Период опроса базы данных для поиска событий начала/завершения сеанса пользователей syslog-источников.
ignore-network-list	Списки IP-адресов, события от которых будут проигнорированы агентом UserID. Запись об игнорировании источника появится в журнале **Агент UserID**. Список может быть создан в разделе библиотек **(IP-адреса)**. Данная настройка является глобальной и относится ко всем источникам.
ignore-user-list	Имена пользователей, события от которых будут проигнорированы агентом UserID. Поиск производится по Common Name (CN) пользователя AD. Данная настройка является глобальной и относится ко всем источникам. Запись об игнорировании пользователя появится в журнале UserID. **Важно!** При задании имени допустимо использовать символ астериск (*), но только в конце строки.

Настройка источника событий

Microsoft Active Directory

Для добавления Microsoft Active Directory в качестве источника событий предназначена следующая команда:

```
Admin@nodename# create users userid-agent active-directory <parameters>
```

При настройке необходимо указать следующие параметры:

Параметр	Описание
enabled	Включение/отключение получения журналов с источника.
name	Название источника.

Параметр	Описание
description	Описание источника (опционально).
address	Адрес Microsoft Active Directory.
protocol	Протокол доступа к AD (WMI).
login	Имя пользователя для подключения к AD.
password	Пароль пользователя для подключения к AD.
sharing-profile	Профиль редистрибуции, который описывает круг устройств UserGate на который будет отправлена информация о найденных пользователях. Подробнее смотрите раздел Профиль редистрибуции.

Syslog

Для добавления отправителя syslog в качестве источника событий предназначена следующая команда:

```
Admin@nodename# create users userid-agent syslog-sender <parameters>
```

При настройке необходимо указать следующие параметры:

Параметр	Описание
enabled	Включение/отключение получения журналов с источника.
name	Название источника.
description	Описание источника.
address	Адрес хоста, с которого UserGate будет получать события по протоколу syslog.
default-domain	Название домена, который используется для поиска найденных в журналах syslog пользователей.
timezone	Часовой пояс, установленный на источнике.
sharing-profile	Профиль редистрибуции который описывает круг устройств UserGate на который будет отправлена информация о найденных пользователях. Подробнее смотрите раздел Профиль редистрибуции.

Параметр	Описание
filters	Фильтры для поиска необходимых записей журнала. Фильтры создаются и настраиваются в разделе **Библиотеки → Syslog фильтры UserID агента.** Подробнее читайте в разделе Syslog фильтры UserID агента.
users-catalogs	Предназначена для выбора LDAP коннектора, который используется для поиска информации о пользователях, найденных в журналах агентом UserID. Можно выбрать настроенный ранее каталог или добавить новый.

Настройка профиля редистрибуции UserID

Профили редистрибуции UserID предназначены для определения круга устройств UserGate, на которые отправляется информация о найденных агентом UserID пользователях.

Настройка профилей редистрибуции UserID в CLI производится на уровне **users sharing-profile**.

Команда для настройки:

```
Admin@nodename# create users sharing-profile <parameters>
```

При настройке необходимо установить следующие параметры:

Параметр	Описание
name	Название профиля.
description	Описание профиля (опционально).
sensors	Выбор сенсоров UserGate, на которые будет отправлена информация о пользователях.

НАСТРОЙКА СЕНСОРОВ

Настройка сенсоров (описание)

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

Сенсоры UserGate

Сенсор UserGate подключает одно устройство типа межсетевого экрана UserGate к LogAn. Для подключения сенсора UserGate необходимо выполнить следующие шаги:

1. На **NGFW** разрешить сервисы **Log Analyzer** и **SNMP** в настройках требуемой зоны:

```
Admin@ngfw-nodename# set network zone <zone-name> enabled-services
[ SNMP "Log Analyzer" ]
```

2. На **NGFW** получить токен устройства:

```
Admin@ngfw-nodename# show settings general log-analyzer

state              : ready
logan-server       : 127.0.0.1
logan-version      : 7.1.0.
device-version     : 7.1.0.
device-code        : 9R4FCVET
```

3. На LogAn разрешить сервис **Log Analyze**r в свойствах требуемой зоны:

```
Admin@nodename# set network zone <zone-name> enabled-services [ "Log
Analyzer" ]
```

4. Создать сенсор UserGate.

Для создания сенсора UserGate используется команда:

```
Admin@ndefornaledo# create sensors ug-sensors <parameters>
```

Необходимо добавить следующие параметры:

Параметр	Описание
enabled	Включает или выключает данный сенсор UserGate.
name	Название сенсора UserGate.
description	Опциональное описание сенсора UserGate.
address	IP-адрес узла UserGate, для которого создается данный сенсор.
logan-address	IP-адрес сервера LogAn, который будет использоваться на узле UserGate, в качестве назначения для отсылки журналов. Для выбора отображаются только те адреса, на интерфейсах зон которых разрешен сервис Log Analyzer.
device-code	Токен, полученный на узле UserGate.

После создания сенсора, узел UserGate начинает отсылать данные на LogAn.

Для просмотра сенсоров UserGate используется команда:

```
Admin@nodename# show sensors ug-sensors
```

Сенсоры SNMP

С помощью сенсора SNMP администратор может подключить SNMP-совместимое сетевое устройство к серверу LogAn для сбора и анализа его метрик. LogAn может отображать любые счетчики, полученные по SNMP с помощью запросов SNMP. Для настройки сенсора SNMP необходимо иметь базы MIB (Management Information Base) на управляемое устройство.

Для настройки сенсора SNMP необходимо выполнить следующие шаги:

1. Загрузить базу MIB того устройства, которое требуется добавить для мониторинга.

2. Создать сенсор SNMP:

```
Admin@nodename# create sensors snmp-sensors <parameters>
```

Далее указать следующие параметры::

Наименование	Описание
enabled	Включает или выключает данный сенсор SNMP.
name	Название сенсора SNMP.
description	Опциональное описание сенсора SNMP.
ip	IP-адрес сенсора SNMP.
port	Порт сенсора SNMP. Обычно для запросов данных по протоколу SNMP используется порт TCP 161.
version	Указывает версию протокола SNMP, которая будет использоваться в данном сенсоре. Возможны варианты SNMP v2 (**2**) и SNMP v3 (**3**).
community	SNMP community - строка для идентификации сервера LogAn и сетевого устройства для версии SNMP v2. Используйте только латинские буквы и цифры.
interval	Интервал в секундах, через который сервер LogAn будет инициировать получение данных с сетевого устройства.
username	Только для SNMP v3. Имя пользователя для аутентификации сетевом устройстве.
auth-type	Выбор режима аутентификации. Возможны варианты: • Без аутентификации, без шифрования (**none**). • С аутентификацией, без шифрования (**no-encrypt**). • С аутентификацией, с шифрованием (**encrypt**).
auth-alg	Алгоритм, используемый для аутентификации: • **md5**; • **sha**; • **sha224**; • **sha256**; • **sha284**; • **sha512**.

Наименование	Описание
auth-password	Пароль, используемый для аутентификации.
encrypt-alg	Алгоритм, используемый для шифрования. Возможно использовать DES и AES.
encrypt-password	Пароль, используемый для шифрования.
counters	Укажите здесь все требуемые данные, которые LogAn будет запрашивать на сетевом устройстве. Счетчики выбираются из баз MIB, которые загружены на устройство. Укажите в собках [ ] SNMP OID счетчика.

Для просмотра сенсоров SNMP используется команда:

```
Admin@nodename# show sensors snmp-sensors
```

Сенсоры WMI

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

Для создания сенсора WMI используется команда:

```
Admin@nodename# create sensors wmi-sensors <parameters>
```

Далее указать следующие параметры::

Наименование	Описание
enabled	Включает или выключает данный сенсор.
name	Название сенсора.
description	Опциональное описание сенсора.
ip	IP-адрес сенсора.
login	Имя пользователя для подключения к устройству.
password	Пароль пользователя для подключения к устройству.

Наименование	Описание
namespace	Пространство имен идентификаторов.
polling-interval	Интервал опроса в секундах.
counters	Указать данные, которые LogAn будет мониторить на сетевом устройстве: • **name** — название счетчика. • **type** — тип счетчика (windows-event-logs). • **filter-query** — WQL запрос (например, Logfile='Security').

Для просмотра сенсоров WMI используется команда:

```
Admin@nodename# show sensors wmi-sensors
```

Конечные устройства

Конечное устройство с установленным программным обеспечением UserGate Client будет отображено при выборе на UGMC данного устройства LogAn в качестве сервера для передачи информации о событиях, при этом LogAn должен быть предварительно зарегистрирован на UGMC (подробнее читайте в разделе Управление устройствами LogAn).

Для просмотра данных конечных устройств используется команда:

```
Admin@nodename# show sensors endpoint-devices
```

Коннекторы

Коннекторы используются для возможности подключения устройства SIEM к различным средствам защиты с целью сбора информации.

Для добавления коннектора предназначена команда:

```
Admin@nodename# create sensors connectors <parameters>
```

Необходимо указать следующие данные:

Параметр	Описание
name	Название коннектора.
description	Описание коннектора (опционально).
server-type	Выбор типа сервера: • **SSH**. • **HTTP**. • **HTTPS** (в текущей версии реализован только для интеграции с ГосСОПКА).
address-format	Тип: • **ip**. • **fqdn**.
ip	IP-адрес сервера; указывается в случае выбора адреса сервера типа **IP**.
port	Порт сервера; указывается в случае выбора адреса сервера типа **IP**.
fqdn	FQDN сервера; указывается в случае выбора адреса сервера типа **FQDN**.
url-path	Используется при управлении устройством по API.
login	Логин пользователя для авторизации на коннекторе.
password	Пароль учётной записи пользователя, необходимый для авторизации на коннекторе.
connamd-group	Указание группы команд доступно только для SSH-сервера, подробнее читайте в разделе Команды.
headers	Указание заголовков доступно только для серверов HTTP и HTTPS.

Для редактирования созданного ранее коннектора используется команда:

```
Admin@nodename# create sensors connectors <connector-name> <parameters>
```

Для просмотра параметров созданных ранее коннекторов используется команда:

```
Admin@nodename# show sensors connectors <connector-name>
```

Для удаления созданных ранее коннекторов используется команда:

```
Admin@nodename# delete sensors connectors <connector-name>
```

НАСТРОЙКА МОНИТОРИНГА

Настройка параметров мониторинга устройства

Настройка параметров мониторинга устройства в интерфейсе CLI производится в режиме конфигурации на уровне **monitoring**. Команды этого уровня позволяют управлять настройкой параметров SNMP устройства, правил мониторинга по SNMP, профилей безопасности для аутентификации SNMP-менеджеров, правилами оповещений. Подробнее о правилах мониторинга и оповещений читайте в разделе Оповещения.

Настройка параметров SNMP устройства

Для настройки параметров SNMP устройства используются команды на уровне **monitoring smnp-parameter**:

```
Admin@nodename# edit monitoring snmp-parameter <parameters>
```

Для редактирования доступны следующие параметры:

Параметр	Описание
agent-name	Название системы, используемое подсистемой управления SNMP.
location	Информация о физическом расположении SNMP-агента.

Параметр	Описание
description	Описание системы.
Engine ID	Каждое устройство UserGate имеет уникальный идентификатор SNMPv3 Engine ID. По умолчанию Engine ID генерируется на основании имени узла UserGate. При редактировании Engine ID необходимо указать длину (**length**), тип и значение идентификатора. Длина может быть определена как фиксированная (не более 8 байт) или динамическая (не более 27 байт). Фиксированная длина идентификатора применима только для типа **text**. Engine ID может быть сформирован в формате: • **ip4** — IPv4. • **ipv6** — IPv6. • **mac** — MAC-адрес. • **text** — Текст. • **octets** — Октеты.

Подробнее о параметрах SNMP устройства UserGate читайте в разделе SNMP.

Настройка правил мониторинга по SNMP

Для настройки правил мониторинга устройства по SNMP используются команды на уровне **monitoring smnp**:

```
Admin@nodename# edit monitoring snmp <parameters>
```

Для редактирования доступны следующие параметры:

Параметр	Описание
name	Название правила.
enabled	Включение/отключение правила
community	SNMP community — строка для идентификации устройства UserGate и сервера управления SNMP для версии SNMP v2c. Используйте только латинские буквы и цифры.
context	Необязательный параметр, определяющий SNMP context. Можно использовать только латинские буквы и цифры.

Параметр	Описание
	На некоторых устройствах может быть несколько копий полного поддерева MIB. Например, на устройстве может быть создано несколько виртуальных маршрутизаторов. Каждый такой виртуальный маршрутизатор будет иметь полное поддерево MIB. В этом случае каждый виртуальный маршрутизатор может быть указан как контекст на сервере SNMP. Контекст определяется по имени. Когда клиент отправляет запрос, он может указать имя контекста. Если имя контекста не указано, будет запрошен контекст по умолчанию.
version	Указывает версию протокола SNMP, которая будет использоваться в данном правиле. Возможны варианты SNMP v2c и SNMP v3.
query	При включении разрешает получение и обработку SNMP-запросов от SNMP-менеджера.
trap	При включении разрешает отправку SNMP-трапов на сервер, настроенный для приема оповещений.
trap-host	IP-адрес сервера для трапов. Данная настройка необходима только в случае, если необходимо отправлять трапы на сервер оповещений.
trap-port	Порт, на котором сервер слушает оповещения. Обычно это порт UDP 162. Данная настройка необходима только в случае, если необходимо отправлять трапы на сервер оповещений.
security-profile	Только для SNMP v3. Подробнее — в разделе Профили безопасности SNMP.
events	Выбор типов параметров, доступных для мониторинга по правилу.

Для работы SNMP-менеджера с устройством UserGate необходимо в свойствах зоны интерфейса, к которому будет осуществляться подключение по протоколу SNMP, разрешить сервис **SNMP** в настройках контроля доступа. Подробнее о настройке зон в CLI читайте в разделе Настройки сети.

Настройка профилей безопасности SNMP

Для настройки профилей безопасности ля аутентификации SNMP-менеджеров используются команды на уровне **monitoring smnp-security-profile**:

```
Admin@nodename# edit monitoring snmp-security-profile <parameters>
```

Для редактирования доступны следующие параметры:

Параметр	Описание
name	Название профиля безопасности SNMP
description	Описание профиля безопасности SNMP
username	Имя пользователя для аутентификации SNMP-менеджера.
auth-type	Выбор режима аутентификации SNMP-менеджера. Возможны варианты: • **none** — без аутентификации, без шифрования. • **no-encrypt** — с аутентификацией, без шифрования. • **encrypt** — с аутентификацией, с шифрованием. Наиболее безопасным считается режим работы authPriv.
auth-alg	Алгоритм, используемый для аутентификации. Возможно использовать: • **sha**; • **md5**; • **sha224**; • **sha256**; • **sha384**; • **sha512**.
auth-password	Пароль, используемый для аутентификации.
encrypt-alg	Алгоритм, используемый для шифрования. Возможно использовать DES и AES.
encrypt-password	Пароль, используемый для шифрования.

Настройка правил оповещений

Для настройки правил оповещений используются команды на уровне **monitoring alert-rules**:

```
Admin@nodename# edit monitoring alert-rules <parameters>
```

Для редактирования доступны следующие параметры:

Параметр	Описание
enabled	Включает/отключает данное правило.
name	Название правила.
description	Описание правила.
notification-profile	Созданный ранее профиль оповещения.
sender	От кого будет приходить оповещение.
subject	Тема оповещения.
timeout	Тайм-аут, в течение которого сервер не будет отправлять сообщение при повторном срабатывании данного правила. Данная настройка позволяет предотвратить шторм сообщений при частом срабатывании правила оповещения.
events	События, для которых необходимо получать оповещения.
phones	Для SMPP-профиля. Группы номеров телефонов, куда отправлять SMS-оповещения.
emails	Для SMTP-профиля. Группы адресов email, на которые будут отправляться почтовые оповещения.

НАСТРОЙКА ИНЦИДЕНТОВ

Настройка инцидентов (описание)

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

Подробнее о функциональности системы IRP читайте в разделе Инциденты в Руководстве пользователя SIEM.

Настройки инцидентов в интерфейсе CLI производятся на уровне **incident**.

Для создания собственной схемы расследования инцидентов необходимо:

1. Создать необходимые решения инцидентов.
2. Создать типы инцидентов.
3. Создать состояния инцидентов.
4. Создать схему инцидентов.
5. Активировать схему инцидентов.

Для создания решения инцидентов используется команда:

```
Admin@nodename# create incident resolutions name <incident-name>
description <incident-description>
```

Для создания типов инцидентов используется команда:

```
Admin@nodename# create incident types name <incident-type-name>
description <incident-type-description>
```

Для создания состояния инцидентов используется команда:

```
Admin@nodename# create incident states name <incident-state-name>
description <incident-state-description> group <open|closed|progress>
```

Для создания схемы инцидентов используется команда:

```
Admin@nodename# create incident schema <parameters>
```

Для редактирования доступны следующие параметры схемы инцидентов:

Параметр	Описание
name	Название схемы.
description	Описание схемы

Параметр	Описание
prefix	Префикс, который будет использован при назначении идентификаторов создаваемым инцидентам. Идентификатор будет иметь вид: префикс — порядковый номер, например INC-99.
initial-state	Начальное состояние, которое принимает инцидент при его создании.
workflow-states	Состояния рабочего процесса — описывает все состояния, которые может принимать инцидент в своем жизненном цикле.
incidents-resolutions	Решения инцидентов — указывает список возможных решений инцидентов.
incidents-types	Типы инцидентов, которые могут быть использованы в этой схеме.
transition	Все возможные переходы между состояниями.

Для всех этапов создания схемы инцидентов также доступны команды **set** (редактирование), **show** (просмотр) и **delete** (удаление).

НАСТРОЙКА АНАЛИТИКИ

Настройка аналитики (описание)

UserGate SIEM позволяет проводить анализ журналов событий безопасности, получаемых с настроенных сенсоров. Все данные хранятся в одной базе данных, что даёт возможность осуществлять сложный поиск, корреляцию повторяющихся событий, их агрегацию, создавая инциденты безопасности, и упростить процесс изучения особенностей инцидентов. Подробнее об архитектуре и принципах работы функциональности SIEM читайте в разделе Аналитика Руководства администратора SIEM.

В интерфейсе CLI возможно создавать и настраивать правила аналитики и действия реагирования. С помощью правил аналитики инженер безопасности может автоматизировать процесс корреляции событий и создание срабатываний, а также назначить определенные действия реагирования (реакцию) системы на создаваемые срабатывания. Все это

позволяет облегчить процесс изучения регистрируемых событий и сократить время между обнаружением проблемы и ее решением.

Правила аналитики и действия реагирования в CLI создаются и настраиваются на уровне **analytics**.

Правила аналитики

С помощью правил аналитики происходит обработка событий журналов. Настройка правил аналитики позволяет производить сложный поиск среди событий информационной безопасности. Срабатывание правила происходит при выявлении корреляции событий с разных источников.

Для создания правила аналитики предназначена команда:

```
Admin@nodename# create analytics analytics-rules <parameters>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
enabled	**on**/**off** — Включение/отключение правила аналитики для работы в режиме реального времени.
name	Название правила аналитики.
description	Описание правила аналитики.
threat-level	Уровень угрозы, который будет отображаться при срабатывании правила. • **informational**: события, сформировавшие срабатывание правила аналитики, представляют очень низкий уровень угрозы, и администратор может не предпринимать никаких действий. • **low**: события, сформировавшие срабатывание правила аналитики, представляют низкий уровень угрозы, и администратор может не предпринимать никаких действий. • **medium**: необходимо обратить внимание на события, попавшие под срабатывание правила аналитики. • **high**: события, требующие исследования и принятия мер. • **critical**: события, требующие исследования и срочного принятия мер.

Параметр	Описание
priority	Показывает приоритет, установленный для срабатывания правила аналитики: • **low**: срабатывания данных правил обладают низким приоритетом реагирования. • **normal**: на срабатывания данных правил необходимо обратить внимание и, возможно, предпринять меры. • **important**: на срабатывания данных правил необходимо обратить внимание и предпринять меры. • **critical**: срабатывания данных правил требуют незамедлительного реагирования. При срабатывании правила установленный приоритет будет указывать на важность срабатывания правила аналитики.
alert-category	Отображает категорию, к которой относится срабатывание. По умолчанию для выбора доступны следующие категории: • **security**: правила данной категории определяют инциденты, приводящие к ухудшению безопасности информационных систем. • **availability**: правила данной категории определяют инциденты, которые приводят к ухудшению доступности информационных систем. • **performance**: правила данной категории определяют инциденты, которые приводят к ухудшению производительности информационных систем. Дополнительные категории срабатываний могут быть созданы в библиотеке **Категории срабатывания**. Подробнее читайте в разделе Настройка категорий срабатывания.
timezone	Указывает на часовой пояс, по времени которого будут работать правила аналитики, т.к. сервер может собирать данные с источников, находящихся в различных часовых поясах.
response-actions	Выбор действий реагирования, которые будут выполнены автоматически при срабатывании правила аналитики. Подробнее о создании действий реагирования и их настройке читайте в разделе Действия реагирования.
conditions	Указание условий срабатывания правила.

Условия срабатывания, которые указываются при создании правила аналитики, имеют следующие параметры настройки:

Параметр	Описание
name	Название условия правила аналитики.
description	Описание условия правила аналитики.
condition-time-enabled	Включить/отключить ограничение времени выполнения условия. При включении ограничения времени правило аналитики сработает, только в том случае, когда за указанный отрезок времени условие выполнится заданное количество раз.
condition-time	Указывает на отрезок времени, за который условие должно выполнится заданное количество раз, чтобы произошло срабатывание правила аналитики. Время указывается в секундах. Указание времени выполнения условия доступно при активированном параметре **condition-time-enabled**.
break-query-enabled	Включить/отключить использование запроса остановки в правиле аналитики.
break-query	SQL-подобный поисковый запрос остановки выполняется вместе с запросом условия. Для формирования запроса используются названия полей, значения полей, ключевые слова и операторы (задаётся аналогично запросу фильтра). Если при выполнении анализа найдётся хотя бы одна запись, соответствующая заданному запросу остановки, до того, как будет найдено заданное количество событий, соответствующих условию правила аналитики, то правило аналитики не сработает, а счётчик количества записей, найденных до выполнения запроса остановки, будет обнулён.
filter-query	Отображает SQL-подобный поисковый запрос условия, который пишется по базе журналов. Для формирования запроса используются названия полей, значения полей, ключевые слова и операторы. Синтаксис написания запроса можно просмотреть в разделе Поиск и фильтрация данных. Запрос также может быть написан с использованием синтаксиса Google/RE2 в операторе MATCH. Подробнее о синтаксисе Google/RE2 в операторе MATCH: https://github.com/google/re2/wiki/Syntax.
group-by	Отображает список параметров, по которым могут быть сгруппированы правила в результате срабатывания. Поля будут отображены при просмотре карточки срабатывания.

Параметр	Описание
	О параметрах, по которым возможна группировка, читайте в разделе Поиск. При указании категорий для группировки правило аналитики сработает только в том случае, если условие выполнится именно для выбранной категории заданное количество раз, указанное в поле параметра **pattern-repeats**.
pattern-repeats	Показывает количество выполнений условия, необходимое для срабатывания правила. Данный параметр может быть использован вместе с параметром **condition-time-enabled** и ли без него.

Для правил аналитики также доступны команды **set** (редактирование), **show** (просмотр) и **delete** (удаление).

Действия реагирования

Действия реагирования позволяют определить методы реагирования при срабатывании правил аналитики информационной безопасности. UserGate SIEM позволяет гибко настраивать правила, используя переменные, относящиеся к категориям срабатывания правил аналитики.

Для создания действия реагирования предназначена команда:

```
Admin@nodename# create analytics response-actions <parameters>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
enabled	on/off — Включение/отключение правила реагирования.
name	Название правила реагирования.
description	Описание правила реагирования.
action	Показывает действие, выбранное для исполнения в случае срабатывания правила аналитики. Действие реагирования выполнится, если оно указано в свойствах правила аналитики. Для выбора доступны следующие виды реагирования: • **send-email**: отправка письма на выбранные почтовые адреса. Настройка действия **Отправить email** будет

Параметр	Описание
	рассмотрена далее в разделе Действие типа send-email. • **send-message**: отправка сообщения на указанные номера телефонов. Настройка действия **Отправить сообщение** будет рассмотрена далее в разделе Действие типа send-message. • **webhook**: получение уведомления о срабатывании правила на веб-странице, адрес которой был указан при настройке действия. Настройка действия **Webhook** будет рассмотрена далее в разделе Действие типа webhook. • **create-incident**: автоматическое создание инцидента в результате срабатывания правил аналитики. О настройке действия **Создать инцидент** читайте в разделе Настройки инцидентов. • **send-command-to-connector**: отправка команды на выбранный коннектор. Настройка действия Послать команду на коннектор будет рассмотрена далее в разделе Действие типа послать send-command-to-connector. • **send-command-to-endpoint**: отправка команды на конечное устройство с установленным ПО UserGate Client. Подробнее читайте в раздел Действие типа send-command-to-endpoint.
enable-logging	Включает/отключает журналирование данных о срабатывании действия реагирования. Данные записываются в журнал событий SIEM.
grouping	Для удобства при настройке действий реагирования возможно использование функции группировки срабатываний. Группировка возможна по следующим параметрам: • **never** — никогда. • **period** — при настройке группировки срабатываний правила аналитики за период времени действие реагирования выполнится, если в течение указанного времени произошло хотя бы одно срабатывание. • **number** — при настройке группировки по количеству срабатываний правила аналитики действие реагирования выполнится только после указанного количества срабатываний.
time-period	Отображает период группировки в минутах. Задание параметра возможно только при выборе группировки похожих срабатываний за период времени.

Параметр	Описание
alerts-number	Отображает заданное количество срабатываний. Задание параметра возможно только при выборе группировки похожих срабатываний по их количеству.

Для действий реагирования также доступны команды **set** (редактирование), **show** (просмотр) и **delete** (удаление).

Действие типа send-email

Если в качестве действия реагирования была выбрана отправка email, то в свойствах правила реагирования необходимо указать следующие параметры.

Наименование	Описание
notification-profile	Профиль оповещения SMTP, который будет использован для отправки email. Подробнее о настройке профилей SMTP читайте в главе Настройка профилей оповещений.
sender	Имя отправителя письма.
subject	Тема письма.
emails	Список почтовых адресов получателей. Получатели должны быть добавлены в списки в библиотеке элементов. О добавлении почтовых адресов читайте в разделе Настройка почтовых адресов.
template	Шаблон письма уведомления с возможностью передачи значений различных переменных, относящихся к срабатыванию. Подробнее читайте в разделе Шаблон уведомлений и Переменные для уведомлений и команд.

Действие типа send-message

Если в качестве действия реагирования была выбрана отправка сообщения, то в свойствах правила реагирования необходимо указать следующие параметры.

Наименование	Описание
notification-profile	Профиль оповещения SMPP, который будет использован для отправки сообщения. Подробнее о настройке профилей SMPP читайте в главе Настройка профилей оповещений.

Наименование	Описание
sender	Имя отправителя письма.
phones	Список номеров телефонов получателей. Получатели должны быть добавлены в библиотеке элементов. О добавлении телефонных номеров читайте в разделе Настройка номеров телефонов.
template	Шаблон сообщения с возможностью передачи значений различных переменных, относящихся к срабатыванию. Подробнее читайте в разделе Шаблон уведомлений и Переменные для уведомлений и команд.

Действие типа webhook

Для настройки webhook в свойствах правила реагирования необходимо указать следующие параметры.

Наименование	Описание
url	Адрес веб-сайта, на котором будут отображаться оповещения о срабатывании правила.
template	Шаблон уведомления с возможностью передачи значений различных переменных, относящихся к срабатыванию. Подробнее читайте в разделе Шаблон уведомлений и Переменные для уведомлений и команд.

Для тестирования webhook можно воспользоваться сервисом https://webhook.site. Для этого необходимо перейти на сайт Webhook.site и скопировать сгенерированную ссылку. Далее её необходимо указать в свойствах правила реагирования в поле **url** параметра **action**.

Действие типа send-command-to-connector

В качестве одного из действий реагирования может быть настроена отправка команды на коннектор.

Если в качестве действия реагирования настроена передача команды для исполнения на коннекторе, то необходимо указать следующие параметры:

Наименование	Описание
connectors	Выбор устройств, на которые необходимо отправить команду в случае срабатывания правила аналитики.

Наименование	Описание
	Коннектор должен быть заранее добавлен и настроен. Подробнее читайте в разделе Коннекторы. **Важно!** Могут выбраны только коннекторы с одинаковой группой команд.
command	Определение команды, которая будет передана на коннектор для выполнения; представлены команды группы, указанной для выбранных коннекторов. В случае наличия в команде переменных, будут отображены дополнительные поля для указания их значений. Подробнее о командах читайте в разделе Настройка команд.

Действие типа send-command-to-endpoint

В качестве одного из действий реагирования может быть настроена отправка команды на конечное устройство с установленным ПО UserGate Client. Доступны следующие команды:

- **block** — блокировка доступа к сети Интернет.
- **kill** — завершение указанного в запросе фильтра процесса.

Шаблон уведомлений

В параметре **template** необходимо указать текст уведомления. Можно передавать не только фиксированный текст, но и данные, относящиеся к срабатыванию или его записям в журнале.

Чтобы передать данные, относящиеся к срабатыванию, необходимо в поле **template** ввести название одного из параметров, представленных в таблице. Например, если ввести **{ANALYTICS_RULE_NAME}**, то в тексте уведомления, настроенном как отправка email, SMS или webhook, будет отражено название правила аналитики, которое сработало. Если заполнить шаблон при настройке действия **create incident**, то текст будет отображён в описании инцидента.

ДАШБОРД

Дашборд (описание)

Данный раздел позволяет посмотреть текущее состояние сервера и серверов, которые подключены к нему для отправки логов, их загрузку, статус лицензии и так далее.

Отчеты предоставлены в виде виджетов, которые могут быть настроены администратором системы в соответствии с его требованиями. Виджеты можно добавлять, удалять, изменять расположение и размер на странице **Дашборд**. По умолчанию созданы страницы с виджетами Log Analyzer (отображение состояния сервера Log Analyzer), NOC (Network Operation Center) и SOC (Security Operation Center).

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

Наименование	Описание
Название	Название виджета, которое будет отображаться в Дашборд.
Описание	Опциональное описание виджета.
Количество записей	Максимальное количество записей для отображения.
Группировать по	Поле данных, по которому будут сгруппированы данные в виджете.
Диаграмма	Выбор типа представления данных. Доступны значения: • Число • Круговая диаграмма • Вертикальная гистограмма • Горизонтальная гистограмма • Таблица • График • Карта мира

Наименование	Описание
Запрос фильтра	SQL-подобная строка запроса, позволяющая ограничить объем информации, используемой при построении виджета. Для формирования запросов используются названия полей, значения полей, ключевые слова и операторы. Ключевые слова и операторы, а также примеры их использования можно посмотреть в разделе документации Поиск и фильтрация данных.
Сенсор	Сенсор, данные с которого используются для данного виджета.

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Техническая поддержка (описание)

Раздел технической поддержки на сайте компании https://www.usergate.com/ru/support содержит дополнительную информацию по настройке LogAn. Кроме этого, здесь же вы можете оставить заявку на решение вашей проблемы.

ADMIN

ADMIN (описание)

Данный раздел позволяет зарегистрированному администратору сменить свой пароль, изменить некоторые настройки профиля и выйти из системы.

Наименование	Описание
Сменить пароль	Для смены пароля необходимо указать свой текущий пароль и два раза указать новый пароль.
Предпочтения	• Количество элементов на странице — устанавливает количество строк, отображаемых в одном диалоговом окне, например, список правил межсетевого экрана. • Ночной режим — устанавливает черный цвет темы графического интерфейса UGOS.

Наименование	Описание
	• Популярные фильтры — изменение названия или удаление фильтров различных журналов, созданных данным пользователем.
Выход	Завершение сеанса работы в веб-консоли устройства.

ИЗБРАННЫЕ

Избранные (описание)

В веб-интерфейсе имеется возможность фильтрации отображаемых разделов путем их добавления в избранное и поиск разделов по их названию. Фильтрация позволяет скрыть неиспользуемые разделы. Отображение только избранных разделов не влияет на функциональность или конфигурацию устройств. Чтобы добавить раздел в избранные, необходимо отметить символ звездочки напротив названия раздела; для настройки отображения используйте переключатель **Только избранные**, расположенный в нижней части панели.

ПРИЛОЖЕНИЯ

Требования к сетевому окружению

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
Веб-консоль	TCP	8010	Входящий (к веб-консоли LogAn)	Доступ к веб-интерфейсу управления устройством .
CLI по SSH	TCP	2200	Входящий (к CLI по SSH)	Доступ к интерфейсу командной строки (CLI)

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
				UserGate по протоколу SSH.
XML-RPC	TCP	4041	Входящий (к UserGate по API)	Управление устройством UserGate по API.
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.

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
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 LogAn к UGMC)	Первоначальная установка связи и обмен ключами шифрования с сервером UGMC.
		2022	Исходящий (от LogAn к UGMC)	Построение SSH-туннеля для обмена данными с помощью полученных ключей.
Сервис LogAn	TCP	9713	Исходящий (от LogAn к NGFW)	Первоначальная установка связи и обмен ключами шифрования с сервером NGFW.
		2023	Исходящий (от LogAn к NGFW)	Построение SSH-туннеля для обмена данными с помощью полученных ключей.
	TCP			

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
		22699 (приём данных от NGFW 6.x.x), 22711 (приём данных от NGFW 7.x.x, использующих SSL)	Входящий (от NGFW к LogAn)	Сервис сбора журналов LogAn.
SNMP	UDP	161	Входящий (до LogAn)	Доступ к серверу UserGate по протоколу SNMP.
Сборщик логов	TCP/UDP	514	Входящий (до LogAn)	Сервис сбора информации с удалённых устройств по протоколу Syslog.
SMTP	TCP	25	Исходящий (до постового сервера)	Отправка уведомлений на электронную почту.
DHCP	UDP	67, 68	Исходящий (запрос на получение адреса от UserGate на сервер DHCP)	Сервис службы DHCP.
LDAP	TCP	389, 636	Исходящий (на LDAP-коннектор)	Выполнение запросов LDAP (389 - для LDAP и 636 - для LDAP over SSL).
RADIUS	UDP	1812	Исходящий (на сервер	Аутентификация

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
			аутентификации RADIUS)	пользователей по протоколу RADIUS.
TACACS+	TCP	49	Исходящий (на сервер аутентификации TACACS+)	Аутентификация пользователей по протоколу TACACS+.
FTP (экпорт журналов)	TCP	21	Исходящий (до сервера FTP)	Экспорт журналов на сервер FTP.
SSH (экпорт журналов)	TCP	22	Исходящий (до сервера SSH)	Экспорт журналов на сервер SSH.
Syslog (экпорт журналов)	TCP/UDP	514	Исходящий (до сервера Syslog)	Экспорт журналов на сервер Syslog.

ОПИСАНИЕ ФОРМАТОВ ЖУРНАЛОВ

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.	NGFW
	Device Version	Версия продукта.	7

Тип поля	Название поля	Описание	Пример значения
	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@erstheta tica
	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	Attributes

Тип поля	Название поля	Описание	Пример значения
		указания деталей события.	
	cs1	Детали события в формате JSON.	{"name":"MIME_BUILTIN_COMPOSITE", "module":"nlist_import"}

Формат журнала веб-доступа

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

Тип поля	Название поля	Описание	Пример значения
	act	Действие, принятое устройством в соответствии с настроенными политиками.	captive
	reason	Причина, по которой было создано событие, например, причина блокировки сайта.	{"id": 39,"name":"Social Networking","threat_level":3}
	proto	Используемый протокол 4-го уровня.	TCP.
	app	Протокол прикладного уровня и его версия.	HTTP/1.1
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	requestMethod	Метод, используемый для доступа к URL-адресу (POST, GET и т.п.).	GET

Тип поля	Название поля	Описание	Пример значения
	request	В случае HTTP-запроса поле содержит URL-адрес запрашиваемого ресурса с указанием используемого протокола.	http://www.secure.com
	requestContext	URL источника запроса (реферер HTTP).	https://www.google.com/
	requestClientApplication	Useragent пользовательского браузера.	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	40
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Default Allow

Тип поля	Название поля	Описание	Пример значения
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)
	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		URL Categories

Тип поля	Название поля	Описание	Пример значения
		Поле указывает на категорию запрашиваемого URL-адреса.	
	flexString2	Категория URL.	Computers & Technology
	cn1Label	Поле используется для указания количества переданных пакетов в направлении источник — назначение.	Packets sent
	cn1	Количество переданных пакетов в направлении источник — назначение.	3
	cn2Label	Поле используется для указания количества переданных пакетов в направлении назначение — источник.	Packets received
	cn2	Количество переданных пакетов в направлении назначение — источник.	1
	cn3Label	Поле указывает исходный ответ сервера.	Response
	cn3	Код ответа HTTP.	302

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

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

Формат журнала DNS

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	dns
	Name	Тип источника.	log
	Threat Level	Уровень угрозы категории URL.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	**rt**	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1701085036026
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorereaeda

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

Тип поля	Название поля	Описание	Пример значения
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535. Для DNS обычно используется порт 53.
	cs1Label	Поле используется для указания сработавшего правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Rule1
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted

Тип поля	Название поля	Описание	Пример значения
	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**:

Формат журнала трафика

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

Тип поля	Название поля	Описание	Пример значения
	proto	Используемый протокол 4-го уровня.	TCP или UDP
	app	Имя сработавшего приложения	my_app
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	smac	MAC-адрес источника.	00:50:56:80:28:08
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	dmac	MAC-адрес назначения.	00:50:56:80:7D:21
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении	40

Тип поля	Название поля	Описание	Пример значения
		назначение — источник.	
	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	Source Country

Тип поля	Название поля	Описание	Пример значения
		указания страны источника.	
	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

Тип поля	Название поля	Описание	Пример значения
	cn2Label	Поле используется для указания количества пакетов, переданных в направлении назначение — источник.	Packets received
	cn2	Количество пакетов, переданных в направлении назначение — источник.	1

Формат журнала трафика **CEF Compact**:

Формат журнала СОВ

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

Тип поля	Название поля	Описание	Пример значения
	proto	Используемый протокол 4-го уровня.	TCP или UDP
	app	Протокол прикладного уровня.	HTTP
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	40

Тип поля	Название поля	Описание	Пример значения
	msg	Уровень угрозы сигнатуры и её название.	[2] BlackSun
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	IDPS Rule Example
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country

Тип поля	Название поля	Описание	Пример значения
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)

Формат журнала СОВ **CEF Compact**:

Формат журнала АСУ ТП

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	scada
	Name	Тип источника.	log
	PDU Severity	Критичность АСУ ТП.	Может принимать значения: • 1 — очень низкий. • 2 — низкий. • 3 — средний. • 4 — высокий. • 5 — очень высокий.
CEF [расширение]	**rt**	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@erstheta tica
	act	Действие, принятое устройством в соответствии с	accept

Тип поля	Название поля	Описание	Пример значения
		настроенными политиками.	
	app	Протокол прикладного уровня.	Modbus
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Scada Rule Example
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	

Тип поля	Название поля	Описание	Пример значения
			RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)
	cs6Label	Поле указывает на информацию об устройстве.	PDU Details
	cs6	Информация об устройстве в формате JSON.	{"protocol":"modbus","pdu_severity":0,"pdu_func":"3","pdu_address":0,"mb_value":0,"mb_quantity":0,"mb_payload":"AAIAAA==","mb_message":"response","mb_addr":0}

Формат журнала инспектирования SSH

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

Тип поля	Название поля	Описание	Пример значения
	Device Version	Версия продукта.	7
	Source	Название журнала.	ssh
	Name	Тип источника.	log
	Threat Level	Уровень угрозы приложения.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	**rt**	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@erstheta tica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	app	Протокол прикладного уровня.	SSH или SFTP
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.10.10

Тип поля	Название поля	Описание	Пример значения
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	smac	MAC-адрес источника.	FA:16:3E:65:1C:B4
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	SSH inspection rule
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone

Тип поля	Название поля	Описание	Пример значения
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)
	cs6Label	Указание на команду, передаваемую по SSH.	Command
	cs6	Команда, передаваемая по SSH, в формате JSON.	whoami

Формат журнала инспектирования SSH **CEF Compact**:

Формат журнала защиты почтового трафика

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

Тип поля	Название поля	Описание	Пример значения
		Протокол прикладного уровня.	
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4-адрес источника.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	dst	IPv4-адрес назначения.	10.10.10.10
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	10
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	10
	cs1Label	Поле используется для указания названия правила.	Rule
	cs1	Название правила защиты почтового трафика.	Mail security rule

Тип поля	Название поля	Описание	Пример значения
	cs2Label	Поле используется для указания зоны источника.	Source Zone
	cs2	Зона источника.	Untrusted
	cs3Label	Поле используется для индикации страны источника трафика.	Source Country
	cs3	Страна источника трафика.	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для указания зоны назначения трафика.	Destination Zone
	cs4	Название зоны назначения трафика.	Untrusted
	cs5Label	Поле используется для индикации страны назначения трафика.	Destination Country
	cs5	Страна назначения.	RU (отображается двухбуквенный код страны)
	cs6Label	Поле используется для указания почтового адреса получателя.	To
	cs6	Email получателя.	receiver@example.com
	flexString1Label	Поле используется для указания	From

Тип поля	Название поля	Описание	Пример значения
		почтового адреса отправителя.	
	flexString1	Email отправителя.	sender@example.com
	cn1Label	Поле используется для указания количества переданных пакетов в направлении источник — назначение.	Packets sent
	cn1	Количество переданных пакетов в направлении источник — назначение.	3
	cn2Label	Поле используется для указания количества переданных пакетов в направлении назначение — источник.	Packets received
	cn2	Количество переданных пакетов в направлении назначение — источник.	1

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

Формат журнала событий конечных устройств

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	endpoint_log
	Name	Тип источника.	log
	Severity	Важность события.	Может принимать значения: • 1 — error; • 2 — warning; • 3 — info; • 4 — audit success; • 5 — audit failure.
CEF [расширение]	**rt**	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Идентификатор устройства, сгенерировавшего это событие.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	msg	Подробная информация о событии.	Состояние Windows Defender успешно изменено на SECURITY_PRODUCT_STATE_ON.
	suser	Имя пользователя.	Admin

Тип поля	Название поля	Описание	Пример значения
	cs1Label	Поле используется для указания идентификатора конечного устройства.	endpointId
	cs1	Идентификатор конечного устройства или сенсора.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	cs2Label	Поле используется для индикации имени конечного устройства или сенсора.	endpointName
	cs2	Имя конечного устройства или сенсора.	DESKTOP-0731NFQ
	cs3Label	Поле используется для указания на тип события.	logLevel
	cs3	Тип события.	Аудит успеха, Предупреждение, Сведения, Аудит отказа, Ошибка
	cs4Label	Поле используется для указания категории события.	logCategoryString
	cs4	Категория события.	Special Logon
	cs5Label	Поле используется для индикации типа журнала.	logFile
	cs5	Тип журнала, содержащего	Security (файл журнала

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

Тип поля	Название поля	Описание	Пример значения
		индикации строки вставки.	
	flexString1	Строка вставки – данные блока EventData события Windows.	Windows DefenderSECURITY_PRODUCT_STATE_ON

Формат журнала правил конечных устройств

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	endpoint_log
	Name	Тип источника.	log
	Threat Level	Уровень угрозы категории URL.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	**rt**	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Идентификатор устройства, сгенерировавшего это событие.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	act	Действие, принятое	accept

Тип поля	Название поля	Описание	Пример значения
		устройством в соответствии с настроенными политиками.	
	proto	Используемый протокол 4-го уровня.	TCP
	shost	Имя хоста.	www.google.com
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	filePath	Приложение, к которому было применено правило межсетевого экрана.	C:\\Program Files (x86)\\Microsoft\ \Edge\ \Application\ \msedge.exe
	cs1Label	Поле используется для указания идентификатора конечного устройства.	endpointId
	cs1	Идентификатор конечного устройства или сенсора.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	cs2Label	Поле используется для указания на имя NetBIOS	endpointName

Тип поля	Название поля	Описание	Пример значения
		конечного устройства.	
	cs2	Имя NetBIOS конечного устройства.	DESKTOP-0731NFQ
	cs3Label	Поле используется для указания правила, срабатывание которого создало запись в журнале.	Rule
	cs3	Название правила.	Test rule name
	flexString1Label	Поле указывает на тип контента.	Media type
	flexString1	Тип контента.	text/html
	flexString2Label	Поле указывает на категорию запрашиваемого URL-адреса.	Categories
	flexString2	Категория URL.	Computers & Technology

Формат журнала правил конечных устройств **CEF Format**:

Формат журнала приложений конечных устройств

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	endpoint_applications
	Name	Тип источника.	log
	Threat Level	Значение по умолчанию.	0
CEF [расширение]	**rt**	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Идентификатор устройства, сгенерировавшего это событие.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	act	Действие (запуск или остановка приложения).	start, stop
	suser	Пользователь.	DESKTOP-0731NFQ\User
	filePath	Расположение файла.	C:\\Windows\\system32\\cmd.exe
	spid	Идентификатор процесса.	3860

Тип поля	Название поля	Описание	Пример значения
	fileHash	Хэш приложения.	B4979A9F970029889713D756C3F123643DDE73DA
	cs1Label	Поле используется для указания идентификатора конечного устройства.	endpointId
	cs1	Идентификатор конечного устройства.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	cs2Label	Поле используется для указания на имя NetBIOS конечного устройства.	endpointName
	cs2	Имя NetBIOS конечного устройства.	DESKTOP-0731NFQ
	cs3Label	Поле используется для индикации командной строки.	cmdLine
	cs3	Запрос командной строки.	C:\\Windows\\system32\\sc.exe start w32time task_started
	cs4Label	Поле используется для указания идентификатора сессии.	sessionId
	cs4	Идентификатор сессии.	1656395717

Формат журнала аппаратуры конечных устройств

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	endpoint_hardware
	Name	Тип источника.	log
	Threat Level	Значение по умолчанию.	0
CEF [расширение]	**rt**	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Идентификатор устройства, сгенерировавшего это событие.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	act	Действие (подключение или извлечение устройства).	add_device, remove_device
	sourceServiceName	Драйвер Windows, обеспечивающий взаимодействие компьютера с оборудованием/устройством.	USBHUB3
	cs1Label	Поле используется для указания идентификатора конечного устройства.	endpointId

Тип поля	Название поля	Описание	Пример значения
	cs1	Идентификатор конечного устройства.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	cs2Label	Поле используется для указания на имя NetBIOS конечного устройства.	endpointName
	cs2	Имя NetBIOS конечного устройства.	DESKTOP-0731NFQ
	cs3Label	Поле используется для указания идентификатора подключаемого/извлекаемого устройства.	deviceId
	cs3	Идентификатор устройства.	USB\\VID_0E0F&PID_0002\\6&201153C1&0&8
	cs4Label	Поле используется для индикации имени устройства.	deviceName
	cs4	Название устройства.	Kingston DataTraveler 2.0 USB Device

Формат журнала 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.	NGFW

Тип поля	Название поля	Описание	Пример значения
	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).
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: %

Тип поля	Название поля	Описание	Пример значения
			{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

Тип поля	Название поля	Описание	Пример значения
			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	endpointId

Тип поля	Название поля	Описание	Пример значения
		— источника события.	
	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
	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

Тип поля	Название поля	Описание	Пример значения
	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\

Тип поля	Название поля	Описание	Пример значения
			\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.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	syslog
	Name	Тип источника.	log
	Threat Level	Уровень угрозы.	Может принимать значения: • 0 — emergencies; • 1 — alerts; • 2 — critical; • 3 — errors; • 4 — warnings; • 5 — notifications; • 6 — informational; • 7 — debugging.

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
	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	node1

Тип поля	Название поля	Описание	Пример значения
		произошло событие.	
	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 UserID

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

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

Тип поля	Название поля	Описание	Пример значения
	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),

Название поля	Описание	Пример значения
		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

Название поля		Описание	Пример значения
bytes_recv		Количество пакетов, переданных в направлении назначение — источник.	100
packets_sent		Количество пакетов, переданных в направлении источник — назначение.	2
packets_recv		Количество байтов, переданных в направлении назначение — источник.	5
request_method		Метод, используемый для доступа к URL-адресу (POST, GET и т.п.).	GET
url		Поле содержит URL-адрес запрашиваемого ресурса с указанием используемого протокола.	http://www.secure.com
media_type		Тип контента.	application/json
status_code		Код ответа HTTP.	302
http_referer		URL источника запроса (реферер HTTP).	https://www.google.com/
decrypted		Поле указывает было ли содержимое расшифровано.	true, false
useragent		Useragent пользовательского браузера.	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/ 20100101 Firefox/96.0
application	**id**	Идентификатор приложения.	20
	name	Название приложения.	Youtube
	threat_ level	Уровень угрозы приложения.	0
	app_pr otocol	Протокол прикладного уровня и его версия.	HTTP\/1.1"
url_cat egories	**id**	Идентификатор категории, к которой относится URL.	39

Название поля			Описание	Пример значения
	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	f93da24d-74f9-4f8c-9e9b-8e6d02346fb4

Название поля			Описание	Пример значения
			которого вызвало создание события.	
	name		Название правила.	Default allow
	type		Тип сработавшего правила.	
user	**guid**		Уникальный идентификатор пользователя.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name		Имя пользователя	user_name
	groups	**guid**	Уникальный идентификатор группы, в которой состоит пользователь.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Название группы, в которой состоит пользователь.	Default Group

Описание журнала DNS

Название поля	Описание	Пример значения
timestamp	Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
session	Идентификатор сессии.	00000000-0000-0000-0000-000000000000
node	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorereaeda
reasons	Причина, по которой было создано событие, например, url категория, на которых сработало правило.	{"url_cats":[{"id":37,"name":"Search Engines & Portals","threat_level":1}]}
proto	Используемый протокол 4-го уровня.	UDP
host	Имя хоста.	google.com

Название поля			Описание	Пример значения
data			Поле используется для указания передаваемых данных.	{"question": [{"domain":"google.com","type":"A","class":"IN"}], "answer": [{"domain":"google.com","type":"TXT","class":"IN","ttl": 5,"data":"Blocked"}, {"domain":"google.com","type": "A","class":"IN","ttl": 5,"data":"10.10.0.1"}]}
url_categories	**id**		Идентификатор сработавшей URL-категории.	37
	threat_level		Уровень угрозы сработавшей категории.	Может принимать значения: • 1 — очень низкий. • 2 — низкий. • 3 — средний. • 4 — высокий. • 5 — очень высокий.
	name		Название сработавшей категории.	Search Engines & Portals
action			Действие, принятое устройством в соответствии с настроенными политиками.	block
application		**id**	Идентификатор приложения.	5
		name	Название приложения.	
		threat_level	Уровень угрозы приложения.	0
		app_protocol	Протокол прикладного уровня.	DNS
source	**zone**	**guid**	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		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.
	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

Название поля			Описание	Пример значения
	name		Имя пользователя.	user1
	groups	**guid**	Уникальный идентификатор группы, в которых состоит пользователь.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Название группы, в которой состоит пользователь.	Default Group

Описание журнала трафика

Название поля	Описание	Пример значения
timestamp	Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
session	Идентификатор сессии.	a7a3cd49-8232-4f1a-962a-3659af89e96f (если System: 00000000-0000-0000-0000-000000000000)
node	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
proto	Используемый протокол 4-го уровня.	TCP или UDP
action	Действие, принятое устройством в соответствии с настроенными политиками.	accept
bytes_sent	Количество байтов, переданных в направлении источник — назначение.	100
bytes_recv	Количество байтов, переданных в направлении назначение — источник.	6
packets_recv	Количество пакетов, переданных в направлении назначение — источник.	1

Название поля			Описание	Пример значения
packets_sent			Количество пакетов, переданных в направлении источник — назначение.	1
json_data			Дополнительные данные.	null
application	**id**		Идентификатор приложения.	195
	threat_level		Уровень угрозы приложения.	Может принимать значения: • 1 — очень низкий. • 2 — низкий. • 3 — средний. • 4 — высокий. • 5 — очень высокий.
	app_protocol		Протокол прикладного уровня.	HTTP
	name		Название приложения.	Youtube
source	**zone**	**guid**	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника трафика.	Trusted
	country		Название страны источника.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика.	10.10.10.10
	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)

Название поля			Описание	Пример значения
	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 СОВ

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_sent		Количество пакетов, переданных в направлении источник — назначение.	1
packets_recv		Количество пакетов, переданных в направлении назначение — источник.	1
json_data		Дополнительные данные.	null
application	**id**	Идентификатор приложения.	195
	threat_level	Уровень угрозы приложения.	Может принимать значения: • 1 — очень низкий. • 2 — низкий.

Название поля			Описание	Пример значения
				• 3 — средний. • 4 — высокий. • 5 — очень высокий.
	name		Название приложения.	Youtube
	app_protocol		Протокол прикладного уровня.	HTTP
user	**guid**		Уникальный идентификатор пользователя. Если пользователь типа Unknown, то идентификатор: 00000000-0000-0000-0000-000000000000.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name		Имя пользователя.	Admin
	groups	**guid**	Уникальный идентификатор группы, в которых состоит пользователь.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Название группы, в которой состоит пользователь.	Default Group
rule	**guid**		Уникальный идентификатор правила, срабатывание которого создало событие.	59e38e06-533a-4771-9664-031c3e8b2e1f
	name		Название правила, срабатывание которого вызвало событие.	Allow trusted to untrusted
	type		Тип сработавшего правила	idps
signatures	**id**		Идентификатор сработавшей сигнатуры.	999999
	threat_level		Уровень угрозы сработавшей сигнатуры.	Может принимать значения: • 1 — очень низкий. • 2 — низкий. • 3 — средний. • 4 — высокий. • 5 — очень высокий.

Название поля			Описание	Пример значения
	name		Название сработавшей сигнатуры.	BlackSun Test
source	**zone**	**guid**	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника трафика.	Trusted
	country		Название страны источника.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика.	10.10.10.10
	port		Порт источника.	Может принимать значения от 0 до 65535.
	mac		MAC-адрес источника.	01:23:45:67:89:AB
destination	**zone**	**guid**	Уникальный идентификатор зоны назначения трафика.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика.	Untrusted
	country		Название страны назначения.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес назначения трафика.	104.19.197.151
	port		Порт назначения.	Может принимать значения от 0 до 65535.
	mac		MAC-адрес назначения.	01:23:45:67:89:AB

Описание журнала АСУ ТП

Название поля	Описание	Пример значения
timestamp	Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
pdu_severity	Критичность АСУ ТП.	1

Название поля		Описание	Пример значения
pdu_func		Код функции (говорит ведомому устройству, какие данные или выполнение какого действия требует от него ведущее устройство).	12
pdu_address		Адрес регистра, с которым необходимо провести операцию.	3154
node		Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
details	**pdu_varname**	Имя переменной. Параметр, в основном, используется для обмена данными в режиме реального времени. Параметр относится к протоколу MMS.	VAR
	pdu_device	Адрес устройства, используемый в протоколах MMS и OPCUA.	DEV
	mb_write_quantity	Количество значений для записи (команда Read Write Register).	998
	mb_write_addr	Начальный адрес регистра для записи (команда Read Write Register).	776
	mb_value	Записываемое значение (для команд Write Single Coil, Write Single Register).	322
	mb_unit_id	Адрес устройства.	186
	mb_read_quantity	Количество значений для чтения (команда Read Write Register).	658
	mb_read_addr	Начальный адрес регистра для чтения (команда Read Write Register).	122

Название поля		Описание	Пример значения
	mb_quantity	Количество значений для чтения.	875
	mb_payload	Значения регистров (для команд Read Coil, Read Holding Registers, Read Input Registers, Read/Write Multiple registers, Write Multiple Coil).	75be5ecdc24f9883
	mb_or_mask	Значение маски OR команды Mask Write Register.	1024
	mb_message	Сообщение Modbus.	exception
	mb_exception_code	Код ошибки. Актуален для типа сообщения error_response.	255
	mb_and_mask	Значение маски AND команды Mask Write Register.	121
	mb_addr	Адрес регистра.	3154
	iec104_msgtype	Тип запроса.	request, response, error_response
	iec104_ioa	Адрес объекта информации, который позволяет однозначно идентифицировать приёмной стороной тип события.	23
	iec104_cot	Причина передачи протокольного блока данных прикладного уровня (Application Protocol Data Unit, APDU).	6
	iec104_asdu	Адрес ASDU (COA — Common Object Address). Параметр относится к протоколу IEC-104.	123
app_protocol		Протокол прикладного уровня.	Modbus
action			pass

Название поля			Описание	Пример значения
			Действие, принятое устройством в соответствии с настроенными политиками.	
source	**zone**	**guid**	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника трафика.	Trusted
	country		Название страны источника.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика.	10.10.10.10
	port		Порт источника.	Может принимать значения от 0 до 65535.
destination	**zone**	**guid**	Уникальный идентификатор зоны назначения трафика.	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.
rule	**guid**		Уникальный идентификатор правила, срабатывание которого создало событие.	59e38e06-533a-4771-9664-031c3e8b2e1f
	name		Название правила, срабатывание которого вызвало событие.	SCADA Sample Rule

Описание журнала инспектирования SSH

Название поля			Описание	Пример значения
timestamp			Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node			Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
command			Команда, передаваемая по SSH.	whoami
action			Действие, принятое устройством в соответствии с настроенными политиками.	block
application		**id**	Идентификатор приложения.	195
		name	Название приложения.	
		threat_level	Уровень угрозы приложения.	Может принимать значения от 2 до 10 (установленный уровень угрозы приложения, умноженный на 2).
		app_protocol	Протокол прикладного уровня.	SSH или SFTP
source	**zone**	**guid**	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника трафика.	Trusted
	country		Название страны источника.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика.	10.10.10.10
	port		Порт источника.	Может принимать значения от 0 до 65535.
	mac		MAC-адрес источника.	FA:16:3E:65:1C:B4

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

Описание журнала защиты почтового трафика

Название поля		Описание	Пример значения
timestamp		Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node		Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
action		Действие, принятое устройством в соответствии с настроенными политиками.	mark
bytes_sent		Количество байтов, переданных в направлении источник — назначение.	0
bytes_recv		Количество байтов, переданных в направлении назначение — источник.	0
packets_sent		Количество пакетов, переданных в направлении источник — назначение.	0
packets_rcv		Количество пакетов, переданных в направлении назначение — источник.	0
decrypted		Поле указывает было ли содержимое расшифровано.	true, false
from		Почтовый адрес отправителя.	sender@example.com
to		Почтовый адрес получателя.	receiver@example.com
application	**id**	Идентификатор приложения.	9
	name	Название приложения.	

Название поля			Описание	Пример значения
		threat_level	Уровень угрозы приложения.	Может принимать значения от 2 до 10 (установленный уровень угрозы приложения, умноженный на 2).
		app_protocol	Сетевой протокол прикладного уровня.	SMTP
source	**zone**	**guid**	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника трафика.	Trusted
	country		Название страны источника.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика.	10.10.10.10
	port		Порт источника.	Может принимать значения от 0 до 65535.
	mac		MAC-адрес источника.	01:23:45:67:89:AB
destination	**zone**	**guid**	Уникальный идентификатор зоны назначения трафика.	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.	10.10.10.10
	port		Порт назначения.	Может принимать значения от 0 до 65535.
	port		MAC-адрес назначения.	01:23:45:67:89:AB
rule	**guid**		Уникальный идентификатор правила, срабатывание которого создало событие.	59e38e06-533a-4771-9664-031c3e8b2e1f

Название поля			Описание	Пример значения
	name		Название правила, срабатывание которого вызвало событие.	Mail security rule
	type		Тип сработавшего правила.	Mail security rule
user	**guid**		Уникальный идентификатор пользователя.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name		Имя пользователя.	user_name
	groups	**guid**	Уникальный идентификатор группы, в которой состоит пользователь.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Название группы, в которой состоит пользователь.	Default Group

Описание журнала событий конечных устройств

Название поля	Описание	Пример значения
user_name	Имя пользователя.	DESKTOP-0731NFQ\\Username
timestamp	Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
status	Результат выполнения WMI или SNMP запроса.	OK, Error
source_name	Источник журнала событий.	Microsoft-Windows-Security-Auditing
endpoint_name	Название конечного устройства или сенсора.	DESKTOP-0731NFQ
endpoint_id	Идентификатор конечного устройства или сенсора.	35fb5820-74db-4eac-b05b-d01bc284c4e8
node	Идентификатор конечного устройства или узла, на котором запущен сенсор.	35fb5820-74db-4eac-b05b-d01bc284c4e8
log_level	Тип события.	

Название поля	Описание	Пример значения
		Аудит успеха, Предупреждение, Сведения, Аудит отказа, Ошибка
log_file	Тип журнала, содержащего важную информацию о программных и аппаратных событиях.	Security (файл журнала безопасности), Application (файл журнала приложений), System (файл системного журнала), Windows PowerShell
log_event_type	Тип события лога.	1 (error), 2 (warning), 3 (information), 4 (audit success), 5 (audit failure).
log_event_id	Идентификатор события.	4672
log_event_code	Код события журнала.	14056
log_category_string	Категория события.	Special Logon
insertion_string	Строка вставки – данные блока EventData события Windows.	Windows DefenderSECURITY_PRODUCT_STATE_ON
error	Ошибка WMI или SNMP, возникшая в результате выполнения запроса.	0
data	Подробная информация о событии.	Тип запуска службы "Установщик модулей Windows" был изменен с "Автоматически" на "Вручную".
counter_id	Идентификатор счётчика, добавленного в WMI или SNMP сенсор.	35fb5820-74db-4eac-b05b-d01bc284c4e8
computer_name	Имя компьютера.	DESKTOP-0731NFQ

Описание журнала правил конечных устройств

Название поля		Описание	Пример значения
timestamp		Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
session		Идентификатор сессии.	00000006-0000-0000-f04d-14bdad0f01bb
proto		Используемый протокол 4-го уровня.	TCP
host		Имя хоста.	www.google.com
action		Действие, принятое устройством в соответствии с настроенными политиками.	drop, accept, nat
endpoint_name		Имя конечного устройства.	DESKTOP-0731NFQ
endpoint_id		Идентификатор конечного устройства.	35fb5820-74db-4eac-b05b-d01bc284c4e8
media_type		Тип контента.	application/json
app_name		Приложение, к которому было применено правило межсетевого экрана.	C:\\Program Files (x86)\\Microsoft\\Edge\\Application\\msedge.exe
source	**ip**	IPv4-адрес источника.	10.10.10.10
	port	Порт источника.	Может принимать значения от 0 до 65535.
destination	**ip**	IPv4-адрес назначения.	104.19.197.151
	port	Порт назначения	Может принимать значения от 0 до 65535.
rule	**guid**	Уникальный идентификатор правила, срабатывание которого создало событие.	f93da24d-74f9-4f8c-9e9b-8e6d02346fb4
	name	Название правила, срабатывание которого вызвало событие.	Default allow

Название поля		Описание	Пример значения
	type	Тип сработавшего правила.	
url_categories	**id**	Идентификатор категории, к которой относится URL.	39
	threat_level	Уровень угрозы категории URL.	Может принимать значения: • 1 — очень низкий. • 2 — низкий. • 3 — средний. • 4 — высокий. • 5 — очень высокий.
	name	Название категории, к которой относится URL.	Social Networking

Описание журнала приложений конечных устройств

Название поля	Описание	Пример значения
user_name	Имя пользователя, под учётной записью которого выполнен вход на конечном устройстве.	DESKTOP-0731NFQ\\User
timestamp	Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
endpoint_name	Название конечного устройства или сенсора.	DESKTOP-0731NFQ
endpoint_id	Идентификатор конечного устройства или сенсора.	35fb5820-74db-4eac-b05b-d01bc284c4e8
process_id	Идентификатор процесса.	3916
hash	Хэш приложения.	B4CE5C3495FEA0A4FDBAC8ABDCD199F7E4CA8C1F
app_name	Приложение, которое было запущено/остановлено.	C:\\Program Files (x86)\\Microsoft\\Edge\\Application\\msedge.exe
action	Действие (запуск или остановка приложения).	start, stop

Название поля	Описание	Пример значения
version	Версия приложения.	6.2.19041.746
subject	Субъект подписи.	Microsoft Corporation
issuer	Издатель сертификата для приложения.	Microsoft Windows Production PCA 2011
cmd_line	Запрос командной строки.	C:\\Windows\\system32\ \svchost.exe -k wsappx -p -s AppXSvc
session_id	Идентификатор сессии.	1656038456

Описание журнала аппаратуры конечных устройств

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

Описание журнала 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
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:

Название поля	Описание	Пример значения
		\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.

Название поля	Описание	Пример значения
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.	
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

Название поля	Описание	Пример значения
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)

Название поля		Описание	Пример значения
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 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-1-5-21-3795870133-522032 5-2125745684-513\", \"S-1-5-21-3795870133-522032 5-2125745684-512\", \"S-1-5-21-3795870133-522032 5-2125745684-572\"], \"user_sid\": \"S-1-5-21-3795870133-522032 5-2125745684-1103\",\"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

Название поля			Описание	Пример значения
	name		Название правила, срабатывание которого вызвало событие.	dev.local
	type		Тип сработавшего правила.	syslog
user	**guid**		Уникальный идентификатор пользователя. Если пользователь типа Unknown, то идентификатор: 00000000-0000-0000-0000-000000000000.	745591c3-9d21-092d-8db4-5b9b0000044f
	name		Имя пользователя.	user1
	groups	**guid**	Уникальный идентификатор группы, в которых состоит пользователь.	aa218609-8716-9252-df20-88c43a0d0bf6
		name	Название группы, в которой состоит пользователь.	CN=Domain Users,CN=Users,DC=dev,DC=local