

Table of Contents

Table of Contents	1
Сенсоры	2
Общие сведения	3
Сенсоры UserGate	4
Сенсоры SNMP	6
Управление SNMP MIB	8
Сенсоры WMI	9
Конечные устройства	10
Коннекторы	11

Общие сведения

Documentation: 

Version: 7.x

Product: SIEM

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

Version: 7.x

Product: SIEM

Documentation: 

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

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

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

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

Настройка интеграции с UserGate NGFW

Для настройки интеграции UserGate SIEM с UserGate NGFW необходимо:

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

Получение кода устройства UserGate NGFW

Примечание Инструкция ниже выполняется в веб-консоли UserGate NGFW.

Чтобы получить код устройства:

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

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

Подключение UserGate NGFW в качестве сенсора

Примечание Инструкция ниже выполняется в веб-консоли UserGate SIEM.

Чтобы подключить UserGate NGFW к UserGate SIEM в качестве сенсора:

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

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

Управление сенсорами UserGate

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

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

- Зеленый — соединение между серверами сенсора UserGate и UserGate SIEM установлено.

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

Вы можете управлять подключенными сенсорами:

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

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

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

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

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

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

По умолчанию для сенсора в таблице отображаются следующие данные:

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

Сенсоры SNMP

Version: 7.x

Product: SIEM

Documentation: ☒

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

Для настройки сенсора SNMP необходимо выполнить следующие шаги:

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

При создании сенсора SNMP необходимо заполнить следующие поля:

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

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

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

Управление SNMP MIB

Product: SIEM

Version: 7.x

Documentation: 

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

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

Сенсоры WMI

Version: 7.x

Product: SIEM

Documentation: ☒

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

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

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

Конечные устройства

Version: 7.x

Product: SIEM

Documentation: ☒

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

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

Отображена следующая информация:

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

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

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

Коннекторы

Version: 7.x

Product: SIEM

Documentation: ☒

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

Для добавления коннектора необходимо указать следующие данные:

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

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

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

