

Table of Contents

Table of Contents	1
Настройка устройства	2
Раздел настройки	3
Управление устройством	5
Администраторы	9
Управление сертификатами	15
Серверы аутентификации	17
Профили аутентификации	19
Роли и ролевые разрешения пользователей	20
Каталоги пользователей	28
Расширение системного раздела	29

Раздел настройки

Documentation: ☒
Version: 7.1.x
Product: SIEM

Раздел **Настройки** определяет базовые установки SIEM:

Наименование	Описание
Настройки интерфейса	Настройки интерфейса SIEM: • 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. • Таймер автоматического закрытия сессии (мин.) — настройка таймера автоматического закрытия сессии в случае отсутствия активности администратора в веб-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.
Центр обновлений	Настройки для управления скачиванием обновлений программного обеспечения и системных библиотек, предоставляемых по подписке. Обновления ПО — настройка канала обновлений (стабильные, бета), проверки наличия новых обновлений ПО и скачивание офлайн-обновлений. Обновления библиотек — проверка наличия обновлений библиотек, скачивание обновлений и настройка расписания автоматической проверки и скачивания библиотек. Проверить наличие обновлений библиотек и скачать последние обновления можно по ссылке Проверить обновления. Настроить автоматическое обновление библиотек можно по ссылке Настроить. Для каждой библиотеки можно настроить расписание автоматической проверки и скачивания обновлений. При задании расписания 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". При установке флажка Единое расписание для всех обновлений расписание текущей библиотеки будет применено ко всем библиотекам.

Наименование	Описание
Учет изменений	При включении данной опции и создания Типов изменений любое изменение в конфигурацию, вносимое администратором через веб-консоль, будет требовать указание типа изменения и описания вносимого изменения. В качестве типов изменения могут быть, например, указаны: • Распоряжение. • Приказ. • Регламентные работы, и т.д. Количество типов изменений не ограничено.
Системные DNS-серверы	Укажите корректные IP-адреса серверов DNS в настройках.
Состояние Log Analyzer	Отображается текущее состояние сервера: • Состояние — показывает текущее состояние сервиса статистики. • Версия устройства — версия SIEM. • Метрики — количество приходящих событий для сервиса статистики (усредненное значение за последние 5 сек.).
Состояние сборщика логов	Отображается текущее состояние сборщика логов: • Состояние — показывает текущее состояние сервиса статистики. • Метрики — количество приходящих событий для сервиса syslog (усредненное значение за последние 5 сек.).
Агент UserGate Management Center	Настройки для подключения устройства к центральной консоли управления, позволяющей управлять парком устройств SIEM 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.

Компания UserGate постоянно работает над улучшением качества своего программного обеспечения и предлагает обновления продукта SIEM 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 SIEM.

Для установки обновлений необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл резервного копирования	Создать резервную копию состояния SIEM, 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 SIEM будет перезагружен.

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

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

Диагностика

В данном разделе задаются параметры диагностики сервера, необходимые службе технической поддержки SIEM 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 SIEM.
Журналы диагностики	• Скачать журналы — скачать диагностические журналы для передачи их в службу поддержки UserGate. • Очистить журналы — удалить архивные (т.е. не активные в настоящий момент) журналы.
Удаленный помощник	• 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 SIEM для диагностики и решения проблем. Для успешной активации удаленного помощника SIEM 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 SIEM. • Выключить — выключение сервера SIEM.
Настройки вышестоящего прокси для проверки лицензий и обновлений	Настройка параметров вышестоящего HTTP(S) прокси-сервера для обновления лицензии и обновления ПО сервера UserGate. Необходимо указать IP-адрес и порт вышестоящего прокси сервера. При необходимости указать логин и пароль для аутентификации на вышестоящем прокси-сервере.

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 <i>PRODUCT</i> — тип продукта: NGFW, LogAn, MC; <i>NODE-NAME</i> — имя узла UserGate; <i>DATE</i> — 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 использования 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 находиться на SSH-сервере в директории пользовательских ключей <code>/home/user/.ssh/</code> в файле <code>authorized_keys</code>. При первоначальной настройке правила экспорта резервного копирования по SSH обязательна проверка соединения (кнопка Проверить соединение); при проверке соединения fingerprint помещается в <code>known_hosts</code>, 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.

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

ПримечаниеЭкспорт/импорт настроек не восстанавливает состояние интерфейсов и информацию о лицензии. После окончания процедуры импорта необходимо повторно зарегистрировать SIEM 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 SIEM. version — версия SIEM. 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.

Наименование	Описание
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

Version: 7.1.x
Product: SIEM
Documentation: ☒

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

Примечание При первоначальной настройке SIEM создается локальный суперпользователь Admin.

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

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

При создании профиля доступа администратора необходимо указать следующие параметры:

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

Ролевые разрешения для ролей, созданных в системе по умолчанию:

Ролевое разрешение	Описание	Administrator	Supervisor	Investigator	Analyst
--------------------	----------	---------------	------------	--------------	---------

Роль	Описание	Administrator	Supervisor	Investigator	Analyst
Назначаемый пользователь	Пользователь с этим ролевым разрешением может быть назначен на инцидент при создании или редактировании инцидента.		+	+	+
Назначение инцидентов	Возможность назначать пользователей на инциденты при создании или редактировании инцидента.		+	+	+
Закрытие инцидента	Возможность закрыть инцидент.		+	+	+
Создание инцидентов	Возможность создавать инциденты.		+	+	+
Изменение инцидента	Возможность изменять инциденты.		+	+	+
Переоткрытие инцидента	Возможность переоткрывать инциденты.		+	+	+
Редактирование наблюдателей	Возможность добавлять и удалять наблюдателей.		+	+	+
Оставление комментариев	Возможность комментировать инциденты.		+	+	+
Удаление любых комментариев	Возможность удалять любые комментарии к инцидентам.		+		
Удаление собственных комментариев	Возможность удалять собственные комментарии к инцидентам.		+	+	+
Редактирование любых комментариев	Возможность редактировать любые комментарии к инцидентам.		+		
Редактирование своих комментариев	Возможность редактировать свои комментарии к инцидентам.		+	+	+
Создание вложений	Возможность добавлять вложения к инцидентам.		+	+	+
Удаление любых вложений	Возможность удалять любые вложения.		+	+	
Удаление своих вложений	Возможность удалять свои вложения.		+	+	+
Редактирование улик	Возможность создания и редактирования улик.		+	+	+
Обновление обогащений	Возможность обновлять/запрашивать обогащения улик.		+	+	
Создание отчёта	Возможность создавать, загружать и посылать отчёты инцидентов.		+	+	+
Добавление журналов к инциденту	Возможность добавлять журналы к инциденту.		+	+	+
Удалить все срабатывания/журналы из инцидента	Возможность удаления всех срабатываний/журналов из инцидента.		+	+	
Удаление собственных срабатываний, журналов к инцидентам	Возможность удалять собственные срабатывания/журналы к инцидентам.		+	+	+
Создание схемы инцидента	Возможность создавать схемы инцидентов.		+		

Ролевое разрешение	Описание	Administrator	Supervisor	Investigator	Analyst
Редактирование схемы инцидента	Возможность редактировать схемы инцидентов.		+		
Удаление схемы инцидента	Возможность удалять схемы инцидентов.		+		
Установка схемы инцидентов по умолчанию	Возможность установки схем инцидентов по умолчанию.		+		
Создание состояния инцидента	Возможность создавать состояния инцидентов.	+	+		
Редактирование состояния инцидента	Возможность редактировать состояния инцидентов.	+	+		
Удаление состояния инцидента	Возможность удалять состояния инцидентов.	+	+		
Создание типа инцидента	Возможность создавать типы инцидентов.	+	+		
Редактирование типа инцидента	Возможность редактировать типы инцидентов.	+	+		
Удаление типа инцидента	Возможность удалять типы инцидентов.	+	+		
Создание решения инцидента	Возможность создавать решения инцидентов.	+	+		
Редактирование решения инцидента	Возможность редактировать решения инцидентов.	+	+		
Удаление решения инцидентов	Возможность удалять решения инцидентов.	+	+		
Создание правила аналитики	Возможность создавать правила аналитики.		+	+	
Удаление правила аналитики	Возможность удалять правила аналитики.		+		
Редактирование правила аналитики	Возможность редактировать правила аналитики.		+	+	
Включение/выключение правила аналитики	Возможность включать/выключать правила аналитики.		+	+	
Запуск правила аналитики	Возможность запустить правило аналитики не в режиме реального времени.		+		
Создание действия реагирования	Возможность создавать действия реагирования.		+	+	
Редактирование действия реагирования	Возможность редактировать действия реагирования.		+	+	
Удаление действия реагирования	Возможность удалять действия реагирования.		+	+	
Включение/выключение действия реагирования	Возможность включать/выключать действия реагирования.		+	+	
Создание сенсора UserGate	Возможность создавать сенсоры UserGate.	+	+		
Редактирование сенсора UserGate	Возможность редактировать сенсоры UserGate.	+	+		

Ролевое разрешение	Описание	Administrator	Supervisor	Investigator	Analyst
Включение/выключение сенсора UserGate	Возможность включать/выключать сенсоры UserGate.	+	+		
Удаление сенсора UserGate	Возможность удалять сенсоры UserGate.	+	+		
Создание сенсора SNMP	Возможность создавать сенсоры SNMP.	+	+		
Редактирование сенсора SNMP	Возможность редактировать сенсоры SNMP.	+	+		
Включение/выключение сенсора SNMP	Возможность включать/выключать сенсоры SNMP.	+	+		
Удаление сенсора SNMP	Возможность удалять сенсоры SNMP.	+	+		
Создание сенсора WMI	Возможность создавать сенсоры WMI.	+	+		
Редактирование сенсора WMI	Возможность редактировать сенсоры WMI.	+	+		
Включение/выключение сенсора WMI	Возможность включать/выключать сенсоры WMI.	+	+		
Удаление сенсора WMI	Возможность удалять сенсоры WMI.	+	+		
Добавление SNMP MIB файла	Возможность добавлять SNMP MIB файлы.	+	+		
Удаление SNMP MIB файла	Возможность удалять SNMP MIB файлы.	+	+		
Создание коннекторов	Возможность создавать коннекторы.	+	+		
Редактирование коннекторов	Возможность редактирования коннекторов.	+	+		
Удаление коннекторов	Возможность удалять коннекторы.	+	+		
Создание правила Syslog	Возможность создавать правила Syslog.	+	+		
Удаление правила Syslog	Возможность удалять правила Syslog.	+	+		
Редактирование правил и коннектора Syslog	Возможность редактировать правила Syslog и настраивать Syslog.	+	+		
Включение/выключение правила Syslog	Возможность включать/выключать правила Syslog.	+	+		
Создание группы email	Возможность создавать почтовые адреса/почтовые группы.	+	+		
Редактирование группы email	Возможность редактировать почтовые адреса/почтовые группы.	+	+		
Удаление группы email	Возможность удалять почтовые адреса/почтовые группы.	+	+		

Ролевое разрешение	Описание	Administrator	Supervisor	Investigator	Analyst
Создание группы номеров телефонов	Возможность создавать номера телефонов/группы телефонных номеров.	+	+		
Редактирование группы номеров телефонов	Возможность редактировать номера телефонов/группы телефонных номеров.	+	+		
Удаление группы номеров телефонов	Возможность удалять номера телефонов/группы телефонных номеров.	+	+		
Создание команд.	Возможность создавать команды к коннекторам.	+	+		
Редактирование команд.	Возможность редактировать команды к коннекторам.	+	+		
Удаление команд.	Возможность удалять команды к коннекторам.	+	+		
Создание профиля оповещения	Возможность создавать профиль оповещения.	+	+		
Редактирование профиля оповещения	Возможность редактировать профиль оповещения.	+	+		
Удаление профиля оповещения	Возможность редактировать профиль оповещения.	+	+		
Создание категории срабатывания	Возможность создавать категории срабатывания.	+	+		
Редактирование категории срабатывания	Возможность редактировать категории срабатывания.	+	+		
Удаление категории срабатывания	Возможность удалять категории срабатывания.	+	+		
Редактирование настройки обогащения	Возможность редактировать настройки обогащений.	+	+		
Включение/выключение сервиса обогащения	Возможность включать/выключать сервисы обогащений.	+	+		
Создание правила нормализации	Возможность создавать правила нормализации журналов.	+	+		
Редактирование правила нормализации	Возможность редактировать правила нормализации журналов.	+	+		
Удаление правила нормализации	Возможность удалять правила нормализации журналов.	+	+		
Включение/выключение правила нормализации	Возможность включать/выключать правила нормализации журналов.	+	+		

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

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

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

Для настройки этих параметров необходимо:

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

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

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

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

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

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

Управление сертификатами

Version: 7.1.x
Product: SIEM
Documentation: ☒

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

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

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

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

Для экспорта сертификата необходимо:

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

ПримечаниеРекомендуется сохранять сертификат для возможности его последующего восстановления.

ПримечаниеВ целях безопасности SIEM не разрешает экспорт приватных ключей сертификатов.

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

Наименование	Описание
Шаг 1. Начать импорт	Нажать на кнопку Импорт .

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

Серверы аутентификации

Version: 7.1.x
Product: SIEM
Documentation: ☒

Серверы аутентификации — это внешние источники учетных записей пользователей для авторизации в веб-консоли управления UserGate SIEM. SIEM 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 SIEM через домены Active Directory/FreeIPA.

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

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

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

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

domain\user/system или user@domain/system

Сервер аутентификации RADIUS

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

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

Наименование	Описание
Включено	Включение/отключение использования данного сервера аутентификации.

Наименование	Описание
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

Version: 7.1.x

Product: SIEM

Documentation: ☒

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

Роли и ролевые разрешения пользователей

Version: 7.1.x
Product: SIEM
Documentation: ☒

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

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

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

Для пользователей могут быть указаны следующие ролевые разрешения.

Наименование	Описание
Назначаемый пользователь	Пользователь с этим разрешением может быть назначен на инцидент. Ответственный за инцидент может быть указан при создании или редактировании инцидента.
Назначение инцидентов	Возможность назначать пользователей на инциденты. Указать ответственного можно при создании или редактировании инцидента.
Закрытие инцидента	Возможность закрыть инцидент. Часто бывает полезно, когда разработчики разрешают инциденты, а тестировщики закрывают их. Закрыть инцидент можно во вкладке Инциденты → <INC-N:Название инцидента> (где N — порядковый номер инцидента). Закрытие инцидента возможно только из состояний, для которых в схеме инцидента настроен переход в состояние Закрыт . Подробнее читайте в Настройках инцидентов .
Создание инцидентов	Возможность создавать инциденты. Инциденты могут быть созданы во вкладке Инциденты → Журнал инцидентов или автоматически при срабатывании правила аналитики. О создании инцидентов подробнее читайте в разделе Создание инцидентов безопасности .
Изменение инцидента	Возможность изменять инциденты. Редактирование инцидентов доступно во вкладке Инциденты → <INC-N:Название инцидента> (где N — порядковый номер инцидента). Подробнее читайте в разделе 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 .

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

Наименование	Описание
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.
Установка схемы инцидентов по умолчанию	Возможность установки схем 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.
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.

Наименование	Описание
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. 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.

Наименование	Описание
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. 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. Коннекторы доступны во вкладке Настройки в разделе Сенсоры → Коннекторы . Подробнее читайте в разделе Коннекторы.

Наименование	Описание
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. 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 быть 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 быть 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 .

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

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

Каталоги пользователей

Product: SIEM

Version: 7.1.x

Documentation: 

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

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

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

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

Расширение системного раздела

Version: 7.1.x
Product: SIEM
Documentation: ☒

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.
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.

