

Table of Contents

Table of Contents	1
Настройка устройства	2
Настройка общих параметров	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
Кластеризация и отказоустойчивость	30

Настройка общих параметров

Documentation: ☒
Version: 7.x
Product: SIEM

В этом разделе описаны общие параметры UserGate SIEM, а также приведены рекомендации по настройке этих параметров.

Блок параметров	Параметр	Описание
Настройки интерфейса	Часовой пояс	Часовой пояс, соответствующий вашему местоположению. Используется для работы расписаний, настроенных в правилах, а также для корректного отображения времени и даты, например в отчетах или в журналах
	Язык интерфейса по умолчанию	Язык, используемый в веб-консоли устройства по умолчанию
	Таймер автоматического закрытия сессии (мин.)	Для настройки таймера необходимо указать, по истечении скольких минут бездействия администратора в веб-консоли должна завершаться его сессия
Настройка времени сервера	Использовать NTP	При включенном параметре для синхронизации времени на устройстве будут использоваться серверы NTP из указанного списка
	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 (UTC)	Время на сервере в часовом поясе UTC
Обновления ПО (в версиях 7.1.x, 7.2.x, 7.3.x доступен общий блок параметров с обновлениями — Центр обновлений)	Канал обновлений	Настройка канала для получения обновлений программного обеспечения UserGate (UGOS) из репозитория UserGate. Вы можете выбрать Стабильные (стабильные версии ПО) или Бета (версии ПО для бета-тестирования). Если настроена интеграция с UserGate Management Center, параметр примет значение Management Center и будет недоступен для изменения
	Обновления	Проверка наличия обновлений UGOS в репозитории UserGate. После проверки вы можете вручную загрузить и установить доступные обновления. В процессе установки обновления UGOS вы можете создать точку восстановления. Это позволит восстановить предыдущую версию UGOS при возникновении проблем. Действие будет доступно в стартовом меню после установки обновления UGOS
	Офлайн-обновление	Загрузка файла обновления UGOS офлайн
	Обновления	Проверка наличия обновлений системных библиотек, предоставляемых по подписке, в репозитории UserGate. После проверки вы можете вручную обновить необходимые библиотеки

Блок параметров	Параметр	Описание
Обновления библиотек (в версиях 7.1.x, 7.2.x, 7.3.x доступен общий блок параметров с обновлениями — Центр обновлений)	Расписание автоматических обновлений	Настройка расписания автоматического обновления библиотек. При настройке расписания вы можете выбрать одно из предустановленных значений или указать время вручную в cron-формате: <минуты: 0-59> <часы: 0-23> <дни месяца: 1-31> <месяцы: 1-12> <дни недели: 0-6, где 0 — воскресенье>. Для ручного ввода вы можете использовать следующие символы: - Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что резервное копирование должно выполняться каждый час. - Дефис (-) — для указания диапазона значений. - Запятая (,) — в качестве разделителя значений. - Косая черта (/) — для указания шага между значениями. При установке флажка Единое расписание для всех обновлений расписание выбранной библиотеки будет применено ко всем библиотекам в списке
Учет изменений	Настройка учета изменений	Для настройки учета изменений в веб-консоли устройства необходимо включить параметр и добавить типы изменений (например, распоряжение, приказ или регламентные работы). Учет изменений предполагает, что при внесении какого-либо изменения через веб-консоль администратору необходимо указать тип и причину этого изменения
Системные DNS-серверы		Для настройки DNS-серверов необходимо указать их IP-адреса
Состояние базы данных журналов	Состояние	Состояние модуля статистики
	Версия устройства	Версия ПО UserGate SIEM
	Метрики	Количество событий, которые получает модуль статистики (среднее значение за последние 5 секунд)
Состояние сборщика логов	Состояние	Состояние модуля сбора событий syslog
	Метрики	Количество событий, которые получает модуль сбора событий syslog (среднее значение за последние 5 секунд)
Агент UserGate Management Center	Настройка агента	Настройка интеграции с UserGate Management Center (UGMC). Для настройки доступны следующие параметры: Включено — управление состоянием подключения UserGate SIEM к UGMC. Адрес UserGate Management Center — адрес сервера UGMC в формате IPv4-адреса или FQDN (возможно использование IDN-адреса). Код устройства — идентификатор UserGate SIEM для подключения к UGMC

В разделе **Настройки → UserGate → Управление устройством** вы можете настраивать следующие параметры устройства:

- кластеры отказоустойчивости;
- кластер конфигурации;
- диагностика;
- операции с сервером;
- резервное копирование;
- экспорт и импорт настроек.

Информация о настройке кластеров приведена в разделе «[Кластеризация и отказоустойчивость](#)».

Диагностика

В этом блоке вы можете управлять параметрами диагностики, необходимыми службе технической поддержки UserGate для решения возможных проблем в работе устройства.

Параметр	Описание
Детализация диагностики	Доступны следующие уровни журналирования: • Off — ведение журналов диагностики отключено. • Error — журналировать только ошибки в работе SIEM-системы. • Warning — журналировать только ошибки и предупреждения. • Info — журналировать только ошибки, предупреждения и дополнительную информацию. • Debug — журналировать все возможные события. При журналировании уровней Warning, Info и Debug может снижаться производительность SIEM-системы, поэтому рекомендуется устанавливать уровни Error или Off, если технической поддержкой UserGate не было предложено иное
Журналы диагностики	Вы можете: • Скачать журналы — скачать диагностические журналы для их передачи в службу технической поддержки UserGate. Для скачивания доступны журналы веб-консоли и системные журналы. Скачать выбранные журналы можно только после их архивирования по кнопке Начать архивирование журналов. • Очистить файлы логов — удалить архивные (неактивные в настоящий момент) журналы
Удаленный помощник	Удаленный помощник позволяет специалисту технической поддержки UserGate безопасно подключаться к серверу UserGate SIEM для диагностики и решения проблем. Для активации удаленного помощника устройство должно иметь доступ к серверу удаленного помощника по протоколу SSH. При включенном удаленном помощнике отображаются его идентификатор и токен, которые необходимо сообщить специалисту технической поддержки UserGate

Операции с сервером

В этом блоке вы можете перезагрузить или выключить сервер UserGate SIEM, а также настроить вышестоящий прокси-сервер для получения лицензий и обновлений устройства.

Наименование	Описание
Операции с сервером	Доступны следующие действия: • Перезагрузить — перезагрузка сервера UserGate SIEM. • Выключить — выключение сервера UserGate SIEM

Наименование	Описание
Настройки вышестоящего прокси для проверки лицензий и обновлений	Настройка параметров вышестоящего HTTP или HTTPS прокси-сервера, используемого для получения лицензий и обновлений устройства. Вы можете настроить IP-адрес и порт вышестоящего прокси-сервера, а также логин и пароль, если необходима аутентификация на этом прокси-сервере

UserGate поставяет обновления в рамках лицензии на модуль Security Update (см. раздел « [Лицензирование UserGate SIEM](#) »). При наличии обновлений в блоке **Операции с сервером** отобразится соответствующее оповещение. Установка обновлений может занять длительное время, поэтому рекомендуется планировать этот процесс с учетом возможного времени простоя UserGate SIEM.

Перед установкой обновлений рекомендуется создать резервную копию UserGate SIEM. Это позволит восстановить предыдущее состояние устройства, если возникнут проблемы, связанные с применением обновлений.

Управление резервным копированием

В этом блоке вы можете:

- [создавать резервные копии](#);
- [восстанавливать состояние устройства из резервной копии](#);
- [настраивать расписание экспорта резервных копий на удаленный сервер](#);
- [настраивать SSH-ключи](#).

Чтобы создать резервную копию устройства:

В разделе **Настройки → UserGate → Управление устройством → Управление резервным копированием** нажмите **Создание резервной копии**.

Начнется создание резервной копии. Вы можете прервать процесс по кнопке **Остановить**.

По окончании процесса резервная копия UserGate SIEM будет сохранена в файле backup_PRODUCT_NODENAME_DATE.gpg, где:

- PRODUCT — тип устройства: SIEM;
- NODENAME — имя узла устройства;
- DATE — дата и время создания резервной копии в формате YYYY-MM-DD-HH-MM (в часовом поясе UTC+0).

Запись о создании резервной копии отобразится в журнале событий устройства.

Чтобы восстановить состояние устройства из резервной копии:

1. В разделе **Настройки → UserGate → Управление устройством → Управление резервным копированием** нажмите **Восстановление резервной копии** и подтвердите восстановление.

2. Укажите путь к файлу с резервной копией UserGate SIEM.

Восстановление будет предложено в консоли TTY при перезагрузке сервера UserGate SIEM.

Администраторы могут создавать правила экспорта, по которым резервные копии будут выгружаться на удаленные серверы по расписанию.

Чтобы создать правило экспорта резервной копии устройства:

1. В разделе **Настройки → UserGate → Управление устройством → Управление резервным копированием** нажмите **Добавить**.

2. На вкладке **Общие** укажите имя правила.

3. На вкладке **Удаленный сервер** укажите параметры удаленного сервера:

- тип — FTP или SSH;
- адрес;
- порт для подключения;
- логин и пароль учетной записи;
- путь к существующей папке для сохранения файлов экспорта.

Внимание!Если вы создаете правило для SSH-сервера, необходимо [предварительно настроить SSH-ключи](#). Кроме того, необходимо проверить соединение с SSH-сервером по кнопке «Проверить соединение». Во время проверки устанавливается первичное соединение, при котором отпечаток открытого ключа автоматически добавляется на удаленный сервер. Это обеспечивает безопасность последующих соединений.

4. На вкладке **Расписание** укажите время экспорта резервной копии.

Вы можете выбрать одно из предустановленных значений или указать время вручную в cron-формате: <минуты: 0—59> <часы: 0—23> <дни месяца: 1—31> <месяцы: 1—12> <дни недели: 0—6, где 0 — воскресенье>.

При ручном вводе также можно использовать следующие символы:

- Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что резервное копирование должно выполняться каждый час.
- Дефис (-) — для указания диапазона значений.
- Запятая (,) — в качестве разделителя значений.
- Косая черта (/) — для указания шага между значениями.

5. Нажмите **Сохранить**.

Перед подключением к удаленному SSH-серверу, необходимо настроить SSH-ключи, используемые для авторизации на этом сервере.

Чтобы настроить SSH-ключи:

1. В разделе **Настройки → UserGate → Управление устройством → Управление резервным копированием** нажмите **Настроить SSH-ключ**.

2. Нажмите **Сгенерировать новый ключ**.

Будет сгенерирована пара SSH-ключей (закрытый и открытый). Открытый ключ отобразится в окне настройки, закрытый ключ будет автоматически сохранен на сервере UserGate SIEM.

Примечание Если у вас уже есть пара SSH-ключей, вы можете добавить закрытый ключ на сервер UserGate SIEM вручную по кнопке «Загрузить ключ».

3. Добавьте открытый SSH-ключ на удаленный сервер.

По умолчанию SSH-ключи хранятся в папке `/home/user/.ssh/` в файле `authorized_keys`.

Экспорт и импорт настроек

В этом блоке вы можете экспортировать текущие параметры UserGate SIEM в виде файлов экспорта в формате BIN. Впоследствии такие файлы могут понадобиться [для восстановления параметров устройства](#), а также для импорта в другие системы SIEM.

Экспорт может выполняться вручную или [по расписанию](#). Вы можете экспортировать [все текущие параметры](#) или [только сетевые](#). К сетевым относятся параметры зон, интерфейсов, шлюзов, маршрутов. Сетевые параметры настраиваются в разделе **Настройки → Сеть**.

Чтобы экспортировать все параметры устройства:

В разделе **Настройки → UserGate → Управление устройством → Экспорт и импорт настроек** нажмите **Экспорт → Экспортировать все настройки**.

Параметры будут сохранены в файле `siem_core-siem_core@NODENAME_VERSION_DATE.bin`, где:

- NODENAME — имя узла устройства;
- VERSION — версия UGOS;
- DATE — дата и время выгрузки параметров в формате YYYYMMDD_HHMMSS (в часовом поясе UTC+0).

Чтобы экспортировать только сетевые параметры устройства:

В разделе **Настройки → UserGate → Управление устройством → Экспорт и импорт настроек** нажмите **Экспорт → Экспортировать сетевые настройки**.

Параметры будут сохранены в файле `network-siem_core-siem_core@NODENAME_VERSION_DATE.bin`, где:

- NODENAME — имя узла устройства;
- VERSION — версия UGOS;
- DATE — дата и время выгрузки параметров в формате YYYYMMDD_HHMMSS (в часовом поясе UTC+0).

Администраторы могут создавать правила экспорта, по которым параметры устройства будут выгружаться на удаленные серверы по расписанию. Если узлы устройства объединены в кластер, то при создании правила экспорта на одном из узлов это правило будет распространяться на все узлы кластера. Параметры каждого узла при экспорте будут сохраняться в отдельном файле.

Чтобы создать правило экспорта параметров устройства:

1. В разделе **Настройки → UserGate → Управление устройством → Экспорт и импорт настроек** нажмите **Добавить**.

2. На вкладке **Общие** укажите имя правила.

3. На вкладке **Удаленный сервер** укажите параметры удаленного сервера:

- тип — FTP или SSH;
- адрес;
- порт для подключения;
- логин и пароль учетной записи;
- путь к существующей папке для сохранения файлов экспорта.

Примечание Для авторизации на удаленном SSH-сервере вы можете использовать SSH-ключи. Для этого их нужно [предварительно](#)

[настроить](#).

Внимание!Если вы создаете правило для SSH-сервера с авторизацией по SSH-ключам, вам необходимо проверить соединение с этим сервером по кнопке «Проверить соединение». Во время проверки устанавливается первичное соединение, при котором отпечаток открытого ключа автоматически добавляется на удаленный сервер. Это обеспечивает безопасность последующих соединений.

4. На вкладке **Расписание** укажите время экспорта параметров.

Вы можете выбрать одно из предустановленных значений или указать время вручную в cron-формате: <минуты: 0—59> <часы: 0—23> <дни месяца: 1—31> <месяцы: 1—12> <дни недели: 0—6, где 0 — воскресенье>.

При ручном вводе также можно использовать следующие символы:

- Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что резервное копирование должно выполняться каждый час.
- Дефис (-) — для указания диапазона значений.
- Запятая (,) — в качестве разделителя значений.
- Косая черта (/) — для указания шага между значениями.

5. Нажмите **Сохранить**.

Вы можете восстанавливать параметры устройства из файлов экспорта. Эти файлы не содержат данные о кластерах и лицензии, поэтому после восстановления параметров вам потребуется повторно активировать лицензию и настроить кластеры. Кроме того, если для входа в UserGate SIEM вы используете многофакторную аутентификацию через TOTP, после восстановления необходимо повторно добавить ключи инициализации.

Чтобы восстановить параметры устройства из файла экспорта:

1. В разделе **Настройки → UserGate → Управление устройством → Экспорт и импорт настроек** нажмите **Импорт**.
2. Выберите файл экспорта.
3. В окне **Импортировать настройки** выберите тип импорта (все параметры или только сетевые).
4. Нажмите **Старт**.

Начнется восстановление параметров. По окончании процесса сервер UserGate SIEM будет перезагружен.

Администраторы

Version: 7.x
Product: SIEM
Documentation: ☒

Доступ к веб-консоли UserGate 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 UserGate 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 помощью разрешения 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.		+	+	

Рольовое разрешение	Описание	Administrator	Supervisor	Investigator	Analyst
Удаление собственных срабатываний, журналов к инцидентам	Возможность удалять собственные срабатывания/журналы к инцидентам.		+	+	+
Создание схемы инцидента	Возможность создавать схемы инцидентов.		+		
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.		+		

Ролевое разрешение	Описание	Administrator	Supervisor	Investigator	Analyst
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.	+	+		
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.	+	+		

Ролевое разрешение	Описание	Administrator	Supervisor	Investigator	Analyst
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.	+	+		
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.	+	+		

Рольовое разрешение	Описание	Administrator	Supervisor	Investigator	Analyst
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 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 UserGate 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).

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

Version: 7.x
Product: SIEM
Documentation: ☒

UserGate SIEM использует защищенный протокол HTTPS для управления устройством. Для выполнения данной функции UserGate SIEM 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 UserGate SIEM. Для этого необходимо выделить необходимый сертификат в списке сертификатов, нажать на кнопку Редактировать и указать тип сертификата — SSL веб-консоли . После этого UserGate SIEM перезагрузит сервис веб-консоли и предложит вам подключиться уже с использованием нового сертификата.

UserGate 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 UserGate 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.x
Product: SIEM
Documentation: ☒

Серверы аутентификации — это внешние источники учетных записей пользователей для авторизации в веб-консоли управления UserGate SIEM. Устройство 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 UserGate 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

Documentation: ☒
Version: 7.x
Product: SIEM

Профиль позволяет определить набор способов авторизации пользователей в консоли администрирования UserGate SIEM. 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.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 SIEM 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

Version: 7.x

Product: SIEM

Documentation: ☒

В разделе **Каталоги пользователей** можно добавить LDAP-коннектор для организации доступа серверов UserGate 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.x
Product: SIEM
Documentation: ☒

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

Наименование	Описание
Шаг 1. Добавить дополнительный виртуальный диск.	Средствами гипервизора добавить новый диск необходимого размера в свойствах виртуальной машины UserGate SIEM.
Шаг 2. Расширить размер раздела в системных утилитах.	В меню загрузки узла UserGate SIEM 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.

Technology: Clustering and HA

Version: 7.x

Product: SIEM

Documentation: 

Общие принципы

Для построения отказоустойчивого решения UserGate SIEM необходимо настроить два типа кластеров — кластер конфигурации и кластер отказоустойчивости.

Кластер конфигурации — это объединение нескольких узлов в одну общую схему. Входящие в кластер конфигурации узлы «видят» друг друга и синхронизируют свою конфигурацию. При этом часть настроек для каждого из узлов кластера уникальна, например, настройки сетевых интерфейсов, шлюзов, маршрутов, настройки диагностики.

Кластер отказоустойчивости обеспечивает работу сетевых операций на узлах, входящих в кластер конфигурации, например, переключаемый виртуальный IP, который по определённым правилам мигрирует с одного узла на другой.

Кластер отказоустойчивости и кластер конфигурации работают на разных протоколах и в разных окружениях. При этом информация о статусе кластера отказоустойчивости распространяется между узлами через кластер конфигурации. Речь идёт именно об информации о статусе, а не о данных, которыми кластер отказоустойчивости поддерживает свою работу. Статус узлов кластера отображается в веб-консоли.

Минимальный состав отказоустойчивого решения UserGate SIEM состоит из двух узлов UserGate SIEM и узла-арбитра.

Максимальное количество узлов в кластере — 4, один из которых является арбитром.

Узел-арбитр предназначен для определения кворума в конфигурации для обеспечения консистентности данных. Он не несёт в себе функции полноценного UserGate SIEM (сбор, хранение, обработка данных), но участвует в процедуре определения большинства согласно алгоритму распределённого консенсуса для согласования операций в отказоустойчивом кластере.

На данном этапе отказоустойчивым кластером UserGate SIEM поддерживается режим работы **Актив-Пассив**. В режиме Актив-Пассив один из узлов выступает в роли мастер-узла, обрабатывающего трафик, а другой — в качестве резервного. Для кластера указывается один или более виртуальных IP-адресов. Переключение виртуальных адресов с главного на один из запасных узлов происходит при следующих событиях:

- Запасной узел не получает подтверждения о том, что главный узел в сети, например, если он выключен или отсутствует сетевая доступность узлов.
- Изменение приоритета мастер-узла. Например, приоритет мастер-узла уменьшается при отключении одного или нескольких сетевых интерфейсов, на которых назначены виртуальные IP-адреса. Также приоритет узла может быть изменен явным образом через смену мастера в веб-консоли устройства.
- Сбой в работе ПО.

Создание отказоустойчивого кластера UserGate SIEM

Для создания отказоустойчивого кластера UserGate SIEM необходимо сначала настроить кластер конфигурации, объединив в него необходимые узлы, затем настроить кластер отказоустойчивости.

Настройка кластера конфигурации

Для создания кластера конфигурации необходимо выполнить следующие шаги:

1. Выполнить первоначальную настройку на первом узле. Подробнее читайте в главе [Первоначальная настройка](#).

2. Настроить на первом узле зону, через интерфейсы которой будет выполняться репликация кластера.

В разделе **Зоны** создать выделенную зону для репликации настроек кластера. В настройках доступа зоны разрешить следующие сервисы:

- Консоль администрирования
- Кластер

Важно! Не следует использовать для репликации зоны, интерфейсы которых подключены к недоверенным сетям, например, к интернету.

3. В разделе **Кластер конфигурации** указать IP-адрес, который будет использоваться для связи с другими узлами кластера.

4. Сгенерировать секретный код на первом узле, нажав одноимённую кнопку в разделе **Кластер конфигурации**. Полученный код скопировать в буфер обмена. Данный секретный код необходим для одноразовой авторизации следующего узла при добавлении его в кластер.

5. Подключить второй узел в кластер.

В процессе первоначальной установки второго узла подключиться к его веб-консоли, выбрать язык установки.

Указать интерфейс, который будет использован для подключения к первому узлу кластера и назначить ему IP-адрес. Оба узла кластера должны находиться в одной подсети. В противном случае необходимо указать IP-адрес шлюза, через который будет доступен первый узел кластера.

Указать IP-адрес первого узла, настроенный на шаге 3, вставить секретный код и нажать на кнопку **Подключить**:

Если IP-адреса кластера, настроенные на шаге 2, назначены корректно, то второй узел будет добавлен в кластер и настройки первого узла кластера реплицируются на второй.

Состояние узлов кластера конфигурации отображается в разделе **Кластер конфигурации**:

6. Назначить зоны интерфейсам второго узла. В веб-консоли второго узла кластера в разделе **Сеть → Интерфейсы** необходимо назначить каждому интерфейсу корректную зону. Зоны и их настройки получены в результате репликации данных с первого узла кластера.

7. Подключить в кластер узел, который будет в дальнейшем исполнять роль арбитра.

Сгенерировать секретный код на первом узле, нажав одноимённую кнопку в разделе **Кластер конфигурации**. Полученный код скопировать в буфер обмена. Данный код необходим для одноразовой авторизации нового узла при добавлении его в кластер.

В процессе первоначальной установки третьего узла подключиться к его веб-консоли, выбрать язык установки.

Указать интерфейс, который будет использован для подключения к первому узлу кластера и назначить ему IP-адрес. Оба узла кластера должны находиться в одной подсети. В противном случае необходимо указать IP-адрес шлюза, через который будет доступен первый узел кластера. Поставить флажок **Перевести ноду в режим арбитра**.

Указать IP-адрес первого узла, настроенный на шаге 3, вставить секретный код и нажать на кнопку **Подключить**:

Если IP-адреса кластера, настроенные на шаге 2, назначены корректно, то второй узел будет добавлен в кластер и настройки первого узла кластера реплицируются на новый узел.

Состояние узлов кластера конфигурации отображается в разделе **Кластер конфигурации**. Узел-арбитр помечается в списке узлов кластера соответствующей иконкой:

8. Настроить параметры, индивидуальные для каждого узла кластера (опционально). Настроить шлюзы, маршруты, параметры OSPF, BGP, индивидуальные для каждого из узлов.

Настройка кластера отказоустойчивости

Узлы кластера конфигурации можно объединить в отказоустойчивый кластер. В настоящий момент поддерживается режим кластера отказоустойчивости **Актив-Пассив**.

В режиме Актив-Пассив один из узлов UserGate SIEM выступает в роли мастер-узла, принимающего трафик, а другой — в качестве резервного. На каждом из узлов кластера выбираются сетевые интерфейсы, у которых обязательно должны быть определены IP-адреса.

Администратор назначает виртуальные IP-адреса. Между этими интерфейсами передаются VRRP-объявления (ADVERTISEMENT) — сообщения, с помощью которых узлы обмениваются информацией о своём состоянии.

Для создания кластера отказоустойчивости необходимо в разделе **Кластеры отказоустойчивости** нажать иконку "+" :

В открывшемся окне свойств кластера отказоустойчивости произвести следующие настройки:

На вкладке **Общие**:

- Указать название кластера отказоустойчивости.
- Задать значение идентификатора виртуального маршрутизатора. VRID должен быть уникален для каждого VRRP-кластера в локальной сети.
- Поставить флажок **Включено** для активации кластера.

На вкладке **Узлы** выбрать узлы кластера конфигурации, которые войдут в создаваемый кластер отказоустойчивости.

На вкладке **Виртуальные IP** указать виртуальный IP-адрес и маску сети кластера отказоустойчивости, выбрать основные узлы и порты, на которых будет работать VRRP.

Отображение состояния кластера отказоустойчивости

Состояние и роль входящих в кластер узлов можно увидеть в разделе **Кластеры отказоустойчивости**. Роли узлов отмечены соответствующими иконками: звёздочкой отмечен активный мастер-узел, свистком — узел-арбитр.

При успешном создании кластера его состояние отображается следующим образом:

В случае недоступности мастер-узла кластера его роль перейдёт к резервному узлу. В веб-консоли второго узла поменяется статус состояния кластера и недоступного узла. При наведении на иконку статуса кластера указателя мыши отображается подсказка о причине изменения состояния кластера:

В журнале событий отобразится соответствующая запись:

В случае неконсистентного состояния кластера отказоустойчивости его статус помечается соответствующей иконкой. При наведении на иконку указателя мыши отображается подсказка о причине данного состояния кластера:

