

Table of Contents

Table of Contents	1
Настройка UGMC	2
Настройка общих параметров	3
Управление устройством	5
Администраторы	13
Сертификаты	17
Серверы аутентификации	19
Профили аутентификации	21
Библиотеки элементов	22
Расширение системного раздела	27
Обновление ПО кластера UserGate MC	28

Настройка общих параметров

Version: 7.x

Product: UGMC

Documentation: 

В этом разделе описаны общие параметры UserGate Management Center (UGMC), которые отображаются на странице веб-интерфейса **Центр управления** в разделе **Консоль администратора → Настройки**, 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 даты и времени, например в отчетах или в журналах
	Язык интерфейса по умолчанию	Язык, используемый в веб-интерфейсе продукта по умолчанию
	Таймер автоматического закрытия сессии (мин.)	Для настройки таймера необходимо указать, по истечении скольких минут бездействия администратора в веб-интерфейсе должна завершаться его сессия. Также необходимо включить параметр Автоматическое закрытие сессии по таймеру
	Автоматическое закрытие сессии по таймеру (параметр доступен начиная с версии 7.5.0)	При включенном параметре сессия администратора будет завершаться по истечении таймера автоматического закрытия сессии. По умолчанию параметр отключен
Настройка времени сервера	Использовать NTP	При включенном параметре для синхронизации времени в продукте будут использоваться серверы NTP из указанного списка
	Основной NTP-сервер	Адрес основного сервера точного времени. Значение по умолчанию — pool.ntp.org
	Запасной NTP-сервер	Адрес запасного сервера точного времени
	Время на сервере (UTC)	Время на сервере UGMC 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)
	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 продукта. Это позволит восстановить предыдущую версию UGOS при возникновении проблем. Действие будет доступно в стартовом меню продукта 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 соп-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-интерфейсе продукта необходимо включить параметр и добавить типы изменений (например, распоряжение, приказ или регламентные работы). Учет изменений предполагает, что при внесении какого-либо изменения через веб-интерфейс администратору необходимо указать тип и причину этого изменения
Системные DNS-серверы		Для настройки DNS-серверов необходимо указать их IP-адреса

Documentation: ☒
Version: 7.x
Product: UGMC

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

- Кластеризация.
- Настройки диагностики.
- Операции с сервером.
- Резервное копирование.
- Экспорт и импорт настроек.

Кластеризация и отказоустойчивость

UGMC поддерживает 2 типа кластеров:

1. **Кластер конфигурации.** Узлы, объединенные в кластер конфигурации, поддерживают единые настройки в рамках кластера.
2. **Кластер отказоустойчивости.** До 4-х узлов кластера конфигурации могут быть объединены в кластер отказоустойчивости, поддерживающий работу в режиме Актив-Актив или Актив-Пассив.

ПримечаниеПри внедрении UGMC в режиме отказоустойчивости необходимо выполнить как настройки кластера конфигурации, так и настройки кластера отказоустойчивости.

Ряд настроек уникален для каждого из узлов кластера, например, настройка сетевых интерфейсов и IP-адресация. Список уникальных настроек:

Наименование	Описание
Настройки, уникальные для каждого узла	Настройки диагностики Настройки интерфейсов Настройки шлюзов Маршруты

Для создания кластера конфигурации необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Выполнить первоначальную настройку на первом узле кластера.	Смотрите главу Первоначальная настройка .
Шаг 2. Настроить на первом узле кластера зону, через интерфейсы которой будет выполняться репликация кластера.	В разделе Зоны создать выделенную зону для репликации настроек кластера. В настройках зоны разрешить следующие сервисы: • Консоль администрирования. • Кластер. Не используйте для репликации зоны, интерфейсы которых подключены к недоверенным сетям, например, к интернету.
Шаг 3. Указать IP-адрес, который будет использоваться для связи с другими узлами кластера.	В разделе Управление устройством в окне Кластер конфигурации выбрать текущий узел кластера и нажать на кнопку Редактировать . Указать IP-адрес интерфейса, входящего в зону, настроенную на шаге 2.
Шаг 4. Сгенерировать Секретный код на первом узле кластера.	В разделе Управление устройством нажать на кнопку Сгенерировать секретный код . Полученный код скопировать в буфер обмена. Данный секретный код необходим для одноразовой авторизации второго узла при добавлении его в кластер.

Наименование	Описание
Шаг 5. Подключить второй узел в кластер.	Второй и последующие узлы подключаются в кластер на моменте первоначальной инициализации. Если инициализация уже была проведена, то необходимо перезагрузить устройство и выполнить возврат к заводским установкам (Factory reset). Подключиться к веб-консоли второго узла кластера, 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, например, интерфейсам port2 обоих узлов назначены IP-адреса 192.168.100.5/24 и 192.168.100.6/24. 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 все настройки первого узла кластера реплицируются на второй.
Шаг 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.
Шаг 7. Настроить параметры, индивидуальные для каждого узла кластера (опционально).	Настроить шлюзы, маршруты и другие настройки, индивидуальные для каждого из узлов.

До четырех узлов кластера конфигурации можно объединить в отказоустойчивый кластер. Самых кластеров отказоустойчивости может быть несколько. Поддерживаются 2 режима — **Актив-Актив** и **Актив-Пассив**.

В режиме **Актив-Пассив** один из серверов выступает в роли Мастер-узла, обрабатывающего трафик, а остальные — в качестве резервных. Для кластера указывается один или более виртуальных IP-адресов. Переключение виртуальных адресов с главного на один из запасных узлов происходит при следующих событиях:

- Запасной сервер не получает подтверждения о том, что главный узел в сети, например, если он выключен или отсутствует сетевая доступность узлов.
- На главном узле настроена проверка доступа в интернет.
- Сбой в работе ПО UserGate.

Ниже представлен пример сетевой диаграммы отказоустойчивого кластера в режиме **Актив-Пассив**. Интерфейсы настроены следующим образом:

- **Зона Trusted:** IP1, IP2, IP3, IP4 и IP cluster (Trusted).
- **Зона Management:** интерфейсы в зоне Management используются для управления узлами UGMC.

Кластерный IP-адрес находится на узле UGMC 1. Если узел UGMC 1 становится недоступным, то кластерный IP-адрес перейдет на следующий сервер, который станет мастер-сервером, например, UGMC 2.

В режиме **Актив-Актив** один из серверов выступает в роли Мастер-узла, распределяющего трафик на все остальные узлы кластера. Поскольку IP-адрес кластера находится на Мастер-узле, то Мастер-узел отвечает на ARP-запросы клиентов. Выдавая последовательно MAC-адреса всех узлов отказоустойчивого кластера, Мастер-узел обеспечивает равномерное распределение трафика на все узлы кластера, учитывая при этом необходимость неразрывности пользовательских сессий. Для кластера указывается один или более виртуальных IP-адресов. Перемещение роли Мастер-узла на один из запасных узлов происходит при следующих событиях:

- Запасной сервер не получает подтверждения о том, что главный узел в сети, например, если он выключен или отсутствует сетевая доступность узлов.
- На главном узле настроена проверка доступа в интернет.
- Сбой в работе ПО UserGate.

Ниже представлен пример сетевой диаграммы отказоустойчивого кластера в режиме **Актив-Актив**. Интерфейсы настроены следующим образом:

- Зона **Trusted**: IP1, IP2, IP3, IP4 и IP cluster (Trusted).
- Зона **Management**: интерфейсы в зоне Management используются для управления узлами UGMC.

Кластерный IP-адрес находится на узле UGMC 1, который является мастер-узлом. При этом трафик распределяется на все узлы кластера. Если узел UGMC 1 становится недоступным, то роль мастера и кластерный IP-адрес перейдет на следующий сервер, например, UGMC 2.

Для создания отказоустойчивого кластера необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать кластер конфигурации.	Создать кластер конфигурации, как это описано на предыдущем шаге.
Шаг 2. Настроить зоны, интерфейсы которых будут участвовать в отказоустойчивом кластере.	В разделе Зоны следует разрешить сервис VRRP для всех зон, где планируется добавлять кластерный виртуальный IP-адрес (зона Trusted на диаграммах выше).
Шаг 3. Создать кластер отказоустойчивости.	В разделе Управление устройством → Кластер отказоустойчивости нажать на кнопку Добавить и указать параметры кластера отказоустойчивости.

Параметры отказоустойчивого кластера:

Наименование	Описание
Включено	Включение/отключение отказоустойчивого кластера.
Название	Название отказоустойчивого кластера.

Наименование	Описание
Описание	Описание отказоустойчивого кластера.
Режим кластера	Режим отказоустойчивого кластера: • Актив-Актив — нагрузка распределяется на все узлы кластера. • Актив-Пассив — нагрузка идет на Мастер-узел и переключается на запасной узел в случае недоступности Мастер-узла.
Мультикаст идентификатор кластера	В одном кластере конфигурации может быть создано несколько кластеров отказоустойчивости. Для синхронизации сессий используется определенный мультикастовый адрес, определяемый данным параметром. Для каждой группы кластеров отказоустойчивости, в которой должна поддерживаться синхронизация сессий, требуется установить уникальный идентификатор.
Идентификатор виртуального роутера (VRID)	Идентификатор виртуального роутера должен быть уникален для каждого VRRP-кластера в локальной сети. Если в сети не присутствуют сторонние кластеры VRRP, то рекомендуется оставить значение по умолчанию.
Узлы	Выбираются узлы кластера конфигурации для объединения их в кластер отказоустойчивости. Здесь же можно назначить роль Мастер-сервера одному из выбранных узлов.
Виртуальные IP-адреса	Назначаются виртуальные IP-адреса и их соответствие интерфейсам узлов кластера.

Диагностика

Этот блок предназначен для настройки параметров диагностики и предоставления удаленного доступа службе технической поддержки UserGate с целью анализа и устранения неисправностей.

Параметры диагностики

С помощью параметра **Детализация диагностики** вы можете установить уровень журналирования устройства. Доступны следующие уровни:

- **Off** — ведение журналов диагностики отключено.
- **Error** — журналировать только ошибки в работе устройства.
- **Warning** — журналировать только ошибки и предупреждения.
- **Info** — журналировать только ошибки, предупреждения и дополнительную информацию.
- **Debug** — журналировать все возможные события.

При журналировании с уровнями **Warning**, **Info** и **Debug** может снижаться производительность устройства, поэтому рекомендуется устанавливать уровни **Error** или **Off**, если технической поддержкой UserGate не было предложено иное.

Управление журналами

Вы можете скачать диагностические журналы для их передачи в службу технической поддержки UserGate. Для скачивания доступны журналы веб-консоли и системные журналы. Скачать выбранные журналы можно после их архивирования командой **Начать архивирование журналов**.

Чтобы удалить архивные (не активные в настоящий момент) журналы, нажмите **Очистить файлы логов**.

Удаленный помощник

Чтобы предоставить доступ к устройству для службы технической поддержки UserGate с целью диагностирования и устранения неисправностей, необходимо активировать функцию удаленного помощника и получить параметры сеансового доступа.

Процесс подключения к устройству происходит следующим образом:

1. Администратор устройства UserGate активирует функцию удаленного помощника.
2. Устройство устанавливает защищенное соединение с сервером удаленного помощника UserGate по протоколу SSH. При успешном подключении в интерфейсе устройства UserGate отобразятся параметры сеансового доступа: идентификатор и токен.
3. Администратор устройства UserGate передает параметры сеансового доступа специалисту технической поддержки UserGate.
4. Специалист технической поддержки устанавливает защищенное соединение по протоколу SSH с сервером удаленного помощника UserGate и с помощью параметров сеансового доступа подключается к устройству UserGate.

Операции с сервером

Данный раздел позволяет произвести следующие операции с сервером:

Наименование	Описание
Операции с сервером	• Перезагрузить — перезагрузка сервера UGMC. • Выключить — выключение сервера UGMC.
Обновления	Выбор канала обновлений ПО UGMC • Стабильные — проверка наличия стабильных обновлений ПО. • Бета — проверка наличия экспериментальных обновлений.
Обновления сервера	Индикация имеющихся обновлений UGMC. Запуск процесса обновления сервера с возможностью создания точки восстановления. Просмотр списка изменений ПО в обновлении.
Офлайн обновления	Загрузка файла для офлайн обновления.
Настройки вышестоящего прокси для проверки лицензий и обновлений	Настройка параметров вышестоящего HTTP(S) прокси-сервера для обновления лицензии и обновления ПО UGMC. Необходимо указать IP-адрес и порт вышестоящего прокси сервера. При необходимости указать логин и пароль для аутентификации на вышестоящем прокси-сервере.

Компания UserGate постоянно работает над улучшением качества своего программного обеспечения и предлагает обновления продукта UGMC в рамках подписки на модуль лицензии Security Update (подробно о лицензировании смотрите в разделе [Лицензирование UGMC](#)). 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 UGMC.

Для установки обновлений необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл резервного копирования.	Создать резервную копию состояния UGMC в разделе Управление устройством → Управление резервным копированием → Создание резервной копии . 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 UGMC будет перезагружен.

Управление резервным копированием

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

Для создания резервной копии необходимо выполнить следующие действия:

Наименование	Описание

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 known_hosts, без проверки файлы не будут отправляться. Важно! Если сменить сервер SSH или его переустановить, то файлы резервного копирования будут недоступны, так как fingerprint изменится — это защита от спуфинга.

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 UGMC в файл и впоследствии восстановить эти настройки на этом же или другом сервере UGMC. 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 настроить интерфейсы и повторно зарегистрировать UGMC с помощью имеющегося ПИН-кода.

Для экспорта настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Экспорт настроек.	В разделе Управление устройством → Экспорт и импорт настроек нажать на ссылку Экспорт и выбрать Экспортировать все настройки или Экспортировать сетевые настройки. Система сохранит: - текущие настройки сервера под именем: cc_core-mc_core@nodename_version_YYYYMMDD_HHMMSS.bin - сетевые настройки под именем: network-cc_core-mc_core@nodename_version_YYYYMMDD_HHMMSS.bin nodename — имя узла UserGate Management Center. version — версия UserGate Management Center. YYYYMMDD_HHMMSS — дата и время выгрузки настроек в часовом поясе UTC. Например, cc_core-mc_core@ediasaionedi_7.0.0.93R-1_20220715_084853.bin или network-cc_core-mc_core@ediasaionedi_7.0.0.93R-1_20220715_084929.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 на ссылку Импорт и указать путь к ранее созданному файлу настроек. Указанные настройки применятся к серверу, после чего сервер будет перезагружен

ПримечаниеДля корректного импорта правил, использующих обновляемые списки UserGate (приложения, категории URL и т.п.), необходимо наличие лицензии на модули SU и ATP, а также загруженных списков UserGate.

Подробнее об особенностях импорта настроек кластерного решения читайте в статье [Обновление ПО кластера UGMC](#).

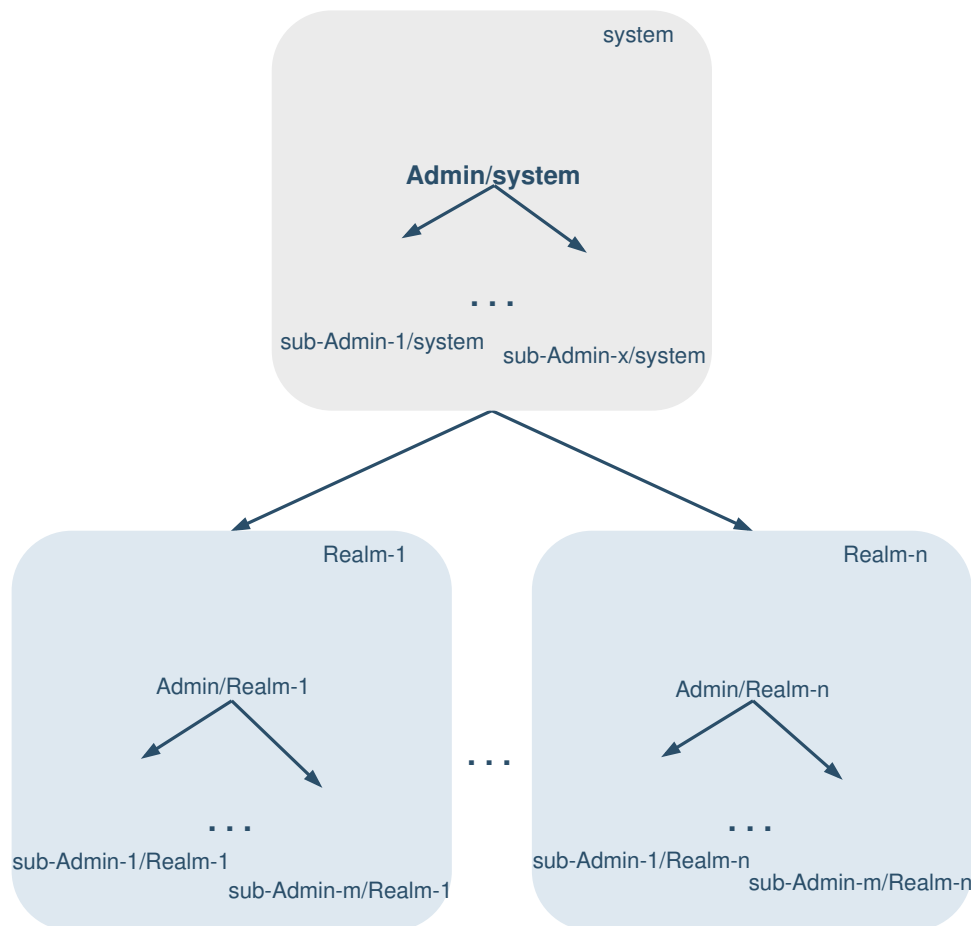
Дополнительно администратор может настроить сохранение настроек на внешние серверы (FTP, SSH) по расписанию. Для создания расписания выгрузки настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать правило экспорта.	В разделе Управление устройством → Экспорт 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/Подтверждение пароля — 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".

Иерархическая система учетных записей администраторов

В UGMC реализована иерархическая система учетных записей администраторов. Верхний уровень (system) образуют учетные записи администраторов самой системы UGMC. Нижний уровень образуют учетные записи администраторов управляемых областей (Realm) — логических объектов, предназначенных для управления группой подконтрольных устройств (подробнее об управляемых областях — в разделе «[Управление областями](#)»).



При первоначальной настройке UGMC создается локальный администратор с логином `Admin/system`, который является корневым администратором системы. Администратор UGMC может управлять общими и сетевыми параметрами UGMC, активировать лицензии UGMC, создавать и редактировать элементы системной библиотеки, управлять политиками обновления и резервного копирования, мониторить работу UGMC по системным журналам. Администратор UGMC может создавать дополнительные учетные записи субадминистраторов UGMC, делегируя им часть прав по управлению системой.

Администратор UGMC также создает управляемые области (Realm), но при этом не обладает полномочиями на управление устройствами, входящими в эти области. Для этого администратор UGMC создает учетные записи корневых администраторов управляемых областей (Admin/Realm). Корневой администратор области имеет все права на управление областью и относящимися к ней устройствами. Он может создавать серверы и профили аутентификации области, каталоги пользователей, шаблоны параметров управляемых устройств, объединять шаблоны в группы и подключать к ним объекты управляемых устройств. Корневой администратор управляемой области может также создавать учетные записи субадминистраторов (региональных администраторов) своей области (sub-Admin/Realm), делегируя им права на администрирование только отдельных выделенных устройств.

Управление учетными записями администраторов

Чтобы добавить администратора:

1. Создайте профиль администратора. Профиль определяет список полномочий администратора. Можно создавать несколько профилей с разными полномочиями. Также можно создать профиль корневого администратора области.
2. Создайте учетную запись администратора. На этом этапе можно выбрать способ авторизации администратора: локальный, через LDAP-коннектор или с помощью профиля аутентификации.

Создание профиля администратора

Чтобы создать профиль администратора UGMC:

1. В веб-консоли управления UGMC в разделе **Центр управления → Администраторы** в блоке **Профили администраторов** нажмите

Добавить.

2. В окне **Настройка профиля** на вкладке **Общие** укажите название профиля.
3. Выберите тип администратора **Администратор UserGate Management Center**.
4. На вкладке **Права доступа** выберите, какими правами доступа будет обладать администратор с этим профилем. В качестве разрешений для доступа можно указать **Нет доступа**, **Чтение** или **Чтение и запись**.
5. Сохраните изменения.

Чтобы создать профиль корневого администратора области:

1. Убедитесь, что в системе создана нужная область. Подробнее об областях — в разделе « [Создание управляемых областей](#) ».
2. В веб-консоли управления UGMC в разделе **Центр управления → Администраторы** в блоке **Профиль администраторов** нажмите **Добавить**.
2. В окне **Настройка профиля** на вкладке **Общие** укажите название профиля.
3. Выберите тип администратора **Администратор области** и ранее настроенную управляемую область.
4. Сохраните изменения.

Корневые администраторы областей обладают всеми правами в рамках своей области. В режиме управления областью они могут создавать учетные записи субадминистраторов области и управлять их правами доступа.

Создание учетной записи локального администратора

Чтобы создать учетную запись локального администратора:

1. В веб-консоли управления UGMC в разделе **Центр управления → Администраторы** в блоке **Администраторы** нажмите **Добавить** и выберите **Добавить локального администратора**.
2. В окне **Свойства администратора** укажите имя, логин и пароль администратора.
3. Выберите созданный ранее профиль администратора.
4. Установите флажок **Включено**, чтобы разрешить вход в систему под этой учетной записью.
5. Сохраните изменения.

Важно! Для корневого администратора области можно создать только учетную запись локального администратора. Это связано с тем, что LDAP-серверы, используемые для аутентификации администраторов сервиса UGMC и для аутентификации администраторов области, могут быть разными. Если для управления областью требуется использовать LDAP-администраторов, их необходимо создать в веб-интерфейсе самой области. Более подробно об администраторах области — в разделе « [Администраторы области](#) ».

Создание учетной записи LDAP-администратора

Чтобы создать учетную запись пользователя из существующего домена:

1. Убедитесь, что в разделе **Серверы аутентификации** предварительно настроен соответствующий LDAP-коннектор. Подробнее о настройке LDAP-коннектора — в разделе « [Серверы аутентификации](#) ».
2. В веб-консоли управления UGMC в разделе **Центр управления → Администраторы** в блоке **Администраторы** нажмите **Добавить** и выберите **Добавить пользователя LDAP**.
3. В окне **Свойства LDAP-администратора** нажмите кнопку **Выбрать**, выберите настроенный LDAP-коннектор и затем добавьте логин нужного пользователя.
4. Выберите созданный ранее профиль администратора.
5. Установите флажок **Включено**, чтобы разрешить вход в систему под этой учетной записью.
6. Сохраните изменения.

При входе в веб-интерфейс администрирования под этой учетной записью необходимо указывать логин в формате <логин>@<домен>/system или <домен>\<логин>/system.

Чтобы добавить учетную запись для группы пользователей из существующего домена:

1. Убедитесь, что в разделе **Серверы аутентификации** предварительно настроен соответствующий LDAP-коннектор. Подробнее о настройке LDAP-коннектора — в разделе « [Серверы аутентификации](#) ».
2. В веб-консоли управления UGMC в разделе **Центр управления → Администраторы** в блоке **Администраторы** нажмите **Добавить** и выберите **Добавить группу LDAP**.
3. В окне **Свойства LDAP-администратора** нажмите кнопку **Выбрать**, выберите настроенный LDAP-коннектор и затем добавьте логин группы пользователей.
4. Выберите созданный ранее профиль администратора.
5. Установите флажок **Включено**, чтобы разрешить вход в систему под этой учетной записью.
6. Сохраните изменения.

При входе в веб-интерфейс администрирования под этой учетной записью необходимо указывать логин в формате <логин>@<домен>/system или <домен>\<логин>/system.

Создание учетной записи администратора с профилем аутентификации

Вы можете управлять доступом администраторов в веб-консоль управления UGMC с помощью профиля аутентификации, в котором в списке доступных методов аутентификации указаны заранее настроенные серверы, такие как LDAP, TACACS+ или RADIUS. Если в профиле аутентификации указано сразу несколько методов аутентификации, будут перебираться все методы по очереди до первого сработавшего.

Чтобы добавить учетную запись администратора с профилем аутентификации:

1. Убедитесь, что в разделе **Серверы аутентификации** добавлены данные о настроенном сервере аутентификации. Подробнее о сервере аутентификации — в разделе «[Серверы аутентификации](#)».
2. Убедитесь, что в разделе **Профили аутентификации** создан профиль с нужным методом аутентификации. Подробнее о создании профиля — в разделе «[Профили аутентификации](#)».
3. В веб-консоли управления UGMC в разделе **Центр управления → Администраторы** в блоке **Администраторы** нажмите **Добавить** и выберите **Добавить администратора с профилем аутентификации**.
4. В окне **Свойства администратора с профилем аутентификации** укажите имя, логин и пароль администратора.
5. Выберите созданный ранее профиль администратора.
6. Выберите созданный ранее профиль аутентификации.
7. Установите флажок **Включено**, чтобы разрешить вход в систему под этой учетной записью.
8. Сохраните изменения.

Дополнительные параметры защиты учетных записей администраторов

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

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.

Чтобы настроить дополнительные параметры защиты:

1. В разделе **Центр управления → Администраторы** в блоке **Администраторы** нажмите **Настроить**.
2. Настройте нужные параметры:
 - **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.

3. Сохраните изменения.

Сессии администраторов

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

Сертификаты

Version: 7.x
Product: UGMC
Documentation: ☒

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

UGMC 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. • Экспорт CSR — экспортирует CSR сертификата, например, для подписи его удостоверяющим центром.

ПримечаниеРекомендуется сохранять сертификат для возможности его последующего восстановления.

ПримечаниеВ целях безопасности UGMC 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. • Загрузите файл, содержащий данные сертификата. • Загрузите 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.

Version: 7.x

Product: UGMC

Documentation: 

Серверы аутентификации — это внешние источники учетных записей пользователей, которые можно использовать для авторизации в веб-консоли управления UGMC. UGMC 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.
- Выполнять авторизацию администраторов UGMC через домены Active Directory и FreeIPA.

Чтобы добавить LDAP-коннектор:

1. На странице **Центр управления** в разделе **Центр управления → Серверы аутентификации** нажмите **Добавить** и выберите **Добавить LDAP-коннектор**.
2. В окне **Свойства коннектора LDAP** укажите название LDAP-коннектора.
3. В поле **Доменное имя LDAP или IP-адрес** укажите IP-адрес контроллера домена, FQDN контроллера домена или FQDN домена (например, test.local). Если указан FQDN контроллера домена, то UserGate получит адрес контроллера домена с помощью DNS-запроса. Если указан FQDN домена, то при отключении основного контроллера домена UserGate будет использовать резервный контроллер.
4. В поле **Привязать DN (логин)** укажите логин, который необходимо использовать для подключения к серверу LDAP. Логин необходимо указать в формате <домен>\<логин> или <логин>@<домен>. Этот пользователь уже должен быть создан в домене.
5. Укажите пароль пользователя для подключения к домену.
6. Если необходимо, на вкладке **Домены LDAP** добавьте домены, которые обслуживаются указанным контроллером домена. Например, если используется дерево доменов или лес доменов Active Directory. Здесь же можно указать короткое netbios-имя домена.
7. На вкладке **Пути поиска** укажите пути, начиная с которых система будет осуществлять поиск пользователей и групп. Необходимо указывать полное имя, например ou=Office,dc=example,dc=com.
8. Если необходимо, на вкладке **Настройки** установите флажок **Использовать для соединений SSL**, чтобы использовать SSL-соединение для подключения к LDAP-серверу.
9. Установите флажок **Включено**, чтобы начать использовать LDAP-коннектор, и сохраните изменения.

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 веб-консоль управления UGMC пользователям LDAP необходимо указывать логин в формате <домен>\<логин>/system или <логин>@<домен>/system.

Сервер аутентификации RADIUS

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

Важно! Перед выполнением описанных ниже шагов убедитесь, что RADIUS-сервер настроен для работы с UGMC (в раздел «RADIUS Clients and Servers» добавлена запись с IP-адресом UGMC). В противном случае сервер не будет отвечать на запросы. Пример настройки RADIUS-сервера — в разделе «[Авторизация с помощью RADIUS](#)».

Чтобы добавить RADIUS-сервер:

1. На странице **Центр управления** в разделе **Центр управления → Серверы аутентификации** нажмите **Добавить** и выберите **Добавить RADIUS-сервер**.
2. В окне **Свойства RADIUS-сервера коннектора** укажите название RADIUS-сервера.
3. Добавьте IP-адрес RADIUS-сервера и UDP-порт, на котором RADIUS-сервис слушает запросы на аутентификацию (по умолчанию — 1812).
4. В поле **Секрет** введите пароль, указанный при настройке RADIUS-сервера.
5. Установите флажок **Включено**, чтобы начать использовать RADIUS-сервер, и сохраните изменения.

Для авторизации пользователей в веб-консоли управления UGMC с помощью RADIUS-сервера необходимо настроить профиль аутентификации. Подробнее о создании и настройке профилей — в разделе «[Профили аутентификации](#)».

Сервер аутентификации TACACS+

Сервер TACACS+ позволяет производить авторизацию пользователей в веб-консоли управления UGMC. При использовании сервера TACACS+ UserGate MC передает на него информацию с именем и паролем пользователя, после чего сервер TACACS+ отвечает, успешно прошла аутентификация или нет.

Чтобы добавить сервер TACACS+:

1. На странице **Центр управления** в разделе **Центр управления → Серверы аутентификации** нажмите **Добавить** и выберите **Добавить TACACS+ сервер**.
2. В окне **Свойства TACACS+ сервера** укажите название сервера.
3. В поле **Секретный ключ** введите общий ключ, используемый протоколом TACACS+ для аутентификации.
4. Укажите IP-адрес сервера TACACS+ и UDP-порт, на котором сервер TACACS+ слушает запросы на аутентификацию.
5. Если необходимо использовать одно TCP-соединение для работы с сервером TACACS+, установите соответствующий флажок.
6. Если необходимо, измените время ожидания сервера TACACS+ для прохождения аутентификации. По умолчанию — 4 секунды.
7. Установите флажок **Включен**, чтобы начать использовать RADIUS-сервер, и сохраните изменения.

Для авторизации пользователей в веб-консоли управления UGMC с помощью сервера TACACS+ необходимо настроить профиль аутентификации. Подробнее о создании и настройке профилей — в разделе «[Профили аутентификации](#)».

Профили аутентификации

Documentation: ☒

Version: 7.x

Product: UGMC

Профиль позволяет определить набор методов аутентификации пользователей в веб-консоли управления UGMC.

Важно! Перед добавлением профиля аутентификации необходимо настроить нужный [сервер аутентификации](#).

Чтобы добавить профиль аутентификации:

1. В разделе **Центр управления → Профили аутентификации** нажмите **Добавить**.
2. В окне **Свойства профиля аутентификации** на вкладке **Общие** укажите название профиля.
3. Если необходимо, настройте один или несколько параметров:
 - **Время бездействия до отключения** — время, по истечении которого будет отменена авторизация пользователя в случае его неактивности (при отсутствии сетевых пакетов с IP-адресами пользователя). После чего пользователю потребуется повторно авторизоваться.
 - **Время жизни аутентифицированного пользователя** — время, по истечении которого будет отменена авторизация пользователя. После чего пользователю потребуется повторно авторизоваться.
 - **Число неудачных попыток аутентификации (локальные пользователи)** — разрешенное количество неудачных попыток авторизации до блокировки учетной записи локального пользователя.
 - **Время блокировки локального пользователя** — время, на которое будет заблокирована учетная запись локального пользователя при достижении указанного числа неудачных попыток авторизации.
4. На вкладке **Методы аутентификации** нажмите **Добавить**, и по кнопке **Добавить** выберите предварительно настроенный сервер аутентификации: LDAP-коннектор, RADIUS-сервер или сервер TACACS+.
5. Сохраните изменения.

Теперь вы можете использовать созданный профиль при создании учетных записей администраторов.

Version: 7.x
Product: UGMC
Documentation: ☒

IP-адреса

Раздел IP-адреса содержит список диапазонов IP-адресов, которые могут быть использованы при настройке UGMC. Первоначальный список адресов поставляется вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Для добавления нового списка адресов необходимо выполнить следующие шаги:

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

Администратор имеет возможность создавать свои списки IP-адресов и централизованно распространять их на все устройства с установленным UserGate. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми IP-адресами.	Создать файл list.txt со списком адресов. Список адресов записывается в обычный текстовый файл, где адреса прописываются в столбик без знаков препинания. Например: x.x.x.x y.y.y.y z.z.z.z
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip .
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.

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

Почтовые адреса

Элемент библиотеки **Почтовые адреса** позволяет создать группы почтовых адресов, которые впоследствии можно использовать в правилах оповещения.

Для добавления новой группы почтовых адресов необходимо выполнить следующие шаги:

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

Администратор имеет возможность создавать списки почтовых адресов и централизованно распространять их на все компьютеры с установленным UserGate. Для создания такого списка необходимо выполнить следующие действия:

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

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

Номера телефонов

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

Для добавления новой группы телефонных номеров необходимо выполнить следующие шаги:

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

Администратор имеет возможность создавать списки телефонных номеров и централизованно распространять их на все компьютеры с установленным UserGate. Для создания такого списка необходимо выполнить следующие действия:

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

Наименование	Описание
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.
Шаг 5. Создать список телефонных номеров и указать URL для обновления.	На каждом UserGate создать список номеров. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. UserGate будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: - Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. - Ежедневно. - Еженедельно. - 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".

Профили оповещений

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

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

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

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

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

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

Расширение системного раздела

Version: 7.x
Product: NGFW, UGMC, LogAn, 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.

Version: 7.x
Product: UGMC

Прямое обновление ПО узлов кластера MC

Прямое обновление программного обеспечения узлов кластера UserGate MC можно инициировать в **Центре обновлений** каждого узла кластера. Для корректного обновления кластера необходимо, чтобы все узлы были включены и доступны на момент обновления первого узла.

Рекомендуется производить обновление кластера по следующему алгоритму:

1. Перед началом обновления создайте резервную копию узла — это позволит восстановить его работоспособность в случае сбоя. Подробнее о создании резервной копии — в разделе «[Управление устройством](#)».
2. Начните обновление с резервного узла кластера отказоустойчивости. Перейдите в раздел **Центр управления → Настройки → Центр обновлений** и запустите обновление.

Примечание После обновления программного обеспечения на первом узле, узлы кластера конфигурации временно отобразятся как недоступные из-за различий в версиях. После приведения всех узлов к одной версии отображение состояния кластера восстановится. Перевод роли мастер-узла в кластере отказоустойчивости будет доступен.

3. После успешного обновления резервного узла переведите его в статус мастер-узла и проверьте работоспособность ключевых функций. При отсутствии ошибок в работе узла приступайте к обновлению следующего узла кластера.

Обновление может занять длительное время. Рекомендуется планировать установку обновлений с учетом возможного времени простоя системы. Во время обновления устройство может несколько раз перезагружаться. Как правило, после первой перезагрузки происходит установка обновления, в это время в CLI доступен ограниченный набор команд, веб-интерфейс недоступен. После установки обновлений устройство также будет перезагружено.

Важно! Не вносите изменения в конфигурацию во время обновления кластера во избежание проблем синхронизации узлов.

Запись об установке обновления будет отображена в журнале событий (раздел **Центр управления → Журналы и отчеты**).

Обновление ПО узлов кластера MC с импортом конфигурации

В случае если прямое обновление программного обеспечения узлов кластера UserGate MC невозможно, например при переходе между разными ветками версий (6.x → 7.x), необходимо выполнить чистую установку узлов. Перенос конфигурации узла при таком варианте обновления программного обеспечения можно сделать с помощью операций экспорта и импорта конфигурации.

Экспорт настроек является кластерной функцией: экспортируется конфигурация всех узлов кластера. При импорте конфигурации будет предложен выбор нужного узла кластера для восстановления.

В отличие от резервного копирования, экспорт и импорт настроек не сохраняет текущее состояние всех компонентов устройства, сохраняются только текущие параметры.

Процедура импорта конфигурации узлов кластера MC включает в себя следующие основные шаги:

1. Экспорт настроек конфигурации узлов исходного кластера MC.
2. Импорт настроек конфигурации на мастер-узле нового кластера.
3. Подключение резервного узла нового кластера.

Важно! Импорт настроек конфигурации предназначен для восстановления конфигурации узла после чистой переустановки. Не рекомендуется проводить импорт полной конфигурации на работающем кластере (например, для проверки).

Экспорт настроек конфигурации узлов исходного кластера MC

Для экспорта настроек конфигурации узлов исходного кластера MC:

1. В веб-консоли администратора любого из узлов кластера перейдите в раздел **Центр управления → Управление устройством → Экспорт и импорт настроек**, нажмите **Экспорт** и выберите **Экспортировать все настройки**.
2. Сохраните созданный файл экспорта конфигурации узлов кластера.

Импорт настроек конфигурации мастер-узла кластера

Для импорта настроек конфигурации мастер-узла исходного кластера MC:

1. В веб-консоли узла, на который необходимо перенести конфигурацию мастер-узла кластера, перейдите в раздел **Центр управления → Управление устройством → Экспорт и импорт настроек** и нажмите **Импорт**.
2. В открывшемся окне импорта нажмите **Выберите файл** и выберите сохраненный ранее файл экспорта конфигурации узлов кластера.
3. Выберите **Импортировать все настройки** и нажмите **Выбрать узлы**.
4. Выберите название мастер-узла из файла экспорта и нажмите **Старт**. Узел перейдет в режим перезагрузки. В процессе перезагрузки будет выполнена процедура factory reset (возвращение к первоначальному состоянию), затем применятся

импортированные настройки конфигурации и узел загрузится с конфигурацией мастер-узла из файла экспорта.

5. После окончания процедуры импорта повторно зарегистрируйте устройство в разделе **Дашборд → Лицензия** с помощью имеющегося ПИН-кода. Это необходимо, так как импорт настроек не восстанавливает информацию о лицензии.

6. Перейдите в раздел **Центр управления → Управление устройством → Кластер конфигурации** и выберите IP-адрес кластерного интерфейса текущего узла. После установки IP-адреса устройство перезагрузится.

7. После перезагрузки узла перейдите в раздел **Центр управления → Управление устройством → Кластер отказоустойчивости** и в свойствах импортированного кластера на вкладке **Узлы** выберите текущий узел.

8. На вкладке **Виртуальные IP** выберите интерфейс устройства, на котором будет работать VRRP.

9. Сохраните настройки кластера.

Импорт настроек конфигурации мастер-узла завершен.

Подключение резервного узла кластера

Для подключения резервного узла кластера:

1. Выполните первоначальную установку узла MC в качестве дополнительного узла в кластере. Подробнее о добавлении дополнительного узла в кластер MC — в разделе «[Управление устройством](#)».

2. В разделе **Центр управления → Сеть → Интерфейсы** назначьте каждому интерфейсу корректную зону. Зоны и их параметры получены в результате репликации данных с первого узла кластера. При необходимости настройте шлюзы, маршруты.

3. После завершения синхронизации кластера конфигурации перейдите в раздел **Центр управления → Управление устройством → Кластер отказоустойчивости** и в свойствах кластера на вкладке **Узлы** выберите текущий узел.

4. На вкладке **Виртуальные IP** выберите интерфейс устройства, на котором будет работать VRRP.

5. Сохраните настройки кластера.

Импорт настроек конфигурации узлов кластера завершен.

