

Table of Contents

Table of Contents	1
Настройка UGMC	2
Общие настройки	3
Управление устройством	4
Администраторы	10
Управление сертификатами	12
Профили оповещений	14
Серверы авторизации UserGate Management Center	15
Офлайн операции с сервером	16

Общие настройки

Documentation: ☒
Version: 6.1.9, 7.0.1, 7.1.0
Product: UGMC

Раздел **Общие настройки** определяет базовые установки UGMC:

Наименование	Описание
Часовой пояс	Часовой пояс, соответствующий вашему местоположению. Часовой пояс используется в расписаниях, применяемых в правилах, а также для корректного отображения даты и времени в отчетах, журналах и т.п.
Язык интерфейса по умолчанию	Язык, который будет использоваться по умолчанию в консоли.
Настройка времени сервера	Настройка параметров установки точного времени. • Использовать NTP — использовать сервера NTP из указанного списка для синхронизации времени. • Основной сервер NTP — адрес основного сервера точного времени. Значение по умолчанию — pool.ntp.org. • Запасной сервер NTP — адрес запасного сервера точного времени. • Время на сервере — позволяет установить время на сервере. Время должно быть указано в часовом поясе UTC.
Системные DNS-серверы	Укажите корректные IP-адреса серверов DNS в настройке.

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

- Кластеризация.
- Настройки диагностики.
- Операции с сервером.
- 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.

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.

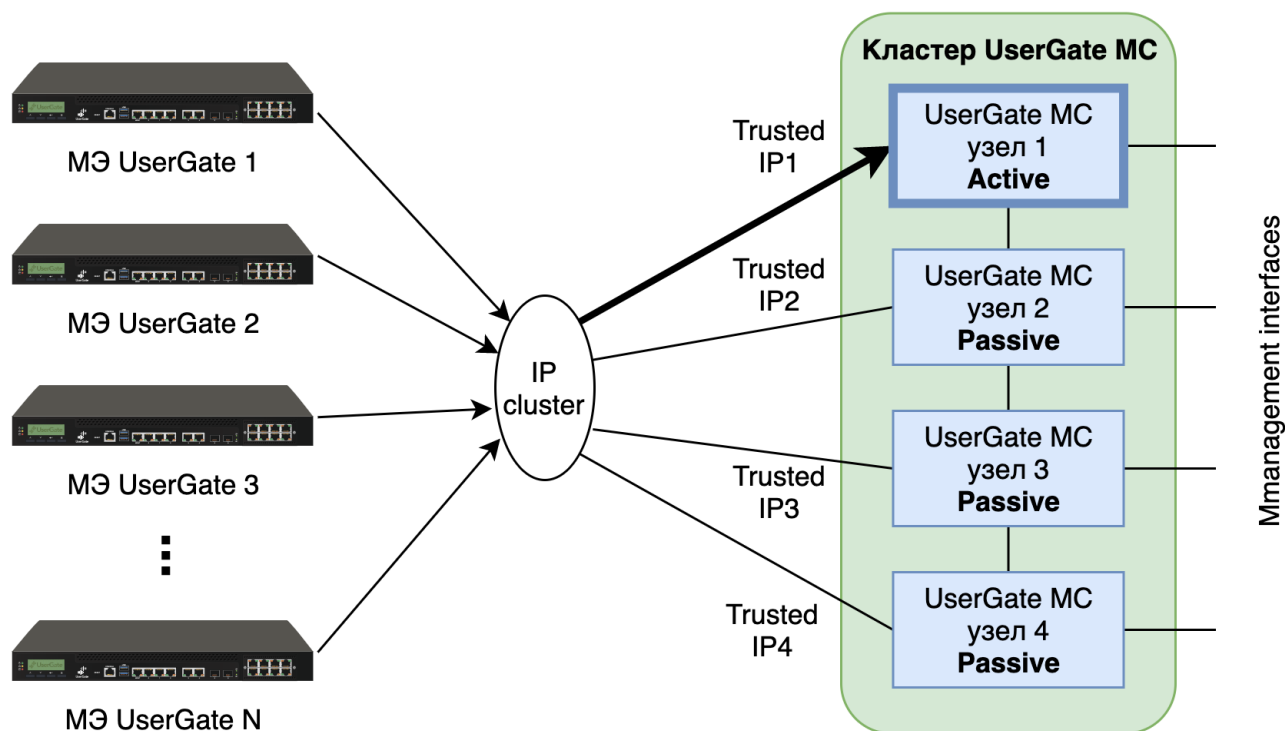
До четырех узлов кластера конфигурации можно объединить в отказоустойчивый кластер. Самых кластеров отказоустойчивости может быть несколько. Поддерживаются 2 режима - **Актив-Актив** и **Актив-Пассив**.

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.



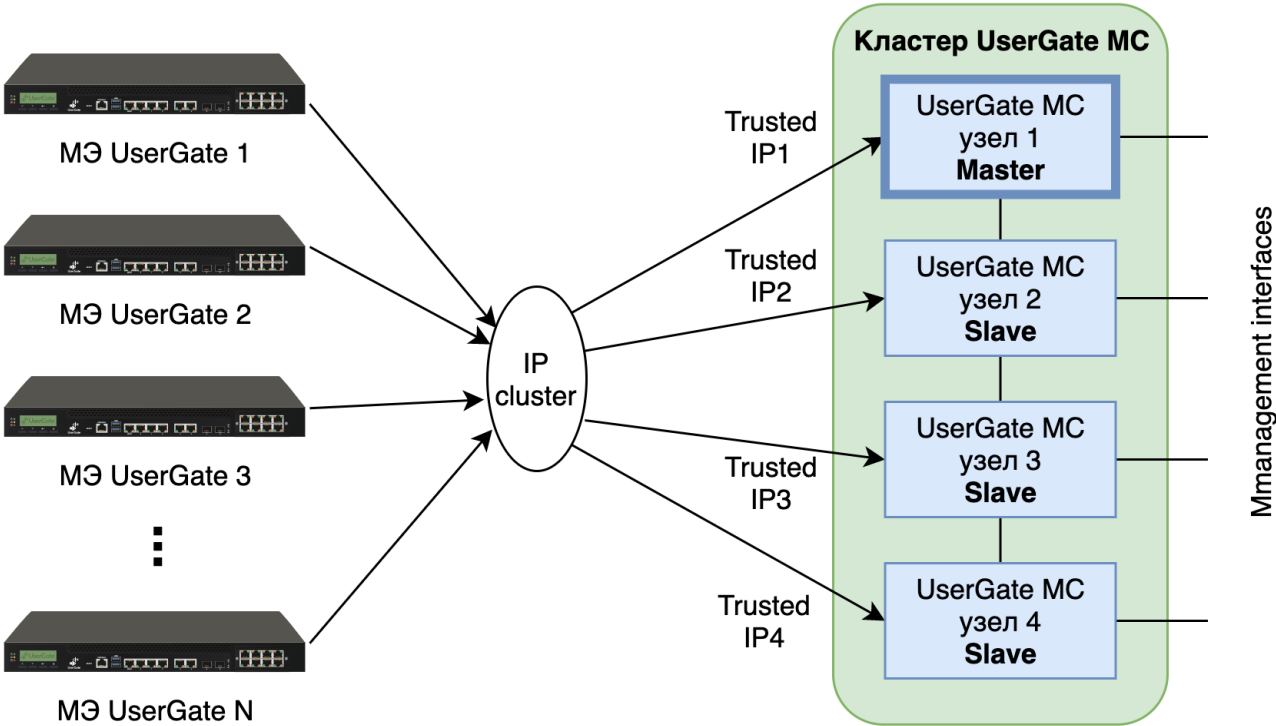
Кластерный IP-адрес находится на узле UGMC 1. Если узел UGMC 1 становится недоступным, то кластерный IP-адрес перейдет на следующий сервер, который станет мастер-сервером, например, UGMC 2.

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

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

Наименование	Описание
Детализация диагностики	• Off — ведение журналов диагностики отключено. • Error — журналировать только ошибки работы сервера. • Warning — журналировать только ошибки и предупреждения. • Info — журналировать только ошибки, предупреждения и дополнительную информацию. • Debug — максимум детализации. Рекомендуется установить значение параметра Детализация диагностики в Error (только ошибки) или Off (Отключено), если техническая поддержка UserGate не попросила вас установить иные значения. Любые значения, отличные от Error (только ошибки) или Off (Отключено), негативно влияют на производительность UGMC.
Журналы диагностики	• Скачать журналы — скачать диагностические журналы для передачи их в службу поддержки UserGate. • Очистить журналы — очистить содержимое журналов.
Удаленный помощник	• Включено/Отключено — включение/отключение режима удаленного помощника. Удаленный помощник позволяет инженеру технической поддержки UserGate, зная значения идентификатора и токена удаленного помощника, произвести безопасное подключение к серверу UGMC для диагностики и решения проблем. Для успешной активации удаленного помощника UGMC должен иметь доступ к серверу удаленного помощника компании UserGate по протоколу SSH. • Идентификатор удаленного помощника — полученное случайным образом значение. Уникально для каждого включения удаленного помощника. • Токен удаленного помощника — полученное случайным образом значение токена. Уникально для каждого включения удаленного помощника.

Операции с сервером

Данный раздел позволяет произвести следующие операции с сервером:

Наименование	Описание
Операции с сервером	• Перезагрузить — перезагрузка сервера UGMC. • Выключить — выключение сервера UGMC.
Обновления	Выбор канала обновлений ПО UGMC • Стабильные — проверка наличия стабильных обновлений ПО. • Бета — проверка наличия экспериментальных обновлений.

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.

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.

Примечание Экспорт/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 нажать на ссылку Экспорт настроек → 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 нажать на ссылку Экспорт настроек → Импорт и указать путь к ранее созданному файлу настроек. Указанные настройки применятся к серверу, после чего сервер будет перезагружен

Примечание Для 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.

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
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".

Администраторы

Version: 6.1.9, 7.0.1, 7.1.0
Product: UGMC
Documentation: ☒

Доступ к веб-консоли UGMC 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 UGMC создается локальный суперпользователь Admin/system.

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/system или domain\user/system. 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/system или domain\user/system. Назначить созданный ранее профиль. • Добавить администратора с профилем аутентификации — создать пользователя, назначить созданный ранее профиль администратора и профиль аутентификации (необходимы корректно настроенные серверы аутентификации). Важно! В данном разделе настроек сервисов консоли управления администратором области может быть назначен только локальный администратор. Это связано с тем, что LDAP серверы, используемые для аутентификации администраторов сервиса UGMC и для аутентификации администраторов области, могут быть разными. При необходимости использования LDAP администраторов для управления Областью, их необходимо создать в самой области. Более подробно об администраторах области смотрите в разделе Администраторы области.

При создании профиля доступа администратора необходимо указать следующие параметры:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Тип администратора	Для предоставления полномочий управления сервисами UGMC необходимо выбрать тип Администратор UGMC . Вариант Администратор области следует выбирать при создании корневого администратора управляемой области.
Управляемая область	Если в качестве параметра Тип администратора был выбран вариант Администратор области , то необходимо указать управляемую область, для которой создается корневой администратор. Область должна уже быть создана к этому моменту.
Права доступа	Список объектов дерева веб-консоли, доступных для делегирования. В качестве доступа можно указать: • Нет доступа. • Чтение. • Чтение и запись.

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

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.

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

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

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

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

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

Управление сертификатами

Product: UGMC
Version: 6.1.9, 7.0.1, 7.1.0
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.

Профили оповещений

Version: 6.1.9

Product: UGMC

Documentation: ☒

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

- SMTP, доставка сообщений с помощью e-mail
- 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.
Авторизация	Включает авторизацию 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.

Серверы авторизации UserGate Management Center

Version: 6.1.9

Product: UGMC

Documentation: 

Серверы авторизации — это внешние источники учетных записей пользователей для авторизации в веб-консоли управления UGMC. UGMC поддерживает только сервер авторизации 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 UGMC 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 авторизации.
Название	Название сервера авторизации.
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*

Офлайн операции с сервером

Version: 6.1.9
Product: UGMC
Documentation: ☒

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

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

Наименование	Описание
1. UserGate MC (serial console)	Загрузка UGMC с выводом диагностической информации о загрузке в последовательный порт.
2. UserGate MC (verbouse mode)	Загрузка UGMC с выводом диагностической информации о загрузке в консоль tty1 (монитор).
3. Support menu	Войти в раздел системных утилит с выводом информации в консоль tty1 (монитор).
4. Support menu (serial console)	Войти в раздел системных утилит с выводом информации в последовательный порт. При подключении через последовательный порт загрузочное меню не отображается. Для выбора раздела Support menu необходимо во время загрузки нажимать клавишу "4". Для выбора одного из пунктов меню в разделе Support menu необходимо нажать клавишу, соответствующую первой букве названия пункта меню, например, для выбора Restore backup , необходимо нажать клавишу "R", затем клавишу "Ввод".
5. Memory test	Запуск проверки оперативной памяти устройства.

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

Наименование	Описание
Check filesystems	Запуск проверки файловой системы устройства на наличие ошибок и их автоматическое исправление.
Clear logs	Очистка диагностических журналов для освобождения пространства на системном разделе.
Export logs	Выгрузка диагностических журналов на внешний USB носитель. Все данные на внешнем носителе будут удалены.
Expand log partition	Увеличение раздела для журналов на весь выделенный диск. Эта операция обычно используется после увеличения дискового пространства, выделенного гипервизором для виртуальной машины UGMC. Данные и настройки UGMC не сбрасываются.
Backup full	Создать полную копию диска UGMC на внешний USB носитель. Все данные на внешнем носителе будут удалены.
Backup system only	Создать копию системного раздела UGMC, исключая журналы на внешний USB носитель. Все данные на внешнем носителе будут удалены.
Restore from backup	Восстановление UGMC с внешнего USB носителя.

Наименование	Описание
Update from USB	Установка обновления ПО UGMC с внешнего USB носителя. Обновление должно быть скопировано в корень съемного диска, диск должен иметь формат NTFS или FAT32. Название файла обновления должно быть в следующем формате: update_XXXX (где XXXX - номер сборки). Без расширения .bin.
Refresh NIC names	Упорядочивание имен сетевых портов в необходимом порядке. Упорядочивание производится в соответствии с номером порта на шине PCI. Эту операцию необходимо выполнять после добавления сетевых портов в настроенный аплаенс UGMC, например, после установки дополнительной сетевой карты в физический аплаенс или после добавления портов в виртуальный аплаенс. Данные и настройки UGMC не сбрасываются.
Factory reset	Сброс состояния UGMC к первоначальному состоянию системы. Все данные и настройки будут утеряны.
Exit	Выход и перезагрузка устройства.

