

Table of Contents

Table of Contents	1
Быстрый старт	2
Подключение к UserGate и первоначальная настройка	3
Переход на UserGate NGFW	7
Подключение к CLI-консоли UserGate	8
Развертывание виртуального образа	9
Установка ПО UserGate на аппаратных платформах C100, D200, D500, E1000, E3000, F8000	12
Установка ПО UserGate на аппаратных платформах E1010, E3010, F8010	21
Обновление компонентов ПО с использованием PMC на аппаратных платформах B50, C150, C151, D250, FG, X10	32
Установка ПО UserGate на платформу C150	37
Лицензирование	38

Подключение к UserGate и первоначальная настройка

Version: 5.x, 6.1.8, 6.1.9, 7.0.0, 6.x, 7.x
Product: UserGate NGFW
Documentation: 

Интерфейс port0 настроен на получение IP-адреса в автоматическом режиме (DHCP) и назначен в зону **Management**. Первоначальная настройка осуществляется через подключение администратора к веб-консоли через интерфейс port0.

Если нет возможности назначить адрес для Management-интерфейса в автоматическом режиме с помощью DHCP, то его можно явно задать, используя CLI (Command Line Interface). Более подробно об использовании CLI смотрите в главе Интерфейс командной строки (CLI) соответствующей версии: [6.x.x](#), [7.x.x](#).

Остальные интерфейсы отключены и требуют последующей настройки.

Первоначальная настройка требует выполнения следующих шагов:

Наименование	Описание

Наименование	Описание
Шаг 1. Подключиться к интерфейсу управления.	При наличии DHCP-сервера Подключить интерфейс port0 в сеть предприятия с работающим DHCP-сервером. Включить UserGate. После загрузки UserGate укажет IP-адрес, на который необходимо подключиться для дальнейшей активации продукта. Статический IP-адрес Включить UserGate. Используя CLI (Command Line Interface), назначить необходимый IP-адрес на интерфейс port0. Детали использования CLI смотрите в главе Интерфейс командной строки (CLI) (версий 6.x.x, 7.x.x). В случае использования ПАК подключение к CLI можно выполнить через стандартные порты VGA/клавиатуры (при наличии таких портов на оборудовании UserGate), через последовательный порт или с помощью SSH по сети. Важно! При подключении к CLI по протоколу SSH адрес интерфейса управления должен быть известен, т.е. предварительно получен по DHCP или назначен статически любым удобным способом. При подключении через консольный порт настройте следующий режим работы (также доступен в руководстве эксплуатации соответствующей модели ПАК): • Скорость передачи данных: 115200 • Биты данных: 8 • Контроль чётности: нет • Стоповый бит: 1 В случае подключения по IPMI — платформы D, E и F, подключите кабель в порт Management (MGMT). Адрес интерфейса IPMI по умолчанию: https://192.168.0.100; пользователь с логин/паролем admin/admin. Подробнее читайте Удаленное управление с помощью IPMI. Далее первоначальная настройка ПАК и виртуальных машин производится аналогично. Важно! Настройка, представленная далее, доступна только для версий 7.0.1 и выше. После подключения к CLI пройдите авторизацию, учетные данные администратора, созданного по умолчанию: • Для версии 7.0.1 логин — Admin, пароль — без пароля. • Для версий 7.1.0 и выше логин — Admin, пароль — usergate. Для отображения адреса, полученного по DHCP: <pre>Admin@UGOS> show network interface port0</pre> или <pre>Admin@UGOS> configure Admin@UGOS# show network interface adapter port0</pre> Важно! Первая команда выполняется в режиме диагностики и мониторинга, вторая — в режиме конфигурации. Для назначения статического IP-адреса на интерфейс управления перейдите в режим конфигурации: <pre>Admin@UGOS> configure</pre> и задайте необходимый адрес: <pre>Admin@UGOS# set network interface adapter port0 ip-addresses [IP-address/mask]</pre> Важно! Назначение статического адреса доступно только в режиме конфигурации; в режиме диагностики и мониторинга данная команда недоступна. При указании адреса пробел перед и после адреса обязателен. При необходимости настройте шлюз по умолчанию (также в режиме конфигурации): <pre>Admin@UGOS# create network gateway name GATEWAY_NAME ip IP_ADDRESS virtual-router default default on enabled on</pre> Подробнее об интерфейсе командной строки читайте в соответствующих разделах: • Для версии 7.0.1. • Для версии 7.1.0. Подключиться к веб-консоли UserGate по указанному адресу, он должен выглядеть примерно следующим образом: https://UserGate_IP-address:8001. Первоначальная инициализация также может быть произведена с использованием интерфейса командной строки. Подробнее читайте в соответствующих разделах: • Для версии 7.0.1. • Для версии 7.1.0.
Шаг 2. Выбрать язык.	Выбрать язык, на котором будет продолжена первоначальная настройка.

Наименование	Описание
Шаг 3. Задать пароль.	Задать логин и пароль для входа в веб-интерфейс управления.
Шаг 4. Настроить зоны, IP-адреса интерфейсов, подключить UserGate в сеть предприятия.	В разделе Интерфейсы включить необходимые интерфейсы, установить корректные IP-адреса, соответствующие вашим сетям, и назначить интерфейсы соответствующим зонам. Подробно об управлении интерфейсами читайте в главе Настройка интерфейсов. Система поставляется с предопределенными зонами: • Зона Management (сеть управления), интерфейс port0. • Зона Trusted (LAN). • Зона Untrusted (Internet). • Зона DMZ. • Зона Cluster. • Зона VPN for remote access. • Зона VPN for Site-to-Site.
Шаг 5. Настроить шлюз в Интернет.	В разделе Шлюзы указать IP-адрес шлюза в интернет на интерфейсе, подключенном в интернет, зона Untrusted . Подробно о настройке шлюзов в интернет читайте в главе Настройка шлюзов .
Шаг 6. Указать системные DNS-серверы.	В разделе DNS укажите IP-адреса серверов DNS, вашего провайдера или серверов, используемых в вашей организации. Подробно об управлении DNS читайте в главе Настройка DNS.
Шаг 7. Настроить время сервера.	В разделе UserGate → Настройки → Настройка времени сервера настроить синхронизацию времени с серверами NTP.
Шаг 8. Зарегистрировать продукт UserGate.	Для регистрации продукта ввести ПИН-код и заполнить форму. Для активации системы необходим доступ UserGate в Интернет. Более подробно о лицензировании продукта читайте в главе Лицензирование UserGate.
Шаг 9. Создать правила NAT.	В разделе NAT и Маршрутизация создать необходимые правила NAT. Для доступа в интернет пользователей сети Trusted правило NAT уже создано: «NAT from Trusted to Untrusted». Подробно о правилах NAT читайте в главе NAT и маршрутизация.
Шаг 10. Создать правила межсетевого экрана.	В разделе Межсетевой экран создать необходимые правила межсетевого экрана. Для неограниченного доступа в интернет пользователей сети Trusted правило межсетевого экрана уже создано — «Allow trusted to untrusted», необходимо только включить его. Подробно о правилах межсетевого экрана читайте в главе Межсетевой экран.
Шаг 11. Создать дополнительных администраторов (опционально).	В разделе Администраторы UserGate создать дополнительных администраторов системы, наделить их необходимыми полномочиями (ролями).
Шаг 12. Настроить авторизацию пользователей (опционально).	В разделе Пользователи и устройства создать необходимые методы авторизации пользователей. Самый простой вариант — это создать локальных пользователей UserGate с заданными IP-адресами или использовать систему без идентификации пользователей (использовать пользователя Any во всех правилах). Для других вариантов авторизации пользователей смотрите главу Пользователи и устройства.
Шаг 13. Создать правила контентной фильтрации (опционально).	В разделе Фильтрация контента создать правила фильтрации HTTP(S). Более подробно о фильтрации контента читайте в главе Фильтрация контента.
Шаг 14. Создать правила веб-безопасности (опционально).	В разделе Веб-безопасность создать дополнительные правила защиты веб. Более подробно о веб-безопасности читайте в главе Веб-безопасность.
Шаг 15. Создать правила инспектирования SSL (опционально).	В разделе Инспектирование SSL создать правила для перехвата и расшифровывания HTTPS-трафика. Более подробно о дешифровании HTTPS читайте в главе Инспектирование SSL.

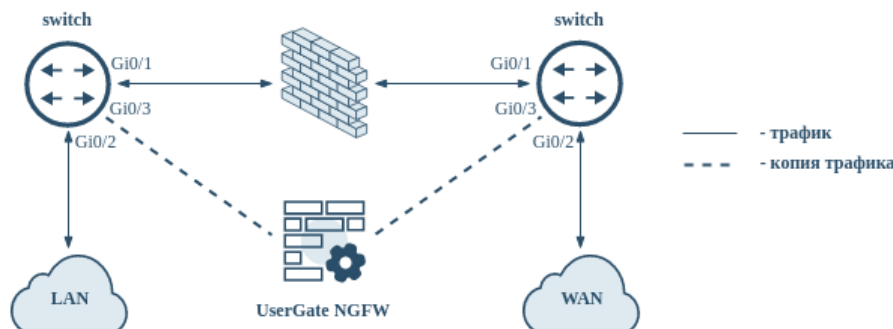
После выполнения вышеперечисленных действий UserGate готов к работе. Для более детальной настройки обратитесь к необходимым главам справочного руководства.

Переход на UserGate NGFW

Version: 6.x, 7.x

Product: NGFW

Технологию зеркалирования портов коммутатора можно использовать для проверки переноса сервисов и трафика с существующего межсетевого экрана (МЭ) на UserGate NGFW. Для этого необходимо продублировать правила существующего МЭ на МЭ UserGate и перевести копию трафика на МЭ UserGate.



В соответствии с представленной схемой UserGate NGFW принимает копию трафика, который поступает и обрабатывается существующим межсетевым экраном, работающим в штатном режиме. UserGate NGFW обрабатывает копию трафика, но коммутаторы не принимают (порты Gi0/3) трафик от UserGate NGFW.

Примечание При выполнении данных настроек рекомендуется включить журналирование срабатываний правил и на используемом МЭ, и на UserGate NGFW для возможности последующего анализа корректности обработки трафика. На МЭ UserGate необходимо включить журналирование начала сессии.

Для корректного перехода на UserGate NGFW необходимо произвести следующие настройки:

1. На UserGate NGFW:

- в разделе **Сеть → Интерфейсы** произвести настройку интерфейсов, указав IP и MAC-адреса, идентичные адресам интерфейсов используемого МЭ;
- произвести настройки политик: продублировать правила существующего МЭ на UserGate. Перенос правил может быть выполнен вручную или с использованием скриптов (доступно не для всех вендоров; обратитесь в техническую поддержку UserGate для уточнения информации). Включить журналирование правил.

2. На обоих коммутаторах включить зеркалирование входящего трафика (порт Gi0/2) в сторону UserGate NGFW (порт Gi0/3). Для настройки зеркалирования портов обратитесь к соответствующей документации производителя вашего оборудования.

3. После настройки произвести анализ журналов работы используемого МЭ и МЭ UserGate.

Примечание В такой конфигурации доступна только проверка работы модулей COB и L7; анализ корректности обработки трафика правилами инспектирования SSL и контентной фильтрации невозможен.

В случае совпадения записей журналов принимается решение о корректности настройки UserGate NGFW. Далее возможен перенос реального трафика на порты UserGate через физическую коммутацию портов или настройки коммутаторов.

Подключение к CLI-консоли UserGate

Version: 6.x, 7.x, 8.x

Product: UserGate NGFW, NGFW

Подключиться к интерфейсу командной строки (Command Line Interface, CLI) UserGate можно следующими способами:

- с помощью виртуальной консоли в случае использования виртуальной машины UserGate;
- используя монитор (подключённый к разъёму VGA (HDMI) и клавиатуру (подключённую к разъёму USB) при наличии портов у используемого программно-аппаратного комплекса (ПАК);
- с использованием последовательного порта в случае ПАК: для подключения используется терминал, позволяющий подключение через последовательный порт (например, Putty для Windows или minicom для Linux). Параметры подключения: 115200 8n1;
- через порт управления IPMI (Intelligent Platform Management Interface) в случае аппаратных платформ UserGate модели D, E и F. Подробнее о настройке читайте [Удалённое управление с помощью IPMI](#);
- по протоколу SSH. Данный способ подходит и для виртуальных машин, и для ПАК. Подключение по SSH доступно только после окончания загрузки системы, соответственно, раздел системных утилит (резервное копирование, восстановление и т.п.) недоступны. Подключение производится с использованием порта 2200; команда для подключения:

ssh Admin@UserGateIP -p 2200

где UserGateIP — IP-адрес интерфейса UserGate, через который производится подключение. Интерфейс должен принадлежать зоне, на которой разрешён сервис **CLI по SSH** (по умолчанию сервис разрешён только на зоне Management).

Для входа используются логин / пароль администратора с корневым профилем или профилем, имеющим разрешения для доступа в CLI. В случае, если устройство UserGate не прошло первоначальную инициализацию, то используйте логин / пароль — **Admin / usergate** (в более ранних релизах использовалась комбинация Admin / utm).

Подробнее об интерфейсе командной строки читайте в соответствующем [разделе](#) руководства.

Развертывание виртуального образа

Version: 7.x

Product: NGFW

Documentation: 

UserGate NGFW Virtual Appliance позволяет быстро развернуть виртуальную машину с уже настроенными компонентами. Образ предоставляется в формате OVF (Open Virtualization Format), который поддерживают системы виртуализации VMware, Oracle VirtualBox, и в формате Qcow2 для систем виртуализации QEMU-KVM. Для Microsoft Hyper-V поставляется образ диска виртуальной машины.

Примечание Для корректной работы виртуальной машины рекомендуется использовать минимум 12 ГБ оперативной памяти и 2-ядерный виртуальный процессор. Гипервизор должен поддерживать работу 64-битных операционных систем.

Примечание Для корректной работы внутренней базы данных требуется поддержка набора микрокоманд SSE4.2 архитектуры x86 процессорами виртуальной среды. Любой процессор на базе архитектуры x86, выпущенный после 2008 года, должен поддерживать SSE4.2.

Работа с виртуальным образом

Для начала работы с виртуальным образом выполните следующие шаги:

1. Скачайте последнюю версию виртуального образа в личном кабинете клиента на официальном сайте usergate.com.
2. Импортируйте образ в свою систему виртуализации. Инструкцию по импорту образа вы можете найти на сайтах систем виртуализации, например VirtualBox или VMware. Для Microsoft Hyper-V необходимо создать виртуальную машину и указать в качестве диска скачанный образ, после чего отключить службы интеграции в настройках созданной виртуальной машины.
3. До включения виртуальной машины настройте её параметры в своей системе виртуализации:
 - Увеличьте размер оперативной памяти виртуальной машины. Используя свойства виртуальной машины, установите минимум 12 ГБ и добавляйте по 1 ГБ на каждые 100 пользователей.
 - Добавьте дополнительный диск нужного размера. Размер диска по умолчанию составляет 100 ГБ, чего обычно недостаточно для хранения всех журналов и параметров. Используя свойства виртуальной машины, установите размер диска не меньше 200 ГБ. Рекомендованный размер — 300 ГБ или больше.
4. Для систем виртуализации QEMU-KVM размер системной области по умолчанию составляет 8 ГБ. При первом запуске система сама определит наличие дополнительного диска и расширит свои системные разделы. Команда для добавления диска размером 100 ГБ для систем QEMU-KVM:

```
qemu-img create -f qcow2 -o preallocation=metadata,refcount_bits=16,lazy_refcounts=on,cluster_size=4K <имя-вашего-диска>.qcow2 100G
```
5. Запустите виртуальную машину UserGate. Во время загрузки выполняется процедура Factory reset. Система UserGate настраивает сетевые адаптеры и увеличивает размер раздела на жестком диске до полного размера диска, увеличенного ранее.

UserGate NGFW поставляется с четырьмя интерфейсами, на каждом из которых назначена своя зона:

- **Management** — на первом интерфейсе виртуальной машины;
- **Trusted** — на втором интерфейсе виртуальной машины;
- **Untrusted** — на третьем интерфейсе виртуальной машины;
- **DMZ** — на четвертом интерфейсе виртуальной машины.

Порядок нумерации интерфейсов в виртуальной среде

В веб-консоли администратора сетевые интерфейсы отображаются по своим названиям. Сопоставление названия интерфейса и его адреса (H/W path или MAC) называется маппингом. Данные о маппинге интерфейсов хранятся в специальном системном файле. Посмотреть содержимое файла маппинга интерфейсов можно с помощью CLI-команды:

```
Admin@nodename> show network interface-mapping
```

После сброса до первоначального состояния (factory reset) при изменении количества сетевых адаптеров в системе (при добавлении или удалении адаптеров средствами гипервизора) происходит сортировка интерфейсов и их маппинг.

Выбор метода сортировки (по H/W path или по MAC-адресам) зависит от типа гипервизора и используемого эмулятора аппаратного обеспечения. В некоторых случаях (VirtualBox, QEMU, Bochs) сортировка интерфейсов производится по параметру H/W path, в остальных — по MAC-адресам интерфейсов.

При сортировке интерфейсов по параметру H/W path :

- Все имеющиеся на устройстве интерфейсы при любом изменении их количества (удаление, добавление) будут пересортированы в порядке возрастания аппаратных адресов (H/W path); системный файл с данными маппинга будет полностью перезаписан.
- Удаленные интерфейсы отображаются как неиспользуемые, помечаются соответствующим значком и помещаются в конец списка интерфейсов в веб-консоли.

При сортировке интерфейсов по MAC-адресам :

- Интерфейсы, уже добавленные в систему, остаются на своих местах.
- Удаляемые интерфейсы отмечаются в веб-консоли как неиспользуемые и помечаются специальными значками.
- Новые добавленные интерфейсы добавляются в конец списка в порядке возрастания MAC-адресов.

Если использовать консольную команду `clear network interface-mapping`, файл существующего маппинга интерфейсов будет удален и все имеющиеся интерфейсы после перезапуска машины будут пересортированы заново по принципу возрастания адресов.

Важно! Виртуальный образ устройства UserGate, доступный для скачивания в личном кабинете, не имеет файла маппинга интерфейсов. Сортировка интерфейсов и их маппинг осуществляются при первом запуске в виртуальной среде пользователя. При подготовке собственного виртуального образа устройства UserGate для его разворачивания впоследствии на облачной платформе необходимо также удалить данные маппинга сетевых адаптеров перед сохранением образа. Файл маппинга можно удалить консольной командой: `clear network interface-mapping`.

Примечание Если виртуальная машина UserGate клонируется через vSphere, то в VMX-файле параметров скопированной виртуальной машины необходимо удалить MAC-адреса, принадлежащие виртуальной машине источника.

Оптимизация производительности сетевых интерфейсов на основе virtio

Для оптимизации производительности сетевых интерфейсов на основе virtio в средах виртуализации KVM, oVirt, zVirt рекомендуется включить на гипервизоре режим Multi Queues и устанавливать 8 очередей на сетевой интерфейс. Например, в случае платформы Ovirt (см. [документацию oVirt](#)), для того чтобы выставить 8 очередей для vNIC, необходимо подключиться к CLI гипервизора и ввести команду:

```
engine-config -s "CustomDeviceProperties={type=interface;prop={other-nic-properties;queues=[1-9][0-9]*}}"
```

Вместо параметра `other-nic-properties` нужно вставить список существующих кастомизированных правил (если такие правила есть). Посмотреть, существуют ли кастомизированные правила, можно с помощью команды:

```
engine-config -g "CustomDeviceProperties"
```

После ввода команды необходимо на портале администратора зайти в профили vNIC.

Далее необходимо выбрать редактирование профиля сетевых карт, назначенного для NGFW, в выпадающем списке **Custom Properties** выбрать **queues**, после чего указать нужное количество очередей.

Product: UserGate NGFW

Важно! Процедура, описанная в этой статье, применима только к аппаратным платформам UserGate C100, D200, D500, E1000, E3000, F8000.

Процедура установки ПО UserGate на аппаратных платформах C100, D200, D500, E1000, E3000, F8000 состоит из следующих этапов:

1. Создание [загрузочного USB-носителя](#) с образом ПО UserGate.
2. Загрузка образа ПО на аппаратную платформу. Загрузку можно выполнить **одним** из двух способов:
 - а) с помощью [консольного подключения](#);
 - б) с помощью [подключения через IPMI](#).
3. [Распаковка образа ПО](#) на аппаратной платформе.

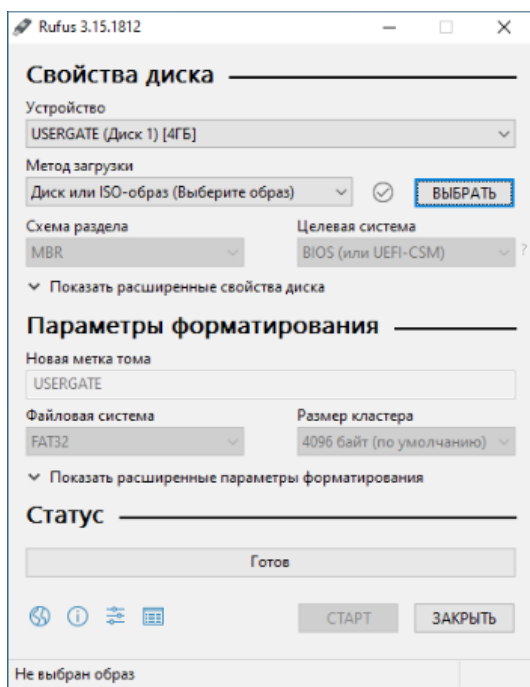
Примечание Если вы выполняете обновление версии ПО на устройстве с помощью метода чистой установки, перед началом обязательно сохраните (экспортируйте) параметры настройки устройства, а после завершения установки восстановите (импортируйте) ранее сохраненные параметры.

Важно! Лицензионные ключи для версий 6 и 7 не взаимозаменяемы. Для обновления до версии 7 требуется получить новый ключ.

Создание загрузочного USB-носителя с образом ПО UserGate

Для создания загрузочного USB-носителя:

1. Загрузите файл образа прошивки ПО [из личного кабинета UserGate](#) (требуется авторизация в личном кабинете), либо запросите его в службе технической поддержки UserGate.
2. Загрузите образ установочного носителя [по ссылке](#) (md5hash: 2a61c4d41bf9a5da9f12bbdac65fb0cc, ufix: 191C6251).
3. Скачайте [ПО Rufus](#) и запустите его.
4. Настройте Rufus, указав следующие параметры:
 - **Устройство:** выберите USB-носитель, на который будет записан образ.
 - **Метод загрузки:** выберите «Диск или ISO-образ».
 - Нажмите **Выбрать** и укажите загруженный на шаге 2 файл образа установочного носителя `usergate_light_image.iso`.



- Нажмите **Старт** для создания установочного носителя.
4. Когда установочный носитель будет создан, скопируйте образ прошивки ПО, полученный в личном кабинете UserGate, либо предоставленный службой технической поддержки, и сохраните его в директории `/utm_image` на подготовленном загрузочном USB-носителе.

Для продолжения процедуры установки ПО перейдите к этапу загрузки образа ПО на аппаратную платформу.

Загрузка образа ПО на аппаратную платформу

Загрузку образа ПО на аппаратную платформу можно выполнить **одним** из двух способов:

- а) с помощью [консольного подключения](#);
- б) с помощью [подключения через IPMI](#).

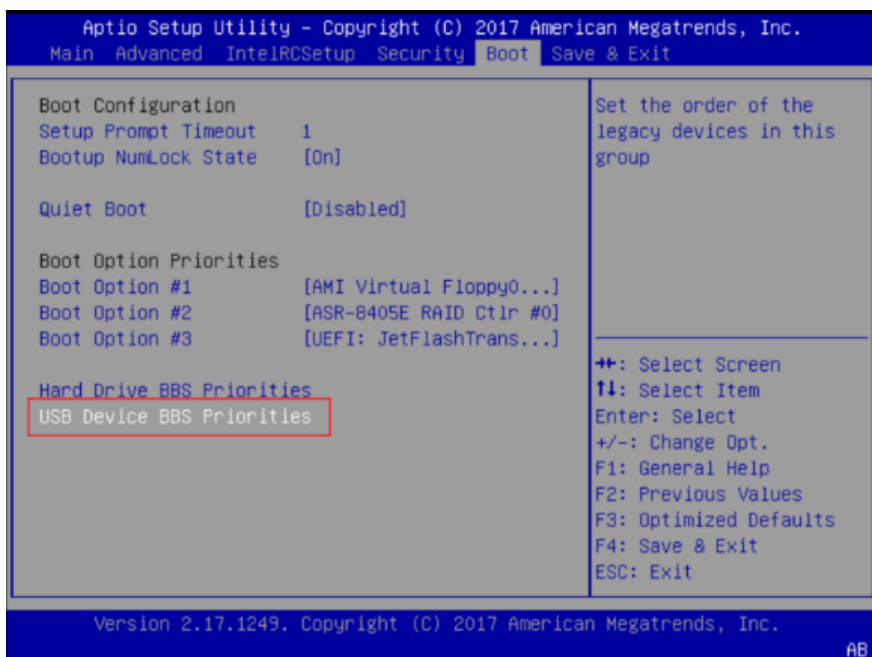
Загрузка образа ПО с помощью консольного подключения

Если вы выбрали способ загрузки образа ПО на аппаратную платформу с помощью консольного подключения, выполните следующие шаги:

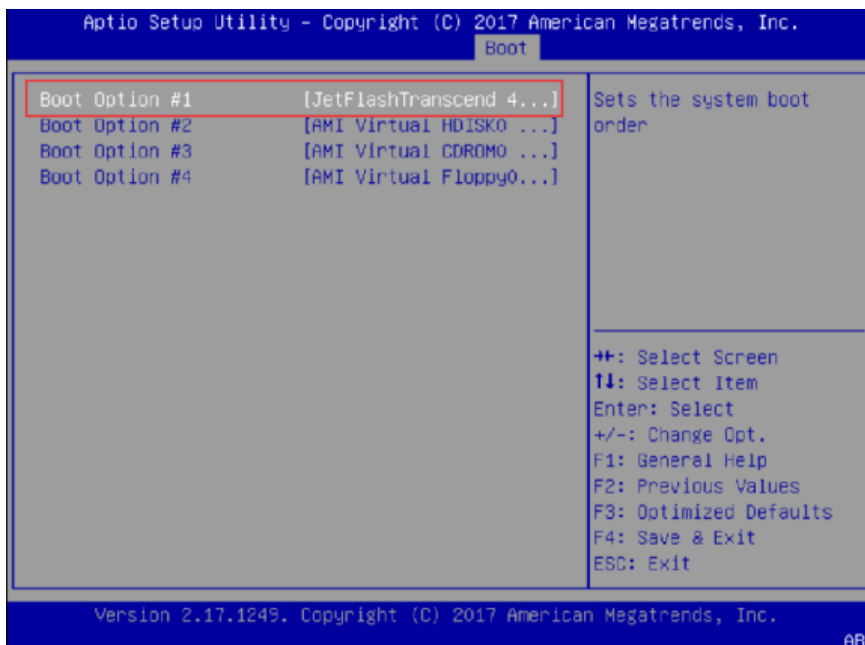
1. Подключите к устройству (ПАК UserGate) внешний монитор и USB-клавиатуру.
2. Войдите в BIOS устройства. Для этого включите устройство и нажмите клавишу Delete после появления на экране следующего оповещения.



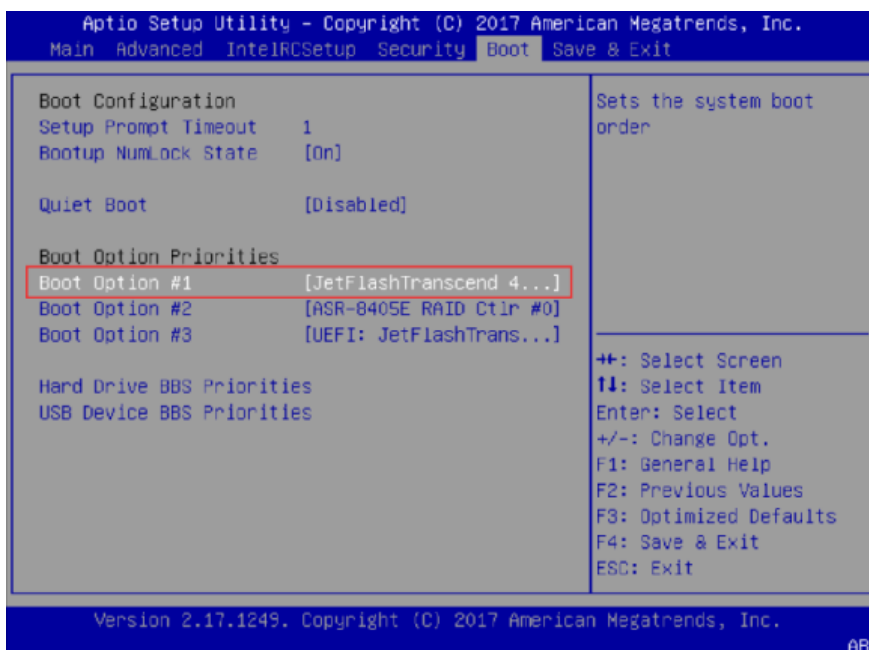
3. На вкладке **Boot** перейдите в раздел **USB Device BBS Priorities**; если такой раздел отсутствует, перейдите в раздел **Hard Drive BBS Priorities**.



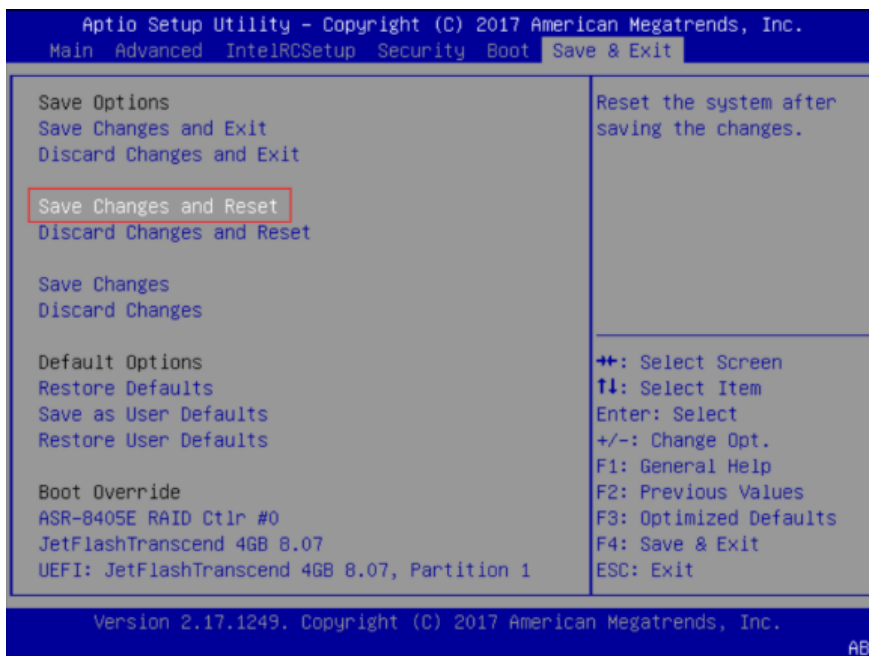
4. В параметре **Boot Option #1** выберите USB-носитель с Ghost4Linux. Общее количество Boot-опций может отличаться на разных устройствах.



5. Вернитесь в предыдущее меню и установите приоритет загрузки устройств. В параметре **Boot Option #1** выберите USB-накопитель с Ghost4Linux (не UEFI раздел).



6 Перейдите на вкладку **Save & Exit** и выберите команду **Save Changes and Reset**.



После перезагрузки устройство начнет загружаться с USB-накопителя.

Для продолжения процедуры установки ПО перейдите к этапу [распаковки образа ПО на аппаратной платформе](#).

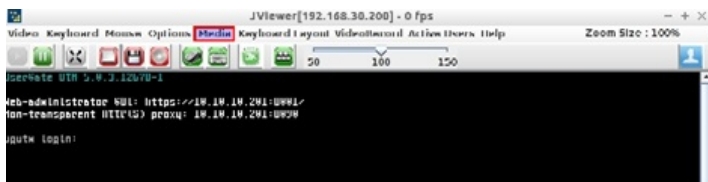
Загрузка образа ПО с помощью подключения через IPMI

Если вы выбрали способ загрузки образа ПО на аппаратную платформу с помощью подключения через IPMI, выполните следующие шаги:

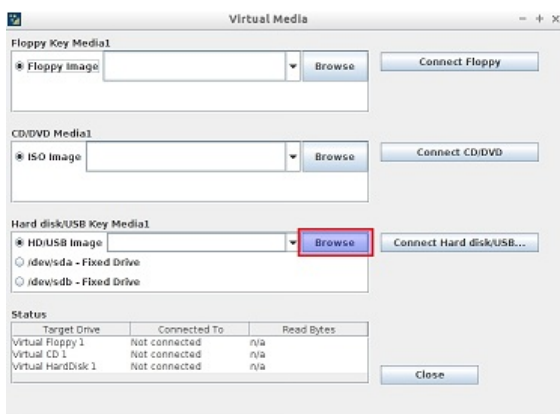
1. Сделайте имидж подготовленного на первом этапе USB-накопителя с расширением .img. Вы можете воспользоваться утилитой USB Image Tool [по ссылке](#).
2. Подключитесь к модулю IPMI устройства. О настройке подключения — в инструкции « [Удаленное управление с помощью IPMI](#) ».

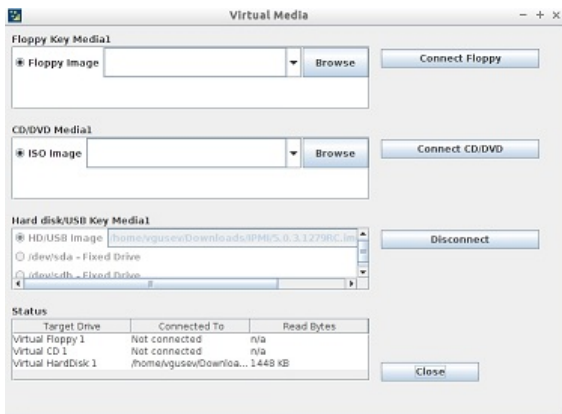
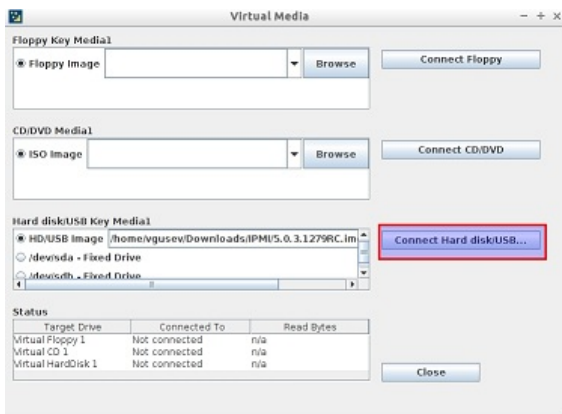
Важно! Для корректной работы с IPMI необходимо иметь на компьютере установленную 32-х битную версию ПО Java.

3. Перейдите в раздел **Media → Virtual Media Wizard**.

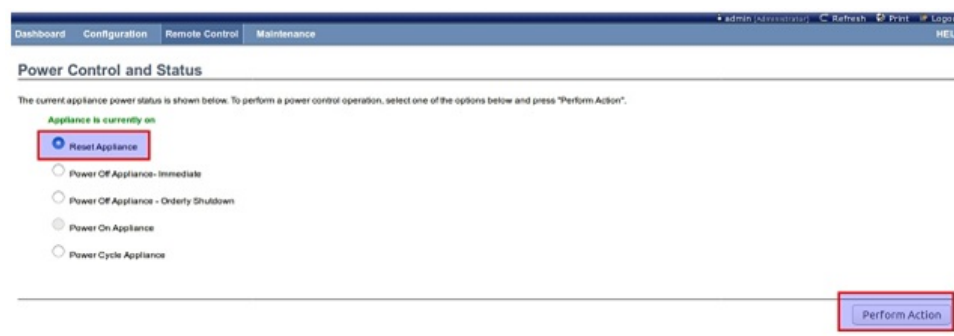
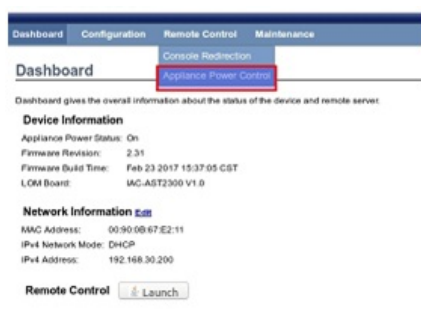


4. Выберите сохраненный ранее имидж USB-накопителя и подключите USB Key Media.

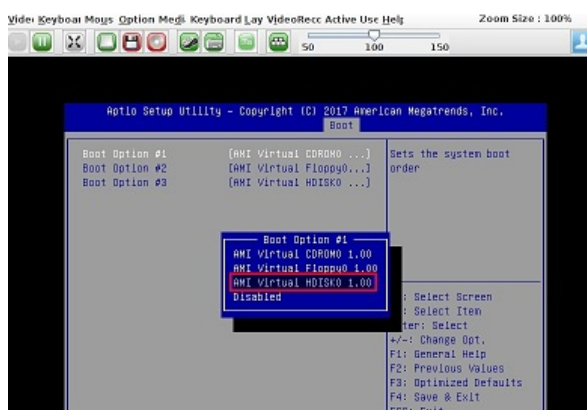


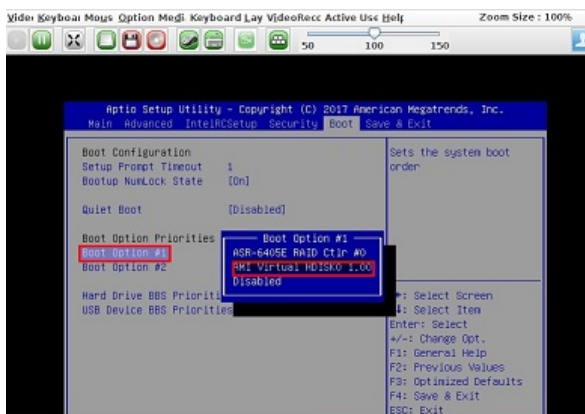


5 Перезагрузите устройство. Для этого выберите **Remote Control → Appliance Power Control → Reset Appliance** и нажмите **Perform action**.



6. Во время загрузки устройства нажмите клавишу Delete и зайдите в BIOS. Установите загрузку устройства с образа с Ghost4Linux:





После перезагрузки устройство начнет загрузаться с имиджа USB-накопителя.

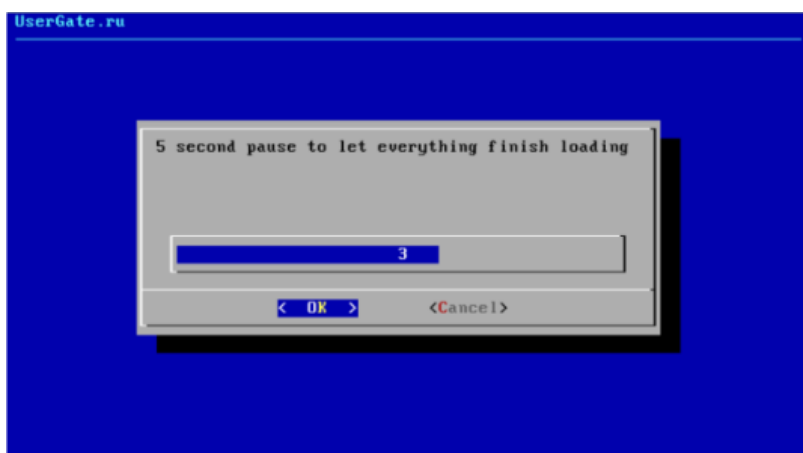
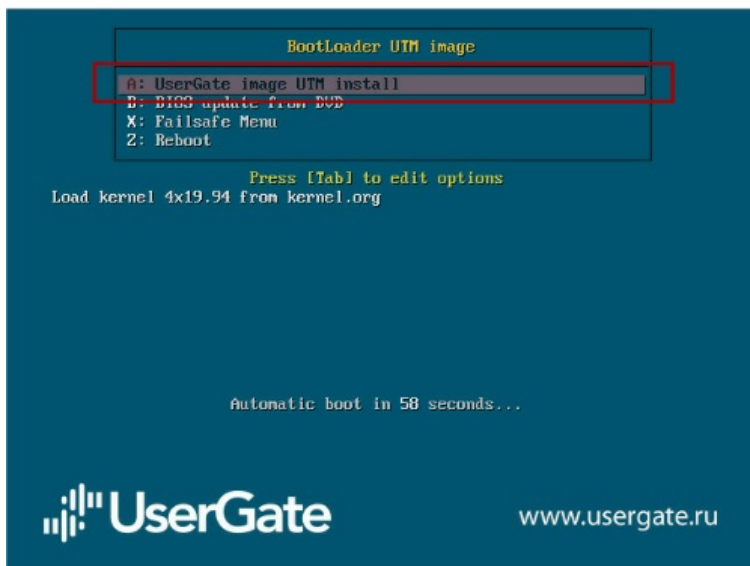
Для продолжения процедуры установки ПО перейдите к этапу [распаковки образа ПО на аппаратной платформе](#).

Распаковка образа ПО на аппаратной платформе

Важно! Для проведения процедуры распаковки образа нельзя использовать компьютер, подключенный через консольный порт к ПАК UserGate, поскольку в консольных программах (putty, securecrt и т. п.) не отображается меню настроек, описанное в этом разделе. Процедура корректно работает только при подключении к ПАК с помощью монитора и USB-клавиатуры (подробнее в главе [Загрузка образа ПО через консольное подключение](#)) или через IPMI (подробнее в главе [Загрузка образа ПО через IPMI](#)).

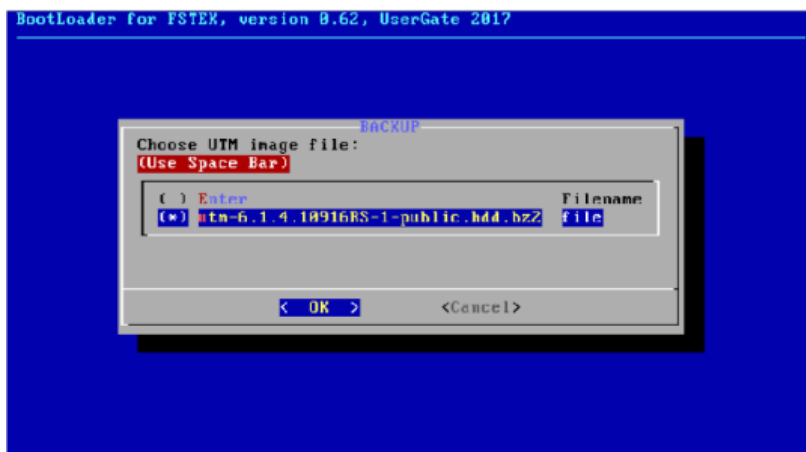
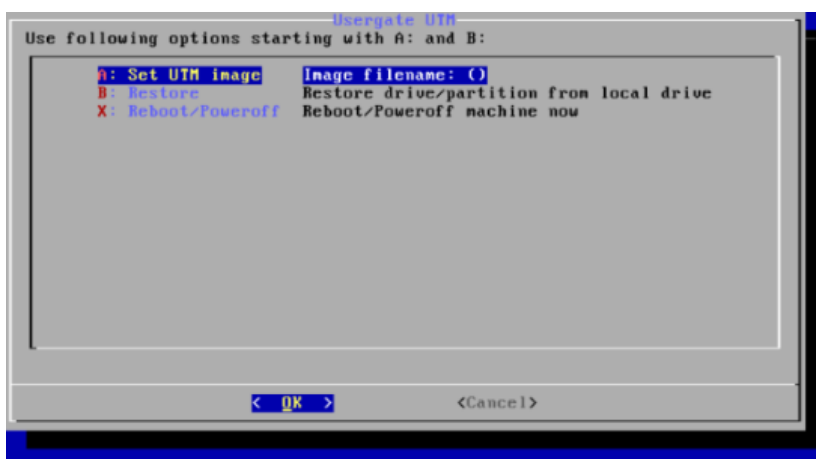
Для распаковки образа ПО выполните следующие шаги:

1. В Boot Menu выберите **UserGate image UTM install** и дождитесь окончания загрузки.

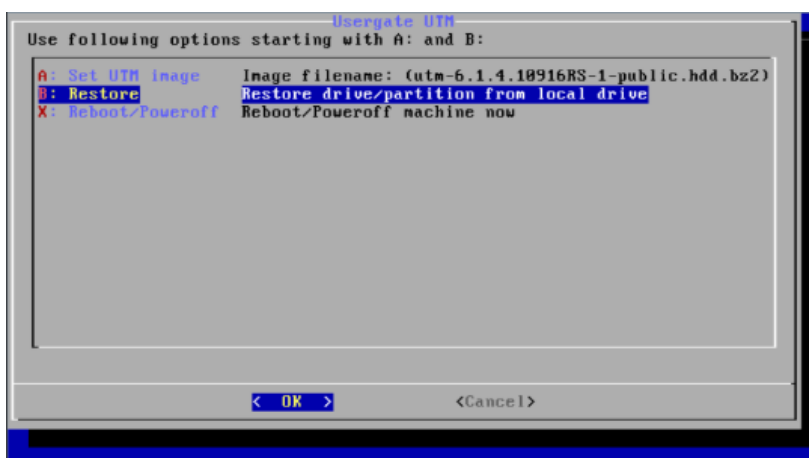


2. Выберите пункт меню **Set UTM image** и в следующем окне при помощи клавиши Space выберите образ ПО:

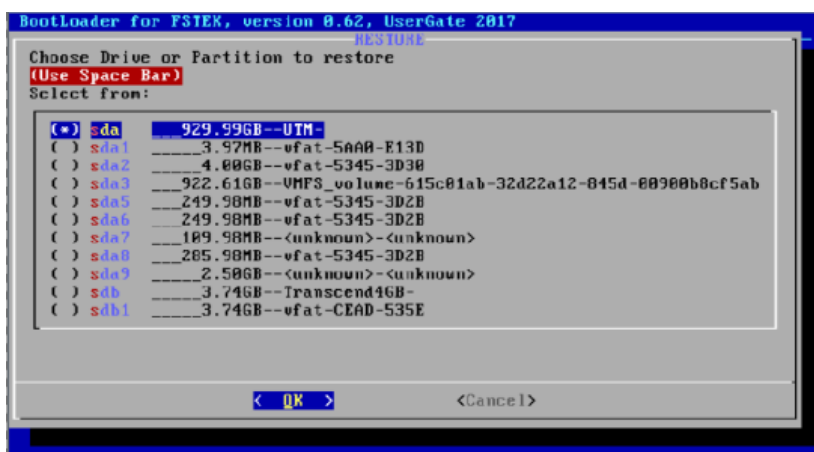
- utm-6.<НОМЕР-ВЕРСИИ>-public.hdd.bz2 — для версий 6.x;
- ngfw-x86-64-<НОМЕР-ВЕРСИИ>-release-public.hdd.bz2 — для версий 7.x.



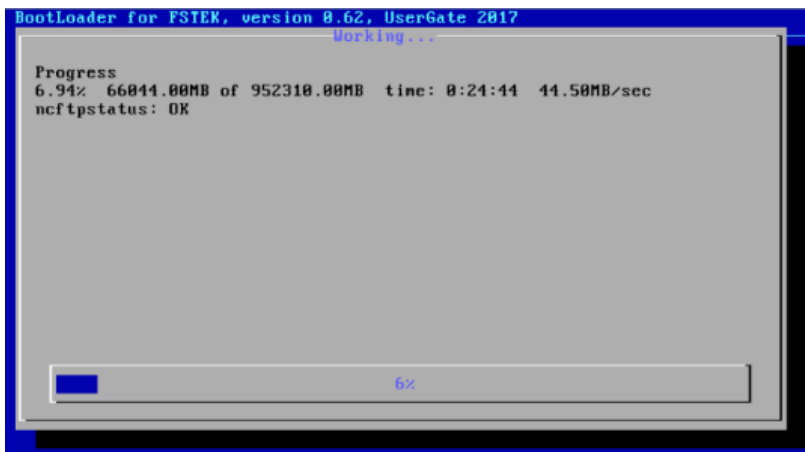
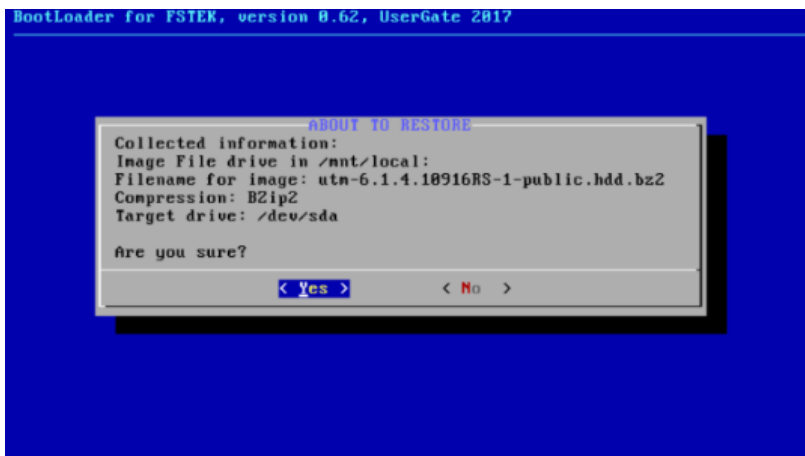
3. Выберите пункт меню **Restore**.



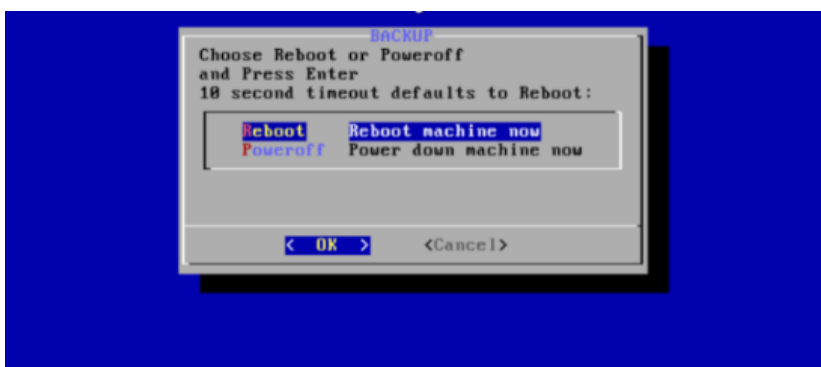
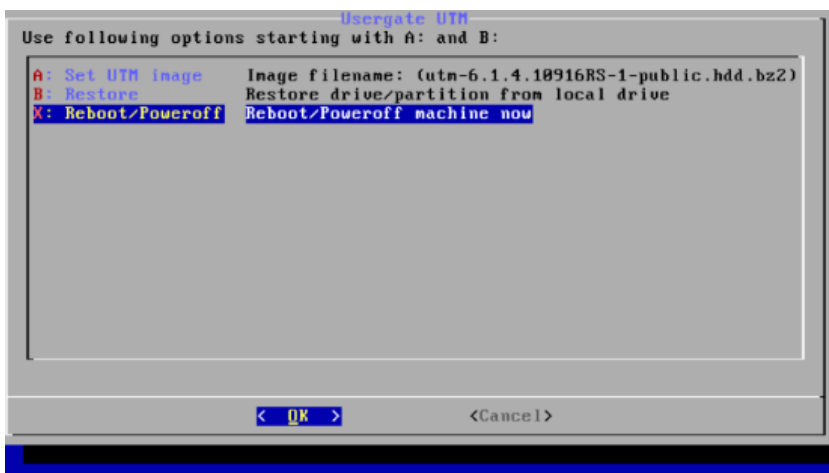
4. Выберите физический диск (например, sda), на котором будет развернут образ ПО.



5 После подтверждения действий начнется распаковка образа.

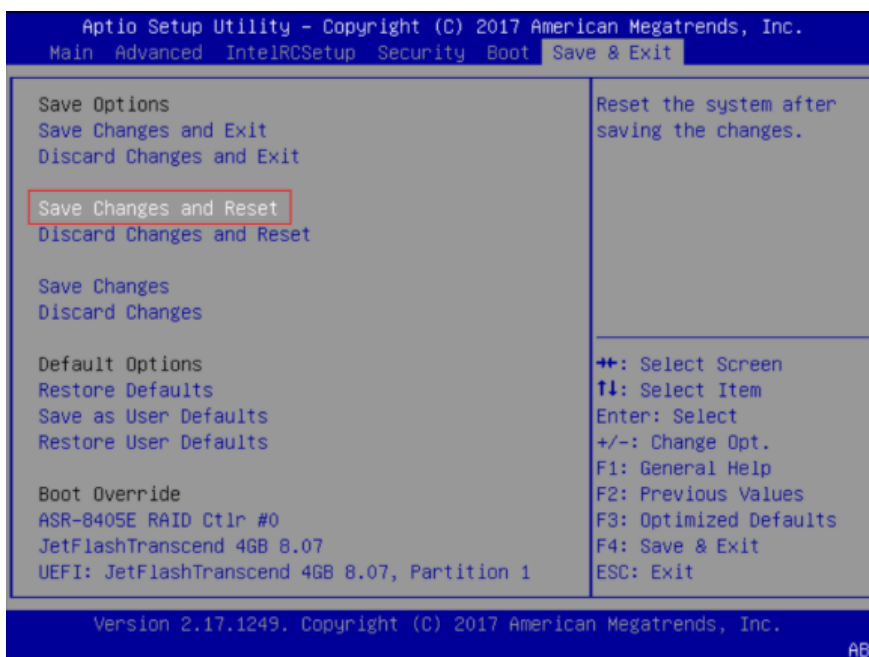
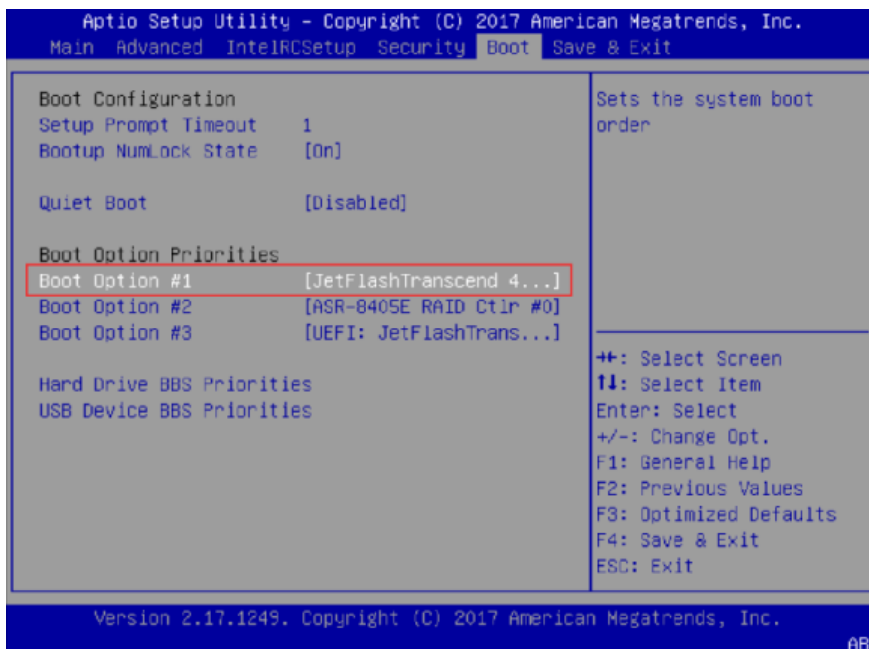


6. После окончания установки перезагрузите устройство, выбрав пункт меню **Reboot/Poweroff**.



7. При загрузке устройства войдите в BIOS и на вкладке **Boot** установите загрузку с жесткого диска.

Если на вкладке **Boot** отсутствует раздел **USB Device BBS Priorities**, перейдите в раздел **Hard Drive BBS Priorities** и выберите жесткий диск в опции **Boot Option #1**.



Важно! В настройках BIOS параметр BMC Support в разделе Server MGMT должен оставаться в отключенном состоянии (Disabled). Удаленное управление устройством через IPMI при этом доступно.

Установка ПО UserGate на аппаратных платформах E1010, E3010, F8010

Product: UserGate NGFW

Важно! Процедура, описанная в этой статье, применима только к аппаратным платформам UserGate E1010, E3010, F8010.

Процедура установки ПО UserGate на аппаратных платформах E1010, E3010, F8010 состоит из следующих этапов:

1. Загрузка образа ПО на аппаратную платформу. Загрузку можно выполнить **одним** из двух способов:
 - а) с помощью [консольного подключения](#);
 - б) с помощью [подключения через IPMI](#).
2. [Распаковка образа ПО](#) на аппаратной платформе.

Примечание Если вы выполняете обновление версии ПО на устройстве с помощью метода чистой установки, перед началом обязательно сохраните (экспортируйте) параметры настройки устройства, а после завершения установки восстановите (импортируйте) ранее сохраненные параметры.

Загрузка образа ПО с помощью консольного подключения

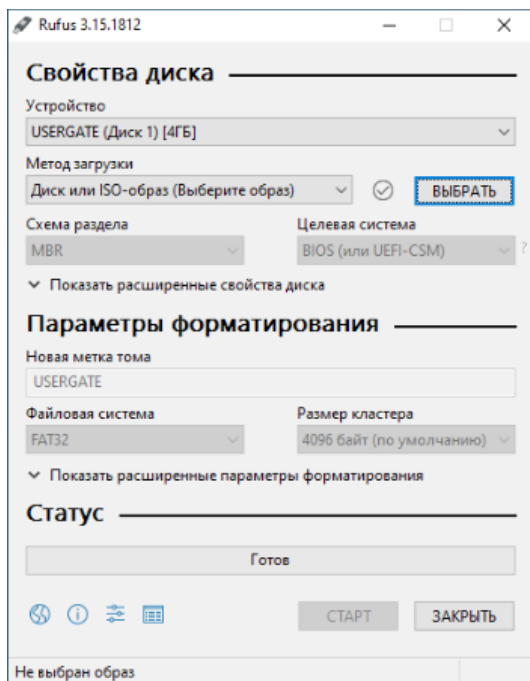
Если вы выбрали способ загрузки образа ПО на аппаратную платформу с помощью консольного подключения, вам необходимо:

1. [Создать загрузочный USB-носитель](#) с образом ПО UserGate.
2. [Загрузить образ ПО](#) на аппаратную платформу.

Создание загрузочного USB-носителя с образом ПО UserGate

Для создания загрузочного USB-носителя:

1. Загрузите файл образа прошивки ПО [из личного кабинета UserGate](#) (необходима авторизация в личном кабинете), либо запросите его в службе технической поддержки UserGate.
2. Загрузите образ установочного носителя [по ссылке](#) (md5hash: 2a61c4d41bf9a5da9f12bbdac65fb0cc, ufix: 191C6251).
3. Скачайте [ПО Rufus](#) и запустите его.
4. Настройте Rufus, указав следующие параметры:
 - **Устройство:** выберите USB-носитель, на который будет записан образ.
 - **Метод загрузки:** выберите «Диск или ISO-образ».
 - Нажмите **Выбрать** и укажите загруженный на шаге 2 файл образа установочного носителя `usergate_light_image.iso`.



- Нажмите **Старт** для создания установочного носителя.
4. Когда установочный носитель будет создан, скопируйте образ прошивки ПО, полученный в личном кабинете UserGate, либо предоставленный службой технической поддержки, и сохраните его в директории `/utm_image` на подготовленном загрузочном USB-носителе.

Перейдите к загрузке образа ПО на аппаратную платформу.

Загрузка образа ПО на аппаратную платформу

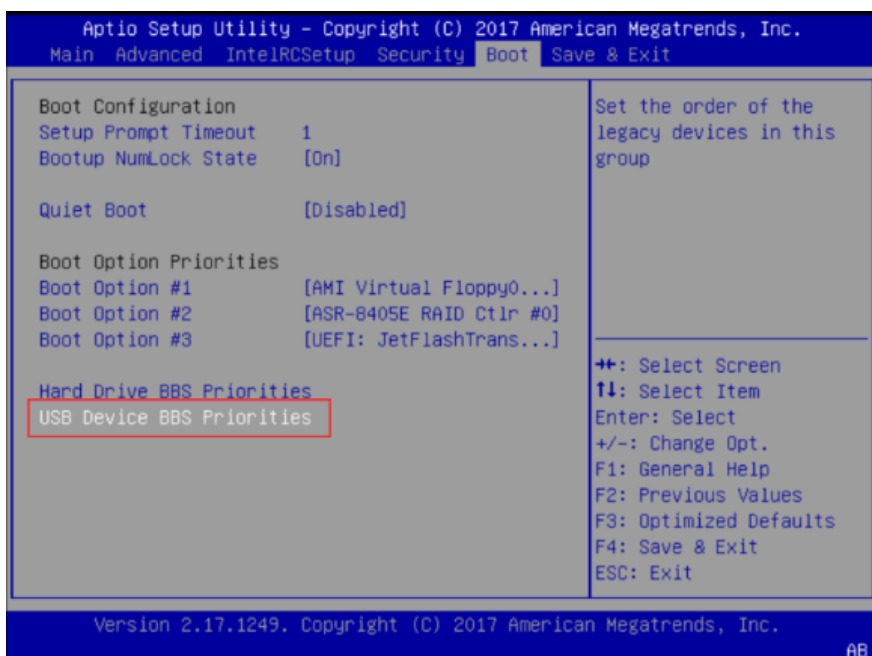
Для загрузки образа выполните следующие шаги:

1. Подключите к устройству (ПАК UserGate) внешний монитор и USB-клавиатуру.

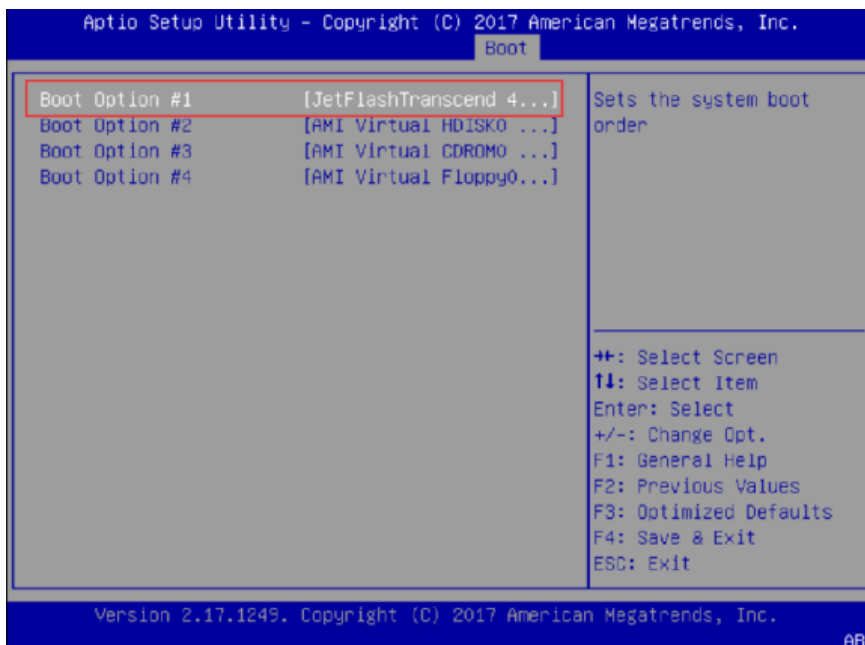
2. Войдите в BIOS устройства. Для этого включите устройство и нажмите клавишу Delete после появления на экране следующего оповещения.



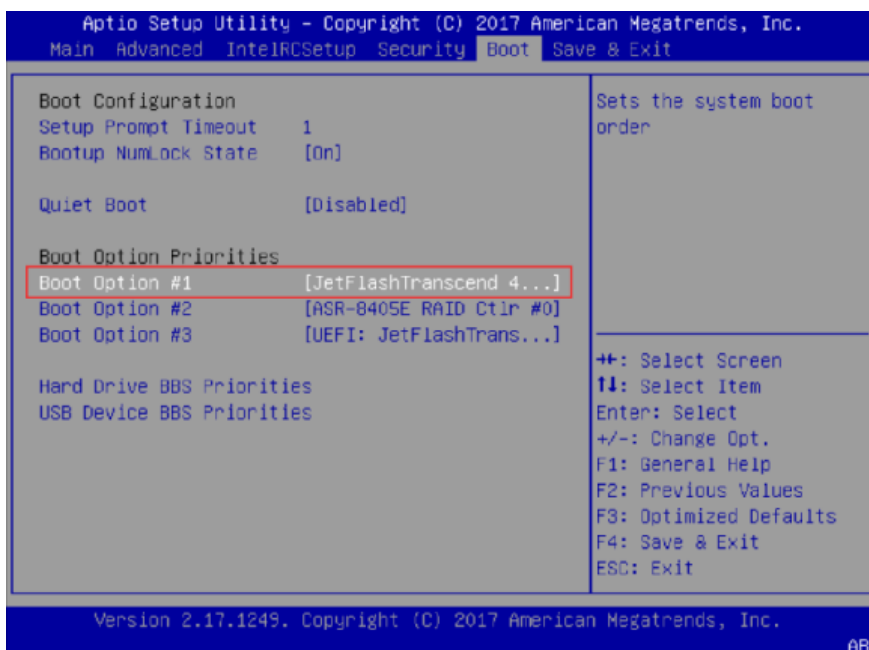
3. На вкладке **Boot** перейдите в раздел **USB Device BBS Priorities**; если такой раздел отсутствует, перейдите в раздел **Hard Drive BBS Priorities**.



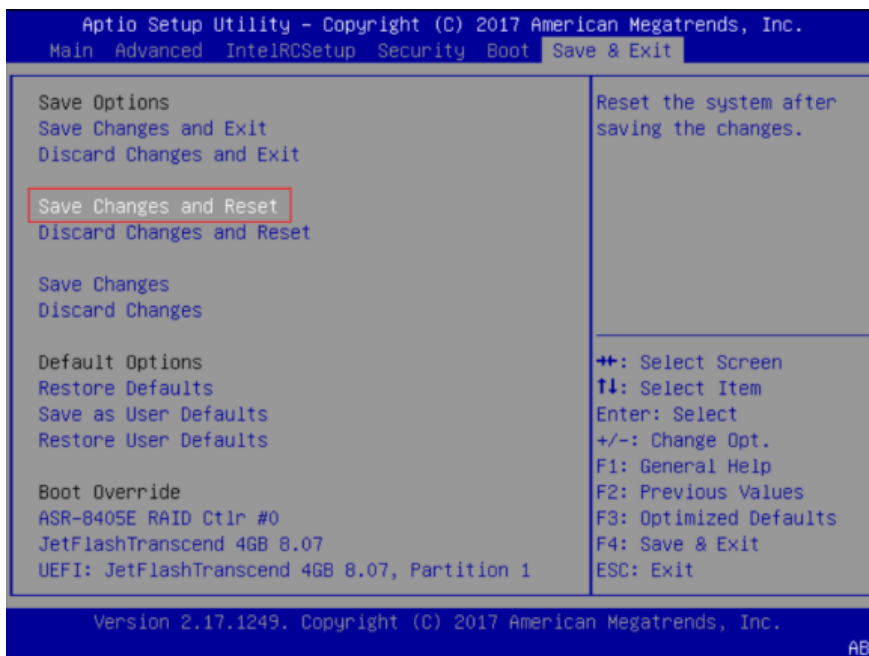
4. В параметре **Boot Option #1** выберите USB-носитель с Ghost4Linux. Общее количество Boot-опций может отличаться на разных устройствах.



5. Вернитесь в предыдущее меню и установите приоритет загрузки устройств. В параметре **Boot Option #1** выберите USB-накопитель с Ghost4Linux (не UEFI раздел).



6 Перейдите на вкладку **Save & Exit** и выберите команду **Save Changes and Reset**.



После перезагрузки устройство начнет загружаться с USB-накопителя.

Для продолжения процедуры установки ПО перейдите к этапу [распаковки образа ПО на аппаратной платформе](#).

Загрузка образа ПО с помощью подключения через IPMI

Если вы выбрали способ загрузки образа ПО на аппаратную платформу с помощью подключения через IPMI, вам необходимо:

1. [Создать загрузочный образ](#) ПО UserGate.
2. [Загрузить образ ПО](#) на аппаратную платформу.

Создание загрузочного образа ПО UserGate

Для создания загрузочного образа ПО UserGate:

1. Загрузите файл `ugbmc.iso` по [ссылке](#).
2. Загрузите файл для чистой установки UserGate ПАК с расширением `.bz2` [из личного кабинета UserGate](#).
2. Загрузите ПО UltraISO [по ссылке](#) и запустите его.
3. В приложении UltraISO перейдите в пункт меню **Файл → Открыть файл-образ**, или нажмите комбинацию клавиш **Ctrl+O**. Выберите загруженный на первом шаге файл `ugbmc.iso`.
4. Выберите папку `utm_image`:

5. Добавьте загруженный из личного кабинета на втором шаге файл с ПО UserGate (`*.bz2`) и переместите его в правую область окна:

6. Сохраните имидж, для чего перейдите пункт меню **Файл → Сохранить как**.

Перейдите к загрузке образа ПО на аппаратную платформу.

Загрузка образа ПО на аппаратную платформу

Для загрузки образа выполните следующие шаги:

1. Подключитесь к IPMI (для настройки используйте [Руководство по управлению устройствами UserGate с помощью IPMI](#)).
2. Запустите KVM кнопкой **Start KVM**:

3. Выберите сохраненный ранее образ в правом верхнем углу окна (**Browse File**):

4. Нажмите **Start Media** в правом верхнем углу окна.

5. Перезагрузите устройство, выбрав в меню Power → Hard Reset:

6. При загрузке устройства нажмите клавишу Delete, чтобы зайти в BIOS:

7. Перейдите на вкладку **Save & Exit** и выберите пункт **LNR Virtual CDROM 1.00**:

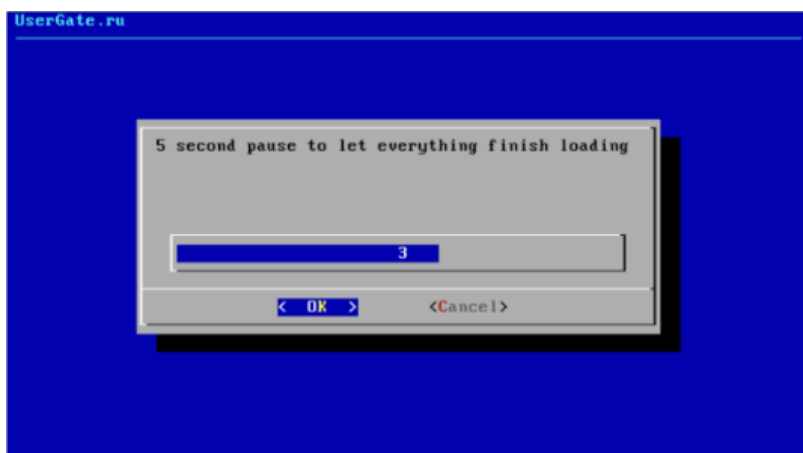
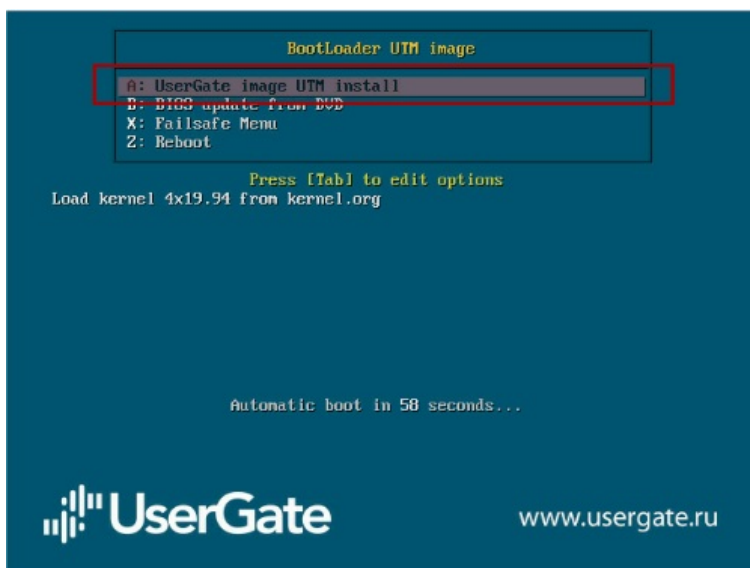
Для продолжения процедуры установки ПО перейдите к этапу [распаковки образа ПО на аппаратной платформе](#).

Распаковка образа ПО на аппаратной платформе

Важно! Для проведения процедуры распаковки образа нельзя использовать компьютер, подключенный через консольный порт к ПАК UserGate, поскольку в консольных программах (putty, securecrt и т. п.) не отображается меню настроек, описанное в этом разделе. Процедура корректно работает только при подключении к ПАК с помощью монитора и USB-клавиатуры (подробнее в главе [Загрузка образа ПО с помощью консольного подключения](#)) или через IPMI (подробнее в главе [Загрузка образа ПО с помощью подключения через IPMI](#)).

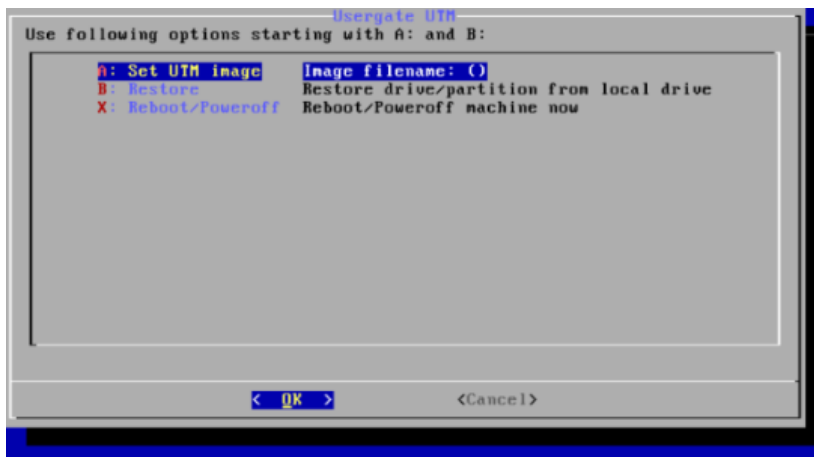
Для распаковки образа ПО выполните следующие шаги:

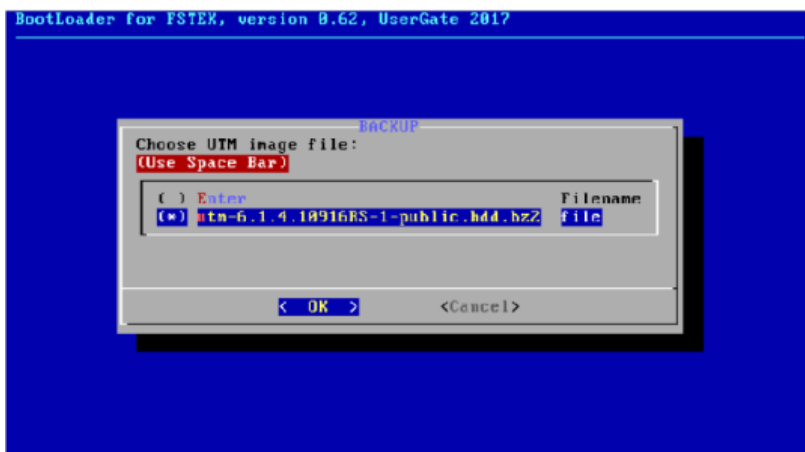
1. В Boot Menu выберите **UserGate image UTM install** и дождитесь окончания загрузки.



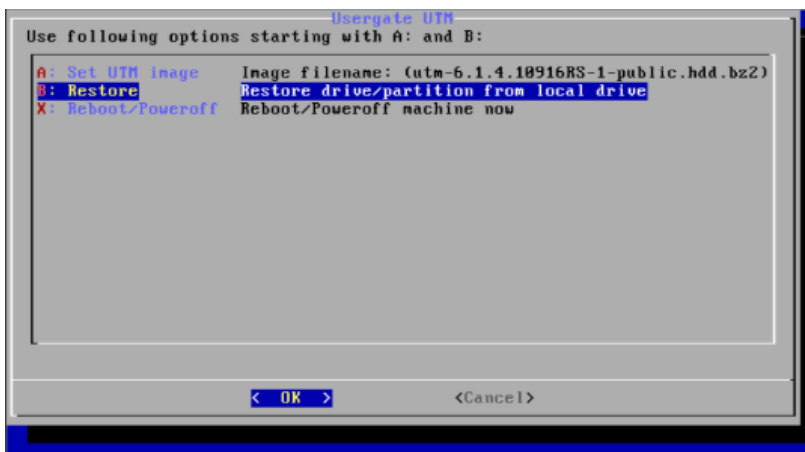
2. Выберите пункт меню **Set UTM image** и в следующем окне при помощи клавиши Space выберите образ ПО:

- ngfw-x86-64-<НОМЕР-ВЕРСИИ>-release-public.hdd.bz2 — для версий 7.x.



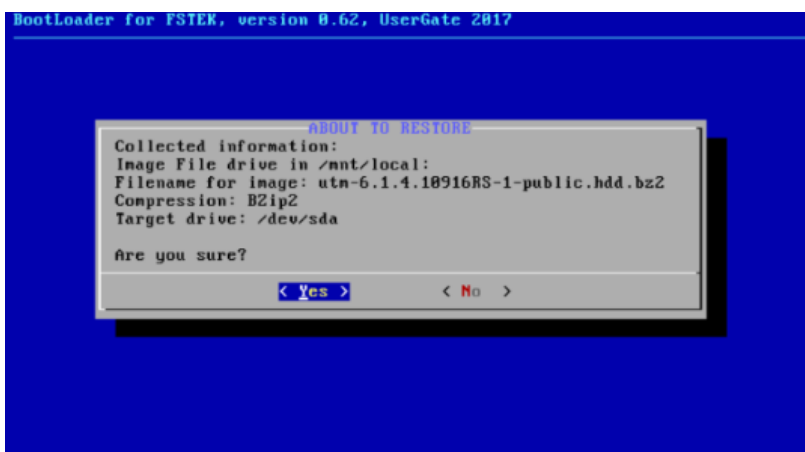


3. Выберите пункт меню **Restore**.



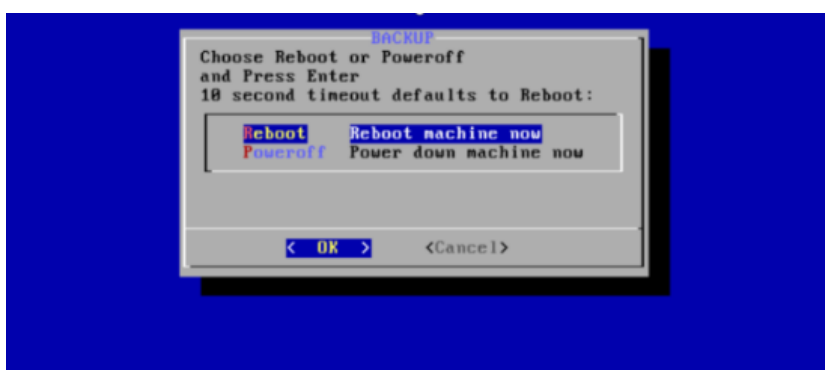
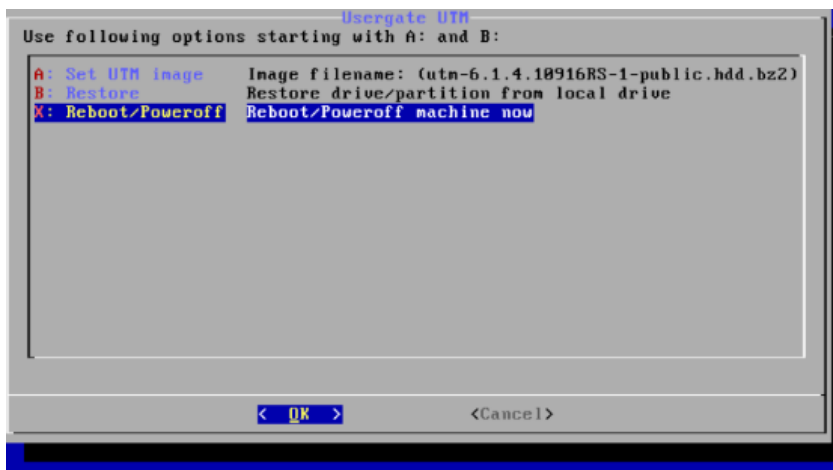
4. Выберите физический диск, на котором будет развернут образ ПО.

5 После подтверждения действий начнется распаковка образа.



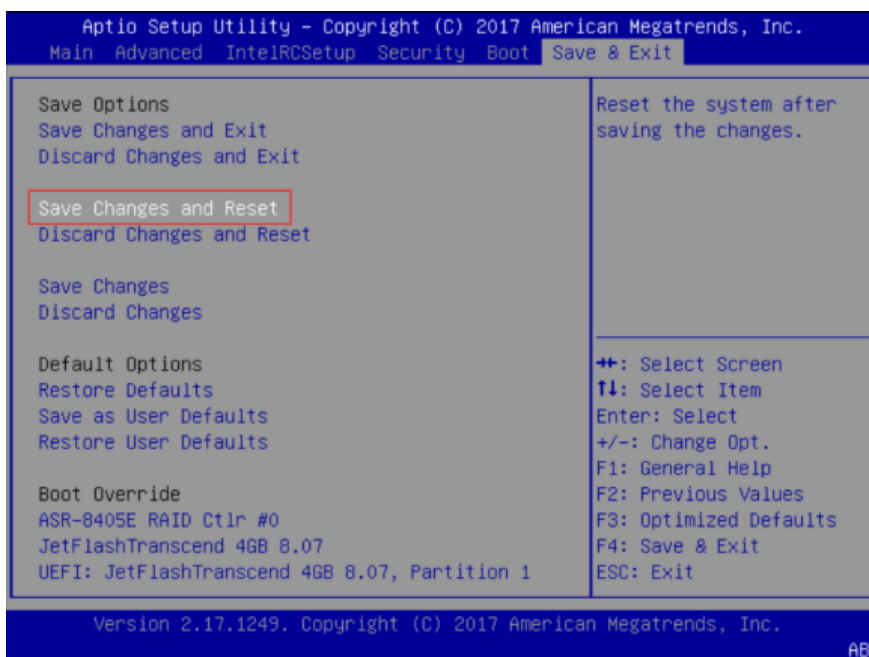
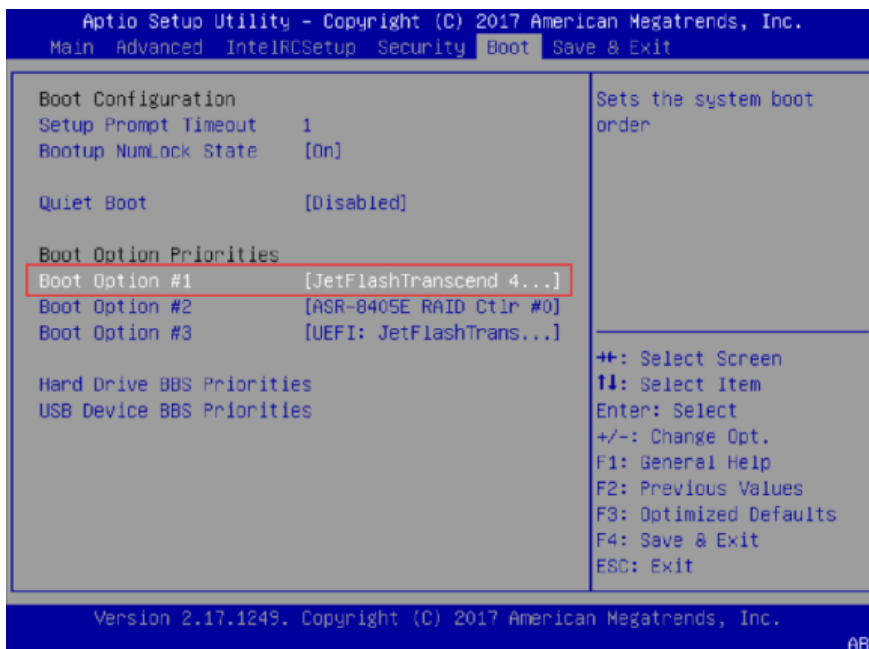


6. После окончания установки перезагрузите устройство, выбрав пункт меню **Reboot/Poweroff**.



7. При загрузке устройства войдите в BIOS и на вкладке **Boot** установите загрузку с жесткого диска.

Если на вкладке **Boot** отсутствует раздел **USB Device BBS Priorities**, перейдите в раздел **Hard Drive BBS Priorities** и выберите жесткий диск в опции **Boot Option #1**.



Важно! В настройках BIOS параметр BMC Support в разделе Server MGMT должен оставаться в отключенном состоянии (Disabled). Удаленное управление устройством через IPMI при этом доступно.

Version: 7.x

Product: UserGate NGFW

Documentation: 

Некоторые модели аппаратных платформ UserGate оснащены модулем PMC (Platform Management Controller), предназначенным для мониторинга состояния платформы и управления ее аппаратными компонентами.

Если устройство становится недоступным по основному интерфейсу управления, доступ к модулю PMC можно получить одним из следующих способов:

- через выделенный сетевой интерфейс MGMT в режиме PMC CLI;
- через консольный порт USB Type-C.

С помощью PMC можно обновить все программные компоненты программно-аппаратного комплекса (ПАК), за исключением основного образа продукта (UGOS).

Программные компоненты устройства:

- `pmc` — основная прошивка модуля PMC. Используется для мониторинга состояния платформы и управления ее аппаратными компонентами.
- `pmc-backup` — резервная прошивка PMC. Может быть загружена из режима загрузчика с помощью команды `autoboot backup`. Для обновления используется тот же образ прошивки, что и для компонента `pmc`.
- `boot` — загрузчик (bootloader) хост-процессора платформы. Выполняет начальную инициализацию оборудования и запуск операционной системы.
- `sys-recovery` — минимальный образ UGOS, предназначенный для первоначальной установки основного образа системы, а также для аварийного восстановления работоспособности устройства.
- `pcrptc` — прошивка контроллера PMC, установленного на сетевой плате. Присутствует только на платформе UserGate FG. Во время обновления этого компонента временно отключаются все вторичные источники питания платформы.

Для подключения к PMC с помощью SSH через интерфейс MGMT потребуется эмулятор терминала (например, `minicom` или `PuTTY`). При первичной инициализации используйте IP-адрес по умолчанию: 192.168.1.2.

Подробнее о PMC CLI — в разделе [Интерфейс командной строки PMC](#).

Обновление программных компонентов устройств через PMC можно выполнить одним из двух способов:

- с помощью [утилиты TFTP](#);
- с помощью [утилиты SCP](#).

Обновление основного образа продукта можно выполнить с помощью [процедуры sys-recovery](#) или штатными средствами продукта в разделе обновления ПО в веб-интерфейсе.

Обновление программных компонентов через PMC с использованием утилиты TFTP

Для обновления программных компонентов с помощью утилиты TFTP:

1. Настройте TFTP-сервер в сети, доступной через интерфейс MGMT.
2. Скачайте [в личном кабинете](#) архив («Файл для чистой установки UserGate на ПАК типа C150 и FG, версия 7.x.x.xxxxxx») и извлеките из папки `images` файлы прошивок:
 - `pmc-main-<model>-7.x.x.xxx.img`;
 - `ugos-ugls-Model-C-recovery-7.x.x.xxx.img`;
 - `ugos-ugls-Model-C-boot-7.x.x.xxx.img`.

Примечание Версии прошивок `ugos-ugls-Model-C-recovery` и `ugos-ugls-Model-C-boot` и версия операционной системы UGOS должны совпадать.

3. Загрузите прошивки на TFTP-сервер.

4. Подключитесь к PMC CLI через консоль (CON) или по SSH через интерфейс MGMT. Войдите в интерфейс CLI с помощью созданного ранее логина и пароля (по умолчанию — `admin/password`; начиная с версии ПО 7.5.0 — `Admin/usergate`).

Примечание Если при подключении по SSH через интерфейс MGMT появится ошибка, необходимо загрузить сертификат. Подробнее о процедуре — в разделе [Загрузка сертификата](#).

5. Войдите в режим конфигурирования устройства. Этот пункт следует выполнять только для версий ПО старше 7.1.0:

```
PMC> configure
PMC#
```

6. Остановите процессор:

```
PMC# set platform soc stop
SoC stoped
```

7. При необходимости настройте сеть на MGMT-интерфейсе:

```
PMC# set network ip 192.168.1.2/24
Set ip address complete
PMC# set network gateway 192.168.1.1
Set gateway complete
```

PMC#

8. Проверьте установленную версию образа контроллера и сравните с последней доступной версией:

PMC> version

PMC(Main) Firmware 7.0.1 build 20R (2023-03-22 — 10:18:23)

9. Если версия прошивки не соответствует последней доступной, ее необходимо обновить. Укажите в команде настроенный ранее TFTP-сервер и файл для обновления:

```
PMC# update firmware pmc tftp 192.168.1.1 pmc-main-<model>-7.x.x.xxx.img
TFTP from server 192.168.1.1; our IP address is 192.168.1.2
Filename 'pmc-main-<model>-7.x.x.xxx.img'.
Update at QSPI offset: 0x07080000.
Updating...
```

```
Bytes transferred = 319280 (0x4DF30) in 3 seconds (103 KiB/s)
TFTP update OK
PMC#
```

10. Перезапустите устройство:

PMC# reset

Device will be reset. Continue? (y/n): y

PMC(Loader) Firmware 7.0.1 build 20R (2023-03-22 — 10:18:23)

11. Войдите в PMC CLI. Логин/пароль по умолчанию — admin/password (начиная с версии ПО 7.5.0 — Admin/usergate):

PMC login: Admin

Password:

PMC>

12. Войдите в режим конфигурирования устройства:

PMC> configure

PMC#

13. Остановите процессор:

PMC# set platform soc stop

14. Обновите образ загрузчика UGOS до последней доступной версии:

```
PMC# update firmware boot tftp 192.168.1.7 ugos-ugls-Model-C-boot-7.x.x.xxx.img
TFTP from server 192.168.1.7; our IP address is 192.168.1.2
Filename ugos-ugls-Model-C-boot-7.x.x.xxx.img.
Update at QSPI offset: 0x00000000.
Updating...
```

```
Bytes transferred = 5312345 (0x510F59) in 33 seconds (157 KiB/s)
TFTP update OK
```

15. Обновите образ sys-recovery до последней доступной версии:

```
PMC# update firmware sys-recovery tftp 192.168.1.7 ugos-ugls-Model-C-recovery-7.x.x.xxx.img
TFTP from server 192.168.1.7; our IP address is 192.168.1.2
Filename 'ugos-ugls-Model-C-recovery--7.x.x.xxx.img'.
Update at QSPI offset: 0x01000000.
Updating...
```

```
Bytes transferred = 52895516 (0x3271F1C) in 262 seconds (197 KiB/s)
TFTP update OK
```

PMC> reset

Обновление программных компонентов через PMC с использованием утилиты SCP

Для обновления программных компонентов с помощью утилиты SCP:

1. Скачайте [в личном кабинете](#) архив («Файл для чистой установки UserGate на ПАК типа C150 и FG, версия 7.x.x.xxxxxxx») и извлеките из папки images файлы прошивок:

- pmc-main-<model>-7.x.x.xxx.img,
- ugos-ugls-Model-C-recovery-7.x.x.xxx.img,
- ugos-ugls-Model-C-boot-7.x.x.xxx.img.

Примечание Версии прошивок ugos-ugls-Model-C-recovery и ugos-ugls-Model-C-boot и версия операционной системы UGOS должны совпадать.

2. Включите устройство и дождитесь его полной загрузки, или остановите запуск на этапе запуска PMC. В процессе запуска устройства функция обновления ПО недоступна.

(pmc) Hit 'Enter' key to stop autoboot: 2

Press '^]' for autoboot and connect to aux

PMC login:

3. Подключитесь к PMC CLI через консоль (CON) или по SSH через интерфейс MGMT. Войдите в интерфейс CLI с использованием созданного

ранее пользователя и пароля (по умолчанию — admin/password; начиная с версии ПО 7.5.0 — Admin/usergate):

```
PMC login: Admin
Password:
PMC>
```

Примечание Если при подключении по SSH через интерфейс MGMT появится ошибка, необходимо загрузить сертификат. Подробнее о процедуре — в разделе [Загрузка сертификата](#).

4. Войдите в режим конфигурирования устройства:

```
PMC> configure
PMC#
```

5. Настройте сетевые параметры в PMC, указав адрес и шлюз по умолчанию вручную, или включив DHCP:

```
PMC# set network dhcp on
DHCP client start complete
PMC#
```

6. Если используется DHCP, убедитесь, что параметры сети были получены:

```
PMC# show network status
-----
Network status:
IP address type: dhcp
IP address: 192.168.1.2
Gateway address: 192.168.1.1
Netmask: 255.255.255.0
-----
PMC#
```

7. Проверьте версию образа контроллера и сравните с последней доступной версией:

```
PMC> version
PMC(Main) Firmware 7.x.x build YYY
```

8. Если версия не совпадает, требуется обновить прошивку контроллера до последней доступной версии. Укажите в команде настроенный ранее на устройстве IP-адрес:

```
scp pmc-main-<model>-7.x.x.xxx.img Admin@192.168.1.2:/firmware/pmc
Admin@192.168.1.2's password:
pmc-main-<model>-7.x.x.xxx.img
100% 6144KB 249.3KB/s 00:24
```

9. Перезапустите устройство:

```
PMC# reset
Device will be reset. Continue? (y/n): y
```

```
PMC(Loader) Firmware 7.0.1 build 20R (2023-03-22 — 10:18:23)
```

10. Войдите в PMC CLI (по умолчанию — admin/password; начиная с версии ПО 7.5.0 — Admin/usergate):

```
PMC login: Admin
Password:
PMC>
```

11. Войдите в режим конфигурирования устройства:

```
PMC> configure
PMC#
```

12. Остановите процессор:

```
PMC# set platform soc stop
```

13. Обновите образ загрузчика UGOS до последней доступной версии:

```
scp ugos-ugls-Model-C-boot-7.x.x.xxx.img Admin@192.168.1.2:/firmware/boot
Admin@192.168.1.2's password:
ugos-ugls-Model-C-boot-7.x.x.xxx.img
100% 6144KB 249.3KB/s 00:24
```

14. Обновите образ sys-recovery до последней доступной версии:

```
scp ugos-ugls-Model-C-recovery-7.x.x.xxx.img Admin@192.168.1.2:/firmware/sys-recovery
Admin@192.168.1.2's password:
ugos-ugls-Model-C-recovery-7.x.x.xxx.img
100% 6144KB 249.3KB/s 00:24
```

15. Подключитесь к устройству и перезапустите его:

```
PMC# reset
Device will be reset. Continue? (y/n): y
```

```
PMC(Loader) Firmware 7.0.1 build 20R (2023-03-22 — 10:18:23)
```

Обновление UGOS через sys-recovery (с использованием внешнего TFTP/FTP/HTTP/SSH-сервера)

Эта инструкция подходит для случаев:

- когда необходимо в первый раз установить UGOS на устройство;
- необходимо полностью перезаписать образ UGOS.

Обязательные условия для обновления:

- к устройству имеется доступ по сети Ethernet;
- на устройстве установлен образ sys-recovery.

Порядок обновления:

1. Скачайте [в личном кабинете](#) архив прошивки (file for clean installing) в виде файла:
 - ngfw_uqls_full_update_7.x.x.xxxxxR.tar.gz — для моделей C150, C151, X10, D250, FG;
 - ngfw_ugrc_full_update_7.x.x.xxxxxR.tar.gz — для модели B50.
 2. Распакуйте полученный архив.
 3. В распакованном архиве перейдите в папку images.
 4. В папке images найдите файл образа UGOS в виде:
 - ngfw-uqls-7.x.x.xxx-public.ssd.gz — для моделей C150, C151, X10, D250, FG;
 - ngfw-ugrc-7.x.x.xxx-public.ssd.gz — для модели B50.
 5. Загрузите образ UGOS на TFTP-сервер.
 6. Подключитесь к PMC через консольный интерфейс (USB Type-C) или по SSH через интерфейс MGMT.
- Примечание** Если при подключении по SSH через интерфейс MGMT появится ошибка, необходимо загрузить сертификат. Подробнее о процедуре — в разделе [Загрузка сертификата](#).
7. Войдите в интерфейс CLI с использованием созданного ранее пользователя и пароля (по умолчанию — admin/password; начиная с версии ПО 7.5.0 — Admin/usergate):

```
PMC login: Admin
Password:
PMC>
```

8. Войдите в режим конфигурирования устройства:

```
PMC> configure
PMC#
```

9. Остановите работу CPU и запустить образ sys-recovery:

```
PMC# set platform soc stop
SoC stoped
PMC# autoboot recovery
Connected to CPU at speed 115200.
...
```

UGOS login:

10. Для входа используйте логин/пароль — root/root:

```
UGOS login: root
Password: root
```

11. Подключите устройство к локальной сети через интерфейс port0 и настройте IP-адрес на интерфейсе (DHCP или статический):

```
root@UGOS:~# dhclient port0
root@UGOS:~# ip ro
default via 192.168.75.1 dev port0
192.168.75.0/24 dev port0 proto kernel scope link src 192.168.75.217
root@UGOS:~#
```

12. Загрузите обновление с настроенного ранее TFTP-сервера:

```
root@UGOS:~# curl ftp://192.168.1.2/ugos/ngfw-uqls-7.x.x.xxx-public.ssd.gz -o /ugos.ssd.gz
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 766M 100 766M 0 0 2322k 0 0:05:37 0:05:37 --:--:-- 2329k
100 766M 100 766M 0 0 2322k 0 0:05:37 0:05:37 --:--:-- 2322k
root@UGOS:~#
```

13. Запишите образ на SSD-накопитель с помощью одной из следующих команд:

- для моделей C150, C151, X10, B50:

```
curl file:///ugos.ssd.gz | gzip -d | dd of=/dev/sda
```

- для моделей D250, FG:

```
curl file:///ugos.ssd.gz | gzip -d | dd of=/dev/nvme0n1
```

Пример выполнения команды на модели FG:

```
root@UGOS:~# curl file:///ugos.ssd.gz | gzip -d | dd of=/dev/nvme0n1
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
```

```
100 766M 100 766M 0 0 2015k 0 0:06:29 0:06:29 --:--:-- 507k
100 766M 100 766M 0 0 2015k 0 0:06:29 0:06:29 --:--:-- 2015k
41943040+0 records in
41943040+0 records out
21474836480 bytes (20 G) copied, 395.429293 s, 52 M/s
root@UGOS:~#
```

14. Выйдите обратно в PMC CLI с помощью нажатия комбинации клавиш **Ctrl +]**:

```
root@UGOS:~# ^]
Disconnected from CPU
```

PMC#

15. Остановите работу CPU и запустите основной образ UGOS:

```
PMC# set platform soc stop
SoC stoped
PMC# autoboot
...
UGOS login:
```

Загрузка сертификата

Если при подключении по SSH через интерфейс MGMT появится ошибка, необходимо загрузить сертификат. Загрузка сертификата осуществляется только при подключении через COM-порт.

1. Сгенерируйте сертификат для SSH:

```
openssl ecparam -genkey -name prime256v1 -noout -outform DER -out privatekey.der
```

2. Загрузите сертификат на TFTP-сервер.

3. Подключитесь к устройству через COM-порт. Перейдите в режим PMC CLI. Во время загрузки устройства при появлении строки: «(pmc) Hit 'Enter' key to stop autoboot:» нажмите Enter.

4. Обновите сертификат на устройстве с помощью TFTP-сервера. По окончании обновления перезагрузите устройство:

```
PMC> update key ssh tftp 192.168.1.7 privatekey.der
TFTP from server 192.168.1.7; our IP address is 192.168.1.2
Filename 'privatekey.der'.
Update at QSPI offset: 0x07100000.
Updating...
Bytes transferred = 121 (0x79) in 9 ms (13 KiB/s)
TFTP update OK
```

```
PMC> reset
Device will be reset. Continue? (y/n): y
```

5. После перезагрузки подключитесь через интерфейс MGMT по SSH.

```
PMC login: Admin
Password:
PMC>
```

Version: 7.x
Product: UserGate C150
Documentation: 

Установка UserGate на аппаратную платформу C150

1. Скачать архив **ngfw_ugls_full_update_7.m.n.XXX.Y.tar.gz** из личного кабинета My.UserGate (<https://my.usergate.com>).

Примечание В результате установки прошивки настройки текущей версии UserGate будут удалены, а состояние устройства сброшено до первоначальной инициализации.

USB-накопитель должен быть отформатирован в формате FAT32 как диск для хранения и переноса данных. На USB-накопителе не должно быть посторонних файлов.

2. Распаковать содержимое архива на USB-накопитель. После распаковки архива в корне накопителя должны присутствовать 2 директории - **bin** и **images** - и скрипт **full-updater.sh**.

Важно! Перед началом процедуры устройство UserGate должно быть обесточено.

3. Подключить USB-накопитель к ПАК UserGate C150.

4. Подключить консольный кабель и подать питание на устройство.

5. Остановить загрузку PMC: во время загрузки системы необходимо нажать **Enter** после второго вывода сообщения "Hit 'Enter' key to stop autoboot":

```
(pmc) Hit 'Enter' key to stop autoboot: 3
Press '^]' for autoboot and connect to aux
PMC login:
```

6. Авторизоваться под пользователем с логин/паролем: admin/password.

7. Запустить образ sys-recovery, выполнив следующую команду:

```
PMC> autoboot recovery
Connected to CPU at speed 115200.
Escape character is '^]'.
...
```

8. Дождаться запуска UGOS и авторизоваться под пользователем с логин/паролем: root/root:

```
UGOS login: root
Password:
-----
UGOS NGFW 7.0.0.138A
-----
root@UGOS:~#
```

9. Смонтировать USB-накопитель с помощью следующих команд (где: /usb — точка монтирования, где можно увидеть содержимое usb-накопителя, /dev/sdb1 — системное имя usb-накопителя, узнать имя в вашем случае можно командой fdisk -l.):

```
root@UGOS:~# mkdir -p /usb && mount /dev/sdb1 /usb
root@UGOS:~# cd /usb
```

Внимание! В процессе выполнения команды mkdir возможен вывод следующего сообщения:

[71.540684] FAT-fs (sdb1): Volume was not properly unmounted. Some data may be corrupt. Please run fsck.

Эта ошибка не является критичной, и установка может быть продолжена.

10. Запустить выполнение скрипта full-updater.sh:

```
root@UGOS:/usb# ./full-updater.sh
```

Дождаться сообщения:

```
*****
Update installed successfully. Please restart device by power.
*****
```

11. Отключить питание устройства и извлечь накопитель USB.

12. Повторно подать питание на устройство и дождаться запуска UGOS актуальной версии 7.m.n.XXX.Y:

Примечание При запуске устройство самостоятельно перезагрузится несколько раз, что является штатным поведением после выполнения полного обновления.

Лицензирование

Version: 6.x, 7.x, 7.5.x
Product: NGFW, UGMC, LogAn, SIEM, DCFW, WAF, SWG

Модель лицензирования решений UserGate включает два основных компонента:

1. Базовая лицензия (обязательная) — обеспечивает основные функциональные возможности устройства.
2. Дополнительные модули (опциональные) — позволяют активировать расширенные функции.

Базовая лицензия определяется параметрами производительности:

- для физических устройств — зависит от типа аппаратной платформы;
- для виртуальных образов — определяется количеством поддерживаемых ядер виртуальной машины.

Базовая лицензия является бессрочной (без обновлений).

Дополнительные модули можно активировать выборочно.

Модули включают регулярные обновления:

- программного обеспечения;
- встроенных библиотек и баз данных;
- сигнатур и аналитических моделей;
- экспертных правил и сервисов.

Способы активации лицензий на устройстве:

- Онлайн-активация (требуется подключение к интернету).
- Офлайн-активация (через сервис офлайн-активации ПИН-кодов).

Подробнее об особенностях лицензирования решений:

Категория продукта	Версия ПО
NGFW (New Generation Firewall)	6.x
	7.x
DCFW (Datacenter Firewall)	8.x
WAF (Web Application Firewall)	7.x
SWG (Secure Web Gateway)	7.5.x
MC (Management Center)	6.x
	7.x
LogAn (Log Analyzer)	6.x
	7.x
SIEM (Security Information and Event Management)	7.2
	7.x

