

Table of Contents

Table of Contents	1
Установка и обновление	2
Политика обновления программного обеспечения UserGate NGFW	3
Политика обновления программного обеспечения UserGate WAF	4
Обновление ПО UserGate	5
Обновление ПО кластера UserGate NGFW	7
Обновление ПАК с внешнего USB-носителя	8
Процедура перехода с UserGate 5 на UserGate 6	9
Процесс перехода на UserGate версии 7.x	10
Порядок обновления ПО UserGate LogAn	12
Развертывание образа UserGate на Hyper-V	13
Установка ПО UserGate на платформу C150	19
Обновление ПО кластера UserGate MC	20
Установка ПО UserGate на аппаратных платформах C100, D200, D500, E1000, E3000, F8000	21
Установка ПО UserGate на аппаратных платформах E1010, E3010, F8010	28
Обновление микрокода IPMI на аппаратных платформах D200, D500, E1000, E3000, F8000	39
Обновление микрокода IPMI на аппаратных платформах E1010, E3010, F8010	36
Обновление компонентов ПО с использованием PMC на аппаратных платформах B50, C150, C151, D250, FG, X10	41
Офлайн-активация лицензий	45
Экспорт и импорт настроек	49
Экспорт и импорт политик UserGate через CLI	50
Импорт настроек из файлов конфигурации кластера NGFW	52

Product: NGFW

Обновление программного обеспечения — это критически важная процедура, напрямую влияющая на безопасность, стабильность и доступность сети. Своевременная установка обновлений необходима для защиты от новых уязвимостей и получения доступа к актуальным функциям безопасности. Одним из ключевых аспектов этого процесса является соблюдение рекомендованного пути обновления.

Путь обновления — это последовательность версий ПО, через которые необходимо пройти при переходе от текущей версии системы к целевой. В некоторых случаях обновление нельзя выполнить за один шаг, потребуется последовательная установка промежуточных версий с использованием [конвертера конфигураций](#).

Рекомендованный путь обновления протестирован и гарантирует корректную миграцию конфигурации и внутренних компонентов системы при соблюдении процедуры обновления.

Таблица совместимости версий для обновления продукта

Текущая версия	Целевая версия									
	7.1.2	7.2.x	7.3.2	7.3.3	7.4.0	7.4.1	7.4.2	7.4.3	7.5.0	7.5.1
6.1.9				+		+				
7.1.2										
7.2.x										
7.3.2				+		+				
7.3.3						+		+	+	+
7.4.0						+		+		
7.4.1							+	+	+	+
7.4.2								+	+	+
7.4.3									+	+
7.5.0										+

Прямое обновление программного обеспечения до целевой версии рекомендуется выполнять с совместимых версий. Обновление с остальных версий возможно только после предварительного обновления до указанных совместимых версий в соответствии с данной таблицей.

Варианты обновления программного обеспечения

Обновление программного обеспечения UserGate NGFW может быть выполнено следующими способами:

- Прямое обновление штатными средствами продукта. Обновление возможно для версий, указанных [в таблице совместимости](#). Подробнее — в разделе «[Обновление ПО UserGate](#)».
- Чистая установка с импортом конфигурации. Если устройство не используется в продуктивной среде, возможна чистая установка целевой версии программного обеспечения с переносом конфигурации с помощью конвертера конфигурации.

Подробнее о конвертере — в разделе «[Конвертер конфигураций UserGate](#)».

Подробнее о чистой установке ПО UserGate на аппаратных платформах:

- «[Установка ПО UserGate на аппаратных платформах C100, D200, D500, E1000, E3000, F8000](#)»;
- «[Установка ПО UserGate на аппаратных платформа E1010, E3010, F8010](#)»;
- «[Обновление компонентов ПО с использованием PMC на аппаратных платформах B50, C150, C151, D250, FG](#)».

Общие рекомендации по обновлению программного обеспечения

Чтобы минимизировать риски при обновлениях, рекомендуется:

- Проверить текущую и целевую версии ПО устройства.
- Ознакомиться с информацией о версиях в разделе «[Описание версий](#)».
- Сделать [резервную копию конфигурации устройства](#), чтобы в случае возникновения проблем во время обновления можно было восстановить его предыдущее состояние.
- Во время установки обновления создать [точку восстановления системы](#). Это позволит оперативно вернуть систему в рабочее состояние.

В случае возникновения аварийной ситуации при обновлении обратиться в службу технической поддержки.

Обновление до версии 7.5.1

Прямое обновление до версии 7.5.1 возможно с версий 7.3.3, 7.4.1, 7.4.2, 7.4.3 и 7.5.0.

Обновление с остальных версий возможно только после предварительного последовательного обновления до одной из перечисленных выше версий в соответствии [с таблицей совместимости](#).

Version: 7.6.x
Product: WAF

Обновление программного обеспечения — это критически важная процедура, напрямую влияющая на безопасность, стабильность и доступность сети. Своевременная установка обновлений необходима для защиты от новых уязвимостей и получения доступа к актуальным функциям безопасности. Одним из ключевых аспектов этого процесса является соблюдение рекомендованного пути обновления.

Путь обновления — это последовательность версий ПО, через которые необходимо пройти при переходе от текущей версии системы к целевой. В некоторых случаях обновление нельзя выполнить за один шаг, потребуется последовательная установка промежуточных версий.

Рекомендованный путь обновления протестирован и гарантирует корректную миграцию конфигурации и внутренних компонентов системы при соблюдении процедуры обновления.

Таблица совместимости версий для обновления продукта

Текущая версия	Целевая версия					
	7.3.1	7.4.0	7.4.1	7.5.0	7.6.0	7.7.0
7.3.0	+	+				
7.3.1		+	+			
7.4.0			+	+		
7.4.1				+	+	
7.5.0					+	+
7.6.0						+

Прямое обновление программного обеспечения до целевой версии рекомендуется выполнять с совместимых версий. Обновление с остальных версий возможно только после предварительного обновления до указанных совместимых версий в соответствии с данной таблицей.

Варианты обновления программного обеспечения

Обновление программного обеспечения UserGate WAF может быть выполнено следующими способами:

- Прямое обновление штатными средствами продукта. Обновление возможно для версий, указанных [в таблице совместимости](#). Подробнее — в разделе «[Обновление ПО UserGate](#)».
- Чистая установка с импортом конфигурации. Если устройство не используется в продуктивной среде, возможна чистая установка целевой версии программного обеспечения с переносом конфигурации.

Подробнее о чистой установке ПО UserGate на аппаратных платформах:

- «[Установка ПО UserGate на аппаратных платформах C100, D200, D500, E1000, E3000, F8000](#) »;
- «[Установка ПО UserGate на аппаратных платформа E1010, E3010, F8010](#) ».

Общие рекомендации по обновлению программного обеспечения

Чтобы минимизировать риски при обновлениях, рекомендуется:

- Проверить текущую и целевую версии ПО устройства.
- Ознакомиться с информацией о версиях в разделе «[Описание версий](#)».
- Сделать [резервную копию конфигурации устройства](#), чтобы в случае возникновения проблем во время обновления можно было восстановить его предыдущее состояние.
- Во время установки обновления создать [точку восстановления системы](#). Это позволит оперативно вернуть систему в рабочее состояние.

В случае возникновения аварийной ситуации при обновлении обратитесь в службу технической поддержки.

Обновление до версии 7.6.0

Прямое обновление до версии 7.6.0 возможно с версии 7.4.1 или 7.5.0.

Обновление с остальных версий возможно только после предварительного последовательного обновления до одной из перечисленных выше версий в соответствии [с таблицей совместимости](#).

Version: 6.1.9, 7.x, 7.0.1

Команда UserGate постоянно работает над улучшением качества своего программного обеспечения и предлагает обновления продуктов UserGate в рамках подписки на модуль лицензии Security Update.

Обновление ПО

При наличии обновлений в разделе **Управление устройством** → **Операции с сервером** отобразится соответствующее оповещение. Обновление продукта может занять довольно длительное время, рекомендуется планировать установку обновлений с учетом возможного времени простоя UserGate.

Порядок установки обновлений:

1. Создайте резервную копию устройства. Наличие резервной копии позволит восстановить предыдущее состояние устройства в случае возникновения каких-либо проблем во время применения обновлений.
2. Установите обновление. В разделе **Управление устройством** при наличии оповещения **Доступны новые обновления** нажмите **Установить сейчас**. Система установит скачанные обновления, по окончании установки устройство будет перезагружено.

Важно! Для корректного обновления кластера конфигурации необходимо, чтобы все узлы были включены и доступны на момент обновления первого узла.

Офлайн-обновление ПО

В случае, если устройства UserGate не имеют доступа в интернет, вы можете выполнить офлайн-обновление программного обеспечения. Файлы для обновления доступны в личном кабинете [по ссылке](#) (требуется авторизация).

Для загрузки файлов на устройство UserGate:

1. В веб-интерфейсе устройства на вкладке **Настройки** перейдите в раздел **UserGate** → **Управление устройством**, в разделе **Операции с сервером** найдите **Офлайн обновление** и нажмите **Загрузить файл**.
2. Выберите файл обновления, загруженный из личного кабинета.
3. После загрузки файла отобразится соответствующее уведомление. Установите обновление (нажмите **Установить сейчас**).

Обновление может занять довольно длительное время, рекомендуется планировать установку обновлений с учетом возможного времени простоя устройства. После установки обновлений устройство UserGate будет перезагружено. Запись об установке обновления будет отображена в журнале событий (вкладка **Журналы и отчёты**, раздел **Журналы** → **Журнал событий**).

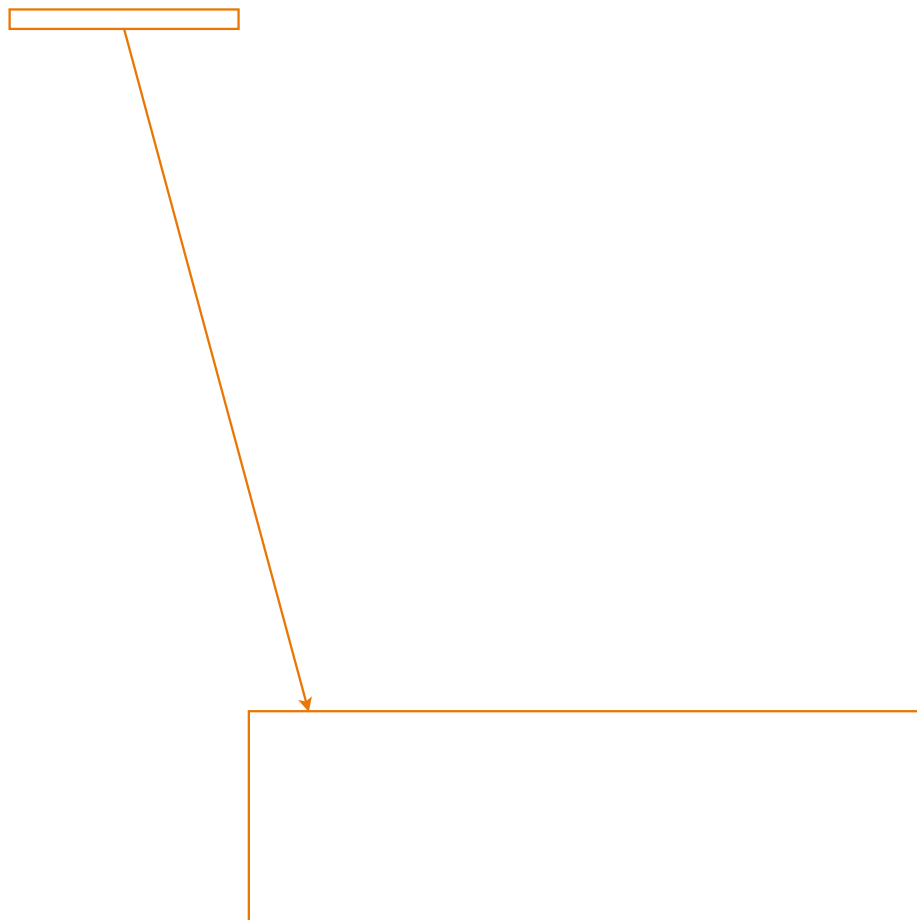
Обновление библиотек

Для загрузки файлов обновлений на устройство UserGate:

1. В веб-интерфейсе устройства на вкладке **Настройки** перейдите в раздел **UserGate** → **Управление устройством**, в блоке **Операции с сервером** найдите **Офлайн обновление** и нажмите **Загрузить файл**.
2. Выберите файл обновления, загруженный из личного кабинета. Обновление библиотек производится автоматически. Записи об обновлении списков появятся в журнале событий (вкладка **Журналы и отчёты**, раздел **Журналы** → **Журнал событий**).

Центр обновлений

Важно! Начиная с версии 7.1.2 управление обновлением ПО в веб-консоли устройства находится в разделе «UserGate» → «Настройки» → «Центр обновлений».



Примечание Рекомендуется создать резервную копию состояния UserGate, которая позволит восстановить предыдущее состояние устройства в случае возникновения каких-либо проблем во время применения обновлений.

Обновление ПО

Для установки обновлений на устройство UserGate:

1. В веб-консоли устройства на вкладке **Настройки** перейдите в раздел **UserGate → Настройки → Центр обновлений → Обновление ПО → Обновление** и нажмите **Проверить обновления**.
2. Если имеются обновления, они отобразятся в открывшемся окне проверки обновлений. Выберите нужную версию обновления и нажмите **Скачать**.
3. Когда обновление будет скачано на устройство, запустите установку обновления. При установке обновления можно задать точку восстановления устройства.

Обновления библиотек устанавливаются аналогичным образом через подраздел **Обновления библиотек**, или с помощью настройки автоматического обновления.

Подробнее об опциях обновления в версиях ПО 7.x — в разделе « [Общие настройки](#) » Руководства администратора.

Офлайн-обновление ПО

Для загрузки файлов обновлений на устройство UserGate:

1. В веб-консоли устройства на вкладке **Настройки** перейдите в раздел **UserGate → Настройки → Центр обновлений → Обновление ПО → Офлайн обновление** и нажмите **Загрузить файл**.
2. Выберите файл обновления, загруженный из личного кабинета и установите обновление.

Подробнее об опциях обновления в версиях ПО 7.x — в разделе « [Общие настройки](#) » Руководства администратора.

Обновление ПО кластера UserGate NGFW

Version: 5.x, 6.x, 7.x

Product: UserGate NGFW

Для корректного обновления кластера конфигурации необходимо, чтобы все узлы были включены и доступны на момент обновления первого узла.

Важно! Перед обновлением рекомендуется создать резервную копию устройства, которая позволит восстановить предыдущее состояние в случае возникновения каких-либо проблем во время применения обновлений.

Обновление ПО кластера UserGate NGFW рекомендуется выполнять в следующем порядке:

1. Начните обновление с резервного узла кластера отказоустойчивости.

Примечание После обновления на узлах кластера будет установлено ПО разных версий, поэтому узлы будут отображаться в кластере конфигурации как недоступные. После обновления всех узлов до одной версии кластер соберётся. Перевод роли мастера в кластере отказоустойчивости будет доступен.

2. В случае успешного обновления резервного узла назначьте его мастер-узлом и проверьте основные используемые функции. При отсутствии проблем произведите обновление узла, который был мастером.

Обновление может занять довольно 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.

Примечание Не вносите изменения в конфигурацию во время обновления кластера во избежание последующих проблем в синхронизации узлов.

Запись об установке обновления будет отображена в журнале событий (вкладка **Журналы и отчёты**, раздел **Журналы** → **Журнал событий**).

Обновление ПАК с внешнего USB-носителя

Version: 6.x

Product: UserGate NGFW, UserGate MC, UserGate LogAn

KnowledgeBase: 

1. Подготовьте USB-носитель, диск должен иметь формат NTFS или FAT32 (рекомендуем FAT32).
2. Из личного кабинета UserGate скачайте необходимый файл обновления и сохраните его в корень съёмного USB-носителя.

ПримечаниеНазвание файла обновления должно быть в следующем формате: update_xxxx (где xxxx - номер версии). Без расширения .bin.

3. Вставьте USB-носитель в устройство и проверьте, что в BIOS в приоритете выставлена загрузка со встроенного в устройство HDD.

ПримечаниеПроверьте, что в BIOS в приоритете выставлена загрузка со встроенного в устройство HDD, а НЕ со съёмного USB-носителя (Boot Option Priorities → Hard Drive BBS Priorities).

4. Запустите устройство. При запуске в **Support Menu** выберите **Update from USB**.

В процессе обновления сервер перезагрузится дважды. В первый раз перезагрузится со старой версией, во второй раз уже с новой. Между перезагрузками управление устройством через веб-интерфейс и CLI недоступно.

Процедура перехода с UserGate 5 на UserGate 6

Version: 5.x, 6.1.8, 6.1.9

Product: UserGate NGFW

1. Скачать update для UserGate 5 по ссылке: <https://static.usergate.com/tools/api5beam.zip>.
- Если установлен UserGate версии utm-5.0.6.4729R или ниже — установить update из папки update_old_key.
- Если установленная версия UserGate utm-5.0.6.4825R или выше, то установить update из папки update_new_key.

Загрузить его через веб-консоль UserGate и выполнить установку.

2. Включить сервис XML-RPC на зоне интерфейса, с которого предполагается выгрузка данных.

Для этого нужно выполнить запрос в браузере (указать IP-адрес интерфейса UserGate 5): `https://<X.X.X.X>:8001?features=zone-xml-rpc` и включить сервис XML-RPC для управления на нужной зоне.

3. Загрузить архив `ug_ngfw_converter.zip`.

Архив доступен по ссылке: <https://docs.usergate.com/konvertery-konfiguracij-722/>. Архив необходимо распаковать и сделать файл `ug_ngfw_converter` исполняемым.

4. Экспортировать данные с UserGate 5.

ПримечаниеВ момент выгрузки данных LDAP-сервер и DNS должны быть доступны с устройства UserGate 5.

Для выгрузки данных в терминале необходимо запустить скрипт `ug_ngfw_converter`, ввести данные для подключения и выполнить экспорт данных (инструкция по работе скрипта: https://github.com/usergate/Migrations/tree/main/ug_ngfw_converter).

5. Развернуть образ UserGate 6.
6. После окончания установки UserGate 6 выполнить настройку DNS и LDAP-коннектора.
7. Выполнить импорт данных на UserGate 6.

Для импорта данных нужно запустить в терминале скрипт `ug_ngfw_converter`, ввести данные для подключения и выполнить импорт данных (инструкция по работе скрипта: https://github.com/usergate/Migrations/tree/main/ug_ngfw_converter).

Процесс перехода на UserGate версии 7.x

Product: UserGate NGFW, UserGate MC, UserGate LogAn
Version: 7.x

Переход на версию 7.x с последующим импортом конфигурации возможен только с версий 6.1.9 и 7.0.x. Для перехода с более ранних версий нужно предварительно обновить устройства UserGate до последней стабильной версии 6.1.9.

Важно! Лицензионные ключи версий 6.x и 7.x несовместимы. Перед переходом на версию 7.x необходимо запросить у менеджера новый лицензионный ключ для каждого из продуктов.

Примечание Переход на версию 7.x может занять длительное время, поэтому рекомендуется запланировать технологическое окно для обновления UserGate. Также, если у вас развернуты UserGate Management Center (далее — UGMC) и несколько кластеров NGFW, рекомендуется сначала обновить UGMC, временно подключить к нему кластеры NGFW текущей версии, чтобы избежать длительного простоя, и затем по очереди на каждом из кластеров выполнить переход на версию 7.x.

В качестве примера ниже описан сценарий перехода на версию 7.x для конфигурации, в которой развернуты устройства UGMC, UserGate LogAn и кластер из двух узлов UserGate NGFW версии 6.1.9. В случае если в вашей сети развернуты не все эти устройства, следует выполнять только те шаги, которые относятся к соответствующим устройствам.

Подготовка к переходу

Перед обновлением устройств выполните следующие действия:

1. Убедитесь, что в UGMC синхронизация со всеми подключенными устройствами переведена в ручной режим. Автоматическую синхронизацию устройств рекомендуется включить только после их полного обновления до версии 7.x.
2. Старайтесь избегать кириллицы и спецсимволов в названиях правил, сигнатур, узлов и других элементов. В противном случае в процессе импорта конфигурации могут возникать ошибки.
3. Выполните экспорт конфигурации текущих версий штатными средствами.

- [Экспорт конфигурации UGMC](#).
- [Экспорт конфигурации UserGate LogAn](#).
- [Экспорт всех конфигурационных параметров кластера UserGate NGFW](#).

Примечание Вы также можете выполнить экспорт конфигурации UGMC и UserGate NGFW с помощью [специальной программы](#).

4. Создайте резервные копии ваших устройств, чтобы в случае возникновения каких-либо проблем во время перехода можно было восстановить предыдущее состояние устройств.

- [Резервное копирование UGMC](#).
- [Резервное копирование UserGate LogAn](#).
- [Резервное копирование UserGate NGFW](#).

5. Скачайте последние стабильные версии ПО из кабинета клиента.

Примечание Информацию об актуальных стабильных версиях ПО можно получить, обратившись в техническую поддержку UserGate.

Порядок перехода

Переход на версию 7.x выполняется последовательно: сначала следует обновить UGMC, затем — UserGate LogAn и потом — UserGate NGFW.

Чтобы перейти на версию 7.x:

1. Выполните чистую установку новой версии ПО UGMC и затем выполните [импорт конфигурации](#).
2. Выполните чистую установку новой версии ПО UserGate LogAn и затем выполните [импорт конфигурации](#).
3. [Подключите устройство UserGate LogAn](#) как новое устройство, но с прежними шаблонами, к устройству UGMC, если ранее оно было подключено. Убедитесь, что репликация параметров из шаблонов выполняется корректно.
4. Выполните чистую установку новой версии ПО UserGate NGFW на первый узел кластера, активируйте его с помощью ключа кластера для версии 7.x и затем выполните [импорт конфигурации всех параметров для роли Master](#).
5. [Подключите первый узел](#) как новое устройство к UGMC и UserGate LogAn. Убедитесь, что все параметры импортированы корректно и синхронизация работает.
6. Выполните чистую установку новой версии ПО UserGate NGFW на дополнительный узел кластера и затем выполните на нем [импорт параметров конфигурации для резервного узла кластера](#).

После завершения перехода на новую версию рекомендуется проверить базовые параметры конфигурации и корректность работы основных функций:

1. Проверьте разрешения в импортированных профилях администраторов (кроме профиля Admin). Начиная с версии 7.2 структура и список разрешений были изменены: разрешения для CLI и API настраиваются в окне настроек профиля администратора на одной вкладке **Разрешения для API**.
2. Если в версии ПО UGMC 6.1.9 в шаблонах использовались учетные записи LDAP-пользователей, после перехода на новую версию в разделе **Управление областью → Центр управления → Каталоги пользователей** добавьте каталог с указанием LDP-домена, чтобы использовать учетные записи LDAP-пользователей в версии 7.x.
3. В случае с кластером отказоустойчивости проверьте корректность его работы, выполнив на узлах смену роли мастер-узла.
4. Включите автоматическую синхронизацию для UserGate NGFW или LogAn, подключенных к UGMC, если она была отключена на время обновления.
5. Выполните аудит сенсоров на UserGate LogAn. Индикация подключения должна быть активной, а журналирование событий сенсоров выполняется.
6. Убедитесь, что в журнале событий нет записей об ошибках или предупреждениях.

Ограничения и особенности импорта конфигурации

Импорт конфигурации на устройства версии 7.x имеет следующие ограничения и особенности:

- Импортированные правила межсетевого экрана, предназначенные для анализа трафика на уровне приложений (седьмом уровне модели OSI), будут принудительно выключены с назначенным действием **Разрешить**, и в них будет добавлен созданный L7-профиль. Профили создаются на базе правил с добавлением фильтров для каждой группы приложений:
 - для группы All — фильтр "Any signatures";
 - для групп по категориям — фильтр вида "category = <имя или номер категории>";
 - для пользовательских групп — фильтр, включающий идентификаторы сигнатур, вида "id IN (...)".
- Профили COB при импорте будут преобразованы в новый формат. В новых профилях будет один фильтр вида "id IN (...)", который будет включать все идентификаторы сигнатур COB из профиля COB старой версии.
- Правила COB не будут импортированы. Необходимо заново настроить IDPS после завершения импорта, используя новые профили COB и правила межсетевого экрана.
- После импорта сигнатур COB и приложений необходимо выполнить обновление сигнатур.
- В импортированные профили приложений необходимо добавить сигнатуры новых типов, которые появились в версии 7.x: зависимые от типа протокола и связанные с другими сигнатурами. Подробнее о новых типах сигнатур приложений — в разделе «[Приложения](#)».
- Журналы не будут импортированы.
- При импорте конфигурации UserGate NGFW версии 6.1.9 или 7.0.x в UGMC могут создаваться списки IP-адресов с необычными алфавитно-цифровыми названиями. Причиной является то, что в UserGate NGFW этих версий в свойствах зон, в параметрах защиты от IP-спуфинга, используются одиночные IP-адреса или диапазоны адресов. В UserGate NGFW версий 7.x в этих параметрах используются списки IP-адресов. При импорте конфигурации из версии 6.1.9 или 7.0.x конвертер создает списки с автоматически сгенерированными названиями и помещает в них IP-адреса из параметров зон. В начале сгенерированного имени списка указывается название зоны, для которой он создавался при конвертации. Созданные при конвертации списки можно переименовать вручную.

Ограничения в работе UGMC 7.x с UserGate NGFW версий 6.1.9 и 7.0.1

В совместной работе UGMC версии 7.x и UserGate NGFW версии 6.1.9 или 7.0.x есть следующие ограничения:

- не поддерживаются VPN, COB и L7;
- недоступна аутентификация в веб-консоли UserGate NGFW с использованием профилей сертификатов (поддержка PKI есть только в версии 7.x);
- недоступна аутентификация пользователей в captive-портале (так как введен новый режим аутентификации — PKI).

Порядок обновления ПО UserGate LogAn

Version: 7.0.1, 7.1.0, 7.x

Product: UserGate LogAn, UserGate SIEM

После обновления ПО и запуска LogAn, в нем начинается обновление внутренней базы данных. Миграция данных может занимать до нескольких часов в зависимости от объема накопленных данных.

Во время миграции данные от сенсоров-источников (например, от узлов NGFW) продолжают поступать на LogAn. При этом данные не отправляются сразу в базу данных LogAn, а накапливаются в специальном файловом кеше. Это дополнительно увеличивает нагрузку на диск, увеличивает утилизацию CPU, уменьшает свободное место на диске, и в итоге может помешать процессу миграции данных.

В целях оптимизации процесса миграции данных рекомендуется придерживаться следующего порядка обновления ПО LogAn:

1. Выключить в консоли администратора LogAn/SIEM сенсоры NGFW. Для этого в разделе **Настройки --> Сенсоры --> Сенсоры UserGate** отметить необходимые узлы и нажать кнопку **Отключить**. NGFW в это время будут накапливать данные у себя.
2. Выполнить обновление ПО LogAn.
3. Дождаться окончания процесса миграции данных. Для контроля статуса обновления перейти в раздел **Настройки --> Настройки** в консоли администратора и проверить статус **Состояние Log Analyzer --> Работает**.

Процесс миграции может параллельно контролироваться по системным логам (utm-statistics/main.log и clickhouse/server.log).

Пример записей в логе utm-statistics/main.log, по которым можно отслеживать миграцию:

```
2023-12-05 16:38:41.416373<0.1107.0> [notice][db,upgrade,db] : Set up database version 228
2023-12-05 16:44:41.234234<0.1107.0> [notice][db,upgrade,db] : Set up database version 229
2023-12-06 00:58:41.546453<0.1107.0> [notice][db,upgrade,db] : Set up database version 232
2023-12-06 00:58:41.989056<0.1081.0> [critical][db] : Database is ready to accept connections
```

Последняя запись означает успешное завершение миграции и переход состояния в **Работает** на странице **Настройки**.

4. После окончания миграции включить ранее выключенные сенсоры NGFW. Для этого в разделе **Настройки --> Сенсоры --> Сенсоры UserGate** отметить необходимые узлы и нажать кнопку **Включить**. NGFW подключатся к LogAn и начнут передавать накопленные данные.

Важно Если в это время пропадает связь **NGFW → LogAn**, то все неотправленные данные останутся на NGFW. Второй попытки нет, возможно только запустить отправку вручную с дубликатами событий. При следующем перезапуске NGFW данные удалятся безвозвратно.

На NGFW может накопиться до нескольких GB данных, это нормально. Если не разрывать связь и не перезапускать сервисы utm-core, logan_core, utm_statistics, то все данные постепенно передадутся в LogAn.

Приём накопленных данных от NGFW хорошо видно на графике входящего трафика в дашборде LogAn.

5. Если на LogAn/SIEM есть активные правила аналитики, то после окончания приёма ранее накопленных данных из NGFW (спад входящего трафика до обычных значений), их нужно запустить вручную (ретроспективно) на интервале времени, когда сенсоры были выключены.

Примечание Важно не перезапускать LogAn до завершения миграции, особенно если сенсоры не выключались в п. 1. Если перезапуск всё-таки случился, то миграция перезапустится с незавершённого шага, но при этом необходимо производить мониторинг ошибок в логах.

Примечание Операции reset или shutdown, выполненные не из веб-консоли управления, с высокой вероятностью могут привести к повреждению данных в базе данных, в том числе в процессе миграции.

Примечание Импорт конфигурации на LogAn/MC/NGFW выполняет Factory Reset и все данные, в том числе база данных статистики, очищаются.

Развертывание образа UserGate на Hyper-V

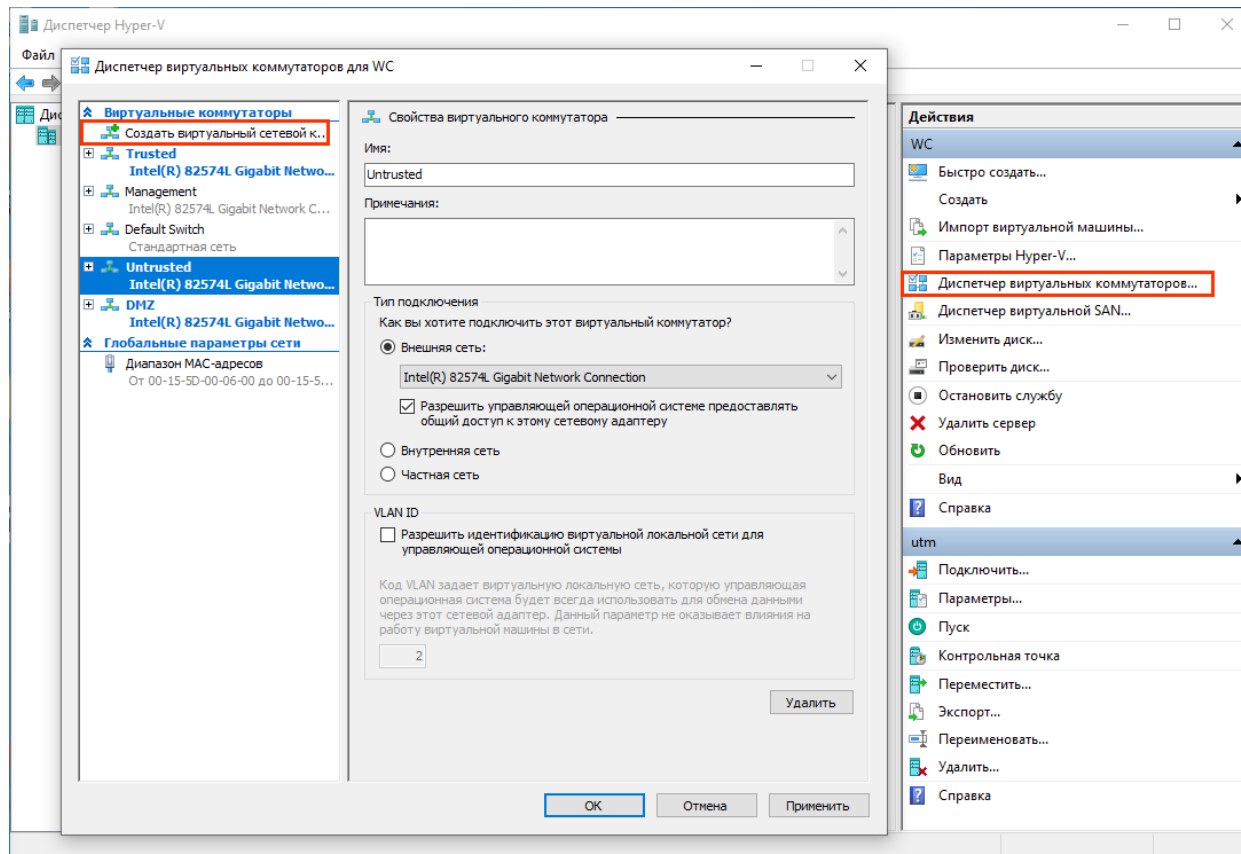
Product: UserGate NGFW
Version: 5.x, 6.1.8, 6.1.9

В данном разделе рассмотрена настройка UserGate для среды виртуализации Microsoft Hyper-V.

1. Скачать образ UserGate с официального сайта (**Hyper-V образ**).
2. Распаковать файл **utm-hyperv.zip**.
3. Проверить сетевые интерфейсы на хостовой машине с Hyper-V.
4. Создать виртуальные коммутаторы для необходимых интерфейсов.

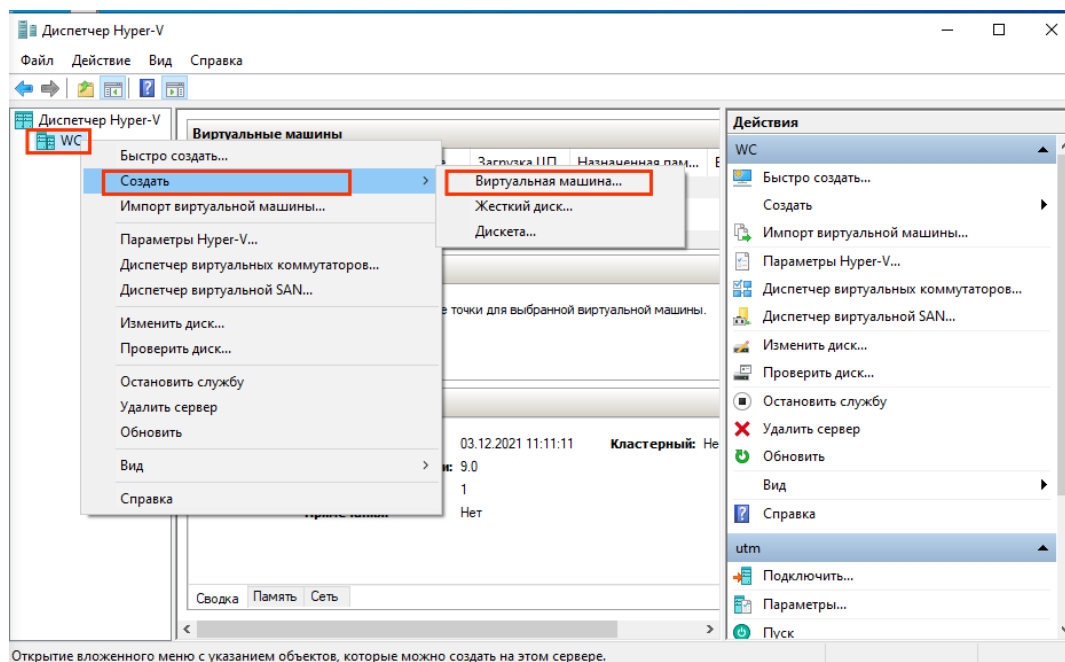
По умолчанию в UserGate имеются четыре зоны **Management**, **Trusted**, **Untrusted** и **DMZ**.

Для примера созданы четыре виртуальных коммутатора по одному на каждый интерфейс. Названия совпадают с названиями у зон, т.е. **Management**, **Trusted**, **Untrusted** и **DMZ**.



Если на сервере используются один или два сетевых интерфейса, тогда достаточно создать один или два виртуальных коммутатора и подключить их к требуемым интерфейсам.

5. Создать виртуальную машину.



Далее откроется окно мастера создания виртуальной машины.

6. Задать необходимые настройки виртуальной машины.

Во вкладке **Укажите имя и местонахождение** задайте имя виртуальной машины. Если хотите изменить папку, в которой будет сохранена виртуальная машина, отметьте чекбокс **Сохранить виртуальную машину в другом месте** и выберите нужную папку.

Мастер создания виртуальной машины

Укажите имя и местонахождение

Приступая к работе

Укажите имя и местонахождение

Укажите поколение

Выделить память

Настройка сети

Подключить виртуальный жесткий диск

Параметры установки

Сводка

Выберите имя и местонахождение для этой виртуальной машины.

Имя отображается в диспетчере Hyper-V. Рекомендуется использовать легко узнаваемое имя, например, имя операционной системы на виртуальной машине или рабочей нагрузки.

Имя:

Для сохранения виртуальной машины можно использовать существующую или создать новую папку. Если папка не выбрана, виртуальная машина будет сохранена в папке по умолчанию для этого сервера.

☐ Сохранить виртуальную машину в другом месте

Расположение: Обзор...

Если вы планируете создавать контрольные точки этой виртуальной машины, выберите расположение, где достаточно свободного пространства. Контрольные точки включают данные виртуальной машины и могут занимать много места.

< Назад Далее > Готово Отмена

7. Для корректной работы следует выбрать Поколение 1.

Мастер создания виртуальной машины

Укажите поколение

Приступая к работе

Укажите имя и местонахождение

Укажите поколение

Выделить память

Настройка сети

Подключить виртуальный жесткий диск

Параметры установки

Сводка

Выберите поколение виртуальной машины.

☒ Поколение 1

Это поколение виртуальных машин поддерживает 32- и 64-разрядные гостевые ОС и предоставляет виртуальное оборудование, которое было доступно во всех предыдущих версиях Hyper-V.

☐ Поколение 2

Виртуальные машины этого поколения поддерживают новые возможности виртуализации. Они оснащены встроенным ПО на основе UEFI и работают под управлением только поддерживаемой 64-разрядной версии гостевой ОС.

⚠ Поколение созданной виртуальной машины невозможно изменить.

[Подробнее о поддержке виртуальных машин данного поколения](#)

< Назад Далее > Готово Отмена

8. Во вкладке **Выделить память** увеличьте размер оперативной памяти виртуальной машины. Используя свойства виртуальной машины, установите минимум 8Gb и добавьте по 1Gb на каждые 100 пользователей.

Мастер создания виртуальной машины

Выделить память

Приступая к работе

Укажите имя и местонахождение

Укажите поколение

Выделить память

Настройка сети

Подключить виртуальный жесткий диск

Параметры установки

Сводка

Укажите размер памяти, выделяемый для этой виртуальной машины. Размер может быть указан в пределах от 32 до 251658240 МБ включительно. В целях повышения производительности укажите размер, превышающий минимальный рекомендованный размер памяти для операционной системы.

Память, выделяемая при запуске: МБ

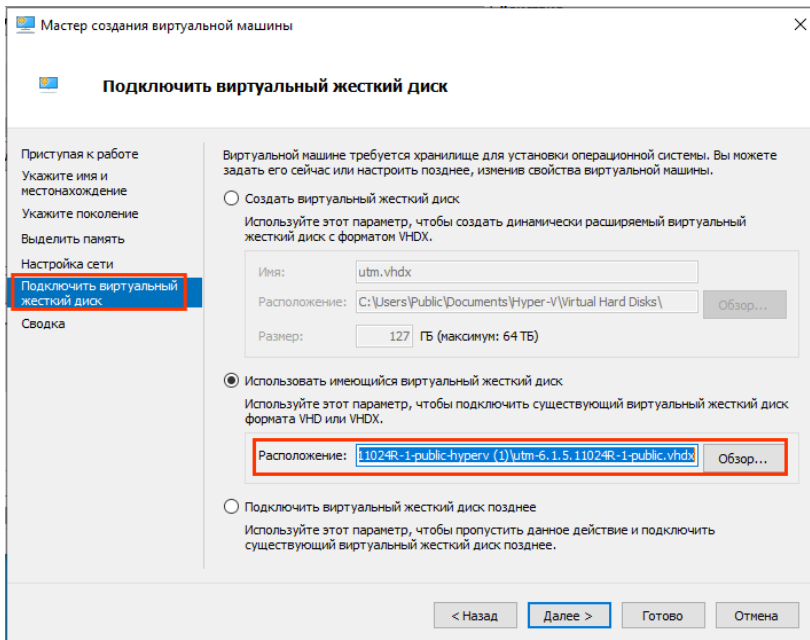
☐ Использовать для этой виртуальной машины динамическую память.

Принимая решение об объеме памяти, выделяемой виртуальной машине, следует учесть, для каких целей будет использоваться виртуальная машина и запущенная на ней операционная система.

< Назад Далее > Готово Отмена

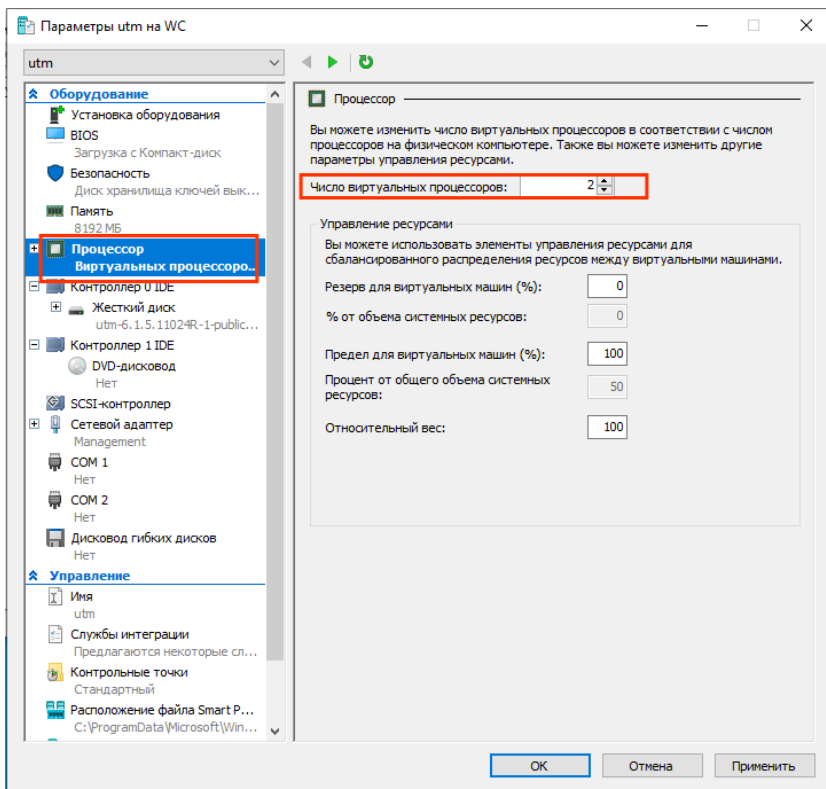
9. Во вкладке **Настройка сети** указать подключение к виртуальному коммутатору **Management**.

10. Во вкладке **Подключить жёсткий виртуальный диск** выбрать виртуальный жесткий диск из папки, в которую был распакован скачанный файл utm-hyperv.zip.

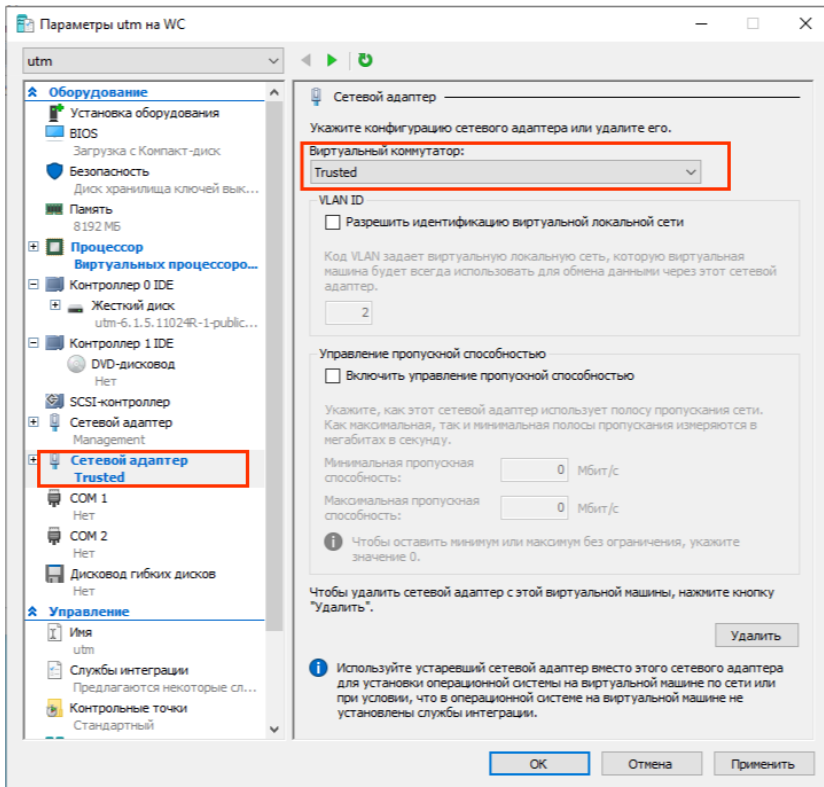
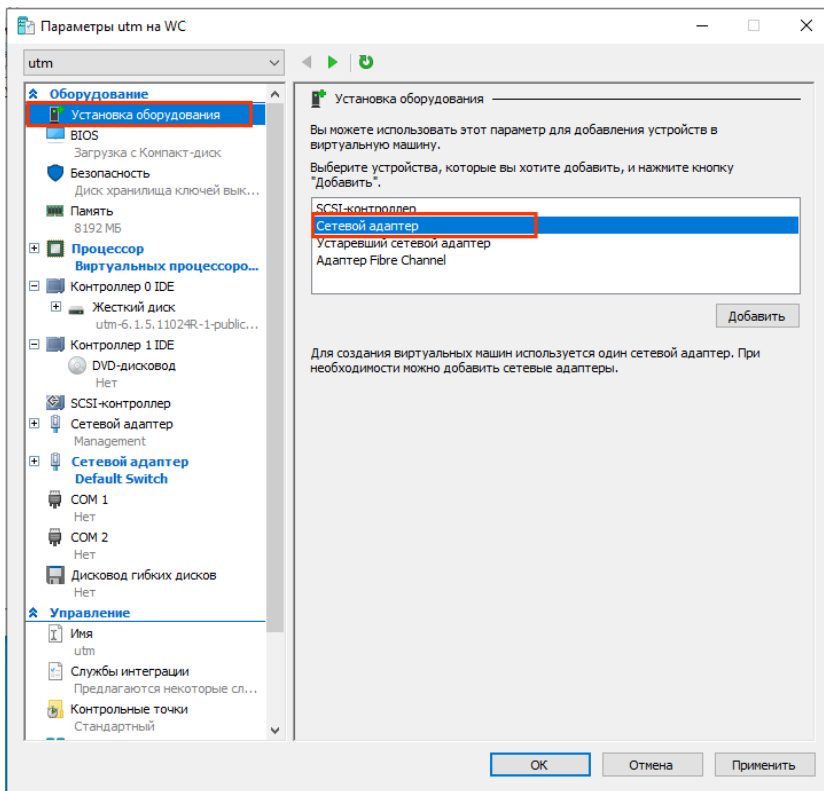


11. Во вкладке **Сводка** представлена информация о созданной виртуальной машине. Далее необходимо произвести настройку.

Откройте меню **Параметры** в разделе Действия. В разделе **Оборудование** → **Процессор** увеличьте число виртуальных процессоров до двух. Количество процессоров необходимо определять в зависимости от количества пользователей и ресурсов вашего сервера.



Создайте четыре сетевых адаптера и подключите их к созданным ранее виртуальным коммутаторам. Для этого перейдите во вкладку **Оборудование** → **Установка оборудования** выделите **Сетевой адаптер** и нажмите кнопку **Добавить**. Далее будет создан сетевой адаптер: укажите виртуальный коммутатор.

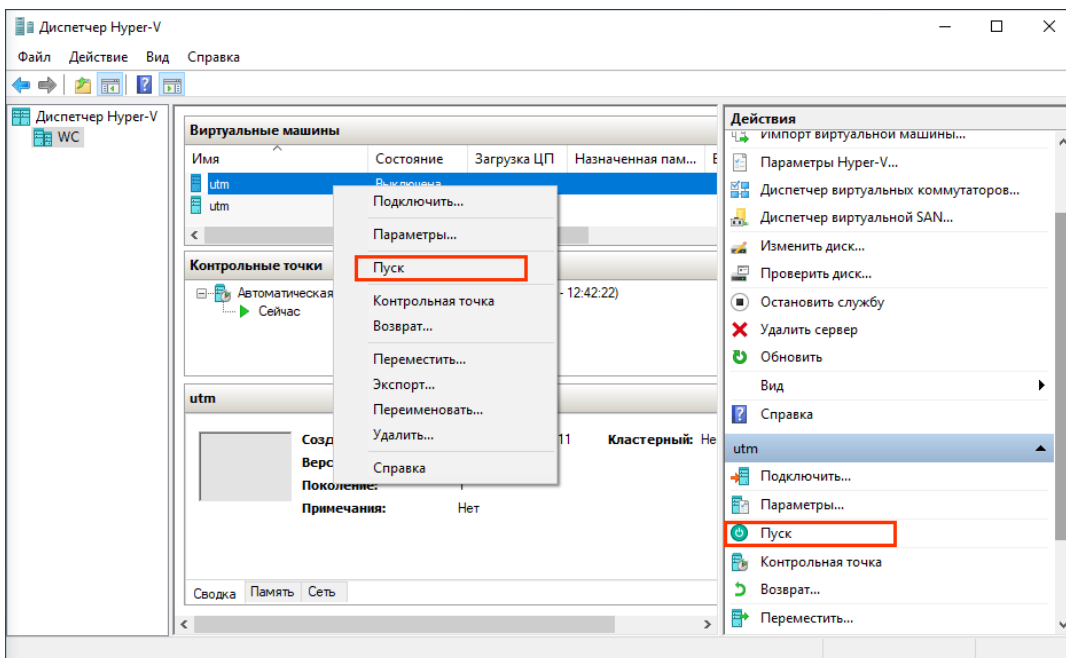


Аналогично добавьте остальные сетевые адаптеры.

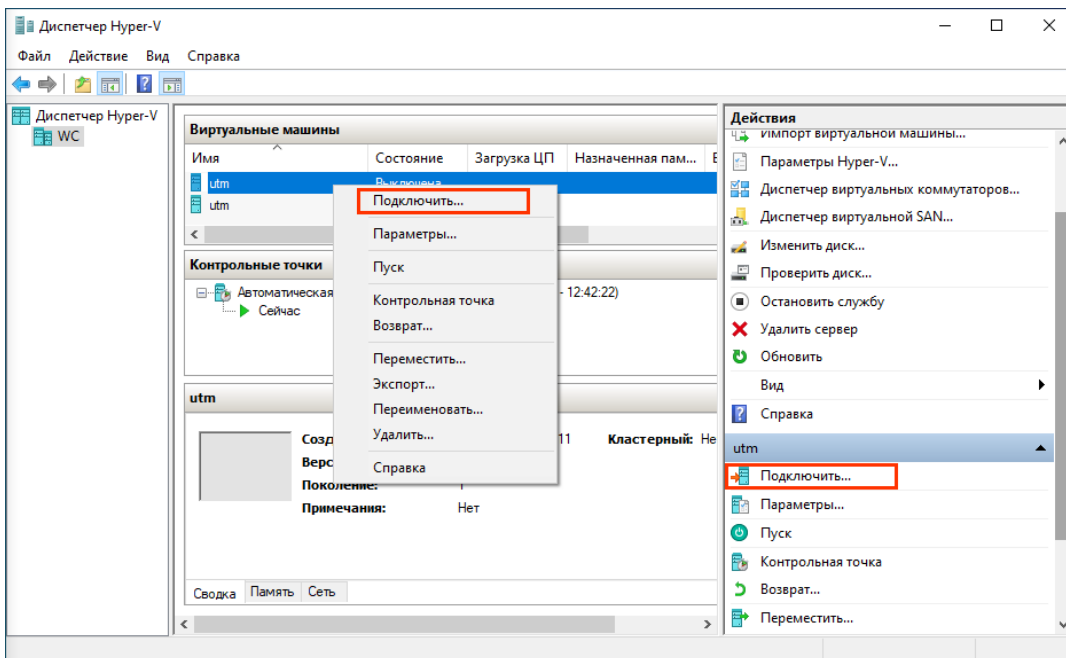
Во вкладке **Оборудование** → **Контроллер 0 IDE** → **Жесткий диск** нажмите **Правка**. В открывшемся окне мастера изменения виртуального жёсткого диска перейдите в раздел **Выбрать действие**, отметьте чекбокс **Преобразовать** и нажмите **Далее**. В разделе **Настройка диска** проверьте размер диска виртуальной машины. Установите размер диска в 100Gb или более. Рекомендованный размер - 300Gb.

Отключите службы интеграции во вкладке **Управление** → **Службы интеграции**. Виртуальная машина настроена.

12. Запустить виртуальную машину, нажав на **Пуск** в разделе **Действия** или в контекстном меню.



За старт можно наблюдать, подключившись к виртуальной консоли. Для этого выберите **Подключить** в разделе **Действия** или в контекстном меню.



13. Во время первой загрузки выполнится процедура Factory reset. Во время этого шага UserGate настраивает сетевые адаптеры и увеличивает размер раздела на жестком диске до полного размера диска, увеличенного в предыдущих пунктах.
14. После перезагрузки, если в сети, подключенной к первому виртуальному коммутатору (Management) и, соответственно, интерфейсу port0, есть DHCP-сервер, то в приглашении будут отображены адрес и порт, для управления через веб-консоль.

Если DHCP-сервера нет, то адрес для интерфейса необходимо задать самостоятельно. Авторизуйтесь в CLI-консоли с логином **Admin** и паролем **utm**. С помощью следующей команды:

- Для UserGate версий 6.1.x:

UTM> iface config -name port0 -ipv4 A.B.C.D/M -enabled true -mode static

где A.B.C.D/M - выделенный адрес и маска локальной сети.

14. Настройка UserGate.

Дальнейшая настройка UserGate производится через веб-консоль, к которой необходимо подключиться по полученному или заданному адресу. На странице предупреждения о небезопасном соединении нажмите **Дополнительные** и **Перейти на сайт A.B.C.D/M (небезопасно)**, где A.B.C.D/M - адрес для управления через веб-консоль.

Далее откроется окно установки UserGate. Выберите язык установки и часовой пояс, примите лицензионное соглашение, задайте логин и пароль администратора. После заполнения откроется веб-консоль UserGate.

Перейдите в раздел **Сеть** → **Интерфейсы**. Интерфейсу **port0** уже назначен IP-адрес и зона **Management**. Укажите зону **Trusted** (во вкладке **Общие**) и IP-адрес (во вкладке **Сеть**) для интерфейса **port1**.

Для интерфейса **port2** установите зону **Untrusted** (во вкладке **Общие**) и выберите получение IP-адреса по DHCP (во вкладке **Сеть**).

Для интерфейса **port3** установите зону **DMZ** (во вкладке **Общие**) и укажите IP-адрес (во вкладке **Сеть**).

Перейдите во вкладку **Сеть** → **Шлюзы**. Задайте шлюз по умолчанию для интерфейса, через который будет осуществляться выход в сеть Интернет. В данном случае для выхода в Интернет будет использоваться интерфейс **port2**.

Для интерфейса **port0** также адрес и шлюз выданы DHCP-сервером, поэтому во вкладке **Сеть** → **Шлюзы** будут отображены два шлюза. Оставьте один шлюз по умолчанию для выхода в Интернет.

Укажите адрес DNS-сервера во вкладке **Сеть** → **DNS**.

15. Проверить корректность сетевых настроек.

Для проверки подключитесь через виртуальную CLI-консоль и наберите команду **ping ya.ru**. Успешное выполнение команды говорит о правильности произведённых настроек.

```

[UTM] ping ya.ru
PING ya.ru.esafeline.com (127.0.0.1) 56(84) bytes of data:
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.025 ms
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.058 ms
64 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.058 ms
64 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0.064 ms
--- ya.ru.esafeline.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 307ms
rtt min/avg/max/mdev = 0.025/0.051/0.064/0.016 ms

```

16. Зарегистрировать продукт UserGate.

Для регистрации нажмите на **Незарегистрированная версия** в верхней части окна, введите пин-код и заполните необходимые данные.

После регистрации начнется обновление баз данных контентной фильтрации, антивирусных и т. д. Посмотреть версию баз и ход обновления можно во вкладке **Дашборд**. После обновления баз продукт готов к работе.

Version: 7.x
Product: UserGate C150
Documentation: ☒

Установка UserGate на аппаратную платформу C150

1. Скачать архив **ngfw_ucls_full_update_7.m.n.XXXY.tar.gz** из личного кабинета My.UserGate (<https://my.usergate.com>).

ПримечаниеВ 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.XXXY:

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

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.

ПримечаниеПосле обновления программного обеспечения на первом узле, узлы кластера конфигурации временно отображаются 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 сохраняют 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.

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.

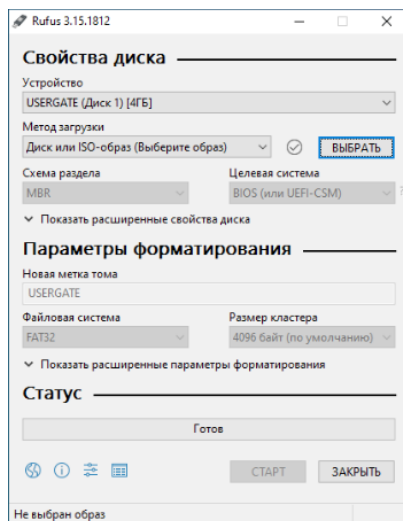
Примечание Если вы выполняете обновление версии ПО на устройстве с помощью метода чистой установки, перед началом обязательно сохраните (экспортируйте) параметры настройки устройства, а после завершения установки восстановите (импортируйте) ранее сохраненные параметры.

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](#).

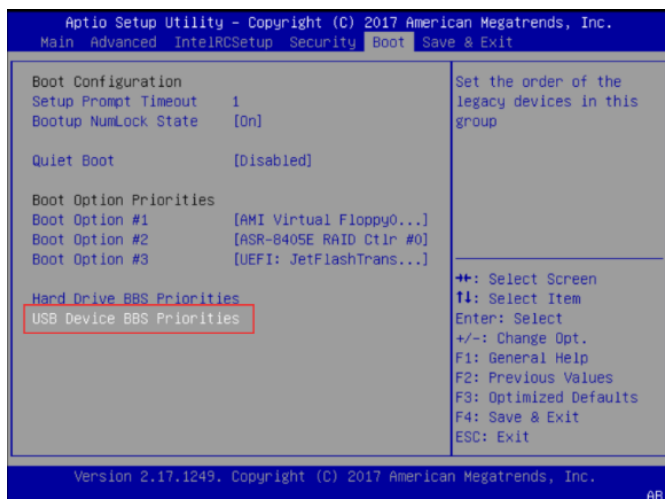
Загрузка образа ПО с помощью консольного подключения

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

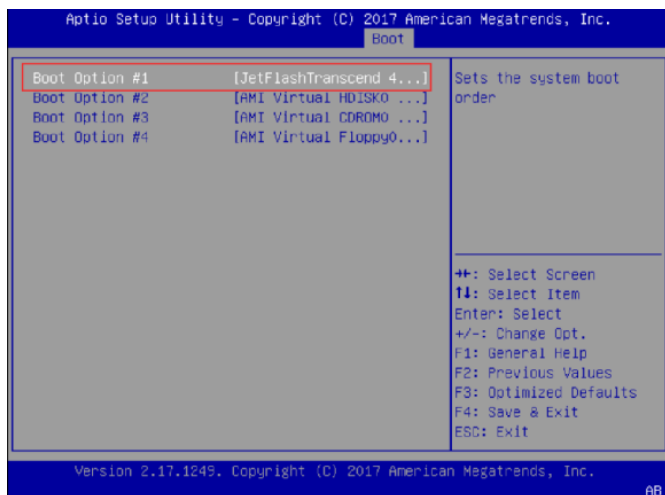
1. Подключите к устройству (ПАК UserGate) внешний монитор и USB-клавиатуру.
2. Войдите в BIOS устройства. Для этого включите устройство и нажмите клавишу Delete после появления на экране следующего оповещения.



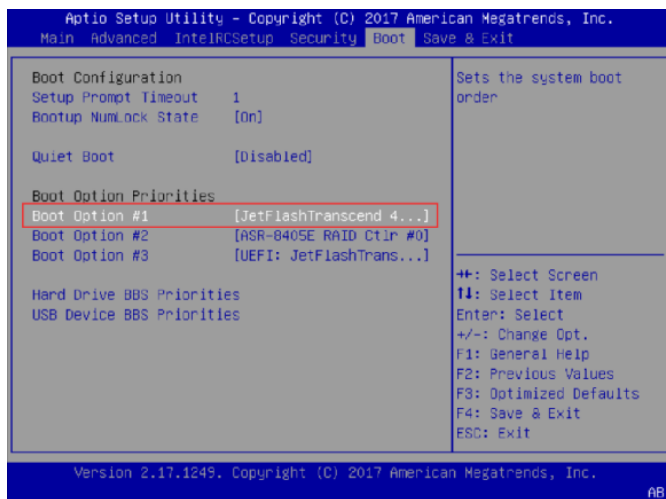
3. На вкладке **Boot** перейдите в раздел **USB Device BBS Priorities**; если такой раздел отсутствует, перейдите в раздел **Hard Drive BBS Priorities**.



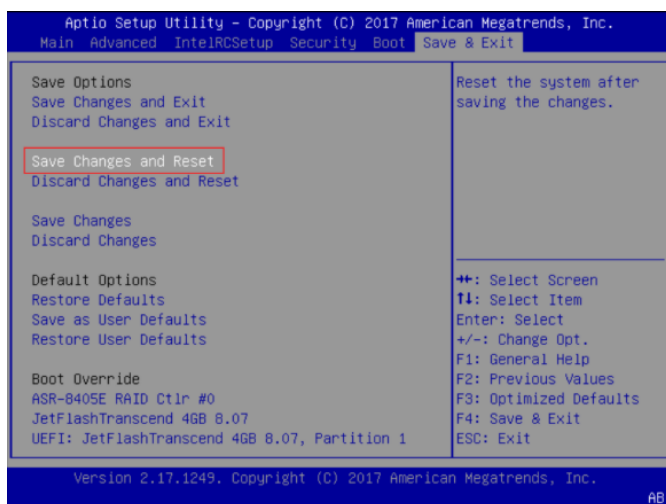
4. В параметре **Boot Option #1** выберите USB-носитель с Ghost4Linux. Общее количество Boot-опций может отличаться на разных устройствах.



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 загрузаться с USB-накопителя.

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

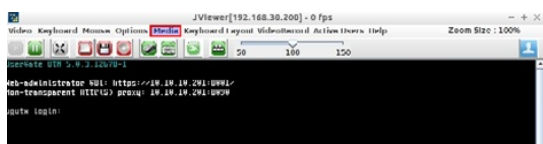
Загрузка образа ПО с помощью подключения через IPMI

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

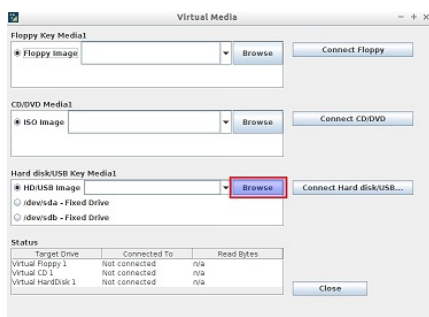
1. Сделайте имидж подготовленного на первом этапе USB-накопителя с расширением .img. Вы можете воспользоваться утилитой USB Image Tool [по ссылке](#).
2. Подключитесь к модулю IPMI устройства. О настройке подключения — в инструкции « [Удаленное управление с помощью IPMI](#) ».

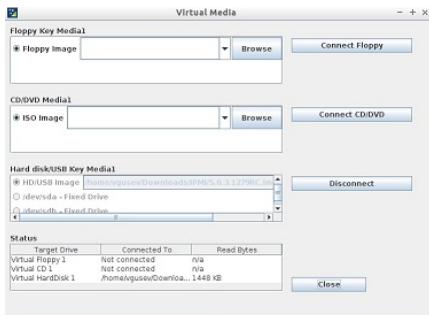
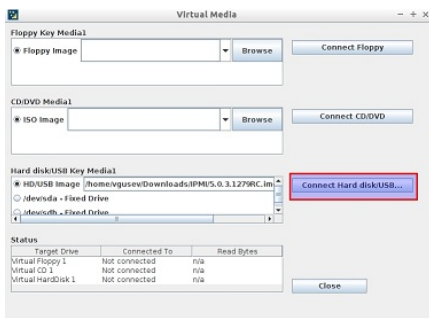
Важно!Для корректной работы с IPMI необходимо иметь на компьютере установленную 32-х битную версию ПО Java.

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

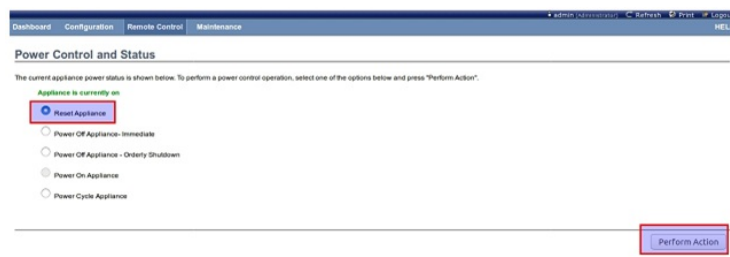
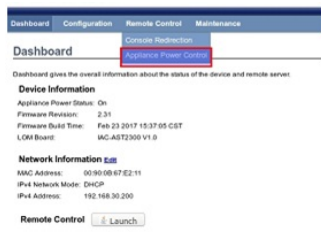


4. Выберите сохраненный ранее имидж USB-накопителя и подключите USB Key Media.

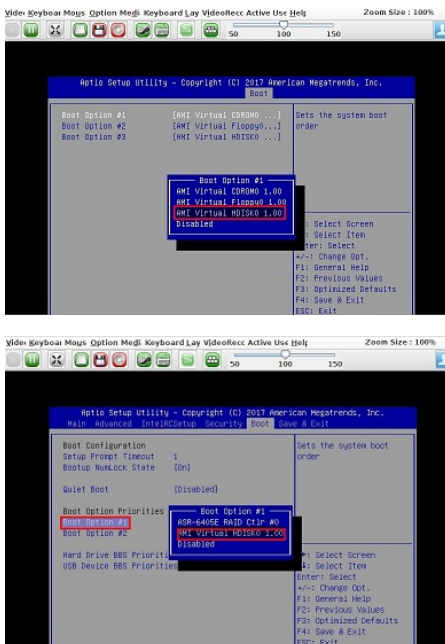




5 Перезагрузите устройство. Для этого выберите **Remote Control → Appliance Power Control → Reset Appliance** и нажмите **Perform action**.



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



После перезагрузки устройство начнет загружаться с имиджа USB-накопителя.

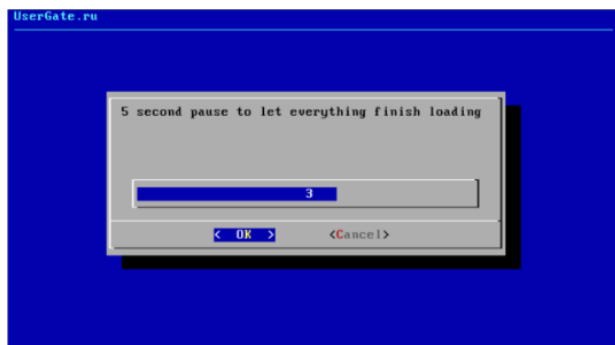
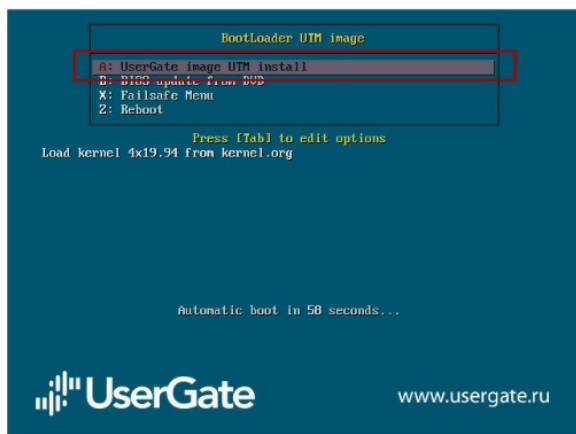
Для продолжения процедуры установки ПО перейдите к этапу [распаковки образа ПО на аппаратной платформе](#).

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](#)).

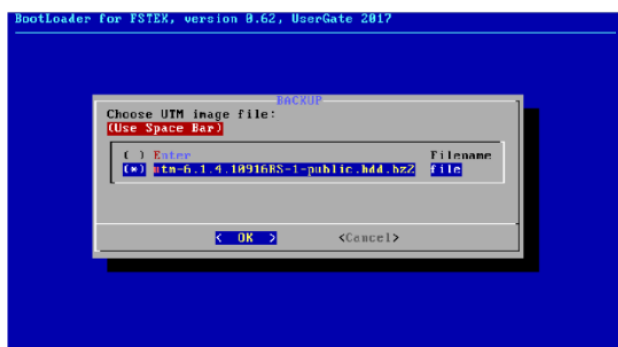
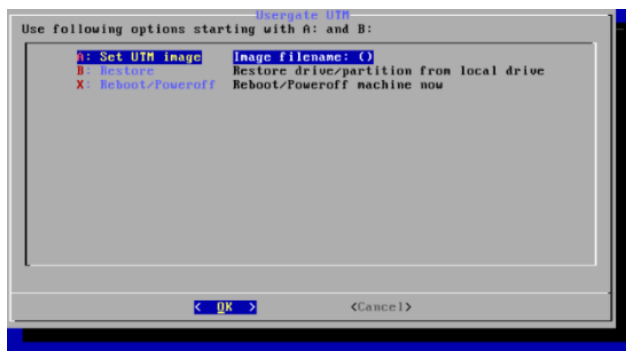
Для распаковки образа ПО выполните следующие шаги:

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

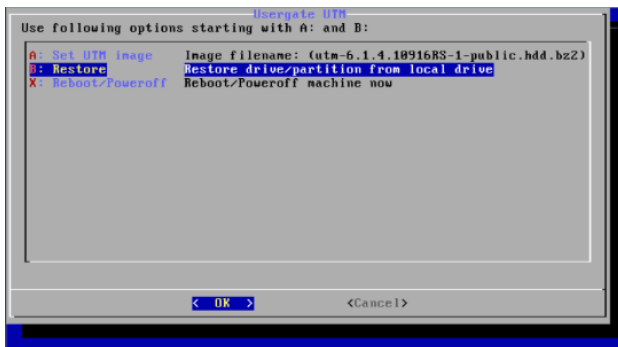


2. Выберите пункт меню **Set UTM image** и в следующем окне при помощи клавиши Space выберите образ ПО:

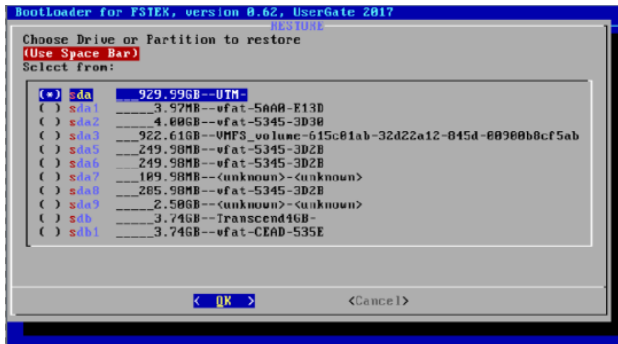
- utm-6-<НОМЕР-ВЕРСИИ>-public.hdd.bz2 — для версий 6.x;
- ngfw-x86-64-<НОМЕР-ВЕРСИИ>-release-public.hdd.bz2 — для версий 7.x.



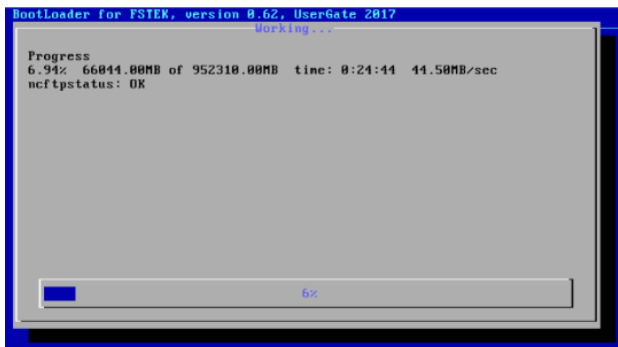
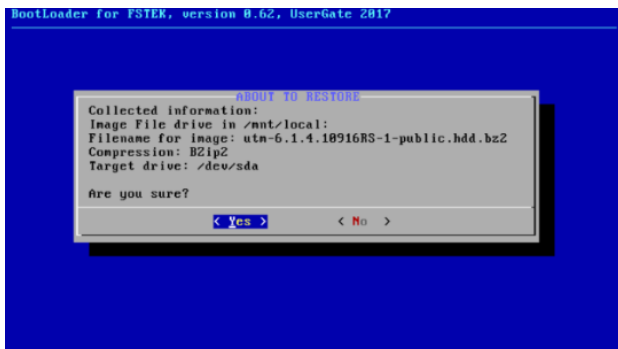
3. Выберите пункт меню **Restore**.



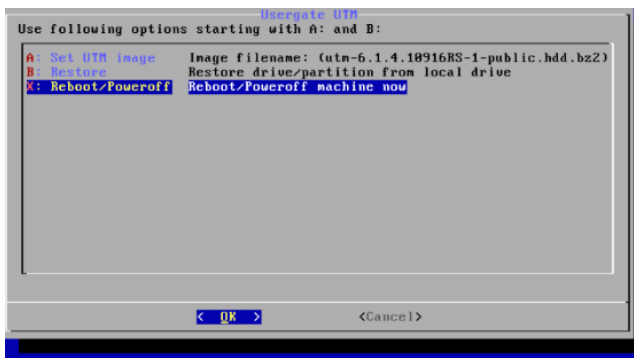
4. Выберите физический диск (например, sda), на котором будет развернут образ ПО.

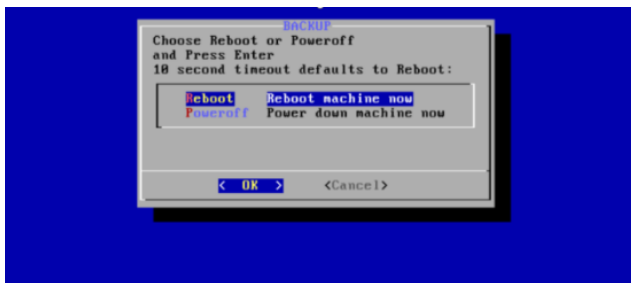


5 После подтверждения действий начнется распаковка образа.



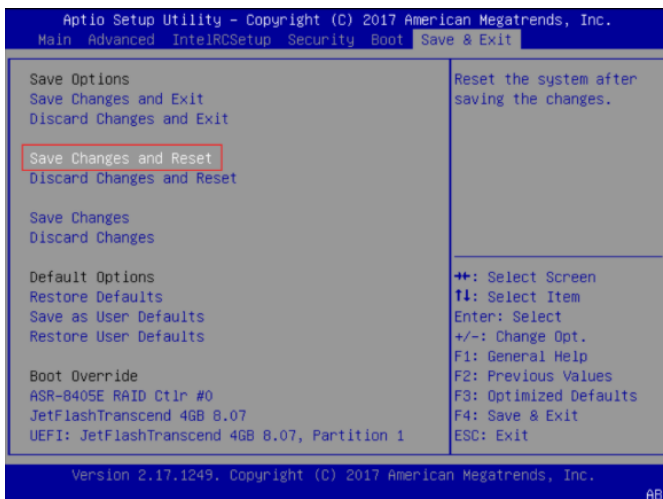
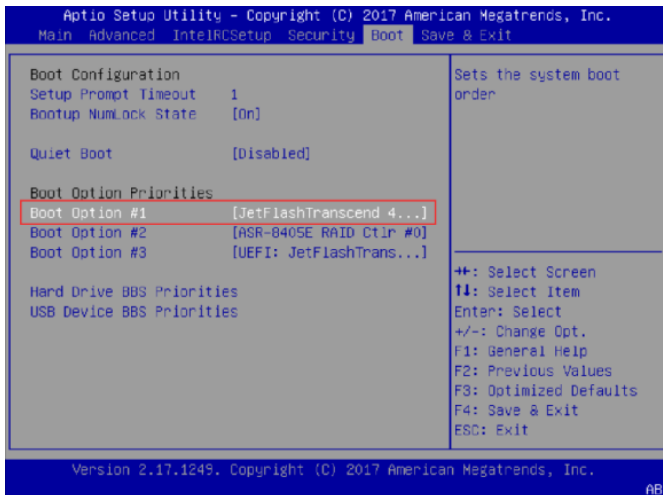
6. После окончания установки перезагрузите устройство, выбрав пункт меню Reboot/Poweroff.





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.

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

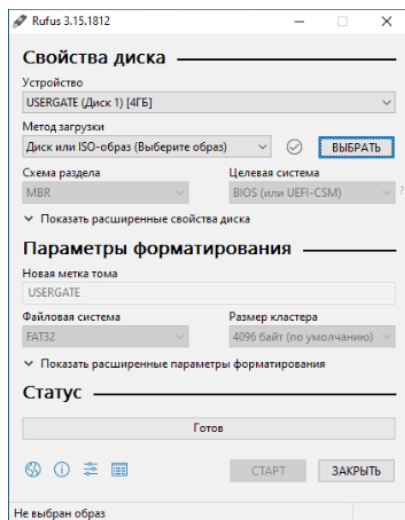
Если вы выбрали способ загрузки образа ПО на аппаратную платформу с помощью консольного подключения, вам необходимо:

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.

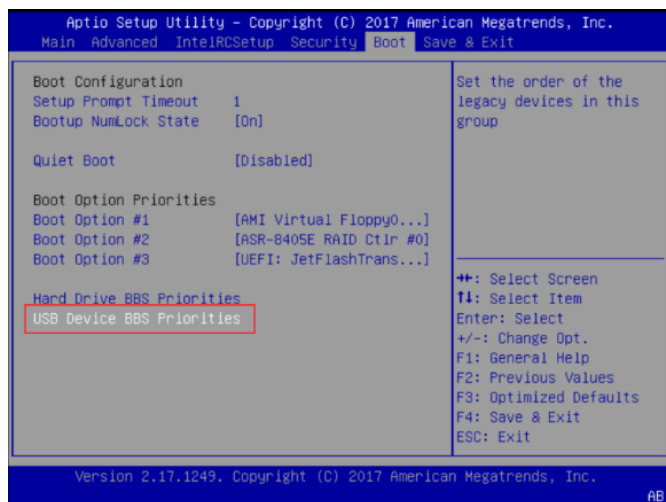
Загрузка образа ПО на аппаратную платформу

Для загрузки образа выполните следующие шаги:

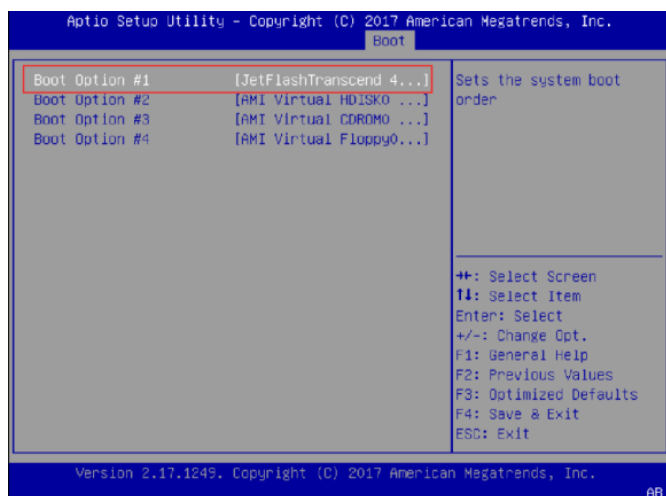
1. Подключите к устройству (ПАК UserGate) внешний монитор и USB-клавиатуру.
2. Войдите в BIOS устройства. Для этого включите устройство и нажмите клавишу Delete после появления на экране следующего оповещения.



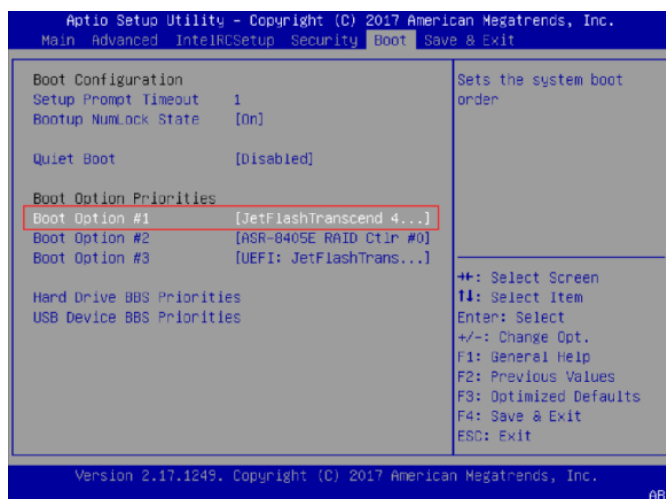
3. На вкладке **Boot** перейдите в раздел **USB Device BBS Priorities**; если такой раздел отсутствует, перейдите в раздел **Hard Drive BBS Priorities**.



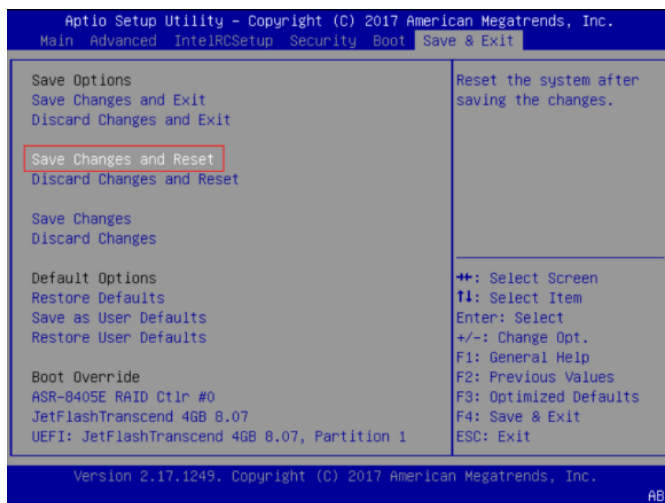
4. В параметре **Boot Option #1** выберите USB-носитель с Ghost4Linux. Общее количество Boot-опций может отличаться на разных устройствах.



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**:

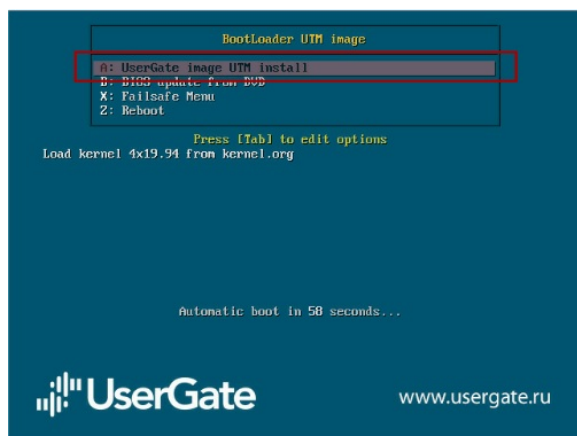
Для продолжения процедуры установки ПО перейдите к этапу [распаковки образа ПО на аппаратной платформе](#).

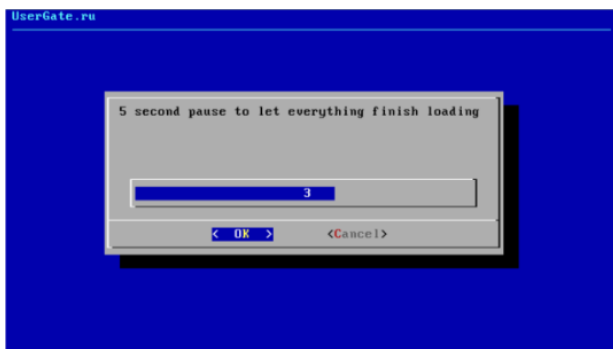
Распаковка образа ПО на аппаратной платформе

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:

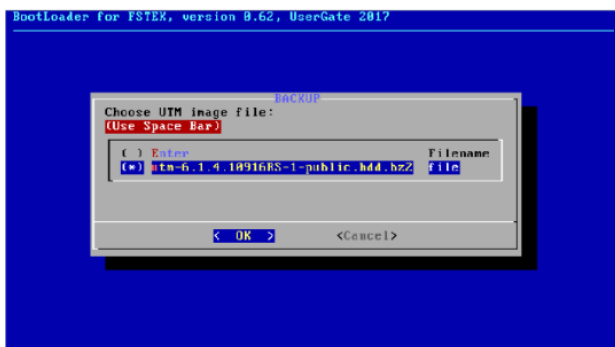
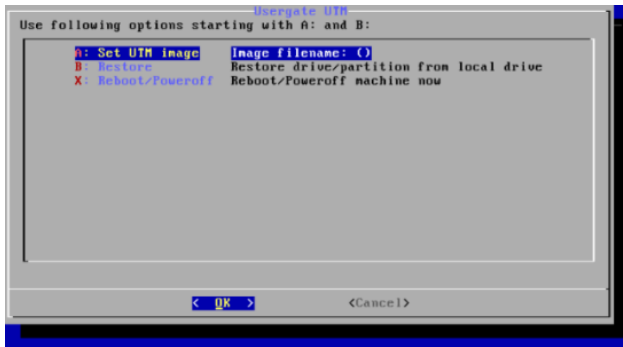
1. В Boot Menu выберите **UserGate image UTM install** и дождитесь окончания загрузки.



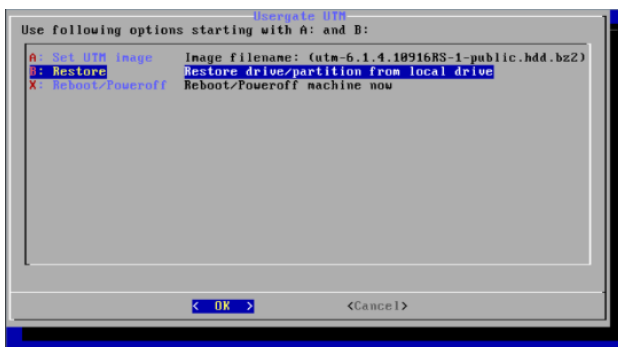


2. Выберите пункт меню **Set UTM image** и в следующем окне при помощи клавиши Space выберите образ ПО:

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

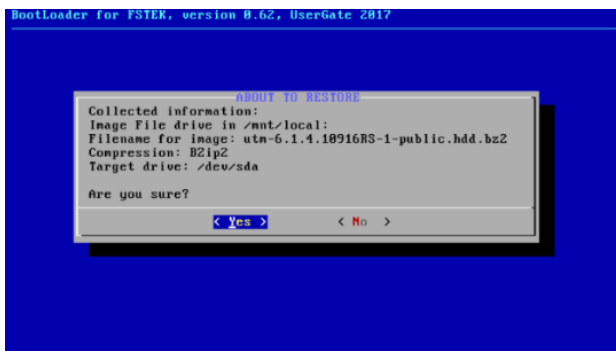


3. Выберите пункт меню **Restore**.

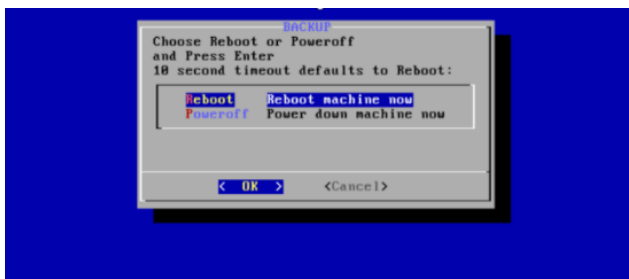
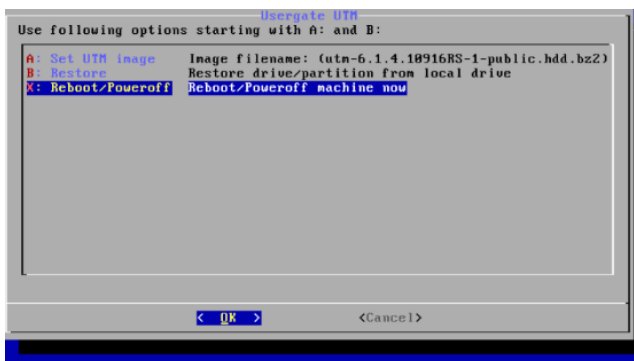


4. Выберите физический диск, на котором будет развернут образ ПО.

5 После подтверждения действий начнется распаковка образа.

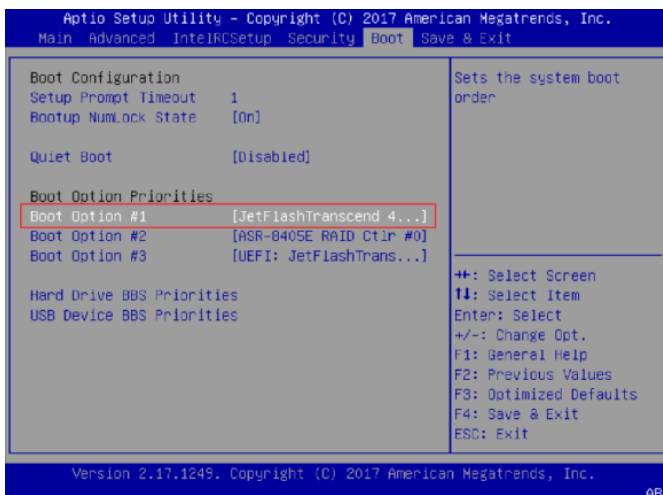


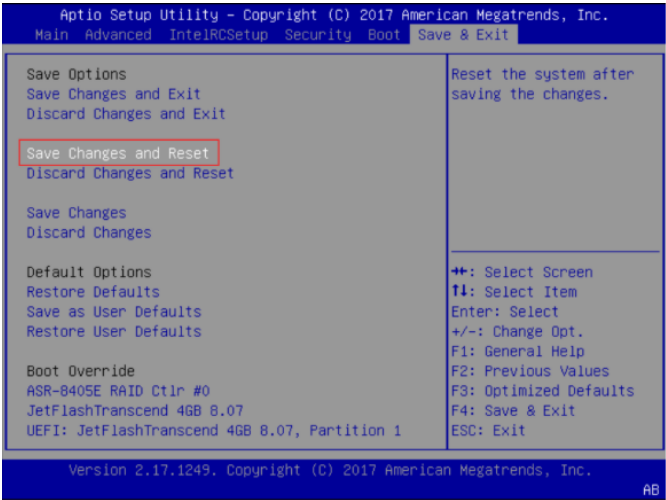
6. После окончания установки перезагрузите устройство, выбрав пункт меню **Reboot/Poweroff**.



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.

Обновление микрокода IPMI на аппаратных платформах D200, D500, E1000, E3000, F8000

Product: UserGate D200/D500, UserGate E1000/E3000, UserGate F8000

Модели D, E и F аппаратных платформ UserGate оснащены модулем IPMI (Intelligent Platform Management Interface), который необходим для удаленного управления и мониторинга аппаратной части. Управление по IPMI работает независимо от операционной системы сервера. Для удаленного управления используется веб-интерфейс.

Примечание Данная процедура обновления микрокода контроллера модуля удаленного управления IPMI предназначена для аппаратных платформ UserGate D200/D500, E1000/E3000 и F8000.

Обновление микрокода платы IPMI

Для управления по IPMI используется Ethernet-порт «Management» (MGMT).

Для обновления IPMI выполните следующие шаги:

1. Скачайте архив с последним обновлением по [ссылке](#).
 - SHA-256: d6fb3902e886ae000073b414479ccff4f08bb639b70841a710dc903605f68a05
 - MD5: 0d464c86b82efe0fb0d6235ec487d133
 - СТРИБОГ-256: 85A54244D9B393CE304EEDE53BF7AAF86BC908F9238E7E6101AAAC63AC5B64E
 2. Извлеките из архива файлы обновления.
 3. Подключите компьютер к порту управления IPMI на устройстве.
 4. Откройте веб-браузер и перейдите по адресу управления IPMI (<https://192.168.0.100>). Для первоначальной авторизации используйте «admin» в качестве логина и пароля пользователя. Сетевой адаптер вашего компьютера должен быть настроен с IP-адресом из сети 192.168.0.0/24.
- Примечание** При изменении пароля пользователя его длина не должна превышать 16 символов.
5. Перейдите на вкладку **Maintenance** и выберите **Firmware Update**.

6. При обновлении микрокода с целью устранения критической уязвимости убедитесь, что флажок в поле **Preserve all configuration** не установлен. В этом случае в процессе обновления произойдет сброс всех настроек IPMI. Нажмите **Enter Update Mode** для перехода в режим обновления микрокода.

7. В поле **Upload Firmware** выберите файл `ipmi_UG.ima` из раскрытого ранее архива обновления и нажмите **Upload**. Проверьте информацию о текущей и новой версии микрокода и нажмите **Proceed**. По окончании обновления плата IPMI будет перезагружена.

Примечание При обновлении прошивки микрокода IPMI версии 1.10 для устранения уязвимости SUM-23033 номер версии не меняется. Изменится дата создания прошивки (NOV 25 2025).

8. Проверьте результат. Подключитесь снова к веб-консоли управления: в браузере перейдите по адресу <https://192.168.0.100>. Проверьте результат обновления. Дата создания прошивки должна измениться.

Обновление завершено.

Обновление микрокода платы IPMI с помощью USB-накопителя

Если доступ к консоли управления IPMI утерян, вы можете обновить микрокод с помощью USB-накопителя.

Примечание При обновлении микрокода с помощью USB-накопителя произойдет сброс всех настроек IPMI.

Для обновления микрокода с помощью USB-накопителя выполните следующие шаги:

1. Скачайте ПО Rufus по [ссылке](#) и запустите его.
2. С помощью ПО Rufus отформатируйте USB-накопитель в формате FAT16/32 и сделайте его загрузочным (метод загрузки MS-DOS):

3. Скачайте архив с последним обновлением по [ссылке](#).

- SHA-256: d6fb3902e886ae00000073b414479ccff4f08bb639b70841a710dc903605f68a05
- MD5: 0d464c86b82efe0fb0d6235ec487d133
- СТРИБОГ-256: 85A54244D9B393CE304EEDE53BF7AAF86BC908F9238E7E6101AAAAC63AC5B64E

4. Распакуйте архив и скопируйте файлы на подготовленный ранее USB-накопитель.

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

6. Подключите к устройству подготовленный USB-накопитель с файлами обновления микрокода.

7. Войдите в BIOS устройства, нажав клавишу **Delete** на первоначальном этапе загрузки. В меню настроек **Boot** в параметре **Boot Option #1** выберите USB-устройство:

8. Выйдите из настроек BIOS с сохранением изменений.

9. Загрузите устройство с USB-накопителя. При загрузке выберите пункт меню **2** (выбор будет доступен в течении нескольких секунд):

10. Введите команду: `ipmi.bat`.

11. Дождитесь завершения процесса (примерно 5 минут).

12. После обновления прошивки выключите устройство и отключите кабели питания от него на 5 минут.

13. Подключите кабели питания, дождитесь появления линка на порту Management, попробуйте подключиться:

- В браузере перейдите по адресу <https://192.168.0.100> (сетевой адаптер вашего компьютера должен быть настроен с IP-адресом из сети 192.168.0.0/24);
- Для первоначальной авторизации используйте «admin» в качестве логина и пароля.

Примечание При изменении пароля пользователя его длина не должна превышать 16 символов.

Обновление завершено.

Обновление микрокода IPMI на аппаратных платформах E1010, E3010, F8010

Product: UserGate E1010/E3010, UserGate F8010

Documentation: 

Эта процедура обновления микрокода контроллера модуля удаленного управления IPMI предназначена для аппаратных платформ UserGate E1010/E3010 и F8010.

Для обновления микрокода необходимо выполнить следующие шаги:

1. Скачайте ПО Rufus по [ссылке](#) и запустите его.
2. С помощью ПО Rufus отформатируйте USB-накопитель в формате FAT16/32 и сделайте его загрузочным (метод загрузки MS-DOS):
3. Скачайте архив обновления микрокода контроллера из личного кабинета [на официальном сайте UserGate](#).
4. Распакуйте архив и скопируйте файлы на подготовленный ранее USB-накопитель.
5. Подключите к устройству (ПАК UserGate) внешний монитор и USB-клавиатуру.
6. Подключите к устройству подготовленный USB-накопитель с файлами обновления микрокода.
7. Войдите в BIOS устройства, нажав клавишу **Delete** на первоначальном этапе загрузки. В меню настройки **Boot** в параметре **Boot Option #1** выберите USB-устройство:
8. Выйдите из настройки BIOS с сохранением изменений.
9. Загрузите устройство с USB-накопителя. При загрузке выберите пункт меню **2** (выбор будет доступен в течении нескольких секунд):

10. Введите команду: `ipmi.bat`.

11. Подтвердите начало процесса прошивки, нажав клавишу **Y**:

12. Дождитесь завершения процесса (примерно 25 минут).

13. После обновления прошивки выключите устройство и отключите кабели питания от него на 5 минут.

14. Подключите кабели питания, дождитесь появления линка на порту MGMT, попробуйте подключиться:

- В браузере перейдите по адресу URL <https://192.168.0.100> (сетевой адаптер вашего компьютера должен быть настроен с IP-адресом из сети 192.168.0.0/24);
- Для первоначальной авторизации используйте в качестве логина/пароля: `admin/admin`.

Примечание При изменении пароля придерживайтесь следующих правил: длина пароля — от 8 до 16 символов; обязательно использование символов не менее чем из трех категорий: строчные латинские буквы, заглавные латинские буквы, цифры (0-9), специальные символы (~, !, @, #, \$, %, ^, &, *).

Обновление завершено.

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.
- ncpmc — 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.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.

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_ugls_full_update_7.x.x.xxxxxxR.tar.gz — для моделей C150, C151, X10, D250, FG;
- ngfw_ugrc_full_update_7.x.x.xxxxxxR.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-ugls-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 http://192.168.1.2/ugos/ngfw-ugls-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>
```

Офлайн-активация лицензий необходима для устройств UserGate, находящихся в изолированной сети без доступа к интернету.

Процесс лицензирования включает следующие этапы:

1. Генерация запроса — создание на лицензируемом устройстве файла запроса на офлайн-активацию.
2. Активация запроса — обработка сгенерированного файла запроса с помощью сервиса офлайн-активации ПИН-кодов.
3. Применение лицензии — загрузка активированного файла обратно на лицензируемое устройство.

Генерация запроса

Чтобы сгенерировать файл запроса на офлайн-активацию лицензии, зайдите с помощью веб-браузера на лицензируемое устройство по следующему адресу:

- <https://IP-address:8001?features=offline-reg> — для NGFW, WAF, DCFW;
- <https://IP-address:8010?features=offline-reg> — для MC, LogAn, SIEM.

Где IP-address — это IP-адрес лицензируемого устройства.

В веб-консоли устройства перейдите на вкладку **Дашборд**.

В виджете **Лицензия** нажмите на строку **Нет лицензии**.

В окне активации продукта нажмите на строку **Начать активацию в автономном режиме**:



Введите ПИН-код устройства а нажмите **Далее**:

Скачайте сгенерированный файл запроса на офлайн-активацию:

Активация запроса

С компьютера, имеющего доступ в интернет, обратитесь в [сервис офлайн-активации ПИН-кодов](#). Для входа в сервис потребуется авторизация в [Едином центре авторизации](#).

На странице сервиса офлайн-активации нажмите **Выбрать** и добавьте файл с запросом на офлайн-активацию, полученный с лицензируемого устройства:

Выберите версию ПО активируемого устройства и нажмите **Обработать**:

Подтвердите операцию активации:

В случае успешной активации файла отобразится статус: «Успешно активирован». Скачайте активированный файл, нажав на значок со стрелкой в столбце **Действия**:

Если активация не была успешной, отобразится статус: «Ошибка активации».

При нажатии на статус отобразится описание возможной причины ошибки.

Применение лицензии

Загрузите активированный файл на лицензируемое устройство. Для этого:

1. В виджете **Лицензия** на вкладке **Дашборд** лицензируемого устройства откройте окно офлайн-активации.
2. Выберите опцию **Завершить активацию в автономном режиме**:

A rectangular box with an orange border, representing a screenshot of a software interface window.

3. В открывшемся окне укажите активированный файл, полученный в сервисе офлайн-активации, и нажмите **Далее**:

Процесс лицензирования завершен.

Экспорт и импорт политик UserGate через CLI

Product: NGFW
Version: 7.x
ПримечаниеЭкспорт и импорт правил с использованием CLI доступен с версии 7.0.0.

Импорт доступен в следующих разделах:

- Сеть: правила DNS;
- Пользователи и устройства: правила captive-портала;
- Политики сети: правила межсетевого экрана, NAT и маршрутизации, пропускной способности;
- Политики безопасности: правила фильтрации контента, веб-безопасности, инспектирования туннелей, инспектирования SSL, инспектирования SSH, защиты почтового трафика, ICAP, защиты DoS, системы обнаружения и предотвращения вторжений, сценарии;
- Глобальный портал: правила веб-портала и reverse-прокси;
- VPN: серверные и клиентские правила.

Указанные выше правила настраиваются с использованием UserGate Policy Language (UPL), подробную информацию о котором вы можете найти в соответствующем [разделе](#) руководства администратора.

Рассмотрим экспорт и импорт правил на примере правил межсетевого экрана. На NGFW созданы следующие правила:

Межсетевой экран														
+ Добавить Редактировать Удалить Переместить Копировать Включить Отключить Скопировать ID правила Открыть логи Сбросить счётчики Все Принуд														
✓														
#	С...	Название	Действие	Зона источ...	Адрес ...	Зона назначения	Адрес н...	Пользовате...	Сервис	Приложения	Время	Сценарий	Кол-во с...	Исто...
1	(...)	web1	Запретить	Trusted	Любой	Любая	Любой	Любой	Любой	Любое	Любое	—	0	Среа...
2	(...)	web2	Запретить	DMZ	Любой	Untrusted	Любой	Любой	Любой	Любое	Любое	—	0	Среа...
3	(...)	web3	Разрешить	Любая	Любой	Любая	Любой	Любой	Любой	Любое	Любое	—	0	Среа...
4	(...)	Default block	Запретить	Любая	Любой	Любая	Любой	Любой	Любой	Любое	Любое	—	—	—

ПримечаниеПравила созданы для демонстрации примера.
ПримечаниеПосле выполнения импорта все существующие правила раздела будут заменены на импортированные.

1. Для редактирования правила могут быть сохранены в файл конфигурации или скопированы из интерфейса командной строки. В обоих вариантах используется подключение к интерфейсу командной строки по SSH.

Для сохранения правил в файл, например, `fw_config.cfg`, выполните следующую команду:

```
ssh Admin@IP_ADDRESS -p 2200 show network-policy firewall >fw_config.cfg
```

где Admin - имя администратора;

IP_ADDRESS - адрес интерфейса UserGate.

Введите пароль учетной записи администратора, файл со списком правил будет сохранён на вашем устройстве.

Для копирования правил из интерфейса командной строки подключитесь к CLI по SSH:

```
ssh Admin@IP_ADDRESS -p 2200
```

где Admin - имя администратора;

IP_ADDRESS - адрес интерфейса UserGate.

Подключение по SSH необходимо для возможности копирования правил.

ПримечаниеКоманды выполняются в режиме конфигурации.

Для перехода в режим конфигурации используйте следующую команду:

```
Admin@UGOS> configure
```

Отобразите в CLI правила раздела, которые необходимо выгрузить:

```
Admin@UGOS# show network-policy firewall
```

ПримечаниеИспользуйте `Tab` или `?` для просмотра текущих возможных значений или автодополнения.

Также действия над правилами могут быть выполнены после перехода на уровень раздела, в таком случае не нужно указывать уровень для каждой команды:

```
Admin@UGOS# edit network-policy firewall
```

```
[ network-policy firewall ]  
Admin@UGOS# show
```

Результат выполнения команды:

```
[ network-policy firewall ]  
Admin@UGOS# show  
% ----- 1 -----  
DENY \  
  src.zone = Trusted \  
  enabled(true) \  
  id(ba1abe50-f492-4e12-8a12-86df83b40a81) \  
  name(web1)  
% ----- 2 -----  
DENY \  
  src.zone = DMZ \  
  dst.zone = Untrusted \  
  enabled(true) \  
  id(dd3b23e2-261d-48a5-8e63-3967ceb840b6) \  
  name(web2)  
% ----- 3 -----  
PASS \  
  enabled(true) \  
  id("4e537010-322e-45e8-a1e1-7390f2300bce") \  
  name(web3)
```

2. Скопируйте правила для редактирования; используйте, например, текстовый редактор.

ПримечаниеНе копируйте строку с позицией первого правила.

Отредактируйте необходимые параметры правила. Для примера изменим названия правил на `cli1`, `cli2` и `cli3`, соответственно:

```
DENY \  
  src.zone = Trusted \  
  enabled(true) \  
  id(ba1abe50-f492-4e12-8a12-86df83b40a81) \  
  name(cli1)
```

```
name(cli1)
% ----- 2 -----
DENY \
src.zone = DMZ \
dst.zone = Untrusted \
enabled(true) \
id(dd3b23e2-261d-48a5-8e63-3967ceb840b6) \
name(cli2)
% ----- 3 -----
PASS \
enabled(true) \
id("4e537010-322e-45e8-a1e1-7390f2300bce") \
name(cli3)
```

3. Импортируйте правила. Выделите и скопируйте правила в редакторе. Перейдите в CLI, введите команду **import upl-rule** и вставьте скопированные правила:

```
[ network-policy firewall ]
Admin@UGOS# import upl-rule DENY \
... src.zone = Trusted \
... enabled(true) \
... id(ba1abe50-f492-4e12-8a12-86df83b40a81) \
... name(cli1)
... % ----- 2 -----
... DENY \
... src.zone = DMZ \
... dst.zone = Untrusted \
... enabled(true) \
... id(dd3b23e2-261d-48a5-8e63-3967ceb840b6) \
... name(cli2)
... % ----- 3 -----
... PASS \
... enabled(true) \
... id("4e537010-322e-45e8-a1e1-7390f2300bce") \
... name(cli3)
...
[ network-policy firewall ]
Admin@UGOS#
```

4. Проверьте изменения в CLI:

```
[ network-policy firewall ]
Admin@UGOS# show

% ----- 1 -----
DENY \
src.zone = Trusted \
enabled(true) \
id("082ed6ed-20b6-4c93-921a-047eb9ff40a4") \
name(cli1)
% ----- 2 -----
DENY \
src.zone = DMZ \
dst.zone = Untrusted \
enabled(true) \
id(f5f08dbd-019f-490a-8cfa-342c34a348fa) \
name(cli2)
% ----- 3 -----
PASS \
enabled(true) \
id(b5ad3589-98d4-4911-8cf2-9590d0f3f4ea) \
name(cli3)
```

или веб-интерфейсе:

Межсетевой экран

Добавить

Редактировать

Удалить

Переместить

Копировать

Включить

Отключить

Скопировать ID правила

Открыть логи

Сбросить счётчики

Все

Принуд

✓

🔍

#	C...	Название	Действие	Зона источ...	Адрес ...	Зона назначения	Адрес н...	Пользовате...	Сервис	Приложения	Время	Сценарий	Кол-во с...	Исто...
1	(...)	cli1	🚫 Запретить	🖥️ Trusted	Любой	Любая	Любой	Любой	Любой	Любое	Любое	—	0	Среа...
2	(...)	cli2	🚫 Запретить	🖥️ DMZ	Любой	🖥️ Untrusted	Любой	Любой	Любой	Любое	Любое	—	0	Среа...
3	(...)	cli3	✅ Разрешить	Любая	Любой	Любая	Любой	Любой	Любой	Любое	Любое	—	0	Среа...
4	(...)	Default block	🚫 Запретить	Любая	Любой	Любая	Любой	Любой	Любой	Любое	Любое	—	—	—

Импорт настроек из файлов конфигурации кластера NGFW

Product: NGFW
Version: 7.x

Внимание!Лицензионные ключи версий 6 и 7 несовместимы. Перед обновлением до версии 7 необходимо запросить у менеджера ключ.

Администратор UserGate NGFW имеет возможность импортировать настройки узлов кластера NGFW из сохраненного ранее файла экспорта настроек кластера. В отличие от резервного копирования, экспорт/импорт настроек не сохраняет текущее состояние всех компонентов комплекса, сохраняются только текущие настройки.

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

Процедура импорта настроек узлов кластера NGFW включает в себя следующие основные шаги:

- 1. Экспорт настроек узлов исходного кластера NGFW.
- 2. Импорт настроек мастер-узла нового кластера.
- 3. Импорт настроек резервного узла нового кластера.

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

Импорт настроек мастер-узла приведёт к перезагрузке. В процессе перезагрузки будет выполнена процедура factory reset (откат к первоначальному состоянию), затем узел загрузится с импортированными настройками, кроме настроек кластера конфигурации (настройки кластера отказоустойчивости будут импортированы). Мастер-узел перестанет "видеть" резервный узел. Резервный узел нужно будет добавить в кластер конфигурации заново.

Импорт настроек резервного узла приведёт к перезагрузке. В процессе перезагрузки будет выполнена процедура factory reset (откат к первоначальному состоянию), затем узел загрузится в состояние первоначальной настройки. Внутреннее имя узла будет соответствовать импортированному имени старого резервного узла.

Экспорт настроек узлов кластера NGFW

1. Для экспорта настроек узлов исходного кластера NGFW в веб-консоли администратора любого из узлов кластера перейдите на вкладку **Настройки**, затем в раздел **UserGate → Управление устройством → Экспорт и импорт настроек**, нажмите **Экспорт** и выберите **Экспортировать все настройки**.



2. Сохраните созданный файл экспорта настроек узлов кластера.

Импорт настроек мастер-узла кластера

Важно!При импорте конфигурации NGFW с версий 7.X, при наличии в правилах доменных пользователей/групп, обязательно должен быть доступен LDAP-сервер для валидации пользователей, иначе правила будут импортированы без условия «Пользователи».

1. В веб-консоли узла, на который необходимо перенести настройки мастер-узла кластера, перейдите на вкладку **Настройки**, затем в раздел **UserGate → Управление устройством → Экспорт и импорт настроек** и нажмите **Импорт**:



2. В открывшемся окне импорта нажмите **Выберите файл** и выберите сохраненный ранее файл экспорта настроек узлов кластера:

3. Выберите **Импортировать все настройки** и нажмите **Выбрать узлы**:

4. Выберите будущую роль узла в кластере (в данном случае **Мастер-узел**) и название узла из файла экспорта. Нажмите **Старт**:

5. Узел перейдет в режим перезагрузки:

В процессе перезагрузки будет выполнена процедура factory reset (откат к первоначальному состоянию), затем применятся импортированные настройки конфигурации и узел загрузится с настройками мастер-узла из файла экспорта, включая импортированное название старого узла.

ПримечаниеИмпорт настроек не восстанавливает информацию о лицензии. После окончания процедуры импорта необходимо повторно зарегистрировать NGFW с помощью имеющегося ПИН-кода.

Импорт настроек мастер-узла завершен.

Импорт настроек резервного узла кластера

Импорт настроек резервного узла кластера состоит из следующих основных этапов:

1. Первичная инициализация узла без добавления его в кластер и активации лицензии.
2. Импорт всех настроек резервного узла. Узел уйдёт в перезагрузку, в процессе перезагрузки будет выполнена процедура factory reset (откат к первоначальному состоянию), затем узел загрузится в состояние первоначальной настройки.
3. Добавление узла в кластер конфигурации.
4. Импорт только сетевых настроек узла.

Подробнее о шагах импорта настроек резервного узла кластера:

1. Выполните первичную инициализацию узла согласно процедуре в разделе [«Первоначальная настройка»](#).
2. Импортируйте настройки резервного узла.
 - 2.1. В веб-консоли узла, на который необходимо перенести настройки резервного узла кластера, перейдите на вкладку **Настройки**, затем в раздел **UserGate → Управление устройством → Экспорт и импорт настроек** и нажмите **Импорт**:



2.2.. В открывшемся окне импорта нажмите **Выберите файл** и выберите сохраненный ранее файл экспорта настроек узлов кластера:

2.3. Выберите **Импортировать все настройки** и нажмите **Выбрать узлы**:

2.4. Выберите будущую роль узла в кластере (в данном случае **Slave-узел**) и название узла из файла экспорта. Нажмите **Старт**:

2.5. Узел перейдет в режим перезагрузки:

В процессе перезагрузки будет выполнена процедура factory reset (откат к первоначальному состоянию), затем узел загрузится в состояние первоначальной настройки. Внутреннее имя узла будет соответствовать выбранному имени старого резервного узла — это необходимо, чтобы кластер отказоустойчивости собрался корректно. Само отображение имени можно будет изменить в веб-интерфейсе на вкладке **Настройки** → **UserGate** → **Управление устройством** → **Кластер конфигурации**.

3. Добавьте узел в кластер конфигурации.

Необходимо произвести первоначальную установку узла как дополнительного узла в кластере:



4. Импортируйте сетевые настройки узла.

4.1. После добавления узла в кластер в качестве резервного узла необходимо импортировать только сетевые настройки резервного узла из файла экспорта. Для этого в веб-консоли узла перейдите на вкладку **Настройки**, затем в раздел **UserGate** → **Управление устройством** → **Экспорт и импорт настроек** и нажмите **Импорт**.

Выберите **Импортировать только сетевые настройки** и нажмите **Выбрать узлы**.

4.2. Выберите название резервного узла и нажмите **Старт**:

4.3. Резервный узел импортирует сетевые настройки из файла конфигурации.

Если лицензия на узле не отображается активной, можно ускорить процесс импорта лицензии с мастер-узла, нажав **Проверить лицензию** в Дашборде резервного узла.

Импорт настроек узлов кластера завершен.

