

Table of Contents

Table of Contents	1
Управление конечными устройствами	2
Общие сведения	3
Создание шаблонов конечных устройств	4
Настройка параметров шаблонов конечных устройств	5
Создание группы шаблонов конечных устройств	14
Настройка интеграции конечных устройств с UserGate MC	15
Управление списком устройств	17
Настройка проверки требований безопасности (HIP)	20
Журналирование данных конечных устройств	22

Общие сведения

Version: 7.x

Product: UGMC

Documentation: 

Под конечными устройствами в UserGate Management Center (далее также — UserGate MC) понимаются устройства с операционной системой Windows, на которых установлен UserGate Client.

В веб-консоли UserGate MC [администраторы управляемой области](#) могут централизованно управлять подключенными конечными устройствами, а также настраивать параметры этих устройств. Подробная информация о взаимодействии UserGate MC и конечных устройств приведена в разделе «[Работа UserGate Client в связке с UserGate MC](#)» Руководства администратора UserGate Client.

Для подключения конечных устройств к UserGate MC необходимо выполнить следующее:

- 1) [создать шаблоны конечных устройств](#);
- 2) [настроить параметры шаблонов конечных устройств](#);
- 3) [создать группу шаблонов конечных устройств](#);
- 4) [настроить интеграцию конечных устройств с UserGate MC](#).

Подробнее об объектах, используемых в управляемой области UserGate MC, таких как шаблоны, группы шаблонов и управляемые устройства, — в разделе «[Шаблоны и группы шаблонов](#)».

После подключения конечных устройств вы также можете:

- [настроить проверку требований безопасности \(комплаенса\)](#) с помощью технологии Host Information Profile (HIP);
- [настроить подключение к внешнему серверу журналирования](#) для хранения и анализа событий конечных устройств.

Version: 7.x

Product: UGMC

Documentation: 

ПримечаниеРекомендуется создавать отдельные шаблоны для разных категорий параметров, например такие, как шаблон общих параметров или шаблон библиотек. Это упростит дальнейшую работу с шаблонами при их объединении в группы.

Чтобы создать шаблон конечных устройств:

1. В разделе **Управление областью → Конечные устройства → Шаблоны** нажмите **Добавить**.
2. На вкладке **Общие** укажите название и при необходимости описание шаблона.
3. При необходимости на вкладке **Разделы** установите флажок **Настроить отображение разделов** и выберите разделы веб-консоли, которые должны отображаться в шаблоне.

ПримечаниеВыбор разделов доступен начиная с версии 7.6.0.

4. Нажмите **Сохранить**.

Созданный шаблон отобразится в таблице **Шаблоны**. Теперь вы можете перейти к настройке его параметров. Параметры шаблона распространятся на все управляемые конечные устройства, к которым будет применен шаблон в составе группы.

Documentation: 

Version: 7.x

Product: UGMC

Вы можете настраивать параметры выбранного шаблона конечных устройств в следующих разделах:

- **Консоль администратора → Настройки** — [общие параметры](#) работы UserGate Client. С помощью этих параметров вы можете настроить:
 - сбор данных конечных устройств;
 - сетевую доступность конечного устройства при остановке UserGate Client;
 - режим отключения правил межсетевого экрана;
 - режим удаления UserGate Client;
 - оповещения на конечном устройстве;
 - интеграцию с сервером журналирования (UserGate Log Analyzer или UserGate SIEM).
- **Консоль администратора → Настройка VPN** — [параметры VPN-профилей](#). В профиле вы можете указать адрес VPN-сервера, протокол VPN-соединения, алгоритм шифрования и способ аутентификации.
- **Политики сети → Межсетевой экран** — [правила межсетевого экрана](#) для фильтрации трафика конечных устройств.
- **Библиотеки** — [списки элементов](#) (например, IP-адресов, URL-адресов, типов контента) для использования в правилах межсетевого экрана.

При настройке параметров шаблона конечных устройств следует учитывать следующее:

- Если в шаблоне не указано значение параметра, используется значение по умолчанию.
- Библиотеки элементов шаблона (например, IP-адреса, URL-списки, а также типы контента) по умолчанию не содержат данных. Перед настройкой параметров шаблона следует добавить необходимые элементы библиотек.

Настройка общих параметров

Важно! Для применения изменений на конечном устройстве при настройке любого из общих параметров в окне свойств этого параметра необходимо установить флажок «Синхронизировать».

Чтобы настроить общие параметры шаблона конечных устройств:

1. В разделе **Конечные устройства** (для версий ниже 7.6.0 раздел **Конечные устройства-конфигурация**) для объекта **Шаблон** в выпадающем списке выберите шаблон, параметры которого необходимо настроить.
2. Выберите раздел **Консоль администратора → Настройки**.
3. В блоке параметров **Настройки инсталляции UserGate Client** выполните следующие действия:

- Если требуется, отключите сбор информации о конечном устройстве.

При этом UserGate MC будет получать только основную информацию о конечном устройстве: IP-адрес, имя, версию UserGate Client, версию Windows, текущее время на устройстве и время его последнего подключения к UserGate MC, а также данные об объеме используемой памяти и о загрузке центрального процессора конечного устройства.

Важно! При отключенном сборе информации о конечном устройстве HIP-профили могут работать некорректно.

- Если требуется, запретите сетевой доступ к конечному устройству при остановке работы UserGate Client.

- Если требуется, настройте режим отключения правил межсетевого экрана.

Вы можете запретить или разрешить пользователям конечного устройства самостоятельно отключать правила межсетевого экрана. Кроме того, вы можете установить доступное количество и продолжительность отключений, а также указать код для подтверждения отключения на конечном устройстве.

- Если требуется, настройте режим удаления UserGate Client на конечном устройстве.

Вы можете запретить или разрешить пользователям конечного устройства самостоятельно удалять UserGate Client. Кроме того, вы можете указать код подтверждения удаления на конечном устройстве.

4. В блоке параметров **Оповещения** выполните следующие действия:

- Если требуется, отключите отображение иконки UserGate Client в области уведомлений панели задач Windows.
- Если требуется, настройте показ оповещений на конечном устройстве с помощью параметра **Показывать тултипы оповещений**:
 - при включенном параметре оповещения отображаются;
 - при отключенном параметре оповещения не отображаются (даже если они настроены для конкретных событий).
- Если требуется, настройте оповещения для конкретных событий: о блокировании и разблокировании конечного устройства, а также о блокировании адреса ресурса.

5. Если требуется отправлять данные конечных устройств в UserGate Log Analyzer или UserGate SIEM, в блоке параметров **Настройки устройства LogAn/SIEM** настройте интеграцию с внешним сервером журналирования. Подробная информация приведена в разделе «[Журналирование данных конечных устройств](#)».

Настройка параметров VPN-профиля

Примечание Подключение конечных устройств к VPN-серверу доступно на Windows 10 и выше. При разрыве соединения UserGate Client выполняет попытки восстановить его в течение 40 секунд. Если соединение не будет восстановлено, отобразится окно выбора VPN-сервера.

Настройка параметров VPN-профиля для версий ниже 7.6.0

Чтобы настроить параметры VPN-профиля шаблона конечных устройств:

1. В разделе **Конечные устройства-конфигурация** для объекта **Шаблон** в выпадающем списке выберите шаблон, параметры которого необходимо настроить.
2. Выберите раздел **Консоль администратора → Настройка VPN**.
3. Нажмите **Добавить**.
3. На вкладке **Общие** выполните следующее:
 - Включите VPN-профиль.
 - Укажите название и при необходимости описание VPN-профиля.
 - Укажите доменное имя или IP-адрес VPN-сервера.

Примечание Если доменному имени VPN-сервера соответствует несколько IP-адресов, UserGate Client использует первый адрес, от которого пришел ответ на запрос.

- Выберите протокол:
 - **IPSec L2TP**: для создания туннеля используется протокол L2TP, для защиты передаваемых данных — протокол IPSec.
При выборе **IPSec L2TP** также необходимо выбрать режим работы протокола IKE для согласования алгоритмов шифрования и аутентификации и указать общий ключ шифрования.
Примечание Начиная с версии 7.5.0 поддержка IPSec L2TP прекращена.
 - **IKEv2 с сертификатом**: для создания туннеля используется протокол IKEv2, для проверки подлинности сервера и клиента — сертификаты.
Важно! При генерации клиентского сертификата необходимо указать идентификатор пользователя (CN).
 - **IKEv2 с именем и паролем**: для создания туннеля используется IKEv2, для проверки клиента — логин и пароль (EAP-MSCHAP v2). Метод доступен только для пользователей доменного RADIUS-сервера.

Примечание При использовании протокола IKEv2 вы можете настроить многофакторную аутентификацию через одноразовые коды TOTP. Код вводится на конечном устройстве после выбора сертификата или ввода логина и пароля. Перед настройкой TOTP для пользователей доменного RADIUS-сервера необходимо разрешить на этом сервере использование протокола PAP.

4. На вкладке **Фаза 1** укажите параметры первой фазы создания VPN-соединения:

- **Время жизни ключа** — время, по истечении которого выполняется повторная аутентификация.
- **Dead peer detection** — проверка доступности соседнего устройства:
 - **Отключена** — проверка не выполняется.
 - **Всегда включена** — проверка выполняется с указанным интервалом. При отсутствии ответа каждые 5 секунд отправляются дополнительные DPD-запросы. Количество этих запросов задается в поле **Неудачных попыток**. При отсутствии ответа соединение разрывается.
 - **При отсутствии трафика** — проверка выполняется, только когда нет трафика через туннель. Если в течение двойного

указанного интервала нет пакетов, отправляется DPD-запрос. При отсутствии ответа каждые 5 секунд отправляются дополнительные DPD-запросы. Количество этих запросов задается в поле **Неудачных попыток**. При отсутствии ответа соединение разрывается.

- **Diffie-Hellman группы** — выбор группы для обмена ключами (чем выше номер группы, тем надежнее ключ шифрования).
- **Безопасность** — выбор способов аутентификации и алгоритмов шифрования (применяются поочередно сверху вниз).

5. На вкладке **Фаза 2** укажите параметры второй фазы создания VPN-соединения:

- **Время жизни ключа** — время, по истечении которого ключ шифрования будет изменен.
- **Максимальный размер данных** — объем данных, после передачи которого ключ шифрования будет изменен.

Примечание Если заданы оба параметра (время жизни ключа и максимальный размер данных), ключ шифрования будет изменен по достижении первого из лимитов.

- **Безопасность** — выбор способов аутентификации и алгоритмов шифрования (применяются поочередно сверху вниз).

6. Нажмите **Сохранить**.

Настройка параметров VPN-профиля для версий 7.6.0 и выше

Вы можете настраивать VPN-профили шаблона конечных устройств для протоколов DTLS и IKEv2. Использование протокола IKEv2 является стандартным решением с широкой совместимостью и подходит для большинства корпоративных сценариев. Протокол DTLS может применяться для подключения удаленных сотрудников, так как обеспечивает более высокую производительность и устойчивость к потерям пакетов. Ниже приведены инструкции по настройке VPN-профилей для каждого из этих протоколов.

Примечание При использовании протокола IKEv2 вы можете настроить многофакторную аутентификацию через одноразовые коды TOTP. Код вводится на конечном устройстве после выбора сертификата или ввода логина и пароля. Перед настройкой TOTP для пользователей доменного RADIUS-сервера необходимо разрешить на этом сервере использование протокола PAP.

Чтобы настроить параметры VPN-профиля для протокола DTLS:

1. В разделе **Конечные устройства** для объекта **Шаблон** в выпадающем списке выберите шаблон, параметры которого необходимо настроить.
2. Выберите раздел **Консоль администратора → Настройка VPN**.
3. Нажмите **Добавить → DTLS**.
4. На вкладке **Общие** выполните следующее:
 - Включите VPN-профиль, установив флажок **Включено**.
 - Укажите название и при необходимости описание VPN-профиля.
 - Укажите доменное имя или IP-адрес VPN-сервера.

Примечание Если доменному имени VPN-сервера соответствует несколько IP-адресов, UserGate Client использует первый адрес, от которого пришел ответ на запрос.

- Выберите режим аутентификации:
 - **AAA** — по логину и паролю (только для пользователей доменного RADIUS-сервера).
 - **PKI** — с использованием цифровых сертификатов.

5. На вкладке **Фаза 1** укажите параметры первой фазы создания VPN-соединения:

- **Время жизни ключа** — время, по истечении которого выполняется повторная аутентификация.
- **Dead peer detection** — проверка доступности соседнего устройства:
 - **Отключена** — проверка не выполняется.
 - **Всегда включена** — проверка выполняется с указанным интервалом. При отсутствии ответа каждые 5 секунд отправляются дополнительные DPD-запросы. Количество этих запросов задается в поле **Неудачных попыток**. При отсутствии ответа соединение разрывается.
 - **При отсутствии трафика** — проверка выполняется, только когда нет трафика через туннель. Если в течение двойного указанного интервала нет пакетов, отправляется DPD-запрос. При отсутствии ответа каждые 5 секунд отправляются дополнительные DPD-запросы. Количество этих запросов задается в поле **Неудачных попыток**. При отсутствии ответа соединение разрывается.
- **Безопасность** — выбор набора шифров DTLS из списка (применяются поочередно сверху вниз).

6. На вкладке **Фаза 2** укажите объем данных, после передачи которого ключ шифрования будет изменен.

7. Нажмите **Сохранить**.

Чтобы настроить параметры VPN-профиля для протокола IKEv2:

1. В разделе **Конечные устройства** для объекта **Шаблон** в выпадающем списке выберите шаблон, параметры которого необходимо настроить.
2. Выберите раздел **Консоль администратора → Настройка VPN**.

3. Нажмите **Добавить** → **IKEv2**.

4. На вкладке **Общие** выполните следующее:

- Включите VPN-профиль, установив флажок **Включено**.
- Укажите название и при необходимости описание VPN-профиля.
- Укажите доменное имя или IP-адрес VPN-сервера.

Примечание Если доменному имени VPN-сервера соответствует несколько IP-адресов, UserGate Client использует первый адрес, от которого пришел ответ на запрос.

- Выберите режим аутентификации:
 - **AAA** — по логину и паролю (только для пользователей доменного RADIUS-сервера).
 - **PKI** — с использованием цифровых сертификатов.

5. На вкладке **Фаза 1** укажите параметры первой фазы создания VPN-соединения:

- **Время жизни ключа** — время, по истечении которого выполняется повторная аутентификация.
- **Dead peer detection** — проверка доступности соседнего устройства:
 - **Отключена** — проверка не выполняется.
 - **Всегда включена** — проверка выполняется с указанным интервалом. При отсутствии ответа каждые 5 секунд отправляются дополнительные DPD-запросы. Количество этих запросов задается в поле **Неудачных попыток**. При отсутствии ответа соединение разрывается.
 - **При отсутствии трафика** — проверка выполняется, только когда нет трафика через туннель. Если в течение двойного указанного интервала нет пакетов, отправляется DPD-запрос. При отсутствии ответа каждые 5 секунд отправляются дополнительные DPD-запросы. Количество этих запросов задается в поле **Неудачных попыток**. При отсутствии ответа соединение разрывается.
- **Diffie-Hellman группы** — выбор группы для обмена ключами (чем выше номер группы, тем надежнее ключ шифрования).
- **Безопасность** — выбор способов аутентификации и алгоритмов шифрования (применяются поочередно сверху вниз).

6. На вкладке **Фаза 2** укажите параметры второй фазы создания VPN-соединения:

- **Время жизни ключа** — время, по истечении которого ключ шифрования будет изменен.
- **Максимальный размер данных** — объем данных, после передачи которого ключ шифрования будет изменен.

Примечание Если заданы оба параметра (время жизни ключа и максимальный размер данных), ключ шифрования будет изменен по достижении первого из лимитов.

- **Безопасность** — выбор способов аутентификации и алгоритмов шифрования (применяются поочередно сверху вниз).

7. Нажмите **Сохранить**.

Настройка правил межсетевого экрана

Важно! Если правила межсетевого экрана не настроены, фильтрация трафика на конечных устройствах не выполняется.

Чтобы настроить правила межсетевого экрана шаблона конечных устройств:

1. В разделе **Конечные устройства** (для версий ниже 7.6.0 раздел **Конечные устройства-конфигурация**) для объекта **Шаблон** в выпадающем списке выберите шаблон, параметры которого необходимо настроить.

2. Выберите раздел **Политики сети** → **Межсетевой экран**.

3. Нажмите **Добавить**.

4. На вкладке **Общие** выполните следующее:

- Включите правило, установив флажок.
- Укажите название и при необходимости описание правила.
- Выберите область применения правила:
 - **Везде** — правило будет применяться всегда, независимо от местоположения конечного устройства.
 - **Внутри периметра** — правило будет применяться, если конечное устройство находится в доменной сети.
 - **Снаружи периметра** — правило будет применяться, если конечное устройство находится вне доменной сети.
- Выберите действие при срабатывании правила.
- При необходимости включите журналирование срабатываний правила.
- Укажите местоположение правила в списке правил.

5. На соответствующих вкладках укажите условия срабатывания правила.

Важно! Не рекомендуется одновременно использовать в правиле условия фильтрации по IP-адресу и URL-адресу, по IP-адресу и URL-категории, а также по IP-адресу и типу контента. Такое правило будет срабатывать на разных уровнях модели OSI, что может привести к

некорректной обработке трафика.

- На вкладке **Пользователи** укажите пользователей или группы пользователей LDAP, для которых будет применяться правило. Подробнее — в разделе «[Каталоги пользователей](#)».
- На вкладках **Источник**, **Назначение**, **Сервис**, **Приложения**, **URL**, **Категории URL**, **Типы контента**, **Время** выберите соответствующие [объекты библиотек](#) или создайте новые по ссылке **Создать и добавить новый объект**.

Начиная с версии 7.6.0 вы можете добавлять списки IP-адресов, сервисы, группы сервисов, а также URL-списки из общей библиотеки элементов (см. раздел «[Общая библиотека](#)»).

Примечание Для добавления условий срабатывания по URL-адресам, URL-категориям и типам контента в правиле должны быть указаны сервисы.

- На вкладке **НIP-профили** выберите [НIP-профили конечных устройств](#) из списка (по кнопке **Добавить**) или создайте новые (по ссылке **Создать и добавить новый объект**).
- На вкладке **Устройства** выберите конечные устройства, на которые будет распространяться правило.

Примечание На некоторых вкладках вы можете установить флажок «Инvertировать» (соответствует логическому отрицанию) — выбранные элементы будут исключены из условий срабатывания правила.

6. Нажмите **Сохранить**.

Управление библиотеками

Библиотеки содержат списки и группы таких элементов, как сервисы, IP-адреса, приложения, URL-адреса, URL-категории, типы контента и календари. Вы можете использовать эти списки и группы в правилах межсетевого экрана.

Настройка библиотеки сервисов

В библиотеке **Сервисы** вы можете добавлять сервисы, содержащие списки сетевых протоколов и портов. Для сервисов конечных устройств доступен выбор протоколов TCP и UDP.

Чтобы добавить сервис:

1. В разделе **Конечные устройства** (для версий ниже 7.6.0 раздел **Конечные устройства-конфигурация**) для объекта **Шаблон** в выпадающем списке выберите шаблон, параметры которого необходимо настроить.
2. Выберите раздел **Библиотеки → Сервисы**.
3. Нажмите **Добавить**.
4. В открывшемся окне выполните следующее:
 - укажите название и при необходимости описание сервиса;
 - нажмите **Добавить** и укажите сетевой протокол и порт;
 - нажмите **Сохранить**;
 - при необходимости добавьте другие порты и протоколы.
5. Нажмите **Сохранить**.

Настройка библиотеки групп сервисов

В библиотеке **Группы сервисов** вы можете объединять сервисы в группы. Это может понадобиться, например, если в нескольких правилах межсетевого экрана необходимо использовать одни и те же наборы сервисов.

Чтобы добавить группу сервисов:

1. В разделе **Конечные устройства** (для версий ниже 7.6.0 раздел **Конечные устройства-конфигурация**) для объекта **Шаблон** в выпадающем списке выберите шаблон, параметры которого необходимо настроить.
2. Выберите раздел **Библиотеки → Группы сервисов**.
3. В блоке **Группы сервисов** нажмите **Добавить**.
4. Укажите название и при необходимости описание группы сервисов.
5. Нажмите **Сохранить**.
6. Выберите добавленную группу сервисов.
7. В блоке **Элементы** нажмите **Добавить**.
8. С помощью клавиши Ctrl или Shift выберите сервисы из списка и нажмите **Добавить**.
9. Нажмите **Заккрыть**.

Добавленные сервисы отобразятся в блоке **Элементы** для выбранной группы.

Настройка библиотеки IP-адресов

В библиотеке **IP-адреса** вы можете добавлять статические группы IP-адресов (хранятся в UserGate MC) [и обновляемые группы IP-адресов](#) (загружаются с внешнего сервера).

Чтобы добавить статическую группу IP-адресов:

1. В разделе **Конечные устройства** (для версий ниже 7.6.0 раздел **Конечные устройства-конфигурация**) для объекта **Шаблон** в выпадающем списке выберите шаблон, параметры которого необходимо настроить.
2. Выберите раздел **Библиотеки → IP-адреса**.
3. В блоке **Группы** нажмите **Добавить**.
4. На вкладке **Общие** укажите параметры группы IP-адресов:
 - название и при необходимости описание;
 - уровень угрозы.
5. Нажмите **Сохранить**.
6. Выберите добавленную группу IP-адресов.
7. В блоке **Адреса из выбранной группы** нажмите **Добавить → Добавить элемент**.
8. Укажите IP-адрес.

Примечание В поле допускается вводить IP-адрес (например, 192.0.2.25), диапазоны IP-адресов (например, 192.0.2.1-192.0.2.25), а также адреса подсетей в формате CIDR (например, 192.0.2.0/24).

9. Нажмите **Сохранить**.
10. Для добавления других IP-адресов в группу повторите шаги 7-9 инструкции.

Добавленные IP-адреса отобразятся в блоке **Адреса из выбранной группы** для выбранной группы.

При необходимости вы можете добавить в статическую группу IP-адресов другие группы. Для этого в блоке **Адреса из выбранной группы** нажмите **Добавить → Добавить список**.

Настройка библиотеки групп приложений

В библиотеке **Группы приложений** вы можете добавлять статические группы приложений (хранятся в UserGate MC) [и обновляемые группы приложений](#) (загружаются с внешнего сервера).

Чтобы добавить статическую группу приложений:

1. В разделе **Конечные устройства** (для версий ниже 7.6.0 раздел **Конечные устройства-конфигурация**) для объекта **Шаблон** в выпадающем списке выберите шаблон, параметры которого необходимо настроить.
2. Выберите раздел **Библиотеки → Группы приложений**.
3. В блоке **Группы приложений** нажмите **Добавить**.
4. На вкладке **Общие** укажите параметры группы приложений:
 - название и при необходимости описание;
 - уровень угрозы.
5. Нажмите **Сохранить**.
6. Выберите добавленную группу приложений.
7. В блоке параметров **Приложения** нажмите **Добавить**.
8. Укажите название приложения и хеш-сумму его исполняемого файла (по алгоритму SHA1).

Примечание Вы можете определить хеш-сумму с помощью утилиты `fciv`.

9. Нажмите **Сохранить**.
10. Для добавления других приложений в группу повторите шаги 7-9 инструкции.

Добавленные приложения отобразятся в блоке **Приложения** для выбранной группы.

Настройка библиотеки URL-списков

В библиотеке **Списки URL** вы можете добавлять статические URL-списки (хранятся в UserGate MC) [и обновляемые URL-списки](#) (загружаются с внешнего сервера).

Чтобы добавить статический URL-список:

1. В разделе **Конечные устройства** (для версий ниже 7.6.0 раздел **Конечные устройства-конфигурация**) для объекта **Шаблон** в выпадающем списке выберите шаблон, параметры которого необходимо настроить.
2. Выберите раздел **Библиотеки → Списки URL**.
3. В блоке **Списки URL** нажмите **Добавить**.

4. На вкладке **Общие** укажите параметры URL-списка:

- название и при необходимости описание;
- содержимое:
 - **Чувствительный к регистру** — URL-адреса с учетом регистра (для контентной фильтрации);
 - **Нечувствительный к регистру** — URL-адреса без учета регистра (для контентной фильтрации);
 - **Домен** — доменные имена (для DNS-фильтрации).

5. Нажмите **Сохранить**.

6. Выберите добавленный URL-список.

7. В блоке **URL** нажмите **Добавить**.

8. Укажите URL-адрес или доменное имя.

Примечание При указании URL-адреса или доменного имени вы можете использовать символы «*» (любое количество произвольных символов), «^» (начало строки), «\$» (конец строки). Не допускается использование символов «?» и «#».

Например:

- ^example.domain.com\$ — доменное имя без поддоменов (с любыми протоколами и путями);
- ^http://domain.com/example\$ — только указанный URL-адрес;
- domain.com — доменное имя и все его поддомены (с любыми протоколами и путями);
- *example* — любые URL-адреса или доменные имена, содержащие example;
- ^example.domain.com/\$ — некорректное значение (символ «/» требует указания протокола).

9. Нажмите **Сохранить**.

10. Для добавления других URL-адресов и доменных имен повторите шаги 7-9 инструкции.

Добавленные URL-адреса и доменные имена отобразятся в блоке **URL** для выбранного списка.

Настройка библиотеки URL-категорий

В библиотеке **Категории URL** вы можете объединять URL-категории в статические группы URL-категорий (хранятся в UserGate MC) [и обновляемые группы URL-категорий](#) (загружаются с внешнего сервера). Это может понадобиться, например, если в нескольких правилах межсетевого экрана необходимо использовать одни и те же наборы URL-категорий.

Чтобы добавить статическую группу URL-категорий:

1. В разделе **Конечные устройства** (для версий ниже 7.6.0 раздел **Конечные устройства-конфигурация**) для объекта **Шаблон** в выпадающем списке выберите шаблон, параметры которого необходимо настроить.
2. Выберите раздел **Библиотеки → Категории URL**.
3. В блоке **Группы URL категорий** нажмите **Добавить**.
4. На вкладке **Общие** укажите название и при необходимости описание группы URL-категорий.
5. Нажмите **Сохранить**.
6. Выберите добавленную группу URL-категорий.
7. В блоке **Категории** нажмите **Добавить**.
8. С помощью клавиши Ctrl или Shift выберите URL-категории из списка категорий UserGate URL filtering и нажмите **Добавить**.

Подробнее о списке категорий UserGate URL filtering — в разделе «[Фильтрация контента](#)» руководства администратора UserGate NGFW.

9. Нажмите **Заккрыть**.

Добавленные URL-категории отобразятся в блоке **Категории** для выбранной группы.

Настройка библиотеки типов контента

В библиотеке **Типы контента** вы можете добавлять статические группы типов контента (хранятся в UserGate MC) [и обновляемые группы типов контента](#) (загружаются с внешнего сервера). Это может понадобиться, например, если в нескольких правилах межсетевого экрана необходимо использовать одни и те же наборы типов контента.

Чтобы добавить статическую группу типов контента:

1. В разделе **Конечные устройства** (для версий ниже 7.6.0 раздел **Конечные устройства-конфигурация**) для объекта **Шаблон** в выпадающем списке выберите шаблон, параметры которого необходимо настроить.
2. Выберите раздел **Библиотеки → Типы контента**.
3. В блоке **Категории** нажмите **Добавить**.

4. На вкладке **Общие** укажите название и при необходимости описание группы типов контента. 5. Нажмите **Сохранить**.

6. Выберите добавленную группу типов контента.

7. В блоке **Типы контента** нажмите **Добавить**.

8. Укажите тип контента в формате MIME.

Например, для ZIP-архивов необходимо указать `application/zip`.

Примечание Вы можете ознакомиться с реестром зарегистрированных MIME-типов на сайте www.iana.org.

9. Нажмите **Сохранить**.

10. Для добавления других типов контента повторите шаги 7-9 инструкции.

Добавленные типы контента отобразятся в блоке **Типы контента** для выбранной группы.

Настройка библиотеки календарей

В библиотеке **Календари** вы можете добавлять статические группы календарей (хранятся в UserGate MC) [и обновляемые группы календарей](#) (загружаются с внешнего сервера). Это может понадобиться, например, если для нескольких правил межсетевого экрана необходимо использовать одно и то же расписание.

Чтобы добавить статическую группу календарей:

1. В разделе **Конечные устройства** (для версий ниже 7.6.0 раздел **Конечные устройства-конфигурация**) для объекта **Шаблон** в выпадающем списке выберите шаблон, параметры которого необходимо настроить.

2. Выберите раздел **Библиотеки → Календари**.

3. В блоке **Группы** нажмите **Добавить**.

4. На вкладке **Общие** укажите название и при необходимости описание группы календарей. 5. Нажмите **Сохранить**.

6. Выберите добавленную группу календарей.

7. В блоке **Элементы** нажмите **Добавить**.

8. Укажите параметры календаря:

- название;
- тип повторения (ежедневно, еженедельно, ежемесячно, единократно, повтор событий, диапазон времени);
- расписание повторения (набор параметров зависит от выбранного типа повторения).

9. Нажмите **Сохранить**.

10. Для добавления других календарей повторите шаги 7-9 инструкции.

Добавленные календари отобразятся в блоке **Элементы** для выбранной группы.

Настройка обновляемых списков (групп) элементов

Списки и группы некоторых элементов могут автоматически пополняться из файлов, размещенных на внешнем сервере. Вы можете настраивать такие списки (группы) для IP-адресов, приложений, URL-адресов, URL-категорий, типов контента и календарей. Для этого необходимо подготовить файл со списком элементов (создать его и разместить на внешнем сервере), а затем добавить обновляемый список (группу) в соответствующей библиотеке шаблона.

Чтобы подготовить файл со списком элементов:

1. Создайте текстовый файл (например, `list.txt`) и добавьте в него список элементов.

Примечание Элементы должны быть записаны в столбик без знаков препинания.

2. Поместите файл в архив (например, `list.txt` в `list.zip`).

3. Создайте текстовый файл (например, `version.txt`) и укажите в нем номер версии списка (например, 3).

Примечание Значение номера версии необходимо инкрементировать при каждом обновлении списка.

4. Разместите архив со списком элементов и файл с номером версии списка (например, `list.zip` и `version.txt`) на внешнем сервере, чтобы они были доступны для скачивания.

Чтобы добавить обновляемый список (группу) элементов:

1. В разделе **Конечные устройства** (для версий ниже 7.6.0 раздел **Конечные устройства-конфигурация**) для объекта **Шаблон** в выпадающем списке выберите шаблон, параметры которого необходимо настроить.

2. В разделе **Библиотеки** выберите нужную библиотеку: **IP-адреса**, **Группы приложений**, **Списки URL**, **Категории URL**, **Типы контента** или **Календари**.

3. В блоке слева нажмите **Добавить**.

4. На вкладке **Общие** укажите название и при необходимости описание списка (группы).

Примечание Для некоторых элементов доступны дополнительные параметры (например, уровень угрозы).

5. На вкладке **Автоматическое обновление** установите флажок **Включено** и укажите следующие параметры:

- URL-адрес внешнего сервера для получения обновлений в формате `http://<IP-адрес или доменное имя сервера>` или `ftp://<IP-адрес или доменное имя сервера>`.
- Расписание получения обновлений от внешнего сервера.

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

При ручном вводе также можно использовать следующие символы:

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

6. Нажмите **Сохранить**.

Создание группы шаблонов конечных устройств

Version: 7.x

Product: UGMC

Documentation: 

После создания шаблонов конечных устройств эти шаблоны необходимо объединить в группы. Группа шаблонов позволяет создать конфигурацию параметров, которая будет применена к одному или нескольким управляемым устройствам. Эта конфигурация формируется в результате слияния параметров всех шаблонов, входящих в группу, с учетом их расположения.

Чтобы создать группу шаблонов конечных устройств:

1. В разделе **Управление областью → Конечные устройства → Группы шаблонов** нажмите **Добавить**.
2. На вкладке **Общие** укажите название и при необходимости описание группы шаблонов.
3. На вкладке **Шаблоны** нажмите **Добавить**:
 - выберите шаблон в списке и добавьте его в группу по кнопке **Добавить**;
 - повторите действие для всех шаблонов, которые требуется добавить в группу;
 - нажмите **Закрыть**.

Порядок расположения шаблонов в списке соответствует порядку применения параметров шаблонов в конфигурации. При необходимости вы можете изменять порядок с помощью кнопок **Наверх**, **Выше**, **Ниже**, **Вниз**.

Вы также можете создавать и добавлять новые шаблоны по ссылке **Создать и добавить новый объект**.

4. Нажмите **Сохранить**.

Созданная группа шаблонов отобразится в таблице **Группы шаблонов**. Теперь вы можете перейти к настройке интеграции конечных устройств с UserGate MC.

Настройка интеграции конечных устройств с UserGate MC

Version: 7.x

Product: UGMC

Documentation: 

Для настройки интеграции в управляемой области создается логическое устройство с уникальным кодом. С помощью этого кода сервер UserGate MC идентифицирует подключаемое конечное устройство, привязывает его к логическому устройству и применяет конфигурацию параметров выбранной группы шаблонов.

Конечные устройства, для которых настроена интеграция с UserGate MC, называются управляемыми устройствами. Каждое включенное логическое устройство с активной лицензией использует [одну лицензию на управляемое устройство](#).

Одно логическое устройство позволяет настроить интеграцию с UserGate MC [одиночного конечного устройства](#). Если требуется подключить [группу конечных устройств](#) и распространить на них одинаковую конфигурацию параметров, вы можете создать общий код подключения. При использовании этого кода для каждого конечного устройства в UserGate MC автоматически создается логическое устройство и применяется одна и та же группа шаблонов. Это может потребоваться, например, для устройств, входящих в домен Microsoft Active Directory (далее также — домен AD).

Данные между конечным устройством и UserGate MC передаются по защищенному каналу (порт TCP 4045). Для его создания при первом подключении устройство обменивается с сервером UserGate MC ключами шифрования (порт TCP 9712).

Перед подключением конечного устройства администратору центра управления UserGate MC необходимо:

- Проверить наличие сетевой связности между серверами UserGate MC и конечного устройства (подробнее — в разделе «[Требования к сетевому окружению](#)»).
- Настроить сетевую зону для подключения конечных устройств и назначить ее интерфейсу. В свойствах этой зоны должен быть разрешен доступ к сервису **Контроль конечных устройств** (подробнее о настройке зон и интерфейсов — в разделе «[Настройка сети](#)»).

Вы можете [просматривать информацию о подключении конечного устройства](#) в веб-консоли UserGate MC в разделе **Управление областью → Конечные устройства → Устройства**. Для каждого устройства в управляемой области (логического устройства) отображаются статус и дата последнего подключения привязанного к нему конечного устройства, а также дополнительная информация, включая объем используемой памяти и время непрерывной работы.

Настройка интеграции одиночного конечного устройства

Для настройки интеграции одиночного конечного устройства с UserGate MC необходимо:

- 1) создать устройство в управляемой области;
- 2) подключить конечное устройство к UserGate MC.

Создание устройства в управляемой области

Примечание Инструкция ниже выполняется администратором управляемой области в веб-консоли UserGate MC.

Чтобы создать устройство в управляемой области:

1. В разделе **Управление областью → Конечные устройства → Устройства** нажмите **Добавить**.
2. В открывшемся окне проверьте, что устройство включено и использует лицензию (флажки **Включено** и **Лицензирован** соответственно).
3. Укажите название и при необходимости описание устройства.
4. Укажите группу шаблонов, параметры которой должны применяться к подключенному конечному устройству.
5. Укажите режим синхронизации параметров между группой шаблонов и подключенным конечным устройством.
4. Нажмите **Сохранить**.
5. Выберите созданное устройство в списке и получите код подключения конечного устройства по кнопке **Показать уникальный код устройства**.
6. Сохраните код подключения конечного устройства.

В интерфейсе UserGate MC вы можете [просматривать список созданных устройств](#).

Подключение конечного устройства к UserGate MC

Примечание Инструкция ниже выполняется в интерфейсе конечного устройства.

Чтобы подключить конечное устройство к UserGate MC:

1. Запустите установочный файл UserGate Client на конечном устройстве.

Подробнее — в разделе «[Установка UserGate Client](#)» Руководства администратора UserGate Client.

2. В окне мастера настройки UserGate Client укажите доменное имя или IP-адрес UserGate MC (например, 192.0.2.4) и код подключения конечного устройства, [сгенерированный в веб-консоли UserGate MC](#).

3. Нажмите **Register**.

Подключение займет некоторое время. По окончании отобразится окно с подтверждением.

При успешном подключении конфигурация параметров группы шаблонов будет применена к конечному устройству.

Настройка интеграции группы конечных устройств

Для настройки интеграции группы конечных устройств с UserGate MC необходимо:

- 1) создать код подключения конечных устройств;
- 2) подключить конечные устройства к UserGate MC.

Создание кода подключения конечных устройств

Примечание Инструкция ниже выполняется администратором управляемой области в веб-консоли UserGate MC.

Чтобы создать код подключения конечных устройств:

1. В разделе **Управление областью → Конечные устройства → Коды для конечных устройств** нажмите **Добавить**.
2. В открывшемся окне проверьте, что код активирован (флажок **Включено**).
3. Укажите название и при необходимости описание кода.
4. Укажите группу шаблонов, параметры которой должны применяться к подключенным с использованием кода устройствам.
5. Укажите режим синхронизации параметров между группой шаблонов и подключенными устройствами.

В процессе синхронизации к управляемым устройствам применяется конфигурация параметров группы шаблонов. По умолчанию указан автоматический режим. В этом режиме параметры конечных устройств синхронизируются с конфигурацией параметров при каждом ее изменении.

При необходимости синхронизацию можно отключить. Это может понадобиться, например, если нужно одновременно изменить параметры нескольких шаблонов группы. В этом случае вы можете применить сразу все внесенные изменения в таблице **Устройства**, выполнив синхронизацию вручную по кнопке **Синхронизировать сейчас**.

4. Нажмите **Сохранить**.
5. Выберите созданный код в списке и нажмите **Уникальный код конечного устройства**.
6. Сохраните код подключения конечных устройств.

Подключение конечных устройств к UserGate MC

Если конечные устройства не входят в домен AD, подключение к UserGate MC выполняется [локально на каждом устройстве](#).

Если конечные устройства находятся в домене AD, подключение к UserGate MC выполняется централизованно для всех конечных устройств домена [с помощью редактора групповых политик](#).

Примечание Инструкция ниже выполняется в интерфейсе конечного устройства.

Чтобы подключить конечное устройство к UserGate MC:

1. Запустите установочный файл UserGate Client на конечном устройстве.

Подробнее — в разделе «[Установка UserGate Client](#)» Руководства администратора UserGate Client.

2. В окне мастера настройки UserGate Client укажите IP-адрес или доменное имя UserGate MC (например, 192.0.2.4), а также код подключения конечных устройств, [сгенерированный в веб-консоли UserGate MC](#).

3. Нажмите **Register**.

Подключение займет некоторое время. По окончании отобразится окно с подтверждением.

При успешном подключении конфигурация параметров группы шаблонов будет применена к конечному устройству.

Для подключения конечных устройств через групповые политики:

1. Скачайте файл [UserGateClient.adm](#).
2. В этом файле в полях ServerIP и DeviceCode соответственно укажите IP-адрес или доменное имя UserGate MC, а также код подключения конечных устройств.

Например:

```
ServerIP="MC server IP: 192.0.2.4"
DeviceCode="DeviceCode: a4mqwmcr"
```

3. На контроллере домена добавьте в групповую политику конечных устройств установочный файл UserGate Client и измененный файл UserGateClient.adm.
4. Примените групповую политику.

Установка UserGate Client, подключение к UserGate MC и применение конфигурации параметров будут выполнены автоматически при обновлении групповых политик на конечных устройствах или при перезагрузке этих устройств.

Version: 7.x
Product: UGMC
Documentation: 

Раздел **Управление областью → Конечные устройства → Устройства** содержит список устройств в управляемой области. В этом списке вы можете:

- Включать и отключать устройства по кнопкам **Включить** и **Отключить** соответственно. При отключении будет разорвано соединение привязанного конечного устройства с сервером UserGate MC.
- Удалять устройства по кнопке **Удалить**.
- [Просматривать параметры устройства](#).
- Изменять параметры устройства по кнопке **Редактировать**.
- Включать и отключать передачу данных привязанного конечного устройства по кнопкам **Блокировать** и **Разблокировать** соответственно.
- Переподключать конечное устройство по кнопке **Переподключить устройство**. В результате будет сгенерирован новый код для подключения к UserGate MC. Это может понадобиться, например, при переустановке UserGate Client на конечном устройстве.
- [Просматривать подробную информацию о привязанном конечном устройстве](#) по ссылке **Информация о конечном устройстве** в строке устройства в колонке **Мониторинг**.

Кроме того, вы можете настраивать отображение устройств в списке с помощью следующих фильтров:

- **Все** — все устройства (фильтр по умолчанию).
- **Включенные** и **Выключенные** — устройства в выбранном состоянии.
- **Онлайн** — для привязанных конечных устройств установлено соединение с сервером UserGate MC.
- **Офлайн** — для привязанных конечных устройств не установлено соединение с сервером UserGate MC.
- **Не привязанные** — устройства, к которым не привязаны конечные устройства.
- **Консистентные устройства** — устройства, к которым привязаны конечные устройства с параметрами, синхронизированными с конфигурацией параметров группы шаблонов.
- **Неконсистентные устройства** — устройства, к которым привязаны конечные устройства с параметрами, не синхронизированными с конфигурацией параметров группы шаблонов.
- **Подходящие под HIP-профиль устройства** — устройства, к которым привязаны конечные устройства, соответствующие [требованиям проверки безопасности](#).
- **Не подходящие под HIP-профиль устройства** — устройства, к которым привязаны конечные устройства, не соответствующие [требованиям проверки безопасности](#).

Вы также можете управлять синхронизацией параметров между группой шаблонов и конечными устройствами. В процессе синхронизации к управляемому устройству применяется конфигурация параметров группы шаблонов.

Доступны ручной и автоматический режимы синхронизации. Вручную вы можете запускать синхронизацию сразу для всех управляемых устройств (по кнопке **Действия → Запустить полную синхронизацию**) или только для выбранных (по кнопке **Запросить синхронизацию**).

В автоматическом режиме параметры управляемого устройства синхронизируются с конфигурацией параметров группы шаблонов при каждом ее изменении. Кроме того, при автоматической синхронизации подключенное конечное устройство отправляет UserGate MC сведения о своем состоянии каждые 20 секунд, в результате чего обновляется время последней успешной синхронизации для устройства.

При необходимости синхронизацию можно отключить. Это может понадобиться, например, если нужно одновременно изменить параметры нескольких шаблонов группы. В этом случае вы можете применить сразу все внесенные изменения в таблице **Устройства**, выполнив синхронизацию вручную по кнопке **Синхронизировать сейчас**.

Просмотр параметров устройства

Для каждого устройства в списке отображаются следующие параметры.

Параметр	Описание
Название	Название устройства
Версия ОС	Версия ОС Windows, установленной на конечном устройстве
Версия	Версия UserGate Client, установленного на конечном устройстве

Параметр	Описание
Последнее подключение	Дата и время последнего подключения конечного устройства
Телеметрия	Информация о конечном устройстве. Например, IP-адрес, NetBIOS-имя, время последнего подключения к UserGate MC и имя пользователя, выполнившего вход в систему
Мониторинг	Статус синхронизации параметров между конечным устройством и примененной группой шаблонов. При возникновении ошибки синхронизации доступен просмотр отчета по кнопке Показать отчет. Примечание Ошибка синхронизации не влияет на работу правил межсетевого экрана: конечное устройство использует последнюю успешно примененную конфигурацию. Также остается доступным управление сервисами, процессами и запросами в реестр Windows. Доступен просмотр подробной информации о конечном устройстве по ссылке Информация о конечном устройстве
Группы шаблонов	Примененная группа шаблонов
NIP-профили	NIP-профили, которые используются в правилах межсетевого экрана. Соответствие конечного устройства профилю обозначается цветовым индикатором: - Зеленый — устройство соответствует профилю. - Красный — устройство не соответствует профилю. При этом доступен просмотр отчета по кнопке Посмотреть отчет. В отчете отображаются время последнего получения данных, название NIP-профиля и NIP-объектов, тип NIP-объекта и критерий, по которому выявлено несоответствие
Устройства LogAn/SIEM	При подключенном внешнем сервере журналирования отображается его название
Время последней синхронизации	Режим синхронизации, а также время и дата последней успешной синхронизации
Дата лицензирования	Статус активации лицензии на управляемое устройство (флажок Лицензирован в свойствах устройства), а также время и дата последней активации лицензии

Просмотр подробной информации о конечном устройстве

В разделе **Управление областью → Конечные устройства → Устройства** вы можете просматривать подробную информацию о конечных устройствах. Для этого в строке выбранного устройства в колонке **Мониторинг** нажмите **Информация о конечном устройстве**. Откроется окно со следующими вкладками.

Вкладка	Описание
Общие	Сведения о конечном устройстве (имя компьютера, версия и тип ОС, версия UserGate Client, IP-адрес, время загрузки системы и текущее время на устройстве) и о пользователе, выполнившем вход в систему (фотография, имя, статус, тип учетной записи — локальная или доменная, телефон, электронная почта)
Производительность	В виде графика и таблиц отображаются следующие показатели производительности конечного устройства: - загрузка центрального процессора; - загрузка процессора процессом UserGate Client; - использование виртуальной памяти; - использование оперативной памяти; - объем памяти, используемый UserGate Client; - информация о дисках (размер, тип, производительность)
Безопасность	Информация о состоянии межсетевого экрана, антивируса, центра обеспечения безопасности Windows, а также о шифровании дисков (BitLocker)
USB-устройства	Список подключенных USB-устройств

Вкладка	Описание
Элементы автозагрузки	Список приложений, для которых настроен автоматический запуск при входе в систему
Процессы	Список запущенных процессов. Вы можете принудительно завершить процесс по кнопке Завершить процесс
Службы	Список служб конечного устройства и их состояний. Вы можете запустить или остановить службу с помощью кнопок Запустить службу и Остановить службу соответственно
Ключи реестра	Разделы реестра Windows HKEY_LOCAL_MACHINE и HKEY_USERS. При выборе ключа реестра отображаются его название, тип и значение
Программное обеспечение	Список установленных программ
Установленные обновления	Список установленных обновлений
Точки восстановления	Список доступных точек восстановления системы

Кроме того, на каждой вкладке отображаются дата и время получения данных, а также статус подключения конечного устройства:

- **Онлайн** — соединение между конечным устройством и сервером UserGate MC установлено, данные передаются;
- **Офлайн** — соединение между конечным устройством и сервером UserGate MC не установлено, данные не передаются;
- **Отключен** — соединение между конечным устройством и сервером UserGate MC разорвано (по кнопке **Отключить** для устройства в управляемой области), данные не передаются.

Настройка проверки требований безопасности (HIP)

Documentation: 

Version: 7.x

Product: UGMC

Примечание Для использования возможностей, описанных в этом разделе, необходима лицензия на модуль NAC. Подробнее — в разделе «[Лицензирование UserGate MC](#)».

Проверка конечных устройств на соответствие требованиям безопасности (комплаенсу) выполняется с помощью технологии Host Information Profile (HIP). Для этого создаются HIP-объекты и HIP-профили.

HIP-объект содержит критерии, которым должно соответствовать конечное устройство (например, версия ОС, состояние антивируса, наличие обновлений). Критерии внутри HIP-объекта объединяются по условию «И» — устройство должно удовлетворять каждому из них. Из нескольких HIP-объектов формируется HIP-профиль.

HIP-профили используются в правилах межсетевого экрана и позволяют управлять сетевым доступом конечного устройства. Так, например, можно разрешить доступ к сетевой зоне или приложению только устройствам с включенным межсетевым экраном и актуальными обновлениями.

Для настройки проверки требований безопасности необходимо:

- 1) создать HIP-объекты;
- 2) создать HIP-профиль, добавив в него HIP-объекты и выбрав условие проверки объектов в профиле;
- 3) указать HIP-профили [в правилах межсетевого экрана](#).

Начиная с версии 7.6.0 создание HIP-объектов и HIP-профилей выполняется в разделе **Управление областью → Общая библиотека**. Подробнее — в разделе «[Общая библиотека](#)».

Создание HIP-объекта

Примечание Для проверки некоторых критериев требуется [лицензия на модуль Security Updates](#). Модуль необходим для скачивания обновлений библиотек, используемых при проверке комплаенса.

Чтобы создать HIP-объект:

1. В разделе **Управление областью → Конечные устройства → HIP-объекты** нажмите **Добавить**.
2. На вкладке **Общие** выполните следующее:
 - Укажите название и при необходимости описание HIP-объекта.
 - Укажите версию Windows конечного устройства.
При выборе значения ANY версия ОС может быть любой. Для указания конкретной версии доступны операторы: = (версия совпадает с указанной) и != (версия не совпадает с указанной).
 - Укажите версию UserGate Client конечного устройства.
При выборе значения ANY версия UserGate Client может быть любой. Для указания конкретной версии доступны операторы сравнения (=, !=, <, >, <=, >=), а также операторы соответствия маске (~ и !~).
3. На вкладке **Безопасность** укажите состояние межсетевого экрана, антивируса, а также функций автоматического обновления (AutoUpdate) и шифрования дисков (BitLocker) на конечном устройстве:
 - **Не проверять** — состояние не учитывается;
 - **Нет** — компонент отключен;
 - **Да** — компонент включен.

Важно! При проверке BitLocker считается включенным, если шифрование активно хотя бы на одном из дисков конечного устройства.

4. На вкладке **Продукты** добавьте типы программного обеспечения конечного устройства:
 - **Антивирус** — для антивирусного ПО укажите статус установки, состояние и актуальность антивирусных баз, а также выберите необходимые продукты из списка по кнопке **Добавить**.
 - **Межсетевой экран** — для межсетевых экранов укажите статус установки, состояние и версию, а также выберите необходимые продукты из списка по кнопке **Добавить**.
 - **Резервное копирование** — для ПО резервного копирования укажите статус установки и версию, а также выберите необходимые продукты из списка по кнопке **Добавить**.
 - **Шифрование диска** — для ПО шифрования диска укажите статус установки и версию, а также выберите необходимые продукты из списка по кнопке **Добавить**.
 - **DLP** — для ПО предотвращения утечек информации укажите статус установки и версию, а также выберите необходимые продукты из списка по кнопке **Добавить**.
 - **Управление обновлениями** — для ПО управления обновлениями укажите статус установки и версию, а также выберите необходимые продукты из списка по кнопке **Добавить**.
5. На вкладке **Процессы** добавьте процессы конечного устройства.

Список запущенных на конечном устройстве процессов доступен [при просмотре подробной информации о конечном устройстве](#).

6. На вкладке **Запущенные службы** добавьте службы конечного устройства.

Список запущенных на конечном устройстве служб доступен [при просмотре подробной информации о конечном устройстве](#).

7. На вкладке **Ключи реестра** добавьте ключи реестра Windows конечного устройства.

Список ключей реестра конечного устройства доступен [при просмотре подробной информации о конечном устройстве](#).

Примечание Вы можете добавлять ключи из разделов HKEY_LOCAL_MACHINE и HKEY_USERS.

При добавлении ключа реестра выполните следующее:

- Укажите полный путь к ключу. Путь должен начинаться с символа \ (например, \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run).
- Укажите название параметра внутри ключа. Название не должно содержать символ \. Например, для пути \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run названием параметра может быть SecurityHealth.
- Выберите тип данных (**REG_SZ** — строковый, **REG_BINARY** — двоичный, **REG_DWORD** — 32-разрядное целое число), оператор сравнения и значение параметра.

Подробнее о разделах реестра Windows — [в документации Microsoft](#).

8. На вкладке **Установленные обновления** настройте проверку наличия обновлений Microsoft на конечном устройстве:

- выберите условие проверки: **Все** (все указанные обновления) или **Любой** (хотя бы одно из указанных обновлений);
- выберите режим проверки: **MATCH** (обновления установлены) или **NOT MATCH** (обновления не установлены);
- нажмите **Добавить** и укажите номер статьи базы знаний Microsoft (KB) (например, KB5013624).

9. Нажмите **Сохранить**.

Создание HIP-профиля

Чтобы создать HIP-профиль:

1. В разделе **Управление областью → Конечные устройства → HIP-профили** нажмите **Добавить**.
2. На вкладке **Общие** укажите название и при необходимости описание профиля.
3. На вкладке **HIP-объекты** нажмите **Добавить**.
4. Выберите HIP-объект в списке по кнопке **Добавить**.

При добавлении второго и последующих HIP-объектов вы можете выбрать условие применения каждого объекта в HIP-профиле:

- **И** — устройство должно соответствовать этому объекту и всем остальным;
- **ИЛИ** — устройство должно соответствовать этому объекту или любому другому;
- **И НЕ** — устройство должно соответствовать всем объектам, кроме этого;
- **ИЛИ НЕ** — устройство должно соответствовать любому объекту, кроме этого.

Вы также можете создавать и добавлять новые HIP-объекты по ссылке **Создать и добавить новый объект**.

5. Нажмите **Сохранить**.

Созданный HIP-профиль отобразится в таблице **HIP-профили**. Теперь вы можете использовать его в правилах межсетевого экрана.

Version: 7.x
Product: UGMC
Documentation:

UserGate Management Center (UGMC) получает от подключенных конечных устройств информацию о событиях, например, данные о действиях пользователей, изменениях параметров устройств, а также о работе приложений, установленных на устройствах. Эта информация используется для анализа состояния конечных устройств и контроля их доступа к корпоративной сети.

В веб-интерфейсе UGMC [администраторы управляемой области](#) могут настраивать отправку данных конечных устройств в другие продукты экосистемы UserGate SUMMA, такие как UserGate Log Analyzer и UserGate SIEM (начиная с версии 7.5.0). Данные будут передаваться в выбранный продукт транзитом через UGMC и записываться в виде журналов для хранения и дальнейшего анализа. Подробная информация о UserGate Log Analyzer и UserGate SIEM, а также инструкции по настройке и работе с ними приведены в Руководстве администратора Log Analyzer и Руководстве администратора UserGate SIEM соответственно.

Настройка отправки данных конечных устройств

В веб-интерфейсе управляемой области UGMC вы можете настроить отправку данных конечных устройств в UserGate Log Analyzer или UserGate SIEM, используя [шаблоны устройств](#).

ПримечаниеПеред выполнением инструкции вам необходимо подключить UserGate Log Analyzer или UserGate SIEM к UGMC, см. разделы «[Управление устройствами LogAn](#)» и «[Управление устройствами UserGate SIEM](#)» соответственно. Для каждого подключения на сервере UGMC автоматически назначается порт из диапазона 22000-22711.

Чтобы настроить отправку данных конечных устройств:

1. В разделе **Конечные устройства - конфигурация** выберите шаблон устройства.
2. В разделе боковой панели **UserGate → Настройки** в блоке **Устройство LogAn/SIEM** нажмите ссылку для выбора продукта, в который нужно отправлять данные.
3. В открывшемся окне настройте следующие параметры:
 - установите флажок **Синхронизировать**;
 - в выпадающем списке выберите подключенный UserGate Log Analyzer или UserGate SIEM.
4. Нажмите **Сохранить**.

Просмотр журналов конечных устройств

В веб-интерфейсе UserGate Log Analyzer или UserGate SIEM данные конечных устройств отображаются в разделе **Журналы и отчёты → Журналы → Конечные устройства**. Для просмотра доступны следующие журналы:

- [Журнал событий](#).
- [Журнал правил](#).
- [Приложения](#).
- [Аппаратура](#).

ПримечаниеДля записи журналов на английском языке необходимо установить языковой пакет Английский (США). Кроме того, этот язык должен быть доступен для выбора в качестве языка интерфейса.

При просмотре каждого журнала вы можете:

- просматривать подробную информацию о выбранной записи в отдельном окне (по кнопке **Показать**);
- добавлять выбранные записи к сведениям об инциденте (по кнопке **Добавить в инцидент**);
- скачивать выбранные записи в CSV-файл для дальнейшего анализа (по кнопке **Экспортировать в CSV**).

Журнал событий

Журнал содержит данные о событиях, зарегистрированных на конечных устройствах.

Параметр	Описание
Узел	Идентификатор конечного устройства или узла, на котором запущен сенсор
Время	Время регистрации события. Отображается в часовом поясе, настроенном в продукте
Конечное устройство/сенсор	Названия конечного устройства или сенсора

Параметр	Описание
Уровень лога	Уровень важности зарегистрированного события: • Аудит успеха (Audit Success) — событие при успешном обращении к ресурсу аудита; • Аудит отказа (Audit Failure) — событие при неуспешном обращении к ресурсу аудита; • Ошибка (Error) — событие указывает на существенные проблемы, которые могут стать причиной потери функциональности или данных; • Предупреждение (Warning) — событие указывает на проблемы, которые не требуют немедленного решения, но могут привести к ошибкам в будущем; • Сведения (Information) — информационное событие, которое, как правило, не требует внимания администратора
Данные	Подробная информация о событии
Источник журнала событий	Название источника, зарегистрировавшего событие
Категория журнала	Код категории журнала. Отображаются данные, полученные из журнала событий Windows (Application Event Log). Каждый источник журнала событий может определять собственные категории
Категория инцидента	Название категории, к которой относится инцидент
Имя компьютера	Полное название конечного устройства или узла, на котором запущен сенсор
Имя пользователя	Пользователь, с учетной записи которого был выполнен вход в систему конечного устройства
Код события лога	Код события
Идентификатор события лога	Идентификатор события
Тип события лога	Тип события, которому соответствует уровень события: • 1 — ошибка (error); • 2 — предупреждение (warning); • 3 — сведения (information); • 4 — аудит успеха (audit success); • 5 — аудит отказа (audit failure)
Строка вставки	Данные о событии, полученные от элемента eventData журнала события Windows
Файл журнала лога	Тип журнала, к которому относится событие: • Application (журнал приложений) — содержит события приложений и служб; • Security (журнал безопасности) — содержит события системы аудита; • System (системный журнал) — содержит события драйверов устройств; • CustomLog — содержит события, зарегистрированные приложениями, которые ведут запись в пользовательский журнал

Журнал правил

Журнал содержит информацию о срабатываниях [правил межсетевого экрана](#) конечных устройств, в которых включен параметр **Журналирование**.

Параметр	Описание

Параметр	Описание
Узел	Идентификатор конечного устройства
Время	Время срабатывания правила. Отображается в часовом поясе, настроенном в продукте
Конечное устройство	Название конечного устройства
Действие	Действие для конечного устройства, которое выполняется при срабатывании правила: • Разрешить; • NAT; • Запретить
Правило	Название правила межсетевого экрана
Приложение	Приложение, через которое осуществляется доступ к ресурсу
Домен	Имя домена, используемое для подключения
Категория сайтов	Категория сайтов, к которой относится адрес назначения. Отображается только при наличии правил с условием «Категории сайтов»
Тип контента	Название типа контента
Сетевой протокол	Транспортный протокол, используемый для подключения к ресурсу
IP источника	IP-адрес источника трафика
Порт источника	Номер порта, через который осуществляется подключение
IP назначения	IP-адрес назначения трафика
Порт назначения	Номер порта назначения, используемый транспортным протоколом

Журнал приложений

Журнал содержит информацию о приложениях, которые запускались на конечных устройствах.

Параметр	Описание
Узел	Идентификатор конечного устройства
Время	Время запуска приложения на конечном устройстве. Отображается в часовом поясе, настроенном в продукте
Конечное устройство	Название конечного устройства
Действие	Запуск или остановка приложения
Хэш	Хеш-сумма приложения
Приложение	Название приложения, которое было запущено или остановлено
Версия	Версия приложения

Параметр	Описание
Субъект подписи	Владелец сертификата для приложения
Подписано	Издатель сертификата для приложения
Идентификатор процесса	Идентификатор процесса для приложения
Пользователь	Пользователь, запустивший приложение
Командная строка	Команда запуска приложения

Журнал устройств

Журнал содержит информацию об устройствах, которые подключались к конечным устройствам.

Параметр	Описание
Узел	Идентификатор конечного устройства
Время	Дата и время регистрации события
Конечное устройство	Название конечного устройства
Действие	Добавление или удаление устройства
Устройство	Название устройства, которое было подключено или удалено
Идентификатор устройства	Идентификатор подключенного или удаленного устройства
Служба	Драйверы, использующиеся для работы с устройством

