

Table of Contents

Table of Contents	1
Управление конечными устройствами	2
Управление конечными устройствами UserGate Client (Описание)	3
Установка ПО UserGate Client	4
Шаблоны управляемых устройств UGC	6
Группы шаблонов управляемых устройств UGC	17
Добавление управляемых устройств UGC под управление UGMC	18
Управление устройством UGC из консоли UGMC	20
Сбор и анализ данных с устройств UGC	23
NIP профили	28
Объекты NIP	29

Documentation: 

Version: 7.0.1

Product: UGMC

Конечное управляемое устройство — это пользовательский компьютер под управлением операционной системы Windows с установленным ПО UserGate Client (UGC). ПО UserGate Client является компонентом экосистемы UserGate SUMMA, которое позволяет администратору централизованно управлять парком управляемых устройств UGC и получать с них информацию о состоянии устройств, например, такую как, загрузка процессора, критические события, произошедшие на устройстве, журналы различных сервисов, журналы и оповещения от антивирусных продуктов и т.п. Объем информации, получаемой с управляемого устройства UGC, будет постоянно расширяться.

С использованием ПО UserGate Client администратор может произвести гибкую настройку политик безопасности с помощью правил межсетевого экрана, позволяющих фильтровать трафик на основе адреса источника/назначения, пользователей, сервисов, списков и категорий URL, приложений, типов контента и соответствия требованиям безопасности, реализованного на основе профилей HIP (подробнее читайте в разделе [HIP профили](#)).

Телеметрическая информация, журналы Windows и другие данные о безопасности конечных устройств передаются в систему анализа событий LogAp и могут быть использованы для автоматического реагирования на угрозы безопасности.

Централизованное управление устройствами UGC можно разделить на следующие этапы:

1. Создание управляемой области. Смотрите раздел [Создание управляемых областей](#).
2. Создание шаблона или нескольких шаблонов, каждый из которых опишет свою часть настроек управляемых устройств UGC. Смотрите раздел [Шаблоны управляемых устройств UGC](#) для более детальной информации.
3. Объединение необходимых шаблонов в группу шаблонов в требуемом порядке, чтобы получить корректную результирующую настройку управляемых устройств UGC. Смотрите раздел [Группы шаблонов управляемых устройств UGC](#) для более детальной информации.
4. Установка ПО UserGate Client на пользовательские компьютеры. Смотрите раздел [Установка ПО UserGate Client](#) для более детальной информации.
5. Добавление управляемого устройства UGC и применение к нему группы шаблонов. Смотрите раздел [Добавление устройств UGC под управление UGMC](#) для более детальной информации.
6. Управление устройством UGC из консоли UGMC. Смотрите раздел [Управление устройством UGC из консоли UGMC](#) для более детальной информации.

Установка ПО UserGate Client

Version: 7.0.1

Product: UGMC

Documentation: ☒

Описание

Программный продукт UserGate Client может быть установлен на компьютеры с версией ОС Windows 7/8/10/11. Для минимальной работоспособности необходимо от 2 Гб оперативной памяти, а также процессор тактовой частотой не ниже 2 ГГц и 200 Мб свободного пространства на жестком диске.

ПО UserGate Client поставляется в виде инсталляционного msi или exe-файла для систем Windows, который может быть установлено как в ручном режиме, так и при помощи средств автоматизации.

Для установки ПО в ручном режиме, запустите установочный файл, подходящий для вашей системы (32 или 64-битной). Во время установки запустится мастер настройки агента, который предложит ввести настройки подключения к UserGate Management Center - IP-адрес UGMC и код конечного устройства, созданный в центре управления.

Установка ПО в автоматическом режиме осуществляется с помощью групповых политик Microsoft Active Directory. Для публикации приложения в Active Directory требуется msi-файл с инсталлятором и административный шаблон [UserGateClient.adm](#), который используется для указания IP-адреса UGMC и кода конечных устройств, созданного в центре управления.

После завершения установки UserGate Client получает конфигурацию, назначенную ему в UGMC, и передает информацию о конечном устройстве в центр управления.

На конечном устройстве доступна следующая информация:

Наименование	Описание
General	Информация о конечном устройстве (пользователь, имя компьютера, IP-адрес для выхода в Интернет, версия ОС Windows) и VPN-подключении (статус подключения, VPN IP-адрес конечного устройства, количество байтов, переданных/полученных с момента подключения по VPN, время подключения). Также доступно сохранение логина пользователя для подключения по VPN после перезагрузки конечного устройства (чекбокс Save login).
Logs	Информация о: • Logging level - уровень детализации диагностики: ◦ Off: отключить ведение журнала диагностики. ◦ Error: журналировать только ошибки. ◦ Warning: журналировать только ошибки и предупреждения. ◦ Info: журналировать только ошибки, предупреждения и дополнительную информацию. ◦ Debug: максимум детализации. Журнал находится: %ALLUSERSPROFILE%\UserGate\UserGate Client\var\log\usergateclient\ug_client.txt. • Tooltips history - история оповещений. • Export logs - скачать журнал диагностики (после скачивания откроется каталог, в который был сохранён файл журнала диагностики).
Network	Просмотр следующей информации: • IPCONFIG - информация о всех сетевых адаптерах и текущей конфигурации TCP/IP. • ROUTING - записи локальной таблицы маршрутизации. • SOCKETS - список активных подключений (тип порта, адреса, состояние соединения, идентификатор процесса). Чтобы скопировать информацию нажмите Copy.
Policy	Просмотр информации о безопасности конечного устройства (статус межсетевого экрана, антивируса, центров обновления и безопасности Windows). Значение индикации: • Жёлтый - выключен. • Зелёный - включен.

Наименование	Описание
Advanced	Управление контентной фильтрацией (возможность самостоятельного отключения контентной фильтрации в соответствии с политиками, настроенными на сервере UserGate Management Center).

Данные для подключения к UserGate Management Center (IP-адрес и код для подключения УУ UGC) указываются:
 %PROGRAMFILES%\UserGate\UserGate Client\usergateclient\bin\endpoint_gui.

Рекомендации по установке ПО UserGate Client

В данном разделе представлены дополнительные настройки конечных устройств, позволяющие повысить информативность и расширить возможности функции аудита событий операционных систем Microsoft Windows.

Примечание Настройки, представленные в данном разделе, носят рекомендательный характер.

1. Установить Sysmon, предоставляющий подробные сведения о создании процессов, сетевых подключениях и изменениях времен создания файлов. Подробная информация и файл установки доступны по [ссылке](#).
2. Добавить раздел для возможности запроса журнала Sysmon (Microsoft-Windows-Sysmon/Operational) и передачи его на сервер UserGate Log Analyzer. Добавление можно произвести с помощью приложения Редактор реестра или выполнением следующей команды:

```
REG ADD "HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Microsoft-Windows-Sysmon\Operational"
```

3. Включить журналирование всех запускаемых PowerShell команд и результатов вывода.

```
REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging" /v EnableScriptBlockLogging /t REG_DWORD /d 1
```

Примечание Для быстрого запуска приложения Редактор реестра используйте сочетание клавиш Win+R и введите regedit.

В случае включения через Редактор реестра необходимо создать переменную **EnableScriptBlockLogging** в каталоге **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging**, указав тип данных **REG_DWORD** и значение **1**.

Примечание Данная настройка возможна в реестрах HKEY_LOCAL_MACHINE и HKEY_CURRENT_USER. Конфигурация HKEY_LOCAL_MACHINE преобладает над конфигурацией HKEY_CURRENT_USER.

Добавить реестр для возможности запроса и передачи журнала PowerShell (Microsoft-Windows-Powershell/Operational) на сервер UserGate Log Analyzer:

```
REG ADD "HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Microsoft-Windows-Powershell\Operational"
```

4. Включить регистрацию дополнительных данных о событиях создания процессов из командной строки в журнал событий безопасности (данные будут добавлены в событие аудита создания процессов «4688: создан процесс»). Для включения используйте приложение Редактор реестра или выполните следующую команду:

```
REG ADD "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system\Audit\" /v ProcessCreationIncludeCmdLine_Enabled /t REG_DWORD /d 1
```

В случае включения через Редактор реестра необходимо создать переменную **ProcessCreationIncludeCmdLine_Enabled** в каталоге **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\Audit**, указав тип данных **REG_DWORD** и значение **1**.

Примечание Данная настройка поддерживается на устройствах с версией ОС не ниже Windows Server 2012 R2 и Windows 8.1.

Version: 7.0.1
Product: UGMC
Documentation: ☒

Шаблон — это базовый блок, с помощью которого можно настроить все параметры работы: сетевые настройки, правила межсетевого экрана, контентной фильтрации. Для создания шаблона необходимо в разделе **Управление конечными устройствами → Шаблоны** нажать на кнопку **Добавить** и дать шаблону имя и опциональное описание.

После создания шаблона можно производить настройку его параметров. Для этого необходимо перейти в раздел верхнего меню **Шаблоны конечных устройств** и в выпадающем меню выбрать необходимый шаблон.

Настройки параметров шаблона отображаются в виде дерева. При настройке параметров следует придерживаться следующих правил:

1. Если значение настройки не определено в шаблоне, то ничего передаваться в управляемое устройство UGC не будет. В данном случае будет использована настройка по умолчанию.
2. Библиотеки, например, такие как IP-адреса, списки URL, списки типов контента MIME, приложения и другие, по умолчанию не содержат никакого контента в UGMC. Для использования библиотек в политиках фильтрации, необходимо предварительно добавить элементы в эти библиотеки.
3. Рекомендуется создавать отдельные шаблоны для разных групп настроек, это позволит избежать конфликтов настроек при объединении шаблонов в группы шаблонов и упростит понимание результирующей настройки, которая будет применена к управляемым устройствам UGC. Например, шаблон правил межсетевого экрана, шаблон правил контентной фильтрации, шаблон библиотек и т.д.

При создании шаблона администратор может использовать следующие разделы — Настройки, Настройки VPN, Политики сети, Библиотеки.

Настройки

Определяют общие настройки параметров управляемых устройств UGC:

Наименование	Описание

Наименование	Описание
Настройки инсталляции UserGate Client	Настройки инсталляции ПО UserGate Client: Собирать информацию о конечном устройстве: сбор информации о конечном устройстве (IP-адрес, время последнего подключения к UGMC, пользователь, имя компьютера, версия ОС, версия ПО UGC, загрузка CPU и памяти, запущенные процессы, сервисы и т.д.). Значение по умолчанию: Да. Если отключить данную функцию, то UGMC будет получать информацию только об IP-адресе, имени конечного устройства, версии ПО UGC и ОС Windows, текущем времени и времени загрузки устройства, загрузке CPU и памяти. Важно! Отключение сбора информации о конечном устройстве влияет на работу профилей HIP. Разрешить сетевой доступ при остановленном приложении: настройка сетевого доступа при остановленном ПО UserGate Client. Значение по умолчанию: Да. Разрешить отключение межсетевого экрана: разрешение пользователю самостоятельно, используя графический интерфейс, отключать контентную фильтрацию на конечном устройстве: Нет — не разрешать самостоятельно отключать контентную фильтрацию. Да — разрешить самостоятельно отключать контентную фильтрацию. Разрешить с использованием кода — разрешить самостоятельно отключать контентную фильтрацию с использованием кода. Для разрешения пользователю самостоятельно отключать контентную фильтрацию необходимо указать/сгенерировать код, который клиент должен ввести на конечном устройстве; также можно указать срок действия кода. При разрешении пользователю отключать фильтрацию самостоятельно можно указать количество разрешённых отключений и/или время, на которое фильтрация будет отключена. Значение по умолчанию: Да (отключение фильтрации на 10 минут без использования кода). Важно! В случае использования счётчика количества отключений: если внести изменения в настройки разрешения отключения межсетевого экрана, то счётчик на конечном устройстве обнулится. Разрешить удалять приложение UserGate Client: возможность удаления ПО UserGate Client. При использовании опции Разрешить с использованием кода необходимо указать/сгенерировать код, который необходимо ввести клиенту при удалении ПО. Значение по умолчанию: Да. Важно! Настройки не будут применены, если не включена синхронизация (флаг <u>Синхронизировать</u>).
Оповещения	Настройка оповещений: Показывать иконку в трее: отображение иконки UserGate Client в области уведомлений на панели задач. Показывать тултипы оповещений: включение/отключение отправки оповещений на конечное устройство. Если оповещения отключены, то уведомления не будут отображаться на конечном устройстве вне зависимости от настроек отдельных уведомлений (о добавлении/удалении устройства из карантина, блокировке ресурса, соответствии/несоответствии HIP профилю). Сообщение о добавлении устройства в карантин: отправка уведомлений о блокировке устройства. Для настройки уведомления необходимо указать текст сообщения и тип. Уведомление будет отображено в виде всплывающего окна. Сообщение об удалении устройства из карантина: отправка уведомлений о разблокировке устройства. Для настройки уведомления необходимо указать текст сообщения и тип. Уведомление будет отображено в виде всплывающего окна. Сообщение о блокировке ресурса: отправка уведомления при блокировке перехода по адресу электронного ресурса. Для настройки уведомления необходимо указать текст сообщения и тип. Уведомление будет отображено в виде всплывающего окна. Сообщение о соответствии HIP профилю: отправка уведомлений в случае соответствия конечного устройства профилю HIP. Уведомление будет отображено в виде всплывающего окна. Сообщение о несоответствии HIP профилю: отправка уведомлений в случае несоответствия конечного устройства профилю HIP. Уведомление будет отображено в виде всплывающего окна. Важно! Настройки не будут применены, если не включена синхронизация (флаг <u>Синхронизировать</u>).

Наименование	Описание
Настройки устройства LogAn	Установка для конечного устройства сервера LogAn, на которое устройство будет отсылать информацию о событиях. Сервер LogAn должен быть предварительно зарегистрирован в UGMC. Важно! Настройки не будут применены, если не включена синхронизация (флаг <u>Синхронизировать</u>).

Настройка VPN

Данный раздел позволяет настроить профили безопасности VPN, которые определяют такие настройки, как общий ключ шифрования (Pre-shared key) и алгоритмы для шифрования и аутентификации. Настройки передаются на управляемое устройство UserGate Client; пользователь сможет выбрать необходимый VPN-сервер для подключения.

Примечание После разрыва соединения попытки подключения будут производиться в течение 40 секунд. Если за это время соединение не будет установлено, то у пользователя отобразится окно для выбора VPN-сервера.

Настройка VPN-соединений возможна только для конечных устройств с версией ОС Windows 10 и выше.

Для настройки VPN необходимо указать:

Наименование	Описание
Включено	Включение/отключение правила.
Название	Название профиля безопасности.
Описание	Описание профиля.
VPN-адрес	Имя хоста (FQDN) или IP-адрес VPN сервера. Важно! При использовании FQDN в качестве адреса VPN-сервера, не предусматривается возможность перебора IP-адресов. В случае, если DNS-сервер вернет несколько адресов, будет выполнена попытка подключения к первому адресу в списке.
Протокол	VPN-протоколы для создания туннеля. IPsec L2TP. Для создания туннелей используется протокол Layer 2 Tunnelling Protocol (L2TP), а для защиты передаваемых данных — протокол IPsec.
Режим IKE	Режим IKE: Основной или Агрессивный. Разница между режимами: в агрессивном режиме используется меньшее количество пакетов, что позволяет достичь более быстрого установления соединения. Агрессивный режим не передает некоторые параметры согласования, что требует предварительной идентичной настройки их на точках подключения. Основной режим. В основном режиме происходит обмен шестью сообщениями. Во время первого обмена (сообщения 1 и 2) происходит согласование алгоритмов шифрования и аутентификации. Второй обмен (сообщения 3 и 4) предназначен для обмена ключами Диффи-Хеллмана (DH). После второго обмена служба IKE на каждом из устройств создаёт основной ключ, который будет использоваться для защиты проверки подлинности. Третий обмен (сообщения 5 и 6) предусматривает аутентификацию инициатора соединения и получателя (проверка подлинности); информация защищена алгоритмом шифрования, установленным ранее. Агрессивный режим. В агрессивном режиме происходит 2 обмена, всего 3 сообщения. В первом сообщении инициатор передаёт информацию, соответствующую сообщениям 1 и 3 основного режима, т.е. информацию об алгоритмах шифрования и аутентификации и ключ DH. Второе сообщение предназначено для передачи получателем информации, соответствующей сообщениям 2 и 4 основного режима, а также аутентификации получателя. Третье сообщение аутентифицирует инициатора и подтверждает обмен.
Аутентификация с пиром	Общий ключ — аутентификация устройств с использованием общего ключа (Pre-shared key).
Общий ключ	Строка, которая должна совпадать на сервере и клиенте для успешного подключения.
Вставить	Место вставки создаваемого правила в списке правил — наверх, вниз или выше выбранного существующего правила.

Наименование	Описание
Фаза 1	Во время первой фазы происходит согласование защиты IKE. Аутентификация происходит на основе общего ключа в режиме, выбранном ранее. Необходимо указать следующие параметры: • Время жизни ключа. По истечению данного времени происходят повторные аутентификация и согласование настроек первой фазы. • Diffie-Hellman группы: выбор группы Диффи-Хеллмана, которая будет использоваться для обмена ключами. Сам ключ не передаётся, а передаются общие сведения, необходимые алгоритму определения ключа DH для создания общего секретного ключа. Чем больше номер группы Диффи-Хеллмана, тем больше бит используется для обеспечения надёжности ключа. • Алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетаскивайте необходимую пару вверх/вниз или используйте кнопки Выше/Низе.
Фаза 2	Во второй фазе осуществляется выбор способа защиты IPsec подключения. Необходимо указать: • Время жизни ключа. По истечению данного времени узлы должны сменить ключ шифрования. Время жизни, заданное во второй фазе, меньше, чем у первой фазы, т.к. ключ необходимо менять чаще. • Максимальный размер данных, шифруемых одним ключом. Время жизни ключа может быть задано в байтах. Если заданы оба значения (Время жизни ключа и Максимальный размер данных, шифруемых одним ключом), то счётчик, первый достигнувший лимита, запустит пересоздание ключей сессии. • Алгоритмы аутентификации и шифрования. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетаскивайте необходимую пару вверх/вниз или используйте кнопки Выше/Низе.

Политики сети

Данный раздел содержит настройки политик фильтрации, таких как политика межсетевого экранирования и контентной фильтрации.

С помощью правил межсетевого экрана администратор может разрешить или запретить любой тип сетевого трафика проходящий или исходящий с управляемого устройства UGC. В качестве условий правила могут выступать IP-адреса источника/назначения, пользователи и группы пользователей, сервисы, приложения, списки и категории URL, типы контента, профили HIP и время.

Правила, создаваемые в шаблонах, могут быть созданы как пре-правила или пост-правила. Пре-правила всегда помещаются выше в списке правил, и следовательно, имеют более высокий приоритет относительно пост-правил. Пост-правила всегда помещаются ниже относительно пре-правил и имеют более низкий приоритет. Наличие возможности создавать пре- и пост-правила дает администратору области создавать гибкие настройки политики безопасности.

ПримечаниеПравила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки Наверх/Вниз, Выше/Низе или перетаскивание мышью для изменения порядка применения правил.

ПримечаниеЧекбокс Инвертировать меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

ПримечаниеЕсли не создано ни одного правила, то любой трафик с/на управляемом устройстве UGC разрешен.

Чтобы создать правило межсетевого экрана, необходимо нажать на кнопку **Добавить** в разделе **Политики сети → Межсетевой экран**, выбрать местоположение правила — пре или пост и указать необходимые параметры.

Наименование	Описание
Включено	Включает или отключает правило
Название	Название правила
Описание	Описание правила
Область применения	Указывает область применения данного правила на управляемом устройстве UGC. Возможны следующие варианты: • Внутри периметра — правило будет применено, если компьютер с установленным ПО UGC находится в доменной сети. • Снаружи периметра — правило будет применено, если компьютер с установленным ПО UGC находится не в доменной сети. • Везде — правило будет применено всегда независимо от местоположения компьютера пользователя.

Наименование	Описание
Действие	Действие правила: • Запретить — блокирует трафик. • Разрешить — разрешает трафик. • Перенаправить в прокси — перенаправляет трафик, соответствующий условиям правила в указанный прокси сервер. При выборе действия указание параметров Списки URL, Категории, Типы контента недоступно.
Журналирование	Определяет, записывать ли срабатывание данного правила в журнал на сервере LogAn.
Прокси-сервер	Выбор прокси-сервера, при указании действия Перенаправить в прокси . Прокси сервер указывается через выбор профиля прокси сервера. Более подробно об профилях прокси-серверов читайте в главе Профили прокси .
Пользователи	Указание пользователей или групп пользователей LDAP, для которых будет применено данное правило межсетевого экрана. Для указания пользователей необходим корректно настроенный LDAP-коннектор. Подробнее читайте в разделе Каталоги пользователей .
Источник	Списки IP-адресов источника трафика. Список может быть создан предварительно в разделе Библиотеки → IP-адреса или при настройке правила. Более подробно об списках IP-адресов читайте в главе IP-адреса.
Назначение	Списки IP-адресов назначения трафика. Список может быть создан предварительно в разделе Библиотеки → IP-адреса или при настройке правила. Более подробно об списках IP-адресов читайте в главе IP-адреса.
Сервис	Тип сервиса, например, HTTP, HTTPS, или группа сервисов. Сервисы или группы сервисов могут быть предварительно созданы в разделах Библиотеки → Сервисы и разделе Библиотеки → Группы сервисов, соответственно, а также при настройке правил межсетевого экрана. Более подробно об сервисах читайте в главе Сервисы.
Приложения	Список приложений, для которых применяется данное правило. Приложение может быть создано предварительно в разделе Библиотеки → Приложения или при настройке правила межсетевого экрана. Более подробно об приложениях читайте в главе Приложения.
Списки URL	Списки адресов URL. Списки URL можно создать в разделе Библиотеки → Списки URL или в свойствах правил межсетевого экрана. Более подробно о работе со списками URL читайте в главе Списки URL. Важно! При использовании списков URL в качестве условий фильтрации трафика указание сервисов обязательно.
Категории сайтов	Списки категорий UserGate URL filtering 4.0. В руках администратора находится управление доступом к таким категориям, как порнография, вредоносные сайты, онлайн-казино, игровые и развлекательные сайты, социальные сети и многие другие. Также для добавления доступны группы URL-категорий, которые могут быть созданы в разделе Библиотеки → Категории URL или при настройке правил. Более подробно об категориях читайте в главе Категории URL. Важно! При использовании категорий сайтов как одного из условий правила межсетевого экрана указание сервисов обязательно.
Типы контента	Списки типов контента. Предусмотрена возможность управления видеоконтентом, аудио контентом, изображениями, исполняемыми файлами и другими типами. Администраторы также могут создавать собственные группы типов контента. Создание доступно в разделе Библиотеки → Типы контента, а также в свойствах правила межсетевого экрана. Более подробно о работе с MIME-типами читайте в главе Типы контента. Важно! При использовании типов контента в качестве одного из условий правила межсетевого экрана указание сервисов обязательно.

Наименование	Описание
Время	Время, когда правило активно. Администратор может добавить необходимые ему временные интервалы в разделе Календари или при настройке правила. Важно! Расписание работает в часовом поясе конечного устройства с установленным ПО UserGate Client.
НIP профили	Список профилей НIP. Правило межсетевого экрана будет применено только в случае соответствия конечного устройства объектам НIP, указанным в профиле. Подробнее о профилях и объектах НIP читайте в соответствующих разделах НIP профили и Объекты НIP .
Конечные устройства	Конкретные конечные устройства, к которым будет применено данное правило. Если ничего не указано, то данное правило применяется ко всем устройствам, к которым данный шаблон применен.

Библиотеки элементов

Данный раздел содержит в себе адреса-сайтов, IP-адреса, приложения и прочие элементы, которые используются при настройке правил управляемых устройств UGC.

Сервисы

Раздел сервисы содержит список общеизвестных сервисов, основанных на протоколе TCP/IP, например, таких, как HTTP, HTTPS, FTP и другие. Данные сервисы могут быть использованы при построении правил управляемых устройств UGC. Первоначальный список сервисов поставляются вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Для добавления нового сервиса необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать сервис.	Нажать на кнопку Добавить , дать сервису название, ввести комментарий.
Шаг 2. Указать протокол и порт.	Нажать на кнопку Добавить , выбрать из списка необходимый протокол, указать порты назначения и, опционально, порты источника. Для указания диапазона портов можно использовать — (тире), например, 33333-33355.

IP-адреса

Раздел **IP-адреса** содержит список диапазонов IP-адресов, которые могут быть использованы при построении правил управляемых устройств UGC.

Администратор может добавлять необходимые ему элементы в процессе работы. Для добавления нового списка адресов необходимо выполнить следующие шаги:

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

Администратор имеет возможность создавать свои списки IP-адресов и централизованно управлять ими. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание

Наименование	Описание
Шаг 1. Создать файл с необходимыми IP-адресами.	Создать файл list.txt со списком адресов.
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip .
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.
Шаг 5. Создать список IP-адресов и указать URL для обновления.	На каждом UserGate создать список IP-адресов. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. UserGate будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

Приложения

Элемент библиотеки **Приложения** позволяет создать группы приложений для более удобного использования в правилах фильтрации сетевого трафика. Например, администратор может создать группу приложений «Бизнес приложения» и поместить в нее необходимые приложения.

ПО UserGate Client определяет приложение по его контрольной сумме, что дает администратору возможность очень точно и выборочно управлять доступом в сеть для определенных приложений, например, разрешать доступ в сеть только для определенной версии приложения, блокируя при этом все остальные версии данного приложения.

Для добавления новой группы приложений необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать группу приложений.	В панели Группы приложений нажать на кнопку Добавить , дать название группе.

Наименование	Описание
Шаг 2. Добавить приложения.	Выделить созданную группу и в панели Приложения нажать на кнопку Добавить и указать название и контрольную сумму приложения. Контрольная сумма исполняемого файла Windows должна быть определена по алгоритму SHA1, например, с помощью утилиты fciv.

Пользователь может производить экспорт и импорт списков с использованием одноимённых кнопок (**Экспорт** и **Импорт**). Записи списка/файла со списком приложений должны соответствовать следующему формату: **НАЗВАНИЕ_ПРИЛОЖЕНИЯ ХЭШ**.

Списки URL

Страница предназначена для задания списков указателей URL, которые могут быть использованы в правилах контентной фильтрации в качестве черных и белых списков.

Для фильтрации с помощью списков URL необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать список URL.	В панели Списки URL нажать на кнопку Добавить , задать название нового списка.
Шаг 2. Добавить необходимые записи в новый список.	Добавить записи URL в новый список. В списках можно использовать специальные символы «^», «\$» и «*»: • «*» — любое количество любых символов. • «^» — начало строки. • «\$» — конец строки. Символы «?» и «#» не могут быть использованы.
Шаг 3. Создать правило межсетевого экрана конечного устройства, содержащее один или несколько списков.	Смотрите раздел Политики сети .

Если вы хотите заблокировать точный адрес, используйте символы «^» и «\$»:

`^http://domain.com/exacturl$`

Для блокирования точного URL всех дочерних папок используйте символ «^»:

`^http://domain.com/exacturl/`

Для блокирования домена со всеми возможными URL используйте запись такого вида:

`domain.com`

Пример интерпретации URL-записей:

Пример записи	Обработка HTTP-запросов
yahoo.com или *yahoo.com*	Блокируется весь домен и все URL этого домена и домены 3 уровня, например: http://sport.yahoo.com http://mail.yahoo.com https://mail.yahoo.com http://sport.yahoo.com/123
^mail.yahoo.com\$	Заблокированы только http://mail.yahoo.com https://mail.yahoo.com
^mail.yahoo.com/\$	Ничего не заблокировано, так как последний символ слэш определяет URL, но не указаны «https» или «http»

Пример записи	Обработка HTTP-запросов
^http://finance.yahoo.com/personal-finance/\$	Заблокирован только http://finance.yahoo.com/personal-finance/
^yahoo.com/12345/	Заблокированы http://yahoo.com/12345/whatever/ https://yahoo.com/12345/whatever/

Администратор имеет возможность создавать собственные списки и централизованно распространять их. Для создания таких списков необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимым списком URL.	Создать текстовый файл list.txt со списком URL в следующем формате: www.site1.com/url1 www.site2.com/url2 ... www.siteend.com/urlN
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip .
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.
Шаг 5. Создать список типа контента и указать URL для обновления.	На каждом UserGate создать список URL. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. UserGate будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

Категории URL

Элемент библиотеки **Категории URL** позволяет создать группы категорий UserGate URL filtering для более удобного использования в правилах фильтрации контента. Например, администратор может создать группу категорий «Бизнес категории» и поместить в нее необходимые категории.

Для добавления новой группы категорий необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать группу категорий.	В панели Группы URL категорий нажать на кнопку Добавить , дать название группе.
Шаг 2. Добавить категории.	Выделить созданную группу и в панели Категории нажать на кнопку Добавить и выбрать необходимые категории из списка.

Типы контента

С помощью фильтрации типов контента доступна возможность управления видео и аудио контентом, изображениями, исполняемыми файлами и другими типами.

Для фильтрации по типу контента необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать список типов контента.	В панели Категории нажать на кнопку Добавить , задать название нового списка типа контента и, опционально, описание списка и URL обновления.
Шаг 2. Добавить необходимые MIME-типы в новый список.	Добавить необходимый тип контента в данный список в формате MIME. Различные типы MIME описаны в интернете, например, https://www.iana.org/assignments/media-types/media-types.xhtml . Например, для блокировки документов типа *.doc необходимо добавить MIME-тип «application/msword».
Шаг 3. Создать правило фильтрации контента, содержащее один или несколько списков.	Смотрите раздел Политики сети .

Администратор имеет возможность создавать свои списки типов контента и централизованно распространять их. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми типами контента.	Создать файл list.txt со списком типов контента.
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip .
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.

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

Календари

Календари позволяют создать временные интервалы, которые затем можно использовать в правилах. Администратор может добавлять необходимые ему элементы в процессе работы. Для добавления нового календаря необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать календарь.	В панели Группы нажать на кнопку Добавить , указать название календаря и его описание.
Шаг 2. Добавить временные интервалы в календарь.	В панели Элементы нажать на кнопку Добавить и добавить интервал. Дать название интервалу и указать время.

Version: 7.0.1

Product: UGMC

Documentation: 

Группы шаблонов объединяют несколько шаблонов в единую конфигурацию, которая применяется к управляемому устройству.

Результирующие настройки, применяемые к устройству, формируются в результате слияния всех настроек шаблонов, входящих в группу шаблонов, с учетом расположения шаблонов внутри группы. Подробнее о результирующих настройках смотрите главу руководства [Шаблоны и группы шаблонов](#).

Для создания группы шаблонов необходимо в разделе **Управление конечными устройствами → Группы шаблонов** нажать на кнопку **Добавить**, дать группе имя и опциональное описание и добавить в него созданные ранее шаблоны. После добавления шаблонов их можно расположить в требуемом порядке, используя кнопки **Выше**, **Ниже**, **Наверх**, **Вниз**, создав таким образом необходимую результирующую конфигурацию.

Добавление управляемых устройств UGC под управление UGMC

Version: 7.0.1
Product: UGMC
Documentation: ☒

Для управления устройствами они должны быть добавлены в UGMC. Добавление управляемых устройств UGC возможно двумя способами:

- 1. Добавление управляемых устройств UGC по одному устройству. Данный вариант подходит для компаний с небольшим количеством управляемых устройств UGC.
- 2. Массовое добавление устройств. Вариант для компаний с большим количеством устройств.

Процесс единичного добавления устройств

Для добавления одного управляемого устройства UGC необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Обеспечить доступ от управляемого устройства UGC до UGMC.	На сервере UGMC необходимо разрешить сервис Контроль конечных устройств на зоне, к интерфейсу которой подключаются управляемое устройство. Сервер UGMC слушает подключения от управляемых устройств UGC на портах TCP 4043 и 9712. Передача данных между сервером UGMC и управляемым устройством осуществляется по зашифрованному каналу.
Шаг 2. Создать запись для управляемого устройства UGC в UGMC.	В консоли управления областью в разделе Управление конечными устройствами → Конечные устройства нажать кнопку Добавить и указать необходимые настройки.
Шаг 3. Отобразить уникальный код созданного устройства.	В консоли управления областью в разделе Управление конечными устройствами → Конечные устройства нажать кнопку Показать уникальный код устройства и зафиксировать его. Данный код потребуется указать при установке ПО UGC на конкретное устройство (компьютер) пользователя.
Шаг 4. Установить ПО UGC на конкретное устройство (компьютер) пользователя.	Установить ПО на конечный компьютер пользователя. В мастере установки указать IP-адрес UGMC и уникальный код устройства, созданный на предыдущем шаге. Подробнее об установке ПО на конечное устройство смотрите в разделе Установка ПО UserGate Client .

При создании записи управляемого устройства UGC необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает объект управляемого устройства UGC. Если объект управляемого устройства UGC включен, то он занимает одну лицензию.
Название	Название для управляемого устройства UGC. Можно вводить произвольное название.
Описание	Описание управляемого устройства UGC.
Группы шаблонов	Группа шаблонов, настройки которой следует применить к этому управляемому устройству UGC. Настройки (политики) применяются после синхронизации с UserGate Management Center.
Синхронизация	Режим синхронизации: отключено, автоматическая или ручная синхронизация.

Процесс массового добавления устройств

Рассмотрим процесс массового добавления управляемых устройств UGC:

Наименование	Описание

Наименование	Описание
Шаг 1. Обеспечить доступ от управляемых устройств UGC до UGMC.	На сервере UGMC необходимо разрешить сервис Контроль конечных устройств на зоне, к интерфейсу которой подключаются управляемые устройства. Сервер UGMC слушает подключения от управляемых устройств UGC на портах TCP 4043 и 9712. Передача данных между сервером UGMC и управляемыми устройствами осуществляется по зашифрованному каналу.
Шаг 2. Создать код для группы конечных устройств.	В консоли управления областью в разделе Управление конечными устройствами → Коды для конечных устройств нажать кнопку Добавить и указать необходимые параметры.
Шаг 3. Отобразить уникальный код для созданной группы устройств.	В консоли управления областью в разделе Управление конечными устройствами → Коды для конечных устройств нажать кнопку Уникальный код конечного устройства и зафиксировать его. Данный код потребуется указать при инсталляции ПО UGC на группу устройств.
Шаг 4. Установить ПО UGC на устройства пользователей.	Установить ПО на конечные компьютеры пользователей. В мастере установки или в административном шаблоне Active Directory указать уникальный код группы устройств, созданный на предыдущем шаге и IP-адрес интерфейса UGMC, к которому будут подключены управляемые устройства. После завершения установки ПО автоматически создается запись для каждого устройства в UGMC в разделе Управление конечными устройствами → Конечные устройства , и каждое конечное устройство получает все настройки, указанные в примененной к нему группе шаблонов. Подробнее об установке ПО на конечное устройство смотрите в разделе Установка ПО UserGate Client .

При создании кода для группы конечных устройств необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает данный код. Если код отключен, то он не может быть использован для добавления новых устройств, но все устройства, созданные ранее с применением данного кода, продолжат работать.
Название	Название для кода. Можно вводить произвольное название.
Описание	Описание данного кода.
Группы шаблонов	Группа шаблонов, настройки которой следует применить к управляемым устройствам UGC, активированными с данным кодом. Настройки (политики) применяются после синхронизации с UGMC.

Version: 7.0.1
Product: UGMC
Documentation: 

После добавления управляемое устройство UGC отобразится в разделе веб-консоли **Управление конечными устройствами → Конечные устройства**.

Раздел веб-консоли **Управление конечными устройствами → Конечные устройства** позволяет совершать следующие действия над управляемыми устройствами:

- Добавление нового конечного устройства. Добавление конечного устройства было рассмотрено ранее в разделе [Добавление управляемых устройств UGC под управление UGMC](#).
- Редактирование свойств конечного устройства, т.е. изменение названия, описания конечного устройства, применённых к нему групп шаблонов и типа синхронизации.
- Удаление выбранного конечного устройства.
- Включение/Отключение синхронизации с конечным устройством.
- Блокирование/Разблокирование передачи данных по сети.
- Задание частоты синхронизации соединений UGMC и управляемых устройств UGC.
- Отображение уникального кода устройства, необходимого для подключения управляемых устройств UGC к UGMC.
- Запуск процесса принудительной синхронизации.

Данный раздел также позволяет просмотреть следующие параметры каждого конечного устройства:

Наименование	Описание
Название	Отображено название конечного устройства.
Версия	Отображена версия UserGate Client, установленная на устройстве.
Последнее подключение	Показаны дата и время последнего подключения конечного устройства.
Телеметрия	Представлена следующая информация: • IP-адрес конечного устройства, который используется для выхода в Интернет. • Netbios имя. • Время последнего подключения управляемого устройства UGC к UGMC. • Пользователь, с учётной записи которого был совершён вход в систему. • Имя компьютера в локальной сети. • Версия ОС, установленная на конечном устройстве. • Версия UserGate Client, установленная на устройстве. • Загрузка CPU клиентом UserGate показывает на сколько загружен центральный процессор конечного устройства. • Загрузка памяти клиентом UserGate - количество памяти, используемое UserGate Client. • Загрузка физической памяти отображает загруженность оперативной памяти на конечном устройстве. • Загрузка виртуальной памяти показывает степень загруженности виртуальной памяти на конечном устройстве.
Мониторинг конечных устройств	Показана подробная информация о конечном устройстве. Более подробно данный пункт будет рассмотрен ниже. В случае возникновения ошибки синхронизации конфигурации конечного устройства доступен просмотр отчёта (нажать Показать отчёт), в котором отображены время последнего подключения к управляемому устройству, название правила, тип объекта, ставшего причиной сбоя синхронизации, и описание ошибки. При возникновении ошибки применение правил межсетевого экрана к конечному устройству не изменяется (т.е. действуют правила межсетевого экрана, которые были синхронизированы до появления ошибки), доступны управление сервисами и процессами и выполнение запросов в реестр.

Наименование	Описание
Группа шаблонов конечных устройств	Отображены группы шаблонов, применённые к управляемому устройству UGC. Создание групп шаблонов было рассмотрено в главе Группы шаблонов управляемых устройств UGC.
НIP профили	Представлен список профилей НIP. Профиль НIP будет отображен в списке, только в случае его применения в правилах межсетевого экрана. О соответствии или несоответствии конечного устройства профилю НIP говорит цветовая индикация: - Зелёный - конечное устройство соответствует профилю. - Красный - конечное устройство не соответствует профилю. В случае несоответствия к просмотру доступен отчёт (нажмите Посмотреть отчёт), содержащий информацию о времени последнего получения данных, название профиля и объекта НIP, тип и несоответствующий элемент объекта. Подробнее читайте в разделе НIP профили.
Устройства LogAn	Название сервера LogAn, на который конечное устройство отправляет журналы диагностики и телеметрию.
Время последней синхронизации	Отображён режим, а также дата и время последней синхронизации конечного устройства и UGMC. Работа возможна в одном из следующих режимов: Автоматическая синхронизация — настройки применяются к устройству автоматически. При изменении любой настройки из любого шаблона, включенного в группу шаблонов, примененную к УУ, это изменение применяется без задержек. Отключено — синхронизация выключена. Ручная синхронизация — режим синхронизации, при котором настройки применяются при нажатии кнопки Синхронизировать сейчас. Полезно в случаях, когда необходимо изменить много настроек в шаблонах и одновременно отослать их на устройство. В этом случае необходимо отключить синхронизацию, произвести необходимые изменения в шаблонах, после чего включить синхронизацию в режим Ручная синхронизация.

Вкладка мониторинг конечных устройств необходима для отслеживания состояния управляемых устройств UGC. Она позволяет просмотреть следующие параметры конечного устройства:

Наименование	Описание
Общие	Представлена общая информация об устройстве (имя компьютера, версия и тип ОС, версия ПО UserGate Client, IP-адрес, время загрузки системы и текущее время на устройстве в часовом поясе, настроенном на конечном устройстве) и пользователя, под учётной записью которого был совершён вход в систему (фотография, имя и статус пользователя, тип аккаунта (локальный или доменный), телефон и электронная почта).
Производительность	Представлена следующая информация: - Использование процессора, т.е. степень загруженности центрального процессора. - Степень загрузки центрального процессора конечного устройства процессом UserGate Client. - Информация о виртуальной памяти конечного устройства. - Информация о физической памяти - оперативной памяти. - Загрузка памяти клиентом UserGate. - Информация о дисках компьютера: размер диска, тип и производительность. - Статус управляемого устройства UGC показывает статус UserGate Client: онлайн/офлайн (доступность конечного устройства) или отключено (UserGate Client был отключен с использованием UGMC кнопкой Отключить).
Безопасность	Представлена информация о безопасности конечного устройства: статус межсетевого экрана, антивируса, центров обновления и безопасности Windows, а также информация о шифровании дисков (BitLocker).

Наименование	Описание
USB устройства	Отображена информация о подключённых устройствах USB: • Идентификатор устройства: пара идентификаторов VID/PID (Vendor ID/Product ID) и номер версии устройства. • Название устройства. • USB класс, например mouse, printer. • Сервис: драйверы, использующиеся для работы с устройством.
Элементы автозагрузки	Отображён список приложений, для которых настроен автоматический запуск при входе в систему.
Процессы	Показан список запущенных на конечном устройстве процессов. Нажатие кнопки Завершить процесс позволяет завершить процесс на конечном устройстве, используя UGMC.
Службы	Отображён список служб, запущенных/остановленных на конечном устройстве. Нажатие кнопок Остановить службу/Запустить службу позволяет выполнить попытку отключения/включения службы на управляемом устройстве UGC с использованием UGMC.
Ключи реестра	Просмотр реестра. Доступны: • HKEY_LOCAL_MACHINE. • HKEY_USERS. Также доступен поиск по ключам реестра. Для этого необходимо нажать Найти (отображается при наведении указателя мыши на название каталога).
Программное обеспечение	Отображён список установленных на управляемом устройстве UGC ПО с указанием производителя и версии.
Установленные обновления	Представлен список установленных обновлений на управляемом устройстве UGC с отображением соответствующего номера базы знаний Microsoft, информации о продукте, производителе и дате установки обновления.

В веб-интерфейсе UGMC доступна фильтрация управляемых устройств UserGate Client. В случае использования фильтрации доступно отображение:

- включенных/выключенных конечных устройств;
- заблокированных/незаблокированных устройств;
- устройств онлайн (подключенных к UGMC)/офлайн (неподключенных к UGMC)/не привязанных (устройств, которые еще не были подключены к UGMC);
- консистентных (синхронизация конечного устройства завершилась успешно)/неконсистентных (при синхронизации конфигурации конечного устройства возникли ошибки) устройств;
- соответствующих/несоответствующих требованиям безопасности.

Также имеется возможность формирования более сложных фильтров в режиме расширенного поиска, используя специальный язык запросов.

Version: 7.0.1
Product: UGMC
Documentation: ☒

LogAn является продуктом компании UserGate, входящим в состав экосистемы UserGate SUMMA. LogAn устанавливается на отдельном сервере, использование которого позволяет обеспечить высокую надёжность и хорошую масштабируемость системы. LogAn предоставляет возможность осуществления сбора и анализа данных с различных устройств, мониторинга событий безопасности и создания отчётов. Для получения подробной информации о LogAn обратитесь к соответствующей документации.

Для отправки данных на сервер LogAn, его необходимо назначить, используя шаблон конечных устройств. Для передачи журналов и телеметрии с UG Client на сервер UG LogAn используется один из портов из диапазона (22000-22711), автоматически выделенный в MC для данного конечного устройства, передача данных происходит через UGMC. Настройка сервера LogAn для конечных устройств производится с использованием шаблонов конечных устройств. Подробнее читайте в разделе [Настройки](#).

Получая данные, LogAn осуществляет анализ произошедших событий и отслеживает активность пользователей. Полученные с управляемого устройства UGC события будут записаны в следующие журналы:

- Журнал событий конечных устройств;
- Журнал правил конечных устройств;
- Журнал приложений конечных устройств;
- Журнал аппаратуры.

Для просмотра данных с устройств UGC используется раздел веб-консоли **Журналы и отчёты → Журналы → Конечные устройства**.

Формирование данных журналов будет рассмотрено далее в разделах [Журнал событий конечных устройств](#), [Журнал правил конечных устройств](#), [Приложения конечных устройств](#) и [Аппаратура конечных устройств](#).

Журнал событий конечных устройств

В журнале событий конечных устройств отражены события, получаемые от конечных устройств, контролируемых с использованием программного обеспечения UserGate Client.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например, диапазон дат, важности, типу события и т.п.

В UserGate LogAn также представлен режим расширенного поиска для формирования сложных фильтров поиска с использованием специального языка запросов, синтаксис которого рассмотрен далее в разделе [Режим расширенного поиска](#).

После выбора необходимых параметров настроенный фильтр можно сохранить, нажав кнопку **Сохранить как**. Список сохранённых фильтров можно будет увидеть во вкладке **Популярные фильтры**.

Администратор может сам выбрать столбцы, которые будут отражаться в журнале. Для этого необходимо навести указатель мыши на название любого столбца, нажать на появившуюся справа от названия столбца стрелку, выбрать **Столбцы** и в появившемся контекстном меню выбрать необходимые параметры.

В журнале событий конечных устройств можно увидеть следующую информацию:

Наименование	Описание
Узел	Идентификатор конечного устройства или узла, на котором запущен сенсор.
Время	Время события. Отображается в часовом поясе, настроенном на LogAn.
Конечное устройство/сенсор	Отображено имя компьютера.

Наименование	Описание
Уровень лога	Отображен тип события: • Аудит успеха (Audit Success): событие журнала безопасности, которое происходит при успешном обращении к аудируемым ресурсам; • Аудит отказа (Audit Failure): событие журнала безопасности, которое происходит при неуспешном обращении к аудируемым ресурсам; • Ошибка (Error): событие указывает на существенные проблемы, которые могут стать причиной потери функциональности или данных; • Сведения (Information): информационные события, которые, как правило, не требуют внимания администратора; • Предупреждение (Warning): события указывают на проблемы, которые не требуют немедленного исправления, однако могут привести к ошибкам в будущем.
Данные	Представлена подробная информация о событии.
Источник журнала событий	Показан источника журнала событий.
Категория журнала	Отображена категория лога, необходимая для упорядочивания событий. Данные берутся из Windows EventLog. Каждый источник может определять свои идентификаторы категорий. Относится к записям журнала событий конечных устройств.
Категория инцидента	Показана категория инцидента.
Имя компьютера	Показано полное имя компьютера.
Имя пользователя	Показано имя пользователя, с учётной записи которого был совершен вход в систему конечного устройства.
Код события лога	Представлен код, соответствующий определённому событию.
Идентификатор события лога	Отображён идентификатор события лога, который определяет первичный идентификатор события.
Тип события лога	Отображён тип события лога, соответствующий определённому уровню лога: • 1 - уровень лога: ошибка (error); • 2 - уровень лога: предупреждение (warning); • 3 - уровень лога: сведения (information); • 4 - уровень лога: аудит успеха (audit success); • 5 - уровень лога: аудит отказа (audit failure).
Строка вставки	Содержит данные блока eventData события Windows.
Файл журнала лога	Показано к какому типу файла журнала относится событие: • Application (файл журнала приложений): для событий приложений и служб; • Security (файл журнала безопасности): для событий системы аудита; • System (файл системного журнала): для событий драйверов устройств; • CustomLog: журнал содержит события, регистрируемые приложениями, которые создают пользовательский журнал. Использование пользовательского журнала позволяет приложению управлять размером журнала или присоединять списки управления доступом в целях безопасности, не затрагивая другие приложения.

С использованием кнопки **Показать** можно просмотреть выбранную запись журнала событий конечных устройств.

Запись журнала может быть добавлена к сведениям об инциденте нажатием кнопки **Добавить в инцидент**.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Журнал правил конечных устройств

Журнал правил конечных устройств отображает события срабатывания правил межсетевого экрана конечных устройств, в настройках которых включена функция **Журналирование**. Настройка правил межсетевого экрана рассматривается в разделе [Политики сети](#).

Для удобства поиска необходимых событий записи срабатываний правил межсетевого экрана могут быть отфильтрованы по различным критериям, например, диапазон дат, названию правил и т.п.

В UserGate LogAn также представлен режим расширенного поиска для формирования сложных фильтров поиска с использованием специального языка запросов, синтаксис которого рассмотрен далее в разделе [Режим расширенного поиска](#).

После выбора необходимых параметров настроенный фильтр можно сохранить, нажав кнопку **Сохранить как**. Список сохранённых фильтров можно будет увидеть во вкладке **Популярные фильтры**.

Администратор может сам выбрать столбцы, которые будут отражаться в журнале. Для этого необходимо навести указатель мыши на название любого столбца, нажать на появившуюся справа от названия столбца стрелку, выбрать **Столбцы** и в появившемся контекстном меню выбрать необходимые параметры.

В журнале правил конечных устройств можно увидеть следующую информацию:

Наименование	Описание
Узел	Идентификатор конечного устройства.
Время	Указано время срабатывания правила. Отображается в часовом поясе, настроенном на LogAn.
Конечное устройство	Отображено имя компьютера.
Действие	Представлено действие, которое выполняется в соответствии с правилом: • Разрешить; • NAT; • Запретить.
Правило	Показано название правила межсетевого экрана.
Приложение	Указано приложение, через которое осуществляется доступ к ресурсу.
Домен	Отображено имя домена, к которому было выполнено подключение.
Категория сайтов	Указаны категории сайтов, к которым относится адрес назначения. Категории сайтов будут отображены только в случае наличия правил с условием Категории сайтов.
Тип контента	Отображён тип контента.
Сетевой протокол	Указан транспортный протокол, использующийся для подключения к ресурсу.
IP источника	Показан IP-адрес источника трафика.
Порт источника	Отображён номер порта, через который осуществляется подключение.
IP назначения	Показан IP-адрес назначения трафика.
Порт назначения	Указан номер порта назначения, используемый транспортным протоколом.

Нажав кнопку **Показать**, можно просмотреть подробную информацию о выбранной записи журнала правил конечных устройств.

Запись журнала может быть добавлена к сведениям об инциденте нажатием кнопки **Добавить в инцидент**.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Приложения конечных устройств

Журнал приложений конечных устройств отображает приложения, которые запускались на конечных устройствах.

Для удобства формирования журнала записи могут быть отфильтрованы по различным критериям.

В UserGate LogAn также представлен режим расширенного поиска для формирования сложных фильтров поиска с использованием специального языка запросов, синтаксис которого рассмотрен далее в разделе [Режим расширенного поиска](#).

После настройки фильтра его можно сохранить, нажав кнопку **Сохранить как**. После сохранения фильтр будет доступен во вкладке **Популярные фильтры**.

Администратор может сам выбрать столбцы, которые будут отражаться в журнале. Для этого необходимо навести указатель мыши на название любого столбца, нажать на появившуюся справа от названия столбца стрелку, выбрать **Столбцы** и в появившемся контекстном меню выбрать необходимые параметры.

В журнале приложений конечных устройств отображается следующая информация:

Наименование	Описание
Узел	Идентификатор конечного устройства.
Время	Время запуска приложения на конечном устройстве. Отображается в часовом поясе, настроенном на LogAn.
Конечное устройство	Отображено имя компьютера.
Действие	Запуск или остановка приложения.
Хэш	Хэш приложения.
Приложение	Название приложения, которое было запущено или остановлено.
Версия	Версия приложения.
Субъект подписи	Владелец сертификата.
Подписано	Издатель сертификата для приложения.
Идентификатор процесса	Идентификатор процесса приложения (PID).
Пользователь	Пользователь, запустивший приложение.
Командная строка	Команда запуска приложения.

Нажатие кнопки **Показать** позволяет открыть окно с информацией о записи журнала приложений.

Запись журнала может быть добавлена к сведениям об инциденте нажатием кнопки **Добавить в инцидент**.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Аппаратура конечных устройств

Данный журнал содержит информацию об устройствах, подключаемых к управляемому устройству UGC.

Для удобства формирования журнала записи могут быть отфильтрованы по различным критериям.

В LogAn также представлен режим расширенного поиска для формирования сложных фильтров поиска с использованием специального языка запросов, синтаксис которого рассмотрен далее в разделе [Режим расширенного поиска](#).

После настройки фильтра его можно сохранить, нажав кнопку **Сохранить как**. После сохранения фильтр будет доступен во вкладке **Популярные фильтры**.

Администратор может сам выбрать столбцы, которые будут отражаться в журнале. Для этого необходимо навести указатель мыши на название любого столбца, нажать на появившуюся справа от названия столбца, нажать на появившуюся справа от названия столбца стрелку, выбрать **Столбцы** и в появившемся контекстном меню выбрать необходимые параметры.

Журнал аппаратуры конечных устройств содержит следующую информацию:

Наименование	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/удалённого устройства.
Служба	Драйверы, использующиеся для работы с устройством.

Нажатие кнопки **Показать** позволяет открыть окно с информацией о записи журнала аппаратуры конечных устройств.

Запись журнала может быть добавлена к сведениям об инциденте нажатием кнопки **Добавить в инцидент**.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

HIP профили

Product: UGMC

Version: 7.0.1

Documentation: ☒

Host Information Profile (HIP) позволяет производить сбор и анализ информации о степени защиты конечного устройства с установленным ПО UserGate Client. HIP профили представляют собой набор объектов HIP и предназначены для проверки соответствия конечного устройства требованиям безопасности. С использованием профилей HIP можно настроить гибкие политики доступа к зоне сети или приложению.

Для конечных устройств будут отображены только те профили HIP, которые используются в правилах межсетевого экрана.

При создании профиля необходимо указать:

Наименование	Описание
Включено	Включение/отключение использования профиля.
Название	Название профиля HIP.
Описание	Описание профиля HIP (опционально).
Объекты HIP	Выбор логического элемента (И, ИЛИ, И НЕ, ИЛИ НЕ) и объектов HIP. Подробнее о создании объектов читайте в разделе Объекты HIP .

Объекты HIP

Version: 7.0.1
Product: UGMC
Documentation: ☒

Объекты HIP позволяют настроить критерии соответствия для конечных устройств, к которым необходимо применить политики.

Для добавления объекта необходимо указать:

Наименование	Описание
Включено	Включение/отключение использования объекта.
Название	Название объекта HIP.
Описание	Описание объекта HIP (опционально).
Версия ОС	Версия операционной системы устройства пользователя.
Версия UserGate Client	Версия ПО UserGate Client.
Продукты	Проверка на соответствие статуса: • Антивирус. Проверка соответствия антивирусного ПО на устройстве пользователя. ◦ Включено: проверка статуса ПО; ◦ Базы антивируса обновлены: да, нет, не проверять; ◦ Версия ПО; ◦ Вендор: производитель и название продукта. • Межсетевой экран. Проверка соответствия межсетевого экрана на конечном устройстве. При настройке необходимо указать: ◦ Установлен: проверка наличия установленного ПО; ◦ Включено: проверка статуса ПО (да, нет, не проверять); ◦ Версия ПО; ◦ Вендор: производитель и название продукта. • Резервное копирование. Проверка ПО для резервного копирования: ◦ Установлен: проверка наличия установленного ПО; ◦ Версия ПО; ◦ Вендор: производитель и название продукта. • Шифрование диска. Проверка соответствия статуса шифрования диска на конечном устройстве. ◦ Установлен: проверка наличия установленного ПО; ◦ Версия ПО; ◦ Вендор: производитель и название продукта. • DLP. Проверка соответствия системы предотвращения утечек информации. ◦ Установлен: проверка наличия установленного ПО; ◦ Версия ПО; ◦ Вендор: производитель и название продукта.
Процессы	Проверка процессов, запущенных на конечном устройстве.
Запущенные службы	Проверка служб, запущенных на конечном устройстве.

Наименование	Описание
Ключи реестра	Ключ реестра Microsoft Windows - каталог, в котором хранятся настройки и параметры операционной системы. Поддерживаются следующие типы параметров реестра: • REG_SZ: строка Unicode или ANSI с нулевым символом в конце; • REG_BINARY: двоичные данные в любой форме; • REG_DWORD: 32-разрядное число. Доступно использование следующих ключей реестра: • HKEY_LOCAL_MACHINE (аббревиатура: local_machine, hklm); • HKEY_USERS (аббревиатура: users, hku). Важно! При указании пути также доступно использование аббревиатуры корневого каталога реестр. Путь указывается с использованием обратного слэша (\), например, \hklm. Описание ключей реестра читайте в документации Microsoft (https://docs.microsoft.com/ru-ru/troubleshoot/developer/webapps/iis/general/use-registry-keys).
Установленные обновления	Проверка наличия указанного обновления на конечном устройстве. Необходимо указать номер статьи базы знаний Microsoft (KB), например, KB5013624.

