

Table of Contents

Table of Contents	1
Management Center 7.0.1 Руководство администратора	3
Принятые обозначения и сокращения	4
Введение	5
Описание	6
Управляемые области	7
Шаблоны и группы шаблонов	8
Управляемые устройства	10
Управление UGMC	11
Лицензирование UGMC	13
Лицензирование UGMC	14
Планирование внедрения UGMC	15
Планирование внедрения UGMC (Описание)	16
Первоначальная настройка	19
Первоначальная настройка	20
Офлайн операции с сервером	22
Офлайн операции с сервером(Описание)	23
Настройка UGMC	24
Общие настройки	25
Управление устройством	26
Администраторы	33
Управление сертификатами	35
Серверы аутентификации UGMC	37
Профили аутентификации UGMC	39
Библиотеки элементов	40
Расширение системного раздела	44
Настройка сети	45
Настройка сети(Описание)	46
Интерфейс командной строки (CLI)	51
Интерфейс командной строки (CLI) Описание	52
Диагностика и мониторинг	55
Диагностика и мониторинг	56
Журналы и отчёты	67
Журнал событий	68
Режим расширенного поиска	69
Экспорт журналов	71
Управление областями	74
Создание управляемых областей	75
Администраторы области	76
Серверы аутентификации области	78
Профили аутентификации области	80
Каталоги пользователей	81
Управление областями (Описание)	82
Управление межсетевыми экранами UserGate	83
Управление межсетевыми экранами UserGate (Описание)	84
Управление устройствами LogAn	92
Управление устройствами LogAn (Описание)	93
Управление конечными устройствами	99
Управление конечными устройствами UserGate Client (Описание)	100
Установка ПО UserGate Client	101

Шаблоны управляемых устройств UGC	103
Группы шаблонов управляемых устройств UGC	114
Добавление управляемых устройств UGC под управление UGMC	115
Управление устройством UGC из консоли UGMC	117
Сбор и анализ данных с устройств UGC	120
NIP профили	125
Объекты NIP	126
Приложения	128
Описание форматов журналов	129
Требования к сетевому окружению	131

Принятые обозначения и сокращения

Описание

Documentation: ☒

Product: UGMC

Version: 6.1.9, 7.0.1, 7.1.0

UserGate Management Center (UGMC) — это продукт, который позволяет контролировать большое количество управляемых устройств. Управляемым устройством может служить межсетевой экран UserGate или устройство сбора и анализа данных LogAn.

UGMC предоставляет единую точку управления, из которой администратор может выполнять мониторинг управляемых устройств, применять необходимые настройки, создавать политики, применяемые к группам устройств для обеспечения безопасности корпоративной сети. Использование UGMC позволяет улучшить эффективность управления и поддержки распределенного парка межсетевых экранов UserGate и устройств сбора и анализа данных LogAn. Количество управляемых устройств, которое можно подключить, ограничено только лицензией.

UGMC поставляется в виде программно-аппаратного комплекса (ПАК, appliance) либо в виде образа виртуальной машины (virtual appliance), предназначенного для развертывания в виртуальной среде.

Управляемые области

Documentation: ☒

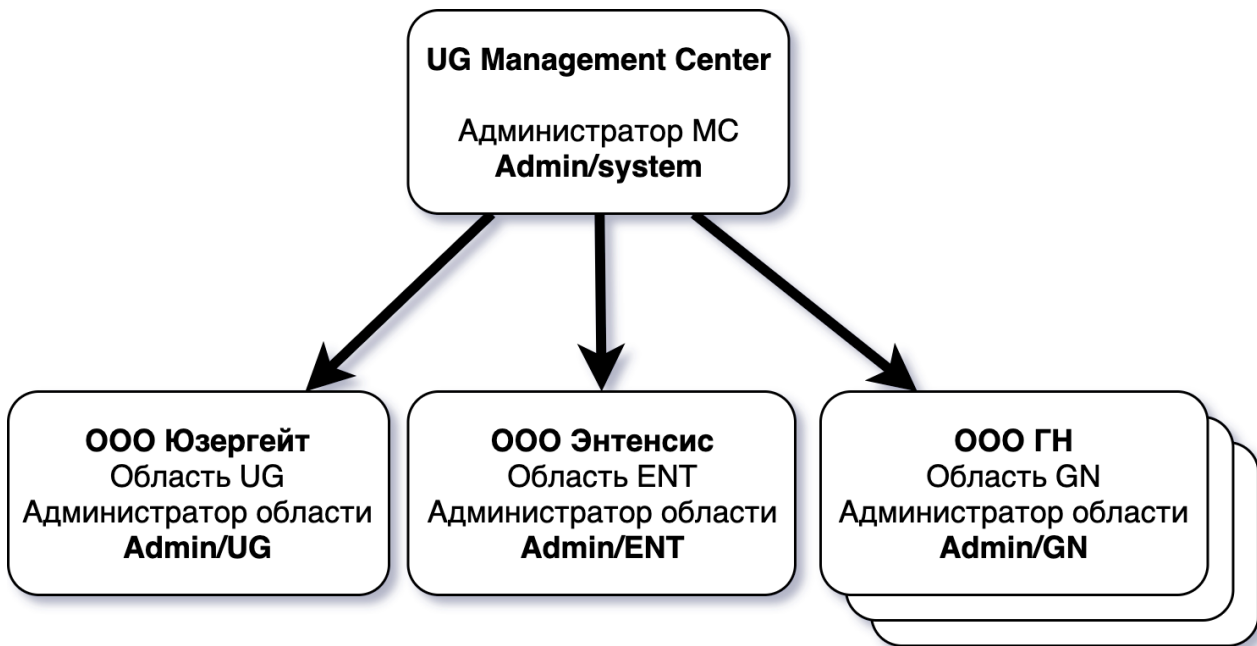
Product: UGMC

Version: 6.1.9, 7.0.1, 7.1.0

UGMC поддерживает облачную модель управления, то есть предоставляет возможность полностью независимого управления устройствами разных предприятий, используя единый сервер управления. Разделение полномочий происходит на уровне управляемых областей.

Управляемая область UserGate — это логический объект, представляющий одно предприятие или группу предприятий, управляемых одним администратором. Каждой области назначается отдельный администратор, который может администрировать только одну назначенную ему область. Администратор одной области не может ни при каких обстоятельствах получить доступ к другой области. Администратор сервера UGMC имеет полномочия создавать управляемые области и назначать в них администраторов, не имея при этом доступа к объектам самой области. Более подробно о разграничении прав администраторов смотрите в главе [Администраторы](#).

Пример UGMC с несколькими управляемыми областями:



Для управления устройствами UserGate одной организации достаточно создать одну управляемую область.

Настройки параметров устройств UserGate производятся внутри управляемой области с помощью шаблонов и групп шаблонов.

Шаблоны и группы шаблонов

Documentation: ☒

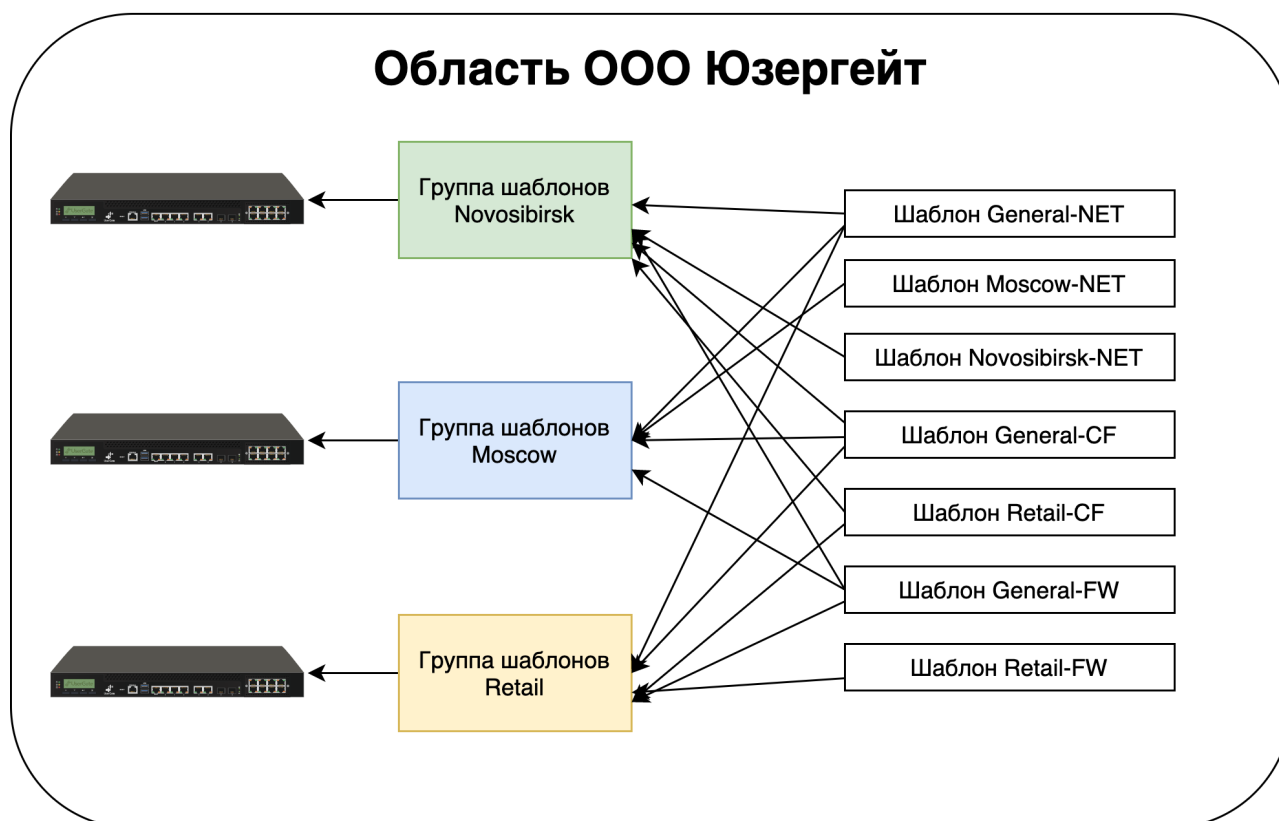
Product: UGMC

Version: 6.1.9, 7.0.1, 7.1.0

С помощью шаблонов и групп шаблонов администратор управляемой области настраивает находящиеся в ней устройства. Шаблон — это базовый блок, с помощью которого настраиваются все параметры работы управляемых устройств, например, межсетевого экрана — сетевые настройки, правила межсетевого экрана, контентной фильтрации, системы обнаружения вторжений и других.

Группы шаблонов объединяют несколько шаблонов в единую конфигурацию, которая применяется к управляемому устройству. Группы упрощают централизованное управление, поскольку позволяют задать базовую конфигурацию для всех типов устройств с помощью одного или нескольких шаблонов, входящих в группу, оставив при этом возможность специфичной настройки каждого устройства UserGate, добавляя специфичные настройки отдельными шаблонами. Результирующие настройки, применяемые к устройству, формируются в результате слияния всех настроек шаблонов, входящих в группу шаблонов, с учетом расположения шаблонов внутри группы. Это позволяет определить группы шаблонов на основе функции географического расположения МЭ (например, Москва, Екатеринбург, Новосибирск и т. п.) или функциональной принадлежности МЭ (например, офис продаж, офис разработки, производство и т. п.).

Пример области с несколькими группами шаблонов для управления МЭ UserGate:



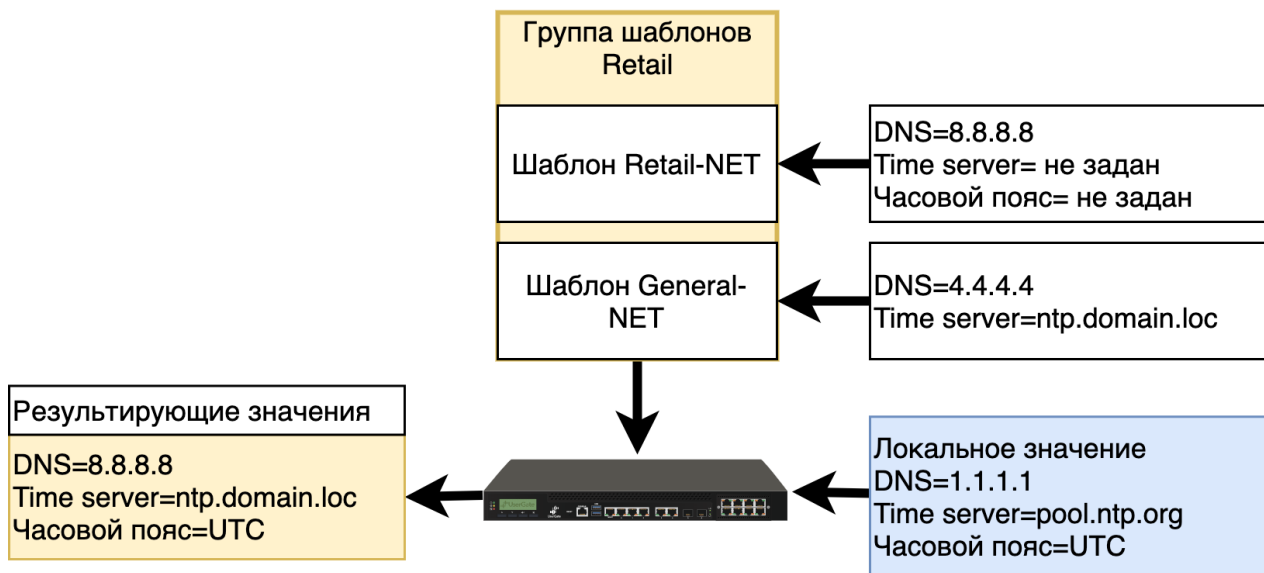
Конфигурация, передаваемая на устройство, может быть двух типов:

- Настройка параметра, например, IP-адрес сервера DNS.
- Правило политики, например, правило межсетевого экрана или контентной фильтрации.

От типа конфигурации зависит способ определения результирующего значения. Правила политики всегда передаются на все устройства, результирующая политика — это набор всех правил, выстроенных в соответствии с их порядком в групповом шаблоне. Правила, указанные в более верхнем шаблоне, помещаются вверх в результирующем списке правил на конечном устройстве.

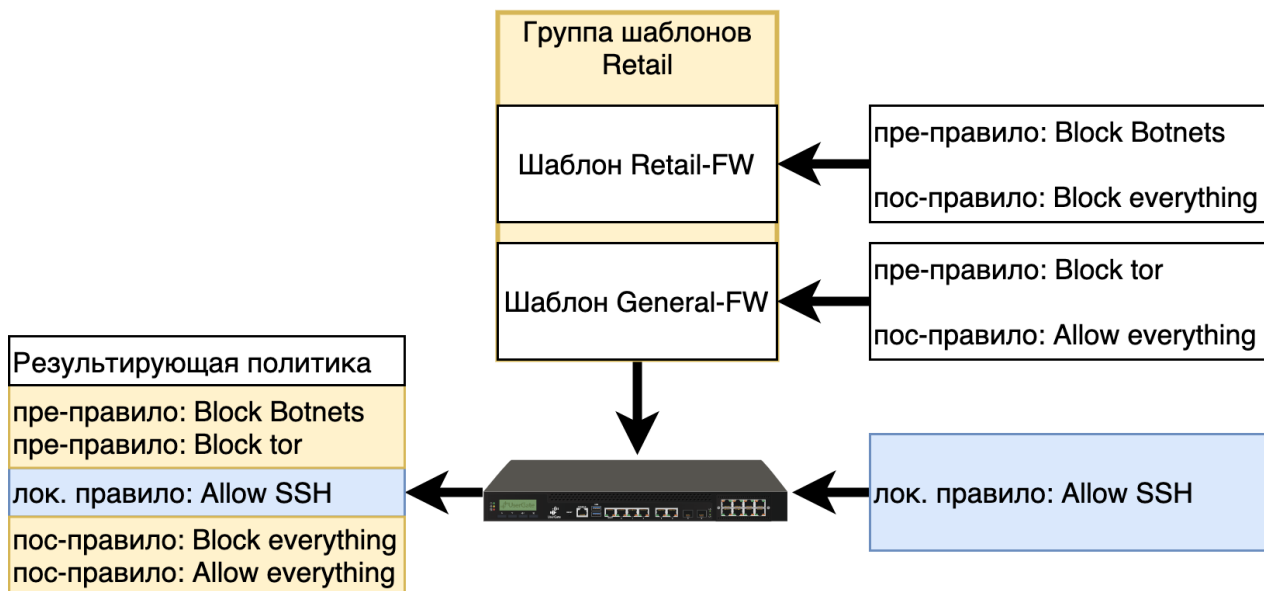
Настройка параметра при конфликтующих значениях в разных шаблонах одной группы шаблонов принимает значение, заданное в наиболее верхнем шаблоне. Локально указанные настройки данного параметра игнорируются.

Пример результирующего значения параметра, определенного в нескольких шаблонах:



Правила, создаваемые в шаблонах, могут быть созданы как пре-правила или пост-правила. Пре- и пост-правила — это местоположение созданного правила относительно правил, создаваемых локальным администратором МЭ UserGate. Пре-правила всегда помещаются выше в списке правил и, следовательно, имеют более высокий приоритет относительно локально созданных правил. Пост-правила всегда помещаются ниже относительно локальных правил и имеют более низкий приоритет. Наличие возможности создавать пре- и пост-правила дает администратору области создавать гибкие настройки политики безопасности, давая локальному администратору больше полномочий (пост-правила), или ограничивая его полномочия (пре-правила).

Пример результирующей политики при наличии пре-, пост- и локальных правил:



Управляемые устройства

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

Группа шаблонов всегда применяется к одному или нескольким устройствам UserGate. NGFW, LogAn являются конечными управляемыми устройствами в терминологии UGMC.

Для совместимости разных версий UGMC и управляемых устройств используются разные версии протокола синхронизации. Для обеспечения возможности управления устройствами NGFW и LogAn из UGMC запрашиваемая управляемыми устройствами версия протокола синхронизации должна быть не выше поддерживаемой UGMC.

Версия МС	Версия NGFW	Версия LogAn
6.x.x	UGMC совместим с устройствами версий 6.x.x. UGMC несовместим с устройствами версий 7.x.x.	Управление LogAn не поддерживается.
7.0.x	UGMC совместим с устройствами версий 6.x.x, 7.0.x. Для NGFW версий 6.x.x версия протокола синхронизации ниже поддерживаемой UGMC. В таком случае UGMC определит возможность конвертирования конфигурации до меньшей версии и, если конвертирование возможно, передаст конфигурацию на конечное устройство. Если конвертация невозможна — в конфигурации присутствуют параметры, отсутствующие в ранних версиях, то будет отображена ошибка синхронизации. Ошибка будет показана для соответствующего устройства в разделе Управление NGFW → Устройства NGFW консоли управления областью. UGMC не совместим с NGFW версий 7.1.x и выше. Причина: версия протокола синхронизации устройства выше версии протокола, поддерживаемой UGMC.	UGMC совместим с устройствами версий 6.x.x, 7.0.x. UGMC несовместим с устройствами версий 7.1.x и выше. Причина: версия протокола синхронизации устройства выше версии протокола, поддерживаемой UGMC.
7.1.x	UGMC совместим с устройствами версий 6.x.x, 7.0.x, 7.1.x. Начиная с версии 7.1.x произошли изменения в конфигурации следующих компонентов: • Система обнаружения и предотвращения вторжений; • Приложения L7; • VPN; • Аутентификация пользователей (добавлен режим аутентификации PKI). UGMC 7.1.x ограниченно поддерживает синхронизацию настроек выше перечисленных разделов при работе с NGFW версий ниже, чем 7.1.x. При синхронизации конфигурации с UGMC 7.1.x на NGFW версий 6.1.x и 7.0.x, ранее подключенных к МС версии ниже: • COB: после обновления UGMC правила COB, полученные от UGMC более ранней версии, станут недоступными для редактирования. • VPN: после обновления UGMC все настройки данного раздела, полученные от UGMC более ранней версии, станут недоступными для редактирования. • Все правила межсетевого экрана, в которых указан профиль приложений/COB, перед синхронизацией будут принудительно выключены (т.е. данные правила будут отображаться в консоли UGMC, но не будут работать). Для NGFW версий 6.x.x и 7.0.x версия протокола синхронизации ниже поддерживаемой UGMC. В таком случае UGMC определит возможность конвертирования конфигурации до меньшей версии и, если конвертирование возможно, передаст конфигурацию на конечное устройство. Если конвертация невозможна — в конфигурации присутствуют параметры, отсутствующие в ранних версиях, то будет отображена ошибка синхронизации. Ошибка будет показана для соответствующего устройства в разделе Управление NGFW → Устройства NGFW консоли управления областью.	UGMC совместим с устройствами версий 7.0.x, 7.1.x. Управление устройствами версий 6.x.x не предусмотрено.

Управление UGMC

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

Управление UGMC делится на управление сервисами самой консоли и управление областями, которые в ней созданы.

Управление сервисами UGMC

Управление сервисами UGMC включает в себя следующие задачи:

Наименование	Описание
Настройка UGMC	• назначение IP-адресов; • конфигурирование зон; • задание DNS-серверов; • создание подключений к серверам LDAP; • настройка оповещений; • создание дополнительных администраторов UGMC с необходимым уровнем полномочий. Все эти настройки влияют только на функционирование самого сервиса UGMC и не влияют на администрирование управляемых областей.
Лицензирование	Лицензирование продукта (ввод ПИН-кода и регистрация продукта), а также опциональное назначение количества управляемых устройств каждой управляемой области. Если ограничения на область не установлены, то любая область может использовать любое количество управляемых устройств, в сумме не превышающих лицензируемое количество. Подробнее о лицензировании смотрите в главе Лицензирование UserGate Management Center .
Создание управляемых областей	Создание управляемых областей. Количество управляемых областей не ограничено.
Создание корневых администраторов управляемых областей	Создание корневых администраторов управляемых областей.

Управление областями UGMC

Управление областями выполняется администратором области и включает в себя следующие задачи:

Наименование	Описание
Создание дополнительных администраторов области	При добавлении управляемой области для неё создается корневой администратор, обладающий всеми полномочиями для управления данной областью. Корневой администратор области может создать дополнительных администраторов и наделить их необходимым уровнем полномочий.
Настройка серверов аутентификации	Создание подключений к серверам LDAP для возможности использования пользователей LDAP в качестве администраторов области.
Создание шаблонов устройств	Создание и настройка шаблонов устройств.
Создание групп шаблонов	Создание групп шаблонов, объединяющих в себя созданные ранее шаблоны.

Наименование	Описание
Добавление управляемых устройств	Добавление управляемых устройств в UGMC и назначение им групп шаблонов.

Ролевое управление

При первоначальной настройке UGMC и создании хотя бы одной управляемой области создаются следующие администраторы:

- **Администратор UGMC.** Как правило это пользователь с именем Admin. Для входа в консоль необходимо указать имя в виде Admin/system, где system означает, что вход осуществляется для управления сервисами UGMC, а не управляемой областью.
- **Корневой администратор созданной области.** Имя пользователя может быть любым, например, Admin. Для входа в консоль необходимо указать имя в виде Admin/realn_code, где realm_code - это код управляемой области.

Администратор UGMC может создать дополнительных администраторов UGMC и наделить их специальными полномочиями (профили администраторов) по управлению сервисами UGMC. При этом администраторы UGMC ограничены только возможностью управления сервисами UGMC (смотрите главу [Настройка UserGate Management Center](#)), не имея доступа к управлению областями. Пример прав доступа администраторов UGMC:

Администратор	Профиль администратора	Уровень доступа
Admin/system	Корневой профиль	Полный. Администратор и его профиль создаются при инициализации сервисов UGMC.
AdminRO/system	ReadOnly	Доступ ко всем сервисам UGMC в режиме просмотра без возможности модификации.
AdminRealm/system	RO+realms	Только создание управляемых областей и их администраторов и просмотр без модификации всех остальных настроек UGMC.
AdminDash/system	Dashboard	Только просмотр показаний раздела Дашборд .

Корневой администратор области может создать дополнительных администраторов в своей области и наделить их специальными полномочиями (профили администраторов). Администраторы области ограничены только возможностью управления своей областью (смотрите главу [Управляемые области](#)), не имея доступа к управлению другими областями или сервисами UGMC. Корневой администратор области может быть только локальным, он не может быть администратором, привязанным к каталогу LDAP. Дополнительные администраторы, созданные корневым администратором области, могут иметь тип локального администратора или администратора, привязанного к каталогу LDAP. Примеры прав доступа администраторов области:

Администратор	Профиль администратора	Уровень доступа
Admin/realm_code	Корневой профиль	Полный. Администратор и его профиль создаются администратором UGMC.
AdminRO/realm_code	ReadOnly	Доступ ко всем настройкам области в режиме просмотра без возможности модификации.
AdminTemplates/realm_code	Templates	Создание и модификация всех шаблонов области.
AdminTemplateGeneral/realm_code	TemplateGeneral	Только модификация шаблона General.
AdminTemplateGeneralNET/realm_code	TemplateGeneralNET	Только модификация сетевых настроек в шаблоне General.

Лицензирование UGMC

Documentation: ☒
Product: UGMC
Version: 6.1.9, 7.0.1

UGMC лицензируется по количеству активных управляемых устройств. При достижении максимального количества добавление нового управляемого устройства станет невозможным. Учитываются только активные управляемые устройства, которые включены в разделе **Управляемые устройства**. При наличии нескольких управляемых областей администратор может выделить необходимое количество лицензируемых устройств на каждую область. Общее количество управляемых устройств во всех областях не может превышать количество лицензируемых устройств.

Лицензия на UGMC дает право бессрочного пользования продуктом.

Дополнительно лицензируются следующие модули:

Наименование	Описание
Модуль Security Update (SU)	Модуль SU дает право на получение: • обновлений ПО UGMC; • обновлений сигнатур системы обнаружения вторжений; • обновление сигнатур приложений L7. Модуль выписывается на 1 год, по истечении данного срока для получения обновлений необходимо продление лицензии.
Модуль Cluster	Модуль включает подписку на работу устройств UserGate в режиме "кластер".

Для регистрации продукта необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Перейти в Дашборд.	Находясь в разделе администрирования консоли, нажать на пиктограмму Дашборд в правом верхнем углу.
Шаг 2. В разделе Лицензия зарегистрировать продукт.	В разделе Лицензия нажать на ссылку Нет лицензии , ввести ПИН-код и заполнить регистрационную форму.

Посмотреть статус установленной лицензии можно, находясь в разделе администрирования консоли в разделе **Дашборд** в виджете **Лицензия**.

Планирование внедрения UGMC

Планирование внедрения UGMC (Описание)

Documentation: ☒

Product: UGMC

Version: 7.0.1, 7.1.0

Развертывание UGMC на предприятии требует тщательного планирования. От того, насколько качественно продумана архитектура шаблонов и групп шаблонов, зависит простота и гибкость применения политик управления на устройства UserGate. UGMC позволяет эффективно применять общие политики, группируя их по географическому, функциональному или смешанному принципам.

При планировании архитектуры рекомендуется:

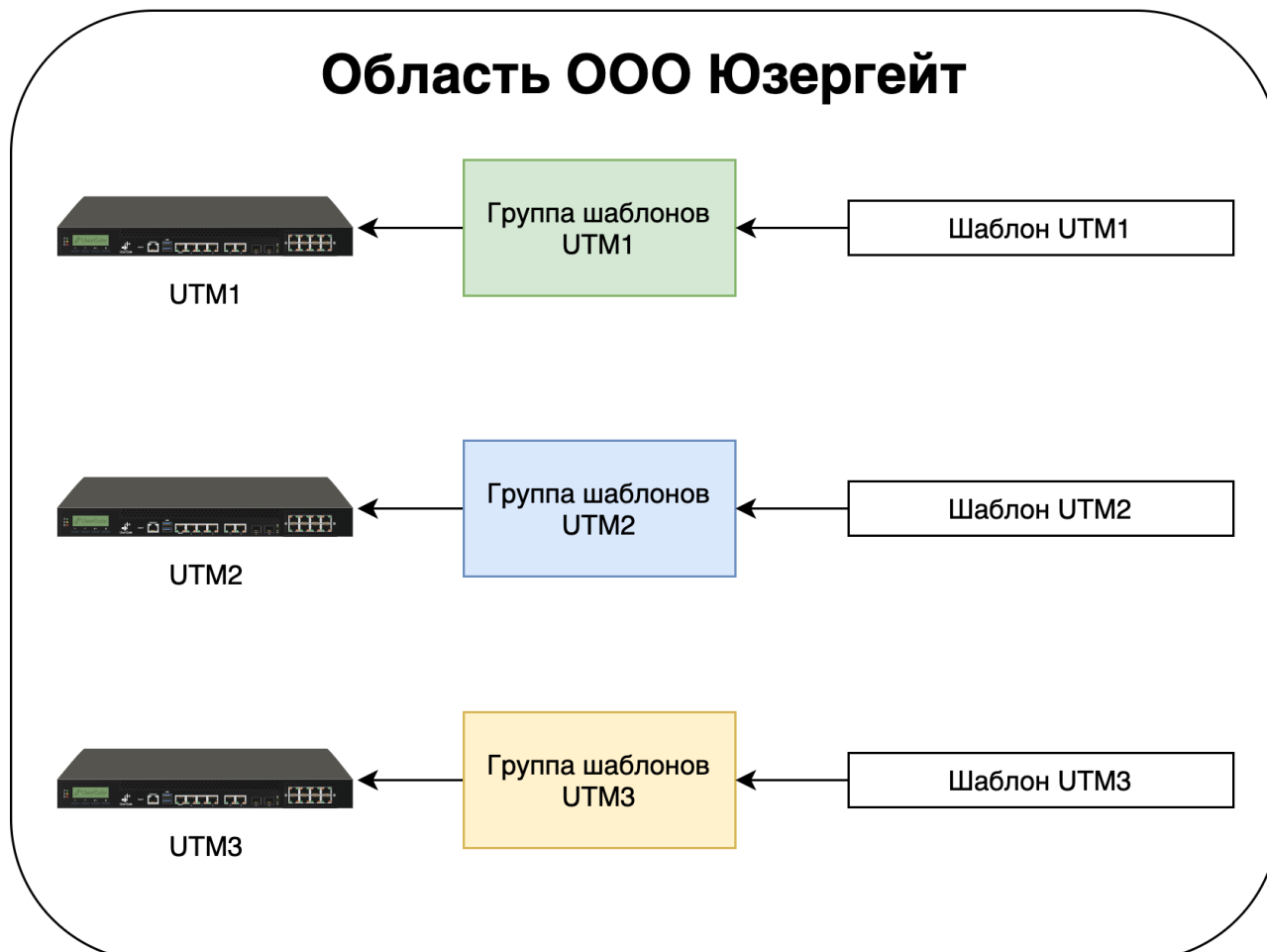
- Избегать конфликта настроек при добавлении шаблонов в группы шаблонов. Наличие конфликтов всегда усложняет управление конечными устройствами. Это основополагающий принцип, из которого вытекают следующие рекомендации.
- Разделять различные группы настроек в разные шаблоны, например, общие настройки управляемых устройств — в одном, политики контентной фильтрации — в другом, политики межсетевого экранирования — в третьем, политики COB — в четвертом и так далее. Разнесение блоков настроек по разным шаблонам позволит избежать конфликта настроек и сделает централизованное управление проще.
- Создавать глобальные настройки в одних шаблонах, а необходимые для некоторых устройств специфические настройки — в других. Например, создать шаблон с правилами контентной фильтрации, применяемый для всех управляемых устройств, и еще один шаблон с правилами контентной фильтрации, применяемый только для группы устройств. Варьируя положение этих двух шаблонов в группах устройств, администратор может выстроить правильный порядок результирующих правил на конечных устройствах. Данная рекомендация допускает контролируемое количество конфликтных настроек.
- Помнить про полномочия локальных администраторов. Если предполагается наличие локальных администраторов, то их полномочия будут ограничены настройками тех параметров, которые не заданы через шаблоны UGMC, а правила, созданные локальными администраторами, всегда помещаются между пре- и пост- правилами, применяемыми из UGMC.

Рассмотрим несколько типичных сценариев внедрения UGMC на примере использования UGMC для управления МЭ UserGate.

Один шаблон и одна группа шаблонов на каждое управляемое устройство

Самый простой вариант развертывания UGMC. К его преимуществам следует отнести простоту и прозрачность настроек, к недостаткам — отсутствие централизованного применения политик — для каждого из устройств придется настраивать свою собственную политику. Настройки сетевых подключений могут производиться как через шаблоны UGMC, так и локальным администратором.

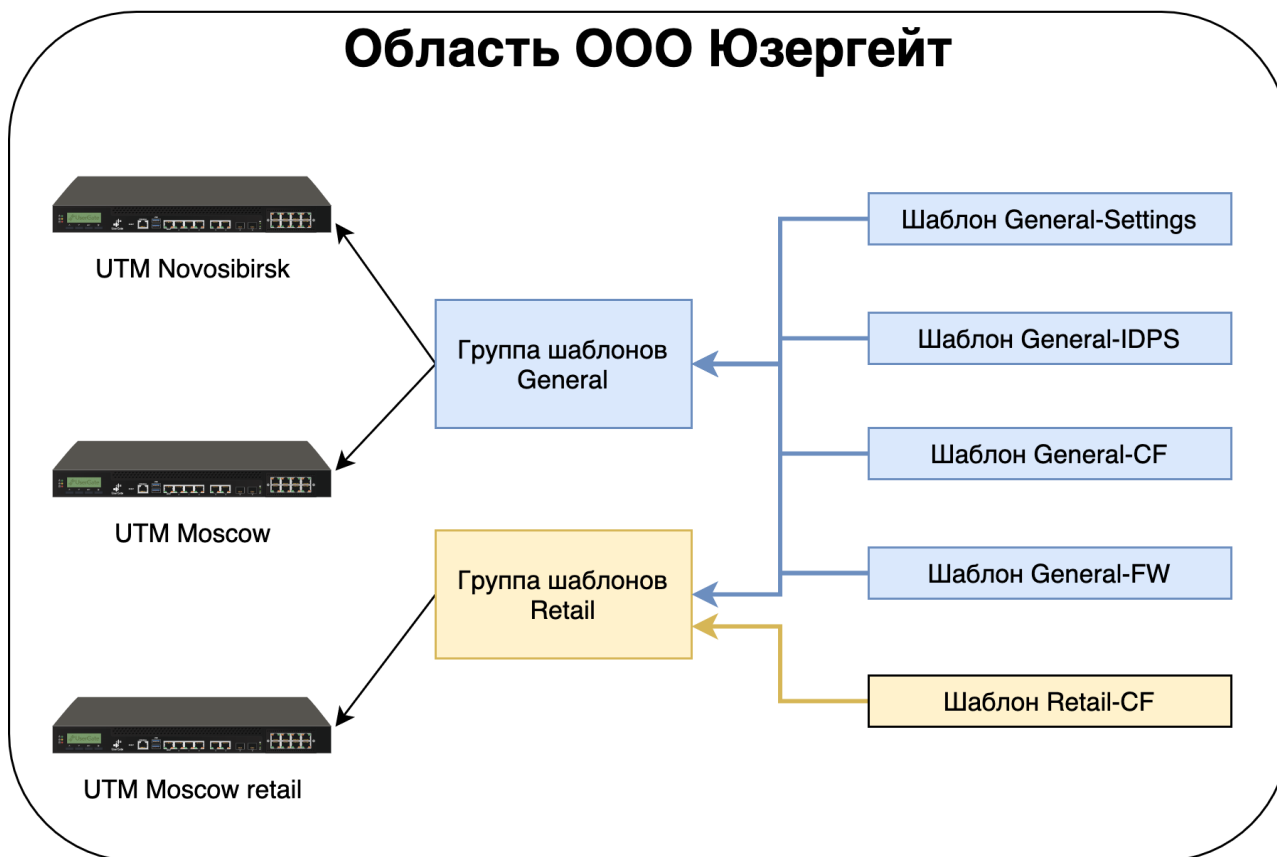
Рекомендуется для простых внедрений с небольшим количеством МЭ UserGate. Пример такой настройки представлен на рисунке ниже.



Набор шаблонов с настройками каждого модуля. Специфичные настройки некоторых модулей для определенной группы управляемых устройств. Сеть настраивается локально

Настройки разбиты по шаблонам, каждый из которых отвечает за настройки специфического модуля, что позволяет избежать конфликта настроек. Суммарно все шаблоны формируют центрально управляемую политику, применяемую ко всем управляемым устройствам в компании. Для специфических управляемых устройств UG, которым необходима специальная политика, добавляются отдельные шаблоны. Сетевые интерфейсы настраиваются локальными администраторами.

Рекомендуется для большинства предприятий. Пример такой настройки представлен на рисунке ниже.



В данном примере шаблоны содержат следующие настройки:

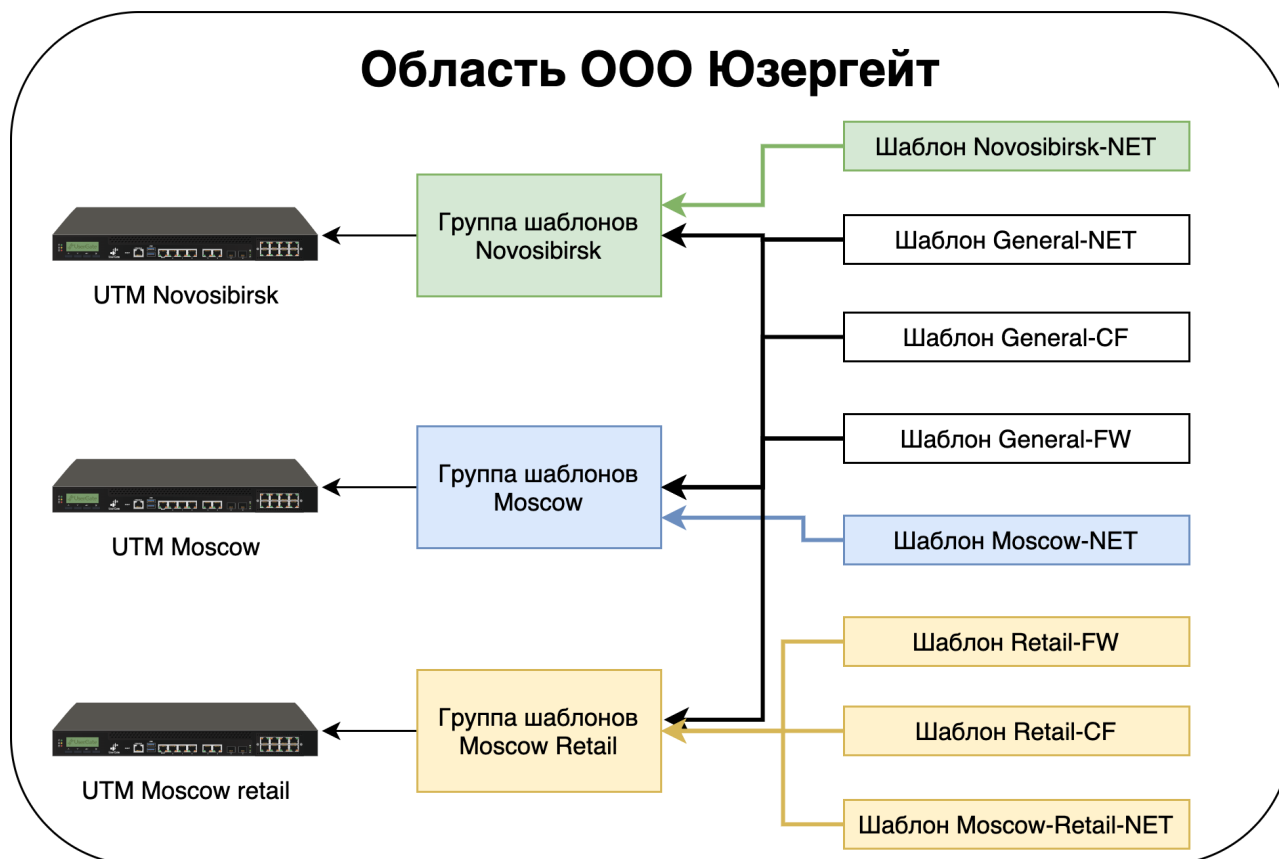
- Шаблон General-Settings — общие для всех настройки (time zone, уровень журналирования, сервера DNS, и т.п.);
- Шаблон General-IDPS — общие для всех политики системы обнаружения вторжений;
- Шаблон General-CF — общие для всех политики контентной фильтрации;
- Шаблон General-FW — общие для всех политики межсетевого экранирования;
- Шаблон Retail-CF — специфичные для ритейловых подразделений политики контентной фильтрации.

Набор шаблонов с настройками каждого модуля. Специфичные настройки некоторых модулей для определенной группы управляемых устройств UG. Сеть настраивается через UGMC

Аналогично предыдущему варианту, но с дополнительным шаблоном сетевых настроек для каждого из МЭ UserGate.

Рекомендуется для большинства предприятий, где необходима централизованная настройка сетевых интерфейсов. Пример такой настройки представлен на рисунке ниже.

Область ООО Юзергейт



В данном примере шаблоны содержат следующие настройки:

- Шаблон General-NET — общие для всех настройки сетевых портов;
- Шаблон General-CF — общие для всех политики контентной фильтрации;
- Шаблон General-FW — общие для всех политики межсетевого экранирования;
- Шаблон Retail-CF — специфичные для ритейловых подразделений политики контентной фильтрации;
- Шаблон Novosibirsk-NET — специфичные для Новосибирского подразделения настройки сетевых портов;
- Шаблон Moscow-NET — специфичные для Московского подразделения настройки сетевых портов;
- Шаблон Moscow-Retail-NET — специфичные для Московского ритейл подразделения настройки сетевых портов.

Примеры шаблонов устройств

UserGate Management Center поставляется с созданной по умолчанию областью (Example realm), которая содержит в себе шаблоны NGFW.

Примечание Область и представленные в ней шаблоны созданы исключительно для удобства пользователей. Элементы могут быть использованы или удалены за ненадобностью.

Для входа в область Example realm используйте созданный по умолчанию профиль администратора области с логином/паролем - ex_admin/Example.

В области представлены следующие шаблоны NGFW:

- **example_content_template**: примеры настройки правил контентной фильтрации;
- **example_firewall_template**: примеры настройки правил межсетевого экранирования;
- **example_settings**: общие настройки UserGate (часовой пояс, язык интерфейса, настройки времени сервера);
- **UserGate Libraries template**: набор зон и элементов библиотек: сервисы, календари, полосы пропускания, шаблоны страниц, категории URL, профили SSL.

Примечание В случае удаления шаблона UserGate Libraries template все элементы, добавленные UserGate по умолчанию, станут недоступными для использования и будут удалены. Рекомендуется не удалять данный шаблон и при настройке политик, связанных с наборами этого шаблона, использовать сам шаблон или его копию.

Первоначальная настройка

Первоначальная настройка

Documentation: ☒
Product: UGMC
Version: 7.0.1, 7.1.0

UGMC поставляется в виде программно-аппаратного комплекса (ПАК, appliance) либо в виде образа виртуальной машины (virtual appliance), предназначенного для развертывания в виртуальной среде. В случае виртуальной машины UGMC поставляется с четырьмя Ethernet-интерфейсами. В случае поставки в виде ПАК UGMC может содержать 8 или более Ethernet-портов.

Развертывание программно-аппаратного комплекса

В случае поставки решения в виде ПАК, программное обеспечение уже загружено и готово к первоначальной настройке. Перейдите к главе [Подключение к UGMC](#) для дальнейшей настройки.

Развертывание виртуального образа

UserGate Management Center Virtual Appliance позволяет быстро развернуть виртуальную машину с уже настроенными компонентами. Образ предоставляется в формате OVF (Open Virtualization Format), который поддерживают такие вендоры как VMWare, Oracle VirtualBox. Для Microsoft Hyper-v и KVM поставляются образы дисков виртуальной машины.

Примечание Для корректной работы виртуальной машины рекомендуется использовать минимум 8 Гб оперативной памяти и 2-ядерный виртуальный процессор. Гипервизор должен поддерживать работу 64-битных операционных систем.

Для начала работы с виртуальным образом, выполните следующие шаги:

Наименование	Описание
Шаг 1. Скачайте образ и распакуйте.	Скачайте последнюю версию виртуального образа с официального сайта https://www.usergate.com/ru .
Шаг 2. Импортируйте образ в свою систему виртуализации.	Инструкцию по импорту образа вы можете посмотреть на сайтах VirtualBox и VMWare. Для Microsoft Hyper-v и KVM необходимо создать виртуальную машину и указать в качестве диска скачанный образ, после чего отключить службы интеграции в настройках созданной виртуальной машины.
Шаг 3. Настройте параметры виртуальной машины.	Увеличьте размер оперативной памяти виртуальной машины. Используя свойства виртуальной машины, установите минимум 8Gb.
Шаг 4. Важно! Увеличьте размер диска виртуальной машины.	Размер диска по умолчанию составляет 100Gb, что обычно недостаточно для хранения всех журналов и настроек. Используя свойства виртуальной машины, установите размер диска в 300Gb или более. Рекомендованный размер - 500Gb или более.
Шаг 5. Настройте виртуальные сети.	UserGate Management Center поставляется с четырьмя интерфейсами, два из которых назначены в зоны: • Management - первый интерфейс виртуальной машины; • Trusted - второй интерфейс виртуальной машины, предназначенный для связи с управляемыми МЭ UserGate.
Шаг 6. Выполните сброс к заводским настройкам.	Запустите виртуальную машину. Во время загрузки выберите Support Menu и выполните Factory reset . Этот шаг крайне важен. Во время этого шага UGMC настраивает сетевые адаптеры и увеличивает размер раздела на жестком диске до размера, указанного в 4-м пункте.

Подключение к UGMC

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

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

Остальные интерфейсы отключены и требуют последующей настройки.

Первоначальная настройка требует выполнения следующих шагов:

Наименование	Описание
Шаг 1. Подключиться к интерфейсу управления.	При наличии DHCP-сервера Подключить интерфейс port0 в сеть предприятия с работающим DHCP-сервером. Включить UGMC. После загрузки консоль UGMC укажет IP-адрес, на который необходимо подключиться для дальнейшей активации продукта. Статический IP-адрес Включить UGMC. Используя CLI (Command Line Interface), назначить необходимый IP-адрес на интерфейс port0. Детали использования CLI смотрите в главе Интерфейс командной строки (CLI). Подключиться к веб-консоли UGMC по указанному адресу, он должен выглядеть примерно следующим образом: https://UGMC_IP_address:8010
Шаг 2. Выбрать язык.	Выбрать язык, на котором будет продолжена первоначальная настройка.
Шаг 3. Задать пароль корневого администратора UserGate Management Center.	Задать логин и пароль для входа в веб-интерфейс управления.
Шаг 4. Зарегистрировать систему.	Ввести ПИН-код для активации продукта и заполнить регистрационную форму. Для активации системы необходим доступ UGMC в интернет. Если на данном этапе выполнить регистрацию не удастся, то ее следует повторить после настройки сетевых интерфейсов на шаге 8.
Шаг 5. Настроить зоны, IP-адреса интерфейсов, подключить UserGate Management Center в сеть предприятия.	В разделе Интерфейсы включить необходимые интерфейсы, установить корректные IP-адреса, соответствующие вашим сетям, и назначить интерфейсы соответствующим зонам. Подробно об управлении интерфейсами читайте в главе Настройка интерфейсов. Система поставляется с предопределенными зонами: • Зона Management (сеть управления), интерфейс port0. • Зона Trusted (LAN). Предполагается, что через эту зону UGMC будет подключаться к управляемым устройствам, а также получит доступ в интернет. Для работы UGMC достаточно одного настроенного интерфейса. Разделение функций управления устройством UGMC и управления управляемыми устройствами UserGate на разные сетевые интерфейсы рекомендовано для обеспечения безопасности, но не является обязательным требованием.
Шаг 6. Настроить шлюз в интернет.	В разделе Шлюзы указать IP-адрес шлюза в интернет на интерфейсе, который имеет доступ в интернет, как правило, это зона Trusted. Подробно о настройке шлюзов в интернет читайте в главе Настройка шлюзов.
Шаг 7. Указать системные DNS-серверы.	В разделе Настройки укажите IP-адреса серверов DNS вашего провайдера или серверов, используемых в вашей организации.
Шаг 8. Зарегистрировать продукт (если не был зарегистрирован на шаге 4).	Зарегистрировать продукт с помощью ПИН-кода. Для успешной регистрации необходимо подключение к интернету и выполнение предыдущих шагов. Более подробно о лицензировании продукта читайте в главе Лицензирование UGMC.
Шаг 9. Создать как минимум одну управляемую область.	В разделе Управляемые области → Области добавить управляемую область.
Шаг 10. Создать администратора созданной управляемой области.	В разделе Администраторы создать профиль администратора и дать ему права на управление созданной областью. Создать администратора с данным профилем.
Шаг 11. Создать дополнительных администраторов UGMC (опционально).	В разделе Администраторы создать необходимые профили для управления сервисами UGMC и создать администраторов UGMC с этими профилями.

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

Офлайн операции с сервером

Офлайн операции с сервером(Описание)

Documentation: ☒
Product: UGMC
Version: 7.0.1, 7.1.0

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

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

Наименование	Описание
UGOS MC	Загрузка UserGate с выводом диагностической информации о загрузке в последовательный порт.
UGOS MC (failsafe)	Загрузка UserGate в упрощённом видеорежиме.
Support menu	Войти в раздел системных утилит с выводом информации в консоль tty1 (монитор).
Restore previous version	Раздел доступен после обновления или создания резервной копии.

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

Наименование	Описание
Check filesystems	Запуск проверки файловой системы устройства на наличие ошибок и их автоматическое исправление.
Expand data partition	Увеличение раздела для хранения данных на весь выделенный диск. Эта операция обычно используется после увеличения дискового пространства, выделенного гипервизором для виртуальной машины UserGate. Данные и настройки UserGate не сбрасываются.
Create backup	Создать полную копию диска UserGate на внешний USB носитель. Все данные на внешнем носителе будут удалены.
Restore from backup	Восстановление UserGate с внешнего USB носителя.
Factory reset	Сброс состояния UserGate к первоначальному состоянию системы. Все данные и настройки будут утеряны.
Exit	Выход и перезагрузка устройства.

Общие настройки

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

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

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

Version: 7.0.1
Product: UGMC
Documentation: ☒

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

- Кластеризация;
- Настройки диагностики;
- Операции с сервером;
- Резервное копирование;
- Экспорт и импорт настроек.

Кластеризация и отказоустойчивость

UGMC поддерживает 2 типа кластеров:

1. **Кластер конфигурации.** Узлы, объединенные в кластер конфигурации, поддерживают единые настройки в рамках кластера.
2. **Кластер отказоустойчивости.** До 4-х узлов кластера конфигурации могут быть объединены в кластер отказоустойчивости, поддерживающий работу в режиме Актив-Актив или Актив-Пассив.

Примечание При внедрении UGMC в режиме отказоустойчивости необходимо выполнить как настройки кластера конфигурации, так и настройки кластера отказоустойчивости.

Ряд настроек уникален для каждого из узлов кластера, например, настройка сетевых интерфейсов и IP-адресация. Список уникальных настроек:

Наименование	Описание
Настройки, уникальные для каждого узла	Настройки диагностики; Настройки интерфейсов; Настройки шлюзов; Маршруты.

Для создания кластера конфигурации необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Выполнить первоначальную настройку на первом узле кластера.	Смотрите главу Первоначальная настройка .
Шаг 2. Настроить на первом узле кластера зону, через интерфейсы которой будет выполняться репликация кластера.	В разделе Зоны создать выделенную зону для репликации настроек кластера. В настройках зоны разрешить следующие сервисы: • Консоль администрирования; • Кластер. Не используйте для репликации зоны, интерфейсы которых подключены к недоверенным сетям, например, к интернету.
Шаг 3. Указать IP-адрес, который будет использоваться для связи с другими узлами кластера.	В разделе Управление устройством в окне Кластер конфигурации выбрать текущий узел кластера и нажать на кнопку Редактировать . Указать IP-адрес интерфейса, входящего в зону, настроенную на шаге 2.
Шаг 4. Сгенерировать Секретный код на первом узле кластера.	В разделе Управление устройством нажать на кнопку Сгенерировать секретный код . Полученный код скопировать в буфер обмена. Данный секретный код необходим для одноразовой авторизации второго узла при добавлении его в кластер.

Наименование	Описание
Шаг 5. Подключить второй узел в кластер.	Второй и последующие узлы подключаются в кластер на моменте первоначальной инициализации. Если инициализация уже была проведена, то необходимо перезагрузить устройство и выполнить возврат к заводским установкам (Factory reset). Подключиться к веб-консоли второго узла кластера, выбрать язык установки. Указать интерфейс, который будет использован для подключения к первому узлу кластера, и назначить ему IP-адрес. Оба узла кластера должны находиться в одной подсети, например, интерфейсам port2 обоих узлов назначены IP-адреса 192.168.100.5/24 и 192.168.100.6/24. В противном случае необходимо указать IP-адрес шлюза, через который будет доступен первый узел кластера. Указать IP-адрес первого узла, настроенный на шаге 3, вставить секретный код и нажать на кнопку Подключить. Если IP-адреса кластера, настроенные на шаге 2, назначены корректно, то второй узел будет добавлен в кластер, и все настройки первого узла кластера реплицируются на второй.
Шаг 6. Назначить зоны интерфейсам второго узла.	В веб-консоли второго узла кластера в разделе Сеть → Интерфейсы необходимо назначить каждому интерфейсу корректную зону. Зоны и их настройки получены в результате репликации данных с первого узла кластера.
Шаг 7. Настроить параметры, индивидуальные для каждого узла кластера (опционально).	Настроить шлюзы, маршруты и другие настройки, индивидуальные для каждого из узлов.

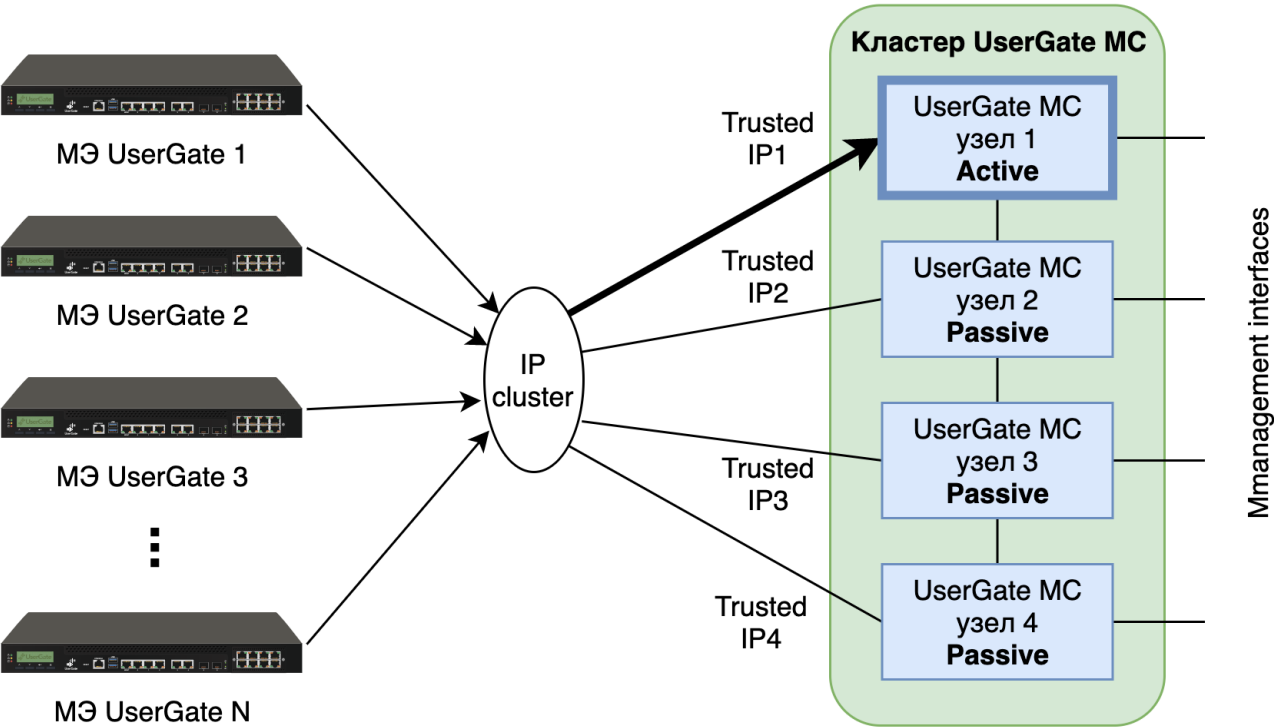
До четырех узлов кластера конфигурации можно объединить в отказоустойчивый кластер. Самих кластеров отказоустойчивости может быть несколько. Поддерживаются 2 режима — **Актив-Актив** и **Актив-Пассив**.

В режиме **Актив-Пассив** один из серверов выступает в роли Мастер-узла, обрабатывающего трафик, а остальные — в качестве резервных. Для кластера указывается один или более виртуальных IP-адресов. Переключение виртуальных адресов с главного на один из запасных узлов происходит при следующих событиях:

- Запасной сервер не получает подтверждения о том, что главный узел в сети, например, если он выключен или отсутствует сетевая доступность узлов.
- На главном узле настроена проверка доступа в интернет.
- Сбой в работе ПО UserGate.

Ниже представлен пример сетевой диаграммы отказоустойчивого кластера в режиме **Актив-Пассив**. Интерфейсы настроены следующим образом:

- **Зона Trusted:** IP1, IP2, IP3, IP4 и IP cluster (Trusted).
- **Зона Management:** интерфейсы в зоне Management используются для управления узлами UGMC.



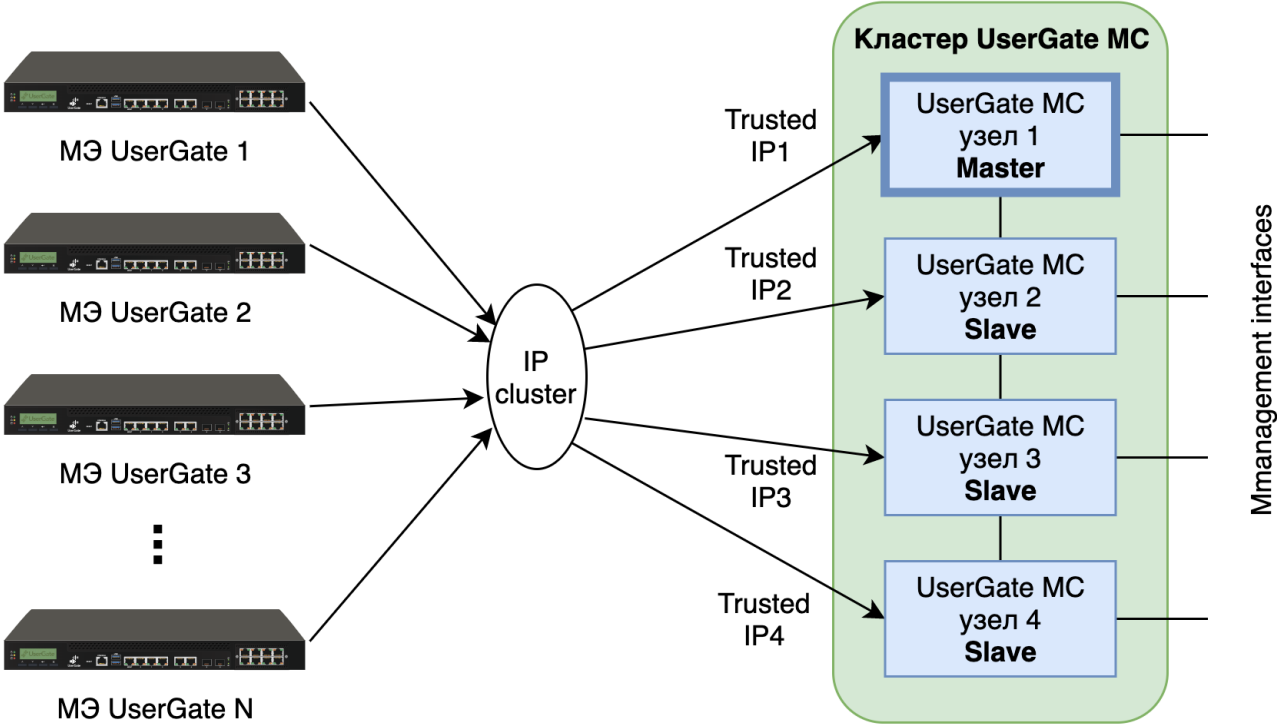
Кластерный IP-адрес находится на узле UGMC 1. Если узел UGMC 1 становится недоступным, то кластерный IP-адрес перейдет на следующий сервер, который станет мастер-сервером, например, UGMC 2.

В режиме **Актив-Актив** один из серверов выступает в роли Мастер-узла, распределяющего трафик на все остальные узлы кластера. Поскольку IP-адрес кластера находится на Мастер-узле, то Мастер-узел отвечает на ARP-запросы клиентов. Выдавая последовательно MAC-адреса всех узлов отказоустойчивого кластера, Мастер-узел обеспечивает равномерное распределение трафика на все узлы кластера, учитывая при этом необходимость неразрывности пользовательских сессий. Для кластера указывается один или более виртуальных IP-адресов. Перемещение роли Мастер-узла на один из запасных узлов происходит при следующих событиях:

- Запасной сервер не получает подтверждения о том, что главный узел в сети, например, если он выключен или отсутствует сетевая доступность узлов.
- На главном узле настроена проверка доступа в интернет.
- Сбой в работе ПО UserGate.

Ниже представлен пример сетевой диаграммы отказоустойчивого кластера в режиме **Актив-Актив**. Интерфейсы настроены следующим образом:

- Зона **Trusted**: IP1, IP2, IP3, IP4 и IP cluster (Trusted).
- Зона **Management**: интерфейсы в зоне Management используются для управления узлами UGMC.



Кластерный IP-адрес находится на узле UGMC 1, который является мастер-узлом. При этом трафик распределяется на все узлы кластера. Если узел UGMC 1 становится недоступным, то роль мастера и кластерный IP-адрес перейдет на следующий сервер, например, UGMC 2.

Для создания отказоустойчивого кластера необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать кластер конфигурации.	Создать кластер конфигурации, как это описано на предыдущем шаге.
Шаг 2. Настроить зоны, интерфейсы которых будут участвовать в отказоустойчивом кластере.	В разделе Зоны следует разрешить сервис VRRP для всех зон, где планируется добавлять кластерный виртуальный IP-адрес (зона Trusted на диаграммах выше).
Шаг 3. Создать кластер отказоустойчивости.	В разделе Управление устройством → Кластер отказоустойчивости нажать на кнопку Добавить и указать параметры кластера отказоустойчивости.

Параметры отказоустойчивого кластера:

Наименование	Описание
Включено	Включение/отключение отказоустойчивого кластера.
Название	Название отказоустойчивого кластера.

Наименование	Описание
Описание	Описание отказоустойчивого кластера.
Режим кластера	Режим отказоустойчивого кластера: • Актив-Актив — нагрузка распределяется на все узлы кластера; • Актив-Пассив — нагрузка идет на Мастер-узел и переключается на запасной узел в случае недоступности Мастер-узла.
Мультикаст идентификатор кластера	В одном кластере конфигурации может быть создано несколько кластеров отказоустойчивости. Для синхронизации сессий используется определенный мультикастовый адрес, определяемый данным параметром. Для каждой группы кластеров отказоустойчивости, в которой должна поддерживаться синхронизация сессий, требуется установить уникальный идентификатор.
Идентификатор виртуального роутера (VRID)	Идентификатор виртуального роутера должен быть уникален для каждого VRRP-кластера в локальной сети. Если в сети не присутствуют сторонние кластеры VRRP, то рекомендуется оставить значение по умолчанию.
Узлы	Выбираются узлы кластера конфигурации для объединения их в кластер отказоустойчивости. Здесь же можно назначить роль Мастер-сервера одному из выбранных узлов.
Виртуальные IP-адреса	Назначаются виртуальные IP-адреса и их соответствие интерфейсам узлов кластера.

Диагностика

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

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

Операции с сервером

Данный раздел позволяет произвести следующие операции с сервером:

Наименование	Описание
--------------	----------

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

Компания UserGate постоянно работает над улучшением качества своего программного обеспечения и предлагает обновления продукта UGMC в рамках подписки на модуль лицензии Security Update (подробно о лицензировании смотрите в разделе [Лицензирование UGMC](#)). При наличии обновлений в разделе **Управление устройством** отобразится соответствующее оповещение. Обновление продукта может занять довольно длительное время, рекомендуется планировать установку обновлений с учетом возможного времени простоя UGMC.

Для установки обновлений необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл резервного копирования.	Создать резервную копию состояния UGMC в разделе Управление устройством → Управление резервным копированием → Создание резервной копии . Данный шаг рекомендуется всегда выполнять перед применением обновлений, поскольку он позволит восстановить предыдущее состояние устройства в случае возникновения каких-либо проблем во время применения обновлений.
Шаг 2. Установить обновления.	В разделе Управление устройством при наличии оповещения Доступны новые обновления нажать на ссылку Установить сейчас . Система установит скачанные обновления, по окончании установки UGMC будет перезагружен.

Управление резервным копированием

Данный раздел позволяет управлять резервным копированием UserGate: настройка правил экспорта конфигурации, создание резервной копии, восстановление устройства UserGate.

Для создания резервной копии необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать резервную копию	В разделе Управление устройством → Управление резервным копированием нажать Создание резервной копии . Система сохранит текущие настройки сервера под следующим именем: backup_PRODUCT_NODE-NAME_DATE.gpg, где <i>PRODUCT</i> — тип продукта: NGFW, LogAn, MC; <i>NODE-NAME</i> — имя узла UserGate; <i>DATE</i> — дата и время создания резервной копии в формате YYYY-MM-DD-HH-MM; время указывается в часовом поясе UTC. Процесс создания резервной копии может быть прерван нажатием кнопки Остановить . Запись о создании резервной копии отобразится в журнале событий устройства.

Для восстановления состояния устройства необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Восстановить состояние устройства	В разделе Управление устройством → Управление резервным копированием нажать Восстановление из резервной копии и указать путь к ранее созданному файлу настроек для его загрузки на сервер. Восстановление будет предложено в консоли tty при перезагрузке устройства.

Дополнительно администратор может настроить сохранение файлов на внешние серверы (FTP, SSH) по расписанию. Для создания расписания выгрузки настроек необходимо выполнить следующие действия:

Наименование	Описание

Наименование	Описание
Шаг 1. Создать правило экспорта конфигурации	В разделе Управление устройством → Управление резервным копированием нажать кнопку Добавить , указать имя и описание правила.
Шаг 2. Указать параметры удаленного сервера	Во вкладке правила Удаленный сервер указать параметры удаленного сервера: • Тип сервера — FTP или SSH; • Адрес сервера — IP-адрес сервера; • Порт — порт сервера; • Логин — учетная запись на удаленном сервере; • Пароль/Повторите пароль — пароль учетной записи; • Путь на сервере — путь на сервере, куда будут выгружены настройки. В случае использования SSH-сервера возможно использование авторизации по ключу. Для импорта или генерации ключа необходимо выбрать Настроить SSH-ключ и указать Сгенерировать ключи или Импортировать ключ. Важно! При повторном создании ключа существующий SSH-ключ будет удален. Публичный ключ должен находиться на SSH-сервере в директории пользовательских ключей <code>/home/user/.ssh/</code> в файле <code>authorized_keys</code>. При первоначальной настройке правила экспорта резервного копирования по SSH обязательна проверка соединения (кнопка Проверить соединение); при проверке соединения fingerprint помещается в <code>known_hosts</code>, без проверки файлы не будут отправляться. Важно! Если сменить сервер SSH или его переустановить, то файлы резервного копирования будут недоступны, так как fingerprint изменится — это защита от спуфинга.
Шаг 3. Выбрать расписание выгрузки	Во вкладке правила Расписание указать необходимое время отправки настроек. В случае задания времени в crontab-формате, задайте его в следующем виде: (минуты:0-59) (часы:0-23) (дни месяца:1-31) (месяц:1-12) (день недели:0-6, 0-воскресенье) Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего); • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7; • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23" • Звездочка и тире используются для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

Экспорт и импорт настроек

Администратор имеет возможность сохранить текущие настройки UGMC в файл и впоследствии восстановить эти настройки на этом же или другом сервере UGMC. В отличие от резервного копирования, экспорт/импорт настроек не сохраняет текущее состояние всех компонентов комплекса, сохраняются только текущие настройки.

Примечание Экспорт/импорт настроек не восстанавливает состояние интерфейсов и информацию о лицензии. После окончания процедуры импорта необходимо настроить интерфейсы и повторно зарегистрировать UGMC с помощью имеющегося ПИН-кода.

Для экспорта настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Экспорт настроек.	В разделе Управление устройством → Экспорт и импорт настроек нажать на ссылку Экспорт и выбрать Экспортировать все настройки или Экспортировать сетевые настройки. Система сохранит: • текущие настройки сервера под именем: <code>cc_core-mc_core@nodename_version_YYYYMMDD_HHMMSS.bin</code> • сетевые настройки под именем: <code>network-cc_core-mc_core@nodename_version_YYYYMMDD_HHMMSS.bin</code> nodename — имя узла UserGate Management Center. version — версия UserGate Management Center. YYYYMMDD_HHMMSS — дата и время выгрузки настроек в часовом поясе UTC. Например, <code>cc_core-mc_core@ediasaionedi_7.0.0.93R-1_20220715_084853.bin</code> или <code>network-cc_core-mc_core@ediasaionedi_7.0.0.93R-1_20220715_084929.bin</code>.

Для применения созданных ранее настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Импорт настроек.	В разделе Управление устройством → Экспорт и импорт настроек нажать на ссылку Импорт и указать путь к ранее созданному файлу настроек. Указанные настройки применятся к серверу, после чего сервер будет перезагружен

Примечание Для корректного импорта правил, использующих обновляемые списки UserGate (приложения, категории URL и т.п.), необходимо наличие лицензии на модули SU и ATP, а также загруженных списков UserGate.

Дополнительно администратор может настроить сохранение настроек на внешние серверы (FTP, SSH) по расписанию. Для создания расписания выгрузки настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать правило экспорта.	В разделе Управление устройством → Экспорт настроек нажать кнопку Добавить , указать имя и описание правила
Шаг 2. Указать параметры удаленного сервера.	Во вкладке правила Удаленный сервер указать параметры удаленного сервера: • Тип сервера — FTP или SSH; • Адрес сервера — IP-адрес сервера; • Порт — порт сервера; • Логин — учетная запись на удаленном сервере; • Пароль/Подтверждение пароля — пароль учетной записи; • Путь на сервере — путь на сервере, куда будут выгружены настройки.
Шаг 3. Выбрать расписание выгрузки.	Во вкладке правила Расписание указать необходимое время отправки настроек. В случае задания времени в CRONTAB-формате, задайте его в следующем виде: (минуты:0-59) (часы:0-23) (дни месяца:1-31) (месяц:1-12) (день недели:0-6, 0-воскресенье) Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего); • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7; • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23"; • Звездочка и тире используются для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "<u>*/2</u>" в поле "часы" будет означать "каждые два часа".

Администраторы

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

Доступ к веб-консоли UGMC регулируется с помощью создания дополнительных учетных записей администраторов, назначения им профилей доступа, создания политики управления паролями администраторов и настройки доступа к веб-консоли на уровне разрешения сервиса в свойствах зоны сети.

Примечание При первоначальной настройке UGMC создается локальный суперпользователь Admin/system.

Для создания дополнительных учетных записей администраторов устройства необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать профиль доступа администратора.	В разделе Администраторы → Профили администраторов нажать кнопку Добавить и указать необходимые настройки.
Шаг 2. Создать учетную запись администратора и назначить ей один из созданных ранее профилей администратора.	В разделе Администраторы нажать кнопку Добавить и выбрать необходимый вариант: • Добавить локального администратора — создать локального пользователя, задать ему пароль доступа и назначить созданный ранее профиль доступа. • Добавить пользователя LDAP — добавить пользователя из существующего домена. Для этого должен быть корректно настроен LDAP-коннектор в разделе Серверы аутентификации. При входе в консоль администрирования необходимо указывать имя пользователя в формате user@domain/system или domain\user/system. Назначить созданный ранее профиль. • Добавить группу LDAP — добавить группу пользователей из существующего домена. Для этого должен быть корректно настроен LDAP-коннектор в разделе Серверы аутентификации. При входе в консоль администрирования необходимо указывать имя пользователя в формате user@domain/system или domain\user/system. Назначить созданный ранее профиль. • Добавить администратора с профилем аутентификации — создать пользователя, назначить созданный ранее профиль администратора и профиль аутентификации (необходимы корректно настроенные серверы аутентификации). Важно! В данном разделе настроек сервисов консоли управления администратором области может быть назначен только локальный администратор. Это связано с тем, что LDAP серверы, используемые для аутентификации администраторов сервиса UGMC и для аутентификации администраторов области, могут быть разными. При необходимости использования LDAP администраторов для управления Областью, их необходимо создать в самой области. Более подробно об администраторах области смотрите в разделе Администраторы области.

При создании профиля доступа администратора необходимо указать следующие параметры:

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

Администратор UGMC может настроить дополнительные параметры защиты учетных записей администраторов, такие как сложность пароля

и блокировку учетной записи на определенное время при превышении количества неудачных попыток аутентификации.

Для настройки этих параметров необходимо:

Наименование	Описание
Шаг 1. Настроить политику паролей.	В разделе Администраторы → Администраторы нажать кнопку Настроить .
Шаг 2. Заполнить необходимые поля.	Указать значения следующих полей: • Сложный пароль — включает дополнительные параметры сложности пароля, задаваемые ниже, такие как минимальная длина, минимальное число символов в верхнем регистре, минимальное число символов в нижнем регистре, минимальное число цифр, минимальное число специальных символов, максимальная длина блока из одного и того же символа. • Число неверных попыток аутентификации — количество неудачных попыток аутентификации администратора, после которых учетная запись заблокируется на Время блокировки. • Время блокировки — время, на которое блокируется учетная запись.

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

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

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

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

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

Управление сертификатами

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

UGMC использует защищенный протокол HTTPS для управления устройством. Для выполнения данной функции UGMC использует сертификат типа **SSL веб-консоли**.

Для того чтобы создать новый сертификат, необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать сертификат.	Нажать на кнопку Создать в разделе Сертификаты
Шаг 2. Заполнить необходимые поля.	Указать значения следующих полей: • Название — название сертификата, под которым он будет отображен в списке сертификатов. • Описание — описание сертификата. • Страна — страна, в которой выписывается сертификат. • Область или штат — область или штат, в котором выписывается сертификат • Город — город, в котором выписывается сертификат. • Название организации — название организации, для которой выписывается сертификат. • Common name — имя сертификата. Рекомендуется использовать только символы латинского алфавита для совместимости с большинством браузеров. • E-mail — email вашей компании
Шаг 3. Указать, для чего будет использован данный сертификат.	После создания сертификата необходимо указать его роль в UGMC. Для этого необходимо выделить необходимый сертификат в списке сертификатов, нажать на кнопку Редактировать и указать тип сертификата - SSL веб-консоли. После этого UGMC перезагрузит сервис веб-консоли и предложит вам подключиться уже с использованием нового сертификата.

UGMC позволяет экспортировать созданные сертификаты и импортировать сертификаты, созданные на других системах, например, сертификат, выписанный доверенным удостоверяющим центром вашей организации.

Для экспорта сертификата необходимо:

Наименование	Описание
Шаг 1. Выбрать сертификат для экспорта.	Выделить необходимый сертификат в списке сертификатов.
Шаг 2. Экспортировать сертификат.	Выбрать тип экспорта: • Экспорт сертификата — экспортирует данные сертификата в der-формате без экспортирования приватного ключа сертификата. • Экспорт CSR — экспортирует CSR сертификата, например, для подписи его удостоверяющим центром.

ПримечаниеРекомендуется сохранять сертификат для возможности его последующего восстановления.

ПримечаниеВ целях безопасности UGMC не разрешает экспорт приватных ключей сертификатов.

Для импорта сертификата необходимо иметь файлы сертификата и - опционально - приватного ключа сертификата и выполнить следующие действия:

Наименование	Описание
Шаг 1. Начать импорт.	Нажать на кнопку Импорт .

Наименование	Описание
Шаг 2. Заполнить необходимые поля.	Указать значения следующих полей: • Название — название сертификата, под которым он будет отображен в списке сертификатов. • Описание — описание сертификата. • Загрузите файл, содержащий данные сертификата. • Загрузите файл, содержащий приватный ключ сертификата. • Пароль для приватного ключа, если таковой требуется. • Цепочка сертификатов — файл, содержащий сертификаты вышестоящих центров сертификации, которые участвовали в создании сертификата. Необязательное поле.

Серверы аутентификации UGMC

Version: 7.0.1, 7.1.0
Product: UGMC
Documentation: ☒

Серверы аутентификации — это внешние источники учетных записей пользователей для авторизации в веб-консоли управления UGMC. UGMC поддерживает следующие серверы аутентификации: LDAP-коннектор, RADIUS и TACACS+.

LDAP-коннектор

LDAP-коннектор позволяет:

- Получать информацию о пользователях и группах Active Directory или других LDAP-серверов. Поддерживается работа с LDAP-сервером FreeIPA.
- Осуществлять авторизацию администраторов UGMC через домены Active Directory/FreeIPA.

Для создания LDAP-коннектора необходимо нажать на кнопку **Добавить**, выбрать **Добавить LDAP-коннектор** и указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данного сервера аутентификации.
Название	Название сервера аутентификации.
SSL	Определяет, требуется ли SSL-соединение для подключения к LDAP-серверу.
Доменное имя LDAP или IP-адрес	IP-адрес контроллера домена, FQDN контроллера домена или FQDN домена (например, test.local). Если указан FQDN, то UserGate получит адрес контроллера домена с помощью DNS-запроса. Если указан FQDN домена, то при отключении основного контроллера домена, UserGate будет использовать резервный.
Bind DN («login»)	Имя пользователя, которое необходимо использовать для подключения к серверу LDAP. Имя необходимо использовать в формате DOMAIN\username или username@domain. Данный пользователь уже должен быть заведен в домене
Пароль	Пароль пользователя для подключения к домену.
Домены LDAP	Список доменов, которые обслуживаются указанным контроллером домена, например, в случае дерева доменов или леса доменов Active Directory. Здесь же можно указать короткое netbios имя домена.
Пути поиска	Список путей в сервере LDAP, начиная с которых система будет осуществлять поиск пользователей и групп. Необходимо указывать полное имя, например, ou=Office,dc=example,dc=com.

После создания сервера необходимо проверить корректность параметров, нажав на кнопку **Проверить соединение**. Если параметры указаны верно, система сообщит об этом либо укажет на причину невозможности соединения.

Настройка LDAP-коннектора завершена. Для входа в консоль пользователям LDAP необходимо указывать имя в формате:

`domain\user/system` или `user@domain/system`

Сервер аутентификации RADIUS

Сервер аутентификации RADIUS позволяет производить авторизацию пользователей в веб-консоли UserGate, который выступает в роли RADIUS-клиента. При авторизации через RADIUS-сервер UserGate посылает на серверы RADIUS информацию с именем и паролем пользователя, а RADIUS-сервер отвечает, успешно прошла аутентификация или нет.

Для добавления сервера аутентификации RADIUS необходимо нажать **Добавить**, выбрать **Добавить RADIUS-сервер** и указать следующие параметры:

Наименование	Описание
Включено	Включение/отключение использования данного сервера аутентификации.

Наименование	Описание
Название	Название сервера аутентификации RADIUS.
Описание	Описание сервера (опционально).
Секрет	Общий ключ, используемый протоколом RADIUS для аутентификации.
Адреса	Указание IP-адреса сервера и UDP-порта, на котором сервер RADIUS слушает запросы на аутентификацию (по умолчанию, 1812).

Для авторизации пользователей в веб-интерфейсе UserGate с помощью сервера RADIUS необходимо настроить профиль аутентификации. Подробнее о создании и настройке профилей читайте в разделе [Профили аутентификации UGMC](#).

Сервер аутентификации TACACS+

Сервер TACACS+ позволяет производить авторизацию пользователей в консоли администрирования UserGate. При использовании сервера UserGate передаёт на серверы аутентификации информацию с именем и паролем пользователя, после чего серверы TACACS+ отвечают, успешно прошла аутентификация или нет.

Для добавления сервера аутентификации TACACS+ необходимо нажать **Добавить**, выбрать **Добавить TACACS+ сервер** и указать следующие параметры:

Наименование	Описание
Включено	Включение/отключение использования данного сервера аутентификации.
Название	Название сервера аутентификации TACACS+.
Описание	Описание сервера (опционально).
Секретный ключ	Общий ключ, используемый протоколом TACACS+ для аутентификации.
Адрес	IP-адрес сервера TACACS+.
Порт	UDP-порт, на котором сервер TACACS+ слушает запросы на аутентификацию.
Использовать одно TCP-соединение	Использовать одно TCP-соединение для работы с сервером TACACS+.
Таймаут (сек)	Время ожидания сервера TACACS+ для получения аутентификации. По умолчанию 4 секунды.

Для авторизации пользователей в веб-интерфейсе UserGate с помощью сервера TACACS+ необходимо настроить профиль аутентификации. Подробнее о создании и настройке профилей читайте в разделе [Профили аутентификации UGMC](#).

Профили аутентификации UGMC

Documentation: ☒
Version: 7.0.1, 7.1.0
Product: UGMC

Профиль позволяет определить набор способов авторизации пользователей в консоли администрирования UserGate. При создании или настройке профиля достаточно указать:

Наименование	Описание
Название	Название профиля аутентификации.
Описание	Описание профиля (опционально).
Методы аутентификации	Методы аутентификации пользователей, настроенные ранее: LDAP-коннектор, серверы аутентификации RADIUS, TACACS+.

Почтовые адреса

Элемент библиотеки **Почтовые адреса** позволяет создать группы почтовых адресов, которые впоследствии можно использовать в правилах оповещения.

Для добавления новой группы почтовых адресов необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать группу почтовых адресов.	В панели Группы почтовых адресов нажать на кнопку Добавить , дать название группе.
Шаг 2. Добавить почтовые адреса в группу.	Выделить созданную группу и в панели Почтовые адреса нажать на кнопку Добавить и добавить необходимые почтовые адреса.

Администратор имеет возможность создавать списки почтовых адресов и централизованно распространять их на все компьютеры с установленным UserGate. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми списком почтовых адресов.	Создать файл list.txt со списком почтовых 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.

Наименование	Описание
Шаг 5. Создать список почтовых адресов и указать URL для обновления.	На каждом UserGate создать список 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".

Номера телефонов

Элемент библиотеки **Номера телефонов** позволяет создать группы номеров, которые впоследствии можно использовать в правилах оповещения SMPP.

Для добавления новой группы телефонных номеров необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать группу телефонных номеров.	В панели Группы телефонных номеров нажать на кнопку Добавить , дать название группе.
Шаг 2. Добавить номера телефонов в группу.	Выделить созданную группу и в панели Группа телефонных номеров нажать на кнопку Добавить и добавить необходимые номера.

Администратор имеет возможность создавать списки телефонных номеров и централизованно распространять их на все компьютеры с установленным UserGate. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми списком номеров.	Создать файл list.txt со списком номеров.
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 телефонных номеров и указать URL для обновления.	На каждом UserGate создать список номеров. 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 "*" в поле "часы" будет означать "каждые два часа".

Профили оповещений

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

- SMTP, доставка сообщений с помощью email.
- SMPP, доставка сообщений с помощью SMS практически через любого оператора сотовой связи или через большое количество SMS-центров рассылки.

Для создания профиля сообщений SMTP необходимо нажать на кнопку **Добавить** в разделе **Профили оповещений**, выбрать вариант **Добавить профиль оповещения SMTP** и заполнить необходимые поля:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Хост	IP-адрес сервера SMTP, который будет использоваться для отсылки почтовых сообщений.
Порт	Порт TCP, используемый сервером SMTP. Обычно для протокола SMTP используется порт 25, для SMTP с использованием SSL — 465. Уточните данное значение у администратора почтового сервера.
Безопасность	Варианты безопасности отправки почты, возможны варианты: Нет, STARTTLS, SSL.
Аутентификация	Включает аутентификацию при подключении к SMTP-серверу.
Логин	Имя учетной записи для подключения к SMTP-серверу.
Пароль	Пароль учетной записи для подключения к SMTP-серверу.

Для создания профиля сообщений SMPP необходимо нажать на кнопку **Добавить** в разделе **Профили оповещений**, выбрать вариант **Добавить профиль оповещения SMPP** и заполнить необходимые поля:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Хост	IP-адрес сервера SMPP, который будет использоваться для отсылки SMS сообщений.
Порт	Порт TCP, используемый сервером SMPP. Обычно для протокола SMPP используется порт 2775, для SMPP с использованием SSL — 3550.
SSL	Использовать или нет шифрацию с помощью SSL.
Логин	Имя учетной записи для подключения к SMPP-серверу.
Пароль	Пароль учетной записи для подключения к SMPP-серверу.
Правила трансляции номеров	В некоторых случаях SMPP-провайдер ожидает номер телефона в определенном формате, например, в виде 89123456789. Для соответствия требованиям провайдера можно указать замену первых символов номеров с одних на другие. Например, заменить все номера, начинающиеся на +7, на 8.

Расширение системного раздела

Version: 7.0.1, 7.1.0
Product: NGFW, UGMC, LogAn, SIEM
Documentation: ☒

Для расширения системного раздела с сохранением конфигурации и данных узла UserGate необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Добавить дополнительный виртуальный диск.	Средствами гипервизора добавить новый диск необходимого размера в свойствах виртуальной машины UserGate.
Шаг 2. Расширить размер раздела в системных утилитах.	В меню загрузки узла UserGate войти в раздел Support menu . В открывшемся разделе выбрать Expand data partition и запустить процесс расширения раздела.
Шаг 3. Проверить размер системного раздела.	После завершения процесса расширения загрузить узел и в разделе Дашборд → Диски проверить размер системного раздела.

Настройка сети(Описание)

Documentation: ☒
Product: UGMC
Version: 7.0.1, 7.1.0

В данном разделе описаны сетевые настройки UGMC.

Настройка зон

Зона в UGMC — это логическое объединение сетевых интерфейсов. Политики безопасности UGMC используют зоны интерфейсов, а не непосредственно интерфейсы.

Рекомендуется объединять интерфейсы в зоне на основе их функционального назначения, например, зона LAN-интерфейсов, зона интернет-интерфейсов, зона интерфейсов управления.

По умолчанию UGMC поставляется со следующими зонами:

Наименование	Описание
Management	Зона для подключения доверенных сетей, из которых разрешено управление UGMC.
Trusted	Зона для подключения управляемых устройств и получения доступ в сеть интернет.

Для работы UGMC достаточно одного настроенного интерфейса. Разделение функций управления устройством UGMC и управления УУ UserGate на разные сетевые интерфейсы рекомендовано для обеспечения безопасности, но не является жестким требованием.

Администраторы UGMC могут изменять настройки зон, созданных по умолчанию, а также создавать дополнительные зоны.

ПримечаниеМожно создать не более 255 зон.

Для создания зоны необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать зону.	Нажать на кнопку Добавить и дать название зоне.
Шаг 2. Настроить параметры защиты зоны от DoS (опционально).	Указать параметры защиты зоны от сетевого флуда для протоколов TCP (SYN-flood), UDP, ICMP: Порог уведомления — при превышении количества запросов с одного IP-адреса над указанным значением происходит запись события в системный журнал. Порог отбрасывания пакетов — при превышении количества запросов с одного IP-адреса над указанным значением UGMC начинает отбрасывать пакеты, поступившие с этого IP-адреса, и записывает данное событие в системный журнал. Рекомендованные значения для порога уведомления — 300 запросов в секунду, для порога отбрасывания пакетов — 600 запросов в секунду. Исключения защиты от DoS — позволяет указать список IP-адресов серверов, которые необходимо исключить из защиты. Это может быть полезно, например, для шлюзов UserGate, которые могут слать большой объем данных на сервера LogAn.

Наименование	Описание
Шаг 3. Настроить параметры контроля доступа зоны (опционально).	Указать предоставляемые UGMC сервисы, которые будут доступны клиентам, подключенным к данной зоне. Для зон, подключенных к неконтролируемым сетям, таким, как интернет, рекомендуется отключить все сервисы. Сервисы: • Ping — позволяет пинговать UGMC. • SNMP — доступ к UserGate по протоколу SNMP (UDP 161). • Консоль администрирования — доступ к веб-консоли управления (TCP 8010 и 8300). • XML-RPC для управления — позволяет управлять продуктом по API (TCP 4041). • VRRP — сервис, необходимый для объединения нескольких NGFW в отказоустойчивый кластер (IP протокол 112). • Кластер — сервис, необходимый для объединения нескольких NGFW в кластер (TCP 4369, TCP 9000-9100). • CLI по SSH — доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200. • Сервис UserGate Management Center — сервис подключения NGFW и LogAn (TCP 2022, 9712). Подробнее о требованиях сетевой доступности читайте в Приложение 1. Требования к сетевому окружению.
Шаг 4. Настроить параметры защиты от IP-спуфинг атак (опционально).	Атаки на основе IP-спуфинга позволяют передать пакет из одной сети, например, из Trusted, в другую, например, в Management. Для этого атакующий подменяет IP-адрес источника на предполагаемый адрес необходимой сети. В таком случае ответы на этот пакет будут пересылаться на внутренний адрес. Для защиты от подобных атак администратор может указать диапазоны IP-адресов, адреса источников которых допустимы в выбранной зоне. Сетевые пакеты с адресами источников, отличными от указанных, будут отброшены. С помощью чекбокса Инвертировать администратор может указать адреса источников, которые не могут быть получены на интерфейсах данной зоны. В этом случае будут отброшены пакеты с указанными диапазонами IP-адресов источников. Например, можно указать диапазоны "серых" IP-адресов 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 и включить опцию Инвертировать.

Настройка интерфейсов

Раздел **Интерфейсы** отображает все физические и виртуальные интерфейсы, имеющиеся в системе, позволяет менять их настройки и добавлять VLAN и бонд-интерфейсы.

Кнопка **Редактировать** позволяет изменять параметры сетевого интерфейса:

- Включить или отключить интерфейс.
- Указать тип интерфейса — Layer 3.
- Назначить зону интерфейсу.
- Изменить физические параметры интерфейса — MAC-адрес и размер MTU.
- Выбрать тип присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP.

Кнопка **Добавить** позволяет добавить следующие типы логических интерфейсов:

- VLAN.
- Бонд.

Объединение интерфейсов в бонд

С помощью кнопки **Добавить бонд-интерфейс** администратор может объединить несколько физических интерфейсов в один логический агрегированный интерфейс для повышения пропускной способности или для отказоустойчивости канала. При создании бонда необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает бонд.
Название	Название бонда.
Зона	Зона, к которой принадлежит бонд.

Наименование	Описание
Интерфейсы	Один или более интерфейсов, которые будут использованы для построения бонда.
Режим	Режим работы бонда должен совпадать с режимом работы на том устройстве, куда подключается бонд. Может быть: • Round robin. Пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. Эта политика применяется для балансировки нагрузки и отказоустойчивости. • Active backup. Только один сетевой интерфейс из объединенных будет активным. Другой интерфейс может стать активным только в том случае, когда упадет текущий активный интерфейс. При такой политике MAC-адрес бонд-интерфейса виден снаружи только через один сетевой порт, во избежание появления проблем с коммутатором. Эта политика применяется для отказоустойчивости. • XOR. Передача распределяется между сетевыми картами используя формулу: [(«MAC-адрес источника» XOR «MAC-адрес назначения») по модулю «число интерфейсов»]. Получается, одна и та же сетевая карта передает пакеты одним и тем же получателям. Опционально распределение передачи может быть основано и на политике «xmit_hash». Политика XOR применяется для балансировки нагрузки и отказоустойчивости. • Broadcast. Передает все на все сетевые интерфейсы. Эта политика применяется для отказоустойчивости. • IEEE 802.3ad — режим работы, установленный по умолчанию, поддерживается большинством сетевых коммутаторов. Создаются агрегированные группы сетевых карт с одинаковой скоростью и дуплексом. При таком объединении передача задействует все каналы в активной агрегации согласно стандарту IEEE 802.3ad. Выбор, через какой интерфейс отправлять пакет, определяется политикой; по умолчанию используется XOR-политика, можно также использовать «xmit_hash» политику. • Adaptive transmit load balancing. Исходящий трафик распределяется в зависимости от загруженности каждой сетевой карты (определяется скоростью загрузки). Не требует дополнительной настройки на коммутаторе. Входящий трафик приходит на текущую сетевую карту. Если она выходит из строя, то другая сетевая карта берет себе MAC-адрес вышедшей из строя карты. • Adaptive load balancing. Включает в себя предыдущую политику плюс осуществляет балансировку входящего трафика. Не требует дополнительной настройки на коммутаторе. Балансировка входящего трафика достигается путем ARP-переговоров. Драйвер перехватывает ARP-ответы, отправляемые с локальных сетевых карт наружу, и переписывает MAC-адрес источника на один из уникальных MAC-адресов сетевой карты, участвующей в объединении. Таким образом, различные пиры используют различные MAC-адреса сервера. Балансировка входящего трафика распределяется последовательно (round-robin) между интерфейсами.
MII monitoring period (мсек)	Устанавливает периодичность MII-мониторинга в миллисекундах. Определяет, как часто будет проверяться состояние линии на наличие отказов. Значение по умолчанию — 0 — отключает MII-мониторинг.
Down delay (мсек)	Определяет время (в миллисекундах) задержки перед отключением интерфейса, если произошел сбой соединения. Эта опция действительна только для мониторинга MII (miimon). Значение параметра должно быть кратным значениям miimon. Если оно не кратно, то округлится до ближайшего кратного значения. Значение по умолчанию 0.
Up delay (мсек)	Задаёт время задержки в миллисекундах, перед тем как поднять канал при обнаружении его восстановления. Этот параметр возможен только при MII-мониторинге (miimon). Значение параметра должно быть кратным значениям miimon. Если оно не кратно, то округлится до ближайшего кратного значения. Значение по умолчанию 0.
LACP rate	Определяет, с каким интервалом будут передаваться партнером LACPDU-пакеты в режиме 802.3ad. Возможные значения: • Slow — запрос партнера на передачу LACPDU-пакетов каждые 30 секунд. • Fast — запрос партнера на передачу LACPDU-пакетов каждую 1 секунду.
Failover MAC	Определяет, как будут прописываться MAC-адреса на объединенных интерфейсах в режиме active-backup при переключении интерфейсов. Обычным поведением является одинаковый MAC-адрес на всех интерфейсах. Возможные значения: • Отключено — устанавливает одинаковый MAC-адрес на всех интерфейсах во время переключения. • Active — MAC-адрес на бонд-интерфейсе будет всегда таким же, как на текущем активном интерфейсе. MAC-адреса на резервных интерфейсах не изменяются. MAC-адрес на бонд-интерфейсе меняется во время обработки отказа. • Follow — MAC-адрес на бонд-интерфейсе будет таким же, как на первом интерфейсе, добавленном в объединение. На втором и последующем интерфейсе этот MAC не устанавливается, пока они в резервном режиме. MAC-адрес прописывается во время обработки отказа, когда резервный интерфейс становится активным, он принимает новый MAC (тот, что на бонд-интерфейсе), а старому активному интерфейсу прописывается MAC, который был на текущем активном.

Наименование	Описание
Xmit hash policy	Определяет хэш-политику передачи пакетов через объединенные интерфейсы в режиме XOR или IEEE 802.3ad. Возможные значения: Layer 2 — использует только MAC-адреса для генерации хэша. При этом алгоритме трафик для конкретного сетевого хоста будет отправляться всегда через один и тот же интерфейс. Алгоритм совместим с IEEE 802.3ad. Layer 2+3 — использует как MAC-адреса, так и IP-адреса для генерации хэша. Алгоритм совместим с IEEE 802.3ad. Layer 3+4 — используются IP-адреса и протоколы транспортного уровня (TCP или UDP) для генерации хэша. Алгоритм не всегда совместим с IEEE 802.3ad, так как в пределах одного и того же TCP- или UDP-взаимодействия могут передаваться как фрагментированные, так и нефрагментированные пакеты. Во фрагментированных пакетах порт источника и порт назначения отсутствуют. В результате в рамках одной сессии пакеты могут дойти до получателя не в том порядке, так как отправляются через разные интерфейсы.
Сеть	Способ присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP.

Настройка шлюзов

Для подключения UGMC к интернету необходимо указать IP-адрес одного или нескольких шлюзов.

Можно указать несколько шлюзов, если для подключения к интернету используется несколько провайдеров. Пример настройки сети с двумя провайдерами:

- Интерфейс port1 с IP-адресом 192.168.11.2 подключен к интернет-провайдеру 1. Для выхода в интернет с этого провайдера необходимо добавить шлюз с IP-адресом 192.168.11.1
- Интерфейс port2 с IP-адресом 192.168.12.2 подключен к интернет-провайдеру 2. Для выхода в интернет с этого провайдера необходимо добавить шлюз с IP-адресом 192.168.12.1

При наличии двух или более шлюзов возможны 2 варианта работы:

Наименование	Описание
Балансировка трафика между шлюзами	Установить флажок Балансировка и указать Вес каждого шлюза. В этом случае весь трафик в интернет будет распределен между шлюзами в соответствии с указанными весами (чем больше вес, тем большая доля трафика идет через шлюз).
Основной шлюз с переключением на запасной	Выбрать один из шлюзов в качестве основного и настроить Проверку сети , нажав на одноименную кнопку в интерфейсе. Проверка сети проверяет доступность хоста в интернет с указанной в настройках периодичностью, и в случае, если хост перестает быть доступен, переводит весь трафик на запасные шлюзы в порядке их расположения в консоли.

По умолчанию проверка доступности сети настроена на работу с публичным DNS-сервером Google (8.8.8.8), но может быть изменена на любой другой хост по желанию администратора.

Маршруты

Данный раздел позволяет указать маршрут в сеть, доступную за определенным маршрутизатором. Например, в локальной сети может быть маршрутизатор, который объединяет несколько IP-подсетей.

Для добавления маршрута необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Задать название и описание данного маршрута.	В разделе Сеть выберите в меню Маршруты , нажмите кнопку Добавить . Укажите имя для данного маршрута. Опционально можно задать описание маршрута.
Шаг 2. Указать адрес назначения.	Задайте подсеть, куда будет указывать маршрут, например, 172.16.20.0/24 или 172.16.20.5/32.
Шаг 3. Указать шлюз.	Задайте IP-адрес шлюза, через который указанная подсеть будет доступна. Этот IP-адрес должен быть доступен с сервера UGMC.
Шаг 4. Указать интерфейс.	Выберите интерфейс, через который будет добавлен маршрут. Если оставить значение Автоматически , то UGMC сам определит интерфейс, исходя из настроек IP-адресации сетевых интерфейсов.

Наименование	Описание
Шаг 5. Указать метрику.	Задайте метрику маршрута. Чем меньше метрика, тем приоритетней маршрут, если маршрутов несколько в данную сеть несколько.

Интерфейс командной строки (CLI)

Интерфейс командной строки (CLI) Описание

Documentation: ☒
Product: UGMC
Version: 7.0.1, 7.1.0

UGMC позволяет создавать базовые настройки устройства с помощью интерфейса командной строки, CLI (Command Line Interface). С помощью CLI администратор может выполнить ряд диагностирующих команд, таких как ping, nslookup, traceroute, осуществить настройку сетевых интерфейсов и зон, а также перезагрузить или выключить устройство.

CLI полезно использовать для диагностики сетевых проблем или в случае, когда доступ к веб-консоли утерян, например, некорректно указан IP-адрес интерфейса или ошибочно установлены параметры контроля доступа для зоны, запрещающие подключение к веб-интерфейсу.

Подключение к CLI можно выполнить через стандартные порты VGA/клавиатуры (при наличии таких портов на оборудовании UGMC), через последовательный порт или с помощью SSH по сети.

Для подключения к CLI с использованием монитора и клавиатуры необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Подключить монитор и клавиатуру к UGMC	Подключить монитор к разъему VGA(HDMI), клавиатуру к разъему USB.
Шаг 2. Войти в CLI	Войти в CLI, используя имя и пароль пользователя с правами корневого администратора UGMC (по умолчанию Admin/system). Если устройство UGMC не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin/system, в качестве пароля - utm.

Для подключения к CLI с использованием последовательного порта необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Подключиться к UserGate Management Center	Используя специальный кабель для последовательного порта или переходник USB-Serial, подключить свой компьютер к UGMC.
Шаг 2. Запустить терминал	Запустить терминал, позволяющий подключение через последовательный порт, например, Putty для Windows или minicom для Linux. Установить подключение через последовательный порт, указав параметры подключения 115200 8n1.
Шаг 3. Войти в CLI	Войти в CLI, используя имя и пароль пользователя с правами корневого администратора UGMC (по умолчанию Admin/system). Если устройство UGMC не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin/system, в качестве пароля - utm.

Для подключения к CLI по сети с использованием протокола SSH необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Разрешить доступ к CLI (SSH) для выбранной зоны	Разрешить доступ для протокола CLI по SSH в настройках зоны, к которой вы собираетесь подключаться для управления с помощью CLI. Будет открыт порт TCP 2200.
Шаг 2. Запустить SSH-терминал	Запустить у себя на компьютере SSH-терминал, например, SSH для Linux или Putty для Windows. Указать в качестве адреса адрес UGMC, в качестве порта подключения - 2200, в качестве имени пользователя - имя пользователя правами корневого администратора UGMC (по умолчанию Admin/system). Для Linux команда на подключение должна выглядеть так: <code>ssh Admin/system@IPUserGateMC -p 2200</code>

Наименование	Описание
Шаг 3. Войти в CLI	Войти в CLI, используя пароль пользователя, указанного на предыдущем шаге. Если устройство UGMC не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin/system, в качестве пароля - utm.

После успешного входа в CLI можно посмотреть список возможных команд с помощью команды **help**. Для подробного описания любой команды необходимо использовать синтаксис

help command

Например, для получения подробной справки по использованию команды настройки сетевого интерфейса iface необходимо выполнить

help iface

Полный список команд:

Наименование	Описание
help	Показывает список доступных команд.
exit quit Ctrl+D	Выйти из CLI.
date	Посмотреть текущее время на сервере.
gateway	Посмотреть или задать значения шлюза. Смотрите gateway help для детальной информации.
iface	Набор команд для просмотра и настройки параметров сетевого интерфейса. Смотрите iface help для детальной информации.
license	Посмотреть информацию о лицензии.
netcheck	Проверить доступность стороннего HTTP/HTTPS-сервера. netcheck [-t TIMEOUT] [-d] URL Опции: -t - максимальный таймаут ожидания ответа от веб-сервера -d - запросить содержание сайта. По умолчанию запрашиваются только заголовки.
nslookup	Выполнить определение IP-адреса по имени хоста.
ping	Выполнить ping определенного хоста.
radmin	Включить или отключить удаленный доступ к серверу для технической поддержки UserGate.
radmin_e	Включить или отключить удаленный доступ к серверу для технической поддержки UserGate, в случаях, когда сервер UGMC завис.
reboot	Перезагрузить сервер UserGate Management Center.
route	Создать, изменить, удалить маршрут.
shutdown	Выключить сервер UGMC.
traceroute	Выполнить трассировку соединения до определенного хоста.

Наименование	Описание
zone	Набор команд для просмотра и настройки параметров зоны. Смотрите zone help для детальной информации.

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

Мониторинг маршрутов

Раздел **Маршруты** позволяет получить список всех маршрутов, указанных на определенном узле UserGate. Для просмотра маршрутов необходимо нажать на кнопку **Фильтр** и указать типы маршрутов, которые необходимо отобразить. Возможно указать следующие типы маршрутов:

- **Подключенные к интерфейсам** — маршруты к сетям, которые подключены непосредственно к интерфейсам UserGate. Данные маршруты будут помечены символом **С** в списке маршрутов.
- **Заданные статически** — маршруты, заданные статически в разделе **Сеть → Маршруты**. Данные маршруты будут помечены символом **К** в списке маршрутов.
- **OSPF** — маршруты, полученные по протоколу OSPF. Данные маршруты будут помечены символом **О** в списке маршрутов.
- **BGP** — маршруты, полученные по протоколу BGP. Данные маршруты будут помечены символом **В** в списке маршрутов.
- **RIP** — маршруты, полученные по протоколу RIP. Данные маршруты будут помечены символом **Р** в списке маршрутов.

Отображаемый список маршрутов можно скачать в виде текстового файла с помощью кнопки **Скачать все маршруты**.

Ping

С помощью утилиты ping можно диагностировать доступность сетевых ресурсов. Параметры команды ping:

Наименование	Описание
Ping host	Хост, который необходимо проверить.
TTL	Максимальное количество промежуточных хостов, которое разрешено пройти на пути к проверяемому хосту.
Интерфейс	Адрес выбранного интерфейса будет использоваться в качестве адреса источника для выполнения ping, а интерфейс отправки пакета будет выбран согласно таблице маршрутизации.
Счетчик	Количество повторов.
Показывать временные метки	Добавляет временные метки в вывод команды.
Не резолвить имена	Оперировать IP-адресами, не преобразовывая их в доменные имена.

Traceroute

С помощью утилиты traceroute можно проверить путь следования сетевых пакетов к определенному хосту. Параметры команды traceroute:

Наименование	Описание
Traceroute host	Хост, который необходимо проверить.
Использовать ICMP	Использовать протокол ICMP для выполнения команды traceroute. Если не указано, то используется протокол UDP.
Интерфейс	Сетевой интерфейс, с которого необходимо выполнять команду.
Не разрешать доменные имена	Оперировать IP-адресами, не преобразовывая их в доменные имена.

Запрос DNS

Используя запрос DNS, администратор может проверить работу DNS-серверов.

Наименование	Описание
DNS-запрос (хост)	DNS имя для проверки.
IP источника запроса	Один из IP-адресов, назначенных UserGate.
DNS сервер	Адрес DNS-сервера, на который будет отправлен запрос.
Порт	UDP порт, используемый для запроса.
Тип DNS-запроса	Тип запроса.

Оповещения

Правила оповещений

Данный раздел позволяет определить правила оповещений, которые в дальнейшем можно использовать для отсылки оповещений о различных типах событий, например, высокой загрузке CPU или недоступности сервера. Для создания правила оповещений необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать один или несколько профилей оповещения.	Смотрите раздел Профили оповещений .
Шаг 2. Создать группы получателей оповещений.	Смотрите разделы Почтовые адреса и Номера телефонов .
Шаг 3. Создать правило оповещения.	В разделе Оповещения → Правила оповещений добавить правило.

При добавлении правила необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает данное правило.
Название	Название правила.
Описание	Описание правила.
Профиль оповещения	Созданный ранее профиль оповещения. Для профилей SMPP появится закладка для указания адресатов в виде телефонных номеров, для SMTP появится закладка для указания адресатов в виде email-адресов.
От	От кого будет приходить оповещение.
Тема	Тема оповещения.
Таймаут перед повторной отправкой, секунд	Укажите таймаут, в течение которого сервер не будет отправлять сообщение при повторном срабатывании данного правила. Данная настройка позволяет предотвратить шторм сообщений при частом срабатывании правила оповещения.
События	Укажите события, для которых необходимо получать оповещения.
Телефоны	Для SMPP-профиля. Укажите группы номеров телефонов, куда отправлять SMS-оповещения.

Наименование	Описание
Emails	Для SMTP-профиля. Укажите группы адресов email, на которые будут отправляться почтовые оповещения.

SNMP

UserGate поддерживает мониторинг с помощью протоколов SNMP v2c и SNMP v3. Поддерживается управление как с помощью запросов (SNMP queries), так и с помощью отсылки оповещений (SNMP traps). Это позволяет наблюдать за критическими параметрами UserGate с помощью программного обеспечения SMNP-управления, используемого в компании.

Для настройки мониторинга с помощью SNMP необходимо:

1. В свойствах зоны интерфейса, к которому будет осуществляться подключение по протоколу SNMP, во вкладке **Контроль доступа** разрешить сервис **SNMP**.
2. Создать правило SNMP.

Для настройки мониторинга с помощью SNMP необходимо создать правила SNMP. Для создания правила SNMP необходимо в разделе **SNMP** нажать на кнопку **Добавить** и указать следующие параметры:

Наименование	Описание
Название	Название правила.
Описание	Описание правила SNMP (опционально).
IP-адрес сервера для трапов	IP-адрес сервера для трапов и порт, на котором сервер слушает оповещения. Обычно это порт UDP 162. Данная настройка необходима только в случае, если необходимо отправлять трапы на сервер оповещений.
Community	SNMP community — строка для идентификации сервера UserGate и сервера управления SNMP для версии SNMP v2c. Используйте только латинские буквы и цифры.
Контекст	Необязательный параметр, определяющий SNMP context. Можно использовать только латинские буквы и цифры. На некоторых устройствах может быть несколько копий полного поддерева MIB. Например, на устройстве может быть создано несколько виртуальных маршрутизаторов. Каждый такой виртуальный маршрутизатор будет иметь полное поддерево MIB. В этом случае каждый виртуальный маршрутизатор может быть указан как контекст на сервере SNMP. Контекст определяется по имени. Когда клиент отправляет запрос, он может указать имя контекста. Если имя контекста не указано, будет запрошен контекст по умолчанию.
Версия	Указывает версию протокола SNMP, которая будет использоваться в данном правиле. Возможны варианты SNMPv2c и SNMPv3.
Разрешить SNMP-запросы	При включении разрешает получение и обработку SNMP-запросов от SNMP-менеджера.
Разрешить SNMP-трапы	При включении разрешает отправку SNMP-трапов на сервер, настроенный для приема оповещений.
Пользователь	Только для SNMP v3. Имя пользователя для аутентификации SNMP-менеджера.
Тип аутентификации	Выбор режима аутентификации SNMP-менеджера. Возможны варианты: • Без аутентификации, без шифрования (noAuthNoPriv). • С аутентификацией, без шифрования (authNoPriv). • С аутентификацией, с шифрованием (authPriv). Наиболее безопасным считается режим работы authPriv.
Алгоритм аутентификации	Алгоритм, используемый для аутентификации.

Наименование	Описание
Пароль аутентификации	Пароль, используемый для аутентификации.
Алгоритм шифрования	Алгоритм, используемый для шифрования. Возможно использовать DES и AES.
Пароль шифрования	Пароль, используемый для шифрования.
События	Выбор типов параметров, доступных для мониторинга по правилу.

Примечание Настройки аутентификации для SNMP v2c (community) и для SNMP v3 (пользователь, тип аутентификации, алгоритм аутентификации, пароль аутентификации, алгоритм шифрования, пароль шифрования) на SNMP-менеджере должны совпадать с настройками SNMP в UserGate.

Информацию по настройке параметров аутентификации для вашего SNMP-менеджера смотрите в руководстве по настройке выбранного вами программного обеспечения для управления SNMP.

Кнопка **Скачать MIB** позволяет скачать MIB-файлы с параметрами мониторинга UserGate для последующего использования их в SNMP-менеджере. UserGate выделен уникальный идентификатор **SNMP PEN** (Private Enterprise Number) **45741**.

Для скачивания доступны следующие MIB-файлы:

- UTM-TRAPS-MIB.
- UTM-TRAPS-BINDINGS-MIB.
- UTM-MIB.
- UTM-INTERFACES-MIB.

UTM-TRAPS-MIB

Наименование	Описание
trapCoreCrush	Сбой ядра.
trapStatDown	Сервис статистики (UserGate Log Analyzer) недоступен.
trapCoreBootstrapEnd	Загрузка сервера завершена успешно.
trapDefaultGatewayChanged	Изменение шлюза по умолчанию.
trapHighSessionsCounter	Таблица сессий заполнена на 90%.
trapHighUsersCounter	Количество активных пользователей достигло 90% от порога лицензии.
trapStatusChanged	Изменение статуса узла отказоустойчивого кластера.
trapMemberUp	Статус узла отказоустойчивого кластера изменился на «Подключен».
trapMemberDown	Узел отказоустойчивого кластера отключен.
trapAttackDetected	Обнаружена атака COB.
trapChecksumFailed	Нарушение целостности бинарных файлов.
trapHighCPUUsage	Высокая загрузка центрального процессора.

Наименование	Описание
trapLowMemory	Высокая загрузка памяти.
trapLowLogdiskSpace	Недостаточно места на диске для хранения журналов.
trapRaidStatus	Изменение статуса RAID.
trapPowerSupply	Первый источник питания отключен.
trapCableStatus	Кабель был подключен или отключен от интерфейса.
trapTrafficDrop	Срабатывание запрещающего правила межсетевого экрана.
trapLDAPServerDown	Сервер LDAP недоступен.

UTM-TRAPS-BINDINGS-MIB

Наименование	Тип данных	Описание
utmSessions	integer	Текущее количество активных сессий.
utmSessionsMax	integer	Максимальное количество активных сессий.
utmUsers	Integer	Количество активных пользователей на данный момент.
utmUsersMax	integer	Максимальное количество активных пользователей.
utmHASstatus	integer	Текущий статус узла кластера отказоустойчивости: • 0 — master-узел. • 1 — slave-узел. • 3 — fault.
utmHASstatusReason	integer	Причина изменения статуса узла отказоустойчивого кластера: • 1 — связь с узлом потеряна. • 2 — HTTP прокси-сервер недоступен. • 3 — ни один из шлюзов недоступен. • 4 — DNS-сервер недоступен. • 5 — узел UserGate Management Center недоступен.
utmCPUUsage	integer	Загруженность центрального процессора; отображается в %.
utmMemory	integer	Использование оперативной памяти; отображается в %.
utmLogdiskSpace	integer	Пространство на диске, используемое под журналы; отображается в %.

Наименование	Тип данных	Описание
utmAdaptecRaidStatus	integer	Текущий статус RAID (Redundant Array of Independent Disks), построенного на контроллере Adaptec: • no_raid. • 0 — optimal — массив в оптимальном состоянии. • 1 — degraded — полный или частичный выход из строя одного из дисков. • 2 — rebuild — восстановление массива.
utmBroadcomRaidStatus	integer	Текущий статус RAID (Redundant Array of Independent Disks), построенного на контроллере Broadcom: • no_raid. • 0 — optimal — массив в оптимальном состоянии. • 1 — degraded — полный или частичный выход из строя одного из дисков. Переход в данный статус произойдёт при выходе из строя 2-х дисков. • 2 — partialDegraded — полный или частичный выход из строя одного из дисков. • 3 — failed — не работает из-за наличия ошибки. • 4 — offline — диск не доступен для RAID-контроллера.
utmPowerSupply	integer	Количество источников питания: • 1 — один блок питания. • 2 — два блока питания.
utmPowerSupplyStatus	integer	Состояние источника питания: • no_power_supplies. • 0 — off. • 1 — on.
utmCSCIfName	string	Название интерфейса.
utmCSCStatus	integer	Статус сетевого адаптера: • 1 — кабель подключен. • 2 — кабель не подключен.
utmLDAPServerName	string	Название LDAP-сервера.
utmLDAPServerAddress	string	IP-адрес LDAP-сервера.

UTM-MIB

Наименование	Тип данных	Описание
vcpuCount	integer	Количество виртуальных процессоров в системе.
vcpuUsage	integer	Загруженность виртуальных процессоров системы; отображается в %.
usersCounter	integer	Количество активных пользователей на текущий момент времени.
cpuLoad	integer	Загруженность центрального процессора системы; отображается в %.
memoryUsed	integer	Использование оперативной памяти; отображается в %.

Наименование	Тип данных	Описание
logDiskSpace	integer	Пространство на диске, используемое под журналы; отображается в %.
Sys_power_supply1_status	string	Состояние первого источника питания: • no_power_supplies. • on. • off.
Sys_power_supply2_status	string	Состояние второго источника питания. • no_power_supplies. • on. • off.
Sys_raid_status	integer	Текущий статус RAID (Redundant Array of Independent Disks): • no_raid. • 0 — optimal — массив в оптимальном состоянии. • 1 — degraded — полный или частичный выход из строя одного из дисков. • 2 — rebuild — восстановление массива.

UTM-INTERFACES-MIB

Наименование	Тип данных	Описание
ifNumber	integer	Количество сетевых интерфейсов.
ifIndex	integer	Значение уникально для каждого интерфейса и может принимать значения от 1 до ifNumber.
ifDescr	string	Описание интерфейса.

Наименование	Тип данных	Описание
ifType	integer	Тип интерфейса, определённый в соответствии с протоколом физического/канального уровней: • 1 — other — неизвестный тип. • 2 — regular1822 — определён в BBN Report 1822. • 3 — hdh1822 — определён в BBN Report 1822. • 4 — ddn-x25 — определён в BBN Report 1822. • 5 — rfc877-x25 — определён в стандарте канального уровня сетевой модели OSI X.25. • 6 — ethernet-csmacd — сетевой интерфейс типа Ethernet, независимо от скорости (определён в RFC 3635). • 7 — iso88023-csmacd — определён в IEEE 802.3. • 8 — iso88024-tokenBus — определён в стандарте IEEE 802.4. • 9 — iso88025-tokenRing — сетевой интерфейс использует подключение Token Ring; определяется в стандарте IEEE 802.5. • 10 — iso88026-man — определён в стандарте ISO 88026 "MAN". • 11 — starLan — определён в стандарте IEEE 802.3e. • 12 — proteon-10Mbit — Proteon 10 Mbit • 13 — proteon-80Mbit — Proteon 80 Mbit. • 14 — hyperchannel — высокоскоростной канал, используемы в сети ISDN. • 15 — fddi — сетевой интерфейс использует подключение FDDI (Fiber Distributed Data Interface). FDDI — это набор стандартов передачи данных по оптоволоконным линиям в локальной сети. • 16 — lapb — протокол канального уровня, используемым для передачи пакетов стандарта X.25. • 17 — sdhc — протокол канального уровня для системной сетевой архитектуры IBM. • 18 — ds1 — способен обрабатывать 24 одновременных соединения на общей скорости 1,544 Мбит/с; также называется T1. • 19 — e1 — европейский аналог T1. • 20 — basicISDN — для связи аппаратуры абонента и ISDN-станции. • 21 — primaryISDN — используется для подключения к широкополосным магистралям, связывающим местные и центральные АТС или сетевые коммутаторы. • 22 — propPointToPointSerial — определён в стандарте RFC1213. • 23 — ppp — сетевой интерфейс использует подключение PPP (Point-To-Point Protocol). • 24 — softwareLoopback — сетевой интерфейс является петлевым адаптером. Такие интерфейсы часто используются для тестирования; они не отправляют трафик в сеть. • 25 — eon — ConnectionLess Network Protocol (CLNP) over Internet Protocol (IP); определён в ISO/IEC 8473-1. • 26 — ethernet-3Mbit — сетевой интерфейс использует подключение Ethernet со скоростью 3 Мбит/с. Эта версия Ethernet определяется в стандарте IETF RFC 895. • 27 — nsip — XNS over IP — предназначен для использования в разнообразных средах передачи данных. • 28 — slip — сетевой интерфейс использует подключение SLIP (Serial Line Internet Protocol). SLIP определяется в стандарте IETF RFC 1055. • 29 — ultra -ULTRA Technologies. • 30 — ds3 — высокоскоростной интерфейс передачи данных, сформированный мультиплексированием сигналов DS1 и DS2; также называется T3. • 31 — sip — сетевой интерфейс использует подключение SLIP (Serial Line Internet Protocol). SLIP определяется в стандарте IETF RFC 1055. • 32 — frame-relay — обеспечивает возможность передачи данных с коммутацией пакетов через интерфейс между устройствами пользователя и оборудованием сети.

Наименование	Тип данных	Описание
ifMtu	integer	Максимальный размер пакета сетевого уровня, который можно послать через этот интерфейс.
ifSpeed	gauge32	Пропускная способность интерфейса в битах в секунду.
ifPhysAddress	string	Физический адрес интерфейса (MAC-адрес).
ifAdminStatus	integer	Состояние интерфейса, назначаемое администратором: 1 — up — готов для передачи пакетов. 2 — down — не работает. 3 — testing — в режиме тестирования; рабочие пакеты не могут быть переданы.
ifOperStatus	integer	Текущий статус работы интерфейса: 1 — up — интерфейс готов для передачи пакетов. 2 — down — интерфейс не может передавать пакеты данных. 3 — testing — выполняется тестирование сетевого интерфейса; рабочие пакеты не могут быть переданы. 4 — unknown — интерфейс находится в неизвестном состоянии. 5 — dormant — сетевой интерфейс не может передавать пакеты данных, он ожидает внешнее событие. 6 — notPresente — сетевой интерфейс не может передавать пакеты данных из-за отсутствующего компонента, обычно аппаратного. 7 — lowerLayerDown — сетевой интерфейс не может передавать пакеты данных, потому что он работает поверх одного или нескольких других интерфейсов, и не менее одного из этих интерфейсов "нижнего уровня" не работает.
ifLastChange	timeticks	Значение SysUpTime, когда интерфейс оказался в данном состоянии.
ifInOctets	counter32	Количество байтов, принятое данным интерфейсом, включая служебные.
ifInUcastPkts	counter32	Количество доставленных пакетов одноадресной рассылки.
ifInNUcastPkts	counter32	Количество доставленных многоадресных и широковещательных пакетов.
ifInDiscards	counter32	Количество входящих пакетов, которые были отброшены, даже если не было обнаружено ошибок, препятствующих их доставке. Одна из возможных причин отбрасывания: освобождение буферного пространства.
ifInErrors	counter32	Количество входящих пакетов, которые содержат ошибки, препятствующие их доставке.
ifInUnknownProtos	counter32	Количество пакетов, которые были получены через этот интерфейс и отброшены из-за использования неизвестного или неподдерживаемого протокола.
ifOutOctets	counter32	Количество байтов, переданное данным интерфейсом, включая служебные.
ifOutUcastPkts	counter32	Количество отправленных пакетов одноадресной рассылки, включая пакеты, которые были отброшены или не отправлены.
ifOutNUcastPkts	counter32	Количество отправленных многоадресных и широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены.

Наименование	Тип данных	Описание
ifOutDiscards	counter32	Количество исходящих пакетов, которые были отброшены, даже если не было обнаружено ошибок, препятствующих их передаче. Одна из возможных причин отбрасывания: освобождение буферного пространства.
ifOutErrors	counter32	Количество исходящих пакетов, передача которых невозможна вследствие наличия ошибок.
ifOutQLen	gauge32	Число пакетов в очереди на отправку.
ifInMulticastPkts	counter32	Количество доставленных пакетов многоадресной рассылки.
ifInBroadcastPkts	counter32	Количество доставленных широковещательных пакетов.
ifOutMulticastPkts	counter32	Количество отправленных пакетов многоадресной рассылки, включая пакеты, которые были отброшены или не отправлены.
ifOutBroadcastPkts	counter32	Количество отправленных широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены.
ifHCInOctets	counter64	Смысл одинаков со смыслом объекта ifInOctets — количество байтов, принятое данным интерфейсом, включая служебные; используется счётчик большей ёмкости.
ifHCInUcastPkts	counter64	Смысл одинаков со смыслом объекта ifInUcastPkts — количество доставленных пакетов одноадресной рассылки; используется счётчик большей ёмкости.
ifHCInMulticastPkts	counter64	Смысл одинаков со смыслом объекта ifInMulticastPkts — количество доставленных пакетов многоадресной рассылки; используется счётчик большей ёмкости.
ifHCInBroadcastPkts	counter64	Смысл одинаков со смыслом объекта ifInBroadcastPkts — количество доставленных широковещательных пакетов; используется счётчик большей ёмкости.
ifHCOctets	counter64	Смысл одинаков со смыслом объекта ifOutOctets — количество байтов, переданное данным интерфейсом, включая служебные; используется счётчик большей ёмкости.
ifHCOUcastPkts	counter64	Смысл одинаков со смыслом объекта ifOutUcastPkts — количество отправленных пакетов одноадресной рассылки, включая пакеты, которые были отброшены или не отправлены; используется счётчик большей ёмкости.
ifHCOmulticastPkts	counter64	Смысл одинаков со смыслом объекта ifOutMulticastPkts — количество отправленных пакетов многоадресной рассылки, включая пакеты, которые были отброшены или не отправлены; используется счётчик большей ёмкости.
ifHCObroadcastPkts	counter64	Смысл одинаков со смыслом объекта ifOutBroadcastPkts — количество отправленных широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены; используется счётчик большей ёмкости.
ifLinkUpDownTrapEnable	integer	Указывает, должен ли создаваться трап при изменении статуса соединения: • 1 — enabled — включено. • 2 — disabled — отключено.
ifHighSpeed	gauge32	Оценка текущей полосы пропускания интерфейса; указывается в бит/с, кбит/с, Мбит/с, Гбит/с.

Наименование	Тип данных	Описание
ifPromiscuousMode	integer	"Неразборчивый" режим. Может принимать значения: • 1 — true — станция принимает все пакеты/кадры независимо от того, кому они адресованы. • 2 — false — интерфейс принимает только пакеты/кадры, адресованные этой станции. Значение объекта не влияет на приём широковещательных и многоадресных пакетов/кадров.
ifAlias	string	Название интерфейса, заданное администратором.
ifCounterDiscontinuityTime	timeticks	Значение SysUpTime, когда произошло событие, ставшее причиной сбоя работы одного или более счётчиков интерфейса.

Журнал событий

Documentation: ☒

Product: UGMC

Version: 7.0.1, 7.1.0

В журнале отображены события, связанные с изменением настроек сервера UserGate Management Center, а также все события авторизации в консоли, старта, выключения, перезагрузки сервера и т.п.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например, диапазон дат, компонент, важность, тип события.

В UserGate Management Center также представлен режим расширенного поиска для формирования сложных фильтров 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 отражены 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.

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

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Режим расширенного поиска

Documentation: ☒
Product: UGMC
Version: 7.0.1, 7.1.0

Помимо простого поиска, для которого используется графический интерфейс, в LogAn представлена возможность расширенного поиска с формированием более сложных фильтров поиска и использованием специального языка запросов. Для формирования запросов используются названия полей, значения полей, ключевые слова и операторы. Значения полей могут быть введены с использованием одинарных или двойных кавычек, или без них, если значения не содержат пробелов. Для группировки нескольких условий можно использовать круглые скобки.

Ключевые слова отделяются пробелами и могут быть следующими:

Наименование	Описание
AND или and	Логическое И, требует выполнение всех условий, заданных в запросе.
OR или or	Логическое ИЛИ, требует выполнение одного из условий запроса.

Операторы определяют условия фильтра и могут быть следующими:

Наименование	Описание
=	Равно. Требует полного совпадения значения поля указанному значению, например, ip=172.16.31.1 будут отображены все записи журнала, в котором поле IP будет точно соответствовать значению 172.16.31.1.
!=	Не равно. Значение указанного поля не должно совпадать с указанным значением, например, ip!=172.16.31 будут отображены все записи журнала, в котором поле IP не будет равно значению 172.16.31.1.
<=	Меньше либо равно. Значение поля должно быть меньше либо равны указанному в запросе значению. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, date <= '2019-03-28T20:59:59' AND statusCode=303.
>=	Больше либо равно. Значение поля должно быть больше либо равны указанному в запросе значению. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, date >= "2019-03-13T21:00:00" AND statusCode=200.
<	Меньше. Значение поля должно быть меньше указанного в запросе значения. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, date < '2019-03-28T20:59:59' AND statusCode=404.
>	Больше. Значение поля должно быть больше указанного в запросе значения. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, (statusCode>200 AND statusCode<300) OR (statusCode=404).
IN	Позволяет указать несколько значений поля в запросе. Список значений необходимо указывать в круглых скобках, например, category IN (botnets, compromised, 'illegal software', 'phishing and fraud','reputation high risk','unknown category').
NOT IN	Позволяет указать несколько значений поля в запросе; будут отображены записи, не содержащие указанные значения. Список значений необходимо указывать в круглых скобках, например, category NOT IN (botnets, compromised, 'illegal software', 'phishing and fraud','reputation high risk','unknown category').

Наименование	Описание
~	Содержит. Позволяет указать подстроку, которая должна находиться в указанном поле, например, browser ~ "Mozilla/5.0". Данный оператор может быть применен только к полям, в которых хранятся строковые данные.
!~	Не содержит. Позволяет указать подстроку, которая не должна присутствовать в указанном поле, например, browser !~ "Mozilla/5.0". Данный оператор может быть применен только к полям, в которых хранятся строковые данные.
MATCH	При использовании оператора MATCH подстрока, которая должна присутствовать в указанном поле, задаётся в формате JSON и с использованием одинарных кавычек, например, details MATCH {"module":"threats"}. Синтаксис запросов с использованием данного оператора соответствует стандарту RE2. Подробнее о синтаксисе Google/RE2: https://github.com/google/re2/wiki/Syntax.
NOT MATCH	При использовании оператора NOT MATCH подстрока, которая не должна присутствовать в указанном поле, задаётся в формате JSON и с использованием одинарных кавычек, например, details NOT MATCH {"module":"threats"}. Синтаксис запросов с использованием данного оператора соответствует стандарту RE2. Подробнее о синтаксисе Google/RE2: https://github.com/google/re2/wiki/Syntax.

При переключении режима поиска с основного на расширенный LogAn автоматически формирует строку с поисковым запросом, которая соответствует фильтру, указанному в основном режиме поиска.

Экспорт журналов

Documentation: ☒
Product: UGMC
Version: 7.0.1, 7.1.0

Функция экспорта журналов UserGate позволяет выгружать информацию на внешние серверы для последующего анализа или для обработки в системах SIEM (Security information and event management).

Поддерживается отправка журналов на серверы SSH (SFTP), FTP и Syslog. Отправка на серверы SSH и FTP проводится по указанному в конфигурации расписанию или разово (кнопка **Послать разово**). Отправка на серверы Syslog происходит сразу же при добавлении записи в журнал.

Для отправки журналов необходимо в режиме администратора устройства создать правила экспорта журналов в разделе **Журналы и отчеты → Экспорт журналов**.

ПримечаниеНастройки экспорта журналов не являются кластерными. Если UGMC работает в кластерной конфигурации, правила экспорта журналов создаются отдельно на каждом узле.

При создании конфигурации требуется указать следующие параметры:

Наименование	Описание
Название правила	Название правила экспорта журналов.
Описание	Опциональное поле для описания правила.
Журналы для экспорта	Выбор файлов журналов, которые необходимо экспортировать: - Журнал событий. Для каждого из журналов возможно указать синтаксис выгрузки: - CEF — Common Event Format (ArcSight). - JSON — JSON format. @CEE: JSON — CEE Log Syntax (CLS) Encoding JSON. Обратитесь к документации на используемую у вас систему SIEM для выбора необходимого формата выгрузки журналов. Подробное описание форматов журналов читайте в Приложение 2. Описание форматов журналов.
Тип сервера	SSH (SFTP), FTP, Syslog.
Адрес сервера	IP-адрес или доменное имя сервера.
Транспорт	Только для типа серверов Syslog — TCP или UDP.
Порт	Порт сервера, на который следует отправлять данные.
Протокол	Только для типа серверов Syslog — RFC5424 или BSD syslog RFC 3164. Выберите протокол, совместимый с используемой у вас системой SIEM.

Наименование	Описание
Критичность	Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас систему SIEM. Возможны следующие значения: • Тревога: состояние, требующее незамедлительного вмешательства. • Критическая: состояние, требующее незамедлительного вмешательства либо предупреждающее о сбое в системе. • Ошибки: в системе возникли ошибки. • Предупреждения: предупреждения о возможном возникновении ошибок, если не будут предприняты никакие действия. • Уведомительная: события, которые относятся к необычному поведению системы, но не являются ошибками. • Информативная: информационные сообщения.
Facility	Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас систему SIEM. Возможны следующие значения: • Сообщения пользовательские. • Системный сервис. • Безопасность/авторизация. • Аудит. • Тревога. • Local 0. • Local 1. • Local 2. • Local 3. • Local 4. • Local 5. • Local 6. • Local 7.
Имя хоста	Только для типа серверов Syslog. Уникальное имя хоста, идентифицирующее сервер, отправляющий данные на сервер syslog, в формате Fully Qualified Domain Name (FQDN).
App-Name	Только для типа серверов Syslog. Уникальное имя приложения, которое отправляет данные на сервер syslog.
Логин	Имя учетной записи для подключения к удаленному серверу. Не применяется к методу отправки Syslog.
Пароль	Пароль учетной записи для подключения к удаленному серверу. Не применяется к методу отправки Syslog.
Путь на сервере	Каталог на сервере для копирования файлов журналов. Не применяется к методу отправки Syslog. В кластерной конфигурации UGMC при экспорте журналов с разных узлов кластера необходимо указывать разные каталоги на сервере для каждого узла UGMC, поскольку имена файлов журналов на каждом узле идентичны.

Наименование	Описание
Расписание	Выбор расписания для отправки логов. Не применяется к методу отправки Syslog. Возможны варианты: • 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 "<u>*/2</u>" в поле "часы" будет означать "каждые два часа".
Управление журналами	Управление временными файлами журналов, подготавливаемых для отправки на удаленные серверы ssh и ftp. При отправке журналов на сервера ssh и ftp UserGate сохраняет данные для отправки во временных файлах в кодировке UTF-8. Журналы за предыдущие дни (по количеству дней ротации) хранятся в виде архивов, журнал за текущий день не архивирован. По указанному расписанию все созданные для отправки файлы копируются на удаленный сервер, при этом файлы не очищаются и не удаляются. Данная настройка позволяет указать период ротации временных файлов (в днях) или удалить любой из временных файлов вручную. Ротация файлов происходит один раз в сутки.

Примечание Возможно сохранение журнала администратором вручную непосредственно из веб-консоли. При этом данные сохраняются только в формате CSV.

Создание управляемых областей

Documentation: ☒
Version: 7.0.1, 7.1.0
Product: UGMC

Для создания управляемой области администратор UGMC должен выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать область.	В разделе веб-консоли Управляемые области → Области нажать кнопку Добавить , заполнить необходимые поля.
Шаг 2. Создать профиль администратора с типом администратор области.	В разделе веб-консоли Администраторы → Профили администраторов нажать кнопку Добавить и создать профиль администратора с типом администратор области и правом на созданную на предыдущем шаге область.
Шаг 3. Создать администратора области.	В разделе веб-консоли Администраторы → Администраторы нажать кнопку Добавить и создать администратора с созданным ранее профилем.

При создании области необходимо указать следующие поля:

Наименование	Описание
Область по умолчанию	Если данная галочка установлена, то при авторизации в веб-консоль необязательно указывать имя области через слэш.
Название	Название области, например, ООО Юзергейт.
Код области	Код из нескольких букв и/или цифр. Код области необходимо указывать при входе в веб-консоль для управления данной областью. Например, UG.
Описание	Опциональное описание области.
Количество устройств	Если указано, то администратор области будет ограничен этим количеством и не сможет создать большее количество управляемых устройств. Заданное количество не может превышать количество лицензированных подключений.

При создании профиля администратора необходимо указать тип администратора - администратор области и в качестве управляемой области указать созданную область. Для создания администратора области необходимо выбрать данный профиль администратора области. Подробнее о создании администраторов смотрите в главе данного руководства [Администраторы](#).

После создания области и администратора данной области можно переключиться в режим управления данной областью. Для этого необходимо выйти из-под учетной записи администратора UGMC в веб-консоли и заново зайти под учетной записью администратора управляемой области. Имя администратора следует указать в следующем виде:

имя_администратора/код_области, например, *Admin/UG*.

Для возврата в консоль под администратором UGMC необходимо указать имя в следующем виде:

имя_администратора/system, например, *Admin/system*.

Администраторы области

Version: 7.0.1, 7.1.0
Product: UGMC
Documentation: ☒

Доступ к веб-консоли управления областью регулируется с помощью создания дополнительных учетных записей администраторов области и назначения им профилей доступа.

Примечание При создании управляемой области администратор UGMC создает корневого администратора области, обладающего всеми полномочиями на данную зону.

Для создания дополнительных учетных записей администраторов области необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Войти в веб-консоль управления под корневым администратором области.	Войти в консоль управления под корневым администратором, созданным для данной области, указав имя в виде <i>имя_администратора/код_области</i> , например, <i>Admin/UG</i> .
Шаг 2. Создать профиль доступа администратора области.	В консоли управления областью в разделе Администраторы → Профили администраторов нажать кнопку Добавить и указать необходимые настройки.
Шаг 3. Создать учетную запись администратора и назначить ей один из созданных ранее профилей администратора.	В разделе Администраторы нажать кнопку Добавить и выбрать необходимый вариант: • Добавить локального администратора — создать локального пользователя, задать ему пароль доступа и назначить созданный ранее профиль доступа. • Добавить пользователя LDAP — добавить пользователя из существующего домена. Для этого должен быть корректно настроен LDAP-коннектор в разделе Серверы аутентификации области. При входе в консоль администрирования необходимо указывать имя пользователя в формате <i>user@domain</i>. Назначить созданный ранее профиль. • Добавить группу LDAP — добавить группу пользователей из существующего домена. Для этого должен быть корректно настроен LDAP-коннектор в разделе Серверы аутентификации области. При входе в консоль администрирования необходимо указывать имя пользователя в формате <i>user@domain</i>. Назначить созданный ранее профиль. • Добавить администратора с профилем аутентификации — создать пользователя, назначить созданный ранее профиль администратора и профиль аутентификации (необходимы корректно настроенные серверы аутентификации).

При создании профиля доступа администратора необходимо указать следующие параметры:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Права доступа на область	Укажите права доступа на разделы настроек области, такие как администраторы, серверы аутентификации, шаблоны устройств, группы шаблонов, управляемые устройства, журналы и отчеты. В качестве доступа можно указать: • Нет доступа. • Чтение. • Чтение и запись.

Наименование	Описание
Права доступа на шаблон	Укажите здесь права на просмотр и/или изменение настроек всех или конкретных имеющихся шаблонов. Настройки представлены в виде объектов дерева веб-консоли МЭ UserGate, доступных для делегирования. В качестве доступа можно указать: • Нет доступа. • Чтение. • Чтение и запись. Например, можно разрешить сетевые настройки одной группе администраторов, а политики МЭ — другой.

Серверы аутентификации области

Version: 7.0.1, 7.1.0
Product: UGMC
Documentation: ☒

Серверы аутентификации - это внешние источники учетных записей пользователей для авторизации в веб-консоли управления области. Работа сервера аутентификации области аналогична работе сервера аутентификации для UGMC, отличие только в месте их использования.

LDAP-коннектор

LDAP-коннектор позволяет:

- Получать информацию о пользователях и группах Active Directory или других LDAP-серверов. Поддерживается работа с LDAP-сервером FreeIPA.
- Осуществлять авторизацию администраторов UGMC через домены Active Directory/FreeIPA.

Для создания LDAP-коннектора необходимо нажать на кнопку **Добавить**, выбрать **Добавить LDAP-коннектор** и указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данного сервера аутентификации.
Название	Название сервера аутентификации.
SSL	Определяет, требуется ли SSL-соединение для подключения к LDAP-серверу.
Доменное имя LDAP или IP-адрес	IP-адрес контроллера домена, FQDN контроллера домена или FQDN домена (например, test.local). Если указан FQDN, то UserGate получит адрес контроллера домена с помощью DNS-запроса. Если указан FQDN домена, то при отключении основного контроллера домена, UserGate будет использовать резервный.
Bind DN («login»)	Имя пользователя, которое необходимо использовать для подключения к серверу LDAP. Имя необходимо использовать в формате DOMAIN\username или username@domain. Данный пользователь уже должен быть заведен в домене
Пароль	Пароль пользователя для подключения к домену.
Домены LDAP	Список доменов, которые обслуживаются указанным контроллером домена, например, в случае дерева доменов или леса доменов Active Directory. Здесь же можно указать короткое netbios имя домена.
Пути поиска	Список путей в сервере LDAP, начиная с которых система будет осуществлять поиск пользователей и групп. Необходимо указывать полное имя, например, ou=Office,dc=example,dc=com.

После создания сервера необходимо проверить корректность параметров, нажав на кнопку **Проверить соединение**. Если параметры указаны верно, система сообщит об этом либо укажет на причину невозможности соединения.

Настройка LDAP-коннектора завершена. Для входа в консоль пользователям LDAP необходимо указывать имя в формате:

`domain\user/system` или `user@domain/system`

Сервер аутентификации RADIUS

Сервер аутентификации RADIUS позволяет производить авторизацию пользователей в веб-консоли UserGate, который выступает в роли RADIUS-клиента. При авторизации через RADIUS-сервер UserGate посылает на серверы RADIUS информацию с именем и паролем пользователя, а RADIUS-сервер отвечает, успешно прошла аутентификация или нет.

Для добавления сервера аутентификации RADIUS необходимо нажать **Добавить**, выбрать **Добавить RADIUS-сервер** и указать следующие параметры:

Наименование	Описание
Включено	Включение/отключение использования данного сервера аутентификации.

Наименование	Описание
Название	Название сервера аутентификации RADIUS.
Описание	Описание сервера (опционально).
Секрет	Общий ключ, используемый протоколом RADIUS для аутентификации.
Адреса	Указание IP-адреса сервера и UDP-порта, на котором сервер RADIUS слушает запросы на аутентификацию (по умолчанию, 1812).

Для авторизации пользователей в веб-интерфейсе UserGate с помощью сервера RADIUS необходимо настроить профиль аутентификации. Подробнее о создании и настройке профилей читайте в разделе [Профили аутентификации области](#).

Сервер аутентификации TACACS+

Сервер TACACS+ позволяет производить авторизацию пользователей в консоли администрирования UserGate. При использовании сервера UserGate передаёт на серверы аутентификации информацию с именем и паролем пользователя, после чего серверы TACACS+ отвечают, успешно прошла аутентификация или нет.

Для добавления сервера аутентификации RADIUS необходимо нажать **Добавить**, выбрать **Добавить TACACS+ сервер** и указать следующие параметры:

Наименование	Описание
Включено	Включение/отключение использования данного сервера аутентификации.
Название	Название сервера аутентификации TACACS+.
Описание	Описание сервера (опционально).
Секретный ключ	Общий ключ, используемый протоколом TACACS+ для аутентификации.
Адрес	IP-адрес сервера TACACS+.
Порт	UDP-порт, на котором сервер TACACS+ слушает запросы на аутентификацию.
Использовать одно TCP-соединение	Использовать одно TCP-соединение для работы с сервером TACACS+.
Таймаут (сек)	Время ожидания сервера TACACS+ для получения аутентификации. По умолчанию 4 секунды.

Для авторизации пользователей в веб-интерфейсе UserGate с помощью сервера TACACS+ необходимо настроить профиль аутентификации. Подробнее о создании и настройке профилей читайте в разделе [Профили аутентификации области](#).

Профили аутентификации области

Documentation: ☒
Version: 7.0.1, 7.1.0
Product: UGMC

Профиль позволяет определить набор способов авторизации пользователей в консоли администрирования UserGate. При создании или настройке профиля достаточно указать:

Наименование	Описание
Название	Название профиля аутентификации.
Описание	Описание профиля (опционально).
Методы аутентификации	Методы аутентификации пользователей, настроенные ранее: LDAP-коннектор, серверы аутентификации RADIUS, TACACS+.

Каталоги пользователей

Version: 7.0.1, 7.1.0

Product: UGMC

Documentation: ☒

Для работы с каталогами пользователей необходим корректно настроенный LDAP-коннектор, который позволяет получать информацию о пользователях и группах Active Directory или других LDAP-серверов. Пользователи и группы могут быть использованы при настройке политик, применяемых к управляемым устройствам.

Примечание При настройке политик безопасности серверы аутентификации, настраиваемые в шаблонах управляемых устройств, не используются для добавления пользователей и групп в правила.

Для создания каталога необходимо нажать на кнопку **Добавить** и указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данного LDAP-коннектора.
Название	Название LDAP-коннектора.
SSL	Определяет, требуется ли SSL-соединение для подключения к LDAP-серверу.
Доменное имя LDAP или IP-адрес	IP-адрес контроллера домена, FQDN контроллера домена или FQDN домена (например, test.local). Если указан FQDN, то UserGate получит адрес контроллера домена с помощью DNS-запроса. Если указан FQDN домена, то при отключении основного контроллера домена, UserGate будет использовать резервный.
Bind DN («login»)	Имя пользователя, которое необходимо использовать для подключения к серверу LDAP. Имя необходимо использовать в формате DOMAIN\username или username@domain. Данный пользователь уже должен быть заведен в домене.
Пароль	Пароль пользователя для подключения к домену.
Домены LDAP	Список доменов, которые обслуживаются указанным контроллером домена, например, в случае дерева доменов или леса доменов Active Directory. Здесь же можно указать короткое netbios имя домена.
Пути поиска	Список путей в сервере LDAP, начиная с которых система будет осуществлять поиск пользователей и групп. Необходимо указывать полное имя, например, ou=Office,dc=example,dc=com.

После создания сервера необходимо проверить корректность параметров, нажав на кнопку **Проверить соединение**. Если параметры указаны верно, система сообщит об этом либо укажет на причину невозможности соединения.

Для добавления пользователя или группы пользователей LDAP в свойствах правила необходимо нажать на **Добавить пользователя LDAP/Добавить группу LDAP**, в поле поиска указать как минимум один символ, входящий в имена искомых объектов, после чего нажать на **Поиск** и выбрать необходимые группы или пользователей.

Управление областями (Описание)

Version: 7.0.1, 7.1.0

Product: UGMC

Documentation: 

Управляемая область UserGate — это логический объект, представляющий одно предприятие или группу предприятий, управляемых единым администратором или группой администраторов. Для управления устройствами UserGate корневой администратор UGMC (или администратор UGMC с соответствующими полномочиями) должен создать как минимум одну область.

Управление межсетевыми экранами UserGate (Описание)

Documentation: ☒

Product: UGMC

Version: 7.0.1, 7.1.0

Централизованное управление МЭ UserGate можно разделить на 4 этапа:

1. Создание управляемой области. Смотрите раздел [Создание управляемых областей](#).
2. Создание шаблона или несколько шаблонов, каждый из которых опишет свою часть настроек МЭ. Смотрите раздел [Шаблоны устройств](#) для более детальной информации.
3. Объединение необходимых шаблонов в группу шаблонов в требуемом порядке, чтобы получить корректную результирующую настройку управляемых устройств. Смотрите раздел [Группы шаблонов](#) для более детальной информации.
4. Добавление управляемого устройства (МЭ) и применения к нему группы шаблонов. Смотрите раздел [Добавление устройств UserGate под управление UGMC](#) для более детальной информации.

При необходимости настройки, заданные в шаблонах можно изменять, чтобы эти отражения применялись ко всем МЭ, к которым применимы данные шаблоны.

UGMC позволяет создавать и управлять кластерами конфигурации и отказоустойчивости. Подробно тонкости управления кластерами описаны в разделе [Кластеризация МЭ UserGate с помощью UGMC](#).

Шаблоны устройств

Шаблон — это базовый блок, с помощью которого можно настроить все параметры работы межсетевого экрана — сетевые настройки, правила межсетевого экрана, контентной фильтрации, системы обнаружения вторжений и других. Для создания шаблона необходимо в разделе **Управление NGFW → Шаблоны устройств** 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 **Управление шаблонами** и в выпадающем меню выбрать необходимый шаблон.

Настройки параметров шаблона отображаются в виде дерева, полностью аналогично, как они представлены в МЭ UserGate. При настройке параметров следует придерживаться следующих правил:

1. Если значение настройки не определено в шаблоне, то ничего передаваться в МЭ UserGate не будет. В данном случае в МЭ UserGate будет использована либо настройка по умолчанию, либо настройка, которую указал локальный администратор МЭ UserGate.
2. Если настройка параметра выполнена в шаблоне, то эта настройка переопределит значение этой же настройки, назначенной локальным администратором.

После получения настроек с Management Center настройки следующих разделов могут быть изменены локально на NGFW:

- общие настройки устройства: вкладка **Настройки**, раздел **UserGate → Настройки**;
- настройки сетевых интерфейсов: вкладка **Настройки**, раздел **Сеть → Интерфейсы**.

Примечание Настройка будет переопределена после изменения данной настройки в шаблоне NGFW администратором области на UGMC.

3. Правила политик не переопределяют правила, созданные локальным администратором, а добавляются к ним в виде пре- и пост-правил. Подробно о применении правил смотрите раздел данного руководства [Шаблоны и группы шаблонов](#).
4. При настройке сетевых интерфейсов первый физический интерфейс, доступный для конфигурирования — это **port1**. Интерфейс **port0** нельзя настроить с помощью средств UGMC, он всегда настраивается локальным администратором и необходим для обеспечения первичной связи управляемых устройств с UGMC.
5. При настройке сетевых интерфейсов возможно создать интерфейс и оставить его конфигурирование локальному администратору. Для этого необходимо включить чекбокс **Настраивается на устройстве** в настройках сетевого интерфейса.
6. В некоторых настройках и правилах политик доступна опция применения данного правила или настройки только к конкретному устройству. Для этого необходимо выбрать управляемое устройство в свойствах правила/настройки в закладке **Управляемые устройства**. Хотя это и предоставляет определенную гибкость, следует избегать чрезмерного использования данной опции, поскольку это приводит к сложности понимания применения настроек к группам МЭ UserGate.
7. Библиотеки, например, такие как IP-адреса, списки URL, типы контента и другие, по умолчанию не содержат никакого контента в UGMC в отличие от библиотек, создаваемых по умолчанию на устройствах МЭ UserGate. Для использования библиотек в политиках UGMC, необходимо предварительно добавить элементы в эти библиотеки. Элементы библиотек не участвуют в синхронизации: если список был создан, но не используется в политиках, то данный список не появится в разделе библиотек NGFW.
8. 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. Например, шаблон сетевых настроек, шаблон правил межсетевого экрана, шаблон правил контентной фильтрации, шаблон библиотек и т.д.

Группы шаблонов

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

Результирующие настройки, применяемые к устройству МЭ, 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 NGFW → 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 устройств UserGate под управление UGMC

Группа шаблонов всегда применяется к одному или нескольким управляемым устройствам МЭ UserGate. Процедура добавления управляемого устройства в UserGate Management Center состоит из следующих шагов:

Наименование	Описание
Шаг 1. Обеспечить доступ от управляемого устройства до UGMC	На сервере UGMC необходимо разрешить сервис UserGate Management Center зоне, к которой подключены управляемые устройства. Сервер UGMC слушает подключения от управляемых устройств на портах TCP 2022 и 9712. Передача данных между сервером UGMC и управляемыми устройствами осуществляется по зашифрованному каналу.
Шаг 2. Создать объект управляемого устройства	В консоли управления областью в разделе Управление NGFW → Устройства NGFW нажать кнопку Добавить и указать необходимые настройки.
Шаг 3. Связать созданный объект управляемого устройства с реальным устройством МЭ UserGate.	В консоли управления МЭ UserGate настройте связь между UGMC и устройством. Данную операцию можно произвести в момент первоначальной установки МЭ UserGate, либо уже на настроенный МЭ. Оба варианта подробно описаны далее в этой главе.

При создании объекта управляемого устройства необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает объект управляемого устройства. Если объект управляемого устройства включен, то он занимает одну лицензию.
Название	Название для управляемого устройства. Можно вводить произвольное название.
Описание	Описание управляемого устройства.
Группа шаблонов	Группа шаблонов, настройки которой следует применить к этому управляемому устройству.
Синхронизация	Выбор режима синхронизации настроек группы шаблонов к устройству. Возможны 3 варианта: • Автоматическая синхронизация — синхронизация включена. Настройки применяются к устройству. При изменении любой настройки из любого шаблона, включенного в группу шаблонов, примененную к управляемому устройству, это изменение применяется к МЭ без задержек. • Отключено — синхронизация выключена. • Ручная синхронизация — режим синхронизации, при котором настройки применяются однократно при нажатии кнопки Запросить синхронизацию. 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. Вне зависимости от выбранного режима доступен запуск синхронизации всех настроек для выбранных устройств (раздел Управление NGFW → Устройства NGFW кнопка Действия → Запустить полную синхронизацию).

Для осуществления связи МЭ с UGMC во время первоначальной настройки МЭ UserGate необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Скопировать Код устройства	В UGMC выбрать созданный объект управляемого устройства и нажать на кнопку Показать уникальный код устройства . Скопировать данный код в буфер обмена.

Наименование	Описание
Шаг 2. На МЭ в момент первоначальной инициализации выбрать установку с помощью UGMC	В момент первоначальной инициализации на этапе задания имени администратора и его пароля необходимо выбрать ссылку Настроить через UGMC .
Шаг 3. Указать необходимые настройки нового узла и ввести уникальный код устройства	Указать следующие параметры: - Сетевые настройки данного МЭ UserGate (IP, маска, шлюз). Данные настройки будут применены к указанному интерфейсу. Необходимо, чтобы после задания сетевых настроек появилась сетевая доступность с этого МЭ до сервера UGMC. - Имя локального администратора и его пароль. - IP-адрес сервера UGMC и уникальный код устройства, сохраненный на первом шаге.
Шаг 4. Проверить подключение	После подключения к UGMC МЭ UserGate должен получить все настройки, подготовленные для него в UGMC. В МЭ настройки отображаются со значком замочка, означающим, что данную настройку локальный администратор не может изменять. В консоли UGMC в объекте управляемого устройства появится дополнительная информация о подключенном устройстве, такая как ПИН-код, серийный номер, информация о лицензии, используемой памяти и т.п.

Для осуществления связи уже настроенного МЭ с UGMC необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Скопировать Код устройства	В UGMC выбрать созданный объект управляемого устройства и нажать на кнопку Показать уникальный код устройства . Скопировать данный код в буфер обмена.
Шаг 2. Указать IP-адрес сервера UGMC и ввести уникальный код устройства	В разделе Настройки → Агент UGMC выбрать Настроить , указать IP-адрес сервера UGMC, вставить уникальный код устройства и включить данное подключение. Для успешного выполнения данного шага необходимо, чтобы была сетевая доступность с этого МЭ до сервера UGMC.
Шаг 3. Проверить подключение	После подключения к UGMC МЭ UserGate должен получить все настройки, подготовленные для него в UGMC. В МЭ настройки отображаются со значком замочка, означающим, что данную настройку локальный администратор не может изменять. В консоли UGMC в объекте управляемого устройства появится дополнительная информация о подключенном устройстве, такая как ПИН-код, серийный номер, информация о лицензии, используемой памяти и т.п.

После того, как МЭ UserGate успешно добавлен в UGMC администратор управляемого устройства может:

Наименование	Описание
Посмотреть расширенную информацию о состоянии управляемого устройства	В консоли UGMC необходимо выбрать объект управляемого устройства и нажать на кнопку Показать детальную информацию. Будет отображена следующая информация о подключенном устройстве: - Версия ПО устройства. - ПИН-код устройства. - Серийный номер ПАК. - Время непрерывной работы. - Показатели загрузки устройства — загрузка ЦП, оперативной памяти, своп-файла, количество пользователей, подключенных через устройство.
Подключиться к консоли управляемого устройства	В консоли UGMC необходимо выбрать объект управляемого устройства и нажать на кнопку Открыть консоль . В новом окне откроется консоль МЭ UserGate.
Изменить настройки	В консоли UGMC измените настройки одного из шаблонов, входящего в группу шаблонов, примененного к устройству. Новые настройки будут применены к МЭ UserGate.

Кластеризация МЭ UserGate с помощью UGMC

Шаблоны устройств позволяют объединить несколько устройств UserGate в кластер конфигурации с едиными настройками на всех узлах кластера и создать на базе узлов кластера конфигурации один или несколько кластеров отказоустойчивости.

Подробнее о различных режимах кластеризации, используемых в UserGate, описано в разделе **Кластеризация и отказоустойчивость** документа **UserGate 6. Руководство администратора**.

Кластер конфигурации

Создание кластера конфигурации, управляемого из UGMC, практически идентично созданию отдельно стоящего кластера. Отличие лишь в том, что первый узел кластера должен быть подключен под управление UGMC до создания кластера конфигурации. Каждому узлу кластера конфигурации, подключаемому в UGMC, назначается **идентификатор узла** — уникальный идентификатор вида *node_1*, *node_2*, *node_3* и так далее.

Для создания кластера конфигурации необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Выполнить первоначальную настройку на первом узле кластера	Смотрите главу Первоначальная настройка документа UserGate 6. Руководство администратора .
Шаг 2. Настроить на первом узле кластера зону, через интерфейсы которой будет выполняться репликация кластера	В разделе Зоны создать выделенную зону для репликации настроек кластера или использовать существующую (Cluster). В настройках зоны разрешить следующие сервисы: - Консоль администрирования - Кластер Не используйте для репликации зоны, интерфейсы которых подключены к недоверенным сетям, например, к интернету.
Шаг 3. Указать IP-адрес, который будет использоваться для связи с другими узлами кластера	В разделе Управление устройством в окне Кластер конфигурации выбрать текущий узел кластера и нажать на кнопку Редактировать . Указать IP-адрес интерфейса, входящего в зону, настроенную на шаге 2.
Шаг 4. Сгенерировать Секретный код на первом узле кластера	В разделе Управление устройством нажать на кнопку Сгенерировать секретный код . Полученный код скопировать в буфер обмена. Данный секретный код необходим для одноразовой авторизации второго узла при добавлении его в кластер.
Шаг 5. Подключить первый узел кластера конфигурации в UGMC	Подключение первого узла ничем не отличается от подключения отдельно стоящего устройства UserGate. Процедура подключения подробно описана в разделе Добавление устройств UserGate под управление UGMC. Первому узлу автоматически назначается идентификатор <i>node_1</i>.
Шаг 6. Подключить второй узел в кластер	Важно! Добавление в кластер конфигурации второго и последующих узлов возможно только при первоначальной инициализации этих узлов. Подключиться к веб-консоли второго узла кластера, выбрать язык установки. Указать интерфейс, который будет использован для подключения к первому узлу кластера, и назначить ему IP-адрес. Оба узла кластера должны находиться в одной подсети, например, интерфейсам eth2 обоих узлов назначены IP-адреса 192.168.100.5/24 и 192.168.100.6/24. В противном случае необходимо указать IP-адрес шлюза, через который будет доступен первый узел кластера. Указать IP-адрес первого узла, настроенный на шаге 3, вставить секретный код и нажать на кнопку Подключить. Если IP-адреса кластера, настроенные на шаге 2, назначены корректно, то система предложит назначить идентификатор кластера для добавляемого устройства в виде <i>node_2</i>, <i>node_3</i>, <i>node_4</i> и так далее. Идентификатор <i>node_1</i> уже был закреплен за первым узлом кластера. После назначения идентификатора второй узел будет добавлен в кластер, и все настройки первого узла реплицируются на второй. После успешного добавления узла в кластер, данный узел будет отображаться в качестве второго узла в списке управляемых устройств с выбранным идентификатором.

Настройка добавленного узла, включая настройки интерфейсов, зон, политик фильтрации, может производиться либо локально, либо через политики шаблонов UGMC. Если эти настройки уже были выполнены в шаблонах UGMC на момент подключения второго узла, то они будут применены к добавленному узлу сразу же после его добавления в кластер.

Добавление третьего и последующих узлов в кластер конфигурации выполняется аналогично.

Кластер отказоустойчивости

До 4-х узлов кластера конфигурации могут быть объединены в кластер отказоустойчивости, поддерживающий работу в режиме Актив-Актив или Актив-Пассив. Возможно собрать несколько кластеров отказоустойчивости. Для создания кластера отказоустойчивости с помощью UGMC необходимо выполнение следующих условий:

Наименование	Описание
Наличие кластера конфигурации	Должен быть создан кластер конфигурации. Кластер конфигурации должен корректно отображаться в списке управляемых устройств.
Наличие управляемых из UGMC интерфейсов	Наличие на устройствах UserGate интерфейсов, которые созданы и управляются из UGMC. Виртуальные IP-адреса могут быть назначены только на интерфейсы, которые созданы в шаблонах UGMC.
Выполнение требований, предъявляемых к кластеру отказоустойчивости	Выполнение всех требований, предъявляемых к узлам, при создании кластера отказоустойчивости без использования UGMC. Подробно о кластерах отказоустойчивости описано в разделе Кластеризация и отказоустойчивость документа UserGate 6. Руководство администратора .

Для создания кластера отказоустойчивости необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Настроить зоны, интерфейсы которых будут участвовать в отказоустойчивом кластере	В одном из шаблонов UGMC , где настроены зоны для управляемых устройств, в разделе Зоны следует разрешить сервис VRRP для всех зон, где планируется добавлять кластерный виртуальный IP-адрес.
Шаг 2. Создать кластер отказоустойчивости	В одном из шаблонов UGMC , в разделе Управление устройством → Кластер отказоустойчивости нажать на кнопку Добавить и указать параметры кластера отказоустойчивости.
Шаг 3. Указать виртуальный IP-адрес для хостов auth.captive, logout.captive, block.captive, ftpclient.captive	Если предполагается использовать авторизацию с помощью Captive-портала, то необходимо, чтобы системные имена хостов auth.captive и logout.captive, которые используются процедурами авторизации в Captive, резолвились в IP-адрес, назначенный в качестве кластерного виртуального адреса. Данную настройку можно выполнить в одном из шаблонов UGMC , в разделе Настройки . Более детально эти параметры описаны в разделе Настройка устройства документа UserGate 6. Руководство администратора .

Параметры отказоустойчивого кластера:

Наименование	Описание
Вкл	Включение/отключение отказоустойчивого кластера.
Название	Название отказоустойчивого кластера.
Описание	Описание отказоустойчивого кластера.
Режим кластера	Режим отказоустойчивого кластера: Актив-Актив — нагрузка распределяется на все узлы кластера Актив-Пассив — нагрузка идет на Мастер-узел и переключается на запасной узел в случае недоступности Мастер-узла.
Синхронизировать сессии	Включает режим синхронизации пользовательских сессий между всеми узлами, входящими в кластер отказоустойчивости. Включение данной опции делает переключение пользователей с одного устройства на другое прозрачным для пользователей, но добавляет существенную нагрузку на платформу UserGate. Имеет смысл только для режима кластера Актив-Пассив.
Мультикаст идентификатор кластера	В одном кластере конфигурации может быть создано несколько кластеров отказоустойчивости. Для синхронизации сессий используется определенный мультикастовый адрес, определяемый данным параметром. Для каждой группы кластеров отказоустойчивости, в которой должна поддерживаться синхронизация сессий, требуется установить уникальный идентификатор.

Наименование	Описание
Идентификатор виртуального роутера (VRID)	Идентификатор виртуального роутера должен быть уникален для каждого VRRP-кластера в локальной сети. Если в сети не присутствуют сторонние кластеры VRRP, то рекомендуется оставить значение по умолчанию.
Узлы	Выбираются узлы кластера конфигурации для объединения их в кластер отказоустойчивости. Узлы кластера представлены идентификаторами, назначенными узлам кластера конфигурации при создании кластера конфигурации.
Виртуальные IP-адреса	Назначаются виртуальные IP-адреса и их соответствие интерфейсам узлов кластера. В качестве интерфейсов могут быть использованы только интерфейсы, которые были созданы в одном из шаблонов UGMC.

Управление обновлениями управляемых устройств

UserGate Management Center позволяет создать централизованную политику обновления программного обеспечения UserGate (UGOS) и обновляемыми библиотеками, предоставляемыми по подписке (база категорий URL-фильтрации, COB, списки IP-адресов, URL, типов контента и другие).

Примечание После добавления МЭ UserGate под управление UGMC, устройство UserGate автоматически начинает скачивать все обновления с сервера UGMC.

Для управления обновлениями с помощью UGMC необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Настроить расписание проверки обновлений	Расписание проверки устанавливает время и периодичность проверки обновлений. Оно может быть настроено локально на каждом из устройств UserGate, либо централизованно с помощью настройки шаблонов в UGMC. В обоих случаях настройка выполняется идентично. В случае локальной настройки она производится в разделе Общие настройки в веб-консоли управления устройством. В случае настройки через UGMC настройка производится в одном из шаблонов в разделе Общие настройки . Подробнее о настройке расписания обновлений смотрите главу Общие настройки документа UserGate 6. Руководство администратора .
Шаг 2. Настроить политику обновления ПО для устройств UserGate	Политика обновлений ПО позволяет задать обновление, доступное для установки на все или выборочные УО. Подробнее об обновлениях ПО смотрите в разделе Обновление ПО .
Шаг 3. Настроить политику обновления библиотек для устройств UserGate	Политика обновления библиотек позволяет выбрать необходимые обновления библиотек для установки на УО. Подробнее об обновлениях библиотек смотрите в разделе Обновление библиотек .

Обновление ПО

Компания UserGate периодически выпускает обновления программного обеспечения МЭ UserGate. Эти обновления выкладываются в репозиторий UserGate (<http://static.usergate.com>), откуда они уже доступны для скачивания МЭ. Если МЭ UserGate подключен к управлению через Management Center, то он проверяет наличие обновлений на сервере Management Center, который сам будет являться репозитарием. Репозиторий UserGate при этом будет использован сервером UGMC для получения новых обновлений.

В некоторых случаях служба поддержки UserGate может рекомендовать к установке определенным клиентам специфические обновления, недоступные для скачивания из репозитория. Такие обновления следует добавлять в UGMC с помощью импорта обновления из файла.

Порядок установки обновлений, следующий:

Наименование	Описание

Наименование	Описание
Шаг 1. Загрузить обновления в репозиторий UGMC	Загрузить обновления можно либо из репозитория UserGate, либо импортировав файл обновления вручную. Для загрузки обновлений из репозитория необходимо в разделе Управление NGFW → Обновления ПО нажать на кнопку Выбрать онлайн-обновления, отобразится список обновлений, доступных для скачивания из репозитория UserGate. Выделить необходимые обновления и нажать кнопку Выбрать. Выделенные обновления будут загружены в UGMC. Для загрузки вручную необходимо в разделе Управление NGFW → Обновления ПО нажать на кнопку Импортировать обновление, выбрать файл с обновлением. Если для файла обновлений в самом обновлении не указаны название и версия обновления, то необходимо указать их в соответствующих полях. Кнопка Сохранить загрузит выбранное обновление в UGMC.
Шаг 2. Утвердить обновление для всех или для конкретных устройств	Для установки обновления на все устройства необходимо выбрать интересующее обновление и нажать на кнопку Утвердить обновление. Только одно обновление может быть утверждено для всех устройств. Если требуется установить данное обновление на группу устройств (например, для проведения тестирования), то необходимо в свойствах обновления указать управляемые устройства, для которых данное обновление будет доступно, и установить чекбокс Утвердить обновление.
Шаг 3. Провести установку обновления	После утверждения обновление становится доступным для скачивания для всех или группы управляемых устройств. УО скачивает обновление в соответствии с расписанием проверки обновлений. После скачивания обновление может быть установлено администратором в консоли МС или в ручном режиме администратором управляемого устройства.

Обновление в репозитории UGMC имеет следующие свойства:

Наименование	Описание
Название	Название обновления. Обычно не доступно для изменения, содержится в коде изменения.
Описание	Произвольное описание обновления.
Версия	Версия обновления. Не доступно для изменения, содержится в коде изменения.
Размер	Размер обновления.
Версия релиза	Версия релиза UserGate, для которого это обновление выпущено. Не доступно для изменения, содержится в коде изменения.
Статус	Статус обновления, например, скачано.
Прогресс	Показывает прогресс загрузки обновления с репозитория UserGate.
Канал обновлений	Канал обновлений репозитория UserGate: - Стабильные — канал стабильных обновлений ПО. - Бета — канал экспериментальных обновлений.
Список изменений	Ссылка на список изменений, содержащихся в данном обновлении.
Управляемые устройства	Список управляемых устройств, которым назначено данное обновление.
Добавлено	Дата добавления обновления в репозиторий UGMC и имя администратора, который выполнил добавление.
Утверждено	Дата утверждения обновления и имя администратора, который выполнил утверждение.

Обновление библиотек

Библиотеки — это обновляемые базы ресурсов, предоставляемых по подписке клиентам UserGate (база категорий URL-фильтрации, сигнатуры COV, списки IP-адресов, URL, MIME-типов, морфологические базы и другие). Эти обновления выкладываются в репозиторий

UserGate (<http://static.usergate.com>), откуда они уже доступны для скачивания МЭ UserGate. Если МЭ UserGate подключен к управлению через Management Center, то он проверяет наличие обновлений на сервере Management Center, который сам будет являться репозитарием. Репозитарий UserGate при этом будет использован сервером UGMC для получения новых обновлений. По умолчанию UGMC проверяет и скачивает обновления библиотек автоматически.

В случаях, когда UGMC не имеет доступа до репозитария UserGate, имеется возможность импортировать обновление вручную из файла, полученного в личном кабинете клиента UserGate (<https://my.usergate.com>).

Библиотеки, находящиеся в репозитарии UGMC доступны всем управляемым устройствам UserGate. УО скачивают и устанавливают доступные обновления автоматически в соответствии с расписанием проверки обновлений.

Обновление библиотек в репозитарии UGMC имеет следующие свойства:

Наименование	Описание
Название	Название обновления. Не доступно для изменения, содержится в коде изменения.
Описание	Произвольное описание обновления.
Скачивать	Режим скачивания новых версий. По умолчанию установлен режим Автоматически — UGMC автоматически проверяет наличие новых версий в репозитарии UserGate и скачивает их. При выборе режима Ручное — UserGate не обновляет выбранную библиотек в автоматическом режиме.
Размер	Размер обновления.
Версия	Версия обновления библиотеки.
Обновлено	Дата и время последнего обновления конкретной библиотеки.

Управление устройствами LogAn (Описание)

Documentation: ☒

Product: UGMC

Version: 7.0.1, 7.1.0

Централизованное управление устройствами LogAn можно разделить на 4 этапа:

1. Создание управляемой области. Смотрите раздел [Создание управляемых областей](#).
2. Создание шаблона или несколько шаблонов, каждый из которых опишет свою часть настроек LogAn. Смотрите раздел [Шаблоны устройств LogAn](#) для более детальной информации.
3. Объединение необходимых шаблонов в группу шаблонов в требуемом порядке, чтобы получить корректную результирующую настройку управляемых устройств. Смотрите раздел [Группы шаблонов LogAn](#) для более детальной информации.
4. Добавление управляемого устройства LogAn и применения к нему группы шаблонов. Смотрите раздел [Добавление устройств LogAn под управление UGMC](#) для более детальной информации.

При необходимости настройки, заданные в шаблонах, можно изменять, чтобы эти отражения применялись ко всем управляемым устройствам LogAn, к которым применимы данные шаблоны.

Шаблоны устройств LogAn

Шаблон — это базовый блок, с помощью которого можно настроить все параметры работы межсетевого экрана — сетевые настройки, правила межсетевого экрана, контентной фильтрации, системы обнаружения вторжений и других. Для создания шаблона необходимо в разделе **LogAn → 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 **LogAn-конфигурация** и в выпадающем меню **Выберите шаблон** выбрать необходимый шаблон.

Настройки параметров шаблона отображаются в виде дерева, полностью аналогично, как они представлены в LogAn. При настройке параметров следует придерживаться следующих правил:

1. Если значение настройки не определено в шаблоне, то ничего передаваться в LogAn не будет. В данном случае в LogAn будет использована либо настройка по умолчанию, либо настройка, которую указал локальный администратор.
2. Если настройка параметра выполнена в шаблоне, то эта настройка переопределит значение этой же настройки, назначенной локальным администратором.

После получения настроек с Management Center настройки следующих разделов могут быть изменены локально на Log Analyzer:

- общие настройки устройства: вкладка **Настройки**, раздел **Консоль администратора → Настройки**;
- настройки сетевых интерфейсов: вкладка **Настройки**, раздел **Сеть → Интерфейсы**.

Примечание Настройка будет переопределена после изменения данной настройки в шаблоне LogAn администратором области на UGMC.

3. При настройке сетевых интерфейсов первый физический интерфейс, доступный для конфигурирования — это **port1**. Интерфейс **port0** нельзя настроить с помощью средств UGMC, он всегда настраивается локальным администратором и необходим для обеспечения первичной связи управляемого устройства с UGMC.
4. При настройке сетевых интерфейсов возможно создать интерфейс и оставить его конфигурирование локальному администратору. Для этого необходимо поставить флаг **Настраивается на устройстве** в настройках сетевого интерфейса.
5. В некоторых настройках и правилах политик доступна опция применения данного правила или настройки только к конкретному устройству. Для этого необходимо выбрать управляемое устройство в свойствах правила/настройки в закладке **Управляемые устройства**. Хотя это и предоставляет определенную гибкость, следует избегать чрезмерного использования данной опции, поскольку это приводит к сложности понимания применения настроек к группам устройств LogAn.
6. Библиотеки, например, такие как IP-адреса, списки URL, типы контента и другие, по умолчанию не содержат никакого контента в UGMC в отличие от библиотек, создаваемых по умолчанию на устройствах UserGate. Для использования библиотек в политиках UGMC, необходимо предварительно добавить элементы в эти библиотеки.
7. 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. Например, шаблон сетевых настроек, шаблон библиотек и т.д.

Группы шаблонов LogAn

Группы шаблонов объединяют несколько шаблонов в единую конфигурацию, которая применяется к управляемому устройству. Результирующие настройки, применяемые к устройству LogAn, 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 **LogAn → 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 устройств LogAn под управление UGMC

Группа шаблонов всегда применяется к одному или нескольким управляемым устройствам LogAn. Процедура добавления управляемых устройств в UGMC состоит из следующих шагов:

Наименование	Описание
Шаг 1. Обеспечить доступ от управляемого устройства до UGMC.	На сервере UGMC необходимо разрешить сервис UserGate Management Center на зоне, к которой подключены управляемые устройства. Сервер UGMC слушает подключения от управляемого устройства на портах TCP 2022 и 9712. Передача данных между сервером UGMC и управляемым устройством осуществляется по зашифрованному каналу.
Шаг 2. Создать объект управляемого устройства LogAn.	В консоли управления областью в разделе LogAn → Устройства нажать кнопку Добавить и указать необходимые настройки.
Шаг 3. Связать созданный объект управляемого устройства LogAn с реальным устройством LogAn.	В консоли управления LogAn настройте связь между UGMC и устройством. Данную операцию можно произвести в момент первоначальной установки LogAn либо уже на настроенном устройстве LogAn. Оба варианта подробно описаны далее в этой главе.

При создании объекта управляемого устройства LogAn необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает объект управляемого устройства . Если объект управляемого устройства включен, то он занимает одну лицензию.
Название	Название для управляемого устройства . Можно вводить произвольное название.
Описание	Описание управляемого устройства.
Группа шаблонов	Группа шаблонов, настройки которой следует применить к этому управляемому устройству .
Синхронизация	Выбор режима синхронизации настроек группы шаблонов к устройству. Возможны 3 варианта: • Автоматическая синхронизация — настройки применяются к устройству автоматически. При изменении любой настройки из любого шаблона, включенного в группу шаблонов, примененную к управляемому устройству, это изменение применяется к LogAn без задержек. • Отключено — синхронизация выключена. • Ручная синхронизация — режим синхронизации, при котором настройки применяются при нажатии кнопки Запросить синхронизацию. 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. Вне зависимости от выбранного режима доступен запуск синхронизации всех настроек для выбранных устройств (раздел LogAn → Устройства кнопка Действия → Запустить полную синхронизацию).

Для осуществления связи LogAn с UGMC во время первоначальной настройки необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Скопировать Код устройства.	В UGMC выбрать созданный объект управляемого устройства и нажать Действия → Показать уникальный код устройства . Скопировать данный код в буфер обмена.
Шаг 2. На LogAn в момент первоначальной инициализации выбрать установку с помощью UGMC.	В момент первоначальной инициализации на этапе задания имени администратора и его пароля необходимо выбрать ссылку Настроить через UGMC .

Наименование	Описание
Шаг 3. Указать необходимые настройки нового узла и ввести уникальный код устройства.	Указать следующие параметры: - Сетевые настройки данного LogAn (IP, маска, шлюз). Данные настройки будут применены к указанному интерфейсу. Необходимо, чтобы после задания сетевых настроек появилась сетевая доступность с этого устройства до сервера UGMC. - Имя локального администратора и его пароль. - IP-адрес сервера UGMC и уникальный код устройства, сохраненный на первом шаге.
Шаг 4. Проверить подключение.	После подключения к UGMC LogAn должен получить все настройки, подготовленные для него в UGMC. В LogAn настройки отображаются со значком замочка, означающим, что данную настройку локальный администратор не может изменять. В консоли UGMC в объекте управляемого устройства появится дополнительная информация о подключенном устройстве, такая как ПИН-код, серийный номер, информация о лицензии, используемой памяти и т.п.

Для осуществления связи уже настроенного устройства LogAn с UGMC необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Скопировать Код устройства.	В UGMC выбрать созданный объект управляемого устройства и нажать на кнопку Действия → Показать уникальный код устройства . Скопировать данный код в буфер обмена.
Шаг 2. Указать IP-адрес сервера UGMC и ввести уникальный код устройства.	В разделе Настройки → Агент UGMC выбрать Настроить , указать IP-адрес сервера UGMC, вставить уникальный код устройства и включить данное подключение. Для успешного выполнения данного шага необходимо, чтобы была сетевая доступность с этого LogAn до сервера UGMC.
Шаг 3. Проверить подключение.	После подключения к UGMC LogAn должен получить все настройки, подготовленные для него в UGMC. В LogAn настройки отображаются со значком замочка, означающим, что данную настройку локальный администратор не может изменять. В консоли UGMC в объекте управляемого устройства появится дополнительная информация о подключенном устройстве, такая как ПИН-код, серийный номер, информация о лицензии, используемой памяти и т.п.

После того, как LogAn успешно добавлен в UGMC администратор может редактировать, включать/отключать, удалять управляемое устройство, а также:

Наименование	Описание
Посмотреть расширенную информацию о состоянии управляемого устройства	В консоли UGMC необходимо выбрать объект управляемого устройства и нажать на кнопку Показать детальную информацию. Будет отображена следующая информация о подключенном управляемом устройстве: - Версия ПО управляемого устройства. - ПИН-код управляемого устройства. - Серийный номер ПАК. - Время непрерывной работы. - Показатели загрузки устройства — загрузка ЦП, оперативной памяти, своп-файла.
Подключиться к консоли управляемого устройства	В консоли UGMC необходимо выбрать объект управляемого устройства и нажать Действия → Открыть консоль . В новом окне откроется консоль LogAn.
Изменить настройки	В консоли UGMC измените настройки одного из шаблонов, входящего в группу шаблонов, примененного к управляемому устройству. Новые настройки будут применены к LogAn.

В веб-интерфейсе UserGate Management Center администратор может производить фильтрацию, отображая:

- все устройства;
- включенные/выключенные устройства;

- устройства онлайн (подключенные к UGMC)/офлайн (неподключенные к UGMC)/не привязанные устройства (устройства, которые еще не были подключены к UGMC);
- консистентные (синхронизация управляемого устройства завершилась успешно)/неконсистентные (при синхронизации конфигурации управляемого устройства возникли ошибки) устройств.

Управление обновлениями управляемых устройств LogAn

UGMC позволяет создать централизованную политику обновления программного обеспечения UserGate (UGOS) и обновляемыми библиотеками, предоставляемыми по подписке (база категорий URL-фильтрации, COB, списки IP-адресов, URL, MIME-типов и другие).

ПримечаниеПосле добавления управляемого устройства LogAn под управление UGMC, устройство автоматически начинает скачивать все обновления с сервера UGMC.

Для управления обновлениями с помощью UGMC необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Настроить расписание проверки обновлений.	Расписание проверки устанавливает время и периодичность проверки обновлений. Оно может быть настроено локально на каждом из устройств LogAn либо централизовано с помощью настройки шаблонов в UGMC. В обоих случаях настройка выполняется идентично. В случае локальной настройки она производится в разделе Настройки в веб-консоли управления устройством. В случае настройки через UGMC настройка производится в одном из шаблонов в разделе Настройки .
Шаг 2. Настроить политику обновления ПО для устройств LogAn.	Политика обновлений ПО позволяет задать обновление, доступное для установки на все или выборочные управляемые устройства. Подробно об обновлениях ПО смотрите в разделе Обновление ПО LogAn .
Шаг 3. Настроить политику обновления библиотек для устройств LogAn.	Политика обновления библиотек позволяет выбрать необходимые обновления библиотек для установки на управляемое устройство. Подробно об обновлениях библиотек смотрите в разделе Обновление библиотек LogAn .

Обновление ПО LogAn

Компания UserGate периодически выпускает обновления программного обеспечения UserGate LogAn. Эти обновления выкладываются в репозиторий UserGate (<https://static.usergate.com>), откуда они уже доступны для скачивания LogAn. Если UserGate LogAn подключен к управлению через Management Center, то он проверяет наличие обновлений на сервере Management Center, который сам будет являться репозитарием. Репозитарий UserGate при этом будет использован сервером UGMC для получения новых обновлений.

В некоторых случаях служба поддержки UserGate может рекомендовать к установке определенным клиентам специфические обновления, недоступные для скачивания из репозитария. Такие обновления следует добавлять в UGMC с помощью импорта обновления из файла.

Порядок установки обновлений следующий:

Наименование	Описание
Шаг 1. Загрузить обновления в репозитарий UGMC.	Загрузить обновления можно либо из репозитария UserGate, либо импортировав файл обновления вручную. Для загрузки обновлений из репозитария необходимо в разделе LogAn → Обновление ПО нажать на кнопку Выбрать онлайн-обновления , отобразится список обновлений, доступных для скачивания из репозитария UserGate. Выделить необходимые обновления и нажать кнопку Выбрать . Выделенные обновления будут загружены в UGMC. Для загрузки вручную необходимо в разделе LogAn → Обновление ПО нажать на кнопку Импортировать обновление , выбрать файл с обновлением. Если для файла обновлений в самом обновлении не указаны название и версия обновления, то необходимо указать их в соответствующих полях. Кнопка Сохранить загрузит выбранное обновление в UGMC.
Шаг 2. Утвердить обновление для всех или для конкретных устройств.	Для установки обновления на все устройства необходимо выбрать интересующее обновление и нажать на кнопку Утвердить обновление . Только одно обновление может быть утверждено для всех устройств. Если требуется установить данное обновление на группу устройств (например, для проведения тестирования), то необходимо в свойствах обновления указать управляемые устройства, для которых данное обновление будет доступно, и установить флаг Утвердить обновление .

Наименование	Описание
Шаг 3. Провести установку обновления.	После утверждения обновление становится доступным для скачивания для всех или группы управляемых устройств. Управляемое устройство скачивает обновление в соответствии с расписанием проверки обновлений. После скачивания обновление может быть установлено администратором в консоли UGMC или в ручном режиме администратором управляемого устройства.

Обновление в репозитории UGMC имеет следующие свойства:

Наименование	Описание
Название	Название обновления. Обычно не доступно для изменения, содержится в коде изменения.
Описание	Произвольное описание обновления.
Версия	Версия обновления. Не доступно для изменения, содержится в коде изменения.
Размер	Размер обновления.
Версия релиза	Версия релиза LogAn, для которого это обновление выпущено. Не доступно для изменения, содержится в коде изменения.
Статус	Статус обновления, например, скачено.
Прогресс	Показывает прогресс загрузки обновления с репозитория UserGate.
Канал обновлений	Канал обновлений репозитория UserGate: • Стабильные — канал стабильных обновлений ПО. • Бета — канал экспериментальных обновлений.
Список изменений	Ссылка на список изменений, содержащихся в данном обновлении.
Управляемые устройства	Список управляемых устройств, которым назначено данное обновление.
Добавлено	Дата добавления обновления в репозиторий UGMC и имя администратора, который выполнил добавление.
Утверждено	Дата утверждения обновления и имя администратора, который выполнил утверждение.

Обновление библиотек LogAn

Библиотеки — это обновляемые базы ресурсов, предоставляемых по подписке клиентам UserGate (база категорий URL-фильтрации, сигнатуры COB, списки IP-адресов, URL, MIME-типов, морфологические базы и другие). Эти обновления выкладываются в репозиторий UserGate (<https://static.usergate.com>), откуда они уже доступны для скачивания LogAn. Если LogAn подключен к управлению через Management Center, то он проверяет наличие обновлений на сервере Management Center, который сам будет являться репозитарием. Репозиторий UserGate при этом будет использован сервером UGMC для получения новых обновлений. По умолчанию UGMC проверяет и скачивает обновления библиотек автоматически.

В случаях, когда UGMC не имеет доступа до репозитория UserGate, имеется возможность импортировать обновление вручную из файла, полученного в личном кабинете клиента UserGate (<https://my.usergate.com>).

Библиотеки, находящиеся в репозитории UGMC доступны всем управляемым устройствам LogAn. Управляемые устройства скачивают и устанавливают доступные обновления автоматически в соответствии с расписанием проверки обновлений.

Обновление библиотек в репозитории UGMC имеет следующие свойства:

Наименование	Описание
Название	Название обновления. Не доступно для изменения, содержится в коде изменения.

Наименование	Описание
Описание	Произвольное описание обновления.
Скачивать	Режим скачивания новых версий. По умолчанию установлен режим Автоматически — UGMC автоматически проверяет наличие новых версий в репозитории UserGate и скачивает их. При выборе режима Ручное — UserGate не обновляет выбранную библиотек в автоматическом режиме.
Размер	Размер обновления.

Управление конечными устройствами UserGate Client (Описание)

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.

Наименование	Описание
Policy	Просмотр информации о безопасности конечного устройства (статус межсетевого экрана, антивируса, центров обновления и безопасности Windows). Значение индикации: • Жёлтый - выключен. • Зелёный - включен.
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.

Шаблоны управляемых устройств UGC

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 это 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 "*/2" 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.

Группы шаблонов управляемых устройств UGC

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 установке 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, продолжают 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.

Управление устройством UGC из консоли 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.

Сбор и анализ данных с устройств UGC

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 МС 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.

Наименование	Описание
Запущенные службы	Проверка служб, запущенных на конечном устройстве.
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.

Описание форматов журналов

Documentation: ☒
Product: UGMC
Version: 7.0.1

Формат журнала событий

CEF

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта	7
	Source	Тип журнала.	events
	Origin	Модуль, в котором произошло событие	admin_console
	Severity	Важность события	Может принимать значения: • 0 — информационные; • 6 — предупреждения; • 8 — ошибки; • 10 — критичные.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	mc_core@einsonstal
	suser	Имя пользователя	Administrator (Admin)
	cat	Компонент, в котором произошло событие	console_auth
	act	Тип события	administrator_login
	src	IPv4-адрес источника	192.168.117.254
	cs1Label	Поле используется для указания деталей события	Attributes
	cs1	Детали события в формате JSON	{"login":"ex_admin","realm_id":"31d8fcb6-e51d-4e3f-b799-181d31a45b06"}

JSON

Название поля	Описание	Пример значения
user	Имя пользователя	Admin

Название поля	Описание	Пример значения
timestamp	Время получения события в формате: уууу-mm-ddThh:mm:ssZ	2022-05-12T08:11:46.15869Z
ip_address	IPv4-адрес источника события	192.168.174.134
node	Имя, которое однозначно идентифицирует устройство, генерирующее это событие	mc_core@einersonstal
attributes	Детали события в формате JSON	{"rule":{"logrotate":12,"attributes":{"timezone":"Asia/Novosibirsk"},"id":"66f9de9f-d698-4bec-b3b0-ba65b46d3608"},"name":"Example log export ftp"}
event_type	Тип события	logexport_rule_updated
event_severity	Важность события	info (информационные), warning (предупреждения), error (ошибки), critical (критичные).
event_origin	Модуль, в котором произошло событие	core
event_component	Компонент, в котором произошло событие	console_auth

Требования к сетевому окружению

Documentation: ☒

Product: UGMC

Version: 7.0.1

Сервис	Протокол	Порт	Исходящий/Входящий	Функция
Веб-консоль	TCP	8010	Входящий (до веб-консоли UserGate Management Center)	Доступ к веб-интерфейсу управления устройством
	TCP	8300	Входящий (до веб-консоли UserGate NGFW, подключённого к UGMC)	Доступ к веб-интерфейсу управления UG NGFW, подключённого к UGMC
CLI по SSH	TCP	2200	Входящий (к CLI по SSH)	Доступ к интерфейсу командной строки (CLI) UserGate по протоколу SSH
XML-RPC	TCP	4041	Входящий (к UserGate по API)	Управление устройством UserGate по API
Удалённый помощник	TCP	22	Исходящий (до серверов технической поддержки)	Удалённый доступ к серверу технической поддержки Доступ к серверам: 93.91.171.46; 178.154.221.222; - ra.entensys.com.
NTP	UDP	123	Исходящий (до сервера точного времени)	Синхронизация времени
DNS	UDP	53	Исходящий (от UserGate до DNS-сервера)	Сервис получения информации (IP-адрес) о доменах
Регистрация сервера UserGate	TCP	443	Исходящий (до сервера регистрации)	Доступ до сервера регистрации продуктов UserGate reg2.usergate.com
Обновление ПО и библиотек	TCP	443	Исходящий (до серверов обновления)	Обновление программного обеспечения и элементов библиотек: доступ до сервера updates.usergate.com
Репликация настроек	TCP	4369	Входящий (с первого узла кластера на второй и последующие узлы)	Сервис, необходимый для работы кластера конфигурации; Установка управляющего соединения.
		9000-9100	Входящий (приём конфигурации от первого узла кластера)	Передача информации об изменении конфигурации кластера (реплика настроек)
Сервис UserGate Management Center	TCP	9712	Входящий (к UGMC от NGFW)	Первоначальная установка связи и обмен ключами шифрования управляемых устройств и сервера UserGate Management Center
		2022	Входящий (к UGMC от NGFW)	Построение SSH-туннеля для обмена данными с помощью полученных ключей
		9712	Входящий (к UGMC от UG Client)	Первоначальная установка связи и обмен ключами шифрования управляемых устройств UserGate Client и сервера UserGate Management Center

Контроль конечных устройств (начиная с версии 7.1.0)	TCP	Порт	Исходящий/Входящий	Функция
		4045	Входящий (к UGMC от UG Client)	Построение SSL-туннеля для обмена данными с помощью ключей, полученных при установке связи
		22000-22711	Входящий (к UGMC от UG Client)	Передача журналов и телеметрии с UG Client на UG LogAn транзитом через UGMC
LDAP	TCP	389, 636	Исходящий (на LDAP-коннектор)	Выполнение запросов LDAP (389 - для LDAP и 636 - для LDAP over SSL)
SNMP	UDP	161	Входящий (до UserGate)	Доступ к серверу UserGate по протоколу SNMP
SMTP	TCP	25	Исходящий (до почтового сервера)	Отправка уведомлений на электронную почту
DHCP	UDP	67, 68	Исходящий (запрос на получение адреса от UserGate на сервер DHCP)	Сервис службы DHCP
FTP (экспорт журналов) (начиная с версии 7.1.0)	TCP	21	Исходящий (до сервера FTP)	Экспорт журналов на сервер FTP
SSH (экспорт журналов) (начиная с версии 7.1.0)	TCP	22	Исходящий (до сервера SSH)	Экспорт журналов на сервер SSH
Syslog (экспорт журналов) (начиная с версии 7.1.0)	TCP/UDP	514	Исходящий (до сервера Syslog)	Экспорт журналов на сервер Syslog
Ручная проверка сайтов по категориям	TCP	80/443	Исходящий (до updates.usergate.com)	Ручная проверка сайтов по категориям

