

UserGate Management Center

Руководство администратора

Оглавление

1	Принятые обозначения и сокращения	4
2	Введение	5
2.1	Управляемые области	5
2.2	Шаблоны и группы шаблонов	6
2.3	Управляемые устройства	8
2.4	Управление UserGate Management Center	8
2.4.1	Управление сервисами UGMC	8
2.4.2	Управление областями UGMC	8
2.4.3	Ролевое управление	9
3	Лицензирование UserGate Management Center	11
4	Планирование внедрения UserGate Management Center	12
4.1	Один шаблон и одна группа шаблонов на каждое управляемое устройство	12
4.2	Набор шаблонов с настройками каждого модуля. Специфичные настройки для некоторых модулей для определенной группы УУ. Сеть настраивается локально	13
4.3	Набор шаблонов с настройками каждого модуля. Специфичные настройки для некоторых модулей для определенной группы УУ UG. Сеть настраивается через UGMC	14
5	Первоначальная настройка	16
5.1	Развертывание программно-аппаратного комплекса	16
5.2	Развертывание виртуального образа	16
5.3	Подключение к UserGate Management Center	17
6	Настройка UserGate Management Center	19
6.1	Общие настройки	19
6.2	Управление устройством	19
6.2.1	Кластеризация и отказоустойчивость	19
6.2.2	Диагностика	23
6.2.3	Операции с сервером	24
6.2.4	Экспорт настроек	25
6.3	Администраторы	26
6.4	Управление сертификатами	29
6.5	Профили оповещений	30
6.6	Серверы авторизации UserGate Management Center	32
7	Офлайн операции с сервером	33
8	Настройка сети	35
8.1	Настройка зон	35
8.2	Настройка интерфейсов	36
8.2.1	Объединение интерфейсов в бонд	37
8.3	Настройка шлюзов	39
8.4	Маршруты	40
9	Интерфейс командной строки (CLI)	41

10 Управление областями.....	44
10.1 Создание управляемых областей	44
10.2 Администраторы области.....	45
10.3 Серверы авторизации области.....	46
11 Управление межсетевыми экранами UserGate	48
11.1 Шаблоны устройств.....	48
11.2 Группы шаблонов	49
11.3 Добавление устройств UserGate под управление UGMC.....	49
11.4 Кластеризация МЭ UserGate с помощью UserGate Management Center	52
11.4.1 Кластер конфигурации	52
11.4.2 Кластер отказоустойчивости.....	53
11.5 Управление обновлениями управляемых устройств	55
11.5.1 Обновление ПО	56
11.5.2 Обновление библиотек	57
12 Управление устройствами UserGate LogAn.....	59
12.1 Шаблоны устройств LogAn.....	59
12.2 Группы шаблонов LogAn	60
12.3 Добавление устройств LogAn под управление UGMC	60
12.4 Управление обновлениями управляемых устройств LogAn	63
12.4.1 Обновление ПО LogAn.....	63
12.4.2 Обновление библиотек LogAn.....	65
13 Управление конечными устройствами UserGate Client	66
13.1 Шаблоны устройств УУ UGC	66
13.1.1 Настройки	67
13.1.2 Политики сети.....	67
13.1.3 Библиотеки элементов	69
13.2 Группы шаблонов УУ UGC	74
13.3 Установка ПО UserGate Client.....	75
13.4 Добавление устройств УУ UGC под управление UGMC	75
13.4.1 Процесс единичного добавления устройств	75
13.4.2 Процесс массового добавления устройств	76
13.5 Управление устройством UGC из консоли UGMC	77
13.6 Сбор и анализ данных с устройств UGC.....	79
13.6.1 Журнал событий конечных устройств.....	80
13.6.2 Журнал правил конечных устройств	82
13.6.3 Приложения конечных устройств	84
13.6.4 Режим расширенного поиска.....	86
13.7 Управление обновлениями УУ UGC.....	87
13.7.1 Обновление ПО UserGate Client	88
13.7.2 Обновление библиотек UserGate Client	89

1 ПРИНЯТЫЕ ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

Сокращение	Значение
UGMC	UserGate Management Center.
МЭ	Межсетевой экран UserGate.
ПАК	Программно-аппаратный комплекс.
SU	Модуль лицензирования Security Update.
УО	Управляемая область.
УУ	Управляемое устройство.
УУ UG	Управляемое устройство МЭ UserGate.
УУ UGC	Конечное управляемое устройство, пользовательский компьютер под управлением операционной системы Windows с установленным ПО UserGate Client.
УУ LogAn	Управляемое устройство UserGate Log Analyzer.
ПО	Программное обеспечение.
ЦП	Центральный процессор.

2 ВВЕДЕНИЕ

UserGate Management Center (UGMC) – это продукт, который позволяет контролировать большое количество управляемых устройств. Управляемым устройством может служить межсетевой экран UserGate (УУ UG), устройство сбора и анализа данных UserGate LogAn (УУ LogAn) или пользовательское конечное устройство под управлением операционной системы Windows с установленным ПО UserGate Client (УУ UGC).

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, устройств сбора и анализа данных UserGate LogAn и пользовательских конечных устройств. 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.

2.1 Управляемые области

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 в одной организации достаточно создать одну управляемую область.

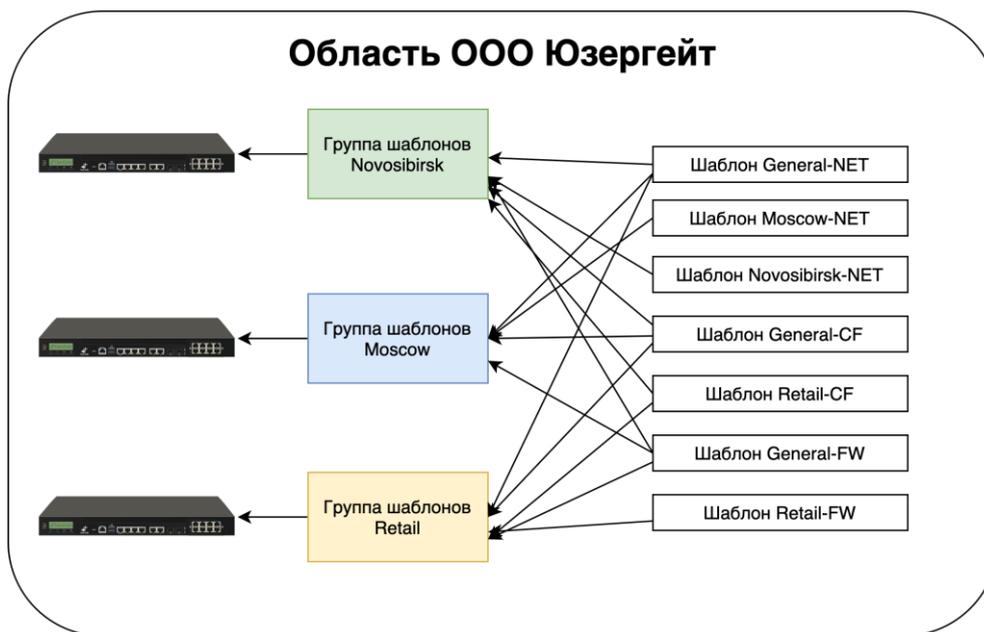
Настройки параметров устройств UserGate производятся внутри управляемой области с помощью шаблонов и групп шаблонов.

2.2 Шаблоны и группы шаблонов

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:



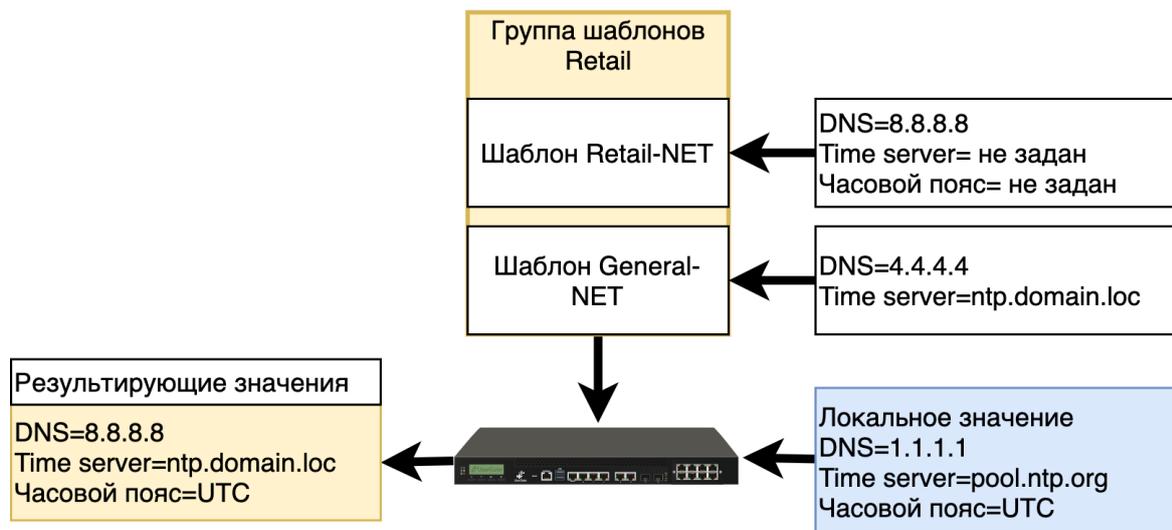
Конфигурация, передаваемая на устройство, может быть двух типов:

- 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.

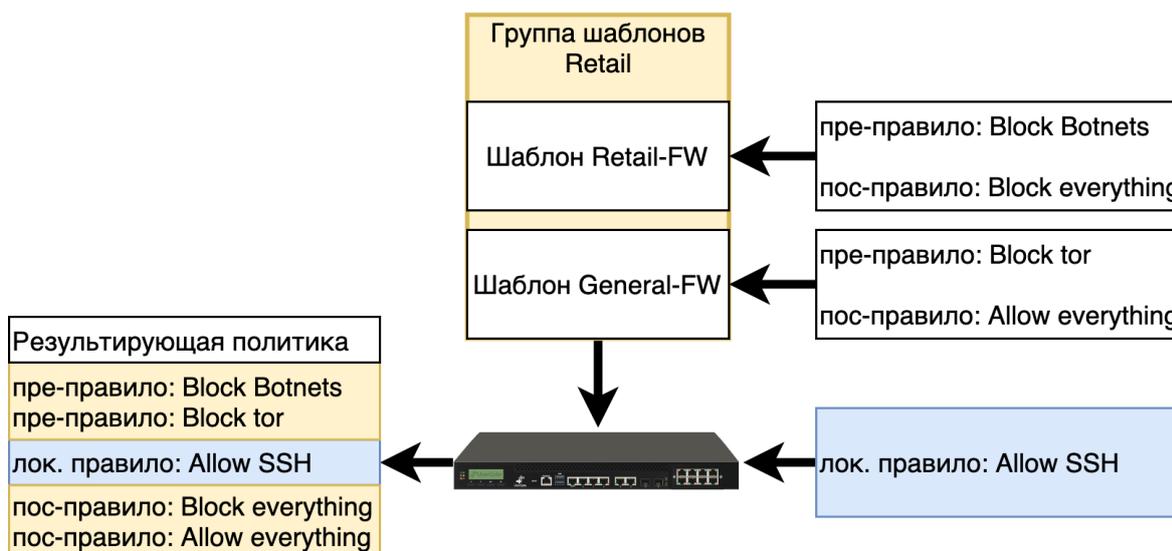
Настройка параметра при конфликтующих значениях в разных шаблонах одной группы шаблонов принимает значение, заданное в наиболее верхнем шаблоне. Локально указанные настройки данного параметра игнорируются.

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:



2.3 Управляемые устройства

Группа шаблонов всегда применяется к одному или нескольким устройствам UserGate. МЭ UserGate, UserGate LogAn и управляемые устройства UserGate Client являются конечными управляемыми устройствами (УУ) в терминологии UserGate Management Center.

2.4 Управление UserGate Management Center

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

2.4.1 Управление сервисами UGMC

Управление сервисами UGMC включает в себя следующие задачи:

Наименование	Описание
Настройка UGMC	<ul style="list-style-type: none">• Назначение IP-адресов.• Конфигурирование зон.• Задание DNS-серверов.• Создание подключений к серверам LDAP.• Настройка оповещений.• Создание дополнительных администраторов UGMC с необходимым уровнем полномочий. <p>Все эти настройки влияют только на функционирование самого сервиса UGMC и не влияют на администрирование управляемых областей.</p>
Лицензирование	Лицензирование продукта (ввод ПИН-кода и регистрация продукта), а также опциональное назначение количества управляемых устройств каждой управляемой области. Если ограничение 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.

2.4.2 Управление областями UGMC

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

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

Создание дополнительных администраторов области	При создании управляемой области ей 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 авторизации	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.
Добавление управляемых устройств	Добавление управляемых устройств в UGMC и назначению им групп шаблонов.

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

3 ЛИЦЕНЗИРОВАНИЕ USERGATE MANAGEMENT CENTER

UserGate Management Center лицензируется по количеству активных управляемых МЭ UserGate. При достижении максимального количества МЭ в UGMC, добавление нового МЭ станет невозможным. Учитываются только активные МЭ, 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)	<p>Модуль SU дает право на получение:</p> <ul style="list-style-type: none">• обновлений ПО UGMC• технической поддержки. <p>Модуль выписывается на 1 год, по истечении данного срока для получения обновлений ПО и технической поддержки необходимо приобрести продление лицензии.</p>

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**.

4 ПЛАНИРОВАНИЕ ВНЕДРЕНИЯ USERGATE MANAGEMENT CENTER

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:

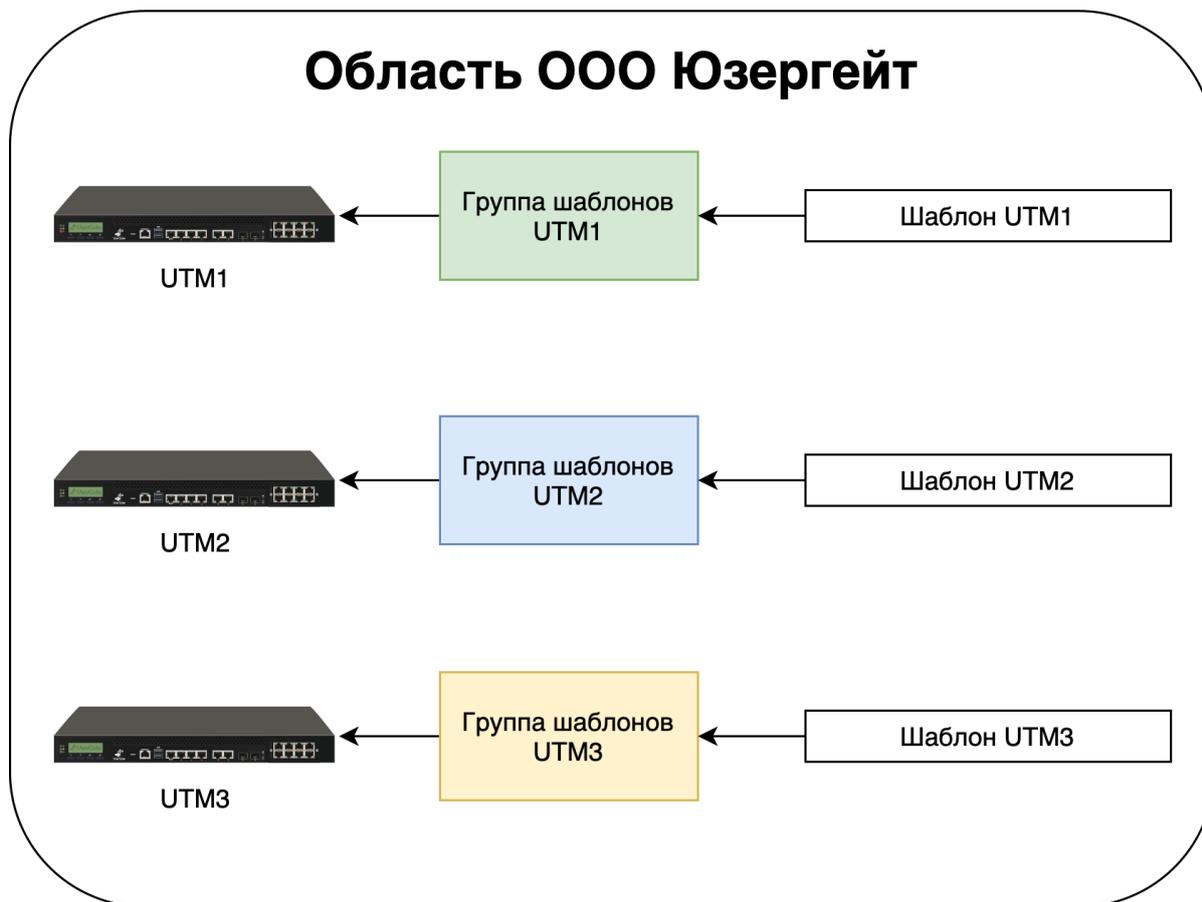
- Избегать конфликта настроек при добавлении шаблонов в группы шаблонов. Наличие конфликтов всегда усложняет управление конечными УУ. Это основополагающий принцип, из которого вытекают следующие рекомендации.
- Разделять различные группы настроек в разные шаблоны, например, общие настройки УУ в одном, политики контентной фильтрации в другом, политики межсетевого экранирования в третьем, политики СОВ 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 УУ, 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 MC для управления МЭ UserGate. Планирование внедрения UGMC для управления устройствами UserGate Client производится аналогично.

4.1 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.

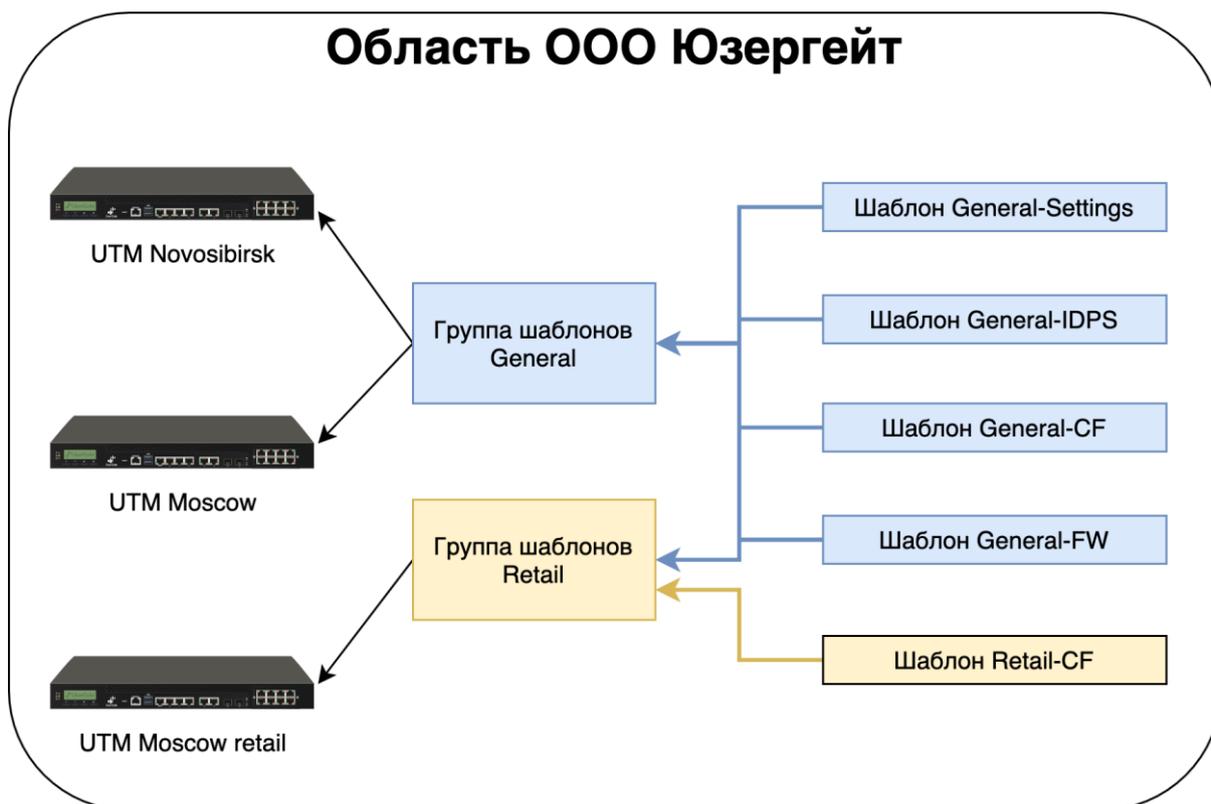
Рекомендуется для простых внедрений с небольшим количеством МЭ UserGate. Пример такой настройки представлен на рисунке ниже.



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

Настройки разбиты по шаблонам, каждый из которых отвечает за настройки специфического модуля, что позволяет избежать конфликта настроек. Суммарно все шаблоны формируют централизованно управляемую политику, применяемую ко всем УУ в компании. Для специфических УУ УГ, 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:

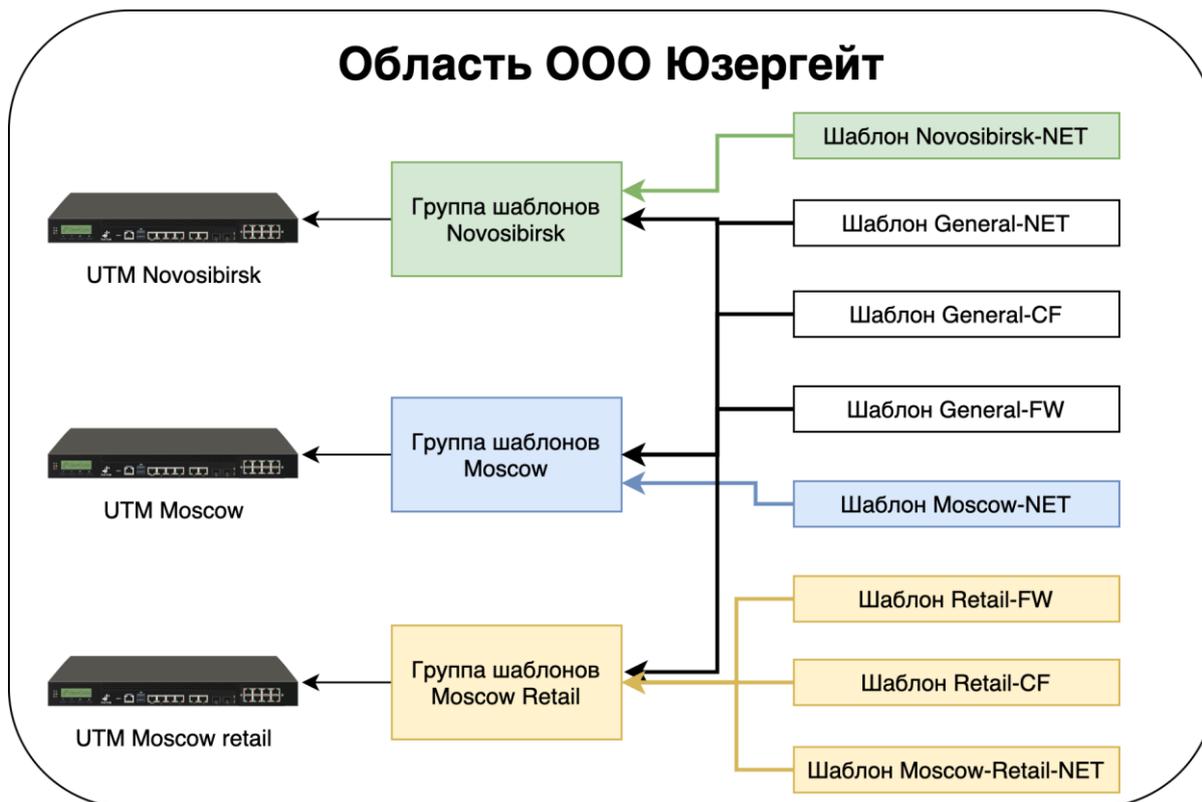
- Шаблон General-Settings - общие для всех настройки (time zone, уровень журналирования, сервера DNS, и т.п.).
- Шаблон General-IDPS - общие для всех политики системы обнаружения вторжений.
- Шаблон General-CF - общие для всех политики контентной фильтрации.
- Шаблон General-FW - общие для всех политики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

4.3 Набор шаблонов с настройками каждого модуля. Специфичные настройки для некоторых модулей для определенной группы УУ 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 межсетевое 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.

5 ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА

UserGate Management Center 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 UserGate Management Center поставляется с двумя Ethernet-интерфейсами. В случае поставки в виде ПАК UserGate Management Center может содержать 8 или более Ethernet-портов.

5.1 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 UserGate Management Center](#) для дальнейшей настройки.

5.2 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.

<p>Шаг 5. Настройте виртуальные сети.</p>	<p>UserGate Management Center поставляется с двумя интерфейсами, назначенными в зоны:</p> <ul style="list-style-type: none"> • Management - первый интерфейс виртуальной машины. • Trusted - второй интерфейс виртуальной машины, предназначенный для связи с управляемыми МЭ UserGate.
<p>Шаг 6. Выполните сброс к заводским настройкам.</p>	<p>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 полного размера диска, увеличенного в 4-м пункте.</p>

5.3 Подключение к UserGate Management Center

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
<p>Шаг 1. Подключиться к интерфейсу управления.</p>	<p>При наличии DHCP-сервера</p> <p>Подключить интерфейс port0 в сеть предприятия с работающим DHCP-сервером. Включить сервер UGMC UserGate. После загрузки консоль UserGate укажет IP-адрес, на который необходимо подключиться для дальнейшей активации продукта.</p> <p>Статический IP-адрес</p> <p>Включить сервер UGMC UserGate. Используя CLI (Command Line Interface), назначить необходимый IP-адрес на интерфейс port0. Детали использования CLI смотрите в главе Интерфейс командной строки (CLI).</p> <p>Подключиться к веб-консоли UGMC UserGate по указанному адресу, он должен выглядеть примерно следующим образом:</p> <p>https://UserGate_CC_IP_address:8010</p>
<p>Шаг 2. Выбрать язык.</p>	<p>Выбрать язык, на котором будет продолжена первоначальная настройка.</p>
<p>Шаг 3. Задать пароль корневого администратора UserGate Management Center.</p>	<p>Задать логин и пароль для входа в веб-интерфейс управления.</p>

<p>Шаг 4. Зарегистрировать систему.</p>	<p>Ввести ПИН-код для активации продукта и заполнить регистрационную форму. Для активации системы необходим доступ UGMC UserGate в интернет. Если на данном этапе выполнить регистрацию не удается, то ее следует повторить после настройки сетевых интерфейсов на шаге 8.</p>
<p>Шаг 5. Настроить зоны, IP-адреса интерфейсов, подключить UserGate Management Center в сеть предприятия.</p>	<p>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:</p> <ul style="list-style-type: none"> • Зона Management (сеть управления), интерфейс port0. • Зона Trusted (LAN). Предполагается, что через эту зону UGMC будет подключаться к МЭ UserGate, а также через которую она получит доступ в интернет. <p>Для работы UGMC UserGate достаточно одного настроенного интерфейса. Разделение функций управления устройством и управления МЭ UserGate на разные сетевые интерфейсы рекомендовано для обеспечения безопасности, но не является обязательным требованием.</p>
<p>Шаг 6. Настроить шлюз в интернет.</p>	<p>В разделе Шлюзы указать IP-адрес шлюза в интернет на интерфейсе, имеющим доступ в интернет, как правило, это зона Trusted. Подробно о настройке шлюзов в интернет читайте в главе Настройка шлюзов.</p>
<p>Шаг 7. Указать системные DNS-серверы.</p>	<p>В разделе DNS укажите IP-адреса серверов DNS, вашего провайдера или серверов, используемых в вашей организации.</p>
<p>Шаг 8. Зарегистрировать продукт (если не был зарегистрирован на шаге 4).</p>	<p>Зарегистрировать продукт с помощью ПИН-кода. Для успешной регистрации необходимо подключение к интернету и выполнение предыдущих шагов.</p> <p>Более подробно о лицензировании продукта читайте в главе Лицензирование UserGate Management Center.</p>
<p>Шаг 9. Создать как минимум одну управляемую область.</p>	<p>В разделе Управляемые области - Области добавить управляемую область.</p>
<p>Шаг 10. Создать администратора созданной управляемой области.</p>	<p>В разделе Администраторы создать профиль администратора и дать ему права на управление созданной областью. Создать администратора с данным профилем.</p>
<p>Шаг 11. Создать дополнительных администраторов UGMC (опционально).</p>	<p>В разделе Администраторы создать необходимые профили для управления сервисами UGMC и создать администраторов UGMC с этими профилями.</p>

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

6 НАСТРОЙКА USERGATE MANAGEMENT CENTER

В данном разделе руководства описываются настройки сервиса консоли UserGate. Настройка управляемых областей и применение политик безопасности к МЭ UserGate описано в главе данного руководства [Управление областями UGMC](#).

6.1 Общие настройки

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

Наименование	Описание
Часовой пояс	Часовой пояс, соответствующий вашему местоположению. Часовой пояс используется в расписаниях, применяемых в правилах, а также для корректного отображения времени и даты 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. <ul style="list-style-type: none">• 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.

6.2 Управление устройством

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

- Кластеризация.
- Настройки диагностики.
- Операции с сервером.
- Экспорт настроек.

6.2.1 Кластеризация и отказоустойчивость

UGMC UserGate 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.

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	<p>Настройки диагностики</p> <p>Настройки интерфейсов</p> <p>Настройки шлюзов</p> <p>Маршруты</p>

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.	<p>В разделе Зоны создать выделенную зону для репликации настроек кластера. В настройках зоны разрешить следующие сервисы:</p> <ul style="list-style-type: none"> • Консоль администрирования. • Кластер. <p>Не используйте для репликации зоны, интерфейсы которых подключены к недоверенным сетям, например, к интернету.</p>
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 второй узел в кластер.	<p>Подключиться к веб-консоли второго узла кластера, выбрать язык установки.</p> <p>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.</p> <p>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</p>

	первого 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.

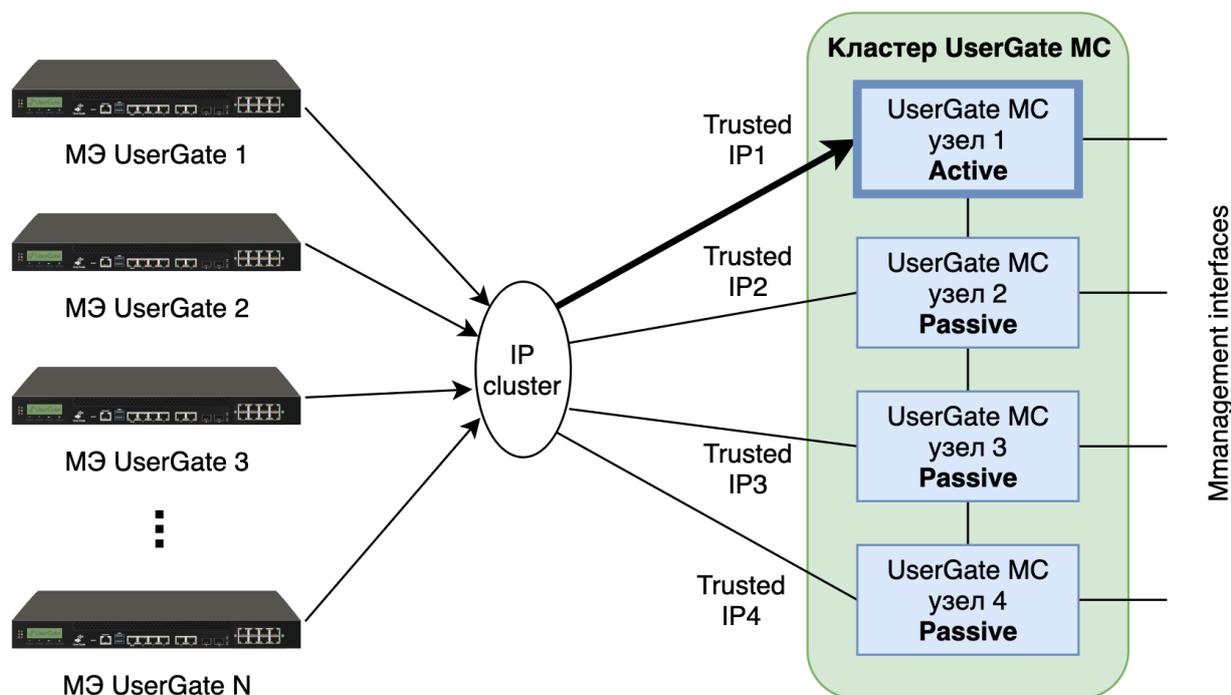
До четырех узлов кластера конфигурации можно объединить в отказоустойчивый кластер. Самих кластеров отказоустойчивости может быть несколько. Поддерживаются 2 режима - **Актив-Актив** и **Актив-Пассив**.

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 представлена 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 UserGate.



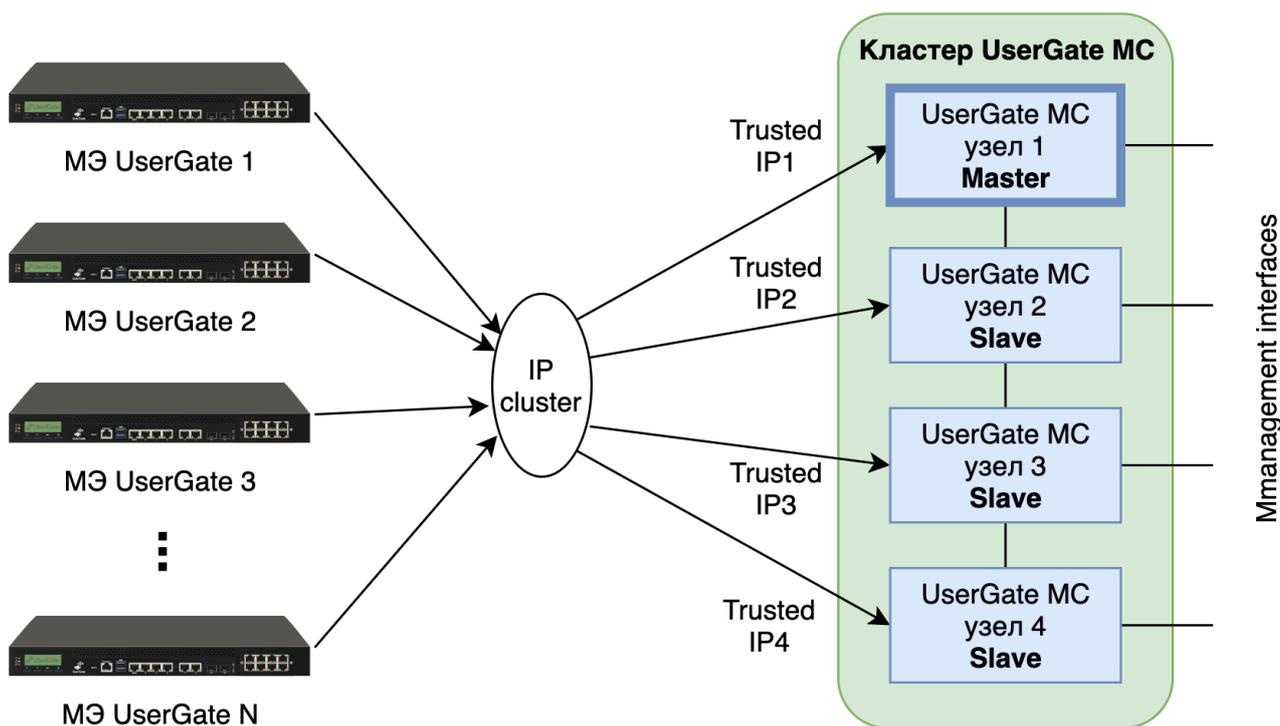
Кластерный IP-адрес находится на узле UGMC UserGate 1. Если узел UGMC UserGate 1 становится недоступным, то кластерный IP-адрес перейдет на следующий сервер, который станет мастер сервером, например, UGMC UserGate 2.

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 UserGate.



Кластерный IP-адрес находится на узле UGMC UserGate 1, который является мастер-узлом. При этом трафик распределяется на все узлы кластера. Если узел UGMC UserGate 1 становится недоступным, то роль мастера и кластерный IP-адрес перейдет на следующий сервер, например, UGMC UserGate 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.
Описание	Описание отказоустойчивого кластера.
Режим кластера	Режим отказоустойчивого кластера: <ul style="list-style-type: none"> • 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.

6.2.2 Диагностика

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

Наименование	Описание
Детализация диагностики	<ul style="list-style-type: none"> • 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. <p>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 UserGate.</p>
Журналы диагностики	<ul style="list-style-type: none"> • Скачать журналы - скачать диагностические журналы для передачи их в службу поддержки UserGate. • Очистить журналы - очистить содержимое журналов.
Удаленный помощник	<ul style="list-style-type: none"> • 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 UserGate для диагностики и решения проблем. Для успешной активации удаленного помощника UGMC UserGate 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

6.2.3 Операции с сервером

Данный раздел позволяет произвести следующие операции с сервером:

Наименование	Описание
Операции с сервером	<ul style="list-style-type: none"> • Перезагрузить - перезагрузка сервера UGMC UserGate. • Выключить - выключение сервера UGMC UserGate.
Обновления	<p>Выбор канала обновлений ПО UGMC UserGate</p> <ul style="list-style-type: none"> • 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 UserGate в рамках подписки на модуль лицензии Security Update (подробно о лицензировании смотрите в разделе [Лицензирование UserGate Management Center](#)). При наличии обновлений в разделе **Управление продуктом** отобразится соответствующее оповещение.

Обновление продукта может занять довольно длительное время, рекомендуется планировать установку обновлений с учетом возможного времени простоя UGMC UserGate.

Для установки обновлений необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл резервного копирования.	Создать резервную копию состояния UGMC UserGate, как это описано в разделе Управление устройством --> Резервное копирование и восстановление первоначальных настроек . 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 UserGate будет перезагружен.

6.2.4 Экспорт настроек

Администратор имеет возможность сохранить текущие настройки UGMC UserGate в файл и впоследствии восстановить эти настройки на этом же или другом сервере UGMC UserGate. 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 UserGate с помощью имеющегося ПИН-кода.

Для экспорта настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Экспорт настроек.	В разделе Управление устройством нажать на ссылку Экспорт настроек --> Экспорт . Система сохранит текущие настройки сервера под именем database.bin.

Для применения созданных ранее настроек необходимо выполнить следующие действия:

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

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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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".

6.3 Администраторы

Доступ к веб-консоли UGMC UserGate 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 UserGate 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.	<p>В разделе Администраторы нажать кнопку Добавить и выбрать необходимый вариант:</p> <ul style="list-style-type: none"> • 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 авторизации. 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 авторизации. 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 авторизации – создать пользователя, назначить созданный ранее профиль администратора и профиль авторизации (необходимы корректно настроенные серверы авторизации). <p>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.</p>

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	Если в качестве параметра тип администратора был выбран вариант Администратор области , то необходимо указать управляемую область, для которой создается корневой администратор.

область	Область должна уже быть создана к этому моменту.
Права доступа	<p>Список объектов дерева веб-консоли, доступных для делегирования. В качестве доступа можно указать:</p> <ul style="list-style-type: none"> • Нет доступа. • Чтение. • Чтение и запись.

Администратор UGMC UserGate может настроить дополнительные параметры защиты учетных записей администраторов, такие, как сложность пароля и блокировку учетной записи на определенное время при превышении количества неудачных попыток авторизации.

Для настройки этих параметров необходимо:

Наименование	Описание
Шаг 1. Настроить политику паролей.	В разделе Администраторы --> Администраторы нажать кнопку Настроить .
Шаг 2. Заполнить необходимые поля.	<p>Указать значения следующих полей:</p> <ul style="list-style-type: none"> • 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.

В разделе **Администраторы --> Сессии администраторов** отображаются все администраторы, выполнившие вход в веб-консоль администрирования UGMC UserGate. 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).

Примечание

Не 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 в разделе контроль доступа разрешить доступ к сервису **Консоль администрирования**. Более подробно о настройке контроля доступа к зонам можно прочитать в разделе [Настройка зон](#).

6.4 Управление сертификатами

UGMC UserGate использует защищенный протокол HTTPS для управления устройством. Для выполнения данной функции UGMC UserGate 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: <ul style="list-style-type: none">• 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 UserGate. Для этого необходимо выделить необходимый сертификат в списке сертификатов, нажать на кнопку Редактировать и указать тип сертификата - SSL веб-консоли. После этого UGMC UserGate перезагрузит сервис веб-консоли и предложит вам подключиться уже с использованием нового сертификата.

UGMC UserGate 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: <ul style="list-style-type: none">• Экспорт сертификата - экспортирует данные сертификата в der-формате без экспортирования приватного ключа сертификата.• Экспорт CSR - экспортирует CSR сертификата, например, для подписи его удостоверяющим центром.

Примечание

Рекомендуется сохранять сертификат для возможности его последующего восстановления.

Примечание

В целях безопасности UGMC UserGate не разрешает экспорт частных ключей сертификатов.

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

Наименование	Описание
Шаг 1. Начать импорт.	Нажать на кнопку Импорт .
Шаг 2. Заполнить необходимые поля.	Указать значения следующих полей: <ul style="list-style-type: none">• Название - название сертификата, под которым он будет отображен в списке сертификатов.• Описание - описание сертификата.• Загрузите файл, содержащий данные сертификата.• Загрузите файл, содержащий частный ключ сертификата.• Пароль для частного ключа, если таковой требуется.• Цепочка сертификатов – файл, содержащий сертификаты вышестоящих центров сертификации, которые участвовали в создании сертификата. Необязательное поле.

6.5 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.
Авторизация	Включает авторизацию 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.
Авторизация	Включает авторизацию при подключении к SMPP-серверу.
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.

6.6 Серверы авторизации UserGate Management Center

Серверы авторизации - это внешние источники учетных записей пользователей для авторизации в веб-консоли управления UGMC. UGMC поддерживает только сервер авторизации 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 авторизации.
Название	Название сервера авторизации.
SSL	Определяет, требуется ли SSL-соединение для подключения к LDAP-серверу.
Доменное имя LDAP или IP-адрес	IP-адрес контроллера домена или название домена LDAP. Если указано доменное имя, то UserGate получит адрес сервера LDAP с помощью DNS-запроса.
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*

7 ОФЛАЙН ОПЕРАЦИИ С СЕРВЕРОМ

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 UserGate MC. 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
1. UserGate MC (serial console)	Загрузка UserGate MC с выводом диагностической информации о загрузке в последовательный порт.
2. UserGate MC (verbose mode)	Загрузка UserGate MC с выводом диагностической информации о загрузке в консоль tty1 (монитор).
3. Support menu	Войти в раздел системных утилит с выводом информации в консоль tty1 (монитор).
4. Support menu (serial console)	Войти в раздел системных утилит с выводом информации в последовательный порт. При подключении через последовательный порт загрузочное меню не отображается. Для выбора раздела Support menu необходимо во время загрузки нажимать клавишу "4" . Для выбора одного из пунктов меню в разделе Support menu необходимо нажать клавишу, соответствующую первой букве названия пункта меню, например, для выбора Restore backup , необходимо нажать клавишу "R" , затем клавишу "Ввод" .
5. Memory test	Запуск проверки оперативной памяти устройства.

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.
Clear logs	Очистка диагностических журналов для освобождения пространства на системном разделе.
Export logs	Выгрузка диагностических журналов на внешний USB носитель. Все данные на внешнем носителе будут удалены.
Expand log partition	Увеличение раздела для журналов на весь выделенный диск. Эта операция обычно используется после увеличения дискового пространства, выделенного гипервизором для виртуальной машины UserGate MC. Данные и настройки UserGate MC не сбрасываются.

Backup full	Создать полную копию диска UserGate MC на внешний USB носитель. Все данные на внешнем носителе будут удалены.
Backup system only	Создать копию системного раздела UserGate MC, исключая журналы на внешний USB носитель. Все данные на внешнем носителе будут удалены.
Restore from backup	Восстановление UserGate MC с внешнего USB носителя.
Update from USB	Установка обновления ПО UserGate MC с внешнего USB носителя. Обновление должно быть скопировано в корень съемного диска, диск должен иметь формат NTFS или FAT32.
Refresh NIC names	Упорядочивание имен сетевых портов в необходимом порядке. Упорядочивание производится в соответствии с номером порта на шине PCI. Эту операцию необходимо выполнять после добавления сетевых портов в настроенный аплаенс UserGate MC, например, после установки дополнительной сетевой карты в физический аплаенс или после добавления портов в виртуальный аплаенс. Данные и настройки UserGate MC не сбрасываются.
Factory reset	Сброс состояния UserGate MC к первоначальному состоянию системы. Все данные и настройки будут утеряны.
Exit	Выход и перезагрузка устройства.

8 НАСТРОЙКА СЕТИ

В данном разделе описаны сетевые настройки UGMC UserGate.

8.1 Настройка зон

Зона в UGMC - это логическое объединение сетевых интерфейсов. Политики безопасности UGMC UserGate 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 UserGate поставляется со следующими зонами:

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

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

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



Примечание

Можно 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: <ul style="list-style-type: none">• 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 UserGate начинает отбрасывать пакеты, поступившие с этого IP-адреса, и записывает данное

	<p>событие в системный журнал.</p> <p>Рекомендованные значения для порога уведомления - 300 запросов в секунду, для порога отбрасывания пакетов - 600 запросов в секунду.</p> <p>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.</p>
<p>Шаг 3. Настроить параметры контроля доступа зоны (опционально).</p>	<p>Указать предоставляемые UGMC UserGate сервисы, которые будут доступны клиентам, подключенным к данной зоне. Для зон, подключенных к неконтролируемым сетям, таким, как интернет, рекомендуется отключить все сервисы.</p> <p>Сервисы:</p> <ul style="list-style-type: none"> • Ping - позволяет пинговать UGMC UserGate. • Консоль администрирования - доступ к веб-консоли управления (TCP 8010 и 8300). • XML-RPC для управления - позволяет управлять продуктом по API (TCP 4040). • VRRP - сервис, необходимый для объединения нескольких МЭ UserGate в отказоустойчивый кластер (IP протокол 112). • Контроль конечных устройств - сервис подключения конечных устройств UserGate Client (TCP 4043, 9712). • Кластер - сервис, необходимый для объединения нескольких МЭ UserGate 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 МЭ UserGate и UserGate LogAn (TCP 2022, 9712).
<p>Шаг 4. Настроить параметры защиты от IP-спуфинга атак (опционально).</p>	<p>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.</p> <p>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.</p> <p>С помощью галочки 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.</p>

8.2 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.

8.2.1 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.
Интерфейсы	Один или более интерфейсов, которые будут использованы для построения бонда.
Режим	<p>Режим работы бонда должен совпадать с режимом работы на том устройстве, куда подключается бонд. Может быть:</p> <ul style="list-style-type: none"> • 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»

	<p>политику.</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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.

Xmit hash policy	<p>Определяет хэш-политику передачи пакетов через объединенные интерфейсы в режиме XOR или IEEE 802.3ad. Возможные значения:</p> <ul style="list-style-type: none"> • 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 прийти 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.

8.3 Настройка шлюзов

Для подключения UGMC UserGate 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.

8.4 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 UserGate.
Шаг 4. Указать интерфейс.	Выберите интерфейс, через который будет добавлен маршрут. Если оставить значение Автоматически , то UGMC UserGate сам определит интерфейс, исходя из настроек IP-адресации сетевых интерфейсов.
Шаг 5. Указать метрику.	Задайте метрику маршрута. Чем меньше метрика, тем приоритетней маршрут, если маршрутов несколько в данную сеть несколько.

9 ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ (CLI)

UGMC UserGate позволяет создавать базовые настройки устройства с помощью интерфейса командной строки, или 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 UserGate), 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 UserGate.	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 UserGate 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 UGMC UserGate.	Используя специальный кабель для последовательного порта или переходник USB-Serial, подключить свой компьютер к UGMC UserGate.
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 UserGate 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 UserGate, 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@IPUserGateCC -p 2200</code>
Шаг 3. Войти в CLI.	Войти в CLI, используя пароль пользователя, указанного на предыдущем шаге. Если устройство UGMC UserGate 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	Выйти из CLI.
quit	
Ctrl+D	
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.

	<p>netcheck [-t TIMEOUT] [-d] URL</p> <p>Опции:</p> <p>-t – максимальный таймаут ожидания ответа от веб-сервера</p> <p>-d – запросить содержание сайта. По умолчанию запрашиваются только заголовки.</p>
nslookup	Выполнить определение IP-адреса по имени хоста.
ping	Выполнить ping определенного хоста.
radmin	Включить или отключить удаленный доступ к серверу для технической поддержки UGMC UserGate.
radmin_e	Включить или отключить удаленный доступ к серверу для технической поддержки UGMC UserGate, в случаях, когда сервер UGMC UserGate завис.
reboot	Перезагрузить сервер UGMC UserGate.
route	Создать, изменить, удалить маршрут.
shutdown	Выключить сервер UGMC UserGate.
traceroute	Выполнить трассировку соединения до определенного хоста.
zone	Набор команд для просмотра и настройки параметров зоны. Смотрите zone help для детальной информации.

10 УПРАВЛЕНИЕ ОБЛАСТЯМИ

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.

10.1 Создание управляемых областей

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*.

10.2 Администраторы области

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 UserGate создает корневого администратора области, обладающего всеми полномочиями на данную зону. Смотрите раздел для более детальной информации.

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: <ul style="list-style-type: none">• 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 авторизации области. При входе в консоль администрирования необходимо указывать имя пользователя в формате user@domain. Назначить созданный ранее профиль.• Добавить группу LDAP - добавить группу пользователей из существующего домена. Для этого должен быть корректно настроен LDAP-коннектор в разделе Серверы авторизации области. При входе в консоль администрирования необходимо указывать имя пользователя

- в формате [user@domain](#). Назначить созданный ранее профиль.
- **Добавить администратора с профилем авторизации** – создать пользователя, назначить созданный ранее профиль администратора и профиль авторизации (необходимы корректно настроенные серверы авторизации).

При создании профиля доступа администратора необходимо указать следующие параметры:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Права доступа на область	<p>Укажите права доступа на разделы настроек области, такие как - администраторы, серверы авторизации, шаблоны устройств, группы шаблонов, управляемые устройства, журналы и отчеты.</p> <p>В качестве доступа можно указать:</p> <ul style="list-style-type: none"> • Нет доступа. • Чтение. • Чтение и запись.
Права доступа на шаблон	<p>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:</p> <ul style="list-style-type: none"> • Нет доступа. • Чтение. • Чтение и запись. <p>Например, можно разрешить сетевые настройки одной группе администраторов, а политики МЭ - другой.</p>

10.3 Серверы авторизации области

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

- Получать информацию о пользователях и группах Active Directory или других LDAP-серверов. Поддерживается работа с LDAP-сервером FreeIPA.
- Осуществлять авторизацию администраторов областей 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 авторизации.
Название	Название сервера авторизации.
SSL	Определяет, требуется ли SSL-соединение для подключения к LDAP-серверу.
Доменное имя LDAP или IP-адрес	IP-адрес контроллера домена или название домена LDAP. Если указано доменное имя, то UserGate получит адрес сервера LDAP с помощью DNS-запроса.
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/ realm или *user@domain/ realm*

11 УПРАВЛЕНИЕ МЕЖСЕТЕВЫМИ ЭКРАНАМИ USERGATE

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 УУ. 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.

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

11.1 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** 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 NGFW** 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.
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 УУ с UGMC.
5. При настройке сетевых интерфейсов возможно создать интерфейс, но 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.
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 УУ. Например, шаблон сетевых настроек, шаблон правил межсетевого экрана, шаблон правил контентной фильтрации, шаблон библиотек и т.д.

11.2 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.

11.3 Добавление устройств UserGate под управление UGMC

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

Наименование	Описание
Шаг 1. Обеспечить доступ от УУ до UGMC.	На сервере UGMC необходимо разрешить Сервис UserGate Management Center на зоне, к которой подключены УУ. Сервер UGMC слушает подключения от УУ на портах TCP 2022 и 9712. Передача данных между сервером UGMC и УУ осуществляется по зашифрованному каналу.
Шаг 2. Создать объект УУ.	В консоли управления областью в разделе Управление NGFW --> Устройства NGFW нажать кнопку Добавить и указать необходимые настройки.
Шаг 3. Связать созданный объект УУ с реальным	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

При создании объекта УУ необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает объект УУ. Если объект УУ включен, то он занимает одну лицензию.
Название	Название для УУ. Можно вводить произвольное название.
Описание	Описание УУ.
Группа шаблонов	Группа шаблонов, настройки которой следует применить к этому УУ.
Синхронизация	<p>Выбор режима синхронизации настроек группы шаблонов к устройству. Возможны 3 варианта:</p> <ul style="list-style-type: none"> • 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.

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 УУ и нажать на кнопку Показать уникальный код устройства . Скопировать данный код в буфер обмена.
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.	<p>Указать следующие параметры:</p> <ul style="list-style-type: none"> • 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 УУ 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 УУ 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 и 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 УУ 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 УУ может:

Наименование	Описание
Посмотреть расширенную информацию о состоянии УУ	В консоли UGMC необходимо выбрать объект УУ и нажать на кнопку Показать детальную информацию . Будет отображена следующая информация о подключенном УУ: <ul style="list-style-type: none">• Версия ПО УУ.• ПИН-код УУ.• Серийный номер ПАК.• Время непрерывной работы.• Показатели загрузки устройства - загрузка ЦП, оперативной памяти, своп-файла, количество пользователей, подключенных через УУ.
Подключиться к консоли УУ	В консоли UGMC необходимо выбрать объект УУ 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 УУ. Новые настройки будут применены к МЭ UserGate.

11.4 Кластеризация МЭ UserGate с помощью UserGate Management Center

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.

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

11.4.1 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: <ul style="list-style-type: none">• 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	Подключение первого узла ничем не отличается от подключения отдельно стоящего устройства UserGate. Процедура подключения подробно описана в

кластера конфигурации в UGMC.	разделе Добавление устройств UserGate под управление UGMC . Первому узлу автоматически назначается идентификатор <i>node_1</i> .
Шаг 6. Подключить второй узел в кластер.	<p>Подключиться к веб-консоли второго узла кластера, выбрать язык установки.</p> <p>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.</p> <p>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.</p> <p>После успешного добавления узла в кластер, данный узел будет отображаться в качестве второго узла в списке управляемых устройств с выбранным идентификатором.</p>

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.

11.4.2 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, разрешались 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
Включено	Включение/отключение отказоустойчивого кластера.
Название	Название отказоустойчивого кластера.
Описание	Описание отказоустойчивого кластера.
Режим кластера	Режим отказоустойчивого кластера: <ul style="list-style-type: none"> • 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.

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.

11.5 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, MIME-типов и другие).

Примечание

После добавления УУ 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 централизовано 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 .

11.5.1 Обновление ПО

Компания UserGate периодически выпускает обновления программного обеспечения МЭ UserGate. Эти обновления выкладываются в репозиторий UserGate (<https://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 репозитария. Такие обновления следует добавлять в UGMC с помощью импорта обновления из файла.

Порядок установки обновлений следующий:

Наименование	Описание
Шаг 1. Загрузить обновления в репозиторий UGMC.	<p>Загрузить обновления можно либо из репозитария UserGate, либо импортировав файл обновления вручную.</p> <p>Для загрузки обновлений из репозитария необходимо в разделе Управление NGFW--> 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.</p> <p>Для загрузки вручную необходимо в разделе Управление NGFW--> 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.</p>
Шаг 2. Утвердить обновление для всех или для конкретных устройств.	<p>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.</p> <p>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.</p>
Шаг 3. Провести установку обновления.	<p>После утверждения обновление становится доступным для скачивания для всех или группы управляемых устройств. УУ скачивает обновление в соответствии с расписанием проверки обновлений. После скачивания обновление устанавливается в ручном режиме администратором устройства.</p>

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: <ul style="list-style-type: none"> • 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.

11.5.2 Обновление библиотек

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 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. 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>).

Созданные в МС элементы библиотек, не использующиеся в политиках, не будут отображены в списках элементов межсетевых экранов UserGate.

Библиотеки, находящиеся в репозитории UGMC доступны всем управляемым устройствам UserGate. УУ 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.
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.
Версия	Версия обновления библиотеки.
Обновлено	Дата и время последнего обновления конкретной библиотеки.

12 УПРАВЛЕНИЕ УСТРОЙСТВАМИ USERGATE LOGAN

Централизованное управление устройствами UserGate Log Analyzer (УУ 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 УУ. 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 УУ LogAn, к которым применимы данные шаблоны.

12.1 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 **Управление 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 **Шаблоны LogAn** и в выпадающем меню 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.
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 УУ с UGMC.
4. При настройке сетевых интерфейсов возможно создать интерфейс, но оставить его конфигурирование локальному администратору. Для этого необходимо включить чекбокс **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 УУ. Например, шаблон сетевых настроек, шаблон библиотек и т.д.

12.2 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 **Управление 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.

12.3 Добавление устройств LogAn под управление UGMC

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

Наименование	Описание
Шаг 1. Обеспечить доступ от УУ до UGMC.	На сервере UGMC необходимо разрешить Сервис UserGate Management Center на зоне, к которой подключены УУ. Сервер UGMC слушает подключения от УУ на портах TCP 2022 и 9712. Передача данных между сервером UGMC и УУ осуществляется по зашифрованному каналу.
Шаг 2. Создать объект УУ LogAn.	В консоли управления областью в разделе Управление LogAn --> Устройства LogAn нажать кнопку Добавить и указать необходимые настройки.
Шаг 3. Связать созданный объект УУ LogAn с реальным устройством МЭ UserGate.	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 УУ LogAn необходимо указать следующие параметры:

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

Включено	Включает объект УУ. Если объект УУ включен, то он занимает одну лицензию.
Название	Название для УУ. Можно вводить произвольное название.
Описание	Описание УУ.
Группа шаблонов	Группа шаблонов, настройки которой следует применить к этому УУ.
Синхронизация	<p>Выбор режима синхронизации настроек группы шаблонов к устройству. Возможны 3 варианта:</p> <ul style="list-style-type: none"> • Автоматическая синхронизация – настройки применяются к устройству автоматически. При изменении любой настройки из любого шаблона, включенного в группу шаблонов, примененную к УУ, это изменение применяется к LogAn 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.

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 УУ и нажать на кнопку 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 .
Шаг 3. Указать необходимые настройки нового узла и ввести уникальный код устройства.	<p>Указать следующие параметры:</p> <ul style="list-style-type: none"> • 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 UserGate 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 УУ 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 УУ 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 и 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.	<p>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.</p> <p>В консоли UGMC в объекте УУ появится дополнительная информация о подключенном устройстве, такая как ПИН-код, серийный номер, информация о лицензии, используемой памяти и т.п.</p>

После того, как LogAn успешно добавлен в UGMC администратор УУ может:

Наименование	Описание
Посмотреть расширенную информацию о состоянии УУ	<p>В консоли UGMC необходимо выбрать объект УУ и нажать на кнопку Показать детальную информацию. Будет отображена следующая информация о подключенном УУ:</p> <ul style="list-style-type: none">• Версия ПО УУ.• ПИН-код УУ.• Серийный номер ПАК.• Время непрерывной работы.• Показатели загрузки устройства - загрузка ЦП, оперативной памяти, своп-файла.
Подключиться к консоли УУ	В консоли UGMC необходимо выбрать объект УУ и нажать на кнопку Открыть консоль . В новом окне откроется консоль LogAn.
Изменить настройки	В консоли UGMC измените настройки одного из шаблонов, входящего в группу шаблонов, примененного к УУ. Новые настройки будут применены к LogAn.

12.4 Управление обновлениями управляемых устройств LogAn

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, MIME-типов и другие).

Примечание

После добавления УУ 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 централизованно 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 УУ. 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 УУ. Подробно об обновлениях библиотек смотрите в разделе Обновление библиотек LogAn .

12.4.1 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. 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
Шаг 1. Загрузить обновления в	Загрузить обновления можно либо из репозитория UserGate, либо импортировав файл

репозиторий UGMC.	<p>обновления вручную.</p> <p>Для загрузки обновлений из репозитория необходимо в разделе Управление LogAn --> Обновление 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.</p> <p>Для загрузки вручную необходимо в разделе Управление 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.</p>
Шаг 2. Утвердить обновление для всех или для конкретных устройств.	<p>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.</p> <p>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.</p>
Шаг 3. Провести установку обновления.	<p>После утверждения обновление становится доступным для скачивания для всех или группы управляемых устройств. УУ скачивает обновление в соответствии с расписанием проверки обновлений. После скачивания обновление устанавливается в ручном режиме администратором устройства.</p>

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, скачано.
Прогресс	Показывает прогресс загрузки обновления с репозитория UserGate.
Канал обновлений	<p>Канал обновлений репозитория UserGate:</p> <ul style="list-style-type: none"> • 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.

12.4.2 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. УУ 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.
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.

13 УПРАВЛЕНИЕ КОНЕЧНЫМИ УСТРОЙСТВАМИ USERGATE CLIENT

Конечное управляемое устройство - это пользовательский компьютер под управлением операционной системы Windows с установленным ПО UserGate Client (УУ UGC). ПО UserGate Client позволяет администратору централизованно управлять парком УУ 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 другая информация. Объем информации, получаемой с УУ UGC, будет постоянно расширяться. Данная информация отображается в системе анализа событий UserGate LogAn и может быть использована для автоматического реагирования на угрозы безопасности.

Централизованное управление УУ UGC можно разделить на следующие этапы:

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

13.1 Шаблоны устройств УУ UGC

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 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 УУ 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 УУ UGC. Например, шаблон правил межсетевого экрана, шаблон правил контентной фильтрации, шаблон библиотек и т.д.

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

13.1.1 Настройки

Определяют общие настройки параметров УУ UGC:

Устройство LogAn - устанавливает для конечного устройства сервер LogAn, куда оно будет отсылать информацию о событиях. Сервер LogAn должен быть предварительно зарегистрирован в UGMC.

13.1.2 Политики сети

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

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, сервисы и приложения.

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.

Примечание

Правила 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 Вверх/Вниз или перетаскивание мышью для изменения порядка применения правил.

Примечание

Чекбокс **Инvertировать** меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

Примечание

Если не создано ни одного правила, то любой трафик с/на УУ 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 УУ UGC. Возможны следующие варианты: <ul style="list-style-type: none">• 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.
Действие	Запретить - блокирует трафик. Разрешить - разрешает трафик. Перенаправить в прокси - перенаправляет трафик, соответствующий условиям правила в указанный прокси сервер. Перенаправить можно только трафик TCP и, если в правиле не указаны такие параметры, как Списки URL, Категории, Типы контента .
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 .
Источник	Списки IP-адресов источника трафика. Более подробно об списках IP-адресов читайте в главе IP-адреса .
Назначение	Списки IP-адресов назначения трафика. Более подробно об списках IP-адресов читайте в главе IP-адреса .
Сервис	Тип сервиса, например, HTTP, HTTPS или telnet. Сервис должен быть предварительно создан в разделе Библиотеки --> Сервисы . Более подробно об сервисах читайте в главе Сервисы .
Приложение	Список приложений, для которых применяется данное правило. Приложение должно быть

	предварительно создано в разделе Библиотеки --> Приложения . Более подробно об приложениях читайте в главе Приложения .
Списки URL	Списки адресов URL. Более подробно о работе со списками URL читайте в главе Списки URL .
Категории	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. Более подробно об категориях читайте в главе Категории URL .
Типы контента	Списки MIME-типов. Предусмотрена возможность управления видеоконтентом, аудио контентом, изображениями, исполняемыми файлами и другими типами. Администраторы также могут создавать собственные группы MIME-типов. Более подробно о работе с MIME-типами читайте в главе Типы контента .
Время	Время, когда правило активно. Администратор может добавить необходимые ему временные интервалы в разделе Календари .
Конечные устройства	Конкретные конечные устройства, к которым может быть применено данное правило. Если ничего не указано, то данное правило применяется ко всем устройствам, к которым данный шаблон применен через группу шаблонов.

13.1.3 Библиотеки элементов

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

13.1.3.1 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 УУ 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.

13.1.3.2 IP-адреса

Раздел IP-адреса содержит список диапазонов IP-адресов, которые могут быть использованы при построении правил УУ 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
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.	При создании списка IP-адресов в UGMC указать адрес, откуда необходимо загружать обновления. UGMC будет проверять наличие новой версии на вашем сайте каждые 4 часа и обновлять список при наличии новой версии.

13.1.3.3 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.
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.

13.1.3.4 Профили прокси

13.1.3.5 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.	<p>Добавить записи URL в новый список. В списках можно использовать специальные символы «^», «\$» и «*»:</p> <ul style="list-style-type: none"> • «*» - любое количество любых символов. • «^» - начало строки. • «\$» - конец строки. <p>Символы «?» и «#» не могут быть использованы.</p>
Шаг 3. Создать правило межсетевое 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»
^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: <i>www.site1.com/url1</i> <i>www.site2.com/url2</i> ... <i>www.siteend.com/urlN</i>
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 адрес, откуда необходимо загружать обновления. UserGate будет проверять наличие новой версии на вашем сайте каждые 4 часа и обновлять список при наличии новой версии.

13.1.3.6 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.

13.1.3.7 Типы контента

С помощью фильтрации типов контента можно блокировать загрузку файлов определенного типа, например, запретить все файлы типа *.doc.

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.
Шаг 5. Создать список типа контента и указать URL для обновления.	На каждом UserGate создать список типа контента. При создании указать адрес, откуда необходимо загружать обновления. UserGate будет проверять наличие новой версии на вашем сайте каждые 4 часа и обновлять список при наличии новой версии.

13.1.3.8 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.

13.2 Группы шаблонов УУ UGC

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.

13.3 Установка ПО UserGate Client

Программный продукт UserGate client может быть установлен на компьютеры с версией ОС Windows 8/10. Для минимальной работоспособности необходимо от 6 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-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. 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 ugclient.adm, который используется для указания IP-адреса UGMC и кода конечного устройства, созданного в центре управления.

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

13.4 Добавление устройств УУ UGC под управление UGMC

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

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

13.4.1 Процесс единичного добавления устройств

Для добавления одного УУ UGC необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Обеспечить доступ от УУ UGC до UGMC.	На сервере UGMC необходимо разрешить сервис Контроль конечных устройств на зоне, к которой подключены УУ. Сервер UGMC слушает подключения от УУ UGC на портах TCP 4043 и 9712. Передача данных между сервером UGMC и УУ осуществляется по зашифрованному каналу.
Шаг 2. Создать запись для УУ UGC в UGMC.	В консоли управления областью в разделе Управление конечными устройствами --> Конечные устройства нажать кнопку Добавить и указать необходимые настройки.

<p>Шаг 3. Отобразить уникальный код созданного устройства.</p>	<p>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.</p>
<p>Шаг 4. Установить ПО UGC на конкретное устройство (компьютер) пользователя.</p>	<p>Установить ПО на конечный компьютер пользователя. В мастере установки указать уникальный код устройства, созданный на предыдущем шаге.</p> <p>Подробнее о установке ПО на конечное устройство смотрите в разделе Установка ПО UserGate Client.</p>

При создании записи УУ UGC необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает объект УУ UGC. Если объект УУ UGC включен, то он занимает одну лицензию.
Название	Название для УУ UGC. Можно вводить произвольное название.
Описание	Описание УУ UGC.
Группа шаблонов	Группа шаблонов, настройки которой следует применить к этому УУ UGC. Настройки (политики) применяются сразу же после установки ПО UGC на компьютер пользователя.
LogAn сервер	Сервер LogAn, куда УУ UGC будет отправлять телеметрическую информацию.

13.4.2 Процесс массового добавления устройств

Рассмотрим процесс массового добавления УУ UGC:

Наименование	Описание
<p>Шаг 1. Обеспечить доступ от УУ UGC до UGMC.</p>	<p>На сервере UGMC необходимо разрешить Сервис Контроль конечных устройств на зоне, к которой подключены УУ. Сервер UGMC слушает подключения от УУ UGC на портах TCP 4043 и 9712.</p> <p>Передача данных между сервером UGMC и УУ осуществляется по зашифрованному каналу.</p>
<p>Шаг 2. Создать код для группы конечных устройств.</p>	<p>В консоли управления областью в разделе Управление конечными устройствами --> Коды для конечных устройств нажать кнопку Добавить и указать необходимые параметры.</p>
<p>Шаг 3. Отобразить уникальный код для созданной группы устройств.</p>	<p>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.</p>

<p>Шаг 4. Установить ПО UGC на устройства пользователей.</p>	<p>Установить ПО на конечные компьютеры пользователей. В мастере установки или в административном шаблоне Active Directory указать уникальный код группы устройств, созданный на предыдущем шаге.</p> <p>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.</p> <p>Подробнее о установке ПО на конечное устройство смотрите в разделе Установка ПО UserGate Client.</p>
---	---

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

Наименование	Описание
Вкл	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.
Группа шаблонов	Группа шаблонов, настройки которой следует применить к УУ UGC, активированными с данным кодом. Настройки (политики) применятся сразу же после установки ПО UGC на компьютер пользователя.
LogAn сервер	Сервер LogAn, куда УУ UGC будет отсылать телеметрическую информацию.

13.5 Управление устройством UGC из консоли UGMC

После добавления УУ 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 устройств УУ 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 УУ UGC.
- Отображение уникального кода устройства, необходимого для подключения УУ UGC к UGMC.
- Запуск процесса принудительной синхронизации.

Данный раздел также позволяет просмотреть следующие параметры каждого конечного устройства:

Наименование	Описание
Название	Название конечного устройства.
Версия	Версия UserGate Client, установленная на устройстве.
Последнее подключение	Дата и время последнего подключения конечного устройства.
Телеметрия	<p>Представлена следующая информация:</p> <ul style="list-style-type: none"> • IP-адрес конечного устройства, который используется для выхода в Интернет. • Время последнего подключения УУ 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 информация о конечном устройстве. Более подробно данный пункт будет рассмотрен ниже.
Группа шаблонов конечных устройств	<p>Отображены группы шаблонов, применённые к УУ UGC.</p> <p>Создание групп шаблонов было рассмотрено в главе Группы шаблонов УУ UGC.</p>
Время последней синхронизации	<p>Данный параметр позволяет изменять режим синхронизации УУ UGC с UGMC. Возможен выбор работы в одном из следующих режимов:</p> <ul style="list-style-type: none"> • 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. <p>Отображены дата и время последней синхронизации конечного устройства и UGMC.</p>

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

Наименование	Описание
Производительность	<p>Представлена следующая информация:</p> <ul style="list-style-type: none"> • 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 УУ UGC показывает статус UserGate Client: онлайн/офлайн (UserGate Client запущен/не запущен на конечном устройстве) или отключено (UserGate Client был отключен с использованием UGMC кнопкой Отключить).
Запущенные процессы	<p>Показан список запущенных на конечном устройстве процессов.</p> <p>Нажатие кнопки Завершить процесс позволяет завершить процесс на конечном устройстве, используя UGMC.</p>
Список служб	<p>Отображён список служб, запущенных/остановленных на конечном устройстве.</p> <p>Нажатие кнопок Остановить службу/Запустить службу позволяет остановить/запустить службу на УУ UGC с использованием UGMC.</p>
Оборудование	<p>Представлена информация из Диспетчера устройств конечного устройства - установленные устройства, драйверы устройств.</p>
Программное обеспечение	<p>Отображён список установленных на УУ UGC ПО с указанием производителя и версии.</p>
Установленные обновления	<p>Представлен список установленных обновлений на УУ UGC с отображением информации о продукте, вендоре и дате релиза обновления.</p>

13.6 Сбор и анализ данных с устройств UGC

UserGate Log Analyzer является продуктом компании UserGate, входящим в состав экосистемы UserGate SUMMA. UserGate Log Analyzer устанавливается на отдельном сервере, использование которого позволяет обеспечить высокую надёжность и хорошую масштабируемость системы. UserGate LogAn предоставляет возможность осуществления сбора и анализа данных с различных устройств, мониторингу событий безопасности и созданию отчётов.

Доступ в веб-консоль UserGate LogAn осуществляется по адресу https://UserGate_LogAn_IP_address:8010. Более подробную информацию смотрите в соответствующей документации UserGate LogAn 6. Руководство администратора.

Сервер UserGate LogAn должен быть назначенным для конечных устройств, чтобы устройства отсылали данные на него. Настройка сервера LogAn для конечных устройств производится через шаблоны конечных устройств. Подробно об этом описано в разделе [Настройки](#).

Получая данные, LogAn осуществляет анализ произошедших событий и отслеживает активность пользователей. На основании полученных с УУ UGC данных могут быть сформированы:

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

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](#) и [Приложения конечных устройств](#).

13.6.1 Журнал событий конечных устройств

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

События могут быть отфильтрованы по различным параметрам:

Наименование	Описание
Дата	Выбор даты или диапазона дат, события которых нужно отобразить.
Конечное устройство/сенсор	Выбор одного или нескольких конечных устройств.
Файл журнала лога	Отображение информации из Журнала событий конечного устройства, т.е. информация о важных программных и аппаратных событиях. Тип файла журнала: <ul style="list-style-type: none">• 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.
Уровень лога	Выбор типа события: <ul style="list-style-type: none">• Audit Success (успешный аудит): событие журнала безопасности, которое происходит при успешном обращении к аудируемым ресурсам.• Audit Failure (неуспешный аудит): событие журнала безопасности, которое происходит при неуспешном обращении к аудируемым ресурсам.• Error (ошибка): событие указывает на существенные проблемы, которые могут стать причиной потери функциональности или данных.• Information (информация): информационные события, которые, как правило, не требуют внимания администратора.• Warning (предупреждение): события указывают на проблемы, которые не требуют немедленного исправления, однако могут привести к ошибкам в

	будущем.
Источник журнала событий	Отображение списка источников событий.
Узел	Для отображения параметра фильтрации используется кнопка Ещё . Представление списка имён узлов UserGate.
Категория задачи	Отображение категорий задач, по которым возможна фильтрация.
Категория лога	Для отображения параметра фильтрации используется кнопка Ещё . Категории лога помогают упорядочить события, чтобы просмотр событий можно было отфильтровать. Каждый источник события может определять собственные категории.
Имя компьютера	Для отображения параметра фильтрации используется кнопка Ещё . Представление списка имён конечных устройств.
Код события лога	Для отображения параметра фильтрации используется кнопка Ещё . Отображение списка кодов событий логов, соответствующих определённым событиям.
Идентификатор события лога	Для отображения параметра фильтрации используется кнопка Ещё . Идентификатор события лога определяет первичный идентификатор события.
Тип события лога	Для отображения параметра фильтрации используется кнопка Ещё . Тип события лога представлен параметрами, каждый из которых соответствует уровню лога: <ul style="list-style-type: none"> • 1 - уровень лога: error. • 2 - уровень лога: warning. • 3 - уровень лога: information. • 4 - уровень лога: audit success. • 5 - уровень лога: audit failure.

В UserGate LogAn также представлен режим расширенного поиска, который будет 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	Имя узла UserGate.
Время	Время события. Отображается в часовом поясе, настроенном на UserGate LogAn.
Конечное устройство	Отображено имя компьютера.
Уровень лога	Отображен тип события: Audit Success, Audit Failure, Error, Warning или Information.
Данные	Представлена подробная информация о событии.
Источник журнала событий	Показан источника журнала событий.
Категория лога	Отображена категория лога.
Категория задачи	Показана категория задачи.
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 событию.
Идентификатор события лога	Отображён идентификатор события лога.
Тип события лога	Отображён тип события лога, соответствующий определённому уровню лога.
Строка вставки	Содержит данные блока eventData события Windows.
Файл журнала лога	Показано к какому типу файла журнала относится событие.

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

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

13.6.2 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](#).

Нажатием кнопки **Ещё** могут быть дополнительные параметры фильтрации: правило, приложение, домен, категории сайтов, тип контента, протокол, IP источника, порт источника, IP назначения, порт назначения.

Фильтрация правил межсетевого экрана возможна по следующим параметрам:

Наименование	Описание
Дата	Выбор даты или диапазона дат, события которых нужно отобразить.
Конечное устройство/сенсор	Выбор одного или нескольких конечных устройств.
Действие	Выбор действия. Будут отображены все правила, в которых настроено выбранное действие. Действия: <ul style="list-style-type: none"> • Разрешить. • NAT. • Запретить.
Узел	Имя узла UserGate.
Правило	Применение фильтрации с использованием названия правила межсетевого экрана.
Приложение	Названия приложений, с помощью которых осуществляется подключение к ресурсу.
Домен	Имена доменов, к которым было выполнено подключение.
Категории сайтов	Выбор категорий сайтов, которые необходимо отобразить в журнале правил.
Тип контента	Выбор типа контента.
Протокол	Выбор транспортного протокола подключения, использующегося для доступа к ресурсу.
IP источника	Фильтрация правил по IP-адресу источника.
Порт источника	Фильтрация правил по номеру порта источника, используемого для подключения.
IP назначения	Фильтрация правил по IP-адресу назначения.
Порт назначения	Фильтрация правил по номеру используемого порта назначения.

В UserGate LogAn также представлен режим расширенного поиска, который будет 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	Показано имя узла UserGate.
Время	Указано время срабатывания правила. Отображается в часовом поясе, настроенном на UserGate LogAn.
Конечное устройство	Отображено имя компьютера.
Действие	Представлено действие, которое выполняется в соответствии с правилом.
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.
Тип контента	Отображён тип контента.
Протокол	Указан транспортный протокол, используемый 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.

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

13.6.3 Приложения конечных устройств

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

Для удобства формирования журнала доступна фильтрация по следующим параметрам:

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

Узел	Имя узла UserGate.
Дата	Выбор даты или диапазона дат, события которых нужно отобразить.
Конечное устройство	Выбор одного или нескольких конечных устройств, для которых необходимо сформировать журнал.
Приложение	Выбор приложения, запуск которого необходимо отобразить в журнале.

В UserGate LogAn также представлен режим расширенного поиска, который будет 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 привести 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	Имя узла UserGate.
Время	Указано время запуска приложения на конечном устройстве. Отображается в часовом поясе, настроенном на UserGate LogAn.
Конечное устройство	Отображено имя компьютера.
Хэш	Хэш приложения.
Приложение	Показано название приложения, которое было запущено.
Версия	Указана версия приложения.
Субъект подписи	Указан владелец сертификата.
Подписано	Указан издатель сертификата для приложения.

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

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

13.6.4 Режим расширенного поиска

Помимо простого поиска, для которого используется графический интерфейс, в UserGate 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	<p>Позволяет указать несколько значений поля в запросе. Список значений необходимо указывать в круглых скобках, например,</p> <p>category IN (botnets, compromised, 'illegal software', 'phishing and fraud','reputation high risk','unknown category').</p>
NOT IN	<p>Позволяет указать несколько значений поля в запросе; будут отображены записи, не содержащие указанные значения. Список значений необходимо указывать в круглых скобках, например,</p> <p>category NOT IN (botnets, compromised, 'illegal software', 'phishing and fraud','reputation high risk','unknown category').</p>
~	<p>Содержит. Позволяет указать подстроку, которая должна находиться в указанном поле, например,</p> <p>browser ~ "Mozilla/5.0".</p> <p>Данный оператор может быть применен только к полям, в которых хранятся строковые данные.</p>
!~	<p>Не содержит. Позволяет указать подстроку, которая не должна присутствовать в указанном поле, например,</p> <p>browser !~ "Mozilla/5.0".</p> <p>Данный оператор может быть применен только к полям, в которых хранятся строковые данные.</p>
MATCH	<p>При использовании оператора MATCH подстрока, которая должна присутствовать в указанном поле, задаётся в формате JSON и с использованием одинарных кавычек, например,</p> <p>details MATCH {"module":"threats"}.</p> <p>Синтаксис запросов с использованием данного оператора соответствует стандарту RE2. Подробнее о синтаксисе Google/RE2: https://github.com/google/re2/wiki/Syntax.</p>
NOT MATCH	<p>При использовании оператора NOT MATCH подстрока, которая не должна присутствовать в указанном поле, задаётся в формате JSON и с использованием одинарных кавычек, например,</p> <p>details NOT MATCH {"module":"threats"}.</p> <p>Синтаксис запросов с использованием данного оператора соответствует стандарту RE2. Подробнее о синтаксисе Google/RE2: https://github.com/google/re2/wiki/Syntax.</p>

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

13.7 Управление обновлениями УУ UGC

Компания UserGate постоянно улучшает качество разрабатываемого программного обеспечения и периодически выпускает его обновления. Произвести обновление ПО UserGate Client возможно с использованием UGMC. Для этого необходимо авторизоваться в веб-консоли UGMC под учётной записью администратора области (создание и настройка учётных записей администраторов описаны в разделе

[Администраторы области](#)). Обновления доступны во вкладке **Управление областью --> Управление конечными устройствами**.

13.7.1 Обновление ПО UserGate Client

Обновления доступны во вкладке **Управление областью --> Управление конечными устройствами --> Обновление ПО**.

UGMC предлагает возможности онлайн-обновления (загрузка обновления из репозитория UserGate: <http://static.usergate.com>) и импорта файла обновления (вручную).

Порядок установки обновлений:

Наименование	Описание
Шаг 1. Загрузить файл обновления.	<p>Для загрузки обновлений из репозитория необходимо нажать на кнопку Выбрать онлайн-обновления в разделе Управление конечными устройствами --> Обновление ПО: отобразится список обновлений, доступных для скачивания из репозитория UserGate. Далее нужно выделить необходимые обновления и нажать кнопку Выбрать. Выбранные обновления будут загружены в UGMC.</p> <p>Для загрузки файла обновления вручную необходимо в разделе Управление конечными устройствами --> Обновление ПО нажать кнопку Импортировать обновление и выбрать файл с обновлением. Если в файле не указаны версия и название обновления, то их необходимо указать в соответствующих полях. Кнопка Сохранить загрузит выбранное обновление в UGMC.</p>
Шаг 2. Утвердить обновления.	<p>Для установки обновления необходимо выбрать нужное обновление и нажать на кнопку Утвердить.</p> <p>Если требуется установить обновление на группу устройств (например, для проведения тестирования), то в свойствах обновления нужно указать УУ UGC, для которых будет доступно данное обновление, и установить чекбокс Утвердить обновление.</p>
Шаг 3. Установить обновление.	<p>После утверждения обновление становится доступным для скачивания и установки администратором на конечные устройства.</p>

Обновление в репозитории UGMC обладает следующими свойствами:

Наименование	Описание
Название	Название обновления. Обычно не доступно для изменения, содержится в коде изменения.
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	Прогресс загрузки обновления с репозитория UserGate.
Канал обновлений	Канал обновлений репозитория UserGate: <ul style="list-style-type: none"> • Стабильные - канал стабильных обновлений ПО. • Бета - канал экспериментальных обновлений.
Список изменений	Ссылка на список изменений, содержащихся в данном обновлении.
Утверждено	Дата утверждения обновления и имя администратора, который выполнил утверждение.
Добавлено	Дата добавления обновления в репозиторий UGMC и имя администратора, который выполнил добавление.

13.7.2 Обновление библиотек UserGate Client

Библиотеки – это обновляемые базы ресурсов, предоставляемых по подписке клиентам UserGate. Эти обновления выкладываются в репозиторий UserGate (<http://static.usergate.com>), откуда они уже доступны для скачивания. 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>).

Обновления доступны во вкладке **Управление областью --> Управление конечными устройствами --> Обновление библиотек**.

Обновление библиотек 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.
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.
Обновлено	Дата и время последнего обновления конкретной библиотеки.

