UserGate

Management Center 7.1.x Руководство администратора

Оглавление

- Принятые обозначения и сокращения
  - Принятые обозначения и сокращения
- Введение
  - Описание
  - Управление UGMC
  - Управляемые области
  - Шаблоны и группы шаблонов
  - Управляемые устройства
  - Поддержка в UGMC конфигурации ранних версии ПО UserGate
- Лицензирование UGMC
  - Лицензирование UGMC
- Планирование внедрения UGMC
  - Планирование внедрения UGMC (Описание)
- Первоначальная настройка
  - Первоначальная настройка
- Офлайн операции с сервером
  - Офлайн операции с сервером(Описание)
- Настройка UGMC
  - Общие настройки
  - Управление устройством
  - Администраторы
  - Сертификаты
  - Серверы аутентификации
  - Профили аутентификации
  - Библиотеки элементов
  - Расширение системного раздела
- Настройка сети
  - Настройка сети (описание)
- Журналы и отчёты
  - Журнал событий
  - Экспорт журналов
  - Режим расширенного поиска
- Диагностика и мониторинг
  - Маршруты
  - Ping
  - Traceroute
  - Запрос DNS
  - Оповещения
    - SNMP
    - Параметры SNMP

        - Правила оповещений
        - Профили безопасности SNMP
- Управление областями
    - Управление областями (Описание)
    - Создание управляемых областей
    - Администраторы области
    - Серверы аутентификации области
    - Профили аутентификации области
    - Каталоги пользователей
- Управление межсетевыми экранами UserGate
    - Управление межсетевыми экранами UserGate (Описание)
    - Практика работы с шаблонами в UserGate MC
- Управление устройствами LogAn
    - Управление устройствами LogAn (Описание)
- Управление конечными устройствами UserGate Client
    - Конечные управляемые устройства UserGate Client
    - Управление конечными устройствами UserGate Client (Описание)
    - Работа UserGate Client в связке с UGMC
    - Шаблоны управляемых устройств UGC
    - Группы шаблонов управляемых устройств UGC
    - Добавление устройств UGC под управление UGMC
    - Управление устройством UGC из консоли UGMC
    - Установка ПО UserGate Client
    - HIP профили
    - HIP объекты
    - Сбор и анализ данных с устройств UGC
- Интерфейс командной строки (CLI)
    - Общие положения
        - Общие положения (описание)
    - Команды, доступные до первичной инициализации узла
        - Команды, доступные до первичной инициализации узла (Описание)
    - Первоначальная инициализация
        - Первоначальная инициализация (Описание)
    - Режим конфигурации
        - Режим конфигурации (описание)
    - Настройка устройства
        - Настройка устройства (Описание)
        - Настройка кластеров
        - Настройка управления доступом к консоли устройства
        - Настройка сертификатов
        - Настройка серверов аутентификации
        - Настройка профилей аутентификации
    - Настройка сети
        - Зоны

        - Интерфейсы
        - Шлюзы
        - Настройка маршрутизации
        - DNS-настройки
    - Настройка мониторинга
        - Настройка параметров мониторинга устройства
    - Настройка библиотек
        - Настройка библиотек (Описание)
    - Управление областями
        - Настройка управляемых областей
    - Режим администратора управляемой области
        - Режим администратора управляемой области (Описание)
        - Режим конфигурации администратора управляемой области
        - Общие настройки консоли управляемой области
        - Администраторы управляемой области
        - Серверы аутентификации управляемой области
        - Профили аутентификации управляемой области
        - Каталоги пользователей управляемой области
        - Управление межсетевыми экранами UserGate
        - Управление конечными устройствами UserGate
        - Управление устройствами LogAn
- ADMIN
    - ADMIN (описание)
- Избранные
    - Избранные (описание)
- Приложения
    - Требования к сетевому окружению
    - Описание форматов журналов

ПРИНЯТЫЕ ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

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 LogAn	Управляемое устройство UserGate Log Analyzer
ПО	Программное обеспечение
ЦП	Центральный процессор

ВВЕДЕНИЕ

Описание

UserGate Management Center (UGMC) — это решение, которое позволяет контролировать большое количество управляемых устройств. Управляемыми устройствами могут быть межсетевые экраны UserGate, устройства сбора и

анализа данных LogAn, конечные устройства с установленным ПО UserGate Client.

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

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

Управление UGMC

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

Управление сервисами UGMC

Управление сервисами UGMC включает в себя следующие задачи:

Наименование	Описание
Настройка UGMC	• Назначение IP-адресов. • Конфигурирование зон. • Задание DNS-серверов. • Создание подключений к серверам LDAP. • Настройка оповещений. • Создание дополнительных администраторов UGMC с необходимым уровнем полномочий. Все эти настройки влияют только на функционирование самого сервиса UGMC и не влияют на администрирование управляемых областей.
Лицензирование	Лицензирование продукта (ввод ПИН-кода и регистрация продукта), а также опциональное назначение количества управляемых устройств каждой управляемой области. Если ограничения на область не установлены, то любая область может использовать любое количество управляемых

Наименование	Описание
	устройств, в сумме не превышающих лицензируемое количество. Подробнее о лицензировании смотрите в главе Лицензирование UserGate Management Center.
Создание управляемых областей	Создание управляемых областей. Количество управляемых областей не ограничено.
Создание корневых администраторов управляемых областей	Создание корневых администраторов управляемых областей.

Управление областями UGMC

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

Наименование	Описание
Создание дополнительных администраторов области	При добавлении управляемой области для неё создается корневой администратор, обладающий всеми полномочиями для управления данной областью. Корневой администратор области может создать дополнительных администраторов и наделить их необходимым уровнем полномочий.
Настройка серверов аутентификзации	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 назначение им групп шаблонов.

Ролевое управление

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

- **Администратор UGMC.** Как правило это пользователь с именем Admin. Для входа в консоль необходимо указать имя в виде Admin/system; 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**.

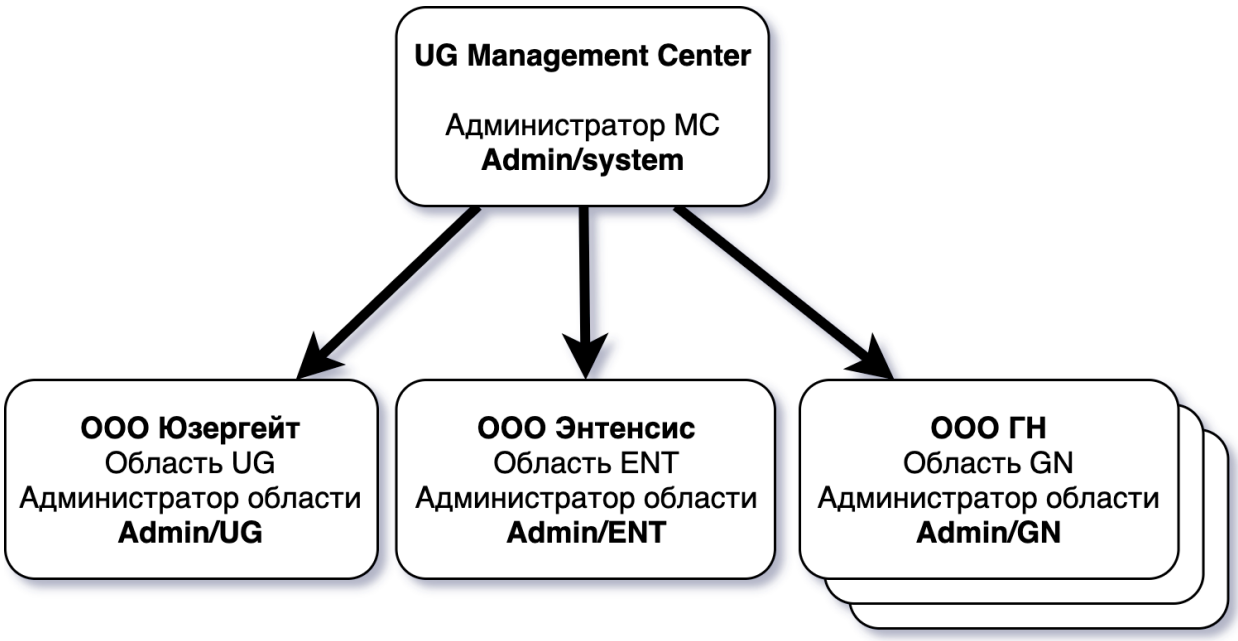
Корневой администратор области может создать дополнительных администраторов в своей области и наделить их специальными полномочиями (профили администраторов). Администраторы области ограничены только возможностью управления своей областью (смотрите главу Управляемые области), не имея доступа к управлению 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/realm_code	Корневой профиль	Полный. Администратор и его профиль создаются администратором UGMC.
AdminRO/realm_code	ReadOnly	Доступ ко всем настройкам области в режиме просмотра без возможности модификации.
AdminTemplates/ realm_code	Templates	Создание и модификация всех шаблонов области.
AdminTemplateGeneral/ realm_code	TemplateGeneral	Только модификация шаблона General.
AdminTemplateGeneralNET /realm_code	TemplateGeneralNET	Только модификация сетевых настроек в шаблоне General.

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 одной организации достаточно создать одну управляемую область.

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

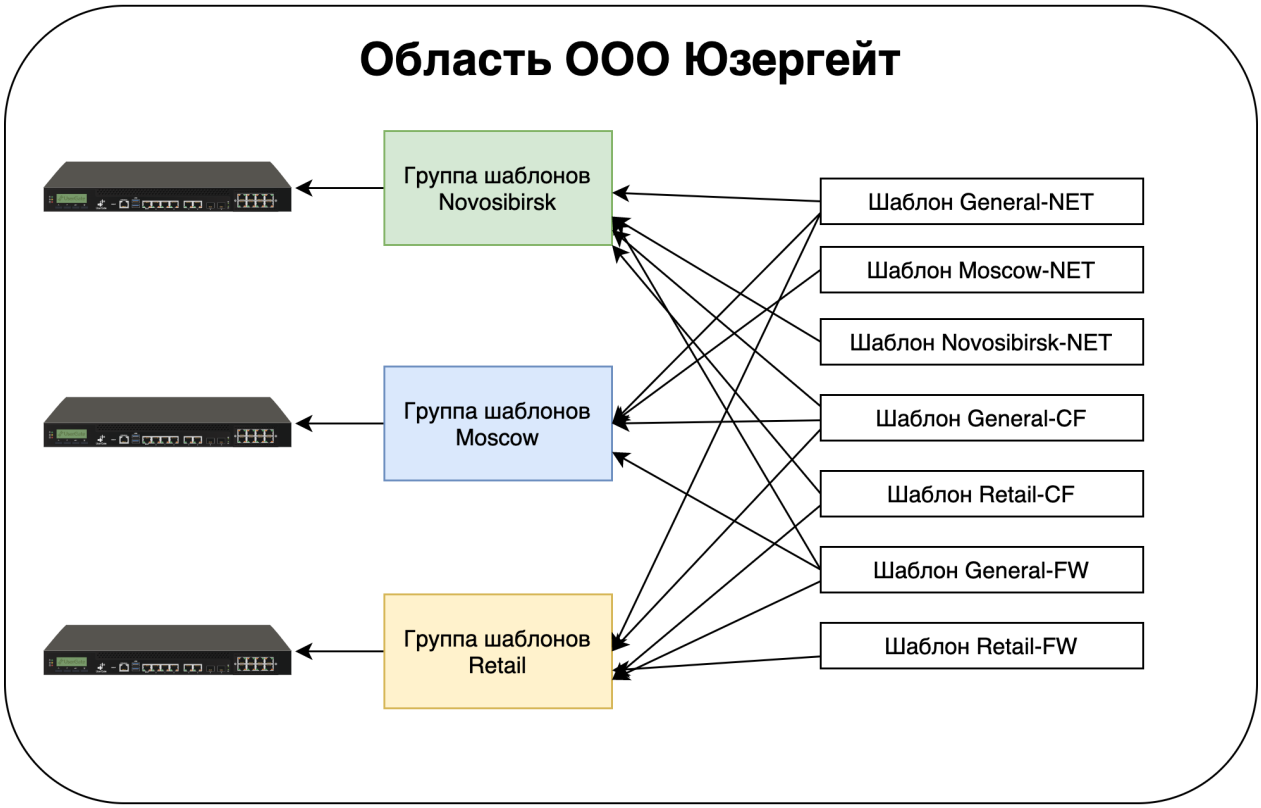
Шаблоны и группы шаблонов

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

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

Новосибирск и т. п.) или функциональной принадлежности МЭ (например, офис продаж, офис разработки, производство и т. п.).

Пример области с несколькими группами шаблонов для управления МЭ UserGate:



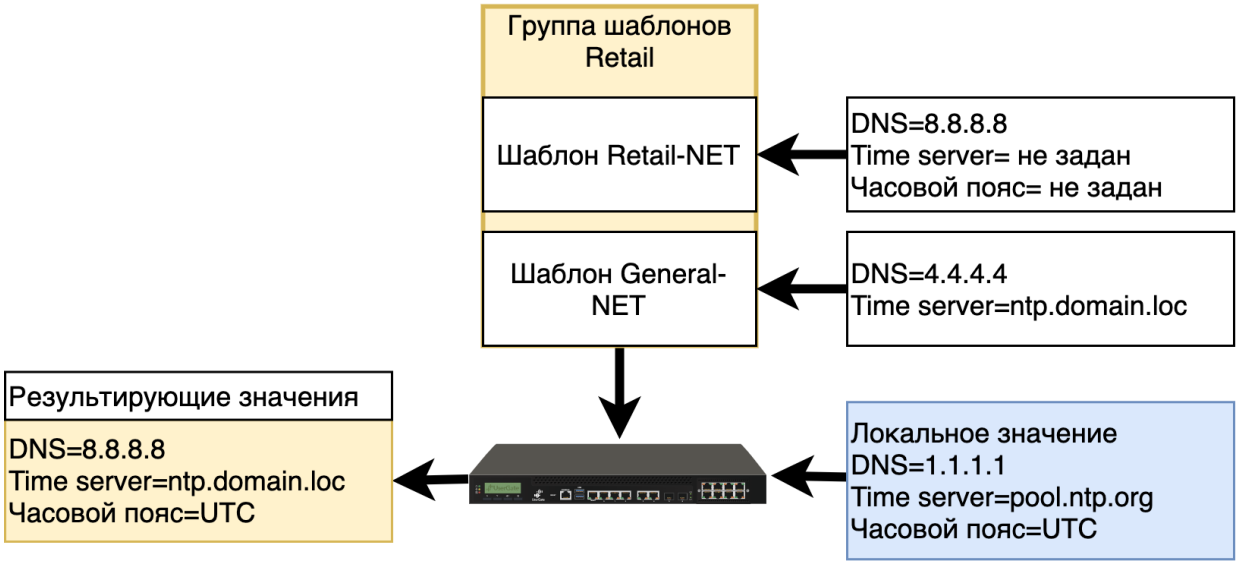
Конфигурация, передаваемая на устройство, может быть двух типов:

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

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

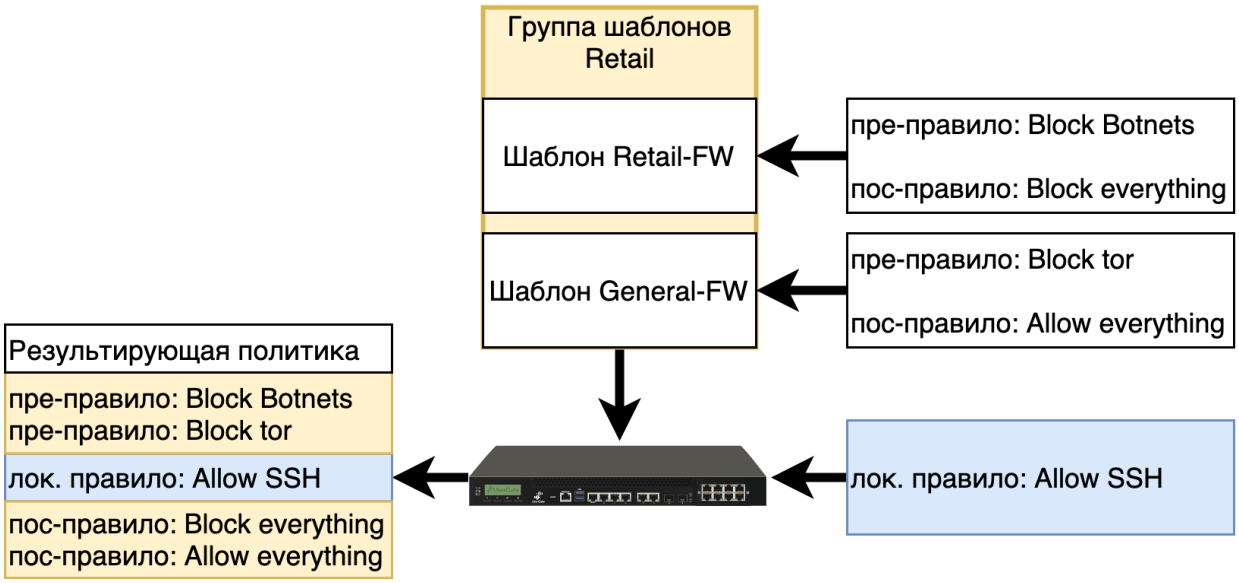
Настройка параметра при конфликтующих значениях в разных шаблонах одной группы шаблонов принимает значение, заданное в наиболее верхнем шаблоне. Локально указанные настройки данного параметра игнорируются.

Пример результирующего значения параметра, определенного в нескольких шаблонах:



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

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



Управляемые устройства

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

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

Версия UGMC	Версия NGFW	Версия LogAn
6.x.x	UGMC совместим с устройствами версий 6.x.x. UGMC несовместим с устройствами версий 7.x.x.	Управление LogAn не поддерживается.
7.0.x	UGMC совместим с устройствами версий 6.x.x, 7.0.x. Для NGFW версий 6.x.x версия протокола синхронизации ниже поддерживаемой UGMC. В таком случае UGMC определит возможность конвертирования конфигурации до меньшей версии и, если конвертирование возможно, передаст конфигурацию на конечное устройство. Если конвертация невозможна — в конфигурации присутствуют параметры, отсутствующие в ранних версиях, то будет отображена ошибка синхронизации. Ошибка будет показана для соответствующего устройства в разделе **Управление NGFW → Устройства NGFW** консоли управления областью. UGMC не совместим с NGFW версий 7.1.x и выше. Причина:	UGMC совместим с устройствами версий 6.x.x, 7.0.x. UGMC несовместим с устройствами версий 7.1.x и выше. Причина: версия протокола синхронизации устройства выше версии протокола, поддерживаемой UGMC.

Версия UGMC	Версия NGFW	Версия LogAn
	версия протокола синхронизации устройства выше версии протокола, поддерживаемой UGMC.	
7.1.x	UGMC совместим с устройствами версий 6.x.x, 7.0.x, 7.1.x. Начиная с версии 7.1.x произошли изменения в конфигурации следующих компонентов: • Система обнаружения и предотвращения вторжений; • Приложения L7; • VPN; • Аутентификация пользователей (добавлен режим аутентификации PKI). UGMC 7.1.x ограниченно поддерживает синхронизацию настроек выше перечисленных разделов при работе с NGFW версий ниже, чем 7.1.x. При синхронизации конфигурации с UGMC 7.1.x на NGFW версий 6.1.x и 7.0.x, ранее подключенных к MC версии ниже: • **СОВ**: после обновления UGMC правила СОВ, полученные от UGMC более ранней версии, станут недоступными для редактирования. • **VPN**: после обновления UGMC все настройки данного раздела, полученные от UGMC более ранней версии, станут	UGMC совместим с устройствами версий 7.0.x, 7.1.x. Управление устройствами версий 6.x.x не предусмотрено.

Версия UGMC	Версия NGFW	Версия LogAn
	недоступными для редактирования. • Все правила межсетевого экрана, в которых указан профиль приложений/СОВ, перед синхронизацией будут принудительно выключены (т.е. данные правила будут отображаться в консоли UGMC, но не будут работать). Для NGFW версий 6.x.x и 7.0.x версия протокола синхронизации ниже поддерживаемой UGMC. В таком случае UGMC определит возможность конвертирования конфигурации до меньшей версии и, если конвертирование возможно, передаст конфигурацию на конечное устройство. Если конвертация невозможна — в конфигурации присутствуют параметры, отсутствующие в ранних версиях, то будет отображена ошибка синхронизации. Ошибка будет показана для соответствующего устройства в разделе **Управление NGFW → Устройства NGFW** консоли управления областью.	

Поддержка в UGMC конфигурации ранних версии ПО UserGate

Поддержка в UGMC 7.1.0 конфигурации ранних версии ПО UserGate

UGMC 7.1.0 ограниченно поддерживает работу NGFW версий 6.1.X и 7.0.X, а именно, не будут работать следующие компоненты системы:

- VPN (NGFW версии 7.0 будут отображаться настройки VPN заблокированными, без возможности редактирования. Ранняя конфигурация VPN продолжает работать, но новая спускаться с UGMC не будет, пока NGFW не обновится до версии 7.1.0);
- IPS&L7;
- Аутентификация в веб-консоль с использованием профилей пользовательских сертификатов (поддержка PKI на NGFW есть только в версии 7.1);
- Аутентификация пользователей в Captive портале с использованием профилей пользовательских сертификатов;
- Правила МЭ, в которых указан L7 или СОВ профиль, отправляются на NGFW 7.0.1/6.1.9 в принудительно выключенном виде.
- Если к UGMC 7.1 подключен NGFW 7.0, на котором настроены правила СОВ, то эти правила будут отображаться в консоли NGFW заблокированными, без возможности редактировать, так как UGMC новой версии ничего про них не знает.

ЛИЦЕНЗИРОВАНИЕ UGMC

Лицензирование UGMC

UGMC лицензируется по количеству активных управляемых устройств. При достижении максимального количества добавление нового управляемого устройства станет невозможным. Учитываются только активные управляемые

устройства, которые включены в разделе **Управляемые устройства**. При наличии нескольких управляемых областей администратор может выделить необходимое количество лицензируемых устройств на каждую область. Общее количество управляемых устройств во всех областях не может превышать количество лицензируемых устройств.

Лицензия на UGMC дает право бессрочного пользования продуктом.

Дополнительно лицензируются следующие модули:

Наименование	Описание
Модуль Security Update (SU)	Модуль SU дает право на получение: • Обновлений ПО UGMC. • Обновлений сигнатур системы обнаружения вторжений. • Обновление сигнатур приложений L7. • Доступ к обновлениям библиотеки соответствия требованиям безопасности (комплаенса). Модуль выписывается на 1 год, по истечении данного срока для получения обновлений необходимо продление лицензии.
Модуль Cluster	Модуль включает лицензию на работу устройств UserGate в режиме "кластер".
Модуль Конечные устройства	Модуль включает в себя работу с конечными устройствами с установленным ПО UserGate Client, являющимся одним из компонентов экосистемы UserGate SUMMA. Подписка на модуль позволяет производить: • Централизованное управление из консоли UGMC конечными устройствами и их доступом в сеть, кроме контроля доступа по результатам проверки соответствия требованиям безопасности (комплаенса). • Сбор телеметрии и событий безопасности конечных устройств. Модуль является бессрочным и выписывается по количеству лицензируемых конечных управляемых устройств.
Модуль Контроль доступа в сеть на уровне хоста	Дополнительный модуль к модулю лицензирования **Конечные устройства**. Подписка на модуль включает в себя: • Проверка конечного устройства на соответствие требованиям безопасности (комплаенса).

Наименование	Описание
	• Контроль доступа в сеть на уровне хоста по результатам проверки. Модуль выписывается на 1 год. По истечении срока действия лицензии, контроль доступа по результатам проверки соответствия требованиям безопасности, становится недоступным. Правила межсетевого экрана, использующие HIP профиль в качестве одного из условий, перестают работают.

Для регистрации продукта необходимо выполнить следующие шаги:

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

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

ПЛАНИРОВАНИЕ ВНЕДРЕНИЯ UGMC

Планирование внедрения UGMC (Описание)

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

При планировании архитектуры рекомендуется:

- Избегать конфликта настроек при добавлении шаблонов в группы шаблонов. Наличие конфликтов всегда усложняет управление конечными устройствами. Это основополагающий принцип, из которого вытекают следующие рекомендации.

- Разделять различные группы настроек в разные шаблоны, например, общие настройки управляемых устройств — в одном, политики контентной фильтрации — в другом, политики межсетевого экранирования — в третьем, политики 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 управляемых устройств, и еще один шаблон с правилами контентной фильтрации, применяемый только для группы устройств. Варьируя положение этих двух шаблонов в группах устройств, администратор может выстроить правильный порядок результирующих правил на конечных устройствах. Данная рекомендация допускает контролируемое количество конфликтных настроек.

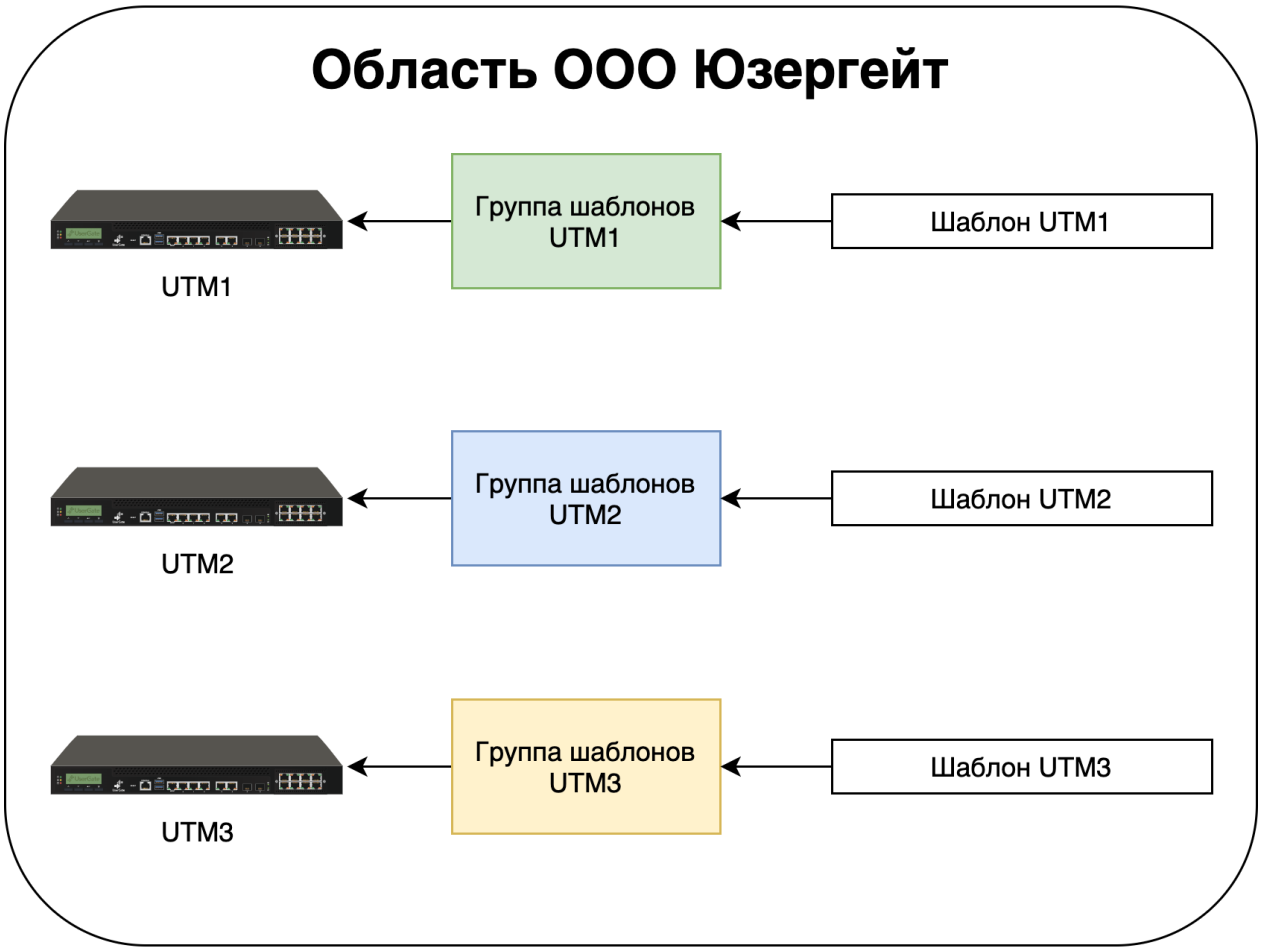
- Помнить про полномочия локальных администраторов. Если предполагается наличие локальных администраторов, то их полномочия будут ограничены настройками тех параметров, которые не заданы через шаблоны UGMC, а правила, созданные локальными администраторами, всегда помещаются между пре- и пост- правилами, применяемыми из UGMC.

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

Один шаблон и одна группа шаблонов на каждое управляемое устройство

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

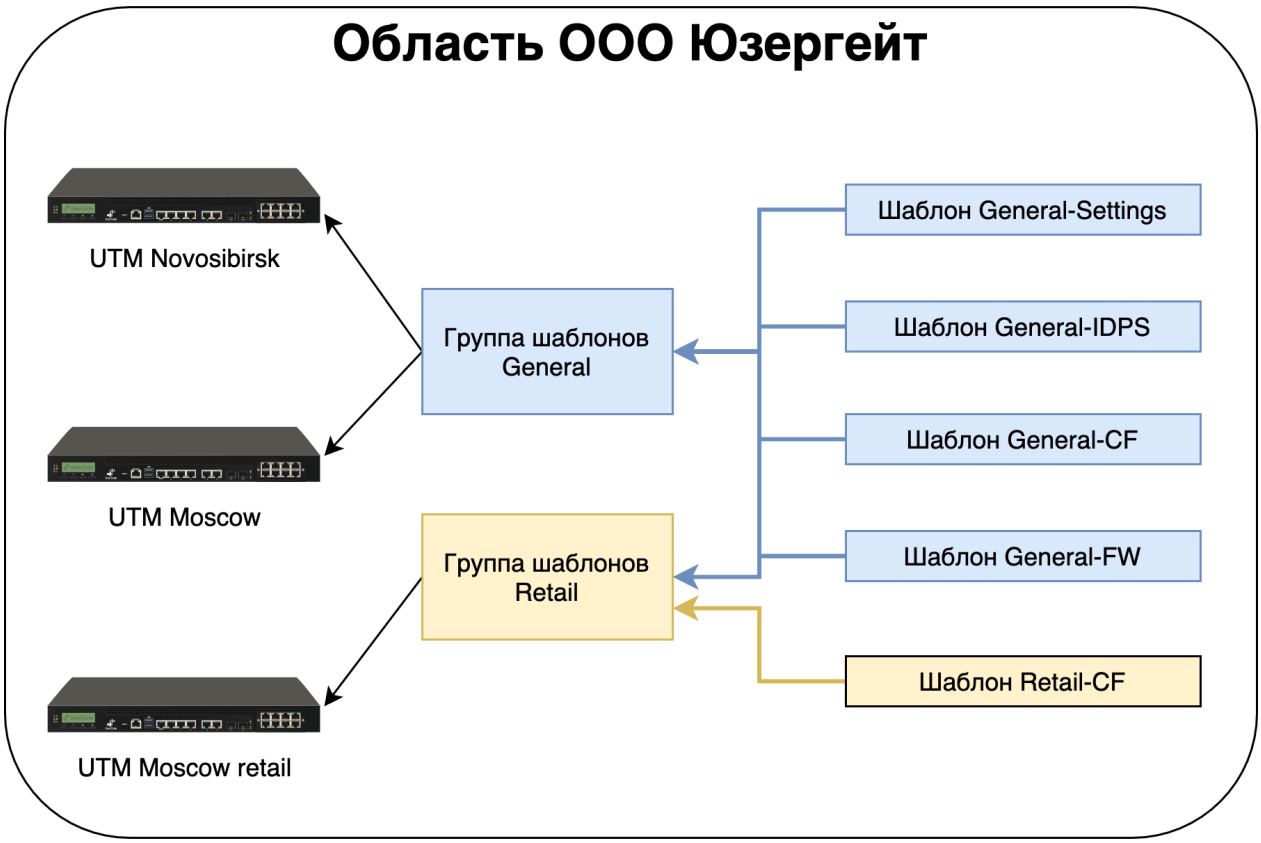
Рекомендуется для простых внедрений с небольшим количеством МЭ UserGate. Пример такой настройки представлен на рисунке ниже.



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

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

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



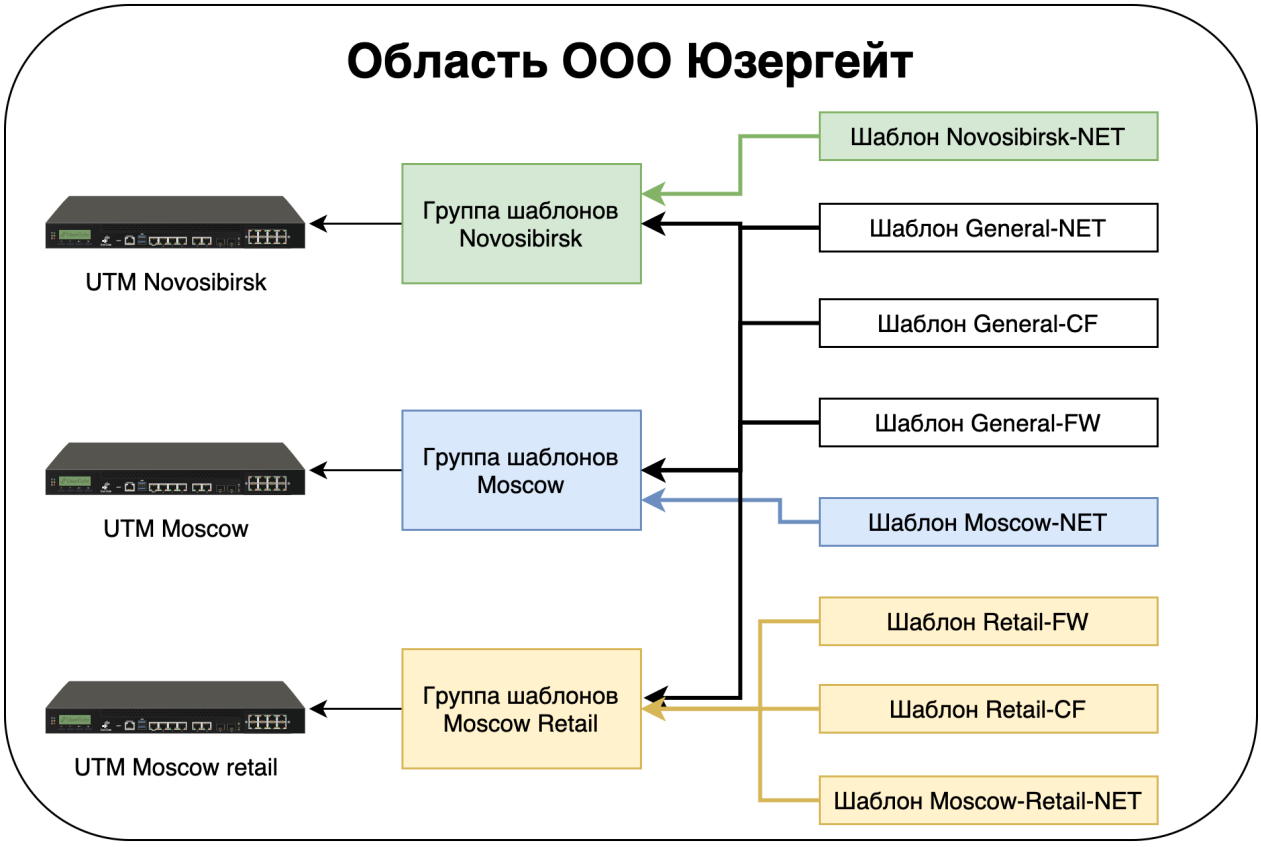
В данном примере шаблоны содержат следующие настройки:

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

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

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

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



В данном примере шаблоны содержат следующие настройки:

- Шаблон General-NET — общие для всех настройки сетевых портов.
- Шаблон General-CF — общие для всех политики контентной фильтрации.
- Шаблон General-FW — общие для всех политики межсетевого экранирования.
- Шаблон Retail-CF — специфичные для ритейловых подразделений политики контентной фильтрации.

- Шаблон Novosibirsk-NET — специфичные для Новосибирского подразделения настройки сетевых портов.
- Шаблон Moscow-NET — специфичные для Московского подразделения настройки сетевых портов.
- Шаблон Moscow-Retail-NET — специфичные для Московского ритейл подразделения настройки сетевых портов.

Примеры шаблонов устройств

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

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

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

В области представлены следующие шаблоны NGFW:

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

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

ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА

Первоначальная настройка

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

Развертывание программно-аппаратного комплекса

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

Развертывание виртуального образа

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

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

Для начала работы с виртуальным образом, выполните следующие шаги:

Наименование	Описание
Шаг 1. Скачайте образ и распакуйте.	Скачайте последнюю версию виртуального образа с официального сайта https://www.usergate.com/ru.

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

Подключение к UGMC

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

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

> **Примечание**
>
> **Если устройство не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать имя администратора системы: "*Admin/system*", В качестве пароля: "*usergate*".**

Остальные интерфейсы отключены и требуют последующей настройки.

Первоначальная настройка требует выполнения следующих шагов:

Наименование	Описание
Шаг 1. Подключиться к интерфейсу управления.	**При наличии DHCP-сервера** Подключить интерфейс port0 в сеть предприятия с работающим DHCP-сервером. Включить UGMC. После загрузки консоль UGMC укажет IP-адрес, на который необходимо подключиться для дальнейшей активации продукта. **Статический IP-адрес** Включить UGMC. Используя CLI (Command Line Interface), назначить необходимый IP-адрес на интерфейс port0. Детали использования CLI смотрите в главе Интерфейс командной строки (CLI). Подключиться к веб-консоли UGMC по указанному адресу, он должен выглядеть примерно следующим образом: https://UGMC_IP_address:8010
Шаг 2. Выбрать язык.	Выбрать язык, на котором будет продолжена первоначальная настройка.
Шаг 3. Задать пароль корневого администратора UserGate Management Center.	Задать логин и пароль для входа в веб-интерфейс управления.
Шаг 4. Зарегистрировать систему.	Ввести ПИН-код для активации продукта и заполнить регистрационную форму. Для активации системы необходим доступ UGMC в интернет. Если на данном этапе выполнить регистрацию не удается, то ее следует повторить после настройки сетевых интерфейсов на шаге 8.
Шаг 5. Настроить зоны, IP-адреса интерфейсов, подключить UserGate Management Center в сеть предприятия.	В разделе **Интерфейсы** включить необходимые интерфейсы, установить корректные IP-адреса, соответствующие вашим сетям, и назначить интерфейсы соответствующим зонам. Подробно об управлении

Наименование	Описание
	интерфейсами читайте в главе Настройка интерфейсов. Система поставляется с предопределенными зонами: • Зона **Management** (сеть управления), интерфейс port0. • Зона **Trusted** (LAN). Предполагается, что через эту зону UGMC будет подключаться к управляемым устройствам, а также получит доступ в интернет. Для работы UGMC достаточно одного настроенного интерфейса. Разделение функций управления устройством UGMC и управления управляемыми устройствами UserGate на разные сетевые интерфейсы рекомендовано для обеспечения безопасности, но не является обязательным требованием.
Шаг 6. Настроить шлюз в интернет.	В разделе **Шлюзы** указать IP-адрес шлюза в интернет на интерфейсе, который имеет доступ в интернет, как правило, это зона Trusted. Подробно о настройке шлюзов в интернет читайте в главе Настройка шлюзов.
Шаг 7. Указать системные DNS-серверы.	В разделе **Настройки** укажите IP-адреса серверов DNS вашего провайдера или серверов, используемых в вашей организации.
Шаг 8. Зарегистрировать продукт (если не был зарегистрирован на шаге 4).	Зарегистрировать продукт с помощью ПИН-кода. Для успешной регистрации необходимо подключение к интернету и выполнение предыдущих шагов. Более подробно о лицензировании продукта читайте в главе Лицензирование UGMC.
Шаг 9. Создать как минимум одну управляемую область.	В разделе **Управляемые области → Области** добавить управляемую область.
Шаг 10. Создать администратора созданной управляемой области.	В разделе **Администраторы** создать профиль администратора и дать ему права на управление созданной областью. Создать администратора с данным профилем.
Шаг 11. Создать дополнительных администраторов UGMC (опционально).	В разделе **Администраторы** создать необходимые профили для управления сервисами UGMC и создать администраторов UGMC с этими профилями.

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

ОФЛАЙН ОПЕРАЦИИ С СЕРВЕРОМ

Офлайн операции с сервером(Описание)

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

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

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

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

Наименование	Описание
Check filesystems	Запуск проверки файловой системы устройства на наличие ошибок и их автоматическое исправление.
Expand data partition	Увеличение раздела для хранения данных на весь выделенный диск. Эта операция обычно используется после увеличения дискового пространства, выделенного

Наименование	Описание
	гипервизором для виртуальной машины UserGate. Данные и настройки UserGate не сбрасываются.
Create backup	Создать полную копию диска UserGate на внешний USB носитель. Все данные на внешнем носителе будут удалены.
Restore from backup	Восстановление UserGate с внешнего USB носителя.
Factory reset	Сброс состояния UserGate к первоначальному состоянию системы. Все данные и настройки будут утеряны.
Exit	Выход и перезагрузка устройства.

НАСТРОЙКА UGMC

Общие настройки

Раздел **Настройки** определяет базовые установки UGMC:

Наименование	Описание
Часовой пояс	Часовой пояс, соответствующий вашему местоположению. Часовой пояс используется в расписаниях, применяемых в правилах, а также для корректного отображения даты и времени в отчетах, журналах и т.п.
Язык интерфейса по умолчанию	Язык, который будет использоваться по умолчанию в консоли.
Таймер автоматического закрытия сессии (мин.)	Настройка таймера автоматического закрытия сессии в случае отсутствия активности администратора в веб-консоли.
Настройка времени сервера	Настройка параметров установки точного времени. • **Использовать NTP** — использовать сервера NTP из указанного списка для синхронизации времени. • **Основной NTP-сервер** — адрес основного сервера точного времени. Значение по умолчанию — pool.ntp.org. • **Запасной NTP-сервер** — адрес запасного сервера точного времени.

Наименование	Описание
	• **Время на сервере (UTC)** — позволяет установить время на сервере. Время должно быть указано в часовом поясе UTC.
Расписание скачивания обновлений	Настройки для управления скачиванием обновлений программного обеспечения UserGate (UGOS) и обновляемыми библиотеками, предоставляемыми по подписке. • **Обновления ПО** — настройка расписания проверки наличия новых обновлений UGOS и скачивания обновлений. • **Обновления библиотек** — настройка расписания проверки наличия новых обновлений библиотек и скачивания библиотек. Флажок **Единое расписание для всех обновлений** применяет расписание ко всем библиотекам, иначе для каждой библиотеки необходимо настроить собственное расписание. При задании расписания возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а

Наименование	Описание
	выражение "*/2" в поле "часы" будет означать "каждые два часа.
Настройка учета изменений	При включении данной опции и создания **Типов изменений** любое изменение в конфигурацию, вносимое администратором через веб-консоль, будет требовать указание типа изменения и описания вносимого изменения. В качестве типов изменения могут быть, например, указаны: • Распоряжение. • Приказ. • Регламентные работы, и т.д. Количество типов изменений не ограничено.
Системные DNS-серверы	Укажите корректные IP-адреса серверов DNS в настройке.

Управление устройством

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

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

Кластеризация и отказоустойчивость

UGMC поддерживает 2 типа кластеров:

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

Примечание

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

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

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

Для создания кластера конфигурации необходимо выполнить следующие шаги:

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

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

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

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

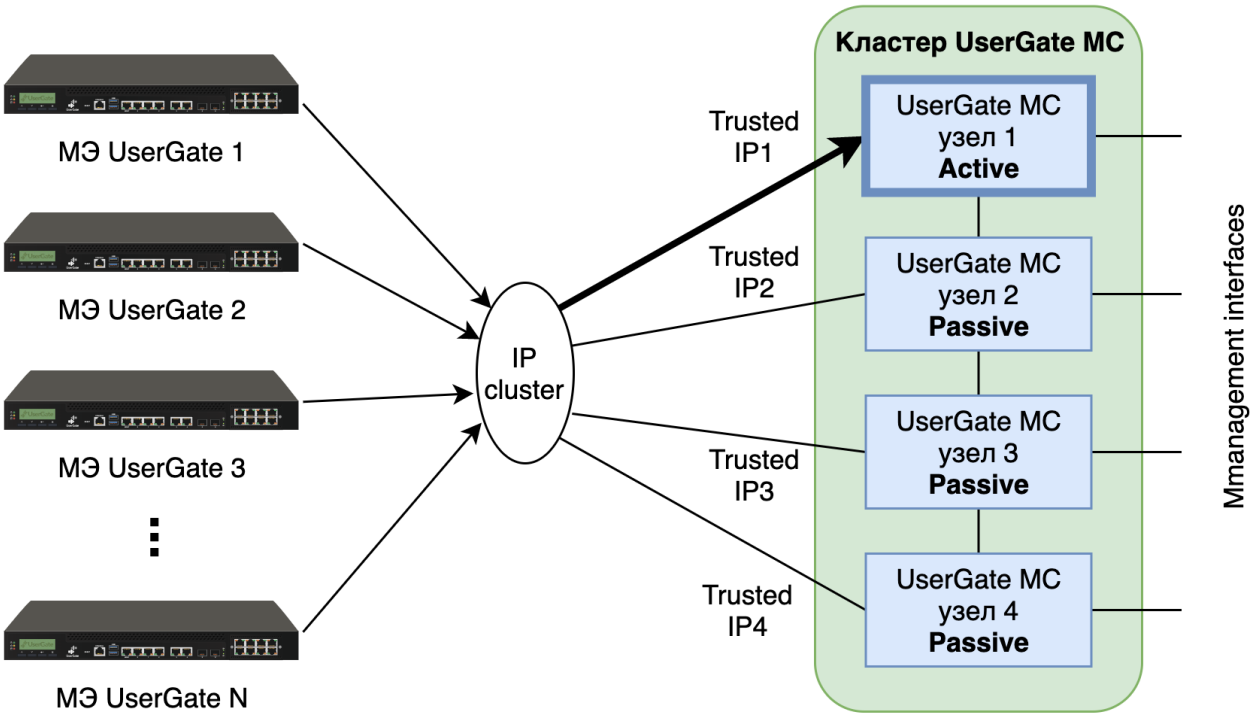
- Запасной сервер не получает подтверждения о том, что главный узел в сети, например, если он выключен или отсутствует сетевая доступность узлов.

На главном узле настроена проверка доступа в интернет.

- Сбой в работе ПО UserGate.

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

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



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

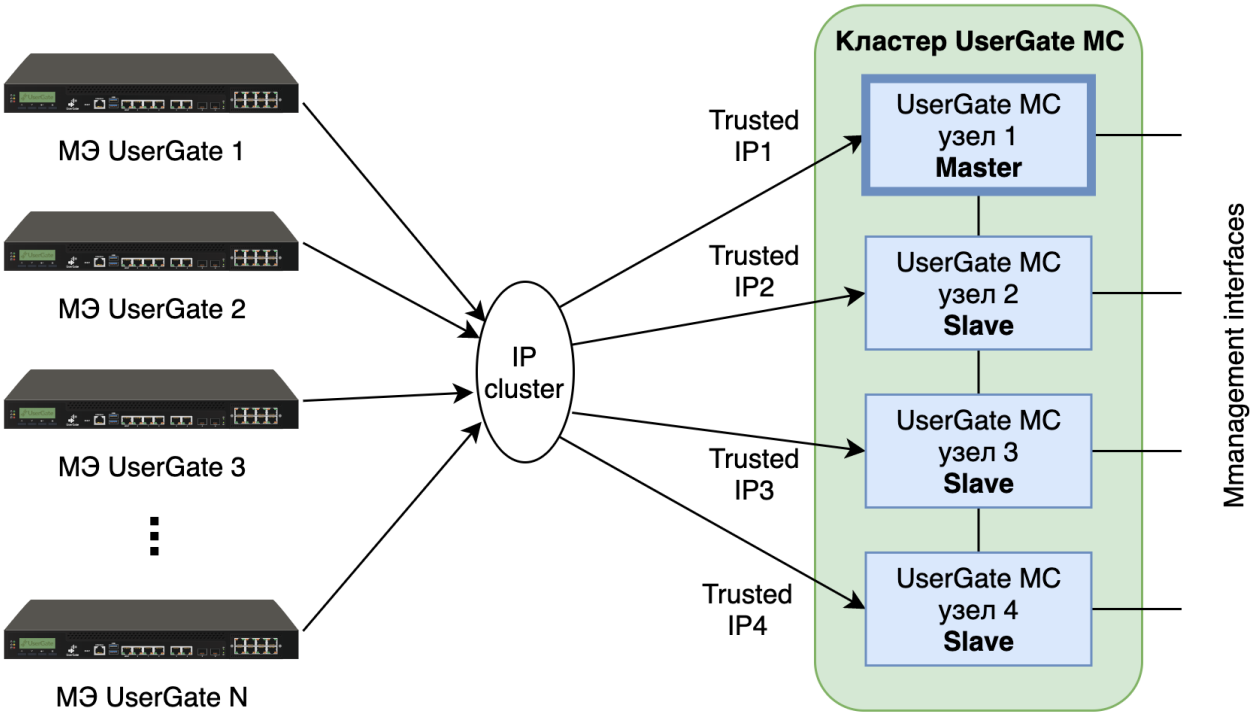
В режиме **Актив-Актив** один из серверов выступает в роли Мастер-узла, распределяющего трафик на все остальные узлы кластера. Поскольку IP-адрес кластера находится на Мастер-узле, то Мастер-узел отвечает на ARP-запросы клиентов. Выдавая последовательно MAC-адреса всех узлов отказоустойчивого кластера,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

виртуальных IP-адресов. Перемещение роли Мастер-узла на один из запасных узлов происходит при следующих событиях:

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

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

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



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

Для создания отказоустойчивого кластера необходимо выполнить следующие шаги:

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

Параметры отказоустойчивого кластера:

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

Наименование	Описание
Виртуальные IP-адреса	Назначаются виртуальные IP-адреса и их соответствие интерфейсам узлов кластера.

Диагностика

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

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

Наименование	Описание
	• **Токен удаленного помощника** — полученное случайным образом значение токена. Уникально для каждого включения удаленного помощника.

Операции с сервером

Данный раздел позволяет произвести следующие операции с сервером:

Наименование	Описание
Операции с сервером	• **Перезагрузить** — перезагрузка сервера UGMC. • **Выключить** — выключение сервера UGMC.
Обновления	Выбор канала обновлений ПО UGMC • **Стабильные** — проверка наличия стабильных обновлений ПО. • **Бета** — проверка наличия экспериментальных обновлений.
Обновления сервера	Индикация имеющихся обновлений UGMC. Запуск процесса обновления сервера с возможностью создания точки восстановления. Просмотр списка изменений ПО в обновлении.
Офлайн обновления	Загрузка файла для офлайн обновления.
Настройки вышестоящего прокси для проверки лицензий и обновлений	Настройка параметров вышестоящего HTTP(S) прокси-сервера для обновления лицензии и обновления ПО UGMC. Необходимо указать IP-адрес и порт вышестоящего прокси сервера. При необходимости указать логин и пароль для аутентификации на вышестоящем прокси-сервере.

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

Для установки обновлений необходимо выполнить следующие действия:

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

Управление резервным копированием

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

Для создания резервной копии необходимо выполнить следующие действия:

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

Для восстановления состояния устройства необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Восстановить состояние устройства	В разделе **Управление устройством → Управление резервным копированием** нажать **Восстановление из резервной копии** и указать путь к ранее созданному файлу

Наименование	Описание
	настроек для его загрузки на сервер. Восстановление будет предложено в консоли tty при перезагрузке устройства.

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

Наименование	Описание
Шаг 1. Создать правило экспорта конфигурации	В разделе **Управление устройством → Управление резервным копированием** нажать кнопку **Добавить**, указать имя и описание правила.
Шаг 2. Указать параметры удаленного сервера	Во вкладке правила **Удаленный сервер** указать параметры удаленного сервера: • **Тип сервера** — FTP или SSH. • **Адрес сервера** — IP-адрес сервера. • **Порт** — порт сервера. • **Логин** — учетная запись на удаленном сервере. • **Пароль**/**Повторите пароль** — пароль учетной записи. • **Путь на сервере** — путь на сервере, куда будут выгружены настройки. В случае использование SSH-сервера возможно использование авторизации по ключу. Для импорта или генерации ключа необходимо выбрать **Настроить SSH-ключ** и указать **Сгенерировать ключи** или **Импортировать ключ**. **Важно!** При повторном создании ключа существующий SSH-ключ будет удален. Публичный ключ должен находиться на SSH-сервере в директории пользовательских ключей **/home/user/.ssh/** в файле **authorized_keys**. При первоначальной настройке правила экспорта резервного копирования по SSH обязательна проверка соединения (кнопка **Проверить соединение**); при проверке соединения fingerprint помещается в known_hosts, без проверки файлы не будут отправляться. **Важно!** Если сменить сервер SSH или его переустановить, то файлы резервного копирования будут недоступны, так как fingerprint изменится — это защита от спуфинга.
Шаг 3. Выбрать расписание выгрузки	Во вкладке правила **Расписание** указать необходимое время отправки настроек. В случае задания времени в crontab-формате, задайте его в следующем виде: (минуты:0-59) (часы:0-23) (дни месяца:1-31) (месяц:1-12) (день недели:0-6, 0-воскресенье)

Наименование	Описание
	Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка и тире используются для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

Экспорт и импорт настроек

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

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

Для экспорта настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Экспорт настроек.	В разделе **Управление устройством → Экспорт и импорт настроек** нажать на ссылку **Экспорт** и выбрать **Экспортировать все настройки** или **Экспортировать сетевые настройки**. Система сохранит: • текущие настройки сервера под именем: cc_core-mc_core@nodename_version_YYYYMMDD_HHMMSS.bin • сетевые настройки под именем: network-cc_core-mc_core@nodename_version_YYYYMMDD_HHMMSS.bin

Наименование	Описание
	nodename — имя узла UserGate Management Center. version — версия UserGate Management Center. YYYYMMDD_HHMMSS — дата и время выгрузки настроек в часовом поясе UTC. Например, cc_core-mc_core@ediasaionedi_7.0.0.93R-1_20220715_084853.bin или network-cc_core-mc_core@ediasaionedi_7.0.0.93R-1_20220715_084929.bin.

Для применения созданных ранее настроек необходимо выполнить следующие действия:

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

Примечание

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

Подробнее об особенностях импорта настроек кластерного решения читайте в статье Импорт настроек из файлов конфигурации кластера NGFW.

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

Наименование	Описание
Шаг 1. Создать правило экспорта.	В разделе **Управление устройством → Экспорт настроек** нажать кнопку **Добавить**, указать имя и описание правила
Шаг 2. Указать параметры удаленного сервера.	Во вкладке правила **Удаленный сервер** указать параметры удаленного сервера: • **Тип сервера** — FTP или SSH. • **Адрес сервера** — IP-адрес сервера. • **Порт** — порт сервера. • **Логин** — учетная запись на удаленном сервере.

Наименование	Описание
	• **Пароль/Подтверждение пароля** — пароль учетной записи. • **Путь на сервере** — путь на сервере, куда будут выгружены настройки.
Шаг 3. Выбрать расписание выгрузки.	Во вкладке правила **Расписание** указать необходимое время отправки настроек. В случае задания времени в CRONTAB-формате, задайте его в следующем виде: (минуты:0-59) (часы:0-23) (дни месяца:1-31) (месяц:1-12) (день недели:0-6, 0-воскресенье) Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка и тире используются для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

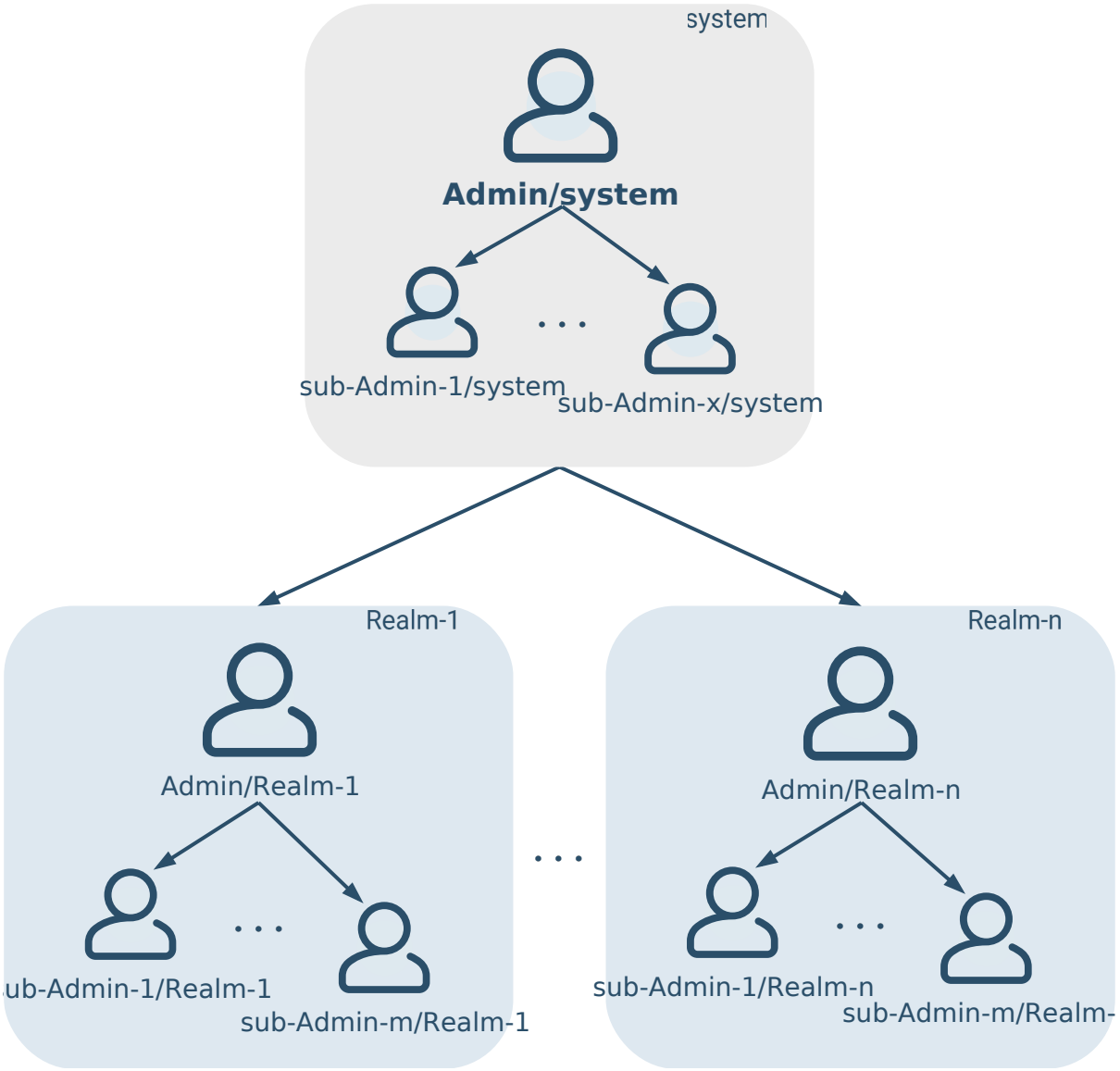
Администраторы

Иерархическая система учетных записей администраторов

В UserGate MC (UGMC) реализована иерархическая система учетных записей администраторов.

Верхний уровень (system) образуют учетные записи администраторов самой системы UGMC.

Нижний уровень образуют учетные записи администраторов управляемых областей (Realms) — логических объектов, предназначенных для управления группой подконтрольных устройств (подробнее об управляемых областях читайте в разделе Управление областями).



При первоначальной настройке UGMC создается локальный администратор с логином **Admin/system**, который является корневым администратором системы. Администратор UGMC может управлять общими и сетевыми настройками UGMC, активировать лицензии UGMC, создавать и редактировать элементы системной библиотеки, управлять политиками обновления и резервного копирования, мониторить работу UGMC по системным журналам. Администратор UGMC может создавать дополнительные учетные записи суб-администраторов UGMC, делегируя им часть прав по управлению системой.

Администратор UGMC создаёт управляемые области (Realms). Управлять устройствами, входящими в управляемые области, администратор UGMC не может. Для этого администратор UGMC создает учетные записи корневых администраторов управляемых областей (*Admin/Realm*). Корневой администратор области имеет все права на управление областью и подконтрольными устройствами в своей области. Он может создавать серверы

и профили аутентификации области, каталоги пользователей, шаблоны настроек управляемых устройств, объединять шаблоны в группы настроек и подключать к ним объекты управляемых устройств. Корневой администратор управляемой области может также создавать учетные записи суб-администраторов своей области (*sub-Admin/Realm*) или, иначе говоря, региональных администраторов, делегируя им права на администрирование только отдельных выделенных устройств.

Создание учетных записей администраторов

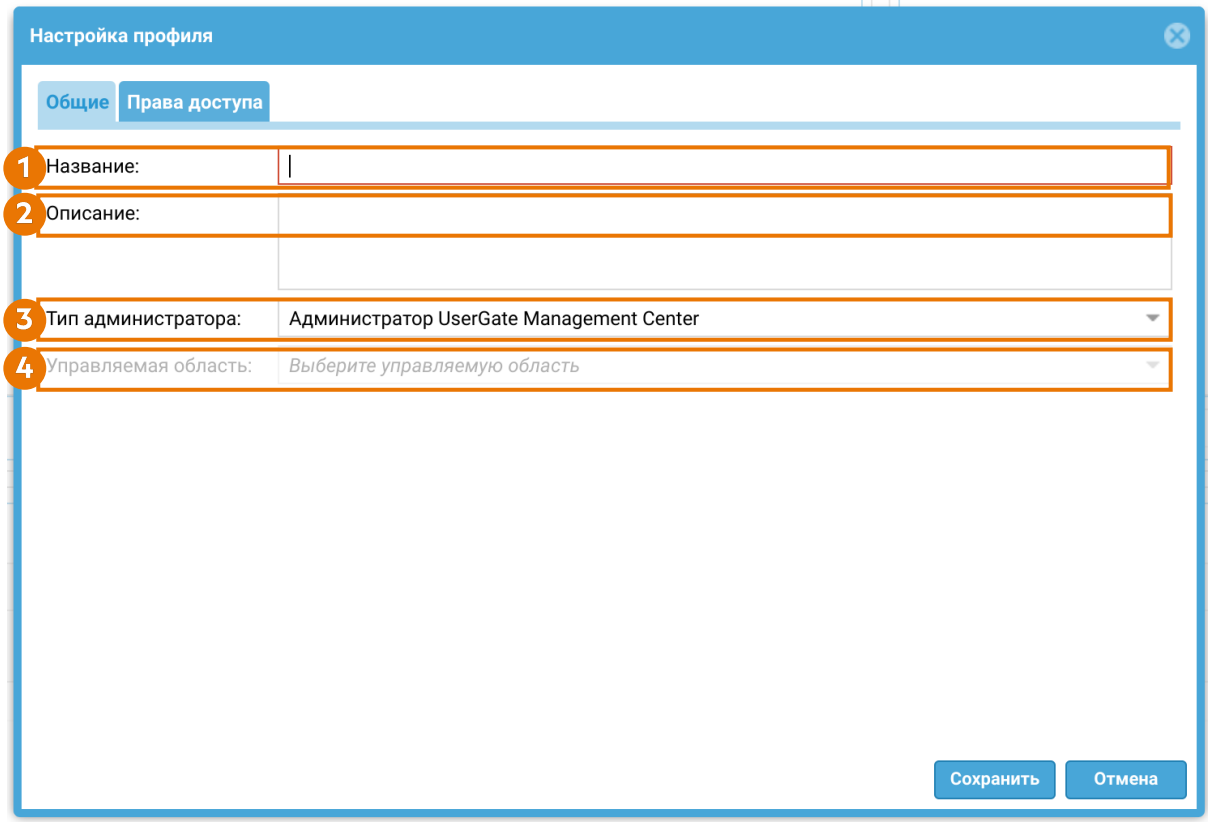
Для создания учетных записей администраторов необходимо выполнить следующие действия:

1. Создать профиль администратора.

2. Создать учетную запись администратора и назначить ей один из созданных ранее профилей администратора.

Создание профиля администратора

Для создания профиля администратора в веб-консоли управления UGMC необходимо перейти в раздел **Администраторы → Профили администраторов**, нажать кнопку **Добавить** и указать необходимые настройки:

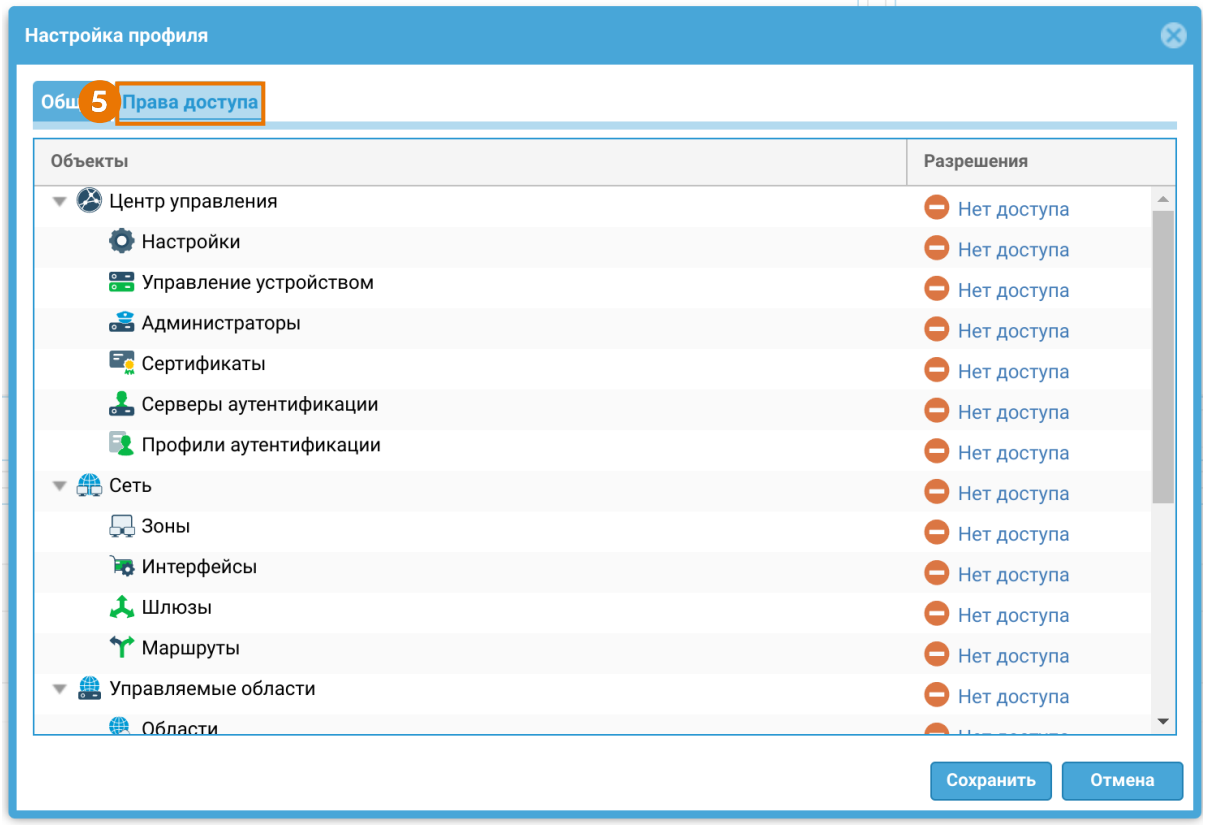


1. Задать **название профиля**.

2. Опционально **описать** назначение профиля.

3. Выбрать **тип администратора**. Для предоставления полномочий управления системой UGMC необходимо выбрать тип **Администратор UserGate Management Center**. Вариант **Администратор области** следует выбирать при создании корневого администратора управляемой области.

4. При создании корневого администратора управляемой области выбрать **управляемую область**.Область должна быть создана заранее.

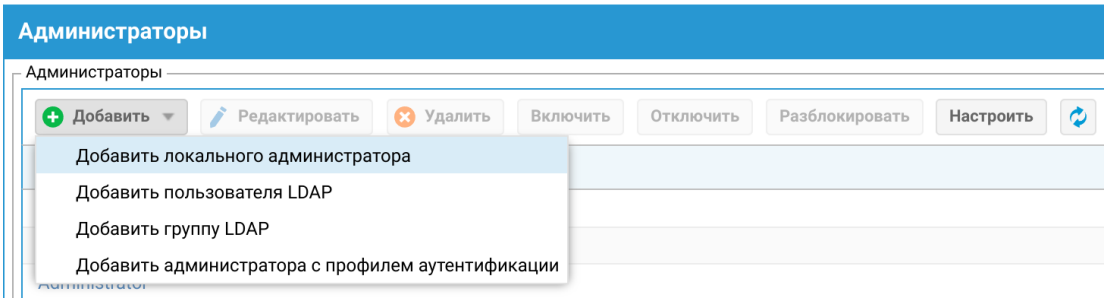


5. Администратор системы UGMC может выбрать делегируемые права доступа суб-администраторам системы. Корневые администраторы областей создаются с полными правами на свою область.

На вкладке **Права доступа** указан список объектов дерева веб-консоли, доступных для делегирования. В поле разрешений для доступа можно выбрать: **Нет доступа**; **Чтение**; **Чтение и запись**.

Создание учетной записи администратора

Для создания учетной записи администратора в веб-консоли управления UGMC необходимо перейти в раздел **Администраторы**, нажать кнопку **Добавить** и выбрать необходимый вариант:



- **Добавить локального администратора** — создать локального пользователя, задать ему пароль доступа и назначить созданный ранее профиль доступа.
- **Добавить пользователя LDAP** — добавить пользователя из существующего домена. Для этого должен быть корректно настроен LDAP-коннектор в разделе **Серверы аутентификации**. При входе в консоль администрирования необходимо указывать имя пользователя в формате user@domain/system или domain\user/system. Назначить созданный ранее профиль.
- **Добавить группу LDAP** — добавить группу пользователей из существующего домена. Для этого должен быть корректно настроен LDAP-коннектор в разделе **Серверы аутентификации**. При входе в консоль администрирования необходимо указывать имя пользователя в формате user@domain/system или domain\user/system. Назначить созданный ранее профиль.
- **Добавить администратора с профилем аутентификации** — создать пользователя, назначить созданный ранее профиль администратора и профиль аутентификации (необходимы корректно настроенные серверы аутентификации).

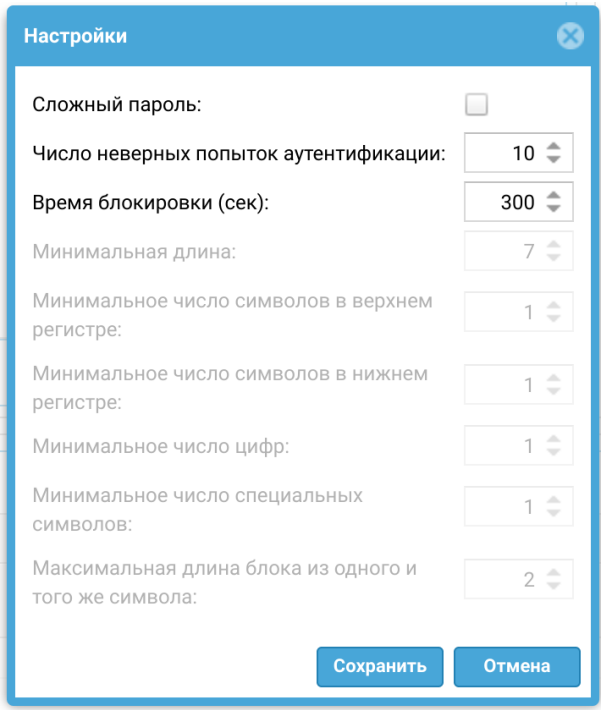
Важно!

В данном разделе настроек 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.

Дополнительные настройки

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

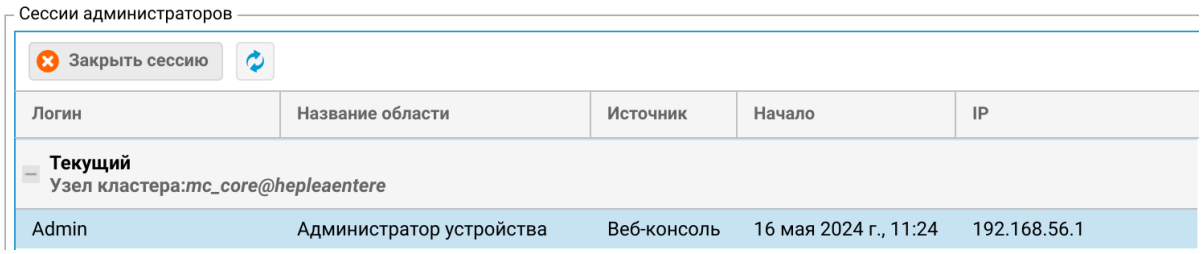
Для настройки этих параметров в веб-консоли управления UGMC необходимо в разделе **Администраторы → Администраторы** нажать кнопку **Настроить**. Далее необходимо заполнить следующие поля:



- **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.

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

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



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

> **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 во вкладке **Контроль доступа** разрешить доступ к сервису **Консоль администрирования**. Более подробно о настройке контроля доступа к зонам можно прочитать в разделе Настройка зон.

Сертификаты

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

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

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

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

Для экспорта сертификата необходимо:

Наименование	Описание
Шаг 1. Выбрать сертификат для экспорта.	Выделить необходимый сертификат в списке сертификатов.
Шаг 2. Экспортировать сертификат.	Выбрать тип экспорта: • **Экспорт сертификата** — экспортирует данные сертификата в der-формате без экспортирования приватного ключа сертификата.

Наименование	Описание
	• **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 не разрешает экспорт приватных ключей сертификатов.

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

Наименование	Описание
Шаг 1. Начать импорт.	Нажать на кнопку **Импорт.**
Шаг 2. Заполнить необходимые поля.	Указать значения следующих полей: • Название — название сертификата, под которым он будет отображен в списке сертификатов. • Описание — описание сертификата. • Загрузите файл, содержащий данные сертификата. • Загрузите файл, содержащий приватный ключ сертификата. • Пароль для приватного ключа, если таковой требуется. • Цепочка сертификатов — файл, содержащий сертификаты вышестоящих центров сертификации, которые участвовали в создании сертификата. Необязательное поле.

Серверы аутентификации

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

LDAP-коннектор

LDAP-коннектор позволяет:

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

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

Наименование	Описание
Включено	Включает или отключает использование данного сервера аутентификации.
Название	Название сервера аутентификации.
SSL	Определяет, требуется ли SSL-соединение для подключения к LDAP-серверу.
Доменное имя LDAP или IP-адрес	IP-адрес контроллера домена, FQDN контроллера домена или FQDN домена (например, test.local). Если указан FQDN, то UserGate получит адрес контроллера домена с помощью DNS-запроса. Если указан FQDN домена, то при отключении основного контроллера домена, UserGate будет использовать резервный.
Bind DN («login»)	Имя пользователя, которое необходимо использовать для подключения к серверу LDAP. Имя необходимо использовать в формате DOMAIN\username или username@domain. Данный пользователь уже должен быть заведен в домене
Пароль	Пароль пользователя для подключения к домену.
Домены LDAP	Список доменов, которые обслуживаются указанным контроллером домена, например, в случае дерева доменов

Наименование	Описание
	или леса доменов Active Directory. Здесь же можно указать короткое netbios имя домена.
Пути поиска	Список путей в сервере LDAP, начиная с которых система будет осуществлять поиск пользователей и групп. Необходимо указывать полное имя, например, ou=Office,dc=example,dc=com.

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

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

domain\user/system или *user@domain/system*

Сервер аутентификации RADIUS

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

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

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

Для авторизации пользователей в веб-интерфейсе UserGate с помощью сервера RADIUS необходимо настроить профиль аутентификации. Подробнее о

создании и настройке профилей читайте в разделе Профили аутентификации UGMC.

Сервер аутентификации TACACS+

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

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

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

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

Профили аутентификации

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

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

Библиотеки элементов

IP-адреса

Раздел IP-адреса содержит список диапазонов IP-адресов, которые могут быть использованы при настройке UGMC. Первоначальный список адресов поставляется вместе с продуктом. 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 **Д обавить** и ввести адреса. IP-адреса вводятся в виде IP-адрес, IP-адрес/маска сети или диапазон IP-адресов, например: 192.168.1.5, 192.168.1.0/24 или 192.168.1.5-192.168.2.100.

Администратор имеет возможность создавать свои списки IP-адресов и централизованно распространять их на все устройства с установленным

UserGate. 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.
	Список адресов записывается в обычный текстовый файл, где адреса прописываются в столбик без знаков препинания. Например:
	`x.x.x.x`
	`y.y.y.y`
	`z.z.z.z`

Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем **list.zip.**
Шаг 3. Создать файл с версией списка.	Создать файл **version.txt**, внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте **list.zip** и **version.txt**, чтобы они были доступны для скачивания.
Шаг 5. Создать список IP-адресов и указать URL для обновления.	На каждом устройстве создать список IP-адресов. При создании указать тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. Устройства будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. **Примечание**URL списка задается в формате: http://x.x.x.x/ или ftp://x.x.x.x/. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную.

Наименование	Описание
	При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

Почтовые адреса

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

Для добавления новой группы почтовых адресов необходимо выполнить следующие шаги:

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

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

Наименование	Описание
	Создать файл **list.txt** со списком почтовых адресов.

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

Наименование	Описание
	черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

Номера телефонов

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

Для добавления новой группы телефонных номеров необходимо выполнить следующие шаги:

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

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

Наименование	Описание
Шаг 1. Создать файл с необходимыми списком номеров.	Создать файл **list.txt** со списком номеров.
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем **list.zip**.
Шаг 3. Создать файл с версией списка.	Создать файл **version.txt**, внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте **list.zip и version.txt**, чтобы они были доступны для скачивания.
Шаг 5. Создать список телефонных номеров и указать URL для обновления.	На каждом UserGate создать список номеров. При создании указать тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. UserGate будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания

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

Профили оповещений

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

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

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

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

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

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Хост	IP-адрес сервера SMPP, который будет использоваться для отсылки SMS сообщений.
Порт	Порт TCP, используемый сервером SMPP. Обычно для протокола SMPP используется порт 2775, для SMPP с использованием SSL — 3550.
SSL	Использовать или нет шифрацию с помощью SSL.
Логин	Имя учетной записи для подключения к SMPP-серверу.

Наименование	Описание
Пароль	Пароль учетной записи для подключения к SMPP-серверу.
Правила трансляции номеров	В некоторых случаях SMPP-провайдер ожидает номер телефона в определенном формате, например, в виде 89123456789. Для соответствия требованиям провайдера можно указать замену первых символов номеров с одних на другие. Например, заменить все номера, начинающиеся на +7, на 8.

Расширение системного раздела

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

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

Примечание

Расширение системного раздела путем увеличения размера *имеющегося* диска виртуальной машины возможно только при сбросе узла до заводских настроек, т.е. при выполнении операции factory reset.

НАСТРОЙКА СЕТИ

Настройка сети (описание)

В данном разделе описаны сетевые настройки UGMC.

Настройка зон

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

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

По умолчанию UGMC поставляется со следующими зонами:

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

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

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

> **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).	

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

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

Настройка интерфейсов

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

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

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

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

- VLAN.
- Бонд.

Объединение интерфейсов в бонд

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

Наименование	Описание
Включено	Включает бонд.
Название	Название бонда.
Зона	Зона, к которой принадлежит бонд.
Интерфейсы	Один или более интерфейсов, которые будут использованы для построения бонда.
Режим	

Наименование	Описание
	Режим работы бонда должен совпадать с режимом работы на том устройстве, куда подключается бонд. Может быть: • **Round robin.** Пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. Эта политика применяется для балансировки нагрузки и отказоустойчивости. • **Active backup**. Только один сетевой интерфейс из объединенных будет активным. Другой интерфейс может стать активным только в том случае, когда упадет текущий активный интерфейс. При такой политике MAC-адрес бонд-интерфейса виден снаружи только через один сетевой порт, во избежание появления проблем с коммутатором. Эта политика применяется для отказоустойчивости. • **XOR.** Передача распределяется между сетевыми картами используя формулу: [(«MAC-адрес источника» XOR «MAC-адрес назначения») по модулю «число интерфейсов»]. Получается, одна и та же сетевая карта передает пакеты одним и тем же получателям. Опционально распределение передачи может быть основано и на политике «xmit_hash». Политика XOR применяется для балансировки нагрузки и отказоустойчивости. • **Broadcast.** Передает все на все сетевые интерфейсы. Эта политика применяется для отказоустойчивости. • **IEEE 802.3ad** — режим работы, установленный по умолчанию, поддерживается большинством сетевых коммутаторов. Создаются агрегированные группы сетевых карт с одинаковой скоростью и дуплексом. При таком объединении передача задействует все каналы в активной агрегации согласно стандарту IEEE 802.3ad. Выбор, через какой интерфейс отправлять пакет, определяется политикой; по умолчанию используется XOR-политика, можно также использовать «xmit_hash» политику. • **Adaptive transmit load balancing.** Исходящий трафик распределяется в зависимости от загруженности каждой сетевой карты (определяется скоростью загрузки). Не требует дополнительной настройки на коммутаторе. Входящий трафик приходит на текущую сетевую карту. Если она выходит из строя, то другая сетевая карта берет себе MAC-адрес вышедшей из строя карты. • **Adaptive load balancing.** Включает в себя предыдущую политику плюс осуществляет балансировку входящего трафика. Не требует дополнительной настройки на коммутаторе. Балансировка входящего трафика достигается путем ARP-переговоров.

Наименование	Описание
	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)	Задает время задержки в миллисекундах, перед тем как поднять канал при обнаружении его восстановления. Этот параметр возможен только при MII-мониторинге (miimon). Значение параметра должно быть кратным значениям miimon. Если оно не кратно, то округлится до ближайшего кратного значения. Значение по умолчанию 0.
LACP rate	Определяет, с каким интервалом будут передаваться партнером LACPDU-пакеты в режиме 802.3ad. Возможные значения: • **Slow** — запрос партнера на передачу LACPDU-пакетов каждые 30 секунд. • **Fast** — запрос партнера на передачу LACPDU-пакетов каждую 1 секунду.
Failover MAC	Определяет, как будут прописываться MAC-адреса на объединенных интерфейсах в режиме active-backup при переключении интерфейсов. Обычным поведением является одинаковый MAC-адрес на всех интерфейсах. Возможные значения: • **Отключено** — устанавливает одинаковый MAC-адрес на всех интерфейсах во время переключения. • **Active** — MAC-адрес на бонд-интерфейсе будет всегда таким же, как на текущем активном интерфейсе. MAC-адреса на резервных интерфейсах

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

Настройка шлюзов

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

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

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

При наличии двух или более шлюзов возможны 2 варианта работы:

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

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

Маршруты

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

Для добавления маршрута необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Задать название и описание данного маршрута.	В разделе **Сеть** выберите в меню **Маршруты**, нажмите кнопку **Добавить**. Укажите имя для данного маршрута. Опционально можно задать описание маршрута.

Наименование	Описание
Шаг 2. Указать адрес назначения.	Задайте подсеть, куда будет указывать маршрут, например, 172.16.20.0/24 или 172.16.20.5/32.
Шаг 3. Указать шлюз.	Задайте IP-адрес шлюза, через который указанная подсеть будет доступна. Этот IP-адрес должен быть доступен с сервера UGMC.
Шаг 4. Указать интерфейс.	Выберите интерфейс, через который будет добавлен маршрут. Если оставить значение **Автоматически**, то UGMC сам определит интерфейс, исходя из настроек IP-адресации сетевых интерфейсов.
Шаг 5. Указать метрику.	Задайте метрику маршрута. Чем меньше метрика, тем приоритетней маршрут, если маршрутов несколько в данную сеть несколько.

ЖУРНАЛЫ И ОТЧЁТЫ

Журнал событий

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

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

В UserGate Management Center также представлен режим расширенного поиска для формирования сложных фильтров с использованием специального языка запросов, синтаксис которого рассмотрен далее в разделе Режим расширенного поиска.

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

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

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

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

Экспорт журналов

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

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

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

> **Примечание**
>
> **Настройки экспорта журналов не являются кластерными. Если UGMC работает в кластерной конфигурации, правила экспорта журналов создаются отдельно на каждом узле.**

При создании конфигурации требуется указать следующие параметры:

Наименование	Описание
Название правила	Название правила экспорта журналов.
Описание	Опциональное поле для описания правила.
Журналы для экспорта	Выбор файлов журналов, которые необходимо экспортировать: • Журнал событий. Для каждого из журналов возможно указать синтаксис выгрузки: • CEF — Common Event Format (ArcSight).

Наименование	Описание
	• JSON — JSON format. • @CEE: JSON — CEE Log Syntax (CLS) Encoding JSON. Обратитесь к документации на используемую у вас систему SIEM для выбора необходимого формата выгрузки журналов. Подробное описание форматов журналов читайте в приложении Описание форматов журналов.
Тип сервера	SSH (SFTP), FTP, Syslog.
Адрес сервера	IP-адрес или доменное имя сервера.
Транспорт	Только для типа серверов Syslog — TCP или UDP.
Порт	Порт сервера, на который следует отправлять данные.
Протокол	Только для типа серверов Syslog — RFC5424 или BSD syslog RFC 3164. Выберите протокол, совместимый с используемой у вас системой SIEM.
Критичность	Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас систему SIEM. Возможны следующие значения: • **Тревога**: состояние, требующее незамедлительного вмешательства. • **Критическая**: состояние, требующее незамедлительного вмешательства либо предупреждающее о сбое в системе. • **Ошибки**: в системе возникли ошибки. • **Предупреждения**: предупреждения о возможном возникновении ошибок, если не будут предприняты никакие действия. • **Уведомительная**: события, которые относятся к необычному поведению системы, но не являются ошибками. • **Информативная**: информационные сообщения.
Facility	Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас систему SIEM. Возможны следующие значения: • **Сообщения пользовательские**. • **Системный сервис**. • **Безопасность/авторизация**.

Наименование	Описание
	• **Аудит**. • **Тревога**. • **Local 0**. • **Local 1**. • **Local 2**. • **Local 3**. • **Local 4**. • **Local 5**. • **Local 6**. • **Local 7**.
Имя хоста	Только для типа серверов Syslog. Уникальное имя хоста, идентифицирующее сервер, отправляющий данные на сервер syslog, в формате Fully Qualified Domain Name (FQDN).
App-Name	Только для типа серверов Syslog. Уникальное имя приложения, которое отправляет данные на сервер syslog.
Логин	Имя учетной записи для подключения к удаленному серверу. Не применяется к методу отправки Syslog.
Пароль	Пароль учетной записи для подключения к удаленному серверу. Не применяется к методу отправки Syslog.
Путь на сервере	Каталог на сервере для копирования файлов журналов. Не применяется к методу отправки Syslog. В кластерной конфигурации UGMC при экспорте журналов с разных узлов кластера необходимо указывать разные каталоги на сервере для каждого узла UGMC, поскольку имена файлов журналов на каждом узле идентичны.
Расписание	Выбор расписания для отправки логов. Не применяется к методу отправки Syslog. Возможны варианты: • Ежедневно. • Еженедельно. • Ежемесячно • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть

Наименование	Описание
	полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".
Управление журналами	Управление временными файлами журналов, подготавливаемых для отправки на удаленные серверы ssh и ftp. При отправке журналов на сервера ssh и ftp UserGate сохраняет данные для отправки во временных файлах в кодировке UTF-8. Журналы за предыдущие дни (по количеству дней ротации) хранятся в виде архивов, журнал за текущий день не архивирован. По указанному расписанию все созданные для отправки файлы копируются на удаленный сервер, при этом файлы не очищаются и не удаляются. Данная настройка позволяет указать период ротации временных файлов (в днях) или удалить любой из временных файлов вручную. Ротация файлов происходит один раз в сутки.

Примечание

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

Режим расширенного поиска

Помимо простого поиска, для которого используется графический интерфейс, в LogAn представлена возможность расширенного поиска с формированием более сложных фильтров поиска и использованием специального языка

запросов. Для формирования запросов используются названия полей, значения полей, ключевые слова и операторы. Значения полей могут быть введены с использованием одинарных или двойных кавычек, или без них, если значения не содержат пробелов. Для группировки нескольких условий можно использовать круглые скобки.

Ключевые слова отделяются пробелами и могут быть следующими:

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

Операторы определяют условия фильтра и могут быть следующими:

Наименование	Описание
=	Равно. Требует полного совпадения значения поля указанному значению, например, ip=172.16.31.1 будут отображены все записи журнала, в котором поле IP будет точно соответствовать значению 172.16.31.1.
!=	Не равно. Значение указанного поля не должно совпадать с указанным значением, например, ip!=172.16.31 будут отображены все записи журнала, в котором поле IP не будет равно значению 172.16.31.1.
<=	Меньше либо равно. Значение поля должно быть меньше либо равны указанному в запросе значению. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, date <= '2019-03-28T20:59:59' AND statusCode=303.
>=	Больше либо равно. Значение поля должно быть больше либо равны указанному в запросе значению. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, date >= "2019-03-13T21:00:00" AND statusCode=200.

Наименование	Описание
<	Меньше. Значение поля должно быть меньше указанного в запросе значения. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, date < '2019-03-28T20:59:59' AND statusCode=404.
>	Больше. Значение поля должно быть больше указанного в запросе значения. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, (statusCode>200 AND statusCode<300) OR (statusCode=404).
IN	Позволяет указать несколько значений поля в запросе. Список значений необходимо указывать в круглых скобках, например, category IN (botnets, compromised, 'illegal software', 'phishing and fraud','reputation high risk','unknown category').
NOT IN	Позволяет указать несколько значений поля в запросе; будут отображены записи, не содержащие указанные значения. Список значений необходимо указывать в круглых скобках, например, category NOT IN (botnets, compromised, 'illegal software', 'phishing and fraud','reputation high risk','unknown category').
~	Содержит. Позволяет указать подстроку, которая должна находиться в указанном поле, например, browser ~ "Mozilla/5.0". Данный оператор может быть применен только к полям, в которых хранятся строковые данные.
!~	Не содержит. Позволяет указать подстроку, которая не должна присутствовать в указанном поле, например, browser !~ "Mozilla/5.0". Данный оператор может быть применен только к полям, в которых хранятся строковые данные.
MATCH	При использовании оператора MATCH подстрока, которая должна присутствовать в указанном поле, задаётся в формате JSON и с использованием одинарных кавычек, например, details MATCH '\"module\":\"threats\"'. Синтаксис запросов с использованием данного оператора соответствует стандарту RE2. Подробнее о синтаксисе Google/RE2: https://github.com/google/re2/wiki/Syntax.

Наименование	Описание
NOT MATCH	При использовании оператора NOT MATCH подстрока, которая не должна присутствовать в указанном поле, задаётся в формате JSON и с использованием одинарных кавычек, например, details NOT MATCH '\"module\":\"threats\"'. Синтаксис запросов с использованием данного оператора соответствует стандарту RE2. Подробнее о синтаксисе Google/RE2: https://github.com/google/re2/wiki/Syntax.

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

ДИАГНОСТИКА И МОНИТОРИНГ

Маршруты

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

- **Подключенные к интерфейсам** — маршруты к сетям, которые подключены непосредственно к интерфейсам UserGate. Данные маршруты будут помечены символом **C** в списке маршрутов.
- **Заданные статически** — маршруты, заданные статически в разделе **Сеть → Маршруты**. Данные маршруты будут помечены символом **S** в списке маршрутов.
- **OSPF** — маршруты, полученные по протоколу OSPF. Данные маршруты будут помечены символом **O** в списке маршрутов.
- **BGP** — маршруты, полученные по протоколу BGP. Данные маршруты будут помечены символом **B** в списке маршрутов.

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

Ping

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

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

Traceroute

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

Наименование	Описание
Traceroute host	Хост, который необходимо проверить.
Использовать ICMP	Использовать протокол ICMP для выполнения команды traceroute. Если не указано, то используется протокол UDP.
Интерфейс	С какого сетевого интерфейса выполнять команду.
Не резолвить имена	Оперировать IP-адресами, не преобразовывая их в доменные имена.

Запрос DNS

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

Наименование	Описание
DNS-запрос (хост)	DNS имя для проверки.
IP источника запроса	Один из IP-адресов, назначенных UserGate.
DNS сервер	DNS сервер, куда посылать запрос.
Порт	UDP порт, используемый для запроса.
Тип DNS-запроса	Тип запроса.

ОПОВЕЩЕНИЯ

SNMP

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

Для настройки мониторинга с помощью SNMP необходимо:

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

2. Создать правило SNMP

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

Наименование	Описание
Название правила	Название правила.
IP-адрес сервера для трапов	IP-адрес сервера для трапов и порт, на котором сервер слушает оповещения. Обычно это порт UDP 162. Данная настройка необходима только в случае, если необходимо отправлять трапы на сервер оповещений.
Комьюнити	SNMP community - строка для идентификации сервера UserGate и сервера управления SNMP для версии SNMP v2c. Используйте только латинские буквы и цифры.
Контекст	Необязательный параметр, определяющий SNMP context. Можно использовать только латинские буквы и цифры. На некоторых устройствах может быть несколько копий полного поддерева MIB. Например, на устройстве может быть создано несколько виртуальных маршрутизаторов. Каждый такой виртуальный маршрутизатор будет иметь полное поддерево MIB. В этом случае каждый виртуальный маршрутизатор может быть указан как контекст на сервере SNMP. Контекст определяется по имени. Когда клиент отправляет запрос, он может указать имя контекста. Если имя контекста не указано, будет запрошен контекст по умолчанию.
Версия	Указывает версию протокола SNMP, которая будет использоваться в данном правиле. Возможны варианты SNMP v2c и SNMP v3.
Разрешить SNMP-запросы	При включении разрешает получение и обработку SNMP-запросов от SNMP-менеджера.
Разрешить SNMP-трапы	При включении разрешает отправку SNMP-трапов на сервер, настроенный для приема оповещений.
Название профиля безопасности SNMP	Только для SNMP v3. Подробнее — в разделе Профили безопасности SNMP.
События	Выбор типов параметров, доступных для мониторинга по правилу.

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

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

UserGate выделен уникальный идентификатор **SNMP PEN** (Private Enterprise Number) **45741**.

Актуальные mib-файлы UserGate с параметрами мониторинга можно скачать из консоли администратора устройства. Для этого необходимо перейти на вкладку **Диагностика и мониторинг**, далее в разделе **Оповещения → SNMP** нажать **Скачать MIB**.

Для скачивания доступны следующие MIB-файлы:

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

UTM-TRAPS-MIB

Наименование	Описание
trapCoreCrush	Сбой ядра.
trapStatDown	Сервис статистики (UserGate Log Analyzer) недоступен.
trapCoreBootstrapEnd	Загрузка сервера завершена успешно.
trapDefaultGatewayChanged	Изменение шлюза по умолчанию.
trapHighSessionsCounter	Таблица сессий заполнена на 90%.

Наименование	Описание
trapHighUsersCounter	Количество активных пользователей достигло 90% от порога лицензии.
trapDataPartitionFSStatus	Стутус файловой системы. Состояние файловой системы изменилось на "not_clean".
trapStatusChanged	Изменение статуса узла отказоустойчивого кластера.
trapMemberUp	Статус узла отказоустойчивого кластера изменился на «Подключен».
trapMemberDown	Узел отказоустойчивого кластера отключен.
trapAttackDetected	Обнаружение атаки системой СОВ.
trapChecksumFailed	Нарушение целостности бинарных файлов.
trapHighCPUUsage	Высокая загрузка центрального процессора.
trapLowMemory	Высокая загрузка памяти.
trapLowLogdiskSpace	Недостаточно места на диске для хранения журналов.
trapRaidStatus	Изменение статуса RAID.
trapPowerSupply	Первый источник питания отключен.
trapCableStatus	Кабель был подключен или отключен от интерфейса.
trapHighDiskIOUtilization	Высокая загрузка диска. Оповещение отправляется при загруженности >=95% за 5 минут хотя бы на одном из дисковых устройств.
trapTrafficDrop	Срабатывание запрещающего правила межсетевого экрана.
trapLDAPServerDown	Сервер LDAP недоступен.
trapCriticalTemperature	Критическая температура на одном из сенсоров. Оповещение отправляется при пересечении одного из пределов рабочей температуры (нижнего или верхнего). Нижний предел рабочей температуры обычно равен 0°C (для устройств серии X -40°C), верхний предел равен 85°C.

UTM-TRAPS-BINDINGS-MIB

Наименование	Тип данных	Описание
utmSessions	integer	Текущее количество активных сессий.
utmSessionsMax	integer	Максимальное количество активных сессий.
utmUsers	integer	Количество активных пользователей на данный момент.
utmUsersMax	integer	Максимальное количество активных пользователей.
utmDataPartionFSStatus	integer	Состояние файловой системы. • **0** — clean. • **1** — not clean.
utmHAStatus	integer	Текущий статус узла кластера отказоустойчивости: • **0** — master-узел. • **1** — slave-узел. • **3** — fault.
utmHAStatusReason	integer	Причина изменения статуса узла отказоустойчивого кластера: • **1** — связь с узлом потеряна. • **2** — HTTP прокси-сервер недоступен. • **3** — ни один из шлюзов недоступен. • **4** — DNS-сервер недоступен. • **5** — узел UserGate Management Center недоступен.
utmCPUUsage	integer	Загруженность центрального процессора (%).

Наименование	Тип данных	Описание
utmMemory	integer	Использование оперативной памяти (%).
utmLogdiskSpace	integer	Пространство на диске, используемое под журналы (%).
utmAdaptecRaidStatus	integer	Текущий статус RAID (Redundant Array of Independent Disks), построенного на контроллере Adaptec: • **no_raid**. • **0** — optimal — массив в оптимальном состоянии. • **1** — degraded — полный или частичный выход из строя одного из дисков. • **2** — rebuild — восстановление массива.
utmBroadcomRaidStatus	integer	Текущий статус RAID (Redundant Array of Independent Disks), построенного на контроллере Broadcom: • **no_raid** • **0** — optimal — массив в оптимальном состоянии. • **1** — degraded — полный или частичный выход из строя одного из дисков. Переход в данный статус произойдёт при выходе из строя 2-х дисков. • **2** — partialDegraded — полный или частичный выход из

Наименование	Тип данных	Описание
		строя одного из дисков. • **3** — failed — не работает из-за наличия ошибки. • **4** — offline — диск не доступен для RAID-контроллера.
utmPowerSupply	integer	Количество источников питания: • **1** — один блок питания. • **2** — два блока питания.
utmPowerSupplyStatus	integer	Состояние источника питания: • **no_power_supplies**. • **0** — off. • **1** — on.
utmCSCIfName	string	Название интерфейса.
utmCSCStatus	integer	Статус сетевого адаптера: • **1** — кабель подключен. • **2** — кабель не подключен.
utmDiskIOUtilization	integer	Текущая утилизация диска (%).
utmLDAPServerName	string	Название LDAP-сервера.
utmLDAPServerAddress	string	IP-адрес LDAP-сервера.
utmThermSensor	string	Название температурного сенсора.
utmThermValue	integer	Значение температуры, измеренное сенсором.

UTM-MIB

Наименование	Тип данных	Описание
vcpuCount	integer	Количество виртуальных процессоров в системе.
vcpuUsage	integer	Загруженность виртуальных процессоров системы; отображается в %.
usersCounter	integer	Количество активных пользователей на текущий момент времени. (*)
sessionsCounter	integer	Количество активных сессий на текущий момент времени. (*)
tcpsessionsCounter	integer	Количество активных TCP сессий на текущий момент времени. (*)
udpsessionsCounter	integer	Количество активных UPD сессий на текущий момент времени. (*)
icmpsessionsCounter	integer	Количество активных ICMP сессий на текущий момент времени. (*)
sessionsRate10	integer	Количество новых сессий в секунду. Среднее значение за последние 10 секунд. (*)
sessionsRate60	integer	Количество новых сессий в секунду. Среднее значение за последние 60 секунд. (*)
sessionsRate300	integer	Количество новых сессий в секунду. Среднее значение за последние 300 секунд. (*)
tcpsessionsRate10	integer	Количество новых TCP сессий в секунду. Среднее значение за последние 10 секунд. (*)
tcpsessionsRate60	integer	Количество новых TCP сессий в секунду. Среднее значение за последние 60 секунд. (*)

Наименование	Тип данных	Описание
tcpsessionsRate300	integer	Количество новых TCP сессий в секунду. Среднее значение за последние 300 секунд. (*)
udpsessionsRate10	integer	Количество новых UPD сессий в секунду. Среднее значение за последние 10 секунд. (*)
udpsessionsRate60	integer	Количество новых UPD сессий в секунду. Среднее значение за последние 60 секунд. (*)
udpsessionsRate300	integer	Количество новых UPD сессий в секунду. Среднее значение за последние 300 секунд. (*)
icmpsessionsRate10	integer	Количество новых ICMP сессий в секунду. Среднее значение за последние 10 секунд. (*)
icmpsessionsRate60	integer	Количество новых ICMP сессий в секунду. Среднее значение за последние 60 секунд. (*)
icmpsessionsRate300	integer	Количество новых ICMP сессий в секунду. Среднее значение за последние 300 секунд. (*)
dnsRequestCounter	integer	Общее количество DNS запросов. (*)
dnsBlockedRequestCounter	integer	Количество заблокированных DNS запросов. (*)
dnsRequestRate	integer	Количество DNS запросов в секунду. (*)
httpRequestCounter	integer	Общее количество HTTP запросов. (*)

Наименование	Тип данных	Описание
httpBlockedRequestCounter	integer	Количество заблокированных HTTP запросов. (*)
httpRequestRate	integer	Количество HTTP запросов в секунду. (*)
dataPartitionFSStatus	string	Состояние файловой системы.
haStatus	integer	Текущее состояние узла кластера.
cpuLoad	integer	Загруженность центрального процессора системы; отображается в %.
memoryUsed	integer	Использование оперативной памяти; отображается в %.
logDiskSpace	integer	Пространство на диске, используемое под журналы; отображается в %.
powerSupply1Status	string	Состояние первого источника питания: • **no_power_supplies**. • **on**. • **off**.
powerSupply2Status	string	Состояние второго источника питания: • **no_power_supplies**. • **on**. • **off**.
raidType	string	Тип RAID массива.
raidStatus	string	Текущий статус RAID (Redundant Array of Independent Disks): • **no_raid**.

Наименование	Тип данных	Описание
		• **0** — optimal — массив в оптимальном состоянии. • **1** — degraded — полный или частичный выход из строя одного из дисков. • **2** — rebuild — восстановление массива.
diskIOUtilization	integer	Текущая утилизация диска (%).
diskIOUtilization60	integer	Утилизация диска (%). Среднее значение за последние 60 секунд.
diskIOUtilization300	integer	Утилизация диска (%). Среднее значение за последние 300 секунд.

Примечание

Метрики, отмеченные в описании символом (*) не актуальны для *UGMC* и *LogAn*.

Значения метрик для этих устройств будут всегда равны нулю.

UTM-INTERFACES-MIB

Наименование	Тип данных	Описание
ifNumber	integer	Количество сетевых интерфейсов.
ifIndex	integer	Значение уникально для каждого интерфейса и может принимать значения от 1 до ifNumber.
ifDescr	string	Описание интерфейса.
ifType	integer	Тип интерфейса, определённый в соответствии с протоколом

Наименование	Тип данных	Описание
		физического/канального уровней: • **1** — other — неизвестный тип. • **2** — regular1822 — определён в BBN Report 1822. • **3** — hdh1822 — определён в BBN Report 1822. • **4** — ddn-x25 — определён в BBN Report 1822. • **5** — определён в стандарте канального уровня сетевой модели OSI X.25. • **6** — ethernet-csmacd — сетевой интерфейс типа Ethernet, независимо от скорости (определён в RFC 3635). • **7** — iso88023-csmacd — определён в IEEE 802.3. • **8** — iso88024-tokenBus — определён в стандарте IEEE 8802.4. • **9** — iso88025-tokenRing — сетевой интерфейс использует подключение Token Ring; определяется в стандарте IEEE 802.5. • **10** — iso88026-man — определён в стандарте ISO 88026 "MAN". • **11** — starLan — определён в стандарте IEEE 802.3e. • **12** — proteon-10Mbit — Proteon 10 Mbit • **13** — proteon-80Mbit — Proteon 80 Mbit.

Наименование	Тип данных	Описание
		• **14** — hyperchannel — высокоскоростной канал, используемы в сети ISDN. • **15** — fddi — сетевой интерфейс использует подключение FDDI (Fiber Distributed Data Interface). FDDI — это набор стандартов передачи данных по оптоволоконным линиям в локальной сети. • **16** — lapb — протокол канального уровня, используемым для передачи пакетов стандарта X.25. • **17** — sdlc — протокол канального уровня для системной сетевой архитектуры IBM. • **18** — ds1 — способен обрабатывать 24 одновременных соединения на общей скорости 1,544 Мбит/с; также называется T1 • **19** — e1 — европейский аналог T1. • **20** — basicISDN — для связи аппаратуры абонента и ISDN-станции. • **21** — primaryISDN — используется для подключения к широкополосным магистралям, связывающим местные и центральные АТС или сетевые коммутаторы. • **22** — propPointToPointSeri

Наименование	Тип данных	Описание
		al — определён в стандарте RFC1213. • **23** — ppp — сетевой интерфейс использует подключение PPP (Point-To-Point Protocol). • **24** — softwareLoopback — сетевой интерфейс является петлевым адаптером. Такие интерфейсы часто используются для тестирования; они не отправляют трафик в сеть. • **25** — eon — ConnectionLess Network Protocol (CLNP) over Internet Protocol (IP); определён в ISO/IEC 8473-1. • **26** — ethernet-3Mbit — сетевой интерфейс использует подключение Ethernet со скоростью 3 Мбит/с. Эта версия Ethernet определяется в стандарте IETF RFC 895. • **27** — nsip — XNS over IP — предназначен для использования в разнообразных средах передачи данных. • **28** — slip — сетевой интерфейс использует подключение SLIP (Serial Line Internet Protocol). SLIP определяется в стандарте IETF RFC 1055. • **29** — ultra — ULTRA Technologies.

Наименование	Тип данных	Описание
		• **30** — ds3 — высокоскоростной интерфейс передачи данных, сформированный мультиплексированием сигналов DS1 и DS2; также называется T3. • **31** — sip — сетевой интерфейс использует подключение SLIP (Serial Line Internet Protocol). SLIP определяется в стандарте IETF RFC 1055. • **32** — frame-relay — обеспечивает возможность передачи данных с коммутацией пакетов через интерфейс между устройствами пользователя и оборудованием сети.
ifMtu	integer	Максимальный размер пакета сетевого уровня, который можно послать через этот интерфейс.
ifSpeed	gauge32	Пропускная способность интерфейса в битах в секунду.
ifPhysAddress	string	Физический адрес интерфейса (MAC-адрес).
ifAdminStatus	integer	Состояние интерфейса, назначаемое администратором: • **1** — up — готов для передачи пакетов. • **2** — down — не работает. • **3** — testing — в режиме тестирования;

Наименование	Тип данных	Описание
		рабочие пакеты не могут быть переданы.
ifOperStatus	integer	Текущий статус работы интерфейса: • **1** — up — интерфейс готов для передачи пакетов. • **2** — down — интерфейс не может передавать пакеты данных. • **3** — testing — выполняется тестирование сетевого интерфейса; рабочие пакеты не могут быть переданы. • **4** — unknown — интерфейс находится в неизвестном состоянии. • **5** — dormant — сетевой интерфейс не может передавать пакеты данных, он ожидает внешнее событие. • **6** — notPresente — сетевой интерфейс не может передавать пакеты данных из-за отсутствующего компонента, обычно аппаратного. • **7** — lowerLayerDown — сетевой интерфейс не может передавать пакеты данных, потому что он работает поверх одного или нескольких других интерфейсов, и не менее одного из этих интерфейсов "нижнего уровня" не работает.

Наименование	Тип данных	Описание
ifLastChange	timeticks	Значение SysUpTime, когда интерфейс оказался в данном состоянии.
ifInOctets	counter32	Количество байтов, принятое данным интерфейсом, включая служебные.
ifInUcastPkts	counter32	Количество доставленных пакетов одноадресной рассылки.
fInNUcastPkts	counter32	Количество доставленных многоадресных и широковещательных пакетов.
ifInDiscards	counter32	Количество входящих пакетов, которые были отброшены, даже если не было обнаружено ошибок, препятствующих их доставке. Одна из возможных причин отбрасывания: освобождение буферного пространства.
ifInErrors	counter32	Количество входящих пакетов, которые содержат ошибки, препятствующие их доставке.
ifInUnknownProtos	counter32	Количество пакетов, которые были получены через этот интерфейс и отброшены из-за использования неизвестного или неподдерживаемого протокола.
ifOutOctets	counter32	Количество байтов, переданное данным интерфейсом, включая служебные.
ifOutUcastPkts	counter32	Количество отправленных пакетов одноадресной

Наименование	Тип данных	Описание
		рассылки, включая пакеты, которые были отброшены или не отправлены.
ifOutNUcastPkts	counter32	Количество отправленных многоадресных и широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены.
ifOutDiscards	counter32	Количество исходящих пакетов, которые были отброшены, даже если не было обнаружено ошибок, препятствующих их передачи. Одна из возможных причин отбрасывания: освобождение буферного пространства.
ifOutErrors	counter32	Количество исходящих пакетов, передача которых невозможна вследствие наличия ошибок.
ifOutQLen	gauge32	Длина выходной очереди (в пакетах).
ifInMulticastPkts	counter32	Количество доставленных пакетов многоадресной рассылки.
ifInBroadcastPkts	counter32	Количество доставленных широковещательных пакетов.
ifOutMulticastPkts	counter32	Количество отправленных пакетов многоадресной рассылки, включая пакеты, которые были отброшены или не отправлены.
ifOutBroadcastPkts	counter32	Количество отправленных широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены.

Наименование	Тип данных	Описание
ifHCInOctets	counter64	Смысл одинаков со смыслом объекта **ifInOctets** — количество байтов, принятое данным интерфейсом, включая служебные; используется счётчик большей ёмкости.
ifHCInUcastPkts	counter64	Смысл одинаков со смыслом объекта **ifInUcastPkts** — количество доставленных пакетов одноадресной рассылки; используется счётчик большей ёмкости.
ifHCInMulticastPkts	counter64	Смысл одинаков со смыслом объекта **ifInMulticastPkts** — количество доставленных пакетов многоадресной рассылки; используется счётчик большей ёмкости.
ifHCInBroadcastPkts	counter64	Смысл одинаков со смыслом объекта **ifInBroadcastPkts** — количество доставленных широковещательных пакетов; используется счётчик большей ёмкости.
ifHCOutOctets	counter64	Смысл одинаков со смыслом объекта **ifOutOctets** — количество байтов, переданное данным интерфейсом, включая служебные; используется счётчик большей ёмкости.
ifHCOutUcastPkts	counter64	Смысл одинаков со смыслом объекта **ifOutUcastPkts** — количество отправленных пакетов одноадресной рассылки, включая пакеты, которые были отброшены или не отправлены; используется счётчик большей ёмкости.
ifHCOutMulticastPkts	counter64	Смысл одинаков со смыслом объекта **ifOutMulticastPkts**

Наименование	Тип данных	Описание
		— количество отправленных пакетов многоадресной рассылки, включая пакеты, которые были отброшены или не отправлены; используется счётчик большей ёмкости.
ifHCOutBroadcastPkts	counter64	Смысл одинаков со смыслом объекта **ifOutBroadcastPkts** — количество отправленных широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены; используется счётчик большей ёмкости.
ifLinkUpDownTrapEnable	integer	Указывает, должен ли создаваться трап при изменении статуса соединения: • **1** — enabled — включено. • **2** — disabled — отключено.
ifHighSpeed	gauge32	Оценка текущей полосы пропускания интерфейса; указывается в бит/с, кбит/с, Мбит/с, Гбит/с.
ifPromiscuousMode	integer	"Неразборчивый" режим. Может принимать значения: • **1** — true — станция принимает все пакеты/кадры независимо от того, кому они адресованы. • **2** — false — интерфейс принимает только пакеты/кадры, адресованные этой станции. Значение объекта не влияет на приём широковещательных и

Наименование	Тип данных	Описание
		многоадресных пакетов/ кадров.
ifAlias	string	Название интерфейса, заданное администратором.
ifCounterDiscontinuityTime	timeticks	Значение SysUpTime, когда произошло событие, ставшее причиной сбоя работы одного или более счётчиков интерфейса.

UTM-TEMPERATURE-MIB

Наименование	Тип данных	Описание
termNumber	integer	Количество температурных сенсоров на данной платформе.
thermLowerThreshold	integer	Нижний предел рабочей температуры.
thermUpperThreshold	integer	Верхний предел рабочей температуры.
thermTable	sequence	Таблица температурных сенсоров с показаниями (thermEntry).
thermEntry	sequence	Информация о конкретном сенсоре: • thermName (string) — название сенсора. • thermValue (integer) — показание сенсора. • thermUnit (string) — единица измерения показаний сенсора.

Примечание

Данные температурных сенсоров будут отображаться только для поддерживаемых аппаратных платформ. В настоящий момент поддерживаются устройства UserGate C150, C151, FG, X10. Для неподдерживаемых платформ или виртуальных решений таблица сенсоров будет пустой, а значения количества сенсоров и пределы рабочих температур будут равны нулю.

Примечание

Если с сенсора не удалось снять показание температуры, он не будет передан в таблице, при этом параметр thermNumber подсчитывает общее количество температурных сенсоров, даже с учётом неработающих. В таком случае количество сенсоров в таблице и значение thermNumber могут не совпадать.

Параметры SNMP

Данный раздел используется для задания настроек по выдаче информации SNMP-агентом по протоколу SNMP. Параметры SNMP задаются для каждого узла индивидуально.

Наименование	Описание
SNMP имя системы	Название системы, используемое подсистемой управления SNMP.
SNMP локация системы	Информация о физическом расположении SNMP-агента.
SNMP описание системы	Описание системы.
Engine ID	Каждое устройство UserGate имеет уникальный идентификатор SNMPv3 Engine ID. По умолчанию Engine ID генерируется на основании имени узла UserGate. При редактировании Engine ID необходимо указать длину, тип и значение идентификатора. Длина может быть определена как **фиксированная** (не более 8 байт) или **динамическая** (не более 27 байт). Фиксированная длина идентификатора применима только для типа **text**. Engine ID может быть сформирован в формате: • IPv4 (ip4). • IPv6 (ipv6).

Наименование	Описание
	• MAC-адрес (mac). • Текст (text). • Октеты (jctets).

Правила оповещений

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

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

При добавлении правила необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает данное правило.
Название	Название правила.
Описание	Описание правила.
Профиль оповещения	Созданный ранее профиль оповещения. Для профилей SMPP появится закладка для указания адресатов в виде телефонных номеров, для SMTP появится закладка для указания адресатов в виде email-адресов.
От	От кого будет приходить оповещение.
Тема	Тема оповещения.

Наименование	Описание
Таймаут перед повторной отправкой, секунд	Укажите таймаут, в течение которого сервер не будет отправлять сообщение при повторном срабатывании данного правила. Данная настройка позволяет предотвратить шторм сообщений при частом срабатывании правила оповещения.
События	Укажите события, для которых необходимо получать оповещения.
Телефоны	Для SMPP-профиля. Укажите группы номеров телефонов, куда отправлять SMS-оповещения.
Emails	Для SMTP-профиля. Укажите группы адресов email, на которые будут отправляться почтовые оповещения.

Профили безопасности SNMP

В данном разделе производиться настройка профилей безопасности для аутентификации SNMPv3-менеджера.

> **Примечание**
> **Настройки аутентификации для SNMP v3 (имя пользователя, пароль, тип и алгоритм аутентификации, алгоритм и пароль шифрования) на SNMP-менеджере должны совпадать с настройками SNMP в UserGate**

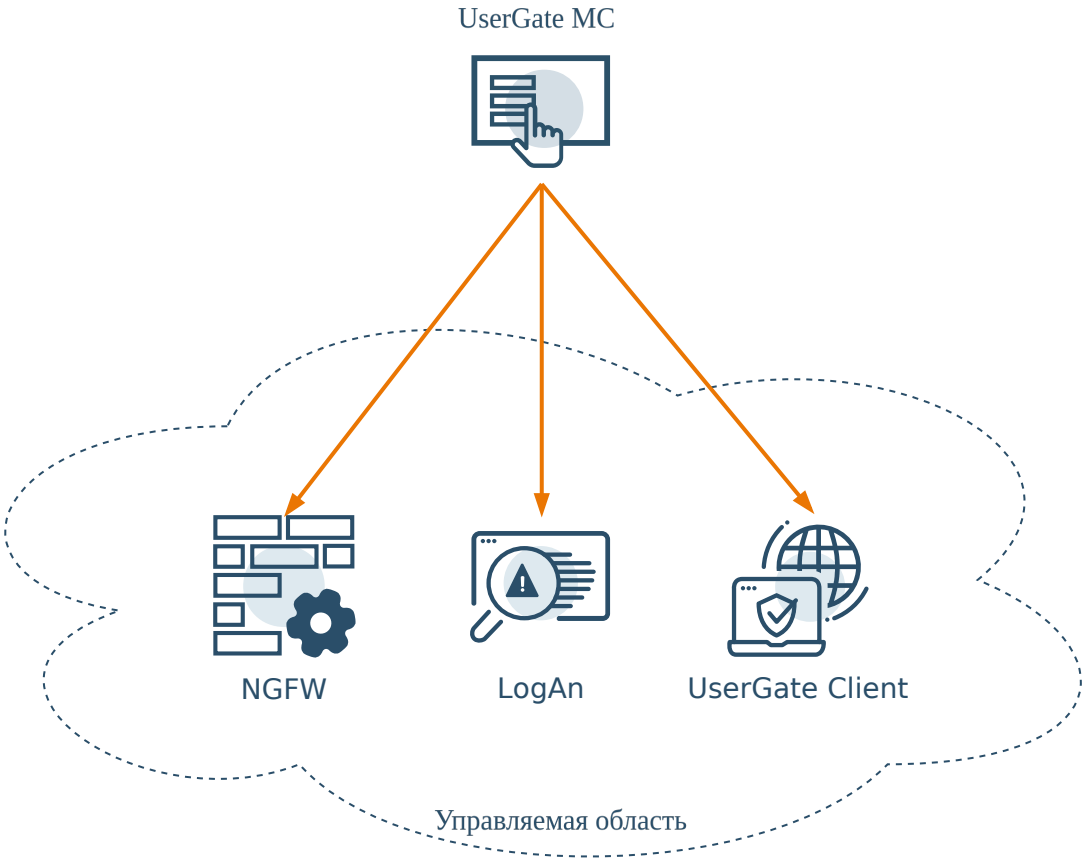
Наименование	Описание
Название	Название профиля безопасности SNMP
Описание	Описание профиля безопасности SNMP
Пользователь	Имя пользователя для аутентификации SNMP-менеджера.
Тип аутентификации	Выбор режима аутентификации SNMP-менеджера. Возможны варианты: • Без аутентификации, без шифрования (noAuthNoPriv). • С аутентификацией, без шифрования (authNoPriv). • С аутентификацией, с шифрованием (authPriv). Наиболее безопасным считается режим работы authPriv.

Наименование	Описание
Алгоритм аутентификации	Алгоритм, используемый для аутентификации. Возможно использовать: • SHA1; • MD5; • SHA224; • SHA256; • SHA384; • SHA512.
Пароль аутентификации	Пароль, используемый для аутентификации.
Алгоритм шифрования	Алгоритм, используемый для шифрования. Возможно использовать DES и AES.
Пароль шифрования	Пароль, используемый для шифрования.

УПРАВЛЕНИЕ ОБЛАСТЯМИ

Управление областями (Описание)

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



В качестве устройств, управляемых с помощью UGMC, могут быть:

- Межсетевые экраны UserGate (подробнее — в разделе Управление межсетевыми экранами UserGate).
- Устройства UserGate LogAn (подробнее — в разделе Управление устройствами LogAn).
- Конечные устройства с установленным ПО UserGate Client (подробнее — в разделе Управление конечными устройствами UserGate Client).

Создание управляемых областей

Управляемые области создаются администратором UGMC. Для создания управляемой области необходимо выполнить следующие действия:

1. Создать область.

2. Создать профиль администратора области.

3. Создать администратора области.

Создание области

В веб-консоли перейти в раздел **Управляемые области → Области**, нажать кнопку **Добавить**, заполнить необходимые поля:

Наменование	Описание
Область по умолчанию	Если установлен этот флажок, 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.

Создание профиля администратора области

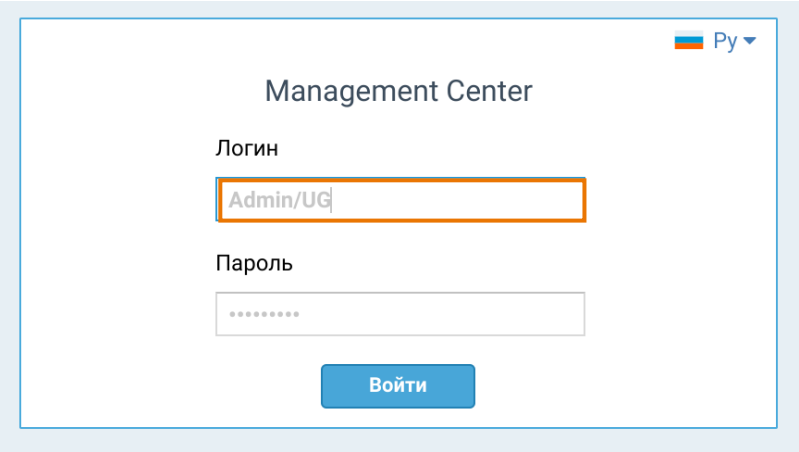
В разделе веб-консоли **Администраторы → Профили администраторов** нажать кнопку **Добавить** и создать профиль администратора с типом **Администратор области**. В качестве управляемой области указать созданную область.

Создание администратора области

В разделе веб-консоли **Администраторы → Администраторы** нажать кнопку **Добавить** и создать администратора с созданным ранее профилем. Подробнее о создании администраторов смотрите в главе данного руководства Администраторы области.

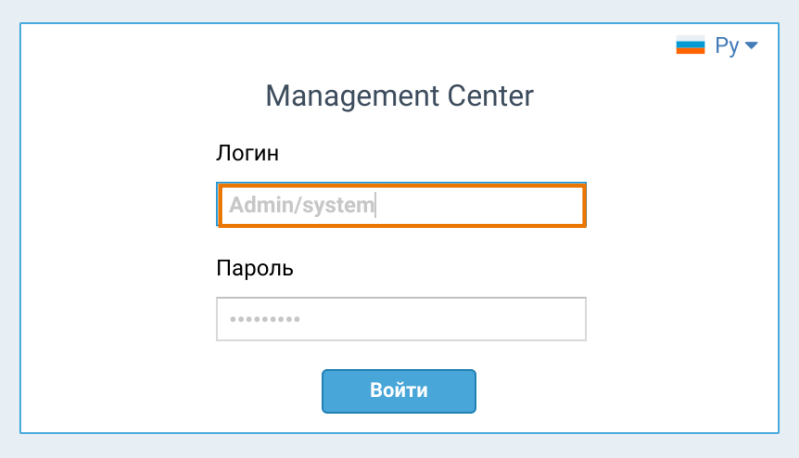
После создания области и корневого администратора этой области можно переключиться в режим управления областью. Для этого необходимо в веб-консоли выйти из-под учетной записи администратора UGMC и заново зайти под учетной записью администратора управляемой области. Имя администратора следует указать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

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



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

имя_администратора/system, например, **Admin/system:**



Администраторы области

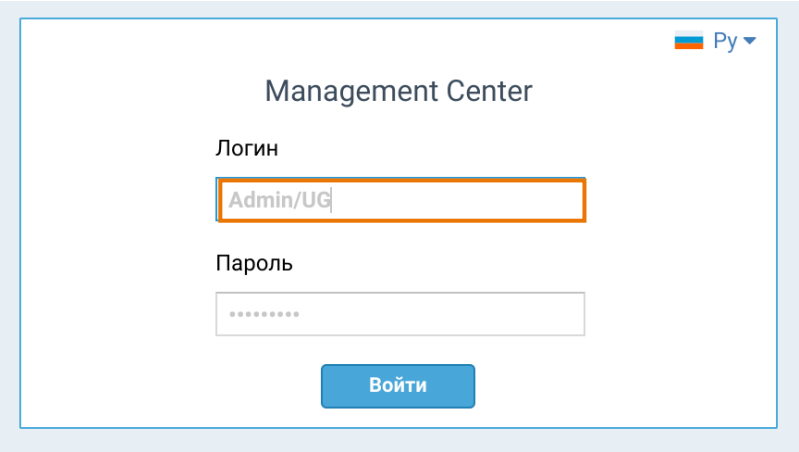
Корневой администратор управляемой области может создавать дополнительные учетные записи суб-администраторов области (региональных администраторов), делегируя им часть прав на управление областью или шаблонами.

Примечание

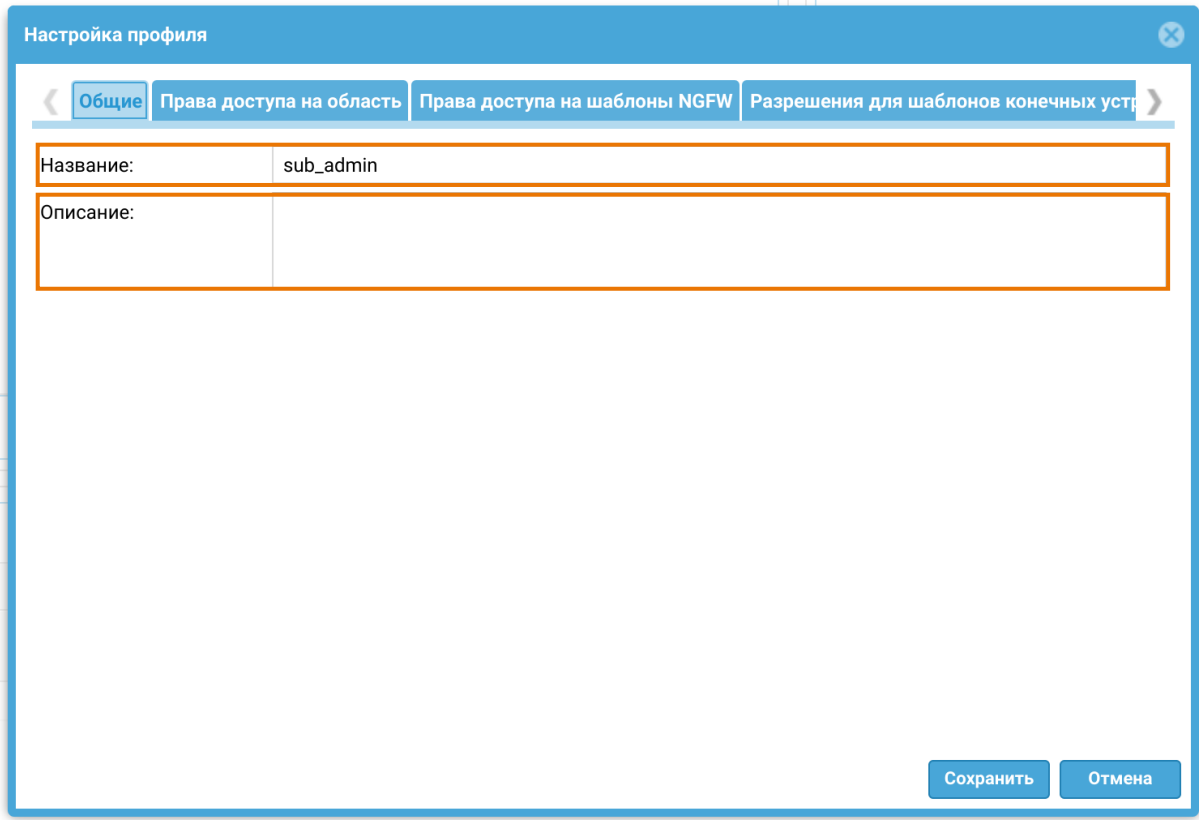
При создании управляемой области администратор UGMC создает корневого администратора области, обладающего всеми полномочиями на данную зону.

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

1. Войти в веб-консоль управления под корневым администратором области, указав имя в виде *имя_администратора/код_области,* например, ***Admin/UG***:



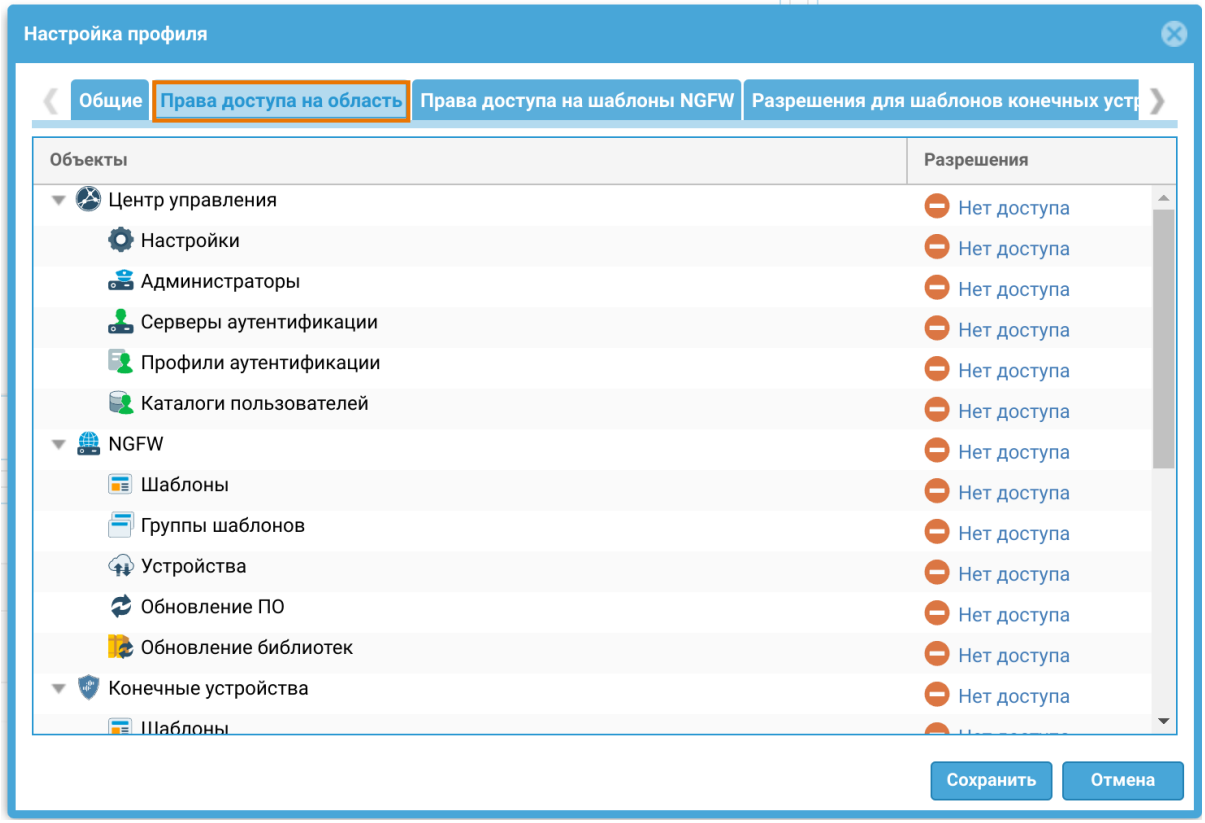
2. Создать профиль доступа дополнительного администратора области. В консоли управления областью в разделе **Администраторы → Профили администраторов** нажать кнопку **Добавить** и указать необходимые настройки:



На вкладке **Общие**:

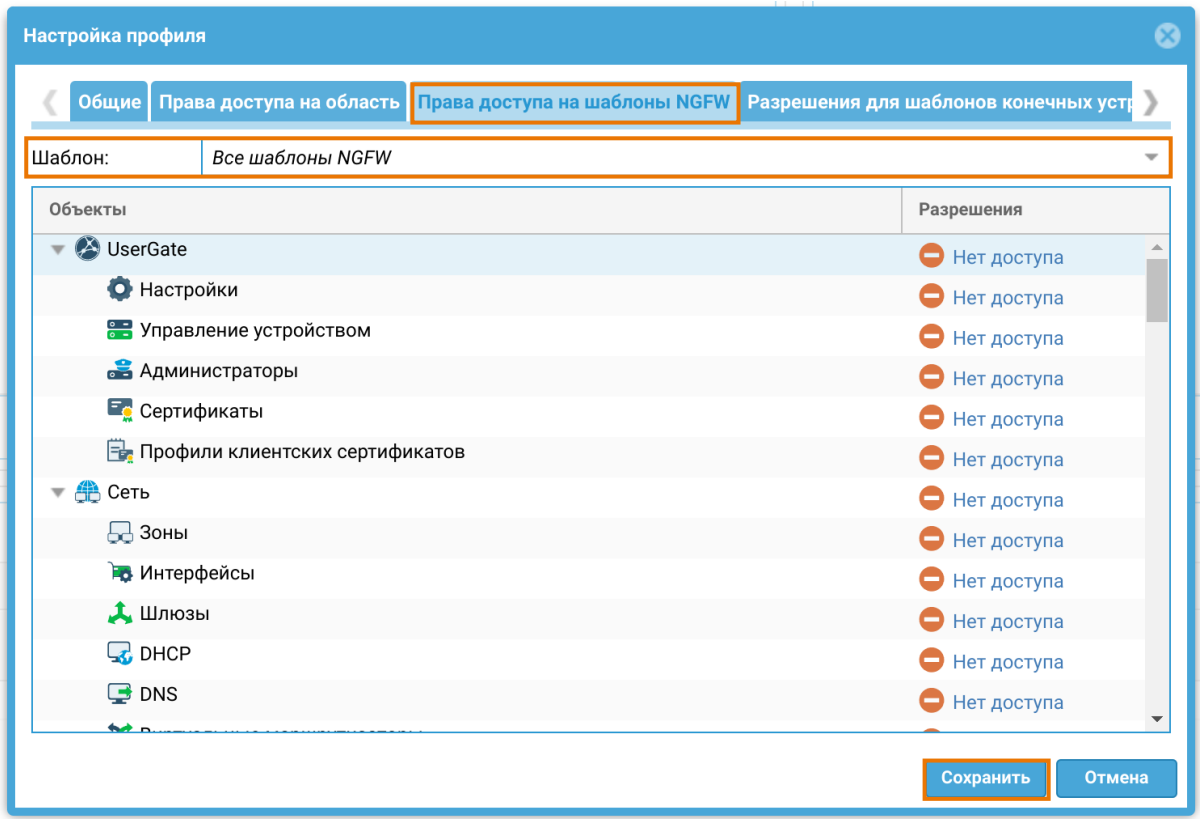
- Указать название профиля.

- Опционально описать назначение профиля.



На вкладке **Права доступа на область**:

- Указать права доступа на разделы настроек области. В качестве разрешений для доступа можно указать: **Нет доступа**; **Чтение**; **Чтение и запись**.

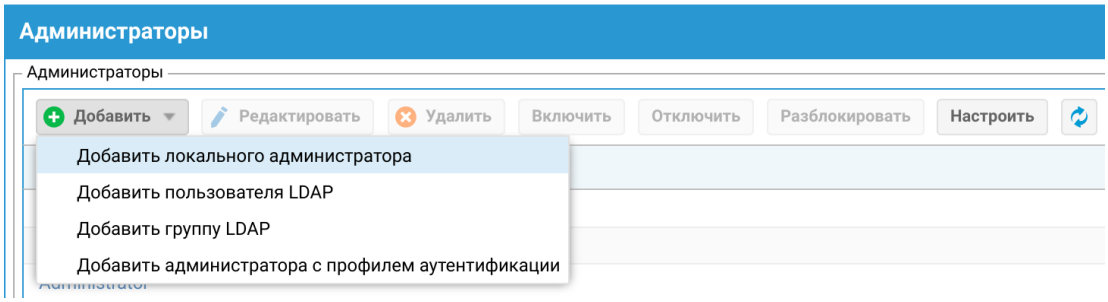


На вкладках **Права доступа на шаблоны ...**:

- В строке **Шаблон** выбрать конкретный шаблон или **Все шаблоны** для настройки прав доступа.
- В области ниже указать права доступа к настройкам шаблонов управляемых устройств. Настройки представлены в виде доступных для делегирования объектов дерева консоли управления устройств. В качестве разрешений для доступа можно указать: **Нет доступа**; **Чтение**; **Чтение и запись**.

3. Создать учетную запись дополнительного администратора области и назначить ей один из созданных ранее профилей администратора.

В разделе **Администраторы** нажать кнопку **Добавить** и выбрать необходимый вариант:



- **Добавить локального администратора** — создать локального пользователя, задать ему пароль доступа и назначить созданный ранее профиль доступа.
- **Добавить пользователя LDAP** — добавить пользователя из существующего домена. Для этого должен быть корректно настроен LDAP-коннектор в разделе **Серверы аутентификации** области. При входе в консоль администрирования необходимо указывать имя пользователя в формате 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 аутентификации** области. При входе в консоль администрирования необходимо указывать имя пользователя в формате user@domain. Назначить созданный ранее профиль.
- **Добавить администратора с профилем аутентификации** — создать пользователя, назначить созданный ранее профиль администратора и профиль аутентификации (необходимы корректно настроенные серверы аутентификации).

Серверы аутентификации области

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

LDAP-коннектор

LDAP-коннектор позволяет:

- Получать информацию о пользователях и группах Active Directory или других LDAP-серверов. Поддерживается работа с LDAP-сервером FreeIPA.

- Осуществлять авторизацию администраторов UGMC через домены Active Directory/FreeIPA.

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

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

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

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

domain\user/system или *user@domain/system*

Сервер аутентификации RADIUS

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

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

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

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

Сервер аутентификации TACACS+

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

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

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

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

Профили аутентификации области

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

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

Каталоги пользователей

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

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

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

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

Наименование	Описание
Пути поиска	Список путей в сервере LDAP, начиная с которых система будет осуществлять поиск пользователей и групп. Необходимо указывать полное имя, например, ou=Office,dc=example,dc=com.

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

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

УПРАВЛЕНИЕ МЕЖСЕТЕВЫМИ ЭКРАНАМИ USERGATE

Управление межсетевыми экранами UserGate (Описание)

Централизованное управление МЭ UserGate можно разделить на 4 этапа:

1. Создание управляемой области. Смотрите раздел Создание управляемых областей.
2. Создание шаблона или несколько шаблонов, каждый из которых опишет свою часть настроек МЭ. Смотрите раздел Шаблоны устройств для более детальной информации.
3. Объединение необходимых шаблонов в группу шаблонов в требуемом порядке, чтобы получить корректную результирующую настройку управляемых устройств. Смотрите раздел Группы шаблонов для более детальной информации.

4. Добавление управляемого устройство (МЭ) и применения к нему группы шаблонов. Смотрите раздел Добавление устройств UserGate под управление UGMC для более детальной информации.

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

UGMC позволяет создавать и управлять кластерами конфигурации и отказоустойчивости. Подробно тонкости управления кластерами описаны в разделе Кластеризация UserGate NGFW с помощью UGMC.

Шаблоны устройств

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

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

1. Если значение настройки не определено в шаблоне, то ничего передаваться в NGFW не будет. В данном случае в NGFW будет использована либо настройка по умолчанию, либо настройка, которую указал локальный администратор NGFW.

2. Если настройка параметра выполнена в шаблоне, то эта настройка переопределит значение этой же настройки, назначенной локальным администратором.

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

   - общие настройки устройства: вкладка **Настройки**, раздел **UserGate → Настройки**;

- настройки сетевых интерфейсов: вкладка **Настройки**, раздел **Сеть → Интерфейсы**.

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

3. Правила политик не переопределяют правила, созданные локальным администратором, а добавляются к ним в виде пре- и пост- правил. Подробно о применении правил смотрите раздел данного руководства Шаблоны и группы шаблонов.

4. При настройке сетевых интерфейсов первый физический интерфейс, доступный для конфигурирования — это **port1**. Интерфейс **port0** нельзя настроить с помощью средств UGMC, он всегда настраивается локальным администратором и необходим для обеспечения первичной связи управляемых устройств с UGMC.

5. При настройке сетевых интерфейсов возможно создать интерфейс и оставить его конфигурирование локальному администратору. Для этого необходимо поставить флажок **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 Межсетевых Экранов 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 NGFW. Для использования библиотек в политиках UGMC, необходимо предварительно добавить элементы в эти библиотеки. Элементы библиотек не участвуют в синхронизации: если список был создан, но не используется в политиках, то данный список не появится в разделе библиотек NGFW.

8. Рекомендуется создавать отдельные шаблоны для разных групп настроек, это позволит избежать конфликтов настроек при объединении шаблонов в

группы шаблонов и упростит понимание результирующей настройки, которая будет применена к управляемым устройствам. Например, шаблон сетевых настроек, шаблон правил межсетевого экрана, шаблон правил контентной фильтрации, шаблон библиотек и т.д.

Группы шаблонов

Группы шаблонов объединяют несколько шаблонов в единую конфигурацию, которая применяется к управляемому устройству. Результирующие настройки, применяемые к устройству, 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 **NGFW → Группы шаблонов** нажать на кнопку **Добавить**, дать группе имя и опциональное описание и добавить в него созданные ранее шаблоны. После добавления шаблонов их можно расположить в требуемом порядке, используя кнопки **Выше**, **Ниже**, **Наверх**, **Вниз**, создав таким образом необходимую результирующую конфигурацию.

Добавление устройств UserGate под управление UGMC

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

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

Наименование	Описание
устройством UserGate NGFW.	либо уже на настроенный NGFW. Оба варианта подробно описаны далее в этой главе.

При создании объекта управляемого устройства необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает объект управляемого устройства. Если объект управляемого устройства включен, то он занимает одну лицензию.
Название	Название для управляемого устройства. Можно вводить произвольное название.
Описание	Описание управляемого устройства.
Группа шаблонов	Группа шаблонов, настройки которой следует применить к этому управляемому устройству.
Синхронизация	Выбор режима синхронизации настроек группы шаблонов к устройству. Возможны 3 варианта: • **Автоматическая синхронизация** — синхронизация включена. Настройки применяются к устройству. При изменении любой настройки из любого шаблона, включенного в группу шаблонов, примененную к управляемому устройству, это изменение применяется к МЭ без задержек. • **Отключено** — синхронизация выключена. • **Ручная синхронизация** — режим синхронизации, при котором настройки применяются однократно при нажатии кнопки **Запросить синхронизацию**. Полезно в случаях, когда необходимо изменить много настроек в шаблонах и единовременно отослать их на устройство. В этом случае необходимо отключить синхронизацию, произвести необходимые изменения в шаблонах, после чего включить синхронизацию в режим Ручная синхронизация. Вне зависимости от выбранного режима доступен запуск синхронизации всех настроек для выбранных устройств (раздел **NGFW → Устройства** кнопка **Действия → Запустить полную синхронизацию**).
Адреса UserGate для связи с LogAn	Указание IP-адреса на управляемом NGFW для связи с LogAn.

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

Наименование	Описание
Шаг 1. Скопировать Код устройства	В UGMC выбрать созданный объект управляемого устройства и нажать на кнопку **Показать уникальный код устройства**. Скопировать данный код в буфер обмена.
Шаг 2. На NGFW в момент первоначальной инициализации выбрать установку с помощью UGMC	В момент первоначальной инициализации на этапе задания имени администратора и его пароля необходимо выбрать ссылку **Настроить через UGMC**.
Шаг 3. Указать необходимые настройки нового узла и ввести уникальный код устройства	Указать следующие параметры: • Сетевые настройки данного NGFW (IP, маска, шлюз). Данные настройки будут применены к указанному интерфейсу. Необходимо, чтобы после задания сетевых настроек появилась сетевая доступность с этого NGFW до UGMC. • Имя локального администратора и его пароль. • IP-адрес UGMC и уникальный код устройства, сохраненный на первом шаге.
Шаг 4. Проверить подключение	После подключения к UGMC, NGFW должен получить все настройки, подготовленные для него в UGMC. В NGFW настройки отображаются со значком замочка, означающим, что данную настройку локальный администратор не может изменять. В консоли UGMC в объекте управляемого устройства появится дополнительная информация о подключенном устройстве, такая как ПИН-код, серийный номер, информация о лицензии, используемой памяти и т.п.

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

Наименование	Описание
Шаг 1. Скопировать Код устройства	В UGMC выбрать созданный объект управляемого устройства и нажать на кнопку **Показать уникальный код устройства**. Скопировать данный код в буфер обмена.
Шаг 2. Указать IP-адрес сервера UGMC и ввести уникальный код устройства	В разделе **Настройки → Агент UGMC** выбрать **Настроить**, указать IP-адрес сервера UGMC, вставить уникальный код устройства и включить данное подключение. Для успешного

Наименование	Описание
	выполнения данного шага необходимо, чтобы была сетевая доступность с этого NGFW до сервера UGMC.
Шаг 3. Проверить подключение	После подключения к UGMC МЭ UserGate должен получить все настройки, подготовленные для него в UGMC. В МЭ настройки отображаются со значком замочка, означающим, что данную настройку локальный администратор не может изменять. В консоли UGMC в объекте управляемого устройства появится дополнительная информация о подключенном устройстве, такая как ПИН-код, серийный номер, информация о лицензии, используемой памяти и т.п.

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

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

Кластеризация UserGate NGFW с помощью UGMC

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

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** в документе Руководство администратора NGFW.
Шаг 2. Настроить на первом узле кластера зону, через интерфейсы которой будет выполняться репликация кластера	В разделе **Зоны** создать выделенную зону для репликации настроек кластера или использовать существующую (**Cluster**). В настройках зоны разрешить следующие сервисы: • Консоль администрирования • Кластер Не используйте для репликации зоны, интерфейсы которых подключены к недоверенным сетям, например, к интернету.
Шаг 3. Указать IP-адрес, который будет использоваться для связи с другими узлами кластера	В разделе **Управление устройством** в окне **Кластер конфигурации** выбрать текущий узел кластера и нажать на кнопку **Редактировать**. Указать IP-адрес интерфейса, входящего в зону, настроенную на шаге 2.
Шаг 4. Сгенерировать **Секретный код** на первом узле кластера	В разделе **Управление устройством** нажать на кнопку **Сгенерировать секретный код**. Полученный код скопировать в буфер обмена. Данный секретный код необходим для одноразовой авторизации второго узла при добавлении его в кластер.
Шаг 5. Подключить первый узел кластера конфигурации в UGMC	Подключение первого узла ничем не отличается от подключения отдельно стоящего устройства UserGate. Процедура подключения подробно описана в разделе Добавление устройств UserGate под управление UGMC. Первому узлу автоматически назначается идентификатор *node_1*.
Шаг 6. Подключить второй узел в кластер	**Важно!** Добавление в кластер конфигурации второго и последующих узлов возможно только при первоначальной инициализации этих узлов.

Наименование	Описание
	Подключиться к веб-консоли второго узла кластера, выбрать язык установки. Указать интерфейс, который будет использован для подключения к первому узлу кластера, и назначить ему IP-адрес. Оба узла кластера должны находиться в одной подсети, например, интерфейсам eth2 обоих узлов назначены IP-адреса 192.168.100.5/24 и 192.168.100.6/24. В противном случае необходимо указать IP-адрес шлюза, через который будет доступен первый узел кластера. Указать IP-адрес первого узла, настроенный на шаге 3, вставить секретный код и нажать на кнопку **Подключить**. Если IP-адреса кластера, настроенные на шаге 2, назначены корректно, то система предложит назначить идентификатор кластера для добавляемого устройства в виде *node_2, node_3, node_4* и так далее. Идентификатор *node_1* уже был закреплен за первым узлом кластера. После назначения идентификатора второй узел будет добавлен в кластер, и все настройки первого узла реплицируются на второй. После успешного добавления узла в кластер, данный узел будет отображаться в качестве второго узла в списке управляемых устройств с выбранным идентификатором.

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

Добавление третьего и последующих узлов в кластер конфигурации выполняется аналогично.

Кластер отказоустойчивости

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

Наименование	Описание
Наличие кластера конфигурации	Должен быть создан кластер конфигурации. Кластер конфигурации должен корректно отображаться в списке управляемых устройств.

Наименование	Описание
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** в документе Руководство администратора NGFW.

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 аутентификацию с помощью Captive-портала, то необходимо, чтобы системные имена auth.captive и logout.captive, которые используются процедурами аутентификации в Captive, определялись в IP-адрес, назначенный в качестве кластерного виртуального адреса. Данную настройку можно выполнить в одном из шаблонов **UGMC**, в разделе **Настройки**.

Параметры отказоустойчивого кластера:

Наименование	Описание
Вкл	Включение/отключение отказоустойчивого кластера.
Название	Название отказоустойчивого кластера.
Описание	Описание отказоустойчивого кластера.
Режим кластера	

Наименование	Описание
	Режим отказоустойчивого кластера: • **Актив-Актив** — нагрузка распределяется на все узлы кластера • **Актив-Пассив** — нагрузка идет на Мастер-узел и переключается на запасной узел в случае недоступности Мастер-узла.
Синхронизировать сессии	Включает режим синхронизации пользовательских сессий между всеми узлами, входящими в кластер отказоустойчивости. Включение данной опции делает переключение пользователей с одного устройства на другое прозрачным для пользователей, но добавляет существенную нагрузку на платформу UserGate. Имеет смысл только для режима кластера Актив-Пассив.
Мультикаст идентификатор кластера	В одном кластере конфигурации может быть создано несколько кластеров отказоустойчивости. Для синхронизации сессий используется определенный мультикастовый адрес, определяемый данным параметром. Для каждой группы кластеров отказоустойчивости, в которой должна поддерживаться синхронизация сессий, требуется установить уникальный идентификатор.
Идентификатор виртуального роутера (VRID)	Идентификатор виртуального роутера должен быть уникален для каждого VRRP-кластера в локальной сети. Если в сети не присутствуют сторонние кластеры VRRP, то рекомендуется оставить значение по умолчанию.
Узлы	Выбираются узлы кластера конфигурации для объединения их в кластер отказоустойчивости. Узлы кластера представлены идентификаторами, назначенными узлам кластера конфигурации при создании кластера конфигурации.
Виртуальные IP-адреса	Назначаются виртуальные IP-адреса и их соответствие интерфейсам узлов кластера. В качестве интерфейсов могут быть использованы только интерфейсы, которые были созданы в одном из шаблонов UGMC.

Управление обновлениями управляемых устройств

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

> **Примечание**
> **После добавления UserGate NGFW 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 **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 UserGate	Политика обновлений ПО позволяет задать обновление, доступное для установки на все или выборочные управляемые устройства. Подробно 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 управляемые устройства. Подробно об обновлениях библиотек смотрите в разделе Обновление библиотек.

Обновление ПО

Компания UserGate периодически выпускает обновления программного обеспечения UserGate NGFW. Эти обновления выкладываются в репозитарий UserGate, откуда они уже доступны для скачивания NGFW. Если NGFW подключен к управлению через UGMC, то он проверяет наличие обновлений на сервере UGMC, который сам будет являться репозитарием. Репозитарий UserGate при этом будет использован сервером UGMC для получения новых обновлений.

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

Порядок установки обновлений, следующий:

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

Обновление в репозитарии 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.

Наименование	Описание
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 репозитария UserGate.
Канал обновлений	Канал обновлений репозитария UserGate: • Стабильные — канал стабильных обновлений ПО. • Бета — канал экспериментальных обновлений.
Список изменений	Ссылка на список изменений, содержащихся в данном обновлении.
Управляемые устройства	Список управляемых устройств, которым назначено данное обновление.
Добавлено	Дата добавления обновления в репозитарий UGMC и имя администратора, который выполнил добавление.
Утверждено	Дата утверждения обновления и имя администратора, который выполнил утверждение.

Обновление библиотек

Библиотеки — это обновляемые базы ресурсов, предоставляемых по подписке клиентам UserGate (база категорий URL-фильтрации, сигнатуры СОВ, списки IP-адресов, URL, MIME-типов, морфологические базы и другие). Эти обновления выкладываются в репозитарий UserGate, откуда они уже доступны для скачивания UserGate NGFW. Если NGFW подключен к управлению через UGMC, то он проверяет наличие обновлений на сервере UGMC, который сам будет являться репозитарием. Репозитарий UserGate при этом будет использован сервером UGMC для получения новых обновлений. По умолчанию UGMC проверяет и скачивает обновления библиотек автоматически.

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

Библиотеки, находящиеся в репозитарии UGMC доступны всем управляемым устройствам UserGate. Управляемые устройства скачивают и устанавливают

доступные обновления автоматически в соответствии с расписанием проверки обновлений.

Обновление библиотек в репозитарии UGMC имеет следующие свойства:

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

Аварийное отключение NGFW от MC

При необходимости NGFW может быть отключен от MC, с которым он был интегрирован, с помощью команды аварийного отключения.

Команда выполняется на NGFW в интерфейсе командной строки (CLI) в режиме конфигурации (подробнее читайте в статье Режим конфигурации руководства администратора NGFW):

```
Admin@nodename# execute mc-force-disconnect <arg>
```

В зависимости от выбранного аргумента импортированные из MC объекты сохраняются локально или удаляются:

- **keep** — отключение от MC с сохранением всех импортированных из MC объектов (библиотеки, правила итд.). Импортированные из MC объекты конвертируются в локальные.

- **delete** — отключение от МС с удалением всех импортированных из МС объектов (библиотеки, правила итд.). Импортированные объекты, которые в настоящий момент используются, конвертируются в локальные.

```
Admin@nodename# execute mc-force-disconnect keep
Admin@nodename# execute mc-force-disconnect delete
```

Практика работы с шаблонами в UserGate MC

В UserGate MC реализована гибкая система управления конфигурациями устройств благодаря иерархической системе администрирования (подробнее читайте в разделе Администраторы) и использованию метода шаблонов (подробнее читайте в разделе Управление межсетевыми экранами UserGate).

Управление устройствами осуществляется в пределах управляемой области. Управляемая область может иметь в своем составе множество филиалов (городов), в которых установлены подконтрольные устройства.

Корневой администратор области имеет все права на управление областью. Он может создавать шаблоны настроек управляемых устройств, объединять шаблоны в группы и назначать эти группы на управляемые устройства. Корневой администратор управляемой области может создавать учетные записи дополнительных администраторов области или, иначе говоря, региональных администраторов, делегируя им права на администрирование только отдельных выделенных устройств в филиалах.

Группы шаблонов могут включать в себя шаблоны, которые настраивает как сам администратор области, так и региональные администраторы.

Порядок шаблонов в группе имеет значение и определяет приоритет политик или используемых в них объектов.

Порядок применения правил на управляемом устройстве следующий:

1. Пре-правила первого шаблона, пре-правила второго шаблона и т.д.
2. Локальные правила политики на устройстве.
3. Пост-правила первого шаблона, пост-правила второго шаблона и т.д.

Это позволяет вставить правила в любое место в списке правил управляемого устройства.

Порядок применения объектов, которые не являются правилами — берётся первый найденный подходящий объект при проходе по списку шаблонов из группы.

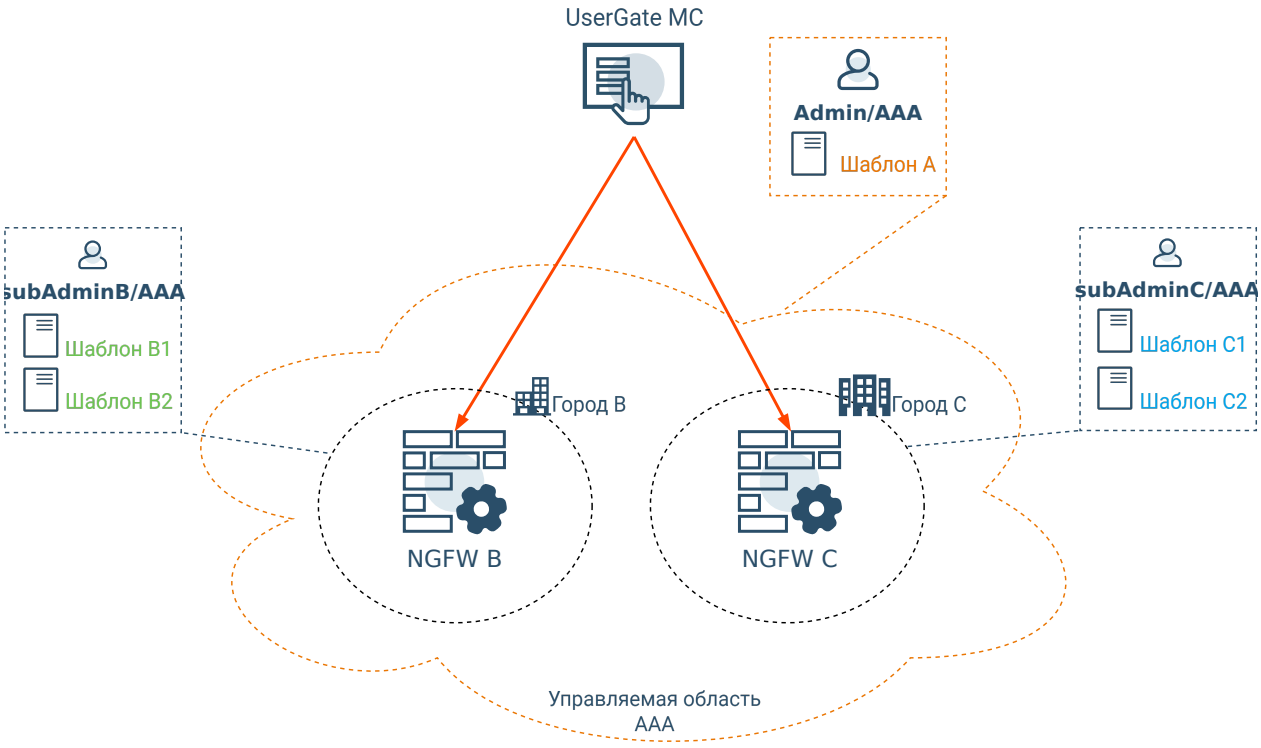
Благодаря такому подходу реализуется иерархическая система администрирования — администратор области управляет политиками на уровне организации, а региональные администраторы управляют политиками в своих филиалах. Администратор области создает шаблон общих политик для всех филиалов, который он может добавлять в группы шаблонов для региональных устройств. Таким образом решается задача управления политиками информационной безопасности на уровне организации. В свою очередь, региональные администраторы через свои шаблоны решают локальные задачи своих филиалов.

Рассмотрим два примера работы с шаблонами в пределах управляемой области.

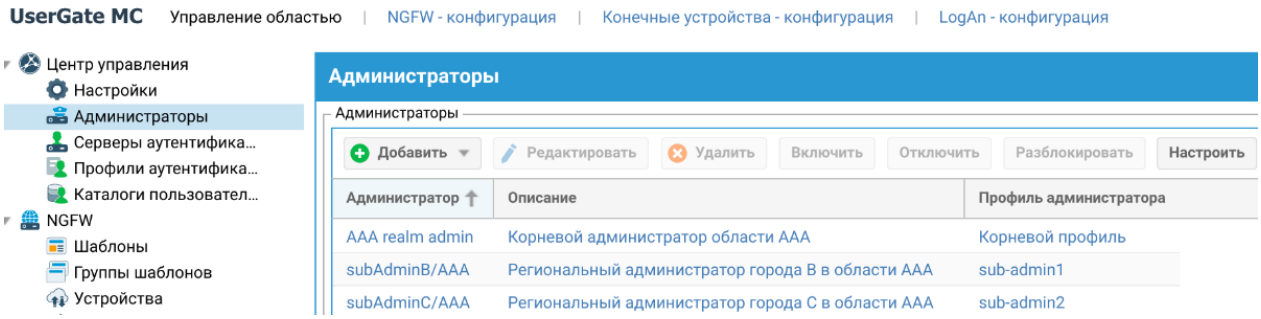
Пример 1. Группирование шаблонов

Пример группирования шаблонов для филиалов в управляемой области.

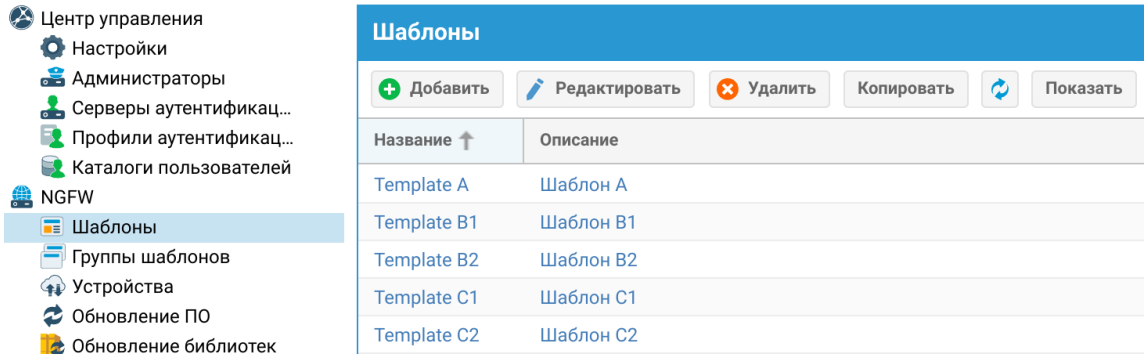
В UserGate MC создана управляемая область AAA с корневым администратором области **Admin/AAA**.



Администратор области создает двух региональных администраторов для управления узлами NGFW в городах B и C (**subAdminB/AAA** и **subAdminC/AAA** соответственно).

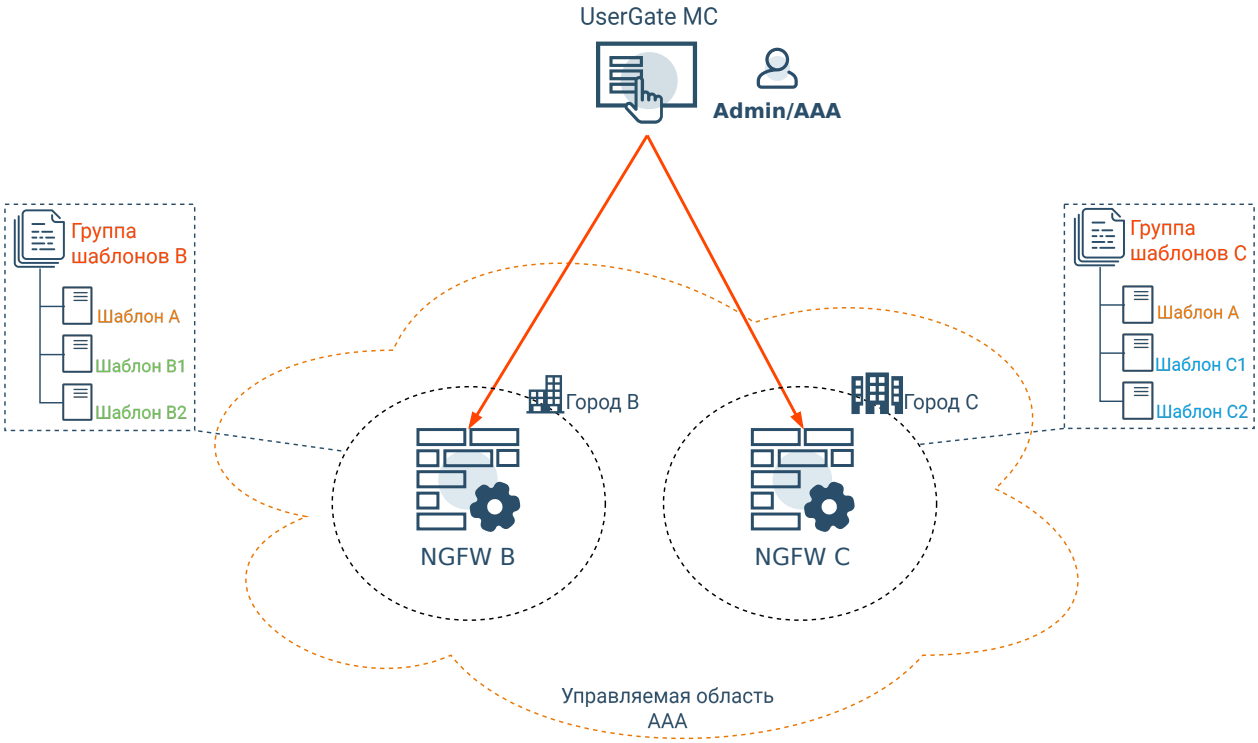


Администратор области создает шаблоны для управления региональными узлами и предоставляет права на редактирование части шаблонов региональным администраторам:

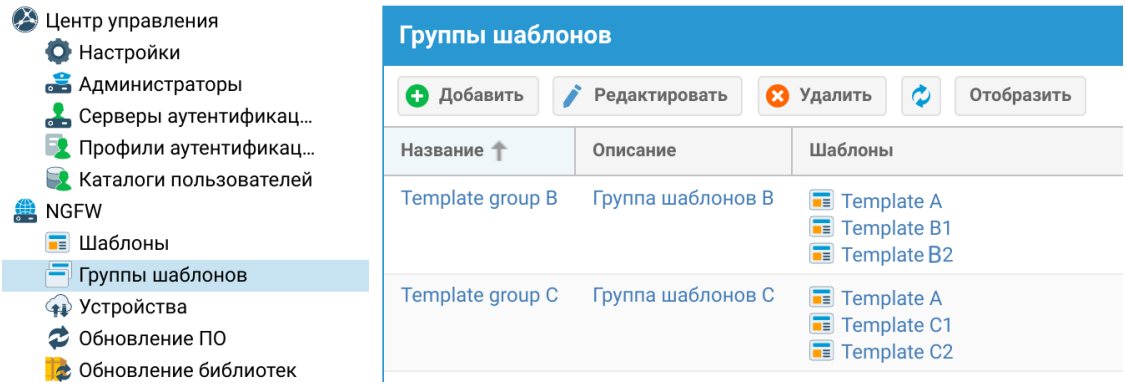


- Шаблон A — для настройки базовых политик конфигурации сети администратором области.
- Шаблоны B1 и B2 — для локальных настроек политик узла в филиале B. Региональному администратору в городе B (**subAdminB/AAA**) делегируются права для настройки этих шаблонов.
- Шаблоны C1 и C2 — для локальных настроек политик узла в городе C. Региональному администратору в городе C (**subAdminC/AAA**) делегируются права для настройки этих шаблонов.

Администратор области создает группы шаблонов, в которые он может добавить любые шаблоны, созданные и настраиваемые в любом регионе своей области.



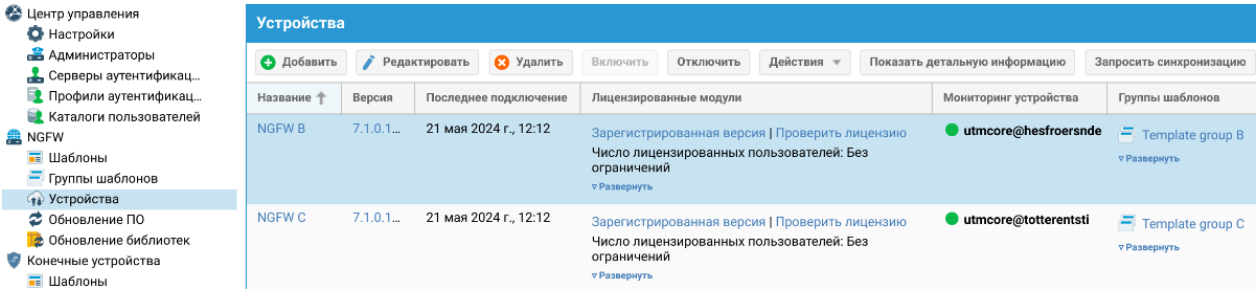
В этом примере администратор области создает для каждого города свою группу шаблонов, куда он добавляет общий шаблон с базовыми политиками конфигурации сети и шаблоны с локальнями настройками политик, редактируемые региональными алминистраторами:



- Группа шаблонов для города B:
  - Шаблон A;
  - Шаблон B1;
  - Шаблон B2;
- Группа шаблонов для города C:
  - Шаблон A;

- Шаблон C1;
- Шаблон C2.

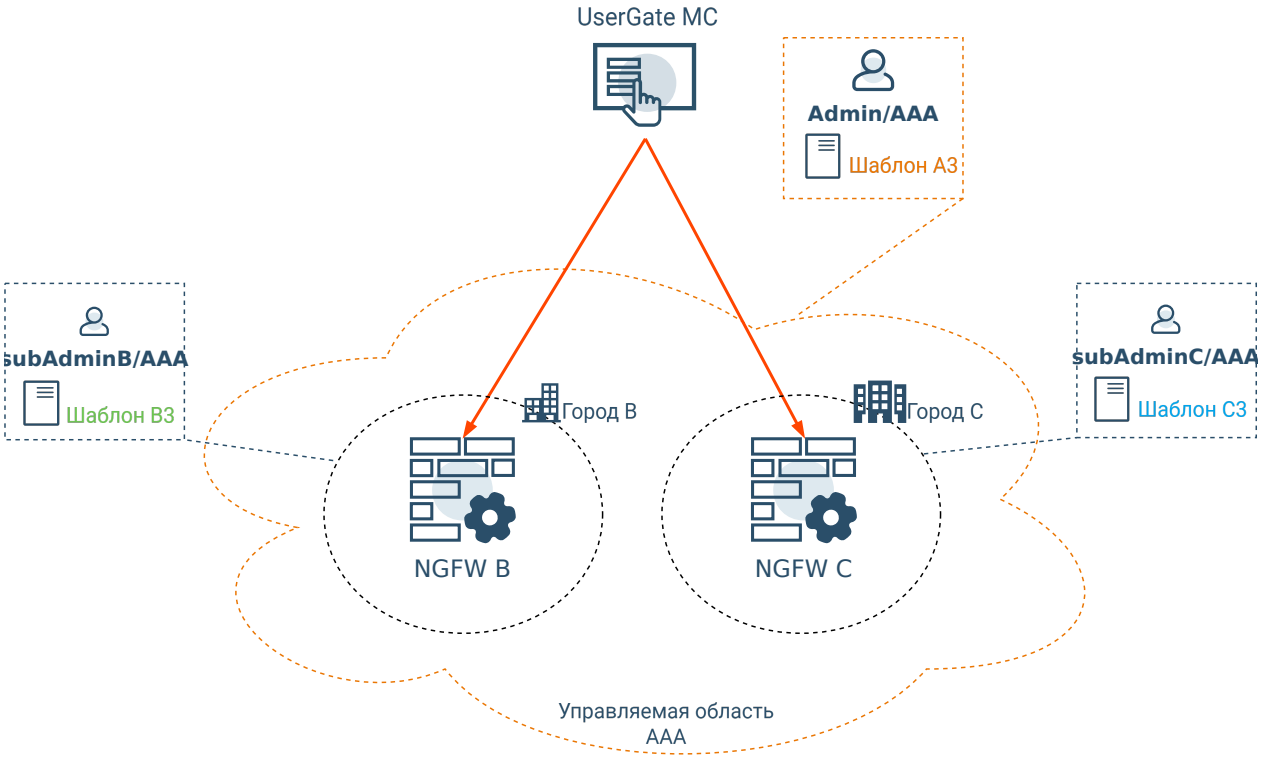
Администратор области назначает группы шаблонов на конкретные управляемые устройства.



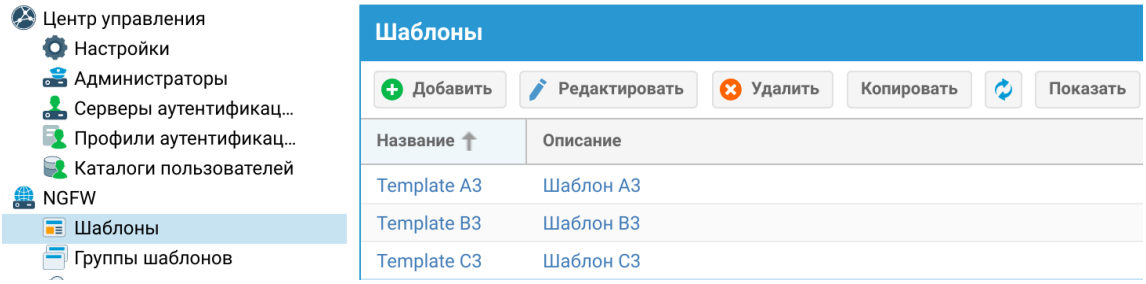
Пример 2. Схема с главной политикой

В такой схеме есть одна центральная политика, но её конкретная финальная форма будет разной для разных регионов.

Как и в Примере 1 в управляемой области AAA есть два города B и C, в каждом из которых установлены свои NGFW, они оба подключены к MC. Созданы два региональных администратора для управления узлами NGFW в городах B и C (**subAdminB/AAA** и **subAdminC/AAA** соответственно).



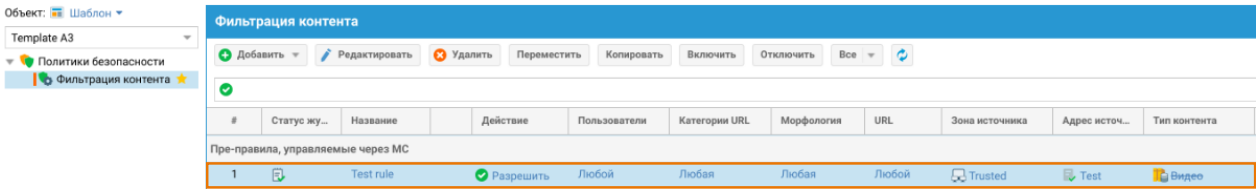
Администратор области имеет шаблон общей политики, который ограничивает доступ группы с IP-адресами Test к сайтам с видеоконтентом. Для каждого города есть свои шаблоны, в которых региональные администраторы определяют список своих локальных адресов для группы Test:

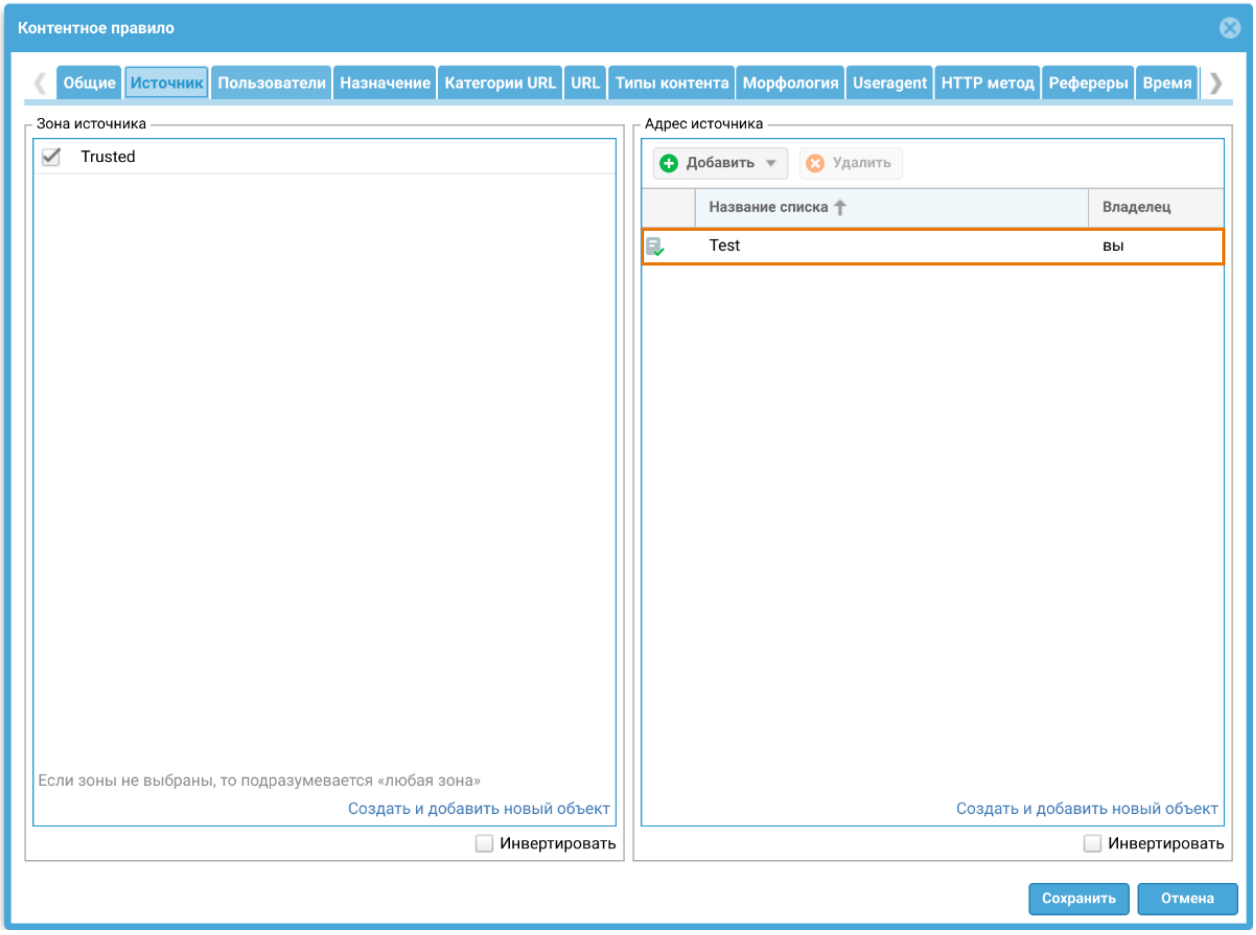


- Шаблон A3 — шаблон общей политики администратора области с настройкой ограничения доступа к видеоконтенту.
- Шаблон B3 — для настройки группы IP-адресов, к которым должна быть применена политика. Региональному администратору города B (**subAdminB/AAA**) делегируются права для настройки параметров этого шаблона.
- Шаблон C3 — для настройки группы IP-адресов, к которым должна быть применена политика. Региональному администратору города C (**subAdminC/AAA**) делегируются права для настройки параметров этого шаблона.

Настройка шаблонов

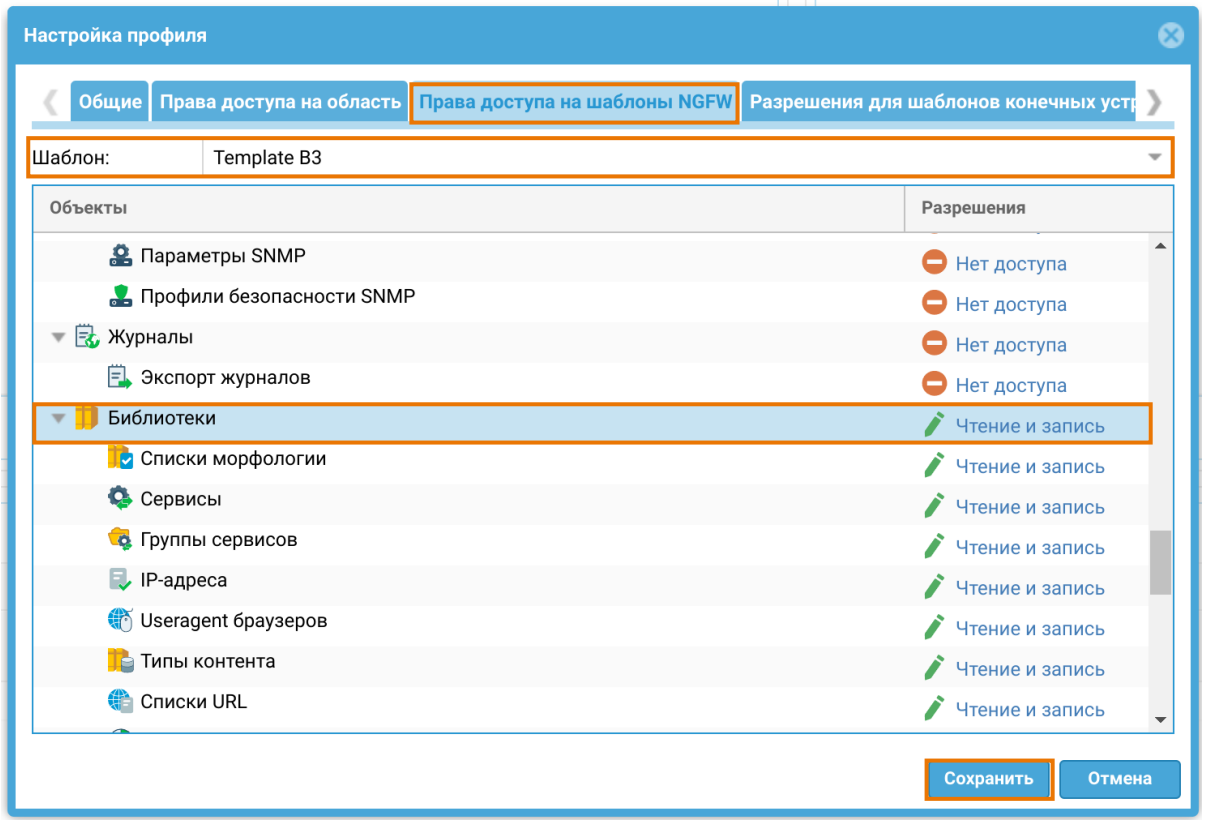
Администратор области в шаблоне A3 создает правило фильтрации видеоконтента, в котором на вкладке **Источник** указывает группу IP-адресов **Test**, но сами адреса в этом шаблоне не задаются. Списки IP адресов, к которым будет применено правило общей политики, будут создаваться в группе адресов **Test** региональными администраторами в своих шаблонах.



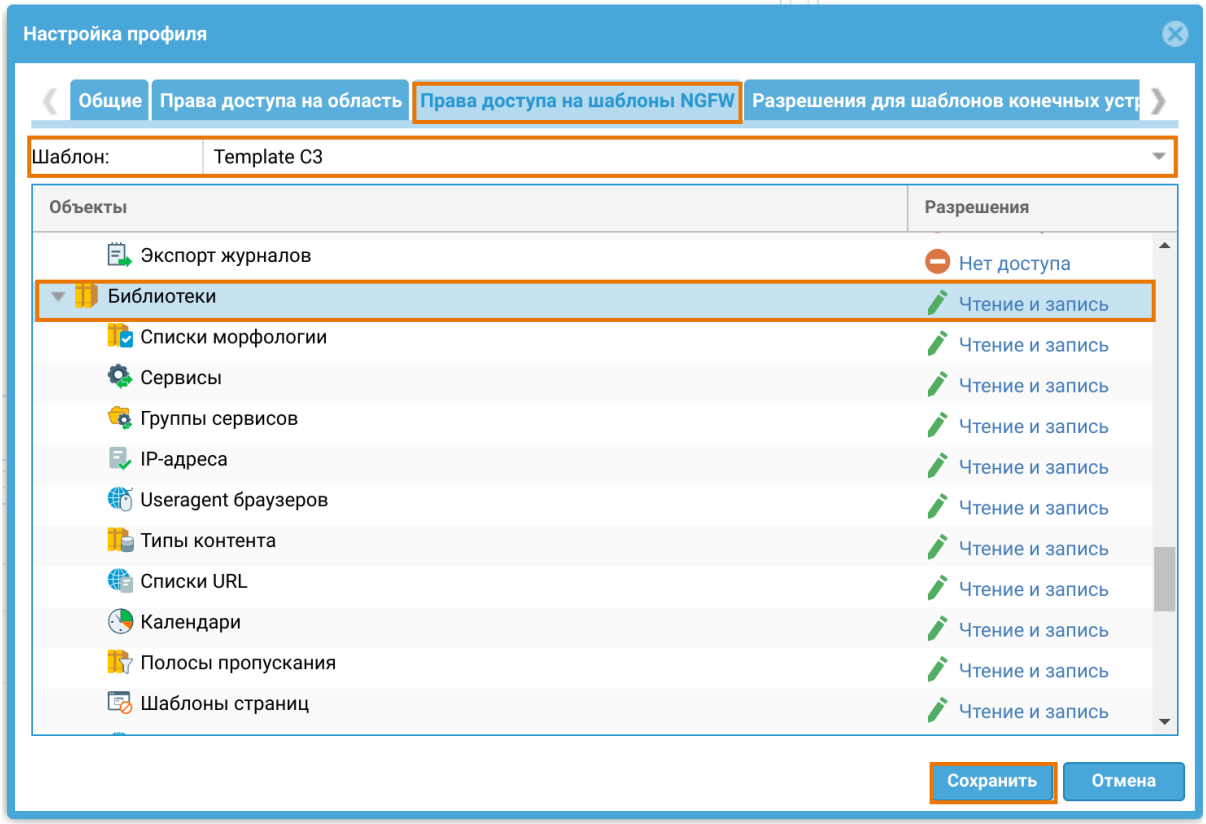


Администратор области делегирует региональным администраторам права для настройки библиотек элементов в шаблонах B3 и C3. Для этого в веб-консоли администратора области необходимо перейти в раздел **Центр управления → Администраторы → Профили администраторов** и в профилях региональных администраторов предоставить права на чтение и запись для раздела **Библиотеки элементов**.

Региональному администратору города B необходимо делегировать права в шаблоне B3:

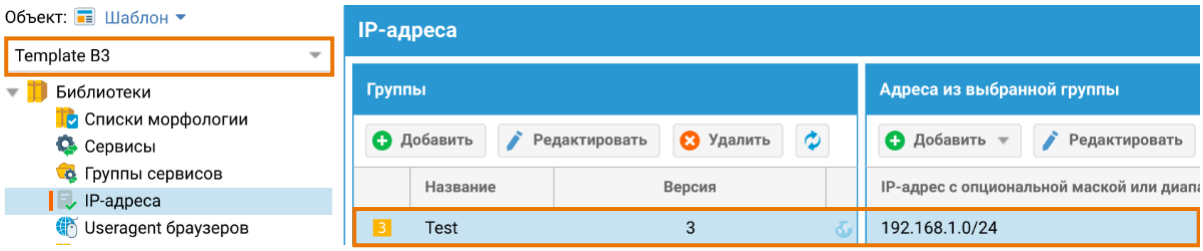


Региональному администратору города С необходимо делегировать права в шаблоне С3:

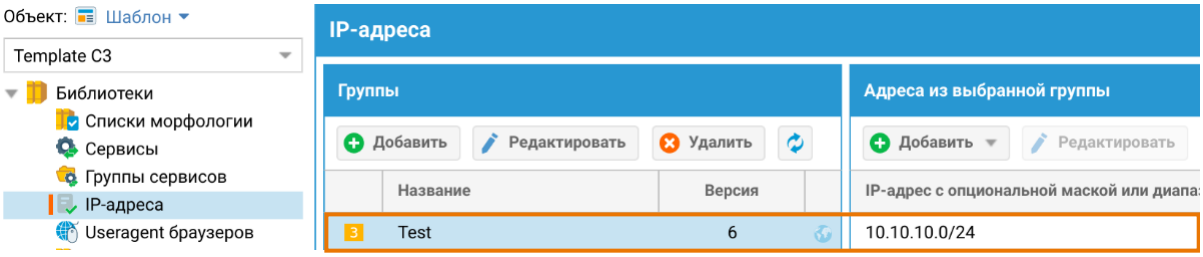


Региональные администраторы создают в своих шаблонах группу IP-адресов **Test**. Для этого каждый региональный администратор должен войти в веб-консоль администратора со своим логином (**subAdminB/AAA** и **subAdminC/AAA** соответственно), перейти в раздел настройки шаблона (шаблон B3 и шаблон C3 соответственно) и создать группу IP-адресов **Test** со своими актуальными адресами:

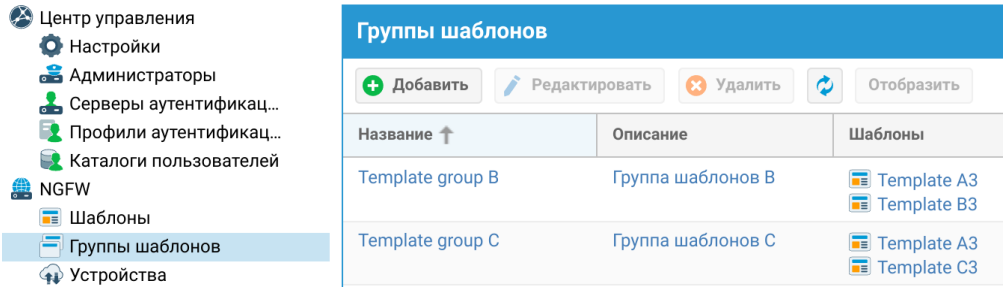
Региональный администратор города B редактирует шаблон B3:



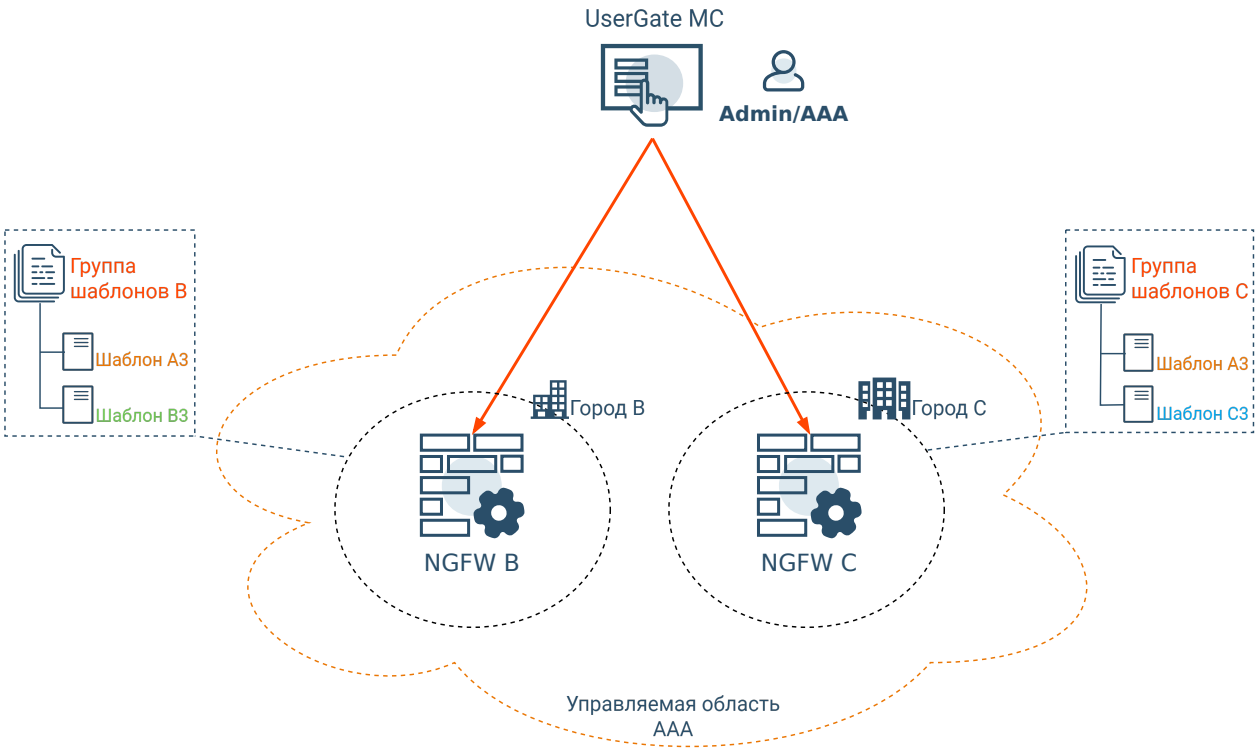
Региональный администратор города C редактирует шаблон C3:



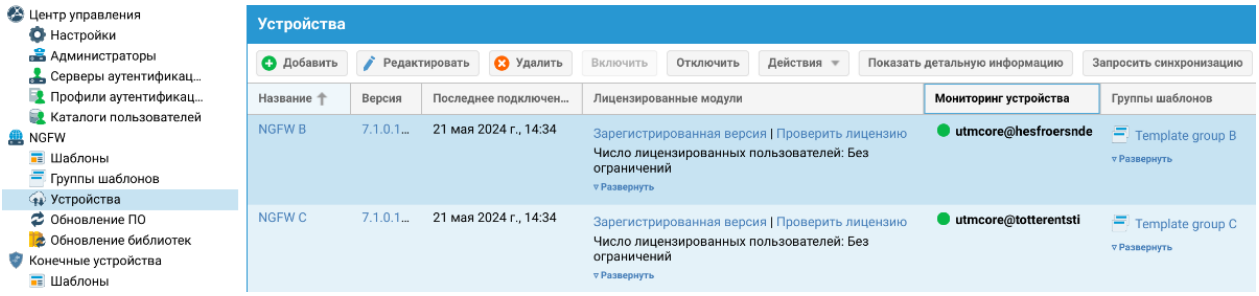
Администратор области объединяет шаблоны в группы:



- Группа шаблонов для города B:
  - Шаблон A3;
  - Шаблон B3;
- Группа шаблонов для города C:
  - Шаблон A3;
  - Шаблон C3.



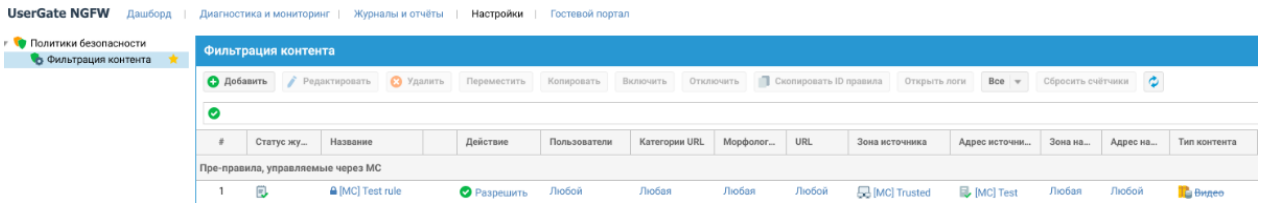
Администратор области назначает группы шаблонов на конкретные управляемые устройства.

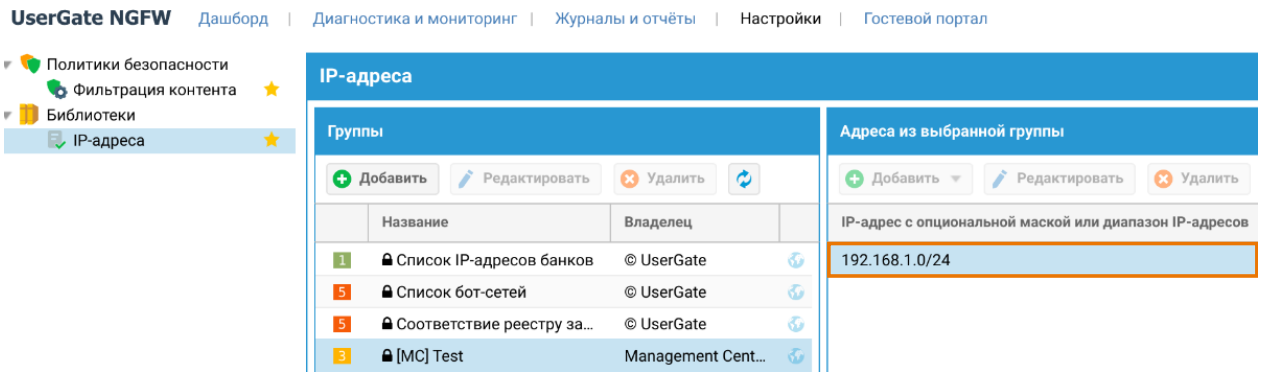


Проверка работы схемы

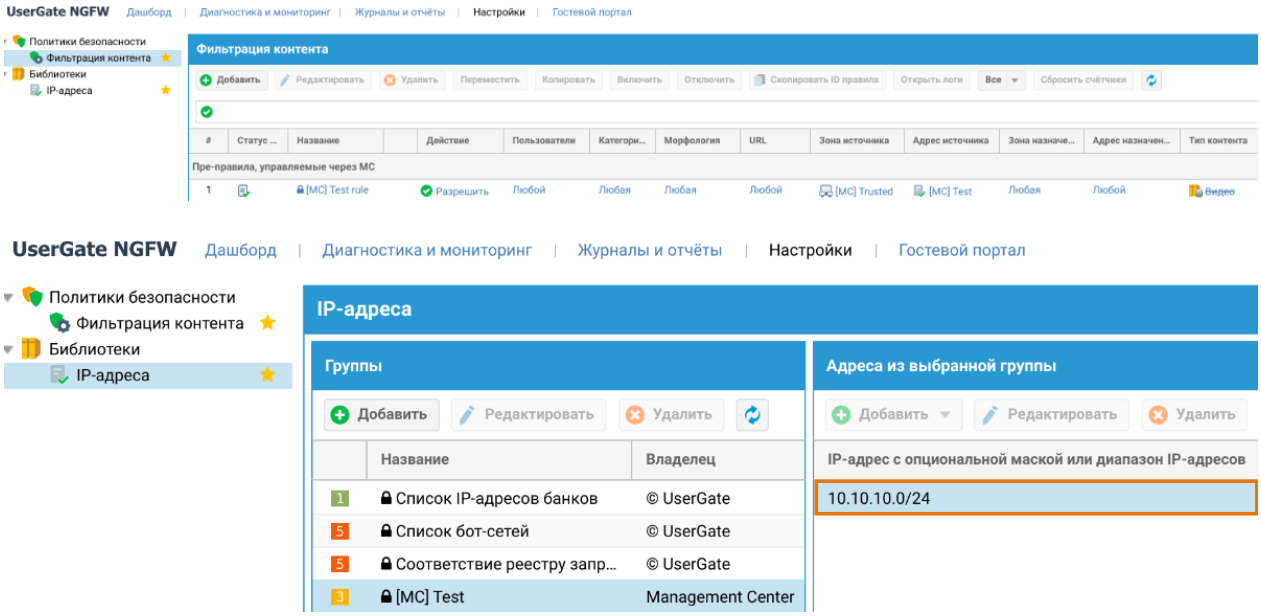
У каждого регионального устройства есть собственные политики со своими собственными правилами фильтрации видео-контента.

NGFW B:





NGFW C:



Таким образом, в данном примере используется централизованное управление политикой доступа к сайтам с видеоконтентом для двух городов, но при этом учитываются региональные особенности (разные подсети) каждого филиала. Администратор области отвечает за создание и управление общим шаблоном политики, а региональные администраторы отвечают за настройку и управление своими устройствами с учетом региональных особенностей.

УПРАВЛЕНИЕ УСТРОЙСТВАМИ LOGAN

Управление устройствами LogAn (Описание)

Централизованное управление устройствами LogAn можно разделить на 4 этапа:

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

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

Шаблоны устройств LogAn

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

После создания шаблона можно производить настройку его параметров. Для этого необходимо перейти в раздел верхнего меню **LogAn-конфигурация** и в выпадающем меню **Выбрать шаблон** выбрать необходимый шаблон.

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

1. Если значение настройки не определено в шаблоне, то ничего передаваться в LogAn не будет. В данном случае в LogAn будет

использована либо настройка по умолчанию, либо настройка, которую указал локальный администратор.

2. Если настройка параметра выполнена в шаблоне, то эта настройка переопределит значение этой же настройки, назначенной локальным администратором.

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

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

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

3. При настройке сетевых интерфейсов первый физический интерфейс, доступный для конфигурирования — это **port1**. Интерфейс **port0** нельзя настроить с помощью средств UGMC, он всегда настраивается локальным администратором и необходим для обеспечения первичной связи управляемого устройства с UGMC.

4. При настройке сетевых интерфейсов возможно создать интерфейс и оставить его конфигурирование локальному администратору. Для этого необходимо поставить флаг **Настраивается на устройстве** в настройках сетевого интерфейса.

5. В некоторых настройках и правилах политик доступна опция применения данного правила или настройки только к конкретному устройству. Для этого необходимо выбрать управляемое устройство в свойствах правила/настройки в закладке **Управляемые устройства**. Хотя это и предоставляет определенную гибкость, следует избегать чрезмерного использования данной опции, поскольку это приводит к сложности понимания применения настроек к группам устройств LogAn.

6. Библиотеки, например, такие как IP-адреса, списки URL, типы контента и другие, по умолчанию не содержат никакого контента в UGMC в отличие от библиотек, создаваемых по умолчанию на устройствах UserGate. Для

использования библиотек в политиках UGMC, необходимо предварительно добавить элементы в эти библиотеки.

7. Рекомендуется создавать отдельные шаблоны для разных групп настроек, это позволит избежать конфликтов настроек при объединении шаблонов в группы шаблонов и упростит понимание результирующей настройки, которая будет применена к управляемым устройствам. Например, шаблон сетевых настроек, шаблон библиотек и т.д.

Группы шаблонов LogAn

Группы шаблонов объединяют несколько шаблонов в единую конфигурацию, которая применяется к управляемому устройству. Результирующие настройки, применяемые к устройству LogAn, формируются в результате слияния всех настроек шаблонов, входящих в группу шаблонов, с учетом расположения шаблонов внутри группы. Подробнее о результирующих настройках смотрите главу руководства Шаблоны и группы шаблонов.

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

Добавление устройств LogAn под управление UGMC

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

Наименование	Описание
Шаг 1. Обеспечить доступ от управляемого устройства до UGMC.	На сервере UGMC необходимо разрешить сервис **UserGate Management Center** на зоне, к которой подключены управляемые устройства. Сервер UGMC слушает подключения от управляемого устройства на портах TCP 2022 и 9712. Передача данных между сервером UGMC и управляемым устройством осуществляется по зашифрованному каналу.

Наименование	Описание
Шаг 2. Создать объект управляемого устройства LogAn.	В консоли управления областью в разделе **LogAn → Устройства** нажать кнопку **Добавить** и указать необходимые настройки.
Шаг 3. Связать созданный объект управляемого устройства LogAn с реальным устройством LogAn.	В консоли управления LogAn настройте связь между UGMC и устройством. Данную операцию можно произвести в момент первоначальной установки LogAn либо уже на настроенном устройстве LogAn. Оба варианта подробно описаны далее в этой главе.

При создании объекта управляемого устройства LogAn необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает объект управляемого устройства . Если объект управляемого устройства включен, то он занимает одну лицензию.
Название	Название для управляемого устройства . Можно вводить произвольное название.
Описание	Описание управляемого устройства.
Группа шаблонов	Группа шаблонов, настройки которой следует применить к этому управляемому устройству .
Синхронизация	Выбор режима синхронизации настроек группы шаблонов к устройству. Возможны 3 варианта: • **Автоматическая синхронизация** — настройки применяются к устройству автоматически. При изменении любой настройки из любого шаблона, включенного в группу шаблонов, примененную к управляемому устройству, это изменение применяется к LogAn без задержек. • **Отключено** — синхронизация выключена. • **Ручная синхронизация** — режим синхронизации, при котором настройки применяются при нажатии кнопки **Запросить синхронизацию**. Полезно в случаях, когда необходимо изменить много настроек в шаблонах и единовременно отослать их на устройство. В этом случае необходимо отключить синхронизацию, произвести необходимые изменения в шаблонах, после чего включить синхронизацию в режим Ручная синхронизация.

Наименование	Описание
	Вне зависимости от выбранного режима доступен запуск синхронизации всех настроек для выбранных устройств (раздел **LogAn → Устройства** кнопка **Действия → Запустить полную синхронизацию**).

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

Наименование	Описание
Шаг 1. Скопировать Код устройства.	В UGMC выбрать созданный объект управляемого устройства и нажать **Действия → Показать уникальный код устройства**. Скопировать данный код в буфер обмена.
Шаг 2. На LogAn в момент первоначальной инициализации выбрать установку с помощью UGMC.	В момент первоначальной инициализации на этапе задания имени администратора и его пароля необходимо выбрать ссылку **Настроить через UGMC**.
Шаг 3. Указать необходимые настройки нового узла и ввести уникальный код устройства.	Указать следующие параметры: • Сетевые настройки данного LogAn (IP, маска, шлюз). Данные настройки будут применены к указанному интерфейсу. Необходимо, чтобы после задания сетевых настроек появилась сетевая доступность с этого устройства до сервера UGMC. • Имя локального администратора и его пароль. • IP-адрес сервера UGMC и уникальный код устройства, сохраненный на первом шаге.
Шаг 4. Проверить подключение.	После подключения к UGMC LogAn должен получить все настройки, подготовленные для него в UGMC. В LogAn настройки отображаются со значком замочка, означающим, что данную настройку локальный администратор не может изменять. В консоли UGMC в объекте управляемого устройства появится дополнительная информация о подключенном устройстве, такая как ПИН-код, серийный номер, информация о лицензии, используемой памяти и т.п.

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

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

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

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

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

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

Управление обновлениями управляемых устройств LogAn

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

> **Примечание**
> **После добавления управляемого устройства LogAn под управление UGMC, устройство автоматически начинает скачивать все обновления с сервера UGMC.**

Для управления обновлениями с помощью UGMC необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Настроить расписание проверки обновлений.	Расписание проверки устанавливает время и периодичность проверки обновлений. Оно может быть настроено локально на каждом из устройств LogAn либо централизовано с помощью настройки шаблонов в UGMC. В обоих случаях настройка выполняется идентично. В случае локальной настройки она производится в разделе **Настройки** в веб-консоли управления устройством. В случае настройки через UGMC настройка производится в одном из шаблонов в разделе **Настройки**.
	Политика обновлений ПО позволяет задать обновление, доступное для установки на все или выборочные

Наименование	Описание
Шаг 2. Настроить политику обновления ПО для устройств LogAn.	управляемые устройства. Подробно об обновлениях ПО смотрите в разделе Обновление ПО LogAn.
Шаг 3. Настроить политику обновления библиотек для устройств LogAn.	Политика обновления библиотек позволяет выбрать необходимые обновления библиотек для установки на управляемое устройство. Подробно об обновлениях библиотек смотрите в разделе Обновление библиотек LogAn.

Обновление ПО LogAn

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

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

Порядок установки обновлений следующий:

Наименование	Описание
Шаг 1. Загрузить обновления в репозитарий UGMC.	Загрузить обновления можно либо из репозитария UserGate, либо импортировав файл обновления вручную. Для загрузки обновлений из репозитария необходимо в разделе **LogAn → Обновление ПО** нажать на кнопку **Выбрать онлайн-обновления**, отобразится список обновлений, доступных для скачивания из репозитария UserGate. Выделить необходимые обновления и нажать кнопку **Выбрать**. Выделенные обновления будут загружены в UGMC. Для загрузки вручную необходимо в разделе **LogAn → Обновление ПО** нажать на кнопку **Импортировать обновление**, выбрать файл с обновлением. Если для файла обновлений в самом обновлении не указаны название и версия обновления, то необходимо указать их в соответствующих полях. Кнопка **Сохранить** загрузит выбранное обновление в UGMC.

Наименование	Описание
Шаг 2. Утвердить обновление для всех или для конкретных устройств.	Для установки обновления на все устройства необходимо выбрать интересующее обновление и нажать на кнопку **Утвердить обновление**. Только одно обновление может быть утверждено для всех устройств. Если требуется установить данное обновление на группу устройств (например, для проведения тестирования), то необходимо в свойствах обновления указать управляемые устройства, для которых данное обновление будет доступно, и установить флаг **Утвердить обновление**.
Шаг 3. Провести установку обновления.	После утверждения обновление становится доступным для скачивания для всех или группы управляемых устройств. Управляемое устройство скачивает обновление в соответствии с расписанием проверки обновлений. После скачивания обновление может быть установлено администратором в консоли UGMC или в ручном режиме администратором управляемого устройства.

Обновление в репозитарии 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 репозитария UserGate.
Канал обновлений	Канал обновлений репозитария UserGate: • **Стабильные** — канал стабильных обновлений ПО. • **Бета** — канал экспериментальных обновлений.
Список изменений	

Наименование	Описание
	Ссылка на список изменений, содержащихся в данном обновлении.
Управляемые устройства	Список управляемых устройств, которым назначено данное обновление.
Добавлено	Дата добавления обновления в репозитарий UGMC и имя администратора, который выполнил добавление.
Утверждено	Дата утверждения обновления и имя администратора, который выполнил утверждение.

Обновление библиотек LogAn

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

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

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

Обновление библиотек в репозитарии UGMC имеет следующие свойства:

Наименование	Описание
Название	Название обновления. Не доступно для изменения, содержится в коде изменения.
Описание	Произвольное описание обновления.
Скачивать	Режим скачивания новых версий. По умолчанию установлен режим **Автоматически** — UGMC автоматически проверяет наличие новых версий в репозитарии UserGate и скачивает

Наименование	Описание
	их. При выборе режима **Ручное** — UserGate не обновляет выбранную библиотек в автоматическом режиме.
Размер	Размер обновления.

УПРАВЛЕНИЕ КОНЕЧНЫМИ УСТРОЙСТВАМИ USERGATE CLIENT

Конечные управляемые устройства UserGate Client

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

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

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

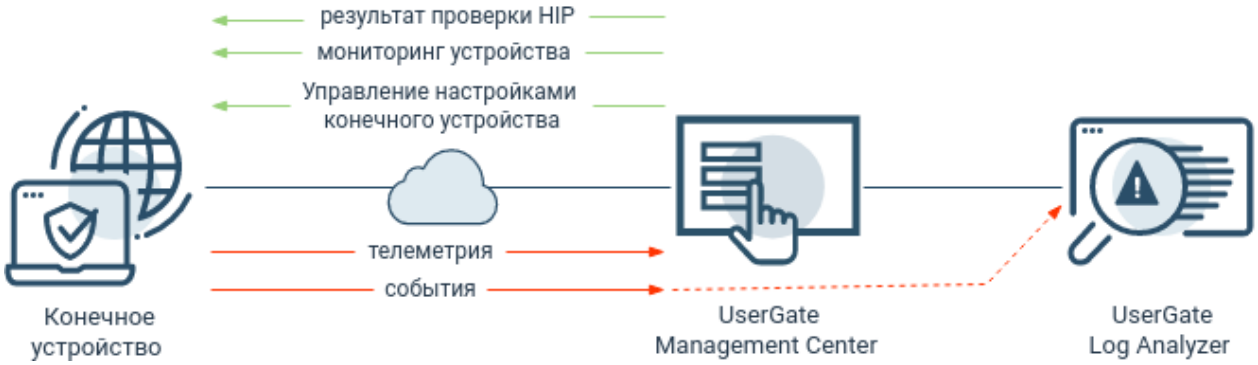
Управление конечными устройствами UserGate Client (Описание)

Централизованное управление устройствами UGC можно разделить на следующие этапы:

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

Работа UserGate Client в связке с UGMC

В случае подключения конечных устройств к UGMC администратор может централизованно управлять большим количеством конечных устройств, производить гибкую настройку политик безопасности с помощью правил межсетевого экран, производить проверку комплаенса конечного устройства.



Для регистрации конечного устройства на UGMC используется порт 4045; регистрация производится с использованием пин-кода. После регистрации конечному устройству присваивается уникальный идентификатор, который будет использован в дальнейшем для общения с сервером.

После регистрации конечное устройство запрашивает конфигурацию у UGMC каждые 10 секунд. UGMC отправляет на конечное устройство настройки межсетевого экрана и VPN, общие настройки шаблонов, библиотеки элементов, HIP объекты и профили, если они используются в правила межсетевого экрана. Отправка конфигурации на конечное устройство происходит в случае ее изменения на UGMC.

Конечное устройство отправляет на UGMC телеметрию (загруженность процессора, информацию о дисках, время работы системы и т.п.), а также конфигурацию, которая используется для проверки HIP: информация об уровне защищенности системы (статус антивируса, межсетевого экрана, автоматического обновления системы, BitLocker), список запущенных процессов и служб, список установленных обновлений, информация об установленном ПО. Конфигурация будет отправлена только в случае наличия изменений.

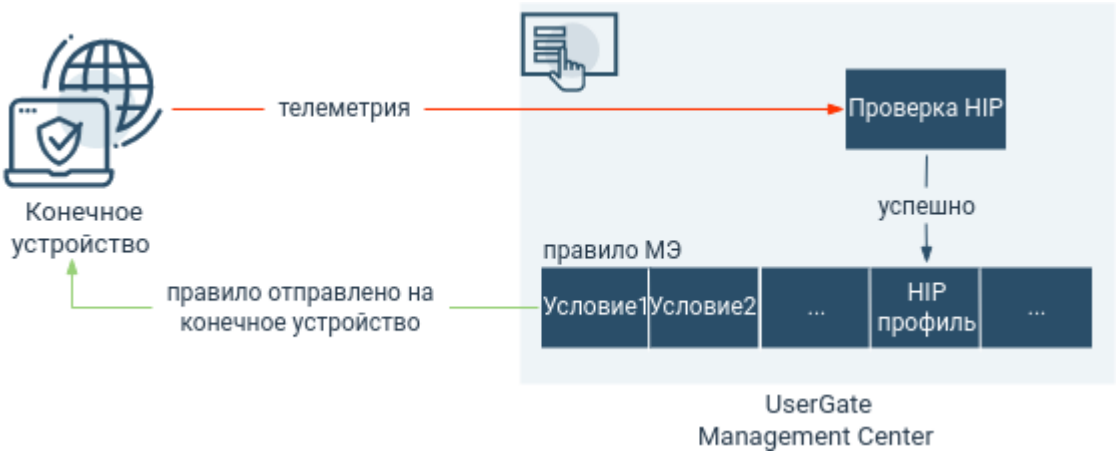
Также существует дополнительный блок информации, который передается на UGMC при открытии окна с информацией о конечном устройстве (рабочий стол **Управление областью** раздел, **Конечные устройства → Устройства**). В данном блоке передается информация о текущем времени и времени загрузки конечного устройства (с указанием часового пояса), подключенных к устройствах USB, элементах автозагрузки, точках восстановления, процессах, сервисах, производительности (данные о загруженности ЦП, памяти, размере и типе дисков, статус UserGate Client), установленных обновлениях системы и ключах реестра (передаются, в случае использования поиска в соответствующей вкладке).

В случае использования UserGate Log Analyzer: для каждого и активного сервера LogAn открывается порт из диапазона 22000 – 22711. На данном порту принимается телеметрия, журналы Windows и другие данные о безопасности

конечных устройств, которые передаются на LogAn транзитом через UGMC. Полученные данные могут быть использованы для анализа и автоматического реагирования на угрозы безопасности.

Проверка HIP на UGMC

В UserGate реализована возможность проверки конечного устройства на соответствие требованиям безопасности (комплаенса). Проверка работает на основе профилей HIP (подробнее читайте в соответствующем разделе руководства администратора) и производится по следующей схеме:



Конечное устройство отправляет на UGMC:

- информацию о пользователях;
- данные о системе (версия, издание, netbios имя);
- список запущенных процессов;
- список запущенных служб;
- список установленного программного обеспечения (название, вендор, версия);
- ключи реестра;
- список обновлений системы;
- элементы автозагрузки;
- информацию о защищенности системы (антивирус, межсетевой экран, BitLocker и т.п.);
- информацию о точках восстановления системы.

> **Примечание**
> **Если HIP профиль не указан, то правило МЭ применяется на все конечные устройства.**

> **Примечание**
> **Если ОС конечного устройства возвращает некорректную задвоенную информацию об установленном одинаковом антивирусном ПО с различными статусами (один со статусом включен, другой — выключен), то при проверке HIP учитывается наихудший случай (антивирус выключен). Статус обновления баз антивирусного ПО проверяется только для включенного антивируса.**

Для проверки на соответствие требованиям безопасности используются только профили HIP, указанные в правилах межсетевого экрана в качестве одного из условий фильтрации. Результат проверки будет отображен в консоли UGMC на рабочем столе **Управление областью** в разделе **Конечные устройства → Устройства**. В случае успешной проверки правило будет отправлено на конечное устройство.

Шаблоны управляемых устройств UGC

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

После создания шаблона можно производить настройку его параметров. Для этого необходимо перейти на рабочий стол **Конечные устройства — конфигурация** и в выпадающем меню выбрать необходимый шаблон.

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

1. Если значение настройки не определено в шаблоне, то ничего передаваться в управляемое устройство UGC не будет. В данном случае будет использована настройка по умолчанию.

2. Библиотеки, например, такие как IP-адреса, списки URL, списки типов контента MIME, приложения и другие, по умолчанию не содержат никакого

контента в UGMC. Для использования библиотек в политиках фильтрации, необходимо предварительно добавить элементы в эти библиотеки.

3. Рекомендуется создавать отдельные шаблоны для разных групп настроек, это позволит избежать конфликтов настроек при объединении шаблонов в группы шаблонов и упростит понимание результирующей настройки, которая будет применена к управляемому устройству UGC. Например, шаблон правил межсетевого экрана, шаблон правил контентной фильтрации, шаблон библиотек и т.д.

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

Настройки

Определяют общие настройки параметров управляемого устройства UGC:

Наименование	Описание
Настройки инсталляции UserGate Client	Настройки инсталляции ПО UserGate Client: • **Собирать информацию о конечном устройстве**: сбор информации о конечном устройстве (IP-адрес, время последнего подключения к UGMC, пользователь, имя компьютера, версия ОС, версия ПО UGC, загрузка CPU и памяти, запущенные процессы, сервисы и т.д.). Значение по умолчанию: **Да**. Если отключить данную функцию, то UGMC будет получать информацию только об IP-адресе, имени конечного устройства, версии ПО UGC и ОС Windows, текущем времени и времени загрузки устройства, загрузке CPU и памяти. **Важно!** Отключение сбора информации о конечном устройстве влияет на работу профилей HIP. • **Разрешить сетевой доступ при остановленном приложении**: настройка сетевого доступа при остановленном ПО UserGate Client. Значение по умолчанию: **Да**. • **Разрешить отключение межсетевого экрана**: разрешение пользователю самостоятельно, используя графический интерфейс, отключать контентную фильтрацию на конечном устройстве: ◦ **Нет** — не разрешать самостоятельно отключать контентную фильтрацию. ◦ **Да** — разрешить самостоятельно отключать контентную фильтрацию.

Наименование	Описание
	◦ **Разрешить с использованием кода** — разрешить самостоятельно отключать контентную фильтрацию с использованием кода. Для разрешения пользователю самостоятельно отключать контентную фильтрацию необходимо указать/сгенерировать код, который клиент должен ввести на конечном устройстве; также можно указать срок действия кода. При разрешении пользователю отключать фильтрацию самостоятельно можно указать количество разрешённых отключений и/или время, на которое фильтрация будет отключена. Значение по умолчанию: **Да** (отключение фильтрации на 10 минут без использования кода). **Важно!** В случае использования счётчика количества отключений: если внести изменения в настройки разрешения отключения межсетевого экрана, то счётчик на конечном устройстве обнулится. • **Разрешить удалять приложение UserGate Client**: возможность удаления ПО UserGate Client. При использовании опции **Разрешить с использованием кода** необходимо указать/сгенерировать код, который необходимо ввести клиенту при удалении ПО. Значение по умолчанию: **Да**. **Важно!** **Настройки не будут применены, если не включена синхронизация (флаг *Синхронизировать*). В случае отсутствия флага будет использовано значение по умолчанию.**
Оповещения	Настройка оповещений: • **Показывать иконку в трее**: отображение иконки UserGate Client в области уведомлений на панели задач. • **Показывать тултипы оповещений**: включение/отключение отправки оповещений на конечное устройство. Если оповещения отключены, то уведомления не будут отображаться на конечном устройстве вне зависимости от настроек отдельных уведомлений (о

Наименование	Описание
	добавлении/удалении устройства из карантина, блокировке ресурса). • **Сообщение о добавлении устройства в карантин**: отправка уведомлений о блокировке устройства. Для настройки уведомления необходимо указать текст сообщения и тип. Уведомление будет отображено в виде всплывающего окна. • **Сообщение об удалении устройства из карантина**: отправка уведомлений о разблокировке устройства. Для настройки уведомления необходимо указать текст сообщения и тип. Уведомление будет отображено в виде всплывающего окна. • **Сообщение о блокировке ресурса**: отправка уведомления при блокировке перехода по адресу электронного ресурса. Для настройки уведомления необходимо указать текст сообщения и тип. Уведомление будет отображено в виде всплывающего окна. **Важно!** **Настройки не будут применены, если не включена синхронизация (флаг *Синхронизировать*). В случае отсутствия флага будет использовано значение по умолчанию.**
Настройки устройства LogAn	Установка для конечного устройства сервера LogAn, на которое устройство будет отсылать информацию о событиях. Сервер LogAn должен быть предварительно зарегистрирован в UGMC. **Важно!** **Настройки не будут применены, если не включена синхронизация (флаг *Синхронизировать*). В случае отсутствия флага будет использовано значение по умолчанию.**

Настройка VPN

Данный раздел позволяет настроить профили безопасности VPN, которые определяют такие настройки, как общий ключ шифрования (Pre-shared key), протокол соединения и алгоритмы для шифрования и аутентификации. Также реализована поддержка мультифакторной аутентификации пользователей, где в качестве второго фактора может быть использован одноразовый код TOTP. Настройки VPN передаются на управляемое устройство UserGate Client; пользователь сможет выбрать необходимый VPN-сервер для подключения в начальном окне графического интерфейса.

Примечание

Настройка VPN-соединений возможна только для конечных устройств с версией ОС Windows 10 и выше. После разрыва соединения попытки подключения будут производиться в течение 40 секунд. Если за это время соединение не будет установлено, то у пользователя отобразится окно для выбора VPN-сервера.

Для настройки профиля VPN-сервера необходимо указать:

Наименование	Описание
Включено	Включение/отключение правила.
Название	Название профиля безопасности для подключения к серверу VPN.
Описание	Описание профиля.
VPN-адрес	Имя хоста (FQDN) или IP-адрес VPN-сервера. **Важно!** Необходимо учитывать, что при указании адреса VPN-сервера в виде FQDN перебор IP-адресов не предусмотрен. В случае, если DNS-сервер вернет несколько адресов, будет выполнена попытка подключения к первому адресу в списке.
Протокол	VPN-протоколы для создания туннеля: • **IPSec L2TP**. Для создания туннелей используется протокол Layer 2 Tunnelling Protocol (L2TP), а для защиты передаваемых данных — протокол IPSec. • **IKEv2 с сертификатом**. Для создания защищенного канала будет использоваться протокол IKEv2, а для взаимной проверки подлинности сервера и клиента — сертификаты.

Наименование	Описание
	Важно! При генерации клиентского сертификата обязательно должно быть указано поле *CN* — идентификатор пользователя, которому этот сертификат предназначается. • **IKEv2 с именем и паролем**. Для создания защищенного канала будет использоваться протокол IKEv2, а для проверки клиента — логин и пароль (EAP-MSCHAP v2). Данный метод доступен только для пользователей доменного RADIUS-сервера.
Режим IKE	Режим IKE (указать при выборе протокола **IPSec L2TP**): **Основной** или **Агрессивный**. Разница между режимами: в агрессивном режиме используется меньшее количество пакетов, что позволяет достичь более быстрого установления соединения. Агрессивный режим не передает некоторые параметры согласования, что требует предварительной идентичной настройки их на точках подключения. **Основной режим**. В основном режиме происходит обмен шестью сообщениями. Во время первого обмена (сообщения 1 и 2) происходит согласование алгоритмов шифрования и аутентификации. Второй обмен (сообщения 3 и 4) предназначен для обмена ключами Диффи-Хеллмана (DH). После второго обмена служба IKE на каждом из устройств создаёт основной ключ, который будет использоваться для защиты проверки подлинности. Третий обмен (сообщения 5 и 6) предусматривает аутентификацию инициатора соединения и получателя (проверка подлинности); информация защищена алгоритмом шифрования, установленным ранее. **Агрессивный режим**. В агрессивном режиме происходит 2 обмена, всего 3 сообщения. В первом сообщении инициатор передаёт информацию, соответствующую сообщениям 1 и 3 основного режима, т.е. информацию об алгоритмах шифрования и аутентификации и ключ DH. Второе сообщение предназначено для передачи получателем информации, соответствующей сообщениям 2 и 4 основного режима, а также аутентификации получателя. Третье сообщение аутентифицирует инициатора и подтверждает обмен.
Общий ключ	Строка, которая должна совпадать на сервере и клиенте для успешного подключения. Указывается для протокола **IPSec L2TP**.
Фаза 1	Во время первой фазы происходит согласование защиты IKE. Аутентификация происходит на основе общего ключа в

Наименование	Описание
	режиме, выбранном ранее. Необходимо указать следующие параметры: • **Время жизни ключа** – по истечению данного времени происходят повторные аутентификация и согласование настроек первой фазы. • **Интервал проверки dead peer detection** – для проверки состояния и доступности соседних устройств используется механизм Dead Peer Detection (DPD). DPD периодически отправляет сообщения R-U-THERE для проверки доступности IPsec-соседа. Минимальный интервал проверки: 10 секунд; значение 0 отключает проверку. • **Неудачных попыток** – максимальное количество запросов обнаружения недоступных IPsec-соседей, которое необходимо отправить до того, как IPsec-сосед будет признан недоступным. • **Diffie-Hellman группы** – выбор группы Диффи-Хеллмана, которая будет использоваться для обмена ключами. Сам ключ не передаётся, а передаются общие сведения, необходимые алгоритму определения ключа DH для создания общего секретного ключа. Чем больше номер группы Диффи-Хеллмана, тем больше бит используется для обеспечения надёжности ключа. • **Безопасность** – алгоритмы аутентификации и шифрования используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх/вниз или используйте кнопки **Выше**/**Ниже**.

Наименование	Описание
Фаза 2	Во второй фазе осуществляется выбор способа защиты IPsec подключения. Необходимо указать: • **Время жизни ключа**. По истечению данного времени узлы должны сменить ключ шифрования. Время жизни, заданное во второй фазе, меньше, чем у первой фазы, т.к. ключ необходимо менять чаще. • **Максимальный размер данных, шифруемых одним ключом**. Время жизни ключа может быть задано в байтах. Если заданы оба значения (**Время жизни ключа** и **Максимальный размер данных, шифруемых одним ключом**), то счётчик, первый достигнувший лимита, запустит пересоздание ключей сессии. • **Безопасность** – алгоритмы аутентификации и шифрования используются в порядке, котором они отображены. Для изменения порядка перетащите необходимую пару вверх/вниз или используйте кнопки **Выше**/**Ниже**.

В случае использования многофакторной аутентификации через одноразовые коды TOTP, токен вводится в отдельном окне, которое будет отображено на конечном устройстве после выбора сертификата или ввода логина/пароля.

Примечание

Использование многофакторной аутентификации через одноразовые коды TOTP доступно только при установке соединения по протоколу IKEv2.

Примечание

Для пользователей доменного RADIUS-сервера, в случае проведения первоначальной инициализации TOTP-устройства по URL, на сервере сетевых политик необходимо дополнительно разрешить проверку подлинности открытым текстом (PAP).

Политики сети

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

С помощью правил межсетевого экрана администратор может разрешить или запретить любой тип сетевого трафика приходящий или исходящий с

управляемого устройства UGC. В качестве условий правила могут выступать IP-адреса источника/назначения, пользователи и группы пользователей, сервисы, приложения, списки и категории URL, типы контента, профили HIP и расписание работы правил.

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 Наверх/Вниз, Выше/Ниже или перетаскивание мышью для изменения порядка применения правил.

Примечание

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

Примечание

Если не создано ни одного правила, то любой трафик с/на управляемого устройства 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.

Наименование	Описание
Описание	Описание правила.
Область применения	Указывает область применения данного правила на управляемом устройстве UGC. Возможны следующие варианты: • **Внутри периметра** — правило будет применено, если компьютер с установленным ПО UGC находится в доменной сети. • **Снаружи периметра** — правило будет применено, если компьютер с установленным ПО UGC находится не в доменной сети. • **Везде** — правило будет применено всегда независимо от местоположения компьютера пользователя.
Действие	Действие правила: • **Запретить** — блокирует трафик. • **Разрешить** — разрешает трафик. • **Перенаправить в прокси** — перенаправляет трафик, соответствующий условиям правила в указанный прокси сервер. При выборе действия указание параметров **Списки URL, Категории, Типы контента** недоступно.
Журналирование	Определяет, записывать ли срабатывание данного правила в журнал на сервере LogAn.
Прокси-сервер	Выбор прокси-сервера, при указании действия **Перенаправить в прокси.** Прокси сервер указывается через выбор профиля прокси сервера.
Пользователи	Указание пользователей или групп пользователей LDAP, для которых будет применено данное правило межсетевого экрана. Для указания пользователей необходим корректно настроенный LDAP-коннектор. Подробнее читайте в разделе Каталоги пользователей.
Источник	Списки IP-адресов источника трафика. **Важно!** Не рекомендуется создание правил, одновременно содержащих условия фильтрации трафика по адресу источника и URL/категории URL/типу контента, — возможна некорректная работа таких правил. Список может быть создан предварительно в разделе **Библиотеки → IP-адреса** или при настройке правила. Более подробно об списках IP-адресов читайте в главе IP-адреса.

Наименование	Описание
Назначение	Списки IP-адресов назначения трафика. Список может быть создан предварительно в разделе **Библиотеки → IP-адреса** или при настройке правила. Более подробно об списках IP-адресов читайте в главе IP-адреса.
Сервис	Тип сервиса, например, HTTP, HTTPS, или группа сервисов. Сервисы или группы сервисов могут быть предварительно созданы в разделах **Библиотеки → Сервисы** и разделе **Библиотеки → Группы сервисов**, соответственно, а также при настройке правил межсетевого экрана. Более подробно об сервисах читайте в главе Сервисы.
Приложения	Список приложений, для которых применяется данное правило. Приложение может быть создано предварительно в разделе **Библиотеки → Приложения** или при настройке правила межсетевого экрана. Более подробно об приложениях читайте в главе Приложения.
Списки URL	Списки адресов URL. Списки URL можно создать в разделе **Библиотеки → Списки URL** или в свойствах правил межсетевого экрана. Более подробно о работе со списками URL читайте в главе Списки URL. **Важно!** При использовании списков URL в качестве условий фильтрации трафика указание сервисов обязательно.
Категории сайтов	Списки категорий UserGate URL filtering 4.0. В руках администратора находится управление доступом к таким категориям, как порнография, вредоносные сайты, онлайн-казино, игровые и развлекательные сайты, социальные сети и многие другие. Также для добавления доступны группы URL-категорий, которые могут быть созданы в разделе **Библиотеки → Категории URL** или при настройке правил. Более подробно об категориях читайте в главе Категории URL. **Важно!** При использовании категорий сайтов как одного из условий правила межсетевого экрана указание сервисов обязательно.
Типы контента	Списки типов контента. Предусмотрена возможность управления видеоконтентом, аудио контентом, изображениями, исполняемыми файлами и другими типами. Администраторы также могут создавать собственные группы типов контента. Создание доступно в разделе **Библиотеки → Типы контента**, а также в свойствах правила межсетевого экрана. Более

Наименование	Описание
	подробно о работе с MIME-типами читайте в главе Типы контента. **Важно!** При использовании типов контента в качестве одного из условий правила межсетевого экрана указание сервисов обязательно.
Время	Время, когда правило активно. Администратор может добавить необходимые ему временные интервалы в разделе Календари или при настройке правила. **Важно!** Расписание работает в часовом поясе конечного устройства с установленным ПО UserGate Client.
HIP профили	Список профилей HIP. Правило межсетевого экрана будет применено только в случае соответствия конечного устройства объектам HIP, указанным в профиле. Подробнее о профилях и объектах HIP читайте в соответствующих разделах HIP профили и Объекты HIP. **Важно!** Для осуществления фильтрации трафика по результатам проверки комплаенса необходимо наличие лицензии на модуль **Контроль доступа в сеть на уровне хоста**.
Конечные устройства	Конкретные конечные устройства, к которым будет применено данное правило. Если ничего не указано, то данное правило применяется ко всем устройствам, к которым данный шаблон применен.

Библиотеки элементов

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

Сервисы

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

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

IP-адреса

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

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

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

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

Наименование	Описание
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**.

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

Группы приложений

Элемент библиотеки **Группы приложений** 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.

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

Списки URL

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

Для фильтрации с помощью списков URL необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать список URL.	В панели **Списки URL** нажать на кнопку **Добавить**, задать: • Название списка; • Описание (опционально),

Наименование	Описание
	• Тип списка: **Локальный** или **Обновляемый**; • Чувствительность к регистру; ◦ **Чувствительный к регистру** — список URL адресов, чувствительных к регистру букв в адресе. ◦ **Нечувствительный к регистру** — список URL адресов, нечувствительных к регистру букв в адресе. Использование списка этой категории исключает необходимость перебора вариантов написания одного и того же выражения с буквами в различных регистрах. ◦ **Домен** — список адресов доменов для использования в правилах DNS-фильтрации. • URL обновления, если список обновляемый.
Шаг 2. Добавить необходимые записи в новый список.	Добавить записи URL в новый список. В списках можно использовать специальные символы «^», «$» и «*»: • «*» — любое количество любых символов. • «^» — начало строки. • «$» — конец строки. Символы «?» и «#» не могут быть использованы.
Шаг 3. Создать правило межсетевого экрана конечного устройства, содержащее один или несколько списков.	Смотрите раздел Политики сети.

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

^http://domain.com/exacturl$

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

^http://domain.com/exacturl/

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

domain.com

Пример интерпретации URL-записей:

Пример записи	Обработка HTTP-запросов
yahoo.com или *yahoo.com*	Блокируется весь домен и все URL этого домена и домены 3 уровня, например: http://sport.yahoo.com http://mail.yahoo.com https://mail.yahoo.com http://sport.yahoo.com/123
^mail.yahoo.com$	Заблокированы только http://mail.yahoo.com https://mail.yahoo.com
^mail.yahoo.com/$	Ничего не заблокировано, так как последний символ слэш определяет URL, но не указаны «https» или «http»
^http://finance.yahoo.com/personal-finance/$	Заблокирован только http://finance.yahoo.com/personal-finance/
^yahoo.com/12345/	Заблокированы http://yahoo.com/12345/whatever/ https://yahoo.com/12345/whatever/

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

Наименование	Описание
Шаг 1. Создать файл с необходимым списком URL.	Создать текстовый файл **list.txt** со списком URL в следующем формате: *www.site1.com/url1* *www.site2.com/url2* ... *www.siteend.com/urlN*
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем **list.zip**.
Шаг 3. Создать файл с версией списка.	Создать файл **version.txt**, внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте **list.zip** и **version.txt**, чтобы они были доступны для скачивания.

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

Категории URL

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

Для добавления новой группы категорий необходимо выполнить следующие шаги:

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

Типы контента

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

Для фильтрации по типу контента необходимо выполнить следующие действия:

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

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

Наименование	Описание
Шаг 1. Создать файл с необходимыми типами контента.	Создать файл **list.txt** со списком типов контента.

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

Календари

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

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

Группы шаблонов управляемых устройств UGC

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

Добавление устройств UGC под управление UGMC

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

1. Добавление управляемых устройств UGC по одному устройству. Данный вариант подходит для компаний с небольшим количеством управляемых устройств UGC.

2. Массовое добавление устройств. Вариант для компаний с большим количеством устройств.

Процесс единичного добавления устройств

Для добавления одного управляемого устройства UGC необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Обеспечить доступ от управляемого устройства UGC до UGMC.	На сервере UGMC необходимо разрешить сервис **Контроль конечных устройств** на зоне, к интерфейсу которой подключаются управляемое устройство. Сервер UGMC слушает подключения от управляемых устройств UGC на портах TCP 4045 и 9712. Передача данных между сервером UGMC и управляемыми устройствами осуществляется по зашифрованному каналу.
Шаг 2. Создать запись для управляемого устройства UGC в UGMC.	В консоли управления областью в разделе **Конечные устройства → Устройства** нажать кнопку **Добавить** и указать необходимые настройки.
Шаг 3. Отобразить уникальный код созданного устройства.	В консоли управления областью в разделе **Конечные устройства → Устройства** выбрать запись, нажать кнопку **По казать уникальный код устройства** и зафиксировать его. Данный код потребуется указать при инсталляции ПО UGC на конкретное устройство (компьютер) пользователя.
Шаг 4. Установить ПО UGC на конкретное устройство (компьютер) пользователя.	Установить ПО на конечный компьютер пользователя. В мастере установки указать IP-адрес UGMC и уникальный код устройства, созданный на предыдущем шаге. Подробно об установке ПО на конечное устройство смотрите в разделе Установка ПО UserGate Client.

При создании записи управляемого устройства UGC необходимо указать следующие параметры:

Наименование	Описание
Включено	Включение объекта управляемого устройства UGC.
Лицензирован	Лицензирование конечного устройства: если флаг поставлен, то он использует одну лицензию. В случае отсутствия лицензии конечное устройство не сможет подключиться к UGMC.

Наименование	Описание
	Если флаг будет убран после регистрации устройства на UGMC, то: • правила межсетевого экрана, полученные от MC ранее, продолжают работать; • подключение по VPN с настройками, полученными ранее от MC доступно; • новые настройки конечное устройство от MC не получает.
Название	Название для управляемого устройства UGC. Можно вводить произвольное название.
Описание	Описание управляемого устройства UGC.
Группы шаблонов	Группа шаблонов, настройки которой следует применить к этому управляемому устройству UGC. Настройки (политики) применятся после синхронизации с UGMC.
Синхронизация	Режим синхронизации: отключено, автоматическая или ручная синхронизация.

Процесс массового добавления устройств

Рассмотрим процесс массового добавления управляемых устройств UGC:

Наименование	Описание
Шаг 1. Обеспечить доступ от управляемых устройств UGC до UGMC.	На сервере UGMC необходимо разрешить сервис **Контроль конечных устройств** на зоне, к интерфейсу которой подключаются управляемые устройства. Сервер UGMC слушает подключения от управляемых устройств UGC на портах TCP 4045 и 9712. Передача данных между сервером UGMC и управляемыми устройствами осуществляется по зашифрованному каналу.
Шаг 2. Создать код для группы конечных устройств.	В консоли управления областью в разделе **Конечные устройства → Коды для конечных устройств** нажать кнопку **Добавить** и указать необходимые параметры.
Шаг 3. Отобразить уникальный код для созданной группы устройств.	В консоли управления областью в разделе **Конечные устройства → Коды для конечных устройств** нажать кнопку **Уникальный код конечного устройства** и зафиксировать его. Данный код потребуется указать при инсталляции ПО UGC на группу устройств.

Наименование	Описание
Шаг 4. Установить ПО UGC на устройства пользователей.	Установить ПО на конечные компьютеры пользователей. В мастере установки или в административном шаблоне Active Directory указать уникальный код группы устройств, созданный на предыдущем шаге и IP-адрес интерфейса UGMC, к которому будут подключены управляемые устройства. После завершения установки ПО автоматически создается запись для каждого устройства в UGMC в разделе **Конечные устройства → Устройства,** и каждое конечное устройство получает все настройки, указанные в примененной к нему группе шаблонов. Подробно об установке ПО на конечное устройство смотрите в разделе Установка ПО UserGate Client.

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

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

Примечание

После регистрации конечного устройства с использованием кода индивидуально для каждого устройства можно изменить используемую группу шаблонов. В случае возникновения проблем, переустановки ПО UserGate Client и необходимости повторной регистрации на UGMC, необходимо использовать процедуру переподключения устройства (раздел *Конечные устройства → Устройства* кнопка *Переподключить устройство*). Если повторная регистрация будет произведена с использованием общего кода, то на UGMC произойдёт создание новой записи о регистрации конечного устройства с привязкой устройства к группе шаблонов, указанной в настройках кода; информация о предыдущей регистрации также будет сохранена.

Управление устройством UGC из консоли UGMC

После добавления управляемое устройство UGC отобразится в веб-консоли управления областью в разделе **Конечные устройства → Устройства**.

Раздел **Конечные устройства → Устройства** позволяет совершать следующие действия над управляемыми устройствами:

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

- Переподключение устройства, т.е. повторная регистрация конечного устройства на UGMC, код для подключения будет сгенерирован повторно.
- Запуск процесса принудительной синхронизации.
- Отображение настроек, применимых к данному конечному устройству (кнопка **Отобразить**).

Данный раздел также позволяет просмотреть следующие параметры каждого конечного устройства:

Наименование	Описание
Название	Отображено название конечного устройства.
Версия	Отображена версия UserGate Client, установленная на устройстве.
Последнее подключение	Показаны дата и время последнего подключения конечного устройства.
Телеметрия	Представлена следующая информация: • IP-адрес конечного устройства, который используется для выхода в Интернет. • Netbios имя. • Время последнего подключения управляемого устройства UGC к UGMC. • Пользователь, с учётной записи которого был совершён вход в систему. • Имя компьютера в локальной сети. • Версия ОС, установленная на конечном устройстве. • Версия UserGate Client, установленная на устройстве. • Загрузка CPU клиентом UserGate показывает на сколько загружен центральный процессор конечного устройства. • Загрузка памяти клиентом UserGate — количество памяти, используемое UserGate Client. • Загрузка физической памяти отображает загруженность оперативной памяти на конечном устройстве. • Загрузка виртуальной памяти показывает степень загруженности виртуальной памяти на конечном устройстве.

Наименование	Описание
Мониторинг конечных устройств	Показана подробная информация о конечном устройстве. Более подробно данный пункт будет рассмотрен ниже. В случае возникновения ошибки синхронизации конфигурации конечного устройства доступен просмотр отчёта (нажать **Показать отчёт**), в котором отображены время последнего подключения к управляемому устройству, название правила, тип объекта, ставшего причиной сбоя синхронизации, и описание ошибки. При возникновении ошибки применение правил межсетевого экрана к конечному устройству не изменяется (т.е. действуют правила межсетевого экрана, которые были синхронизированы до появления ошибки), доступны управление сервисами и процессами и выполнение запросов в реестр.
Группа шаблонов конечных устройств	Отображены группы шаблонов, применённые к управляемым устройствам UGC. Создание групп шаблонов было рассмотрено в главе Группы шаблонов управляемых устройств UGC.
HIP профили	Представлен список профилей HIP. Профиль HIP будет отображен в списке, только в случае его применения в правилах межсетевого экрана. О соответствии или несоответствии конечного устройства профилю HIP говорит цветовая индикация: • Зелёный — конечное устройство соответствует профилю. • Красный — конечное устройство не соответствует профилю. В случае несоответствия к просмотру доступен отчёт (нажмите **Посмотреть отчёт**), содержащий информацию о времени последнего получения данных, название профиля и объекта HIP, тип и несоответствующий элемент объекта. Подробнее читайте в разделе HIP профили.
Устройства LogAn	Название сервера UserGate Log Analyzer, на который конечное устройство отправляет журналы диагностики и телеметрию.
Время последней синхронизации	Отображён режим, а также дата и время последней синхронизации конечного устройства и UGMC. Работа возможна в одном из следующих режимов: • **Автоматическая синхронизация** — настройки применяются к устройству автоматически. При изменении любой настройки из любого шаблона, включенного в группу шаблонов, примененную к

Наименование	Описание
	управляемому устройству, 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 единовременно отослать их на устройство. В этом случае необходимо отключить синхронизацию, произвести необходимые изменения в шаблонах, после чего включить синхронизацию в режим Ручная синхронизация.

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

Наименование	Описание
Общие	Представлена общая информация об устройстве (имя компьютера, версия и тип ОС, версия ПО UserGate Client, IP-адрес, время загрузки системы и текущее время на устройстве в часовом поясе, настроенном на конечном устройстве) и пользователе, под учётной записью которого был совершён вход в систему (фотография, имя и статус пользователя, тип аккаунта (локальный или доменный), телефон и электронная почта). **Важно!** Для отображения полной информации о доменных пользователях, необходимо подключить LDAP-коннектор в разделе **Центр управления → Каталоги пользователей**.
Производительность	Представлена следующая информация: • Использование процессора, т.е. степень загруженности центрального процессора. • Степень загрузки центрального процессора конечного устройства процессом UserGate Client. • Информация о виртуальной памяти конечного устройства. • Информация о физической памяти — оперативной памяти. • Загрузка памяти клиентом UserGate. • Информация о дисках компьютера: размер диска, тип и производительность. • Статус управляемых устройств UGC показывает статус UserGate Client: онлайн/офлайн (доступность конечного устройства) или отключено (UserGate Client

Наименование	Описание
	был отключен с использованием UGMC кнопкой **Откл ючить**).
Безопасность	Представлена информация о безопасности конечного устройства: статус межсетевого экрана, антивируса, центров обновления и безопасности Windows, а также информация о шифровании дисков (BitLocker).
USB устройства	Отображена информация о подключённых устройствах USB: • **Идентификатор** устройства: пара идентификаторов VID/PID (Vendor ID/Product ID) и номер версии устройства. • **Название** устройства. • **USB класс**, например mouse, printer. • **Сервис**: драйверы, использующиеся для работы с устройством.
Элементы автозагрузки	Отображён список приложений, для которых настроен автоматический запуск при входе в систему.
Процессы	Показан список запущенных на конечном устройстве процессов. Нажатие кнопки **Завершить процесс** позволяет завершить процесс на конечном устройстве, используя UGMC.
Службы	Отображён список служб, запущенных/остановленных на конечном устройстве. Нажатие кнопок **Остановить службу**/**Запустить службу** позволяет выполнить попытку отключения/ включения службы на управляемых устройствах UGC с использованием UGMC.
Ключи реестра	Просмотр реестра. Доступны: • **HKEY_LOCAL_MACHINE**. • **HKEY_USERS**. Также доступен поиск по ключам реестра. Для этого необходимо нажать **Найти** (отображается при наведении указателя мыши на название каталога).
Программное обеспечение	Отображён список установленных на управляемом устройстве UGC ПО с указанием производителя и версии.

Наименование	Описание
Установленные обновления	Представлен список установленных обновлений на управляемом устройстве UGC с отображением соответствующего номера базы знаний Microsoft, информации о продукте, производителе и дате установки обновления.
Точки восстановления	Представлен список доступных точек восстановления и информация о них.

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

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

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

Установка ПО UserGate Client

Описание

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

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

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

Примечание

Чтобы отложить подключение к UserGate Management Center нажмите *Cancel*.

Примечение

После установки ПО UserGate Client компьютер будет перезагружен. Это необходимо для корректной работы приложения.

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

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

На конечном устройстве доступна следующая информация:

Наименование	Описание
General	Информация о конечном устройстве (пользователь, имя компьютера, IP-адрес для выхода в Интернет, версия ОС Windows) и VPN-подключении (статус подключения, VPN IP-адрес конечного устройства, количество байтов, переданных/полученных с момента подключения по VPN, время подключения). Также доступны следующие настройки: • чекбокс **Save login** — сохранение логина пользователя для подключения по VPN после перезагрузки конечного устройства; • чекбокс **Reconnect** — переподключение к VPN-серверу в случае обрыва связи. В случае потери соединения пользователю будет отображено начальное окно графического интерфейса. Если опция переподключения активна, то приложение будет производить повторные попытки подключения к

Наименование	Описание
	серверу; если функция отключена — будет отображено начальное окно с выбором сервера. Окно будет отображено в центре экрана (если активен чекбок **Popup in center**) или в месте его последнего расположения. • чекбокс **Popup in center** — отображение начального окна графического интерфейса в центре экрана в случае обрыва VPN-соединения.
Logs	Информация о: • **Logging level** — уровень детализации диагностики: ◦ **Off**: отключить ведение журнала диагностики. ◦ **Error**: журналировать только ошибки. ◦ **Warning**: журналировать только ошибки и предупреждения. ◦ **Info**: журналировать только ошибки, предупреждения и дополнительную информацию. ◦ **Debug**: максимум детализации. Журнал находится: %ALLUSERSPROFILE% \UserGate\UserGate Client\var\log\usergateclient\ug_client.txt. • **Tooltips history** — история оповещений. • **Export logs** — скачать журнал диагностики (после скачивания откроется каталог, в который был сохранён файл журнала диагностики).
Network	Просмотр следующей информации: • **IPCONFIG** — информация о всех сетевых адаптерах и текущей конфигурации TCP/IP. • **ROUTING** — записи локальной таблицы маршрутизации. • **SOCKETS** — список активных подключений (тип порта, адреса, состояние соединения, идентификатор процесса). Чтобы скопировать информацию нажмите **Copy**.
Policy	Просмотр информации о безопасности конечного устройства (статус межсетевого экрана, антивируса, центров обновления и безопасности Windows). Значение индикации: • **Жёлтый** — выключен.

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

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

Рекомендации по установке ПО UserGate Client

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

Примечание

Для возможности передачи журналов конечных на UserGate Log Analyzer на английском языке, необходимо установить языковой пакет *Английский (США)*; английский язык должен быть доступен для выбора в качестве языка интерфейса.

Примечание

Настройки, представленные в данном разделе, носят рекомендательный характер.

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

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

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

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

Примечание

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

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

Примечание

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

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

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

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

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

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

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

События в журнале Windows

В ПО UserGate Client реализована возможность отображения событий в журнале приложений Windows. На данный момент добавлено журналирование следующих событий:

- запуск и остановка сервиса (события **UG0101 Service started**, **UG0102 Service stopped**);
- подключение к МС и потеря связи (события **UG0201 MC connected**, **UG0202 MC connection lost**);
- подключение по VPN и завершение сессии, в том числе ошибки подключения — недоступность сервера, неправильно указанные данные (события **UG0301 VPN connected**, **UG0302 VPN disconnected**);
- получение конфигурации от Management Center (событие **UG0401 MC rules propagated**).

HIP профили

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

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

> **Примечание**
> **Для проверки соответствия требованиям безопасности (комплаенса) и работы правил фильтрации, в которых в качестве одного из условий указан профиль HIP, необходимо наличие лицензии на модуль *Контроль доступа в сеть на уровне хоста*.**

При создании профиля необходимо указать:

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

HIP объекты

Объекты HIP позволяют настроить критерии соответствия для конечных устройств и могут быть использованы в качестве одного из условий при настройке политик безопасности.

> **Примечание**
> **Для указания некоторых условий требуется наличие лицензированного модуля *Security Updates*, необходимого для скачивания обновлений библиотек.**

Для добавления объекта необходимо указать:

Наименование	Описание
Название	Название объекта HIP.
Описание	Описание объекта HIP (опционально).
Версия ОС	Версия операционной системы устройства пользователя. При использовании операторов **=** и **!=** необходимо указывать полную версию Windows.
Версия UserGate Client	Версия ПО UserGate Client.
Безопасность	Статусы компонентов безопасности конечного устройства: • Межсетевой экран; • Антивирус; • Автоматическое обновление; • Bitlocker.

Наименование	Описание
	Важно! BitLocker считается включенным, если он включен хотя бы на одном из дисков.
Продукты	Проверка соответствия программного обеспечения, установленного на конечном устройстве: • **Антивирус**. Проверка соответствия антивирусного ПО на устройстве пользователя. ◦ **Включено**: проверка статуса ПО; ◦ **Базы антивируса обновлены**: проверка актуальности баз (да, нет, не проверять) — производится только в случае, когда в предыдущем пункте включена проверка статуса антивируса в явном виде; ◦ **Версия** ПО; ◦ **Вендор**: производитель и название продукта. • **Межсетевой экран**. Проверка соответствия межсетевого экрана на конечном устройстве. При настройке необходимо указать: ◦ **Установлен**: проверка наличия установленного ПО; ◦ **Включено**: проверка статуса ПО (да, нет, не проверять); ◦ **Версия** ПО; ◦ **Вендор**: производитель и название продукта; • **Резервное копирование**. Проверка ПО для резервного копирования: ◦ **Установлен**: проверка наличия установленного ПО; ◦ **Версия** ПО; ◦ **Вендор**: производитель и название продукта. • **Шифрование диска**. Проверка установленных на конечном устройстве программ для шифрования диска: ◦ **Установлен**: проверка наличия установленного ПО; ◦ **Версия** ПО; ◦ **Вендор**: производитель и название продукта. • **DLP**. Проверка соответствия системы предотвращения утечек информации. ◦ **Установлен**: проверка наличия установленного ПО; ◦ **Версия** ПО; ◦ **Вендор**: производитель и название продукта.

Наименование	Описание
	• **Управление обновлениями.** Проверка актуальности обновления. ◦ **Установлен**: проверка наличия установленного ПО; ◦ **Версия** ПО; ◦ **Вендор**: производитель и название продукта.
Процессы	Проверка процессов, запущенных на конечном устройстве.
Запущенные службы	Проверка служб, запущенных на конечном устройстве.
Ключи реестра	Ключ реестра Microsoft Windows — каталог, в котором хранятся настройки и параметры операционной системы. Поддерживаются следующие типы параметров реестра: • **REG_SZ**: строка Unicode или ANSI с нулевым символом в конце. • **REG_BINARY**: двоичные данные в любой форме. • **REG_DWORD**: 32-разрядное число. Доступна проверка ключей следующих разделов реестра: • **HKEY_LOCAL_MACHINE** • **HKEY_USERS** **Важно!** Путь указывается с использованием обратного слэша (****), например, \HKEY_LOCAL_MACHINE, после которых через (****) указывается полный путь к параметру. Описание ключей реестра читайте в документации Microsoft (https://docs.microsoft.com/ru-ru/troubleshoot/developer/webapps/iis/general/use-registry-keys).
Установленные обновления	Проверка наличия указанного обновления на конечном устройстве. Необходимо указать номер статьи базы знаний Microsoft (KB), например, KB5013624.

Сбор и анализ данных с устройств UGC

LogAn является продуктом компании UserGate, входящим в состав экосистемы UserGate SUMMA. LogAn устанавливается на отдельном сервере, использование которого позволяет обеспечить высокую надёжность и хорошую масштабируемость системы. LogAn предоставляет возможность осуществления

сбора и анализа данных с различных устройств, мониторинга событий безопасности и создания отчётов. Для получения подробной информации об LogAn обратитесь к соответствующей документации.

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

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

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

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

Формирование данных журналов будет рассмотрено далее в разделах Журнал событий конечных устройств, Журнал правил конечных устройств, Приложения конечных устройств и Аппаратура конечных устройств.

Журнал событий конечных устройств

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

> **Примечание**
>
> **Для возможности передачи журналов конечных на LogAn на английском языке, необходимо установить языковой пакет *Английский (США)*; английский язык должен быть доступен для выбора в качестве языка интерфейса.**

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

В LogAn также представлен режим расширенного поиска для формирования сложных фильтров поиска с использованием специального языка запросов.

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

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

В журнале событий конечных устройств можно увидеть следующую информацию:

Наименование	Описание
Узел	Идентификатор конечного устройства или узла, на котором запущен сенсор.
Время	Время события. Отображается в часовом поясе, настроенном на LogAn.
Конечное устройство/ сенсор	Отображено имя компьютера.
Уровень лога	Отображен тип события: • **Аудит успеха** (Audit Success): событие журнала безопасности, которое происходит при успешном обращении к аудируемым ресурсам. • **Аудит отказа** (Audit Failure): событие журнала безопасности, которое происходит при неуспешном обращении к аудируемым ресурсам. • **Ошибка** (Error): событие указывает на существенные проблемы, которые могут стать причиной потери функциональности или данных. • **Сведения** (Information): информационные события, которые, как правило, не требуют внимания администратора. • **Предупреждение** (Warning): события указывают на проблемы, которые не требуют немедленного исправления, однако могут привести к ошибкам в будущем.

Наименование	Описание
Данные	Представлена подробная информация о событии.
Источник журнала событий	Показан источника журнала событий.
Категория журнала	Отображена категория лога, необходимая для упорядочивания событий. Данные берутся из Windows EventLog. Каждый источник может определять свои идентификаторы категорий. Относится к записям журнала событий конечных устройств.
Категория инцидента	Показана категория инцидента.
Имя компьютера	Показано полное имя компьютера.
Имя пользователя	Показано имя пользователя, с учётной записи которого был совершен вход в систему конечного устройства.
Код события лога	Представлен код, соответствующий определённому событию.
Идентификатор события лога	Отображён идентификатор события лога, который определяет первичный идентификатор события.
Тип события лога	Отображён тип события лога, соответствующий определённому уровню лога: • 1 — уровень лога: ошибка (error). • 2 — уровень лога: предупреждение (warning). • 3 — уровень лога: сведения (information). • 4 — уровень лога: аудит успеха (audit success). • 5 — уровень лога: аудит отказа (audit failure).
Строка вставки	Содержит данные блока EventData события Windows.
Файл журнала лога	Показано к какому типу файла журнала относится событие: • **Application** (файл журнала приложений): для событий приложений и служб. • **Security** (файл журнала безопасности): для событий системы аудита. • **System** (файл системного журнала): для событий драйверов устройств. • **CustomLog**: журнал содержит события, регистрируемые приложениями, которые создают пользовательский журнал. Использование

Наименование	Описание
	пользовательского журнала позволяет приложению управлять размером журнала или присоединять списки управления доступом в целях безопасности, не затрагивая другие приложения.

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

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

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

Журнал правил конечных устройств

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

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

В UserGate LogAn также представлен режим расширенного поиска для формирования сложных фильтров поиска с использованием специального языка запросов.

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

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

В журнале правил конечных устройств можно увидеть следующую информацию:

Наименование	Описание
Узел	Идентификатор конечного устройства.

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

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

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

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

Приложения конечных устройств

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

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

В UserGate LogAn также представлен режим расширенного поиска для формирования сложных фильтров поиска с использованием специального языка запросов.

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

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

В журнале приложений конечных устройств отображается следующая информация:

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

Наименование	Описание
Идентификатор процесса	Идентификатор процесса приложения (PID).
Пользователь	Пользователь, запустивший приложение.
Командная строка	Команда запуска приложения.

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

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

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

Аппаратура конечных устройств

Данный журнал содержит информацию об устройствах, подключаемых к управляемым устройствам UGC.

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

В LogAn также представлен режим расширенного поиска для формирования сложных фильтров поиска с использованием специального языка запросов.

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

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

Журнал аппаратуры конечных устройств содержит следующую информацию:

Наименование	Описание
Узел	Идентификатор конечного устройства.
Время	Дата и время регистрации события.
Конечное устройство	Название конечного устройства.

Наименование	Описание
Действие	Добавление или удаление устройства.
Устройство	Название устройства, которое было подключено или удалено.
Идентификатор устройства	Идентификатор подключенного/удалённого устройства.
Служба	Драйверы, использующиеся для работы с устройством.

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

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

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

ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ (CLI)

ОБЩИЕ ПОЛОЖЕНИЯ

Общие положения (описание)

В UserGate MC (UGMC) имеется возможность производить настройку устройства с помощью интерфейса командной строки CLI (Command Line Interface).

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

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

Внимание

Если устройство не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя *Admin*, в качестве пароля — *usergate*.

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

Наименование	Описание
Шаг 1. Подключить монитор и клавиатуру к устройству	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).

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

Наименование	Описание
Шаг 1. Подключиться к устройству	Используя специальный кабель для последовательного порта или переходник USB-Serial, подключить свой компьютер к устройству.
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).

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.

Наименование	Описание
Шаг 2. Запустить SSH-терминал	Запустить у себя на компьютере SSH-терминал, например, SSH для Linux или Putty для Windows. Указать в качестве адреса адрес UGMC, в качестве порта подключения - 2200, в качестве имени пользователя - имя пользователя правами корневого администратора UGMC (по умолчанию Admin/system). Для Linux команда на подключение должна выглядеть так: *ssh Admin/system@IPUserGateMC -p 2200*
Шаг 3. Войти в CLI	Войти в CLI, используя пароль пользователя, указанного на предыдущем шаге.

После успешной авторизации в CLI появится строка, ожидающая ввода команды (режим диагностики). Для просмотра текущих возможных значений или автодополнения необходимо использовать клавишу **Tab**. Доступны:

- **configure** — переход в режим конфигурации.
- **date** — просмотр текущих даты и времени на устройстве.
- **dig** — проверка записи DNS-домена.
- **exit** — выход из командной строки.
- **netcheck** — проверка доступности стороннего HTTP/HTTPS-сервера.
- **ping** — выполнение ping определённого хоста.
- **reboot** — перезагрузка устройства.
- **shutdown** — выключение устройства.
- **traceroute** — трассировка соединения до определённого хоста.

Данные команды доступны в режиме конфигурации; подробнее читайте в разделах Команды execute.

Для отмены ввода текущей команды используется сочетание **Ctrl + C**; для просмотра истории команд — ↑, ↓.

Все команды интерфейса командной строки имеют следующую структуру:

```
<action> <level> <filter> <configuration_info>
```

где:

<action>: действие, которое необходимо выполнить.

<level>: уровень конфигурации; уровни соответствуют разделам веб-интерфейса NGFW.

<filter>: идентификатор объекта, к которому происходит обращение.

<configuration_info>: значение параметров, которые необходимо применить к объекту <filter>.

CLI поддерживает ввод команды в несколько строк (многострочный ввод). Для перехода на новую строку необходимо добавить "\" в конце строки. Начиная со второй строки ввод "\" необязателен; чтобы завершить ввод необходимо ввести одну пустую строку.

КОМАНДЫ, ДОСТУПНЫЕ ДО ПЕРВИЧНОЙ ИНИЦИАЛИЗАЦИИ УЗЛА

Команды, доступные до первичной инициализации узла (Описание)

Если устройство не прошло первоначальную инициализацию, то в CLI доступны команды диагностики и мониторинга, а в режиме конфигурации — только команды настройки сети, т.е. настройка зон, интерфейсов, шлюзов и виртуальных маршрутизаторов, а также включение/отключение удалённого доступа к серверу radmin-emergency.

ПЕРВОНАЧАЛЬНАЯ ИНИЦИАЛИЗАЦИЯ

Первоначальная инициализация (Описание)

Первоначальную инициализацию устройства с использованием интерфейса командной строки можно произвести несколькими способами.

Установка как главного узла.

Для настройки устройства в качестве главного узла используется команда:

```
Admin/system@nodename# execute install master
```

Необходимо указать параметры:

Параметр	Описание
login	Задать логин администратора.
password	Задать пароль учётной записи администратора. Указание пароля также доступно при нажатии **Enter** после указания логина администратора; необходимо дважды ввести пароль учётной записи.

Установка как дополнительного узла кластера.

Для настройки узла в качестве дополнительного узла кластера используется команда:

```
Admin/system@nodename# execute install slave
```

Необходимо указать параметры:

Параметр	Описание
interface	Интерфейс для подключения к кластеру.
slave-ip	IP-адрес, который будет назначен на интерфейс, использующийся для подключения к кластеру.
gateway-address	IP-адрес шлюза. Шлюз необходимо указывать, если узлы кластера находятся в разных подсетях.
master-ip	IP-адрес мастер-сервера.

Параметр	Описание
master-secret	Секретный код, использующийся для подключения узла в кластер.
login	Логин системного администратора.
password	Пароль учётной записи администратора.

После первоначальной инициализации будет доступно полное управление из CLI.

РЕЖИМ КОНФИГУРАЦИИ

Режим конфигурации (описание)

Для перехода в режим конфигурации используется команда:

```
Admin/system@nodename> configure
```

После перехода в режим конфигурации командная строка будет выглядеть следующим образом:

```
Admin/system@nodename#
```

Для просмотра подсказки о текущих возможных значениях или для автодополнения команд необходимо нажать клавишу **Tab**. В подсказке могут использоваться следующие вспомогательные символы:

***** — обязательное поле в командах create и ряде других команд;

+ — необязательное/вариативное поле;

> — вложенное поле, после его введения предыдущий список полей становится недоступным, появляется новый список полей, которые можно ввести.

Например:

```
Admin/system@nodename# set network zone Trusted
* name                    Name
+ antispoof-enable        Enable/Disable IP spoofing protection
+ antispoof-negate        Enable/Disable Negate ip-spoof addresses
+ description             Description
+ enabled-services        Services list to enable
+ geoip                   IP spoofing protection by geo IP code
+ ip-list                 IP spoofing protection by IP list
> dos-protection-icmp     Confugure DoS protection per IP for ICMP
packets
> dos-protection-syn      Confugure DoS protection per IP for SYN
packets
> dos-protection-udp      Confugure DoS protection per IP for UDP
packets
> service-addresses       Access control service addresses
```

Общая структура команд в режиме конфигурации

Команды интерфейса командной строки имеют следующую структуру:

```
<action> <level> <filter> <configuration_info>
```

где:

<action> — действие, которое необходимо выполнить.

<level> — уровень конфигурации; уровни соответствуют разделам веб-интерфейса UGMC.

<filter> — идентификатор объекта, к которому происходит обращение.

<configuration_info> — значение параметров, которые необходимо применить к объекту <filter>.

Наименование	Описание
<action>	В режиме конфигурации доступны следующие действия: • **execute** — выполнение команд, которые не относятся к конфигурации UserGate (ping, date, traceroute и т.п.)

Наименование	Описание

	Команда доступна независимо от уровня конфигурации (<level>).
	• **set** — редактирование всех объектов, а также включение различных параметров, например, radmin.
	• **end** — переход на один уровень выше.
	• **show** — отображение текущих значений. Можно использовать на любом уровне конфигурации — будет отображено всё, что находится глубже текущего уровня.
	• **edit** — переход на какой-либо уровень конфигурации. Уровень конфигурации будет отображён под командной строкой.
	• **top** — возврат на самый верхний уровень конфигурации.
	• **exit** — выход из режима конфигурации.
	• **export** — экспорт конфигурации.
	• **import** — импорт конфигурации.
	• **create** — создание новых объектов.
	• **delete** — удаление объекта или параметра из списка параметров.
	
	Например, для просмотра информации о всех интерфейсах необходимо выполнить команду:
	
	`Admin/system@nodename# show network interface`
	
	С использованием следующей команды производится переход на уровень **network interface.** Текущий уровень будет отображён под командной строкой:
	
	`Admin/system@nodename# edit network interface`
	`Admin/system@nodename#`
	`Level: network interface`
	
	После перехода на уровень **network interface** для отображения всех интерфейсов используется команда show без указания уровня:
	
	`Admin/system@nodename# show`
	
	`adapter:`

Наименование	Описание
	port0 interface-name : port0 node-name : node1 zone : Management enabled : on ip-addresses : 192.168.56.3/24 iface-mode : dhcp ... ... Level: network interface Для возвращения с уровня **network interface** обратно на общий уровень режима конфигурации необходимо набрать команду **end**: Admin/system@nodename# end Level: network interface Admin/system@nodename# end Level: network Admin/system@nodename#
<level>	Уровни в командной строке повторяют веб-интерфейс системной консоли UGMC: • **network** — соответствует разделу веб-интерфейса **Сеть**. • **settings** — соответствует разделу веб-интерфейса **UserGate**. • **users** — соответствует разделу веб-интерфейса **Пользователи и устройства**. • **libraries** — соответствует разделу веб-интерфейса **Библиотеки**. • **monitoring** — соответствует разделу веб-интерфейса **Диагностика и мониторинг**. • **realms** — соответствует разделу веб-интерфейса **Управляемые области**.
<filter>	Идентификатор объекта, к которому происходит обращение. Идентификация происходит по имени объекта.

Наименование	Описание

	Если имеются объекты с одинаковыми именами или удобнее идентифицировать объект по другому параметру, то используются круглые скобки, в которых необходимо указать <configuration_info> (рассмотрено далее в разделе). В результате будет найден объект, для которого совпали все поля, указанные в круглых скобках.
	Например, необходимо вывести информацию об интерфейсе port0 на другом узле кластера. Если использовать команду:
	`Admin/system@nodename# show network interface adapter port0`
	то будет отображена информация об интерфейсе port0 текущего узла UGMCe. Чтобы отобразить информацию об интерфейсе port0 другого узла (например, с именем another_node), необходимо в скобках явно указать имя узла:
	`Admin/system@nodename# show network interface adapter ( node-name another_nodename interface port0 )`
	Важно! Круглые скобки должны быть отделены пробелами с обеих сторон.

<configuration_info>	Набор пар: параметр-аргумент. Параметр — имя поля, для которого нужно установить аргумент. Аргумент может быть одиночным или множественным. **Одиночный аргумент** — значение, соответствующее параметру. Если строка содержит пробелы, то необходимо использовать кавычки. Например, необходимо создать профиль аутентификации с именем New profile: `Admin/system@nodename# create users auth-profile name "New profile"` **Множественные аргументы** используются для установки множества значений какого-либо параметра; записываются в квадратных скобках и разделяются пробелами. Например, необходимо создать список IP-адресов в библиотеке элементов и добавить в него два IP-адреса 10.10.0.1 и 10.10.0.2:

Наименование	Описание
	`Admin/system@nodename# create libraries ip-list name testlist ips [ 10.10.0.1 10.10.0.2 ]` **Важно!** Квадратные скобки должны быть отделены пробелами с обеих сторон.

Команды execute

Команды имеет следующую структуру:

```
Admin/system@nodename# execute <command-name>
```

Доступны следующие команды:

Параметр	Описание
traceroute	Трассировка соединения до определённого хоста. Доступны параметры: • **hostname <ip-or-domain>** — IP-адрс или имя домена, для которого производится трассировка. • **interface <iface-name>** — интерфейс, с которого будут отправляться пакеты. • **not-map-ip** — не искать hostname для IP-адреса при отображении. • **use-icmp-echo** — использовать ICMP echo. • **port** — указать порт вместо порта по умолчанию (1 — 65535). • **min-interval** — минимальный интервал между пакетами. `Admin/system@nodename# execute traceroute hostname <hostname>`
termination	Закрытие сессий администраторов. Подробнее читайте в разделе Управление сессиями администраторов.
ping	Выполнение ping определенного хоста. Можно задать следующие параметры: • **hostname** — IP-адрес или доменное имя хоста.

Параметр	Описание
	• **count** — количество отправляемых echo-запросов. Если параметр не задан, то отправка пакетов будет происходить, пока соединение не будет прервано пользователем (чтобы прервать отправку: Ctrl+C). • **numeric** — не резолвить имена. • **timestamp** — отображение временных меток. • **interval** — интервал времени, через который будет производиться отправка пакетов; указывается в секундах. • **ttl** — время жизни пакета. • **interface** — адрес выбранного интерфейса будет использоваться в качестве адреса источника для выполнения ping. • **mtu** — размер mtu отправляемых пакетов. • **virtual-router** — имя виртуального маршрутизатора. `Admin/system@nodename# execute ping hostname <hostname> count <number>`
reboot	Перезагрузка устройства.
date	Просмотр текущих даты и времени на сервере.
shutdown	Выключение устройства.
netcheck	Проверка доступности стороннего HTTP/HTTPS-сервера. Могут быть использованы следующие параметры: • **address** — доменное имя хоста для проверки доступности по TCP или URL для HTTP. • **dns-ip** — IP-адрес сервера DNS. • **dns-tcp** — использование TCP вместо UDP для DNS-запроса. • **check-cert** — проверка SSL-сертификата • **type** — проверка доступности по: ◦ **http**. ◦ **tcp** (если порт не указан, то используется порт 80). • **data** — запрос содержимого сайта. По умолчанию запрашиваются только заголовки. • **timeout** — максимальный таймаут ожидания ответа от веб-сервера.

Параметр	Описание

	• **user-agent** — параметр для указания типа браузера (useragent). На некоторых сайтах может быть разрешен доступ только с определенных браузеров. Значение параметра указывается в двойных кавычках.
	
	`Admin/system@nodename# execute netcheck type tcp address <host-domain-name> data on`
	`Admin/system@nodename# execute netcheck address <host-domain-name>`

dig	Проверка записи DNS домена.
	
	• **hostname** — доменное имя хоста или IP-адрес для реверсивного поиска.
	• **reverse-lookup** — получение хоста по IP-адресу.
	• **dns** — указание IP-адреса DNS-сервера.
	• **tcp** — использование протокола TCP вместо UDP.
	
	`Admin/system@nodename# execute dig hostname <host-domain-name>`
	`Admin/system@nodename# execute dig hostname <IP-address> reverse-lookup on`

Часть представленных выше команд также доступны в режиме диагностики и мониторинга. Для их выполнения используется команда:

```
Admin/system@nodename> <command-name>
```

НАСТРОЙКА УСТРОЙСТВА

Настройка устройства (Описание)

Общие настройки UserGate

Общие настройки устройства задаются на уровне **settings general**. Структура команды для настройки одного из разделов (<settings-module>):

```
Admin/system@nodename# set settings general <settings-module>
```

Доступна настройка следующих разделов:

Параметр	Описание
admin-console	Настройки интерфейса (уровень **settings general admin-console**): • **timezone**: 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. • **language**: язык интерфейса: ◦ **ru** — русский. ◦ **en** — английский. • **api-session-lifetime**: время ожидания сеанса администратора в секундах.
server-time	Настройка параметров установки точного времени (уровень **settings general server-time**): • **ntp-enabled**: включение/отключение использования NTP-серверов: ◦ **on**. ◦ **off**. • **primary-ntp-server**: указание основного ntp-сервера. • **second-ntp-server**: указание запасного ntp-сервера. • **time**: установка времени на сервере; время указывается в часовом поясе UTC в формате yyyy-mm-ddThh:mm:ss (например, 2022-02-15T12:00:00)
change-tracker	

Параметр	Описание
	Настройка учёта изменений (уровень **settings general change-tracker**): • **enabled**: включение/отключение учёта изменений. ◦ **on**. ◦ **off**. • **event-tracker-types**: типы изменений задаются администратором. Для удаления типа изменения используется команда: `Admin/system@nodename# delete settings general change-tracker event-tracker-types [ type1 ... ]`

updates-schedule	Настройка расписания скачивания обновлений программного обеспечения и библиотек (уровень **settings general updates-schedule**).
	Для расписания обновления программного обеспечения UserGate:
	`Admin/system@nodename# set settings general updates-schedule software schedule <schedule/disabled>`
	Расписание скачивания обновлений библиотек может быть единым:
	`Admin/system@nodename# set settings general updates-schedule all-libraries schedule <schedule/disabled>`
	или может быть настроено отдельно для каждого элемента:
	`Admin/system@nodename# set settings general updates-schedule libraries [ lib-module ... ] schedule <schedule/disabled>`
	Время задаётся в crontab-формате: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом:
	• Звездочка (*) — обозначает весь диапазон (от первого до последнего).

Параметр	Описание
	• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа". Команда для просмотра расписания обновлений: `Admin/system@nodename# show settings general updates-schedule`

Настройка управления устройством

Настройка Radmin-emergency

Для активации удаленного помощника при возникновении проблемы с программным ядром узла администратор может зайти в CLI под учетной записью корневого администратора, которая была создана при инициализации UserGate. Обычно это учетная запись Admin, хотя может быть и другой. Для входа необходимо указать имя в виде Admin/system@emergency, в качестве пароля — пароль корневого администратора. Команда включения/отключения удалённого доступа к серверу для технической поддержки в таких случаях:

```
Admin/system@emergency# set radmin-emergency enabled <on | off>
```

Параметр	Описание
interface	Название интерфейса.
ip-addr	IP-адрес и маска интерфейса.
gateway-address	IP-адрес шлюза.

Настройка операций с сервером

Следующая команда позволяет определить канал обновлений:

```
Admin/system@nodename# set settings device-mgmt updates-channel <stable
| beta>
```

Для просмотра наличия обновлений и выбранного канал обновления используется команда:

```
Admin/system@nodename# show settings device-mgmt updates-channel
```

Для настройки активации лицензии и обновления ПО устройства через внешний прокси-сервер используется команда:

```
Admin@UGOS# set settings device-mgmt licensing-upstream-proxy
<parameters>
```

В качестве дополнительных параметров указываются:

Параметр	Описание
enabled	Включение/выключение режима активации лицензии и обновления ПО через внешний прокси-сервер: • **on** — включено. • **off** — выключено.
ip	IP-адрес внешнего прокси-сервера.
port	Порт внешнего прокси-сервера.
auth	Аутентификация на внешнем прокси-сервере: • **on** — включена. • **off** — выключена.
name	Логин на внешнем прокси-сервере.
password	Пароль на внешнем прокси-сервере.

Для просмотра созданных настроек активации лицензии и обновления ПО устройства UserGate через внешний прокси-сервер используется команда:

```
Admin@UGOS# show settings device-mgmt licensing-upstream-proxy
```

Управление резервным копированием

Создание резервной копии устройства осуществляется на уровне **settings device-mgmt**. Для создания правила резервного копирования и выгрузки файлов на внешние серверы (FTP/SSH) используется следующая команда:

```
Admin/system@nodename# create settings device-mgmt settings-backup
<parameters>
```

Для настройки доступны следующие параметры:

Параметр	Описание
enabled	Включение/отключение правила создания резервной копии устройства.
name	Название правила резервного копирования.
description	Описание правила резервного копирования.
type	Выбор удалённого сервера для экспорта файлов: • **ssh**. • **ftp**.
address	IP-адрес удалённого сервера.
port	Порт сервера.
login	Учётная запись на удалённом сервере.
password	Пароль учётной записи.
path	Путь на сервере, куда будут выгружены файлы.
schedule	Расписание экспорта файлов резервных копий. Время задаётся в Crontab-формате: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.

Параметр	Описание
	• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

Редактирование существующего правила резервного копирования устройства производится с использованием следующей команды:

```
Admin/system@nodename# set settings device-mgmt settings-backup <rule-name>
```

Список параметров, доступных для изменения аналогичен списку параметров, доступных при создании правила.

Команда для удаления правила резервного копирования:

```
Admin/system@nodename# delete settings device-mgmt settings-backup <rule-name>
```

Команда для отображения правила резервного копирования:

```
Admin/system@nodename# show settings device-mgmt settings-backup <rule-name>
```

Также, для команд редактирования, удаления или отображения правил в качестве <filter> возможно использование не только названия правила, но и заданные в существующем правиле параметры (удобно, например, при наличии нескольких правил с одинаковым названием). Параметры, с использованием которых можно произвести идентификацию правила экспорта, аналогичны параметрам команды **set**.

Экспорт настроек

Создание и настройка правил экспорта настроек происходит на уровне **settings device-mgmt settings-export**.

Для создания правила экспорта настроек:

```
Admin/system@nodename# create settings device-mgmt settings-export
( <parameters> )
```

Доступны параметры:

Параметр	Описание
enabled	Включение/отключение правила экспорта настроек сервера UserGate.
name	Название правила экспорта.
description	Описание правила экспорта.
type	Выбор удалённого сервера для экспорта настроек: • **ssh**. • **ftp**.
address	IP-адрес удалённого сервера.
port	Порт сервера.
login	Учётная запись на удалённом сервере.
password	Пароль учётной записи.
path	Путь на сервере, куда будут выгружены настройки.
schedule	Расписание экспорта настроек. Время задаётся в Crontab-формате: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а

Параметр	Описание
	выражение "*/2" в поле "часы" будет означать "каждые два часа".

Обновление существующего правила экспорта настроек устройства производится с использованием следующей команды:

```
Admin/system@nodename# set settings device-mgmt settings-export <rule-name>
```

Список параметров, доступных для изменения аналогичен списку параметров, доступных при создании правила.

Команда для удаления правила экспорта настроек:

```
Admin/system@nodename# delete settings device-mgmt settings-export <rule-name>
```

Команда для отображения правила экспорта настроек:

```
Admin/system@nodename# show settings device-mgmt settings-export <rule-name>
```

Также, для команд обновления, удаления или отображения правил в качестве <filter> возможно использование не только названия правила, но и заданные в существующем правиле параметры (удобно, например, при наличии нескольких правил с одинаковым названием). Параметры, с использованием которых можно произвести идентификацию правила экспорта, аналогичны параметрам команды **set**.

Настройка кластеров

Настройка кластера конфигурации

Данный раздел находится на уровне **settings device-mgmt configuration-cluster**.

Команда обновления существующего узла кластера:

```
Admin/system@nodename# set settings device-mgmt configuration-cluster
<node-name>
```

Доступно изменение следующих параметров:

Параметр	Описание
name	Изменить имя узла кластера.
description	Обновить описание узла кластера.
ip	Задать IP-адрес интерфейса, входящего в зону, выделенную для кластера.

Команды для удаления и отображения настроек узла кластера:

```
Admin/system@nodename# delete settings device-mgmt configuration-
cluster <node-name>
...
Admin/system@nodename# show settings device-mgmt configuration-cluster
<node-name>
```

Команда для генерации секретного кода для добавления нового узла в кластер конфигурации:

```
Admin/system@nodename# execute configurate-cluster generate-secret-key
```

Настройка кластера отказоустойчивости

Настройка кластеров отказоустойчивости производится на уровне **settings device-mgmt ha-clusters**.

Для создания кластера отказоустойчивости:

```
Admin/system@nodename# create settings device-mgmt ha-clusters
```

Далее необходимо указать следующие параметры:

Параметр	Описание
enabled	Включение/отключение кластера отказоустойчивости: • **on**. • **off**.
name	Название кластера отказоустойчивости.
description	Описание кластера отказоустойчивости.
mode	Выбор режима работы кластера: • **active-passive**: режим работы Актив-Пассив (один из серверов выступает в роли Мастер-узла, обрабатывающего трафик, а остальные — в качестве резервных). • **active-active**: режим работы Актив-Актив (один из серверов выступает в роли Мастер-узла, распределяющего трафик на все остальные узлы кластера).
session-sync	Настройка синхронизации пользовательских сессий в кластере: • **off** — отключение синхронизации пользовательских сессий. • **on** — включение синхронизации пользовательских сессий. • **ha-cluster-id:** ◦ <num> — мультикаст идентификатор кластера (может принимать значения от 0 до 8). Синхронизация пользовательских сессий (кроме сессий, использующих прокси-сервер, например, трафик HTTP/S) включится автоматически.
virtual-router-id	Идентификатор виртуального маршрутизатора (VRID).
nodes	Выбор узлов кластера конфигурации для объединения их в кластер отказоустойчивости.
virtual-ips	Задание виртуального IP-адреса для кластера и выбор рабочего интерфейса для каждого узла (на зоне выбранного интерфейса должен быть разрешён сервис VRRP; подробнее о настройке зон через CLI читайте в разделе Зоны). Добавление виртуального IP-адреса в кластер:

Параметр	Описание
	`Admin/system@nodename# create settings device-mgmt ha-cluster virtual-ips <virtual-ips-filter> <virtual-ip-info>` Доступные параметры для <virtual-ips-filter>: • **new**: создать виртуальный IP-адрес для заданного кластера. • <ip>: изменить данные для выбранного виртуального адреса. Доступные параметры для <virtual-ip-info>: • **ip**: задать IP-адрес для кластера отказоустойчивости (указывается в формате IP/mask). • **ha-interfaces**: задать интерфейсы для узлов кластера (указываются в формате node-name/interface).
session-sync-all	Включение/отключение режима синхронизации всех пользовательских сессий, включая UDP/ICMP сессии. В случае, если этот параметр не активирован, а настройка **session-sync** активирована, синхронизироваться будут только TCP сессии.
excluded-sync-ips	Указание IP-адресов, с которыми отключена синхронизация всех пользовательских сессий.

Пример команды создания кластера:

```
Admin/system@nodename# create settings device-mgmt ha-clusters nodes [ node_1 ] name "Test HA cluster" description "Test HA cluster description" mode active-passive enabled on virtual-ips new ha-interfaces [ node_1/port3 ] ip 192.168.1.5/24
```

Для редактирования настроек кластера:

```
Admin/system@nodename# set settings device-mgmt ha-cluster <cluster-name>
```

Параметры для редактирования:

Параметр	Описание
enabled	Включение/отключение кластера отказоустойчивости: • **on**. • **off**.
name	Название кластера отказоустойчивости.
description	Описание кластера отказоустойчивости.
mode	Выбор режима работы кластера: • **active-passive**: режим работы Актив-Пассив (один из серверов выступает в роли Мастер-узла, обрабатывающего трафик, а остальные — в качестве резервных). • **active-active**: режим работы Актив-Актив (один из серверов выступает в роли Мастер-узла, распределяющего трафик на все остальные узлы кластера).
master-node	Назначение мастер-узла кластера отказоустойчивости.
session-sync	Настройка синхронизации сессий в кластере: • **off** — отключение синхронизации пользовательских сессий. • **on** — включение синхронизации пользовательских сессий. • **ha-cluster-id:** ◦ <num> — мультикаст идентификатор кластера (может принимать значения от 0 до 8). Синхронизация пользовательских сессий (кроме сессий, использующих прокси-сервер, например, трафик HTTP/S) включится автоматически.
virtual-router-id	Идентификатор виртуального маршрутизатора (VRID).
nodes	Выбор узлов кластера конфигурации для объединения их в кластер отказоустойчивости.
virtual-ips	Задание виртуального IP-адреса для кластера и выбор рабочего интерфейса для каждого узла (на зоне выбранного интерфейса должен быть разрешён сервис VRRP; подробнее о настройке зон через CLI читайте в разделе Зоны).

Параметр	Описание
	Добавление виртуального IP-адреса в кластер: `Admin/system@nodename# create settings device-mgmt ha-cluster virtual-ips <virtual-ips-filter> <virtual-ip-info>` Доступные параметры для <virtual-ips-filter>: • **new**: создать виртуальный IP-адрес для заданного кластера. • <ip>: изменить данные для выбранного виртуального адреса. Доступные параметры для <virtual-ip-info>: • **ip**: задать IP-адрес для кластера отказоустойчивости (указывается в формате IP/mask). • **ha-interfaces**: задать интерфейсы для узлов кластера (указываются в формате node-name/interface).
session-sync-all	Включение/отключение режима синхронизации всех пользовательских сессий, включая UDP/ICMP сессии. В случае, если этот параметр не активирован, а настройка **session-sync** активирована, синхронизироваться будут только TCP сессии.
excluded-sync-ips	Указание IP-адресов, с которыми отключена синхронизация всех пользовательских сессий.

Примеры редактироания настроек кластера:

```
Admin/system@nodename# set settings device-mgmt ha-clusters "Test HA cluster" nodes [ node_1 node_2 ] virtual-ips 192.168.1.5/24 ha-interfaces [ node_1/port3 node_2/port3 ]
...
Admin/system@nodename# set settings device-mgmt ha-clusters "Test HA cluster" master-node node_2
```

Для удаления кластера:

```
Admin/system@nodename# delete settings device-mgmt ha-clusters <cluster-name>
```

Также доступно удаление отдельных параметров:

- **nodes**.
- **virtual-ips**.

Для отображения информации о всех кластерах отказоустойчивости:

```
Admin/system@nodename# show settings device-mgmt ha-cluster
```

Для отображения информации об определённом кластере:

```
Admin/system@nodename# show settings device-mgmt ha-cluster <cluster-
name>
```

Настройка управления доступом к консоли устройства

Настройка данного раздела производится на уровне **settings administrators**. В разделе описаны настройка параметров защиты учётных записей, настройка администраторов и их профилей.

Общие настройки доступа

Данный раздел позволяет настроить дополнительные параметры защиты учётных записей администраторов. Настройка производится на уровне **settings administrators general**.

Для изменения параметров используется следующая команда:

```
Admin/system@nodename# set settings administrators general
```

Параметры, доступные для редактирования:

Параметр	Описание
password	Изменить пароля текущего администратора.

Параметр	Описание
unblock	Разблокировать администратора.
strong-password	Использовать сложный пароль: • **on**. • **off**.
num-auth-attempts	Установить максимальное количество неверных попыток аутентификации.
block-time	Указать время блокировки учётной записи в случае достижения администратором максимального количества попыток аутентификации; указывается в секундах (максимальное значение: 3600 секунд).
min-length	Определить минимальную длину пароля (максимальное значение: 100 символов).
min-uppercase	Определить минимальное количество символов в верхнем регистре (максимальное значение: 100 символов).
min-lowercase	Определить минимальное количество символов в нижнем регистре (максимальное значение: 100 символов).
min-digits	Определить минимальное количество цифр (максимальное значение: 100 символов).
spec-characters	Определить минимальное количество специальных символов (максимальное значение: 100 символов).
char-repetition	Указать максимальную длину блока из одного и того же символа (максимальное значение: 100 символов).

Пример редактирования параметров учетных записей:

```
Admin/system@nodename# set settings administrators general block-time
400
```

Для просмотра текущих параметров защиты учётных записей администраторов используется следующая команда:

```
Admin/system@nodename# show settings administrators general
```

```
strong-password      : off
block-time           : 400
min-length           : 7
min-uppercase        : 1
min-lowercase        : 1
min-digits           : 1
spec-characters      : 1
char-repetition      : 2
num-auth-attempts    : 10
```

Настройка учётных записей администраторов

Настройка учётных записей администраторов производится на уровне **settings administrators administrators**.

Для создания учётной записи администратора используется следующая команда:

```
Admin/system@nodename# create settings administrators administrators
```

Далее необходимо указать тип учётной записи администратора (локальный, пользователь LDAP, группа LDAP, с профилем аутентификации) и установить соответствующие параметры:

Параметр	Описание
local	Добавить локального администратора: • **enabled**: включение/отключение учётной записи администратора: ◦ **on**. ◦ **off**. • **login**: логин администратора. • **display-name**: отображаемое имя администратора. • **description**: описание учётной записи администратора. • **admin-profile**: профиль администратора. Создание профилей администраторов рассмотрено далее. • **password**: пароль администратора.
ldap-user	

Параметр	Описание
	Добавить пользователя из существующего домена (необходим корректно настроенный LDAP-коннектор; подробнее читайте в разделе Настройка LDAP-коннектора): • **enabled**: включение/отключение учётной записи администратора: ◦ **on**. ◦ **off**. • **login**: логин администратора в формате **domain\user**. Структура команды при указании данного параметра: • **display-name**: отображаемое имя администратора. • **connector**: название сконфигурированного ранее LDAP-коннектора. • **description**: описание учётной записи администратора. • **admin-profile**: профиль администратора. Создание профилей администраторов рассмотрено далее. `Admin/system@nodename# create settings administrators administrators ldap-user admin-profile "test profile 1" connector "LDAP connector" description "Admin as domain user" login testd.local\user1 enabled on`
ldap-group	Добавить группу пользователей из существующего домена (необходим корректно настроенный LDAP-коннектор; подробнее читайте в разделе Настройка LDAP-коннектора): • **enabled**: включение/отключение учётной записи администратора: ◦ **on**. ◦ **off**. • **login**: логин администратора • **display-name**: отображаемое имя администратора. • **connector**: название используемого LDAP-коннектора. • **description**: описание учётной записи администратора. • **admin-profile**: профиль администратора. Создание профилей администраторов рассмотрено далее. `Admin/system@nodename# create settings administrators administrators ldap-group`

Параметр	Описание
	`admin-profile "test profile 1" connector "LDAP connector" description "Domain admin group" login testd.local\users enabled on`
admin-auth-profile	Добавить администратора с профилем аутентификации (необходимы корректно настроенные серверы аутентификации; подробнее читайте в разделе Настройка серверов аутентификации): • **enabled**: включение/отключение учётной записи администратора: ◦ **on**. ◦ **off**. • **login**: логин администратора. • **display-name**: отображаемое имя администратора. • **description**: описание учётной записи администратора. • **admin-profile**: профиль администратора. Создание профилей администраторов рассмотрено далее. • **auth-profile**: выбор профиля аутентификации из созданных ранее; подробнее о профилях аутентификации читайте в разделе Настройка профилей аутентификации.

Для редактирования параметров профиля используется команда:

```
Admin/system@nodename# set settings administrators administrators
<admin-type> <admin-login>
```

Параметры для редактирования аналогичны параметрам создания профиля администратора.

Для отображения информации о всех учётных записях администраторов:

```
Admin/system@nodename# show settings administrators administrators
```

Для отображения информации об определённой учётной записи администратора:

```
Admin/system@nodename# show settings administrators administrators
<admin-type> <admin-login>
```

Пример выполнения команды:

```
Admin/system@nodename# show settings administrators administrators
ldap-user testd.local\user1

login            : testd.local\user1
enabled          : on
type             : ldap_user
locked           : off
admin-profile    : test profile 1
```

Для удаления учётной записи используется команда:

```
Admin/system@nodename# delete settings administrators administrators
<admin-type> <admin-login>
```

Пример команды:

```
Admin/system@nodename# delete settings administrators administrators
ldap-user testd.local\user1
```

Настройка прав доступа профилей администраторов

Настройка прав доступа профилей администраторов производится на уровне **settings administrators profiles**.

Для создания профиля администратора используется следующая команда:

```
Admin/system@nodename# create settings administrators profiles
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля администратора.
description	Описание профиля администратора.
admin-type	Роль администратора: • **device** — администратор устройства UGMC. • **realm** — администратор управляемой области.
permissions	Права доступа: • **no-access**: нет доступа. • **read**: только чтение. • **write**: чтение и запись.

Для редактирования профиля используется команда:

```
Admin/system@nodename# set settings administrators profiles <profile-
name> <parameter>
```

Параметры для редактирования аналогичны параметрам создания профиля администратора.

Для просмотра информации о всех профилях администраторов:

```
Admin/system@nodename# show settings administrators profiles
```

Для отображения информации об определённом профиле:

```
Admin/system@nodename# show settings administrators profiles <profile-
name>
```

Чтобы удалить профиль администратора:

```
Admin/system@nodename# delete settings administrators profiles
<profile-name>
```

Управление сессиями администраторов

С использованием следующих команд возможен просмотр активных сессий администраторов, прошедших авторизацию в веб-консоли или CLI, и закрытие сессий (уровень: **settings administrators admin-sessions**).

Просмотр сессий администраторов текущего узла UserGate (возможен просмотр сессии отдельного администратора: необходимо из предложенного списка выбрать IP-адрес, с которого была произведена авторизация):

```
Admin/system@nodename# show settings administrators admin-sessions
```

Для отображения сессий доступно использование фильтра:

- **ip**: IP-адрес, с которого авторизован администратор.
- **source**: где была произведена авторизация: CLI (**cli**), веб-консоль (**web**) или подключение по SSH (**ssh**).
- **admin-login**: имя администратора.
- **node**: узел кластера UserGate.

```
Admin/system@nodename# show settings administrators admin-sessions
( node <node-name> ip <session-ip> source <cli | web | ssh> admin-login
<administrator-login> )
```

Команда для закрытия сессии администратора; необходимо из предложенного списка выбрать IP-адрес, с которого была произведена авторизация:

```
Admin/system@nodename# execute termination admin-sessions <IP-address/
connection type>
```

Пример выполнения команд:

```
Admin/system@nodename# show settings administrators admin-sessions

admin-login           : Admin
source                : ssh
```

```
session_start_date    : 2023-08-10T11:33:47Z
ip                    : 127.0.0.1
node                  : utmcore@dineanoulwer

admin-login           : Admin
source                : web
session_start_date    : 2023-08-10T11:33:10Z
ip                    : 10.0.2.2
node                  : utmcore@dineanoulwer

Admin/system@nodename# execute termination admin-sessions 10.0.2.2/web

Admin/system@nodename# show settings administrators admin-sessions

admin-login           : Admin
source                : ssh
session_start_date    : 2023-08-10T11:33:47Z
ip                    : 127.0.0.1
node                  : utmcore@dineanoulwer
```

При закрытии сессии администраторов возможно использование фильтра (<filter>). Параметры фильтрации аналогичны параметрам команды **show**.

```
Admin/system@nodename# execute termination admin-sessions ( node <node-
name> ip <session-ip> source <cli | web | ssh> admin-login
<administrator-login> )
```

Настройка сертификатов

Раздел **Сертификаты** находится на уровне **settings certificates**.

Для импорта сертификатов предназначена команда:

```
Admin/system@nodename# import settings certificates
```

Далее необходимо указать параметры:

Параметр	Описание
name	Название сертификата, которое будет отображено в списке.
description	Описание сертификата.
certificate-data	Сертификат в формате PEM.
certificate-chain	Цепочка сертификатов в формате PEM.
private-key	Приватный ключ в формате PEM.
passphrase	Пароль для приватного ключа или контейнера PKCS12 (необязательное значение).

Для экспорта доступны сертификаты, вся цепочка сертификатов:

```
Admin/system@nodename# export settings certificates <certificate-name>
Admin/system@nodename# export settings certificates <certificate-name>
with-chain on
```

С использованием командной строки возможно создание сертификата и CSR:

```
Admin/system@nodename# create settings certificates type <certificate |
csr>
```

Далее необходимо указание следующих параметров:

Параметр	Описание
name	Название сертификата.
description	Описание сертификата.
country	Страна, в которой выписывается сертификат.
state	Область/штат, в котором выписывается сертификат.
locality	Город, в котором выписывается сертификат.
organization	Название организации, для которой выписывается сертификат.

Параметр	Описание
common-name	Имя сертификата. Рекомендуется использовать только символы латинского алфавита для совместимости с большинством браузеров.
email	Email компании.

Команда для управления сертификатом:

```
Admin/system@nodename# set settings certificates <certificate-name>
```

Доступны параметры:

Параметр	Описание
name	Название сертификата.
description	Описание сертификата.
role	Тип сертификата: • **web-cert-chain**: цепочка сертификатов веб-консоли. • **web-ssl**: сертификат, использующийся для создания безопасного HTTPS-подключения администратора к веб-консоли UserGate. • **none**.
certificate-chain	Цепочка сертификатов в формате PEM.

Для удаления сертификата:

```
Admin/system@nodename# delete settings certificates <certificate-name>
```

Команды для просмотра информации об определённом сертификате или о всех сертификатах:

```
Admin/system@nodename# show settings certificates
Admin/system@nodename# show settings certificates <certificate-name>
```

Настройка серверов аутентификации

Раздел Серверы аутентификации позволяет произвести настройку LDAP-коннектора, серверов RADIUS, TACACS+. Настройка серверов аутентификации производится на уровне **users auth-server** и будет рассмотрена далее в соответствующих разделах.

Настройка LDAP-коннектора

Настройка LDAP-коннектора производится на уровне **users auth-server ldap**.

Для создания LDAP-коннектора используется команда:

```
Admin/system@nodename# create users auth-server ldap <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя LDAP-коннектора.
enabled	Включение/отключение сервера аутентификации.
description	Описание LDAP-коннектора.
ssl	Определяет: • **on** — использование SSL-соединения для подключения к LDAP-серверу. • **off** — подключение к LDAP-серверу без использования SSL-соединения.
address	IP-адрес контроллера или название домена LDAP.
bind-dn	Имя пользователя, которое будет использоваться для подключения к серверу; указывается в формате DOMAIN\username или username@domain. Пользователь должен быть заведён в домене.
password	Пароль пользователя для подключения к домену.
domains	Список доменов, которые обслуживаются указанным контроллером домена.
search-roots	

Параметр	Описание
	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. Если пути поиска не указаны, то поиск производится по всему каталогу, начиная от корня.

Для редактирования информации о существующем LDAP-коннекторе используется команда:

```
Admin/system@nodename# set users auth-server ldap <ldap-server-name>
<parameter>
```

Параметры, доступные для обновления, аналогичны параметрам создания LDAP-коннектора.

Команда для отображения информации о LDAP-коннекторе:

```
Admin/system@nodename# show users auth-server ldap <ldap-server-name>
```

Примеры команд создания и редактирования LDAP-коннектора:

```
Admin/system@nodename# create users auth-server ldap name "New LDAP
connector" ssl on address 10.10.0.10 bind-dn ug@testd.local password
12345 domains [ testd.local ] search-roots [ dc=testd,dc=local ]
enabled on
Admin/system@nodename# show users auth-server ldap "New LDAP connector"

name             : New LDAP connector
enabled          : on
ssl              : on
address          : 10.10.0.10
bind-dn          : ug@testd.local
domains          : testd.local
search-roots     : dc=testd,dc=local
keytab_exists    : off
Admin/system@nodename# set users auth-server ldap "New LDAP connector"
description "New LDAP connector description"
Admin/system@nodename# show users auth-server ldap "New LDAP connector"
```

```
name              : New LDAP connector
description       : New LDAP connector description
enabled           : on
ssl               : on
address           : 10.10.0.10
bind-dn           : ug@testd.local
domains           : testd.local
search-roots      : dc=testd,dc=local
keytab_exists     : off
```

Для удаления LDAP-коннектора используется команда:

```
Admin/system@nodename# delete users auth-server ldap <ldap-server-name>
<parameter>
```

Также возможно удаления отдельных параметров LDAP-коннектора. Для удаления доступны следующие параметры:

- **domains**.
- **search-roots**.

Настройка RADIUS-сервера

Настройка RADIUS-сервера производится на уровне **users auth-server radius**.

Для создания сервера аутентификации RADIUS используется команда со следующей структурой:

```
Admin/system@nodename# create users auth-server radius <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя RADIUS-сервера.
enabled	Включение/отключение сервера аутентификации.
description	Описание сервера аутентификации.

Параметр	Описание
secret	Общий ключ, используемый протоколом RADIUS для аутентификации.
addresses	IP-адрес и UDP-порт, на котором сервер RADIUS слушает запросы (по умолчанию порт 1812); указывается в формате <ip:port>.

Команда для обновления информации о сервере RADIUS:

```
Admin/system@nodename# set users auth-server radius <radius-server-
name> <parameter>
```

Параметры, которые могут быть обновлены, соответствуют параметрам, указание которых возможно при создании сервера аутентификации.

Команда для отображения информации о RADIUS-сервере:

```
Admin/system@nodename# show users auth-server radius <radius-server-
name>
```

Примеры команд создания и редактирования RADIUS-сервера:

```
Admin/system@nodename# create users auth-server radius name "New RADIUS
server" addresses [ 10.10.0.9:1812 ] secret 12345 enabled on
Admin/system@nodename# show users auth-server radius "New RADIUS
server"

name           : New RADIUS server
enabled        : on
addresses      :
    host    : 10.10.0.9
    port    : 1812
Admin/system@nodename# set users auth-server radius "New RADIUS server"
description "New RADIUS server description"
Admin/system@nodename# show users auth-server radius "New RADIUS
server"

name           : New RADIUS server
```

```
description    : New RADIUS server description
enabled        : on
addresses      :
    host    : 10.10.0.9
    port    : 1812
```

Для удаления сервера:

```
Admin/system@nodename# delete users auth-server radius <radius-server-
name> <parameter>
```

Также возможно удаления отдельных параметров RADIUS-сервера. Для удаления доступны следующие параметры:

- **addresses**.

Настройка сервера TACACS+

Настройка сервера TACACS+ производится на уровне **users auth-server tacacs**.

Для создания сервера аутентификации TACACS+ используется команда со следующей структурой:

```
Admin/system@nodename# create users auth-server tacacs <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя сервера TACACS+.
enabled	Включение/отключение сервера.
description	Описание сервера аутентификации.
secret	Общий ключ, используемый протоколом TACACS+ для аутентификации.
address	IP-адрес сервера TACACS+.
port	UDP-порт, на котором сервер TACACS+ слушает запросы на аутентификацию. По умолчанию это порт UDP 1812.

Параметр	Описание
single-connection	Использовать одно TCP-соединение для работы с сервером TACACS+.
timeout	Время ожидания сервера TACACS+ для получения аутентификации. По умолчанию 4 секунды.

Команда для редактирования информации о сервере TACACS+:

```
Admin/system@nodename# set users auth-server tacacs <tacacs-server-
name> <parameter>
```

Параметры, которые могут быть обновлены, соответствуют параметрам, указание которых возможно при создании сервера аутентификации.

Команда для отображения информации о сервере TACACS+:

```
Admin/system@nodename# show users auth-server tacacs <tacacs-server-
name>
```

Примеры команд для создания и редактирования сервера TACACS+:

```
Admin/system@nodename# create users auth-server tacacs address
10.10.0.11 name "New TACACS+ server" port 1812 secret 12345 enabled on
Admin/system@nodename# show users auth-server tacacs "New TACACS+
server"

name                : New TACACS+ server
enabled             : on
address             : 10.10.0.11
port                : 1812
single-connection   : off
timeout             : 4
Admin/system@nodename# set users auth-server tacacs "New TACACS+
server" description "New TACACS+ server description"
Admin/system@nodename# show users auth-server tacacs "New TACACS+
server"

name                : New TACACS+ server
```

```
description          : New TACACS+ server description
enabled              : on
address              : 10.10.0.11
port                 : 1812
single-connection    : off
timeout              : 4
```

Для удаления сервера:

```
Admin/system@nodename# delete users auth-server tacacs <tacacs-server-name>
```

Настройка профилей аутентификации

Настройка профилей аутентификации производится на уровне **users auth-profile**.

Для создания профиля аутентификации используется следующая команда:

```
Admin/system@nodename# create users auth-profile <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля.
description	Описание профиля.
idle-time	Время бездействия до отключения; указывается в секундах. Через указанный промежуток времени при отсутствии активности пользователь перейдёт в статус Unknown user.
expiration-time	Время жизни аутентифицированного пользователя; указывается в секундах. Через указанный промежуток времени пользователь перейдёт в статус Unknown user; необходима повторная аутентификация пользователя.

Параметр	Описание
max-attempts	Число неудачных попыток аутентификации до блокировки учётной записи пользователя.
lockout-time	Время, на которое блокируется учетная запись пользователя при достижении указанного числа неудачных попыток аутентификации; указывается в секундах.
auth-methods	Метод аутентификации: • **ldap**: аутентификация с использованием LDAP-коннектора. • **radius**: аутентификация с использованием RADIUS-сервера. • **tacacs**: аутентификация с использованием сервера TACACS+.

Команда для редактирования настроек профилей аутентификации:

```
Admin/system@nodename# set users auth-profile <auth-profile-name>
<parameter>
```

Для обновления доступен список параметров, аналогичный списку параметров команды **create**.

Пример создания и редактирования профиля аутентификации пользователя:

```
Admin/system@nodename# create users auth-profile name "New LDAP auth
profile" auth-methods ldap [ "New LDAP connector" ]
Admin/system@nodename# show users auth-profile "New LDAP auth profile"

name                : New LDAP auth profile
max-attempts        : 5
idle-time           : 900
expiration-time     : 86400
lockout-time        : 300
mfa                 : none
auth-methods        :
    http-basic          : off
    local-user-auth     : off
    policy-accept       : off
```

```
Admin/system@nodename# set users auth-profile "New LDAP auth profile"
description "New LDAP auth profile description"
Admin/system@nodename# show users auth-profile "New LDAP auth profile"

name                : New LDAP auth profile
description         : New LDAP auth profile description
max-attempts        : 5
idle-time           : 900
expiration-time     : 86400
lockout-time        : 300
mfa                 : none
auth-methods        :
    http-basic          : off
    local-user-auth     : off
    policy-accept       : off
    ldap                : New LDAP connector
```

Через интерфейс командной строки возможно удаления всего профиля или отдельных способов аутентификации, заданных в профиле. Для этого используются следующие команды.

Для удаления профиля аутентификации:

```
Admin/system@nodename# delete users auth-profile <auth-profile-name>
```

Для удаления методов аутентификации, заданных в профиле, необходимо указать метод аутентификации (доступные методы авторизации перечислены в таблице выше):

```
Admin/system@nodename# delete users auth-profile <auth-profile-name>
auth-methods <auth-metod>
```

НАСТРОЙКА СЕТИ

Зоны

Данный раздел находится на уровне **network zone**. Команда для создания новой зоны:

```
Admin/system@nodename# create network zone
```

Далее необходимо указать параметры зоны:

Параметр	Описание
name	Название зоны.
description	Описание зоны.
dos-protection-syn	Защита зоны от сетевого флуда для протокола TCP (SYN-flood): • **enabled**: включение/отключение защиты. ◦ **on**. ◦ **off**. • **aggregate**: ◦ **on** — считаются все пакеты, входящие в интерфейсы данной зоны. ◦ **off** — пакеты считаются отдельно для каждого IP-адреса. • **alert-threshold**: порог уведомления; если количество запросов превышает данный порог, то происходит запись события в системный журнал. • **drop-threshold**: порог отбрасывания пакетов; если количество запросов превышает указанное значение, то UserGate отбрасывает пакеты и записывает данное событие в системный журнал. • **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-udp	Защита зоны от сетевого флуда для протокола UDP: • **enabled**: включение/отключение защиты. ◦ **on**. ◦ **off**. • **aggregate**: ◦ **on** — считаются все пакеты, входящие в интерфейсы данной зоны.

Параметр	Описание
	◦ **off** — пакеты считаются отдельно для каждого IP-адреса. • **alert-threshold**: порог уведомления; если количество запросов превышает данный порог, то происходит запись события в системный журнал. • **drop-threshold**: порог отбрасывания пакетов; если количество запросов превышает указанное значение, то UserGate отбрасывает пакеты и записывает данное событие в системный журнал. • **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-icmp	Защита зоны от сетевого флуда для протокола ICMP: • **enabled**: включение/отключение защиты. ◦ **on**. ◦ **off**. • **aggregate**: ◦ **on** — считаются все пакеты, входящие в интерфейсы данной зоны. ◦ **off** — пакеты считаются отдельно для каждого IP-адреса. • **alert-threshold**: порог уведомления; если количество запросов превышает данный порог, то происходит запись события в системный журнал. • **drop-threshold**: порог отбрасывания пакетов; если количество запросов превышает указанное значение, то UserGate отбрасывает пакеты и записывает данное событие в системный журнал. • **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты.
enabled-services	Параметры контроля доступа зоны: • **"Any ICMP"**: разрешение использования команды ping адреса UserGate. • **SNMP**: доступ к UserGate по протоколу SNMP (UDP 161). • **rpc**: XML-RPC для управления - позволяет управлять продуктом по API (TCP 4040). • **VRRP**: сервис, необходимый для объединения нескольких узлов UserGate в отказоустойчивый кластер (IP протокол 112). • **"CLI over SSH"**: доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200.

Параметр	Описание
	• **Cluster**: сервис, необходимый для объединения нескольких узлов UserGate в кластер (TCP 4369, TCP 9000-9100). • **"Admin Console"**: доступ к веб-консоли управления (TCP 8001).
service-addresses	Указание разрешённых IP-адресов для сервисов: • **service**: выбор сервисов (список соответствует **enabled-services**). • **allowed-addresses**: разрешённые IP-адреса: ◦ **geoip** — код GeoIP. ◦ **ip-list** — заранее созданный в библиотеке элементов список IP-адресов.
antispoof-enable	Включение/отключение защиты от IP-спуфинга: • **on**. • **off**.
antispoof-negate	Возможные значения: • **on**. • **off**. При **antispoof-negate on** адреса источников, указанные в значении **ip-spoofing-networks**, будут являться адресами, которые не могут быть получены на интерфейсах данной зоны. В этом случае будут отброшены пакеты с указанными IP-адресами источников.
sessions-limit-enabled	Включение ограничения количества одновременных сессий с одного IP-адреса: • **on**. • **off**.
sessions-limit-exclusions	Добавление списка IP-адресов, для которых ограничение на количество одновременных сессий не будет действовать.
sessions-limit-threshold	Максимально возможное количество одновременных сессий с одного IP-адреса.
geoip	Коды GeoIP, которые используются в защите от IP-спуфинга.
ip-list	

Параметр	Описание
	Список IP-адресов, которые используются в защите от IP-спуфинга.

Пример создания новой зоны:

```
Admin/system@nodename# create network zone name Test_zone description
"Test_zone description" antispoof-enable on enabled-services [ "Any
ICMP" DNS ] dos-protection-icmp enabled on
```

Для редактирования параметров зоны:

```
Admin/system@nodename# set network zone <zone-name>
```

Пример редактирования параметров зоны:

```
Admin/system@nodename# set network zone Test_zone dos-protection-syn
enabled on
```

Команда удаления зоны или её параметров:

```
Admin/system@nodename# delete network zone <zone-name>
```

Параметры, доступные для удаления:

Параметр	Описание
dos-protection-syn	Защита зоны от сетевого флуда для протокола TCP (SYN-flood): • **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-udp	Защита зоны от сетевого флуда для протокола UDP: • **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-icmp	

Параметр	Описание
	Защита зоны от сетевого флуда для протокола ICMP: • **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты.
enabled-services	Установленные ранее параметры контроля доступа в данной зоне
geoip	Коды GeoIP, которые используются в защите от IP-спуфинга.
ip-list	Список IP-адресов, которые используются в защите от IP-спуфинга.

Команда для просмотра настроек зоны:

```
Admin/system@nodename# show network zone <zone-name>
```

Интерфейсы

Настройка интерфейсов производится на уровне **network interface:**

Настройка adapter

Сетевые адаптеры настраиваются на уровне **network interface adapter**.

Создать сетевой адаптер нельзя. Для обновления существующего сетевого адаптера используется команда:

```
Admin/system@nodename# set network interface adapter <adapter_name>
```

Далее необходимо указать параметры сетевого адаптера:

Параметр	Описание
enabled	Включение/отключение сетевого интерфейса: • **on**. • **off**.

Параметр	Описание
description	Описание сетевого интерфейса.
alias	Алиас/псевдоним интерфейса.
iface-type	Тип интерфейса: • **l3**: интерфейс, работающий в режиме Layer 3 (можно назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах, это стандартный режим работы интерфейса). • **mirror**: интерфейс, работающий в режиме Mirror (может получать трафик со SPAN-порта сетевого оборудования для его анализа).
iface-mode	Режим назначения IP-адреса: • **dhcp**: получение динамического IP-адреса по DHCP. • **manual**: без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса.
zone	Зона, которой будет принадлежать интерфейс.
link-info	Настройка параметров сетевого интерфейса: • **bc_forwarding**: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • **proxy_arp**, **proxy_arp_vlan**: механизм Proxy ARP. Параметр **proxy_arp** — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; **proxy_arp_vlan** — UserGate будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: `Admin/system@nodename# create network interface <iface-type> … link-info [ key/value ]` где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения.

Параметр	Описание
	Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. **Важно!** Удаление заданных параметров недоступно.
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся в следующем виде: **[<ip_address/mask>]** или **[<ip_address/mask> <ip_address/mask>]**, если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел); маска подсети задаётся в десятичном виде. **Важно!** Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса.
mtu	Указание размера MTU.

Команда удаления адаптера или его параметров:

```
Admin/system@nodename# delete network interface adapter <adapter-name>
```

Параметры, доступные для удаления:

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay server-address	IP-адрес сервера DHCP.

Команда для отображения информации о всех сетевых адаптерах:

```
Admin/system@nodename# show network interface adapter
```

Для отображения информации об адаптере:

```
Admin/system@nodename# show network interface adapter <adapter-name>
```

Настройка VLAN

Интерфейсы VLAN настраиваются на уровне **network interface vlan**.

Команда для добавления нового VLAN-интерфейса:

```
Admin/system@nodename# create network interface vlan
```

Далее необходимо указать параметры:

Параметр	Описание
enabled	Включение/отключение VLAN-интерфейса: • **on**. • **off**.
description	Описание интерфейса.
alias	Алиас/псевдоним интерфейса.
iface-type	Тип интерфейса: • **l3**: Layer 3 (можно назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах, это стандартный режим работы интерфейса). • **mirror**: интерфейс, работающий в режиме Mirror (может получать трафик со SPAN-порта сетевого оборудования для его анализа).
iface-mode	Режим назначения IP-адреса: • **dhcp**: получение динамического IP-адреса по DHCP. • **manual**: без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса.
tag	Тег VLAN. Допускается создание до 4094 интерфейсов.
node-name	Имя узла кластера, на котором создаётся VLAN.
interface	Физический интерфейс, на котором создается VLAN.
zone	Зона, которой будет принадлежать интерфейс.

Параметр	Описание
link-info	Настройка параметров сетевого интерфейса: • **bc_forwarding**: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • **proxy_arp**, **proxy_arp_vlan**: механизм Proxy ARP. Параметр **proxy_arp** — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; **proxy_arp_vlan** — UserGate будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: `Admin/system@nodename# create network interface <iface-type> … link-info [ key/value ]` где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. **Важно!** Удаление заданных параметров недоступно.
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся в следующем виде: **[<ip_address/mask>]** или **[<ip_address/mask> <ip_address/mask>]**, если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел); маска подсети задаётся в десятичном виде. **Важно!** Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса.
mtu	Указание размера MTU.
dhcp-relay	

Параметр	Описание
	Настройка работы DHCP-релея на интерфейсе. Необходимо указать: • **enabled**: включение/отключения релея: ◦ **on**. ◦ **off**. • **utm-address**: IP-адрес интерфейса UserGate, на который добавляется функция релея. • **server-address**: адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Редактирование существующего VLAN:

```
Admin/system@nodename# set network interface vlan <vlan-name>
```

Параметры, доступные для обновления, аналогичны параметрам создания VLAN, кроме **tag**, **node-name**, **interface** (изменение значений этих параметров недоступно).

Команда удаления VLAN-интерфейса или его параметров:

```
Admin/system@nodename# delete network interface vlan <vlan-name>
```

Параметры, доступные для удаления:

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay server-address	IP-адрес сервера DHCP.

Чтобы отобразить информацию о всех интерфейсах VLAN:

```
Admin/system@nodename# show network interface vlan
```

или об определённом интерфейсе:

```
Admin/system@nodename# show network interface vlan <vlan-name>
```

Настройка bond-интерфейса

Настройка бонд-интерфейса производится на уровне **network interface bond**.

Команда для создания бонд-интерфейса:

```
Admin/system@nodename# create network interface bond
```

Параметры, которые необходимо указать:

Параметр	Описание
enabled	Включение/отключение интерфейса: • **on**. • **off**.
interface-name	Необходимо ввести номер, который будет отображён в имени интерфейса (например 1, тогда название созданного интерфейса будет bond1).
description	Описание интерфейса.
alias	Алиас/псевдоним интерфейса.
node-name	Узел кластера, на котором будет создан бонд-интерфейс.
zone	Зона, которой будет принадлежать бонд.
link-info	Настройка параметров сетевого интерфейса: • **bc_forwarding**: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • **proxy_arp**, **proxy_arp_vlan**: механизм Proxy ARP. Параметр **proxy_arp** — UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; **proxy_arp_vlan** — UserGate будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: `Admin/system@nodename# create network interface <iface-type> … link-info [ key/value ]`

Параметр	Описание
	где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. **Важно!** Удаление заданных параметров недоступно.
bonding	Дополнительные параметры бонд-интерфейса: • **mode** — режим работы бонда: ◦ **round-robin**: режим Round robin (пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. Эта политика применяется для балансировки нагрузки и отказоустойчивости). ◦ **active-backup**: режим 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. Данная политика применяется для обеспечения отказоустойчивости). ◦ **xor**: режим 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 обеспечения отказоустойчивости). ◦ **broadcast**: режим Broadcast (передает все на все сетевые интерфейсы. Эта политика применяется для отказоустойчивости). ◦ **802.3ad**: режим IEEE 802.3ad (режим работы, установленный по умолчанию, поддерживается большинством сетевых коммутаторов. Создаются агрегированные группы сетевых карт с одинаковой скоростью и дуплексом. При

Параметр	Описание
	таком объединении передача задействует все каналы в активной агрегации согласно стандарту IEEE 802.3ad. Выбор, через какой интерфейс отправлять пакет, определяется политикой; по умолчанию используется XOR-политика, можно также использовать «xmit_hash» политику). ◦ **transmit**: режим 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). ◦ **load**: режим 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**: периодичность MII-мониторинга в миллисекундах. Определяет, как часто будет проверяться состояние линии на наличие отказов. • **down-delay**: 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. • **up-delay**: 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. • **lacp-rate**: интервал, с которым будут передаваться партнером LACPDU-пакеты в режиме 802.3ad. Возможные значения: ◦ **slow**: запрос партнера на передачу LACPDU-пакетов каждые 30 секунд.

Параметр	Описание
	◦ **fast**: запрос партнера на передачу LACPDU-пакетов каждую секунду. • **failover-mac**: определение способа назначения MAC-адресов на объединенные интерфейсы в режиме Active backup при переключении интерфейсов. Возможные значения: ◦ **disabled**: 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**: определение хэш-политики передачи пакетов через объединенные интерфейсы в режиме XOR или IEEE 802.3ad. Возможные значения: ◦ **l2**: 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. ◦ **l2-3**: использует как MAC-адреса, так и IP-адреса для генерации хэша. Алгоритм совместим с IEEE 802.3ad. ◦ **l3-4**: используются IP-адреса и протоколы транспортного уровня (TCP или UDP) для генерации хэша. Алгоритм не всегда совместим с IEEE 802.3ad, так как в пределах одного и того же TCP- или UDP-взаимодействия могут передаваться как фрагментированные, так и нефрагментированные пакеты. Во фрагментированных пакетах порт источника и порт назначения отсутствуют. В результате в рамках одной сессии пакеты могут дойти до получателя не в том порядке, так как отправляются через разные интерфейсы.

Параметр	Описание
	• **interface**: интерфейсы, которые будут объединены в бонд.
iface-mode	Режим назначения IP-адреса: • **dhcp**: получение динамического IP-адреса по DHCP. • **manual**: без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса.
iface-type	Тип создаваемого интерфейса: • **l3** — Layer 3 интерфейс. • **mirror** — интерфейс зеркалирования трафика.
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся в следующем виде: **[<ip_address/mask>]** или **[<ip_address/mask> <ip_address/mask>]**, если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел); маска подсети задаётся в десятичном виде. **Важно!** Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса.
mtu	Указание размер MTU.

Обновление существующего бонд-интерфейса:

```
Admin/system@nodename# set network interface bond <bond-name>
```

Параметры, доступные для обновления, аналогичны параметрам создания бонд-интерфейс, кроме **interface-name**, **node-name** (изменение значений этих параметров недоступно).

Команда удаления бонд-интерфейса или его параметров:

```
Admin/system@nodename# delete network interface bond <bond-name>
```

Параметры, доступные для удаления:

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay server-address	IP-адрес сервера DHCP.
bonding interface	Интерфейсы, объединённые в бонд.

Чтобы отобразить информацию о всех бонд-интерфейсах:

```
Admin/system@nodename# show network interface bond
```

или об определённом интерфейсе:

```
Admin/system@nodename# show network interface bond <bond-name>
```

Шлюзы

Данный раздел находится на уровне **network gateway**.

Для добавления нового шлюза используется команда:

```
Admin/system@nodename# create network gateway
```

Доступные параметры:

Параметр	Описание
enabled	Включение/отключение шлюза: • **on**. • **off**.
name	Название шлюза.
description	Описание шлюза.
interface	Интерфейс, использующийся для выхода в Интернет.

Параметр	Описание
ip	IP-адрес шлюза.
node-name	Выбор узла кластера, для которого настраивается шлюз.
weight	Вес шлюза (чем больше вес, тем большая доля трафика идет через шлюз).
balancing	Режим балансировки - весь трафик в интернет будет распределен между шлюзами в соответствии с указанными весами: • **on**. • **off**.
default	Использование данного шлюза в качестве шлюза по умолчанию: • **on**. • **off**.

Обновление параметров шлюза:

```
Admin/system@nodename# set network gateway <gateway-name>
```

Список параметров, доступных для изменения, аналогичен списку, доступному при создании шлюза.

Команда для удаления шлюза:

```
Admin/system@nodename# delete network gateway <gateway-name>
```

Чтобы отобразить информацию о всех шлюзах:

```
Admin/system@nodename# show network gateway
```

или об определённом шлюзе:

```
Admin/system@nodename# show network gateway <gateway-name>
```

Настройка маршрутизации

В данном разделе описана настройка маршрутизации с использованием интерфейса командной строки. Настройка производится на уровне **network routes**.

Для добавления нового статического маршрута используется команда:

```
Admin/system@nodename# create network routes <parameters>
```

Далее указываются параметры:

Параметр	Описание
enabled	Включение/отключение использования статического маршрута: • **on**. • **off**.
name	Имя маршрута.
description	Описание маршрута.
node-name	Выбор узла кластера для настройки маршрутизации.
type	Тип маршрута: • **unicast** — стандартный тип маршрута. Пересылает трафик, адресованный на адреса назначения, через заданный шлюз. • **unreachable** — трафик отбрасывается. Источнику отправляется ICMP сообщение host unreachable (type 3 code 1). • **prohibit** — трафик отбрасывается. Источнику отправляется ICMP сообщение host unreachable (type 3 code 13). • **blackhole** — трафик отбрасывается (теряется), не сообщая источнику о том, что данные не достигли адресата.
destination-ip	IP-адрес подсети назначения; указывается в формате <ip/mask>.

Параметр	Описание
gateway	IP-адрес шлюза, через который будет доступна указанная подсеть; этот IP-адрес должен быть доступен с устройства.
interface	Интерфейс, через который будет добавлен маршрут.
metric	Метрика маршрута. Если маршрутов в данную сеть несколько: чем меньше метрика, тем более приоритетен маршрут.

Пример добавления статического маршрута:

```
Admin/system@nodename# create network routes name test_route
description "Test static route" destination-ip 192.168.200.0/2
4 gateway 192.168.100.100 interface port1 type unicast metric 1 enabled
on
Admin/system@nodename#

Admin/system@nodename# show network routes test_route

name              : test_route
description       : Test static route
enabled           : on
node-name         : testnode1
interface         : port1
type              : unicast
destination-ip    : 192.168.200.0/24
gateway           : 192.168.100.100
metric            : 1
```

Чтобы изменить параметры созданного ранее статического маршрута, используйте команду:

```
Admin/system@nodename# set network routes <route-name>
```

Параметры, доступные для изменения, представлены в таблице выше.

Используйте следующую команду для удаления статического маршрута:

```
Admin/system@nodename# delete network routes <route-name>
```

Пример удаления статического маршрута:

```
Admin/system@nodename# delete network routes test_route
```

Для отображения статических маршрутов:

```
Admin/system@nodename# show network routes
```

DNS-настройки

Настройка системных серверов DNS производится на уровне **network dns system-dns-servers**.

Для добавления новых DNS-серверов или обновления существующего списка используются следующие команды:

```
Admin/system@nodename# set network dns system-dns-servers ip [ <ip>
<ip> ... ]
```

Для удаления всего списка адресов серверов DNS:

```
Admin/system@nodename# delete network dns system-dns-servers
```

Для удаления определённых серверов:

```
Admin/system@nodename# delete network dns system-dns-servers ip [ <ip>
<ip> ... ]
```

Для отображения списка системных DNS-серверов используется команда:

```
Admin/system@nodename# show network dns
```

НАСТРОЙКА МОНИТОРИНГА

Настройка параметров мониторинга устройства

Настройка параметров мониторинга устройства в интерфейсе CLI производится в режиме конфигурации на уровне **monitoring**. Команды этого уровня позволяют управлять настройкой параметров SNMP устройства, правил мониторинга по SNMP, профилей безопасности для аутентификации SNMP-менеджеров, правилами оповещений. Подробнее о правилах мониторинга и оповещений читайте в разделе Оповещения.

Настройка параметров SNMP устройства

Для настройки параметров SNMP устройства используются команды на уровне **monitoring smnp-parameter**:

```
Admin/system@nodename# edit monitoring snmp-parameter <parameters>
```

Для редактирования доступны следующие параметры:

Параметр	Описание
agent-name	Название системы, используемое подсистемой управления SNMP.
location	Информация о физическом расположении SNMP-агента.
description	Описание системы.
Engine ID	Каждое устройство UserGate имеет уникальный идентификатор SNMPv3 Engine ID. По умолчанию Engine ID генерируется на основании имени узла UserGate. При редактировании Engine ID необходимо указать длину (**length**), тип и значение идентификатора. Длина может быть определена как фиксированная (не более 8 байт) или

Параметр	Описание
	динамическая (не более 27 байт). Фиксированная длина идентификатора применима только для типа **text**. Engine ID может быть сформирован в формате: • **ip4** — IPv4. • **ipv6** — IPv6. • **mac** — MAC-адрес. • **text** — Текст. • **octets** — Октеты.

Подробнее о параметрах SNMP устройства UserGate читайте в разделе SNMP.

Настройка правил мониторинга по SNMP

Для настройки правил мониторинга устройства по SNMP используются команды на уровне **monitoring smnp**:

```
Admin/system@nodename# edit monitoring snmp <parameters>
```

Для редактирования доступны следующие параметры:

Параметр	Описание
name	Название правила.
enabled	Включение/отключение правила
community	SNMP community — строка для идентификации сервера UserGate и сервера управления SNMP для версии SNMP v2c. Используйте только латинские буквы и цифры.
context	Необязательный параметр, определяющий SNMP context. Можно использовать только латинские буквы и цифры. На некоторых устройствах может быть несколько копий полного поддерева MIB. Например, на устройстве может быть создано несколько виртуальных маршрутизаторов. Каждый такой виртуальный маршрутизатор будет иметь полное поддерево MIB. В этом случае каждый виртуальный маршрутизатор может быть указан как контекст на сервере SNMP. Контекст определяется по имени. Когда клиент отправляет запрос, он может указать имя контекста. Если имя контекста не указано, будет запрошен контекст по умолчанию.

Параметр	Описание
version	Указывает версию протокола SNMP, которая будет использоваться в данном правиле. Возможны варианты SNMP v2c и SNMP v3.
query	При включении разрешает получение и обработку SNMP-запросов от SNMP-менеджера.
trap	При включении разрешает отправку SNMP-трапов на сервер, настроенный для приема оповещений.
trap-host	IP-адрес сервера для трапов. Данная настройка необходима только в случае, если необходимо отправлять трапы на сервер оповещений.
trap-port	Порт, на котором сервер слушает оповещения. Обычно это порт UDP 162. Данная настройка необходима только в случае, если необходимо отправлять трапы на сервер оповещений.
security-profile	Только для SNMP v3. Подробнее — в разделе Профили безопасности SNMP.
events	Выбор типов параметров, доступных для мониторинга по правилу.

Для работы SNMP-менеджера с устройством UserGate необходимо в свойствах зоны интерфейса, к которому будет осуществляться подключение по протоколу SNMP, разрешить сервис **SNMP** в настройках контроля доступа. Подробнее о настройке зон в CLI читайте в разделе Настройки сети.

Настройка профилей безопасности SNMP

Для настройки профилей безопасности ля аутентификации SNMP-менеджеров используются команды на уровне **monitoring smnp-security-profile**:

```
Admin/system@nodename# edit monitoring snmp-security-profile
<parameters>
```

Для редактирования доступны следующие параметры:

Параметр	Описание
name	Название профиля безопасности SNMP

Параметр	Описание
description	Описание профиля безопасности SNMP
username	Имя пользователя для аутентификации SNMP-менеджера.
auth-type	Выбор режима аутентификации SNMP-менеджера. Возможны варианты: • **none** — без аутентификации, без шифрования. • **no-encrypt** — с аутентификацией, без шифрования. • **encrypt** — с аутентификацией, с шифрованием. Наиболее безопасным считается режим работы authPriv.
auth-alg	Алгоритм, используемый для аутентификации. Возможно использовать: • **sha**; • **md5**; • **sha224**; • **sha256**; • **sha384**; • **sha512**.
auth-password	Пароль, используемый для аутентификации.
encrypt-alg	Алгоритм, используемый для шифрования. Возможно использовать DES и AES.
encrypt-password	Пароль, используемый для шифрования.

Настройка правил оповещений

Для настройки правил оповещений используются команды на уровне **monitoring alert-rules**:

```
Admin/system@nodename# edit monitoring alert-rules <parameters>
```

Для редактирования доступны следующие параметры:

Параметр	Описание
enabled	Включает/отключает данное правило.

Параметр	Описание
name	Название правила.
description	Описание правила.
notification-profile	Созданный ранее профиль оповещения.
sender	От кого будет приходить оповещение.
subject	Тема оповещения.
timeout	Тайм-аут, в течение которого сервер не будет отправлять сообщение при повторном срабатывании данного правила. Данная настройка позволяет предотвратить шторм сообщений при частом срабатывании правила оповещения.
events	События, для которых необходимо получать оповещения.
phones	Для SMPP-профиля. Группы номеров телефонов, куда отправлять SMS-оповещения.
emails	Для SMTP-профиля. Группы адресов email, на которые будут отправляться почтовые оповещения.

НАСТРОЙКА БИБЛИОТЕК

Настройка библиотек (Описание)

Настройка IP-адресов

Данный раздел находится на уровне **libraries ip-list**.

Для создания группы IP-адресов используется следующая команда:

```
Admin/system@nodename# create libraries ip-list <parameter>
```

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название списка адресов.
description	Описание списка.
threat-lvl	Уровень угрозы: • **very-low** — очень низкий уровень угрозы. • **low** — низкий уровень угрозы. • **medium** — средний уровень угрозы. • **high** — высокий уровень угрозы. • **very-high** — высокий уровень угрозы.
type	Тип списка: • **local** — локальный. • **updatable** — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (**url**). Периодичность обновления списка указывается параметром **shedule** в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".
lists	Выбор существующих IP-листов для добавления в создаваемый лист.
ips	IP-адреса или диапазон IP-адресов, которые необходимо включить в список. Указывается в формате: <ip>, <ip/mask> или <ip_range_start-ip_range_end>.

Для редактирования списка (список параметров, доступных для обновления, аналогичен списку параметров команды создания списка):

```
Admin/system@nodename# set libraries ip-list <ip-list-name> <parameter>
```

Чтобы добавить в список новые адреса:

```
Admin/system@nodename# set libraries ip-list <ip-list-name> [ <ip1>
<ip2> ... ]
```

Следующие команды используются для удаления всего списка адресов или IP-адресов, содержащихся в нём:

```
Admin/system@nodename# delete libraries ip-list <ip-list-name>
Admin/system@nodename# delete libraries ip-list <ip-list-name> ips
[ <ip1> <ip2>... ]
```

Команда отображения информации о всех имеющихся списках:

```
Admin/system@nodename# show libraries ip-list
```

Чтобы отобразить информацию об определённом списке, необходимо указать название интересующего списка IP-адресов:

```
Admin/system@nodename# show libraries ip-list <ip-list-name>
```

Также доступен просмотр содержимого списка IP-адресов:

```
Admin/system@nodename# show libraries ip-list <ip-list-name> items
```

Настройка почтовых адресов

Раздел находится на уровне **libraries email-list**.

Чтобы добавить новую группу почтовых адресов используется следующая команда:

```
Admin/system@nodename#& create libraries email-list <parameter>
```

Далее указываются параметры:

Параметр	Описание
name	Название группы почтовых адресов.
description	Описание группы почтовых адресов.
type	Тип списка: • **local** — локальный. • **updatable** — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (**url**). Периодичность обновления списка указывается параметром **shedule** в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".
emails	Почтовые адреса, которые необходимо добавить в данную группу.

Команда, предназначенная для редактирования информации о группе почтовых адресов:

```
Admin/system@nodename# set libraries email-list <email-list-name>
<parameter>
```

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании группы почтовых адресов.

Для удаления группы или почтовых адресов из неё используются следующие команды:

```
Admin/system@nodename# delete libraries email-list <email-list-name>
Admin/system@nodename# delete libraries email-list <email-list-name>
emails [ <email> ... ]
```

Следующие команды используются для просмотра информации о всех созданных группах, об определённых группах или для просмотра почтовых адресов, входящих в группу:

```
Admin/system@nodename# show libraries email-list
Admin/system@nodename# show libraries email-list <email-list-name>
Admin/system@nodename# show libraries email-list <email-list-name>
emails
```

Настройка номеров телефонов

Настройка раздела **Номера телефонов** производится на уровне **libraries phone-list**.

Для создания группы телефонных номеров:

```
Admin/system@nodename# create libraries phone-list <parameter>
```

Далее необходимо указать следующие данные:

Параметр	Описание
name	Название группы телефонных номеров.
description	Описание группы телефонных номеров.
type	Тип списка: • **local** — локальный.

Параметр	Описание
	• **updatable** — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (**url**). Периодичность обновления списка указывается параметром **shedule** в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".
phones	Номера телефонов, которые необходимо добавить в данную группу.

Для редактирования информации о группе телефонных номеров используется команда:

```
Admin/system@nodename# set libraries phone-list <phone-list-name>
<parameter>
```

Параметры, доступные для обновления, представлены в таблице выше.

Для удаления группы или номеров телефонов из неё используются следующие команды:

```
Admin/system@nodename# delete libraries phone-list <phone-list-name>
Admin/system@nodename# delete libraries phone-list <phone-list-name>
phones [ <phone> ... ]
```

Следующие команды используются для просмотра информации о всех созданных группах:

```
Admin/system@nodename# show libraries phone-list
```

или об определённых группах телефонных номеров:

```
Admin/system@nodename# show libraries phone-list <phone-list-name>
```

Для просмотра номеров, содержащихся в группе, используется команда:

```
Admin/system@nodename# show libraries phone-list <phone-list-name>
phones
```

Настройка профилей оповещений

Профили оповещений SMTP (по email) и SMPP (по SMS) настраиваются на уровне **libraries notification-profiles**.

Для добавления нового профиля оповещения SMTP:

```
Admin/system@nodename# create libraries notification-profiles smtp
<parameter>
```

Далее необходимо указать:

Параметр	Описание
name	Название профиля.
description	Описание профиля.
host	IP-адрес или FQDN сервера SMTP, который будет использоваться для отсылки почтовых сообщений.
port	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.
connection-security	Варианты безопасности отправки почты; возможны варианты: • **none**. • **starttls**.

Параметр	Описание
	• **ssl**.
authentication	Включение/отключение авторизации при подключении к серверу SMTP: • **on**. • **off**.
login	Имя учётной записи для подключения к SMTP-серверу.
password	Пароль учётной записи для подключения к SMTP-серверу.

Для создания профиля оповещения по SMS (SMPP):

```
Admin/system@nodename# create libraries notification-profiles smpp
<parameter>
```

Далее необходимо указать значения следующих параметров:

Параметр	Описание
name	Название профиля.
description	Описание профиля.
host	IP-адрес или FQDN сервера SMPP, который будет использоваться для отсылки SMS.
port	Порт TCP, который используется для подключения к серверу SMPP. Обычно для протокола SMPP используется порт 2775; при использовании SSL — 3550.
ssl	Включение/отключение шифрования SSL: • **on**. • **off**.
login	Имя учётной записи для подключения к SMPP-серверу.
password	Пароль учётной записи для подключения к SMPP-серверу.
phone-translation-rules	Правила трансляции телефонных номеров. Правила используются для соответствия требованиям провайдера.

Параметр	Описание
	Например, если необходимо заменить все номера, начинающиеся на +7, на 8: `Admin/system@nodename# set libraries notification-profiles smpp <profile-name> phone-translation-rules + [ +7¦8 ]`
source-ton	Тип номера (Type of Number) для источника сообщения: • **0** — Unknown (Неизвестный). • **1** — International (Международный). • **2** — National (Государственный). • **3** — Network Specific (Сетевой Специальный). • **4** — Subscriber Number (Номер абонента). • **5** — Alphanumeric (Алфавитно-цифровой). • **6** — Abbreviated (Сокращённый).
dest-ton	Тип номера (Type of Number) для адресата: • **0** — Unknown (Неизвестный). • **1** — International (Международный). • **2** — National (Государственный). • **3** — Network Specific (Сетевой Специальный). • **4** — Subscriber Number (Номер абонента). • **5** — Alphanumeric (Алфавитно-цифровой). • **6** — Abbreviated (Сокращённый).
source-npi	Индикатор схемы присвоения номеров (Numbering Plan Indicator) для источника: • **0** — Unknown. • **1** — ISDN/telephone numbering plan (E.163/E.164). • **3** — Data numbering plan (X.121). • **4** — Telex numbering plan (F.69). • **6** — Land Mobile (E.212). • **8** — National numbering plan. • **9** — Private numbering plan. • **10** — ERMES numbering plan (ETSI DE/PS 3 01-3). • **13** — Internet (IP). • **18** — WAP Client Id (to be defined by WAP Forum).

Параметр	Описание
dest-npi	Индикатор схемы присвоения номеров (Numbering Plan Indicator) для адресата: • **0** — Unknown. • **1** — ISDN/telephone numbering plan (E.163/E.164). • **3** — Data numbering plan (X.121). • **4** — Telex numbering plan (F.69). • **6** — Land Mobile (E.212). • **8** — National numbering plan. • **9** — Private numbering plan. • **10** — ERMES numbering plan (ETSI DE/PS 3 01-3). • **13** — Internet (IP). • **18** — WAP Client Id (to be defined by WAP Forum).

Для редактирования профиля оповещения используется команда:

```
Admin/system@nodename# set libraries notification-profiles <smtp |
smpp> <profile-name> <parameter>
```

Параметры профилей SMTP и SMPP, доступные для изменения, представлены в соответствующих таблицах выше.

Для удаления профиля:

```
Admin/system@nodename# delete libraries notification-profiles <smtp |
smpp> <profile-name>
```

Также для профилей оповещений SMPP доступно удаления правил трансляции номеров:

```
Admin/system@nodename# delete libraries notification-profiles smpp
<profile-name> phone-translation-rules [ phone1¦phone2 ]
```

Следующие команды предназначены для отображения информации о всех имеющихся профилях оповещений:

```
Admin/system@nodename# show libraries notification-profiles
```

о всех профилях одного типа:

```
Admin/system@nodename# show libraries notification-profiles <smtp |
smpp>
```

об определённом профиле оповещения:

```
Admin/system@nodename#show libraries notification-profiles <smtp |
smpp> <profile-name>
```

УПРАВЛЕНИЕ ОБЛАСТЯМИ

Настройка управляемых областей

Для возможности управление областями администратор UGMC должен выполнить следующие действия:

1. Создать область.
2. Создать профиль администратора с типом администратора области.
3. Создать администратора области.

Подробнее об управлении областями в UGMC читайте в разделе Управление областями.

Создание управляемой области

Настройка управляемых областей производится на уровне **realms**.

Для создания управляемой области используется команда:

```
Admin/system@nodename# create realm <parameters>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название управляемой области.
description	**Описание управляемой области.**
code-name	Код области. Состоит из нескольких букв и/или цифр. Код области необходимо указывать при входе в консоль для управления данной областью. Например, UG.
is-default	**Область по умолчанию. Если данная опция установлена, то при аутентификации в консоль необязательно указывать имя области через слэш.**
max-devices	Максимальное количество управляемых устройств UserGate NGFW в области.
max-ep-devices	Максимальное количество управляемых конечных устройств (UserGate Client) в области.

Пример создания управляемой области:

```
Admin/system@nodename# create realms name "Test realm" code-name
tstrlm1 is-default on max-devices 10 max-ep-devices 100
```

Пример команды для просмотра имеющихся управляемых областей:

```
Admin/system@nodename# show realms

Example realm
    name              : Example realm
    is-default        : off
    description       : Example realm created for demo purpose. Can be
changed or deleted if necessary.
    code-name         : EX
    num-devices       : 1
    num-ep-devices    : 0
    max-devices       : unlimited
    max-ep-devices    : unlimited

Test realm
    name              : Test realm
    is-default        : on
```

```
    code-name          : tstrlm1
    num-devices        : 0
    num-ep-devices     : 0
    max-devices        : 10
    max-ep-devices     : 100
```

Пример команды для редактирования параметров созданных ранее управляемых областей:

```
Admin/system@nodename# set realms "Test realm" max-devices 50
Admin/system@nodename# show realms "Test realm"

name               : Test realm
is-default         : off
code-name          : tstrlm1
num-devices        : 0
num-ep-devices     : 0
max-devices        : 50
max-ep-devices     : 100
```

Пример команды удаления созданной ранее управляемой области:

```
Admin/system@nodename# delete realms "Test realm"
```

Создание администратора управляемой области

Для управления созданной ранее областью необходимо создать администратора области.

Профиль администратора с типом администратора области создается, как описано в разделе Настройка прав доступа профилей администраторов.

Учетная запись администратора области создаются, как описано в разделе Настройка учетных записей администраторов.

РЕЖИМ АДМИНИСТРАТОРА УПРАВЛЯЕМОЙ ОБЛАСТИ

Режим администратора управляемой области (Описание)

После создания управляемой области и администратора области можно переключиться в режим управления данной областью. Для этого необходимо выйти из учетной записи администратора UGMC и заново зайти под учетной записью администратора управляемой области. Например, для входа по ssh в консоль управления областью **realm** для администратора области с учетной записью **realmadmin** необходимо указать следующее:

```
ssh realmadmin/realm@<UGMC-IP-address> -p 2200
```

После успешной аутентификации в CLI появится строка ожидания ввода команды (режим диагностики). Для просмотра текущих возможных значений или автодополнения необходимо использовать клавишу **Tab**. Доступны:

- **configure** — переход в режим конфигурации.
- **date** — просмотр текущих даты и времени на устройстве.
- **exit** — выход из командной строки.
- **show** — просмотр версии ПО UGOS и статистики по открытым сессиям TCP, UDP, ICMP.
- **clear** — очистить статистику по открытым сессиям.

Для отмены ввода текущей команды используется сочетание **Ctrl + C**; для просмотра истории команд — ↑, ↓.

Режим конфигурации администратора управляемой области

Для перехода в режим конфигурации используется команда:

```
realmadmin/realm@nodename> configure
```

После перехода в режим конфигурации командная строка будет выглядеть следующим образом:

```
realmadmin/realm@nodename#
```

Для просмотра подсказки о текущих возможных значениях или для автодополнения команд необходимо нажать клавишу **Tab**. В подсказке могут использоваться следующие вспомогательные символы:

***** — обязательное поле в командах create и ряде других команд;

+ — необязательное/вариативное поле;

> — вложенное поле, после его введения предыдущий список полей становится недоступным, появляется новый список полей, которые можно ввести.

Общая структура команд в режиме конфигурации

Команды интерфейса командной строки имеют следующую структуру:

```
<action> <level> <filter> <configuration_info>
```

где:

<action> — действие, которое необходимо выполнить.

<level> — уровень конфигурации; уровни соответствуют разделам веб-интерфейса управляемой области в UGMC.

<filter> — идентификатор объекта, к которому происходит обращение.

<configuration_info> — значение параметров, которые необходимо применить к объекту <filter>.

Наименование	Описание
<action>	В режиме конфигурации доступны следующие действия: • **create** — создание новых объектов. • **set** — редактирование всех объектов, а также включение различных параметров. • **show** — отображение текущих значений. Можно использовать на любом уровне конфигурации — будет отображено всё, что находится глубже текущего уровня. • **delete** — удаление объекта или параметра из списка параметров. • **edit** — переход на какой-либо уровень конфигурации. Уровень конфигурации будет отображён под командной строкой. • **end** — переход на один уровень выше. • **top** — возврат на самый верхний уровень конфигурации. • **import** — импорт конфигурации. • **export** — экспорт конфигурации. • **go** — переход в режим настройки параметров шаблона управляемых устройств. • **exit** — выход из режима конфигурации.
<level>	Уровни в командной строке повторяют веб-интерфейс консоли управления областью: • **ngfw** — соответствует разделу веб-интерфейса **NGFW**. • **endpoint** — соответствует разделу веб-интерфейса **Конечные устройства**. • **logan** — соответствует разделу веб-интерфейса **LogAn**. • **settings** — соответствует разделам веб-интерфейса **Центр управления** — **Настройки, Администраторы, Профили аутентификации**. • **users** — соответствует разделам веб-интерфейса **Центр управления** — **Каталог пользователей**.
<filter>	Идентификатор объекта, к которому происходит обращение. Идентификация происходит по имени объекта.
<configuration_info>	Набор пар: параметр-аргумент. Параметр — имя поля, для которого нужно установить аргумент. Аргумент может быть одиночным или множественным.

Наименование	Описание
	Одиночный аргумент — значение, соответствующее параметру. Если строка содержит пробелы, то необходимо использовать кавычки. **Множественные аргументы** используются для установки множества значений какого-либо параметра; записываются в квадратных скобках и разделяются пробелами.

Общие настройки консоли управляемой области

Общие настройки консоли управляемой области задаются на уровне **settings general**. Структура команды для настройки одного из разделов (<settings-module>):

```
realmadmin/realm@nodename# set settings general <settings-module>
```

Доступна настройка следующих разделов:

Параметр	Описание
admin-console	Настройки интерфейса (уровень **settings general admin-console**): • **timezone**: 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 • **api-session-lifetime**: время ожидания сеанса администратора в секундах.
change-tracker	Настройка учета изменений (уровень settings general change-tracker): • **enabled**: включение/отключение учёта изменений. ◦ **on**. ◦ **off**. • **event-tracker-types**: типы изменений задаются администратором. Для удаления типа изменения используется команда:

Параметр	Описание
	`realmadmin/realm@nodename# delete settings general change-tracker event-tracker-types [ type1 ... ]`

Администраторы управляемой области

Администратор управляемой области может сам создать дополнительных администраторов своей области аналогично командам, описанным в разделах Настройка прав доступа профилей администраторов и Настройка учетных записей администраторов.

Настройка данного раздела производится на уровне **settings administrators**. В разделе описаны настройка настройка администраторов и их профилей.

Настройка учётных записей администраторов

Настройка учётных записей администраторов производится на уровне **settings administrators administrators**.

Для создания учётной записи администратора используется следующая команда:

```
realmadmin/realm@nodename# create settings administrators
administrators
```

Далее необходимо указать тип учётной записи администратора (локальный, пользователь LDAP, группа LDAP, с профилем аутентификации) и установить соответствующие параметры:

Параметр	Описание
local	Добавить локального администратора: • **enabled**: включение/отключение учётной записи администратора: ◦ **on**. ◦ **off**. • **login**: логин администратора.

Параметр	Описание
	• **display-name**: отображаемое имя администратора. • **description**: описание учётной записи администратора. • **admin-profile**: профиль администратора. Создание профилей администраторов рассмотрено далее. • **password**: пароль администратора.
ldap-user	Добавить пользователя из существующего домена (необходим корректно настроенный LDAP-коннектор; подробнее читайте в разделе Настройка LDAP-коннектора): • **enabled**: включение/отключение учётной записи администратора: ◦ **on**. ◦ **off**. • **login**: логин администратора в формате **domain\user**. Структура команды при указании данного параметра: • **display-name**: отображаемое имя администратора. • **connector**: название сконфигурированного ранее LDAP-коннектора. • **description**: описание учётной записи администратора. • **admin-profile**: профиль администратора. Создание профилей администраторов рассмотрено далее. `realmadmin/realm@nodename# create settings administrators administrators ldap-user admin-profile "test profile 1" connector "LDAP connector" description "Admin as domain user" login testd.local\user1 enabled on`
ldap-group	Добавить группу пользователей из существующего домена (необходим корректно настроенный LDAP-коннектор; подробнее читайте в разделе Настройка LDAP-коннектора): • **enabled**: включение/отключение учётной записи администратора: ◦ **on**. ◦ **off**. • **login**: логин администратора • **display-name**: отображаемое имя администратора. • **connector**: название используемого LDAP-коннектора.

Параметр	Описание
	• **description**: описание учётной записи администратора. • **admin-profile**: профиль администратора. Создание профилей администраторов рассмотрено далее. `realmadmin/realm@nodename# create settings administrators administrators ldap-group admin-profile "test profile 1" connector "LDAP connector" description "Domain admin group" login testd.local\users enabled on`
admin-auth-profile	Добавить администратора с профилем аутентификации (необходимы корректно настроенные серверы аутентификации; подробнее читайте в разделе Настройка серверов аутентификации): • **enabled**: включение/отключение учётной записи администратора: ◦ **on**. ◦ **off**. • **login**: логин администратора. • **display-name**: отображаемое имя администратора. • **description**: описание учётной записи администратора. • **admin-profile**: профиль администратора. Создание профилей администраторов рассмотрено далее. • **auth-profile**: выбор профиля аутентификации из созданных ранее; подробнее о профилях аутентификации читайте в разделе Настройка профилей аутентификации.

Для редактирования параметров профиля используется команда:

```
realmadmin/realm@nodename# set settings administrators administrators
<admin-type> <admin-login>
```

Параметры для редактирования аналогичны параметрам создания профиля администратора.

Для отображения информации о всех учётных записях администраторов:

```
realmadmin/realm@nodename# show settings administrators administrators
```

Для отображения информации об определённой учётной записи администратора:

```
realmadmin/realm@nodename# show settings administrators administrators
<admin-type> <admin-login>
```

Настройка прав доступа профилей администраторов

Настройка прав доступа профилей администраторов производится на уровне **settings administrators profiles**.

Для создания профиля администратора используется следующая команда:

```
realmadmin/realm@nodename# create settings administrators profiles
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля администратора.
description	Описание профиля администратора.
realm-permissions	Права доступа к управлению области: • **no-access**: нет доступа. • **read**: только чтение. • **write**: чтение и запись.
ngfw-permissions	Права доступа к управлению устройствами NGFW: • **no-access**: нет доступа. • **read**: только чтение. • **write**: чтение и запись.
ep-permissions	Права доступа к управлению конечными устройствами: • **no-access**: нет доступа.

Параметр	Описание
	• **read**: только чтение. • **write**: чтение и запись.
logan-permissions	Права доступа к управлению устройствами LogAn: • **no-access**: нет доступа. • **read**: только чтение. • **write**: чтение и запись.

Для редактирования профиля используется команда:

```
realmadmin/realm@nodename# set settings administrators profiles
<profile-name> <parameter>
```

Параметры для редактирования аналогичны параметрам создания профиля администратора.

Для просмотра информации о всех профилях администраторов:

```
realmadmin/realm@nodename# show settings administrators profiles
```

Для отображения информации об определённом профиле:

```
realmadmin/realm@nodename# show settings administrators profiles
<profile-name>
```

Чтобы удалить профиль администратора:

```
realmadmin/realm@nodename# delete settings administrators profiles
<profile-name>
```

Просмотр сессий администраторов текущей области (возможен просмотр сессии отдельного администратора: необходимо из предложенного списка выбрать IP-адрес, с которого была произведена авторизация):

```
realmadmin/realm@nodename# show settings administrators admin-sessions
```

Серверы аутентификации управляемой области

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

Раздел **Серверы аутентификации** позволяет произвести настройку LDAP-коннектора, серверов RADIUS, TACACS+. Настройка серверов аутентификации производится на уровне **users auth-server** и будет рассмотрена далее в соответствующих разделах.

Настройка LDAP-коннектора

Настройка LDAP-коннектора производится на уровне **users auth-server ldap**.

Для создания LDAP-коннектора используется команда:

```
realmadmin/realm@nodename# create users auth-server ldap <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя LDAP-коннектора.
enabled	Включение/отключение сервера аутентификации.
description	Описание LDAP-коннектора.
ssl	Определяет: • **on** — использование SSL-соединения для подключения к LDAP-серверу. • **off** — подключение к LDAP-серверу без использования SSL-соединения.
address	IP-адрес контроллера или название домена LDAP.

Параметр	Описание
bind-dn	Имя пользователя, которое будет использоваться для подключения к серверу; указывается в формате DOMAIN\username или username@domain. Пользователь должен быть заведён в домене.
password	Пароль пользователя для подключения к домену.
domains	Список доменов, которые обслуживаются указанным контроллером домена.
search-roots	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. Если пути поиска не указаны, то поиск производится по всему каталогу, начиная от корня.

Для редактирования информации о существующем LDAP-коннекторе используется команда:

```
realmadmin/realm@nodename# set users auth-server ldap <ldap-server-
name> <parameter>
```

Параметры, доступные для обновления, аналогичны параметрам создания LDAP-коннектора.

Команда для отображения информации о LDAP-коннекторе:

```
realmadmin/realm@nodename# show users auth-server ldap <ldap-server-
name>
```

Примеры команд создания и редактирования LDAP-коннектора:

```
realmadmin/realm@nodename# create users auth-server ldap name "New LDAP
connector" ssl on address 10.10.0.10 bind-dn ug@testd.local password
12345 domains [ testd.local ] search-roots [ dc=testd,dc=local ]
enabled on
realmadmin/realm@nodename# show users auth-server ldap "New LDAP
connector"

name             : New LDAP connector
```

```
enabled          : on
ssl              : on
address          : 10.10.0.10
bind-dn          : ug@testd.local
domains          : testd.local
search-roots     : dc=testd,dc=local
keytab_exists    : off
realmadmin/realm@nodename# set users auth-server ldap "New LDAP
connector" description "New LDAP connector description"
realmadmin/realm@nodename# show users auth-server ldap "New LDAP
connector"

name             : New LDAP connector
description      : New LDAP connector description
enabled          : on
ssl              : on
address          : 10.10.0.10
bind-dn          : ug@testd.local
domains          : testd.local
search-roots     : dc=testd,dc=local
keytab_exists    : off
```

Для удаления LDAP-коннектора используется команда:

```
realmadmin/realm@nodename# delete users auth-server ldap <ldap-server-
name> <parameter>
```

Также возможно удаления отдельных параметров LDAP-коннектора. Для удаления доступны следующие параметры:

- **domains**.
- **search-roots**.

Настройка RADIUS-сервера

Настройка RADIUS-сервера производится на уровне **users auth-server radius**.

Для создания сервера аутентификации RADIUS используется команда со следующей структурой:

```
realmadmin/realm@nodename# create users auth-server radius <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя RADIUS-сервера.
enabled	Включение/отключение сервера аутентификации.
description	Описание сервера аутентификации.
secret	Общий ключ, используемый протоколом RADIUS для аутентификации.
addresses	IP-адрес и UDP-порт, на котором сервер RADIUS слушает запросы (по умолчанию порт 1812); указывается в формате <ip:port>.

Команда для обновления информации о сервере RADIUS:

```
realmadmin/realm@nodename# set users auth-server radius <radius-server-
name> <parameter>
```

Параметры, которые могут быть обновлены, соответствуют параметрам, указание которых возможно при создании сервера аутентификации.

Команда для отображения информации о RADIUS-сервере:

```
realmadmin/realm@nodename# show users auth-server radius <radius-
server-name>
```

Примеры команд создания и редактирования RADIUS-сервера:

```
realmadmin/realm@nodename# create users auth-server radius name "New
RADIUS server" addresses [ 10.10.0.9:1812 ] secret 12345 enabled on
realmadmin/realm@nodename# show users auth-server radius "New RADIUS
server"

name           : New RADIUS server
enabled        : on
```

```
addresses      :
    host    : 10.10.0.9
    port    : 1812
realmadmin/realm@nodename# set users auth-server radius "New RADIUS
server" description "New RADIUS server description"
realmadmin/realm@nodename# show users auth-server radius "New RADIUS
server"

name           : New RADIUS server
description    : New RADIUS server description
enabled        : on
addresses      :
    host    : 10.10.0.9
    port    : 1812
```

Для удаления сервера:

```
realmadmin/realm@nodename# delete users auth-server radius <radius-
server-name> <parameter>
```

Также возможно удаления отдельных параметров RADIUS-сервера. Для удаления доступны следующие параметры:

- **addresses**.

Настройка сервера TACACS+

Настройка сервера TACACS+ производится на уровне **users auth-server tacacs**.

Для создания сервера аутентификации TACACS+ используется команда со следующей структурой:

```
realmadmin/realm@nodename# create users auth-server tacacs <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя сервера TACACS+.

Параметр	Описание
enabled	Включение/отключение сервера.
description	Описание сервера аутентификации.
secret	Общий ключ, используемый протоколом TACACS+ для аутентификации.
address	IP-адрес сервера TACACS+.
port	UDP-порт, на котором сервер TACACS+ слушает запросы на аутентификацию. По умолчанию это порт UDP 1812.
single-connection	Использовать одно TCP-соединение для работы с сервером TACACS+.
timeout	Время ожидания сервера TACACS+ для получения аутентификации. По умолчанию 4 секунды.

Команда для редактирования информации о сервере TACACS+:

```
realmadmin/realm@nodename# set users auth-server tacacs <tacacs-server-
name> <parameter>
```

Параметры, которые могут быть обновлены, соответствуют параметрам, указание которых возможно при создании сервера аутентификации.

Команда для отображения информации о сервере TACACS+:

```
realmadmin/realm@nodename# show users auth-server tacacs <tacacs-
server-name>
```

Примеры команд для создания и редактирования сервера TACACS+:

```
realmadmin/realm@nodename# create users auth-server tacacs address
10.10.0.11 name "New TACACS+ server" port 1812 secret 12345 enabled on
realmadmin/realm@nodename# show users auth-server tacacs "New TACACS+
server"

name                  : New TACACS+ server
enabled               : on
```

```
address              : 10.10.0.11
port                 : 1812
single-connection    : off
timeout              : 4
realmadmin/realm@nodename#set users auth-server tacacs "New TACACS+
server" description "New TACACS+ server description"
realmadmin/realm@nodename# show users auth-server tacacs "New TACACS+
server"

name                 : New TACACS+ server
description          : New TACACS+ server description
enabled              : on
address              : 10.10.0.11
port                 : 1812
single-connection    : off
timeout              : 4
```

Для удаления сервера:

```
realmadmin/realm@nodename# delete users auth-server tacacs <tacacs-
server-name>
```

Профили аутентификации управляемой области

Профиль позволяет определить набор способов аутентификации пользователей в консоли администрирования UserGate.

Настройка профилей аутентификации производится на уровне **users auth-profile**.

Для создания профиля аутентификации используется следующая команда:

```
realmadmin/realm@nodename# create users auth-profile <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля.
description	Описание профиля.
auth-methods	Метод аутентификации: • **ldap**: аутентификация с использованием LDAP-коннектора. • **radius**: аутентификация с использованием RADIUS-сервера. • **tacacs**: аутентификация с использованием сервера TACACS+.
expiration-time	Время жизни авторизованного пользователя; указывается в секундах. Через указанный промежуток времени пользователь перейдёт в статус Unknown user; необходима повторная авторизация пользователя.
idle-time	Время бездействия до отключения; указывается в секундах. Через указанный промежуток времени при отсутствии активности пользователь перейдёт в статус Unknown user.
lockout-time	Время, на которое блокируется учетная запись пользователя при достижении указанного числа неудачных попыток аутентификации; указывается в секундах.
max-attempts	Число неудачных попыток аутентификации до блокировки учётной записи пользователя.

Команда для редактирования настроек профилей аутентификации:

```
realmadmin/realm@nodename# set users auth-profile <auth-profile-name>
<parameter>
```

Для обновления доступен список параметров, аналогичный списку параметров команды **create**.

Пример создания и редактирования профиля аутентификации пользователя:

```
realmadmin/realm@nodename# create users auth-profile name "New LDAP
auth profile" auth-methods ldap [ "New LDAP connector" ]
realmadmin/realm@nodename# show users auth-profile "New LDAP auth
profile"
```

```
name                : New LDAP auth profile
max-attempts        : 5
idle-time           : 900
expiration-time     : 86400
lockout-time        : 300
mfa                 : none
auth-methods        :
    http-basic          : off
    local-user-auth     : off
    policy-accept       : off
    ldap                : New LDAP connector
realmadmin/realm@nodename# set users auth-profile "New LDAP auth
profile" description "New LDAP auth profile description"
realmadmin/realm@nodename# show users auth-profile "New LDAP auth
profile"

name                : New LDAP auth profile
description         : New LDAP auth profile description
max-attempts        : 5
idle-time           : 900
expiration-time     : 86400
lockout-time        : 300
mfa                 : none
auth-methods        :
    http-basic          : off
    local-user-auth     : off
    policy-accept       : off
    ldap                : New LDAP connector
```

Через интерфейс командной строки возможно удаления всего профиля или отдельных способов аутентификации, заданных в профиле. Для этого используются следующие команды.

Для удаления профиля аутентификации:

```
realmadmin/realm@nodename# delete users auth-profile <auth-profile-
name>
```

Для удаления методов аутентификации, заданных в профиле, необходимо указать метод аутентификации (доступные методы авторизации перечислены в таблице выше):

```
realmadmin/realm@nodename# delete users auth-profile <auth-profile-
name> auth-methods <auth-metod>
```

Каталоги пользователей управляемой области

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

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

Создание и настройка каталога пользователей производится на уровне **users catalogs ldap**.

Для создания каталога используется команда:

```
realmadmin/realm@nodename# create users catalogs ldap <parameter>
```

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя LDAP-коннектора.
enabled	Включение/отключение сервера аутентификации.
description	Описание LDAP-коннектора.
ssl	

Параметр	Описание
	Определяет: • **on** — использование SSL-соединения для подключения к LDAP-серверу. • **off** — подключение к LDAP-серверу без использования SSL-соединения.
address	IP-адрес контроллера или название домена LDAP.
bind-dn	Имя пользователя, которое будет использоваться для подключения к серверу; указывается в формате DOMAIN\username или username@domain. Пользователь должен быть заведён в домене.
password	Пароль пользователя для подключения к домену.
domains	Список доменов, которые обслуживаются указанным контроллером домена.
search-roots	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. Если пути поиска не указаны, то поиск производится по всему каталогу, начиная от корня.

Для редактирования информации о существующем каталоге используется команда:

```
realmadmin/realm@nodename# set users catalogs ldap <ldap-server-name>
<parameter>
```

Параметры, доступные для обновления, аналогичны параметрам создания каталога.

Команда для отображения информации о каталоге пользователей:

```
realmadmin/realm@nodename# show users catalogs ldap <ldap-server-name>
```

Для удаления каталога используется команда:

```
realmadmin/realm@nodename# delete users catalogs ldap <ldap-server-
name> <parameter>
```

Также возможно удаления отдельных параметров LDAP-коннектора. Для удаления доступны следующие параметры:

- **domains**.
- **search-roots**.

Управление межсетевыми экранами UserGate

Для централизованного управления межсетевыми экранами UserGate (NGFW) в управляемой области необходимо создать шаблоны и группы шаблонов, описывающие настройки NGFW, затем добавить управляемые NGFW и применить к ним созданные ранее шаблоны.

В интерфейсе CLI создание шаблонов, групп шаблонов и добавление управляемых устройств NGFW происходит на уровне **ngfw**.

Шаблоны устройств

Для создания шаблона NGFW используется команда:

```
realmadmin/realm@nodename# create ngfw template <name, description>
```

Для редактирования названия/описания шаблона NGFW используется команда:

```
realmadmin/realm@nodename# set ngfw template <name, description>
```

Для просмотра созданных ранее шаблонов NGFW используется команда:

```
realmadmin/realm@nodename# show ngfw template <template-name>
```

Для удаления созданных ранее шаблонов NGFW используется команда:

```
realmadmin/realm@nodename# delete ngfw template <template-name>
```

После создания шаблона NGFW можно начать производить настройку его параметров. Для этого необходимо перейти в режим настройки параметров шаблона управляемых устройств следующей командой:

```
realmadmin/realm@nodename# go ngfw-template <template-name>
```

В режиме настройки параметров шаблона доступны те же команды настройки параметров NGFW, которые определены в разделе Интерфейс командной строки Руководства администратора NGFW.

При настройке параметров следует придерживаться следующих правил:

1. Если значение настройки не определено в шаблоне, то ничего передаваться в NGFW не будет. В данном случае в NGFW будет использована либо настройка по умолчанию, либо настройка, которую указал локальный администратор NGFW.

2. Если настройка параметра выполнена в шаблоне, то эта настройка переопределит значение этой же настройки, назначенной локальным администратором.

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

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

- общие настройки устройства;
- настройки сетевых интерфейсов.

3. Правила политик не переопределяют правила, созданные локальным администратором, а добавляются к ним в виде пре- и пост- правил. Подробно о применении правил смотрите раздел данного руководства Шаблоны и группы шаблонов.

4. При настройке сетевых интерфейсов первый физический интерфейс, доступный для конфигурирования — это **port1**. Интерфейс **port0** нельзя настроить с помощью средств UGMC, он всегда настраивается локальным

администратором и необходим для обеспечения первичной связи управляемых устройств с UGMC.

5. При настройке сетевых интерфейсов возможно создать интерфейс и оставить его конфигурирование локальному администратору. Для этого необходимо активировать параметр **on-device** (**on-device on**) в настройках интерфейса.

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 NGFW. Для использования библиотек в политиках UGMC, необходимо предварительно добавить элементы в эти библиотеки. Элементы библиотек не участвуют в синхронизации: если список был создан, но не используется в политиках, то данный список не появится в разделе библиотек NGFW.

7. Рекомендуется создавать отдельные шаблоны для разных групп настроек, это позволит избежать конфликтов настроек при объединении шаблонов в группы шаблонов и упростит понимание результирующей настройки, которая будет применена к управляемым устройствам. Например, шаблон сетевых настроек, шаблон правил межсетевого экрана, шаблон правил контентной фильтрации, шаблон библиотек и т.д.

Группы шаблонов

Группы шаблонов объединяют несколько шаблонов в единую конфигурацию, которая применяется к управляемому устройству. Результирующие настройки, применяемые к устройству, формируются в результате слияния всех настроек шаблонов, входящих в группу шаблонов, с учетом расположения шаблонов внутри группы.

Для создания группы шаблонов NGFW используется команда:

```
realmadmin/realm@nodename# create ngfw groups name <group-name>
description <group description> templates [ teplate1-name template2-
name ... ]
```

Для редактирования группы шаблонов NGFW используется команда:

```
realmadmin/realm@nodename# set ngfw groups name <group-name>
<description, templates>
```

Для просмотра созданных ранее групп шаблонов NGFW используется команда:

```
realmadmin/realm@nodename# show ngfw groups <group-name>
```

Для удаления созданных ранее групп шаблонов NGFW используется команда:

```
realmadmin/realm@nodename# delete ngfw groups <group-name>
```

В созданной ранее группе шаблонов возможно удаление входящих в нее шаблонов:

```
realmadmin/realm@nodename# delete ngfw groups <group-name> templates
[ template-name template-name ... ]
```

Добавление NGFW под управление UGMC

Группа шаблонов всегда применяется к одному или нескольким управляемым устройствам UserGate NGFW. Для добавления управляемого NGFW в UGMC необходимо выполнить следующие шаги:

1. Обеспечить доступ от управляемого NGFW до UGMC, для этого на сервере UGMC необходимо разрешить сервис **Management** в свойствах контроля доступа зоны, к которой подключены управляемые устройства

2. Создать объект управляемого устройства.

3. Связать созданный объект управляемого устройства с реальным устройством UserGate NGFW.

Для обеспечения доступа от управляемого NGFW до UGMC необходимо в режиме администратора UGMC выполнить следующую команду:

```
Admin/system@nodename# set network zone <zone-nfme> enabled-services
[ Management ]
```

Для создания объекта управляемого устройства используется команда:

```
realmadmin/realm@nodename# create ngfw devices <parameters>
```

Необходимо указать следующие параметры:

Параметр	Описание
enabled	Включает объект управляемого устройства. Если объект управляемого устройства включен, то он занимает одну лицензию.
name	Название для управляемого устройства. Можно вводить произвольное название.
description	Описание управляемого устройства.
templates-group	Группа шаблонов, настройки которой следует применить к этому управляемому устройству.
sync-mode	Выбор режима синхронизации настроек группы шаблонов к устройству. Возможны 3 варианта: • **auto** — автоматическая синхронизация. При изменении любой настройки из любого шаблона, включенного в группу шаблонов, примененную к управляемому устройству, это изменение применяется к NGFW без задержек. • **disabled** — синхронизация выключена. • **manual** — режим синхронизации, при котором настройки применяются однократно при запросе синхронизации.

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

1. Получить Код устройства

2. Указать IP-адрес сервера UGMC и ввести уникальный код устройства

Код созданного объекта управляемого устройства (**device-code**) можно посмотреть следующей командой:

```
realmadmin/realm@nodename# show ngfw devices <device-name>

name                          : <device-name>
enabled                       : on
```

```
device-code                  : 9W8W14UC
templates-group              : <template-group-name>
...
```

В консоли управляемого устройства NGFW необходимо добавить IP-адрес управляющего UGMC и указать код созданного объекта управляемого устройства:

```
Admin@ngfw-nodename# set settings general management-center mc-address
<ugmc-ip-address> device-code 9W8W14UC enabled on
```

Проверить подключение на стороне UGMC можно командой просмотра управляемого устройства:

```
realmadmin/realm@nodename# show ngfw devices <device-name>
```

Кластеризация UserGate NGFW с помощью UGMC

Кластер конфигурации

Создание кластера конфигурации, управляемого из UGMC, практически идентично созданию отдельностоящего 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.

Первоначальная настройка на первом узле кластера должна быт выполнена, как описано в разделе Первоначальная инициализация Руководства администратора NGFW.

Настройка зоны, через которую будет осуществляться репликация кластера, на первом узле кластера должна быть выполнена, как указано в разделе Настройка сети Руководства администратора NGFW. Необходимо разрешить сервисы **ha** и A**dmin Console** в соответствующей зоне.

Настройка IP-адреса на первом узле кластера, который будет использоваться для связи с другими узлами кластера, производится как указано в разделе Настройка кластеров Руководства администратора NGFW:

```
Admin@ngfw-nodename# set settings device-mgmt configuration-cluster
```

Генерация секретного кода на первом узле кластера производится как указано в разделе Настройка кластеров Руководства администратора NGFW:

```
Admin@ngfw-nodename# execute configurate-cluster generate-secret-key
```

Добавление первого узла кластера под управление UGMC производится как указано в предыдущей главе Добавление NGFW под управление UGMC.

Добавление в кластер конфигурации второго и последующих узлов возможно только при первоначальной инициализации этих узлов. Подробнее читайте в разделе Первоначальная инициализация Руководства администратора NGFW.

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.

Кластер отказоустойчивости

Узлы 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:

1. Наличие кластера конфигурации.

2. Наличие управляемых из UGMC интерфейсов. Виртуальные IP-адреса могут быть назначены только на интерфейсы, которые созданы в шаблонах UGMC.

3. Выполнение всех требований, предъявляемых к узлам, при создании кластера отказоустойчивости без использования UGMC. Подробно о кластерах отказоустойчивости описано в разделе Кластеризация и отказоустойчивость в Руководстве администратора NGFW.

Для создания кластера отказоустойчивости необходимо выполнить следующие шаги:

1. В одном из шаблонов UGMC, где настроены зоны для управляемых устройств, разрешить сервис VRRP для всех зон, где планируется добавлять кластерный

виртуальный IP-адрес. Подробнее о настройке зон читайте в разделе Настройка сети Руководства администратора NGFW.

```
realmadmin/realm@nodename# go ngfw-template <template-name>

realmadmin/realm@nodename# set network zone name <zone-name> enabled-
services [ VRRP ]
Template: <ntmplate-name>
```

2. В одном из шаблонов UGMC указать параметры кластера отказоустойчивости:

```
realmadmin/realm@nodename# create settings device-mgmt ha-clusters
<parameters>
Template: <template-name>
```

3. Если предполагается использовать аутентификацию с помощью Captive-портала, то необходимо, чтобы системные имена auth.captive и logout.captive, которые используются процедурами аутентификации в Captive, определялись в IP-адрес, назначенный в качестве кластерного виртуального адреса. Данную настройку можно выполнить в одном из шаблонов UGMC, в разделе **settings general**.

```
realmadmin/realm@nodename# set settings general modules auth-captive
sync on value <domain_name>

realmadmin/realm@nodename# set settings general modules logout-captive
sync on value <domain_name>
```

Параметры отказоустойчивого кластера:

Параметр	Описание
enabled	Включение/отключение отказоустойчивого кластера.
name	Название отказоустойчивого кластера.
description	Описание отказоустойчивого кластера.
mode	

Параметр	Описание
	Выбор режима работы кластера: • **active-passive**: режим работы Актив-Пассив (один из серверов выступает в роли Мастер-узла, обрабатывающего трафик, а остальные — в качестве резервных). • **active-active**: режим работы Актив-Актив (один из серверов выступает в роли Мастер-узла, распределяющего трафик на все остальные узлы кластера).
session-sync	Настройка синхронизации пользовательских сессий в кластере: • **off** — отключение синхронизации пользовательских сессий. • **on** — включение синхронизации пользовательских сессий. • **ha-cluster-id:** ◦ <num> — мультикаст идентификатор кластера (может принимать значения от 0 до 8). Синхронизация пользовательских сессий (кроме сессий, использующих прокси-сервер, например, трафик HTTP/S) включится автоматически.
session-sync-all	Включение/отключение режима синхронизации всех пользовательских сессий, включая UDP/ICMP сессии. В случае, если этот параметр не активирован, а настройка session-sync активирована, синхронизироваться будут только TCP сессии.
excluded-sync-ips	Указание IP-адресов, с которыми отключена синхронизация всех пользовательских сессий.
virtual-router-id	Идентификатор виртуального маршрутизатора (VRID).
nodes	Выбор узлов кластера конфигурации для объединения их в кластер отказоустойчивости.
virtual-ips	Задание виртуального IP-адреса для кластера и выбор рабочего интерфейса для каждого узла. Доступные параметры для <virtual-ips-filter>: • **new**: создать виртуальный IP-адрес для заданного кластера.

Параметр	Описание
	• <**ip**>: изменить данные для выбранного виртуального адреса. Доступные параметры для <virtual-ip-info>: • **ip**: задать IP-адрес для кластера отказоустойчивости (указывается в формате IP/mask). • **ha-interfaces**: задать интерфейсы для узлов кластера (указываются в формате node-name/interface).

Управление обновлениями управляемых устройств

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

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

Обновление ПО

Порядок установки обновлений, следующий:

1. Загрузить обновления в репозитарий UGMC. Управление загрузками обновлений в репозиторий UGMC управляется командой:

```
realmadmin/realm@nodename# set settings general updates-schedule
software
```

Подробнее — в главе Общие настройки в Руководстве администратора UGMC.

2, Утвердить обновление для всех или для конкретных устройств:

```
realmadmin/realm@nodename# set ngfw software-updates <sw-update-name>
devices <device-name>
```

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

Обновление библиотек

Библиотеки — это обновляемые базы ресурсов, предоставляемых по подписке клиентам UserGate (база категорий URL-фильтрации, сигнатуры СОВ, списки IP-адресов, URL, MIME-типов, морфологические базы и другие). Эти обновления выкладываются в репозитарий UserGate, откуда они уже доступны для скачивания UserGate NGFW. Если NGFW подключен к управлению через UGMC, то он проверяет наличие обновлений на сервере UGMC, который сам будет являться репозитарием. Репозитарий UserGate при этом будет использован сервером UGMC для получения новых обновлений. По умолчанию UGMC проверяет и скачивает обновления библиотек автоматически.

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

Для настройки скачивания обновлений в UGMC из репозитария UserGate используется следующая команда:

```
realmadmin/realm@nodename#set ngfw libraries-updates <library-name>
download <auto/manual>
```

Управление конечными устройствами UserGate

Для централизованного управления конечными устройствами UserGate в управляемой области необходимо создать шаблоны и группы шаблонов, описывающие настройки конечных устройств, затем добавить управляемые конечные устройства и применить к ним созданные ранее шаблоны.

В интерфейсе CLI создание шаблонов, групп шаблонов и добавление управляемых конечных устройств происходит на уровне **endpoint**.

Шаблоны устройств

Для создания шаблона конечных устройств используется команда:

```
realmadmin/realm@nodename# create endpoint template <name, description>
```

Для редактирования названия/описания шаблона конечных устройств используется команда:

```
realmadmin/realm@nodename# set endpoint template <name, description>
```

Для просмотра созданных ранее шаблонов конечных устройств используется команда:

```
realmadmin/realm@nodename# show endpoint template <template-name>
```

Для удаления созданных ранее шаблонов конечных устройств используется команда:

```
realmadmin/realm@nodename# delete endpoint template <template-name>
```

После создания шаблона конечных устройств можно начать производить настройку его параметров. Для этого необходимо перейти в режим настройки параметров шаблона управляемых устройств следующей командой:

```
realmadmin/realm@nodename# go endpoint-template <template-name>
```

При настройке параметров шаблона следует придерживаться следующих правил:

1. Если значение настройки не определено в шаблоне, то ничего передаваться в управляемое устройство 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 управляемому устройству.

При создании шаблона администратор может использовать следующие разделы — Общие настройки, Настройки VPN, Библиотеки.

Общие настройки

В этом разделе устанавливаются параметры общих настроек управляемого устройства. Для настройки параметров используется следующая команда:

```
realmadmin/realm@nodename# set settings general <parameters>
```

Параметры для настройки:

Параметр	Описание
installation-settings	Настройки инсталляции ПО UserGate Client: • **collect-ep-data**: сбор информации о конечном устройстве (IP-адрес, время последнего подключения к UGMC, пользователь, имя компьютера, версия ОС, версия ПО UserGate Client, загрузка CPU и памяти, запущенные процессы, сервисы и т.д.). Значение по умолчанию: enabled. Если отключить данную функцию, то UGMC будет получать информацию только об IP-адресе, имени конечного устройства, версии ПО UserGate Client и ОС Windows, текущем времени и времени загрузки устройства, загрузке CPU и памяти. Важно! Отключение сбора информации о конечном устройстве влияет на работу профилей HIP. • **network-access**: настройка сетевого доступа при остановленном ПО UserGate Client. Значение по умолчанию: enabled. • **firewall-access**: разрешение пользователю самостоятельно, используя графический интерфейс, отключать контентную фильтрацию на конечном устройстве: ◦ **off** — не разрешать самостоятельно отключать контентную фильтрацию. ◦ **on** — разрешить самостоятельно отключать контентную фильтрацию.

Параметр	Описание
	◦ **by code** — разрешить самостоятельно отключать контентную фильтрацию с использованием кода. Для разрешения пользователю самостоятельно отключать контентную фильтрацию необходимо указать/сгенерировать код, который клиент должен ввести на конечном устройстве; также можно указать срок действия кода (code-expiration-date). При разрешении пользователю отключать фильтрацию самостоятельно можно указать количество разрешённых отключений (number-of-shutdowns) и/или время, на которое фильтрация будет отключена (duration). Значение по умолчанию: on (отключение фильтрации на 10 минут без использования кода). Важно! В случае использования счётчика количества отключений: если внести изменения в настройки разрешения отключения межсетевого экрана, то счётчик на конечном устройстве обнулится. • **uninstall-access**: возможность удаления ПО UserGate Client. При использовании опции uninstall-code (Разрешить с использованием кода) необходимо указать/сгенерировать код, который необходимо ввести клиенту при удалении ПО. Значение по умолчанию: enabled. Важно! Настройки не будут применены, если не включена синхронизация (параметр sync on). Иначе будут использованы значения по умолчанию.
notification	Настройка оповещений: • **show-icons**: отображение иконки UserGate Client в области уведомлений на панели задач. • **notification-tooltips**: включение/отключение отправки оповещений на конечное устройство. Если оповещения отключены, то уведомления не будут отображаться на конечном устройстве вне зависимости от настроек отдельных уведомлений (о добавлении/удалении устройства из карантина, блокировке ресурса). • **add-to-quarantine-message**: отправка уведомлений о блокировке устройства. Для настройки уведомления необходимо указать текст сообщения и тип. Уведомление будет отображено в виде всплывающего окна.

Параметр	Описание
	• **remove-from-quarantine-message**: отправка уведомлений о разблокировке устройства. Для настройки уведомления необходимо указать текст сообщения и тип. Уведомление будет отображено в виде всплывающего окна. • **resource-blocked-message**: отправка уведомления при блокировке перехода по адресу электронного ресурса. Для настройки уведомления необходимо указать текст сообщения и тип. Уведомление будет отображено в виде всплывающего окна. Важно! Настройки не будут применены, если не включена синхронизация (араметр sync on). Иначе будут использованы значения по умолчанию.
logan-device	Установка для конечного устройства сервера LogAn, на которое устройство будет отсылать информацию о событиях. Сервер LogAn должен быть предварительно зарегистрирован в UGMC. Важно! Настройки не будут применены, если не включена синхронизация (араметр sync on). Иначе будут использованы значения по умолчанию.

Настройка VPN

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

> **Примечание**
>
> **Настройка VPN-соединений возможна только для конечных устройств с версией ОС Windows 10 и выше. После разрыва соединения попытки подключения будут производиться в течение 40 секунд. Если за это время соединение не будет установлено, то у пользователя отобразится окно для выбора VPN-сервера.**

Для настройки параметров используется следующая команда:

```
realmadmin/realm@nodename# create settings vpn-settings <parameters>
```

Для настройки профиля VPN-сервера необходимо указать:

Параметр	Описание
enabled	Включение/отключение правила.
name	Название профиля безопасности для подключения к серверу VPN.
descriptipon	Описание профиля.
vpn-address	Имя хоста (FQDN) или IP-адрес VPN-сервера. Важно! Необходимо учитывать, что при указании адреса VPN-сервера в виде FQDN перебор IP-адресов не предусмотрен. В случае, если DNS-сервер вернет несколько адресов, будет выполнена попытка подключения к первому адресу в списке.
protocol	VPN-протоколы для создания туннеля: • **ipsec2**. Для создания туннелей используется протокол Layer 2 Tunnelling Protocol (L2TP), а для защиты передаваемых данных — протокол IPsec. • i**kev2-with-certificate**. Для создания защищенного канала будет использоваться протокол IKEv2, а для взаимной проверки подлинности сервера и клиента — сертификаты. **Важно!** При генерации клиентского сертификата обязательно должно быть указано поле CN — идентификатор пользователя, которому этот сертификат предназначается. • **ikev2**. Для создания защищенного канала будет использоваться протокол IKEv2, а для проверки клиента — логин и пароль (EAP-MSCHAP v2). Данный метод доступен только для пользователей доменного RADIUS-сервера.
ike-mode	Режим IKE (указать при выборе опции протоколаIPsec L2TP): main, aggressive. Разница между режимами: в агрессивном режиме используется меньшее количество пакетов, что позволяет достичь более быстрого установления соединения. Агрессивный режим не передает некоторые параметры согласования, что требует предварительной идентичной настройки их на точках подключения.
psk	Строка, которая должна совпадать на сервере и клиенте для успешного подключения. Указывается для протокола IPsec L2TP.

Параметр	Описание
Фаза 1	Во время первой фазы происходит согласование защиты IKE. Аутентификация происходит на основе общего ключа в режиме, выбранном ранее. Необходимо указать следующие параметры: • **phase1-key-lifetime** – по истечению данного времени происходят повторные аутентификация и согласование настроек первой фазы. • **dpd-interval** – для проверки состояния и доступности соседних устройств используется механизм Dead Peer Detection (DPD). DPD периодически отправляет сообщения R-U-THERE для проверки доступности IPsec-соседа. Минимальный интервал проверки: 10 секунд; значение 0 отключает проверку. • **dpd-max-failures** – максимальное количество запросов обнаружения недоступных IPsec-соседей, которое необходимо отправить до того, как IPsec-сосед будет признан недоступным. • **dh-groups** – выбор группы Диффи-Хеллмана, которая будет использоваться для обмена ключами. Сам ключ не передаётся, а передаются общие сведения, необходимые алгоритму определения ключа DH для создания общего секретного ключа. Чем больше номер группы Диффи-Хеллмана, тем больше бит используется для обеспечения надёжности ключа. • **phase1-security** – алгоритмы аутентификации и шифрования используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх/вниз или используйте кнопки Выше/Ниже.
Фаза 2	Во второй фазе осуществляется выбор способа защиты IPsec подключения. Необходимо указать: • **phase2-key-lifetime**. По истечению данного времени узлы должны сменить ключ шифрования. Время жизни, заданное во второй фазе, меньше, чем у первой фазы, т.к. ключ необходимо менять чаще. • **key-lifesize-enabled, key-lifesize**. Время жизни ключа может быть задано в байтах. Если заданы оба значения (key-lifetime и key-lifesize), то счётчик, первый достигнувший лимита, запустит пересоздание ключей сессии. • **phase2-security** – алгоритмы аутентификации и шифрования.

Библиотеки элементов

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

Настройка библиотек в шаблонах конечных устройств происходит на уровне **libraries**.

Для создания списков используется команда:

```
realmadmin/realm@nodename# create libraries <parameters>
```

Для редактирования ранее созданных списков используется команда:

```
realmadmin/realm@nodename# set libraries <parameters>
```

Для просмотра ранее созданных списков используется команда:

```
realmadmin/realm@nodename# show libraries <parameters>
```

Для удаления ранее созданных списков используется команда:

```
realmadmin/realm@nodename# delete libraries <parameters>
```

Сервисы

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

Для создания списков сервисов используется команда:

```
realmadmin/realm@nodename# create libraries services <parameters>
```

В качестве параметров указываются название и описание списка, необходимый протокол, порты назначения и источника.

Группы сервисов

Списки из библиотеки сервисов могут быть объединены в группы. Для создания группы сервисов используется комада:

```
realmadmin/realm@nodename# create libraries service-groups <parameters>
```

В качестве параметров в команде указываются название и описание списка, указываются необходимые списки сервисов, например:

```
realmadmin/realm@nodename# create libraries service-groups name
<service-group-name> services [ service-name1 service-name2 ... ]
```

IP-адреса

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

Администратор может добавлять необходимые ему элементы в процессе работы. Для добавления нового списка IP-адресов используется команда:

```
realmadmin/realm@nodename# create libraries ip-list <parameters>
```

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название списка адресов.
description	Описание списка.
threat-lvl	Уровень угрозы: • **very-low** — очень низкий уровень угрозы. • **low** — низкий уровень угрозы. • **medium** — средний уровень угрозы. • **high** — высокий уровень угрозы. • **very-high** — высокий уровень угрозы.

Параметр	Описание
type	Тип списка: • **local** — локальный. • **updatable** — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (**url**). Периодичность обновления списка указывается параметром **shedule** в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".
lists	Выбор существующих IP-листов для добавления в создаваемый лист.
ips	IP-адреса или диапазон IP-адресов, которые необходимо включить в список. Указывается в формате: <ip>, <ip/mask> или <ip_range_start-ip_range_end>.

Для редактирования списка (список параметров, доступных для обновления, аналогичен списку параметров команды создания списка):

```
realmadmin/realm@nodename# set libraries ip-list <ip-list-name>
<parameter>
```

Чтобы добавить в список новые адреса:

```
realmadmin/realm@nodename# set libraries ip-list <ip-list-name> [ <ip1>
<ip2> ... ]
```

Следующие команды используются для удаления всего списка адресов или IP-адресов, содержащихся в нём:

```
realmadmin/realm@nodename# delete libraries ip-list <ip-list-name>
realmadmin/realm@nodename# delete libraries ip-list <ip-list-name> ips
[ <ip1> <ip2>... ]
```

Команда отображения информации о всех имеющихся списках:

```
realmadmin/realm@nodename# show libraries ip-list
```

Чтобы отобразить информацию об определённом списке, необходимо указать название интересующего списка IP-адресов:

```
realmadmin/realm@nodename# show libraries ip-list <ip-list-name>
```

Также доступен просмотр содержимого списка IP-адресов:

```
realmadmin/realm@nodename# show libraries ip-list <ip-list-name> items
```

Группы приложений

Элемент библиотеки **Группы приложений** позволяет создать группы приложений для более удобного использования в правилах фильтрации сетевого трафика.

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 используется команда:

```
realmadmin/realm@nodename# create libraries application-
groups <parameters>
```

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название списка адресов.
description	Описание списка.
threat-lvl	Уровень угрозы: • **very-low** — очень низкий уровень угрозы. • **low** — низкий уровень угрозы. • **medium** — средний уровень угрозы. • **high** — высокий уровень угрозы. • **very-high** — высокий уровень угрозы.
type	Тип списка: • **local** — локальный. • **updatable** — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (**url**). Периодичность обновления списка указывается параметром **shedule** в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".
apps	Указание названия (**name**) и контрольной суммы (**hash**) приложения. Контрольная сумма исполняемого файла Windows должна быть определена по алгоритму SHA1, например, с помощью утилиты fciv.

Для редактирования группы приложений используется команда:

```
realmadmin/realm@nodename# set libraries application-groups <group-
name> <parameter>
```

Чтобы добавить в список новые приложения:

```
realmadmin/realm@nodename# set libraries application-groups <group-
name> apps new name <app-name> hash <app-hash>
```

Следующие команды используются для удаления всего списка адресов или IP-адресов, содержащихся в нём:

```
realmadmin/realm@nodename# delete libraries application-groupst <group-
name>
realmadmin/realm@nodename# delete libraries application-groups <group-
name> apps <app-name>
```

Команда отображения информации о всех имеющихся списках:

```
realmadmin/realm@nodename# show libraries application-groups
```

Чтобы отобразить информацию об определённом списке, необходимо указать название интересующего списка IP-адресов:

```
realmadmin/realm@nodename# show libraries application-groups <group-
name>
```

Также доступен просмотр содержимого списка IP-адресов:

```
realmadmin/realm@nodename# show libraries application-groups <group-
name> apps
```

Списки URL

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

Настройка списков URL производится на уровне **libraries url-list**.

Для добавления нового списка URL предназначена следующая команда:

```
realmadmin/realm@nodename# create libraries url-list <parameters>
```

Далее указывается следующая информация:

Параметр	Описание
name	Название списка URL.
description	Описание списка URL.
type	Тип списка: • **local** — локальный. • **updatable** — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (**url**). Периодичность обновления списка указывается параметром **shedule** в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 –вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".
urls	URL, которые необходимо добавить в список.
case-sensitivity	Чувствительность к регистру в написании адреса URL: • **sensitive** — чувствительно к регистру букв в адресе. • **insensitive** — нечувствительно к регистру букв в адресе. • **domain** — список адресов доменов.

Для редактирования списка URL используется команда:

```
realmadmin/realm@nodename# set libraries url-list <url-list-name>
<parameters>
```

Параметры, значения которых можно обновить, представлены в таблицы выше.

Далее представлены команды, с использованием которых доступно удаление всего списка URL или отдельных адресов URL:

```
realmadmin/realm@nodename# delete libraries url-list <url-list-name>
realmadmin/realm@nodename# delete libraries url-list <url-list-name>
urls [ <url> ... ]
```

Для просмотра информации о всех списках URL, об определённом списке URL или об адресах, входящих в определённый список, используются команды:

```
realmadmin/realm@nodename# show libraries url-list <url-list-name>
realmadmin/realm@nodename# show libraries url-list <url-list-name> urls
```

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.

Раздел находится на уровне **libraries url-categories**.

Для создания группы категорий URL используется следующая команда:

```
realmadmin/realm@nodename# create libraries url-categories <parameter>
```

Параметры, которые необходимо указать:

Параметр	Описание
name	Название группы URL-категорий.
description	Описание группы.

Параметр	Описание
categories	Категории URL, которые необходимо добавить в группу.

Команда для редактирования параметров группы:

```
realmadmin/realm@nodename# set libraries url-categories <list-name>
<parameter>
```

Для добавления категорий URL в существующую группу:

```
realmadmin/realm@nodename# set libraries url-categories <list-name>
categories [ <url-category> ... ]
```

Команды для удаления группы URL-категорий:

```
realmadmin/realm@nodename# delete libraries url-categories <list-name>
```

или отдельных категорий из группы:

```
realmadmin/realm@nodename# delete libraries url-categories <list-name>
categories [ <url-category> ... ]
```

Команды для просмотра информации о всех группах URL-категорий:

```
realmadmin/realm@nodename# show libraries url-categories
```

об определённой группе:

```
realmadmin/realm@nodename# show libraries url-categories <list-name>
```

Чтобы отобразить список категорий URL, входящих в группу:

```
realmadmin/realm@nodename# show libraries url-categories <list-name>
categories
```

Тип контента

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

Раздел **Типы контента** находится на уровне **libraries content-types**.

Добавление нового списка типов контента доступно с использованием следующей команды:

```
realmadmin/realm@nodename# create libraries content-types <parameters>
```

Далее указывается следующая информация:

Параметр	Описание
name	Название списка типов контента.
description	Описание списка.
type	Тип списка: • **local** — локальный. • **updatable** — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления (**url**). Периодичность обновления списка указывается параметром **shedule** в формате crontab. Crontab-формат: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".
mime	

Параметр	Описание
	Типы контента, которые необходимо добавить в список. Различные типы контента и их описание доступны по ссылке https://www.iana.org/assignments/media-types/media-types.xhtml.

Для редактирования списка используется следующая команда:

```
realmadmin/realm@nodename# set libraries content-types <content-types-list-name> <parameter>
```

Параметры, доступные для обновления, представлены в таблице выше.

Следующая команда используется для удаления списка с типами контента:

```
realmadmin/realm@nodename# delete libraries content-types <content-types-list-name>
```

Также доступно удаление отдельных типов контента из списка:

```
realmadmin/realm@nodename# delete libraries content-types <content-types-list-name> mime [ <mime-type> ... ]
```

Следующие команды используются для отображения информации о списках типов контента:

```
realmadmin/realm@nodename# show libraries content-types
realmadmin/realm@nodename# show libraries content-types <content-types-list-name>
```

Для отображения типов контента, содержащихся в списке, используется команда:

```
realmadmin/realm@nodename# show libraries content-types <content-types-list-name> mime
```

Календари

Календари позволяют создать временные интервалы, которые затем можно использовать в правилах. Администратор может добавлять необходимые ему элементы в процессе работы.

Данный раздел находится на уровне **libraries time-sets**.

Для создания группы используется следующая команда:

```
realmadmin/realm@nodename# create libraries time-sets <parameter>
```

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название группы.
description	Описание группы.
time-set	• **interval-name** — название интервала повторения. • **type** — тип интервала повторения: ◦ **daily** — ежедневно: ■ **time-from** — время начала (указывается в формате HH:MM). ■ **time-to** — время окончания (указывается в формате HH:MM). ■ **all-day on** — весь день. ◦ **weekly** — каждую неделю: ■ **time-from** — время начала (указывается в формате HH:MM). ■ **time-to** — время окончания (указывается в формате HH:MM). ■ **all-day on** — весь день. ■ **days [Mon | Tue | Wed | Thu | Fri | Sat | Sun]** — дни недели. ◦ **monthly** — каждый месяц: ■ **time-from** — время начала (указывается в формате HH:MM). ■ **time-to** — время окончания (указывается в формате HH:MM). ■ **all-day on** — весь день. ■ **days** — числа месяца (от 1 до 31).

Параметр	Описание
	◦ **fixed** — единовременно: ■ **time-from** — время начала (указывается в формате HH:MM). ■ **time-to** — время окончания (указывается в формате HH:MM). ■ **all-day on** — весь день. ■ **fixed-date** — нужная дата (указывается в формате YYYY-MM-DD). ◦ **span** — повторяющиеся события: ■ **time-from** — время начала (указывается в формате HH:MM). ■ **time-to** — время окончания (указывается в формате HH:MM). ■ **all-day on** — весь день. ■ **fixed-date-from** — дата начала (указывается в формате YYYY-MM-DD). ■ **fixed-date-to** — дата окончания (указывается в формате YYYY-MM-DD). ◦ **range** — диапазон дат: ■ **time-from-enabled <on | off>** — включение/отключение указания даты начала интервала. ■ **fixed-date-from** — дата начала (указывается в формате YYYY-MM-DD). ■ **time-from** — время начала (указывается в формате HH:MM). ■ **time-to-enabled <on | off>** — включение/отключение указания даты окончания интервала. ■ **fixed-date-to** — дата окончания (указывается в формате YYYY-MM-DD). ■ **time-to** — время окончания (указывается в формате HH:MM).

Для редактирования календаря:

```
realmadmin/realm@nodename# set libraries time-sets <time-sets-name>
<parameter>
```

Параметры, доступные для обновления, представлены в таблице выше.

Для редактирования интервала, заданного в календаре:

```
realmadmin/realm@nodename# set libraries time-sets <time-sets-name> ...
time-set <time-set-type> ( <time-set-filter> )
```

Далее указываются новые значения; <time-set-filter> — фильтр из текущих значений интервала.

Добавление нового элемента в существующую группу:

```
realmadmin/realm@nodename# create libraries time-sets <time-sets-
name> ... time-set <time-set-type> new
```

Команда для удаления группы элементов:

```
realmadmin/realm@nodename# delete libraries time-sets <time-sets-name>
```

Для удаления элемента календаря:

```
realmadmin/realm@nodename# delete libraries time-sets <time-sets-name>
<time-set-type> ( <time-set-filter> )
```

Для отображения информации о всех календарях:

```
realmadmin/realm@nodename# show libraries time-sets
```

Для отображения информации об определённом календаре:

```
realmadmin/realm@nodename# show libraries time-sets <time-sets-name>
```

Для отображения информации об элементах группы с одинаковым типом повторения:

```
realmadmin/realm@nodename# show libraries time-sets <time-sets-name>
<time-set-type>
```

Группы шаблонов

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.

Для создания группы шаблонов конечных устройств используется команда:

```
realmadmin/realm@nodename# create endpoint groups name <group-name>
description <group description> templates [ teplate1-name template2-
name ... ]
```

Для редактирования группы шаблонов конечных устройств используется команда:

```
realmadmin/realm@nodename# set endpoint groups name <group-name>
<description, templates>
```

Для просмотра созданных ранее групп шаблонов конечных устройств используется команда:

```
realmadmin/realm@nodename# show endpoint groups <group-name>
```

Для удаления созданных ранее групп шаблонов конечных устройств используется команда:

```
realmadmin/realm@nodename# delete endpoint groups <group-name>
```

В созданной ранее группе шаблонов возможно удаление входящих в нее шаблонов:

```
realmadmin/realm@nodename# delete endpoint groups <group-name>
templates [ template-name template-name ... ]
```

Добавление конечных устройств UGC под управление UGMC

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

1. Добавление конечных устройств UGC по одному устройству. Данный вариант подходит для компаний с небольшим количеством управляемых устройств UGC.

2. Массовое добавление устройств. Вариант для компаний с большим количеством устройств.

Добавление по одному устройству

1. На UGMC необходимо разрешить сервис **Контроль конечных устройств** в свойствах контроля доступа зоны, к интерфейсу которой подключаются управляемое устройство.

2. Необходимо создать запись для конечного устройства UGC в UGMC.

3. Получить уникальный код созданного устройства.

4. Установить ПО UGC на конкретное устройство (компьютер) пользователя.

Для разрешения сервиса **Контроль конечных устройств** в свойствах контроля доступа зоны, к интерфейсу которой подключаются управляемое устройство, необходимо в режиме администратора UGMC выполнить следующую команду:

```
Admin/system@nodename# set network zone <zone-nfme> enabled-services
[ "Device net" ]
```

Для создания записи для конечного устройства UGC используется команда:

```
realmadmin/realm@nodename# create endpoint devices <parameters>
```

Необходимо указать следующие параметры:

Параметр	Описание
enabled	Включение объекта управляемого устройства UGC.

Параметр	Описание
licensed	Лицензирование конечного устройства: on/off. Если on, то он использует одну лицензию. В случае отсутствия лицензии конечное устройство не сможет подключиться к UGMC. Если параметр будет поставлен в off после регистрации устройства на UGMC, то: • правила межсетевого экрана, полученные от MC ранее, продолжают работать; • подключение по VPN с настройками, полученными ранее от MC доступно; • новые настройки конечное устройство от MC не получает.
name	Название для управляемого устройства UGC. Можно вводить произвольное название.
description	Описание управляемого устройства UGC.
templates-group	Группа шаблонов, настройки которой следует применить к этому управляемому устройству UGC. Настройки (политики) применятся после синхронизации с UGMC.
sync-mode	Режим синхронизации: отключено (disabled), автоматическая (auto) или ручная (manual) синхронизация.

Для получения уникального кода созданного устройства (**device-code**) используется команда:

```
realmadmin/realm@nodename# show endpoint devices <device-name>

name                          : <device-name>
enabled                       : on
device-code                   : g8wkh31z
templates-group               : <group-name>
sync-mode                     : auto
```

Установка ПО UGC на компьютер пользователя описана в разделе Установка ПО Usergate Client.

Массовое добавление устройств

1. На UGMC необходимо разрешить сервис **Контроль конечных устройств** в свойствах контроля доступа зоны, к интерфейсу которой подключаются управляемое устройство.

2. Создать код для группы конечных устройств.

3. Получить уникальный код для группы устройств.

4. Установить ПО UGC на конкретное устройство (компьютер) пользователя.

Для разрешения сервиса **Контроль конечных устройств** в свойствах контроля доступа зоны, к интерфейсу которой подключаются управляемое устройство, необходимо в режиме администратора UGMC выполнить следующую команду:

```
Admin/system@nodename# set network zone <zone-nfme> enabled-services
[ "Device net" ]
```

Для создания кода для группы конечных устройств используется команда:

```
realmadmin/realm@nodename# create endpoint codes <parameters>
```

Необходимо указать следующие параметры:

Параметр	Описание
enabled	Включение объекта управляемого устройства UGC.
name	Название для управляемого устройства UGC. Можно вводить произвольное название.
description	Описание управляемого устройства UGC.
group	Группа шаблонов, настройки которой следует применить к этому управляемому устройству UGC. Настройки (политики) применятся после синхронизации с UGMC.

Для получения уникального кода для группы устройств (**device-code**) используется команда:

```
realmadmin/realm@nodename# show endpoint codes <code-name>

name           : <code-name>
enabled        : on
group          : <groupe-name>
device-code    : 4shmps46
```

Установка ПО UGC на компьютер пользователя описана в разделе Установка ПО Usergate Client.

HIP-объекты

Объекты HIP позволяют настроить критерии соответствия для конечных устройств и могут быть использованы в качестве одного из условий при настройке политик безопасности.

Для создания HIP объекта используется команда:

```
realmadmin/realm@nodename# create endpoint hip-object <parameters>
```

Необходимо указать следующие параметры:

Параметр	Описание
name	Название объекта HIP.
description	Описание объекта HIP (опционально).
os-version	Версия операционной системы устройства пользователя. При использовании операторов = и != необходимо указывать полную версию Windows.
ug-client-version	Версия ПО UserGate Client.
security	Статусы компонентов безопасности конечного устройства: • firewall — межсетевой экран; • virus-protection — Антивирус; • automatic-update — Автоматическое обновление; • bitlocker. Важно! BitLocker считается включенным, если он включен хотя бы на одном из дисков.

Параметр	Описание
products	Проверка соответствия программного обеспечения, установленного на конечном устройстве: • antimalware. Проверка соответствия антивирусного ПО на устройстве пользователя. ◦ enabled: проверка статуса ПО; ◦ database-updated: проверка актуальности баз (да, нет, не проверять); ◦ version ПО; ◦ vendor: производитель и название продукта. • firewall. Проверка соответствия межсетевого экрана на конечном устройстве. При настройке необходимо указать: ◦ installed: проверка наличия установленного ПО; ◦ enabled: проверка статуса ПО (да, нет, не проверять); ◦ version ПО; ◦ vendor: производитель и название продукта; • backup. Проверка ПО для резервного копирования: ◦ installed: проверка наличия установленного ПО; ◦ version ПО; ◦ vendor: производитель и название продукта. • disk-encryption. Проверка установленных на конечном устройстве программ для шифрования диска: ◦ installed: проверка наличия установленного ПО; ◦ version ПО; ◦ vendor: производитель и название продукта. • dlp. Проверка соответствия системы предотвращения утечек информации. ◦ installed: проверка наличия установленного ПО; ◦ version ПО; ◦ vendor: производитель и название продукта. • patch-management. Проверка актуальности обновления. ◦ installed: проверка наличия установленного ПО; ◦ version ПО; ◦ vendor: производитель и название продукта.
processes	Проверка процессов, запущенных на конечном устройстве.
running-services	Проверка служб, запущенных на конечном устройстве.

Параметр	Описание
registry-keys	Ключ реестра Microsoft Windows — каталог, в котором хранятся настройки и параметры операционной системы. Поддерживаются следующие типы параметров реестра: • REG_SZ: строка Unicode или ANSI с нулевым символом в конце. • REG_BINARY: двоичные данные в любой форме. • REG_DWORD: 32-разрядное число. Доступна проверка ключей следующих разделов реестра: • HKEY_LOCAL_MACHINE • HKEY_USERS Важно! Путь указывается с использованием обратного слэша (\), например, \HKEY_LOCAL_MACHINE, после которых через (\) указывается полный путь к параметру. Описание ключей реестра читайте в документации Microsoft (https://docs.microsoft.com/ru-ru/troubleshoot/developer/webapps/iis/general/use-registry-keys).
installed-updates	Проверка наличия указанного обновления на конечном устройстве. Необходимо указать номер статьи базы знаний Microsoft (KB), например, KB5013624.

HIP-профили

HIP-профили представляют собой набор объектов HIP и предназначены для проверки соответствия конечного устройства требованиям безопасности (комплаенса). С использованием профилей HIP можно настроить гибкие политики доступа к зоне сети или приложению.

Для создания HIP-профиля используется команда:

```
realmadmin/realm@nodename# create endpoint hip-objects <parameters>
```

Необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля HIP.
description	Описание профиля HIP (опционально).

Параметр	Описание
hip-objects	Выбор логического элемента (and, or, and-not, or-not) и объектов HIP. Подробнее о создании объектов читайте в разделе Объекты HIP.

Управление устройствами LogAn

Для централизованного управления устройствами LogAn в управляемой области необходимо создать шаблоны и группы шаблонов, описывающие настройки LogAn, затем добавить управляемые устройства LogAn и применить к ним созданные ранее шаблоны.

В интерфейсе CLI создание шаблонов, групп шаблонов и добавление управляемых устройств LogAn происходит на уровне **logan**.

Шаблоны устройств

Для создания шаблона устройств LogAn используется команда:

```
realmadmin/realm@nodename# create logan template <name, description>
```

Для редактирования названия/описания шаблона устройств LogAn используется команда:

```
realmadmin/realm@nodename# set logan template <name, description>
```

Для просмотра созданных ранее шаблонов устройств LogAn используется команда:

```
realmadmin/realm@nodename# show logan template <template-name>
```

Для удаления созданных ранее устройств LogAn используется команда:

```
realmadmin/realm@nodename# delete logan template <template-name>
```

После создания шаблона устройств LogAn можно начать производить настройку его параметров. Для этого необходимо перейти в режим настройки параметров шаблона управляемых устройств LogAn следующей командой:

```
realmadmin/realm@nodename# go logan-template <template-name>
```

В режиме настройки параметров шаблона доступны те же команды настройки параметров LogAn, которые определены в разделе Интерфейс командной строки Руководства администратора LogAn.

При настройке параметров следует придерживаться следующих правил:

1. Если значение настройки не определено в шаблоне, то ничего передаваться в LogAn не будет. В данном случае в LogAn будет использована либо настройка по умолчанию, либо настройка, которую указал локальный администратор.

2. Если настройка параметра выполнена в шаблоне, то эта настройка переопределит значение этой же настройки, назначенной локальным администратором.

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

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

- общие настройки устройства;
- настройки сетевых интерфейсов.

3. При настройке сетевых интерфейсов первый физический интерфейс, доступный для конфигурирования — это **port1**. Интерфейс **port0** нельзя настроить с помощью средств UGMC, он всегда настраивается локальным администратором и необходим для обеспечения первичной связи управляемого устройства с UGMC.

4. При настройке сетевых интерфейсов возможно создать интерфейс и оставить его конфигурирование локальному администратору. Для этого необходимо активировать параметр **on-device** (**on-device on**) в настройках сетевого интерфейса.

5. 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.

6. Рекомендуется создавать отдельные шаблоны для разных групп настроек, это позволит избежать конфликтов настроек при объединении шаблонов в группы шаблонов и упростит понимание результирующей настройки, которая будет применена к управляемым устройствам. Например, шаблон сетевых настроек, шаблон библиотек и т.д.

Группы шаблонов

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.

Для создания группы шаблонов LogAn используется команда:

```
realmadmin/realm@nodename# create logan groups name <group-name>
description <group description> templates [ teplate1-name template2-
name ... ] template-enabled <on/off>
```

Для редактирования группы шаблонов LogAn используется команда:

```
realmadmin/realm@nodename# set logan groups name <group-name>
<description, templates>
```

Для просмотра созданных ранее групп шаблонов LogAn используется команда:

```
realmadmin/realm@nodename# show logan groups <group-name>
```

Для удаления созданных ранее групп шаблонов LogAn используется команда:

```
realmadmin/realm@nodename# delete logan groups <group-name>
```

В созданной ранее группе шаблонов возможно удаление входящих в нее шаблонов:

```
realmadmin/realm@nodename# delete logan groups <group-name> templates
[ template-name template-name ... ]
```

Добавление устройств LogAn под управление UGMC

Группа шаблонов всегда применяется к одному или нескольким управляемым устройствам LogAn. Для добавления управляемых устройств LogAn в UGMC необходимо выполнить следующие шаги:

1. Обеспечить доступ от управляемого устройства LogAn до UGMC, для этого на UGMC необходимо разрешить сервис **Management** в свойствах контроля доступа зоны, к которой подключены управляемые устройства

2. Создать объект управляемого устройства LogAn.

3. Связать созданный объект управляемого устройства LogAn с реальным устройством UserGate LogAn.

Для обеспечения доступа от управляемого устройства LogAn до UGMC необходимо в режиме администратора UGMC выполнить следующую команду:

```
Admin/system@nodename# set network zone <zone-nfme> enabled-services
[ Management ]
```

Для создания объекта управляемого устройства используется команда:

```
realmadmin/realm@nodename# create logan devices <parameters>
```

Необходимо указать следующие параметры:

Наименование	Описание
enabled	Включает объект управляемого устройства. Если объект управляемого устройства включен, то он занимает одну лицензию.
name	Название для управляемого устройства. Можно вводить произвольное название.

Наименование	Описание
description	Описание управляемого устройства.
templates-group	Группа шаблонов, настройки которой следует применить к этому управляемому устройству.
sync-mode	Выбор режима синхронизации настроек группы шаблонов к устройству. Возможны 3 варианта: • **auto** — автоматическая синхронизация. При изменении любой настройки из любого шаблона, включенного в группу шаблонов, примененную к управляемому устройству, это изменение применяется к управляемому устройству без задержек. • **disabled** — синхронизация выключена. • **manual** — режим синхронизации, при котором настройки применяются однократно при запросе синхронизации.

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

1. Получить Код устройства

2. Указать IP-адрес UGMC и ввести уникальный код устройства

Код созданного объекта управляемого устройства (**device-code**) можно посмотреть следующей командой:

```
realmadmin/realm@nodename# show logan devices <device-name>

name                          : <device-name>
enabled                       : on
device-code                   : 7w1lecpt
templates-group               : <template-group-name>
...
```

В консоли управляемого устройства LogAn необходимо добавить IP-адрес управляющего UGMC и указать код созданного объекта управляемого устройства:

```
Admin@logan-nodename# set settings general management-center mc-address
<ugmc-ip-address> device-code 7w1lecpt enabled on
```

Проверить подключение на стороне UGMC можно командой просмотра управляемого устройства:

```
realmadmin/realm@nodename# show logan devices <device-name>
```

Управление обновлениями управляемых устройств

UGMC позволяет создать централизованную политику обновления программного обеспечения UserGate (UGOS) и обновляемыми библиотеками, предоставляемыми по подписке.

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

Обновление ПО

Порядок установки обновлений, следующий:

1. Загрузить обновления в репозитарий UGMC. Управление загрузками обновлений в репозиторий UGMC управляется командой:

```
realmadmin/realm@nodename# set settings general updates-schedule
software
```

Подробнее — в главе Общие настройки в Руководстве администратора UGMC.

2. Утвердить обновление для всех или для конкретных устройств:

```
realmadmin/realm@nodename# set logan software-updates <sw-update-name>
devices <device-name>
```

3. Провести установку обновления. После утверждения обновление становится доступным для скачивания для всех или группы управляемых устройств.

Управляемое устройство скачивает обновление в соответствии с расписанием проверки обновлений. После скачивания обновление может быть установлено администратором в консоли UGMC или в ручном режиме администратором управляемого устройства.

Обновление библиотек

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

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

Для настройки скачивания обновлений в UGMC из репозитария UserGate используется следующая команда:

```
realmadmin/realm@nodename#set logan libraries-updates <library-name>
download <auto/manual>
```

ADMIN

ADMIN (описание)

Данный раздел позволяет зарегистрированному администратору сменить свой пароль, изменить некоторые настройки профиля и выйти из системы.

Наименование	Описание
Сменить пароль	Для смены пароля необходимо указать свой текущий пароль и два раза указать новый пароль.
Предпочтения	• Количество элементов на странице — устанавливает количество строк, отображаемых в одном диалоговом окне, например, список правил межсетевого экрана. • Ночной режим — устанавливает черный цвет темы графического интерфейса UGOS.
Выход	Завершение сеанса работы в веб-консоли устройства.

ИЗБРАННЫЕ

Избранные (описание)

В веб-интерфейсе имеется возможность фильтрации отображаемых разделов путем их добавления в избранное и поиск разделов по их названию. Фильтрация позволяет скрыть неиспользуемые разделы. Отображение только избранных разделов не влияет на функциональность или конфигурацию устройств. Чтобы добавить раздел в избранные, необходимо отметить символ звездочки напротив названия раздела; для настройки отображения используйте переключатель **Только избранные**, расположенный в нижней части панели.

В шаблонах управляемых устройств консоли управления областью (рабочие столы **NGFW — конфигурация**, **Конечные устройства — конфигурация**, **LogAn — конфигурация**) также доступно отображение только разделов, в которых были произведены настройки.

ПРИЛОЖЕНИЯ

Требования к сетевому окружению

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
Веб-консоль	TCP	8010	Входящий (до веб-консоли UserGate Management Center)	Доступ к веб-интерфейсу управления устройством.
	TCP	8300	Входящий (до веб-консоли UserGate NGFW, подключённого к UGMC)	Доступ к веб-интерфейсу управления UG NGFW, подключённого к UGMC.
CLI по SSH	TCP	2200	Входящий (к CLI по SSH)	Доступ к интерфейсу командной строки (CLI) UserGate по протоколу SSH.
XML-RPC	TCP	4041	Входящий (к UserGate по API)	Управление устройством UserGate по API.
Удалённый помощник	TCP	22	Исходящий (до серверов технической поддержки)	Удалённый доступ к серверу технической поддержки. Доступ к серверам: • 93.91.171.46; • 178.154.221.222; • ra.entensys.com.

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
NTP	UDP	123	Исходящий (до сервера точного времени)	Синхронизация времени.
DNS	UDP	53	Исходящий (от UserGate до DNS-сервера)	Сервис получения информации (IP-адрес) о доменах.
Регистрация сервера UserGate	TCP	443	Исходящий (до сервера регистрации)	Доступ до сервера регистрации продуктов UserGate reg2.usergate.com.
Обновление ПО и библиотек	TCP	443	Исходящий (до серверов обновления)	Обновление программного обеспечения и элементов библиотек: доступ до сервера updates.usergate.com.
Репликация настроек	TCP	4369	Входящий (с первого узла кластера на второй и последующие узлы)	Сервис, необходимый для работы кластера конфигурации. Установка управляющего соединения.
		9000-9100	Входящий (приём конфигурации от первого узла кластера)	Передача информации об изменении конфигурации кластера

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
				(реплика настроек)
Сервис UserGate Management Center	TCP	9712	Входящий (к UGMC от NGFW)	Первоначальная установка связи и обмен ключами шифрования управляемых устройств и сервера UserGate Management Center.
		2022	Входящий (к UGMC от NGFW)	Построение SSH-туннеля для обмена данными с помощью полученных ключей.
Контроль конечных устройств (начиная с версии 7.1.0)	TCP	9712	Входящий (к UGMC от UG Client)	Первоначальная установка связи и обмен ключами шифрования управляемых устройств UserGate Client и сервера UserGate Management Center.
		4045	Входящий (к UGMC от UG Client)	Построение SSL-туннеля для обмена данными с помощью ключей, полученных при

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
				установке связи.
		22000-22711	Входящий (к UGMC от UG Client)	Передача журналов и телеметрии с UG Client на UG LogAn транзитом через UGMC.
LDAP	TCP	389, 636	Исходящий (на LDAP-коннектор)	Выполнение запросов LDAP (389 - для LDAP и 636 - для LDAP over SSL).
SNMP	UDP	161	Входящий (до UserGate)	Доступ к серверу UserGate по протоколу SNMP.
SMTP	TCP	25	Исходящий (до почтового сервера)	Отправка уведомлений на электронную почту.
DHCP	UDP	67, 68	Исходящий (запрос на получение адреса от UserGate на сервер DHCP)	Сервис службы DHCP.
FTP (экспорт журналов) (начиная с версии 7.1.0)	TCP	21	Исходящий (до сервера FTP)	Экспорт журналов на сервер FTP.
SSH (экспорт журналов) (начиная с версии 7.1.0)	TCP	22	Исходящий (до сервера SSH)	Экспорт журналов на сервер SSH.
	TCP/UDP	514		

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
Syslog (экспорт журналов) (начиная с версии 7.1.0)			Исходящий (до сервера Syslog)	Экспорт журналов на сервер Syslog.
Ручная проверка сайтов по категориям	TCP	80/443	Исходящий (до updates.usergate.com)	Ручная проверка сайтов по категориям.

Описание форматов журналов

Формат журнала событий

CEF

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	events
	Origin	Модуль, в котором произошло событие.	admin_console
	Severity	Важность события.	Может принимать значения: • 0 — информационные. • 6 — предупреждения. • 8 — ошибки.

Тип поля	Название поля	Описание	Пример значения
			• 10 — критичные.
CEF [расширение]	**rt**	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	mc_core@einerson stal
	suser	Имя пользователя.	Administrator (Admin)
	cat	Компонент, в котором произошло событие.	console_auth
	act	Тип события.	administrator_login
	src	IPv4-адрес источника.	192.168.117.254
	cs1Label	Поле используется для указания деталей события.	Attributes
	cs1	Детали события в формате JSON.	{"login":"ex_admin", "realm_id":"31d8fcb6-e51d-4e3f-b799-181d31a45b06"}

JSON

Название поля	Описание	Пример значения
user	Имя пользователя.	Admin
timestamp		2022-05-12T08:11:46.15869Z

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