**Table of Contents**


Table of Contents 1
Management Center 6
Management Center 6.1.x Руководство администратора 7
Введение 8
Описание 9
Управляемые области 10
Шаблоны и группы шаблонов 11
Управляемые устройства 13
Управление UGMC 14
Лицензирование UGMC 16
Лицензирование UGMC 17
Планирование внедрения UGMC 18
Принципы планирования 19
Один шаблон и одна группа шаблонов на каждое управляемое устройство 20
Набор шаблонов с настройками каждого модуля. Специфичные настройки для некоторых модулей для определенной группы управляемых устройств. Сеть настраивается локально 21
Набор шаблонов с настройками каждого модуля. Специфичные настройки для некоторых модулей для определенной группы управляемых устройств. Сеть настраивается через UGMC 22
Примеры шаблонов устройств 23
Первоначальная настройка 24
Описание 25
Развертывание программно-аппаратного комплекса 26
Развертывание виртуального образа 27
Подключение к UGMC 28
Настройка UGMC 29
Общие настройки 30
Управление устройством 31
Администраторы 35
Управление сертификатами 36
Профили оповещений 37
Серверы авторизации UserGate Management Center 38
Офлайн операции с сервером 39
Настройка сети 40
Настройка зон 41
Настройка интерфейсов 42
Настройка шлюзов 44
Маршруты 45
Интерфейс командной строки (CLI) 46
Описание и команды 47
Диагностика и мониторинг 49
Диагностика и мониторинг 50
Управление областями 56
Создание управляемых областей 57
Администраторы области 58
Серверы авторизации области 59
Управление межсетевыми экранами UserGate 60
Описание 61
Шаблоны устройств 62

Группы шаблонов 63
Добавление устройств UserGate под управление UGMC 64
Кластеризация МЭ UserGate с помощью UGMC 66
Управление обновлениями управляемых устройств 68
Приложения 70
Требования к сетевому окружению 71
Описание форматов журналов 72
Management Center 7.0.1 Руководство администратора 73
Принятые обозначения и сокращения 74
Введение 75
Описание 76
Управляемые области 77
Шаблоны и группы шаблонов 78
Управляемые устройства 80
Управление UGMC 81
Лицензирование UGMC 83
Лицензирование UGMC 84
Планирование внедрения UGMC 85
Планирование внедрения UGMC (Описание) 86
Первоначальная настройка 89
Первоначальная настройка 90
Офлайн операции с сервером 92
Офлайн операции с сервером(Описание) 93
Настройка UGMC 94
Общие настройки 95
Управление устройством 96
Администраторы 101
Управление сертификатами 102
Серверы аутентификации UGMC 103
Профили аутентификации UGMC 105
Библиотеки элементов 106
Расширение системного раздела 108
Настройка сети 109
Настройка сети(Описание) 110
Интерфейс командной строки (CLI) 113
Интерфейс командной строки (CLI) Описание 114
Диагностика и мониторинг 116
Диагностика и мониторинг 117
Журналы и отчёты 123
Журнал событий 124
Режим расширенного поиска 125
Экспорт журналов 126
Управление областями 128
Создание управляемых областей 129
Администраторы области 130
Серверы аутентификации области 131
Профили аутентификации области 133
Каталоги пользователей 134
Управление областями (Описание) 135
Управление межсетевыми экранами UserGate 136
Управление межсетевыми экранами UserGate (Описание) 137
Управление устройствами LogAn 142

Управление устройствами LogAn (Описание) 143
Управление конечными устройствами 147
Управление конечными устройствами UserGate Client (Описание) 148
Установка ПО UserGate Client 149
Шаблоны управляемых устройств UGC 150
Группы шаблонов управляемых устройств UGC 156
Добавление управляемых устройств UGC под управление UGMC 157
Управление устройством UGC из консоли UGMC 158
Сбор и анализ данных с устройств UGC 160
HIP профили 163
Объекты HIP 164
Приложения 165
Описание форматов журналов 166
Требования к сетевому окружению 167
Management Center 7.x Руководство администратора 168
Введение 169
Описание 170
Управление UGMC 171
Управляемые области 173
Шаблоны и группы шаблонов 174
Совместимость версий UserGate MC с версиями продуктов UserGate 176
Совместимость версий UserGate MC с аппаратными платформами 177
Лицензирование 178
Лицензирование UserGate MC 179
Планирование внедрения UGMC 181
Планирование внедрения UGMC (Описание) 182
Первоначальная настройка 185
Первоначальная настройка 186
Интерфейс 188
Веб-консоль UserGate MC 189
Офлайн операции с сервером 191
Офлайн операции с сервером(Описание) 192
Настройка UGMC 193
Настройка общих параметров 194
Управление устройством 195
Администраторы 200
Сертификаты 202
Серверы аутентификации 203
Профили аутентификации 204
Библиотеки элементов 205
Расширение системного раздела 208
Обновление ПО кластера UserGate MC 209
Настройка сети 210
Настройка сети (описание) 211
Журналы и отчёты 214
Журнал событий 215
Экспорт журналов 216
Режим расширенного поиска 218
Описание форматов журналов 219
Диагностика и мониторинг 220
Маршруты 221
Ping 222

Traceroute 223
Запрос DNS 224
Оповещения 225
SNMP 226
Параметры SNMP 233
Правила оповещений 234
Профили безопасности SNMP 235
Управление областями 236
Управление областями (Описание) 237
Создание управляемых областей 238
Администраторы области 239
Серверы аутентификации области 241
Профили аутентификации области 242
Каталоги пользователей 243
Управление устройствами UserGate NGFW 244
Управление устройствами UserGate NGFW (описание) 245
Практика работы с шаблонами в UserGate MC 250
Перенос объектов между шаблонами 255
Копирование правил в шаблонах управляемых устройств (версия 7.6.0 и выше) 259
Настройка прокси-сервера 260
Управление устройствами UserGate DCFW 261
Управление устройствами UserGate DCFW (Описание) 262
Перенос объектов между шаблонами DCFW 265
Управление устройствами UserGate WAF (версия 7.6.0 и выше) 266
Интеграция с устройствами UserGate WAF 267
Управление устройствами UserGate Log Analyzer 268
Управление устройствами UserGate Log Analyzer (описание) 269
Управление конечными устройствами 272
Общие сведения 273
Создание шаблонов конечных устройств 274
Настройка параметров шаблонов конечных устройств 275
Создание группы шаблонов конечных устройств 281
Настройка интеграции конечных устройств с UserGate MC 282
Управление списком устройств 284
Настройка проверки требований безопасности (HIP) 286
Журналирование данных конечных устройств 288
Управление устройствами UserGate SIEM 291
Управление устройствами UserGate SIEM (описание) 292
Общая библиотека (версия 7.6.0 и выше) 294
Общие сведения 295
IP-адреса 296
Списки URL 297
Сервисы 298
Группы сервисов 299
HIP-объекты 300
HIP-профили 301
Профили тайм-аутов 302
Настройка обновляемых списков элементов 303
Использование общей библиотеки 304
Просмотр зависимостей элементов общей библиотеки 305
Просмотр истории изменений элемента 306
Перенос объектов из библиотек шаблонов в общую библиотеку 307

Интерфейс командной строки 309
Общие положения 310
Общие положения (описание) 311
Команды, доступные до первичной инициализации узла 312
Команды, доступные до первичной инициализации узла (Описание) 313
Первоначальная инициализация 314
Первоначальная инициализация (Описание) 315
Режим конфигурации 316
Режим конфигурации (описание) 317
Настройка устройства 320
Настройка устройства (Описание) 321
Настройка кластеров 324
Настройка управления доступом к консоли устройства 326
Настройка сертификатов 329
Настройка серверов аутентификации 330
Настройка профилей аутентификации 333
Настройка сети 334
Зоны 335
Интерфейсы 337
Шлюзы 342
Настройка маршрутизации 343
DNS-настройки 344
Настройка мониторинга 345
Настройка параметров мониторинга устройства 346
Настройка библиотек 348
Настройка библиотек (Описание) 349
Управление областями 353
Настройка управляемых областей 354
Режим администратора управляемой области 355
Режим администратора управляемой области (Описание) 356
Режим конфигурации администратора управляемой области 357
Общие настройки консоли управляемой области 358
Администраторы управляемой области 359
Серверы аутентификации управляемой области 361
Профили аутентификации управляемой области 364
Каталоги пользователей управляемой области 365
Управление межсетевыми экранами UserGate 366
Управление устройствами UserGate DCFW 370
Управление устройствами LogAn 374
Управление конечными устройствами UserGate 376
Admin 385
Настройка учетной записи администратора 386
Приложения 387
Требования к сетевому окружению 388

**Введение**

**Описание**

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

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

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

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

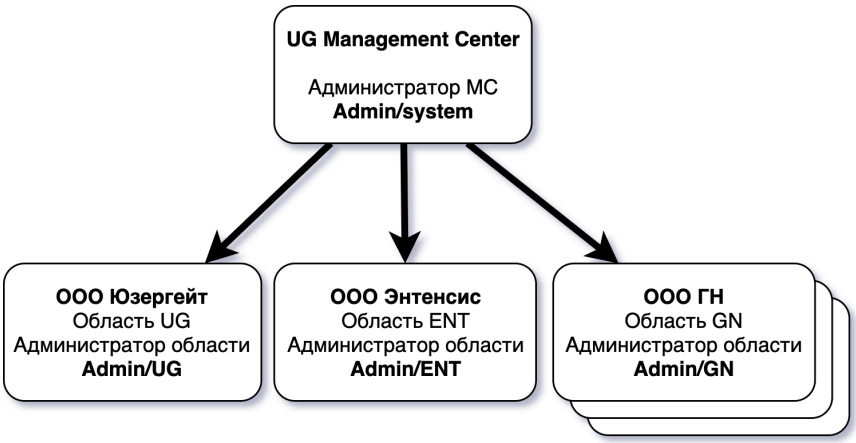
**Управляемые области**

---

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

UGMC поддерживает облачную модель управления, то есть предоставляет возможность полностью независимого управления устройствами разных предприятий, используя единый сервер управления. Разделение полномочий происходит на уровне управляемых областей. Управляемая область UserGate — это логический объект, представляющий одно предприятие или группу предприятий, управляемых одним администратором. Каждой области назначается отдельный администратор, который может администрировать только одну назначенную ему область. Администратор одной области не может ни при каких обстоятельствах получить доступ к другой области. Администратор сервера UGMC имеет полномочия создавать управляемые области и назначать в них администраторов, не имея при этом доступа к объектам самой области. Более подробно о разграничении прав администраторов смотрите в главе Администраторы.

Пример UGMC с несколькими управляемыми областями:




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

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

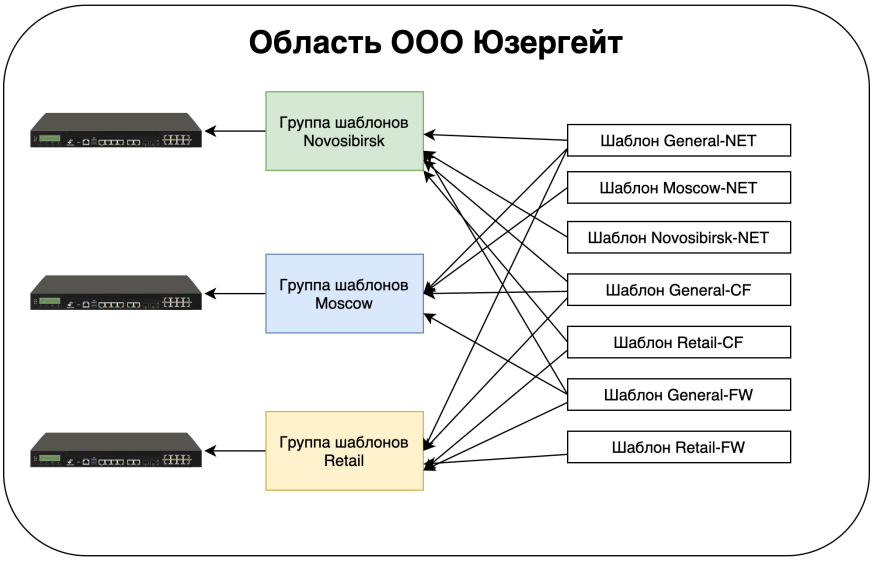
**Шаблоны и группы шаблонов**

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

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

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

Пример области с несколькими группами шаблонов для управления МЭ UserGate:



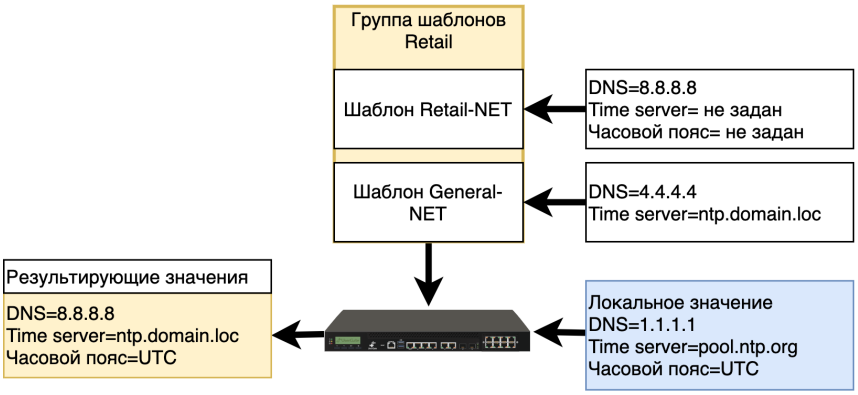

Конфигурация, передаваемая на устройство, может быть двух типов:

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

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

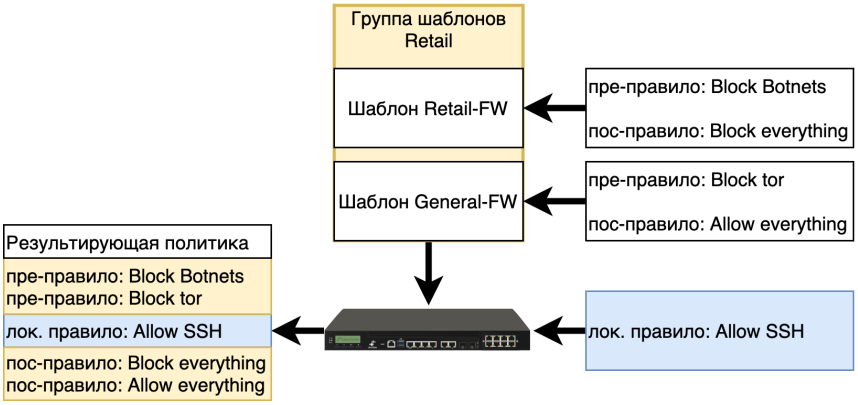
Настройка параметра при конфликтующих значениях в разных шаблонах одной группы шаблонов принимает значение, заданное в наиболее верхнем шаблоне. Локально указанные настройки данного параметра игнорируются.

Пример результирующего значения параметра, определенного в нескольких шаблонах:




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

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



**Управляемые устройства**

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

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

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

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

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

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

## Управление сервисами UGMC

Управление сервисами UGMC включает в себя следующие задачи:

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

## Управление областями UGMC

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

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

## Ролевое управление

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

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

| Администратор | Профиль администратора | Уровень доступа |
|---|---|---|
| AdminTemplates/realm_code | Templates | Создание и модификация всех шаблонов области. |
| AdminTemplateGeneral/realm_code | TemplateGeneral | Только модификация шаблона General. |
| AdminTemplateGeneralNET/realm_code | TemplateGeneralNET | Только модификация сетевых настроек в шаблоне General. |

**Лицензирование UGMC**

**Лицензирование UGMC**

---

Documentation: ☑
Product: UGMC
Version: 6.1.9, 7.0.1

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

Лицензия на UGMC дает право бессрочного пользования продуктом.

Дополнительно лицензируются следующие модули:

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

Для регистрации продукта необходимо выполнить следующие шаги:

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

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

**Планирование внедрения UGMC**

**Принципы планирования**

---

Documentation: ☑
Product: UGMC
Version: 6.1.9

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.

Для вывода устройств из-под управления UGMC необходимо отменить применение всех шаблонов с настройками (например, создать пустую группу шаблонов и назначить её управляемому устройству) и выполнить синхронизацию управляемого устройства и UGMC.

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

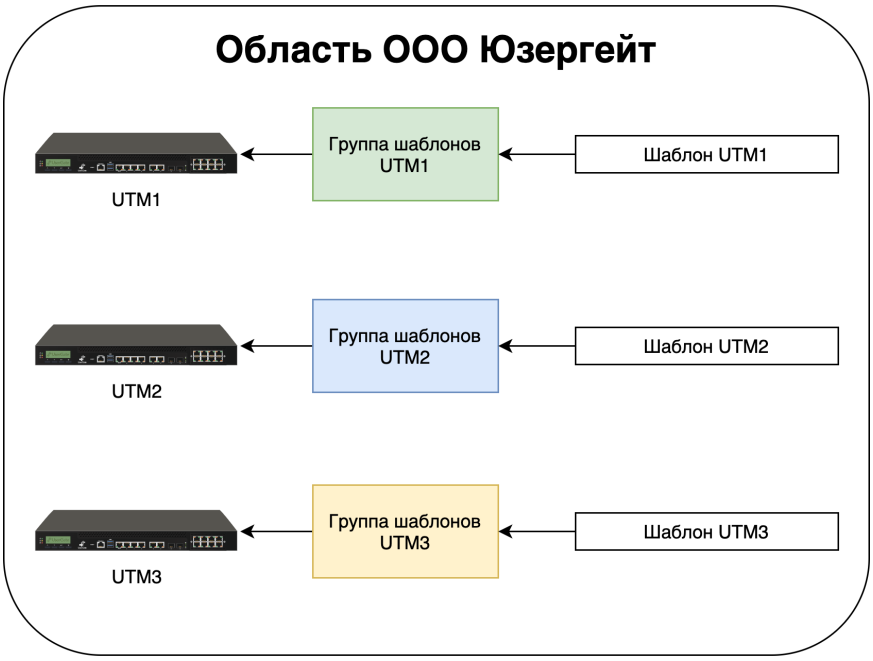
**Один шаблон и одна группа шаблонов на каждое управляемое устройство**

---

Documentation: ☑
Product: UGMC
Version: 6.1.9

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.



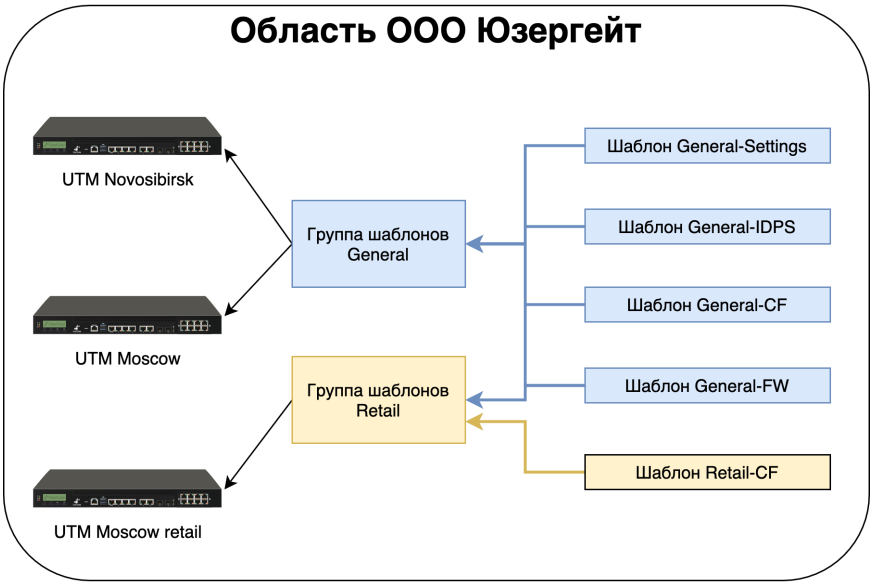
**Набор шаблонов с настройками каждого модуля. Специфичные настройки для некоторых модулей для определенной группы управляемых устройств. Сеть настраивается локально**

---

Documentation: ☑
Product: UGMC
Version: 6.1.9

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

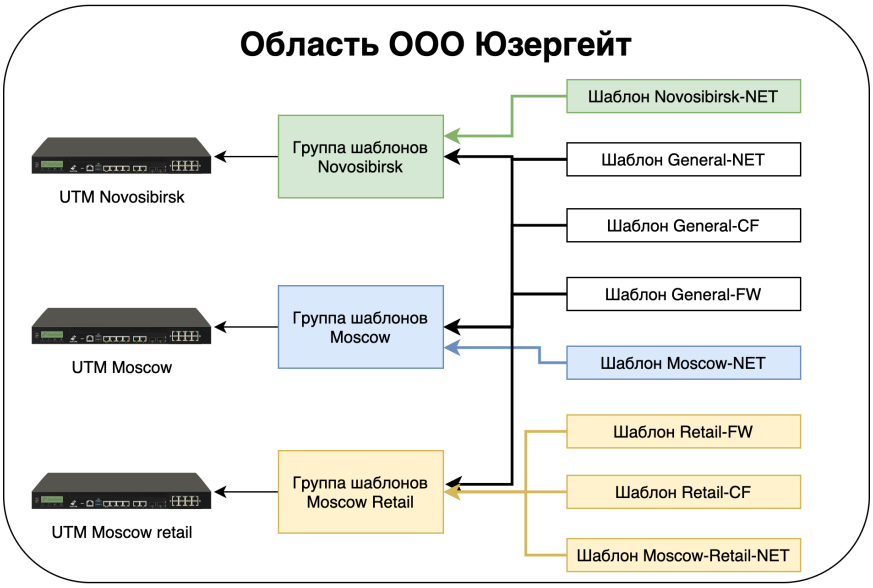
**Набор шаблонов с настройками каждого модуля. Специфичные настройки для некоторых модулей для определенной группы управляемых устройств. Сеть настраивается через UGMC**

---

Documentation: ☑
Product: UGMC
Version: 6.1.9

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**

---

Documentation: ☑
Product: UGMC
Version: 6.1.9

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**

**Описание**

---

Documentation: ☑
Product: UGMC
Version: 6.1.9

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**

---

Documentation: ☑
Product: UGMC
Version: 6.1.9

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**

---

Documentation: ☑
Product: UGMC
Version: 6.1.9

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

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

Для начала работы с виртуальным образом, выполните следующие шаги:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Скачайте образ и распакуйте. | Скачайте последнюю версию виртуального образа с официального сайта https://www.usergate.com/ru. |
| **Шаг 2.** Импортируйте образ в свою систему виртуализации. | Инструкцию по импорту образа вы можете посмотреть на сайтах VirtualBox и VMWare. Для Microsoft Hyper-v и KVM необходимо создать виртуальную машину и указать в качестве диска скачанный образ, **после чего отключить службы интеграции** в настройках созданной виртуальной машины. |
| **Шаг 3.** Настройте параметры виртуальной машины. | Увеличьте размер оперативной памяти виртуальной машины. Используя свойства виртуальной машины, установите минимум 8Gb. |
| **Шаг 4. Важно!** Увеличьте размер диска виртуальной машины. | Размер диска по умолчанию составляет 100Gb, что обычно недостаточно для хранения всех журналов и настроек. Используя свойства виртуальной машины, установите размер диска в 300Gb или более. Рекомендованный размер — 500Gb или более. |
| **Шаг 5.** Настройте виртуальные сети. | UserGate Management Center поставляется с четырьмя интерфейсами, два из которых назначены в зоны:<br>• **Management** — первый интерфейс виртуальной машины.<br>• **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**

Documentation: ☑
Product: UGMC
Version: 6.1.9

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

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

Остальные интерфейсы отключены и требуют последующей настройки.

Первоначальная настройка требует выполнения следующих шагов:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Подключиться к интерфейсу управления. | **При наличии DHCP-сервера**<br>Подключить интерфейс port0 в сеть предприятия с работающим DHCP-сервером. Включить сервер UGMC. После загрузки консоль UserGate укажет IP-адрес, на который необходимо подключиться для дальнейшей активации продукта.<br>**Статический IP-адрес**<br>Включить сервер UGMC. Используя CLI (Command Line Interface), назначить необходимый IP-адрес на интерфейс port0. Детали использования CLI смотрите в главе Интерфейс командной строки (CLI).<br>Подключиться к веб-консоли UGMC по указанному адресу, он должен выглядеть примерно следующим образом:<br>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 интерфейсами читайте в главе Настройка интерфейсов. Система поставляется с предопределенными зонами:<br>• Зона **Management** (сеть управления), интерфейс port0.<br>• Зона **Trusted** (LAN). Предполагается, что через эту зону UGMC будет подключаться к УУ, а также получит доступ в интернет.<br>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 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.<br>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 UserGate Management Center готов к работе. Для более детальной настройки обратитесь к необходимым главам справочного руководства.

**Настройка UGMC**

**Общие настройки**

---

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

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

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

Version: 6.1.9
Product: UGMC
Documentation: ☑

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

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

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<br>Настройки интерфейсов<br>Настройки шлюзов<br>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:<br>• Консоль администрирования.<br>• Кластер.<br>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 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).<br>Подключиться к веб-консоли второго узла кластера, выбрать язык установки.<br>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.<br>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. |

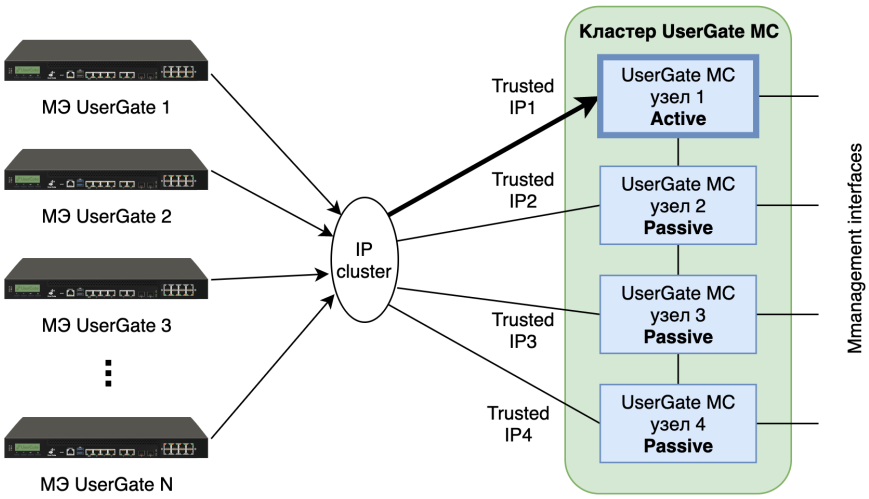
До четырех узлов кластера конфигурации можно объединить в отказоустойчивый кластер. Самих кластеров отказоустойчивости может быть несколько. Поддерживаются 2 режима - **Актив-Актив** и **Актив-Пассив**.

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.



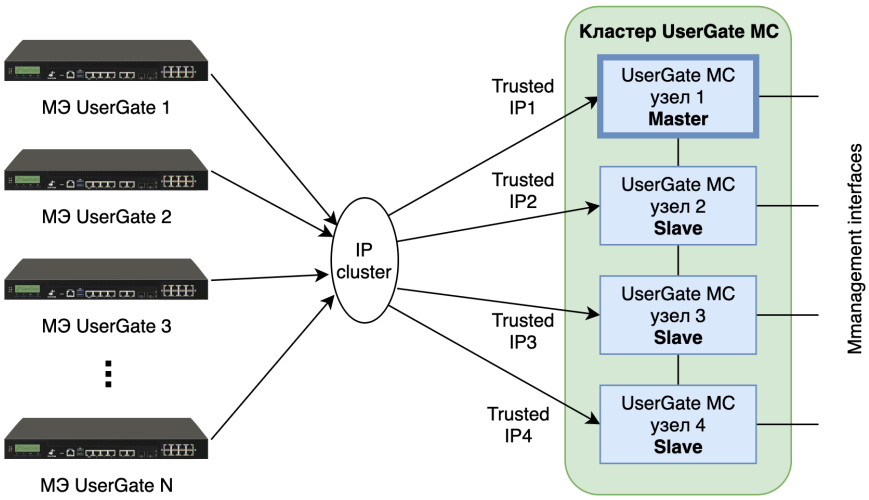

Кластерный IP-адрес находятся на узле UGMC 1. Если узел UGMC 1 становится недоступным, то кластерный IP-адрес перейдет на следующий сервер, который станет мастер-сервером, например, UGMC 2.

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:<br>• **Актив-Актив** — нагрузка распределяется на все узлы кластера.<br>• **Актив-Пассив** — нагрузка идет на Мастер-узел и переключается на запасной узел в случае недоступности Мастер-узла. |

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

## Диагностика

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

| Наименование | Описание |
|---|---|
| **Детализация диагностики** | • **Off** — ведение журналов диагностики отключено.<br>• **Error** — журналировать только ошибки работы сервера.<br>• **Warning** — журналировать только ошибки и предупреждения.<br>• **Info** — журналировать только ошибки, предупреждения и дополнительную информацию.<br>• **Debug** — максимум детализации.<br>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.<br>• **Очистить журналы** — очистить содержимое журналов. |
| **Удаленный помощник** | • **Включено**/**Отключено** — включение/отключение режима удаленного помощника. Удаленный помощник позволяет инженеру технической поддержки UserGate, зная значения идентификатора и токена удаленного помощника, произвести безопасное подключение к серверу UGMC для диагностики и решения проблем. Для успешной активации удаленного помощника UGMC должен иметь доступ к серверу удаленного помощника компании UserGate по протоколу SSH.<br>• **Идентификатор удаленного помощника** — полученное случайным образом значение. Уникально для каждого включения удаленного помощника.<br>• **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.<br>• **Выключить** — выключение сервера UGMC. |
| **Обновления** | Выбор канала обновлений ПО UGMC<br>• **Стабильные** — проверка наличия стабильных обновлений ПО.<br>• **Бета** — проверка наличия экспериментальных обновлений. |

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

Для установки обновлений необходимо выполнить следующие действия:

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

## 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 |
|---|---|

| Наименование | Описание |
|---|---|
| **Шаг 1.** Экспорт настроек. | В разделе **Управление устройством** нажать на ссылку **Экспорт настроек → Экспорт** и выбрать **Экспортировать все настройки** или **Экспортировать сетевые настройки**. Система сохранит:<br>• текущие настройки сервера под именем: cc_core-mc_core @nodename_version_YYYYMMDD_HHMMSS.bin<br>• сетевые настройки под именем: network-cc_core-mc_core @nodename_version_YYYYMMDD_HHMMSS.bin<br>nodename — имя узла UserGate Management Center.<br>version — версия UserGate Management Center.<br>YYYYMMDD_HHMMSS — дата и время выгрузки настроек в часовом поясе UTC.<br>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** нажать на ссылку **Экспорт настроек → Импорт** и указать путь к ранее созданному файлу настроек. Указанные настройки применятся к серверу, после чего сервер будет перезагружен |

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

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

| Наименование | Описание |
|---|---|
| **Шаг 1.** Создать правило экспорта. | В разделе **Управление устройством → Экспорт настроек** нажать кнопку **Добавить**, указать имя и описание правила |
| **Шаг 2.** Указать параметры удаленного сервера. | Во вкладке правила **Удаленный сервер** указать параметры удаленного сервера:<br>• **Тип сервера** — FTP или SSH.<br>• **Адрес сервера** — IP-адрес сервера.<br>• **Порт** — порт сервера.<br>• **Логин** — учетная запись на удаленном сервере.<br>• **Пароль**/**Подтверждение пароля** — пароль учетной записи.<br>• **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:<br>(минуты:0-59) (часы:0-23) (дни месяца:1-31) (месяц:1-12) (день недели:0-6, 0-воскресенье)<br>Каждое из первых пяти полей может быть задано следующим образом:<br>• Звездочка (*) — обозначает весь диапазон (от первого до последнего).<br>• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.<br>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".<br>• 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**

---

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

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

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

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

| Наименование | Описание |
|---|---|
| **Шаг 1.** Создать профиль доступа администратора. | В разделе **Администраторы → Профили администраторов** нажать кнопку **Добавить** и указать необходимые настройки. |
| **Шаг 2.** Создать учетную запись администратора и назначить ей один из созданных ранее профилей администратора. | В разделе **Администраторы** нажать кнопку **Добавить** и выбрать необходимый вариант:<br>• **Добавить локального администратора** — создать локального пользователя, задать ему пароль доступа и назначить созданный ранее профиль доступа.<br>• **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.<br>• **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.<br>• **Добавить администратора с профилем аутентификации** — создать пользователя, назначить созданный ранее профиль администратора и профиль аутентификации (необходимы корректно настроенные серверы аутентификации).<br>**Важно!** В данном разделе настроек сервисов консоли управления администратором области может быть назначен только локальный администратор. Это связано с тем, что LDAP серверы, используемые для аутентификации администраторов сервиса UGMC и для аутентификации администраторов области, могут быть разными. При необходимости использования LDAP администраторов для управления Областью, их необходимо создать в самой области. Более подробно об администраторах области смотрите в разделе Администраторы области. |

При создании профиля доступа администратора необходимо указать следующие параметры:

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

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

Для настройки этих параметров необходимо:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Настроить политику паролей. | В разделе **Администраторы → Администраторы** нажать кнопку **Настроить**. |
| **Шаг 2.** Заполнить необходимые поля. | Указать значения следующих полей:<br>• **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.<br>• **Число неверных попыток аутентификации** — количество неудачных попыток аутентификации администратора, после которых учетная запись заблокируется на **Время блокировки**.<br>• **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.

**Управление сертификатами**

---

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

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

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

| Наименование | Описание |
|---|---|
| **Шаг 1.** Создать сертификат. | Нажать на кнопку **Создать** в разделе **Сертификаты** |
| **Шаг 2.** Заполнить необходимые поля. | Указать значения следующих полей:<br>• **Название** — название сертификата, под которым он будет отображен в списке сертификатов.<br>• **Описание** — описание сертификата.<br>• **Страна** — страна, в которой выписывается сертификат.<br>• **Область или штат** — область или штат, в котором выписывается сертификат<br>• **Город** — город, в котором выписывается сертификат.<br>• **Название организации** — название организации, для которой выписывается сертификат.<br>• **Common name** — имя сертификата. Рекомендуется использовать только символы латинского алфавита для совместимости с большинством браузеров.<br>• **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:<br>• **Экспорт сертификата** — экспортирует данные сертификата в der-формате без экспортирования приватного ключа сертификата.<br>• **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:<br>• Название — название сертификата, под которым он будет отображен в списке сертификатов.<br>• Описание — описание сертификата.<br>• Загрузите файл, содержащий данные сертификата.<br>• Загрузите файл, содержащий приватный ключ сертификата.<br>• Пароль для приватного ключа, если таковой требуется.<br>• Цепочка сертификатов — файл, содержащий сертификаты вышестоящих центров сертификации, которые участвовали в создании сертификата. Необязательное поле. |

**Профили оповещений**

---

Version: 6.1.9
Product: UGMC
Documentation: ☑

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

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

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

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

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

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

**Серверы авторизации UserGate Management Center**

---

Version: 6.1.9
Product: UGMC
Documentation: ☑

Серверы авторизации — это внешние источники учетных записей пользователей для авторизации в веб-консоли управления UGMC. UGMC поддерживает только сервер авторизации LDAP-коннектор. LDAP-коннектор позволяет:

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

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

| Наименование | Описание |
|---|---|
| **Включено** | Включает или отключает использование данного сервера авторизации. |
| **Название** | Название сервера авторизации. |
| **SSL** | Определяет, требуется ли SSL-соединение для подключения к LDAP-серверу. |
| **Доменное имя LDAP или IP-адрес** | IP-адрес контроллера домена, 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*

**Офлайн операции с сервером**

---

Version: 6.1.9
Product: UGMC
Documentation: ☑

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

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

| Наименование | Описание |
|---|---|
| **Check filesystems** | Запуск проверки файловой системы устройства на наличие ошибок и их автоматическое исправление. |
| **Clear logs** | Очистка диагностических журналов для освобождения пространства на системном разделе. |
| **Export logs** | Выгрузка диагностических журналов на внешний USB носитель. Все данные на внешнем носителе будут удалены. |
| **Expand log partition** | Увеличение раздела для журналов на весь выделенный диск. Эта операция обычно используется после увеличения дискового пространства, выделенного гипервизором для виртуальной машины UGMC. Данные и настройки UGMC не сбрасываются. |
| **Backup full** | Создать полную копию диска UGMC на внешний USB носитель. Все данные на внешнем носителе будут удалены. |
| **Backup system only** | Создать копию системного раздела UGMC, исключая журналы на внешний USB носитель. Все данные на внешнем носителе будут удалены. |
| **Restore from backup** | Восстановление UGMC с внешнего USB носителя. |
| **Update from USB** | Установка обновления ПО UGMC с внешнего USB носителя. Обновление должно быть скопировано в корень съемного диска, диск должен иметь формат NTFS или FAT32.<br>Название файла обновления должно быть в следующем формате: **update_xxxxx** (где xxxxx - номер сборки). Без расширения .bin. |
| **Refresh NIC names** | Упорядочивание имен сетевых портов в необходимом порядке. Упорядочивание производится в соответствии с номером порта на шине PCI. Эту операцию необходимо выполнять после добавления сетевых портов в настроенный аплаенс UGMC, например, после установки дополнительной сетевой карты в физический аплаенс или после добавления портов в виртуальный аплаенс. Данные и настройки UGMC не сбрасываются. |
| **Factory reset** | Сброс состояния UGMC к первоначальному состоянию системы. Все данные и настройки будут утеряны. |
| **Exit** | Выход и перезагрузка устройства. |

**Настройка сети**

**Настройка зон**

---

Documentation: ☑
Product: UGMC
Version: 6.1.9

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). | Указать параметры защиты зоны от сетевого флуда для протоколов TCP (SYN-flood), UDP, ICMP:<br>• **Порог уведомления** — при превышении количества запросов с одного IP-адреса над указанным значением происходит запись события в системный журнал.<br>• **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.<br>Рекомендованные значения для порога уведомления — 300 запросов в секунду, для порога отбрасывания пакетов — 600 запросов в секунду.<br>**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. |
| **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.<br>Сервисы:<br>• **Ping** — позволяет пинговать UGMC.<br>• **SNMP** — доступ к UserGate по протоколу SNMP (UDP 161).<br>• **Консоль администрирования** — доступ к веб-консоли управления (TCP 8010 и 8300).<br>• **XML-RPC для управления** — позволяет управлять продуктом по API (TCP 4041).<br>• **VRRP** — сервис, необходимый для объединения нескольких NGFW в отказоустойчивый кластер (IP протокол 112).<br>• **Кластер** — сервис, необходимый для объединения нескольких NGFW в кластер (TCP 4369, TCP 9000-9100).<br>• **CLI по SSH** — доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200.<br>• **Сервис UserGate Management Center** — сервис подключения NGFW и LogAn (TCP 2022, 9712).<br>Подробнее о требованиях сетевой доступности читайте в Приложение 1. Требования к сетевому окружению. |
| **Шаг 4.** Настроить параметры защиты от IP-спуфинг атак (опционально). | Атаки на основе IP-спуфинга позволяют передать пакет из одной сети, например, из **Trusted**, в другую, например, в **Management**. Для этого атакующий подменяет IP-адрес источника на предполагаемый адрес необходимой сети. В таком случае ответы на этот пакет будут пересылаться на внутренний адрес.<br>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.<br>С помощью флага **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**. |

Documentation: ☑
Product: UGMC
Version: 6.1.9

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** | Режим работы бонда должен совпадать с режимом работы на том устройстве, куда подключается бонд. Может быть:<br>• **Round robin.** Пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. Эта политика применяется для балансировки нагрузки и отказоустойчивости.<br>• **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.<br>• **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.<br>• **Broadcast.** Передает все на все сетевые интерфейсы. Эта политика применяется для отказоустойчивости.<br>• **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.<br>• **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.<br>• **Adaptive load balancing.** Включает в себя предыдущую политику плюс осуществляет балансировку входящего трафика. Не требует дополнительной настройки на коммутаторе. Балансировка входящего трафика достигается путем ARP-переговоров. Драйвер перехватывает ARP-ответы, отправляемые с локальных сетевых карт наружу, и переписывает MAC-адрес источника на один из уникальных MAC-адресов сетевой карты, участвующей в объединении. Таким образом, различные пиры используют различные MAC-адреса сервера. Балансировка входящего трафика распределяется последовательно (round-robin) между интерфейсами. |
| **MII monitoring period (мсек)** | Устанавливает периодичность MII-мониторинга в миллисекундах. Определяет, как часто будет проверяться состояние линии на наличие отказов. Значение по умолчанию — 0 — отключает MII-мониторинг. |
| **Down delay (мсек)** | Определяет время (в миллисекундах) задержки перед отключением интерфейса, если произошел сбой соединения. Эта опция действительна только для мониторинга MII (miimon). Значение параметра должно быть кратным значениям miimon. Если оно не кратно, то округлится до ближайшего кратного значения. Значение по умолчанию 0. |
| **Up delay (мсек)** | 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:<br>• **Slow** — запрос партнера на передачу LACPDU-пакетов каждые 30 секунд.<br>• **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:<br>• **Отключено** — устанавливает одинаковый MAC-адрес на всех интерфейсах во время переключения.<br>• **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.<br>• **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:<br>• **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.<br>• **Layer 2+3** — использует как MAC-адреса, так и IP-адреса для генерации хэша. Алгоритм совместим с IEEE 802.3ad.<br>• **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. |

| Наименование | Описание |
| --- | --- |
| **Сеть** | Способ присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. |

**Настройка шлюзов**

---

Documentation: ☑
Product: UGMC
Version: 6.1.9

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**

---

Documentation: ☑
Product: UGMC
Version: 6.1.9

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

Для добавления маршрута необходимо выполнить следующие шаги:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Задать название и описание данного маршрута. | В разделе **Сеть** выберите в меню **Маршруты**, нажмите кнопку **Добавить**. Укажите имя для данного маршрута. Опционально можно задать описание маршрута. |
| **Шаг 2.** Указать адрес назначения. | Задайте подсеть, куда будет указывать маршрут, например, 172.16.20.0/24 или 172.16.20.5/32. |
| **Шаг 3.** Указать шлюз. | Задайте IP-адрес шлюза, через который указанная подсеть будет доступна. Этот IP-адрес должен быть доступен с сервера UGMC. |
| **Шаг 4.** Указать интерфейс. | Выберите интерфейс, через который будет добавлен маршрут. Если оставить значение **Автоматически**, то UGMC сам определит интерфейс, исходя из настроек IP-адресации сетевых интерфейсов. |
| **Шаг 5.** Указать метрику. | Задайте метрику маршрута. Чем меньше метрика, тем приоритетней маршрут, если маршрутов несколько в данную сеть несколько. |

**Интерфейс командной строки (CLI)**

**Описание и команды**

---

Documentation: ☑
Product: UGMC
Version: 6.1.9

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

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

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

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

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

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

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

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

| Наименование | Описание |
|---|---|
| **Шаг 1.** Разрешить доступ к CLI (SSH) для выбранной зоны | Разрешить доступ для протокола CLI по SSH в настройках зоны, к которой вы собираетесь подключаться для управления с помощью CLI. Будет открыт порт TCP 2200. |
| **Шаг 2.** Запустить SSH-терминал | Запустить у себя на компьютере SSH-терминал, например, SSH для Linux или Putty для Windows. Указать в качестве адреса адрес UGMC, в качестве порта подключения — 2200, в качестве имени пользователя — имя пользователя правами корневого администратора UGMC (по умолчанию Admin/system). Для Linux команда на подключение должна выглядеть так:<br>*ssh Admin/system@IPUserGateMC -p 2200* |
| **Шаг 3.** Войти в CLI | Войти в CLI, используя пароль пользователя, указанного на предыдущем шаге. Если устройство UGMC не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin/system, в качестве пароля — utm. |

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

**help command**

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

**help Iface**

Полный список команд:

| Наименование | Описание |
|---|---|
| **help** | Показывает список доступных команд. |
| **exit**<br>**quit**<br>**Ctrl+D** | Выйти из CLI. |
| **date** | Посмотреть текущее время на сервере. |
| **gateway** | Посмотреть или задать значения шлюза. Смотрите gateway help для детальной информации. |
| **iface** | Набор команд для просмотра и настройки параметров сетевого интерфейса. Смотрите iface help для детальной информации. |
| **license** | Посмотреть информацию о лицензии. |
| **netcheck** | Проверить доступность стороннего HTTP/HTTPS-сервера.<br>**netcheck [-t TIMEOUT] [-d] URL**<br>Опции:<br>-t —м максимальный таймаут ожидания ответа от веб-сервера<br>-d — запросить содержание сайта. По умолчанию запрашиваются только заголовки. |
| **nslookup** | Выполнить определение IP-адреса по имени хоста. |
| **ping** | Выполнить ping определенного хоста. |

| Наименование | Описание |
| --- | --- |
| **radmin** | Включить или отключить удаленный доступ к серверу для технической поддержки UserGate. |
| **radmin_e** | Включить или отключить удаленный доступ к серверу для технической поддержки UserGate, в случаях, когда сервер UGMC завис. |
| **reboot** | Перезагрузить сервер UserGate Management Center. |
| **route** | Создать, изменить, удалить маршрут. |
| **shutdown** | Выключить сервер UGMC. |
| **traceroute** | Выполнить трассировку соединения до определенного хоста. |
| **zone** | Набор команд для просмотра и настройки параметров зоны. Смотрите zone help для детальной информации. |

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

## Мониторинг маршрутов

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

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

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

## Ping

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

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

## Traceroute

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

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

## Запрос DNS

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

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

## Оповещения

## Правила оповещений

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

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

При добавлении правила необходимо указать следующие параметры:

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

## SNMP

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

Для настройки мониторинга с помощью SNMP необходимо:

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

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

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

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

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

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

Для скачивания доступны следующие MIB-файлы:

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

**UTM-TRAPS-MIB**

| Наименование | Описание |
|---|---|
| **trapCoreCrush** | Сбой ядра. |
| **trapStatDown** | Сервис статистики (UserGate Log Analyzer) недоступен. |
| **trapCoreBootstrapEnd** | Загрузка сервера завершена успешно. |
| **trapDefaultGatewayChanged** | Изменение шлюза по умолчанию. |
| **trapHighSessionsCounter** | Таблица сессий заполнена на 90%. |
| **trapHighUsersCounter** | Количество активных пользователей достигло 90% от порога лицензии. |
| **trapStatusChanged** | Изменение статуса узла отказоустойчивого кластера. |
| **trapMemberUp** | Статус узла отказоустойчивого кластера изменился на «Подключен». |
| **trapMemberDown** | Узел отказоустойчивого кластера отключен. |
| **trapAttackDetected** | Обнаружена атака 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. |
| **trapTrafficDrop** | Срабатывание запрещающего правила межсетевого экрана. |
| **trapLDAPServerDown** | Сервер LDAP недоступен. |

**UTM-TRAPS-BINDINGS-MIB**

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

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

**UTM-MIB**

| Наименование | Тип данных | Описание |
|---|---|---|
| **vcpuCount** | integer | Количество виртуальных процессоров в системе. |
| **vcpuUsage** | integer | Загруженность виртуальных процессоров системы; отображается в %. |
| **usersCounter** | integer | Количество активных пользователей на текущий момент времени. |
| **cpuLoad** | integer | Загруженность центрального процессора системы; отображается в %. |
| **memoryUsed** | integer | Использование оперативной памяти; отображается в %. |
| **logDiskSpace** | integer | Пространство на диске, используемое под журналы; отображается в %. |
| **Sys_power_supply1_status** | string | Состояние первого источника питания:<br>• **no_power_supplies**.<br>• **on**.<br>• **off**. |
| **Sys_power_supply2_status** | string | Состояние второго источника питания.<br>• **no_power_supplies**.<br>• **on**.<br>• **off**. |
| **Sys_raid_status** | integer | Текущий статус RAID (Redundant Array of Independent Disks):<br>• **no_raid**.<br>• **0** — optimal — массив в оптимальном состоянии.<br>• **1** — degraded — полный или частичный выход из строя одного из дисков.<br>• **2** — rebuild — восстановление массива. |

**UTM-INTERFACES-MIB**

| Наименование | Тип данных | Описание |
|---|---|---|

| 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 физического/канального уровней:<br>• **1** — other — неизвестный тип.<br>• **2** — regular1822 — определён в BBN Report 1822.<br>• **3** — hdh1822 — определён в BBN Report 1822.<br>• **4** — ddn-x25 — определён в BBN Report 1822.<br>• **5** — rfc877-x25 — определён в стандарте канального уровня сетевой модели OSI X.25.<br>• **6** — ethernet-csmacd — сетевой интерфейс типа Ethernet, независимо от скорости (определён в RFC 3635).<br>• **7** — iso88023-csmacd — определён в IEEE 802.3.<br>• **8** — iso88024-tokenBus — определён в стандарте IEEE 8802.4.<br>• **9** — iso88025-tokenRing — сетевой интерфейс использует подключение Token Ring; определяется в стандарте IEEE 802.5.<br>• **10** — iso88026-man — определён в стандарте ISO 88026 "MAN".<br>• **11** — starLan — определён в стандарте IEEE 802.3e.<br>• **12** — proteon-10Mbit — Proteon 10 Mbit<br>• **13** — proteon-80Mbit — Proteon 80 Mbit.<br>• **14** — hyperchannel — высокоскоростной канал, используемы в сети ISDN.<br>• **15** — fddi — сетевой интерфейс использует подключение FDDI (Fiber Distributed Data Interface). FDDI — это набор стандартов передачи данных по оптоволоконным линиям в локальной сети.<br>• **16** — lapb — протокол канального уровня, используемым для передачи пакетов стандарта X.25.<br>• **17** — sdlc — протокол канального уровня для системной сетевой архитектуры IBM.<br>• **18** — ds1 — способен обрабатывать 24 одновременных соединения на общей скорости 1,544 Мбит/с; также называется T1.<br>• **19** — e1 — европейский аналог T1.<br>• **20** — basicISDN — для связи аппаратуры абонента и ISDN-станции.<br>• **21** — primaryISDN — используется для подключения к широкополосным магистралям, связывающим местные и центральные АТС или сетевые коммутаторы.<br>• **22** — propPointToPointSerial — определён в стандарте RFC1213.<br>• **23** — ppp — сетевой интерфейс использует подключение PPP (Point-To-Point Protocol).<br>• **24** — softwareLoopback — сетевой интерфейс является петлевым адаптером. Такие интерфейсы часто используются для тестирования; они не отправляют трафик в сеть.<br>• **25** — eon — ConnectionLess Network Protocol (CLNP) over Internet Protocol (IP); определён в ISO/IEC 8473-1.<br>• **26** — ethernet-3Mbit — сетевой интерфейс использует подключение Ethernet со скоростью 3 Мбит/с. Эта версия Ethernet определяется в стандарте IETF RFC 895.<br>• **27** — nsip — XNS over IP — предназначен для использования в разнообразных средах передачи данных.<br>• **28** — slip — сетевой интерфейс использует подключение SLIP (Serial Line Internet Protocol). SLIP определяется в стандарте IETF RFC 1055.<br>• **29** — ultra -ULTRA Technologies.<br>• **30** — ds3 — высокоскоростной интерфейс передачи данных, сформированный мультиплексированием сигналов DS1 и DS2; также называется T3.<br>• **31** — sip — сетевой интерфейс использует подключение SLIP (Serial Line Internet Protocol). SLIP определяется в стандарте IETF RFC 1055.<br>• **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:<br>• **1** — up — готов для передачи пакетов.<br>• **2** — down — не работает.<br>• **3** — testing — в режиме тестирования; рабочие пакеты не могут быть переданы. |
| **ifOperStatus** | integer | Текущий статус работы интерфейса:<br>• **1** — up — интерфейс готов для передачи пакетов.<br>• **2** — down — интерфейс не может передавать пакеты данных.<br>• **3** — testing — выполняется тестирование сетевого интерфейса; рабочие пакеты не могут быть переданы.<br>• **4** — unknown — интерфейс находится в неизвестном состоянии.<br>• **5** — dormant — сетевой интерфейс не может передавать пакеты данных, он ожидает внешнее событие.<br>• **6** — notPresente — сетевой интерфейс не может передавать пакеты данных из-за отсутствующего компонента, обычно аппаратного.<br>• **7** — lowerLayerDown — сетевой интерфейс не может передавать пакеты данных, потому что он работает поверх одного или нескольких других интерфейсов, и не менее одного из этих интерфейсов "нижнего уровня" не работает. |
| **ifLastChange** | timeticks | Значение SysUpTime, когда интерфейс оказался в данном состоянии. |
| **ifInOctets** | counter32 | Количество байтов, принятое данным интерфейсом, включая служебные. |

| Наименование | Тип данных | Описание |
|---|---|---|
| **ifInUcastPkts** | counter32 | Количество доставленных пакетов одноадресной рассылки. |
| **ifInNUcastPkts** | counter32 | Количество доставленных многоадресных и широковещательных пакетов. |
| **ifInDiscards** | counter32 | Количество входящих пакетов, которые были отброшены, даже если не было обнаружено ошибок, препятствующих их доставке. Одна из возможных причин отбрасывания: освобождение буферного пространства. |
| **ifInErrors** | counter32 | Количество входящих пакетов, которые содержат ошибки, препятствующие их доставке. |
| **ifInUnknownProtos** | counter32 | Количество пакетов, которые были получены через этот интерфейс и отброшены из-за использования неизвестного или неподдерживаемого протокола. |
| **ifOutOctets** | counter32 | Количество байтов, переданное данным интерфейсом, включая служебные. |
| **ifOutUcastPkts** | counter32 | Количество отправленных пакетов одноадресной рассылки, включая пакеты, которые были отброшены или не отправлены. |
| **ifOutNUcastPkts** | counter32 | Количество отправленных многоадресных и широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены. |
| **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 | Число пакетов в очереди на отправку. |
| **ifInMulticastPkts** | counter32 | Количество доставленных пакетов многоадресной рассылки. |
| **ifInBroadcastPkts** | counter32 | Количество доставленных широковещательных пакетов. |
| **ifOutMulticastPkts** | counter32 | Количество отправленных пакетов многоадресной рассылки, включая пакеты, которые были отброшены или не отправлены. |
| **ifOutBroadcastPkts** | counter32 | Количество отправленных широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены. |
| **ifHCInOctets** | counter64 | Смысл одинаков со смыслом объекта **ifInOctets** — количество байтов, принятое данным интерфейсом, включая служебные; используется счётчик большей ёмкости. |
| **ifHCInUcastPkts** | counter64 | Смысл одинаков со смыслом объекта **ifInUcastPkts** — количество доставленных пакетов одноадресной рассылки; используется счётчик большей ёмкости. |
| **ifHCInMulticastPkts** | counter64 | Смысл одинаков со смыслом объекта **ifInMulticastPkts** — количество доставленных пакетов многоадресной рассылки; используется счётчик большей ёмкости. |
| **ifHCInBroadcastPkts** | counter64 | Смысл одинаков со смыслом объекта **ifInBroadcastPkts** — количество доставленных широковещательных пакетов; используется счётчик большей ёмкости. |
| **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** — 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:<br>• **1** — enabled — включено.<br>• **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:<br>• **1** — true — станция принимает все пакеты/кадры независимо от того, кому они адресованы.<br>• **2** — false — интерфейс принимает только пакеты/кадры, адресованные этой станции.<br>Значение объекта не влияет на приём широковещательных и многоадресных пакетов/кадров. |
| **ifAlias** | string | Название интерфейса, заданное администратором. |
| **ifCounterDiscontinuityTime** | timeticks | Значение SysUpTime, когда произошло событие, ставшее причиной сбоя работы одного или более счётчиков интерфейса. |

**Управление областями**

**Создание управляемых областей**

---

Documentation: ☑
Product: UGMC
Version: 6.1.9

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

Для создания управляемой области администратор UGMC должен выполнить следующие действия:

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

При создании области необходимо указать следующие поля:

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

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

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

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

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

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

**Администраторы области**

---

Documentation: ☑
Product: UGMC
Version: 6.1.9

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

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

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

| Наименование | Описание |
|---|---|
| **Шаг 1.** Создать профиль доступа администратора области | В консоли управления областью в разделе **Администраторы → Профили администраторов** нажать кнопку **Добавить** и указать необходимые настройки. |
| **Шаг 2.** Создать учетную запись администратора и назначить ей один из созданных ранее профилей администратора | В разделе **Администраторы** нажать кнопку **Добавить** и выбрать необходимый вариант:<br>• **Добавить локального администратора** - создать локального пользователя, задать ему пароль доступа и назначить созданный ранее профиль доступа.<br>• **Добавить пользователя LDAP** - добавить пользователя из существующего домена. Для этого должен быть корректно настроен LDAP-коннектор в разделе **Серверы авторизации области**. При входе в консоль администрирования необходимо указывать имя пользователя в формате user@domain. Назначить созданный ранее профиль.<br>• **Добавить группу LDAP** - добавить группу пользователей из существующего домена. Для этого должен быть корректно настроен LDAP-коннектор в разделе **Серверы авторизации области**. При входе в консоль администрирования необходимо указывать имя пользователя в формате user@domain. Назначить созданный ранее профиль. |

При создании профиля доступа администратора необходимо указать следующие параметры:

| Наименование | Описание |
|---|---|
| **Название** | Название профиля |
| **Описание** | Описание профиля |
| **Права доступа на область** | Укажите права доступа на разделы настроек области, такие как администраторы, серверы авторизации, шаблоны устройств, группы шаблонов, управляемые устройства, журналы и отчеты.<br>В качестве доступа можно указать:<br>• Нет доступа.<br>• Чтение.<br>• Чтение и запись. |
| **Права доступа на шаблон** | Укажите здесь права на просмотр и/или изменение настроек всех или конкретных имеющихся шаблонов. Настройки представлены в виде объектов дерева веб-консоли МЭ UserGate, доступных для делегирования. В качестве доступа можно указать:<br>• Нет доступа.<br>• Чтение.<br>• Чтение и запись.<br>Например, можно разрешить сетевые настройки одной группе администраторов, а политики МЭ — другой. |

**Серверы авторизации области**

---

Documentation: ☑
Product: UGMC
Version: 6.1.9

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

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

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

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

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

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

*domain\user/ realm* или *user@domain/ realm*

**Описание**

---

Documentation: ☑
Version: 6.1.9
Product: UGMC

Централизованное управление МЭ UserGate можно разделить на 4 этапа:

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

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

**Шаблоны устройств**

---

Version: 6.1.9
Product: UGMC
Documentation: ☑

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

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

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

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

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

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

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

**Группы шаблонов**

---

Version: 6.1.9
Product: UGMC
Documentation: ☑

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

Для создания группы шаблонов необходимо в разделе **Объекты → 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**

Version: 6.1.9
Product: UGMC
Documentation: ☑

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

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

При создании объекта управляемого устройства необходимо указать следующие параметры:

| Наименование | Описание |
|---|---|
| **Включено** | Включает объект управляемого устройства. Если объект управляемого устройства включен, то он занимает одну лицензию. |
| **Название** | Название для управляемого устройства. Можно вводить произвольное название. |
| **Описание** | Описание управляемого устройства. |
| **Группа шаблонов** | Группа шаблонов, настройки которой следует применить к этому управляемому устройству. |
| **Синхронизация** | Выбор режима синхронизации настроек группы шаблонов к устройству. Возможны 3 варианта:<br>• **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.<br>• **Отключено** — синхронизация выключена.<br>• **Ручная синхронизация** — режим синхронизации, при котором настройки применяются однократно. 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**. |

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

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

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

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

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

| Наименование | Описание |
|---|---|
| | |

| 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:<br>• Версия ПО устройства.<br>• ПИН-код устройства.<br>• Серийный номер ПАК.<br>• Время непрерывной работы.<br>• Показатели загрузки устройства — загрузка ЦП, оперативной памяти, своп-файла, количество пользователей, подключенных через управляемое устройство. |
| **Подключиться к консоли управляемого устройства** | В консоли UGMC необходимо выбрать объект управляемого устройства и нажать на кнопку **Открыть консоль**. В новом окне откроется консоль МЭ UserGate. |
| **Изменить настройки** | В консоли UGMC измените настройки одного из шаблонов, входящего в группу шаблонов, примененного к управляемому устройствау. Новые настройки будут применены к МЭ UserGate. |

**Кластеризация МЭ UserGate с помощью UGMC**

Documentation: ☑
Version: 6.1.9
Product: 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.

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

## Кластер конфигурации

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

Для создания кластера конфигурации необходимо выполнить следующие шаги:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Выполнить первоначальную настройку на первом узле кластера | Смотрите главу **Первоначальная настройка** документа **UserGate 6. Руководство администратора**. |
| **Шаг 2.** Настроить на первом узле кластера зону, через интерфейсы которой будет выполняться репликация кластера | В разделе **Зоны** создать выделенную зону для репликации настроек кластера или использовать существующую (**Cluster**). В настройках зоны разрешить следующие сервисы:<br>• Консоль администрирования<br>• Кластер<br>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.<br>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.<br>Подключиться к веб-консоли второго узла кластера, выбрать язык установки.<br>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.<br>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.<br>После успешного добавления узла в кластер, данный узел будет отображаться в качестве второго узла в списке управляемых устройств с выбранным идентификатором. |

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

Добавление третьего и последующих узлов в кластер конфигурации выполняется аналогично.

## Кластер отказоустойчивости

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

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

Для создания кластера отказоустойчивости необходимо выполнить следующие шаги:

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

Параметры отказоустойчивого кластера:

| Наименование | Описание |
|---|---|
| **Включено** | Включение/отключение отказоустойчивого кластера. |
| **Название** | Название отказоустойчивого кластера. |
| **Описание** | Описание отказоустойчивого кластера. |
| **Режим кластера** | Режим отказоустойчивого кластера:<br>• **Актив-Актив** - нагрузка распределяется на все узлы кластера<br>• **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**

Version: 6.1.9
Product: UGMC
Documentation: ☑

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

Для управления обновлениями с помощью UGMC необходимо выполнить следующие действия:

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

## Обновление ПО

Компания UserGate периодически выпускает обновления программного обеспечения МЭ UserGate. Эти обновления выкладываются в репозитарий UserGate ( http://static.usergate.com), откуда они уже доступны для скачивания МЭ. Если МЭ UserGate подключен к управлению через Management Center, то он проверяет наличие обновлений на сервере Management Center, который сам будет являться репозитарием. 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.<br>Для загрузки обновлений из репозитария необходимо в разделе **Объекты → 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.<br>Для загрузки вручную необходимо в разделе **Объекты → 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.<br>Если требуется установить данное обновление на группу устройств (например, для проведения тестирования), то необходимо в свойствах обновления указать управляемые устройства, для которых данное обновление будет доступно, и установить чекбокс **Утвердить обновление**. |
| **Шаг 3.** Провести установку обновления | После утверждения обновление становится доступным для скачивания для всех или группы управляемых устройств. УО скачивает обновление в соответствии с расписанием проверки обновлений. После скачивания обновление может быть установлено администратором в консоли МС или в ручном режиме администратором управляемого устройства. |

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

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

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

Обновление библиотек в репозитарии UGMC имеет следующие свойства:

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

**Приложения**

**Требования к сетевому окружению**

Documentation: ☑
Product: UGMC
Version: 6.1.9

| 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.<br>Доступ к серверам:<br>• 93.91.171.46;<br>• 178.154.221.222;<br>• ra.entensys.com. |
| **NTP** | UDP | 123 | Исходящий (до сервера точного времени) | Синхронизация времени. |
| **DNS** | UDP | 53 | Исходящий (от UserGate до DNS-сервера) | Сервис получения информации (IP-адрес) о доменах. |
| **Регистрация сервера UserGate** | TCP | 443 | Исходящий (до сервера регистрации) | Доступ до сервера регистрации продуктов UserGate reg2.entensys.com. |
| **Обновление ПО и библиотек** | TCP | 443 | Исходящий (до серверов обновления) | Обновление программного обеспечения и элементов библиотек: доступ до сервера static.entensys.com. |
| **Репликация настроек** | TCP | 4369 | Входящий (с первого узла кластера на второй и последующие узлы) | Сервис, необходимый для работы кластера конфигурации.<br>Установка управляющего соединения. |
| | | 9000-9100 | Входящий (приём конфигурации от первого узла кластера) | Передача информации об изменении конфигурации кластера (реплика настроек) |
| **Сервис UserGate Management Center** | TCP | 9712 | Входящий (к UGMC от NGFW) | Первоначальная установка связи и обмен ключами шифрования управляемых устройств и сервера UserGate Management Center. |
| | | 2022 | Входящий (к UGMC от NGFW) | Построение SSH-туннеля для обмена данными с помощью полученных ключей. |
| **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 установке связи. |
| | | 22000-22711 | Входящий (к UGMC от UG Client) | Передача журналов и телеметрии с UG Client на UG LogAn транзитом через UGMC. |
| **LDAP** | TCP | 389, 636 | Исходящий (на LDAP-коннектор) | Выполнение запросов LDAP (389 - для LDAP и 636 - для LDAP over SSL). |
| **SNMP** | UDP | 161 | Входящий (до UserGate) | Доступ к серверу UserGate по протоколу SNMP. |
| **SMTP** | TCP | 25 | Исходящий (до почтового сервера) | Отправка уведомлений на электронную почту. |
| **DHCP** | UDP | 67, 68 | Исходящий (запрос на получение адреса от UserGate на сервер DHCP) | Сервис службы DHCP. |
| **FTP (экспорт журналов)** (начиная с версии 7.1.0) | TCP | 21 | Исходящий (до сервера FTP) | Экспорт журналов на сервер FTP. |
| **SSH (экспорт журналов)** (начиная с версии 7.1.0) | TCP | 22 | Исходящий (до сервера SSH) | Экспорт журналов на сервер SSH. |
| **Syslog (экспорт журналов)** (начиная с версии 7.1.0) | TCP/UDP | 514 | Исходящий (до сервера Syslog) | Экспорт журналов на сервер Syslog. |
| **Ручная проверка сайтов по категориям** | TCP | 80/443 | Исходящий (до updates.usergate.com) | Ручная проверка сайтов по категориям. |

Documentation: ☑
Product: UGMC
Version: 6.1.9

## 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:<br>• 0 — информационные.<br>• 6 — предупреждения.<br>• 8 — ошибки.<br>• 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@einersonstal |
| | **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** | Время получения события в формате: yyyy-mm-ddThh:mm:ssZ. | 2022-05-12T08:11:46.15869Z |
| **ip_address** | IPv4-адрес источника события. | 192.168.174.134 |
| **node** | Имя, которое однозначно идентифицирует устройство, генерирующее это событие. | mc_core@einersonstal |
| **attributes** | Детали события в формате JSON. | {"rule":{"logrotate":12,"attributes":{"timezone":"Asia/Novosibirsk"},"id":"66f9de9f-d698-4bec-b3b0-ba65b46d3608","name":"Example log export ftp"} |
| **event_type** | Тип события. | logexport_rule_updated |
| **event_severity** | Важность события. | info (информационные), warning (предупреждения), error (ошибки), critical (критичные). |
| **event_origin** | Модуль, в котором произошло событие. | core |
| **event_component** | Компонент, в котором произошло событие. | console_auth |

**Принятые обозначения и сокращения**

**Введение**

**Описание**

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

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

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

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

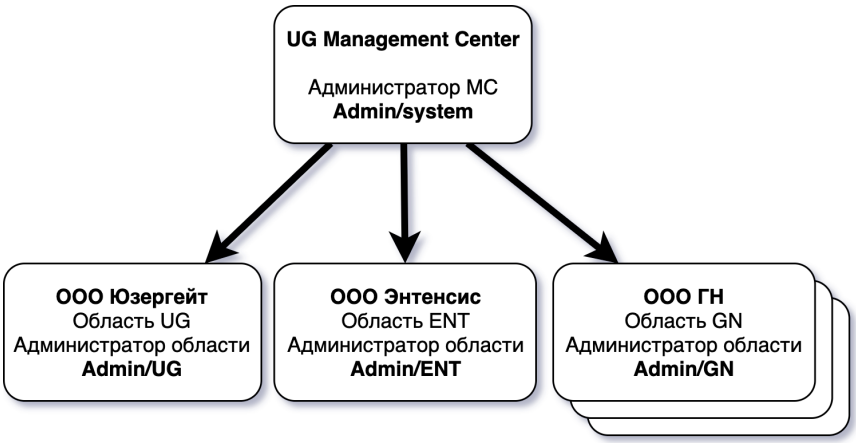
**Управляемые области**

---

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

UGMC поддерживает облачную модель управления, то есть предоставляет возможность полностью независимого управления устройствами разных предприятий, используя единый сервер управления. Разделение полномочий происходит на уровне управляемых областей. Управляемая область UserGate — это логический объект, представляющий одно предприятие или группу предприятий, управляемых одним администратором. Каждой области назначается отдельный администратор, который может администрировать только одну назначенную ему область. Администратор одной области не может ни при каких обстоятельствах получить доступ к другой области. Администратор сервера UGMC имеет полномочия создавать управляемые области и назначать в них администраторов, не имея при этом доступа к объектам самой области. Более подробно о разграничении прав администраторов смотрите в главе Администраторы.

Пример UGMC с несколькими управляемыми областями:




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

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

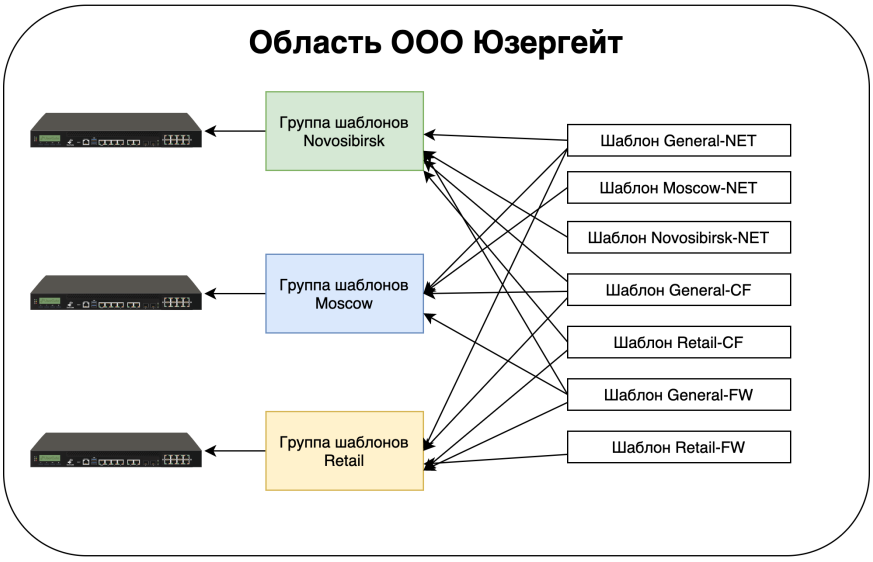
**Шаблоны и группы шаблонов**

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

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

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

Пример области с несколькими группами шаблонов для управления МЭ UserGate:



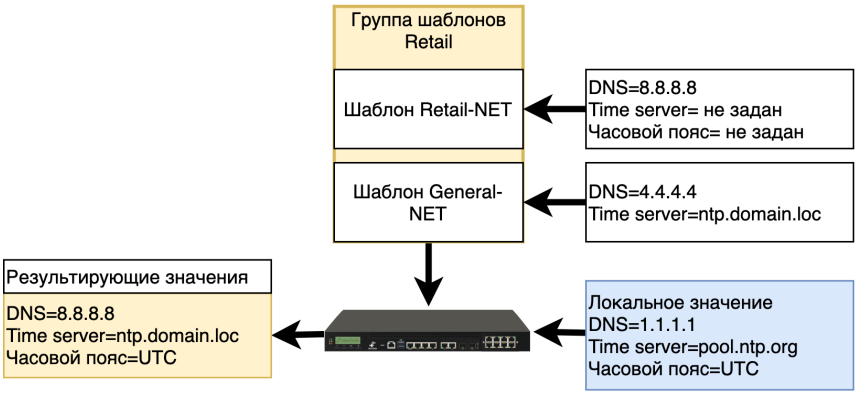

Конфигурация, передаваемая на устройство, может быть двух типов:

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

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

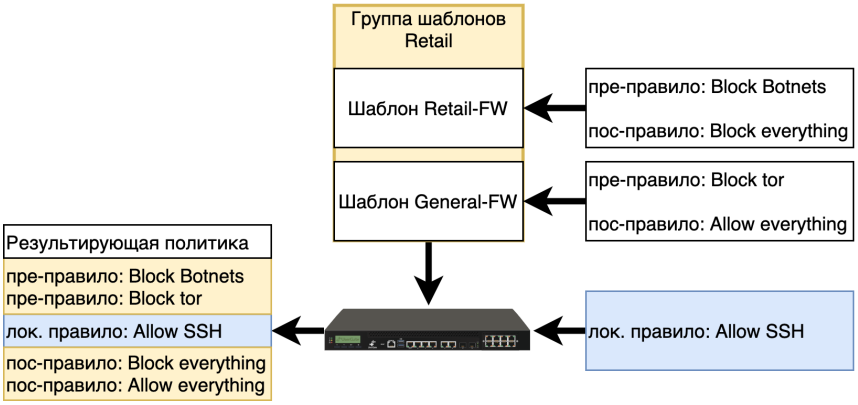
Настройка параметра при конфликтующих значениях в разных шаблонах одной группы шаблонов принимает значение, заданное в наиболее верхнем шаблоне. Локально указанные настройки данного параметра игнорируются.

Пример результирующего значения параметра, определенного в нескольких шаблонах:




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

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



**Управляемые устройства**

---

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

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

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

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

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

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

## Управление сервисами UGMC

Управление сервисами UGMC включает в себя следующие задачи:

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

## Управление областями UGMC

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

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

## Ролевое управление

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

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

| Администратор | Профиль администратора | Уровень доступа |
|---|---|---|
| AdminTemplates/realm_code | Templates | Создание и модификация всех шаблонов области. |
| AdminTemplateGeneral/realm_code | TemplateGeneral | Только модификация шаблона General. |
| AdminTemplateGeneralNET/realm_code | TemplateGeneralNET | Только модификация сетевых настроек в шаблоне General. |

**Лицензирование UGMC**

**Лицензирование UGMC**

---

Documentation: ☑
Product: UGMC
Version: 6.1.9, 7.0.1

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

Лицензия на UGMC дает право бессрочного пользования продуктом.

Дополнительно лицензируются следующие модули:

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

Для регистрации продукта необходимо выполнить следующие шаги:

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

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

**Планирование внедрения UGMC**

**Планирование внедрения UGMC (Описание)**

Documentation: ☑
Product: UGMC
Version: 7.0.1, 7.1.0

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

При планировании архитектуры рекомендуется:

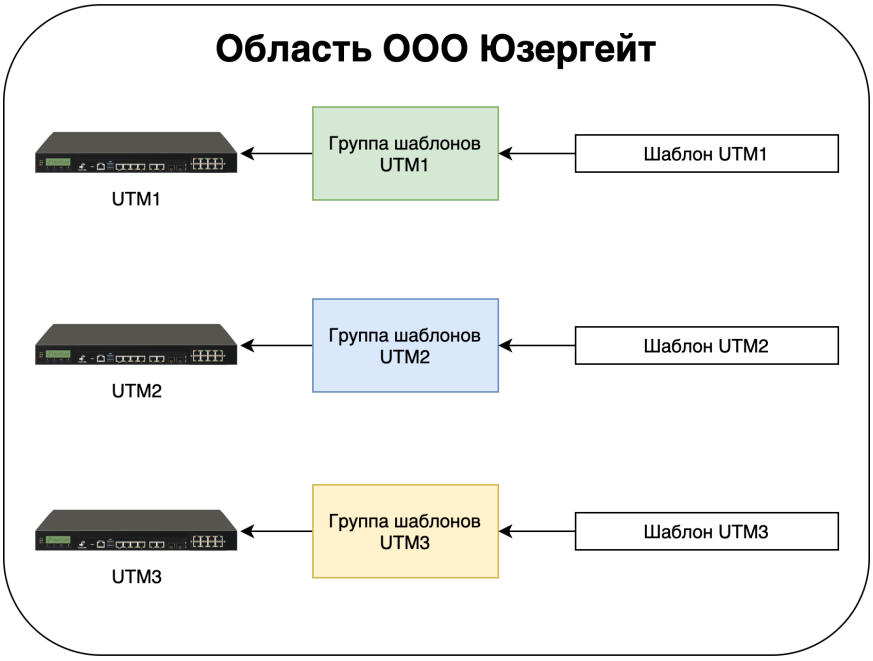
- Избегать конфликта настроек при добавлении шаблонов в группы шаблонов. Наличие конфликтов всегда усложняет управление конечными устройствами. Это основополагающий принцип, из которого вытекают следующие рекомендации.
- Разделять различные группы настроек в разные шаблоны, например, общие настройки управляемых устройств — в одном, политики контентной фильтрации — в другом, политики межсетевого экранирования — в третьем, политики 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.

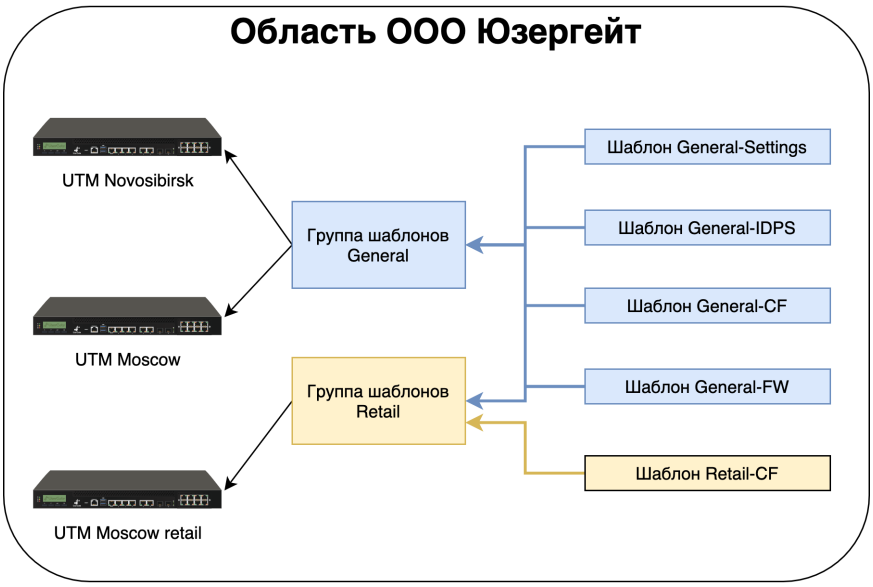
Рекомендуется для простых внедрений с небольшим количеством МЭ UserGate. Пример такой настройки представлен на рисунке ниже.




## 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 централизованно 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.



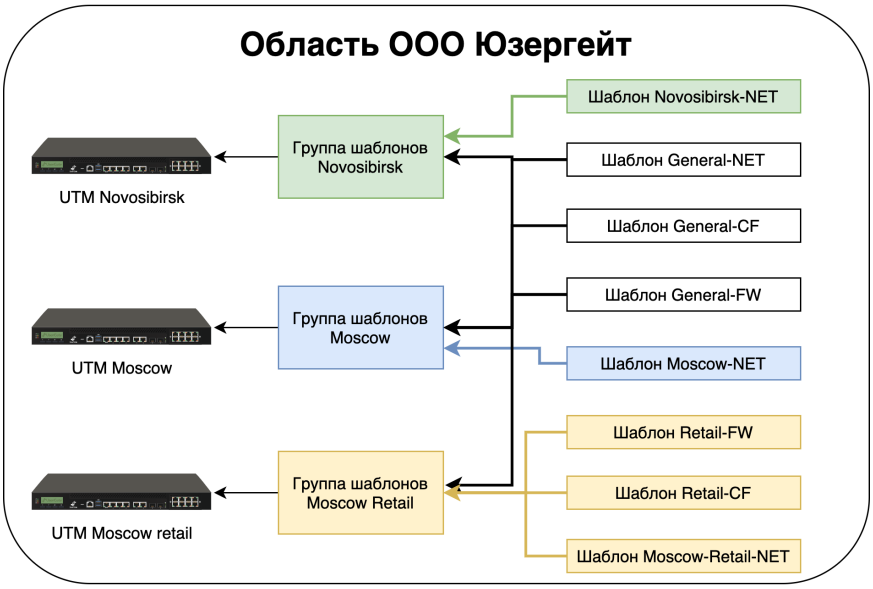

В данном примере шаблоны содержат следующие настройки:

- 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**

Documentation: ☑
Product: UGMC
Version: 7.0.1, 7.1.0

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

## Развертывание программно-аппаратного комплекса

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

## Развертывание виртуального образа

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

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

Для начала работы с виртуальным образом, выполните следующие шаги:

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

## Подключение к UGMC

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

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

Остальные интерфейсы отключены и требуют последующей настройки.

Первоначальная настройка требует выполнения следующих шагов:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Подключиться к интерфейсу управления. | **При наличии DHCP-сервера**<br>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.<br>**Статический IP-адрес**<br>Включить UGMC. Используя CLI (Command Line Interface), назначить необходимый IP-адрес на интерфейс port0. Детали использования CLI смотрите в главе Интерфейс командной строки (CLI).<br>Подключиться к веб-консоли UGMC по указанному адресу, он должен выглядеть примерно следующим образом:<br>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 интерфейсами читайте в главе Настройка интерфейсов. Система поставляется с предопределенными зонами:<br>• Зона **Management** (сеть управления), интерфейс port0.<br>• Зона **Trusted** (LAN). Предполагается, что через эту зону UGMC будет подключаться к управляемым устройствам, а также получит доступ в интернет.<br>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. |

| Наименование | Описание |
| --- | --- |
| **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.<br>Более подробно о лицензировании продукта читайте в главе Лицензирование UGMC. |
| **Шаг 9.** Создать как минимум одну управляемую область. | В разделе **Управляемые области → Области** добавить управляемую область. |
| **Шаг 10.** Создать администратора созданной управляемой области. | В разделе **Администраторы** создать профиль администратора и дать ему права на управление созданной областью. Создать администратора с данным профилем. |
| **Шаг 11.** Создать дополнительных администраторов UGMC (опционально). | В разделе **Администраторы** создать необходимые профили для управления сервисами UGMC и создать администраторов UGMC с этими профилями. |

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

**Офлайн операции с сервером**

**Офлайн операции с сервером(Описание)**

---

Documentation: ☑
Product: UGMC
Version: 7.0.1, 7.1.0

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

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

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

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

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

**Настройка UGMC**

**Общие настройки**

---

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

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

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

**Управление устройством**

Version: 7.0.1
Product: UGMC
Documentation: ☑

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

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

## Кластеризация и отказоустойчивость

UGMC поддерживает 2 типа кластеров:

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

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

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

| Наименование | Описание |
|---|---|
| Настройки, уникальные для каждого узла | Настройки диагностики;<br>Настройки интерфейсов;<br>Настройки шлюзов;<br>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:<br>• Консоль администрирования;<br>• Кластер.<br>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 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).<br>Подключиться к веб-консоли второго узла кластера, выбрать язык установки.<br>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.<br>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. |

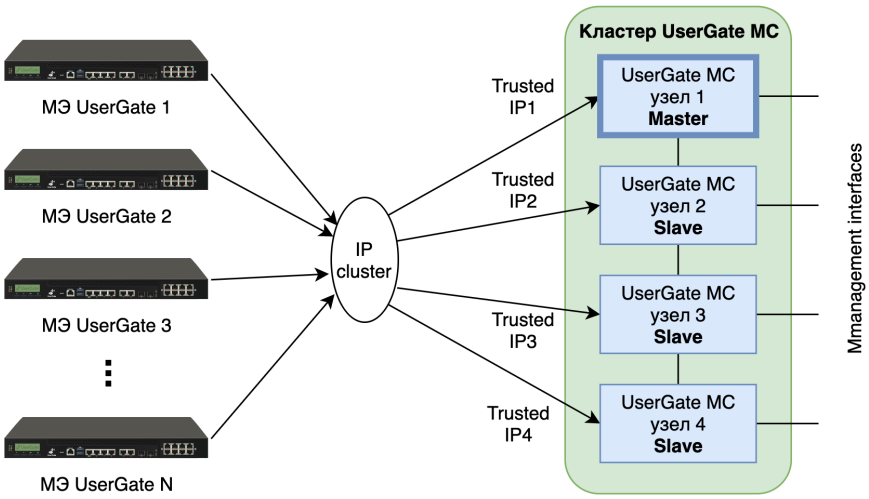
До четырех узлов кластера конфигурации можно объединить в отказоустойчивый кластер. Самих кластеров отказоустойчивости может быть несколько. Поддерживаются 2 режима — **Актив-Актив** и **Актив-Пассив**.

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.



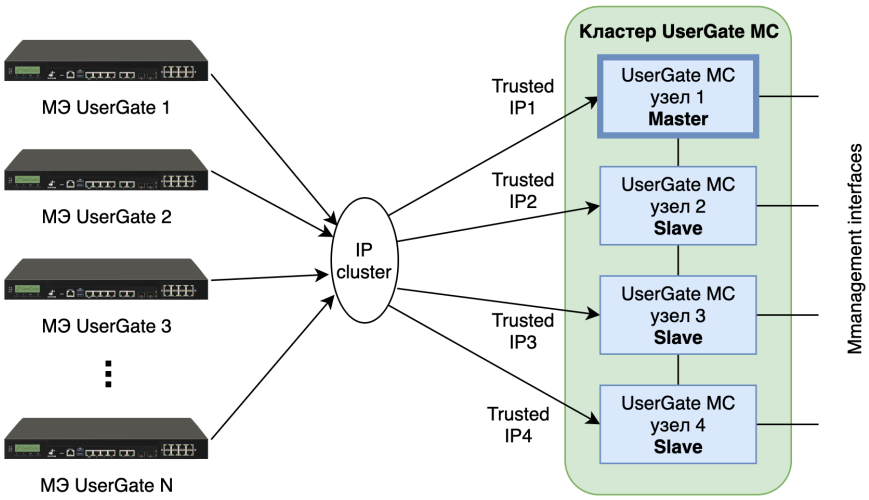

Кластерный IP-адрес находятся на узле UGMC 1. Если узел UGMC 1 становится недоступным, то кластерный IP-адрес перейдет на следующий сервер, который станет мастер-сервером, например, UGMC 2.

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:<br>• **Актив-Актив** — нагрузка распределяется на все узлы кластера;<br>• **Актив-Пассив** — нагрузка идет на Мастер-узел и переключается на запасной узел в случае недоступности Мастер-узла. |

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

## Диагностика

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

| Наименование | Описание |
|---|---|
| **Детализация диагностики** | • **Off** — ведение журналов диагностики отключено;<br>• **Error** — журналировать только ошибки работы сервера;<br>• **Warning** — журналировать только ошибки и предупреждения;<br>• **Info** — журналировать только ошибки, предупреждения и дополнительную информацию;<br>• **Debug** — максимум детализации.<br>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;<br>• **Очистить журналы** — очистить содержимое журналов. |
| **Удаленный помощник** | • **Включено**/**Отключено** — включение/отключение режима удаленного помощника. Удаленный помощник позволяет инженеру технической поддержки UserGate, зная значения идентификатора и токена удаленного помощника, произвести безопасное подключение к серверу UGMC для диагностики и решения проблем. Для успешной активации удаленного помощника UGMC должен иметь доступ к серверу удаленного помощника компании UserGate по протоколу SSH.<br>• **Идентификатор удаленного помощника** — полученное случайным образом значение. Уникально для каждого включения удаленного помощника.<br>• **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;<br>• **Выключить** — выключение сервера UGMC. |
| **Обновления** | Выбор канала обновлений ПО UGMC<br>• **Стабильные** — проверка наличия стабильных обновлений ПО;<br>• **Бета** — проверка наличия экспериментальных обновлений. |

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

Для установки обновлений необходимо выполнить следующие действия:

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

## Управление резервным копированием

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

Для создания резервной копии необходимо выполнить следующие действия:

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

Для восстановления состояния устройства необходимо выполнить следующие действия:

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

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

| Наименование | Описание |
|---|---|
| **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:<br>• **Тип сервера** — FTP или SSH;<br>• **Адрес сервера** — IP-адрес сервера;<br>• **Порт** — порт сервера;<br>• **Логин** — учетная запись на удаленном сервере;<br>• **Пароль**/**Повторите пароль** — пароль учетной записи;<br>• **Путь на сервере** — путь на сервере, куда будут выгружены настройки.<br>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**.<br>**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**.<br>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.<br>**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:<br>(минуты:0-59) (часы:0-23) (дни месяца:1-31) (месяц:1-12) (день недели:0-6, 0-воскресенье)<br>Каждое из первых пяти полей может быть задано следующим образом:<br>• Звездочка (*) — обозначает весь диапазон (от первого до последнего);<br>• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7;<br>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23"<br>• 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:<br>• текущие настройки сервера под именем: cc_core-mc_core @nodename_version_YYYYMMDD_HHMMSS.bin<br>• сетевые настройки под именем: network-cc_core-mc_core @nodename_version_YYYYMMDD_HHMMSS.bin<br>nodename — имя узла UserGate Management Center.<br>version — версия UserGate Management Center.<br>YYYYMMDD_HHMMSS — дата и время выгрузки настроек в часовом поясе UTC.<br>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.

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:<br>• **Тип сервера** — FTP или SSH;<br>• **Адрес сервера** — IP-адрес сервера;<br>• **Порт** — порт сервера;<br>• **Логин** — учетная запись на удаленном сервере;<br>• **Пароль**/**Подтверждение пароля** — пароль учетной записи;<br>• **Путь на сервере** — путь на сервере, куда будут выгружены настройки. |

| Наименование | Описание |
| --- | --- |
| **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:<br>(минуты:0-59) (часы:0-23) (дни месяца:1-31) (месяц:1-12) (день недели:0-6, 0-воскресенье)<br>Каждое из первых пяти полей может быть задано следующим образом:<br>• Звездочка (*) — обозначает весь диапазон (от первого до последнего);<br>• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7;<br>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23";<br>• 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**

---

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

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

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

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

| Наименование | Описание |
|---|---|
| **Шаг 1.** Создать профиль доступа администратора. | В разделе **Администраторы → Профили администраторов** нажать кнопку **Добавить** и указать необходимые настройки. |
| **Шаг 2.** Создать учетную запись администратора и назначить ей один из созданных ранее профилей администратора. | В разделе **Администраторы** нажать кнопку **Добавить** и выбрать необходимый вариант:<br>• **Добавить локального администратора** — создать локального пользователя, задать ему пароль доступа и назначить созданный ранее профиль доступа.<br>• **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.<br>• **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.<br>• **Добавить администратора с профилем аутентификации** — создать пользователя, назначить созданный ранее профиль администратора и профиль аутентификации (необходимы корректно настроенные серверы аутентификации).<br>**Важно!** В данном разделе настроек сервисов консоли управления администратором области может быть назначен только локальный администратор. Это связано с тем, что LDAP серверы, используемые для аутентификации администраторов сервиса UGMC и для аутентификации администраторов области, могут быть разными. При необходимости использования LDAP администраторов для управления Областью, их необходимо создать в самой области. Более подробно об администраторах области смотрите в разделе Администраторы области. |

При создании профиля доступа администратора необходимо указать следующие параметры:

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

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

Для настройки этих параметров необходимо:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Настроить политику паролей. | В разделе **Администраторы → Администраторы** нажать кнопку **Настроить**. |
| **Шаг 2.** Заполнить необходимые поля. | Указать значения следующих полей:<br>• **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.<br>• **Число неверных попыток аутентификации** — количество неудачных попыток аутентификации администратора, после которых учетная запись заблокируется на **Время блокировки**.<br>• **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.

**Управление сертификатами**

---

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

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

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

| Наименование | Описание |
|---|---|
| **Шаг 1.** Создать сертификат. | Нажать на кнопку **Создать** в разделе **Сертификаты** |
| **Шаг 2.** Заполнить необходимые поля. | Указать значения следующих полей:<br>• **Название** — название сертификата, под которым он будет отображен в списке сертификатов.<br>• **Описание** — описание сертификата.<br>• **Страна** — страна, в которой выписывается сертификат.<br>• **Область или штат** — область или штат, в котором выписывается сертификат<br>• **Город** — город, в котором выписывается сертификат.<br>• **Название организации** — название организации, для которой выписывается сертификат.<br>• **Common name** — имя сертификата. Рекомендуется использовать только символы латинского алфавита для совместимости с большинством браузеров.<br>• **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:<br>• **Экспорт сертификата** — экспортирует данные сертификата в der-формате без экспортирования приватного ключа сертификата.<br>• **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:<br>• Название — название сертификата, под которым он будет отображен в списке сертификатов.<br>• Описание — описание сертификата.<br>• Загрузите файл, содержащий данные сертификата.<br>• Загрузите файл, содержащий приватный ключ сертификата.<br>• Пароль для приватного ключа, если таковой требуется.<br>• Цепочка сертификатов — файл, содержащий сертификаты вышестоящих центров сертификации, которые участвовали в создании сертификата. Необязательное поле. |

**Серверы аутентификации UGMC**

Version: 7.0.1, 7.1.0
Product: UGMC
Documentation: ☑

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

## LDAP-коннектор

LDAP-коннектор позволяет:

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

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

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

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

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

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

## Сервер аутентификации RADIUS

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

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

| Наименование | Описание |
|---|---|
| **Включено** | Включение/отключение использования данного сервера аутентификации. |
| **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. |

| Наименование | Описание |
| --- | --- |
| **Использовать одно TCP-соединение** | Использовать одно TCP-соединение для работы с сервером TACACS+. |
| **Таймаут (сек)** | Время ожидания сервера TACACS+ для получения аутентификации. По умолчанию 4 секунды. |

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

**Профили аутентификации UGMC**

---

Documentation: ☑
Version: 7.0.1, 7.1.0
Product: UGMC

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

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

Version: 7.0.1, 7.1.0
Product: UGMC
Documentation: ☑

## Почтовые адреса

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

Для добавления новой группы почтовых адресов необходимо выполнить следующие шаги:

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

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

| Наименование | Описание |
|---|---|
| **Шаг 1.** Создать файл с необходимыми списком почтовых адресов. | Создать файл **list.txt** со списком почтовых адресов. |
| **Шаг 2.** Создать архив, содержащий этот файл. | Поместить файл в архив zip с именем **list.zip**. |
| **Шаг 3.** Создать файл с версией списка. | Создать файл **version.txt**, внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка. |
| **Шаг 4.** Разместить файлы на веб-сервере. | Разместить у себя на сайте **list.zip и version.txt**, чтобы они были доступны для скачивания. |
| **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:<br>• Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет.<br>• Ежедневно.<br>• Еженедельно.<br>• Ежемесячно.<br>• Каждые ... часов.<br>• Каждые ... минут.<br>• Задать вручную.<br>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:<br>• Звездочка (*) — обозначает весь диапазон (от первого до последнего).<br>• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.<br>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".<br>Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа". |

## Номера телефонов

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

Для добавления новой группы телефонных номеров необходимо выполнить следующие шаги:

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

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

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

| Наименование | Описание |
|---|---|
| **Шаг 5.** Создать список телефонных номеров и указать URL для обновления. | На каждом UserGate создать список номеров. При создании указать тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. UserGate будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты:<br>• Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет.<br>• Ежедневно.<br>• Еженедельно.<br>• Ежемесячно.<br>• Каждые ... часов.<br>• Каждые ... минут.<br>• Задать вручную.<br>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:<br>• Звездочка (*) — обозначает весь диапазон (от первого до последнего).<br>• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.<br>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".<br>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. |
| **Пароль** | Пароль учетной записи для подключения к SMPP-серверу. |
| **Правила трансляции номеров** | В некоторых случаях SMPP-провайдер ожидает номер телефона в определенном формате, например, в виде 89123456789. Для соответствия требованиям провайдера можно указать замену первых символов номеров с одних на другие. Например, заменить все номера, начинающиеся на +7, на 8. |

**Расширение системного раздела**

---

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

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

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

**Настройка сети**

Documentation: ☑
Product: UGMC
Version: 7.0.1, 7.1.0

В данном разделе описаны сетевые настройки UGMC.

## Настройка зон

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

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

По умолчанию UGMC поставляется со следующими зонами:

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

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

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

**Примечание**Можно создать не более 255 зон.

Для создания зоны необходимо выполнить следующие шаги:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Создать зону. | Нажать на кнопку **Добавить** и дать название зоне. |
| **Шаг 2.** Настроить параметры защиты зоны от DoS (опционально). | Указать параметры защиты зоны от сетевого флуда для протоколов TCP (SYN-flood), UDP, ICMP:<br>• **Порог уведомления** — при превышении количества запросов с одного IP-адреса над указанным значением происходит запись события в системный журнал.<br>• **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.<br>Рекомендованные значения для порога уведомления — 300 запросов в секунду, для порога отбрасывания пакетов — 600 запросов в секунду.<br>**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. |
| **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.<br>Сервисы:<br>• **Ping** — позволяет пинговать UGMC.<br>• **SNMP** — доступ к UserGate по протоколу SNMP (UDP 161).<br>• **Консоль администрирования** — доступ к веб-консоли управления (TCP 8010 и 8300).<br>• **XML-RPC для управления** — позволяет управлять продуктом по API (TCP 4041).<br>• **VRRP** — сервис, необходимый для объединения нескольких NGFW в отказоустойчивый кластер (IP протокол 112).<br>• **Кластер** — сервис, необходимый для объединения нескольких NGFW в кластер (TCP 4369, TCP 9000-9100).<br>• **CLI по SSH** — доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200.<br>• **Сервис UserGate Management Center** — сервис подключения NGFW и LogAn (TCP 2022, 9712).<br>Подробнее о требованиях сетевой доступности читайте в Приложение 1. Требования к сетевому окружению. |
| **Шаг 4.** Настроить параметры защиты от IP-спуфинг атак (опционально). | Атаки на основе IP-спуфинга позволяют передать пакет из одной сети, например, из **Trusted**, в другую, например, в **Management**. Для этого атакующий подменяет IP-адрес источника на предполагаемый адрес необходимой сети. В таком случае ответы на этот пакет будут пересылаться на внутренний адрес.<br>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.<br>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 |
|---|---|

| 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** | Режим работы бонда должен совпадать с режимом работы на том устройстве, куда подключается бонд. Может быть:<br>• **Round robin.** Пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. Эта политика применяется для балансировки нагрузки и отказоустойчивости.<br>• **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.<br>• **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.<br>• **Broadcast.** Передает все на все сетевые интерфейсы. Эта политика применяется для отказоустойчивости.<br>• **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.<br>• **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.<br>• **Adaptive load balancing.** Включает в себя предыдущую политику плюс осуществляет балансировку входящего трафика. Не требует дополнительной настройки на коммутаторе. Балансировка входящего трафика достигается путем ARP-переговоров. Драйвер перехватывает ARP-ответы, отправляемые с локальных сетевых карт наружу, и переписывает MAC-адрес источника на один из уникальных MAC-адресов сетевой карты, участвующей в объединении. Таким образом, различные пиры используют различные MAC-адреса сервера. Балансировка входящего трафика распределяется последовательно (round-robin) между интерфейсами. |
| **MII monitoring period (мсек)** | Устанавливает периодичность MII-мониторинга в миллисекундах. Определяет, как часто будет проверяться состояние линии на наличие отказов. Значение по умолчанию — 0 — отключает MII-мониторинг. |
| **Down delay (мсек)** | Определяет время (в миллисекундах) задержки перед отключением интерфейса, если произошел сбой соединения. Эта опция действительна только для мониторинга MII (miimon). Значение параметра должно быть кратным значениям miimon. Если оно не кратно, то округлится до ближайшего кратного значения. Значение по умолчанию 0. |
| **Up delay (мсек)** | 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:<br>• **Slow** — запрос партнера на передачу LACPDU-пакетов каждые 30 секунд.<br>• **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:<br>• **Отключено** — устанавливает одинаковый MAC-адрес на всех интерфейсах во время переключения.<br>• **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.<br>• **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:<br>• **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.<br>• **Layer 2+3** — использует как MAC-адреса, так и IP-адреса для генерации хэша. Алгоритм совместим с IEEE 802.3ad.<br>• **Layer 3+4** — используются IP-адреса и протоколы транспортного уровня (TCP или UDP) для генерации хэша. Алгоритм не всегда совместим с IEEE 802.3ad, так как в пределах одного и того же TCP- или UDP-взаимодействия могут передаваться как фрагментированные, так и нефрагментированные пакеты. Во фрагментированных пакетах порт источника и порт назначения отсутствуют. В результате в рамках одной сессии пакеты могут дойти до получателя не в том порядке, так как отправляются через разные интерфейсы. |
| **Сеть** | Способ присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. |

### Настройка шлюзов

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

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

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

При наличии двух или более шлюзов возможны 2 варианта работы:

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

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

### Маршруты

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

Для добавления маршрута необходимо выполнить следующие шаги:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Задать название и описание данного маршрута. | В разделе **Сеть** выберите в меню **Маршруты**, нажмите кнопку **Добавить**. Укажите имя для данного маршрута. Опционально можно задать описание маршрута. |
| **Шаг 2.** Указать адрес назначения. | Задайте подсеть, куда будет указывать маршрут, например, 172.16.20.0/24 или 172.16.20.5/32. |
| **Шаг 3.** Указать шлюз. | Задайте IP-адрес шлюза, через который указанная подсеть будет доступна. Этот IP-адрес должен быть доступен с сервера UGMC. |
| **Шаг 4.** Указать интерфейс. | Выберите интерфейс, через который будет добавлен маршрут. Если оставить значение **Автоматически**, то UGMC сам определит интерфейс, исходя из настроек IP-адресации сетевых интерфейсов. |
| **Шаг 5.** Указать метрику. | Задайте метрику маршрута. Чем меньше метрика, тем приоритетней маршрут, если маршрутов несколько в данную сеть несколько. |

**Интерфейс командной строки (CLI)**

**Интерфейс командной строки (CLI) Описание**

---

Documentation: ☑
Product: UGMC
Version: 7.0.1, 7.1.0

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

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

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

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

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

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

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

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

| Наименование | Описание |
|---|---|
| **Шаг 1.** Разрешить доступ к CLI (SSH) для выбранной зоны | Разрешить доступ для протокола CLI по SSH в настройках зоны, к которой вы собираетесь подключаться для управления с помощью CLI. Будет открыт порт TCP 2200. |
| **Шаг 2.** Запустить SSH-терминал | Запустить у себя на компьютере SSH-терминал, например, SSH для Linux или Putty для Windows. Указать в качестве адреса адрес UGMC, в качестве порта подключения - 2200, в качестве имени пользователя - имя пользователя правами корневого администратора UGMC (по умолчанию Admin/system). Для Linux команда на подключение должна выглядеть так:<br>*ssh Admin/system@IPUserGateMC -p 2200* |
| **Шаг 3.** Войти в CLI | Войти в CLI, используя пароль пользователя, указанного на предыдущем шаге. Если устройство UGMC не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin/system, в качестве пароля - utm. |

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

**help command**

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

**help Iface**

Полный список команд:

| Наименование | Описание |
|---|---|
| **help** | Показывает список доступных команд. |
| **exit**<br>**quit**<br>**Ctrl+D** | Выйти из CLI. |
| **date** | Посмотреть текущее время на сервере. |
| **gateway** | Посмотреть или задать значения шлюза. Смотрите gateway help для детальной информации. |
| **iface** | Набор команд для просмотра и настройки параметров сетевого интерфейса. Смотрите iface help для детальной информации. |
| **license** | Посмотреть информацию о лицензии. |
| **netcheck** | Проверить доступность стороннего HTTP/HTTPS-сервера.<br>**netcheck [-t TIMEOUT] [-d] URL**<br>Опции:<br>-t - максимальный таймаут ожидания ответа от веб-сервера<br>-d - запросить содержание сайта. По умолчанию запрашиваются только заголовки. |
| **nslookup** | Выполнить определение IP-адреса по имени хоста. |
| **ping** | Выполнить ping определенного хоста. |

| Наименование | Описание |
| --- | --- |
| **radmin** | Включить или отключить удаленный доступ к серверу для технической поддержки UserGate. |
| **radmin_e** | Включить или отключить удаленный доступ к серверу для технической поддержки UserGate, в случаях, когда сервер UGMC завис. |
| **reboot** | Перезагрузить сервер UserGate Management Center. |
| **route** | Создать, изменить, удалить маршрут. |
| **shutdown** | Выключить сервер UGMC. |
| **traceroute** | Выполнить трассировку соединения до определенного хоста. |
| **zone** | Набор команд для просмотра и настройки параметров зоны. Смотрите zone help для детальной информации. |

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

## Мониторинг маршрутов

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

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

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

## Ping

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

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

## Traceroute

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

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

## Запрос DNS

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

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

## Оповещения

## Правила оповещений

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

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

При добавлении правила необходимо указать следующие параметры:

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

## SNMP

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

Для настройки мониторинга с помощью SNMP необходимо:

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

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

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

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

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

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

Для скачивания доступны следующие MIB-файлы:

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

**UTM-TRAPS-MIB**

| Наименование | Описание |
|---|---|
| **trapCoreCrush** | Сбой ядра. |
| **trapStatDown** | Сервис статистики (UserGate Log Analyzer) недоступен. |
| **trapCoreBootstrapEnd** | Загрузка сервера завершена успешно. |
| **trapDefaultGatewayChanged** | Изменение шлюза по умолчанию. |
| **trapHighSessionsCounter** | Таблица сессий заполнена на 90%. |
| **trapHighUsersCounter** | Количество активных пользователей достигло 90% от порога лицензии. |
| **trapStatusChanged** | Изменение статуса узла отказоустойчивого кластера. |
| **trapMemberUp** | Статус узла отказоустойчивого кластера изменился на «Подключен». |
| **trapMemberDown** | Узел отказоустойчивого кластера отключен. |
| **trapAttackDetected** | Обнаружена атака 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. |
| **trapTrafficDrop** | Срабатывание запрещающего правила межсетевого экрана. |
| **trapLDAPServerDown** | Сервер LDAP недоступен. |

**UTM-TRAPS-BINDINGS-MIB**

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

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

**UTM-MIB**

| Наименование | Тип данных | Описание |
|---|---|---|
| **vcpuCount** | integer | Количество виртуальных процессоров в системе. |
| **vcpuUsage** | integer | Загруженность виртуальных процессоров системы; отображается в %. |
| **usersCounter** | integer | Количество активных пользователей на текущий момент времени. |
| **cpuLoad** | integer | Загруженность центрального процессора системы; отображается в %. |
| **memoryUsed** | integer | Использование оперативной памяти; отображается в %. |
| **logDiskSpace** | integer | Пространство на диске, используемое под журналы; отображается в %. |
| **Sys_power_supply1_status** | string | Состояние первого источника питания:<br>• **no_power_supplies**.<br>• **on**.<br>• **off**. |
| **Sys_power_supply2_status** | string | Состояние второго источника питания.<br>• **no_power_supplies**.<br>• **on**.<br>• **off**. |
| **Sys_raid_status** | integer | Текущий статус RAID (Redundant Array of Independent Disks):<br>• **no_raid**.<br>• **0** — optimal — массив в оптимальном состоянии.<br>• **1** — degraded — полный или частичный выход из строя одного из дисков.<br>• **2** — rebuild — восстановление массива. |

**UTM-INTERFACES-MIB**

| Наименование | Тип данных | Описание |
|---|---|---|

| 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 физического/канального уровней:<br>• **1** — other — неизвестный тип.<br>• **2** — regular1822 — определён в BBN Report 1822.<br>• **3** — hdh1822 — определён в BBN Report 1822.<br>• **4** — ddn-x25 — определён в BBN Report 1822.<br>• **5** — rfc877-x25 — определён в стандарте канального уровня сетевой модели OSI X.25.<br>• **6** — ethernet-csmacd — сетевой интерфейс типа Ethernet, независимо от скорости (определён в RFC 3635).<br>• **7** — iso88023-csmacd — определён в IEEE 802.3.<br>• **8** — iso88024-tokenBus — определён в стандарте IEEE 8802.4.<br>• **9** — iso88025-tokenRing — сетевой интерфейс использует подключение Token Ring; определяется в стандарте IEEE 802.5.<br>• **10** — iso88026-man — определён в стандарте ISO 88026 "MAN".<br>• **11** — starLan — определён в стандарте IEEE 802.3e.<br>• **12** — proteon-10Mbit — Proteon 10 Mbit<br>• **13** — proteon-80Mbit — Proteon 80 Mbit.<br>• **14** — hyperchannel — высокоскоростной канал, используемы в сети ISDN.<br>• **15** — fddi — сетевой интерфейс использует подключение FDDI (Fiber Distributed Data Interface). FDDI — это набор стандартов передачи данных по оптоволоконным линиям в локальной сети.<br>• **16** — lapb — протокол канального уровня, используемым для передачи пакетов стандарта X.25.<br>• **17** — sdlc — протокол канального уровня для системной сетевой архитектуры IBM.<br>• **18** — ds1 — способен обрабатывать 24 одновременных соединения на общей скорости 1,544 Мбит/с; также называется T1.<br>• **19** — e1 — европейский аналог T1.<br>• **20** — basicISDN — для связи аппаратуры абонента и ISDN-станции.<br>• **21** — primaryISDN — используется для подключения к широкополосным магистралям, связывающим местные и центральные АТС или сетевые коммутаторы.<br>• **22** — propPointToPointSerial — определён в стандарте RFC1213.<br>• **23** — ppp — сетевой интерфейс использует подключение PPP (Point-To-Point Protocol).<br>• **24** — softwareLoopback — сетевой интерфейс является петлевым адаптером. Такие интерфейсы часто используются для тестирования; они не отправляют трафик в сеть.<br>• **25** — eon — ConnectionLess Network Protocol (CLNP) over Internet Protocol (IP); определён в ISO/IEC 8473-1.<br>• **26** — ethernet-3Mbit — сетевой интерфейс использует подключение Ethernet со скоростью 3 Мбит/с. Эта версия Ethernet определяется в стандарте IETF RFC 895.<br>• **27** — nsip — XNS over IP — предназначен для использования в разнообразных средах передачи данных.<br>• **28** — slip — сетевой интерфейс использует подключение SLIP (Serial Line Internet Protocol). SLIP определяется в стандарте IETF RFC 1055.<br>• **29** — ultra -ULTRA Technologies.<br>• **30** — ds3 — высокоскоростной интерфейс передачи данных, сформированный мультиплексированием сигналов DS1 и DS2; также называется T3.<br>• **31** — sip — сетевой интерфейс использует подключение SLIP (Serial Line Internet Protocol). SLIP определяется в стандарте IETF RFC 1055.<br>• **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:<br>• **1** — up — готов для передачи пакетов.<br>• **2** — down — не работает.<br>• **3** — testing — в режиме тестирования; рабочие пакеты не могут быть переданы. |
| **ifOperStatus** | integer | Текущий статус работы интерфейса:<br>• **1** — up — интерфейс готов для передачи пакетов.<br>• **2** — down — интерфейс не может передавать пакеты данных.<br>• **3** — testing — выполняется тестирование сетевого интерфейса; рабочие пакеты не могут быть переданы.<br>• **4** — unknown — интерфейс находится в неизвестном состоянии.<br>• **5** — dormant — сетевой интерфейс не может передавать пакеты данных, он ожидает внешнее событие.<br>• **6** — notPresente — сетевой интерфейс не может передавать пакеты данных из-за отсутствующего компонента, обычно аппаратного.<br>• **7** — lowerLayerDown — сетевой интерфейс не может передавать пакеты данных, потому что он работает поверх одного или нескольких других интерфейсов, и не менее одного из этих интерфейсов "нижнего уровня" не работает. |
| **ifLastChange** | timeticks | Значение SysUpTime, когда интерфейс оказался в данном состоянии. |
| **ifInOctets** | counter32 | Количество байтов, принятое данным интерфейсом, включая служебные. |

| Наименование | Тип данных | Описание |
|---|---|---|
| **ifInUcastPkts** | counter32 | Количество доставленных пакетов одноадресной рассылки. |
| **ifInNUcastPkts** | counter32 | Количество доставленных многоадресных и широковещательных пакетов. |
| **ifInDiscards** | counter32 | Количество входящих пакетов, которые были отброшены, даже если не было обнаружено ошибок, препятствующих их доставке. Одна из возможных причин отбрасывания: освобождение буферного пространства. |
| **ifInErrors** | counter32 | Количество входящих пакетов, которые содержат ошибки, препятствующие их доставке. |
| **ifInUnknownProtos** | counter32 | Количество пакетов, которые были получены через этот интерфейс и отброшены из-за использования неизвестного или неподдерживаемого протокола. |
| **ifOutOctets** | counter32 | Количество байтов, переданное данным интерфейсом, включая служебные. |
| **ifOutUcastPkts** | counter32 | Количество отправленных пакетов одноадресной рассылки, включая пакеты, которые были отброшены или не отправлены. |
| **ifOutNUcastPkts** | counter32 | Количество отправленных многоадресных и широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены. |
| **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 | Число пакетов в очереди на отправку. |
| **ifInMulticastPkts** | counter32 | Количество доставленных пакетов многоадресной рассылки. |
| **ifInBroadcastPkts** | counter32 | Количество доставленных широковещательных пакетов. |
| **ifOutMulticastPkts** | counter32 | Количество отправленных пакетов многоадресной рассылки, включая пакеты, которые были отброшены или не отправлены. |
| **ifOutBroadcastPkts** | counter32 | Количество отправленных широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены. |
| **ifHCInOctets** | counter64 | Смысл одинаков со смыслом объекта **ifInOctets** — количество байтов, принятое данным интерфейсом, включая служебные; используется счётчик большей ёмкости. |
| **ifHCInUcastPkts** | counter64 | Смысл одинаков со смыслом объекта **ifInUcastPkts** — количество доставленных пакетов одноадресной рассылки; используется счётчик большей ёмкости. |
| **ifHCInMulticastPkts** | counter64 | Смысл одинаков со смыслом объекта **ifInMulticastPkts** — количество доставленных пакетов многоадресной рассылки; используется счётчик большей ёмкости. |
| **ifHCInBroadcastPkts** | counter64 | Смысл одинаков со смыслом объекта **ifInBroadcastPkts** — количество доставленных широковещательных пакетов; используется счётчик большей ёмкости. |
| **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** — 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:<br>• **1** — enabled — включено.<br>• **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:<br>• **1** — true — станция принимает все пакеты/кадры независимо от того, кому они адресованы.<br>• **2** — false — интерфейс принимает только пакеты/кадры, адресованные этой станции.<br>Значение объекта не влияет на приём широковещательных и многоадресных пакетов/кадров. |
| **ifAlias** | string | Название интерфейса, заданное администратором. |
| **ifCounterDiscontinuityTime** | timeticks | Значение SysUpTime, когда произошло событие, ставшее причиной сбоя работы одного или более счётчиков интерфейса. |

**Журналы и отчёты**

**Журнал событий**

---

Documentation: ☑
Product: UGMC
Version: 7.0.1, 7.1.0

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

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

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

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

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

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

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

**Режим расширенного поиска**

---

Documentation: ☑
Product: UGMC
Version: 7.0.1, 7.1.0

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

Ключевые слова отделяются пробелами и могут быть следующими:

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

Операторы определяют условия фильтра и могут быть следующими:

| Наименование | Описание |
|---|---|
| **=** | Равно. Требует полного совпадения значения поля указанному значению, например, ip=172.16.31.1 будут отображены все записи журнала, в котором поле IP будет точно соответствовать значению 172.16.31.1. |
| **!=** | Не равно. Значение указанного поля не должно совпадать с указанным значением, например, ip!=172.16.31 будут отображены все записи журнала, в котором поле IP не будет равно значению 172.16.31.1. |
| **<=** | Меньше либо равно. Значение поля должно быть меньше либо равны указанному в запросе значению. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например,<br>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,<br>date >= "2019-03-13T21:00:00" AND statusCode=200. |
| **<** | Меньше. Значение поля должно быть меньше указанного в запросе значения. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например,<br>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,<br>(statusCode>200 AND statusCode<300) OR (statusCode=404). |
| **IN** | Позволяет указать несколько значений поля в запросе. Список значений необходимо указывать в круглых скобках, например,<br>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,<br>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,<br>browser ~ "Mozilla/5.0".<br>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,<br>browser !~ "Mozilla/5.0".<br>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,<br>details MATCH '\"module\":\"threats\"'.<br>Синтаксис запросов с использованием данного оператора соответствует стандарту RE2. Подробнее о синтаксисе Google/RE2: https://github.com/google/re2/wiki/Syntax. |
| **NOT MATCH** | При использовании оператора NOT MATCH подстрока, которая не должна присутствовать в указанном поле, задаётся в формате JSON и с использованием одинарных кавычек, например,<br>details NOT MATCH '\"module\":\"threats\"'.<br>Синтаксис запросов с использованием данного оператора соответствует стандарту RE2. Подробнее о синтаксисе Google/RE2: https://github.com/google/re2/wiki/Syntax. |

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

**Экспорт журналов**

Documentation: ☑
Product: UGMC
Version: 7.0.1, 7.1.0

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

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

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

**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:<br>• Журнал событий.<br>Для каждого из журналов возможно указать синтаксис выгрузки:<br>• CEF — Common Event Format (ArcSight).<br>• JSON — JSON format.<br>• @CEE: JSON — CEE Log Syntax (CLS) Encoding JSON.<br>Обратитесь к документации на используемую у вас систему SIEM для выбора необходимого формата выгрузки журналов.<br>Подробное описание форматов журналов читайте в Приложение 2. Описание форматов журналов. |
| **Тип сервера** | SSH (SFTP), FTP, Syslog. |
| **Адрес сервера** | IP-адрес или доменное имя сервера. |
| **Транспорт** | Только для типа серверов Syslog — TCP или UDP. |
| **Порт** | Порт сервера, на который следует отправлять данные. |
| **Протокол** | Только для типа серверов Syslog — RFC5424 или BSD syslog RFC 3164. Выберите протокол, совместимый с используемой у вас системой SIEM. |
| **Критичность** | Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас систему SIEM. Возможны следующие значения:<br>• **Тревога**: состояние, требующее незамедлительного вмешательства.<br>• **Критическая**: состояние, требующее незамедлительного вмешательства либо предупреждающее о сбое в системе.<br>• **Ошибки**: в системе возникли ошибки.<br>• **Предупреждения**: предупреждения о возможном возникновении ошибок, если не будут предприняты никакие действия.<br>• **Уведомительная**: события, которые относятся к необычному поведению системы, но не являются ошибками.<br>• **Информативная**: информационные сообщения. |
| **Facility** | Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас систему SIEM. Возможны следующие значения:<br>• **Сообщения пользовательские**.<br>• **Системный сервис**.<br>• **Безопасность/авторизация**.<br>• **Аудит**.<br>• **Тревога**.<br>• **Local 0**.<br>• **Local 1**.<br>• **Local 2**.<br>• **Local 3**.<br>• **Local 4**.<br>• **Local 5**.<br>• **Local 6**.<br>• **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.<br>В кластерной конфигурации UGMC при экспорте журналов с разных узлов кластера необходимо указывать разные каталоги на сервере для каждого узла UGMC, поскольку имена файлов журналов на каждом узле идентичны. |

| Наименование | Описание |
| --- | --- |
| **Расписание** | Выбор расписания для отправки логов. Не применяется к методу отправки Syslog. Возможны варианты:<br>• Ежедневно.<br>• Еженедельно.<br>• Ежемесячно<br>• Каждые ... часов.<br>• Каждые ... минут.<br>• Задать вручную.<br>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:<br>• Звездочка (*) — обозначает весь диапазон (от первого до последнего).<br>• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.<br>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".<br>• 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.<br>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.

**Управление областями**

**Создание управляемых областей**

---

Documentation: ☑
Version: 7.0.1, 7.1.0
Product: UGMC

Для создания управляемой области администратор UGMC должен выполнить следующие действия:

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

При создании области необходимо указать следующие поля:

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

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

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

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

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

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

**Администраторы области**

---

Version: 7.0.1, 7.1.0
Product: UGMC
Documentation: ☑

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

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

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

| Наименование | Описание |
|---|---|
| **Шаг 1.** Войти в веб-консоль управления под корневым администратором области. | Войти в консоль управления под корневым администратором, созданным для данной области, указав имя в виде *имя_администратора/код_области,* например, *Admin/UG.* |
| **Шаг 2.** Создать профиль доступа администратора области. | В консоли управления областью в разделе **Администраторы → Профили администраторов** нажать кнопку **Добавить** и указать необходимые настройки. |
| **Шаг 3.** Создать учетную запись администратора и назначить ей один из созданных ранее профилей администратора. | В разделе **Администраторы** нажать кнопку **Добавить** и выбрать необходимый вариант:<br>• **Добавить локального администратора** — создать локального пользователя, задать ему пароль доступа и назначить созданный ранее профиль доступа.<br>• **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.<br>• **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.<br>• **Добавить администратора с профилем аутентификации** — создать пользователя, назначить созданный ранее профиль администратора и профиль аутентификации (необходимы корректно настроенные серверы аутентификации). |

При создании профиля доступа администратора необходимо указать следующие параметры:

| Наименование | Описание |
|---|---|
| **Название** | Название профиля. |
| **Описание** | Описание профиля. |
| **Права доступа на область** | Укажите права доступа на разделы настроек области, такие как администраторы, серверы аутентификации, шаблоны устройств, группы шаблонов, управляемые устройства, журналы и отчеты.<br>В качестве доступа можно указать:<br>• Нет доступа.<br>• Чтение.<br>• Чтение и запись. |
| **Права доступа на шаблон** | Укажите здесь права на просмотр и/или изменение настроек всех или конкретных имеющихся шаблонов. Настройки представлены в виде объектов дерева веб-консоли МЭ UserGate, доступных для делегирования. В качестве доступа можно указать:<br>• Нет доступа.<br>• Чтение.<br>• Чтение и запись.<br>Например, можно разрешить сетевые настройки одной группе администраторов, а политики МЭ — другой. |

**Серверы аутентификации области**

Version: 7.0.1, 7.1.0
Product: UGMC
Documentation: ☑

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

## LDAP-коннектор

LDAP-коннектор позволяет:

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

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

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

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

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

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

## Сервер аутентификации RADIUS

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

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

| Наименование | Описание |
|---|---|
| **Включено** | Включение/отключение использования данного сервера аутентификации. |
| **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. |

| Наименование | Описание |
| --- | --- |
| **Использовать одно TCP-соединение** | Использовать одно TCP-соединение для работы с сервером TACACS+. |
| **Таймаут (сек)** | Время ожидания сервера TACACS+ для получения аутентификации. По умолчанию 4 секунды. |

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

**Профили аутентификации области**

---

Documentation: ☑
Version: 7.0.1, 7.1.0
Product: UGMC

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

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

**Каталоги пользователей**

---

Version: 7.0.1, 7.1.0
Product: UGMC
Documentation: ☑

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

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

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

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

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

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

**Управление областями (Описание)**

---

Version: 7.0.1, 7.1.0
Product: UGMC
Documentation: ☑

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

**Управление межсетевыми экранами UserGate (Описание)**

---

Documentation: ☑
Product: UGMC
Version: 7.0.1, 7.1.0

Централизованное управление МЭ UserGate можно разделить на 4 этапа:

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

## Шаблоны устройств

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

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

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

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

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

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

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

## Группы шаблонов

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

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

## Добавление устройств UserGate под управление UGMC

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

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

При создании объекта управляемого устройства необходимо указать следующие параметры:

| Наименование | Описание |
|---|---|
| **Включено** | Включает объект управляемого устройства. Если объект управляемого устройства включен, то он занимает одну лицензию. |
| **Название** | Название для управляемого устройства. Можно вводить произвольное название. |
| **Описание** | Описание управляемого устройства. |
| **Группа шаблонов** | Группа шаблонов, настройки которой следует применить к этому управляемому устройству. |

| Наименование | Описание |
|---|---|
| **Синхронизация** | Выбор режима синхронизации настроек группы шаблонов к устройству. Возможны 3 варианта:<br>• **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.<br>• **Отключено** — синхронизация выключена.<br>• **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.<br>Вне зависимости от выбранного режима доступен запуск синхронизации всех настроек для выбранных устройств (раздел **Управление NGFW → Устройства NGFW** кнопка **Действия → Запустить полную синхронизацию**). |

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

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

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

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

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

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

## Кластеризация МЭ UserGate с помощью UGMC

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

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

## Кластер конфигурации

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

Для создания кластера конфигурации необходимо выполнить следующие шаги:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Выполнить первоначальную настройку на первом узле кластера | Смотрите главу **Первоначальная настройка** документа **UserGate 6. Руководство администратора**. |

| Наименование | Описание |
|---|---|
| **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:<br>• Консоль администрирования<br>• Кластер<br>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 .<br>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.<br>Подключиться к веб-консоли второго узла кластера, выбрать язык установки.<br>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.<br>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.<br>После успешного добавления узла в кластер, данный узел будет отображаться в качестве второго узла в списке управляемых устройств с выбранным идентификатором. |

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

Добавление третьего и последующих узлов в кластер конфигурации выполняется аналогично.

## Кластер отказоустойчивости

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

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

Для создания кластера отказоустойчивости необходимо выполнить следующие шаги:

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

Параметры отказоустойчивого кластера:

| Наименование | Описание |
|---|---|
| **Вкл** | Включение/отключение отказоустойчивого кластера. |
| **Название** | Название отказоустойчивого кластера. |
| **Описание** | Описание отказоустойчивого кластера. |
| **Режим кластера** | Режим отказоустойчивого кластера:<br>• **Актив-Актив** — нагрузка распределяется на все узлы кластера<br>• **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. |

| Наименование | Описание |
|---|---|
| **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

UserGate Management Center 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 МЭ UserGate под управление UGMC, устройство UserGate автоматически начинает скачивать все обновления с сервера UGMC.

Для управления обновлениями с помощью UGMC необходимо выполнить следующие действия:

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

## Обновление ПО

Компания UserGate периодически выпускает обновления программного обеспечения МЭ UserGate. Эти обновления выкладываются в репозиторий UserGate ( http://static.usergate.com), откуда они уже доступны для скачивания МЭ. Если МЭ UserGate подключен к управлению через Management Center, то он проверяет наличие обновлений на сервере Management Center, который сам будет являться репозитарием. 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.<br>Для загрузки обновлений из репозитария необходимо в разделе **Управление 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.<br>Для загрузки вручную необходимо в разделе **Управление NGFW → Обновления ПО** нажать на кнопку **Импортировать обновление**, выбрать файл с обновлением. Если для файла обновлений в самом обновлении не указаны название и версия обновления, то необходимо указать их в соответствующих полях. Кнопка **Сохранить** загрузит выбранное обновление в UGMC. |
| **Шаг 2.** Утвердить обновление для всех или для конкретных устройств | Для установки обновления на все устройства необходимо выбрать интересующее обновление и нажать на кнопку **Утвердить обновление**. Только одно обновление может быть утверждено для всех устройств.<br>Если требуется установить данное обновление на группу устройств (например, для проведения тестирования), то необходимо в свойствах обновления указать управляемые устройства, для которых данное обновление будет доступно, и установить чекбокс **Утвердить обновление**. |
| **Шаг 3.** Провести установку обновления | После утверждения обновление становится доступным для скачивания для всех или группы управляемых устройств. УО скачивает обновление в соответствии с расписанием проверки обновлений. После скачивания обновление может быть установлено администратором в консоли МС или в ручном режиме администратором управляемого устройства. |

Обновление в 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 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. |

| Наименование | Описание |
|---|---|
| **Канал обновлений** | Канал обновлений репозитария UserGate:<br>• Стабильные — канал стабильных обновлений ПО.<br>• 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 (http://static.usergate.com), откуда они уже доступны для скачивания МЭ UserGate. Если МЭ UserGate подключен к управлению через Management Center, то он проверяет наличие обновлений на сервере Management Center, который сам будет являться репозитарием. Репозитарий UserGate при этом будет использован сервером UGMC для получения новых обновлений. По умолчанию UGMC проверяет и скачивает обновления библиотек автоматически.

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

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

Обновление библиотек в репозитарии UGMC имеет следующие свойства:

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

**Управление устройствами LogAn**

**Управление устройствами LogAn (Описание)**

Documentation: ☑
Product: UGMC
Version: 7.0.1, 7.1.0

Централизованное управление устройствами LogAn можно разделить на 4 этапа:

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

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

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

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

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

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

## Группы шаблонов LogAn

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

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

## Добавление устройств LogAn под управление UGMC

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

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

При создании объекта управляемого устройства LogAn необходимо указать следующие параметры:

| Наименование | Описание |
|---|---|
| **Включено** | Включает объект управляемого устройства . Если объект управляемого устройства включен, то он занимает одну лицензию. |
| **Название** | Название для управляемого устройства . Можно вводить произвольное название. |
| **Описание** | Описание управляемого устройства. |
| **Группа шаблонов** | Группа шаблонов, настройки которой следует применить к этому управляемому устройству . |

| Наименование | Описание |
|---|---|
| **Синхронизация** | Выбор режима синхронизации настроек группы шаблонов к устройству. Возможны 3 варианта:<br>• **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.<br>• **Отключено** — синхронизация выключена.<br>• **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.<br>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:<br>• 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.<br>• Имя локального администратора и его пароль.<br>• 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.<br>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.<br>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:<br>• Версия ПО управляемого устройства.<br>• ПИН-код управляемого устройства.<br>• Серийный номер ПАК.<br>• Время непрерывной работы.<br>• 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 |
|---|---|
| | |

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

## Обновление ПО LogAn

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

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

Порядок установки обновлений следующий:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Загрузить обновления в репозитарий UGMC. | Загрузить обновления можно либо из репозитария UserGate, либо импортировав файл обновления вручную.<br>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.<br>Для загрузки вручную необходимо в разделе **LogAn → Обновление ПО** нажать на кнопку **Импортировать обновление**, выбрать файл с обновлением. Если для файла обновлений в самом обновлении не указаны название и версия обновления, то необходимо указать их в соответствующих полях. Кнопка **Сохранить** загрузит выбранное обновление в UGMC. |
| **Шаг 2.** Утвердить обновление для всех или для конкретных устройств. | Для установки обновления на все устройства необходимо выбрать интересующее обновление и нажать на кнопку **Утвердить обновление**. Только одно обновление может быть утверждено для всех устройств.<br>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:<br>• **Стабильные** — канал стабильных обновлений ПО.<br>• **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 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 (https://static.usergate.com), откуда они уже доступны для скачивания LogAn. Если LogAn подключен к управлению через Management Center, то он проверяет наличие обновлений на сервере Management Center, который сам будет являться репозитарием. 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 |
|---|---|

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

**Управление конечными устройствами**

**Управление конечными устройствами UserGate Client (Описание)**

---

Documentation: ☑
Version: 7.0.1
Product: UGMC

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

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

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

Централизованное управление устройствами UGC можно разделить на следующие этапы:

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

Version: 7.0.1
Product: UGMC
Documentation: ☑

## Описание

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

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

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

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

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

На конечном устройстве доступна следующая информация:

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

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

## Рекомендации по установке ПО UserGate Client

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**Шаблоны управляемых устройств UGC**

Version: 7.0.1
Product: UGMC
Documentation: ☑

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

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

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

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

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

## Настройки

Определяют общие настройки параметров управляемых устройств UGC:

| Наименование | Описание |
|---|---|
| **Настройки инсталляции UserGate Client** | Настройки инсталляции ПО UserGate Client:<br>• **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.).<br>Значение по умолчанию: **Да**.<br>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.<br>**Важно!** Отключение сбора информации о конечном устройстве влияет на работу профилей HIP.<br>• **Разрешить сетевой доступ при остановленном приложении**: настройка сетевого доступа при остановленном ПО UserGate Client.<br>Значение по умолчанию: **Да**.<br>• **Разрешить отключение межсетевого экрана**: разрешение пользователю самостоятельно, используя графический интерфейс, отключать контентную фильтрацию на конечном устройстве:<br>◦ **Нет** — не разрешать самостоятельно отключать контентную фильтрацию.<br>◦ **Да** — разрешить самостоятельно отключать контентную фильтрацию.<br>◦ **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.<br>При разрешении пользователю отключать фильтрацию самостоятельно можно указать количество разрешённых отключений и/или время, на которое фильтрация будет отключена.<br>Значение по умолчанию: **Да** (отключение фильтрации на 10 минут без использования кода).<br>**Важно!** В случае использования счётчика количества отключений: если внести изменения в настройки разрешения отключения межсетевого экрана, то счётчик на конечном устройстве обнулится.<br>• **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.<br>Значение по умолчанию: **Да**.<br>**Важно!** Настройки не будут применены, если не включена синхронизация (флаг *Синхронизировать*). |
| **Оповещения** | Настройка оповещений:<br>• **Показывать иконку в трее**: отображение иконки UserGate Client в области уведомлений на панели задач.<br>• **Показывать тултипы оповещений**: включение/отключение отправки оповещений на конечное устройство.<br>Если оповещения отключены, то уведомления не будут отображаться на конечном устройстве вне зависимости от настроек отдельных уведомлений (о добавлении/удалении устройства из карантина, блокировке ресурса, соответствии/несоответствии HIP профилю).<br>• **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.<br>• **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.<br>• **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.<br>• **Сообщение о соответствии Hip профилю**: отправка уведомлений в случае соответствия конечного устройства профилю HIP. Уведомление будет отображено в виде всплывающего окна.<br>• **Сообщение о несоответствии HIP профилю**: отправка уведомлений в случае несоответствия конечного устройства профилю HIP. Уведомление будет отображено в виде всплывающего окна.<br>**Важно!** Настройки не будут применены, если не включена синхронизация (флаг *Синхронизировать*). |
| **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.<br>**Важно!** Настройки не будут применены, если не включена синхронизация (флаг *Синхронизировать*). |

## Настройка VPN

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

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

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

Для настройки VPN необходимо указать:

| Наименование | Описание |
|---|---|
| | |

| Наименование | Описание |
|---|---|
| **Включено** | Включение/отключение правила. |
| **Название** | Название профиля безопасности. |
| **Описание** | Описание профиля. |
| **VPN-адрес** | Имя хоста (FQDN) или IP-адрес VPN сервера.<br>**Важно!** При использовании FQDN в качестве адреса VPN-сервера, не предусматривается возможность перебора IP-адресов. В случае, если DNS-сервер вернет несколько адресов, будет выполнена попытка подключения к первому адресу в списке. |
| **Протокол** | VPN-протоколы для создания туннеля.<br>• **IPsec L2TP**. Для создания туннелей используется протокол Layer 2 Tunnelling Protocol (L2TP), а для защиты передаваемых данных — протокол IPsec. |
| **Режим IKE** | Режим IKE: **Основной** или **Агрессивный**.<br>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.<br>**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.<br>**Агрессивный режим**. В агрессивном режиме происходит 2 обмена, всего 3 сообщения. В первом сообщении инициатор передаёт информацию, соответствующую сообщениям 1 и 3 основного режима, т.е. информацию об алгоритмах шифрования и аутентификации и ключ DH. Второе сообщение предназначено для передачи получателем информации, соответствующей сообщениям 2 и 4 основного режима, а также аутентификации получателя. Третье сообщение аутентифицирует инициатора и подтверждает обмен. |
| **Аутентификация с пиром** | Общий ключ — аутентификация устройств с использованием общего ключа (Pre-shared key). |
| **Общий ключ** | Строка, которая должна совпадать на сервере и клиенте для успешного подключения. |
| **Вставить** | Место вставки создаваемого правила в списке правил — наверх, вниз или выше выбранного существующего правила. |
| **Фаза 1** | Во время первой фазы происходит согласование защиты IKE. Аутентификация происходит на основе общего ключа в режиме, выбранном ранее. Необходимо указать следующие параметры:<br>• **Время жизни ключа**. По истечению данного времени происходят повторные аутентификация и согласование настроек первой фазы.<br>• **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.<br>• **Алгоритмы аутентификации и шифрования**. Алгоритмы 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:<br>• **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.<br>• **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.<br>• **Алгоритмы аутентификации и шифрования**. Алгоритмы используются в порядке, котором они отображены. Для изменения порядка перетащите необходимую пару вверх/вниз или используйте кнопки **Выше**/**Ниже**. |

## 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 время.

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

**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 управляемом устройстве UGC разрешен.

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

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

| Наименование | Описание |
|---|---|
| **Действие** | Действие правила:<br>• **Запретить** — блокирует трафик.<br>• **Разрешить** — разрешает трафик.<br>• **Перенаправить в прокси** — перенаправляет трафик, соответствующий условиям правила в указанный прокси сервер. При выборе действия указание параметров **Списки URL, Категории, Типы контента** недоступно. |
| **Журналирование** | Определяет, записывать ли срабатывание данного правила в журнал на сервере LogAn. |
| **Прокси-сервер** | Выбор прокси-сервера, при указании действия **Перенаправить в прокси.** Прокси сервер указывается через выбор профиля прокси сервера. Более подробно об профилях прокси-серверов читайте в главе Профили прокси. |
| **Пользователи** | Указание пользователей или групп пользователей LDAP, для которых будет применено данное правило межсетевого экрана. Для указания пользователей необходим корректно настроенный LDAP-коннектор. Подробнее читайте в разделе Каталоги пользователей. |
| **Источник** | Списки IP-адресов источника трафика.<br>Список может быть создан предварительно в разделе **Библиотеки → IP-адреса** или при настройке правила. Более подробно об списках IP-адресов читайте в главе IP-адреса. |
| **Назначение** | Списки IP-адресов назначения трафика.<br>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.<br>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.<br>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.<br>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.<br>**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.<br>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.<br>**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.<br>Создание доступно в разделе **Библиотеки → Типы контента**, а также в свойствах правила межсетевого экрана. Более подробно о работе с MIME-типами читайте в главе Типы контента.<br>**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.<br>**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. |
| **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. |

| Наименование | Описание |
|---|---|
| **Шаг 3.** Добавить IP-адреса. | На панели **Адреса** из выбранной группы нажать на кнопку **Добавить** и ввести адреса.<br>IP-адреса вводятся в виде IP-адрес или IP-адрес/маска сети, например, 192.168.1.5 192.168.1.0/24. |

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

| Наименование | Описание |
|---|---|
| **Шаг 1.** Создать файл с необходимыми IP-адресами. | Создать файл **list.txt** со списком адресов. |
| **Шаг 2.** Создать архив, содержащий этот файл. | Поместить файл в архив zip с именем **list.zip**. |
| **Шаг 3.** Создать файл с версией списка. | Создать файл **version.txt**, внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка. |
| **Шаг 4.** Разместить файлы на веб-сервере. | Разместить у себя на сайте **list.zip** и **version.txt**, чтобы они были доступны для скачивания. |
| **Шаг 5.** Создать список IP-адресов и указать URL для обновления. | 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:<br>• Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет.<br>• Ежедневно.<br>• Еженедельно.<br>• Ежемесячно.<br>• Каждые ... часов.<br>• Каждые ... минут.<br>• Задать вручную.<br>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:<br>• Звездочка (*) — обозначает весь диапазон (от первого до последнего).<br>• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.<br>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".<br>Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа". |

### *Приложения*

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

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

Для добавления новой группы приложений необходимо выполнить следующие шаги:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Создать группу приложений. | В панели **Группы приложений** нажать на кнопку **Добавить**, дать название группе. |
| **Шаг 2.** Добавить приложения. | Выделить созданную группу и в панели **Приложения** нажать на кнопку **Добавить** и указать название и контрольную сумму приложения. Контрольная сумма исполняемого файла Windows должна быть определена по алгоритму SHA1, например, с помощью утилиты fciv. |

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

### *Списки URL*

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

Для фильтрации с помощью списков URL необходимо выполнить следующие действия:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Создать список URL. | В панели **Списки URL** нажать на кнопку **Добавить**, задать название нового списка. |
| **Шаг 2.** Добавить необходимые записи в новый список. | Добавить записи URL в новый список. В списках можно использовать специальные символы «^», «$» и «*»:<br>• «*» — любое количество любых символов.<br>• «^» — начало строки.<br>• «$» — конец строки.<br>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<br>или<br>*yahoo.com* | Блокируется весь домен и все URL этого домена и домены 3 уровня, например:<br>http://sport.yahoo.com<br>http://mail.yahoo.com<br>https://mail.yahoo.com<br>http://sport.yahoo.com/123 |
| ^mail.yahoo.com$ | Заблокированы только http://mail.yahoo.com<br>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<br>http://finance.yahoo.com/personal-finance/ |
| ^yahoo.com/12345/ | Заблокированы<br>http://yahoo.com/12345/whatever/<br>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:<br>*www.site1.com/url1*<br>*www.site2.com/url2*<br>*...*<br>*www.siteend.com/urlN* |
| **Шаг 2.** Создать архив, содержащий этот файл. | Поместить файл в архив zip с именем **list.zip**. |
| **Шаг 3.** Создать файл с версией списка. | Создать файл **version.txt**, внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка. |
| **Шаг 4.** Разместить файлы на веб-сервере. | Разместить у себя на сайте **list.zip** и **version.txt**, чтобы они были доступны для скачивания. |
| **Шаг 5.** Создать список типа контента и указать URL для обновления. | На каждом UserGate создать список URL. При создании указать тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. UserGate будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты:<br>• Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет.<br>• Ежедневно.<br>• Еженедельно.<br>• Ежемесячно.<br>• Каждые ... часов.<br>• Каждые ... минут.<br>• Задать вручную.<br>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:<br>• Звездочка (*) — обозначает весь диапазон (от первого до последнего).<br>• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.<br>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".<br>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.<br>Например, для блокировки документов типа *.doc необходимо добавить MIME-тип «application/msword». |
| **Шаг 3.** Создать правило фильтрации контента, содержащее один или несколько списков. | Смотрите раздел Политики сети. |

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

| Наименование | Описание |
|---|---|
| **Шаг 1.** Создать файл с необходимыми типами контента. | Создать файл **list.txt** со списком типов контента. |
| **Шаг 2.** Создать архив, содержащий этот файл. | Поместить файл в архив zip с именем **list.zip**. |
| **Шаг 3.** Создать файл с версией списка. | Создать файл **version.txt**, внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка. |
| **Шаг 4.** Разместить файлы на веб-сервере. | Разместить у себя на сайте **list.zip** и **version.txt**, чтобы они были доступны для скачивания. |
| **Шаг 5.** Создать список типа контента и указать URL для обновления. | На каждом UserGate создать список 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:<br>• Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет.<br>• Ежедневно.<br>• Еженедельно.<br>• Ежемесячно.<br>• Каждые ... часов.<br>• Каждые ... минут.<br>• Задать вручную.<br>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:<br>• Звездочка (*) — обозначает весь диапазон (от первого до последнего).<br>• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.<br>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".<br>Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа". |

### *Календари*

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

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

**Группы шаблонов управляемых устройств UGC**

---

Version: 7.0.1
Product: UGMC
Documentation: ☑

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

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

**Добавление управляемых устройств UGC под управление UGMC**

Version: 7.0.1
Product: UGMC
Documentation: ☑

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

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

## Процесс единичного добавления устройств

Для добавления одного управляемого устройства UGC необходимо выполнить следующие шаги:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Обеспечить доступ от управляемого устройства UGC до UGMC. | На сервере UGMC необходимо разрешить сервис **Контроль конечных устройств** на зоне, к интерфейсу которой подключаются управляемое устройство. Сервер UGMC слушает подключения от управляемых устройств UGC на портах TCP 4043 и 9712.<br>Передача данных между сервером UGMC и управляемым устройством осуществляется по зашифрованному каналу. |
| **Шаг 2.** Создать запись для управляемого устройства UGC в UGMC. | В консоли управления областью в разделе **Управление конечными устройствами → Конечные устройства** нажать кнопку **Добавить** и указать необходимые настройки. |
| **Шаг 3.** Отобразить уникальный код созданного устройства. | В консоли управления областью в разделе **Управление конечными устройствами → Конечные устройства** нажать кнопку **Показать уникальный код устройства** и зафиксировать его. Данный код потребуется указать при 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.<br>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** | Включает объект управляемого устройства UGC. Если объект управляемого устройства UGC включен, то он занимает одну лицензию. |
| **Название** | Название для управляемого устройства UGC. Можно вводить произвольное название. |
| **Описание** | Описание управляемого устройства UGC. |
| **Группы шаблонов** | Группа шаблонов, настройки которой следует применить к этому управляемому устройству UGC. Настройки (политики) применятся после синхронизации с UserGate Management Center. |
| **Синхронизация** | Режим синхронизации: отключено, автоматическая или ручная синхронизация. |

## Процесс массового добавления устройств

Рассмотрим процесс массового добавления управляемых устройств UGC:

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

**Управление устройством UGC из консоли UGMC**

---

Version: 7.0.1
Product: UGMC
Documentation: ☑

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

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

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

Данный раздел также позволяет просмотреть следующие параметры каждого конечного устройства:

| Наименование | Описание |
|---|---|
| **Название** | Отображено название конечного устройства. |
| **Версия** | Отображена версия UserGate Client, установленная на устройстве. |
| **Последнее подключение** | Показаны дата и время последнего подключения конечного устройства. |
| **Телеметрия** | Представлена следующая информация:<br>• IP-адрес конечного устройства, который используется для выхода в Интернет.<br>• Netbios имя.<br>• Время последнего подключения управляемого устройства UGC к UGMC.<br>• Пользователь, с учётной записи которого был совершён вход в систему.<br>• Имя компьютера в локальной сети.<br>• Версия ОС, установленная на конечном устройстве.<br>• Версия UserGate Client, установленная на устройстве.<br>• Загрузка CPU клиентом UserGate показывает на сколько загружен центральный процессор конечного устройства.<br>• Загрузка памяти клиентом UserGate - количество памяти, используемое UserGate Client.<br>• Загрузка физической памяти отображает загруженность оперативной памяти на конечном устройстве.<br>• Загрузка виртуальной памяти показывает степень загруженности виртуальной памяти на конечном устройстве. |
| **Мониторинг конечных устройств** | Показана подробная информация о конечном устройстве. Более подробно данный пункт будет рассмотрен ниже.<br>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 управляемому устройству UGC.<br>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.<br>О соответствии или несоответствии конечного устройства профилю HIP говорит цветовая индикация:<br>• Зелёный - конечное устройство соответствует профилю.<br>• Красный - конечное устройство не соответствует профилю.<br>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.<br>Подробнее читайте в разделе HIP профили. |
| **Устройства LogAn** | Название сервера LogAn, на который конечное устройство отправляет журналы диагностики и телеметрию. |
| **Время последней синхронизации** | Отображён режим, а также дата и время последней синхронизации конечного устройства и UGMC. Работа возможна в одном из следующих режимов:<br>• **Автоматическая синхронизация** — настройки применяются к устройству автоматически. При изменении любой настройки из любого шаблона, включенного в группу шаблонов, примененную к УУ, это изменение применяется без задержек.<br>• **Отключено** — синхронизация выключена.<br>• **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). |

| Наименование | Описание |
|---|---|
| **Производительность** | Представлена следующая информация:<br>• Использование процессора, т.е. степень загруженности центрального процессора.<br>• Степень загрузки центрального процессора конечного устройства процессом UserGate Client.<br>• Информация о виртуальной памяти конечного устройства.<br>• Информация о физической памяти - оперативной памяти.<br>• Загрузка памяти клиентом UserGate.<br>• Информация о дисках компьютера: размер диска, тип и производительность.<br>• Статус управляемого устройства UGC показывает статус UserGate Client: онлайн/офлайн (доступность конечного устройства) или отключено (UserGate Client был отключен с использованием UGMC кнопкой **Отключить**). |
| **Безопасность** | Представлена информация о безопасности конечного устройства: статус межсетевого экрана, антивируса, центров обновления и безопасности Windows, а также информация о шифровании дисков (BitLocker). |
| **USB устройства** | Отображена информация о подключённых устройствах USB:<br>• **Идентификатор** устройства: пара идентификаторов VID/PID (Vendor ID/Product ID) и номер версии устройства.<br>• **Название** устройства.<br>• **USB класс**, например mouse, printer.<br>• **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.<br>Нажатие кнопки **Завершить процесс** позволяет завершить процесс на конечном устройстве, используя UGMC. |
| **Службы** | Отображён список служб, запущенных/остановленных на конечном устройстве.<br>Нажатие кнопок **Остановить службу**/**Запустить службу** позволяет выполнить попытку отключения/ включения службы на управляемом устройстве UGC с использованием UGMC. |
| **Ключи реестра** | Просмотр реестра. Доступны:<br>• **HKEY_LOCAL_MACHINE**.<br>• **HKEY_USERS**.<br>Также доступен поиск по ключам реестра. Для этого необходимо нажать **Найти** (отображается при наведении указателя мыши на название каталога). |
| **Программное обеспечение** | Отображён список установленных на управляемом устройстве UGC ПО с указанием производителя и версии. |
| **Установленные обновления** | Представлен список установленных обновлений на управляемом устройстве UGC с отображением соответствующего номера базы знаний Microsoft, информации о продукте, производителе и дате установки обновления. |

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

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

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

**Сбор и анализ данных с устройств UGC**

Version: 7.0.1
Product: UGMC
Documentation: ☑

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

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

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

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

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

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

## Журнал событий конечных устройств

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

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

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

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

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

В журнале событий конечных устройств можно увидеть следующую информацию:

| Наименование | Описание |
|---|---|
| **Узел** | Идентификатор конечного устройства или узла, на котором запущен сенсор. |
| **Время** | Время события. Отображается в часовом поясе, настроенном на LogAn. |
| **Конечное устройство/сенсор** | Отображено имя компьютера. |
| **Уровень лога** | Отображен тип события:<br>• **Аудит успеха** (Audit Success): событие журнала безопасности, которое происходит при успешном обращении к аудируемым ресурсам;<br>• **Аудит отказа** (Audit Failure): событие журнала безопасности, которое происходит при неуспешном обращении к аудируемым ресурсам;<br>• **Ошибка** (Error): событие указывает на существенные проблемы, которые могут стать причиной потери функциональности или данных;<br>• **Сведения** (Information): информационные события, которые, как правило, не требуют внимания администратора;<br>• **Предупреждение** (Warning): события указывают на проблемы, которые не требуют немедленного исправления, однако могут привести к ошибкам в будущем. |
| **Данные** | Представлена подробная информация о событии. |
| **Источник журнала событий** | Показан источника журнала событий. |
| **Категория журнала** | Отображена категория лога, необходимая для упорядочивания событий. Данные берутся из Windows EventLog. Каждый источник может определять свои идентификаторы категорий. Относится к записям журнала событий конечных устройств. |
| **Категория инцидента** | Показана категория инцидента. |
| **Имя компьютера** | Показано полное имя компьютера. |
| **Имя пользователя** | Показано имя пользователя, с учётной записи которого был совершен вход в систему конечного устройства. |
| **Код события лога** | Представлен код, соответствующий определённому событию. |
| **Идентификатор события лога** | Отображён идентификатор события лога, который определяет первичный идентификатор события. |
| **Тип события лога** | Отображён тип события лога, соответствующий определённому уровню лога:<br>• 1 - уровень лога: ошибка (error);<br>• 2 - уровень лога: предупреждение (warning);<br>• 3 - уровень лога: сведения (information);<br>• 4 - уровень лога: аудит успеха (audit success);<br>• 5 - уровень лога: аудит отказа (audit failure). |
| **Строка вставки** | Содержит данные блока EventData события Windows. |

| Наименование | Описание |
|---|---|
| **Файл журнала лога** | Показано к какому типу файла журнала относится событие:<br>• **Application** (файл журнала приложений): для событий приложений и служб;<br>• **Security** (файл журнала безопасности): для событий системы аудита;<br>• **System** (файл системного журнала): для событий драйверов устройств;<br>• **CustomLog**: журнал содержит события, регистрируемые приложениями, которые создают пользовательский журнал. Использование пользовательского журнала позволяет приложению управлять размером журнала или присоединять списки управления доступом в целях безопасности, не затрагивая другие приложения. |

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

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

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

## Журнал правил конечных устройств

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

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

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

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

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

В журнале правил конечных устройств можно увидеть следующую информацию:

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

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

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

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

## Приложения конечных устройств

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

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

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

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

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

В журнале приложений конечных устройств отображается следующая информация:

| Наименование | Описание |
|---|---|
| **Узел** | Идентификатор конечного устройства. |
| **Время** | Время запуска приложения на конечном устройстве. Отображается в часовом поясе, настроенном на LogAn. |

| Наименование | Описание |
|---|---|
| **Конечное устройство** | Отображено имя компьютера. |
| **Действие** | Запуск или остановка приложения. |
| **Хэш** | Хэш приложения. |
| **Приложение** | Название приложения, которое было запущено или остановлено. |
| **Версия** | Версия приложения. |
| **Субъект подписи** | Владелец сертификата. |
| **Подписано** | Издатель сертификата для приложения. |
| **Идентификатор процесса** | Идентификатор процесса приложения (PID). |
| **Пользователь** | Пользователь, запустивший приложение. |
| **Командная строка** | Команда запуска приложения. |

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

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

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

## Аппаратура конечных устройств

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

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

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

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

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

Журнал аппаратуры конечных устройств содержит следующую информацию:

| Наименование | Описание |
|---|---|
| **Узел** | Идентификатор конечного устройства. |
| **Время** | Дата и время регистрации события. |
| **Конечное устройство** | Название конечного устройства. |
| **Действие** | Добавление или удаление устройства. |
| **Устройство** | Название устройства, которое было подключено или удалено. |
| **Идентификатор устройства** | Идентификатор подключенного/удалённого устройства. |
| **Служба** | Драйверы, использующиеся для работы с устройством. |

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

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

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

**HIP профили**

---

Product: UGMC
Version: 7.0.1
Documentation: ☑

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

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

При создании профиля необходимо указать:

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

**Объекты HIP**

---

Version: 7.0.1
Product: UGMC
Documentation: ☑

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

Для добавления объекта необходимо указать:

| Наименование | Описание |
|---|---|
| **Включено** | Включение/отключение использования объекта. |
| **Название** | Название объекта HIP. |
| **Описание** | Описание объекта HIP (опционально). |
| **Версия ОС** | Версия операционной системы устройства пользователя. |
| **Версия UserGate Client** | Версия ПО UserGate Client. |
| **Продукты** | Проверка на соответствие статуса:<br>• **Антивирус**. Проверка соответствия антивирусного ПО на устройстве пользователя.<br>◦ **Включено**: проверка статуса ПО;<br>◦ **Базы антивируса обновлены**: да, нет, не проверять;<br>◦ **Версия** ПО;<br>◦ **Вендор**: производитель и название продукта.<br>• **Межсетевой экран**. Проверка соответствия межсетевого экрана на конечном устройстве. При настройке необходимо указать:<br>◦ **Установлен**: проверка наличия установленного ПО;<br>◦ **Включено**: проверка статуса ПО (да, нет, не проверять);<br>◦ **Версия** ПО;<br>◦ **Вендор**: производитель и название продукта.<br>• **Резервное копирование**. Проверка ПО для резервного копирования:<br>◦ **Установлен**: проверка наличия установленного ПО;<br>◦ **Версия** ПО;<br>◦ **Вендор**: производитель и название продукта.<br>• **Шифрование диска**. Проверка соответствия статуса шифрования диска на конечном устройстве.<br>◦ **Установлен**: проверка наличия установленного ПО;<br>◦ **Версия** ПО;<br>◦ **Вендор**: производитель и название продукта.<br>• **DLP**. Проверка соответствия системы предотвращения утечек информации.<br>◦ **Установлен**: проверка наличия установленного ПО;<br>◦ **Версия** ПО;<br>◦ **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.<br>Поддерживаются следующие типы параметров реестра:<br>• **REG_SZ**: строка Unicode или ANSI с нулевым символом в конце;<br>• **REG_BINARY**: двоичные данные в любой форме;<br>• **REG_DWORD**: 32-разрядное число.<br>Доступно использование следующих ключей реестра:<br>• **HKEY_LOCAL_MACHINE** (аббревиатура: local_machine, hklm);<br>• **HKEY_USERS** (аббревиатура: users, hku).<br>**Важно!** При указании пути также доступно использование аббревиатуры корневого каталога реестр. Путь указывается с использованием обратного слэша ( \), например, \hklm.<br>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. |

**Приложения**

Documentation: ☑
Product: UGMC
Version: 7.0.1

## Формат журнала событий

### CEF

| Тип поля | Название поля | Описание | Пример значения |
|---|---|---|---|
| **CEF заголовок** | **CEF:Version** | Версия CEF | CEF:0 |
| | **Device Vendor** | Производитель продукта. | UserGate |
| | **Device Product** | Тип продукта. | NGFW |
| | **Device Version** | Версия продукта | 7 |
| | **Source** | Тип журнала. | events |
| | **Origin** | Модуль, в котором произошло событие | admin_console |
| | **Severity** | Важность события | Может принимать значения:<br>• 0 — информационные;<br>• 6 — предупреждения;<br>• 8 — ошибки;<br>• 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@einersonstal |
| | **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** | Время получения события в формате: yyyy-mm-ddThh:mm:ssZ | 2022-05-12T08:11:46.15869Z |
| **ip_address** | IPv4-адрес источника события | 192.168.174.134 |
| **node** | Имя, которое однозначно идентифицирует устройство, генерирующее это событие | mc_core@einersonstal |
| **attributes** | Детали события в формате JSON | {"rule":{"logrotate":12,"attributes":{"timezone":"Asia/Novosibirsk"},"id":"66f9de9f-d698-4bec-b3b0-ba65b46d3608","name":"Example log export ftp"} |
| **event_type** | Тип события | logexport_rule_updated |
| **event_severity** | Важность события | info (информационные), warning (предупреждения), error (ошибки), critical (критичные). |
| **event_origin** | Модуль, в котором произошло событие | core |
| **event_component** | Компонент, в котором произошло событие | console_auth |

**Требования к сетевому окружению**

Documentation: ☑
Product: UGMC
Version: 7.0.1

| Сервис | Протокол | Порт | Исходящий/Входящий | Функция |
|---|---|---|---|---|
| **Веб-консоль** | TCP | 8010 | Входящий (до веб-консоли UserGate Management Center) | Доступ к веб-интерфейсу управления устройством |
| | TCP | 8300 | Входящий (до веб-консоли UserGate NGFW, подключённого к UGMC) | Доступ к веб-интерфейсу управления UG NGFW, подключённого к UGMC |
| **CLI по SSH** | TCP | 2200 | Входящий (к CLI по SSH) | Доступ к интерфейсу командной строки (CLI) UserGate по протоколу SSH |
| **XML-RPC** | TCP | 4041 | Входящий (к UserGate по API) | Управление устройством UserGate по API |
| **Удалённый помощник** | TCP | 22 | Исходящий (до серверов технической поддержки) | Удалённый доступ к серверу технической поддержки<br>Доступ к серверам:<br>• 93.91.171.46;<br>• 178.154.221.222;<br>• ra.entensys.com. |
| **NTP** | UDP | 123 | Исходящий (до сервера точного времени) | Синхронизация времени |
| **DNS** | UDP | 53 | Исходящий (от UserGate до DNS-сервера) | Сервис получения информации (IP-адрес) о доменах |
| **Регистрация сервера UserGate** | TCP | 443 | Исходящий (до сервера регистрации) | Доступ до сервера регистрации продуктов UserGate reg2.usergate.com |
| **Обновление ПО и библиотек** | TCP | 443 | Исходящий (до серверов обновления) | Обновление программного обеспечения и элементов библиотек: доступ до сервера updates.usergate.com |
| **Репликация настроек** | TCP | 4369 | Входящий (с первого узла кластера на второй и последующие узлы) | Сервис, необходимый для работы кластера конфигурации;<br>Установка управляющего соединения. |
| | | 9000-9100 | Входящий (приём конфигурации от первого узла кластера) | Передача информации об изменении конфигурации кластера (реплика настроек) |
| **Сервис UserGate Management Center** | TCP | 9712 | Входящий (к UGMC от NGFW) | Первоначальная установка связи и обмен ключами шифрования управляемых устройств и сервера UserGate Management Center |
| | | 2022 | Входящий (к UGMC от NGFW) | Построение SSH-туннеля для обмена данными с помощью полученных ключей |
| **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 установке связи |
| | | 22000-22711 | Входящий (к UGMC от UG Client) | Передача журналов и телеметрии с UG Client на UG LogAn транзитом через UGMC |
| **LDAP** | TCP | 389, 636 | Исходящий (на LDAP-коннектор) | Выполнение запросов LDAP (389 - для LDAP и 636 - для LDAP over SSL) |
| **SNMP** | UDP | 161 | Входящий (до UserGate) | Доступ к серверу UserGate по протоколу SNMP |
| **SMTP** | TCP | 25 | Исходящий (до почтового сервера) | Отправка уведомлений на электронную почту |
| **DHCP** | UDP | 67, 68 | Исходящий (запрос на получение адреса от UserGate на сервер DHCP) | Сервис службы DHCP |
| **FTP (экспорт журналов)** (начиная с версии 7.1.0) | TCP | 21 | Исходящий (до сервера FTP) | Экспорт журналов на сервер FTP |
| **SSH (экспорт журналов)** (начиная с версии 7.1.0) | TCP | 22 | Исходящий (до сервера SSH) | Экспорт журналов на сервер SSH |
| **Syslog (экспорт журналов)** (начиная с версии 7.1.0) | TCP/UDP | 514 | Исходящий (до сервера Syslog) | Экспорт журналов на сервер Syslog |
| **Ручная проверка сайтов по категориям** | TCP | 80/443 | Исходящий (до updates.usergate.com) | Ручная проверка сайтов по категориям |

**Введение**

**Описание**

---

Version: 6.1.9, 7.0.1, 7.1.0

Product: UGMC

Documentation: ☑

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.

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

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

## Управление областями UGMC

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

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

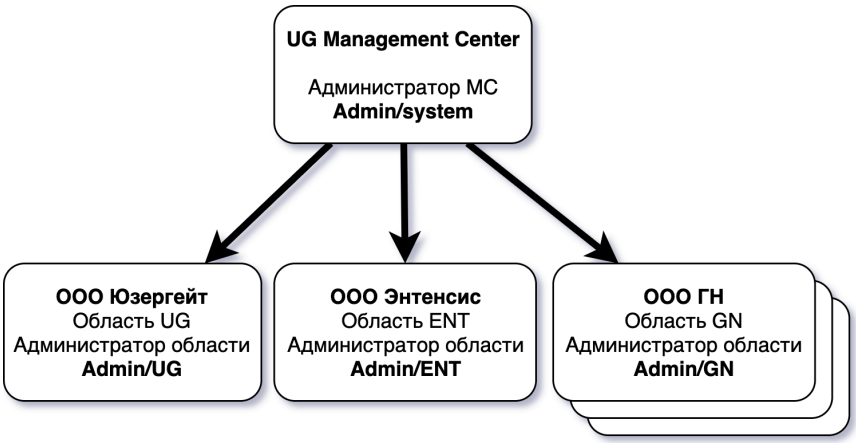
| Администратор | Профиль администратора | Уровень доступа |
|---|---|---|
| AdminTemplates/realm_code | Templates | Создание и модификация всех шаблонов области. |
| AdminTemplateGeneral/realm_code | TemplateGeneral | Только модификация шаблона General. |
| AdminTemplateGeneralNET/realm_code | TemplateGeneralNET | Только модификация сетевых настроек в шаблоне General. |

**Управляемые области**

Version: 7.x
Product: UGMC
Documentation: ☑

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. Подробнее о разграничении прав администраторов — в разделе «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.

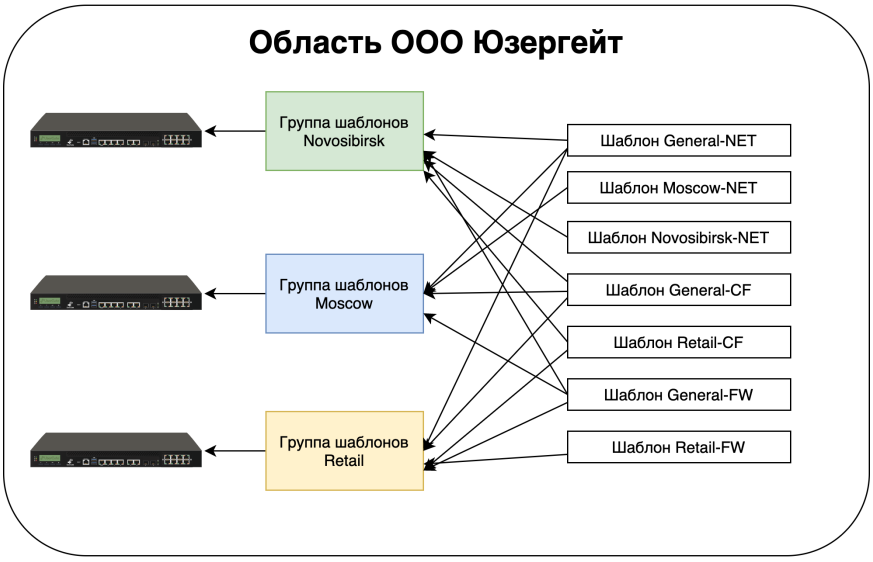
**Шаблоны и группы шаблонов**

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

С помощью шаблонов и групп шаблонов администратор области настраивает находящиеся в ней устройства. Шаблон — это базовый блок, с помощью которого настраиваются все параметры работы управляемых устройств, например, межсетевого экрана — сетевые параметры, 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:



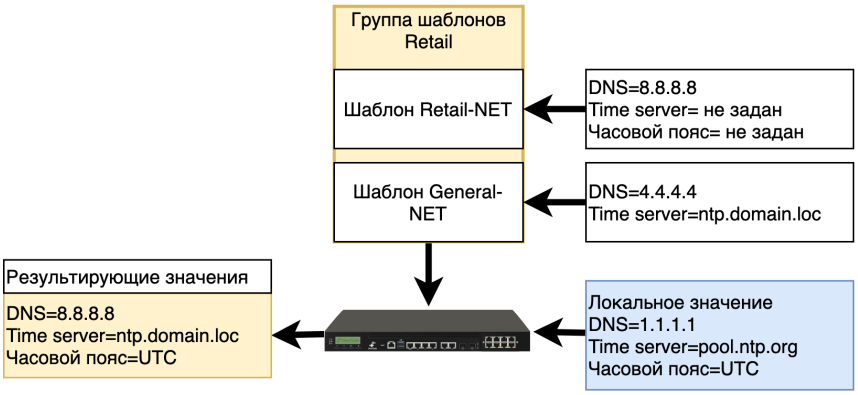

Конфигурация, передаваемая на устройство, может быть двух типов:

- 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.

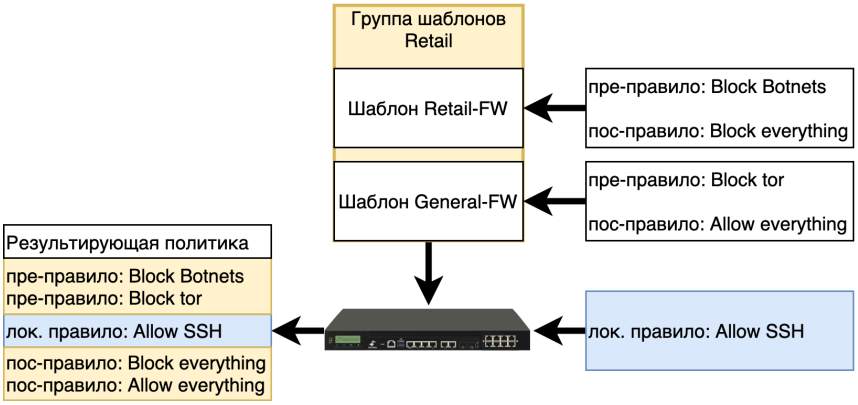
Настройка параметра при конфликтующих значениях в разных шаблонах одной группы шаблонов принимает значение, заданное в наиболее верхнем шаблоне. Локально указанные настройки данного параметра игнорируются.

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:



**Совместимость версий UserGate MC с версиями продуктов UserGate**

Documentation: ☑
Version: 7.x
Product: UGMC

В таблице представлена матрица совместимости версий UserGate MC с версиями ПО UserGate.

| UserGate MC | UserGate NGFW | UserGate DCFW | UserGate Logan | UserGate SIEM | UserGate WAF | UserGate SWG | UserGate Client |
|---|---|---|---|---|---|---|---|
| 7.1.0 | 6.1.9<br>7.0.1<br>7.1.0 | — | 7.0.1<br>7.1.0<br>7.1.1<br>7.1.2 | — | — | — | — |
| 7.1.1 | 6.1.9<br>7.0.1<br>7.1.0<br>7.1.1 | — | 7.0.1<br>7.1.0<br>7.1.1<br>7.1.2 | — | — | — | — |
| 7.1.2 | 6.1.9<br>7.0.1<br>7.1.0<br>7.1.1 | — | 7.0.1<br>7.1.0<br>7.1.1<br>7.1.2 | — | — | — | — |
| 7.3.0<br>7.3.1<br>7.3.2<br>7.3.3 | 6.1.9<br>7.0.1<br>7.1.x<br>7.2.x<br>7.3.x | — | 7.0.1<br>7.1.x<br>7.2.x<br>7.3.x | — | — | — | — |
| 7.4.0<br>7.4.1<br>7.4.2<br>7.4.3 | 6.1.9<br>7.0.1<br>7.1.x<br>7.2.x<br>7.3.x<br>7.4.x | 8.0.0 | 7.0.x<br>7.1.x<br>7.2.x<br>7.3.x<br>7.4.x | 7.4.x | — | — | — |
| 7.5.0 | 6.1.9<br>7.0.1<br>7.1.x<br>7.2.x<br>7.3.x<br>7.4.x<br>7.5.0 | 8.0.0 | 7.0.x<br>7.1.x<br>7.2.x<br>7.3.x<br>7.4.x<br>7.5.x | 7.4.x<br>7.5.x | — | — | — |
| 7.5.1 | 6.1.9<br>7.0.1<br>7.1.x<br>7.2.x<br>7.3.x<br>7.4.x<br>7.5.0<br><br>7.5.1 | 8.0.0 | 7.0.x<br>7.1.x<br>7.2.x<br>7.3.x<br>7.4.x<br>7.5.x | 7.4.x<br>7.5.x | — | — | 7.5.0 |
| 7.6.0 | 6.1.9<br>7.0.1<br>7.1.x<br>7.2.x<br>7.3.x<br>7.4.x<br>7.5.0<br><br>7.5.1 | 8.1.0 | 7.0.x<br>7.1.x<br>7.2.x<br>7.3.x<br>7.4.x<br>7.5.x | 7.4.x<br>7.5.x | 7.6.0<br>(поддержка добавления продукта и базовой телеметрии, без настройки шаблонов) | — | 7.5.0<br>7.5.1 |

## Поддержка в UserGate MC 7.1.0 конфигурации ранних версии ПО UserGate

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

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

**Совместимость версий UserGate MC с аппаратными платформами**

---

Version: 7.x
Product: UGMC

UserGate MC версии 7.6.0 совместим со следующим моделями аппаратных платформ:

- C151;
- D200;
- D250;
- D500;
- E1000;
- E1010;
- E3000;
- E3010

**Важно!**Перед обновлением обязательно сверьтесь со списком совместимости для вашего устройства.

**Лицензирование**

Documentation: ☑
Product: UGMC
Version: 7.x

## Базовая лицензия

UGMC лицензируется по типам и 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.

Базовая лицензия на продукт является бессрочной (обновления ПО и библиотек не включены).

## Дополнительно лицензируемые модули

Дополнительно лицензируются следующие модули.

| Модуль | Описание |
|---|---|
| **Security Updates (SU)** | Модуль SU дает право на получение обновлений:<br>• ПО UGMC;<br>• сигнатур системы обнаружения вторжений;<br>• сигнатур приложений L7;<br>• библиотек соответствия требованиям безопасности (комплаенса).<br>Модуль поставляется на один год, по истечении этого срока для получения обновлений необходимо продление лицензии |
| **Сенсоры** | Модуль определяет тип и количество устройств, которыми управляет UGMC.<br>Модуль выписывается сроком на один год и требует ежегодного платного продления |
| **Cluster** | Модуль включает лицензию на работу устройств UserGate в режиме «кластер». Срок действия лицензии не ограничен |
| **UserGate Client** | Модуль предназначен для взаимодействия с конечными устройствами с установленным ПО UserGate Client, являющимся одним из компонентов экосистемы UserGate SUMMA.<br>Лицензия на модуль включает в себя:<br>• централизованное управление конечными устройствами и их доступом в сеть за исключением контроля доступа в соответствии с требованиям безопасности (комплаенса);<br>• сбор телеметрии и событий безопасности конечных устройств.<br>Выписывается по количеству лицензируемых конечных управляемых устройств наборами по 10, 100, 1000 и 10000 шт. Срок действия лицензии не ограничен |
| **NAC** | Дополнительный модуль к модулю лицензирования UserGate Client.<br>Лицензия на модуль включает в себя:<br>• проверку конечных устройств на соответствие требованиям безопасности (комплаенса);<br>• контроль доступа в сеть на уровне конечного устройства по результатам проверки.<br>Поставляется на срок от 1 года до 5 лет и выписывается по количеству лицензируемых конечных управляемых устройств наборами по 10, 100, 1000 и 10000 шт.<br>По истечении срока действия лицензии контроль доступа по результатам проверки комплаенса становится недоступным. Правила межсетевого экрана, использующие профиль HIP в качестве одного из условий, перестают работать.<br>Для продолжения работы сервисов необходимо продление лицензии |

## Процедуры активации лицензий

## Онлайн-активация

При онлайн-активации устройство UserGate обращается к серверу лицензирования https://reg2.usergate.com. На сервер передается следующая техническая информация: номер версии ПО UserGate, ПИН-код, название продукта, модель устройства и т. д. В ответ приходят данные о сроке действия лицензии и список модулей, разрешенных данной лицензией.

Если модули, ранее числившиеся в системе, отсутствуют в этом списке, они деактивируются, а их лицензия аннулируется. Вновь появившиеся модули активируются.

В процессе эксплуатации устройства UserGate лицензионная проверка выполняется один раз в сутки. При подтверждении лицензии устройство продолжает работу в нормальном режиме. Успешная проверка фиксируется в журнале событий соответствующим событием.

Если серверы лицензирования недоступны, делается 14 попыток подключения с интервалом в 120 секунд. В случае неуспеха попытки прекращаются на сутки, после чего снова следуют 14 попыток подключения к серверу активации. В случае если в период действия лицензии не удается подключиться к серверу активации, лицензия блокируется в связи с истечением срока действия (модули, лицензия которых просрочена, перестают работать). При каждой ошибке подключения к серверу активации в журналы заносится сообщение об ошибке.

## Порядок действий при онлайн-активации

Для регистрации устройства:

1. В веб-консоли администратора устройства перейдите в раздел **Дашборды**,

2. В виджете **Лицензия** нажмите **Нет лицензии**, введите ПИН-код и зарегистрируйте устройство.

Если узел находится в закрытом контуре без прямого доступа в интернет активировать или обновить лицензию можно через прокси-сервер. Для этого выберите режим **Использовать прокси-сервер для активации и апдейтов**. Далее укажите IP-адрес и порт вышестоящего прокси-сервера. При необходимости укажите логин и пароль для аутентификации на прокси-сервере.

## Офлайн-активация

Офлайн-активация лицензий необходима для устройств UserGate, находящихся в изолированной сети без доступа к интернету и без возможности активации через прокси-сервер.

Процесс офлайн-лицензирования включает следующие этапы:

1. Генерация запроса — создание на лицензируемом устройстве файла запроса для офлайн-активации.

2. Активация запроса — обработка сгенерированного файла запроса с помощью сервиса офлайн-активации ПИН-кодов.

3. Применение лицензии — загрузка активированного файла обратно на лицензируемое устройство.

## Генерация запроса

Чтобы сгенерировать файл запроса для офлайн-активации лицензии:

1. Зайдите с помощью веб-браузера на лицензируемое устройство по следующему адресу: https://<IP-address>:8010?features=offline-reg .

IP-address — это IP-адрес лицензируемого устройства.

2. В веб-консоли устройства перейдите в раздел **Дашборды**.

3. В виджете **Лицензия** нажмите **Нет лицензии**.

4. В окне активации устройства нажмите **Начать активацию в автономном режиме**.

5. Введите ПИН-код устройства и скачайте сгенерированный файл запроса для офлайн-активации.

### Активация запроса

С компьютера, имеющего доступ в интернет, обратитесь в сервис офлайн-активации (для входа в сервис потребуется авторизация в Едином центре авторизации) и активируйте сгенерированный файл запроса.

### Применение лицензии

Загрузите активированный файл на лицензируемое устройство. Для этого:

1. В разделе **Дашборды** лицензируемого устройства в виджете **Лицензия** откройте окно офлайн-активации.

2. Выберите **Завершить активацию в автономном режиме**.

3. Укажите активированный файл, полученный в сервисе офлайн-активации.

Процесс лицензирования завершен.

Подробнее о процедуре офлайн-активации лицензии — в разделе «Офлайн-активация лицензий».

**Планирование внедрения UGMC**

**Планирование внедрения UGMC (Описание)**

Documentation: ☑
Product: UGMC
Version: 7.x

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:

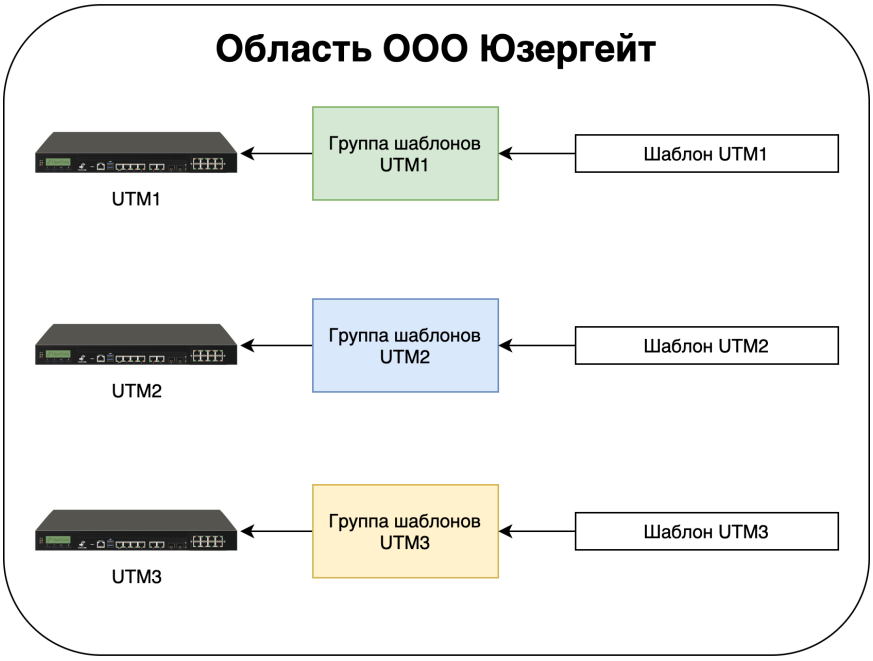
- Избегать конфликта настроек при добавлении шаблонов в группы шаблонов. Наличие конфликтов всегда усложняет управление конечными устройствами. Это основополагающий принцип, из которого вытекают следующие рекомендации.
- Разделять различные группы настроек в разные шаблоны, например, общие настройки 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.

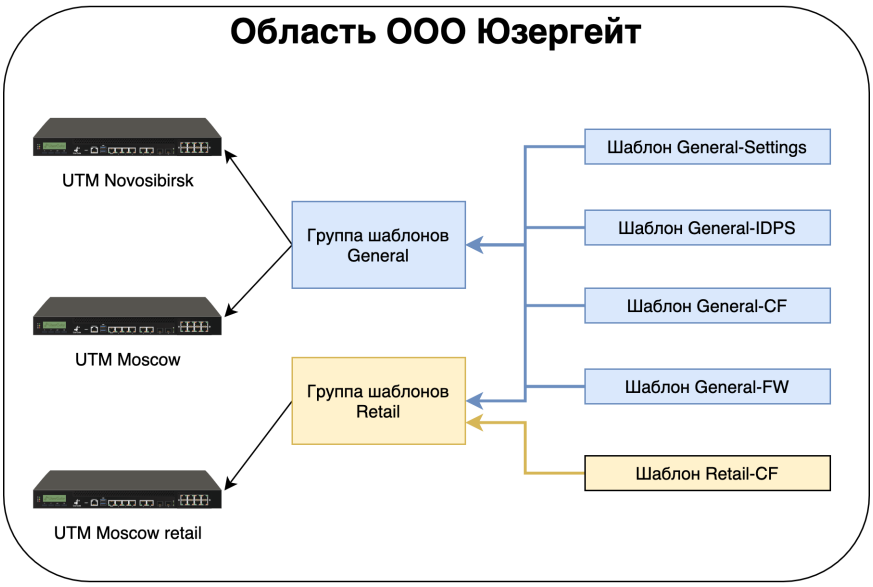
Рекомендуется для простых внедрений с небольшим количеством МЭ UserGate. Пример такой настройки представлен на рисунке ниже.




## 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 централизованно 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.



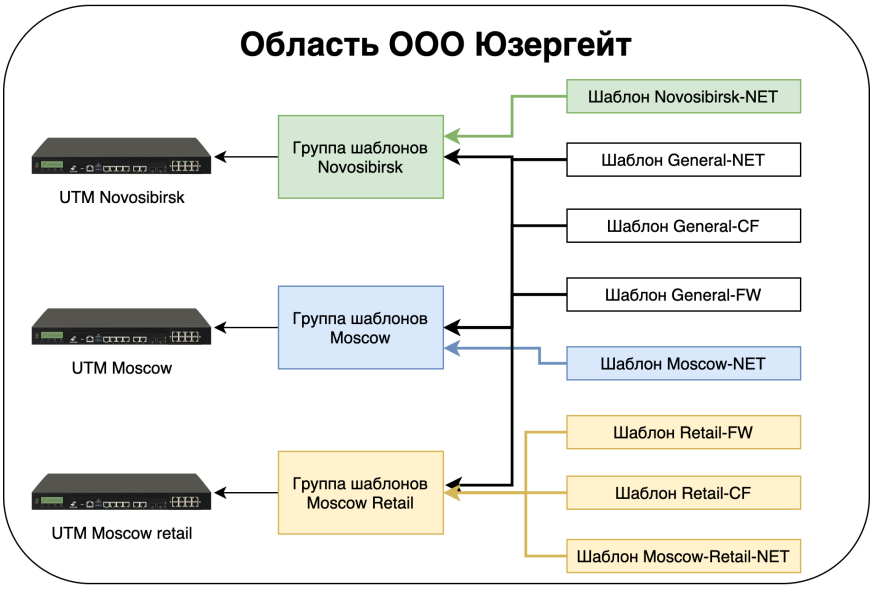

В данном примере шаблоны содержат следующие настройки:

- 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**

Documentation: ☑
Product: UGMC
Version: 7.x

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.
**Примечание**Для корректной работы внутренней базы данных требуется поддержка набора микрокоманд SSE4.2 архитектуры x86 процессорами виртуальной среды. Любой процессор на базе архитектуры x86, выпущенный после 2008 года, должен поддерживать SSE4.2.

Для начала работы с виртуальным образом, выполните следующие шаги:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Скачайте образ и распакуйте. | Скачайте последнюю версию виртуального образа с официального сайта https://www.usergate.com/ru. |
| **Шаг 2.** Импортируйте образ в свою систему виртуализации. | Инструкцию по импорту образа вы можете посмотреть на сайтах VirtualBox и VMWare. Для Microsoft Hyper-v и KVM необходимо создать виртуальную машину и указать в качестве диска скачанный образ, **после чего отключить службы интеграции** в настройках созданной виртуальной машины. |
| **Шаг 3.** Настройте параметры виртуальной машины. | Увеличьте размер оперативной памяти виртуальной машины. Используя свойства виртуальной машины, установите минимум 8Gb. |
| **Шаг 4. Важно!** Увеличьте размер диска виртуальной машины. | Размер диска по умолчанию составляет 100Gb, что обычно недостаточно для хранения всех журналов и настроек. Используя свойства виртуальной машины, установите размер диска в 300Gb или более. Рекомендованный размер - 500Gb или более. |
| **Шаг 5.** Настройте виртуальные сети. | UserGate Management Center поставляется с четырьмя интерфейсами, два из которых назначены в зоны:<br>• **Management** - первый интерфейс виртуальной машины.<br>• **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**<br>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.<br>**Статический IP-адрес**<br>Включить UGMC. Используя CLI (Command Line Interface), назначить необходимый IP-адрес на интерфейс port0. Детали использования CLI смотрите в главе Интерфейс командной строки (CLI).<br>Подключиться к веб-консоли UGMC по указанному адресу, он должен выглядеть примерно следующим образом:<br>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 интерфейсами читайте в главе Настройка интерфейсов. Система поставляется с предопределенными зонами:<br>• Зона **Management** (сеть управления), интерфейс port0.<br>• Зона **Trusted** (LAN). Предполагается, что через эту зону UGMC будет подключаться к управляемым устройствам, а также получит доступ в интернет.<br>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. |

| Наименование | Описание |
| --- | --- |
| **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.<br>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.

**Интерфейс**

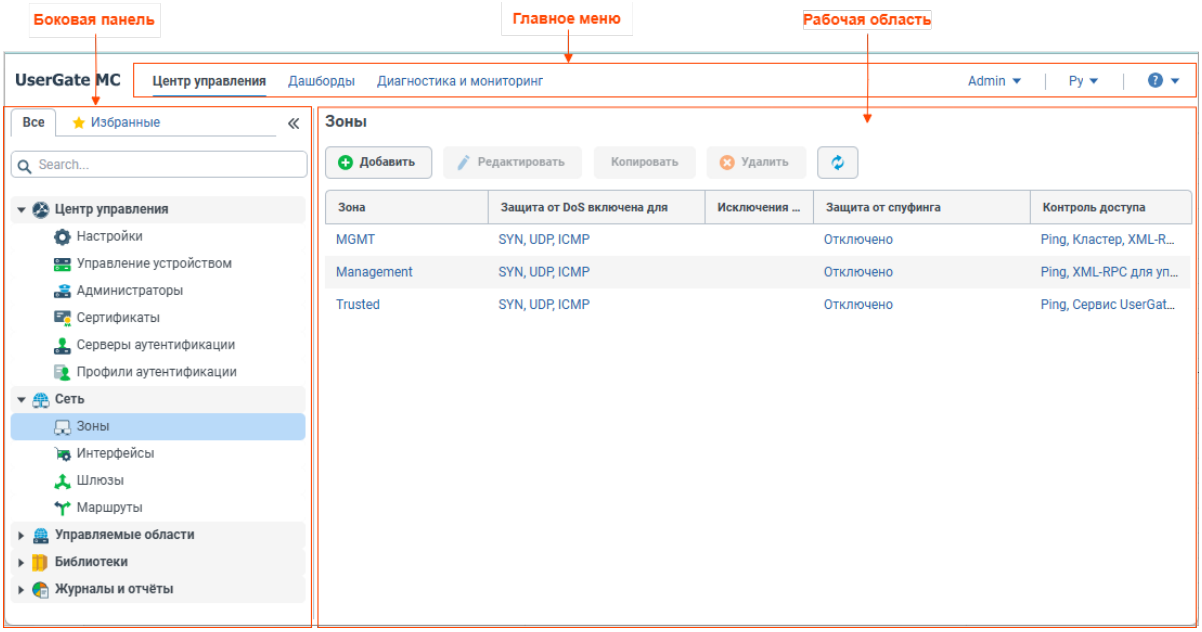
**Веб-консоль UserGate MC**

Product: UserGate MC
Version: 7.x

Все действия вы можете выполнять в веб-интерфейсе, доступном после входа в UGMC.

Состав разделов в веб-интерфейсе меняется в зависимости от роли администратора. Администратору системы доступен весь набор элементов и функций, связанных с управлением устройством. Администратору области доступны все возможности UGMC в рамках назначенной ему области. На рисунке ниже представлен веб-интерфейс администратора системы.

На рисунке ниже представлена веб-консоль администратора системы.




## Главное меню

В верхней части любой страницы расположено главное меню, которое содержит разделы для перехода к страницам веб-консоли.

Главное меню веб-консоли администратора системы предоставляет доступ к следующим страницам:

- **Центр управления** — страница для настройки общесистемных и сетевых параметров (см. разделы « Настройка UserGate MC» и «Настройка сети» соответственно).

  Также на этой странице можно добавлять и настраивать области.

- **Дашборды** — страница со статистическими данными о состоянии устройства и результатах его работы, представленными в виде таблиц, списков и графиков.
- **Диагностика и мониторинг** — страница для просмотра маршрутов, запуска базовых сетевых утилит, управления SNMP-мониторингом устройства, а также для настройки оповещений о важных событиях (см. раздел «Диагностика и мониторинг»).

Главное меню веб-консоли администратора области предоставляет доступ к следующим страницам:

- **Управление областью** — страница для создания шаблонов параметров управляемых устройств и групп шаблонов, а также для подключения соответствующих управляемых устройств и управления другими администраторами области.
- **NGFW**, **DCFW**, **Конечные устройства**, **LogAn** и **SIEM** — страницы для настройки параметров соответствующих управляемых устройств UserGate.

  Подробнее о настройке — в разделах «Управление устройствами UserGate NGFW», «Управление устройствами UserGate DCFW», «Управление конечными устройствами», «Управление устройствами UserGate Log Analyzer», «Управление устройствами UserGate SIEM» соответственно.

Также в главном меню находятся следующие элементы управления:

- Логин вашей учетной записи — раскрывает меню для настройки учетной записи администратора.

  В этом меню вы можете сменить пароль учетной записи, выбрать тему оформления веб-консоли, настроить число отображаемых записей на страницах с табличными данными, а также указать время ожидания ответа от сервера UserGate MC при выполнении операций. Кроме того, вы можете завершить работу с текущей учетной записью, нажав в этом меню **Выход**.

  В веб-консоли администратора области в меню также отображается имя узла устройства и информация об области (ее код и название), к которой принадлежит учетная запись.

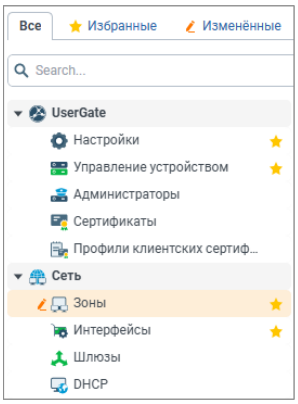
- Язык — выбор языка веб-консоли.
- Значок вопроса — раскрывает меню, в котором можно выбрать просмотр документации или обучающего видео, а также перейти на портал технической поддержки https://www.usergate.com/ru/support, где вы можете получить дополнительную информацию по настройке UserGate MC или оставить заявку на решение возникшей проблемы.

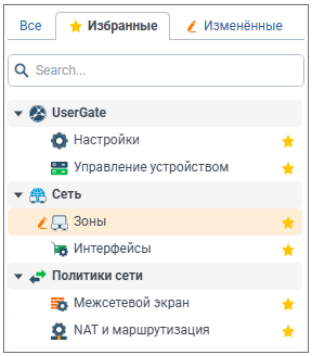
## Страницы веб-консоли

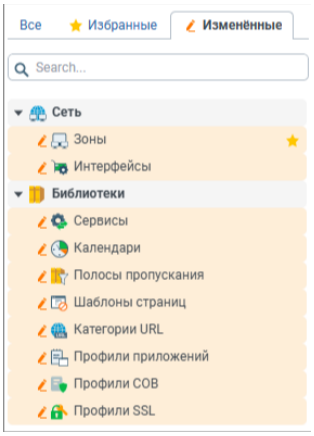
Все страницы, кроме страницы **Дашборды**, состоят из рабочей области и боковой панели. Содержимое и вид рабочей области зависят от выбранной страницы, информация может отображаться в виде таблицы, виджетов или блоков параметров. Боковая панель содержит список разделов, предоставляющих доступ к различным возможностям UserGate MC, например к настройке конфигурации, созданию политики безопасности, просмотру журналов и диагностической информации.

Вкладка **Избранные** на боковой панели предназначена для формирования списка разделов, с которыми вы работаете чаще всего. Чтобы раздел отобразился в избранном, на вкладке **Все** его нужно отметить звездочкой.

На страницах для настройки параметров управляемых устройств UserGate на боковой панели также есть вкладка **Измененные**, на которой собраны только те разделы, в которых производились изменения.


Все
Избранные
Изменённые
Search...
UserGate
Настройки
Управление устройством
Администраторы
Сертификаты
Профили клиентских сертиф...
Сеть
Зоны
Интерфейсы
Шлюзы
DHCP


Все
Избранные
Изменённые
Search...
UserGate
Настройки
Управление устройством
Сеть
Зоны
Интерфейсы
Политики сети
Межсетевой экран
NAT и маршрутизация


Все
Избранные
Изменённые
Search...
Сеть
Зоны
Интерфейсы
Библиотеки
Сервисы
Календари
Полосы пропускания
Шаблоны страниц
Категории URL
Профили приложений
Профили СОВ
Профили SSL

**Офлайн операции с сервером**

**Офлайн операции с сервером(Описание)**

---

Documentation: ☑
Product: UGMC
Version: 7.x

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

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

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

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

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

**Настройка UGMC**

**Настройка общих параметров**

---

Version: 7.x
Product: UGMC
Documentation: ☑

В этом разделе описаны общие параметры UserGate Management Center (UGMC), которые отображаются на странице веб-интерфейса **Центр управления** в разделе **Консоль администратора → Настройки**, а также приведены рекомендации по настройке этих параметров.

| Блок параметров | Параметр | Описание |
|---|---|---|
| **Настройки интерфейса** | **Часовой пояс** | Часовой пояс, соответствующий вашему местоположению. Используется для работы расписаний, настроенных в правилах, а также для корректного отображения даты и времени, например в отчетах или в журналах |
| | **Язык интерфейса по умолчанию** | Язык, используемый в веб-интерфейсе продукта по умолчанию |
| | **Таймер автоматического закрытия сессии (мин.)** | Для настройки таймера необходимо указать, по истечении скольких минут бездействия администратора в веб-интерфейсе должна завершаться его сессия.<br>Также необходимо включить параметр **Автоматическое закрытие сессии по таймеру** |
| | **Автоматическое закрытие сессии по таймеру** (параметр доступен начиная с версии 7.5.0) | При включенном параметре сессия администратора будет завершаться по истечении таймера автоматического закрытия сессии.<br>По умолчанию параметр отключен |
| **Настройка времени сервера** | **Использовать NTP** | При включенном параметре для синхронизации времени в продукте будут использоваться серверы NTP из указанного списка |
| | **Основной NTP-сервер** | Адрес основного сервера точного времени. Значение по умолчанию — pool.ntp.org |
| | **Запасной NTP-сервер** | Адрес запасного сервера точного времени |
| | **Время на сервере (UTC)** | Время на сервере UGMC в часовом поясе UTC |
| **Обновления ПО** (в версиях 7.1.x, 7.2.x, 7.3.x доступен общий блок параметров с обновлениями — **Центр обновлений**) | **Канал обновлений** | Настройка канала для получения обновлений программного обеспечения UserGate (UGOS) из репозитория UserGate.<br>Вы можете выбрать **Стабильные** (стабильные версии ПО) или **Бета** (версии ПО для бета-тестирования) |
| | **Обновления** | Проверка наличия обновлений UGOS в репозитории UserGate.<br>После проверки вы можете вручную загрузить и установить доступные обновления.<br>В процессе установки обновления UGOS вы можете создать точку восстановления продукта. Это позволит восстановить предыдущую версию UGOS при возникновении проблем. Действие будет доступно в стартовом меню продукта после установки обновления UGOS |
| | **Офлайн-обновление** | Загрузка файла обновления UGOS офлайн |
| **Обновления библиотек** (в версиях 7.1.x, 7.2.x, 7.3.x доступен общий блок параметров с обновлениями — **Центр обновлений**) | **Обновления** | Проверка наличия обновлений системных библиотек, предоставляемых по подписке, в репозитории UserGate.<br>После проверки вы можете вручную обновить необходимые библиотеки |
| | **Расписание автоматических обновлений** | Настройка расписания автоматического обновления библиотек.<br>При настройке расписания вы можете выбрать одно из предустановленных значений или указать время вручную в cron-формате: <минуты: 0-59> <часы: 0-23> <дни месяца: 1-31> <месяцы: 1-12> <дни недели: 0-6, где 0 — воскресенье>.<br>Для ручного ввода вы можете использовать следующие символы:<br>• Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что резервное копирование должно выполняться каждый час.<br>• Дефис (-) — для указания диапазона значений.<br>• Запятая (,) — в качестве разделителя значений.<br>• Косая черта (/) — для указания шага между значениями.<br>При установке флажка **Единое расписание для всех обновлений** расписание выбранной библиотеки будет применено ко всем библиотекам в списке |
| **Учет изменений** | **Настройка учета изменений** | Для настройки учета изменений в веб-интерфейсе продукта необходимо включить параметр и добавить типы изменений (например, распоряжение, приказ или регламентные работы).<br>Учет изменений предполагает, что при внесении какого-либо изменения через веб-интерфейс администратору необходимо указать тип и причину этого изменения |
| **Системные DNS-серверы** | | Для настройки DNS-серверов необходимо указать их IP-адреса |

**Управление устройством**

---

Documentation: ☑
Version: 7.x
Product: UGMC

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<br>Настройки интерфейсов<br>Настройки шлюзов<br>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:<br>• Консоль администрирования.<br>• Кластер.<br>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 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).<br>Подключиться к веб-консоли второго узла кластера, выбрать язык установки.<br>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.<br>Указать IP-адрес первого узла, настроенный на шаге 3, вставить секретный код и нажать на кнопку **Подключить**. Если IP-адреса кластера, настроенные на шаге 2, назначены корректно, то второй узел будет добавлен в кластер, и все настройки первого узла кластера реплицируются на второй. |
| **Шаг 6.** Назначить зоны интерфейсам второго узла. | В веб-консоли второго узла кластера в разделе **Сеть → Интерфейсы** необходимо назначить каждому интерфейсу корректную зону. Зоны и их настройки получены в результате репликации данных с первого узла кластера. |
| **Шаг 7.** Настроить параметры, индивидуальные для каждого узла кластера (опционально). | Настроить шлюзы, маршруты и другие настройки, индивидуальные для каждого из узлов. |

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

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

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

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

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

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

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

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

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

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

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

Для создания отказоустойчивого кластера необходимо выполнить следующие шаги:

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

Параметры отказоустойчивого кластера:

| Наименование | Описание |
|---|---|
| **Включено** | Включение/отключение отказоустойчивого кластера. |
| **Название** | Название отказоустойчивого кластера. |
| **Описание** | Описание отказоустойчивого кластера. |
| **Режим кластера** | Режим отказоустойчивого кластера:<br>• **Актив-Актив** — нагрузка распределяется на все узлы кластера.<br>• **Актив-Пассив** — нагрузка идет на Мастер-узел и переключается на запасной узел в случае недоступности Мастер-узла. |

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

## Диагностика

Этот блок предназначен для настройки параметров диагностики и предоставления удаленного доступа службе технической поддержки UserGate с целью анализа и устранения неисправностей.

## Параметры диагностики

С помощью параметра **Детализация диагностики** вы можете установить уровень журналирования устройства. Доступны следующие уровни:

- **Off** — ведение журналов диагностики отключено.
- **Error** — журналировать только ошибки в работе устройства.
- **Warning** — журналировать только ошибки и предупреждения.
- **Info** — журналировать только ошибки, предупреждения и дополнительную информацию.
- **Debug** — журналировать все возможные события.

При журналировании с уровнями **Warning**, **Info** и **Debug** может снижаться производительность устройства, поэтому рекомендуется устанавливать уровни **Error** или **Off**, если технической поддержкой UserGate не было предложено иное.

## Управление журналами

Вы можете скачать диагностические журналы для их передачи в службу технической поддержки UserGate. Для скачивания доступны журналы веб-консоли и системные журналы. Скачать выбранные журналы можно после их архивирования командой **Начать архивирование журналов**.

Чтобы удалить архивные (не активные в настоящий момент) журналы, нажмите **Очистить файлы логов**.

## Удаленный помощник

Чтобы предоставить доступ к устройству для службы технической поддержки UserGate с целью диагностирования и устранения неисправностей, необходимо активировать функцию удаленного помощника и получить параметры сеансового доступа.

Процесс подключения к устройству происходит следующим образом:

1. Администратор устройства UserGate активирует функцию удаленного помощника.

2. Устройство устанавливает защищенное соединение с сервером удаленного помощника UserGate по протоколу SSH. При успешном подключении в интерфейсе устройства UserGate отобразятся параметры сеансового доступа: идентификатор и токен.

3. Администратор устройства UserGate передает параметры сеансового доступа специалисту технической поддержки UserGate.

4. Специалист технической поддержки устанавливает защищенное соединение по протоколу SSH с сервером удаленного помощника UserGate и с помощью параметров сеансового доступа подключается к устройству UserGate.

## Операции с сервером

Данный раздел позволяет произвести следующие операции с сервером:

| Наименование | Описание |
|---|---|
| **Операции с сервером** | • **Перезагрузить** — перезагрузка сервера UGMC.<br>• **Выключить** — выключение сервера UGMC. |
| **Обновления** | Выбор канала обновлений ПО UGMC<br>• **Стабильные** — проверка наличия стабильных обновлений ПО.<br>• **Бета** — проверка наличия экспериментальных обновлений. |
| **Обновления сервера** | Индикация имеющихся обновлений UGMC.<br>Запуск процесса обновления сервера с возможностью создания точки восстановления.<br>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.<br>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. |

| Наименование | Описание |
|---|---|
| **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:<br>backup_PRODUCT_NODE-NAME_DATE.gpg, где<br>*PRODUCT* — тип продукта: NGFW, LogAn, MC;<br>*NODE-NAME* — имя узла UserGate;<br>*DATE* — дата и время создания резервной копии в формате YYYY-MM-DD-HH-MM; время указывается в часовом поясе UTC.<br>Процесс создания резервной копии может быть прерван нажатием кнопки **Остановить**. Запись о создании резервной копии отобразится в журнале событий устройства. |

Для восстановления состояния устройства необходимо выполнить следующие действия:

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

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

| Наименование | Описание |
|---|---|
| **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:<br>• **Тип сервера** — FTP или SSH.<br>• **Адрес сервера** — IP-адрес сервера.<br>• **Порт** — порт сервера.<br>• **Логин** — учетная запись на удаленном сервере.<br>• **Пароль**/**Повторите пароль** — пароль учетной записи.<br>• **Путь на сервере** — путь на сервере, куда будут выгружены настройки.<br>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**.<br>**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**.<br>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.<br>**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:<br>(минуты:0-59) (часы:0-23) (дни месяца:1-31) (месяц:1-12) (день недели:0-6, 0-воскресенье)<br>Каждое из первых пяти полей может быть задано следующим образом:<br>• Звездочка (*) — обозначает весь диапазон (от первого до последнего).<br>• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.<br>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".<br>• 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:<br>• текущие настройки сервера под именем: cc_core-mc_core @nodename_version_YYYYMMDD_HHMMSS.bin<br>• сетевые настройки под именем: network-cc_core-mc_core@nodename_version_YYYYMMDD_HHMMSS.bin<br>nodename — имя узла UserGate Management Center.<br>version — версия UserGate Management Center.<br>YYYYMMDD_HHMMSS — дата и время выгрузки настроек в часовом поясе UTC.<br>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 Обновление ПО кластера UGMC .

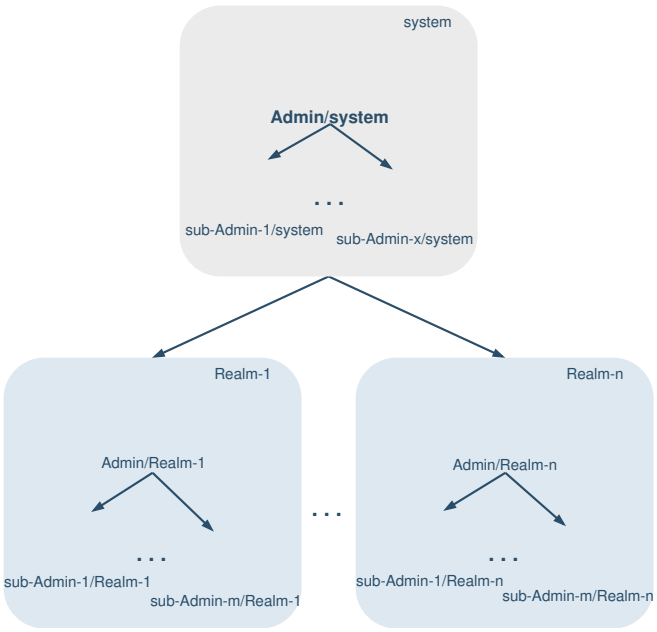
Дополнительно администратор может настроить сохранение настроек на внешние серверы (FTP, SSH) по расписанию. Для создания расписания выгрузки настроек необходимо выполнить следующие действия:

| 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:<br>• **Тип сервера** — FTP или SSH.<br>• **Адрес сервера** — IP-адрес сервера.<br>• **Порт** — порт сервера.<br>• **Логин** — учетная запись на удаленном сервере.<br>• **Пароль**/**Подтверждение пароля** — пароль учетной записи.<br>• **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:<br>(минуты:0-59) (часы:0-23) (дни месяца:1-31) (месяц:1-12) (день недели:0-6, 0-воскресенье)<br>Каждое из первых пяти полей может быть задано следующим образом:<br>• Звездочка (*) — обозначает весь диапазон (от первого до последнего).<br>• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.<br>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".<br>• 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". |

Version: 7.x
Product: UGMC

## Иерархическая система учетных записей администраторов

В 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 (Realm) — логических объектов, предназначенных для управления группой подконтрольных устройств (подробнее об управляемых областях — 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 параметрами 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 субадминистраторов UGMC, делегируя им часть прав по управлению системой.

Администратор UGMC также создает управляемые области (Realm), но при этом не обладает полномочиями на управление устройствами, входящими в эти области. Для этого администратор UGMC создает учетные записи корневых администраторов управляемых областей (Admin/Realm). Корневой администратор области имеет все права на управление областью и относящимися к ней устройствами. Он может создавать серверы и профили аутентификации области, каталоги пользователей, шаблоны параметров управляемых устройств, объединять шаблоны в группы и подключать к ним объекты управляемых устройств. Корневой администратор управляемой области может также создавать учетные записи субадминистраторов (региональных администраторов) своей области (sub-Admin/Realm), делегируя им права на администрирование только отдельных выделенных устройств.

## Управление учетными записями администраторов

Чтобы добавить администратора:

1. Создайте профиль администратора. Профиль определяет список полномочий администратора. Можно создавать несколько профилей с разными полномочиями. Также можно создать профиль корневого администратора области.
2. Создайте учетную запись администратора. На этом этапе можно выбрать способ авторизации администратора: локальный, через LDAP-коннектор или с помощью профиля аутентификации.

## Создание профиля администратора

Чтобы создать профиль администратора UGMC:

1. В веб-консоли управления UGMC в разделе **Центр управления → Администраторы** в блоке **Профили администраторов** нажмите **Добавить**.
2. В окне **Настройка профиля** на вкладке **Общие** укажите название профиля.
3. Выберите тип администратора **Администратор UserGate Management Center**.
4. На вкладке **Права доступа** выберите, какими правами доступа будет обладать администратор с этим профилем. В качестве разрешений для доступа можно указать **Нет доступа**, **Чтение** или **Чтение и запись**.
5. Сохраните изменения.

Чтобы создать профиль корневого администратора области:

1. Убедитесь, что в системе создана нужная область. Подробнее об областях — в разделе « Создание управляемых областей».
2. В веб-консоли управления UGMC в разделе **Центр управления → Администраторы** в блоке **Профиль администраторов** нажмите **Добавить**.
2. В окне **Настройка профиля** на вкладке **Общие** укажите название профиля.
3. Выберите тип администратора **Администратор области** и ранее настроенную управляемую область.
4. Сохраните изменения.

Корневые администраторы областей обладают всеми правами в рамках своей области. В режиме управления областью они могут создавать учетные записи субадминистраторов области и управлять их правами доступа.

## Создание учетной записи локального администратора

Чтобы создать учетную запись локального администратора:

1. В веб-консоли управления UGMC в разделе **Центр управления → Администраторы** в блоке **Администраторы** нажмите **Добавить** и выберите **Добавить локального администратора**.
2. В окне **Свойства администратора** укажите имя, логин и пароль администратора.
3. Выберите созданный ранее профиль администратора.
4. Установите флажок **Включено**, чтобы разрешить вход в систему под этой учетной записью.
5. Сохраните изменения.

**Важно!**Для корневого администратора области можно создать только учетную запись локального администратора. Это связано с тем, что LDAP-серверы, используемые для аутентификации администраторов сервиса UGMC и для аутентификации администраторов области, могут быть разными. Если для управления областью требуется использовать LDAP-администраторов, их необходимо создать в веб-интерфейсе самой области. Более подробно об администраторах области — в разделе «Администраторы области».

## Создание учетной записи LDAP-администратора

Чтобы создать учетную запись пользователя из существующего домена:

1. Убедитесь, что в разделе **Серверы аутентификации** предварительно настроен соответствующий LDAP-коннектор. Подробнее о настройке LDAP-коннектора — в разделе « Серверы аутентификации».
2. В веб-консоли управления UGMC в разделе **Центр управления → Администраторы** в блоке **Администраторы** нажмите **Добавить** и выберите **Добавить пользователя LDAP**.
3. В окне **Свойства LDAP-администратора** нажмите кнопку **Выбрать**, выберите настроенный LDAP-коннектор и затем добавьте логин нужного пользователя.
4. Выберите созданный ранее профиль администратора.
5. Установите флажок **Включено**, чтобы разрешить вход в систему под этой учетной записью.
6. Сохраните изменения.

При входе в веб-интерфейс администрирования под этой учетной записью необходимо указывать логин в формате <логин>@<домен>/system или <домен>\<логин>/system.

Чтобы добавить учетную запись для группы пользователей из существующего домена:

1. Убедитесь, что в разделе **Серверы аутентификации** предварительно настроен соответствующий LDAP-коннектор. Подробнее о настройке LDAP-коннектора — в разделе « Серверы аутентификации».
2. В веб-консоли управления UGMC в разделе **Центр управления → Администраторы** в блоке **Администраторы** нажмите **Добавить** и выберите **Добавить группу LDAP**.
3. В окне **Свойства LDAP-администратора** нажмите кнопку **Выбрать**, выберите настроенный LDAP-коннектор и затем добавьте логин группы пользователей.
4. Выберите созданный ранее профиль администратора.
5. Установите флажок **Включено**, чтобы разрешить вход в систему под этой учетной записью.
6. Сохраните изменения.

При входе в веб-интерфейс администрирования под этой учетной записью необходимо указывать логин в формате <логин>@<домен>/system или <домен>\<логин>/system.

## Создание учетной записи администратора с профилем аутентификации

Вы можете управлять доступом администраторов в веб-консоль управления UGMC с помощью профиля аутентификации, в котором в списке доступных методов аутентификации указаны заранее настроенные серверы, такие как LDAP, TACACS+ или RADIUS. Если в профиле аутентификации указано сразу несколько методов аутентификации, будут перебираться все методы по очереди до первого сработавшего.

Чтобы добавить учетную запись администратора с профилем аутентификации:

1. Убедитесь, что в разделе **Серверы аутентификации** добавлены данные о настроенном сервере аутентификации. Подробнее о сервере аутентификации — в разделе « Серверы аутентификации».
2. Убедитесь, что в разделе **Профили аутентификации** создан профиль с нужным методом аутентификации. Подробнее о создании профиля— в разделе « Профили аутентификации».
3. В веб-консоли управления UGMC в разделе **Центр управления → Администраторы** в блоке **Администраторы** нажмите **Добавить** и выберите **Добавить администратора с профилем аутентификации**.
4. В окне **Свойства администратора с профилем аутентификации** укажите имя, логин и пароль администратора.
5. Выберите созданный ранее профиль администратора.
6. Выберите созданный ранее профиль аутентификации.
7. Установите флажок **Включено**, чтобы разрешить вход в систему под этой учетной записью.
8. Сохраните изменения.

## Дополнительные параметры защиты учетных записей администраторов

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

**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.

Чтобы настроить дополнительные параметры защиты:

1. В разделе **Центр управления → Администраторы** в блоке **Администраторы** нажмите **Настроить**.
2. Настройте нужные параметры:
   - **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.
3. Сохраните изменения.

## Сессии администраторов

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

**Сертификаты**

---

Version: 7.x
Product: UGMC
Documentation: ☑

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

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

| Наименование | Описание |
|---|---|
| **Шаг 1.** Создать сертификат. | Нажать на кнопку **Создать** в разделе **Сертификаты** |
| **Шаг 2.** Заполнить необходимые поля. | Указать значения следующих полей:<br>• **Название** — название сертификата, под которым он будет отображен в списке сертификатов.<br>• **Описание** — описание сертификата.<br>• **Страна** — страна, в которой выписывается сертификат.<br>• **Область или штат** — область или штат, в котором выписывается сертификат<br>• **Город** — город, в котором выписывается сертификат.<br>• **Название организации** — название организации, для которой выписывается сертификат.<br>• **Common name** — имя сертификата. Рекомендуется использовать только символы латинского алфавита для совместимости с большинством браузеров.<br>• **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:<br>• **Экспорт сертификата** — экспортирует данные сертификата в der-формате без экспортирования приватного ключа сертификата.<br>• **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:<br>• Название — название сертификата, под которым он будет отображен в списке сертификатов.<br>• Описание — описание сертификата.<br>• Загрузите файл, содержащий данные сертификата.<br>• Загрузите файл, содержащий приватный ключ сертификата.<br>• Пароль для приватного ключа, если таковой требуется.<br>• Цепочка сертификатов — файл, содержащий сертификаты вышестоящих центров сертификации, которые участвовали в создании сертификата. Необязательное поле. |

**Серверы аутентификации**

---

Version: 7.x
Product: UGMC
Documentation: ☑

Серверы аутентификации — это внешние источники учетных записей пользователей, которые можно использовать 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.
- Выполнять авторизацию администраторов UGMC через домены Active Directory и FreeIPA.

Чтобы добавить LDAP-коннектор:

1. На странице **Центр управления** в разделе **Центр управления → Серверы аутентификации** нажмите **Добавить** и выберите **Добавить LDAP-коннектор**.
2. В окне **Свойства коннектора LDAP** укажите название LDAP-коннектора.
3. В поле **Доменное имя LDAP или IP-адрес** укажите IP-адрес контроллера домена, FQDN контроллера домена или FQDN домена (например, test.local). Если указан FQDN контроллера домена, то UserGate получит адрес контроллера домена с помощью DNS-запроса. Если указан FQDN домена, то при отключении основного контроллера домена UserGate будет использовать резервный контроллер.
4. В поле **Привязать DN (логин)** укажите логин, который необходимо использовать для подключения к серверу LDAP. Логин необходимо указать в формате <домен>\<логин> или <логин>@<домен>. Этот пользователь уже должен быть создан в домене.
5. Укажите пароль пользователя для подключения к домену.
6. Если необходимо, на вкладке **Домены LDAP** добавьте домены, которые обслуживаются указанным контроллером домена. Например, если используется дерево доменов или лес доменов Active Directory. Здесь же можно указать короткое netbios-имя домена.
7. На вкладке **Пути поиска** укажите пути, начиная с которых система будет осуществлять поиск пользователей и групп. Необходимо указывать полное имя, например ou=Office,dc=example,dc=com.
8. Если необходимо, на вкладке **Настройки** установите флажок **Использовать для соединений SSL**, чтобы использовать SSL-соединение для подключения к LDAP-серверу.
9. Установите флажок **Включено**, чтобы начать использовать LDAP-коннектор, и сохраните изменения.

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 веб-консоль управления UGMC пользователям LDAP необходимо указывать логин в формате <домен>\<логин>/system или <логин>@<домен>/system.

## Сервер аутентификации RADIUS

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

**Важно!**Перед выполнением описанных ниже шагов убедитесь, что RADIUS-сервер настроен для работы с UGMC (в раздел «RADIUS Clients and Servers» добавлена запись с IP-адресом UGMC). В противном случае сервер не будет отвечать на запросы. Пример настройки RADIUS-сервера — в разделе «Авторизация с помощью RADUIS ».

Чтобы добавить RADIUS-сервер:

1. На странице **Центр управления** в разделе **Центр управления → Серверы аутентификации** нажмите **Добавить** и выберите **Добавить RADIUS-сервер**.
2. В окне **Свойства RADIUS-сервера коннектора** укажите название RADIUS-сервера.
3. Добавьте IP-адрес RADIUS-сервера и UDP-порт, на котором RADIUS-сервис слушает запросы на аутентификацию (по умолчанию — 1812).
4. В поле **Секрет** введите пароль, указанный при настройке RADIUS-сервера.
5. Установите флажок **Включено**, чтобы начать использовать RADIUS-сервер, и сохраните изменения.

Для авторизации пользователей в веб-консоли управления UGMC с помощью RADIUS-сервера необходимо настроить профиль аутентификации. Подробнее о создании и настройке профилей — в разделе «Профили аутентификации».

## Сервер аутентификации TACACS+

Сервер TACACS+ позволяет производить авторизацию пользователей в веб-консоли управления UGMC. При использовании сервера TACACS+ UserGate MC передает на него информацию с именем и паролем пользователя, после чего сервер TACACS+ отвечает, успешно прошла аутентификация или нет.

Чтобы добавить сервер TACACS+:

1. На странице **Центр управления** в разделе **Центр управления → Серверы аутентификации** нажмите **Добавить** и выберите **Добавить TACACS+ сервер**.
2. В окне **Свойства TACACS+ сервера** укажите название сервера.
3. В поле **Секретный ключ** введите общий ключ, используемый протоколом TACACS+ для аутентификации.
4. Укажите IP-адрес сервера TACACS+ и UDP-порт, на котором сервер TACACS+ слушает запросы на аутентификацию.
5. Если необходимо использовать одно TCP-соединение для работы с сервером TACACS+, установите соответствующий флажок.
6. Если необходимо, измените время ожидания сервера TACACS+ для прохождения аутентификации. По умолчанию — 4 секунды.
7. Установите флажок **Включен**, чтобы начать использовать RADIUS-сервер, и сохраните изменения.

Для авторизации пользователей в веб-консоли управления UGMC с помощью сервера TACACS+ необходимо настроить профиль аутентификации. Подробнее о создании и настройке профилей — в разделе «Профили аутентификации».

**Профили аутентификации**

---

Documentation: ☑
Version: 7.x
Product: UGMC

Профиль позволяет определить набор методов аутентификации пользователей в веб-консоли управления UGMC.

**Важно!**Перед добавлением профиля аутентификации необходимо настроить нужный сервер аутентификации.

Чтобы добавить профиль аутентификации:

1. В разделе **Центр управления → Профили аутентификации** нажмите **Добавить**.
2. В окне **Свойства профиля аутентификации** на вкладке **Общие** укажите название профиля.
3. Если необходимо, настройте один или несколько параметров:
   - **Время бездействия до отключения** — время, по истечении которого будет отменена авторизация пользователя в случае его неактивности (при отсутствии сетевых пакетов с IP-адресами пользователя). После чего пользователю потребуется повторно авторизоваться.
   - **Время жизни аутентифицированного пользователя** — время, по истечении которого будет отменена авторизация пользователя. После чего пользователю потребуется повторно авторизоваться.
   - **Число неудачных попыток аутентификации (локальные пользователи)** — разрешенное количество неудачных попыток авторизации до блокировки учетной записи локального пользователя.
   - **Время блокировки локального пользователя** — время, на которое будет заблокирована учетная запись локального пользователя при достижении указанного числа неудачных попыток авторизации.
4. На вкладке **Методы аутентификации** нажмите **Добавить**, и по кнопке **Добавить** выберите предварительно настроенный сервер аутентификации: LDAP-коннектор, RADIUS-сервер или сервер TACACS+.
5. Сохраните изменения.

Теперь вы можете использовать созданный профиль при создании учетных записей администраторов.

Version: 7.x
Product: UGMC
Documentation: ☑

## 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 **Добавить** и ввести адреса.<br>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.<br>Список адресов записывается в обычный текстовый файл, где адреса прописываются в столбик без знаков препинания. Например:<br>x.x.x.x<br>y.y.y.y<br>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.<br>**Примечание**URL списка задается в формате: http://x.x.x.x/ или ftp://x.x.x.x/.<br>Расписание можно настроить в свойствах списка; возможно указать следующие варианты:<br>• Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет.<br>• Ежедневно.<br>• Еженедельно.<br>• Ежемесячно.<br>• Каждые ... часов.<br>• Каждые ... минут.<br>• Задать вручную.<br>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:<br>• Звездочка (*) — обозначает весь диапазон (от первого до последнего).<br>• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.<br>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".<br>• 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 |
|---|---|
| **Шаг 1.** Создать файл с необходимыми списком почтовых адресов. | Создать файл **list.txt** со списком почтовых адресов. |

| 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 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:<br>• Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет.<br>• Ежедневно.<br>• Еженедельно.<br>• Ежемесячно.<br>• Каждые ... часов.<br>• Каждые ... минут.<br>• Задать вручную.<br>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:<br>• Звездочка (*) — обозначает весь диапазон (от первого до последнего).<br>• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.<br>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".<br>Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа". |

### Номера телефонов

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

Для добавления новой группы телефонных номеров необходимо выполнить следующие шаги:

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

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

| Наименование | Описание |
|---|---|
| **Шаг 1.** Создать файл с необходимыми списком номеров. | Создать файл **list.txt** со списком номеров. |
| **Шаг 2.** Создать архив, содержащий этот файл. | Поместить файл в архив zip с именем **list.zip**. |
| **Шаг 3.** Создать файл с версией списка. | Создать файл **version.txt**, внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка. |
| **Шаг 4.** Разместить файлы на веб-сервере. | Разместить у себя на сайте **list.zip и version.txt**, чтобы они были доступны для скачивания. |
| **Шаг 5.** Создать список телефонных номеров и указать URL для обновления. | На каждом UserGate создать список номеров. При создании указать тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. UserGate будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты:<br>• Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет.<br>• Ежедневно.<br>• Еженедельно.<br>• Ежемесячно.<br>• Каждые ... часов.<br>• Каждые ... минут.<br>• Задать вручную.<br>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:<br>• Звездочка (*) — обозначает весь диапазон (от первого до последнего).<br>• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.<br>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".<br>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. |
| **Пароль** | Пароль учетной записи для подключения к SMPP-серверу. |
| **Правила трансляции номеров** | В некоторых случаях SMPP-провайдер ожидает номер телефона в определенном формате, например, в виде 89123456789. Для соответствия требованиям провайдера можно указать замену первых символов номеров с одних на другие. Например, заменить все номера, начинающиеся на +7, на 8. |

**Расширение системного раздела**

---

Version: 7.x
Product: NGFW, UGMC, LogAn, SIEM
Documentation: ☑

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

| Наименование | Описание |
|---|---|
| **Шаг 1.** Добавить дополнительный виртуальный диск. | Средствами гипервизора добавить **новый** диск необходимого размера в свойствах виртуальной машины UserGate. |
| **Шаг 2.** Расширить размер раздела в системных утилитах. | В меню загрузки узла UserGate войти в раздел **Support menu**.<br>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.

**Обновление ПО кластера UserGate MC**

Version: 7.x
Product: UGMC

## Прямое обновление ПО узлов кластера MC

Прямое обновление программного обеспечения узлов кластера UserGate MC можно инициировать в **Центре обновлений** каждого узла кластера. Для корректного обновления кластера необходимо, чтобы все узлы были включены и доступны на момент обновления первого узла.

Рекомендуется производить обновление кластера по следующему алгоритму:

1. Перед началом обновления создайте резервную копию узла — это позволит восстановить его работоспособность в случае сбоя. Подробнее о создании резервной копии — в разделе « Управление устройством».

2. Начните обновление с резервного узла кластера отказоустойчивости. Перейдите в раздел **Центр управления → Настройки → Центр обновлений** и запустите обновление.

**Примечание**После обновления программного обеспечения на первом узле, узлы кластера конфигурации временно отобразятся как недоступные из-за различий в версиях. После приведения всех узлов к одной версии отображение состояния кластера восстановится. Перевод роли мастер-узла в кластере отказоустойчивости будет доступен.

3. После успешного обновления резервного узла переведите его в статус мастер-узла и проверьте работоспособность ключевых функций. При отсутствии ошибок в работе узла приступайте к обновлению следующего узла кластера.

Обновление может занять длительное время. Рекомендуется планировать установку обновлений с учетом возможного времени простоя системы. Во время обновления устройство может несколько раз перезагружаться. Как правило, после первой перезагрузки происходит установка обновления, в это время в CLI доступен ограниченный набор команд, веб-интерфейс недоступен. После установки обновлений устройство также будет перезагружено.

**Важно!**Не вносите изменения в конфигурацию во время обновления кластера во избежание проблем синхронизации узлов.

Запись об установке обновления будет отображена в журнале событий (раздел **Центр управления → Журналы и отчеты** ).

## Обновление ПО узлов кластера MC с импортом конфигурации

В случае если прямое обновление программного обеспечения узлов кластера UserGate MC невозможно, например при переходе между разными ветками версий (6.x → 7.x), необходимо выполнить чистую установку узлов. Перенос конфигурации узла при таком варианте обновления программного обеспечения можно сделать с помощью операций экспорта и импорта конфигурации.

Экспорт настроек является кластерной функцией: экспортируется конфигурация всех узлов кластера. При импорте конфигурации будет предложен выбор нужного узла кластера для восстановления.

В отличие от резервного копирования, экспорт и импорт настроек не сохраняет текущее состояние всех компонентов устройства, сохраняются только текущие параметры.

Процедура импорта конфигурации узлов кластера MC включает в себя следующие основные шаги:

1. Экспорт настроек конфигурации узлов исходного кластера MC.
2. Импорт настроек конфигурации на мастер-узле нового кластера.
3. Подключение резервного узла нового кластера.

**Важно!**Импорт настроек конфигурации предназначен для восстановления конфигурации узла после чистой переустановки. Не рекомендуется проводить импорт полной конфигурации на работающем кластере (например, для проверки).

## Экспорт настроек конфигурации узлов исходного кластера MC

Для экспорта настроек конфигурации узлов исходного кластера MC:

1. В веб-консоли администратора любого из узлов кластера перейдите в раздел **Центр управления → Управление устройством → Экспорт и импорт настроек** , нажмите **Экспорт** и выберите **Экспортировать все настройки**.

2. Сохраните созданный файл экспорта конфигурации узлов кластера.

## Импорт настроек конфигурации мастер-узла кластера

Для импорта настроек конфигурации мастер-узла исходного кластера MC:

1. В веб-консоли узла, на который необходимо перенести конфигурацию мастер-узла кластера, перейдите в раздел **Центр управления → Управление устройством → Экспорт и импорт настроек** и нажмите **Импорт**.

2. В открывшемся окне импорта нажмите **Выберите файл** и выберите сохраненный ранее файл экспорта конфигурации узлов кластера.

3. Выберите **Импортировать все настройки** и нажмите **Выбрать узлы**.

4. Выберите название мастер-узла из файла экспорта и нажмите **Старт**. Узел перейдет в режим перезагрузки. В процессе перезагрузки будет выполнена процедура factory reset (возвращение к первоначальному состоянию), затем применятся импортированные настройки конфигурации и узел загрузится с конфигурацией мастер-узла из файла экспорта.

5. После окончания процедуры импорта повторно зарегистрируйте устройство в разделе **Дашборд → Лицензия** с помощью имеющегося ПИН-кода. Это необходимо, так как импорт настроек не восстанавливает информацию о лицензии.

6. Перейдите в раздел **Центр управления → Управление устройством → Кластер конфигурации** и выберите IP-адрес кластерного интерфейса текущего узла. После установки IP-адреса устройство перезагрузится.

7. После перезагрузки узла перейдите в раздел **Центр управления → Управление устройством → Кластер отказоустойчивости** и в свойствах импортированного кластера на вкладке **Узлы** выберите текущий узел.

8. На вкладке **Виртуальные IP** выберите интерфейс устройства, на котором будет работать VRRP.

9. Сохраните настройки кластера.

Импорт настроек конфигурации мастер-узла завершен.

## Подключение резервного узла кластера

Для подключения резервного узла кластера:

1. Выполните первоначальную установку узла MC в качестве дополнительного узла в кластере. Подробнее о добавлении дополнительного узла в кластер MC — в разделе « Управление устройством».

2. В разделе **Центр управления → Сеть → Интерфейсы** назначьте каждому интерфейсу корректную зону. Зоны и их параметры получены в результате репликации данных с первого узла кластера. При необходимости настройте шлюзы, маршруты.

3. После завершения синхронизации кластера конфигурации перейдите в раздел **Центр управления → Управление устройством → Кластер отказоустойчивости** и в свойствах кластера на вкладке **Узлы** выберите текущий узел.

4. На вкладке **Виртуальные IP** выберите интерфейс устройства, на котором будет работать VRRP.

5. Сохраните настройки кластера.

Импорт настроек конфигурации узлов кластера завершен.

**Настройка сети**

**Настройка сети (описание)**

---

Documentation: ☑
Product: UGMC
Version: 7.x

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). | Указать параметры защиты зоны от сетевого флуда для протоколов TCP (SYN-flood), UDP, ICMP:<br>• **Порог уведомления** — при превышении количества запросов с одного IP-адреса над указанным значением происходит запись события в системный журнал.<br>• **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.<br>Рекомендованные значения для порога уведомления — 300 запросов в секунду, для порога отбрасывания пакетов — 600 запросов в секунду.<br>**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. |
| **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.<br>Сервисы:<br>• **Ping** — позволяет пинговать UGMC.<br>• **SNMP** — доступ к UserGate по протоколу SNMP (UDP 161).<br>• **Консоль администрирования** — доступ к веб-консоли управления (TCP 8010 и 8300).<br>• **XML-RPC для управления** — позволяет управлять продуктом по API (TCP 4041).<br>• **VRRP** — сервис, необходимый для объединения нескольких NGFW в отказоустойчивый кластер (IP протокол 112).<br>• **Кластер** — сервис, необходимый для объединения нескольких NGFW в кластер (TCP 4369, TCP 9000-9100).<br>• **CLI по SSH** — доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200.<br>• **Сервис UserGate Management Center** — сервис подключения NGFW и LogAn (TCP 2022, 9712).<br>• **API XML RPC поверх HTTPS** — разрешает доступ к API поверх HTTPS (TCP 4443). Доступен в версии 7.3.3 и выше.<br>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.<br>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.<br>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, размер MTU, размер MSS.
- 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.

## Создание интерфейса VLAN

С помощью кнопки **Добавить VLAN** администратор может создавать сабинтерфейсы. При создании VLAN необходимо указать следующие параметры:

| Наименование | Описание |
|---|---|

| Наименование | Описание |
|---|---|
| **Включено** | Включает VLAN. |
| **Название** | Название VLAN. Название присваивается автоматически на основе имени физического порта и тега VLAN. |
| **Описание** | Опциональное описание интерфейса. |
| **Тип интерфейса** | Указать тип интерфейса — Layer 3 или Mirror. |
| **Тег VLAN** | Номер сабинтерфейса. Допускается создание до 4094 интерфейсов. |
| **Имя узла** | Имя узла в кластере, на котором создается данный VLAN. |
| **Интерфейс** | Физический интерфейс, на котором создается VLAN. |
| **Зона** | Зона, которой принадлежит VLAN. |
| **Алиас/Псевдоним** | Альтернативное имя интерфейса, заданное администратором. Параметр является опциональным и используется для работы с SNMP. Значение параметра — строка длиной не более 64-х символов.<br>**Важно!** Значение параметра не может содержать символы кириллицы. |
| **Сеть** | Способ присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Возможность изменить MAC-адрес, размер MTU, размер MSS (доступно начиная с релиза ПО 7.3.x). |

### 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** | Режим работы бонда должен совпадать с режимом работы на том устройстве, куда подключается бонд. Может быть:<br>• **Round robin.** Пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. Эта политика применяется для балансировки нагрузки и отказоустойчивости.<br>• **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.<br>• **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.<br>• **Broadcast.** Передает все на все сетевые интерфейсы. Эта политика применяется для отказоустойчивости.<br>• **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.<br>• **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.<br>• **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 устройства 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:<br>• **Slow** — запрос партнера на передачу LACPDU-пакетов каждые 30 секунд.<br>• **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:<br>• **Отключено** — устанавливает одинаковый MAC-адрес на всех интерфейсах во время переключения.<br>• **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.<br>• **Follow** — MAC-адрес на бонд-интерфейсе будет таким же, как на первом интерфейсе, добавленном в объединение. На втором и последующем интерфейсе этот MAC не устанавливается, пока они в резервном режиме. MAC-адрес прописывается во время обработки отказа, когда резервный интерфейс становится активным, он принимает новый MAC (тот, что на бонд-интерфейсе), а старому активному интерфейсу прописывается MAC, который был на текущем активном. |

| Наименование | Описание |
|---|---|
| **Xmit hash policy** | Определяет хэш-политику передачи пакетов через объединенные интерфейсы в режиме XOR или IEEE 802.3ad. Возможные значения:<br>• **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.<br>• **Layer 2+3** — использует как MAC-адреса, так и IP-адреса для генерации хэша. Алгоритм совместим с IEEE 802.3ad.<br>• **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. Возможность изменить MAC-адрес, размер MTU, размер MSS (доступно начиная с релиза ПО 7.3.x). |

### Настройка шлюзов

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

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

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

При наличии двух или более шлюзов возможны 2 варианта работы:

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

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

### Маршруты

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

Для добавления маршрута необходимо выполнить следующие шаги:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Задать название и описание данного маршрута. | В разделе **Сеть** выберите в меню **Маршруты**, нажмите кнопку **Добавить**. Укажите имя для данного маршрута. Опционально можно задать описание маршрута. |
| **Шаг 2.** Указать адрес назначения. | Задайте подсеть, куда будет указывать маршрут, например, 172.16.20.0/24 или 172.16.20.5/32. |
| **Шаг 3.** Указать шлюз. | Задайте IP-адрес шлюза, через который указанная подсеть будет доступна. Этот IP-адрес должен быть доступен с сервера UGMC. |
| **Шаг 4.** Указать интерфейс. | Выберите интерфейс, через который будет добавлен маршрут. Если оставить значение **Автоматически**, то UGMC сам определит интерфейс, исходя из настроек IP-адресации сетевых интерфейсов. |
| **Шаг 5.** Указать метрику. | Задайте метрику маршрута. Чем меньше метрика, тем приоритетней маршрут, если маршрутов в данную сеть несколько. |

**Журналы и отчёты**

**Журнал событий**

---

Documentation: ☑
Product: UGMC
Version: 7.x

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**

Documentation: ☑
Product: UGMC
Version: 7.x

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:<br>• Журнал событий.<br>Для каждого из журналов возможно указать синтаксис выгрузки:<br>• CEF — Common Event Format (ArcSight).<br>• JSON — JSON format.<br>• @CEE: JSON — CEE Log Syntax (CLS) Encoding JSON.<br>Обратитесь к документации на используемую у вас систему SIEM для выбора необходимого формата выгрузки журналов.<br>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:<br>• **Тревога**: состояние, требующее незамедлительного вмешательства.<br>• **Критическая**: состояние, требующее незамедлительного вмешательства либо предупреждающее о сбое в системе.<br>• **Ошибки**: в системе возникли ошибки.<br>• **Предупреждения**: предупреждения о возможном возникновении ошибок, если не будут предприняты никакие действия.<br>• **Уведомительная**: события, которые относятся к необычному поведению системы, но не являются ошибками.<br>• **Информативная**: информационные сообщения. |
| **Facility** | Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас систему SIEM. Возможны следующие значения:<br>• **Сообщения пользовательские**.<br>• **Системный сервис**.<br>• **Безопасность/авторизация**.<br>• **Аудит**.<br>• **Тревога**.<br>• **Local 0**.<br>• **Local 1**.<br>• **Local 2**.<br>• **Local 3**.<br>• **Local 4**.<br>• **Local 5**.<br>• **Local 6**.<br>• **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.<br>В кластерной конфигурации UGMC при экспорте журналов с разных узлов кластера необходимо указывать разные каталоги на сервере для каждого узла UGMC, поскольку имена файлов журналов на каждом узле идентичны. |

| Наименование | Описание |
| --- | --- |
| **Расписание** | Выбор расписания для отправки логов. Не применяется к методу отправки Syslog. Возможны варианты:<br>• Ежедневно.<br>• Еженедельно.<br>• Ежемесячно<br>• Каждые ... часов.<br>• Каждые ... минут.<br>• Задать вручную.<br>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:<br>• Звездочка (*) — обозначает весь диапазон (от первого до последнего).<br>• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.<br>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".<br>• 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.<br>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**

Documentation: ☑
Product: UGMC
Version: 7.x

Объем данных, регистрируемых в журналах, как правило, значителен, поэтому в стандартном режиме просмотра отображается лишь часть доступных полей. Для быстрого доступа к необходимой информации в UserGate MC предусмотрены средства поиска и фильтрации журналов. Поиск может выполняться как в простом, так и в расширенном режиме.

В режиме простого поиска фильтрация записей осуществляется с помощью графического интерфейса. Настройка условий поиска выполняется в удобной форме и не требует знания специальных команд или синтаксиса.

Для создания более сложных условий отбора предназначен режим расширенного поиска, использующий специализированный язык запросов. В этом режиме доступны поля журналов, которые не отображаются и не могут использоваться в стандартном режиме поиска. Запросы формируются с использованием имен полей, их значений, ключевых слов и логических операторов. Значения, содержащие пробелы, необходимо заключать в одинарные (' ') или двойные (" ") кавычки. Для значений без пробелов кавычки не требуются. Для объединения и группировки нескольких условий в запросе можно использовать круглые скобки.

Ключевые слова отделяются пробелами и могут быть следующими:

| **Ключевые поля** | **Значение** |
|---|---|
| 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:

| **Оператор** | **Значение** |
|---|---|
| = | Равно — требует полного совпадения значения поля с указанным значением.<br>Пример: ip = 172.16.31.1 .<br>Будут отображены все записи журнала, в которых поле ip будет точно соответствовать значению 172.16.31.1 |
| != | Не равно — значение поля не должно совпадать с указанным значением.<br>Пример: ip != 172.16.31.<br>Будут отображены все записи журнала, в которых поле ip не будет равно значению 172.16.31.1 |
| <= | Меньше либо равно — значение поля должно быть меньше или равно указанному в запросе значению. Оператор применим для полей, поддерживающих сравнение. Например, поля даты, portSource, portDest, statusCode и т. п.<br>Пример: date <= '2019-03-28T20:59:59' AND statusCode = 303 |
| >= | Больше либо равно — значение поля должно быть больше или равно указанному в запросе значению. Оператор применим для полей, поддерживающих сравнение. Например, поля даты, portSource, portDest, statusCode и т. п.<br>Пример: date >= "2019-03-13T21:00:00" AND statusCode = 200 |
| < | Меньше — значение поля должно быть меньше указанного в запросе значения. Оператор применим для полей, поддерживающих сравнение. Например, поля даты, portSource, portDest, statusCode и т. п.<br>Пример: date < '2019-03-28T20:59:59' AND statusCode = 404 |
| > | Больше — значение поля должно быть больше указанного в запросе значения. Оператор применим для полей, поддерживающих сравнение. Например, поля даты, portSource, portDest, statusCode и т. п.<br>Пример: (statusCode > 200 AND statusCode < 300) OR (statusCode = 404) |
| IN | Позволяет указать в запросе несколько значений поля. Список значений необходимо заключать в круглые скобки.<br>Пример: category IN (botnets, compromised, 'illegal software', 'phishing and fraud',' reputation high risk', 'unknown category') |
| NOT IN | Позволяет указать в запросе несколько значений поля. Будут отображены записи, в которых значение поля не совпадает ни с одним из указанных. Список значений необходимо заключать в круглые скобки.<br>Пример: category NOT IN (botnets, compromised, 'illegal software', 'phishing and fraud', 'reputation high risk', 'unknown category') |
| ~ | Содержит — позволяет указать подстроку, которая должна присутствовать в значении выбранного поля. Поиск выполняется без учета регистра.<br>Пример: browser ~ "Mozilla/5.0".<br>Оператор применяется только к полям, содержащим строковые значения |
| !~ | Не содержит — позволяет указать подстроку, которая не должна присутствовать в значении выбранного поля. Поиск выполняется без учета регистра.<br>Пример: browser !~ "Mozilla/5.0".<br>Оператор применяется только к полям, содержащим строковые значения |
| MATCH | Поиск по полю с помощью регулярного выражения. Будут показаны только те записи, в которых значение поля соответствует заданному шаблону.<br>Пример: details MATCH NAT — будут отфильтрованы все записи журнала, в которых в проверяемом поле details найдется слово «NAT» |
| NOT MATCH | Поиск записей, в которых значение поля не совпадает с заданным регулярным выражением. Будут показаны только те записи, в которых значение поля не соответствует заданному шаблону.<br>Пример: details NOT MATCH NAT — будут отфильтрованы все записи журнала, в которых в проверяемом поле details не найдется слово «NAT» |

При формировании запроса в режиме расширенного поиска UserGate MC предлагает варианты названий полей, допустимых операторов и возможных значений. Это упрощает создание сложных поисковых выражений и снижает вероятность ошибок при вводе. Набор доступных полей и перечень допустимых значений зависят от типа просматриваемого журнала.

При переходе из режима простого поиска в режим расширенного поиска UserGate MC автоматически преобразует заданные параметры фильтрации в строку запроса, соответствующую условиям, указанным в базовом режиме. Вы можете продолжить формирование строки поиска с использованием расширенных возможностей языка запросов без необходимости повторного ввода критериев отбора.

Documentation: ☑
Product: UGMC
Version: 7.x

## 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:<br>• 0 — информационные.<br>• 6 — предупреждения.<br>• 8 — ошибки.<br>• 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@einersonstal |
| | **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** | Время получения события в формате: yyyy-mm-ddThh:mm:ssZ. | 2022-05-12T08:11:46.15869Z |
| **ip_address** | IPv4-адрес источника события. | 192.168.174.134 |
| **node** | Имя, которое однозначно идентифицирует устройство, генерирующее это событие. | mc_core@einersonstal |
| **attributes** | Детали события в формате JSON. | {"rule":{"logrotate":12,"attributes":{"timezone":"Asia/Novosibirsk"},"id":"66f9de9f-d698-4bec-b3b0-ba65b46d3608","name":"Example log export ftp"} |
| **event_type** | Тип события. | logexport_rule_updated |
| **event_severity** | Важность события. | info (информационные), warning (предупреждения), error (ошибки), critical (критичные). |
| **event_origin** | Модуль, в котором произошло событие. | core |
| **event_component** | Компонент, в котором произошло событие. | console_auth |

**Маршруты**

---

Documentation: ☑
Product: UGMC
Version: 7.x

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 **K** 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**

---

Documentation: ☑
Product: UGMC
Version: 7.x

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**

---

Documentation: ☑
Product: UGMC
Version: 7.x

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**

---

Documentation: ☑
Product: UGMC
Version: 7.x

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**

Documentation: ☑
Product: UGMC
Version: 7.x

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 цифры и латинские буквы. |
| **Контекст** | Необязательный параметр, определяющий SNMP context. Можно использовать только латинские буквы и цифры.<br>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%. |
| **trapHighUsersCounter** | Количество активных пользователей достигло 90% от порога лицензии. |
| **trapDataPartitionFSStatus** | Статус 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. |

| Наименование | Описание |
|---|---|
| **trapChecksumFailed** | Нарушение целостности бинарных файлов. |
| **trapHighCPUUsage** | Высокая загрузка центрального процессора (95%). |
| **trapLowMemory** | Высокая загрузка памяти (95%). |
| **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 -40ºC), верхний предел равен 85ºC. |

**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.<br>• **0** — clean.<br>• **1** — not clean. |
| **utmHAStatus** | integer | Текущий статус узла кластера отказоустойчивости:<br>• **0** — master-узел.<br>• **1** — slave-узел.<br>• **3** — fault. |
| **utmHAStatusReason** | integer | Причина изменения статуса узла отказоустойчивого кластера:<br>• **1** — связь с узлом потеряна.<br>• **2** — HTTP прокси-сервер недоступен.<br>• **3** — ни один из шлюзов недоступен.<br>• **4** — DNS-сервер недоступен.<br>• **5** — узел UserGate Management Center недоступен. |
| **utmCPUUsage** | integer | Загруженность центрального процессора (%). |
| **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:<br>• **no_raid**.<br>• **0** — optimal — массив в оптимальном состоянии.<br>• **1** — degraded — полный или частичный выход из строя одного из дисков.<br>• **2** — rebuild — восстановление массива. |
| **utmBroadcomRaidStatus** | integer | Текущий статус RAID (Redundant Array of Independent Disks), построенного на контроллере Broadcom:<br>• **no_raid**<br>• **0** — optimal — массив в оптимальном состоянии.<br>• **1** — degraded — полный или частичный выход из строя одного из дисков. Переход в данный статус произойдёт при выходе из строя 2-х дисков.<br>• **2** — partialDegraded — полный или частичный выход из строя одного из дисков.<br>• **3** — failed — не работает из-за наличия ошибки.<br>• **4** — offline — диск не доступен для RAID-контроллера. |

| Наименование | Тип данных | Описание |
|---|---|---|
| **utmPowerSupply** | integer | Количество источников питания:<br>• **1** — один блок питания.<br>• **2** — два блока питания. |
| **utmPowerSupplyStatus** | integer | Состояние источника питания:<br>• **no_power_supplies**.<br>• **0** — off.<br>• **1** — on. |
| **utmCSCIfName** | string | Название интерфейса. |
| **utmCSCStatus** | integer | Статус сетевого адаптера:<br>• **1** — кабель подключен.<br>• **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 фактическое число загруженных виртуальных процессоров. |
| **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. ( *) |
| **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. (*) |
| **httpBlockedRequestCounter** | integer | Количество заблокированных HTTP запросов. (*) |

| Наименование | Тип данных | Описание |
|---|---|---|
| **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:<br>• **no_power_supplies**.<br>• **on**.<br>• **off**. |
| **powerSupply2Status** | string | Состояние второго источника питания:<br>• **no_power_supplies**.<br>• **on**.<br>• **off**. |
| **raidType** | string | Тип RAID массива. |
| **raidStatus** | string | Текущий статус RAID (Redundant Array of Independent Disks):<br>• **no_raid**.<br>• **0** — optimal — массив в оптимальном состоянии.<br>• **1** — degraded — полный или частичный выход из строя одного из дисков.<br>• **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. |

| Наименование | Тип данных | Описание |
|---|---|---|
| **ifType** | integer | Тип интерфейса, определённый в соответствии с протоколом физического/канального уровней:<br>• **1** — other — неизвестный тип.<br>• **2** — regular1822 — определён в BBN Report 1822.<br>• **3** — hdh1822 — определён в BBN Report 1822.<br>• **4** — ddn-x25 — определён в BBN Report 1822.<br>• **5** — определён в стандарте канального уровня сетевой модели OSI X.25.<br>• **6** — ethernet-csmacd — сетевой интерфейс типа Ethernet, независимо от скорости (определён в RFC 3635).<br>• **7** — iso88023-csmacd — определён в IEEE 802.3.<br>• **8** — iso88024-tokenBus — определён в стандарте IEEE 8802.4.<br>• **9** — iso88025-tokenRing — сетевой интерфейс использует подключение Token Ring; определяется в стандарте IEEE 802.5.<br>• **10** — iso88026-man — определён в стандарте ISO 88026 "MAN".<br>• **11** — starLan — определён в стандарте IEEE 802.3e.<br>• **12** — proteon-10Mbit — Proteon 10 Mbit<br>• **13** — proteon-80Mbit — Proteon 80 Mbit.<br>• **14** — hyperchannel — высокоскоростной канал, используемы в сети ISDN.<br>• **15** — fddi — сетевой интерфейс использует подключение FDDI (Fiber Distributed Data Interface). FDDI — это набор стандартов передачи данных по оптоволоконным линиям в локальной сети.<br>• **16** — lapb — протокол канального уровня, используемым для передачи пакетов стандарта X.25.<br>• **17** — sdlc — протокол канального уровня для системной сетевой архитектуры IBM.<br>• **18** — ds1 — способен обрабатывать 24 одновременных соединения на общей скорости 1,544 Мбит/с; также называется T1<br>• **19** — e1 — европейский аналог T1.<br>• **20** — basicISDN — для связи аппаратуры абонента и ISDN-станции.<br>• **21** — primaryISDN — используется для подключения к широкополосным магистралям, связывающим местные и центральные АТС или сетевые коммутаторы.<br>• **22** — propPointToPointSerial — определён в стандарте RFC1213.<br>• **23** — ppp — сетевой интерфейс использует подключение PPP (Point-To-Point Protocol).<br>• **24** — softwareLoopback — сетевой интерфейс является петлевым адаптером. Такие интерфейсы часто используются для тестирования; они не отправляют трафик в сеть.<br>• **25** — eon — ConnectionLess Network Protocol (CLNP) over Internet Protocol (IP); определён в ISO/IEC 8473-1.<br>• **26** — ethernet-3Mbit — сетевой интерфейс использует подключение Ethernet со скоростью 3 Мбит/с. Эта версия Ethernet определяется в стандарте IETF RFC 895.<br>• **27** — nsip — XNS over IP — предназначен для использования в разнообразных средах передачи данных.<br>• **28** — slip — сетевой интерфейс использует подключение SLIP (Serial Line Internet Protocol). SLIP определяется в стандарте IETF RFC 1055.<br>• **29** — ultra — ULTRA Technologies.<br>• **30** — ds3 — высокоскоростной интерфейс передачи данных, сформированный мультиплексированием сигналов DS1 и DS2; также называется T3.<br>• **31** — sip — сетевой интерфейс использует подключение SLIP (Serial Line Internet Protocol). SLIP определяется в стандарте IETF RFC 1055.<br>• **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:<br>• **1** — up — готов для передачи пакетов.<br>• **2** — down — не работает.<br>• **3** — testing — в режиме тестирования; рабочие пакеты не могут быть переданы. |
| **ifOperStatus** | integer | Текущий статус работы интерфейса:<br>• **1** — up — интерфейс готов для передачи пакетов.<br>• **2** — down — интерфейс не может передавать пакеты данных.<br>• **3** — testing — выполняется тестирование сетевого интерфейса; рабочие пакеты не могут быть переданы.<br>• **4** — unknown — интерфейс находится в неизвестном состоянии.<br>• **5** — dormant — сетевой интерфейс не может передавать пакеты данных, он ожидает внешнее событие.<br>• **6** — notPresente — сетевой интерфейс не может передавать пакеты данных из-за отсутствующего компонента, обычно аппаратного.<br>• **7** — lowerLayerDown — сетевой интерфейс не может передавать пакеты данных, потому что он работает поверх одного или нескольких других интерфейсов, и не менее одного из этих интерфейсов "нижнего уровня" не работает. |
| **ifLastChange** | timeticks | Значение SysUpTime, когда интерфейс оказался в данном состоянии. |
| **ifInOctets** | counter32 | Количество байтов, принятое данным интерфейсом, включая служебные. |
| **ifInUcastPkts** | counter32 | Количество доставленных пакетов одноадресной рассылки. |
| **ifInNUcastPkts** | counter32 | Количество доставленных многоадресных и широковещательных пакетов. |
| **ifInDiscards** | counter32 | Количество входящих пакетов, которые были отброшены, даже если не было обнаружено ошибок, препятствующих их доставке. Одна из возможных причин отбрасывания: освобождение буферного пространства. |

| Наименование | Тип данных | Описание |
|---|---|---|
| **ifInErrors** | counter32 | Количество входящих пакетов, которые содержат ошибки, препятствующие их доставке. |
| **ifInUnknownProtos** | counter32 | Количество пакетов, которые были получены через этот интерфейс и отброшены из-за использования неизвестного или неподдерживаемого протокола. |
| **ifOutOctets** | counter32 | Количество байтов, переданное данным интерфейсом, включая служебные. |
| **ifOutUcastPkts** | counter32 | Количество отправленных пакетов одноадресной рассылки, включая пакеты, которые были отброшены или не отправлены. |
| **ifOutNUcastPkts** | counter32 | Количество отправленных многоадресных и широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены. |
| **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. |
| **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** — 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:<br>• **1** — enabled — включено.<br>• **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:<br>• **1** — true — станция принимает все пакеты/кадры независимо от того, кому они адресованы.<br>• **2** — false — интерфейс принимает только пакеты/кадры, адресованные этой станции.<br>Значение объекта не влияет на приём широковещательных и многоадресных пакетов/кадров. |
| **ifAlias** | string | Название интерфейса, заданное администратором. |
| **ifCounterDiscontinuityTime** | timeticks | Значение SysUpTime, когда произошло событие, ставшее причиной сбоя работы одного или более счётчиков интерфейса. |

**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:<br>• thermName (string) — название сенсора.<br>• thermValue (integer) — показание сенсора.<br>• 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**

Documentation: ☑
Product: UGMC
Version: 7.x

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**.<br>Engine ID может быть сформирован в формате:<br>• IPv4 (ip4).<br>• IPv6 (ipv6).<br>• MAC-адрес (mac).<br>• Текст (text).<br>• Октеты (jctets). |

**Правила оповещений**

Documentation:
Product: UGMC
Version: 7.x

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. |
| **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**

Documentation:
Product: UGMC
Version: 7.x

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:<br>• Без аутентификации, без шифрования (noAuthNoPriv).<br>• С аутентификацией, без шифрования (authNoPriv).<br>• С аутентификацией, с шифрованием (authPriv).<br>Наиболее безопасным считается режим работы authPriv. |
| **Алгоритм аутентификации** | Алгоритм, используемый для аутентификации. Возможно использовать:<br>• SHA1;<br>• MD5;<br>• SHA224;<br>• SHA256;<br>• SHA384;<br>• SHA512. |
| **Пароль аутентификации** | Пароль, используемый для аутентификации. |
| **Алгоритм шифрования** | Алгоритм, используемый для шифрования. Возможно использовать DES и AES. |
| **Пароль шифрования** | Пароль, используемый для шифрования. |

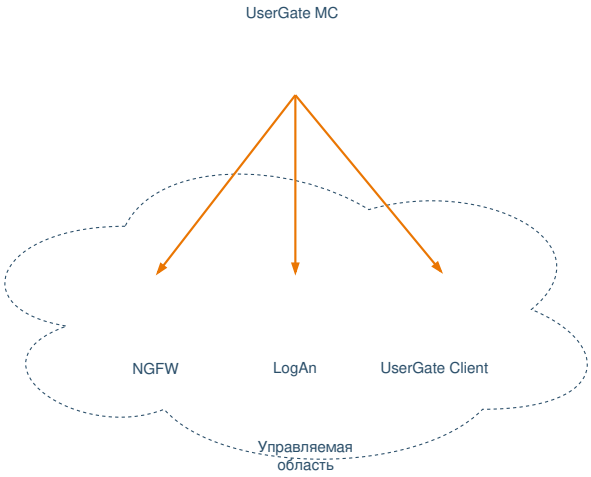
**Управление областями**

**Управление областями (Описание)**

---

Documentation:
Version: 7.x
Product: UGMC

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).

**Создание управляемых областей**

---

Version: 7.x
Product: UGMC
Documentation: ☑

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**

Version: 7.x
Product: UGMC
Documentation: ☑
**Важно!**Для управления областью администратору UGMC необходимо создать корневого администратора области, обладающего всеми полномочиями на эту область, в том числе правами на добавление дополнительных администраторов области. Подробнее о создании корневого администратора области — в разделе «Администраторы».

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

Чтобы добавить дополнительного администратора области:

1. Войдите в веб-консоль управления под учетной записью корневого администратора области , указав логин в виде <логин_корневого_администратора_области>/<код_области>, например Admin/UG.

2. Создайте профиль аутентификации дополнительного администратора области. Профиль определяет список полномочий администратора. Можно создавать несколько профилей с разными полномочиями.

3. Создайте учетную запись администратора области. На этом этапе можно выбрать способ авторизации администратора: локальный, через LDAP-коннектор или с помощью профиля аутентификации.

## Создание профиля дополнительного администратора области

Чтобы создать профиль дополнительного администратора области:

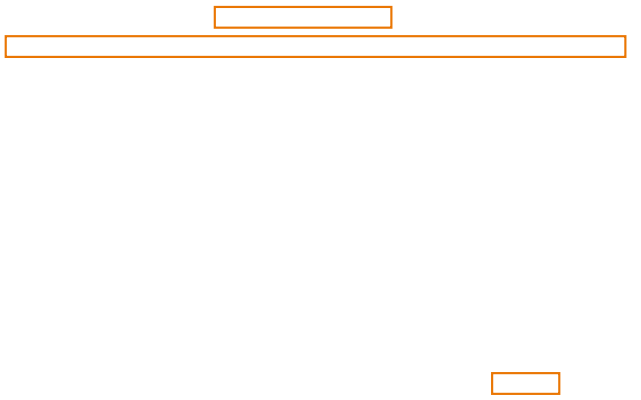
1. В разделе **Управление областью → Центр управления → Администраторы** в блоке **Профили администраторов** нажмите **Добавить**.

2. В окне **Настройка профиля** на вкладке **Общие** укажите название профиля и, если необходимо, его описание.

3. На вкладке **Права доступа на область** укажите, какими правами доступа будет обладать администратор с этим профилем. В качестве разрешений для доступа можно указать **Нет доступа**, **Чтение** или **Чтение и запись**.

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

- В строке **Шаблон** выберите конкретный шаблон или **Все шаблоны** для настройки прав доступа.
- В списке ниже укажите права доступа к параметрам шаблонов управляемых устройств. Параметры представлены в виде доступных для делегирования объектов дерева веб-консоли управления устройств. В качестве разрешений для доступа можно указать **Нет доступа**, **Чтение** или **Чтение и запись**.



5. Сохраните изменения.

## Создание учетной записи локального администратора области

Чтобы создать учетную запись локального администратора области:

1. В разделе **Управление областью → Центр управления → Администраторы** в блоке **Администраторы** нажмите **Добавить** и выберите **Добавить локального администратора**.

2. В окне **Свойства администратора** укажите имя, логин и пароль администратора

3. Выберите созданный ранее профиль администратора.

4. Установите флажок **Включено**, чтобы разрешить вход в систему под этой учетной записью.

5. Сохраните изменения.

## Создание учетной записи LDAP-администратора области

Чтобы создать учетную запись пользователя из существующего домена:

1. Убедитесь, что в разделе **Управление областью → Центр управления → Серверы аутентификации** предварительно настроен соответствующий LDAP-коннектор. Подробнее о настройке LDAP-коннектора — в разделе «Серверы аутентификации области».

2. В разделе **Администраторы** в блоке **Администраторы** нажмите **Добавить** и выберите **Добавить пользователя LDAP**.

3. В окне **Свойства LDAP-администратора** нажмите кнопку **Выбрать**, выберите настроенный LDAP-коннектор и затем добавьте логин нужного пользователя.

4. Выберите созданный ранее профиль администратора.

5. Установите флажок **Включено**, чтобы разрешить вход в систему под этой учетной записью.

6. Сохраните изменения.

При входе в веб-интерфейс администрирования под этой учетной записью необходимо указывать логин в формате <логин>@<домен>/system или <домен>\<логин>/system.

Чтобы добавить учетную запись для группы пользователей из существующего домена:

1. Убедитесь, что в разделе **Управление областью → Центр управления → Серверы аутентификации** предварительно настроен соответствующий LDAP-коннектор. Подробнее о настройке LDAP-коннектора — в разделе «Серверы аутентификации области».

2. В разделе **Администраторы** в блоке **Администраторы** нажмите **Добавить** и выберите **Добавить группу LDAP**.

3. В окне **Свойства LDAP-администратора** нажмите кнопку **Выбрать**, выберите настроенный LDAP-коннектор и затем добавьте логин группы пользователей.

4. Выберите созданный ранее профиль администратора.

5. Установите флажок **Включено**, чтобы разрешить вход в систему под этой учетной записью.

6. Сохраните изменения.

При входе в веб-интерфейс администрирования под этой учетной записью необходимо указывать имя пользователя в формате user@domain/system или domain\user/system.

## Создание учетной записи администратора области с профилем аутентификации

Как корневой администратор области, вы можете управлять доступом дополнительных администраторов области к веб-консоли управления областью с помощью профиля аутентификации, в котором в списке доступных методов аутентификации указаны заранее настроенные серверы, такие как LDAP, TACACS+ или RADIUS. Если в профиле аутентификации указано сразу несколько методов аутентификации, будут перебираться все методы по очереди до первого сработавшего.

Чтобы добавить учетную запись дополнительного администратора области с профилем аутентификации:

1. Убедитесь, что в разделе **Управление областью → Центр управления → Серверы аутентификации** добавлены данные о настроенном сервере аутентификации. Подробнее о сервере аутентификации — в разделе «Серверы аутентификации области».

2. Убедитесь, что в разделе **Профили аутентификации** создан профиль с нужным методом аутентификации. Подробнее о создании профиля— в разделе « Профили аутентификации области».

3. В разделе **Администраторы** в блоке **Администраторы** нажмите **Добавить** и выберите **Добавить администратора с профилем аутентификации**.

4. В окне **Свойства администратора с профилем аутентификации** укажите имя, логин и пароль администратора.

5. Выберите созданный ранее профиль администратора.

6. Выберите созданный ранее профиль аутентификации.

7. Установите флажок **Включено**, чтобы разрешить вход в систему под этой учетной записью.

8. Сохраните изменения.

**Серверы аутентификации области**

---

Documentation: ☑
Version: 7.x
Product: UGMC

Серверы аутентификации — это внешние источники учетных записей пользователей для авторизации в веб-консоли управляемой области. Работа сервера аутентификации области аналогична работе сервера аутентификации для UGMC — отличается только место 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.
- Выполнять авторизацию администраторов области через домены Active Directory и FreeIPA.

Чтобы добавить LDAP-коннектор:

1. В веб-консоли управляемой области в разделе **Управление областью → Центр управления → Серверы аутентификации** нажмите **Добавить** и выберите **Добавить LDAP-коннектор**.
2. В окне **Свойства коннектора LDAP** укажите название LDAP-коннектора.
3. В поле **Доменное имя LDAP или IP-адрес** укажите IP-адрес контроллера домена, FQDN контроллера домена или FQDN домена (например, test.local). Если указан FQDN контроллера домена, то UserGate получит адрес контроллера домена с помощью DNS-запроса. Если указан FQDN домена, то при отключении основного контроллера домена, UserGate будет использовать резервный контроллер.
4. В поле **Привязать DN (логин)** укажите имя пользователя, которое необходимо использовать для подключения к серверу LDAP. Имя необходимо указать в формате <ДОМЕН>\<логин> или <логин>@<домен>. Этот пользователь уже должен быть создан в домене.
5. Укажите пароль пользователя для подключения к домену.
6. Если необходимо, на вкладке **Домены LDAP** добавьте домены, которые обслуживаются указанным контроллером домена. Например, если используется дерево доменов или лес доменов Active Directory. Здесь же можно указать короткое netbios-имя домена.
7. На вкладке **Пути поиска** укажите пути, начиная с которых система будет осуществлять поиск пользователей и групп. Необходимо указывать полное имя, например ou=Office,dc=example,dc=com.
8. Если необходимо, на вкладке **Настройки** установите флажок **Использовать для соединений SSL**, чтобы использовать SSL-соединение для подключения к LDAP-серверу.
9. Установите флажок **Включено**, чтобы начать использовать LDAP-коннектор, и сохраните изменения.

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 веб-консоль управляемой области пользователям LDAP необходимо указывать имя в формате <домен>\<логин>/system или <логин>@<домен>/system.

## Сервер аутентификации RADIUS

Сервер аутентификации RADIUS позволяет производить авторизацию пользователей в веб-консоли управляемой области, которая 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.

**Важно!**Перед выполнением описанных ниже шагов убедитесь, что RADIUS-сервер настроен для работы с UGMC (в раздел «RADIUS Clients and Servers» добавлена запись с IP-адресом UGMC). В противном случае сервер не будет отвечать на запросы. Пример настройки RADIUS-сервера — в разделе «Авторизация с помощью RADUIS ».

Чтобы добавить RADIUS-сервер:

1. В веб-консоли управляемой области в разделе **Управление областью → Центр управления → Серверы аутентификации** нажмите **Добавить** и выберите **Добавить RADIUS-сервер**.
2. В окне **Свойства RADIUS-сервера коннектора** укажите название RADIUS-сервера.
3. Добавьте IP-адрес RADIUS-сервера и UDP-порт, на котором RADIUS-сервис слушает запросы на аутентификацию (по умолчанию — 1812).
4. В поле **Секрет** введите пароль, указанный при настройке RADIUS-сервера.
5. Установите флажок **Включено**, чтобы начать использовать RADIUS-сервер, и сохраните изменения.

Для авторизации пользователей в веб-консоли управляемой области с помощью сервера RADIUS необходимо настроить профиль аутентификации. Подробнее о создании и настройке профилей — в разделе «Профили аутентификации области».

## Сервер аутентификации TACACS+

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

Чтобы добавить сервер TACACS+:

1. В веб-консоли управляемой области в разделе **Управление областью → Центр управления → Серверы аутентификации** нажмите **Добавить** и выберите **Добавить TACACS+ сервер**.
2. В окне **Свойства TACACS+ сервера** укажите название сервера.
3. В поле **Секретный ключ** введите общий ключ, используемый протоколом TACACS+ для аутентификации.
4. Укажите IP-адрес сервера TACACS+ и UDP-порт, на котором сервер TACACS+ слушает запросы на аутентификацию.
5. Если необходимо использовать одно TCP-соединение для работы с сервером TACACS+, установите соответствующий флажок.
6. Если необходимо, измените время ожидания сервера TACACS+ для прохождения аутентификации. По умолчанию — 4 секунды.
7. Установите флажок **Включен**, чтобы начать использовать RADIUS-сервер, и сохраните изменения.

Для авторизации пользователей в веб-консоли управляемой области с помощью сервера TACACS+ необходимо настроить профиль аутентификации. Подробнее о создании и настройке профилей — в разделе «Профили аутентификации области».

**Профили аутентификации области**

---

Version: 7.x
Product: UGMC
Documentation: ☑

Профиль позволяет определить набор способов авторизации администраторов в веб-консоли управляемой области.

**Важно!**Перед добавлением профиля аутентификации необходимо настроить нужный сервер аутентификации.

Чтобы добавить профиль аутентификации:

1. В разделе **Управление областью → Центр управления → Профили аутентификации** нажмите **Добавить**.
2. В окне **Свойства профиля аутентификации** на вкладке **Общие** укажите название профиля.
3. Если необходимо, настройте один или несколько параметров:
   - **Время бездействия до отключения** — время, по истечении которого будет отменена авторизация пользователя в случае его неактивности (при отсутствии сетевых пакетов с IP-адресами пользователя). После чего пользователю потребуется повторно авторизоваться.
   - **Время жизни аутентифицированного пользователя** — время, по истечении которого будет отменена авторизация пользователя. После чего пользователю потребуется повторно авторизоваться.
   - **Число неудачных попыток аутентификации (локальные пользователи)** — разрешенное количество неудачных попыток авторизации до блокировки учетной записи локального пользователя.
   - **Время блокировки локального пользователя** — время, на которое будет заблокирована учетная запись локального пользователя при достижении указанного числа неудачных попыток авторизации.
4. На вкладке **Методы аутентификации** нажмите **Добавить**, и по кнопке **Добавить** выберите предварительно настроенный сервер аутентификации: LDAP-коннектор, RADIUS-сервер или сервер TACACS+.
5. Сохраните изменения.

Теперь вы можете использовать созданный профиль при создании учетных записей администраторов.

**Каталоги пользователей**

---

Version: 7.x
Product: UGMC
Documentation: ☑

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

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

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

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

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

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

**Управление устройствами UserGate NGFW (описание)**

Documentation:
Product: UGMC
Version: 7.x

В веб-консоли UserGate Management Center (далее также — UserGate MC) администраторы управляемой области могут централизованно управлять подключенными UserGate NGFW, а также настраивать параметры этих устройств. Для этого необходимо выполнить следующее:

1) создать шаблоны UserGate NGFW;

2) настроить параметры шаблонов UserGate NGFW;

3) создать группу шаблонов UserGate NGFW;

4) настроить интеграцию UserGate NGFW с UserGate MC.

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

**Важно!**Начиная с версии 7.2.0 названия объектов, используемых в UserGate MC, стали чувствительны к регистру. Во избежание конфликтов названий при переходе с более низких версий на версию 7.2.0 или выше названия всех объектов UGMC автоматически переводятся в нижний регистр. При необходимости после обновления вы можете изменить названия объектов.

## Создание шаблонов UserGate NGFW

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

Чтобы создать шаблон UserGate NGFW:

1. В разделе **Управление областью → NGFW → Шаблоны** нажмите **Добавить**.

2. На вкладке **Общие** укажите название и при необходимости описание шаблона.

3. При необходимости на вкладке **Разделы** установите флажок **Настроить отображение разделов** и выберите разделы веб-консоли, которые должны отображаться в шаблоне.

   **Примечание**Выбор разделов доступен начиная с версии 7.6.0.

4. Нажмите **Сохранить**.

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

## Настройка параметров шаблонов UserGate NGFW

Чтобы настроить параметры шаблона UserGate NGFW:

В разделе **NGFW** для объекта **Шаблон** в выпадающем списке выберите шаблон, параметры которого необходимо настроить.

Настройка параметров шаблона выполняется в разделах боковой панели аналогично настройке параметров локального UserGate NGFW (подробнее — в Руководстве администратора UserGate NGFW).

При настройке параметров шаблона UserGate NGFW следует учитывать следующее:

- Значения параметров в шаблоне имеют более высокий приоритет, чем указанные администратором UserGate NGFW локально. Если значение параметра не указано ни в шаблоне, ни на стороне UserGate NGFW, будет использоваться значение по умолчанию.
- Для UserGate NGFW предусмотрен системный шаблон UserGate Libraries template, который создается в UGMC автоматически. Этот шаблон содержит сетевые зоны UserGate NGFW по умолчанию, а также библиотеки таких элементов, как сервисы, календари, полосы пропускания, шаблоны страниц, категории URL, профили SSL, профили приложений и профили СОВ.

  В версии 7.5.0 и выше в библиотеках профилей приложений и СОВ шаблона UserGate Libraries template по умолчанию создано по два профиля:

  - профиль, содержащий все сигнатуры, за исключением принадлежащих к категории ICS/IoT;
  - профиль, содержащий только сигнатуры, принадлежащие к категории ICS/IoT.
- После применения параметров шаблона к управляемым устройствам администраторы могут изменять базовые параметры и параметры сетевых интерфейсов локально на каждом UserGate NGFW. Подробная информация об этих параметрах приведена в разделах «Настройка общих параметров» и «Настройка интерфейсов» Руководства администратора UserGate NGFW.
- При настройке параметров сетевых интерфейсов в шаблоне невозможно конфигурировать интерфейс port0. Первым физическим интерфейсом, доступным для настройки в шаблоне, будет port1.

  Параметры интерфейса port0 настраиваются администратором UserGate NGFW при первоначальной настройке устройства. По умолчанию этот интерфейс используется для подключения UserGate NGFW к UserGate MC.

  При необходимости можно сконфигурировать сетевые интерфейсы локально на UserGate NGFW, для этого в параметрах выбранного интерфейса шаблона должен быть установлен флажок **Настраивается на устройстве**.

  Если вы создаете интерфейс в шаблоне, этот интерфейс автоматически будет добавлен в UserGate NGFW. Удаление интерфейса из шаблона не удаляет интерфейс на межсетевом экране. Если требуется удалить интерфейс на межсетевом экране, необходимо сделать это вручную.
- Правила политик в шаблоне не переопределяют правила, созданные администраторами межсетевых экранов UserGate NGFW локально, а добавляются к ним в виде преправил и постправил.
- Для некоторых правил политик в шаблоне можно указать управляемые устройства, к которым будут применяться эти правила. Действие доступно в окне свойств правила на вкладке **Устройства**.

  Следует учитывать, что частое использование этой функции может усложнить для администраторов понимание того, какие правила политик будут применяться к устройству.
- Библиотеки элементов шаблона (например, библиотеки IP-адресов, URL-списков, а также типов контента) по умолчанию не содержат данных, в отличие от библиотек UserGate NGFW (подробнее — в разделе «Библиотеки элементов» Руководства администратора UserGate NGFW). Перед настройкой параметров шаблона следует добавить необходимые элементы библиотек.

  **Важно!**Данные библиотек не синхронизируются: если добавленные элементы не используются в параметрах шаблона, они не будут добавлены в библиотеки UserGate NGFW. Поэтому, чтобы на управляемых устройствах отображались, например, списки IP-адресов, созданные в шаблоне, необходимо использовать эти списки при настройке параметров шаблона.
  **Примечание**Корректность работы проприетарных сигнатур СОВ и приложений зависит от актуальности библиотек для этих сигнатур — рекомендуется проверять актуальность библиотек после обновления UserGate MC или восстановления его параметров. Если по какой-либо причине библиотеки не обновились автоматически, их можно обновить вручную. Действие выполняется администратором UserGate MC в разделе «Центр управления» ➔ «Настройки» ➔ «Обновления библиотек».
- При создании в шаблоне профиля СОВ в списке совпавших сигнатур может отображаться несколько копий одной и той же проприетарной сигнатуры (см. рисунок ниже).

  Такая ситуация возникает, если в шаблоне переопределяются параметры проприетарных сигнатур СОВ (в разделе боковой панели **Библиотеки → Сигнатуры СОВ** для выбранного шаблона), например действие по обнаружению сигнатуры. В этом случае для конфигурации параметров выбирается сигнатура, которая относится к выбранному шаблону.
- Начиная с версии 7.4.0 если идентификатор правила политик, созданного локально на UserGate NGFW, совпадает с идентификатором правила, созданного в шаблоне, то в конфигурацию параметров войдет правило из шаблона, а локальное правило будет удалено.

- При настройке шаблонов UserGate NGFW для узлов кластера конфигурации в свойствах параметров, которые не являются кластерными (например, в свойствах параметров агента UserID), вы можете указывать узел кластера, к которому будут применяться эти параметры.

## Создание группы шаблонов UserGate NGFW

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

Чтобы создать группу шаблонов UserGate NGFW:

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

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

   Вы также можете создавать и добавлять новые шаблоны по кнопке **Создать и добавить новый объект**.
4. Нажмите **Сохранить**.

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

## Настройка интеграции UserGate NGFW с UserGate MC

Настройка интеграции с UserGate MC осуществляется путем создания в управляемой области логического объекта — устройства, к которому будут привязаны реальные UserGate NGFW при их подключении к UserGate MC. Каждый такой логический объект во включенном состоянии использует одну лицензию на управляемое устройство.

С помощью одного устройства, созданного в управляемой области, вы можете настроить интеграцию с UserGate MC одиночного UserGate NGFW или кластера межсетевых экранов. Для UserGate NGFW, объединенных в кластер, достаточно подключить к UserGate MC первый узел, остальные узлы будут подключены автоматически при их добавлении в кластер.

Для настройки интеграции UserGate NGFW с UserGate MC необходимо:

1) создать устройство в управляемой области;

2) подключить UserGate NGFW к UserGate MC.

Все UserGate NGFW, для которых настроена интеграция с UserGate MC, называются управляемыми устройствами.

## Создание устройства в управляемой области

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

Чтобы создать устройство в управляемой области:

1. В разделе **Управление областью → NGFW → Устройства** нажмите **Добавить**.
2. На вкладке **Общие** укажите параметры устройства:
   - название и описание;
   - группу шаблонов, параметры которой должны применяться к подключенным UserGate NGFW;
   - режим синхронизации параметров между группой шаблонов и подключенными UserGate NGFW.
3. Если вы планируете настроить интеграцию UserGate NGFW с внешним сервером UserGate Log Analyzer, на вкладке **Адреса UserGate для связи с LogAn** укажите IP-адрес UserGate NGFW.
4. Нажмите **Сохранить**.
5. Выберите созданное устройство в списке и получите код для подключения UserGate NGFW, нажав **Действия → Показать уникальный код устройства**.
6. Сохраните код для подключения UserGate NGFW.

В интерфейсе UserGate MC вы можете просматривать список созданных устройств.

## Подключение UserGate NGFW к UserGate MC

Вы можете подключить UserGate NGFW к UserGate MC при первоначальной настройке межсетевого экрана по кнопке **Настроить через UserGate Management Center**, а также при его дальнейшем использовании (см. инструкцию ниже).

Перед подключением UserGate NGFW администратору центра управления UserGate MC необходимо:

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

**Примечание**Инструкция ниже выполняется в веб-консоли UserGate NGFW.

Чтобы подключить UserGate NGFW к UserGate MC:

1. В разделе **Настройки → Консоль администратора → Настройки** в блоке **Агент UserGate Management Center** нажмите **Настроить**.
2. Укажите IP-адрес UserGate MC (например, 192.0.2.4) и код для подключения UserGate NGFW, сгенерированный в веб-консоли UserGate MC.
3. Нажмите **Сохранить**.

   Статус подключения отобразится в блоке **Агент UserGate Management Center** в виде цветового индикатора:
   - Зеленый — соединение с сервером UserGate MC установлено, интеграция выполняется штатно.
   - Красный — соединение с сервером UserGate MC не установлено, межсетевой экран UserGate NGFW отключен или на нем остановлена работа агента **UserGate Management Center**.

   При успешном подключении конфигурация параметров группы шаблонов будет применена к UserGate NGFW. Параметры этой конфигурации (за исключением базовых параметров и параметров сетевых интерфейсов) будут недоступны для изменения на стороне UserGate NGFW.

   Кроме того, вы можете просматривать информацию о подключении UserGate NGFW в веб-консоли UserGate MC в разделе **Управление областью → NGFW → Устройства**. UserGate MC проверяет подключение к UserGate NGFW на портах TCP 2022 и 9712. Для каждого устройства в управляемой области отображаются статус и дата последнего подключения привязанных к нему UserGate NGFW, а также дополнительная информация, включая объем используемой памяти и время непрерывной работы межсетевых экранов.

В интерфейсе UserGate MC вы можете управлять подключенными UserGate NGFW.

## Просмотр списка устройств в управляемой области

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

- Включать и отключать устройства по кнопкам **Включить** и **Отключить** соответственно. При отключении устройства для всех привязанных к нему UserGate NGFW будут разорваны соединения с сервером UserGate MC.
- Удалять устройства по кнопке **Удалить**.
- Изменять параметры устройства по кнопке **Редактировать**.
- Просматривать информацию об устройстве в отдельном окне по кнопке **Показать детальную информацию**.

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

- **Все** — все устройства (фильтр по умолчанию).
- **Включенные** и **Выключенные** — устройства в выбранном состоянии.
- **Онлайн** — для привязанных к устройствам UserGate NGFW установлено соединение с сервером UserGate MC.
- **Офлайн** — для привязанных к устройствам UserGate NGFW не установлено соединение с сервером UserGate MC.
- **Не привязанные** — устройства, к которым не привязаны UserGate NGFW.
- **Консистентные устройства** — устройства, к которым привязаны UserGate NGFW с параметрами, синхронизированными с конфигурацией параметров группы шаблонов.
- **Неконсистентные устройства** — устройства, к которым привязаны UserGate NGFW с параметрами, не синхронизированными с конфигурацией параметров группы шаблонов.

Вы также можете управлять синхронизацией параметров между группой шаблонов и UserGate NGFW, для этого доступны ручной и автоматический режимы. Вручную вы можете запускать синхронизацию сразу для всех управляемых устройств (по кнопке **Действия → Запустить полную синхронизацию**) или только для выбранных (по кнопке **Запросить синхронизацию**).

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

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

## Управление подключенными UserGate NGFW

В разделе **Управление областью → NGFW → Устройства** вы можете управлять подключенными UserGate NGFW:

- Переходить в веб-консоль UserGate NGFW по кнопке **Открыть консоль**. Для UserGate NGFW, объединенных в кластер, по этой кнопке открывается окно выбора узла для перехода в веб-консоль этого узла.
- Перезагружать и выключать питание сервера одиночного UserGate NGFW или каждого из узлов кластера межсетевых экранов по ссылкам **Перезагрузить** и **Выключить** соответственно.
- Управлять лицензией UserGate NGFW: выполнять активацию лицензии по ссылке **Нет лицензии**, проверять срок ее действия по ссылке **Проверить лицензию**, а также обновлять лицензию по ссылке **Зарегистрированная версия**.
- Устанавливать обновление программного обеспечения (UGOS), загруженного локально на сервер одиночного UserGate NGFW или узла кластера межсетевых экранов, по ссылке **Установить обновление**.
- Изменять параметры UserGate NGFW посредством настройки параметров шаблонов, входящих в примененную конфигурацию.

## Кластеризация UserGate NGFW

Вы можете объединять два или более UserGate NGFW (узлов) в кластер конфигурации и настраивать на них единые параметры для работы с трафиком, используя шаблоны.

Между узлами кластера конфигурации выполняется синхронизация параметров, что обеспечивает бесперебойную фильтрацию и обработку сетевого трафика при недоступности одного из узлов.

Кроме того, вы можете объединять до четырех узлов кластера конфигурации в кластер отказоустойчивости. Этот кластер поддерживает следующие режимы работы:

- «активный — активный», в котором один из межсетевых экранов выполняет роль основного узла, распределяя трафик на все остальные узлы кластера;
- «активный — пассивный», в котором обработку транзитного трафика выполняет основной узел, при сбоях в работе этого узла трафик перенаправляется на резервные узлы кластера.

В параметрах кластера отказоустойчивости вы можете настроить синхронизацию сессий между узлами (исключение составляют сессии, использующие прокси-сервер). Это может понадобиться для кластера в режиме «активный — пассивный», например при недоступности основного узла вы можете переключиться на резервный узел без потери установленных сессий.

На базе одного кластера конфигурации может быть создано несколько кластеров отказоустойчивости. В этом случае каждому кластеру отказоустойчивости вы можете присвоить уникальный мультикаст-идентификатор, который будет использоваться для синхронизации сессий между узлами.

## Создание кластера конфигурации

Для создания кластера конфигурации необходимо:

1) настроить первый узел кластера конфигурации;

2) подключить первый узел кластера конфигурации к UserGate MC;

3) добавить дополнительные узлы в кластер конфигурации.

**Примечание**Инструкция ниже выполняется в интерфейсе UserGate NGFW.

Чтобы настроить первый узел кластера конфигурации:

1. Выполните первоначальную настройку UserGate NGFW, который будет выполнять роль первого узла кластера, согласно инструкции раздела « Подключение к UserGate NGFW » Руководства администратора UserGate NGFW.

2. Настройте зону, через интерфейсы которой будет выполняться репликация параметров между узлами кластера.

   Для этого в разделе **Настройки → Сеть → Зоны** создайте новую зону или используйте зону **Cluster**, созданную по умолчанию. В параметрах зоны в блоке **Контроль доступа** разрешите сервисы **Консоль администрирования** и **Кластер**.

   **Важно!**Не используйте для репликации параметров зоны, интерфейсы которых подключены к недоверенным сетям, например к интернету.

3. Укажите IP-адрес первого узла для подключения к другим узлам кластера.

   Для этого в разделе **Настройки → Консоль администратора → Управление устройством** в блоке параметров **Кластер конфигурации** выберите первый узел кластера, нажмите **Редактировать** и укажите IP-адрес интерфейса, входящего в зону, настроенную на шаге 2.

4. В блоке **Кластер конфигурации** нажмите **Сгенерировать секретный код** и сохраните полученный код. Этот код потребуется для подключения второго и последующих узлов к кластеру.

После настройки первого узла необходимо подключить его к UserGate MC. В результате подключения узлу будет автоматически присвоен идентификатор node_1. Теперь вы можете добавить в кластер конфигурации дополнительные узлы.

**Примечание**Инструкция ниже выполняется при первоначальной настройке UserGate NGFW.

Чтобы добавить дополнительный узел в кластер конфигурации:

1. Подключитесь к веб-интерфейсу UserGate NGFW, который будет выполнять роль дополнительного узла кластера.

2. Следуйте указаниям мастера первоначальной настройки:

   - выберите язык веб-консоли;
   - выберите часовой пояс;
   - ознакомьтесь с условиями лицензионного соглашения.

3. В окне с вариантами использования узла выберите **Дополнительный узел кластера**.

4. В окне настройки узла укажите параметры подключения к кластеру:

   - Название, IP-адрес и маску подсети сетевого интерфейса, который будет использоваться для подключения.
   - Если первый и дополнительный узлы кластера находятся в разных подсетях, укажите IP-адрес шлюза, через который будет доступен первый узел кластера.
   - IP-адрес первого узла кластера.
   - Код для подключения, полученный при настройке первого узла кластера.

5. Нажмите **Подключить**.

6. При успешном подключении мастер первоначальной настройки предложит ввести идентификатор узла кластера. Укажите этот идентификатор в формате node_<номер узла кластера>, например node_2.

   Дополнительный узел добавлен в кластер конфигурации. На этот узел будут автоматически реплицированы параметры, настроенные на первом узле. В интерфейсе UserGate MC дополнительный узел кластера отобразится в разделе **Управление областью → NGFW → Устройства** в строке управляемого устройства, к которому ранее был подключен первый узел кластера конфигурации.

При необходимости вы можете добавить другие дополнительные узлы, повторив шаги инструкции для каждого из них.

## Создание кластера отказоустойчивости

Перед созданием кластера отказоустойчивости:

1. Создайте кластер конфигурации (см. инструкцию выше).

2. Проверьте, что:

- Выполняются требования аналогичные тем, что предъявляются к узлам при создании кластера отказоустойчивости без использования UserGate MC (подробнее — в руководстве администратора UserGate NGFW в разделе «Кластеризация и отказоустойчивость» или для версии 7.5.0 и выше в разделе « Кластеризация и отказоустойчивость (версия 7.5.0 и выше)»).
- На каждом из узлов кластера конфигурации созданы сетевые интерфейсы, управляемые UserGate MC. Вы можете назначать виртуальные IP-адреса только тем интерфейсам, которые созданы в шаблоне.

2. В UserGate MC под учетной записью администратора управляемой области выполните следующее:

- В разделе **Управление областью → NGFW → Устройства** проверьте, что все узлы кластера конфигурации доступны.
- Создайте шаблон сетевых зон и шаблон кластера отказоустойчивости.
- В шаблоне сетевых зон в разделе **Настройки → Сеть → Зоны** разрешите доступ к сервису **VRRP** тем зонам, для которых планируете добавлять кластерный виртуальный IP-адрес (подробнее — в разделе «Настройка зон» Руководства администратора UserGate NGFW).

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

## Создание кластера отказоустойчивости версии ниже 7.5.0

Чтобы создать кластер отказоустойчивости:

1. В шаблоне кластера отказоустойчивости в разделе **Консоль администратора → Управление устройством** в блоке параметров **Кластер отказоустойчивости** нажмите **Добавить**.

2. На вкладке **Общие** выполните следующие действия:

- Включите кластер.
- Укажите название и при необходимости описание кластера.
- Выберите режим работы отказоустойчивого кластера:
  - **Актив-Актив** — распределение нагрузки между узлами кластера;
  - **Актив-Пассив** — переключение нагрузки на резервные узлы в случае недоступности основного узла.
- Если между узлами кластера требуется выполнять синхронизацию пользовательских TCP-сессий, установите флажок **Синхронизировать сессии**.

  Если в локальной сети присутствуют другие отказоустойчивые кластеры, вы можете указать уникальный мультикаст-идентификатор создаваемого кластера, который будет использоваться для синхронизации сессий между узлами.

  **Важно!**Синхронизация сессий между узлами создает существенную нагрузку на кластер.

  На вкладке **Синхронизация UDP/ICMP** вы можете управлять режимом синхронизации пользовательских сессий:

  - Если между узлами кластера требуется выполнять синхронизацию всех пользовательских сессий, включая UDP- и ICMP-трафик, установите флажок **Синхронизовать все сессии**.
  - Если из синхронизации требуется исключить определенные пользовательские сессии, укажите IP-адреса, к которым привязаны эти сессии.
- При необходимости укажите уникальный идентификатор виртуального маршрутизатора (VRID).

  Если в локальной сети отсутствуют сторонние VRRP-кластеры, рекомендуется оставить значение по умолчанию.

3. На вкладке **Узлы** укажите идентификаторы тех узлов кластера конфигурации, которые требуется объединить в кластер отказоустойчивости.

4. На вкладке **Виртуальные IP** назначьте виртуальные IP-адреса интерфейсам на узлах кластера отказоустойчивости. Вы можете назначать виртуальные IP-адреса только тем интерфейсам, которые созданы в шаблонах.

5. Нажмите **Сохранить**.

Созданный кластер отобразится в блоке параметров **Кластер отказоустойчивости**. Вы можете просматривать данные о состоянии кластера отказоустойчивости в разделе **Управление областью → NGFW → Устройства** в строке управляемого устройства, к которому подключены узлы этого кластера.

Если для авторизации пользователей в локальной сети планируется использовать captive-портал, после создания кластера отказоустойчивости в одном из шаблонов UserGate NGFW в разделе **Консоль администратора → Настройки** в блоке параметров **Модули** для служебных доменных имен (например, auth.captive и logout.captive) укажите IP-адрес, назначенный в качестве кластерного виртуального адреса (подробнее — в разделе «Настройка общих параметров» Руководства администратора UserGate NGFW).

## Создание кластера отказоустойчивости версии 7.5.0 и выше

Настройка кластера отказоустойчивости выполняется в разделе **NGFW → Консоль администратора → Кластеры отказоустойчивости** в соответствии с инструкциями из раздела « Кластеризация и отказоустойчивость (версия 7.5.0 и выше)» руководства администратора UserGate NGFW и с учетом следующих особенностей настройки кластера в UserGate MC:

- При настройке кластере отказоустойчивости в UserGate MC используются не имена конкретных узлов, а системные имена ( node_1, node_2, node_3 и т. д.). UserGate MC автоматически связывает эти имена с узлами в настроенном кластере конфигурации.
- В разделе **Настройки → Сеть → Интерфейсы** необходимо добавить интерфейсы для каждого узла, который будет добавлен в кластер отказоустойчивости, и назначить этим интерфейсам и назначить им зоны с соответствующими разрешенными сервисами (например, для обмена VRRP-объявления или синхронизации сессий).
- При добавлении узлов на вкладке **Узлы** в блоке **Доступные узлы** следует выбрать от двух до четырех узлов из списка системных имен, для которых ранее были добавлены интерфейсы.
- При настройке режима **Мультикаст** интерфейсы не назначаются автоматически, их необходимо выбрать.

**Примечание**Статусы кластера и узлов недоступны в разделе «NGFW» ➔ «Консоль администратора» ➔ «Кластеры отказоустойчивости». Вы можете посмотреть состояния кластера и узлов в разделе «Управление областью» ➔ «NGFW» ➔ «Устройства».

## Обновление UserGate NGFW

UserGate MC получает файлы обновлений программного обеспечения (UGOS) и системных библиотек из репозитория UserGate в рамках лицензии на модуль Security Update . При этом все UserGate NGFW, подключенные к управляемым устройствам, используют в качестве источника обновлений сервер UserGate MC.

В интерфейсе UserGate MC вы можете управлять обновлением UGOS:

- проверять наличие файлов обновлений в репозитории UserGate;
- загружать файлы обновлений из репозитория;
- изменять параметры обновления управляемых устройств;
- загружать файлы обновлений, полученные в личном кабинете my.usergate.com, в офлайн-режиме при отсутствии доступа к репозиторию UserGate.

Также вы можете управлять обновлением системных библиотек:

- управлять автоматическим обновлением библиотек на сервере UserGate MC;
- настраивать расписание автоматического обновления;
- загружать файлы обновлений, полученные в личном кабинете my.usergate.com, в офлайн-режиме при отсутствии доступа к репозиторию UserGate.

## Управление обновлением UGOS

Вы можете загружать файлы обновлений UGOS на сервер UserGate MC напрямую из репозитория UserGate или в офлайн-режиме.

**Примечание**Инструкции ниже выполняются администратором управляемой области в веб-консоли UserGate MC.

Чтобы загрузить файл обновления UGOS из репозитория UserGate:

1. В разделе **Управление областью → NGFW → Обновления ПО** нажмите **Выбрать онлайн-обновления**.

Начнется проверка наличия обновлений UGOS в репозитории UserGate. По окончании проверки будет сформирован список доступных файлов обновлений.

2. Укажите файл обновления в списке и нажмите **Выбрать**.

Обновление отобразится в таблице **Обновление ПО**. Вы можете отслеживать статус и прогресс его загрузки в соответствующих столбцах.

Чтобы загрузить файл обновления UGOS в офлайн-режиме:

1. В разделе **Управление областью → NGFW → Обновления ПО** нажмите **Импортировать обновление**.
2. По кнопке **Обзор** выберите файл обновления.

   Начнется загрузка файла обновления. По окончании процесса в окне загрузки отобразятся название и версия обновления UGOS.
3. При необходимости в поле **Совместимость** укажите версию UGOS, совместимую с загруженным обновлением.
4. Нажмите **Сохранить**.

   Обновление отобразится в таблице **Обновление ПО**.

После загрузки вам необходимо утвердить нужные обновления, чтобы они стали доступны для установки на подключенных UserGate NGFW. Для этого выберите обновление в таблице и нажмите **Утвердить обновление**. Действие также доступно при изменении параметров обновления. Кроме того, вы можете удалять обновления в таблице по кнопке **Удалить обновление**.

Чтобы изменить параметры обновления UGOS:

1. В разделе **Управление областью → NGFW → Обновления ПО** нажмите ссылку в столбце **Название** для обновления.
2. Если необходимо, на вкладке **Общие**:
   - измените описание обновления;
   - утвердите обновление с помощью флажка **Утвердить обновление**.
3. Если необходимо, на вкладке **Устройства** по кнопке **Добавить** добавьте управляемые устройства, которым будет доступно обновление.
4. Нажмите **Сохранить**.

Администраторы UserGate NGFW могут вручную устанавливать загруженные и утвержденные обновления UGOS локально на устройствах.

## Управление обновлением библиотек

По умолчанию системные библиотеки на сервере UserGate MC обновляются автоматически. В разделе **Управление областью → NGFW → Обновления библиотек** администраторы управляемой области UserGate MC могут отключить автоматическое обновление выбранной библиотеки по кнопке **Не обновлять**, а также включить его обратно по кнопке **Обновлять автоматически**. Кроме того, по кнопке **Импортировать обновление** доступна загрузка файла обновления библиотек на сервер UserGate MC в офлайн-режиме.

Системные библиотеки, находящиеся в репозитории UserGate MC, доступны всем UserGate NGFW, подключенным в качестве управляемых устройств. Эти библиотеки обновляются на UserGate NGFW автоматически по расписанию. Вы можете настраивать расписание автоматического обновления на каждом UserGate NGFW локально (подробнее — в разделе «Настройка общих параметров» Руководства администратора UserGate NGFW) или с помощью шаблонов устройств на UserGate MC. Ниже приведена инструкция по настройке расписания в шаблоне, которая выполняется администратором управляемой области в веб-консоли UserGate MC.

Чтобы настроить расписание автоматического обновления системных библиотек:

1. В одном из шаблонов UserGate NGFW в разделе **Консоль администратора → Настройки → Обновления библиотек** для параметра **Расписание автоматических обновлений** нажмите **Настроить**.
2. Выберите библиотеку в списке и укажите для нее вариант расписания.

   При выборе варианта **Задать вручную** вы можете указать время в cron-формате: <минуты: 0-59> <часы: 0-23> <дни месяца: 1-31> <месяцы: 1-12> <дни недели: 0-6, где 0 — воскресенье>.

   Для ручного ввода вы можете использовать следующие символы:
   - Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что резервное копирование должно выполняться каждый час.
   - Дефис (-) — для указания диапазона значений.
   - Запятая (,) — в качестве разделителя значений.
   - Косая черта (/) — для указания шага между значениями.

   При установке флажка **Единое расписание для всех обновлений** расписание выбранной библиотеки будет применено ко всем библиотекам в списке.
3. Нажмите **Сохранить**.

## Аварийное отключение UserGate NGFW от UserGate MC

При настроенной интеграции вы можете отключить UserGate NGFW от UserGate MC с помощью команды аварийного отключения. Эта команда выполняется в интерфейсе командной строки UserGate NGFW в режиме конфигурации (подробнее — в разделе «Режим конфигурации» руководства администратора NGFW):

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

В качестве значения аргумента (arg) вы можете указать следующие параметры:

- keep — при отключении все импортированные из UserGate MC объекты (например, библиотеки и правила политик) будут сохранены локально в UserGate NGFW.
- delete — при отключении все импортированные из UserGate MC объекты (например, библиотеки и правила политик) будут удалены. Исключение составляют объекты, используемые в настоящий момент, они будут сохранены локально в UserGate NGFW.

Например:

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

**Примечание**В версии 7.4.0 и выше при отключении UserGate NGFW от UserGate MC с аргументом keep у всех объектов NGFW, ранее импортированных из UserGate MC, в названии будет удален префикс [MC]. Если при удалении префикса может возникнуть дубликат названия другого существующего объекта, префикс не удаляется.

**Практика работы с шаблонами в UserGate MC**

Product: UGMC
Version: 7.x

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 C необходимо делегировать права в шаблоне C3:

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.

**Перенос объектов между шаблонами**

Product: UGMC
Version: 7.x

Объекты одного типа (правила или списки) могут быть перенесены из одного шаблона NGFW в другой (доступно в версии 7.4.0 и выше).

## Работа со списками

При копировании или переносе списков копируется все их содержимое.

Если в списках есть вложенные списки (например, списки IP-адресов или списки URL), переносятся ссылки на такие вложенные списки.

Если в целевом шаблоне нет списков IP-адресов, которые передаются в него ссылками, такие списки в целевом шаблоне будут помечены, как отсутствующий объект.

Если в целевом шаблоне нет списков URL, которые передаются в него ссылками, такие списки не будут перенесены в целевой шаблон.

Чтобы выполнить операцию копирования или переноса списков между шаблонами необходимо в исходном шаблоне, в панели инструментов раздела списка, нажать **Перенести объекты** и выбрать нужное действие.

Пример работы со списками IP-адресов:



Доступны операции копирования или перемещения как отдельных выбранных объектов (списков), так и всех объектов раздела целиком.

При копировании или перемещении выбранных объектов раздела в другой шаблон выводится диалоговое окно, в заголовке которого указана выполняемая операция и количество копируемых или перемещаемых объектов.

В поле **Шаблон** необходимо выбрать шаблон назначения и нажать кнопку действия ( **Копировать** или **Переместить** в зависимости от выбранной операции):





При копировании выбранные списки скопируются в шаблон назначения с теми же названиями, при перемещении — будут скопированы в шаблон назначения с теми же названиями и удалены из текущего шаблона.

При копировании или перемещении всех объектов раздела в другой шаблон выводится диалоговое окно, в заголовке которого указана выполняемая операция и количество копируемых или перемещаемых объектов.

В поле **Шаблон** необходимо выбрать шаблон назначения и нажать кнопку действия ( **Копировать** или **Переместить** в зависимости от выбранной операции):





При копировании все списки текущего раздела будут скопированы в шаблон назначения с теми же названиями, при перемещении — все списки текущего раздела будут скопированы в шаблон назначения с теми же названиями и удалены из текущего шаблона.

Если в шаблоне назначения уже есть объекты с такими же названиями, возникает конфликт имен. Выводится окно с указанием количества ошибок и списка пересекающихся имен (выводится не более 10 имен), операция копирования/перемещения полностью отменяется для всех объектов:



Для разрешения конфликта имен администратор должен вручную переименовать объекты с аналогичными именами и выполнить операцию копирования/перемещения заново.

## Работа с правилами

Правила являются упорядоченными объектами и для них можно указать раздел (пре- или пост-правила) и место вставки (начало, конец раздела и т. д.).

При копировании или переносе правил переносится основная запись правила со ссылками на все вложенные объекты.

Чтобы выполнить операцию копирования или переноса правил между шаблонами необходимо в исходном шаблоне, в панели инструментов раздела правил, нажать **Перенести объекты** и выбрать нужное действие.

Пример работы с правилами межсетевого экрана:



Доступны операции копирования или перемещения как отдельных выбранных объектов (правил), так и всех объектов раздела целиком.

При копировании или перемещении выбранных объектов раздела (правил) в другой шаблон выводится диалоговое окно, в заголовке которого указана выполняемая операция и количество копируемых/перемещаемых объектов.

В поле **Шаблон** необходимо выбрать шаблон назначения.

В поле **Раздел** необходимо выбрать секцию, в которую будет скопировано правило (пре-правила или пост-правила).

В области **Вставить** необходимо выбрать место в разделе, куда будут скопированы правила (начало или конец раздела, или перед конкретным объектом в списке имеющихся в разделе целевого шаблона правил).

Флаг **Открыть целевой шаблон после копирования** откроет настройки целевого шаблона после выполнения операции.

Далее необходимо нажать кнопку действия (**Копировать** или **Переместить** в зависимости от выбранной операции):





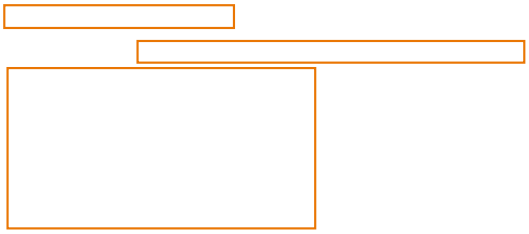
При копировании выбранные правила будут скопированы в шаблон назначения в указанные места с теми же названиями, при перемещении — выбранные правила будут скопированы в шаблон назначения с теми же названиями и удалены из текущего шаблона.

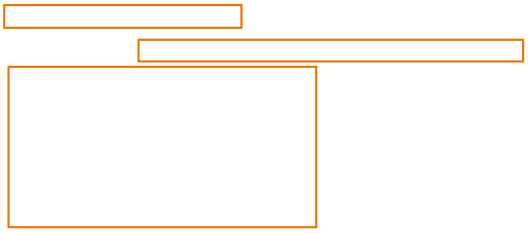
При копировании или перемещении всех объектов раздела (правил) в другой шаблон выводится диалоговое окно, в заголовке которого указана выполняемая операция и количество копируемых/перемещаемых объектов.

В поле **Шаблон** необходимо выбрать шаблон назначения.

Указать место размещения правил в соответствующих секциях раздела (пре- и пост-правила).

Далее необходимо нажать кнопку действия (**Копировать** или **Переместить** в зависимости от выбранной операции):





При копировании все правила текущего раздела будут скопированы в указанные места шаблона назначения с теми же названиями, при перемещении — все правила текущего раздела будут скопированы в указанные места шаблона назначения с теми же названиями и удалены из текущего шаблона.

Если в шаблоне назначения уже есть объекты (правила) с такими же названиями, возникает конфликт имен. Выводится окно с указанием количества ошибок и списка пересекающихся имен (выводится не более 10 имен) и операция копирования или переноса полностью отменяется для всех объектов:



Для разрешения конфликта имен администратор должен вручную переименовать объекты с аналогичными именами и выполнить операцию копирования/перемещения заново.

## Пример использования

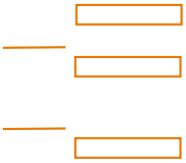
Правила межсетевого экрана в шаблоне Template 3 (правила на иллюстрациях созданы исключительно для демонстрации функции переноса объектов):



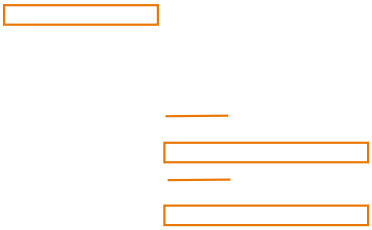
Правила межсетевого экрана в шаблоне Template 1 и выбор операции копирования всех правил из шаблона Template 1 в шаблон Template 3:



Настройка операции копирования:



Результат копирования правил межсетевого экрана в шаблоне Template 3:



**Копирование правил в шаблонах управляемых устройств (версия 7.6.0 и выше)**

---

Product: UserGate MC
Version: 7.x, 7.6.x

Если при настройке правил в шаблонах управляемых устройств UserGate NGFW, UserGate DCWF, а также в шаблонах конечных устройств нужно создать несколько похожих правил, можно воспользоваться функцией копирования.

Чтобы копировать правило:

1. В веб-консоли управляемой области выберите **NGFW**, **DCFW** или **Конечные устройства** и перейдите в нужный раздел создания правил, например **Политики сети → Межсетевой экран**.

2. Найдите или настройте правило, которое нужно скопировать. Инструкции по настройке правил для UserGate NGFW и UserGate DCFW приведены в соответствующих руководствах администратора, для конечных устройств — в разделе «Настройка параметров шаблонов конечных устройств» этого руководства.

3. В меню действий нажмите **Копировать** и выберите способ создания копии:

- **С редактированием** — создается копия правила и открывается окно свойств правила для внесения изменений. Здесь можно указать, где разместить копию: в начале или в конце списка правил.
- **Выше** — копия правила размещается строкой выше оригинала. Для изменения свойств нажмите **Редактировать**.
- **Ниже** — копия правила размещается строкой ниже оригинала. Для изменения свойств правила нажмите **Редактировать**.

**Настройка прокси-сервера**

---

Product: UGMC
Version: 7.x

Вы можете настроить в веб-интерфейсе UGMC такие параметры прокси-сервера, как добавление заголовков HTTP, тайм-ауты на подключение к сайтам и загрузку контента, защита исполняемого кода продукта и другие.

Чтобы настроить прокси-сервер:

1. В веб-интерфейсе администратора области в разделе **NGFW-конфигурация → UserGate → Настройки** в области **Расширенные настройки** нажмите **Настроить**.
2. В окне **Настройки прокси-сервера** настройте нужные параметры (см. таблицу ниже).
3. Сохраните изменения.

Ниже описаны настраиваемые параметры прокси-сервера.

| Параметр | Описание |
|---|---|
| Флажок **Синхронизировать** | Если установлен, параметры прокси-сервера будут применены на всех устройствах UserGate NGFW в этой области |
| **Телеметрия** | Если включено, устройство отправляет разработчику анонимную статистику, такую как популярность веб-сайтов, веб-сайты с неизвестной категорией, вирусные атаки, события СОВ, активность вредоносного ПО. Данные телеметрии обезличены и не содержат персональной информации. По умолчанию выключена |
| **Контроль изменения кода** | Настройка защиты исполняемого кода продукта от потенциального несанкционированного изменения. Проверка целостности исполняемого кода происходит каждый раз после загрузки UserGate.<br>Можно выбрать одно из следующих значений:<br>• **Log** — активирует режим отслеживания несанкционированных изменений исполняемого кода. При обнаружении изменений UserGate записывает информацию о факте изменения в журнал событий.<br>• **Block** — активирует режим отслеживания несанкционированных изменений исполняемого кода. При обнаружении изменений UserGate записывает информацию о факте изменения в журнал событий и создает блокирующее правило межсетевого экрана, запрещающее любой транзитный трафик через UserGate. Для возможности отключения созданного правила межсетевого экрана необходимо отключить отслеживание несанкционированных изменений.<br>• **Off** — отключает отслеживание несанкционированных изменений исполняемого кода |
| **Контроль изменения настроек** | Настройка защиты конфигурации продукта от изменения. Функция позволяет «заморозить» параметры после настройки продукта в соответствии с требованиями организации. Любое изменение параметров через веб-интерфейс, CLI или другими способами будет приводить к журналированию и/или блокировке транзитного трафика в зависимости от выбранного режима. Проверка целостности конфигурации происходит каждые несколько минут после загрузки UserGate.<br>Можно выбрать одно из следующих значений:<br>• **Log** — активирует режим отслеживания изменений конфигурации. При обнаружении изменений UserGate записывает информацию о факте изменения в журнал событий.<br>• **Block** — активирует режим отслеживания изменений конфигурации. При обнаружении изменений UserGate записывает информацию о факте изменения в журнал событий и создает блокирующее правило межсетевого экрана, запрещающее любой транзитный трафик через UserGate.<br>• **Off** — отключает отслеживание изменений конфигурации |
| **Пароль контроля изменения настроек** | Если указан, изменение режима отслеживания конфигурации продукта возможно только после ввода этого пароля |
| **Добавлять HTTP-заголовок Via** | Если включено, прокси-сервер добавляет в запросы и ответы заголовок Via |
| **Добавлять HTTP-заголовок Forwarded** | Если включено, прокси-сервер добавляет в запросы заголовок Forwarded |
| **Добавлять HTTP-заголовок X-Forwarded-For** | Если включено, прокси-сервер добавляет в запросы заголовок X-Forwarded-For |
| **Включить режим прокси fast-mode** | Включает режим ускорения загрузки контента. Режим может быть несовместим с работой некоторых сайтов. По умолчанию выключено |
| **Включить SYN-прокси** | Включает механизм защиты от DDoS-атак, основанных на SYN-флуде. По умолчанию выключено |
| **Настройка модуля L7** | Включает загрузку модуля L7. По умолчанию модуль загружен.<br>**Важно!** После изменения данного параметра требуется перезагрузка устройства UserGate |
| **Разрешить HTTP proxy 1.1 без указания host** | В режиме **Relaxed** разрешает принимать запросы HTTP/1.1 без заголовка host. Данный режим противоречит RFC, но необходим для совместимости с некоторыми программами. По умолчанию установлено значение **Strict** (соблюдающее RFC) |
| **Время ожидания соединения HTTP (сек)** | Время, выделяемое на установление HTTP-соединения. По умолчанию — 20 секунд |
| **Время ожидания загрузки HTTP (сек)** | Время, выделяемое на загрузку контента по HTTP-протоколу. По умолчанию — 60 секунд |
| **Время ожидания сервера ICAP (сек)** | Время, в течение которого сервер UserGate ждет ответа от ICAP-сервера. Если по истечении этого времени ответ ICAP-сервера не был получен, UserGate NGFW либо отправит данные пользователю, не изменяя их (если для сработавшего ICAP-правила выбрано действие **Переслать и игнорировать**), либо данные не будут переданы пользователю (если для сработавшего ICAP-правила выбрано действие **Переслать**). Значение по умолчанию — 10 секунд |

**Управление устройствами UserGate DCFW**

**Управление устройствами UserGate DCFW (Описание)**

Product: UGMC
Version: 7.x

Начиная с версии 7.4.0 в веб-консоли UserGate Management Center (далее также — UserGate MC) администраторы управляемой области могут централизованно управлять подключенными UserGate DCFW, а также настраивать параметры этих устройств. Для этого необходимо выполнить следующее:

1) создать шаблоны UserGate DCFW;

2) настроить параметры шаблонов UserGate DCFW;

3) создать группу шаблонов UserGate DCFW;

4) настроить интеграцию UserGate DCFW с UserGate MC.

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

## Создание шаблонов UserGate DCFW

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

Чтобы создать шаблон UserGate DCFW:

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

   **Примечание**Выбор разделов доступен начиная с версии 7.6.0.
4. Нажмите **Сохранить**.

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

## Настройка параметров шаблонов UserGate DCFW

Чтобы настроить параметры шаблона UserGate DCFW:

В разделе **DCFW** для объекта **Шаблон** в выпадающем списке выберите шаблон, параметры которого необходимо настроить.

Настройка параметров шаблона выполняется в разделах боковой панели аналогично настройке параметров локального UserGate DCFW (подробнее — в Руководстве администратора UserGate DCFW).

При настройке параметров шаблона UserGate DCFW следует учитывать следующее:

- Значения параметров в шаблоне имеют более высокий приоритет, чем указанные администратором UserGate DCFW локально. Если значение параметра не указано ни в шаблоне, ни на стороне UserGate DCFW, будет использоваться значение по умолчанию.
- После применения параметров шаблона к управляемым устройствам администраторы могут изменять базовые параметры и параметры сетевых интерфейсов локально на каждом UserGate DCFW. Подробная информация об этих параметрах приведена в разделах «Настройка общих параметров» и «Настройка интерфейсов» Руководства администратора UserGate DCFW.
- При настройке параметров сетевых интерфейсов в шаблоне невозможно конфигурировать интерфейс port0. Первым физическим интерфейсом, доступным для настройки в шаблоне, будет port1.

  Параметры интерфейса port0 настраиваются администратором UserGate DCFW при первоначальной настройке устройства. По умолчанию этот интерфейс используется для подключения UserGate DCFW к UserGate MC.

  При необходимости можно сконфигурировать сетевые интерфейсы локально на UserGate DCFW, для этого в параметрах выбранного интерфейса шаблона должен быть установлен флажок **Настраивается на устройстве**.

  Если вы создаете интерфейс в шаблоне, этот интерфейс автоматически будет добавлен в UserGate DCFW. Удаление интерфейса из шаблона не удаляет интерфейс на межсетевом экране. Если требуется удалить интерфейс на межсетевом экране, необходимо сделать это вручную.
- Правила политик в шаблоне не переопределяют правила, созданные администраторами межсетевых экранов UserGate DCFW локально, а добавляются к ним в виде преправил и постправил.
- Для некоторых правил политик в шаблоне можно указать управляемые устройства, к которым будут применяться эти правила. Действие доступно в окне свойств правила на вкладке **Устройства**.

  Следует учитывать, что частое использование этой функции может усложнить для администраторов понимание того, какие правила политик будут применяться к устройству.
- Библиотеки элементов шаблона (например, библиотеки IP-адресов, URL-списков, а также типов контента) по умолчанию не содержат данных, в отличие от библиотек UserGate DCFW (подробнее — в разделе «Библиотеки элементов» Руководства администратора UserGate DCFW). Перед настройкой параметров шаблона следует добавить необходимые элементы библиотек.

  **Важно!**Данные библиотек не синхронизируются: если добавленные элементы не используются в параметрах шаблона, они не будут добавлены в библиотеки UserGate DCFW. Поэтому, чтобы на управляемых устройствах отображались, например, списки IP-адресов, созданные в шаблоне, необходимо использовать эти списки при настройке параметров шаблона.
  **Примечание**Корректность работы проприетарных сигнатур СОВ и приложений зависит от актуальности библиотек для этих сигнатур — рекомендуется проверять актуальность библиотек после обновления UserGate MC или восстановления его параметров. Если по какой-либо причине библиотеки не обновились автоматически, их можно обновить вручную. Действие выполняется администратором UserGate MC в разделе «Центр управления» → «Настройки» → «Обновления библиотек».
- При настройке шаблонов UserGate DCFW для узлов кластера конфигурации в свойствах параметров, которые не являются кластерными (например, в свойствах параметров агента UserID), вы можете указывать узел кластера, к которому будут применяться эти параметры.

## Создание группы шаблонов UserGate DCFW

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

Чтобы создать группу шаблонов UserGate DCFW:

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

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

   Вы также можете создавать и добавлять новые шаблоны по кнопке **Создать и добавить новый объект**.
4. Нажмите **Сохранить**.

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

## Настройка интеграции UserGate DCFW с UserGate MC

Настройка интеграции с UserGate MC осуществляется путем создания в управляемой области логического объекта — устройства, к которому будут привязаны реальные UserGate DCFW при их подключении к UserGate MC. Каждый такой логический объект во включенном состоянии использует одну лицензию на управляемое устройство.

С помощью одного устройства, созданного в управляемой области, вы можете настроить интеграцию с UserGate MC одиночного UserGate DCFW или кластера межсетевых экранов. Для UserGate DCFW, объединенных в кластер, достаточно подключить к UserGate MC первый узел, остальные узлы будут подключены автоматически при их добавлении в кластер.

Для настройки интеграции UserGate DCFW с UserGate MC необходимо:

1) создать устройство в управляемой области;

2) подключить UserGate DCFW к UserGate MC.

Все UserGate DCFW, для которых настроена интеграция с UserGate MC, называются управляемыми устройствами.

## Создание устройства в управляемой области

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

Чтобы создать устройство в управляемой области:

1. В разделе **Управление областью → DCFW → Устройства** нажмите **Добавить**.
2. На вкладке **Общие** укажите параметры устройства:
   - название и при необходимости описание;
   - группу шаблонов, параметры которой должны применяться к подключенным UserGate DCFW;
   - режим синхронизации параметров между группой шаблонов и подключенными UserGate DCFW.
3. Если вы планируете настроить интеграцию UserGate DCFW с внешним сервером UserGate Log Analyzer, на вкладке **Адреса UserGate для связи с LogAn** укажите IP-адрес UserGate DCFW.
4. Нажмите **Сохранить**.
5. Выберите созданное устройство в списке и получите код для подключения UserGate DCFW, нажав **Действия → Показать уникальный код устройства**.
6. Сохраните код для подключения UserGate DCFW.

В интерфейсе UserGate MC вы можете просматривать список созданных устройств.

## Подключение UserGate DCFW к UserGate MC

Вы можете подключить UserGate DCFW к UserGate MC при первоначальной настройке межсетевого экрана по кнопке **Настроить через UserGate Management Center**, а также при его дальнейшем использовании (см. инструкцию ниже).

Перед подключением UserGate DCFW администратору центра управления UserGate MC необходимо:

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

**Примечание**Инструкция ниже выполняется в веб-консоли UserGate DCFW.

Чтобы подключить UserGate DCFW к UserGate MC:

1. В разделе **Настройки → Консоль администратора → Настройки** в блоке **Агент UserGate Management Center** нажмите **Настроить**.
2. Укажите IP-адрес UserGate MC (например, 192.0.2.4) и код для подключения UserGate DCFW, сгенерированный в веб-консоли UserGate MC.
3. Нажмите **Сохранить**.

   Статус подключения отобразится в блоке **Агент UserGate Management Center** в виде цветового индикатора:
   - Зеленый — соединение с сервером UserGate MC установлено, интеграция выполняется штатно.
   - Красный — соединение с сервером UserGate MC не установлено, межсетевой экран UserGate DCFW отключен или на нем остановлена работа агента **UserGate Management Center**.

   При успешном подключении конфигурация параметров группы шаблонов будет применена к UserGate DCFW. Параметры этой конфигурации (за исключением базовых параметров и параметров сетевых интерфейсов) будут недоступны для изменения на стороне UserGate DCFW.

   Кроме того, вы можете просматривать информацию о подключении UserGate DCFW в веб-консоли UserGate MC в разделе **Управление областью → DCFW → Устройства**. UserGate MC проверяет подключение к UserGate DCFW на портах TCP 2022 и 9712. Для каждого устройства в управляемой области отображаются статус и дата последнего подключения привязанных к нему UserGate DCFW, а также дополнительная информация, включая объем используемой памяти и время непрерывной работы межсетевых экранов.

   В интерфейсе UserGate MC вы можете управлять подключенными UserGate DCFW.

## Просмотр списка устройств в управляемой области

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

- Включать и отключать устройства по кнопкам **Включить** и **Отключить** соответственно. При отключении устройства для всех привязанных к нему UserGate DCFW будут разорваны соединения с сервером UserGate MC.
- Удалять устройства по кнопке **Удалить**.
- Изменять параметры устройства по кнопке **Редактировать**.
- Просматривать информацию об устройстве в отдельном окне по кнопке **Показать детальную информацию**.

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

- **Все** — все устройства (фильтр по умолчанию).
- **Включенные** и **Выключенные** — устройства в выбранном состоянии.
- **Онлайн** — для привязанных к устройствам UserGate DCFW установлено соединение с сервером UserGate MC.
- **Офлайн** — для привязанных к устройствам UserGate DCFW не установлено соединение с сервером UserGate MC.
- **Не привязанные** — устройства, к которым не привязаны UserGate DCFW.
- **Консистентные устройства** — устройства, к которым привязаны UserGate DCFW с параметрами, синхронизированными с конфигурацией параметров группы шаблонов.
- **Неконсистентные устройства** — устройства, к которым привязаны UserGate DCFW с параметрами, не синхронизированными с конфигурацией параметров группы шаблонов.

Вы также можете управлять синхронизацией параметров между группой шаблонов и UserGate DCFW, для этого доступны ручной и автоматический режимы. Вручную вы можете запускать синхронизацию сразу для всех управляемых устройств (по кнопке **Действия → Запустить полную синхронизацию**) или только для выбранных (по кнопке **Запросить синхронизацию**).

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

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

## Управление подключенными UserGate DCFW

В разделе **Управление областью → DCFW → Устройства** вы можете управлять подключенными UserGate DCFW:

- Переходить в веб-консоли UserGate DCFW по кнопке **Открыть консоль**. Для UserGate DCFW, объединенных в кластер, по этой кнопке открывается окно выбора узла для перехода в веб-консоль этого узла.
- Перезагружать и выключать питание сервера одиночного UserGate DCFW или каждого из узлов кластера межсетевых экранов по ссылкам **Перезагрузить** и **Выключить** соответственно.
- Управлять лицензией UserGate DCFW: выполнять активацию лицензии по ссылке **Нет лицензии**, проверять срок ее действия по ссылке **Проверить лицензию**, а также обновлять лицензию по ссылке **Зарегистрированная версия**.
- Устанавливать обновление программного обеспечения (UGOS), загруженного локально на сервер одиночного UserGate DCFW или узла кластера межсетевых экранов, по ссылке **Установить обновление**.
- Изменять параметры UserGate DCFW посредством настройки параметров шаблонов, входящих в примененную конфигурацию.

## Кластеризация UserGate DCFW

Вы можете объединять два или более UserGate DCFW (узлов) в кластер конфигурации и настраивать на них единые параметры для работы с трафиком, используя шаблоны.

Создание кластера под управлением UserGate MC аналогично созданию автономного кластера. Отличие в том, что первый узел необходимо подключить к UserGate MC до создания кластера, остальные узлы будут подключены автоматически при их добавлении в кластер. При подключении каждому узлу присваивается уникальный идентификатор: node_1, node_2, node_3 и т. д.

Настраивать узел кластера (интерфейсы, сетевые зоны, политики фильтрации) можно двумя способами: локально или через шаблоны UserGate MC. Если на момент подключения узла параметры уже заданы в шаблонах, они применятся к новому узлу сразу после его добавления в кластер.

Между узлами кластера конфигурации выполняется синхронизация параметров, что обеспечивает бесперебойную фильтрацию и обработку сетевого трафика при недоступности одного из узлов.

Также вы можете объединять до четырех узлов кластера конфигурации в кластер отказоустойчивости. Этот кластер поддерживает следующие режимы работы:

- «активный — активный», в котором один из межсетевых экранов выполняет роль основного узла, распределяя трафик на все остальные узлы кластера;
- «активный — пассивный», в котором обработку транзитного трафика выполняет основной узел, при сбоях в работе этого узла трафик перенаправляется на резервные узлы кластера.

## Обновление UserGate DCFW

UserGate MC получает файлы обновлений программного обеспечения (UGOS) и системных библиотек из репозитория UserGate в рамках лицензии на модуль Security Update. При этом все UserGate DCFW, подключенные к управляемым устройствам, используют в качестве источника обновлений сервер UserGate MC.

В интерфейсе UserGate MC вы можете управлять обновлением UGOS:

- проверять наличие файлов обновлений в репозитории UserGate;
- загружать файлы обновлений из репозитория;
- изменять параметры обновления управляемых устройств;
- загружать файлы обновлений, полученные в личном кабинете my.usergate.com, в офлайн-режиме при отсутствии доступа к репозиторию UserGate.

Также вы можете управлять обновлением системных библиотек:

- управлять автоматическим обновлением библиотек на сервере UserGate MC;
- настраивать расписание автоматического обновления;
- загружать файлы обновлений, полученные в личном кабинете my.usergate.com, в офлайн-режиме при отсутствии доступа к репозиторию UserGate.

## Управление обновлением UGOS

Вы можете загружать файлы обновлений UGOS на сервер UserGate MC напрямую из репозитория UserGate или в офлайн-режиме.

**Примечание**Инструкции ниже выполняются администратором управляемой области в веб-консоли UserGate MC.

Чтобы загрузить файл обновления UGOS из репозитория UserGate:

1. В разделе **Управление областью → DCFW → Обновления ПО** нажмите **Выбрать онлайн-обновления**.

   Начнется проверка наличия обновлений UGOS в репозитории UserGate. По окончании проверки будет сформирован список доступных файлов обновлений.

2. Укажите файл обновления в списке и нажмите **Выбрать**.

   Обновление отобразится в таблице **Обновление ПО**. Вы можете отслеживать статус и прогресс его загрузки в соответствующих столбцах.

Чтобы загрузить файл обновления UGOS в офлайн-режиме:

1. В разделе **Управление областью → DCFW → Обновления ПО** нажмите **Импортировать обновление**.
2. По кнопке **Обзор** выберите файл обновления.

   Начнется загрузка файла обновления. По окончании процесса в окне загрузки отобразятся название и версия обновления UGOS.

3. При необходимости в поле **Совместимость** укажите версию UGOS, совместимую с загруженным обновлением.
4. Нажмите **Сохранить**.

   Обновление отобразится в таблице **Обновление ПО**.

После загрузки вам необходимо утвердить нужные обновления, чтобы они стали доступны для установки на подключенных UserGate DCFW. Для этого выберите обновление в таблице и нажмите **Утвердить обновление**. Действие также доступно при изменении параметров обновления. Кроме того, вы можете удалять обновления в таблице по кнопке **Удалить обновление**.

Чтобы изменить параметры обновления UGOS:

1. В разделе **Управление областью → DCFW → Обновления ПО** нажмите ссылку в столбце **Название** для обновления.
2. Если необходимо, на вкладке **Общие**:
   - измените описание обновления;
   - утвердите обновление с помощью флажка **Утвердить обновление**.
3. Если необходимо, на вкладке **Устройства** по кнопке **Добавить** добавьте управляемые устройства, которым будет доступно обновление.
4. Нажмите **Сохранить**.

Администраторы UserGate DCFW могут вручную устанавливать загруженные и утвержденные обновления UGOS локально на устройствах.

## Управление обновлением библиотек

По умолчанию системные библиотеки на сервере UserGate MC обновляются автоматически. В разделе **Управление областью → DCFW → Обновления библиотек** администраторы управляемой области UserGate MC могут отключить автоматическое обновление выбранной библиотеки по кнопке **Не обновлять**, а также включить его обратно по кнопке **Обновлять автоматически**. Кроме того, по кнопке **Импортировать обновление** доступна загрузка файла обновления библиотек на сервер UserGate MC в офлайн-режиме.

Системные библиотеки, находящиеся в репозитории UserGate MC, доступны всем UserGate DCFW, подключенным в качестве управляемых устройств. Эти библиотеки обновляются на UserGate DCFW автоматически по расписанию. Вы можете настраивать расписание автоматического обновления на каждом UserGate DCFW локально (подробнее — в разделе «Настройка общих параметров» Руководства администратора UserGate DCFW) или с помощью шаблонов устройств на UserGate MC. Ниже приведена инструкция по настройке расписания в шаблоне, которая выполняется администратором управляемой области в веб-консоли UserGate MC.

Чтобы настроить расписание автоматического обновления системных библиотек:

1. В одном из шаблонов UserGate DCFW в разделе **Консоль администратора → Настройки → Обновления библиотек** для параметра **Расписание автоматических обновлений** нажмите **Настроить**.
2. Выберите библиотеку в списке и укажите для нее вариант расписания.

   При выборе варианта **Задать вручную** вы можете указать время в cron-формате: <минуты: 0-59> <часы: 0-23> <дни месяца: 1-31> <месяцы: 1-12> <дни недели: 0-6, где 0 — воскресенье>.

   Для ручного ввода вы можете использовать следующие символы:

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

   При установке флажка **Единое расписание для всех обновлений** расписание выбранной библиотеки будет применено ко всем библиотекам в списке.

3. Нажмите **Сохранить**.

**Перенос объектов между шаблонами DCFW**

Product: DCFW
Version: 7.x

Функция переноса объектов между шаблонами в UserGate MC позволяет переносить или копировать объекты одинакового типа из одного шаблона в другой.

В шаблонах UserGate DCFW функция работает в разделах правил межсетевого экрана и правил NAT и маршрутизации.

Правила представляют собой упорядоченные объекты, для которых задается раздел (пре- или пост-правила) и позиция вставки (начало, конец раздела или место перед конкретным правилом).

При дублировании или переносе правил копируется основная запись вместе со ссылками на все вложенные элементы.

Чтобы скопировать или перенести правила между шаблонами, в исходном шаблоне на панели инструментов раздела правил нажмите **Перенести объекты** и выберите необходимое действие. Доступны операции как с выбранными объектами, так и со всем разделом целиком.

## Работа с выбранными правилами

При работе с выбранными правилами откроется диалоговое окно, в котором:

1. Выберите шаблон назначения.
2. Укажите раздел (пре- или пост-правила).
3. В области **Вставить** укажите позицию правила (начало, конец или перед конкретным объектом).
4. При необходимости установите флаг **Открыть целевой шаблон после копирования**.
5. Нажмите кнопку действия (**Копировать** или **Переместить**):
   - При копировании объекты переносятся в целевой шаблон с сохранением исходных названий.
   - При перемещении объекты копируются в целевой шаблон, а затем удаляются из исходного.

## Работа со всем разделом

При дублировании или перемещении всех правил раздела в диалоговом окне выберите шаблон назначения и укажите места размещения правил в соответствующих секциях (пре- и пост-правила), после чего нажмите кнопку действия.

- Копирование: все правила раздела дублируются в заданные места целевого шаблона.
- Перемещение: правила копируются в целевой шаблон и стираются из исходного.

## Конфликт имен

Если в целевом шаблоне уже существуют объекты с идентичными названиями, операция будет отменена. Появится окно со списком конфликтующих имен (не более 10) и количеством ошибок. Для успешного завершения операции вам необходимо вручную переименовать объекты с совпадающими именами и повторить действие.

**Управление устройствами UserGate WAF (версия 7.6.0 и выше)**

**Интеграция с устройствами UserGate WAF**

Product: UserGate MC
Version: 7.x, 7.6.x

Начиная с версии 7.6.0 в веб-консоли UserGate MC администраторы области могут централизованно управлять несколькими подключенными узлами UserGate WAF и получать телеметрию с подключенных устройств. Для этого необходимо настроить интеграцию UserGate MC с UserGate WAF.

Настройка интеграции с UserGate MC выполняется с помощью создания в управляемой области логического объекта — управляемого устройства, к которому будут привязаны реальные узлы UserGate WAF при их подключении к UserGate MC. Каждый такой логический объект во включенном состоянии использует одну лицензию на управляемое устройство.

С помощью одного управляемого устройства вы можете настроить интеграцию UserGate MC как с автономным узлом UserGate WAF, так и с кластером из нескольких устройств. В случае использования кластера конфигурации UserGate WAF достаточно подключить к UserGate MC первый узел, остальные узлы будут подключаться автоматически при добавлении в кластер.

Настройка интеграции UserGate WAF с UserGate MC выполняется в два этапа:

1. Создание управляемого устройства в UserGate MC.
2. Подключение узла UserGate WAF к управляемому устройству в UserGate MC.

## Создание управляемого устройства UserGate WAF

**Примечание**Действия, описанные ниже, выполняются администратором управляемой области в веб-интерфейсе UserGate MC.

Чтобы создать управляемое устройство UserGate WAF:

1. Войдите в веб-консоль управляемой области, в которой будет выполняться подключение UserGate WAF.
2. В разделе **Управление областью → WAF → Устройства** нажмите **Добавить**.
3. В открывшемся окне укажите название управляемого устройства, установите флажок **Включено** и сохраните изменения.
4. Выберите созданное управляемое устройство в списке и нажмите **Действия → Показать код подключения**.
5. Скопируйте код для подключения узла UserGate WAF.

## Подключение узла UserGate WAF к управляемому устройству в UserGate MC

Перед подключением узла UserGate WAF администратору UserGate MC в центре управления UserGate MC необходимо выбрать и настроить зону для управляемых устройств. В свойствах этой зоны нужно разрешить использование сервиса **UserGate Management Center** и затем эту зону назначить интерфейсу (подробнее о настройке зон и интерфейсов — в разделе « Настройка сети»). Также необходимо убедиться, что между узлами UserGate WAF и UserGate MC есть сетевая связность.

Чтобы подключить узел UserGate WAF к управляемому устройству:

1. Перейдите в веб-консоль подключаемого узла UserGate WAF.

2. В разделе **Настройки → Консоль администратора → Настройки** в блоке **Агент UserGate Management Center** нажмите **Настроить**.

3. В окне **Настройка агента UserGate Management Center** в поле **Адрес сервера UserGate Management Center** укажите IP-адрес интерфейса UserGate MC, которому была назначена зона для управляемых устройств (например, 192.0.2.4).

4. В поле **Код устройства** укажите код подключения узла UserGate WAF, сгенерированный в UserGate MC на этапе создания управляемого устройства.

5. Нажмите **Сохранить**.

Статус подключения отобразится в блоке **Агент UserGate Management Center** в виде цветового индикатора:

- Зеленый — соединение с сервером UserGate MC установлено, интеграция выполняется штатно.
- Красный — соединение с сервером UserGate MC не установлено, узел UserGate WAF отключен или на нем остановлена работа агента **UserGate Management Center**.

Кроме того, после подключения узла UserGate WAF в веб-консоли соответствующей управляемой области в разделе **Управление областью → WAF → Устройства** отобразится информация о подключенном узле. UserGate MC проверяет подключение к узлу UserGate WAF на портах TCP 2022 и 9712. По нажатию значка «плюс» слева от названия управляемого устройства отобразится информация о подключенном к нему узлу (или узлах) UserGate WAF: дата последнего подключения узла, версии ПО и лицензии.

## Управление устройствами UserGate WAF

В веб-консоли управляемой области с подключенными узлами UserGate WAF в разделе **Управление областью → WAF → Устройства** вы можете выполнять следующие действия:

- Приостанавливать или возобновлять работу управляемого устройства по кнопкам **Отключить** и **Включить** соответственно. При отключении устройства для всех привязанных к нему узлов UserGate WAF будут разорваны соединения с сервером UserGate MC.
- Удалять управляемое устройство.
- Изменять название и описание управляемого устройства по кнопке **Редактировать**.
- Перезагружать и выключать питание автономного узла UserGate WAF или каждого из узлов кластера. После отключения питания возобновление работы узла возможно только при включении питания непосредственно на самом узле.
- Переходить в веб-консоль нужного узла.
- Просматривать сведения о подключенном узле. Окно свойств подключенного узла доступно, если нажать значок «плюс» слева от названия управляемого устройства, затем выбрать нужный узел и нажать **Редактировать**.
- Управлять лицензией UserGate WAF (в том числе выполнять активацию лицензии) в окне свойств подключенного узла на вкладке **Лицензия**.

**Управление устройствами UserGate Log Analyzer**

**Управление устройствами UserGate Log Analyzer (описание)**

---

Documentation: ☑
Product: UGMC
Version: 7.x

В веб-консоли UserGate Management Center (далее также — UserGate MC) администраторы управляемой области могут централизованно управлять подключенными UserGate Log Analyzer (далее также — UserGate LogAn), а также настраивать параметры этих устройств. Для этого необходимо выполнить следующее:

1) создать шаблоны UserGate LogAn;

2) настроить параметры шаблонов UserGate LogAn;

3) создать группу шаблонов UserGate LogAn;

4) настроить интеграцию UserGate LogAn с UserGate MC.

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

## Создание шаблонов UserGate LogAn

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

Чтобы создать шаблон UserGate LogAn:

1. В разделе **Управление областью → LogAn → Шаблоны** нажмите **Добавить**.

2. На вкладке **Общие** укажите название и при необходимости описание шаблона.

3. При необходимости на вкладке **Разделы** установите флажок **Настроить отображение разделов** и выберите разделы веб-консоли, которые должны отображаться в шаблоне.

**Примечание**Выбор разделов доступен начиная с версии 7.6.0.

4. Нажмите **Сохранить**.

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

## Настройка параметров шаблонов UserGate LogAn

Чтобы настроить параметры шаблона UserGate LogAn:

В разделе **LogAn** для объекта **Шаблон** в выпадающем списке выберите шаблон, параметры которого необходимо настроить.

Настройка параметров шаблона выполняется в разделах боковой панели аналогично настройке параметров локального UserGate LogAn (подробнее — в Руководстве администратора UserGate Log Analyzer).

При настройке параметров шаблона UserGate LogAn следует учитывать следующее:

- Значения параметров в шаблоне имеют более высокий приоритет, чем указанные администратором UserGate LogAn локально. Если значение параметра не указано ни в шаблоне, ни на стороне UserGate LogAn, будет использоваться значение по умолчанию.
- После применения параметров шаблона к управляемым устройствам администраторы могут изменять базовые параметры и параметры сетевых интерфейсов локально на каждом UserGate LogAn. Подробная информация об этих параметрах приведена в разделах «Настройка общих параметров» и «Настройка интерфейсов» Руководства администратора UserGate Log Analyzer.
- При настройке параметров сетевых интерфейсов в шаблоне невозможно конфигурировать интерфейс port0. Первым физическим интерфейсом, доступным для настройки в шаблоне, будет port1.

  Параметры интерфейса port0 настраиваются администратором UserGate LogAn при первоначальной настройке устройства. По умолчанию этот интерфейс используется для подключения UserGate LogAn к UserGate MC.

  При необходимости можно сконфигурировать сетевые интерфейсы локально на UserGate LogAn, для этого в параметрах выбранного интерфейса шаблона должен быть установлен флажок **Настраивается на устройстве**.

  Если вы создаете интерфейс в шаблоне, этот интерфейс автоматически будет добавлен в UserGate LogAn. Удаление интерфейса из шаблона не удаляет интерфейс на межсетевом экране. Если требуется удалить интерфейс на межсетевом экране, необходимо сделать это вручную.
- Правила syslog в шаблоне не переопределяют правила, созданные администраторами UserGate LogAn локально, а добавляются к ним в виде преправил и постправил.
- Библиотеки элементов шаблона (например, библиотеки IP-адресов, URL-списков, а также типов контента) по умолчанию не содержат данных, в отличие от библиотек UserGate LogAn (подробнее — в разделе «Библиотеки» Руководства администратора UserGate LogAn). Перед настройкой параметров шаблона следует добавить необходимые элементы библиотек.

  **Важно!**Данные библиотек не синхронизируются: если добавленные элементы не используются в параметрах шаблона, они не будут добавлены в библиотеки UserGate LogAn. Поэтому, чтобы на управляемых устройствах отображались, например, списки IP-адресов, созданные в шаблоне, необходимо использовать эти списки при настройке параметров шаблона.

## Создание группы шаблонов UserGate LogAn

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

Чтобы создать группу шаблонов UserGate LogAn:

1. В разделе **Управление областью → LogAn → Группы шаблонов** нажмите **Добавить**.

2. На вкладке **Общие** укажите название и при необходимости описание группы шаблонов.

3. На вкладке **Шаблоны** нажмите **Добавить**:

   - выберите шаблон в списке и добавьте его в группу по кнопке **Добавить**;
   - повторите действие для всех шаблонов, которые требуется добавить в группу;
   - нажмите **Закрыть**.

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

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

4. Нажмите **Сохранить**.

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

## Настройка интеграции UserGate LogAn с UserGate MC

Настройка интеграции с UserGate MC осуществляется путем создания в управляемой области логического объекта — устройства, к которому будут привязаны реальные UserGate LogAn при их подключении к UserGate MC. Каждый такой логический объект во включенном состоянии использует одну лицензию на управляемое устройство.

Для настройки интеграции UserGate LogAn с UserGate MC необходимо:

1) создать устройство в управляемой области;

2) подключить UserGate LogAn к UserGate MC.

Все UserGate LogAn, для которых настроена интеграция с UserGate MC, называются управляемыми устройствами.

## Создание устройства в управляемой области

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

Чтобы создать устройство в управляемой области:

1. В разделе **Управление областью → LogAn → Устройства** нажмите **Добавить**.

2. Укажите следующие параметры устройства:

   - название и при необходимости описание;
   - группу шаблонов, параметры которой должны применяться к подключенным UserGate LogAn;
   - режим синхронизации параметров между группой шаблонов и подключенными UserGate LogAn.

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

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

4. Нажмите **Сохранить**.

5. Выберите созданное устройство в списке и получите код для подключения UserGate LogAn, нажав **Действия → Показать уникальный код устройства**.

6. Сохраните код для подключения UserGate LogAn.

В интерфейсе UserGate MC вы можете просматривать список созданных устройств.

## Подключение UserGate LogAn к UserGate MC

Вы можете подключить UserGate LogAn к UserGate MC при первоначальной настройке устройства UserGate LogAn по кнопке **Настроить через UserGate Management Center**, а также при его дальнейшем использовании (см. инструкцию ниже).

Перед выполнением инструкции необходимо в свойствах зоны для подключения UserGate LogAn разрешить использование сервиса **UserGate Management Center**. Действие выполняется администратором UserGate MC в разделе **Центр управления → Зоны**. Также необходимо убедиться, что между серверами UserGate LogAn и UserGate MC есть сетевая связность.

**Примечание**Инструкция ниже выполняется в веб-консоли UserGate LogAn.

Чтобы подключить UserGate LogAn к UserGate MC:

1. В разделе **Настройки → Консоль администратора → Настройки** в блоке **Агент UserGate Management Center** нажмите **Настроить**.

2. Укажите IP-адрес UserGate MC (например, 192.0.2.4) и код для подключения UserGate LogAn, сгенерированный в веб-консоли UserGate MC.

3. Нажмите **Сохранить**.

   Статус подключения отобразится в блоке **Агент UserGate Management Center** в виде цветового индикатора:

   - Зеленый — соединение с сервером UserGate MC установлено, интеграция выполняется штатно.
   - Красный — соединение с сервером UserGate MC не установлено, межсетевой экран UserGate LogAn отключен или на нем остановлена работа агента **UserGate Management Center**.

   При успешном подключении конфигурация параметров группы шаблонов будет применена к UserGate LogAn. Параметры этой конфигурации (за исключением базовых параметров и параметров сетевых интерфейсов) будут недоступны для изменения на стороне UserGate LogAn.

   Кроме того, вы можете просматривать информацию о подключении UserGate LogAn в веб-консоли UserGate MC в разделе **Управление областью → LogAn → Устройства**. UserGate MC проверяет подключение к UserGate LogAn на портах TCP 2022 и 9712. Для каждого устройства в управляемой области отображаются статус и дата последнего подключения привязанных к нему UserGate LogAn, а также дополнительная информация, включая объем используемой памяти и время непрерывной работы межсетевых экранов.

В интерфейсе UserGate MC вы можете управлять подключенными UserGate LogAn.

## Просмотр списка устройств в управляемой области

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

- Включать и отключать устройства по кнопкам **Включить** и **Отключить** соответственно. При отключении устройства для всех привязанных к нему UserGate LogAn будут разорваны соединения с сервером UserGate MC.
- Удалять устройства по кнопке **Удалить**.
- Изменять параметры устройства по кнопке **Редактировать**.
- Просматривать информацию об устройстве в отдельном окне по кнопке **Показать детальную информацию**.

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

- **Все** — все устройства (фильтр по умолчанию).
- **Включенные** и **Выключенные** — устройства в выбранном состоянии.
- **Онлайн** — для привязанных к устройствам UserGate LogAn установлено соединение с сервером UserGate MC.
- **Офлайн** — для привязанных к устройствам UserGate LogAn не установлено соединение с сервером UserGate MC.
- **Не привязанные** — устройства, к которым не привязаны UserGate LogAn.
- **Консистентные устройства** — устройства, к которым привязаны UserGate LogAn с параметрами, синхронизированными с конфигурацией параметров группы шаблонов.
- **Неконсистентные устройства** — устройства, к которым привязаны UserGate LogAn с параметрами, не синхронизированными с конфигурацией параметров группы шаблонов.

Вы также можете управлять синхронизацией параметров между группой шаблонов и UserGate LogAn, для этого доступны ручной и автоматический режимы. Вручную вы можете запускать синхронизацию сразу для всех управляемых устройств (по кнопке **Действия → Запустить полную синхронизацию**) или только для выбранных (по кнопке **Запросить синхронизацию**).

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

## Управление подключенными UserGate LogAn

В разделе **Управление областью → LogAn → Устройства** вы можете управлять подключенными UserGate LogAn:

- Переходить в веб-консоли UserGate LogAn по кнопке **Открыть консоль**. Для UserGate LogAn, объединенных в кластер, по этой кнопке открывается окно выбора узла для перехода в веб-консоль этого узла.
- Перезагружать и выключать питание сервера одиночного UserGate LogAn или каждого из узлов кластера межсетевых экранов по ссылкам **Перезагрузить** и **Выключить** соответственно.
- Управлять лицензией UserGate LogAn: выполнять активацию лицензии по ссылке **Нет лицензии**, проверять срок ее действия по ссылке **Проверить лицензию**, а также обновлять лицензию по ссылке **Зарегистрированная версия**.
- Устанавливать обновление программного обеспечения (UGOS), загруженного локально на сервер одиночного UserGate LogAn или узла кластера межсетевых экранов, по ссылке **Установить обновление**.
- Изменять параметры UserGate LogAn посредством настройки параметров шаблонов, входящих в примененную конфигурацию.

## Обновление UserGate LogAn

UserGate MC получает файлы обновлений программного обеспечения (UGOS) и системных библиотек из репозитория UserGate в рамках лицензии на модуль Security Update. При этом все UserGate LogAn, подключенные к управляемым устройствам, используют в качестве источника обновлений сервер UserGate MC.

В интерфейсе UserGate MC вы можете управлять обновлением UGOS:

- проверять наличие файлов обновлений в репозитории UserGate;
- загружать файлы обновлений из репозитория;
- изменять параметры обновления управляемых устройств;
- загружать файлы обновлений, полученные в личном кабинете my.usergate.com, в офлайн-режиме при отсутствии доступа к репозиторию UserGate.

Также вы можете управлять обновлением системных библиотек:

- управлять автоматическим обновлением библиотек на сервере UserGate MC;
- настраивать расписание автоматического обновления;
- загружать файлы обновлений, полученные в личном кабинете my.usergate.com, в офлайн-режиме при отсутствии доступа к репозиторию UserGate.

## Управление обновлением UGOS

Вы можете загружать файлы обновлений UGOS на сервер UserGate MC напрямую из репозитория UserGate или в офлайн-режиме.

**Примечание**Инструкции ниже выполняются администратором управляемой области в веб-консоли UserGate MC.

Чтобы загрузить файл обновления UGOS из репозитория UserGate:

1. В разделе **Управление областью → LogAn → Обновления ПО** нажмите **Выбрать онлайн-обновления**.

   Начнется проверка наличия обновлений UGOS в репозитории UserGate. По окончании проверки будет сформирован список доступных файлов обновлений.

2. Укажите файл обновления в списке и нажмите **Выбрать**.

   Обновление отобразится в таблице **Обновление ПО**. Вы можете отслеживать статус и прогресс его загрузки в соответствующих столбцах.

Чтобы загрузить файл обновления UGOS в офлайн-режиме:

1. В разделе **Управление областью → LogAn → Обновления ПО** нажмите **Импортировать обновление**.
2. По кнопке **Обзор** выберите файл обновления.

   Начнется загрузка файла обновления. По окончании процесса в окне загрузки отобразятся название и версия обновления UGOS.

3. При необходимости в поле **Совместимость** укажите версию UGOS, совместимую с загруженным обновлением.
4. Нажмите **Сохранить**.

   Обновление отобразится в таблице **Обновление ПО**.

После загрузки вам необходимо утвердить нужные обновления, чтобы они стали доступны для установки на подключенных UserGate LogAn. Для этого выберите обновление в таблице и нажмите **Утвердить обновление**. Действие также доступно при изменении параметров обновления. Кроме того, вы можете удалять обновления в таблице по кнопке **Удалить обновление**.

Чтобы изменить параметры обновления UGOS:

1. В разделе **Управление областью → LogAn → Обновления ПО** нажмите ссылку в столбце **Название** для обновления.
2. Если необходимо, на вкладке **Общие**:
   - измените описание обновления;
   - утвердите обновление с помощью флажка **Утвердить обновление**.
3. Если необходимо, на вкладке **Устройства** по кнопке **Добавить** добавьте управляемые устройства, которым будет доступно обновление.
4. Нажмите **Сохранить**.

Администраторы UserGate LogAn могут вручную устанавливать загруженные и утвержденные обновления UGOS локально на устройствах.

## Управление обновлением библиотек

По умолчанию системные библиотеки на сервере UserGate MC обновляются автоматически. В разделе **Управление областью → LogAn → Обновления библиотек** администраторы управляемой области UserGate MC могут отключить автоматическое обновление выбранной библиотеки по кнопке **Не обновлять**, а также включить его обратно по кнопке **Обновлять автоматически**. Кроме того, по кнопке **Импортировать обновление** доступна загрузка файла обновления библиотек на сервер UserGate MC в офлайн-режиме.

Системные библиотеки, находящиеся в репозитории UserGate MC, доступны всем UserGate LogAn, подключенным в качестве управляемых устройств. Эти библиотеки обновляются на UserGate LogAn автоматически по расписанию. Вы можете настраивать расписание автоматического обновления на каждом UserGate LogAn локально (подробнее — в разделе «Настройка общих параметров» Руководства администратора UserGate LogAn) или с помощью шаблонов устройств на UserGate MC. Ниже приведена инструкция по настройке расписания в шаблоне, которая выполняется администратором управляемой области в веб-консоли UserGate MC.

Чтобы настроить расписание автоматического обновления системных библиотек:

1. В одном из шаблонов UserGate LogAn в разделе **Консоль администратора → Настройки → Обновления библиотек** для параметра **Расписание автоматических обновлений** нажмите **Настроить**.
2. Выберите библиотеку в списке и укажите для нее вариант расписания.

   При выборе варианта **Задать вручную** вы можете указать время в cron-формате: <минуты: 0-59> <часы: 0-23> <дни месяца: 1-31> <месяцы: 1-12> <дни недели: 0-6, где 0 — воскресенье>.

   Для ручного ввода вы можете использовать следующие символы:

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

   При установке флажка **Единое расписание для всех обновлений** расписание выбранной библиотеки будет применено ко всем библиотекам в списке.

3. Нажмите **Сохранить**

**Управление конечными устройствами**

**Общие сведения**

---

Version: 7.x
Product: UGMC
Documentation: ☑

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

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

Для подключения конечных устройств к UserGate MC необходимо выполнить следующее:

1) создать шаблоны конечных устройств;

2) настроить параметры шаблонов конечных устройств;

3) создать группу шаблонов конечных устройств;

4) настроить интеграцию конечных устройств с UserGate MC .

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

После подключения конечных устройств вы также можете:

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

**Создание шаблонов конечных устройств**

---

Version: 7.x

Product: UGMC

Documentation: ☑

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

Чтобы создать шаблон конечных устройств:

1. В разделе **Управление областью → Конечные устройства → Шаблоны** нажмите **Добавить**.

2. На вкладке **Общие** укажите название и при необходимости описание шаблона.

3. При необходимости на вкладке **Разделы** установите флажок **Настроить отображение разделов** и выберите разделы веб-консоли, которые должны отображаться в шаблоне.

   **Примечание**Выбор разделов доступен начиная с версии 7.6.0.

4. Нажмите **Сохранить**.

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

**Настройка параметров шаблонов конечных устройств**

---

Documentation:
Version: 7.x
Product: UGMC

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

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

При настройке параметров шаблона конечных устройств следует учитывать следующее:

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

## Настройка общих параметров

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

Чтобы настроить общие параметры шаблона конечных устройств:

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

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

     **Важно!**При отключенном сборе информации о конечном устройстве HIP-профили могут работать некорректно.
   - Если требуется, запретите сетевой доступ к конечному устройству при остановке работы UserGate Client.
   - Если требуется, настройте режим отключения правил межсетевого экрана.

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

     Вы можете запретить или разрешить пользователям конечного устройства самостоятельно удалять UserGate Client. Кроме того, вы можете указать код подтверждения удаления на конечном устройстве.
4. В блоке параметров **Оповещения** выполните следующие действия:
   - Если требуется, отключите отображение иконки UserGate Client в области уведомлений панели задач Windows.
   - Если требуется, настройте показ оповещений на конечном устройстве с помощью параметра **Показывать тултипы оповещений**:
     - при включенном параметре оповещения отображаются;
     - при отключенном параметре оповещения не отображаются (даже если они настроены для конкретных событий).
   - Если требуется, настройте оповещения для конкретных событий: о блокировании и разблокировании конечного устройства, а также о блокировании адреса ресурса.
5. Если требуется отправлять данные конечных устройств в UserGate Log Analyzer или UserGate SIEM, в блоке параметров **Настройки устройства LogAn/SIEM** настройте интеграцию с внешним сервером журналирования. Подробная информация приведена в разделе «Журналирование данных конечных устройств».

## Настройка параметров VPN-профиля

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

## Настройка параметров VPN-профиля для версий ниже 7.6.0

Чтобы настроить параметры VPN-профиля шаблона конечных устройств:

1. В разделе **Конечные устройства-конфигурация** для объекта **Шаблон** в выпадающем списке выберите шаблон, параметры которого необходимо настроить.
2. Выберите раздел **Консоль администратора → Настройка VPN**.
3. Нажмите **Добавить**.
3. На вкладке **Общие** выполните следующее:

- Включите VPN-профиль.
- Укажите название и при необходимости описание VPN-профиля.
- Укажите доменное имя или IP-адрес VPN-сервера.

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

- Выберите протокол:
  - **IPSec L2TP**: для создания туннеля используется протокол L2TP, для защиты передаваемых данных — протокол IPSec.

    При выборе **IPSec L2TP** также необходимо выбрать режим работы протокола IKE для согласования алгоритмов шифрования и аутентификации и указать общий ключ шифрования.

    **Примечание**Начиная с версии 7.5.0 поддержка IPSec L2TP прекращена.
  - **IKEv2 с сертификатом**: для создания туннеля используется протокол IKEv2, для проверки подлинности сервера и клиента — сертификаты.

    **Важно!**При генерации клиентского сертификата необходимо указать идентификатор пользователя (CN).
  - **IKEv2 с именем и паролем**: для создания туннеля используется IKEv2, для проверки клиента — логин и пароль (EAP-MSCHAP v2). Метод доступен только для пользователей доменного RADIUS-сервера.

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

4. На вкладке **Фаза 1** укажите параметры первой фазы создания VPN-соединения:
   - **Время жизни ключа** — время, по истечении которого выполняется повторная аутентификация.
   - **Dead peer detection** — проверка доступности соседнего устройства:
     - **Отключена** — проверка не выполняется.
     - **Всегда включена** — проверка выполняется с указанным интервалом. При отсутствии ответа каждые 5 секунд отправляются дополнительные DPD-запросы. Количество этих запросов задается в поле **Неудачных попыток**. При отсутствии ответа соединение разрывается.
     - **При отсутствии трафика** — проверка выполняется, только когда нет трафика через туннель. Если в течение двойного указанного интервала нет пакетов, отправляется DPD-запрос. При отсутствии ответа каждые 5 секунд отправляются дополнительные DPD-запросы. Количество этих запросов задается в поле **Неудачных попыток**. При отсутствии ответа соединение разрывается.
   - **Diffie-Hellman группы** — выбор группы для обмена ключами (чем выше номер группы, тем надежнее ключ шифрования).
   - **Безопасность** — выбор способов аутентификации и алгоритмов шифрования (применяются поочередно сверху вниз).
5. На вкладке **Фаза 2** укажите параметры второй фазы создания VPN-соединения:
   - **Время жизни ключа** — время, по истечении которого ключ шифрования будет изменен.
   - **Максимальный размер данных** — объем данных, после передачи которого ключ шифрования будет изменен.

     **Примечание**Если заданы оба параметра (время жизни ключа и максимальный размер данных), ключ шифрования будет изменен по достижении первого из лимитов.
   - **Безопасность** — выбор способов аутентификации и алгоритмов шифрования (применяются поочередно сверху вниз).
6. Нажмите **Сохранить**.

## Настройка параметров VPN-профиля для версий 7.6.0 и выше

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

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

Чтобы настроить параметры VPN-профиля для протокола DTLS:

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

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

   - Выберите режим аутентификации:
     - **AAA** — по логину и паролю (только для пользователей доменного RADIUS-сервера).
     - **PKI** — с использованием цифровых сертификатов.
5. На вкладке **Фаза 1** укажите параметры первой фазы создания VPN-соединения:
   - **Время жизни ключа** — время, по истечении которого выполняется повторная аутентификация.
   - **Dead peer detection** — проверка доступности соседнего устройства:
     - **Отключена** — проверка не выполняется.
     - **Всегда включена** — проверка выполняется с указанным интервалом. При отсутствии ответа каждые 5 секунд отправляются дополнительные DPD-запросы. Количество этих запросов задается в поле **Неудачных попыток**. При отсутствии ответа соединение разрывается.
     - **При отсутствии трафика** — проверка выполняется, только когда нет трафика через туннель. Если в течение двойного указанного интервала нет пакетов, отправляется DPD-запрос. При отсутствии ответа каждые 5 секунд отправляются дополнительные DPD-запросы. Количество этих запросов задается в поле **Неудачных попыток**. При отсутствии ответа соединение разрывается.
   - **Безопасность** — выбор набора шифров DTLS из списка (применяются поочередно сверху вниз).
6. На вкладке **Фаза 2** укажите объем данных, после передачи которого ключ шифрования будет изменен.
7. Нажмите **Сохранить**.

Чтобы настроить параметры VPN-профиля для протокола IKEv2:

1. В разделе **Конечные устройства** для объекта **Шаблон** в выпадающем списке выберите шаблон, параметры которого необходимо настроить.
2. Выберите раздел **Консоль администратора → Настройка VPN**.
3. Нажмите **Добавить → IKEv2**.
4. На вкладке **Общие** выполните следующее:
   - Включите VPN-профиль, установив флажок **Включено**.
   - Укажите название и при необходимости описание VPN-профиля.
   - Укажите доменное имя или IP-адрес VPN-сервера.

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

   - Выберите режим аутентификации:

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

5. На вкладке **Фаза 1** укажите параметры первой фазы создания VPN-соединения:
   - **Время жизни ключа** — время, по истечении которого выполняется повторная аутентификация.
   - **Dead peer detection** — проверка доступности соседнего устройства:
     - **Отключена** — проверка не выполняется.
     - **Всегда включена** — проверка выполняется с указанным интервалом. При отсутствии ответа каждые 5 секунд отправляются дополнительные DPD-запросы. Количество этих запросов задается в поле **Неудачных попыток**. При отсутствии ответа соединение разрывается.
     - **При отсутствии трафика** — проверка выполняется, только когда нет трафика через туннель. Если в течение двойного указанного интервала нет пакетов, отправляется DPD-запрос. При отсутствии ответа каждые 5 секунд отправляются дополнительные DPD-запросы. Количество этих запросов задается в поле **Неудачных попыток**. При отсутствии ответа соединение разрывается.
   - **Diffie-Hellman группы** — выбор группы для обмена ключами (чем выше номер группы, тем надежнее ключ шифрования).
   - **Безопасность** — выбор способов аутентификации и алгоритмов шифрования (применяются поочередно сверху вниз).
6. На вкладке **Фаза 2** укажите параметры второй фазы создания VPN-соединения:
   - **Время жизни ключа** — время, по истечении которого ключ шифрования будет изменен.
   - **Максимальный размер данных** — объем данных, после передачи которого ключ шифрования будет изменен.

     **Примечание**Если заданы оба параметра (время жизни ключа и максимальный размер данных), ключ шифрования будет изменен по достижении первого из лимитов.
   - **Безопасность** — выбор способов аутентификации и алгоритмов шифрования (применяются поочередно сверху вниз).
7. Нажмите **Сохранить**.

## Настройка правил межсетевого экрана

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

Чтобы настроить правила межсетевого экрана шаблона конечных устройств:

1. В разделе **Конечные устройства** (для версий ниже 7.6.0 раздел **Конечные устройства-конфигурация**) для объекта **Шаблон** в выпадающем списке выберите шаблон, параметры которого необходимо настроить.
2. Выберите раздел **Политики сети → Межсетевой экран**.
3. Нажмите **Добавить**.
4. На вкладке **Общие** выполните следующее:
   - Включите правило, установив флажок.
   - Укажите название и при необходимости описание правила.
   - Выберите область применения правила:
     - **Везде** — правило будет применяться всегда, независимо от местоположения конечного устройства.
     - **Внутри периметра** — правило будет применяться, если конечное устройство находится в доменной сети.
     - **Снаружи периметра** — правило будет применяться, если конечное устройство находится вне доменной сети.
   - Выберите действие при срабатывании правила.
   - При необходимости включите журналирование срабатываний правила.
   - Укажите местоположение правила в списке правил.
5. На соответствующих вкладках укажите условия срабатывания правила.

   **Важно!**Не рекомендуется одновременно использовать в правиле условия фильтрации по IP-адресу и URL-адресу, по IP-адресу и URL-категории, а также по IP-адресу и типу контента. Такое правило будет срабатывать на разных уровнях модели OSI, что может привести к некорректной обработке трафика.
   - На вкладке **Пользователи** укажите пользователей или группы пользователей LDAP, для которых будет применяться правило. Подробнее — в разделе « Каталоги пользователей».
   - На вкладках **Источник**, **Назначение**, **Сервис**, **Приложения**, **URL**, **Категории URL**, **Типы контента**, **Время** выберите соответствующие объекты библиотек или создайте новые по ссылке **Создать и добавить новый объект**.

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

     **Примечание**Для добавления условий срабатывания по URL-адресам, URL-категориям и типам контента в правиле должны быть указаны сервисы.
   - На вкладке **HIP-профили** выберите HIP-профили конечных устройств из списка (по кнопке **Добавить**) или создайте новые (по ссылке **Создать и добавить новый объект** ).
   - На вкладке **Устройства** выберите конечные устройства, на которые будет распространяться правило.

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

## Управление библиотеками

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

## Настройка библиотеки сервисов

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

Чтобы добавить сервис:

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

## Настройка библиотеки групп сервисов

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

Чтобы добавить группу сервисов:

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

2. Выберите раздел **Библиотеки → Группы сервисов**.

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

4. Укажите название и при необходимости описание группы сервисов.

5. Нажмите **Сохранить**.

6. Выберите добавленную группу сервисов.

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

8. С помощью клавиши Ctrl или Shift выберите сервисы из списка и нажмите **Добавить**.

9. Нажмите **Закрыть**.

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

## Настройка библиотеки IP-адресов

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

Чтобы добавить статическую группу IP-адресов:

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

2. Выберите раздел **Библиотеки → IP-адреса**.

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

4. На вкладке **Общие** укажите параметры группы IP-адресов:

   - название и при необходимости описание;
   - уровень угрозы.

5. Нажмите **Сохранить**.

6. Выберите добавленную группу IP-адресов.

7. В блоке **Адреса из выбранной группы** нажмите **Добавить → Добавить элемент**.

8. Укажите IP-адрес.

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

9. Нажмите **Сохранить**.

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

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

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

## Настройка библиотеки групп приложений

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

Чтобы добавить статическую группу приложений:

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

2. Выберите раздел **Библиотеки → Группы приложений**.

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

4. На вкладке **Общие** укажите параметры группы приложений:

   - название и при необходимости описание;
   - уровень угрозы.

5. Нажмите **Сохранить**.

6. Выберите добавленную группу приложений.

7. В блоке параметров **Приложения** нажмите **Добавить**.

8. Укажите название приложения и хеш-сумму его исполняемого файла (по алгоритму SHA1).

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

9. Нажмите **Сохранить**.

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

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

## Настройка библиотеки URL-списков

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

Чтобы добавить статический URL-список:

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

2. Выберите раздел **Библиотеки → Списки URL**.

3. В блоке **Списки URL** нажмите **Добавить**.

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

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

5. Нажмите **Сохранить**.

6. Выберите добавленный URL-список.

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

8. Укажите URL-адрес или доменное имя.

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

Например:

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

9. Нажмите **Сохранить**.

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

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

## Настройка библиотеки URL-категорий

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

Чтобы добавить статическую группу URL-категорий:

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

2. Выберите раздел **Библиотеки → Категории URL**.

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

4. На вкладке **Общие** укажите название и при необходимости описание группы URL-категорий.

5. Нажмите **Сохранить**.

6. Выберите добавленную группу URL-категорий.

7. В блоке **Категории** нажмите **Добавить**.

8. С помощью клавиши Ctrl или Shift выберите URL-категории из списка категорий UserGate URL filtering и нажмите **Добавить**.

Подробнее о списке категорий UserGate URL filtering — в разделе « Фильтрация контента » руководства администратора UserGate NGFW.

9. Нажмите **Закрыть**.

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

## Настройка библиотеки типов контента

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

Чтобы добавить статическую группу типов контента:

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

2. Выберите раздел **Библиотеки → Типы контента**.

3. В блоке **Категории** нажмите **Добавить**.

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

6. Выберите добавленную группу типов контента.

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

8. Укажите тип контента в формате MIME.

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

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

9. Нажмите **Сохранить**.

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

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

## Настройка библиотеки календарей

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

Чтобы добавить статическую группу календарей:

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

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

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

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

6. Выберите добавленную группу календарей.

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

8. Укажите параметры календаря:

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

9. Нажмите **Сохранить**.

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

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

## Настройка обновляемых списков (групп) элементов

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

Чтобы подготовить файл со списком элементов:

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

**Примечание**Элементы должны быть записаны в столбик без знаков препинания.

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

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

**Примечание**Значение номера версии необходимо инкрементировать при каждом обновлении списка.

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

Чтобы добавить обновляемый список (группу) элементов:

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

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

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

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

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

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

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

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

  При ручном вводе также можно использовать следующие символы:

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

6. Нажмите **Сохранить**.

**Создание группы шаблонов конечных устройств**

---

Version: 7.x
Product: UGMC
Documentation: ☑

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

Чтобы создать группу шаблонов конечных устройств:

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

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

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

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

**Настройка интеграции конечных устройств с UserGate MC**

Version: 7.x
Product: UGMC
Documentation: ☑

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

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

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

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

Перед подключением конечного устройства администратору центра управления UserGate MC необходимо:

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

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

## Настройка интеграции одиночного конечного устройства

Для настройки интеграции одиночного конечного устройства с UserGate MC необходимо:

1) создать устройство в управляемой области;

2) подключить конечное устройство к UserGate MC.

### Создание устройства в управляемой области

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

Чтобы создать устройство в управляемой области:

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

В интерфейсе UserGate MC вы можете просматривать список созданных устройств.

### Подключение конечного устройства к UserGate MC

**Примечание**Инструкция ниже выполняется в интерфейсе конечного устройства.

Чтобы подключить конечное устройство к UserGate MC:

1. Запустите установочный файл UserGate Client на конечном устройстве.

   Подробнее — в разделе «Установка UserGate Client» Руководства администратора UserGate Client.

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

3. Нажмите **Register**.

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

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

## Настройка интеграции группы конечных устройств

Для настройки интеграции группы конечных устройств с UserGate MC необходимо:

1) создать код подключения конечных устройств;

2) подключить конечные устройства к UserGate MC.

### Создание кода подключения конечных устройств

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

Чтобы создать код подключения конечных устройств:

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

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

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

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

## Подключение конечных устройств к UserGate MC

Если конечные устройства не входят в домен AD, подключение к UserGate MC выполняется локально на каждом устройстве.

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

**Примечание**Инструкция ниже выполняется в интерфейсе конечного устройства.

Чтобы подключить конечное устройство к UserGate MC:

1. Запустите установочный файл UserGate Client на конечном устройстве.

   Подробнее — в разделе «Установка UserGate Client» Руководства администратора UserGate Client.

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

3. Нажмите **Register**.

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

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

Для подключения конечных устройств через групповые политики:

1. Скачайте файл UserGateClient.adm.

2. В этом файле в полях ServerIP и DeviceCode соответственно укажите IP-адрес или доменное имя UserGate MC, а также код подключения конечных устройств.

   Например:

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

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

4. Примените групповую политику.

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

**Управление списком устройств**

Version: 7.x
Product: UGMC
Documentation: ☑

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

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

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

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

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

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

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

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

## Просмотр параметров устройства

Для каждого устройства в списке отображаются следующие параметры.

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

## Просмотр подробной информации о конечном устройстве

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

| Вкладка | Описание |
|---|---|
| | |

| Вкладка | Описание |
|---|---|
| **Общие** | Сведения о конечном устройстве (имя компьютера, версия и тип ОС, версия UserGate Client, IP-адрес, время загрузки системы и текущее время на устройстве) и о пользователе, выполнившем вход в систему (фотография, имя, статус, тип учетной записи — локальная или доменная, телефон, электронная почта) |
| **Производительность** | В виде графика и таблиц отображаются следующие показатели производительности конечного устройства:<br>• загрузка центрального процессора;<br>• загрузка процессора процессом UserGate Client;<br>• использование виртуальной памяти;<br>• использование оперативной памяти;<br>• объем памяти, используемый UserGate Client;<br>• информация о дисках (размер, тип, производительность) |
| **Безопасность** | Информация о состоянии межсетевого экрана, антивируса, центра обеспечения безопасности Windows, а также о шифровании дисков (BitLocker) |
| **USB-устройства** | Список подключенных USB-устройств |
| **Элементы автозагрузки** | Список приложений, для которых настроен автоматический запуск при входе в систему |
| **Процессы** | Список запущенных процессов.<br>Вы можете принудительно завершить процесс по кнопке **Завершить процесс** |
| **Службы** | Список служб конечного устройства и их состояний.<br>Вы можете запустить или остановить службу с помощью кнопок **Запустить службу** и **Остановить службу** соответственно |
| **Ключи реестра** | Разделы реестра Windows HKEY_LOCAL_MACHINE и HKEY_USERS. При выборе ключа реестра отображаются его название, тип и значение |
| **Программное обеспечение** | Список установленных программ |
| **Установленные обновления** | Список установленных обновлений |
| **Точки восстановления** | Список доступных точек восстановления системы |

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

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

**Настройка проверки требований безопасности (HIP)**

---

Documentation:
Version: 7.x
Product: UGMC

**Примечание**Для использования возможностей, описанных в этом разделе, необходима лицензия на модуль NAC. Подробнее — в разделе « Лицензирование UserGate MC».

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

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

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

Для настройки проверки требований безопасности необходимо:

1) создать HIP-объекты;

2) создать HIP-профиль, добавив в него HIP-объекты и выбрав условие проверки объектов в профиле;

3) указать HIP-профили в правилах межсетевого экрана.

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

## Создание HIP-объекта

**Примечание**Для проверки некоторых критериев требуется лицензия на модуль Security Updates. Модуль необходим для скачивания обновлений библиотек, используемых при проверке комплаенса.

Чтобы создать HIP-объект:

1. В разделе **Управление областью → Конечные устройства → HIP-объекты** нажмите **Добавить**.
2. На вкладке **Общие** выполните следующее:
   - Укажите название и при необходимости описание HIP-объекта.
   - Укажите версию Windows конечного устройства.

     При выборе значения ANY версия ОС может быть любой. Для указания конкретной версии доступны операторы: = (версия совпадает с указанной) и != (версия не совпадает с указанной).
   - Укажите версию UserGate Client конечного устройства.

     При выборе значения ANY версия UserGate Client может быть любой. Для указания конкретной версии доступны операторы сравнения ( =, !=, <, >, <=, >=), а также операторы соответствия маске ( ~ и !~).
3. На вкладке **Безопасность** укажите состояние межсетевого экрана, антивируса, а также функций автоматического обновления (AutoUpdate) и шифрования дисков (BitLocker) на конечном устройстве:
   - **Не проверять** — состояние не учитывается;
   - **Нет** — компонент отключен;
   - **Да** — компонент включен.

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

   Список запущенных на конечном устройстве процессов доступен при просмотре подробной информации о конечном устройстве.
6. На вкладке **Запущенные службы** добавьте службы конечного устройства.

   Список запущенных на конечном устройстве служб доступен при просмотре подробной информации о конечном устройстве.
7. На вкладке **Ключи реестра** добавьте ключи реестра Windows конечного устройства.

   Список ключей реестра конечного устройства доступен при просмотре подробной информации о конечном устройстве.

   **Примечание**Вы можете добавлять ключи из разделов HKEY_LOCAL_MACHINE и HKEY_USERS.

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

     Подробнее о разделах реестра Windows — в документации Microsoft.
8. На вкладке **Установленные обновления** настройте проверку наличия обновлений Microsoft на конечном устройстве:
   - выберите условие проверки: **Все** (все указанные обновления) или **Любой** (хотя бы одно из указанных обновлений);
   - выберите режим проверки: **MATCH** (обновления установлены) или **NOT MATCH** (обновления не установлены);
   - нажмите **Добавить** и укажите номер статьи базы знаний Microsoft (KB) (например, KB5013624).
9. Нажмите **Сохранить**.

## Создание HIP-профиля

Чтобы создать HIP-профиль:

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

   При добавлении второго и последующих HIP-объектов вы можете выбрать условие применения каждого объекта в HIP-профиле:
   - **И** — устройство должно соответствовать этому объекту и всем остальным;
   - **ИЛИ** — устройство должно соответствовать этому объекту или любому другому;
   - **И НЕ** — устройство должно соответствовать всем объектам, кроме этого;
   - **ИЛИ НЕ** — устройство должно соответствовать любому объекту, кроме этого.

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

5. Нажмите **Сохранить**.

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

**Журналирование данных конечных устройств**

Version: 7.x
Product: UGMC
Documentation: ☑

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

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

## Настройка отправки данных конечных устройств

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

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

Чтобы настроить отправку данных конечных устройств:

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

## Просмотр журналов конечных устройств

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

- Журнал событий.
- Журнал правил.
- Приложения.
- Аппаратура.

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

При просмотре каждого журнала вы можете:

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

## Журнал событий

Журнал содержит данные о событиях, зарегистрированных на конечных устройствах.

| Параметр | Описание |
|---|---|
| **Узел** | Идентификатор конечного устройства или узла, на котором запущен сенсор |
| **Время** | Время регистрации события. Отображается в часовом поясе, настроенном в продукте |
| **Конечное устройство/сенсор** | Названия конечного устройства или сенсора |
| **Уровень лога** | Уровень важности зарегистрированного события:<br>• **Аудит успеха** (Audit Success) — событие при успешном обращении к ресурсу аудита;<br>• **Аудит отказа** (Audit Failure) — событие при неуспешном обращении к ресурсу аудита;<br>• **Ошибка** (Error) — событие указывает на существенные проблемы, которые могут стать причиной потери функциональности или данных;<br>• **Предупреждение** (Warning) — событие указывает на проблемы, которые не требуют немедленного решения, но могут привести к ошибкам в будущем;<br>• **Сведения** (Information) — информационное событие, которое, как правило, не требует внимания администратора |
| **Данные** | Подробная информация о событии |
| **Источник журнала событий** | Название источника, зарегистрировавшего событие |
| **Категория журнала** | Код категории журнала. Отображаются данные, полученные из журнала событий Windows (Application Event Log). Каждый источник журнала событий может определять собственные категории |
| **Категория инцидента** | Название категории, к которой относится инцидент |
| **Имя компьютера** | Полное название конечного устройства или узла, на котором запущен сенсор |
| **Имя пользователя** | Пользователь, с учетной записи которого был выполнен вход в систему конечного устройства |
| **Код события лога** | Код события |
| **Идентификатор события лога** | Идентификатор события |

| Параметр | Описание |
|---|---|
| **Тип события лога** | Тип события, которому соответствует уровень события:<br>• 1 — ошибка (error);<br>• 2 — предупреждение (warning);<br>• 3 — сведения (information);<br>• 4 — аудит успеха (audit success);<br>• 5 — аудит отказа (audit failure) |
| **Строка вставки** | Данные о событии, полученные от элемента EventData журнала событии Windows |
| **Файл журнала лога** | Тип журнала, к которому относится событие:<br>• **Application** (журнал приложений) — содержит события приложений и служб;<br>• **Security** (журнал безопасности) — содержит события системы аудита;<br>• **System** (системный журнал) — содержит события драйверов устройств;<br>• **CustomLog** — содержит события, зарегистрированные приложениями, которые ведут запись в пользовательский журнал |

### Журнал правил

Журнал содержит информацию о срабатываниях правил межсетевого экрана конечных устройств, в которых включен параметр **Журналирование**.

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

### Журнал приложений

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

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

| Параметр | Описание |
| --- | --- |
| **Идентификатор процесса** | Идентификатор процесса для приложения |
| **Пользователь** | Пользователь, запустивший приложение |
| **Командная строка** | Команда запуска приложения |

### Журнал устройств

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

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

**Управление устройствами UserGate SIEM (описание)**

Product: UGMC
Version: 7.x

Начиная с версии 7.5.0 в веб-консоли UserGate Management Center (далее также — UserGate MC) администраторы управляемой области могут централизованно управлять подключенными UserGate SIEM, а также настраивать параметры этих устройств. Для этого необходимо выполнить следующее:

1) создать шаблоны UserGate SIEM;

2) настроить параметры шаблонов UserGate SIEM;

3) создать группу шаблонов UserGate SIEM;

4) настроить интеграцию UserGate SIEM с UserGate MC.

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

## Создание шаблонов UserGate SIEM

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

Чтобы создать шаблон UserGate SIEM:

1. В разделе **Управление областью → SIEM → Шаблоны** нажмите **Добавить**.

2. На вкладке **Общие** укажите название и при необходимости описание шаблона.

3. При необходимости на вкладке **Разделы** установите флажок **Настроить отображение разделов** и выберите разделы веб-консоли, которые должны отображаться в шаблоне.

**Примечание**Выбор разделов доступен начиная с версии 7.6.0.

4. Нажмите **Сохранить**.

Созданный шаблон отобразится в списке шаблонов раздела. Теперь вы можете перейти к настройке его параметров. Параметры шаблона распространятся на все управляемые устройства UserGate SIEM, к которым будет применен шаблон в составе группы.

## Настройка параметров шаблонов UserGate SIEM

Чтобы настроить параметры шаблона UserGate SIEM:

В разделе **SIEM** для объекта **Шаблон** в выпадающем списке выберите шаблон, параметры которого необходимо настроить.

Настройка параметров шаблона выполняется в разделах боковой панели аналогично настройке параметров локального UserGate SIEM (см. Руководство администратора UserGate SIEM).

При настройке параметров шаблона UserGate SIEM следует учитывать следующее:

- Значения параметров в шаблоне имеют более высокий приоритет, чем указанные администратором UserGate SIEM локально. Если значение параметра не указано ни в шаблоне, ни на стороне UserGate SIEM, будет использоваться значение по умолчанию.
- После применения параметров шаблона к управляемым устройствам администраторы могут изменять базовые параметры и параметры сетевых интерфейсов локально на каждом UserGate SIEM. Подробная информация об этих параметрах приведена в разделах «Настройка общих параметров» и «Настройка интерфейсов» Руководства администратора UserGate SIEM.
- При настройке параметров сетевых интерфейсов в шаблоне отсутствует возможность конфигурирования интерфейса port0. Первым физическим интерфейсом, доступным для настройки в шаблоне, будет port1.

  Параметры интерфейса port0 настраиваются администратором UserGate SIEM при первоначальной настройке устройства. По умолчанию этот интерфейс используется для подключения UserGate SIEM к UserGate MC.

  При необходимости можно сконфигурировать сетевые интерфейсы локально на UserGate SIEM, для этого в параметрах выбранного интерфейса шаблона должен быть установлен флажок **Настраивается на устройстве**.

  Если вы создаете интерфейс в шаблоне, этот интерфейс автоматически будет добавлен в UserGate SIEM. При удалении интерфейса из шаблона он не удаляется на стороне UserGate SIEM — если необходимо удалить интерфейс на стороне UserGate SIEM, требуется сделать это вручную.
- Правила syslog в шаблоне не переопределяют правила, созданные администраторами UserGate SIEM локально, а добавляются к ним в виде преправил и постправил.
- Библиотеки элементов шаблона (например, библиотеки IP-адресов, URL-списков, а также типов контента) по умолчанию не содержат данных, в отличие от библиотек UserGate SIEM (подробнее — в разделе «Библиотеки» Руководства администратора UserGate SIEM). Перед настройкой параметров шаблона следует добавить необходимые элементы библиотек.

  **Важно!**Данные библиотек не синхронизируются: если добавленные элементы не используются в параметрах шаблона, они не будут добавлены в библиотеки UserGate SIEM. Поэтому, чтобы на управляемых устройствах отображались, например, списки IP-адресов, созданные в шаблоне, необходимо использовать эти списки при настройке параметров шаблона.

## Создание групп шаблонов UserGate SIEM

После создания и настройки шаблонов UserGate SIEM их необходимо объединить в группы. Группа шаблонов позволяет создать конфигурацию параметров, которая применяется к одному или нескольким управляемым устройствам. Эта конфигурация формируется в результате слияния параметров всех шаблонов, входящих в группу, с учетом их расположения.

Чтобы создать группу шаблонов UserGate SIEM:

1. В разделе **Управление областью → SIEM → Группы шаблонов** нажмите **Добавить**.

2. На вкладке **Общие** укажите название и при необходимости описание группы шаблонов.

3. На вкладке **Шаблоны** нажмите **Добавить**:

   - выберите шаблон в списке и добавьте его в группу по кнопке **Добавить**;
   - повторите действие для всех шаблонов, которые требуется добавить в группу;
   - нажмите **Закрыть**.

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

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

4. Нажмите **Сохранить**.

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

## Настройка интеграции UserGate SIEM с UserGate MC

Настройка интеграции с UserGate MC осуществляется путем создания в управляемой области логического объекта — устройства, к которому будут привязаны реальные UserGate SIEM при их подключении к UserGate MC. Каждый такой логический объект во включенном состоянии использует одну лицензию на управляемое устройство.

Для настройки интеграции UserGate SIEM с UserGate MC необходимо:

1) создать устройство в управляемой области;

2) подключить UserGate SIEM к UserGate MC.

Все UserGate SIEM, для которых настроена интеграция с UserGate MC, называются управляемыми устройствами.

## Создание устройства в управляемой области

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

Чтобы создать устройство в управляемой области:

1. В разделе **Управление областью → SIEM → Устройства** нажмите **Добавить**.

2. Укажите параметры управляемого устройства:
   - название и при необходимости описание;
   - группу шаблонов, параметры которой должны применяться к подключенным UserGate SIEM;
   - режим синхронизации параметров между группой шаблонов и подключенными UserGate SIEM.
3. Нажмите **Сохранить**.
4. Выберите созданное устройство в списке и получите код для подключения, нажав **Действия → Показать уникальный код устройства**.
5. Сохраните код для подключения UserGate SIEM.

В интерфейсе UserGate MC вы можете просматривать список созданных устройств.

## Подключение UserGate SIEM к UserGate MC

Вы можете подключить UserGate SIEM к UserGate MC при первоначальной настройке устройства UserGate SIEM по кнопке **Настроить через UserGate Management Center**, а также при его дальнейшем использовании (см. инструкцию ниже).

Перед подключением UserGate SIEM администратору центра управления UserGate MC необходимо:

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

**Примечание**Инструкция ниже выполняется в веб-консоли UserGate SIEM.

Чтобы подключить UserGate SIEM к UserGate MC:

1. В разделе **Настройки → Консоль администратора → Настройки** в блоке **Агент UserGate Management Center** нажмите **Настроить**.
2. Укажите IP-адрес UserGate MC (например, 192.0.2.4) и код для подключения UserGate SIEM, сгенерированный в веб-консоли UserGate MC.
3. Нажмите **Сохранить**.

Статус подключения отобразится в блоке **Агент UserGate Management Center** в виде цветового индикатора:

- Зеленый — соединение с сервером UserGate MC установлено, интеграция выполняется.
- Красный — соединение с сервером UserGate MC не установлено, UserGate SIEM отключен или на нем остановлен агент **UserGate Management Center**.

При успешном подключении конфигурация параметров группы шаблонов будет применена к UserGate SIEM. Параметры этой конфигурации (за исключением базовых параметров и параметров сетевых интерфейсов) будут недоступны для изменения в UserGate SIEM.

Кроме того, вы можете просматривать информацию о подключении UserGate SIEM в веб-консоли UserGate MC в разделе **Управление областью → SIEM → Устройства**. Для каждого устройства в управляемой области отображаются статус и дата последнего подключения привязанных к нему UserGate SIEM, а также дополнительная информация, включая объем используемой памяти и время непрерывной работы UserGate SIEM.

В интерфейсе UserGate MC вы можете управлять подключенными UserGate SIEM.

## Просмотр списка устройств в управляемой области

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

- Включать и отключать устройства по кнопкам **Включить** и **Отключить** соответственно. При отключении устройства для всех привязанных к нему UserGate SIEM будут разорваны соединения с сервером UserGate MC.
- Удалять устройства по кнопке **Удалить**.
- Изменять параметры устройства по кнопке **Редактировать**.
- Просматривать информацию об устройстве в отдельном окне по кнопке **Показать детальную информацию**.

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

- **Все**. Все устройства (фильтр по умолчанию).
- **Включенные** и **Выключенные**. Устройства в выбранном состоянии.
- **Онлайн**. Для привязанных к устройствам UserGate SIEM установлено соединение с сервером UserGate MC.
- **Офлайн**. Для привязанных к устройствам UserGate SIEM не установлено соединение с сервером UserGate MC.
- **Не привязанные**. Устройства, к которым не привязаны UserGate SIEM.
- **Консистентные устройства**. Устройства, к которым привязаны UserGate SIEM с параметрами, синхронизированными с конфигурацией параметров группы шаблонов.
- **Неконсистентные устройства**. Устройства, к которым привязаны UserGate SIEM с параметрами, несинхронизированными с конфигурацией параметров группы шаблонов.

Вы также можете управлять синхронизацией параметров между группой шаблонов и UserGate SIEM, для этого доступны ручной и автоматический режимы. Вручную вы можете запускать синхронизацию сразу для всех управляемых устройств (по кнопке **Действия → Запустить полную синхронизацию**) или только для выбранных (по кнопке **Запросить синхронизацию**).

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

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

## Управление подключенными UserGate SIEM

В разделе **Управление областью → SIEM → Устройства** вы можете управлять подключенными UserGate SIEM:

- Переходить в веб-консоль UserGate SIEM по кнопке **Открыть консоль**.
- Перезагружать и выключать питание UserGate SIEM по ссылкам **Перезагрузить** и **Выключить** соответственно.
- Изменять параметры UserGate SIEM, посредством настройки параметров шаблонов, входящих в примененную конфигурацию.

**Общая библиотека (версия 7.6.0 и выше)**

**Общие сведения**

Version: 7.x, 7.6.x
Product: UserGate MC

В каждом шаблоне конфигурации управляемого устройства UserGate есть собственная библиотека элементов для настройки правил. Элементы из библиотеки шаблона можно использовать только в шаблонах конкретного типа устройства. Общая библиотека служит хранилищем нескольких типов элементов, доступных для настройки правил для любых устройств, а также позволяет просматривать изменения в свойствах этих элементов и отслеживать зависимости объектов — использование элементов в других объектах системы.

Вы можете добавлять элементы в разделы общей библиотеки, создавать их копии, редактировать и удалять.

Доступ к общей библиотеке имеют администраторы области, которым назначен профиль с соответствующим разрешением. Подробнее об этом — в разделе «  Администраторы области».

**IP-адреса**

---

Version: 7.x, 7.6.x
Product: UserGate MC

Списки IP-адресов используются при создании правил для устройств, подключенных к UserGate MC. Например, в правиле межсетевого экрана в качестве адресов источника трафика можно добавить списки IP-адресов из общей библиотеки.

Вы можете создавать статические списки IP-адресов, которые хранятся в UserGate MC, и обновляемые, которые автоматически пополняются из файлов, размещенных на внешнем сервере.

**Примечание**Подробнее о добавлении обновляемых списков элементов — в разделе « Настройка обновляемых списков элементов ».

Чтобы создать статический список IP-адресов:

1. В разделе **Управление областью → Общая библиотека → IP-адреса** в секции **Списки** нажмите **Добавить**.
2. В открывшемся окне на вкладке **Общие** укажите параметры списка IP-адресов:
   - название и при необходимости описание;
   - уровень угрозы.
3. Нажмите **Сохранить**.
4. Выберите добавленный список IP-адресов.
5. В блоке **Элементы списка** нажмите **Добавить → Добавить элемент**.
6. В открывшемся окне укажите IP-адрес.

   **Примечание**В поле допускается вводить IP-адрес (например, 192.0.2.25), диапазоны IP-адресов (например, 192.0.2.1 -192.0.2.25), а также адреса подсетей в формате CIDR (например, 192.0.2.0/24).
7. Нажмите **Сохранить**.
8. Для добавления других IP-адресов в список повторите шаги 5-7 инструкции.

Добавленные IP-адреса отобразятся в блоке **Элементы списка** для выбранного списка.

При необходимости вы можете добавить в статический список IP-адресов другие списки, созданные ранее. Для этого в блоке **Элементы списка** нажмите **Добавить → Добавить список**.

**Списки URL**

---

Version: 7.x, 7.6.x
Product: UserGate MC

Списки URL используются в правилах для устройств, подключенных к UserGate MC, в качестве черных и белых списков.

Вы можете создавать статические списки URL-адресов, которые хранятся в UserGate MC, и обновляемые, которые автоматически пополняются из файлов, размещенных на внешнем сервере.

**Примечание**О добавлении обновляемого списка URL-адресов — в разделе « Настройка обновляемых списков элементов ».

Чтобы создать статический URL-список:

1. В разделе **Управление областью → Общая библиотека → Списки URL** в блоке **Список** нажмите **Добавить**.
2. В открывшемся окне на вкладке **Общие** укажите параметры URL-списка:
   - название и при необходимости описание;
   - содержимое:
     - **Чувствительный к регистру** — URL-адреса с учетом регистра (для контентной фильтрации);
     - **Нечувствительный к регистру** — URL-адреса без учета регистра (для контентной фильтрации);
     - **Домен** — доменные имена (для DNS-фильтрации).
3. Нажмите **Сохранить**.
4. Выберите добавленный URL-список.
5. В блоке **Элементы списка** нажмите **Добавить**.
6. В открывшемся окне укажите URL-адрес или доменное имя.

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

   Например:

   ^example.domain.com$ — доменное имя без поддоменов (с любыми протоколами и путями);

   ^http://domain.com/example$ — только указанный URL-адрес;

   domain.com — доменное имя и все его поддомены (с любыми протоколами и путями);

   *example* — любые URL-адреса или доменные имена, содержащие example;

   ^example.domain.com/$ — некорректное значение (символ / требует указания протокола).
7. Нажмите **Сохранить**.
8. Для добавления других URL-адресов и доменных имен повторите шаги 5-7 инструкции.

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

**Сервисы**

---

Version: 7.x, 7.6.x
Product: UserGate MC

Раздел общей библиотеки **Сервисы** содержит списки сетевых протоколов и портов, которые могут использоваться при настройке правил для управляемых устройств UserGate.

Чтобы создать сервис:

1. В разделе **Управление областью → Общая библиотека → Сервисы** нажмите **Добавить**.

2. В открывшемся окне на вкладке **Общие** выполните следующее:

   - укажите название и при необходимости описание сервиса;
   - нажмите **Добавить** и укажите сетевой протокол, порты назначения и источника и шлюз прикладного уровня;
   - нажмите **Сохранить**;
   - при необходимости добавьте другие порты и протоколы.

3. Нажмите **Сохранить**.

**Группы сервисов**

---

Version: 7.x, 7.6.x
Product: UserGate MC

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

Чтобы создать группу сервисов:

1. В разделе **Управление областью → Общая библиотека → Группы сервисов** в блоке **Список** нажмите **Добавить**.
2. В открывшемся окне на вкладке **Общие** укажите название и при необходимости описание группы сервисов.
3. Нажмите **Сохранить**.
4. Убедитесь, что выбрана созданная группа, и в блоке **Элементы списка** нажмите **Добавить**.
5. В открывшемся окне с помощью клавиши Ctrl или Shift выберите сервисы из группы и нажмите **Добавить**.
6. Нажмите **Закрыть**.

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

**HIP-объекты**

Product: UserGate MC
Version: 7.x, 7.6.x

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

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

Из нескольких HIP-объектов формируется HIP-профиль. Подробнее об этом — в разделе « HIP-профили».

**Примечание**Для проверки некоторых критериев требуется лицензия на модуль Security Updates. Модуль необходим для скачивания обновлений библиотек, используемых при проверке комплаенса.

Чтобы создать HIP-объект:

1. В разделе **Управление областью → Общая библиотека → HIP-объекты** нажмите **Добавить**.
2. В открывшемся окне на вкладке **Общие** выполните следующее:
   - Укажите название и при необходимости описание HIP-объекта.
   - Укажите версию ОС Windows конечного устройства.

     При выборе значения ANY версия ОС может быть любой. Для указания конкретной версии доступны операторы: = (версия совпадает с указанной) и != (версия не совпадает с указанной).
   - Укажите версию UserGate Client конечного устройства.

     При выборе значения ANY версия UserGate Client может быть любой. Для указания конкретной версии доступны операторы сравнения ( =, !=, <, >, <=, >=), а также операторы соответствия маске ( ~ и !~).
3. На вкладке **Безопасность** укажите состояние межсетевого экрана, антивируса, а также функций автоматического обновления (AutoUpdate) и шифрования дисков (BitLocker) на конечном устройстве:
   - **Не проверять** — состояние не учитывается;
   - **Нет** — компонент отключен;
   - **Да** — компонент включен.

   **Важно!**При проверке BitLocker считается включенным, если шифрование активно хотя бы на одном из дисков конечного устройства.
4. На вкладке **Продукты** добавьте типы программного обеспечения конечного устройства:
   - **Антивирус** — для антивирусного ПО укажите статус установки, состояние и актуальность антивирусных баз, а также выберите необходимые продукты из списка по кнопке **Добавить**.
   - **Межсетевой экран** — для межсетевых экранов укажите статус установки, состояние и версию, а также выберите необходимые продукты из списка по кнопке **Добавить**.
   - **Резервное копирование** — для ПО резервного копирования укажите статус установки и версию, а также выберите необходимые продукты из списка по кнопке **Добавить**.
   - **Шифрование диска** — для ПО шифрования диска укажите статус установки и версию, а также выберите необходимые продукты из списка по кнопке **Добавить**.
   - **DLP** — для ПО предотвращения утечек информации укажите статус установки и версию, а также выберите необходимые продукты из списка по кнопке **Добавить**.
   - **Управление обновлениями** — для ПО управления обновлениями укажите статус установки и версию, а также выберите необходимые продукты из списка по кнопке **Добавить**.
5. На вкладке **Процессы** добавьте один или несколько процессов, запущенных на конечном устройстве.
6. На вкладке **Запущенные службы** добавьте службы, запущенные на конечном устройстве.
7. На вкладке **Ключи реестра** добавьте ключи реестра Windows конечного устройства. Вы можете добавлять ключи из разделов HKEY_LOCAL_MACHINE и HKEY_USERS.

   **Примечание**Списки процессов и служб, запущенных на конечном устройстве, а также ключи реестра можно посмотреть в окне соответствующего устройства «Информация о конечном устройстве» на вкладках «Процессы», «Службы»,«Ключи реестра». Подробнее об этом окне — в разделе «Управление списком устройств».

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

   Подробнее о разделах реестра Windows — в документации Microsoft.
8. На вкладке **Установленные обновления** настройте проверку наличия обновлений Microsoft на конечном устройстве:
   - выберите условие проверки: **Все** (все указанные обновления) или **Любой** (хотя бы одно из указанных обновлений);
   - выберите режим проверки: **MATCH** (обновления установлены) или **NOT MATCH** (обновления не установлены);
   - нажмите **Добавить** и укажите номер статьи базы знаний Microsoft (KB) (например, KB5013624).
9. Нажмите **Сохранить**.

**HIP-профили**

---

Version: 7.x, 7.6.x
Product: UserGate MC

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

Чтобы создать HIP-профиль:

1. В разделе **Управление областью → Общая библиотека → HIP-профили** нажмите **Добавить**.

2. В открывшемся окне на вкладке **Общие** укажите название и при необходимости описание профиля.

3. На вкладке **HIP-объекты** нажмите **Добавить**.

4. В открывшемся окне выберите HIP-объект в списке по кнопке **Добавить**.

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

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

5. Выбрав все объекты, нажмите **Закрыть**.

**Примечание**Вы также можете создавать и добавлять новые HIP-объекты на вкладке «HIP-объекты» по кнопке «Создать и добавить новый объект».

6. Нажмите **Сохранить**.

Созданный HIP-профиль отобразится в списке. Теперь вы можете использовать его в правилах межсетевого экрана конечного устройства и UserGate NGFW.

**Профили тайм-аутов**

Version: 7.x, 7.6.x
Product: UserGate MC

Профили тайм-аутов бездействия предназначены для настройки времени сохранения неактивных сетевых сессий. Они содержат значения тайм-аутов для различных состояний протоколов TCP, UDP и ICMP, что позволяет оптимизировать обработку соединений, адаптировать работу межсетевого экрана к особенностям приложений и эффективно использовать системные ресурсы. Вы можете создавать профили тайм-аутов, редактировать их и удалять.

По умолчанию в общей библиотеке создан профиль тайм-аутов Default idle timeouts profile с рекомендованными значениями для большинства сетевых сервисов. Этот профиль защищен от редактирования.

В конфигурации устройства профили могут применяться на двух уровнях:

- глобальном — значения тайм-аутов действуют для всех сессий соответствующего протокола в системе;
- сервисном — значения тайм-аутов профиля переопределяют глобальные параметры для определенного типа трафика.

В общей библиотеке вы можете создавать любое количество профилей, но в одной конфигурации устройства можно использовать не более 15 профилей тайм-аутов. Большее количество приведет к ошибке синхронизации конфигурации.

Чтобы создать профиль тайм-аутов:

1. В разделе **Управление областью → Общая библиотека → Профили соединений** нажмите **Добавить** и выберите **Профиль тайм-аутов**.

2. В открывшемся окне укажите название профиля, произвольное описание и установите необходимые значения тайм-аутов состояний сетевых протоколов.

| **Параметр** | **Описание** | **Значение по умолчанию** | **Диапазон значений** |
|---|---|---|---|
| **ICMP** | | | |
| ICMP timeout | Тайм-аут бездействия для ICMP-сессий (в секундах). Определяет время хранения записи об ICMP-сессии после последнего зарегистрированного ICMP-пакета. Если в течение заданного интервала новые пакеты не поступают, запись о сессии автоматически удаляется | 30 | 5-80 |
| **TCP** | | | |
| TCP timeout close | Тайм-аут бездействия для TCP-соединений в состоянии CLOSE (в секундах). Определяет время, в течение которого запись о завершенном TCP-соединении сохраняется в таблице состояний для обработки задержанных или повторно переданных пакетов. По истечении заданного интервала запись автоматически удаляется | 10 | 5-60 |
| TCP timeout close wait | Тайм-аут бездействия для TCP-соединений в состоянии CLOSE-WAIT (в секундах). Определяет время, в течение которого запись о TCP-соединении сохраняется в таблице состояний после перехода соединения в состояние CLOSE-WAIT. По истечении тайм-аута запись автоматически удаляется | 60 | 5-60 |
| TCP timeout established | Тайм-аут бездействия для TCP-соединений в состоянии ESTABLISHED (в секундах). Определяет время, в течение которого запись об установленном TCP-соединении сохраняется в таблице состояний при отсутствии сетевой активности. По истечении заданного интервала запись автоматически удаляется | 18000 | 3600-28800 |
| TCP timeout fin wait | Тайм-аут бездействия для TCP-соединений в состоянии FIN-WAIT (в секундах). Определяет время, в течение которого запись о TCP-соединении, находящемся в состоянии FIN-WAIT, сохраняется в таблице состояний. По истечении заданного интервала запись автоматически удаляется | 60 | 5-60 |
| TCP timeout last ack | Тайм-аут бездействия для TCP-соединений в состоянии LAST-ACK (в секундах). Определяет время, в течение которого запись о TCP-соединении, находящемся в состоянии LAST-ACK, сохраняется в таблице состояний в ожидании завершающего ACK-пакета. Если в течение заданного интервала подтверждение не поступает, запись автоматически удаляется | 10 | 5-60 |
| TCP timeout max retrans | Тайм-аут бездействия для TCP-соединений (в секундах). Определяет время, в течение которого запись о TCP-соединении, помеченном как проблемное из-за превышения допустимого количества повторных передач сегментов, сохраняется в таблице состояний. По истечении заданного интервала запись автоматически удаляется | 300 | 30-600 |
| TCP timeout syn recv | Тайм-аут бездействия для TCP-соединений в состоянии SYN-RECV (в секундах). Определяет время, в течение которого запись о TCP-соединении, находящемся в состоянии SYN-RECV, сохраняется в таблице состояний в ожидании завершения трехстороннего рукопожатия. Если в течение заданного интервала завершающий ACK-пакет не поступает, запись автоматически удаляется | 5 | 5-60 |
| TCP timeout syn sent | Тайм-аут бездействия для TCP-соединений (в секундах). Определяет время, в течение которого запись о TCP-соединении сохраняется в таблице состояний после отправки пакета SYN в ожидании ответного SYN-ACK. Если до истечения заданного интервала ответ не поступает, запись автоматически удаляется | 5 | 5-60 |
| TCP timeout time wait | Тайм-аут бездействия для TCP-соединений (в секундах). Определяет время, в течение которого запись о TCP-соединении в состоянии TIME-WAIT сохраняется в таблице состояний после завершения соединения. Это необходимо для корректной обработки задержавшихся пакетов и надежного завершения TCP-соединения | 60 | 5-60 |
| TCP timeout unacknowledged | Тайм-аут бездействия для TCP-соединений (в секундах). Определяет время, в течение которого запись о TCP-соединении, для которого не получены подтверждения (ACK) на переданные данные, сохраняется в таблице состояний. Если в течение заданного интервала подтверждение не поступает, запись автоматически удаляется | 300 | 30-600 |
| **UDP** | | | |
| UDP timeout | Базовый тайм-аут бездействия для UDP-сессии (в секундах). Применяется к UDP-сеансам, когда еще не определено наличие двустороннего потока данных (состояние UNREPLIED).<br><br>Если в течение указанного времени в сессии не проходит ни одного пакета, запись удаляется из таблицы состояний | 30 | 5-180 |
| UDP timeout stream | Тайм-аут бездействия для UDP-сессии (в секундах). Определяет время хранения записи о UDP-потоке в таблице состояний. Если в течение указанного интервала не фиксируется активность в рамках потока (для двусторонних UDP-потоков, состояние ASSURED), запись о сессии удаляется.<br><br>Более длительный тайм-аут, чем UDP timeout, поскольку такие сессии характерны для приложений реального времени (голосовой трафик, видеоконференция и т. д.) | 60 | 5-180 |

**Настройка обновляемых списков элементов**

---

Version: 7.x, 7.6.x
Product: UserGate MC

Списки IP-адресов и URL-адресов в общей библиотеке могут автоматически пополняться из файлов, размещенных на внешнем сервере. Для этого необходимо подготовить файл со списком элементов (создать его и разместить на внешнем сервере), а затем добавить обновляемый список в соответствующем разделе общей библиотеки.

Чтобы подготовить файл со списком элементов

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

   **Примечание**Элементы должны быть записаны в столбик без знаков препинания.

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

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

   **Примечание**Значение номера версии необходимо инкрементировать при каждом обновлении списка.

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

Чтобы добавить обновляемый список элементов:

1. В разделе **Общая библиотека** выберите **IP-адреса** или **Списки URL**.
2. В секции **Список** нажмите **Добавить**.
3. На вкладке **Общие** укажите название списка, при необходимости описание и настройте уровень угрозы для списка IP-адресов или чувствительность к регистру для списка URL.
4. На вкладке **Автоматическое обновление** установите флажок **Включено** и настройте следующие параметры:
   - URL-адрес внешнего сервера для получения обновлений. В формате http://<IP-адрес или доменное имя сервера> или ftp://<IP-адрес или доменное имя сервера>.
   - Расписание получения обновлений от внешнего сервера. Вы можете выбрать одно из предустановленных значений или указать время вручную в cron-формате: <минуты: 0-59> <часы: 0-23> <дни месяца: 1-31> <месяцы: 1-12> <дни недели: 0-6, где 0 — воскресенье>. При ручном вводе также можно использовать следующие символы:
     - Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что обновление должно выполняться каждый час.
     - Дефис (-) — для указания диапазона значений.
     - Запятая (,) — в качестве разделителя значений.
     - Косая черта (/) — для указания шага между значениями.
5. Нажмите **Сохранить**.

**Использование общей библиотеки**

Version: 7.x, 7.6.x
Product: UserGate MC

При настройке правил в шаблонах конфигурации управляемого устройства следует учитывать особенности работы с общими библиотеками. В этом разделе описаны действия, для которых в качестве примера выбрана настройка правила межсетевого экрана устройства UserGate NGFW. Действия при настройке других объектов конфигурации, где можно использовать списки элементов из общей библиотеки, аналогичны описанным.

## Добавление существующего списка элементов из общей библиотеки в правило

Чтобы добавить существующий список элементов из общей библиотеки в правило межсетевого экрана:

1. В управляемой области на странице **NGFW** в разделе **Политики сети → Межсетевой экран** откройте окно свойств нового или существующего правила.
2. Перейдите на вкладку с параметрами, для настройки которых можно использовать списки элементов из библиотеки, например на вкладку **Источник**.
3. В секции **Адрес источника** нажмите добавить и выберите **Добавить список IP-адресов** (или **Добавить список доменов**).
4. В окне выбора списков IP-адресов перейдите на нужную вкладку и добавьте списки элементов из общей библиотеки, библиотек шаблонов или из предустановленных списков.

   **Примечание**Вы можете добавлять элементы из одной или из всех библиотек.
5. Закройте окно и продолжите настройку других параметров правила.

## Создание списка элементов для общей библиотеки при настройке правила

При создании правила в шаблоне конфигурации вы можете добавить новый список в окне настройки правила, если существующие списки не подходят. Новый список можно сохранить либо в общую библиотеку, либо в библиотеку шаблонов. Выбор библиотеки зависит от ваших целей: используйте общую библиотеку, если планируете применять этот список в конфигурациях устройств разных типов, а также если вам важны история изменений элемента и отслеживание его зависимостей.

Чтобы создать и добавить новый список элементов в окне настройки правила:

1. В управляемой области на странице **NGFW** в разделе **Политики сети → Межсетевой экран** откройте окно свойств нового или существующего правила.
2. Перейдите на вкладку с параметрами, для настройки которых можно использовать списки элементов из библиотеки, например, на вкладку **Источник**.
3. В открывшемся окне в секции **Адрес источника** нажмите **Создать и добавить новый объект** и выберите один из пунктов в меню, например **Добавить список IP-адресов**.
4. На вкладке **Общие** укажите название и при необходимости описание списка элементов, а также выберите уровень угрозы.
5. В секции **IP-адреса** выберите, в какую библиотеку будет добавлен новый список элементов: в общую (**Сохранить в общей библиотеке**) или в библиотеку конкретного шаблона (**Сохранить в шаблоне**).
6. В секции **IP-адреса** нажмите **Добавить** и выберите **Добавить список**.

   **Примечание**Вы также можете добавлять отдельные элементы, выбрав в этом меню «Добавить элемент».
7. В окне выбора списка добавьте нужные списки элементов и при необходимости предустановленные списки, после чего закройте окно.

   **Важно!**В списки общей библиотеки можно добавлять только объекты из общей библиотеки, а в списки библиотек шаблонов — только объекты из библиотек шаблонов.
8. Нажмите **Сохранить** и продолжите настройку остальных параметров правила.

Созданный список элементов будет сохранен в выбранной библиотеке.

**Просмотр зависимостей элементов общей библиотеки**

---

Version: 7.x, 7.6.x
Product: UserGate MC

Администратор области может просмотреть, с какими объектами системы связан элемент общей библиотеки. Например, входит ли он в состав другого списка в общей библиотеке или используется в правиле.

Чтобы просмотреть зависимости элемента:

1. Перейдите в нужный раздел общей библиотеки, выберите элемент из списка и нажмите **Редактировать**.
2. В окне свойств элемента перейдите на вкладку **Зависимости**.

**Примечание**Информация о зависимостях элемента общей библиотеки с другими объектами становится доступной после создания элемента.

3. Нажмите **Обновить**, чтобы получить актуальный список зависимостей элемента.

На вкладке **Зависимости** отобразится актуальный список объектов, с которыми связан выбранный элемент. Вы можете перейти к просмотру или настройке параметров любого из этих объектов, выбрав его в списке и нажав **Открыть свойства объекта**.

**Просмотр истории изменений элемента**

---

Version: 7.x, 7.6.x
Product: UserGate MC

Администраторы области могут изменять параметры элементов в общей библиотеке. Можно просматривать историю изменений элемента. Например, вы можете посмотреть, кто, когда и на каком узле вносил изменения.

Чтобы посмотреть историю изменений:

1. Перейдите в нужный раздел общей библиотеки, выберите элемент из списка и нажмите **Редактировать**.

2. В окне свойств элемента перейдите на вкладку **История** и посмотрите изменения, касающиеся выбранного элемента.

**Примечание**История изменений элемента общей библиотеки становится доступной после создания элемента.

3. Если необходимо, настройте фильтры, чтобы отобразить конкретные записи об изменениях.

**Перенос объектов из библиотек шаблонов в общую библиотеку**

---

Version: 7.x, 7.6.x
Product: UserGate MC

Элементы из библиотек шаблонов конфигурации устройств можно перенести в общую библиотеку. После этого перенесенные элементы будут доступны для использования во всех шаблонах, независимо от типа устройства.

Поддерживается перенос элементов следующих типов:

- списки IP-адресов;
- списки URL;
- сервисы;
- группы сервисов.

Перенос элементов выполняется в два этапа с помощью скриптов:

- mc-shared-library-objects-migrate.py — переносит все элементы из библиотеки выбранного шаблона в общую библиотеку.
- mc-shared-library-template-rules-convert.py — конвертирует правила, настроенные в выбранном шаблоне. Это обеспечивает корректную работу правил после изменения расположения используемых элементов.

После завершения каждого этапа будет сформирован и сохранен отчет в формате TXT, содержащий сведения о выполненной операции.

Перед началом работы убедитесь, что:

- архив со скриптами скачан в личном кабинете клиента;
- на компьютере, где будут выполняться скрипты, установлен Python версии 3.13 или выше;
- все операции выполняются от имени администратора области, имеющего необходимые права;
- команды запускаются из командной строки.

Поддерживаются два режима выполнения выполнение скрипта:

- в режиме диалога с последовательными запросами значений;
- с помощью полной команды вызова в batch-режиме;

**Примечание**При выполнении команд вы также можете указывать пароль через переменную окружения PASSWORD.

## Этап 1. Перенос элементов в общую библиотеку

Чтобы перенести элементы из библиотеки шаблона в общую библиотеку в диалоговом режиме выполнения скрипта:

1. В командной строке перейдите в директорию, в которой сохранены скрипты, и выполните команду:

```
% python3 mc-shared-library-objects-migrate.py -s <IP-адрес сервера UserGate MC> --user <логин администратора области> --password <пароль администратора области> --insecure
```

Пример команды:

```
% python3 mc-shared-library-objects-migrate.py -s 172.25.250.21 --user ex_admin --password Example --insecure
```

**Примечание**Аргумент --insecure следует указывать, если на сервере UserGate MC используется недоверенный сертификат.
**Примечание**Если в команде не указан аргумент --password, для выполнения команды потребуется ввести пароль в отдельной строке.

Отобразится меню выбора продукта.

```
INFO: Please select source product,
  1 = ngfw
  2 = dcfw
  3 = logan
  4 = siem
  5 = endpoint
> enter corresponding number:
```

2. Введите порядковый номер продукта и подтвердите ввод. Например, чтобы перенести элементы из библиотеки шаблона конфигурации UserGate NGFW, введите 1. После подтверждения ввода отобразится список шаблонов конфигурации, созданных для этого продукта.

```
> enter corresponding number: 1
INFO: selected product: ngfw
INFO: Please select source template,
  1 = UserGate Libraries template
  2 = example_content_template
  3 = example_firewall_template
  4 = example_settings
  5 = t1
> enter corresponding number:
```

3. Введите порядковый номер шаблона конфигурации. После подтверждения ввода отобразится список разделов библиотеки шаблона.

```
> enter corresponding number: 5
INFO: selected template: t1
INFO: Please select source object type,
  1 = nlist-network
  2 = nlist-url
  3 = nlist-servicegroup
  4 = service
```

4. Введите порядковый номер раздела библиотеки шаблона:

- nlists-network — IP-адреса;
- nlists-url — списки URL;
- services — сервисы;
- nlists-servicegroup — группы сервисов.

После подтверждения ввода отобразится меню выбора действий в случае конфликтов, которые могут возникнуть при переносе.

```
> enter corresponding number: 1
INFO: selected product: nlist-network
INFO: Please select error resolution option,
  1 = name_conflict:error
  2 = name_conflict:overwrite
  3 = name_conflict:skip
  4 = missing_dependencies:error
  5 = missing_dependencies:skip
> enter corresponding numbers (comma separated, eg.: 1,4):
```

5. При необходимости введите через запятую, какие действия нужно выполнить в случае конфликтов с именами элементов (пункты 1, 2 и 3) и вложенными объектами (пункты 4 и 5):

- name_conflict:error (действие по умолчанию) — если имя переносимого элемента совпадает с именем элемента в общей библиотеке, перенос будет отменен. В отчете будут указаны имена всех элементов, для которых обнаружен конфликт.
- name_conflict:overwrite — если имя переносимого элемента совпадает с именем элемента в общей библиотеке, существующий элемент общей библиотеки будет заменен переносимым элементом из библиотеки шаблона. Информация о замене будет сохранена в отчете.
- name_conflict:skip — если имя переносимого элемента совпадает с именем элемента в общей библиотеке, существующий элемент общей библиотеки останется без изменений, а перенос конфликтующего элемента будет пропущен. Информация о пропуске будет сохранена в отчете.

- missing_dependencies:error (действие по умолчанию) — если переносимый элемент содержит вложенные объекты, отсутствующие в общей библиотеке, перенос будет отменен. В отчете будут указаны имена всех отсутствующих вложенных объектов.
- missing_dependencies:skip — если переносимый элемент содержит вложенные объекты, отсутствующие в общей библиотеке, эти вложенные объекты будут исключены из переносимого элемента. Перенос будет выполнен, а в отчете будут указаны имена всех исключенных объектов.

**Примечание**Если действия не были указаны, в случае обнаружения конфликтов будут применены действия по умолчанию.

После подтверждения ввода отобразится строка подтверждения запуска переноса элементов.

> Everything is ready to start, continue? Enter 'y' to start or ctrl+c to terminate:

6. Введите Y. После подтверждения ввода начнется процесс переноса элементов в общую библиотеку.

После завершения переноса отобразится сообщение с указанием пути к отчету о переносе элементов.

Также для переноса элементов в общую библиотеку можно выполнить полную команду вызова в batch-режиме, задав в ней все необходимые параметры переноса.

Пример команды.

```
% python3 mc-shared-library-objects-migrate.py -s 172.25.250.21 --user ex_admin --password Example --insecure --source-product ngfw \
  --source-template t1 --source-object-type nlist-network --error-resolution name_conflict:error --batch
```

Пример команды с использованием переменной окружения PASSWORD.

```
% export PASSWORD=Example
% python3 mc-shared-library-objects-migrate.py -s 172.25.250.21 --user ex_admin --insecure --source-product ngfw --source-template t1 \
  --source-object-type nlist-network --error-resolution name_conflict:error --batch --report-download-dir <путь к директории для сохранения отчета (например,/home/iivanov/tmp)>
```

**Примечание**Справка по параметрам выполнения скрипта доступна по команде % python3 mc-shared-library-objects-migrate.py --help.
**Примечание**Если в команде не указана переменная окружения PASSWORD, для выполнения команды потребуется ввести пароль в отдельной строке.

## Этап 2. Конвертация правил

Чтобы выполнить конвертацию правил в диалоговом режиме выполнения скрипта:

1. В командной строке перейдите в директорию, в которой сохранены скрипты, и выполните команду:

```
% python3 mc-shared-library-template-rules-convert.py -s <IP-адрес сервера UserGate MC> --user <логин администратора области> --password <пароль администратора области> --insecure
```

Пример команды.
```
% python3 mc-shared-library-template-rules-convert.py -s 172.25.250.21 --user ex_admin --password Example --insecure
```

**Примечание**Аргумент --insecure следует указывать, если на сервере UserGate MC используется недоверенный сертификат.
**Примечание**Если в команде не указан аргумент --password, для выполнения команды потребуется ввести пароль в отдельной строке.

После подтверждения ввода отобразится меню выбора продукта.

```
INFO: Please select source product,
  1 = ngfw
  2 = dcfw
  3 = logan
  4 = siem
  5 = endpoint
> enter corresponding number:
```

2. Введите порядковый номер продукта, для которого выполнялся перенос элементов в общую библиотеку. После подтверждения ввода отобразится список шаблонов конфигурации, созданных для этого продукта.

```
> enter corresponding number: 1
INFO: selected product: ngfw
INFO: Please select source template,
  1 = UserGate Libraries template
  2 = example_content_template
  3 = example_firewall_template
  4 = example_settings
  5 = t1
> enter corresponding number:
```

3. Введите порядковый номер шаблона конфигурации, в котором нужно конвертировать правила. После подтверждения ввода отобразится строка подтверждения запуска конвертации правил.

> Everything is ready to start, continue? Enter 'y' to start or ctrl+c to terminate:

4. Введите Y. После подтверждения ввода начнется процесс конвертации правил.

После завершения переноса отобразится сообщение с указанием пути к отчету о конвертации правил.

Также для конвертации правил можно выполнить полную команду вызова в batch-режиме, задав в ней все необходимые параметры переноса.

Пример команды.

```
% python3 mc-shared-library-template-rules-convert.py -s 172.25.250.21 --user ex_admin --password Example --insecure --source-product ngfw --source-template t1 --batch
```

Пример команды с использованием переменной окружения PASSWORD.

```
% PASSWORD=Example python3 mc-shared-library-template-rules-convert.py -s 172.25.250.21 --user ex_admin --insecure --source-product ngfw --source-template t1 --batch
```

**Примечание**Справка по параметрам выполнения скрипта доступна по команде % python3 mc-shared-library-template-rules-convert.py --help.

После успешного выполнения обоих скриптов элементы из библиотеки выбранного шаблона будут перенесены в общую библиотеку, а правила шаблона будут обновлены с учетом нового расположения этих элементов. Перенесенные элементы можно будет использовать в шаблонах конфигурации устройств.

**Интерфейс командной строки**

**Общие положения**

**Общие положения (описание)**

---

Documentation: ☑
Product: UGMC
Version: 7.x

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. |
| **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:<br><br>*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)**

---

Documentation: ☑
Product: UGMC
Version: 7.x

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**

Documentation: ☑
Product: UGMC
Version: 7.x

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.<br>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. |
| **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**

Documentation: ☑
Product: UGMC
Version: 7.x

Для перехода в режим конфигурации интерфейса командной строки используется команда:

Admin/system@nodename> configure

В режиме конфигурации приглашение командной строки будет выглядеть следующим образом:

Admin/system@nodename#

## 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.

| Наименование | Описание |
|---|---|
| <action> | В режиме конфигурации доступны следующие действия:<br>• create — создание новых объектов.<br>• set — редактирование объектов, включение различных параметров.<br>• show — отображение текущих значений. Можно использовать на любом уровне конфигурации — будет отображено все, что находится глубже текущего уровня.<br>• delete — удаление объекта или параметра из списка параметров.<br>• edit — переход на какой-либо уровень конфигурации. Уровень конфигурации будет отображен под командной строкой.<br>• end — переход на один уровень выше.<br>• top — возврат на самый верхний уровень конфигурации.<br>• execute — выполнение команд, которые не относятся к конфигурации устройства (ping, date, traceroute и т.п.) Команда доступна независимо от уровня конфигурации. Подробнее — в разделе «Команды execute».<br>• export — экспорт сертификатов. Подробнее — в разделе « Команды export».<br>• import — импорт конфигурации. Подробнее — в разделе « Команды import».<br>• exit — выход из режима конфигурации.<br>Например, для просмотра информации о всех интерфейсах необходимо выполнить команду:<br>Admin/system@nodename# show network interface<br>С использованием следующей команды производится переход на уровень network interface. Текущий уровень будет отображен под командной строкой:<br>Admin/system@nodename# edit network interface<br>Admin/system@nodename#<br>Level: network interface<br>После перехода на уровень network interface для отображения всех интерфейсов используется команда show без указания уровня:<br>Admin/system@nodename# show<br>adapter:<br>port0<br>interface-name : port0<br>node-name : node1<br>zone : Management<br>enabled : on<br>ip-addresses : 192.168.56.3/24<br>iface-mode : dhcp<br>...<br>...<br>...<br>Level: network interface<br>Для возвращения с уровня network interface обратно на общий уровень режима конфигурации необходимо набрать команду end два раза:<br>Admin/system@nodename# end<br>Level: network interface<br>Admin/system@nodename# end<br>Level: network<br>Admin/system@nodename#<br>Для возврата на самый верхний уровень конфигурации с помощью одной команды можно использовать команду top:<br>Admin/system@nodename# top<br>Level: network interface<br>Admin/system@nodename# |
| <level> | Уровни в командной строке повторяют веб-интерфейс системной консоли UGMC:<br>• settings — соответствует разделу веб-интерфейса «UserGate».<br>• users — соответствует разделу веб-интерфейса «Пользователи и устройства».<br>• network — соответствует разделу веб-интерфейса «Сеть».<br>• realms — соответствует разделу веб-интерфейса «Управляемые области».<br>• monitoring — соответствует разделу веб-интерфейса «Диагностика и мониторинг».<br>• libraries — соответствует разделу веб-интерфейса «Библиотеки» |

| Наименование | Описание |
|---|---|
| <filter> | Идентификатор объекта, к которому происходит обращение. Идентификация происходит по имени объекта. Если имеются объекты с одинаковыми именами или удобнее идентифицировать объект по другому параметру, то используются круглые скобки, в которых необходимо указать параметры (<configuration_info>). В результате будет найден объект, для которого совпали все поля, указанные в круглых скобках.<br>Например, необходимо вывести информацию об интерфейсе port0 на другом узле кластера. Если использовать команду:<br>Admin/system@nodename# show network interface adapter port0<br>Будет отображена информация об интерфейсе port0 текущего узла UGMC. Чтобы отобразить информацию об интерфейсе port0 другого узла (например, с именем another_node), необходимо в скобках явно указать имя узла:<br>Admin/system@nodename# show network interface adapter ( node-name another_nodename interface port0 )<br>**Важно!** Круглые скобки должны быть отделены пробелами с обеих сторон |
| <configuration_info> | Указание параметра с аргументом. Параметр — имя поля, для которого нужно установить аргумент. Аргумент может быть одиночным или множественным.<br>Одиночный аргумент — значение, соответствующее параметру. Если строка содержит пробелы, то необходимо использовать кавычки.<br>Например, необходимо создать профиль аутентификации с именем New profile:<br>Admin/system@nodename# create users auth-profile name "New profile"<br>Множественные аргументы используются для установки множества значений какого-либо параметра, записываются в квадратных скобках и разделяются пробелами.<br>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:<br>Admin/system@nodename# create libraries ip-list name testlist ips [ 10.10.0.1 10.10.0.2 ]<br>**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 |
|---|---|
| clear-cli-history | Удаление истории команд интерфейса CLI. Можно удалить историю всех введенных команд интерфейса CLI или только команд в одном из режимов работы интерфейса (в режиме конфигурации или в режиме диагностики):<br>Admin/system@nodename# execute clear-cli-history<br>Admin/system@nodename# execute clear-cli-history modes [ <configure \| diagnostic> ] |
| configurate-cluster | Генерация секретного кода, необходимого для добавления нового узла в кластер конфигурации:<br>Admin/system@nodename# execute configurate-cluster generate-secret-key <parameter><br>Где:<br>• secret — ключ для генерации секретного кола в формате [0-9a-zA-Z]+#[0-9a-zA-Z]+ (например, example#key);<br>• expiration-time — срок действия кода в секундах;<br>• request-limit — срок действия запроса на генерацию кода.<br>**Важно!** Для использования данной команды необходимо наличие лицензии на модуль Cluster, иначе будет отображаться ошибка |
| date | Просмотр текущих даты и времени на узле:<br>Admin/system@nodename# execute date |
| dig | Проверка записи DNS домена:<br>Admin/system@nodename# execute dig host <hostname> <parameters><br>Admin/system@nodename# execute dig host <IP-address> <parameters><br>• host — доменное имя узла или IP-адрес для реверсивного поиска;<br>• reverse-lookup — получение имени узла по IP-адресу;<br>• dns — указание IP-адреса DNS-сервера;<br>• tcp — использование протокола TCP вместо UDP |
| factory-reset | Возврат устройства в первоначальное состояние:<br>Admin/system@nodename# execute factory-reset<br>Все данные и параметры будут утеряны. Версия ПО не изменится: сохранится версия, актуальная на момент запуска команды |
| license | Команда регистрации продукта:<br>Admin/system@nodename# execute license activate <pin-code><br>В качестве <pin-code> укажите код активации продукта |
| netcheck | Проверка доступности стороннего HTTP и HTTPS-сервера. Можно задать следующие параметры:<br>• address — доменное имя узла для проверки доступности по TCP или URL — для HTTP;<br>• dns-ip — IP-адрес сервера DNS;<br>• dns-tcp — использование TCP вместо UDP для DNS-запроса;<br>• check-cert — проверка SSL-сертификата;<br>• type — проверка доступности по:<br>◦ http;<br>◦ tcp (если порт не указан, то используется порт 80).<br>• data — запрос содержимого сайта. По умолчанию запрашиваются только заголовки;<br>• timeout — максимальный тайм-аут ожидания ответа от веб-сервера;<br>• user-agent — параметр для указания типа браузера. На некоторых сайтах может быть разрешен доступ только с определенных браузеров. Значение параметра указывается в двойных кавычках.<br>Admin/system@nodename# execute netcheck type tcp address <host-domain-name> data on<br>Admin/system@nodename# execute netcheck address <host-domain-name> |

| Параметр | Описание |
|---|---|
| ping | Проверка доступности узла. Можно задать следующие параметры:<br>• host — IP-адрес или доменное имя узла.<br>• count — количество отправляемых echo-запросов. Если параметр не задан, то отправка пакетов будет происходить, пока соединение не будет прервано пользователем (для прерывания необходимо нажать комбинацию клавиш Ctrl + C).<br>• numeric — не определять имена.<br>• timestamp — отображение временных меток.<br>• interval — интервал времени, через который будет производиться отправка пакетов. Указывается в секундах.<br>• ttl — время жизни пакета;<br>• interface — адрес выбранного интерфейса будет использоваться в качестве адреса источника для выполнения ping;<br>• mtu — максимальный размер блока данных отправляемых пакетов;<br>• virtual-router — имя виртуального маршрутизатора.<br>Admin/system@nodename# execute ping host <hostname> count <number> |
| reboot | Перезагрузка устройства:<br>Admin/system@nodename# execute reboot |
| shutdown | Выключение устройства:<br>Admin/system@nodename# execute shutdown |
| termination | Закрытие сессий администраторов:<br>Admin@nodename# execute termination <admin-session> |
| traceroute | Трассировка соединения до определенного узла. Параметры команды:<br>• host <ip-or-domain> — IP-адрес или имя домена, для которого производится трассировка;<br>• interface <iface-name> — интерфейс, с которого будут отправляться пакеты;<br>• not-map-ip — не искать hostname для IP-адреса при отображении;<br>• use-icmp-echo — использовать ICMP echo;<br>• port — указать порт вместо порта по умолчанию (1 — 65535);<br>• min-interval — минимальный интервал между пакетами.<br>Admin/system@nodename# execute traceroute host <hostname> |
| update | Доступно начиная с версии ПО 7.3.0.<br>Обновление:<br>• software-updates — обновление программного обеспечения.<br>• libraries-updates — обновление библиотек. Доступно обновление сразу всех библиотек или отдельных библиотек. |

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

Admin/system@nodename> <command-name>

## Команды import

В разделе «Настройки» (settings) можно импортировать сертификаты. Подробнее об управлении сертификатами — в разделе « Сертификаты».

## Команды export

Команда для экспорта сертификатов.

Вы можете экспортировать сертификаты, всю цепочку сертификатов и CSR:

Admin/system@nodename# export settings certificates <certificate-name>
Admin/system@nodename# export settings certificates <certificate-name> with-chain on

Подробнее об управлении сертификатами — в разделе « Сертификаты».

**Настройка устройства**

Documentation: ☑
Version: 7.x
Product: UGMC

## 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**):<br>• **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.<br>• **language**: язык интерфейса:<br>◦ **ru** — русский.<br>◦ **en** — английский.<br>• **api-session-lifetime**: время ожидания сеанса администратора в секундах. |
| **server-time** | Настройка параметров установки точного времени (уровень **settings general server-time**):<br>• **ntp-enabled**: включение/отключение использования NTP-серверов:<br>◦ **on**.<br>◦ **off**.<br>• **primary-ntp-server**: указание основного ntp-сервера.<br>• **second-ntp-server**: указание запасного ntp-сервера.<br>• **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** | Настройка учёта изменений (уровень **settings general change-tracker**):<br>• **enabled**: включение/отключение учёта изменений.<br>◦ **on**.<br>◦ **off**.<br>• **event-tracker-types**: типы изменений задаются администратором. Для удаления типа изменения используется команда:<br>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**).<br>Для расписания обновления программного обеспечения UserGate:<br>Admin/system@nodename# set settings general updates-schedule software schedule <schedule/disabled><br>Расписание скачивания обновлений библиотек может быть единым:<br>Admin/system@nodename# set settings general updates-schedule all-libraries schedule <schedule/disabled><br>или может быть настроено отдельно для каждого элемента:<br>Admin/system@nodename# set settings general updates-schedule libraries [ lib-module ... ] schedule <schedule/disabled><br>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:<br>• Звездочка (*) — обозначает весь диапазон (от первого до последнего).<br>• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.<br>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".<br>• 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".<br>Команда для просмотра расписания обновлений:<br>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:<br>• **on** — включено.<br>• **off** — выключено. |
| **ip** | IP-адрес внешнего прокси-сервера. |
| **port** | Порт внешнего прокси-сервера. |
| **auth** | Аутентификация на внешнем прокси-сервере:<br>• **on** — включена.<br>• **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:<br>• **ssh**.<br>• **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.<br>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:<br>• Звездочка (*) — обозначает весь диапазон (от первого до последнего).<br>• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.<br>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".<br>• 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:<br>• **ssh**.<br>• **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.<br>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:<br>• Звездочка (*) — обозначает весь диапазон (от первого до последнего).<br>• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.<br>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".<br>• 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". |

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**.

Version: 7.x
Product: UGMC
Documentation: ☑

## 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:<br>• **on**.<br>• **off**. |
| **name** | Название кластера отказоустойчивости. |
| **description** | Описание кластера отказоустойчивости. |
| **mode** | Выбор режима работы кластера:<br>• **active-passive**: режим работы Актив-Пассив (один из серверов выступает в роли Мастер-узла, обрабатывающего трафик, а остальные — в качестве резервных).<br>• **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:<br>• **off** — отключение синхронизации пользовательских сессий.<br>• **on** — включение синхронизации пользовательских сессий.<br>• **ha-cluster-id:**<br>◦ <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).<br>Добавление виртуального IP-адреса в кластер:<br>Admin/system@nodename# create settings device-mgmt ha-cluster virtual-ips <virtual-ips-filter> <virtual-ip-info><br>Доступные параметры для <virtual-ips-filter>:<br>• **new**: создать виртуальный IP-адрес для заданного кластера.<br>• <ip>: изменить данные для выбранного виртуального адреса.<br>Доступные параметры для <virtual-ip-info>:<br>• **ip**: задать IP-адрес для кластера отказоустойчивости (указывается в формате IP/mask).<br>• **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:<br>• **on**.<br>• **off**. |
| **name** | Название кластера отказоустойчивости. |
| **description** | Описание кластера отказоустойчивости. |
| **mode** | Выбор режима работы кластера:<br>• **active-passive**: режим работы Актив-Пассив (один из серверов выступает в роли Мастер-узла, обрабатывающего трафик, а остальные — в качестве резервных).<br>• **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:<br>• **off** — отключение синхронизации пользовательских сессий.<br>• **on** — включение синхронизации пользовательских сессий.<br>• **ha-cluster-id:**<br>◦ <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).<br>Добавление виртуального IP-адреса в кластер:<br>Admin/system@nodename# create settings device-mgmt ha-cluster virtual-ips <virtual-ips-filter> <virtual-ip-info><br>Доступные параметры для <virtual-ips-filter>:<br>• **new**: создать виртуальный IP-адрес для заданного кластера.<br>• <ip>: изменить данные для выбранного виртуального адреса.<br>Доступные параметры для <virtual-ip-info>:<br>• **ip**: задать IP-адрес для кластера отказоустойчивости (указывается в формате IP/mask).<br>• **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>

Version: 7.x
Product: UGMC
Documentation: ☑

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 пароль текущего администратора. |
| **unblock** | Разблокировать администратора. |
| **strong-password** | Использовать сложный пароль:<br>• **on**.<br>• **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:<br>• **enabled**: включение/отключение учётной записи администратора:<br>  ◦ **on**.<br>  ◦ **off**.<br>• **login**: логин администратора.<br>• **display-name**: отображаемое имя администратора.<br>• **description**: описание учётной записи администратора.<br>• **admin-profile**: профиль администратора. Создание профилей администраторов рассмотрено далее.<br>• **password**: пароль администратора. |

| Параметр | Описание |
|---|---|
| **ldap-user** | Добавить пользователя из существующего домена (необходим корректно настроенный LDAP-коннектор; подробнее читайте в разделе Настройка LDAP-коннектора):<br>• **enabled**: включение/отключение учётной записи администратора:<br>◦ **on**.<br>◦ **off**.<br>• **login**: логин администратора в формате **domain\user**. Структура команды при указании данного параметра:<br>• **display-name**: отображаемое имя администратора.<br>• **connector**: название сконфигурированного ранее LDAP-коннектора.<br>• **description**: описание учётной записи администратора.<br>• **admin-profile**: профиль администратора. Создание профилей администраторов рассмотрено далее.<br>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):<br>• **enabled**: включение/отключение учётной записи администратора:<br>◦ **on**.<br>◦ **off**.<br>• **login**: логин администратора<br>• **display-name**: отображаемое имя администратора.<br>• **connector**: название используемого LDAP-коннектора.<br>• **description**: описание учётной записи администратора.<br>• **admin-profile**: профиль администратора. Создание профилей администраторов рассмотрено далее.<br>Admin/system@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):<br>• **enabled**: включение/отключение учётной записи администратора:<br>◦ **on**.<br>◦ **off**.<br>• **login**: логин администратора.<br>• **display-name**: отображаемое имя администратора.<br>• **description**: описание учётной записи администратора.<br>• **admin-profile**: профиль администратора. Создание профилей администраторов рассмотрено далее.<br>• **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:<br>• **device** — администратор устройства UGMC.<br>• **realm** — администратор управляемой области. |

| Параметр | Описание |
| --- | --- |
| **permissions** | Права доступа:<br>• **no-access**: нет доступа.<br>• **read**: только чтение.<br>• **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> )

Documentation: ☑
Version: 7.x
Product: UGMC

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. |
| **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:<br>• **web-cert-chain**: цепочка сертификатов веб-консоли.<br>• **web-ssl**: сертификат, использующийся для создания безопасного HTTPS-подключения администратора к веб-консоли UserGate.<br>• **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>

Version: 7.x
Product: UGMC
Documentation: ☑

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:<br>• **on** — использование SSL-соединения для подключения к LDAP-серверу.<br>• **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 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 удаление 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. |

| Параметр | Описание |
|---|---|
| **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:

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 удаление 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. |
| **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**

Technology: Identification and Authentication
Version: 7.x
Product: UGMC
Documentation: ☑

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. |
| **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:<br>• **ldap**: аутентификация с использованием LDAP-коннектора.<br>• **radius**: аутентификация с использованием RADIUS-сервера.<br>• **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 удаление 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**

Documentation:
Product: UGMC
Version: 7.x

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):<br>• **enabled**: включение/отключение защиты.<br>◦ **on**.<br>◦ **off**.<br>• **aggregate**:<br>◦ **on** — считаются все пакеты, входящие в интерфейсы данной зоны.<br>◦ **off** — пакеты считаются отдельно для каждого IP-адреса.<br>• **alert-threshold**: порог уведомления; если количество запросов превышает данный порог, то происходит запись события в системный журнал.<br>• **drop-threshold**: порог отбрасывания пакетов; если количество запросов превышает указанное значение, то UserGate отбрасывает пакеты и записывает данное событие в системный журнал.<br>• **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты. |
| **dos-protection-udp** | Защита зоны от сетевого флуда для протокола UDP:<br>• **enabled**: включение/отключение защиты.<br>◦ **on**.<br>◦ **off**.<br>• **aggregate**:<br>◦ **on** — считаются все пакеты, входящие в интерфейсы данной зоны.<br>◦ **off** — пакеты считаются отдельно для каждого IP-адреса.<br>• **alert-threshold**: порог уведомления; если количество запросов превышает данный порог, то происходит запись события в системный журнал.<br>• **drop-threshold**: порог отбрасывания пакетов; если количество запросов превышает указанное значение, то UserGate отбрасывает пакеты и записывает данное событие в системный журнал.<br>• **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты. |
| **dos-protection-icmp** | Защита зоны от сетевого флуда для протокола ICMP:<br>• **enabled**: включение/отключение защиты.<br>◦ **on**.<br>◦ **off**.<br>• **aggregate**:<br>◦ **on** — считаются все пакеты, входящие в интерфейсы данной зоны.<br>◦ **off** — пакеты считаются отдельно для каждого IP-адреса.<br>• **alert-threshold**: порог уведомления; если количество запросов превышает данный порог, то происходит запись события в системный журнал.<br>• **drop-threshold**: порог отбрасывания пакетов; если количество запросов превышает указанное значение, то UserGate отбрасывает пакеты и записывает данное событие в системный журнал.<br>• **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты. |
| **enabled-services** | Параметры контроля доступа зоны:<br>• **"Any ICMP"**: разрешение использования команды ping адреса UserGate.<br>• **SNMP**: доступ к UserGate по протоколу SNMP (UDP 161).<br>• **rpc**: XML-RPC для управления - позволяет управлять продуктом по API (TCP 4040).<br>• **VRRP**: сервис, необходимый для объединения нескольких узлов UserGate в отказоустойчивый кластер (IP протокол 112).<br>• **"CLI over SSH"**: доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200.<br>• **Cluster**: сервис, необходимый для объединения нескольких узлов UserGate в кластер (TCP 4369, TCP 9000-9100).<br>• **"Admin Console"**: доступ к веб-консоли управления (TCP 8001). |
| **service-addresses** | Указание разрешённых IP-адресов для сервисов:<br>• **service**: выбор сервисов (список соответствует **enabled-services**).<br>• **allowed-addresses**: разрешённые IP-адреса:<br>◦ **geoip** — код GeoIP.<br>◦ **ip-list** — заранее созданный в библиотеке элементов список IP-адресов. |
| **antispoof-enable** | Включение/отключение защиты от IP-спуфинга:<br>• **on**.<br>• **off**. |

| Параметр | Описание |
|---|---|
| **antispoof-negate** | Возможные значения:<br>• **on**.<br>• **off**.<br>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:<br>• **on**.<br>• **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** | 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):<br>• **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты. |
| **dos-protection-udp** | Защита зоны от сетевого флуда для протокола UDP:<br>• **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты. |
| **dos-protection-icmp** | Защита зоны от сетевого флуда для протокола ICMP:<br>• **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>

Documentation: ☑
Product: UGMC
Version: 7.x

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:<br>• **on**.<br>• **off**. |
| **description** | Описание сетевого интерфейса. |
| **alias** | Алиас/псевдоним интерфейса. |
| **iface-type** | Тип интерфейса:<br>• **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).<br>• **mirror**: интерфейс, работающий в режиме Mirror (может получать трафик со SPAN-порта сетевого оборудования для его анализа). |
| **iface-mode** | Режим назначения IP-адреса:<br>• **dhcp**: получение динамического IP-адреса по DHCP.<br>• **manual**: без адреса.<br>Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса. |
| **zone** | Зона, которой будет принадлежать интерфейс. |
| **link-info** | Настройка параметров сетевого интерфейса:<br>• **bc_forwarding**: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс.<br>• **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.<br>Указываются в следующем формате:<br>Admin/system@nodename# create network interface <iface-type> ... link-info [ key/value ]<br>где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_).<br>value — значение параметра. Параметры могут принимать только целые числовые значения.<br>Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0.<br>Поле link-info будет отображено только в случае добавления параметров.<br>**Важно!** Удаление заданных параметров недоступно. |
| **ip-addresses** | Назначение интерфейсу IP-адреса.<br>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.<br>**Важно!** Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон. |
| **mac** | MAC-адрес интерфейса. |
| **mtu** | Указание размера MTU. |
| **mss** | Указание размера MSS (доступно начиная с релиза ПО 7.3.x): 0, или от 4 до введённого значения MTU минус 40. |

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:<br>• **on**.<br>• **off**. |
| **description** | Описание интерфейса. |
| **alias** | Алиас/псевдоним интерфейса. |
| **iface-type** | Тип интерфейса:<br>• **l3**: Layer 3 (можно назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах, это стандартный режим работы интерфейса).<br>• **mirror**: интерфейс, работающий в режиме Mirror (может получать трафик со SPAN-порта сетевого оборудования для его анализа). |
| **iface-mode** | Режим назначения IP-адреса:<br>• **dhcp**: получение динамического IP-адреса по DHCP.<br>• **manual**: без адреса.<br>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. |
| **link-info** | Настройка параметров сетевого интерфейса:<br>• **bc_forwarding**: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс.<br>• **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.<br>Указываются в следующем формате:<br>Admin/system@nodename# create network interface <iface-type> ... link-info [ key/value ]<br>где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_).<br>value — значение параметра. Параметры могут принимать только целые числовые значения.<br>Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0.<br>Поле link-info будет отображено только в случае добавления параметров.<br>**Важно!** Удаление заданных параметров недоступно. |
| **ip-addresses** | Назначение интерфейсу IP-адреса.<br>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.<br>**Важно!** Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон. |
| **mac** | MAC-адрес интерфейса. |
| **mtu** | Указание размера MTU. |
| **mss** | Указание размера MSS (доступно начиная с релиза ПО 7.3.x): 0, или от 4 до введённого значения MTU минус 40. |
| **dhcp-relay** | Настройка работы DHCP-релея на интерфейсе. Необходимо указать:<br>• **enabled**: включение/отключения релея:<br>◦ **on**.<br>◦ **off**.<br>• **utm-address**: IP-адрес интерфейса UserGate, на который добавляется функция релея.<br>• **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:<br>• **on**.<br>• **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:<br>• **bc_forwarding**: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс.<br>• **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.<br>Указываются в следующем формате:<br>Admin/system@nodename# create network interface <iface-type> ... link-info [ key/value ]<br>где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_).<br>value — значение параметра. Параметры могут принимать только целые числовые значения.<br>Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0.<br>Поле link-info будет отображено только в случае добавления параметров.<br>**Важно!** Удаление заданных параметров недоступно. |

| Параметр | Описание |
|---|---|
| **bonding** | Дополнительные параметры бонд-интерфейса:<br>• **mode** — режим работы бонда:<br>◦ **round-robin**: режим Round robin (пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. Эта политика применяется для балансировки нагрузки и отказоустойчивости).<br>◦ **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).<br>◦ **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).<br>◦ **broadcast**: режим Broadcast (передает все на все сетевые интерфейсы. Эта политика применяется для отказоустойчивости).<br>◦ **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 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).<br>◦ **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).<br>◦ **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 устройства используют различные MAC-адреса сервера. Балансировка входящего трафика распределяется последовательно (round-robin) между интерфейсами.<br>• **mii-monitoring**: периодичность MII-мониторинга в миллисекундах. Определяет, как часто будет проверяться состояние линии на наличие отказов.<br>• **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.<br>• **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.<br>• **lacp-rate**: интервал, с которым будут передаваться партнером LACPDU-пакеты в режиме 802.3ad. Возможные значения:<br>◦ **slow**: запрос партнера на передачу LACPDU-пакетов каждые 30 секунд.<br>◦ **fast**: запрос партнера на передачу LACPDU-пакетов каждую секунду.<br>• **failover-mac**: определение способа назначения MAC-адресов на объединенные интерфейсы в режиме Active backup при переключении интерфейсов. Возможные значения:<br>◦ **disabled**: устанавливает одинаковый MAC-адрес на всех интерфейсах во время переключения.<br>◦ **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.<br>◦ **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.<br>• **xmit-hash**: определение хэш-политики передачи пакетов через объединенные интерфейсы в режиме XOR или IEEE 802.3ad. Возможные значения:<br>◦ **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.<br>◦ **l2-3**: использует как MAC-адреса, так и IP-адреса для генерации хэша. Алгоритм совместим с IEEE 802.3ad.<br>◦ **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.<br>• **interface**: интерфейсы, которые будут объединены в бонд. |
| **iface-mode** | Режим назначения IP-адреса:<br>• **dhcp**: получение динамического IP-адреса по DHCP.<br>• **manual**: без адреса.<br>Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса. |
| **iface-type** | Тип создаваемого интерфейса:<br>• **l3** — Layer 3 интерфейс.<br>• **mirror** — интерфейс зеркалирования трафика. |
| **ip-addresses** | Назначение интерфейсу IP-адреса.<br>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.<br>**Важно!** Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон. |
| **mac** | MAC-адрес интерфейса. |
| **mtu** | Указание размер MTU. |
| **mss** | Указание размера MSS (доступно начиная с релиза ПО 7.3.x): 0, или от 4 до введённого значения MTU минус 40. |

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. |

| Параметр | Описание |
| --- | --- |
| **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>

Documentation: ☑
Product: UGMC
Version: 7.x

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:<br>• **on**.<br>• **off**. |
| **name** | Название шлюза. |
| **description** | Описание шлюза. |
| **interface** | Интерфейс, использующийся для выхода в Интернет:<br>• Выбор конкретного порта (**port0**, **port1**, **port2** итд.);<br>• **auto** — после выбора этого параметра порт определится автоматически. Данная опция доступна для узлов, прошедших инициализацию. Для узлов, не прошедших инициализацию, опция доступна начиная с релиза ПО 7.3.0. |
| **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:<br>• **on**.<br>• **off**. |
| **default** | Использование данного шлюза в качестве шлюза по умолчанию:<br>• **on**.<br>• **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>

Documentation: ☑
Product: UGMC
Version: 7.x
Technology: Routing

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:<br>• **on**.<br>• **off**. |
| **name** | Имя маршрута. |
| **description** | Описание маршрута. |
| **node-name** | Выбор узла кластера для настройки маршрутизации. |
| **type** | Тип маршрута:<br>• **unicast** — стандартный тип маршрута. Пересылает трафик, адресованный на адреса назначения, через заданный шлюз.<br>• **unreachable** — трафик отбрасывается. Источнику отправляется ICMP сообщение host unreachable (type 3 code 1).<br>• **prohibit** — трафик отбрасывается. Источнику отправляется ICMP сообщение host unreachable (type 3 code 13).<br>• **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>. |
| **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**

---

Documentation: ☑
Product: UGMC
Version: 7.x

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**

Documentation: ☑
Product: UGMC
Version: 7.x

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 динамическая (не более 27 байт). Фиксированная длина идентификатора применима только для типа **text**.<br>Engine ID может быть сформирован в формате:<br>• **ip4** — IPv4.<br>• **ipv6** — IPv6.<br>• **mac** — MAC-адрес.<br>• **text** — Текст.<br>• **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 цифры и латинские буквы. |
| **context** | Необязательный параметр, определяющий SNMP context. Можно использовать только латинские буквы и цифры.<br>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. |
| **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 |
|---|---|
| | |

| Параметр | Описание |
|---|---|
| **name** | Название профиля безопасности SNMP |
| **description** | Описание профиля безопасности SNMP |
| **username** | Имя пользователя для аутентификации SNMP-менеджера. |
| **auth-type** | Выбор режима аутентификации SNMP-менеджера. Возможны варианты:<br>• **none** — без аутентификации, без шифрования.<br>• **no-encrypt** — с аутентификацией, без шифрования.<br>• **encrypt** — с аутентификацией, с шифрованием.<br>Наиболее безопасным считается режим работы authPriv. |
| **auth-alg** | Алгоритм, используемый для аутентификации. Возможно использовать:<br>• **sha**;<br>• **md5**;<br>• **sha224**;<br>• **sha256**;<br>• **sha384**;<br>• **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. |
| **name** | Название правила. |
| **description** | Описание правила. |
| **notification-profile** | Созданный ранее профиль оповещения. |
| **sender** | От кого будет приходить оповещение. |
| **subject** | Тема оповещения. |
| **timeout** | Время, 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**

Documentation: ☑
Product: UGMC
Version: 7.x

## 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:<br>• **very-low** — очень низкий уровень угрозы.<br>• **low** — низкий уровень угрозы.<br>• **medium** — средний уровень угрозы.<br>• **high** — высокий уровень угрозы.<br>• **very-high** — высокий уровень угрозы. |
| **type** | Тип списка:<br>• **local** — локальный.<br>• **updatable** — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления ( **url**). Периодичность обновления списка указывается параметром **shedule** в формате crontab.<br>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:<br>• Звездочка (*) — обозначает весь диапазон (от первого до последнего).<br>• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.<br>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".<br>• 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. |

| Параметр | Описание |
|---|---|
| **type** | Тип списка:<br>• **local** — локальный.<br>• **updatable** — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления ( **url**). Периодичность обновления списка указывается параметром **shedule** в формате crontab.<br>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:<br>• Звездочка (*) — обозначает весь диапазон (от первого до последнего).<br>• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.<br>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".<br>• 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:<br>• **local** — локальный.<br>• **updatable** — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления ( **url**). Периодичность обновления списка указывается параметром **shedule** в формате crontab.<br>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:<br>• Звездочка (*) — обозначает весь диапазон (от первого до последнего).<br>• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.<br>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".<br>• 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. |

| Параметр | Описание |
|---|---|
| **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:<br>• **none**.<br>• **starttls**.<br>• **ssl**. |
| **authentication** | Включение/отключение авторизации при подключении к серверу SMTP:<br>• **on**.<br>• **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:<br>• **on**.<br>• **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.<br>Например, если необходимо заменить все номера, начинающиеся на +7, на 8:<br>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:<br>• **0** — Unknown (Неизвестный).<br>• **1** — International (Международный).<br>• **2** — National (Государственный).<br>• **3** — Network Specific (Сетевой Специальный).<br>• **4** — Subscriber Number (Номер абонента).<br>• **5** — Alphanumeric (Алфавитно-цифровой).<br>• **6** — Abbreviated (Сокращённый). |
| **dest-ton** | Тип номера (Type of Number) для адресата:<br>• **0** — Unknown (Неизвестный).<br>• **1** — International (Международный).<br>• **2** — National (Государственный).<br>• **3** — Network Specific (Сетевой Специальный).<br>• **4** — Subscriber Number (Номер абонента).<br>• **5** — Alphanumeric (Алфавитно-цифровой).<br>• **6** — Abbreviated (Сокращённый). |

| Параметр | Описание |
|---|---|
| **source-npi** | Индикатор схемы присвоения номеров (Numbering Plan Indicator) для источника:<br>• **0** — Unknown.<br>• **1** — ISDN/telephone numbering plan (E.163/E.164).<br>• **3** — Data numbering plan (X.121).<br>• **4** — Telex numbering plan (F.69).<br>• **6** — Land Mobile (E.212).<br>• **8** — National numbering plan.<br>• **9** — Private numbering plan.<br>• **10** — ERMES numbering plan (ETSI DE/PS 3 01-3).<br>• **13** — Internet (IP).<br>• **18** — WAP Client Id (to be defined by WAP Forum). |
| **dest-npi** | Индикатор схемы присвоения номеров (Numbering Plan Indicator) для адресата:<br>• **0** — Unknown.<br>• **1** — ISDN/telephone numbering plan (E.163/E.164).<br>• **3** — Data numbering plan (X.121).<br>• **4** — Telex numbering plan (F.69).<br>• **6** — Land Mobile (E.212).<br>• **8** — National numbering plan.<br>• **9** — Private numbering plan.<br>• **10** — ERMES numbering plan (ETSI DE/PS 3 01-3).<br>• **13** — Internet (IP).<br>• **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**

Documentation:
Product: UGMC
Version: 7.x

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)**

---

Documentation: ☑
Version: 7.x
Product: UGMC

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 — ↑, ↓.

Version: 7.x
Product: UGMC
Documentation: ☑

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:<br>• **create** — создание новых объектов.<br>• **set** — редактирование всех объектов, а также включение различных параметров.<br>• **show** — отображение текущих значений. Можно использовать на любом уровне конфигурации — будет отображено всё, что находится глубже текущего уровня.<br>• **delete** — удаление объекта или параметра из списка параметров.<br>• **edit** — переход на какой-либо уровень конфигурации. Уровень конфигурации будет отображён под командной строкой.<br>• **end** — переход на один уровень выше.<br>• **top** — возврат на самый верхний уровень конфигурации.<br>• **import** — импорт конфигурации.<br>• **export** — экспорт конфигурации.<br>• **go** — переход в режим настройки параметров шаблона управляемых устройств.<br>• **exit** — выход из режима конфигурации. |
| **<level>** | Уровни в командной строке повторяют веб-интерфейс консоли управления областью:<br>• **ngfw** — соответствует разделу веб-интерфейса **NGFW**.<br>• **endpoint** — соответствует разделу веб-интерфейса **Конечные устройства**.<br>• **logan** — соответствует разделу веб-интерфейса **LogAn**.<br>• **settings** — соответствует разделам веб-интерфейса **Центр управления** — **Настройки, Администраторы, Профили аутентификации**.<br>• **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.<br>**Одиночный аргумент** — значение, соответствующее параметру. Если строка содержит пробелы, то необходимо использовать кавычки.<br>**Множественные аргументы** используются для установки множества значений какого-либо параметра; записываются в квадратных скобках и разделяются пробелами. |

**Общие настройки консоли управляемой области**

---

Version: 7.x
Product: UGMC
Documentation: ☑

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**):<br>• **timezone**: часовой пояс, соответствующий вашему местоположению. Часовой пояс используется в расписаниях, применяемых в правилах, а таюке для корректного отображения времени и даты в отчетах, журналах и т.п<br>• **api-session-lifetime**: время ожидания сеанса администратора в секундах. |
| **change-tracker** | Настройка учета изменений (уровень settings general change-tracker):<br>• **enabled**: включение/отключение учёта изменений.<br>◦ **on**.<br>◦ **off**.<br>• **event-tracker-types**: типы изменений задаются администратором. Для удаления типа изменения используется команда:<br>realmadmin/realm@nodename# delete settings general change-tracker event-tracker-types [ type1 ... ] |

Version: 7.x
Product: UGMC
Documentation: ☑

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:<br>• **enabled**: включение/отключение учётной записи администратора:<br>◦ **on**.<br>◦ **off**.<br>• **login**: логин администратора.<br>• **display-name**: отображаемое имя администратора.<br>• **description**: описание учётной записи администратора.<br>• **admin-profile**: профиль администратора. Создание профилей администраторов рассмотрено далее.<br>• **password**: пароль администратора. |
| **ldap-user** | Добавить пользователя из существующего домена (необходим корректно настроенный LDAP-коннектор; подробнее читайте в разделе Настройка LDAP-коннектора):<br>• **enabled**: включение/отключение учётной записи администратора:<br>◦ **on**.<br>◦ **off**.<br>• **login**: логин администратора в формате **domain\user**. Структура команды при указании данного параметра:<br>• **display-name**: отображаемое имя администратора.<br>• **connector**: название сконфигурированного ранее LDAP-коннектора.<br>• **description**: описание учётной записи администратора.<br>• **admin-profile**: профиль администратора. Создание профилей администраторов рассмотрено далее.<br>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):<br>• **enabled**: включение/отключение учётной записи администратора:<br>◦ **on**.<br>◦ **off**.<br>• **login**: логин администратора<br>• **display-name**: отображаемое имя администратора.<br>• **connector**: название используемого LDAP-коннектора.<br>• **description**: описание учётной записи администратора.<br>• **admin-profile**: профиль администратора. Создание профилей администраторов рассмотрено далее.<br>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):<br>• **enabled**: включение/отключение учётной записи администратора:<br>◦ **on**.<br>◦ **off**.<br>• **login**: логин администратора.<br>• **display-name**: отображаемое имя администратора.<br>• **description**: описание учётной записи администратора.<br>• **admin-profile**: профиль администратора. Создание профилей администраторов рассмотрено далее.<br>• **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:<br>• **no-access**: нет доступа.<br>• **read**: только чтение.<br>• **write**: чтение и запись. |
| **ngfw-permissions** | Права доступа к управлению устройствами NGFW:<br>• **no-access**: нет доступа.<br>• **read**: только чтение.<br>• **write**: чтение и запись. |
| **ep-permissions** | Права доступа к управлению конечными устройствами:<br>• **no-access**: нет доступа.<br>• **read**: только чтение.<br>• **write**: чтение и запись. |
| **logan-permissions** | Права доступа к управлению устройствами LogAn:<br>• **no-access**: нет доступа.<br>• **read**: только чтение.<br>• **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

Version: 7.x
Product: UGMC
Documentation: ☑

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:<br>• **on** — использование SSL-соединения для подключения к LDAP-серверу.<br>• **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 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 удаление 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 |
|---|---|
| | |

| 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 удаление 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+. |
| **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>

Documentation:
Version: 7.x
Product: UGMC

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:<br>• **ldap**: аутентификация с использованием LDAP-коннектора.<br>• **radius**: аутентификация с использованием RADIUS-сервера.<br>• **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 удаление 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>

Version: 7.x
Product: UGMC
Documentation: ☑

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

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

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** | Определяет:<br>• **on** — использование SSL-соединения для подключения к LDAP-серверу.<br>• **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**.

Version: 7.x
Product: UGMC
Documentation: ☑

В интерфейсе командной строки UserGate Management Center (UGMC) администраторы управляемой области могут централизованно настраивать параметры межсетевых экранов UserGate. Для этого в режиме конфигурации необходимо выполнить следующее:

1) настроить параметры шаблонов UserGate NGFW;

2) создать группы шаблонов UserGate NGFW;

3) добавить управляемые устройства UserGate NGFW.

## Настройка параметров шаблонов UserGate NGFW

Перед настройкой параметров шаблонов UserGate NGFW необходимо создать шаблоны устройств. Рекомендуется создавать отдельные шаблоны для разных категорий параметров, например такие, как шаблон сетевых параметров, шаблон правил межсетевого экрана, шаблон правил фильтрации или шаблон библиотек. Это упростит дальнейшую работу с шаблонами при их объединении в группы. В таблице ниже приведены команды, которые вы можете использовать при создании шаблонов UserGate NGFW.

| Действие | Команда | Пример ввода команды |
|---|---|---|
| Создание шаблона | create ngfw template name <название шаблона> description <описание шаблона> | realmadmin/realm@nodename# create ngfw template name example_template_1 description for_example_template |
| Просмотр шаблона | show ngfw template <название шаблона> | realmadmin/realm@nodename# show ngfw template example_template_1 |
| Просмотр всех шаблонов | show ngfw template | realmadmin/realm@nodename# show ngfw template |
| Изменение названия и описания шаблона | set ngfw template <название шаблона> name <новое название шаблона> description <новое описание шаблона> | realmadmin/realm@nodename# set ngfw template example_template_1 name example_template_2 description for_testing_templete |
| Удаление шаблона | delete ngfw template <название шаблона> | realmadmin/realm@nodename# delete ngfw template test_template_2 |

После создания шаблона вы можете настроить его параметры. Эти параметры распространятся на все управляемые устройства UserGate NGFW, к которым будет применен шаблон в составе группы.

При настройке параметров шаблона следует учитывать следующее:

- Значения параметров в шаблоне имеют более высокий приоритет, чем указанные администратором UserGate NGFW локально. Если значение параметра не указано ни в шаблоне, ни на стороне межсетевого экрана, то будет использоваться значение по умолчанию.
- После применения шаблона к управляемым устройствам администраторы могут изменять базовые параметры и параметры сетевых интерфейсов локально на каждом межсетевом экране. Подробная информация об этих параметрах приведена в разделах «Общие настройки» и «Настройка интерфейсов» Руководства администратора UserGate NGFW.
- При настройке параметров сетевых интерфейсов в шаблоне первым физическим интерфейсом, доступным для конфигурирования, будет port1. Интерфейс port0 используется для подключения UserGate NGFW к UGMC. Параметры этого интерфейса настраиваются администратором UserGate NGFW при первоначальной настройке продукта. Локально на UserGate NGFW также можно сконфигурировать и другие сетевые интерфейсы, для этого в параметрах интерфейса шаблона вам необходимо указать свойство on-device (или on-device on).
- Библиотеки элементов шаблона (например, библиотеки IP-адресов, URL-списков, а также типов контента) по умолчанию не содержат данных, в отличие от библиотек UserGate NGFW. Перед настройкой политик в шаблоне необходимо добавить элементы библиотек. Данные библиотек не синхронизируются: если добавленные элементы не используются в политиках шаблона, то они не будут добавлены в библиотеки UserGate NGFW.

Чтобы настроить параметры шаблона UserGate NGFW:

Перейдите в режим настройки параметров шаблона, выполнив команду:

go ngfw-template <название шаблона>

Например:

```
realmadmin/realm@nodename# go ngfw-template test_template_2
```

Для настройки параметров шаблона вы можете использовать команды, которые приведены в разделе « Интерфейс командной строки» Руководства администратора UserGate NGFW.

Правила политик в шаблоне не переопределяют правила, созданные администраторами межсетевых экранов UserGate NGFW локально, а добавляются к ним в виде преправил и постправил. Подробная информация о создании правил политик приведена в разделе UserGate Policy Language Руководства администратора UserGate NGFW.

Кроме того, при создании правила в шаблоне вы можете указывать позицию правила относительно преправил или постправил в списке, используя свойства mc_pre и mc_post соответственно. Ниже приведен пример создания постправила:

```
realmadmin/realm@nodename# create network-policy firewall 1 upl-rule \
...DENY
...enabled(true)
...src.zone = Trusted
...dst.zone = Untrusted
...user = unknown
...rule_log(session)
...mc_post
...name("Example of post rule name")
```

Созданное правило отобразится на первой позиции списка постправил. Это правило запрещает передачу трафика из зоны Trusted в зону Untrusted неидентифицированным пользователям.

## Создание групп шаблонов UserGate NGFW

После создания шаблонов UserGate NGFW их необходимо объединить в группы. Группа шаблонов позволяет создать единую конфигурацию параметров, которая применяется к одному или нескольким управляемым устройствам. Эта конфигурация формируется в результате слияния параметров всех шаблонов, входящих в группу, с учетом их расположения. В таблице ниже приведены команды, которые вы можете использовать при создании группы шаблонов UserGate NGFW.

| Действие | Команда | Пример ввода команды |
|---|---|---|
| Создание группы | create ngfw groups name <название группы> description <описание группы> templates [ <название шаблона 1> ... <название шаблона n> ] | realmadmin/realm@nodename# create ngfw groups name example_group_1 description for_example_group templates [ example_template_1 ] |
| Изменение названия, описания и набора шаблонов, входящих в группу | set ngfw groups <название группы> name <новое название группы> description <новое описание группы> templates [ <название шаблона 1> ... <название шаблона n> ] | realmadmin/realm@nodename# set ngfw groups example_group_1 name example_group_2 description for_testing_group |
| Добавление шаблонов, входящих в группу | set ngfw groups <название группы> templates [ <название шаблона 1> ... <название шаблона n> ] | realmadmin/realm@nodename# set ngfw groups example_group_2 templates [ example_template_2 ] |
| Удаление шаблонов, входящих в группу | delete ngfw groups <название группы> templates [ <название шаблона 1> ... <название шаблона n> ] | realmadmin/realm@nodename# delete ngfw groups example_group_2 templates [ example_template_2 ] |

| Действие | Команда | Пример ввода команды |
|---|---|---|
| | | |
| Просмотр группы | show ngfw groups <название группы> | realmadmin/realm@nodename# show ngfw groups example_group_2 |
| Просмотр всех групп | show ngfw groups | realmadmin/realm@nodename# show ngfw groups |
| Удаление группы | delete ngfw groups <название группы> | realmadmin/realm@nodename# delete ngfw groups example_group_2 |

После создания групп шаблонов вы можете добавить управляемые устройства.

## Добавление управляемых устройств UserGate NGFW

Под управляемым устройством понимается логический объект, созданный в управляемой области, которому соответствует реальный UserGate NGFW, подключенный к UGMC. Каждый такой объект во включенном состоянии использует одну лицензию на управляемое устройство.

Перед добавлением управляемого устройства UserGate NGFW вам необходимо на сервере UGMC в свойствах зоны, к которой подключен UserGate NGFW, разрешить использование сервиса **UserGate Management Center**.

Для этого под учетной записью администратора UGMC в интерфейсе командной строки в режиме конфигурации выполните команду:

set network zone <название зоны> enabled-services [ Management ]

Например:

Admin/system@nodename# set network zone example_zone enabled-services [ Management ]

Для добавления управляемого устройства UserGate NGFW необходимо:

1) создать устройство в управляемой области UGMC;

2) подключить UserGate NGFW к управляемому устройству.

### Создание управляемого устройства

**Примечание**Инструкция выполняется администратором управляемой области в интерфейсе командной строки UGMC в режиме конфигурации.

Чтобы создать управляемое устройство:

1. Выполните команду:

create ngfw devices <параметры управляемого устройства>

Укажите параметры управляемого устройства.

| Параметр | Описание |
|---|---|
| enabled | Состояние:<br>• on — включено;<br>• off — выключено |
| name | Название |
| description | Описание |
| templates-group | Название группы шаблонов, параметры которой должны применяться к управляемому устройству |
| sync-mode | Режим синхронизации параметров между группой шаблонов и управляемым устройством:<br>• auto — автоматическая синхронизация;<br>• disabled — синхронизация выключена;<br>• manual — запуск синхронизации вручную.<br>В процессе синхронизации к UserGate NGFW применяется конфигурация параметров группы шаблонов. По умолчанию указан автоматический режим. В этом режиме параметры UserGate NGFW синхронизируются с конфигурацией параметров при каждом ее изменении.<br>При необходимости синхронизацию можно отключить. Это может понадобиться, например, если нужно одновременно изменить параметры нескольких шаблонов группы. В этом случае вы можете применить сразу все внесенные изменения, выполнив синхронизацию вручную. Синхронизация для всех управляемых устройств выполняется по команде execute ngfw devices resync (действие доступно в версии 7.4.0 и выше) |

Например:

realmadmin/realm@nodename# create ngfw devices enabled on name example_name templates-group example_group sync-mode auto

2. Получите идентификатор созданного управляемого устройства:

show ngfw devices <название управляемого устройства>

Например:

realmadmin/realm@nodename# show ngfw devices example_name

```
name                    : example_name
enabled                 : on
device-code               : 9W8W14UC
templates-group           : example_group
sync-mode               : auto
...
```

Идентификатор управляемого устройства отобразится в выводе команды в параметре device-code. Этот идентификатор потребуется для подключения межсетевого экрана UserGate NGFW к управляемому устройству.

## Подключение UserGate NGFW к управляемому устройству

Вы можете подключить UserGate NGFW к управляемому устройству при первоначальной настройке продукта, а также при его дальнейшем использовании (см. инструкцию ниже).

**Примечание**Инструкция выполняется администратором UserGate NGFW в интерфейсе командной строки в режиме конфигурации.

Чтобы подключить UserGate NGFW к управляемому устройству:

Выполните команду:

set settings general management-center mc-address <IP-адрес UGMC> device-code <идентификатор управляемого устройства> enabled on

Например:

Admin@ngfw-nodename# set settings general management-center mc-address 192.0.2.4 device-code 9W8W14UC enabled on

Вы можете проверить подключение на стороне UGMC.

**Примечание**Инструкция выполняется администратором управляемой области в интерфейсе командной строки UGMC в режиме конфигурации.

Чтобы проверить подключение UserGate NGFW к управляемому устройству:

Выполните команду:

show ngfw devices <название управляемого устройства>

Например:

realmadmin/realm@nodename# show ngfw devices example_name

Параметры подключения отобразятся в выводе команды.

## Кластеризация UserGate NGFW

UserGate Management Center позволяет объединять межсетевые экраны UserGate NGFW в кластер конфигурации. Используя шаблоны устройств, вы можете применять одинаковые параметры на всех узлах этого кластера. Кроме того, в UGMC вы можете создать один или несколько кластеров отказоустойчивости на базе узлов кластера конфигурации.

## Создание кластера конфигурации

Чтобы создать кластер конфигурации:

1. Выполните первоначальную настройку на первом узле кластера.

2. Настройте на первом узле кластера зону, через интерфейсы которой будет выполняться репликация кластера (см. раздел « Настройки сети» Руководства администратора UserGate NGFW). В параметре enabled-services должны быть указаны значения ha и Admin Console, разрешающие доступ к соответствующим сервисам.

3. Укажите IP-адрес, который будет использоваться для связи первого узла с другими узлами кластера (см. раздел « Настройка кластеров» Руководства администратора UserGate NGFW).

4. Сгенерируйте секретный код для первого узла кластера (см. раздел « Настройка кластеров» Руководства администратора UserGate NGFW).

5. Подключите первый узел кластера к UGMC в качестве управляемого устройства. При подключении к UGMC каждому узлу кластера присваивается уникальный идентификатор вида node_n, где n — порядковый номер узла.

6. Добавьте в кластер конфигурации второй и последующие узлы, выполнив первоначальную настройку на каждом узле.

7. Настройте параметры узлов кластера. Вы можете выполнить настройку локально на каждом узле или настроить параметры в шаблонах UGMC.

## Создание кластера отказоустойчивости

Узлы кластера конфигурации могут быть объединены в кластер отказоустойчивости, поддерживающий режимы:

- «активный — активный», в котором один из межсетевых экранов выступает в роли мастер-узла, распределяющего трафик на все остальные узлы кластера;
- «активный — пассивный», в котором один из межсетевых экранов выступает в роли мастер-узла, обрабатывающего транзитный трафик пользователей, а остальные — в качестве резервных, которые находятся в состоянии готовности начать обработку трафика.

Перед созданием кластера отказоустойчивости нужно проверить, что:

- Создан кластер конфигурации.
- На каждом из узлов кластера созданы сетевые интерфейсы, управляемые UGMC. Вы можете назначать виртуальные IP-адреса только интерфейсам, созданным в шаблоне.
- Выполняются требования аналогичные тем, которые предъявляются к узлам при создании кластера отказоустойчивости без использования UGMC (см. раздел « Кластеризация и отказоустойчивость» Руководства администратора UserGate NGFW).

**Примечание**Перед выполнением инструкции должны быть созданы шаблон сетевых зон и шаблон кластера отказоустойчивости. Инструкция выполняется администратором управляемой области в интерфейсе командной строки UGMC в режиме конфигурации.

Чтобы создать кластер отказоустойчивости:

1. Разрешите сервис VRRP для всех сетевых зон, где планируется добавлять кластерный виртуальный IP-адрес, последовательно выполнив команды:

go ngfw-template <название шаблона сетевых зон>

set network zone name <название зоны> enabled-services [ VRRP ]

Например:

realmadmin/realm@nodename# go ngfw-template template_for_zones

realmadmin/realm@nodename# set network zone name zone_name enabled-services [ VRRP ]
Template: template_for_zones

2. Настройте параметры кластера отказоустойчивости, последовательно выполнив команды:

go ngfw-template <название шаблона кластера отказоустойчивости>

create settings device-mgmt ha-clusters <параметры кластера отказоустойчивости>

Укажите параметры кластера отказоустойчивости.

| Параметр | Описание |
|---|---|
| enabled | Состояние:<br>• on — включен;<br>• off — выключен |
| name | Название |
| description | Описание |
| mode | Режим работы:<br>• active-active — «активный — активный»;<br>• active-passive — «активный — пассивный» |

| Параметр | Описание |
| --- | --- |
| session-sync | Режим синхронизации пользовательских TCP-сессий:<br>• on — синхронизация включена;<br>• off — синхронизация выключена;<br>• ha-cluster-id: <идентификатор кластера отказоустойчивости> — если в одном кластере конфигурации создано несколько кластеров отказоустойчивости, то выполняется автоматическая синхронизация сессий с использованием мультикастового адреса (кроме сессий, использующих прокси-сервер).<br>Идентификатор кластера отказоустойчивости — уникальное для каждого кластера значение от 0 до 8 |
| session-sync-all | Режим синхронизации всех пользовательских сессий:<br>• on — синхронизация включена;<br>• off — синхронизация выключена |
| excluded-sync-ips | IP-адреса, с которыми не будут синхронизироваться пользовательские сессии |
| virtual-router-id | Идентификатор виртуального маршрутизатора (VRID). Уникален для каждого VRRP-кластера в локальной сети. Если в сети нет сторонних VRRP-кластеров рекомендуется оставить значение по умолчанию |
| nodes | Названия узлов кластера конфигурации для их объединения в кластер отказоустойчивости |
| virtual-ips <virtual-ips-filter> <virtual-ip-info> | Виртуальные IP-адреса кластера и их назначение сетевым интерфейсам на узлах кластера.<br>Параметр virtual-ips-filter может принимать значения:<br>• new — создание нового виртуального IP-адреса;<br>• <IP-адрес> — изменение существующего виртуального IP-адреса.<br>Параметр virtual-ip-info может принимать значения:<br>• ip <IP-адрес/маска подсети> — назначение виртуального IP-адреса интерфейсу;<br>• ha-interfaces <название узла кластера/название интерфейса> — выбор интерфейса на узле кластера |

Version: 7.x
Product: UGMC

Начиная с версии 7.5.0 в интерфейсе командной строки UserGate Management Center (UGMC) администраторы управляемой области могут централизованно управлять подключенными UserGate DCFW. Для этого в режиме конфигурации необходимо выполнить следующее:

1) настроить параметры шаблонов UserGate DCFW;

2) создать группу шаблонов UserGate DCFW;

3) настроить интеграцию UserGate DCFW с UGMC.

Подробнее об объектах, используемых в управляемой области UGMC, таких как шаблоны, группы шаблонов и управляемые устройства — в разделе «Шаблоны и группы шаблонов».

## Настройка параметров шаблонов UserGate DCFW

Перед настройкой параметров шаблонов UserGate DCFW необходимо создать шаблоны устройств. Рекомендуется создавать отдельные шаблоны для разных категорий параметров, например такие, как шаблон сетевых параметров или шаблон библиотек. Это упростит дальнейшую работу с шаблонами при их объединении в группы.

В таблице ниже приведены команды, которые вы можете использовать при создании шаблонов UserGate DCFW.

| Действие | Команда | Пример ввода команды |
|---|---|---|
| Создание шаблона | create dcfw template name <название шаблона> description <описание шаблона> | realmadmin/realm@nodename# create dcfw template name "example template 1" description "for example template" |
| Просмотр шаблона | show dcfw template <название шаблона> | realmadmin/realm@nodename# show dcfw template "example template 1" |
| Просмотр всех шаблонов | show dcfw template | realmadmin/realm@nodename# show dcfw template |
| Изменение названия и описания шаблона | set dcfw template <название шаблона> name <новое название шаблона> description <новое описание шаблона> | realmadmin/realm@nodename# set dcfw template "example template 1" name "example template 2" description "for testing templete" |
| Удаление шаблона | delete dcfw template <название шаблона> | realmadmin/realm@nodename# delete dcfw template "test template 2" |

После создания шаблона вы можете перейти к настройке его параметров. Параметры шаблона распространятся на все управляемые устройства UserGate DCFW, к которым будет применен шаблон в составе группы.

При настройке параметров шаблона UserGate DCFW следует учитывать следующее:

- Значения параметров в шаблоне имеют более высокий приоритет, чем указанные администратором UserGate DCFW локально. Если значение параметра не указано ни в шаблоне, ни на стороне UserGate DCFW, будет использоваться значение по умолчанию.
- После применения шаблона к управляемым устройствам администраторы могут изменять базовые параметры и параметры сетевых интерфейсов локально на каждом UserGate DCFW. Подробная информация об этих параметрах приведена в разделах «Настройка устройства» и «Интерфейсы» Руководства администратора UserGate DCFW.
- При настройке параметров сетевых интерфейсов в шаблоне невозможно конфигурировать интерфейс port0. Первым физическим интерфейсом, доступным для настройки в шаблоне, будет port1.

  Параметры интерфейса port0 настраиваются администратором UserGate DCFW при первоначальной настройке продукта. По умолчанию этот интерфейс используется для подключения UserGate DCFW к UGMC.

  При необходимости можно сконфигурировать сетевые интерфейсы локально на UserGate DCFW, для этого в параметрах интерфейса шаблона должно быть указано свойство on-device (или on-device on).

  Если вы создаете интерфейс в шаблоне, этот интерфейс автоматически будет добавлен в UserGate DCFW. Удаление интерфейса из шаблона не удаляет интерфейс на межсетевом экране. Если требуется удалить интерфейс на межсетевом экране, необходимо сделать это вручную.
- Библиотеки элементов шаблона (например, библиотеки IP-адресов, URL-списков, а также типов контента) по умолчанию не содержат данных, в отличие от библиотек UserGate DCFW (подробнее — в разделе «Библиотеки элементов» Руководства администратора UserGate DCFW). Перед настройкой политик в шаблоне необходимо добавить элементы библиотек.

  **Важно!**Данные библиотек не синхронизируются: если добавленные элементы не используются в политиках шаблона, они не будут добавлены в библиотеки UserGate DCFW. Поэтому, чтобы на управляемых устройствах отображались, например, списки IP-адресов, созданные в шаблоне, необходимо предварительно добавить эти списки в правила политик шаблона.
  **Примечание**Корректность работы проприетарных сигнатур СОВ и приложений зависит от актуальности библиотек для этих сигнатур — рекомендуется проверять актуальность библиотек после обновления UGMC или восстановления его параметров. Если по какой-либо причине библиотеки не обновились автоматически, их можно обновить вручную. Действие выполняется администратором UGMC в разделе «Центр управления» ➜ «Настройки» ➜ «Обновления библиотек».

Чтобы настроить параметры шаблона UserGate DCFW:

Перейдите в режим настройки параметров шаблона, выполнив команду:

go dcfw-template <название шаблона>

Например:

```
realmadmin/realm@nodename# go dcfw-template "test template 2"
```

Для настройки параметров шаблона вы можете использовать команды, которые приведены в разделе «Интерфейс командной строки» Руководства администратора UserGate DCFW.

**Примечание**Вы можете выйти из режима настройки параметров шаблона, выполнив команду go realm-settings.

Правила политик в шаблоне не переопределяют правила, созданные администраторами межсетевых экранов UserGate DCFW локально, а добавляются к ним в виде преправил и постправил. Подробная информация о создании правил политик межсетевых экранов UserGate приведена в разделе UserGate Policy Language Руководства администратора UserGate NGFW.

Кроме того, при создании правила в шаблоне вы можете указывать позицию правила относительно преправил или постправил в списке, используя свойства mc_pre и mc_post соответственно. Ниже приведен пример создания постправила.

```
realmadmin/realm@nodename# create network-policy firewall 1 upl-rule \
...DENY
...enabled(true)
...src.zone = Trusted
...dst.zone = Untrusted
...user = unknown
...rule_log(session)
...mc_post
...name("Example of post rule name")
```

Созданное правило отобразится на первой позиции списка постправил. Это правило запрещает передачу трафика из зоны Trusted в зону Untrusted неидентифицированным пользователям.

## Создание групп шаблонов UserGate DCFW

После создания шаблонов UserGate DCFW их необходимо объединить в группы. Группа шаблонов позволяет создать единую конфигурацию параметров, которая применяется к одному или нескольким управляемым устройствам. Эта конфигурация формируется в результате слияния параметров всех шаблонов, входящих в группу, с учетом их расположения.

В таблице ниже приведены команды, которые вы можете использовать при создании группы шаблонов UserGate DCFW.

| Действие | Команда | Пример ввода команды |
|---|---|---|

| Действие | Команда | Пример ввода команды |
|---|---|---|
| Создание группы | create dcfw groups name <название группы> description <описание группы> templates [ <название шаблона 1> ... <название шаблона n> ] | realmadmin/realm@nodename# create dcfw groups name "example group 1" description "for example group" templates [ "example template 1" ] |
| Изменение названия, описания и набора шаблонов, входящих в группу | set dcfw groups <название группы> name <новое название группы> description <новое описание группы> templates [ <название шаблона 1> ... <название шаблона n> ] | realmadmin/realm@nodename# set dcfw groups "example group 1" name "example group 2" description "for testing group" |
| Добавление шаблонов, входящих в группу | set dcfw groups <название группы> templates [ <название шаблона 1> ... <название шаблона n> ] | realmadmin/realm@nodename# set dcfw groups "example group 2" templates [ "example template 2" "example template 3" ] |
| Удаление шаблонов, входящих в группу | delete dcfw groups <название группы> templates [ <название шаблона 1> ... <название шаблона n> ] | realmadmin/realm@nodename# delete dcfw groups "example group 2" templates [ "example template 2" ] |
| Просмотр группы | show dcfw groups <название группы> | realmadmin/realm@nodename# show dcfw groups "example group 2" |
| Просмотр всех групп | show dcfw groups | realmadmin/realm@nodename# show dcfw groups |
| Удаление группы | delete dcfw groups <название группы> | realmadmin/realm@nodename# delete dcfw groups "example group 2" |

Шаблоны применяются в порядке их расположения в группе. Вы можете изменять позицию шаблона с помощью следующих параметров.

| Параметр | Описание | Пример ввода команды |
|---|---|---|
| edge-position | Перемещение шаблона:<br>• top — в начало группы;<br>• bottom — в конец группы | realmadmin/realm@nodename# set dcfw groups "example group 2" templates [ "example template 2" ] edge-position top |
| after | Перемещение шаблона на одну позицию после другого шаблона | realmadmin/realm@nodename# set dcfw groups "example group 2" templates [ "example template 2" ] after "example template 3" |
| before | Перемещение шаблона на одну позицию перед другим шаблоном | realmadmin/realm@nodename# set dcfw groups "example group 2" templates [ "example template 2" ] before "example template 3" |

После создания группы шаблонов вы можете перейти к настройке интеграции UserGate DCFW с UGMC.

## Настройка интеграции UserGate DCFW с UGMC

Настройка интеграции с UGMC осуществляется путем создания в управляемой области логического объекта — устройства, к которому будут привязаны реальные UserGate DCFW при их подключении к UGMC. Каждый такой логический объект во включенном состоянии использует одну лицензию на управляемое устройство.

С помощью одного устройства, созданного в управляемой области, вы можете настроить интеграцию с UGMC одиночного UserGate DCFW или кластера межсетевых экранов. Для UserGate DCFW, объединенных в кластер, достаточно подключить к UGMC первый узел, остальные узлы будут подключены автоматически при их добавлении в кластер.

Для настройки интеграции UserGate DCFW с UGMC необходимо:

1) создать устройство в управляемой области;

2) подключить UserGate DCFW к UGMC.

Все UserGate DCFW, для которых настроена интеграция с UGMC, называются управляемыми устройствами.

## Создание устройства в управляемой области

**Примечание**Инструкция ниже выполняется администратором управляемой области в интерфейсе командной строки UGMC в режиме конфигурации.

Чтобы создать устройство в управляемой области:

1. Выполните команду:

create dcfw devices <параметры устройства>

Укажите параметры устройства.

| Параметр | Описание |
|---|---|
| enabled | Состояние:<br>• on — включено;<br>• off — выключено |
| name | Название |
| description | Описание |
| templates-group | Название группы шаблонов, параметры которой должны применяться к подключенным UserGate DCFW |
| sync-mode | Режим синхронизации параметров между группой шаблонов и подключенными UserGate DCFW:<br>• auto — автоматическая синхронизация;<br>• disabled — синхронизация выключена;<br>• manual — запуск синхронизации вручную.<br>В процессе синхронизации к управляемым устройствам применяется конфигурация параметров группы шаблонов. По умолчанию указан автоматический режим. В этом режиме параметры UserGate DCFW синхронизируются с конфигурацией параметров при каждом ее изменении.<br>При необходимости синхронизацию можно отключить. Это может понадобиться, например, если нужно одновременно изменить параметры нескольких шаблонов группы. В этом случае вы можете применить сразу все внесенные изменения, выполнив синхронизацию вручную. Синхронизация для всех управляемых устройств выполняется с помощью команды execute dcfw devices resync |

Например:

realmadmin/realm@nodename# create dcfw devices enabled on name "example name" templates-group "example group" sync-mode auto

2. Получите код для подключения созданного устройства к UGMC:

show dcfw devices <название управляемого устройства>

Например:

realmadmin/realm@nodename# show dcfw devices "example name"

```
name                    : example name
enabled                 : on
device-code               : 9W8W14UC
templates-group           : example group
sync-mode               : auto
...
```

Код для подключения межсетевого экрана UserGate DCFW к UGMC отобразится в выводе команды в параметре device-code.

## Подключение UserGate DCFW к UGMC

Вы можете подключить UserGate DCFW к UGMC при первоначальной настройке межсетевого экрана, а также при его дальнейшем использовании (см. инструкцию ниже).

Перед выполнением инструкции необходимо в свойствах зоны для подключения UserGate DCFW разрешить использование сервиса **UserGate Management Center**. Для этого под учетной записью администратора UGMC в интерфейсе командной строки в режиме конфигурации выполните команду:

set network zone <название зоны> enabled-services [ Management ]

Например:

Admin/system@nodename# set network zone "example zone" enabled-services [ Management ]

**Примечание**Инструкция выполняется администратором UserGate DCFW в интерфейсе командной строки в режиме конфигурации.

Чтобы подключить UserGate DCFW к UGMC:

Выполните команду:

set settings general management-center mc-address <IP-адрес UGMC> device-code <код для подключения, сгенерированный в UGMC> enabled on

Например:

Admin@dcfw-nodename# set settings general management-center mc-address 192.0.2.4 device-code 9W8W14UC enabled on

Вы можете проверить подключение на стороне UGMC.

**Примечание**Инструкция выполняется администратором управляемой области в интерфейсе командной строки UGMC в режиме конфигурации.

Чтобы проверить подключение UserGate DCFW к UGMC:

Выполните команду:

show dcfw devices <название устройства, созданного в управляемой области>

Например:

realmadmin/realm@nodename# show dcfw devices "example name"

Параметры подключения отобразятся в выводе команды.

## Кластеризация UserGate DCFW

Вы можете объединять два или более UserGate DCFW (узлов) в кластер конфигурации и настраивать на них единые параметры для работы с трафиком, используя шаблоны.

Между узлами кластера конфигурации выполняется синхронизация параметров, что обеспечивает бесперебойную фильтрацию и обработку сетевого трафика при недоступности одного из узлов.

Кроме того, вы можете объединять до четырех узлов кластера конфигурации в кластер отказоустойчивости. Этот кластер поддерживает следующие режимы работы:

- «активный — активный», в котором один из межсетевых экранов выполняет роль основного узла, распределяя трафик на все остальные узлы кластера;
- «активный — пассивный», в котором обработку транзитного трафика выполняет основной узел, при сбоях в работе этого узла трафик перенаправляется на резервные узлы кластера.

В параметрах кластера отказоустойчивости вы можете настроить синхронизацию сессий между узлами (исключение составляют сессии, использующие прокси-сервер). Это может понадобиться для кластера в режиме «активный — пассивный», например при недоступности основного узла вы можете переключиться на резервный узел без потери установленных сессий.

На базе одного кластера конфигурации может быть создано несколько кластеров отказоустойчивости. В этом случае каждому кластеру отказоустойчивости вы можете присвоить уникальный мультикаст-идентификатор, который будет использоваться для синхронизации сессий между узлами.

## Создание кластера конфигурации

Чтобы создать кластер конфигурации:

1. Выполните первоначальную настройку на первом узле кластера.

2. Настройте на первом узле кластера зону, через интерфейсы которой будет выполняться репликация параметров между узлами кластера (см. раздел « Настройки сети» Руководства администратора UserGate DCFW). В параметре enabled-services должны быть указаны значения ha и Admin Console, разрешающие доступ к соответствующим сервисам.

3. Укажите IP-адрес, который будет использоваться для связи первого узла с другими узлами кластера (см. раздел « Настройка кластеров» Руководства администратора UserGate DCFW).

4. Сгенерируйте секретный код для первого узла кластера (см. раздел « Настройка кластеров» Руководства администратора UserGate DCFW).

5. Подключите первый узел кластера к UGMC. В результате подключения узлу будет автоматически присвоен идентификатор node_1.

6. Добавьте дополнительные узлы в кластер конфигурации, выполнив первоначальную настройку на каждом из них. В результате на дополнительные узлы кластера будут автоматически реплицированы параметры, настроенные на первом узле.

## Создание кластера отказоустойчивости

Перед созданием кластера отказоустойчивости:

1. Создайте кластер конфигурации (см. инструкцию выше).

2. Проверьте, что:

- Выполняются требования аналогичные тем, что предъявляются к узлам при создании кластера отказоустойчивости без использования UGMC (см. раздел « Кластеризация и отказоустойчивость» Руководства администратора UserGate DCFW).
- На каждом из узлов кластера созданы сетевые интерфейсы, управляемые UGMC. Вы можете назначать виртуальные IP-адреса только тем интерфейсам, которые созданы в шаблоне.

**Примечание**Перед выполнением инструкции необходимо убедиться, что созданы шаблон сетевых зон и шаблон кластера отказоустойчивости. Инструкция ниже выполняется администратором управляемой области в интерфейсе командной строки UGMC в режиме конфигурации.

Чтобы создать кластер отказоустойчивости:

1. В режиме настройки параметров шаблона сетевых зон разрешите доступ к сервису VRRP тем зонам, для которых планируете добавлять кластерный виртуальный IP-адрес. Для этого последовательно выполните команды:

go dcfw-template <название шаблона сетевых зон>

set network zone name <название зоны> enabled-services [ VRRP ]

Например:

realmadmin/realm@nodename# go dcfw-template "template for zones"

realmadmin/realm@nodename# set network zone name "example zone name" enabled-services [ VRRP ]
Template: template for zones

**Примечание**Вы можете выйти из режима настройки параметров шаблона, выполнив команду go realm-settings.

2. Настройте параметры кластера отказоустойчивости, последовательно выполнив команды:

go dcfw-template <название шаблона кластера отказоустойчивости>

create settings device-mgmt ha-clusters <параметры кластера отказоустойчивости>

Укажите параметры кластера отказоустойчивости.

| Параметр | Описание |
|---|---|
| enabled | Состояние:<br>• on — включен;<br>• off — выключен |
| name | Название |
| description | Описание |
| mode | Режим работы:<br>• active-active — «активный — активный»;<br>• active-passive — «активный — пассивный» |
| session-sync | Режим синхронизации пользовательских TCP-сессий:<br>• on — синхронизация включена;<br>• off — синхронизация выключена;<br>• ha-cluster-id: <мультикаст-идентификатор кластера отказоустойчивости> — если в локальной сети присутствуют другие отказоустойчивые кластеры, можно указать уникальный мультикаст-идентификатор создаваемого кластера (значение от 0 до 8), который будет использоваться для синхронизации сессий между узлами |
| session-sync-all | Режим синхронизации всех пользовательских сессий, включая UDP- и ICMP-трафик:<br>• on — синхронизация включена;<br>• off — синхронизация выключена |
| excluded-sync-ips | IP-адреса, привязанные к тем пользовательским сессиям, которые требуется исключить из синхронизации |
| virtual-router-id | Идентификатор виртуального маршрутизатора (VRID) уникальный для каждого VRRP-кластера в локальной сети. Если в сети отсутствуют сторонние VRRP-кластеры, рекомендуется оставить значение по умолчанию |
| nodes | Идентификаторы узлов кластера конфигурации, которые требуется объединить в кластер отказоустойчивости |
| virtual-ips <virtual-ips-filter> <virtual-ip-info> | Назначение виртуальных IP-адресов интерфейсам на узлах кластера отказоустойчивости.<br>Параметр virtual-ips-filter может принимать значения:<br>• new — создание нового виртуального IP-адреса;<br>• <IP-адрес> — изменение существующего виртуального IP-адреса.<br>Параметр virtual-ip-info может принимать значения:<br>• ip <IP-адрес / маска подсети> — назначение виртуального IP-адреса интерфейсу;<br>• ha-interfaces <название узла кластера / название интерфейса> — выбор интерфейса на узле кластера |

Version: 7.x
Product: UGMC
Documentation: ☑

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 и групп шаблонов, а также 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 шаблонов 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.

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

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;
- 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. |
| **description** | Описание управляемого устройства. |

| Наименование | Описание |
|---|---|
| **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:<br>• **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.<br>• **disabled** — синхронизация выключена.<br>• **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>

Для запуска вручную синхронизации всех настроек управляемых устройств предназначена команда (доступно в версии ПО 7.4.0 и выше):

realmadmin/realm@nodename# execute logan devices resync

## 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 репозиторий 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 репозиторий 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 репозиторием. Репозиторий UserGate при этом будет использован сервером UGMC для получения новых обновлений. По умолчанию UGMC проверяет и скачивает обновления библиотек автоматически.

Библиотеки, находящиеся в репозитории 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 репозитория UserGate используется следующая команда:

realmadmin/realm@nodename#set logan libraries-updates <library-name> download <auto/manual>

Version: 7.x
Product: UGMC

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:<br>• **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.).<br>Значение по умолчанию: enabled.<br>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.<br>Важно! Отключение сбора информации о конечном устройстве влияет на работу профилей HIP.<br>• **network-access**: настройка сетевого доступа при остановленном ПО UserGate Client.<br>Значение по умолчанию: enabled.<br>• **firewall-access**: разрешение пользователю самостоятельно, используя графический интерфейс, отключать контентную фильтрацию на конечном устройстве:<br>◦ **off** — не разрешать самостоятельно отключать контентную фильтрацию.<br>◦ **on** — разрешить самостоятельно отключать контентную фильтрацию.<br>◦ **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).<br>При разрешении пользователю отключать фильтрацию самостоятельно можно указать количество разрешённых отключений (number-of-shutdowns) и/или время, на которое фильтрация будет отключена (duration).<br>Значение по умолчанию: on (отключение фильтрации на 10 минут без использования кода).<br>Важно! В случае использования счётчика количества отключений: если внести изменения в настройки разрешения отключения межсетевого экрана, то счётчик на конечном устройстве обнулится.<br>• **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.<br>Значение по умолчанию: enabled.<br>**Важно!**Настройки не будут применены, если не включена синхронизация (параметр sync on). Иначе будут использованы значения по умолчанию. |
| **notification** | Настройка оповещений:<br>• **show-icons**: отображение иконки UserGate Client в области уведомлений на панели задач.<br>• **notification-tooltips**: включение/отключение отправки оповещений на конечное устройство.<br>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).<br>• **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.<br>• **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.<br>• **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.<br>**Важно!**Настройки не будут применены, если не включена синхронизация (параметр 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.<br>**Важно!**Настройки не будут применены, если не включена синхронизация (параметр 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 (FQDN) или IP-адрес VPN-сервера.<br>**Примечание**При использовании FQDN для подключения, если имени VPN-сервера соответствует несколько IP-адресов, клиент устанавливает соединение по первому адресу, который отвечает на запросы. |
| **protocol** | VPN-протоколы для создания туннеля:<br>• **ipsec2**. Для создания туннелей используется протокол Layer 2 Tunnelling Protocol (L2TP), а для защиты передаваемых данных — протокол IPsec.<br>• i**kev2-with-certificate**. Для создания защищенного канала будет использоваться протокол IKEv2, а для взаимной проверки подлинности сервера и клиента — сертификаты.<br>**Важно!** При генерации клиентского сертификата обязательно должно быть указано поле CN — идентификатор пользователя, которому этот сертификат предназначается.<br>• **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 протокола IPsec L2TP): main, aggressive.<br>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. |
| Фаза 1 | Во время первой фазы происходит согласование защиты IKE. Аутентификация происходит на основе общего ключа в режиме, выбранном ранее. Необходимо указать следующие параметры:<br>• **phase1-key-lifetime** - по истечению данного времени происходят повторные аутентификация и согласование настроек первой фазы.<br>• **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.<br>• **dpd-max-failures** - максимальное количество запросов обнаружения недоступных IPsec-соседей, которое необходимо отправить до того, как IPsec-сосед будет признан недоступным.<br>• **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.<br>• **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:<br>• **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.<br>• **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.<br>• **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 команда:

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:<br>• **very-low** — очень низкий уровень угрозы.<br>• **low** — низкий уровень угрозы.<br>• **medium** — средний уровень угрозы.<br>• **high** — высокий уровень угрозы.<br>• **very-high** — высокий уровень угрозы. |
| **type** | Тип списка:<br>• **local** — локальный.<br>• **updatable** — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления ( **url**). Периодичность обновления списка указывается параметром **shedule** в формате crontab.<br>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:<br>• Звездочка (*) — обозначает весь диапазон (от первого до последнего).<br>• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.<br>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".<br>• 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:<br>• **very-low** — очень низкий уровень угрозы.<br>• **low** — низкий уровень угрозы.<br>• **medium** — средний уровень угрозы.<br>• **high** — высокий уровень угрозы.<br>• **very-high** — высокий уровень угрозы. |

| Параметр | Описание |
|---|---|
| **type** | Тип списка:<br>• **local** — локальный.<br>• **updatable** — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления ( **url**). Периодичность обновления списка указывается параметром **shedule** в формате crontab.<br>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:<br>• Звездочка (*) — обозначает весь диапазон (от первого до последнего).<br>• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.<br>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".<br>• 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:<br>• **local** — локальный.<br>• **updatable** — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления ( **url**). Периодичность обновления списка указывается параметром **shedule** в формате crontab.<br>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:<br>• Звездочка (*) — обозначает весь диапазон (от первого до последнего).<br>• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.<br>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".<br>• 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:<br>• **sensitive** — чувствительно к регистру букв в адресе.<br>• **insensitive** — нечувствительно к регистру букв в адресе.<br>• **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. |
| **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:<br>• **local** — локальный.<br>• **updatable** — если список является обновляемым, то необходимо указать адрес, с которого загружаются обновления ( **url**). Периодичность обновления списка указывается параметром **shedule** в формате crontab.<br>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:<br>• Звездочка (*) — обозначает весь диапазон (от первого до последнего).<br>• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.<br>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".<br>• 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** | 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.<br>• **type** — тип интервала повторения:<br>◦ **daily** — ежедневно:<br>▪ **time-from** — время начала (указывается в формате HH:MM).<br>▪ **time-to** — время окончания (указывается в формате HH:MM).<br>▪ **all-day on** — весь день.<br>◦ **weekly** — каждую неделю:<br>▪ **time-from** — время начала (указывается в формате HH:MM).<br>▪ **time-to** — время окончания (указывается в формате HH:MM).<br>▪ **all-day on** — весь день.<br>▪ **days [ Mon** \| **Tue** \| **Wed** \| **Thu** \| **Fri** \| **Sat** \| **Sun ]** — дни недели.<br>◦ **monthly** — каждый месяц:<br>▪ **time-from** — время начала (указывается в формате HH:MM).<br>▪ **time-to** — время окончания (указывается в формате HH:MM).<br>▪ **all-day on** — весь день.<br>▪ **days** — числа месяца (от 1 до 31).<br>◦ **fixed** — единовременно:<br>▪ **time-from** — время начала (указывается в формате HH:MM).<br>▪ **time-to** — время окончания (указывается в формате HH:MM).<br>▪ **all-day on** — весь день.<br>▪ **fixed-date** — нужная дата (указывается в формате YYYY-MM-DD).<br>◦ **span** — повторяющиеся события:<br>▪ **time-from** — время начала (указывается в формате HH:MM).<br>▪ **time-to** — время окончания (указывается в формате HH:MM).<br>▪ **all-day on** — весь день.<br>▪ **fixed-date-from** — дата начала (указывается в формате YYYY-MM-DD).<br>▪ **fixed-date-to** — дата окончания (указывается в формате YYYY-MM-DD).<br>◦ **range** — диапазон дат:<br>▪ **time-from-enabled <on** \| **off>** — включение/отключение указания даты начала интервала.<br>▪ **fixed-date-from** — дата начала (указывается в формате YYYY-MM-DD).<br>▪ **time-from** — время начала (указывается в формате HH:MM).<br>▪ **time-to-enabled <on** \| **off>** — включение/отключение указания даты окончания интервала.<br>▪ **fixed-date-to** — дата окончания (указывается в формате YYYY-MM-DD).<br>▪ **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. |
| **licensed** | Лицензирование конечного устройства: on/off. Если on, то он использует одну лицензию.<br>В случае отсутствия лицензии конечное устройство не сможет подключиться к UGMC.<br>Если параметр будет поставлен в off после регистрации устройства на UGMC, то:<br>• правила межсетевого экрана, полученные от MC ранее, продолжают работать;<br>• подключение по VPN с настройками, полученными ранее от MC доступно;<br>• 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 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.

Для запуска вручную синхронизации всех настроек управляемых устройств предназначена команда (доступно начиная с релиза ПО 7.4.0):

realmadmin/realm@nodename# execute endpoint devices resync

### 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.<br>При использовании операторов = и != необходимо указывать полную версию Windows. |
| **ug-client-version** | Версия ПО UserGate Client. |
| **security** | Статусы компонентов безопасности конечного устройства:<br>• firewall — межсетевой экран;<br>• virus-protection — Антивирус;<br>• automatic-update — Автоматическое обновление;<br>• bitlocker.<br>Важно! BitLocker считается включенным, если он включен хотя бы на одном из дисков. |
| **products** | Проверка соответствия программного обеспечения, установленного на конечном устройстве:<br>• antimalware. Проверка соответствия антивирусного ПО на устройстве пользователя.<br>◦ enabled: проверка статуса ПО;<br>◦ database-updated: проверка актуальности баз (да, нет, не проверять);<br>◦ version ПО;<br>◦ vendor: производитель и название продукта.<br>• firewall. Проверка соответствия межсетевого экрана на конечном устройстве. При настройке необходимо указать:<br>◦ installed: проверка наличия установленного ПО;<br>◦ enabled: проверка статуса ПО (да, нет, не проверять);<br>◦ version ПО;<br>◦ vendor: производитель и название продукта;<br>• backup. Проверка ПО для резервного копирования:<br>◦ installed: проверка наличия установленного ПО;<br>◦ version ПО;<br>◦ vendor: производитель и название продукта.<br>• disk-encryption. Проверка установленных на конечном устройстве программ для шифрования диска:<br>◦ installed: проверка наличия установленного ПО;<br>◦ version ПО;<br>◦ vendor: производитель и название продукта.<br>• dlp. Проверка соответствия системы предотвращения утечек информации.<br>◦ installed: проверка наличия установленного ПО;<br>◦ version ПО;<br>◦ vendor: производитель и название продукта.<br>• patch-management. Проверка актуальности обновления.<br>◦ installed: проверка наличия установленного ПО;<br>◦ version ПО;<br>◦ 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.<br>Поддерживаются следующие типы параметров реестра:<br>• REG_SZ: строка Unicode или ANSI с нулевым символом в конце.<br>• REG_BINARY: двоичные данные в любой форме.<br>• REG_DWORD: 32-разрядное число.<br>Доступна проверка ключей следующих разделов реестра:<br>• HKEY_LOCAL_MACHINE<br>• HKEY_USERS<br>Важно! Путь указывается с использованием обратного слэша (\), например, \HKEY_LOCAL_MACHINE, после которых через (\) указывается полный путь к параметру.<br>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). |
| **hip-objects** | Выбор логического элемента (and, or, and-not, or-not) и объектов HIP.<br>Подробнее о HIP-объектах — в разделе «Настройка проверки требований безопасности (HIP )» |

**Admin**

**Настройка учетной записи администратора**

Product: UserGate MC
Version: 7.x

Вы можете изменить параметры учетной записи, используемой для входа в UGMC: сменить пароль или настроить предпочтения при работе с веб-интерфейсом.

Кроме того, вы можете завершить текущий сеанс работы, нажав в главном меню UGMC на логин вашей учетной записи и выбрав **Выход**.

## Смена пароля учетной записи администратора

В целях безопасности вы можете сменить пароль вашей учетной записи. Подробнее об учетных записях администраторов — в разделе «Администраторы».

Чтобы сменить пароль учетной записи администратора:

1. В главном меню UGMC нажмите на логин вашей учетной записи и выберите **Сменить пароль**.
2. Введите старый пароль.
3. Дважды введите новый пароль.
4. Нажмите **Сохранить**.

## Настройка предпочтений при работе с веб-интерфейсом

Для удобства работы с веб-интерфейсом UGMC вы можете настроить ваши предпочтения.

Чтобы настроить предпочтения при работе с веб-интерфейсом UGMC:

1. В главном меню UGMC нажмите на логин вашей учетной записи и выберите **Предпочтения**.
2. Если необходимо, измените значения следующих параметров:
   - **Количество элементов на странице** — количество записей, отображаемых на одной странице с табличными данными (например, на странице с правилами межсетевого экрана).
   - **Макс. время ожидания ответа** — время ожидания ответа сервера UGMC. Значение параметра по умолчанию — 120 секунд. Если по истечении этого времени ответ от сервера не будет получен, выполняемая операция завершится ошибкой. Параметр доступен начиная с версии 7.5.0.

     Вы можете увеличить время ожидания ответа сервера UGMC для операций, которые требуют длительной обработки (например, поиск правила по параметрам, если количество правил межсетевого экрана превышает 1000). Следует учитывать, что длительное ожидание увеличивает нагрузку на сервер продукта, а также замедляет выполнение операции в случае возникновения ошибок при ее обработке.
   - **Ночной режим** — тема оформления веб-интерфейса. Для выбора темной темы установите флажок.
3. Нажмите **Сохранить**.

Для применения изменений страница веб-интерфейса UGMC будет перезагружена.

**Приложения**

**Требования к сетевому окружению**

Documentation: ☑
Product: UGMC
Version: 7.x

| 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. |
| **XML-RPC поверх HTTPS** | TCP | 4443 | Входящий (к UserGate по API) | Доступ к API поверх HTTPS. |
| **Удалённый помощник** | TCP | 22 | Исходящий (до серверов технической поддержки) | Удалённый доступ к серверу технической поддержки.<br>Доступ к серверам:<br>• 93.91.171.46;<br>• 178.154.221.222;<br>• ra.entensys.com. |
| **NTP** | UDP | 123 | Исходящий (до сервера точного времени) | Синхронизация времени. |
| **DNS** | UDP | 53 | Исходящий (от UserGate до DNS-сервера) | Сервис получения информации (IP-адрес) о доменах. |
| **Регистрация сервера UserGate** | TCP | 443 | Исходящий (до сервера регистрации) | Доступ до сервера регистрации продуктов UserGate reg2.usergate.com. |
| **Обновление ПО и библиотек** | TCP | 443 | Исходящий (до серверов обновления) | Обновление программного обеспечения и элементов библиотек: доступ до сервера updates.usergate.com. |
| **Репликация настроек** | TCP | 4369 | Входящий (с первого узла кластера на второй и последующие узлы) | Сервис, необходимый для работы кластера конфигурации.<br>Установка управляющего соединения. |
| | | 9000-9100 | Входящий (приём конфигурации от первого узла кластера) | Передача информации об изменении конфигурации кластера (реплика настроек) |
| **Сервис UserGate Management Center** | TCP | 9712 | Входящий (к UGMC от NGFW) | Первоначальная установка связи и обмен ключами шифрования управляемых устройств и сервера UserGate Management Center. |
| | | 2022 | Входящий (к UGMC от NGFW) | Построение SSH-туннеля для обмена данными с помощью полученных ключей. |
| **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 установке связи. |
| | | 22000-22711 | Входящий (к UGMC от UG Client) | Передача журналов и телеметрии с UG Client на UG LogAn транзитом через UGMC. |
| **LDAP** | TCP | 389, 636 | Исходящий (на LDAP-коннектор) | Выполнение запросов LDAP (389 - для LDAP и 636 - для LDAP over SSL). |
| **SNMP** | UDP | 161 | Входящий (до UserGate) | Доступ к серверу UserGate по протоколу SNMP. |
| **SMTP** | TCP | 25 | Исходящий (до почтового сервера) | Отправка уведомлений на электронную почту. |
| **DHCP** | UDP | 67, 68 | Исходящий (запрос на получение адреса от UserGate на сервер DHCP) | Сервис службы DHCP. |
| **FTP (экспорт журналов)** (начиная с версии 7.1.0) | TCP | 21 | Исходящий (до сервера FTP) | Экспорт журналов на сервер FTP. |
| **SSH (экспорт журналов)** (начиная с версии 7.1.0) | TCP | 22 | Исходящий (до сервера SSH) | Экспорт журналов на сервер SSH. |
| **Syslog (экспорт журналов)** (начиная с версии 7.1.0) | TCP/UDP | 514 | Исходящий (до сервера Syslog) | Экспорт журналов на сервер Syslog. |
| **Ручная проверка сайтов по категориям** | TCP | 80/443 | Исходящий (до updates.usergate.com) | Ручная проверка сайтов по категориям. |