

Table of Contents

Table of Contents	1
Введение	2
Описание	3
Управляемые области	4
Шаблоны и группы шаблонов	5
Управляемые устройства	7
Управление UGMC	8

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 LogAp.

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 LogAp. 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.

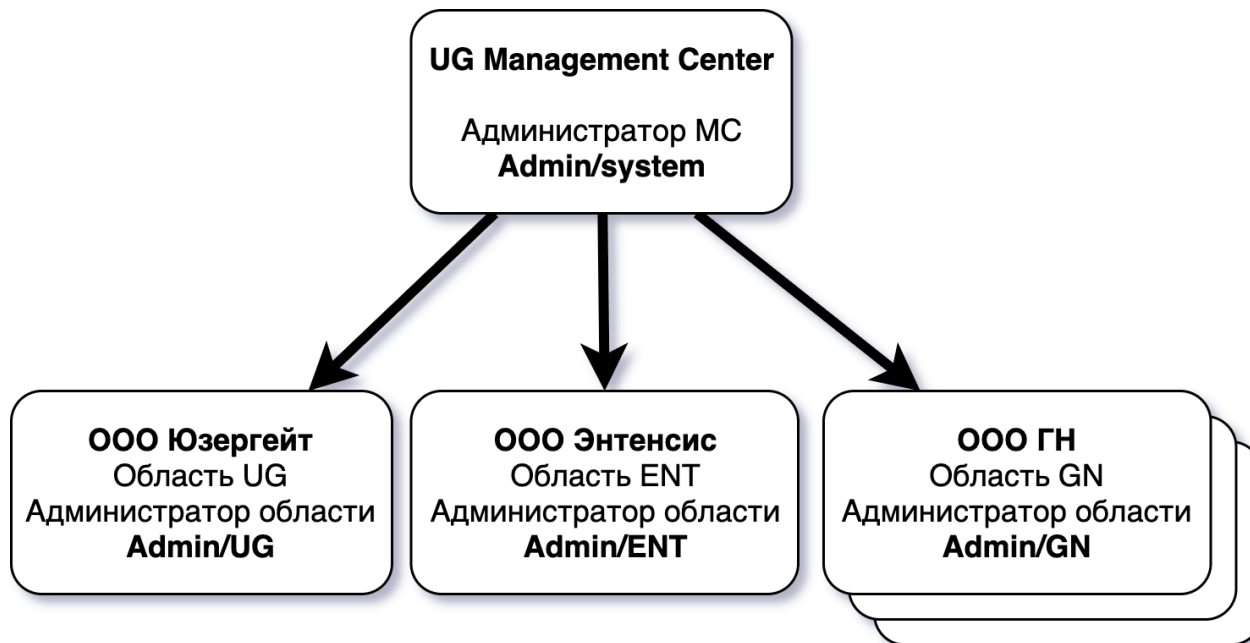
Documentation: ☒

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.

Documentation: ☒

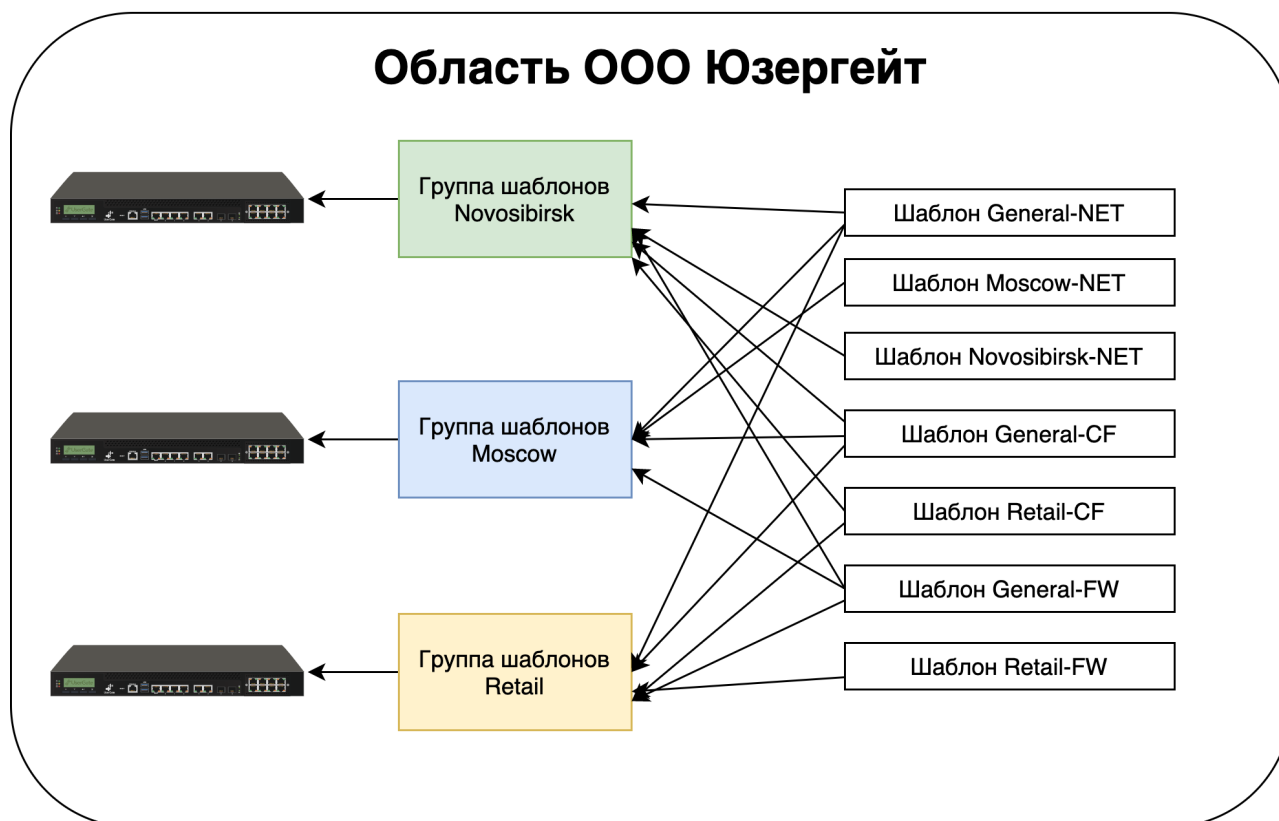
Product: UGMC

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:



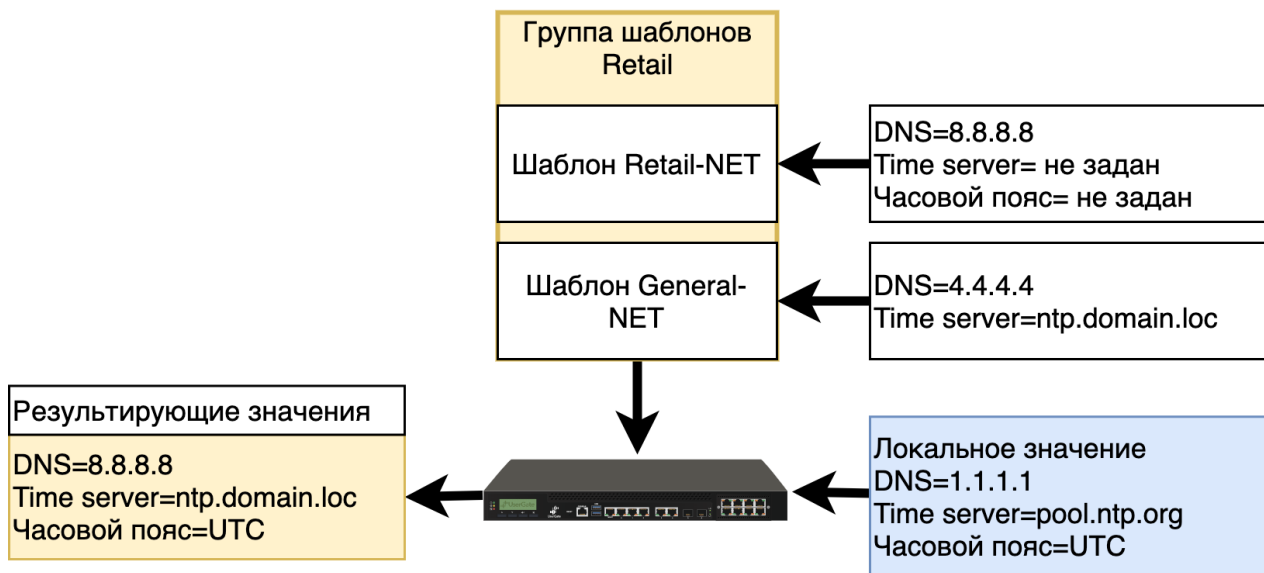
Конфигурация, передаваемая на устройство, может быть двух типов:

- 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.

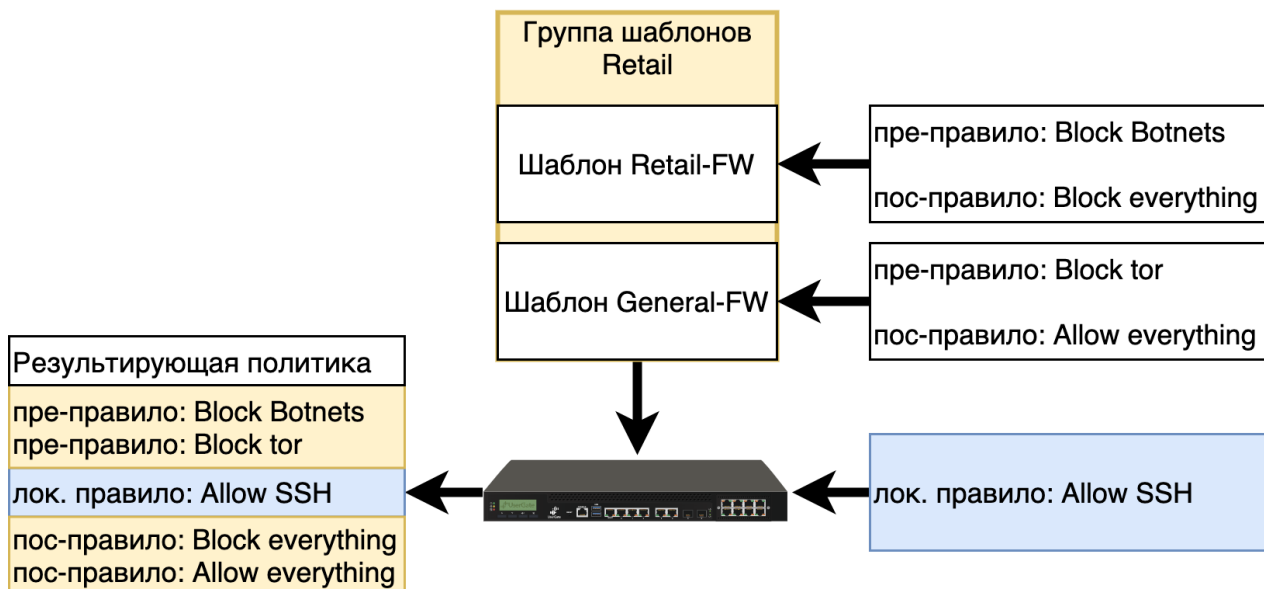
Настройка параметра при конфликтующих значениях в разных шаблонах одной группы шаблонов принимает значение, заданное в наиболее верхнем шаблоне. Локально указанные настройки данного параметра игнорируются.

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

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

Управление сервисами UGMC

Управление сервисами UGMC включает в себя следующие задачи:

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

Управление областями UGMC

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

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

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

Ролевое управление

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

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

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

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

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

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

