

Table of Contents

Table of Contents	1
Управление областями	2
Создание управляемых областей	3
Администраторы области	4
Серверы аутентификации области	6
Профили аутентификации области	8
Каталоги пользователей	9
Управление областями (Описание)	10

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

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

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

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

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

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

Администраторы области

Version: 7.0.1, 7.1.0
Product: UGMC
Documentation: ☒

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

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

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

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

При создании профиля доступа администратора необходимо указать следующие параметры:

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

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

Серверы аутентификации - 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.

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

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

Сервер аутентификации TACACS+

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

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

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

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

Профили аутентификации области

Documentation: ☒
Version: 7.0.1, 7.1.0
Product: UGMC

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

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

Каталоги пользователей

Version: 7.0.1, 7.1.0
Product: UGMC
Documentation: ☒

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

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

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

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

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

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

Управление областями (Описание)

Version: 7.0.1, 7.1.0

Product: UGMC

Documentation: 

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

