

Table of Contents

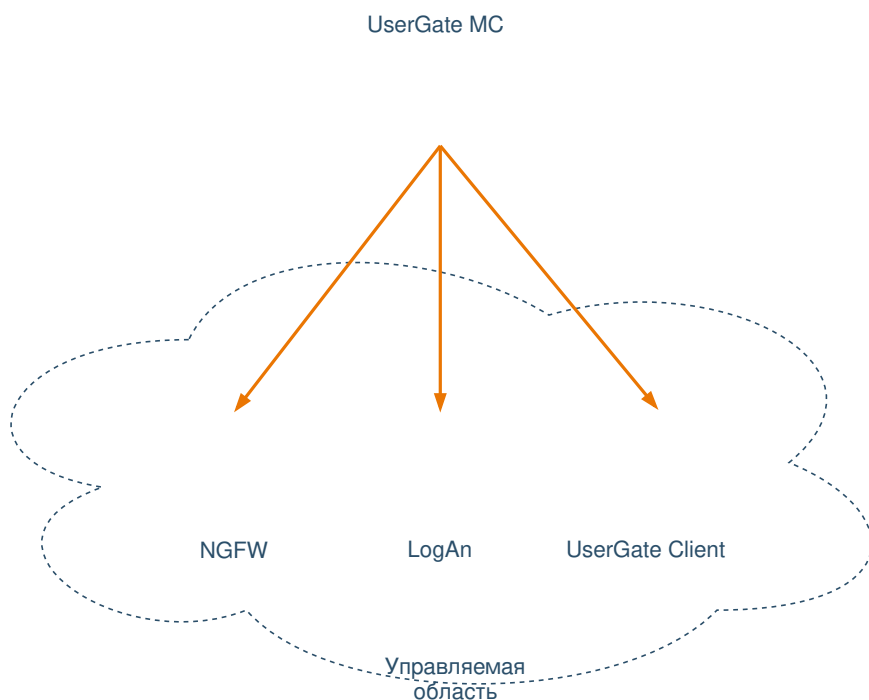
Table of Contents	1
Управление областями	2
Управление областями (Описание)	3
Создание управляемых областей	4
Администраторы области	6
Серверы аутентификации области	8
Профили аутентификации области	10
Каталоги пользователей	11

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:

Наименование	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:**



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.

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 RADIUS](#)».

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.

ПримечаниеПри 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.

