

Аутентификация при помощи внешнего access gateway

Оглавление

- # Аутентификация
- # Конфигурация
- # Как происходит маппинг атрибутов в модель данных UIDM

Аутентификация

Происходит автоматически если IP адрес клиента находится в разрешенном диапазоне адресов и access gateway передал HTTP-заголовок с идентификатором пользователя.

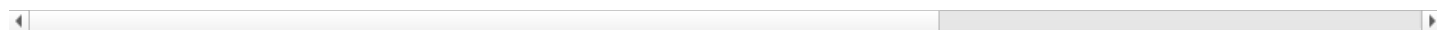
Конфигурация

Чтобы заработал автовход нужно настроить следующие свойства:

Таблица 1. Параметры относящиеся к автовходу

Ключ	Описание	Пример
com.rooxteam.sso.autologin.agw.enabled	Выключатель функциональности	true/false
com.rooxteam.sso.autologin.agw.allowed_networks	Список IP-диапазонов, для которых разрешен автовход	1.1.1.0-1.1.1.255,2.2.2.0-2.2.2.255
com.rooxteam.sso.autologin.agw.headers.principal_id	Имя заголовка, в котором передается идентификатор принципала	x-sso-samaccountname
com.rooxteam.sso.autologin.agw.attributes.map	Перечень атрибутов из модели UIDM, которые надо установить	DISPLAY_NAME_ATTRIBUTE,EMAIL_ATTRIBUTE,MOBI
com.rooxteam.sso.autologin.agw.attributes.use_as_login	Имя атрибута, которое будет использоваться в качестве логина	uid
com.rooxteam.sso.autologin.agw.default_roles	Роли принципала по умолчанию которые будут добавляться к	ROLE_CUSTOMER, ROLE_ADMIN

ролям полученным
из LDAP. Список
ролей через запятую

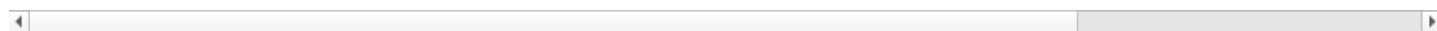


После настройки UIDM будет выполняться автовход, но профиль пользователя будет пустым.

Чтобы профиль обогащался данными из LDAP нужно настроить следующие свойства:

Таблица 2. Параметры относящиеся к обогащению профиля

Ключ	Описание	Пример
com.rooxteam.uidm.ldapv3repository.enabled	Включено ли обращение к LDAP для обогащения профиля	true/false
com.rooxteam.uidm.ldapv3repository.superuserId	Логин административной учетной записи для загрузки профиля	uidm@example.com
com.rooxteam.uidm.ldapv3repository.superuserPassword	Пароль административной учетной записи для загрузки профиля	password
com.rooxteam.uidm.ldapv3repository ldapServerName	Адрес LDAP сервера	dc.demo.rooxteam.com
com.rooxteam.uidm.ldapv3repository ldapPort	Порт LDAP сервера	389
com.rooxteam.uidm.ldapv3repository.ssl	Использовать LDAPS при подключении	true/false
com.rooxteam.uidm.ldapv3repository.baseDN	Базовое дерево для поиска пользователей	DC=dc\\,DC=demo\\,DC=rooxteam\\,DC=com - забываются экранировать запятые
com.rooxteam.uidm.ldapv3repository.userSearchFilter	Дополнительный фильтр по атрибутам пользователя для отбора разрешенных	givenName=autotests1
com.rooxteam.uidm.ldapv3repository.profileAttributesToFetch	Перечень атрибутов LDAP для загрузки в профиль пользователя UIDM	displayName,memberOf,mail,mobile,userAccountControl



Как происходит маппинг атрибутов в модель данных UIDM

1. Атрибуты должны быть перечислены в `com.rooxteam.uidm.ldapv3repository.profileAttributesToFetch`. Имена атрибутов указываются по LDAP-модели. Проверять в логе запись `RX_AGW_SSO____6003`

2. Свойство `com.rooxteam.sso.autologin.agw.attributes.map` определяет соответствие между именами атрибутов UIDM и именами атрибутов в LDAP-модели (используются только атрибуты перечисленные в свойстве `com.rooxteam.uidm.ldapv3repository.profileAttributesToFetch`).
3. Для корректной работы функционала AGW необходимо обеспечить мэппинг таких UIDM-атрибутов как `uid` , `login` .
4. Пароль имеет специальное значение, запрещающее вход по паролю, поскольку UIDM не получает значение пароля и не может осуществлять вход по нему.
5. Все атрибуты LDAP-модели перечисленные в свойстве `com.rooxteam.uidm.ldapv3repository.profileAttributesToFetch` , но не используемые в свойстве мэппинга атрибутов `com.rooxteam.sso.autologin.agw.attributes.map` будут автоматически попадать в `extendedAttributes` записи в таблице `Principal` .
6. Для конфигурации мэппинга ролей необходимо в свойстве `com.rooxteam.uidm.ldapv3repository.profileAttributesToFetch` установить соответствие UIDM-атрибута `roles` атрибуту LDAP-модели (обычно это `memberOf`). В ходе преобразования группы LDAP будет использоваться только имя конечного узла дерева LDAP. Например, если пользователь включен в LDAP группу со следующим DN `CN=Group1,DC=dc,DC=demo,DC=rooxteam,DC=com` , то данное значение будет преобразовано к роли с именем `Group1` .
7. Также в конфигурации мэппинга ролей UIDM используются следующие свойства:
 - `com.rooxteam.sso.autologin.agw.allowed_roles_pattern` - задаёт RegEx-шаблон для разрешенных имён ролей UIDM. Значение по-умолчанию `.*` - разрешены любые имена ролей.
 - `com.rooxteam.sso.autologin.agw.prohibited_roles_pattern` - задаёт RegEx-шаблон для запрещенных имён ролей UIDM. Значение по-умолчанию `(?i)^(role_)?(system|provision|antifraud)$` - запрещает использование системных ролей UIDM.
8. Результат мэппинга можно проверить в лог сообщении `RX_AGW_SSO____6004` .
9. Во время аутентификации все атрибуты попадают в клеймы и доступны для получения через `Token Inspection` (или устаревший `/tokeninfo`). Имена клеймов равны точным именам полей в `extendedAttributes` или специальным значениям если данные нужно получить из модели UIDM: `name`, `phone_number`, `email`, `roles`.

