

# Интеграция KUMA с Active Directory (AD)

При интеграции с AD/ADFS важно иметь единое время на системах, настоятельно рекомендуется настроить NTP

<https://www.youtube.com/embed/1Rw6qOWF7jc?si=vOld0Aj4wFH-Vr47>

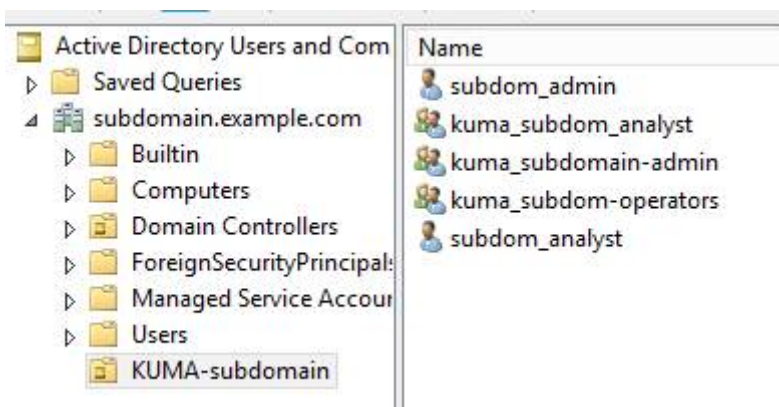
Аутентификация работает только для одного домена. Поэтому все группы должны быть созданы в корневом домене.

Пример инфраструктуры AD:

- корневой домен леса - example.com
- контроллер домена - dc-01.example.com
- дочерний домен - subdomain.example.com

В дочернем домене созданы:

- OU «KUMA subdomain»
- Universal группы безопасности: «kuma\_subdomain\_analyst», «kuma\_subdomain\_admin», «kuma\_subdomain\_operators»
- Пользователи: subdom\_admin, subdom\_analyst



Пользователи являются членами соответствующих групп:

```
PS C:\Users\Administrator> get-aduser -identity subdom_analyst -properties CN,memberOf,UserPrincipalName

CN : subdom_analyst
DistinguishedName : CN=subdom_analyst,OU=KUMA-subdomain,DC=subdomain,DC=example,DC=com
Enabled : True
GivenName : subdom_analyst
MemberOf : {CN=kuma_subdom_analyst,OU=KUMA-subdomain,DC=subdomain,DC=example,DC=com}
Name : subdom_analyst
ObjectClass : user
ObjectGUID : 8eaf5558-0966-4de0-a957-5e0cefcb461d
SamAccountName : subdom_analyst
SID : S-1-5-21-1445412355-99643495-187345912-1112
Surname :
UserPrincipalName : subdom_analyst@subdomain.example.com
```

## Настройки KUMA

Base DN – корневой домен (**не обязательно весь корневой домен**, зависит от вашего AD)

URL – контроллеры корневого домена, порт глобального каталога (**обязательно**)




Важно:

- Все группы доступа должны быть UNIVERSAL
- У пользователей в AD должно быть заполнен атрибут **email**

The screenshot shows the 'Administrator Properties' dialog box. The 'General' tab is active. The 'E-mail' field is highlighted with a red arrow, indicating it is a required field for user creation. The 'Display name' is 'Administrator' and the 'Description' is 'Built-in account for administering the computer/domain'.

Далее – для каждого тенанта указываете DistinguishedName групп, соответствующих правам доступа.

### Connection

*Base DN	<input type="text" value="DC=example,DC=com"/>
*URL	<input type="text" value="dc-01.example.com:3268"/> <small>Use comma as a delimiter to enter multiple URLs</small>
Secret	<input type="text" value=""/>   
TLS mode	<input type="text" value="Disabled"/>
Timeout in seconds	<input type="text" value="0"/>
General administrator	<input type="text" value="CN=kuma_example-admin,OU=KUMA,DC=example,DC=com"/>

### Role filters

*Tenant	<input type="text" value="Main"/>
Operator	<input type="text" value="CN=kuma_subdom_operators,OU=KUMA-subdomain,DC=subdomain,DC=example,DC=com"/>
Analyst	<input type="text" value="CN=kuma_subdom_analyst,OU=KUMA-subdomain,DC=subdomain,DC=example,DC=com"/>

Информация по ролям и их возможностям: <https://support.kaspersky.com/help/KUMA/2.1/ru-RU/218031.htm>

Важный момент:

- Предоставление доступа происходит по принципу **«наименьших прав»**. Если учетка пользователя одновременно состоит нескольких в группах одного тенанта.
- Например: kuma-analysts и kuma-admins, то пользователь получит права аналитика. Поэтому, при переводе работников из операторов в аналитиков или аналитиков в админы, необходимо не только добавить пользователя в соответствующую новую группы, но еще и удалить из старой группы.

## Результат

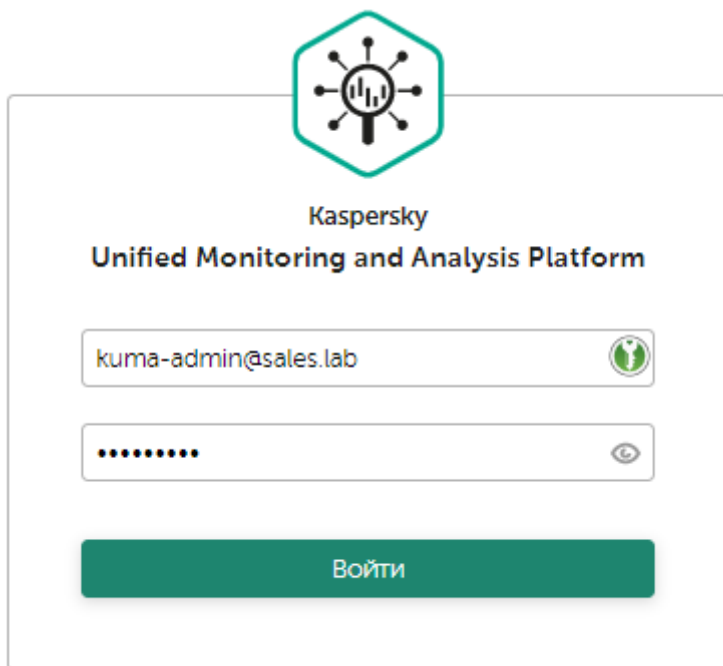
Для доменной аутентификации, как таковой учетки в KUMA не требуется. Когда все настроено, вводится доменный логин и пароль и в этот момент KUMA биндится к LDAP.

При аутентификации, пользователь вводит в консоль свою доменную учетку в формате UPN (user@example.com) и, на основании членства этой учетки в той или иной группе, пользователю предоставляется доступ к разным тенантам с указанными правами.

- Залогинившись под доменной учеткой subdom\_analyst@subdomain.example.com
- Получаем права роли analyst в тенанте Main

The screenshot shows the KUMA dashboard interface. The left sidebar contains navigation links: Dashboard, Alerts, Incidents, Events, Assets, Reports, Resources, and Task manager. The main content area is titled 'Dashboard' and shows two sections: 'Alerts by Priority' and 'Alerts by Assign', both indicating 'No records'. On the right side, there is a 'User' profile section. It includes fields for Name (Subdom\_analyst), Login (subdom\_analyst@subdomain.example.com), and Email (subdom\_analyst@subdomain.example.com). Below these, there are sections for 'Tenants for roles', including 'operator role' (No data) and 'analyst role' (Main). The bottom status bar shows the user is logged in as 'Subdom\_analyst'.

Пример входа в KUMA с доменной учетной записью (kuma-admin@sales.lab):



The image shows the login interface of the Kaspersky Unified Monitoring and Analysis Platform. At the top is a green hexagonal logo with a stylized network icon. Below it, the text "Kaspersky" and "Unified Monitoring and Analysis Platform" are displayed. The login form consists of two input fields: the first contains the email address "kuma-admin@sales.lab" and has a green circular icon with a person inside; the second contains a masked password "....." and has an eye icon to toggle visibility. A green button labeled "Войти" (Login) is positioned below the password field.

Права API можно выдавать только для внутренних пользователей, не из AD

## Порты AD

- Порт **3268**. Этот порт используется для запросов, специально предназначенных для глобального каталога. Запросы LDAP, отправленные на порт 3268, можно использовать для поиска объектов во всем лесу. Однако могут быть возвращены только атрибуты, помеченные для репликации в глобальный каталог. Например, отдел пользователя не может быть возвращен через порт 3268, так как этот атрибут не реплицируется в глобальный каталог.
- Порт **389**. Этот порт используется для запроса информации с локального контроллера домена. Запросы LDAP, отправленные на порт 389, можно использовать для поиска объектов только в домашнем домене глобального каталога. Однако запрашивающее приложение может получить все атрибуты этих объектов. Например, запрос на порт 389 может быть использован для получения отдела пользователя.
- При интеграции с SSL необходимо использовать сертификат Active Directory. В KUMA поддерживаются открытые ключи сертификата X.509 в Base64. Стандартный порт LDAPS - **636**.

## Полезные команды

```
PS C:\Users\osepov> Get-ADUser -Identity kuma-admin

DistinguishedName : CN=kuma-admin,OU=admins,OU=Users,OU=MSK,DC=sales,DC=lab
Enabled           : True
GivenName        : kuma-admin
Name             : kuma-admin
ObjectClass      : user
ObjectGUID       : 0d81928e-e8db-48bb-84b9-d00ad552bdd9
SamAccountName   : kuma-admin
SID              : S-1-5-21-781213047-594974509-2262175553-1700
Surname          :
UserPrincipalName : kuma-admin@sales.lab
```

---

Revision #6

Created 14 September 2023 12:30:20 by Boris RZR

Updated 3 February 2025 08:01:47 by Koala