

Интеграция с Active Directory (LDAP-обогащение)

Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

Официальная документация по данному разделу приведена в Онлайн-справке на продукт: <https://support.kaspersky.com/KUMA/4.0/ru-RU/217926.htm>

Видео «Обогащение событий данными с LDAP сервера»:

<https://rutube.ru/video/e07d36a0ad26ad29143c4aca8e58c672/?playlist=540937>

При наличии интеграции KUMA со службой каталогов Active Directory появляется возможность импортировать информацию о доменных учетных записях пользователей.

Перечень импортируемых атрибутов доступен в [онлайн-справке](#).

После настройки интеграции информация об учетных записях Active Directory становится доступной в карточке событий, окне алертов и инцидентов. Данные из LDAP можно использовать при обогащении событий в коллекторах и в аналитике. Также становится доступным возможность ручного или автоматического запуска действий по реагированию через Active Directory:

- Добавить учетную запись в группу
- Удалить учетную запись из группы
- Сбросить пароль учетной записи
- Блокировать учетную запись

Настройка интеграции KUMA с Active Directory включает следующие этапы:

- Создание секрета в KUMA
- Создание подключения к LDAP-серверу
- Импорт информации о пользователях из Active Directory
- Настройка обогащения событий данными Active Directory

- Проверка работы обогащения

Создание секрета в KUMA

Для импорта информации о доменных учетных записях пользователей предварительно создайте в домене сервисную учетную запись, которая будет использоваться для интеграции KUMA с Active Directory.

После создания сервисной учетной записи требуется добавить секрет в веб-интерфейсе KUMA. Этот ресурс будет хранить учетные данные для подключения к Active Directory. Чтобы создать секрет в KUMA выполните следующие действия:

- Откройте раздел веб-интерфейса KUMA **Ресурсы** → **Секреты**. Отобразится список доступных секретов.
- Нажмите на кнопку **Добавить**, чтобы создать новый секрет.
- В появившемся окне **Создание секрета** введите данные секрета:
 - В поле **Название** укажите имя для добавляемого секрета.
 - В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать создаваемый ресурс.
 - В раскрывающемся списке **Тип** выберите **credentials**.
 - В поле **Пользователь** укажите имя созданной сервисной учетной записи (может быть указано в одном из двух форматов: <user>@<domain> или <domain>\<user>).
 - В поле **Пароль** укажите пароль учетной записи.
 - Нажмите **Создать**.

Создание секрета

×

Название*	Active Directory Integration 1
Тенант*	Main 2
Тип*	credentials 3
Пользователь*	svc.kuma.ldap>truecompany.local 4
Пароль* ⓘ	 5
Описание	

Из соображений безопасности после сохранения секрета строки, указанные в полях **Пользователь** и **Пароль**, скрываются

Создание подключения к LDAP-серверу

Чтобы создать LDAP-подключение к Active Directory:

- Перейдите в раздел **Параметры** → **Интеграции** → **LDAP-сервер** в веб-интерфейсе КУМА.
- Откроется окно **Интеграция с LDAP-сервером по тенантам**.
- Нажмите на кнопку **Добавить параметры для нового тенанта**.
- В появившемся окне **Интеграция с LDAP-сервером** активируйте параметр **Состояние**, выберите тенант и укажите **Интервал обновления данных (час.)** (по умолчанию, 12 часов) и **Время хранения данных** (по умолчанию, 90 дней).
- Далее в секции **Подключения** нажмите **Создать**.

Интеграция с LDAP-сервером



Состояние



Тенант*

Main

Интервал обновления данных (час.)

12

Запланированное обновление: после сохранения

Запустить задачу импорта

Запустить задачу импорта

Время хранения данных

90

Количество дней, в течение которых данные об учетной записи хранятся в KUMA после того, как сведения о ней перестают поступать через LDAP

Подключения

Создать Удалить

☐	Название	Состояние	База поиска (Base DN)
 Пусто			

Всего 0 / Выбрано 0

Добавить

Отмена

- В появившемся окне **Создать подключение**:
 - Активируйте параметр **Состояние**.
 - В поле **Название** введите уникальное имя LDAP-подключения.
 - В поле **Секрет** укажите ранее созданный секрет для подключения к Active Directory.
 - В поле **URL** введите адрес контроллера домена в формате <hostname или IP-адрес сервера>:<порт>. Вы можете указать адреса нескольких серверов с контроллерами домена на случай, если один из них будет недоступен, нажав на кнопку **Добавить**. Все указанные серверы должны находиться в одном

домене.

- В поле **Тип** выберите один из следующих вариантов (в нашем примере будет использоваться **Незащищенный** тип. В продуктивной среде рекомендуется использовать один из вариантов с использованием шифрования передаваемых данных **startTLS** или **LDAPS**):
 - **LDAPS.**
 - При использовании LDAPS устанавливается шифрованное соединение по порту 636.
 - **startTLS.**
 - При использовании метода startTLS сначала устанавливается незащищенное соединение по порту 389, а затем отправляется запрос на шифрование. Если команда STARTTLS завершается с ошибкой, соединение обрывается. Убедитесь, что порт 389 открыт.
 - **Незащищенный.**
- Если на предыдущем шаге вы включили TLS-шифрование, добавьте TLS-сертификат. Следует использовать сертификат удостоверяющего центра, которым подписан сертификат сервера LDAP.
- В поле **Время ожидания в секундах** укажите сколько времени требуется ожидать ответа от сервера контроллера домена.
- В поле **База поиска (Base DN)** введите базовое отличительное имя каталога, в котором должен выполняться поисковый запрос.
- Нажмите на кнопку **Создать**.

Создать подключение



▶ Запустить задачу импорта

Состояние



Название*

truecompany.local 2

Секрет*

Active Directory Integration 3

URL*

10.68.85.91:389 4

+ Добавить

Тип

LDAPS startTLS Незащищенный 5

Сертификат



Время ожидания в секундах

0

База поиска (Base DN)*

dc=truecompany,dc=local 6

Пользовательские поля учетных записей AD



7

Создать

Отмена

LDAP-подключение к Active Directory создано и отображается в окне **Интеграция с LDAP-сервером**. Нажмите **Добавить**.

Импорт информации о пользователях из Active Directory

Чтобы выполнить импорт информации о пользователях из Active Directory:

- Откройте веб-интерфейс KUMA и перейдите в раздел **Параметры → Интеграции → LDAP**.
- Выберите тенант, в котором ранее было создано подключение к Active Directory.
- В появившемся окне **Интеграция с LDAP-сервером** нажмите на кнопку **Импортировать учетные записи**. Будет создана задача по импорту учетных записей.

Интеграция с LDAP-сервером



Состояние

Тенант*

Main

Интервал обновления данных (час.)

12

Запланированное обновление: 03.08.2026 17:43:26

Запустить задачу импорта

▶ Запустить задачу импорта

1

Время хранения данных

90

Количество дней, в течение которых данные об учетной записи хранятся в KUMA после того, как сведения о ней перестают поступать через LDAP

Подключения

+ Создать

Удалить

☐ Название	Состояние	База поиска (Base DN)
☐ Truecompany DC	Включено	dc=truecompany,dc=local

Всего 1 / Выбрано 0

Сохранить

Отмена

- Перейдите в раздел **Диспетчер задач**.
- Нажмите на задачу **Импорт учетных записей** со статусом **Завершено**. В окне справа **Информация о задаче** будет указано количество учетных записей, информация о которых была импортирована в KUMA.



Kaspersky
Unified Monitoring and Analysis Platform

- Выбрано тенантов: 3
- Панель мониторинга
- Алерты
- Инциденты
- События
- Активы
- Отчеты
- Ресурсы
- Диспетчер задач**

Диспетчер задач

☒ Отображать только свои

Статус	Задача	Создал	Создана	Последне
✓ Завершено	Импорт учетных записей 2	Dmitry Borisov	21.02.2025 17:49:53	21.02.2025
⚙️ Неизвестно	Импорт данных WMI	Dmitry Borisov	2025.02.20 14:28:41	2025.02.20
⚙️ Неизвестно	Импорт данных WMI	Dmitry Borisov	2025.02.20 14:07:41	2025.02.20
⚙️ Неизвестно	Импорт данных WMI	Dmitry Borisov	2025.02.20 13:44:41	2025.02.20
⚙️ Неизвестно	Импорт данных WMI	Dmitry Borisov	2025.02.20 13:44:41	2025.02.20
⚙️ Неизвестно	Импорт данных WMI	Dmitry Borisov	2025.02.20 13:44:41	2025.02.20
⚙️ Неизвестно	Импорт данных WMI	Dmitry Borisov	2025.02.20 13:44:41	2025.02.20
⚙️ Неизвестно	Импорт данных WMI	Dmitry Borisov	2025.02.20 13:44:41	2025.02.20
❌ Неудача	Импорт данных WMI	Dmitry Borisov	2025.02.20 13:44:41	2025.02.20
❌ Неудача	Импорт данных WMI	Dmitry Borisov	2025.02.20 14:12:41	2025.02.20
⚙️ Неизвестно	Импорт данных WMI	Dmitry Borisov	2025.02.20 14:08:41	2025.02.20

Информация о задаче

Скачано 15

Информация об учетных записях успешно импортирована.

Настройка обогащения событий данными Active Directory

Обогащение событий данными Active Directory настраивается на уровне коллектора и позволяет дополнить события информацией о доменных учетных записях (атрибутах, импортированных из AD). На основе полученных атрибутов доступно выполнение действий по реагированию с помощью Active Directory, а также написание правил корреляции по атрибуту memberOf. Остальные атрибуты, импортируемые из AD, служат справочной информацией и используются при расследовании алертов и инцидентов.

Чтобы настроить обогащение событий данными Active Directory:

- Перейдите в раздел **Ресурсы** → **Активные сервисы**.
- Выберите ранее созданный сервис коллектора для сбора и обработки событий Windows.

Kaspersky
Unified Monitoring and Analysis Platform

Выбрано тенантов: 3

Панель мониторинга

Алерты

Инциденты

События

Активы

Отчеты

Ресурсы 1

Ресурсы и сервисы / Сервисы

Сервисы

+ Добавить
Обновить параметры
Перезапустить
Перейти к событиям
Смотреть активные листы

windows wec

Статус

Тип

Сервис

Версия

Тенант

Полное доменное имя

IP-адрес

Порт API

Вкл

Коллектор

Windows WEC TCP/5151 2

3.2.0.305

Main

kuma-aio.truecompany.local

10.68.85.89

7791

- В появившемся окне **Редактирование коллектора** перейдите на шаг **Обогащение событий** и нажмите **Добавить сопоставление с учетными записями LDAP**.

Редактирование коллектора

Подключение источников
Транспорт
Парсинг событий
Фильтрация событий
Агрегация событий
Обогащение событий 1
Маршрутизация
Проверка параметров

Обогащение событий

Дополните события необходимыми данными. Подробнее см. [в онлайн-справке](#).

Поле KUMA	Подпись	Примеры
DeviceEventClassID		
DestinationHostName		
SourceNtDomain		
DestinationNtDomain		

+ Добавить обогащение

+ Добавить сопоставление с учетными записями LDAP 2

- Откроется блок параметров обогащения с помощью LDAP.
- В поле **Сопоставление с учетными записями LDAP** введите домен (в верхнем регистре), из которого ранее был выполнен импорт учетных записей. Доменов можно указать несколько.

В случае, если Вы не знаете полного наименования домена для импортированных учетных записей, подключитесь к компоненту Ядра KUMA по SSH. Далее воспользуйтесь следующей [статьей](#).

- В таблице **Обогащение полей KUMA** нажмите **Применить сопоставлению по умолчанию** для заполнения таблицы сопоставления стандартными значениями.
 - В **поле KUMA** указывается поле события KUMA, данные из которого следует сравнить с атрибутом LDAP.

- В **столбце LDAP-атрибут**, указывается атрибут, с которым необходимо сравнить поле события KUMA.
- В столбце **Поле для записи данных** указывается, в какое поле события KUMA следует поместить идентификатор пользовательской учетной записи, импортированной из LDAP, если сопоставление было успешно.

Редактирование коллектора

Подключение источников
Транспорт
Парсинг событий
Фильтрация событий
Агрегация событий
Обогащение событий
Маршрутизация
Проверка параметров

Сопоставление с учетными записями LDAP*

TRUECOMPANY.LOCAL x

1

Обогащение полей KUMA

+ Добавить
Удалить
Применить сопоставление по умолчанию

2

☐	Поле KUMA	LDAP-атрибут	Поле для записи данных
☐	SourceUserID	objectSID	SourceAccountID
☐	DestinationUserID	objectSID	DestinationAccountID
☐	SourceUserName	sAMAccountName	SourceAccountID
☐	DestinationUserName	sAMAccountName	DestinationAccountID
☐	SourceUserName	userPrincipalName	SourceAccountID
☐	DestinationUserName	userPrincipalName	DestinationAccountID
☐	SourceUserName	mail	SourceAccountID
☐	DestinationUserName	mail	DestinationAccountID

3

Сохранить
Отмена

- В событиях журналов ОС Windows вместо DNS-имени домена может содержаться NetBIOS-имя, которое не будет совпадать с DNS-именем домена, импортированных в KUMA учетных записей. Например, TRUECOMPANY вместо TRUECOMPANY.LOCAL.

Message	Учетной записи не удалось выполнить вход в систему
DeviceAssetID	wd10 ▾
DeviceEventCategory	Microsoft-Windows-Security-Auditing
DeviceEventClassID	4625
DeviceHostName	wd10.truecompany.local
DeviceNtDomain	-
DeviceProduct	Windows
DeviceReceiptTime	25.02.2025 15:13:48:375
DeviceTimeZone	+03:00
DeviceVendor	Microsoft
SourceAddress	10.10.10.10
SourceHostName	10.10.10.10
SourceNtDomain	-
SourceProcessName	-
SourceUserID	S-1-0-0
SourceUserName	-
DestinationAssetID	wd10 ▾
DestinationHostName	wd10.truecompany.local
DestinationNtDomain	TRUECOMPANY
DestinationProcessName	-
DestinationUserID	S-1-0-0
DestinationUserName	i.ivanov

Поэтому в данном случае для корректной работы LDAP-обогащения необходимо добавить правило обогащения, с помощью которого NetBIOS-имя в полях SourceNtDomain/DestinationNtDomain будет преобразовано в DNS-имя домена.

Для большого количества доменов рекомендуется настроить обогащение через словарь.

Для настройки правила обогащения:

- На шаге **Обогащение событий** нажмите **Добавить обогащение**.

Редактирование коллектора

Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий 1

Маршрутизация

Проверка параметров

Обогащение событий

Дополните события необходимыми данными. Подробнее см. [в онлайн-справке](#).

Поле KUMA	Подпись	Примеры
DeviceEventClassID		
DestinationHostName		
SourceNtDomain		
DestinationNtDomain		

+ Добавить обогащение 2

Сопоставление с учетными записями LDAP*

TRUECOMPANY.LOCAL x

Обогащение полей KUMA

+ Добавить

Удалить

Применить сопоставление по умолчанию

☐ Поле KUMA	LDAP-атрибут	Поле для записи данных
☐ SourceUserID	objectSID	SourceAccountID

Сохранить

Отмена

- В окне правила обогащения укажите:
 - Название** правила обогащения
 - Исходный тип** – Событие
 - Исходное поле** – SourceNtDomain
 - Целевое поле** – SourceNtDomain
 - Нажмите **Добавить преобразование**
 - Выберите **Тип** преобразования **replaceWithRegexp**
 - В поле **Выражение** укажите регулярное выражение с NetBIOS-именем. В поле **Чем заменить** укажите DNS-имя домена.
- Добавьте аналогичное правило обогащения для поля DestinationNtDomain.

Редактирование коллектора

Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров

Правило обогащения

Создать

Название*

Windows SourceNtDomain Enrichment

1

Исходный тип*

событие

2

Исходное поле*

SourceNtDomain

3

Целевое поле*

SourceNtDomain

4

Отладка

☐

Преобразование 1

🗑

Тип*

replaceWithRegex

5

Выражение

^TRUECOMPANY\$

6

Чем заменить

TRUECOMPANY.LOCAL

7

+ Добавить преобразование

Параметры фильтра

Фильтр

Создать

☐ Сохранить фильтр

📄 Конструктор

</> Код

И ▾

+ Добавить условие

+ Добавить группу

×

Правило обогащения

Создать

Название*

Windows DestinationNtDomain Enrichment

1

Исходный тип*

событие

2

Исходное поле*

DestinationNtDomain

3

Целевое поле*

DestinationNtDomain

4

Отладка

☐

Преобразование 1

Тип*

replaceWithRegex

5

Выражение

^TRUECOMPANY\$

6

Чем заменить

TRUECOMPANY.LOCAL

7

+ Добавить преобразование

Параметры фильтра

Фильтр

Создать

☐ Сохранить фильтр

Конструктор

</> Код

И

+ Добавить условие

+ Добавить группу

- Нажмите **Сохранить**.
- В разделе **Активные сервисы** нажмите **ПКМ** на сервис коллектора Windows и далее **Перезапустить**.

Проверка работы обогащения

- Перейдите в раздел **События** и укажите следующий поисковый запрос:

```
SELECT * FROM `events` WHERE SourceAccountID !='' OR DestinationAccountID!='' ORDER BY  
Timestamp DESC LIMIT 250
```

- В результате будут выведены события, обогащенные информацией об учетных записях Active Directory.
- Нажмите на одно из событий в таблице событий.

- В появившемся окне **Информация о событии** нажмите на имя учетной записи и выберите **Информация об учетной записи**.

The screenshot displays the Kaspersky Unified Monitoring and Analysis Platform interface. On the left is a dark sidebar with navigation options: Панель мониторинга, Алерты, Инциденты, События (highlighted with a red '1'), Активы, Отчеты, Ресурсы, Диспетчер задач, Параметры, Состояние источников, and Метрики. The main area is titled 'События' and contains a SQL query editor with a red '2' next to the first line: `SELECT FROM 'events' WHERE SourceAccountID != OR DestinationAccountID !=`. Below the editor is a table with columns 'TenantID', 'Timestamp', and 'DeviceProduct'. It lists two events from 'Main' tenant, both on '25.02.2025 15:29' with 'Windows' device product. The second row has a red '3' next to it. To the right, a modal window titled 'Информация о событии' is open. It lists various event details. The 'Message' field is highlighted with a red box and contains the text 'Учетной записи не удалось выполнить вход в систему'. The 'DestinationAccountID' field shows 'ivan ivanov' with a red '4' next to it. A dropdown menu is open next to it, showing 'Информация об учетной записи' (highlighted with a red box and a red '5') and 'Найти похожие события'. The 'DestinationNtDomain' field is also highlighted with a red box and contains 'TRUECOMPANY\LOCAL'.

- Откроется окно **Информация об учетной записи** с данными об учетной записи, полученной из Active Directory.

Информация об учетной записи



Реагирование через Active Directory

Display name

ivan ivanov

Common Name

ivan ivanov

Distinguished name

cn=ivan ivanov,cn=users,dc=truecompany,dc=local

User logon name

i.ivanov

Имя участника-пользователя (UPN)

i.ivanov@truecompany.local

Member Of

{ cn=hr,cn=users,dc=truecompany,dc=local }

User account control

512

Mail

i.ivanov@truecompany.local

▼ Дополнительная информация

Physical delivery office name

1-2-3

Telephone number

77777

Создано

20.02.2025 18:32:45

Account expires

14.09.30828 05:48:05

Bad password time

25.02.2025 15:32:43

Обогащение событий Windows данными Active Directory настроено.

Если обогащение событий информацией из Active Directory не выполняется, попробуйте указать только те домены, которые есть в базе Ядра KUMA. Если эта рекомендация не помогла - попробуйте сделать обогащение только по одному домену.