

Агенты и Discovery

Реестр агентов (/agents)

Таблица показывает зарегистрированных AI-агентов тенанта.

Колонка (EN)	Смысл
Name	Имя агента
Type	Тип (llm , tool , workflow , custom и др.)
Predicted	Тип, предсказанный ML
Risk	Оценка риска
Status	active / inactive / error
Version	Версия
Last Seen	Последний heartbeat
Actions	View / Delete

Типовые действия оператора

1. Откройте **Agents**.
2. Отфильтруйте или найдите агента (semantic search).
3. Нажмите на строку → **Agent Details** (/agents/:id): метаданные, heartbeats, связанные audit и anomalies.
4. Удаление (**Delete**) — обычно Admin+; подтвердите в диалоге.

Регистрация агента

Чаще выполняется через API или SDK (не обязательно из UI):

```
curl -X POST http://localhost:8001/api/v1/agents/register \
-H "X-API-Key: $TENANT_API_KEY" \
-H "Content-Type: application/json" \
-d '{
  "name": "prod-billing-llm",
  "type": "llm",
  "version": "1.0.0",
  "capabilities": ["chat", "summarize"]
}'
```

Сохраните возвращённый id (UUID). Агент должен периодически слать heartbeat:

```
curl -X POST "http://localhost:8001/api/v1/agents/$AGENT_ID/heartbeat" \
-H "X-API-Key: $TENANT_API_KEY"
```

Рекомендуемый интервал — около **60 секунд**. Если **Last Seen** устарел, статус станет `inactive` / `error` — проверьте ключ и процесс агента.

Практические советы

- Регистрируйте агента **до** включения в workflow.
- Одно стабильное имя на сервис: `prod-billing-llm`, не «test1».
- Указывайте честные capabilities — от них зависят политики и поиск.

Discovery — Shadow AI (/discovery)

Раздел для **Security Analyst+**. Сюда попадают кандидаты незарегистрированной AI-активности.

Действие UI	Результат
Confirm	Кандидат подтверждается → создаётся запись агента + fingerprint
Dismiss	Кандидат закрывается как нерелевантный

Регламент

1. Ежедневно просматривайте backlog кандидатов.
2. По evidence решайте: Confirm (легитимный сервис без регистрации) или Dismiss (шум / ложное срабатывание).
3. После Confirm проверьте агента в **Agents** и при необходимости добавьте политики / бюджет.

Не игнорируйте backlog

Незарегистрированные агенты обходят реестр и усложняют аудит. Рост кандидатов — сигнал для разработки и безопасности.