

AI Workflow Automation

Устройство, настройка, контроль и границы применения

Для владельцев процессов, технических специалистов и операторов

Версия	0.1.0
Обновлено	2026-07-26
Release tag	ai-workflow-v0.1.0
Источник	conson/ai-workflow / a98ea3ed3438

Документ собран из зафиксированного commit. Идентификатор сборки: 373ca081d579.

Содержание

Назначение	3
Устройство	3
Требования	3
Настройка сценария	4
Scenario	4
Source	4
AI rules	4
Result	4
Human Review	4
Delivery	5
Эксплуатация	5
Безопасность и аудит	5
Ограничения	5
Проверка результата	6
Заключение	7
Поддержка AI Workflow Automation	7

AI Workflow Automation связывает источник данных, правила и AI-обработку, проверку человеком и доставку результата. Каждый сценарий настраивается и публикуется отдельно. Настройка и эксплуатация используют серверное состояние, а интерфейс показывает его безопасную проекцию.

Назначение

Решение применяется к повторяемому процессу, где входные данные имеют проверяемую структуру, результат можно описать схемой, а спорные случаи передать оператору. Примеры включают классификацию заявок, обработку обращений и структурирование пакетных данных.

Сценарий не является произвольным графом. Он проходит фиксированную последовательность:

Scenario -> Source -> AI rules -> Result -> Human Review -> Delivery -> Operations

Устройство

Область	Назначение	Проверяемый результат
Scenario	Изолирует конфигурацию и жизненный цикл	Черновик или защищенная опубликованная версия
Source	Проверяет соединение и структуру входа	Сохраненный образец проверенного JSON
AI rules	Выбирает профиль модели и правила	Валидный структурированный результат
Result	Собирает выходную схему	Проверенный preview без доставки
Human Review	Останавливает требующие решения элементы	Решение оператора и журнал изменений
Delivery	Передает или сохраняет результат	Квитанция, checksum или управляемый файл
Operations	Показывает исполнения и сбои	Состояние очереди, запуска, review и доставки

Сервер владеет готовностью этапов, публикацией, правами, аудитом и идемпотентностью. Состояние браузера не заменяет эти проверки.

Требования

- Node.js и зависимости из **package-lock.json**.
- PostgreSQL для сохраняемого состояния и очередей.
- Настроенный локальный или OpenAI-compatible AI-профиль.
- Явно разрешенные адреса источников и HTTP-доставки.
- Учетные записи и профили доступа с областью сценариев.

- Отдельные секреты окружения; значения не хранятся в конфигурационных JSON.

Параметры окружения перечислены в **.env.example**. Реальные пароли, ключи, токены и закрытые ключи должны передаваться через защищенное окружение установки.

Настройка сценария

Scenario

Создайте сценарий из поддерживаемого шаблона и задайте отдельное имя. Копия получает собственную изменяемую конфигурацию. Опубликованная версия защищена от изменений: для редактирования ее необходимо снять с публикации, проверить изменения и опубликовать повторно.

Source

Источник проверяется до настройки зависимых этапов. Проверенный JSON является единственной основой для сопоставления полей. Интерфейс не должен добавлять поля, отсутствующие в полученном образце.

Для REST Source задаются метод, разрешенный адрес, ограничения размера и времени, способ авторизации и ссылка на credential handle. Проверка соединения не должна возвращать значение секрета.

AI rules

Сценарий выбирает разрешенный профиль модели и задает категории, правила и структуру ответа. Тест на явном примере не создает доказательство готовности публикации. Для публикации используется проверка на текущем Source-образце и текущей конфигурации.

Изменение Source, правил, профиля модели или выходной схемы делает предыдущее доказательство устаревшим.

Result

Result объединяет проверенный Source, принятый AI-ответ и mapping. Preview не создает операторское решение и не выполняет Delivery. Пользовательские поля связываются с путями текущего проверенного входа.

Human Review

Review использует детерминированную политику допуска. Оператор видит деловые поля, может изменить разрешенные значения и принять или отклонить элемент. Первоначальные и проверенные значения сохраняются как отдельное доказательство коррекции.

Delivery

Поддерживаются управляемые файлы и явно настроенные каналы. Перед внешним действием повторно проверяются режим запуска, emergency stop, права, область сценария и идемпотентность.

Исторический replay всегда подавляет внешнюю доставку.

Эксплуатация

Operations отделен от настройки. Он показывает очередь, исполнения, ожидающие решения, инциденты и квитанции доставки. Списки ограничены пагинацией и фильтруются по доступным сценариям.

При диагностике следует зафиксировать:

1. версию приложения и release сценария;
2. роль и область доступных сценариев;
3. этап, команду и безопасный идентификатор запуска;
4. ожидаемое и фактическое состояние;
5. типизированную причину ошибки без исходных данных и секретов.

Безопасность и аудит

- Доступ проверяется на сервере для каждой защищенной операции.
- Секреты доступны только через credential handles и переменные окружения.
- Source и Delivery ограничиваются allowlist и сетевой политикой.
- Критические изменения, публикация, решения оператора и доставка записываются в аудит.
- Ошибки, telemetry и интерфейс не должны раскрывать секреты или исходные чувствительные данные.
- Настройка аккаунтов и соединений отделена от обычной работы оператора.

Ограничения

- Поддерживается конфигуратор заданных сценариев, а не универсальный визуальный конструктор произвольных процессов.
- Новое семейство коннекторов требует отдельного продуктового решения и проверки реального сценария.
- Технически успешный запуск не подтверждает качество бизнес-результата.
- Автоматический режим не расширяется без истории наблюдений или проверенных оператором примеров.

- Возможности внешней доставки зависят от выбранной среды, сетевой политики и отдельной проверки безопасности развертывания.
- Обновление конфигурации опубликованного сценария требует нового цикла проверки.

Проверка результата

1. Проверьте Source на представительном обезличенном примере.
2. Выполните AI-проверку и убедитесь, что ответ проходит строгую схему.
3. Сверьте Result preview с ожидаемым контрактом.
4. Проверьте положительное и отрицательное решение Human Review.
5. Выполните Delivery в безопасный тестовый канал и проверьте квитанцию.
6. Перезапустите приложение и подтвердите сохранность состояния.
7. Проверьте роли, запреты доступа, аудит и отсутствие секретов в ошибках.
8. Зафиксируйте версию приложения, release сценария и условия проверки.

Заключение

AI Workflow Automation связывает один поддерживаемый сценарий, проверенный источник, AI-обработку, решение человека и доставку результата в управляемую последовательность.

Публикация сценария требует повторной проверки после изменений источника, правил, модели, результата или доставки.

Расширение автоматического режима опирается на наблюдаемую историю и проверенные решения операторов, а не только на успешное выполнение технических тестов.

Поддержка AI Workflow Automation

Приложите версию, роль пользователя, идентификатор сценария, последовательность действий и безопасный фрагмент журнала без чувствительных данных.

<https://t.me/Norrskén7>

Источник: `conson/ai-workflow / commit a98ea3ed34385a8fcb3ab75ed393d8099d723485 / ai-workflow-v0.1.0.`

Идентификатор сборки: `373ca081d579195eb93edf32ba2c50cc0cc4a9b5c01409f3d5e975f992b004e0.`