Руководство администратора

ПО «Distil» Правообладатель: ООО «Лэмп Лэбс» ИНН 9714031466; ОГРН 1237700942533 Юридический адрес: 125167, г. Москва, Новый Зыковский пр-д, д. 3, помещ. 16ц Генеральный директор: Суржок Дарья Анатольевна Версия документируемого выпуска: 1.49.41 (тег v1.49.41) Дата: 19 ноября 2026 года

Рабочая редакция для согласования. Маркеры [ЗАПОЛНИТЬ] необходимо устранить до подачи и публикации. Описание основано на текущем репозитории; наличие перечисленных функций именно в поставляемом экземпляре 1.49.41 подлежит сверке перед экспертизой.

Доступ и лицензия

В token mode храните API_SECRET как административный секрет инсталляции. Корпоративный режим AUTH_MODE=oidc использует OIDC, SCIM и роли; подготовьте поставщика идентификации, адрес HTTPS и настройки согласно документации корпоративной установки. Проверьте доступ отдельными учётными записями администратора и обычного пользователя. Legacy machine routes и legacy MCP в SSO отключены; корпоративный MCP настраивается отдельно.

Лицензия инсталляции и лицензия настольного приложения имеют разные области действия. Проверьте требуемые возможности и действительность лицензии перед вводом системы в эксплуатацию. Ключи не включайте в открытые отчёты.

Настройки обработки

В «Администрирование» управляйте обработкой, пользователями и интеграциями. Выберите локальный либо явно разрешённый облачный маршрут; проверьте настройки приватного шлюза. Через «Администрирование → Доверие» получите сводку маршрутов и убедитесь, что внешние назначения согласованы. Для изолированного контура используйте DISTIL_OFFLINE=1, предварительно доставив модели; дополнительно проверьте пользовательские интеграции и входящие ссылки.

Резервное копирование

Настройте назначения и расписание в «Администрирование → Резервные копии». Поддерживаются файловое и S3-совместимое хранилища. Храните пароль резервного хранилища отдельно от сервера. Создайте пробный снимок и проверьте результат задания; наличие расписания не доказывает успешность копирования. Состав и период хранения согласуйте с владельцем данных.

Восстановление выполняйте через мастер либо CLI сервера. CLI server restore --target-config файл .json выводит снимки; выбор задаётся --snapshot, пароль — --password-file. Используйте его на остановленном сервере с корректным DATA_DIR и защищёнными файлами параметров. Перед восстановлением сохраните текущие данные. После него проверьте вход, записи и обработку; Telegram потребуется переподключить. Согласия почтовых подключений после restore выключаются.

Диагностика

Проверьте /health, состояние контейнеров и журналы docker compose logs --tail=100. Состояние HTTP и готовность моделей проверяйте раздельно. При сбое зафиксируйте версию, время, платформу, этап обработки и воспроизводимые шаги; удалите из передаваемых журналов секреты и содержимое встреч. Не отправляйте полную БД в поддержку без согласования владельца.

Основания

INSTALL.md; docs/enterprise-install.md; docs/mcp.md; docs/trust-center.md; docs/licensing.md; docs/mail-for-assistant.md; backend/cmd/server/restore_cli.go; app/lib/screens/admin_backup_section.dart.