Настройки системы

Настройки системы

Маршрут: `/settings` (ADMIN — запись, INFOSEC — чтение).

Вёрстка секций — pref-карточки в том же стиле, что страница **Аккаунт** (`/account`): строки настроек, переключатели, списки токенов/звуков.

Секции

Общие

Вверху вкладки — блок **Статус серверов** (выше формы имени инстанса / часового пояса; tip'ы, latency, время проверки, автообновление 30 с, ресурсы хоста):

Компонент	Как проверяется
API	`GET /api/v1/system/status`
PostgreSQL, ClickHouse	тот же endpoint (backend health; ClickHouse disabled → **Выкл**, не авария)
Документация	клиентская проверка `/docs/` + ссылка **Открыть**
Swagger	клиентская проверка `/swagger-ui/index.html` + ссылка **Открыть**
Ресурсы сервера	тот же endpoint → `host` (CPU %, ОЗУ, свободное место на диске рабочей директории)

Общий индикатор (зелёный / красный) и кнопка **Обновить**. Раньше блок был в модалке **Справка** — см. help-modal.md.

Ниже — поля:

- Имя инстанса
- Часовой пояс отображения времени (сохраняется кнопкой **Сохранить** в карточке настроек; часы в сайдбаре читают `system_timezone` из `/auth/me` — после save UI обновляет профиль; личный пояс в **Аккаунт** перекрывает инстанс)
- **Охват карты состояний** (`monitoring.status_map_coverage`): Россия (по умолчанию), Московская область, Европа, Евразия, СНГ, Казахстан, Узбекистан — UI в **Общие**, ключ API по-прежнему в блоке monitoring

Отдельная карточка **Темы системы**:

- Сетка установленных тем (превью-квадраты): основные темы в сетке, игровые и стилизованные (Киберпанк, Warcraft, EVE, Warhammer, Паук, Zabbix, wiSLA Hub) — в

плитке **Другое** (клик открывает окно поверх страницы). Тема `brand` в UI называется **Фирменная**.
- Клик по плитке выбирает тему в черновике; зелёная метка — **активная** (сохранённая) тема. Пока не нажали **Сохранить** в этой карточке, UI не переключается. Подсказка формата файла — tooltip у «Загрузить».
- **Сбросить / Сохранить** в карточке тем (и в других блоках настроек) затрагивают только поля этого блока.
- **Загрузить новую тему** — `POST /api/v1/settings/themes` (multipart JSON `wisla-theme`, ≤256 KB). Перед отправкой UI проверяет `.json`, размер, `format` / `formatVersion` /id/name/ обязательные tokens; сервер повторно валидирует JSON, токены CSS (без `url(` / `javascript:` и т.п.) и отклоняет коллизию с built-in id. Удаление только загруженных — `DELETE /api/v1/settings/themes/{id}`
- Каталог: `GET /api/v1/settings/themes` (без сессии — нужен для брендинга на login/register; upload/delete — ADMIN)
- White-label пакет: `branding.replaceProductMark`, опционально `branding.mark` (`egg` — яйцо МТС / `letter`), токен `--login-accent` для кнопок входа. Пример: `docs/frontend/themes/mts-operator-wisla6.json`
- Формат пакета: theme-pack.sample.json; обзор тем UI: theme-i18n-responsive

Сбор и хранение

Одна вкладка (`?section=collection`; старые `data` / `monitoring` редиректят сюда). Карточки сверху вниз:

1. **Хранение** — retention метрик и аудита (дней); очистка аудита ежедневным job'ом
2. **Приём trap / syslog** — вкл/выкл (**switch**) + порт; loopback — switch
3. **Обновления агентов** — базовые URL HTTP/HTTPS
4. **Эталон инвентаря** — switch сравнения + интервал, ч
5. **Жизненный цикл проблем** — окно flap-reopen (минуты, default 60), архив решённых (дни, default 14) и шторм аварий: порог (default 25, **0 = выкл**) и окно в минутах (default 10). Ключи API: `problems.flap_reopen_minutes`, `problems.archive_after_days`, `problems.storm_threshold`, `problems.storm_window_minutes` (в grouped JSON — `monitoring.*`).

ICMP ping узлов настраивается **шаблоном** (`Template Module ICMP Ping`): интервал — item `delay`, таймаут ping — item `timeout` (как в wiSLA). Не настраивается на этой вкладке.

Блок **Приём trap / syslog**:

- SNMP trap: вкл/выкл + UDP-порт (стандарт **162**). Для bind портов ниже 1024 на Linux — `CAP_NET_BIND_SERVICE` в wisla-backend.service; при ошибке bind смотрите лог — fallback на 1162 нет.
- SIMPLE ICMP (`icmpping*`): unit также должен иметь **`CAP_NET_RAW`** (вместе с `NoNewPrivileges`) — иначе OS `ping` в дочернем процессе падает, и удалённые Windows/ хосты без TCP echo показывают 100% loss.
- Syslog: вкл/выкл + UDP-порт (стандарт **514**). По умолчанию **выключен**.
- **Принимать с loopback** (`monitoring.incoming_accept_loopback`, default true): для Docker Desktop; в проде часто выкл.
- Смена порта/вкл/loopback — **перезапуск backend**.
- На узле: галочки + шаблоны; триггеры по `{$SNMPTRAP.PROBLEM.REGEXP}` / `{$SYSLOG.PROBLEM.REGEXP}`.
- Docs: incoming-trap-syslog, smoke: incoming-trap-syslog-smoke.

Блок **Обновления агентов** — базовые URL пакетов для протоколов **HTTP** и **HTTPS** (используются при массовой смене протокола и в директиве `update` на heartbeat):

- При **первом запуске** backend автоматически заполняет оба поля по адресу сервера (если в БД ещё пусто).
- Приоритет источника: `wisla.agent.packages-base-url` → `wisla.agent.manager-public-url` → hostname + `server.port`.
- В проде за reverse proxy задайте публичный URL в `wisla.properties`: `wisla.agent.manager-public-url=https://monitoring.example`.
- Ключи в БД: `agents.update.packages_base_url_http` / `_https` (Flyway `V71__agent_update_package_urls`).

Охват карты состояний описан выше в **Общие** (`monitoring.status_map_coverage`). `GET /api/v1/settings/status-map` (все роли); запись — `PUT /api/v1/settings` (ADMIN).

Отдельный блок **Эталон инвентаря**:

- Сравнение с эталоном: enable + интервал в часах (`agents.inventory.compare_*`, default 24ч)

Ключи API по-прежнему разделены: `data.*` (retention) и `monitoring.*` (trap/агенты/эталон).

Безопасность

См. Безопасность: TTL токенов, сессии, brute-force/lockout, политика паролей (минимум **8** символов, нельзя ниже).

Уведомления

Kill-switch `notifications.enabled` и **звук в открытой вкладке** браузера (Web Audio; это не OS push). После сохранения блока звука UI обновляет `/auth/me`, чтобы SSE сразу играл новый пресет. Сценарии «кому и когда» — страница **Воркфлоу** (`/workflows`). Личные email/Telegram/MAX — **Аккаунт** или **Аудит и доступ → Пользователи**. Транспорт — **Интеграции**.

Каналы доставки — в **Интеграциях**. Подробнее: Уведомления, Воркфлоу.

Интеграции

Подключения внешних сервисов. UI: таблица добавленных интеграций, модальное окно выбора типа, раскрываемая форма настройки.

Действие	Описание
Добавить интеграцию	Модальное окно со списком доступных типов (SMTP, Telegram, MAX, Webhook, SIEM, LDAP, **SSO (OIDC)**, **Grafana**, Jira, Yandex Tracker). Произвольный webhook для Тикета в пикер не кладётся — карточка появляется, только если такие подключения уже есть
Строка таблицы	Клик раскрывает форму параметров
Тест	`POST /api/v1/settings/integrations/{type}/test` — пробная отправка без сохранения
Сохранить и активировать	Сохраняет настройки и включает канал (уведомления, SIEM forward, LDAP или Grafana)

Deep link: `/settings?section=integrations&integration=email` (или `telegram`, `max`, `webhook`, `siem`, `ldap`, `grafana`, `jira`, `yandex_tracker`).

Тип	Что настраивается	Статус
Email (SMTP)	host, port, SSL/STARTTLS, auth, TLS, trust, timeouts, from/alias/to; пресеты Yandex / Gmail / corporate	доступно
Telegram	bot token, chat id	доступно
MAX	bot token, user/chat id	доступно
Webhook	URL для HTTP POST	доступно
SIEM	interval, webhook URL (+ forward enable при активации)	доступно
LDAP / AD	LDAPS/StartTLS, bind, filter (sAMAccountName/UPN/email), вложенные группы, карта групп→ролей, PEM, тест пользователя	доступно
Grafana	base URL, service account / API token, embed на `/dashboard`	доступно
Jira	URL, email, API token, проект, тип задачи — пункт **Тикет** на холсте воркфлоу	доступно
Yandex Tracker	org id, OAuth, очередь, тип — пункт **Тикет** на холсте	доступно
Другая система (webhook)	имя, http(s) URL, секретный заголовок — только если нет Jira/Tracker. CRUD: `/api/v1/workflow-http-connections`. В пикер «Добавить интеграцию» не входит	доступно
SSO (OpenID Connect)	корпоративный вход через IdP (Keycloak, Azure AD, Okta…)	доступно

Секреты SMTP password, Telegram/MAX bot token, LDAP bind password, **OIDC client secret**, Jira/Tracker tokens и **Grafana API token** для INFOSEC маскируются (`***REDACTED***`).

Grafana

Внешний слой визуализации (как datasource/embed у wiSLA). После активации на **Дашборд** появляется переключатель **wiSLA | Grafana**.

Поле	Смысл
URL	Базовый URL Grafana, например `https://grafana.company` (без `/` в конце)
API token	Service account token с правом Search dashboards
Embed	Показывать каталог и iframe на `/dashboard`
Источник по умолчанию	`wisla` или `grafana` — что открывать на `/dashboard` без `?source=` / `?id=`. Ссылка с `?id=` всегда wiSLA
Дашборд по умолчанию	

Поле	Смысл
	UID Grafana-дашборда (каталог подгружается после сохранения URL и token)
Каталог на Дашборд	`wisla` — папка **wiSLA 6** и тег `wisla6`; `all` — весь Search-каталог
Авто-provisioning	Папка, managed datasources (CH/PG wiSLA), дашборд «Обзор инфраструктуры»

Подробнее: Grafana: интеграция и provisioning.

Тест: `POST /api/v1/settings/integrations/grafana/test` — `/api/health` + `/api/org`.

Каталог для UI (токен не уходит в браузер):

Метод	Путь
`GET`	`/api/v1/grafana/status`
`GET`	`/api/v1/grafana/dashboards?q=&scope=wisla|all`
`GET`	`/api/v1/grafana/embed-url?uid=&theme=light|dark`
`PUT`	`/api/v1/grafana/defaults`
`POST`	`/api/v1/grafana/provision`

На стороне Grafana: `allow_embedding = true`, CSP `frame-ancestors` на origin wiSLA; для iframe без второго логина — SSO или anonymous org viewer. Datasource-плагин Wisla→Grafana — отдельная фаза.

Email (SMTP)

Транспорт подходит для Yandex, Google и корпоративных relay/Exchange.

Сценарий	Host	Port	SSL	STARTTLS	Auth
Yandex	`smtp.yandex.ru`	465	да	нет	да, пароль приложения
Google / Gmail	`smtp.gmail.com`	587	нет	да (+ required)	да, пароль приложения
Корпоративная	`smtp.company.local` / Exchange	587 (или 25)	нет	да на 587	да, либо выкл. для внутреннего relay

В форме: шаблон провайдера (подставляет host/port/флаги, логин и адреса не трогает). Смена порта 465/587/25 подставляет SSL/STARTTLS.

Дополнительно: версия TLS (`TLSv1.2` / `TLSv1.3`), SSL Trust (пусто = JVM, `*` = любой сертификат — только внутренний CA), таймауты connect/read/write, псевдоним отправителя.

При включённом SSL STARTTLS игнорируется. Тест: `POST /api/v1/settings/integrations/email/test`. Ответ с `details.error_code` (`smtp.auth_failed`, `smtp.ssl_port_mismatch`, `smtp.timeout`…) — UI показывает понятное сообщение на языке интерфейса, без сырого `jakarta.mail…`. Порт 465 без SSL отклоняется до отправки. Для Яндекс/Google нужен **пароль приложения**.

MAX

Бот MAX для тех же событий, что Telegram (`problem.open` / `resolve` / `escalate`). Создайте бота на platform.max.ru, вставьте токен и id назначения.

Поле	Смысл
Bot token	Заголовок `Authorization` к `https://platform-api2.max.ru` (не в URL)
Куда слать	`user` — личный диалог (`user_id`); `chat` — группа/канал (`chat_id`)
Destination id	Числовой id. Пользователь должен написать боту (или бота добавить в чат)

Тест: `POST /api/v1/settings/integrations/max/test`. Если TLS к MAX падает на сертификате Минцифры — добавьте CA в trust store JVM.

LDAP / Active Directory

Гибридный вход:

- Существующие **локальные** пользователи (`auth_source=local`) — только пароль из БД (bcrypt).
- При **включённом LDAP** (`ldap.enabled=true`) неизвестный логин или пользователь с `auth_source=ldap` проверяется в каталоге.
- Логин: `sAMAccountName`, UPN (`user@corp.local`) или email; также `CORP\ivanov`.
- Успешный вход создаёт или обновляет пользователя (JIT): статус `ACTIVE`, роль из карты групп или `default_role`.
- Вложенные группы AD (`memberOf:1.2.840.113556.1.4.1941`) учитываются; в карте можно указать полный DN или CN группы.
- Если учётка в AD отключена, истекла или удалена — локальный LDAP-пользователь переводится в `DISABLED` и вход отклоняется.
- Смена пароля в UI недоступна для LDAP-пользователей. Локальный `admin` остаётся запасным входом при недоступности каталога.

Тест интеграции: bind сервисной учётной записью. Если заполнен «Проверка пользователя» — поиск в каталоге, список групп (включая вложенные), итоговая роль и опционально bind паролем.

API: `POST /api/v1/settings/integrations/ldap/test` (тело — текущий draft настроек, поля `ldap.test_username` / `ldap.test_password` не сохраняются).

На странице входа при активном LDAP показывается подсказка; API `GET /api/v1/auth/login-options` возвращает флаг `ldap_enabled`.

SSO (OpenID Connect)

Этап (2026-08-27): OIDC фазы 1–2 готовы + lab smoke Docker Desktop (фаза 1 и 2). Alpha / тестзона IdP — позже. **SAML** — не реализован. Детали и «просто/сложно из ТЗ»: post-alpha §6.

- Authorization Code + PKCE: `GET /api/v1/auth/oidc/start` ⟶ IdP ⟶ `GET /api/v1/auth/oidc/callback`
- Настройки: `oidc.issuer`, `oidc.client_id`, `oidc.client_secret`, `oidc.redirect_uri`, `oidc.public_ui_url`, claims и `oidc.role_map_json`
- Доп. флаги: `oidc.skip_local_mfa`, `oidc.end_session_enabled`, `oidc.deprovision_empty_groups`

- Redirect URI в IdP: `{backend}/api/v1/auth/oidc/callback` (точное совпадение)
- После успеха backend выставляет refresh cookie и редиректит на UI `/login?sso=1&returnUrl=...`
- При `skip_local_mfa=false` и включённом TOTP: `/login?sso=mfa&mfa_token=...` → `POST /api/v1/auth/oidc/mfa`
- Logout: `POST /api/v1/auth/logout` → `{ "idp_logout_url": "..." }` (если IdP отдаёт `end_session_endpoint`)
- JIT: пользователь `auth_source=oidc`, роль из claim groups; локальный пароль в UI не меняется
- `login-options`: `oidc_enabled`, `oidc_button_label`
- Тест: `POST /api/v1/settings/integrations/oidc/test` (discovery issuer + end_session)
- Lab: oidc-lab.md; smoke: `oidc-lab-smoke.py`, `oidc-lab-phase2-smoke.py`

Остаётся: alpha/тестзона IdP, матрица Azure AD/Okta, Java autotests, SAML (если RFP).

SAML — отдельный backlog (см. post-alpha §6).

API-токены (системные)

Системные (service) Bearer-токены для CI и интеграций:

- ADMIN создаёт / отзывает; INFOSEC только список
- Назначается роль (`ADMIN` / `OPERATOR` / `VIEWER` / `INFOSEC`)
- Формат `wsl.sys....`; секрет один раз с кнопкой **Копировать**; в БД только hash + tip
- Персональные токены — в Аккаунт

API: `GET/POST/DELETE /api/v1/settings/api-tokens` (и `/api/v1/auth/api-tokens` для personal).

Лицензия

Лицензия: отдельная страница (Community / Enterprise / Trial). Кратко:

- По умолчанию on-prem **Trial** (жёсткий лимит **50** сервисов, без срока)
- ADMIN активирует ключ / сбрасывает к **Trial**; INFOSEC — только просмотр
- Community — облачная редакция (не локальный default)
- Кнопка **Справка** — модалка с видами лицензий и форматом ключа
- Ключи: `WSL1/<edition>/<org>/<yyyy-mm-dd|none>/<max>` (`enterprise` / `trial`) и зашифрованные ключи поставщика; opaque ≥12 → trial 30 дней
- Создание сервиса при квоте/истечении — `403` (`LICENSE_QUOTA_EXCEEDED` / `LICENSE_EXPIRED`)

API: `GET/POST/DELETE /api/v1/settings/license`.

Поведение UI

- Левое меню в стиле страницы Аккаунт: название раздела + короткая подсказка.
- **Save / Discard** только у ADMIN.
- JWT/DB secrets в UI не отдаются.

Техническая страница: Администрирование UI.
