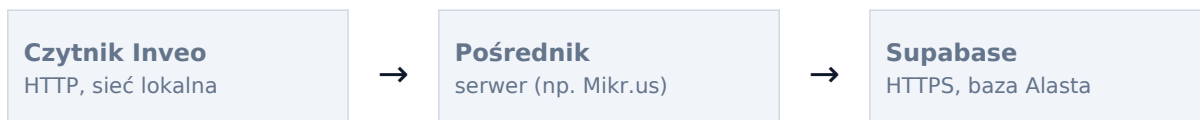


Konfiguracja czytnika Inveo Nano RFID

Rejestracja czasu pracy (RCP) w systemie Alasta — instrukcja krok po kroku

Jak działa system

Czytnik Inveo Nano odczytuje kartę pracownika i wysyła jej numer do systemu Alasta. Ponieważ starsze czytniki (firmware 0.48) komunikują się tylko po HTTP (bez szyfrowania), a baza Supabase wymaga HTTPS, między nimi działa **pośrednik** — mały program na serwerze, który tłumaczy HTTP na HTTPS.



Krok 1 — Dodaj czytnik w systemie Alasta

Zaloguj się do Alasty i przejdź do modułu **RCP** → zakładka **Czytniki**. Kliknij **+ Dodaj czytnik** i wypełnij:

Pole	Wartość
Nazwa	np. „Wejście główne”
Kierunek	Wejście / Wyjście / Auto
Lokalizacja	np. „Hala produkcyjna”
Token	generuje się automatycznie (krótki, 8 znaków)

Po zapisaniu kliknij **Kopiuj URL** przy czytniku. Zapamiętaj **token** (8 znaków po token=) — będzie potrzebny w kroku 4.

WAŻNE: Token czytnika musi być **krótki** (8 znaków). Czytniki Inveo Nano mają mały bufor i ucinają długie tokeny po ok. 22 znakach — wtedy logowanie nie działa. System Alasta generuje teraz krótkie tokeny automatycznie.

Krok 2 — Dodaj karty pracowników

W module **RCP** → **Karty** kliknij **+ Dodaj kartę**, wybierz pracownika i wpisz **numer UID karty**.

Jak poznać UID karty: przyłóż kartę do skonfigurowanego czytnika, następnie wejdź **RCP** → **Czytniki** — w kolumnie „Ostatnie użycie” pojawi się UID ostatnio przyłożonej karty. Skopiuj go.

Krok 3 — Pośrednik HTTP→HTTPS (serwer)

Czytnik z firmware 0.48 nie obsługuje HTTPS, dlatego potrzebny jest pośrednik na serwerze dostępnym całą dobę (np. tani VPS Mikr.us). Pośrednik to kilkanaście linii w Node.js.

Na serwerze (połączenie przez SSH) zainstaluj Node.js i utwórz plik pośrednika. Kluczowy fragment konfiguracji:

```
const LISTEN_PORT = 30507 // port wystawiony na świat
const SUPABASE_HOST = 'twójprojekt.supabase.co'
const FUNCTION_PATH = '/functions/v1/rcp-ingest'
```

Uruchom pośrednik przez menedżer PM2, aby działał 24/7 i startował po restarcie:

```
npm install -g pm2
pm2 start proxy.js --name rfid-proxy
pm2 startup && pm2 save
```

Pełny kod pośrednika (proxy.js) otrzymasz od administratora systemu lub w pakiecie wdrożeniowym Alasta.

Krok 4 — Skonfiguruj czytnik Inveo Nano

Otwórz panel czytnika w przeglądarce (domyślnie `http://192.168.111.15`, login **admin** / hasło **admin00**). Przejdź do ustawień sieci i HTTP.

Ustawienia sieci:

Pole	Wartość
Enable DHCP	odznaczone (stałe IP)
IP Address	adres w Twojej sieci, np. 192.168.50.15
Gateway	adres routera, np. 192.168.50.1
Subnet Mask	255.255.255.0
Primary DNS	8.8.8.8

Ustawienia HTTP (połączenie z pośrednikiem):

Pole	Wartość
HTTP Srv Addr	adres pośrednika, np. maluch2.mikr.us
HTTP Srv Port	port pośrednika, np. 30507
HTTP Resource	<code>/?token=TWOJTOKEN</code>

UWAGA na format HTTP Resource: wpisz dokładnie `/?token=TWOJTOKEN&id=` — zakończony na `&id=` bez wartości. Czytnik sam dokleja numer karty. Używaj **krótkiego tokenu** (8 znaków), bo długi się utnie i zlepi z innymi parametrami.

Krok 5 — Test

- 1 Przyłóż kartę do czytnika.
- 2 Karta przypisana do pracownika → **pojedynczy sygnał + zielona dioda** = wejście zapisane.

3 Karta nieznaną → **trzy sygnały** = dodaj UID karty w RCP → Karty.

4 Sprawdź w Alasie: **RCP → Rejestr czasu** — pracownik ma zdarzenie wejścia.

Weryfikacja połączenia (status.xml):

Wpisz w przeglądarce `http://IP-CZYTNIKA/status.xml`. Pole `<httpClientStatus>` powinno pokazać **200** (połączenie OK). Wartości 3 lub 100 oznaczają problem z siecią/pośrednikiem.

Najczęstsze problemy

Objaw	Przyczyna i rozwiązanie
<code>httpClientStatus = 100</code>	Czytnik nie łączy się z pośrednikiem. Sprawdź czy są w tej samej sieci, czy pośrednik działa, zaporę serwera.
<code>httpClientStatus = 3</code>	Czytnik nie obsługuje HTTPS lub zły adres. Upewnij się, że celuje w pośrednik (HTTP), nie wprost w Supabase.
Trzy sygnały zawsze	Token ucięty (za długi) lub UID karty nieprzypisany. Użyj krótkiego tokenu i dodaj kartę w RCP → Karty.
„Nieznany token” w logach	Token w czytniku różni się od tego w bazie (najczęściej ucięty). Ustaw krótki 8-znakowy token w obu miejscach.
Błąd „too much data POSTed”	Za długie pola w czytniku. Skróć token i ścieżkę HTTP Resource.
„violates check constraint”	Baza odrzuca zapis. Wgraj patch SQL rozszerzający dozwolone wartości (source = reader).
„Missing authorization header”	Funkcja Supabase ma włączone Verify JWT. Wyłącz je w ustawieniach funkcji rcp-ingest.

Alasta — system zarządzania produkcją (WMS / MES / RCP). Dokument wygenerowany automatycznie. W razie problemów skontaktuj się z administratorem systemu.