



Instrukcja obsługi

RAZ-RCP-1 • Rejestrator czasu pracy

Pracownik odbija kartę, a raport liczy się sam.



Aktualna wersja tej instrukcji i pełna deklaracja zgodności
UE: <https://adaraz.com/pl/device/raz-rcp-1?v=1>

ADARAZ

Twoje dane dostępne

Hasła fabryczne i linki do panelu są wydrukowane na etykiecie urządzenia. Etykieta jest z tyłu obudowy, we wnęce na przewody, na półce pod gniazdami (rozdział 2.2). Po zamontowaniu urządzenia na ścianie będzie zasłonięta.

Dlatego w pudełku jest druga etykieta, etykieta zapasowa: jest w ramce w skróconej instrukcji obsługi, czyli kartce dołączonej do urządzenia. Przechowuj tę kartkę w bezpiecznym miejscu. Tej instrukcji (pełnej, online) nie trzeba drukować, żeby mieć dane dostępne.

Panel otworzysz po połączeniu z siecią Wi-Fi urządzenia: wpisz w przeglądarce link z pola LINK DO PANELU / PO PODŁĄCZENIU (rozdział 4.4).

Karta resetująca z pudełka (z naklejką „KARTA RESETUJĄCA”) uruchamia na 5 minut hotspot awaryjny, w którym hasłem panelu z etykiety przywrócisz dane dostępne. Traktuj ją jak kartę płatniczą: schowaj w bezpiecznym miejscu, osobno od urządzenia i od etykiety zapasowej, i nie dawaj jej pracownikom (rozdział 13.1).

Spis treści

	STR.
Twoje dane dostępne	2
1 Bezpieczeństwo	4
2 Poznaj urządzenie	5
3 Sygnały świetlne i dźwiękowe	9
4 Montaż i pierwsze uruchomienie	11
5 Logowanie i konta	13
6 Pracownicy i karty	16
7 Codzienna praca: obecność i czas pracy	18
8 Raporty i eksport	20
9 Ustawienia	22
10 Synchronizacja i Chmura ADARAZ	34
11 Aktualizacje oprogramowania	39
12 Kopia zapasowa	39
13 Reset danych dostępowych, bateria i serwis	40
14 Dane techniczne	49
15 Pasma częstotliwości i maksymalna moc nadawania	53
16 Utylizacja i ochrona środowiska	53
17 Uproszczona deklaracja zgodności UE	54
18 Producent i kontakt	54
19 Gwarancja	54
20 Montaż na ścianie i szablon wiercenia	55

1

Bezpieczeństwo

Przeczytaj ten rozdział, zanim podłączysz urządzenie. Te same informacje są w skróconej instrukcji obsługi (kartce w pudełku).



UWAGA

- Zasilanie: tylko 5 V DC, min. 2 A, przez gniazdo USB-C, z zasilacza z oznakowaniem CE. Nigdy nie podłączaj urządzenia bezpośrednio do sieci 230 V.
- Złącze przekaźnika: tylko prąd stały, najwyżej 24 V DC i 2 A. Zamek musi mieć własny zasilacz. Przewody podłączaj przy odłączonym zasilaniu urządzenia i zamka. Zasilacz zamka może dać prąd kilku amperów: zwarcie zacisków (np. zsunięty wkrętak) iskrzy i może uszkodzić płytkę albo zamek. Zachowaj biegunowość: przy odwrotnym podłączeniu zamek jest zasilany cały czas.
- Gdy przekaźnik steruje drzwiami, ustaw w panelu tryb „tylko karty pracowników”. W trybie „każda karta” zamek otworzy każda karta (rozdział 9.6).
- W środku jest bateria litowa pastylkowa CR2032 (3 V). Trzymaj baterie z dala od dzieci: potknięcie może w ciągu 2 godzin spowodować ciężkie oparzenia wewnętrzne, w razie potknięcia natychmiast jedź do lekarza. Nie ładuj, nie zwieraj, nie rozbieraj, nie wrzucaj do ognia. Używaj tylko baterii CR2032 3 V: inny typ grozi wybuchem. Baterię wymienisz sam (rozdział 13.4). Karty i breloki też trzymaj z dala od małych dzieci.
- Tylko do użytku wewnątrz pomieszczeń, temperatura pracy od 0 do 50 °C. Chroń przed wilgocią i zalaniem. Czyść suchą, miękką ściereczką.
- W czasie aktualizacji oprogramowania nie odłączaj zasilania.

Fale radiowe. Urządzenie nadaje w paśmie 2,4 GHz (Wi-Fi), a czytnik kart wytwarza pole magnetyczne 13,56 MHz (NFC/RFID). Pasma i maksymalną moc nadawania podaje rozdział 15.

Otwieranie obudowy. Obudowę otwierasz tylko wtedy, gdy trzeba nacisnąć przycisk reset (rozdział 13.2) albo wymienić baterię (rozdział 13.4). Przed resetem przyciskiem odetnij zasilanie obwodu, którym steruje przekaźnik (zamek, rygła,

szlabanu), ale samo urządzenie zostaw włączone. Przed wymianą baterii odłącz zasilanie i wszystkie przewody. Otwieraj powoli: w środku są cienkie przewody anteny i czytnika (antena jest podłączona do płytki cienkim przewodem i łatwo ją wyrwać).

Papierowa instrukcja. Papierową wersję tej instrukcji wyślemy bezpłatnie na prośbę: napisz na contact@adaraz.com.

1.1 Symbole na etykiecie

Symbol	Znaczenie
	Znak CE: urządzenie spełnia zasadnicze wymagania unijnego prawodawstwa harmonizacyjnego.
	Przekreślony koszyk: zużytego urządzenia i baterii nie wolno wyrzucać z odpadami komunalnymi (rozdział 16).
	RoHS: urządzenie spełnia wymagania dyrektywy 2011/65/UE w sprawie substancji niebezpiecznych.
	Prąd stały (DC).



2

Poznaj urządzenie

RAZ-RCP-1 to czytnik kart zbliżeniowych do rejestracji czasu pracy. Pracownik przykładą kartę, a urządzenie zapisuje odbicie z datą i godziną w swojej pamięci. Panel w przeglądarce liczy z odbić obecność i czas pracy. Nie trzeba instalować żadnego programu.

Urządzenie działa także bez sieci: odbicia zapisuje u siebie, a czas utrzymuje wbudowany zegar. Może też sterować zamkiem drzwi oraz wysyłać odbicia do Chmury ADARAZ albo na Twój serwer.

2.1 W pudełku

- rejestrator RAZ-RCP-1,
- skrócona instrukcja obsługi (kartka) z etykietą zapasową,
- zamówione karty i breloki RFID (standardowy zestaw: 5 breloków i 5 kart),
- karta resetująca z naklejką „KARTA RESETUJĄCA”.

Zasilacz nie wchodzi w skład zestawu: użyj zasilacza USB-C 5 V DC, min. 2 A, z oznakowaniem CE (można go zamówić osobno).

Tę pełną instrukcję znajdziesz online pod adresem z kartki (kod QR). Karty i breloki przypisujesz pracownikom (rozdział 6). Karta resetująca nie jest kartą pracownika: jest przypisana do tego urządzenia już u producenta, przy pierwszym uruchomieniu na kontroli jakości, i służy do odzyskania dostępu do panelu (rozdział 13.1).

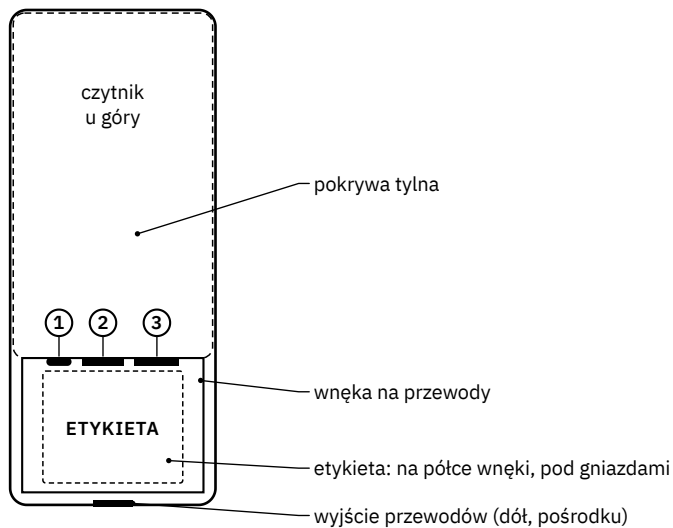
2.2 Tył obudowy i wnęka na przewody

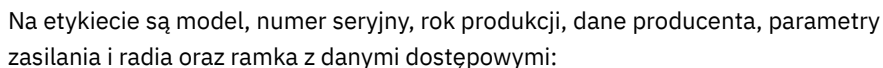
Tak wygląda urządzenie od tyłu, czyli od strony ściany, w pozycji montażu: czytnik kart jest u góry, a przewody wychodzą dołem. W dolnej części tyłu jest wnęka na przewody. Na jej górnej ścianie są gniazda, od lewej:

- ① **Gniazdo USB-C:** zasilanie 5 V DC.
- ② **Złącze przekaźnika:** 3 zaciski śrubowe do zamka drzwi (rozdział 9.6).
- ③ **Gniazdo Ethernet (RJ45):** sieć przewodowa.

Etykieta jest naklejona na półce wnęki, pod gniazdami. Przewody wychodzą z wnęki na dole obudowy, pośrodku.

Tył (strona do ściany)



8

W hasłach wszystkie litery są małe i nie ma znaków 0, o, 1, l ani i. Numer seryjny ma postać RCP1-RR-XXXXXXXX, gdzie RR to dwie ostatnie cyfry roku produkcji, a XXXXXXXX to te same 8 znaków co w nazwie sieci Wi-Fi.

2.4 Jakie karty działają

Czytnik odczytuje karty i breloki zbliżeniowe 13,56 MHz standardu ISO/IEC 14443 typu A (np. MIFARE). Odczytuje tylko numer karty (UID), nie odczytuje innych danych zapisanych na karcie (rozdział 14.3).

Telefony, zegarki i zwykle także karty płatnicze podają przy każdym przyłożeniu inny, losowy numer. Czytnik odrzuca takie numery (czerwone światło i dwa długie niskie dźwięki), więc nie można ich używać zamiast karty.

2.5 Miejsce montażu

Urządzenie jest przeznaczone tylko do pracy wewnątrz pomieszczeń, w temperaturze od 0 do 50 °C. Nie montuj go na zewnątrz budynku ani w miejscu narażonym na wilgoć i zalanie.

Duże metalowe elementy w pobliżu pogarszają odczyt kart i zasięg Wi-Fi. Nie montuj urządzenia na metalowej powierzchni ani tuż obok niej.

3

Sygnały świetlne i dźwiękowe

W spoczynku dioda nie świeci.

Sytuacja	Światło	Dźwięk
Włączenie zasilania	przez chwilę niebieskie i zielone na przemian, potem gaśnie	melodia z 4 rosnących dźwięków
Wejście	zielone	3 dźwięki: niski, wysoki, wysoki
Wyjście	niebieskie	3 dźwięki: wysoki, niski, niski

Sytuacja	Światło	Dźwięk
Odbicie przy włączonej opcji „Zawsze 3 krótkie”	zielone (wejście) lub niebieskie (wyjście)	3 krótkie
Odbicie, gdy na liście jest ponad 256 kart	zielone	3 krótkie
Ta sama karta ponownie w czasie blokady powtórzeń; odbicie NIE jest zapisane	białe	2 krótkie niskie
Karta pozostawiona na czytniku albo przyłożona ponownie w ciągu ok. 2,5 s od poprzedniego odczytu (przy włączonej blokadzie powtórzeń)	brak	brak
Karta odrzucona: spoza listy (tryb „tylko karty pracowników”), telefon, zegarek, karta płatnicza albo błąd zapisu (np. pełna pamięć); odbicie NIE jest zapisane	czerwone	2 długie niskie
Odczyt karty w panelu („Odczytaj kartę”); to nie jest odbicie	białe	5 krótkich
Przycisk reset przytrzymany ponad 1 s	żółte	brak
Karta resetująca: start trybu awaryjnego (rozdział 13.1)	żółte	2 krótkie, potem restart
Reset danych dostępowych (przycisk albo hasło z etykiety w trybie awaryjnym)	żółte	2 krótkie i 1 długi, potem restart
Koniec trybu awaryjnego bez resetu (minął czas albo 5 złych haseł)	brak	2 długie niskie, potem restart
Aktualizacja oprogramowania	miganie na niebiesko; na koniec zielone (udana) albo czerwone (nieudana)	brak

Sytuacja	Światło	Dźwięk
Przywracanie ustawień fabrycznych	miganie na czerwono i żółto na przemian, zwykle około minuty (do 3 minut), na koniec zielone	1 długi na początku
Czytnik kart nie odpowiada	stałe żółte	brak; panel pokazuje „czytnik kart nie odpowiada”
Błąd czytnika przy starcie	czerwone przez 2 s, potem restart	brak

Dźwięk sukcesu urządzenie wydaje dopiero wtedy, gdy odbicie jest już zapisane w pamięci.

Jeśli przy włączaniu dioda świeci na czerwono, a urządzenie wydaje 3 lub 5 niskich dźwięków, skontaktuj się z producentem.

4

Montaż i pierwsze uruchomienie

4.1 Przed montażem

- 1 Etykieta zapasowa jest naklejona w ramce w skróconej instrukcji obsługi (kartce w pudełku). Zachowaj ją: po zamontowaniu etykieta na obudowie będzie zastąpiona.
- 2 Podłącz przewody we wnęce: jeśli chcesz, kabel Ethernet do gniazda RJ45 i przewody zamka do złącza przełącznika (rozdział 9.6), a na końcu przewód zasilacza do gniazda USB-C (4.2). Przewody wyprowadź z wnętrza dołem, przez wyjście przewodów pośrodku dolnej krawędzi obudowy (rozdział 2.2).
- 3 Zawieś urządzenie na ścianie czytnikiem do góry, tak żeby przewody wychodziły dołem: na czterech wkrętach w rozstawie 30 x 60 mm (wkręty, kołki i szablon wiercenia: rozdział 20). Pamiętaj o metalu w pobliżu i o warunkach pracy (rozdział 2.5).

4.2 Zasilanie

Podłącz zasilacz 5 V DC, 2 A do gniazda USB-C. Urządzenie zagra melodię, dioda mignie na przemian na niebiesko i zielono, a potem zgaśnie. Urządzenie jest przeznaczone do pracy ciągłej.

4.3 Połączenie z hotspotem urządzenia

Urządzenie ma własną sieć Wi-Fi (hotspot). Fabrycznie jest ona włączona.

- ① Na telefonie lub komputerze wybierz sieć z pola SIEĆ WI-FI na etykiecie.
- ② Wpisz HASŁO WI-FI z etykiety. Zamiast tego możesz zeskanować aparatem telefonu kod QR „Połącz z Wi-Fi”.
- ③ Jeśli telefon zapyta, czy zostać w sieci bez dostępu do internetu, wybierz pozostanie w sieci.

Do hotspotu mogą być podłączone jednocześnie najwyżej 4 urządzenia. Hotspot działa w paśmie 2,4 GHz i jest zabezpieczony WPA2/WPA3.

4.4 Otwarcie panelu

Po połączeniu z hotspotem wpisz w pasku adresu przeglądarki (nie w wyszukiwarce) jeden z dwóch linków z pola LINK DO PANELU / PO PODŁĄCZENIU na etykiecie. Strona logowania nie otworzy się sama.

- **http://rcp-xxxxxxx.local:** xxxxxxxx to 8 znaków z nazwy sieci Wi-Fi urządzenia, pisane małymi literami. Czy ten link zadziała, zależy od telefonu lub komputera.
- **http://10.10.10.1:** w sieci Wi-Fi urządzenia działa zawsze. Jest taki sam w każdym urządzeniu.

Na hotspocie oba linki otwierają pełny panel. Działa tam też **https://10.10.10.1**, ale przeglądarka pokaże ostrzeżenie o certyfikacie, bo fabryczny certyfikat jest samopodpisany i wystawiony na nazwę urządzenia (rcp-xxxxxxx.local), a nie na adres IP.

Gdy urządzenie jest podłączone do sieci firmowej (Ethernet albo Wi-Fi), z komputera w tej sieci zadziała tylko pierwszy link z etykiety,

http://rcp-xxxxxxx.local, i to dopiero po włączeniu „Dostęp z sieci lokalnej”. Przeglądarka przejdzie wtedy na **https://** (rozdział 9.3). Link **http://10.10.10.1** działa tylko w sieci Wi-Fi urządzenia.

4.5 Logowanie

- ① W polu „Login” jest już wpisane „admin”.
- ② W polu „Hasło” wpisz HASŁO PANELU z etykiety.
- ③ Kliknij „Zaloguj”.

Przy błędnych danych panel pokaże „Nieprawidłowy login lub hasło”.

4.6 Pierwsze ustawienia

- ① **Zegar.** Wejdź w Ustawienia > System > Data i czas i kliknij „Synchronizuj z przeglądarką”. Gdy urządzenie ma dostęp do internetu, samo pobiera czas z sieci.
- ② **Hasło.** Zmień hasło konta admin (rozdział 5.2). Panel nie wymusza zmiany, ale ją zalecamy.
- ③ **Pracownicy.** Dodaj pracowników i ich karty (rozdział 6). Dopóki lista jest pusta, „Pulpit” pokazuje „Zacznij od dodania pracowników” i przycisk „Przejdź do Pracowników”.
- ④ **Sieć firmowa (opcjonalnie).** Jeśli chcesz otwierać panel z komputera w sieci firmowej, przeczytaj rozdziały 9.2 i 9.3.
- ⑤ **Karta resetująca.** Schowaj ją w bezpiecznym miejscu (rozdział 13.1).

5 Logowanie i konta

5.1 Dwa konta

Konto	Co widzi i co może
admin	Wszystko, w tym „Ustawienia”. Konto jest zawsze aktywne.
biuro	„Pulpit”, „Raporty” („Lista obecności”, „Czas pracy”, „Edycja”), „Pracownicy”, „Odśwież dane”, „Kopia zapasowa”. Może edytować pracowników, dodawać i usuwać odbicia oraz odczytywać karty. Nie widzi „Ustawień”. Fabrycznie wyłączone.

Włączenie konta „biuro”: Ustawienia > Bezpieczeństwo > Konta i dostęp, pole Konto „biuro”. Wpisz hasło (podpowiedź w panelu: „ustaw hasło = włącz konto”) i kliknij „Zapisz ustawienia”. Login tego konta to „biuro”. Konto wyłączyz przyciskiem „Wyłącz konto”; osoby zalogowane na nim zostaną wylogowane.

5.2 Hasła

Hasło admina zmienisz w sekcji Ustawienia > Bezpieczeństwo > Konta i dostęp: wpisz nowe hasło w pole „Hasło admina” i kliknij „Zapisz ustawienia”. Zmiana hasła wylogowuje wszystkie sesje admina, więc od razu zalogujesz się nowym hasłem.

Zasady haseł:

- hasło konta admin i konta „biuro”: co najmniej 10 znaków,
- hasło hotspotu Wi-Fi: co najmniej 8 znaków,
- panel odrzuca hasła z jednego powtózonego znaku oraz hasła zawierające m.in. 12345678, password, hasło, qwerty, admin, 0000, 1111 lub abcdef.

Etykieta zawsze pokazuje hasła fabryczne. Reset danych dostępowych (rozdział 13) przywraca właśnie je.

5.3 Ochrona przed zgadywaniem i sesje

- Pierwsze 5 nieudanych prób nie ma skutków. Po każdej kolejnej nieudanej próbie logowanie na to konto jest wstrzymywane: na 2 s, potem na 4, 8, 16, 32 i najwyżej 60 s. W tym czasie panel pokazuje „Nieprawidłowy login lub hasło” nawet przy dobrym hasle, więc odczekaj chwilę. Licznik zeruje się po udanym logowaniu.
- Nieudane logowania, blokady konta i błędne kody 2FA są zapisywane w dzienniku zdarzeń (rozdział 9.9) razem z adresem IP urządzenia, z którego próbowano się zalogować.
- Sesja trwa 16 godzin. Jednocześnie może być otwartych do 8 sesji; kolejne logowanie zamyka najstarszą. Restart urządzenia wylogowuje wszystkich.
- Przycisk „Wyloguj” w menu kończy sesję.

5.4 Drugi składnik logowania (2FA)

Konto admin można dodatkowo chronić kodem z aplikacji uwierzytelniającej (Google Authenticator, Aegis, Bitwarden albo dowolna aplikacja TOTP).

- ① Najpierw ustaw zegar urządzenia (rozdział 9.4).
- ② Wejdź w Ustawienia > Bezpieczeństwo > Drugi składnik (2FA) i kliknij „Włącz”.
- ③ Zeskanuj kod QR w aplikacji. Jeśli to niemożliwe, kliknij „Nie mogę zeskanować” i wpisz klucz ręcznie.
- ④ Wpisz sześć cyfr w pole „Kod z aplikacji” i kliknij „Włącz drugi składnik”.

Przy logowaniu, po hasle, pojawi się „Krok 2 z 2 · kod jednorazowy”. Kod zmienia się co 30 sekund. Po trzech błędnych kodach trzeba zacząć od hasła. Drugi składnik wyłączyz przyciskiem „Wyłącz”, podając aktualny kod.



WSKAZÓWKA

Zgubiony telefon z aplikacją? Reset danych dostępowych (rozdział 13) wyłącza drugi składnik konta admin.

5.5 Język panelu

Panel działa po polsku, angielsku i niemiecku. Język wybierzesz z listy przy ikonie języka na ekranie logowania albo na dole menu bocznego. Wybór jest zapamiętywany tylko w tej przeglądarce. Język dla nowych przeglądarek ustawisz w sekcji Ustawienia > System > Panel, w polu „Domyślny język panelu”.

5.6 Nie pamiętasz hasła?

Na ekranie logowania kliknij „Nie pamiętasz hasła?”. Panel zapyta „Masz kartę resetującą?” i poprowadzi Cię przez reset kartą albo przyciskiem. Opis jest w rozdziale 13. Na ekranie logowania jest też odnośnik „Instrukcja obsługi”.

6

Pracownicy i karty

Urządzenie zapisuje każde odbicie. Dopóki karta nie ma przypisanej osoby, w raportach zobaczysz „Nieznana karta”, a czas pracy nie jest dla niej liczony.

6.1 Dodanie pracownika: przyłóż kartę

- ① Wejść w „Pracownicy” i kliknij „Odczytaj kartę”. Przycisk zmieni napis na „Przyłóż kartę...”.
- ② Przyłóż kartę do czytnika. Dioda zaświeci na biało, a urządzenie piknie 5 razy. Panel pokaże „Odczytano:” i numer karty. W tym trybie przyłożenie karty nie jest odbiciem. Nie przykładaj karty resetującej: także w tym trybie uruchomi tryb awaryjny (rozdział 13.1).
- ③ Otworzy się ramka „Przypisz kartę”. W polu „Do pracownika” zostaw „- nowy pracownik -”, a w polu „Imię i nazwisko” wpisz imię i nazwisko pracownika. Jeśli dodajesz kolejną kartę istniejącej osobie, wybierz ją z listy. Karta z numerem 10-bajtowym (20 znaków) ma w ramce pełny numer i odpowiedź: na listę pracowników trafi 7 pierwszych bajtów (14 znaków), bo po nich urządzenie rozpoznaje taką kartę także w odbiciach.
- ④ Kliknij „Przypisz”. Panel pokaże „Przypisano - pamiętaj zapisać na urządzenie”.
- ⑤ Kliknij „Zapisz”. Panel pokaże „Zapisano listę pracowników”.

Tryb odczytu wyłącza się sam po odczytaniu karty albo po 2 minutach.

6.2 Dodanie pracownika: wpisz numer karty

- ① Na dole strony „Pracownicy” wpisz imię i nazwisko w pole „imię i nazwisko” i kliknij „Dodaj pracownika”.
- ② W wierszu tej osoby wpisz numer karty w pole „dodaj UID (hex)” i kliknij „+”.
- ③ Kliknij „Zapisz”.

Numer karty (UID) wpisuje się szesnastkowo, ma od 4 do 7 bajtów, np. 04a1b2c3. Kartę z numerem 10-bajtowym urządzenie rozpoznaje po 7 pierwszych bajtach: numer 20-znakowy panel sam skróci do 14 znaków i pokaże o tym komunikat. Jeśli numer jest już przypisany, panel pokaże „Ten UID ma już” i nazwisko osoby.

6.3 Przypisanie nieznanej karty z raportów

Przy pozycji „Nieznana karta” na „Pulpicie” (tabela „W pracy teraz”), w „Liście obecności” lub w „Edycji” kliknij „przypisz”. W sekcji „Nieznane karty dziś” na „Pulpicie” kliknij ikonę osoby z plusem przy numerze karty. Otworzy się strona „Pracownicy” z wpisanym numerem karty. Dalej postępuj jak w 6.1, od kroku 3.

6.4 Zmiany na liście

- **Zmiana nazwiska:** popraw tekst w polu z imieniem i nazwiskiem.
- **Usunięcie osoby:** ikona kosza „Usuń pracownika”, potem potwierdzenie.
- **Odpięcie karty:** „x” przy numerze karty („Odepnij kartę”).
- Jedna osoba może mieć kilka kart.
- Osobę rozpoznaje się po imieniu i nazwisku. Dwie osoby nie mogą mieć identycznego wpisu, więc przy takich samych nazwiskach dodaj np. drugie imię.
- Na imię i nazwisko urządzenie ma 37 bajtów: zwykła litera zajmuje jeden, litera z polskim znakiem dwa. Dłuższy wpis zostanie przy zapisie skrócony.



UWAGA

Zmiany na liście pracowników są zapisywane w urządzeniu dopiero po kliknięciu „Zapisz”. Do tego czasu u góry widać pasek „Niezapisane zmiany - pracownicy”.

Jeśli w międzyczasie ktoś inny zmienił listę na urządzeniu, panel ostrzeże, że zapis nadpisze tamte zmiany. Jeśli zapis zostanie przerwany (np. zerwane połączenie z urządzeniem), urządzenie zostawia poprzednią listę; kliknij „Zapisz” jeszcze raz. Rekord listy uszkodzony w pamięci urządzenia (błędna suma kontrolna) nie jest pracownikiem: czytnik go nie uznaje, a panel pomija go na liście i w raportach i pokazuje u góry ostrzeżenie „Uszkodzone rekordy listy pracowników (błędna suma kontrolna): ... - pominięte, czytnik też ich nie uznaje. Sprawdź, czy na liście są wszyscy pracownicy i karty.” (można je zamknąć do następnego pobrania danych). Dodaj brakujące osoby i karty ponownie i kliknij „Zapisz”: panel zapyta, czy zapisać, bo zapis usunie uszkodzone rekordy z urządzenia. Odpowiedź „Anuluj” nic nie zapisuje, a zmiany zostają w panelu.

Panel nie ma importu ani eksportu samej listy pracowników. Listę zawiera kopia zapasowa (rozdział 12).

6.5 Kto może odbić kartę

Ustawienia > Czytnik > Kontrola dostępu, pole „Tryb”:

- **„każda karta”** (fabrycznie): urządzenie zapisuje każdą pasującą kartę. Karty bez osoby pojawiają się w raportach jako „Nieznana karta”.
- **„tylko karty pracowników”**: urządzenie przyjmuje tylko karty z listy. Inne odrzuca (czerwone światło i dwa długie niskie dźwięki) i nie zapisuje. Przy pustej liście panel ostrzega: „Uwaga: lista pracowników jest pusta - nikt nie odbije karty.”

6.6 Ponad 256 kart

Gdy na liście jest więcej niż 256 kart (liczą się karty, nie osoby), czytnik przestaje rozróżniać wejście i wyjście. Przy każdym odbiciu daje zielone światło i 3 krótkie dźwięki, a panel pokazuje „ponad 256 kart - bez wejścia/wyjścia, jeden sygnał”. Godziny w raportach liczą się tak samo, bo panel paruje odbicia po kolei.

7

Codzienna praca: obecność i czas pracy

7.1 Odbicie karty

Pracownik przykładą kartę do czytnika. Pierwsze odbicie to wejście (zielone światło), następne to wyjście (niebieskie światło) i tak na zmianę.

Blokada powtórzeń. Ta sama karta przyłożona ponownie w ciągu 5 sekund od poprzedniego przyłożenia (wartość fabryczna) nie jest zapisywana. Każde przyłożenie, także niezapisane, liczy ten czas od nowa. Urządzenie daje wtedy białe światło i dwa krótkie niskie dźwięki. Czas blokady zmienisz w sekcji Ustawienia > Czytnik > Kontrola dostępu, w polu „Blokada powtórzeń [s]” (od 0 do 3600 s; 0 wyłącza blokadę). Przy wartości 0 karta pozostawiona na czytniku jest zapisywana mniej więcej co sekundę.

Bez sieci. Odbicia zapisują się w pamięci urządzenia także bez sieci. Czas utrzymuje wbudowany zegar.

7.2 Menu panelu

Pozycja	Do czego służy
Pulpit	kto jest teraz w pracy i co trzeba sprawdzić
Raporty › Lista obecności	obecność w kolejnych dniach
Raporty › Czas pracy	godziny pracy i zmiany
Raporty › Edycja	poprawianie odbić
Pracownicy	lista osób i ich kart
Ustawienia	konfiguracja urządzenia (tylko admin)
Odśwież dane	pobranie aktualnych danych z urządzenia
Kopia zapasowa	pobranie kopii danych (plik ZIP)
Wyloguj	koniec sesji

Na dole menu panel pokazuje stan urządzenia („online” i czas od uruchomienia), godzinę pobrania danych („dane z ...”), ostrzeżenia, np. „brak sieci ETH”, „czytnik kart nie odpowiada” i (tylko na koncie admin) „wysyłanie odbić wstrzymane (HTTP poza siecią lokalną)” (rozdział 10.2), a po dołączeniu do sieci Wi-Fi napis „WiFi połączone”.

7.3 Pulpit

- Kafelki: „W pracy teraz”, „Do sprawdzenia”, „Odbicia dziś”, „Pracownicy”.
- **„W pracy teraz”**: osoby, które weszły i jeszcze nie wyszły, z godziną wejścia i czasem w pracy.
- **„Do sprawdzenia”**: zmiany z ostatnich 7 dni, które wyglądają na błędne („zmiana dłuższa niż 9 h” albo „dwa odbicia w kilkadziesiąt sekund”). Przycisk „Popraw” otwiera „Edycję”. Kafelek liczy też osoby, które są w pracy od co najmniej 9 h: w tabeli „W pracy teraz” mają oznaczenie „brak odbicia wyjścia” i ikonę edycji.
- **„Nieznane karty dziś”**: karty bez przypisanej osoby, z ikoną przypisania (osoba z plusem).
- **„Zakończone dziś”**: pierwsze i ostatnie odbicie, liczba odbić i czas.

7.4 Odświeżanie danych

Panel pobiera odbicia i listę pracowników z urządzenia do przeglądarki i tam liczy raporty. **Nowe odbicia nie pojawiają się same.** Kliknij „Odśwież dane”. Rekord odbicia uszkodzony w pamięci urządzenia (błędna suma kontrolna) panel pomija w raportach i eksporcie i pokazuje ostrzeżenie „Uszkodzone rekordy odbić (błędna suma kontrolna): ... - pominięte, nie liczą się w ewidencji.”; urządzenie nie wysyła go też na serwer. Ostrzeżenie można zamknąć („Zamknij”), ale wraca przy kolejnym pobraniu danych. Brakujące odbicie dodasz w „Edycji” (8.4).

Po ponad 5 minutach bezczynności panel pokaże komunikat o bezczynności i przycisk „Przetłóć dane”. Przetłóć dane, zanim zaczniesz dalszą edycję.

8

Raporty i eksport

8.1 Jak liczony jest czas pracy

Odbicia jednej osoby są łączone w pary po kolei: 1. z 2., 3. z 4. i tak dalej. Każda para to jedna zmiana: wejście i wyjście. Zmiana nie jest dzielona o północy, więc nocna zmiana liczy się jako jedna.



UWAGA

Jedno brakujące odbicie przesuwą parowanie wszystkich następnych odbić tej osoby. Popraw je w „Edycji” (8.4).

8.2 Lista obecności

- ① Wybierz „Od” i „Do” albo skorzystaj z „Szybki wybór”: „Dziś”, „Wczoraj”, „Ten miesiąc”, „Poprzedni miesiąc”.
- ② Wybierz osobę albo „- wszyscy -”.

Raport pokazuje dla każdego dnia „Status”: „Obecny” lub „Nieobecny” (sobota i niedziela bez odbić zostają puste) oraz podsumowanie „obecny: ... · nieobecny: ... z ... dni roboczych”.

**UWAGA**

Dni robocze to poniedziałek-piątek. Raport nie uwzględnia świąt.

8.3 Czas pracy

Te same pola wyboru co w „Liście obecności”. Raport pokazuje dla każdego dnia „Zmiany” i „Czas”, a na końcu wiersz „RAZEM”. Zmiana bez wyjścia jest oznaczona jako „niekompletne”.

8.4 Edycja odbić

Każdy wiersz to jedna zmiana: „Osoba”, „Data”, „Wejście”, „Wyjście”, „Czas”, „Potencjalny problem”.

- Kliknij godzinę, żeby ją zmienić.
- **„Dodaj wyjście”**: gdy zmiana nie ma wyjścia.
- **„wstaw”** („Wstaw odbicie”): wstawia brakujące odbicie w środku zmiany; dalsze odbicia tej osoby przeliczą się same.
- **„Usuń samo wejście”, „Usuń samo wyjście”**: usunięcie połowy zmiany przesuną parowanie następnych odbić tej osoby.
- **„Usuń całą zmianę”**: bezpieczne, usuwa wejście i wyjście.
- **„Dodaj odbicie”**: dla osoby, która zapomniała odbić kartę. Wybierz osobę („- wybierz osobę -”), datę i godzinę, potem „Dodaj”. Osoba musi mieć przypisaną kartę.

Po zmianach kliknij „Zapisz” u góry strony albo na pasku „Niezapisane zmiany - odbicia”. Zapis wysyła tylko zmiany, więc odbicia zrobione w międzyczasie nie przepadną.

8.5 Eksport i druk

- **„Eksport XLSX”**: plik Excel z arkuszem „Podsumowanie” i osobnym arkuszem dla każdej osoby. Nazwy plików: czas-pracy_<od>_<do>.xlsx i obecność_<od>_<do>.xlsx.
- **„Drukuj / PDF”** (w „Liście obecności” i „Czasie pracy”): drukowanie raportu z przeglądarki albo zapis do PDF.

8.6 Gdy raporty są w innym systemie

Gdy włączone jest „Usuwanie odbicia po wysłaniu” albo urządzenie jest połączone z Chmurą ADARAZ, urządzenie przechowuje tylko odbicia jeszcze niewysłane. „Pulpit”, „Lista obecności”, „Czas pracy” i „Edycja” pokazują wtedy tylko komunikat „Synchronizacja z serwerem jest aktywna”. Obecność i czas pracy rozliczasz w systemie, do którego trafiają odbicia.

9

Ustawienia

„Ustawienia” widzi tylko konto admin. Mają zakładki: „Sieć”, „Bezpieczeństwo”, „Czytnik”, „Integracje”, „System”.

9.1 Zapisywanie

Jeden przycisk „Zapisz ustawienia” zapisuje wszystkie zakładki. Obok jest „Restartuj urządzenie”. Zmiany hotspotu, Ethernetu i dołączania do sieci Wi-Fi oraz włączenie lub wyłączenie nazwy w sieci lokalnej (mDNS) zaczynają działać dopiero po restarcie. Pozostałe ustawienia działają od razu po zapisie. Panel po zapisie zwykle pokazuje „Ustawienia zapisane - wymagany restart”; jeśli nie zmieniłeś żadnego z tych czterech ustawień, restart nie jest potrzebny. Jeśli zapis się nie uda, panel pokaże błąd zapisu, a ustawienia (także hasła) zostają takie jak przed zapisem; spróbuj ponownie, a gdy błąd się powtarza, skontaktuj się z producentem.

9.2 Sieć

„**Połączenie**”: adres IP z Ethernetu (albo „brak połączenia”) i adres w sieci Wi-Fi, gdy urządzenie do niej dołączyło.

„**Hotspot WiFi**”:

- „Nazwa sieci (SSID)” i „Hasło” (min. 8 znaków; puste pole zostawia obecne hasło),
- „Hotspot włączony”.

**UWAGA**

Jeśli wyłączysz hotspot, a „Dostęp z sieci lokalnej” (9.3) jest wyłączony, panel będzie niedostępny aż do resetu danych dostępowych (rozdział 13).

„Sieć WiFi (dołączanie)”: urządzenie łączy się z Twoją siecią Wi-Fi, a hotspot działa obok.

- ① Włącz „Dołącz do sieci WiFi”.
- ② W „Wyszukaj sieci” kliknij „Skanuj” i przy swojej sieci kliknij „wybierz”. Na czas skanu panel może na chwilę przestać odpowiadać. Sieci ukrytej nie ma na liście: wpisz jej nazwę w „Nazwa sieci (SSID)”.
- ③ Wpisz „Hasło” albo zaznacz „Sieć bez hasła (otwarta)”.
- ④ Kliknij „Zapisz ustawienia” i zrestartuj urządzenie.

Urządzenie obsługuje tylko sieci 2,4 GHz. Gdy połączenie się nie uda, próbuje 5 razy co 10 sekund, a potem co 5 minut.

„Interfejsy”:

- „Ethernet”: fabrycznie włączony. Adres urządzenia dostaje tylko automatycznie (DHCP); stałego adresu IP nie da się ustawić.
- „Nazwa w sieci lokalnej (mDNS)” : urządzenie ogłasza w sieci nazwę `rcp-xxxxxxx.local`. Fabrycznie włączona. Po jej wyłączeniu link **`http://rcp-xxxxxxx.local`** z etykiety przestaje działać; na hotspotcie zostaje **`http://10.10.10.1`**.
- „Moc nadawania WiFi”: od 14 dBm („fabrycznie”) do 2 dBm. Dotyczy hotspotu i dołączania do sieci. Niższa moc to mniej zakłóceń dla czytnika kart.

Gdy urządzenie ma dostęp do internetu, samo ustawia zegar z sieci.

9.3 Panel z sieci firmowej

Fabrycznie panel odpowiada tylko na hotspotcie urządzenia. Z Ethernetu i z sieci Wi-Fi panel jest niedostępny: przeglądarka nie połączy się z urządzeniem, a link **`http://rcp-xxxxxxx.local`** nie odpowiada.

Żeby otwierać panel z sieci firmowej:

- ① Na hotspocie wejdź w Ustawienia > Bezpieczeństwo > Certyfikat i dostęp.
- ② Włącz „Dostęp z sieci lokalnej” i kliknij „Zapisz ustawienia”. Restart nie jest potrzebny.
- ③ Z komputera w sieci firmowej otwórz link **http://rcp-xxxxxxx.local** z etykiety (przeglądarka przejdzie na **https://rcp-xxxxxxx.local**) albo wpisz https:// i adres IP z sekcji Ustawienia > Sieć > Połączenie.

Z sieci firmowej panel działa wyłącznie przez HTTPS; adres http:// przekierowuje na https://. Link **http://10.10.10.1** z etykiety działa tylko w sieci Wi-Fi urządzenia. Na hotspocie oba linki z etykiety działają nadal, także po http://.

Certyfikat. Fabrycznie urządzenie ma certyfikat samopodpisany, więc przy pierwszym wejściu przeglądarka pokaże ostrzeżenie. Porównaj „Odcisk SHA-256” z sekcji Ustawienia > Bezpieczeństwo > Certyfikat i dostęp z odciskiem, który pokaże przeglądarka. W tej samej sekcji widać „Ważny do”.

Jeśli firma ma własny urząd certyfikacji, w „Źródło certyfikatu” wybierz „własny, podpisany przez Twoje CA”:

- ① Kliknij „Pobierz wniosek” (CSR wystawiony na nazwę urządzenia w sieci lokalnej, rcp-xxxxxxx.local).
- ② Podpisz wniosek w swoim urządzie certyfikacji.
- ③ Wklej łańcuch w „Podpisany łańcuch (PEM)” (najpierw certyfikat urządzenia, pod nim pośrednie, bez certyfikatu głównego) i kliknij „Zainstaluj certyfikat”.

Klucz prywatny nigdy nie opuszcza urządzenia.

9.4 Data, czas i język

Ustawienia > System > Data i czas:

- „Czas urządzenia”: panel pokazuje różnicę względem przeglądarki, gdy przekracza 120 s,
- „Synchronizuj z przeglądarką” albo „Ustaw ręcznie” i „Ustaw”,
- „Strefa czasowa”: fabrycznie Europe/Warsaw. Raporty i godziny w panelu są liczone w tej strefie,
- „Serwer czasu 1 (SNTP)” i „Serwer czasu 2 (SNTP)”: fabrycznie tempus1.gum.gov.pl (czas urzędowy RP z Głównego Urzędu Miary) i pool.ntp.org. Urządzenie z dostępem do internetu ustawia czas samo z pierwszego serwera, a gdy ten nie odpowiada, z drugiego. Wpisz nazwę albo adres IP serwera, np. serwera czasu w sieci firmy. Puste pole oznacza, że serwer nie jest używany; przy obu pustych urządzenie nie pobiera czasu z sieci. Zmiana działa po „Zapisz ustawienia”, bez restartu. Urządzenie przyjmuje odpowiedź tylko od serwera, o który zapytało, i tylko z datą od 2026 do 2099 r. Serwer czasu nie może cofnąć zegara wcześniej niż do ostatniego czasu pobranego z serwera (z tolerancją 1 minuty); zegar cofniesz ręcznie przyciskiem „Ustaw” albo „Synchronizuj z przeglądarką”.

Czas jest zapisywany także w zegarze urządzenia, który działa po odłączeniu zasilania.

Ustawienia > System > Panel > „Domyślny język panelu”: język dla nowych przeglądarek (rozdział 5.5).

9.5 Czytnik

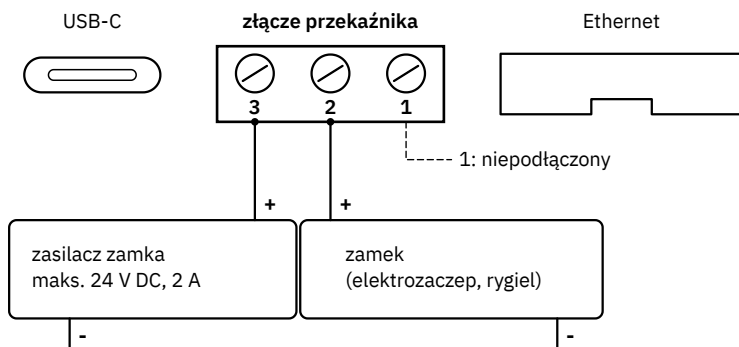
„Kontrola dostępu”:

- „Tryb”: „każda karta” albo „tylko karty pracowników” (rozdział 6.5),
- „Blokada powtórzeń [s]”: od 0 do 3600, fabrycznie 5, 0 = wyłączona (rozdział 7.1),
- „Przełącznik tylko przy wejściu”: wyjście zapisuje odbicie, ale nie otwiera zamka.

„Sygnalizacja”: „Zawsze 3 krótkie” daje ten sam dźwięk przy wejściu i wyjściu. Kolor światła nadal się różni.

9.6 Przekaznik i zamek drzwi

Złącze przekaźnika włącza i wyłącza zasilanie zamka (elektrozaczepu, rygla) przy przyjętym odbiciu. To nie jest zwykły styk przekaźnika, który zwiera dowolny obwód: wyjście przełącza tylko plus zasilania zamka i działa w jednym kierunku. Plus z zasilacza zamka podłączasz do zacisku 3, a z zacisku 2 plus idzie dalej do zamka, jak przedłużenie przewodu plusowego. Minus zamka łączysz bezpośrednio z minusem zasilacza zamka, nie przez urządzenie. Fabrycznie przekaźnik jest wyłączony.



Zacisk	Podłączenie
3 (skrajny, od strony gniazda USB-C)	plus (+) z zasilacza zamka
2 (środkowy)	plus (+) dalej do zamka
1	niepodłączony
(minus zamka)	bezpośrednio do minusa (-) zasilacza zamka, nie do urządzenia

**UWAGA**

- Tylko prąd stały, najwyżej 24 V DC i 2 A.
- Zachowaj biegunowość. Przy odwrotnym podłączeniu zamek będzie zasilany cały czas.
- Zamek ma cewkę. Jeśli nie ma wbudowanej diody gaszącej (sprawdź w jego instrukcji), podłącz równolegle do zamka diodę, np. 1N4007: katodą (paskiem) do plusa zamka, anodą do minusa. Bez niej każde wyłączenie zamka daje przepięcie, które może uszkodzić wyjście urządzenia.
- Przewody podłączaj przy odłączonym zasilaniu.

Ustawienia > Czytnik > Przekaznik / zamek:

- „Tryb pracy”:
 - „wyłączony” (fabrycznie),
 - „normalnie wyłączony, impuls załącza”: impuls włącza zasilanie zamka,
 - „stale załączony, impuls wyłącza”: zasilanie jest stale włączone, a impuls je wyłącza (np. zwora elektromagnetyczna).
- „Czas impulsu [ms]”: od 100 do 10000 ms, fabrycznie 3000 ms.
- „Test”: „Załącz”, „Wyłącz”, „Wyzwól”. „Wyzwól” działa według trybu i czasu zapisanych w urządzeniu, więc najpierw kliknij „Zapisz ustawienia”.

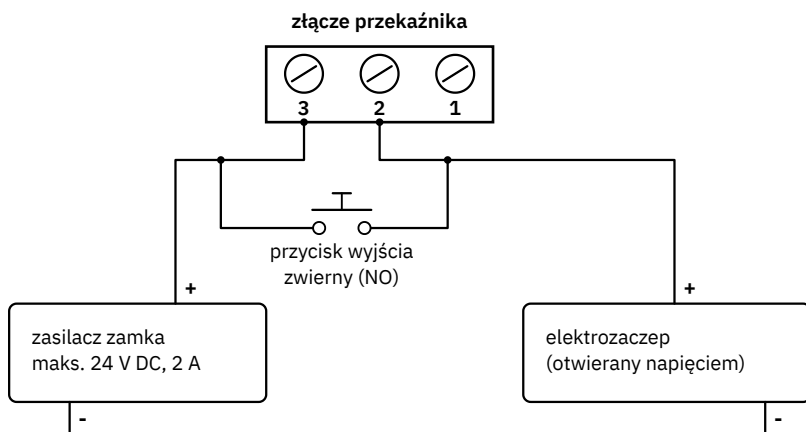
Przekaznik działa przy każdym przyjętym odbiciu (przy włączonej opcji „Przekaznik tylko przy wejściu” tylko przy wejściu; gdy na liście jest ponad 256 kart, przy każdym odbiciu), a nigdy przy odrzuconym ani przy odbiciu w czasie blokady powtórzeń. Kolejne odbicie w trakcie impulsu wydłuża impuls.

**UWAGA**

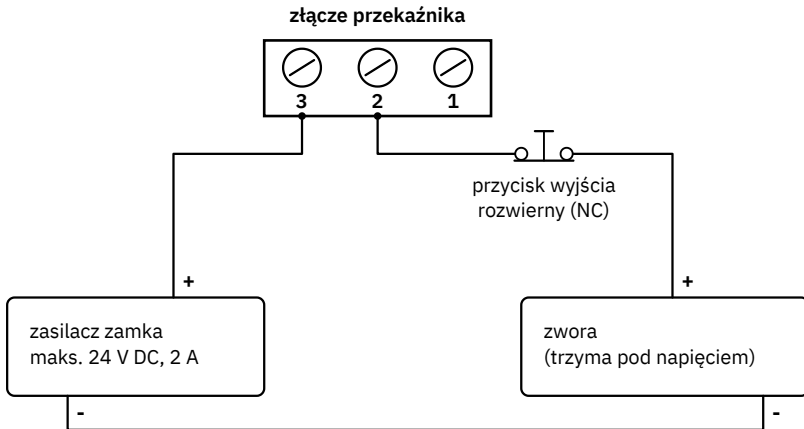
W trybie „każda karta” zamek otworzy każda pasująca karta, także nieprzypisana do nikogo. Jeśli przekaznik steruje drzwiami, ustaw tryb „tylko karty pracowników” w sekcji Ustawienia > Czytnik > Kontrola dostępu.

Otwieranie drzwi z obu stron. Czytnik wisi po jednej stronie drzwi. Z drugiej strony drzwi otwierasz przyciskiem wyjścia. Przycisk podłączasz do tych samych przewodów co urządzenie, więc otwiera zamek niezależnie od czytnika. Sposób podłączenia zależy od zamka.

Elektrozaczep albo rygiel otwierany napięciem (tryb „normalnie wyłączony, impuls załącza”): przycisk zwierny (NO) podłączasz równoległe do urządzenia, czyli jeden przewód przycisku do zacisku 3 (plus z zasilacza), a drugi do zacisku 2 (plus do zamka). Naciśnięcie podaje plus na zamek z pominięciem urządzenia.



Zwora elektromagnetyczna trzymająca drzwi napięciem (tryb „stałe załączony, impuls wyłącza”): przycisk rozwierny (NC) podłączasz szeregowo w przewodzie plusowym, między zaciskiem 2 a zworą. Naciśnięcie przerywa plus i zwora puszcza drzwi.



Zamiast przycisku możesz dać po drugiej stronie drugi czytnik RAZ-RCP-1. Przy elektrozaczeple zaciski drugiego urządzenia łączysz równolegle z pierwszym (zacisk 3 z zaciskiem 3, zacisk 2 z zaciskiem 2). Przy zworze łączysz je szeregowo: zacisk 2 pierwszego urządzenia do zacisku 3 drugiego, a zacisk 2 drugiego do zwory. Każde urządzenie prowadzi własną ewidencję i własną kolejność wejść i wyjść.



UWAGA

- Przycisk musi wytrzymać prąd zamka (do 2 A przy 24 V DC).
- Wyjście przyciskiem nie jest zapisywane w ewidencji. Jeśli rejestrujesz czas pracy, pracownicy odbijają kartę także przy wyjściu. Gdy drzwi i tak otwiera przycisk, włącz „Przełącznik tylko przy wejściu” (rozdział 9.5), żeby odbicie przy wyjściu nie zwalniało zamka bez potrzeby.
- Wyjście ewakuacyjne i zwolnienie zwory w razie pożaru zapewnia osobny obwód zgodny z przepisami, a nie to złącze ani przycisk wyjścia.

9.7 Karta resetująca

Ustawienia > Bezpieczeństwo > Karta resetująca > „UID (hex)”: numer karty, której przyłożenie uruchamia tryb awaryjny do resetu danych dostępowych (rozdział 13.1). Karta resetująca z pudełka (z naklejką „KARTA RESETUJĄCA”) jest już przypisana do tego urządzenia: producent przypisuje ją przy pierwszym

uruchomieniu, na kontroli jakości. Funkcja działa tylko wtedy, gdy numer karty jest zapisany w urządzeniu. Urządzenie pamięta jedną kartę resetującą.

Zmiana karty (np. po zgubieniu): wpisz numer nowej karty szesnastkowo i kliknij „Zapisz ustawienia”. Nowa karta zastępuje poprzednią, a poprzednia przestaje działać. Numer nowej karty odczytasz przyciskiem „Odczytaj kartę” na stronie „Pracownicy” (potem kliknij „Anuluj” w ramce „Przypisz kartę”). Ramka pokazuje pełny numer karty: przepisz go w całości, także wszystkie 20 znaków karty z numerem 10-bajtowym.

Panel nie pokazuje zapisanego numeru: pole jest zawsze puste i ma odpowiedź „brak - funkcja wyłączona”, także wtedy, gdy karta jest ustawiona. Zapis z nietkniętym, pustym polem nie zmienia karty. Czy karta działa, sprawdzisz tylko, przykładając ją do czytnika: urządzenie uruchomi się ponownie w trybie awaryjnym (rozdział 13.1), który bez hasła panelu z etykiety niczego nie zmienia i po 5 minutach kończy się sam. Kartę resetującą może też ustawić serwer zarządzania centralnego (rozdział 10.3).



UWAGA

Nie wpisuj nic w pole „UID (hex)”, jeśli nie zmieniasz karty. Jeśli wpiszesz znaki, potem wyczyścisz pole i klikniesz „Zapisz ustawienia”, urządzenie usunie kartę resetującą i reset kartą przestanie działać. Gdy coś wpiszesz przez pomyłkę, odśwież stronę w przeglądarce zamiast zapisywać. Usuniętą kartę przypiszesz ponownie: odczytaj jej numer przyciskiem „Odczytaj kartę” na stronie „Pracownicy” i zapisz go w tym polu.

9.8 Strefa niebezpieczna

Ustawienia > System > Strefa niebezpieczna:

- **„Przelicz kierunki wejście/wyjście”** i **„Przelicz”**: gdy sygnał czytnika nie zgadza się z raportem. Trwa kilka sekund; w tym czasie czytnik nie przyjmuje kart.
- **„Usuń wszystkie odbicia z urządzenia”** i **„Wyczyść odbicia”**: usuwa wszystkie odbicia. Tego nie da się cofnąć, więc najpierw pobierz kopię zapasową. Tylko konto admin.
- **„Przywróć ustawienia fabryczne”**: usuwa wszystkie dane i ustawienia wprowadzone w urządzeniu. Okno wymaga zaznaczenia „Rozumiem, że tej operacji nie da się cofnąć” i wpisania hasła konta admin. Tylko konto admin. Szczegóły w rozdziale 13.3.

9.9 Dziennik zdarzeń

Ustawienia > Bezpieczeństwo > Dziennik zdarzeń. Dziennik widzi tylko konto admin.

Urządzenie zapisuje w szyfrowanej pamięci zdarzenia dotyczące bezpieczeństwa i ochrony danych. Przechowuje co najmniej 1000 ostatnich zdarzeń; starsze usuwa samo, zaczynając od najstarszych. Dziennik przetrwa restart i zanik zasilania.

Co jest zapisywane:

- uruchomienie urządzenia, zmiana wersji oprogramowania, restart z panelu,
- sformatowanie pamięci odbić przy uruchomieniu („Sformatowano pamięć odbić (była pusta lub uszkodzona)”). Po pierwszym uruchomieniu i po przywróceniu ustawień fabrycznych to normalne. W innej sytuacji oznacza, że pamięć była uszkodzona, a wcześniejsze odbicia, lista pracowników i dziennik przypadły,
- logowanie udane i nieudane, blokada konta, błędny kod 2FA, wylogowanie,
- zmiana haseł (konto admin, konto „biuro”, hotspot), włączenie i wyłączenie 2FA oraz konta „biuro”,
- zmiany ustawień ważnych dla ochrony danych: dostęp z sieci lokalnej, hotspot, Wi-Fi firmy, Ethernet, mDNS, wysyłanie odbić (włączenie, adres, login i hasło, usuwanie po wysłaniu), Chmura ADARAZ, zarządzanie centralne, karta resetująca, tryb dostępu, certyfikat HTTPS; pozostałe zmienione ustawienia jednym wpisem z nazwami pól,

- reset danych dostępowych kartą resetującą i przyciskiem reset (pokazuje je też ramka po zalogowaniu, rozdział 10.4), uruchomienie trybu awaryjnego kartą resetującą, złe hasło z etykiety w trybie awaryjnym i koniec trybu awaryjnego bez resetu,
- usunięcie wszystkich odcisków, przywrócenie odcisków z kopii, ręczne dodanie i usunięcie odcisków, zapis listy pracowników, pobranie odcisków i listy pracowników, włączenie odczytu numeru karty w panelu („Odczytaj kartę”), kopia bazy wysłana na serwer zarządzania centralnego,
- aktualizacje oprogramowania (z internetu, z pliku, zlecone zdalnie) i odrzucone pliki oprogramowania,
- zmiana certyfikatu HTTPS, ręczne sterowanie przekaźnikiem, ręczna zmiana czasu,
- przywrócenie ustawień fabrycznych, potwierdzenie zmian zdalnych (rozdział 10.4),
- wysłanie odcisków na serwer albo do Chmury ADARAZ („Wysłano odcisków na serwer”; w szczegółach liczba wysłanych odcisków i liczba usuniętych z urządzenia po wysłaniu),
- zgłoszenie nieznananych kart do Chmury ADARAZ („Zgłoszono nieznanne karty do Chmury ADARAZ”; w szczegółach liczba kart, bez ich numerów),
- ustawienie wysyłania odcisków na adres <http://> albo włączenie wysyłania na taki adres („Wysyłanie odcisków po <http://> bez szyfrowania”, rozdział 10.2),
- wstrzymanie wysyłki odcisków po HTTP poza sieć lokalną albo przez otwartą sieć Wi-Fi (rozdział 10.2).

Zdarzenia powtarzalne. Logowanie i wylogowanie z tego samego adresu, pobranie danych, ręczne dodanie i usunięcie odcisków, zapis listy pracowników, wysłanie odcisków na serwer oraz zgłoszenie nieznananych kart do Chmury urządzenie zapisuje najwyżej raz na 15 minut, a wstrzymanie wysyłki odcisków raz na dobę. Z nieudanych logowań zapisuje osobno pierwsze 5 prób z rzędu, a dalsze próby z tego samego adresu i próby w czasie blokady najwyżej raz na 15 minut. Powtórzenia z tego okresu trafiają do jednego wpisu zbiorczego z liczbą („wpis zbiorczy: jeszcze ... takich zdarzeń od poprzedniego wpisu”). Przy wielu nieudanych próbach z różnych adresów urządzenie zapisuje najwyżej kilkadziesiąt wpisów na godzinę i wpis zbiorczy „... takich prób z różnych adresów”. Wpis zbiorczy z dotychczasową liczbą pojawia się też od razu, gdy otworzysz albo odświeżysz dziennik. Dzięki temu

powtarzanymi działaniami (np. próbami logowania albo dodawaniem i usuwaniem odbić) nie da się wypchnąć z dziennika starszych zdarzeń.

Gdy w pamięci danych zostaje mniej niż 128 kB, dziennik przestaje rosnąć, żeby zostawić miejsce na odbicia: zapisuje dalej, ale trzyma tylko kilkadziesiąt najnowszych zdarzeń, a starsze usuwa. Zmiany zdalne do potwierdzenia (rozdział 10.4) zapisuje zawsze. Zwolnij wtedy miejsce: pobierz kopię zapasową i usuń odbicia przyciskiem „Wyczyść odbicia” (rozdział 9.8). Gdy pamięć zapełni się całkowicie, panel pokazuje w tej sekcji „Część zdarzeń nie zapisała się w dzienniku (pamięć danych pełna?)”.

Wpis zawiera numer kolejny („Nr”), datę i godzinę („Czas”), zdarzenie i szczegóły, kto („Kto”: admin, biuro, system, zdalnie), skąd („Źródło”: hotspot, sieć lokalna, Chmura ADARAZ, zarządzanie centralne, karta resetująca, przycisk reset, system) oraz adres IP urządzenia, z którego wykonano działanie („Adres IP”). Gdy zegar urządzenia nie był ustawiony, wpis ma numer startu urządzenia i czas od uruchomienia; panel pokazuje wtedy czas przybliżony z dopiskiem „ok.” albo „start nr ..., ... s od uruchomienia”. Dziennik nie zawiera haseł, kodów 2FA ani numerów kart.

Przeglądanie:

- ① Kliknij „Pokaż dziennik”. Najnowsze zdarzenia są na górze; starsze wyświetlisz przyciskiem „Pokaż więcej”.
- ② Wybierz filtr: „Wszystkie”, „Logowanie i konta”, „Ustawienia”, „Dane”, „System i aktualizacje” albo „Zmiany zdalne”.
- ③ „Odśwież” pobiera dziennik ponownie. „Eksport CSV” zapisuje wpisy widoczne po wybranym filtrze. Plik raz-rcp-dziennik_RRRR-MM-DD_GGMM.csv (separator średnik) otworzysz w arkuszu kalkulacyjnym.

Dziennika nie da się wyczyścić: usuwa go tylko przywrócenie ustawień fabrycznych (rozdział 13.3). Karta resetująca i przycisk reset go nie usuwają.



WSKAZÓWKA

Przejrzyj dziennik po nieoczekiwanym zdarzeniu, np. po resecie kartą albo po ramce zmian zdalnych (rozdział 10.4). Jeśli potrzebujesz dłuższej historii niż 1000 zdarzeń, co jakiś czas zachowaj eksport CSV.

10.1 Chmura ADARAZ

Ustawienia > Integracje > Chmura ADARAZ łączy czytnik z panelem ADARAZ w chmurze.

- ① Dodaj czytnik w panelu Chmury ADARAZ i odczytaj tam kod parowania (8 znaków, jednorazowy, np. ABCD-EFGH).
- ② Wpisz kod w pole „Kod parowania” w urządzeniu i kliknij „Połącz”. Urządzenie potrzebuje dostępu do internetu i ustawionego zegara.
- ③ Po połączeniu panel pokaże „Połączono z organizacją ... jako ...”.

Po połączeniu:

- urządzenie samo ustawia wysyłanie odbić i po wystąpieniu usuwa je u siebie; ewidencja i raporty są w chmurze,
- lista pracowników przychodzi z chmury i w urządzeniu jest tylko do odczytu („Lista pracowników jest zarządzana w Chmurze ADARAZ - zmiany wprowadzaj w panelu chmury”),
- nieznane karty są wysyłane do chmury, gdzie można je przypisać,
- „Odczytaj kartę” nadal działa: pokazuje numer karty do wpisania w panelu chmury.

„Rozłącz z chmurą” i „Rozłącz”: odbicia przestają trafiać do chmury, synchronizacja zostaje wyłączona, a lista pracowników zostaje w urządzeniu i znów można ją edytować lokalnie.

10.2 Wysyłanie odbić na własny serwer

Ustawienia > Integracje > Synchronizacja:

- „Wysyłaj odbicia na serwer”,
- „Format”: „http2 - UID jako liczba”, „http3 - UID jako hex”, „Skryba (stara 8 bit)”, „Skryba (stara 10 bit)”,
- „Adres serwera (URL)”: zaczyna się od https:// albo http://; http:// tylko do serwera w sieci lokalnej (niżej),

- „Login” i „Hasło”,
- „ID urządzenia (machineId)”: fabrycznie nazwa sieci Wi-Fi urządzenia,
- „Interwał [min]”: od 1 do 1440, fabrycznie 15; zmiana działa bez restartu,
- „Usuwa odbicia po wystaniu”: urządzenie usuwa odbicie, gdy serwer potwierdzi jego przyjęcie (patrz 8.6).

Formaty Skryba wysyłają numer karty i czas (zawsze polski) jak stara Skryba. Wariant poznasz po numerach kart na serwerze: jeśli któryś jest większy niż 4294967295 (zwykle 12-13 cyfr), wybierz 10 bit, w przeciwnym razie 8 bit. Zły wariant oznacza, że serwer nie rozpozna kart.

Certyfikat serwera. Przy adresie `https://` serwer musi mieć ważny certyfikat wystawiony przez publiczny urząd certyfikacji (np. Let's Encrypt) na nazwę z adresu. Urządzenie sprawdza daty ważności certyfikatu według swojego zegara (rozdział 9.4), więc wygasły certyfikat zatrzymuje wysyłkę, a odbicia czekają w urządzeniu. Urządzenie odrzuca łańcuch certyfikatów podpisany algorytmem SHA-1 albo MD5; certyfikaty publicznych urzędów nie mają takich podpisów od 2016 r.

HTTP bez szyfrowania. Po `http://` login, hasło i odbicia idą przez sieć jawnie: każdy, kto ma dostęp do tej sieci, może je podsłuchać albo podmienić. Używaj `http://` tylko wtedy, gdy cała droga między czytnikiem a serwerem jest niedostępna dla osób postronnych, np. czytnik i serwer są podłączone do przełącznika w zamkniętej szafie, do osobnej sieci VLAN tylko dla nich albo przez VPN. Nie używaj `http://` w sieci, do której mają dostęp goście. W pozostałych przypadkach użyj `https://`. Przy adresie `http://` panel pokazuje ostrzeżenie, a jego ustawienie trafia do dziennika zdarzeń (rozdział 9.9). Przez otwartą sieć Wi-Fi (bez hasła albo z przestarzałym zabezpieczeniem WEP) urządzenie nie wysyła odbić po `http://` wcale: wysyłka jest wstrzymana, panel pokazuje komunikat, a dziennik zdarzeń dostaje wpis. Odbicia czekają w urządzeniu, dopóki nie podłączysz kabla Ethernet, nie użyjesz sieci Wi-Fi z WPA2/WPA3 albo adresu `https://`.

HTTP tylko w sieci lokalnej. Adres `http://` może prowadzić tylko do serwera w sieci lokalnej: adres IP 10.x.x.x, 172.16.x.x-172.31.x.x, 192.168.x.x albo 169.254.x.x, adres IPv6 zaczynający się od fc, fd albo fe80, albo nazwa serwera, która wskazuje taki adres (np. `http://skryba`, `http://skryba.local` albo `http://rcp.firma.pl`, jeśli w Twojej sieci wskazuje serwer w tej sieci). Do serwera w internecie użyj adresu `https://`.

Panel nie zapisze adresu http:// z adresem IP spoza sieci lokalnej i pokaże „Wysyłanie po HTTP jest dozwolone tylko w sieci lokalnej...”. Przy nazwie serwera, która nie kończy się na .local, .lan, .home.arpa ani .internal i nie jest nazwą bez kropki, panel pokaże odpowiedź „Przed każdą wysyłką urządzenie sprawdzi...”, a adres zapisze się normalnie. Przed każdą wysyłką urządzenie sprawdza, dokąd prowadzi nazwa serwera; jeśli wskazuje adres w internecie, wstrzymuje wysyłkę. Przekierowania (3xx) z serwera wykonuje tylko na adres https:// albo na adres w sieci lokalnej.

Adres zapisany wcześniej. Jeśli w urządzeniu był już zapisany adres http:// do serwera w internecie (np. przed aktualizacją oprogramowania), urządzenie wstrzymuje wysyłkę, a panel pokazuje „Wysyłanie odbić jest wstrzymane: adres http:// prowadzi poza sieć lokalną...” albo „Wysyłanie odbić jest wstrzymane: nazwa serwera wskazuje adres poza siecią lokalną...”. Adres nie jest zmieniany ani usuwany. Odbicia czekają w urządzeniu i zostaną wysłane po zmianie adresu na https:// albo na adres w sieci lokalnej. Pozostałe ustawienia możesz zapisywać normalnie.

Bez sieci odbicia czekają w kolejce. Urządzenie ponawia wysyłkę po 30 sekundach, a potem w coraz dłuższych odstępach. Przy adresie https:// wysyłka czeka na ustawiony zegar.

Dla administratora serwera: urządzenie wysyła każde odbicie w osobnym żądaniu HTTP POST (formularz application/x-www-form-urlencoded z polami rfidID, timestamp i machineId) z uwierzytelnianiem HTTP Basic, najwyżej 32 odbicia w jednym cyklu. Pole timestamp ma postać RRRR-MM-DD GG:MM:SS: w UTC w formatach http2 i http3, w czasie polskim w formatach Skryba. Odbicie uznaje się za przyjęte, gdy serwer odpowie kodem 200, także gdy w treści odpowiedzi jest "stored":false. Kod 400 oznacza odbicie odrzucone: urządzenie nie wysyła go ponownie, więc serwer, który odpowiada kodem 400, traci to odbicie po swojej stronie. Przy kodach 401, 403, 404 i innych urządzenie przerywa cykl i wysyła odbicie ponownie przy następnej próbie. Przy adresie http:// z nazwą serwera urządzenie łączy się z adresem IP, na który wskazała nazwa, i wysyła nagłówki Host z tą nazwą. Przekierowanie na adres http:// poza siecią lokalną wstrzymuje wysyłkę.

10.3 Zarządzanie centralne

Ustawienia > Integracje > Zarządzanie centralne > „Zarządzaj z serwera” (domyślnie wyłączone; włącza je i wyłącza wyłącznie administrator w panelu urządzenia, serwer nie może tego zmienić).

Czytnik co kilkanaście minut zgłasza się do serwera („Serwer”, ustawiony fabrycznie razem z kluczem urządzenia, domyślnie <https://devices.adaraz.com>): wysyła stan i liczbę rekordów, pobiera zadane ustawienia, na polecenie wysyła kopię bazy i aktualizuje oprogramowanie.

Serwer zarządzania (także własny serwer integratora) i Chmura ADARAZ muszą mieć certyfikat krótkotrwały, ważny najwyżej 7 dni (np. Let's Encrypt, profil „shortlived”). Certyfikat ważny dłużej urządzenie odrzuca, a panel pokazuje „certyfikat serwera nie jest krótkotrwały (wymagany do 7 dni)”. Taki certyfikat nie wymaga list odwołanych certyfikatów: po kradzieży klucza serwera wygasa sam w ciągu kilku dni.

Serwer może zmieniać: tryb dostępu, blokadę ponownego odbicia, przekaźnik, sygnalizację, moc nadawania Wi-Fi, kartę resetującą, synchronizację, strefę czasową i język. Hasła, 2FA, certyfikat i interfejsy sieciowe zmienia się wyłącznie w panelu urządzenia. Lokalna zmiana pól zarządzanych przez serwer może zostać nadpisana przy następnej zmianie na serwerze. Zmiany wprowadzone przez serwer, które wpływają na ochronę danych osobowych, panel pokazuje adminowi po zalogowaniu (rozdział 10.4).

W tej sekcji są też: „Identyfikator urządzenia”, „Klucz urządzenia”, „Stan”, „Zgłoś się teraz”, „Wersja ustawień z serwera” oraz „Kopia bazy na serwerze” z przyciskiem „Wyślij teraz”.

10.4 Zmiany zdalne: powiadomienie w panelu

Po zalogowaniu na konto admin panel pokazuje u góry strony ramkę „Zmiany zdalne i resety od ostatniego potwierdzenia”, jeśli od ostatniego potwierdzenia coś zmieniono spoza panelu: przez zarządzanie centralne (w przyszłości także przez Chmurę ADARAZ), kartą resetującą albo przyciskiem reset. Ramka dotyczy zmian, które wpływają na ochronę danych osobowych:

- włączenie i wyłączenie wysyłania odbić, adres serwera, login lub hasło do serwera, usuwanie odbić po wystaniu,

- karta resetująca i tryb dostępu,
- kopia bazy pobrana przez serwer zarządzania centralnego,
- aktualizacja oprogramowania zlecona przez serwer,
- reset danych dostępowych kartą resetującą albo przyciskiem reset w obudowie (rozdział 13.1, 13.2): hasła wróciły do haseł z etykiety, 2FA zostało wyłączone, a hotspot włączony.

Każda pozycja ma datę i godzinę, kto wprowadził zmianę („Kto: zarządzanie centralne”, „Kto: karta resetująca” albo „Kto: przycisk w obudowie”), co zmieniono i jaki to ma skutek dla danych osobowych („Skutek dla danych osobowych:”).

- Ramka pokazuje najpierw najstarsze zmiany, do 20 naraz.
- „Rozumiem” potwierdza pokazane zmiany. Jeśli są dalsze, ramka pokaże następne.
- „Przypomnij później” ukrywa ramkę do następnego logowania albo do nowej zmiany zdalnej. Dopóki nie klikniesz „Rozumiem”, ramka wraca przy każdym logowaniu, a zakładka „Bezpieczeństwo” w „Ustawieniach” ma kropkę.

Urządzenie pamięta do 200 niepotwierdzonych zmian zdalnych. Jeśli było ich więcej, ramka podaje, ile starszych się nie zmieściło; znajdziesz je w dzienniku zdarzeń (rozdział 9.9, filtr „Zmiany zdalne”).

Zmian wykonanych samodzielnie w panelu ramka nie pokazuje (są w dzienniku zdarzeń). Konto „biuro” ramki nie widzi. Pełna historia: dziennik zdarzeń (rozdział 9.9).

Jeśli zmiana jest dla Ciebie nieoczekiwana, skontaktuj się z administratorem serwera zarządzania centralnego. Zarządzanie centralne wyłączysz w Ustawienia > Integracje > Zarządzanie centralne (rozdział 10.3). Jeśli resetu kartą albo przyciskiem nie wykonał nikt z Twojej firmy, od razu ustaw nowe hasła i włącz 2FA (rozdział 5), a zgubioną kartę zastąp nową (rozdział 9.7).

11

Aktualizacje oprogramowania

Ustawienia > System > Aktualizacja firmware:

- **Z internetu:** przy „Sprawdź dostępność aktualizacji” kliknij „Sprawdź”. Panel pokaże wersję „zainstalowana” i „na serwerze”. Gdy na serwerze jest nowsza wersja, pojawi się przycisk „Aktualizuj teraz”. Działa także przy wyłączonym zarządzaniu centralnym.
- **Z pliku:** „Wgraj plik firmware” i „Wgraj” wgrywa plik .bin bez internetu.

Urządzenie przyjmuje wyłącznie oprogramowanie podpisane przez producenta.



UWAGA

W czasie aktualizacji nie odłączaj zasilania i nie zamykaj strony. Dioda miga wtedy na niebiesko.

Po aktualizacji urządzenie samo się restartuje, panel przetłumaczy się i trzeba zalogować się ponownie. Jeśli nowe oprogramowanie nie uruchomi się poprawnie, urządzenie samo wraca do poprzedniej wersji.

12

Kopia zapasowa

W menu kliknij „Kopia zapasowa”. Przeglądarka pobierze plik raz-rcp-backup_RRRR-MM-DD_GGMM.zip, a panel pokaże „Kopia zapasowa pobrana”.

W pliku są:

- events.bin: odbicia,
- users.bin: lista pracowników,
- settings.json: ustawienia, bez haseł (tylko w kopii z konta admin).

Panel nie ma funkcji przywracania kopii. W razie potrzeby skontaktuj się z producentem. Przerwane wysyłanie pliku na urządzenie (np. zerwane połączenie) nie zmienia danych: urządzenie przyjmuje plik dopiero w całości. Wyjątek: gdy

pamięć jest prawie pełna, przywracanie odbić najpierw usuwa stare odbicia, a jego przerwanie zostawia pustą ewidencję (w dzienniku zdarzeń wpis „Usunięto wszystkie odbicia” z opisem „przywracanie przerwane”); wtedy przywróć kopię ponownie.

13

Reset danych dostępowych, bateria i serwis

Reset pomaga, gdy nie pamiętasz hasła, zgubiłeś telefon z aplikacją 2FA albo panel jest nieosiągalny. Wykonasz go kartą resetującą razem z hasłem panelu z etykiety (13.1) albo przyciskiem w obudowie (13.2). Skutek jest ten sam.

Reset:

- przywraca fabryczną nazwę i hasło hotspotu Wi-Fi oraz włącza hotspot,
- przywraca fabryczne hasło konta admin,
- wyłącza drugi składnik (2FA) konta admin.

Reset zachowuje: odbicia, listę pracowników, wszystkie pozostałe ustawienia i konto „biuro”.

Reset kartą albo przyciskiem jest zapisywany w dzienniku zdarzeń (rozdział 9.9), a dziennik zostaje. Pełne usunięcie danych i ustawień opisuje rozdział 13.3.

Po resecie połącz się z hotspotem i zaloguj danymi z etykiety (rozdział 4).

13.1 Karta resetująca

W pudełku jest karta resetująca z naklejką „KARTA RESETUJĄCA”. Producent przypisuje ją do tego urządzenia przy pierwszym uruchomieniu, na kontroli jakości, więc działa od razu (rozdział 9.7).

- To nie jest karta pracownika. Jej przyłożenie nie jest zapisywane jako odbicie i nie otwiera zamka.
- Sama karta niczego nie zmienia: uruchamia na 5 minut hotspot awaryjny, a dane dostępowe przywraca dopiero hasło panelu z etykiety wpisane w tym hotspotcie. Karta razem z etykietą daje więc pełny dostęp do panelu. Traktuj ją jak kartę płatniczą: schowaj w bezpiecznym miejscu, osobno od urządzenia i od etykiety

zapasowej, nie dawaj jej pracownikom i nie pozwalaj jej skopiować (każdą kartę zbliżeniową da się skopiować czytnikiem). Gdy nie wiesz, gdzie jest karta, przypisz nową (rozdział 9.7).

- Nie przypisuj jej żadnemu pracownikowi: zamiast odbicia zawsze uruchomi tryb awaryjny.
- Działa także wtedy, gdy na stronie „Pracownicy” trwa „Odczytaj kartę”. Nie przykładaj jej przy odczytywaniu kart pracowników.
- Zgubioną kartę zastąp nową w ustawieniach (rozdział 9.7); stara przestanie działać.

Reset karty:

- ① Upewnij się, że urządzenie jest włączone. Obudowy nie trzeba otwierać. Przygotuj etykietę (zapasową albo tę we wnęce urządzenia).
- ② Przyłóż kartę resetującą do czytnika, tak jak kartę pracownika. Dioda zaświeci na żółto, urządzenie piknie dwa razy krótko i samo się zrestartuje.
- ③ Po restarcie przez 5 minut działa hotspot awaryjny: sieć Wi-Fi z pola SIEĆ WI-FI na etykiecie, z hasłem z pola HASŁO WI-FI (albo kod QR „Połącz z Wi-Fi”). Działa także wtedy, gdy hotspot był wyłączony albo zmieniłeś jego nazwę lub hasło.
- ④ Połącz telefon albo komputer z tą siecią i otwórz w przeglądarce link z pola LINK DO PANELU / PO PODŁĄCZENIU, np. **<http://10.10.10.1>**. Zamiast panelu zobaczysz stronę „Tryb awaryjny” z jednym polem.
- ⑤ Wpisz HASŁO PANELU z etykiety i kliknij „Przywróć / Restore”. Urządzenie przywróci dane dostępowe, piknie dwa razy krótko i raz długo i samo się zrestartuje.
- ⑥ Połącz się z hotspotem i zaloguj danymi z etykiety (rozdział 4).

Tryb awaryjny kończy się bez żadnych zmian po 5 minutach albo po 5 złych hasłach: urządzenie piknie dwa razy nisko i wróci do zwykłej pracy. Żeby spróbować jeszcze raz, zdejmij kartę z czytnika i przyłóż ją ponownie. W czasie trybu awaryjnego urządzenie dalej rejestruje odbicia, a panel z sieci firmy działa normalnie; zwykły hotspot jest wtedy zastąpiony hotspotem awaryjnym.

Po zalogowaniu na konto admin panel pokaże reset w ramce „Zmiany zdalne i resety od ostatniego potwierdzenia” (rozdział 10.4).

Jeśli dioda nie zaświeci na żółto, tylko tak jak przy zwykłej karcie, numer tej karty nie jest zapisany w urządzeniu (np. ktoś zmienił kartę w ustawieniach albo to karta z innego urządzenia). Użyj wtedy przycisku (13.2).

13.2 Reset przyciskiem

- ① Odetnij zasilanie obwodu, którym steruje przekaźnik (zamka, rygla, szlabanu). Samo urządzenie zostaw włączone, inaczej reset się nie wykona.
- ② Otwórz obudowę, powoli i ostrożnie. Uważaj na przewód anteny.
- ③ Obok kontrolera jest mały przycisk reset. Przytrzymaj go 3 sekundy. Po pierwszej sekundzie dioda zaświeci na żółto.
- ④ Trzymaj, aż urządzenie piknie dwa razy krótko i raz długo. Urządzenie zrestartuje się samo z fabrycznymi danymi dostępowymi.

Krótkie naciśnięcie przycisku nic nie zmienia. Reset przyciskiem panel pokaże po załogowaniu w ramce zmian i resetów (rozdział 10.4).

13.3 Przywrócenie ustawień fabrycznych (usunięcie danych)

Przywróć ustawienia fabryczne przed przekazaniem urządzenia innej firmie, sprzedażą, zwrotem albo utylizacją, a także wtedy, gdy chcesz zacząć od zera.

Zanim zaczniesz:

- Jeśli potrzebujesz danych, pobierz kopię zapasową (rozdział 12).
- Jeśli urządzenie jest połączone z Chmurą ADARAZ, usuń je także w panelu chmury.
- Kopie bazy wysłane wcześniej na serwer zarządzania centralnego usuwa administrator tego serwera.
- Jeśli przekazujesz urządzenie, zmień albo usuń kartę resetującą (rozdział 9.7), przed resetem albo po nim.

Przywrócenie:

- ① Wejdź w Ustawienia > System > Strefa niebezpieczna i kliknij „Przywróć ustawienia fabryczne”. Może to zrobić tylko konto admin.
- ② Przeczytaj w oknie, co zostanie usunięte, a co zostaje. Gdy włączone jest zarządzanie centralne, okno ma dodatkowe pole „Wyłącz też zarządzanie centralne”.
- ③ Zaznacz „Rozumiem, że tej operacji nie da się cofnąć” i wpisz hasło w polu „Hasło konta admin”.
- ④ Kliknij „Usuń dane i przywróć ustawienia”.

Po 5 błędnych hasłach obowiązuje ta sama blokada co przy logowaniu (rozdział 5.3). W trakcie aktualizacji oprogramowania i tuż po niej, do restartu, reset nie jest możliwy: spróbuj ponownie po restarcie.

Co jest usuwane:

- wszystkie odbicia i stan wejść/wyjść,
- lista pracowników,
- dziennik zdarzeń,
- wszystkie ustawienia: sieć Wi-Fi firmy z hasłem, wysyłanie odbić z adresem, loginem i hasłem, połączenie z Chmurą ADARAZ, dostęp z sieci lokalnej, przekaźnik, strefa czasowa, język i pozostałe,
- konto „biuro”, drugi składnik (2FA) obu kont i hasła ustawione w panelu,
- certyfikat HTTPS panelu, także wgrany certyfikat Twojego CA.

Pamięć odbić i pracowników jest kasowana w całości, a nie tylko oznaczana jako wolna.

Co zostaje:

- hasła fabryczne z etykiety: konto admin i hotspot znów działają z danymi z etykiety,
- identyfikator i klucze urządzenia,
- karta resetująca,
- zarządzanie centralne w dotychczasowym stanie albo wyłączone, jeśli zaznaczysz „Wyłącz też zarządzanie centralne”; adres i klucz serwera się nie

zmieniają, a serwer nie wgra sam ponownie poprzednich ustawień (nowe ustawienia z serwera panel pokaże w ramce zmian zdalnych, rozdział 10.4); zarządzanie wyłączysz też później w Ustawienia › Integracje › Zarządzanie centralne,

- data i czas oraz wersja oprogramowania.

Hotspot wraca do nazwy „RAZ-RCP-” i 8 znaków z numeru seryjnego (rozdział 2.3). Jeśli urządzenie zamówiono z inną nazwą sieci (nadrukowaną na etykiecie), kod QR z etykiety nie zadziała: wybierz sieć ręcznie i wpisz hasło z etykiety. Ustawienia wgrane na zamówienie (np. sieć Wi-Fi firmy, przekaźnik) też wracają do domyślnych.

Przebieg: urządzenie restartuje się i kasuje pamięć. Dioda miga na czerwono i żółto, zwykle około minuty, najwyżej 3 minuty. Na koniec świeci na zielono i urządzenie startuje normalnie.

Jeśli zamiast potwierdzenia okno pokaże „Brak odpowiedzi z urządzenia - mogło już rozpocząć przywracanie ustawień fabrycznych”, odpowiedź zgubiła się po drodze (np. przy słabym zasięgu hotspotu). Nie odłączaj zasilania i odczekaj około minuty, potem postępuj jak niżej („Potem”). Jeśli urządzenie nadal przyjmuje dotychczasowe hasło konta admin, reset się nie odbył i możesz go powtórzyć.



UWAGA

W czasie kasowania nie odłączaj zasilania. Jeśli zasilanie zaniknie, kasowanie zostanie dokończzone po ponownym włączeniu, od miejsca przerwania. Jeśli przerwie się 5 razy z rzędu (np. przez słaby zasilacz), urządzenie uruchomi się mimo to, a dziennik zdarzeń pokaże przy „Przywrócono ustawienia fabryczne” informację „kasowanie pamięci danych niedokończzone”. Sprawdź wtedy zasilanie i powtórz przywrócenie ustawień fabrycznych.

Potem postępuj jak przy pierwszym uruchomieniu (rozdział 4): połącz się z hotspotem i zaloguj danymi z etykiety. Dostęp z sieci firmowej jest wyłączony (rozdział 9.3). Przeglądarka pokaże ostrzeżenie o nowym certyfikacie z nowym odciskiem (rozdział 9.3). Przekaźnik jest wyłączony: ustaw go ponownie (rozdział 9.6). Nowy dziennik zdarzeń zaczyna się od wpisów „Uruchomienie urządzenia” i „Przywrócono ustawienia fabryczne” (z datą zlecenia

i informacją, kto i skąd je zlecił; bez adresu IP, żeby po resecie nie został ślad poprzedniego użytkownika).

Pojedyncze dane nadal usuniesz osobno: odbicia przyciskiem „Wyczyść odbicia” (rozdział 9.8), a pracowników na stronie „Pracownicy”.

13.4 Wymiana baterii

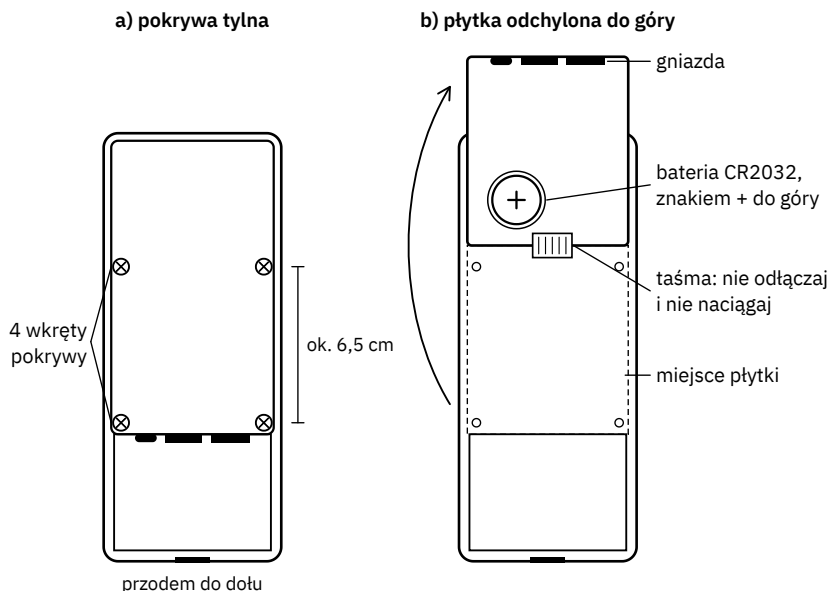
W urządzeniu jest bateria litowa pastylkowa CR2032 (3 V, nietładowalna), włożona fabrycznie do uchwytu na płytce głównej. Podtrzymuje zegar, gdy urządzenie nie ma zasilania. Odbić, listy pracowników i ustawień bateria nie podtrzymuje: są zapisane w pamięci urządzenia i zostają także po wymianie baterii.

Kiedy wymienić. Gdy po odłączeniu zasilania znika data i godzina. Jeśli urządzenie ma dostęp do internetu, samo ustawi potem czas z sieci; bez internetu trzeba go ustawić w panelu (rozdział 9.4).



UWAGA

- Trzymaj nową i zużytą baterię z dala od dzieci. Połknięcie baterii pastylkowej może w ciągu 2 godzin spowodować ciężkie oparzenia wewnętrzne. W razie połknięcia natychmiast jedź do lekarza.
- Baterii nie ładuj, nie zwieraj, nie rozbieraj i nie wrzucaj do ognia.
- Używaj tylko baterii CR2032 3 V. Bateria innego typu grozi wybuchem.



Wymiana i bezpieczne wyjęcie baterii:

- ① Odłącz zasilanie i wszystkie przewody (USB-C, Ethernet, przewody przełącznika), zdejmij urządzenie ze ściany.
- ② Połóż urządzenie przodem do dołu na miękkiej podkładce. Odkręć 4 wkręty pokrywy tylnej i zdejmij pokrywę. Dwa wkręty są tuż nad wnęką na przewody, przy lewej i prawej krawędzi pokrywy, a dwa ok. 6,5 cm wyżej, też przy krawędziach.
- ③ Delikatnie unieś płytkę od strony gniazd (od dołu) i odchyl ją do góry jak stronę książki. Nie odcinaj i nie naciągaj taśmy przy górnej krawędzi: łączy płytkę główną z płytką czytnika. Bateria jest po stronie płytki zwróconej do wnętrza obudowy, w jej górnej części, po lewej (patrząc od tyłu).
- ④ Wysuń starą baterię spod zacisku uchwytu. Nie używaj metalowych narzędzi do podważania (ryzyko zwarcia).
- ⑤ Włóż nową baterię CR2032 znakiem „+” do góry (w stronę zacisku), wsuwając ją do oporu.
- ⑥ Odłóż płytkę na miejsce tak, żeby gniazda weszły w wycięcia, załóż pokrywę i dokręć 4 wkręty z wycuciem (obudowa jest plastikowa).

- ⑦ Podłącz zasilanie i sprawdź datę i godzinę w panelu (ustaw ją, jeśli urządzenie nie ma internetu).
- ⑧ Zużyta baterię oddaj do punktu zbiórki baterii, nie wyrzucaj jej z odpadami komunalnymi (rozdział 16).

13.5 Rozwiązywanie problemów

Problem	Co zrobić
Dioda nie świeci po podłączeniu zasilania, brak melodii	Sprawdź, czy wtyk USB-C jest dociśnięty, a zasilacz daje 5 V DC. Sprawdź kabel na innym urządzeniu.
Nie widać sieci Wi-Fi urządzenia	Hotspot mógł zostać wyłączony w ustawieniach albo zmieniono jego nazwę. Wykonaj reset danych dostępowych (rozdział 13).
Link do panelu z etykiety się nie otwiera	Sprawdź, czy telefon lub komputer jest połączony z siecią Wi-Fi urządzenia i czy nie przetączył się na inną sieć albo dane komórkowe. Wpisz link w pasku adresu, nie w wyszukiwarce. Jeśli nie działa http://rcp-xxxxxxx.local , użyj http://10.10.10.1 . Najwyżej 4 urządzenia mogą być naraz w sieci urządzenia.
Z sieci firmowej panel jest niedostępny	Włącz „Dostęp z sieci lokalnej” (9.3) i używaj adresu https:// .
Nowych odbić nie ma w panelu	Kliknij „Odśwież dane”.
Czytnik nie reaguje na kartę	Użyj karty 13,56 MHz standardu ISO/IEC 14443 typu A. Telefony, zegarki i karty płatnicze z losowym numerem nie działają. Odsuń urządzenie od dużych elementów metalowych.

Problem	Co zrobić
Czerwone światło przy odbiciu	Karta spoza listy w trybie „tylko karty pracowników”, karta z losowym numerem albo błąd zapisu, np. pełna pamięć (odbicie nie jest wtedy zapisane). Kartę przyłóż ponownie dopiero po czasie blokady powtórzeń (fabrycznie 5 s): przyłożona szybciej da białe światło i też nie zostanie zapisana. Dodaj kartę do listy (rozdział 6) albo zwolnij miejsce: pobierz kopię zapasową i usuń odbicia przyciskiem „Wyczyść odbicia” (rozdział 9.8) albo włącz wysyłanie na serwer z opcją „Usuwać odbicia po wysłaniu” (rozdział 10.2). Usuwanie pojedynczych odbić w „Edycji” nie zwalnia miejsca.
Białe światło przy odbiciu	Ta sama karta w czasie blokady powtórzeń. Odczekaj i przyłóż ponownie.
Stałe żółte światło, panel pokazuje „czynnik kart nie odpowiada”	Zrestartuj urządzenie („Restartuj urządzenie” albo odłącz i podłącz zasilanie). Jeśli to nie pomoże, skontaktuj się z producentem.
Zamek się nie otwiera	Sprawdź „Tryb pracy” przełącznika (fabrycznie „wyłączony”), przewody i biegunowość na złączu oraz opcję „Przełącznik tylko przy wejściu”. Zamek musi mieć własne zasilanie.
Zła data lub godzina	Ustawienia > System > Data i czas > „Synchronizuj z przeglądarką”. Sprawdź pole „Strefa czasowa” i serwery czasu (rozdział 9.4).
Panel pokazuje „certyfikat serwera wygaśł albo zegar urządzenia jest zły” albo „certyfikat serwera jeszcze nieważny”	Sprawdź datę i godzinę urządzenia (rozdział 9.4). Gdy zegar jest dobry, certyfikat serwera wygaśł: odnowi go administrator serwera.
Data i godzina znikają po odłączeniu prądu	Bateria podtrzymująca zegar jest rozładowana. Wymień ją (rozdział 13.4). Do tego czasu ustaw zegar po każdym zaniku zasilania (rozdział 9.4); z dostępem do internetu urządzenie ustawi go samo.
Nie pamiętasz hasła albo zgubiłeś telefon z 2FA	Reset danych dostępowych kartą resetującą albo przyciskiem (rozdział 13).

Problem	Co zrobić
Zgubiona karta resetująca	Przypisz nową kartę w sekcji Ustawienia > Bezpieczeństwo > Karta resetująca (rozdział 9.7). Stara przestanie działać.
Panel pokazuje „Synchronizacja z serwerem jest aktywna” zamiast raportów	Odbicia są rozliczane na serwerze lub w Chmurze ADARAZ (8.6).
Panel pokazuje „Wysyłanie odbić jest wstrzymane”	Adres serwera zaczyna się od http:// i prowadzi poza sieć lokalną (adres IP w internecie, nazwa wskazująca adres w internecie albo przekierowanie z serwera). Zmień go na https:// albo na adres IP serwera w sieci lokalnej (10.2). Odbicia czekają w urządzeniu.

14

Dane techniczne

14.1 Parametry

Parametr	Wartość
Model	RAZ-RCP-1
Przeznaczenie	rejestracja czasu pracy, czytnik kart zbliżeniowych
Zasilanie	5 V DC, 2 A, gniazdo USB-C
Warunki pracy	tylko wewnątrz pomieszczeń, temperatura od 0 do 50 °C
Czytnik kart	13,56 MHz, ISO/IEC 14443 typ A (np. MIFARE), numer karty 4-7 bajtów albo 10 bajtów (karta 10-bajtowa rozpoznawana po 7 pierwszych bajtach)
Wi-Fi	2,4 GHz; własny hotspot (WPA2/WPA3, do 4 urządzeń) i dołączanie do sieci Wi-Fi
Bluetooth	nieużywany (wyłączony w oprogramowaniu)
Ethernet	RJ45, adres z DHCP, kabel do ok. 100 m

Parametr	Wartość
Wyjście	złącze przełącznika, 3 zaciski śrubowe, maks. 24 V DC, 2 A
Sygnalizacja	światło RGB i sygnał dźwiękowy
Zegar	zegar czasu rzeczywistego podtrzymywany baterią CR2032 (3 V, nietładowalna)
Pamięć danych	7,5 MB, szyfrowana
Zabezpieczenia	bezpieczny rozruch (Secure Boot), szyfrowanie pamięci, HTTPS, logowanie dwuskładnikowe, dziennik zdarzeń bezpieczeństwa (co najmniej 1000 zdarzeń), przywracanie ustawień fabrycznych z kasowaniem pamięci
Panel	przeglądarka internetowa; polski, angielski, niemiecki
Integracje	Chmura ADARAZ, własny serwer (http2, http3, Skryba 8 bit, Skryba 10 bit), zarządzanie centralne
Wymiary (wys. x szer. x gł.)	17,7 x 7,3 x 3,6 cm
Masa	150 g
Obudowa	tworzywo sztuczne
Tryb pracy	ciągły

14.2 Interfejsy i usługi sieciowe w stanie fabrycznym

Stan fabryczny to ustawienia urządzenia po wyjęciu z pudełka.

Interfejs	Stan fabryczny	Usługi dostępne przez ten interfejs
Hotspot Wi-Fi 2,4 GHz (sieć urządzenia; WPA2/WPA3, do 4 urządzeń)	włączony	adres urządzenia 10.10.10.1; serwer DHCP, który przydziela adresy podłączonym telefonom i komputerom; panel HTTP (port 80) i HTTPS (port 443); nazwa rcp-xxxxxxx.local (mDNS, port UDP 5353)

Interfejs	Stan fabryczny	Usługi dostępne przez ten interfejs
Ethernet (RJ45)	włączony	urządzenie pobiera adres z DHCP i ogłasza w tej sieci swoją nazwę rcp-xxxxxxx.local (mDNS); panel (porty 80 i 443) i zapytania mDNS z tej sieci są odrzucane, dopóki nie włączysz „Dostęp z sieci lokalnej” (rozdział 9.3)
Wi-Fi, dołączanie do sieci firmowej	wyłączone	po włączeniu (rozdział 9.2) tak samo jak Ethernet
Bluetooth	wyłączony w oprogramowaniu	brak

W trybie awaryjnym karty resetującej (5 minut, rozdział 13.1) hotspot ma nazwę i hasło z etykiety i udostępnia wyłącznie stronę do wpisania hasła panelu z etykiety (porty 80 i 443); pozostałe interfejsy działają bez zmian.

W obu sieciach urządzenie odpowiada na ping (ICMP). W stanie fabrycznym jedyne połączenie wychodzące do internetu to synchronizacja czasu (SNTP, port UDP 123, serwery tempus1.gum.gov.pl i pool.ntp.org, razem z zapytaniami DNS o te nazwy), gdy urządzenie ma dostęp do internetu. Serwery czasu zmienisz albo wyłączysz w rozdziale 9.4.

Usługi, które włącza dopiero administrator (fabrycznie wyłączone):

- **„Dostęp z sieci lokalnej”** (rozdział 9.3): panel przez HTTPS (port 443) z Ethernetu i z sieci Wi-Fi; port 80 przekierowuje na HTTPS; odpowiedzi na zapytania mDNS z tych sieci,
- **wysyłanie odbić na własny serwer** (rozdział 10.2): połączenia HTTPS albo HTTP pod podany adres; HTTP wyłącznie do serwera w sieci lokalnej,
- **Chmura ADARAZ** (rozdział 10.1): połączenia HTTPS z Chmurą ADARAZ (parowanie: api.panel.adaraz.com),
- **zarządzanie centralne** (rozdział 10.3): połączenia HTTPS z serwerem devices.adaraz.com,
- **aktualizacja z internetu** (rozdział 11): tylko na polecenie administratora („Sprawdź”, „Aktualizuj teraz”), połączenie HTTPS z serwerem devices.adaraz.com.

Urządzenia przygotowane na zamówienie integratora mogą mieć fabrycznie inne ustawienia, np. włączone zarządzanie centralne albo dołączanie do sieci Wi-Fi firmy.

14.3 Czytnik kart i dane osobowe

Jedyną funkcją urządzenia, która odbiera dane z otoczenia, jest czytnik kart 13,56 MHz. Urządzenie nie ma kamery ani mikrofonu.

- Czytnik odczytuje tylko numer karty (UID) w chwili jej przyłożenia. Nie odczytuje ani nie zapisuje innych danych zapisanych na karcie.
- Odbicie to numer karty z datą i godziną, zapisane w szyfrowanej pamięci urządzenia. Imię i nazwisko przypisuje się do numeru karty w panelu (rozdział 6).
- Numer każdej przyłożonej karty, także karty spoza listy pracowników, urządzenie zapisuje jako odbicie w trybie „każda karta” (rozdział 6.5). Numery losowe telefonów, zegarków i kart płatniczych są odrzucane i nie są zapisywane (rozdział 2.4).
- Odbicia i lista pracowników są pobierane do przeglądarki zalogowanego użytkownika panelu, która liczy z nich raporty (rozdział 7.4), oraz do kopii zapasowej (rozdział 12). Na inne serwery trafiają tylko wtedy, gdy administrator włączy wysyłanie odbić, Chmurę ADARAZ albo zarządzanie centralne (rozdział 14.2). Zapytania o czas do serwerów czasu (rozdział 9.4) nie zawierają danych osobowych, ale serwery te widzą publiczny adres IP sieci firmy; zamiast serwerów publicznych możesz wpisać serwer czasu w sieci firmy.
- Dziennik zdarzeń (rozdział 9.9) zawiera adresy IP urządzeń, z których korzystano z panelu, i nazwy kont, ale nie zawiera numerów kart ani haseł. Usuwa go przywrócenie ustawień fabrycznych (rozdział 13.3).

15

Pasma częstotliwości i maksymalna moc nadawania

Nadajnik	Pasmo częstotliwości	Moc nadawania
Wi-Fi	2400-2483,5 MHz	maks. 14 dBm
NFC/RFID	13,56 MHz (pasmo 13,553-13,567 MHz)	maks. 40 dBμA/m w odległości 10 m

Moc Wi-Fi można obniżyć w ustawieniach (rozdział 9.2, „Moc nadawania WiFi”); 14 dBm to wartość fabryczna i zarazem najwyższa.

16

Utylizacja i ochrona środowiska



Przekreślony koszt oznacza, że zużyte urządzenia ani baterie nie wolno wyrzucać razem z innymi odpadami. Oddaj je do punktu zbiórki zużytego sprzętu elektrycznego i elektronicznego. Sprzęt i baterie zawierają substancje i części, które wyrzucone z odpadami mogą szkodzić środowisku i zdrowiu ludzi. Selektywna zbiórka umożliwia ponowne użycie i recykling.

Zużyta baterię po wymianie (rozdział 13.4) oddaj do punktu zbiórki baterii.

Zużyty sprzęt oddasz bezpłatnie do punktu selektywnego zbierania odpadów komunalnych (PSZOK) w swojej gminie albo sprzedawcy przy zakupie nowego sprzętu tego samego rodzaju. Oddając zużyty sprzęt do zbiórki, gospodarstwo domowe pomaga w jego ponownym użyciu i recyklingu.



Urządzenie spełnia wymagania dyrektywy RoHS 2011/65/UE w sprawie ograniczenia stosowania substancji niebezpiecznych.

17

Uproszczona deklaracja zgodności UE



ADARAZ P.S.A. niniejszym oświadcza, że typ urządzenia radiowego RAZ-RCP-1 jest zgodny z dyrektywą 2014/53/UE. Pełny tekst deklaracji zgodności UE jest dostępny pod następującym adresem internetowym:
<https://adaraz.com/pl/device/raz-rcp-1?v=1>



18

Producent i kontakt

ADARAZ P.S.A.

ul. Towarowa 23

43-100 Tychy

Polska

e-mail: contact@adaraz.com

W sprawie reklamacji, gwarancji (rozdział 19) i wsparcia technicznego napisz na contact@adaraz.com. Papierową wersję tej instrukcji wyślemy bezpłatnie na prośbę.

19

Gwarancja

Gwarantem jest ADARAZ P.S.A., ul. Towarowa 23, 43-100 Tychy, Polska, contact@adaraz.com. Gwarancja dotyczy urządzenia RAZ-RCP-1 o numerze seryjnym podanym na jego etykiecie. Dokumentem gwarancyjnym jest skrócona instrukcja obsługi dołączona do urządzenia.

- **Okres.** 24 miesiące od daty zakupu.

- **Zakres.** Gwarancja obejmuje wady wynikające z przyczyn tkwiących w urządzeniu (wady fabryczne i materiałowe). Gwarant usunie wadę (naprawi urządzenie) albo dostarczy urządzenie wolne od wad, niezwłocznie, nie później niż w ciągu 14 dni od dostarczenia urządzenia.
- **Jak skorzystać z gwarancji.** Zgłoś wadę e-mailem na contact@adaraz.com albo listownie na adres gwaranta. Podaj numer seryjny z etykiety, opis wady i datę zakupu (najlepiej z kopią paragonu lub faktury). Dostarcz urządzenie na koszt gwaranta na adres gwaranta. Gwarant odeśle je na swój koszt.
- **Czego gwarancja nie obejmuje.** Wad i uszkodzeń powstałych wskutek: zasilania innego niż 5 V DC przez gniazdo USB-C; uszkodzeń mechanicznych, termicznych lub chemicznych, w tym zalania; ingerencji w układ elektroniczny lub próby samodzielnej naprawy przez osoby nieuprawnione; niewłaściwego podłączenia urządzeń zewnętrznych, np. zwarcia na złączu przełącznika. Naciśnięcie przycisku reset i wymiana baterii zgodnie z instrukcją obsługi nie powodują utraty gwarancji.
- **Uprawnienia z mocy prawa.** W przypadku braku zgodności rzeczy sprzedanej z umową kupującemu z mocy prawa przysługują środki ochrony prawnej ze strony i na koszt sprzedawcy, a gwarancja nie ma wpływu na te środki ochrony prawnej.

20

Montaż na ścianie i szablon wiercenia

Urządzenie wiesza się na czterech wkrętach w ścianie. Wkręty i kołki nie wchodzi w skład zestawu. W pokrywie tylnej są cztery otwory jak dziurka od klucza: okrągły otwór $\varnothing$ 9,7 mm na łeb wkręta i szczelina szerokości 4,2 mm, która biegnie od niego 10 mm w górę i 10 mm w dół. Otwory są w rozstawie 30 mm w poziomie i 60 mm w pionie, a górne leżą 44,3 mm pod górną krawędzią obudowy.

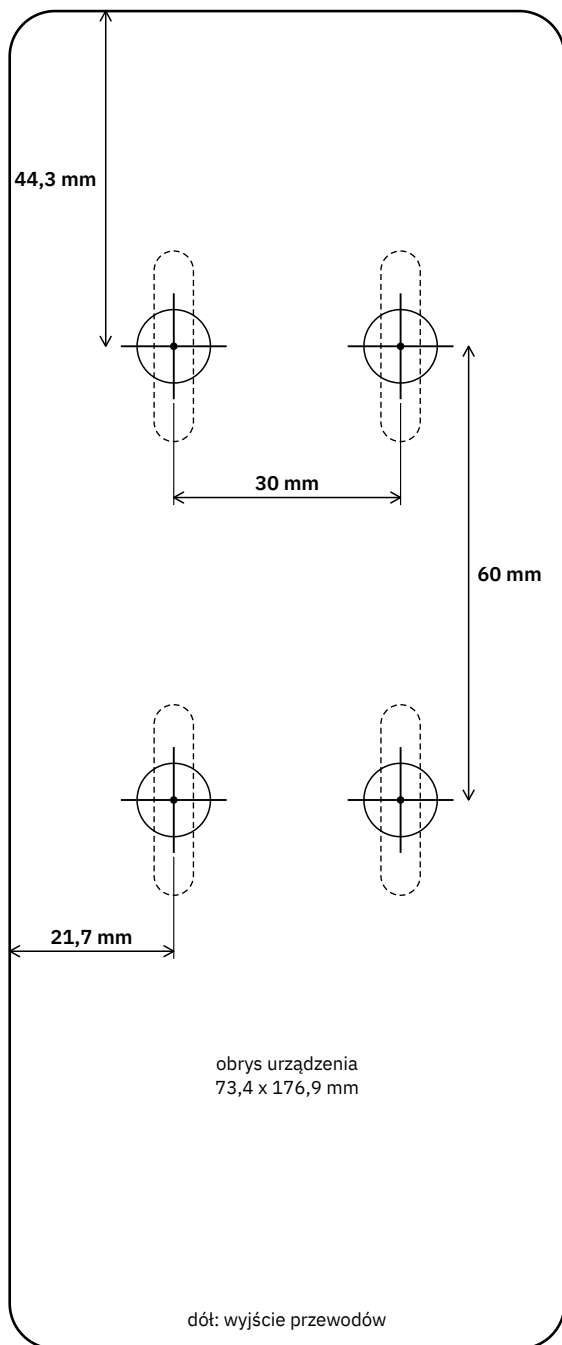
Wkręty: 4 wkręty z łbem płaskim albo półokrągłym (nie stożkowym): trzpień o średnicy najwyżej 4 mm (np. 3,5 mm), łeb o średnicy od 6 do 9 mm i wysokości najwyżej 2,5 mm. Kołki dobierz do podłoża i do wkrętów.

Szablon: szablon wiercenia w skali 1:1 jest na następnej stronie. Wydrukuj ją w skali 100 % (bez dopasowania do strony) i sprawdź na linijce kontrolnej, że odcinek ma 50 mm. Szablon do druku 3D (4 tulejki z otworami $\varnothing$ 5 mm w tym samym rozstawie) pobierzesz ze strony instrukcji (kod QR na okładce).

- ① Wybierz miejsce (rozdział 2.5). Przewody podłączasz we wnęce na przewody, zanim zawieszisz urządzenie (rozdział 4.1).
- ② Przyłóż szablon do ściany czytnikiem do góry, wypoziomuj go i zaznacz 4 punkty wiercenia: środki krzyżyków na szablonie z papieru albo otwory w tulejkach szablonu do druku 3D.
- ③ Nawierć otwory, włóż kołki i wkręć wkręty tak, żeby spód tła był 7 mm od ściany, najwyżej 7,5 mm. Łeb bliżej ściany nie zaczepi się w szczelinie, a dalej od ściany dotknie płytki wewnątrz urządzenia.
- ④ Nałóż urządzenie czytnikiem do góry tak, żeby tły wkrętów weszły w okrągłe otwory w pokrywie tylnej, i zsuń je w dół, aż tły oprą się o koniec szczelin (do 10 mm). Po zsunięciu urządzenie jest do 10 mm niżej niż obrys na szablonie.
- ⑤ Sprawdź, czy urządzenie przylega do ściany i się nie chwieje. Gdy się chwieje, zsuń je w górę, zdejmij i wkręć wkręty odrobinę głębiej. Gdy nie daje się zsunąć, wykręć je odrobinę.

Żeby zdjąć urządzenie ze ściany, przesun je w górę, aż tły wkrętów znajdą się w okrągłych otworach, i odsun od ściany.

GÓRA (czytnik)



Szablon wiercenia

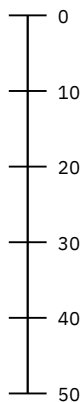
skala 1:1

Drukuj w skali 100 %, bez dopasowania do strony.
Linijka niżej musi mieć dokładnie 50 mm.

Przytóż szablon do ściany czytnikiem do góry, wypoziomuj i zaznacz 4 punkty wiercenia (środki krzyżyków).

Linia przerywana: otwory w pokrywie tylnej.
Po zawieszeniu i zsunięciu w dół urządzenie jest do 10 mm niżej niż obrys.

Wkręty i montaż:
rozdział 20.



linijka kontrolna 50 mm



ADARAZ

ADARAZ P.S.A.
ul. Towarowa 23, 43-100 Tychy, Polska
contact@adaraz.com

<https://adaraz.com/pl/device/raz-rcp-1?v=1>