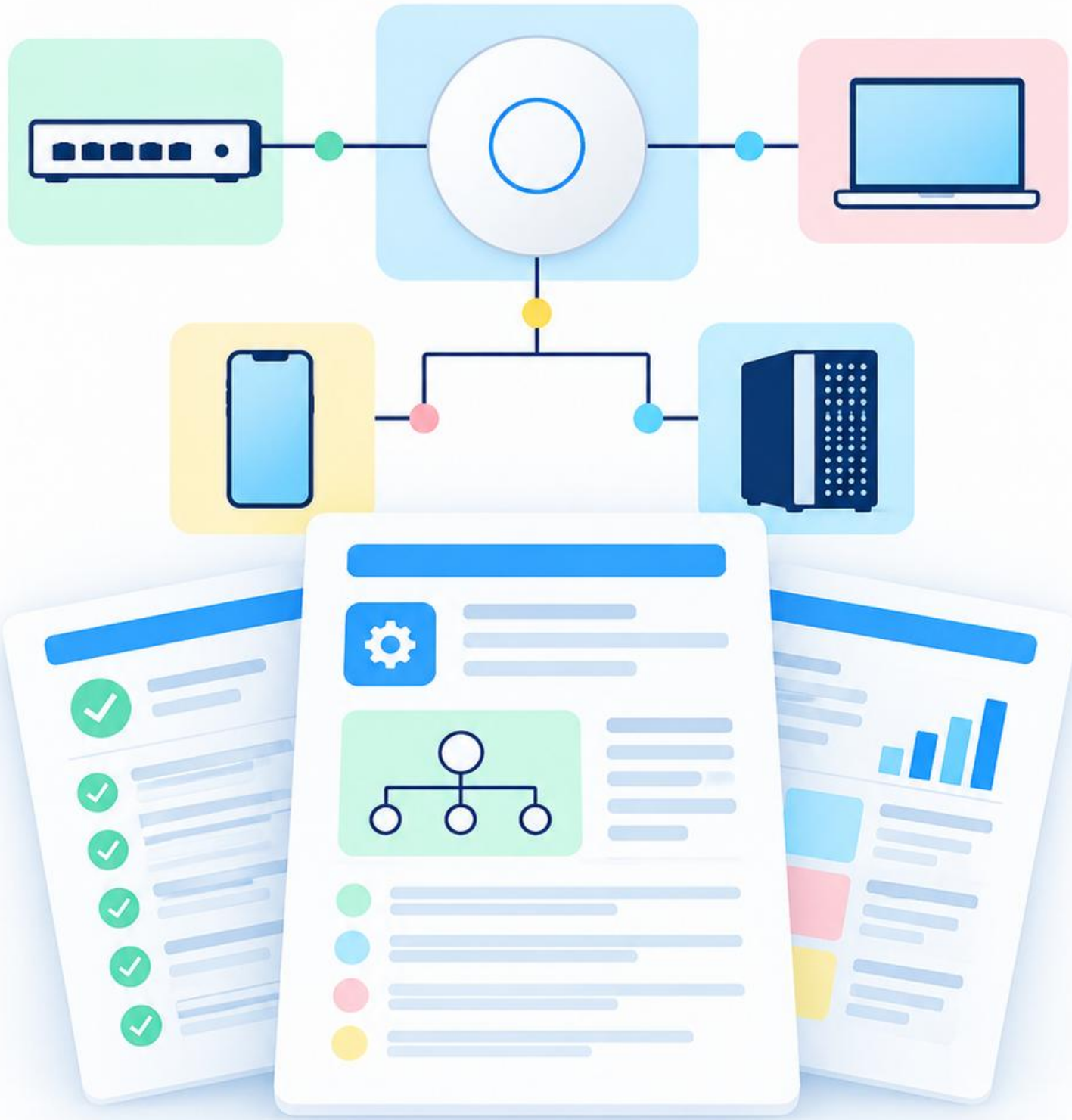
Karta konfiguracji i dokumentacji UniFi

Dane wdrożenia, decyzje i dowody w jednym miejscu



Ostoja

Ostoja · Jak wypełniać karty

Uzupełniaj kartę podczas pracy, a nie dopiero po zakończeniu całego wdrożenia. Oddziel dane potwierdzone od założeń wymagających sprawdzenia.

Dla każdej pozycji podaj nazwę obiektu, datę oraz osobę odpowiedzialną. Puste pole oznacz jako brak danych albo nie dotyczy.

Przykład wypełnienia:

Obiekt	element	stan	dowód
Biuro Łódź	SW-Recepcja	potwierdzony	zdjęcie oznaczenia portu i test klienta.

Wpisz: obiekt i data _____.

Wpisz: autor oraz osoba zatwierdzająca _____.

Wpisz: status i odwołanie do dowodu _____.

Zapisuj nazwy dokładnie tak, jak w instalacji. Identyfikator karty powinien prowadzić do aktualnego rysunku lub bezpiecznie przechowywanego pliku.

Nie umieszczaj haseł ani prywatnych kluczy. Po zmianie porównaj dokument z konfiguracją, popraw zależne karty i zachowaj informację o poprzednim stanie.

Źródła: [8]

Ostoja · Karta · Klient i zakres

Ustal, co jest objęte wdrożeniem i kto podejmuje decyzje. Opis zakresu ogranicza nieporozumienia podczas odbioru i późniejszego serwisu.

Obiekt / adres: _____.

Kontakt organizacyjny / rola: _____.

Zakres i wyłączenia: _____.

Usługi krytyczne / okno prac: _____.

Osoba zatwierdzająca / data: _____.

Przykład wypełnienia: Obiekt: Biuro Łódź. Zakres: sieć pracowników i gości. Usługa krytyczna: obsługa recepcji. Odbiór: kierownik obiektu.

Przy każdej zmianie zakresu dopisz wpływ na dostępność i termin. Nie wpisuj prywatnych danych kontaktowych, jeśli wystarcza zatwierdzony kontakt służbowy.

Sprawdź, czy osoba odbierająca rozumie kryteria działania. Nazwa zakresu powinna odpowiadać późniejszym testom, a otwarte zależności mieć właściciela.

Zapisz zależności od sąsiednich urządzeń, aby późniejsza zmiana nie przerwała sprawdzonej drogi do usługi.



Źródła: [8]

Ostoja · Karta · Inwentarz i wersje

Zapisz urządzenia w sposób pozwalający rozpoznać je fizycznie i w aplikacji. Sama nazwa handlowa nie wystarcza do oceny zgodności.

Nazwa / model / lokalizacja:	_____.
Rola / MAC / numer seryjny:	_____.
Wersja firmware / data odczytu:	_____.
Host Network / wersja aplikacji:	_____.
Gwarancja lub serwis / właściciel:	_____.

Przykład wypełnienia:
Nazwa: SW-Recepcja. Rola: przełącznik dostępowy.
Lokalizacja: szafa recepcji.
Wersja: przepisać z urządzenia podczas odbioru.

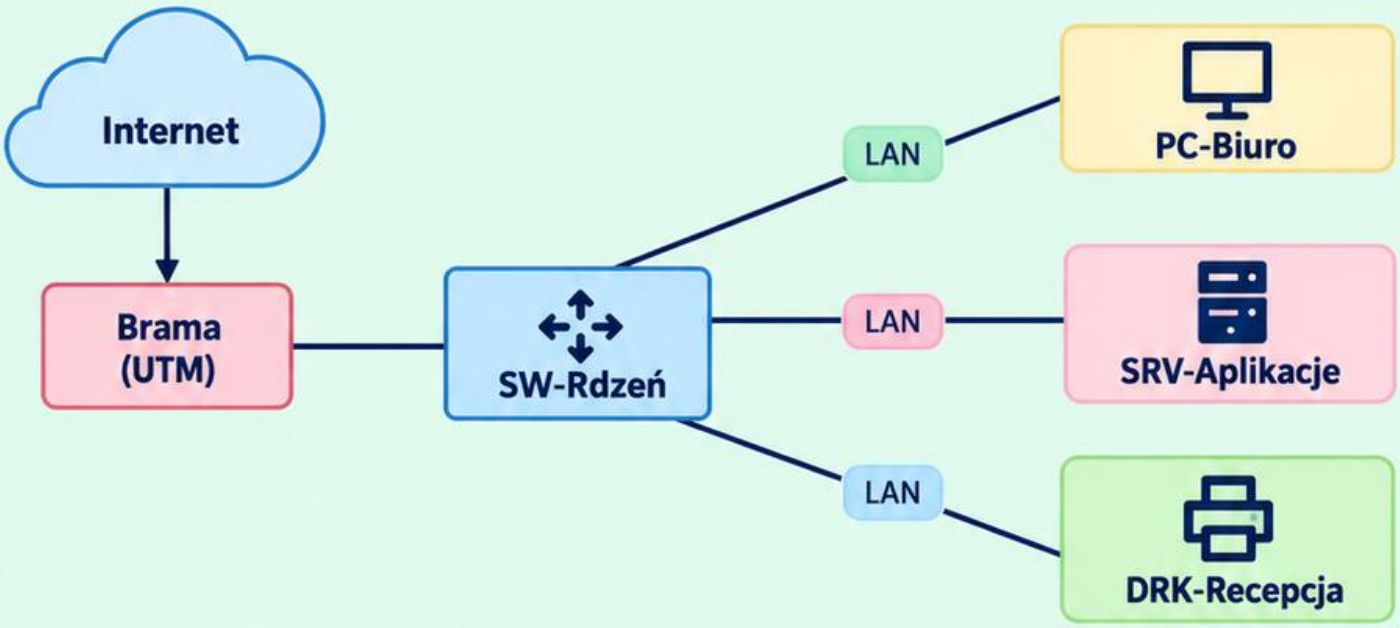
Nie wpisuj zgadywanej wersji z opakowania. Jeśli urządzenie oczekuje na montaż, oznacz stan planowany i zaplanuj potwierdzenie po uruchomieniu.

Porównaj inwentarz z listą Devices i fizycznymi etykietami. Aktualizuj wpis po wymianie sprzętu oraz po zmianie wersji mającej wpływ na procedury.

Źródła: [4]

Ostoja · Karta · Topologia i połączenia

Opisz każdy odcinek przez oba końce, nie tylko przez odbiornik.
Rysunek logiczny i fizyczny powinny mieć wspólne nazwy urządzeń.



1. **Identyfikator przewodu / trasa:** _____.
2. **Koniec A: urządzenie / port:** _____.
3. **Koniec B: urządzenie / port:** _____.
4. **Typ łącza / rola / redundancja:** _____.
5. **Rysunek powiązany / data testu:** _____.

Przykład: REC-UP | SW-Rdzeń/5 → SW-Recepcja/1 | kabel K-12 | Ethernet 1 Gb/s | pojedynczy uplink.

Na rysunku zaznacz kierunek do bramy i połączenia zapasowe.
Nie dodawaj drugiej drogi bez opisanego mechanizmu STP lub zgodnej agregacji.

Potwierdź etykiety po obu stronach i porównaj z aktualnym stanem portów.
Zapis testu powinien umożliwić lokalizację przewodu bez odłączania działającej sieci.

Źródła: [5]

Ostoja · Karta · Plan adresacji i VLAN-ów

Każda sieć potrzebuje jednoznacznej roli, adresacji i miejsca routingu.
Sprawdź nakładanie z innymi lokalizacjami oraz sieciami używanymi przez VPN.

Nazwa / rola / identyfikator VLAN: _____.

Podsieć / brama / rodzina IP: _____.

Serwer DHCP / pula / rezerwacje: _____.

DNS / usługi zależne: _____.

Urządzenie routujące / polityka: _____.

Przykład:
Goście | VLAN 30 | 192.168.30.0/24 | brama .1 | DHCP .100–.220 | DNS .1 | blokada dostępu do biura.

Dla IPv6 zapisz metodę przydziału i wymagane zabezpieczenia oddzielnie.
Nie przyjmuj, że opis reguł IPv4 automatycznie obejmuje całą komunikację.

Przetestuj adres klienta w każdej sieci i porównaj go z kartą.
Każda niezgodność wymaga wyjaśnienia przed podpisaniem odbioru.

Źródła: [1]

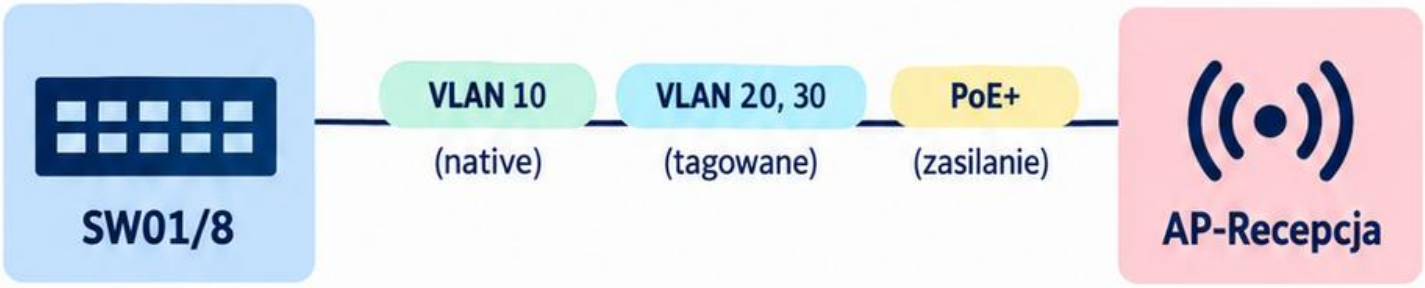
Ostoja • Karta • Porty i zasilanie PoE

Połącz rolę portu z wymaganiami odbiornika i jego zasilaniem.
Nazwa profilu bez opisu nie pokazuje, jakie sieci port rzeczywiście przenosi.

1. **Przełącznik / port / odbiornik:** _____.
2. **Native VLAN / tagowane VLAN-y:** _____.
3. **Tryb portu / prędkość łącza:** _____.
4. **PoE: standard / limit / odbiornik:** _____.
5. **Wynik próby / etykieta przewodu:** _____.

Przykład:

SW01/8 → AP-Recepcja | Native VLAN 10 | tagowane 20, 30 | wymagane PoE+ | pobór i budżet: odczyt w instalacji.



Przy zasilaniu zapisz parametry ze specyfikacji i osobno odczyt obserwowany. Dostępny budżet całego przełącznika sprawdź dla wszystkich podłączonych odbiorników.

Potwierdź adres klientów obu SSID oraz stabilność AP.
W karcie zaznacz uplink, aby kolejna osoba nie zmieniła przypadkowo drogi zarządzania.

Źródła: [6]

Ostoja · Karta · Plan Wi-Fi i radia

Zapisz osobno funkcję SSID oraz ustawienia radia. Dzięki temu zmiana pasma nie zostanie pomylona ze zmianą segmentu lub uprawnień.

SSID / sieć / nadawane AP: _____.

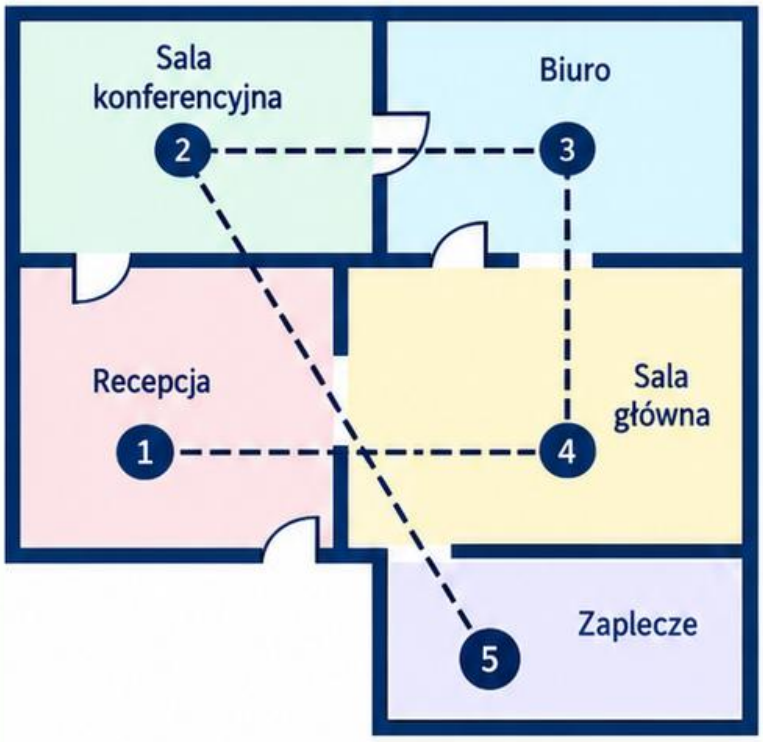
Zabezpieczenia / referencja sekretu: _____.

Kraj instalacji / pasma klientów: _____.

Kanał / szerokość / moc / data: _____.

Pomiar: klient / miejsce / wynik: _____.

Trasa pomiarowa (przykład)



Przykład wypełnienia:
SSID: Ostoja-Goście.
Sieć: Goście.
AP: recepcja i sale.
Ustawienia radia: potwierdzone pomiarem, bez przenoszenia recepty z innego obiektu.

Zanotuj obciążenie i porę pomiaru. Parametry oceniaj w normalnych miejscach pracy odbiorników, uwzględniając przeszkody i sąsiednie sieci.

Po zmianie powtórz tę samą trasę oraz próbę aplikacji. Zachowaj porównanie przed i po, zamiast wpisywać sam największy wynik testu prędkości.

Źródła: [19]

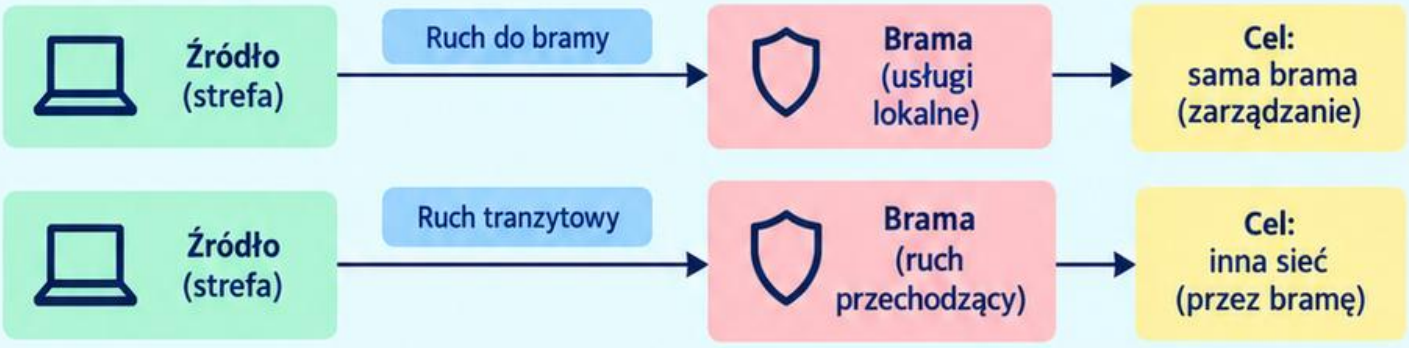
Ostoja · Karta · Macierz dostępu

Opisz oczekiwaną komunikację przed zapisaniem reguły.
Źródło, cel i usługa muszą być na tyle konkretne, aby umożliwiały próbę pozytywną i negatywną.

1. **Źródło / strefa / rodzina IP:** _____.
2. **Cel / strefa / adres usługi:** _____.
3. **Protokół / port / kierunek / decyzja:** _____.
4. **Wyjątek / uzasadnienie / właściciel:** _____.
5. **Test dozwolony / zabroniony / data:** _____.

Przykład wypełnienia:
Źródło: Goście. **Cel:** panel administracyjny bramy.
Decyzja: blokada. Próba kontrolna: internet działa, panel pozostaje niedostępny.

Odróżnij ruch do samej bramy od ruchu przechodzącego przez nią.
Wyjątki dla usług infrastruktury dokumentuj zgodnie z ich rzeczywistym miejscem działania.



Porównaj kartę z kolejnością polityk i przypisaniem sieci do stref.
Zapisz stan używanej wersji oraz dowód testu, zamiast samej nazwy reguły.

Źródła: [3]

Ostoja · Karta · Rejestr VPN bez sekretów

Karta opisuje cel tunelu i odpowiedzialność za dostęp. Klucze prywatne, hasła i pełne profile pozostają w zatwierdzonym bezpiecznym magazynie.

1. **Nazwa / typ / cel tunelu:** _____.
2. **Właściciel / uprawniony użytkownik:** _____.
3. **Punkt końcowy / sieci / trasy:** _____.
4. **DNS / dozwolone usługi / strefy:** _____.
5. **Identyfikator sekretu / cofnięcie dostępu:** _____.

Klucze prywatne, hasła i pełne profile nie w karcie



Zatwierdzony bezpieczny magazyn

Przykład wypełnienia: Tunel: Serwis-Recepcja. Użytkownik: uprawniony serwisant. Cel: wskazana usługa. Sekret: odwołanie do wpisu w magazynie, bez kopiowania zawartości.

Sprawdź nakładanie adresacji oraz to, czy ruch ma być dzielony czy pełny. Nie traktuj samego aktywnego tunelu jako dowodu dostępu do aplikacji.



Zapisz datę próby z sieci zewnętrznej, stan tunelu i obie próby dostępu. Dla WireGuard dopisz świeży handshake; inne VPN mają inne wskaźniki.

- **Data próby** z sieci zewnętrznej
- **Stan tunelu** (np. aktywny / nieaktywny)
- **Dwie próby dostępu** (np. dozwolona / zablokowana)
- \+ **Dla WireGuard:** świeży handshake (inne VPN mają inne wskaźniki)

Źródła: [22]

Ostoja · Karta · Kopia zapasowa i odzyskiwanie

Opisz nie tylko miejsce kopii, lecz także sposób sprawdzenia odzyskania działania. Kopia bez potwierdzonego zakresu może nie obejmować całej instalacji.



System / zakres kopii / wersja: _____.

Data kopii / bezpieczna lokalizacja: _____.

Właściciel dostępu / identyfikator: _____.

Środowisko próby / zależności: _____.

Wynik odtworzenia / data / autor: _____.

Przykład: Network | kopia po odbiorze 21.10.2026 | plik KRK-Network-2026-10-21 | **magazyn B-02** | wersja źródłowa: odczyt z hosta.

Nie zapisuj sekretów dostępu do magazynu w tej karcie. Wskaż zatwierdzoną procedurę ich uzyskania oraz osobę dostępną podczas awarii.

Przed testem ustal wpływ na urządzenia produkcyjne i możliwość wycofania. Po nim potwierdź zarządzanie oraz krytyczne usługi, a nie samo wczytanie pliku.

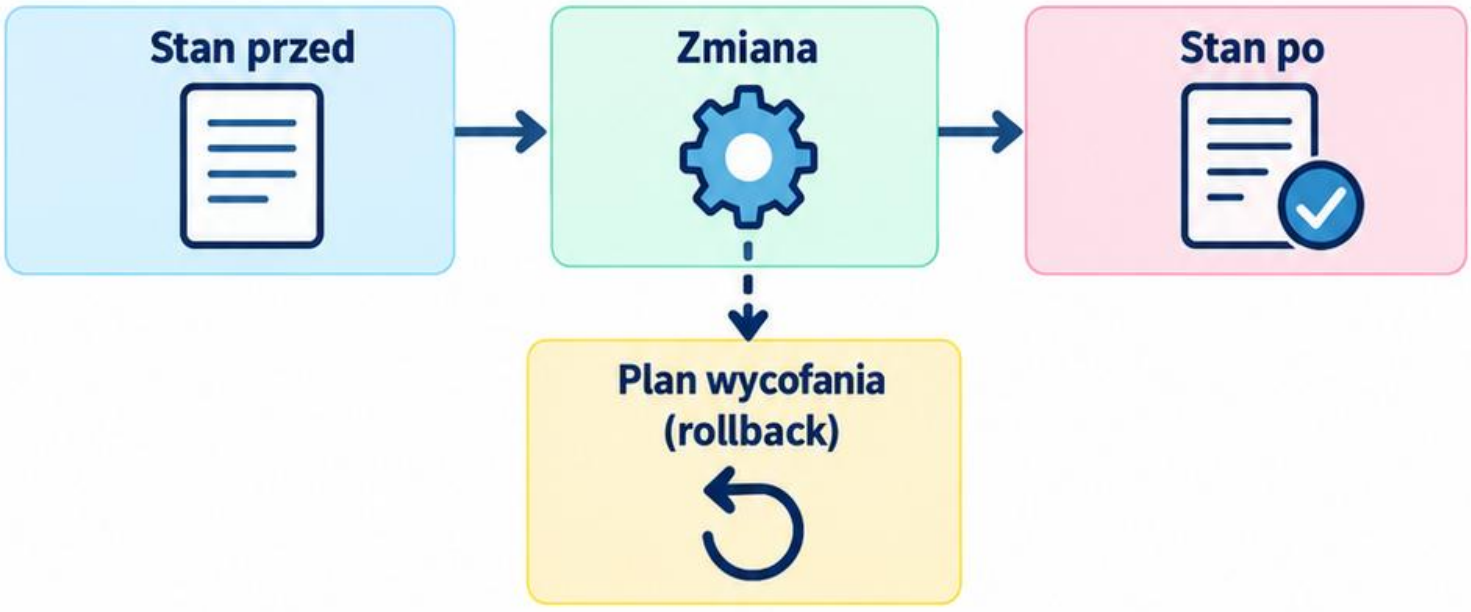
Źródła: [8]

Ostoja · Karta · Rejestr zmian

Każda zmiana powinna mieć powód, właściciela i możliwość oceny wyniku. Opis ostatniej modyfikacji często skraca późniejsze szukanie przyczyny awarii.

1. **Data / autor / zgoda na zmianę:** _____.
2. **Powód / element / stan przed:** _____.
3. **Stan po / zależne urządzenia:** _____.
4. **Plan wycofania / dostęp lokalny:** _____.
5. **Test / wynik / otwarte zadania:** _____.

Przykład wypełnienia: Zmiana: ograniczenie VLAN-ów portu AP. **Powód:** usunięcie niepotrzebnej sieci. **Walidacja:** oba wymagane SSID działają, AP pozostaje online.



Zapisz dokładnie jeden logiczny **zakres zmiany.** Jeśli modyfikujesz kilka zależności, opisz kolejność i warunek zatrzymania prac po nieudanym teście.

Po wykonaniu porównaj wynik z celem i zaktualizuj powiązane karty. Niezakończone zadanie ma wskazanego właściciela, aby nie zniknęło z dokumentacji.

Źródła: [4]

Ostoja • Karta • Testy i odbiór

Odbiór potwierdza zachowanie usług oraz ograniczeń. Sam zielony status urządzeń nie dowodzi, że użytkownik może wykonać swoje rzeczywiste zadanie.

1 **Usługa / oczekiwany wynik:**

_____.

2 **Klient / miejsce / czas próby:**

_____.

3 **Próba pozytywna / wynik:**

_____.

4 **Próba zabroniona / wynik:**

_____.

5 **Uwagi / właściciel / podpis odbioru:**

_____.

Przykład wypełnienia:
Test gości: strona internetowa działa. Panel administracyjny niedostępny. Dwa kontrolowane urządzenia sprawdzone na tym samym oraz na różnych AP.

Dla błędu zapisz wpływ i warunek ponownego testu. Nie podpisuj niezweryfikowanej pozycji jako poprawnej tylko dlatego, że inne elementy działają.

Odbierający powinien znać otwarte ograniczenia i miejsce aktualnej dokumentacji. Po usunięciu usterki dopisz nowy wynik z datą, zachowując historię poprzedniej próby.

Źródła: [20]

Źródła

Dokumentacja Ubiquiti. Stan sprawdzenia: 21.10.2026. Numery odpowiadają odwołaniom w materiale.

[1]
Tworzenie sieci VLAN
https://help.ui.com/hc/en-us/articles/9761080275607

[3]
Zapora strefowa
https://help.ui.com/hc/en-us/articles/115003173168

[4]
Ustawienia przełączników
https://help.ui.com/hc/en-us/articles/33402927617047

[5]
Pętle i STP
https://help.ui.com/hc/en-us/articles/24292724428311

[6]
Tryby i dostępność PoE
https://help.ui.com/hc/en-us/articles/115000263008

[8]
Kopie i migracja
https://help.ui.com/hc/en-us/articles/360008976393

[19]
Stabilność i opóźnienia Wi-Fi
https://help.ui.com/hc/en-us/articles/221029967

[20]
Izolacja sieci i klientów
https://help.ui.com/hc/en-us/articles/18965560820247

[22]
Serwer WireGuard
https://help.ui.com/hc/en-us/articles/115005445768