

Eleve Admin

Czasowe uprawnienia administratora

Kontrolowana instalacja aplikacji i zarządzanie urządzeniami Windows

Przegląd produktu dla firm i zespołów IT

Spis treści

01	Wprowadzenie i panel główny	3-5
02	Zgłoszenia instalacji i czasowe prawa administratora	6-19
03	Inventory i szczegóły urządzeń	20-32
04	Wiadomości, blokady i audyt	33-42
05	Użytkownicy, konfiguracja i aktualizacje agenta	43-75
06	Rozpoczęcie testów i podsumowanie	76-79

Upewnienia przyznawane na czas zadania

- 01** Użytkownik zgłasza potrzebę i podaje uzasadnienie.
- 02** Administrator ocenia zgłoszenie oraz dostępne informacje o pliku.
- 03** Zgoda obejmuje określony czas i rodzaj operacji.
- 04** Historia zgłoszenia i dane urządzenia pomagają rozliczyć wykonanie.

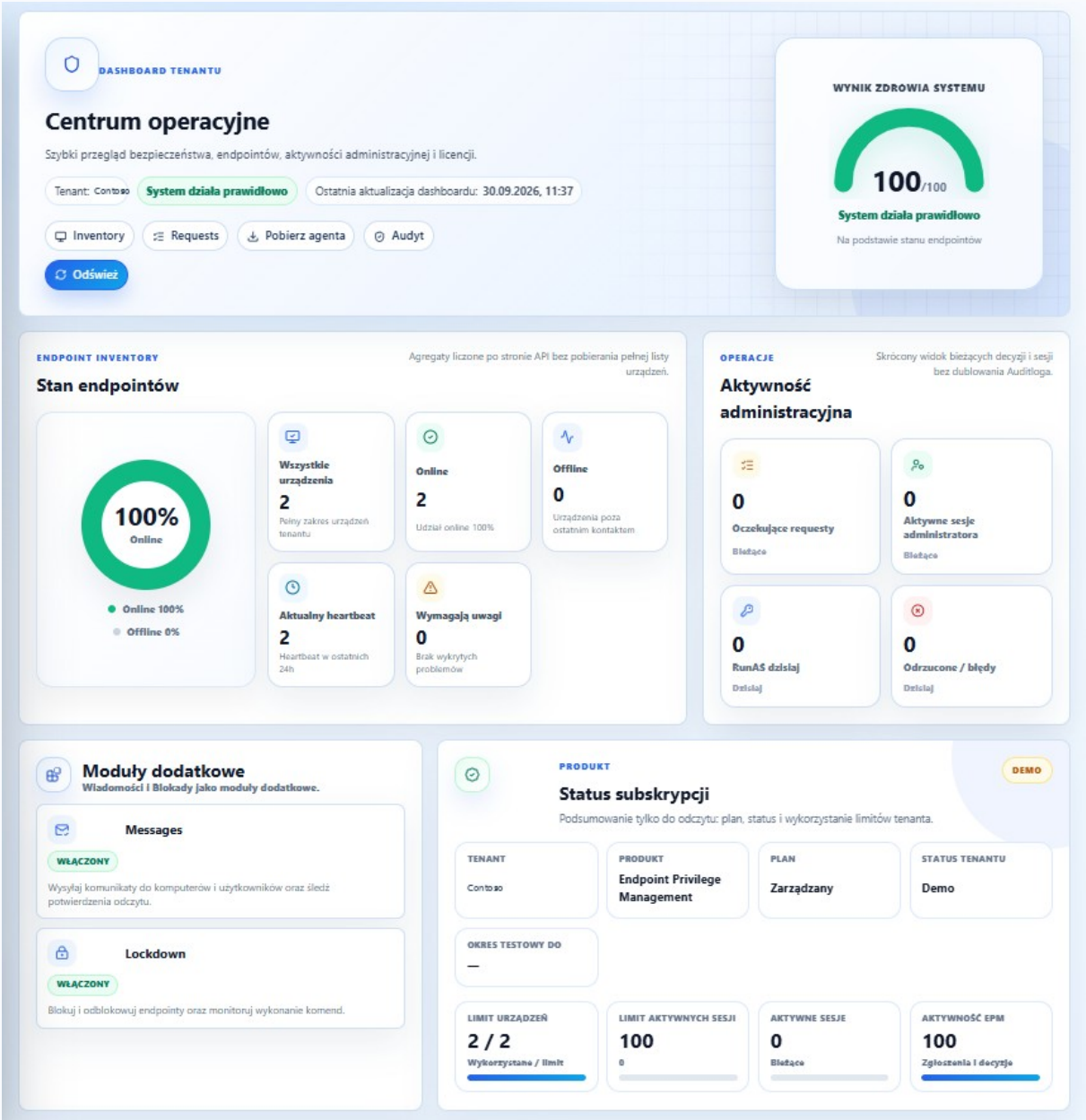
Centrum operacyjne IT

Stan urządzeń i kontakt z agentami.

Zgłoszenia oczekujące na decyzję i aktywne sesje.

Skróty do Inventory, Requests, pobierania i audytu.

Dostępność modułów i informacje o subskrypcji.



Jeden widok do rozpoczęcia codziennej pracy

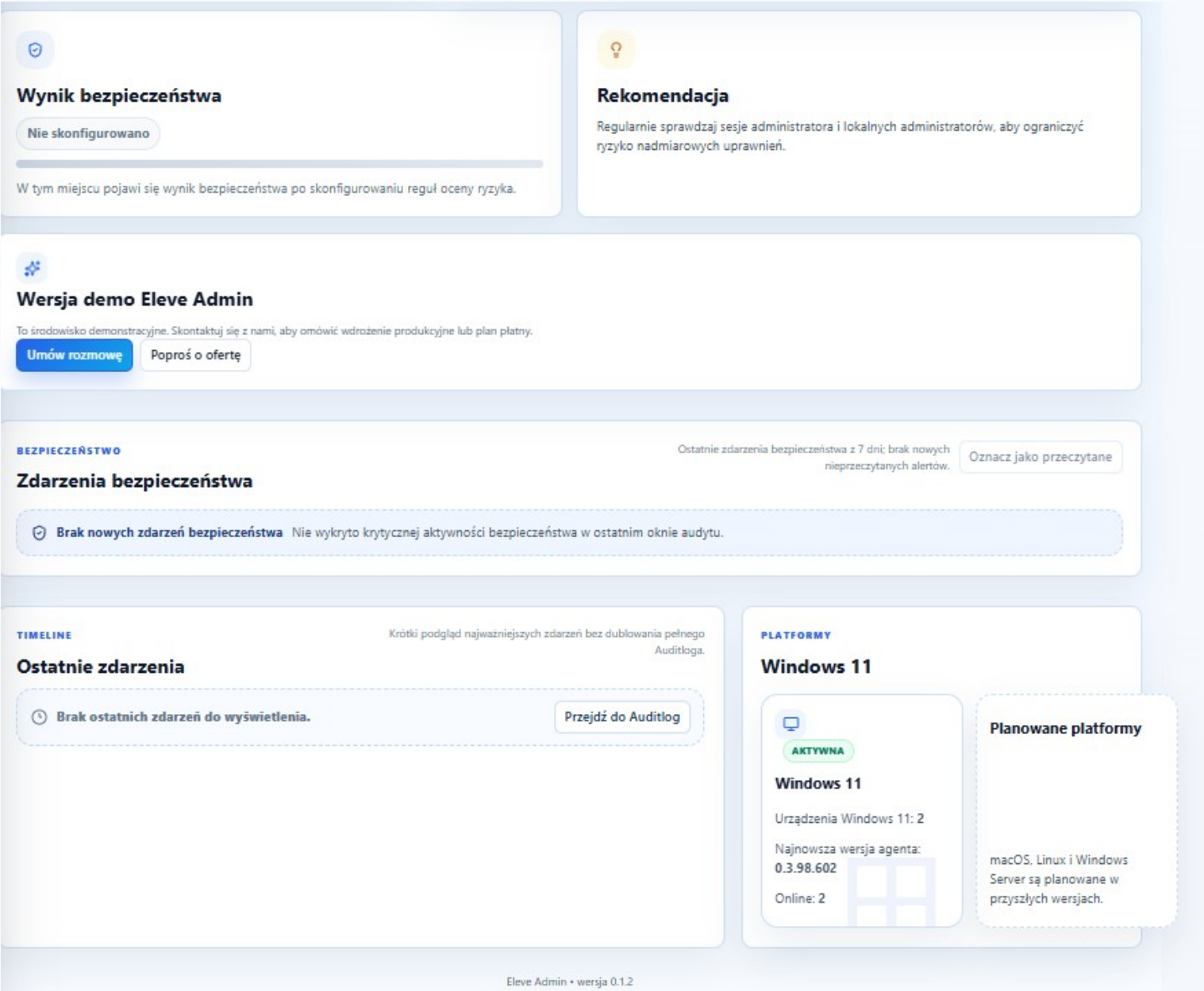
Stan środowiska i sygnały bezpieczeństwa

Kondycja urządzeń i wynik bezpieczeństwa to odrębne wskaźniki.

Ocena bezpieczeństwa wymaga skonfigurowania reguł.

Ostatnie zdarzenia i zalecenia wskazują obszary do sprawdzenia.

Widok informuje również o wersji agenta i obsługiwanych platformach.



Lista zgłoszeń i historia decyzji

Zgłoszenia dotyczą aplikacji lub sesji administratora.

Filtry rozdzielają oczekujące, aktywne, odrzucone i zakończone sprawy.

Wyszukiwanie i zakres dat ułatwiają odtworzenie historii.

Wiersz zgłoszenia prowadzi do decyzji oraz szczegółów wykonania.

REQUESTS

Oczekujące prośby o zatwierdzenie

Przeglądaj i zatwierdzaj/odrzucaj zgłoszenia elevacji tenanta.

0

OCZEKUJĄCE

3

AKTYWNE

18

ODRZUCONE

25

ZAMKNIĘTE

64

ANULOWANE

Odśwież

Widok: Zamknięte — pokazuje sesje zakończone, wygasłe lub cofnięte. Wygasła sesja nie jest traktowana jako anulowana.

Typ:

Wszystkie

Aplikacje

Sesje administratora

Szukaj w historii wniosków

acdsee-free

Zakres

Ostatnie 30 dni

Sortowanie

Najnowsze

Widoczne: 1

W tej zakładce: 25

Typ: Aplikacje

Zakres: 30d

Strona: 1/1

Na stronę

10

Pierwsza

Poprzednia

Następna

Ostatnia

7a3f3d57...7ff9

CLOSED

Aplikacja

🕒 18.09.2026, 13:10

📄 Status: CLOSED

💻 Komputer: LAPTOP-002

👤 Użytkownik: jan.kowalski

✉️ Adres Email: jan.kowalski@example.com

☎️ Telefon: 555010100

📁 Aplikacja / proces: acdsee-free.exe

🏢 Dostawca: CN=ACD Systems International Inc., O=ACD Systems International Inc., L=Victoria, S=British Columbia, C=CA

Decyzja administratora

Decyzja

Zatwierdzono

Zatwierdził

Contoso admin@example.com

Czas decyzji

18.09.2026, 13:11

Komentarz

Zatwierdzono z Requests UI

Brak dostępnych akcji.

Zgłoszenie instalacji przez użytkownika

Użytkownik pobiera instalator przez przeglądarkę.

Agent otwiera formularz instalacji przez Eleve.

Formularz identyfikuje plik i zbiera dane kontaktowe.

Użytkownik opisuje potrzebę i wysła zgłoszenie.

Eleve Admin

Eleve Admin

Zainstaluj aplikację przez Eleve

Wybrano pobrany instalator EXE/MSI do obsługi przez Eleve Admin.
Eleve Admin nie uruchomi pliku teraz. Wyślij prośbę do administratora albo anuluj instalację.

Szczegóły pliku

Nazwa pliku	7z2603-x64.exe
Ścieżka	C:\Users\jan.kowalski\Downloads\7z2603-x64.exe
Wydawca	Nieznane
Produkt	Nieznane
Opis pliku	Nieznane
SHA256	Nieznane

Adres e-mail

jan.kowalski@example.com

Numer telefonu

555010100

Powód

Chcę zainstalować tę pobraną aplikację przez Eleve Admin.

Contoso

Poproś o zgodę administratora

Anuluj instalację

Weryfikacja zgłoszenia przez administratora

Administrator widzi urządzenie, użytkownika i uzasadnienie.

Metadane wskazują źródło wykrycia oraz informacje o pliku.

Szczegóły obejmują wydawcę, rozmiar i identyfikator pliku.

Dostępne decyzje: zatwierdzenie lub odrzucenie.

0d179a9b...1724

PENDING

Aplikacja

🕒 30.09.2026, 12:50

📄 Status: PENDING

💻 Komputer: LAPTOP-001

👤 Użytkownik: jan.kowalski

✉ Adres Email: jan.kowalski@example.com

☎ Telefon: 555010100

📁 Aplikacja / proces: 7z2603-x64.exe

🏢 Dostawca: Igor Pavlov

📄 Plik / ścieżka procesu: C:\Users\jan.kowalski\Downloads\722603-x64.exe

🔒 Informacje bezpieczeństwa: SHA256: 0859c524b8...1a9e6edd · Size: 1.6 MiB

🗨 Powód użytkownika: Chcę zainstalować tę pobraną aplikację przez Eleve Admin.

Zatwierdź

Odrzuć

Metadane elevacji

Źródło przechwycenia	download_guard	
Metoda przechwycenia	download_detected	
Dostawca	Igor Pavlov	
Podmiot podpisu	Brak danych	
SHA256	0859c524b8...1a9e6edd	Kopiuj SHA256
Rozmiar pliku	1.6 MiB	
Ścieżka procesu	C:\Users\jan.kowalski\Downloads\722603-x64.exe	

Reputacja i bezpieczeństwo

Podpis	brak
Status podpisu	Nie udało się zweryfikować
Wydawca / podpisujący	-
Issuer	-
Thumbprint	-
VirusTotal status	found
Malicious	1
Suspicious	0
Harmless	0
Undetected	69

Ocena ryzyka pliku przed decyzją

Widok łączy wynik podpisu i analizę reputacji pliku.

Przykład: 1 wykrycie złośliwości, 0 podejrzeń i 69 wyników bez wykrycia.

Interfejs wskazuje wysokie ryzyko oraz rekomenduje odrzucenie.

Administrator w pokazanym procesie zatwierdził zgłoszenie mimo rekomendacji.

Podpis

brak

Status podpisu

Nie udało się zweryfikować

Wydawca / podpisujący

-

Issuer

-

Thumbprint

-

VirusTotal status

found

Malicious

1

Suspicious

0

Harmless

0

Undetected

69

Total engines

75

Last analysis

2026-09-30T10:46:58+00:00

Raport

[VirusTotal](#)

Poziom ryzyka

high

Rekomendowana akcja

Odrzuć

• virustotal_malicious_1_2

Klasyfikacja instalatora

Aplikacja

7-Zip

Nazwa produktu

7-Zip

Wersja produktu

26.03

Wersja pliku

-

Wykryty typ

Nieznany plik EXE

• downloads_origin

• not_signed

• user_parent_installer_or_user_location

► Zaawansowane (tylko do odczytu)

Stan wykonania: Oczekuje

• Administrator musi zatwierdzić albo odrzucić prośbę.

• Plik: C:\Users\jan.kowalski\Downloads\7z2603-x64.exe

• Źródło: download_guard

• Adres Email: jan.kowalski@example.com

• Telefon: 555010100

Ocena ryzyka wspiera decyzję administratora

Zgoda na instalację z limitem czasu

Administrator ustala czas ważności zgody.

W przykładzie okno uprawnienia wynosi 10 minut.

Polityka automatycznie dobiera strategię instalacji.

Decyzja pozostaje powiązana ze zgłoszeniem.

Zatwierdzenie requestu

Wybierz czas trwania zatwierdzenia. Strategia instalacji zostanie dobrana automatycznie przez politykę.

Czas zatwierdzenia w minutach

Anuluj

Zatwierdź

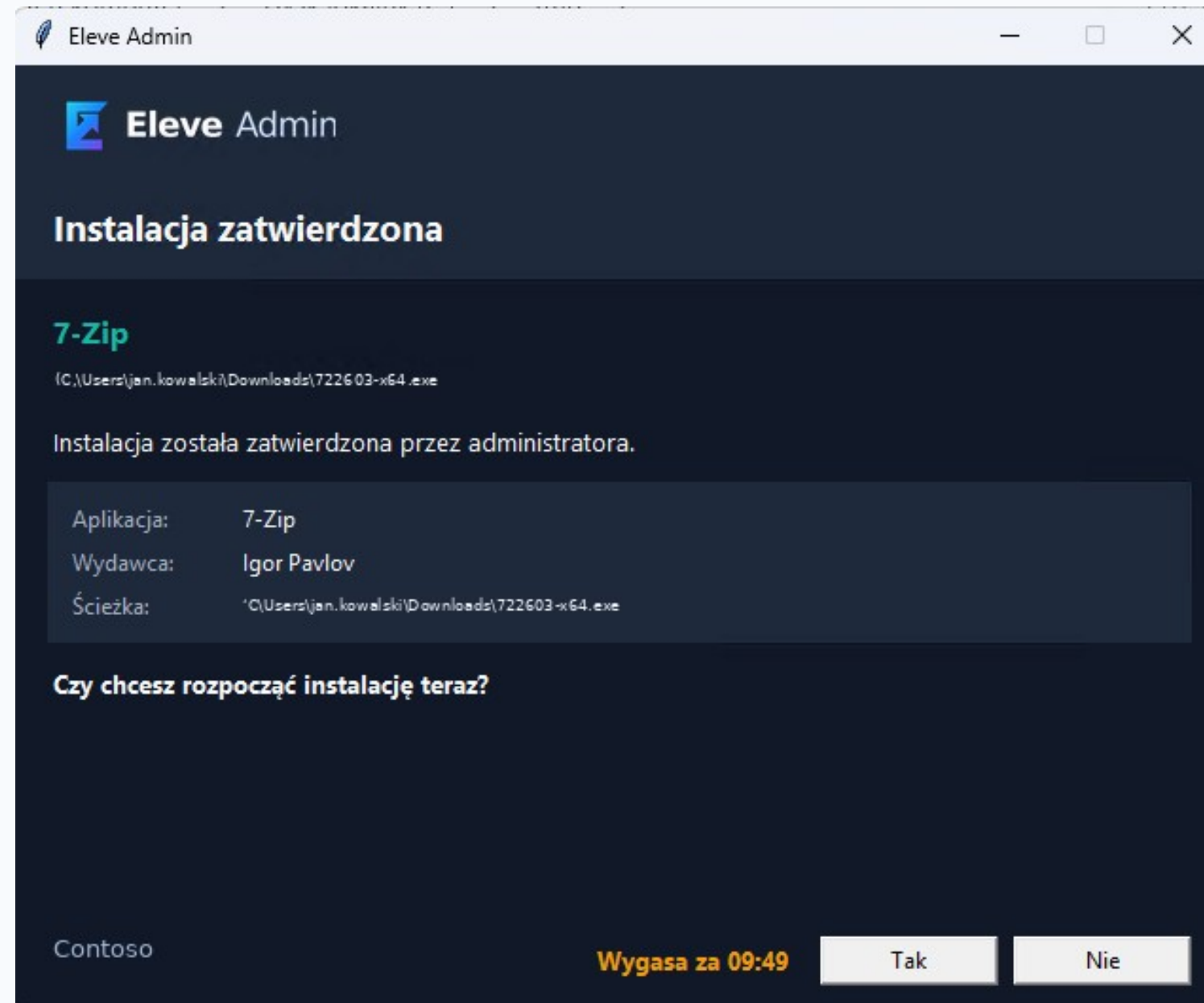
Powiadomienie o zatwierdzeniu

Agent informuje użytkownika o decyzji administratora.

Powiadomienie pokazuje pozostały czas na rozpoczęcie.

Użytkownik potwierdza chęć uruchomienia instalatora.

Proces pozostaje związany z zatwierdzonym plikiem.



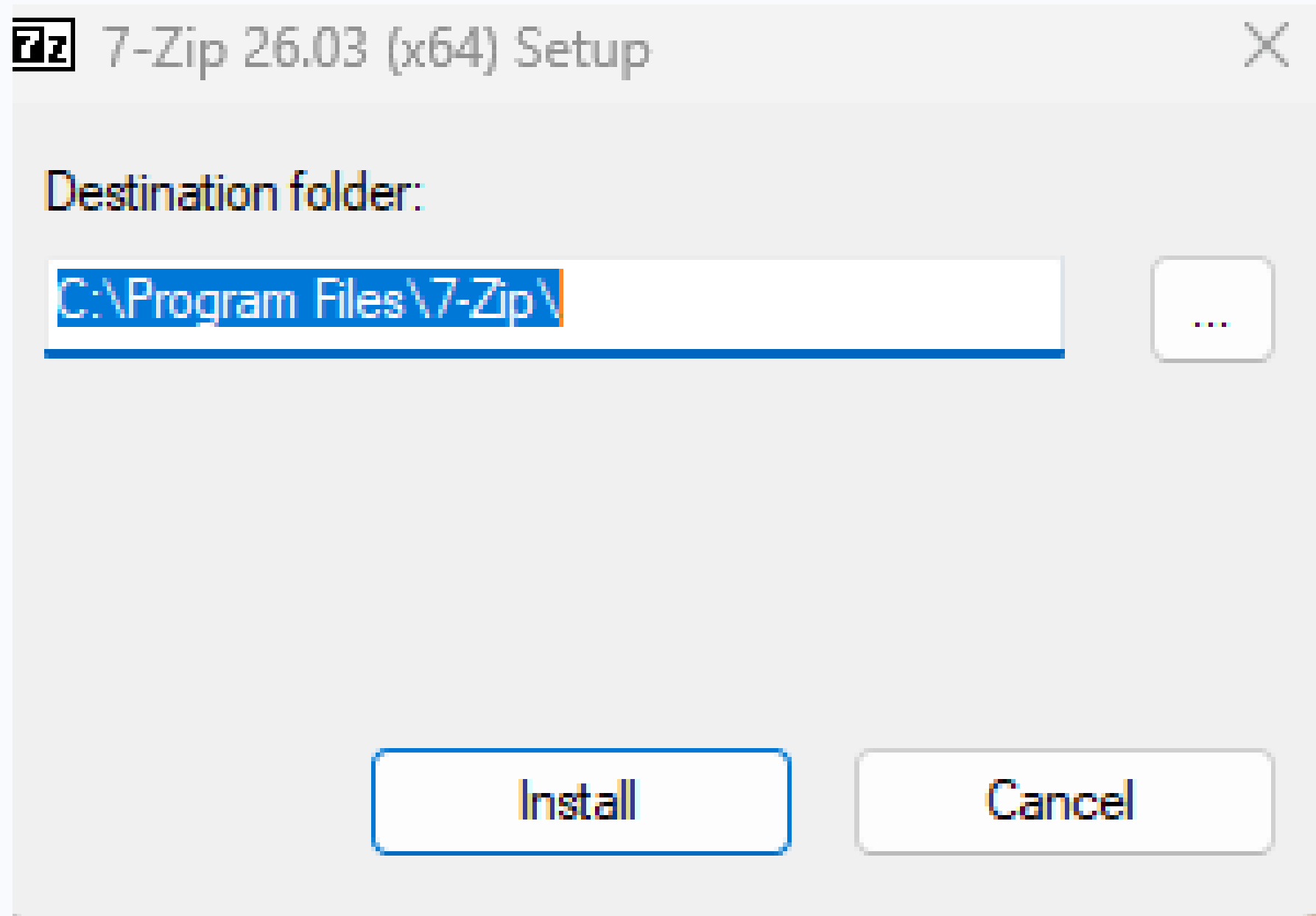
Instalacja bez stałych praw administratora

Użytkownik obsługuje standardowy interfejs instalatora.

Pokazany przykład instaluje 7-Zip w Program Files.

Użytkownik nie otrzymuje stałego członkostwa w grupie administratorów.

Zatwierdzenie dotyczy procesu instalacji aplikacji.



Rezultat wykonania instalatora

Historia rejestruje zakończenie procesu i kod wyjścia.

W przykładzie kod 0 oznacza normalne zakończenie.

Widok podaje czas wykonania i informację o restarcie.

Dla tego EXE obecność produktu nie została automatycznie zweryfikowana.

• user_parent_installer_or_user_location

▶ Zaawansowane (tylko do odczytu)

Stan wykonania: Zakończono

• Czas zatwierdzenia: 10 min

• Zatwierdził: Contoso admin@example.com

• Plik: C:\Users\jan.kowalski\Downloads\722603-x64.exe

• Adres Email: jan.kowalski@example.com

• Telefon: 555010100

• Exit code: 0

• Ostatnia aktualizacja: 30.09.2026, 12:53

• Komentarz: Zatwierdzono z Requests UI

Status końcowy

Zakończono monitorowanie instalatora

Exit code

0

Znaczenie exit code

Proces zakończył się prawidłowo

Czy wymagany restart

Nie

Czas startu

30.09.2026, 12:53

Czas zakończenia

30.09.2026, 12:54

Czas trwania

33 s

Czas zatwierdzenia

30.09.2026, 12:52

Ostatni heartbeat

30.09.2026, 12:53

Śledzone procesy

1

Typ instalatora

EXE

Rezultat instalacji

Instalator zakończył działanie prawidłowo (kod 0). Eleve Admin potwierdził zakończenie całej śledzonej rodziny procesów. Dla instalatorów EXE obecność produktu nie jest automatycznie weryfikowana.

Powód zakończenia

Zakończenie całej śledzonej rodziny procesów

Źródło zakończenia

agent

Wniosek o sesję administratora

Użytkownik wybiera czas potrzebny na zadanie.

Formularz zbiera uzasadnienie i dane kontaktowe.

Wniosek identyfikuje konto Windows i komputer.

Przykład dotyczy sesji trwającej 15 minut.

Czasowe prawa administratora

Eleve Admin

Czasowe prawa administratora

Poproś o czasowe prawa administratora, jeśli musisz wykonać zadanie wymagające uprawnień administracyjnych. Administrator może zatwierdzić lub odrzucić Twoją prośbę.

Konto użytkownika: LAPTOP-001\jan.kowalski

Komputer: LAPTOP-001

Email: jan.kowalski@example.com

Telefon: 555010100

Czas trwania: 15 min

Powód: Na potrzeby testu aplikacji wymagającej prawa admina podczas jej konfiguracji

Wyślij zgłoszenie

Zamknij

Contoso

Decyzja i czas trwania sesji

Administrator rozpatruje wniosek o sesję.

Zgoda wskazuje czas obowiązywania uprawnień.

W przykładzie administrator przyznaje 15 minut.

Limit widoczny w konfiguracji nie oznacza domyślnego czasu każdej sesji.

Zatwierdź sesję administratora

Użytkownik poprosił o: 15 min · Maksymalnie: 72 godziny

Przyznaj na

15

minut



Maksymalnie: 72 godziny

Anuluj

Zatwierdź

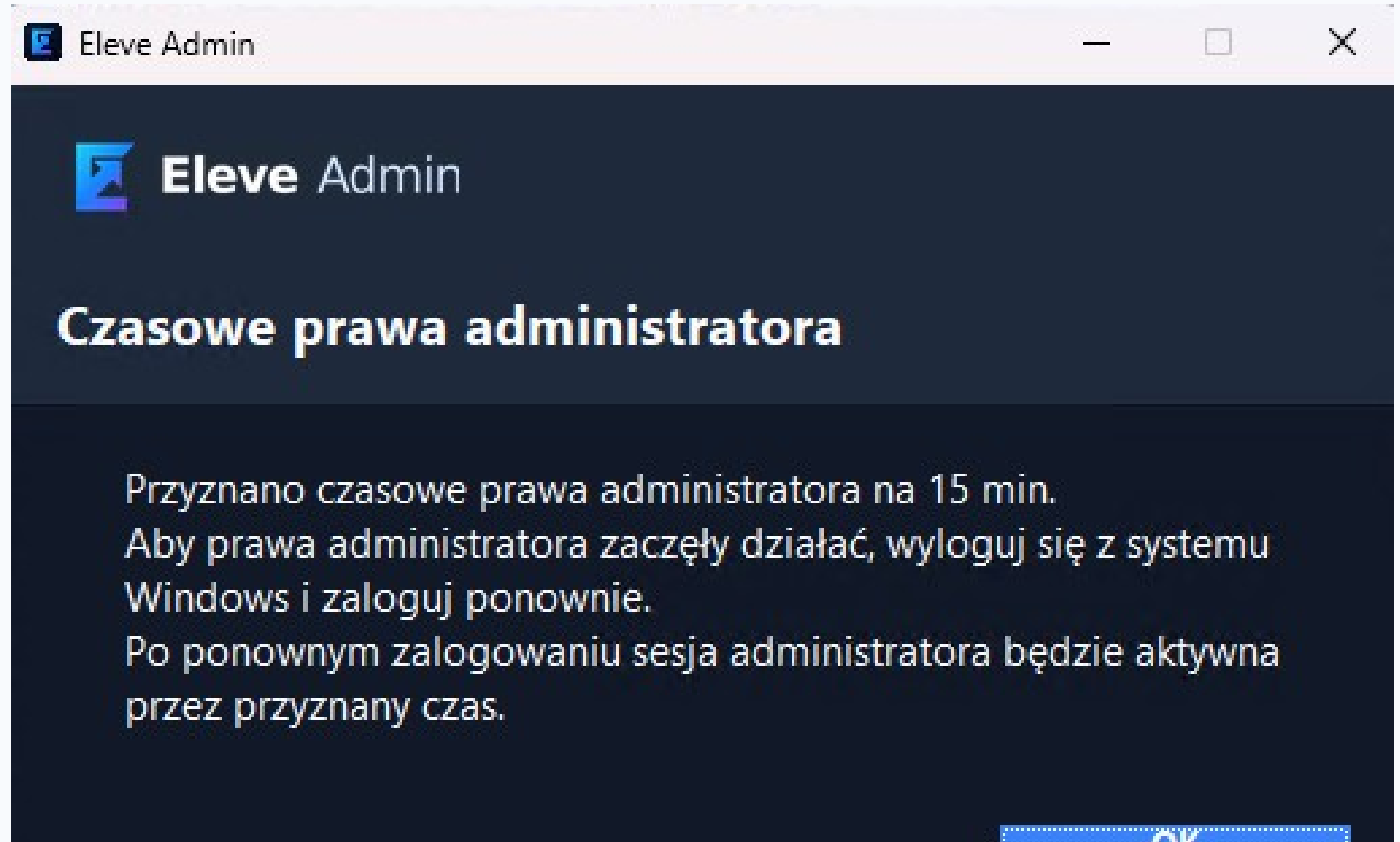
Aktywacja uprawnień w Windows

Agent potwierdza przyznanie czasowych uprawnień.

Pokazany komunikat wymaga wylogowania i ponownego zalogowania.

Użytkownik otrzymuje instrukcję zastosowania uprawnień.

Czas sesji pozostaje ograniczony zgodą administratora.



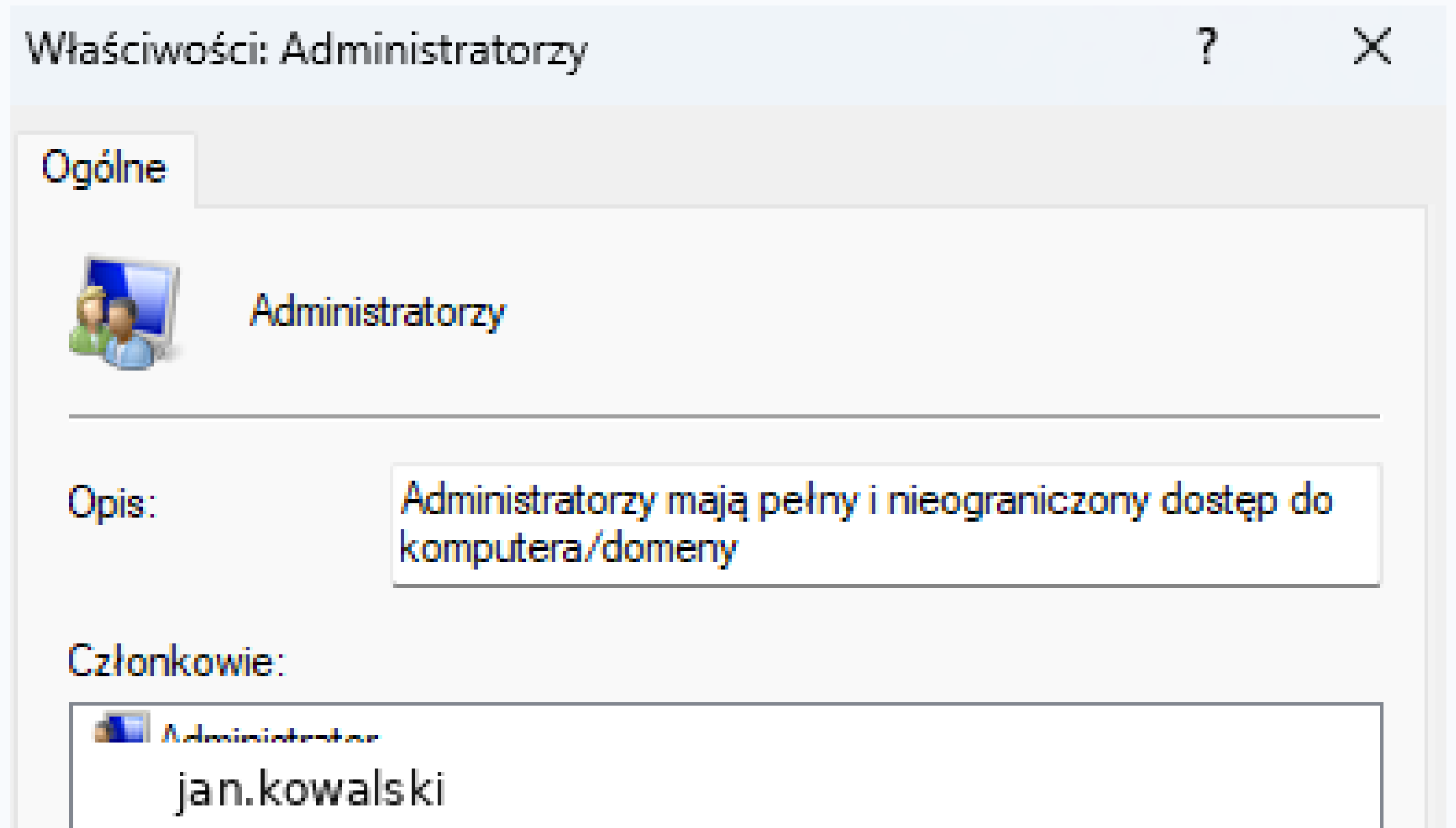
Potwierdzenie członkostwa w grupie

Widok Windows pokazuje członkostwo konta w grupie Administrators.

To potwierdzenie przyznania uprawnień w pokazanym scenariuszu.

Sesja ma określony termin zakończenia.

Po zakończeniu użytkownik wraca do standardowych uprawnień.



Ostrzeżenie przed końcem sesji

Agent informuje o zbliżającym się wygaśnięciu.

Komunikat podaje pozostały czas.

Użytkownik otrzymuje prośbę o zapisanie pracy.

Widok zapowiada odebranie praw i automatyczne wylogowanie.

Eleve Admin

Czasowe prawa administratora wygasają

Automatyczne wylogowanie za:

04:38

Zapisz pracę i zamknij otwarte aplikacje. Po zakończeniu odliczania Eleve odbierze czasowe prawa administratora, a system Windows automatycznie Cię wyloguje.

Po ponownym zalogowaniu konto będzie działać ze standardowymi uprawnieniami.

Wyloguj teraz

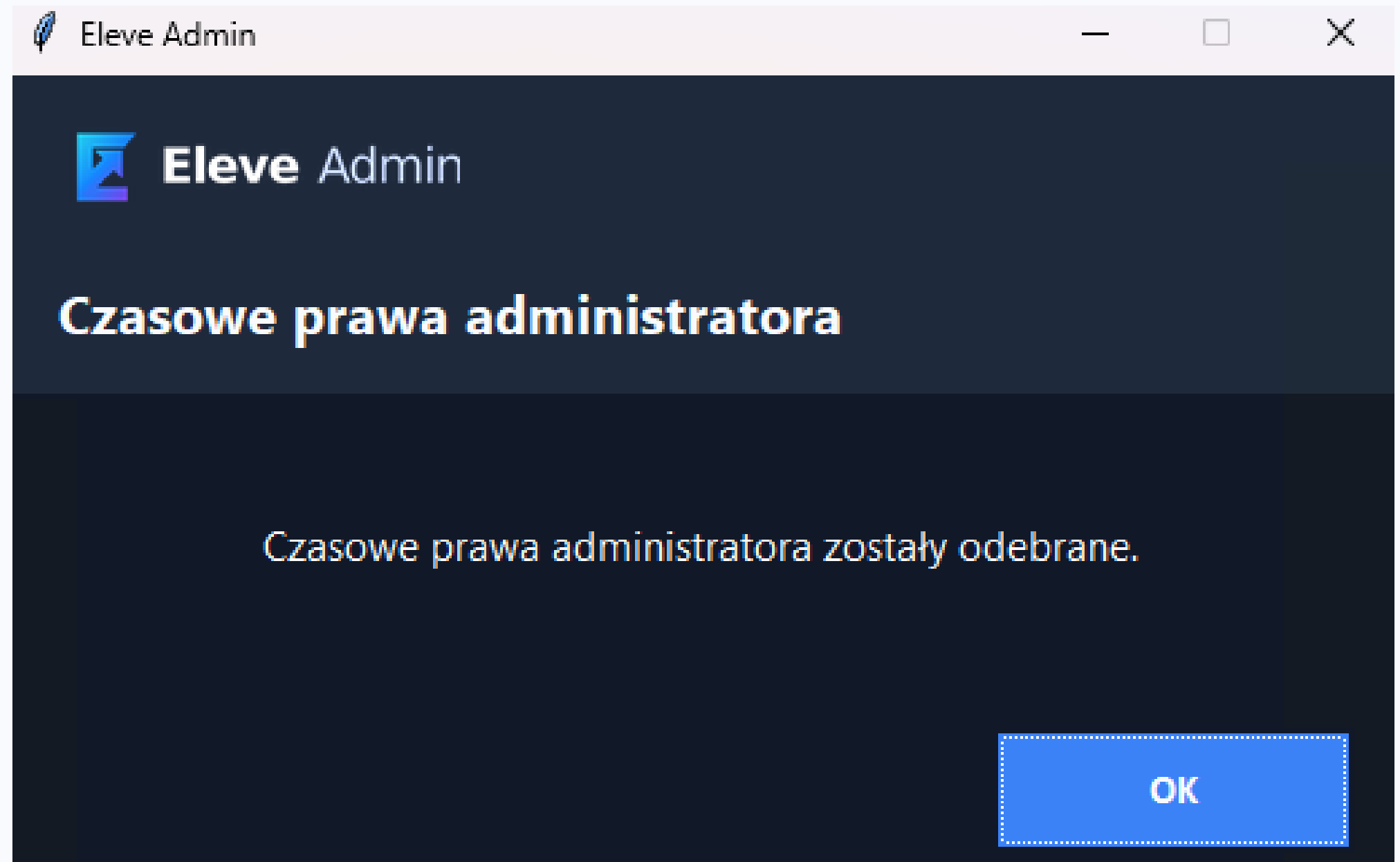
Odebranie czasowych uprawnień

Agent potwierdza zakończenie sesji administratora.

Czasowe prawa zostają odebrane.

Komunikat zamyka proces po stronie użytkownika.

Historia w konsoli pozwala później sprawdzić przebieg sesji.



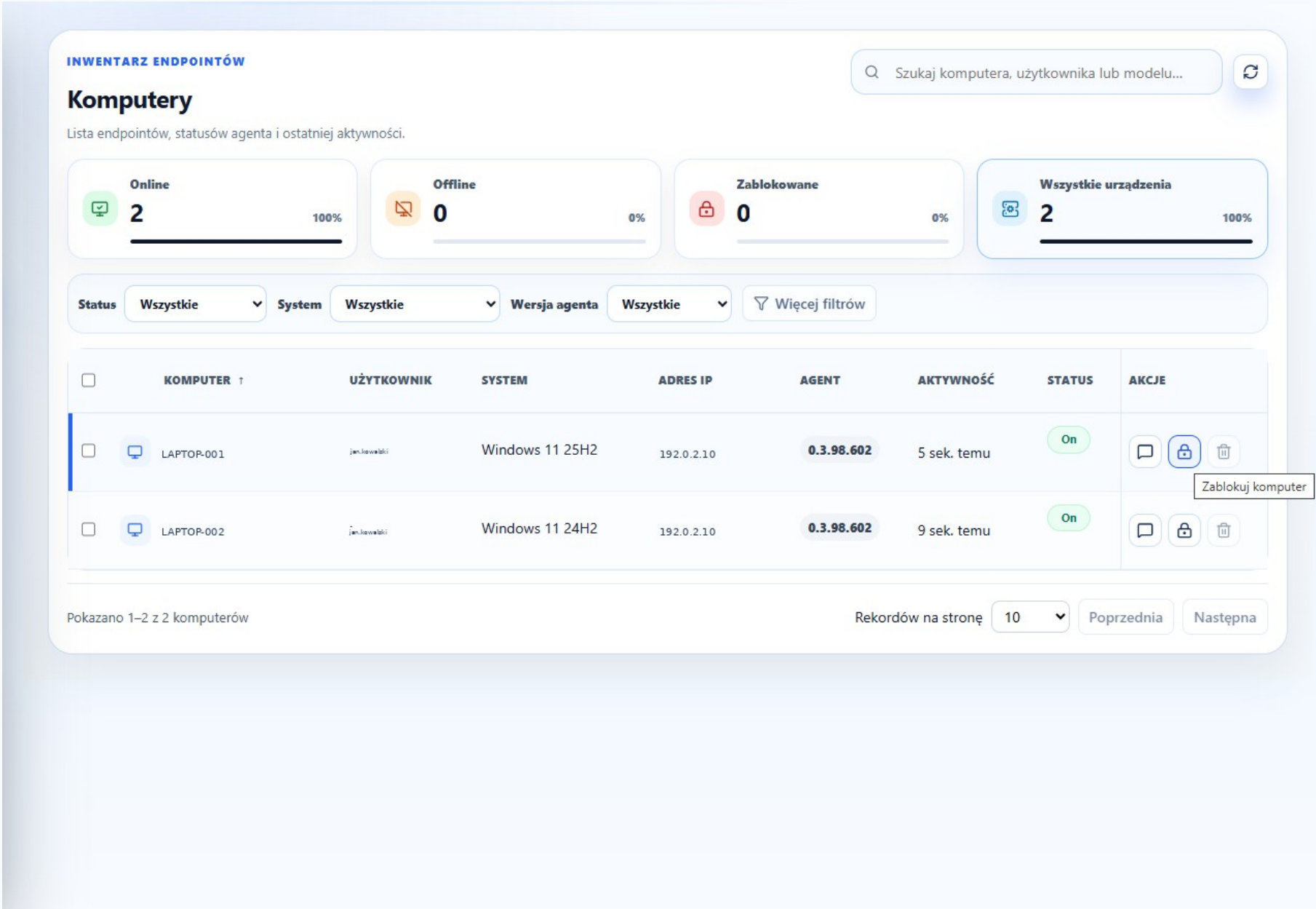
Rejestr urządzeń i akcje IT

Lista przedstawia urządzenia i status kontaktu.

Filtry obejmują dostępność, system i wersję agenta.

Wyszukiwanie pomaga odnaleźć komputer lub użytkownika.

Ikony przy urządzeniu uruchamiają wiadomość i blokadę.



Karta urządzenia i aktualność raportów

Nagłówek podaje stan kontaktu i dane urządzenia.

Osobne wskaźniki oceniają aktualność oprogramowania, sprzętu i lokalnych administratorów.

Zakładki prowadzą do raportów i historii.

Widok właściciela zależy od danych dostarczonych przez agenta.

Świeżość danych

Online

OSTATNIA AKTYWNOŚĆ

30.09.2026, 13:29

przed chwilą

Polityka: offline po 5 min

Online

Źródło polityki: polityka globalna

Aktualne

OSTATNIE INVENTORY SOFTWARE

30.09.2026, 13:29

przed chwilą

Polityka: aktualne do 24h, nieaktualne po 2 dni

Zgodne z polityką

Źródło polityki: polityka globalna

Aktualne

LOKALNI ADMINISTRATORZY

30.09.2026, 13:29

przed chwilą

Polityka: aktualne do 24h, nieaktualne po 3 dni

Zgodne z polityką

Źródło polityki: polityka globalna

Aktualne

INVENTORY SPRZĘTOWE

30.09.2026, 13:29

przed chwilą

Polityka: aktualne do 2 dni, nieaktualne po 4 dni

Zgodne z polityką

Źródło polityki: polityka globalna

Odśwież inventory

Inventory

Hardware

Software

Lokalni administratorzy

Zdarzenia

Auditlog

Właściciel

Wstecz

Komputer

HOSTNAME

LAPTOP-001

STATUS

Online

DEVICE ID

DEMO-ID-001

UŻYTKOWNIK

jan.kowalski

System

NAZWA OS

Windows 11 Pro

SYSTEM OPERACYJNY

windows

ADRES IP

192.0.2.10

WERSJA AGENTA

0.3.98.602

OSTATNIA AKTYWNOŚĆ

30.09.2026, 13:29

Sprzęt i system operacyjny

Identyfikacja komputera, systemu i wersji agenta.

Procesor, pamięć RAM i dostępne sloty.

Dyski, pojemność i wykorzystanie woluminu.

Dane BIOS oraz identyfikatory sprzętowe w raporcie.

HardwareSoftware

Komputer

HOSTNAME

LAPTOP-001

FQDN

LAPTOP-001

DEVICE ID

DEMO-ID-001

NUMER SERYJNY

SERIAL-DEMO

ASSET TAG

—

TYP URZĄDZENIA

desktop

STATUS

Online

CPU / RAM

CPU

Intel(R) Xeon(R) CPU E5-1603 v3 @ 2.80GHz

RDZENIE / WĄTKI

4 / 4

PAMIĘĆ ŁĄCZNIE

32 GB

UŻYTE SLOTSY RAM

2

MODUŁ RAM 1

16 GB · 2133 MHz · Hynix

MODUŁ RAM 2

16 GB · 2133 MHz · Hynix

Lokalizacja / Sieć

System

NAZWA OS

Windows 11 Pro

SYSTEM OPERACYJNY

windows

WYDANIE

25H2

WERSJA OS

10.0.26200

BUILD OS

26200

UBR

9457

ARCHITEKTURA

64-bitowy

OSTATNI START

—

WERSJA AGENTA

0.3.98.602

Dyski i wolumeny

DYSK 1

MTFDDAK256MBF-1AN1ZABHA · 238 GB · Fixed hard disk media

WOLUMEN C:

Zajęte: 130 GB · Wolne: 108 GB · 54.7%

GPU

Sieć, zabezpieczenia i urządzenia peryferyjne

Interfejsy sieciowe i dostępne adresy.

GPU, sterowniki i parametry obrazu.

Pola BIOS, Secure Boot, TPM i BitLocker.

Bateria, audio i monitor, jeśli agent zgłosił dane.

MODUŁ RAM 216 GB · 2133 MHz · Hynix

Lokalizacja / Sieć

ADRES IP192.0.2.10

GLÓWNY IPV4192.0.2.10

ADRES MAC—

Brak danych z ostatniego snapshotu.

BIOS / UEFI / Bezpieczeństwo

BIOSHewlett-Packard · M60 v02.50

SECURE BOOT—

TPMTak 1.2, 2, 3

BITLOCKER—

Monitory / Audio

MONITOR 1Generic PnP Monitor · —x—

MONITOR 2Generic PnP Monitor · —x—

MONITOR 3Monitor domylny · 1920x1080

AUDIO 1NVIDIA High Definition Audio · OK

AUDIO 2Realtek High Definition Audio · OK

AUDIO 3NVIDIA High Definition Audio · OK

GPU

GPU 1NVIDIA Quadro K620 · 32.0.15.8142 · 1920x1200

GPU 2Microsoft Remote Display Adapter · 10.0.26100.9278 · 1920x1080

GPU 3NVIDIA Quadro K620 · 32.0.15.8142 · —

Bateria

STATUS BATERIIBateria obecna

POZIOM—

ELEVE ADMIN

Oprogramowanie na urządzeniu

Lista aplikacji z wersją, wydawcą i źródłem wykrycia.

Filtry obejmują aplikacje Store, składniki systemowe i biblioteki runtime.

Wyszukiwanie ułatwia znalezienie określonego produktu.

Raport uzupełnia historię wykonania instalatorów.

Inventory

Hardware

Software

Lokalni administratorzy

Zdarzenia

Auditlog

Właściciel

Wstecz

SOFTWARE

Inwentarz oprogramowania

Ostatnia aktualizacja: 30.09.2026, 13:29

APLIKACJE
19

MICROSOFT / STORE / APPX
0
bieżąca lista

RUNTIME / FRAMEWORKI
0
bieżąca lista

KOMPONENTY SYSTEMOWE
0
bieżąca lista

OSTATNI SKAN
30.09.2026, 13:29

Szukaj aplikacji, wydawcy, wersji lub źródła...

Zainstalowane aplikacje

Pokaż pakiety Microsoft Store/Appx

Pokaż runtime/frameworki

Pokaż komponenty systemowe

Pokaż ukryte wpisy

NAZWA	WERSJA	KATEGORIA	ŹRÓDŁO	PRZECHWYCONO
7-Zip 26.03 (x64) Igor Pavlov	26.03	Zainstalowane aplikacje	HKLM	30.09.2026, 13:29
Blackmagic RAW Common Components Blackmagic Design	6.0	Zainstalowane aplikacje	HKLM	30.09.2026, 13:29
DaVinci Resolve Blackmagic Design	21.1.00017	Zainstalowane aplikacje	HKLM	30.09.2026, 13:29
DaVinci Resolve Control Panels Blackmagic Design	2.3.5.0	Zainstalowane aplikacje	HKLM	30.09.2026, 13:29
Eleve Admin Agent - Contoso, Ltd Eleve Admin	0.3.98.602	Zainstalowane aplikacje	HKLM	30.09.2026, 13:29
Git The Git Development Community	2.54.0	Zainstalowane aplikacje	HKLM	30.09.2026, 13:29

Eksport raportu oprogramowania

Eksport obejmuje bieżącą stronę lub pełny raport CSV.

Dane można wykorzystać do dalszej analizy poza konsolą.

Źródła wykrycia pomagają ocenić zakres raportu.

Stan raportu należy czytać razem z informacją o jego aktualności.

Szukaj aplikacji, wydawcy, wersji lub źródła...

Zainstalowane aplikacje

Pokaż pakiety Microsoft Store/Appx

Pokaż runtime/frameworki

Pokaż komponenty systemowe

Pokaż ukryte wpisy

NAZWA	WERSJA	KATEGORIA	ŹRÓDŁO	PRZECHWYCONO
7-Zip 26.03 (x64) Igor Pavlov	26.03	Zainstalowane aplikacje	HKLM	30.09.2026, 13:29
Blackmagic RAW Common Components Blackmagic Design	6.0	Zainstalowane aplikacje	HKLM	30.09.2026, 13:29
DaVinci Resolve Blackmagic Design	21.1.00017	Zainstalowane aplikacje	HKLM	30.09.2026, 13:29
DaVinci Resolve Control Panels Blackmagic Design	2.3.5.0	Zainstalowane aplikacje	HKLM	30.09.2026, 13:29
Eleve Admin Agent - Contoso Eleve Admin	0.3.98.602	Zainstalowane aplikacje	HKLM	30.09.2026, 13:29
Git The Git Development Community	2.54.0	Zainstalowane aplikacje	HKLM	30.09.2026, 13:29
Google Chrome Google LLC	154.0.8037.59	Zainstalowane aplikacje	WOW6432	30.09.2026, 13:29
Intel(R) Chipset Device Software Intel(R) Corporation	10.1.2.86	Zainstalowane aplikacje	WOW6432	30.09.2026, 13:29

Pokazano 1–19 z 19

Rekordów na stronę 50

Poprzednia

Następna

Eksport bieżącej strony

Eksport całego CSV

Lokalni administratorzy Windows

Raport pokazuje członków lokalnej grupy administratorów.

Wiersze zawierają źródło danych i czas raportowania.

Wyszukiwanie i eksport CSV wspierają przegląd uprawnień.

Raport pomaga wykryć konta wymagające dalszej weryfikacji.

Lokalni administratorzy (2/2)

Ostatnia aktualizacja: 30.09.2026, 13:29

Konto	Typ	Źródło	Wykryto
Administrator LAPTOP-001	Użytkownik	Inventory	30.09.2026, 13:29
anna.nowak LAPTOP-001	Użytkownik	Inventory	30.09.2026, 13:29

Export CSV

Export CSV (API)

Zdarzenia agenta na urządzeniu

Zdarzenia obejmują aktualizacje, potwierdzenia poleceń i zakończenia sesji.

Filtry zawężają poziom, zakres dat i rezultat.

Eksport CSV ułatwia analizę diagnostyczną.

Przejsście do audytu pozwala sprawdzić kontekst zdarzenia.

Zdarzenia

Ostatnia aktualizacja: 30.09.2026, 13:28

Operacyjny timeline urządzenia: agent, połączenie, komendy, inventory, polityki i skrócone lifecycle zdarzenia.

Wszystkie

Alerty

Ostrzeżenia

Informacyjne

Od czasu

Do czasu

Wynik

Pokaż zdarzenia diagnostyczne

Zastosuj filtry

Eksport CSV

Czas	Kategoria	Zdarzenie	Wynik / status	Użytkownik	Źródło
30.09.2026, 13:28	Agent	Zdarzenie systemowe: Agent update succeeded <a>Otwórz w Auditlog	Completed	—	System
30.09.2026, 13:26	Agent	Zdarzenie systemowe: Agent update started <a>Otwórz w Auditlog	Install started	—	System
30.09.2026, 13:26	Agent	Zdarzenie systemowe: Agent update started <a>Otwórz w Auditlog	Download started	—	System
30.09.2026, 13:26	Agent	Zdarzenie systemowe: Agent update scheduled <a>Otwórz w Auditlog	Update available	—	System
30.09.2026, 13:26	Komendy	Polecenie urządzenia zostało wykonane <a>Otwórz w Auditlog	OK	—	System
30.09.2026, 13:26	Komendy	Agent potwierdził polecenie urządzenia	OK	—	System
30.09.2026, 13:07	Komendy	Polecenie urządzenia zostało wykonane <a>Otwórz w Auditlog	OK	—	System
30.09.2026, 13:07	Komendy	Agent potwierdził polecenie urządzenia	OK	—	System
30.09.2026, 13:03	Sesja administratora	Sesja wygasła i została cofnięta	—	LAPTOP-001 LAPTOP-001@jan.kowalski	System
30.09.2026, 12:54	Agent	Zdarzenie systemowe: Installer execution completed <a>Otwórz w Auditlog	Zatwierdzono	—	System

Audyt uruchomień aplikacji

Historia RunAs identyfikuje zgłoszenie i plik.

Lista rozdziela decyzję oraz rezultat wykonania.

Szczegóły prowadzą do czasu zgody i danych instalatora.

Wynik procesu trzeba interpretować zgodnie z typem instalatora.

Inventory

Hardware

Software

Lokalni administratorzy

Zdarzenia

Auditlog

Właściciel

Wstecz

Auditlog

Ostatnia aktualizacja: brak danych

RunAS

Sesje administratora

Powiązany wpis w Auditlog został podświetlony.

Pokazano 1–50

Rekordów na stronę50

Aplikacja	Użytkownik	Czas	Czas trwania	Aktywność	Status	Szczegóły
7-Zip 7z2603-x64.exe	jen.kowalski desktop.LAPTOP-001	30.09.2026, 12:52	—	installer execution completed Instalacja	Zakończone	Szczegóły
DaVinci_Resolve_21.1_Windows.exe	jen.kowalski LAPTOP-001	22.09.2026, 19:47	—	installer execution completed Instalacja	Zakończone	Szczegóły
DaVinci_Resolve_21.1_Windows.exe	jen.kowalski desktop.LAPTOP-001	21.09.2026, 22:24	Nie dotyczy	Klasyfikacja EXE zakończona Klasyfikacja	Sklasyfikowano	Szczegóły
DaVinci_Resolve_21.1_Windows.exe	jen.kowalski desktop.LAPTOP-001	20.09.2026, 20:49	Nie dotyczy	Klasyfikacja EXE zakończona Klasyfikacja	Sklasyfikowano	Szczegóły
ACDSee Free acdsee-free.exe	jen.kowalski desktop.LAPTOP-001	17.09.2026, 21:53	Nie dotyczy	Klasyfikacja EXE zakończona Klasyfikacja	Sklasyfikowano	Szczegóły
PDFCreator PDFCreator-6_3_1-Setup.exe	jen.kowalski LAPTOP-001	17.09.2026, 21:47	Nie dotyczy	Klasyfikacja EXE zakończona Klasyfikacja	Sklasyfikowano	Szczegóły
PDFCreator PDFCreator-6_3_1-Setup.exe	jen.kowalski desktop.LAPTOP-001	17.09.2026, 02:04	Nie dotyczy	Klasyfikacja EXE zakończona Klasyfikacja	Sklasyfikowano	Szczegóły

Historia sesji administratora

Podsumowanie łączy
uzasadnienie, decyzję i
osobę zatwierdzającą.

Widok podaje przyznany
czas oraz początek i
koniec sesji.

Przykład kończy się
statusem wygaśnięcia.

Zarejestrowany czas sesji
wynosi 14 minut 57
sekund.

Czasowe prawa administratora

Wygasa

× Zamknij szczegóły

LAPTOP-001

DEMO-ID-001

· 30.09.2026, 13:06

Zgłoszenie i użytkownik

KOMPUTER

DEMO-ID-001

UŻYTKOWNIK

LAPTOP-001

EMAIL

jan.kowalski@example.com

TELEFON

555010100

POWÓD

Na potrzeby testu aplikacji wymagającej prawa admina podczas jej konfiguracji

ŻĄDANY CZAS

15 min

Decyzja

STATUS

Wygasa

DECYZJĘ WYKONAŁ

Contoso admin@example.com

ZATWIERDZONY CZAS

15 min

KOMENTARZ

Zatwierdzono z Requests UI

CZAS DECYZJI

30.09.2026, 13:07

Sesja

CZAS PRYZNANIA

30.09.2026, 13:07

CZAS AKTYWACJI

30.09.2026, 13:07

CZAS ZAKOŃCZENIA

30.09.2026, 13:22

CZAS TRWANIA

14m 57s

STATUS

Wygasa

Cykl życia sesji i aktywność

Oś czasu pokazuje nadanie i zakończenie uprawnień.

Historia obejmuje ostrzeżenia i zdarzenia odebrania praw.

Wpisy agenta pomagają wyjaśnić przebieg zakończenia.

Rejestr aktywności stanowi osobny fragment szczegółów sesji.

Czasowe prawa administratora

Wygasła

× Zamknij szczegóły

LAPTOP-001

DEMO-ID-001

· 30.09.2026, 13:06

Sesja

CZAS PRZYZNANIA	30.09.2026, 13:07
CZAS AKTYWACJI	30.09.2026, 13:07
CZAS ZAKOŃCZENIA	30.09.2026, 13:22
CZAS TRWANIA	14m 57s
STATUS	Wygasła

Lifecycle bezpieczeństwa

ODLICZANIE DO WYGAŚNIĘCIA	30.09.2026, 13:17
WYLOGOWANIE PO WYGAŚNIĘCIU	30.09.2026, 13:22
SESJA WINDOWS	—
SESJA WYGASŁA PODCZAS WYŁĄCZENIA KOMPUTERA	30.09.2026, 13:22
PRAWA ODEBRANE PO URUCHOMIENIU AGENTA	30.09.2026, 13:22
WYLOGOWANIE POMINIĘTE: UŻYTKOWNIK NIE BYŁ ZAŁOGOWANY	—
WYKRYTO PRZERWĘ DZIAŁANIA AGENTA PODCZAS AKTYWNEJ SESJI	—
POWÓD	Odświeżenie tokenu Windows po zakończeniu praw administratora

Aktywność administracyjna

Zarejestrowana aktywność w sesji

Szczegóły pokazują wykryte procesy i skrypty.

Przykład zawiera uruchomienia cmd oraz skryptu.

Liczniki rozdzielają procesy podniesione i instalacje.

Raport opisuje zarejestrowaną aktywność w pokazanej sesji.

Czasowe prawa administratora

Wygasła

× Zamknij szczegóły

LAPTOP-001

DEMO-ID-001

· 30.09.2026, 13:06

Aktywność administracyjna

Program	Plik	Vendor	Wersja	Czas	Status
cmd.exe	C:\WINDOWS\system32\cmd.exe	—	—	30.09.2026, 13:08	ok

Polecenia i skrypty

Skrypt	Plik	Wiersz polecenia	Czas
cmd.exe	C:\actions-runner\run.cmd	C:\WINDOWS\system32\cmd.exe /c ""C:\actions-runner\run.cmd" "	30.09.2026, 13:08

Procesy z podniesionymi uprawnieniami

0 · Procesy z podniesionymi uprawnieniami

Zainstalowano

0

Odinstalowano

0

Zaktualizowane oprogramowanie

0

Zainstalowane aplikacje

Informacje o właścicielu urządzenia

Zakładka przeznaczona jest na informacje o właścicielu.

Dane zależą od raportowania agenta.

Pokazane urządzenie nie ma zgłoszonych danych właściciela.

Brak raportu pozostaje jawny w interfejsie.

Właściciel
Brak raportu z agenta.

Wiadomość do użytkownika komputera

Administrator otwiera formularz ikoną w Inventory.

Wskazuje odbiorcę, temat i treść.

Może ustawić priorytet oraz wymóg potwierdzenia.

Przykład: prośba o zwrot komputera zastępczego.

WIADOMOŚCI TENANTA

Pilne

Wyślij wiadomość

Każda wiadomość wymaga potwierdzenia odczytu przez użytkownika.

ODBIORCA

LAPTOP-001

jan.kowalski

Temat

Prosimy o zwrot zastępczego komputera

Treść

Minał termin wypożyczenia komputera zastępczego, w związku z czym prosimy o jego zwrot.

Priorytet

Pilne

POTWIERDZENIE ODCZYTU WYMAGANE

Każda wiadomość wymaga potwierdzenia odczytu przez użytkownika.

Wyślij

Anuluj

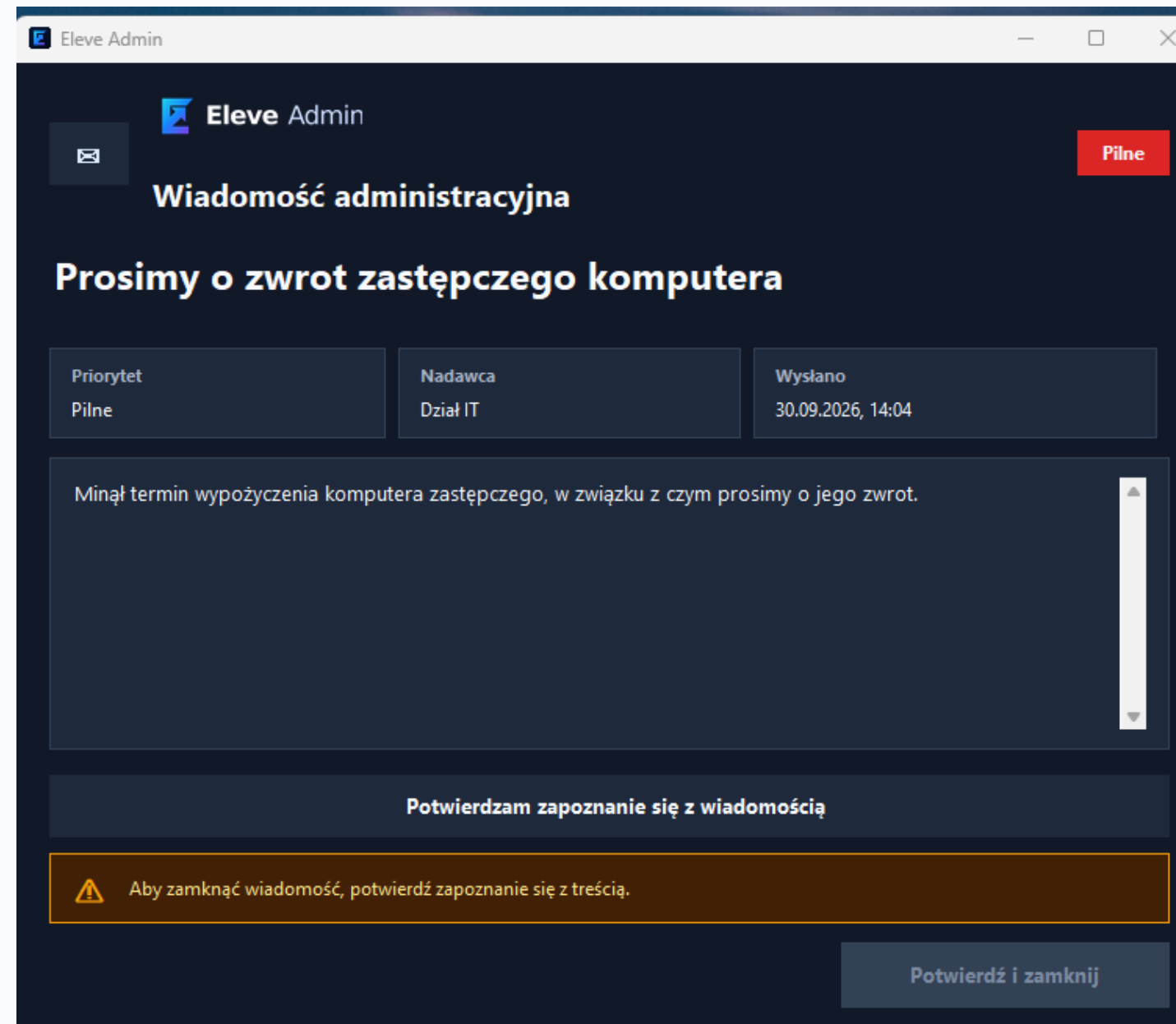
Komunikat na urządzeniu użytkownika

Agent wyświetla temat, treść i nadawcę.

Priorytet Pilne wyróżnia komunikat.

Wymagane potwierdzenie blokuje zamknięcie do czasu zaznaczenia pola.

Użytkownik potwierdza odbiór komunikatu.



The screenshot displays the 'Eleve Admin' web application interface. At the top, the title bar shows 'Eleve Admin' with standard window controls. The main header area includes the 'Eleve Admin' logo, a mail icon, and a red 'Pilne' (Urgent) status badge. Below the header, the message is titled 'Wiadomość administracyjna' (Administrative message) and 'Prosimy o zwrot zastępczego komputera' (We request the return of the replacement computer). A metadata section contains three boxes: 'Priorytet: Pilne' (Priority: Urgent), 'Nadawca: Dział IT' (Sender: IT Department), and 'Wysłano: 30.09.2026, 14:04' (Sent: 30.09.2026, 14:04). The main content area shows the message text: 'Minął termin wypożyczenia komputera zastępczego, w związku z czym prosimy o jego zwrot.' (The loan period for the replacement computer has expired, therefore we request its return). Below the text is a confirmation checkbox labeled 'Potwierdzam zapoznanie się z wiadomością' (I confirm I have read the message). At the bottom, a yellow warning box states: 'Aby zamknąć wiadomość, potwierdź zapoznanie się z treścią.' (To close the message, confirm you have read the content.). A 'Potwierdź i zamknij' (Confirm and close) button is located in the bottom right corner.

Potwierdzenie i historia dostarczenia

Oś czasu rozdziela utworzenie, wysłanie i wyświetlenie.

Końcowy wpis rejestruje potwierdzenie użytkownika.

Szczegóły wiążą wiadomość z urządzeniem i odbiorcą.

Administrator może sprawdzić przebieg dostarczenia.

Minął termin wypożyczenia komputera zastępczego, w związku z czym prosimy o jego zwrot.

Wiadomość została wygenerowana przez system i nie wymaga potwierdzenia.

KOMPUTER

LAPTOP-001

ODBIORCA

jan.kowalski
LAPTOP-001

WYŚŁAŁ

Contoso
admin@example.com

PRIORYTET

Pilne

POTWIERDZENIE ODCZYTU WYMAGANE

Każda wiadomość wymaga potwierdzenia odczytu przez użytkownika.

- Utworzono wiadomość30.09.2026, 14:04
Contoso
admin@example.com
- Wysłano do endpointu30.09.2026, 14:04
LAPTOP-001 · LAPTOP-001
- Wyświetlono użytkownikowi30.09.2026, 14:05
Okno powiadomienia zostało wyświetlone na endpointzie.
- Potwierdzono odczyt30.09.2026, 14:05
jan.kowalski
LAPTOP-001

Rejestr komunikacji z urządzeniami

Lista zbiera wiadomości i ich statusy.

Filtry obejmują daty, komputer, odbiorcę i priorytet.

Liczniki rozdzielają oczekujące, dostarczone, potwierdzone i błędy.

Historia ułatwia znalezienie komunikatu do konkretnego urządzenia.

WIADOMOŚCI TENANTA

Wiadomości

Przegląd wiadomości wysłanych do komputerów i aktywnych użytkowników wraz ze statusem dostarczenia i potwierdzenia.

Odśwież

28

Wszystkie wiadomości

1

Oczekujące lub dostarczone

27

Potwierdzony odczyt

0

Błędne

Data od

dd.mm.rrrr

Data do

dd.mm.rrrr

Komputer / device ID

Użytkownik docelowy

Status

Wszystkie

Priorytet

Wszystkie

Wysłane przez

Szukaj

Szukaj tematu, treści, urządzenia,

TEMAT	TREŚĆ	KOMPUTER	ODBIORCA	PRIORYTET	STATUS	WYŚLANO	POTWIERDZONO	SZCZEGÓŁY
test	test	LAPTOP-002	LAPTOP-001	Standard	Potwierdzono	28.09.2026, 20:05	28.09.2026, 20:06	
test	test	LAPTOP-002	LAPTOP-001	Standard	Potwierdzono	28.09.2026, 16:51	28.09.2026, 16:51	
Szanowny uzytkowni...	Zaraz otrzymasz zgode na instalacj...	LAPTOP-002	LAPTOP-001	Standard	Potwierdzono	18.09.2026, 14:28	18.09.2026, 14:31	
test	test	LAPTOP-001	LAPTOP-001	Pilne	Potwierdzono	17.09.2026, 02:17	17.09.2026, 16:31	
testy	1qa	LAPTOP-001	LAPTOP-001	Pilne	Potwierdzono	15.09.2026, 02:31	15.09.2026, 02:33	
test	test	LAPTOP-001	LAPTOP-001	Standard	Potwierdzono	14.09.2026, 11:12	14.09.2026, 11:13	

Zdalna blokada urządzenia

Administrator wybiera ikonę kłódki w Inventory.

Formularz zbiera powód blokady.

Można ustawić tytuł i treść komunikatu Windows.

Polecenie pozostaje powiązane z wybranym komputerem.

Potwierdź blokadę komputera

LAPTOP-001 · Online

Powód

Użytkownikowi wygasła umowa o pracę.

Tytuł komunikatu blokady

Komputer zablokowany

Treść komunikatu blokady

Twój komputer jest zablokowany. Skontaktuj się z działem wsparcia użytkownika.

Ten tekst zostanie pokazany na ekranie logowania Windows po zablokowaniu komputera.

Potwierdź blokadęAnuluj

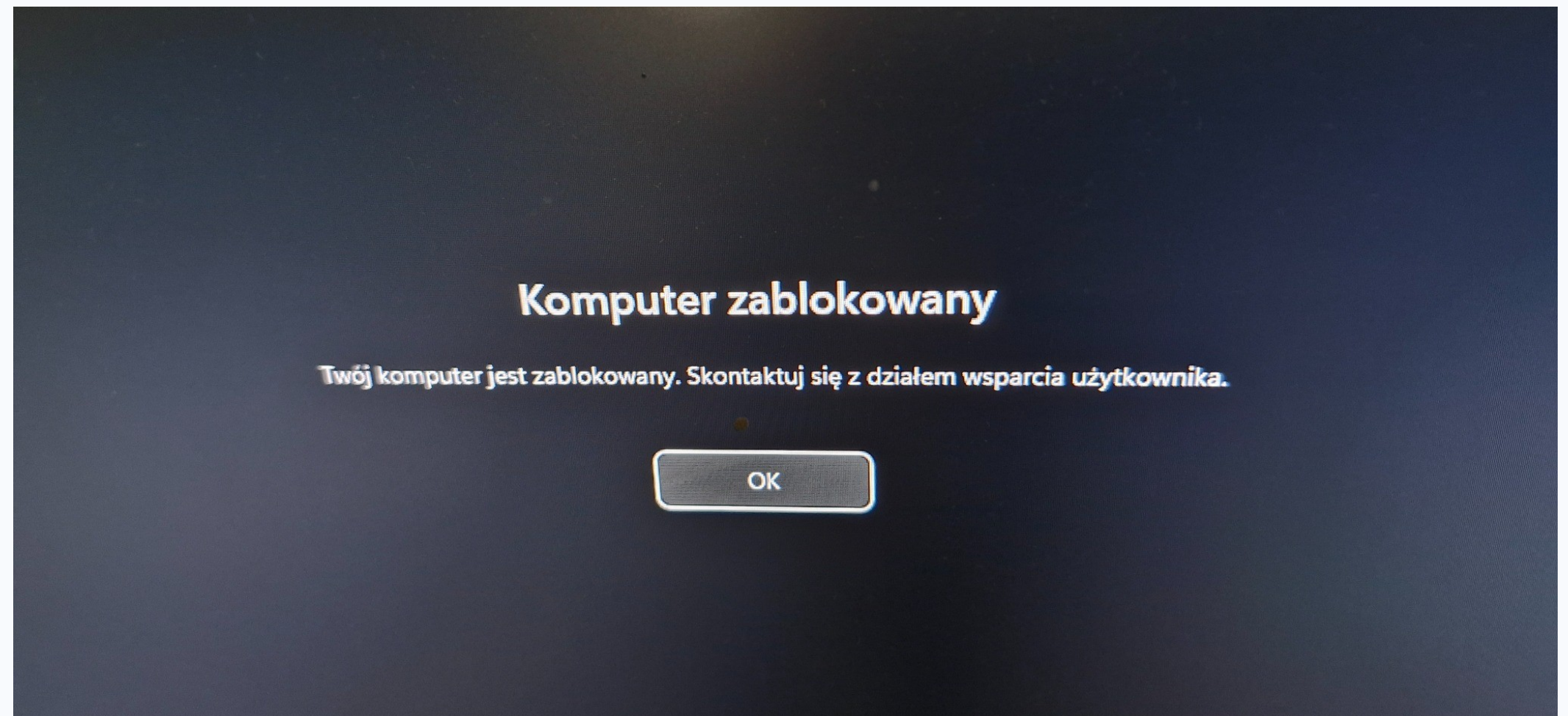
Efekt blokady w Windows

Zdjęcie pokazuje komunikat na zablokowanym komputerze.

Użytkownik otrzymuje informację o blokadzie i kontakcie z IT.

Treść wynika z konfiguracji administratora.

Potwierdzenie wykonania polecenia znajduje się w historii blokady.



Odblokowanie urządzenia

Ikona kłódki pozwala także wywołać odblokowanie.

Administrator podaje uzasadnienie przywrócenia dostępu.

Formularz pokazuje identyfikację i dostępność urządzenia.

Historia rozdziela zlecenie operacji od jej wykonania.

Potwierdź odblokowanie komputera

LAPTOP-001Niedostępne

Powód odblokowania

Komputer dopuszczony do pracy

Potwierdź odblokowanie

Anuluj

Potwierdzenia wykonania i historia

Oś czasu pokazuje
zlecenie, dostarczenie i
wykonanie blokady.

Odblokowanie ma własne
potwierdzenia.

Końcowy widok wskazuje
pomyślne odblokowanie.

Status oczekujący przed
potwierdzeniem opisuje
etap pośredni.

Cykl blokady

LAPTOP-001

POWÓD BLOKADY

Użytkownikowi wygasła umowa o pracę.

POWÓD ODBLOKOWANIA

Ważność konta została przedłużona

Timeline blokady

Zlecono blokadę 30.09.2026, 14:16

Dostarczono blokadę do agenta 30.09.2026, 14:21

Wykonano blokadę na komputerze 30.09.2026, 14:21

Zlecono odblokowanie 30.09.2026, 14:25
Powód odblokowania: Ważność konta została przedłużona

Dostarczono odblokowanie do agenta 30.09.2026, 14:25

Wykonano odblokowanie 30.09.2026, 14:25

Błąd operacji —

Wynik wykonania

KomunikatOdblokowany

Command IDba8c89e5-fdbb-4eac-b52e-06fdda58694c

Anuluj

Dziennik działań w organizacji

Kategorie obejmują bezpieczeństwo, administrację, urządzenia i agenta.

Wiersz podaje czas, obiekt, wykonawcę, wynik i źródło.

Filtry pomagają odnaleźć zdarzenia z określonego obszaru.

Eksport CSV obejmuje zdarzenia pasujące do filtrów.

Eleve Admin

Bezpieczeństwo konta

Podsumowanie

Requests

Inventory

Wiadomości

Blokady

Audyt

Użytkownicy

Pobieranie

Ustawienia

AUDYT

Contoso

admin@example.com

JĘZYK

Polski

Wyświetl

CENTRUM AUDYTU I BEZPIECZEŃSTWA

Eksportuj raport CSV

Odśwież

Dziennik audytu

Przegląd działań administratorów, zmian systemowych, zdarzeń bezpieczeństwa i aktywności komputerów.

Eksport obejmuje wszystkie rekordy zgodnie z aktywnymi filtrami.

Bezpieczeństwo

0

→ 0% vs 7 dni

Zdarzenia bezpieczeństwa

Zdarzenia admin

4

↓ 83% vs 7 dni

Operacje konsoli i tenanta

Zdarzenia urządzeń

16

↓ 33% vs 7 dni

Aktywność agentów i stacji

Agent

57

↓ 26% vs 7 dni

Aktualizacje i aktywność agenta

Tenant

7

↓ 67% vs 7 dni

Ustawienia i użytkownicy

Wszystkie

Bezpieczeństwo

Admin

Urządzenia

Agent

Tenant

Filtry

Szukaj: użytkownik, komputer, zdarzenie lub wynik...

CZAS	ZDARZENIE	OBIEKT	WYKONUJĄCY	WYNIK	ŹRÓDŁO	AKCJA
30.09.2026, 14:33	Zlecono odblokowanie komputera Administrator admin@example.com zlecił odblokowanie komputera D LAPTOP-001	LAPTOP-001	admin@example.com	Oczekuje	Blokady	Pokaż
30.09.2026, 14:30	Zablokowano urządzenie Komputer LAPTOP-001 został zablokowany.	LAPTOP-001	Agent endpointu	Wykonano	Blokady	Pokaż
30.09.2026, 14:30	Zlecono blokadę komputera Administrator admin@example.com zlecił blokadę komputera LAPTOP-001	LAPTOP-001	admin@example.com	Oczekuje	Blokady	Pokaż
30.09.2026, 14:25	Odblokowano urządzenie Komputer DELAPTOP-001 został odblokowany.	LAPTOP-001	Agent endpointu	Odblokowano	Blokady	Pokaż

Szczegóły zdarzenia i powiązane widoki

Panel szczegółów wyjaśnia kontekst zdarzenia.

Przykład dotyczy
potwierdzenia
odblokowania przez
agenta.

Dane obiektu identyfikują urządzenie.

Link prowadzi do historii w sekcji Blokad.

CENTRUM AUDYTU I BEZPIECZEŃSTWA

Eksport

Dziennik audytu

Przegląd działań administratorów, zmian systemowych, zdarzeń bezpieczeństwa i aktywności komputerów.

Eksport obejmuje wszystkie rekordy zgodne z aktywnymi filtrymi.

Bezpieczeństwo

0

→ 0% vs 7 dni

Zdarzenia bezpieczeństwa

Zdarzenia admin

4

↓ 83% vs 7 dni

Operacje konsoli i tenanta

Zdarzenia urządzeń

16

↓ 33% vs 7 dni

Aktywność agentów i stacji

Agent

57

↓ 26% vs 7 dni

Aktualizacje i aktywność agenta

Wszystkie

Bezpieczeństwo

Admin

Urządzenia

Agent

Tenant

Szukaj: użytkownik, komputer, zdarzenie lub wynik...

CZAS	ZDARZENIE	OBIEKT	WYKONUJĄCY	WYNIK	ŹRÓDŁO
30.09.2026, 14:33	Odblokowano urządzenie Komputer LAPTOP-001 został odblokowany.	LAPTOP-001	Agent endpointu	Odblokowano	Blokady
30.09.2026, 14:33	Zlecono odblokowanie komputera Administrator admin@example.com zlecił odblokowanie komputera LAPTOP-001	LAPTOP-001	admin@example.com	Oczekuje	Blokady
30.09.2026, 14:30	Zablokowano urządzenie Komputer LAPTOP-001 został zablokowany.	LAPTOP-001	Agent endpointu	Wykonano	Blokady

Szczegóły zdarzenia

X

Odblokowano urządzenie

Odblokowano

Komputer LAPTOP-001

M został odblokowany.

30.09.2026, 14:33

Najważniejsze informacje

Status Odblokowano

Aktor Agent endpointu

Komputer LAPTOP-001

Użytkownik / kontekst Nieznany użytkownik

Czas 30.09.2026, 14:33

Powiązane miejsce

Otwórz w Blokadach

Konta konsoli i przypisane role

Lista przedstawia konta, status i rolę.

Widok pokazuje ostatnie logowanie oraz stan MFA.

Filtry i wyszukiwanie wspierają przegląd dostępów.

Uprawnienia efektywne można sprawdzić dla konkretnej osoby.

TENANT RBAC

Użytkownicy

Zarządzaj kontami użytkowników i rolami najmniejszych uprawnień wyłącznie w bieżącym tenancie.

Użytkownicy

Role i uprawnienia

Zaproszenia

Aktywni

8

Nieaktywni

0

Właściciele

1

Oczekujące zaproszenia

0

Szukaj użytkowników...

Rola: *

Status: *

Zaproś użytkownika

UŻYTKOWNIK	ROLA	ZAKRES	STATUS	OSTATNIE LOGOWANIE	MFA	AKCJE
Operator 1 operator1@example.com	OPERATOR	Całkowicie	Aktywni	02.08.2026, 22:34	—	Efektywne uprawnienia
IT Admin admin@example.com	OWNER	Całkowicie	Aktywni	30.09.2026, 13:36	—	Efektywne uprawnienia
Operator 2 operator2@example.com	ROLA_TESTOWA	Całkowicie	Aktywni	06.08.2026, 01:16	—	Efektywne uprawnienia
Operator 3 operator3@example.com	OPERATOR	Całkowicie	Aktywni	03.08.2026, 21:39	—	Efektywne uprawnienia
Operator 4 operator4@example.com	OPERATOR	Całkowicie	Aktywni	03.08.2026, 21:51	—	Efektywne uprawnienia
Operator 5 operator5@example.com	OPERATOR	Całkowicie	Aktywni	22.08.2026, 01:30	—	Efektywne uprawnienia
Operator 6						

ELEVE ADMIN

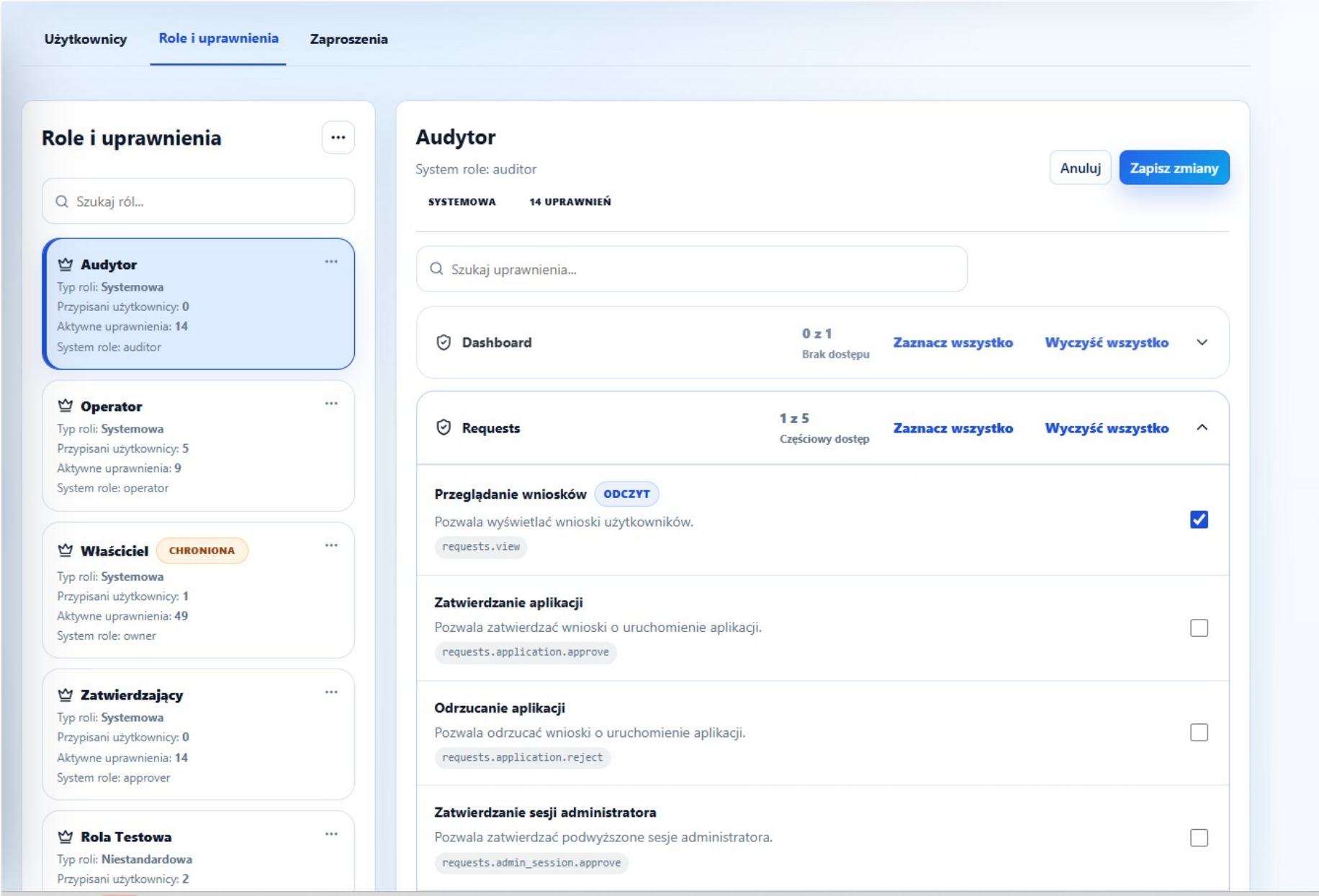
Role i szczegółowe uprawnienia

Role systemowe obejmują Owner, Operator, Approver i Auditor.

Role własne pozwalają dobrać zestaw uprawnień.

Uprawnienia rozdzielają odczyt, decyzje i wykonanie operacji.

Owner ma oznaczenie roli chronionej.



Tworzenie roli i zakres dostępu

Administrator określa nazwę, klucz i opis roli.

Może rozpocząć od pustej roli lub dostępnej bazy.

Uprawnienia poszczególnych modułów mają oddzielne ustawienia.

Konfiguracja pozwala przypisać obowiązki do zakresu dostępu.

ROLE I UPRAWNIENIA

×

Tworzenie roli

Nazwa roli

Klucz roli

Opis

Utwórz na podstawie

Pusta rola

▼

Anuluj

Utwórz

Uprawnienia efektywne i zabezpieczenia konta

Panel zestawia
uprawnienia roli, wyjątki i
wynik efektywny.

Podsumowanie pokazuje stan metod MFA i sesji.

Dostępne akcje obejmują reset MFA i unieważnienie metod.

Operacje administracyjne
zależą od uprawnień osoby
zarządzającej.

operator4@example.com

operator4@example.com

ROLA

operator

STATUS

Aktywni

OSTATNIE LOGOWANIE

—

MFA

—

WYJĄTKI UŻYTKOWNIKA

0

Bezpieczeństwo i logowanie

Stan MFA

MFA

nieaktywne

TOTP

missing

RECOVERY

0

PASSKEY

0

SECURITY KEYS

0

SESJE

0

Operacje administracyjne

Wymuś ponowną konfigurację TOTP

Unieważnij wszystkie passkey i klucze bezpieczeństwa

Unieważnij kody odzyskiwania

Resetuj wszystkie metody MFA

EDYCJA WYJĄTKÓW WŁĄCZONA

FILTRUJ PO MODULE

Wszystkie moduły

Q Szukaj użytkowników...

MODUŁ	UPRAWNIENIE	WARTOŚĆ Z ROLI	WYJĄTEK UŻYTKOWNIKA	WARTOŚĆ EFEKTÓW
Dashboard	Przeglądanie dashboardu dashboard.view	Zabronione	Dziedziczone z roli	Zabronione
Requests	Przeglądanie wniosków requests.view	Dozwolone	Dziedziczone z roli	Dozwolone
Requests	Zatwierdzanie aplikacji requests.application.approve	Zabronione	Dziedziczone z roli	Zabronione
Requests	Odrzucanie aplikacji	Zabronione	Dziedziczone z roli	Zabronione

Zapraszanie użytkownika do organizacji

Administrator wybiera rolę w filtrze listy użytkowników.

Następnie wybiera Zaproś użytkownika i podaje adres e-mail.

Wybrana w filtrze rola trafia do zaproszenia.

Historia zaproszeń pokazuje rolę, status i terminy.

The screenshot displays the 'Zaproszenia' (Invitations) section of the ELEVE ADMIN interface. At the top, there is a modal window for adding a new invitation, featuring an 'Email' input field and 'OK' and 'Anuluj' (Cancel) buttons. Below this, the 'Zaproszenia' section shows three filters: 'Nieaktywni' (Inactive) with a count of 0, 'Właściciele' (Owners) with a count of 1, and 'Oczekujące zaproszenia' (Pending invitations) with a count of 0. At the bottom, there is a search bar, a role filter set to 'auditor', a status filter set to 'Status: *', and a 'Zaproś użytkownika' (Invite user) button. Below these filters is a table with columns: 'ZAKRES' (Scope), 'STATUS' (Status), 'OSTATNIE LOGOWANIE' (Last login), 'MFA' (Multi-Factor Authentication), and 'AKCJE' (Actions).

Instalator agenta dla organizacji

Panel udostępnia pakiet MSI przypisany do tenanta.

Administrator może pobrać lub ponownie zbudować instalator.

Dostępna jest opcja unieważnienia wcześniejszych instalatorów.

Agent można wdrożyć administracyjnie lub przez Intune, Ivanti czy GPO.

POBIERANIE

Pobierz agenta

Pakiet MSI agenta jest dedykowany dla aktualnego tenanta.

POBIERANIE

Pobierz agenta

Pakiet MSI agenta jest dedykowany dla aktualnego tenanta.

Tenant Contoso **sp. z o.o**

PLATFORMA

Agent Windows

Instalator nie wygasa. Można go używać do kolejnych instalacji i reinstalacji, dopóki tenant pozostaje aktywny lub instalator nie zostanie ręcznie unieważniony.

⚙️ Przebuduj MSI ręcznie

⬇️ Pobierz MSI

🛑 Unieważnij dotychczasowe instalatory

Gotowy do pobrania

Instrukcja instalacji

- Wygeneruj agenta.
- Pobierz pakiet MSI.
- Uruchom go jako administrator albo wdróż przez Intune, Ivanti lub GPO.
- Po instalacji agent zarejestruje się w Twoim tenancie.

Bezpieczeństwo

Ten plik jest tenant-scoped. Sekrety i klucze API nigdy nie są pokazywane w UI i nie mogą być logowane w konsoli przeglądarki.

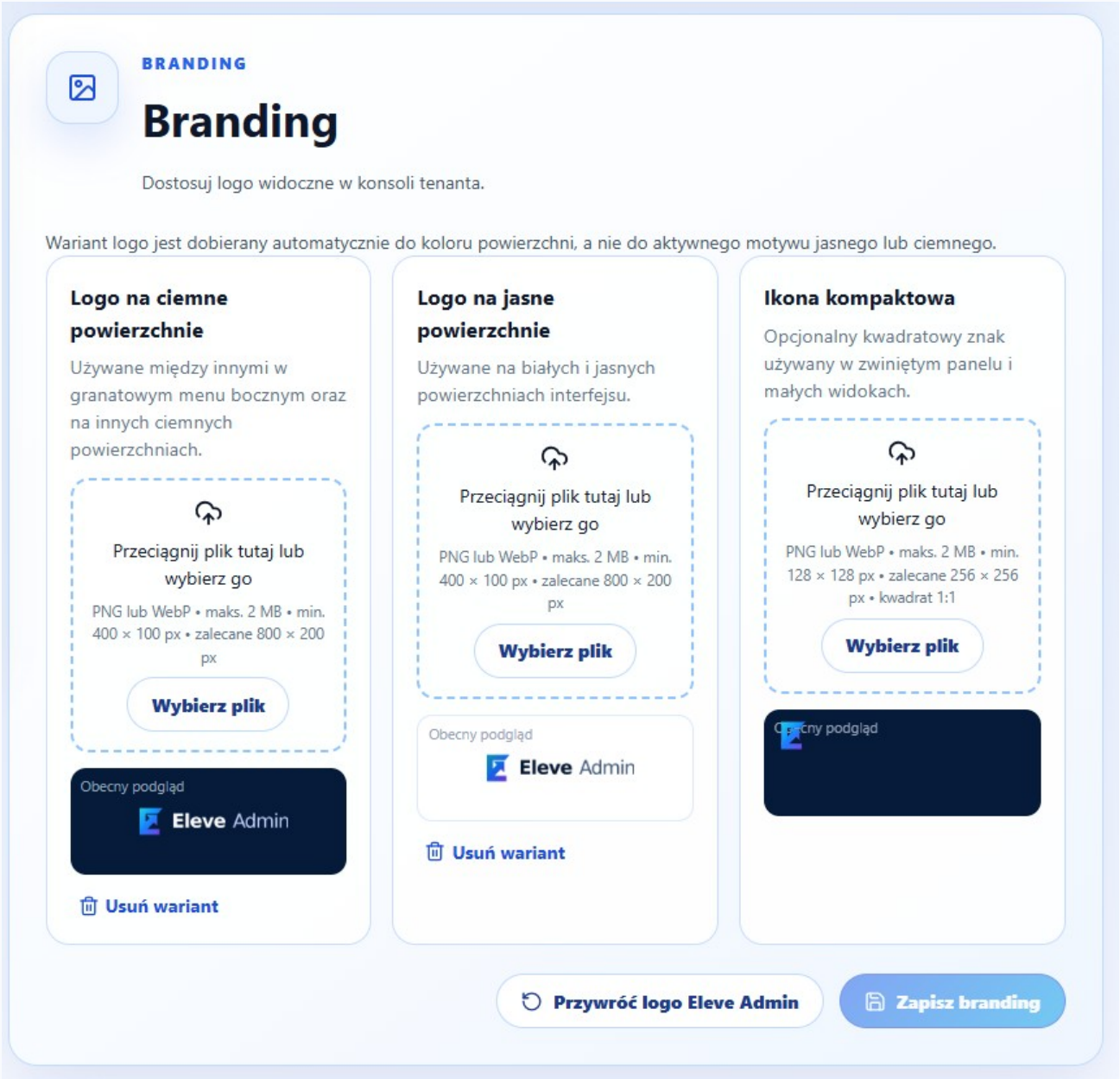
Wygląd konsoli i branding

Motyw jasny, ciemny lub systemowy dotyczy własnej sesji administratora.

Branding umożliwia ustawienie wariantów logo.

Panel pokazuje wymagane formaty i rozmiary.

Podgląd, usuwanie i przywrócenie logo pomagają zarządzać identyfikacją.



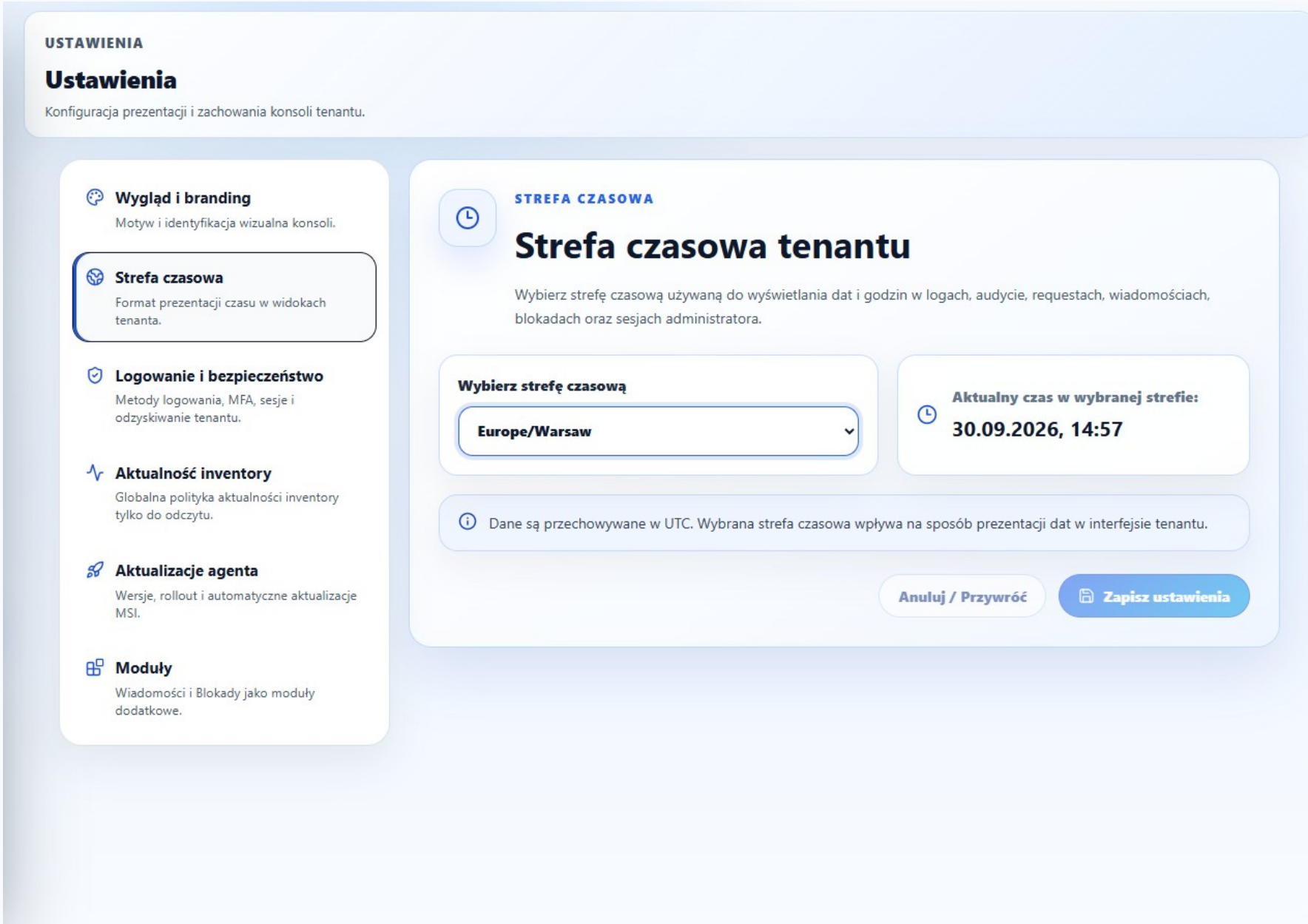
Strefa czasowa organizacji

Strefa czasowa określa prezentację dat w widokach tenanta.

Obejmuje logi, zgłoszenia, wiadomości, blokady i sesje.

Podgląd ułatwia sprawdzenie ustawienia.

Dane zachowują zapis UTC, a widoki stosują wybraną strefę.



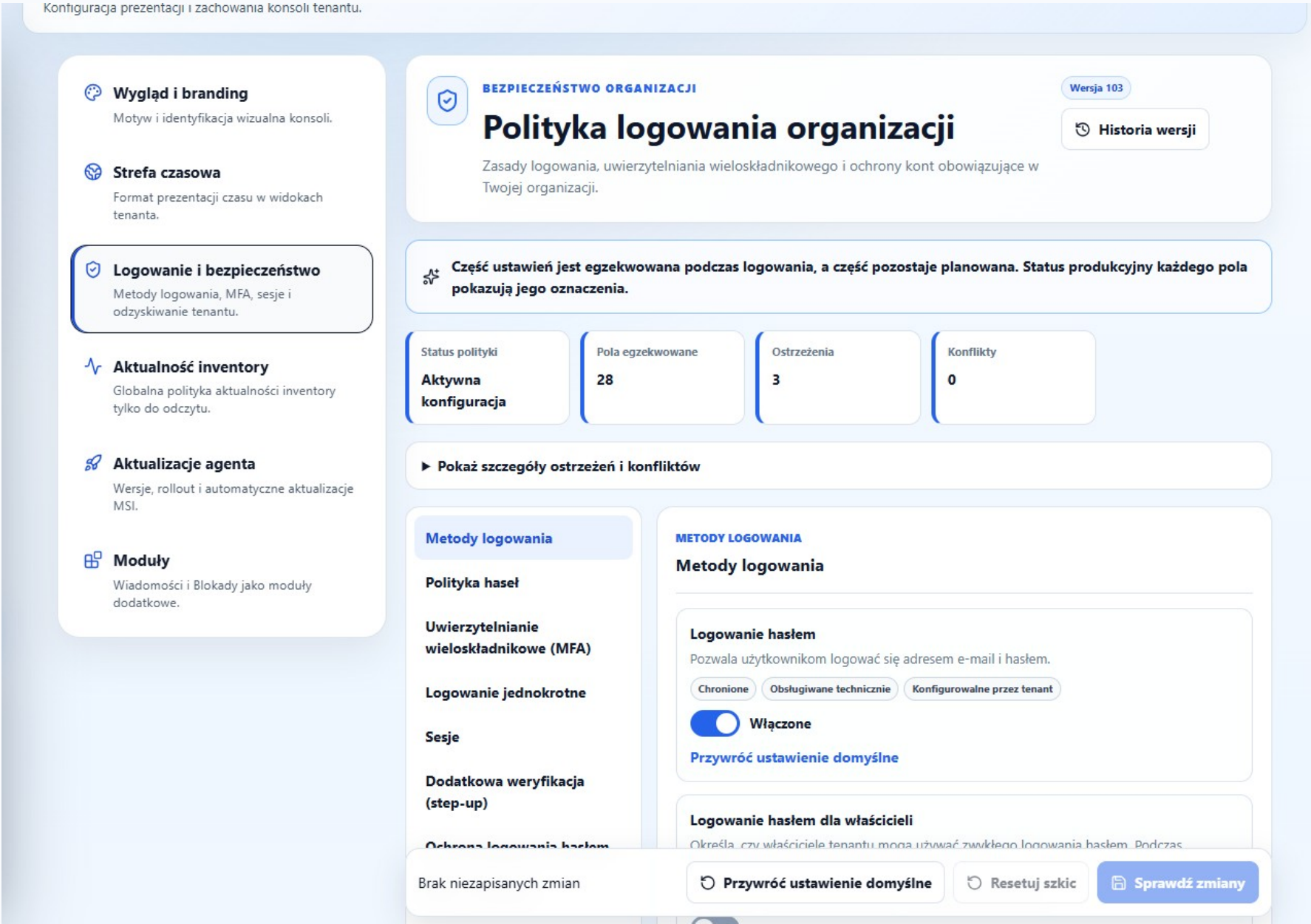
Konfiguracja i faktycznie egzekwowane zasady

Panel pokazuje aktywną wersję polityki i jej historię.

Podsumowanie rozdziela egzekwowane ustawienia, ostrzeżenia i konflikty.

Oznaczenia opisują zakres platformowy i tenantowy.

Funkcje planowane mają jawne etykiety dostępności.



Metody logowania i dostęp awaryjny

Panel określa dostępność logowania hasłem.

Ustawienia rozdzielają zwykłe konta i Ownera.

Kontrolowany dostęp awaryjny SSO ma warunki i ograniczony czas.

Automatyczny fallback lokalny ma oznaczenie funkcji planowanej.

Wygląd i branding

Motyw i identyfikacja wizualna konsoli.

Strefa czasowa

Format prezentacji czasu w widokach tenanta.

Logowanie i bezpieczeństwo

Metody logowania, MFA, sesje i odzyskiwanie tenanta.

Aktualność inventory

Globalna polityka aktualności inventory tylko do odczytu.

Aktualizacje agenta

Wersje, rollout i automatyczne aktualizacje MSI.

Moduły

Wiadomości i Blokady jako moduły dodatkowe.

Metody logowania

Polityka haseł

Uwierzytelnianie wieloskładnikowe (MFA)

Logowanie jednokrotne

Sesje

Dodatkowa weryfikacja (step-up)

Ochrona logowania hasłem

Sieć i lokalizacja

Odzyskiwanie dostępu

Alerty bezpieczeństwa

Logowanie hasłem

Pozwala użytkownikom logować się adresem e-mail i hasłem.

Chronione

Obsługiwane technicznie

Konfigurowalne przez tenant

Włączone

Przywróć ustawienie domyślne

Logowanie hasłem dla właścicieli

Określa, czy właściciele tenantu mogą używać zwykłego logowania hasłem. Podczas logowania sprawdzane jest aktualne członkostwo.

Chronione

Obsługiwane technicznie

Konfigurowalne przez tenant

Wyłączone

Przywróć ustawienie domyślne

Automatyczny fallback lokalny

Planowany automatyczny fallback na podstawie potwierdzonej awarii dostawcy tożsamości. Jest odrębny od kontrolowanego break-glass i nie jest aktywny.

Konfiguracja tenantowa — planowana

Wyłączone

Funkcja planowana.

Kontrolowany SSO break-glass

Pozwala wyłącznie Administratorowi Platformy, po krytycznym step-up, wystawić aktywnemu ownerowi jednorazowy grant na 15–60 minut. Nadal wymagane są istniejące hasło i MFA/WebAuthn; awaria IdP nie uruchamia automatycznego fallbacku.

Obsługiwane technicznie

Konfigurowalne przez tenant

Wyłączone

Przywróć ustawienie domyślne

Brak niezapisanych zmian

Przywróć ustawienie domyślne

Resetuj szkic

Sprawdź zmiany

ELEVE ADMIN

Wymagania dla haseł

Minimalna długość w przykładzie wynosi 13 znaków.

Historia obejmuje 5 poprzednich haseł.

Reguły dotyczą tworzenia, zmiany i resetu hasła.

Zmiana polityki nie zmienia automatycznie istniejących haseł.

Wygląd i branding

Motyw i identyfikacja wizualna konsoli.

Strefa czasowa

Format prezentacji czasu w widokach tenanta.

Logowanie i bezpieczeństwo

Metody logowania, MFA, sesje i odzyskiwanie tenantu.

Aktualność inventory

Globalna polityka aktualności inventory tylko do odczytu.

Aktualizacje agenta

Wersje, rollout i automatyczne aktualizacje MSI.

Moduły

Wiadomości i Blokada jako moduły dodatkowe.

Metody logowania

Polityka haseł

Uwierzytelnianie wieloskładnikowe (MFA)

Logowanie jednokrotne

Sesje

Dodatkowa weryfikacja (step-up)

Ochrona logowania hasłem

Sieć i lokalizacja

Odzyskiwanie dostępu

Alerty bezpieczeństwa

Pokaż szczegóły ostrzeżeń i konfliktów

POLITYKA HASEŁ

Polityka haseł

Minimalna długość hasła

Obowiązuje przy następnym utworzeniu, zmianie lub ресecie hasła. Istniejące hasła i sesje nie są automatycznie sprawdzane ani zmieniane.

Foundation

Obsługiwane technicznie

Konfigurowalne przez tenant

13

Minimum platformowe i techniczny zakres długości hasła · 12–1024

Minimum: 12 · Maksimum: 1024

Przywróć ustawienie domyślne

Historia haseł

Obowiązuje przy przyszłym tworzeniu, zmianie i resetowaniu hasła. Do 24 poprzednich haseł jest przechowywanych wyłącznie jako nieodwracalne hashe. Istniejące hasła nie są odczytywane ani unieważniane, a zmiana polityki nie kończy sesji.

Foundation

Obsługiwane technicznie

Konfigurowalne przez tenant

5

Minimum platformy i dozwolony zakres historii: 4–24. Zero wyłącza kontrolę historii, ale bieżące hasło nadal jest blokowane.

Minimum: 4 · Maksimum: 24

Przywróć ustawienie domyślne

Ważność hasła

0 oznacza brak wygasania haseł i jest ustawieniem zalecanym. Okresowe wygasanie jest opcjonalną kontrolą zgodności wyłącznie dla haseł lokalnych; NIST i Microsoft zalecają

Brak niezapisanych zmian

Przywróć ustawienie domyślne

Resetuj szkie

Sprawdź zmiany

ELEVE ADMIN

Ważność hasła i kontrola wycieków

W przykładzie hasło wygasa po 14 dniach.

Wartość 0 pozwala wyłączyć okresowe wygasanie zgodnie z ustawieniem.

Kontrolę haseł z wycieków egzekwuje platforma.

Kontrola dotyczy nowych haseł przy tworzeniu, zmianie lub resecie.

Wygląd i branding

Motyw i identyfikacja wizualna konsoli.

Strefa czasowa

Format prezentacji czasu w widokach tenanta.

Logowanie i bezpieczeństwo

Metody logowania, MFA, sesje i odzyskiwanie tenantu.

Aktualność inventory

Globalna polityka aktualności inventory tylko do odczytu.

Aktualizacje agenta

Wersje, rollout i automatyczne aktualizacje MSI.

Moduły

Wiadomości i Blokady jako moduły dodatkowe.

Metody logowania

Polityka haseł

Uwierzytelnianie wieloskładnikowe (MFA)

Logowanie jednokrotne

Sesje

Dodatkowa weryfikacja (step-up)

Ochrona logowania hasłem

Sieć i lokalizacja

Odzyskiwanie dostępu

Alerty bezpieczeństwa

5

Minimum platformy i dozwolony zakres historii: 4–24. Zero wyłącza kontrolę historii, ale bieżące hasło nadal jest blokowane.
Minimum: 4 · Maksimum: 24

Przywróć ustawienie domyślne

Ważność hasła

0 oznacza brak wygasania haseł i jest ustawieniem zalecanym. Okresowe wygasanie jest opcjonalną kontrolą zgodności wyłącznie dla haseł lokalnych; NIST i Microsoft zalecają zmianę przy podejrzeniu przejęcia zamiast według arbitralnego kalendarza. Zmiana polityki nie kończy istniejących sesji.

FoundationObsługiwane technicznieKonfigurowalne przez tenant

14

0 — hasło nie wygasa (zalecane); w innym przypadku 14–730 dni
Minimum: 0 · Maksimum: 730

Przywróć ustawienie domyślne

Kontrola przejętych haseł

Sprawdza przyszłe tworzenie, zmiany i resety haseł przez chroniące prywatność wyszukiwanie zakresowe z pięciodzianowym prefiksem. Istniejące hasła nie są analizowane ani unieważniane, a zmiana polityki nie kończy sesji.

FoundationObsługiwane technicznieKonfigurowalne przez tenant

Włączone

Wartość ustawiona przez tenant: Wyłączone
Wartość efektywna wymuszona przez platformę: Włączone
Zarządzane przez platformę

Przywróć ustawienie domyślne

Brak niezapisanych zmian

Przywróć ustawienie domyślne

Resetuj szkic

Sprawdź zmiany

ELEVE ADMIN

Wymaganie MFA i dozwolone metody

Organizacja może wymagać uwierzytelniania wieloskładnikowego.

Metody obejmują aplikację TOTP, kody odzyskiwania i WebAuthn.

Polityka określa zakres wymogu dla ról.

Weryfikacja MFA przez zewnętrznego dostawcę ma oznaczenie planowanej.

Wygląd i branding

Motyw i identyfikacja wizualna konsoli.

Strefa czasowa

Format prezentacji czasu w widokach tenanta.

Logowanie i bezpieczeństwo

Metody logowania, MFA, sesje i odzyskiwanie tenantu.

Aktualność inventory

Globalna polityka aktualności inventory tylko do odczytu.

Aktualizacje agenta

Wersje, rollout i automatyczne aktualizacje MSI.

Moduły

Wiadomości i Blokada jako moduły dodatkowe.

Metody logowania

Polityka haseł

Uwierzytelnianie wieloskładnikowe (MFA)

Logowanie jednokrotne

Sesje

Dodatkowa weryfikacja (step-up)

Ochrona logowania hasłem

Sieć i lokalizacja

Odzyskiwanie dostępu

Alerty bezpieczeństwa

UWIERZYTELNIANIE WIELOSKŁADNIKOWE (MFA)

Uwierzytelnianie wieloskładnikowe (MFA)

MFA dostępne

Określa, czy użytkownicy organizacji mogą korzystać z uwierzytelniania wieloskładnikowego.

Wymaga MFA

Obsługiwane technicznie

Konfigurowalne przez tenant

Włączone

Pole tylko do podglądu.

Wymagaj MFA

Określa, czy uwierzytelnianie wieloskładnikowe jest wymagane podczas logowania.

Wymaga MFA

Obsługiwane technicznie

Konfigurowalne przez tenant

Włączone

Przywróć ustawienie domyślne

Role wymagające MFA

Określa role użytkowników, dla których MFA jest obowiązkowe.

Wymaga MFA

Obsługiwane technicznie

Konfigurowalne przez tenant

Dodaj rolę... ▾

Dozwolone metody MFA

Określa metody uwierzytelniania, których użytkownicy mogą używać jako drugiego składnika.

Wymaga MFA

Obsługiwane technicznie

Konfigurowalne przez tenant

Obsługiwane: Aplikacja uwierzytelniająca TOTP, Kody odzyskiwania, Passkey, Klucz bezpieczeństwa WebAuthn

Planowane: MFA z zewnętrznego dostawcy tożsamości

Brak niezapisanych zmian

Przywróć ustawienie domyślne

Resetuj szkic

Sprawdź zmiany

ELEVE ADMIN

WebAuthn i warunki konfiguracji MFA

Polityka określa wymóg metody odpornej na phishing.

Widoczny okres przejściowy wynosi 168 godzin.

Reset MFA przez administratora ma osobne ustawienie.

Reset Ownera wymaga obsługi platformy według wskazanego procesu.

Wygląd i branding

Motyw i identyfikacja wizualna konsoli.

Strefa czasowa

Format prezentacji czasu w widokach tenanta.

Logowanie i bezpieczeństwo

Metody logowania, MFA, sesje i odzyskiwanie tenantu.

Aktualność inventory

Globalna polityka aktualności inventory tylko do odczytu.

Aktualizacje agenta

Wersje, rollout i automatyczne aktualizacje MSI.

Moduły

Wiadomości i Blokada jako moduły dodatkowe.

Metody logowania

Polityka haseł

Uwierzytelnianie wieloskładnikowe (MFA)

Logowanie jednokrotne

Sesje

Dodatkowa weryfikacja (step-up)

Ochrona logowania hasłem

Sieć i lokalizacja

Odzyskiwanie dostępu

Alerty bezpieczeństwa

Wymagaj MFA odpornego na phishing podczas logowania

Wymaga podczas logowania metody MFA odpornej na phishing. Obecnie wymaganie spełniają passkey i klucze bezpieczeństwa WebAuthn.

Wymaga MFA

Obsługiwane technicznie

Rejestracja dostępna

Logowanie dostępne

Konfigurowalne przez tenanta

Wyłączone

Przywróć ustawienie domyślne

Okres na konfigurację MFA

Określa czas, jaki użytkownik ma na skonfigurowanie MFA po pierwszym logowaniu lub po wymuszeniu ponownej konfiguracji.

Wymaga MFA

Obsługiwane technicznie

Konfigurowalne przez tenanta

168

hours

Administracyjny reset MFA użytkowników

Określa, czy uprawnieni administratorzy organizacji mogą resetować metody MFA innych użytkowników.

Wymaga MFA

Obsługiwane technicznie

Konfigurowalne przez tenanta

Włączone

Przywróć ustawienie domyślne

Reset MFA właściciela wymaga wsparcia platformy

Blokuje reset MFA właściciela organizacji przez administratorów tenanta. Na tym ekranie nie jest dostępny proces odzyskiwania wspomagany przez platformę.

Wymaga MFA

Obsługiwane technicznie

Pole tylko do podglądu.

Włączone

Zarządzane przez platformę

Brak niezapisanych zmian

Przywróć ustawienie domyślne

Resetuj szkic

Sprawdź zmiany

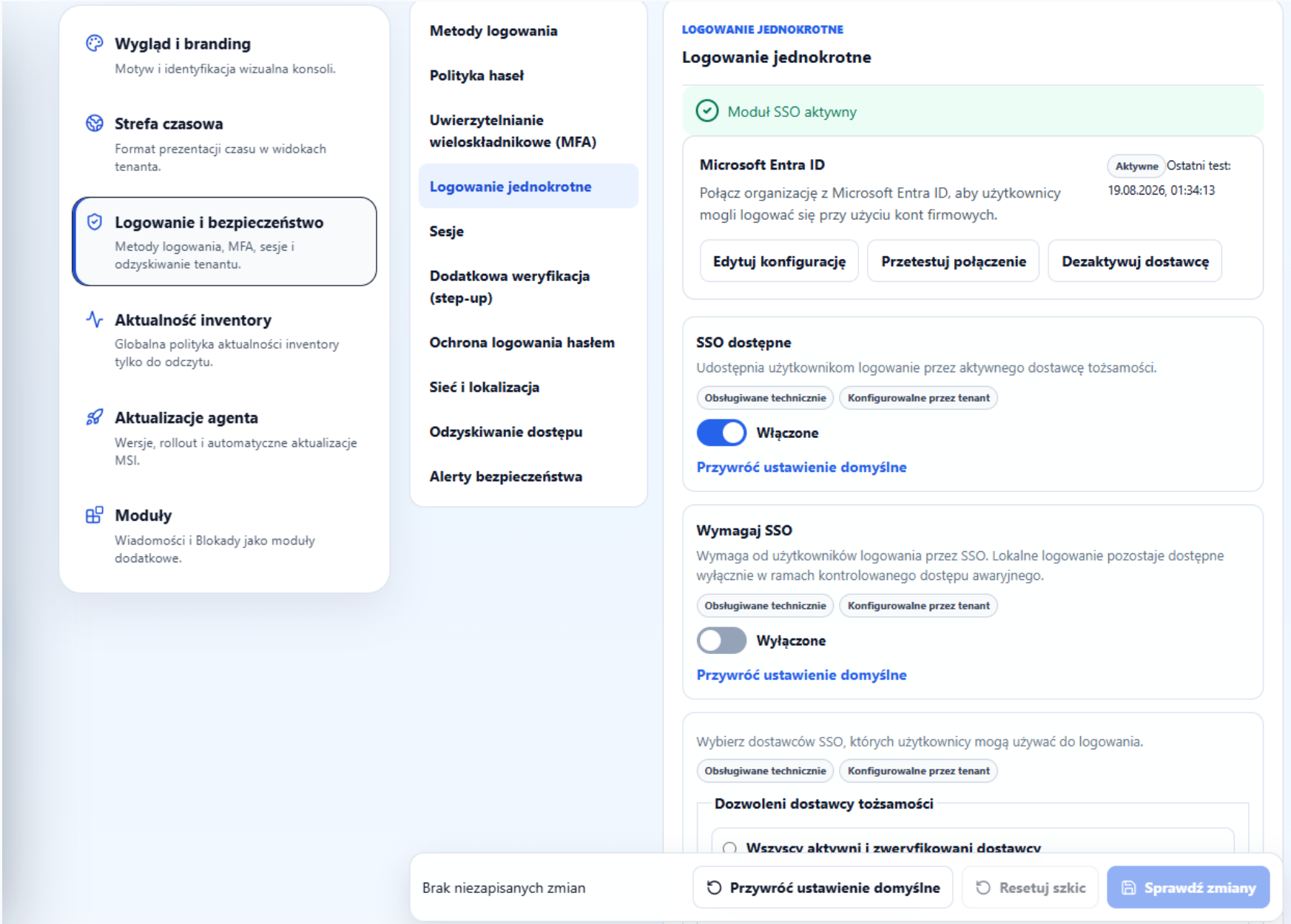
SSO z Microsoft Entra ID

Panel wskazuje aktywny moduł SSO i dostawcę.

Konfiguracja udostępnia edycję, test i dezaktywację.

Dostępność SSO i wymóg logowania przez SSO są odrębne ustawienia.

W przykładzie SSO jest dostępne, a obowiązkowe SSO pozostaje wyłączone.



Dostawca SSO i okres przejściowy

Organizacja może wskazać dozwolonego dostawcę.

Widok pokazuje stan aktywności i weryfikacji konfiguracji.

Okres przejściowy reguluje czas dostosowania.

W przykładzie okres przejściowy wynosi 1 godzinę.

Wygląd i branding

Motyw i identyfikacja wizualna konsoli.

Strefa czasowa

Format prezentacji czasu w widokach tenanta.

Logowanie i bezpieczeństwo

Metody logowania, MFA, sesje i odzyskiwanie tenantu.

Aktualność inventory

Globalna polityka aktualności inventory tylko do odczytu.

Aktualizacje agenta

Wersje, rollout i automatyczne aktualizacje MSI.

Moduły

Wiadomości i Blokada jako moduły dodatkowe.

Metody logowania

Polityka haseł

Uwierzytelnianie wieloskładnikowe (MFA)

Logowanie jednokrotne

Sesje

Dodatkowa weryfikacja (step-up)

Ochrona logowania hasłem

Sieć i lokalizacja

Odzyskiwanie dostępu

Alerty bezpieczeństwa

Wymagaj SSO

Wymaga od użytkowników logowania przez SSO. Lokalne logowanie pozostaje dostępne wyłącznie w ramach kontrolowanego dostępu awaryjnego.

Obsługiwane technicznie

Konfigurowalne przez tenant

Wyłączone

Przywróć ustawienie domyślne

Wybierz dostawców SSO, których użytkownicy mogą używać do logowania.

Obsługiwane technicznie

Konfigurowalne przez tenant

Dozwoleni dostawcy tożsamości

Wszyscy aktywni i zweryfikowani dostawcy

Tylko wybrani dostawcy

Microsoft Entra ID - Staging

Microsoft Entra ID · Aktywny · Zweryfikowany

Przywróć ustawienie domyślne

Okres przejściowy SSO

Określa, jak długo po włączeniu wymogu SSO użytkownicy mogą jeszcze korzystać z dotychczasowego logowania.

Obsługiwane technicznie

Konfigurowalne przez tenant

1

Lokalne logowanie pozostanie dostępne przez 1 godzin od włączenia wymogu SSO.

Minimum: 0 · Maksimum: 720

Przywróć ustawienie domyślne

Brak niezapisanych zmian

Przywróć ustawienie domyślne

Resetuj szkic

Sprawdź zmiany

Limity czasu sesji konsoli

Bezczynność i maksymalna długość sesji mają osobne limity.

Aktywność może przedłużyć limit beczynności.

Aktywność nie znosi maksymalnego czasu sesji.

Efektywny limit beczynności wynosi 30 minut przy żądanych 45.

Wygląd i branding

Motyw i identyfikacja wizualna konsoli.

Strefa czasowa

Format prezentacji czasu w widokach tenanta.

Logowanie i bezpieczeństwo

Metody logowania, MFA, sesje i odzyskiwanie tenantu.

Aktualność inventory

Globalna polityka aktualności inventory tylko do odczytu.

Aktualizacje agenta

Wersje, rollout i automatyczne aktualizacje MSI.

Moduły

Wiadomości i Blokadę jako moduły dodatkowe.

Metody logowania

Polityka haseł

Uwierzytelnianie wieloskładnikowe (MFA)

Logowanie jednokrotne

Sesje

Dodatkowa weryfikacja (step-up)

Ochrona logowania hasłem

Sieć i lokalizacja

Odzyskiwanie dostępu

Alerty bezpieczeństwa

SESJE

Sesje

Limit beczynności sesji

Wylogowuje zwykłych użytkowników po tym czasie bez rzeczywistej interakcji. Aktywność przesuwa tylko termin beczynności; termin maksymalny nigdy się nie przesuwa. Zmiana dotyczy nowych sesji.

Wymaga sesji

Obsługiwane technicznie

Konfigurowalne przez tenant

30

minut

Wartość ustawiona przez tenant: 45

Wartość efektywna wymuszona przez platformę: 30

Minimum: 1 · Maksimum: 60

Przywróć ustawienie domyślne

Maksymalny czas sesji

Określa, po ilu minutach użytkownik musi zalogować się ponownie, niezależnie od aktywności.

Wymaga sesji

Obsługiwane technicznie

Konfigurowalne przez tenant

60

minut

Minimum: 1 · Maksimum: 60

Przywróć ustawienie domyślne

Bezczynność sesji uprzywilejowanej

Wylogowuje właścicieli tenantu po tym czasie bez rzeczywistej interakcji. Aktywność ownera przesuwa tylko termin beczynności; termin maksymalny nigdy się nie przesuwa. Zmiana dotyczy nowych sesji.

Wymaga sesji

Obsługiwane technicznie

Konfigurowalne przez tenant

Brak niezapisanych zmian

Przywróć ustawienie domyślne

Resetuj szkic

Sprawdź zmiany

Sesje uprzywilejowane i równoległe logowania

Owner ma odrębny limit bezczynności.

Efektywny limit wynosi 15 minut przy żądanych 40.

Maksymalna długość wynosi 60 minut.

Limit 2 równoległych sesji kończy najstarszą przy kolejnym logowaniu.

Wygląd i branding

Motyw i identyfikacja wizualna konsoli.

Strefa czasowa

Format prezentacji czasu w widokach tenanta.

Logowanie i bezpieczeństwo

Metody logowania, MFA, sesje i odzyskiwanie tenantu.

Aktualność inventory

Globalna polityka aktualności inventory tylko do odczytu.

Aktualizacje agenta

Wersje, rollout i automatyczne aktualizacje MSI.

Moduły

Wiadomości i Blokada jako moduły dodatkowe.

Metody logowania

Polityka haseł

Uwierzytelnianie wieloskładnikowe (MFA)

Logowanie jednokrotne

Sesje

Dodatkowa weryfikacja (step-up)

Ochrona logowania hasłem

Sieć i lokalizacja

Odzyskiwanie dostępu

Alerty bezpieczeństwa

Bezczynność sesji uprzywilejowanej

Wylogowuje właścicieli tenantu po tym czasie bez rzeczywistej interakcji. Aktywność ownera przesuwana tylko termin bezczynności; termin maksymalny nigdy się nie przesuwana. Zmiana dotyczy nowych sesji.

Wymaga sesji

Obsługiwane technicznie

Konfigurowalne przez tenant

15

minut

Wartość ustawiona przez tenanta: 40

Wartość efektywna wymuszona przez platformę: 15

Minimum: 1 · Maksimum: 60

Przywróć ustawienie domyślne

Maksymalna sesja uprzywilejowana

Określa krótszy maksymalny czas sesji właścicieli tenantu. Nie może być dłuższy niż zwykła sesja.

Wymaga sesji

Obsługiwane technicznie

Konfigurowalne przez tenant

60

minut

Minimum: 1 · Maksimum: 60

Przywróć ustawienie domyślne

Maksymalna liczba sesji

Limit aktywnych sesji jednego użytkownika w tej organizacji. Nowe logowanie kończy najstarszą aktywną sesję. Zmiana obowiązuje przy kolejnych logowaniach.

Wymaga sesji

Obsługiwane technicznie

Konfigurowalne przez tenant

2

Aktywne sesje użytkownika w tej organizacji

Własny limit organizacji. Przywrócenie ustawienia domyślnego ponownie włączy dziedziczenie wartości platformowej.

Brak niezapisanych zmian

Przywróć ustawienie domyślne

Resetuj szkielet

Sprawdź zmiany

Unieważnianie sesji po zmianach konta

Zmiana hasła może zakończyć sesje użytkownika.

Zmiana roli i polityki mają własne ustawienia.

Przejdźcie do lub z roli Owner wymusza zakończenie sesji.

Część zmian polityki jest wykrywana przy kolejnym użyciu sesji.

Wygląd i branding

Motyw i identyfikacja wizualna konsoli.

Strefa czasowa

Format prezentacji czasu w widokach tenanta.

Logowanie i bezpieczeństwo

Metody logowania, MFA, sesje i odzyskiwanie tenantu.

Aktualność inventory

Globalna polityka aktualności inventory tylko do odczytu.

Aktualizacje agenta

Wersje, rollout i automatyczne aktualizacje MSI.

Moduły

Wiadomości i Blokada jako moduły dodatkowe.

Metody logowania

Polityka haseł

Uwierzytelnianie wieloskładnikowe (MFA)

Logowanie jednokrotne

Sesje

Dodatkowa weryfikacja (step-up)

Ochrona logowania hasłem

Sieć i lokalizacja

Odzyskiwanie dostępu

Alerty bezpieczeństwa

Wymaga sesji

Obsługiwane technicznie

Konfigurowalne przez tenant

2

Aktywne sesje użytkownika w tej organizacji

Własny limit organizacji. Przywrócenie ustawienia domyślnego ponownie włączy dziedziczenie wartości platformowej.

Przywróć ustawienie domyślne

Wymaga sesji

Obsługiwane technicznie

Konfigurowalne przez tenant

Włączone

Wyloguj po zmianie hasła

Kończy wszystkie aktywne sesje użytkownika po zmianie lub zresetowaniu jego hasła. Użytkownik musi zalogować się ponownie.

Przywróć ustawienie domyślne

Wymaga sesji

Obsługiwane technicznie

Konfigurowalne przez tenant

Wyłączone

Wyloguj po zmianie roli

Kończy aktywne sesje użytkownika po zmianie jego roli w organizacji. Zmiana między rolą zwykłą a właścicielem zawsze kończy sesje ze względów bezpieczeństwa.

Przywróć ustawienie domyślne

Wymaga sesji

Obsługiwane technicznie

Konfigurowalne przez tenant

Wyłączone

Wyloguj po zmianie polityki logowania

Kończy sesje utworzone na podstawie wcześniejszej polityki logowania. Zmiana jest wykrywana przy następnym użyciu sesji.

Przywróć ustawienie domyślne

Brak niezapisanych zmian

Przywróć ustawienie domyślne

Resetuj szkic

Sprawdź zmiany

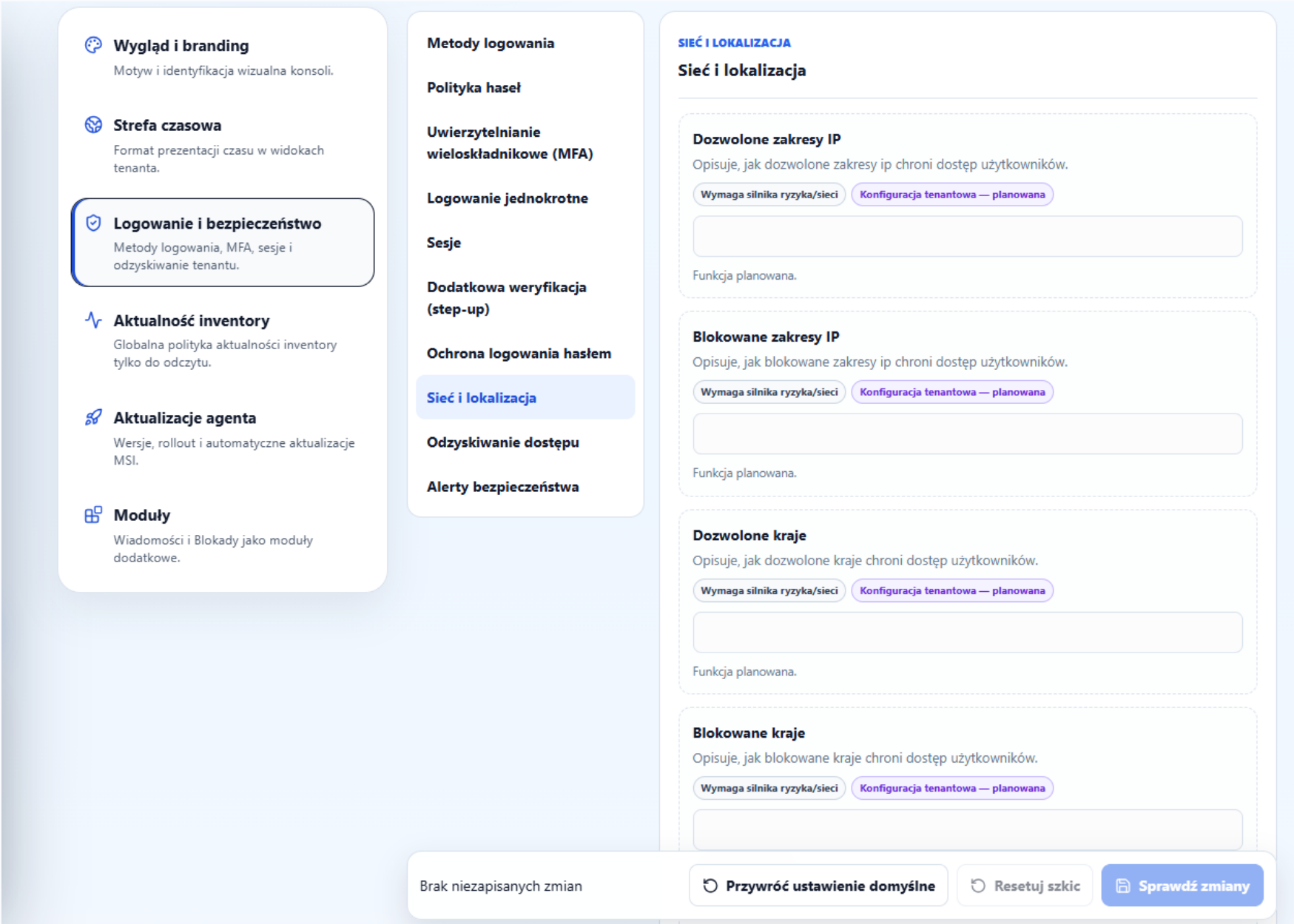
Planowane reguły sieci i lokalizacji

Widok przewiduje listy
dozwolonych i
blokowanych adresów IP.

Osobne reguły dotyczą
krajów.

Wszystkie pokazane
ustawienia mają
oznaczenie planowanej
konfiguracji tenantowej.

Screen prezentuje
kierunek rozwoju polityki
dostępu.



Funkcje oznaczone jako planowane

Planowane zasady odzyskiwania dostępu

Konfiguracja obejmuje wymaganie i liczbę kodów odzyskiwania.

Przewiduje wymaganie kont awaryjnych oraz ich minimalną liczbę.

Te ustawienia tenantowe mają oznaczenie planowanych.

Bieżące kody odzyskiwania MFA działają w sekcji Bezpieczeństwo konta.

Metody logowania

Polityka haseł

Uwierzytelnianie wieloskładnikowe (MFA)

Logowanie jednokrotne

Sesje

Dodatkowa weryfikacja (step-up)

Ochrona logowania hasłem

Sieć i lokalizacja

Odzyskiwanie dostępu

Alerty bezpieczeństwa

Wymagaj kodów odzyskiwania

Opisuje, jak wymagaj kodów odzyskiwania chroni dostęp użytkowników.

Wymaga MFA

Konfiguracja tenantowa — planowana

Wyłączone

Funkcja planowana.

Liczba kodów odzyskiwania

Opisuje, jak liczba kodów odzyskiwania chroni dostęp użytkowników.

Wymaga MFA

Konfiguracja tenantowa — planowana

10

Funkcja planowana.

Wymagaj kont awaryjnych

Opisuje, jak wymagaj kont awaryjnych chroni dostęp użytkowników.

Niejednoznaczne — wyłączone

Konfiguracja tenantowa — planowana

Wyłączone

Funkcja planowana.

Minimalna liczba kont awaryjnych

Opisuje, jak minimalna liczba kont awaryjnych chroni dostęp użytkowników.

Tylko powiadomienia

Konfiguracja tenantowa — planowana

1

Funkcja planowana.

Brak niezapisanych zmian

Przywróć ustawienie domyślne

Resetuj szkielet

Sprawdź zmiany

ELEVE ADMIN

Planowane alerty bezpieczeństwa

Ustawienia obejmują nowe urządzenie i reset MFA.

Przewidują powiadomienia o zmianie polityki i dostępie awaryjnym.

Wartości Włączone występują przy oznaczeniu funkcji planowanej.

Nie traktujemy tych wartości jako dowodu wysyłania alertów.

Metody logowania

Polityka haseł

Uwierzytelnianie wieloskładnikowe (MFA)

Logowanie jednokrotne

Sesje

Dodatkowa weryfikacja (step-up)

Ochrona logowania hasłem

Sieć i lokalizacja

Odzyskiwanie dostępu

Alerty bezpieczeństwa

Powiadamiał o nowym urządzeniu

Opisuje, jak powiadamiał o nowym urządzeniu chroni dostęp użytkowników.

Niejednoznaczne — wyłączone

Konfiguracja tenantowa — planowana

Włączone

Funkcja planowana.

Powiadamiał o resecie MFA

Opisuje, jak powiadamiał o resecie mfa chroni dostęp użytkowników.

Tylko powiadomienia

Konfiguracja tenantowa — planowana

Włączone

Funkcja planowana.

Powiadamiał o zmianie polityki

Opisuje, jak powiadamiał o zmianie polityki chroni dostęp użytkowników.

Tylko powiadomienia

Konfiguracja tenantowa — planowana

Włączone

Funkcja planowana.

Powiadamiał o dostępie awaryjnym

Opisuje, jak powiadamiał o dostępie awaryjnym chroni dostęp użytkowników.

Tylko powiadomienia

Konfiguracja tenantowa — planowana

Włączone

Funkcja planowana.

Brak niezapisanych zmian

Przywróć ustawienie domyślne

Resetuj szkic

Sprawdź zmiany

Konfiguracja widoczna, funkcje oznaczone jako planowane

ELEVE ADMIN

Historia wersji polityki

Lista przedstawia numer i datę zapisanej wersji.

Przy każdej wersji widoczna jest opcja przywrócenia.

Historia pomaga odnaleźć poprzednią konfigurację.

Screen dokumentuje dostępność akcji, bez demonstracji jej wykonania.

Historia wersji		
🕒	Wersja 103 7.09.2026, 22:59:06	Przywróć tę wersję
🕒	Wersja 102 6.09.2026, 04:14:46	Przywróć tę wersję
🕒	Wersja 101 31.08.2026, 01:58:46	Przywróć tę wersję
🕒	Wersja 100 30.08.2026, 22:06:09	Przywróć tę wersję
🕒	Wersja 99 30.08.2026, 03:45:07	Przywróć tę wersję
🕒	Wersja 98 30.08.2026, 03:43:12	Przywróć tę wersję
🕒	Wersja 97 30.08.2026, 03:42:11	Przywróć tę wersję
🕒	Wersja 96 28.08.2026, 02:00:11	Przywróć tę wersję
🕒	Wersja 95 23.08.2026, 22:59:15	Przywróć tę wersję
🕒	Wersja 94 23.08.2026, 22:56:50	Przywróć tę wersję
🕒	Wersja 93 23.08.2026, 22:17:18	Przywróć tę wersję
🕒	Wersja 92 23.08.2026, 22:16:16	Przywróć tę wersję
🕒	Wersja 91 23.08.2026, 02:51:42	Przywróć tę wersję

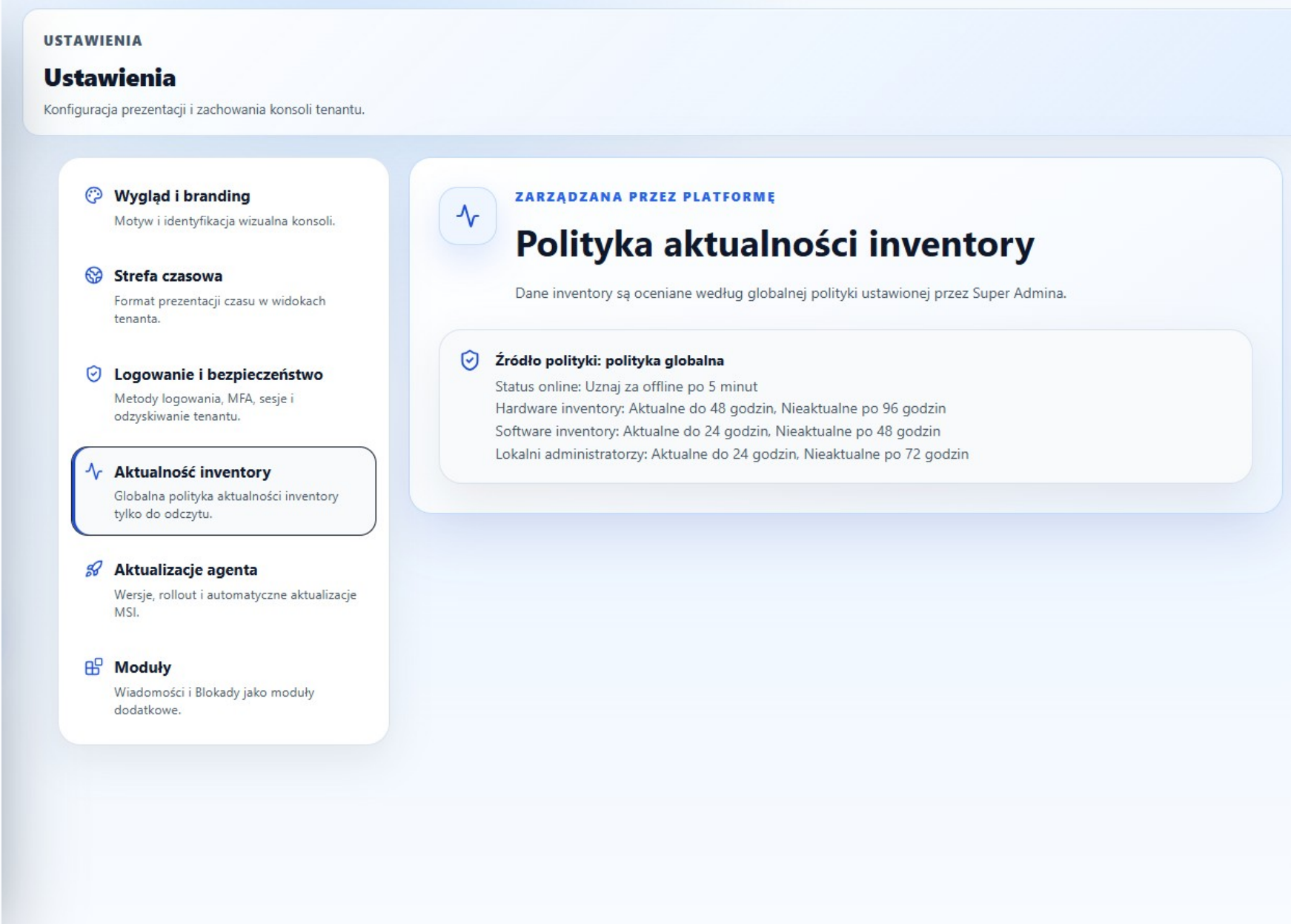
Globalna polityka aktualności Inventory

Super Admin ustala globalne progi aktualności.

Tenant ogląda politykę w trybie tylko do odczytu.

Sprzęt: aktualny do 48 h, nieaktualny po 96 h.

Oprogramowanie: 24/48 h.
Lokalni administratorzy: 24/72 h.



Wersje i postęp wdrożenia

Panel porównuje wersję dostępną i produkcyjną.

Liczniki pokazują potrzebne aktualizacje oraz błędy.

Przykład: wersja 0.3.98.602 na obu urządzeniach.

Historia pokazuje 2 zakończone urządzenia i postęp 100%.

USTAWIENIA

Ustawienia

Konfiguracja prezentacji i zachowania konsoli tenantu.

Ustawienia > Aktualizacje agenta

AKTUALIZACJE MSI AGENTA

Aktualizacje agenta

Zarządzaj wersjami, rollout'em oraz polityką automatycznych aktualizacji MSI agenta.

Dokumentacja

Opublikuj najnowszy MSI

↓

Dostępna wersja agenta

0.3.98.602

Nowa wersja

✓

Wersja produkcyjna

0.3.98.602

Produkcja

↺

Do aktualizacji

0

Wymaga akcji

⚠

Błędy wdrożenia

0

Wymaga uwagi

Plan wdrożenia

✓

2

3

Przygotowanie

Pilot

Etapowy

Aktualny etap:
Ręczny

2 urządzeń

0 błędów

Rollback dostępny

TRYB WDROŻENIA

Ręczny

STATUS PROCESU

Gotowy

WARUNEK PRZEJŚCIA DALEJ

Aktualizacja zostanie wysłana tylko do zaznaczonych komputerów.

POZOSTAŁE URZĄDZENIA

0

Zdrowie rollout'u

100%

postęp

Zakończone

2

100%

W trakcie

0

0%

Oczekujące

0

0%

Nieudane

0

0%

Offline

0

0%

Łącznie urządzeń

2

Ręczne wdrażanie i okno serwisowe

Aktualizacja obejmuje
zaznaczone urządzenia.

Start może nastąpić teraz
lub w oknie serwisowym.

Podgląd pokazuje zakres i automatyczny rollback.

Kontrole dotyczą
dostępności agenta, wersji
i okna serwisowego.

Polityki rollout'u

Ręczny

Pilot

Etapowy

Tryb zapisany: Ręczny

Zgodne z zapisaną polityką

Ręczny wybór urządzeń

Aktualizacja zostanie wysłana tylko do zaznaczonych komputerów.

Wersja docelowa0.3.98.602

Wybrane urządzenia0

Start aktualizacji

Teraz

W oknie serwisowym

Wybierz urządzenia z tabeli poniżej.

Podgląd akcji

Start	Natychmiast po potwierdzeniu
Okno serwisowe	00:01 - 23:59
Zakres	Zaznaczono 0
Rollback	Automatyczny
Ryzyko	Poza oknem serwisowym

Kontrole bezpieczeństwa

Agent online

Wersja zgodna

Rollback dostępny

Poza oknem serwisowym: wymaga potwierdzenia

Okno serwisowe

Początek okna00:01

Koniec okna23:59

Artefakt MSI

OPUBLIKOWANA WERSJA0.3.98.602

ID BUILDU20260928222532-917f93

Kopiuj ID buildu

STATUS BUILDUGotowy

Zaawansowane polityki rollout'u

Zarządzane przez ustawienia platformy

Rozwiń parametry techniczne

Urządzenia w rolloutcie

Wyszukaj komputer

Status update

Online/offline

Filtry

Wymagają

Oczekujące

W trakcie

Nieudane

Offline

Aktualne

Brak urządzeń wymagających aktualizacji

Wszystkie urządzenia są aktualne albo nie pasują do bieżących filtrów.

Wierszy na stronę25

Pokazano 0 z 0

1

Pilotaż nowej wersji

Mała grupa pozwala
sprawdzić aktualizację
przed szerszym
wdrożeniem.

Urządzenia pilota można wskazać bezpośrednio lub przez filtr/tag.

Widoczny warunek
przejścia dalej: czas bez
błędów.

Pokazany tryb Pilot stanowi niezapisany wybór.

Polityki rollout'u

Ręczny

Pilot

Etapowy

Tryb zapisany: Ręczny

Wybrano do zapisania: Pilot

Niezapisane zmiany

Anuluj zmiany

Zapisz politykę

Konfiguracja pilota

Przetestuj aktualizację na małej grupie urządzeń przed szerszym wdrożeniem.

Wybierz urządzenia pilota

Ustaw filtr pilota

Zapisz konfigurację pilota

Uruchom pilota

URZĄDZENIA PILOTA	FILTR/TAG PILOTA	PASUJĄCE URZĄDZENIA
2	Nie wybrano filtra	0
WARUNEK PRZEJŚCIA DALEJ Po czasie bez błędów		

Pasujące urządzenia to aktualnie kwalifikujące się urządzenia z filtra. Wybrane urządzenia pilota mogą obejmować także urządzenia już zaktualizowane.

LAPTOP-001

LAPTOP-002

Okno serwisowe

Początek okna

00:01

Koniec okna

23:59

Artefakt MSI

OPUBLIKOWANA WERSJA

0.3.98.602

ID BUILDU

2026092822532-917f93

Kopiuj ID buildu

STATUS BUILDU

Gotowy

Zaawansowane polityki rollout'u

Zarządzane przez ustawienia platformy

Zwiń parametry techniczne

Aktywny tryb Pilot Zaktualizuj najpierw wybraną grupę pilotażową, zanim udostępnisz wersję większej liczbie urządzeń.	Równoległe aktualizacje 1 Od 1 do 100 urządzeń jednocześnie.	Próg błędów (%) 5 Procent błędów, po którym rollout zostanie zatrzymany.	Liczba prób 3 Ile razy ponowić aktualizację po niepowodzeniu.	Backoff (min) 2 Odstęp w minutach między kolejnymi próbami.
--	---	---	--	--

Wdrażanie etapami z kontrolą błędów

Przykładowe fale: 5%, 20%, 50% i 100%.

Zakres obejmuje kwalifikujące się urządzenia zgodnie z filtrami.

Próg błędów pozwala zatrzymać wdrożenie automatycznie.

Widok pokazuje niezapisany wybór trybu Etapowy.

Ręczny

Pilot

Etapowy

Tryb zapisany: **Ręczny**

Wybrano do zapisania: **Etapowy**

Niezapisane zmiany

Anuluj zmiany

Zapisz politykę

Fale rollout'u

Wdrażaj aktualizację etapami z kontrolą błędów.

Zakres rollout'u

KWALIFIKUJĄCE SIĘ URZĄDZENIA	WYBRANE URZĄDZENIA	ŹRÓDŁO ZAKRESU
2	0	Wszystkie kwalifikujące się urządzenia

Tryb etapowy obejmuje wszystkie kwalifikujące się urządzenia zgodne z filtrami rollout'u.

Konfiguruj fale

Zapisz politykę

Uruchom etapowy rollout

Fala 1: 5%

Aktualna fala

Fala 2: 20%

Następna fala

Fala 3: 50%

Następna fala

Fala 4: 100%

Następna fala

Pozostałe urządzenia: 0

Urządzenia w fali: 1

Zakończone: 2

Nieudane: 0

Następna fala: 20%

Odstęp między falami: 2 min · Postęp fali: 100% · Warunek zatrzymania: 5%

Okno serwisowe

Początek okna

00:01

Koniec okna

23:59

Artefakt MSI

OPUBLIKOWANA WERSJA

0.3.98.602

ID BUILDU

20260928222532-917f93

Kopiuż ID buildu

STATUS BUILDU

Gotowy

Zaawansowane polityki rollout'u

Zarządzane przez ustawienia platformy

Zwiń parametry techniczne

Aktywny tryb	Równoległe aktualizacje	Próg błędów (%)	Liczba prób	Backoff (min)
Etapowy	1	5	3	2

Wdrażaj aktualizację falami procentowymi. Rollout może zatrzymać się automatycznie po przekroczeniu progu błędów.

Od 1 do 100 urządzeń jednocześnie.

Procent błędów, po którym rollout zostanie zatrzymany.

Ile razy ponowić aktualizację po niepowodzeniu.

Odstęp w minutach między kolejnymi próbami.

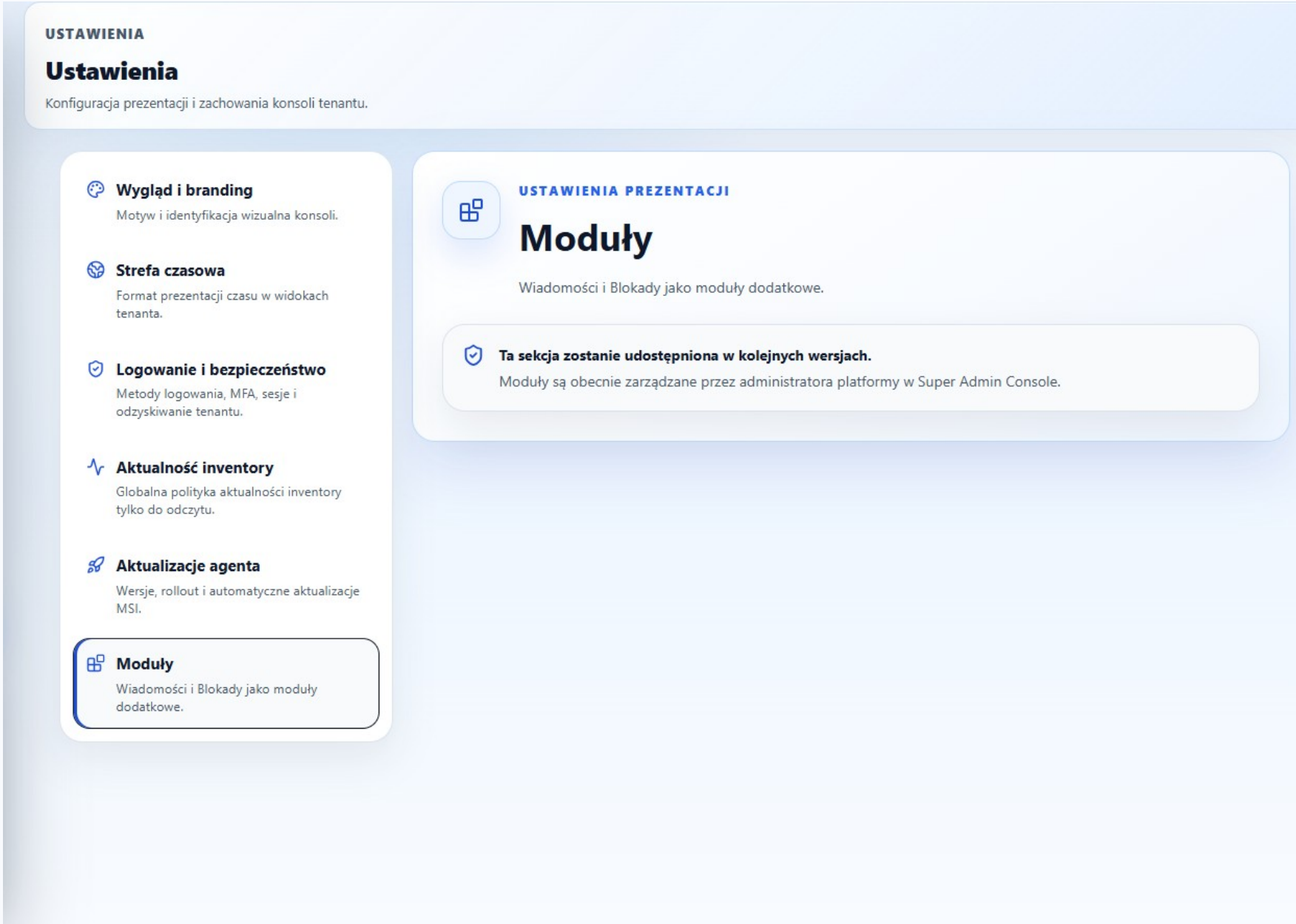
Moduły dodatkowe

Wiadomości i Blokada są modułami dodatkowymi.

Obecnie zarządza nimi administrator platformy w Super Admin Console.

Sekcja zarządzania w ustawieniach tenanta jest planowana.

Działanie modułów dokumentują wcześniejsze przykłady procesów.



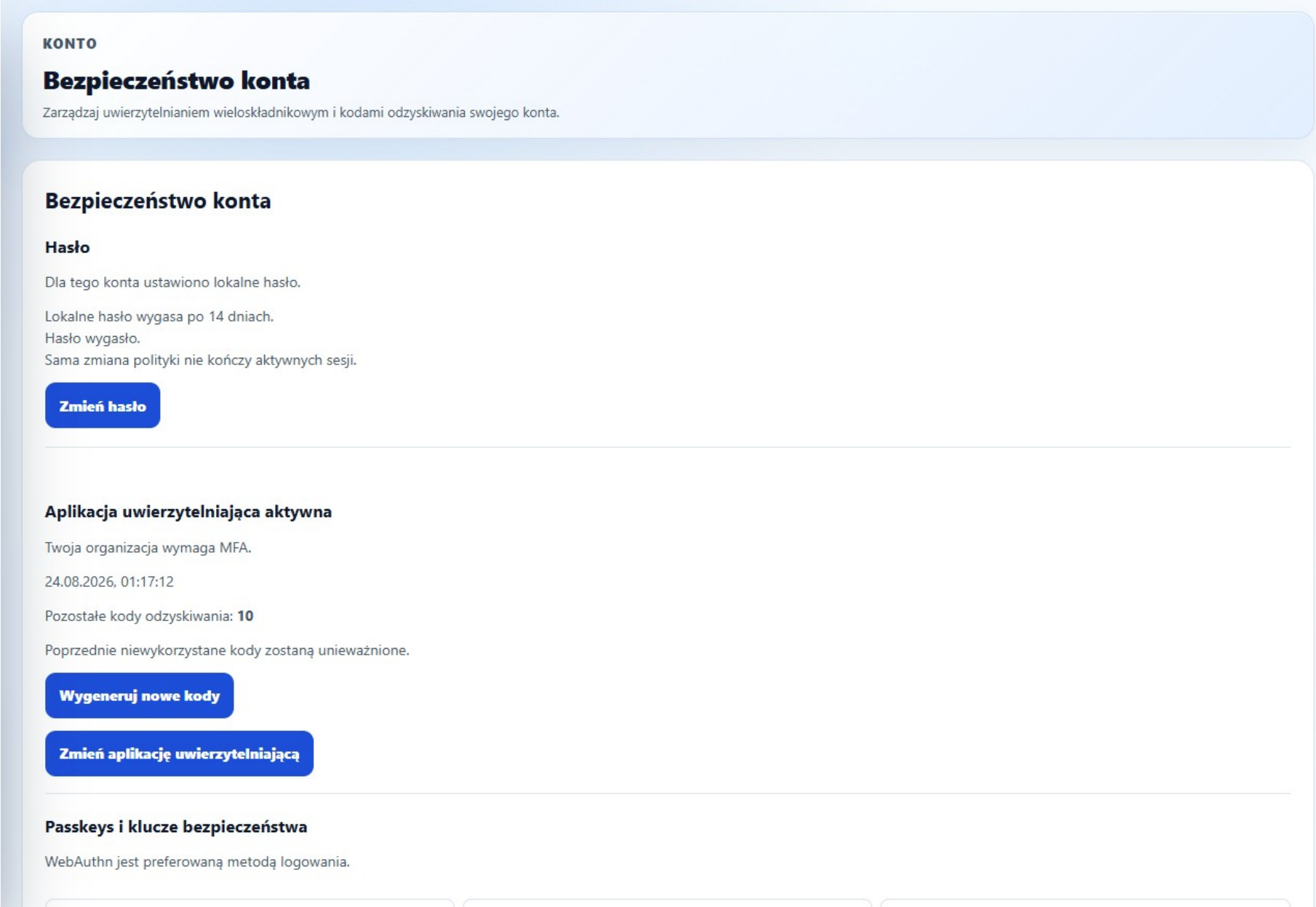
Hasło, MFA i kody odzyskiwania

Użytkownik zarządza zabezpieczeniami własnego konta konsoli.

Widok pokazuje ważność hasła i możliwość jego zmiany.

Aktywna aplikacja uwierzytelniająca realizuje wymóg MFA organizacji.

Nowe kody odzyskiwania unieważniają poprzednie niewykorzystane.



Passkeys i klucze bezpieczeństwa

Użytkownik może dodać passkey lub klucz bezpieczeństwa.

Lista rozdziela metody aktywne i unieważnione.

Widok pokazuje datę utworzenia i ostatniego użycia.

Dostępne akcje obejmują zmianę nazwy i unieważnienie.

Sama zmiana polityki nie kończy aktywnych sesji.

Zmień hasło

Aplikacja uwierzytlniająca aktywna

Twoja organizacja wymaga MFA.

24.08.2026, 01:17:12

Pozostałe kody odzyskiwania: 10

Poprzednie niewykorzystane kody zostaną unieważnione.

Wygeneruj nowe kody

Zmień aplikację uwierzytlniającą

Passkeys i klucze bezpieczeństwa

WebAuthn jest preferowaną metodą logowania.

Bitwarden

Aktywny

Passkey

Urządzenie wbudowane

Utworzono: 24.08.2026, 10:56:25

Ostatnio użyto: 30.09.2026, 14:37:37

Zmień nazwę

Unieważnij

Kopia zapasowa

Bitwarden

Unieważniony

Passkey

Urządzenie wbudowane

Utworzono: 5.08.2026, 21:26:50

Ostatnio użyto: 23.08.2026, 23:18:35

Zmień nazwę

Kopia zapasowa

Bitwarden – komputer testowy

Unieważniony

Passkey

Urządzenie wbudowane

Utworzono: 4.08.2026, 11:58:10

Ostatnio użyto: 5.08.2026, 21:04:36

Zmień nazwę

Kopia zapasowa

Dodaj passkey lub klucz bezpieczeństwa

Rozpoczęcie testów w firmie

01 Logowanie do tenanta

Zaloguj się do udostępnionego środowiska firmy.

02 Wygenerowanie i pobranie agenta

W sekcji „Pobieranie” wygeneruj agenta i pobierz pakiet MSI przypisany do swojego tenanta.

03 Instalacja na komputerach testowych

Zainstaluj pakiet MSI z uprawnieniami administratora na wybranych komputerach z Windows.

04 Sprawdzenie komunikacji

W Inventory sprawdź, czy urządzenia pojawiły się w panelu i komunikują z platformą.

Zgłoszenia na komputerze użytkownika

01 Instalator pobrany przez przeglądarkę

Formularz zgłoszenia otwiera się automatycznie. Użytkownik podaje uzasadnienie i wysyła wniosek do IT.

02 Instalator znajdujący się na komputerze

Kliknij plik prawym przyciskiem myszy. Wybierz „Pokaż więcej opcji”, a następnie „Uruchom z Eleve Admin”.

03 Wniosek o czasowe prawa administratora

Otwórz Eleve Admin z ikonki przy zegarze. Jeśli jest ukryta, rozwiń listę ikon. Wybierz wniosek o prawa administratora i uzupełnij formularz.

IT zatwierdza lub odrzuca wniosek w panelu. Historia zgłoszenia pozostaje dostępna.

Informacje przed rozpoczęciem testów

01 Podpis cyfrowy agenta

Obecna wersja agenta nie jest jeszcze podpisana cyfrowo za pośrednictwem usługi Microsoft.

02 Dopuszczenie pakietu w firmie

Windows lub firmowe zabezpieczenia mogą wyświetlić ostrzeżenie albo zablokować instalację. Uzgodnij dopuszczenie pakietu z zespołem IT lub bezpieczeństwa.

03 Zakres pierwszych testów

Rozpocznij od 2-3 komputerów. Sprawdź instalację aplikacji oraz czasową sesję administratora wraz z zakończeniem uprawnień.

Zakres zastosowania w zespole IT

- 01** Kontrolowana instalacja aplikacji przez użytkownika bez stałych praw administratora.
- 02** Czasowe sesje administratora z informacją o zakończeniu i historią.
- 03** Inventory jako punkt dostępu do raportów i działań na urządzeniu.
- 04** Role konsoli, zabezpieczenia kont i kontrolowane aktualizacje agenta.

<https://jitadmin.com>