Admin By Request

SERVER EDITION

Wielofunkcyjne i efektywne narzędzie typu PAM dla systemów Windows. Aplikacja została stworzona w oparciu o bogate doświadczenie duńskiej firmy FastTrack Software, która specjalizuje się w tworzeniu niezawodnych i wysoce wydajnych aplikacji sieciowych. Narzędzie Admin By Request jest **proste we wdrożeniu, łatwe w użytkowaniu oraz przystępne cenowo** dla firm i organizacji każdej wielkości.

Aplikacja pozwala zoptymalizować ilość użytkowników posiadających uprawnienia administracyjne do systemów firmowych. Admin By Request umożliwia elewację uprawnień za pomocą szeregu opcji:

- przy użyciu unikatowego kodu PIN
- jako uprawnienia przyznawane automatycznie, po uprzednim zdefiniowaniu ustawień, bez konieczności autoryzacji
- dostęp uprzywilejowany do całego systemu lub pojedynczej aplikacji, ograniczony czasowo
- podnoszenie przywilejów po zatwierdzeniu prośby przez administratora bezpieczeństwa

Admin By Request Server Edition, oprócz pełnej kontroli nad zarządzaniem dostępem uprzywilejowanym, zapewnia **wgląd w aktywność użytkowników i raportowanie ich działań** w ramach procesu podnoszenia uprawnień administracyjnych.

Jak działa i czym jest Admin By Request?

Admin By Request składa się z dwóch części:

- **Agenta końcowego**, zainstalowanego w środowisku Windows. Umożliwia on generowanie żądań podniesienia uprawnień. Jeśli agent jest w trybie online, punkt końcowy przekazuje skonfigurowane informacje do Konsoli Zarządzania (np. dzienniki, żądania i ustawienia). Należy też wspomnieć, że aplikacja działa w trybie offline za sprawą dostępnej opcji wygenerowania jednorazowego kodu PIN, umożliwiającego elewację uprawnień nawet, gdy urządzenie nie ma dostępu do Internetu.

- **Konsoli Zarządzania** - bezpiecznego, zarządzanego w Microsoft Azure, środowiska SaaS klasy korporacyjnej, w którym gromadzone są konfiguracje poszczególnych agentów, inwentaryzacja komputerów i żądania dotyczące elewacji uprawnień. Istnieje także możliwość zarządzania aplikacją ABR poprzez aplikację mobilną i API.

Admin by Request nie wymaga rozbudowanej infrastruktury IT (serwerów, maszyn wirtualnych, baz danych itp.) Wszystko, co jest potrzebne do rozpoczęcia pełnego użytkowania, to zarejestrowanie się na portalu. Darmowa wersja aplikacji umożliwia dostęp do pełnej wersji produktu dla maksymalnie 10 serwerów i 25 komputerów Windows i macOS - za darmo, na zawsze.

Kluczowe funkcje Admin By Request

Zarządzanie dostępem uprzywilejowanym

- Ograniczenie możliwości rozprzestrzeniania się programów typu malware i ransomware.
- Automatyczne odbieranie praw administratora lokalnego z ewentualnym wykluczeniem określonych użytkowników.
- Tryb automatycznego podnoszenia uprawnień wybranych aplikacji lub ograniczenia czasowego korzystania z elewacji.
- Zezwalanie lub blokowanie eskalacji uprawnień administratora lokalnego dla określonych aplikacji (lokalizacja pliku, certyfikowanie dostawcy lub suma kontrolna).
- Integracja z bezpiecznym środowiskiem do przechowywania i transferu plików - OPSWAT MetaDefender, które umożliwia pełną kontrolę nad procesami przepływu danych.

Audyt i raportowanie

- Zaawansowane rozwiązanie inwentaryzacyjne.
- Pełna ścieżka audytu aktywności użytkowników, logowań administratora i instalacji oprogramowania.
- Raportowanie kluczowych aktywności użytkowników z możliwością planowania.
- Dostęp API do logów audytu i żądań oraz inwentaryzacji dla SIEM, a także raportowania zewnętrznego.
- Pełny dziennik logów wszystkich zmian

Udogodnienia

- Brak potrzeby zakupu fizycznych urządzeń lub instalacji oprogramowania w istniejącej infrastrukturze serwerowej. **ABR wymaga jedynie instalacji na wybranym endpoincie.**
- Instalator, który zajmuje niecałe 2 MB i nie wymaga żadnej konfiguracji. **Instalowany w trybie cichym za pomocą standardowych narzędzi (SCCM/Intune).**
- Zatwierdzanie wniosków o elewację uprawnień z poziomu **dedykowanej darmowej aplikacji mobilnej**.
- Rozwiązanie działa zarówno w trybie **online jak i offline**.
- **Opcja trybu offline** zarządzana przy wsparciu pliku konfiguracyjnego ADMX, **kontrolującego aktywność użytkowników na komputerze.**

Tryb „Uruchom jako administrator”

Użytkownicy ABR mogą podnieść uprawnienia tylko dla wybranych aplikacji, co **pozwala uniknąć przyznania podwyższonego dostępu do całego systemu**. Otrzymanie uprawnień do danej aplikacji wymaga zatwierdzenia, a prośby przetwarzane są pojedynczo. Tryb ten skierowany jest do użytkowników, którym dostęp uprzywilejowany potrzebny jest sporadycznie, do wykonania pewnych obowiązków. Opcję „Uruchom jako administrator” (Run As Administrator) aktywuje się zgodnie z zasadami funkcjonowania w ramach systemu Windows, więc **zapoznanie się z jej działaniem nie wymaga dodatkowego szkolenia.**

Ograniczona czasowo sesja administratora

Tryb ten aktywuje się poprzez wybranie ikony w zasobniku systemowym, a następnie wystosowanie odpowiedniej prośby o dostęp uprzywilejowany. **Po autoryzacji administratora, użytkownik otrzymuje pełne uprawnienia**, do których dopuszczony jest przez określony czas.
Po jego upłynięciu, **szczegóły dotyczące sesji z dostępem uprzywilejowanym są archiwizowane i zapisywane w panelu Admin By Request.** Opcja ta jest idealna dla osób, które potrzebują swobody w uruchamianiu wielu zaawansowanych aplikacji w określonym czasie.

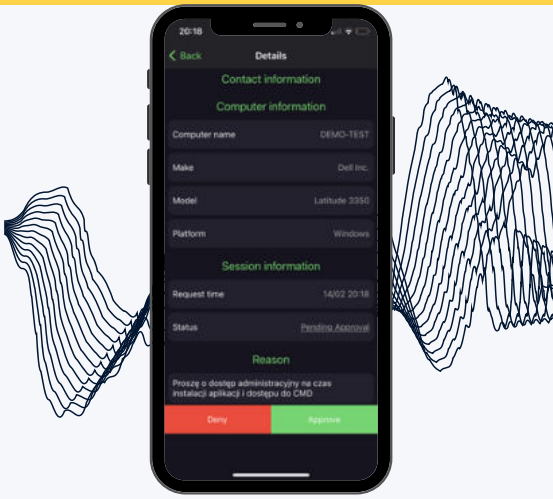
Integracja Admin By Request z OPSWAT MetaDefender

Ta innowacyjna **funkcja umożliwia wstępną weryfikację poziomu bezpieczeństwa eskalacji uprawnień** w trybach „Uruchom jako administrator” oraz „Sesja administracyjna”. Wszelkie operacje podnoszenia uprawnień są sprawdzane w czasie rzeczywistym, w oparciu o obszerną bazę danych zawierającą sumy kontrolne od ponad 20 wiodących, światowych dostawców oprogramowania antywirusowego. Na podstawie analiz, **podejrzana prośba o podniesienie uprawnień może zostać odrzucona lub tymczasowo wstrzymana.**

Funkcja OPSWAT MetaDefender jest w pełni zintegrowana z Admin By Request i nie ingeruje w żaden sposób w inne narzędzia zabezpieczające punkty końcowe.

Zatwierdzanie wniosków o dostęp uprzywilejowany

Wnioski o podniesienie uprawnień można zatwierdzać za pośrednictwem panelu sterowania Admin By Request, aplikacji mobilnej lub interfejsu API. Gdy żądanie zostanie zautoryzowane lub odrzucone przez administratora bezpieczeństwa, użytkownik składający wniosek otrzyma odpowiedź w postaci wiadomości e-mail lub powiadomienia na pulpicie.



Automatyczna autoryzacja wniosków o dostęp uprzywilejowany

Dzięki tej opcji, administrator ma możliwość zdefiniowania zasad, reguł takich jak: lokalizacja plików, certyfikat dostawcy aplikacji lub określona suma kontrolna, w celu uaktywnienia funkcji „wstępnego zatwierdzania". Jest to szczególnie ważne w sytuacji, w której autoryzacja prośby o dostęp uprzywilejowany do określonych aplikacji nie jest konieczna. Eskalacja wcześniej zdefiniowanych aplikacji nie jest poddawana weryfikacji przez oprogramowanie OPSWAT MetaDefender.

Zadania administratora domeny

Będąc zalogowanym do Kontrolera Domeny jako standardowy użytkownik, **Admin By Request może pozwolić zwykłym użytkownikom wykonywać zadania na poziomie Administratora Domeny**, takie jak konfiguracja dostępu, zarządzanie użytkownikami i grupami Active Directory, a także udostępnianie sieci i drukarek. Opcja ta pozwala na zoptymalizowanie liczby użytkowników posiadających dostęp administratora.

Zarządzanie zasobami i przepływem pracy

Logując się do Konsoli Zarządzania możesz grupować i filtrować zasoby według działu w celu delegowania i przetwarzania wniosków.

Endpointy z zainstalowanym programem Admin By Request, które wymagają różnych ustawień (innych niż domyślne ustawienia globalne) **mogą zostać przypisane do dowolnej liczby niestandardowych grup ustawień.** Przykładowo, różne departamenty mogą wysyłać prośby o elewację uprawnień, do przełożonych odpowiednich dla swoich działów.

Dostęp administracyjny do konsoli zarządzania Admin By Request może zostać nadany wielu użytkownikom, którzy uzyskają dostęp tylko do tych zasobów, które zostaną im nadane.

Dostęp za pomocą kodu PIN

Unikalny kod PIN może zostać przyznany użytkownikowi w sytuacji, w której potrzebuje on jednorazowego, ograniczonego czasowo dostępu uprzywilejowanego do całego systemu bądź wybranych aplikacji. Admin By Request, dzięki takiemu rozwiązaniu może działać trybie offline. Administrator ma możliwość wygenerowania jednorazowego hasła, umożliwiającego lokalnemu użytkowników elewację uprawnień nawet, gdy urządzenie nie ma dostępu do Internetu.

Audyt i monitorowanie aktywności

Zaawansowane rozwiązanie do monitorowania oraz audytu aktywności użytkowników dołączone jest w standardzie do narzędzia Admin By Request i nie wymaga dodatkowej implementacji i konfiguracji. System ten **zapewnia wgląd w raport dotyczący każdego urządzenia, zawierający informacje takie jak: zainstalowane w trakcie sesji oprogramowania, członkostwo w grupach użytkowników Active Directory, zdefiniowanych grupach dostępowych oraz przypisane role administracyjne.** Dane można z łatwością wyeksportować w postaci plików formatów PDF, XLS oraz CSV. Mogą one także zostać wygenerowane za pośrednictwem systemu API.

Skuteczna prewencja nadużyć

Admin By Request zawiera szereg zaawansowanych funkcji zapobiegających nadużyciom i niewłaściwemu korzystaniu z narzędzia. Po zainstalowaniu aplikacji ABR, staje się ona jedynym sposobem, dzięki któremu użytkownik może uzyskać podniesione uprawnienia.

Oprócz tego **istnieje możliwość wygenerowania spersonalizowanego komunikatu skierowanego do użytkowników Admin By Request, który ma na celu poinformowanie pracowników o polityce firmy oraz o tym, że ich działania są audytowane.**

Ważną kwestią jest fakt, iż użytkownik nie może samodzielnie odinstalować aplikacji Admin By Request nawet wtedy, kiedy nadane mu są najwyższe uprawnienia administratora.

Deinstalacja za pomocą kodu PIN

Biorąc pod uwagę ograniczenia, jakie mogą powodować funkcje zapobiegające nadużyciom, **w wyjątkowych przypadkach istnieje możliwość odinstalowania narzędzia za pomocą kodu PIN.** Wygenerowane hasło pozwala na całkowite usunięcie Admin By Request z systemu.

IMPLEMENTACJA I WDROŻENIE

Dostępne funkcje implementacji i wdrożenia	Opis funkcji
Niewielki rozmiar pliku (poniżej 2MB)	Szybkie i łatwe wdrożenie, niewielkie zużycie zasobów
Wielojęzyczny interfejs panelu sterowania	Automatyczne wykrywanie języka angielskiego, francuskiego, niemieckiego, hiszpańskiego, norweskiego, szwedzkiego i duńskiego
Wysoce skalowalny	Możliwość wdrożenia ponad 80 000 użytkowników końcowych
Znakowanie punktów końcowych	Możliwość zdefiniowania brandingu danej firmy na komunikatach GUI użytkownika końcowego
Konfiguracja Zero Config	Agent automatycznie konfiguruje się podczas instalacji
Zarządzanie oparte na SaaS	Szybka implementacja, centralne zarządzanie i przejrzysta infrastruktura
Intuicyjny, łatwy w użyciu interfejs zarządzania	Rejestracja i wdrożenie narzędzia, zajmuje mniej niż 5 minut
Brak potrzeby konfiguracji dodatkowego urządzenia sieciowego	Niższe koszty zarządzania
Narzędzie nie musi być przechowywane na serwerach Active Directory	Nie ma potrzeby ingerowania w strukturę AD
Brak konieczności ujawniania i zarządzania hasłami	Idealne rozwiązanie w przypadku wysokich wymagań bezpieczeństwa
Wsparcie techniczne zawarte we wszystkich płatnych planach	Brak dodatkowych kosztów
Repozytorium z dokumentacją	Dostęp do wszelkich potrzebnych informacji w jednym miejscu

ESKALACJA UPRAWNIEŃ

Funkcje związane z eskalacją uprawnień	Opis funkcji
Architektura globalna	Niemal nieograniczone możliwości modyfikacji ustawień
System odbierania praw	Możliwość unieważnienia praw administracyjnych w dowolnej chwili
Natywny tryb elewacji UAC	Podnoszenie uprawnień w systemie Windows bez sterowników
Status audytu przyznanych uprawnień w czasie rzeczywistym	Możliwość monitorowania wszelkich działań związanych z podniesionymi uprawnieniami
Podnoszenie uprawnień	Elewacja uprawnień w zależności od przeprowadzania danego procesu lub użycia aplikacji
Różne tryby podnoszenia uprawnień w trakcie sesji Admin By Request	Dostępne są dwie opcje eskalacji uprawnień: ograniczony czasowo dostęp administracyjny do całego systemu lub elewacja przywilejów jedynie dla wybranej aplikacji
Wymuszenie zakończenia sesji w dowolnym momencie	Możliwość odebrania praw administratora przed zakończeniem sesji
Kod PIN jednorazowego użytku	Umożliwia ręczne przyznanie jednorazowego dostępu uprzywilejowanego

BEZPIECZEŃSTWO

Funkcje związane z bezpieczeństwem	Opis funkcji
Narzędzie OPSWAT do weryfikacji podejrzanych działań	Stała kontrola eskalacji uprawnień w oparciu o ponad 20 dostawców oprogramowania antywirusowego
Automatyczne wykrywanie połączeń Proxy i VPN	Automatyczne wykrywanie rozwiązań, takich jak Z-Scaler i Pulse Secure
Konfigurowalne komunikaty	Możliwość dostarczenia użytkownikom spersonalizowanych wiadomości z instrukcjami postępowania
„Czarna lista”	Zdefiniowanie listy aplikacji o bezwzględnie ograniczonym dostępie
Wyjątek „czarnej listy” – kod PIN	Możliwość ręcznego zatwierdzenia dostępu do aplikacji z czarnej listy
Tryb bezpiecznego pulpitu UAC	Integracja ABR z systemem UAC, co pozwala na stałą kontrolę konta użytkownika
Funkcje antysabotażowe	Prewencja przed manipulowaniem usługami
Dziennik zmian ustawień portalu	Możliwość monitorowania wszelkich zmian ustawień w panelu zarządzania

INTEGRACJA

Funkcja	Opis funkcji
Integracje zewnętrzne systemu za pomocą REST API	Interfejsy API dziennika audytu, panelu sterowania i systemu próśb i żądań
Integracja SCIM z OKTA i Azure AD	Możliwość synchronizacji użytkowników z usługami AAD lub OKTA
Logowanie przy użyciu AAD SSO/O365/SAML	Bezproblemowa i szybka autoryzacja
Integracja systemów ticketowych	Zintegrowanie powiadomień z prośbami o przyznanie elewacji uprawnień oraz statusów zakładanych zgłoszeń

ZARZĄDZANIE

Funkcje zarządzania	Opis funkcji
Aktualizacja agenta końcowego poprzez aktualizację LAN	Automatyzacja procesu aktualizacji za pośrednictwem sieci
Wielojęzyczny interfejs panelu sterowania	Automatyczne wykrywanie języka angielskiego, francuskiego, niemieckiego, hiszpańskiego, norweskiego, szwedzkiego i duńskiego
Aktualizacja agenta końcowego przez Internet	Automatyczna aktualizacja za pomocą jednego przycisku
Możliwość wdrożenia z użyciem Intune i SCCM	Wdrożenie z wykorzystaniem rozwiązań do kompleksowego zarządzania oprogramowaniem
Aplikacja mobilna (Android i Apple)	Zarządzanie Admin By Request z dowolnego miejsca, z dala od komputera
Raporty e-mail	Zautomatyzowane, zaplanowane dostarczanie wiadomości e-mail zawierających raport aktywności
Inwentaryzacja systemu	Większa przejrzystość i wiedza na temat stanu infrastruktury IT
Przechowywanie danych	Możliwość archiwizowania danych na okres od 3 miesięcy do 5 lat
Brak limitu osób administrujących i granulacja uprawnień	Użytkownikowi może zostać przypisana dowolna rola
Filtrowanie danych za pomocą grupy, do której należy użytkownik lub jego roli	Przypisanie użytkownikom miejsca w określonych grupach
Nieograniczone możliwości konfiguracyjne grup dostępowych	Brak limitu ilości ustawień

LICENCJE

	Admin By Request Server POC	Admin By Request Server
Dostępna ilość punktów końcowych	25	Nielimitowana
Model licencji	Darmowa, ograniczona czasowo	Roczna subskrypcja
Wspierany system operacyjny	Windows 2008 R2 lub nowszy	Windows 2008 R2 lub nowszy
Wsparcie	Zawarte	Zawarte

Decydując się na wdrożenie rozwiązania Admin By Request otrzymasz **pełne wsparcie zespołu Securivy w języku polskim.** Jeśli chcesz sprawdzić, jak działa aplikacja, skorzystaj z darmowej wersji, która pozwoli Ci zabezpieczyć 25 komputerów oraz 10 serwerów. Wersja ta jest pełną wersją programu Admin By Request i możesz korzystać z niej bez żadnych ograniczeń funkcjonalnych i czasowych.

Wypróbuj darmową wersję do 10 serwerów oraz 25 komputerów

WYPRÓBUJ

Chcesz dowiedzieć się więcej o zarządzaniu uprawnieniami administracyjnymi?

POBIERZ E-BOOKA

Obejrzyj WEBINAR
Z DEMO PRODUKTU

OBEJRZYJ

Sprawdź, co jeszcze możemy Ci zaoferować

securivy.com

SECURIVY

Securivy - Bezpieczeństwo i Outsourcing IT
ul. Brzeźnicka 14/8
60-133 Poznań
NIP 7792376120
biuro@securivy.com
+48 722 158 258