EKRAN SYSTEM

ZARZĄDZANIE DOSTĘPEM UPRZYWILEJOWANYM

INSTRUKCJA WDROŻENIA

SPIS TREŚCI

5 WAŻNYCH WYZWAŃ ZWIĄZANYCH Z ZARZĄDZANIEM DOSTĘPEM

1. PASSWORD MANAGER: ZMNIEJSZENIE RYZYKA NARUSZENIA DANYCH UWIERZYTELNIAJĄCYCH

2. DODATKOWE UWIERZYTELNIANIE: WIĘKSZA WIDOCZNOŚĆ AKTYWNOŚCI KONT WSPÓŁDZIELONYCH

3. UWIERZYTELNIANIE WIELOSKŁADNIKOWE: ZAPOBIEGANIE NIEAUTORYZOWANEMU DOSTĘPOWI

4. KONTROLA DOSTĘPU DO PUNKTÓW KOŃCOWYCH: WYŁĄCZENIE DOSTĘPU POZA GODZINAMI PRACY DO KRYTYCZNYCH PUNKTÓW KOŃCOWYCH

5. ZARZĄDZANIE ALERTAMI: BLOKADA DOSTĘPU DLA NIEZAUFANYCH UŻYTKOWNIKÓW

PODSUMOWANIE

Właściwe zarządzanie dostępem uprzywilejowanym jest kluczowe dla bezpieczeństwa danych. Organizacje już teraz poświęcają wiele czasu i wysiłku na zabezpieczenie swoich krytycznych danych i systemów przed kompromitacją. Jednak wraz z rosnącą złożonością dzisiejszych infrastruktur IT, muszą one również konfigurować, stale monitorować i zarządzać dziesiątkami poziomów uprawnień dostępu dla wszystkich rodzajów punktów końcowych i grup użytkowników.

Ekran System oferuje kompleksowe i łatwe rozwiązanie dla:

- Bezpiecznego zarządzania uprzywilejowanym dostępem.
- Kontroli nieautoryzowanego dostępu do zasobów korporacyjnych.
- Zapewnienia bezpiecznej pracy z pracownikami zdalnymi i podwykonawcami

W tym przewodniku omawiamy pięć kluczowych wyzwań związanych z zarządzaniem dostępem, z którymi boryka się większość organizacji. Wyjaśniamy również, jak można rozwiązać każde z nich za pomocą Ekran System. Nasze wskazówki dotyczące konfiguracji pomogą lepiej zrozumieć, jak działa każda z opisanych funkcji.

5 WAŻNYCH WYZWAŃ ZWIĄZANYCH Z ZARZĄDZANIEM DOSTĘPEM

Możliwość kontrolowania, kto i co może robić z krytycznymi danymi oraz systemami jest kluczowe dla każdej organizacji. Wiele z nich uważa, że wyzwaniem jest:

1. Zabezpieczyć poświadczenia uprzywilejowane
2. Uzyskać wgląd do współdzielonego konta
3. Ochronić swoje zasoby przed nieautoryzowanym dostępem
4. Ograniczyć dostęp do swoich zasobów poza godzinami pracy
5. Blokować niezaufanych użytkowników

Ekran System może pomóc w skutecznej realizacji każdego z tych zadań dzięki pięciu funkcjom:

Zarządzaj dostępem uprzywilejowanym za pomocą Ekran System

Funkcja	Działanie	Rezultat
Menedżer haseł	• Pozwala ustawić różne poziomy uprawnień dostępu za pomocą konfiguracji poświadczeń • Automatyzuje rotację haseł	Zmniejsza ryzyko naruszenia poświadczeń uprzywilejowanych
Wtórne uwierzytelnianie	• Żąda dodatkowego uwierzytelniania za pomocą indywidualnych danych, w przypadku współdzielonych kont • Przypisuje każdą sesję rozpoczętą na współdzielonym koncie określonemu użytkownikowi	Pozwala na kontrolę działań konkretnego użytkownika korzystającego z konta współdzielonego
Uwierzytelnianie wieloskładnikowe	• Umożliwia dodatkową weryfikację tożsamości użytkownika podczas logowania • Przyznaje dostęp po wprowadzeniu jednorazowego kodu wysłanego na zweryfikowane urządzenie mobilne	Zapobiega nieautoryzowanemu dostępowi do Twojej sieci
Kontrola dostępu do punktu końcowego	• Udziela dostępu do systemu tylko w określonych ramach czasowych • Dostęp do zasobów poza godzinami pracy nie jest przyznawany bez bezpośredniej zgody administratora	Ogranicza dostęp do krytycznych danych poza godzinami pracy
Zarządzanie alertami	• Wykrywa i automatycznie blokuje podejrzanych użytkowników • Natychmiastowo powiadamia administratorów bezpieczeństwa o wykrytych incydentach	Blokuje dostęp do krytycznych danych niezaufanym użytkownikom

Przyjrzyjmy się bliżej możliwościom zarządzania dostępem uprzywilejowanym, z których możesz korzystać za pomocą Ekran System.

1. PASSWORD MANAGER: ZMNIEJSZENIE RYZYKA NARUSZENIA DANYCH UWIERZYTELNIAJĄCYCH

Użytkownicy kont uprzywilejowanych mogą mieć częściowy dostęp (użytkownicy uprzywilejowani) lub pełny dostęp (administratorzy domeny) do krytycznych danych, systemów i usług organizacji. Konta te, jak również dane uwierzytelniające do nich, wymagają ścisłej ochrony.

Podczas pracy z kontami uprzywilejowanymi, organizacje muszą być w stanie:

- Zarządzać wykorzystaniem takich kont
- Regularnie zmieniać ich hasła
- Odzyskać uprawnienia dostępu dla kont administratorów, którzy zakończyli współpracę

Aby zminimalizować ryzyko kradzieży danych uwierzytelniających lub kompromitacji, najlepiej jest zapewnić dostęp do krytycznych zasobów bez ujawniania danych uwierzytelniających użytkownikowi końcowemu. W tym zadaniu świetnie sprawdzi się Password Manager Ekran System.

Użyj tej funkcji, kiedy potrzebujesz:

- Zautomatyzować rotację haseł dla kont uprzywilejowanych
- Unikać ujawniania danych uwierzytelniających konta pracownikom i osobom trzecim

Obsługiwane poświadczenia:

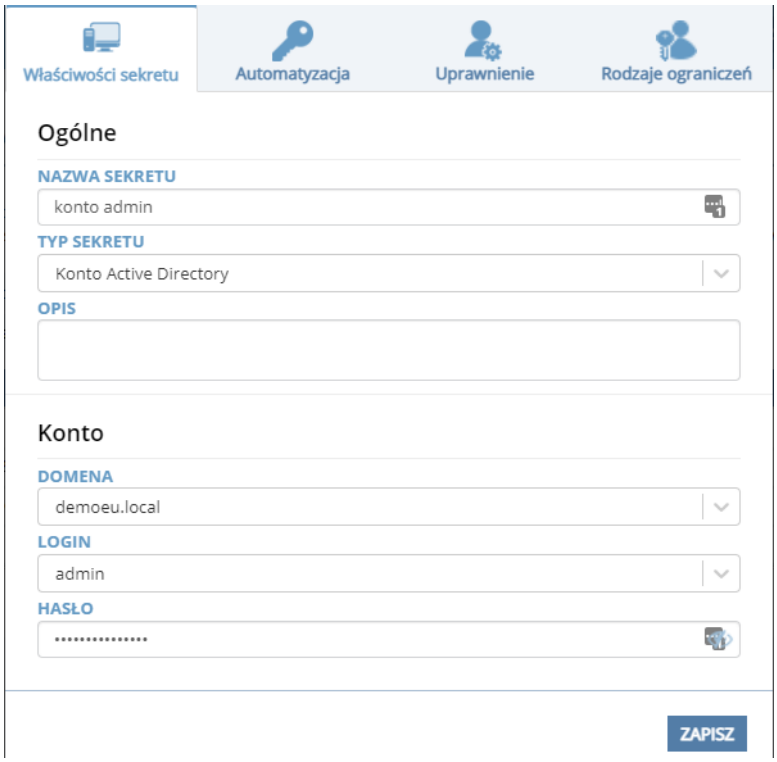
- Windows Account
- SSH
- Web
- MS SQL

Dodawanie poświadczeń

Korzystając z naszego menedżera haseł, możesz tworzyć poświadczenia logowania dla różnych serwisów internetowych, baz danych oraz kont Active Directory. Zobaczmy, jak to działa na przykładzie administratora domeny Active Directory:

1. Utwórz osobne konto domenowe dla każdego administratora systemu jako standardowego użytkownika domeny (bez podwyższonych uprawnień).
2. Utwórz jedno konto administratora domeny.
3. W **Konsoli zarządzania**, utwórz nowe poświadczenie logowania i nadaj mu nazwę.

Jako typ poświadczenia wybierz opcję Konto Active Directory. Dodaj login i hasło do utworzonego wcześniej konta administratora domeny.



Rys. 1 Konfiguracja nowego poświadczenia

Oto znaczenie niektórych terminów, których będziemy używać:

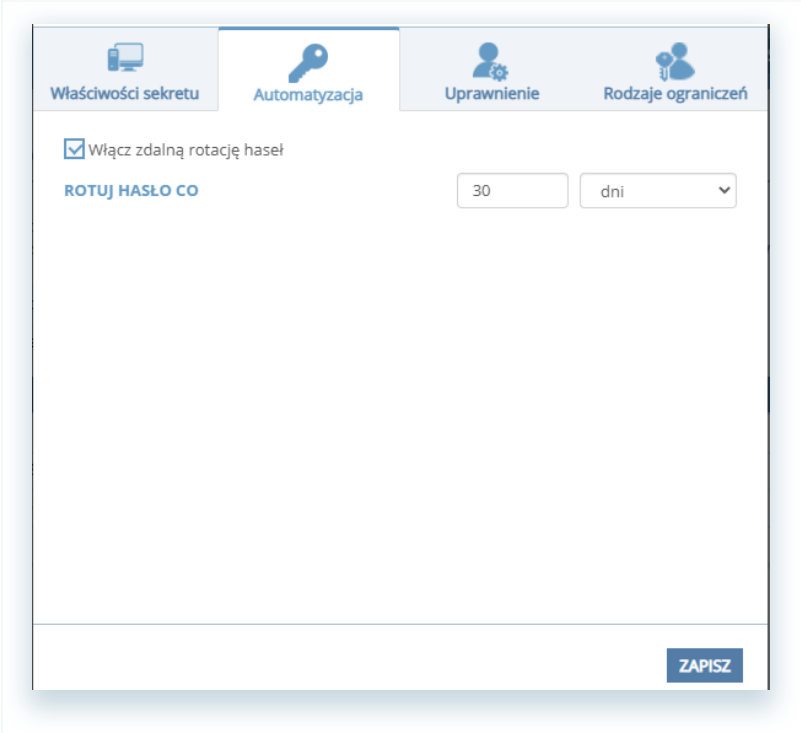
Konsola zarządzania - komponent Ekran System służący do zarządzania platformą i przeglądania monitorowanych danych otrzymywanych od Klientów.

Agent monitorowania - aplikacja agenta Ekran System zainstalowana na monitorowanych punktach końcowych.

Punkt końcowy - docelowy host monitorowany przez Ekran System; może być fizyczny (komputery, serwery) lub wirtualny (DaaS, chmury prywatne).

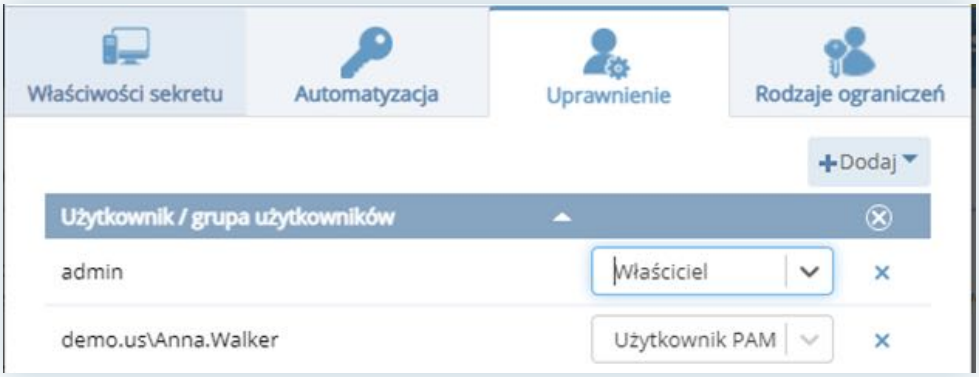
Poświadczenia logowania - jednostka, w której przechowywane są dane uwierzytelniające kont uprzywilejowanych.

4. Przejdź do zakładki **Automatyzacja** i skonfiguruj okresową rotację hasła administratora domeny.



Rys. 2 Okresowa rotacja hasła administratora domeny

5. W karcie **Uprawnienia** ustaw poziomy uprawnień dla administratorów systemu do korzystania z tego poświadczenia.



Rys. 3 Ustawienie poziomu uprawnień do korzystania z poświadczenia

Używając tego poświadczenia, administratorzy systemu będą mogli uzyskać dostęp do każdego punktu końcowego w domenie z uprawnieniami administratora domeny. Administratorzy nie będą mogli nadużywać lub naruszać danych uwierzytelniających administratora domeny, ponieważ nie będą ich znali. Połączenia z docelowymi punktami końcowymi będą realizowane poprzez serwer przesiadkowy (Jump Server).

Dzięki temu wszystkie działania administratorów systemu będą monitorowane przez Ekran System. Wystarczy podać dane logowania w filtrze i obserwować wszystkie nagrane sesje dla tego poświadczenia na stronie Monitoring Results.

Konfiguracja poświadczeń

Wdrożenie poświadczeń zależy od ilości użytkowników i serwerów, do których docelowo będą mieli dostęp. Aby kilku użytkowników mogło pracować z tym samym poświadczeniem, należy skonfigurować rolę Remote Desktop Services Host na swoim serwerze przesiadkowym.

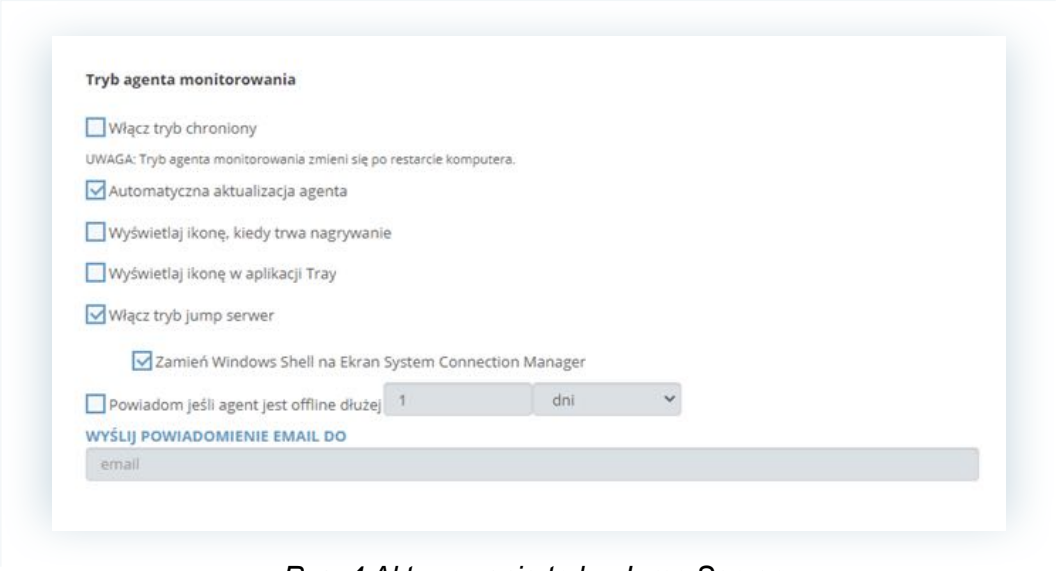
Prześledźmy proces konfiguracji poświadczeń logowania krok po kroku.

Po pierwsze, musisz włączyć tryb **Jump Server** w **Konsoli zarządzania**:

1. Zaloguj się do **Konsoli zarządzania** i przejdź do menu **Zarządzanie agentami monitorowania**.
2. Kliknij przycisk **Edytuj agenta monitorowania**.

3. W zakładce **Właściwości** zaznacz dwie opcje: **Włącz tryb Jump Server** oraz **Zamień Windows Shell na Ekran System Connection Manager**.

4. Zapisz zmiany i wyjdź.



Rys. 4 Aktywowanie trybu Jump Server

Następnie należy dodać do Ekran System standardowe konta domenowe administratorów systemu:

1. Zaloguj się do **Konsoli zarządzania** i przejdź do menu **Zarządzanie użytkownikami**.

2. W otwartym oknie kliknij przycisk **Dodaj użytkownika**.

3. Kliknij przycisk **Dodaj użytkownika Active Directory**.

4. Wybierz domenę i nazwę użytkownika, a następnie kliknij przycisk **Dalej**.

5. W zakładce **Grupy** użytkowników wybierz grupę **Użytkownicy PAM**.

6. Przejdź do zakładki **Uprawnienia administratora** i nie zaznaczaj żadnych uprawnień - w ten sposób użytkownik nie będzie mógł zalogować się do **Konsoli zarządzania** Ekran System, ale będzie mógł korzystać z Poświadczeń PAM.

7. Zapisz zmiany i wyjdź.

Na koniec należy dodać do systemu Active Directory Secret i skonfigurować dla niego rotację haseł:

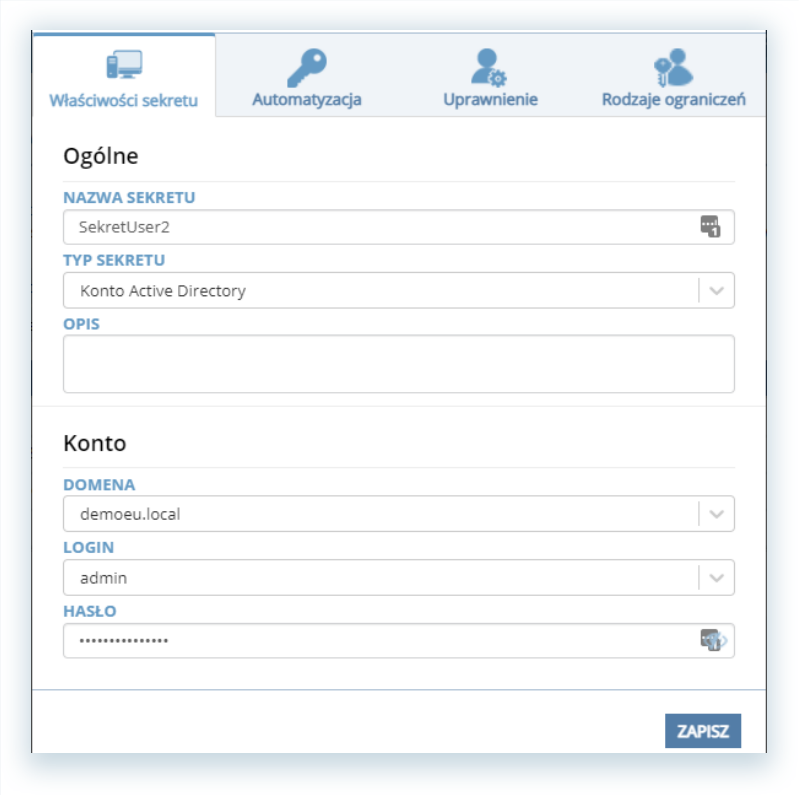
1. Zaloguj się do narzędzia Konsoli zarządzania i przejdź na stronę **Zarządzanie hasłami.**

2. Kliknij przycisk **Dodaj poświadczenia**.

3. Wprowadź nazwę poświadczeń i wybierz **konto Active Directory** jako typ poświadczeń.

4. Ustaw domenę.

5. Wprowadź login i hasło użytkownika dla utworzonego wcześniej konta **Administrator Active Directory.**



Rys. 5 Definiowanie ustawień Secretu

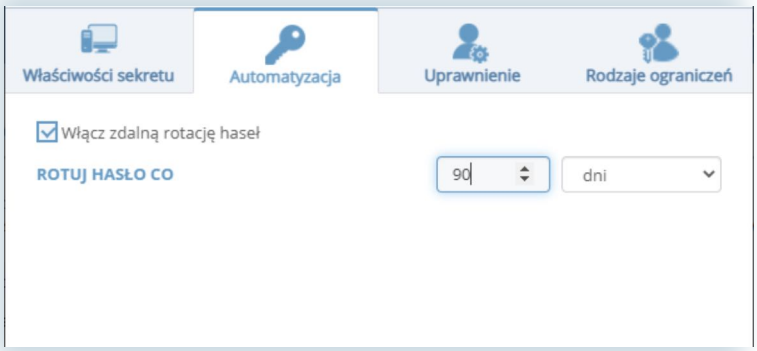
6. Otwórz zakładkę **Uprawnienia**.

7. Dodaj ogólne konta **Active Directory** administratorów systemu i pozwól im na korzystanie z nowo utworzonego poświadczenia logowania.

8. Z listy rozwijanej wybierz typ uprawnienia **Użytkownik PAM**.

Rys. 6 Ustawienia użytkownika dla nowo utworzonego poświadczenia logowania

9. Otwórz zakładkę **Automatyzacja** i określ ustawienia dla automatycznej rotacji haseł.



Rys. 7 Ustawienia dla automatycznej rotacji haseł

10. Zapisz zmiany i wyjdź.

Po tej operacji użytkownicy dodani do tego poświadczenia będą mogli uzyskać dostęp do każdego punktu końcowego w systemie jako administratorzy domeny, bez znajomości hasła do konta administratora domeny. Ponadto, wszystkie działania administratora będą monitorowane na Jump Serverze oraz dostępne do wglądu i audytu na stronie **Monitoring Results**.

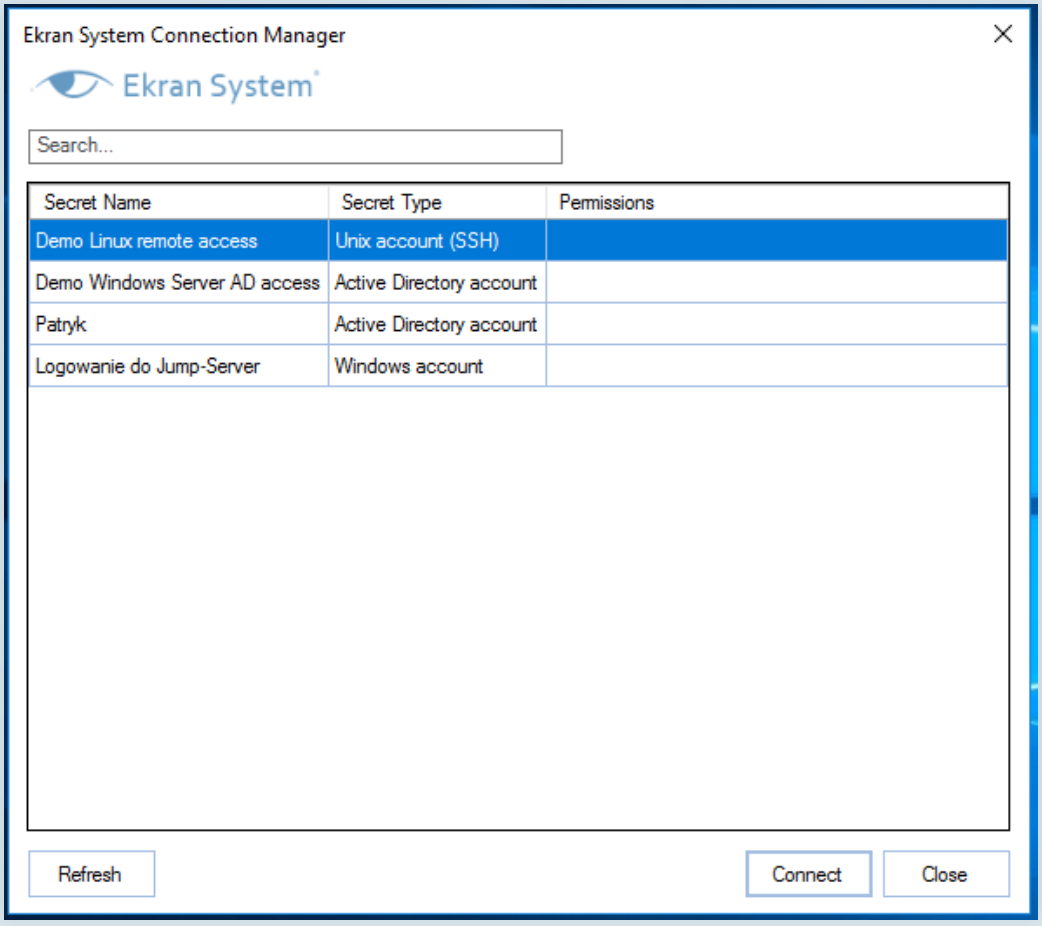
Przyjrzyjmy się teraz bliżej pracy z poświadczeniami logowania z perspektywy administratora systemu.

Praca z poświadczeniami logowania

Aby uzyskać dostęp administracyjny do docelowego hosta, z użyciem poświadczeń logowania zapisanymi w Ekran System, należy wykonać następujące czynności:

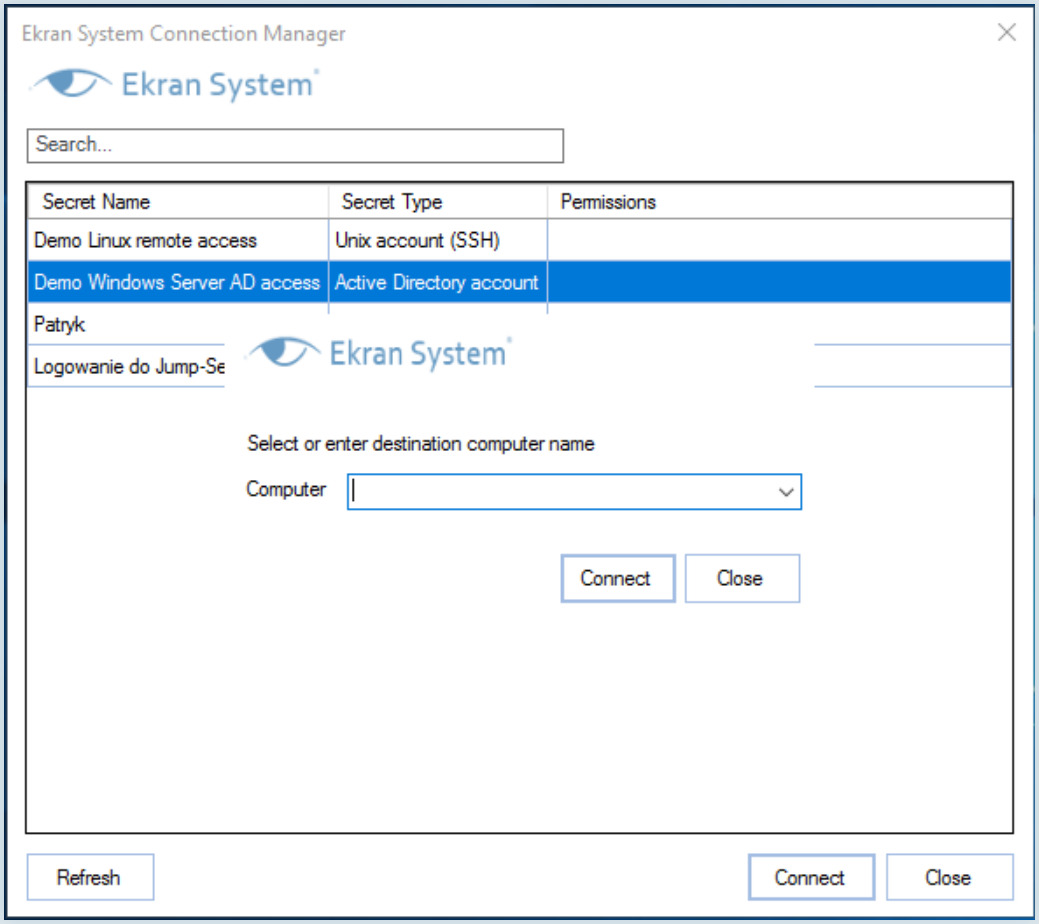
1. Używając **Remote Desktop Protocol (RDP)**, czyli **pulpitu zdalnego**, połącz się z Jump Serverem i zaloguj się do systemu na swoje konto domenowe.

2. W otwartym oknie **Ekran System Connection Manager**, wybierz poświadczenie logowania konta Active Directory spośród dostępnych poświadczeń i kliknij **Connect.**



Rys. 8 Lista dostępnych poświadczeń

3. W kolejnym oknie wpisz nazwę hosta punktu końcowego, z którym chcesz się połączyć.



Rys. 9 Konfiguracja łączenia z punktem końcowym

4. Następnie jeszcze raz kliknij przycisk **Connect.**

W ten sposób uzyskasz zdalny dostęp do wskazanego punktu końcowego z uprawnieniami administratora domeny.

Ten sam schemat można zastosować do innych grup uprzywilejowanych użytkowników, a nawet do podwykonawców. Uzyskają oni niezbędne prawa dostępu bez znajomości poświadczeń kont uprzywilejowanych, z których korzystają. Takie podejście zapewnia większą widoczność aktywności różnych kont uprzywilejowanych, ponieważ wszystkie działania użytkowników na serwerze przesiadkowym są stale monitorowane i rejestrowane.

Jednocześnie fakt, że użytkownicy końcowi nie znają loginów i haseł do kont uprzywilejowanych, z których korzystają, zmniejsza ryzyko wycieku danych uwierzytelniających.

2. DODATKOWE UWIERZYTELNIANIE: WIĘKSZA WIDOCZNOŚĆ AKTYWNOŚCI KONT WSPÓŁDZIELONYCH

Organizacje często używają kont współdzielonych do zarządzania różnymi systemami, dostępem, usługami i aplikacjami. I chociaż takie podejście wydaje się korzystniejsze cenowo, korzystanie ze współdzielonych kont wiąże się z pewnymi problemami dotyczącymi cyberbezpieczeństwa.

Największym wyzwaniem jest rozróżnienie poszczególnych użytkowników zalogowanych na wspólnym koncie.

Użyj tej funkcji, kiedy potrzebujesz:

- Automatyzacji rotacji haseł dla kont uprzywilejowanych
- Uniknąć ujawniania danych logowania pracownikom np. firm zewnętrznych

Podczas gdy nadal można rejestrować wszystkie sesje użytkowników zainicjowane z konta współdzielonego, nie będzie można stwierdzić, który użytkownik jest odpowiedzialny za daną akcję lub ograniczyć dostępu dla poszczególnych użytkowników. Utrudnia to kontrolę aktywności konkretnego użytkownika, jak również zapobieganie ewentualnym incydentom związanym z cyberbezpieczeństwem.

Ekran System oferuje wygodne rozwiązanie tego problemu dzięki funkcji dodatkowego uwierzytelniania. Funkcja ta została zaprojektowana specjalnie do zarządzania wspólnymi kontami i może być włączona dla konkretnego Agenta Ekran System lub grupy.

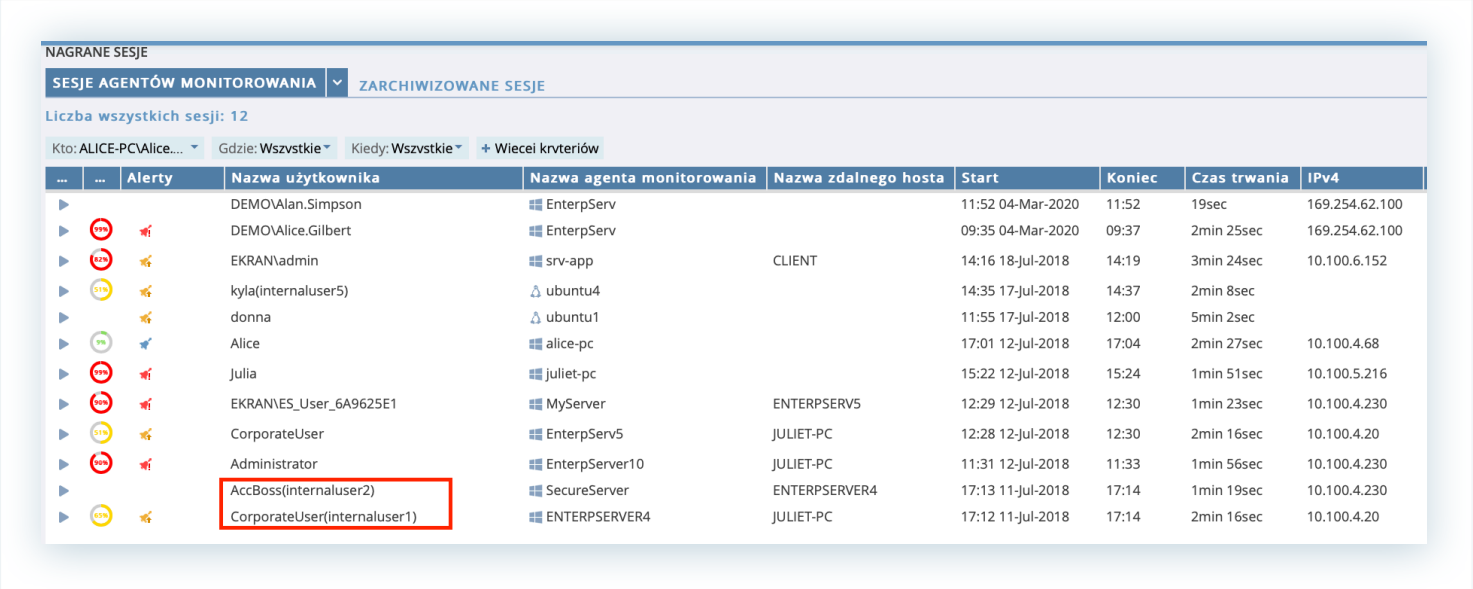
Działa to w następujący sposób: Kiedy użytkownik próbuje uzyskać dostęp do punktu końcowego z włączonym dodatkowym uwierzytelnianiem, musi wprowadzić dwie pary danych uwierzytelniających:

1. Po pierwsze loguje się do systemu, używając poświadczeń pierwotnych - loginu i hasła do konta współdzielonego.
2. Następnie wprowadza poświadczenia dodatkowe - login i hasło do swojego konta, z ktorego standardowo korzysta (przykładowo jego konto domenowe lub wbudowane konto Ekran System).

Dopiero po tym użytkownik uzyskuje dostęp do docelowego punktu końcowego.

Przepływ pracy związany z dodatkowym uwierzytelnianiem

Dzięki wykorzystaniu dodatkowych poświadczeń użytkownika, Ekran System może powiązać każdą sesję zainicjowaną na koncie współdzielonym z konkretnym użytkownikiem, który ją rozpoczął. W sekcji Monitoring Results możesz sprawdzić, kto dokładnie wszedł do systemu, używając konta współdzielonego. Dla każdej takiej sesji Ekran System zapisuje nazwy obu użytkowników.



...	...	Alerty	Nazwa użytkownika	Nazwa agenta monitorowania	Nazwa zdalnego hosta	Start	Koniec	Czas trwania	IPv4
			DEMO\Alan.Simpson	EnterpServ		11:52 04-Mar-2020	11:52	19sec	169.254.62.100
	99%		DEMO\Alice.Gilbert	EnterpServ		09:35 04-Mar-2020	09:37	2min 25sec	169.254.62.100
	62%		EKRAN\admin	srv-app	CLIENT	14:16 18-Jul-2018	14:19	3min 24sec	10.100.6.152
	51%		kyla(internaluser5)	ubuntu4		14:35 17-Jul-2018	14:37	2min 8sec	
			donna	ubuntu1		11:55 17-Jul-2018	12:00	5min 2sec	
	9%		Alice	alice-pc		17:01 12-Jul-2018	17:04	2min 27sec	10.100.4.68
	99%		Julia	juliet-pc		15:22 12-Jul-2018	15:24	1min 51sec	10.100.5.216
	90%		EKRAN\ES_User_6A9625E1	MyServer	ENTERPSERV5	12:29 12-Jul-2018	12:30	1min 23sec	10.100.4.230
	51%		CorporateUser	EnterpServ5	JULIET-PC	12:28 12-Jul-2018	12:30	2min 16sec	10.100.4.20
	90%		Administrator	EnterpServer10	JULIET-PC	11:31 12-Jul-2018	11:33	1min 56sec	10.100.4.230
			AccBoss(internaluser2)	SecureServer	ENTERPSERVER4	17:13 11-Jul-2018	17:14	1min 19sec	10.100.4.230
	51%		CorporateUser(internaluser1)	ENTERPSERVER4	JULIET-PC	17:12 11-Jul-2018	17:14	2min 16sec	10.100.4.20

Rys. 10 Wyświetlanie nazw podstawowych (Klient) i drugorzędnych (Użytkownik) w wynikach monitorowania

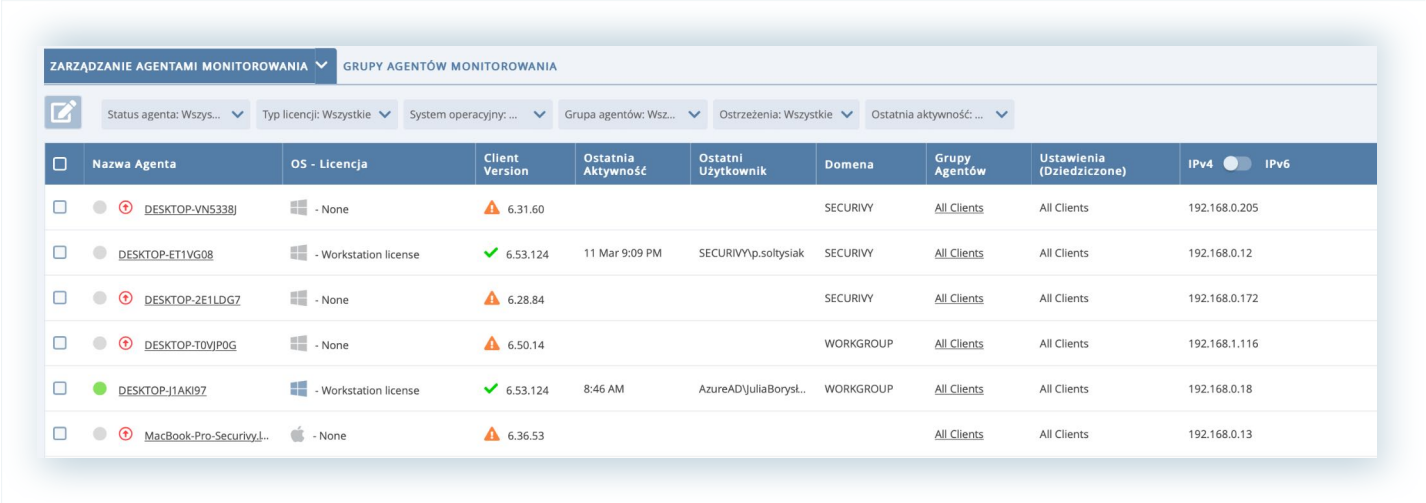
Ekran System dodaje również nazwę drugiego użytkownika do powiadomień e-mail o wykrytych incydentach cyberbezpieczeństwa związanych z kontami współdzielonymi.

Konfiguracja dodatkowego uwierzytelniania dla klienta

Zobaczmy teraz jak można skonfigurować tę funkcję w Konsoli zarządzania Ekran System. Zaczniemy od włączenia wieloskładnikowego uwierzytelniania dla klienta Ekran System:

1. W Narzędziu do zarządzania otwórz stronę **Zarządzanie agentami monitorowania**.

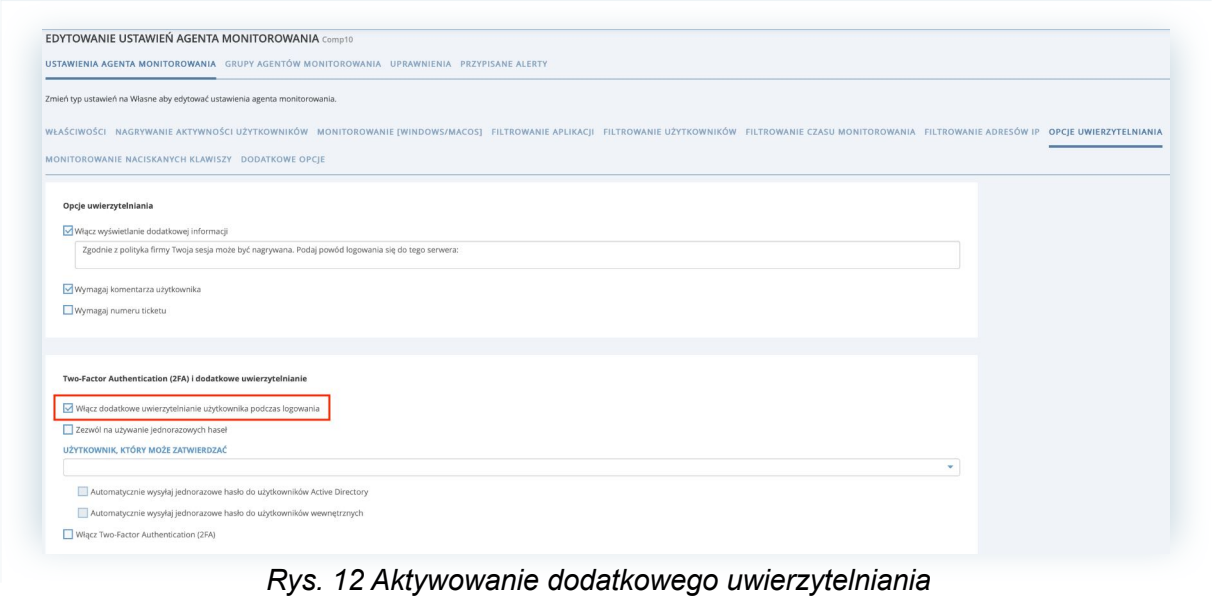
2. Znajdź na liście klienta, którego chcesz skonfigurować, i kliknij przycisk **Edytuj agenta**.



Rys. 11 Zakładka Zarządzanie agentami monitorowania

3. Przejdź do sekcji **Ustawienia agenta monitorowania** i otwórz zakładkę **Opcje uwierzytelniania**.

4. Zaznacz opcję **Włącz dodatkowe uwierzytelnianie** użytkownika podczas logowania.



Rys. 12 Aktywowanie dodatkowego uwierzytelniania

5. Kliknij **Zakończ** i wyjdź.

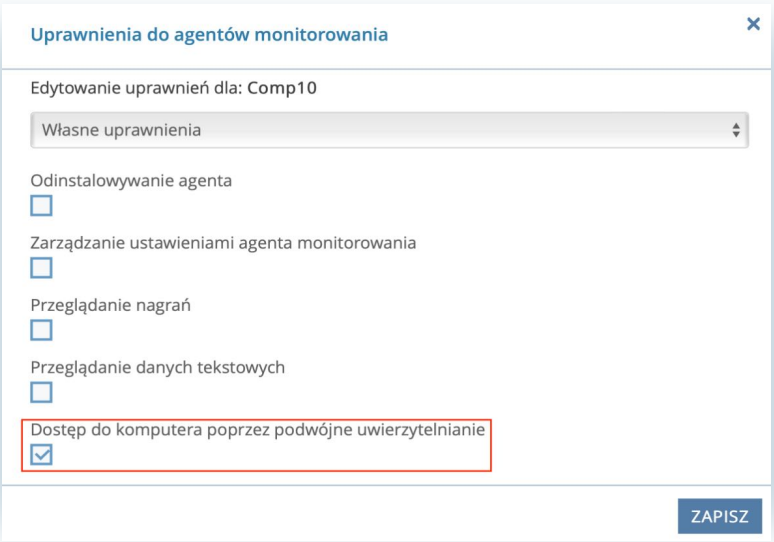
Następnie należy określić użytkowników, którzy będą mogli zalogować się do tego punktu końcowego po wprowadzeniu dodatkowych danych uwierzytelniających.

Konfiguracja dodatkowego uwierzytelniania dla użytkownika

> ***Uwaga:*** *Aby zachować odpowiednie bezpieczeństwo krytycznych serwerów, dostęp do nich powinien być tylko dla administratorów systemu. Zwykli użytkownicy nie powinni mieć dostępu do takich punktów końcowych.*

Zobaczmy, jak można dodać nowego użytkownika do Ekran System i włączyć dodatkowe uwierzytelnianie:

1. Otwórz stronę **Zarządzanie użytkownikami**.
2. Kliknij przycisk **Dodaj użytkownika** i wybierz typ użytkownika (Użytkownik wewnętrzny lub użytkownik Active Directory).
3. Wypełnij informacje o użytkowniku.
4. Przejdź do zakładki **Uprawnienia** i kliknij przycisk **Edytuj uprawnienia dla klienta lub grupy klientów**, dla których chcesz włączyć dodatkowe uwierzytelnianie.
5. W otwartym oknie zaznacz opcję **Dostęp do komputera poprzez podwójne uwierzytelnianie.**



Rys. 13 Aktywowanie opcji podwójnego uwierzytelniania

Jeśli pracownik zrezygnuje z pracy w organizacji, upewnij się, że został usunięty odpowiadający mu użytkownik Ekran System. Jeśli posiadał on konto użytkownika domenowego, należy je zablokować w Active Directory. W ten sposób upewnisz się, że odchodzący pracownik nie będzie miał dostępu do chronionego punktu końcowego poprzez konto współdzielone, nawet jeśli zna do niego login i hasło.

3. UWIERZYTELNIANIE WIELOSKŁADNIKOWE: ZAPOBIEGANIE NIEAUTORYZOWANEMU DOSTĘPOWI

Uwierzytelnianie wieloskładnikowe (MFA) jest złotym standardem cyberbezpieczeństwa i wymogiem wielu regulacji IT, w tym NIST SP 800-53 i PCI DSS. Microsoft sugeruje nawet, że MFA może pomóc powstrzymać ponad 99% ataków na konta. Tak więc nie jest zaskoczeniem, że wiele organizacji polega na tej metodzie uwierzytelniania, aby chronić krytyczne dane i systemy przed nieautoryzowanym dostępem.
Jeśli to możliwe, rozważ włączenie MFA dla wszystkich użytkowników z dostępem do infrastruktury IT, niezależnie od poziomu ich przywilejów.

Użyj tej funkcji, kiedy potrzebujesz:

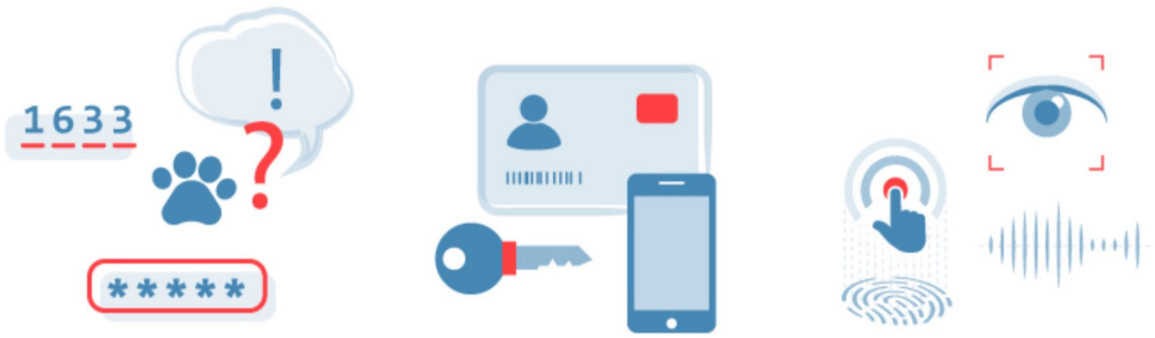
- Zwiększyć ochronę wrażliwych danych i zasobów

Obsługiwane usługi uwierzytelniania:

- Google Authenticator
- Microsoft Authenticator

Jeśli nie możesz włączyć MFA dla wszystkich użytkowników, zacznij od pracowników, którzy mają dostęp do wrażliwych danych oraz krytycznych systemów i usług: menedżerów wyższego szczebla, specjalistów z działu księgowości, administratorów systemów itd. MFA zazwyczaj opiera się na wykorzystaniu dwóch z trzech dowolnych czynników, dlatego też jest często nazywane uwierzytelnianiem dwuskładnikowym (2FA):

3 rodzaje zabezpieczeń w MFA



Wiedza | Własność | Dziedziczenie

Ekran System zapewnia Ci funkcjonalność 2FA, która wykorzystuje dwa czynniki:

- Wiedza - login i hasło do Twojego konta
- Kod - jednorazowy wysyłany na Twoje zweryfikowane urządzenie mobilne.

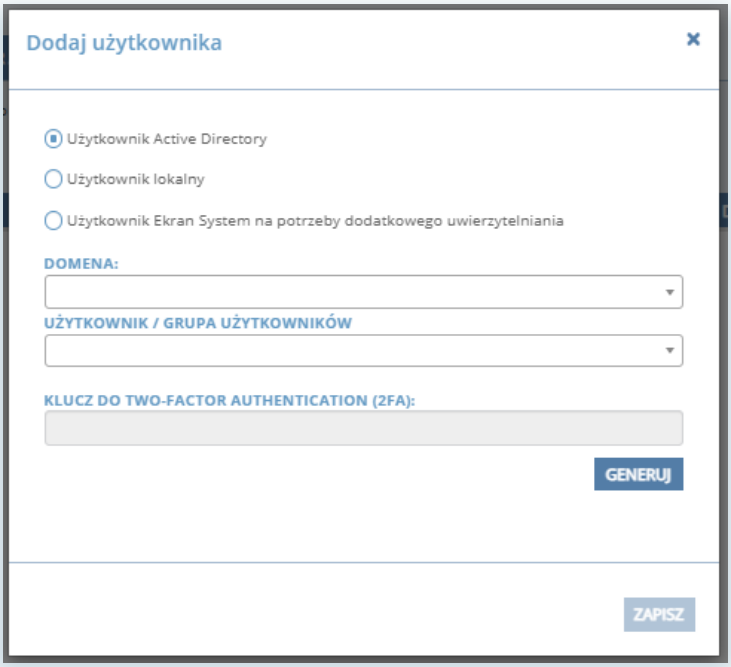
Czynnik kodu sprawdzany jest za pomocą popularnych, wiarygodnych aplikacji uwierzytelniających: Google Authenticator (dla urządzeń z systemem Android) lub Microsoft Authenticator (dla urządzeń z systemem iOS). Zobaczmy, jak w prosty sposób można skonfigurować 2FA dla klientów Ekran System.

Konfiguracja uwierzytelniania wieloskładnikowego

Konfiguracja tej funkcji odbywa się w dwóch krokach. Najpierw należy dodać użytkownika uwierzytelniania dwuskładnikowego do systemu. Następnie, należy włączyć 2FA dla konkretnego klienta Ekran System.

Zacznijmy od pierwszego kroku i dodajmy użytkownika uwierzytelniania dwuskładnikowego do systemu:

1. W **Konsoli zarządzania**, otwórz stronę **Zarządzanie dostępem**.
2. Przejdź do zakładki **Uwierzytelnianie dwuskładnikowe** i kliknij przycisk **Dodaj użytkownika**.

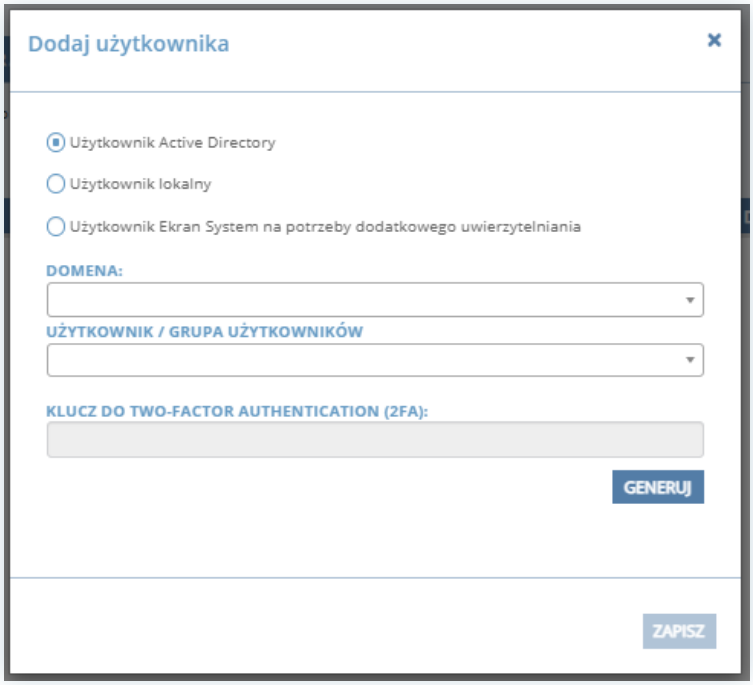


Rys. 14 Dodawanie nowego użytkownika

3. Wybierz typ użytkownika spośród dostępnych opcji.

4. Wypełnij pola **Domena** i **Użytkownik / Grupa użytkownika** odpowiednimi informacjami.

5. Kliknij przycisk **Utwórz**.



Rys. 15 Generowanie kodu weryfikacji dla użytkownika

6. Na urządzeniu mobilnym zeskanuj wygenerowany kod QR w obsługiwanej aplikacji uwierzytelniającej.

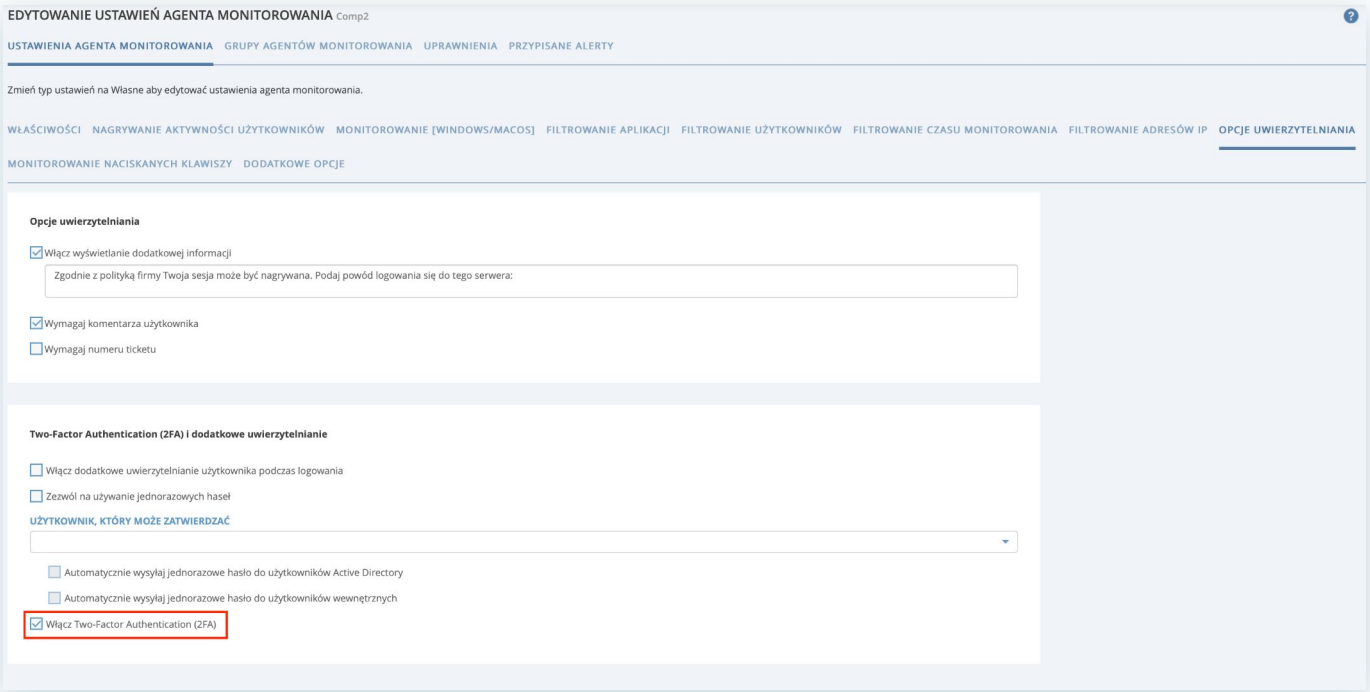
7. Kliknij przycisk **Zapisz**, aby zapisać zmiany.

Następnie należy włączyć 2FA dla docelowego agenta Ekran System:

1. W Konsoli zarządzania, otwórz stronę **Zarządzanie klientami monitorowania**.

2. Kliknij przycisk **Edytuj klienta** dla klienta, dla którego chcesz włączyć 2FA.

3. Otwórz kartę Opcje uwierzytelniania i zaznacz opcję **Włącz 2FA**.



Rys. 16 Aktywowanie 2FA dla danego agenta

4. Zapisz zmiany i wyjdź.

Po tej operacji Ekran System będzie wymagał, aby użytkownik z uwierzytelnianiem dwuskładnikowym, którego dodaliśmy do systemu w pierwszym kroku, przechodził dodatkową weryfikację podczas każdego logowania do tego Klienta.

4. KONTROLA DOSTĘPU DO PUNKTÓW KOŃCOWYCH: WYŁĄCZENIE DOSTĘPU POZA GODZINAMI PRACY DO KRYTYCZNYCH PUNKTÓW KOŃCOWYCH

Zazwyczaj organizacje szybko reagują na podejrzane zdarzenia, które mają miejsce w godzinach pracy, ponieważ mają wystarczającą liczbę specjalistów ds. cyberbezpieczeństwa, aby je zbadać. Jednak poza godzinami pracy, znacznie trudniej jest im zapewnić właściwy monitoring i szybkie reagowanie na incydenty. Dlatego też hakerzy często przeprowadzają ataki w nocy lub w weekendy.

Użyj tej funkcji, kiedy potrzebujesz:

- Wzmocnić bezpieczeństwo krytycznych danych
- Zapobiegać incydentom cyberbezpieczeństwa

Ekran System posiada funkcję Kontroli Dostępu do Punktów Końcowych, która pozwala na ograniczanie dostępu do poszczególnych punktów końcowych w godzinach wolnych od pracy, np. w dni powszednie i weekendy. Po włączeniu tej funkcji, użytkownik nie będzie mógł uzyskać dostępu do chronionego punktu końcowego poza godzinami pracy bez wcześniejszego uzyskania osobistej zgody specjalisty ds. bezpieczeństwa IT.

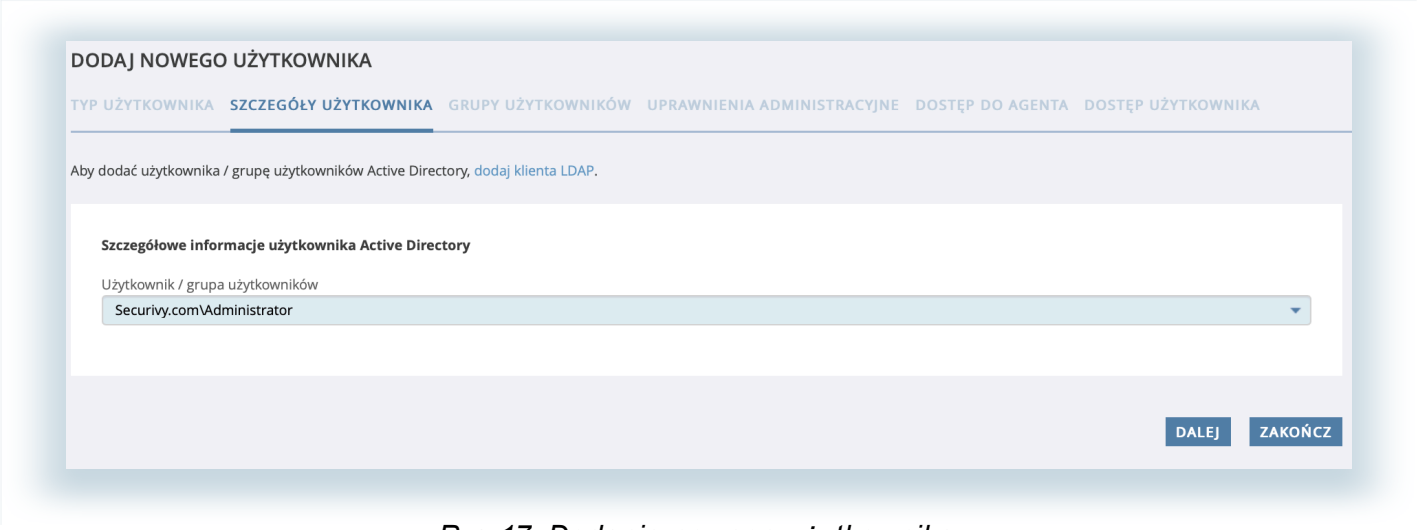
> ***Uwaga:*** *Szczególnie ważne jest, aby takie ograniczenia dostępu skonfigurować dla kont z uprzywilejowanym dostępem do krytycznych punktów końcowych i systemów: administratorzy domen (w Windows) i konta administratorów (w Linux). W godzinach wolnych od pracy dostęp do tych kont powinien być zapewniony tylko po uzyskaniu zgody specjalisty ds. bezpieczeństwa IT.*

Poniżej opisujemy krok po kroku proces konfiguracji tej funkcji.

Konfiguracja kontroli dostępu do punktów końcowych

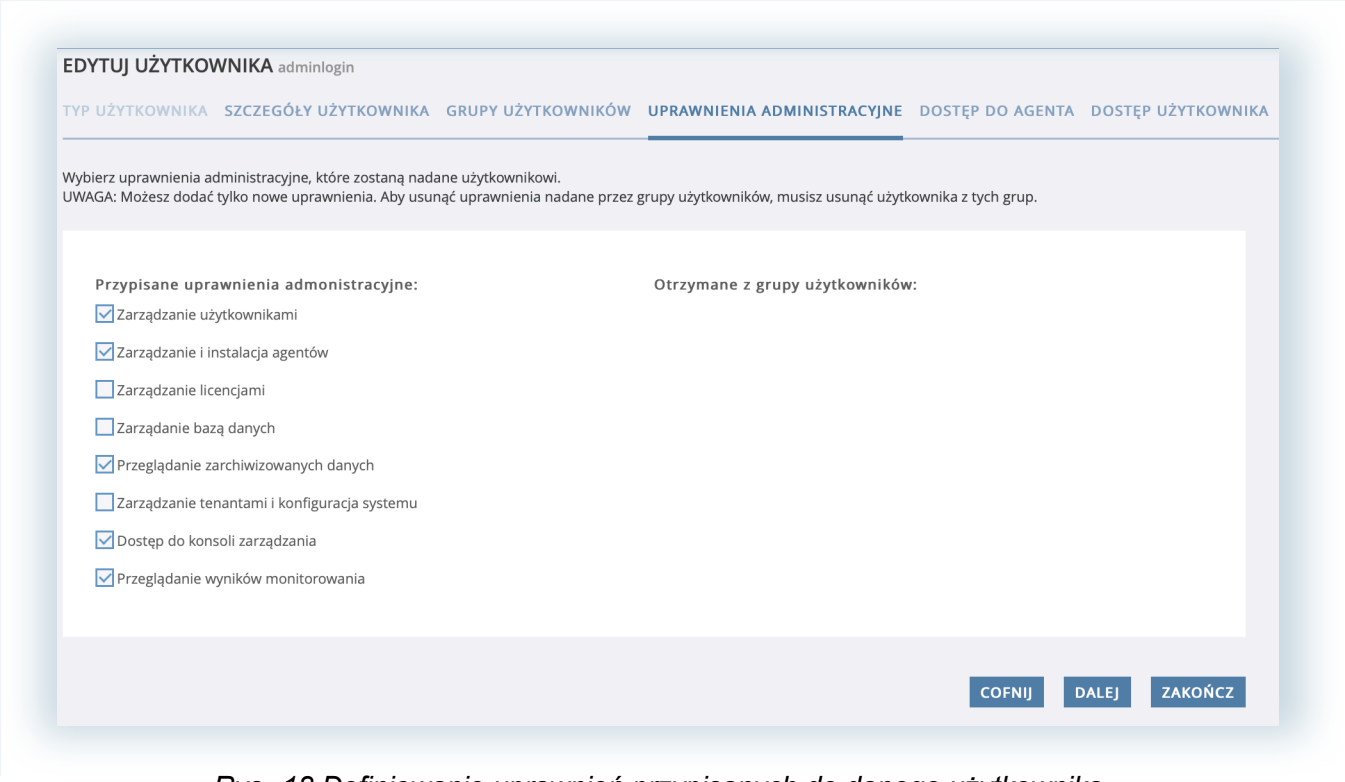
Aby ustawić czasowe ograniczenia dostępu, należy określić użytkowników, którzy mogą zatwierdzać żądania dostępu otrzymane w godzinach wolnych od pracy i utworzyć regułę dostępu do punktów końcowych dla konkretnego użytkownika lub grupy. Zacznijmy od zdefiniowania użytkowników, którzy mogą zatwierdzać żądania dostępu:

1. W **Konsoli zarządzania** otwórz stronę **Zarządzanie użytkownikami** i kliknij przycisk **Dodaj użytkownika**.



Rys. 17. Dodanie nowego użytkownika

2. Dodaj użytkownika i zdefiniuj jego uprawnienia.



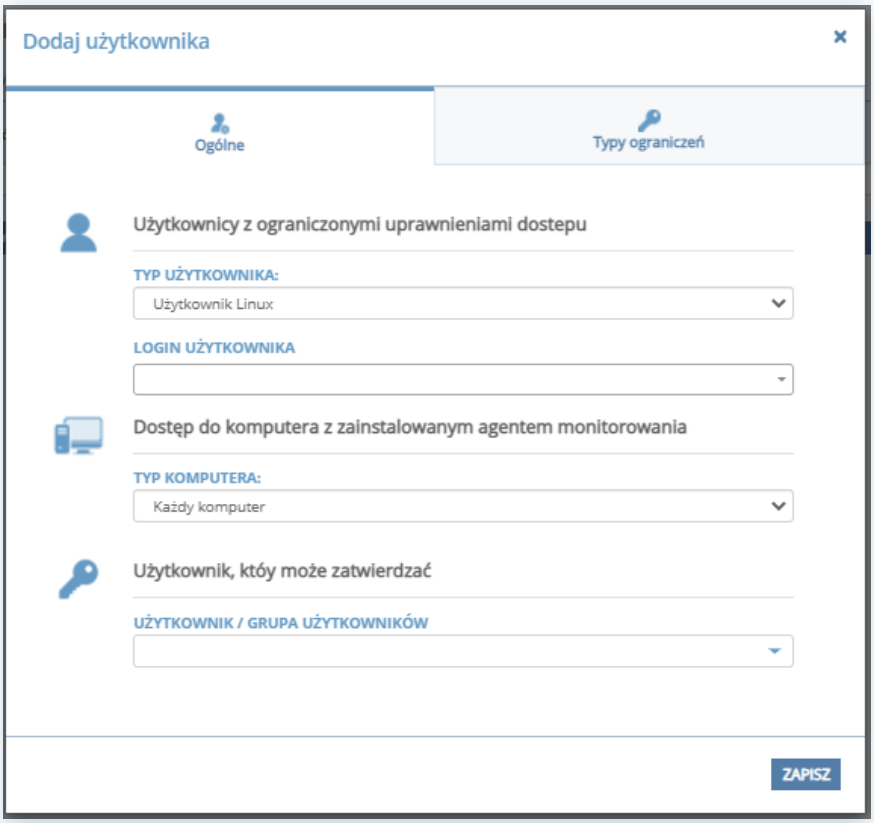
Rys. 18 Definiowanie uprawnień przypisanych do danego użytkownika

3. Kliknij przycisk Zakończ, aby zapisać zmiany i wyjść.

Następnie można przejść do **konfigurowania reguły dostępu do punktów końcowych:**

1. W **Konsoli zarządzania** otwórz stronę **Zarządzanie dostępem**.

2. Otwórz kartę **Kontrola dostępu do punktów końcowych** i kliknij przycisk **Dodaj użytkownika**.



Rys. 19 Ogólna konfiguracja dostępu do punktu końcowego

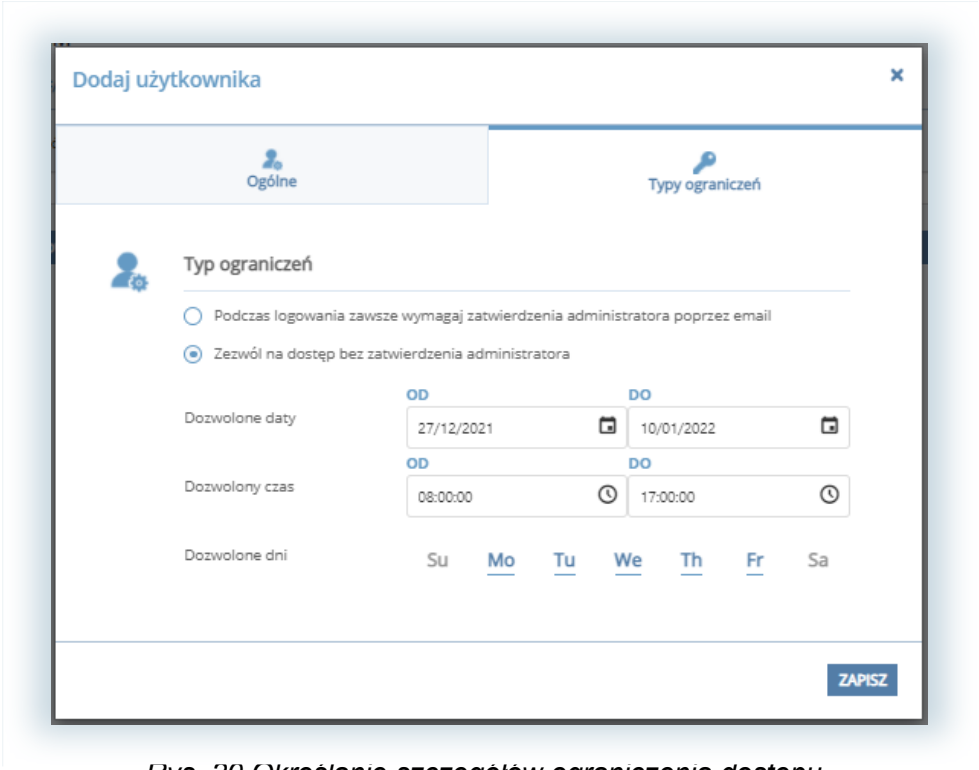
3. Wybierz **typ użytkownika**.

4. Aby ustawić regułę dla konkretnego użytkownika, wprowadź jego login.

5. W sekcji **Dostęp do komputera z zainstalowanym agentem monitorowania** wybierz typ komputera. Zalecamy wybranie opcji **Każdy komputer**.

6. W sekcji **Użytkownicy**, zdefiniuj tych, którzy mogą zatwierdzać żądania dostępu otrzymane w godzinach wolnych od pracy od użytkownika z ograniczonymi prawami dostępu.

7. Przejdź na kartę **Rodzaje ograniczeń** i zaznacz opcję **Dostęp bez ograniczeń w czasie pracy**.



Rys. 20 Określanie szczegółów ograniczenia dostępu

8. Użyj opcji **Dozwolone daty**, aby zdefiniować daty, kiedy użytkownicy mogą uzyskać dostęp do tego punktu końcowego bez zatwierdzenia. Po wygaśnięciu dozwolonych dat, zatwierdzenie będzie wymagane w każdym momencie.

9. Użyj opcji **Dozwolone dni tygdnia**, aby zdefiniować dni, w których dostęp może być dozwolony bez zatwierdzenia.

10. Zapisz zmiany i wyjdź.

Na zrzucie ekranu 20 widać skonfigurowaną regułę dostępu do punktów końcowych, która zezwala użytkownikowi na zalogowanie się do systemu wyłącznie w godzinach pracy (od 8 do 17) od poniedziałku do piątku. Aby uzyskać dostęp do systemu poza tymi ramami czasowymi, użytkownik musi wysłać prośbę o akceptację.

Zdefiniowany uprzednio administrator otrzymuje prośbę (na określony adres e-mail) od użytkownika, który potrzebuje dostępu. Wówczas może on odrzucić lub zaakceptować taki wniosek. W ten sposób dostęp do chronionego punktu końcowego jest w pełni kontrolowany i zarządzany przez wyznaczonego administratora. Bez jego bezpośredniej zgody, użytkownik nie będzie mógł się zalogować do systemu.

5. ZARZĄDZANIE ALERTAMI: BLOKADA DOSTĘPU DLA NIEZAUFANYCH UŻYTKOWNIKÓW

Skuteczną strategią zabezpieczenia danych i systemów jest ograniczenie dostępu do nich dla wszystkich nieuwierzytelnionych użytkowników. Istnieje kilka sposobów, w jaki niezaufany użytkownik może pojawić się w Twojej sieci:

- Domyślne konto administratora nie zostało prawidłowoskonfigurowane lub usunięte z systemu
- Lokalne konto użytkownika nie zostało zlikwidowane po rezygnacji pracownika.
- Pracownik utworzył nowe konto użytkownika, aby później użyć go jako tylnych drzwi.

Użyj tej funkcji, kiedy potrzebujesz:

- Zezwolić na dostęp do zasobów wyłącznie grupie zaufanych użytkowników
- Automatyzacji reakcji na incydenty

Szczególnie trudno jest wykryć obecność takich kont na punktach końcowych, które nie są kontrolowane przez kontroler domeny lub system wykrywania kont. Ekran System jest wyposażony w mechanizm, który może ułatwić to zadanie. Dzięki niemu można otrzymać powiadomienie o rozpoczęciu podejrzanej sesji użytkownika i w razie potrzeby zablokować ją w czasie rzeczywistym.

Można również użyć funkcji zarządzania alertami do ograniczenia dostępu do najbardziej krytycznych punktów końcowych tylko dla wąskiego grona zaufanych użytkowników.

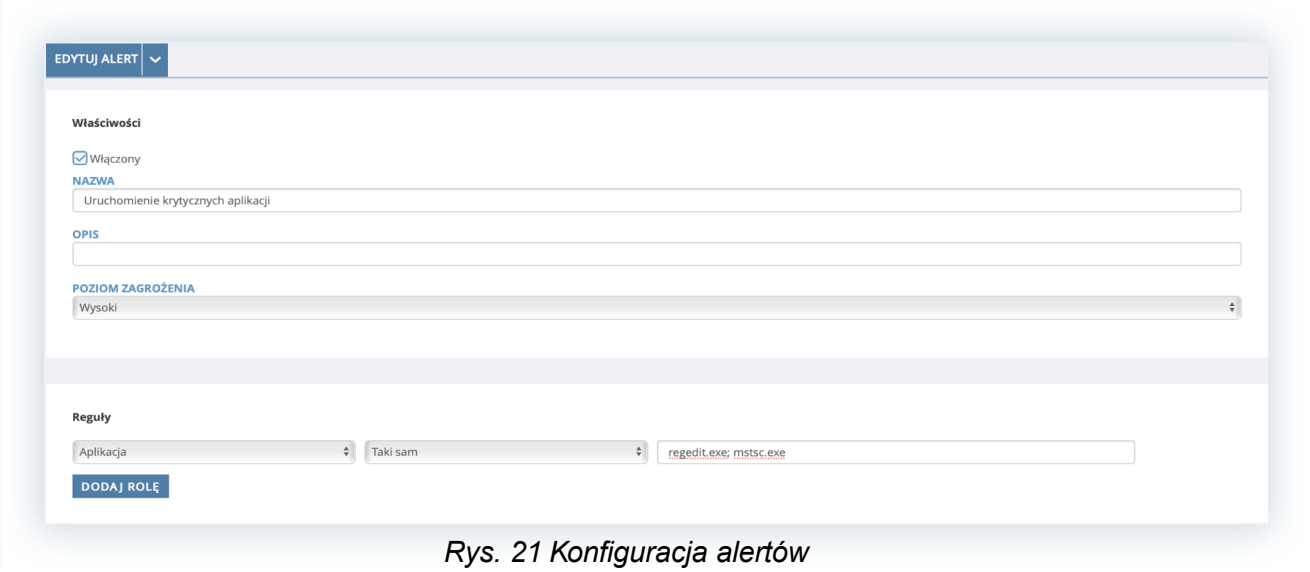
Zobaczmy, jak można uniemożliwić niezaufanym użytkownikom dostęp do określonego punktu końcowego.

Trudniej jest wykryć złośliwe działania, jeśli są one wykonywane przez osobę z legalnym dostęp do infrastruktury. Według raportu Cybersecurity Insiders prawie 70% organizacji czuje się narażonych na ataki insiderów.

Konfigurowanie blokowania sesji niezaufanych użytkowników

Aby zabezpieczyć krytyczne dane i systemy przed niezaufanymi użytkownikami, należy utworzyć alert z **funkcją automatycznego blokowania niezaufanych sesji**.

1. W **Konsoli zarządzania** otwórz stronę **Zarządzanie alertami.**
2. Kliknij przycisk **Dodaj alert** i zaznacz opcję **Włącz**.
3. Wprowadź nazwę dla tego alertu.
4. Zdefiniuj reguły:
   a. W pierwszym polu zdefiniuj **Nazwę użytkownika**.
   b. Wybierz opcję **Nie równa się** w drugim polu.
   c. Zdefiniuj nazwy użytkowników zaufanych w trzecim polu. Można dodać kilka nazw użytkowników oddzielonych średnikami.



Rys. 21 Konfiguracja alertów

5. Wybierz opcję **Agenci monitorowania** lub **Grupy agentów monitorowania**.
6. Przejdź do zakładki **Opcje alertu** i wybierz opcję **Pokaż ostrzeżenie użytkownikowi**.
7. W sekcji **Dodatkowe akcje** zaznacz opcję **Zablokuj użytkownika na wszystkich komputerach.**

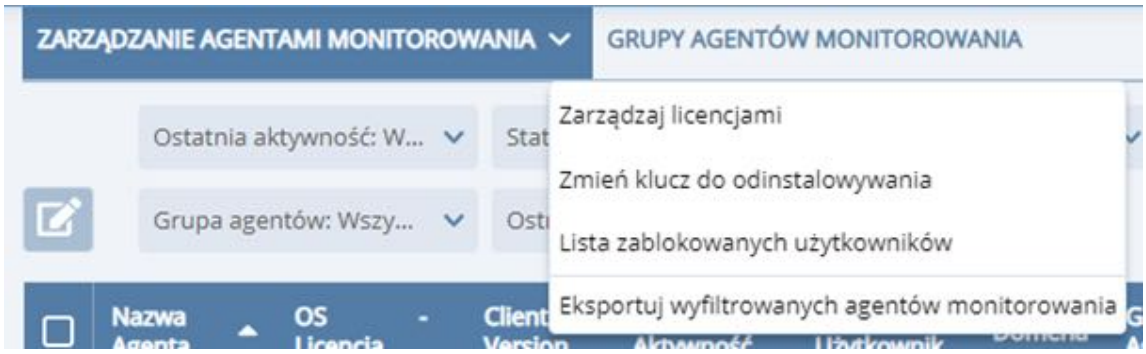
Rys. 22 Konfiguracja alertów

8. Aby otrzymywać powiadomienia e-mail w przypadku wyzwolenia alarmu, wybierz opcję **Wyślij e-mail do...** i wprowadzić adresy e-mail, na które mają być wysyłane powiadomienia.
9. Kliknij przycisk **Zakończ**, aby zapisać zmiany.

Po zapisaniu tej reguły tylko określeni użytkownicy będą mogli logować się do wybranych **Klientów**. Dla pozostałych użytkowników dostęp do tych **Klientów będzie zablokowany**.

Możesz również przejrzeć listę wszystkich użytkowników, którym zablokowano dostęp do danego Klienta w **Konsoli zarządzania**:

1. Przejdź do strony **Zarządzanie agentami monitorowania** i otwórz listę rozwijaną.
2. Wybierz listę zablokowanych użytkowników.



Rys. 23 Dostęp do listy zablokowanych użytkowników

Możesz usunąć użytkownika z listy zablokowanych użytkowników, co umożliwi mu dostęp do tego konkretnego klienta lub grupy klientów. Ale dopóki tego nie zrobisz, taki użytkownik pozostanie niezaufany i nie będzie mógł się zalogować do chronionego punktu końcowego.

PODSUMOWANIE

Aby zapewnić efektywne zarządzanie dostępem uprzywilejowanym, organizacje muszą zadbać o kilka kwestii:

- Bezpieczny uprzywilejowany dostęp dla użytkowników
- Monitorowanie i zarządzanie aktywnością w ramach kont współdzielonych
- Ograniczenie dostępu do krytycznych danych i systemów
- Ograniczenie dostępu do zasobów firmy poza godzinami pracy
- Zablokowanie dostępu dla niezaufanych użytkowników

Ekran System zapewnia solidną funkcjonalność, która może pomóc Ci skutecznie zrealizować każde z tych zadań. Powyżej omówiliśmy podstawowe możliwości i proces konfiguracji pięciu najważniejszych funkcji związanych z zarządzaniem dostępem:

- Menedżer haseł
- Wtórne uwierzytelnianie
- Podwójne uwierzytelnianie
- Kontrola dostępu dla punktów końcowych
- Zarządzanie alertami

Proces wdrożenia i konfiguracji Ekran System jest prosty i intuicyjny.

Ekran System to nie tylko niezwykle wydajna, ale także łatwa w użyciu platforma do zarządzania ryzykiem wewnętrznym i zewnętrznym.

Zarządzaj dostępem uprzywilejowanym już teraz!
Odwiedź www.ekransystem.com/pl i skorzystaj z wersji demo

EKRAN SECURIVY