EKRAN®

SECURIVY

Ekran System

Podsumowanie funkcjonalności oprogramowania

Spis treści//zawartość

O programie

System inteligentnego nagrywania sesji użytkownika

Monitorowanie aktywności użytkowników uprzywilejowanych

Ekran System pozwala na równoczesne tworzenie indeksowanych nagrań na serwerach Windows, Citrix i Linux. Zapisuje wszystkie sesje serwerowe, zdalne i lokalne na stacjach roboczych, a także systemach MacOS.

Nadzór pracy użytkownika

Jesteś zainteresowany bezpieczeństwem swojej firmy?
Chcesz wiedzieć, co w godzinach pracy robią Twoi pracownicy?
Chcesz kontrolować dostęp do wrażliwych danych?

Zarządzanie hasłami i uprzywilejowanym dostępem

Ekran System pomoże Ci przydzielać uprzywilejowany dostęp do zasobów krytycznych i dostosować wymagania zabezpieczenia, zarządzania oraz monitorowania uprzywilejowanych kont i dostępu.

Elastyczne wdrażanie i licencjonowanie

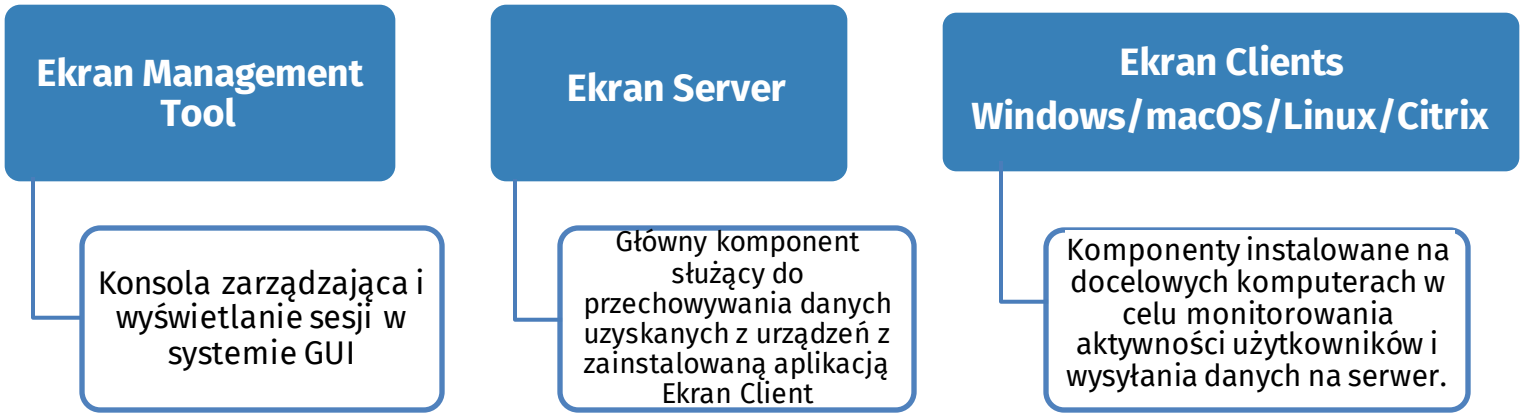
Ekran System obsługuje najszerszą gamę platform i konfiguracji infrastruktury, zapewniając niezawodne wdrożenia dowolnej wielkości, od dziesiątek do dziesiątek tysięcy punktów końcowych. Elastyczne licencjonowanie pomaga dostosować się do budżetu i zmian w projekcie.

O programie

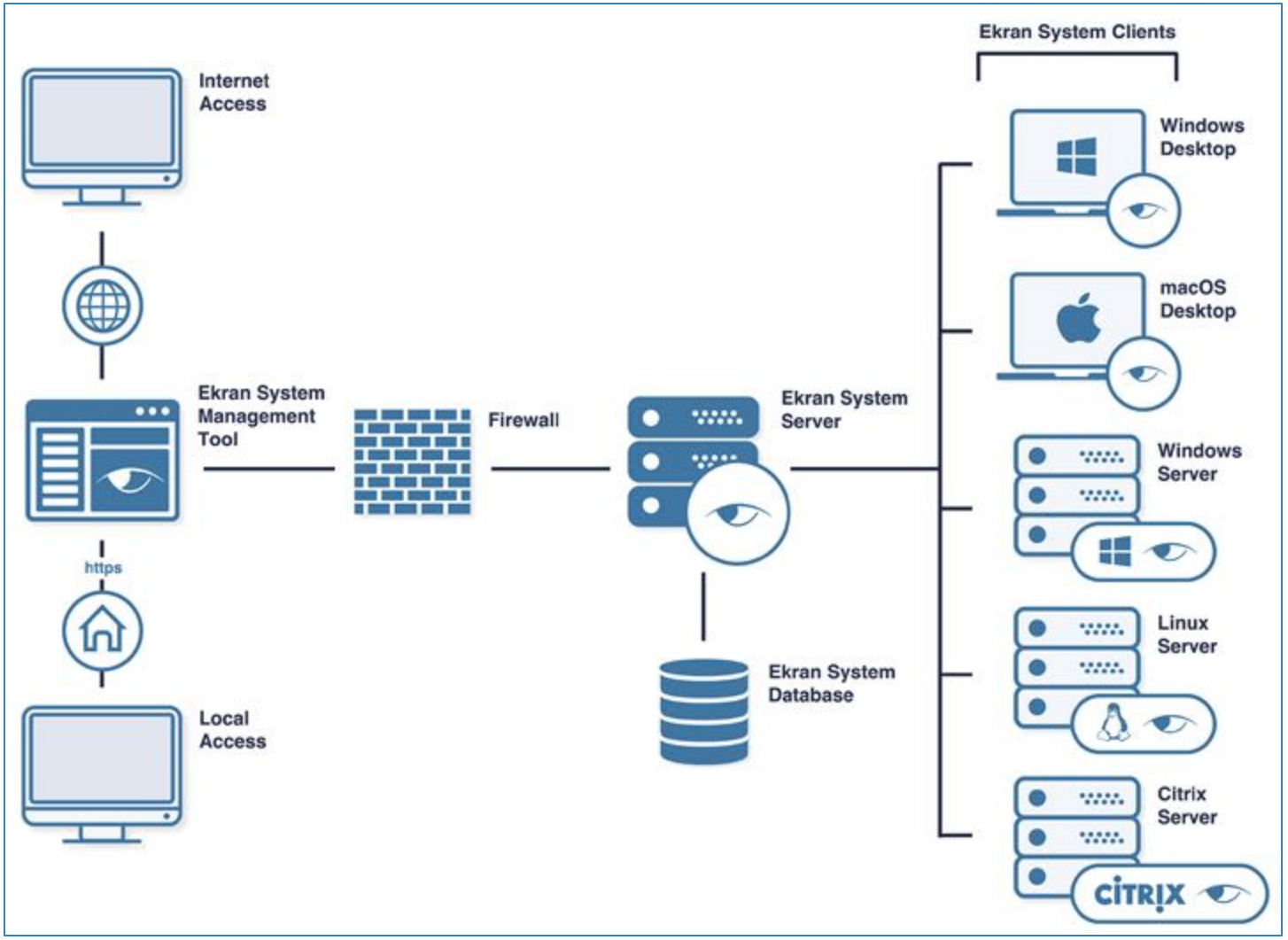
Ekran System jest rozwiązaniem monitorującym użytkowników, które podnosi poziom bezpieczeństwa IT. Służy do powstrzymywania, wykrywania i przerywania zagrożeń wewnętrznych w korporacyjnej infrastrukturze IT, a także pomaga w spełnieniu wymogów dotyczących zachowania zgodności, zarządzaniu uprzywilejowanymi użytkownikami (PAM) itp.

Oprogramowanie umożliwia nagrywanie wszystkich sesji terminalowych, zdalnych oraz użytkowników lokalnych. Dodatkowo może ostrzegać Administratorów o podejrzanej aktywności.

Komponenty Ekran System



Podstawowy schemat wdrożenia Ekran System

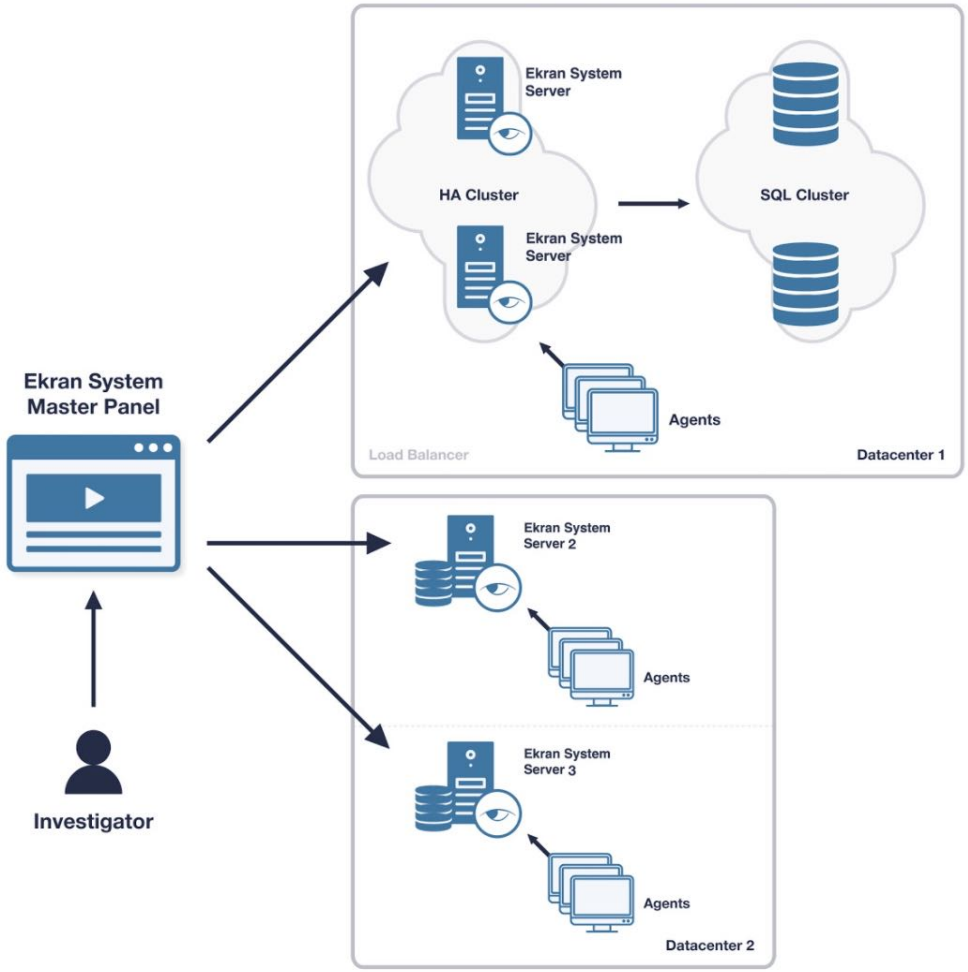


Wdrażanie na dużą skalę

Pod względem skalowalności oraz dużych organizacji, które mogą mieć kilka geograficznie odizolowanych centrów danych, można wdrożyć wiele połączonych instancji serwera aplikacji.

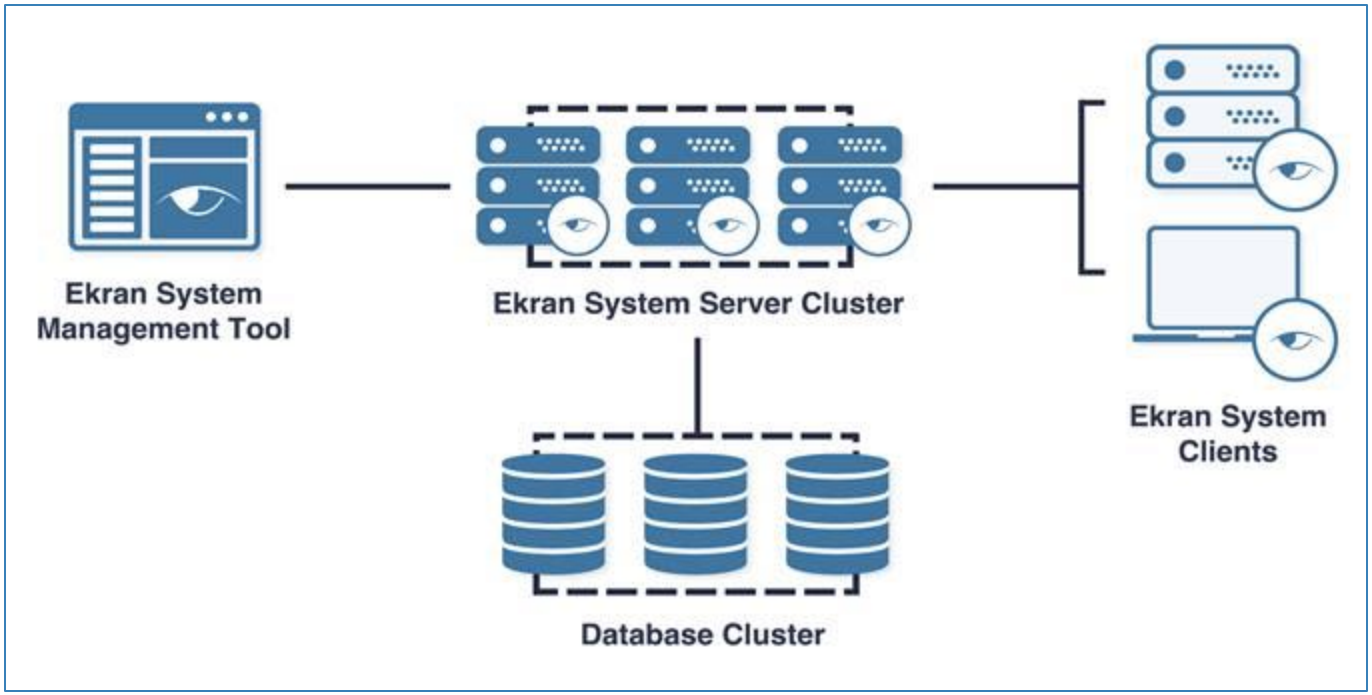
W przypadku złożonych wdrożeń Ekran System oferuje również tryb **High Availability** i **Disaster Recovery** oraz tryb **Multi-Tenant**, a także wspera wykorzystanie oprogramowania **load balancer** innych firm.

Master Panel, który jest dodatkowym samodzielnym komponentem Ekran System, łączy dane ze wszystkich serwerów aplikacji Ekran System w wielu lokalizacjach, umożliwiając zarządzanie nimi poprzez jeden interfejs użytkownika.



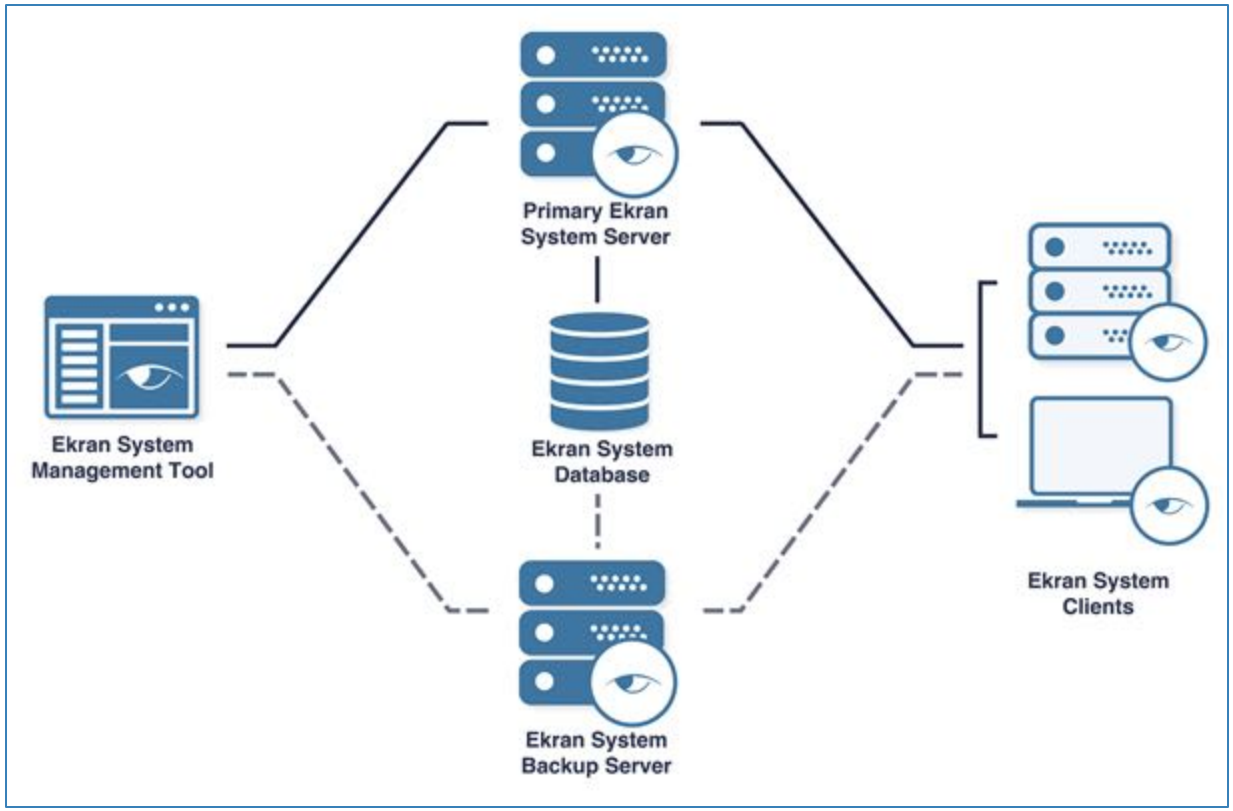
Tryb High Availability (Enterprise Edition)

Tryb High Availability zapewnia wysoki poziom operacyjny i balansuje przesyłanie danych, minimalizuje czas przestoju i zakłóceń serwerowych.



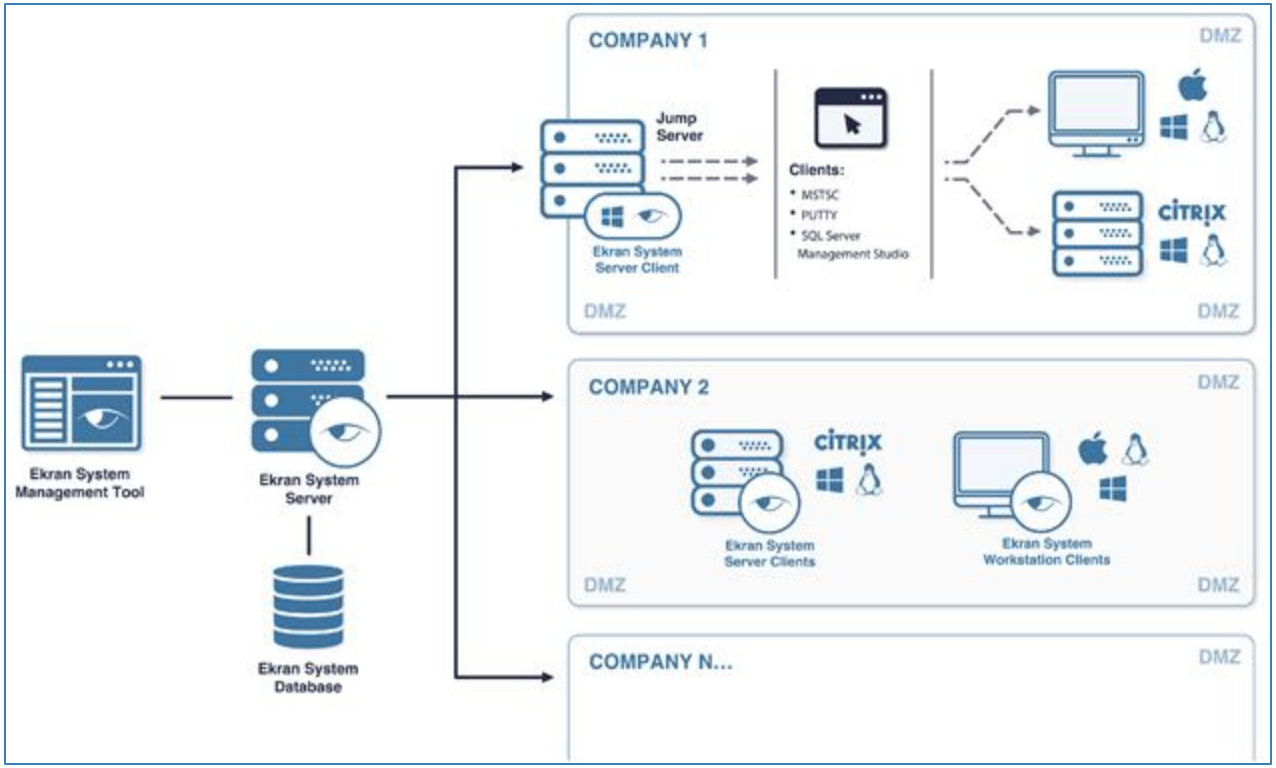
Tryb Disaster Recovery

Tryb Disaster Recovery pozwala na konfigurowanie oraz wdrażanie Ekran System w taki sposób, aby w przypadku przerwania pracy Ekran Server, kolejny serwer mógł go zastąpić bez narażenia na utratę danych i przeinstalowania systemu.



Tryb Single-Tenant/Multi-Tenant

Tryb Multi-tenant pozwala na utworzenie odrębnych środowisk do zarządzania w ramach jednej instancji Ekran System. Dane każdego środowiska są niezależne i niedostępne między sobą.

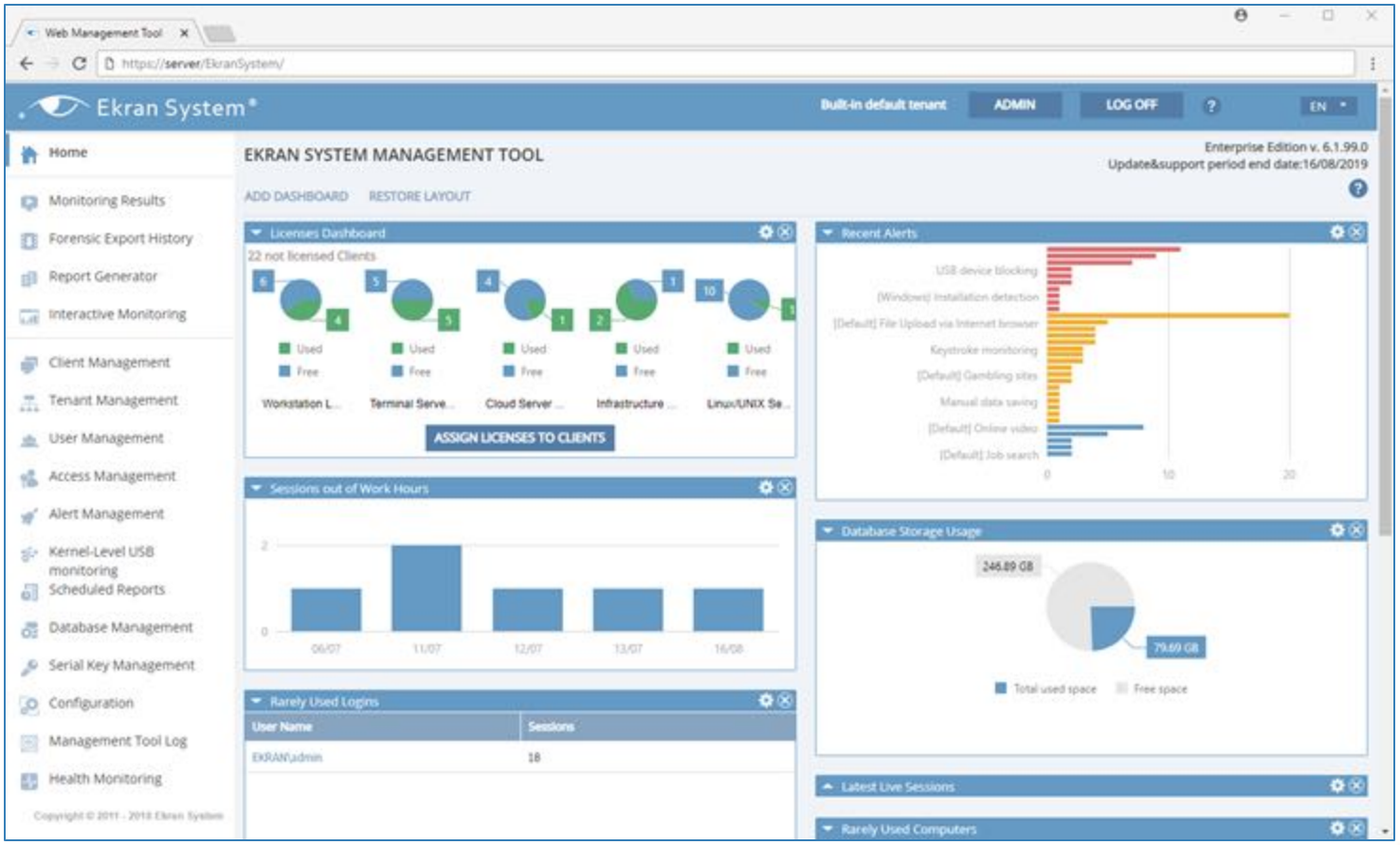


Ekran Server i Management Tool

Zarządzanie użytkownikami, integracja z Active Directory, ustawienia Management Tool

Management Tool

Możliwość zarządzania całym systemem przez Management Tool w przeglądarce internetowej.



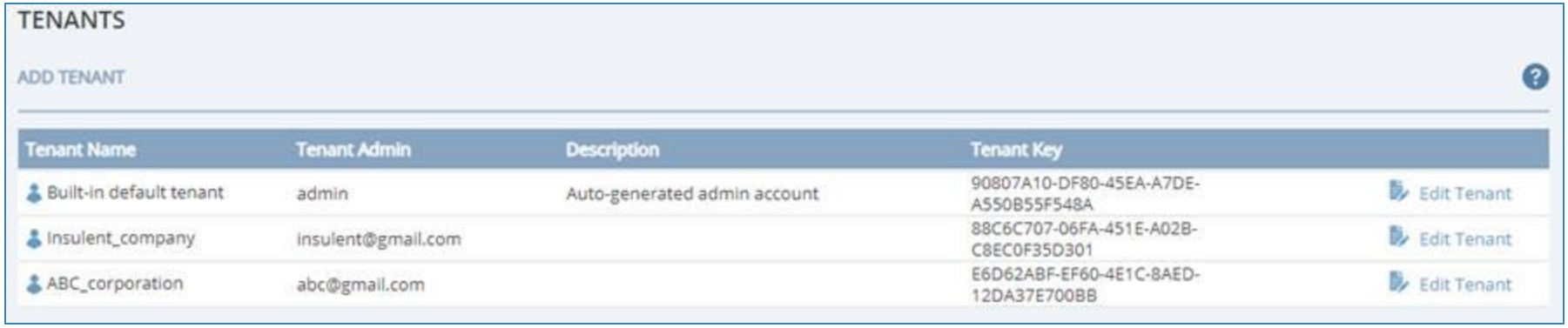
Zarządzanie tenantami

Ekran System posiada dwa tryby pracy **Single-Tenant** i **Multi-Tenant**.

Domyślnie ustawiony jest tryb Single-Tenant. W tym trybie wszyscy użytkownicy mają dostęp do wszystkich oprogramowań Ekran Client i ustawień zgodnych z ich uprawnieniami.

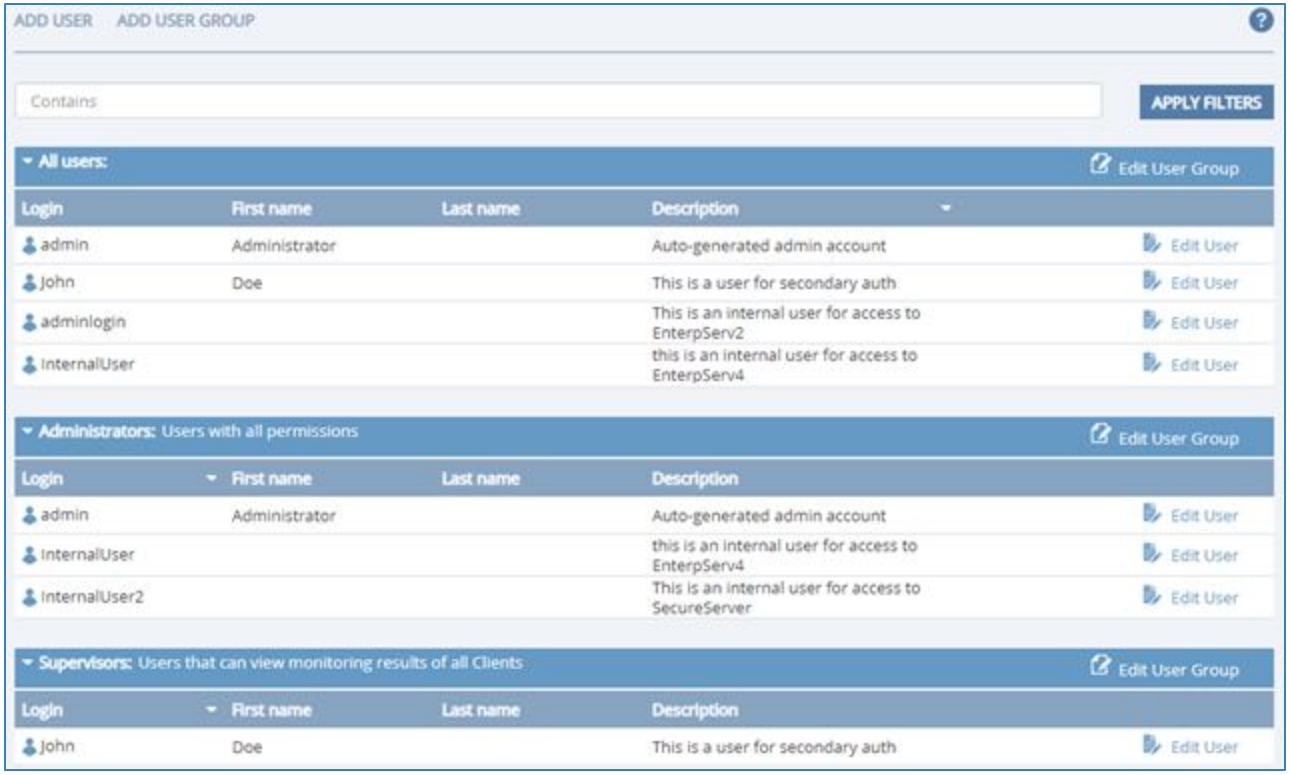
W trybie Multi-Tenant wszyscy użytkownicy tenantu mają dostęp do aplikacji Ekran Client danego środowiska, ale nie mają dostępu do programu Ekran Client innych tenantów, konfiguracji, alertów, raportów itp.

W każdej chwili można przełączyć się do trybu Multi-Tenant.



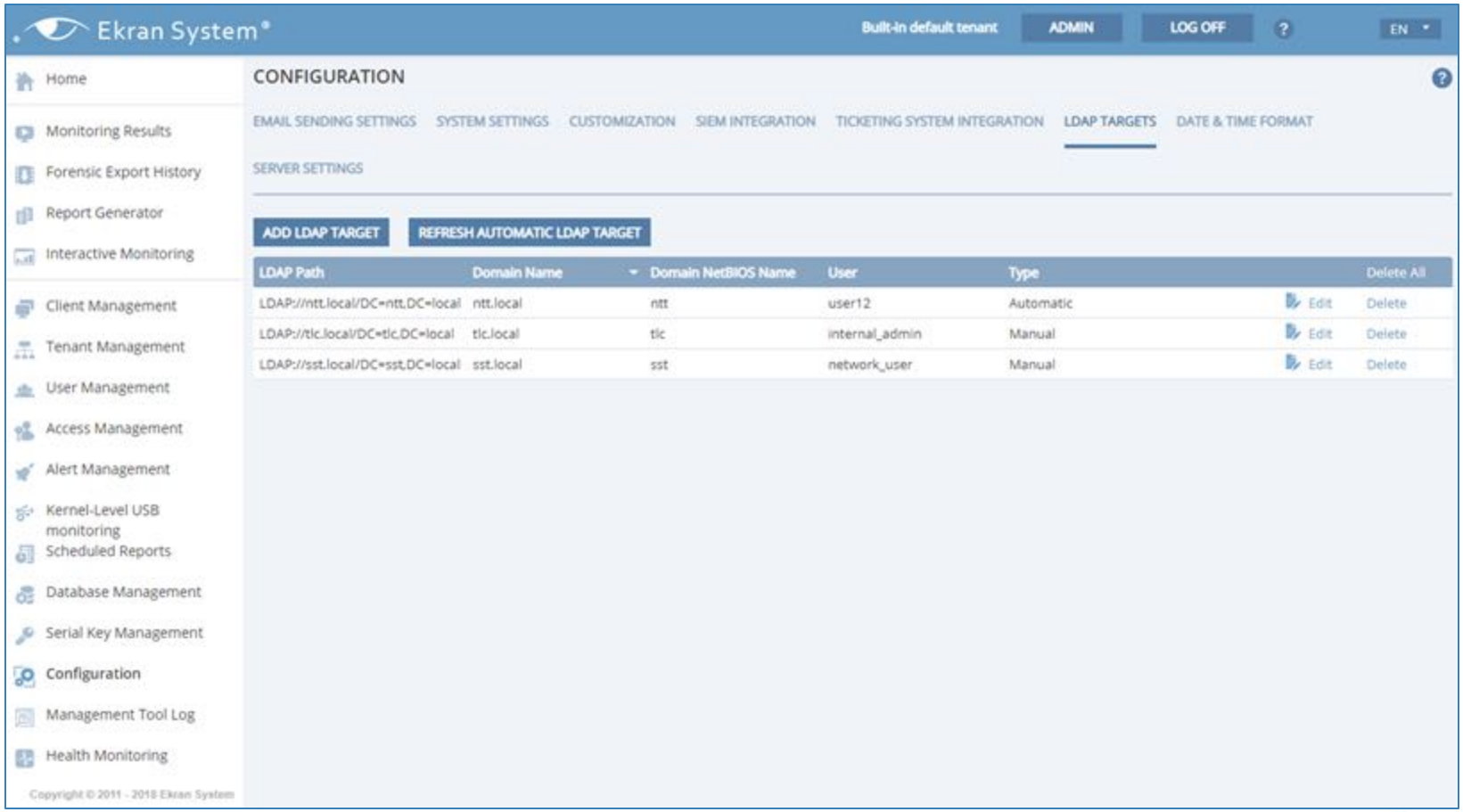
Zarządzanie użytkownikami i uprawnieniami

- Tworzenie dwóch typów użytkowników: **Lokalny** lub **Active Directory** (Windows Domain użytkownik/grupa).
- Budowanie grup użytkowników w celu łatwiejszego zarządzania.
- Możliwość nadawania uprawnień wszystkim użytkownikom.



Integracja z Active Directory

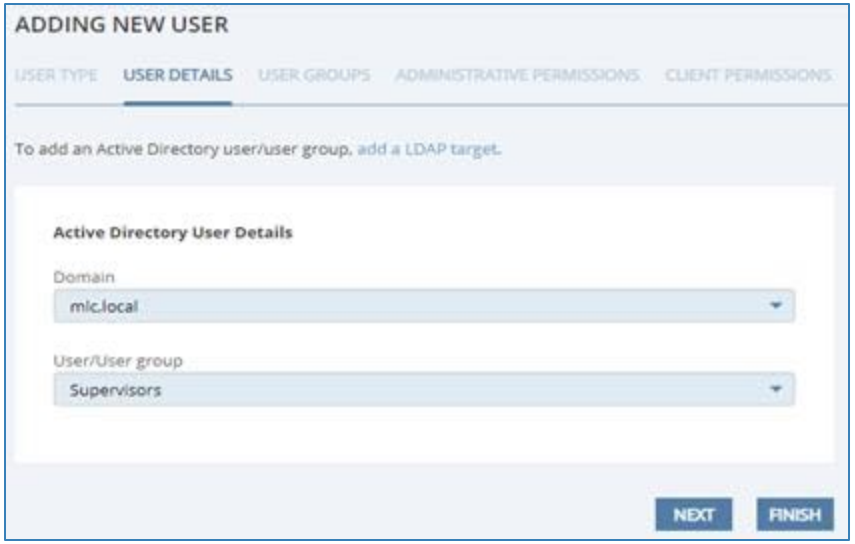
Integracja z Active Directory pozwala na jednoczesne połączenie się z wieloma domenami.



Integracja z Active Directory

Integracja z Active Directory pozwala na:

- Dodawanie **użytkowników i grup użytkowników domen zaufanych** w celu dostępu do Management Tool i komputerów z zainstalowanym oprogramowaniem Ekran Client z włączoną funkcją Forced User Authentication.
- Tworzenie **alertów dla grup domenowych**, celem szybszej reakcji na podejrzaną aktywność użytkownika na komputerach z zainstalowanym oprogramowaniem Ekran Client, należących do domen zaufanych.



Management Tool Log

Audyt wszystkich wykonywanych czynności użytkowników w Management Tool poprzez Management Tool Log ze szczegółowymi informacjami na temat wszystkich zmian.

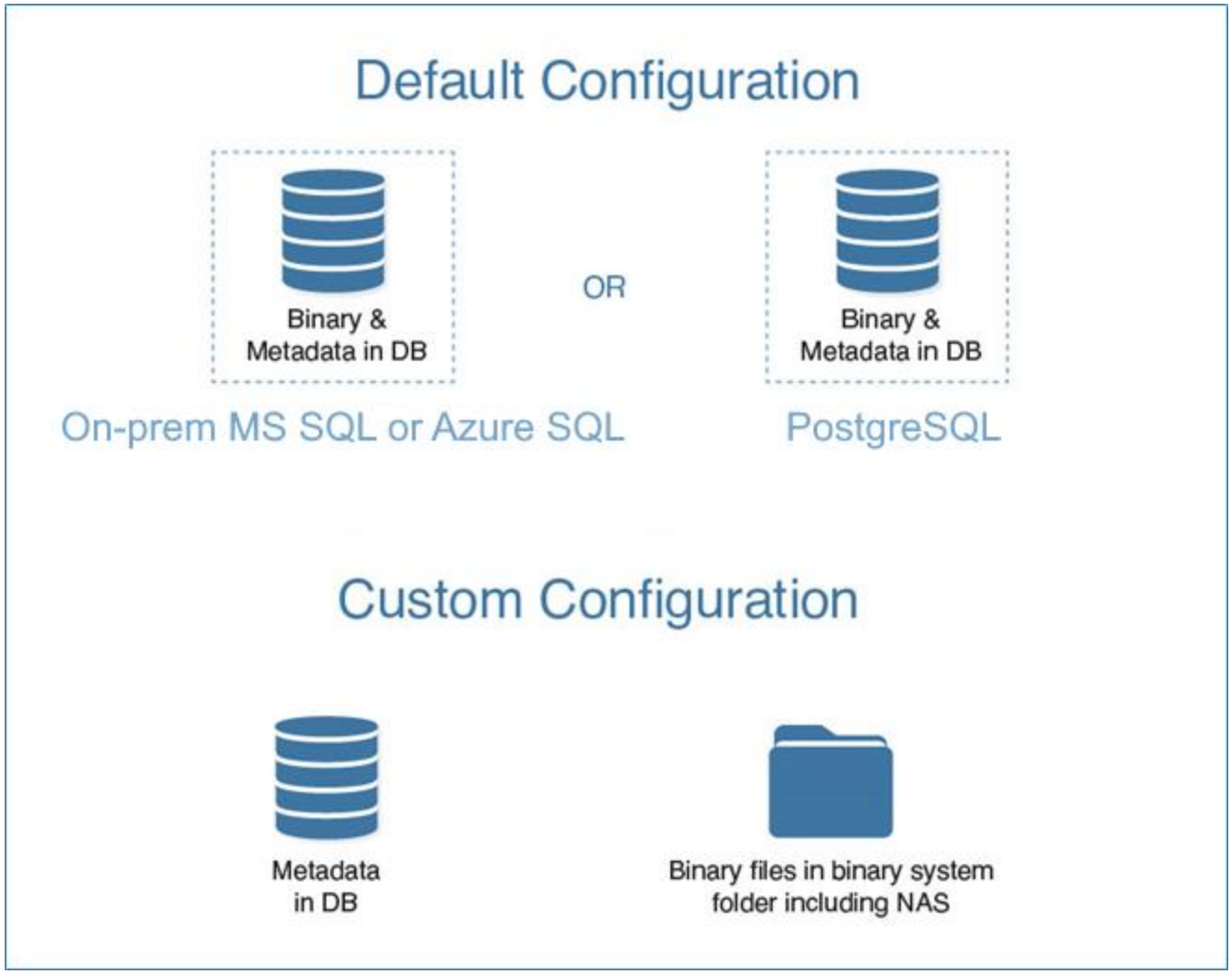
MANAGEMENT TOOL LOG

When: All | Who: All | Action: All | + More criteria

Time	User Name	User Groups	Category	Action	Object	Details
07/11/2018 3:22:54 pm	Administrator	Administrators	Client installation/Uninsta...	Uninstalling	srv-app	Success
07/11/2018 3:24:07 pm	Administrator	Administrators	Alert management	Assigning Clients	File downloa...	**Removed Client Groups:** **Added Client Groups:** **Removed Clients:** **Added Clients:** Comp7
07/11/2018 3:42:31 pm	Administrator	Administrators	User management	Editing description	InternalUser2	Old description: This is an internal user for ac New description: This is an internal user for a
07/12/2018 4:59:22 pm	Administrator	Administrators	Kernel-Level USB monitor...	Editing description	Mass storage...	Old description: New description: This rule is used to block co
07/12/2018 5:29:55 pm	Administrator	Administrators	Kernel-Level USB monitor...	Editing description	Mass storage...	Old description: This rule is used to block cop New description: This rule is used to detect a
07/16/2018 1:19:05 pm	Administrator	Administrators	Client editing	Assigning license	Comp6	License type: Workstation license

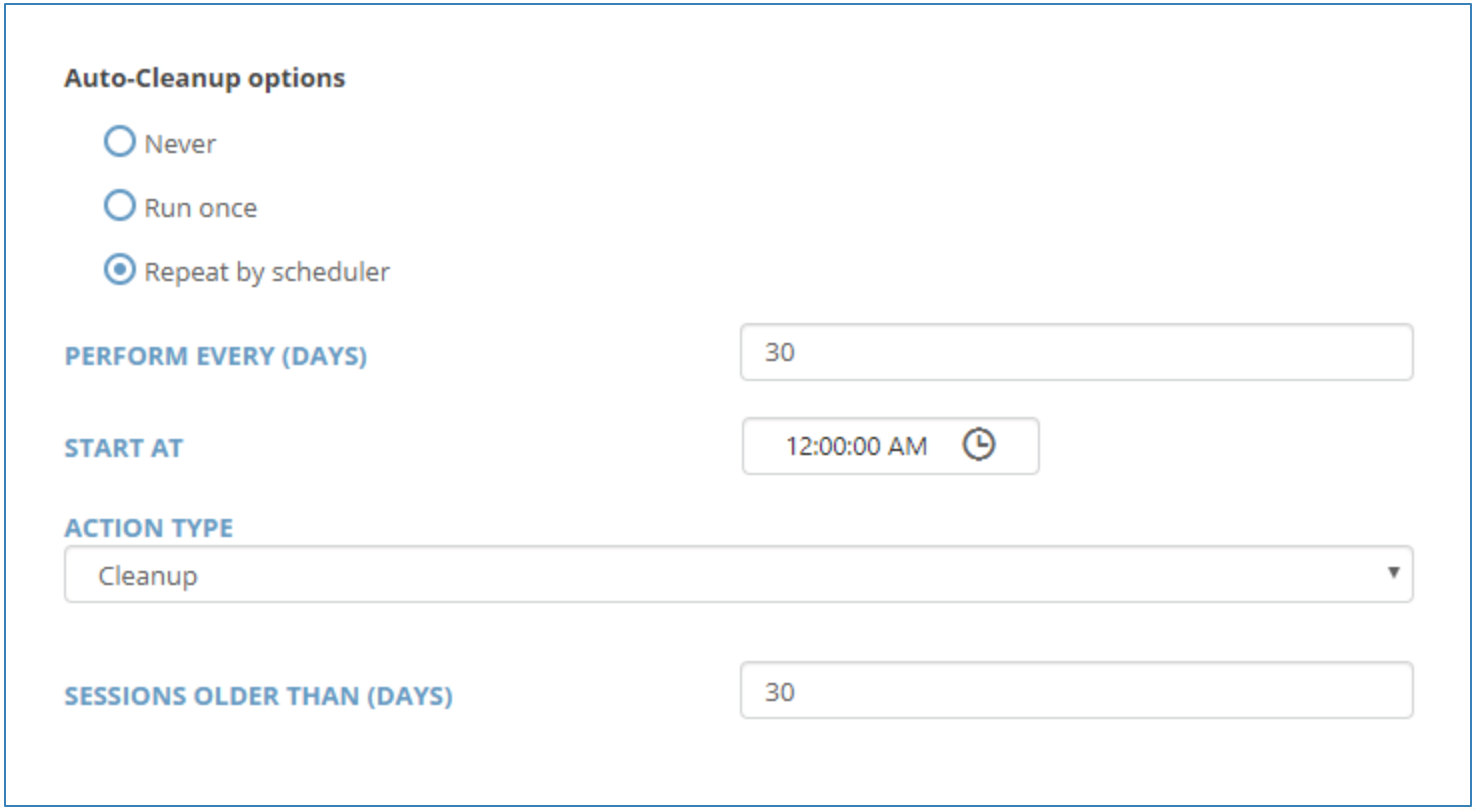
Zarządzanie bazą danych

Konfigurowanie bazy danych



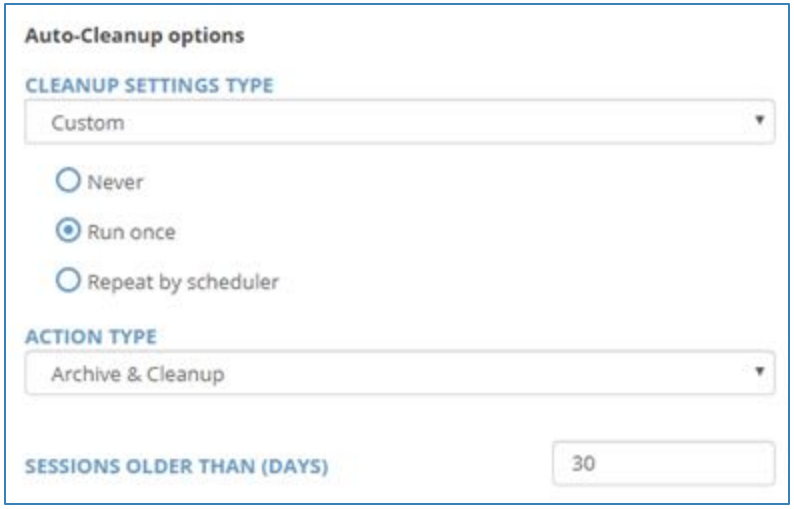
Czyszczenie bazy danych

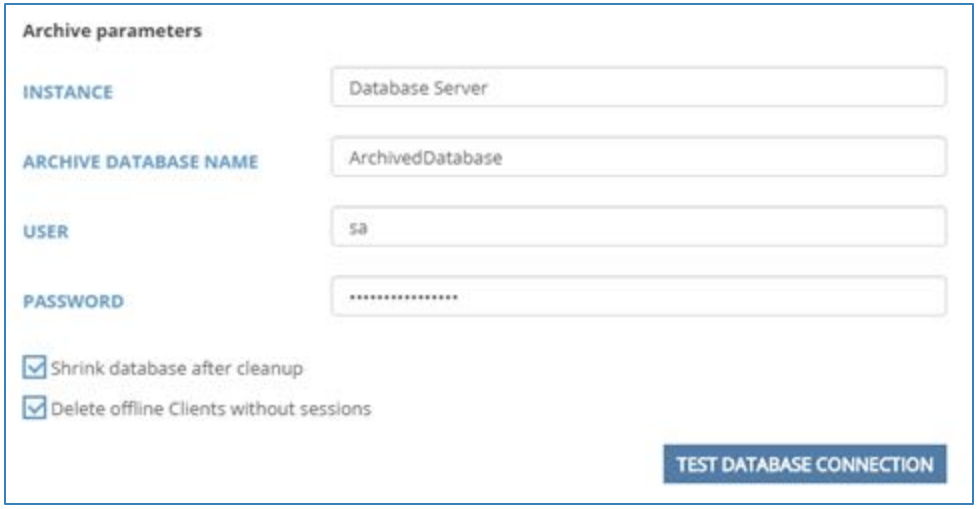
Możliwość skonfigurowania operacji czyszczenia bazy danych, która może być zastosowana zarówno do oddzielnego urządzenia z aplikacją Ekran Client, jak i do grup (Client Group).



Archiwizowanie bazy danych (Opcja Enterprise)

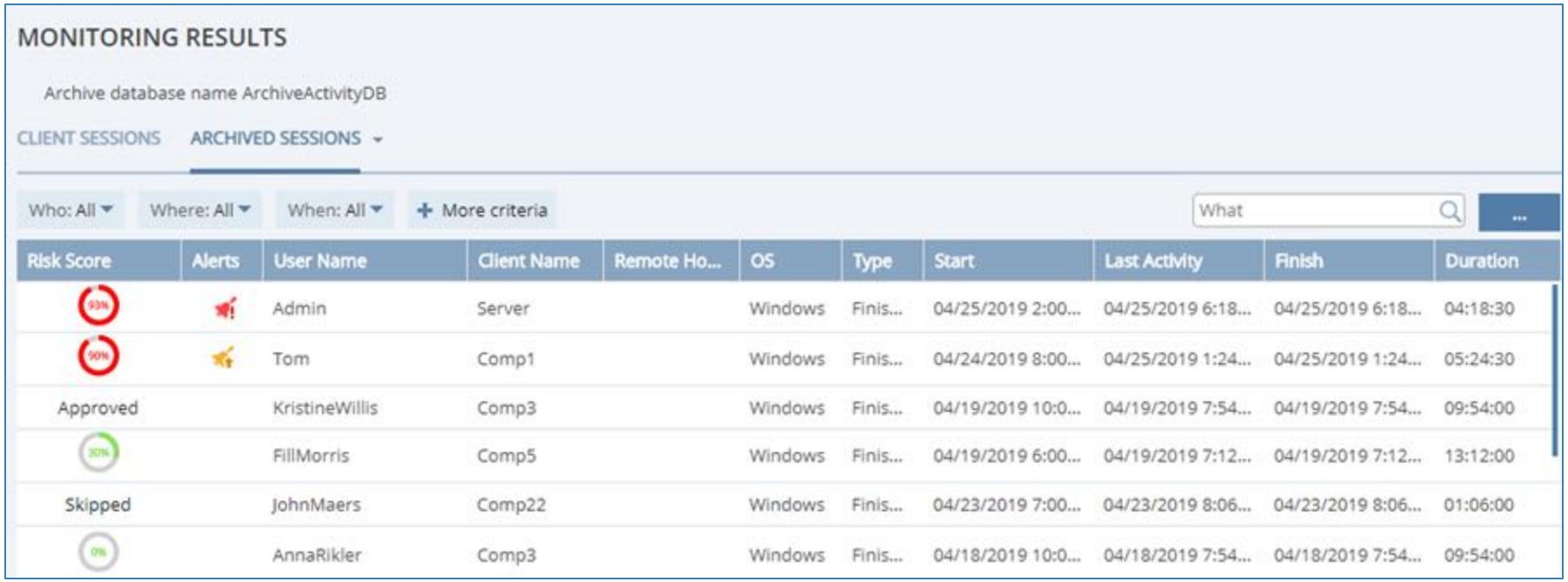
Możliwość archiwizowania i usuwania starych danych monitorowania z bazy. Pozwala to uniknąć całkowitego wykorzystania miejsca na serwerze i zapisać archiwalne dane w bezpiecznych „magazynach”.





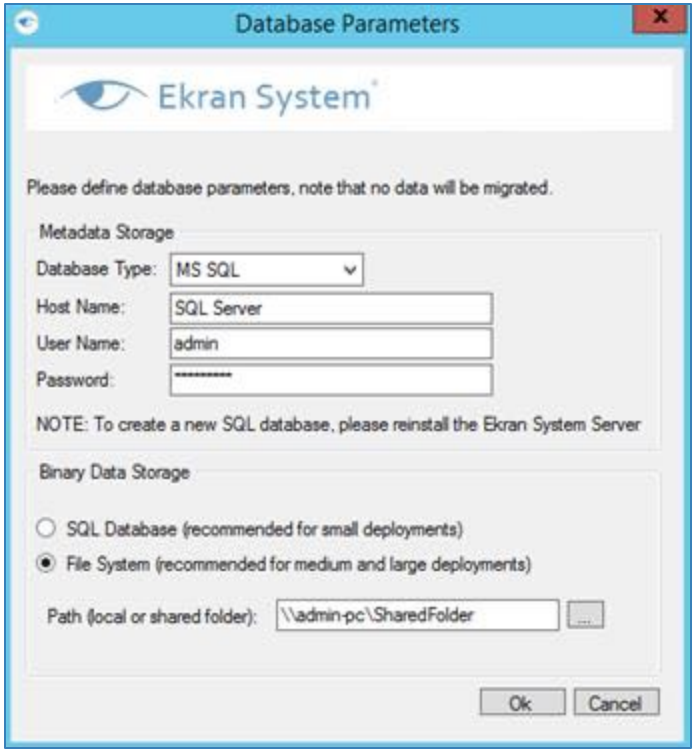
Archiwizowanie bazy danych (Enterprise Edition)

Możliwość **przeglądania sesji z zarchiwizowanej** bazy danych w Session Viewer i przeszukiwania ich w zwykły sposób w dowolnym momencie.



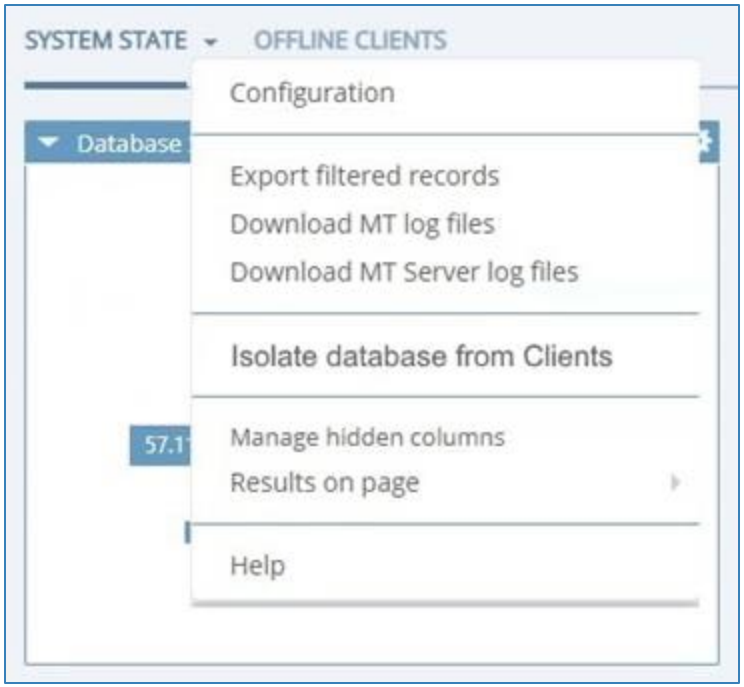
Parametry bazy danych

Jeśli **dane uwierzytelniające bazy danych** zdefiniowane podczas instalacji Ekran Server zostały zmienione zgodnie z polityką firmy, można je łatwo edytować bez konieczności reinstalacji Ekran Server. Można również zdefiniować miejsce przechowywania **danych binarnych** monitorowania.



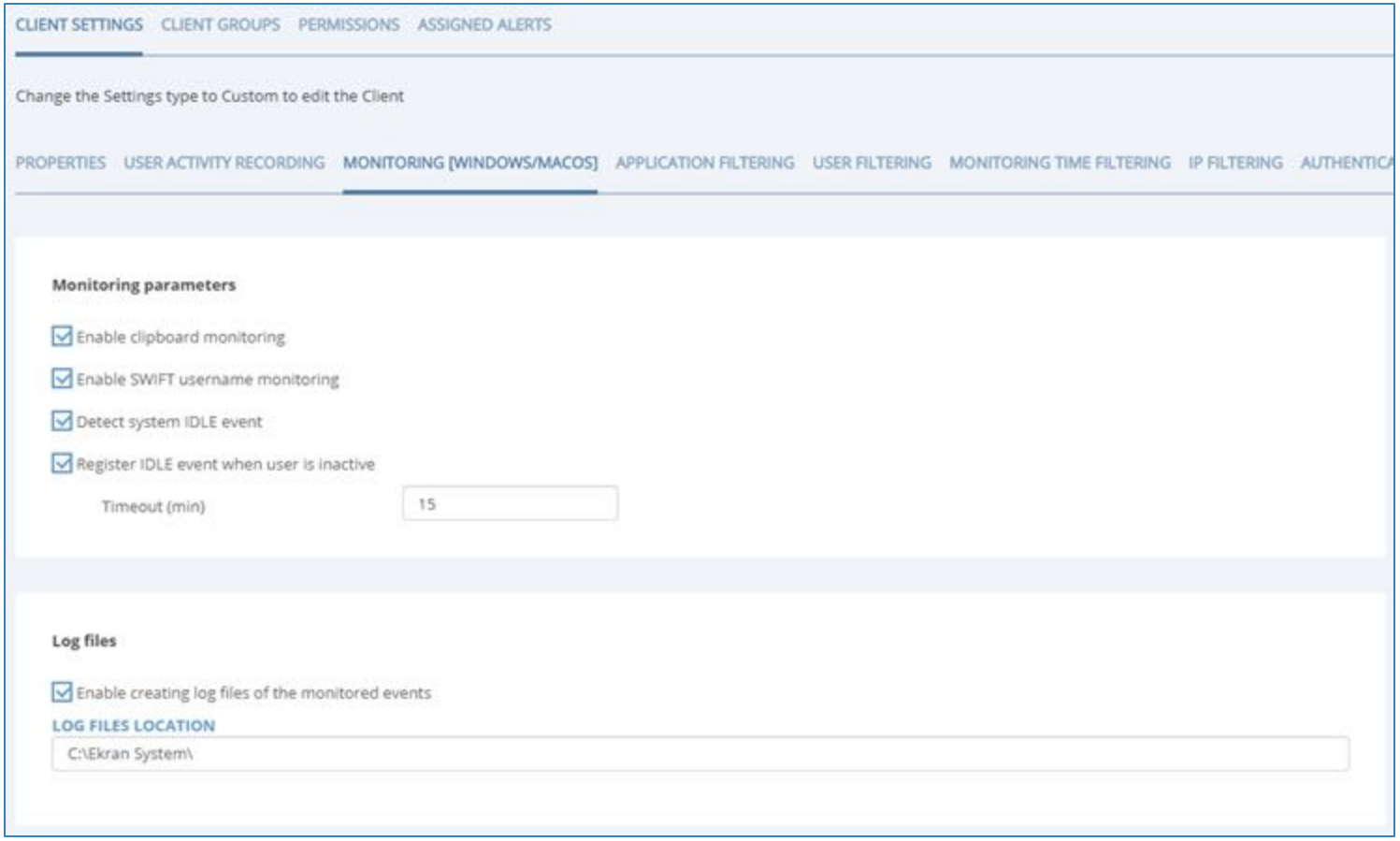
Odizolowanie bazy od Ekran Client (Enterprise Edition)

Istnieje możliwość odłączenia wszystkich aplikacji Ekran Client od bazy danych (w tym czasie dane zbierane są w trybie offline) w celu naprawienia problemów, czyszczenia, czy konserwacji bazy danych bez konieczności zatrzymywania Ekran Server. Po ponownym rozpoczęciu pracy bazy danych możesz przywrócić wszystkie aplikacje Ekran Client do trybu online jednym kliknięciem.



Integracja z systemami SIEM

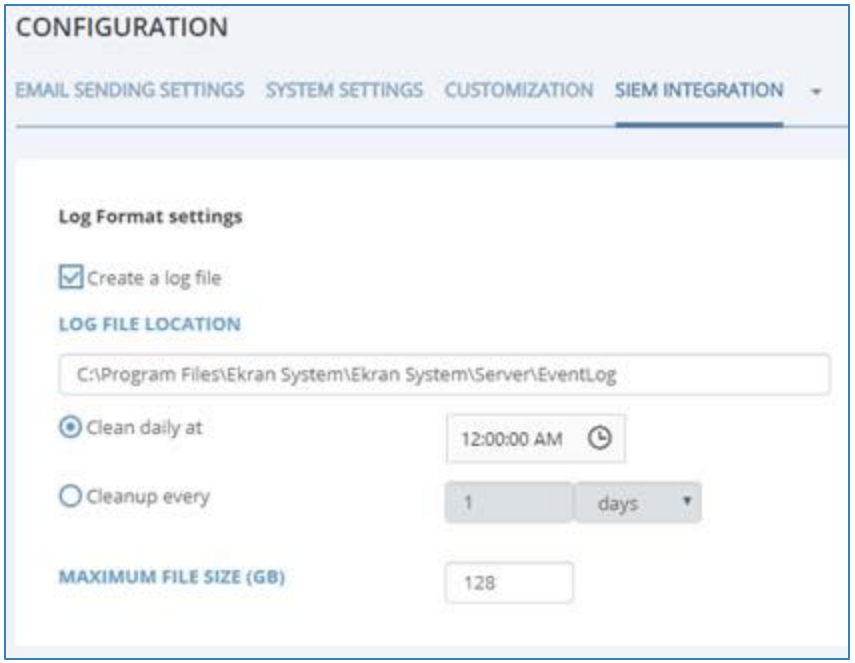
Ekran System integruje się z systemami SIEM, używając logów monitorowanych sesji.

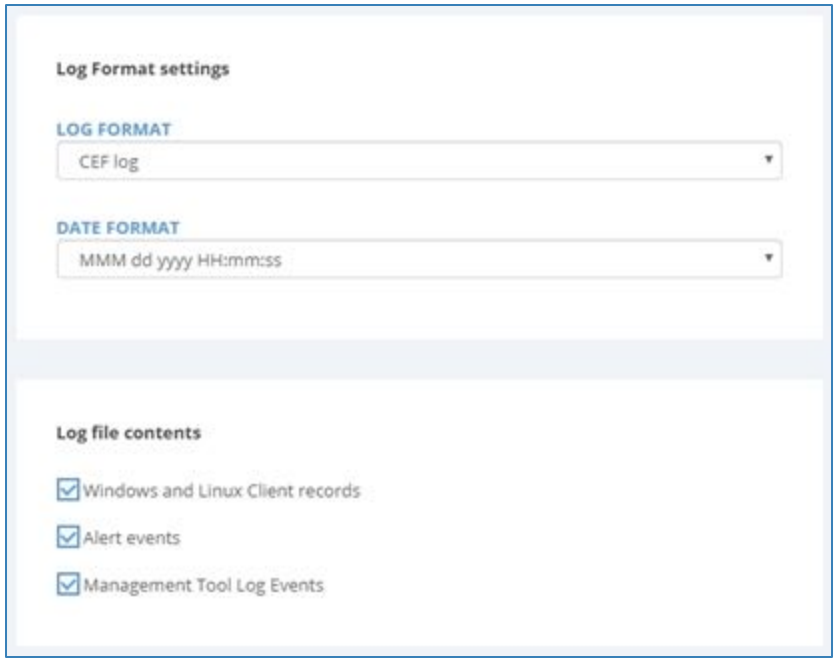


Zaawansowana integracja SIEM

Możliwość uzyskania dostępu do zdarzeń alarmowych (alerts) i monitorowanych danych, tworząc osobny log w jednym z poniższych formatów:

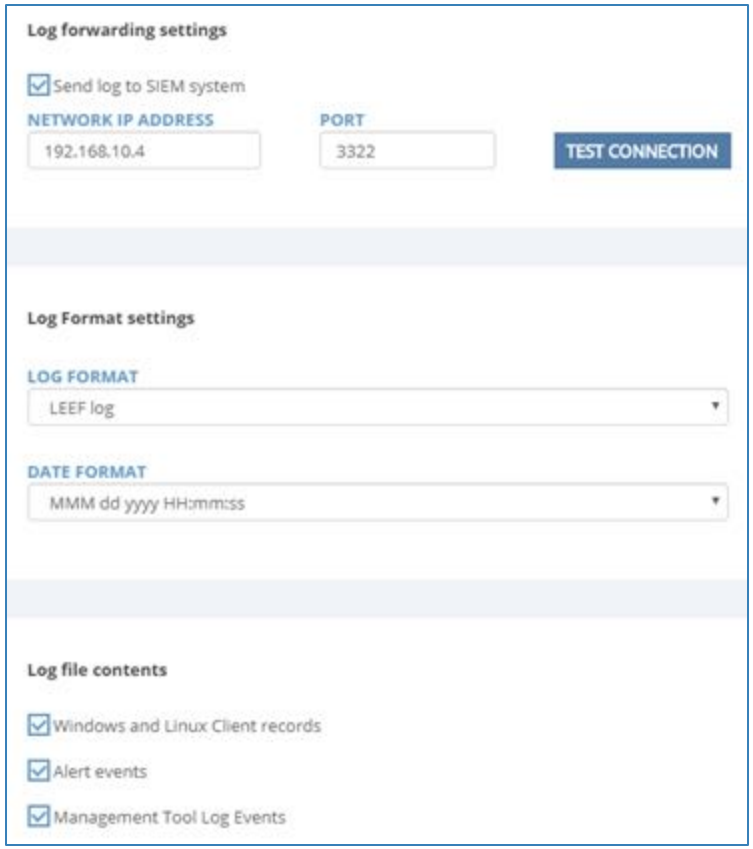
- Common Event Format (CEF)
- Log Event Extended Format (LEEF)





Zaawansowana integracja SIEM

Ekran System pozwala na przesyłanie zapisów zdarzeń alarmowych (alerts) i monitorowanych danych bezpośrednio do systemów SIEM, takich jak Splunk, ArcSight i QRadar.



Licencjonowanie

Rodzaje licencji i zarządzanie kluczami seryjnymi

Licencjonowanie

Ekran System jest licencjonowany według liczby punktów końcowych (aplikacji Ekran Client). Wszystkie komponenty do zarządzania, w tym Ekran Server i Management Tool, są dostarczane bezpłatnie wraz z każdym wdrożeniem.

Rodzaje **licencji** Ekran Client:

- **Workstation** Client license (Windows desktop, macOS, X Window System)
- **Infrastructure Server** Client license (Windows Server, Linux/UNIX Server)
- **Terminal Server** Client license (Windows Server with Terminal Services, Citrix Server, Published App Server, Jump Server, X Window System)

Licencjonowanie

LICENSE MANAGEMENT

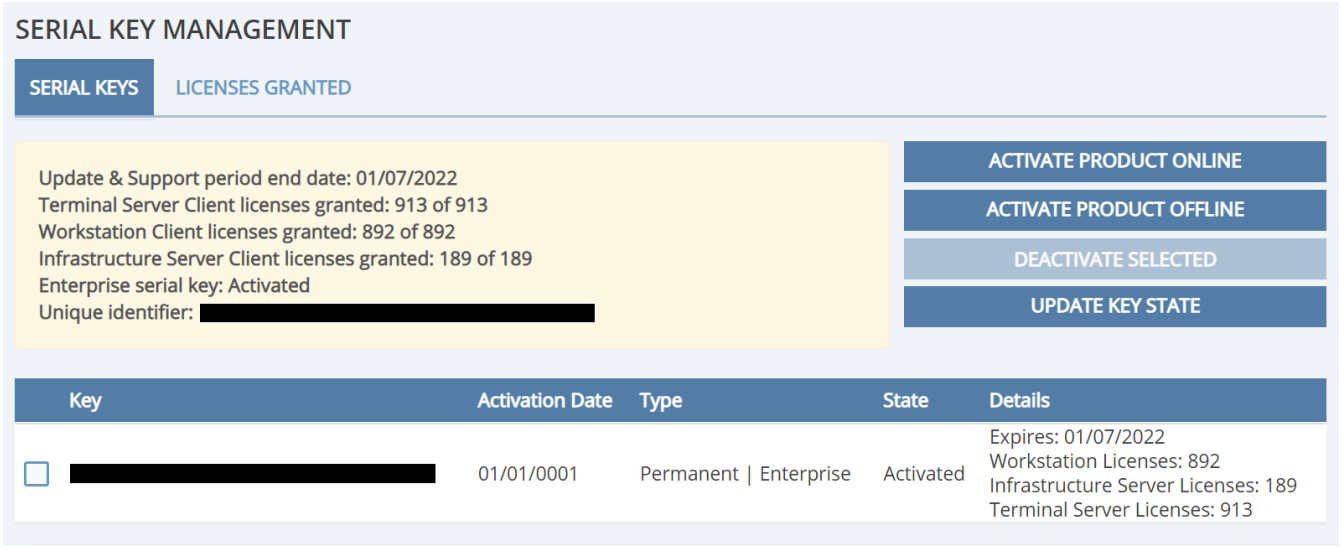
Workstation Client licenses granted: 4 of 10
Linux/UNIX Server Client licenses granted: 1 of 11
Infrastructure Server Client licenses granted: 1 of 3
Terminal Server Client licenses granted: 7 of 10
Not licensed Clients: 0

Name	Description	Recommended license	Assigned license	Client Groups
Comp2	Social media	Workstation license	None	Not Work-related Activity Demo,Dat...
Comp1	Sites with adult content	Workstation license	None	Potentially Illicit Activity Demo,Fraud...
Comp13	Opening a Folder with Potentially N...	Workstation license	None	Windows Workstations
Comp11	Generating Licenses	Workstation license	None	Windows Workstations
Comp19	Blocking user in the live session	Workstation license	None	Windows Workstations
ENTERPSERVER4	Starting RDP Connection from a Ser...	Terminal Server license	None	Fraud Activity,Windows Servers
Comp7	Exporting CRM Database	Workstation license	None	Fraud Activity,Windows Workstations
EnterpServ2	Critical Changes in Regedit	Terminal Server license	Terminal Server license	Fraud Activity,Windows Servers
EnterpServ5	Viewing session of privileged users (...	Terminal Server license	Terminal Server license	PASM (Privileged Users),Fraud Activi...
Paul_Mac	Visiting an Online Gambling Sites (w...	Workstation license	Workstation license	Potentially Illicit Activity Demo,MacOS
Sarah_Mac	Using Skype Web Version Solution	Workstation license	Workstation license	Not Work-related Activity Demo,Dat...
Vanessa_Mac	Using Job Searching Site (simplyhire...	Workstation license	Workstation license	Not Work-related Activity Demo,Mac...
ubuntu2	Adding New Users	Linux license	None	Fraud Activity,Linux
ubuntu1	Loading Sensitive Data to a Flash Dri...	Linux license	Linux license	Fraud Activity,Data Leakage,Linux
srv-app	Manual Data Saving	Terminal Server license	Terminal Server license	App Server (Citrix XenApp, etc.)
cathy-pc		Workstation license	None	

ASSIGN RECOMMENDED LICENSE
ASSIGN LICENSE OF SPECIFIC TYPE
UNASSIGN LICENSE

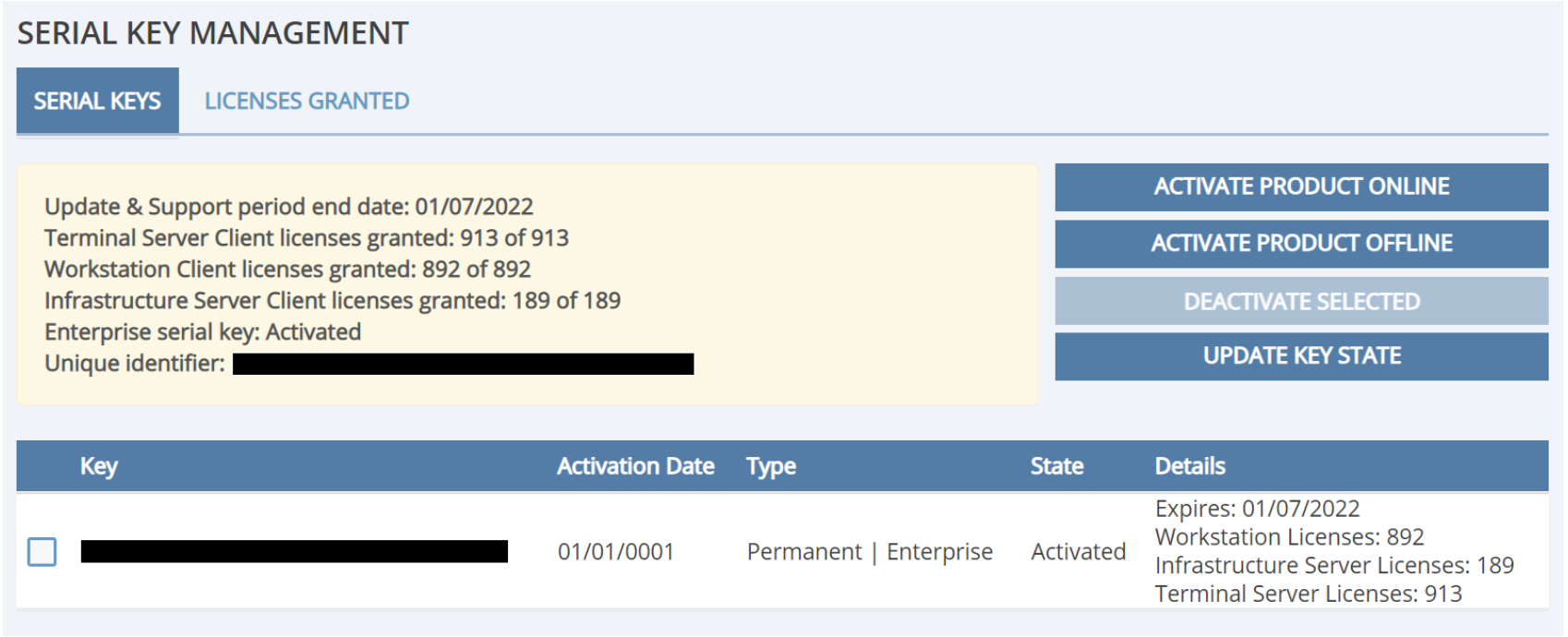
Zarządzanie kluczami seryjnymi i licencjami

W celu zapoznania się z podstawowymi funkcjami oprogramowania należy pobrać 30-dniową wersję trial umożliwiającą monitorowanie 3 stacji roboczych, 3 serwerów Linux/UNIX oraz 1 serwera terminalowego (RDS) Windows. Trial pozwala zapoznać się również z funkcjami Enterprise Edition.
Aby korzystać z Ekran System dłużej, należy przedłużyć **licencjonowanie** poprzez aktywowanie zakupionego klucza. Istnieje możliwość użycia klucza wieczystego lub aktualizację klucza wersji trial.



Licencja Enterprise

Aktywuj **klucz seryjny licencji Enterprise**, aby uzyskać dostęp do zestawu dodatkowych, cennych funkcji Edycji Enterprise Ekran System.



Licencjonowanie Floating Endpoints

Ekran System jest obecnie jedynym produktem na rynku, który oferuje **zmienne licencjonowanie punktów końcowych**.

Ta unikalna funkcjonalność umożliwia **ponowne przypisywanie licencji** między Ekran Clients zarówno ręcznie, jak i automatycznie, dzięki czemu **wystarczy zakupić tylko taką ilość licencji** Ekran System Workstation Client, która **odpowiada maksymalnej możliwej liczbie jednocześnie aktywnych** Ekran **Clients**.

- **Ręczna** zmiana przypisu licencji: można to zrobić **w dowolnym momencie** za pomocą zaledwie **kilku kliknięć**.
- **Automatyczna** zmiana przypisu licencji:
  - **Usuwanie Ekran Clients offline bez sesji**: Ta opcja umożliwia automatyczne zwracanie licencji Ekran Clients, gdy nie mają zapisanych sesji, do puli dostępnych licencji (np. po oczyszczeniu bazy danych).
  - **Korzystanie z golden image** (do monitorowania pulpitu VMware/Citrix): Dynamicznie przypisuje licencje do wirtualnych pulpitów za każdym razem, gdy tworzone są nowe pulpity z systemem Windows i usuwa je za każdym razem, gdy maszyny Ekran Client są wyłączane.

Unikalne funkcje licencji Enterprise

Funkcje dostępne jedynie w **licencji Enterprise:**

- High Availability
- Multi-Load Balancer Support
- Multi-Tenant
- Password Management
- Wykrywanie agentów offline (“Utracony” agent)
- Integracja z systemami zgłoszeń (Help-Desk)
- Zaawansowana integracja systemów SIEM
- Harmonogramowe nadawanie dostępu
- Zarządzanie dostępem i przebiegiem pracy
- User Behavior Analysis (analiza zachowań użytkowników)
- Server Health Monitoring
- Archiwizowanie bazy danych
- Filtrowanie adresów IP
- Rejestrowanie logów w Windows Event Log
- Zarządzanie dostępem USB przez Administratora
- SWIFT Username Monitoring
- Nagrywanie audio

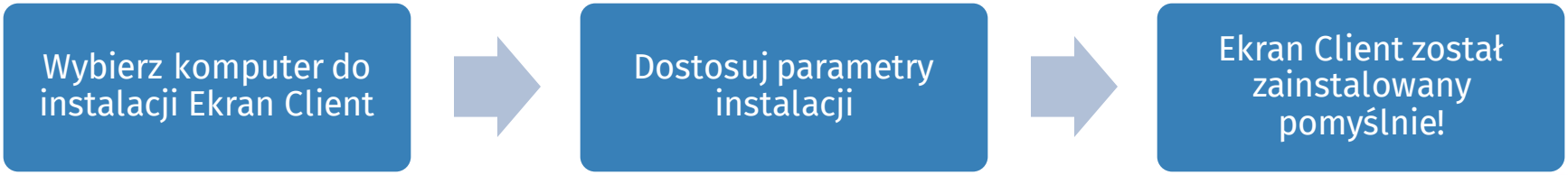
Instalowanie i aktualizacja programu Ekran Client

Instalowanie programu Ekran Client

Wygodna instalacja programu Ekran Client:

- **Lokalna**:
  - Linux Clients (przez tar.gz file)
  - macOS Clients (przez tar.gz file)
  - Windows Clients
    - przy użyciu pliku instalacyjnego z domyślnymi parametrami
    - przy użyciu wygenerowanego pakietu o niestandardowych parametrach
- **Zdalna**
  - dla Windows Clients
  - dla macOS Clients

Zdalna instalacja



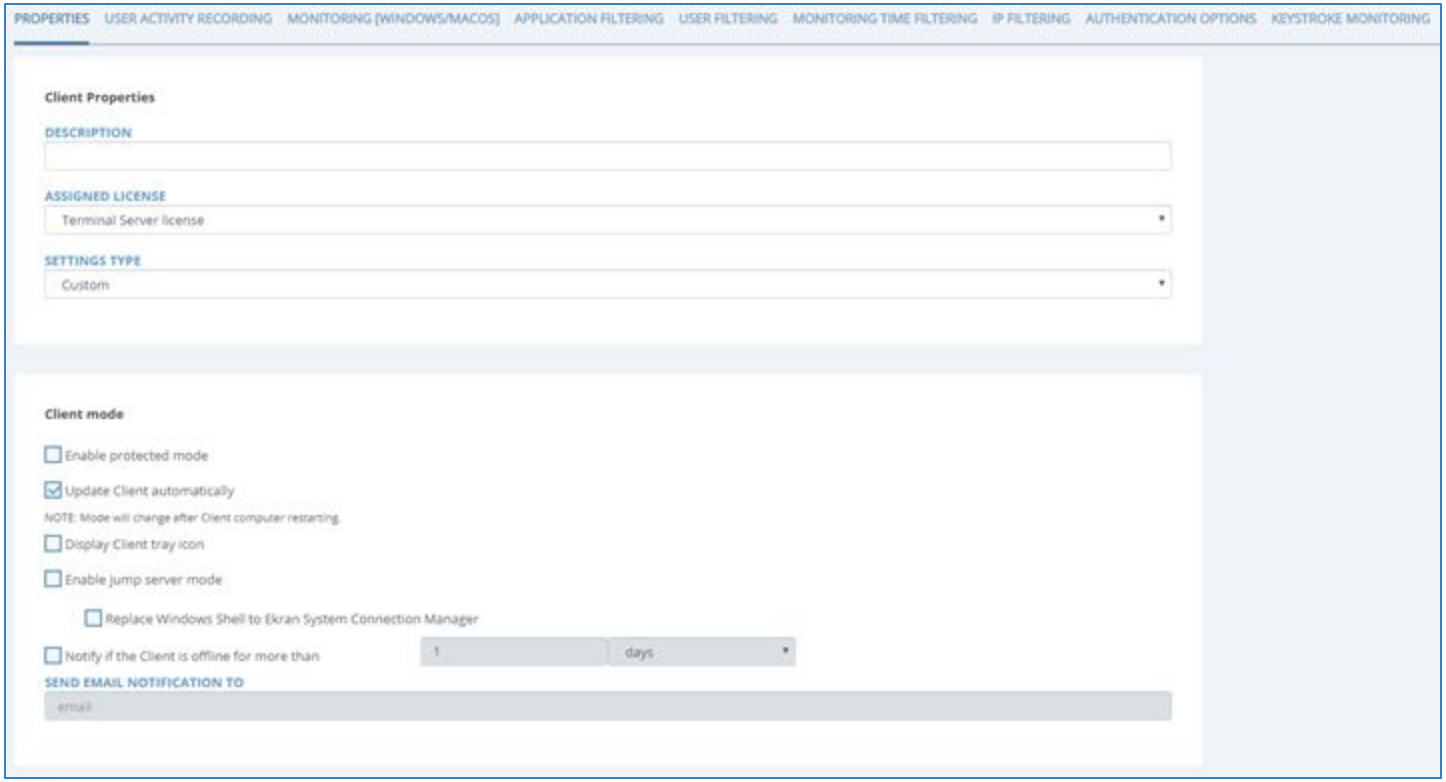
Komputery docelowe do zdalnej instalacji

- Przeskanuj swoją **lokalną sieć komputerową.**
- Zdefiniuj **zakres adresów IP** w celu znalezienia komputera docelowego.
- Wprowadź **nazwę komputera** docelowego.

Aktualizacja programu Ekran Clients

Kiedy Ekran System zostanie zaktualizowany do najnowszej wersji, wszystkie aplikacje Ekran Client zostaną automatycznie zaktualizowane do tej samej wersji po pierwszym połączeniu z Ekran Server.

Jeśli chcesz osobiście nadzorować proces aktualizacji aplikacji Ekran Client, możesz wyłączyć opcję **automatycznej aktualizacji** (Update Client).



Monitorowanie parametrów

Monitorowanie poprzez program Ekran Client

Zrzuty ekranu wysłane przez aplikację Ekran Client są przechowywane w formie delt (różnice pomiędzy nowszym nagraniem ekranu a starszym) w celu zminimalizowania przestrzeni dyskowej.

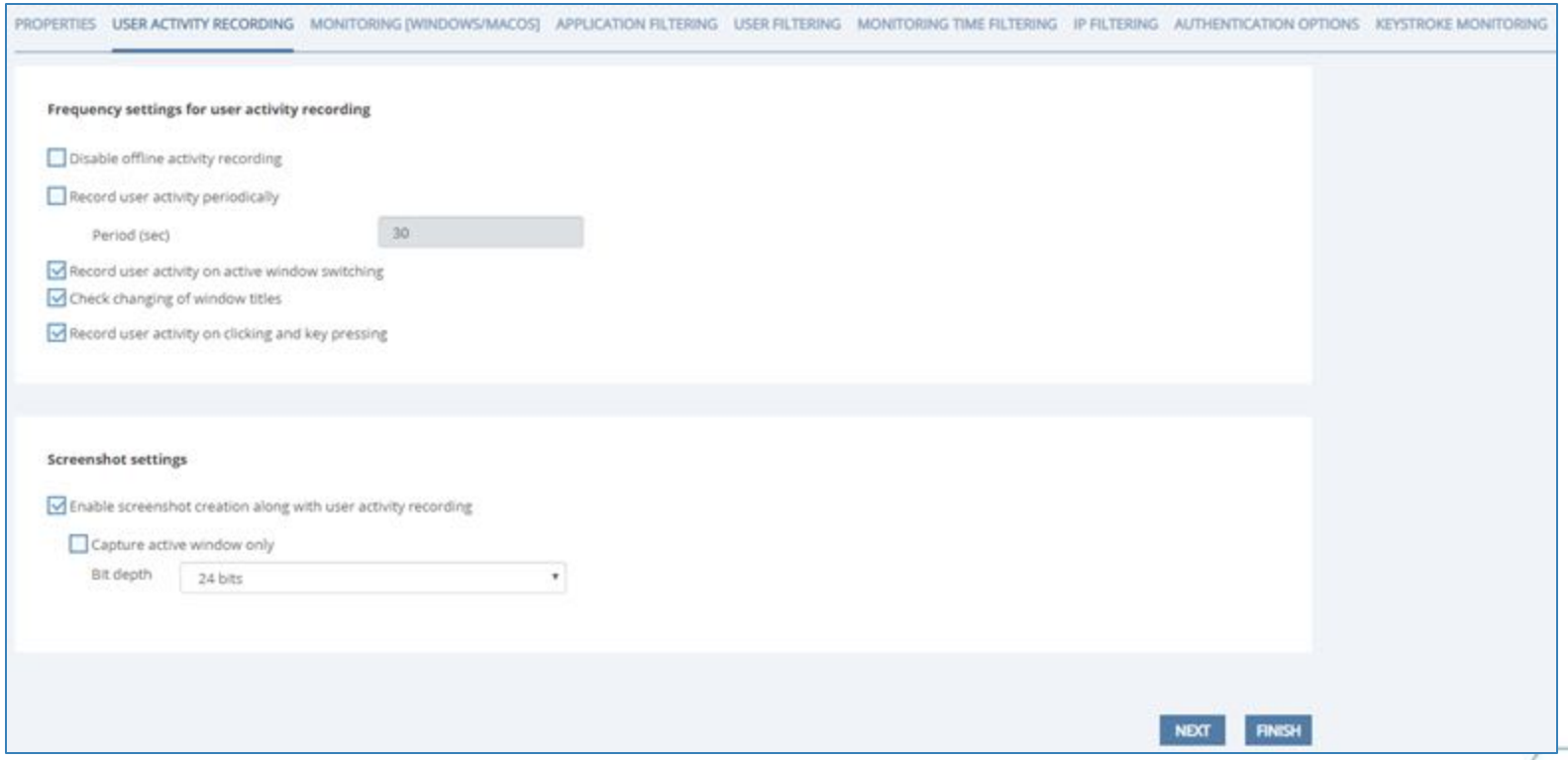
Przechwycone informacje są zapisane w łatwej do odczytania i przeglądania formie:

- Nazwa uruchomionej aplikacji
- Tytuł aktywnego okna
- Wprowadzony adres URL
- Tekst wprowadzany za pomocą klawiatury użytkownika (keylogger)
- Dane tekstowe schowka (skopiowany i wklejony tekst)
- Polecenia wykonywane w Linuksie (zarówno z danych wejściowych użytkownika, jak i poprzez uruchamianie skryptów)
- Informacje na temat podłączonych urządzeń USB

Nagrywanie aktywności użytkownika

Domyślne nagrywanie aktywności użytkownika w aplikacji Ekran Client odbywa się w sposób ciągły.

Istnieje możliwość konfiguracji aplikacji Ekran System, aby podczas nagrywania aktywności wykonywała jedynie zrzuty ekranu lub rejestrowała tylko metadane.

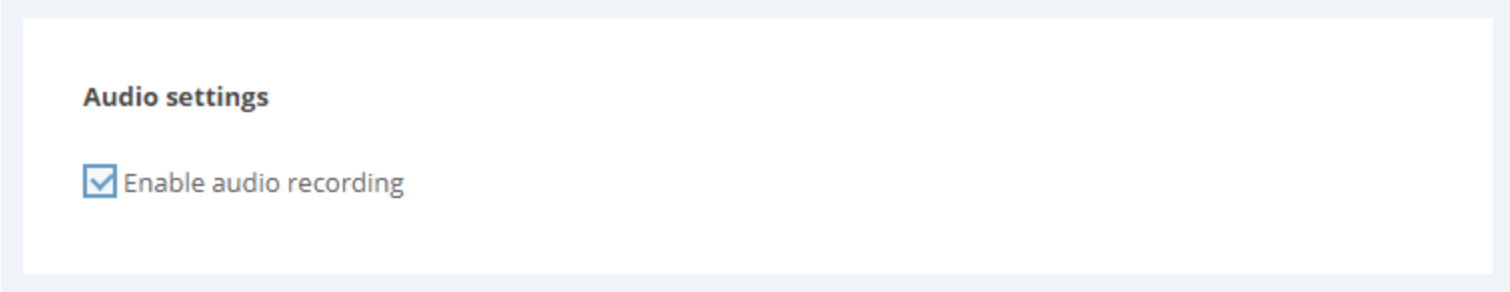


Nagrywanie audio

Ekran System umożliwia nagrywanie dowolnych dźwięków wyjściowych i wejściowych odtwarzanych na komputerach z aplikacją Ekran Client i systemem operacyjnym Windows.

Dane audio mogą być monitorowane i zapisywane w następujących aplikacjach:

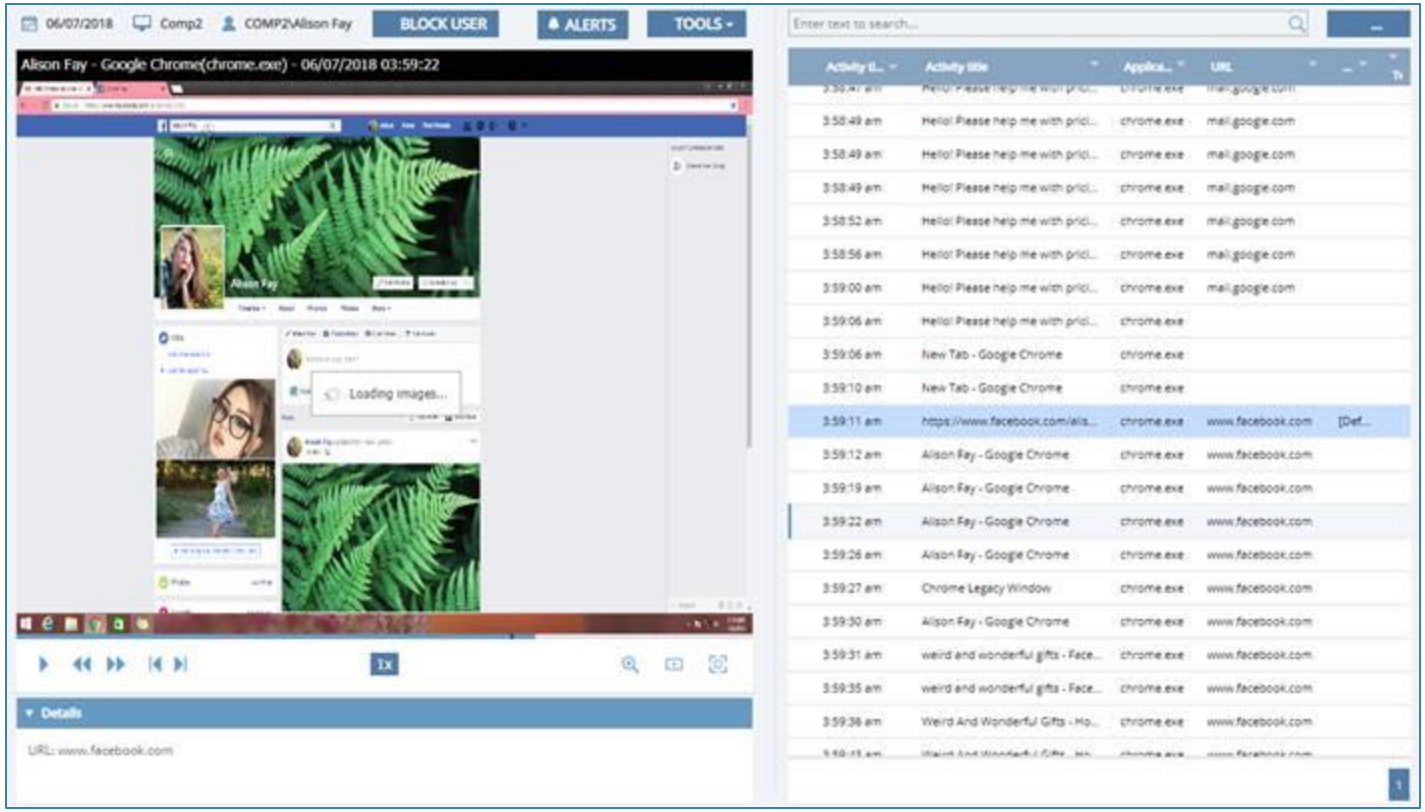
- Skype
- Slack
- Zoom
- Viber
- WhatsApp
- Firefox
- Chrome
- Opera
- Internet Explorer



Monitorowanie adresów URL

Ekran Client monitoruje adresy URL wprowadzone w przeglądarki internetowe.

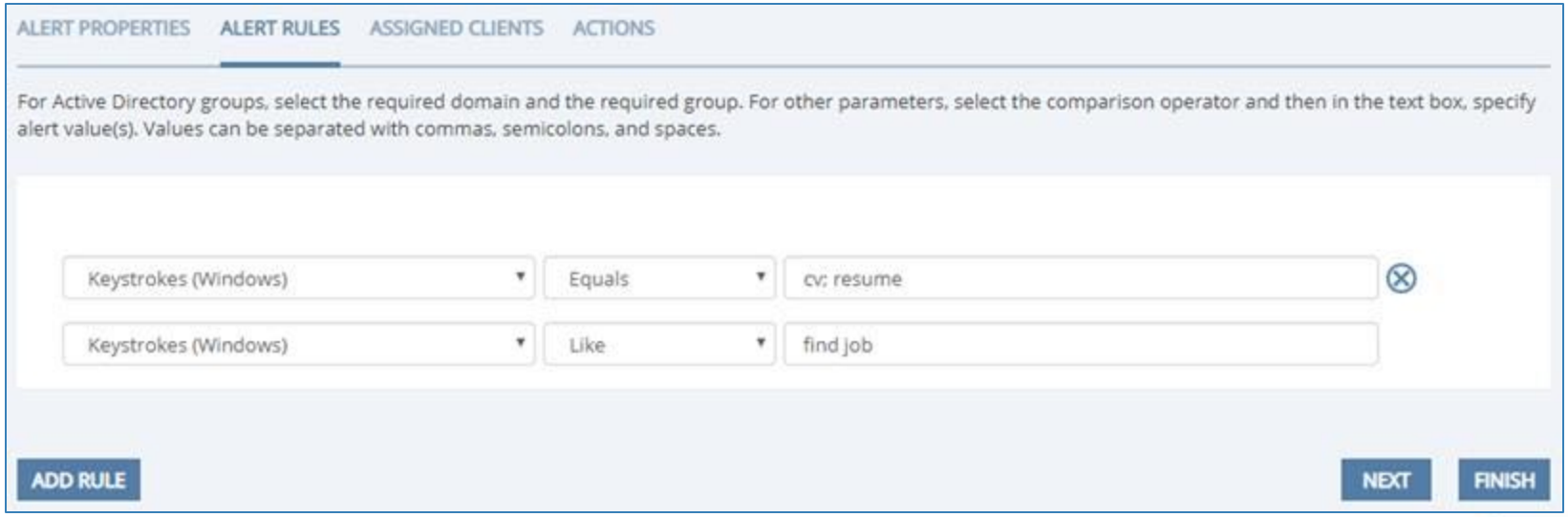
Możesz skonfigurować aplikację Ekran Client tak, aby monitorowała pełne adresy URL lub domeny tylko pierwszego poziomu



Keystroke Logging

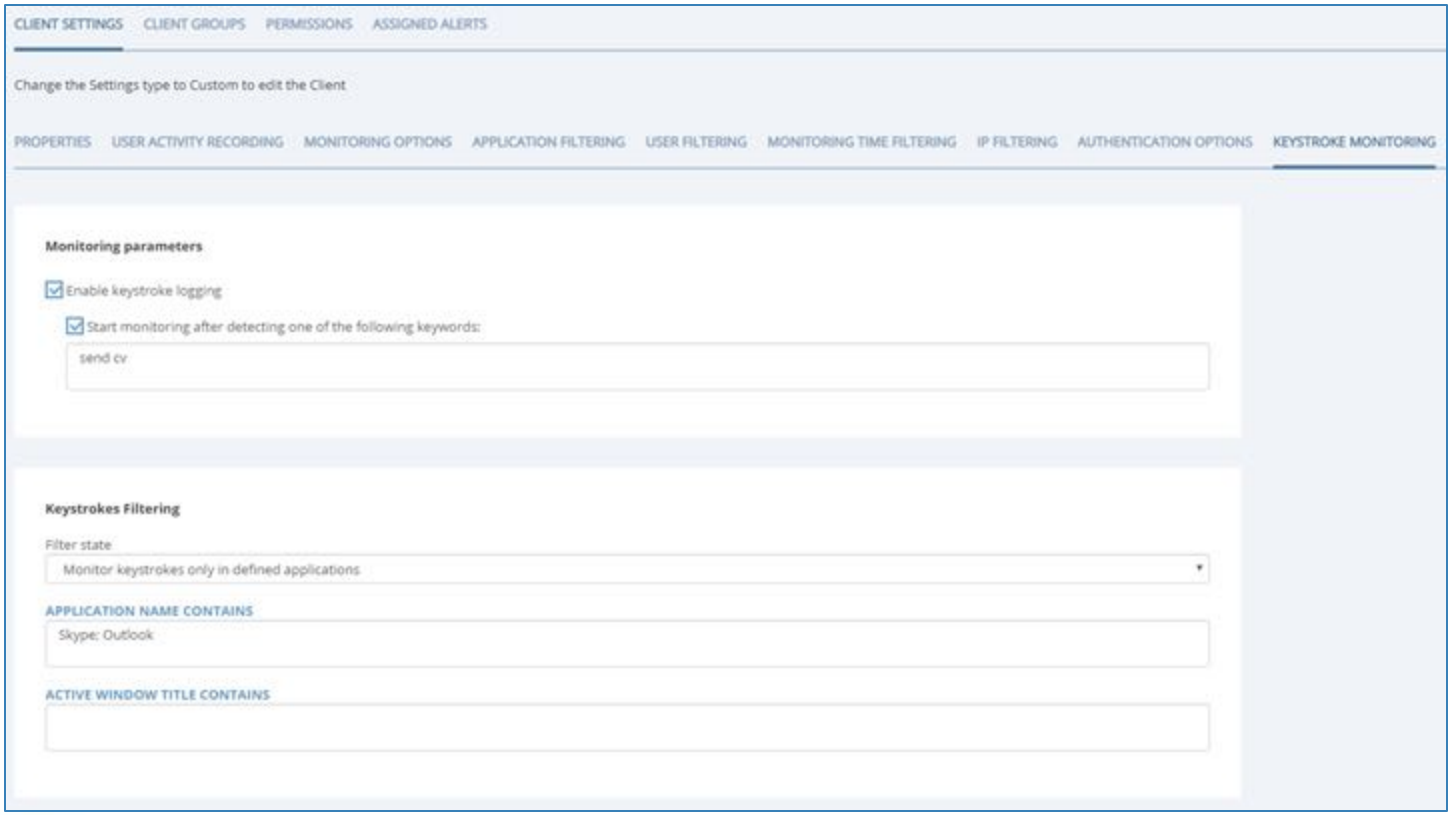
Aby zapewnić zgodność z **RODO**, wszystkie zarejestrowane naciśnięcia klawiszy (keystroke) są **ukryte**, ale można je **przeszukiwać** i tworzyć **alerty**, które są wyzwalane po wpisaniu określonych słów.

Można również **filtrować** aktywność klawiatury, co pozwala zmniejszyć ilość informacji otrzymywanych od Windows Ekran Client i zapewnić, że nie dojdzie do naruszenia prywatności poprzez zdefiniowanie aplikacji, w których wciśnięcia klawiszy będą monitorowane.



Monitorowanie wyzwalanych słów kluczowych

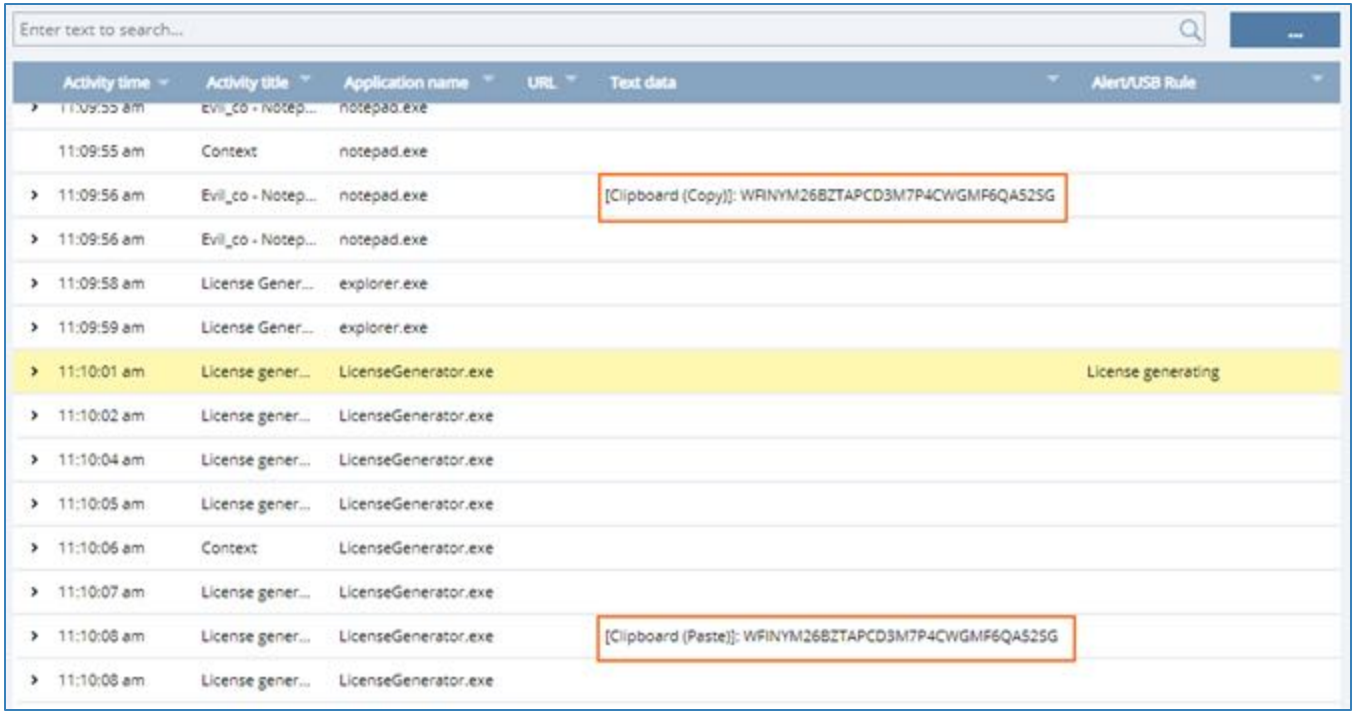
Ekran Client może zostać skonfigurowany tak, aby rozpocząć monitorowanie i tworzenie zrzutów ekranu dopiero po wykryciu zdefiniowanych słów kluczowych wprowadzonych przez użytkownika w określonych aplikacjach.



Monitorowanie schowka

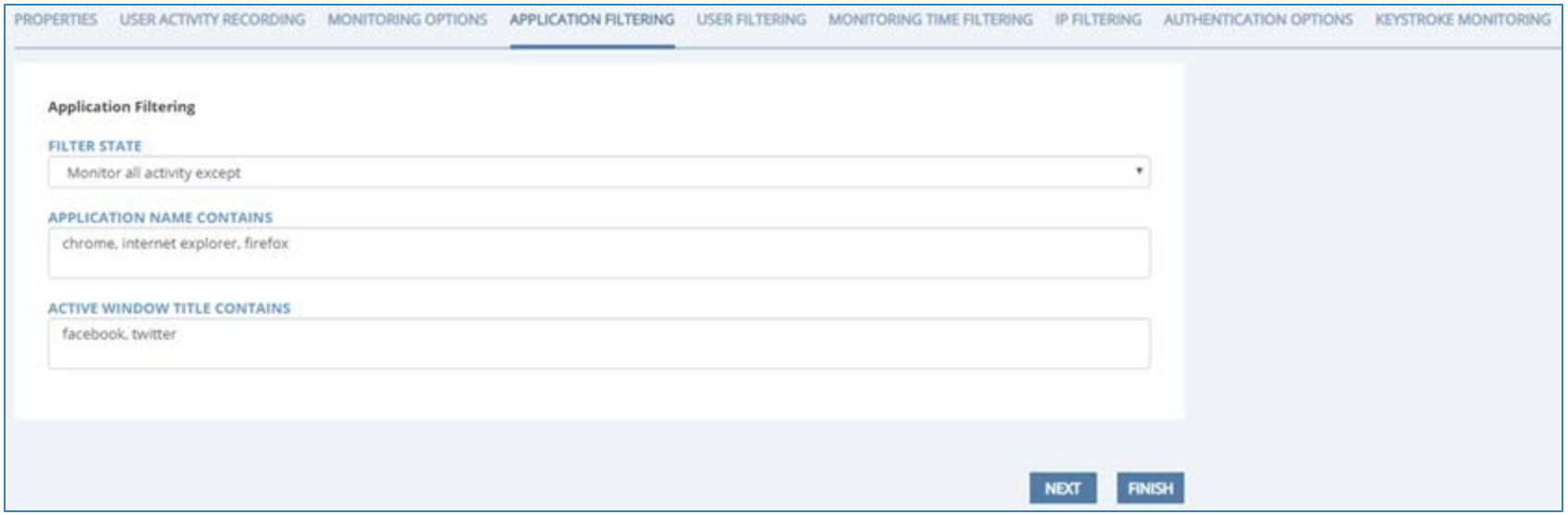
Ekran Client **przechwytuje wszystkie dane tekstowe**, które zostały **skopiowane lub wycięte**, a następnie **wklejone** do dokumentów, plików, aplikacji, paska adresu przeglądarki itp. na komputerach z aplikacją Ekran Client.

Alert może być wyzwalany za każdym razem, gdy użytkownik kopiuje lub wycina informacje i wkleja je.



Filtrowanie aplikacji

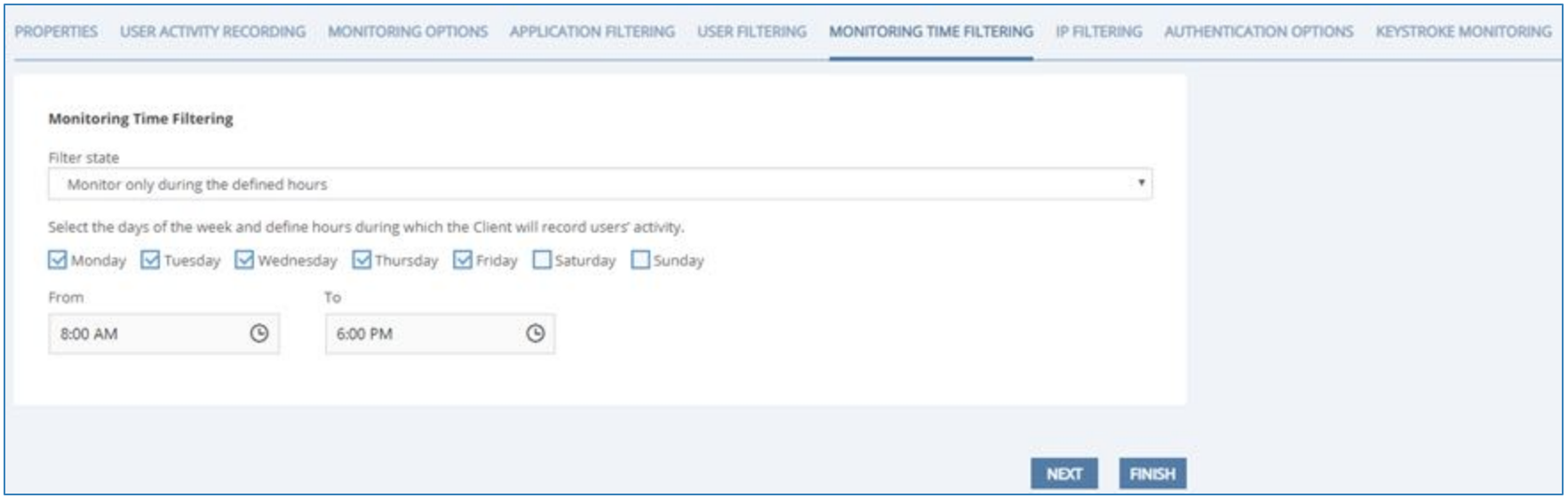
Ekran Client umożliwia zdefiniowanie zasad filtrowania stron internetowych/aplikacji w celu dostosowania ilości monitorowanych danych oraz wyłączenia obszarów, w których można obserwować informacje prywatne. Ma to pozwolić na zachowanie zgodności z zasadami polityki korporacyjnej i przepisami krajowymi dotyczącymi prywatności użytkowników.



Monitorowanie czasu filtrowania

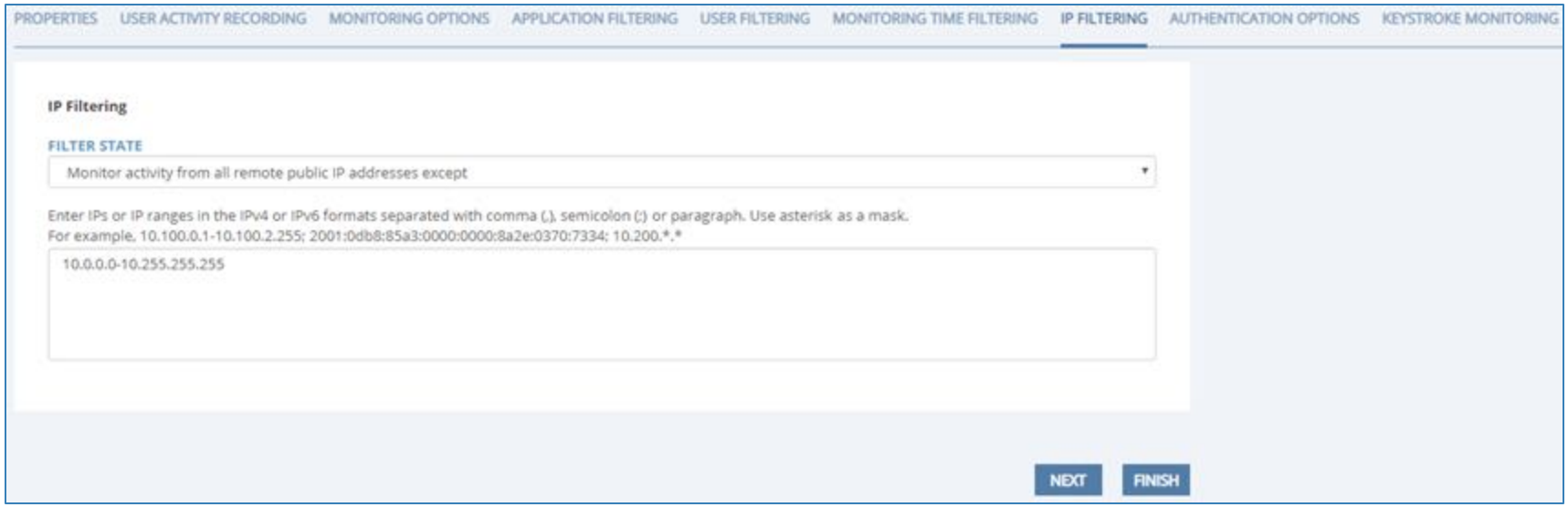
Oprócz reguł filtrowania aplikacji można zdefiniować **reguły monitorowania czasu** filtrowania.

Wybierając odpowiednie **dni tygodnia** i określając konkretne **godziny**, można ustalić granice, w których aplikacja Ekran Client będzie rejestrować całą aktywność użytkowników.



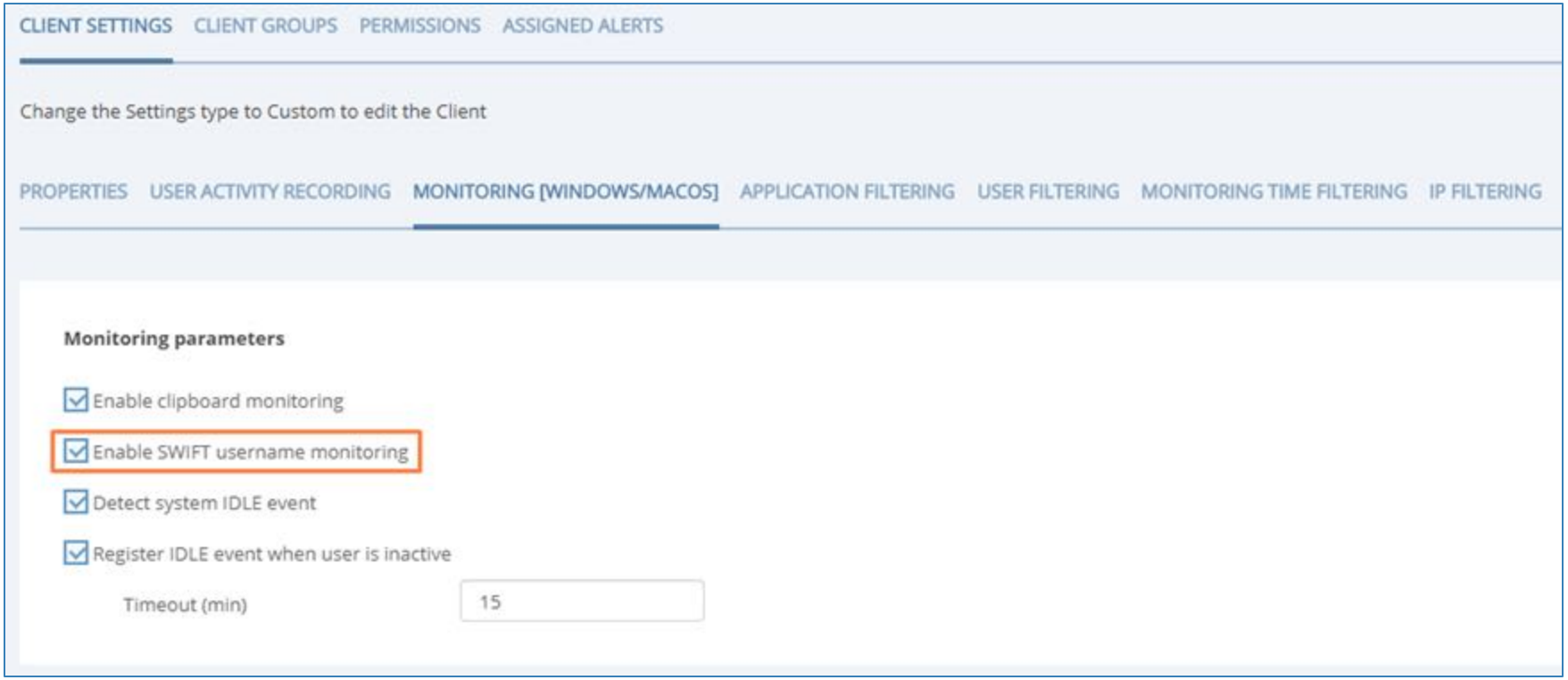
Filtrowanie adresów IP

Dodatkowo można **filtrować** sesje określonych zdalnych adresów IP lub **monitorować** tylko sesje **określonych adresów IP**.



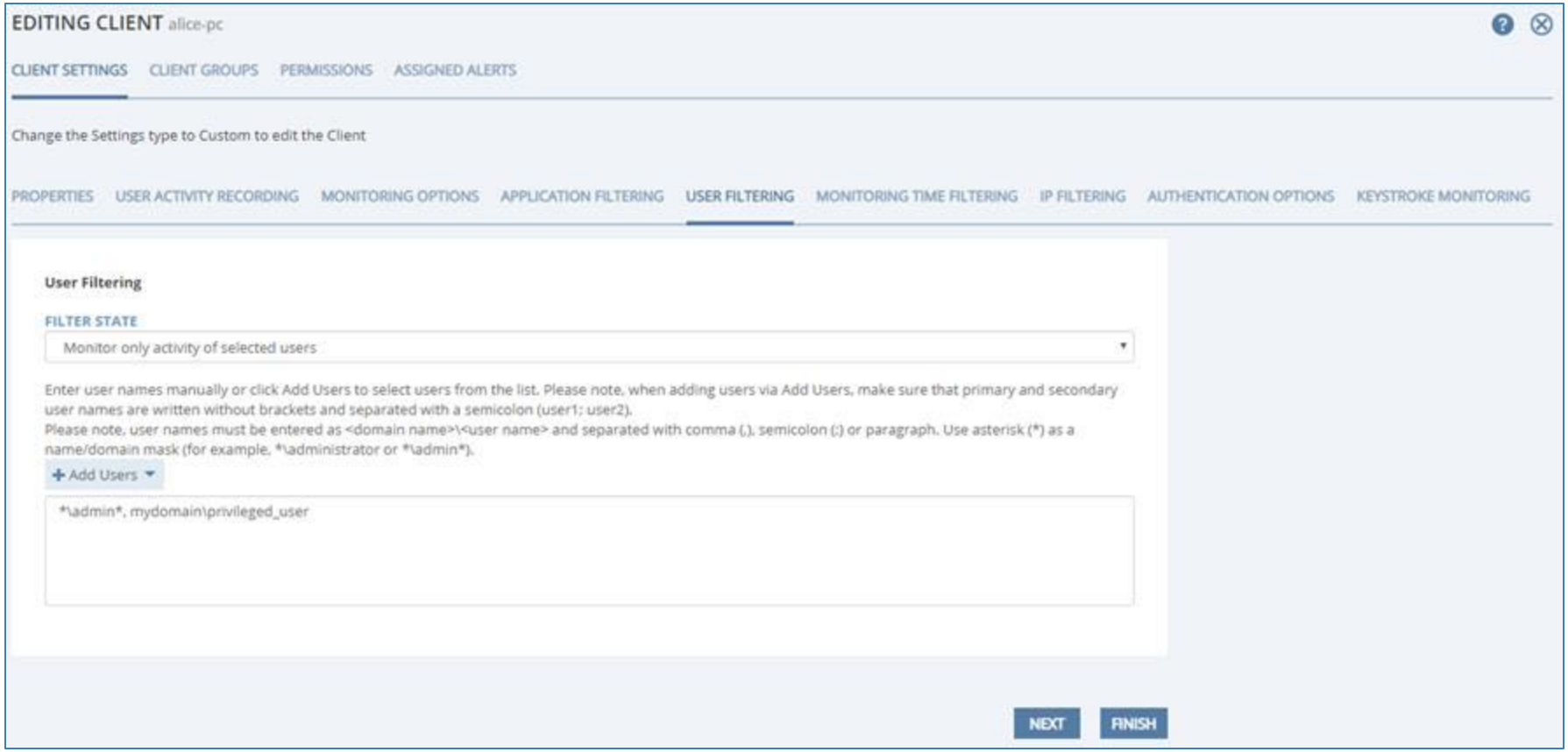
Monitorowanie nazwy użytkownika SWIFT

Ekran System umożliwia nagrywanie sesji na podstawie nazwy użytkownika logowania do sieci SWIFT, dzięki czemu można łatwo zidentyfikować takich użytkowników.



Monitorowanie użytkowników uprzywilejowanych

Monitorowanie aktywności użytkowników logujących się w ramach uprzywilejowanych kont użytkowników.

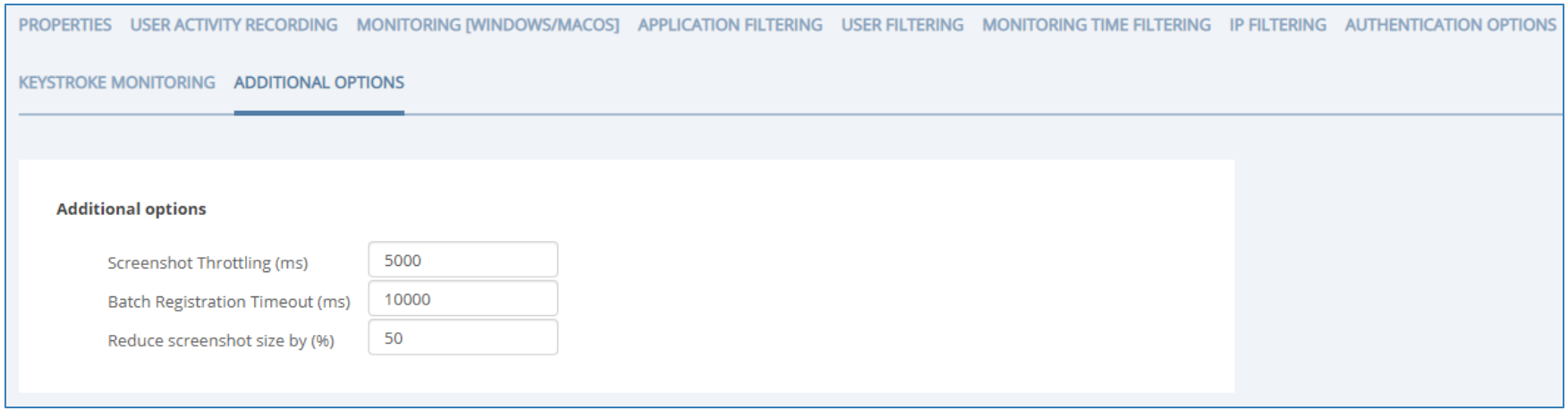


Redukcja zużycia przepustowości

Ekran System pozwala na konfigurację parametrów, które pozwolą **zredukować natężenie** łącza między Agentem a Serwerem.

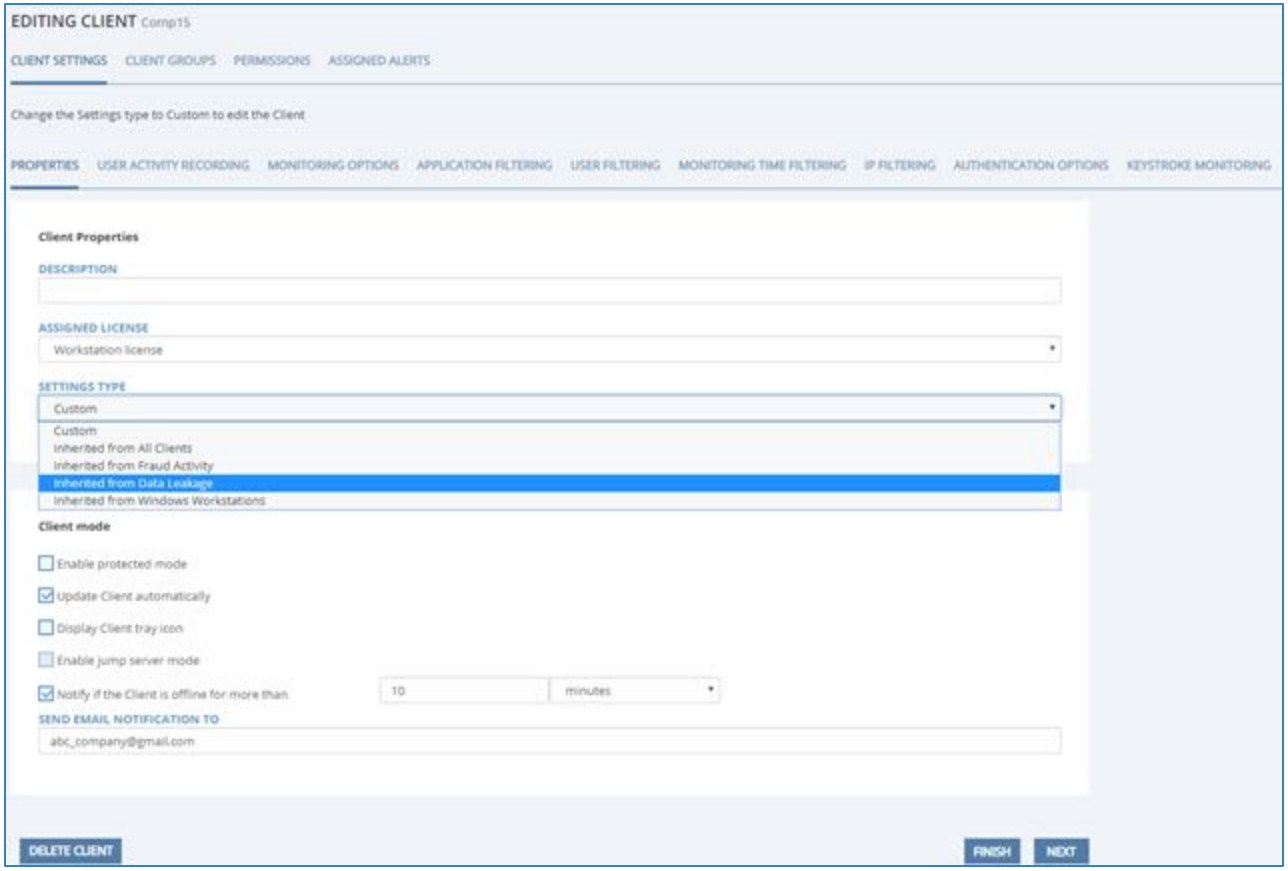
Można konfigurować takie parametry jak:

- **Tłumienie** zrzutów ekranu
- Limit czasu **rejestracji partii**
- **Redukcja rozmiaru** zrzutów ekranu



Ustawienie grup Ekran Client

Możesz zdefiniować ustawienia dla grupy aplikacji Ekran Client, a następnie zastosować je do nowo dodanego użytkownika, aby zaoszczędzić czas.



Monitorowanie przez Linux Clients (X Window System)

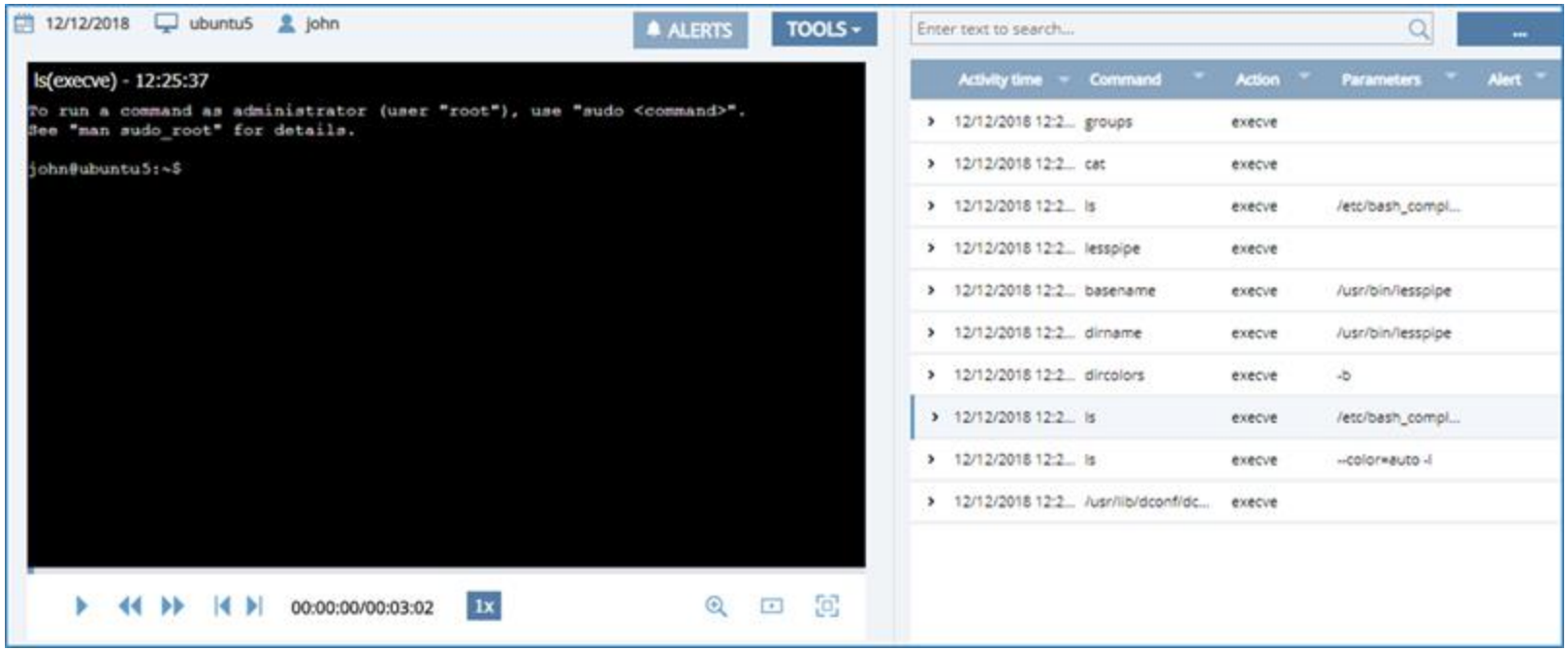
Zdalne monitorowanie **sesji SSH** w systemie Ekran System zapewnia możliwość **monitorowania poleceń wykonywanych w terminalu**.

Obsługiwane jest również monitorowanie sesji Linux rozpoczętych **lokalnie** poprzez **interfejs graficzny**.

Monitorowanie przez Linux Clients (Sesja Zdalna)

Zdalna sesja Linux Client zawiera:

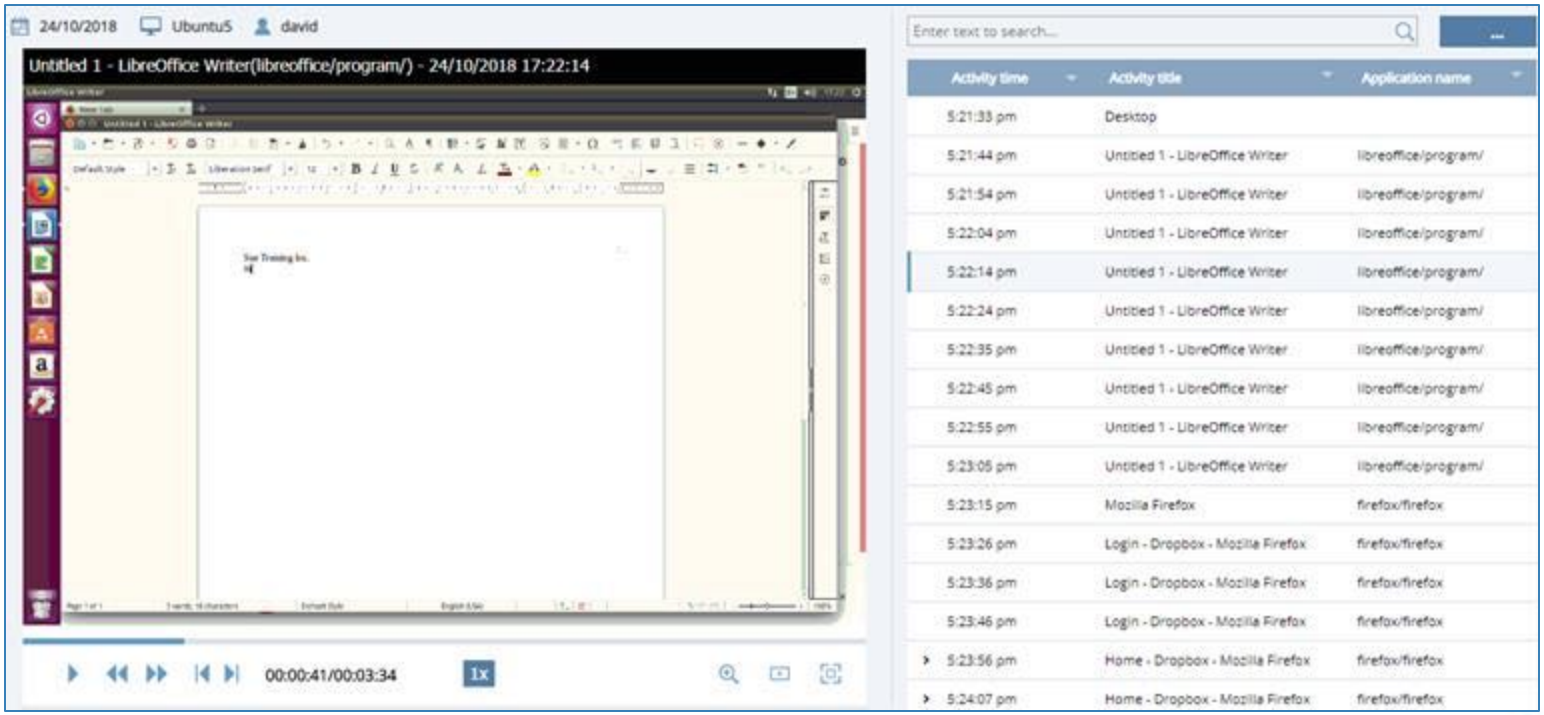
- **Działania użytkownika** (polecenia wejściowe i odpowiedzi z terminala)
- **Wywołania systemu**
- **Polecenia** wykonywane w uruchomionym skrypcie



Monitorowanie przez Linux Clients (Sesja Lokalna)

Lokalna sesja Linux na X Window System zawiera:

- Zrzuty ekranu (screenshots)
- Nazwę aplikacji
- Nazwę aktywności
- Czas aktywności

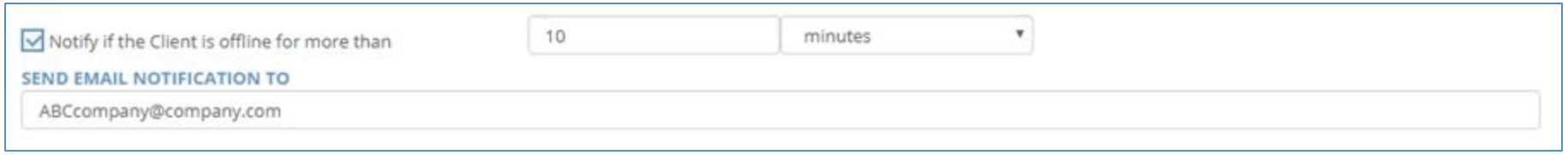


Offline Client Detection ("lost" Client)

Wykrywanie użytkowników offline

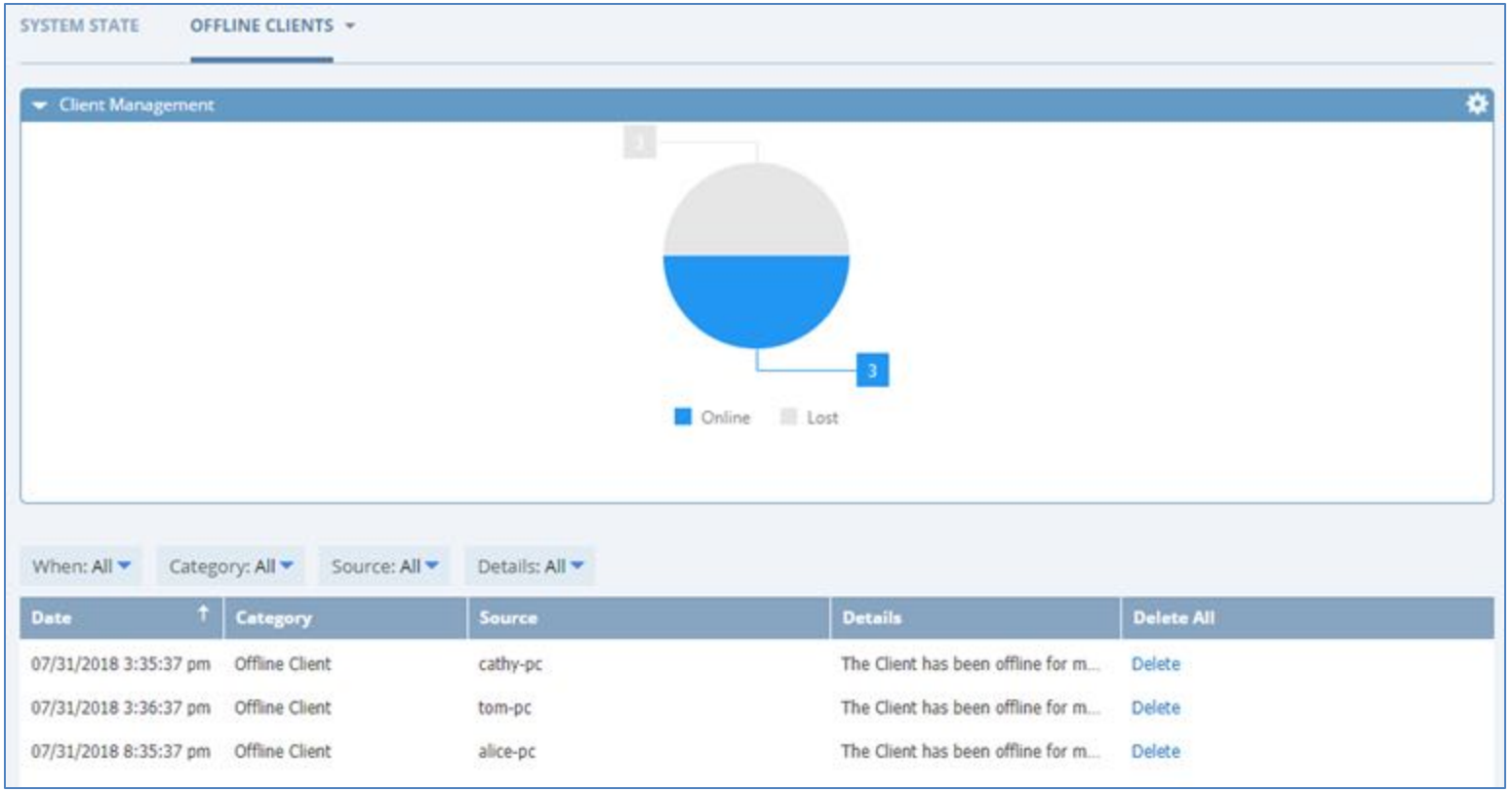
Offline Client Detection (“lost” Client)

Offline Client Detection pomoże Ci w terminowym wykrywaniu użytkowników, którzy przestali przesyłać dane z monitoringu. Wystarczy **zdefiniować czas**, po którego upływie aplikacja Ekran Client będzie uznawała ich za offline, czyli „lost”, aby **otrzymywać informacje** o takich zdarzeniach.



Wyświetlanie użytkowników offline

Po upływie określonego czasu istnieje **możliwość wyświetlenia** wszystkich użytkowników Ekran Client w trybie **offline**.



Ochrona Ekran Client

Tryb ochronny (Protected Mode)

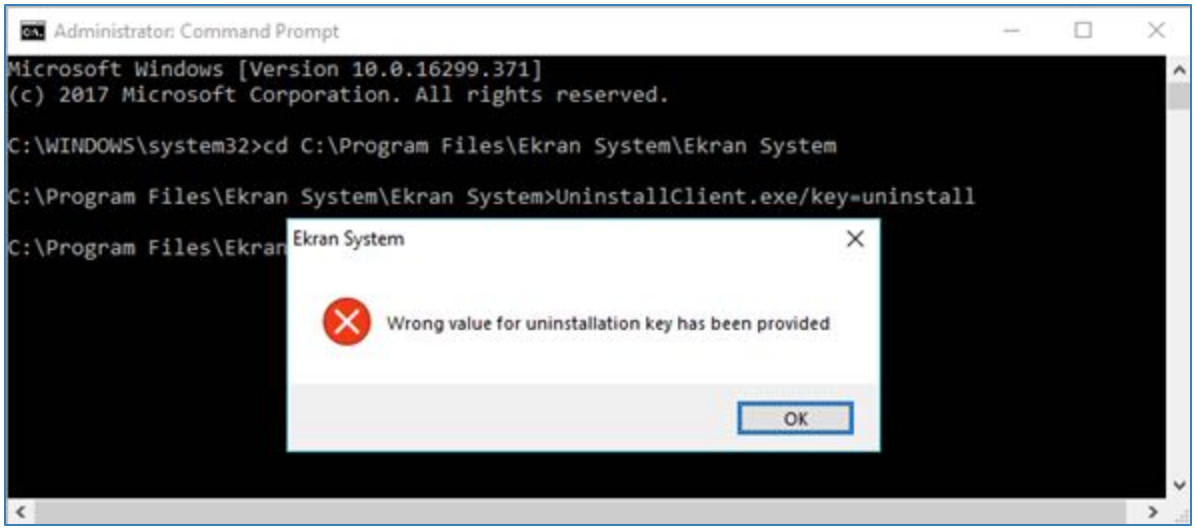
Ekran System umożliwia **ochronę komputerów** Windows z oprogramowaniem Ekran Client i ich **danych** poprzez włączenie trybu ochronnego (**Protected Mode**).

Korzystanie z trybu Protected Mode ma następujące korzyści:

- Zapobiega **dezinstalacji**.
- Zapobiega **zatrzymywaniu procesów**.
- Zapobiega **edycji plików systemowych i logów**.
- Zapobiega **edycji ustawień oprogramowania** Ekran Client w **rejestrze komputera**, na którym znajduje się aplikacja.
- Zapobiega **modyfikacji**, **usuwania** i **zmiany nazwy plików** aplikacji Ekran Client.

Odinstalowywanie aplikacji Ekran Client

Użytkownicy, w tym użytkownicy uprzywilejowani, nie są w stanie powstrzymać pracy aplikacji Ekran Client na swoich maszynach, jak również usunąć jej lokalnie bez pomocy Administratora Ekran System.



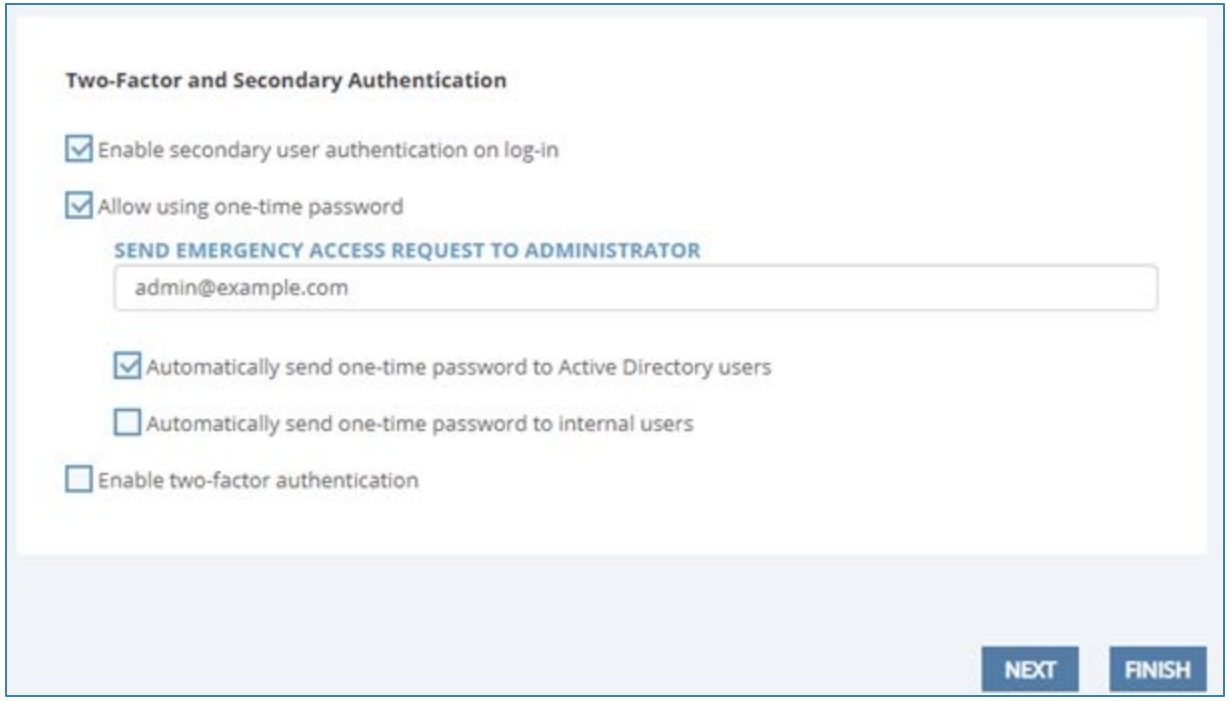
Tylko Administrator Ekran System zna klucz dezinstalacji, ustalony przed instalacją i konieczny do usunięcia lokalnego.

Zaawansowana autoryzacja użytkowników

Zaawansowana autoryzacja użytkowników

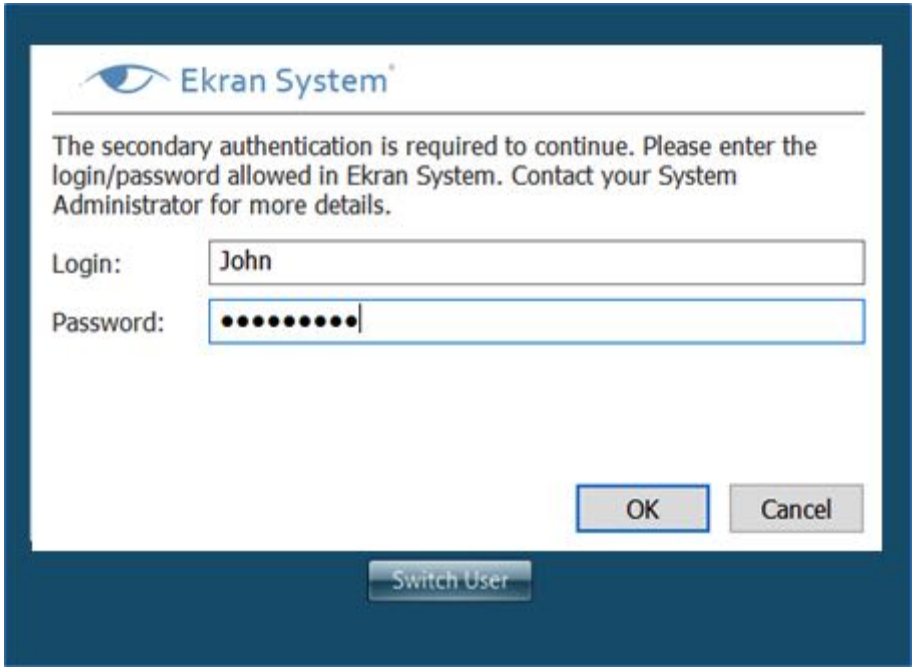
Zaawansowana autoryzacja użytkowników pozwala osiągnąć dwie korzyści:

- **Monitorowanie aktywności** użytkowników, gdy wielu użytkowników używa tych samych danych uwierzytelniających do logowania.
- **Poprawienie bezpieczeństwa**, ograniczając dostęp konkretnych użytkowników, którzy znają dodatkowe dane uwierzytelniające



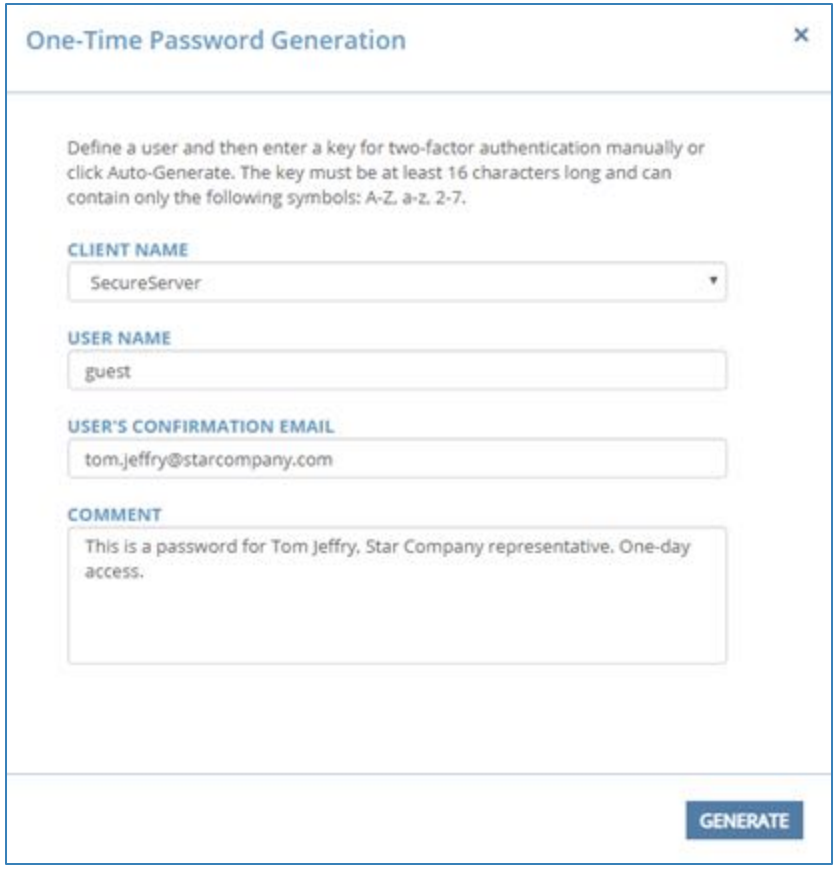
Zaawansowana autoryzacja użytkowników (Windows Client)

Ekran System Client wymaga wprowadzenia danych uwierzytelniających przed zezwoleniem użytkownikowi na pracę z systemem operacyjnym Windows.



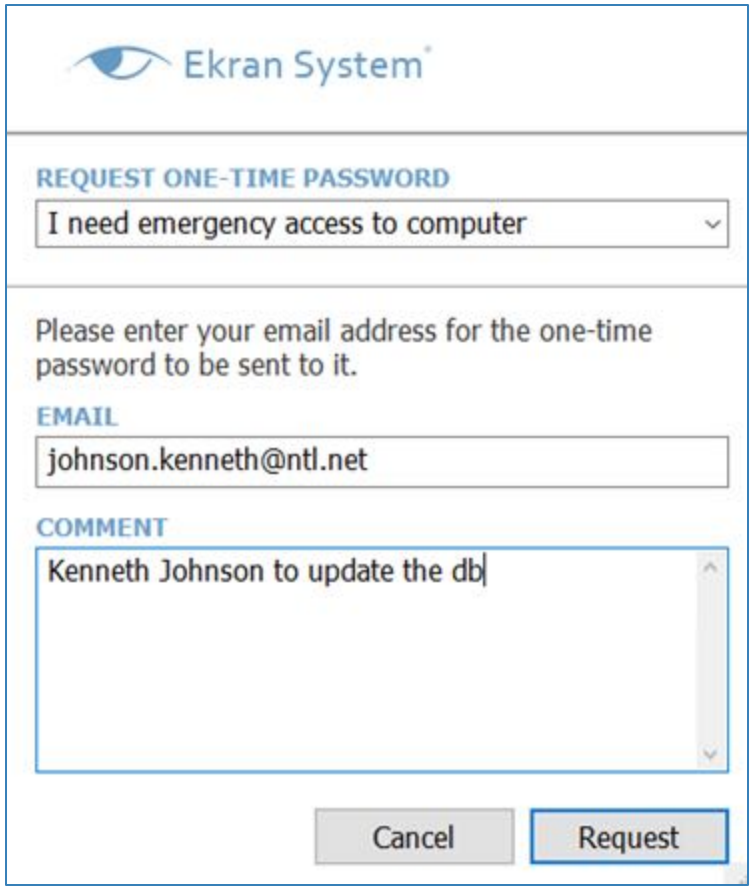
Jednorazowe hasła (Windows Clients)

Edycja Enterprise Ekran System zapewnia administratorowi unikalną możliwość ochrony komputera z zainstalowaną aplikacją Ekran Client za pomocą jednorazowego hasła.



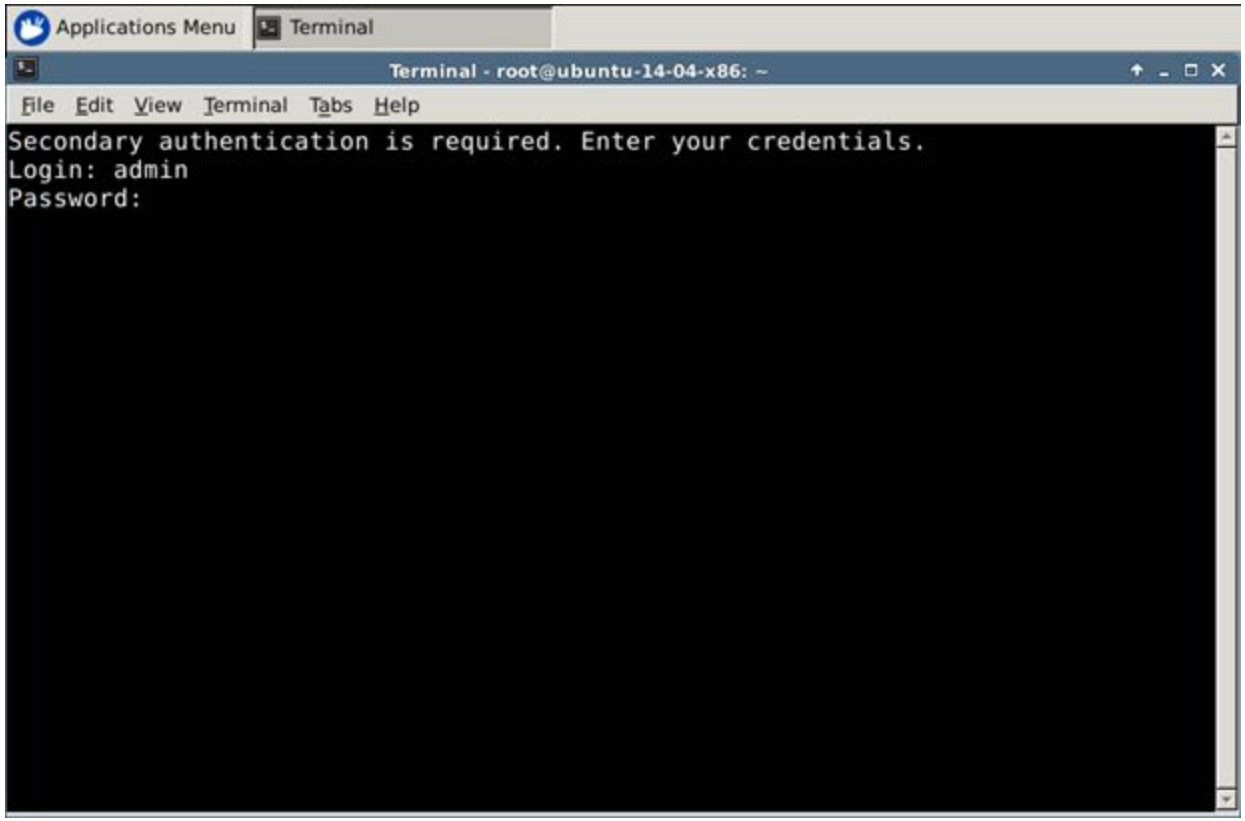
Jednorazowe hasła (Windows Clients)

Użytkownik może zażądać jednorazowego hasła bezpośrednio z dodatkowego okna uwierzytelniania wyświetlanego przy logowaniu do systemu operacyjnego Windows



Zaawansowana autoryzacja użytkowników (Linux Clients)

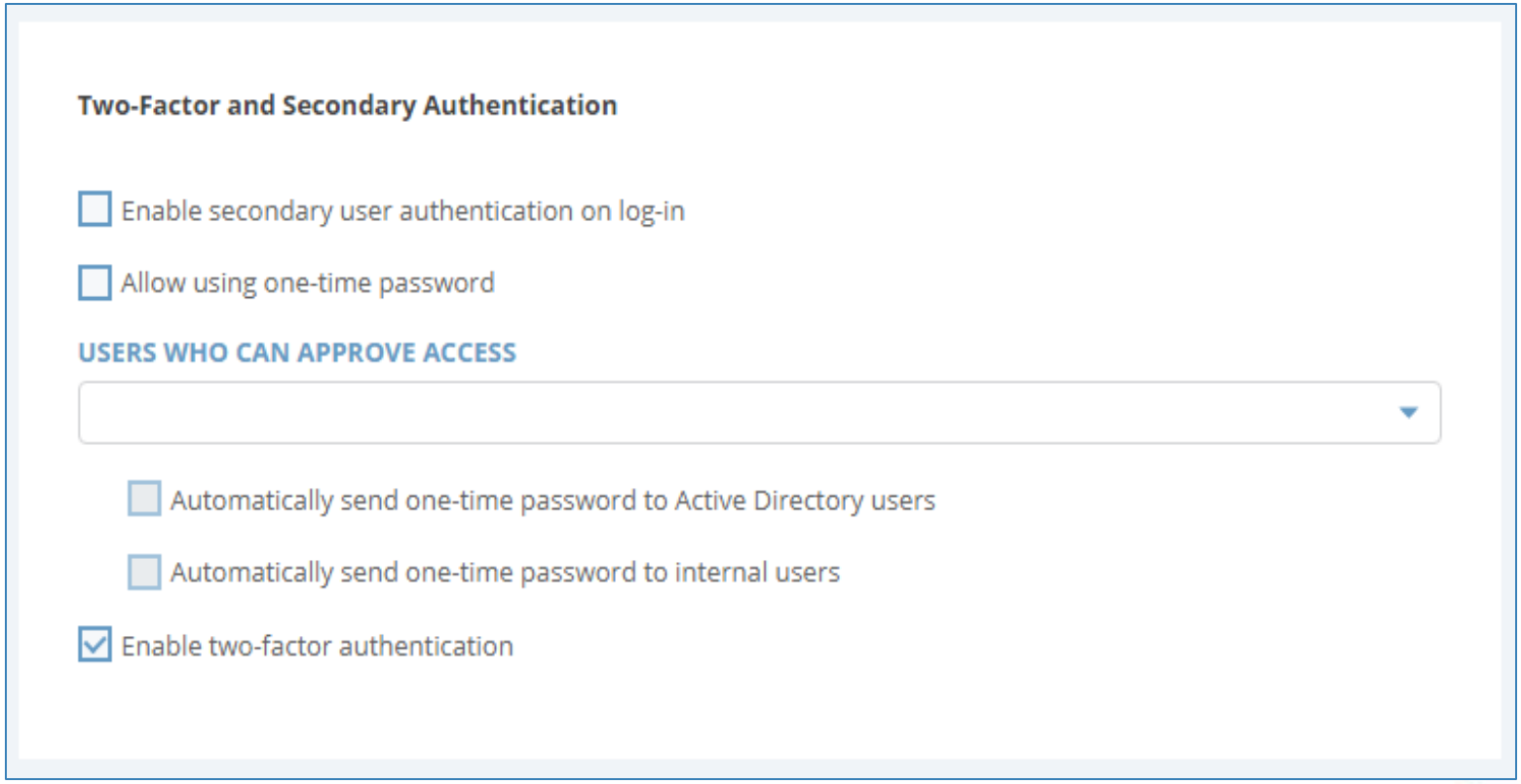
Ekran System Client wymaga wprowadzenia danych uwierzytelniających przed zezwoleniem użytkownikowi na pracę z terminalem na maszynach z aplikacją Ekran Client w systemie Linux.



Dwuskładnikowe uwierzytelnienie (2FA)

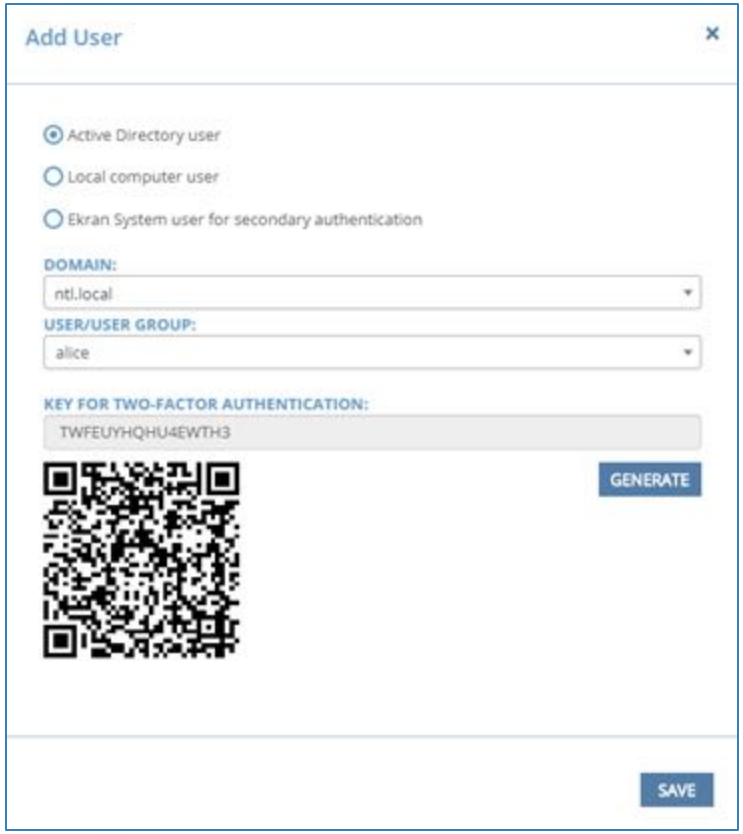
Dwuskładnikowe uwierzytelnienie

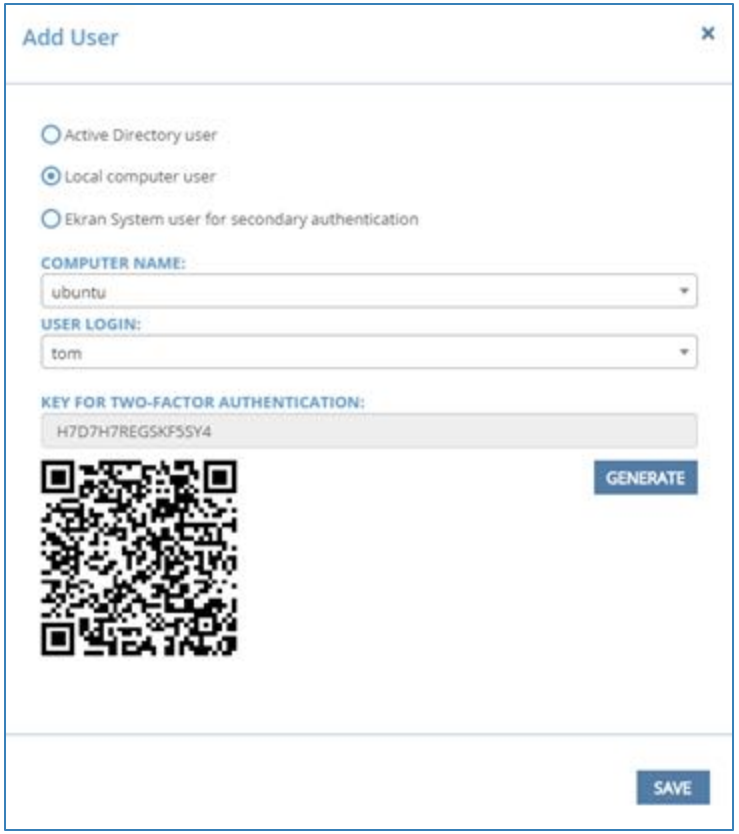
Autoryzacja dwuskładnikowa pozwala na włączenie dodatkowej warstwy zabezpieczeń w celu lepszej ochrony krytycznych punktów końcowych w sieci.



Dwuskładnikowe uwierzytelnienie

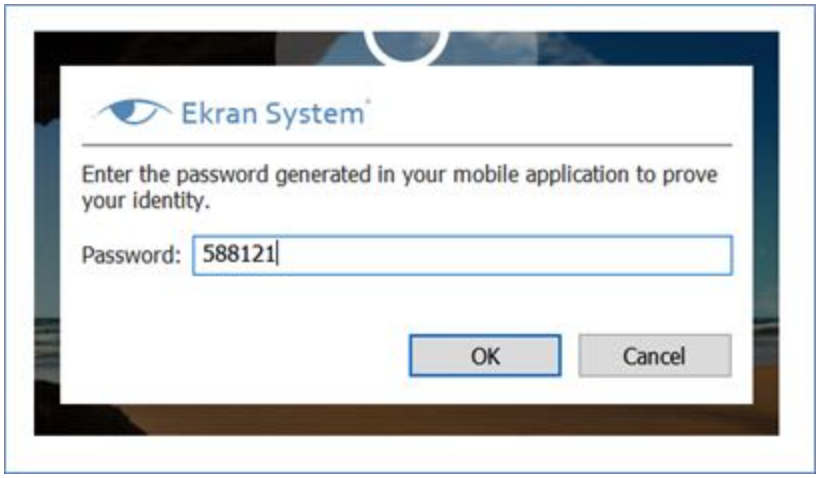
Dodawanie użytkowników, którzy będą mogli logować się na komputerach z zainstalowanym systemem Windows i Linux z aplikacją Ekran Client przy użyciu **jednorazowych haseł** (TOTP) generowanych w aplikacjach mobilnych TOTP.





Dwuskładnikowe uwierzytelnienie

Ekran System Client **prosi użytkownika o wprowadzenie** TOTP w celu rozpoczęcia pracy z systemem.




```
Ubuntu 16.04.2 LTS ubuntu tty2

ubuntu login: May
Password:
Last login: Fri May  3 01:45:16 PDT 2019 on tty2
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

Enter the password generated in your mobile application to prove your identity
Enter pin: _
```

Password Management

Password Management

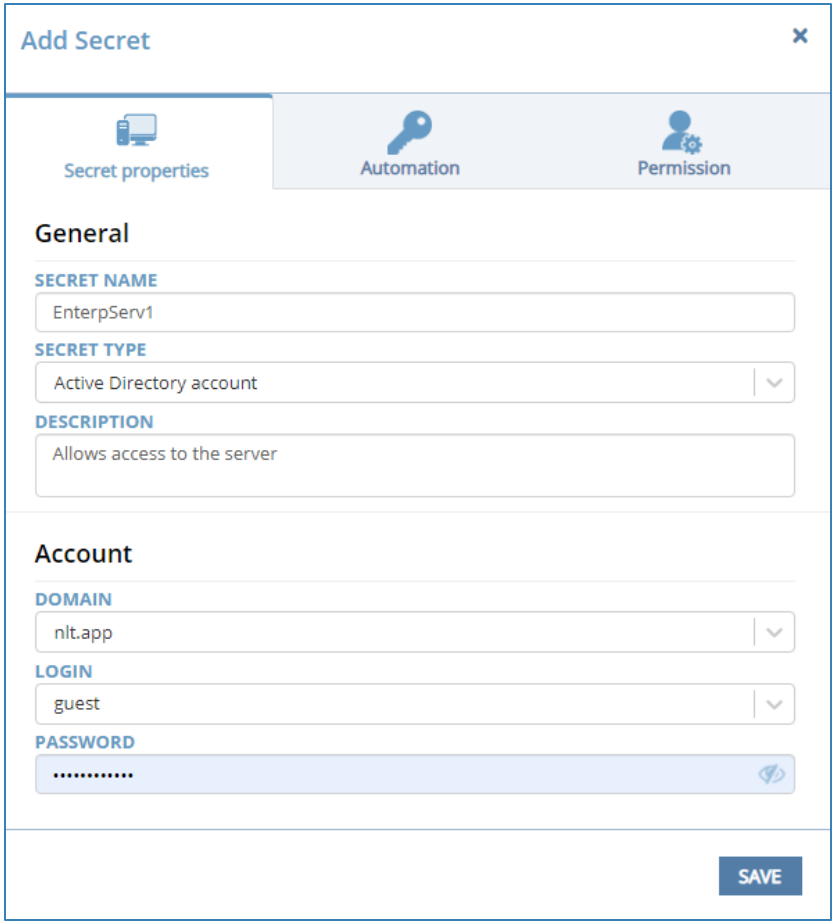
Zarządzanie uprzywilejowanymi kontami i wdrażanie dostępu na podstawie ról ma kluczowe znaczenie dla zespołów ds. bezpieczeństwa w przedsiębiorstwie. Funkcjonalność **zarządzania hasłami (Password Management)** w systemie Ekran System zapewnia pełną kontrolę i przejrzystość w zakresie uprzywilejowanego dostępu użytkowników.

Ekran System pozwala na:

- Bezpieczne **przechowywanie** danych uwierzytelniających.
- **Zapewnienie** użytkownikom **dostępu** do wybranych poświadczeń logowania.
- Zarządzanie hasłami bez zakłócania przepływu pracy uprzywilejowanych użytkowników.
- Umożliwia zdalną rotację haseł (dla kont Active Directory, MS SQL, Windows i Unix SSH) oraz rotację kluczy SSH Unix

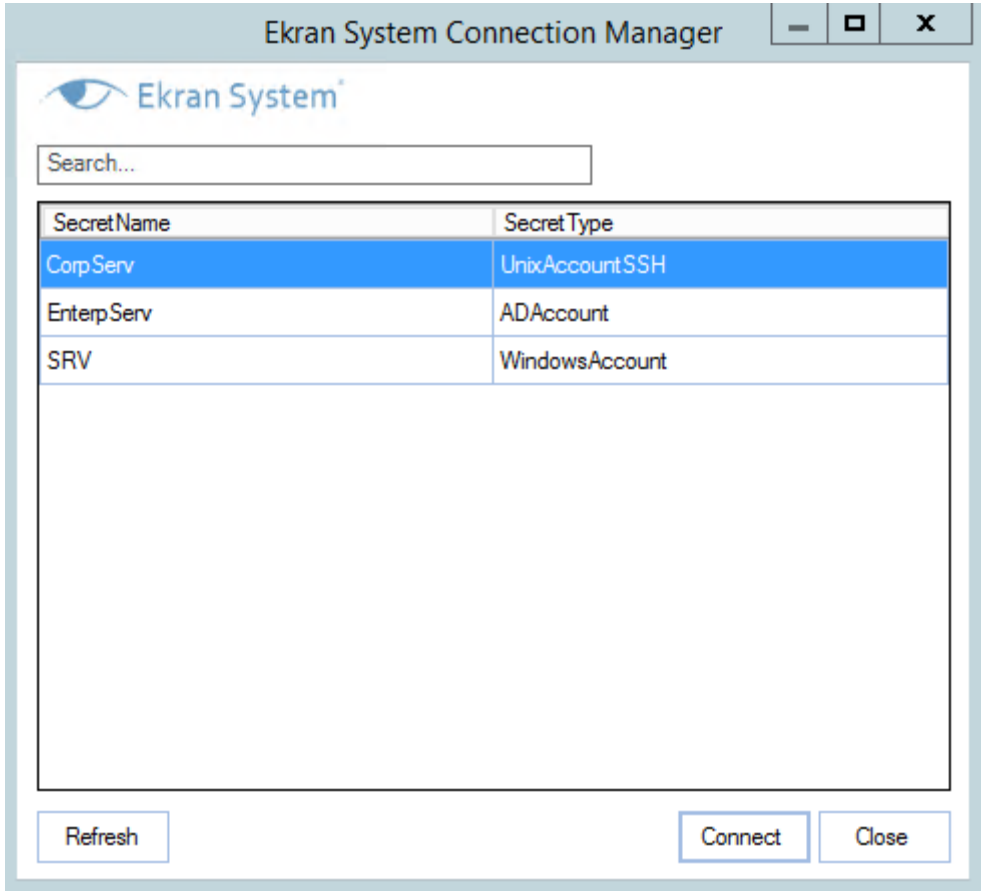
Nadawanie dostępu (Secret)

Wprowadź poświadczenia logowania oraz wybierz użytkownika, który może z nich korzystać. Dane logowania będą przekazane w tle i pozostaną niejawne dla użytkownika.



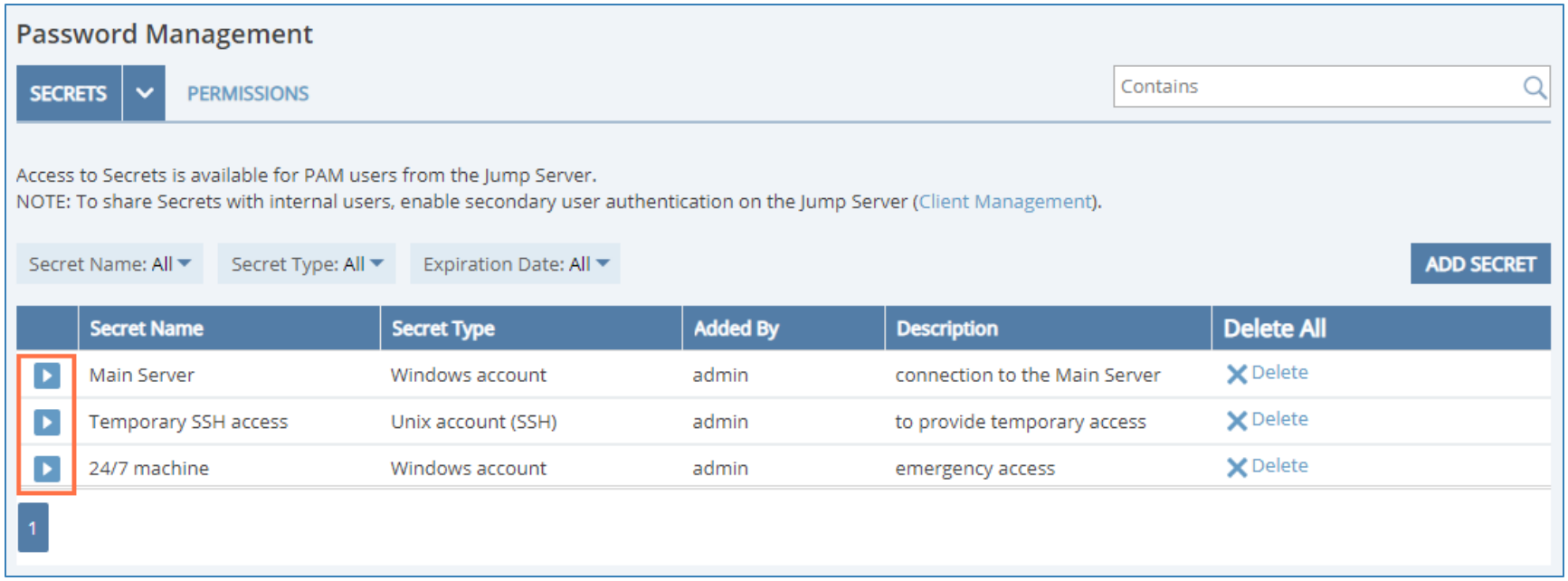
Logowanie przez nadanie dostępu (Secret)

Uprzywilejowany użytkownik może uzyskać dostęp do krytycznego punktu końcowego poprzez nadanie dostępu (Secret) za pomocą Ekran System Connection Manager.



Przeglądanie sesji z nadaniem dostępu (Secret)

Możesz w łatwy sposób przejść do sesji, w której użyto nadawania dostępu (Secret). Dodatkowo w odtwarzaczu, informacje o nadaniu dostępu (Secret) będą podświetlone na niebiesko, dzięki czemu można je szybko i łatwo znaleźć.



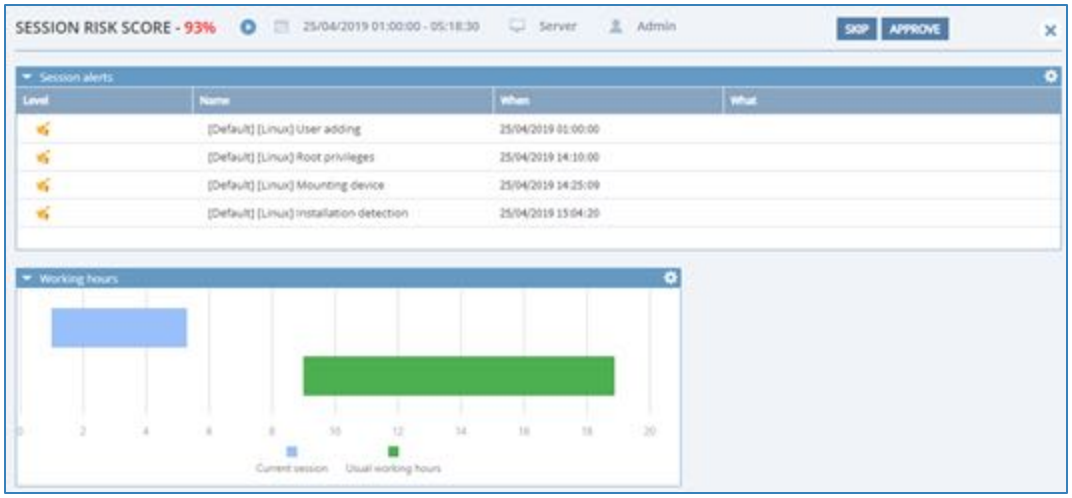
Analiza zachowań użytkowników i podmiotów

Analiza zachowań Użytkowników i Podmiotów

Analiza zachowań użytkowników i podmiotów (UEBA) pozwala lepiej chronić system przed złośliwymi i nielegalnymi osobami mającymi dostęp do informacji poufnych.

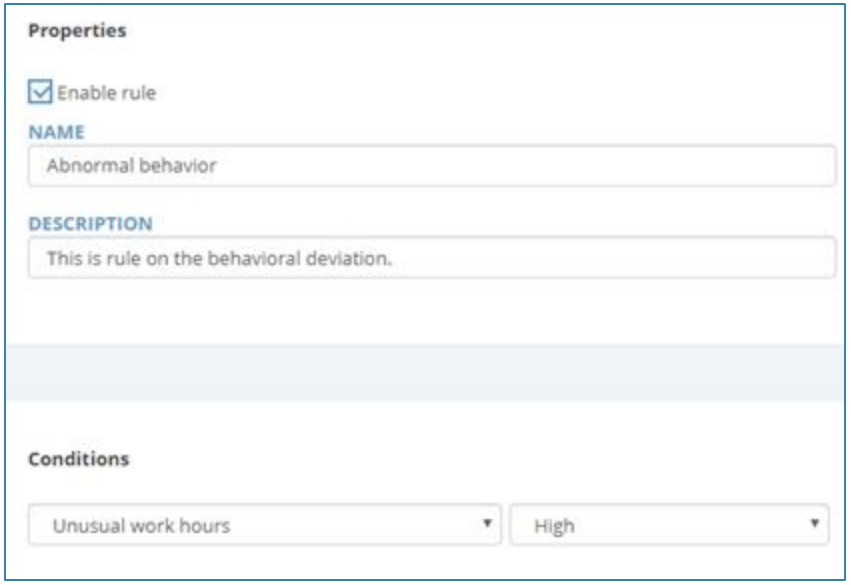
UEBA ma następujące zalety w wykrywaniu podejrzanych działań:

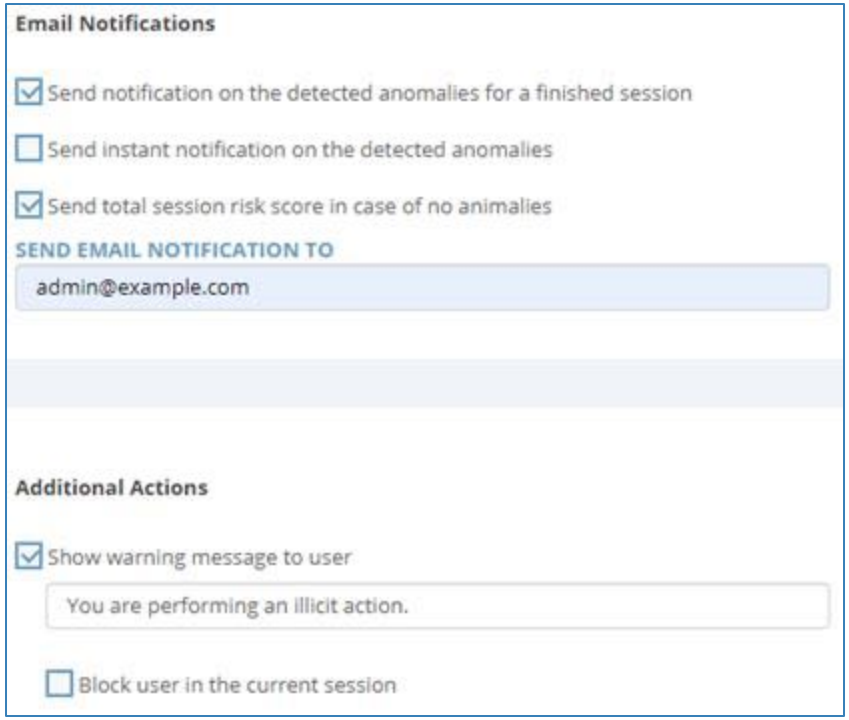
- **Analiza wzorców zachowań** użytkowników i **ustalenie** linii odniesienia dla **normalnych zachowań**.
- Automatyczne **wykrywanie odchyleń** behawioralnych.
- Terminowe **powiadamianie** o potencjalnych zagrożeniach.



Analiza zachowań użytkowników i podmiotów

Dodaj regułę zachowania użytkownika, aby przeglądać profile użytkowników, analizować sesje z wykrytymi anomaliami i otrzymywać na czas powiadomienia o ryzykownej aktywności użytkownika.

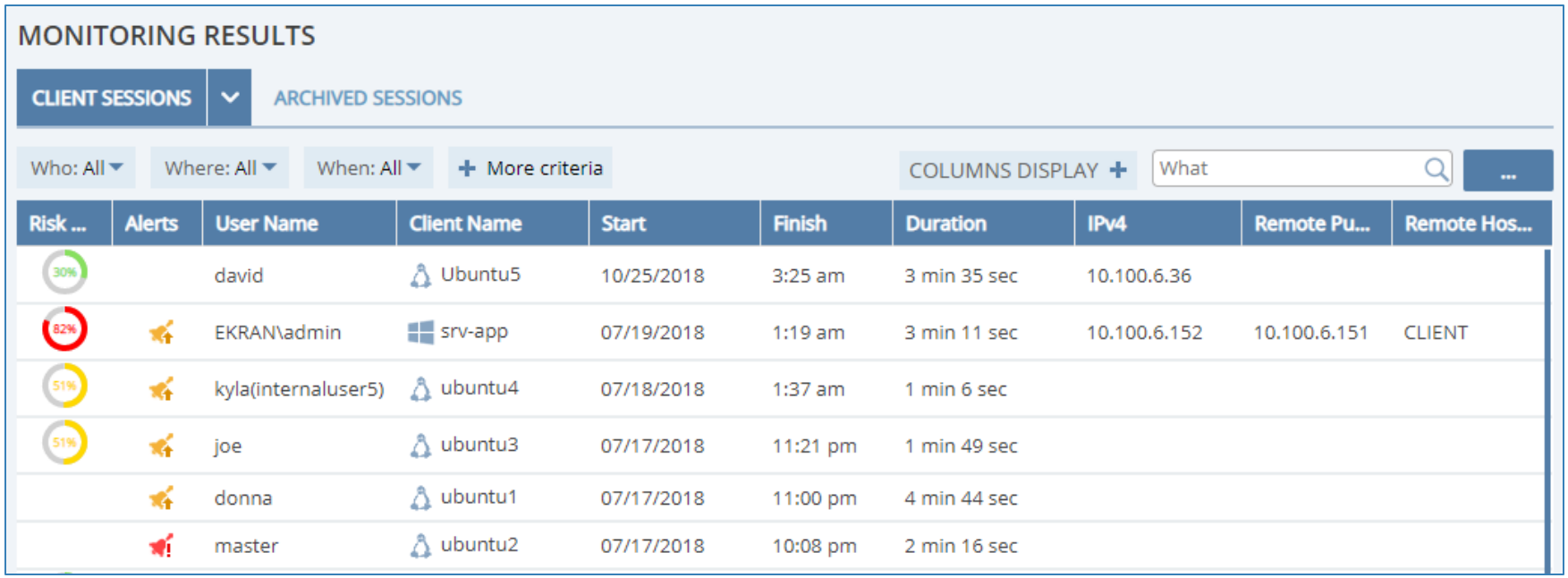




Analiza zachowań użytkowników i podmiotów

Monitorowanym sesjom, które zawierają wykryte anomalie zachowań użytkowników, nadawany jest **wynik ryzyka (risk score).**

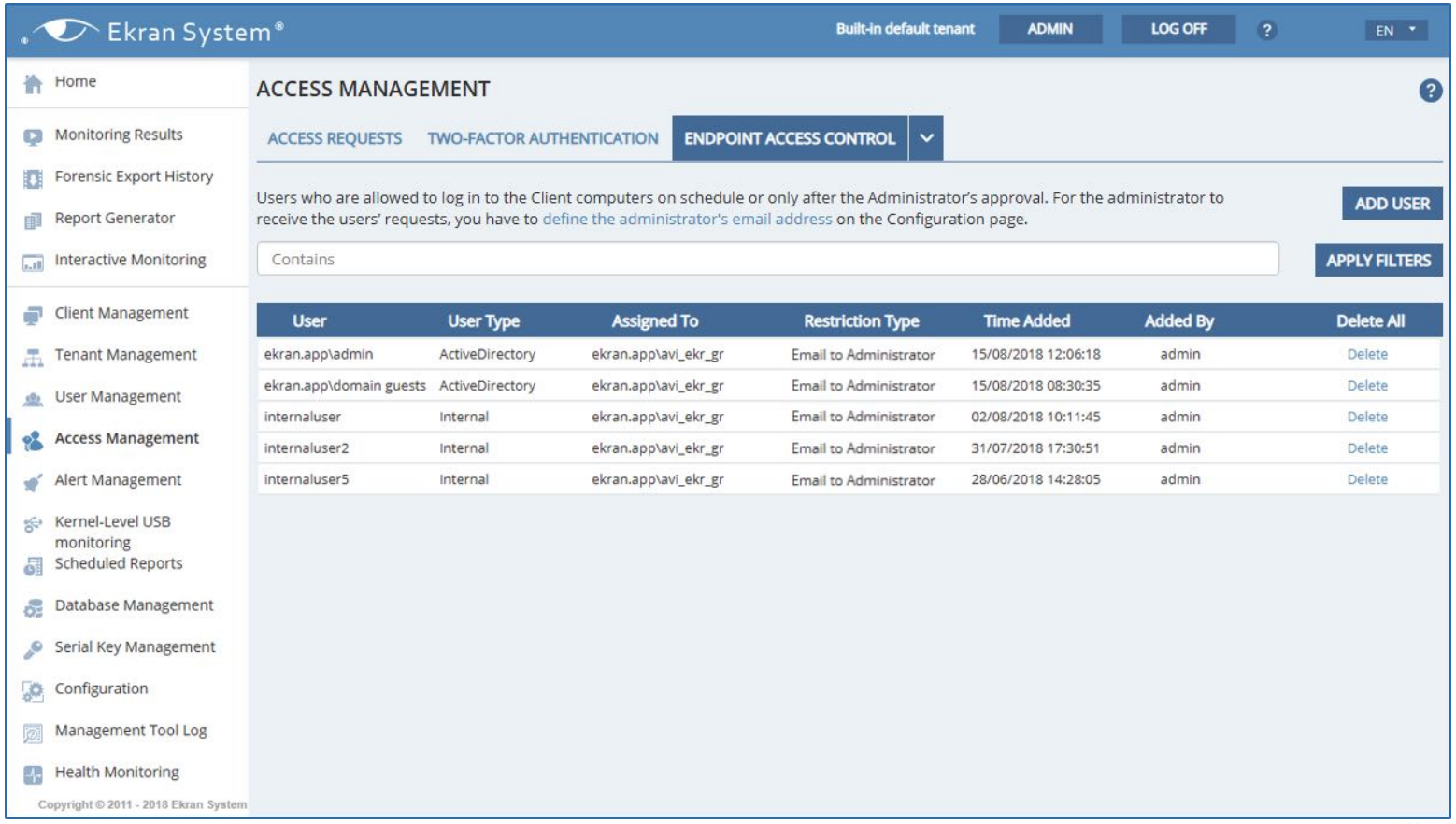
Wynik ryzyka (risk score) wskazuje **stopień zagrożenia sesji** i jest obliczany na podstawie **nieprawidłowych wzorców** zachowań użytkowników i **ostrzeżeń** wykrytych podczas monitorowanej sesji.



Zgoda administratora na logowanie

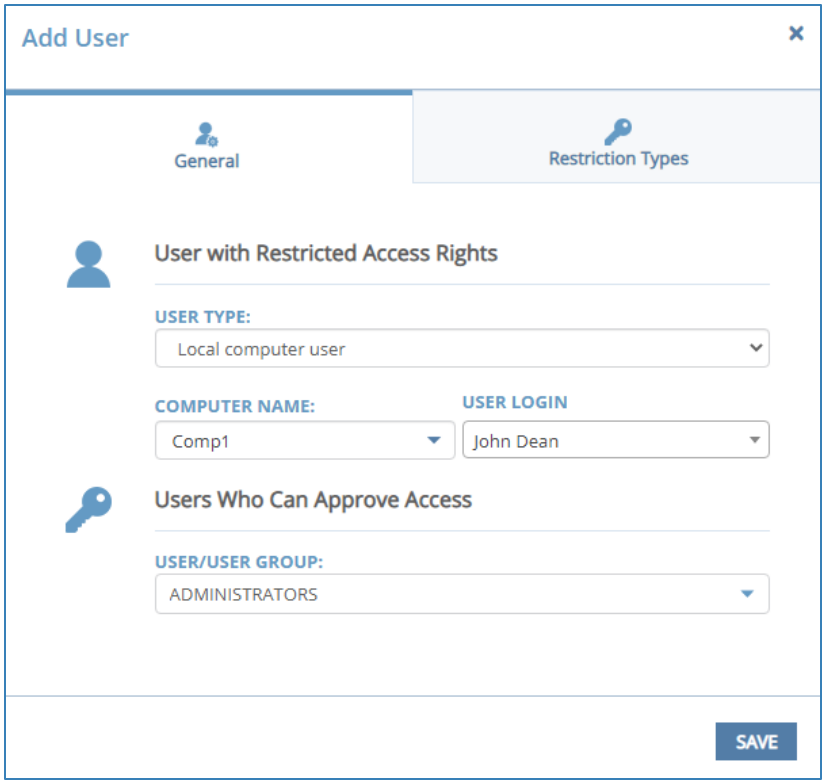
Zgoda administratora na logowanie

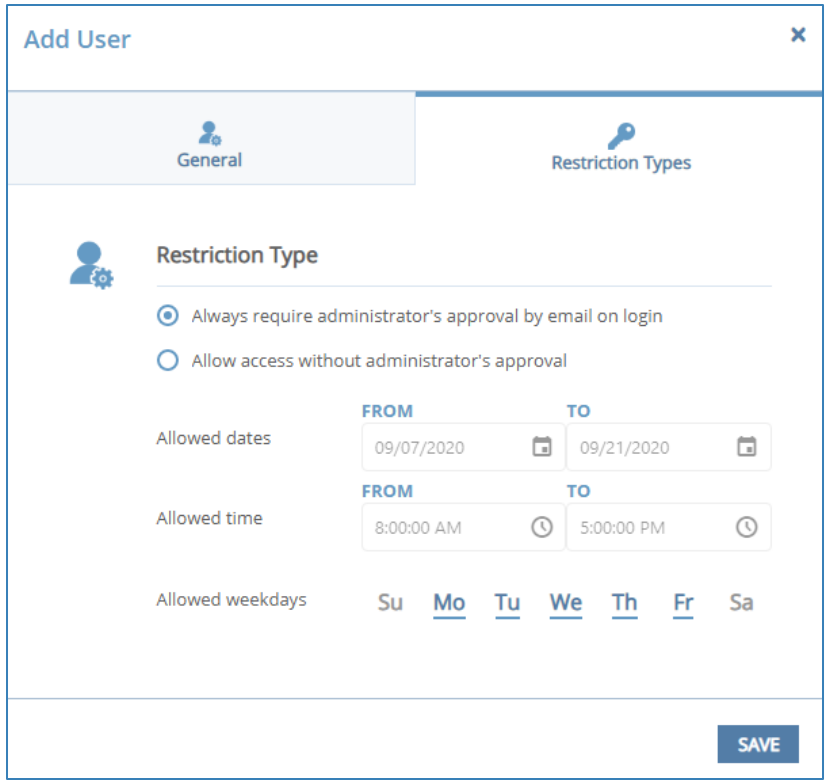
Zgoda administratora na zalogowanie się pozwala na lepszą ochronę komputerów z agentem Ekran Client przed niepożądanym dostępem.



Zgoda administratora na logowanie

Dodaj użytkowników dla których **dostęp** do komputerów z oprogramowaniem Ekran Client musi być **ograniczony**.



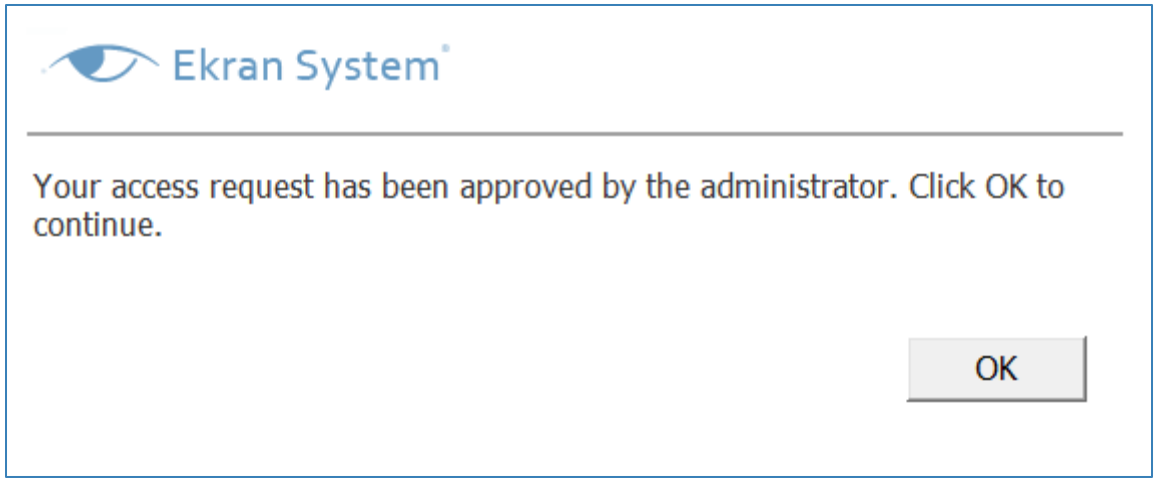


Zgoda administratora na logowanie

Gdy użytkownik z ograniczonym dostępem zaloguje się do komputera, Ekran Client blokuje pulpit i wysyła żądanie dostępu użytkownika do administratora. Dodatkowo żądanie dostępu użytkownika pojawia się również w zakładce Access Management.

Zgoda administratora na logowanie

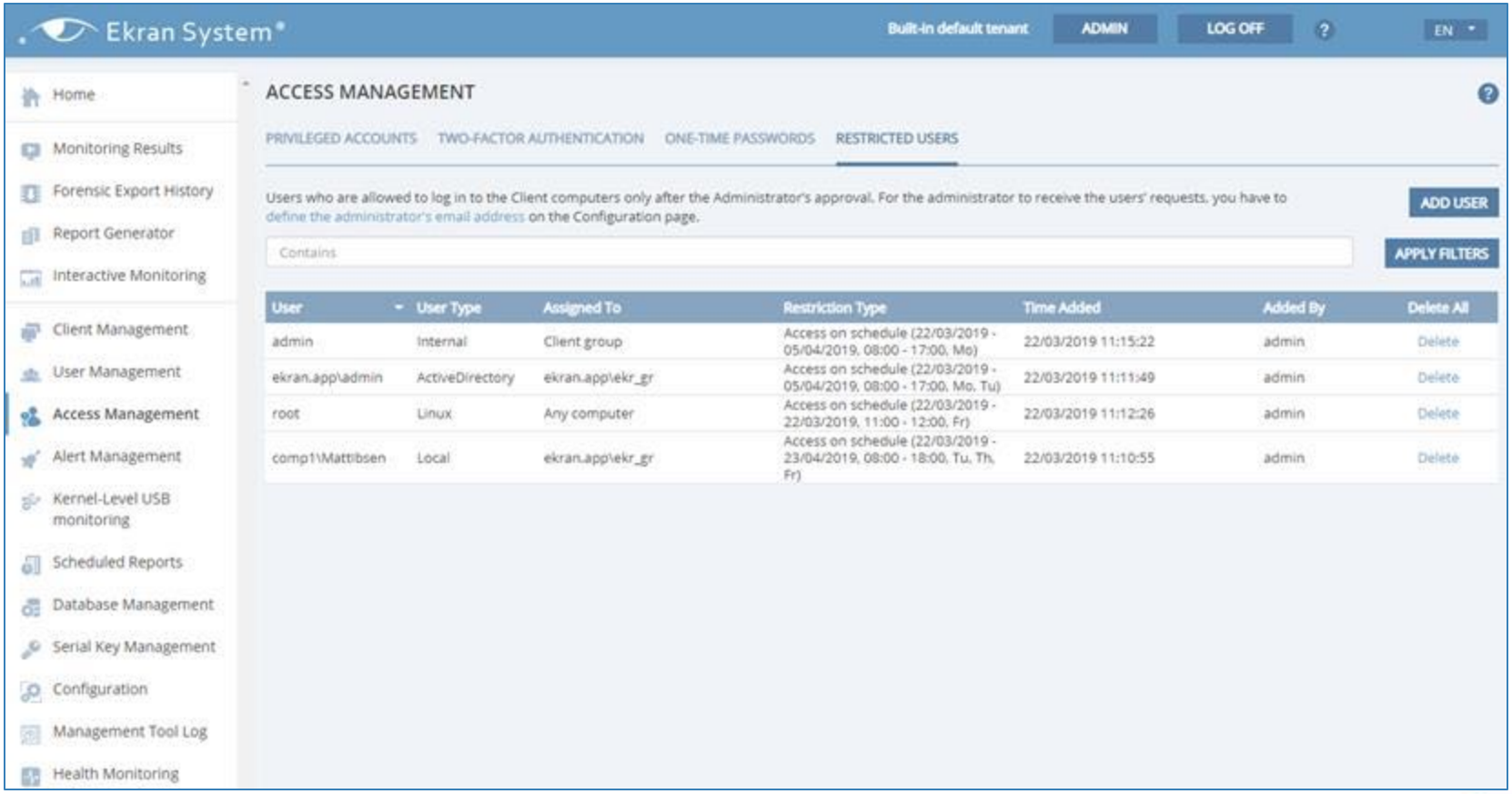
Po zatwierdzeniu przez administratora żądania dostępu, użytkownik może rozpocząć pracę z systemem.



Przyznawanie dostępu według harmonogramu

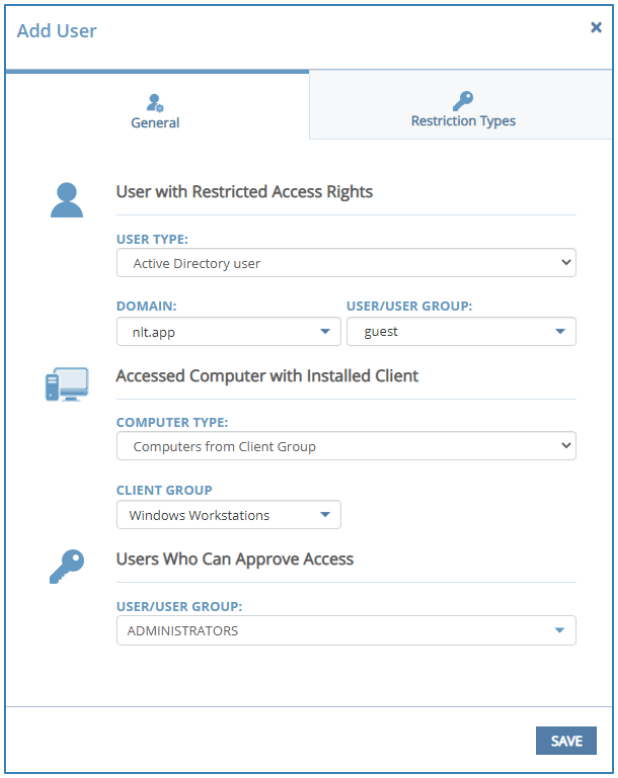
Przyznawanie dostępu według harmonogramu (Enterprise Edition)

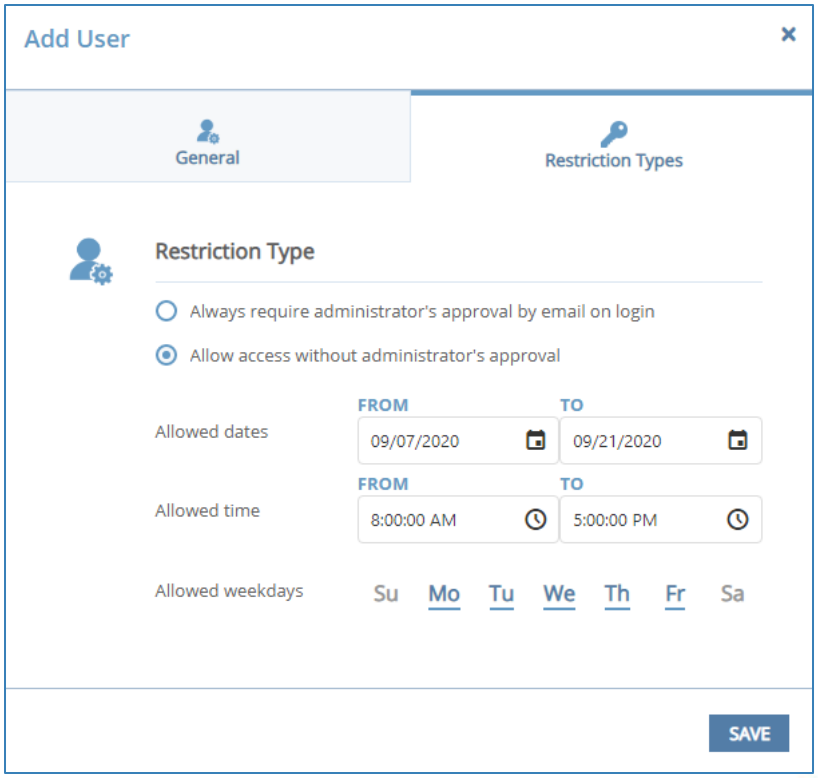
Przyznanie dostępu użytkownika na podstawie harmonogramu pozwala chronić komputery z programem Ekran Client przed dostępem w niepożądanym czasie.



Przyznawanie dostępu użytkownikowi według harmonogramu (Enterprise Edition)

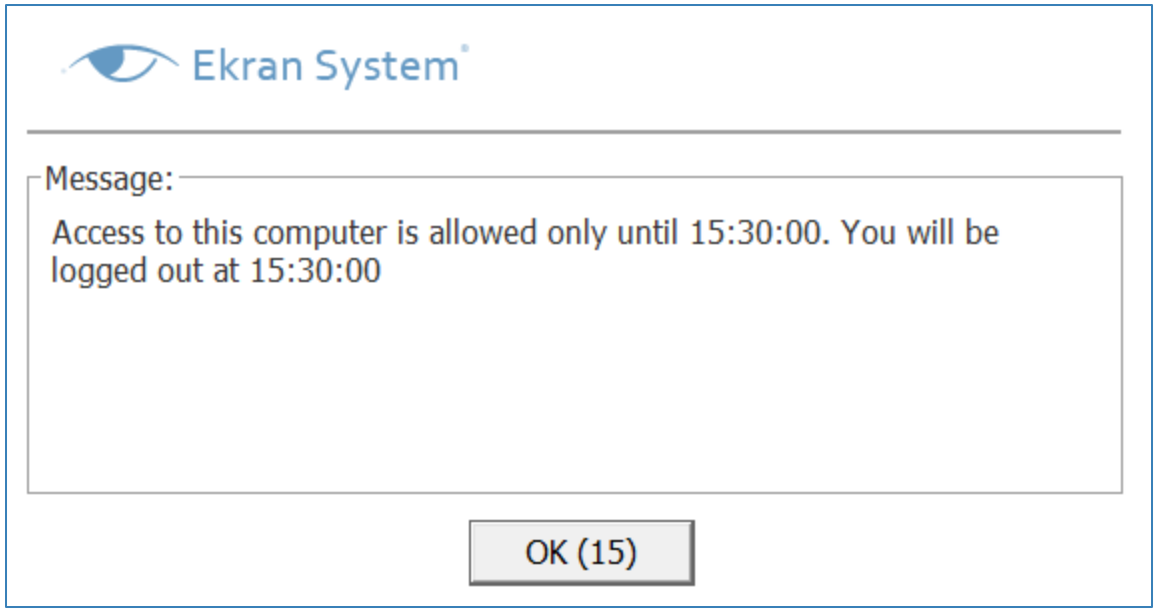
Dodaj użytkowników, których dostęp do komputerów z Ekran Client będzie udzielony tylko na określony czas. Logowanie poza zdefiniowanym przedziałem czasowym będzie wymagało zgody administratora.





Przyznawanie dostępu według harmonogramu (Enterprise Edition)

Użytkownicy o ograniczonym dostępie będą mogli zalogować się do komputerów z Ekran Client w określonym czasie i będą potrzebowali zgody administratora na zalogowanie poza tym okresem.

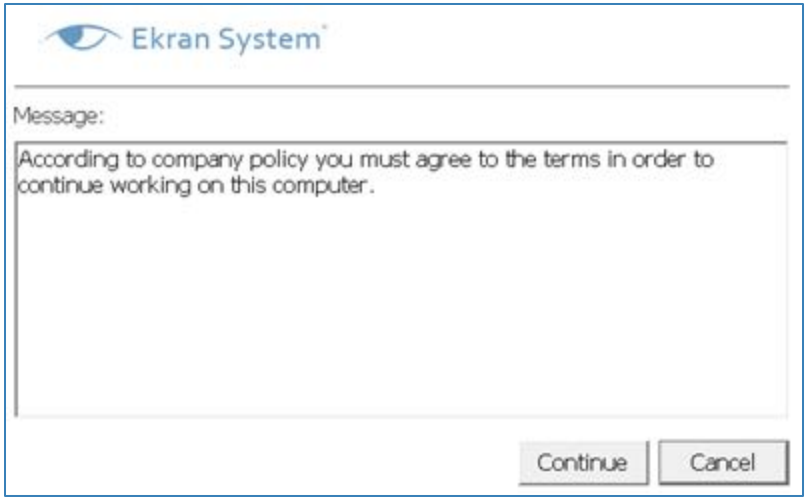


Powiadamianie użytkowników o monitorowaniu

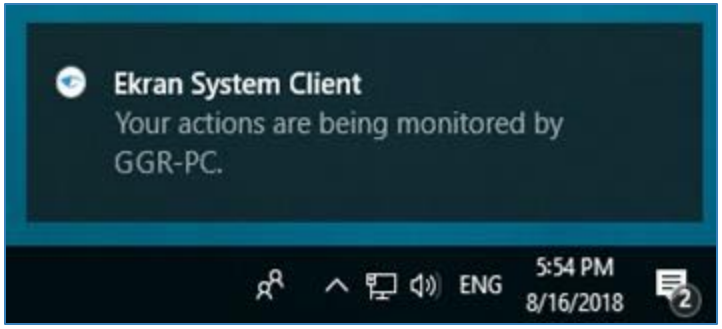
Powiadamianie użytkowników o monitorowaniu

Aby postępować zgodnie z polityką bezpieczeństwa firmy lub przepisami obowiązującymi w danym kraju, możesz:

- Włączyć wyświetlanie dodatkowego komunikatu podczas logowania użytkownika w celu powiadomienia go, że jego praca jest monitorowana.

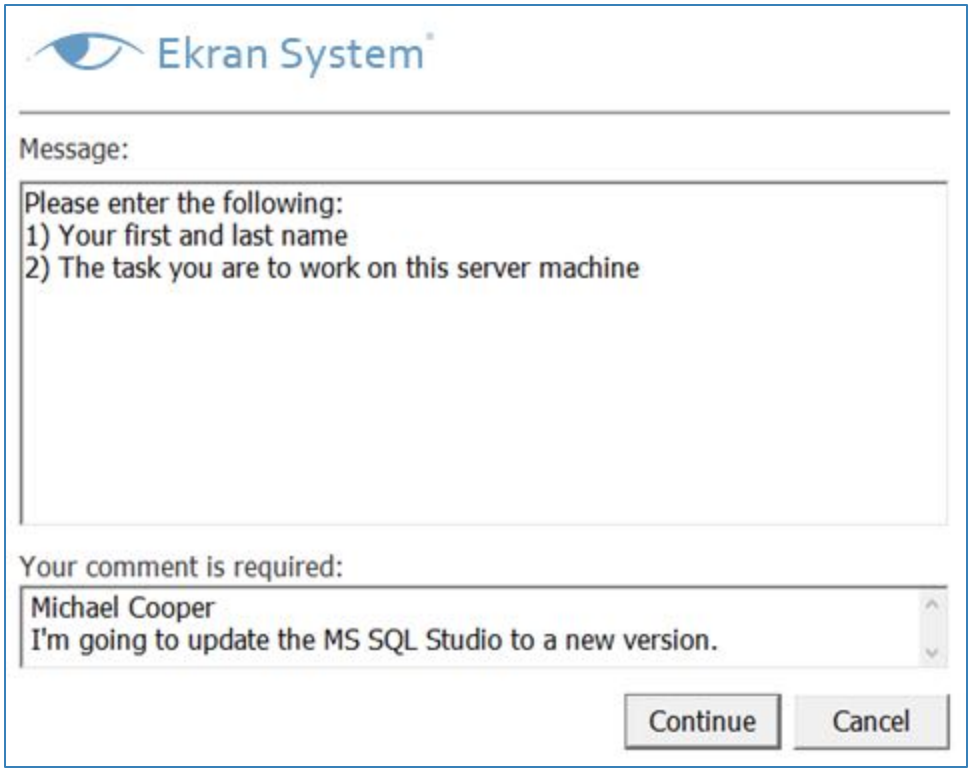


- Włączyć wyświetlanie ikony Ekran Client z powiadomieniem użytkownika o monitorowaniu.



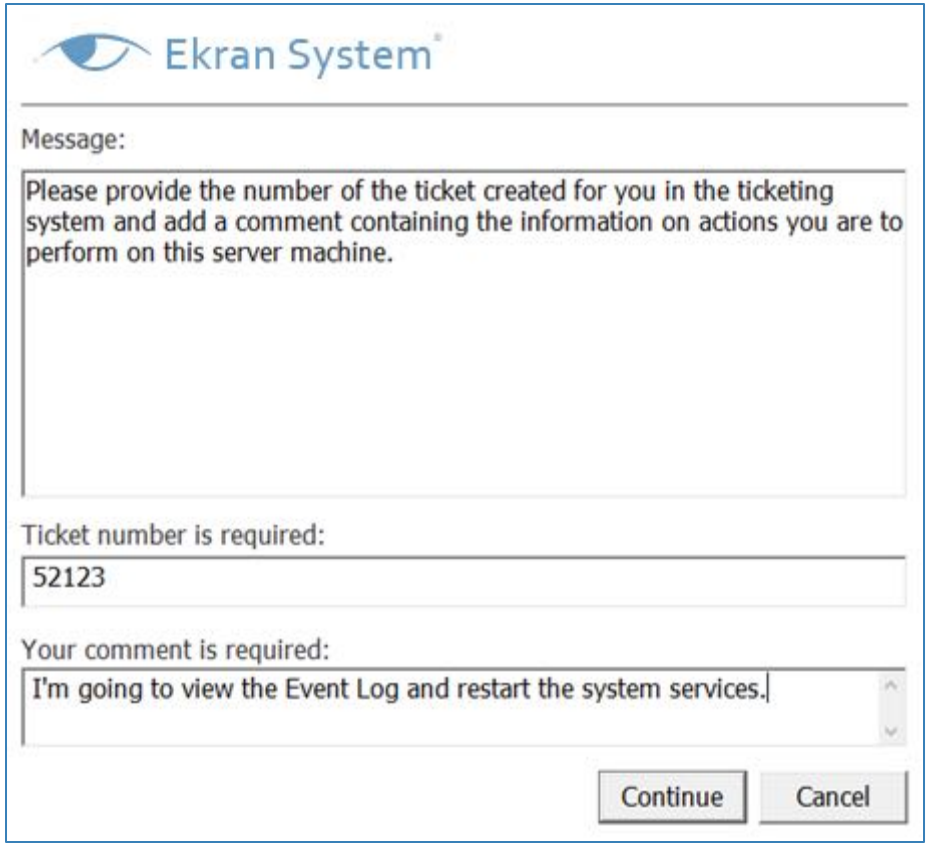
Powiadamianie użytkowników o monitorowaniu

Wymaganie od użytkowników wprowadzenia **komentarza** do dodatkowego **komunikatu wyświetlanego** przy logowaniu do komputerów z aplikacją Ekran Client.



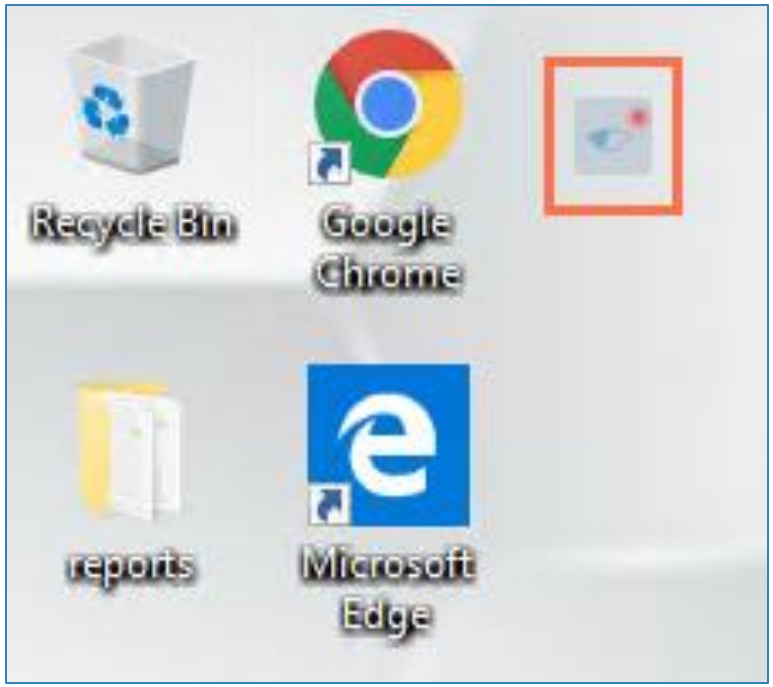
Powiadamianie użytkowników o monitorowaniu

Wymaganie od użytkownika wprowadzenia **numeru zgłoszenia** wygenerowanego w **systemie zgłoszeń**, żeby móc rozpocząć pracę na komputerze z Ekran Client.



Powiadamianie użytkowników o monitorowaniu

Wyświetlenie **ikony** na pulpicie, która będzie informować użytkowników o tym, że ich praca jest **aktualnie nagrywana**.

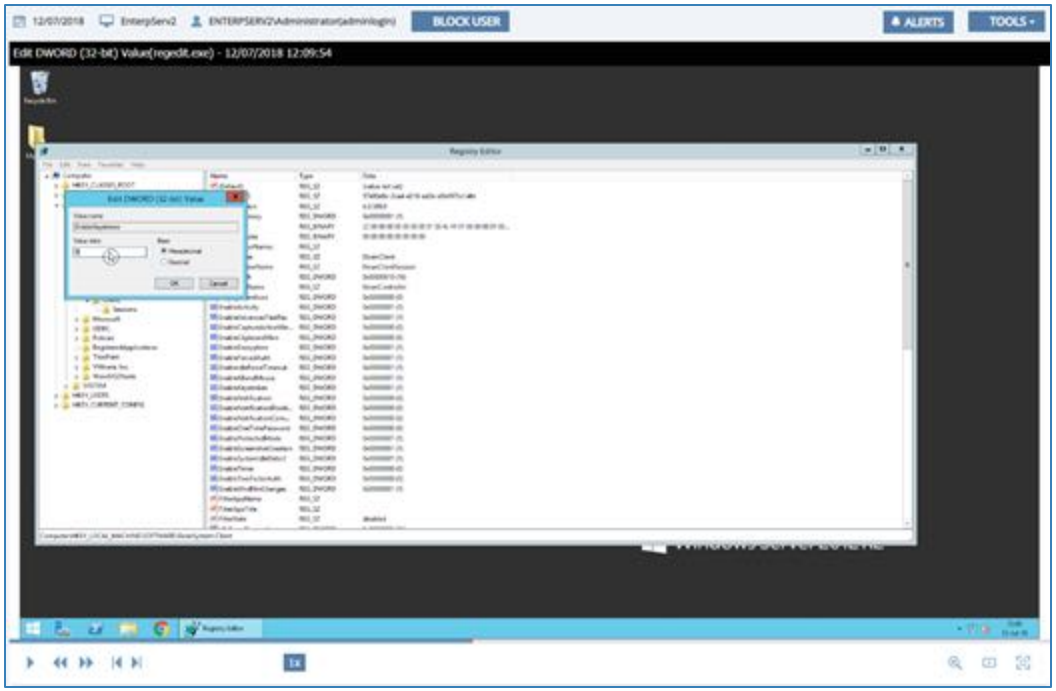


Blokowanie użytkowników

Blokowanie użytkowników

Ekran System umożliwia **blokowanie** użytkowników wykonujących potencjalnie szkodliwe i zabronione działania na komputerach z systemem operacyjnym Windows z zainstalowanym Ekran Client.

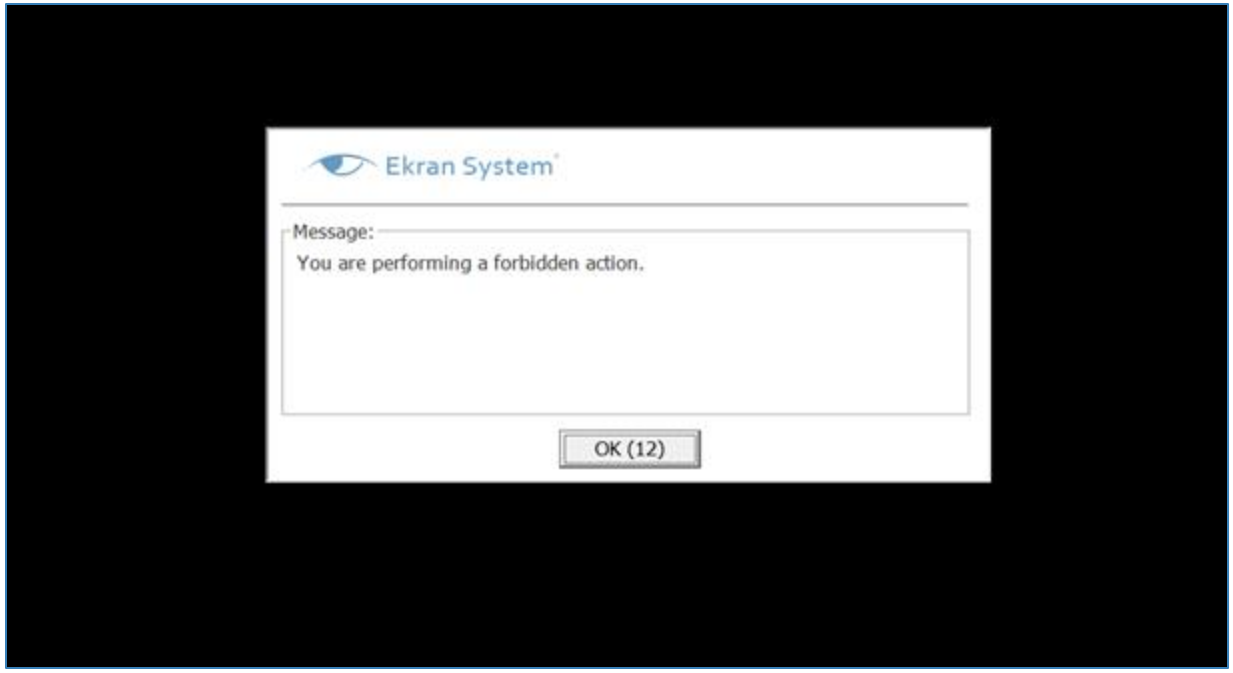
Użytkownicy mogą być blokowani ręcznie zarówno z sesji **Live**, jak i **Finished**, lub automatycznie, gdy wykonują czynność, która wyzwala określone ostrzeżenie.



Blokowanie użytkowników

Pulpit użytkownika jest **blokowany**, a po upływie określonego przedziału czasu użytkownik jest **przymusowo wylogowywany**.

Jeżeli zablokowany użytkownik będzie próbował zalogować się do komputera z Ekran Client, system nie pozwoli mu na to.



Lista zablokowanych użytkowników

Lista zablokowanych użytkowników zawiera informacje o tym, **kiedy** i **dlaczego** użytkownik został **zablokowany**.

Aby **umożliwić** użytkownikom **dostęp** do komputera z Ekran Client, **usuń** ich z listy.

Windows User	Blocked on	Blocked by	Date	Reason	Remove All
COMP19\NickolasSherry	Comp19	admin	10/07/2018 16:26:37	The user is removing necessary database fields	Remove
COMP11\John	Comp11	otheruser	10/07/2018 16:30:57	Social networks	Remove
COMP2\alan	Comp2	otheruser	10/08/2018 15:50:44	Online games	Remove
COMP22\max	Comp22	admin	10/08/2018 16:15:10	Hacking software	Remove
COMP4\kate	Comp4	otheruser	10/10/2018 09:35:23	Online games	Remove

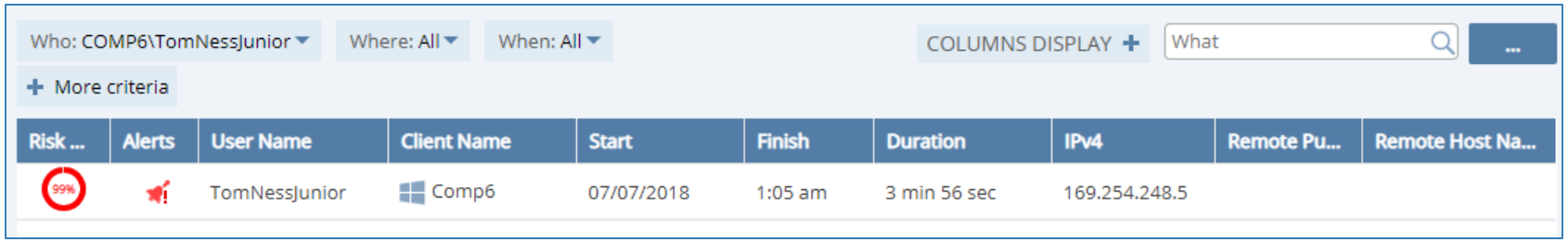
Przeglądanie Sesji

Wyszukiwanie Danych na liście sesji

Narzędzie Ekran System Management Tool umożliwia wyszukiwanie w nagranych sesjach.

Wyszukiwanie odbywa się przy użyciu różnych parametrów:

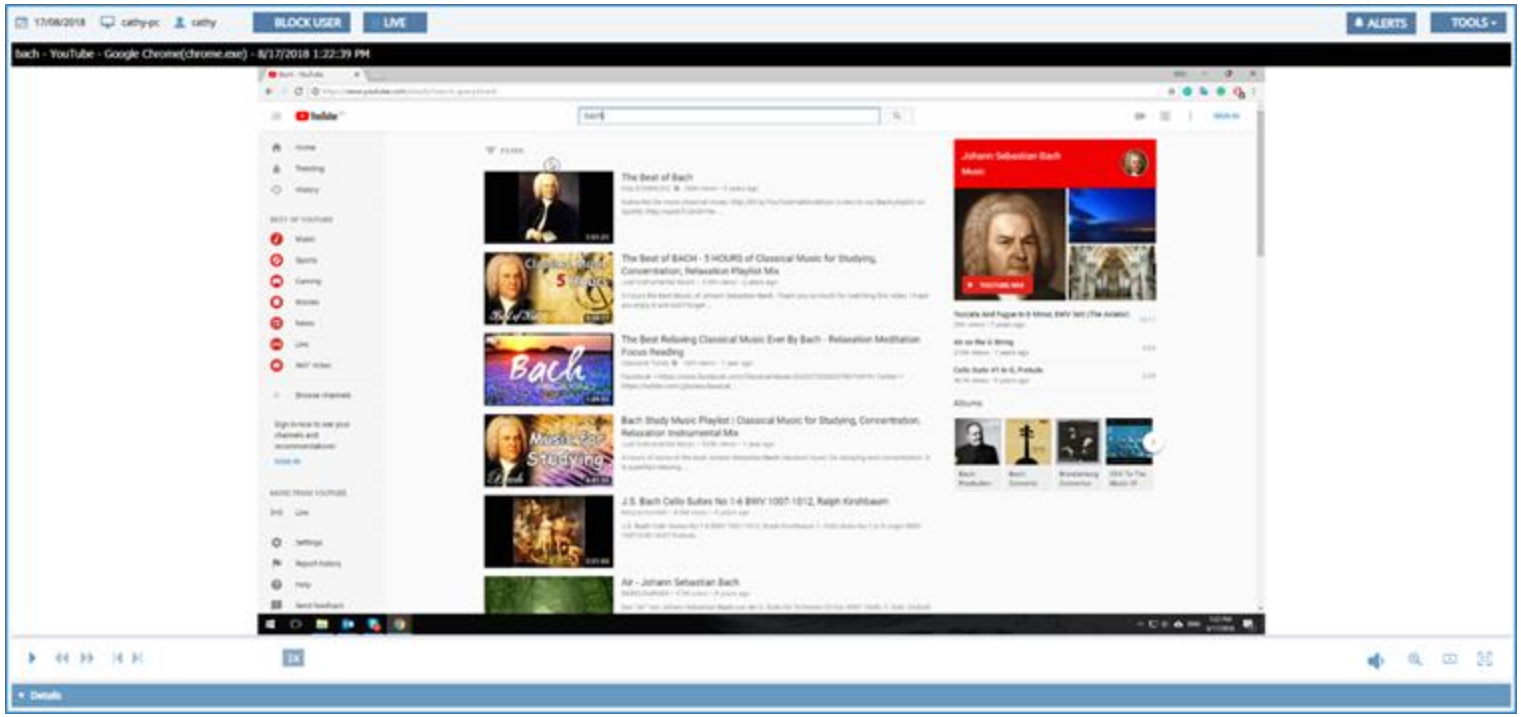
- **W przypadku klientów systemu Windows:** aktywny tytuł okna, nazwa aplikacji, nazwa użytkownika, nazwa klienta, odwiedzony adres URL, dane tekstowe schowka, komentarz użytkownika do dodatkowej wiadomości, numer zgłoszenia, informacje o podłączanych urządzeniach USB.
- **W przypadku klientów systemu MacOS:** aktywny tytuł okna, nazwa aplikacji, nazwa użytkownika, nazwa klienta, odwiedzony adres URL.
- **Dla klientów Linux**: polecenia, parametry poleceń i wyjście poleceń.



Przeglądanie sesji na żywo

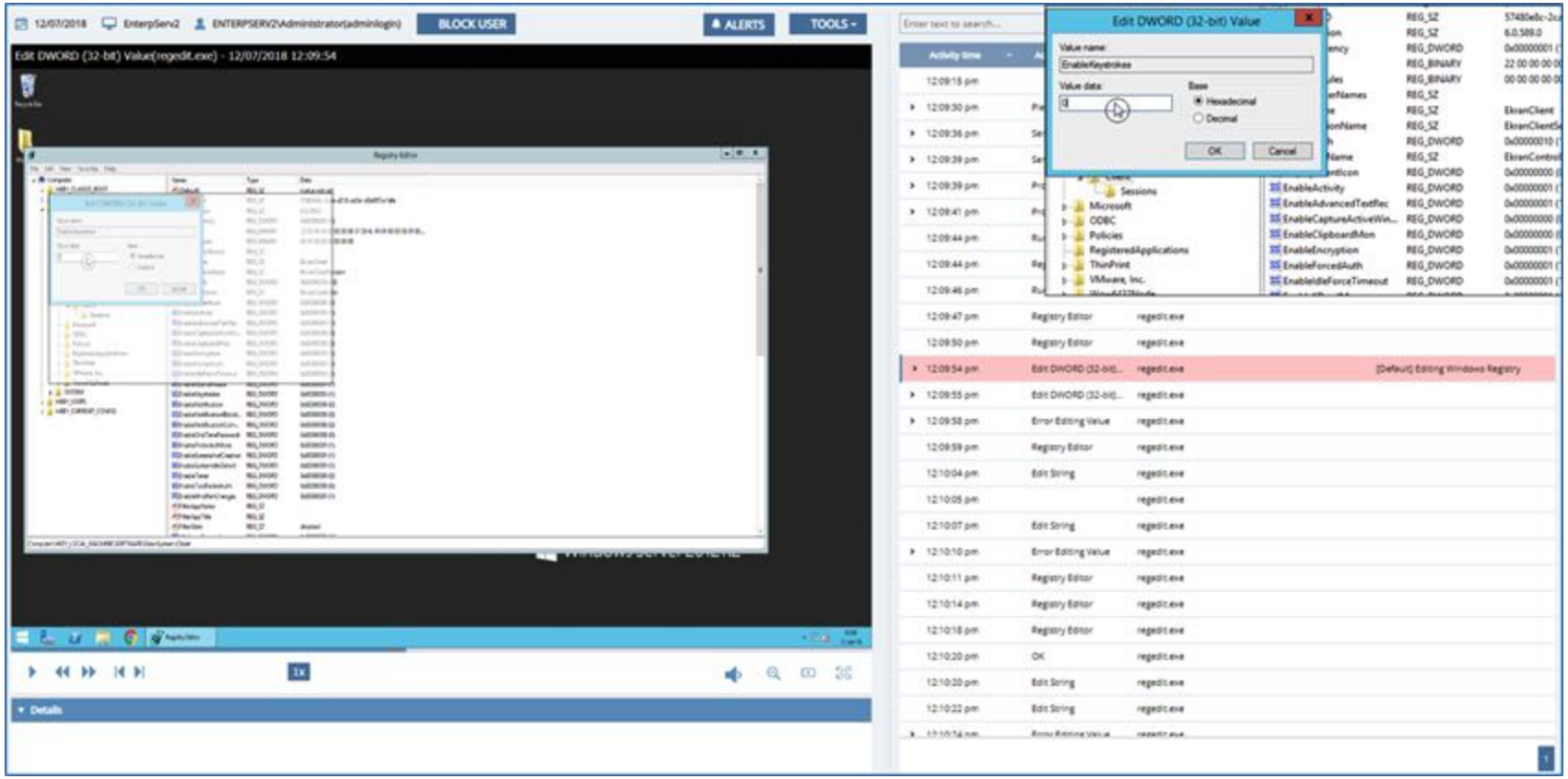
Ekran System umożliwia **monitorowanie** aktywności użytkowników i **odsłuchiwanie dźwięków** odtwarzanych na komputerze z Ekran Client **w czasie rzeczywistym**.

Można połączyć się z sesją **na żywo** i obserwować czynności wykonywane przez użytkownika w danym momencie.



Lupa

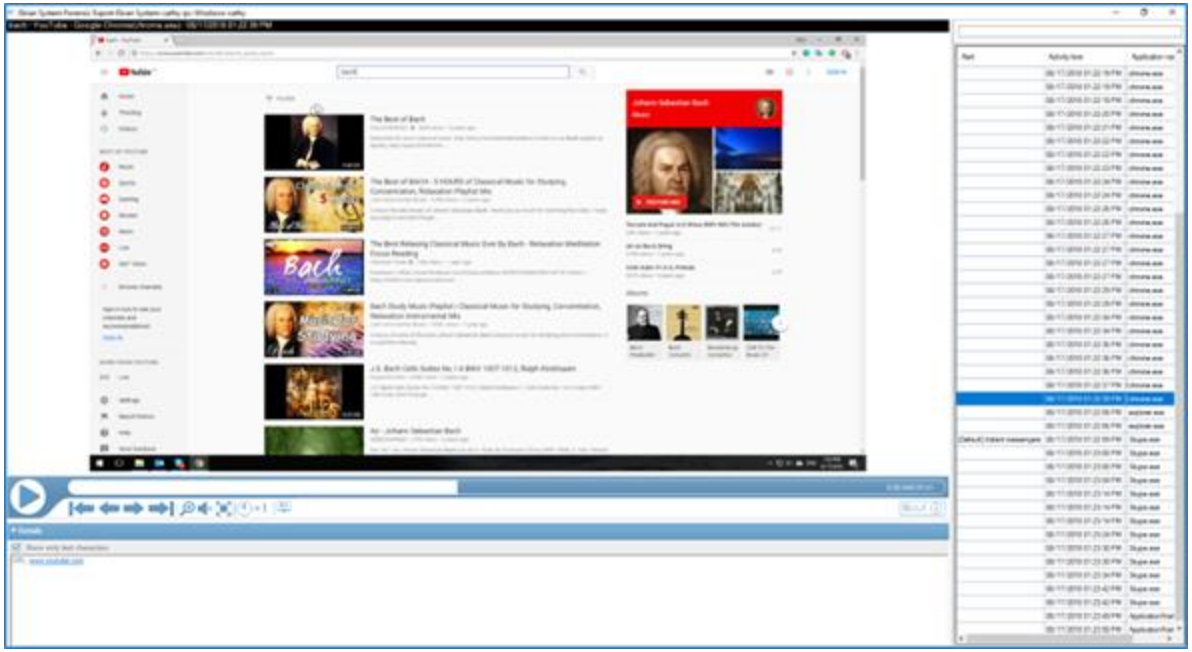
Niektóre części wideo można **powiększyć** w odtwarzaczu sesji za pomocą **lupy**.



Forensic Export

Z Ekran System Forensic Export, możesz:

- **Eksportować monitorowaną sesję** lub jej części do bezpiecznie zaszyfrowanego pliku.
- **Zbadać zarejestrowaną aktywność** użytkownika i dane audio w wbudowanej przeglądarce sesji offline.
- Przedstawić stronom trzecim **niepodważalne dowody** w formacie nieedytowalnym.

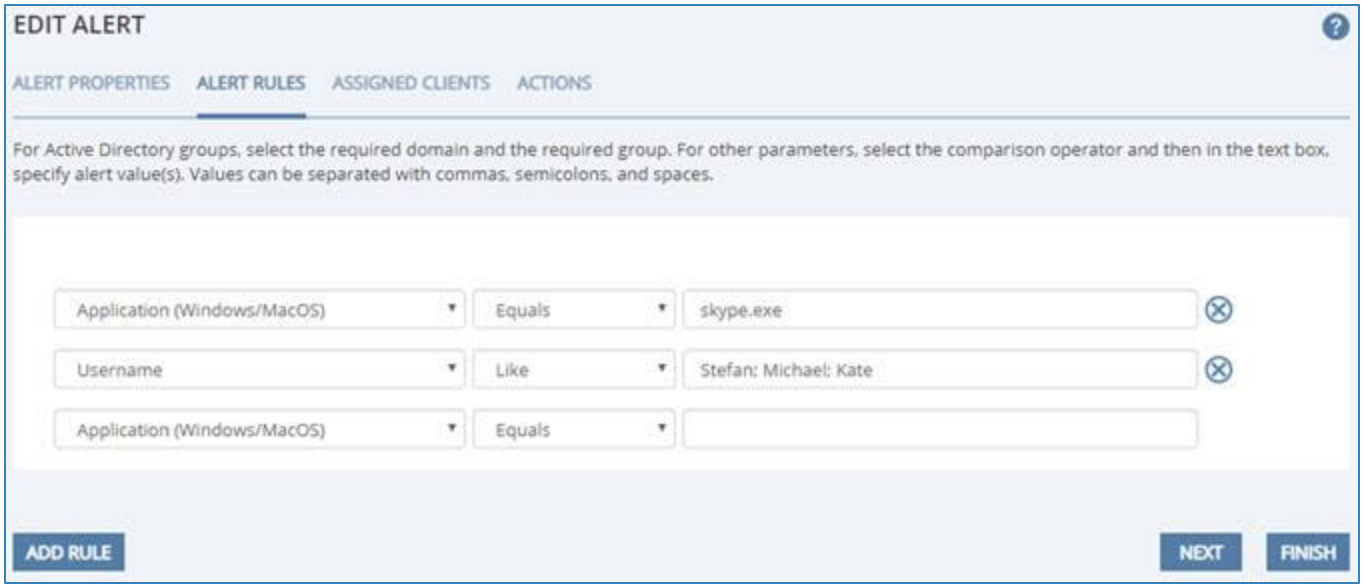


Zdarzenia alarmowe (Alerty)

Ustawienia Alertów

Ekran System umożliwia **szybkie reagowanie na incydenty** za pomocą powiadomień alarmowych:

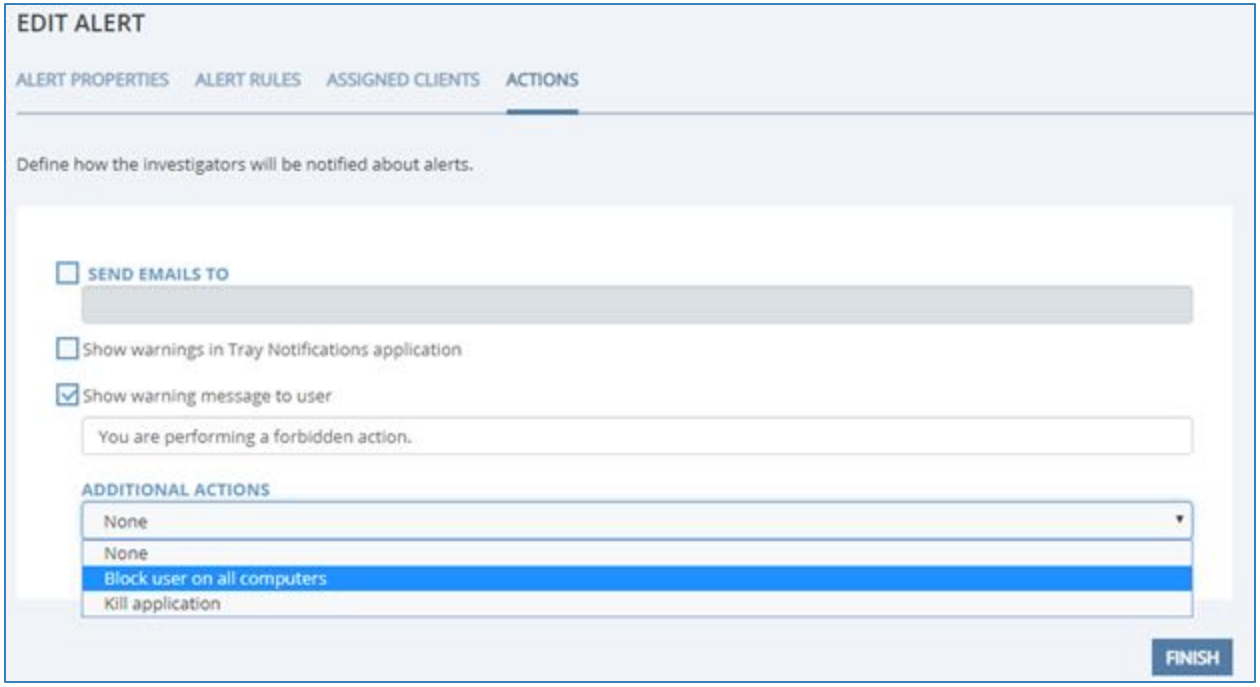
- **Ustawianie powiadomień** o podejrzanej aktywności użytkowników na komputerach z Ekran Client.
- **Określenie osób**, które mają otrzymywać natychmiastowe powiadomienia o zagrożeniu za pośrednictwem poczty elektronicznej lub w aplikacji Tray Notifications.



Akcje po wywołaniu Alertu

Możesz ustawić Alert na:

- Wyświetlenie **komunikatu ostrzegawczego** dla użytkownika, gdy Alert jest wywołany (komunikat może być edytowany).
- **Zablokowanie** użytkownika.
- Natychmiastowe **zatrzymanie aplikacji**.



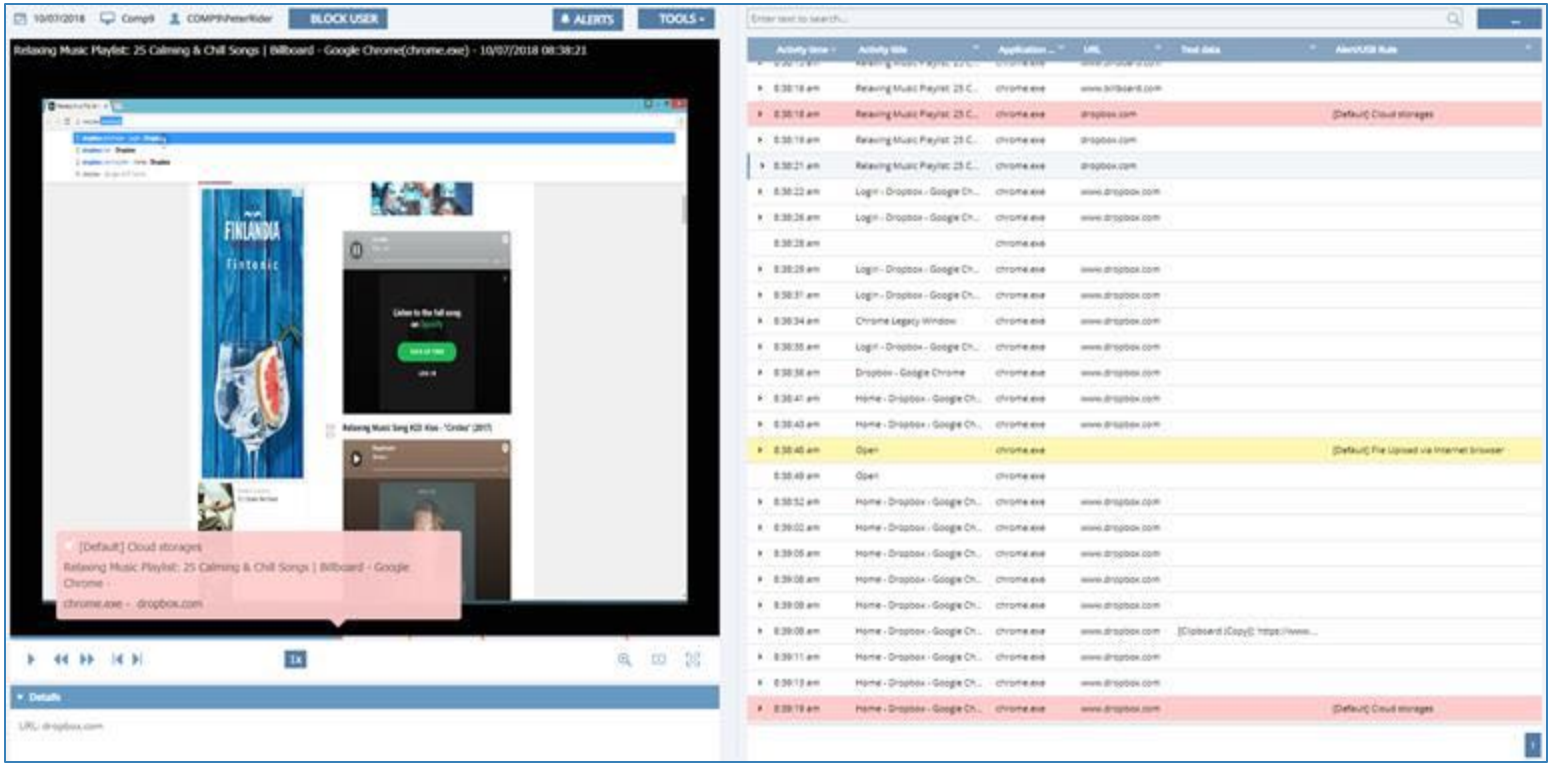
Domyślne Alerty

Ekran System zawiera zestaw domyślnych Alertów przygotowanych przez ekspertów ds. bezpieczeństwa. Alerty zaalarmują Cię o **wycieku danych**, potencjalych **oszustwach**, **nielegalnym** lub **niezwiązanym z pracą działaniu**.

Risk	Name	Description	Assigned To	State	Notification	Email Recipient
	Keystroke monitoring		srv-app	Enabled	None	
	[Linux] User login		All Clients; ubunt...	Enabled	None	
	(Windows) Installatio...	This is alert on detecting installation e...	Comp16	Enabled	None	
	[Default] [Linux] Insta...	This is an alert on detecting installatio...	All Clients; ubunt...	Enabled	Email	admin@example...
	[Default] Online email...	This is an alert for detecting user activ...	All Clients; alice-pc	Enabled	Email	admin@example...
	[Default] Online games	This is an alert for detecting user activ...	All Clients; alice-pc	Enabled	None	
	[Default] Online video	This is an alert for detecting user activ...	All Clients; alice-pc	Enabled	None	
	[Default] Social netwo...	This is an alert for detecting user activ...	All Clients; alice-pc	Enabled	Tray	
	[Default] Job search	This is an alert for detecting user activ...	All Clients; alice-pc	Enabled	None	
	[Default] [Linux] User ...	This is an alert for detecting user crea...	All Clients; ubunt...	Enabled	Email	admin@example...
	[Default] [Linux] Root ...	This is an alert for detecting user gain...	All Clients; ubunt...	Enabled	None	
	[Linux] User adding	This is an alert on adding users on th...	ubuntu2	Enabled	None	
	[Default] Internet Exp...	This is an Alert on changing Internet E...	All Clients; alice-pc	Enabled	None	
	[Default] IIS Binding S...	This is an Alert on changing or adding...	All Clients; alice-pc	Enabled	Email	admin@example...
	[Default] BitTorrent si...	This is an alert on detecting user activ...	All Clients; alice-pc	Enabled	None	
	[Default] Cloud stora...	This is an alert on detecting user activ...	All Clients; alice-pc	Enabled	None	
	Proxy Anonymizers	This is an alert on detecting user activ...	Comp16	Enabled	None	

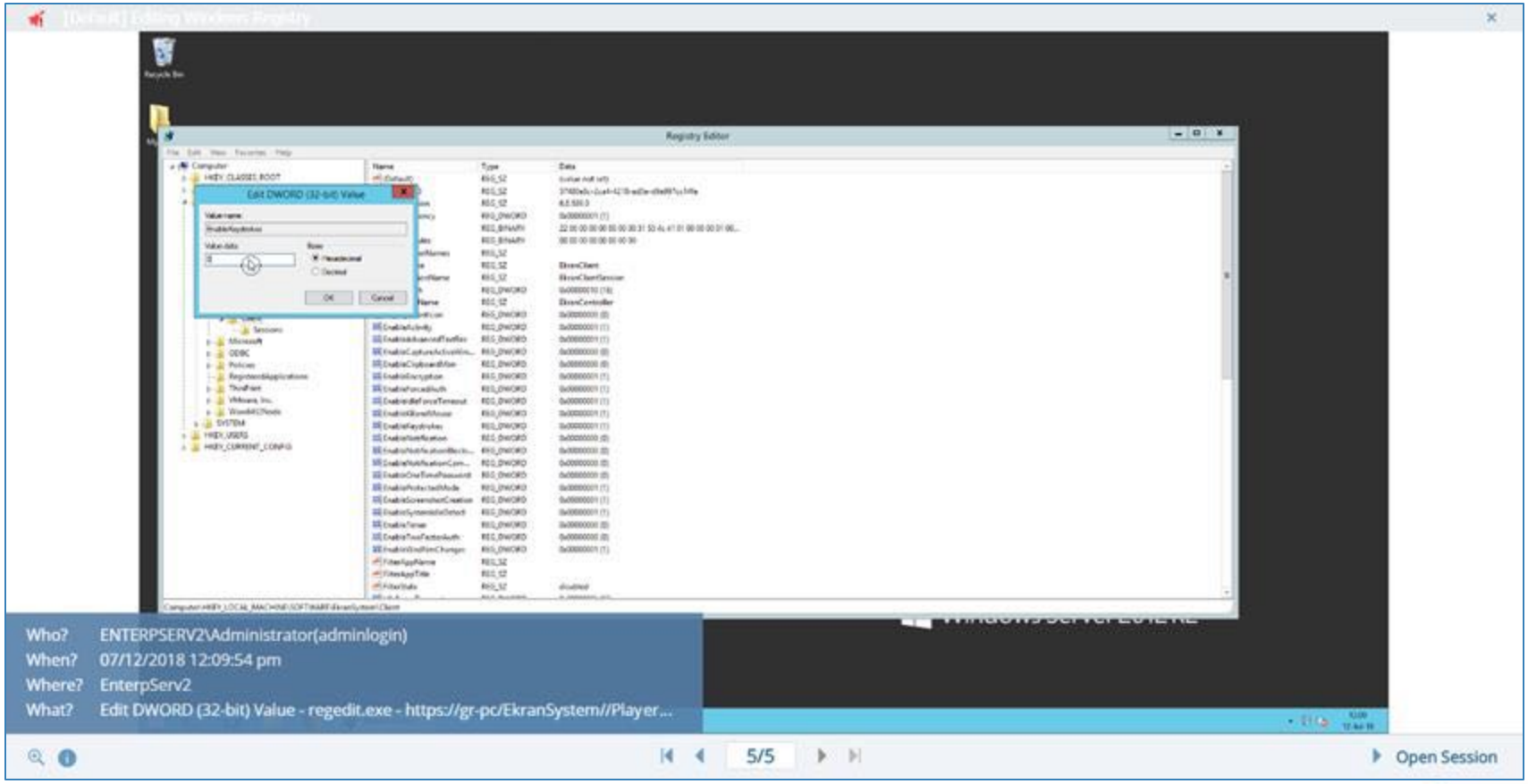
Alerty w odtwarzaczu sesji

Monitorowane dane związane z Alertami są **podświetlane** w odtwarzaczu sesji w różnych **kolorach** w zależności od **poziomu ryzyka**.



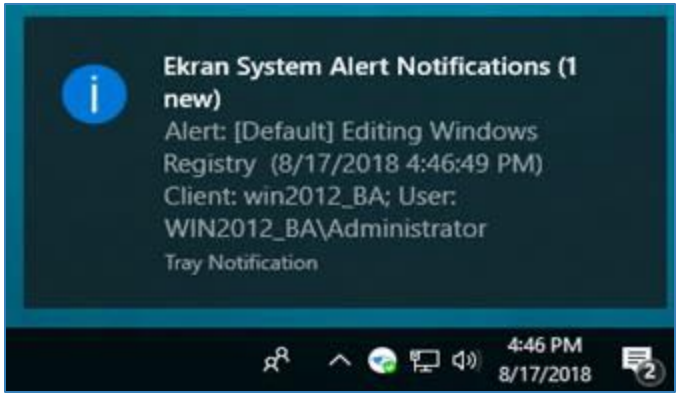
Alert Viewer

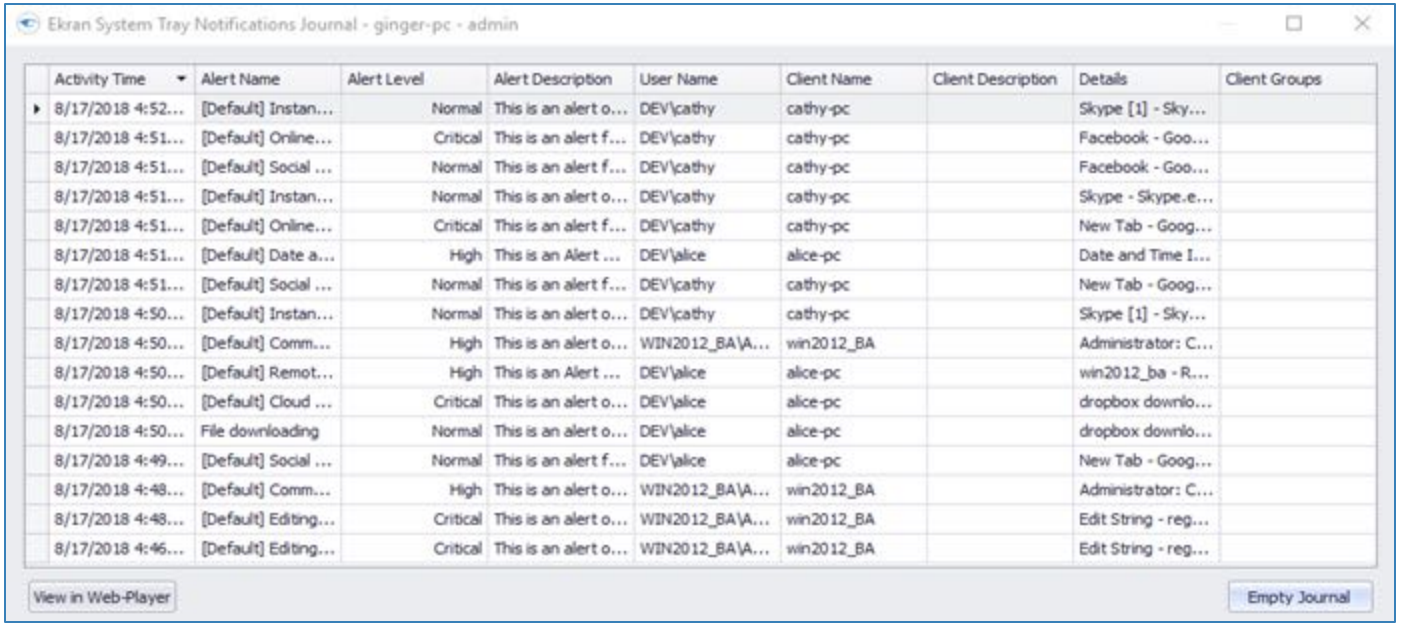
W specjalnej przeglądarce można przeglądać **szczegółowe informacje** o wszystkich Alertach, a także związane z nimi **zrzuty ekranu**.



Otrzymywanie Alertów

Możliwość otrzymywania **powiadomień** o Alertach w **czasie rzeczywistym**, przeglądania ich w Ekran Tray Notifications oraz odtworzenia momentu sesji w którym dany alert został wywołany.





Monitorowanie USB

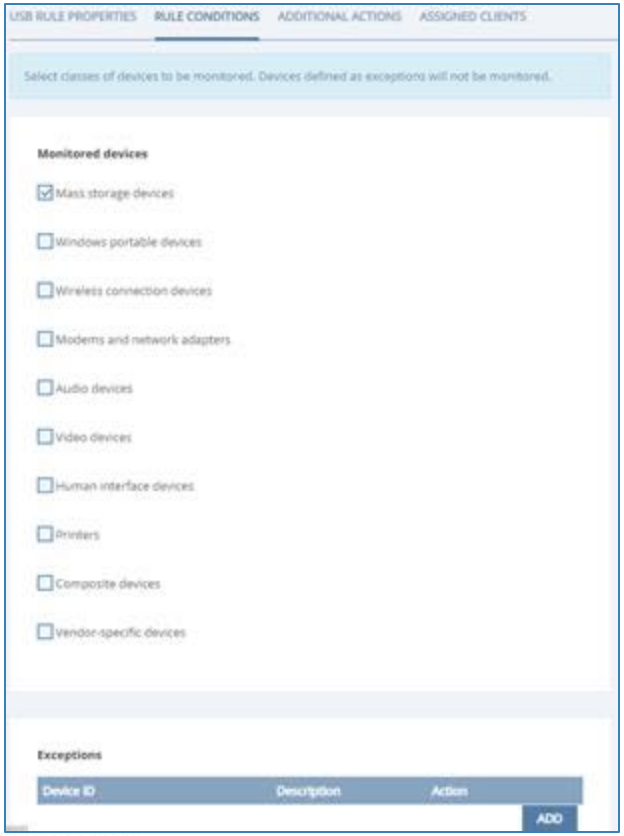
Monitorowanie USB

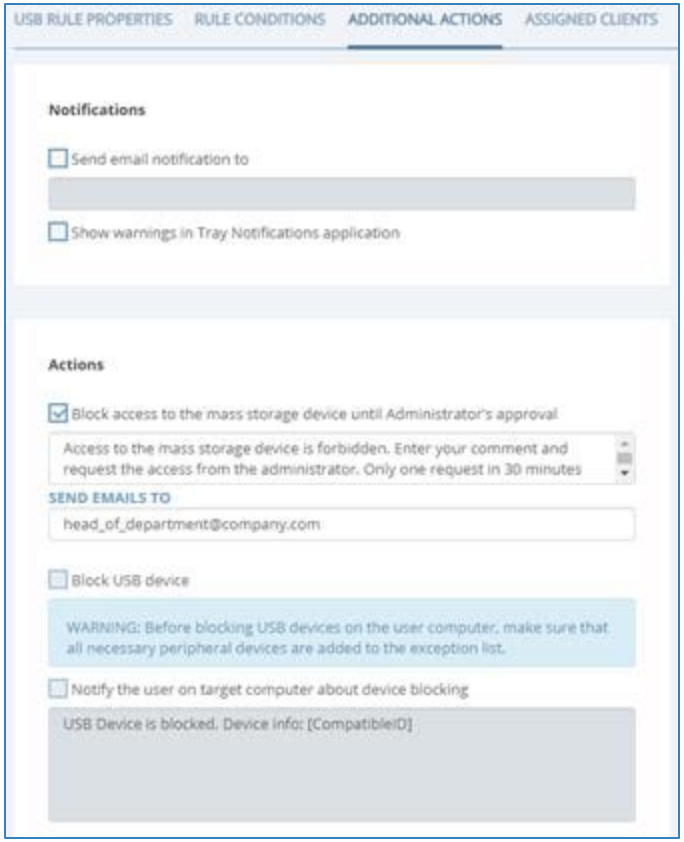
Ekran System oferuje **dwa rodzaje monitorowania** urządzeń USB podłączonych do komputera Windows z Ekran Client:

- **Monitorowanie pamięci USB**, aby wyświetlać informacje o urządzeniach wykrytych przez system Windows jako pamięć masowa i otrzymywać **powiadomienia o zagrożeniu**.
- **Monitorowanie USB na poziomie Kernela**, do dogłębnej **analizy** podłączonych urządzeń i ich **blokowania**.

Ustawienia zasad Kernel-level USB (poziom Kernela)

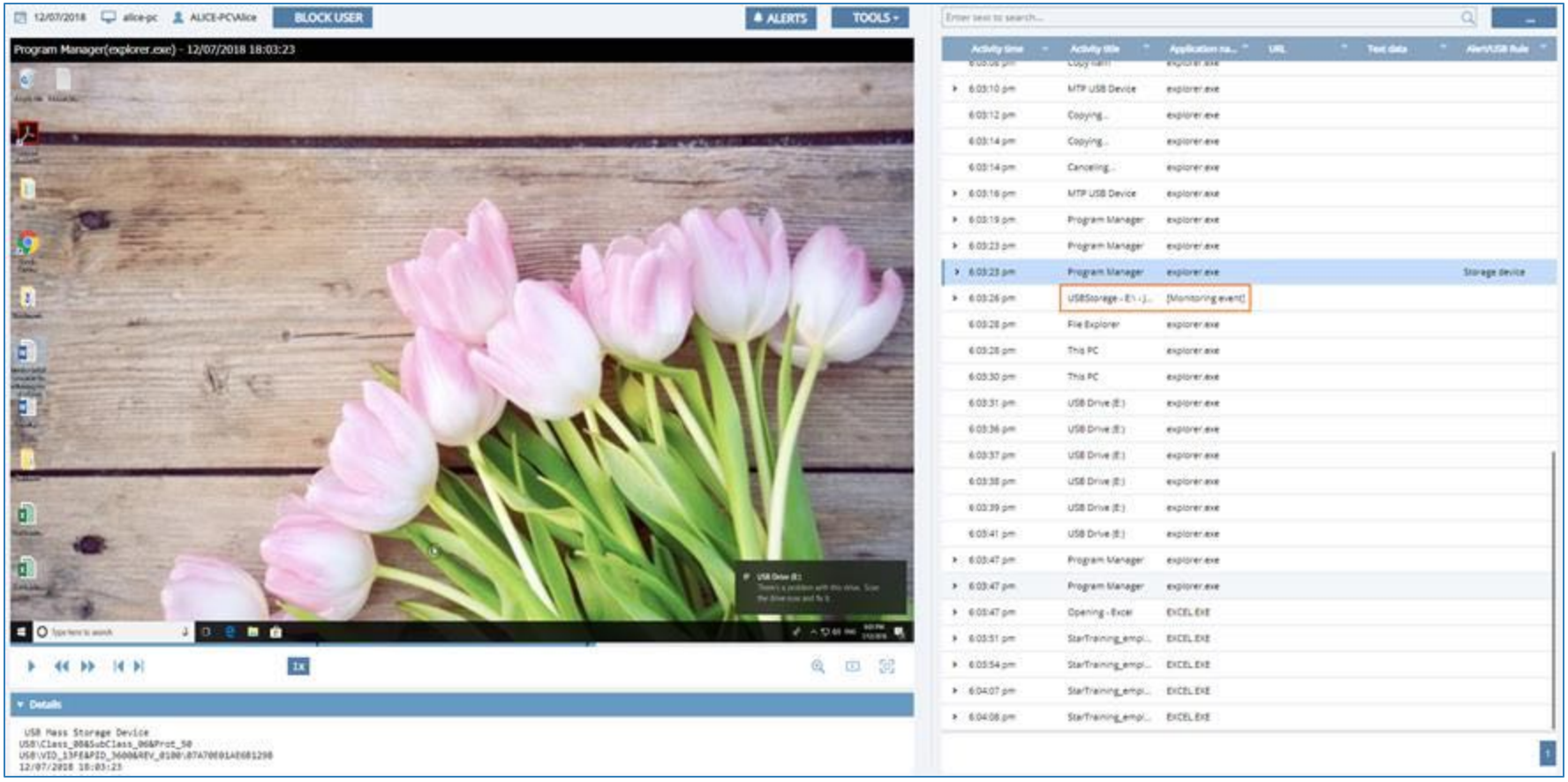
Ekran System może **wykrywać urządzenia USB** podłączone do komputera, **ostrzegać** o podłączeniu urządzenia, **zablokować** jego użytkowanie lub **zabronić** dostępu do nich do czasu uzyskania **zgody administratora** (wszystkie urządzenia danej klasy lub wszystkie z wyjątkiem dozwolonych urządzeń) na komputerze z Ekran Client.





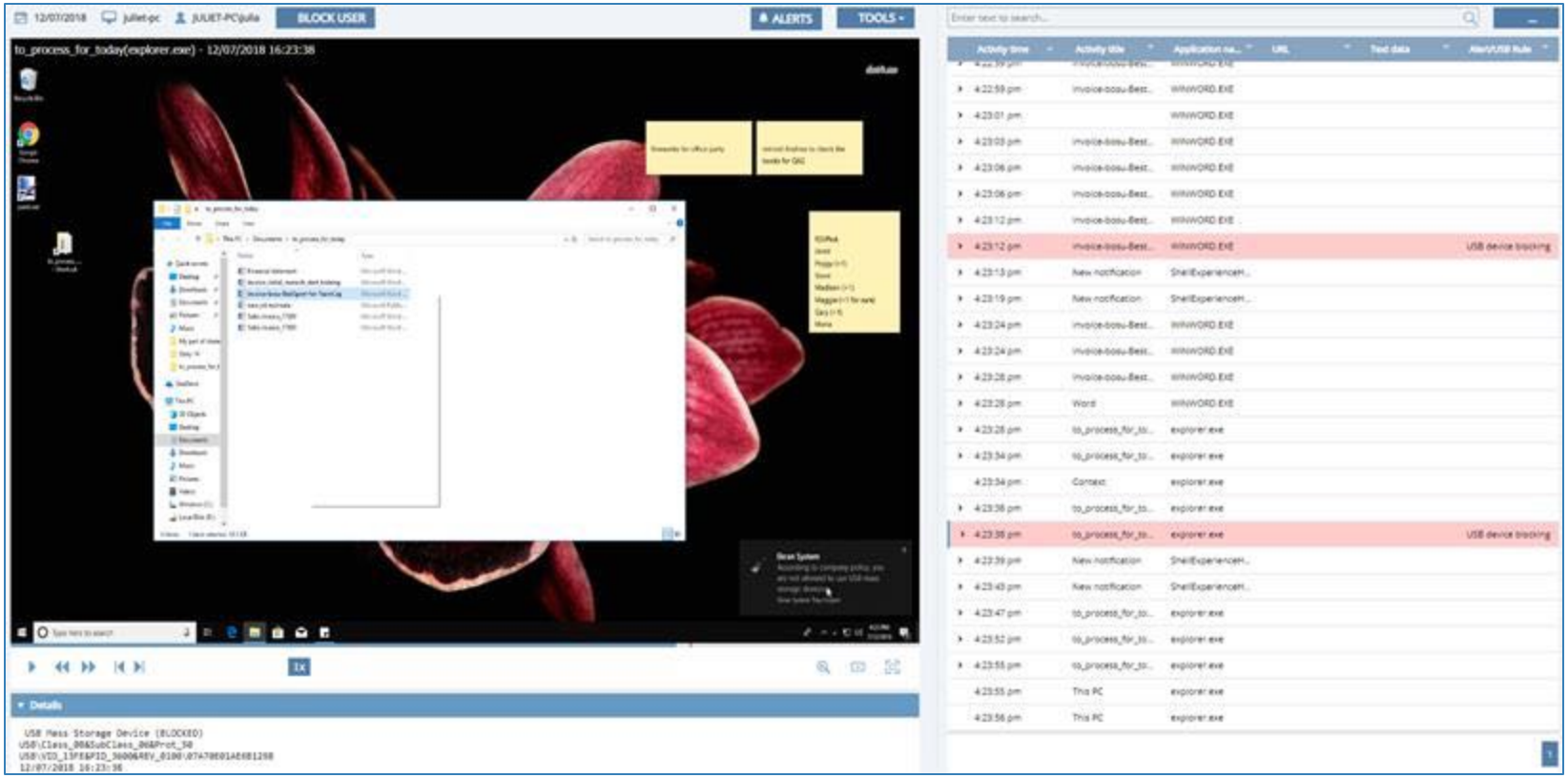
Monitorowanie pamięci USB

Pamięć USB jest wykrywana automatycznie po jej podłączeniu.



Monitorowanie USB na poziomie Kernela

Zrzuty ekranu powiązane z **podłączonymi** lub **blokowanymi** urządzeniami USB są **podświetlone** w odtwarzaczu sesji.

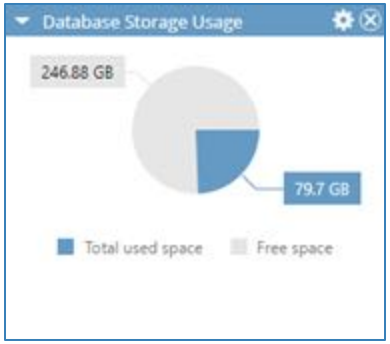


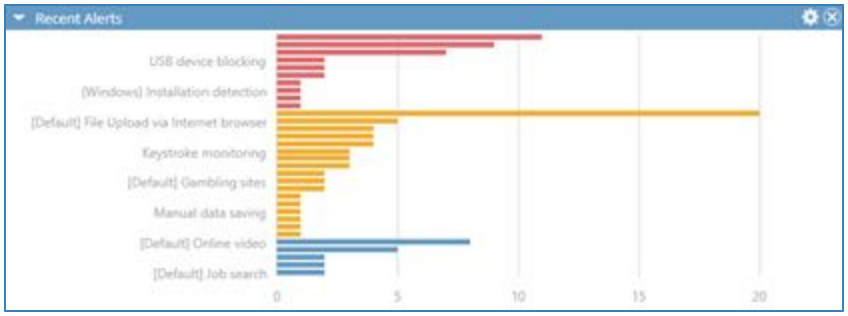
Dashboardy

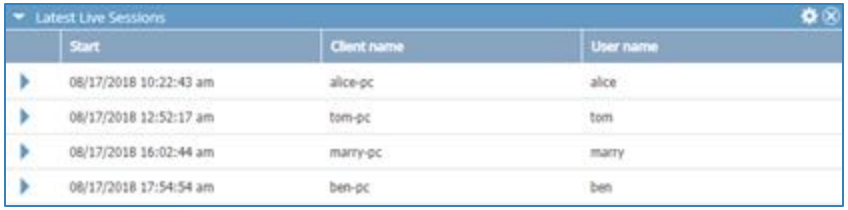
Dashboardy

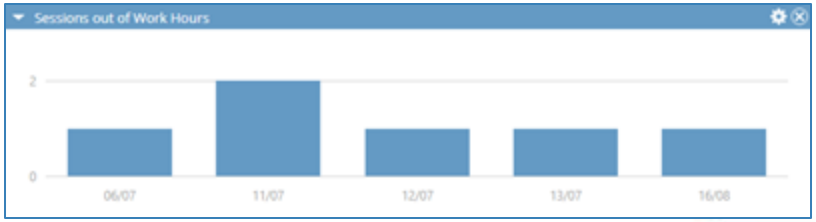
Dashboardy oferują **wygodny podgląd w czasie rzeczywistym najbardziej użytecznych danych** zgrupowanych **w jednym miejscu**.

Istnieje możliwość **dostosowania** dashboardów na stronie głównej Management Tool, dokonując zmian ich **wyglądu** i **ustawień**.









Typy Dashboardów

Istnieją 4 główne typy dashbordów Ekran System:

Dashboardy ze Stanem Systemu

- Licencje
- Komputery z Ekran Client
- Zużycie bazy danych

Dashboardy Monitorowania

- Ostatnie Alerty
- Ostatnie Sesje Live

Dashboardy Sygnalizacji Zagrożeń

- Sesje poza godzinami pracy
- Rzadko używane komputery
- Rzadko używane loginy

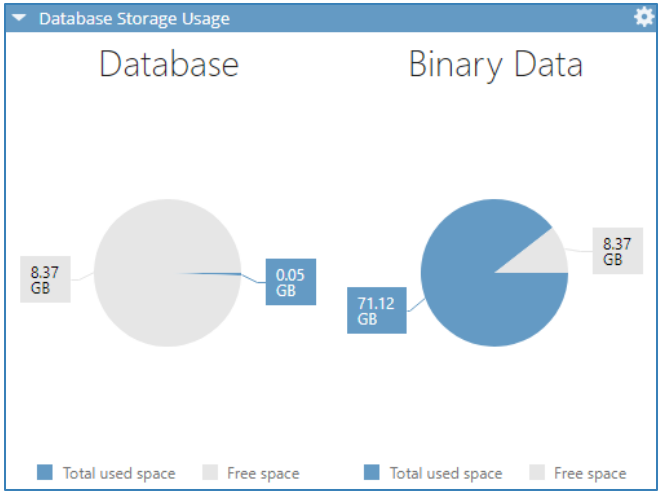
Monitorowanie Zasobów Serwera

- Zużycie procesora
- Zużycie pamięci
- Stan bazy danych

Dashboardy ze Stanem Systemu

Komputery z Ekran Client

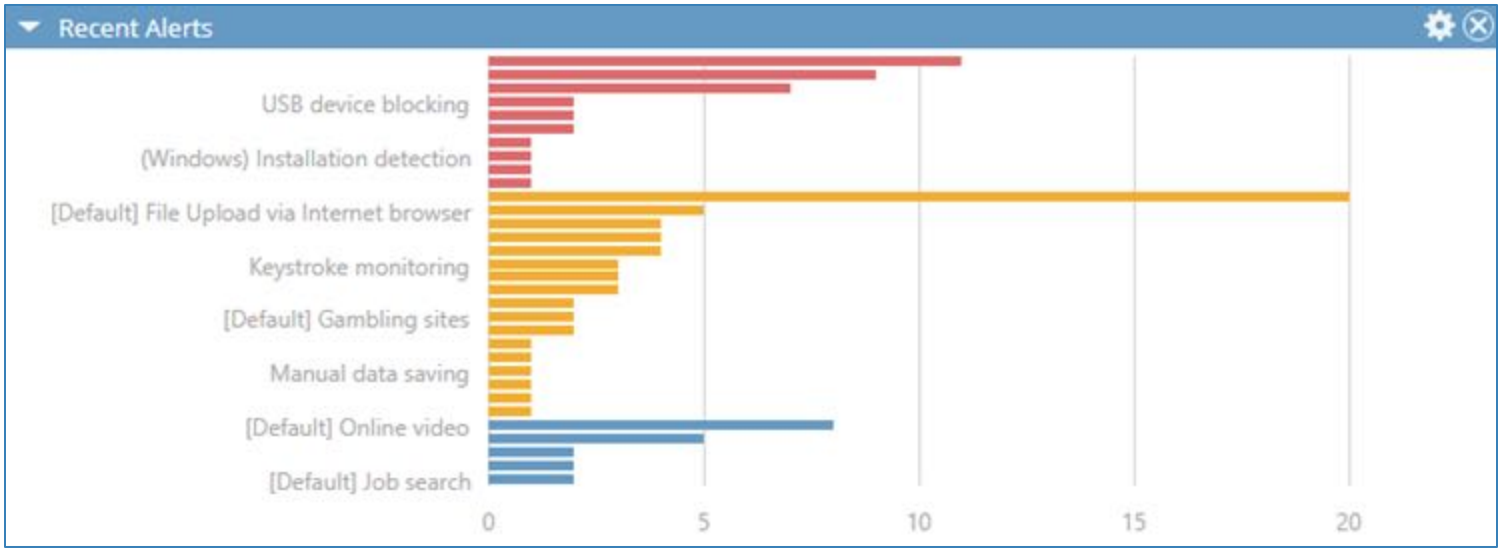
Zużycie bazy danych



Licencje

Dashboardy Monitorowania

Ostatnie Alerty



Ostatnie Sesje

Latest Live Sessions

Start	Client name	User name
08/17/2018 10:22:43 am	alice-pc	alice
08/17/2018 12:52:17 am	tom-pc	tom
08/17/2018 16:02:44 am	marry-pc	marry
08/17/2018 17:54:54 am	ben-pc	ben

Dashboardy Sygnalizacji Zagrożenia

Rzadko używane komputery

Rarely Used Computers

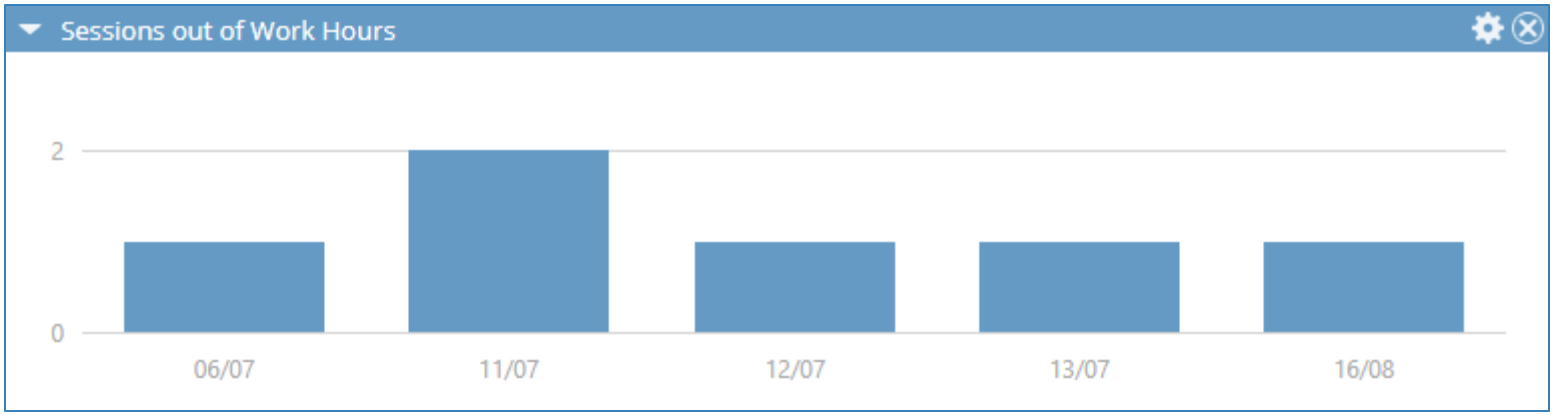
Client Name	Sessions
alice-potter	2
kate-moss	2
tom-pitterson	1

Rzadko używane loginy

Rarely Used Logins

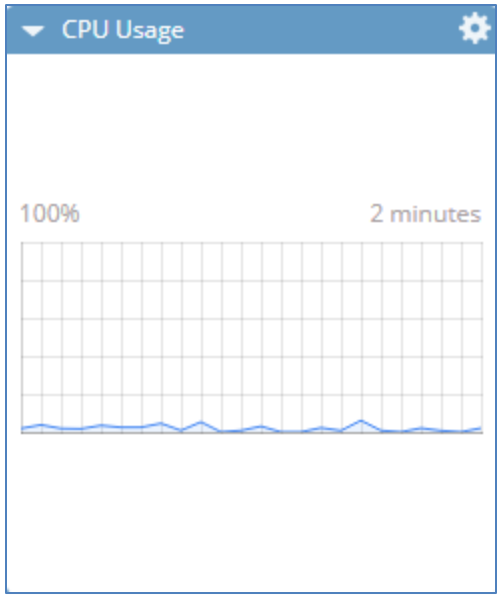
User Name	Sessions
TV\admin	1
User	1
Guest	1

Sesje poza godzinami pracy

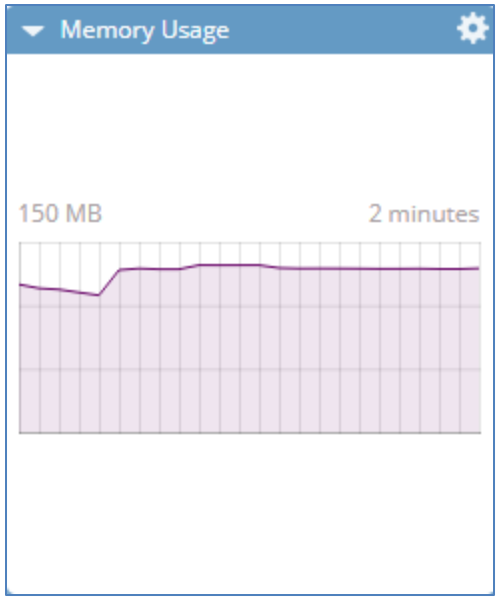


Monitorowanie Zasobów Serwera

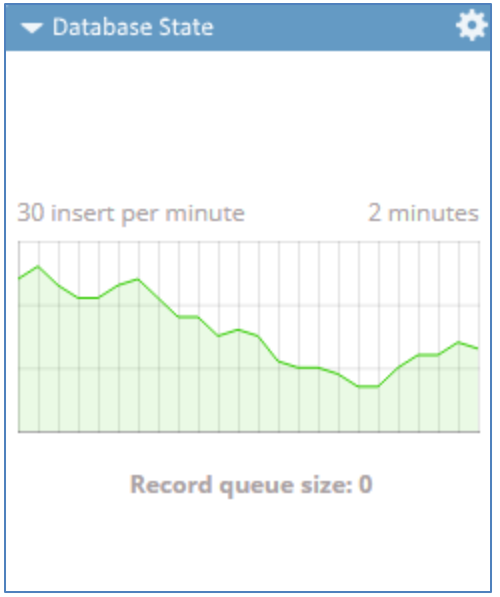
Zużycie procesora



Zużycie pamięci



Stan bazy danych



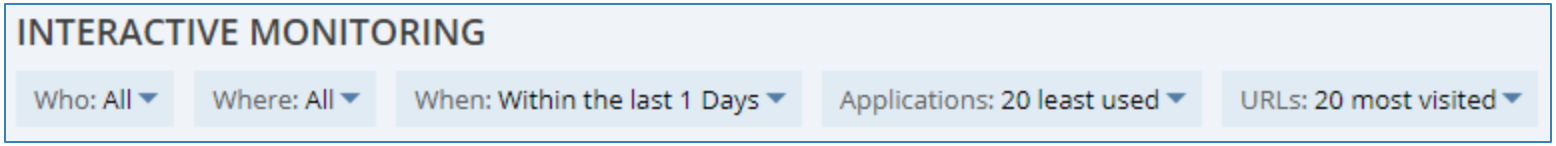
Interactive Monitoring

Interactive Monitoring

Dane można **filtrować** według trzech parametrów:

- **Kto**: filtruje przez konkretnego użytkownika zalogowanego do komputera z Ekran Client.
- **Gdzie**: filtrowanie przez konkretny komputer z Ekran Client.
- **Kiedy**: filtrować według przedziału czasowego.

Dodatkowo można **ustawić kolejność wyświetlanych danych**, korzystając z **filtrów** aplikacji i adresów URL.



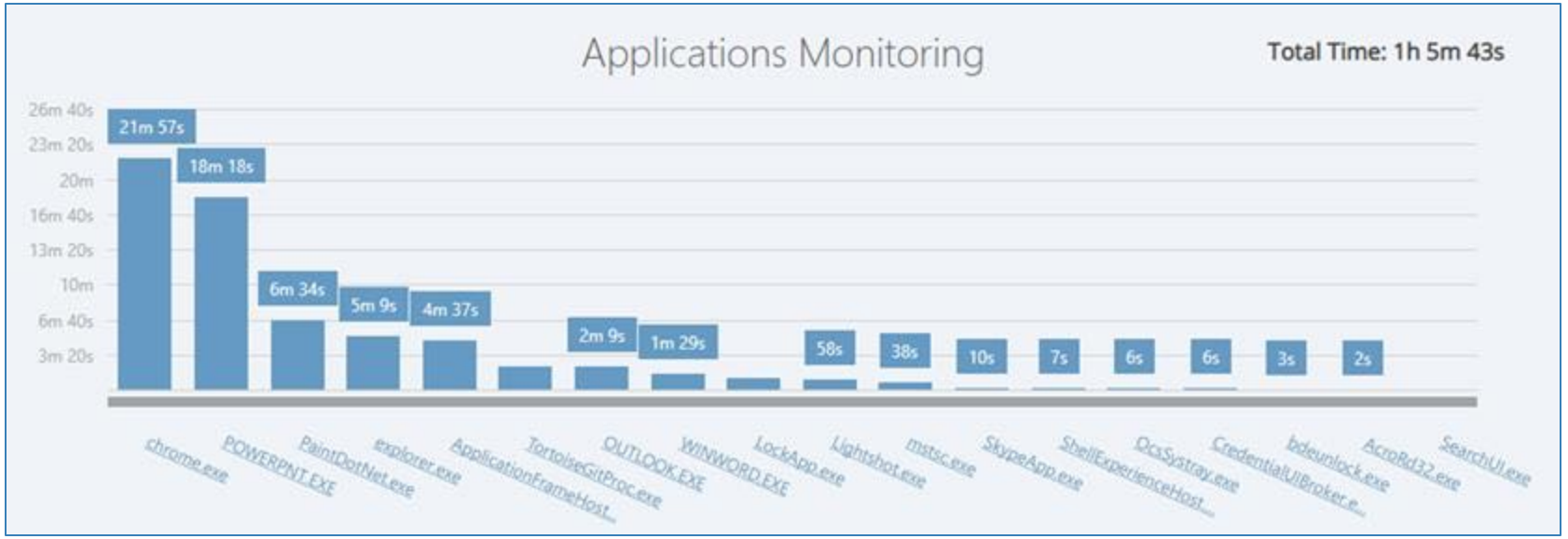
Dane wyświetlane są w postaci dwóch wykresów kolumnowych (wykres **monitorowania aplikacji** i wykres **monitorowania URL**).

Aby zobaczyć listę wpisów aplikacji/stron internetowych, kliknij na kolumnę z nazwą aplikacji/stron internetowych.

Wykres monitorowania Aplikacji

Wykres ten zawiera informacje na temat **częstotliwości korzystania z aplikacji**.

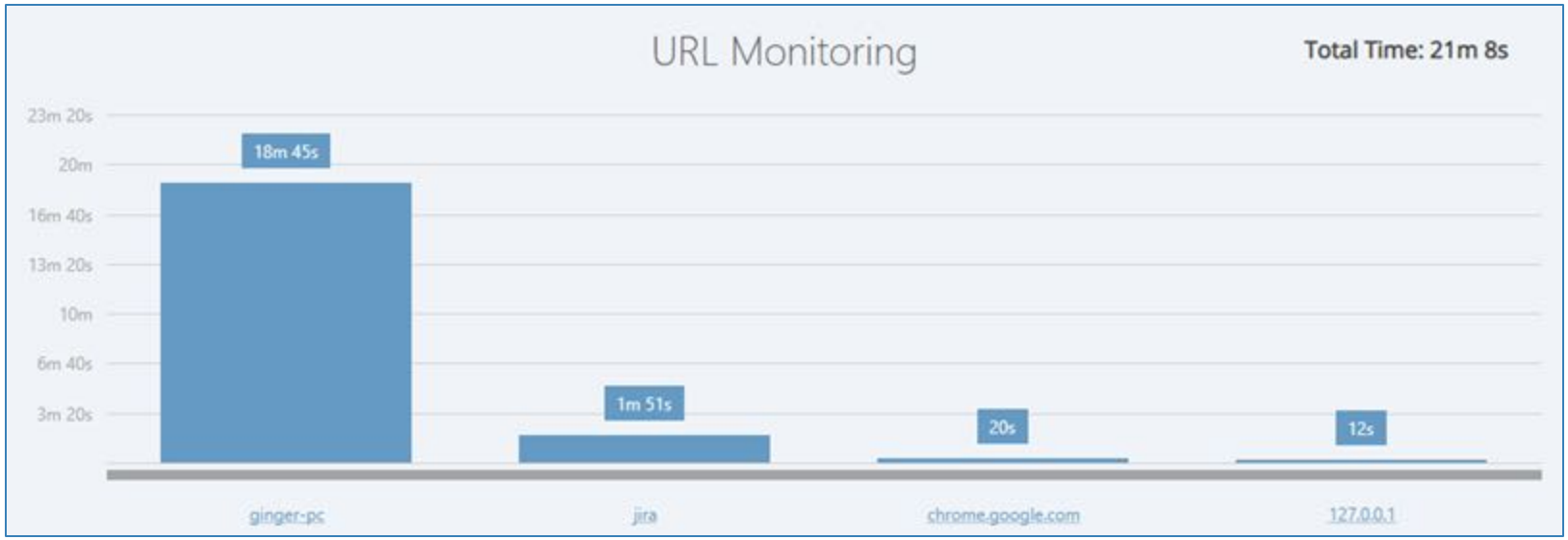
Za pomocą tego wykresu można analizować informacje o **najczęściej** i **najmniej** używanych aplikacjach oraz wykrywać wszelkie zagrożenia i podejrzane działania na monitorowanych komputerach.



Wykres monitorowania adresów URL

Wykres ten zawiera informacje na temat **częstotliwości odwiedzin** stron internetowych.

Za pomocą tego wykresu można również analizować informacje dotyczące **najczęściej** i **najmniej** odwiedzanych stron internetowych oraz wykrywać potencjalnie szkodliwą aktywność na badanych komputerach.



Raporty

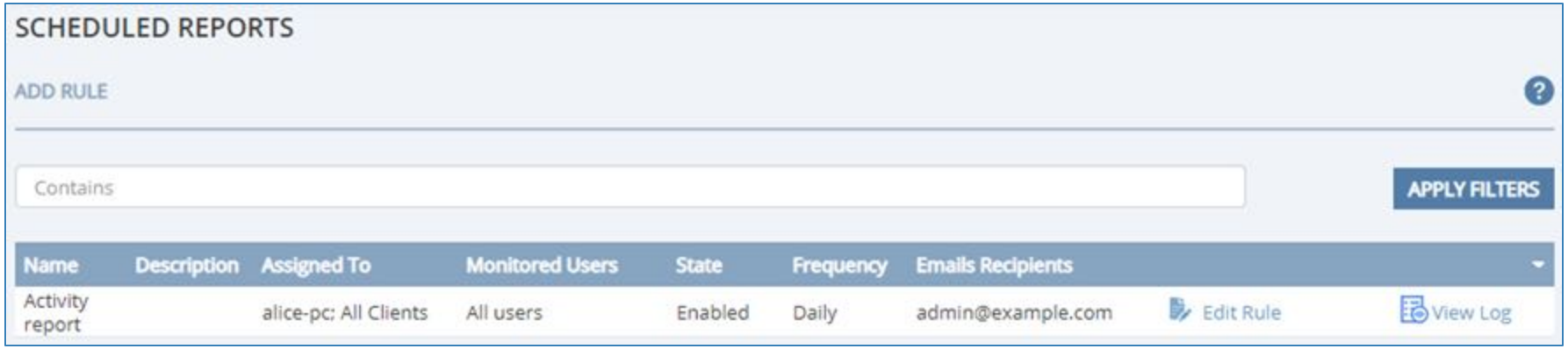
Raporty i Statystyki

Raporty Ekran System zapewniają pełny przegląd czasu spędzonego w aplikacjach i na stronach internetowych odwiedzanych na komputerze użytkownika.

Istnieje możliwość generowania wysoce konfigurowalnego raportu ad-hoc lub ustawienia harmonogramu wysyłania raportów do poczty elektronicznej w trybie dziennym, tygodniowym lub miesięcznym.

Zgłoszona aktywność może obejmować alerty, uruchomione aplikacje, odwiedzane strony internetowe, podłączone/zablokowane urządzenia USB oraz wykonane polecenia systemu Linux.

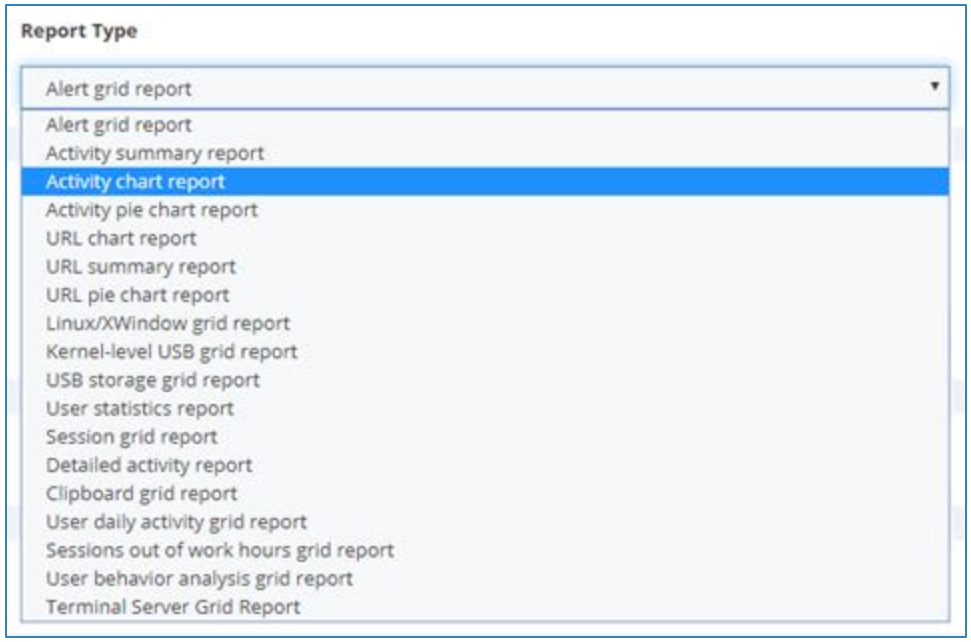
Raporty Okresowe

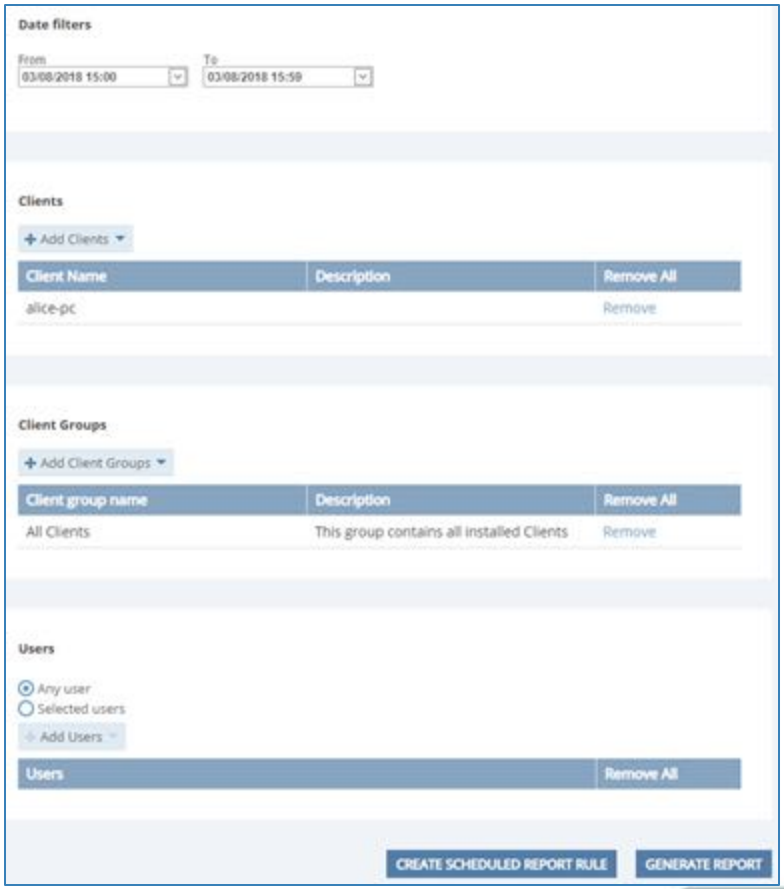


Raporty i Statystyki

Raporty mogą być generowane ręcznie w dowolnym momencie i w dowolnym czasie.

Ręczne Generowanie Raportów





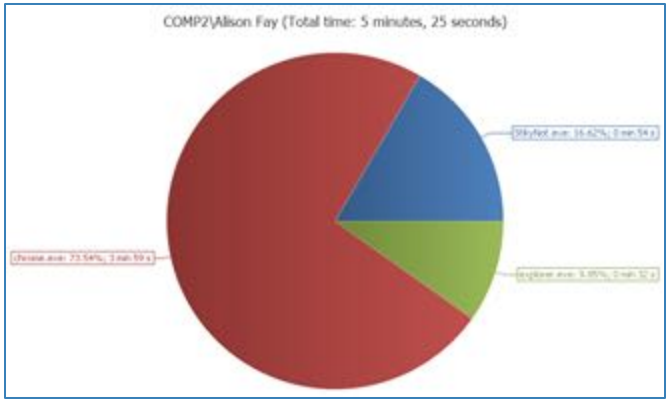
Typy Raportów

Raport podsumowujący aktywność

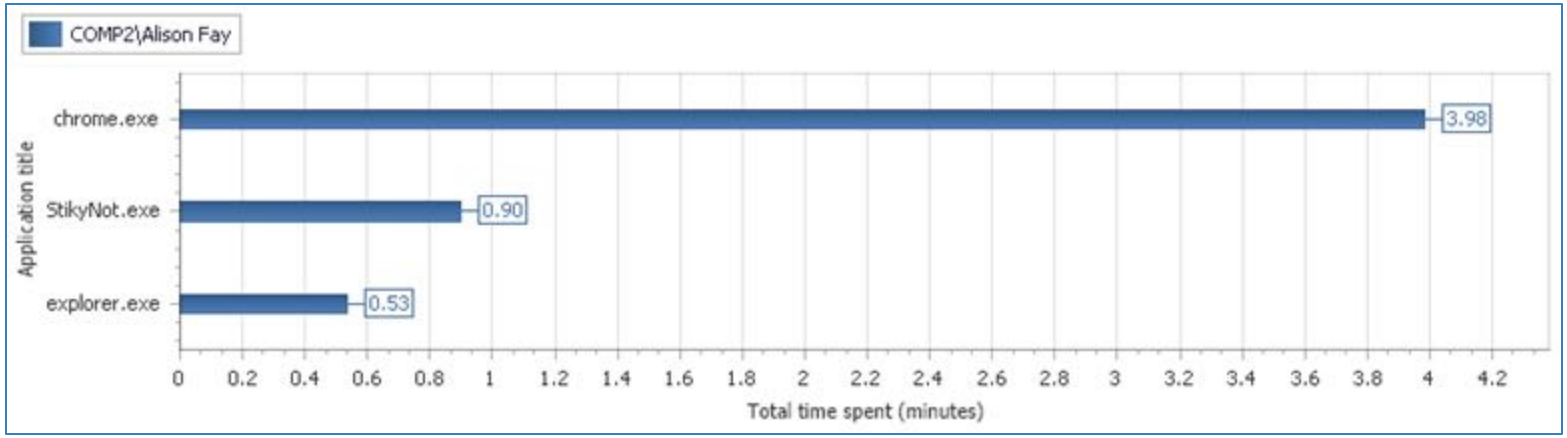
Client name	Comp2
Client description	Social media
User name	COMP2\Alison Fay
Total time	5 minutes, 25 seconds
Active time	5 minutes, 25 seconds

Application name	%	Time spent
chrome.exe	73.54	3 minutes, 59 seconds
StikyNot.exe	16.62	54 seconds
explorer.exe	9.85	32 seconds

Raport z wykresem kołowym podsumowujący aktywność



Raport z wykresem podsumowujący aktywność



Typy Raportów

Raport statystyk użytkownika

User name	Total time spent	Session count	Computers	Remote IPs
COMP18\JasonZena	37m 7s	1	Comp18	None
COMP16\BonnieRoss	9m 6s	1	Comp16	None
COMP1\John Dean	7m 38s	1	Comp1	10.100.5.216
COMP2\Alison Fay	5m 43s	1	Comp2	10.100.4.68
COMP7\AlexisParker	5m 22s	1	Comp7	10.100.4.68
COMP9\PeterRider	5m 12s	1	Comp9	10.100.4.68
COMP8\RobertOakley	5m 2s	1	Comp8	None
COMP15\HelenPeterson	5m 0s	1	Comp15	10.100.4.68
COMP10\BenjaminTeel	4m 50s	1	Comp10	None
donna	4m 44s	1	ubuntu1	

Raport schowka

Client name	Comp15
Client description	Exporting HR Data
User name	COMP15\HelenPeterson

Activity time	Activity title	Application name	Clipboard Operation	Clipboard Text
07/10/2018 08:52:43 AM	My Drive - Google Drive - Google Chrome	chrome.exe	Copy	https://drive.google.com/file/d/19TprsjyVorHH8GcdL0xnHmO8HKh7wlvw/view?usp=sharing
07/10/2018 08:53:01 AM	My Drive - Google Drive - Google Chrome	chrome.exe	Paste	https://drive.google.com/file/d/19TprsjyVorHH8GcdL0xnHmO8HKh7wlvw/view?usp=sharing

Typy Raportów

Raport z sesji

Client name	MyServer
Client description	PASM - Protected Server
Total time	1m 2s

User name	Total time spent	Active time	Session start time	Last activity time	Remote IP	Session URL
EKRAN\ES_User_6A9625E1	1m 2s	1m 2s	07/12/2018 01:29:18 PM	07/12/2018 01:30:20 PM	10.100.4.20	Open Session

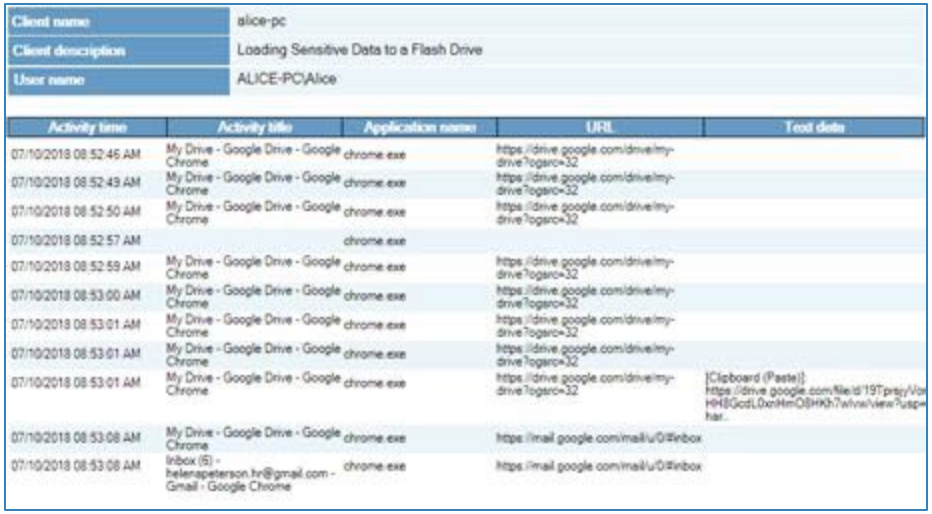
Raport z sesji poza godzinami pracy

Client name	Comp10
Client description	Using BitTorrents (yts.am, qbittorrent.exe)
Total out of work hours	4m 50s

User name	Total time spent	Active out of work hours	Session start time	Last activity time	Remote IP	Session URL
COMP10\BenjaminTeel	4m 50s	4m 50s	07/12/2018 08:44:03 AM	07/12/2018 08:48:53 AM	None	Open Session

Typy Raportów

Szczegółowy raport aktywności



Client name	alice-pc
Client description	Loading Sensitive Data to a Flash Drive
User name	ALICE-PC\Alice

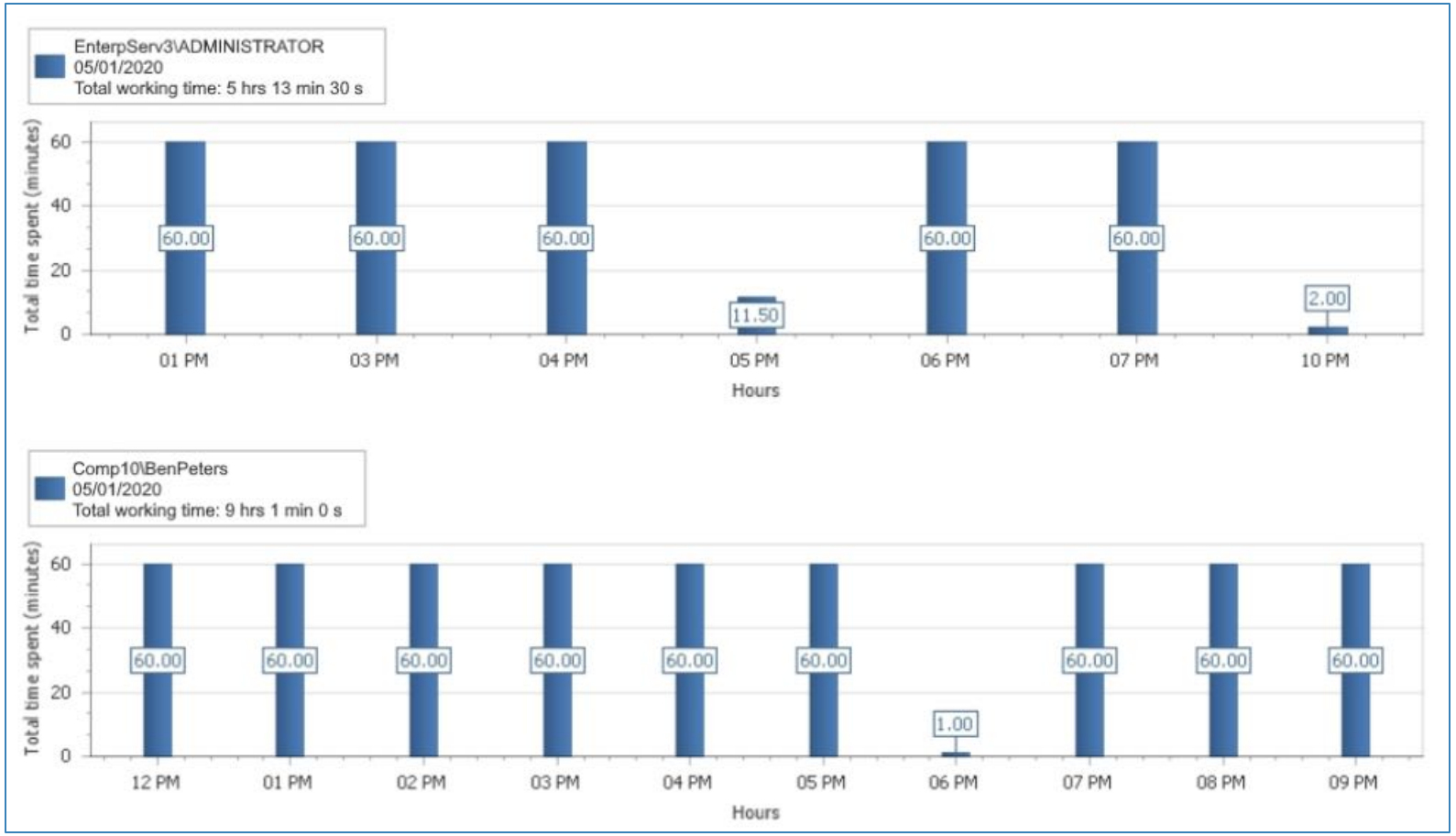
Activity time	Activity title	Application name	URL	Text data
07/10/2018 08:52:46 AM	My Drive - Google Drive - Google Chrome	chrome.exe	https://drive.google.com/drive/my-drive?ogsrc=32	
07/10/2018 08:52:49 AM	My Drive - Google Drive - Google Chrome	chrome.exe	https://drive.google.com/drive/my-drive?ogsrc=32	
07/10/2018 08:52:50 AM	My Drive - Google Drive - Google Chrome	chrome.exe	https://drive.google.com/drive/my-drive?ogsrc=32	
07/10/2018 08:52:57 AM		chrome.exe		
07/10/2018 08:52:59 AM	My Drive - Google Drive - Google Chrome	chrome.exe	https://drive.google.com/drive/my-drive?ogsrc=32	
07/10/2018 08:53:00 AM	My Drive - Google Drive - Google Chrome	chrome.exe	https://drive.google.com/drive/my-drive?ogsrc=32	
07/10/2018 08:53:01 AM	My Drive - Google Drive - Google Chrome	chrome.exe	https://drive.google.com/drive/my-drive?ogsrc=32	
07/10/2018 08:53:01 AM	My Drive - Google Drive - Google Chrome	chrome.exe	https://drive.google.com/drive/my-drive?ogsrc=32	
07/10/2018 08:53:01 AM	My Drive - Google Drive - Google Chrome	chrome.exe	https://drive.google.com/drive/my-drive?ogsrc=32	[Clipboard (Paste)] https://drive.google.com/file/d/19TprsyVo... HH8GcdL0xrHmOBHKh7a/vw/view?usp=... har
07/10/2018 08:53:08 AM	My Drive - Google Drive - Google Chrome	chrome.exe	https://mail.google.com/mail/u/0/#inbox	
07/10/2018 08:53:08 AM	Inbox (6) - helenapeterson.hr@gmail.com - Gmail - Google Chrome	chrome.exe	https://mail.google.com/mail/u/0/#inbox	

Raport dziennej aktywności użytkownika

Client name	Comp16
Client description	Installing an Anonymizer (TOR browser)
Total time	8m 39s

User name	Active time	First Activity Time	Last Activity Time	Remote IP	Session URL
COMP16\BonnieRoss	8m 39s	07/10/2018 10:20:03 AM	07/10/2018 10:28:43 AM	None	Open Session

Raport produktywności użytkownika



Raport Alertów

Client name	Comp11
Client description	Generating Licenses
User name	COMP11\SusieWade

Activity time	Alert name	Alert risk	Details
07/10/2018 11:10:01 AM	License generating	High	LicenseGenerator.exe - License generator -

Client name	Comp12
Client description	Providing Access to Server via TeamViewer
User name	COMP12\AmyHobs

Activity time	Alert name	Alert risk	Details
07/09/2018 12:58:08 PM	[Default] Screen sharing applications	Critical	TeamViewer_.exe - TeamViewer 13 Setup -

Typy Raportów

Raport dotyczący zachowania użytkownika

Risk Level	Critical
Risk Score, %	100 - 76
Session number	3

Who	Where	When	Details	Session Score	Session URL
Admin	Server	04/25/2019 01:00:00 AM - 04/25/2019 05:18:30 AM	WorkingHours: abnormal session start abnormal session end	93%	Open Session
FillMorris	Comp5	04/24/2019 07:00:00 PM - 04/25/2019 12:24:30 AM	WorkingHours: abnormal session start abnormal session end	90%	Open Session
AnnaRikler	Comp3	04/22/2019 05:00:00 AM - 04/22/2019 09:24:00 AM	WorkingHours: abnormal session start	90%	Open Session

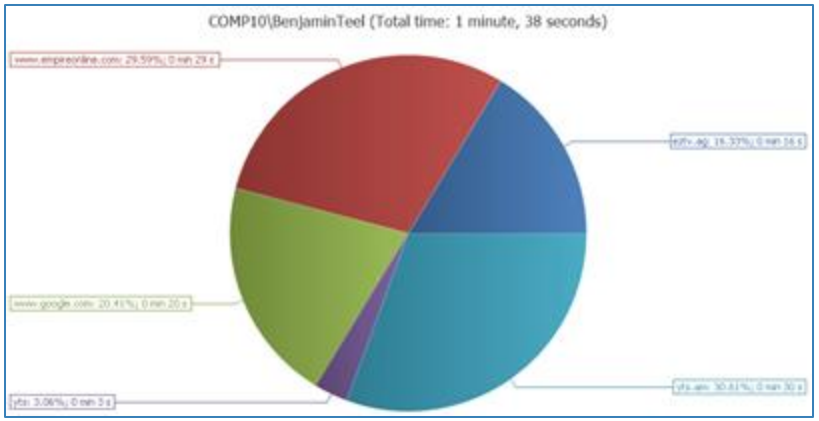
Typy Raportów

Raport podsumowujący korzystanie z adresów URL

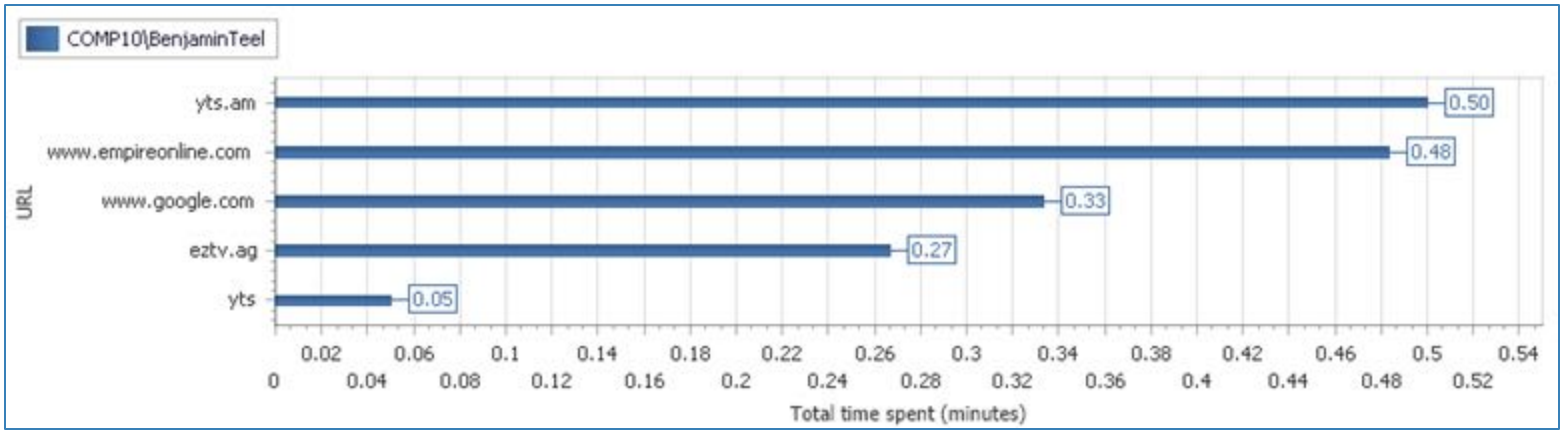
Client name	Comp15
Client description	Exporting HR Data
User name	COMP15\HelenPeterson
Total time	4 minutes, 30 seconds

URL	%	Time spent
https://drive.google.com/drive/my-drive?ogsrc=32	16.67	45 seconds
www.shakespearesglobe.com/whats-on-2018/Hamlet#QAHamlet	12.22	33 seconds
https://secure.zenefits.com/accounts/login/	11.11	30 seconds
https://secure.zenefits.com/dashboard/#/employeebulk/download	11.11	30 seconds
https://basket.shakespearesglobe.com/events/hamlet?startDate=2018-04-25&endDate=2018-08-26&k=globe theatre	9.26	25 seconds
https://secure.zenefits.com/dashboard/	8.52	23 seconds

Kołowy raport korzystania z adresów URL



Raport korzystania z adresów URL z wykresem



Typy Raportów

Raport pamięci USB

Client name	alice-pc
Client description	Loading Sensitive Data to a Flash Drive
User name	ALICE-PC\Alice

Time	Details
07/12/2018 06:02:55 PM	USBStorage - (Standard MTP Device) - MTP USB Device
07/12/2018 06:03:26 PM	USBStorage - E:\ - JULIETTE

Raport pamięci USB Kernel-level

Client name	juliet-pc
Client description	USB device blocking
User name	JULIET-PC\Julia()

Time	Rule Name	Action	Risk Level	Device Class	Device Details
07/12/2018 04:23:12 PM	USB device blocking	Blocked	Critical	USB Mass Storage Device	USB\Class_08&SubClass_06&Prot_50\USB\VID_13FE&PID_3600&REV_0100\07A70E01AE6B1298
07/12/2018 04:23:38 PM	USB device blocking	Blocked	Critical	USB Mass Storage Device	USB\Class_08&SubClass_06&Prot_50\USB\VID_13FE&PID_3600&REV_0100\07A70E01AE6B1298

Raport Serwera Terminalowego

Date	05/24/2019

Client name	Number of users	User name	Number of connections	Total time
Enterprise	2	ryan.daniels	1	4h 17m 9s
		tom.fisher	1	1h 2m 38s
EnterpServ1	1	kate.williams	2	6h 34m 10s
Server	1	admin	1	7h 45m 3s

Date	05/25/2019

Client name	Number of users	User name	Number of connections	Total time
Enterprise	3	admin	3	2h 29m 59s
		phoebe.halliwell	1	37m 3s
		tom.fisher	1	5h 29m 41s

Typy Raportów

W raporcie Linux możesz zobaczyć wszystkie polecenia exec* i sudo wykonane na komputerach z Ekran Client z systemem Linux.

Raport Linux

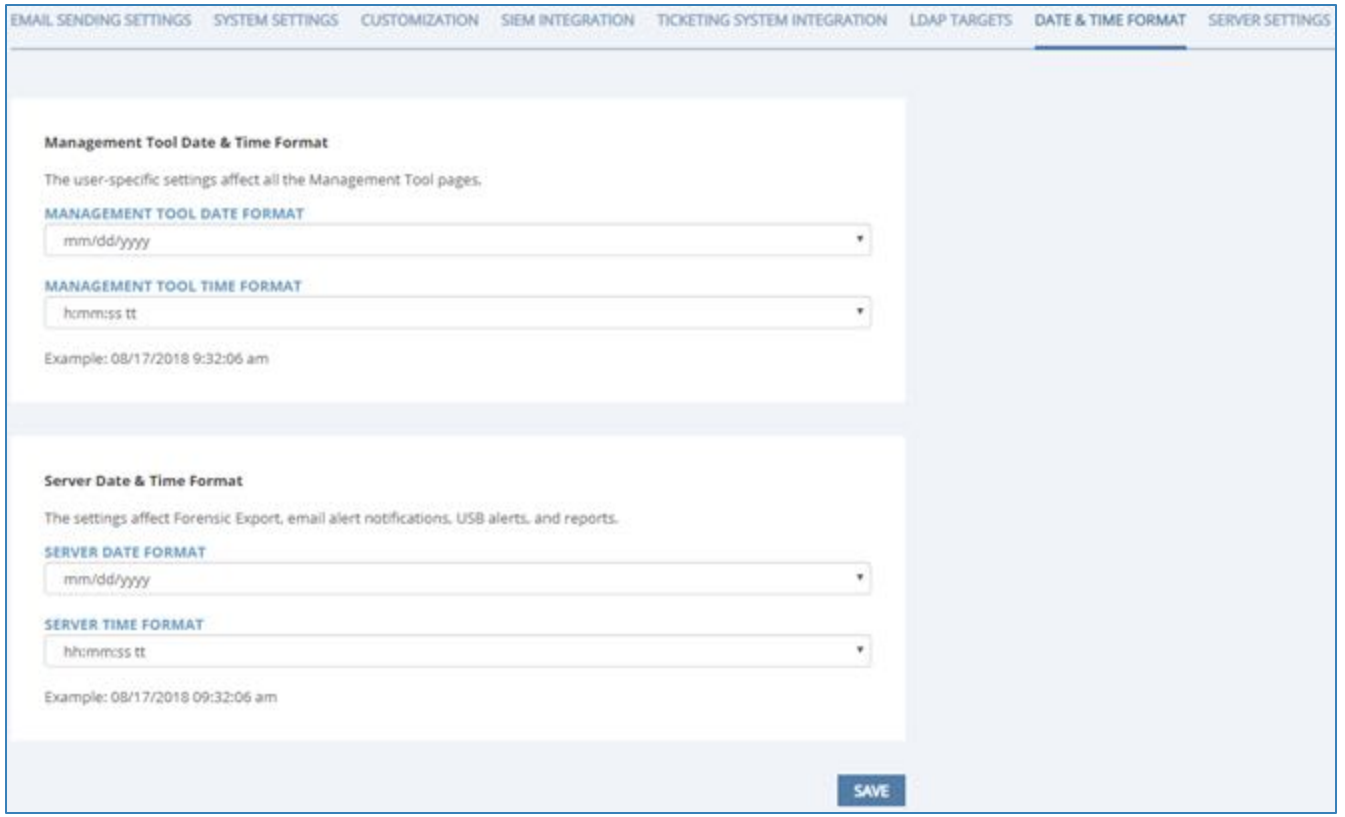
Client name	ubuntu3
Client description	Installation detection
User name	joe

Activity time	Command	Function	Parameters
07/17/2018 01:18:23 PM	grep	execve	-q sshd
07/17/2018 01:18:23 PM	/bin/bash	execve	
07/17/2018 01:18:37 PM	fdisk	execve	-l
07/17/2018 01:19:01 PM	sudo	execve	udisksctl unmount -b/dev/sda
07/17/2018 01:19:12 PM	fdisk	execve	-l
07/17/2018 01:19:20 PM	sudo	execve	fdisk -l
07/17/2018 01:19:38 PM	sudo	execve	apt-get install zip

Ustawienia Aplikacji

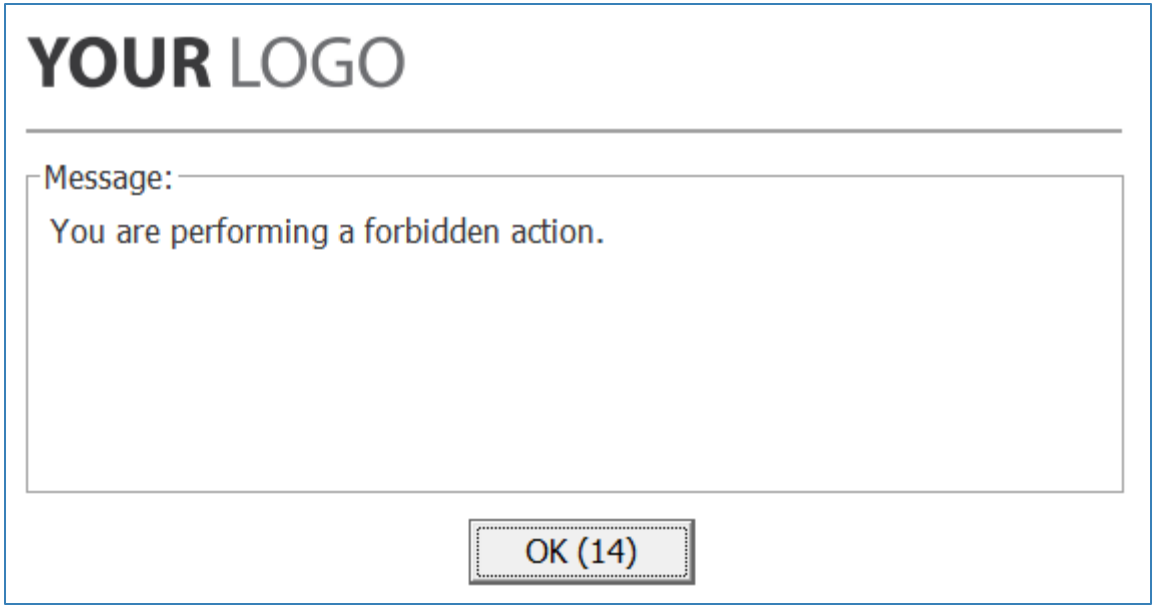
Format Daty i Czasu

Konfiguracja **formatu daty i czasu** pozwala na zdefiniowanie formatu daty i czasu dla Management Tool i dla Serwera.



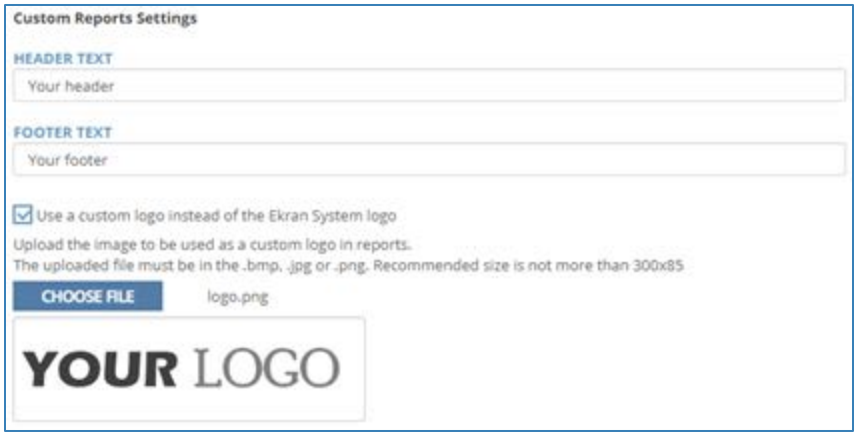
Konfiguracja Logo

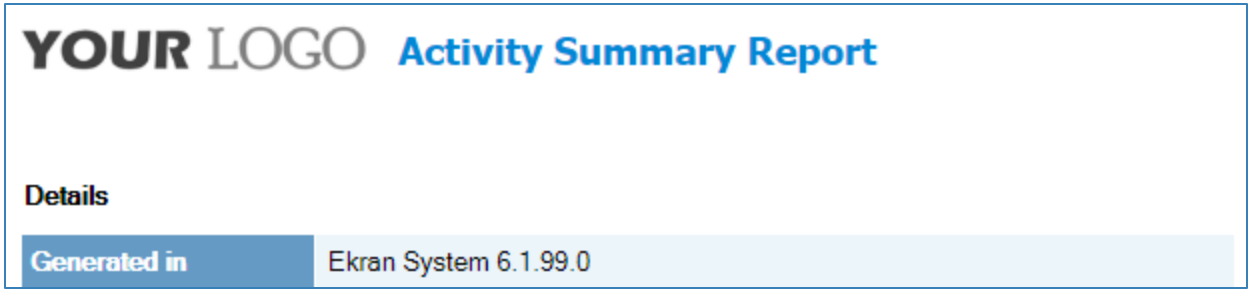
Ustawienia Custom Logo pozwalają na włączenie używania niestandardowych plików graficznych zamiast domyślnego logo na powiadomieniach Ekran Client podczas drugiego uwierzytelniania, blokady użytkownika, itp.



Konfiguracja Raportów

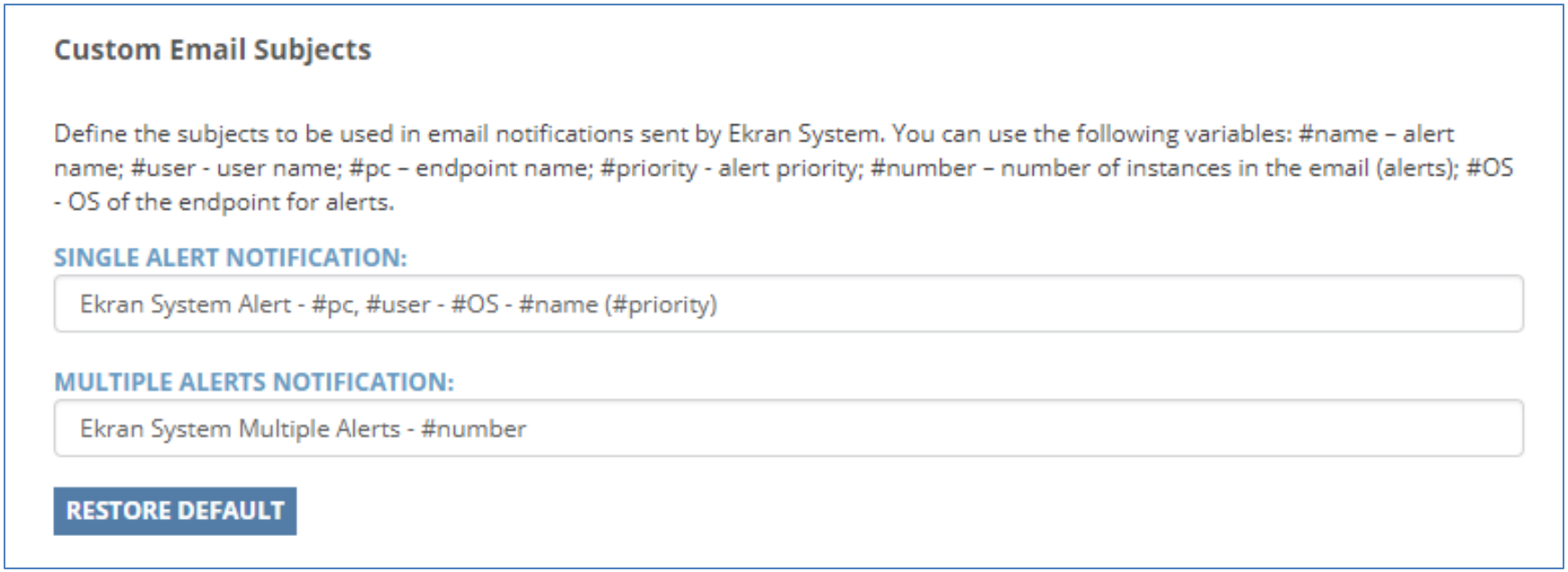
Ustawienia raportów niestandardowych umożliwiają włączenie używania niestandardowego pliku graficznego zamiast domyślnego logo w raportach. Można również dodać nagłówek i stopkę do raportów.





Konfiguracja Email

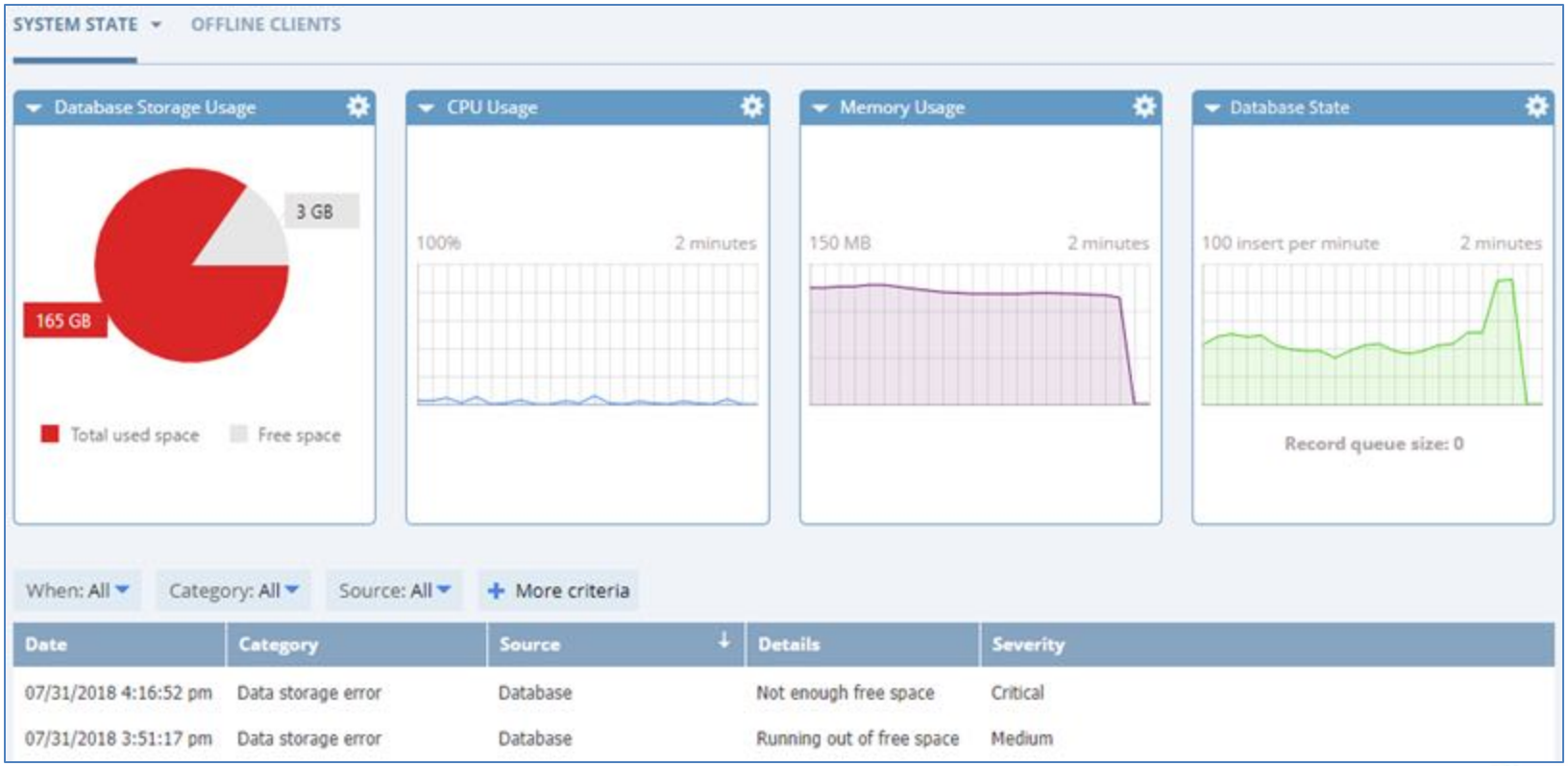
Niestandardowe ustawienia obiektów poczty elektronicznej umożliwiają zdefiniowanie tematów, które mają być używane w powiadomieniach e-mail wysyłanych przez Ekran System.



Health Monitoring

System Health Monitoring

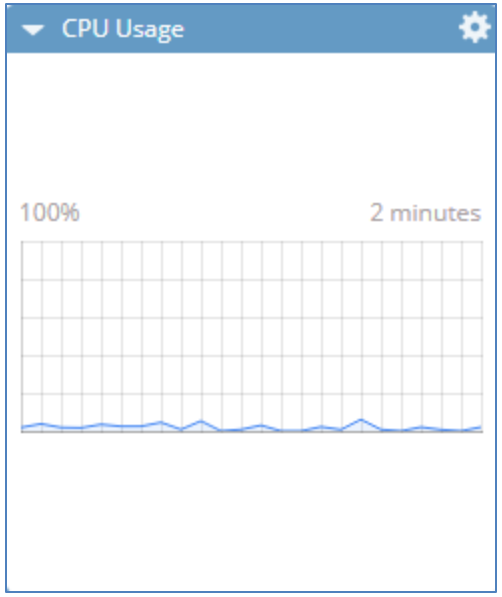
System Health Monitoring pozwala uzyskać **szczegółowe informacje na temat wykorzystania bazy danych i błędów** występujących w systemie Ekran System, co pomaga monitorować „stan zdrowia” systemu i reagować na wszelkie problemy w odpowiednim czasie.

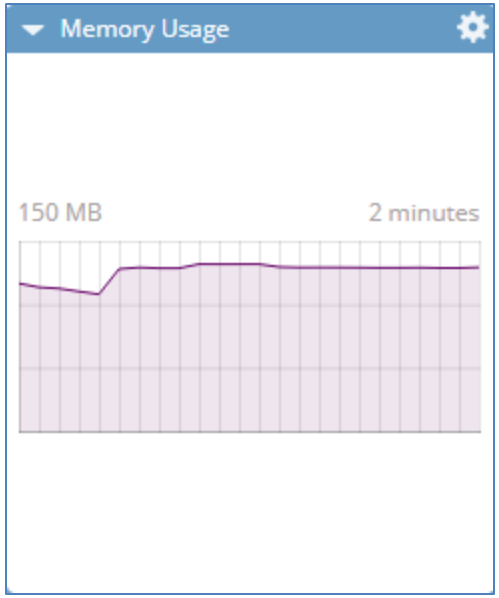


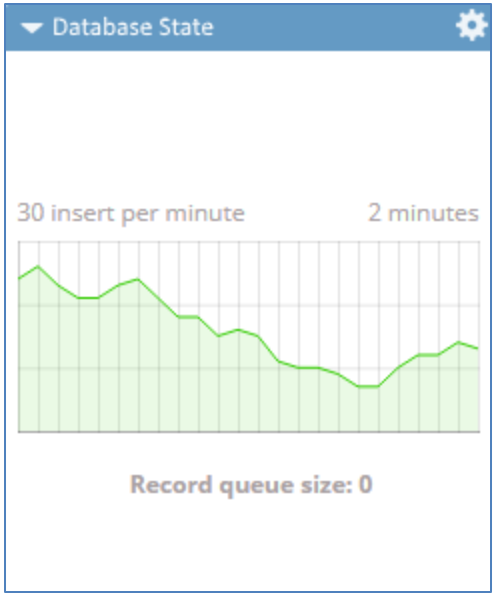
Monitoring Zasobów Serwera

Ekran System umożliwia wgląd w zasoby wykorzystane przez serwer Ekran System w danym momencie:

- Wykorzystywanie procesora przez serwer
- Wykorzystywanie pamięci przez serwer
- Stan bazy danych







EKRAN®

Odwiedź nas na:

www.ekransystem.com