



Ekran System

Podsumowanie funkcjonalności
oprogramowania

- [Podsumowanie funkcjonalności oprogramowania](#)
- [Ekran Server & Management Tool](#)
- [Zarządzanie bazą danych](#)
- [Licencjonowanie](#)
- [Instalowanie i aktualizacja programu Ekran Client](#)
- [Monitorowanie Parametrów](#)
- [Offline Client Detection \("Lost" Clients\)](#)
- [Ochrona Ekran Client](#)
- [Zaawansowana autoryzacja użytkowników](#)
- [Dwuskładnikowe uwierzytelnienie \(2FA\)](#)
- [Password Management](#)
- [Analiza zachowań użytkowników i podmiotów](#)
- [Zgoda administratora na logowanie](#)
- [Przyznawanie dostępu według harmonogramu](#)
- [Powiadamianie użytkowników o monitorowaniu](#)
- [Blokowanie użytkowników](#)
- [Przeglądanie Sesji](#)
- [Zdarzenia alarmowe \(Alerty\)](#)
- [Monitorowanie USB](#)
- [Dashboards](#)
- [Interactive Monitoring](#)
- [Reports](#)
- [Ustawienia Aplikacji](#)
- [Health Monitoring](#)

0 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.

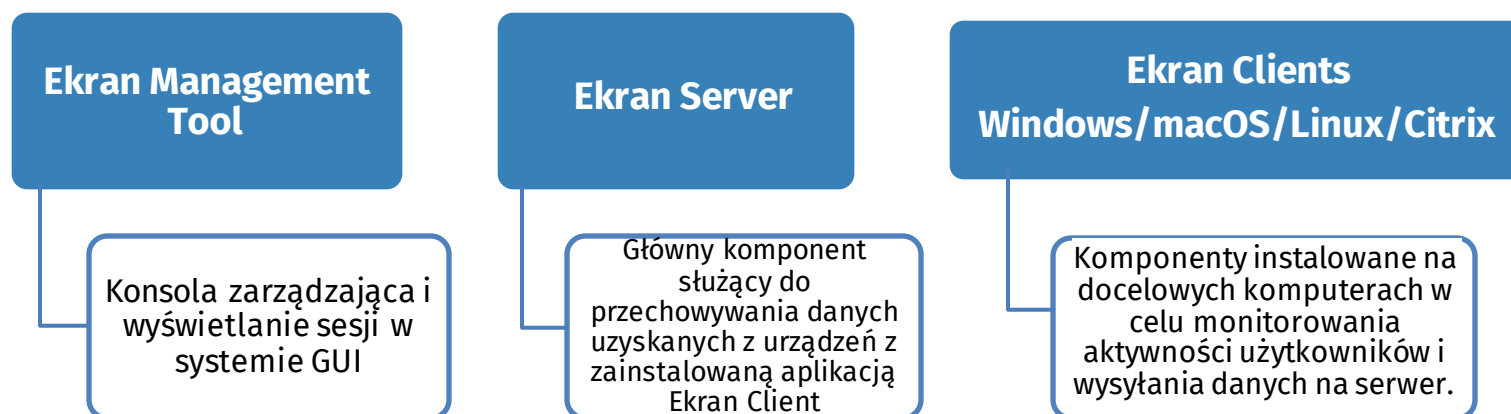
Elastyczne wdrażanie i licencjonowanie

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.

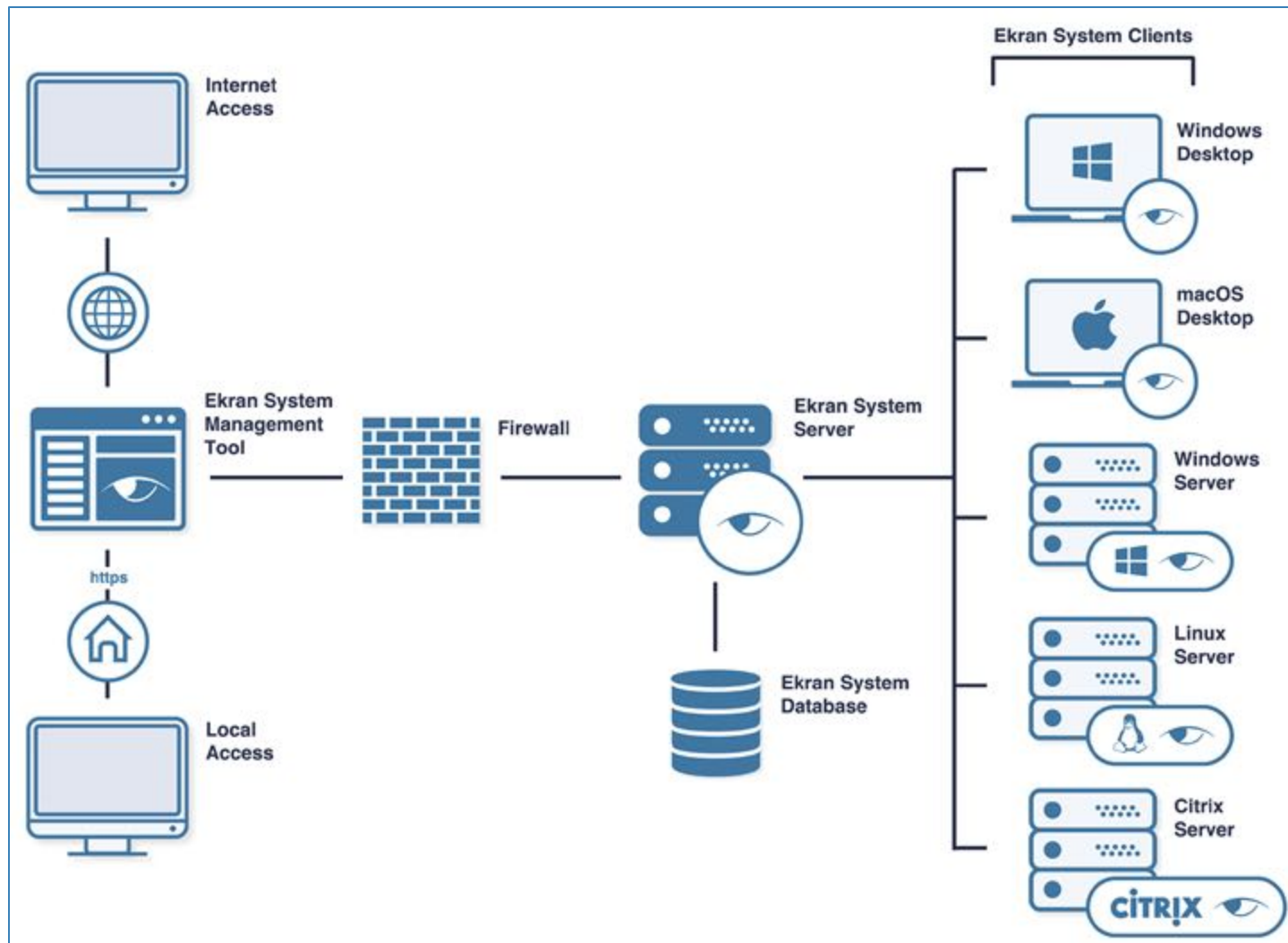
Ekran System jest rozwiązaniem monitorującym użytkowników, które podnosi poziom bezpieczeństwa IT. Służy do powstrzymywania, wykrywania i przerywania zagrożeń wewnętrznych w korporacyjnej infrastrukturze IT, a także pomaga w spełnieniu wymogów dotyczących zachowania zgodności, zarządzaniu uprzywilejowanymi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

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

Komponenty Ekran System



Podstawowy schemat wdrożenia Ekran System^{SECURITY}

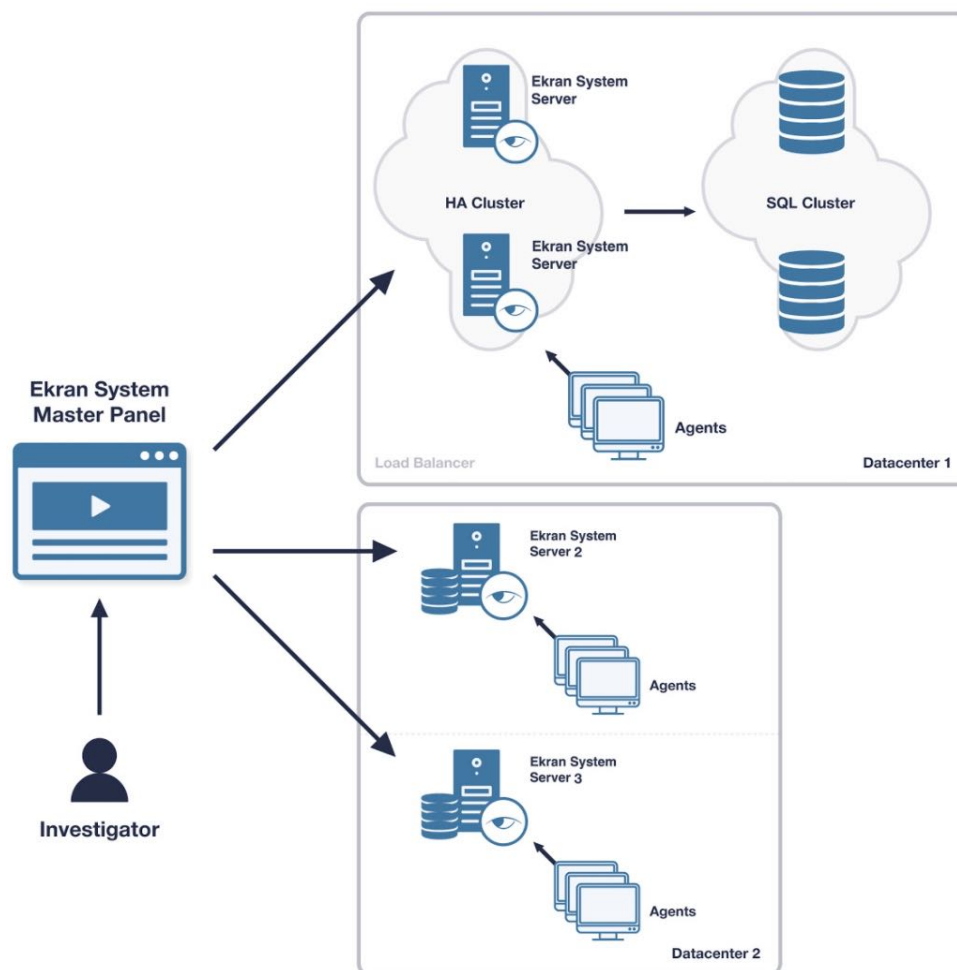


Wdrażanie na dużą skalę

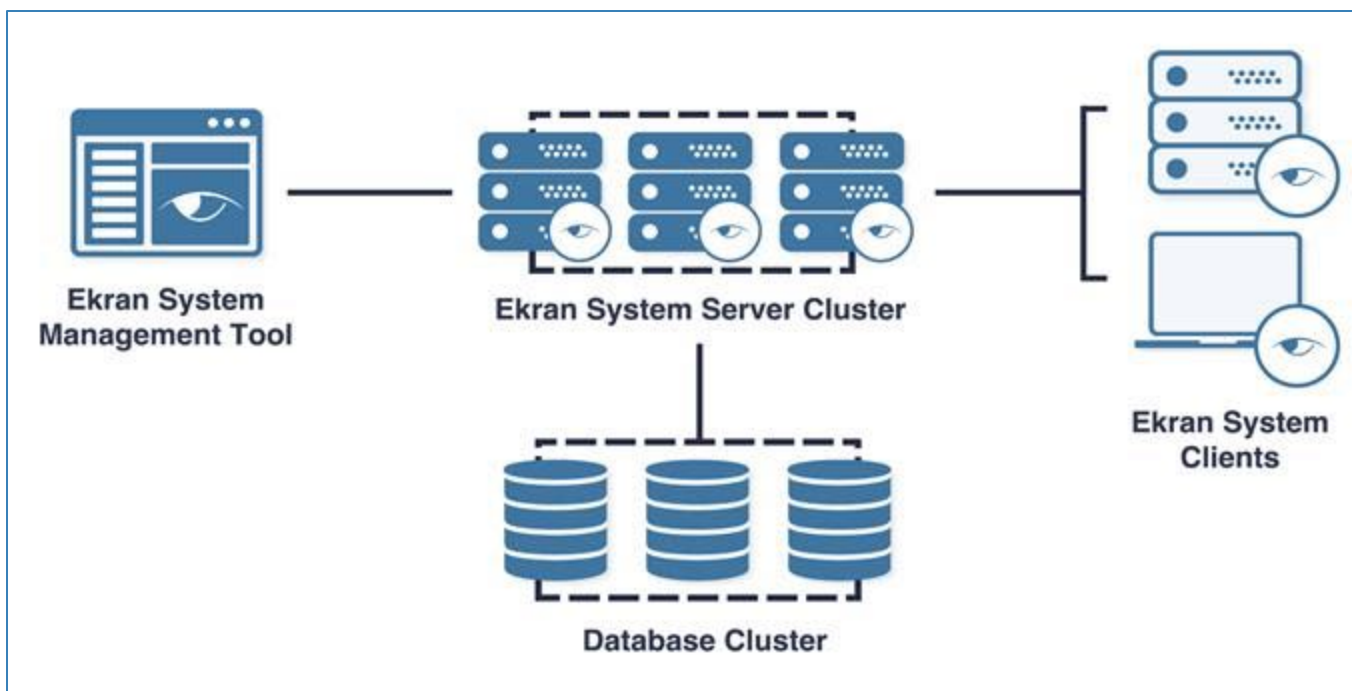
Pod względem skalowalności oraz dużych organizacji, które mogą mieć kilka geograficznie odizolowanych centrów danych, można wdrożyć wiele połączonych instancji serwera aplikacji.

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

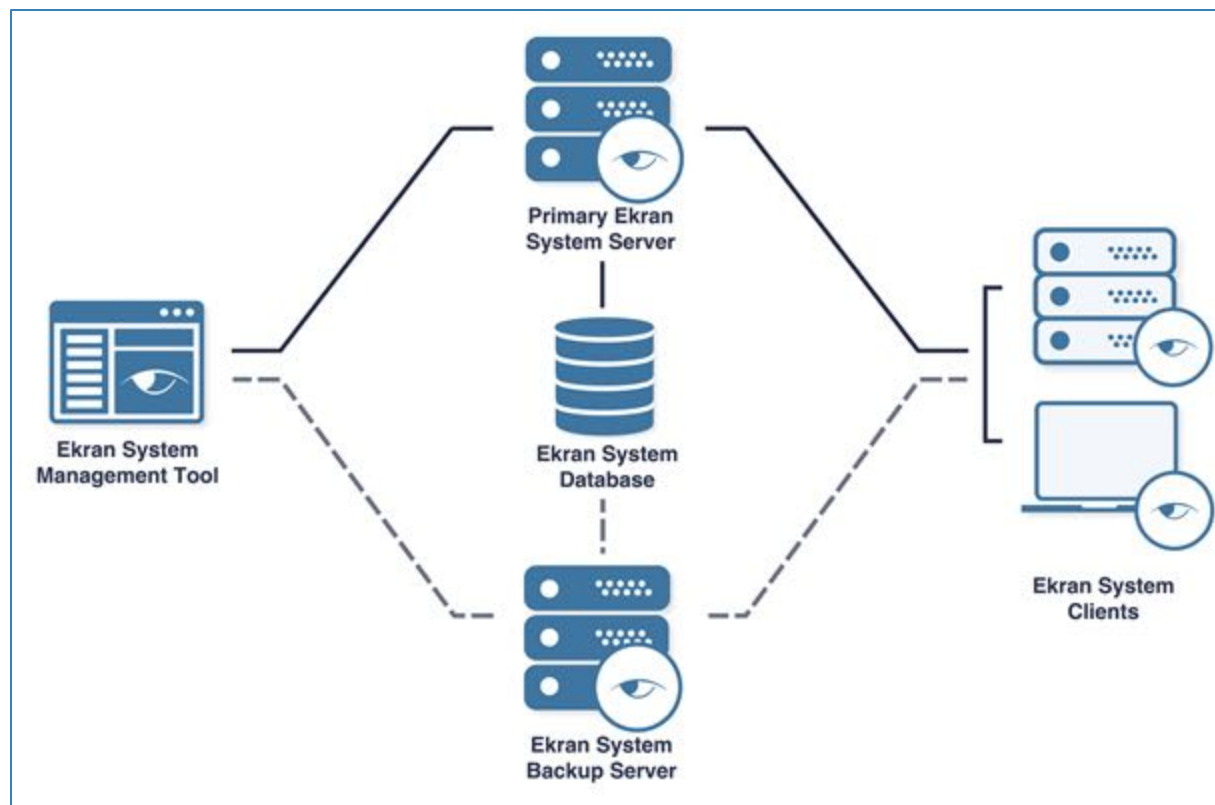
Master Panel, który jest dodatkowym samodzielnym komponentem Ekran System, łączy dane ze wszystkich serwerów aplikacji Ekran System w wielu lokalizacjach, umożliwiając zarządzanie nimi poprzez jeden interfejs użytkownika.



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

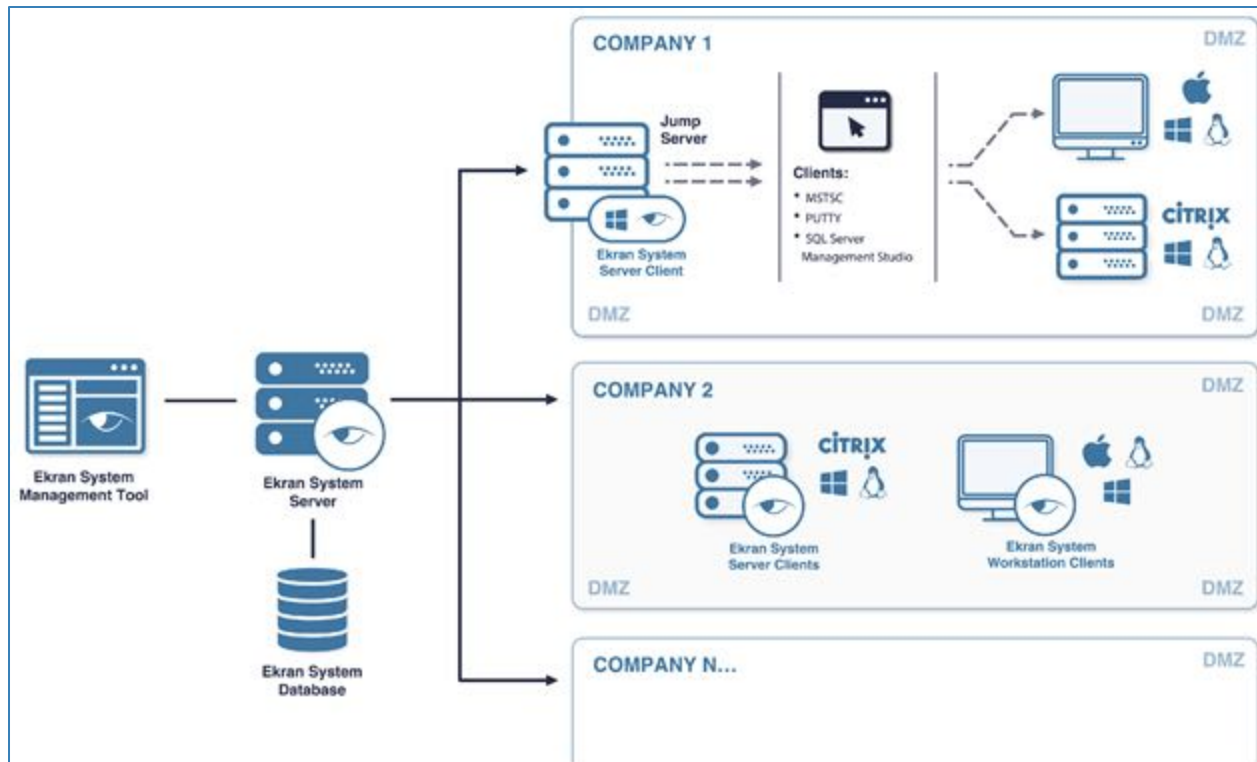


Tryb Disaster Recovery pozwala na konfigurowanie oraz wdrażanie Ekran System w taki sposób, aby w przypadku przerwania pracy Ekran Server, kolejny serwer mógł go zastąpić bez narażenia na utratę danych i przeinstalowania systemu.



Tryb Single-Tenant/Multi-Tenant

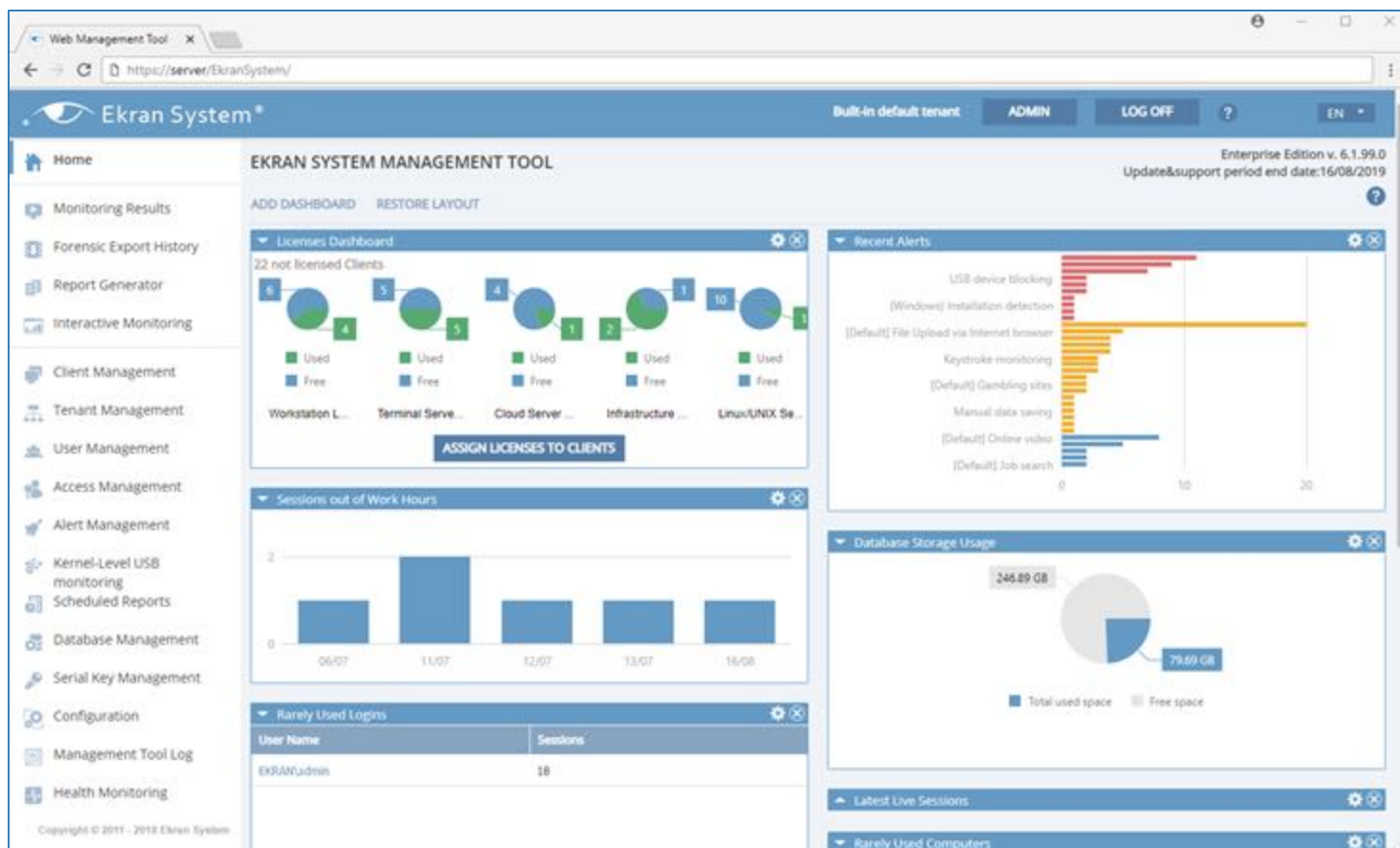
Tryb Multi-tenant pozwala na utworzenie odrębnych środowisk do zarządzania w ramach jednej instancji Ekran System. Dane każdego środowiska są niezależne i niedostępne między sobą.



Ekran Server i Management Tool

Zarządzanie użytkownikami, integracja
z Active Directory, ustawienia
Management Tool

Możliwość zarządzania całym systemem przez Management Tool w przeglądarce internetowej.



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.

TENANTS				
ADD TENANT ?				
Tenant Name	Tenant Admin	Description	Tenant Key	
 Built-in default tenant	admin	Auto-generated admin account	90807A10-DF80-45EA-A7DE-A550B55F548A	 Edit Tenant
 Insulent_company	insulent@gmail.com		88C6C707-06FA-451E-A02B-C8EC0F35D301	 Edit Tenant
 ABC_corporation	abc@gmail.com		E6D62ABF-EF60-4E1C-8AED-12DA37E700BB	 Edit Tenant

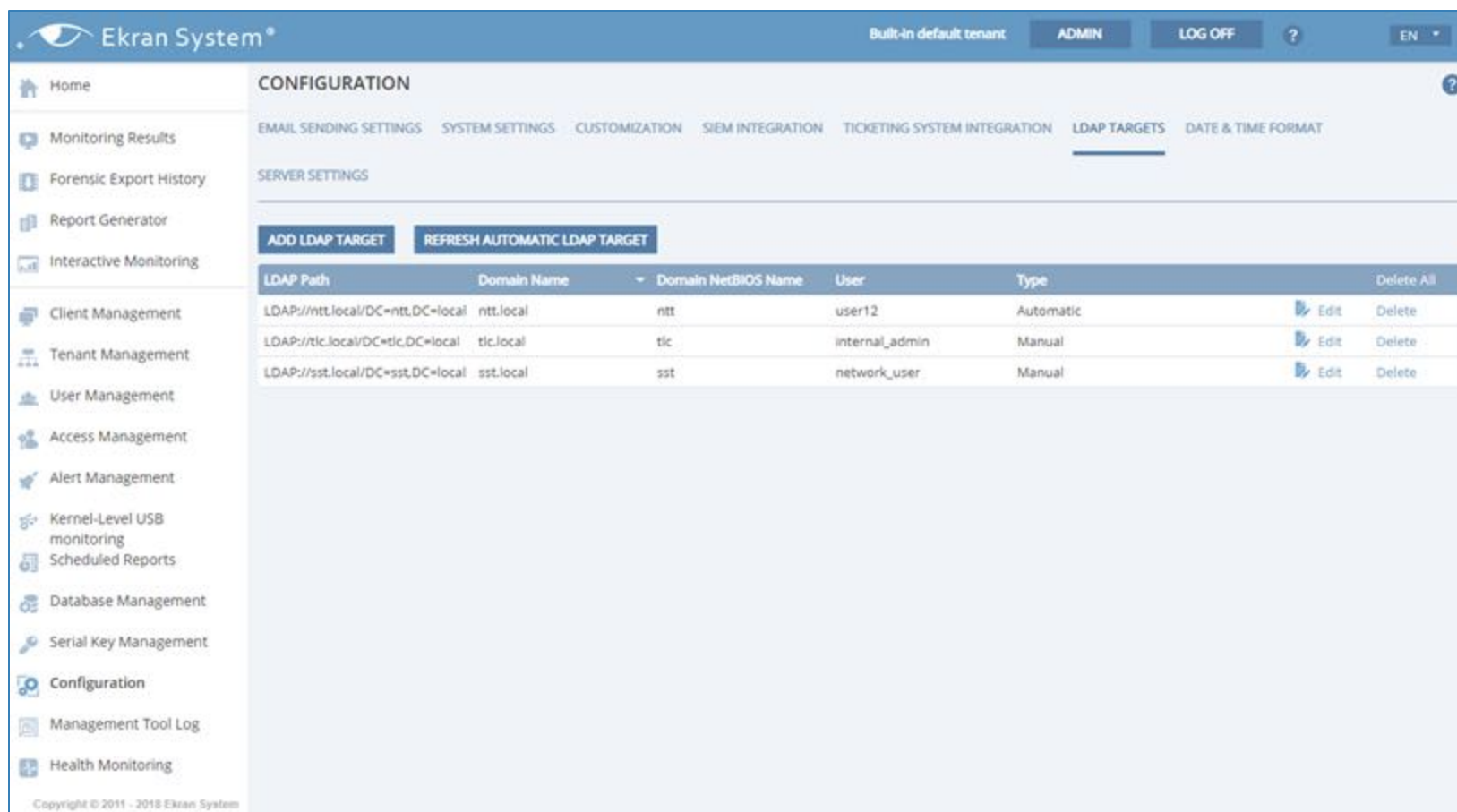
- Tworzenie dwóch typów użytkowników: **Lokalny** lub **Active Directory** (Windows Domain użytkownik/grupa).
- Budowanie grup użytkowników w celu łatwiejszego zarządzania.
- Możliwość nadawania uprawnień wszystkim użytkownikom.



The screenshot displays a user management interface with a search bar at the top and a table of users below. The interface is divided into three sections: 'All users', 'Administrators', and 'Supervisors'. Each section has a table of users with columns for Login, First name, Last name, and Description. Each user entry has an 'Edit User' link.

ADD USER ADD USER GROUP ?			
Contains			
APPLY FILTERS			
▼ All users: Edit User Group			
Login	First name	Last name	Description
admin	Administrator		Auto-generated admin account
John	Doe		This is a user for secondary auth
adminlogin			This is an internal user for access to EnterpServ2
internalUser			this is an internal user for access to EnterpServ4
▼ Administrators: Users with all permissions Edit User Group			
Login	First name	Last name	Description
admin	Administrator		Auto-generated admin account
internalUser			this is an internal user for access to EnterpServ4
internalUser2			This is an internal user for access to SecureServer
▼ Supervisors: Users that can view monitoring results of all Clients Edit User Group			
Login	First name	Last name	Description
John	Doe		This is a user for secondary auth

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

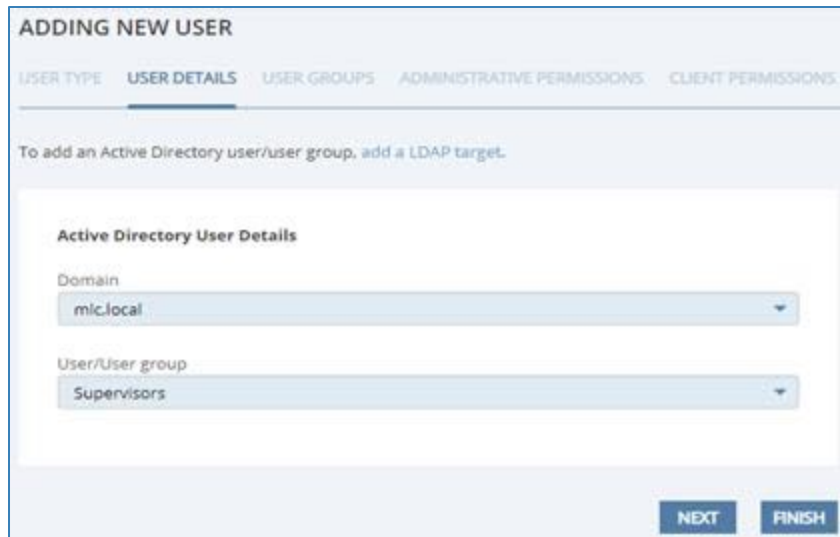


The screenshot shows the Ekran System configuration interface. The left sidebar contains a navigation menu with options like Home, Monitoring Results, Forensic Export History, Report Generator, Interactive Monitoring, Client Management, Tenant Management, User Management, Access Management, Alert Management, Kernel-Level USB monitoring, Scheduled Reports, Database Management, Serial Key Management, Configuration, Management Tool Log, and Health Monitoring. The main content area is titled 'CONFIGURATION' and includes tabs for various settings. The 'LDAP TARGETS' tab is selected, displaying a table of configured LDAP targets.

LDAP Path	Domain Name	Domain NetBIOS Name	User	Type	Actions	
LDAP://ntt.local/DC=ntt,DC=local	ntt.local	ntt	user12	Automatic	Edit	Delete
LDAP://tlc.local/DC=tlc,DC=local	tlc.local	tlc	internal_admin	Manual	Edit	Delete
LDAP://sst.local/DC=sst,DC=local	sst.local	sst	network_user	Manual	Edit	Delete

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.



ADDING NEW USER

USER TYPE USER DETAILS USER GROUPS ADMINISTRATIVE PERMISSIONS CLIENT PERMISSIONS

To add an Active Directory user/user group, add a LDAP target.

Active Directory User Details

Domain
mic.local

User/User group
Supervisors

NEXT FINISH

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

Default Configuration



Custom Configuration



Metadata
in DB



Binary files in binary system
folder including NAS

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

Auto-Cleanup options
☐ Never
☐ Run once
☒ Repeat by scheduler

PERFORM EVERY (DAYS)

START AT 

ACTION TYPE

SESSIONS OLDER THAN (DAYS)



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

Auto-Cleanup options

CLEANUP SETTINGS TYPE

Custom ▼

☐ Never

☒ Run once

☐ Repeat by scheduler

ACTION TYPE

Archive & Cleanup ▼

SESSIONS OLDER THAN (DAYS)

Archive parameters

INSTANCE

ARCHIVE DATABASE NAME

USER

PASSWORD

☒ Shrink database after cleanup

☒ Delete offline Clients without sessions

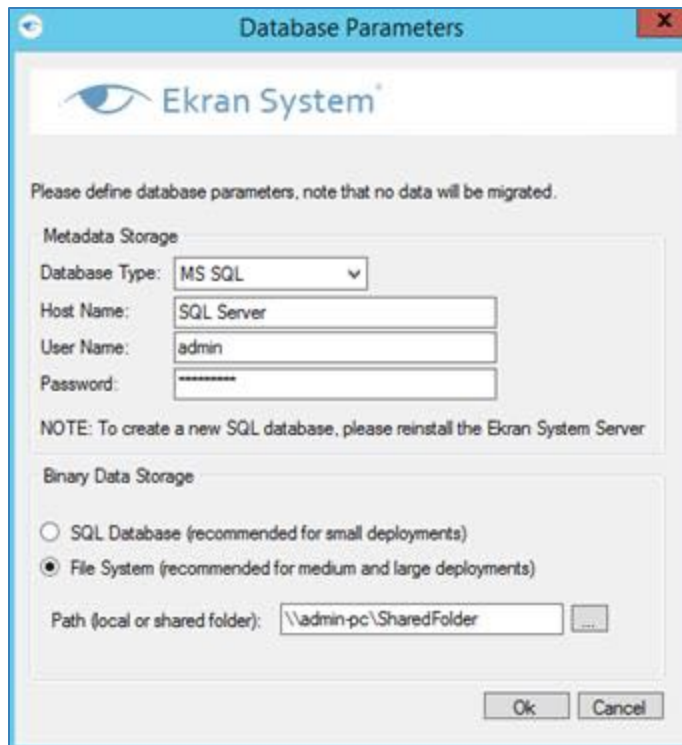
TEST DATABASE CONNECTION



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

MONITORING RESULTS										
Archive database name ArchiveActivityDB										
CLIENT SESSIONS ARCHIVED SESSIONS ▾										
Who: All ▾ Where: All ▾ When: All ▾ + More criteria What Q ...										
Risk Score	Alerts	User Name	Client Name	Remote Ho...	OS	Type	Start	Last Activity	Finish	Duration
		Admin	Server		Windows	Finis...	04/25/2019 2:00...	04/25/2019 6:18...	04/25/2019 6:18...	04:18:30
		Tom	Comp1		Windows	Finis...	04/24/2019 8:00...	04/25/2019 1:24...	04/25/2019 1:24...	05:24:30
Approved		KristineWillis	Comp3		Windows	Finis...	04/19/2019 10:0...	04/19/2019 7:54...	04/19/2019 7:54...	09:54:00
		FillMorris	Comp5		Windows	Finis...	04/19/2019 6:00...	04/19/2019 7:12...	04/19/2019 7:12...	13:12:00
Skipped		JohnMaers	Comp22		Windows	Finis...	04/23/2019 7:00...	04/23/2019 8:06...	04/23/2019 8:06...	01:06:00
		AnnaRikier	Comp3		Windows	Finis...	04/18/2019 10:0...	04/18/2019 7:54...	04/18/2019 7:54...	09:54:00

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.



Database Parameters

Ekran System

Please define database parameters, note that no data will be migrated.

Metadata Storage

Database Type: MS SQL

Host Name: SQL Server

User Name: admin

Password: *****

NOTE: To create a new SQL database, please reinstall the Ekran System Server

Binary Data Storage

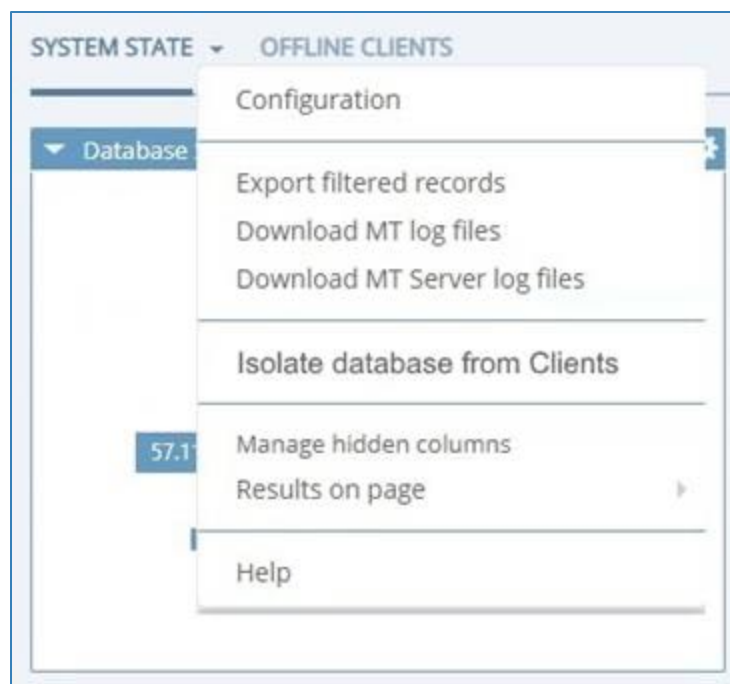
☐ SQL Database (recommended for small deployments)

☒ File System (recommended for medium and large deployments)

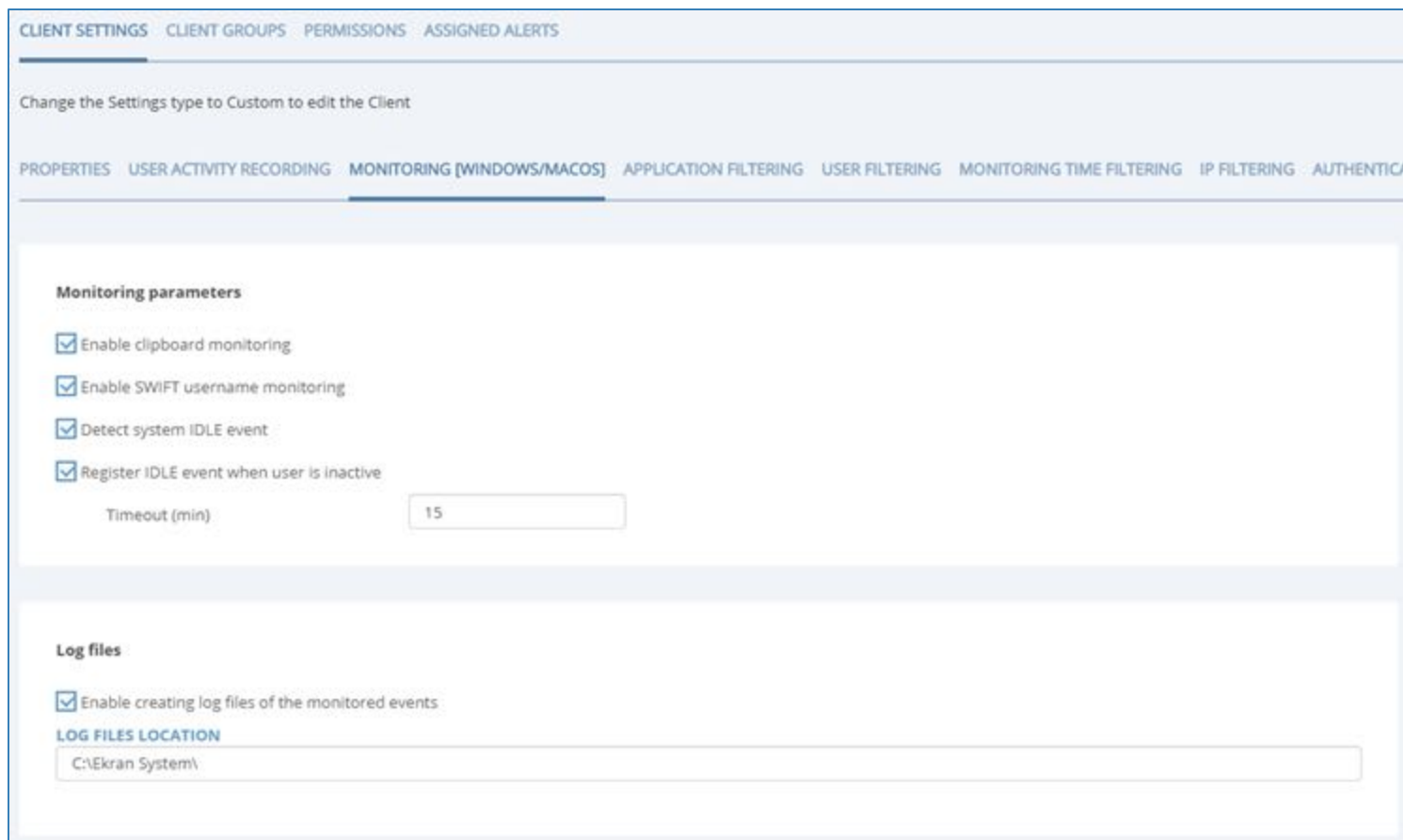
Path (local or shared folder): \\admin-pc\SharedFolder

Ok Cancel

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.



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



The screenshot displays the 'CLIENT SETTINGS' configuration page for a client. The top navigation bar includes 'CLIENT SETTINGS', 'CLIENT GROUPS', 'PERMISSIONS', and 'ASSIGNED ALERTS'. Below this, a message states: 'Change the Settings type to Custom to edit the Client'. The main content area has a sub-navigation bar with 'PROPERTIES', 'USER ACTIVITY RECORDING', 'MONITORING [WINDOWS/MACOS]', 'APPLICATION FILTERING', 'USER FILTERING', 'MONITORING TIME FILTERING', 'IP FILTERING', and 'AUTHENTICATION'. The 'MONITORING [WINDOWS/MACOS]' section is active and contains two main sections: 'Monitoring parameters' and 'Log files'. Under 'Monitoring parameters', there are four checked checkboxes: 'Enable clipboard monitoring', 'Enable SWIFT username monitoring', 'Detect system IDLE event', and 'Register IDLE event when user is inactive'. Below these is a 'Timeout (min)' field with the value '15'. The 'Log files' section has one checked checkbox: 'Enable creating log files of the monitored events'. Below this is a 'LOG FILES LOCATION' field containing the path 'C:\Ekran System\'. The interface is clean with a light blue header and a white main area.

CLIENT SETTINGS CLIENT GROUPS PERMISSIONS ASSIGNED ALERTS

Change the Settings type to Custom to edit the Client

PROPERTIES USER ACTIVITY RECORDING MONITORING [WINDOWS/MACOS] APPLICATION FILTERING USER FILTERING MONITORING TIME FILTERING IP FILTERING AUTHENTICATION

Monitoring parameters

- ☒ Enable clipboard monitoring
- ☒ Enable SWIFT username monitoring
- ☒ Detect system IDLE event
- ☒ Register IDLE event when user is inactive

Timeout (min) 15

Log files

- ☒ Enable creating log files of the monitored events

LOG FILES LOCATION

C:\Ekran System\

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)

CONFIGURATION

EMAIL SENDING SETTINGS SYSTEM SETTINGS CUSTOMIZATION SIEM INTEGRATION ▾

Log Format settings

☒ Create a log file

LOG FILE LOCATION

C:\Program Files\Ekran System\Ekran System\Server\EventLog

☒ Clean daily at 12:00:00 AM ⌚

☐ Cleanup every 1 days ▾

MAXIMUM FILE SIZE (GB) 128

Log Format settings

LOG FORMAT

CEF log ▾

DATE FORMAT

MMM dd yyyy HH:mm:ss ▾

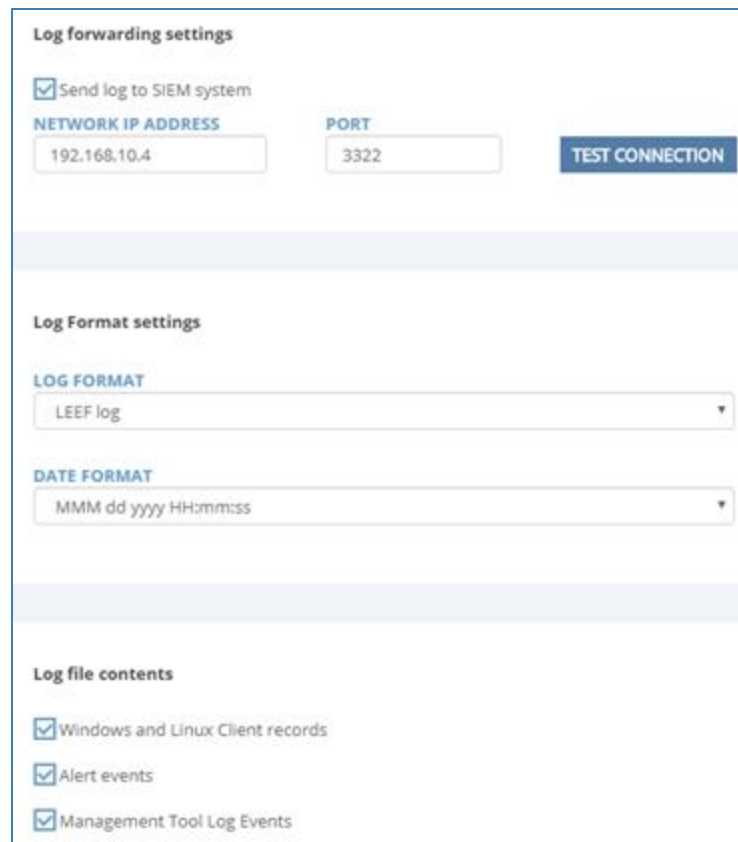
Log file contents

☒ Windows and Linux Client records

☒ Alert events

☒ Management Tool Log Events

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



The screenshot displays the configuration interface for SIEM integration, organized into three main sections:

- Log forwarding settings:** Includes a checked checkbox for "Send log to SIEM system". Below it, the "NETWORK IP ADDRESS" is set to "192.168.10.4" and the "PORT" is set to "3322". A "TEST CONNECTION" button is located to the right of the port field.
- Log Format settings:** Contains two dropdown menus. The "LOG FORMAT" is set to "LEEF log", and the "DATE FORMAT" is set to "MMM dd yyyy HH:mm:ss".
- Log file contents:** Includes three checked checkboxes: "Windows and Linux Client records", "Alert events", and "Management Tool Log Events".

Licencjonowanie

Rodzaje licencji i zarządzanie kluczami
seryjnymi

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)

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	ASSIGN RECOMMENDED LICENSE
☐	Comp2	Social media	Workstation license	None	Not Work-related Activity Demo, Dat...	ASSIGN LICENSE OF SPECIFIC TYPE
☐	Comp1	Sites with adult content	Workstation license	None	Potentially Illicit Activity Demo, Fraud...	UNASSIGN LICENSE
☐	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		

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.

SERIAL KEY MANAGEMENT

SERIAL KEYS | LICENSES GRANTED

Update & Support period end date: 01/07/2022
Terminal Server Client licenses granted: 913 of 913
Workstation Client licenses granted: 892 of 892
Infrastructure Server Client licenses granted: 189 of 189
Enterprise serial key: Activated
Unique identifier: [REDACTED]

ACTIVATE PRODUCT ONLINE
ACTIVATE PRODUCT OFFLINE
DEACTIVATE SELECTED
UPDATE KEY STATE

Key	Activation Date	Type	State	Details
☐ [REDACTED]	01/01/0001	Permanent Enterprise	Activated	Expires: 01/07/2022 Workstation Licenses: 892 Infrastructure Server Licenses: 189 Terminal Server Licenses: 913

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

SERIAL KEY MANAGEMENT

SERIAL KEYS

LICENSES GRANTED

Update & Support period end date: 01/07/2022
Terminal Server Client licenses granted: 913 of 913
Workstation Client licenses granted: 892 of 892
Infrastructure Server Client licenses granted: 189 of 189
Enterprise serial key: Activated
Unique identifier: [REDACTED]

ACTIVATE PRODUCT ONLINE

ACTIVATE PRODUCT OFFLINE

DEACTIVATE SELECTED

UPDATE KEY STATE

Key	Activation Date	Type	State	Details
☐ [REDACTED]	01/01/0001	Permanent Enterprise	Activated	Expires: 01/07/2022 Workstation Licenses: 892 Infrastructure Server Licenses: 189 Terminal Server Licenses: 913

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 pulpików za każdym razem, gdy tworzone są nowe pulpity z systemem Windows i usuwa je za każdym razem, gdy maszyny Ekran Client są wyłączone.

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

Wygodna instalacja programu Ekran Client:

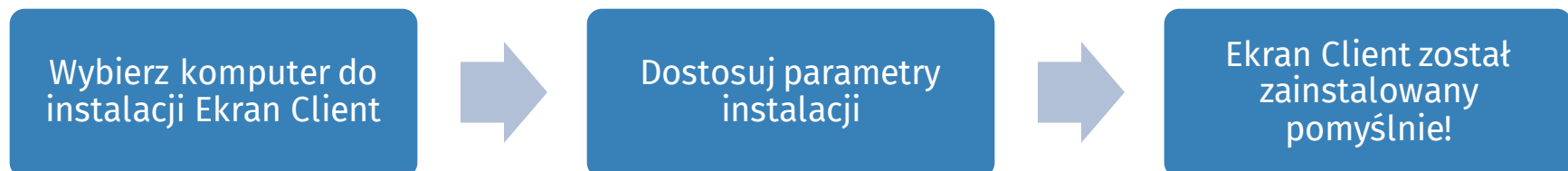
- **Lokalna:**

- 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



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

COMPUTERS WITHOUT CLIENTS

Define computers on which Clients must be installed. If during previous installations Clients were not installed on some computers, these computers will be listed here. The computers will be removed from the list after the Clients are installed on them.

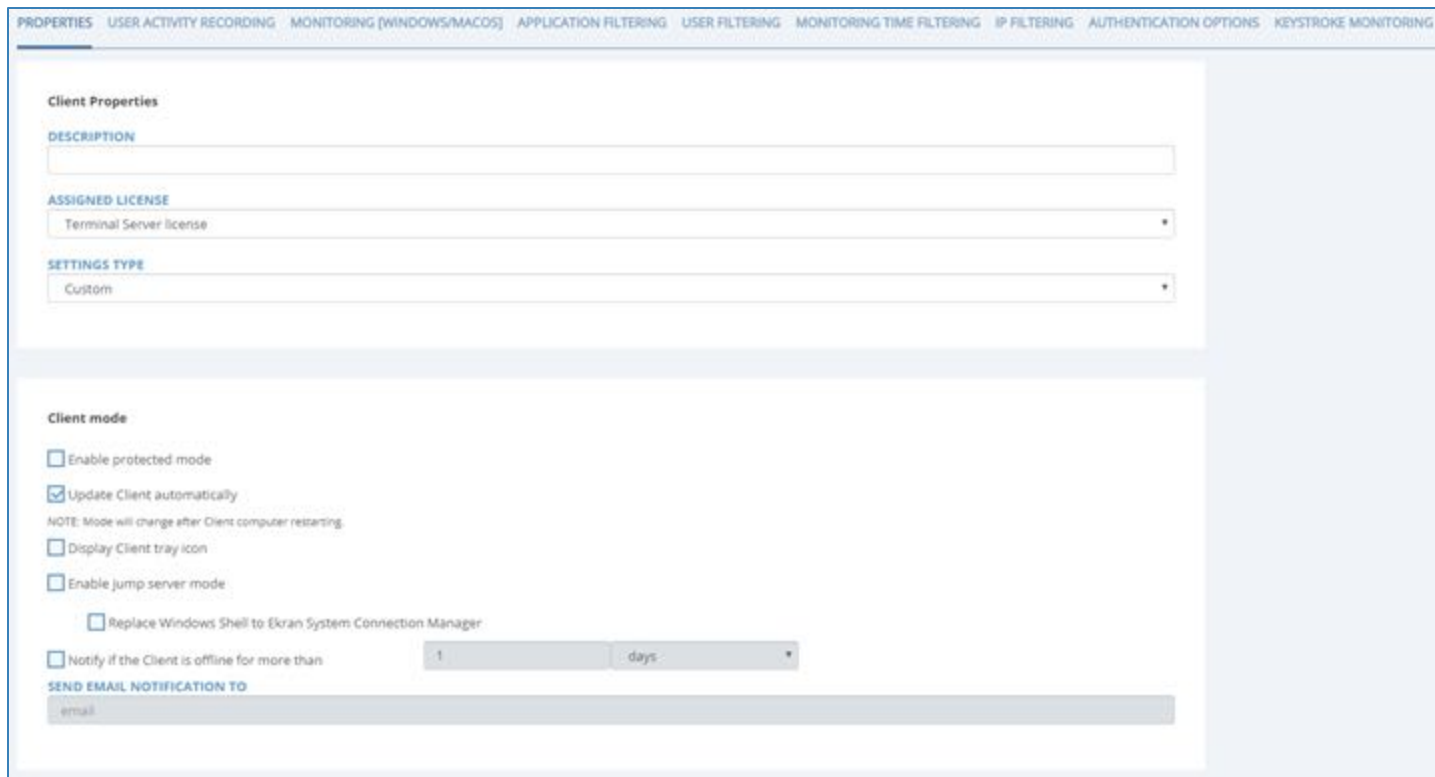
[DEPLOY VIA NETWORK SCAN](#) [DEPLOY VIA IP RANGE](#) [DEPLOY ON SPECIFIC COMPUTERS](#) [DOWNLOAD INSTALLATION FILE](#)

Computer	Workgroup \ Domain	IP	Description	Previous installation failure	Remove all from list
alice-pc	PVC	10.181.100			Remove from list
kate-pc	PVC	10.109.1.18			Remove from list

[READ INSTALLATION PREREQUISITES](#) [INSTALL USING EXISTING .INI FILE](#) [INSTALL](#)

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).



The screenshot shows the 'Client Properties' window in the Ekran System interface. The 'Client mode' section is expanded, showing several options:

- ☐ Enable protected mode
- ☒ Update Client automatically
- NOTE: Mode will change after Client computer restarting.
- ☐ Display Client tray icon
- ☐ Enable jump server mode
- ☐ Replace Windows Shell to Ekran System Connection Manager
- ☐ Notify if the Client is offline for more than days
- SEND EMAIL NOTIFICATION TO**

Monitorowanie parametrów

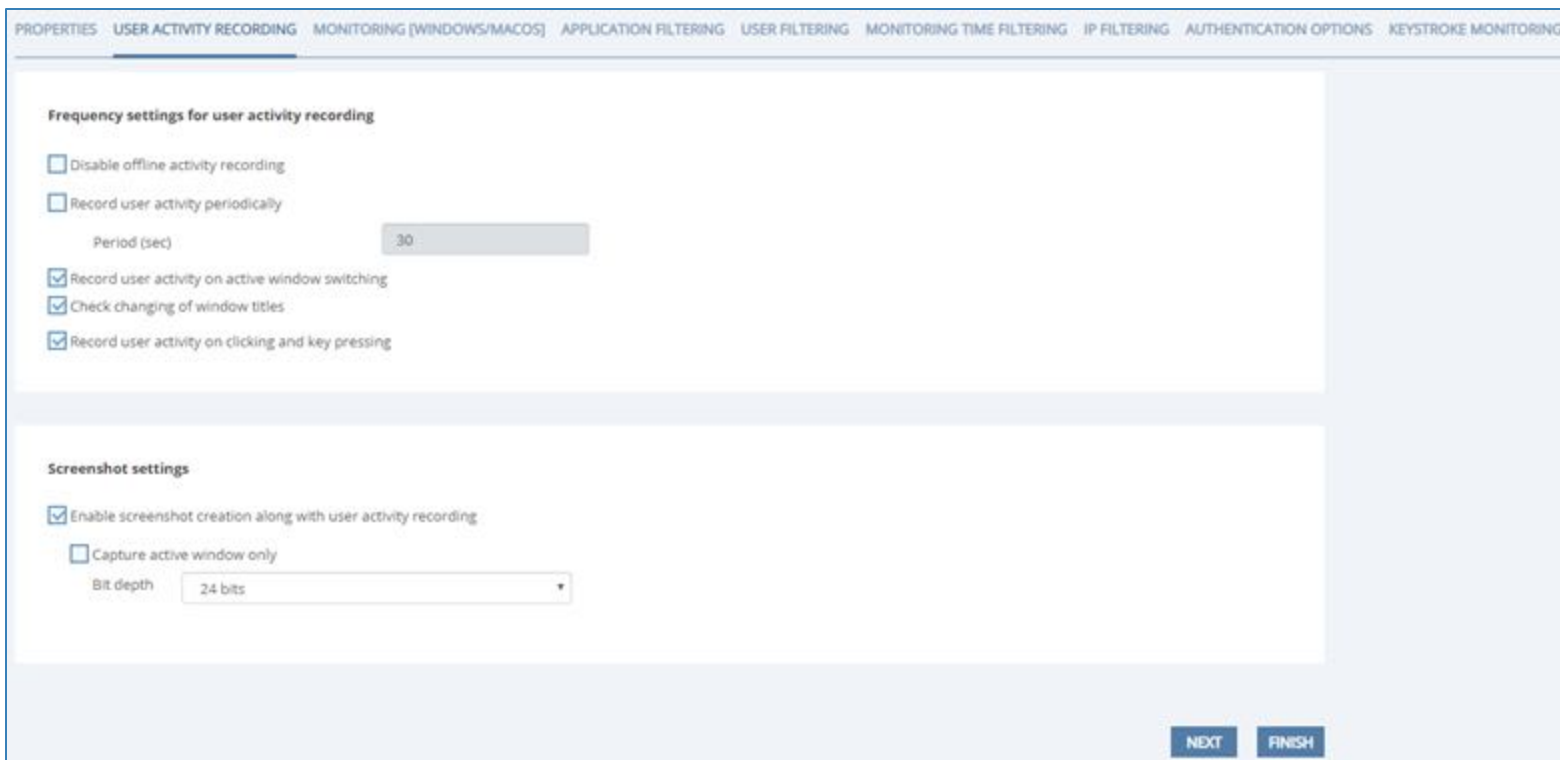
Zrzuty ekranu wysłane przez aplikację Ekran Client są przechowywane w formie delt (różnice pomiędzy nowszym nagraniem ekranu a starszym) w celu zminimalizowania przestrzeni dyskowej.

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

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.



The screenshot displays the 'USER ACTIVITY RECORDING' configuration tab within the Ekran System application. The interface includes a top navigation bar with various settings categories. The main content area is divided into two sections: 'Frequency settings for user activity recording' and 'Screenshot settings'. In the frequency settings section, there are checkboxes for 'Disable offline activity recording' and 'Record user activity periodically'. The 'Record user activity periodically' option is selected, and a 'Period (sec)' input field is set to 30. Below these are three checked checkboxes: 'Record user activity on active window switching', 'Check changing of window titles', and 'Record user activity on clicking and key pressing'. The screenshot settings section has a checked checkbox for 'Enable screenshot creation along with user activity recording'. Below this, there is an unchecked checkbox for 'Capture active window only' and a 'Bit depth' dropdown menu currently set to '24 bits'. At the bottom right of the configuration window, there are 'NEXT' and 'FINISH' buttons.

PROPERTIES USER ACTIVITY RECORDING MONITORING [WINDOWS/MACOS] APPLICATION FILTERING USER FILTERING MONITORING TIME FILTERING IP FILTERING AUTHENTICATION OPTIONS KEYSTROKE MONITORING

Frequency settings for user activity recording

- ☐ Disable offline activity recording
- ☐ Record user activity periodically
 - Period (sec): 30
- ☒ Record user activity on active window switching
- ☒ Check changing of window titles
- ☒ Record user activity on clicking and key pressing

Screenshot settings

- ☒ Enable screenshot creation along with user activity recording
 - ☐ Capture active window only
 - Bit depth: 24 bits

NEXT FINISH

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:

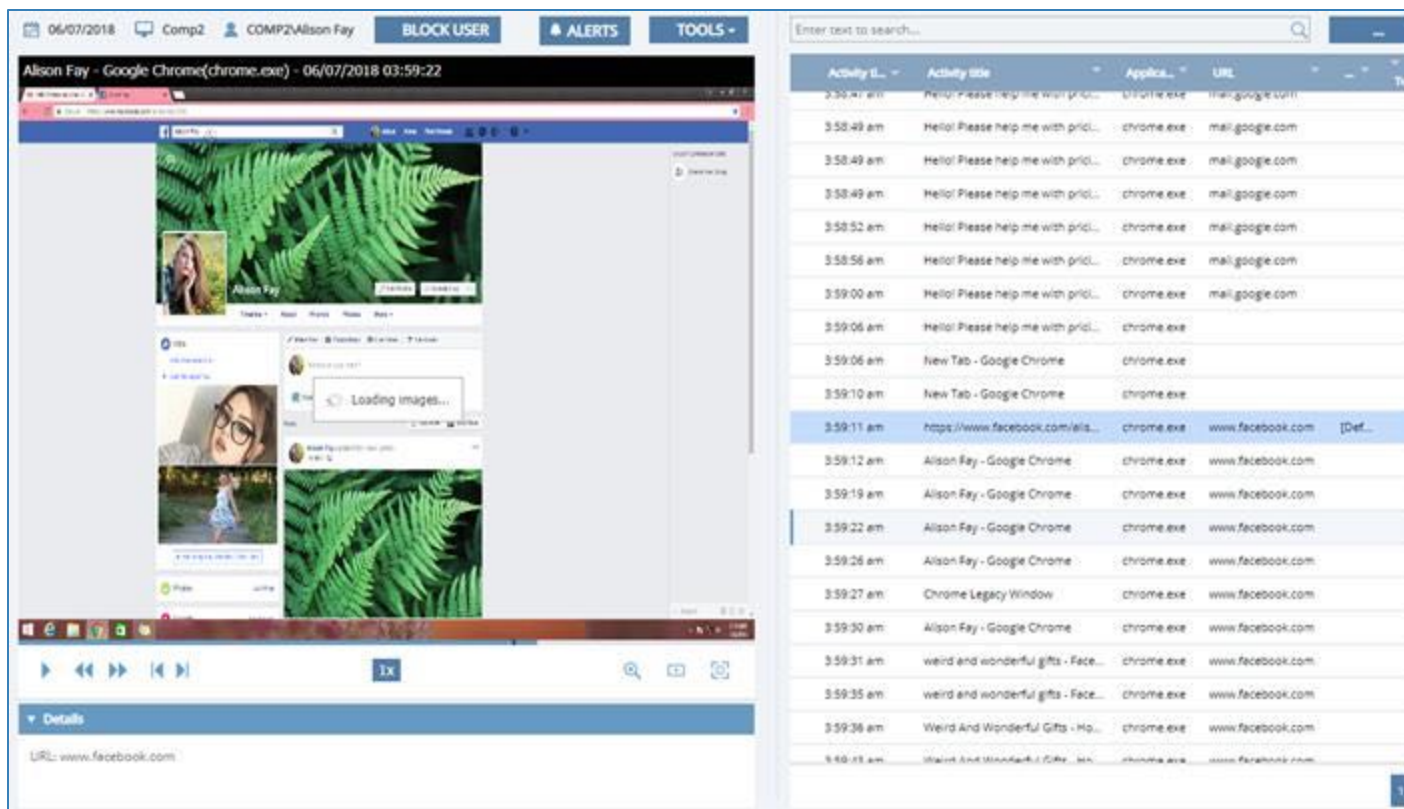
- Skype
- Slack
- Zoom
- Viber
- WhatsApp
- Firefox
- Chrome
- Opera
- Internet Explorer

Audio settings

☒ Enable audio recording

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

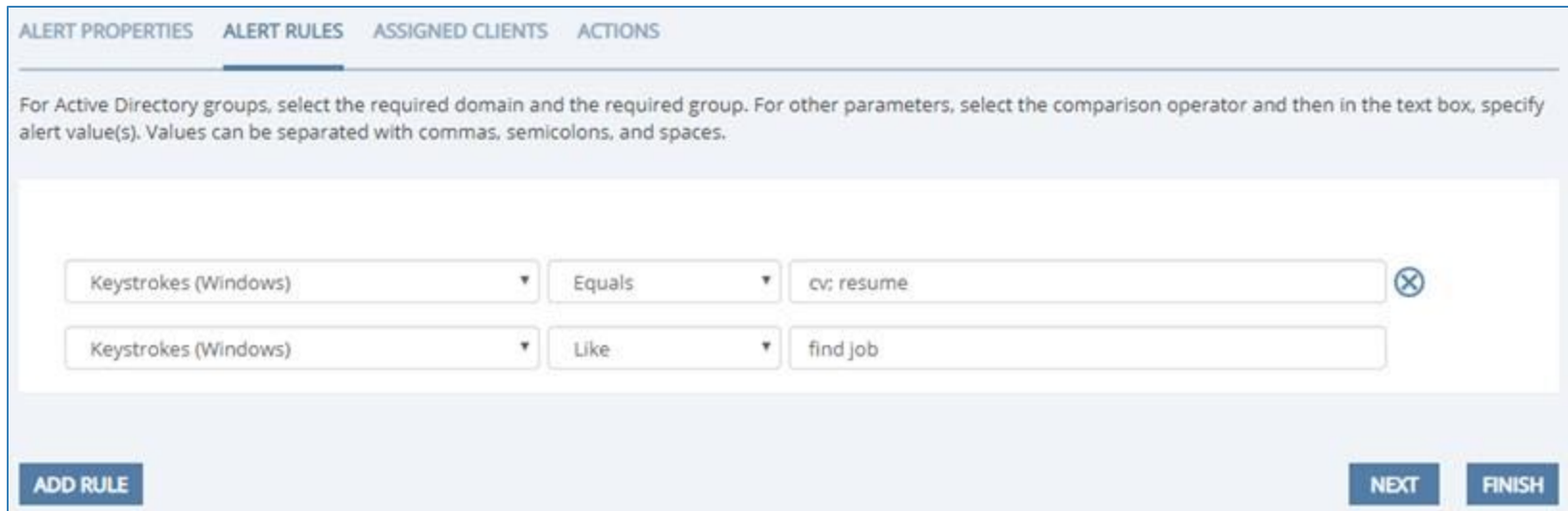


The screenshot displays the Ekran Client interface. On the left, a monitored browser window titled 'Alison Fay - Google Chrome(chrome.exe) - 06/07/2018 03:59:22' is shown, displaying a Facebook profile page. On the right, a table lists the captured activity:

Activity Time	Activity Title	Applica...	URL
3:58:47 am	Hello! Please help me with pri...	chrome.exe	mail.google.com
3:58:49 am	Hello! Please help me with pri...	chrome.exe	mail.google.com
3:58:49 am	Hello! Please help me with pri...	chrome.exe	mail.google.com
3:58:49 am	Hello! Please help me with pri...	chrome.exe	mail.google.com
3:58:52 am	Hello! Please help me with pri...	chrome.exe	mail.google.com
3:58:56 am	Hello! Please help me with pri...	chrome.exe	mail.google.com
3:59:00 am	Hello! Please help me with pri...	chrome.exe	mail.google.com
3:59:06 am	Hello! Please help me with pri...	chrome.exe	
3:59:06 am	New Tab - Google Chrome	chrome.exe	
3:59:10 am	New Tab - Google Chrome	chrome.exe	
3:59:11 am	https://www.facebook.com/alis...	chrome.exe	www.facebook.com [Def...
3:59:12 am	Alison Fay - Google Chrome	chrome.exe	www.facebook.com
3:59:19 am	Alison Fay - Google Chrome	chrome.exe	www.facebook.com
3:59:22 am	Alison Fay - Google Chrome	chrome.exe	www.facebook.com
3:59:26 am	Alison Fay - Google Chrome	chrome.exe	www.facebook.com
3:59:27 am	Chrome Legacy Window	chrome.exe	www.facebook.com
3:59:30 am	Alison Fay - Google Chrome	chrome.exe	www.facebook.com
3:59:31 am	weird and wonderful gifts - Face...	chrome.exe	www.facebook.com
3:59:35 am	weird and wonderful gifts - Face...	chrome.exe	www.facebook.com
3:59:36 am	Weird And Wonderful Gifts - Ho...	chrome.exe	www.facebook.com
3:59:45 am	What's Hot! M... (Def...	chrome.exe	www.facebook.com

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.



ALERT PROPERTIES ALERT RULES ASSIGNED CLIENTS ACTIONS

For Active Directory groups, select the required domain and the required group. For other parameters, select the comparison operator and then in the text box, specify alert value(s). Values can be separated with commas, semicolons, and spaces.

Keystrokes (Windows) Equals cv: resume

Keystrokes (Windows) Like find job

ADD RULE NEXT FINISH

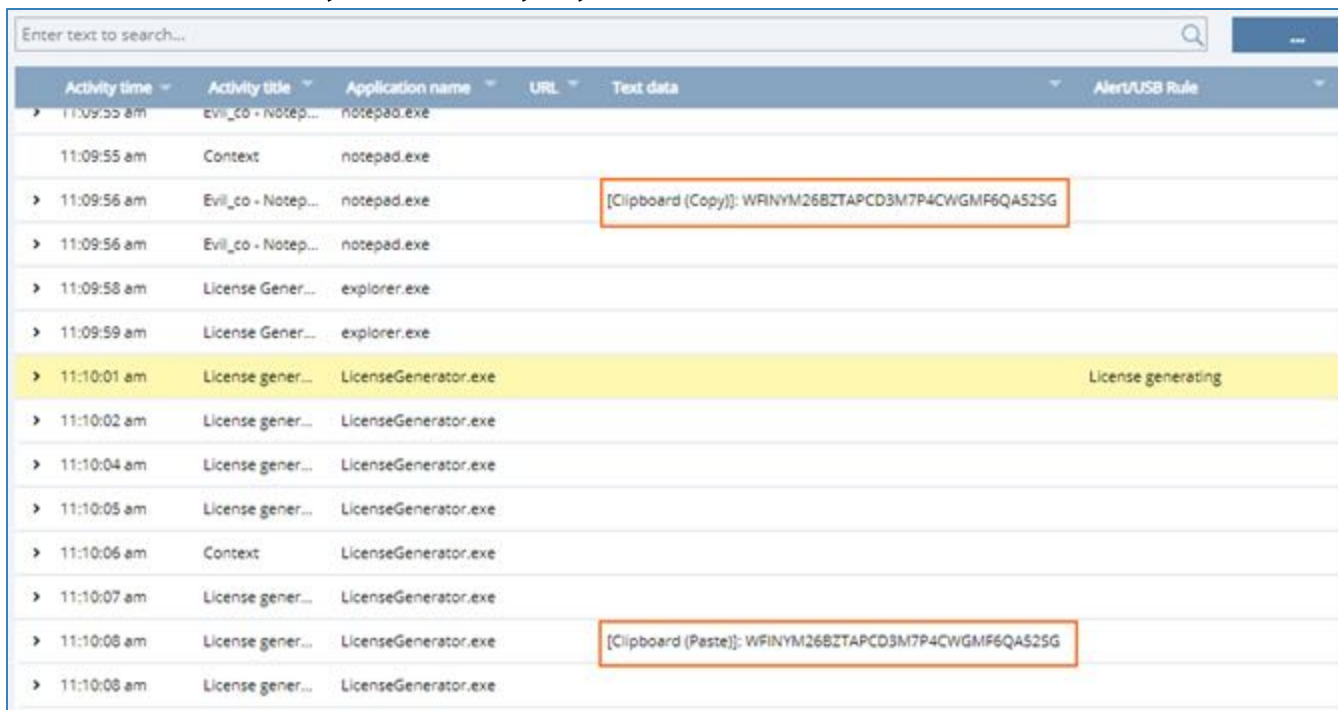


Ekran Client może zostać skonfigurowany tak, aby rozpocząć monitorowanie i tworzenie zrzutów ekranu dopiero po wykryciu zdefiniowanych słów kluczowych wprowadzonych przez użytkownika w określonych aplikacjach.

The screenshot displays the 'CLIENT SETTINGS' interface, specifically the 'KEYSTROKE MONITORING' tab. The interface includes a navigation bar with tabs: CLIENT SETTINGS, CLIENT GROUPS, PERMISSIONS, and ASSIGNED ALERTS. Below the navigation bar, there is a message: 'Change the Settings type to Custom to edit the Client'. The main content area is divided into two sections: 'Monitoring parameters' and 'Keystrokes Filtering'. In the 'Monitoring parameters' section, there are two checkboxes: 'Enable keystroke logging' (checked) and 'Start monitoring after detecting one of the following keywords:' (checked). Below the second checkbox is a text input field containing 'send cv'. In the 'Keystrokes Filtering' section, there is a 'Filter state' dropdown menu with the option 'Monitor keystrokes only in defined applications'. Below this, there are two text input fields: 'APPLICATION NAME CONTAINS' with the value 'Skype; Outlook' and 'ACTIVE WINDOW TITLE CONTAINS' which is empty.

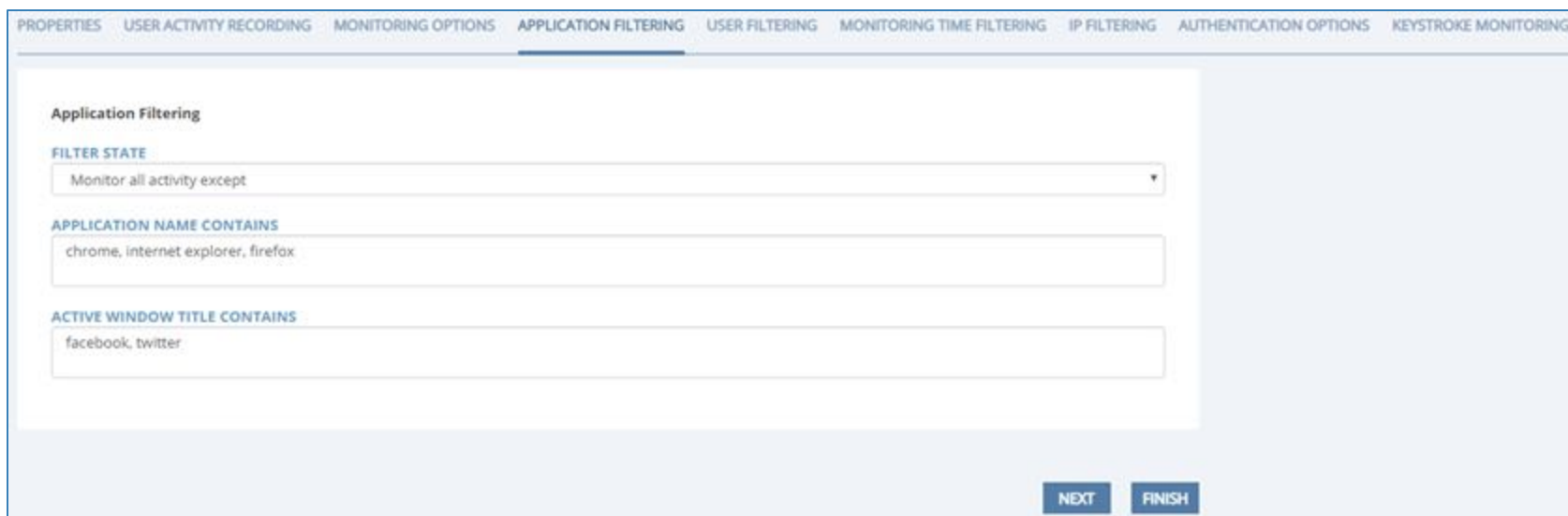
Ekran Client **przechwytuje wszystkie dane tekstowe**, które zostały **skopiowane lub wycięte**, a następnie **wklejone** do dokumentów, plików, aplikacji, paska adresu przeglądarki itp. na komputerach z aplikacją Ekran Client.

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



Activity time	Activity title	Application name	URL	Text data	Alert/USB Rule
11:09:55 am	Evil_co - Notep...	notepad.exe			
11:09:55 am	Context	notepad.exe			
11:09:56 am	Evil_co - Notep...	notepad.exe		[Clipboard (Copy)]: WRINYM26BZTAPCD3M7P4CWGMF6QA525G	
11:09:56 am	Evil_co - Notep...	notepad.exe			
11:09:58 am	License Gener...	explorer.exe			
11:09:59 am	License Gener...	explorer.exe			
11:10:01 am	License gener...	LicenseGenerator.exe			License generating
11:10:02 am	License gener...	LicenseGenerator.exe			
11:10:04 am	License gener...	LicenseGenerator.exe			
11:10:05 am	License gener...	LicenseGenerator.exe			
11:10:06 am	Context	LicenseGenerator.exe			
11:10:07 am	License gener...	LicenseGenerator.exe			
11:10:08 am	License gener...	LicenseGenerator.exe		[Clipboard (Paste)]: WFINYM26BZTAPCD3M7P4CWGMF6QA525G	
11:10:08 am	License gener...	LicenseGenerator.exe			

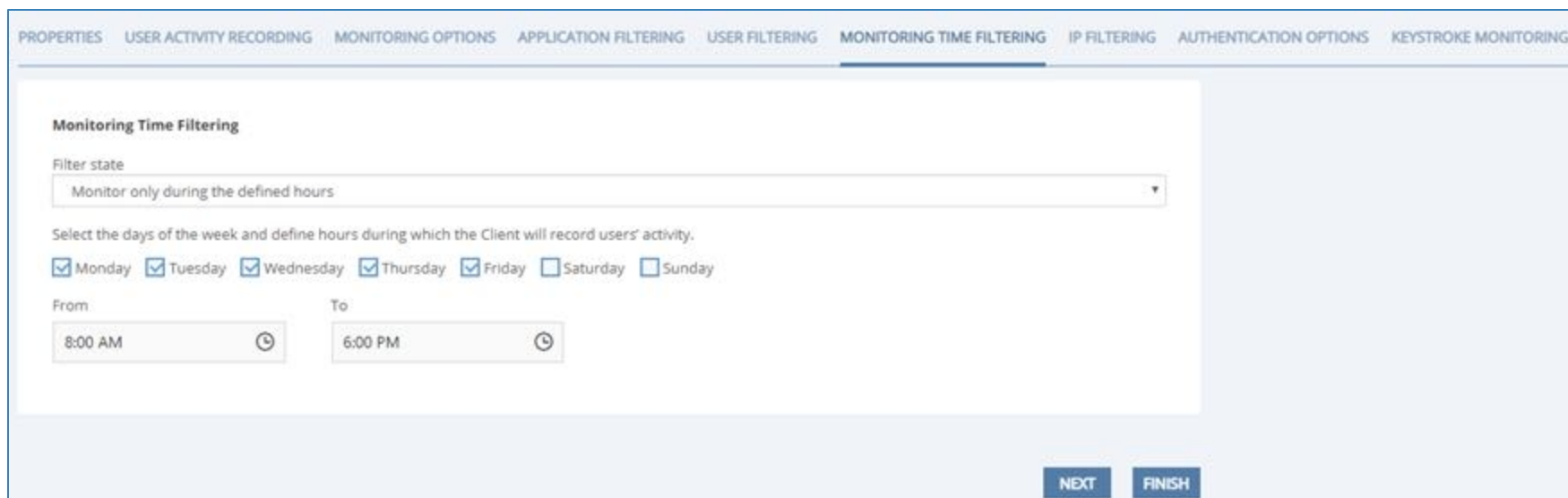
Ekran Client umożliwia zdefiniowanie zasad filtrowania stron internetowych/aplikacji w celu dostosowania ilości monitorowanych danych oraz wyłączenia obszarów, w których można obserwować informacje prywatne. Ma to pozwolić na zachowanie zgodności z zasadami polityki korporacyjnej i przepisami krajowymi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



The screenshot shows the 'APPLICATION FILTERING' tab in the Ekran Client configuration window. The window has a light blue header with several tabs: PROPERTIES, USER ACTIVITY RECORDING, MONITORING OPTIONS, APPLICATION FILTERING (selected), USER FILTERING, MONITORING TIME FILTERING, IP FILTERING, AUTHENTICATION OPTIONS, and KEYSTROKE MONITORING. The main content area is titled 'Application Filtering' and contains three sections: 'FILTER STATE' with a dropdown menu set to 'Monitor all activity except', 'APPLICATION NAME CONTAINS' with a text input field containing 'chrome, internet explorer, firefox', and 'ACTIVE WINDOW TITLE CONTAINS' with a text input field containing 'facebook, twitter'. At the bottom right, there are two buttons: 'NEXT' and 'FINISH'.

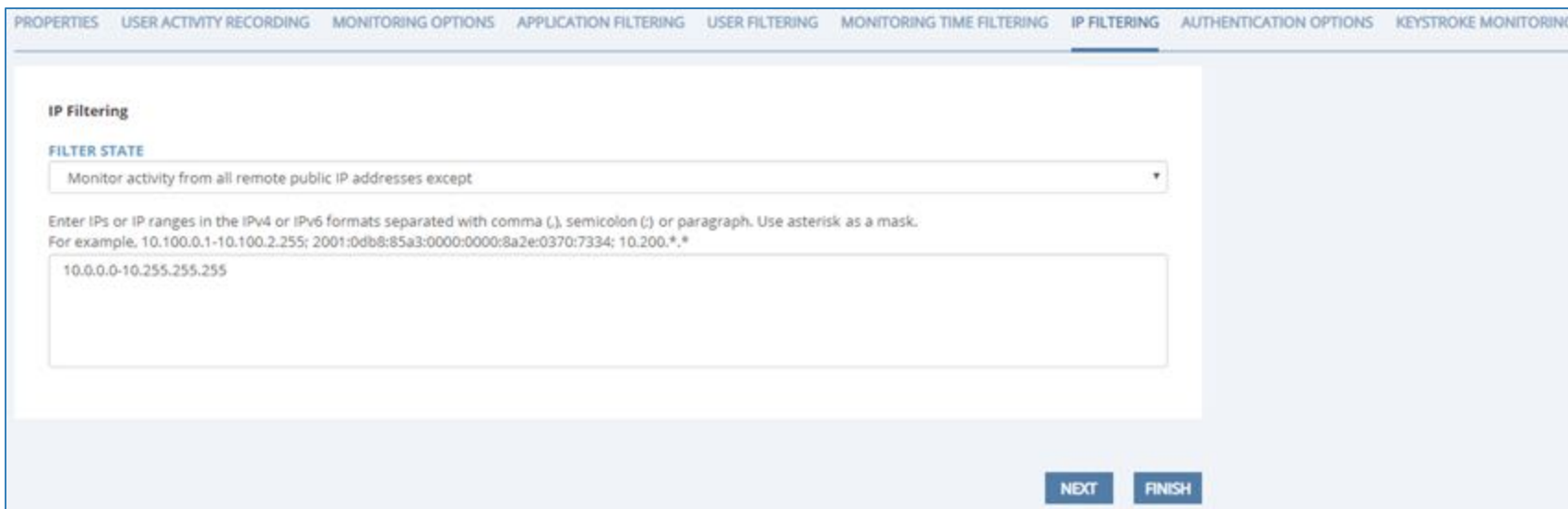
Oprócz reguł filtrowania aplikacji można zdefiniować **reguły monitorowania czasu** filtrowania.

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



The screenshot shows the 'Monitoring Time Filtering' configuration window. At the top, there is a navigation bar with tabs: PROPERTIES, USER ACTIVITY RECORDING, MONITORING OPTIONS, APPLICATION FILTERING, USER FILTERING, MONITORING TIME FILTERING (selected), IP FILTERING, AUTHENTICATION OPTIONS, and KEYSTROKE MONITORING. The main content area is titled 'Monitoring Time Filtering'. It includes a 'Filter state' dropdown menu set to 'Monitor only during the defined hours'. Below this, a text label reads 'Select the days of the week and define hours during which the Client will record users' activity.' There are checkboxes for each day of the week: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. Monday through Friday are checked. Below the checkboxes, there are 'From' and 'To' time selection fields. The 'From' field is set to '8:00 AM' and the 'To' field is set to '6:00 PM'. At the bottom right, there are 'NEXT' and 'FINISH' buttons.

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



The screenshot shows the 'IP FILTERING' tab in a software configuration window. The interface includes a navigation bar at the top with tabs: PROPERTIES, USER ACTIVITY RECORDING, MONITORING OPTIONS, APPLICATION FILTERING, USER FILTERING, MONITORING TIME FILTERING, IP FILTERING (selected), AUTHENTICATION OPTIONS, and KEYSTROKE MONITORING. Below the navigation bar, the 'IP Filtering' section is active. It features a 'FILTER STATE' dropdown menu currently set to 'Monitor activity from all remote public IP addresses except'. Below this, there is instructional text: 'Enter IPs or IP ranges in the IPv4 or IPv6 formats separated with comma (,), semicolon (;) or paragraph. Use asterisk as a mask. For example, 10.100.0.1-10.100.2.255; 2001:0db8:85a3:0000:0000:8a2e:0370:7334; 10.200.*.*'. A text input field below contains the example range '10.0.0.0-10.255.255.255'. At the bottom right of the configuration area are two buttons: 'NEXT' and 'FINISH'.

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

[CLIENT SETTINGS](#) [CLIENT GROUPS](#) [PERMISSIONS](#) [ASSIGNED ALERTS](#)

Change the Settings type to Custom to edit the Client

[PROPERTIES](#) [USER ACTIVITY RECORDING](#) [MONITORING \[WINDOWS/MACOS\]](#) [APPLICATION FILTERING](#) [USER FILTERING](#) [MONITORING TIME FILTERING](#) [IP FILTERING](#)

Monitoring parameters

- ☒ Enable clipboard monitoring
- ☒ Enable SWIFT username monitoring
- ☒ Detect system IDLE event
- ☒ Register IDLE event when user is inactive

Timeout (min)

Monitorowanie aktywności użytkowników logujących się w ramach uprzywilejowanych kont użytkowników.

EDITING CLIENT *alice-pc*?✕

CLIENT SETTINGS CLIENT GROUPS PERMISSIONS ASSIGNED ALERTS

Change the Settings type to Custom to edit the Client.

PROPERTIES USER ACTIVITY RECORDING MONITORING OPTIONS APPLICATION FILTERING **USER FILTERING** MONITORING TIME FILTERING IP FILTERING AUTHENTICATION OPTIONS KEYSTROKE MONITORING

User Filtering

FILTER STATE

Monitor only activity of selected users ▾

Enter user names manually or click Add Users to select users from the list. Please note, when adding users via Add Users, make sure that primary and secondary user names are written without brackets and separated with a semicolon (user1; user2).
Please note, user names must be entered as <domain name>\<user name> and separated with comma (,), semicolon (;) or paragraph. Use asterisk (*) as a name/domain mask (for example, *administrator or *admin*).

+ Add Users ▾

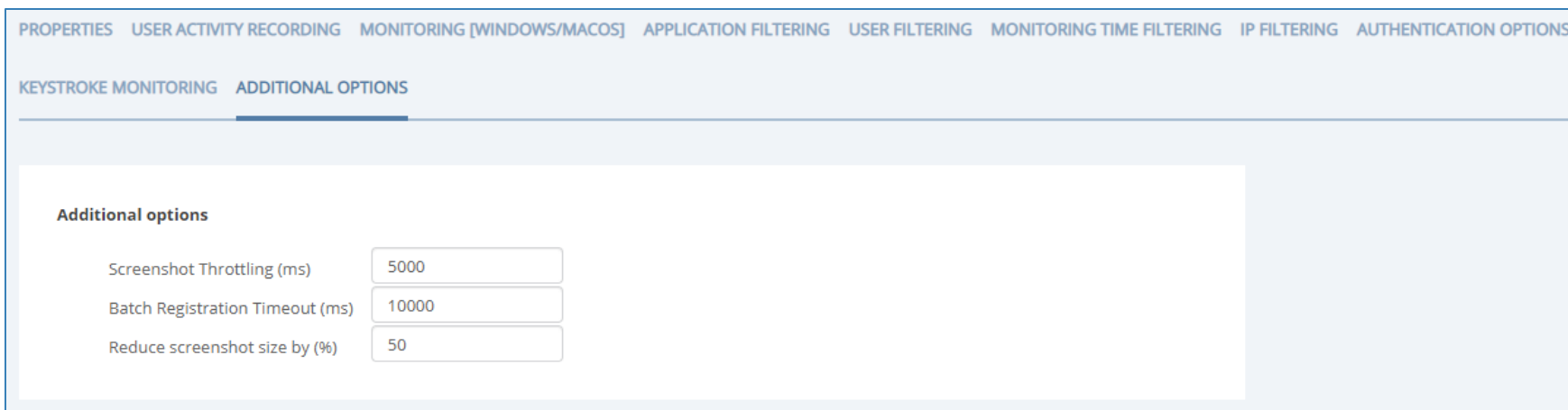
admin, mydomain\privileged_user

NEXT FINISH

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



The screenshot displays the configuration interface of the Ekran System. At the top, a horizontal menu contains several tabs: 'PROPERTIES', 'USER ACTIVITY RECORDING', 'MONITORING [WINDOWS/MACOS]', 'APPLICATION FILTERING', 'USER FILTERING', 'MONITORING TIME FILTERING', 'IP FILTERING', and 'AUTHENTICATION OPTIONS'. Below this menu, the 'KEYSTROKE MONITORING' section is active, and within it, the 'ADDITIONAL OPTIONS' sub-tab is selected. The main content area is titled 'Additional options' and contains three configuration items, each with a label and a text input field:

Parameter	Value
Screenshot Throttling (ms)	5000
Batch Registration Timeout (ms)	10000
Reduce screenshot size by (%)	50

Ustawienie grup Ekran Client



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

EDITING CLIENT Comp15

CLIENT SETTINGS · CLIENT GROUPS · PERMISSIONS · ASSIGNED ALERTS

Change the Settings type to Custom to edit the Client

PROPERTIES · USER ACTIVITY RECORDING · MONITORING OPTIONS · APPLICATION FILTERING · USER FILTERING · MONITORING TIME FILTERING · IP FILTERING · AUTHENTICATION OPTIONS · KEYSTROKE MONITORING

Client Properties

DESCRIPTION

ASSIGNED LICENSE

Workstation license

SETTINGS TYPE

Custom

Custom

Inherited from All Clients

Inherited from Fraud Activity

Inherited from Data Leakage

Inherited from Windows Workstations

Client mode

☐ Enable protected mode

☒ Update Client automatically

☐ Display Client tray icon

☐ Enable jump server mode

☒ Notify if the Client is offline for more than 10 minutes

SEND EMAIL NOTIFICATION TO

abc_company@gmail.com

DELETE CLIENT

FINISH

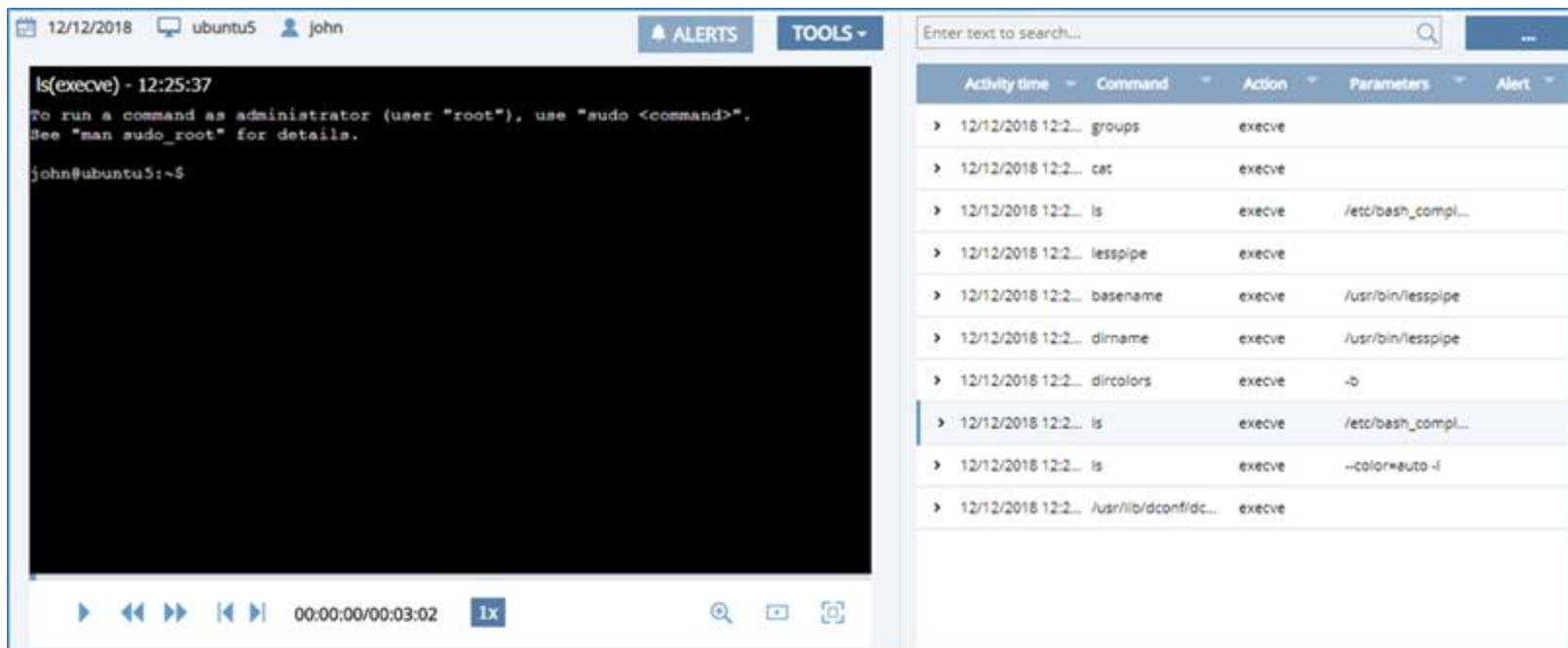
NEXT

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**.

Zdalna sesja Linux Client zawiera:

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



The screenshot displays a remote session interface for a Linux client. The top bar shows the date '12/12/2018', the system 'ubuntu5', and the user 'john'. There are buttons for 'ALERTS' and 'TOOLS'. A search bar is present on the right. The main area is split into two panes. The left pane shows a terminal window with the following content:

```
ls(execve) - 12:25:37
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

john@ubuntu5:~$
```

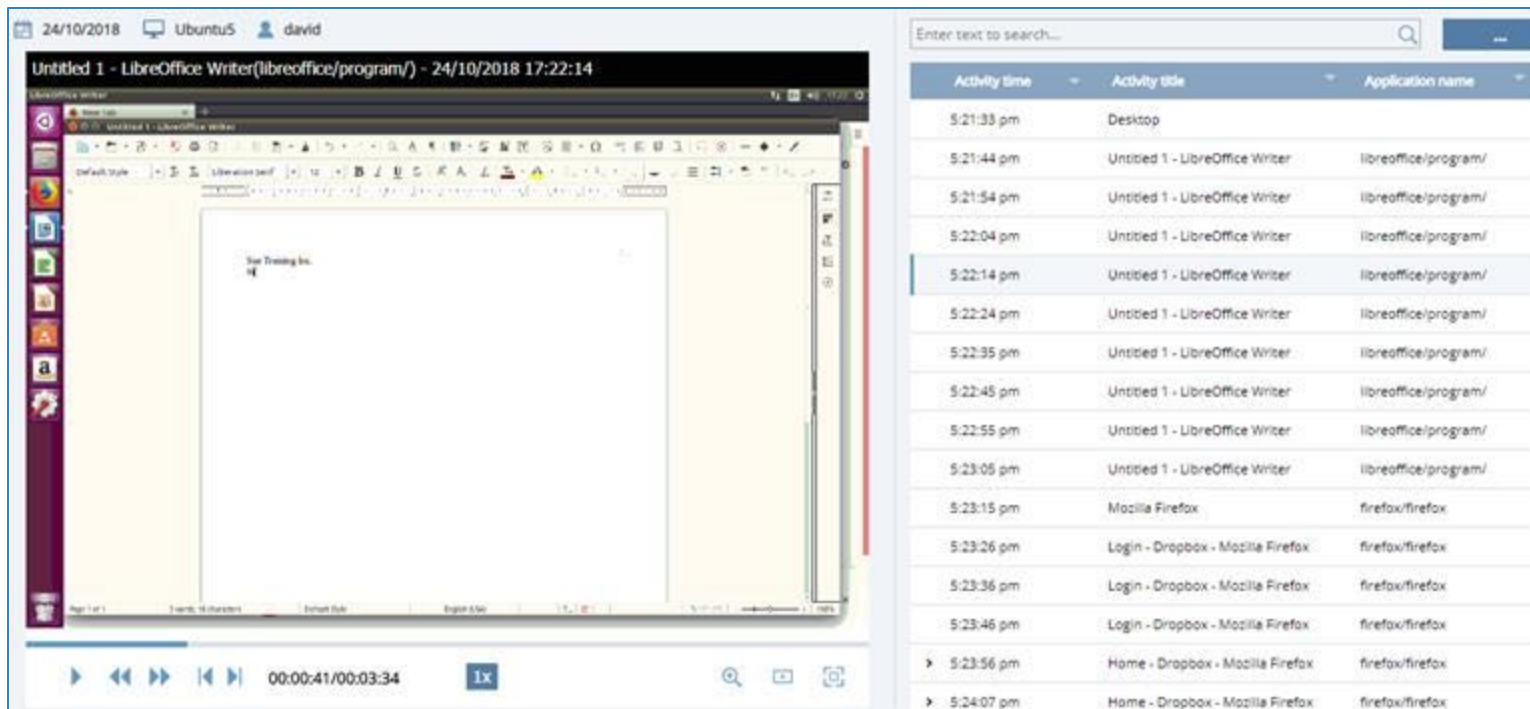
The right pane displays a table of activities:

Activity time	Command	Action	Parameters	Alert
12/12/2018 12:2...	groups	execve		
12/12/2018 12:2...	cat	execve		
12/12/2018 12:2...	ls	execve	/etc/bash_compl...	
12/12/2018 12:2...	lesspipe	execve		
12/12/2018 12:2...	basename	execve	/usr/bin/lesspipe	
12/12/2018 12:2...	dirname	execve	/usr/bin/lesspipe	
12/12/2018 12:2...	dircolors	execve	-b	
12/12/2018 12:2...	ls	execve	/etc/bash_compl...	
12/12/2018 12:2...	ls	execve	--color=auto -l	
12/12/2018 12:2...	/usr/lib/dconf/dc...	execve		

At the bottom of the interface, there is a playback control bar with a play button, a timeline from '00:00:00/00:03:02', a zoom level of '1x', and icons for search, full screen, and zoom in.

Lokalna sesja Linux na X Window System zawiera:

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



The screenshot displays a Linux desktop environment. On the left, a window titled "Untitled 1 - LibreOffice Writer(libreoffice/program/) - 24/10/2018 17:22:14" is open, showing a blank document with a toolbar and a sidebar. The desktop background is a light blue gradient. On the right, a sidebar contains a search bar and a list of activities. The list has three columns: "Activity time", "Activity title", and "Application name".

Activity time	Activity title	Application name
5:21:33 pm	Desktop	
5:21:44 pm	Untitled 1 - LibreOffice Writer	libreoffice/program/
5:21:54 pm	Untitled 1 - LibreOffice Writer	libreoffice/program/
5:22:04 pm	Untitled 1 - LibreOffice Writer	libreoffice/program/
5:22:14 pm	Untitled 1 - LibreOffice Writer	libreoffice/program/
5:22:24 pm	Untitled 1 - LibreOffice Writer	libreoffice/program/
5:22:35 pm	Untitled 1 - LibreOffice Writer	libreoffice/program/
5:22:45 pm	Untitled 1 - LibreOffice Writer	libreoffice/program/
5:22:55 pm	Untitled 1 - LibreOffice Writer	libreoffice/program/
5:23:05 pm	Untitled 1 - LibreOffice Writer	libreoffice/program/
5:23:15 pm	Mozilla Firefox	firefox/firefox
5:23:26 pm	Login - Dropbox - Mozilla Firefox	firefox/firefox
5:23:36 pm	Login - Dropbox - Mozilla Firefox	firefox/firefox
5:23:46 pm	Login - Dropbox - Mozilla Firefox	firefox/firefox
5:23:56 pm	Home - Dropbox - Mozilla Firefox	firefox/firefox
5:24:07 pm	Home - Dropbox - Mozilla Firefox	firefox/firefox

Offline Client Detection (“lost” Client)

Wykrywanie użytkowników offline

Offline Client Detection (“lost” Client)



Offline Client Detection pomoże Ci w terminowym wykrywaniu użytkowników, którzy przestali przysyłać 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.

☒ Notify if the Client is offline for more than

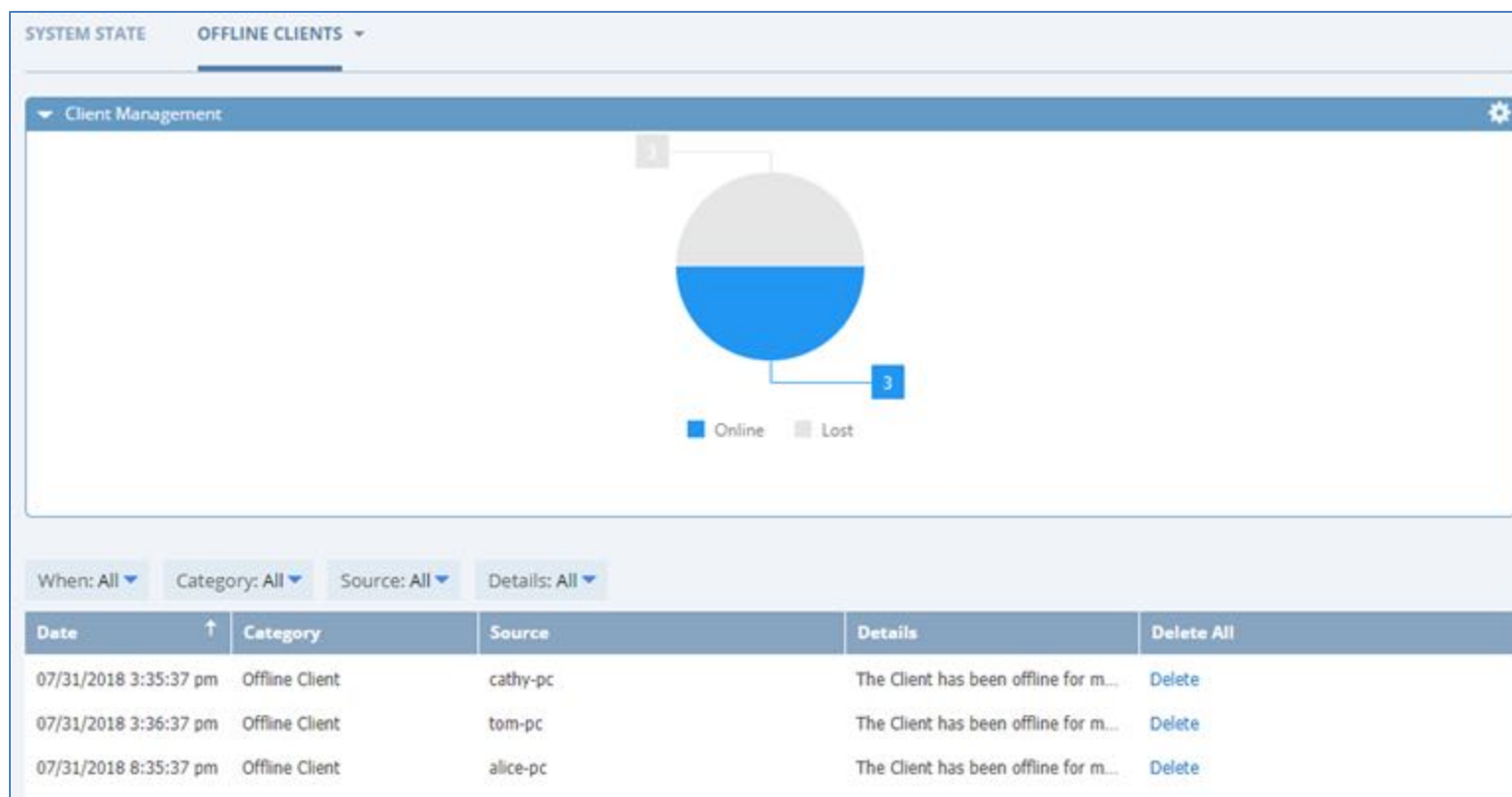
10

minutes

SEND EMAIL NOTIFICATION TO

ABCcompany@company.com

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



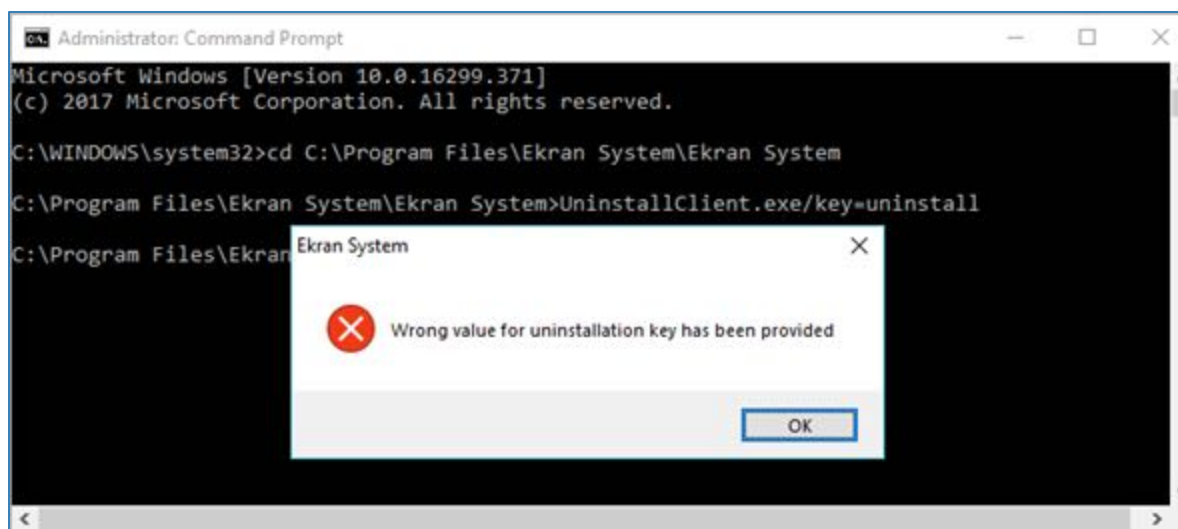
Ochrona Ekran Client

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.

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.

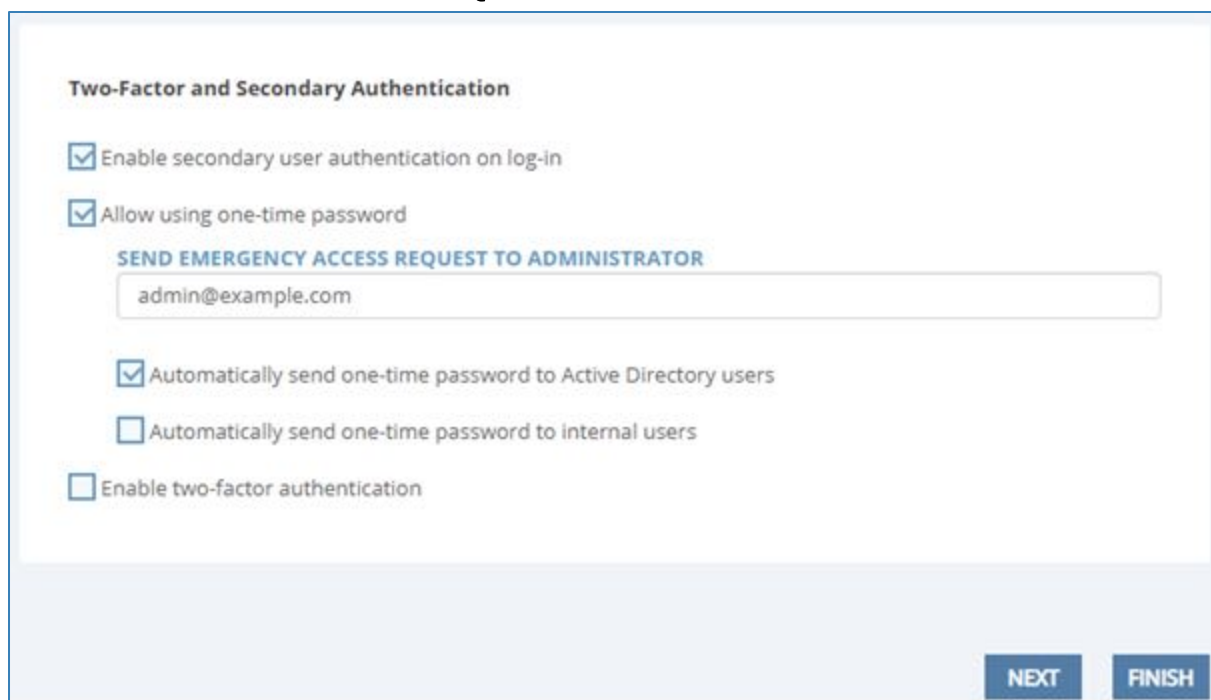


Tylko Administrator Ekran System zna klucz dezinstalacji, ustalony przed instalacją i konieczny do usunięcia lokalnego.

Zaawansowana autoryzacja użytkowników

Zaawansowana autoryzacja użytkowników 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



Two-Factor and Secondary Authentication

☒ Enable secondary user authentication on log-in

☒ Allow using one-time password

SEND EMERGENCY ACCESS REQUEST TO ADMINISTRATOR

☒ Automatically send one-time password to Active Directory users

☐ Automatically send one-time password to internal users

☐ Enable two-factor authentication

NEXT FINISH



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

The screenshot shows a login dialog box for Ekran System. It has a dark blue border and a white background. At the top left is the Ekran System logo. Below it, a message states: "The secondary authentication is required to continue. Please enter the login/password allowed in Ekran System. Contact your System Administrator for more details." There are two input fields: "Login:" with the text "John" and "Password:" with masked characters (dots). At the bottom right are "OK" and "Cancel" buttons. At the bottom center is a "Switch User" button.

Ekran System®

The secondary authentication is required to continue. Please enter the login/password allowed in Ekran System. Contact your System Administrator for more details.

Login: John

Password: ●●●●●●●●

OK Cancel

Switch User

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

One-Time Password Generation

Define a user and then enter a key for two-factor authentication manually or click Auto-Generate. The key must be at least 16 characters long and can contain only the following symbols: A-Z, a-z, 2-7.

CLIENT NAME

SecureServer

USER NAME

guest

USER'S CONFIRMATION EMAIL

tom.jeffry@starcompany.com

COMMENT

This is a password for Tom Jeffry, Star Company representative. One-day access.

GENERATE

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



REQUEST ONE-TIME PASSWORD

I need emergency access to computer

Please enter your email address for the one-time password to be sent to it.

EMAIL

johnson.kenneth@ntl.net

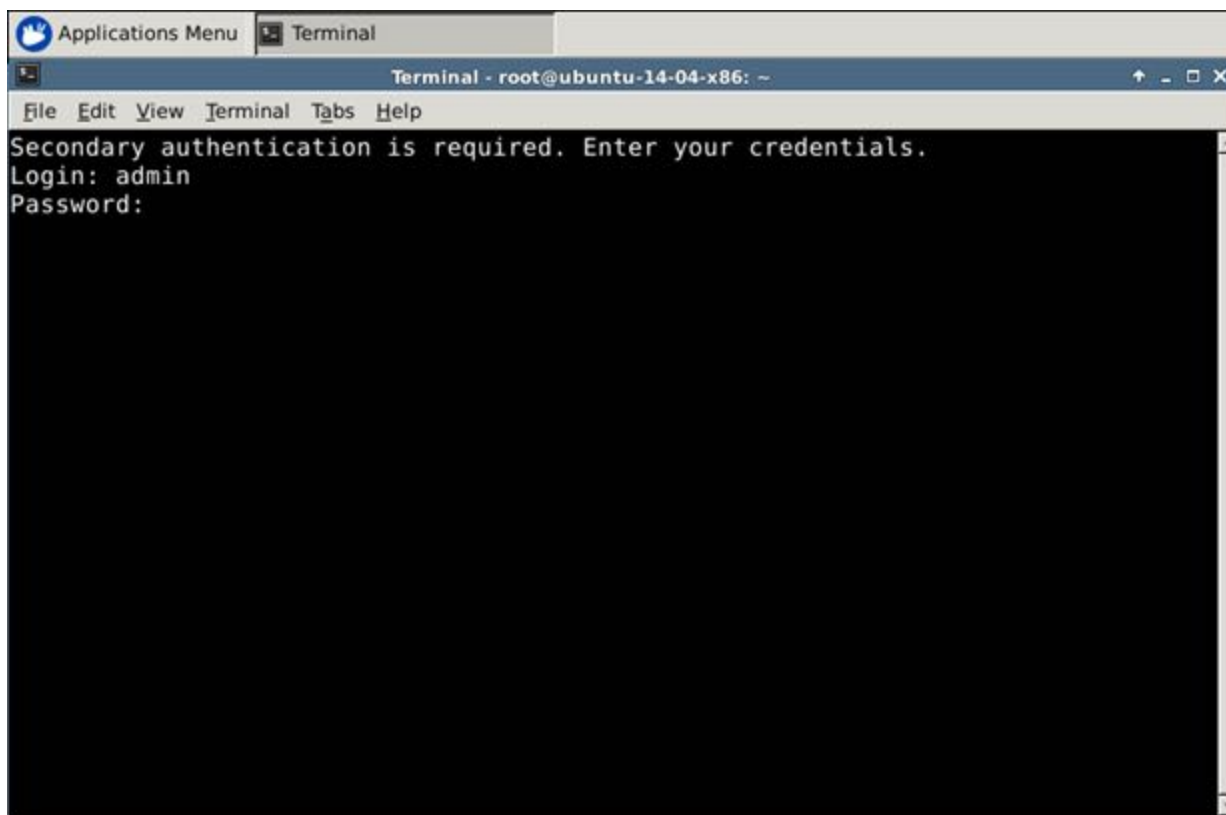
COMMENT

Kenneth Johnson to update the db

Cancel Request



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)

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

Two-Factor and Secondary Authentication

☐ Enable secondary user authentication on log-in

☐ Allow using one-time password

USERS WHO CAN APPROVE ACCESS

☐ Automatically send one-time password to Active Directory users

☐ Automatically send one-time password to internal users

☒ Enable two-factor authentication

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.

Add User

☒ Active Directory user

☐ Local computer user

☐ Ekran System user for secondary authentication

DOMAIN:

ntl.local

USER/USER GROUP:

alice

KEY FOR TWO-FACTOR AUTHENTICATION:

TWFEUYHQHU4EWH3

GENERATE



SAVE

Add User

☐ Active Directory user

☒ Local computer user

☐ Ekran System user for secondary authentication

COMPUTER NAME:

ubuntu

USER LOGIN:

tom

KEY FOR TWO-FACTOR AUTHENTICATION:

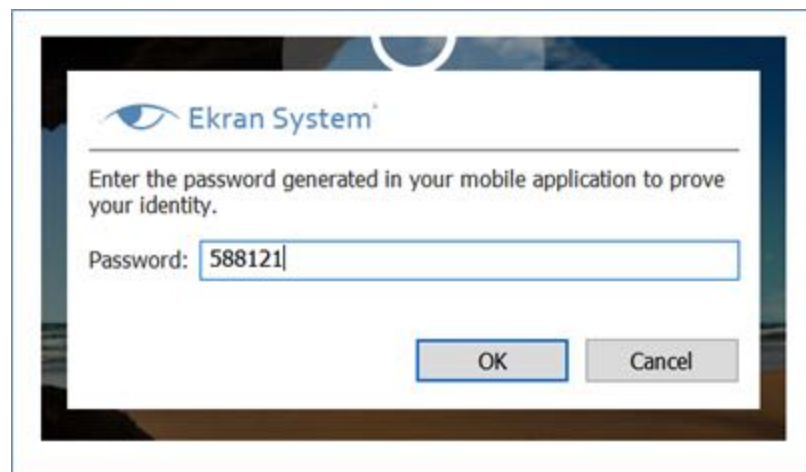
H7D7H7REGSKF5SY4

GENERATE



SAVE

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

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.

Add Secret

Secret properties

Automation

Permission

General

SECRET NAME

EnterpServ1

SECRET TYPE

Active Directory account

DESCRIPTION

Allows access to the server

Account

DOMAIN

nlt.app

LOGIN

guest

PASSWORD

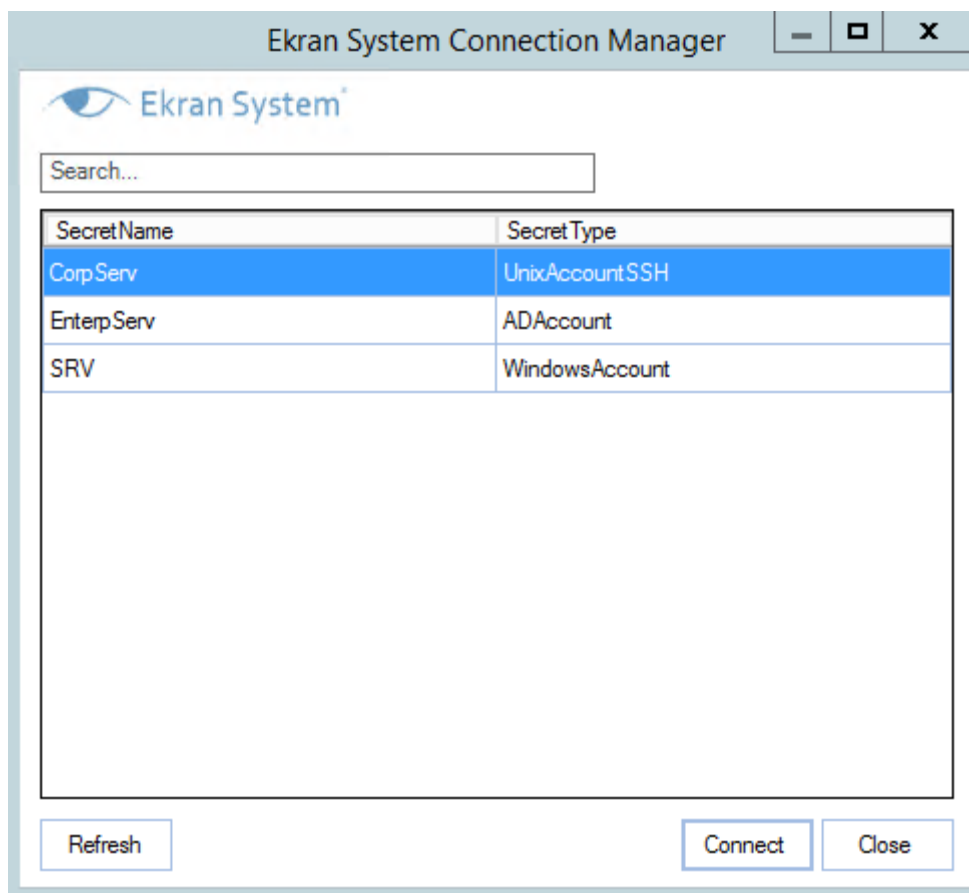
.....

SAVE

Logowanie przez nadanie dostępu (Secret)



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





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.

Password Management

SECRETS

PERMISSIONS

Contains

Access to Secrets is available for PAM users from the Jump Server.
NOTE: To share Secrets with internal users, enable secondary user authentication on the Jump Server ([Client Management](#)).

Secret Name: All Secret Type: All Expiration Date: All

ADD SECRET

	Secret Name	Secret Type	Added By	Description	Delete All
▶	Main Server	Windows account	admin	connection to the Main Server	✕ Delete
▶	Temporary SSH access	Unix account (SSH)	admin	to provide temporary access	✕ Delete
▶	24/7 machine	Windows account	admin	emergency access	✕ Delete

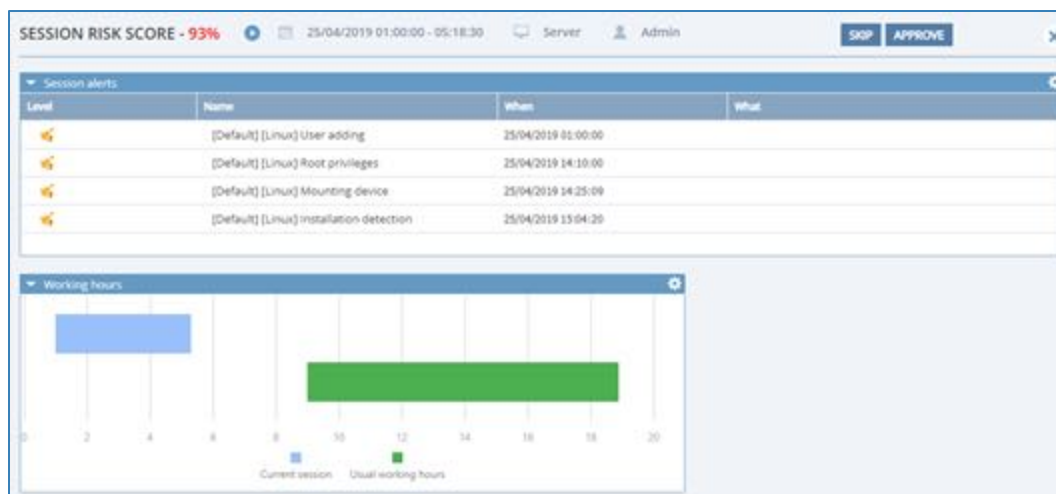
1

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.





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

Properties
☒ Enable rule
NAME

DESCRIPTION

Conditions

Email Notifications
☒ Send notification on the detected anomalies for a finished session
☐ Send instant notification on the detected anomalies
☒ Send total session risk score in case of no anomalies
SEND EMAIL NOTIFICATION TO

Additional Actions
☒ Show warning message to user

☐ Block user in the current session

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.

MONITORING RESULTS

CLIENT SESSIONS

ARCHIVED SESSIONS

Who: All

Where: All

When: All

+ More criteria

COLUMNS DISPLAY +

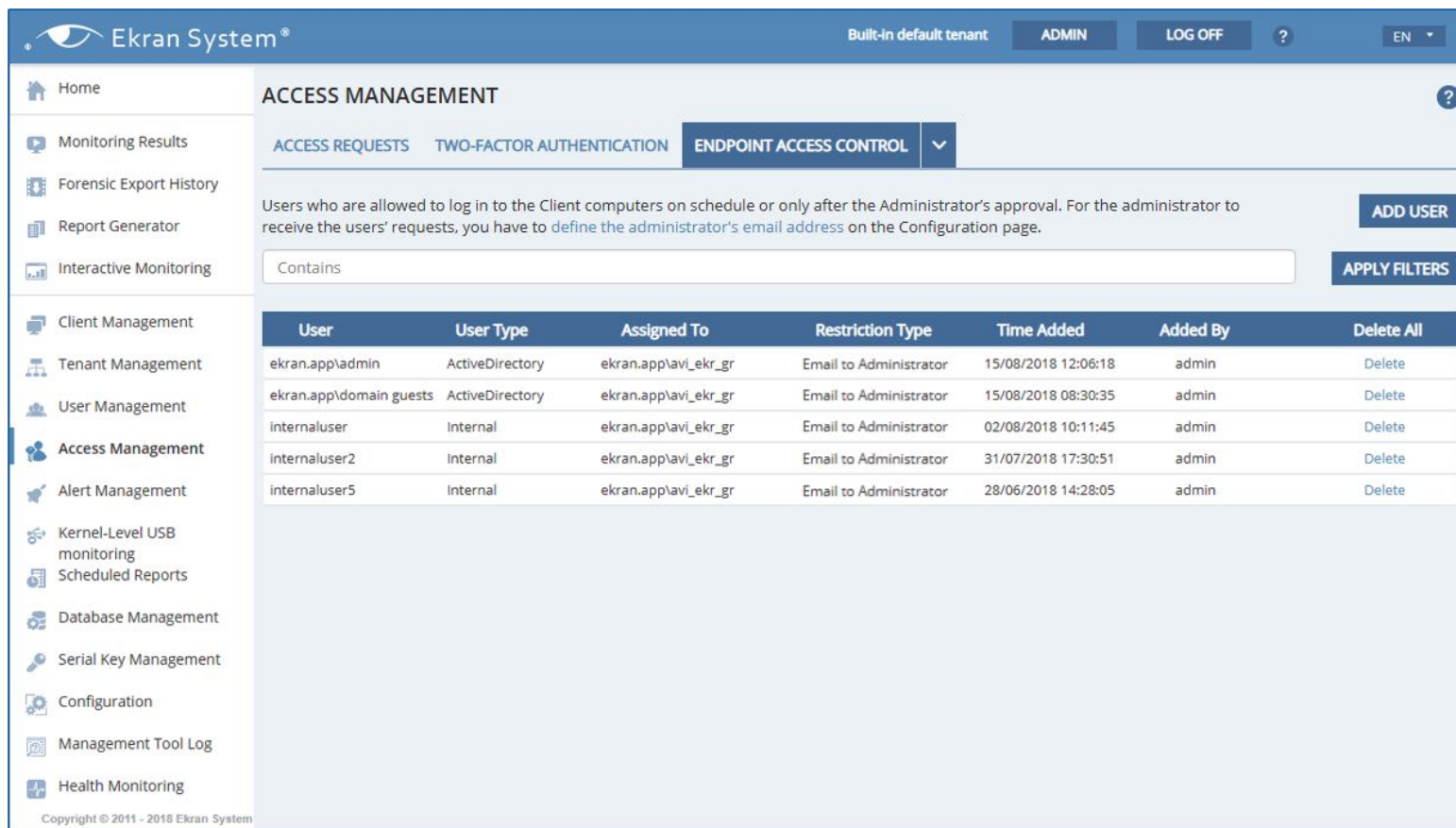
What

...

Risk ...	Alerts	User Name	Client Name	Start	Finish	Duration	IPv4	Remote Pu...	Remote Hos...
30%		david	 Ubuntu5	10/25/2018	3:25 am	3 min 35 sec	10.100.6.36		
82%		EKRAN\admin	 srv-app	07/19/2018	1:19 am	3 min 11 sec	10.100.6.152	10.100.6.151	CLIENT
51%		kyla(internaluser5)	 ubuntu4	07/18/2018	1:37 am	1 min 6 sec			
51%		joe	 ubuntu3	07/17/2018	11:21 pm	1 min 49 sec			
		donna	 ubuntu1	07/17/2018	11:00 pm	4 min 44 sec			
		master	 ubuntu2	07/17/2018	10:08 pm	2 min 16 sec			

Zgoda administratora na logowanie

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



The screenshot displays the Ekran System web interface. The top navigation bar includes the Ekran System logo, a tenant selector (Built-in default tenant), and user controls (ADMIN, LOG OFF, a help icon, and a language dropdown set to EN). A left sidebar contains a menu with items like Home, Monitoring Results, Forensic Export History, Report Generator, Interactive Monitoring, Client Management, Tenant Management, User Management, Access Management (highlighted), Alert Management, Kernel-Level USB monitoring, Scheduled Reports, Database Management, Serial Key Management, Configuration, Management Tool Log, and Health Monitoring.

The main content area is titled "ACCESS MANAGEMENT" and features three tabs: "ACCESS REQUESTS", "TWO-FACTOR AUTHENTICATION", and "ENDPOINT ACCESS CONTROL" (which is active). Below the tabs, a text block explains that users allowed to log in require administrator approval, with a link to the Configuration page for defining the administrator's email address. To the right of this text are "ADD USER" and "APPLY FILTERS" buttons. A search bar labeled "Contains" is positioned above a table.

User	User Type	Assigned To	Restriction Type	Time Added	Added By	Delete All
ekran.app\ladmin	ActiveDirectory	ekran.app\lavi_ekr_gr	Email to Administrator	15/08/2018 12:06:18	admin	Delete
ekran.app\domain guests	ActiveDirectory	ekran.app\lavi_ekr_gr	Email to Administrator	15/08/2018 08:30:35	admin	Delete
internaluser	Internal	ekran.app\lavi_ekr_gr	Email to Administrator	02/08/2018 10:11:45	admin	Delete
internaluser2	Internal	ekran.app\lavi_ekr_gr	Email to Administrator	31/07/2018 17:30:51	admin	Delete
internaluser5	Internal	ekran.app\lavi_ekr_gr	Email to Administrator	28/06/2018 14:28:05	admin	Delete

Copyright © 2011 - 2018 Ekran System

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

Add User

General

Restriction Types



User with Restricted Access Rights

USER TYPE:

Local computer user

COMPUTER NAME:

Comp1

USER LOGIN

John Dean



Users Who Can Approve Access

USER/USER GROUP:

ADMINISTRATORS

SAVE

Add User

General

Restriction Types



Restriction Type

☒ Always require administrator's approval by email on login

☐ Allow access without administrator's approval

Allowed dates

FROM

09/07/2020

TO

09/21/2020

Allowed time

FROM

8:00:00 AM

TO

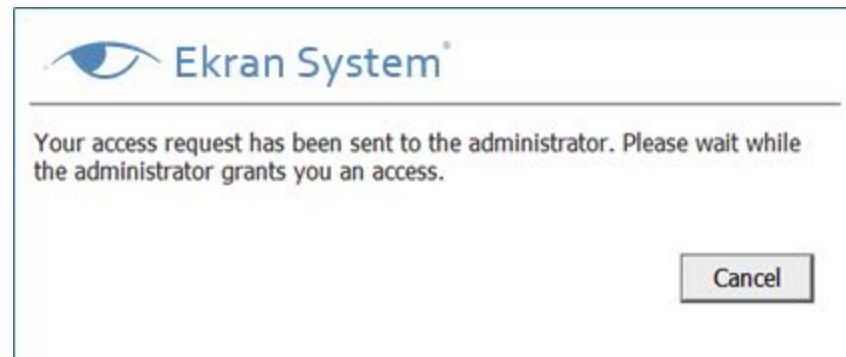
5:00:00 PM

Allowed weekdays

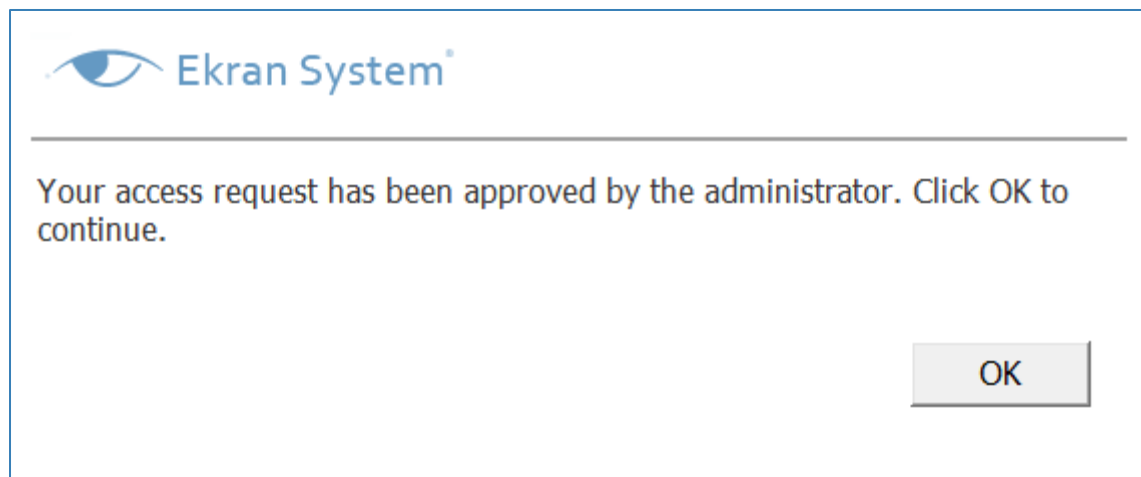
Su Mo Tu We Th Fr Sa

SAVE

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.



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.

Ekran System* Built-in default tenant ADMIN LOG OFF ? EN

ACCESS MANAGEMENT

PRIVILEGED ACCOUNTS TWO-FACTOR AUTHENTICATION ONE-TIME PASSWORDS RESTRICTED USERS

Users who are allowed to log in to the Client computers only after the Administrator's approval. For the administrator to receive the users' requests, you have to define the administrator's email address on the Configuration page.

Contains **ADD USER** **APPLY FILTERS**

User	User Type	Assigned To	Restriction Type	Time Added	Added By	Delete All
admin	Internal	Client group	Access on schedule (22/03/2019 - 05/04/2019, 08:00 - 17:00, Mo)	22/03/2019 11:15:22	admin	Delete
ekran.app\admin	ActiveDirectory	ekran.app\lekr_gr	Access on schedule (22/03/2019 - 05/04/2019, 08:00 - 17:00, Mo, Tu)	22/03/2019 11:11:49	admin	Delete
root	Linux	Any computer	Access on schedule (22/03/2019 - 22/03/2019, 11:00 - 12:00, Fr)	22/03/2019 11:12:26	admin	Delete
comp1\Mattibsen	Local	ekran.app\lekr_gr	Access on schedule (22/03/2019 - 23/04/2019, 08:00 - 18:00, Tu, Th, Fr)	22/03/2019 11:10:55	admin	Delete

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.

The 'Add User' dialog box, General tab, shows the following configuration:

- User with Restricted Access Rights:**
 - USER TYPE:** Active Directory user
 - DOMAIN:** nlt.app
 - USER/USER GROUP:** guest
- Accessed Computer with Installed Client:**
 - COMPUTER TYPE:** Computers from Client Group
 - CLIENT GROUP:** Windows Workstations
- Users Who Can Approve Access:**
 - USER/USER GROUP:** ADMINISTRATORS

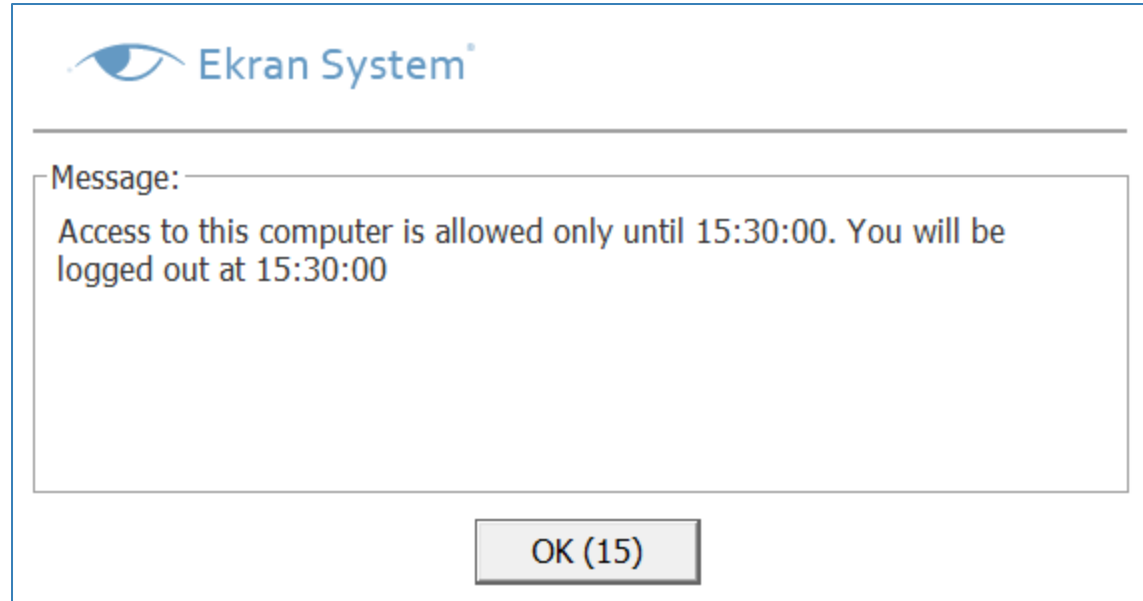
A 'SAVE' button is located at the bottom right.

The 'Add User' dialog box, Restriction Types tab, shows the following configuration:

- Restriction Type:**
 - ☐ Always require administrator's approval by email on login
 - ☒ Allow access without administrator's approval
- Allowed dates:**
 - FROM:** 09/07/2020
 - TO:** 09/21/2020
- Allowed time:**
 - FROM:** 8:00:00 AM
 - TO:** 5:00:00 PM
- Allowed weekdays:** Su, Mo, Tu, We, Th, Fr, Sa

A 'SAVE' button is located at the bottom right.

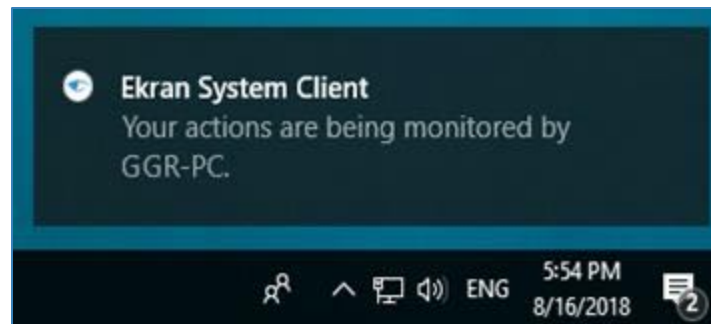
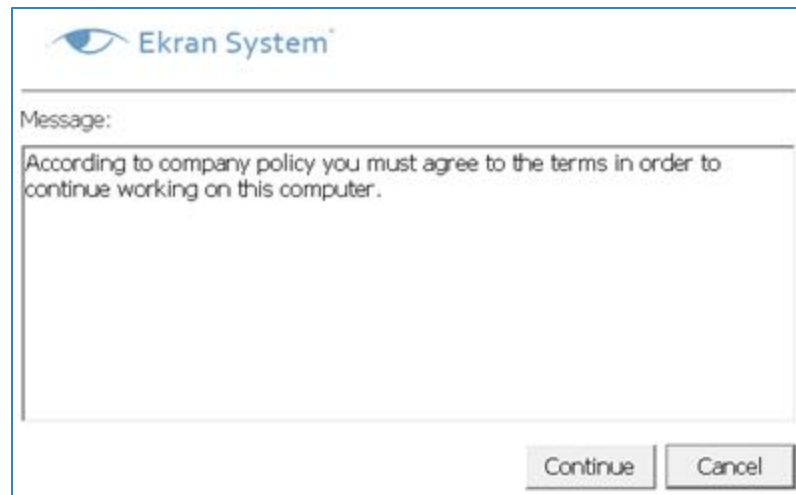
Użytkownicy o ograniczonym dostępie będą mogli zalogować się do komputerów z Ekran Client w określonym czasie i będą potrzebowali zgody administratora na zalogowanie poza tym okresem.



Powiadamianie użytkowników o monitorowaniu

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.





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



Message:

Please enter the following:

- 1) Your first and last name
- 2) The task you are to work on this server machine

Your comment is required:

Michael Cooper
I'm going to update the MS SQL Studio to a new version.

Continue Cancel



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



Message:

Please provide the number of the ticket created for you in the ticketing system and add a comment containing the information on actions you are to perform on this server machine.

Ticket number is required:

52123

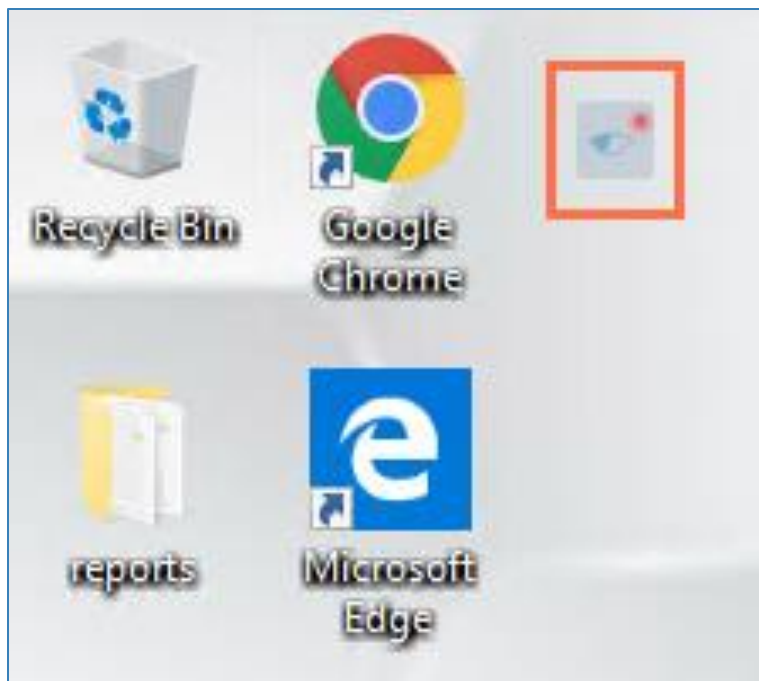
Your comment is required:

I'm going to view the Event Log and restart the system services.

Continue Cancel

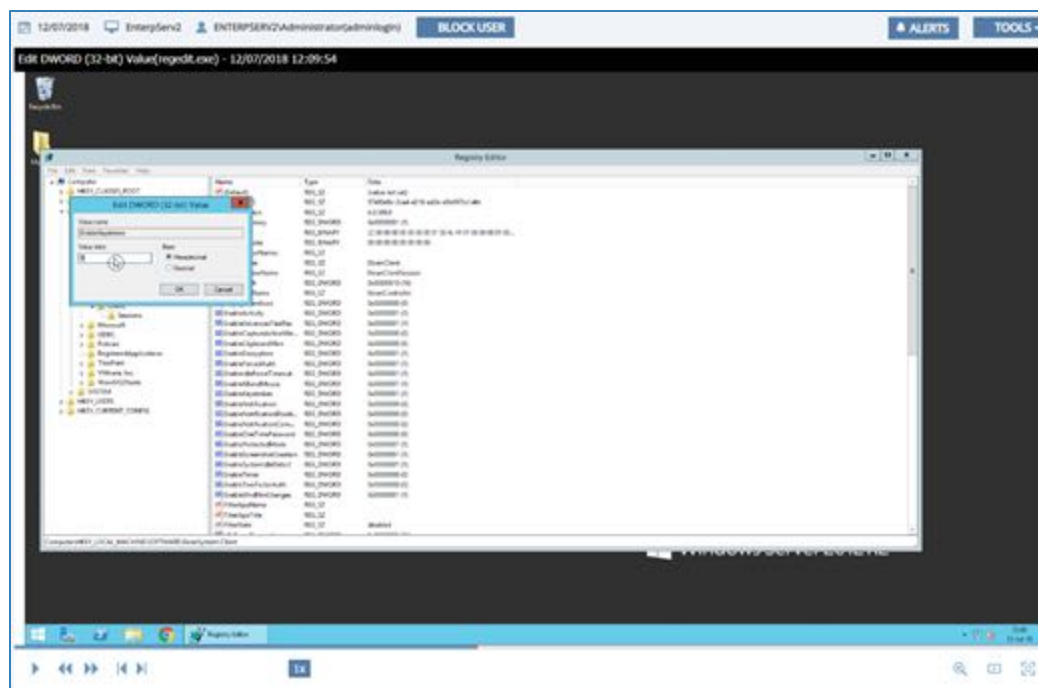


Wyświetlenie **ikony** na pulpicie, która będzie informować użytkowników o tym, że ich praca jest **aktualnie nagrywana**.

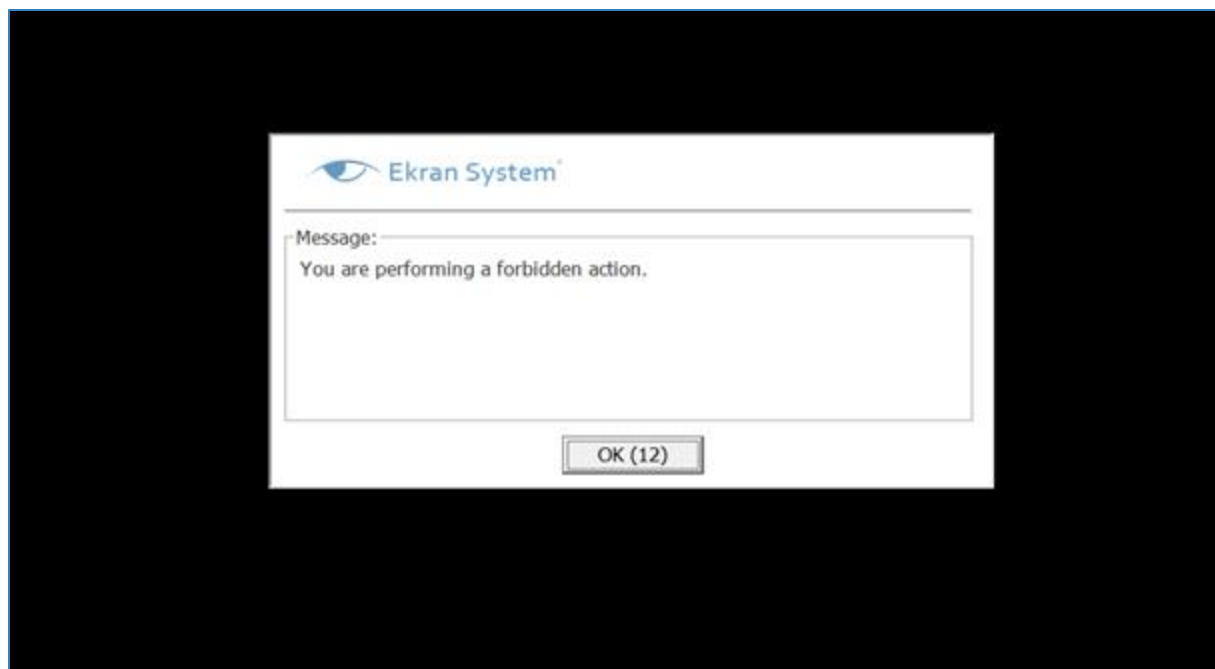


Blokowanie użytkowników

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 wyzwała określone ostrzeżenie.



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

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

BLOCKED USER LIST						
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

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.

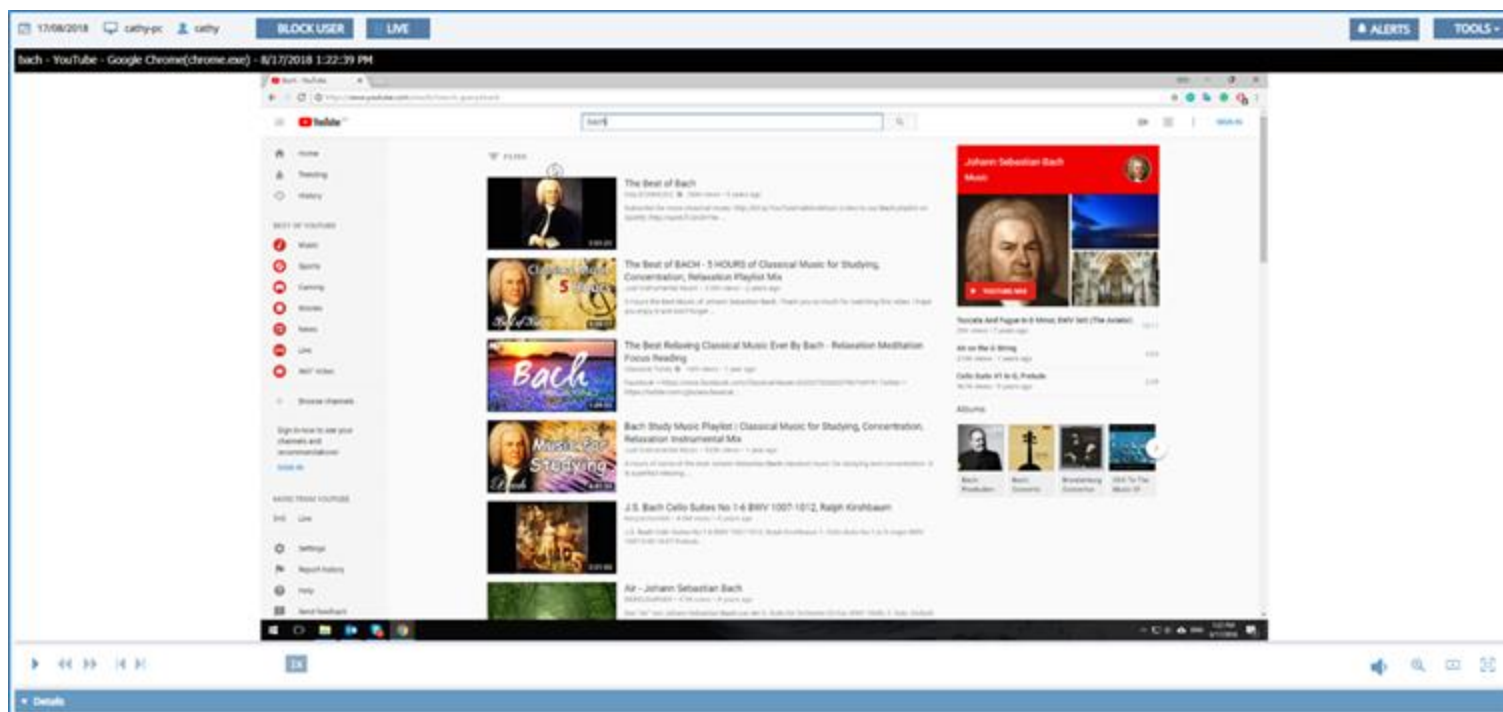
Who: COMP6\TomNessJunior ▾Where: All ▾When: All ▾COLUMNS DISPLAY +What

+ More criteria

Risk ...	Alerts	User Name	Client Name	Start	Finish	Duration	IPv4	Remote Pu...	Remote Host Na...
99%		TomNessJunior	 Comp6	07/07/2018	1:05 am	3 min 56 sec	169.254.248.5		

Ekran System umożliwia **monitorowanie** aktywności użytkowników i **odstuchiwanie 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.

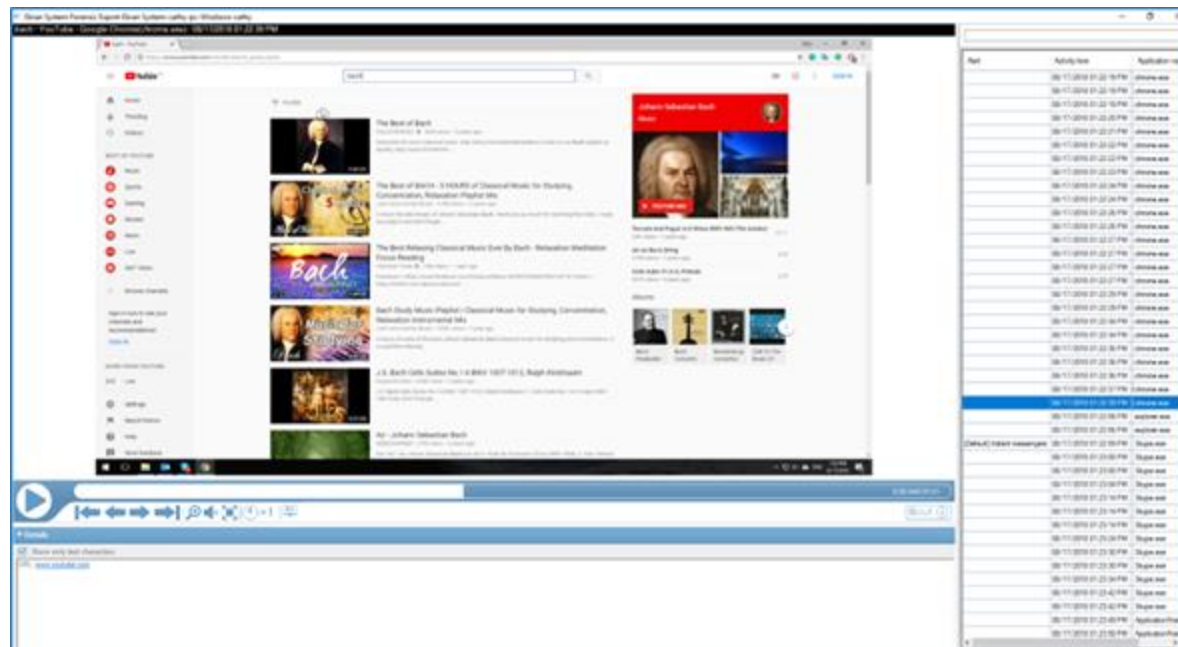


Niektóre części wideo można **powiększyć** w odtwarzaczu sesji za pomocą **lupy**.

The screenshot shows a video player interface with a Windows Registry Editor session. The main window displays the Registry Editor interface with the 'Edit DWORD (32-bit) Value' dialog box open. The dialog box shows the 'Value name' as 'EnableKeyStrokes' and the 'Value data' as '1'. The 'Base' is set to 'Hexadecimal'. The video player interface includes a timeline at the bottom with a list of events, such as 'Edit DWORD (32-bit) Value', 'Error Editing Value', and 'Registry Editor'. The timeline is currently at 12:09:54 pm.

Z Ekran System Forensic Export, możesz:

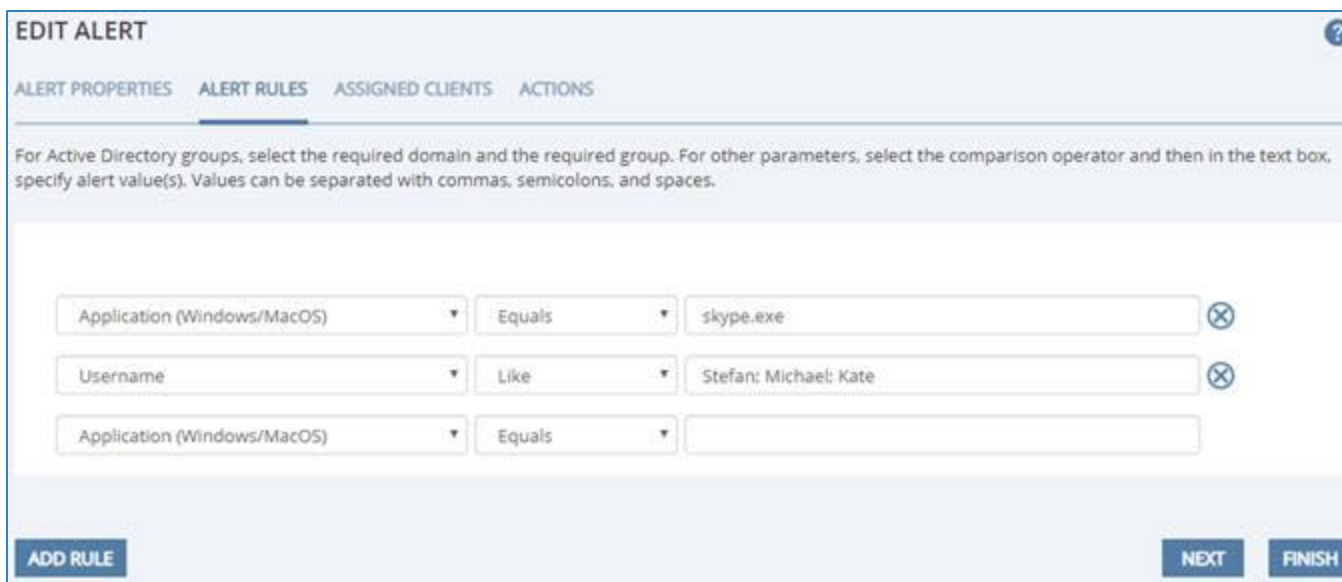
- **Eksportować monitorowaną sesję** lub jej części do bezpiecznie zaszyfowanego pliku.
- **Zbadać zarejestrowaną aktywność** użytkownika i dane audio w wbudowanej przeglądarce sesji offline.
- Przedstawić stronom trzecim **niepodważalne dowody** w formacie nieedytowalnym.



Zdarzenia alarmowe (Alerty)

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.



EDIT ALERT

ALERT PROPERTIES ALERT RULES ASSIGNED CLIENTS ACTIONS

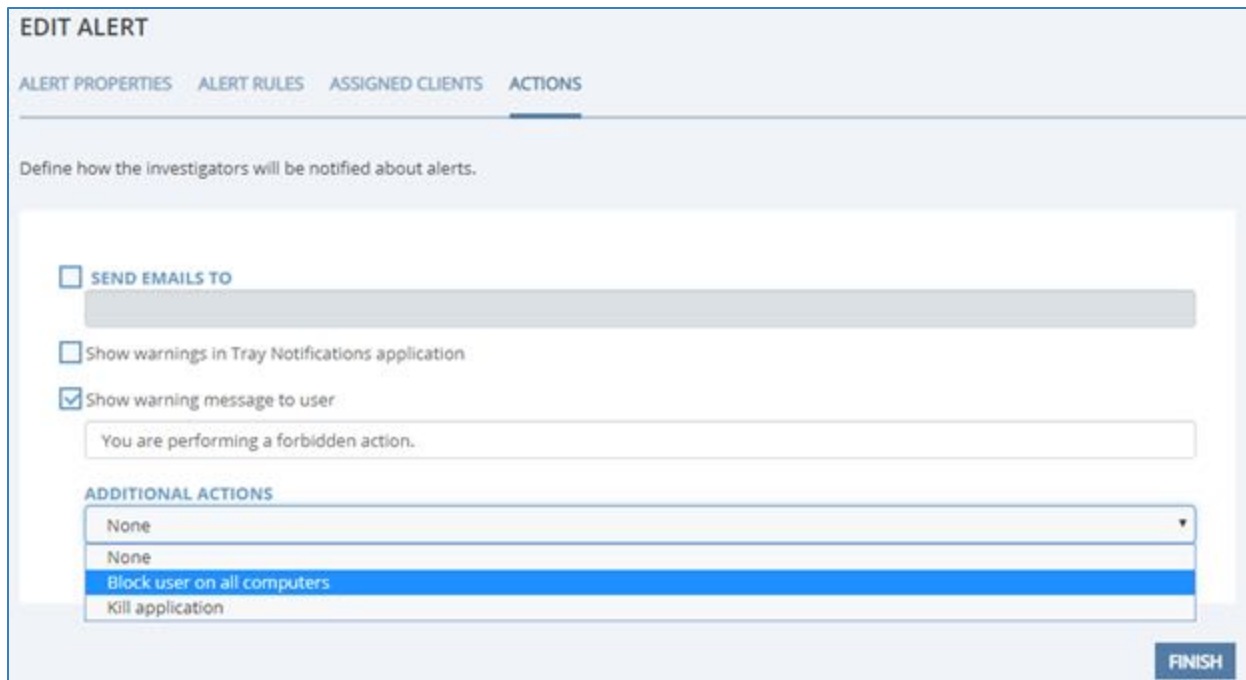
For Active Directory groups, select the required domain and the required group. For other parameters, select the comparison operator and then in the text box, specify alert value(s). Values can be separated with commas, semicolons, and spaces.

Application (Windows/MacOS)	Equals	skype.exe
Username	Like	Stefan; Michael; Kate
Application (Windows/MacOS)	Equals	

ADD RULE NEXT FINISH

Możesz ustawić Alert na:

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



EDIT ALERT

ALERT PROPERTIES | ALERT RULES | ASSIGNED CLIENTS | **ACTIONS**

Define how the investigators will be notified about alerts.

☐ SEND EMAILS TO

☐ Show warnings in Tray Notifications application

☒ Show warning message to user

You are performing a forbidden action.

ADDITIONAL ACTIONS

- None
- None
- Block user on all computers**
- Kill application

FINISH

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

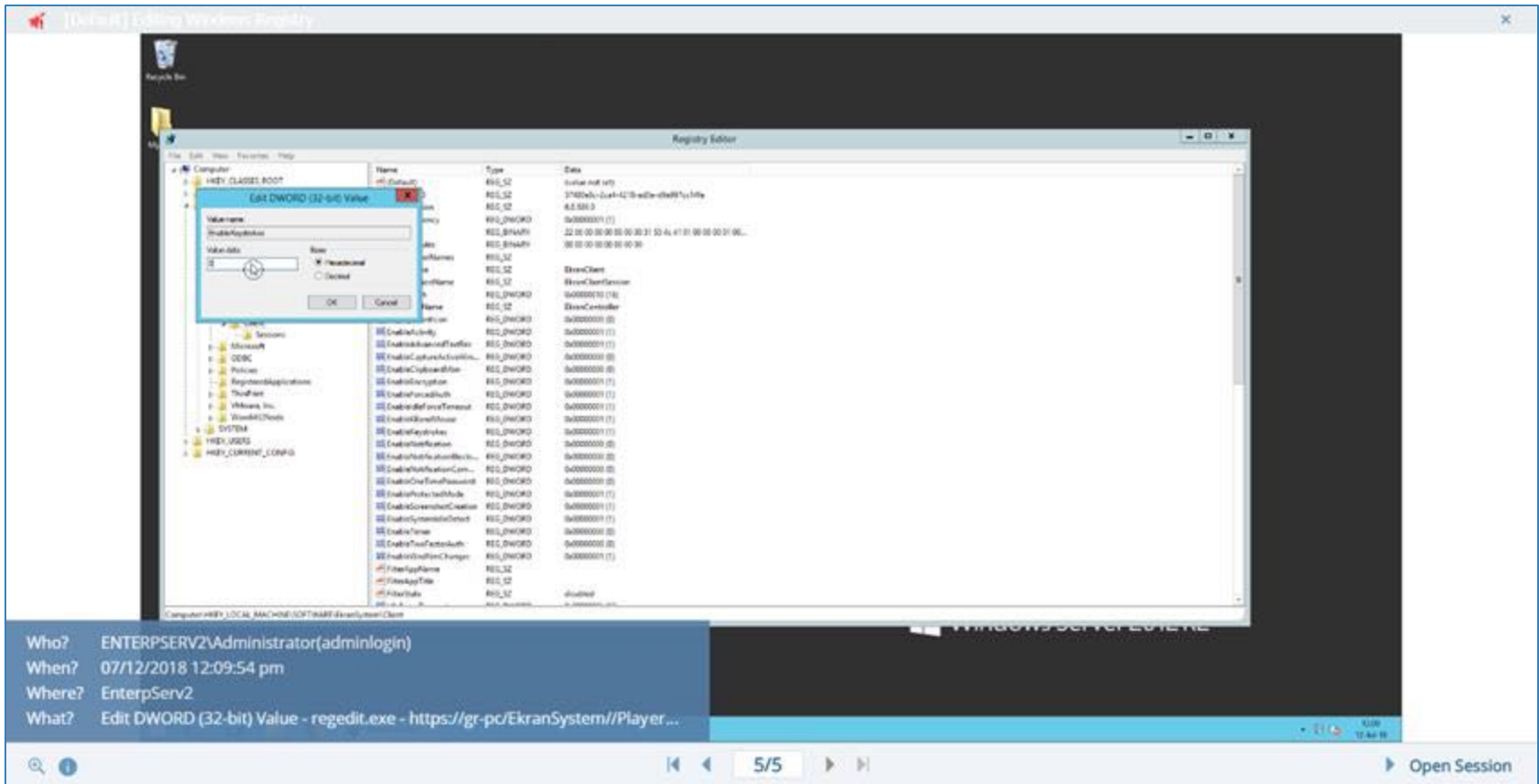
☐	Risk	Name	Description	Assigned To	State	Notification	Email Recipient		
☐		Keystroke monitoring		srv-app	Enabled	None			
☐		[Linux] User login		All Clients; ubunt...	Enabled	None			
☐		(Windows) Installatio...	This is alert on detecting installation e...	Comp16	Enabled	None			
☐		[Default] [Linux] Insta...	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**.

Activity time	Activity title	Application	URL	Alert/URL Rule
8:30:18 am	Relaxing Music Playlist: 25 C...	chrome.exe	www.billboard.com	
8:30:18 am	Relaxing Music Playlist: 25 C...	chrome.exe	dropbox.com	[Default] Cloud storages
8:30:19 am	Relaxing Music Playlist: 25 C...	chrome.exe	dropbox.com	
8:30:21 am	Relaxing Music Playlist: 25 C...	chrome.exe	dropbox.com	
8:30:22 am	Login - Dropbox - Google Ch...	chrome.exe	www.dropbox.com	
8:30:26 am	Login - Dropbox - Google Ch...	chrome.exe	www.dropbox.com	
8:30:28 am		chrome.exe		
8:30:29 am	Login - Dropbox - Google Ch...	chrome.exe	www.dropbox.com	
8:30:31 am	Login - Dropbox - Google Ch...	chrome.exe	www.dropbox.com	
8:30:34 am	Chrome Legacy Window	chrome.exe	www.dropbox.com	
8:30:35 am	Login - Dropbox - Google Ch...	chrome.exe	www.dropbox.com	
8:30:36 am	Dropbox - Google Chrome	chrome.exe	www.dropbox.com	
8:30:41 am	Home - Dropbox - Google Ch...	chrome.exe	www.dropbox.com	
8:30:43 am	Home - Dropbox - Google Ch...	chrome.exe	www.dropbox.com	
8:30:48 am	Open	chrome.exe		[Default] File Upload via Internet browser
8:30:49 am	Open	chrome.exe		
8:30:52 am	Home - Dropbox - Google Ch...	chrome.exe	www.dropbox.com	
8:30:02 am	Home - Dropbox - Google Ch...	chrome.exe	www.dropbox.com	
8:30:05 am	Home - Dropbox - Google Ch...	chrome.exe	www.dropbox.com	
8:30:06 am	Home - Dropbox - Google Ch...	chrome.exe	www.dropbox.com	
8:30:09 am	Home - Dropbox - Google Ch...	chrome.exe	www.dropbox.com	
8:30:06 am	Home - Dropbox - Google Ch...	chrome.exe	www.dropbox.com	[Clipboard (Copy)] https://www...
8:30:11 am	Home - Dropbox - Google Ch...	chrome.exe	www.dropbox.com	
8:30:13 am	Home - Dropbox - Google Ch...	chrome.exe	www.dropbox.com	
8:30:19 am	Home - Dropbox - Google Ch...	chrome.exe	www.dropbox.com	[Default] Cloud storages

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

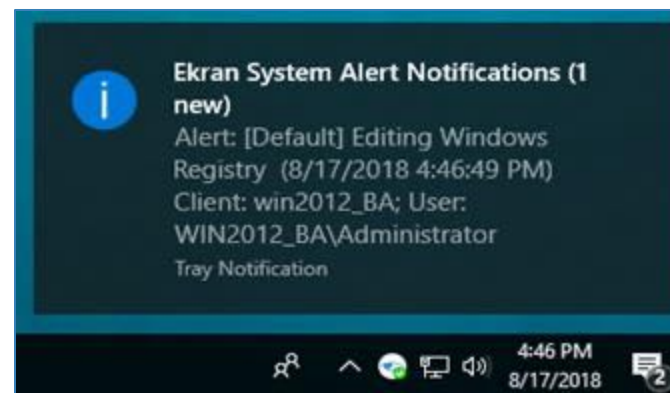


The screenshot displays the Alert Viewer application. The main window shows a Windows Registry Editor window with the 'Edit DWORD (32-bit) Value' dialog box open. The dialog box has 'Value name' set to 'EnableKeyStroke' and 'Value data' set to '1'. The 'Base' is set to 'Hexadecimal'. The 'OK' button is highlighted. The background shows a list of registry values under the 'Computer\HKEY_LOCAL_MACHINE\SOFTWARE\EkranSystem\Player' path. Below the main window, a metadata panel provides details about the alert:

- Who? ENTERSERV2\Administrator(adminlogin)
- When? 07/12/2018 12:09:54 pm
- Where? EnterServ2
- What? Edit DWORD (32-bit) Value - regedit.exe - <https://gr-pc/EkranSystem//Player...>

The bottom of the interface includes a navigation bar with a search icon, a page indicator '5/5', and an 'Open Session' button.

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



Ekran System Tray Notifications Journal - ginger-pc - admin

Activity Time	Alert Name	Alert Level	Alert Description	User Name	Client Name	Client Description	Details	Client Groups
8/17/2018 4:52...	[Default] Instan...	Normal	This is an alert o...	DEV\cathy	cathy-pc		Skype [1] - Sky...	
8/17/2018 4:51...	[Default] Online...	Critical	This is an alert f...	DEV\cathy	cathy-pc		Facebook - Goo...	
8/17/2018 4:51...	[Default] Social ...	Normal	This is an alert f...	DEV\cathy	cathy-pc		Facebook - Goo...	
8/17/2018 4:51...	[Default] Instan...	Normal	This is an alert o...	DEV\cathy	cathy-pc		Skype - Skype.e...	
8/17/2018 4:51...	[Default] Online...	Critical	This is an alert f...	DEV\cathy	cathy-pc		New Tab - Goog...	
8/17/2018 4:51...	[Default] Date a...	High	This is an Alert ...	DEV\alice	alice-pc		Date and Time I...	
8/17/2018 4:51...	[Default] Social ...	Normal	This is an alert f...	DEV\cathy	cathy-pc		New Tab - Goog...	
8/17/2018 4:50...	[Default] Instan...	Normal	This is an alert o...	DEV\cathy	cathy-pc		Skype [1] - Sky...	
8/17/2018 4:50...	[Default] Comm...	High	This is an alert o...	WIN2012_BA\A...	win2012_BA		Administrator: C...	
8/17/2018 4:50...	[Default] Remot...	High	This is an Alert ...	DEV\alice	alice-pc		win2012_ba - R...	
8/17/2018 4:50...	[Default] Cloud ...	Critical	This is an alert o...	DEV\alice	alice-pc		dropbox downlo...	
8/17/2018 4:50...	File downloading	Normal	This is an alert o...	DEV\alice	alice-pc		dropbox downlo...	
8/17/2018 4:49...	[Default] Social ...	Normal	This is an alert f...	DEV\alice	alice-pc		New Tab - Goog...	
8/17/2018 4:48...	[Default] Comm...	High	This is an alert o...	WIN2012_BA\A...	win2012_BA		Administrator: C...	
8/17/2018 4:48...	[Default] Editing...	Critical	This is an alert o...	WIN2012_BA\A...	win2012_BA		Edit String - reg...	
8/17/2018 4:46...	[Default] Editing...	Critical	This is an alert o...	WIN2012_BA\A...	win2012_BA		Edit String - reg...	

View in Web-Player Empty Journal

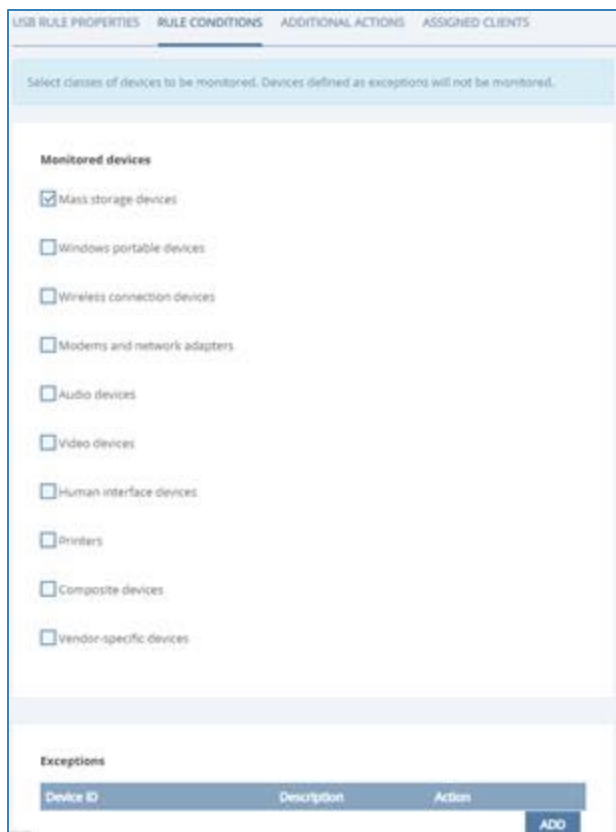
Monitorowanie USB

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 Kernel)

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.



USB RULE PROPERTIES RULE CONDITIONS ADDITIONAL ACTIONS ASSIGNED CLIENTS

Select classes of devices to be monitored. Devices defined as exceptions will not be monitored.

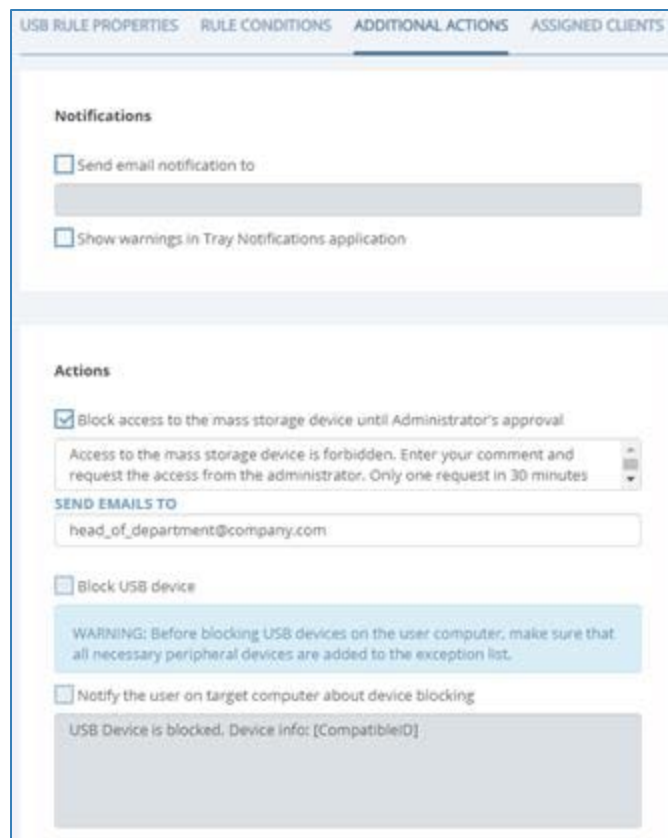
Monitored devices

- ☒ Mass storage devices
- ☐ Windows portable devices
- ☐ Wireless connection devices
- ☐ Modems and network adapters
- ☐ Audio devices
- ☐ Video devices
- ☐ Human interface devices
- ☐ Printers
- ☐ Composite devices
- ☐ Vendor-specific devices

Exceptions

Device ID	Description	Action
-----------	-------------	--------

ADD



USB RULE PROPERTIES RULE CONDITIONS ADDITIONAL ACTIONS ASSIGNED CLIENTS

Notifications

- ☒ Send email notification to
- ☐ Show warnings in Tray Notifications application

Actions

- ☒ Block access to the mass storage device until Administrator's approval

Access to the mass storage device is forbidden. Enter your comment and request the access from the administrator. Only one request in 30 minutes

SEND EMAILS TO

head_of_department@company.com

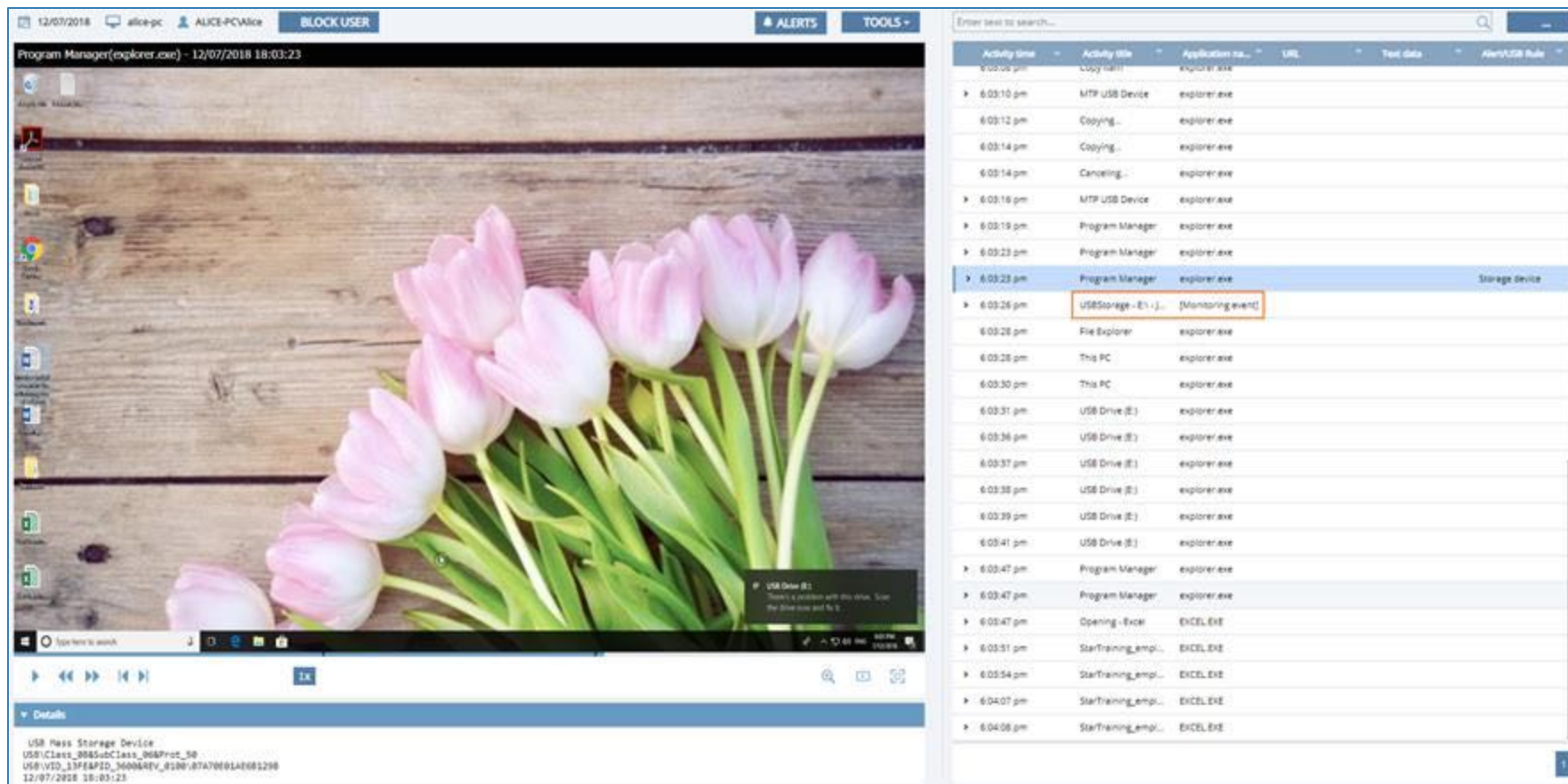
- ☐ Block USB device

WARNING: Before blocking USB devices on the user computer, make sure that all necessary peripheral devices are added to the exception list.

- ☐ Notify the user on target computer about device blocking

USB Device is blocked, Device info: [CompatibleID]

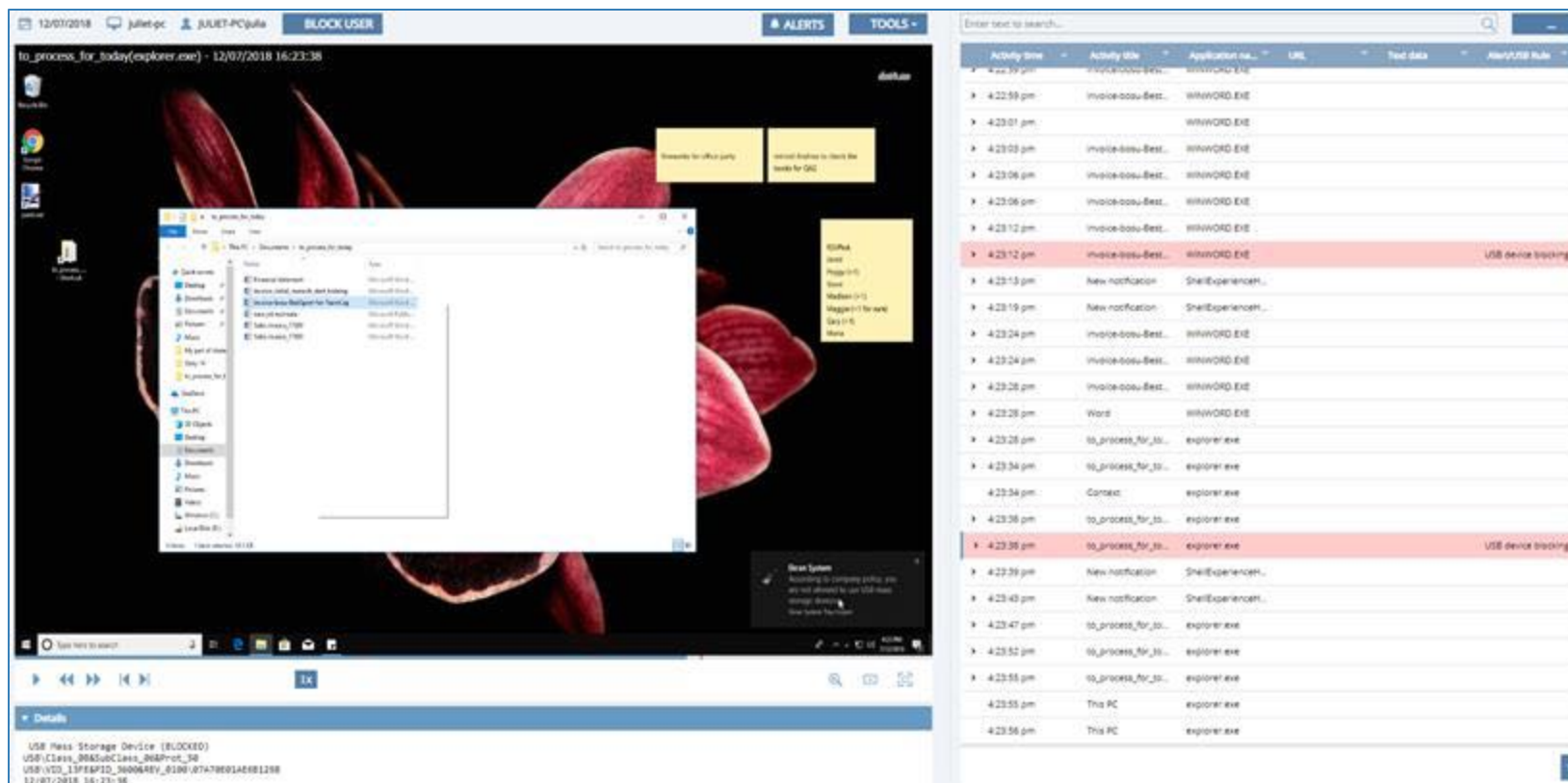
Pamięć USB jest wykrywana automatycznie po jej podłączeniu.



The screenshot displays the Securivy monitoring software interface. On the left, a live video feed shows a Windows desktop with a wallpaper of pink tulips. A notification bubble in the bottom right of the video feed reads: "USB Drive (E:) There's a problem with this drive. Scan the drive now and fix it." Below the video feed, the 'Details' section shows information about the USB Mass Storage Device: "USB\Class_8050&Class_0&Prot_50", "USB\VID_13F6&PID_3400&REV_0100&87A700&L1A1001200", and the timestamp "12/07/2018 18:03:23". On the right, the 'ALERTS' pane shows a list of events. The event at 6:03:26 pm is highlighted with an orange box and labeled as a "Storage device" event. The event details are: "USBStorage - E: - J..." and "[Monitoring event]".

Activity time	Activity title	Application name	URL	Text data	Alert/USB Rule
6:03:06 pm	Logon UI	explorer.exe			
6:03:10 pm	MTP USB Device	explorer.exe			
6:03:12 pm	Copying...	explorer.exe			
6:03:14 pm	Copying...	explorer.exe			
6:03:14 pm	Canceling...	explorer.exe			
6:03:16 pm	MTP USB Device	explorer.exe			
6:03:19 pm	Program Manager	explorer.exe			
6:03:23 pm	Program Manager	explorer.exe			
6:03:26 pm	USBStorage - E: - J...	explorer.exe			Storage device
6:03:26 pm	[Monitoring event]				
6:03:28 pm	File Explorer	explorer.exe			
6:03:28 pm	This PC	explorer.exe			
6:03:30 pm	This PC	explorer.exe			
6:03:31 pm	USB Drive (E:)	explorer.exe			
6:03:36 pm	USB Drive (E:)	explorer.exe			
6:03:37 pm	USB Drive (E:)	explorer.exe			
6:03:38 pm	USB Drive (E:)	explorer.exe			
6:03:39 pm	USB Drive (E:)	explorer.exe			
6:03:41 pm	USB Drive (E:)	explorer.exe			
6:03:47 pm	Program Manager	explorer.exe			
6:03:47 pm	Program Manager	explorer.exe			
6:03:47 pm	Opening - Excel	EXCEL EXE			
6:03:51 pm	StarTraining.empl...	EXCEL EXE			
6:03:54 pm	StarTraining.empl...	EXCEL EXE			
6:04:07 pm	StarTraining.empl...	EXCEL EXE			
6:04:08 pm	StarTraining.empl...	EXCEL EXE			

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



The screenshot displays the Securivy monitoring interface. On the left, a Windows desktop is visible with a file explorer window open, showing a folder named 'to_process_for_log'. The desktop background features a large image of a red chili pepper. On the right, a list of USB events is shown, with several rows highlighted in red to indicate USB device blocking.

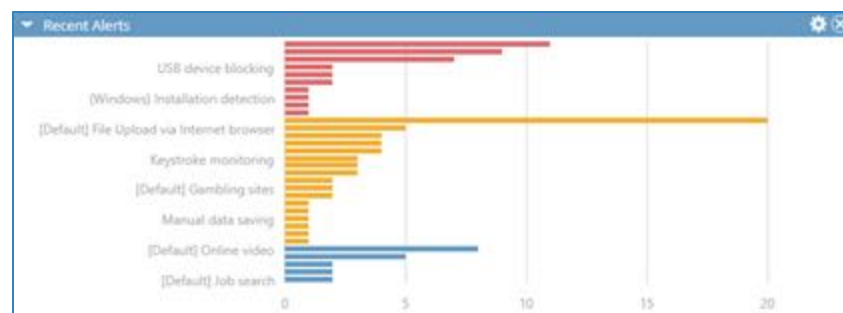
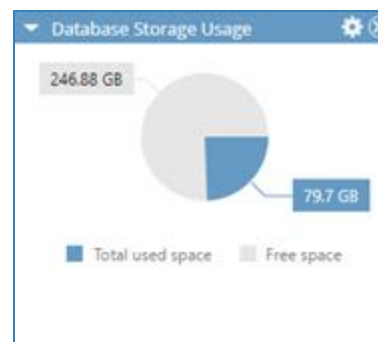
Activity time	Activity file	Application name	URL	Test data	Alert/USB rule
4:22:59 pm	Invoice-000-Best...	WINWORD.EXE			
4:23:01 pm	Invoice-000-Best...	WINWORD.EXE			
4:23:03 pm	Invoice-000-Best...	WINWORD.EXE			
4:23:05 pm	Invoice-000-Best...	WINWORD.EXE			
4:23:06 pm	Invoice-000-Best...	WINWORD.EXE			
4:23:12 pm	Invoice-000-Best...	WINWORD.EXE			
4:23:12 pm	Invoice-000-Best...	WINWORD.EXE			USB device blocking
4:23:13 pm	New notification	ShellExperienceH...			
4:23:19 pm	New notification	ShellExperienceH...			
4:23:24 pm	Invoice-000-Best...	WINWORD.EXE			
4:23:24 pm	Invoice-000-Best...	WINWORD.EXE			
4:23:26 pm	Word	WINWORD.EXE			
4:23:28 pm	to_process_for_log...	explorer.exe			
4:23:34 pm	to_process_for_log...	explorer.exe			
4:23:34 pm	Context	explorer.exe			
4:23:36 pm	to_process_for_log...	explorer.exe			
4:23:38 pm	to_process_for_log...	explorer.exe			USB device blocking
4:23:39 pm	New notification	ShellExperienceH...			
4:23:43 pm	New notification	ShellExperienceH...			
4:23:47 pm	to_process_for_log...	explorer.exe			
4:23:52 pm	to_process_for_log...	explorer.exe			
4:23:55 pm	to_process_for_log...	explorer.exe			
4:23:55 pm	This PC	explorer.exe			
4:23:56 pm	This PC	explorer.exe			

Details

USB Mass Storage Device (BLOCKED)
USB\Class_80ASubClass_80AProt_50
USB\VID_13F8&PID_3606&REV_0190\7A79891A&81298
12/07/2018 16:23:36

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**.

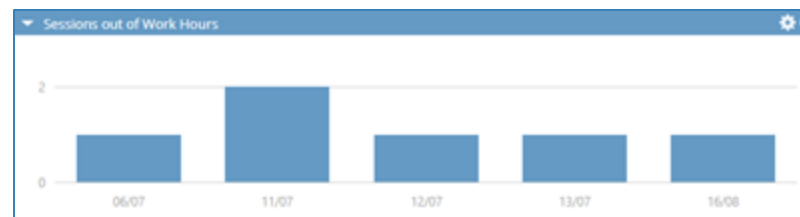


Rarely Used Computers

Client Name	Sessions
alice-potter	2
kate-moss	2
tom-pitterson	1
stefan-welch	13

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



Istnieją 4 główne typy dashboardów 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

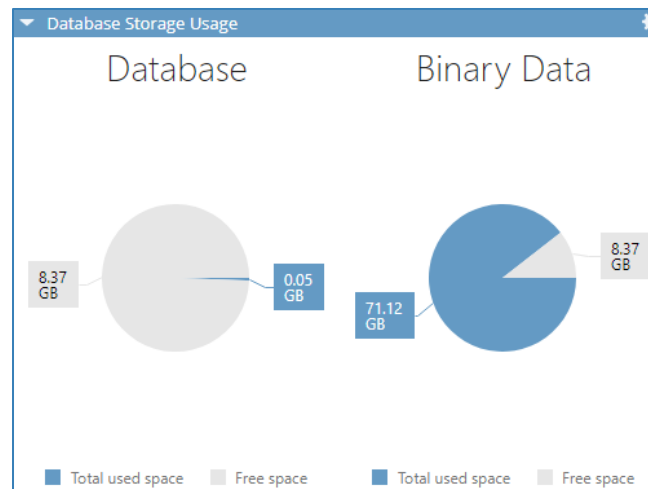
Monitorowanie Zasobów Serwera

- Zużycie procesora
- Zużycie pamięci
- Stan bazy danych

Komputery z Ekran Client



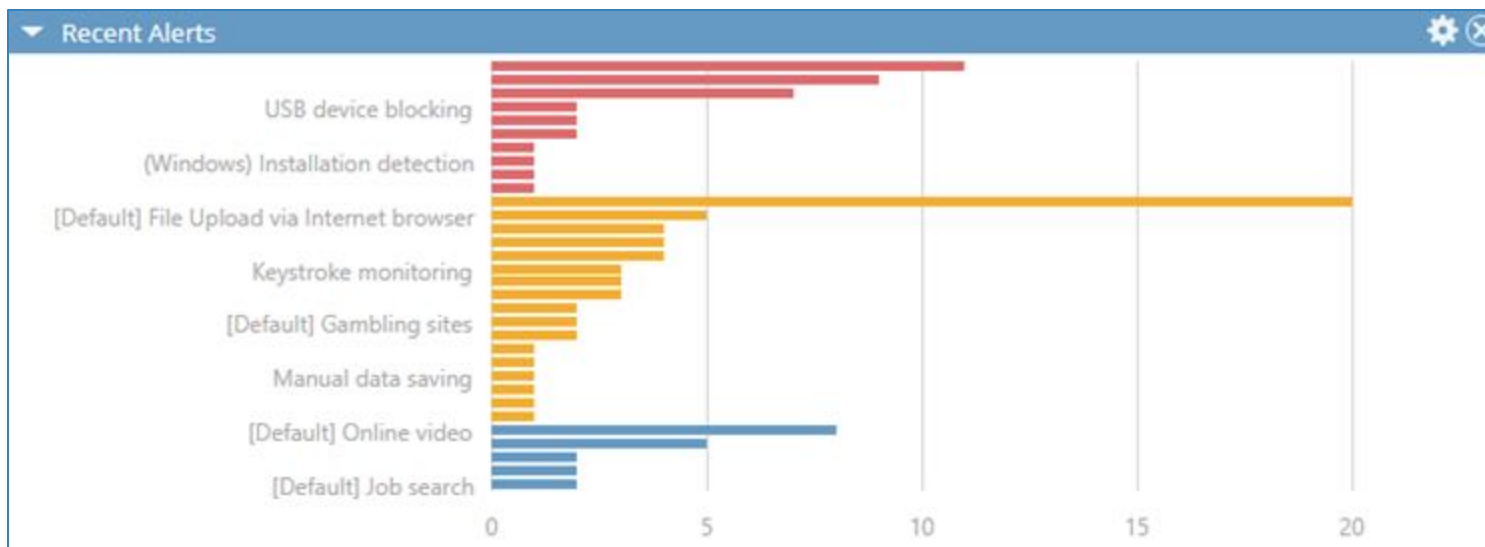
Zużycie bazy danych



Licencje



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

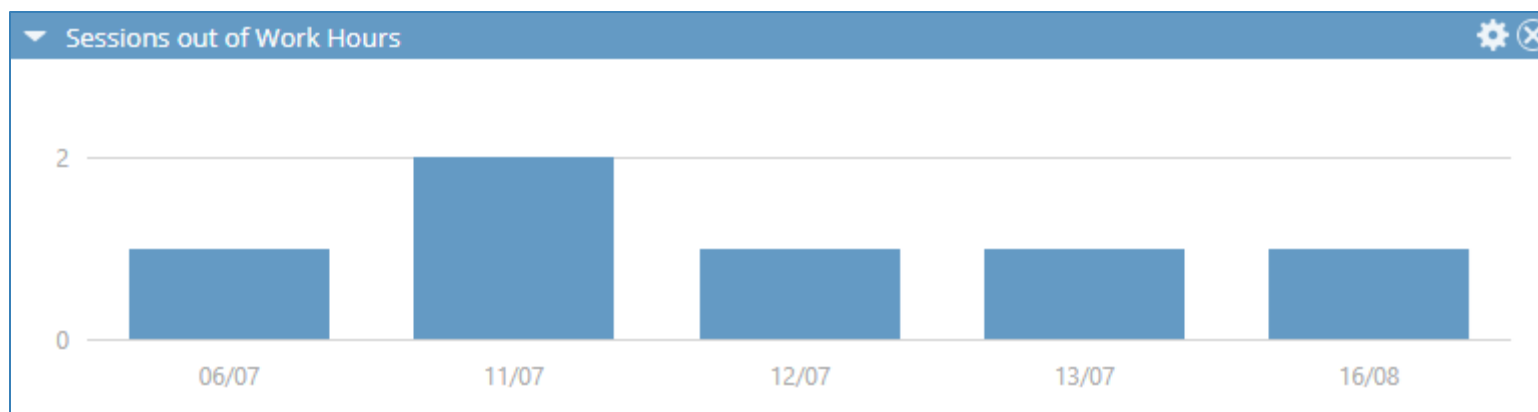
Rzadko używane komputery

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

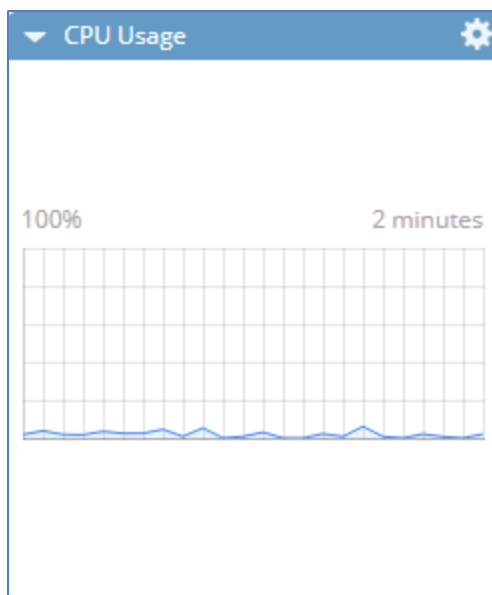
Rzadko używane loginy

Rarely Used Logins	
User Name	Sessions
TV\admin	1
User	1
Guest	1

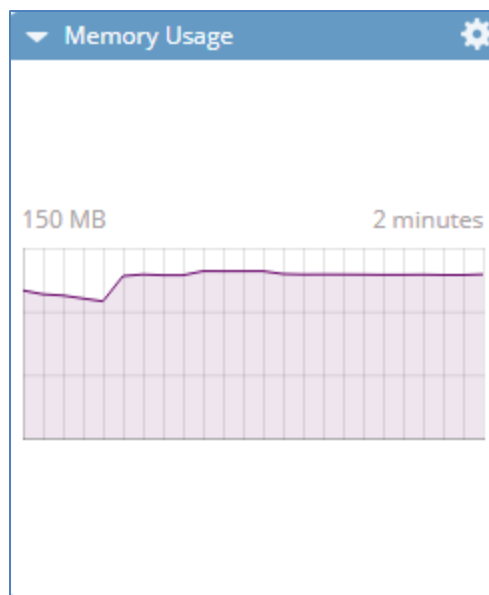
Sesje poza godzinami pracy



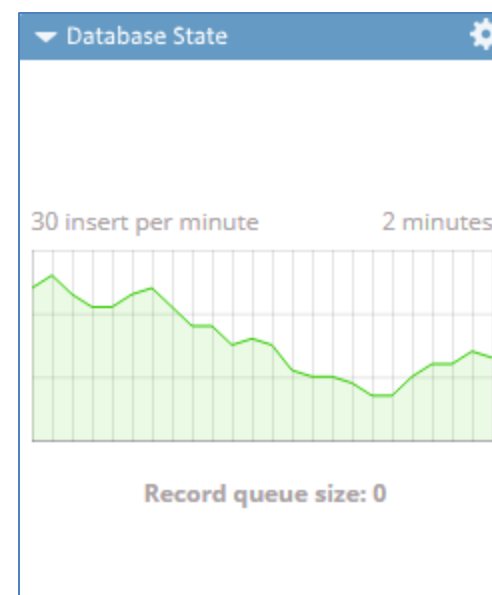
Zużycie procesora



Zużycie pamięci



Stan bazy danych

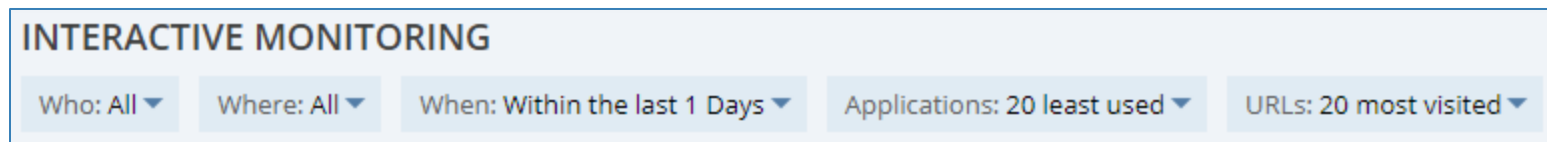


Interactive Monitoring

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.

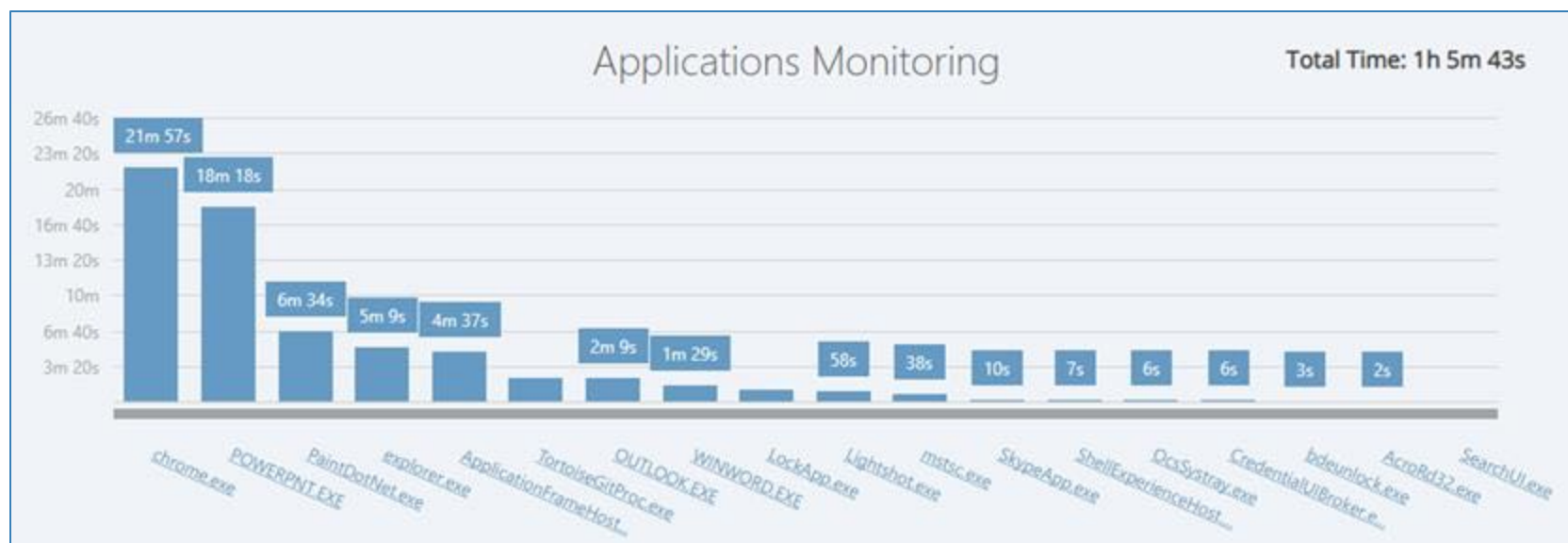


Dane wyświetlane są w postaci dwóch wykresów kolumnowych (wykres **monitorowania aplikacji** i wykres **monitorowania URL**).

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

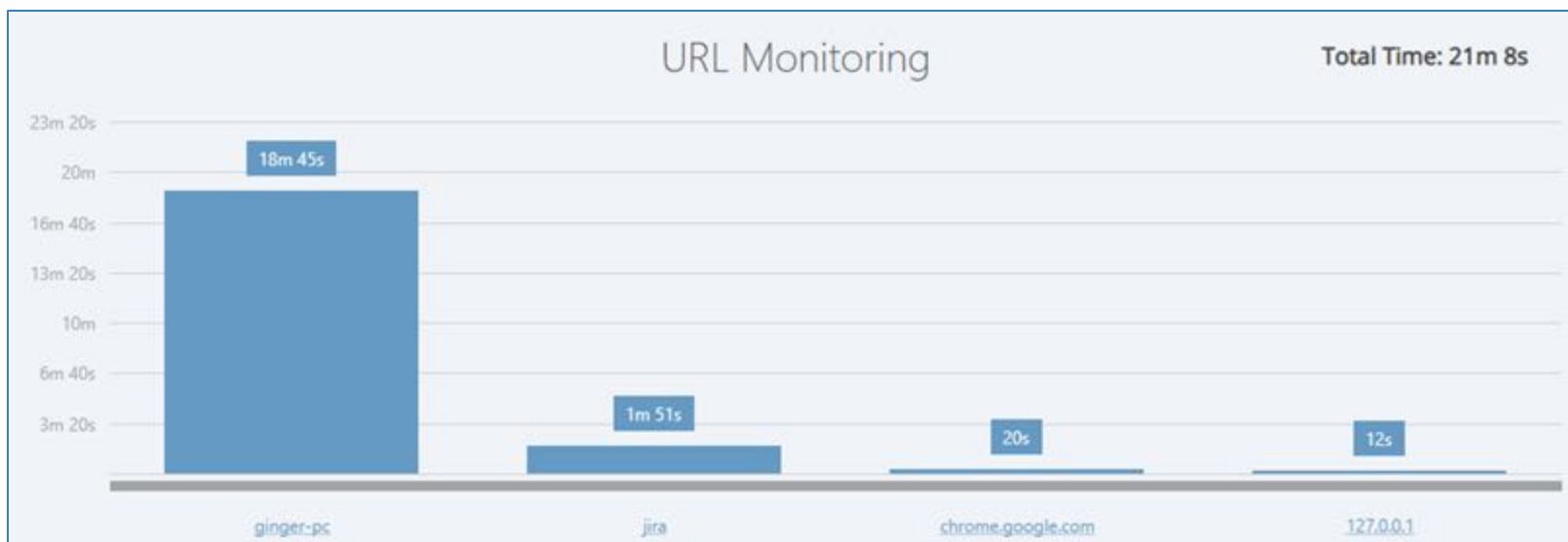
Wykres ten zawiera informacje na temat **częstotliwości korzystania z aplikacji**.

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



Wykres 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 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

SCHEDULED REPORTS						
ADD RULE ?						
Contains APPLY FILTERS						
Name	Description	Assigned To	Monitored Users	State	Frequency	Emails Recipients
Activity report		alice-pc: All Clients	All users	Enabled	Daily	admin@example.com
						Edit Rule View Log

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

Ręczne Generowanie Raportów

Report Type

Alert grid report

Alert grid report

Activity summary report

Activity chart report

Activity pie chart report

URL chart report

URL summary report

URL pie chart report

Linux/XWindow grid report

Kernel-level USB grid report

USB storage grid report

User statistics report

Session grid report

Detailed activity report

Clipboard grid report

User daily activity grid report

Sessions out of work hours grid report

User behavior analysis grid report

Terminal Server Grid Report

Date filters

From: 03/08/2018 15:00 To: 03/08/2018 15:59

Clients

+ Add Clients

Client Name	Description	Remove All
alice-pc		Remove

Client Groups

+ Add Client Groups

Client group name	Description	Remove All
All Clients	This group contains all installed Clients	Remove

Users

☒ Any user
☐ Selected users

+ Add Users

Users	Remove All
-------	------------

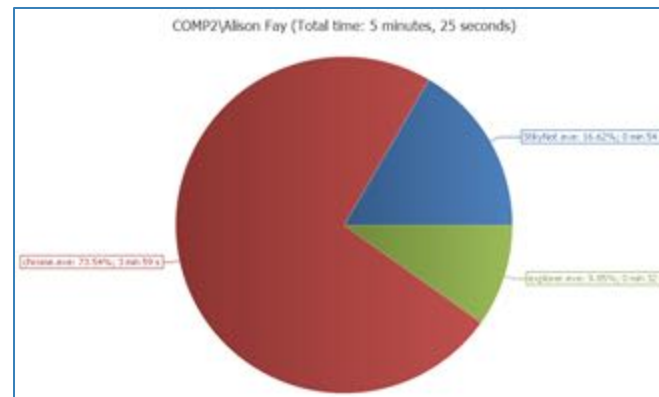
CREATE SCHEDULED REPORT RULE GENERATE REPORT

Raport podsumowujący aktywność

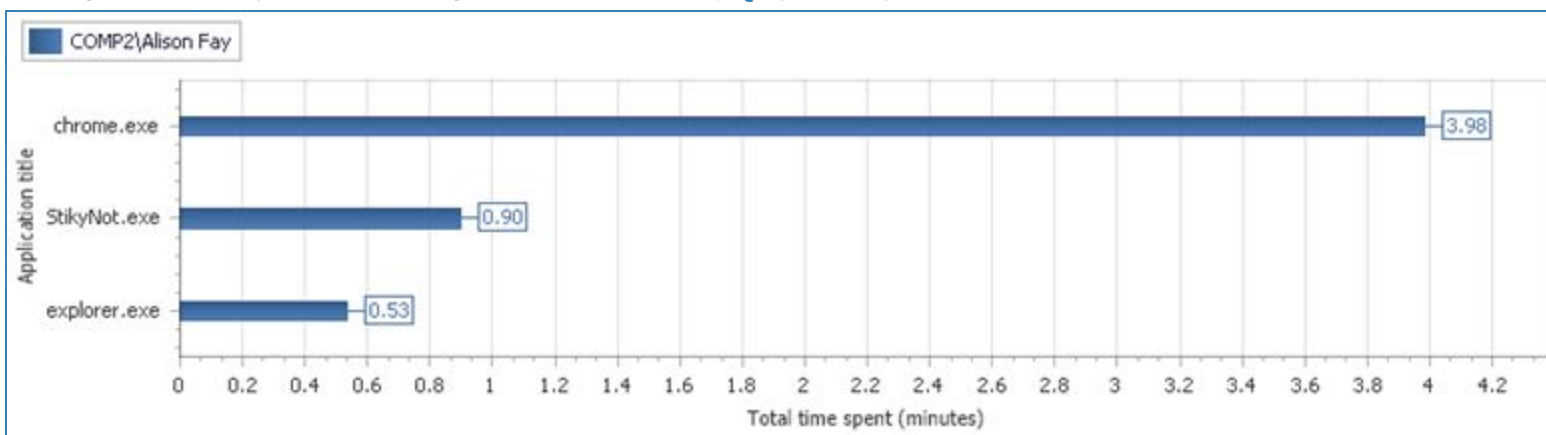
Client name	Comp2
Client description	Social media
User name	COMP2\Alison Fay
Total time	5 minutes, 25 seconds
Active time	5 minutes, 25 seconds

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



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



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_6 A9625E1	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\Benjami nTeel	4m 50s	4m 50s	07/12/2018 08:44:03 AM	07/12/2018 08:48:53 AM	None	Open Session

Szczegółowy raport aktywności

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

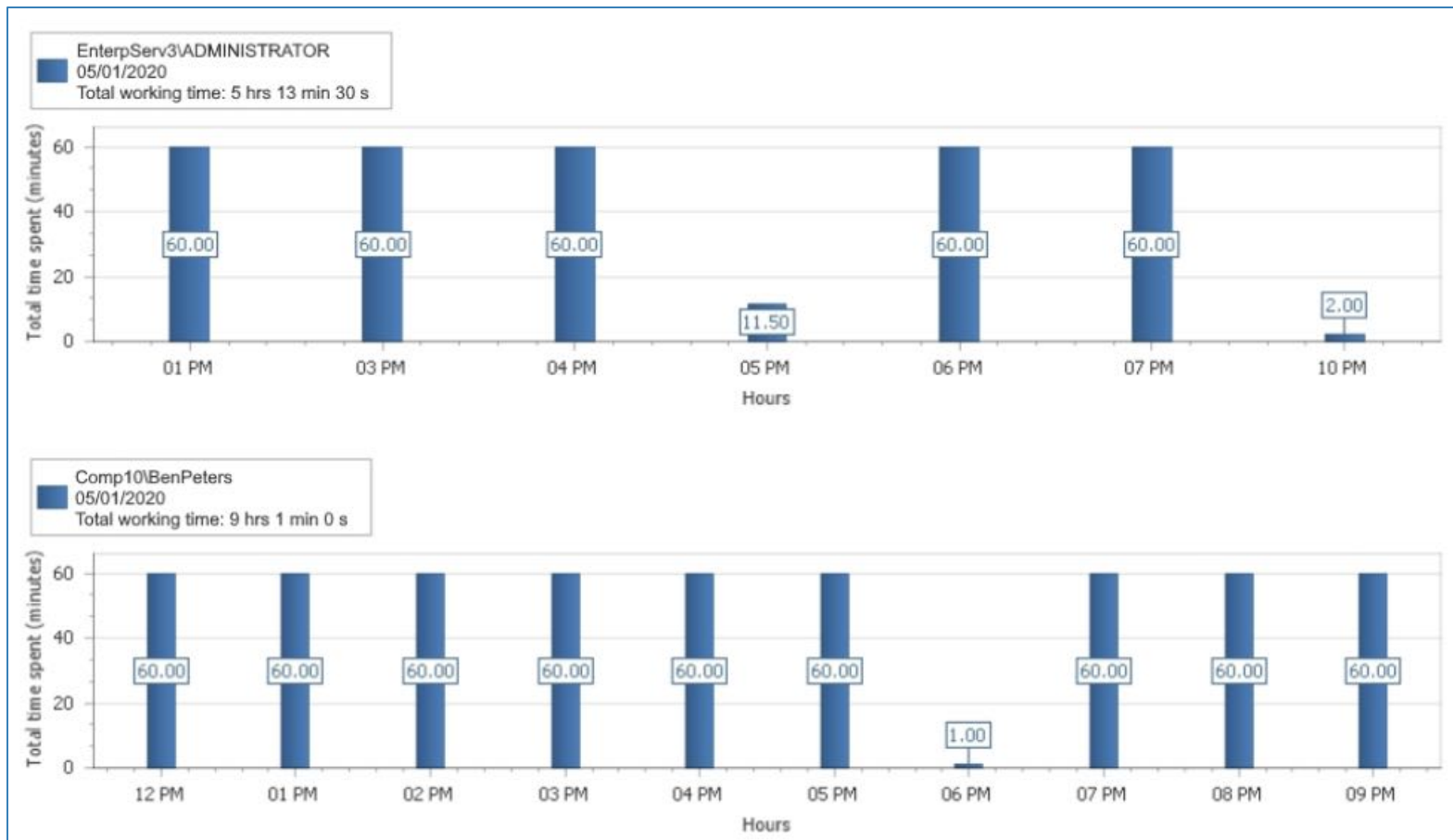
Activity time	Activity title	Application name	URL	Text data
07/10/2018 08:52:45 AM	My Drive - Google Drive - Google Chrome	chrome.exe	https://drive.google.com/drive/my-drive?ogsc=32	
07/10/2018 08:52:49 AM	My Drive - Google Drive - Google Chrome	chrome.exe	https://drive.google.com/drive/my-drive?ogsc=32	
07/10/2018 08:52:50 AM	My Drive - Google Drive - Google Chrome	chrome.exe	https://drive.google.com/drive/my-drive?ogsc=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?ogsc=32	
07/10/2018 08:53:00 AM	My Drive - Google Drive - Google Chrome	chrome.exe	https://drive.google.com/drive/my-drive?ogsc=32	
07/10/2018 08:53:01 AM	My Drive - Google Drive - Google Chrome	chrome.exe	https://drive.google.com/drive/my-drive?ogsc=32	
07/10/2018 08:53:01 AM	My Drive - Google Drive - Google Chrome	chrome.exe	https://drive.google.com/drive/my-drive?ogsc=32	
07/10/2018 08:53:01 AM	My Drive - Google Drive - Google Chrome	chrome.exe	https://drive.google.com/drive/my-drive?ogsc=32	[Clipboard (Paste)] https://drive.google.com/file/d/19TprjVlW-HHSGodL0xHmO8HXh7wlnw/view?usp=sharing
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 (5) - helenapeterson.lv@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 -

Raport dotyczący zachowania użytkownika

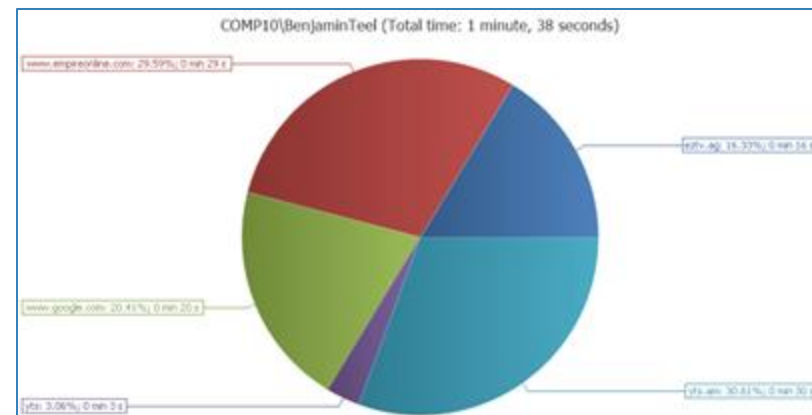
Risk Level	Critical				
Risk Score. %	100 - 76				
Session number	3				
Who	Where	When	Details	Session Score	Session URL
Admin	Server	04/25/2019 01:00:00 AM - 04/25/2019 05:18:30 AM	WorkingHours: abnormal session start abnormal session end	93%	Open Session
FillMorris	Comp5	04/24/2019 07:00:00 PM - 04/25/2019 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

Raport podsumowujący korzystanie z adresów URL

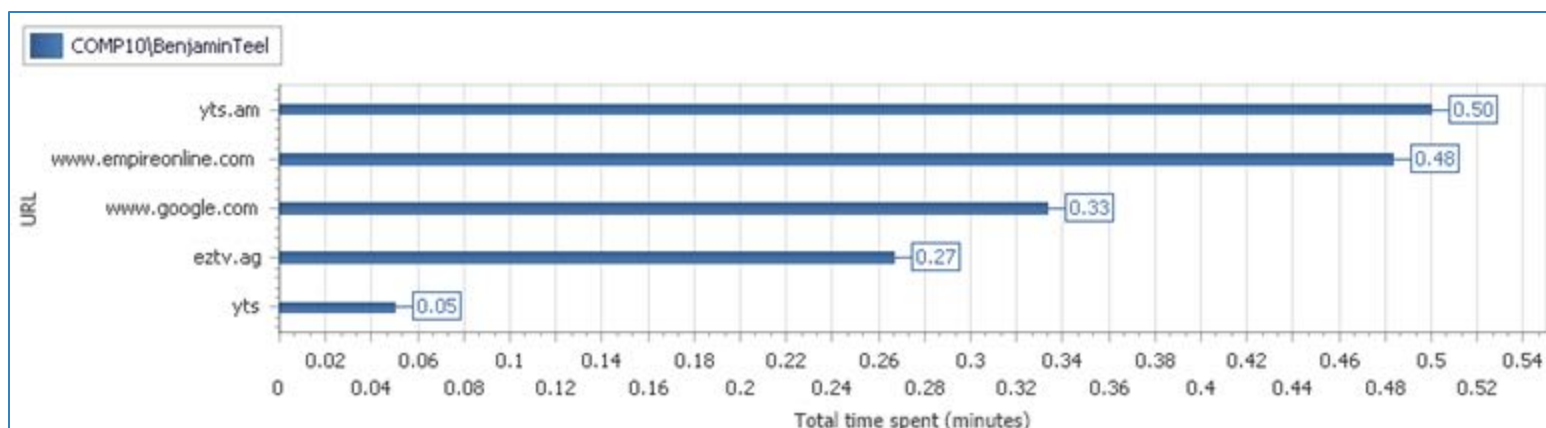
Client name	Comp15
Client description	Exporting HR Data
User name	COMP15\HelenPeterson
Total time	4 minutes, 30 seconds

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



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\07A70E01AE6 B1298
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\07A70E01AE6 B1298

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

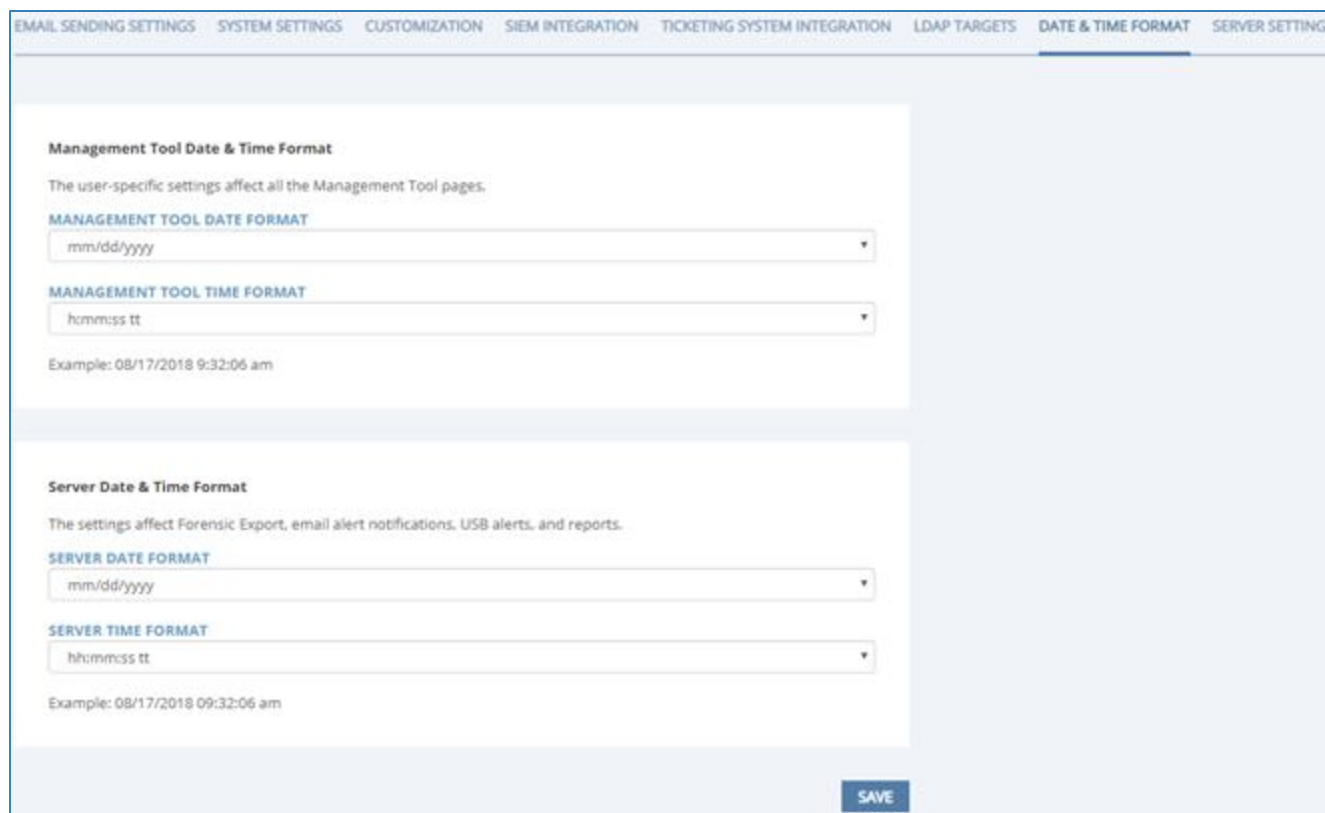
W raporcie Linux możesz zobaczyć wszystkie polecenia `exec*` i `sudo` wykonane na komputerach z Ekran Client z systemem Linux.

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

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



The screenshot shows the 'DATE & TIME FORMAT' configuration page. The page has a navigation bar at the top with the following tabs: EMAIL SENDING SETTINGS, SYSTEM SETTINGS, CUSTOMIZATION, SIEM INTEGRATION, TICKETING SYSTEM INTEGRATION, LDAP TARGETS, DATE & TIME FORMAT (selected), and SERVER SETTINGS.

The page is divided into two main sections:

- Management Tool Date & Time Format**
The user-specific settings affect all the Management Tool pages.
MANAGEMENT TOOL DATE FORMAT: A dropdown menu showing 'mm/dd/yyyy'.
MANAGEMENT TOOL TIME FORMAT: A dropdown menu showing 'h:mm:ss tt'.
Example: 08/17/2018 9:32:06 am
- Server Date & Time Format**
The settings affect Forensic Export, email alert notifications, USB alerts, and reports.
SERVER DATE FORMAT: A dropdown menu showing 'mm/dd/yyyy'.
SERVER TIME FORMAT: A dropdown menu showing 'h:mm:ss tt'.
Example: 08/17/2018 09:32:06 am

A 'SAVE' button is located at the bottom right of the page.

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

YOUR LOGO

Message:

You are performing a forbidden action.

OK (14)

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

Custom Reports Settings

HEADER TEXT

FOOTER TEXT

☒ Use a custom logo instead of the Ekran System logo
Upload the image to be used as a custom logo in reports.
The uploaded file must be in the .bmp, .jpg or .png. Recommended size is not more than 300x85.

CHOOSE FILE logo.png

YOUR LOGO

YOUR LOGO **Activity Summary Report**

Details

Generated in Ekran System 6.1.99.0

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

Custom Email Subjects

Define the subjects to be used in email notifications sent by Ekran System. You can use the following variables: #name – alert name; #user - user name; #pc – endpoint name; #priority - alert priority; #number – number of instances in the email (alerts); #OS - OS of the endpoint for alerts.

SINGLE ALERT NOTIFICATION:

Ekran System Alert - #pc, #user - #OS - #name (#priority)

MULTIPLE ALERTS NOTIFICATION:

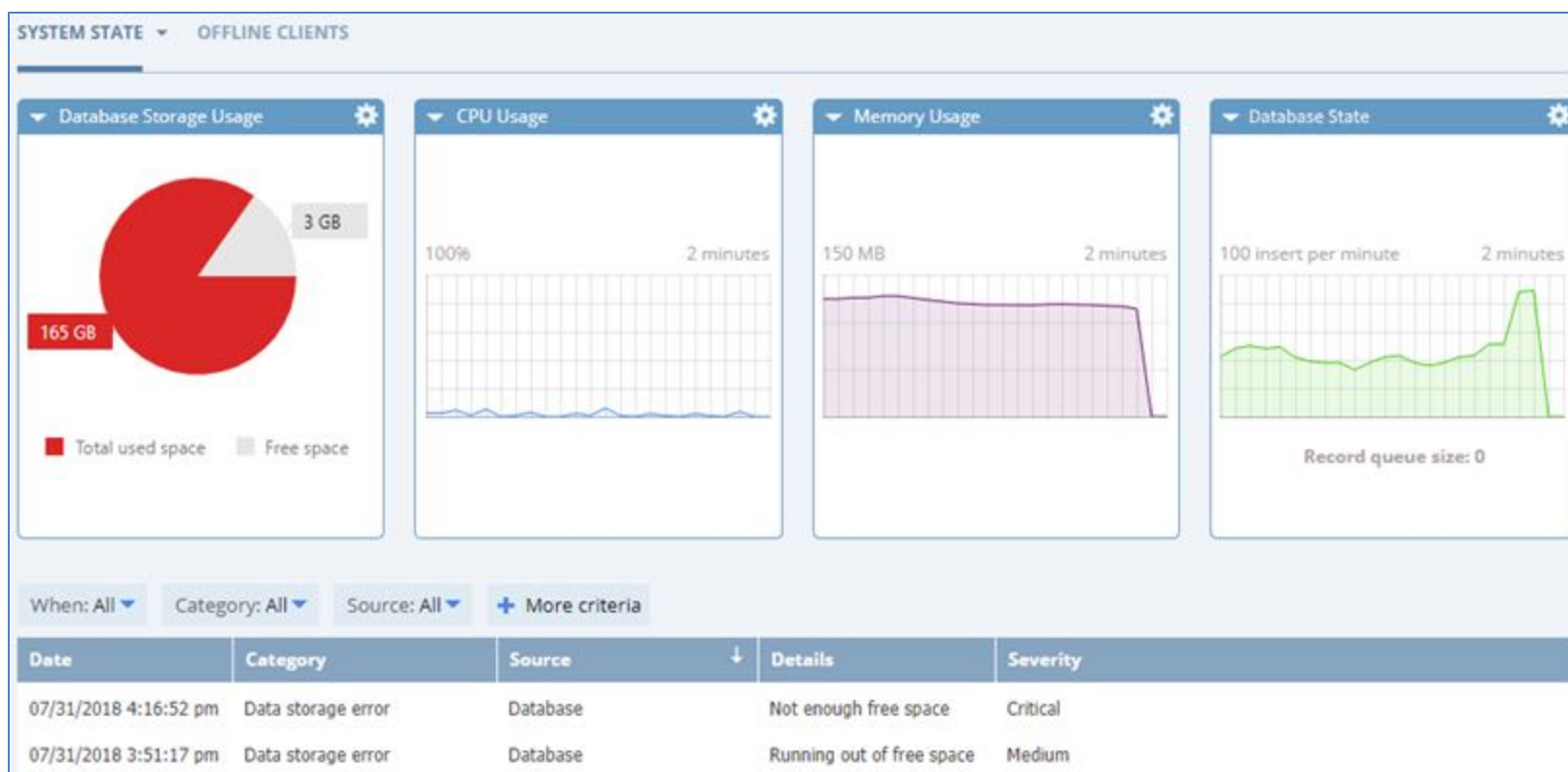
Ekran System Multiple Alerts - #number

RESTORE DEFAULT



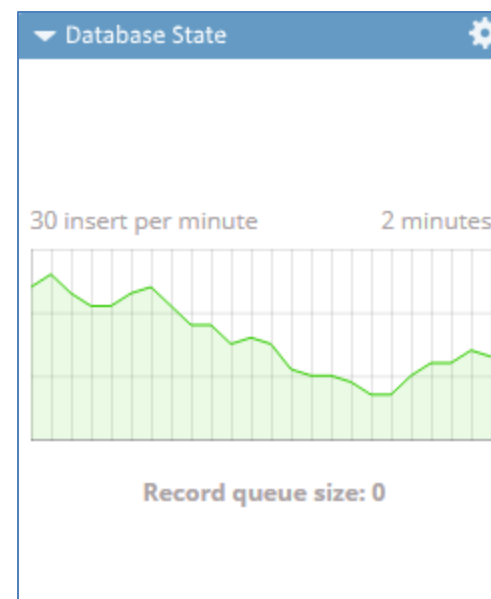
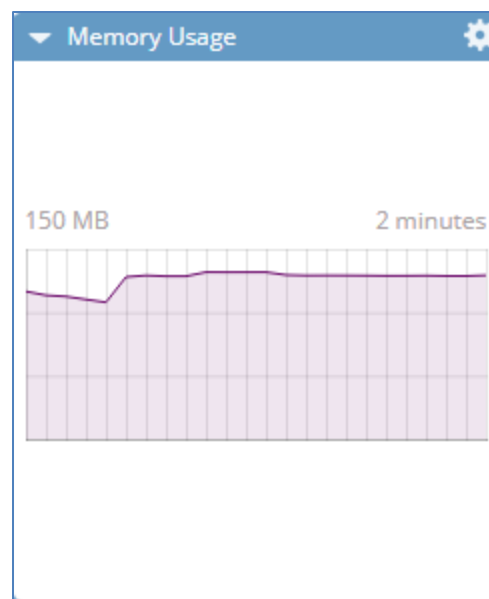
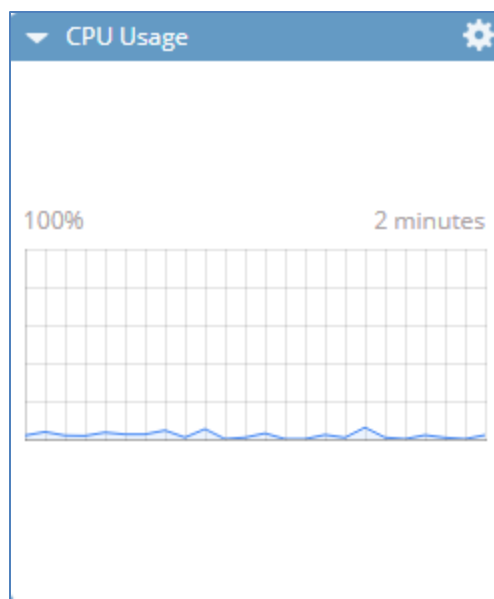
Health Monitoring

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.



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





Odwiedź nas na:

www.ekransystem.com