



Full Feature Presentation

Ekran System

Full Cycle Insider Risk Management

- [System Overview](#)
- [Ekran System Application Server & Management Tool](#)
- [Database Management](#)
- [Licensing](#)
- [Installing & Updating Clients](#)
- [Monitoring Parameters](#)
- [Detection of Disconnected Clients](#)
- [Client Protection](#)
- [Secondary User Authentication](#)
- [Two-Factor Authentication](#)
- [Password Management \(PAM\)](#)
- [User Behavior Analytics \(UEBA\)](#)
- [Administrator Approval on Login](#)
- [Access Request and Approval Workflow](#)
- [Notifying Users about Being Monitored](#)
- [Blocking Users](#)
- [Viewing Client Sessions](#)
- [Anonymizer \(for e.g. GDPR Compliance\)](#)
- [Alerts](#)
- [USB Device Monitoring](#)
- [Dashboards](#)
- [Interactive Monitoring](#)
- [Reports](#)
- [Application Customization](#)
- [Health Monitoring](#)
- [Ekran System API \(& Integration with e.g. Power BI\)](#)

System Overview

An Insider Risk Management User Activity Monitoring Solution

Privileged Activity Monitoring

Ekran System allows the creation of indexed video records of all concurrent terminal sessions on your servers, and the recording of remote and local sessions on endpoint computers, including those running on Windows, macOS and Linux OSs.

Employee Work Control

- Are you interested in enhancing your company's security?
- Do you want to know what your employees do during work hours?
- Do you want to control the use of sensitive information?

Privileged Password and Session Management

Ekran System helps you to provide privileged access (PAM) to critical assets and meet compliance requirements (e.g. GDPR) by securing, managing and monitoring privileged accounts and access.

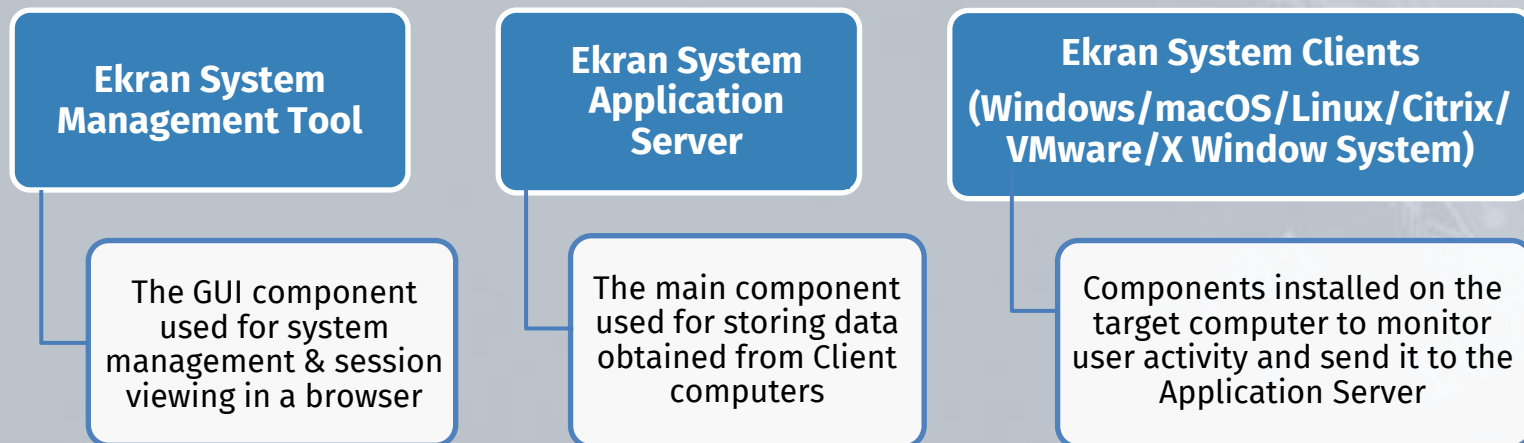
Flexible Deployment and Licensing

Ekran System supports the widest range of platforms and infrastructure configurations on the market, delivering reliable deployments of any size, from piloting dozens to tens of thousands of endpoints. Flexible licensing helps to fit it into your budget and address project changes.

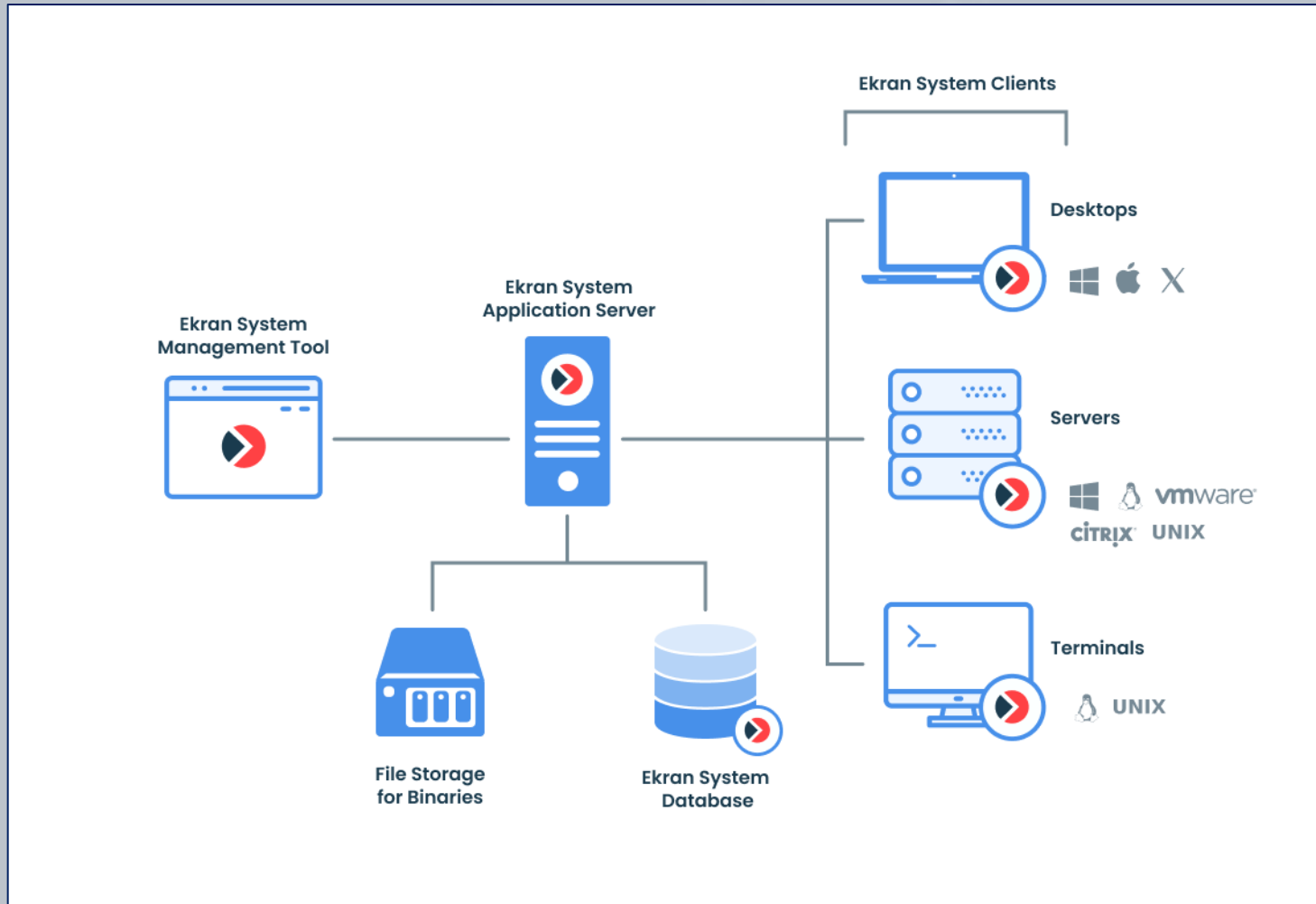
Ekran System is a full-cycle **insider risk management user activity monitoring** software solution for enhanced cybersecurity. It is used to **deter, detect** and **disrupt insider threats** to your corporate IT infrastructure, as well as to assist you in meeting **compliance requirements** (e.g. GDPR), manage **privileged user access** (PAM), immediately respond to potential incidents, etc.

You can **record** all terminal, remote, and local **user sessions**, and **alert** security personnel to suspicious events, and Ekran System is available in both **on-premises** and **SaaS deployments**.

The Main Components of Ekran System



The Basic Deployment Scheme

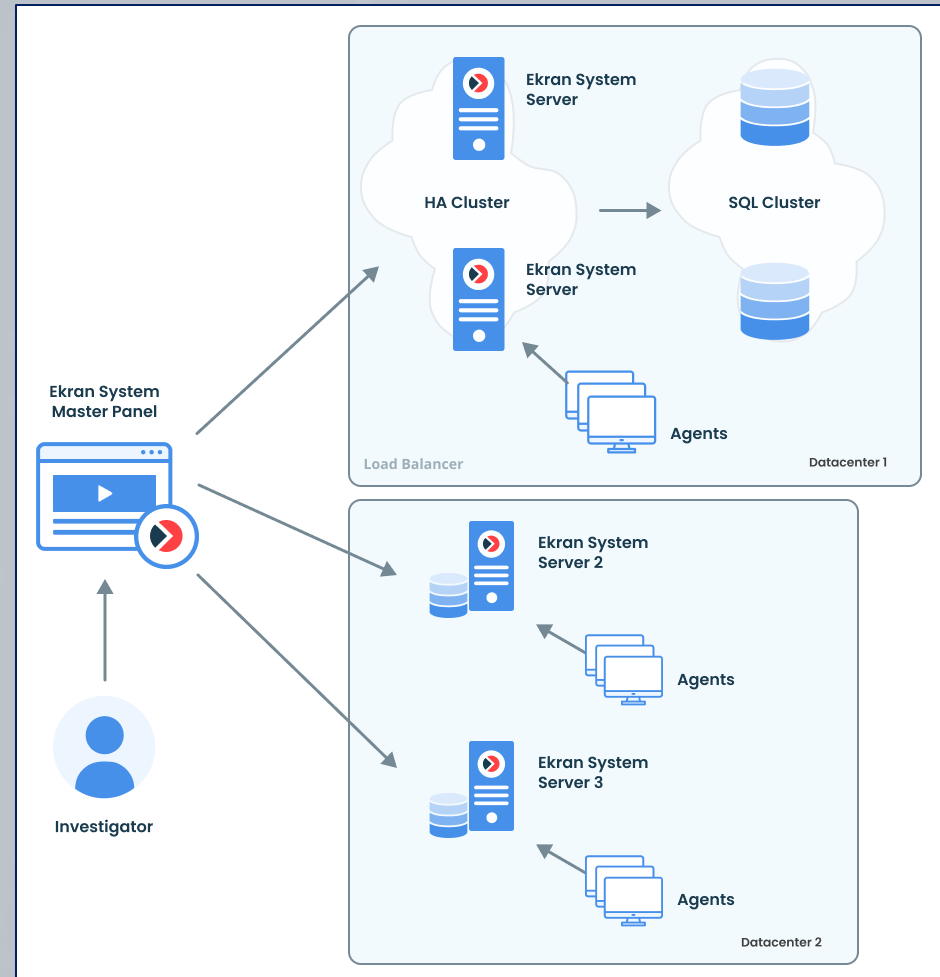


Large-Scale Deployments

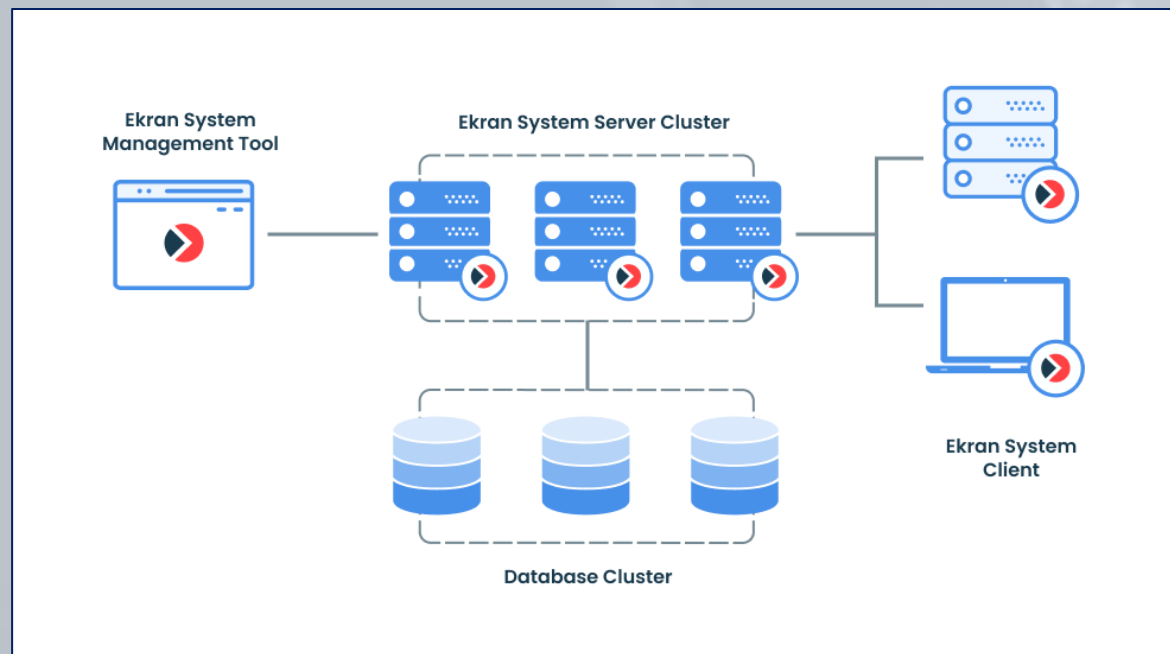
In terms of scalability, and for large organizations which may have several geographically isolated data centers, **multiple connected instances of the Application Server** can be deployed.

For complex deployments, Ekran System also offers **high availability & disaster recovery**, and **multi-tenant** mode, and also supports the use of third-party **load balancing** software.

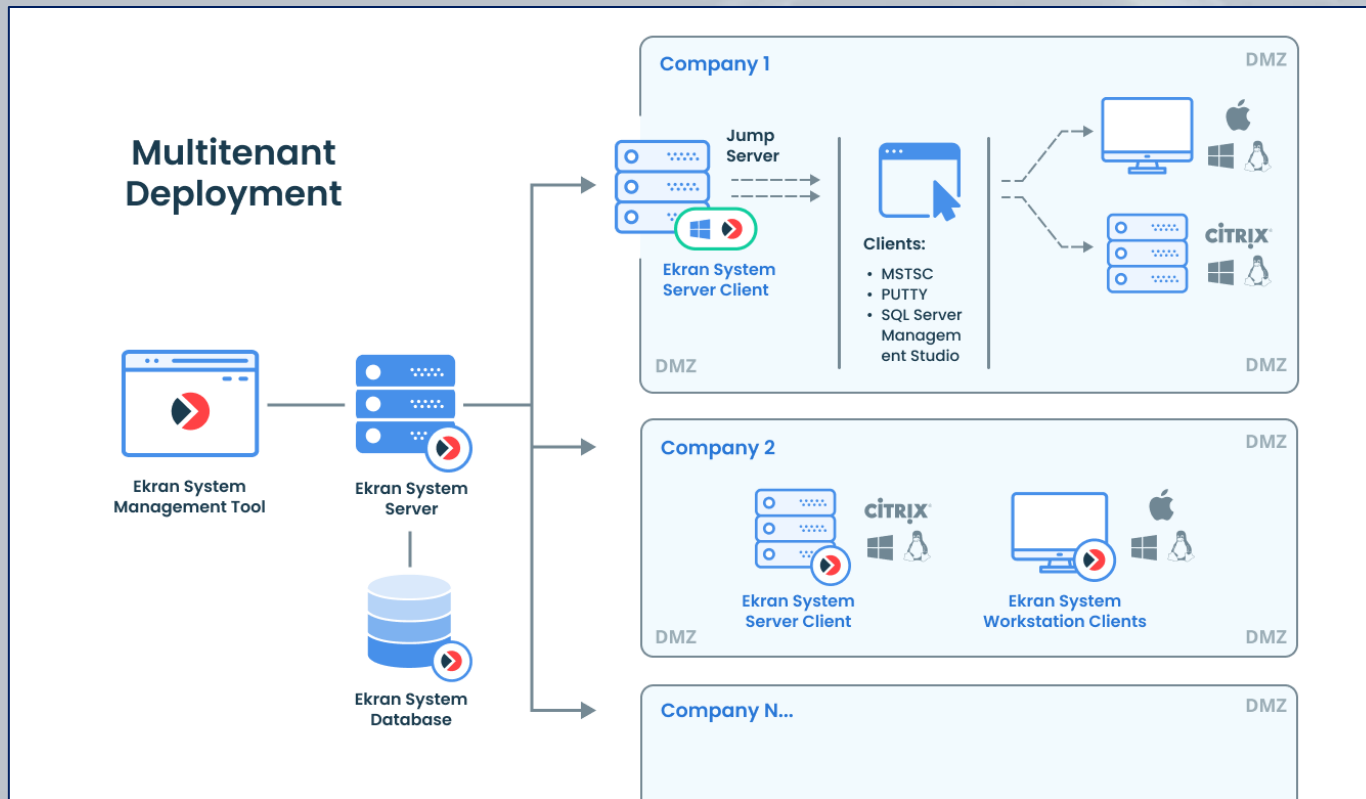
The **Master Panel**, which is an additional stand-alone component of Ekran System, **combines the data** recorded by all Ekran System Applications Servers in multiple locations, allowing the data to be **viewed and managed in a single user interface**.



High Availability mode allows you to configure and deploy Ekran System in such a way that if the Ekran System Application Server stops functioning for any reason, **another Application Server instance will replace it** automatically **without loss of data** or the need for **reinstallation of the system**.



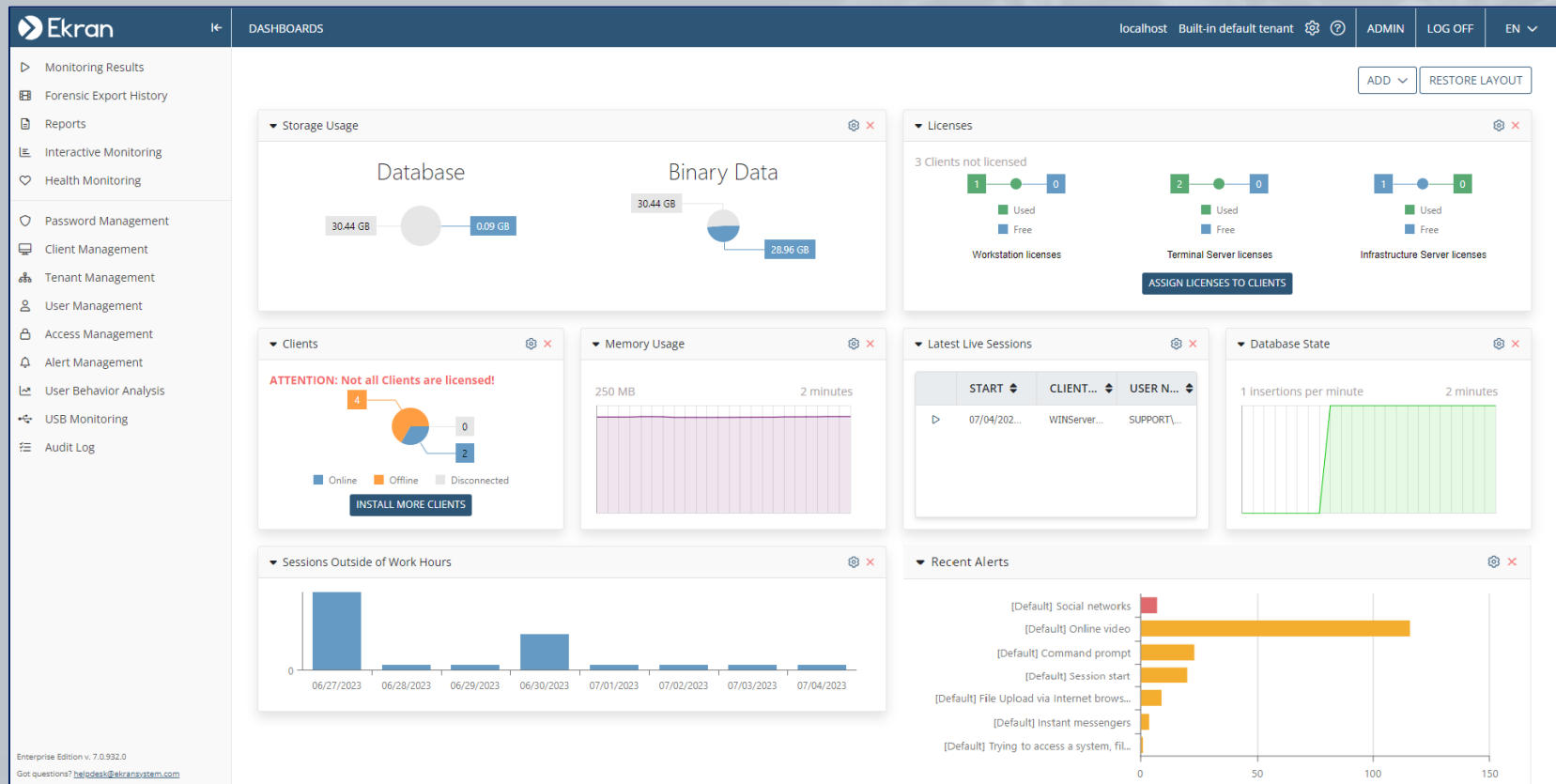
Multi-Tenant mode allows **multiple** completely **isolated tenants** to operate in the Ekran System environment. The **data** in each tenant is **independent** and not accessible to other tenants.



The Ekran System Application Server & the Management Tool

(user management, permissions,
Active Directory integration, and
Management Tool settings)

The **whole system is managed** in a single **browser-based interface**, called the Management Tool.

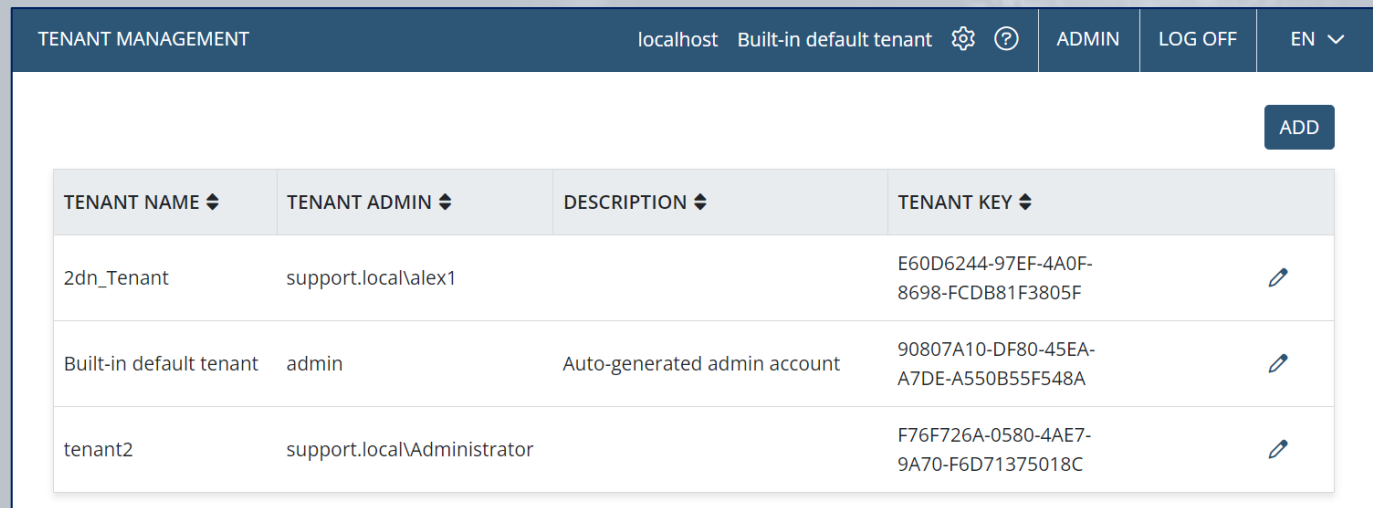


Ekran System can operate in Single-Tenant or Multi-Tenant mode.

Single-Tenant mode is selected by default. In this mode, **all users have access to all Clients and settings** according to their permissions.

In Multi-Tenant mode, all tenant **users** have access to their tenant Clients, but **do not have access to other tenants'** Clients, configurations, alerts, reports, etc.

You can **switch to Multi-Tenant mode at any time.**



The screenshot shows the 'TENANT MANAGEMENT' interface. At the top, there is a navigation bar with 'localhost Built-in default tenant' and icons for settings and help. On the right, there are buttons for 'ADMIN', 'LOG OFF', and a user menu 'EN'. An 'ADD' button is located in the top right corner of the table area. The table has four columns: 'TENANT NAME', 'TENANT ADMIN', 'DESCRIPTION', and 'TENANT KEY'. Each row includes an edit icon on the right side.

TENANT NAME	TENANT ADMIN	DESCRIPTION	TENANT KEY
2dn_Tenant	support.local\alex1		E60D6244-97EF-4A0F-8698-FCDB81F3805F
Built-in default tenant	admin	Auto-generated admin account	90807A10-DF80-45EA-A7DE-A550B55F548A
tenant2	support.local\Administrator		F76F726A-0580-4AE7-9A70-F6D71375018C

- Create two **types of users**: Internal or Active Directory (Windows domain users/groups).
- Use **groups** for easier management of users.
- Define **permissions** for users.

USER MANAGEMENT localhost Built-in default tenant ADMIN LOG OFF EN

Search... ADD USER GROUP ADD USER

▼ ALL USERS: ⚙️

LOGIN ▲	FIRST NAME	LAST NAME	DESCRIPTION	
admin	Administrator		Auto-generated admin account	✎
Nick				✎
Pamuser	Pam	User		✎
Supervisor	Steve	Johns		✎
support.local\Administrator				✎
support.local\alex1				✎




▼ ADMINISTRATORS: Users with all permissions ⚙️

LOGIN ▲	FIRST NAME	LAST NAME	DESCRIPTION	
admin	Administrator		Auto-generated admin account	✎
support.local\Administrator				✎
support.local\alex1				✎

▼ SUPERVISORS: Users who can view the monitoring results of all Clients ⚙️

LOGIN ▲	FIRST NAME	LAST NAME	DESCRIPTION	
Supervisor	Steve	Johns		✎

Integration with Active Directory allows you to establish domain trusts with **multiple domains**.








CONFIGURATION localhost Built-in default tenant   ADMIN LOG OFF EN 

SERIAL KEY MANAGEMENT EMAIL SENDING SETTINGS SYSTEM SETTINGS CUSTOMIZATION SIEM INTEGRATION

TICKETING SYSTEM INTEGRATION **LDAP TARGETS** DATE & TIME FORMAT EXPORT STORAGE SETTINGS

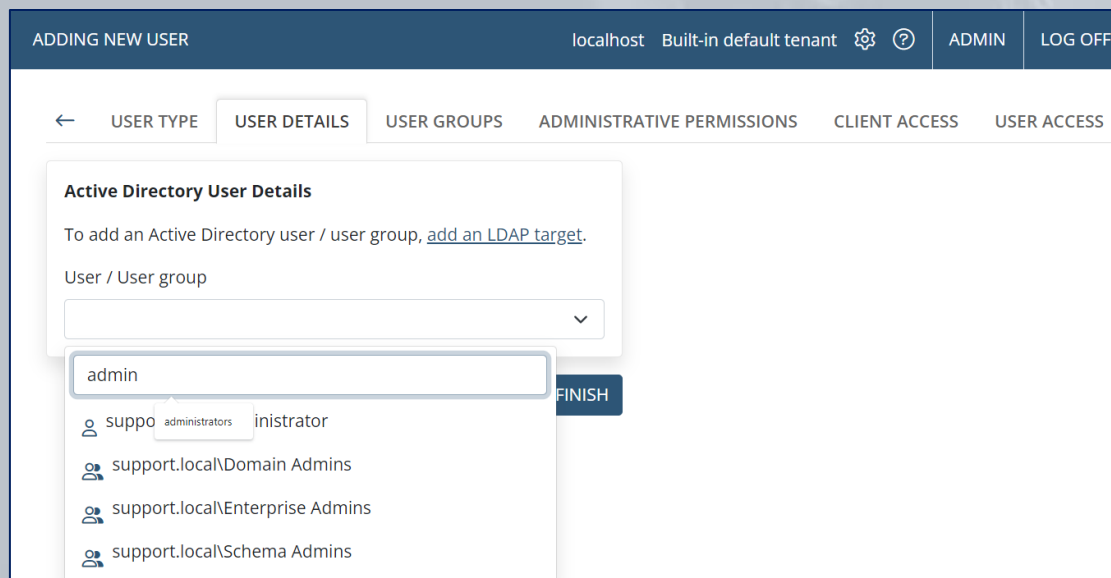
MASTER PANEL ACCESS DATABASE MANAGEMENT APPLICATIONS SSO INTEGRATION

ADD REFRESH AUTOMATIC LDAP TARGET SYNC ACTIVE DIRECTORY USER GROUPS

LDAP PATH 	DOMAIN NAME 	DOMAIN NETBIOS NAME 	USER 	TYPE 	REMOVE ALL
LDAP://10.000.0.000/DC=support,DC=local	support.local	SUPPORT	alex1	Manual 	




Integration with Active Directory allows you to do the following:

- Add **users & user groups** from trusted domains to allow them to access the Management Tool and Client computers with **secondary user authentication** enabled.
- Create **alerts** for domain groups **to quickly respond to suspicious user activity** on Client computers belonging to trusted domains.



The screenshot shows the 'ADDING NEW USER' interface. At the top, there is a navigation bar with 'localhost Built-in default tenant' and 'ADMIN LOG OFF'. Below this is a breadcrumb trail: '← USER TYPE USER DETAILS USER GROUPS ADMINISTRATIVE PERMISSIONS CLIENT ACCESS USER ACCESS'. The main content area is titled 'Active Directory User Details' and contains the instruction: 'To add an Active Directory user / user group, [add an LDAP target](#).' Below this is a dropdown menu labeled 'User / User group' with a search input field containing 'admin'. The dropdown list shows several options: 'admin', 'support administrators inistrator', 'support.local\Domain Admins', 'support.local\Enterprise Admins', and 'support.local\Schema Admins'. A 'FINISH' button is visible to the right of the dropdown.

Audit all **user activities** performed in the Management Tool via the Audit log which contains detailed information on **all changes**.

AUDIT LOG localhost Built-in default tenant   ADMIN LOG OFF EN 

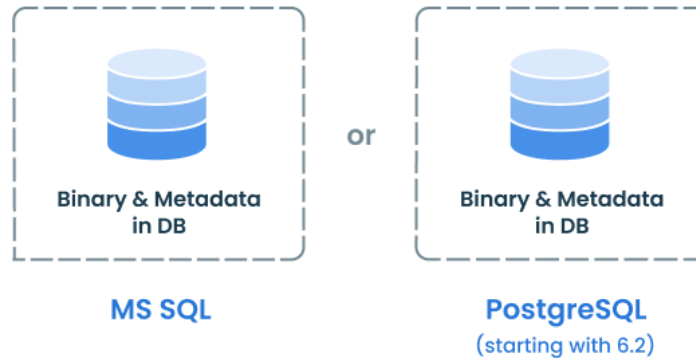
When: All Who: All Action: All [+ More criteria](#) [EXPORT FILTERED RECORDS TO CSV](#) [EXPORT FILTERED RECORDS TO PDF](#)

TIME	USER NAME	USER GROUPS	CATEGORY	ACTION	OBJECT	DETAILS
02/15/2023 11:40...	admin	Administrators	Session viewing	Viewing	WIN10	User: SUPPORT\alex1 Time: 14/12/2022 13:00:49-14/12/2022 13:16:39 View
02/15/2023 11:40...	admin	Administrators	Session viewing	Viewing	WINServer2019	User: WIN-4D\Administrator(pamuser) Time: 20/09/2022 10:57:04-20/09/2022 17:43:07 View
02/15/2023 11:39...	admin	Administrators	Client group editing	Editing settings	Jump Servers	Jump Server mode: No
02/15/2023 11:38...	Pamuser		Secret manager	Using Secret	Support_desktop	Jump Server Name: WINServer2019 Remote IP: 10.1
02/15/2023 11:38...	admin	Administrators	Access management	Granting access	WINServer2019	Approved by: admin Comments: Secret Name: Support_desktop Secret Type: Active Directory account Requested by: support\alex1 (pamuser)
02/15/2023 11:33...	Pamuser		Secret manager	Using Secret	DesktopWin10	Jump Server Name: WINServer2019
02/15/2023 11:31...	Pamuser		Secret manager	Using Secret	WebAccount	Jump Server Name: WINServer2019
02/15/2023 11:31...	Pamuser		Secret manager	Using Secret	WebAccount	Jump Server Name: WINServer2019
02/15/2023 11:31...	Pamuser		Secret manager	Using Secret	DesktopWin10	Jump Server Name: WINServer2019

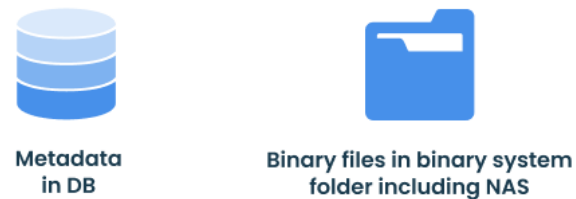
10 50 100 **200** « 1 2 3 4 5 6 »

Database Management

Default Configuration



Custom Configuration (MS SQL or PostgreSQL)



You can configure a **cleanup** (or **archive & cleanup**) operation that can be applied to either a specific **Client** or a specific **Client group**.

Auto-Cleanup options


Never

Run once


Repeat according to schedule

Perform every (days)

Start at

Action type

Sessions older than (days)

It is good practice to archive and delete old monitored data from the database regularly to avoid **running out of space** on the Application Server computer, and to **save the monitored data in secure storage**.

Auto-Cleanup options

Never

Run once

Repeat according to schedule

Action type

Archive & Cleanup ▼

Sessions older than (days)

30

CONFIGURATION

Archive Parameters

Instance

localhost

Archived database name

archivedb

User

postgres

Password

.....

Binary data location:

C:\data\archived

Use separate credentials to access binary storage

User

.....

Password

.....

Delete offline Clients without sessions

TEST DATABASE CONNECTION

Archived sessions in any archived database **can be viewed** in the Session Viewer, and **searches** can be performed on the data, in the usual way at **any time**.

MONITORING RESULTS localhost Built-in default tenant DEVIDAVID.LEE LOG OFF EN

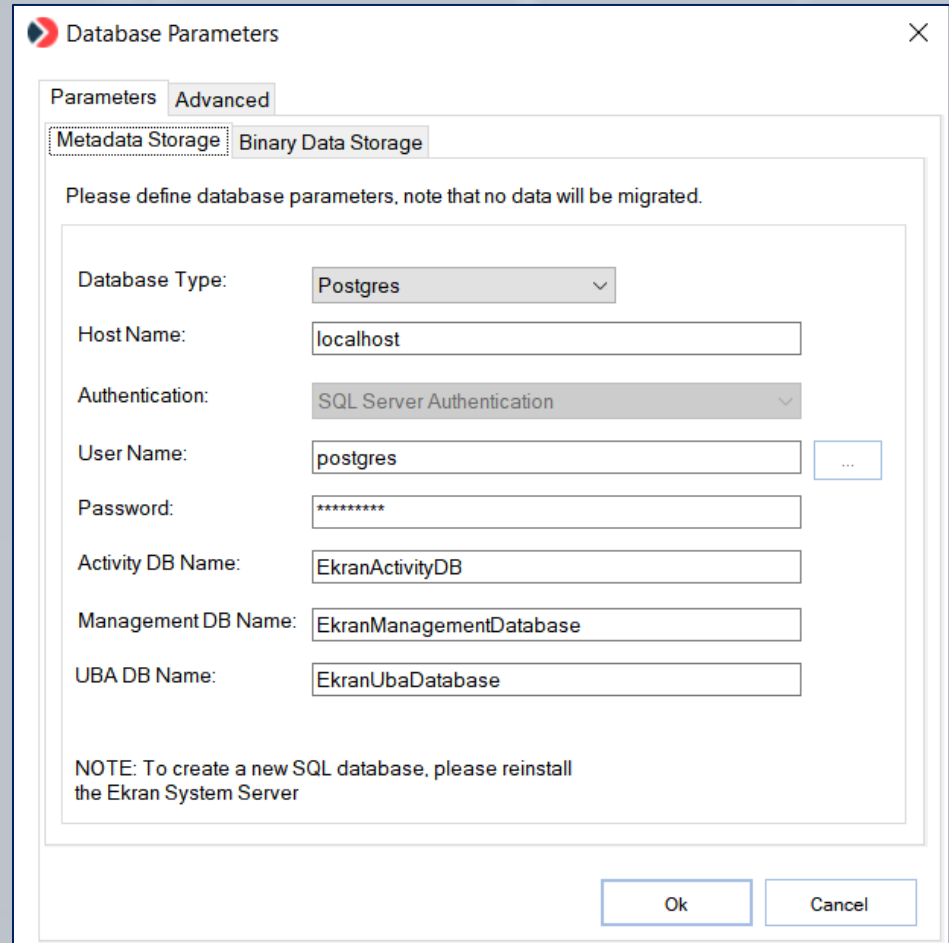
CLIENT SESSIONS ALERTS **ARCHIVED SESSIONS** FILE MONITORING

Select archived database to be investigated:
Archive-Database (es-pg-db.ekran.local) **MANAGE ARCHIVED DATABASE PROFILES**

Who: All Where: All When: All More criteria COLUMNS DISPLAY

PLAY	RISK SC...	ALER...	USER NAME	CLIENT NAME	REMOTE HO...	START	FINISH	DURATION	IPV4	REM...
			user1	RHEL7.6-hal		8:03 pm 13-Jun	8:03 pm	5sec	192.16...	10.10...
			user1	RHEL7.6-hal		8:00 pm 13-Jun	8:03 pm	2min 33sec	192.16...	10.10...
			user1	RHEL7.6-hal		8:00 pm 13-Jun	8:00 pm	8sec	192.16...	10.10...
			ubuntu	ubuntu-20		2:56 pm 09-Jun	2:56 pm	15sec	192.16...	10.20...
			ubuntu	ubuntu-20		1:07 pm 09-Jun	2:13 pm	1h 5min 49sec	192.16...	10.20...
			administrator	DUBL10	HAL-E-PC	7:48 pm 08-Jun	7:48 pm	36sec	192.16...	10.10...
			administrator	DUBL10	HAL-E-PC	7:47 pm 08-Jun	7:47 pm	54sec	192.16...	10.10...
			administrator	DUBL10	HAL-E-PC	7:46 pm 08-Jun	7:46 pm	6sec	192.16...	10.10...

If the **database credentials** defined during installation of the Application Server have been changed (e.g. according to your corporate policy), you can easily **edit them** without reinstalling the Application Server.



Database Parameters

Parameters Advanced

Metadata Storage Binary Data Storage

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

Database Type: Postgres

Host Name: localhost

Authentication: SQL Server Authentication

User Name: postgres

Password: *****

Activity DB Name: EkranActivityDB

Management DB Name: EkranManagementDatabase

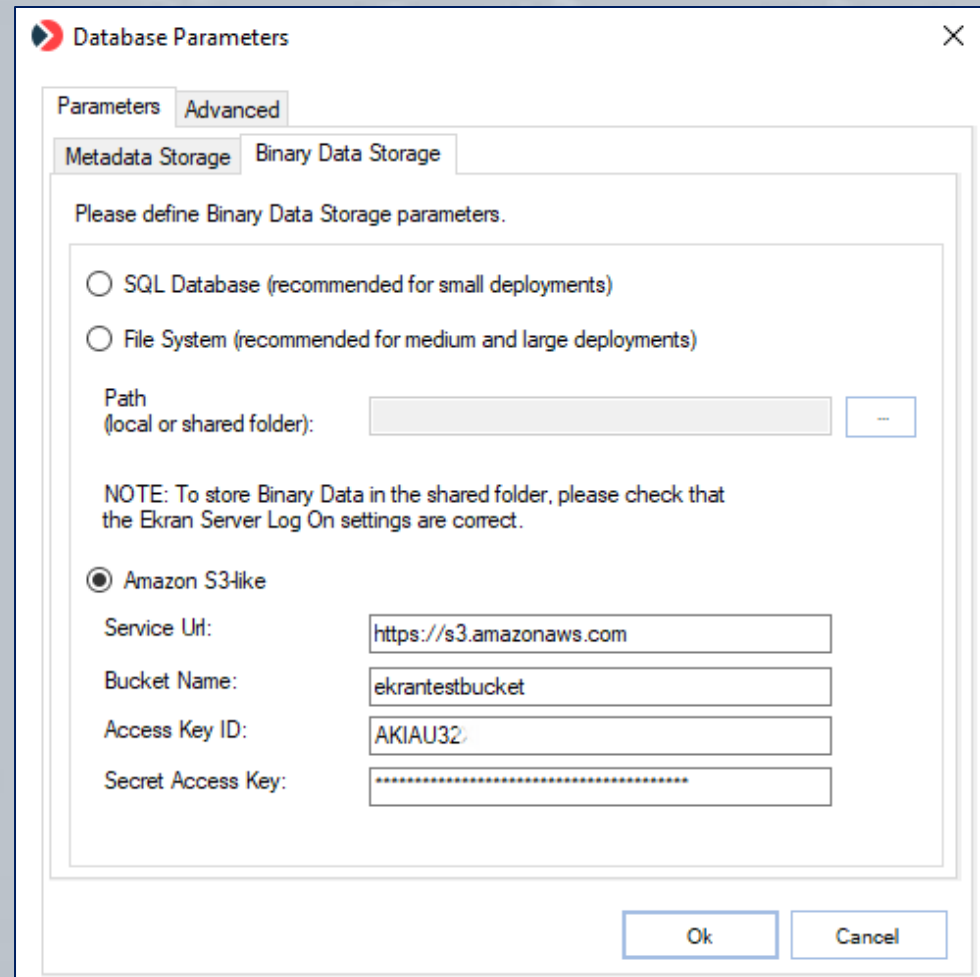
UBA DB Name: EkranUbaDatabase

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

Ok Cancel

A **new location** (e.g. **Amazon S3** storage) can alternatively be used to **store the binary data** (i.e. screen captures) recorded during monitoring.

Network-Attached Storage (NAS) can also be used (by using the **File System** option).



Database Parameters

Parameters Advanced

Metadata Storage Binary Data Storage

Please define Binary Data Storage parameters.

SQL Database (recommended for small deployments)

File System (recommended for medium and large deployments)

Path
(local or shared folder):

NOTE: To store Binary Data in the shared folder, please check that the Ekran Server Log On settings are correct.

Amazon S3-like

Service Url:

Bucket Name:

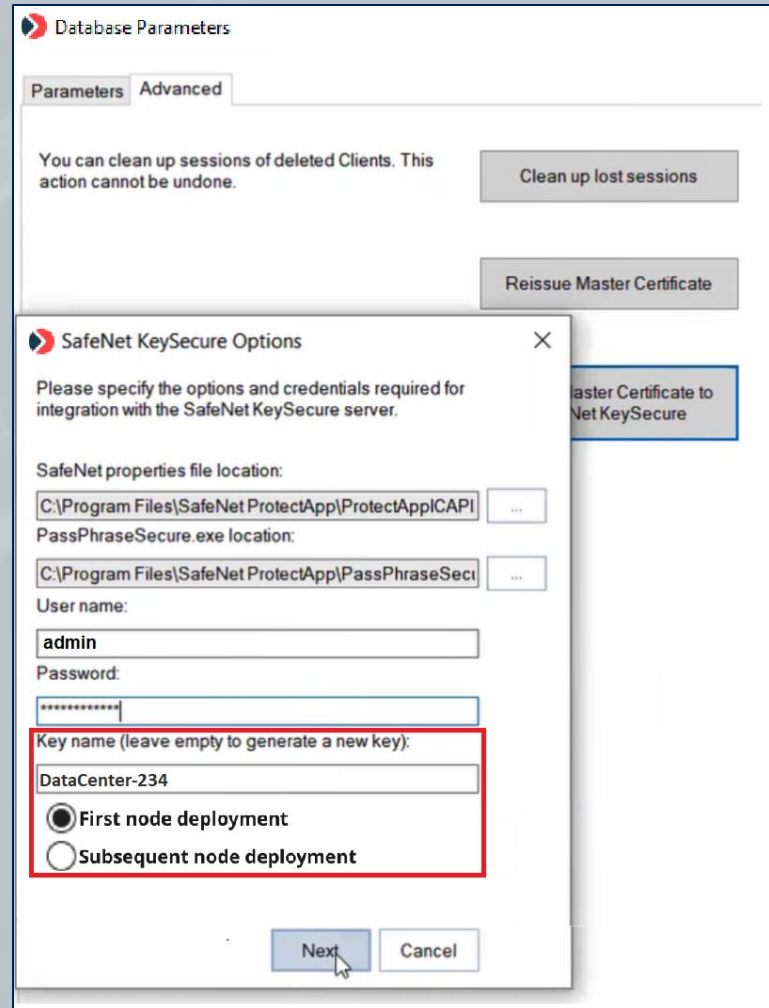
Access Key ID:

Secret Access Key:

Ok Cancel

Database Parameters (Hardware Security Module)

To further enhance security, the RSA-2048 encrypted Ekran System **Master Certificate** can also be **moved** to a Hardware Security Module (**HSM**) **device**, by using **Thales SafeNet KeySecure** with SafeNet ProtectApp.

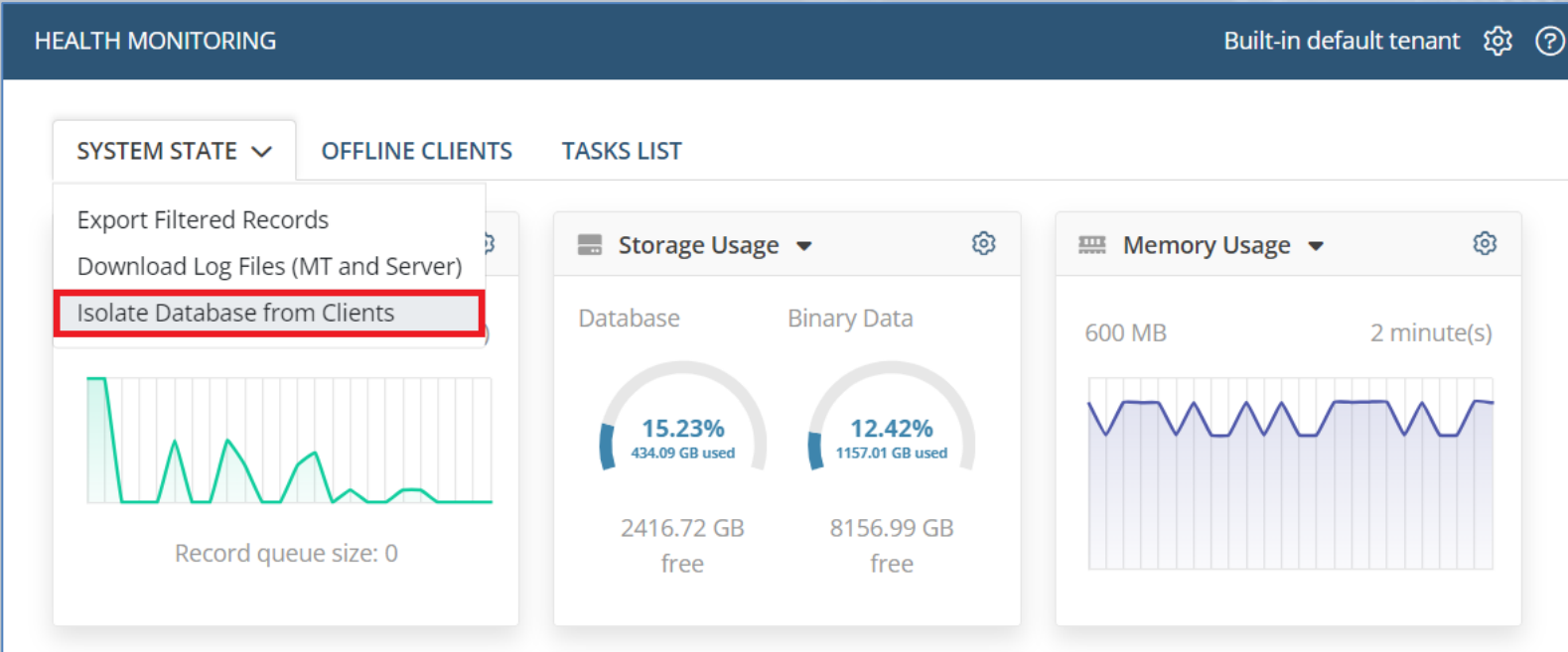


The image shows two overlapping windows from the Ekran System interface. The background window is titled "Database Parameters" and has tabs for "Parameters" and "Advanced". It contains two buttons: "Clean up lost sessions" and "Reissue Master Certificate". The foreground window is titled "SafeNet KeySecure Options" and contains the following fields and options:

- SafeNet properties file location: C:\Program Files\SafeNet ProtectApp\ProtectApp\CAPI\...
- PassPhraseSecure.exe location: C:\Program Files\SafeNet ProtectApp\PassPhraseSeci\...
- User name: admin
- Password: [masked]
- Key name (leave empty to generate a new key): DataCenter-234
- Deployment options: First node deployment, Subsequent node deployment
- Buttons: Next, Cancel

Isolating the Database from Clients

You can **disconnect all Clients** from the **database** to make them go offline, so as to **fix any issues** with the database, and perform database **cleanup and maintenance** without stopping the Ekran System Application Server. Once database operation is restored, you can bring all Clients **back online in just one click**.



The screenshot displays the 'HEALTH MONITORING' dashboard for the 'Built-in default tenant'. The dashboard is divided into three main sections: 'SYSTEM STATE', 'OFFLINE CLIENTS', and 'TASKS LIST'. The 'SYSTEM STATE' section is currently active, showing a dropdown menu with the following options: 'Export Filtered Records', 'Download Log Files (MT and Server)', and 'Isolate Database from Clients'. The 'Isolate Database from Clients' option is highlighted with a red border. Below the menu, there is a line graph showing 'Record queue size: 0'. The 'OFFLINE CLIENTS' section shows 'Storage Usage' for 'Database' (15.23% used, 434.09 GB used, 2416.72 GB free) and 'Binary Data' (12.42% used, 1157.01 GB used, 8156.99 GB free). The 'TASKS LIST' section shows 'Memory Usage' (600 MB, 2 minute(s)) with a line graph.

Ekran System **integrates with your SIEM system** by using the log files of monitored events.

EDITING CLIENT (WIN10)

← 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

Authentication Options Keystroke Monitoring Additional Options

Monitoring Parameters

- Enable clipboard monitoring
- Enable file monitoring
- Detect system IDLE events
- Register IDLE event when user is inactive

Timeout (min)

15

Log Files

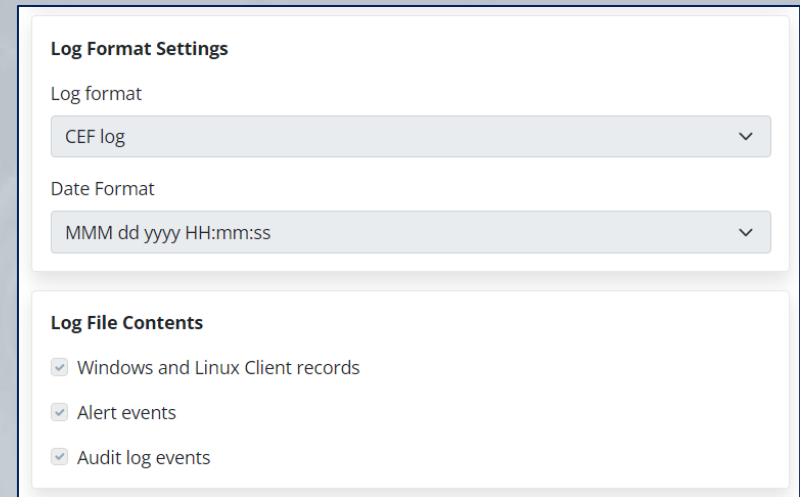
- Enable creating log files of monitored events

Log files location

C:\Ekran System

Get access to Ekran System alert events and monitored data by **creating a separate log file** in one of the following **formats**:

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



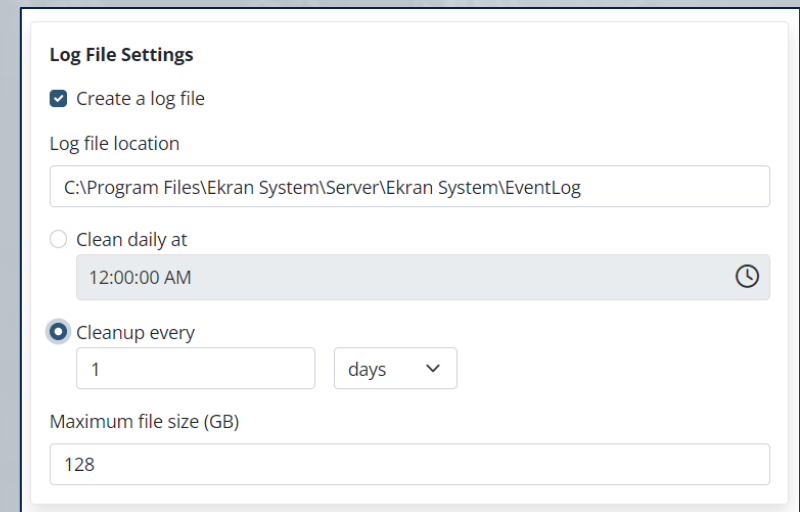
Log Format Settings

Log format
CEF log

Date Format
MMM dd yyyy HH:mm:ss

Log File Contents

- Windows and Linux Client records
- Alert events
- Audit log events



Log File Settings

- Create a log file

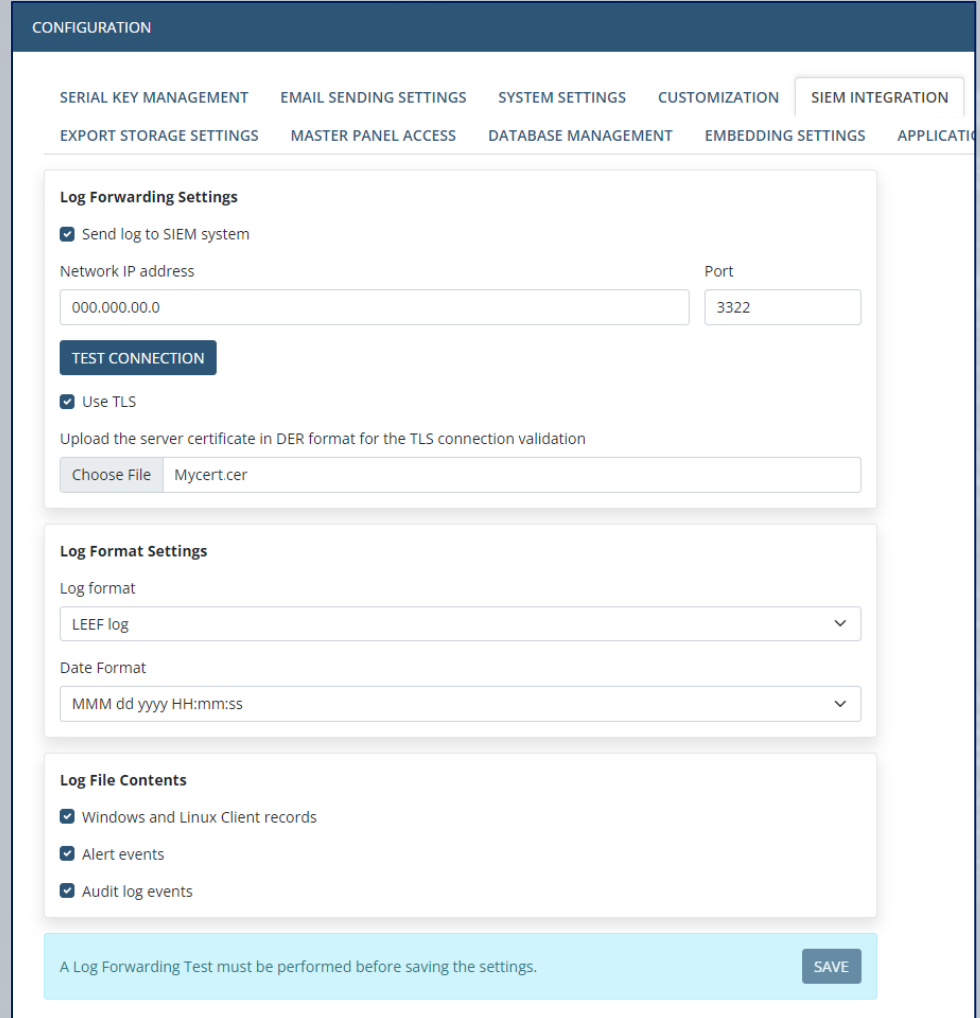
Log file location
C:\Program Files\Ekran System\Server\Ekran System\EventLog

Clean daily at
12:00:00 AM

Cleanup every
1 days

Maximum file size (GB)
128

Ekran System allows the **sending** of records about alert events and monitored data **directly to SIEM systems** such as Splunk, ArcSight, and IBM QRadar, where an encrypted **TLS connection** can also be used to forward the records securely.



The screenshot shows the 'CONFIGURATION' page for 'SIEM INTEGRATION'. The page is divided into three main sections: 'Log Forwarding Settings', 'Log Format Settings', and 'Log File Contents'. A 'TEST CONNECTION' button is located between the first and second sections. A light blue banner at the bottom contains a warning message and a 'SAVE' button.

CONFIGURATION

SERIAL KEY MANAGEMENT EMAIL SENDING SETTINGS SYSTEM SETTINGS CUSTOMIZATION **SIEM INTEGRATION**

EXPORT STORAGE SETTINGS MASTER PANEL ACCESS DATABASE MANAGEMENT EMBEDDING SETTINGS APPLICATIONS

Log Forwarding Settings

- Send log to SIEM system

Network IP address: Port:

TEST CONNECTION

- Use TLS

Upload the server certificate in DER format for the TLS connection validation

Choose File:

Log Format Settings

Log format:

Date Format:

Log File Contents

- Windows and Linux Client records
- Alert events
- Audit log events

A Log Forwarding Test must be performed before saving the settings. **SAVE**

Licensing

(types of licenses, serial key management, and floating endpoint licensing)

Ekran System is **licensed by the number of Ekran System Clients** (i.e. the endpoint computers to be monitored). All management components, including the Application Server and the Management Tool are provided for free with any deployment.

Types of Ekran System Client licenses:

- **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 localhost Built-in default tenant ADMIN LOG OFF EN

←

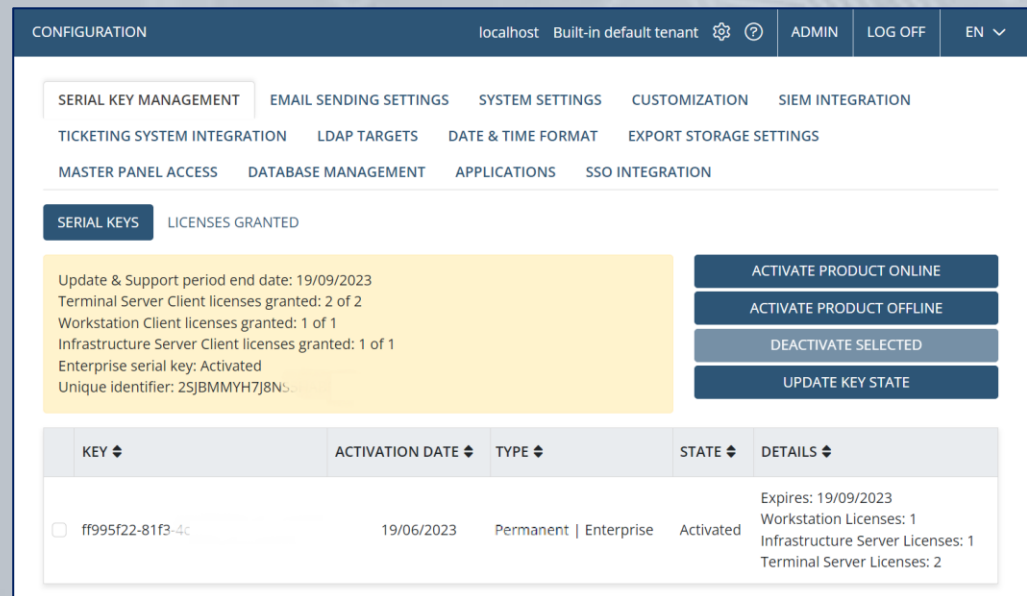
Terminal Server Client licenses used: 2 of 2
Workstation Client licenses used: 1 of 1
Infrastructure Server Client licenses used: 0 of 1
Clients not licensed: 3

<input type="checkbox"/>	NAME	DESCRIP...	RECOMM...	ASSIGNE...	CLIENT G...
<input type="checkbox"/>	WINServer2019		Terminal Server lic...	Terminal Server lic...	Jump Servers
<input type="checkbox"/>	nick-node-2		Terminal Server lic...	Terminal Server lic...	servergroup
<input type="checkbox"/>	WIN10		Workstation license	None	servergroup
<input type="checkbox"/>	UbuntuVM		Infrastructure Serv...	None	
<input type="checkbox"/>	Terminal		Terminal Server lic...	None	DesktopSupport

ASSIGN RECOMMENDED LICENSE
ASSIGN LICENSE OF SPECIFIC TYPE
UNASSIGN LICENSE

You can request a **Trial (or SaaS Trial) serial key** for 30 days to deploy the system and review its features, including those in the Enterprise Edition, and also update the product during this period.

To use Ekran System for a longer period, and with a greater number of Clients, the product needs to be **licensed** by activating purchased serial key on the computer with the Ekran System Application Server installed. You can use either a **Permanent** (aka **Perpetual**), **Subscription** or **SaaS** key.



The screenshot shows the 'SERIAL KEY MANAGEMENT' section of the Ekran System administration interface. The top navigation bar includes 'CONFIGURATION', 'localhost', 'Built-in default tenant', 'ADMIN', 'LOG OFF', and 'EN'. The main menu includes 'SERIAL KEY MANAGEMENT', 'EMAIL SENDING SETTINGS', 'SYSTEM SETTINGS', 'CUSTOMIZATION', 'SIEM INTEGRATION', 'TICKETING SYSTEM INTEGRATION', 'LDAP TARGETS', 'DATE & TIME FORMAT', 'EXPORT STORAGE SETTINGS', 'MASTER PANEL ACCESS', 'DATABASE MANAGEMENT', 'APPLICATIONS', and 'SSO INTEGRATION'. The 'SERIAL KEYS' tab is active, showing a summary of license information and a table of active keys.

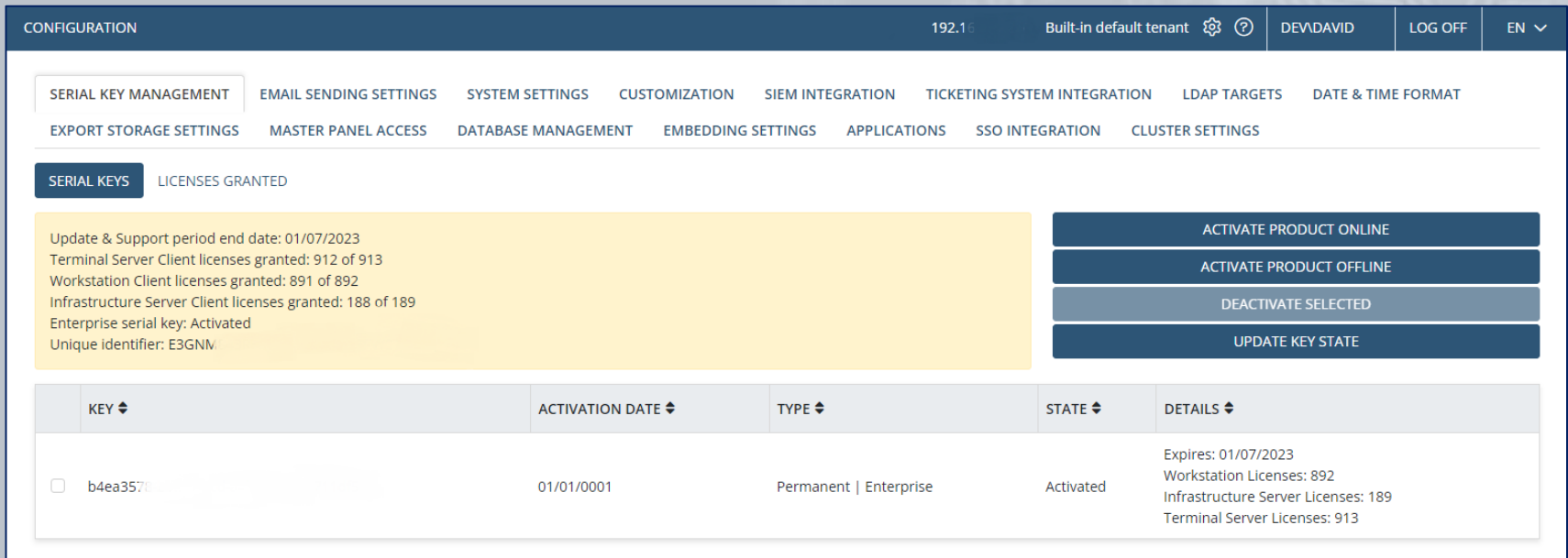
Update & Support period end date: 19/09/2023
Terminal Server Client licenses granted: 2 of 2
Workstation Client licenses granted: 1 of 1
Infrastructure Server Client licenses granted: 1 of 1
Enterprise serial key: Activated
Unique identifier: 25JBMMYH7J8Nb...

ACTIVATE PRODUCT ONLINE
ACTIVATE PRODUCT OFFLINE
DEACTIVATE SELECTED
UPDATE KEY STATE

KEY	ACTIVATION DATE	TYPE	STATE	DETAILS
<input type="checkbox"/> ff95f22-81f3-4c	19/06/2023	Permanent Enterprise	Activated	Expires: 19/09/2023 Workstation Licenses: 1 Infrastructure Server Licenses: 1 Terminal Server Licenses: 2

The Enterprise Serial Key

You can activate an **Enterprise serial key** to get exclusive access to a set of additional valuable features offered only in the **Enterprise Edition** of Ekran System.



The screenshot displays the 'SERIAL KEY MANAGEMENT' section of the Ekran System configuration interface. The top navigation bar includes 'CONFIGURATION', user information '192.168.1.1 Built-in default tenant DEVAVID', and 'LOG OFF'. The main menu lists various settings, with 'SERIAL KEY MANAGEMENT' selected. Below the menu, there are two tabs: 'SERIAL KEYS' (active) and 'LICENSES GRANTED'. A yellow callout box provides summary information: 'Update & Support period end date: 01/07/2023', 'Terminal Server Client licenses granted: 912 of 913', 'Workstation Client licenses granted: 891 of 892', 'Infrastructure Server Client licenses granted: 188 of 189', 'Enterprise serial key: Activated', and 'Unique Identifier: E3GNM'. To the right of this box are four action buttons: 'ACTIVATE PRODUCT ONLINE', 'ACTIVATE PRODUCT OFFLINE', 'DEACTIVATE SELECTED', and 'UPDATE KEY STATE'. Below this is a table with columns for 'KEY', 'ACTIVATION DATE', 'TYPE', 'STATE', and 'DETAILS'. One key is listed with a checkbox, key ID 'b4ea357...', activation date '01/01/0001', type 'Permanent | Enterprise', and state 'Activated'. The details for this key include: 'Expires: 01/07/2023', 'Workstation Licenses: 892', 'Infrastructure Server Licenses: 189', and 'Terminal Server Licenses: 913'.

KEY	ACTIVATION DATE	TYPE	STATE	DETAILS
<input type="checkbox"/> b4ea357...	01/01/0001	Permanent Enterprise	Activated	Expires: 01/07/2023 Workstation Licenses: 892 Infrastructure Server Licenses: 189 Terminal Server Licenses: 913

Ekran System is currently the **only such product on the market** to offer floating endpoint licensing.

This unique functionality allows you to **reassign licenses between Clients** both manually “on the fly”, and automatically, so that you **only need to purchase** the amount of Ekran System Workstation Client **licenses** corresponding to the **maximum possible number** of simultaneously active **Clients**.

- **Manual** reassignment: Can be done **at any time**, in just a **couple of clicks**.
- **Automatic** reassignment:
 - **Delete offline Clients without sessions**: This option allows the licenses of Clients, whenever they do not have sessions stored, to be returned to the pool of available licenses automatically (e.g. after a database cleanup).
 - **Using a golden image** (for VMware/Citrix desktop monitoring): Dynamically assigns licenses to **virtual desktops** whenever new Windows-based desktops are created, and unassigns them whenever Client machines are shut down.

Features only available in the **Enterprise Edition** of Ekran System:

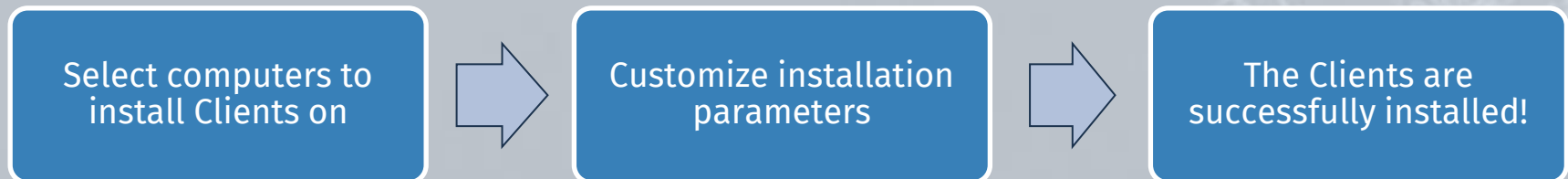
- High Availability
- Load Balancer Support
- Multi-Tenant Mode
- Password Management
- Detection of Disconnected Clients
- Integration with Ticketing Systems
- SIEM Integration
- Access Requests and Approval Workflow
- File Monitoring
- User Behavior Analytics (UEBA)
- Database Archiving
- Remote Host IP Filtering
- Registering Logs to the Windows Event Log
- SWIFT Username Monitoring
- Time-Based Restrictions for User Access
- Anonymizer
- Ekran System API (& Integration with e.g. Power BI)

Installing & Updating Clients

Convenient Ekran Client installation:

- **Locally:**
 - Linux Clients (using a tar.gz file)
 - macOS Clients (using a tar.gz file)
 - Windows Clients:
 - using the installation file with default parameters
 - using a package generated with customized parameters
- **Remotely:**
 - for Windows Clients
 - for macOS Clients (remote mass deployment)

Remote Installation



Target Computers for Remote Installation

- **Scan your local computer network** (Windows Clients)
- Define a **range of IP addresses** to search for the target computers
- Simply enter the target **computer names**

NETWORK SCAN



←


Scan finished. 2 computer(s) detected.

<input type="checkbox"/>	IP ↕	COMPUTER ↕	WORKGROUP / DOMAIN ↕
<input checked="" type="checkbox"/>	10.10	Terminal.support.local (10.10)	
<input type="checkbox"/>	10.10	WINSERVER2019.support.local (10.10)	SUPPORT

NEXT REFRESH STOP


COMPUTERS WITHOUT CLIENTS

localhost Built-in default tenant   ADMIN LOG OFF EN ▾

← 

Define the computers on which Clients will 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

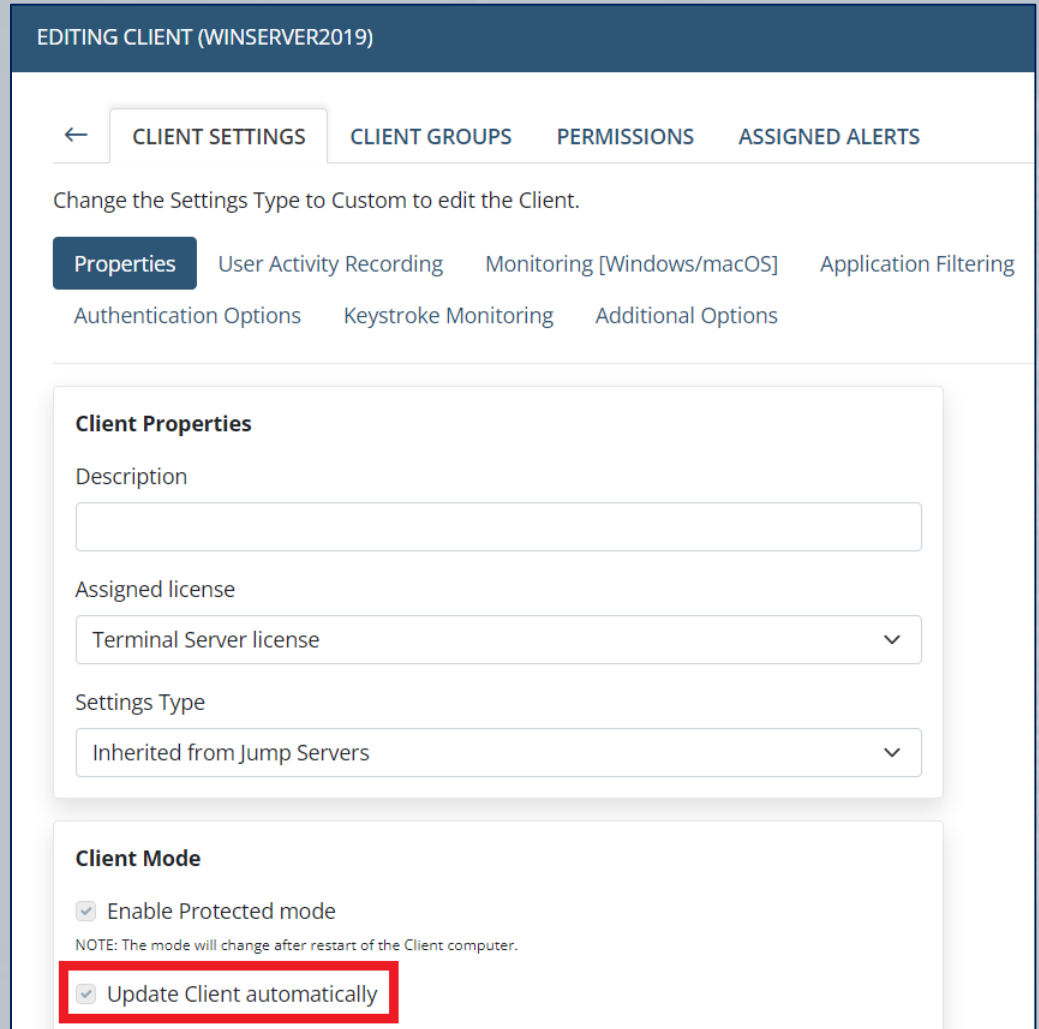
COMPUTER ↕	WORKGROUP / DOMAIN ↕	IP ↕	DESCRIPTION ↕	PREVIOUS INSTALLATION FAILURE ↕	<a>REMOVE ALL
Terminal.support.local		10.10			

READ THE INSTALLATION PREREQUISITES INSTALL INSTALL USING EXISTING .INI FILE

Updating Ekran System Clients

After the Ekran System Application Server is updated to a new version, all **Clients are automatically updated** to the same version on their next connection to the Application Server.

If you want to personally supervise the update process of the target Clients, you can **disable the Update Client automatically** option for them.



EDITING CLIENT (WINSERVER2019)

← 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
Authentication Options Keystroke Monitoring Additional Options

Client Properties

Description

Assigned license
Terminal Server license

Settings Type
Inherited from Jump Servers

Client Mode

Enable Protected mode
NOTE: The mode will change after restart of the Client computer.

Update Client automatically

Monitoring Parameters

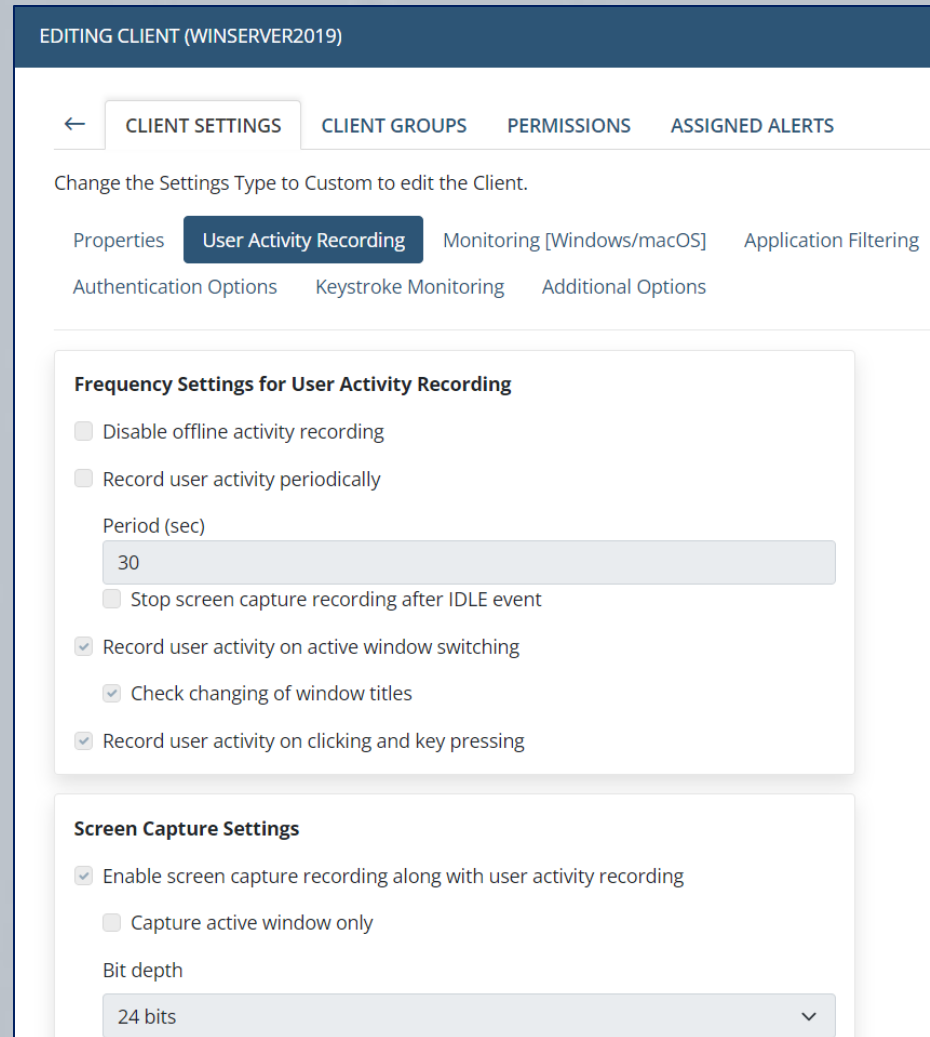
The **screen captures** that the Client sends are stored in the form of deltas (i.e. the differences between a newer recorded screen capture and an older one) to minimize the storage space used.

The information recorded is saved in an easy-to-review and easy-to-search form, including:

- The names of **applications** launched.
- The titles of **active windows**.
- The **URLs** entered.
- Text entered via the user's keyboard (i.e. **keystrokes**).
- **Clipboard** text data (copied/cut or pasted).
- **Commands** executed using **Linux** (from both user input & scripts run) and **responses** output.
- **USB devices** plugged-in.
- File monitoring operations (e.g. **file upload**).
- **Alerts** triggered (on various user activities).

Ekran System Client user activity recording is **event-triggered** by default.

You can easily configure Windows, macOS, and Linux Clients to record screen captures of the active window or to record user activity without recording screen captures, etc.



EDITING CLIENT (WINSERVER2019)

← 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
Authentication Options Keystroke Monitoring Additional Options

Frequency Settings for User Activity Recording

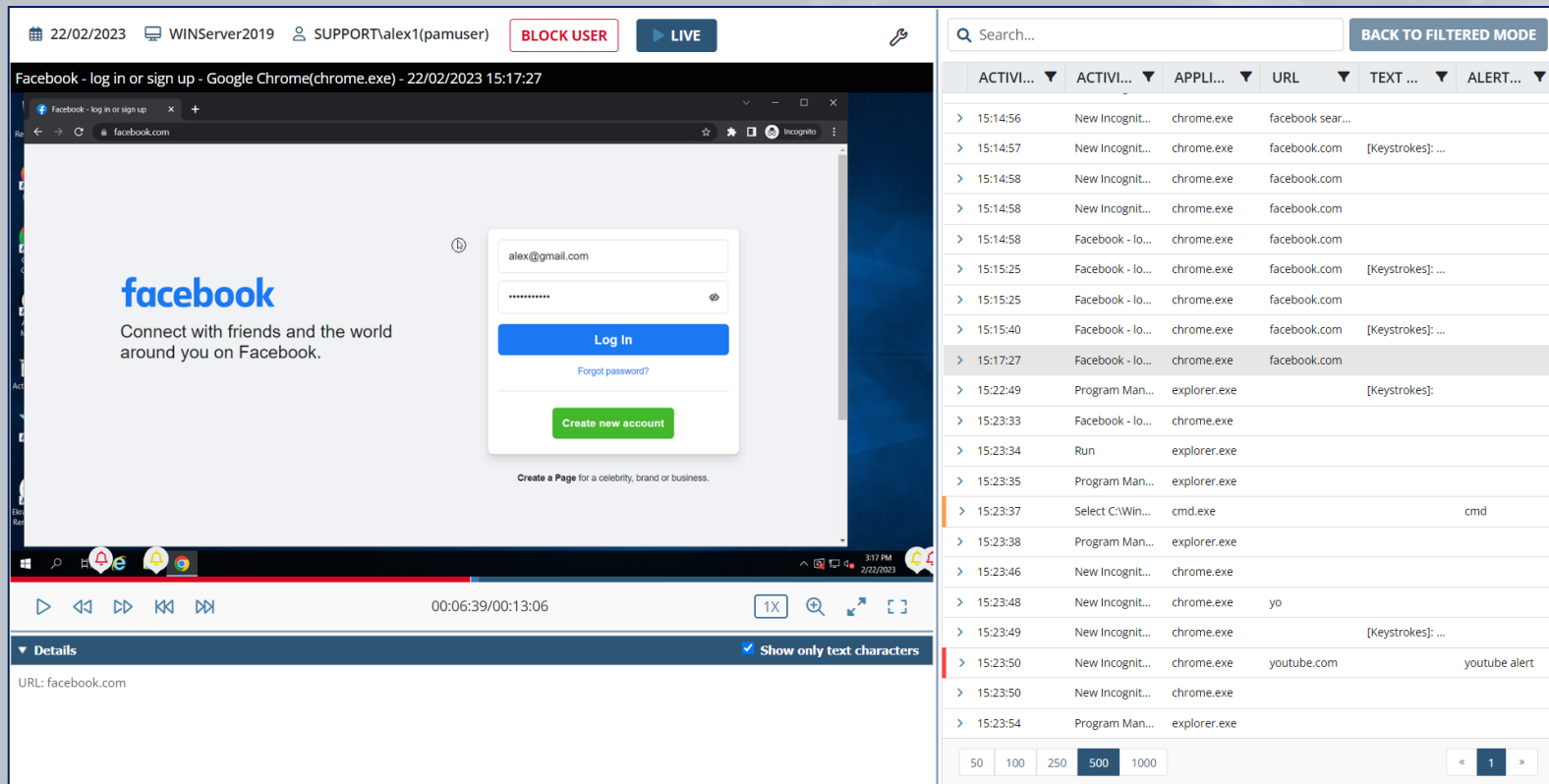
- Disable offline activity recording
- Record user activity periodically
- Period (sec)
30
- Stop screen capture recording after IDLE event
- Record user activity on active window switching
- Check changing of window titles
- Record user activity on clicking and key pressing

Screen Capture Settings

- Enable screen capture recording along with user activity recording
- Capture active window only
- Bit depth
24 bits

The Ekran Client monitors **URLs entered in web browsers.**

You can configure the Client to monitor either full URLs or top and second level domain names only.

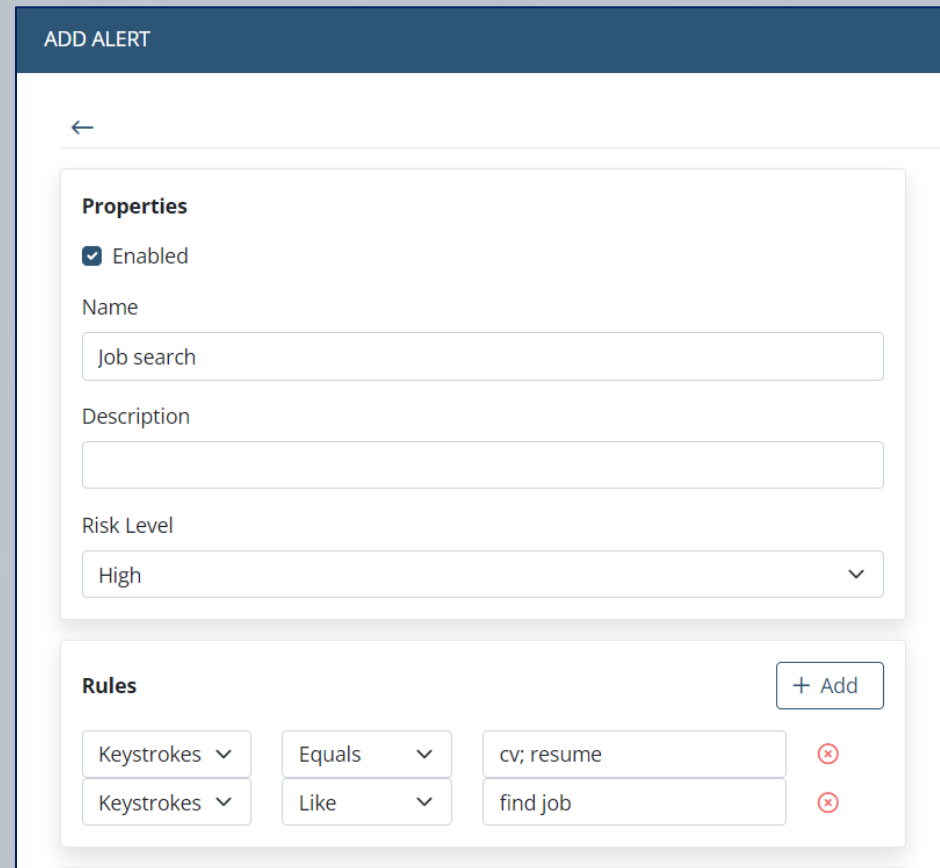


The screenshot displays the Ekran Client interface. On the left, a browser window shows the Facebook login page with the email 'alex@gmail.com' entered. The top of the interface includes a status bar with the date '22/02/2023', system name 'WINServer2019', user 'SUPPORT\alex1(pamuser)', and buttons for 'BLOCK USER' and 'LIVE'. Below the browser window is a 'Details' section showing the URL 'facebook.com'. On the right, a monitoring log table is visible, listing various activities with columns for time, application, and URL. The log shows multiple entries for 'facebook.com' and other applications like 'explorer.exe' and 'cmd.exe'. A search bar and a 'BACK TO FILTERED MODE' button are at the top of the log. At the bottom of the log, there are pagination controls showing '50', '100', '250', '500', and '1000' entries per page, with '1' of 1 page displayed.

ACTIVI...	ACTIVI...	APPLI...	URL	TEXT ...	ALERT...
>	15:14:56	New Incognit...	chrome.exe	facebook sear...	
>	15:14:57	New Incognit...	chrome.exe	facebook.com	[Keystrokes]: ...
>	15:14:58	New Incognit...	chrome.exe	facebook.com	
>	15:14:58	New Incognit...	chrome.exe	facebook.com	
>	15:14:58	Facebook - lo...	chrome.exe	facebook.com	
>	15:15:25	Facebook - lo...	chrome.exe	facebook.com	[Keystrokes]: ...
>	15:15:25	Facebook - lo...	chrome.exe	facebook.com	
>	15:15:40	Facebook - lo...	chrome.exe	facebook.com	[Keystrokes]: ...
>	15:17:27	Facebook - lo...	chrome.exe	facebook.com	
>	15:22:49	Program Man...	explorer.exe		[Keystrokes]:
>	15:23:33	Facebook - lo...	chrome.exe		
>	15:23:34	Run	explorer.exe		
>	15:23:35	Program Man...	explorer.exe		
>	15:23:37	Select C:\Win...	cmd.exe		cmd
>	15:23:38	Program Man...	explorer.exe		
>	15:23:46	New Incognit...	chrome.exe		
>	15:23:48	New Incognit...	chrome.exe	yo	
>	15:23:49	New Incognit...	chrome.exe		[Keystrokes]: ...
>	15:23:50	New Incognit...	chrome.exe	youtube.com	youtube alert
>	15:23:50	New Incognit...	chrome.exe		
>	15:23:54	Program Man...	explorer.exe		

To ensure **compliance** (e.g. with GDPR), **all keystrokes logged are hidden**, but you can **perform searches** on them and **create alerts** to be triggered when specific keywords are typed.

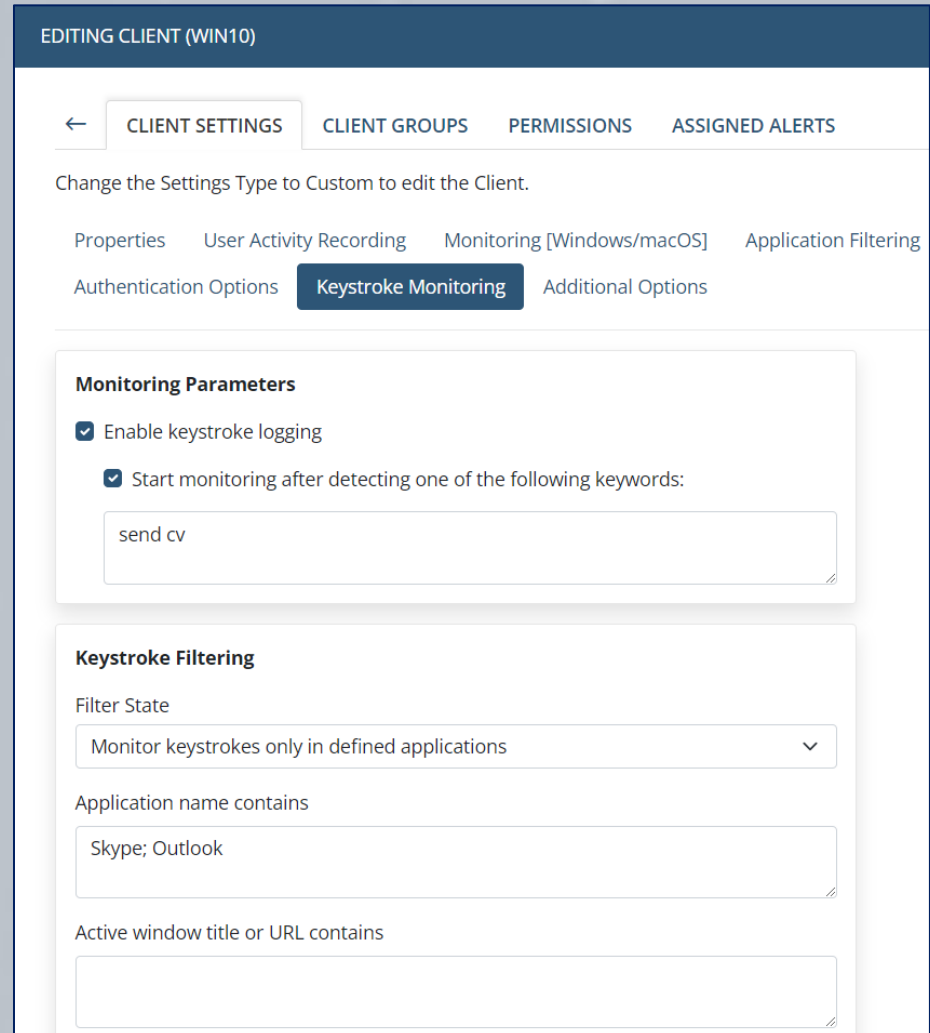
Keystrokes can also be **filtered**. This allows you to both **reduce the amount of data** received from the Client, and to make sure that **no privacy violations** occur by defining the applications for which keystrokes will be monitored.



The screenshot shows the 'ADD ALERT' configuration screen. It features a 'Properties' section with a checked 'Enabled' checkbox, a 'Name' field containing 'Job search', an empty 'Description' field, and a 'Risk Level' dropdown menu set to 'High'. Below this is a 'Rules' section with a '+ Add' button and two existing rules. Each rule consists of a 'Keystrokes' dropdown, an operator dropdown, and a text field with a delete icon. The first rule has 'Keystrokes' selected, 'Equals' as the operator, and 'cv; resume' as the text. The second rule has 'Keystrokes' selected, 'Like' as the operator, and 'find job' as the text.

Keyword-Triggered Monitoring

You can configure Ekran System Clients to start monitoring and recording screen captures only after they **detect** defined **keywords** entered by the user in **specified applications**.



EDITING CLIENT (WIN10)

← 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
Authentication Options **Keystroke Monitoring** Additional Options

Monitoring Parameters

- Enable keystroke logging
 - Start monitoring after detecting one of the following keywords:

Keystroke Filtering

Filter State

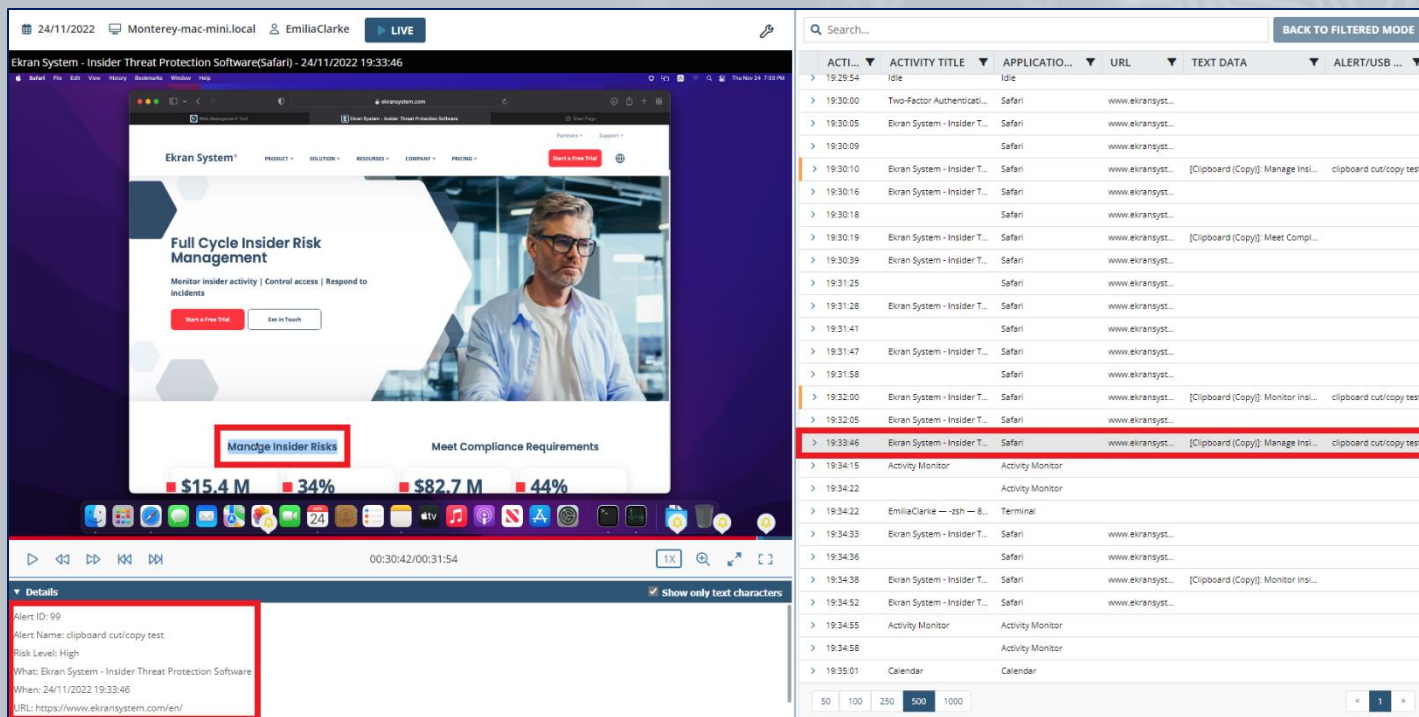
Application name contains

Active window title or URL contains

Clipboard Monitoring

The Ekran Client **captures all text data** that is **copied/cut** from, or **pasted** into documents, files, applications, the browser address bar, etc, on Windows and macOS Client computers.

You can also add an **alert to be triggered** whenever a user copies / pastes.



The screenshot displays the Ekran System interface. On the left, a browser window shows the Ekran System website with a red box highlighting the "Manage Insider Risks" button. On the right, a log table shows various activity events. The event at 19:33:46 is highlighted in red, showing a clipboard copy action with the text "[Clipboard (Copy)] Manage Insi...". Below the log, a "Details" panel shows the alert information for this event.

ACTI...	ACTIVITY TITLE	APPLICATIO...	URL	TEXT DATA	ALERT/USB ...
19:29:54	Idle	Idle			
19:30:00	Two-Factor Authenticati...	Safari	www.ekransyst...		
19:30:05	Ekran System - Insider T...	Safari	www.ekransyst...		
19:30:09	Ekran System - Insider T...	Safari	www.ekransyst...		
19:30:10	Ekran System - Insider T...	Safari	www.ekransyst...	[Clipboard (Copy)] Manage Insi...	clipboard out/copy test
19:30:16	Ekran System - Insider T...	Safari	www.ekransyst...		
19:30:18	Ekran System - Insider T...	Safari	www.ekransyst...		
19:30:19	Ekran System - Insider T...	Safari	www.ekransyst...	[Clipboard (Copy)] Meet Compl...	
19:30:39	Ekran System - Insider T...	Safari	www.ekransyst...		
19:31:25	Ekran System - Insider T...	Safari	www.ekransyst...		
19:31:28	Ekran System - Insider T...	Safari	www.ekransyst...		
19:31:41	Ekran System - Insider T...	Safari	www.ekransyst...		
19:31:47	Ekran System - Insider T...	Safari	www.ekransyst...		
19:31:58	Ekran System - Insider T...	Safari	www.ekransyst...		
19:32:00	Ekran System - Insider T...	Safari	www.ekransyst...	[Clipboard (Copy)] Monitor Insi...	clipboard out/copy test
19:32:05	Ekran System - Insider T...	Safari	www.ekransyst...		
19:33:46	Ekran System - Insider T...	Safari	www.ekransyst...	[Clipboard (Copy)] Manage Insi...	clipboard out/copy test
19:34:15	Activity Monitor	Activity Monitor			
19:34:22	Activity Monitor	Activity Monitor			
19:34:22	EmiliaClarke — ssh — 8...	Terminal			
19:34:33	Ekran System - Insider T...	Safari	www.ekransyst...		
19:34:36	Ekran System - Insider T...	Safari	www.ekransyst...		
19:34:38	Ekran System - Insider T...	Safari	www.ekransyst...	[Clipboard (Copy)] Monitor Insi...	
19:34:52	Ekran System - Insider T...	Safari	www.ekransyst...		
19:34:55	Activity Monitor	Activity Monitor			
19:34:58	Activity Monitor	Activity Monitor			
19:35:01	Calendar	Calendar			

Details

Alert ID: 99
Alert Name: clipboard_out/copy test
Risk Level: High
What: Ekran System - Insider Threat: Protection Software
When: 24/11/2022 19:33:46
URL: https://www.ekransystem.com/en/

Ekran System allows you to define **filtering rules** for **websites** and **applications** to adjust the amount of monitored data, and to exclude areas where personal information can be observed, so as to **comply with corporate policy rules** and **country regulations** (e.g. GDPR) related to user **privacy**.

EDITING CLIENT (WIN10)

← 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**

Authentication Options Keystroke Monitoring Additional Options

Application Filtering

Filter State

Monitor all activity except ▾

Application name contains

chrome; internet explorer, firefox

Active window title or URL contains

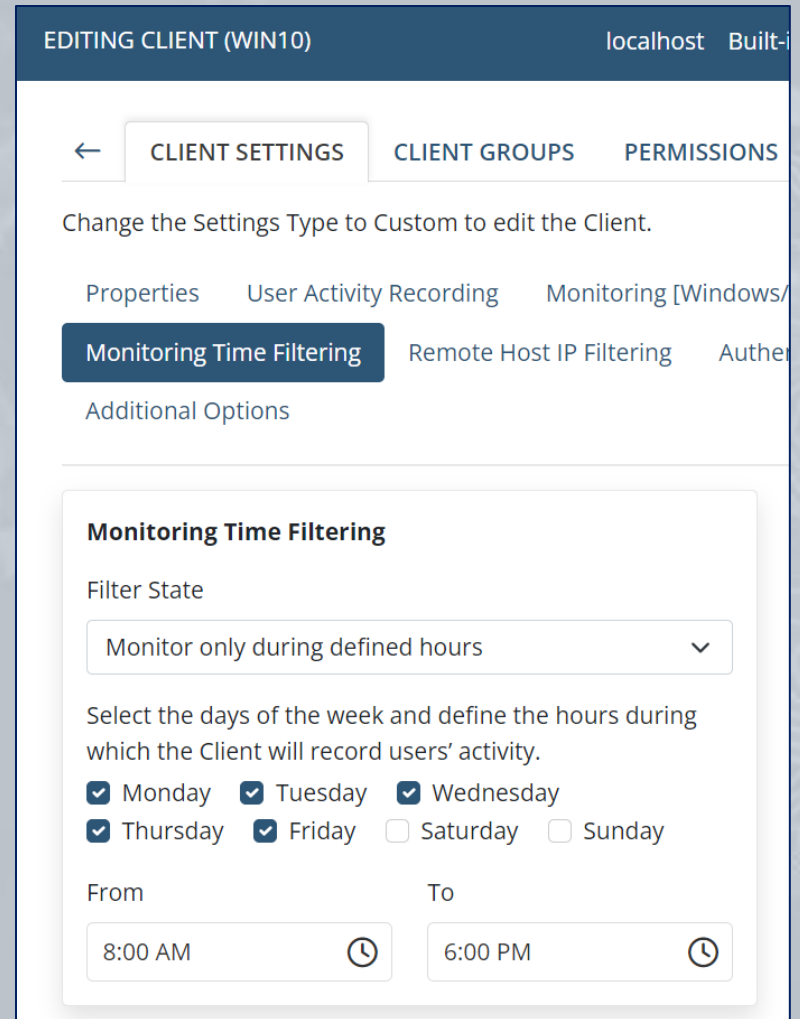
facebook, twitter

NEXT **FINISH**

Monitoring Time Filtering

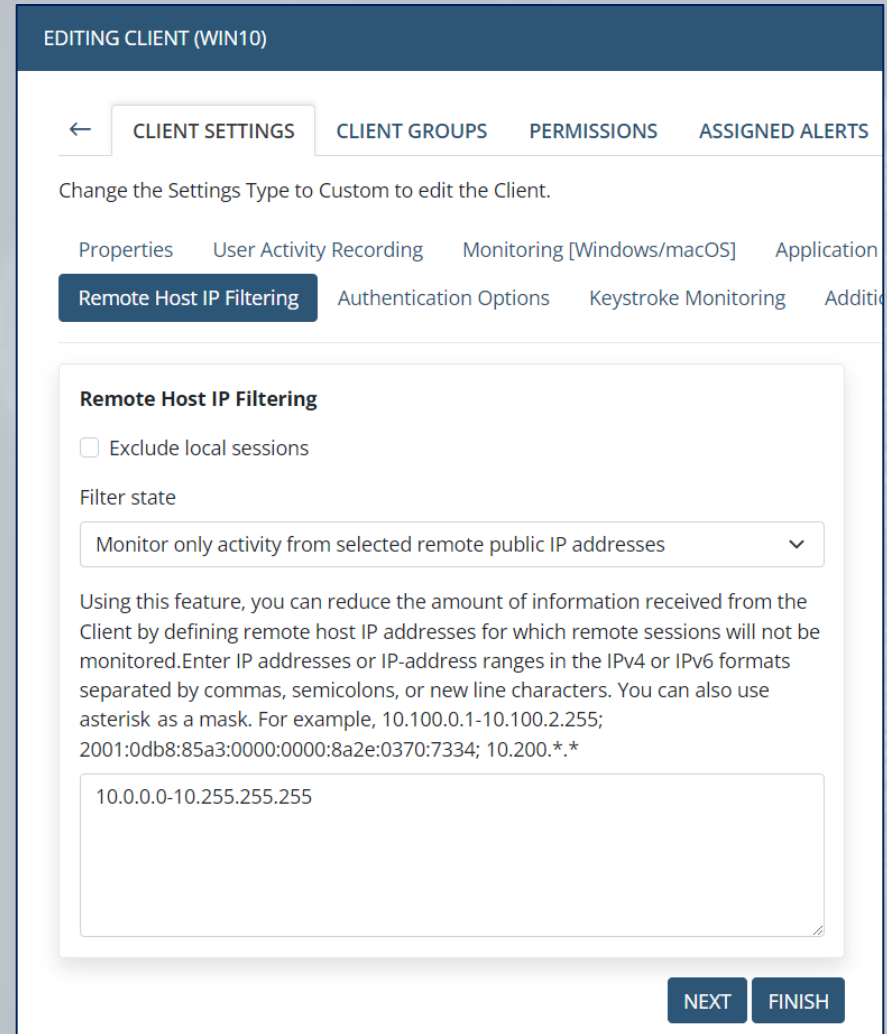
In addition to application filtering rules, you can also define rules for the **time when monitoring** will take place.

By selecting certain **days of the week** and defining **specific hours**, you can establish bounds within which Ekran System Clients will record all user activity.



The screenshot displays the 'EDITING CLIENT (WIN10)' interface. At the top right, it shows 'localhost Built-i'. Below the title bar, there are navigation tabs: 'CLIENT SETTINGS' (selected), 'CLIENT GROUPS', and 'PERMISSIONS'. A message states: 'Change the Settings Type to Custom to edit the Client.' Below this, there are several tabs: 'Properties', 'User Activity Recording', 'Monitoring [Windows/...', 'Monitoring Time Filtering' (selected), 'Remote Host IP Filtering', and 'Authen...'. Under the 'Monitoring Time Filtering' tab, there is a section titled 'Monitoring Time Filtering'. It includes a 'Filter State' dropdown menu set to 'Monitor only during defined hours'. Below this, a message says: 'Select the days of the week and define the hours during which the Client will record users' activity.' There are checkboxes for days 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'. Both fields have a clock icon for time selection.

Additionally, you can **filter** sessions from **certain remote** (public or private) **IP addresses**, or only monitor sessions from certain IP addresses.



EDITING CLIENT (WIN10)

← 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
Remote Host IP Filtering Authentication Options Keystroke Monitoring Additi

Remote Host IP Filtering

Exclude local sessions

Filter state

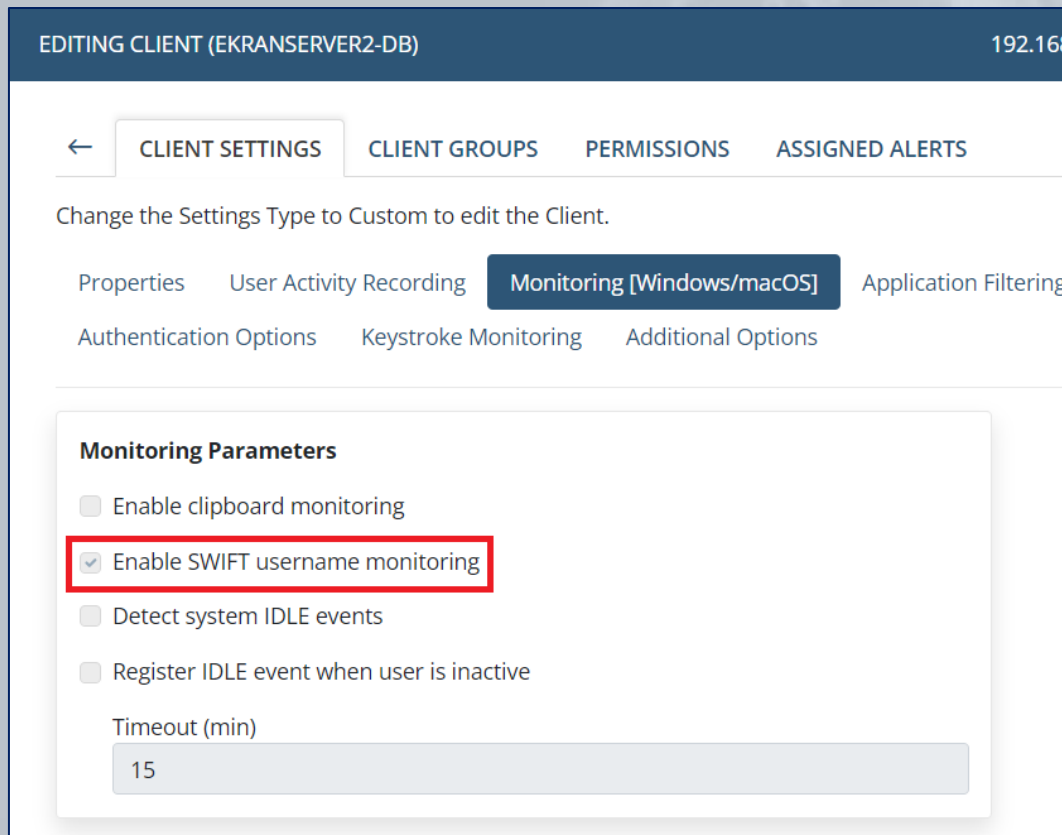
Monitor only activity from selected remote public IP addresses ▾

Using this feature, you can reduce the amount of information received from the Client by defining remote host IP addresses for which remote sessions will not be monitored. Enter IP addresses or IP-address ranges in the IPv4 or IPv6 formats separated by commas, semicolons, or new line characters. You can also 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.*.*

10.0.0.0-10.255.255.255

NEXT FINISH

Ekran System allows the **username** used when logging in to the **SWIFT** network to be recorded, so that you can easily identify such users.



EDITING CLIENT (EKANSERVER2-DB) 192.168.

← 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

Authentication Options Keystroke Monitoring Additional Options

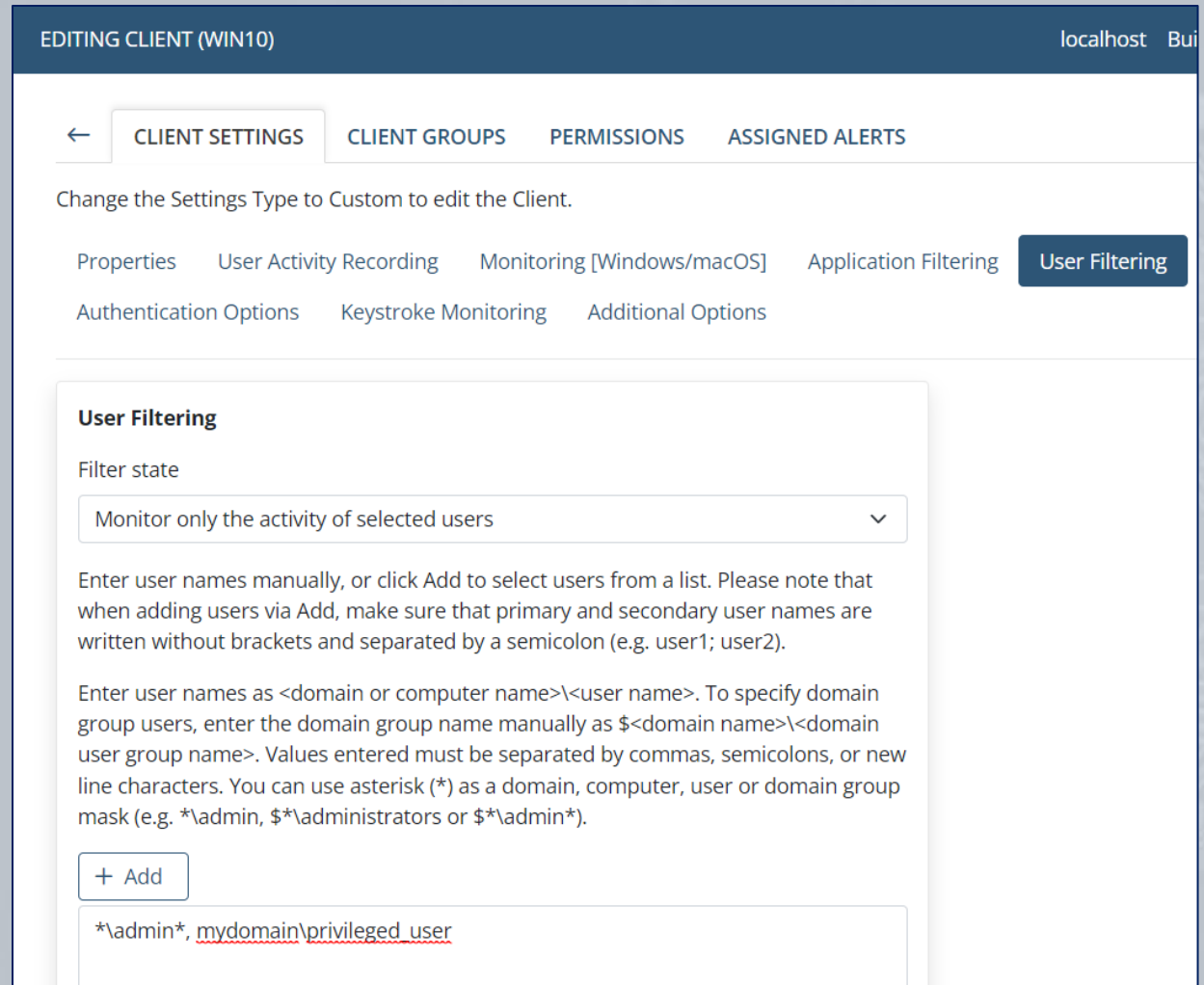
Monitoring Parameters

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

Timeout (min)

15

You can also monitor the activity of users logging in under **privileged access accounts**.



EDITING CLIENT (WIN10) localhost Bui

← 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**

Authentication Options Keystroke Monitoring Additional Options

User Filtering

Filter state

Monitor only the activity of selected users

Enter user names manually, or click Add to select users from a list. Please note that when adding users via Add, make sure that primary and secondary user names are written without brackets and separated by a semicolon (e.g. user1; user2).

Enter user names as <domain or computer name>\<user name>. To specify domain group users, enter the domain group name manually as \$<domain name>\<domain user group name>. Values entered must be separated by commas, semicolons, or new line characters. You can use asterisk (*) as a domain, computer, user or domain group mask (e.g. *\admin, \$*\administrators or \$*\admin*).

+ Add

\admin, mydomain\privileged_user

Ekran System allows you to configure various **bandwidth usage reduction** parameters to manage the **traffic volume** from the Client to the Ekran System Application Server.

EDITING CLIENT (WIN10)

← 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
Authentication Options Keystroke Monitoring **Additional Options**

Additional Options

Screen capture throttling (ms)

Batch registration timeout (ms)

Prevent loading hooks into the following applications

Reduce screen capture size by (%)

Screenshot compression level (1-9)

Agent memory limit (0-disabled)

File monitoring operations (e.g. **file upload**) can be detected, including in many applications such as common browsers and messaging apps.

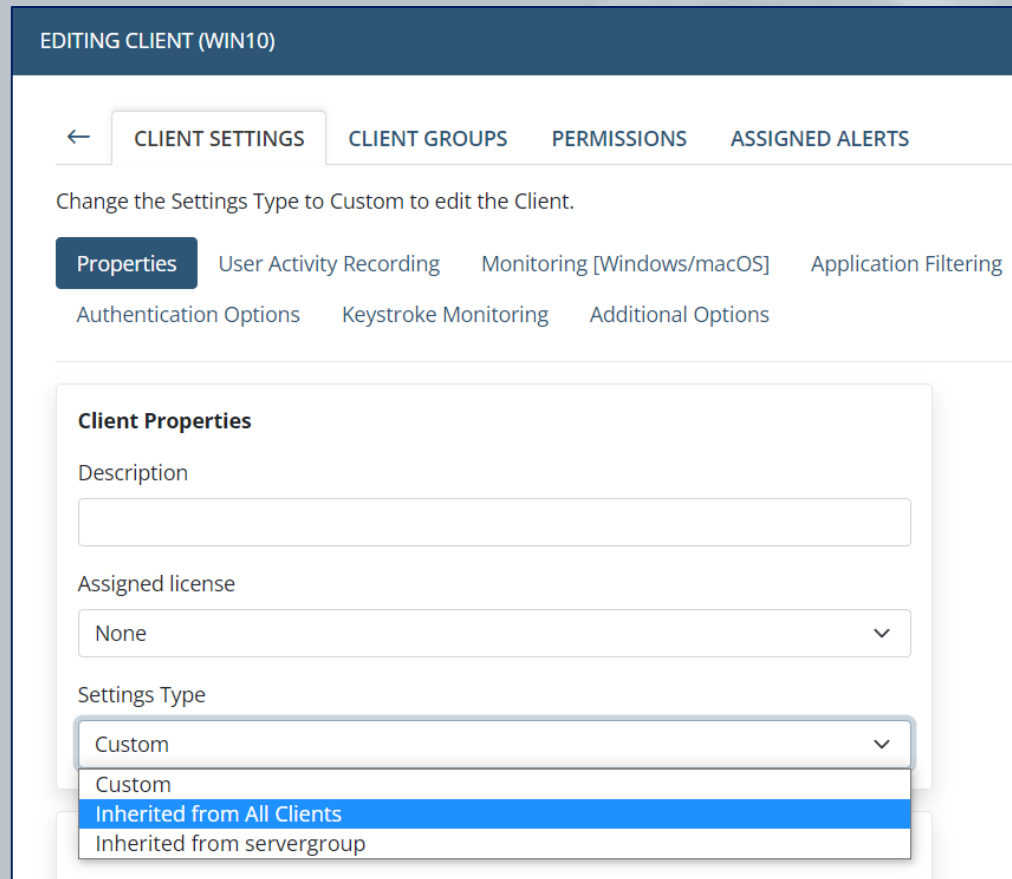
The screenshot displays the Ekran monitoring interface. On the left, a browser window shows a Google search for 'facebook'. A red box highlights the 'Uploading...' progress indicator in the search results. Below the browser, a red box highlights the alert details:

Alert ID: 19218
Alert Name: david file upload
Risk Level: Normal
What: facebook - Google Search - Google Chrome
When: 12/07/2023 18:54:28
URL: google.com/search?q=facebook&riz=1C1GCEU_enUA1022UA1022&oq=facebook&gs_lcrp=EgZjaHJvbnUqBwgAEAAyJwlyBwgAEAAyJwlyDQgBEC4YxwEY0QMYYgAQyBwgCEAAyAQyBw8

On the right, the activity log table shows a list of events. A red box highlights the entry corresponding to the file upload:

A...	ACTIVITY ...	A...	URL	TEXT DATA	ALERT/USB ...
>	18:53:...	Facebook - log in ...	chrom...	facebook...	
>	18:53:...	Facebook - log in ...	chrom...	facebook...	[Keystrokes]: faceboo...
>	18:53:...	Facebook - log in ...	chrom...	facebook...	
>	18:54:...	Facebook - log in ...	chrom...	facebook...	[Keystrokes]:
>	18:54:...	Facebook - log in ...	chrom...	facebook...	[Keystrokes]: copy
>	18:54:...	Facebook - log in ...	chrom...	facebook...	[Keystrokes]:
>	18:54:...	Facebook - log in ...	chrom...	facebook...	[Clipboard (Copy)]: copy david clipboard copy...
>	18:54:...	Facebook - log in ...	chrom...	facebook...	
>	18:54:...	Facebook - log in ...	chrom...	facebook...	[Clipboard (Paste)]: co... david clipboard pasti...
>	18:54:...	Facebook - log in ...	chrom...	facebook...	
>	18:54:...	Facebook - log in ...	chrom...	facebook...	
>	18:54:...	Get back on Face...	chrom...	facebook...	
>	18:54:...	Get back on Face...	chrom...	facebook...	
>	18:54:...	Facebook - log in ...	chrom...	facebook...	
>	18:54:...	facebook - Google...	chrom...	google.com	
>	18:54:...	Open	chrom...		
>	18:54:...	facebook - Google...	chrom...	google.com	
>	18:54:...	facebook - Google...	chrom...	google.com	File operation (Upload... david file upload
>	18:54:...	facebook - Google...	chrom...	google.com	
>	18:54:...	Google Lens - Goo...	chrom...	lens.google...	
>	18:54:...	Google Lens - Goo...	chrom...	lens.google...	
>	18:54:...	facebook - Google...	chrom...	google.com	

You can define the settings for a Client group, and then **apply them to Clients** by inheritance, so as to save time.



EDITING CLIENT (WIN10)

← 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
Authentication Options Keystroke Monitoring Additional Options

Client Properties

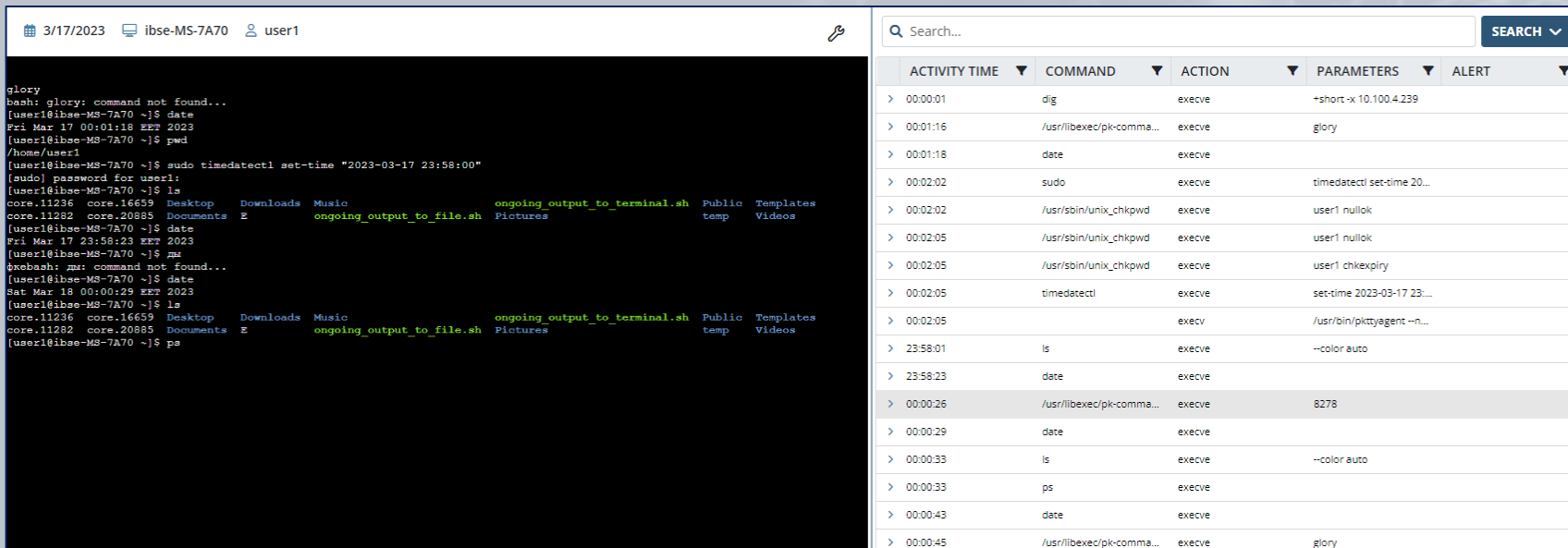
Description

Assigned license
None

Settings Type
Custom

- Custom
- Inherited from All Clients**
- Inherited from servergroup

Ekran System **remote SSH session monitoring** provides the capability to **monitor commands, parameters, and keystrokes input** as well as **function calls** executed and responses **output** in the terminal, and applications opened by users including in **x-forwarded** sessions.



The screenshot displays the Ekran System monitoring interface. On the left, a terminal window shows a user session on a Linux machine (ibse-MS-7A70) with the following commands and output:

```
glory
bash: glory: command not found...
[user1@ibse-MS-7A70 ~]$ date
Fri Mar 17 00:01:18 EET 2023
[user1@ibse-MS-7A70 ~]$ pwd
/home/user1
[user1@ibse-MS-7A70 ~]$ sudo timedatectl set-time "2023-03-17 23:58:00"
[sudo] password for user1:
[user1@ibse-MS-7A70 ~]$ ls
core.11236 core.16659 Desktop Downloads Music ongoing_output_to_terminal.sh Public Templates
core.11282 core.20885 Documents E ongoing_output_to_file.sh Pictures temp Videos
[user1@ibse-MS-7A70 ~]$ date
Fri Mar 17 23:58:23 EET 2023
[user1@ibse-MS-7A70 ~]$ ms
$kebash: ms: command not found...
[user1@ibse-MS-7A70 ~]$ date
Sat Mar 18 00:00:29 EET 2023
[user1@ibse-MS-7A70 ~]$ ls
core.11236 core.16659 Desktop Downloads Music ongoing_output_to_terminal.sh Public Templates
core.11282 core.20885 Documents E ongoing_output_to_file.sh Pictures temp Videos
[user1@ibse-MS-7A70 ~]$ pa
```

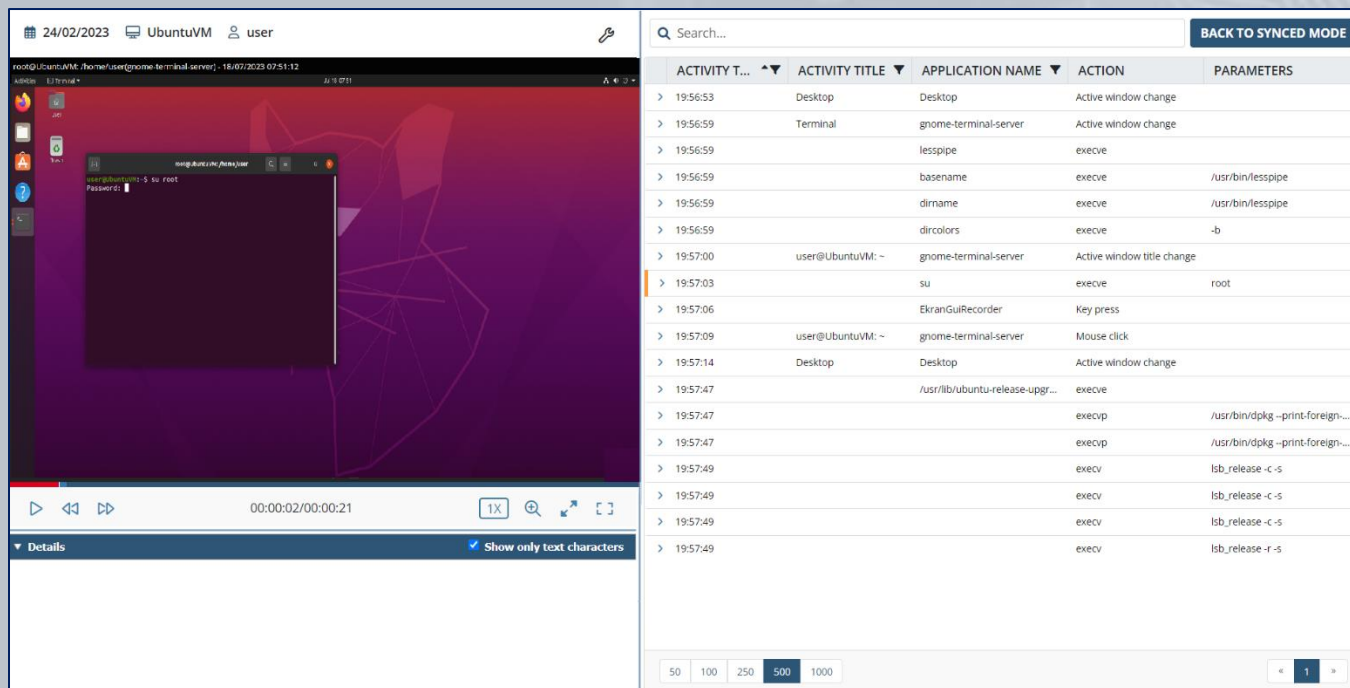
On the right, an activity log table tracks the session's actions:

ACTIVITY TIME	COMMAND	ACTION	PARAMETERS	ALERT
> 00:00:01	dig	execve	+short-x 10.100.4.239	
> 00:01:16	/usr/libexec/pk-comm...	execve	glory	
> 00:01:18	date	execve		
> 00:02:02	sudo	execve	timedatectl set-time 20...	
> 00:02:02	/usr/sbin/unix_chkpwd	execve	user1 nullok	
> 00:02:05	/usr/sbin/unix_chkpwd	execve	user1 nullok	
> 00:02:05	/usr/sbin/unix_chkpwd	execve	user1 chkexpiry	
> 00:02:05	timedatectl	execve	set-time 2023-03-17 23:...	
> 00:02:05		execv	/usr/bin/pktyagent --n...	
> 23:58:01	ls	execve	--color auto	
> 23:58:23	date	execve		
> 00:00:26	/usr/libexec/pk-comm...	execve	8278	
> 00:00:29	date	execve		
> 00:00:33	ls	execve	--color auto	
> 00:00:33	ps	execve		
> 00:00:43	date	execve		
> 00:00:45	/usr/libexec/pk-comm...	execve	glory	

Monitoring of Linux **sessions started locally** via the GUI (**X Window System**) is also supported.

A local Linux Client session for X Window System includes:

- Screen captures
- Activity times
- Activity titles
- Application names / Commands
- Actions / System function calls
- Parameters



The screenshot displays the Ekran system monitoring interface. On the left, a terminal window shows a user logging in as root. On the right, a table lists system activity events.

ACTIVITY T...	ACTIVITY TITLE	APPLICATION NAME	ACTION	PARAMETERS
> 19:56:53	Desktop	Desktop	Active window change	
> 19:56:59	Terminal	gnome-terminal-server	Active window change	
> 19:56:59		lesspipe	execve	
> 19:56:59		basename	execve	/usr/bin/lesspipe
> 19:56:59		dirname	execve	/usr/bin/lesspipe
> 19:56:59		dircolors	execve	-b
> 19:57:00	user@UbuntuVM: ~	gnome-terminal-server	Active window title change	
> 19:57:03		su	execve	root
> 19:57:06		EkranGuiRecorder	Key press	
> 19:57:09	user@UbuntuVM: ~	gnome-terminal-server	Mouse click	
> 19:57:14	Desktop	Desktop	Active window change	
> 19:57:47		/usr/lib/ubuntu-release-upgr...	execve	
> 19:57:47		execvp	execvp	/usr/bin/dpkg --print-foreign...
> 19:57:47		execvp	execvp	/usr/bin/dpkg --print-foreign...
> 19:57:49		execv	execv	lbb_release -c -s
> 19:57:49		execv	execv	lbb_release -c -s
> 19:57:49		execv	execv	lbb_release -c -s
> 19:57:49		execv	execv	lbb_release -r -s

A **remote SSH Linux Client session** can be searched for:

- **User actions** (keystrokes and commands & parameters **input**), and responses **output** from a terminal.
- System **function calls**.
- **Commands** executed in scripts run.

	ACTIVITY TIME ▼	COMMAND ▼	ACTION ▼	PARAMETERS
>	16:14:36	who	execve	
>	16:14:36	kill	kill	0
>	16:14:45	kill	kill	0
>	16:14:45	cat	execve	/home/user/Desktop/hhs.txt
>	16:14:47	kill	kill	0
>	16:14:48	cat	execve	/home/user/Desktop/hhs.txt
>	16:15:02	kill	kill	0
>	16:15:03	sleep	execve	0.05
>	16:15:10	kill	kill	0
>	16:15:10	sleep	execve	0.1

Back to Synced Mode

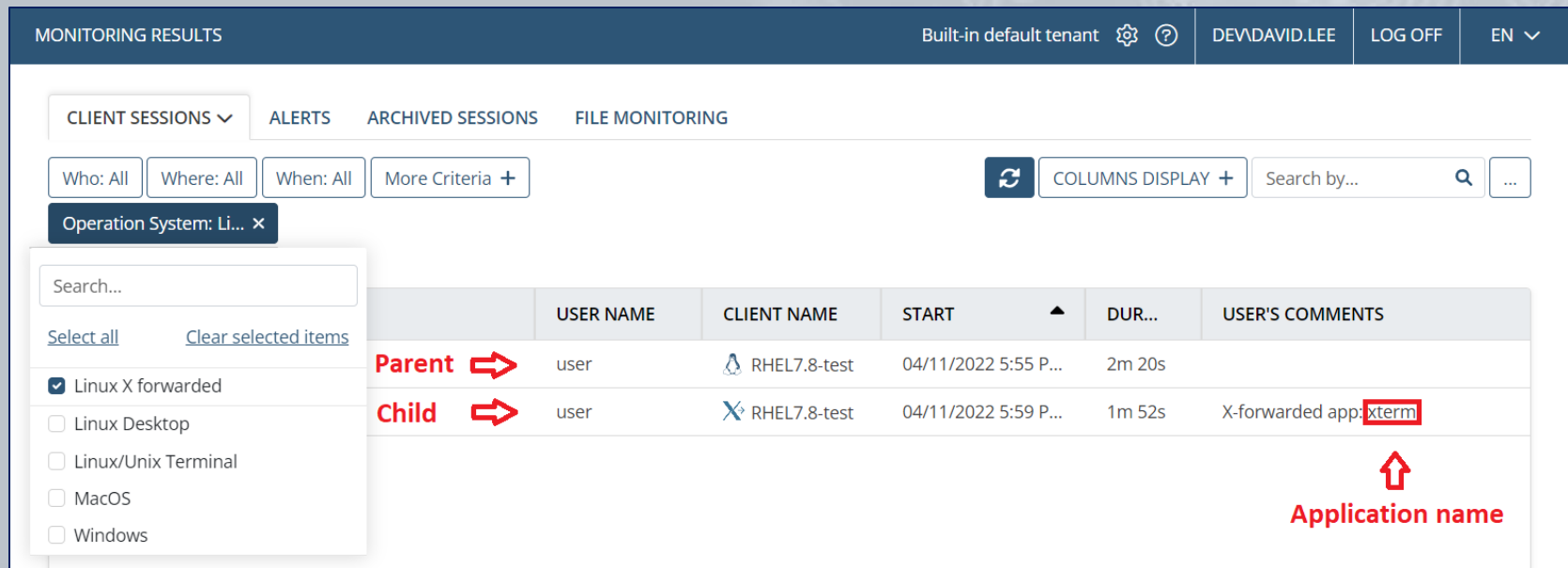
Search in output

Show function calls

Show only execution commands

Show inputs

- **X-forwarding** provides a method to enable **X Window System applications opened by users** in remote SSH sessions to also be monitored.
- These applications are **monitored as separate “child” sessions** of the SSH “parent” session, and the sessions are linked together when playing in the Session Viewer.

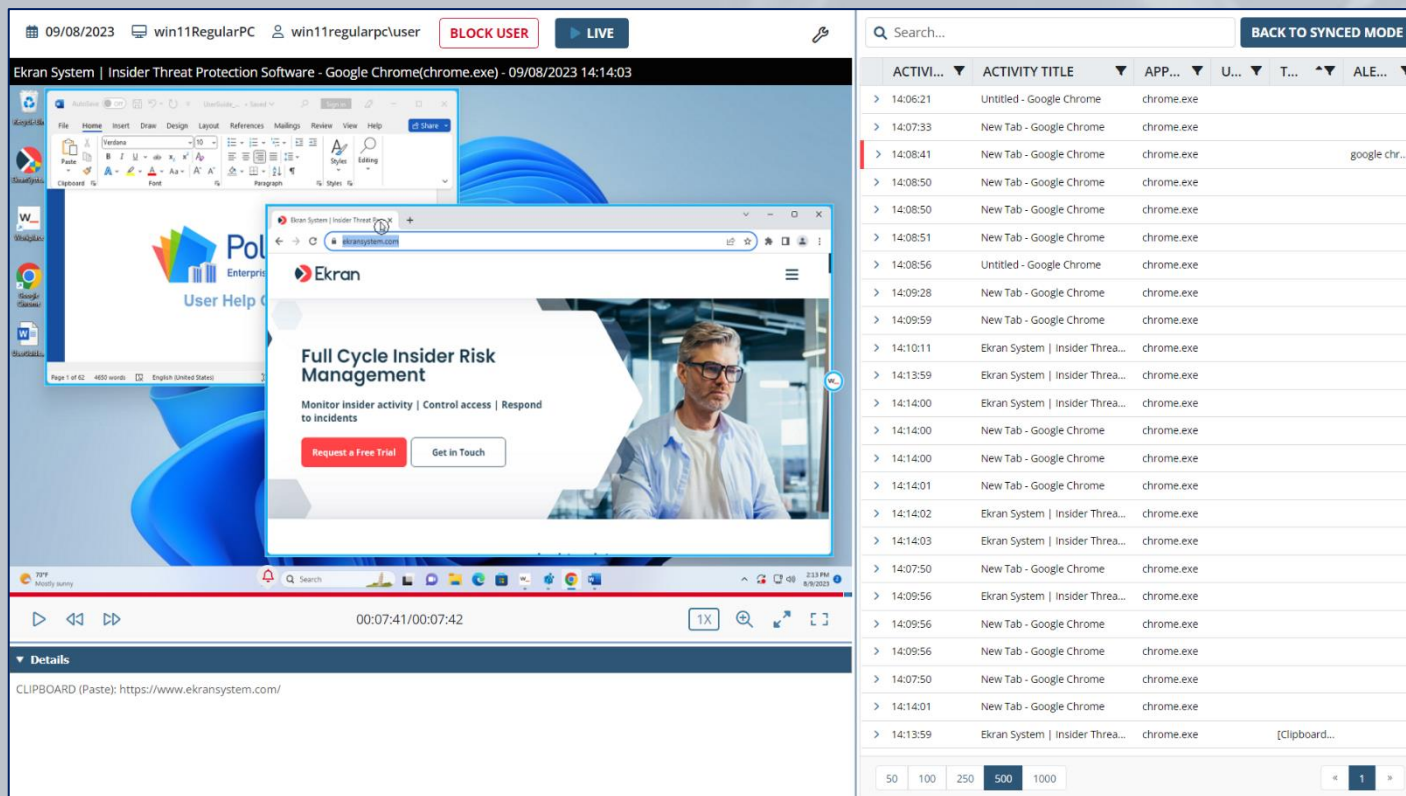


The screenshot displays the 'MONITORING RESULTS' page in the Ekran system. The interface includes a navigation bar with 'CLIENT SESSIONS' selected, and filters for 'Who: All', 'Where: All', and 'When: All'. A search bar is present with a search icon and a refresh button. The main content area shows a table of sessions with columns for 'USER NAME', 'CLIENT NAME', 'START', 'DUR...', and 'USER'S COMMENTS'. Two sessions are listed: a 'Parent' session and a 'Child' session. The 'Child' session is highlighted with a red box around the application name 'xterm' in the 'USER'S COMMENTS' column. A red arrow points to the 'Child' session, and another red arrow points to the 'xterm' application name. A legend at the bottom right indicates that the red arrow symbol represents the 'Application name'.

	USER NAME	CLIENT NAME	START	DUR...	USER'S COMMENTS
Parent →	user	RHEL7.8-test	04/11/2022 5:55 P...	2m 20s	
Child →	user	RHEL7.8-test	04/11/2022 5:59 P...	1m 52s	X-forwarded app: xterm

Monitoring Applications Opened in Venn

Ekran System is also **integrated** with the **Venn app launcher**, and can be configured to **monitor only applications** opened by users in a **Venn workspace**.



The screenshot displays the Ekran System monitoring interface. The top bar shows the date (09/08/2023), user name (win11RegularPC), and a 'BLOCK USER' button. Below this, a live view of the user's desktop is shown, featuring a Microsoft Word document and a Google Chrome browser window displaying the Ekran System website. The website content includes the heading 'Full Cycle Insider Risk Management' and a 'Request a Free Trial' button. The bottom of the interface shows a 'Details' section with a clipboard paste of the URL 'https://www.ekransystem.com/'.

On the right side, there is a table listing application activities. The table has columns for 'ACTIVITY...', 'ACTIVITY TITLE', 'APP...', 'U...', 'T...', and 'ALE...'. The table contains 20 rows of data, showing various activities such as 'Untitled - Google Chrome', 'New Tab - Google Chrome', and 'Ekran System | Insider Threa...'. The table is currently displaying 500 items.

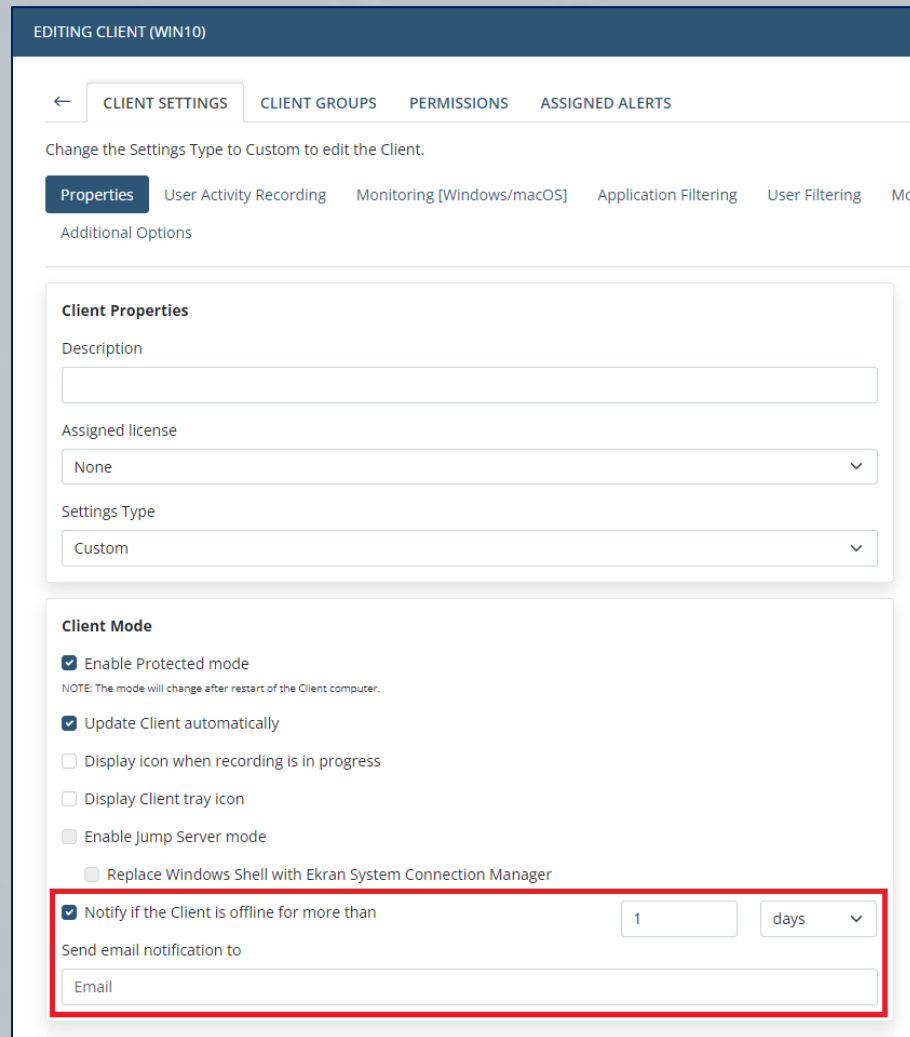
ACTIVITY...	ACTIVITY TITLE	APP...	U...	T...	ALE...
>	14:06:21	Untitled - Google Chrome	chrome.exe		
>	14:07:33	New Tab - Google Chrome	chrome.exe		
>	14:08:41	New Tab - Google Chrome	chrome.exe		google chr...
>	14:08:50	New Tab - Google Chrome	chrome.exe		
>	14:08:50	New Tab - Google Chrome	chrome.exe		
>	14:08:51	New Tab - Google Chrome	chrome.exe		
>	14:08:56	Untitled - Google Chrome	chrome.exe		
>	14:09:28	New Tab - Google Chrome	chrome.exe		
>	14:09:59	New Tab - Google Chrome	chrome.exe		
>	14:10:11	Ekran System Insider Threa...	chrome.exe		
>	14:13:59	Ekran System Insider Threa...	chrome.exe		
>	14:14:00	Ekran System Insider Threa...	chrome.exe		
>	14:14:00	New Tab - Google Chrome	chrome.exe		
>	14:14:00	New Tab - Google Chrome	chrome.exe		
>	14:14:01	New Tab - Google Chrome	chrome.exe		
>	14:14:02	Ekran System Insider Threa...	chrome.exe		
>	14:14:03	Ekran System Insider Threa...	chrome.exe		
>	14:07:50	New Tab - Google Chrome	chrome.exe		
>	14:09:56	Ekran System Insider Threa...	chrome.exe		
>	14:09:56	New Tab - Google Chrome	chrome.exe		
>	14:09:56	New Tab - Google Chrome	chrome.exe		
>	14:07:50	New Tab - Google Chrome	chrome.exe		
>	14:14:01	New Tab - Google Chrome	chrome.exe		
>	14:13:59	Ekran System Insider Threa...	chrome.exe		[Clipboard...]

Detection of Disconnected Clients

Detection of Disconnected Clients

Detection of disconnected Clients will help you to timely detect Clients that have stopped transmitting monitoring data.

Just **define the time period** after which offline Clients will be considered as disconnected, and **get notified** about such incidents.



EDITING CLIENT (WIN10)

← 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 Mor

Additional Options

Client Properties

Description

Assigned license

None

Settings Type

Custom

Client Mode

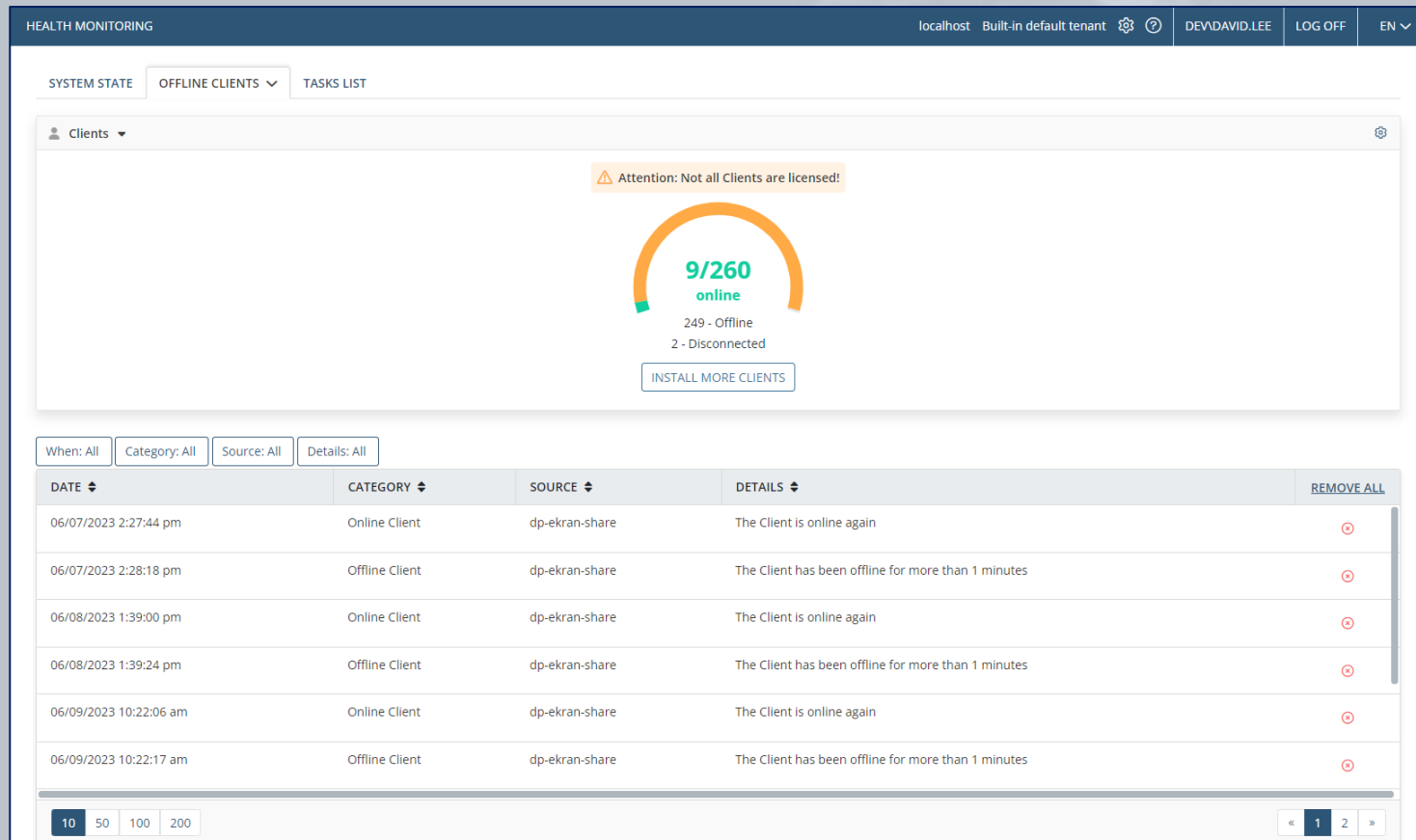
- Enable Protected mode
NOTE: The mode will change after restart of the Client computer.
- Update Client automatically
- Display icon when recording is in progress
- Display Client tray icon
- Enable Jump Server mode
- Replace Windows Shell with Ekran System Connection Manager
- Notify if the Client is offline for more than

Send email notification to

Email

Viewing Disconnected Clients

You can view all Clients that are **offline** for **more than a specified time period** on the Offline Clients page.



HEALTH MONITORING localhost Built-in default tenant DEVDAVID.LEE LOG OFF EN

SYSTEM STATE OFFLINE CLIENTS TASKS LIST

Clients

Attention: Not all Clients are licensed!

9/260
online
249 - Offline
2 - Disconnected

INSTALL MORE CLIENTS

When: All Category: All Source: All Details: All

DATE	CATEGORY	SOURCE	DETAILS	REMOVE ALL
06/07/2023 2:27:44 pm	Online Client	dp-ekran-share	The Client is online again	
06/07/2023 2:28:18 pm	Offline Client	dp-ekran-share	The Client has been offline for more than 1 minutes	
06/08/2023 1:39:00 pm	Online Client	dp-ekran-share	The Client is online again	
06/08/2023 1:39:24 pm	Offline Client	dp-ekran-share	The Client has been offline for more than 1 minutes	
06/09/2023 10:22:06 am	Online Client	dp-ekran-share	The Client is online again	
06/09/2023 10:22:17 am	Offline Client	dp-ekran-share	The Client has been offline for more than 1 minutes	

10 50 100 200 « 1 2 »

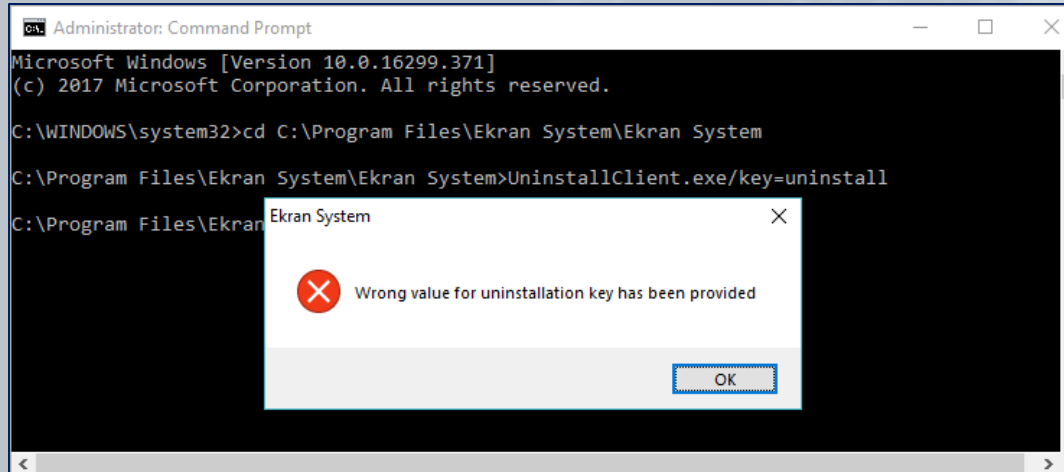
Client Protection

Ekran System allows you to **protect Windows Clients** and their **data** by enabling Protected mode.

The use of Protected mode has the following **advantages**:

- Prevention of Client **uninstallation**.
- Prevention of **stopping** Client **processes**.
- Prevention of **editing** Client **system files and logs**.
- Prevention of **editing** Client **settings** in the **registry** of the Client computer.
- Prevention of **modification, removal, and renaming** of Client **files**.

Users, including privileged ones, are **unable to stop the Client running** on computers, or **remove** the Client locally without the assistance of the administrator.

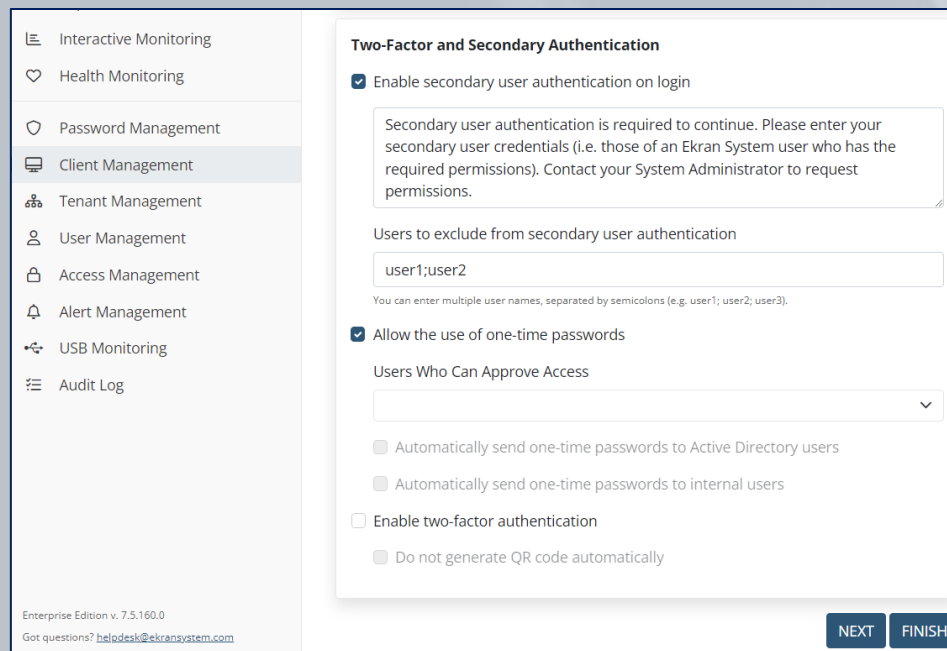


Only the **Ekran System administrator** knows the **Uninstallation key** defined prior to Client installation, and which is required for local removal.

Secondary User Authentication

Secondary user authentication allows you to achieve two goals:

- Monitor the activity of users on a computer when **multiple users** share the **same credentials** to log in.
- Improve your security by requiring users to enter **additional authentication credentials**.



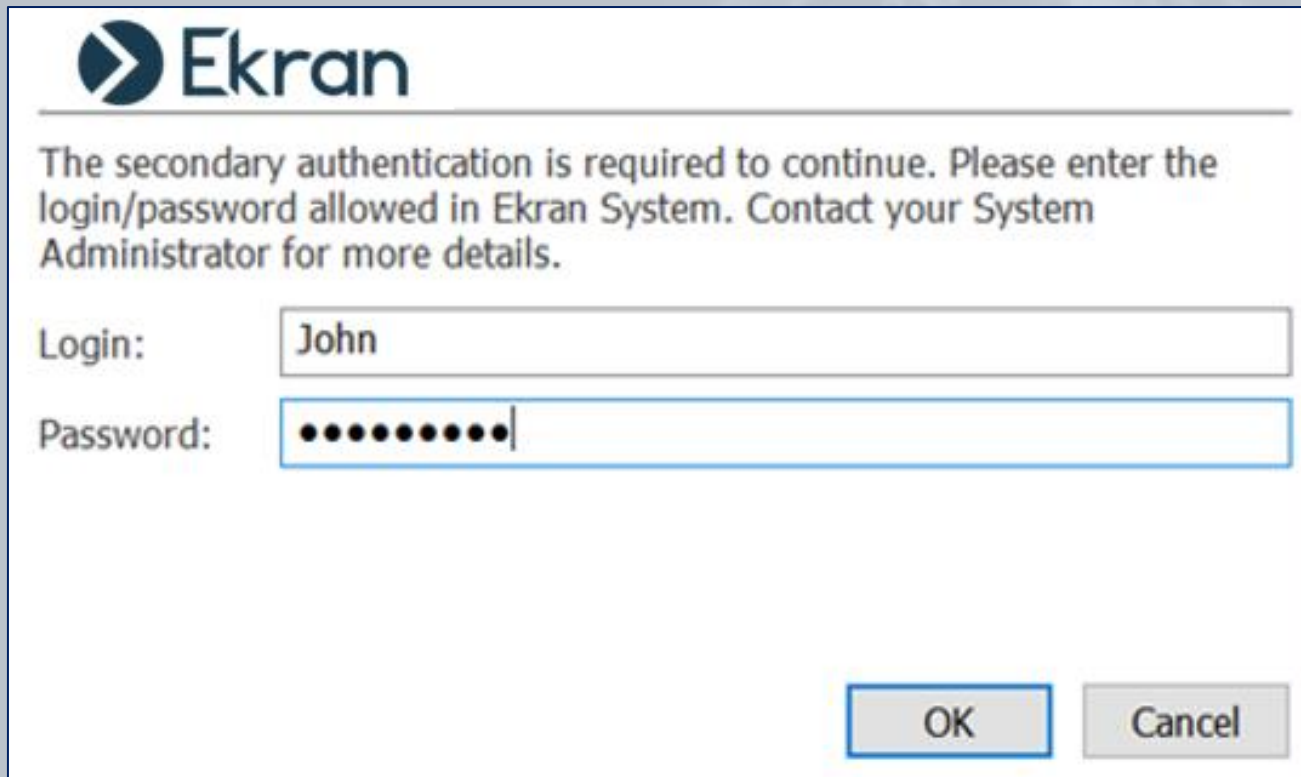
The screenshot shows the 'Two-Factor and Secondary Authentication' configuration page in the Ekran System. The left sidebar contains a navigation menu with the following items: Interactive Monitoring, Health Monitoring, Password Management, Client Management (highlighted), Tenant Management, User Management, Access Management, Alert Management, USB Monitoring, and Audit Log. The main content area is titled 'Two-Factor and Secondary Authentication' and includes the following settings:

- Enable secondary user authentication on login
- Secondary user authentication is required to continue. Please enter your secondary user credentials (i.e. those of an Ekran System user who has the required permissions). Contact your System Administrator to request permissions.
- Users to exclude from secondary user authentication:
You can enter multiple user names, separated by semicolons (e.g. user1; user2; user3).
- Allow the use of one-time passwords
- Users Who Can Approve Access:
- Automatically send one-time passwords to Active Directory users
- Automatically send one-time passwords to internal users
- Enable two-factor authentication
 - Do not generate QR code automatically

At the bottom left, it says 'Enterprise Edition v. 7.5.160.0' and 'Got questions? helpdesk@ekransystem.com'. At the bottom right, there are 'NEXT' and 'FINISH' buttons.

Secondary User Authentication (Windows)

The Ekran System Client requests **credentials** to be entered **before** allowing a user to **access** the Windows OS.



The screenshot shows a dialog box titled "Ekran" with the following text: "The secondary authentication is required to continue. Please enter the login/password allowed in Ekran System. Contact your System Administrator for more details." Below the text are two input fields: "Login:" with the text "John" and "Password:" with a masked password represented by ten dots. At the bottom right are "OK" and "Cancel" buttons.

Ekran

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

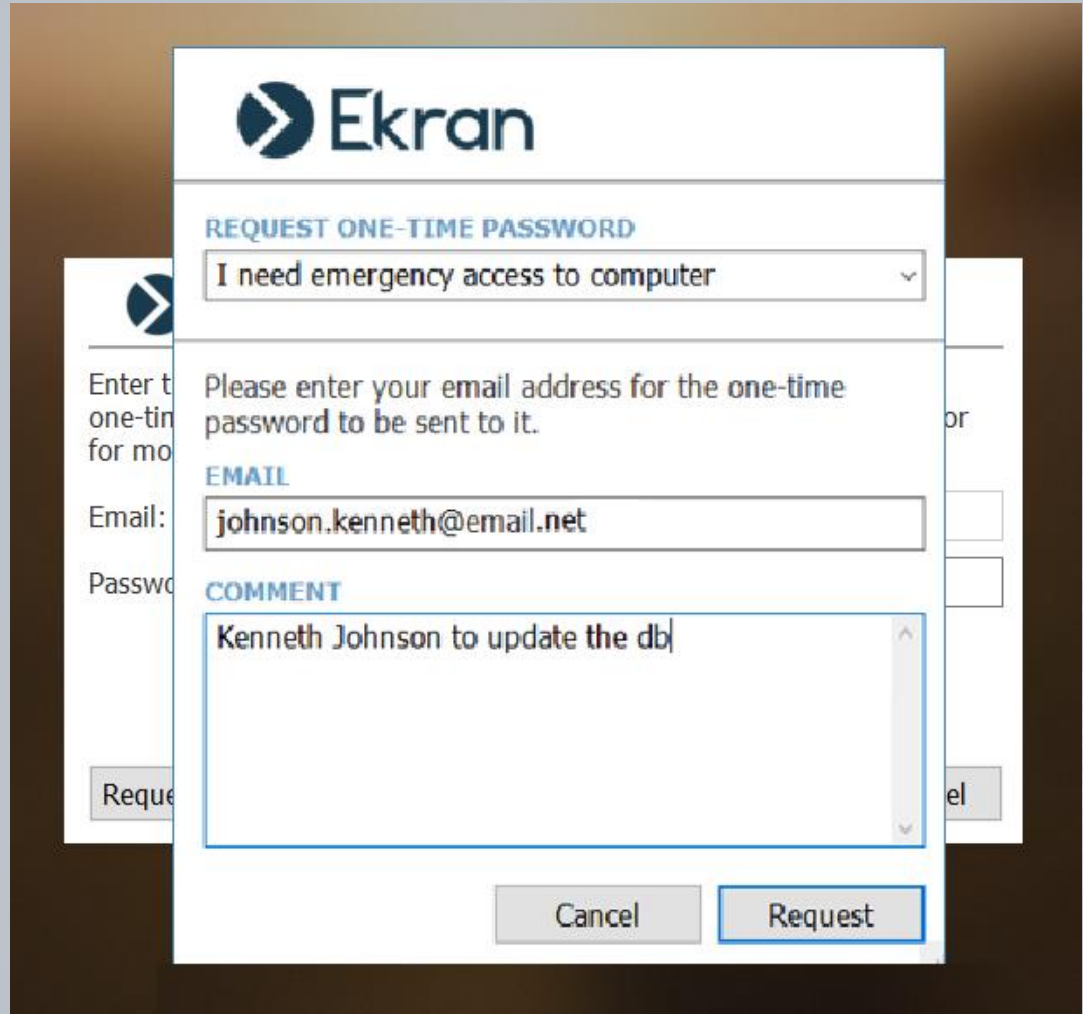
Login:

Password:

One-Time Passwords (Windows Clients)

Ekran System Enterprise Edition provides the **administrator** with the unique **capability** to protect Client computers with one-time passwords.

The **user** can **request** a one-time password directly **from** the secondary user authentication **window** displayed **during login** to the Windows OS.



Ekran

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

Email: johnson.kenneth@email.net

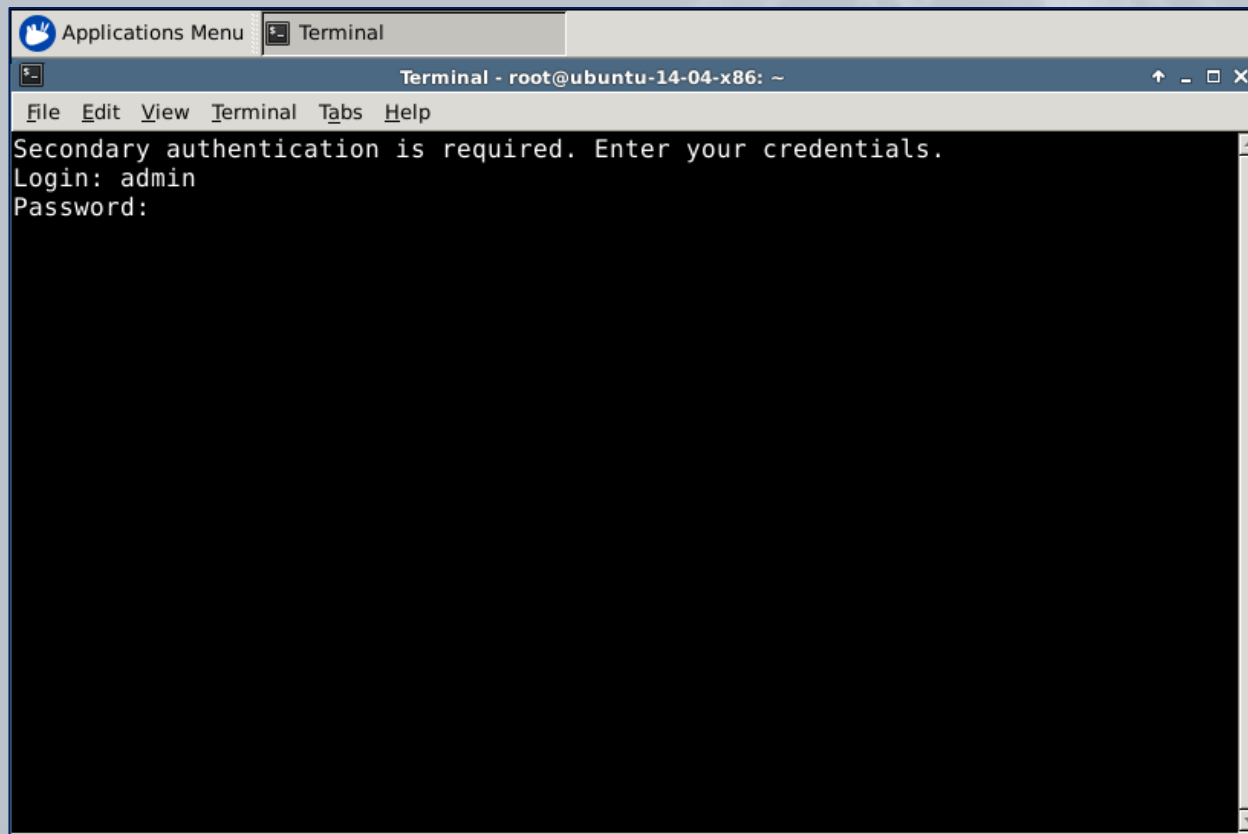
COMMENT

Kenneth Johnson to update the db

Cancel Request

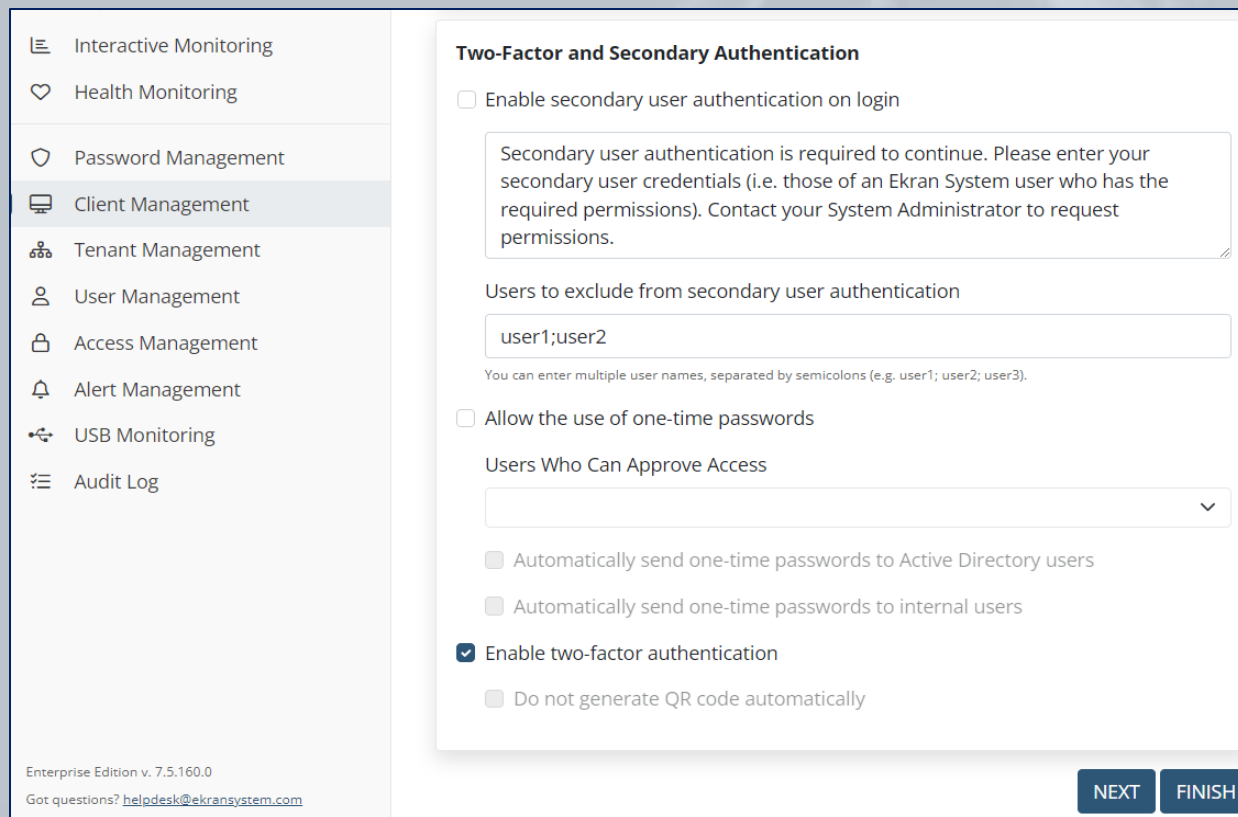
Secondary User Authentication (Linux Clients)

The Ekran System Client requests **credentials** to be entered to allow a user to **log on to the terminal** on **Linux** Client computers.



Two-Factor Authentication

Two-factor authentication allows you to enable an **extra layer of security** to better protect the critical endpoints in your network.



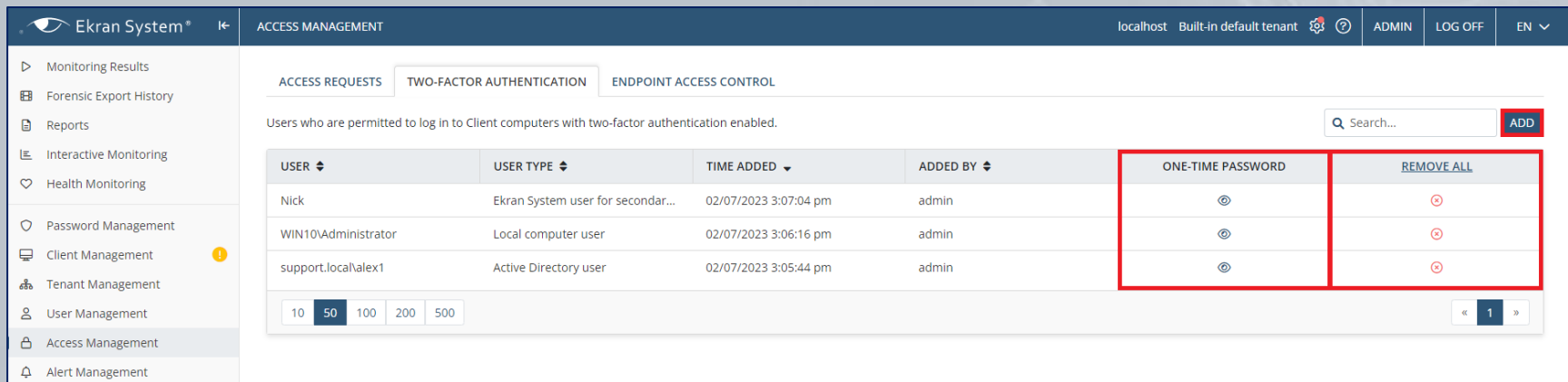
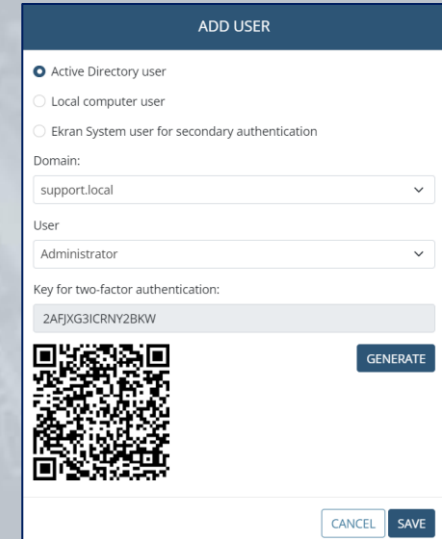
The screenshot shows the configuration page for Two-Factor and Secondary Authentication in the Ekran System. The left sidebar contains a navigation menu with the following items: Interactive Monitoring, Health Monitoring, Password Management, Client Management (highlighted), Tenant Management, User Management, Access Management, Alert Management, USB Monitoring, and Audit Log. The main content area is titled "Two-Factor and Secondary Authentication" and includes the following settings:

- Enable secondary user authentication on login
- Secondary user authentication is required to continue. Please enter your secondary user credentials (i.e. those of an Ekran System user who has the required permissions). Contact your System Administrator to request permissions.
- Users to exclude from secondary user authentication:
You can enter multiple user names, separated by semicolons (e.g. user1; user2; user3).
- Allow the use of one-time passwords
- Users Who Can Approve Access:
- Automatically send one-time passwords to Active Directory users
- Automatically send one-time passwords to internal users
- Enable two-factor authentication
- Do not generate QR code automatically

At the bottom left, it says "Enterprise Edition v. 7.5.160.0" and "Got questions? helpdesk@ekransystem.com". At the bottom right, there are "NEXT" and "FINISH" buttons.

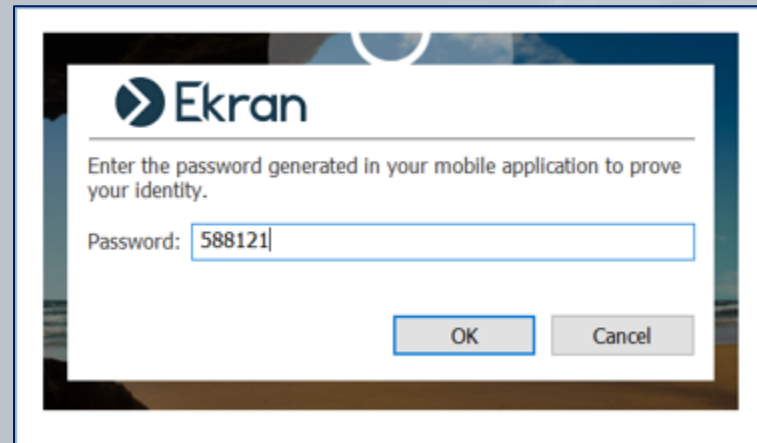
Two-Factor Authentication (Windows/Linux)

You can either enable this feature for all Windows Client computers, or manually add only users who you want to be allowed to log in to Windows and Linux Client computers, using **time-based one-time passwords** (TOTP) generated by way of a mobile authenticator application.



USER	USER TYPE	TIME ADDED	ADDED BY	ONE-TIME PASSWORD	REMOVE ALL
Nick	Ekran System user for secondar...	02/07/2023 3:07:04 pm	admin	👁	⊖
WIN10\Administrator	Local computer user	02/07/2023 3:06:16 pm	admin	👁	⊖
support.local\alex1	Active Directory user	02/07/2023 3:05:44 pm	admin	👁	⊖

The Ekran System Client **prompts the user to enter a TOTP** to access the system.



```
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: _
```

Two-Factor Authentication (for MT users)

Apart from users of monitored endpoints, two-factor authentication can also be enabled for Ekran System **Management Tool users**.

EDITING USER (USER3)

← USER TYPE USER DETAILS USER GROUPS ADMINISTRATIVE PERMISSIONS

Internal User Properties

Define the user credentials and additional information about the user. The login and password are required.

Login
User3

Password
.....


Confirm password
.....

Enable two-factor authentication on login RESET 2FA

First name
Fred

SET UP TWO-FACTOR AUTHENTICATION

Two-Factor authentication is enabled for your user account. Open your authenticator application (Google Authenticator or Microsoft Authenticator) and scan the code before clicking Confirm. On the next login, you will be prompted to enter the code from your authenticator application.



RECOVERY CODE

PSU52 - DHHBE - QNEFK - VMMSW 📄

You will need the recovery code in case you lose access to your authenticator device. Make sure you save it to a safe place.

BACK CONFIRM

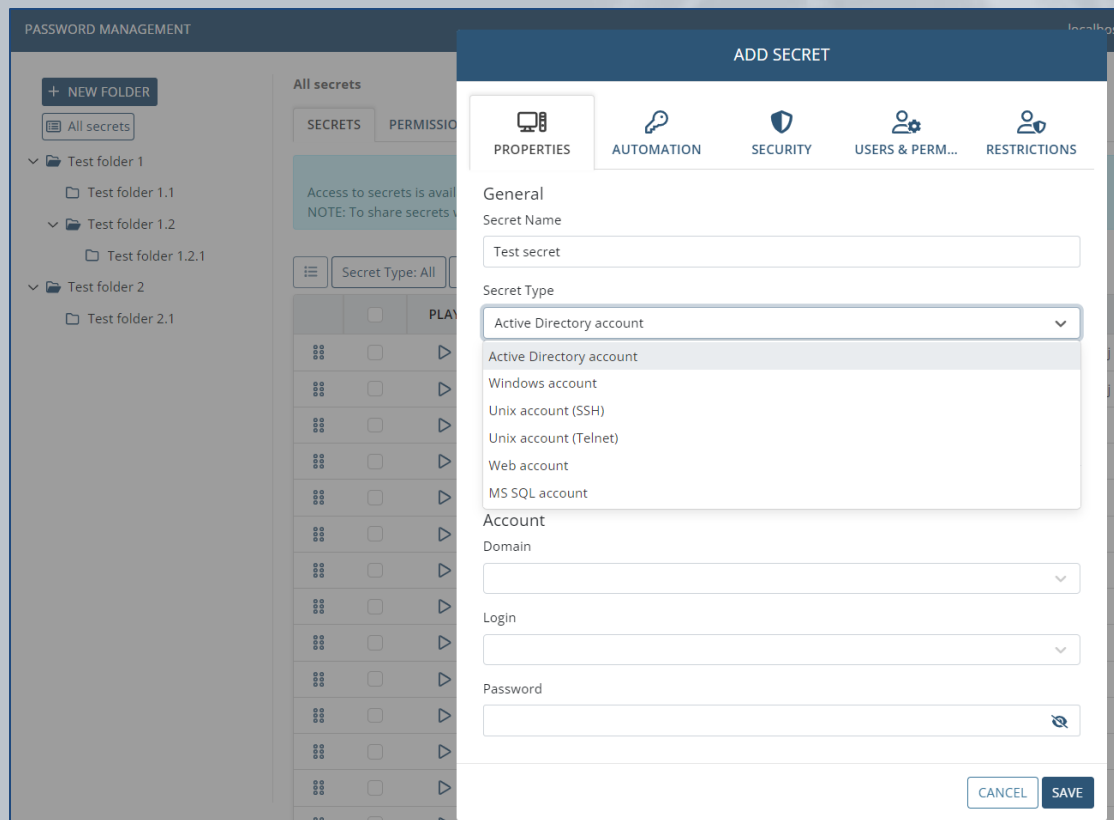
Password Management (Privileged Access Management)

Managing privileged accounts (PAM) and implementing role-based access control is critical for enterprise security teams. Ekran System's **Password Management** functionality uses secrets to provide you with full control and visibility over privileged user access.

With Ekran System, you can:

- Securely **store** account **credentials** in **secrets** for various types of accounts (Active Directory, Windows, Unix (SSH), Unix (Telnet), Web, and MS SQL).
- Provide **granular access** to stored credentials.
- **Manage passwords** without interfering with the workflow of privileged users.
- Enable **remote password rotation** (for Active Directory, Windows, Unix (SSH), and MS SQL account secrets), and **Unix (SSH) key rotation**.
- Require **password checkout** to prevent multiple users from using any specific secret concurrently.
- Allow users to **view a secret's password**, and **transfer files using WinSCP**.

Add a secret and define: an **endpoint** to connect to, privileged account **credentials**, and **users / user groups** to give access to.



Adding a Secret (Enhanced Security Options)

To enhance security further, optionally:

- enable **remote password rotation**
- require **password checkout**

ADD SECRET

PROPERTIES AUTOMATION SECURITY USERS & PERM... RESTRICTIONS

Enable remote password rotation

Rotate Password Every

ADD SECRET

PROPERTIES AUTOMATION SECURITY USERS & PERM... RESTRICTIONS

Requires check out

Change password on check in

Check in automatically after

Adding a Secret (Assigning Users & Permissions)

To define users' access to a secret:

- **Add users** / user groups.
- **Grant them** Role Type (Owner / Editor / PAM User) and advanced **permissions** (View Password / File Transfer via WinSCP).

ADD SECRET

PROPERTIES AUTOMATION SECURITY **USERS & PERM...** RESTRICTIONS

Inherit users and their roles from current folder + Add v

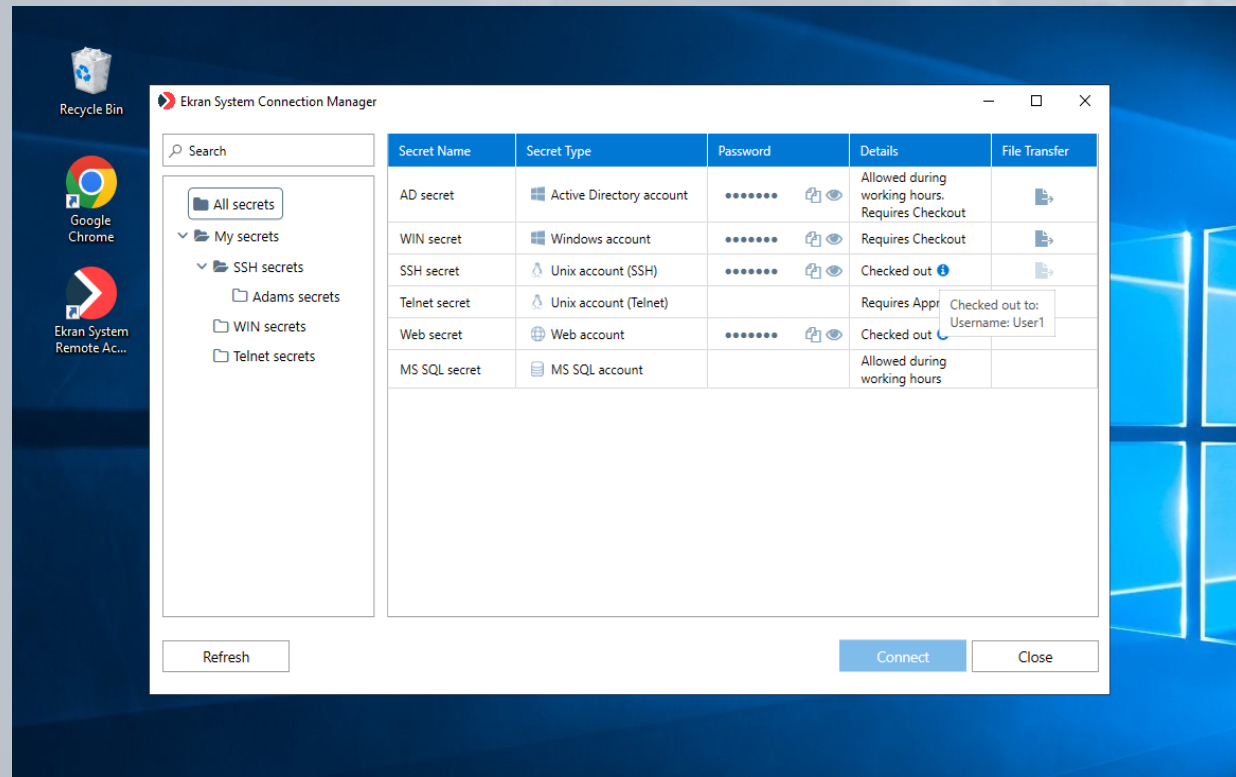
Inherit advanced permissions from current folder

USER / USER GROUP ▼	ROLE TYPE			REMOVE ALL
admin	Owner ▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ekran-5.app\pamuser	Editor ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
User1	PAM User ▼	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
User2	PAM User ▼	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

« 1 »

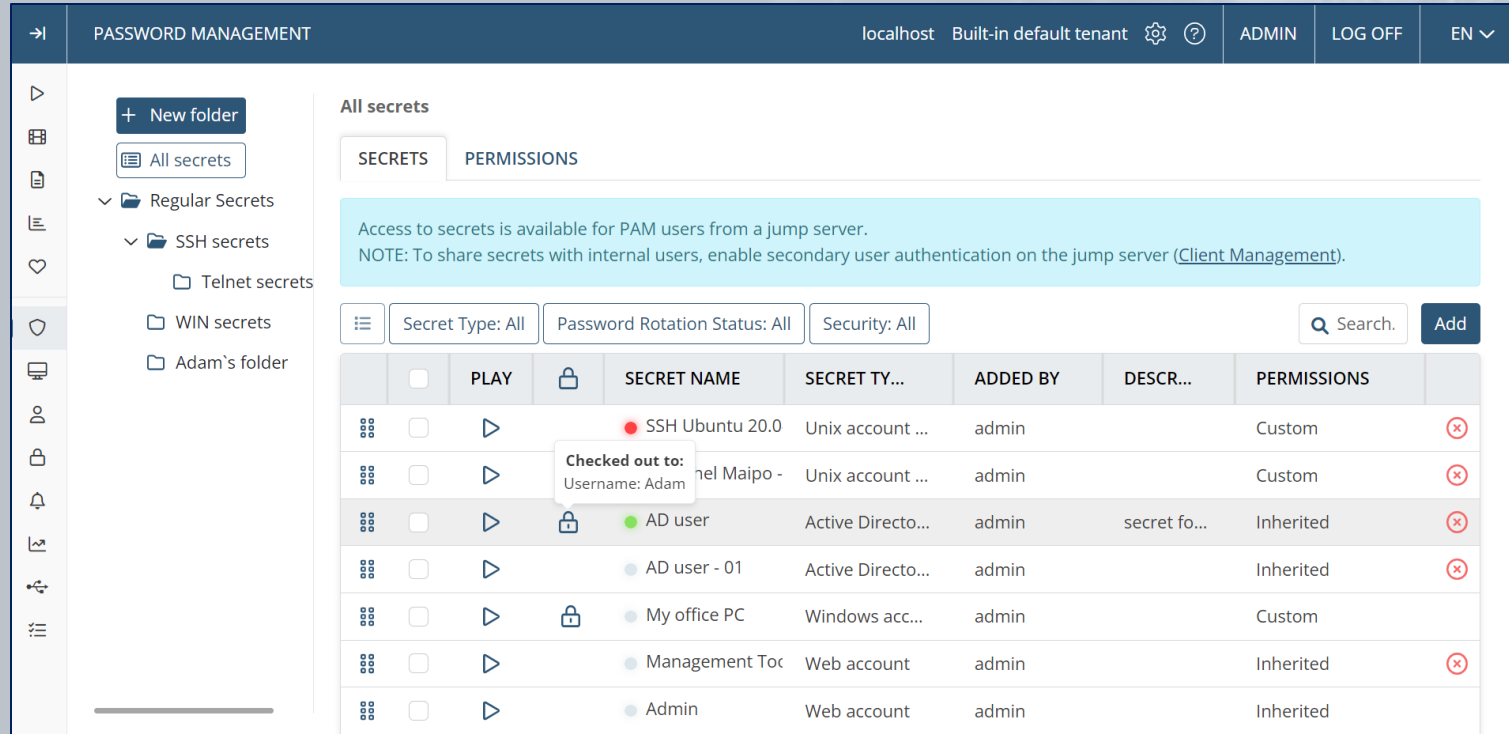
CANCEL SAVE

A **privileged user can access a critical endpoint via a secret** by using the Ekran System Connection Manager. The secrets are stored in a granular **Tree-View folder structure** and have **user permissions** for both folders and secrets.



Viewing Secrets in Sessions

You can **click** on a specific secret (in any folder) **to open the list of sessions in which it was used**. Furthermore, the **secret data is highlighted** when playing the session in the Session Viewer, so you can also quickly find it within any session.



The screenshot displays the 'All secrets' interface in the Ekran system. The top navigation bar shows 'PASSWORD MANAGEMENT', 'localhost', 'Built-in default tenant', and user options 'ADMIN', 'LOG OFF', and 'EN'. The left sidebar contains a 'New folder' button and a tree view of secret folders: 'Regular Secrets', 'SSH secrets' (expanded), 'Telnet secrets', 'WIN secrets', and 'Adam's folder'. The main content area is titled 'All secrets' and has tabs for 'SECRETS' and 'PERMISSIONS'. A light blue notification banner states: 'Access to secrets is available for PAM users from a jump server. NOTE: To share secrets with internal users, enable secondary user authentication on the jump server (Client Management)'. Below the banner are filters for 'Secret Type: All', 'Password Rotation Status: All', and 'Security: All', along with a search bar and an 'Add' button. The main table lists secrets with columns for 'PLAY', 'SECRET NAME', 'SECRET TY...', 'ADDED BY', 'DESCR...', and 'PERMISSIONS'. The 'SSH Ubuntu 20.0' secret is highlighted, and a tooltip indicates it is 'Checked out to: Username: Adam'.

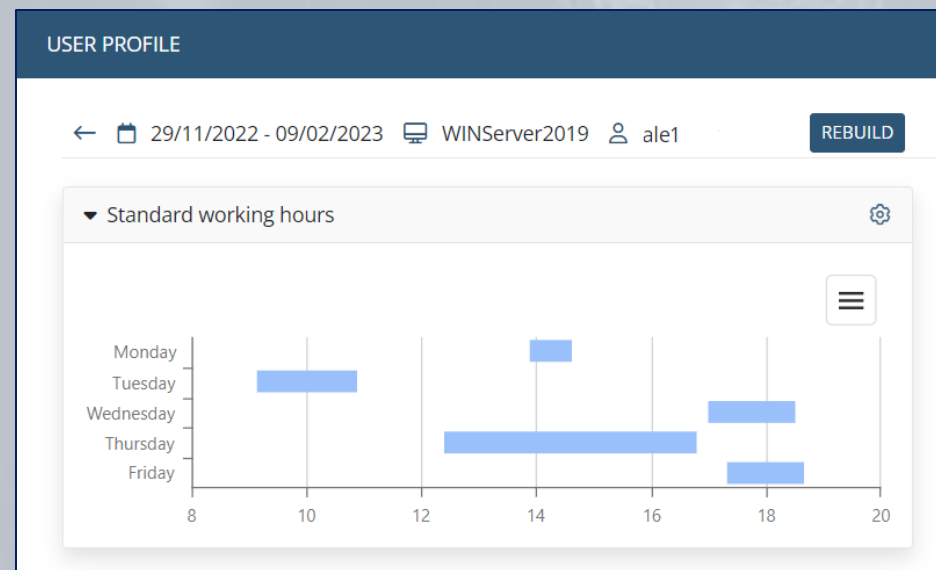
	PLAY	SECRET NAME	SECRET TY...	ADDED BY	DESCR...	PERMISSIONS
		SSH Ubuntu 20.0	Unix account ...	admin		Custom
		nel Maipo -	Unix account ...	admin		Custom
		AD user	Active Directo...	admin	secret fo...	Inherited
		AD user - 01	Active Directo...	admin		Inherited
		My office PC	Windows acc...	admin		Custom
		Management Toc	Web account	admin		Inherited
		Admin	Web account	admin		Inherited

User and Entity Behavior Analytics (UEBA)

Ekran System User & Entity Behavior Analytics (**UEBA**) allows you to **better protect your system** from malicious and illicit insiders.

UEBA has the following advantages for detecting suspicious activities:

- **Analysis** of user **behavior patterns** and establishment of a baseline for **normal behavior**.
- Automatic **detection** of behavioral **anomalies & deviations**.
- Timely **notification** of potential **insider threats**.



Add a user behavior rule to **view user profiles** and **analyze sessions** with the **detected anomalies**, and get timely **notified** about risky user activity.

ADD RULE

Properties

Enable rule

Name

Abnormal behaviour

Description

Conditions

Unusual work hours

High

Email Notifications

Send notification on detected anomalies for a finished session

Send instant notification on detected anomalies

Send total session risk score in case of no anomalies

Send email notification to

admin@example.com

Additional Actions

Show warning message to user

You are performing a forbidden action.

Block user in the current session

FINISH

Monitored sessions that contain **detected user behavior anomalies** have a special **risk score**.

The **risk score** indicates the **severity level** of the session and is calculated according to the risk level of the abnormal user behavior **patterns and alerts** detected in the monitored sessions.

MONITORING RESULTS

CLIENT SESSIONS ▾ ALERTS ARCHIVED SESSIONS FILE MONITORING

Who: All Where: All When: All More Criteria +

Total number of sessions: 82

PLAY	RISK SCORE	ALERTS	USER NAME	CLIENT NAME
▶			SUPPORT\alex...	WIN-4D1MTM6US...
▶	90%		WIN-4D1MTM...	WIN-4D1MTM6US...
▶	51%	🔔	WIN-4D1MTM...	WIN-4D1MTM6US...
▶	51%	🔔	WIN-4D1MTM...	WIN-4D1MTM6US...
▶			WIN-4D1MTM...	WIN-4D1MTM6US...
▶	30%	🔔	WIN-4D1MTM...	WIN-4D1MTM6US...
▶	30%	🔔	WIN-4D1MTM...	WIN-4D1MTM6US...

Administrator Approval on Login

Administrator Approval on Login

Approval by an administrator on login allows you to better **protect** the Client computers in your network against **undesired access**.

ACCESS MANAGEMENT localhost Built-in default tenant DEVIDAVID.LEE LOG OFF EN

ACCESS REQUESTS TWO-FACTOR AUTHENTICATION **ENDPOINT ACCESS CONTROL**

Users who are permitted to log in to Client computers according to a schedule or only after administrator approval. [ADD](#)

[APPLY FILTERS](#)

USER	USER TYPE	ASSIGNED TO	RESTRICTION TYPE	TIME ADDED	ADDED BY	REMOVE ALL
dev.local\tim.day	ActiveDirectory	dev.local\ekranserver	Email to administrator	21/01/2020 15:39:50	annie	
dev.local\guest	ActiveDirectory	dev.local\ekranserver	Email to administrator	05/04/2020 14:13:58	dev.local\karen	
gmkwin10\kay	Local		Email to administrator	16/05/2023 16:48:54	admin	

Administrator Approval on Login

You can **add users** whose **access** to Client computers needs to be **restricted**.

ADD USER

GENERAL RESTRICTION TYPES

User with Restricted Access Rights

User type:
Local computer user

Computer name: W-QA-TA3 User login: andy

Users Who Can Approve Access

User / User group:
ADMINISTRATORS

Allowed weekdays do not occur on the allowed dates. Administrator approval will always be required. CANCEL SAVE

ADD USER

GENERAL RESTRICTION TYPES

Restriction Type

Always require approval on login
 Allow access without approval during work hours

Allowed dates

From: 07/10/2023 To: 07/24/2023

Allowed time

From: 8:00:00 AM To: 5:00:00 PM

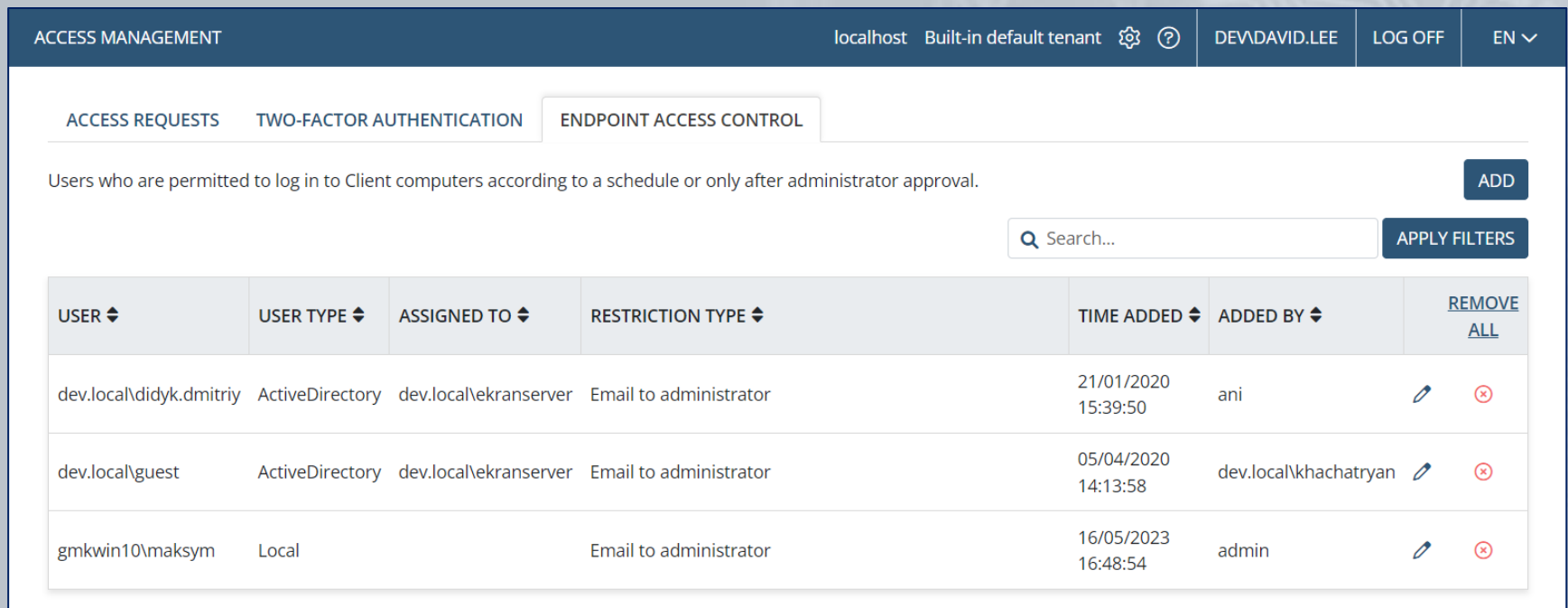
Allowed weekdays

Su Mo Tu We Th Fr Sa

Allowed weekdays do not occur on the allowed dates. Administrator approval will always be required. CANCEL SAVE

Administrator Approval on Login

When a restricted user logs in to a Client computer, the Client blocks the desktop and sends the **user's access request** to a **trusted user** for **approval**. The user's request is displayed on the **Access Requests** tab on the **Access Management** page.



ACCESS MANAGEMENT localhost Built-in default tenant DEV\DAVID.LEE LOG OFF EN

ACCESS REQUESTS TWO-FACTOR AUTHENTICATION ENDPOINT ACCESS CONTROL

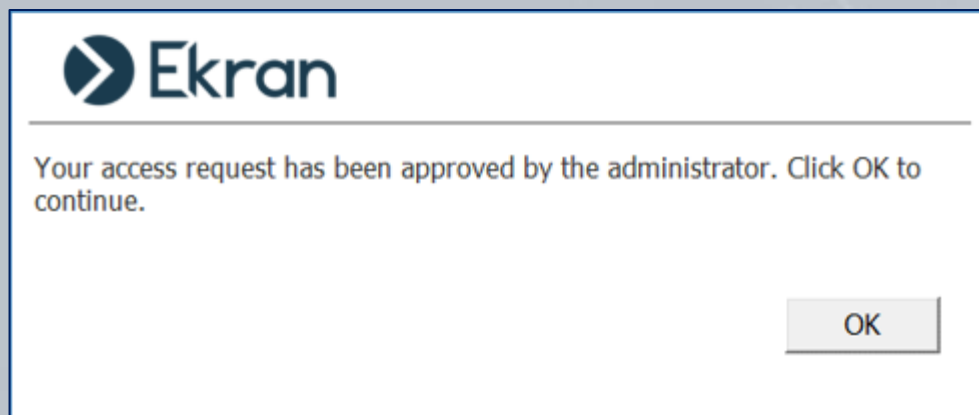
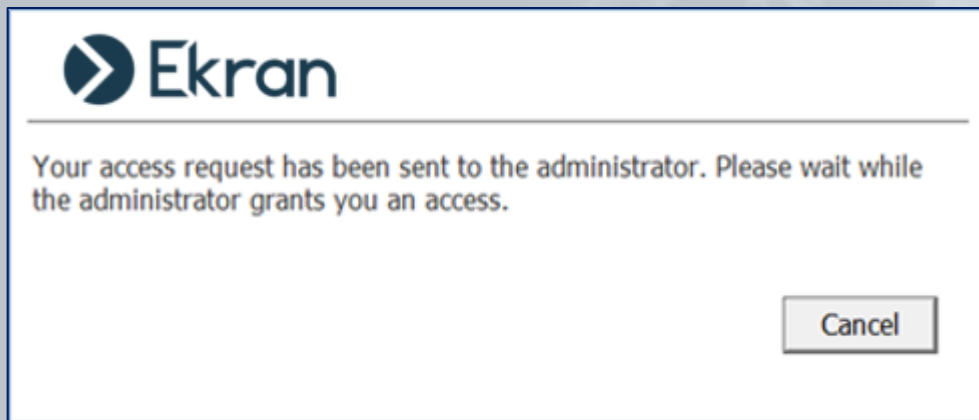
Users who are permitted to log in to Client computers according to a schedule or only after administrator approval. [ADD](#)

[APPLY FILTERS](#)

USER	USER TYPE	ASSIGNED TO	RESTRICTION TYPE	TIME ADDED	ADDED BY	REMOVE ALL
dev.local\didyk.dmitriy	ActiveDirectory	dev.local\ekranserver	Email to administrator	21/01/2020 15:39:50	ani	✎ ✖
dev.local\guest	ActiveDirectory	dev.local\ekranserver	Email to administrator	05/04/2020 14:13:58	dev.local\khachatryan	✎ ✖
gmkwin10\maksym	Local		Email to administrator	16/05/2023 16:48:54	admin	✎ ✖

Administrator Approval on Login

Only after the **trusted user approves** the user's **access request**, is the user allowed to access the system.



Access Request and Approval Workflow

You can minimize cybersecurity risks and control the number of **simultaneously active accounts** with Ekran System's **Just-in-Time Endpoint Access** capabilities.

ACCESS MANAGEMENT localhost Built-in default tenant DEV\DAVID.LEE LOG OFF EN

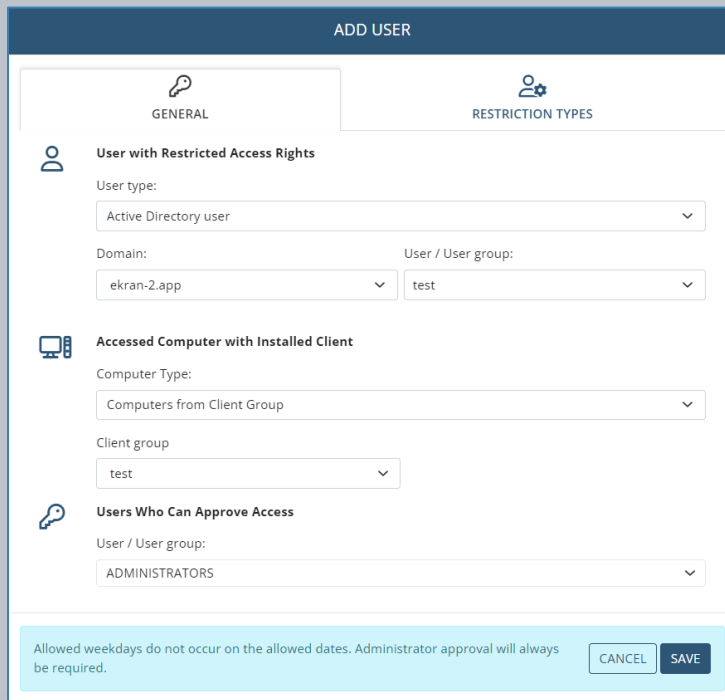
ACCESS REQUESTS TWO-FACTOR AUTHENTICATION **ENDPOINT ACCESS CONTROL**

Users who are permitted to log in to Client computers according to a schedule or only after administrator approval. ADD

APPLY FILTERS

USER	USER TYPE	ASSIGNED TO	RESTRICTION TYPE	TIME ADDED	ADDED BY	REMOVE ALL
dev.local\guest	ActiveDirectory	dev.local\ekranserver	Access on schedule (10/07/2023 - 24/07/2023, 08:00 - 18:00, Mo, Tu, We, Th, Fr)	05/04/2020 14:13:58	dev.local\andy	
w-qa-ta3\andy	Local		Access on schedule (10/07/2023 - 24/07/2023, 08:00 - 18:00, Mo, Tu, We, Th, Fr)	10/07/2023 16:11:50	dev.local\david.lee	

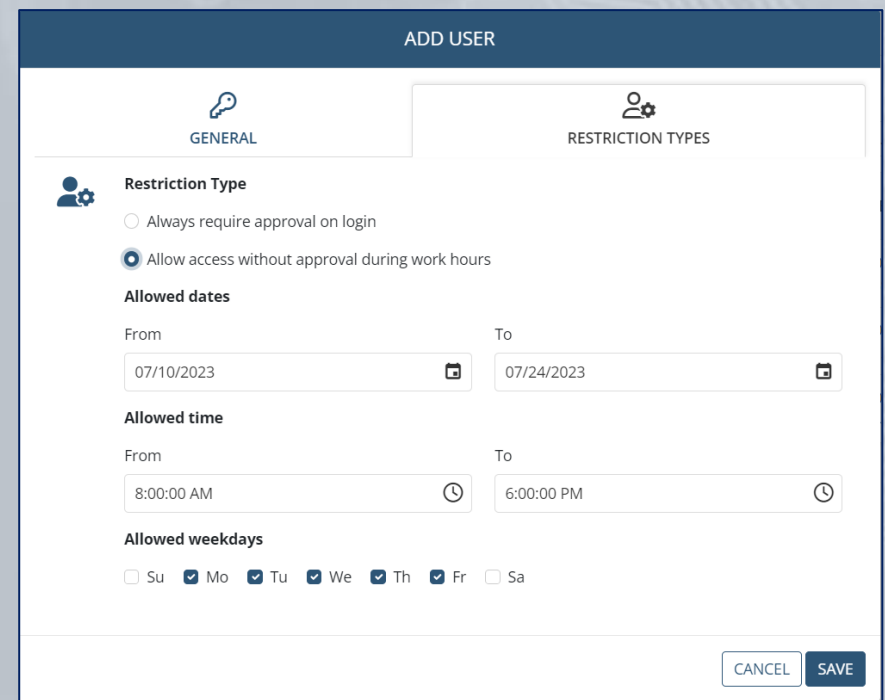
- **Manual access approval** to determine who can access what and when.
- **Time-based user access restrictions** to enhance the protection of critical data and systems.



The screenshot shows the 'ADD USER' form with the 'GENERAL' tab selected. The form is divided into three sections:

- User with Restricted Access Rights:** Includes a dropdown for 'User type' (Active Directory user), a 'Domain' dropdown (ekran-2.app), and a 'User / User group' dropdown (test).
- Accessed Computer with Installed Client:** Includes a 'Computer Type' dropdown (Computers from Client Group) and a 'Client group' dropdown (test).
- Users Who Can Approve Access:** Includes a 'User / User group' dropdown (ADMINISTRATORS).

At the bottom, there is a light blue warning box: "Allowed weekdays do not occur on the allowed dates. Administrator approval will always be required." and two buttons: 'CANCEL' and 'SAVE'.

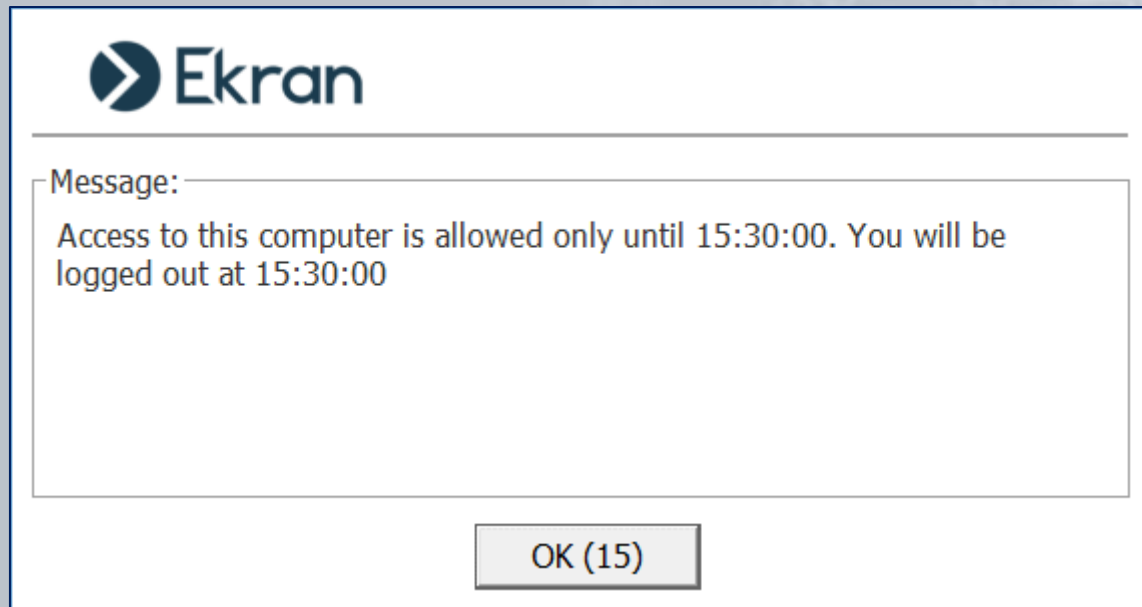


The screenshot shows the 'ADD USER' form with the 'RESTRICTION TYPES' tab selected. The form includes the following options:

- Restriction Type:** Radio buttons for 'Always require approval on login' (unselected) and 'Allow access without approval during work hours' (selected).
- Allowed dates:** 'From' date: 07/10/2023; 'To' date: 07/24/2023.
- Allowed time:** 'From' time: 8:00:00 AM; 'To' time: 6:00:00 PM.
- Allowed weekdays:** Checkboxes for Su (unselected), Mo (checked), Tu (checked), We (checked), Th (checked), Fr (checked), Sa (unselected).

At the bottom right, there are two buttons: 'CANCEL' and 'SAVE'.

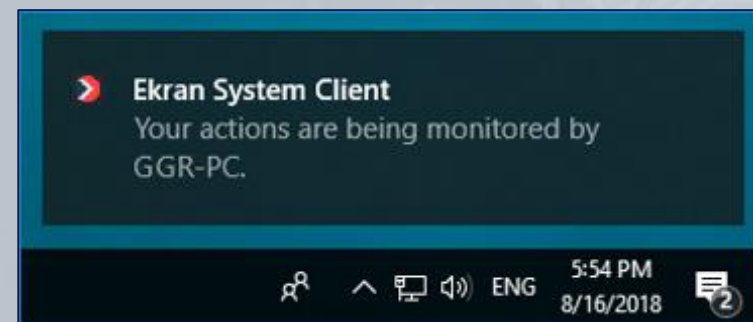
Restricted users will be able to **log in** to Client computers **only during the defined time period**, and will need **additional approval** to log in **outside of this period**.



Notifying Users about Being Monitored

To adhere to the **security policy** of your company or your **country regulations**, you can:

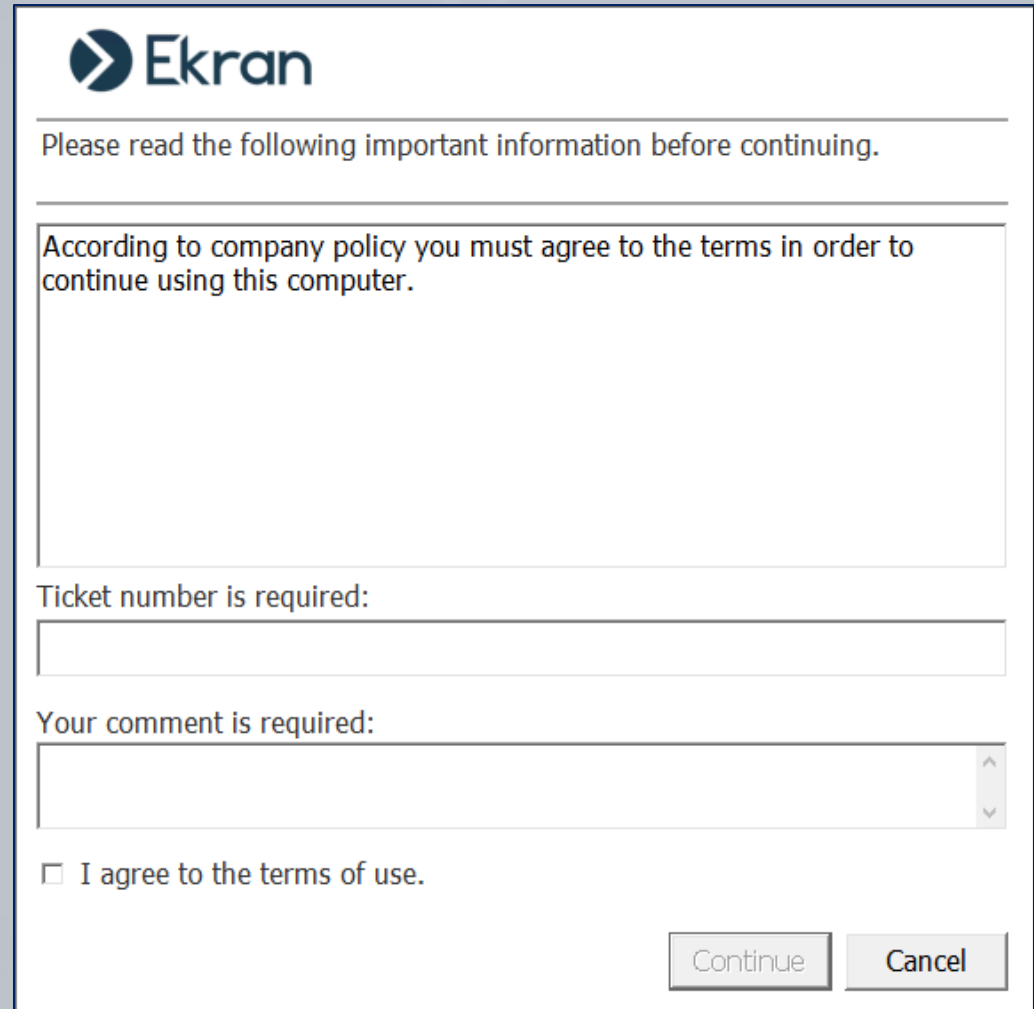
- Enable the **displaying** of a custom **additional message** on user login to notify the user that their activity is being monitored, and obtain their consent.
- Enable the **displaying** of the **Client tray icon** along with a **notification** to the user that their activity is being monitored.



Notifying Users about Being Monitored

Before being allowed to log in to the Client computer, users can also be **required to:**

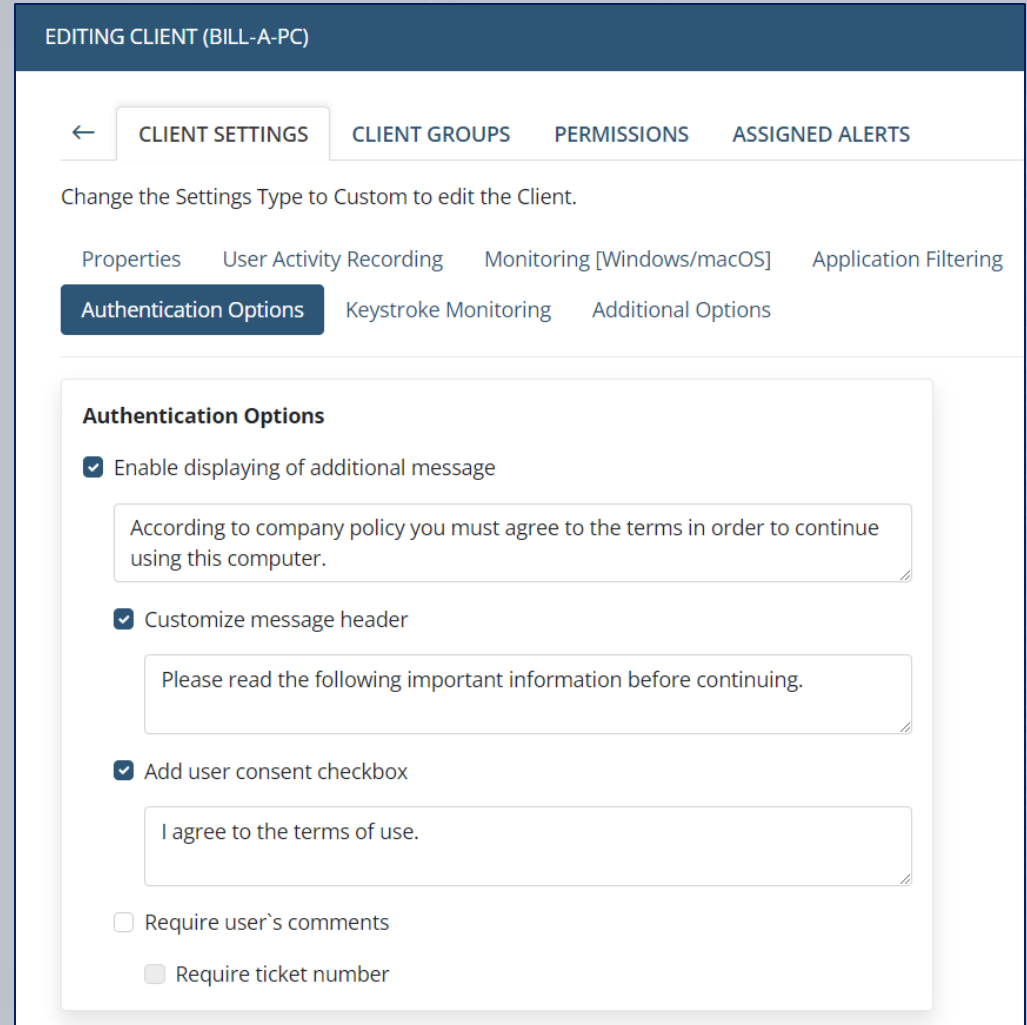
- **Enter** a valid **ticket number**, created in an **integrated ticketing system**.
- **Explain** their **reason for** needing **access**, in a comment.
- **Agree** to the **terms of use**.



The screenshot shows a dialog box with the Ekran logo at the top left. Below the logo, the text reads: "Please read the following important information before continuing." A horizontal line separates this from a larger text area containing: "According to company policy you must agree to the terms in order to continue using this computer." Below this text area, there are two input fields. The first is labeled "Ticket number is required:" and is empty. The second is labeled "Your comment is required:" and is also empty. At the bottom left, there is a checkbox with the text "I agree to the terms of use." At the bottom right, there are two buttons: "Continue" and "Cancel".

Notifying Users about Being Monitored

When enabling the **options** to be displayed to users in the **additional message**, the message texts can be **customized**.



EDITING CLIENT (BILL-A-PC)

← CLIENT SETTINGS CLIENT GROUPS PERMISSIONS ASSIGNED ALERTS

Change the Settings Type to Custom to edit the Client.

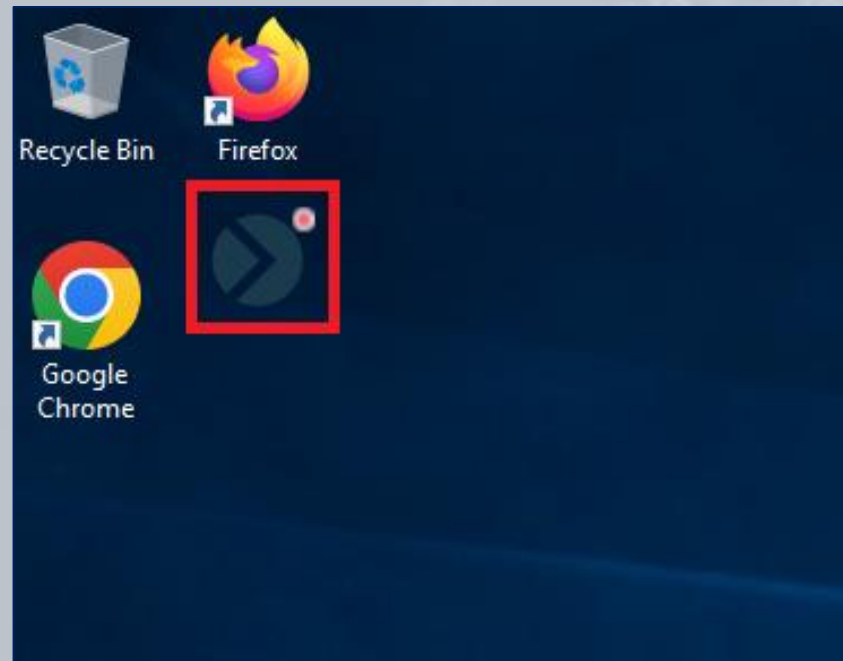
Properties User Activity Recording Monitoring [Windows/macOS] Application Filtering

Authentication Options Keystroke Monitoring Additional Options

Authentication Options

- Enable displaying of additional message
 - According to company policy you must agree to the terms in order to continue using this computer.
- Customize message header
 - Please read the following important information before continuing.
- Add user consent checkbox
 - I agree to the terms of use.
- Require user's comments
- Require ticket number

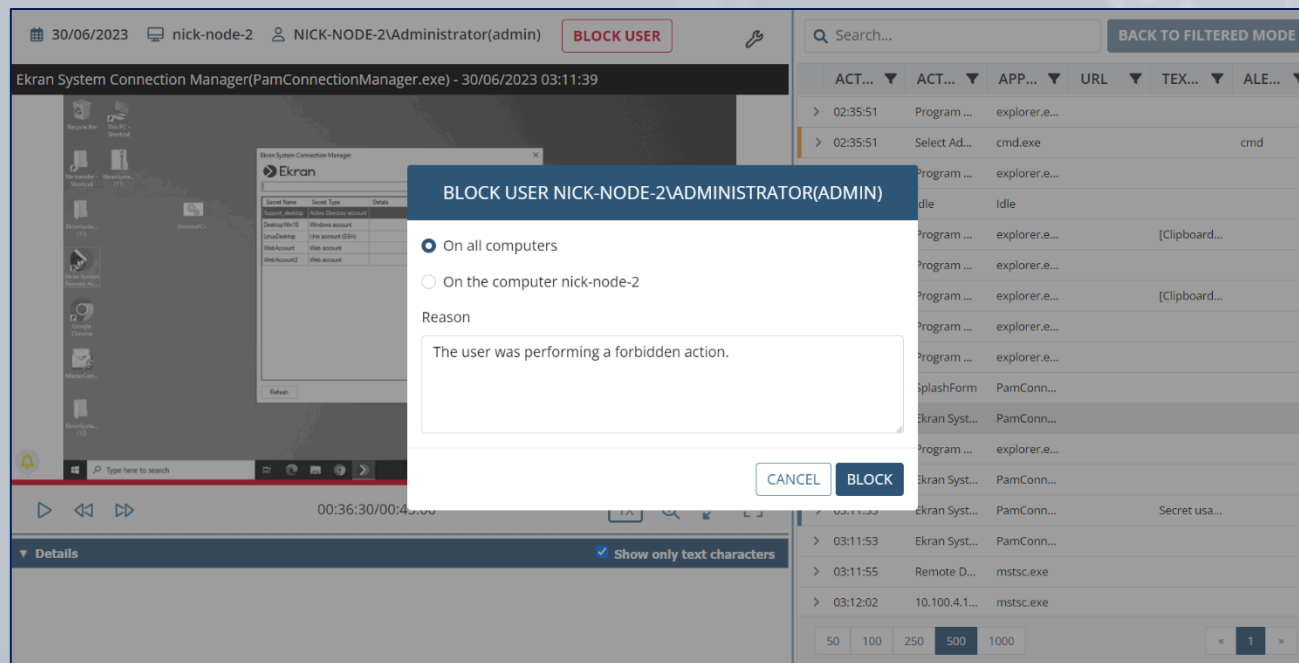
- An **icon** can also be displayed on the desktop (that is always on top of all applications opened) to **inform users** that **their actions** are currently **being monitored and recorded**.



Blocking Users

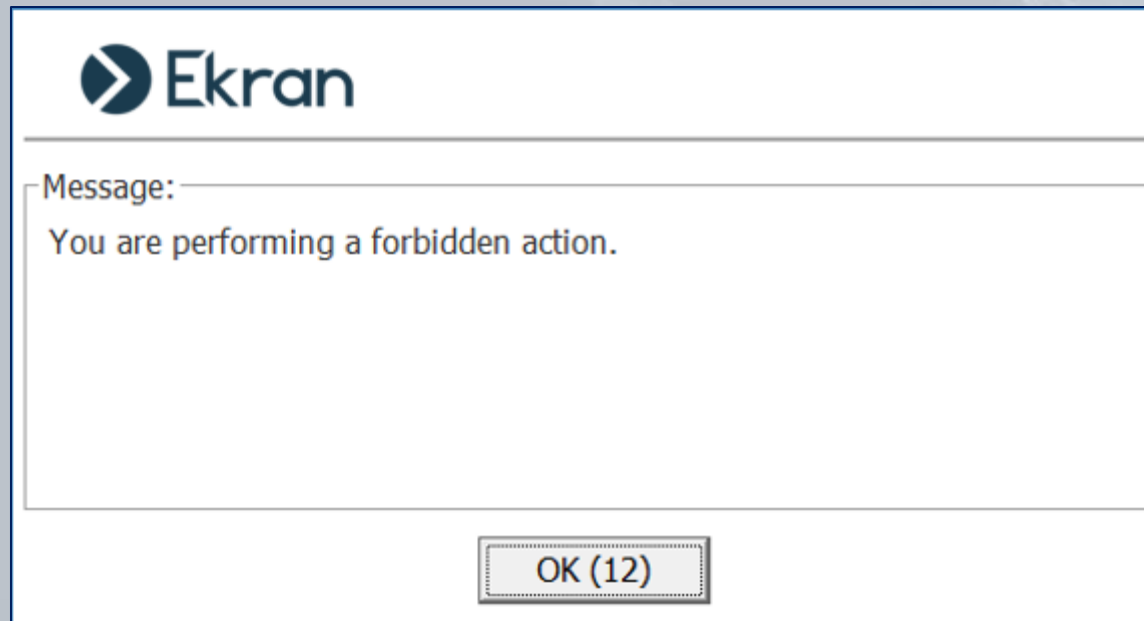
Ekran System allows you to **block endpoint users** from performing potentially harmful and forbidden actions on computers running Windows OS with Ekran System Clients installed on them.

Users can be **blocked manually** from both **Live** and **Finished** sessions, or **automatically** when they perform an action that **triggers a specific alert**.



The endpoint user's **desktop is blocked**, and after a defined time interval the user is **forcibly logged out**.

If the blocked user then tries to re-log in to the Client computer, the system will not allow them to do so.



Viewing the Blocked Users List

The **Blocked Users List** contains information on **when**, and **why** users were blocked.

To **allow** users to **access** Client computers again, simply remove them from the list.

BLOCKED USERS LIST						localhost	Built-in default tenant	⚙️	?	ADMIN	LOG OFF	EN ▾
USER ▾	BLOCKED ON ▾	BLOCKED BY ▾	DATE ▾	REASON ▾	REMOVE ALL							
WINSERVER2019\Administrator(pamuser)	WINServer2019	admin	13/07/2023 14:07:14 +03:00	The user was performing a forbidden action.	⊗							
NICK-NODE-2\Administrator	nick-node-2	admin	13/07/2023 14:08:02 +03:00	The user was performing a forbidden action.	⊗							

The accounts of Ekran System **Management Tool users** can also be **automatically locked** (for a specific duration) if they **enter incorrect login credentials multiple times**.

Administrators can also **lock** and **unlock** a user account **at any time**.

LOG IN

- **Incorrect password or login name.**
- **NOTE: In the event of 5 failed login attempts, the user account will be locked for 5 minutes.**

Use an internal or domain account to log in.

Login

Password

Remember me on this computer **LOG IN**

USER MANAGEMENT

Q Search...

▼ ALL USERS:

LOGIN ▲	FIRST NAME	LAST NAME
admin	Administrator	
user1	John	Doe

▼ ADMINISTRATORS: Users with all permissions

LOGIN ▲	FIRST NAME	LAST NAME
admin	Administrator	
user1	John	Doe

▼ SUPERVISORS: Users who can view the monitoring results of all Clients

LOGIN ▲	FIRST NAME	LAST NAME
---------	------------	-----------

▼ PAM USERS: Group does not have permission to access

LOGIN ▲	FIRST NAME	LAST NAME
---------	------------	-----------

▼ APPLICATION ACCOUNTS:

LOGIN ▲	FIRST NAME	LAST NAME
---------	------------	-----------

USER1

Do you want to unlock this user account?

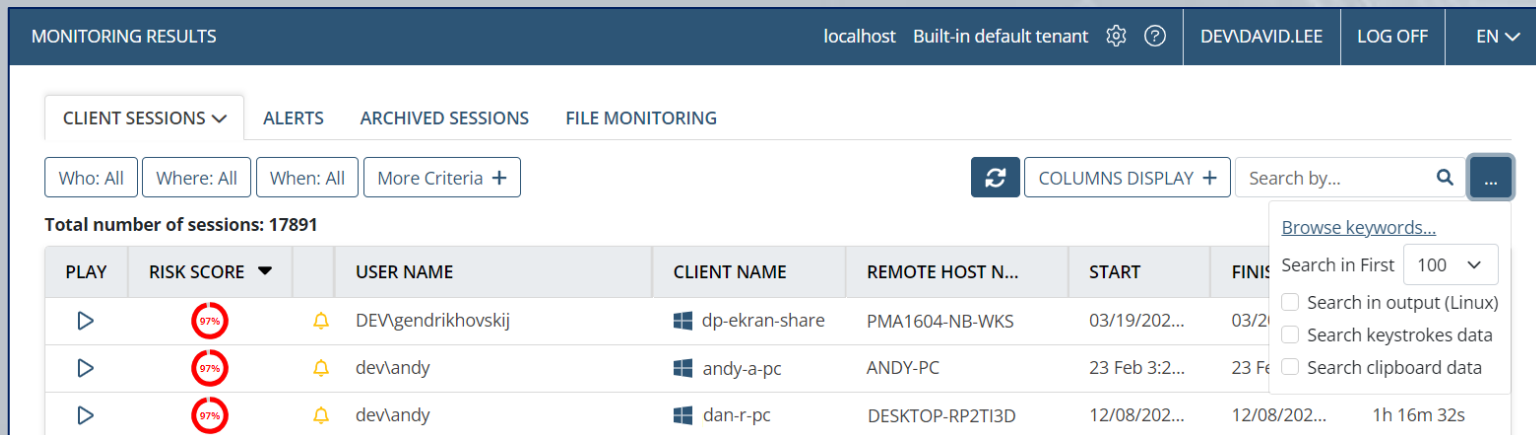
CANCEL CONFIRM

Viewing Client Sessions

Searching the Data in the Client Sessions List

The Ekran System Management Tool allows searching within the monitored sessions that are recorded by various parameters:

- **For Windows Clients:** active window title, application name, user name, Client name, URL visited, keystrokes, clipboard data, user's comment in additional message, ticket number, USB device info, etc.
- **For macOS Clients:** active window title, application name, user name, Client name, URL visited, keystrokes, clipboard data USB device info, etc.
- **For Linux Clients:** keystrokes and commands & parameters input, functions calls executed, responses output, etc.



The screenshot displays the 'MONITORING RESULTS' page in the Ekran System Management Tool. The interface includes a navigation bar with user information (localhost, Built-in default tenant, DEVAVID.LEE, LOG OFF, EN) and a main menu with 'CLIENT SESSIONS' selected. Below the menu are search filters (Who: All, Where: All, When: All, More Criteria +) and a search bar. A table lists session details with columns for PLAY, RISK SCORE, USER NAME, CLIENT NAME, REMOTE HOST N..., START, and FINIS. A search dropdown is open, showing options like 'Search in First 100', 'Search in output (Linux)', 'Search keystrokes data', and 'Search clipboard data'.

PLAY	RISK SCORE	USER NAME	CLIENT NAME	REMOTE HOST N...	START	FINIS
▶	97%	DEV\gendrikhovskij	dp-ekran-share	PMA1604-NB-WKS	03/19/202...	03/2...
▶	97%	devlandy	andy-a-pc	ANDY-PC	23 Feb 3:2...	23 Fe...
▶	97%	devlandy	dan-r-pc	DESKTOP-RP2TI3D	12/08/202...	12/08/202... 1h 16m 32s

Viewing a Session

The panes in the Session Viewer display the **screen captures and metadata** recorded in the session, where the screen captures are **played as video** and **alerts are highlighted and color-coded**.

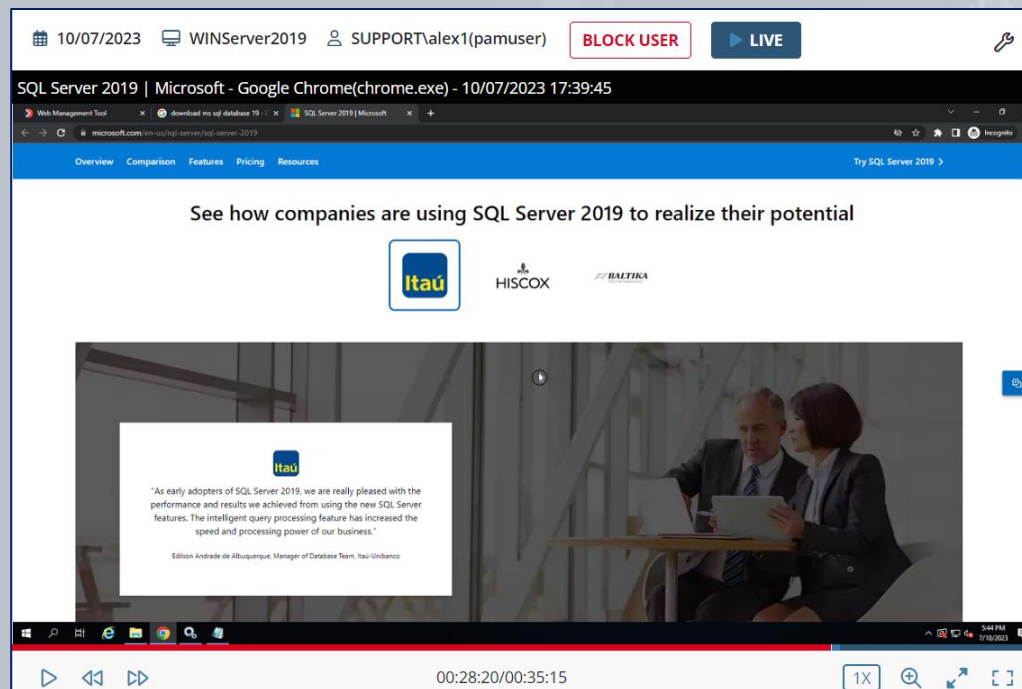
The screenshot displays the Ekran Session Viewer interface. The top bar shows the date (12/07/2023), server name (WINServer2019), user (Administrator(pamuser)), and controls for 'BLOCK USER' and 'LIVE'. The main area is split into two panes. The left pane shows a video playback of a WordPad window with the text 'secret confidential' and a red alert box 'david keystrokes alert1'. The right pane is a table of session events.

A...	ACTIVITY...	APP...	URL	TEXT DATA	ALERT/USB R...
>	19:07:28	Document - Wor...	wordpad.e...		
>	19:07:36	Document - Wor...	wordpad.e...	[Keystrokes]:	david keystrokes alert2
>	19:07:39	Document - Wor...	wordpad.e...		
>	19:07:39	Document - Wor...	wordpad.e...	[Clipboard (Copy)]:	secret
>	19:07:47	Program Manager	explorer.exe		
>	19:07:52	Document - Wor...	wordpad.e...		
>	19:07:53	Document - Wor...	wordpad.e...	[Keystrokes]:	
>	19:07:57	Document - Wor...	wordpad.e...		
>	19:08:15	Lists	wordpad.e...		
>	19:08:17	Lists	wordpad.e...		
>	19:08:18	Document - Wor...	wordpad.e...		
>	19:08:23		wordpad.e...		
>	19:08:28	Document - Wor...	wordpad.e...		
>	19:08:37		wordpad.e...		
>	19:08:38	Document - Wor...	wordpad.e...		
>	19:08:47	Document - Wor...	wordpad.e...	[Keystrokes]:	david keystrokes alert2
>	19:08:48	Document - Wor...	wordpad.e...		
>	19:08:58	Document - Wor...	wordpad.e...	[Keystrokes]:	david keystrokes alert1
>	19:08:59	Document - Wor...	wordpad.e...		
>	19:10:03		explorer.exe		
>	19:10:10	Program Manager	explorer.exe		

Details pane: Alert ID: 19260, Alert Name: david keystrokes alert1, Risk Level: Critical, What: Document - WordPad, When: 12/07/2023 19:08:58

Ekran System allows you to perform **monitoring** of user activity on Clients computer **in real time**.

You can connect to a **Live** session and observe the activities a user is performing at any given moment (and **block the user** if required).



The Magnifying Glass

You can also enlarge any area of the video in the Session Player pane by using the **Magnifying Glass**.

The screenshot displays the Ekran Session Player interface. The main window shows a video player with a magnifying glass icon over a video frame. The video frame shows a man and a woman in a meeting, with a magnifying glass over a text box that reads: "As early adopters of SQL Server 2019, we are really pleased with the performance and results we achieved from using the new SQL Server features. The intelligent query processing feature has increased the speed and processing power of our business." Below the video frame, there is a "Details" pane showing the URL: "microsoft.com/en-us/sql-server/sql-server-2019".

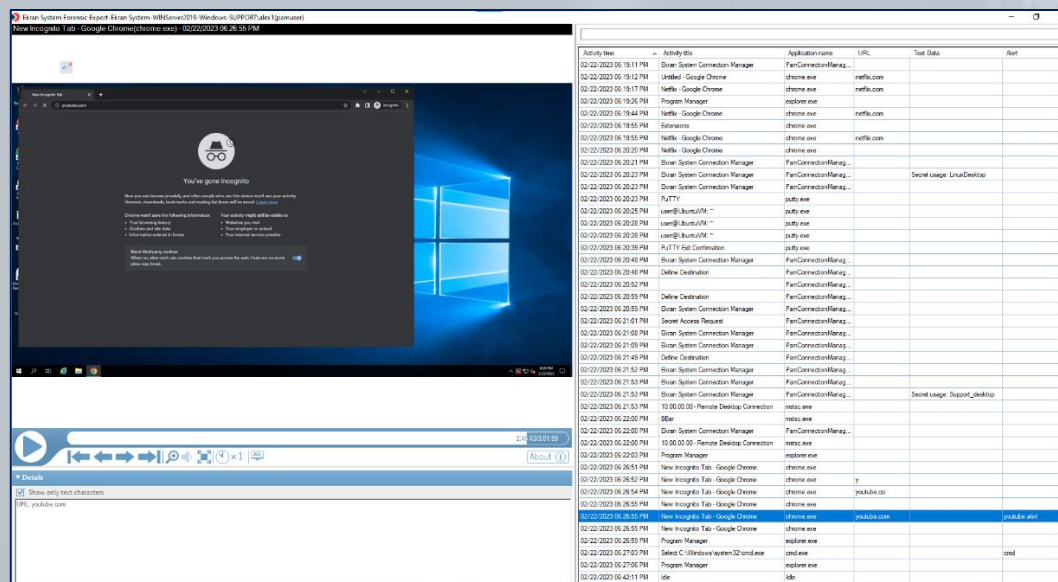
On the right side of the interface, there is an active process list. The list is titled "Search..." and "ACTIVI...". It contains a table of active processes:

Time	Process Name	Process ID	Process Path
17:15:48	Idle		
17:27:10	Web Mana		
17:27:13	Web Mana		
17:27:13	Web Mana		
17:27:15	Web Mana		
17:27:16	Web Manage...	chrome.exe	localhost
17:27:25	Web Manage...	chrome.exe	localhost
17:28:07	localhost/Ekr...	chrome.exe	localhost
17:28:10	Web Manage...	chrome.exe	localhost
17:28:11	Web Manage...	chrome.exe	localhost
17:28:19	localhost/Ekr...	chrome.exe	localhost
17:28:22	Web Manage...	chrome.exe	localhost
17:28:23	Web Manage...	chrome.exe	localhost
17:32:44	explorer.exe		
17:32:44	Services	mmc.exe	
17:32:46	Context	mmc.exe	
17:32:49	EkranServer P...	mmc.exe	
17:32:53	Services	mmc.exe	
17:33:36	Context	mmc.exe	
17:33:38		mmc.exe	
17:33:40	EkranServer P...	mmc.exe	

At the bottom of the process list, there are pagination controls showing "50 100 250 500 1000" and a page number "1".

With Ekran System **Forensic Export**, you can:

- **Export** selected **monitored sessions** (or all or part of one) to a securely **encrypted** file, and **verify its integrity**.
- **Investigate** the user activity **data recorded** by using the offline Ekran Forensic Player.
- Present **evidence** in a **forensic format** to third parties.



Anonymizer

(for e.g. GDPR compliance)

The **Anonymizer** (also known as **Pseudonymizer** or **Monitored Data Anonymization**) feature allows **compliance with data protection and privacy laws**, standards and regulations, such as the European Union's General Data Protection Regulation (**GDPR**) law in relation to protecting personally identifiable information (PII).

PII means any **personal data** that can directly identify an individual person.



Pseudonymizing the PII Data

Protection of the PPI of endpoint users, that is recorded during monitoring of their activities by Ekran System, is achieved by the system **pseudonymizing** this data (i.e. hiding and replacing it with **randomized values** when viewed).

MONITORING RESULTS localhost Built-in default tenant INVESTIGATOR LOG OFF EN

CLIENT SESSIONS ▾ ALERTS

Who: All Where: All When: All More Criteria +

COLUMNS DISPLAY + Search by... 🔍 ...

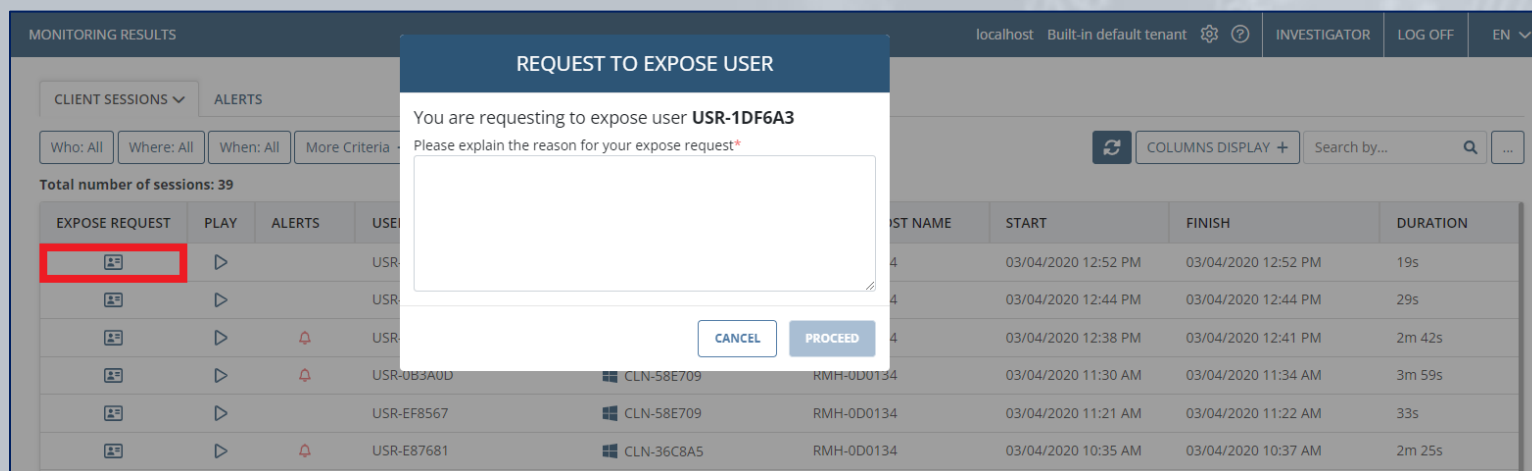
Total number of sessions: 39

EXPOSE REQUEST	PLAY	ALERTS	USER NAME	CLIENT NAME	REMOTE HOST NAME	START	FINISH	DURATION
	▶		USR-1DF6A3	CLN-36C8A5	RMH-0D0134	03/04/2020 12:52 PM	03/04/2020 12:52 PM	19s
	▶		USR-D09E74	CLN-36C8A5	RMH-0D0134	03/04/2020 12:44 PM	03/04/2020 12:44 PM	29s
	▶	🚫	USR-A1699F	CLN-58E709	RMH-0D0134	03/04/2020 12:38 PM	03/04/2020 12:41 PM	2m 42s
	▶	🚫	USR-0B3A0D	CLN-58E709	RMH-0D0134	03/04/2020 11:30 AM	03/04/2020 11:34 AM	3m 59s
	▶		USR-EF8567	CLN-58E709	RMH-0D0134	03/04/2020 11:21 AM	03/04/2020 11:22 AM	33s
	▶	🚫	USR-E87681	CLN-36C8A5	RMH-0D0134	03/04/2020 10:35 AM	03/04/2020 10:37 AM	2m 25s
	▶		USR-3E46EF	CLN-2A5D5F	RMH-0D0134	10/24/2018 5:21 PM	10/24/2018 5:25 PM	3m 35s
	▶	⚠️	USR-5CC3D3	CLN-7250E4	RMH-276CC5	07/18/2018 3:16 PM	07/18/2018 3:19 PM	3m 24s
	▶	⚠️	USR-71D171	CLN-092B04	RMH-0D0134	07/17/2018 3:35 PM	07/17/2018 3:37 PM	2m 8s
	▶	⚠️	USR-6D46B8	CLN-52552D	RMH-0D0134	07/17/2018 1:18 PM	07/17/2018 1:21 PM	3m 17s
	▶	⚠️	USR-FFFA7A	CLN-08149F	RMH-0D0134	07/17/2018 12:55 PM	07/17/2018 1:00 PM	5m 2s
	▶	⚠️	USR-A5054E	CLN-5F454B	RMH-0D0134	07/17/2018 11:59 AM	07/17/2018 12:08 PM	8m 29s
	▶	🚫	USR-97C044	CLN-380515	RMH-0D0134	07/16/2018 12:20 PM	07/16/2018 12:26 PM	5m 45s
	▶	🚫	USR-3ECCAD	CLN-3F4581	RMH-0D0134	07/16/2018 11:25 AM	07/16/2018 11:29 AM	4m 2s

LOAD MORE

Results on page 20 ▾

In **Anonymized mode**, no Management Tool user, including administrators and other users (e.g. **investigators**) that have permission to open and view the sessions of endpoint users, can view the personal data of any endpoint users unless a **request by them is first approved** (by a **supervisor**) to **temporarily de-anonymize** the data of a specific endpoint user (on a specific Client computer).



At the same time, **supervisors do not have permission** to open and **view the sessions** of endpoint users.

Temporarily De-Anonymizing PII Data

If an **investigator's request is approved** (by a supervisor) to **de-anonymize** the PII data of a specific endpoint user (on a specific Client computer), **that user's data is temporarily deanonymized for that investigator only to view.**

MONITORING RESULTS localhost Built-in default tenant INVESTIGATOR LOG OFF EN

CLIENT SESSIONS ▾ ALERTS

Who: All Where: All When: All More Criteria + COLUMNS DISPLAY + Search by...

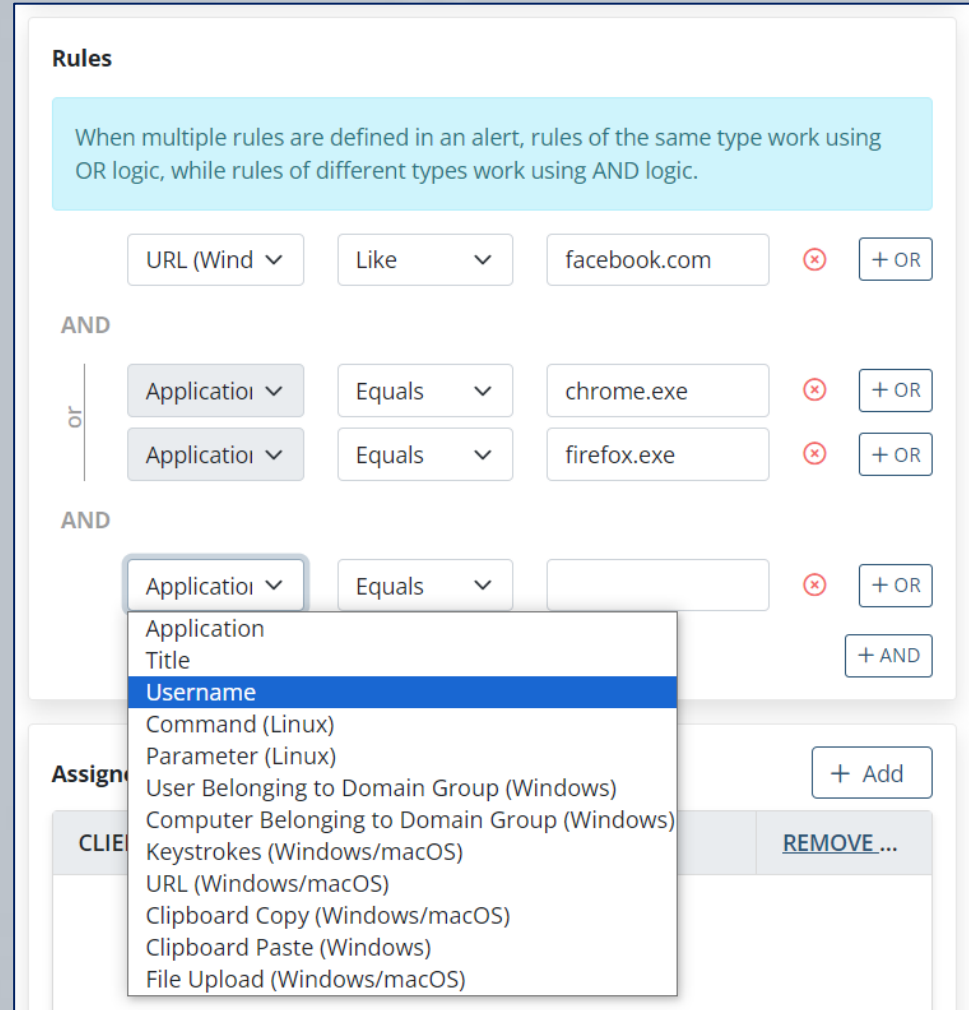
Total number of sessions: 39

EXPOSE REQUEST	PLAY	ALERTS	USER NAME	CLIENT NAME	REMOTE HOST NAME	START	FINISH	DURATION
			DEMO\Alan.Simpson	EnterpServ		03/04/2020 12:52 PM	03/04/2020 12:52 PM	19s
			USR-D09E74	CLN-36C8A5	RMH-0D0134	03/04/2020 12:44 PM	03/04/2020 12:44 PM	29s
			USR-A1699F	CLN-58E709	RMH-0D0134	03/04/2020 12:38 PM	03/04/2020 12:41 PM	2m 42s
			USR-0B3A0D	CLN-58E709	RMH-0D0134	03/04/2020 11:30 AM	03/04/2020 11:34 AM	3m 59s
			USR-EF8567	CLN-58E709	RMH-0D0134	03/04/2020 11:21 AM	03/04/2020 11:22 AM	33s
			USR-E87681	CLN-36C8A5	RMH-0D0134	03/04/2020 10:35 AM	03/04/2020 10:37 AM	2m 25s
			USR-3E46EF	CLN-2A5D5F	RMH-0D0134	10/24/2018 5:21 PM	10/24/2018 5:25 PM	3m 35s
			USR-5CC3D3	CLN-7250E4	RMH-276CC5	07/18/2018 3:16 PM	07/18/2018 3:19 PM	3m 24s
			USR-71D171	CLN-092B04	RMH-0D0134	07/17/2018 3:35 PM	07/17/2018 3:37 PM	2m 8s
			USR-6D46B8	CLN-52552D	RMH-0D0134	07/17/2018 1:18 PM	07/17/2018 1:21 PM	3m 17s

Alerts

Ekran System allows you to facilitate **rapid incident response** by using alert notifications:

- **Add alert rules** to detect specific suspicious user activity on Client computers.
- Specify individuals to receive instant **alert notifications** via email and tray notifications.



The screenshot shows the 'Rules' configuration interface in the Ekran System. A light blue informational box at the top states: 'When multiple rules are defined in an alert, rules of the same type work using OR logic, while rules of different types work using AND logic.'

The interface displays a rule configuration with the following elements:

- Rule 1:** URL (Wind) Like facebook.com
- Logic:** AND
- Rule 2:** Application Equals chrome.exe
- Rule 3:** Application Equals firefox.exe
- Logic:** AND
- Rule 4:** Application Equals (empty)
- Logic:** AND

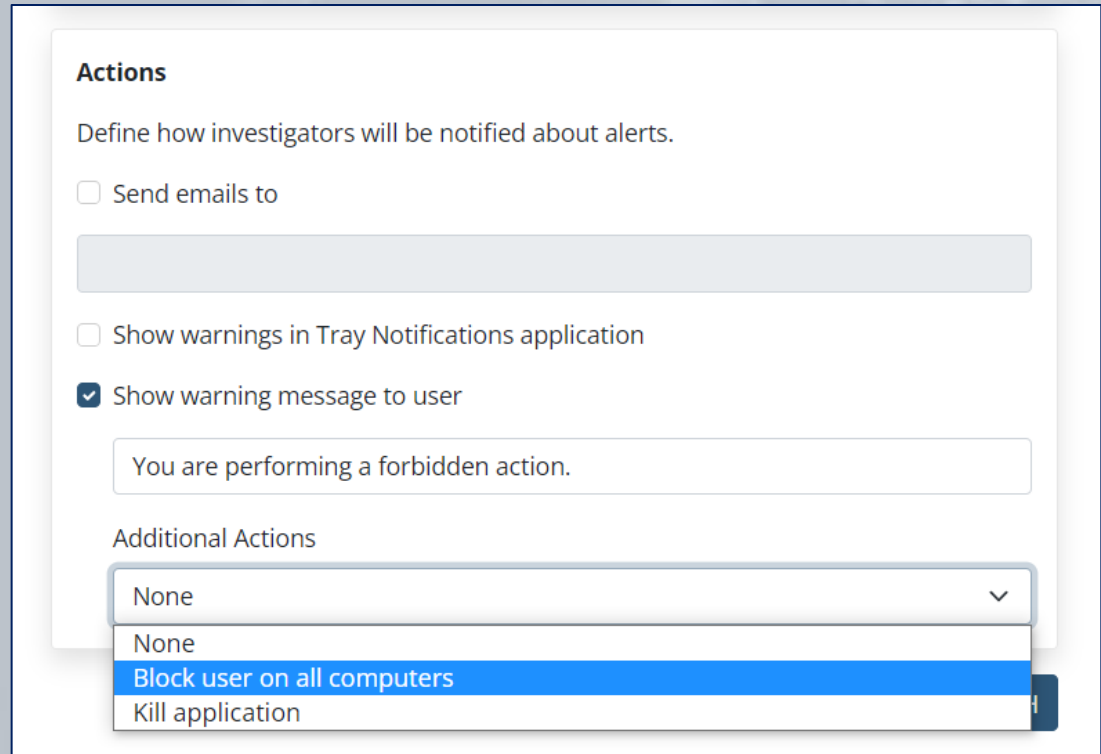
A dropdown menu is open for the 'Application' field of Rule 4, showing the following options:

- Application
- Title
- Username** (highlighted)
- Command (Linux)
- Parameter (Linux)
- User Belonging to Domain Group (Windows)
- Computer Belonging to Domain Group (Windows)
- Keystrokes (Windows/macOS)
- URL (Windows/macOS)
- Clipboard Copy (Windows/macOS)
- Clipboard Paste (Windows)
- File Upload (Windows/macOS)

Buttons for '+ OR', '+ AND', '+ Add', and 'REMOVE...' are visible at the bottom of the interface.

You can also set an alert to:

- Display a **warning message** to the **user** when the alert is triggered (the message can be edited).
- **Block** the **user**.
- Forcibly **stop the application**.



Actions

Define how 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

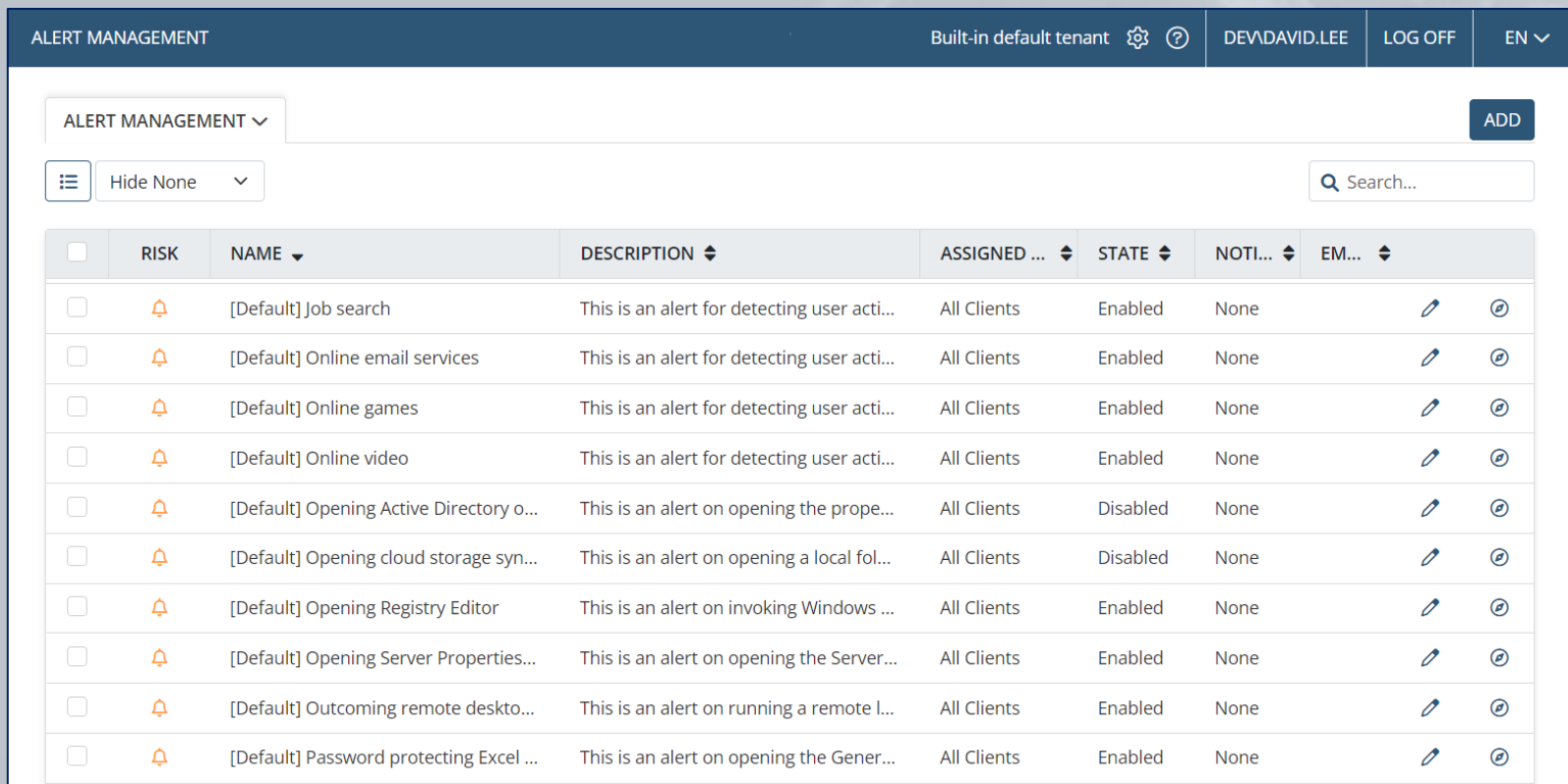
None

None

Block user on all computers

Kill application

Ekran System contains a set of default alerts prepared by the vendor's security experts. They will inform you about **data leakage** or potentially **fraudulent, illicit, or non-work-related** activities.






The screenshot shows the 'ALERT MANAGEMENT' interface. At the top, there's a navigation bar with 'ALERT MANAGEMENT' on the left, and 'Built-in default tenant', 'DEVIDAVID.LEE', 'LOG OFF', and 'EN' on the right. Below the navigation bar, there's a search bar with 'Search...' and an 'ADD' button. A 'Hide None' dropdown is also visible. The main content is a table with columns: RISK, NAME, DESCRIPTION, ASSIGNED, STATE, NOTI..., and EM... The table lists ten default alerts, each with a checkbox, a risk level (bell icon), a name, a description, an assigned entity (All Clients), a state (Enabled or Disabled), and notification options (edit and delete icons).

<input type="checkbox"/>	RISK	NAME	DESCRIPTION	ASSIGNED ...	STATE	NOTI...	EM...
<input type="checkbox"/>	🔔	[Default] Job search	This is an alert for detecting user acti...	All Clients	Enabled	None	
<input type="checkbox"/>	🔔	[Default] Online email services	This is an alert for detecting user acti...	All Clients	Enabled	None	
<input type="checkbox"/>	🔔	[Default] Online games	This is an alert for detecting user acti...	All Clients	Enabled	None	
<input type="checkbox"/>	🔔	[Default] Online video	This is an alert for detecting user acti...	All Clients	Enabled	None	
<input type="checkbox"/>	🔔	[Default] Opening Active Directory o...	This is an alert on opening the prope...	All Clients	Disabled	None	
<input type="checkbox"/>	🔔	[Default] Opening cloud storage syn...	This is an alert on opening a local fol...	All Clients	Disabled	None	
<input type="checkbox"/>	🔔	[Default] Opening Registry Editor	This is an alert on invoking Windows ...	All Clients	Enabled	None	
<input type="checkbox"/>	🔔	[Default] Opening Server Properties...	This is an alert on opening the Server...	All Clients	Enabled	None	
<input type="checkbox"/>	🔔	[Default] Outcoming remote deskto...	This is an alert on running a remote l...	All Clients	Enabled	None	
<input type="checkbox"/>	🔔	[Default] Password protecting Excel ...	This is an alert on opening the Gener...	All Clients	Enabled	None	





























Viewing Alert Events

The list of alerts triggered can be **viewed and managed** on the **Alerts tab**, where the **Status** can be changed and **Notes** added.

MONITORING RESULTS Built-in default tenant   ADMIN LOG OFF EN 

CLIENT SESSIONS **ALERTS** ARCHIVED SESSIONS FORENSIC EXPORT HISTORY

Risk: All Name: All OS: All Who: All When: All Where: All **Status: All**

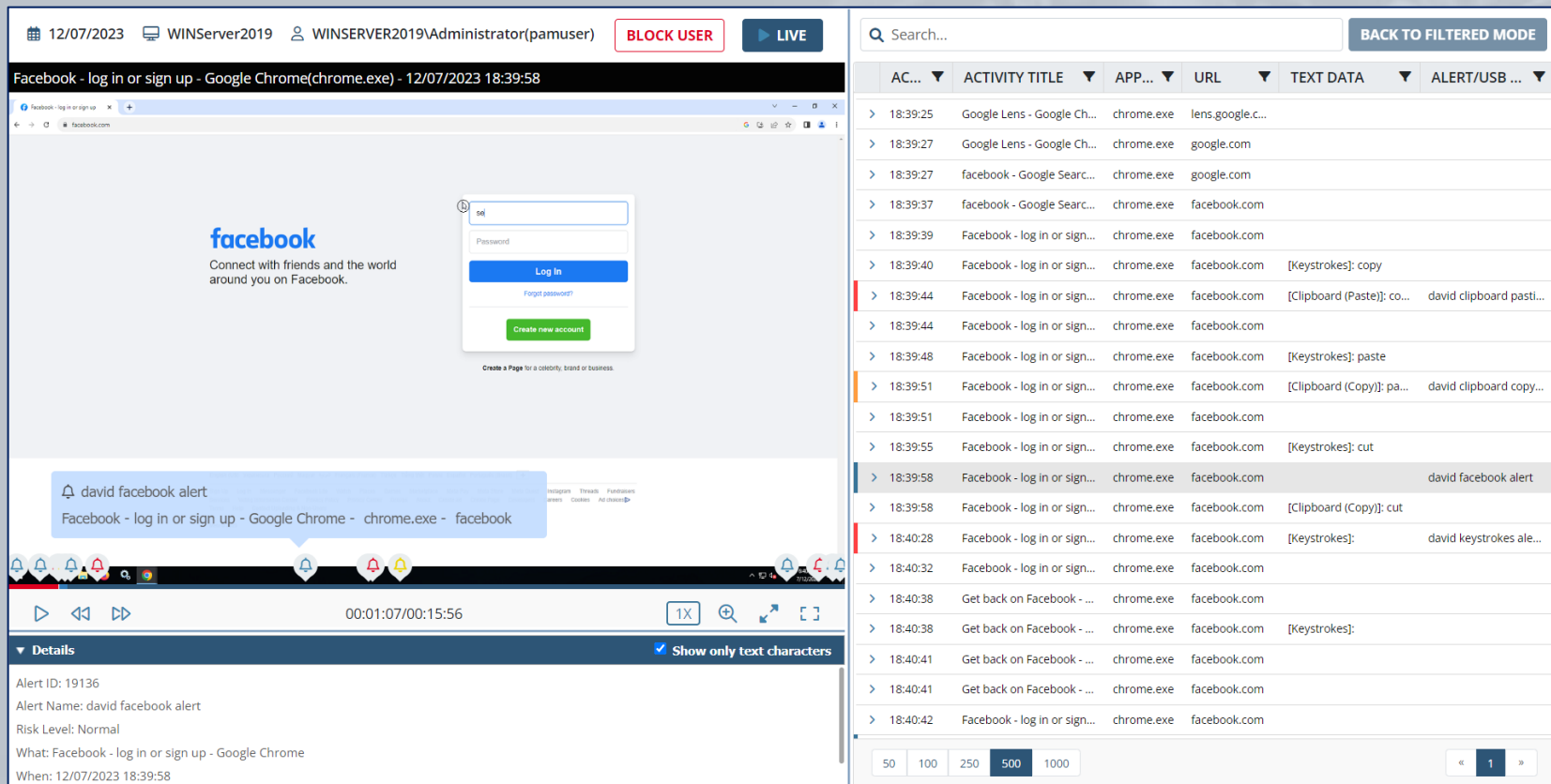
<input type="checkbox"/>	PLAY	ALERT ID	RISK	NAME	WHERE	WHEN	KEY...	STATUS	NOTES
<input type="checkbox"/>		394		using secret documents alert	Test-PC	4:57 PM	ima	New	 Add 
<input type="checkbox"/>		393		alert by url	Test-PC	4:57 PM	wiki	New	 Add 
<input type="checkbox"/>		389		applications with approval	Test-PC	4:42 PM	calc	In Progress	 Add (+3) 
<input type="checkbox"/>		384		terc	Test-PC	4:41 PM	wiki	False Alarm	 Add (+2) 
<input type="checkbox"/>		383		alert by url	Test-PC	4:41 PM	wiki	New	 Add 
<input type="checkbox"/>		382		using secret documents alert	Test-PC	4:41 PM	ima	Resolved	 Add 
<input type="checkbox"/>		371		using secret documents alert	WIN-AG...	4:41 PM	ima	Confirmed Risk	 Add 

Filter dropdown (Status: All):

- Confirmed Risk
- False Alarm
- In Progress
- New
- Resolved

Viewing Alert Events in the Session Viewer

Monitored data associated with alert events is **highlighted** in the Session Viewer (in different **colors** depending on the **alert risk level**).



The screenshot displays the Session Viewer interface. The top bar shows the date 12/07/2023, the system name WINServer2019, the user WINSERVER2019\Administrator(pamuser), and buttons for 'BLOCK USER' and 'LIVE'. The main window shows a Facebook login page with a search bar containing 'david', a password field, and a 'Log In' button. A blue alert notification is visible at the bottom of the browser window: 'david facebook alert' with details 'Facebook - log in or sign up - Google Chrome - chrome.exe - facebook'. The right sidebar contains a search bar and a table of alert events.

AC...	ACTIVITY TITLE	APP...	URL	TEXT DATA	ALERT/USB ...
>	18:39:25	Google Lens - Google Ch...	chrome.exe	lens.google.c...	
>	18:39:27	Google Lens - Google Ch...	chrome.exe	google.com	
>	18:39:27	facebook - Google Sear...	chrome.exe	google.com	
>	18:39:37	facebook - Google Sear...	chrome.exe	facebook.com	
>	18:39:39	Facebook - log in or sign...	chrome.exe	facebook.com	
>	18:39:40	Facebook - log in or sign...	chrome.exe	facebook.com	[Keystrokes]: copy
>	18:39:44	Facebook - log in or sign...	chrome.exe	facebook.com	[Clipboard (Paste)]: co... david clipboard pasti...
>	18:39:44	Facebook - log in or sign...	chrome.exe	facebook.com	
>	18:39:48	Facebook - log in or sign...	chrome.exe	facebook.com	[Keystrokes]: paste
>	18:39:51	Facebook - log in or sign...	chrome.exe	facebook.com	[Clipboard (Copy)]: pa... david clipboard copy...
>	18:39:51	Facebook - log in or sign...	chrome.exe	facebook.com	
>	18:39:55	Facebook - log in or sign...	chrome.exe	facebook.com	[Keystrokes]: cut
>	18:39:58	Facebook - log in or sign...	chrome.exe	facebook.com	david facebook alert
>	18:39:58	Facebook - log in or sign...	chrome.exe	facebook.com	[Clipboard (Copy)]: cut
>	18:40:28	Facebook - log in or sign...	chrome.exe	facebook.com	[Keystrokes]: david keystrokes ale...
>	18:40:32	Facebook - log in or sign...	chrome.exe	facebook.com	
>	18:40:38	Get back on Facebook - ...	chrome.exe	facebook.com	
>	18:40:38	Get back on Facebook - ...	chrome.exe	facebook.com	[Keystrokes]:
>	18:40:41	Get back on Facebook - ...	chrome.exe	facebook.com	
>	18:40:41	Get back on Facebook - ...	chrome.exe	facebook.com	
>	18:40:42	Facebook - log in or sign...	chrome.exe	facebook.com	

Receiving Alert Notifications

You can receive **alert notifications** in **real time**, and review them in the Ekran System Tray Notifications log file, as well as open the sessions with the alert-related data in the Session Viewer.



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

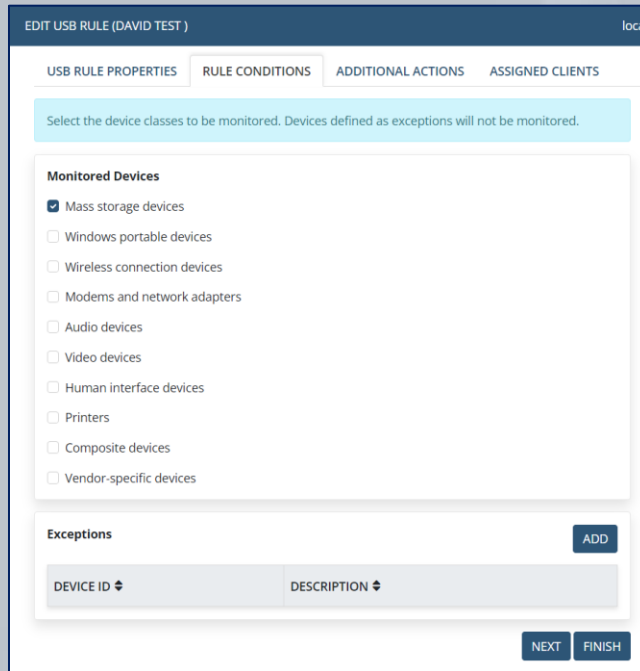
USB Device Monitoring

Ekran System provides **two types of monitoring** for USB devices plugged in to Client computers:

- **Automatic USB device monitoring**, to view information on devices plugged in and detected by Windows Client computers as USB devices.
- **Non-automatic USB device monitoring**, by adding **USB monitoring rules** for in-depth **analysis** of devices plugged in to both Windows or macOS Client computers, and for **alert notifications to be received**, and (for Windows Client computers only) for **blocking** USB devices on Windows Clients.

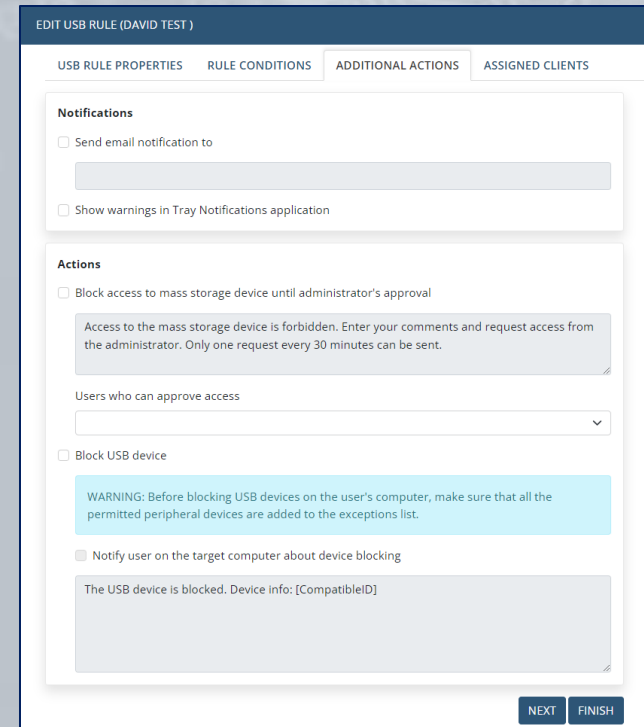
Adding USB Monitoring Rules

Ekran System can **detect USB devices** connected to a computer, **alert** you when a device is plugged in, and block their usage or **forbid** access to them until **administrator approval** (either for all devices of a certain class, or all devices except permitted ones) on a Client computer.



The screenshot shows the 'EDIT USB RULE (DAVID TEST)' interface with the 'RULE CONDITIONS' tab selected. The 'Monitored Devices' section has a list of device classes with checkboxes. 'Mass storage devices' is checked, while others are unchecked. Below this is an 'Exceptions' section with a table for adding exceptions. The table has columns for 'DEVICE ID' and 'DESCRIPTION'. There are 'NEXT' and 'FINISH' buttons at the bottom right.

DEVICE ID	DESCRIPTION
-----------	-------------



The screenshot shows the 'EDIT USB RULE (DAVID TEST)' interface with the 'ADDITIONAL ACTIONS' tab selected. The 'Notifications' section has two checkboxes: 'Send email notification to' and 'Show warnings in Tray Notifications application'. The 'Actions' section has a checkbox for 'Block access to mass storage device until administrator's approval'. Below this is a text area for a warning message: 'Access to the mass storage device is forbidden. Enter your comments and request access from the administrator. Only one request every 30 minutes can be sent.' There is a dropdown for 'Users who can approve access'. Another checkbox is 'Block USB device', followed by a warning message: 'WARNING: Before blocking USB devices on the user's computer, make sure that all the permitted peripheral devices are added to the exceptions list.' Below that is a checkbox for 'Notify user on the target computer about device blocking' and a text area for a notification message: 'The USB device is blocked. Device info: [CompatibleID]'. There are 'NEXT' and 'FINISH' buttons at the bottom right.

Automatic USB Device Monitoring

USB-based devices are **automatically detected** when they are **plugged in** to Windows Client computers.

Screen captures recorded when USB devices are **plugged in** or **blocked** are **highlighted** in the Session Viewer.

30/03/2023 WIN-UEE4P71DD32 WIN-UEE4P71DD32\Administrator(admin) BLOCK USER LIVE

USBStorage - E:\ - EV([Monitoring event]) - 30/03/2023 14:58:11

File Explorer window showing 'This PC' with 'Devices and drives (3)' section. A red box highlights the 'E:' drive with '29.7 GB free of 29.7 GB'.

Activity Log Table:

ACTIVITY TIME	ACTIVITY TITLE	APPLICATION N...	URL	TEXT DATA	ALERT/USB R...
> 14:57:10	Please wait while the a...	ServerManager.exe			
> 14:57:11	Server Manager	ServerManager.exe			
> 14:57:12	Program Manager	explorer.exe			
> 14:57:17		explorer.exe			
> 14:57:35	Program Manager	explorer.exe			
> 14:57:57		explorer.exe			
> 14:57:59	File Explorer	explorer.exe			
> 14:57:59	This PC	explorer.exe			
> 14:58:11	USBStorage - E:\ - EV	[Monitoring event]			
> 14:58:47		explorer.exe			
> 14:58:47	New Incognito Tab - G...	chrome.exe			
> 14:58:49	This PC	explorer.exe			
> 14:58:50	Mozilla Firefox	firefox.exe			
> 14:58:50	Mozilla Firefox	firefox.exe	localhost		
> 14:58:53	Downloads Ekran Sy...	firefox.exe	www.ekra...		
> 14:58:55	Downloads Ekran Sy...	firefox.exe	www.ekra...		
> 14:58:55	Mozilla Firefox	firefox.exe	www.ekra...		
> 14:59:04	Web Management Too...	firefox.exe	localhost		
> 14:59:08	Web Management Too...	firefox.exe	localhost		
> 14:59:25	Web Management Too...	firefox.exe	localhost		
> 14:59:29	Web Management Too...	firefox.exe			
> 14:59:29	Mozilla Firefox	firefox.exe			
> 14:59:29	[Live] WIN-UEE4P71D...	firefox.exe	localhost		

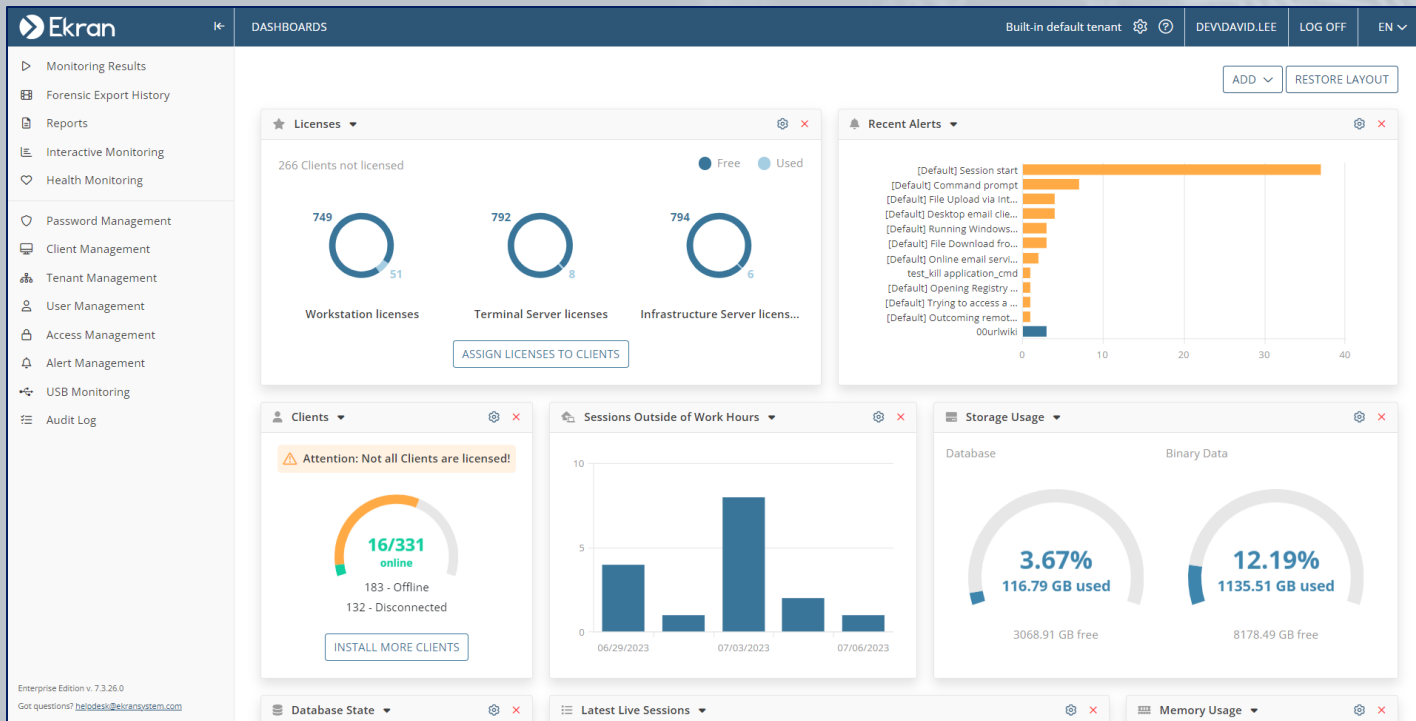
Details pane showing USB device information:

```
USB Mass Storage Device
USB\Class_08&SubClass_06&Prot_50
USB\VID_13FE&PID_3600&REV_0100\07A70E01AE601298
12/07/2018 18:03:23
```

Dashboards

Dashboards offer a **convenient real-time view** of the **most useful data** grouped together in **one place**.

You can **customize** the dashboards (on the **Home** and **Health Monitoring** pages) by adjusting their **appearance and settings**.



There are four main types of Ekran System dashboards:

System State Dashboards

- Licenses
- Clients
- Database Storage Usage

Monitoring Dashboards

- Recent Alerts
- Latest Live Sessions

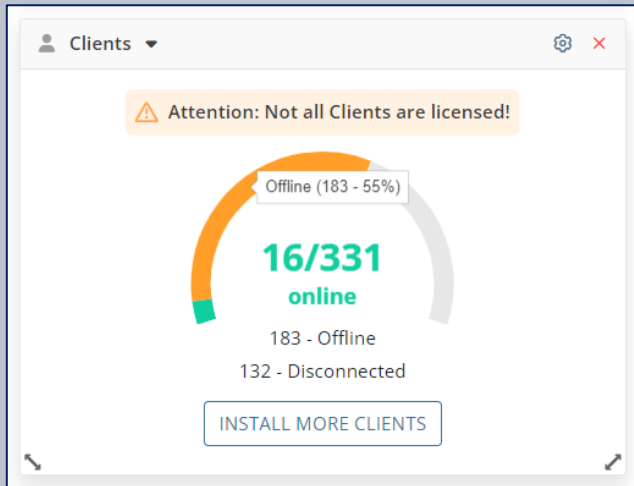
Threat Detection Dashboards

- Sessions Outside of Work Hours
- Rarely Used Computers
- Rarely Used Logins

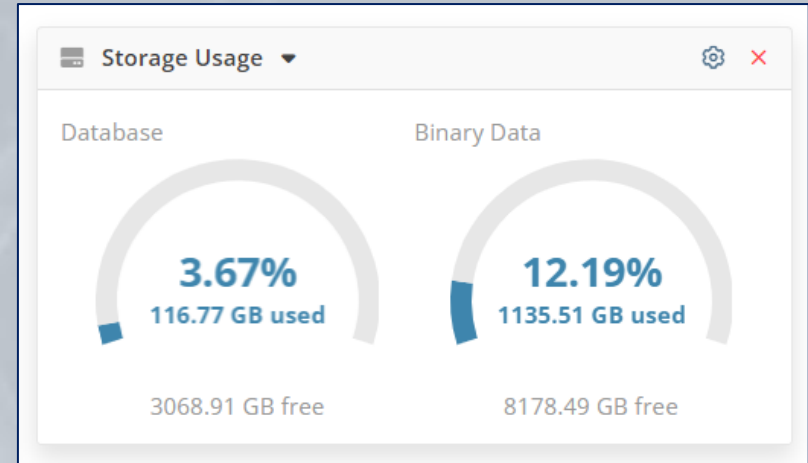
Server Resource Monitoring Dashboards

- CPU Usage
- Memory Usage
- The Database State

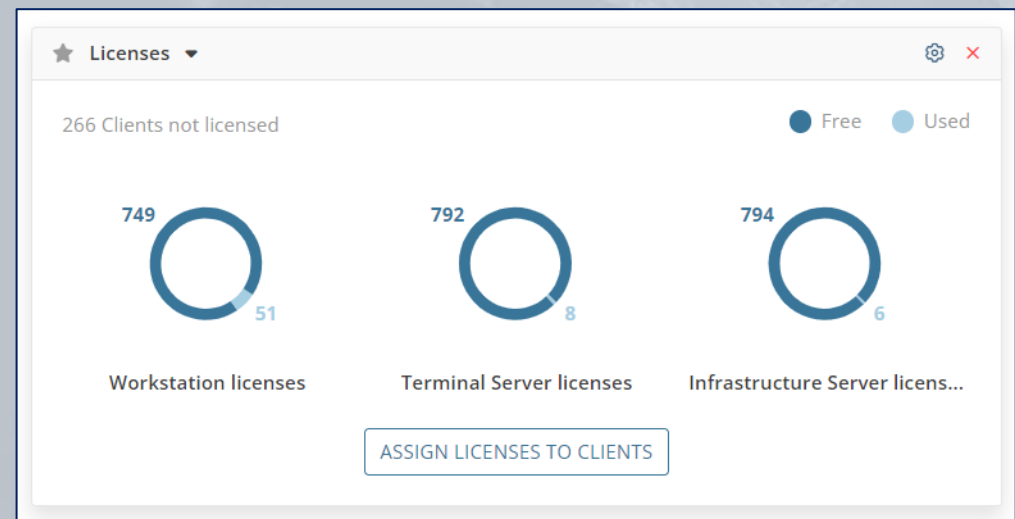
Clients



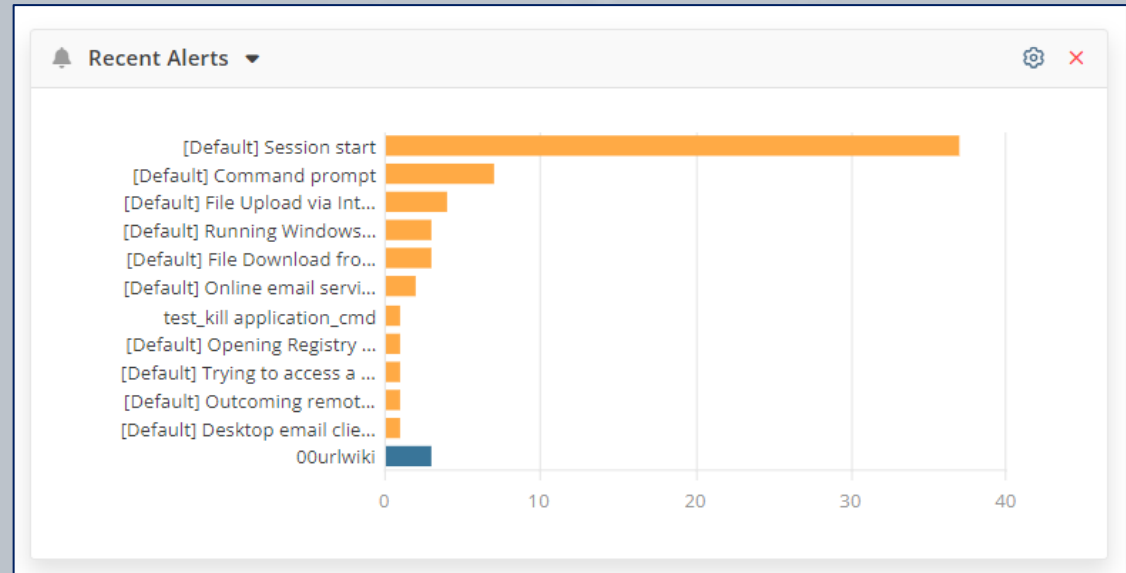
Storage Usage



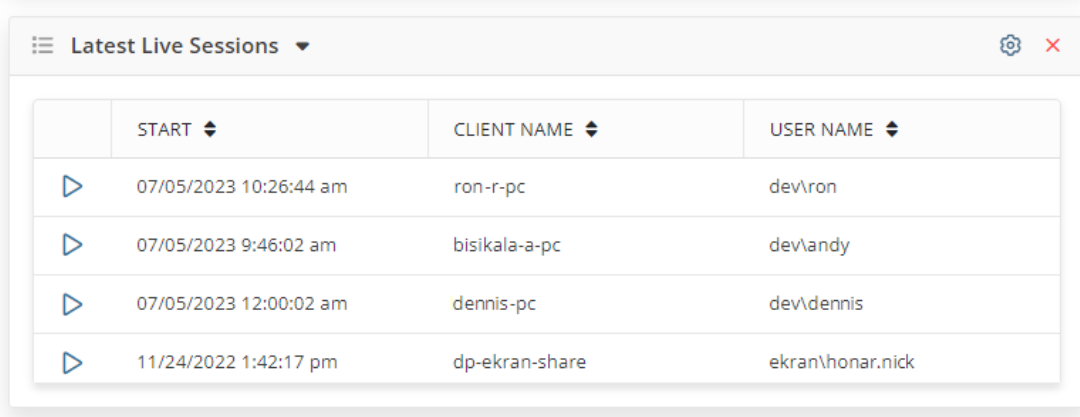
Licenses



Recent Alerts



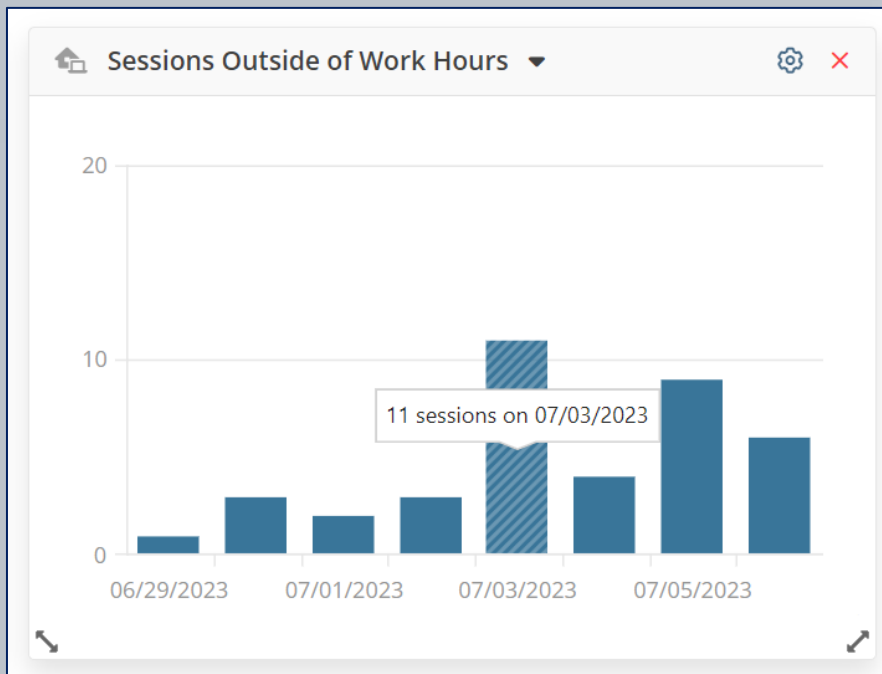
Latest Live Sessions



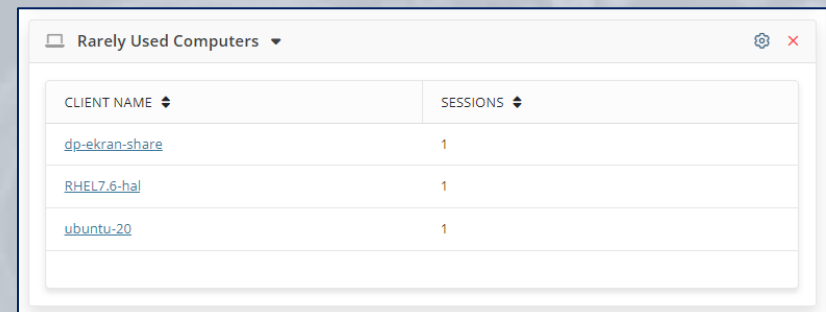
Latest Live Sessions

	START	CLIENT NAME	USER NAME
▶	07/05/2023 10:26:44 am	ron-r-pc	dev\ron
▶	07/05/2023 9:46:02 am	bisikala-a-pc	dev\andy
▶	07/05/2023 12:00:02 am	dennis-pc	dev\dennis
▶	11/24/2022 1:42:17 pm	dp-ekran-share	ekran\honar.nick

Sessions Outside of Work Hours



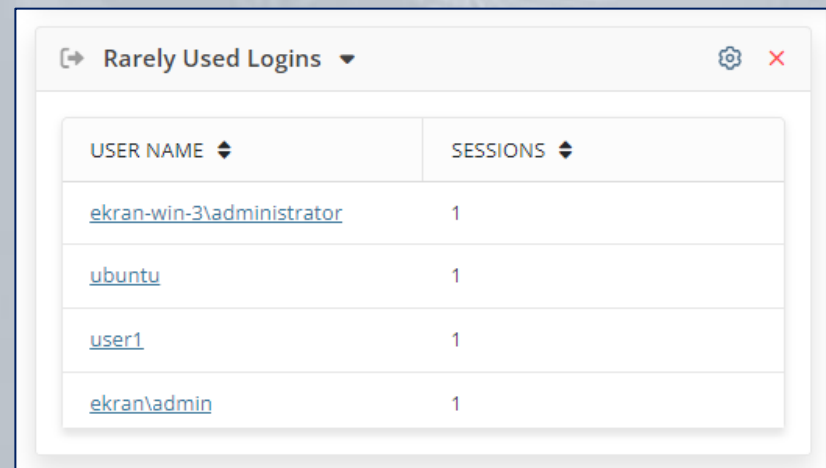
Rarely Used Logins



A screenshot of a dashboard titled "Rarely Used Computers". It displays a table with two columns: "CLIENT NAME" and "SESSIONS".

CLIENT NAME	SESSIONS
dp-ekran-share	1
RHEL7.6-hal	1
ubuntu-20	1

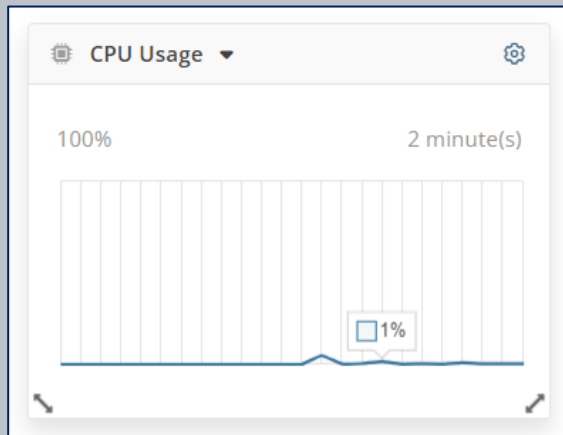
Rarely Used Computers



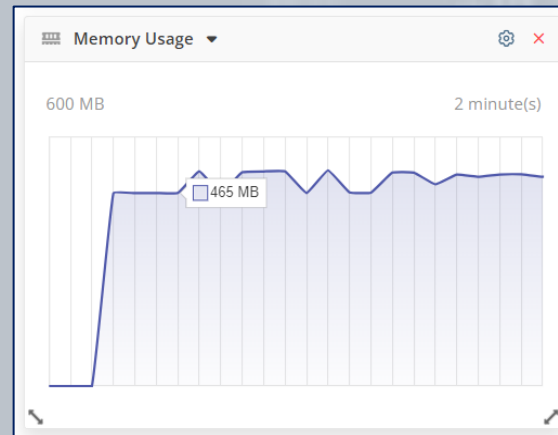
A screenshot of a dashboard titled "Rarely Used Logins". It displays a table with two columns: "USER NAME" and "SESSIONS".

USER NAME	SESSIONS
ekran-win-3\administrator	1
ubuntu	1
user1	1
ekran\admin	1

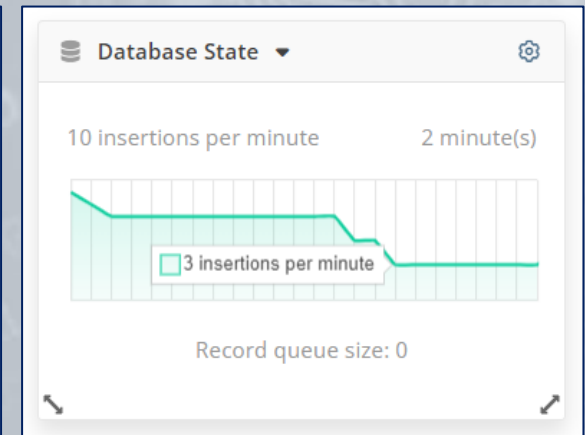
CPU Usage



Memory Usage



Database State

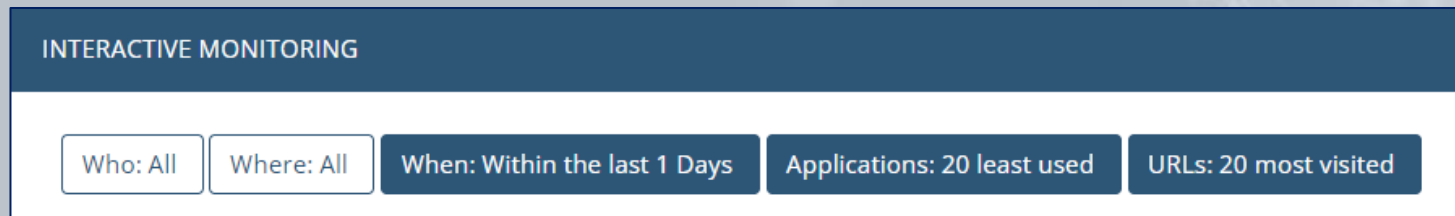


Interactive Monitoring

You can **filter** data by three parameters:

- **Who:** filter by any specific user logged in to a Client computer.
- **Where:** filter by a specific Client computer.
- **When:** filter by a specific time period.

Additionally, you can **modify the order of the bars** displayed, by using the Applications and URLs **filters**.



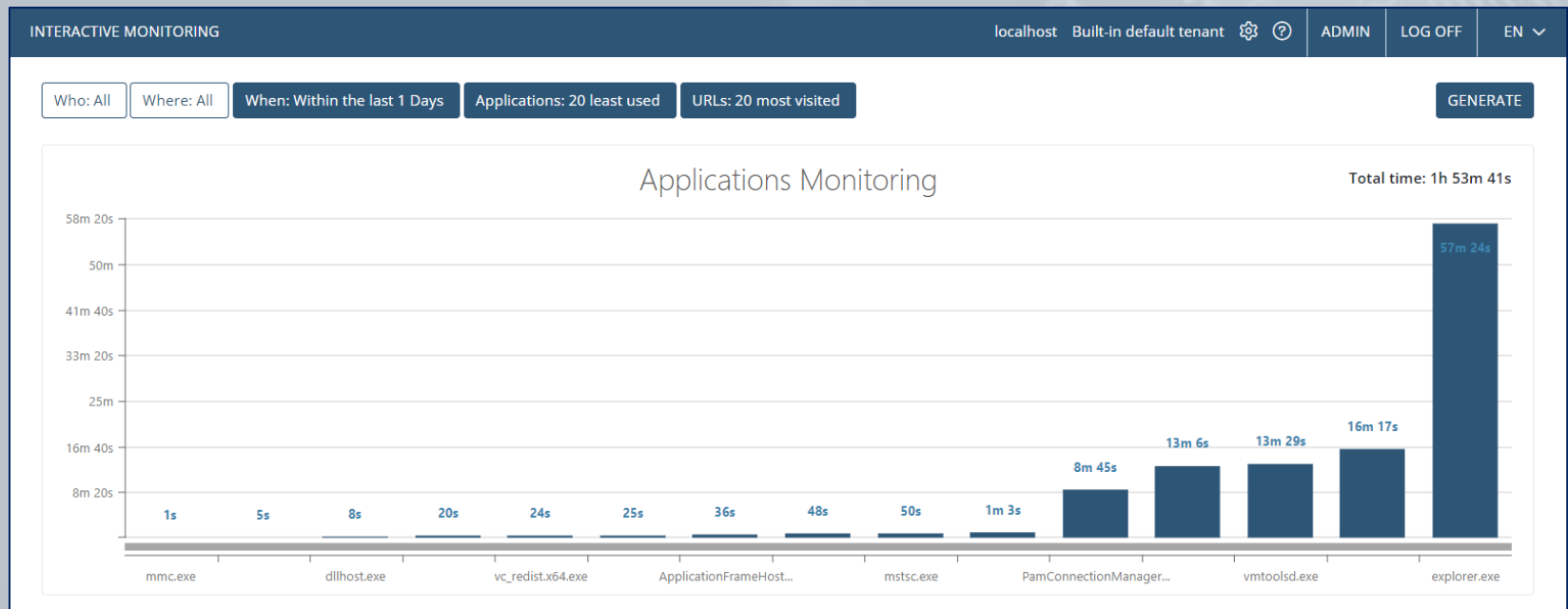
Data is displayed in the form of two column charts (the **Application Monitoring** chart and the **URL Monitoring** chart).

To **view** the list of application/website entries, click on the column with the application/website name.

The Application Monitoring Chart

This chart provides information on the **time spent** by users using different **applications**.

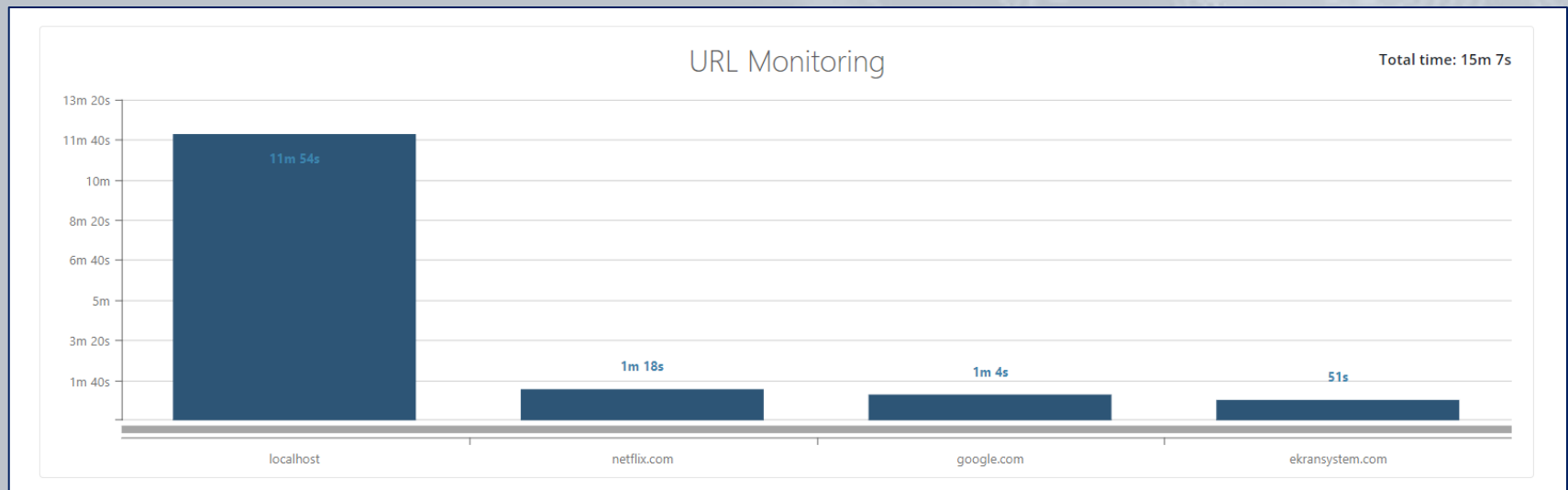
You can also use this chart to analyze information on the **most and least used** applications, and detect any threats and suspicious activity on the computers being investigated.



The URL Monitoring Chart

This chart provides information on the **time spent** by users visiting different **websites**.

You can also use this chart to analyze information on the **most and least visited** websites, and detect potentially harmful activity on the computers being investigated.



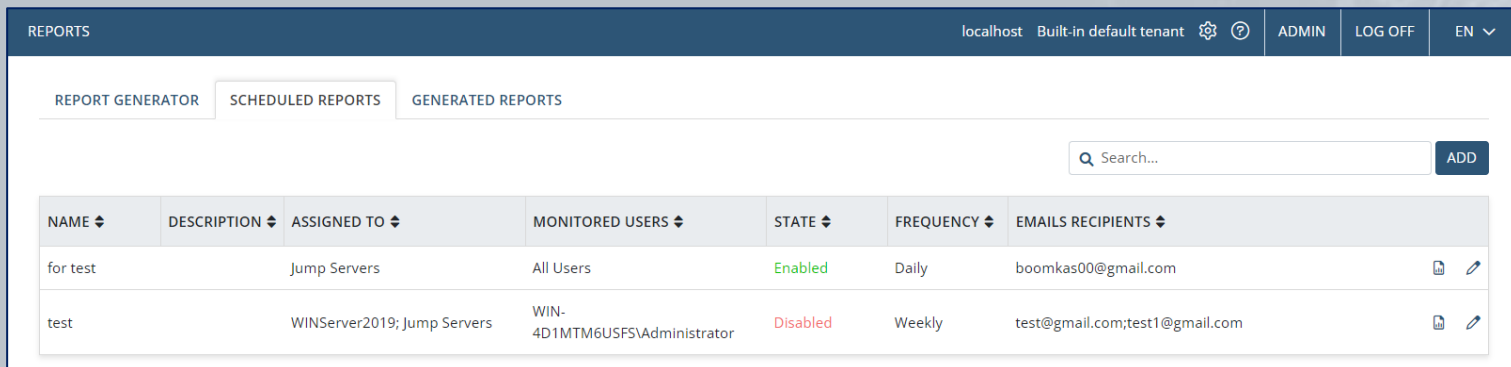
Reports

Ekran System reports provide a full **overview** of **time spent** using **applications**, and on **websites** visited, on the user's computer.

You can generate a highly **customizable** report either **ad-hoc**, or you can **schedule** the sending of reports to your email on a daily, weekly, or monthly basis.

The reported activity can include **alerts**, **applications** launched, **websites** visited, **USB devices** plugged-in/blocked, and **Linux commands** executed, etc.

Scheduled Reports



The screenshot shows the 'REPORTS' section of the Ekran System interface. It features a navigation bar with 'REPORT GENERATOR', 'SCHEDULED REPORTS', and 'GENERATED REPORTS'. Below this is a search bar and an 'ADD' button. A table lists scheduled reports with columns for Name, Description, Assigned To, Monitored Users, State, Frequency, and Emails Recipients.

NAME	DESCRIPTION	ASSIGNED TO	MONITORED USERS	STATE	FREQUENCY	EMAILS RECIPIENTS
for test		Jump Servers	All Users	Enabled	Daily	boomkas00@gmail.com
test		WINServer2019; Jump Servers	WIN-4D1MTM6USFS\Administrator	Disabled	Weekly	test@gmail.com;test1@gmail.com

Reports can be generated **manually at any time** for **any time period**.

Manual Report Generation

REPORTS

REPORT GENERATOR | SCHEDULED REPORTS | GENERATED REPORTS

Report Type

Alert Grid Report PDF

- Activity Chart Report
- Activity Pie Chart Report
- Activity Summary Grid Report
- Alert Grid Report
- Clipboard Grid Report
- Detailed Activity Grid Report
- File Monitoring Grid Report
- Kernel-Level USB Grid Report
- Keystroke Grid Report
- Linux/XWindow Grid Report
- Overtime Work Grid Report
- Session Grid Report
- Sessions Outside of Work Hours Grid Report
- Terminal Server Grid Report
- URL Chart Report
- URL Pie Chart Report
- URL Summary Grid Report
- USB Storage Grid Report
- User Behavior Analytics Grid Report
- User Daily Activity Grid Report

Hours

7/11/2023

+ Add

GENERATE REPORT

REPORTS

Date Filters

Within the last 1 Hours

Between 7/10/2023 and 7/11/2023

Clients + Add

CLIENT NAME	DESCRIPTION	REMOVE ALL
nick-node-2		⊗
WIN10		⊗
Terminal		⊗

Client Groups + Add

CLIENT GROUP NAME	DESCRIPTION	REMOVE ALL
All Clients	This group contains all ...	⊗

Users Any

Who can download Any

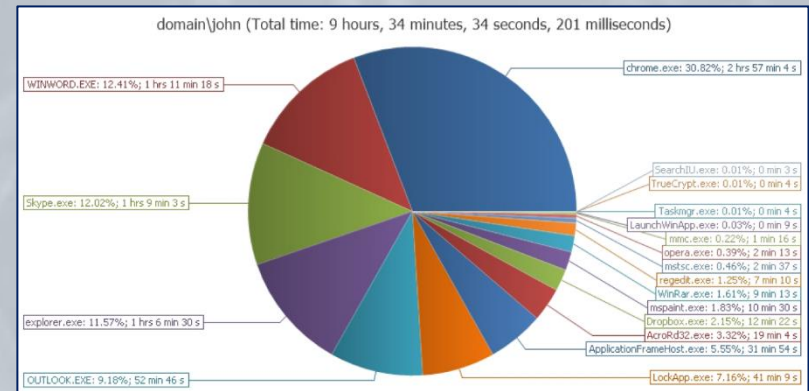
GENERATE REPORT

Activity Summary Grid Report

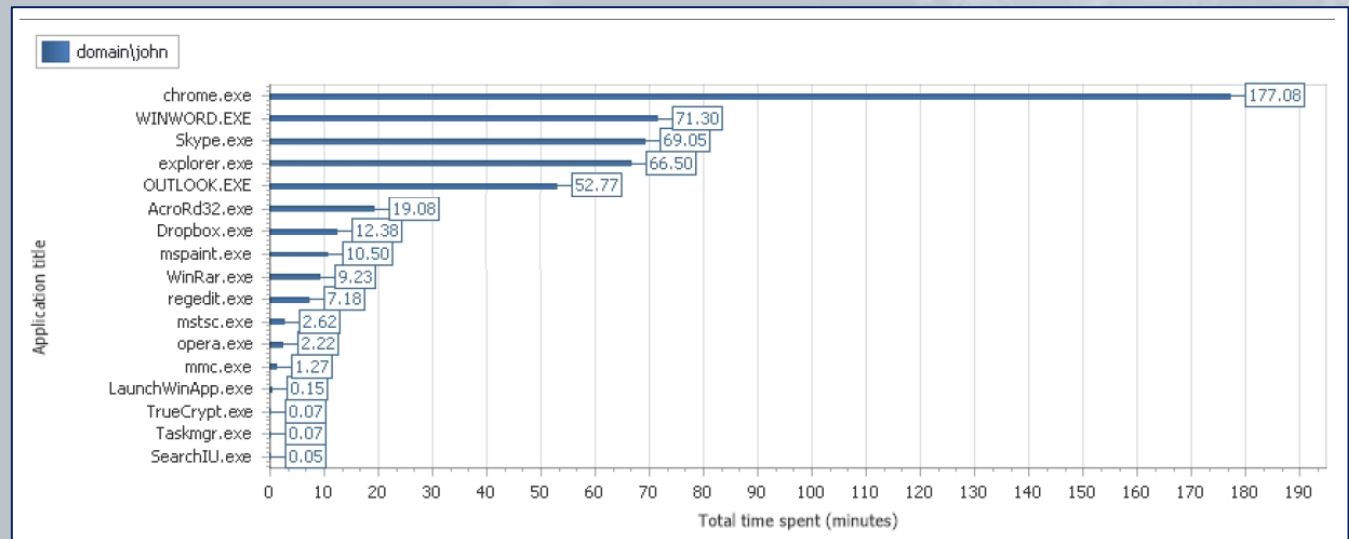
Client name	johnsmith-pc	
Client description	Security AS group	
User name	domain\john	
Total time	6 hours, 42 minutes, 5 seconds	
Active time	6 hours, 20 minutes	

Application name	%	Time spent
chrome.exe	39.35	2 hours, 38 minutes, 14 seconds
WINWORD.EXE	31.24	2 hours, 5 minutes, 36 seconds
Skype.exe	9.39	37 minutes, 45 seconds

Activity Pie Chart Report



Activity Chart Report



User Statistics Report

User name	Total time spent	Session count	Computers	Remote IPs	Remote Public IPs
COMP18\JasonZena	36m 58s	1	Comp18	None	None
COMP16\BonnieRoss	8m 40s	1	Comp16	None	None
COMP33\Ralph.Watson	8m 12s	1	Comp33	None	None
ALICE-PC\Alice	2m 4s	1	alice-pc	None	None
JULIET-PC\Julia	1m 11s	1	juliet-pc	None	None
COMP13\KylieKey	4m 28s	1	Comp13	10.000.0.00	10.000.0.00
COMP19\NickolasSherry	3m 58s	1	Comp19	10.000.0.00	10.000.0.00
COMP6\TomNessJunior	3m 47s	1	Comp6	None	None

Clipboard Grid Report

Client name	johnsmith-pc				
Client description	Security AS group				
User name	domain\john				
Activity time	Activity title	Application name	Clipboard Operation	Clipboard Text	
08/26/2018 03:32:55 PM	Daily report 26/08/2022 - Message (HTML)	OUTLOOK.EXE	Copy	I had a status meeting with the members of the Manual project	
08/26/2018 03:32:56 PM	Daily report 26/08/2022 - Message (HTML)	OUTLOOK.EXE	Paste	I had a status meeting with the members of the Manual project	
08/26/2018 05:48:55 PM	Skype [2] - johnsmith	Skype.exe	Copy	Miscellaneous	
08/26/2018 06:32:30 PM	Metronic - The Most Popular Bootstrap 4 HTML, Angular, VueJS, React & Laravel Admin Dashboard Theme Keenthemes	chrome.exe	Copy	https://keenthemes.com/metronic/?page=metronic7	

Session Grid Report

Client name	EnterpServ							
Client description	Ekran Server, Management Tool and agent							
Total time	3m 13s							
User name	Total time	Active time	Session start	Last activity	Remote IP	Remote Public IP	Session URL	Comment
DEMO\Administrator	29s	29s	03/04/2020 12:44:29 PM	03/04/2020 12:44:58 PM	None	None	Open Session	None
DEMO\Alan.Simerson	19s	19s	03/04/2020 12:52:09 PM	03/04/2020 12:52:28 PM	None	None	Open Session	None

Sessions Outside of Work Hours Grid Report

Client name	alice-pc						
Client description	Loading Sensitive Data to a Flash Drive						
Total out of work hours	2m 4s						
User name	Total time spent	Active out of work hours	Session start time	Last activity time	Remote IP	Remote Public IP	Session URL
ALICE-PC\Alice	2m 20s	2m 4s	07/12/2018 06:01:48 PM	07/12/2018 06:04:08 PM	None	None	Open Session

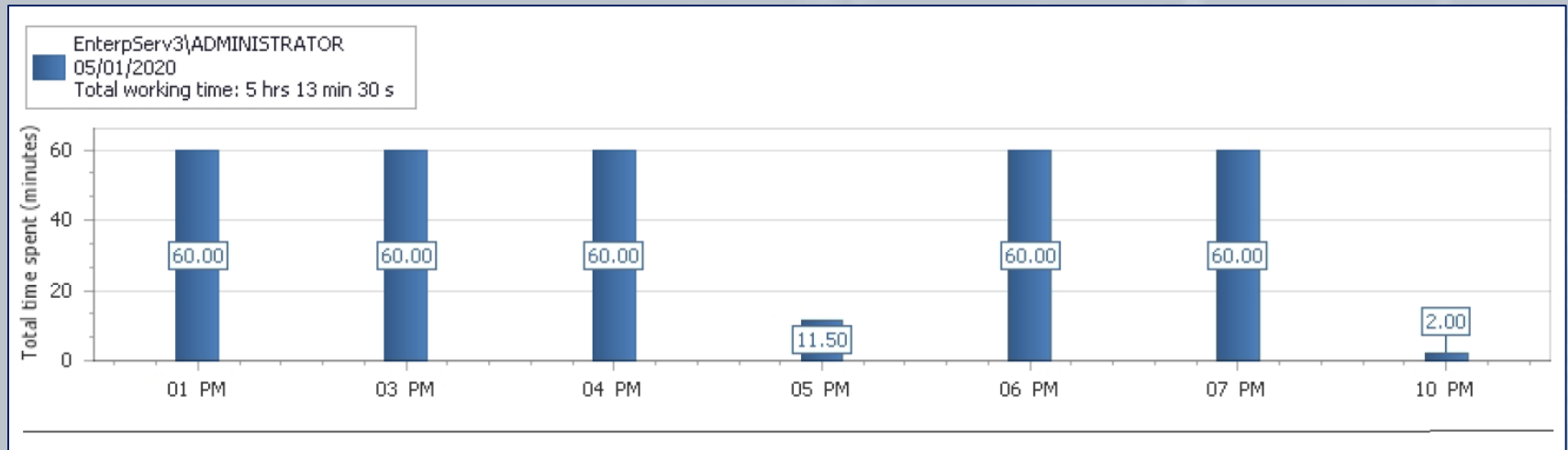
Detailed Activity Grid Report

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 08:53:01 AM	My Drive - Google Drive - Google Chrome	chrome.exe	https://drive.google.com/drive/my-drive?ogsrc=32		
07/10/2018 08:53:01 AM	My Drive - Google Drive - Google Chrome	chrome.exe	https://drive.google.com/drive/my-drive?ogsrc=32		
07/10/2018 08:53:01 AM	My Drive - Google Drive - Google Chrome	chrome.exe	https://drive.google.com/drive/my-drive?ogsrc=32	[Clipboard (Paste)]: https://drive.google.com/file/d/19TprsVorHH8GodL0xnHmO8HKh7ww/view?usp=har...	
07/10/2018 08:53:08 AM	My Drive - Google Drive - Google Chrome	chrome.exe	https://mail.google.com/mail/u/0/#inbox		
07/10/2018 08:53:08 AM	Inbox (6) - helenapeterson.hr@gmail.com - Gmail - Google Chrome	chrome.exe	https://mail.google.com/mail/u/0/#inbox		

User Daily Activity Grid Report

Client name	EnterpServ					
Client description	Ekran Server, Management Tool and agent					
Total time	8m 40s					
User name	Active time	First Activity Time	Last Activity Time	Remote IP	Remote Public IP	Session URL
DEMO\Administrator	26s	03/04/2020 12:44:32 PM	03/04/2020 12:44:58 PM	None	None	Open Session
DEMO\Alan.Simpson	5m 53s	03/04/2020 12:46:34 PM	03/04/2020 12:52:28 PM	None	None	Open Session

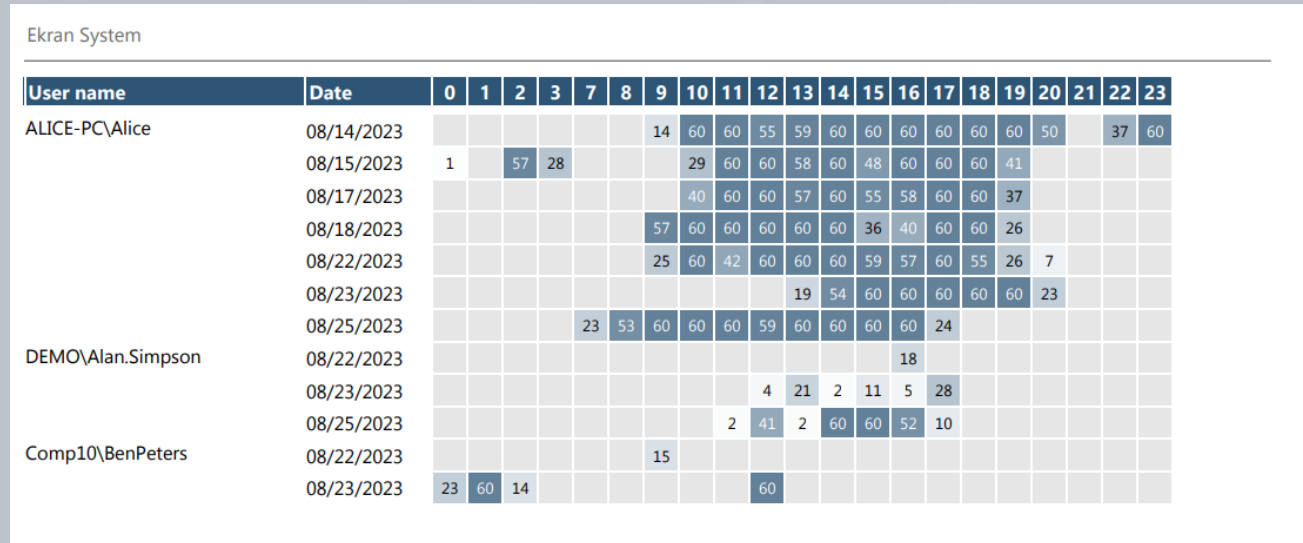
User Productivity Chart Report



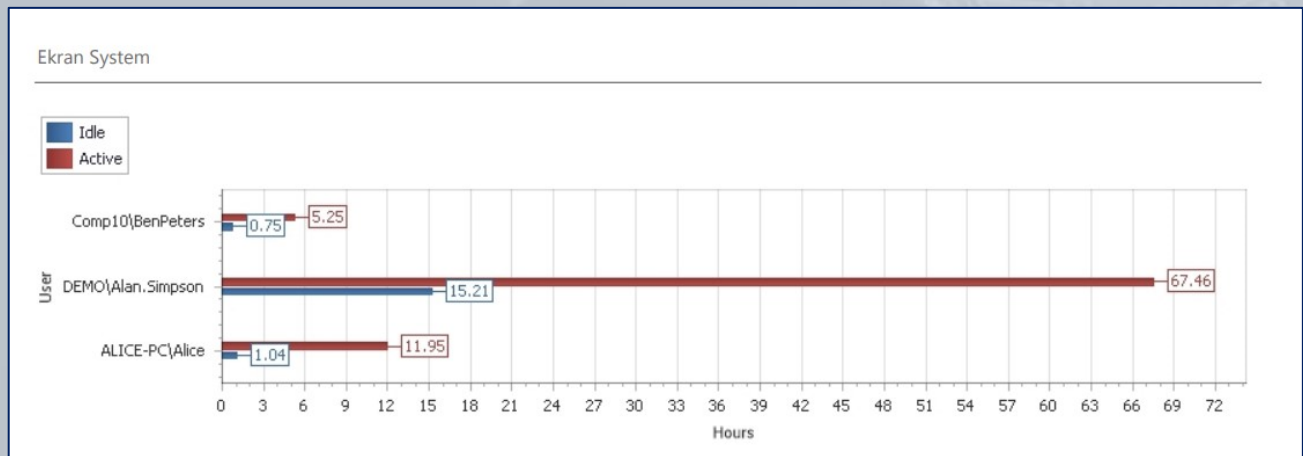
User Productivity Summary Grid Report

User Name	Date	Total Time Spent	Active Time	First Activity Time	Last Activity Time	Idle Time	Top 10 Applications	Top 10 URLs
COMP8\RobertO akley	07/06/2018	4m	4m	04:37:50 PM	04:42:37 PM	-	chrome.exe 3m EXCEL.EXE 1m explorer.exe 34s	bustle.com 5m mail.google.com 1m personalcreate.com 22s

User Productivity Heatmap Report



User Active Time and Idle Time Chart Report



Alert Grid Report

Client name	johnsmith-pc		
Client description	Security AS group		
User name	domain\john		
Activity time	Alert name	Alert risk	Details
08/26/2018 03:32:55 PM	[Default] Command prompt	High	cmd.exe - Command Prompt - cmd-->cmd
08/26/2018 04:00:48 PM	Torrents	Critical	chrome.exe - Person.of.Interest - FREE Torrent Download - ExtraTorrent.cc The World's Largest BitTorrent System
08/26/2018 05:48:55 PM	TeamViewer	Normal	TeamViewer.exe - TeamViewer -
08/26/2018 06:10:32 PM	Media content	High	wmplayer.exe - Windows Media Player -
08/26/2018 06:32:11 PM	[Default] Online email services	Critical	chrome.exe - Gmail - Google Chrome - mail.google.com

User Behavior Analytics Report

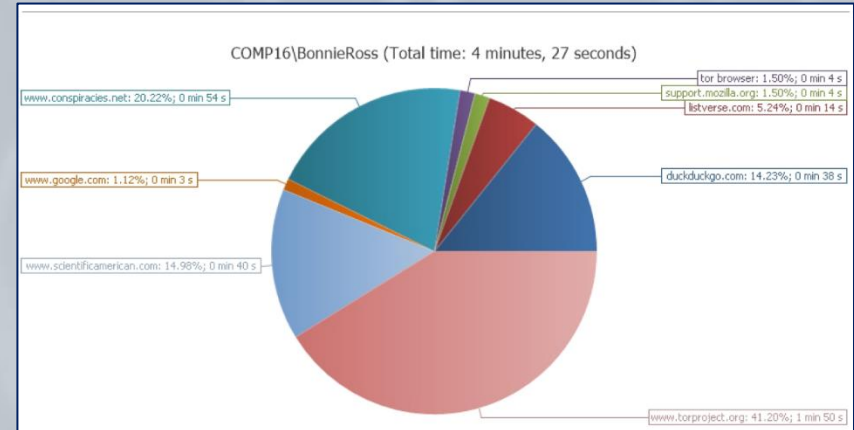
Who	Where	When	Details	Session Score	Session URL						
<table border="1"> <tr> <td>Risk Level</td> <td>Normal</td> </tr> <tr> <td>Risk Score, %</td> <td>50 - 1</td> </tr> <tr> <td>Session number</td> <td>3</td> </tr> </table>						Risk Level	Normal	Risk Score, %	50 - 1	Session number	3
Risk Level	Normal										
Risk Score, %	50 - 1										
Session number	3										
ALICE-PC\Alice	alice-pc	07/12/2018 06:01:48 PM - 07/12/2018 06:04:08 PM	WorkingHours: normal	9%	Open Session						
COMP11\SusieWade	Comp11	07/10/2018 11:08:30 AM - 07/10/2018 11:11:01 AM	WorkingHours: normal	30%	Open Session						
COMP13\KylieKey	Comp13	07/09/2018 08:54:42 AM - 07/09/2018 08:59:23 AM	WorkingHours: abnormal session start abnormal session end	39%	Open Session						

URL Summary Grid Report

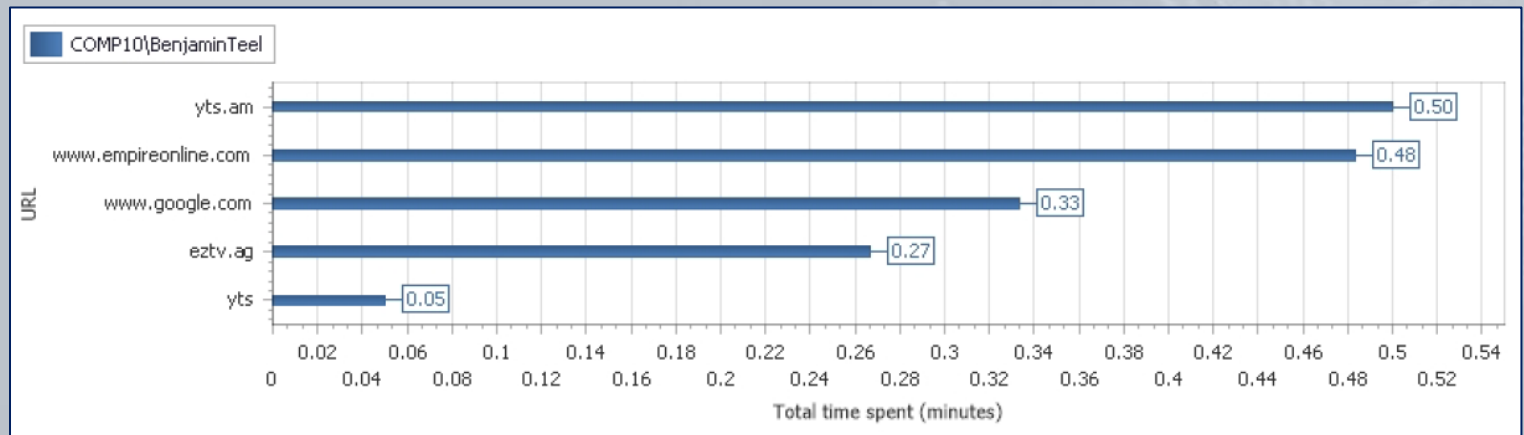
Client name	Comp15
Client description	Exporting HR Data
User name	COMP15\HelenPeterson
Total time	4 minutes, 33 seconds

URL	%	Time spent
https://drive.google.com/drive/my-drive?ogsrc=32	17.22	47 seconds
www.shakespearesglobe.com/whats-on-2018/Hamlet#QAHamlet	12.09	33 seconds
https://secure.zenefits.com/accounts/login/	10.99	30 seconds
https://secure.zenefits.com/dashboard/#/employeebulk/download	10.99	30 seconds
https://basket.shakespearesglobe.com/events/hamlet?startDate=2018-04-25&endDate=2018-08-26&k=globe+theatre	9.16	25 seconds
https://secure.zenefits.com/dashboard/	8.42	23 seconds
https://mail.google.com/mail/u/0/#inbox	7.69	21 seconds

URL Pie Chart Report



URL Chart Report



USB Storage Grid Report

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

Kernel-Level USB Grid Report

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

Terminal Server Grid Report

Date		05/23/2019		
Client name	Number of users	User name	Number of connections	Total time
Enterpserv1	1	Peter Wanderberg	1	4h 15m 25s

Date		05/24/2019		
Client name	Number of users	User name	Number of connections	Total time
Enterpserv2	4	Barbara Burbelo	2	10m 38s
		Emilia Anderson	1	1m 2s
		John Braun	3	1h 23m 8s
		Administrator	5	2h 45m 15s

In the Linux/XWindow Grid Report, you can view all `exec*` and `sudo` commands executed on Linux Client computers.

Linux/XWindow Grid Report

Client name	ubuntu2		
Client description	Adding New Users		
User name	master		
Activity time	Command	Function	Parameters
07/17/2018 11:59:33 AM	grep	execve	-q sshd
07/17/2018 11:59:33 AM	/bin/bash	execve	
07/17/2018 11:59:58 AM	sudo	execve	chmod +x Server-Health.sh
07/17/2018 12:00:10 PM	./server-Health.sh	execve	
07/17/2018 12:00:24 PM	head	execve	-3
07/17/2018 12:00:24 PM	awk	execve	{print "Free/total disk: " \$11 " / " \$9}
07/17/2018 12:00:24 PM	awk	execve	{print "Free/total memory: " \$17 " / " \$8 " MB"}
07/17/2018 12:00:24 PM	ss	execve	-s
07/17/2018 12:00:24 PM	ps	execve	auxf --width 200

The Audit Session Grid Report is a special reports showing which Management Tool users have viewed which sessions.

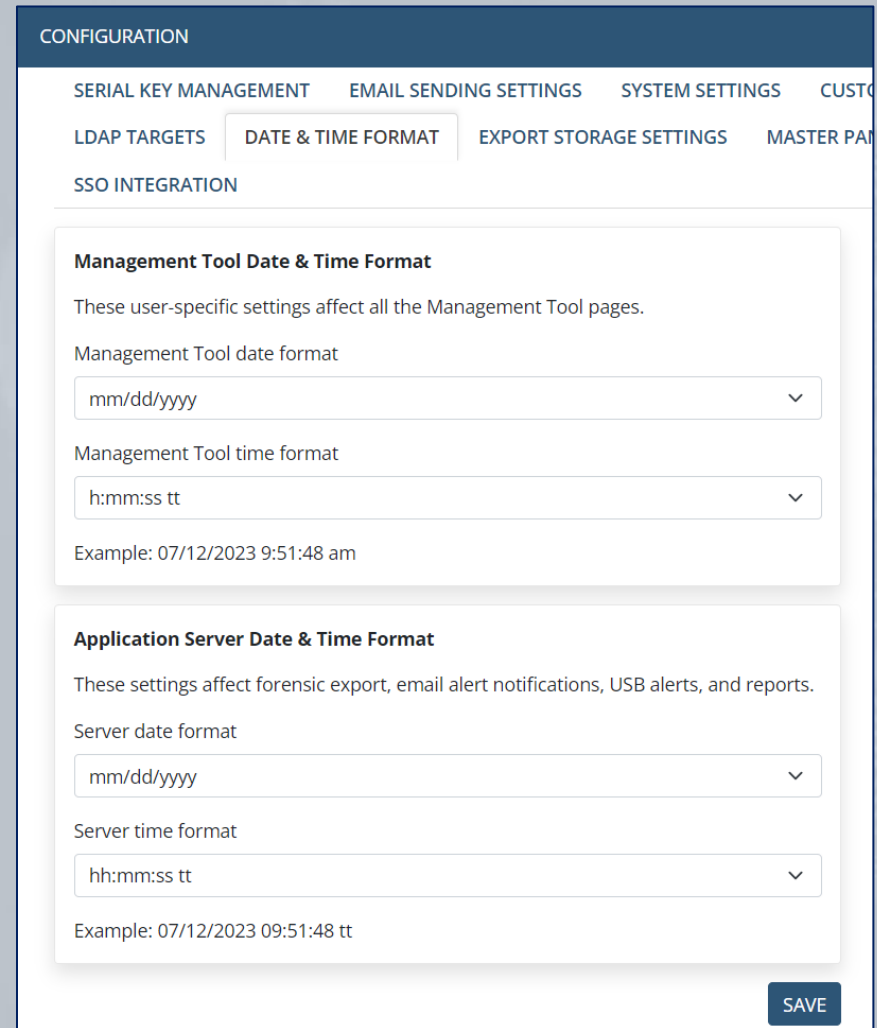
Audit Session Grid Report

Date and time	Viewer user name/Group	Action	Who	Where	Session time
04/27/2023 03:32:47 PM	admin/Administrators	Viewed session	ubuntu	Ubuntu-20.04	04/27/2023 03:18:33 PM - 04/27/2023 03:18:47 PM
04/27/2023 03:40:49 PM	admin/Administrators	Viewed session	root	Ubuntu-20.04	04/27/2023 03:18:33 PM - 04/27/2023 03:18:47 PM
04/27/2023 03:41:01 PM	admin/Administrators	Viewed session	tester	macos-11-vm1	04/27/2023 03:18:54 PM - 04/27/2023 03:19:00 PM

System Customization

Setting the Date & Time Format

Date & time format configuration allows you to **define** the **date and time format** for the Management Tool and the Application Server.



The screenshot shows the 'CONFIGURATION' page with the 'DATE & TIME FORMAT' tab selected. It contains two main sections: 'Management Tool Date & Time Format' and 'Application Server Date & Time Format'. Each section includes a description, a 'Server date format' dropdown menu, a 'Server time format' dropdown menu, and an example of the resulting format. A 'SAVE' button is located at the bottom right of the configuration area.

CONFIGURATION

SERIAL KEY MANAGEMENT EMAIL SENDING SETTINGS SYSTEM SETTINGS CUSTOMIZATION

LDAP TARGETS **DATE & TIME FORMAT** EXPORT STORAGE SETTINGS MASTER PAGE

SSO INTEGRATION

Management Tool Date & Time Format

These user-specific settings affect all the Management Tool pages.

Management Tool date format

mm/dd/yyyy

Management Tool time format

h:mm:ss tt

Example: 07/12/2023 9:51:48 am

Application Server Date & Time Format

These settings affect forensic export, email alert notifications, USB alerts, and reports.

Server date format

mm/dd/yyyy

Server time format

hh:mm:ss tt

Example: 07/12/2023 09:51:48 tt

SAVE

Custom logo settings allow you to use of any **custom graphics file** instead of the default logo on Client **notifications** during **secondary user authentication, user blocking, etc.**



Customizing Reports

Custom Reports settings allow you to use any **custom graphics file** instead of the default logo **in reports**. You can also add **header and footer text** to the reports.



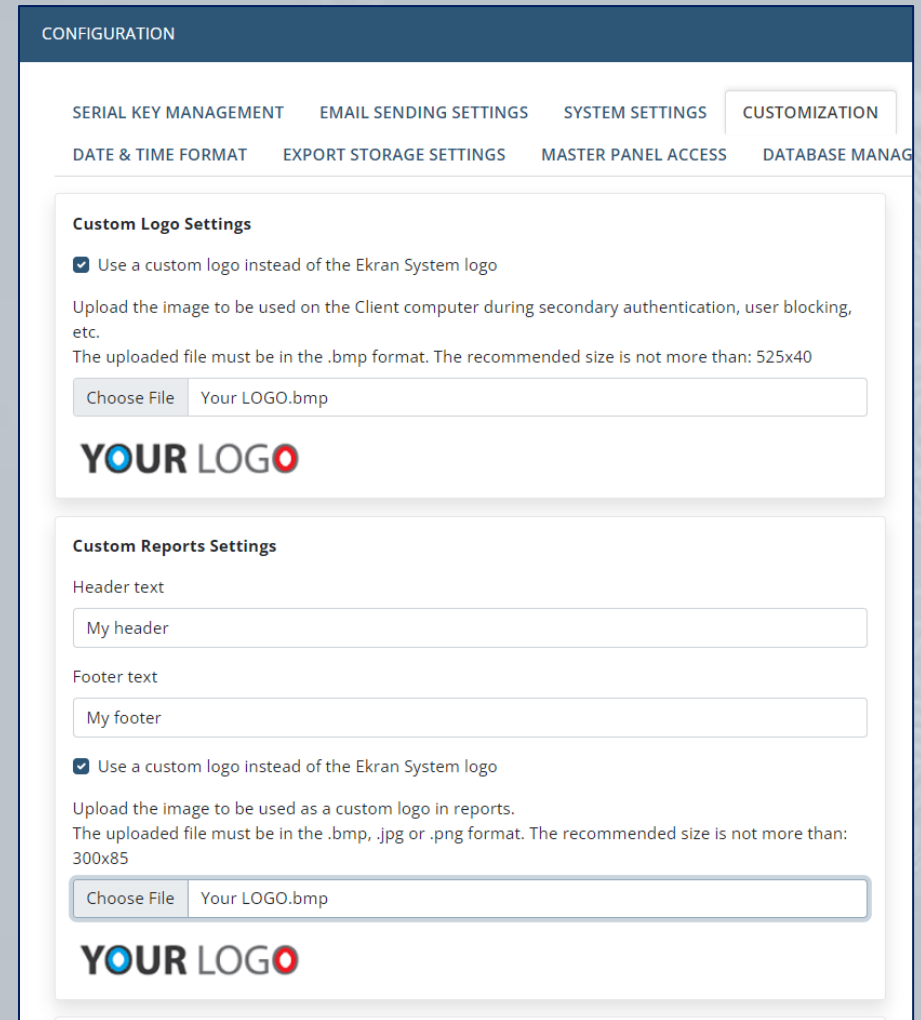
YOUR LOGO Activity Pie Chart Report

Details

Generated in	Ekran System
Server	WEB-DEMO
User	

Filter

Start date	08/11/2003 12:00:00 AM
End date	10/10/2022 11:59:59 PM
Client groups	No
Clients	johnsmith-pc
Users	All Users



CONFIGURATION

SERIAL KEY MANAGEMENT EMAIL SENDING SETTINGS SYSTEM SETTINGS CUSTOMIZATION

DATE & TIME FORMAT EXPORT STORAGE SETTINGS MASTER PANEL ACCESS DATABASE MANAG

Custom Logo Settings

Use a custom logo instead of the Ekran System logo

Upload the image to be used on the Client computer during secondary authentication, user blocking, etc.
The uploaded file must be in the .bmp format. The recommended size is not more than: 525x40

Choose File Your LOGO.bmp

YOUR LOGO

Custom Reports Settings

Header text

My header

Footer text

My footer

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 format. The recommended size is not more than: 300x85

Choose File Your LOGO.bmp

YOUR LOGO

Customizing Email Subjects and Messages

Custom settings allow you to **specify** the **subjects** to be used in **email notifications**, and other various messages, sent by Ekran System.

CONFIGURATION

Upload the image to be used as a custom logo in reports.
The uploaded file must be in the .bmp, .jpg or .png format. The recommended size is not more than: 300x85

Choose File Your LOGO.bmp

YOUR LOGO

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 - the 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

Custom Login Message for Blocked Users

You have been blocked. Contact your system administrator.

Two-Factor Authentication

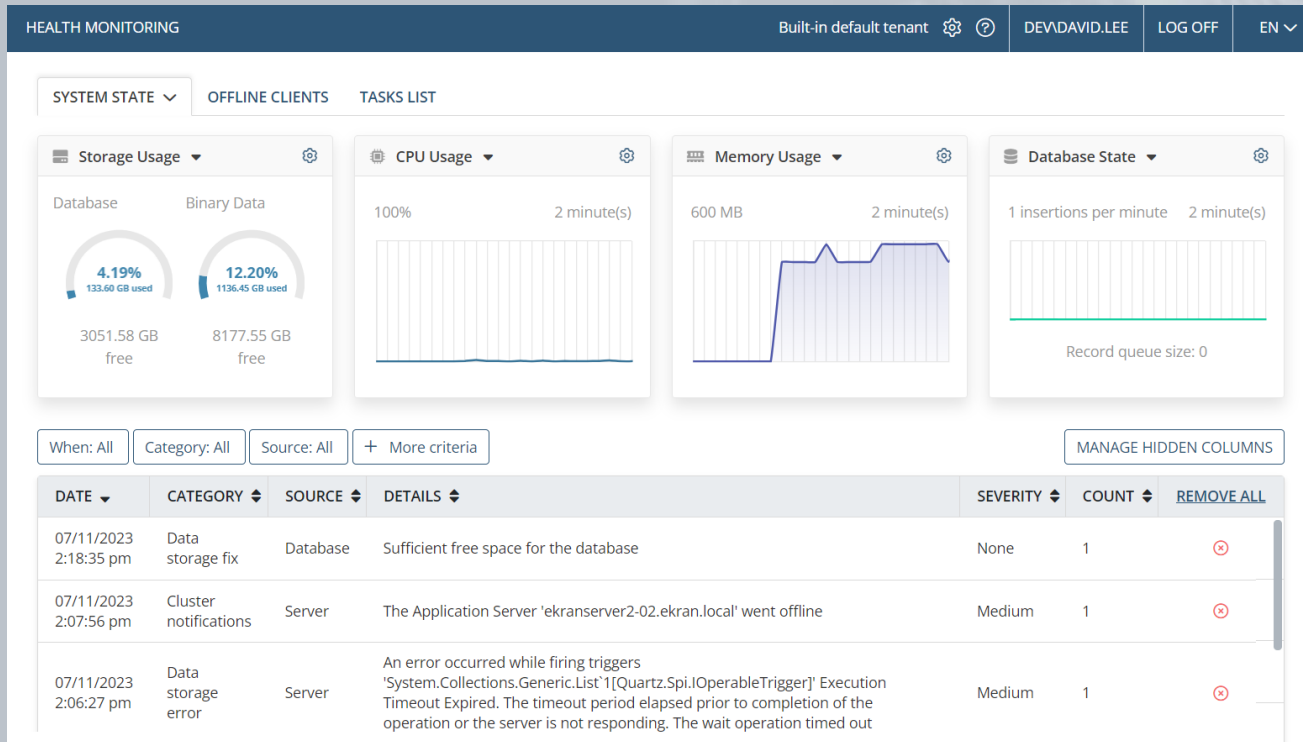
Main Screen

Two-factor authentication is enabled on your workstation. Open your authenticator app (Google ut

SAVE

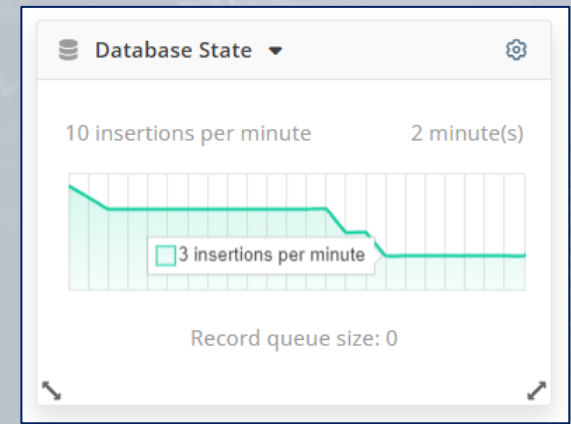
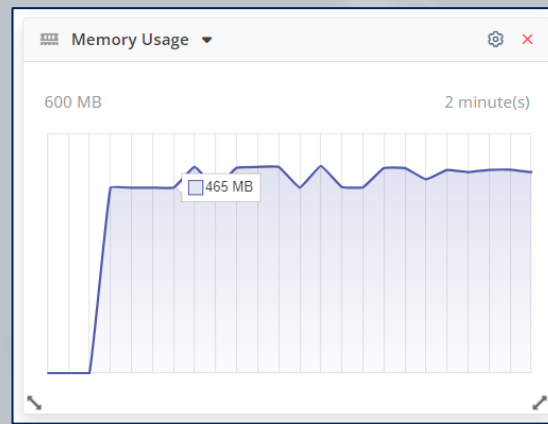
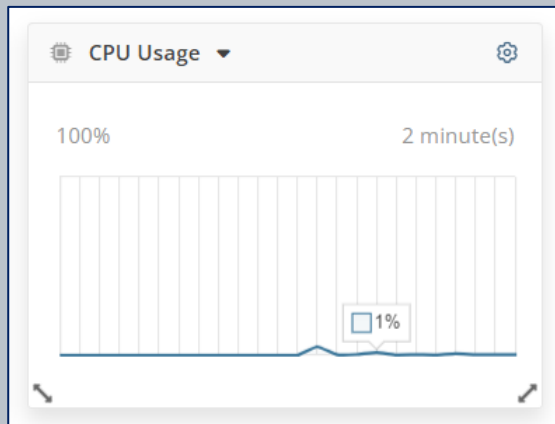
Health Monitoring

System Health Monitoring allows you to get detailed information about e.g. **database storage usage** and any system **errors** and **warnings** to assist you in monitoring the system “health” and **reacting** to any issues in a **timely** manner.

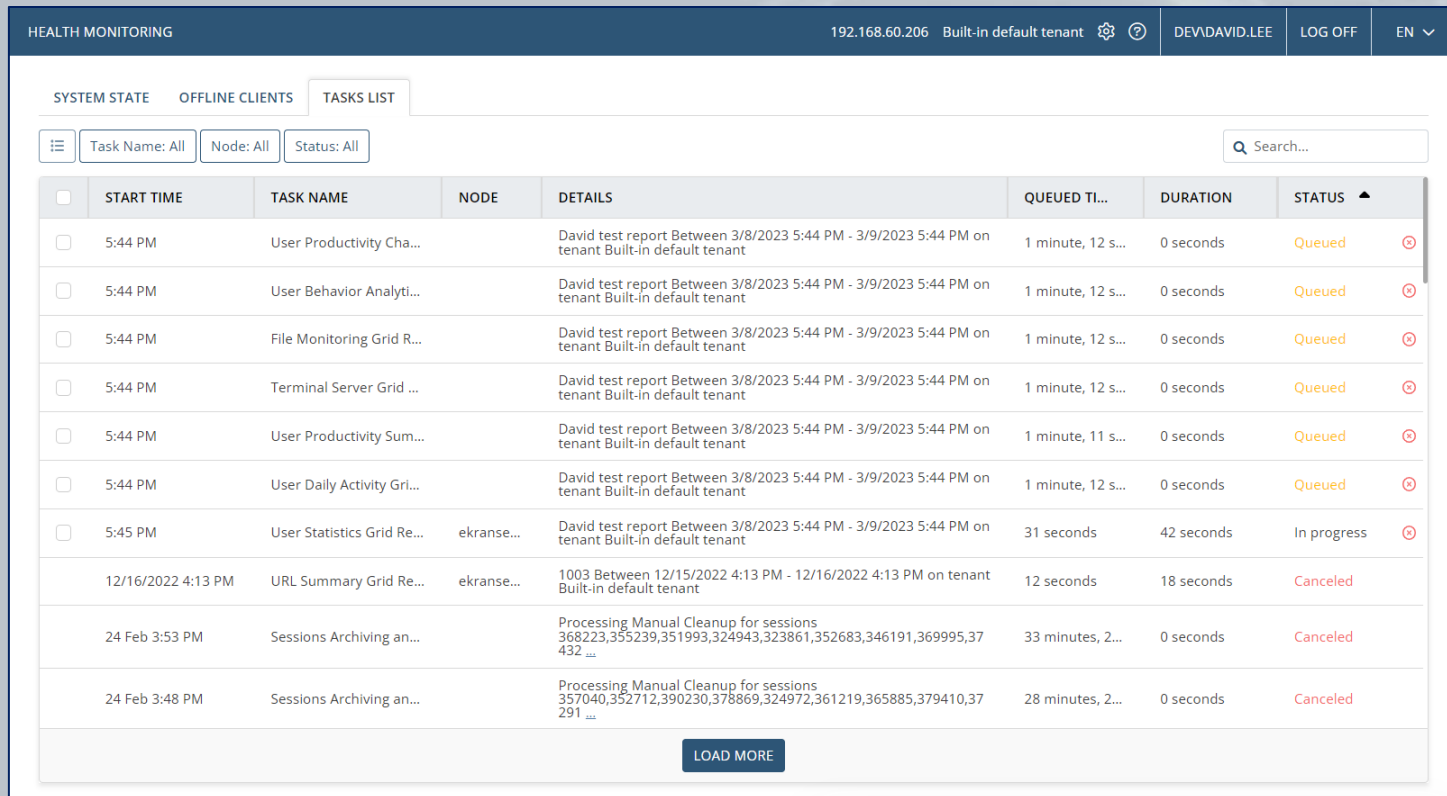


Resource monitoring allows you to view the **current resource usage** by the Ekran System Application Server process:

- **CPU Usage** by the Application Server process
- **Memory Usage** by the Application Server process
- The **Database State**



The **Tasks List** tab (on the **Health Monitoring** page) allows information about various **tasks which may take significant time to process** to be viewed (and canceled).



The screenshot shows the 'HEALTH MONITORING' interface with the 'TASKS LIST' tab selected. The top navigation bar includes the IP address '192.168.60.206', the tenant name 'Built-in default tenant', and user information 'DEVDAVID.LEE'. Below the navigation bar, there are tabs for 'SYSTEM STATE', 'OFFLINE CLIENTS', and 'TASKS LIST'. A search bar and filter buttons for 'Task Name: All', 'Node: All', and 'Status: All' are present. The main content is a table with columns: 'START TIME', 'TASK NAME', 'NODE', 'DETAILS', 'QUEUED TI...', 'DURATION', and 'STATUS'. The table lists various tasks, including 'User Productivity Cha...', 'User Behavior Analyti...', 'File Monitoring Grid R...', 'Terminal Server Grid ...', 'User Productivity Sum...', 'User Daily Activity Gri...', 'User Statistics Grid Re...', 'URL Summary Grid Re...', and 'Sessions Archiving an...'. The status of each task is indicated by a color-coded label: 'Queued' (yellow) or 'In progress' (orange), and 'Canceled' (red). A 'LOAD MORE' button is located at the bottom of the table.

<input type="checkbox"/>	START TIME	TASK NAME	NODE	DETAILS	QUEUED TI...	DURATION	STATUS ▲
<input type="checkbox"/>	5:44 PM	User Productivity Cha...		David test report Between 3/8/2023 5:44 PM - 3/9/2023 5:44 PM on tenant Built-in default tenant	1 minute, 12 s...	0 seconds	Queued
<input type="checkbox"/>	5:44 PM	User Behavior Analyti...		David test report Between 3/8/2023 5:44 PM - 3/9/2023 5:44 PM on tenant Built-in default tenant	1 minute, 12 s...	0 seconds	Queued
<input type="checkbox"/>	5:44 PM	File Monitoring Grid R...		David test report Between 3/8/2023 5:44 PM - 3/9/2023 5:44 PM on tenant Built-in default tenant	1 minute, 12 s...	0 seconds	Queued
<input type="checkbox"/>	5:44 PM	Terminal Server Grid ...		David test report Between 3/8/2023 5:44 PM - 3/9/2023 5:44 PM on tenant Built-in default tenant	1 minute, 12 s...	0 seconds	Queued
<input type="checkbox"/>	5:44 PM	User Productivity Sum...		David test report Between 3/8/2023 5:44 PM - 3/9/2023 5:44 PM on tenant Built-in default tenant	1 minute, 11 s...	0 seconds	Queued
<input type="checkbox"/>	5:44 PM	User Daily Activity Gri...		David test report Between 3/8/2023 5:44 PM - 3/9/2023 5:44 PM on tenant Built-in default tenant	1 minute, 12 s...	0 seconds	Queued
<input type="checkbox"/>	5:45 PM	User Statistics Grid Re...	ekranse...	David test report Between 3/8/2023 5:44 PM - 3/9/2023 5:44 PM on tenant Built-in default tenant	31 seconds	42 seconds	In progress
	12/16/2022 4:13 PM	URL Summary Grid Re...	ekranse...	1003 Between 12/15/2022 4:13 PM - 12/16/2022 4:13 PM on tenant Built-in default tenant	12 seconds	18 seconds	Canceled
	24 Feb 3:53 PM	Sessions Archiving an...		Processing Manual Cleanup for sessions 368223,355239,351993,324943,323861,352683,346191,369995,37432 ...	33 minutes, 2...	0 seconds	Canceled
	24 Feb 3:48 PM	Sessions Archiving an...		Processing Manual Cleanup for sessions 357040,352712,390230,378869,324972,361219,365885,379410,37291 ...	28 minutes, 2...	0 seconds	Canceled

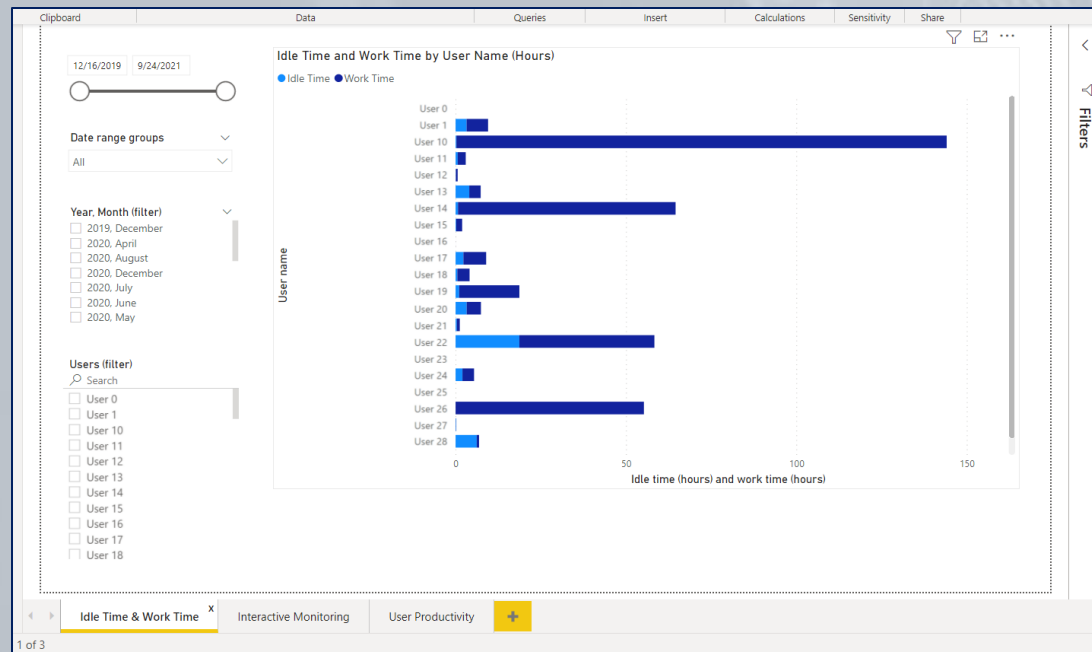
Ekran System API

(& Integration with e.g. Power BI)

Ekran System **Data Connector** is a stand-alone component of Ekran System that is used for **integrating a customer's IT system via the Ekran System API.**

This application is designed to **allow customers to get Ekran System monitoring data** via the API in order to **use for their own business purposes.**

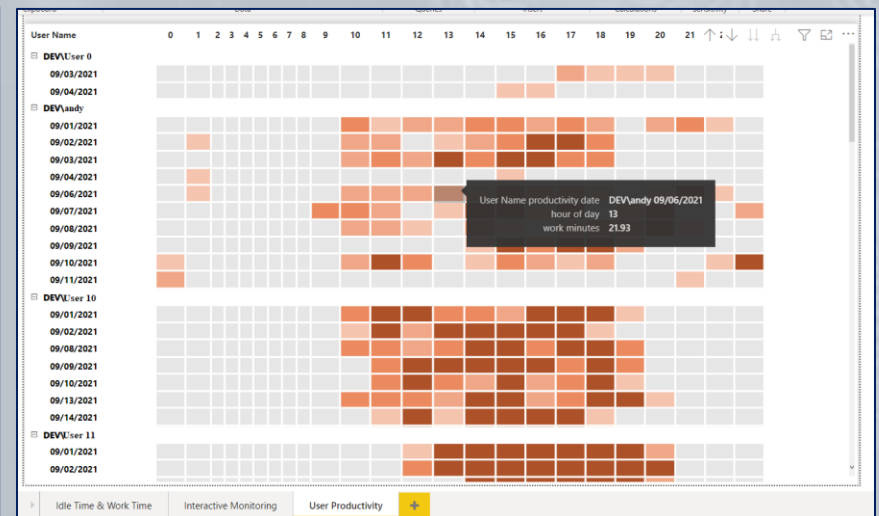
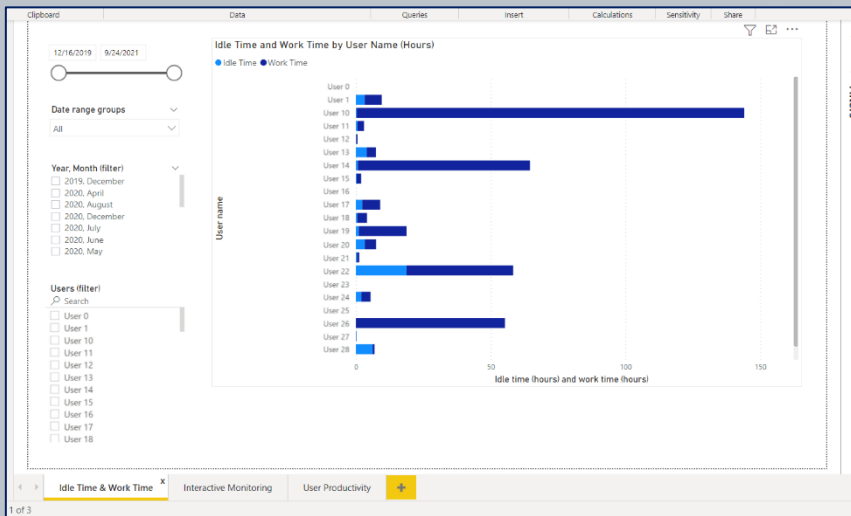
Idle Time & Work Time Report



For example, **Client session records** containing **user productivity data** (such as productivity time, idle time, duration, etc.) can be used to build BI (business intelligence) reports in **Microsoft Power BI**.

Interactive Monitoring Report

User Productivity Report





Visit us online:

www.ekransystem.com