Ekran system

Full Feature Presentation

Ekran System
Full Cycle Insider Risk Management

Contents

System Overview

About the System

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

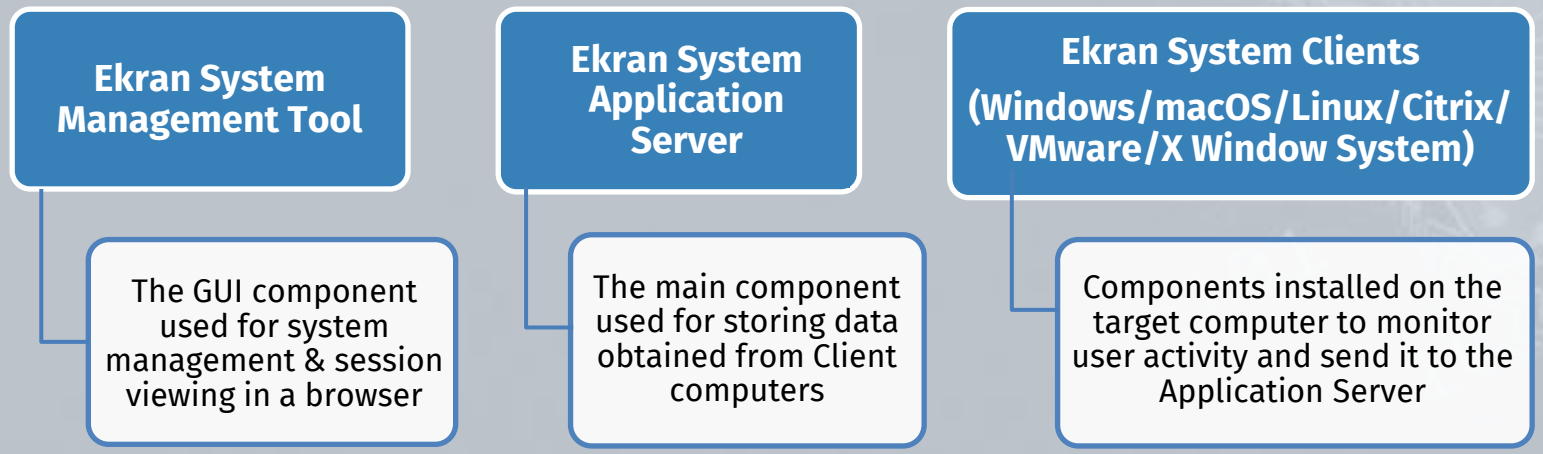
Ekran System supports the widest range of platforms and infrastructure configurations on the market, delivering reliable deployments of any size, from piloting dozens to tens of thousands of endpoints. Flexible licensing helps to fit it into your budget and address project changes.

About the System

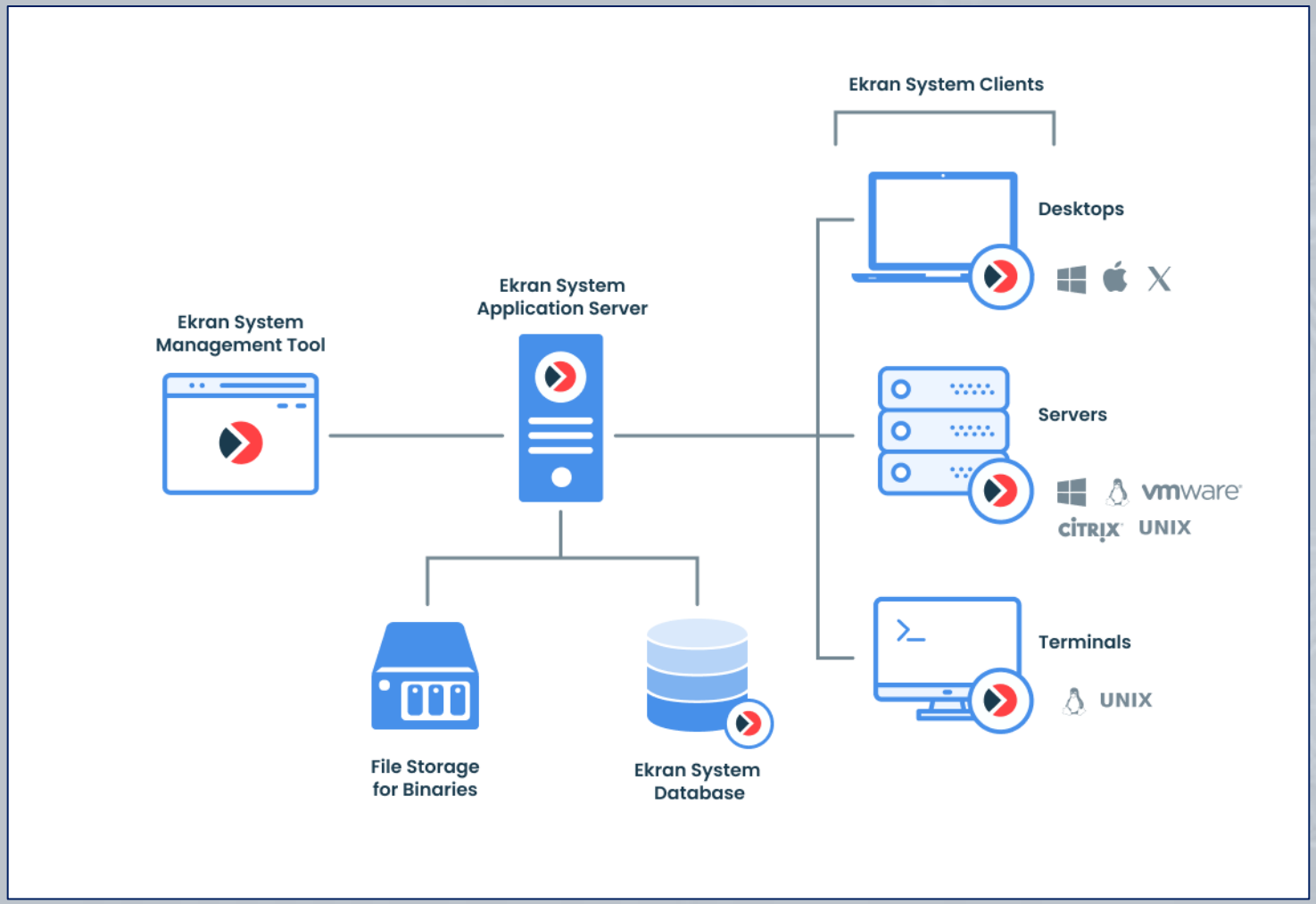
Ekran System is a full-cycle **insider risk management user activity monitoring** software solution for enhanced cybersecurity. It is used to **deter, detect** and **disrupt insider threats** to your corporate IT infrastructure, as well as to assist you in meeting **compliance requirements** (e.g. GDPR),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

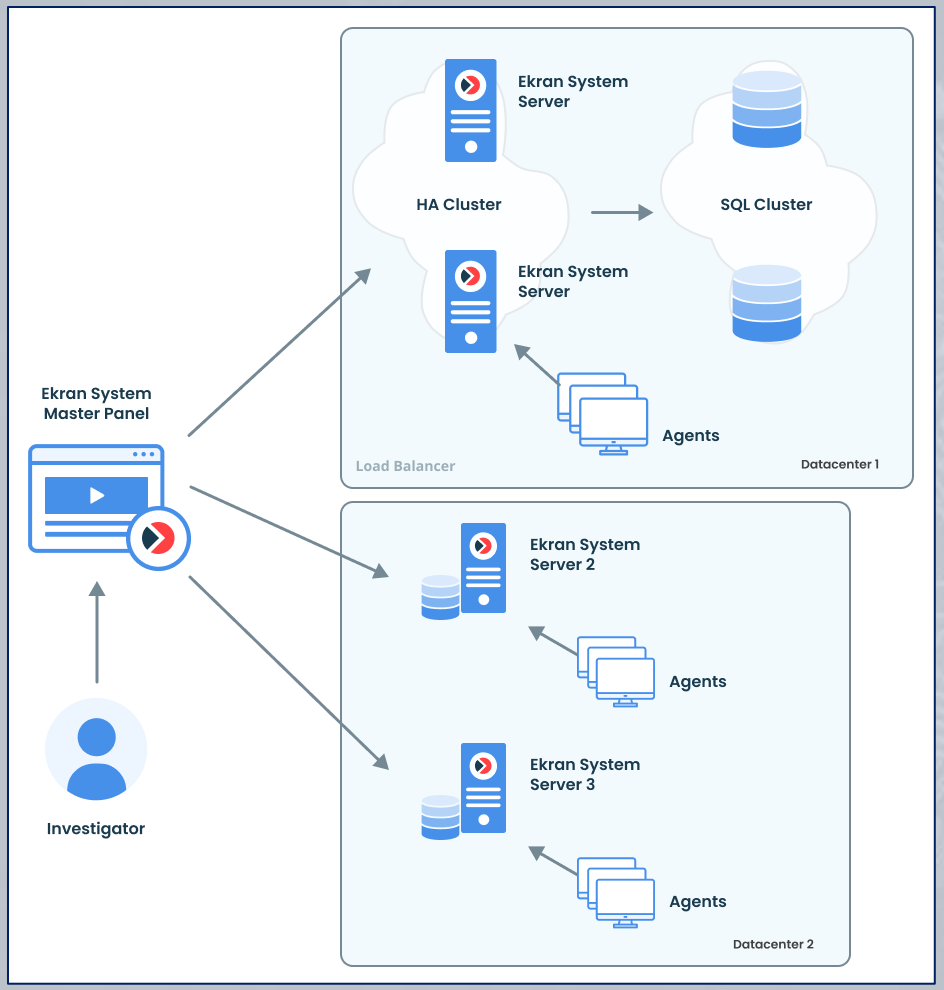


Large-Scale Deployments

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.

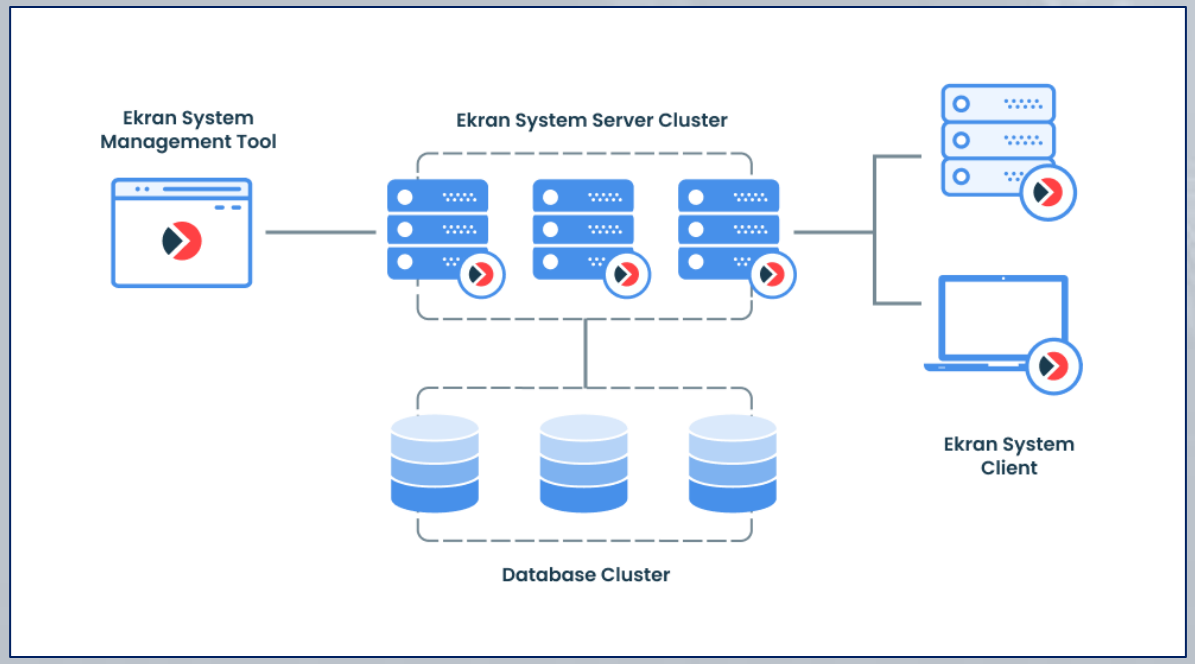
For complex deployments, Ekran System also offers **high availability & disaster recovery**, and **multi-tenant** mode, and also supports the use of third-party **load balancing** software.

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**.



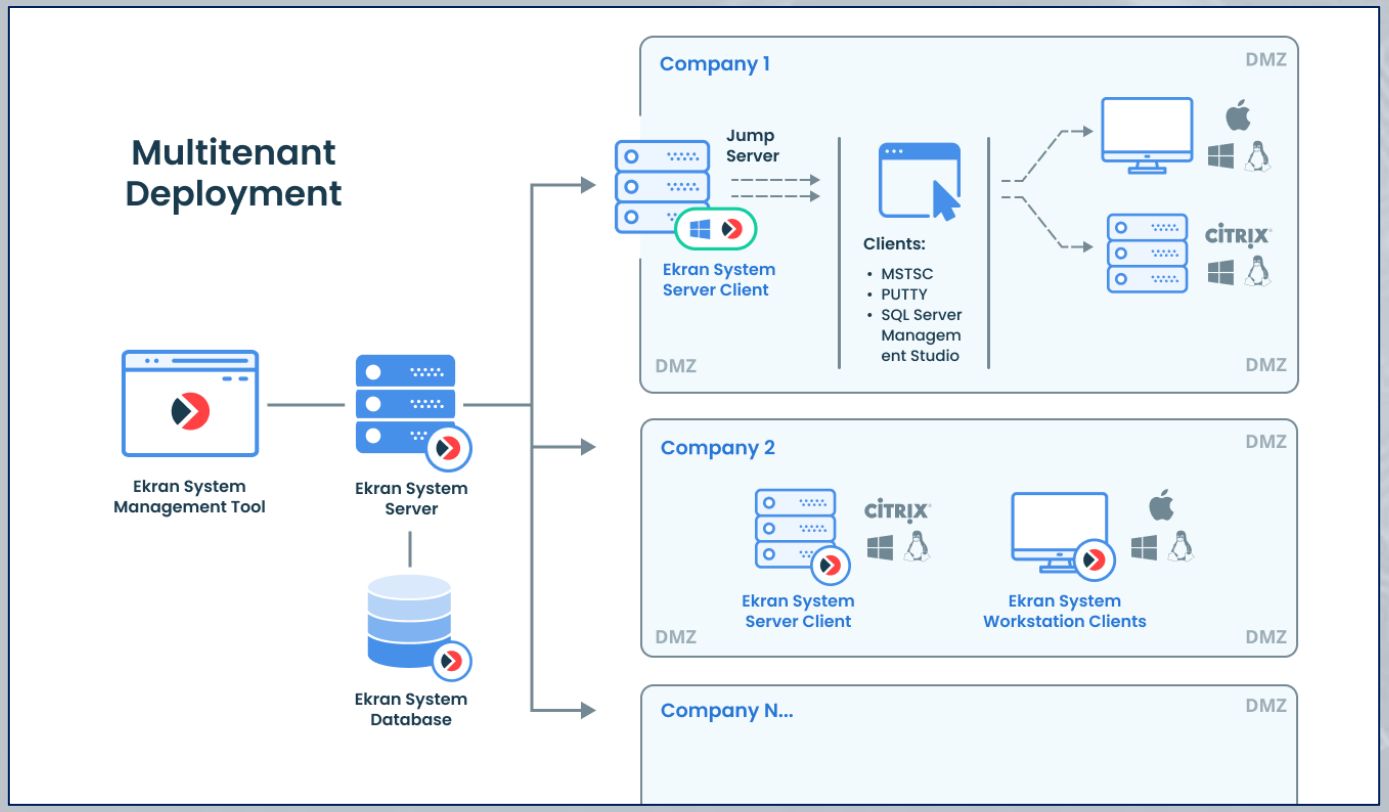
High Availability Mode

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

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.

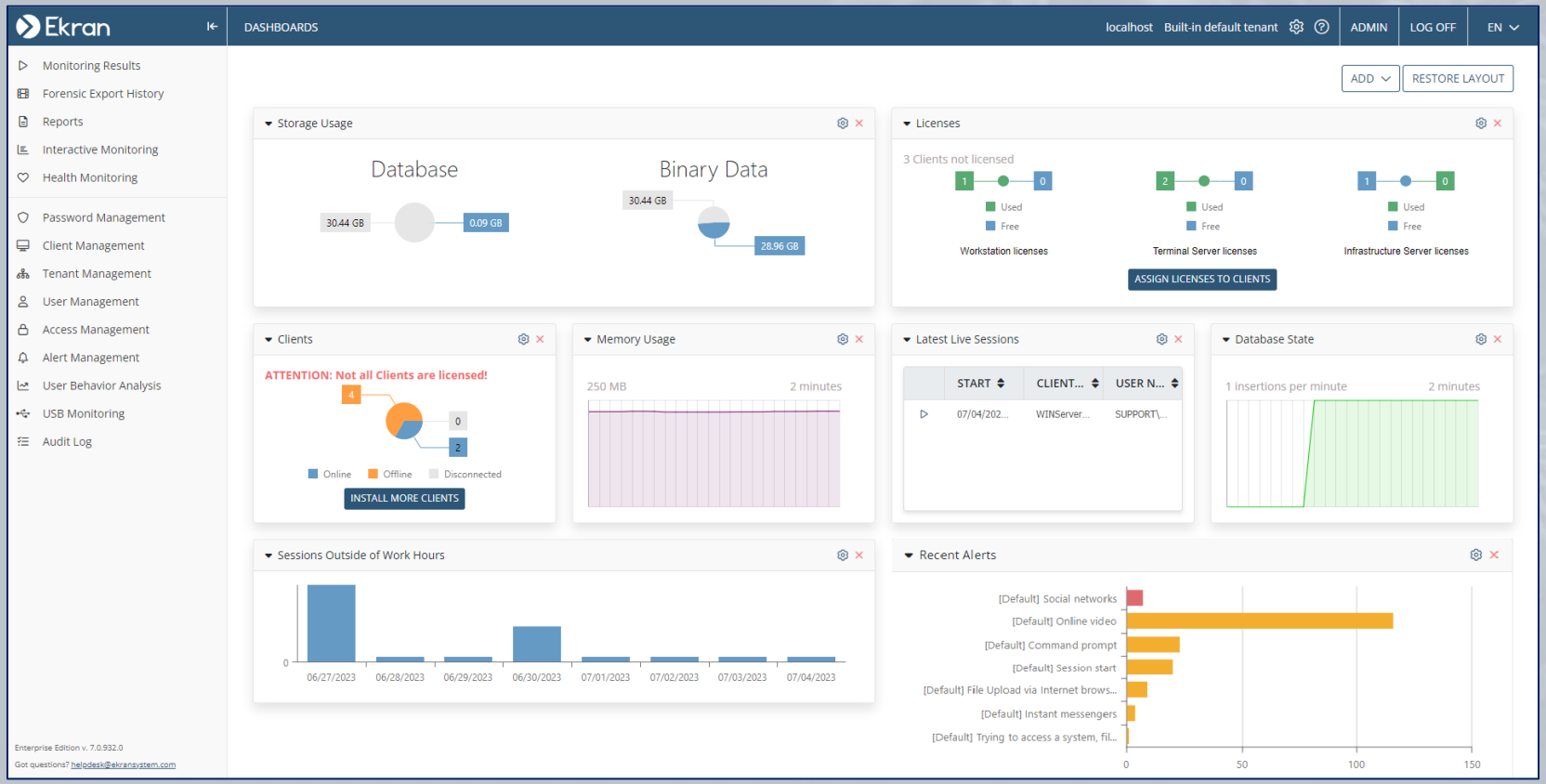


The Ekran System Application Server & the Management Tool

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

The Management Tool

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



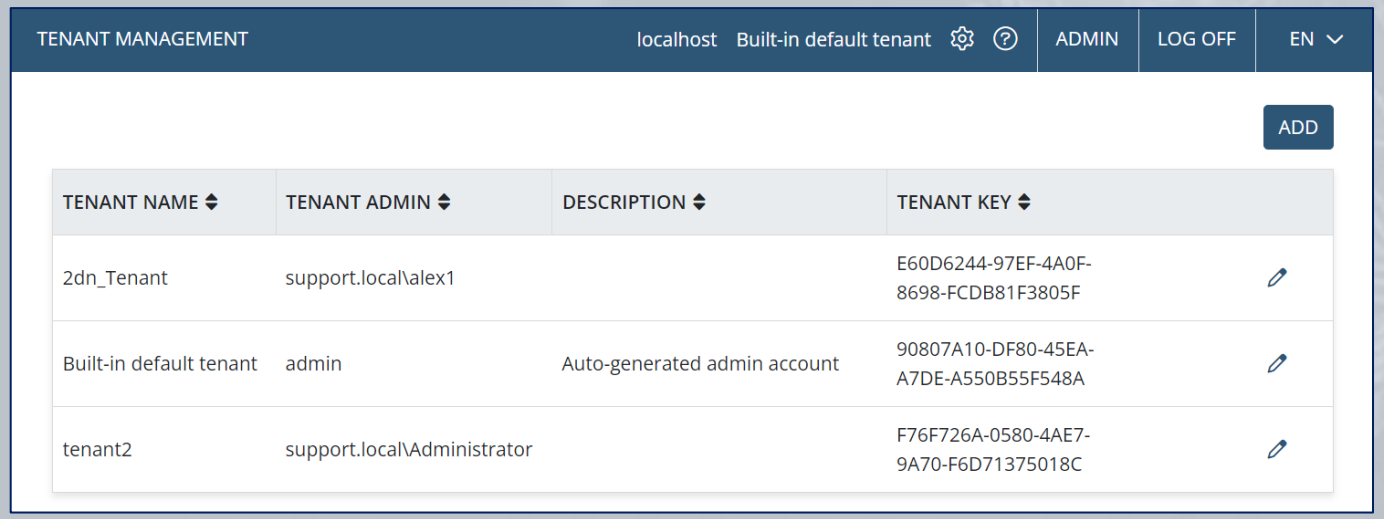
Tenant Management

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.

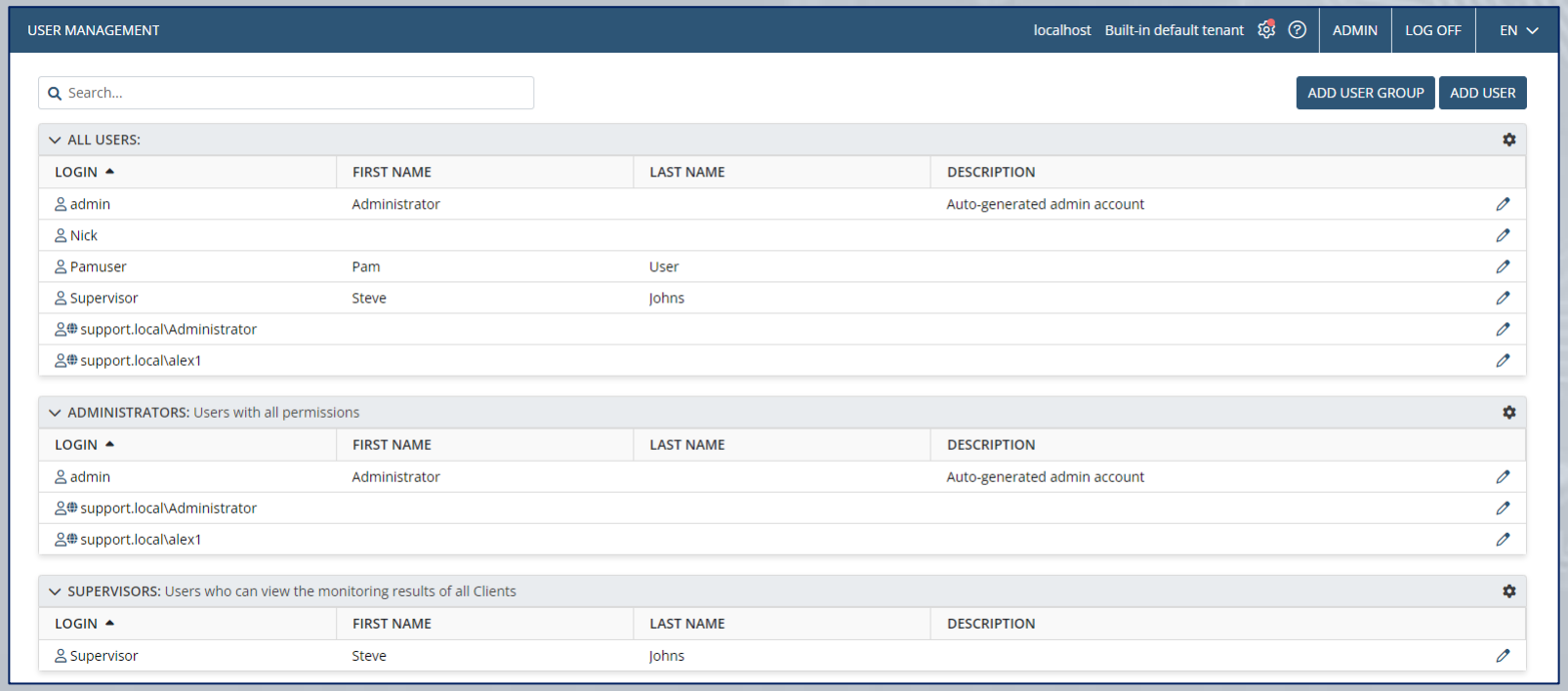
In Multi-Tenant mode, all tenant **users** have access to their tenant Clients, but **do not have access to other tenants'** Clients, configurations, alerts, reports, etc.

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



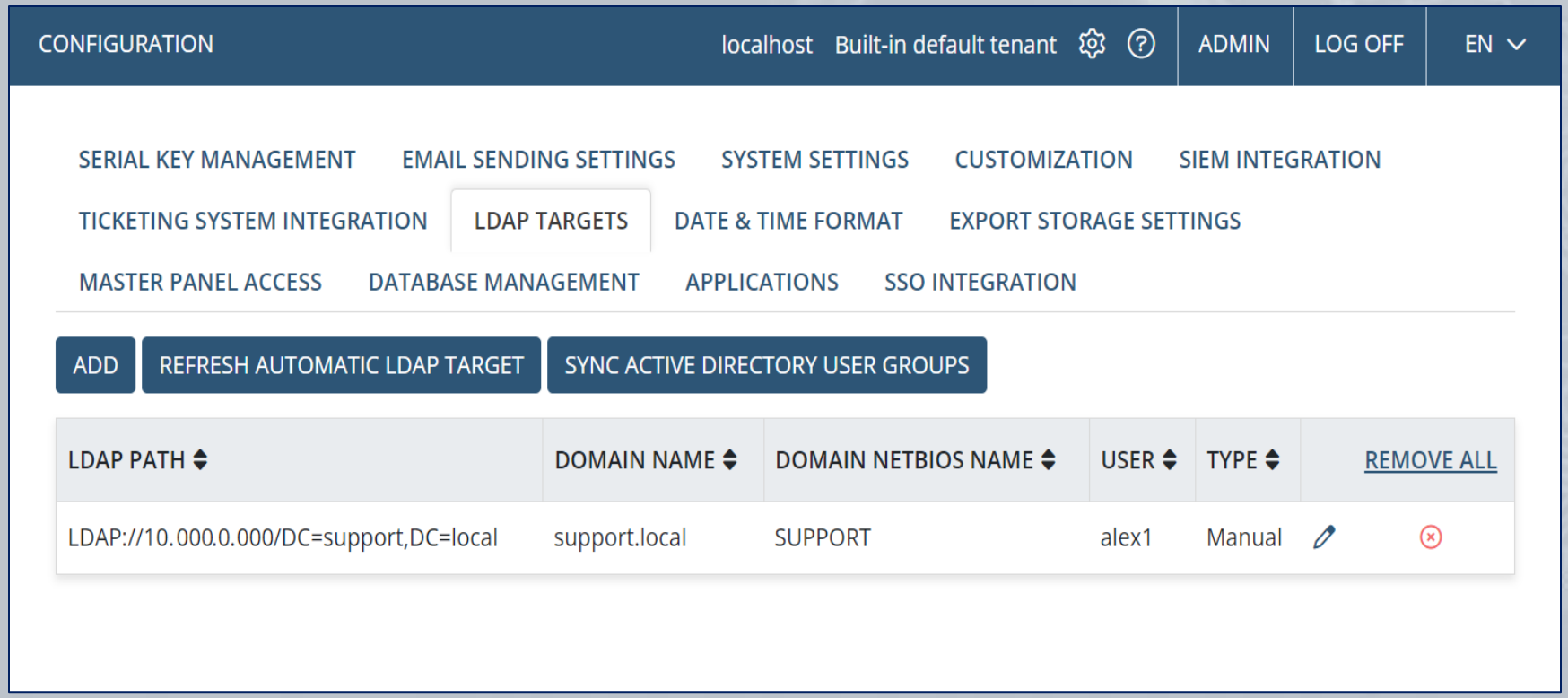
User Management & Permissions

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



Active Directory Integration

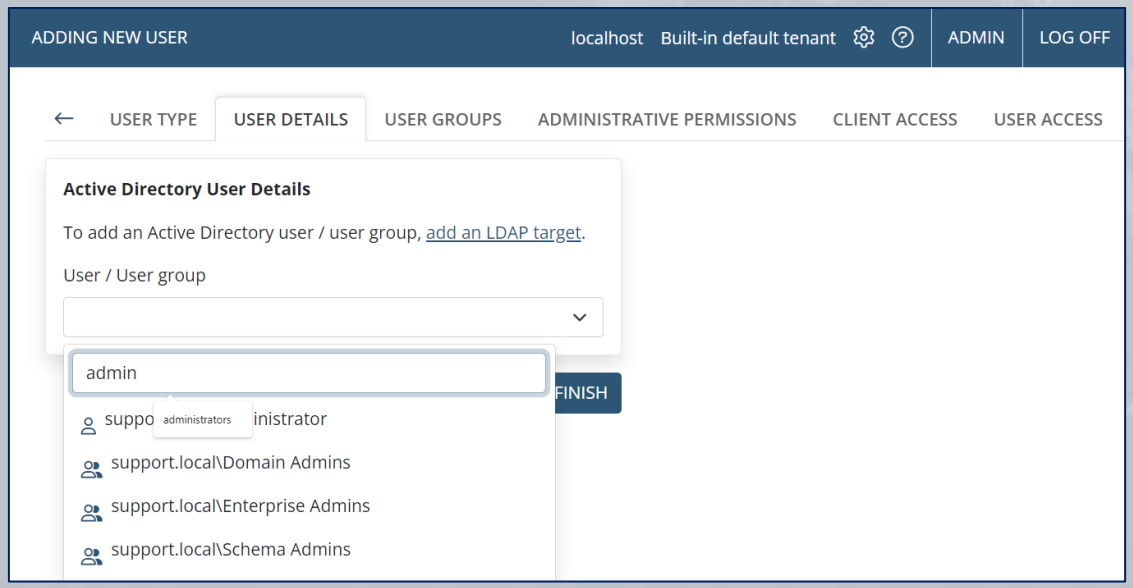
Integration with Active Directory allows you to establish domain trusts with **multiple domains**.



Active Directory Integration

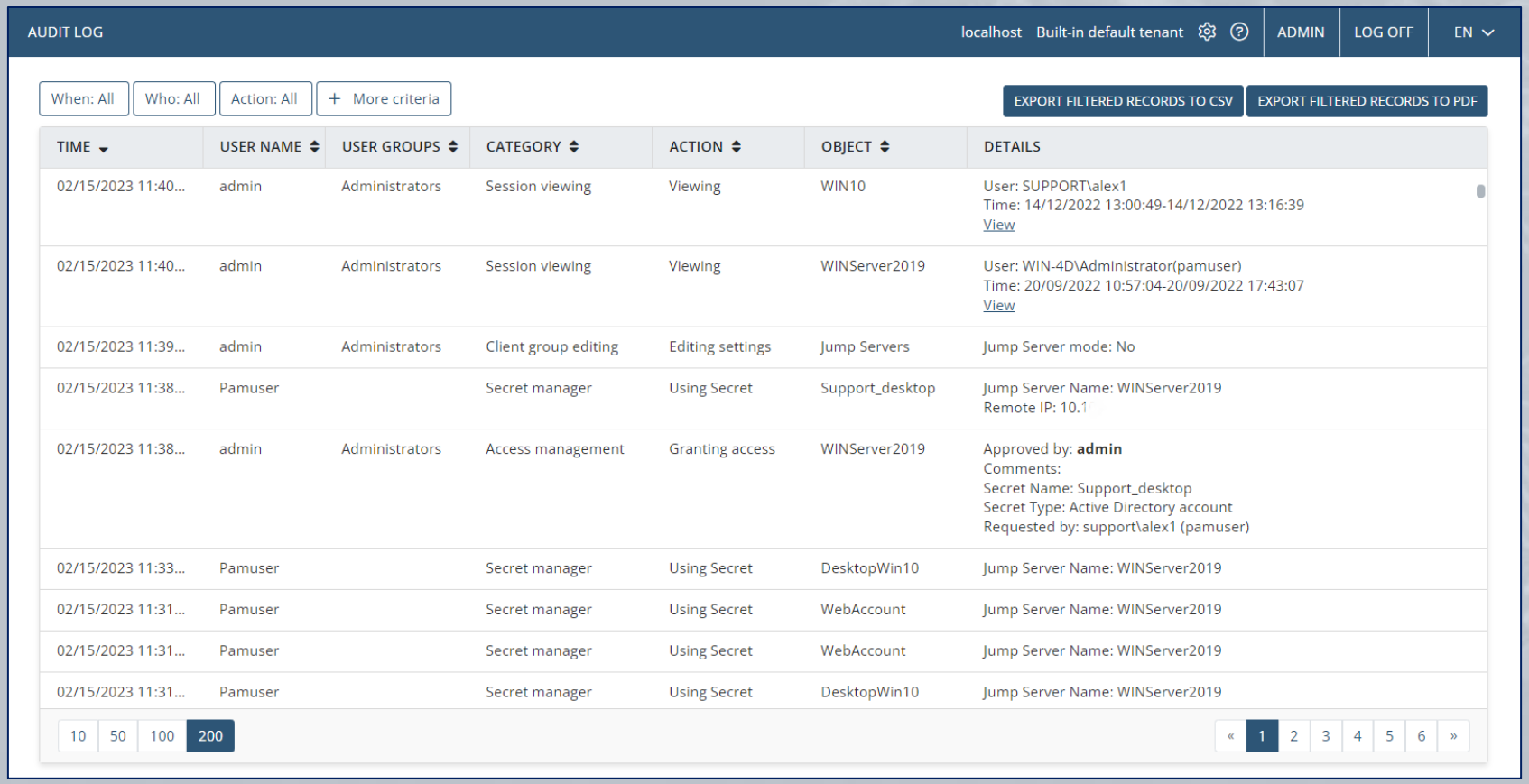
Integration with Active Directory allows you to do the following:

- 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.



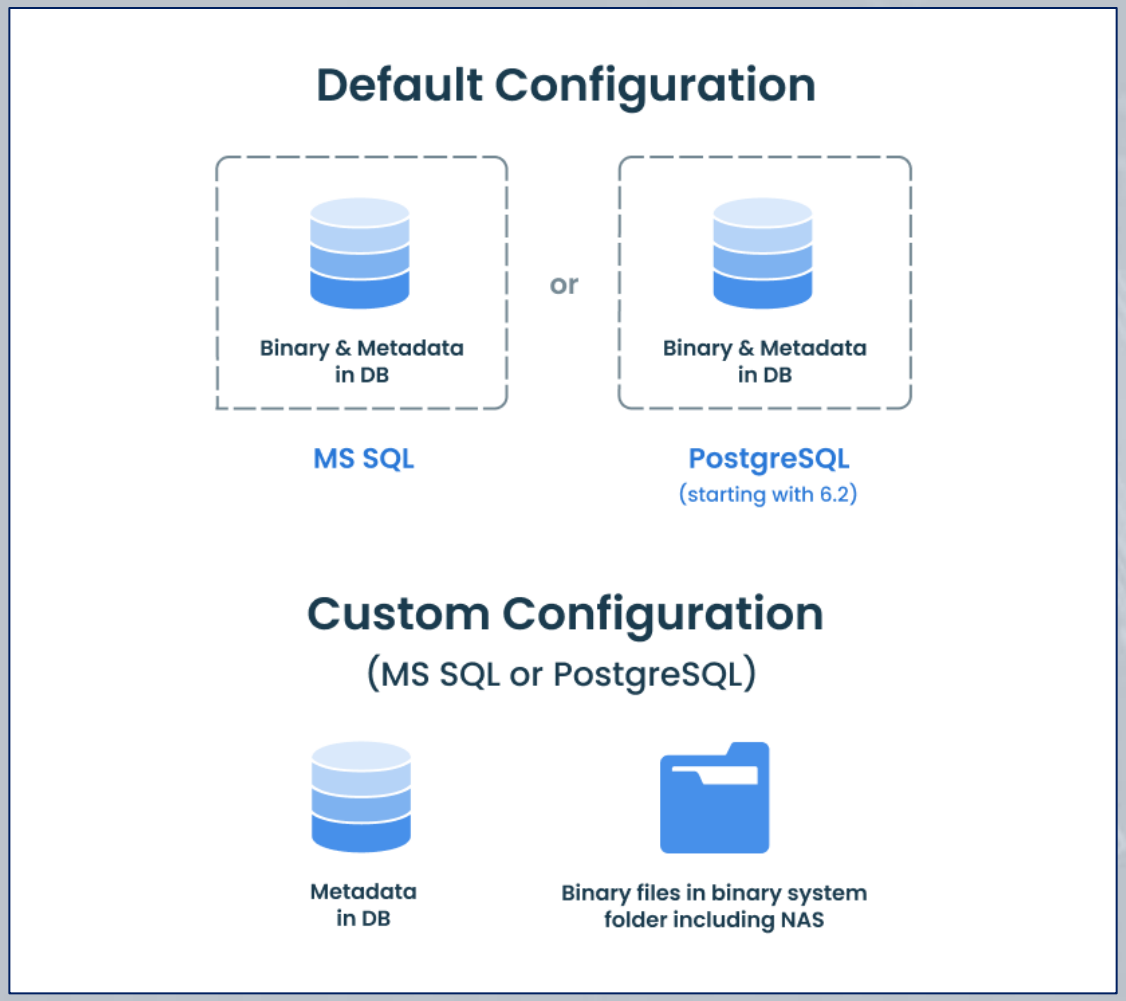
The Audit Log

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



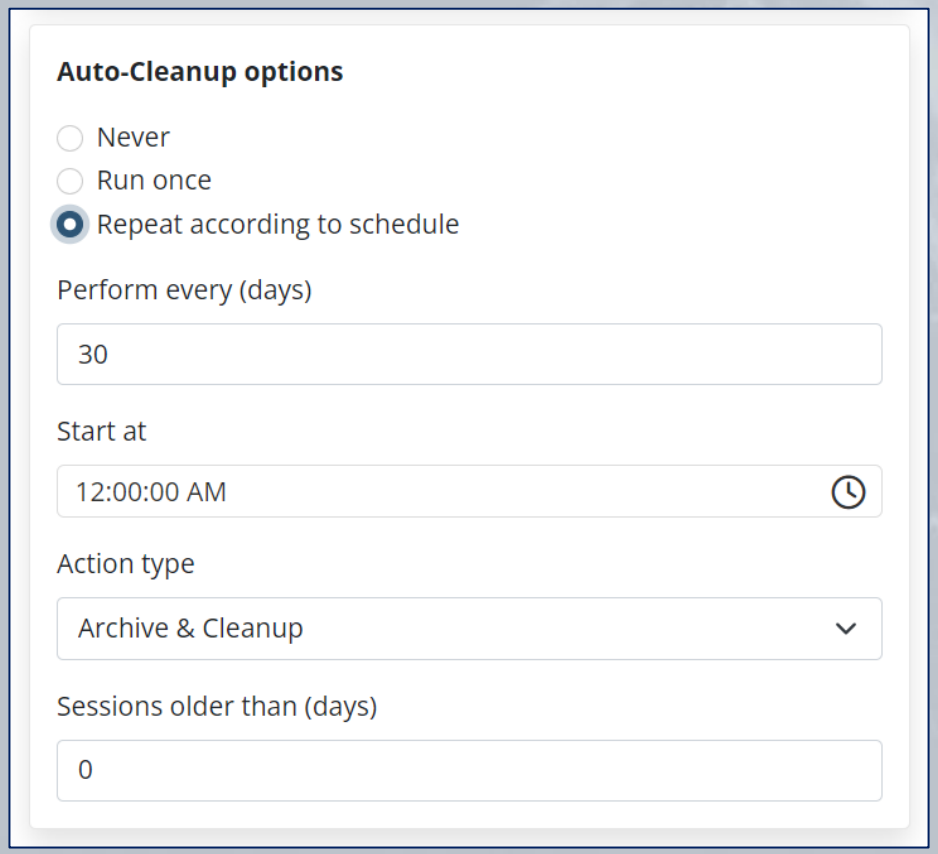
Database Management

Database Configuration



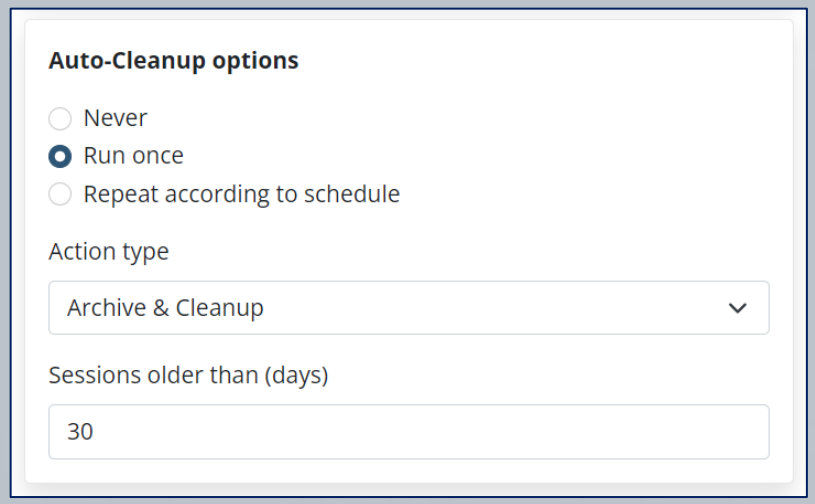
Database Cleanup

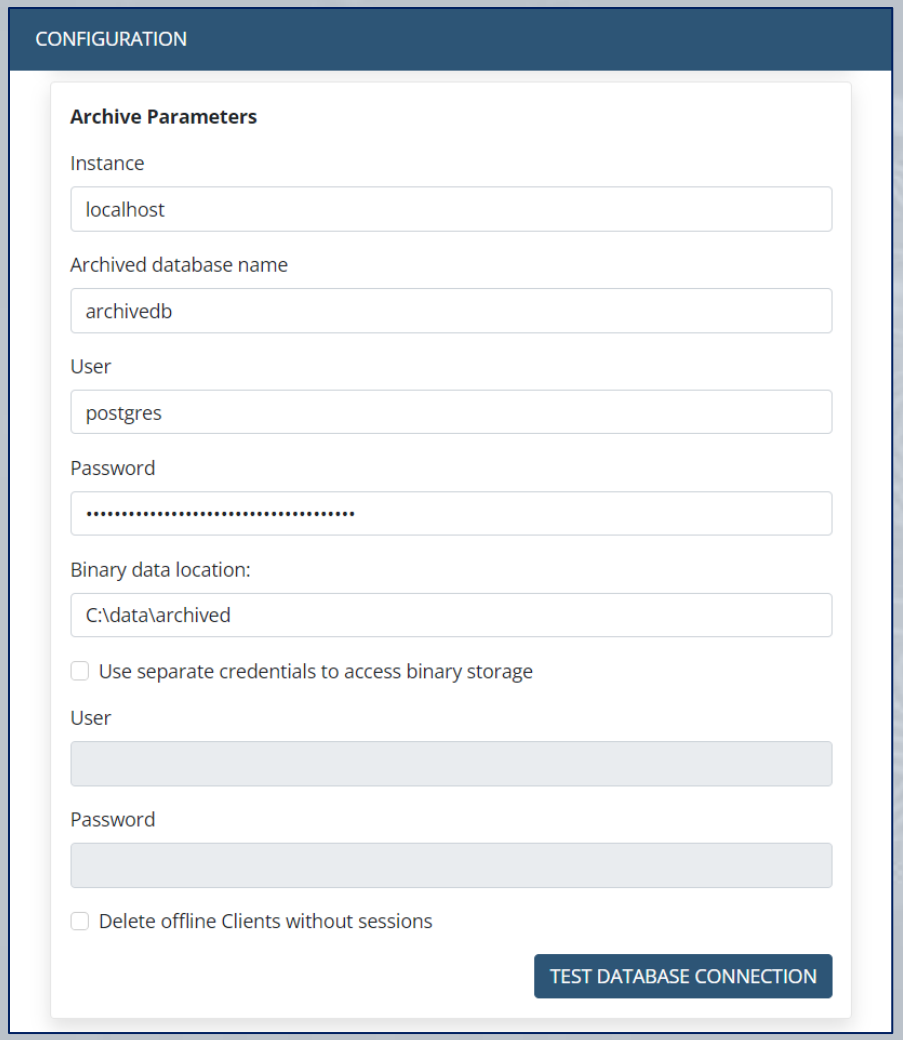
You can configure a **cleanup** (or **archive & cleanup**) operation that can be applied to either a specific **Client** or a specific **Client group**.



Database Archiving

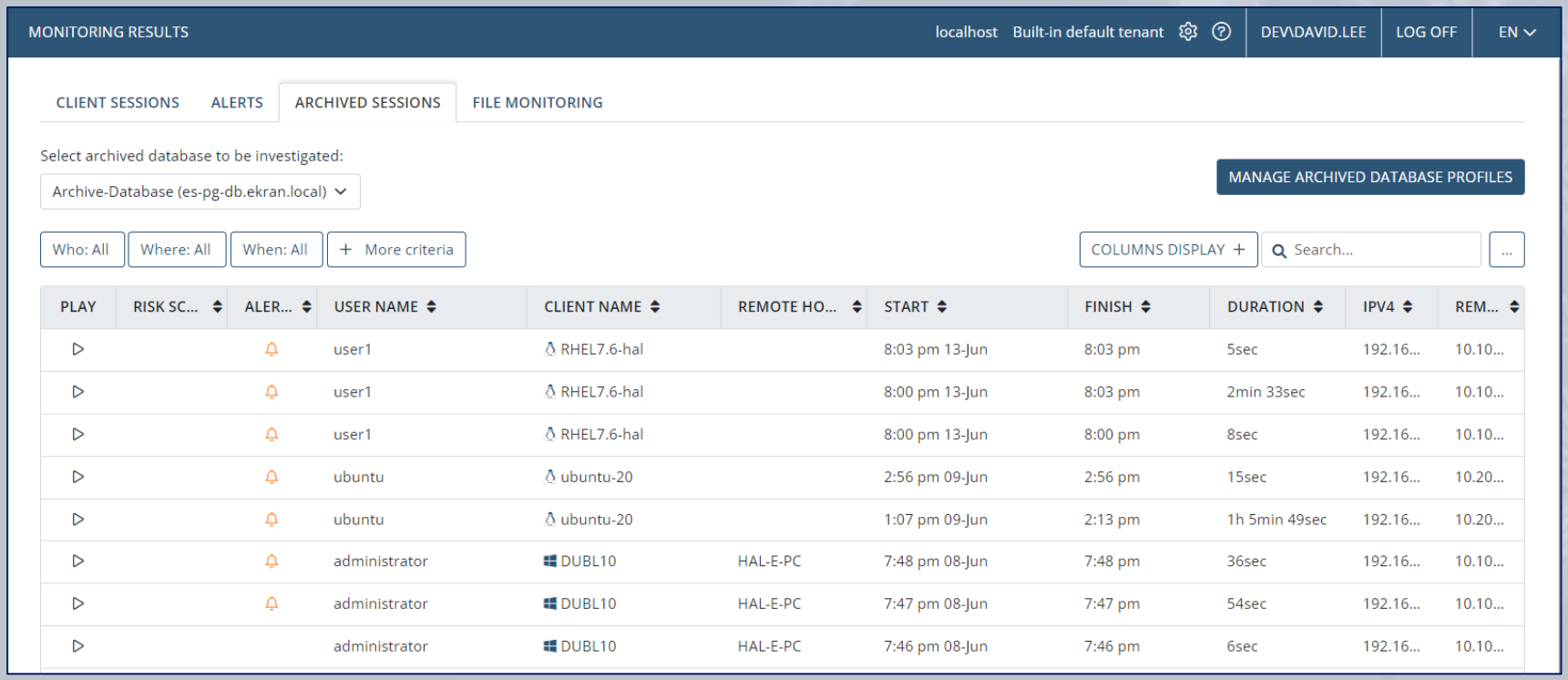
It is good practice to archive and delete old monitored data from the database regularly to avoid **running out of space** on the Application Server computer, and to **save the monitored data** in **secure storage**.





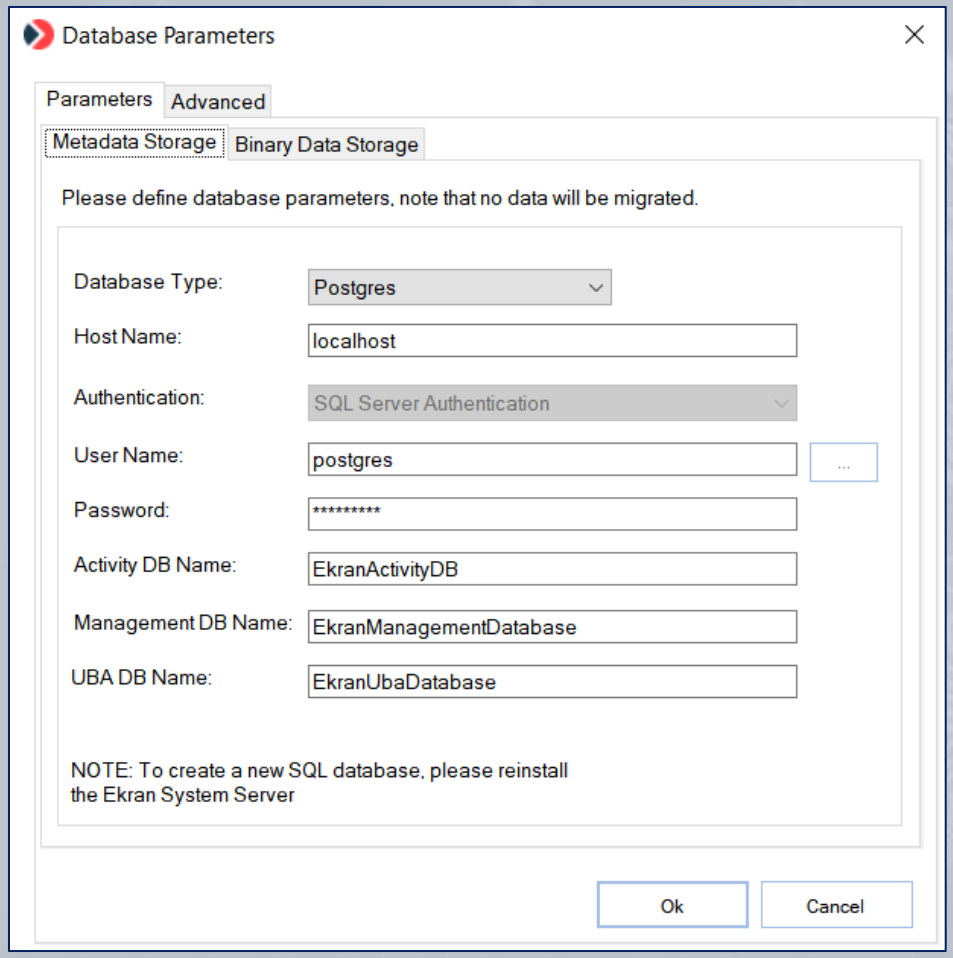
Database Archiving

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**.



Database Parameters

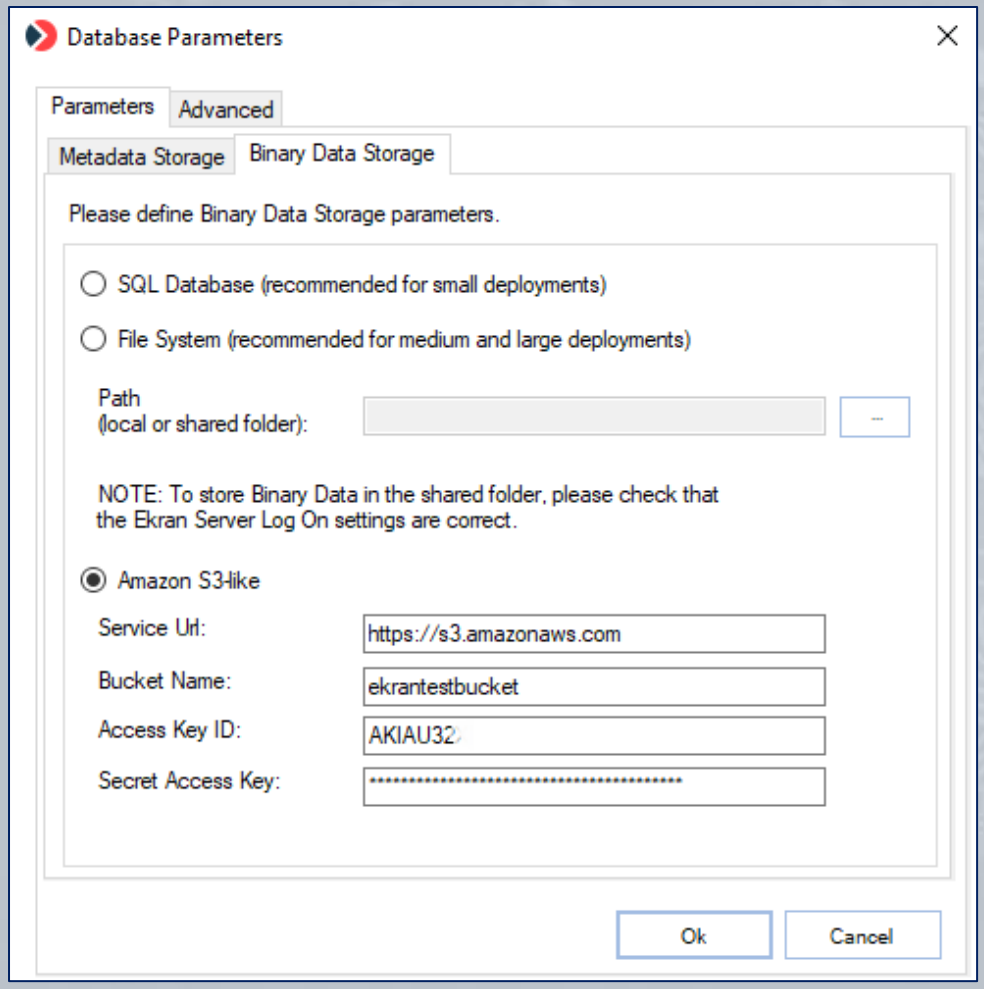
If the **database credentials** defined during installation of the Application Server have been changed (e.g. according to your corporate policy), you can easily **edit them** without reinstalling the Application Server.



Database Parameters (for Binary Data Storage)

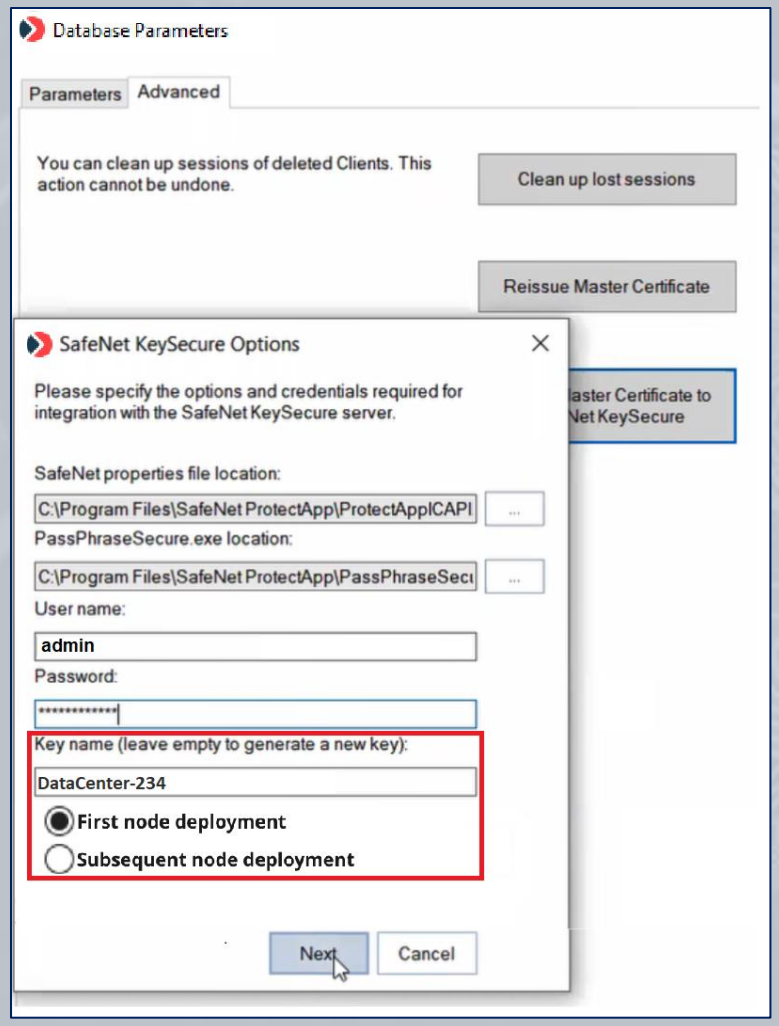
A **new location** (e.g. **Amazon S3** storage) can alternatively be used to **store the binary data** (i.e. screen captures) recorded during monitoring.

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



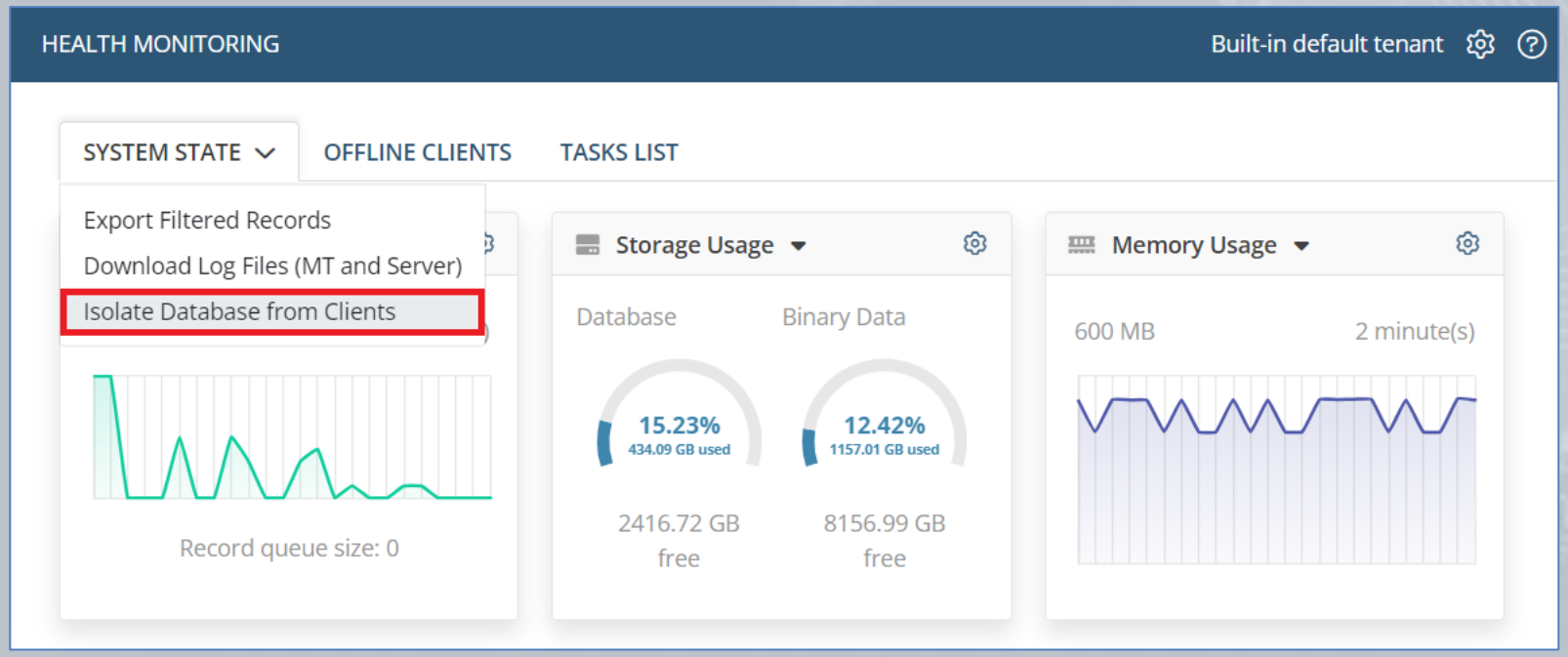
Database Parameters (Hardware Security Module)

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.



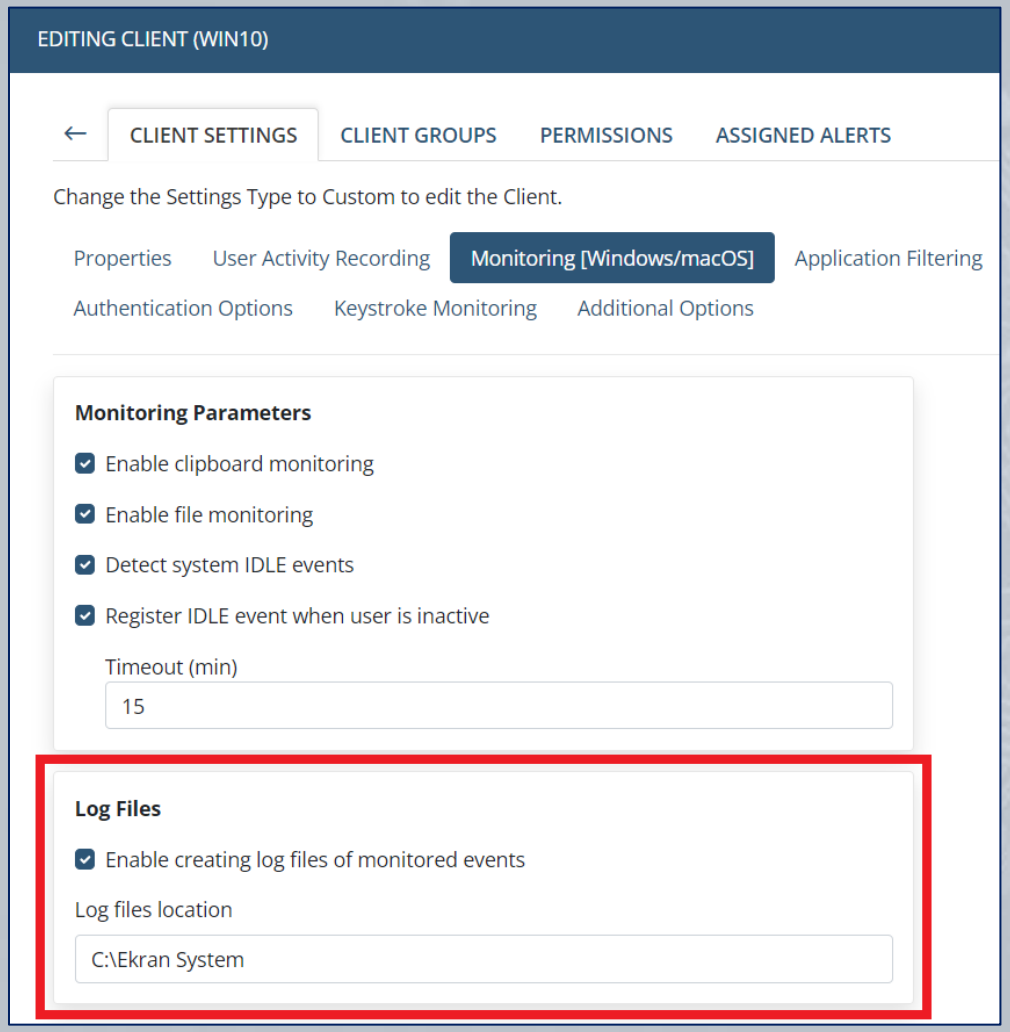
Isolating the Database from Clients

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**.



SIEM Integration

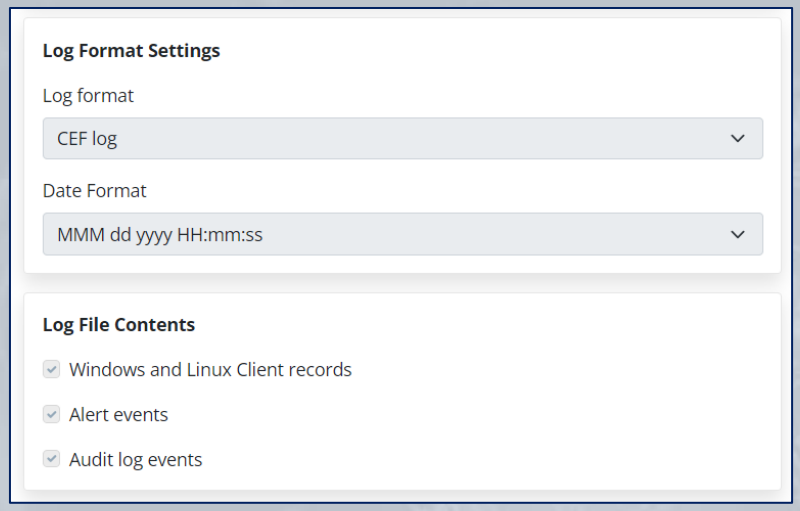
Ekran System **integrates with your SIEM system** by using the log files of monitored events.

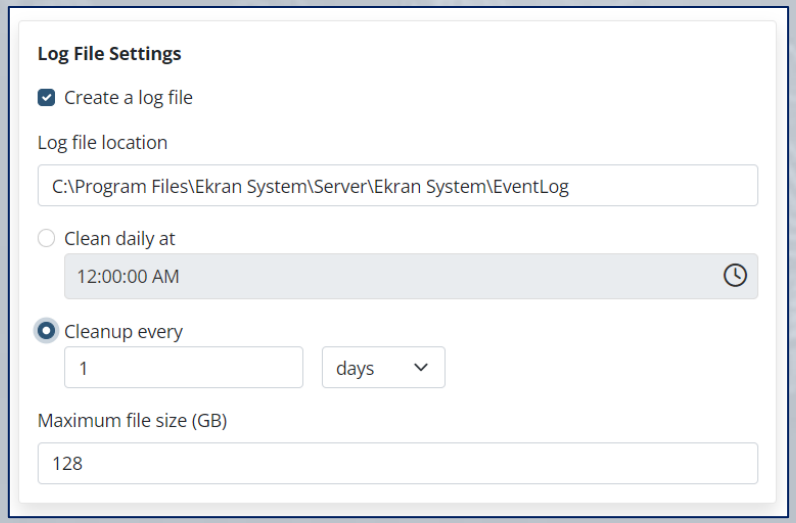


SIEM Integration

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

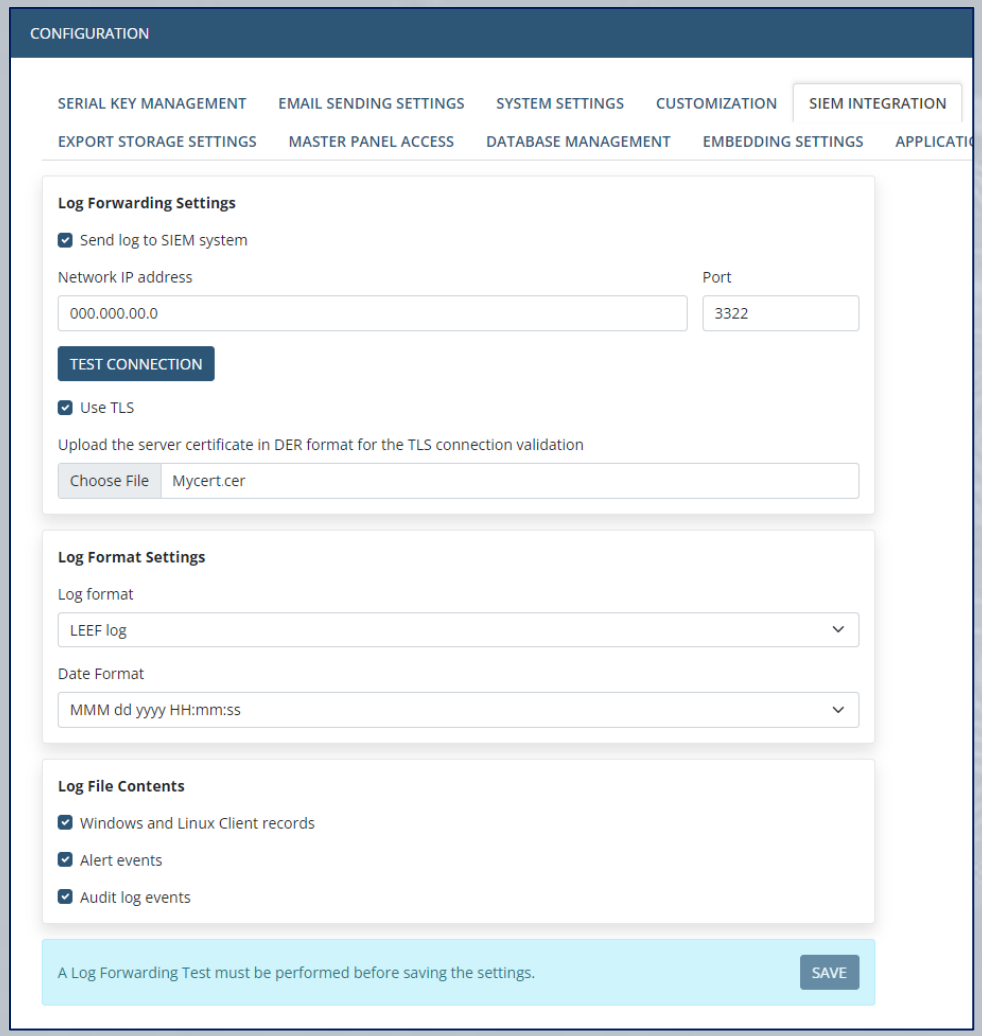
- Common Event Format (CEF)
- Log Event Extended Format (LEEF)





SIEM Integration

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.



Licensing

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

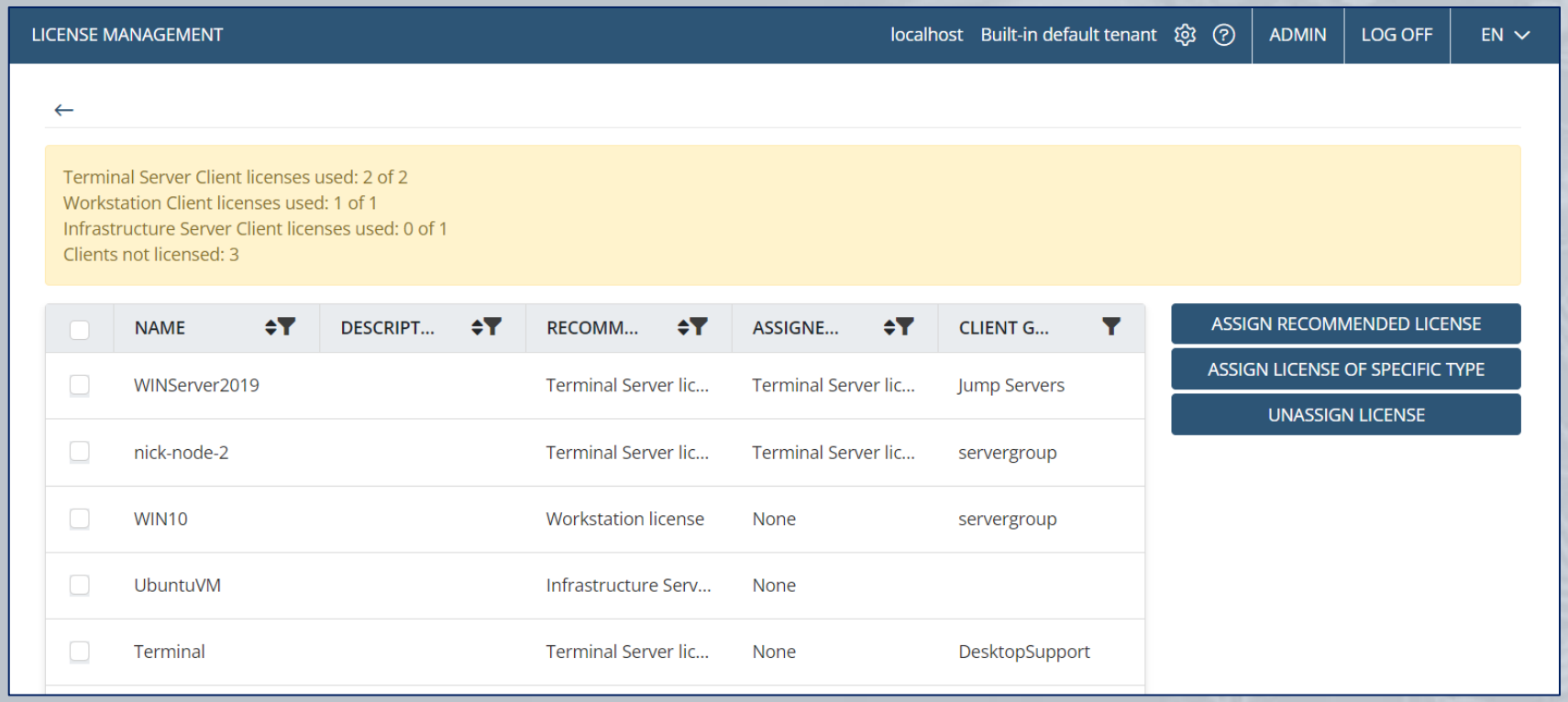
Licensing

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).

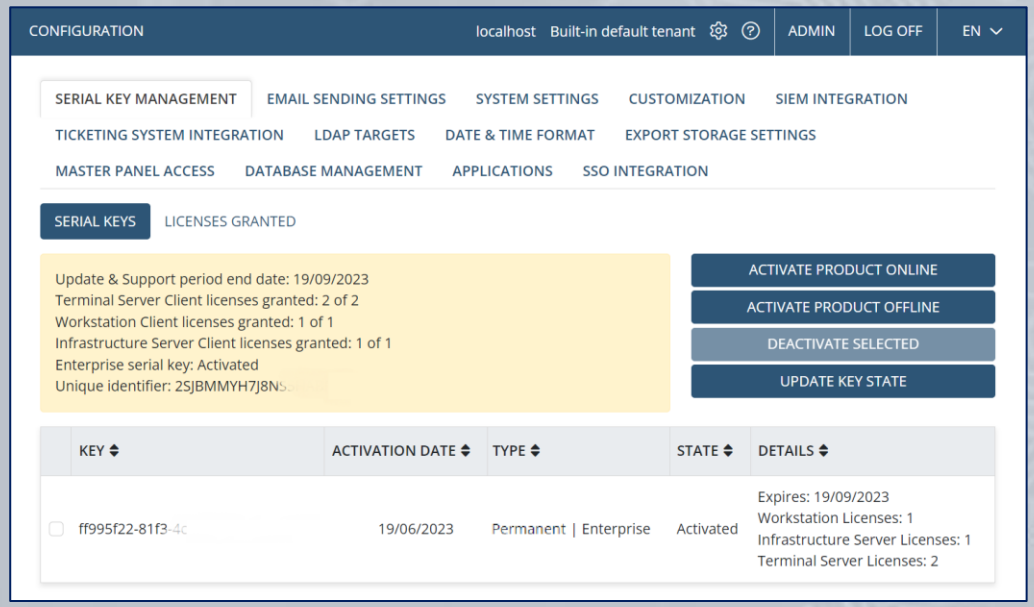
Licensing


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
NAME
DESCRIPT...
RECOMM...
ASSIGNE...
CLIENT G...
WINServer2019
Terminal Server lic...
Terminal Server lic...
Jump Servers
nick-node-2
Terminal Server lic...
Terminal Server lic...
servergroup
WIN10
Workstation license
None
servergroup
UbuntuVM
Infrastructure Serv...
None
Terminal
Terminal Server lic...
None
DesktopSupport
ASSIGN RECOMMENDED LICENSE
ASSIGN LICENSE OF SPECIFIC TYPE
UNASSIGN LICENSE

Serial Key & License Management

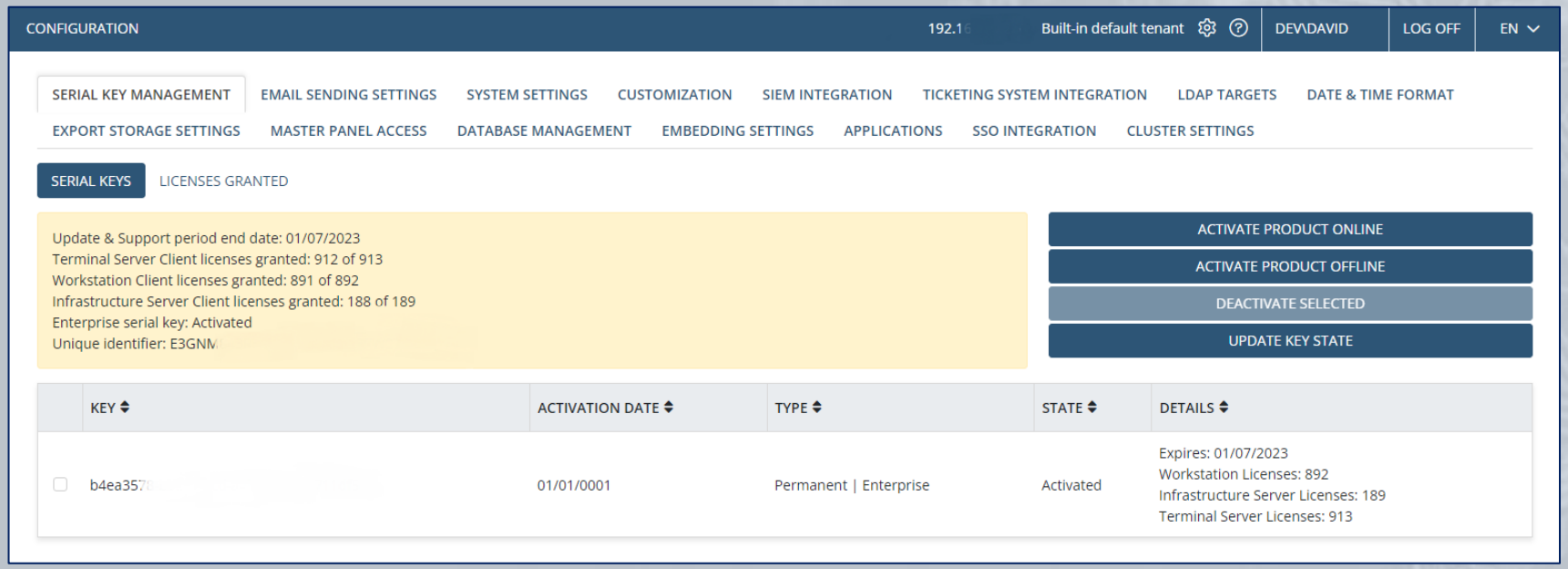
You can request a **Trial (or SaaS Trial) serial key** for 30 days to deploy the system and review its features, including those in the Enterprise Edition, and also update the product during this period.

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 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.



Floating Endpoint Licensing

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.

Unique Enterprise Edition Features

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

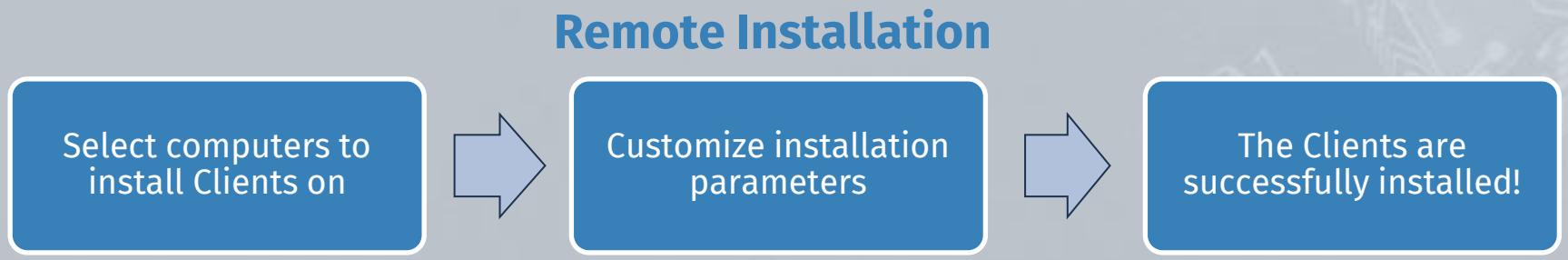
- High Availability
- Load Balancer Support
- Multi-Tenant Mode
- Password Management
- Detection of Disconnected Clients
- Integration with Ticketing Systems
- SIEM Integration
- Access Requests and Approval Workflow
- File Monitoring
- User Behavior Analytics (UEBA)
- Database Archiving
- Remote Host 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

Installing Ekran System Clients

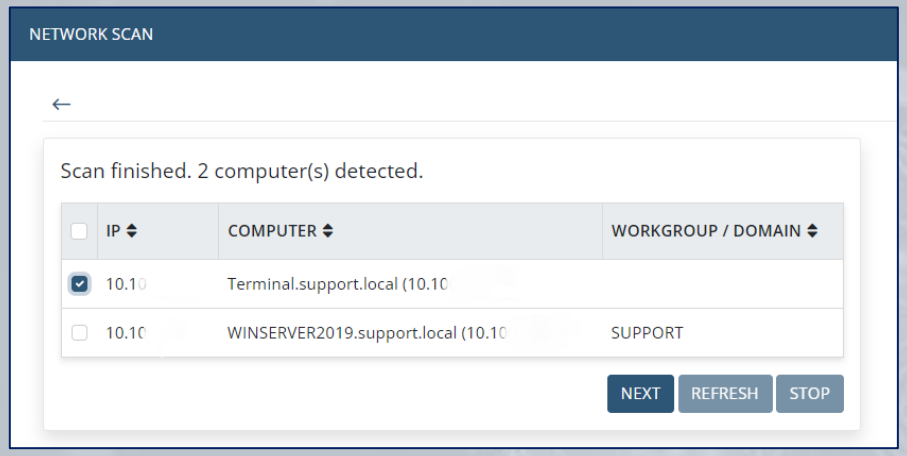
Convenient Ekran Client installation:

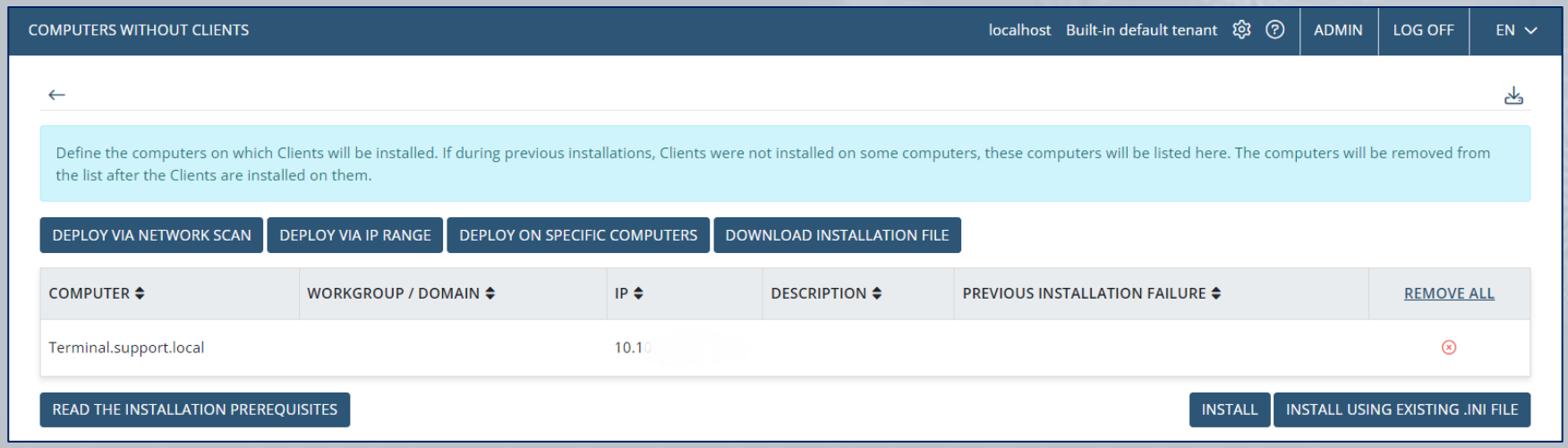
- **Locally**:
  - Linux Clients (using a tar.gz file)
  - macOS Clients (using a tar.gz file)
  - Windows Clients:
    - using the installation file with default parameters
    - using a package generated with customized parameters
- **Remotely:**
  - for Windows Clients
  - for macOS Clients (remote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



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**

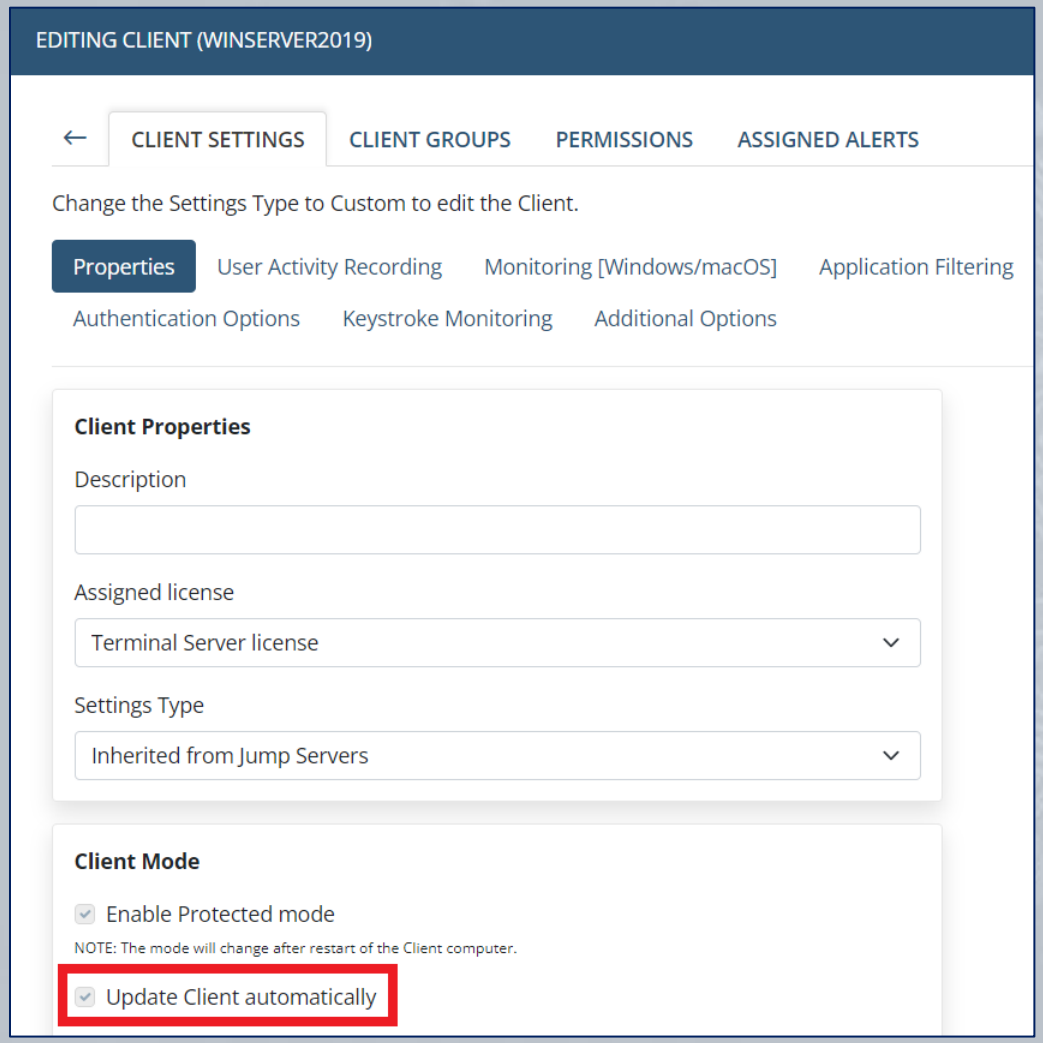




Updating Ekran System Clients

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.



Monitoring Parameters

Client Monitoring

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.

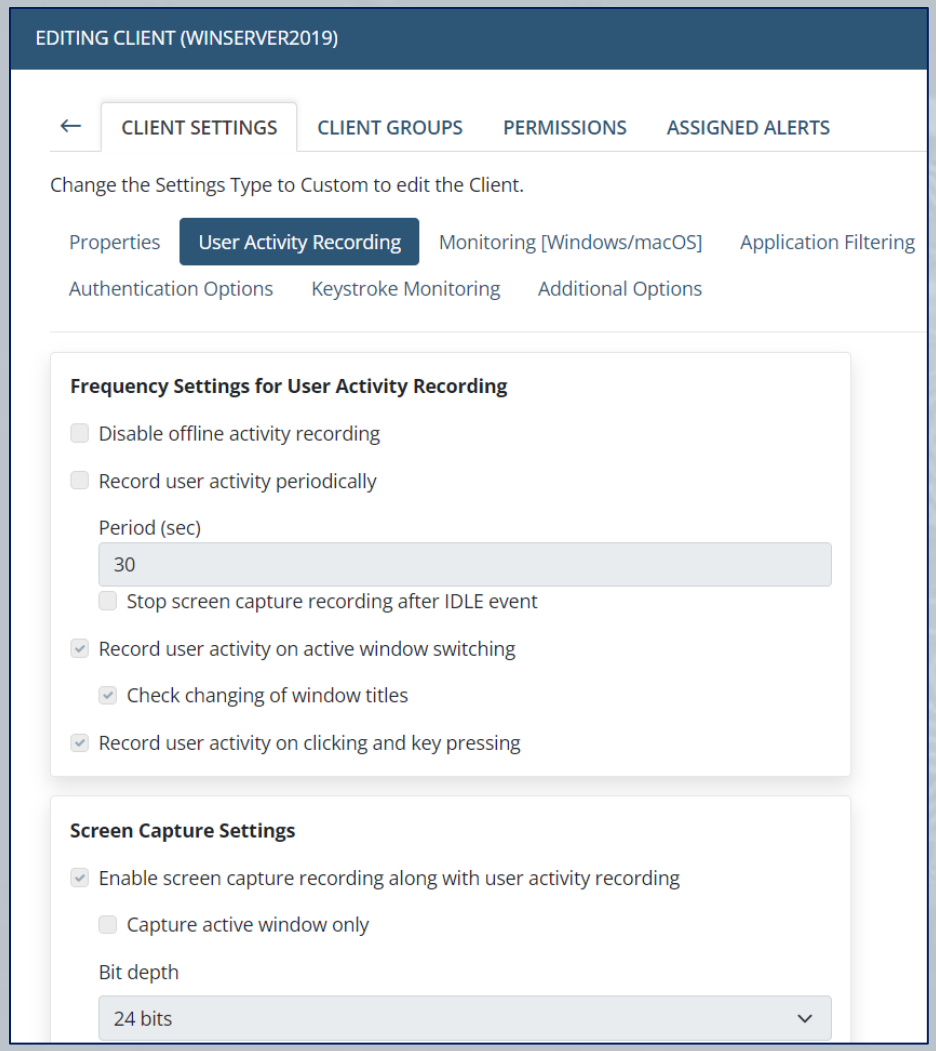
The information recorded is saved in an easy-to-review and easy-to-search form, including:

- 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).

User Activity Recording

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

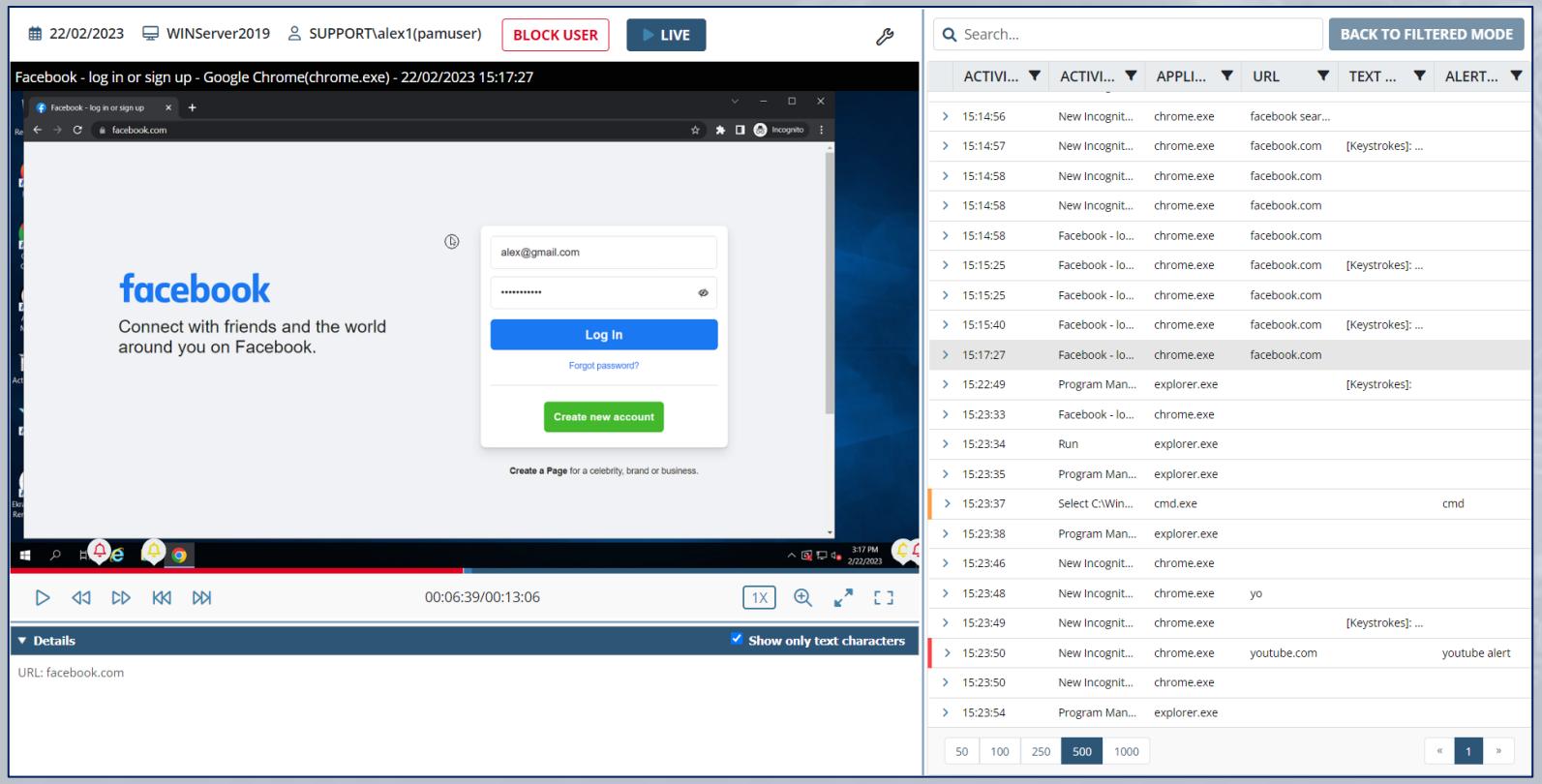
You can easily configure Windows, macOS, and Linux Clients to record screen captures of the active window or to record user activity without recording screen captures, etc.



URL Monitoring

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

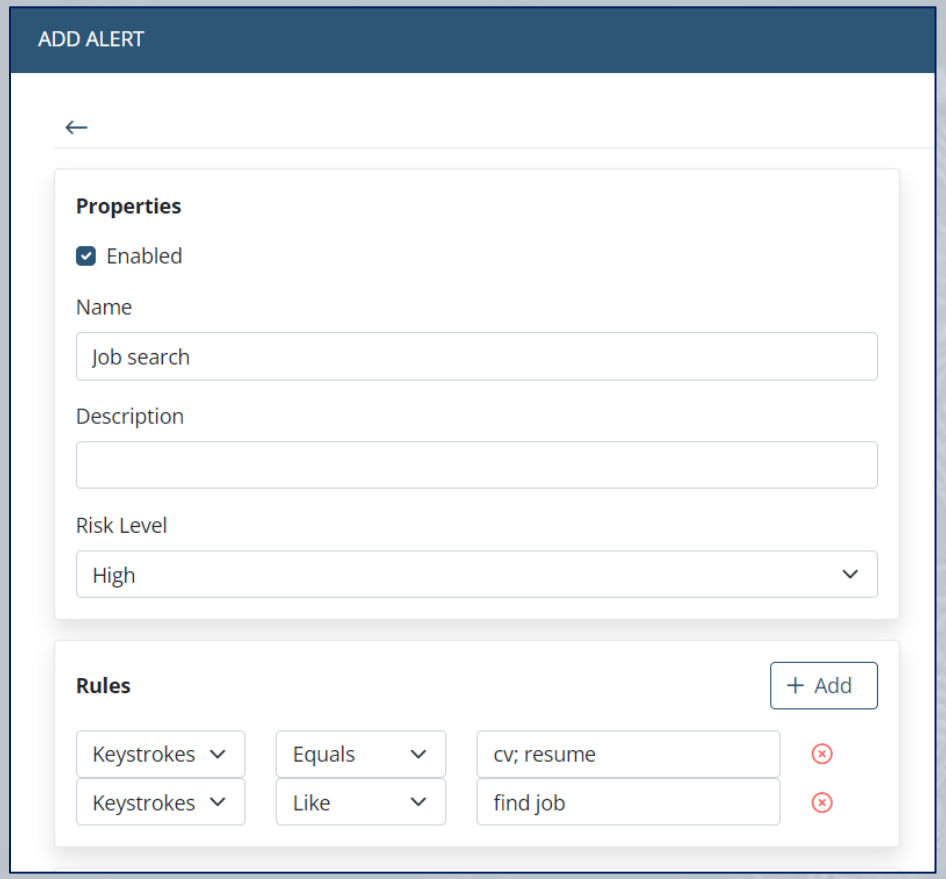
You can configure the Client to monitor either full URLs or top and second level domain names only.



Keystroke Logging

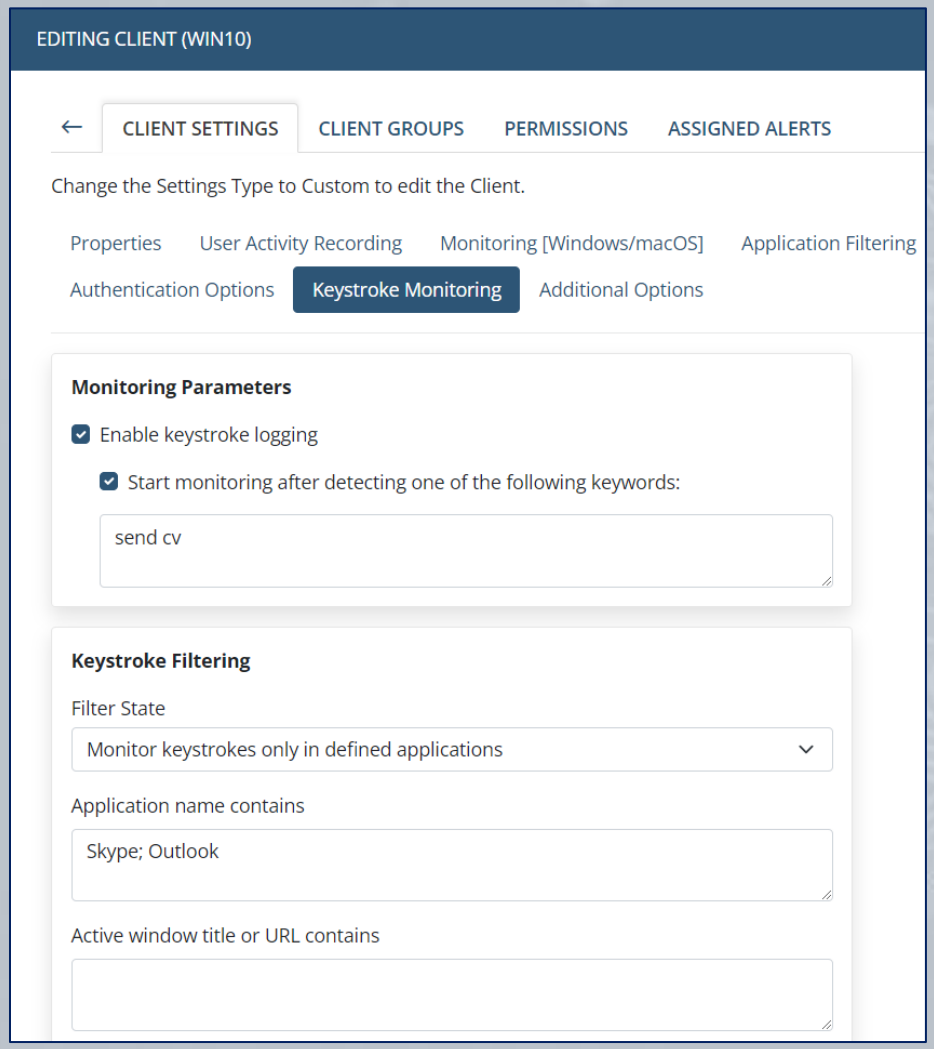
To ensure **compliance** (e.g. with GDPR), **all keystrokes logged are hidden**, but you can **perform searches** on them and **create alerts** to be triggered when specific keywords are typed.

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.



Keyword-Triggered Monitoring

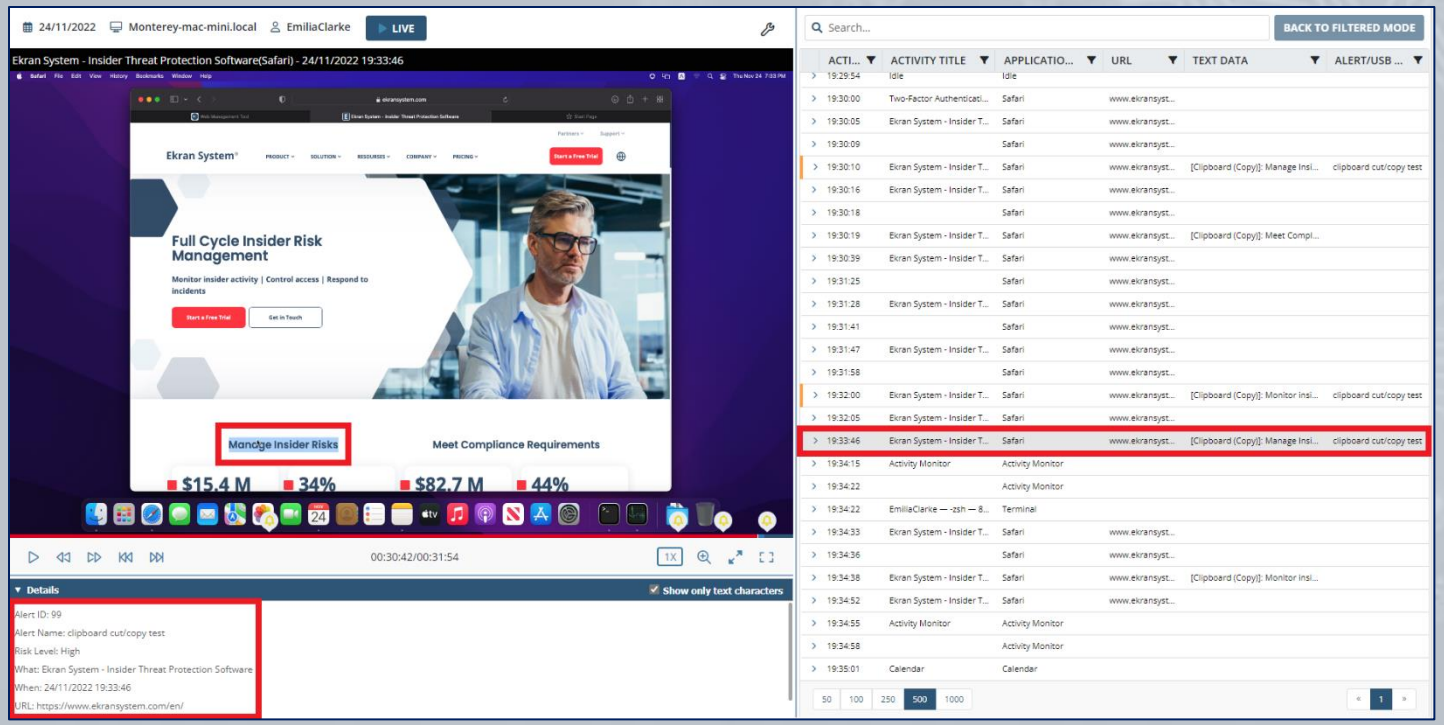
You can configure Ekran System Clients to start monitoring and recording screen captures only after they **detect** defined **keywords** entered by the user in **specified applications**.



Clipboard Monitoring

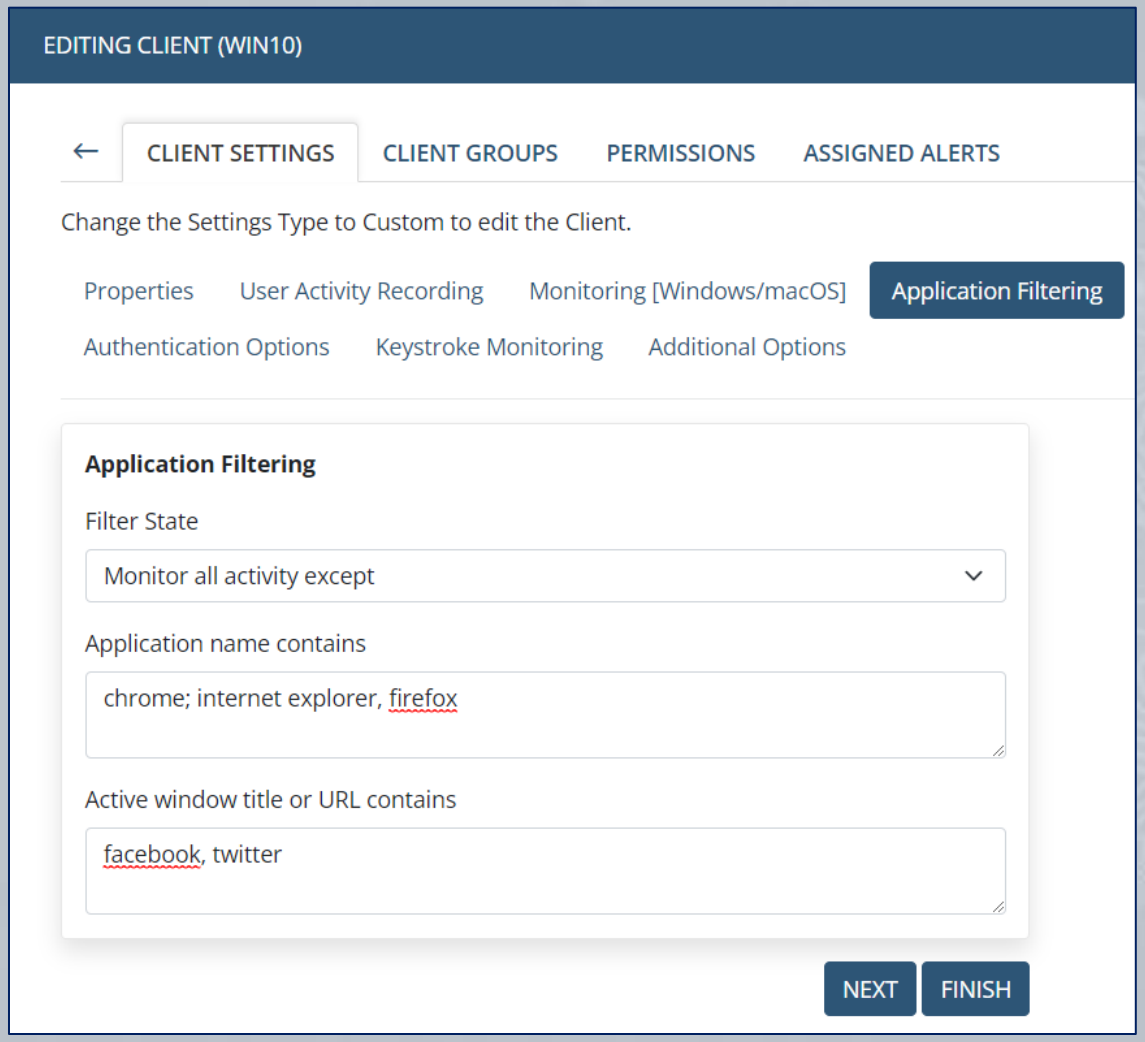
The Ekran Client **captures all text data** that is **copied/cut** from, or **pasted** into documents, files, applications, the browser address bar, etc, on Windows and macOS Client computers.

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



Application Filtering

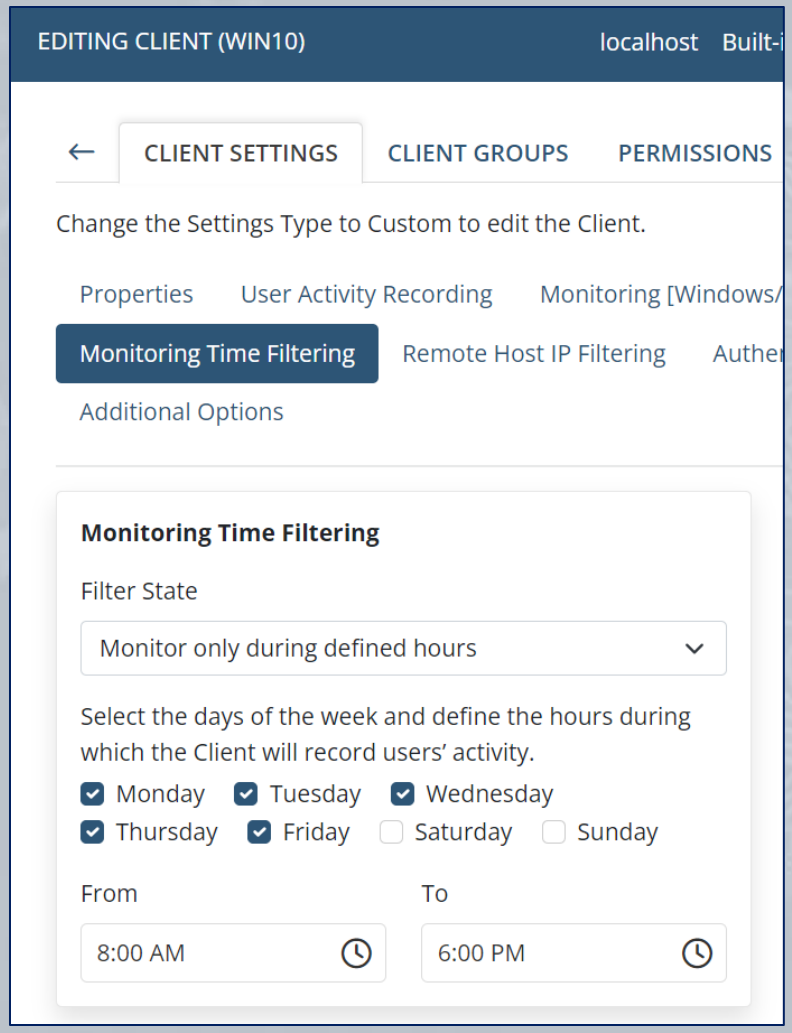
Ekran System allows you to define **filtering rules** for **websites** and **applications** to adjust the amount of monitored data, and to exclude areas where personal information can be observed, so as to **comply** with **corporate policy rules** and **country regulations** (e.g. GDPR) related to user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



Monitoring Time Filtering

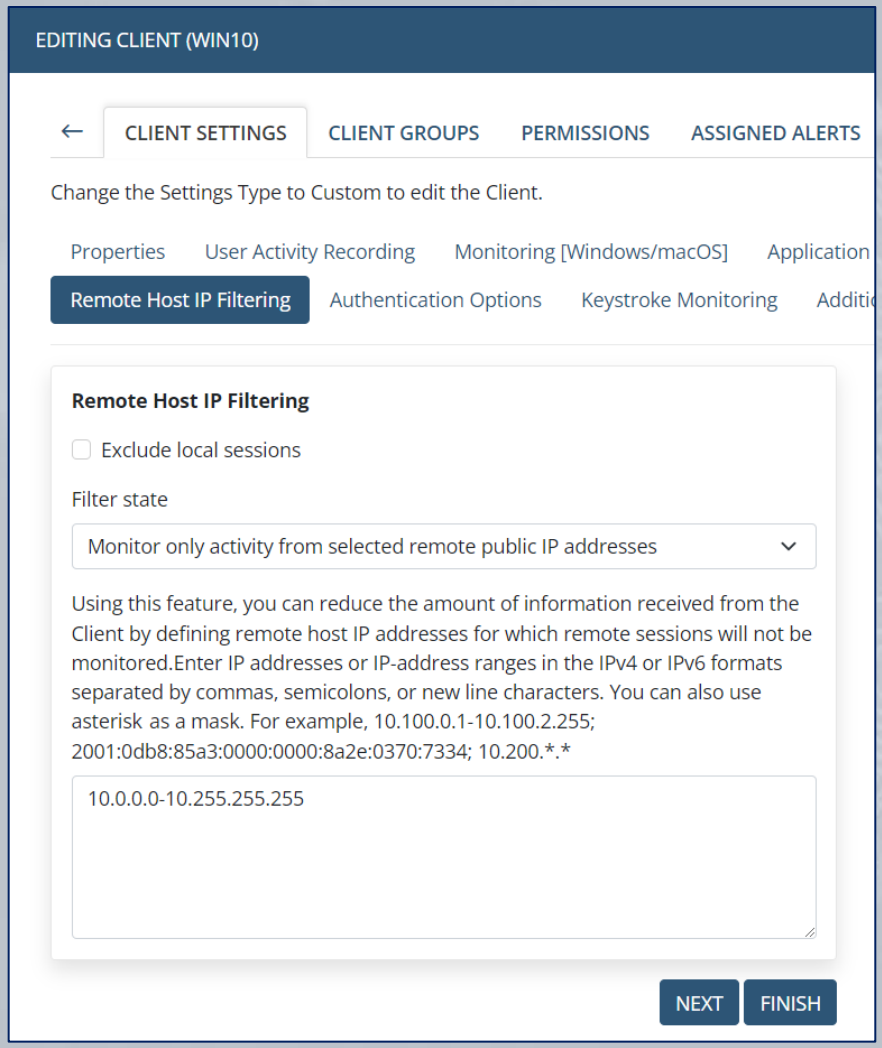
In addition to application filtering rules, you can also define rules for the **time when monitoring** will take place.

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.



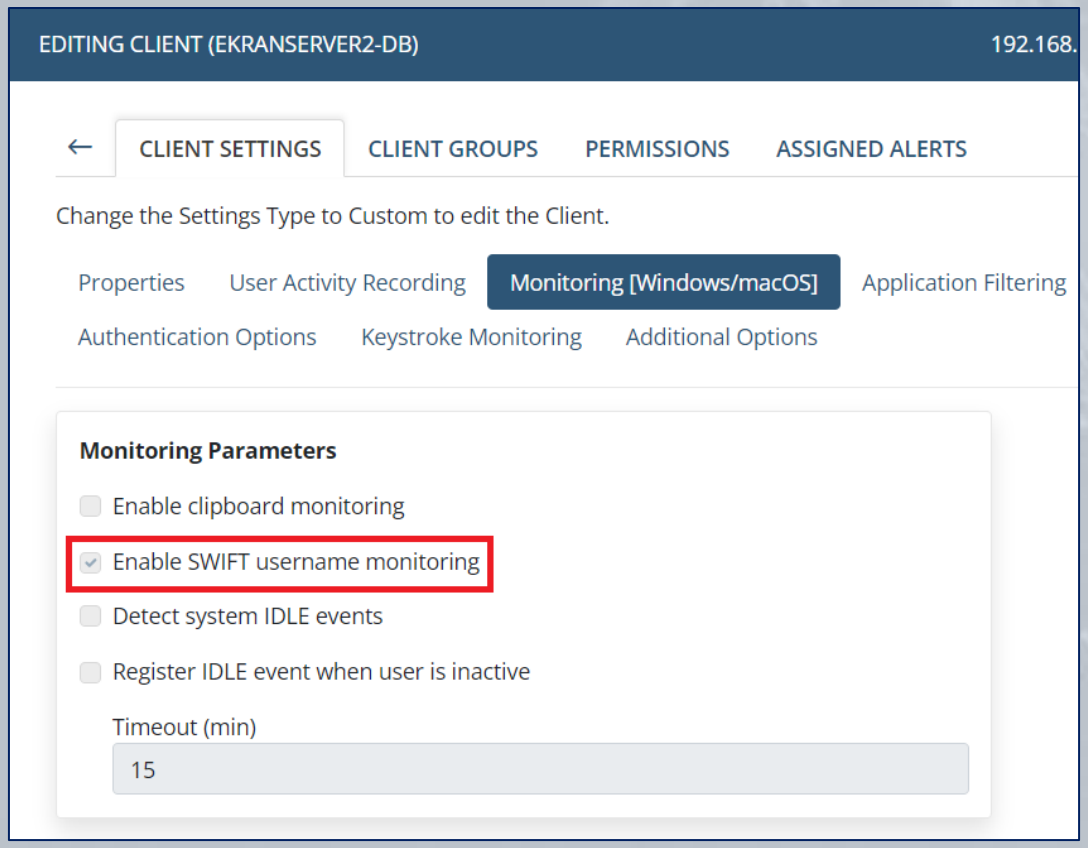
Remote Host IP Filtering

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



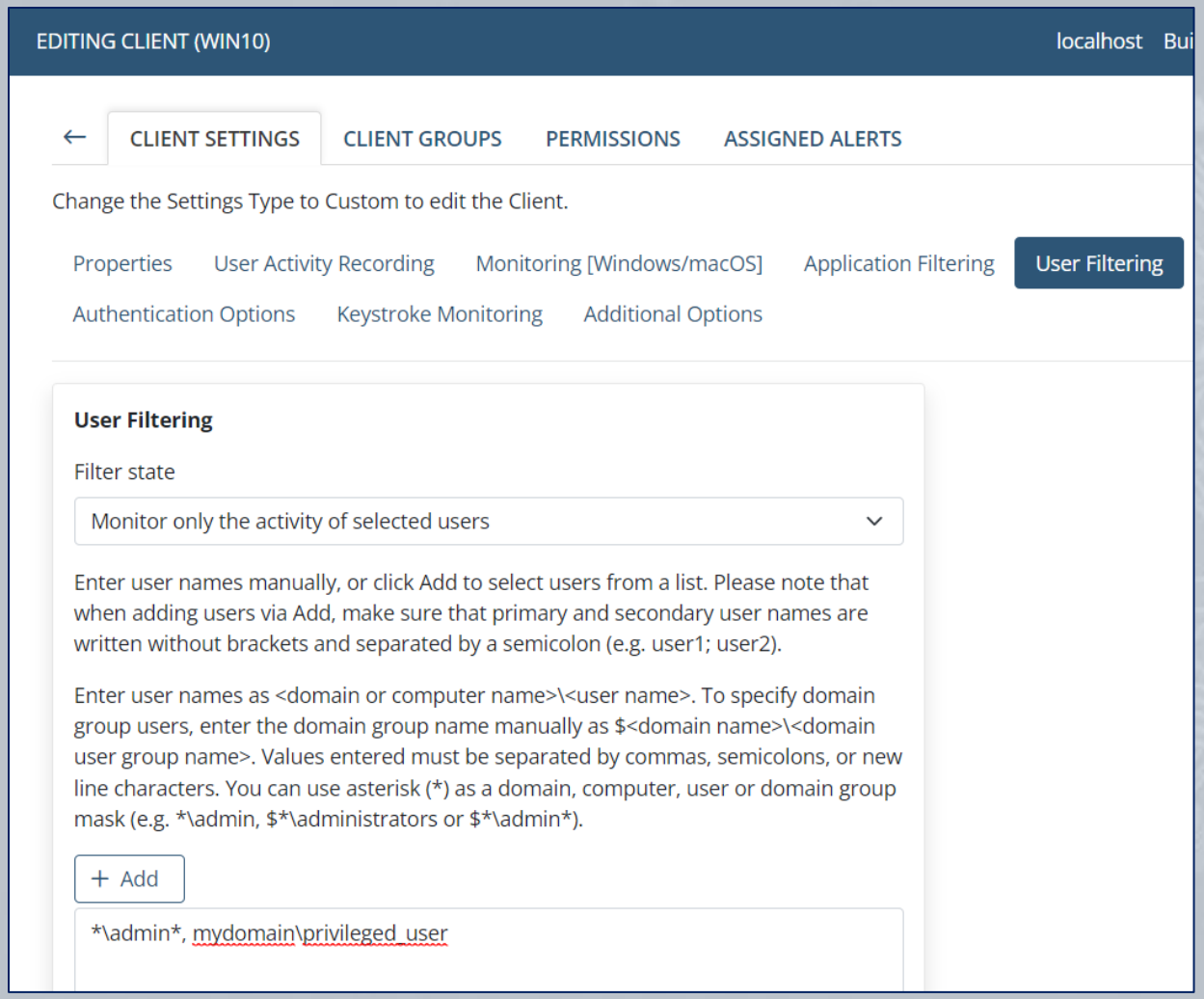
SWIFT Username Monitoring

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



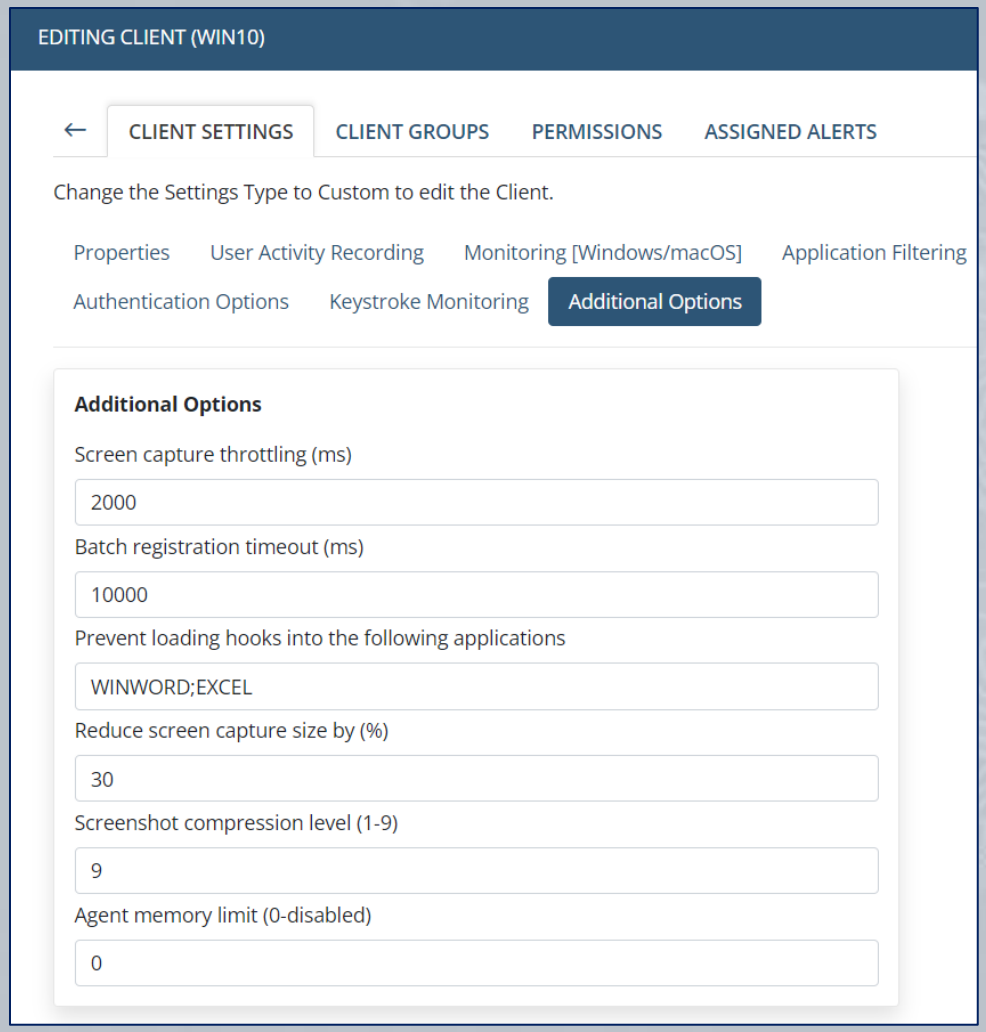
Privileged User Monitoring

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



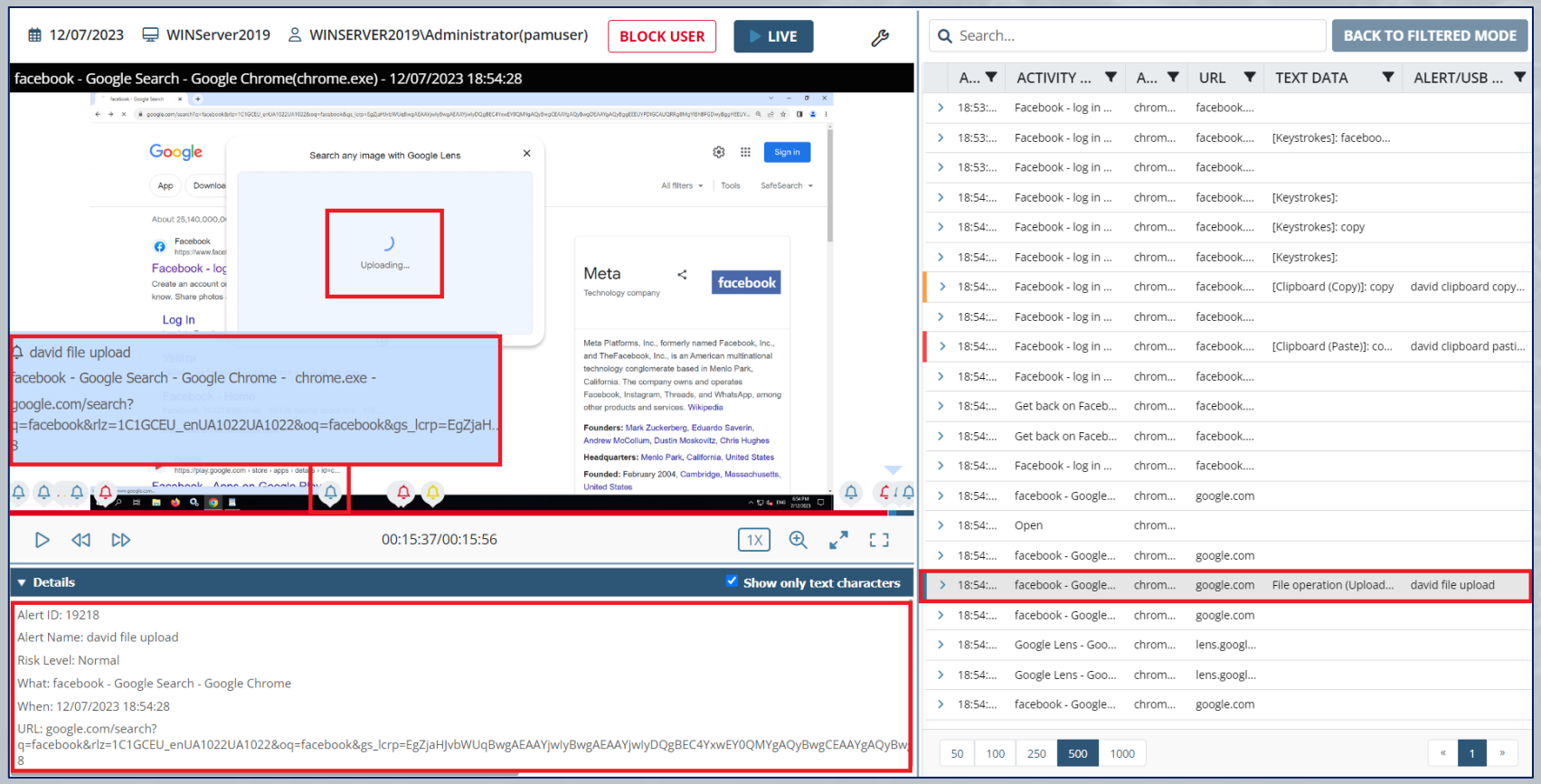
Bandwidth Usage Reduction

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.



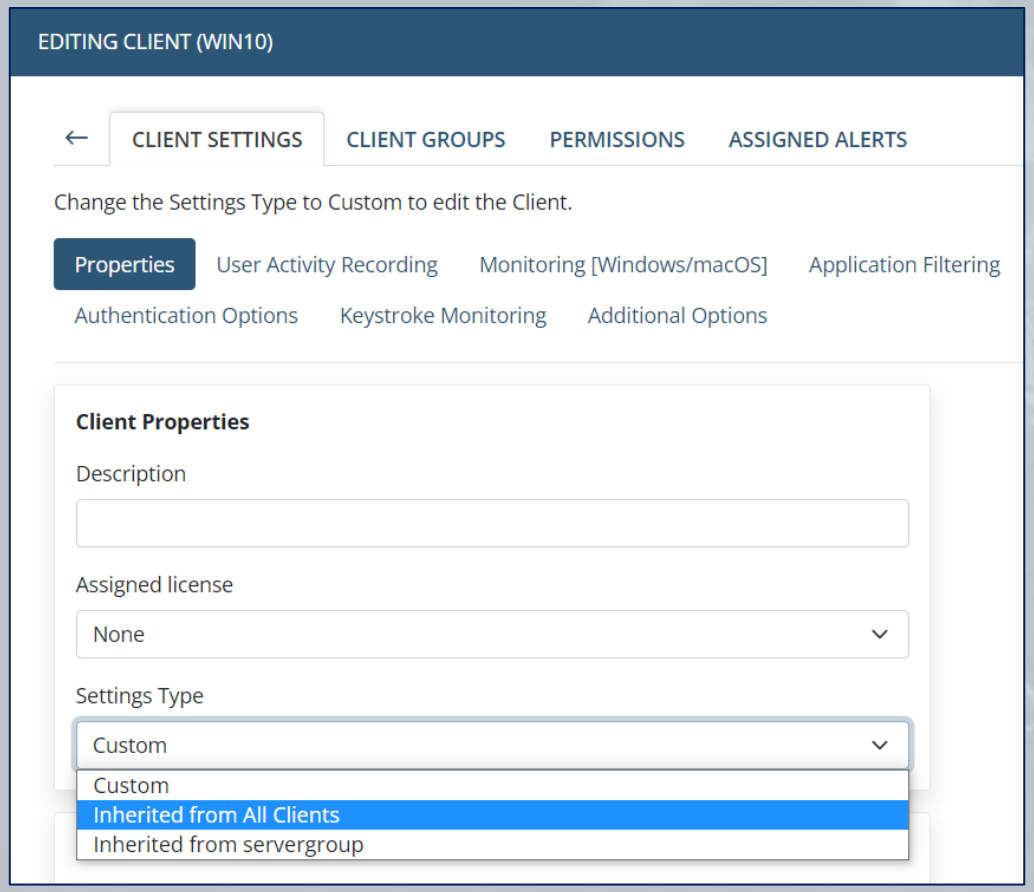
File Monitoring

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



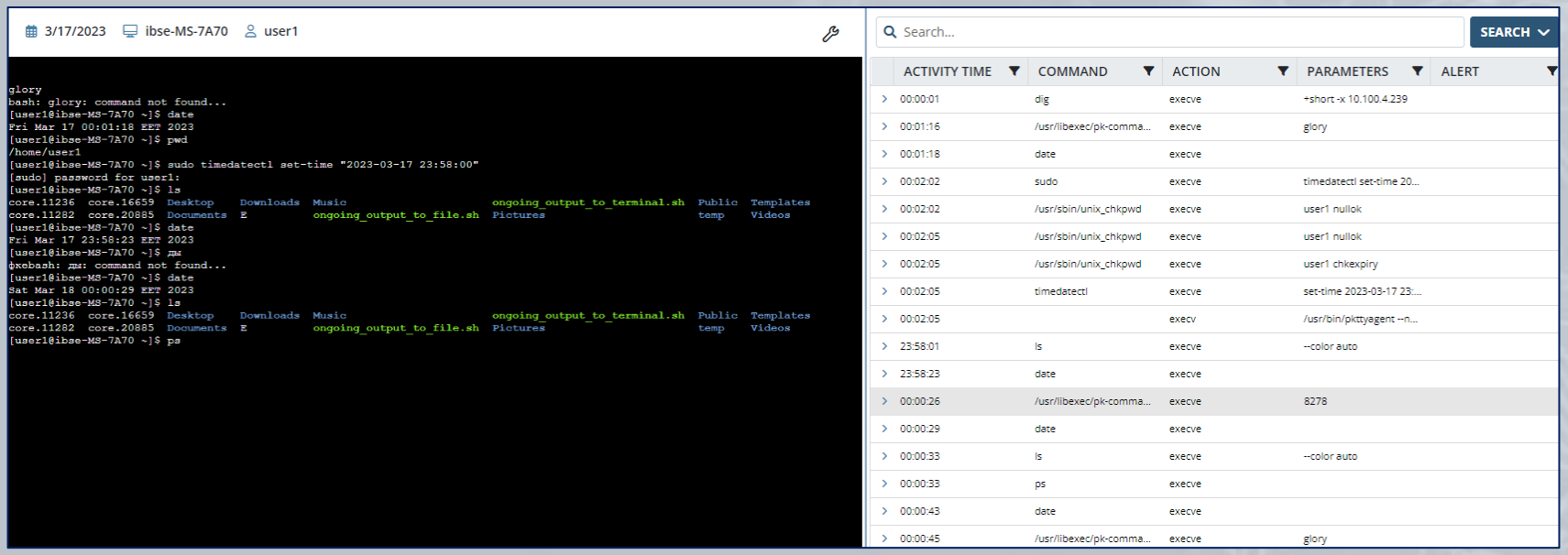
Client Group Settings

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



Monitoring Linux Clients

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.

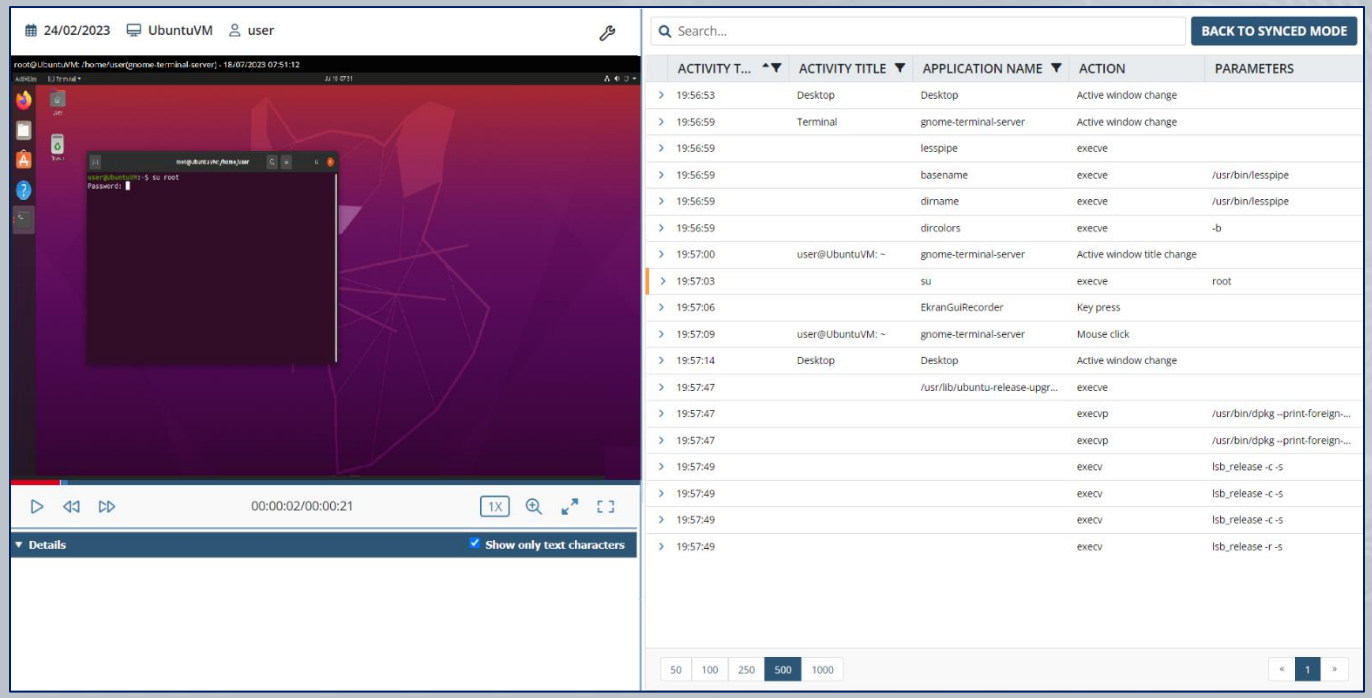


Monitoring of Linux **sessions started locally** via the GUI **(X Window System)** is also supported.

Monitoring Linux Clients (Local Sessions)

A **local Linux Client session** for **X Window System** includes:

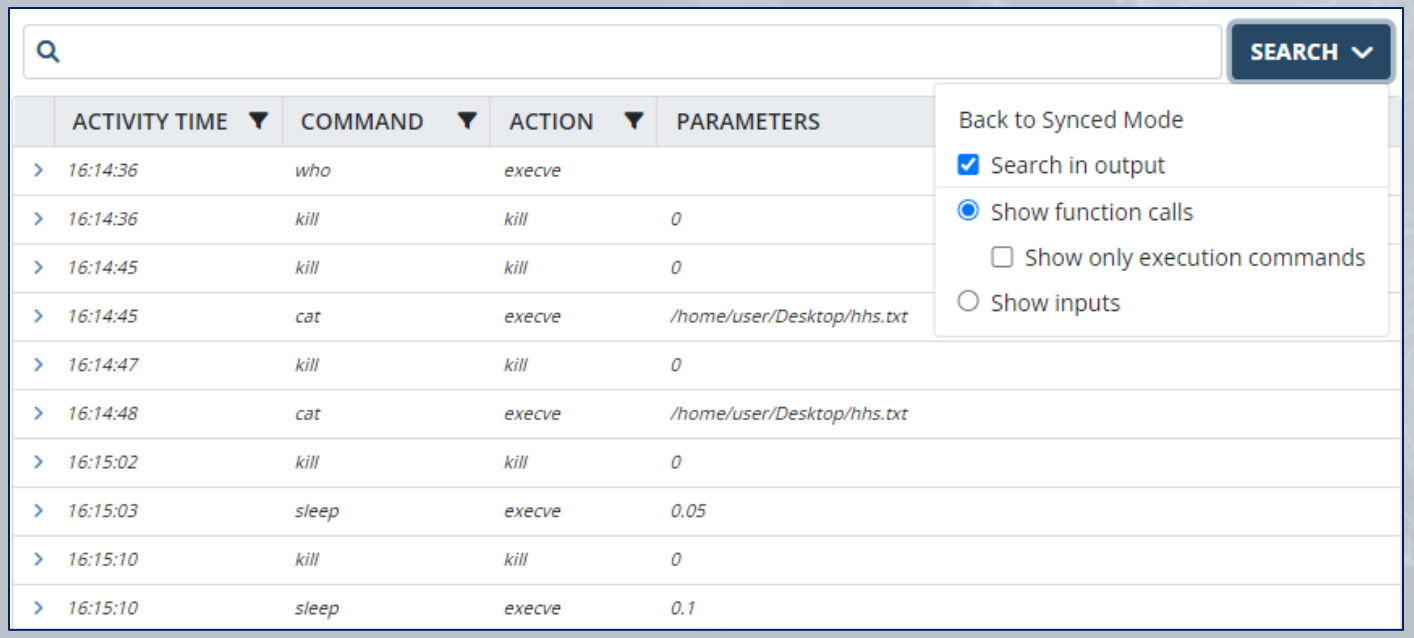
- Screen captures
- Activity times
- Activity titles
- Application names / Commands
- Actions / System function calls
- Parameters



Monitoring Linux Clients (Remote SSH Sessions)

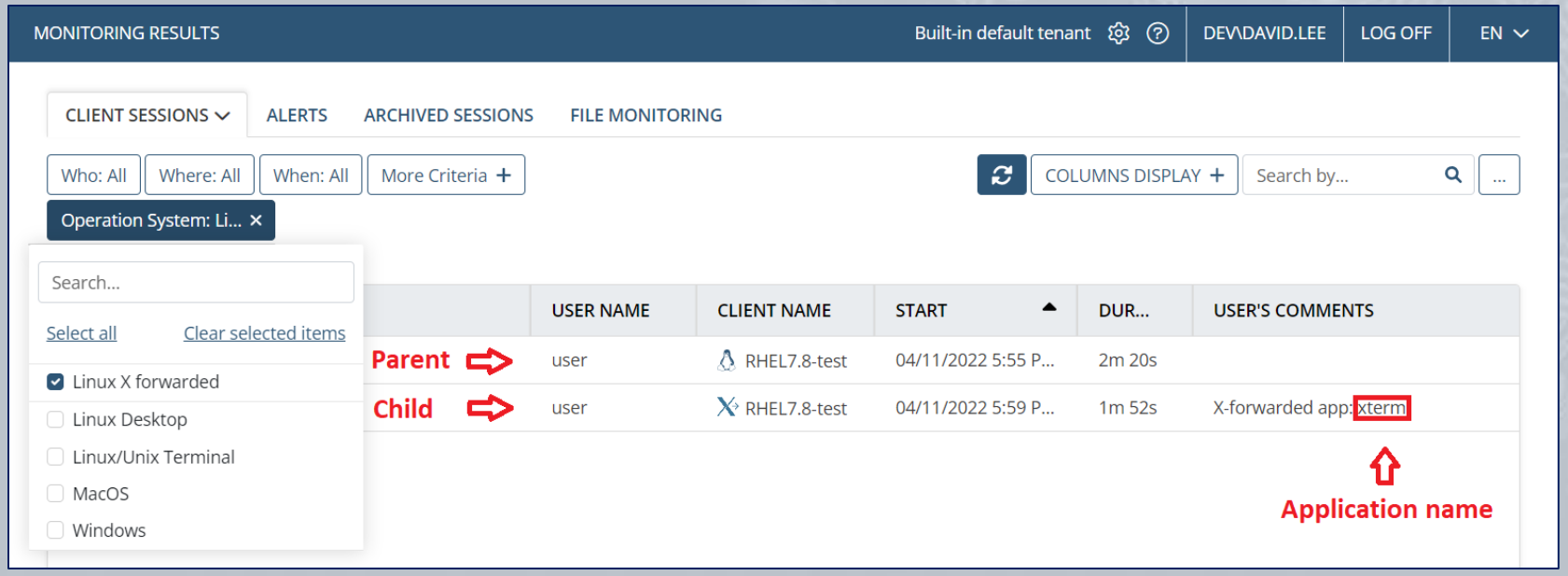
A **remote SSH Linux Client session** can be searched for:

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



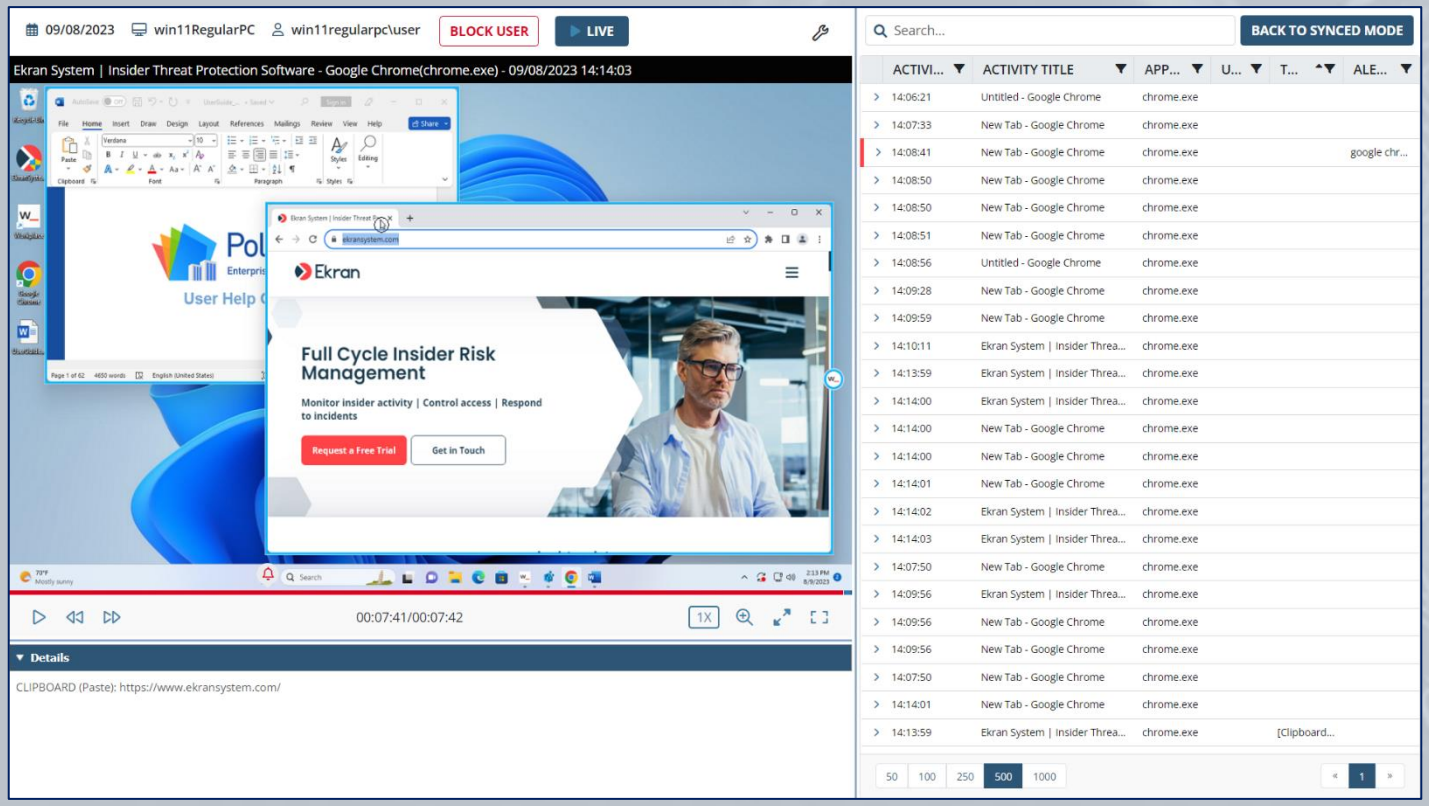
Monitoring Linux Clients (X-Forwarded Sessions)

- **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.



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**.



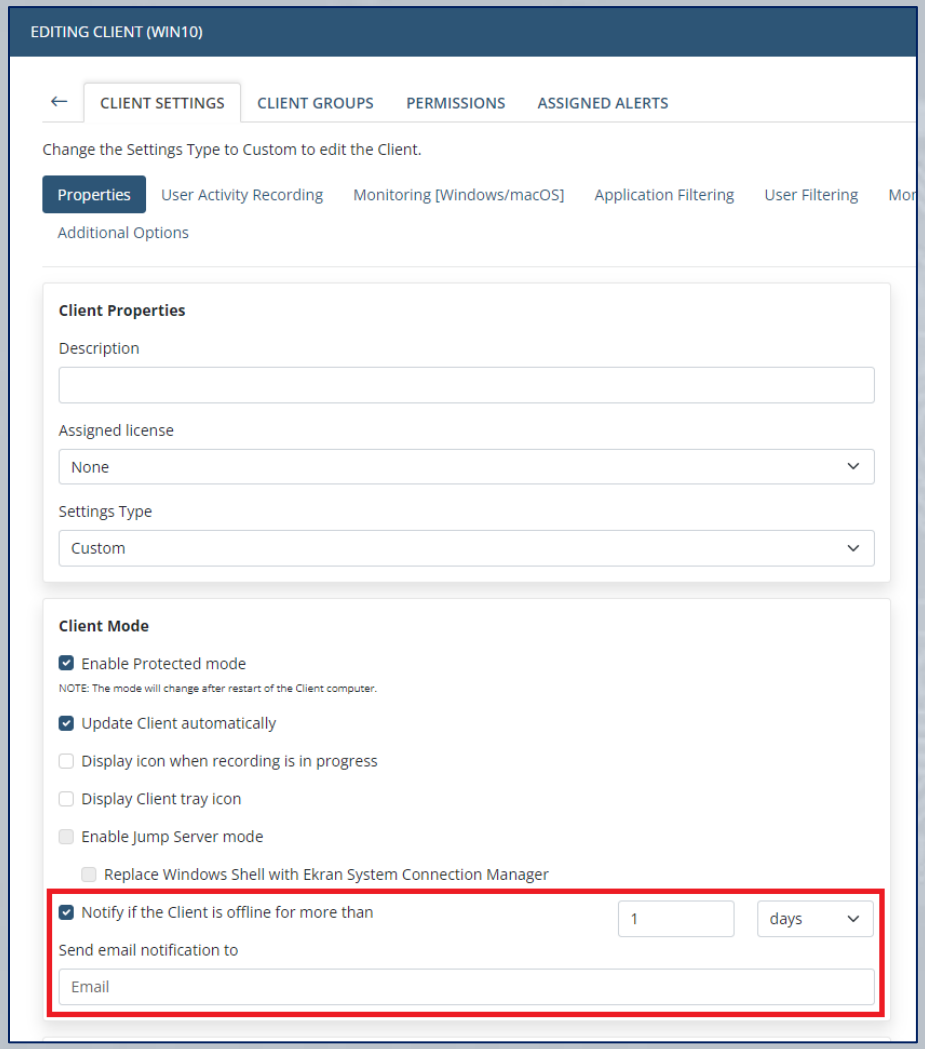
Detection of Disconnected Clients

Detection of Disconnected Clients

Ekran system

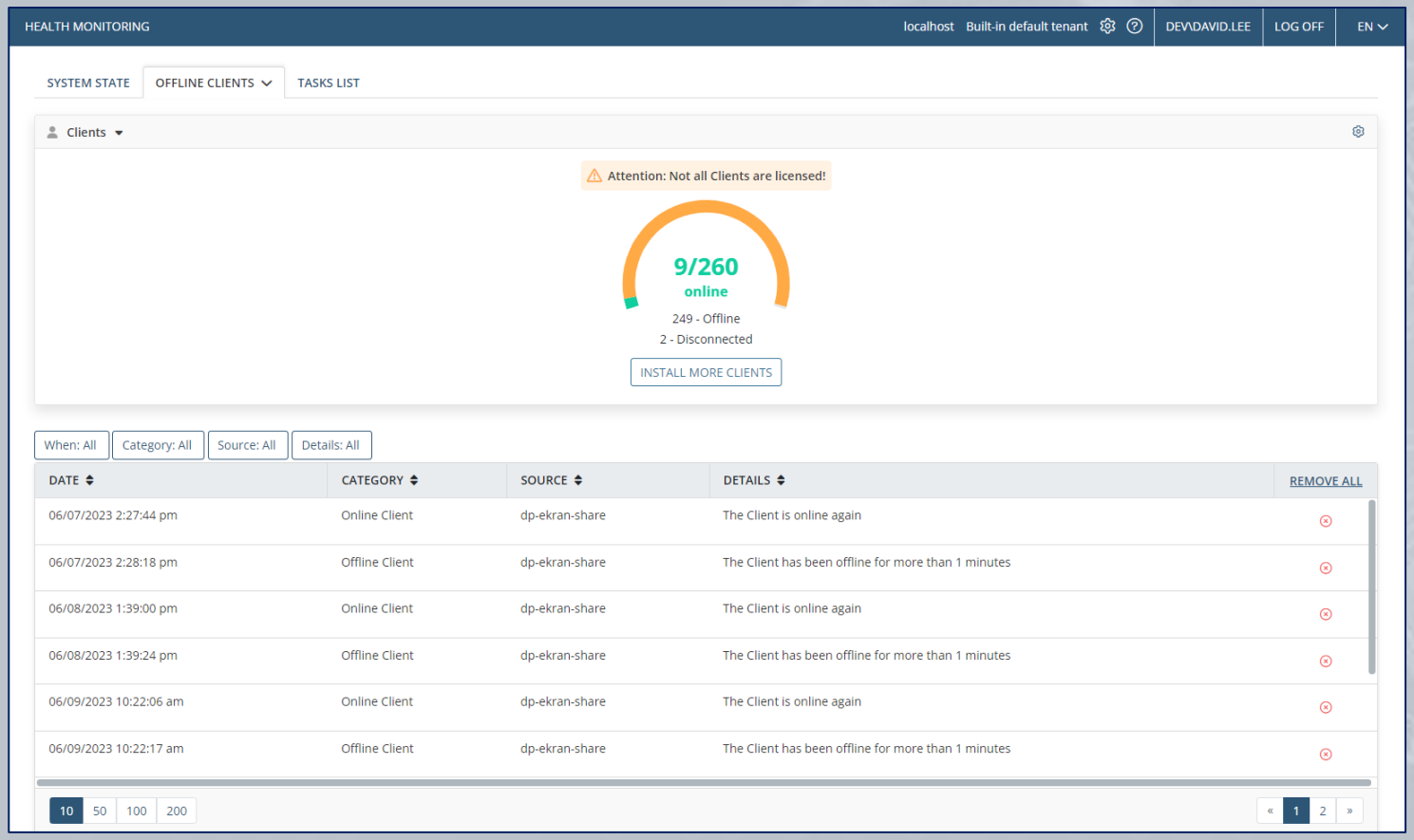
Detection of disconnected Clients will help you to timely detect Clients that have stopped transmitting monitoring data.

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



Viewing Disconnected Clients

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



Client Protection

Protected Mode

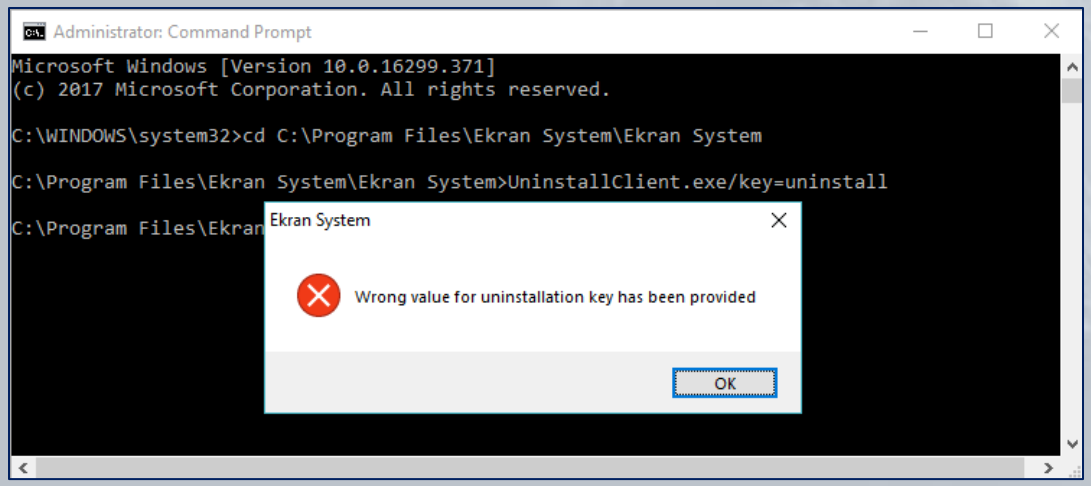
Ekran System allows you to **protect Windows Clients** and their **data** by enabling Protected mode.

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**.

Client Uninstallation

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



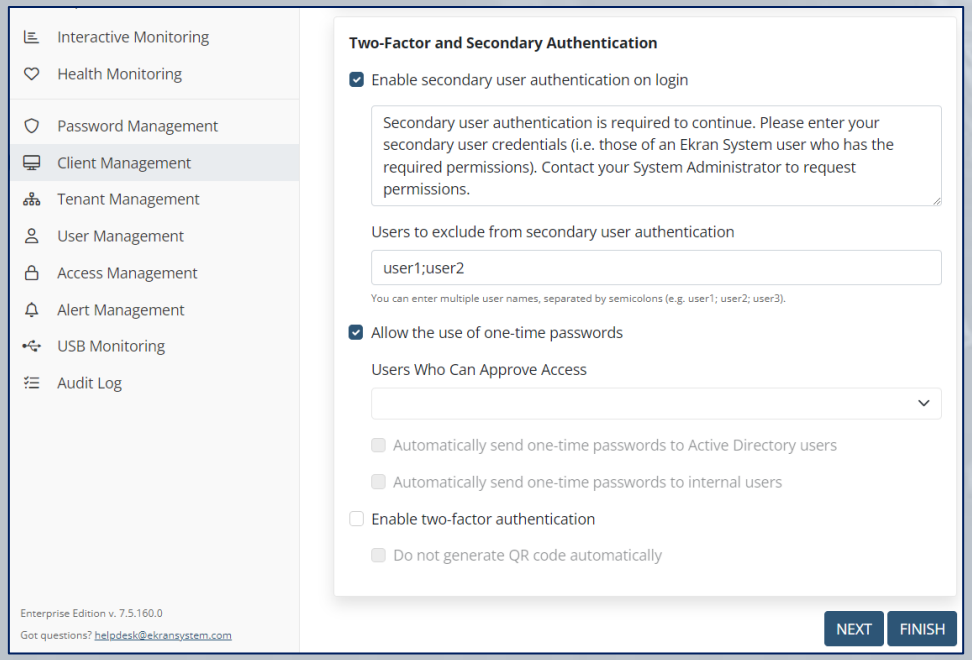
Only the **Ekran System administrator knows the Uninstallation key** defined prior to Client installation, and which is required for local removal.

Secondary User Authentication

Secondary User Authentication (Windows/Linux)

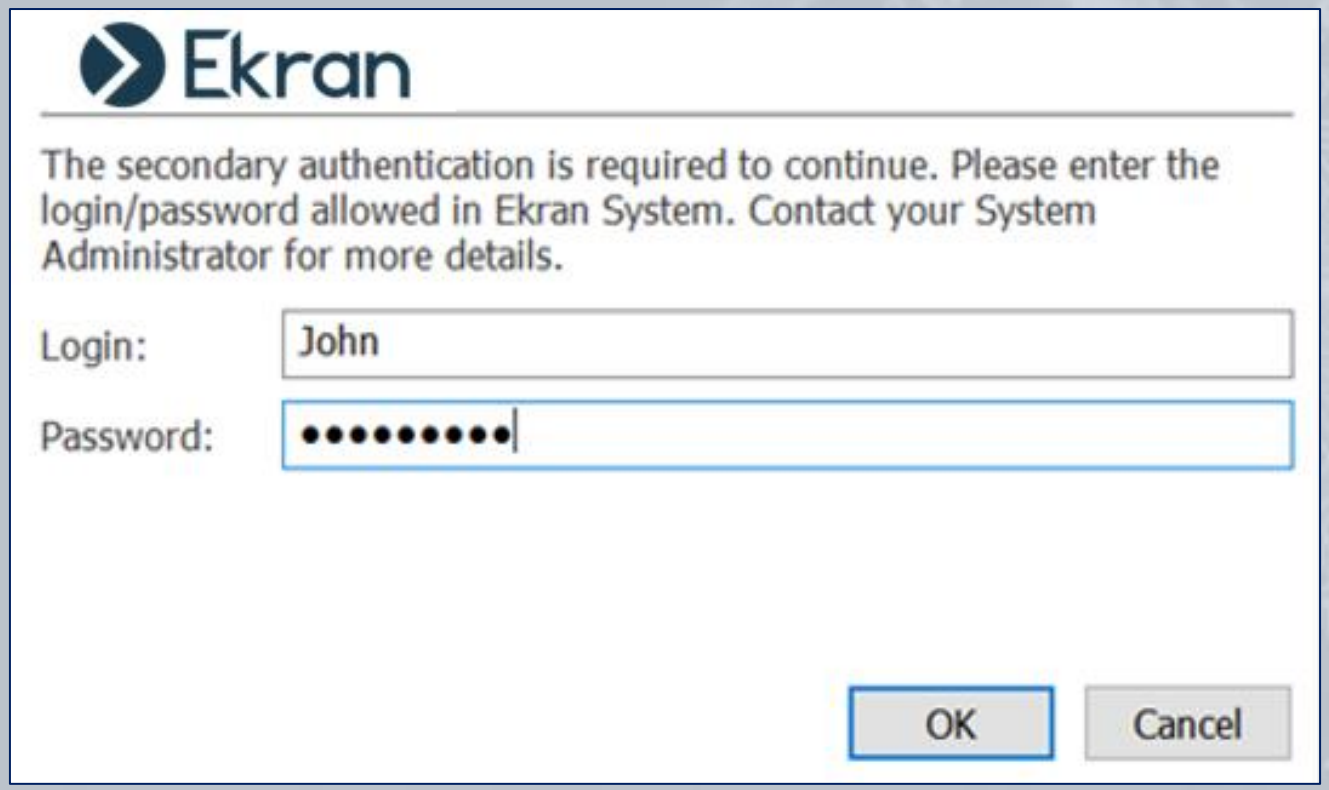
Secondary user authentication allows you to achieve two goals:

- 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**.



Secondary User Authentication (Windows)

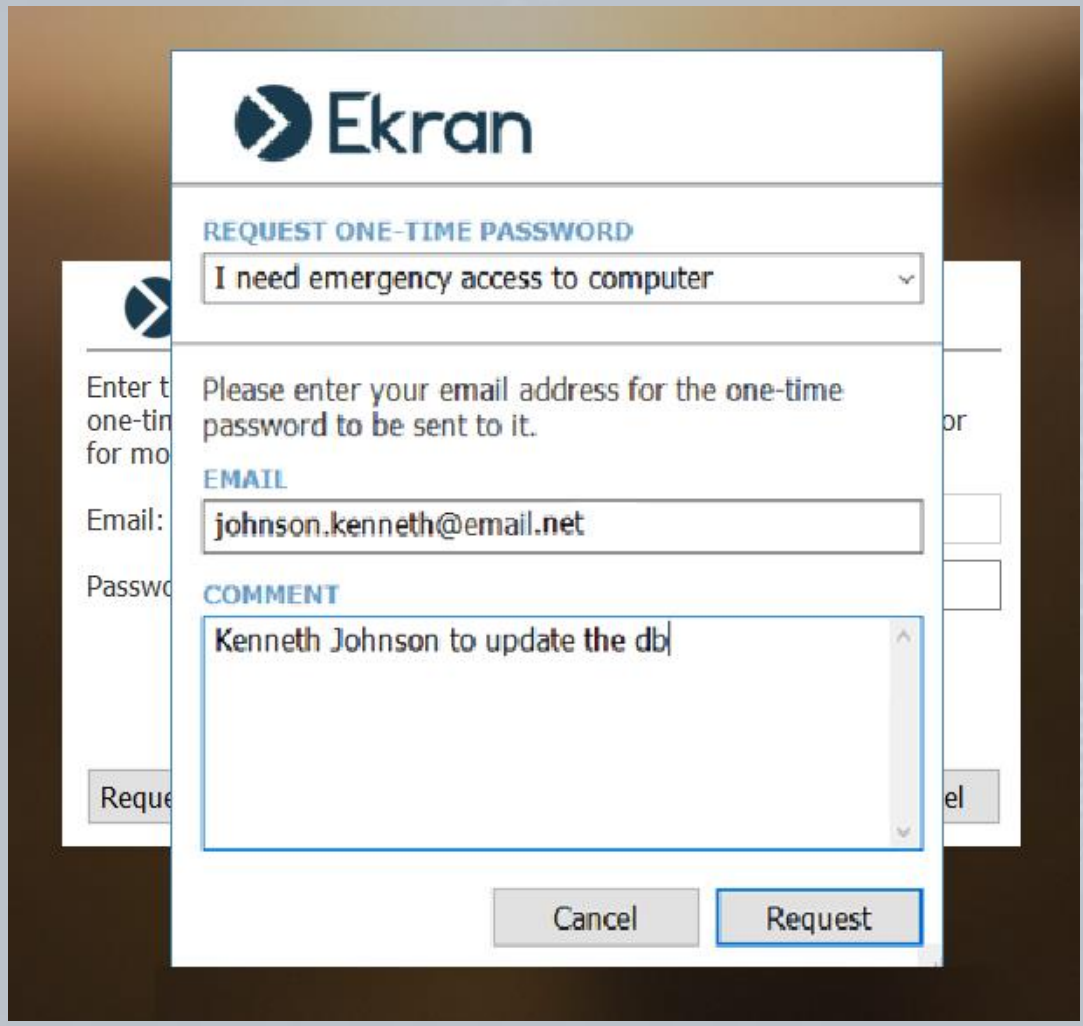
The Ekran System Client requests **credentials** to be entered **before** allowing a user to **access** the Windows OS.



One-Time Passwords (Windows Clients)

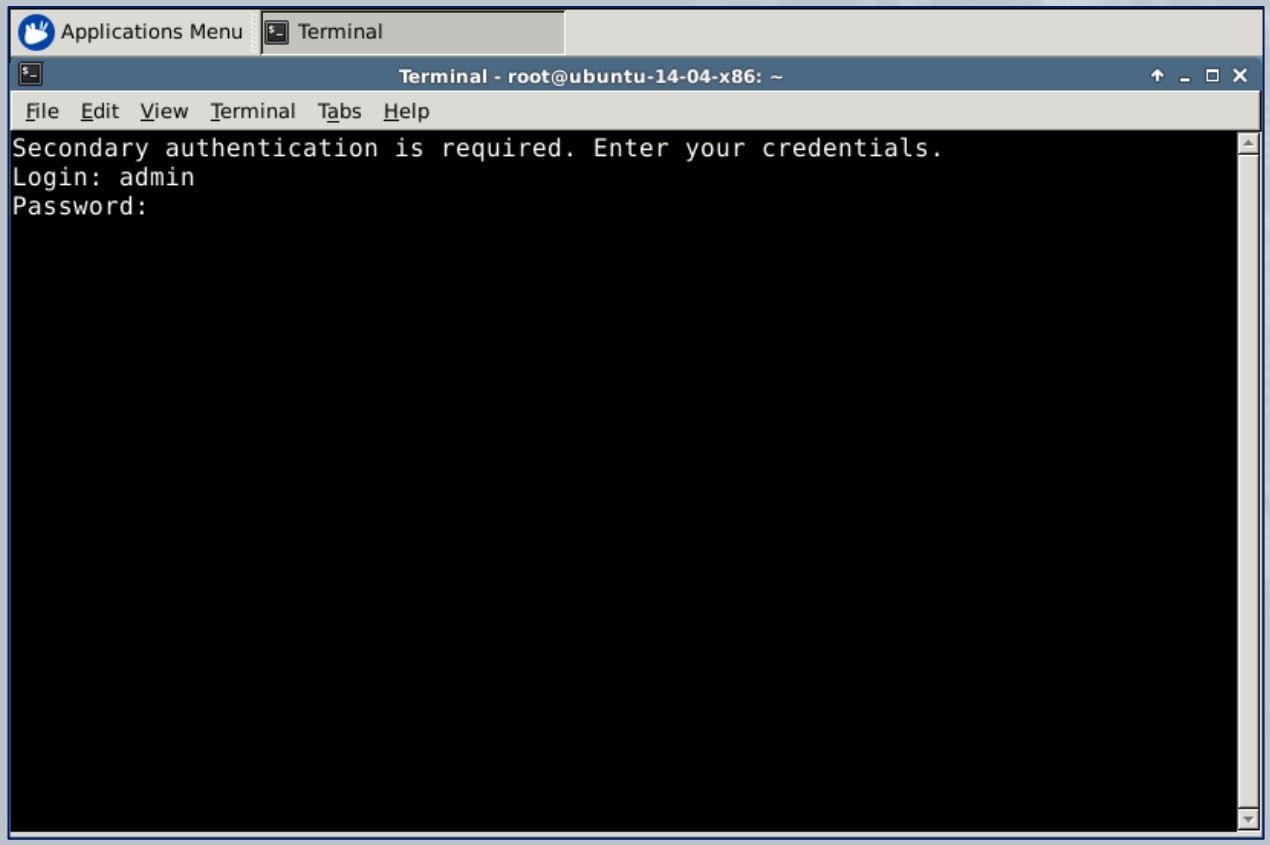
Ekran System Enterprise Edition provides the **administrator** with the unique **capability** to protect Client computers with one-time passwords.

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



Secondary User Authentication (Linux Clients)

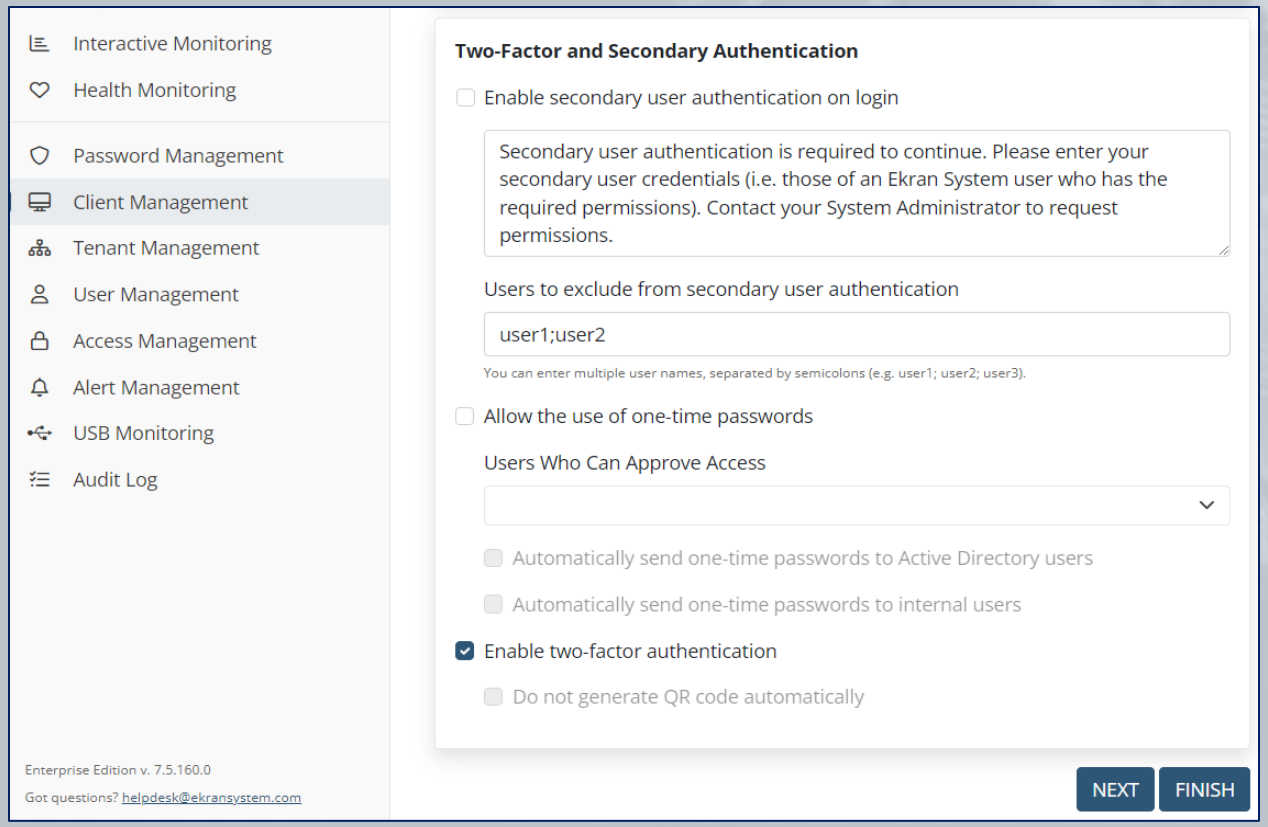
The Ekran System Client requests **credentials** to be entered to allow a user to **log on to the terminal** on **Linux** Client computers.



Two-Factor Authentication

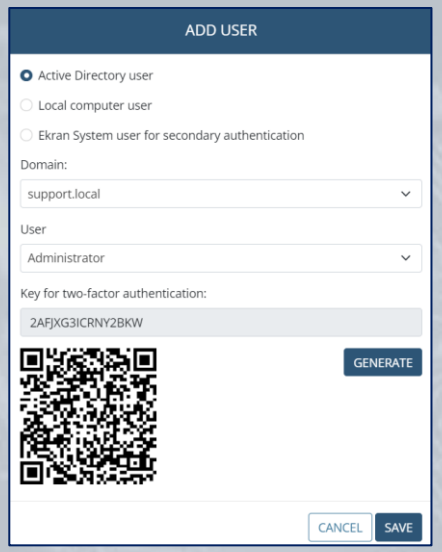
Two-Factor Authentication (Windows/Linux)

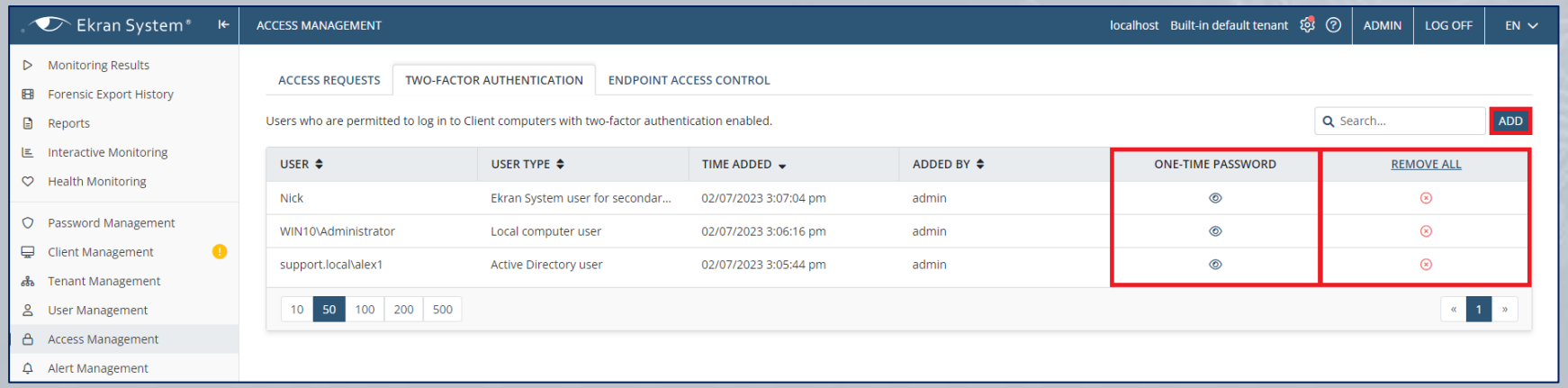
Two-factor authentication allows you to enable an **extra layer of security** to better protect the critical endpoints in your network.



Two-Factor Authentication (Windows/Linux)

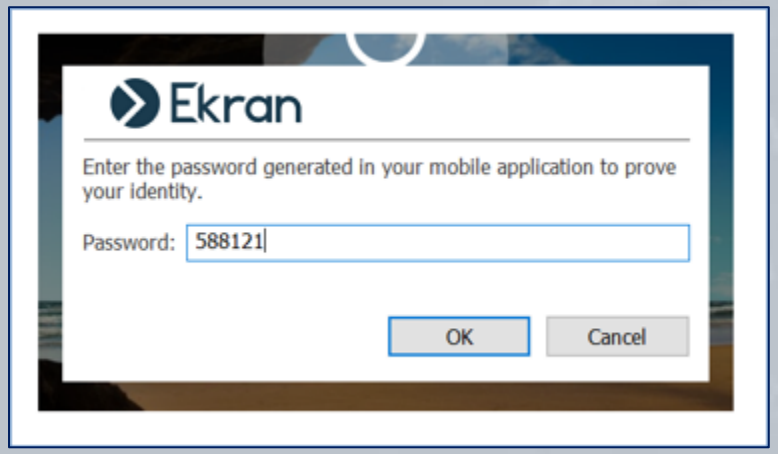
You can either enable this feature for all Windows Client computers, or manually add only users who you want to be allowed to log in to Windows and Linux Client computers, using **time-based one-time passwords** (TOTP) generated by way of a mobile authenticator application.





Two-Factor Authentication (Windows/Linux)

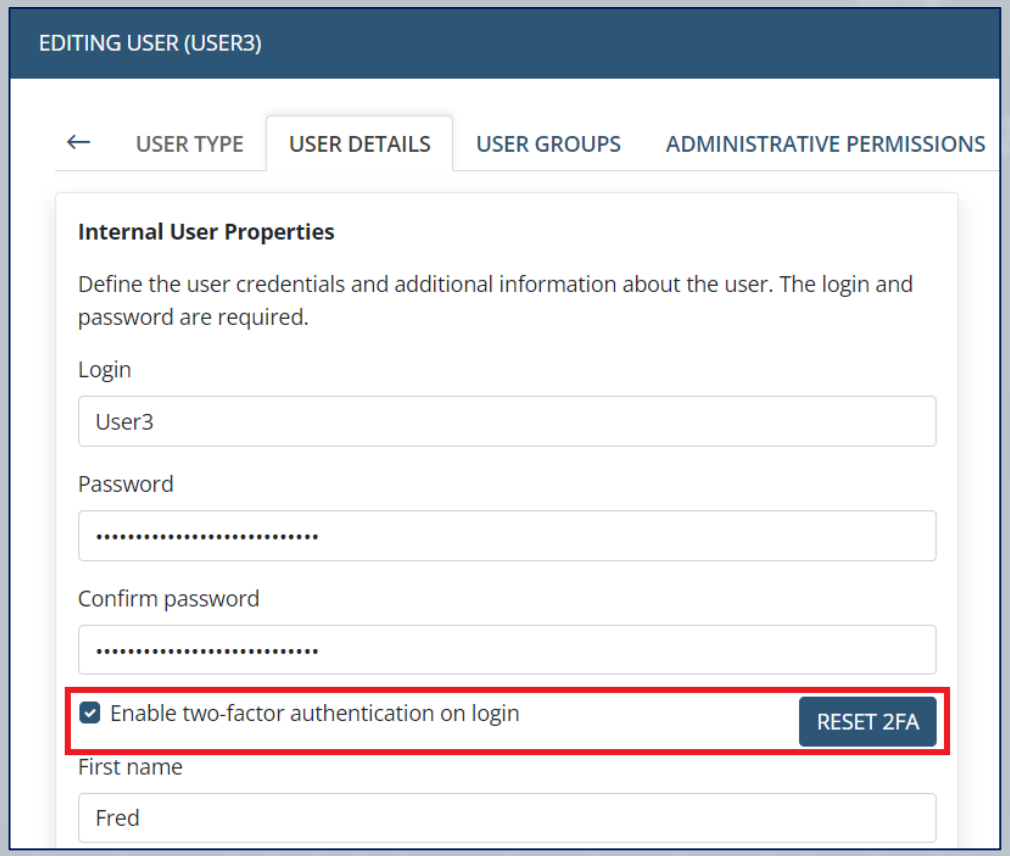
The Ekran System Client **prompts the user to enter a TOTP** to access the system.

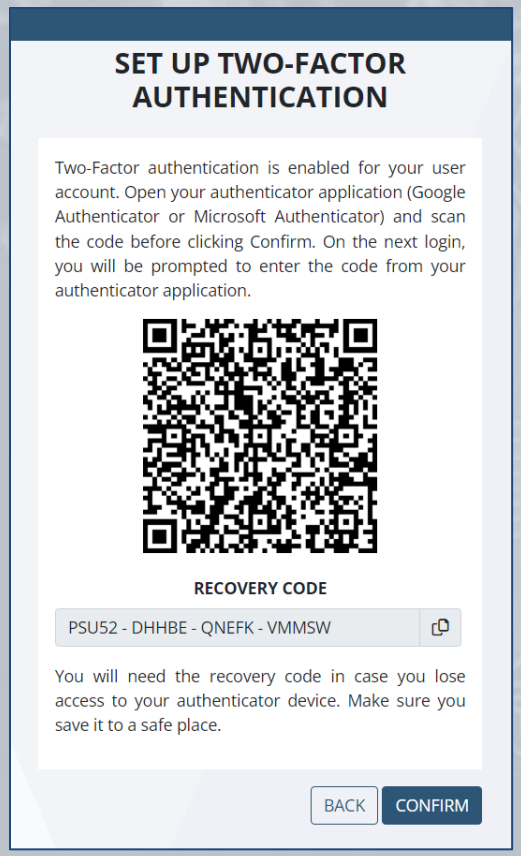



```
Ubuntu 16.04.2 LTS ubuntu tty2

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**.





Password Management (Privileged Access Management)

Password Management

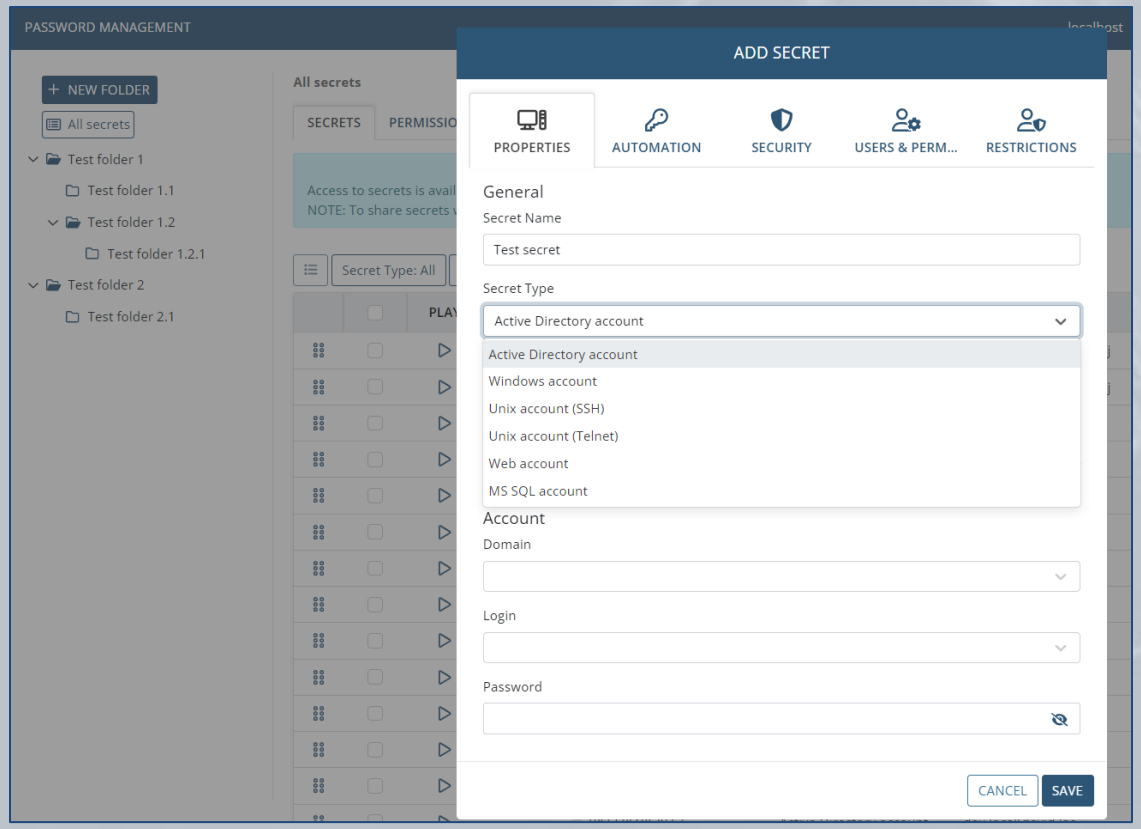
Managing privileged accounts (PAM) and implementing role-based access control is critical for enterprise security teams. Ekran System's **Password Management** functionality uses secrets to provide you with full control and visibility over privileged user access.

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**.

Adding a Secret

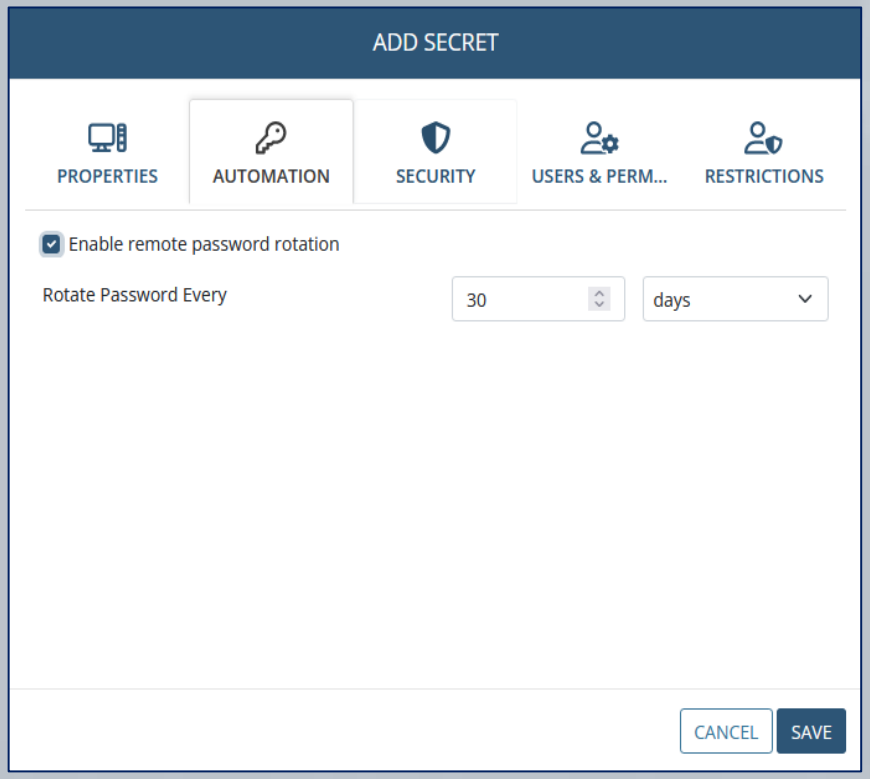
Add a secret and define: an **endpoint** to connect to, privileged account **credentials**, and **users / user groups** to give access to.

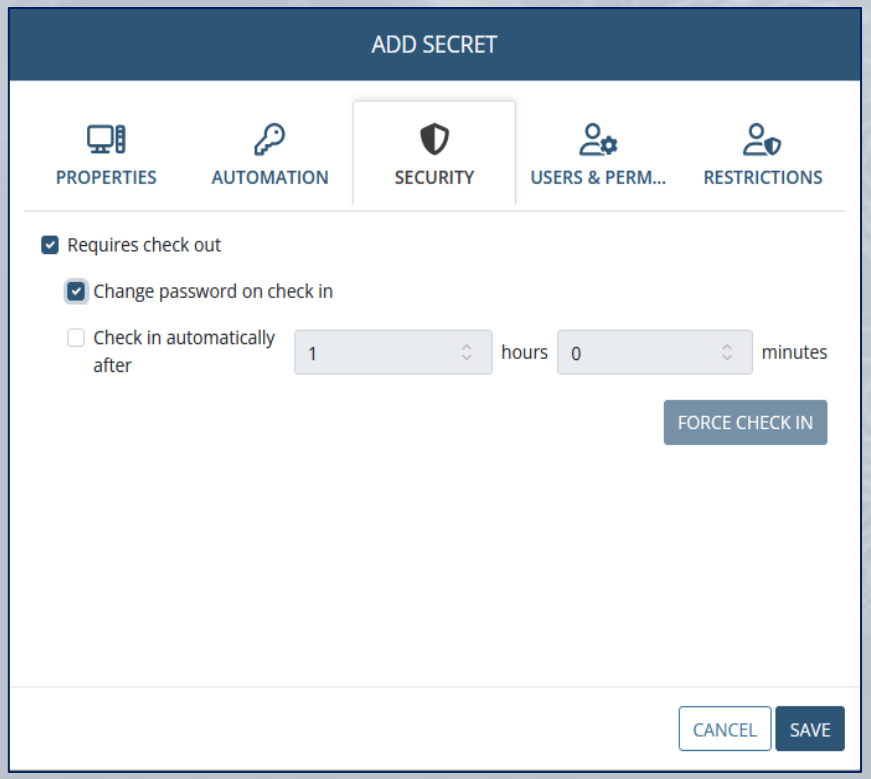


Adding a Secret (Enhanced Security Options)

To enhance security further, optionally:

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

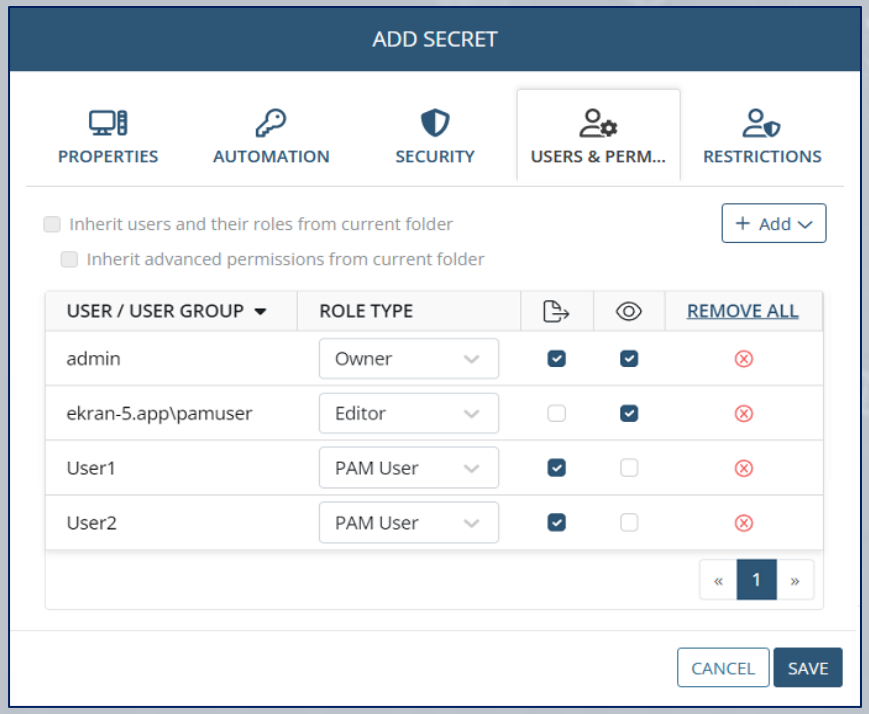




Adding a Secret (Assigning Users & Permissions)

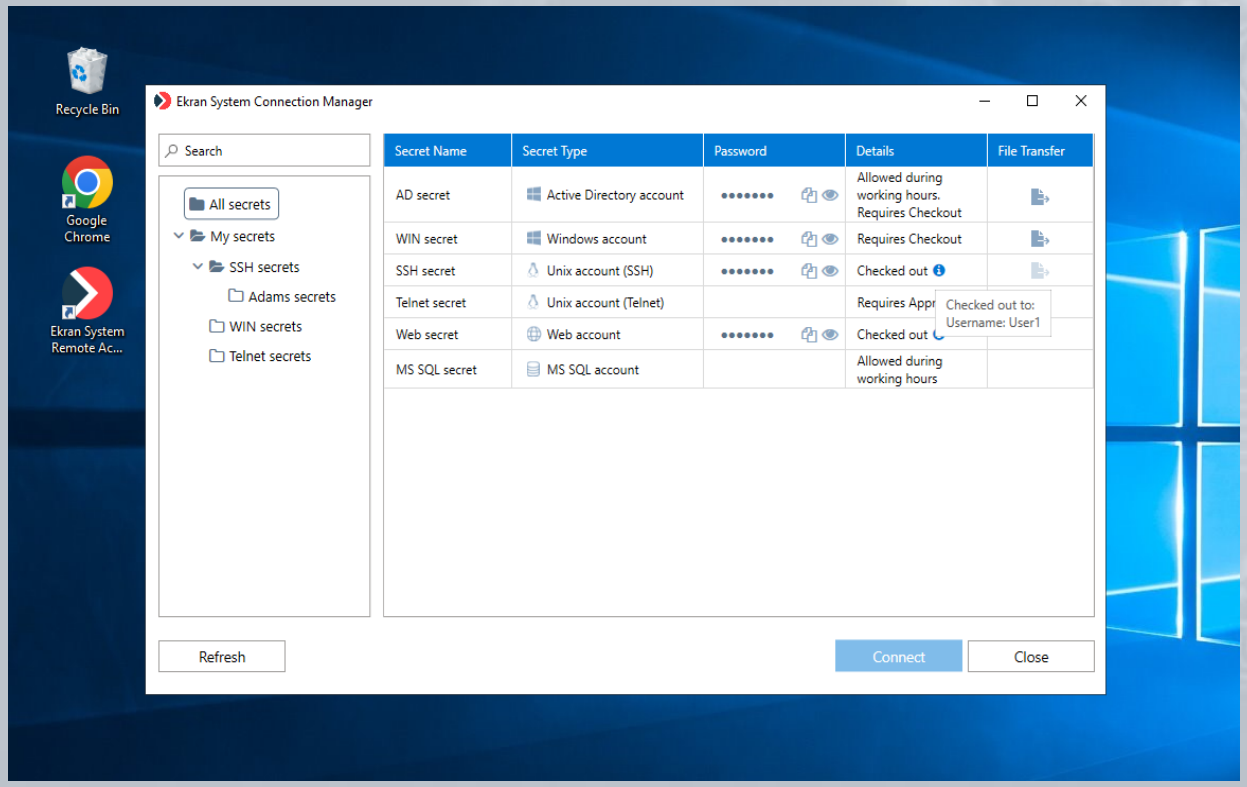
To define users' access to a secret:

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



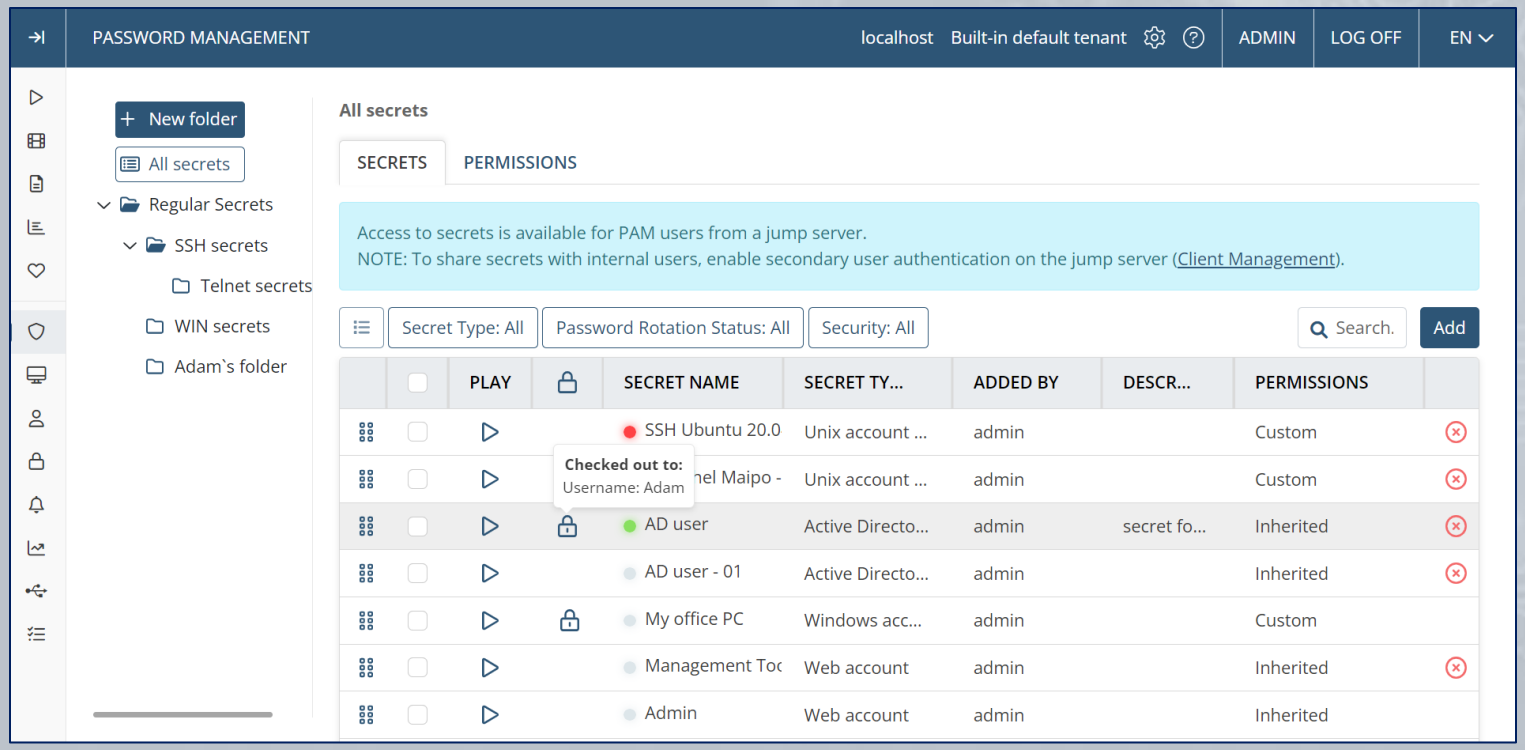
Using a Secret

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.



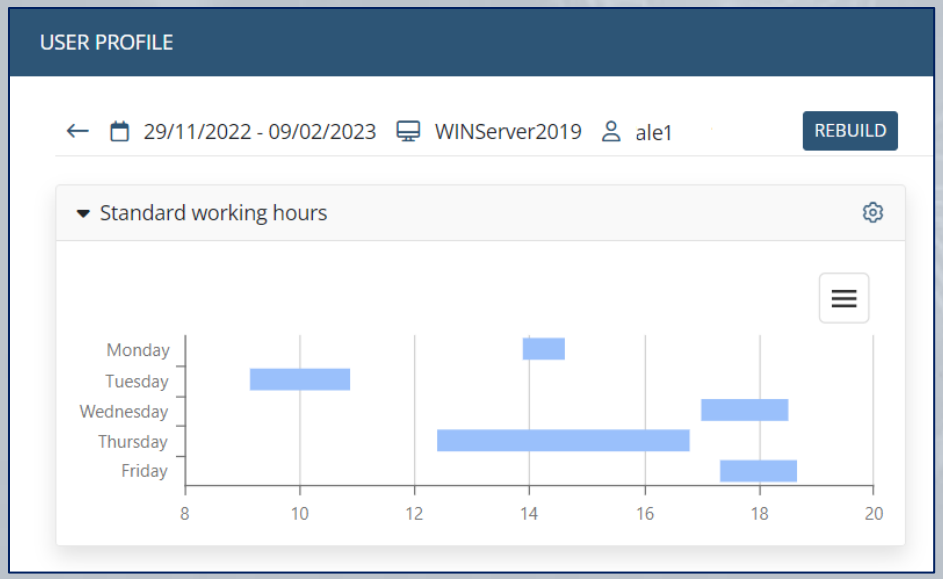
User and Entity Behavior Analytics (UEBA)

User and Entity Behavior Analytics

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

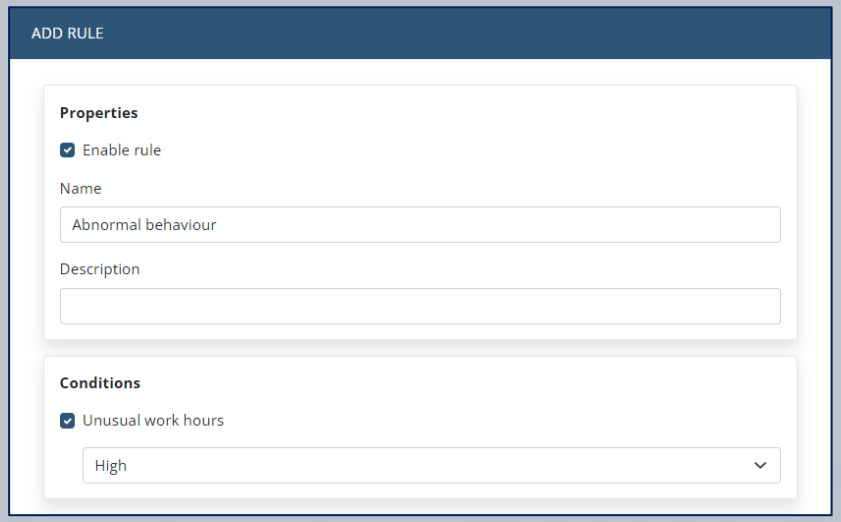
UEBA has the following advantages for detecting suspicious activities:

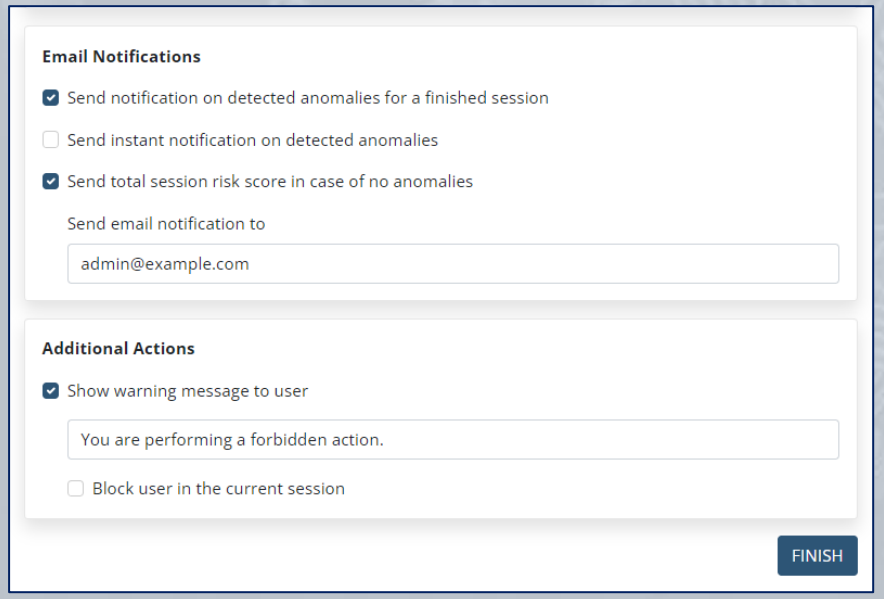
- **Analysis** of user **behavior patterns** and establishment of a baseline for **normal behavior**.
- Automatic **detection** of behavioral **anomalies** & **deviations**.
- Timely **notification** of potential **insider threats**.



User and Entity Behavior Analytics

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

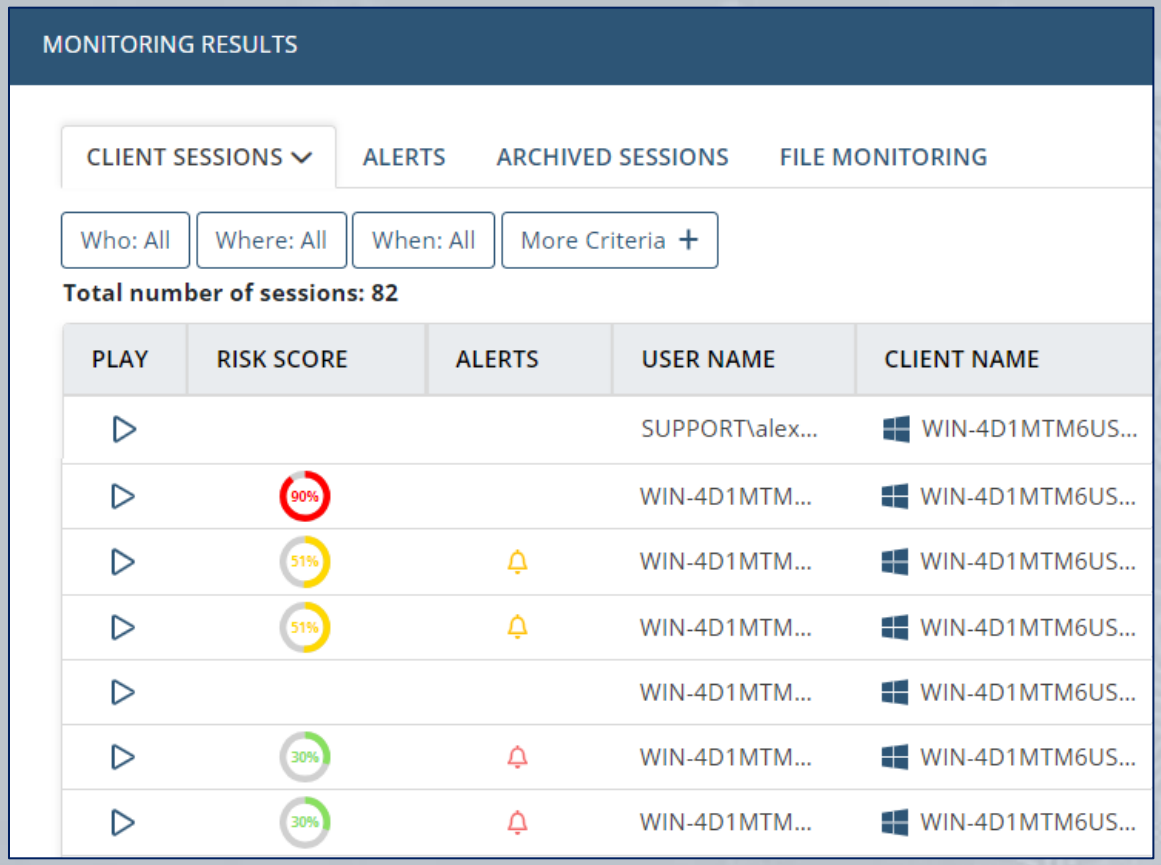




User and Entity Behavior Analytics

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

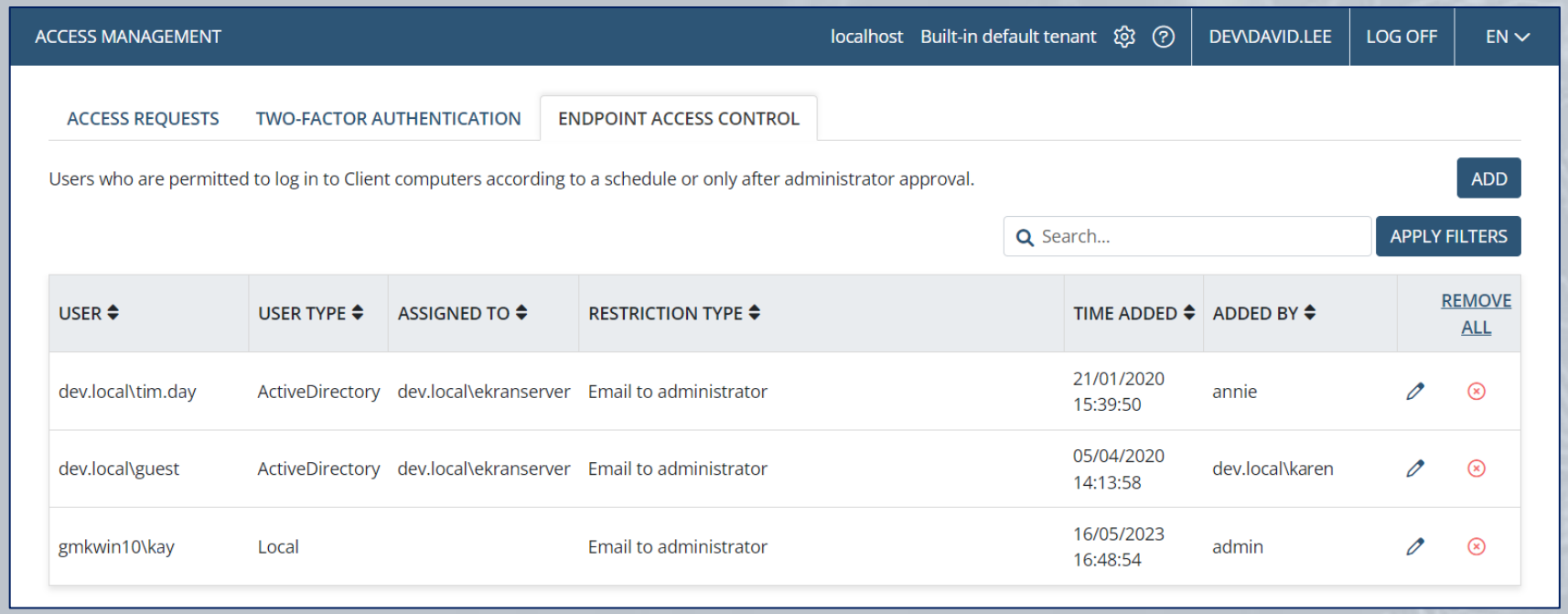
The **risk score** indicates the **severity level** of the session and is calculated according to the risk level of the abnormal user behavior **patterns and alerts** detected in the monitored sessions.



Administrator Approval on Login

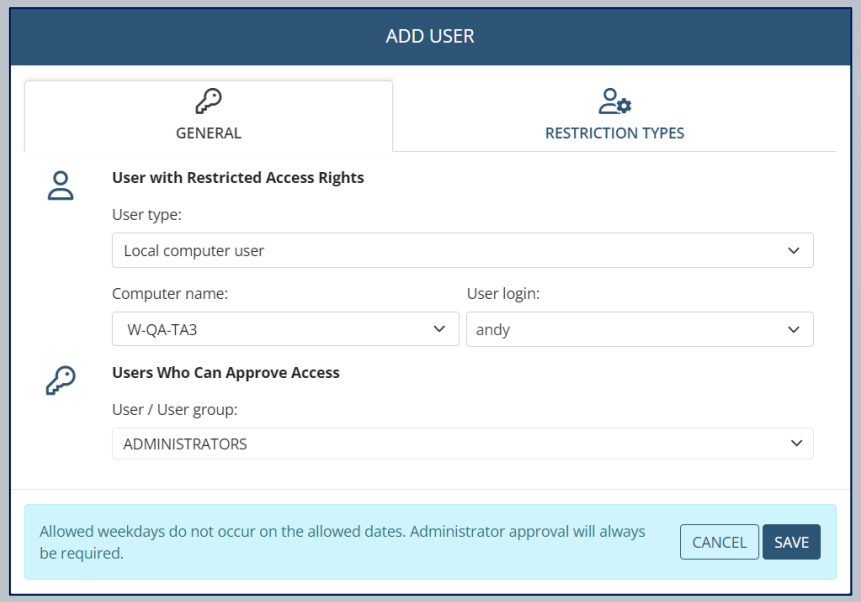
Administrator Approval on Login

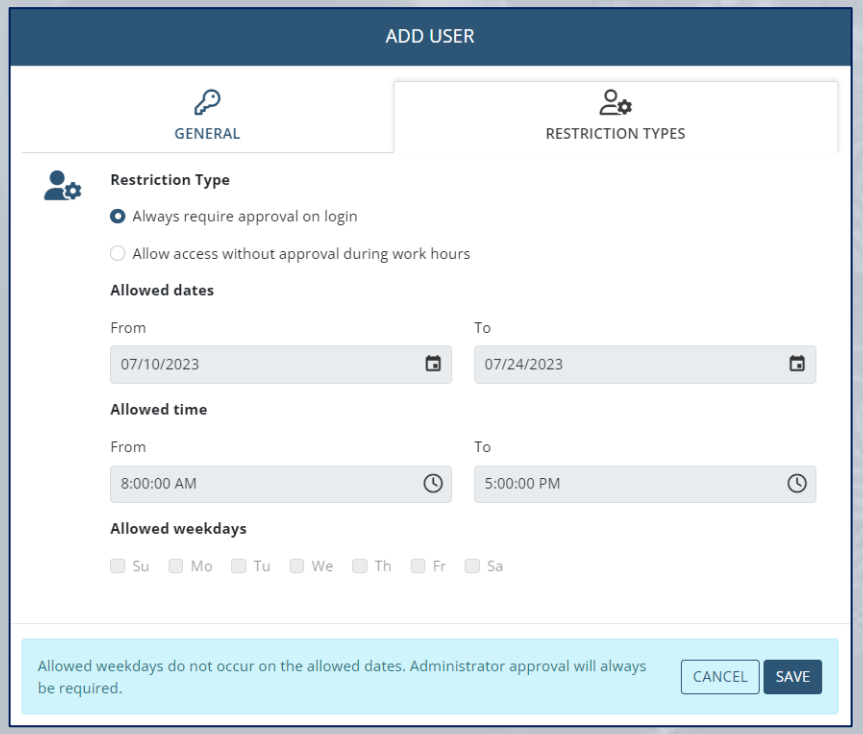
Approval by an administrator on login allows you to better **protect** the Client computers in your network against **undesired access**.



Administrator Approval on Login

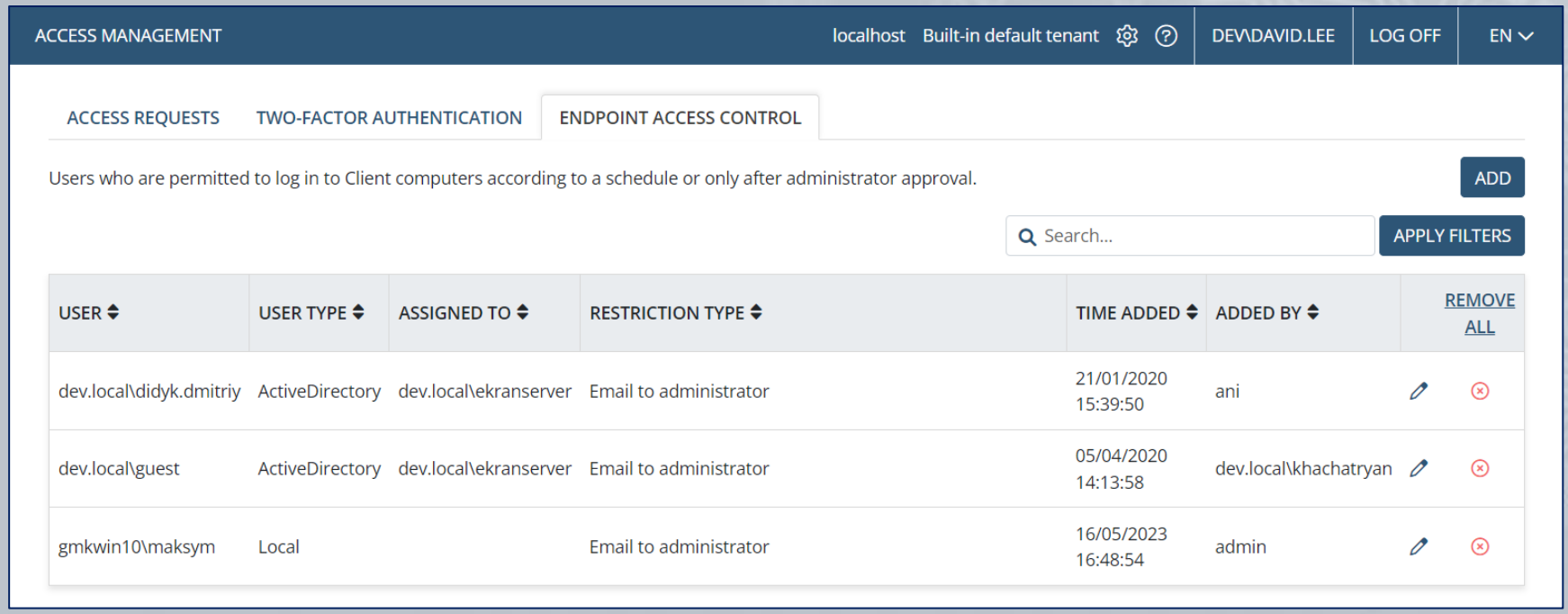
You can **add users** whose **access** to Client computers needs to be **restricted**.





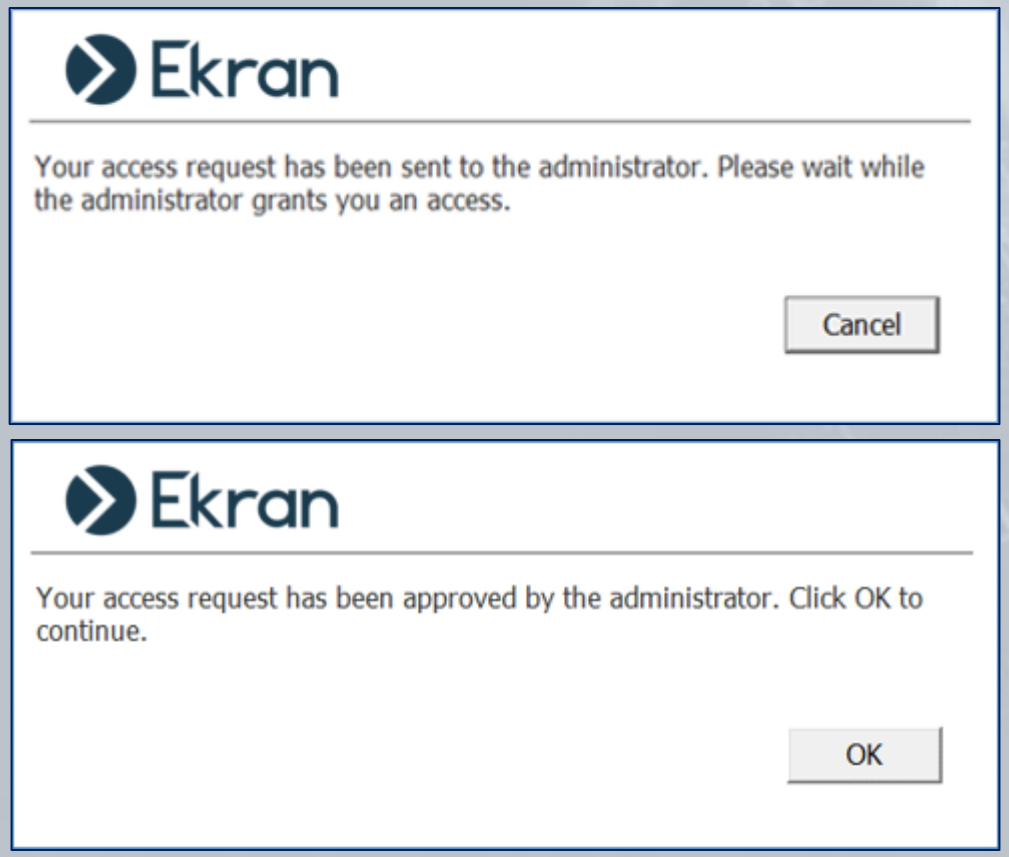
Administrator Approval on Login

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.



Administrator Approval on Login

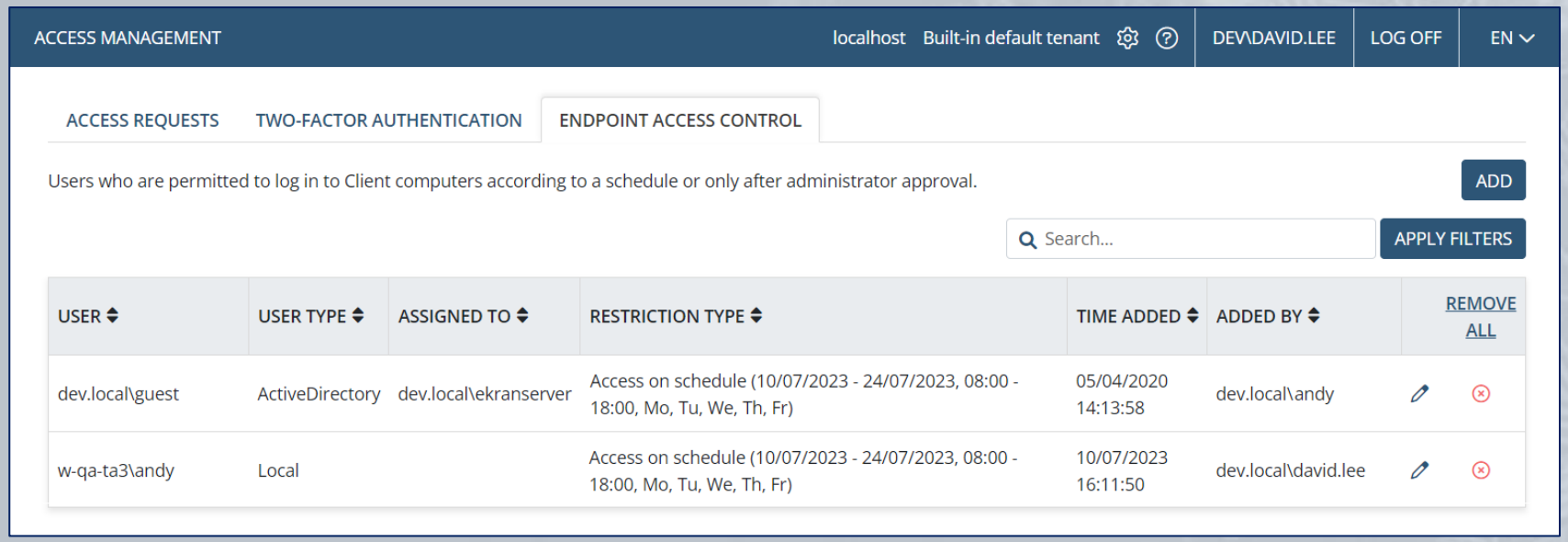
Only after the **trusted user approves** the user's **access request**, is the user allowed to access the system.



Access Request and Approval Workflow

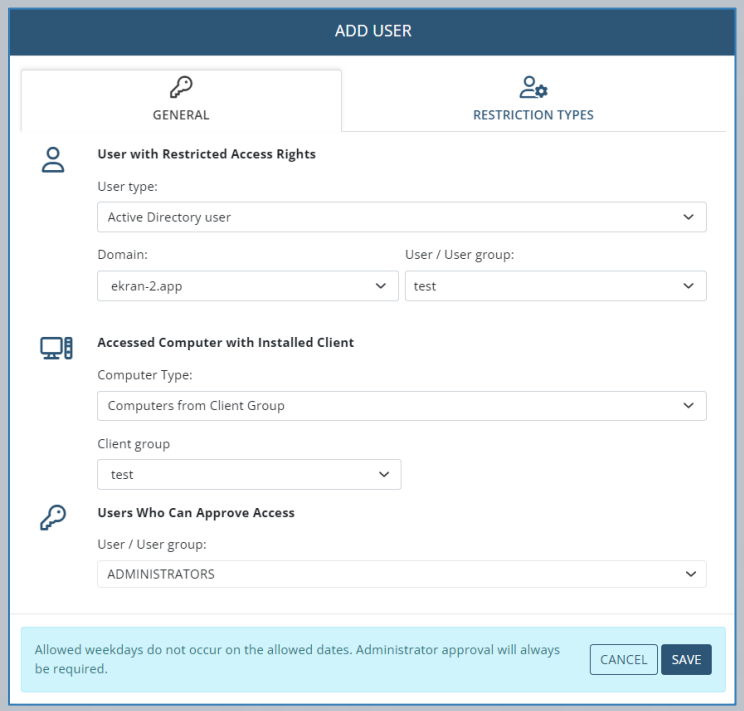
Access Request and Approval Workflow

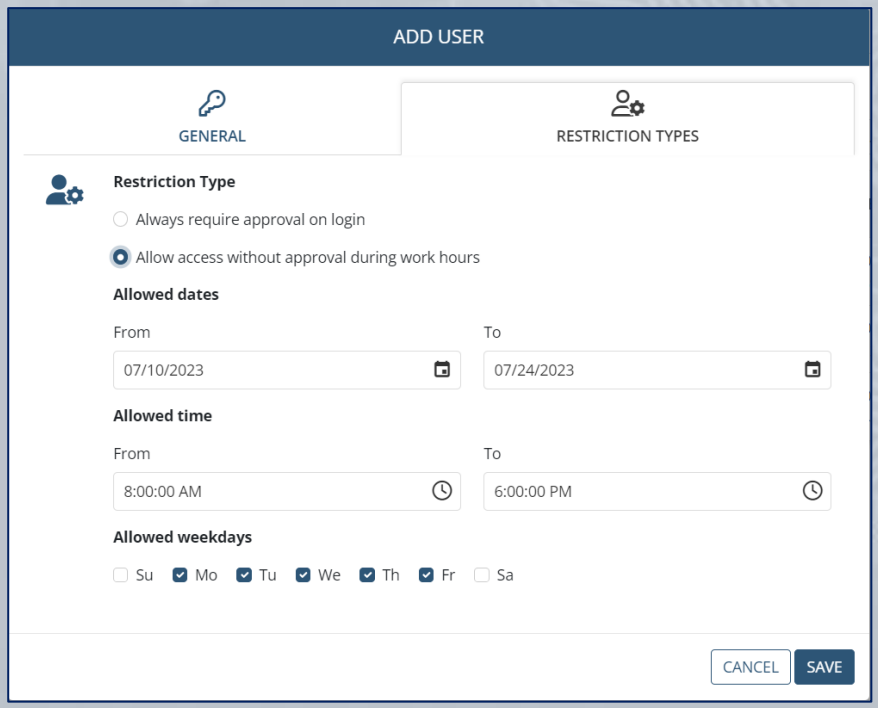
You can minimize cybersecurity risks and control the number of **simultaneously active accounts** with Ekran System's **Just-in-Time Endpoint Access** capabilities.



Access Request and Approval Workflow

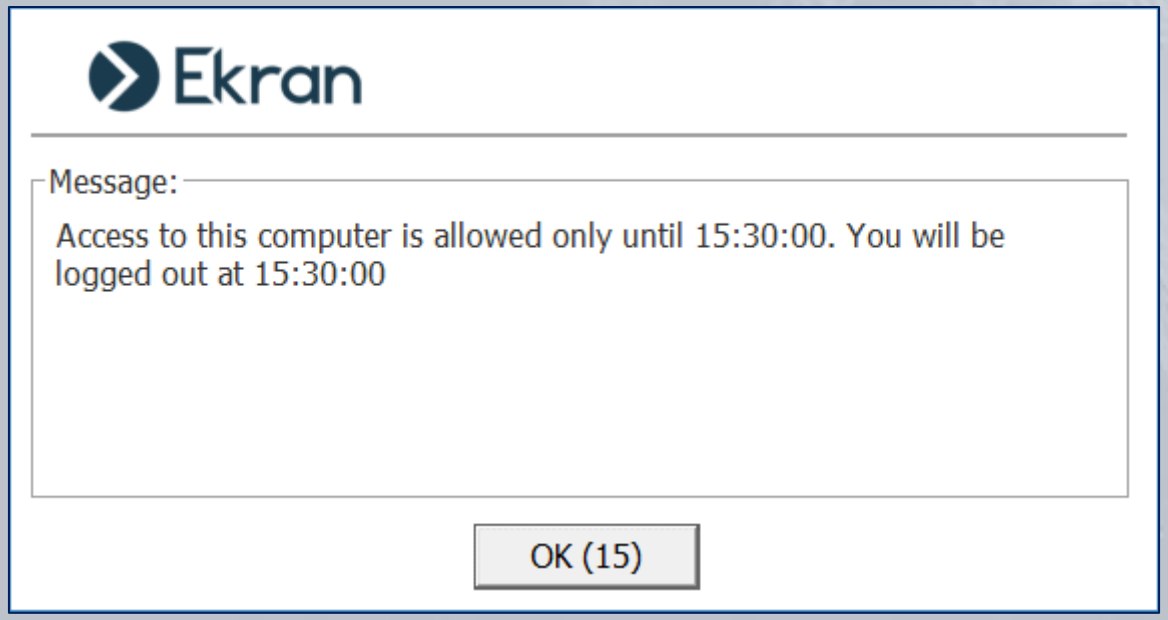
- **Manual access approval** to determine who can access what and when.
- **Time-based user access restrictions** to enhance the protection of critical data and systems.





Access Request and Approval Workflow

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**.

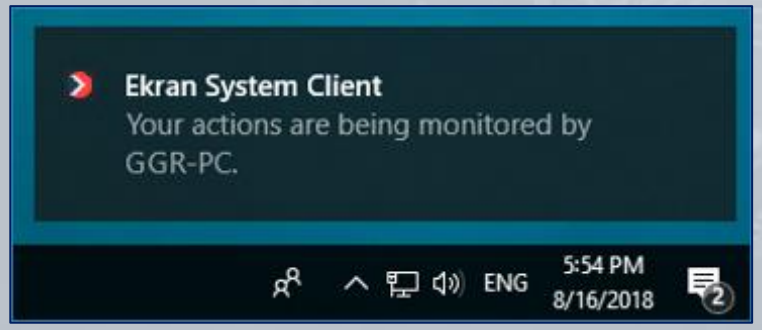


Notifying Users about Being Monitored

Notifying Users about Being Monitored

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

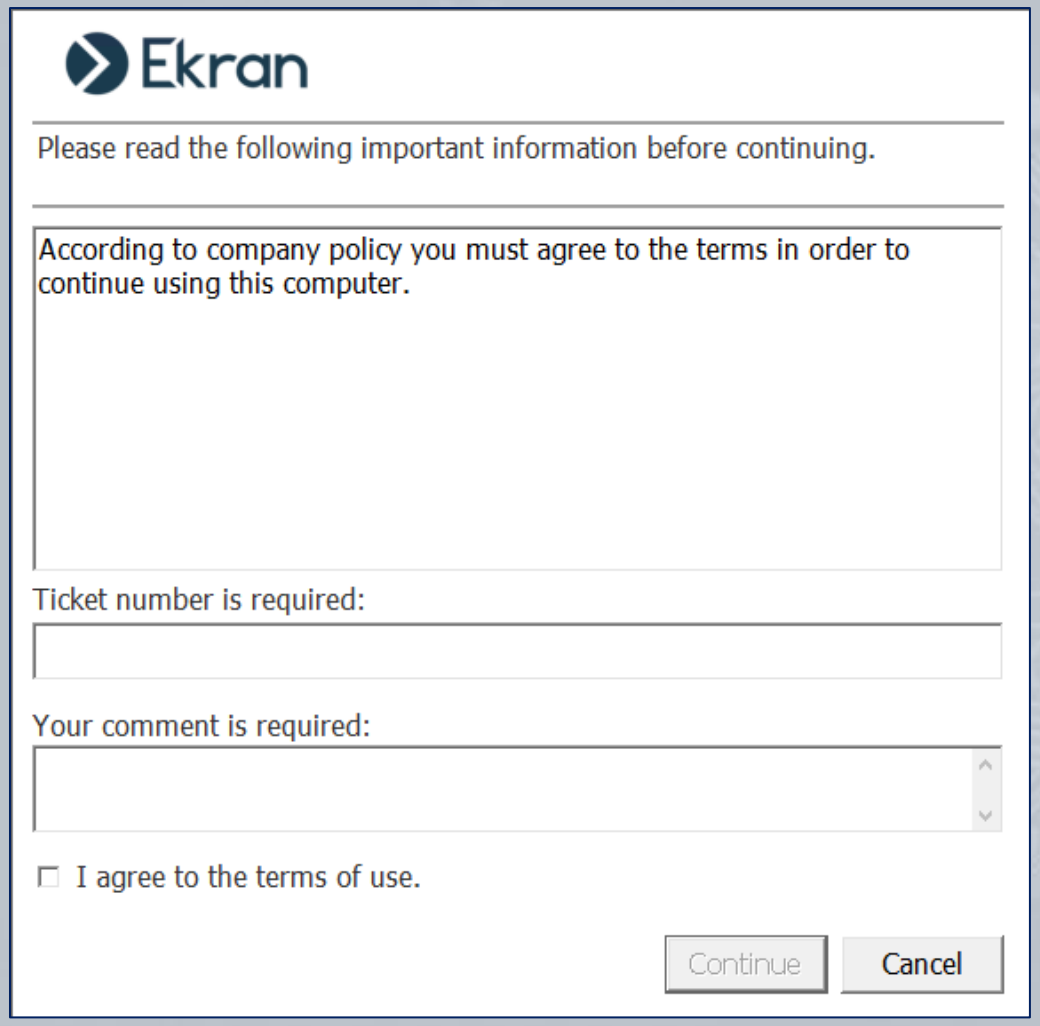
- Enable the **displaying** of a custom **additional message** on user login to notify the user that their activity is being monitored, and obtain their consent.
- Enable the **displaying** of the **Client tray icon** along with a **notification** to the user that their activity is being monitored.



Notifying Users about Being Monitored

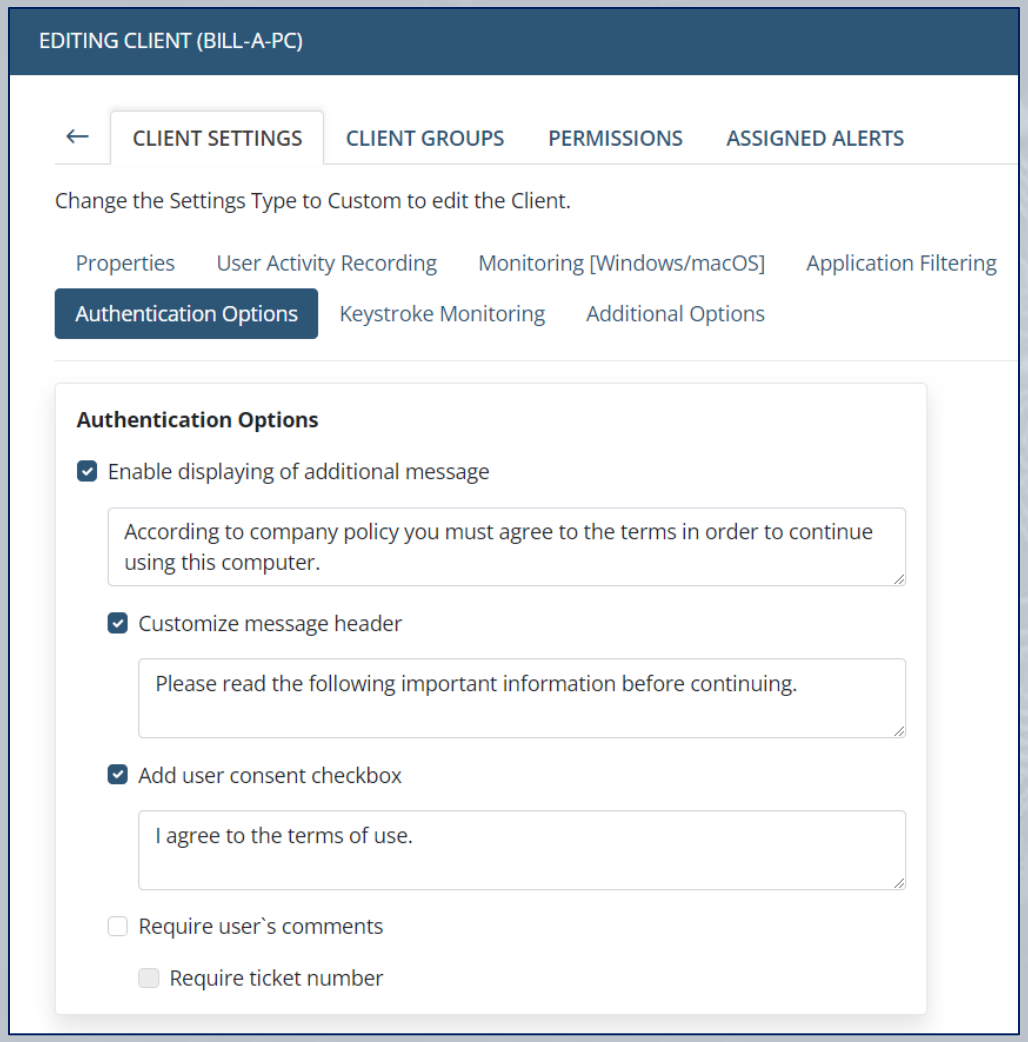
Before being allowed to log in to the Client computer, users can also be **required to**:

- **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**.



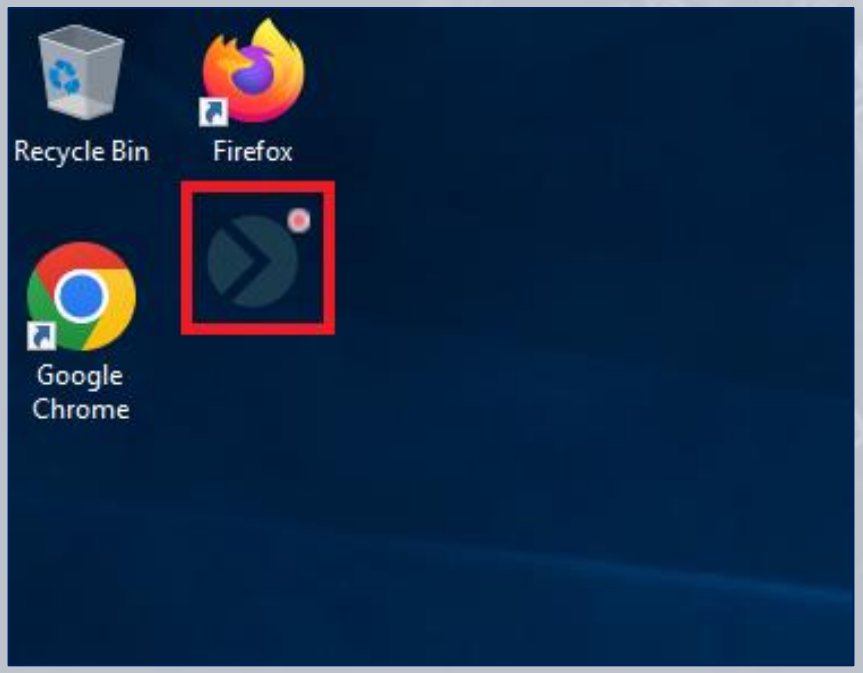
Notifying Users about Being Monitored

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



Notifying Users about Being Monitored

- 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**.

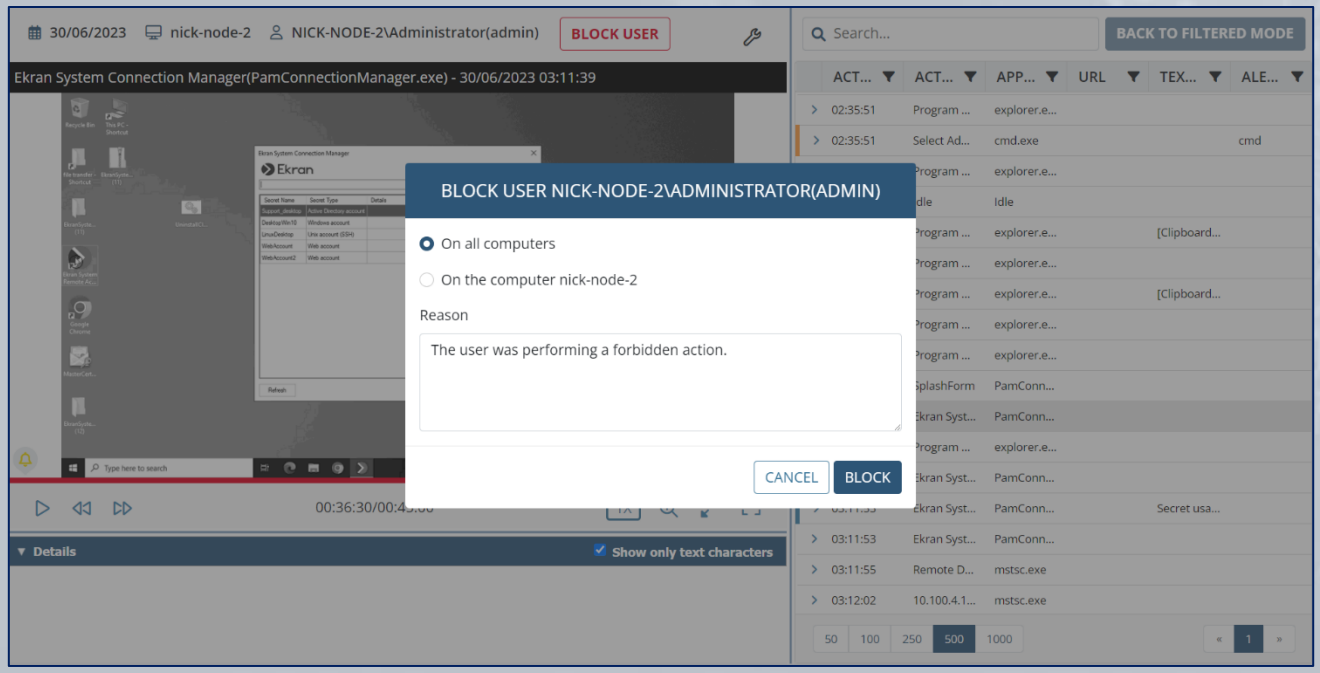


Blocking Users

Blocking Users Overview

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.

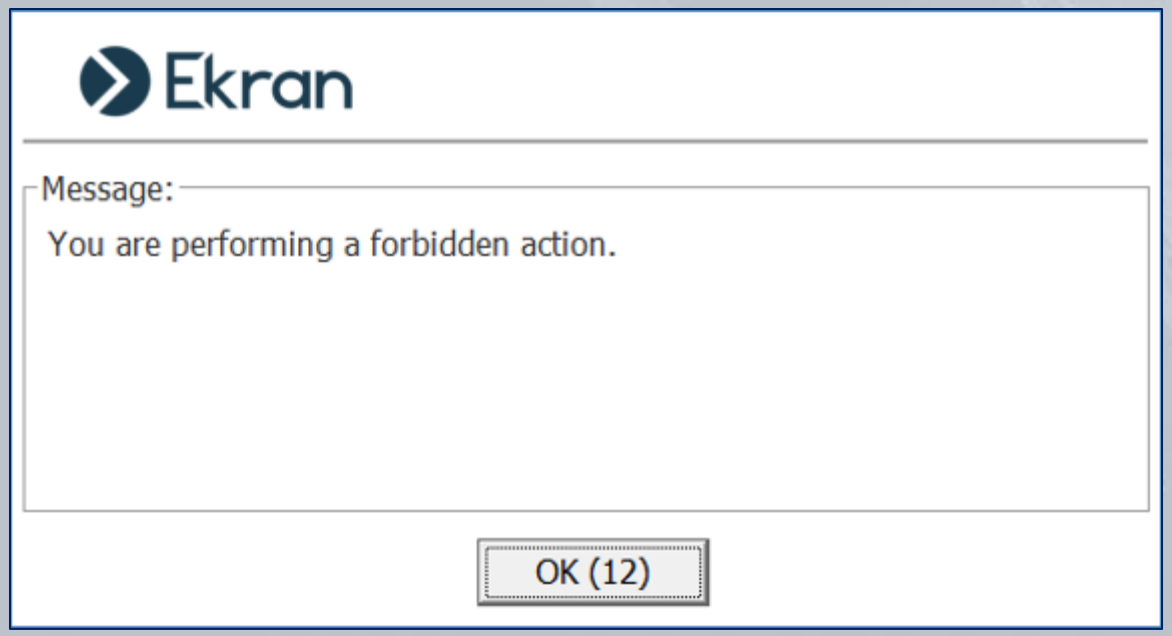
Users can be **blocked manually** from both **Live** and **Finished** sessions, or **automatically** when they perform an action that **triggers a specific alert**.



Blocking Users Overview

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

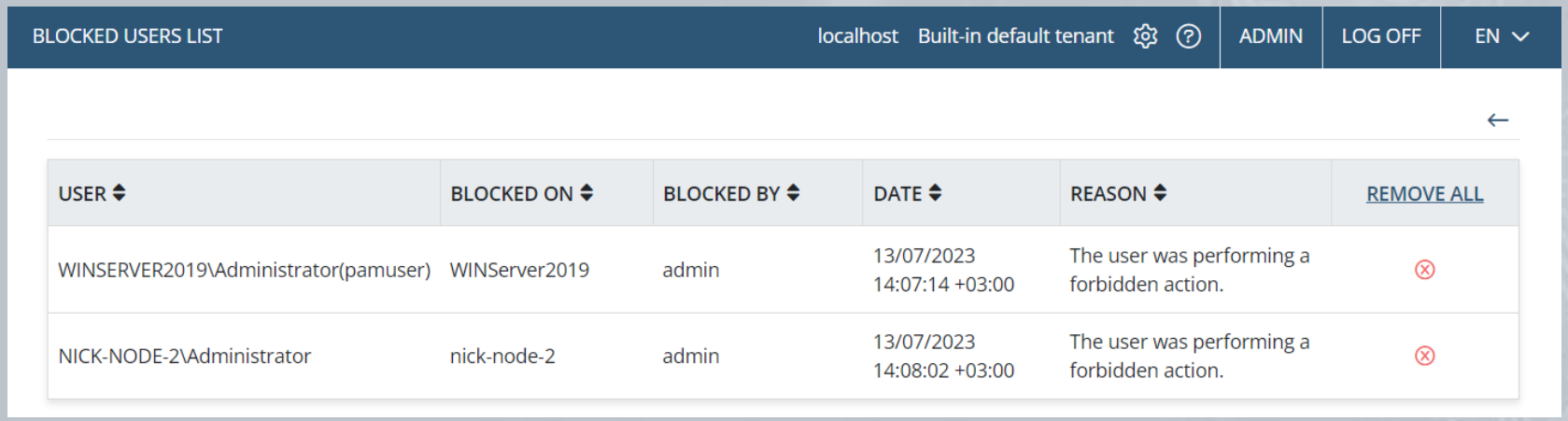
If the blocked user then tries to re-log in to the Client computer, the system will not allow them to do so.



Viewing the Blocked Users List

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

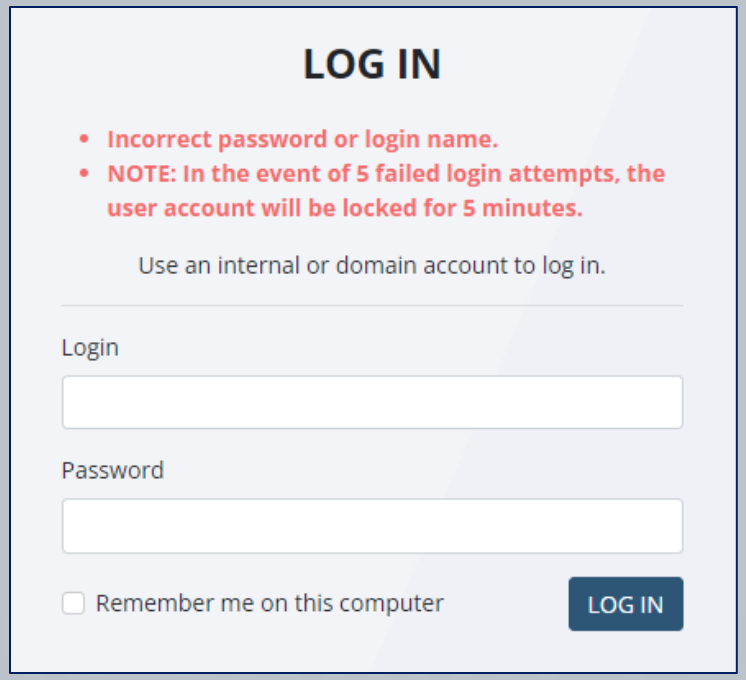
To **allow** users to **access** Client computers again, simply remove them from the list.

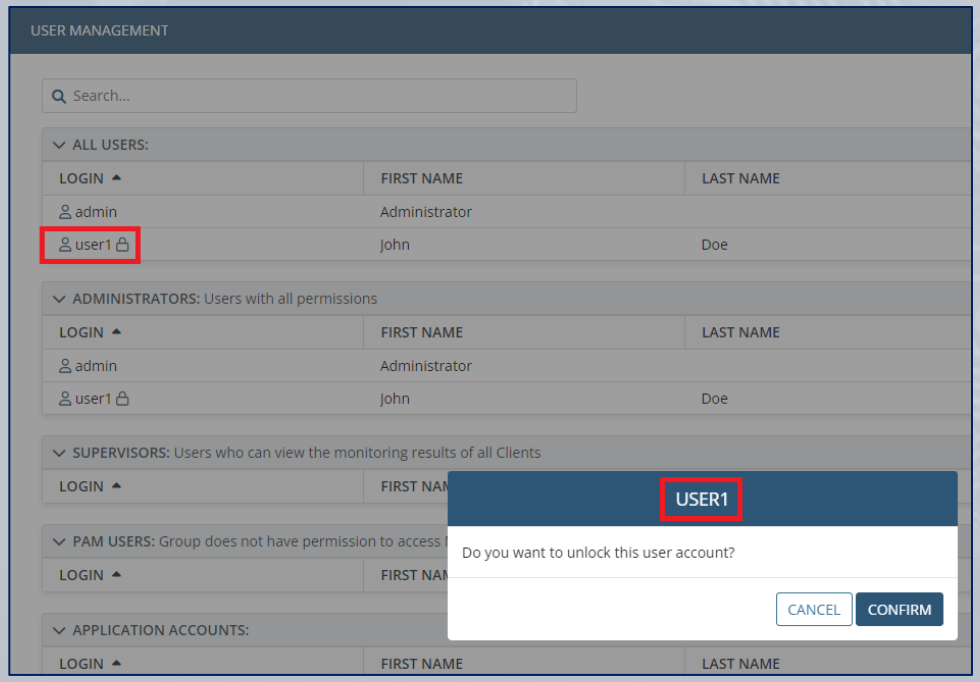


Locking Management Tool User Accounts

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**.



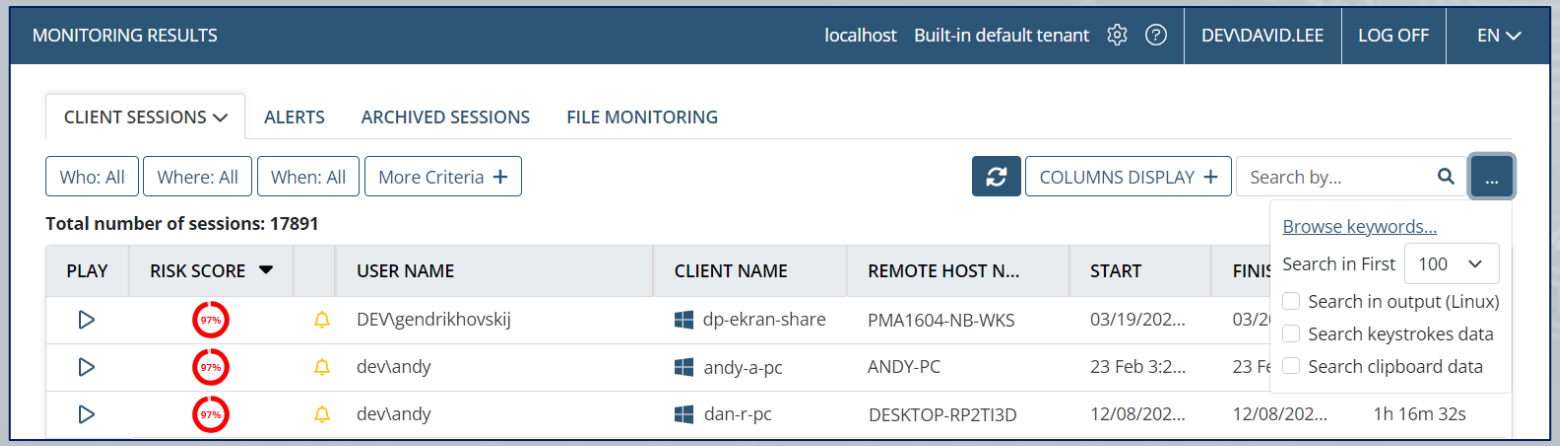


Viewing Client Sessions

Searching the Data in the Client Sessions List

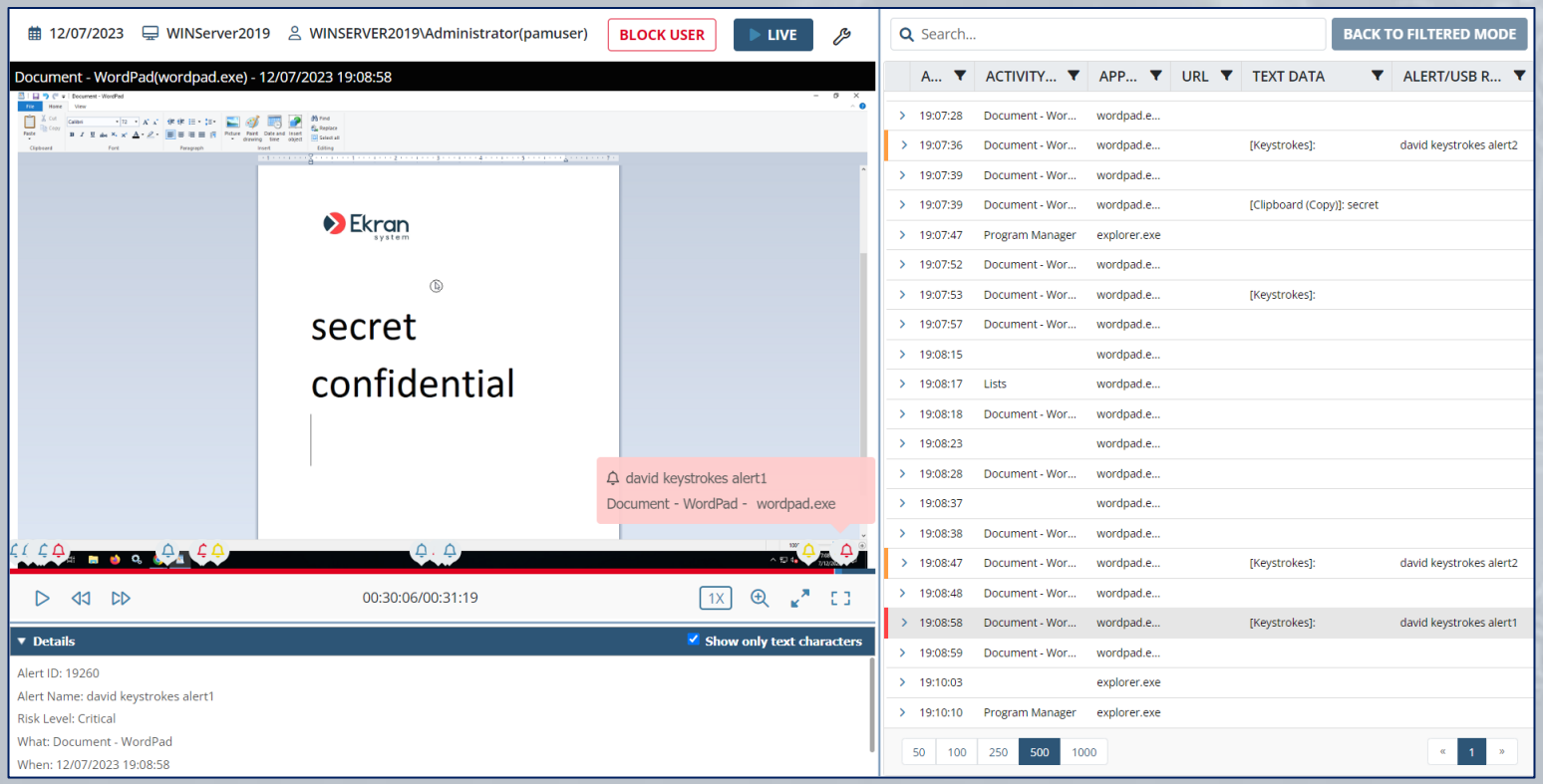
The Ekran System Management Tool allows searching within the monitored sessions that are recorded by various parameters:

- **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.



Viewing a Session

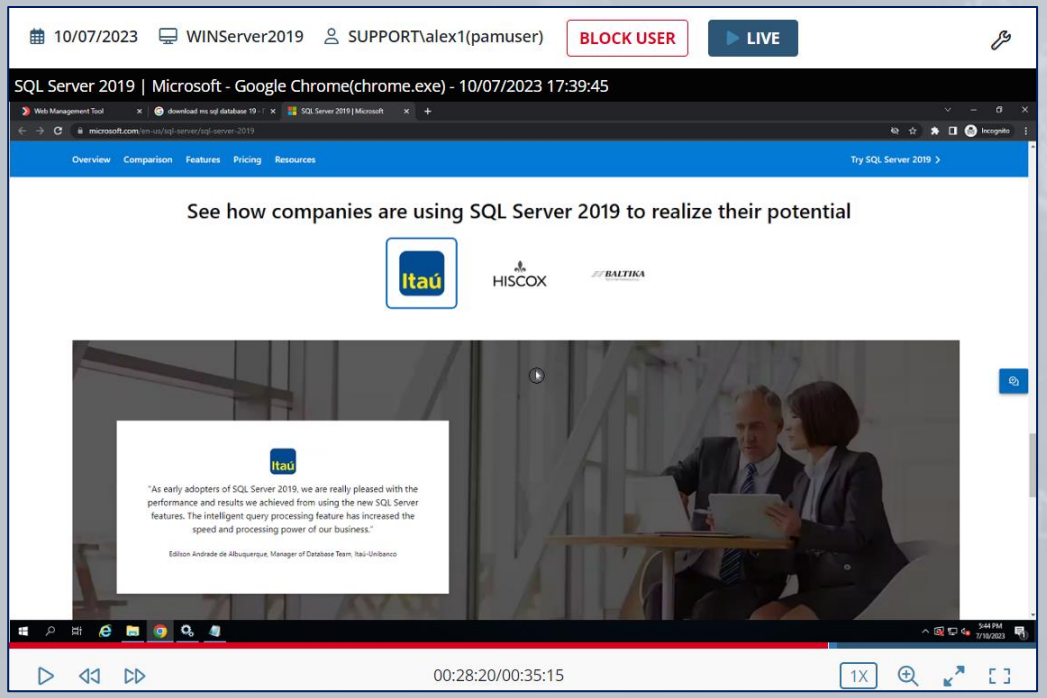
The panes in the Session Viewer display the **screen captures and metadata** recorded in the session, where the screen captures are **played as video** and **alerts are highlighted and color-coded**.



Viewing Live Sessions

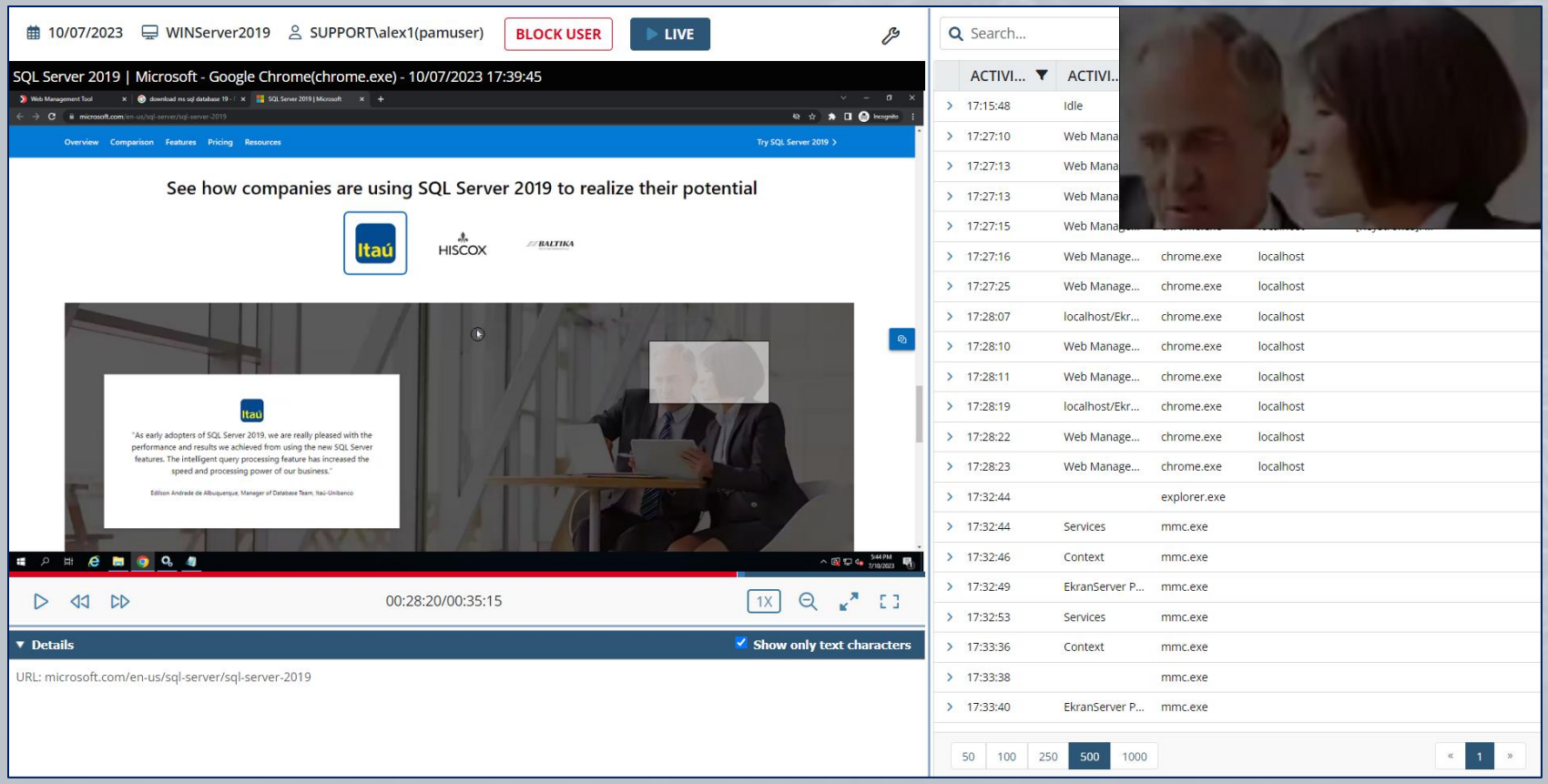
Ekran System allows you to perform **monitoring** of user activity on Clients computer **in real time**.

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

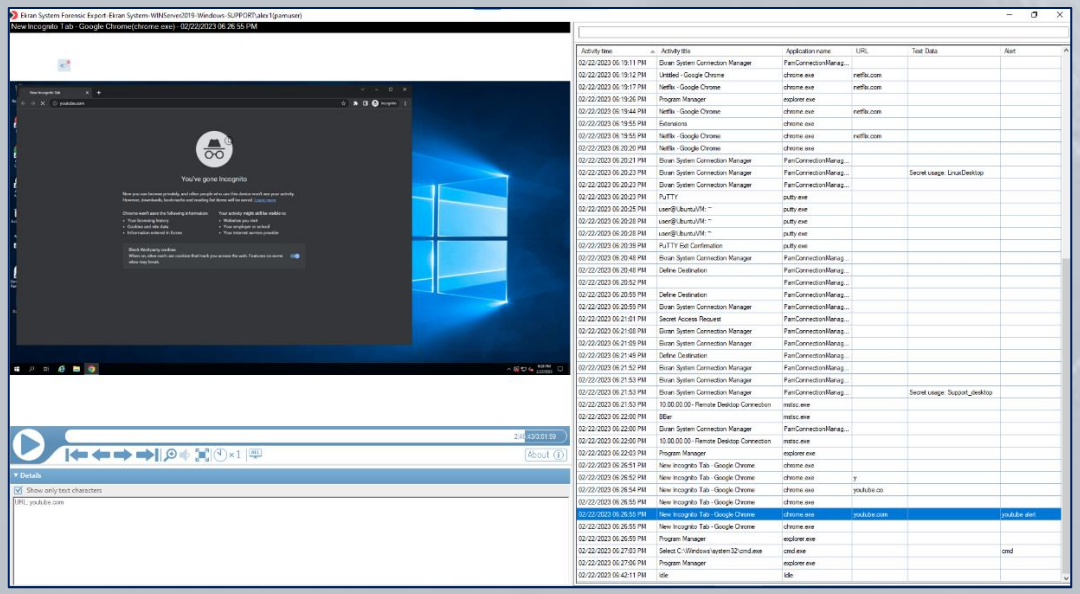
You can also enlarge any area of the video in the Session Player pane by using the **Magnifying Glass**.



Forensic Export

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)

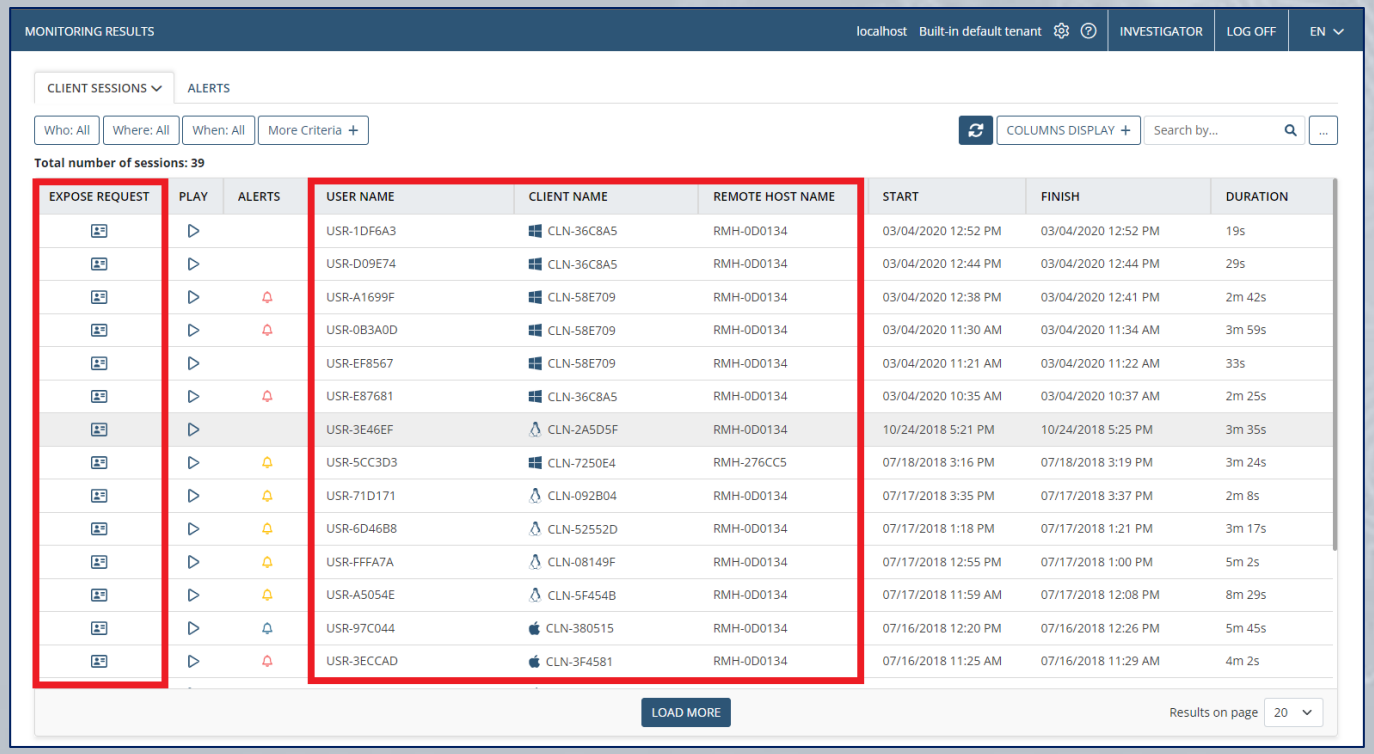
Anonymizer

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.

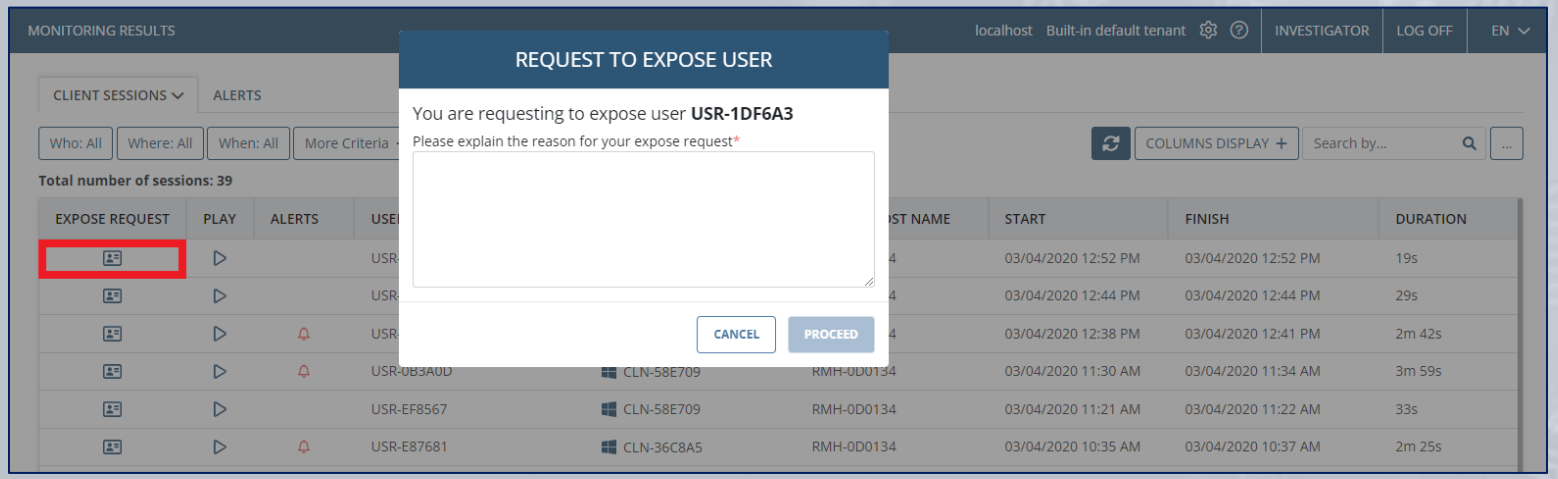
Pseudonymizing the PII Data

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).



Requesting De-Anonymization of PPI Data

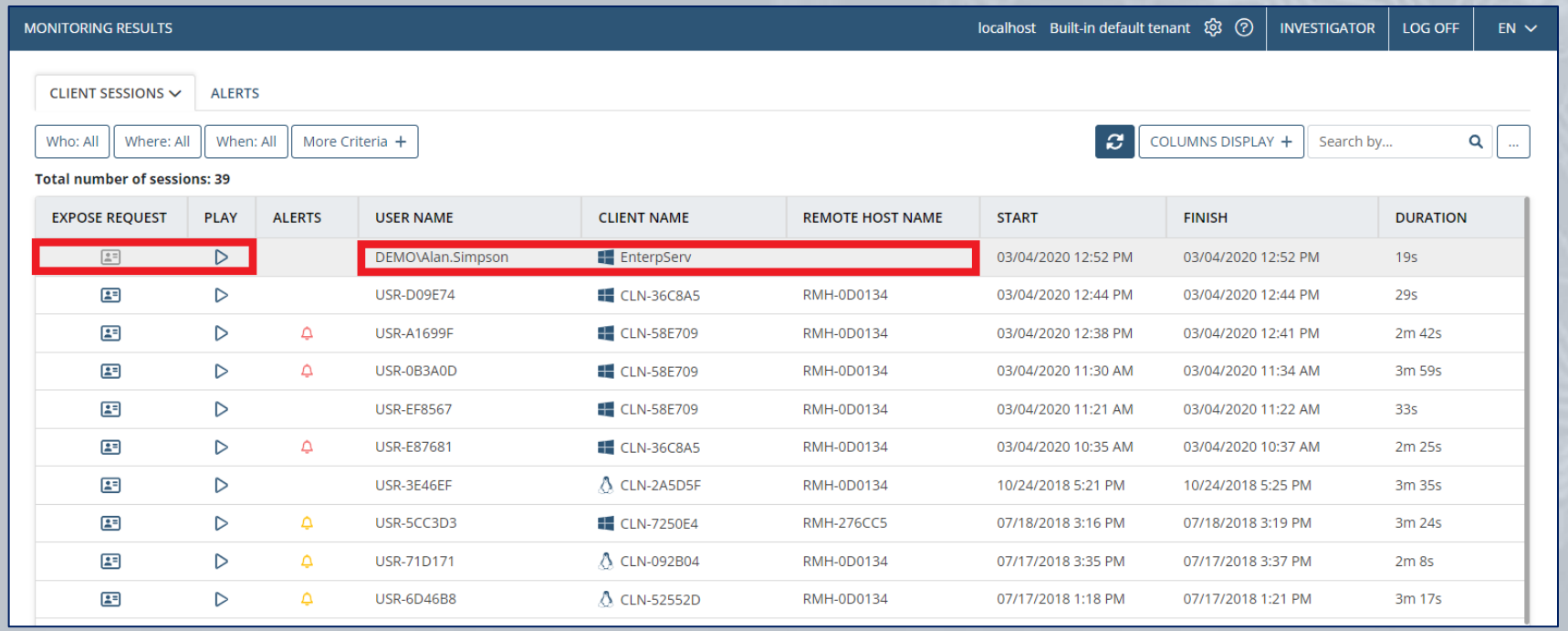
In **Anonymized mode**, no Management Tool user, including administrators and other users (e.g. **investigators**) that have permission to open and view the sessions of endpoint users, can view the personal data of any endpoint users unless a **request by them is first approved** (by a **supervisor**)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

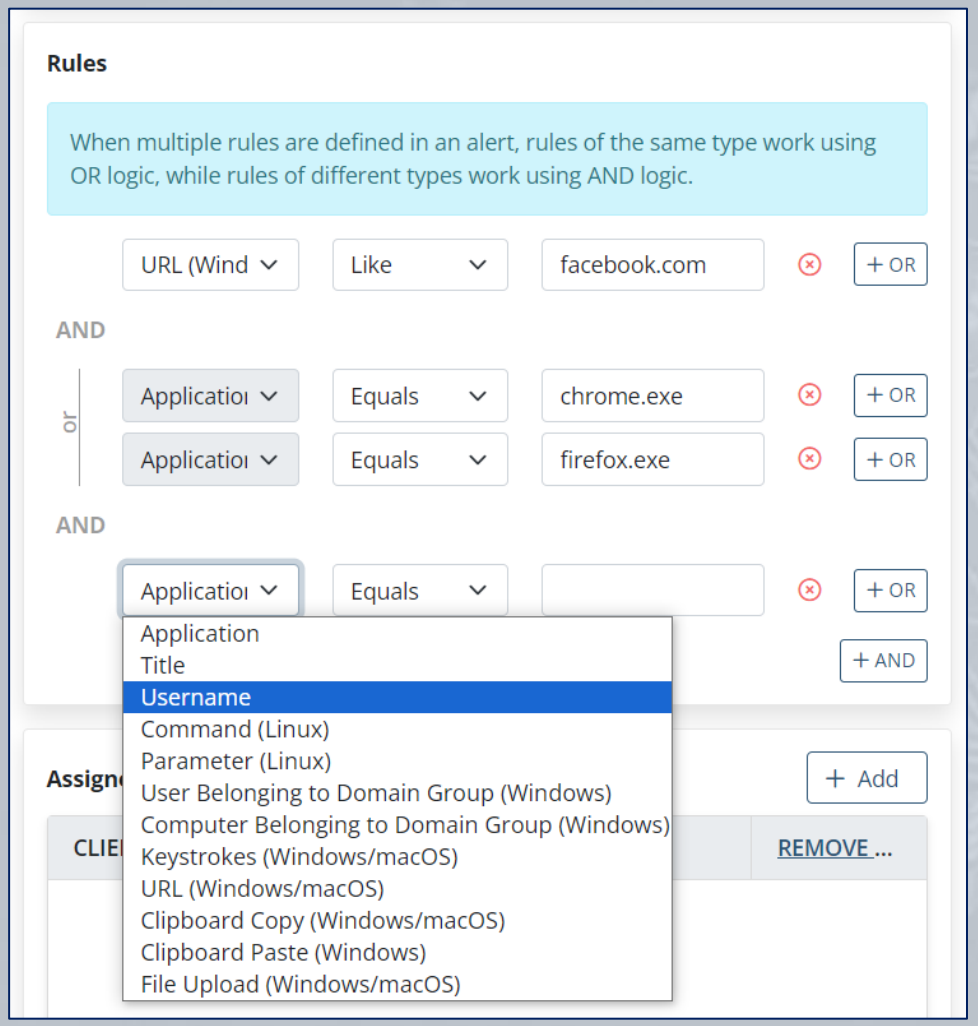


Alerts

Adding Alerts

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

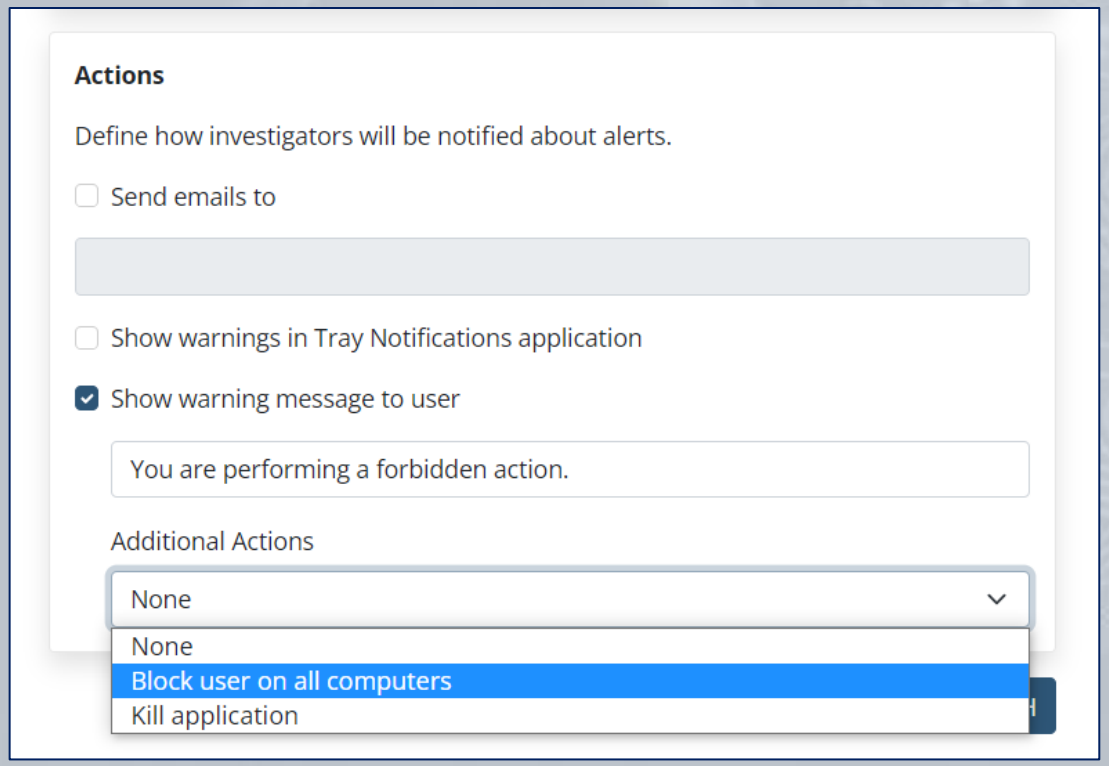
- **Add alert rules** to detect specific suspicious user activity on Client computers.
- Specify individuals to receive instant **alert notifications** via email and tray notifications.



Alert Actions

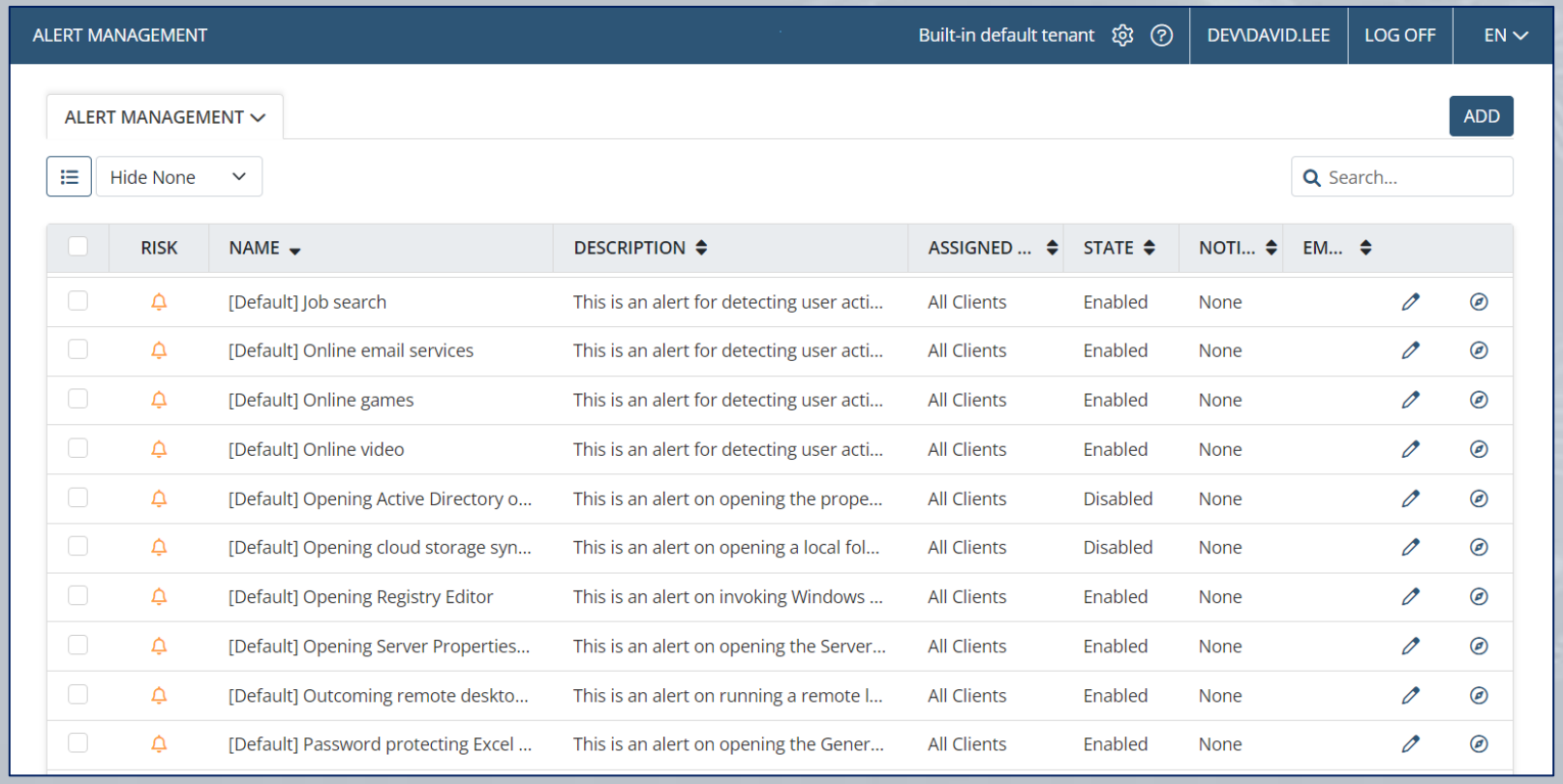
You can also set an alert to:

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



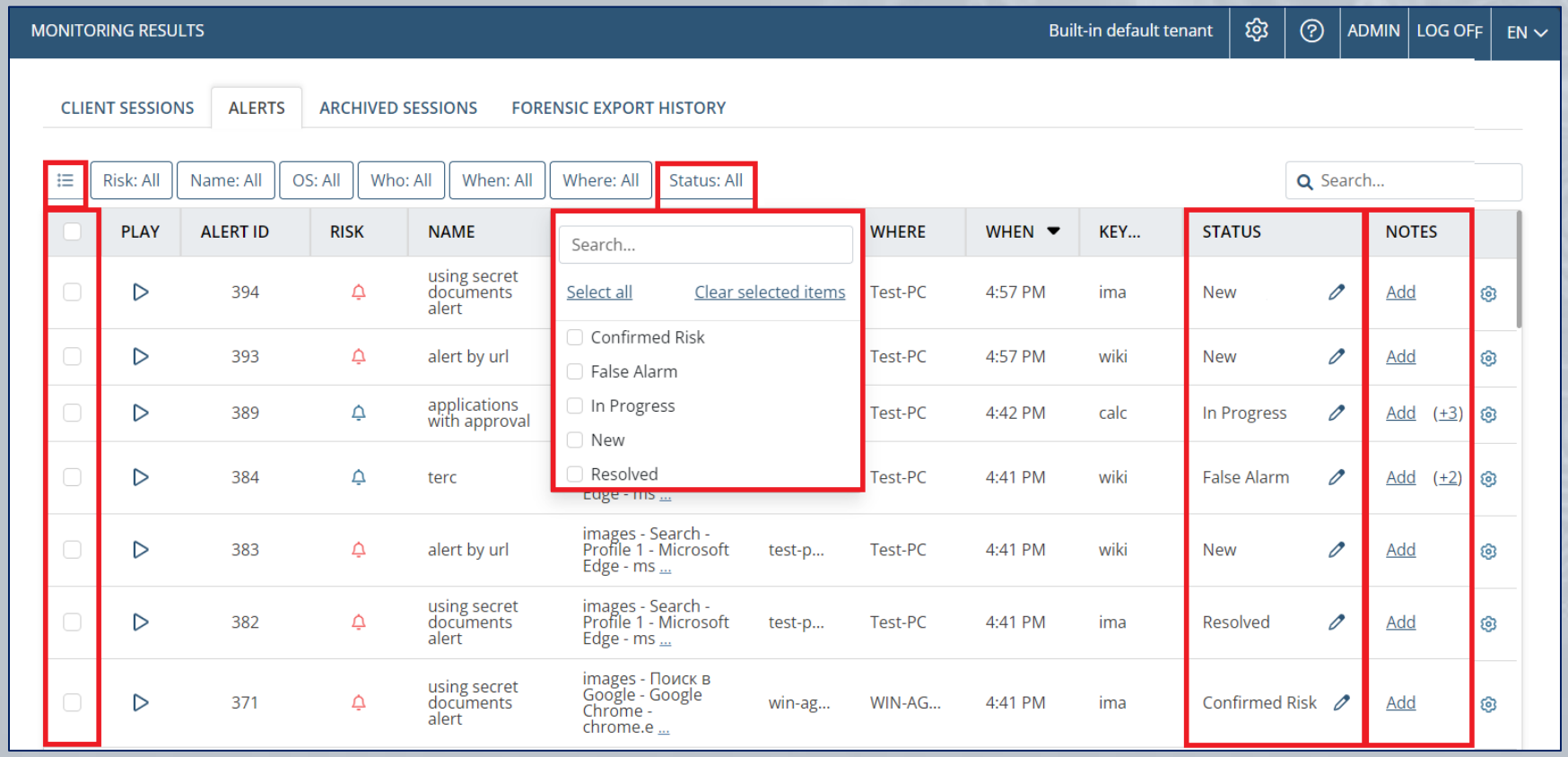
Default Alerts

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.



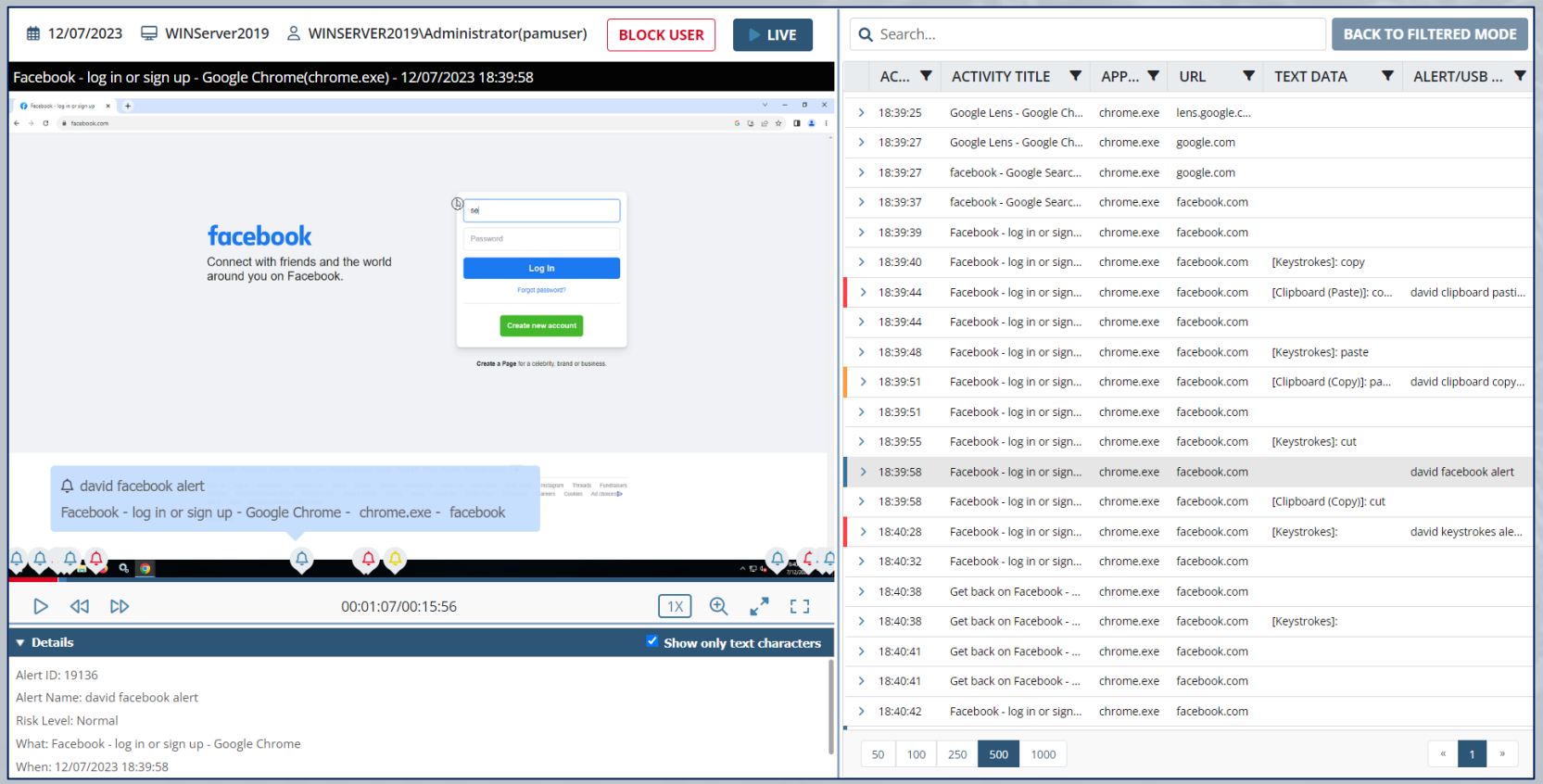
Viewing Alert Events

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



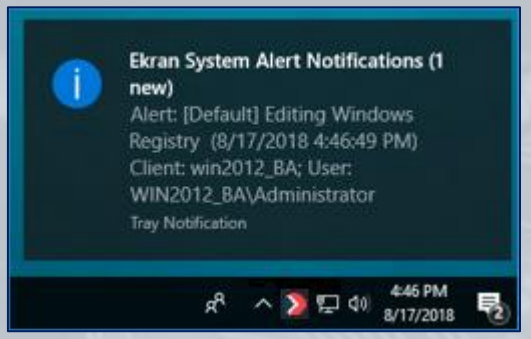
Viewing Alert Events in the Session Viewer

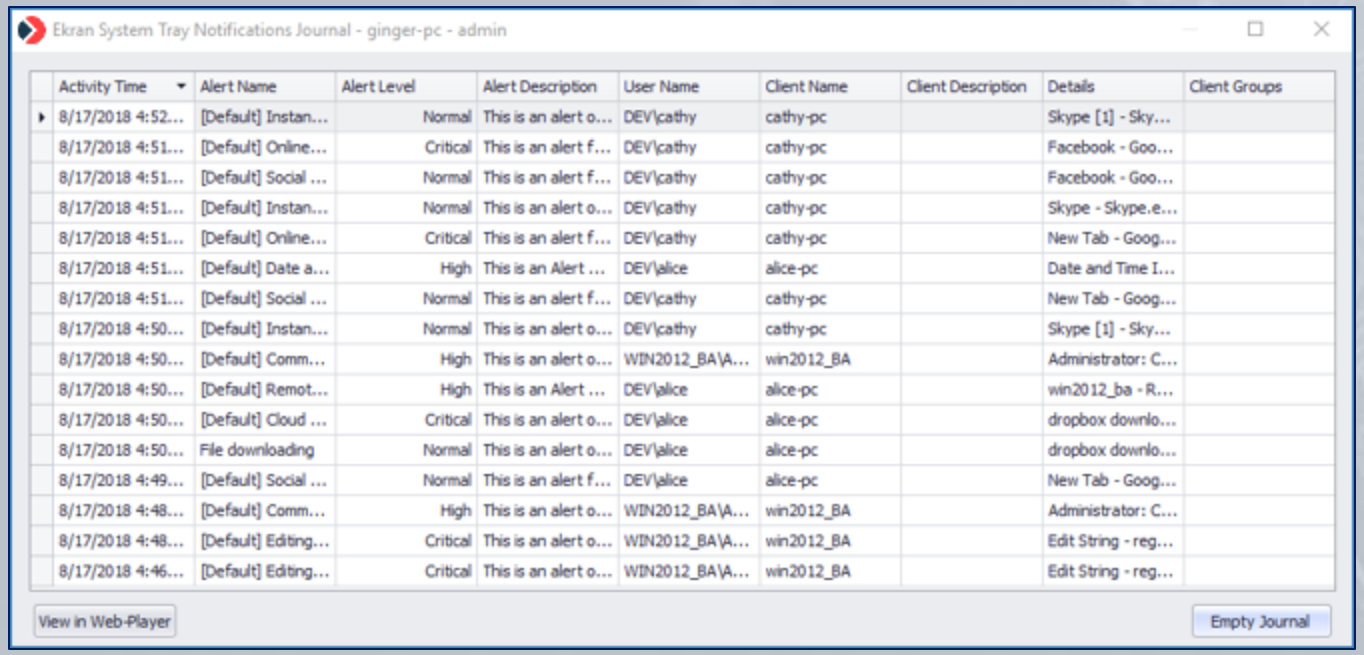
Monitored data associated with alert events is **highlighted** in the Session Viewer (in different **colors** depending on the **alert risk level**).



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.





USB Device Monitoring

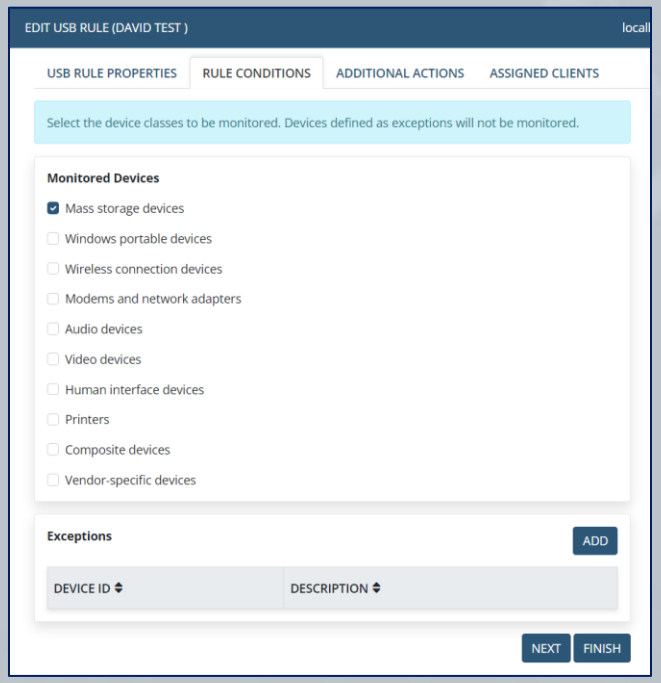
USB Device Monitoring

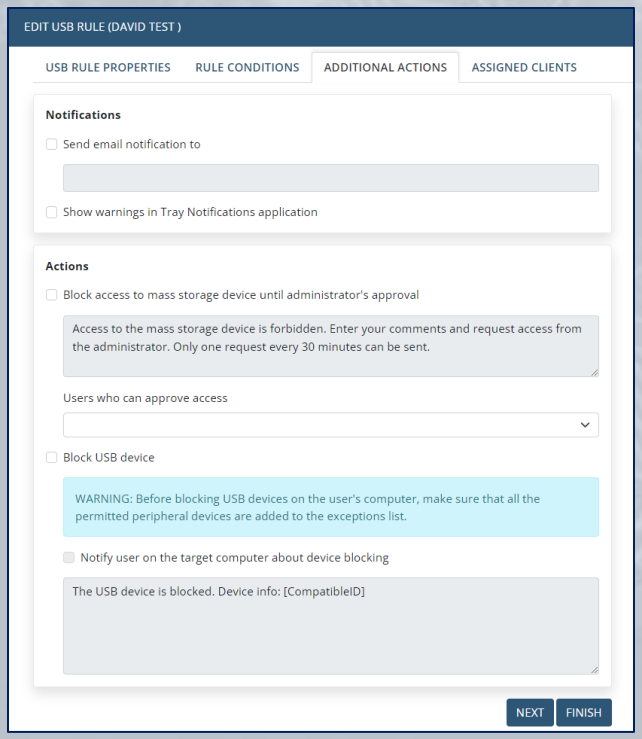
Ekran System provides **two types of monitoring** for USB devices plugged in to Client computers:

- **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.

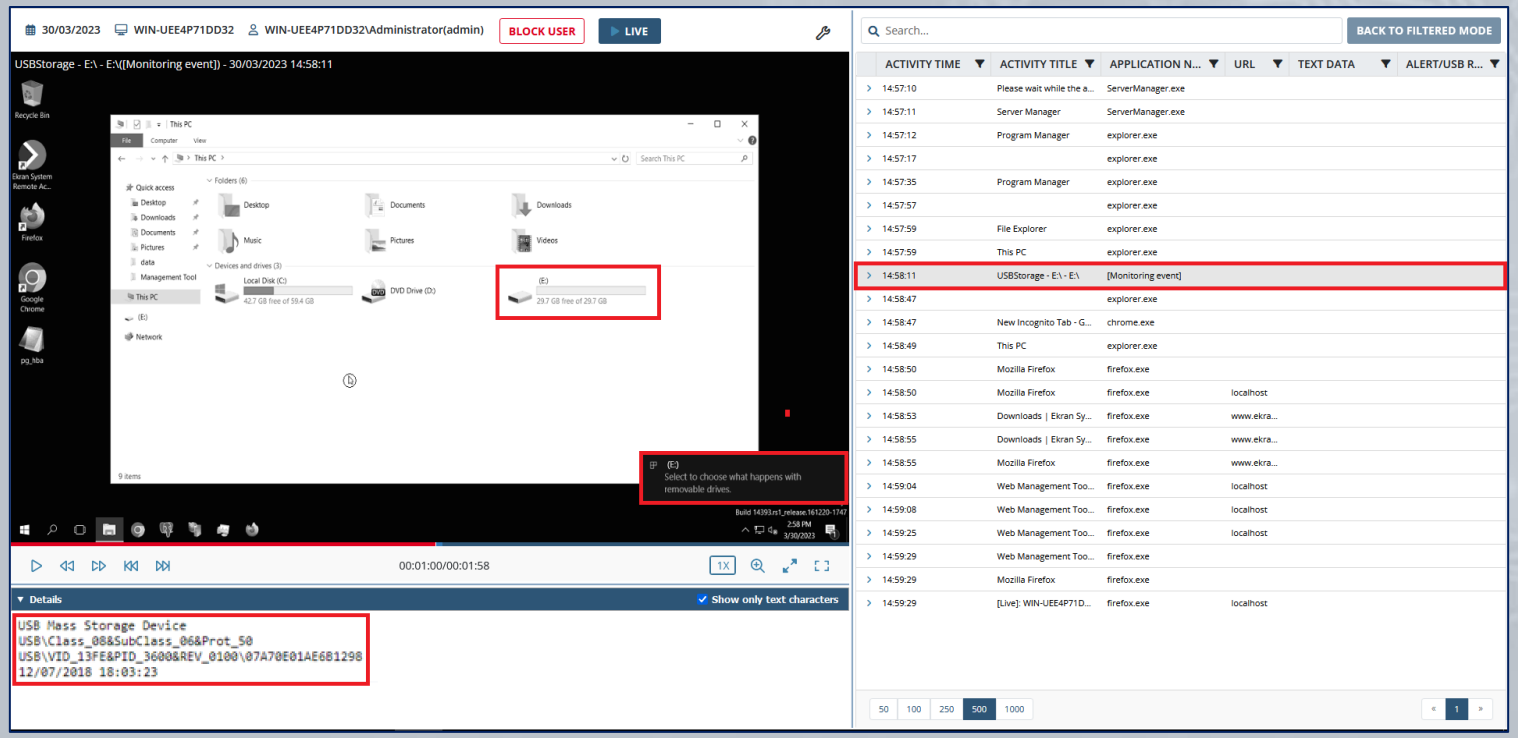




Automatic USB Device Monitoring

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.

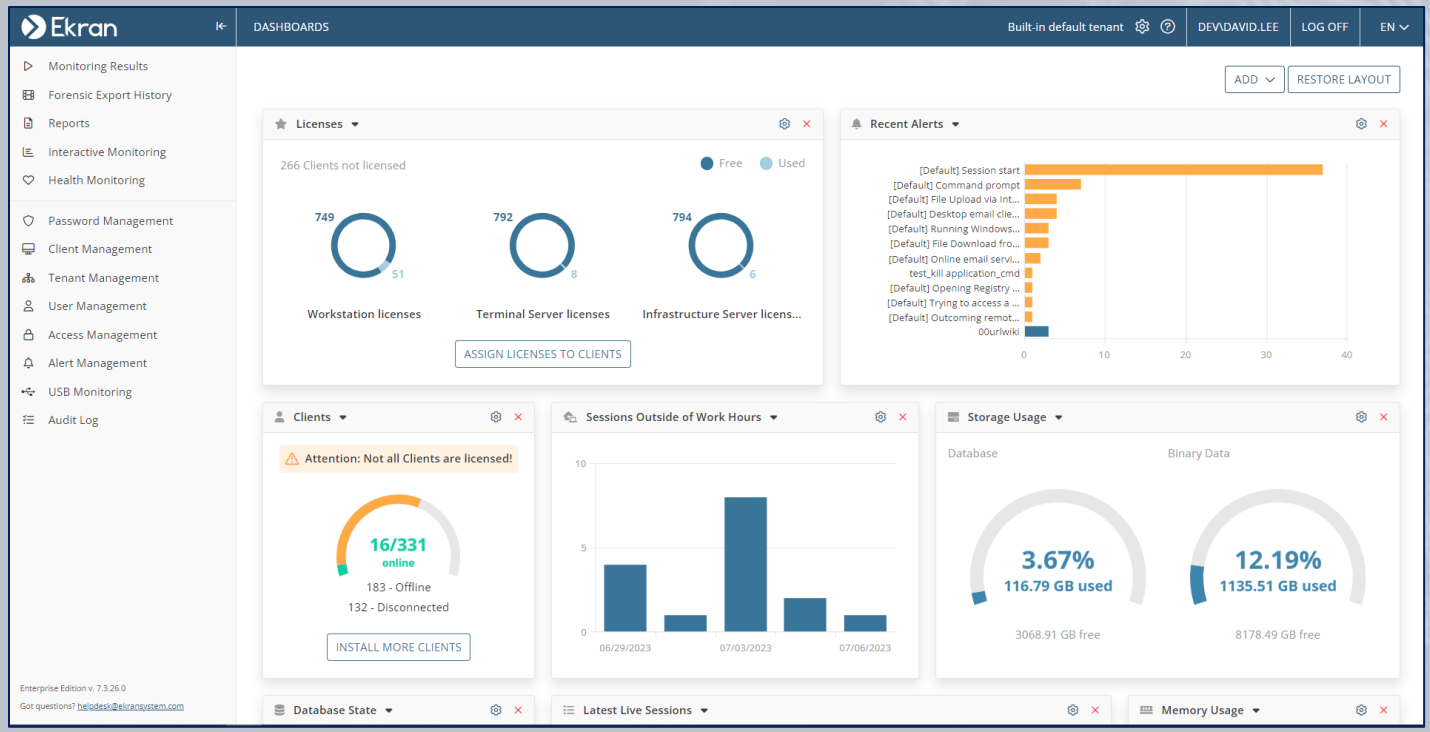


Dashboards

Dashboards Overview

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**.



Dashboard Types

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

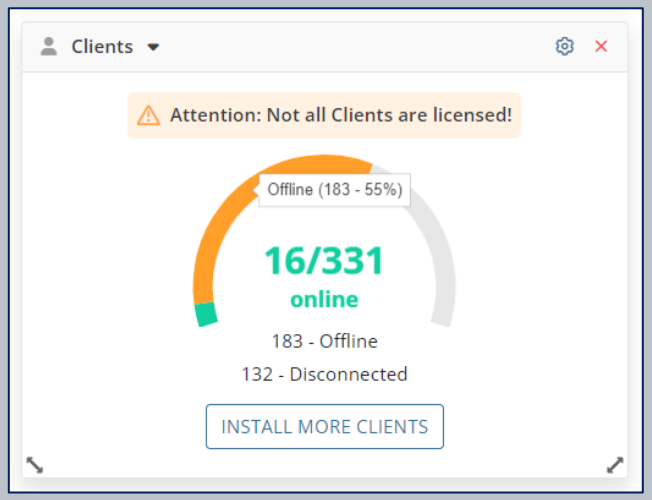
Server Resource Monitoring Dashboards

- CPU Usage
- Memory Usage
- The Database State

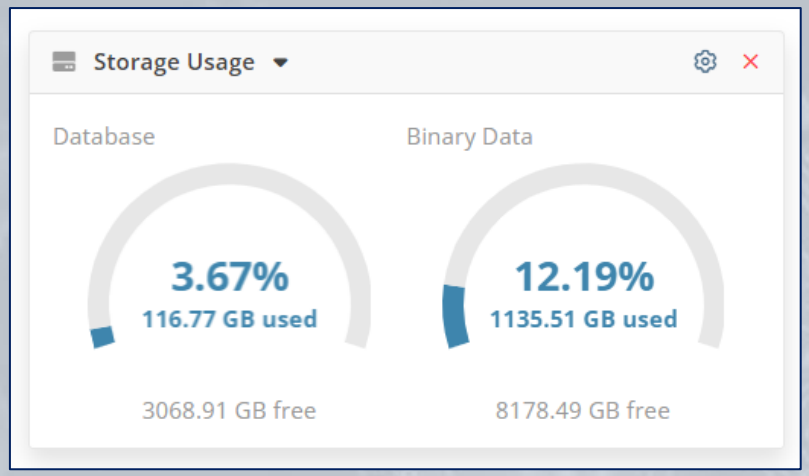
System State Dashboards

Ekran system

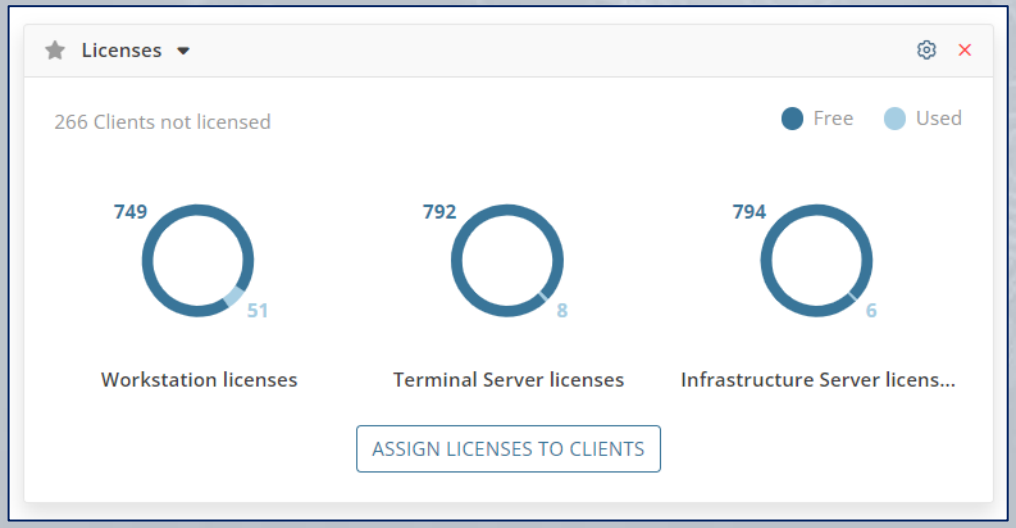
Clients



Storage Usage



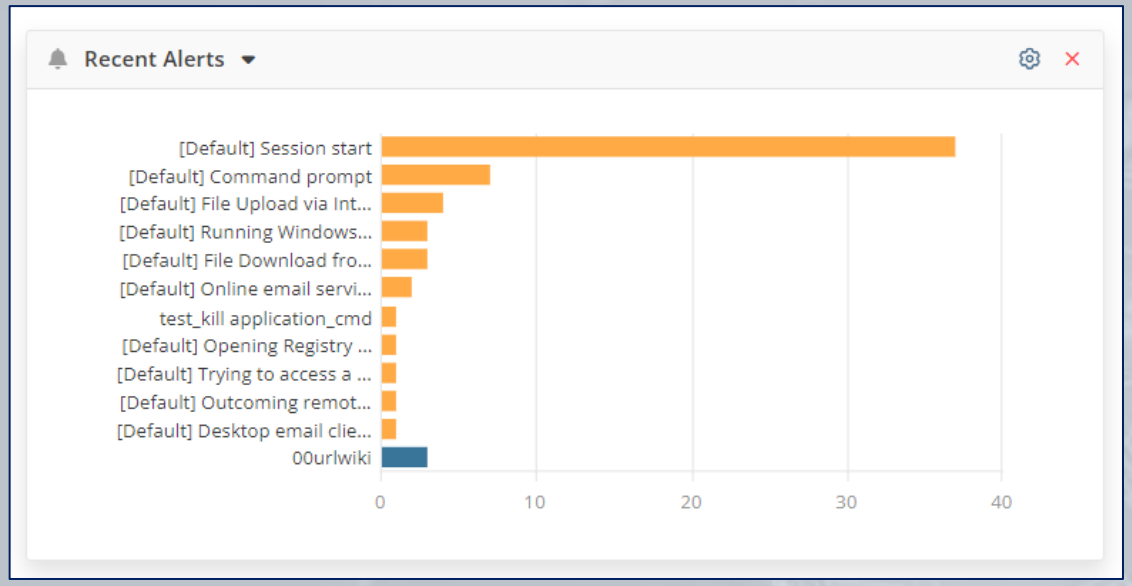
Licenses



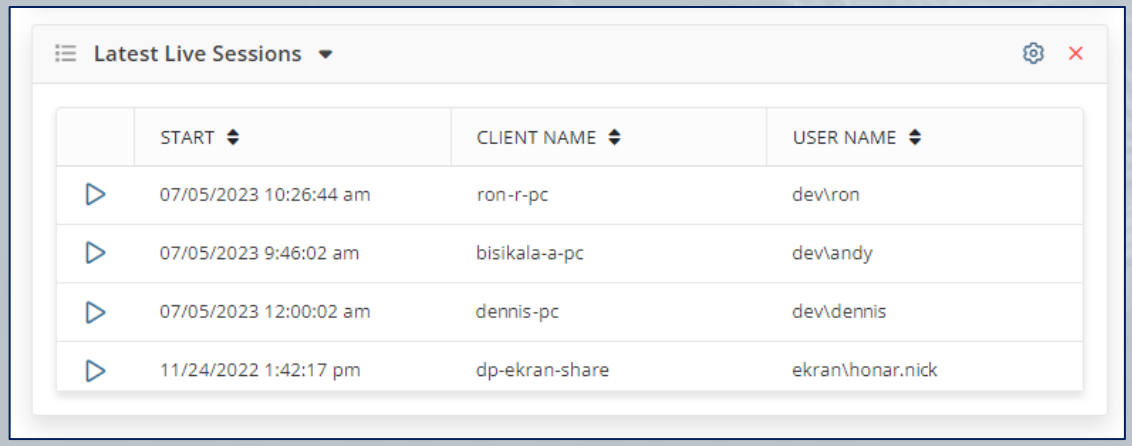
Monitoring Dashboards

Ekran system

Recent Alerts

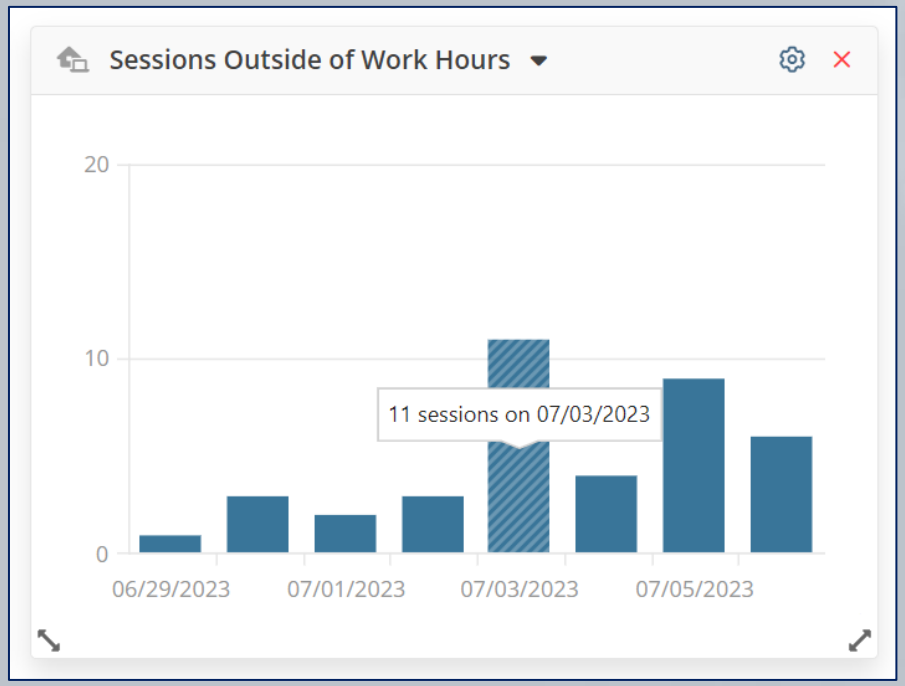


Latest Live Sessions

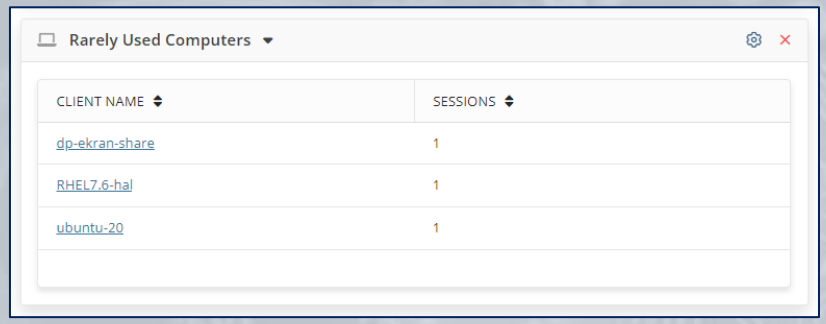


Threat Detection Dashboards

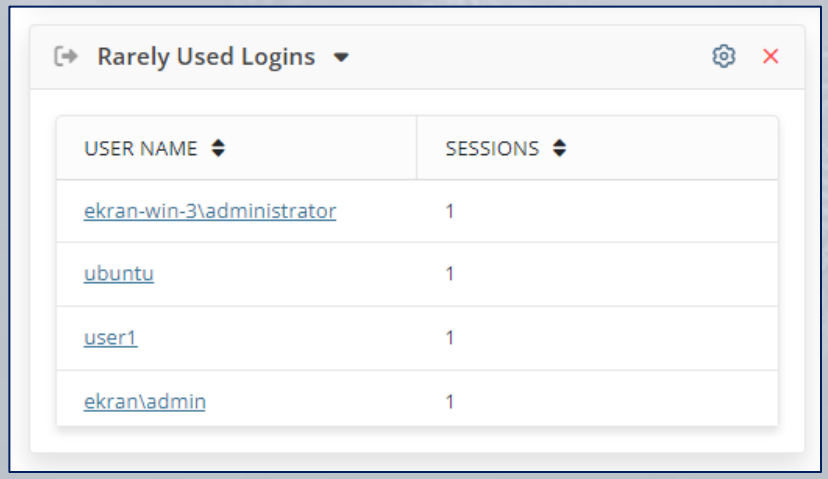
Sessions Outside of Work Hours



Rarely Used Logins

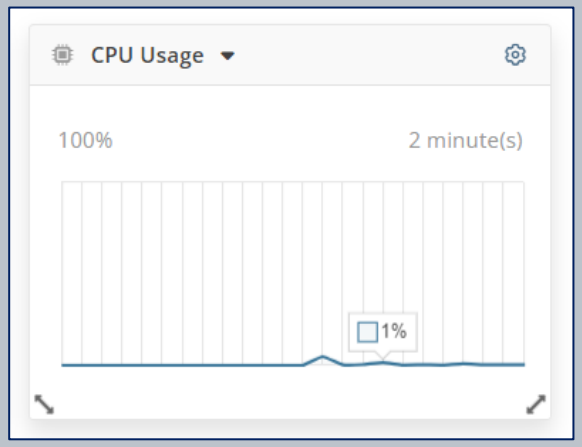


Rarely Used Computers

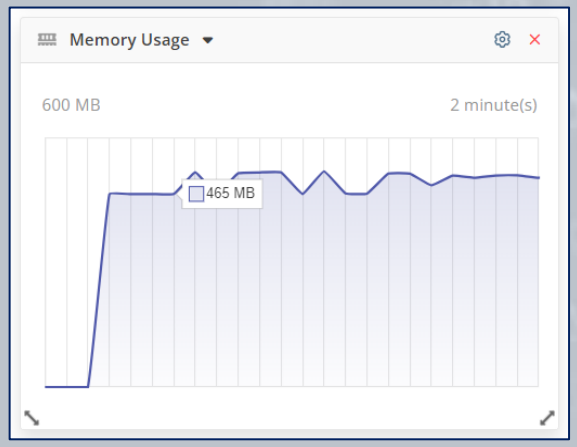


Server Resource Monitoring Dashboards

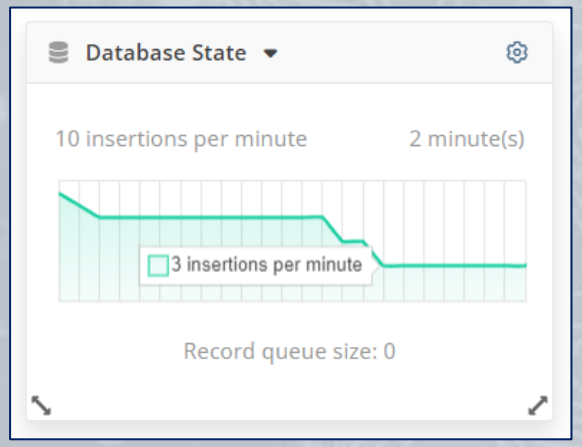
CPU Usage



Memory Usage



Database State



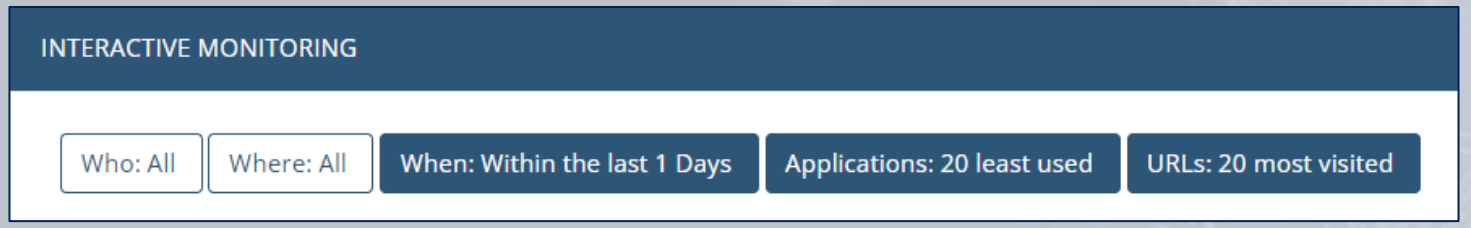
Interactive Monitoring

Interactive Monitoring Overview

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**.



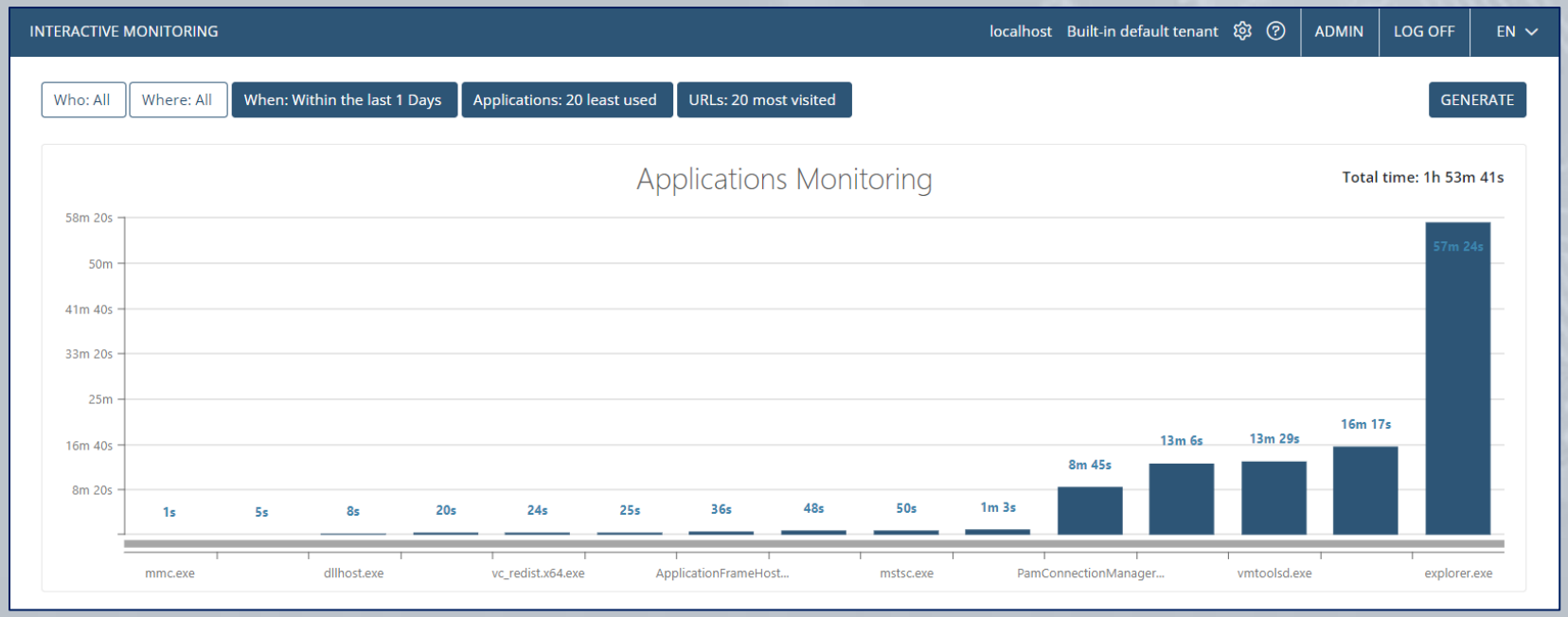
Data is displayed in the form of two column charts (the **Application Monitoring** chart and the **URL Monitoring** chart).

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**.

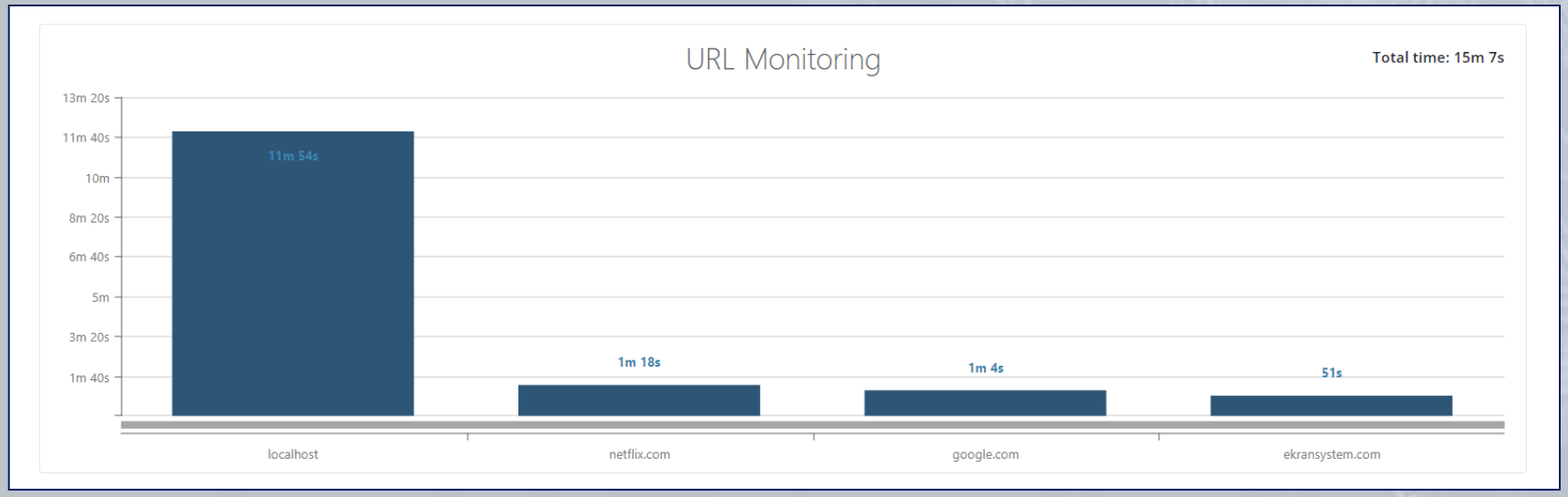
You can also use this chart to analyze information on the **most and least used** applications, and detect any threats and suspicious activity on the computers being investigated.



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

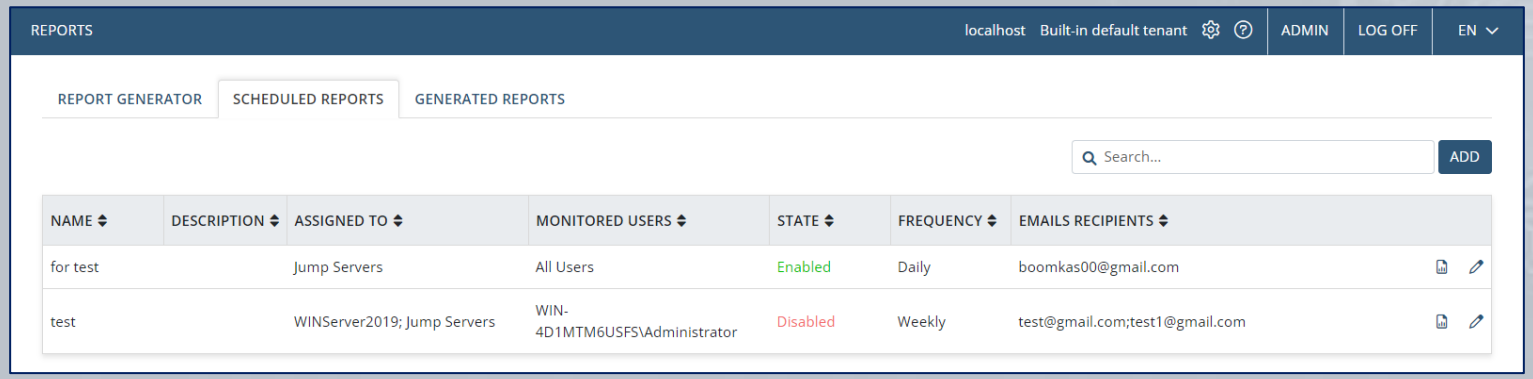
Reports & Statistics

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.

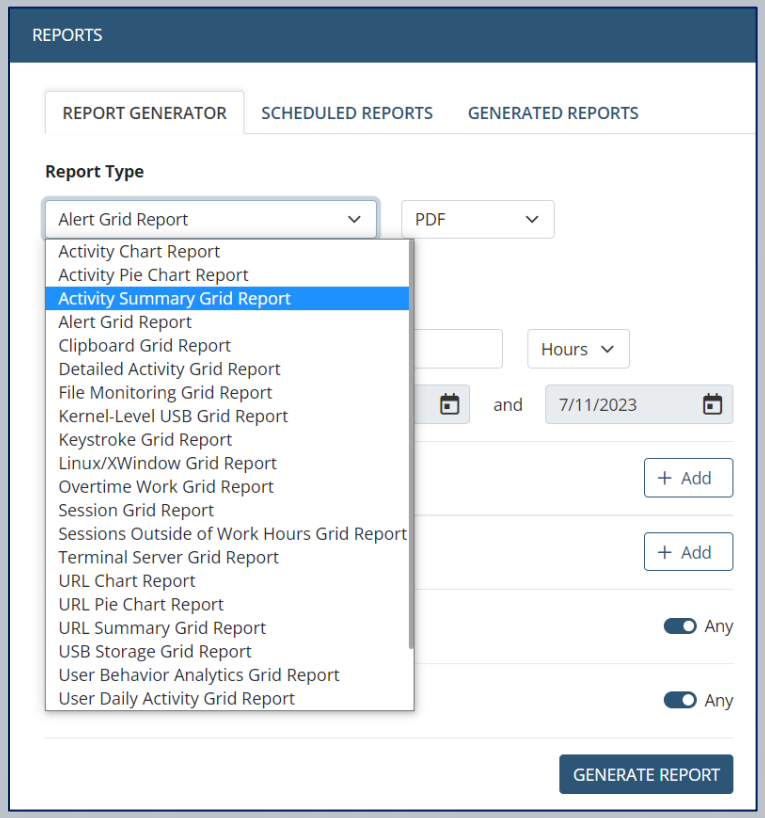
Scheduled Reports

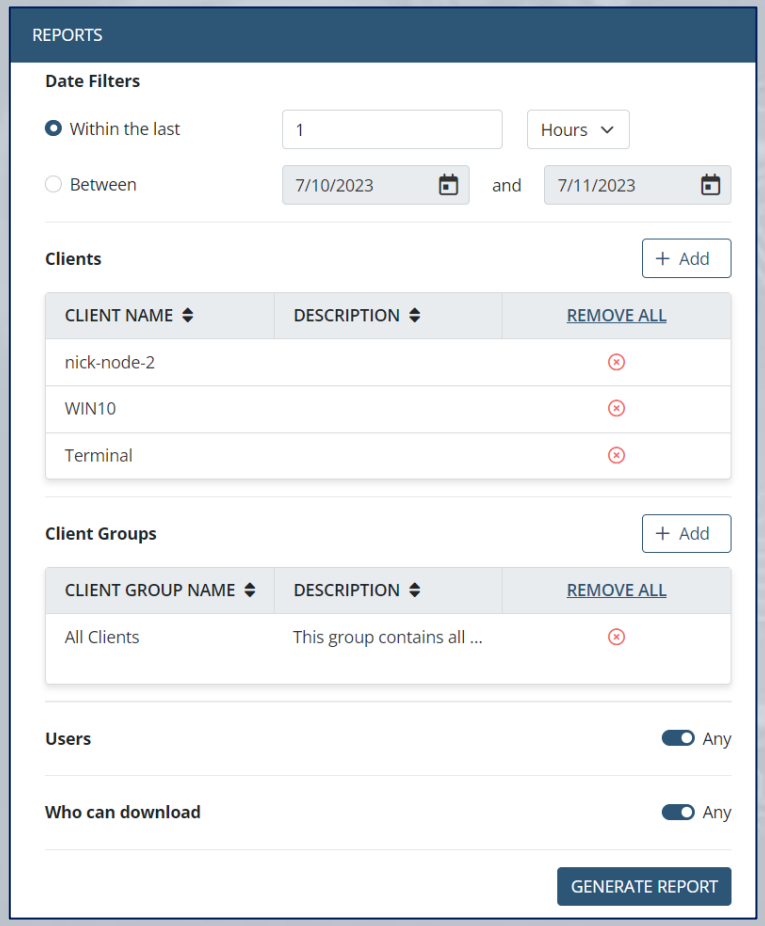


Reports & Statistics

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

Manual Report Generation





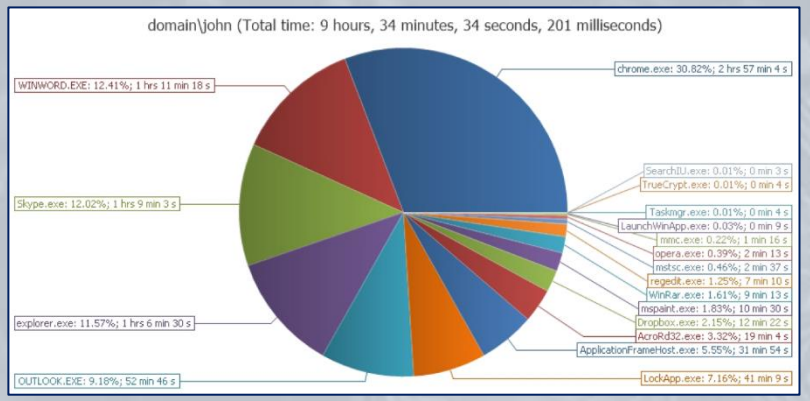
Report Types

Activity Summary Grid Report

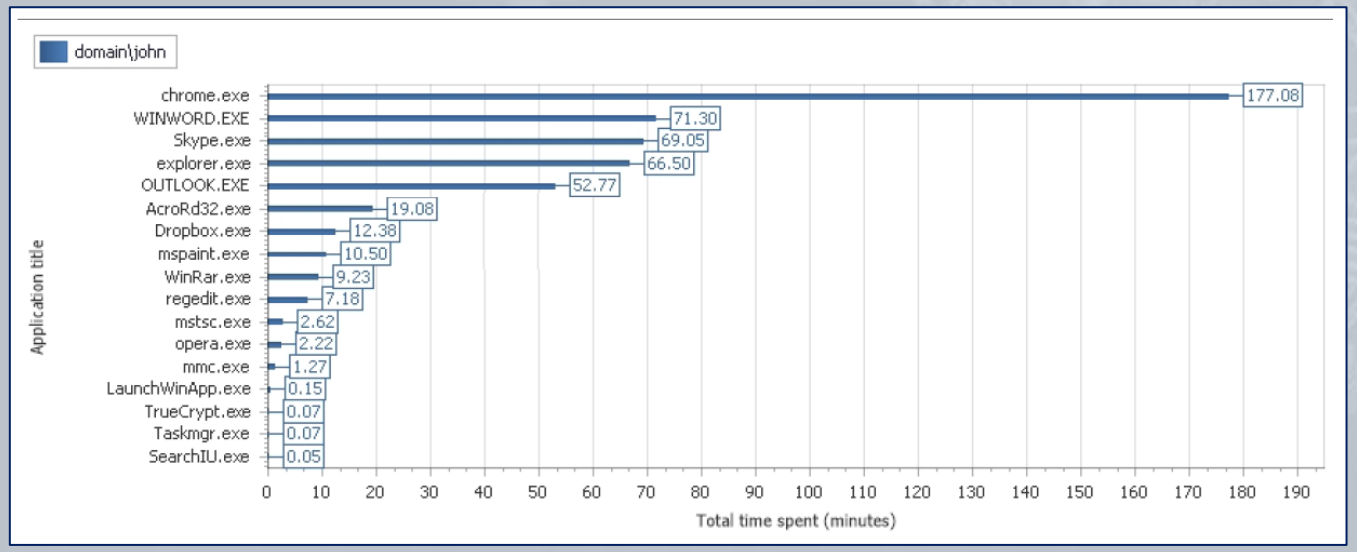
Client name	johnsmith-pc
Client description	Security AS group
User name	domain\john
Total time	6 hours, 42 minutes, 5 seconds
Active time	6 hours, 20 minutes

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



Report Types

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

Report Types

Ekran system

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.Simpson	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

Report Types

Ekran system

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/19TprsVorHH8GcdL0xnHmO8HKh7ww/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	

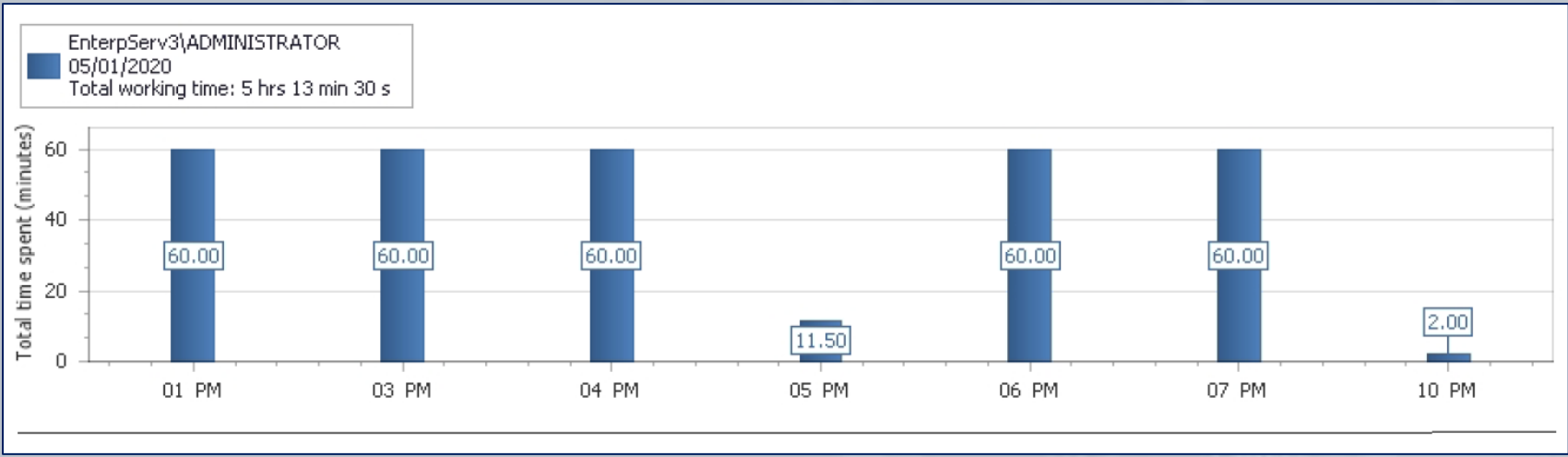
User Daily Activity Grid Report

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

Report Types

User Productivity Chart Report

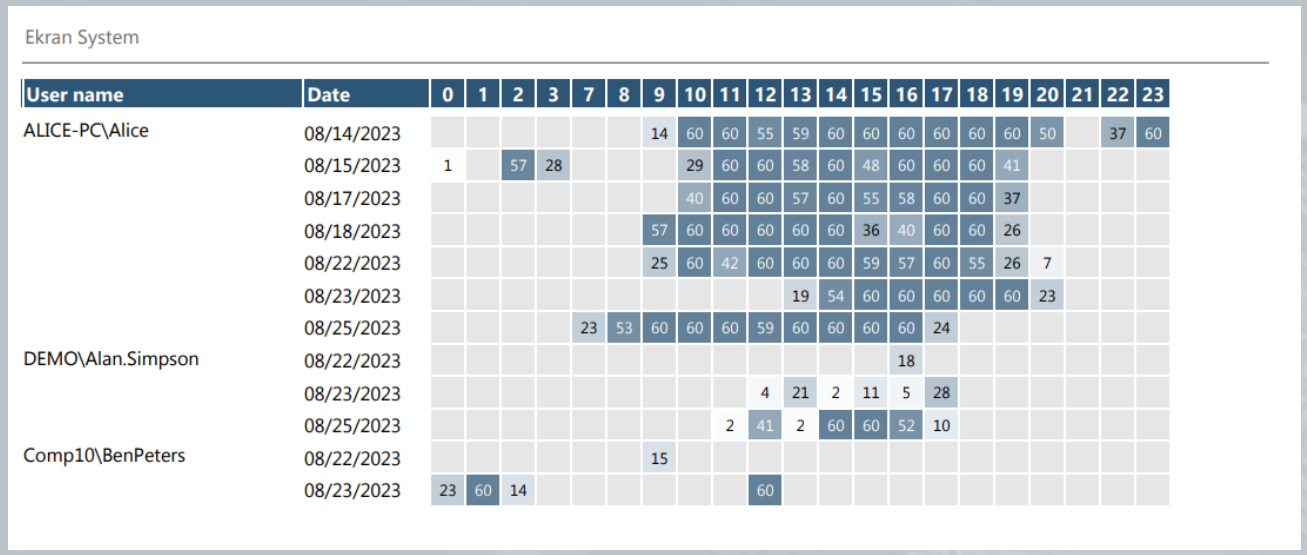


User Productivity Summary Grid Report

User Name	Date	Total Time Spent	Active Time	First Activity Time	Last Activity Time	Idle Time	Top 10 Applications	Top 10 URLs
COMP8\RobertOakley	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

Report Types

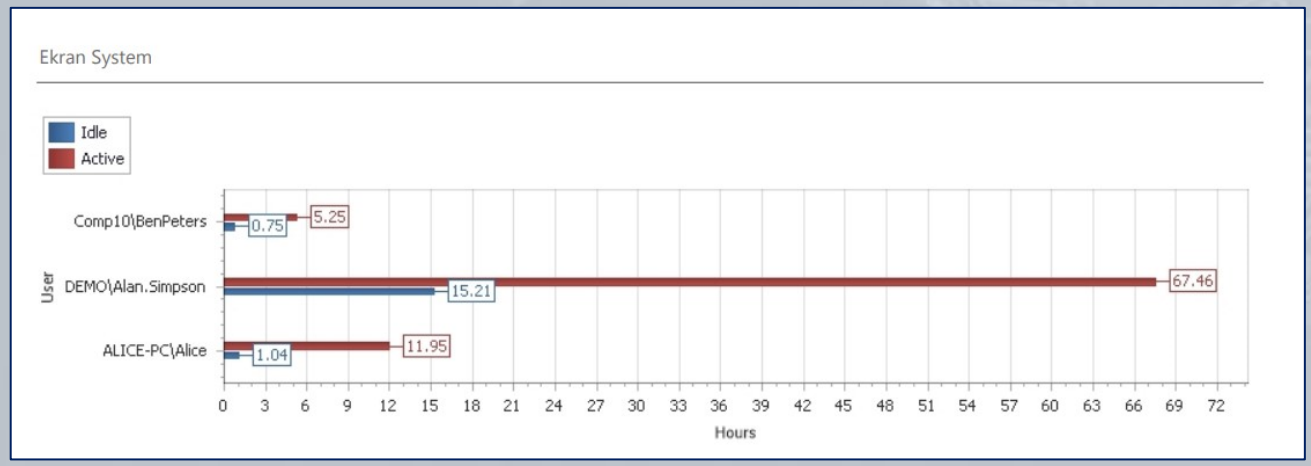
User Productivity Heatmap Report



Ekran System

User name	Date	0	1	2	3	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
ALICE-PC\Alice	08/14/2023							14	60	60	55	59	60	60	60	60	60	60	50		37	60
	08/15/2023	1		57	28				29	60	60	58	60	48	60	60	60	41				
	08/17/2023								40	60	60	57	60	55	58	60	60	37				
	08/18/2023							57	60	60	60	60	60	36	40	60	60	26				
	08/22/2023							25	60	42	60	60	60	59	57	60	55	26	7			
	08/23/2023											19	54	60	60	60	60	60	23			
	08/25/2023					23	53	60	60	60	59	60	60	60	60	24						
DEMO\Alan.Simpson	08/22/2023														18							
	08/23/2023										4	21	2	11	5	28						
	08/25/2023									2	41	2	60	60	52	10						
Comp10\BenPeters	08/22/2023							15														
	08/23/2023	23	60	14							60											

User Active Time and Idle Time Chart Report



Report Types

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

Report Types

User Behavior Analytics Report

Risk Level	Normal
Risk Score, %	50 - 1
Session number	3

Who	Where	When	Details	Session Score	Session URL
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

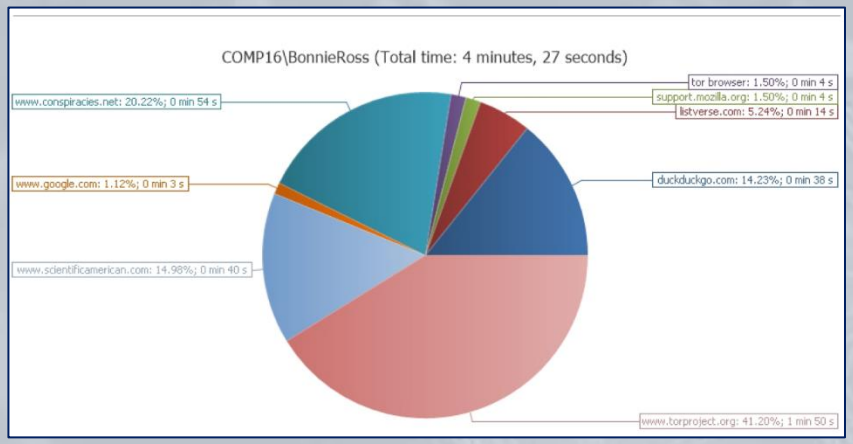
Report Types

URL Summary Grid Report

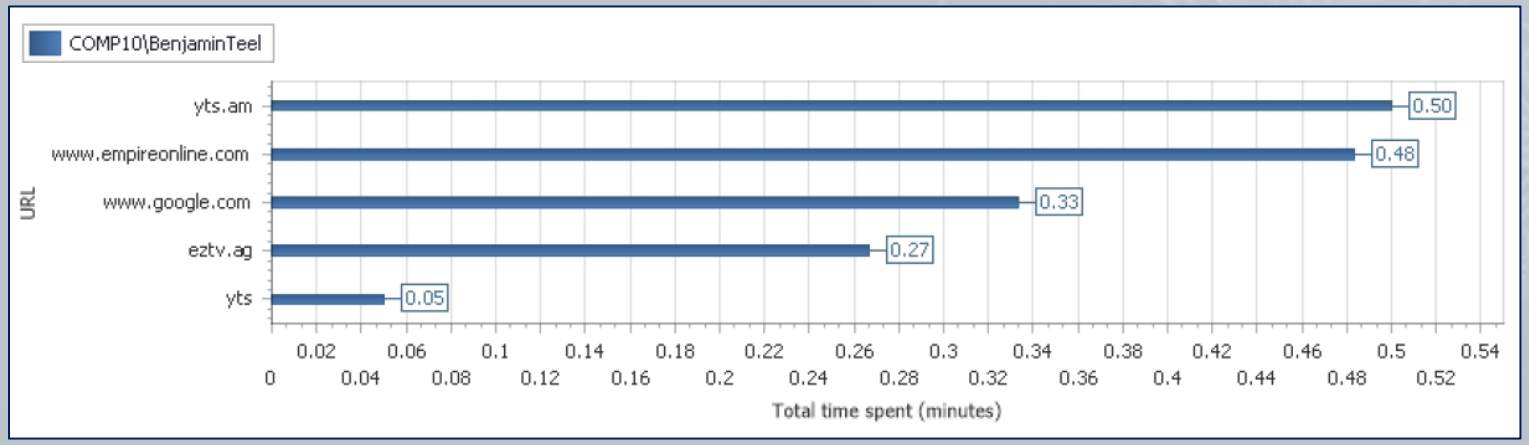
Client name	Comp15
Client description	Exporting HR Data
User name	COMP15\HelenPeterson
Total time	4 minutes, 33 seconds

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



Report Types

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\07A70E01AE6B1298
07/12/2018 04:23:38 PM	usb device blocking	Blocked	Critical	USB Mass Storage Device	USB\Class_08&SubClass_06&Prot_50; USB\VID_13FE&PID_3600&REV_0100\07A70E01AE6B1298

Report Types

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

Report Types

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

Report Types

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

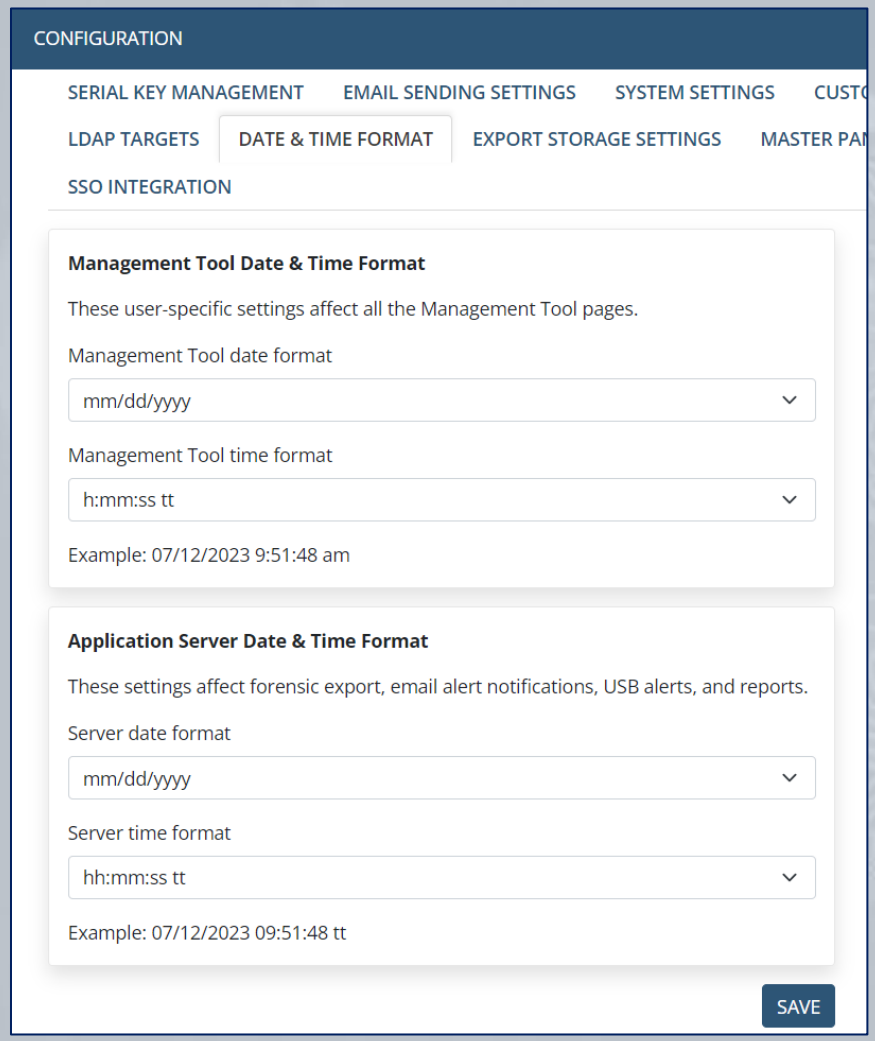
Audit Session Grid Report

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.

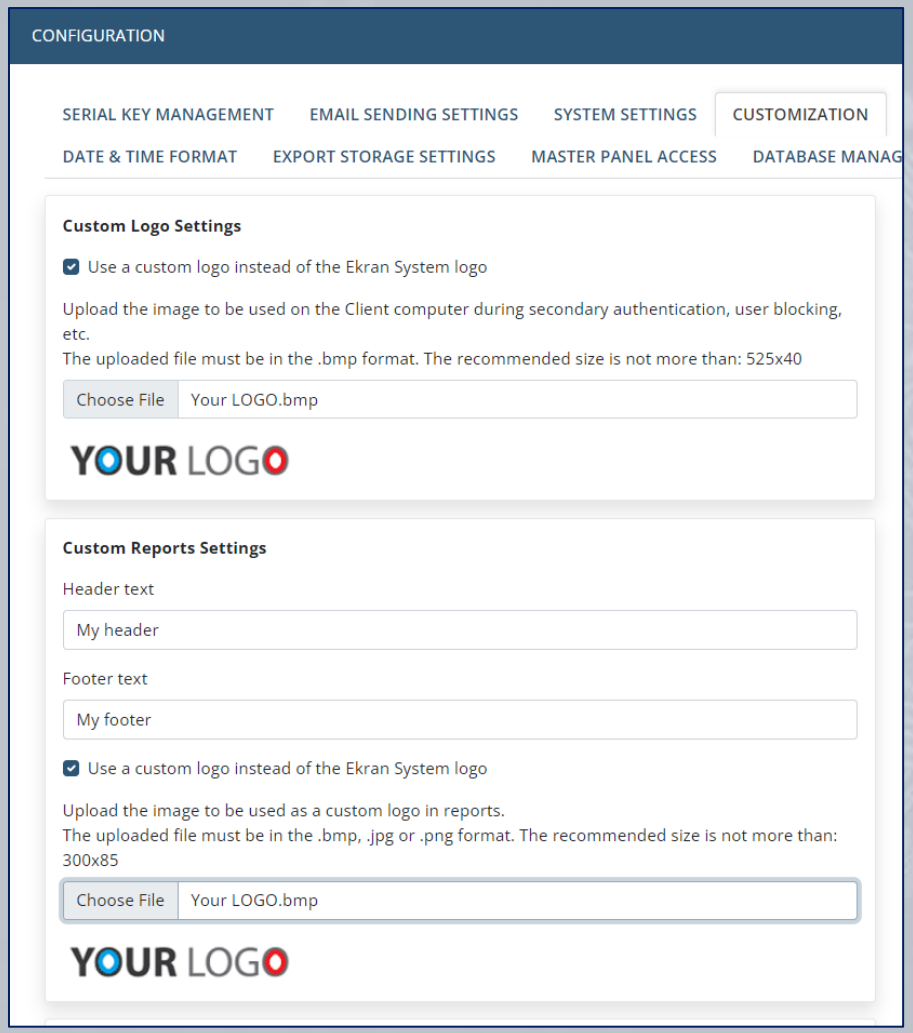


Customizing the Logo on Client Notifications

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.

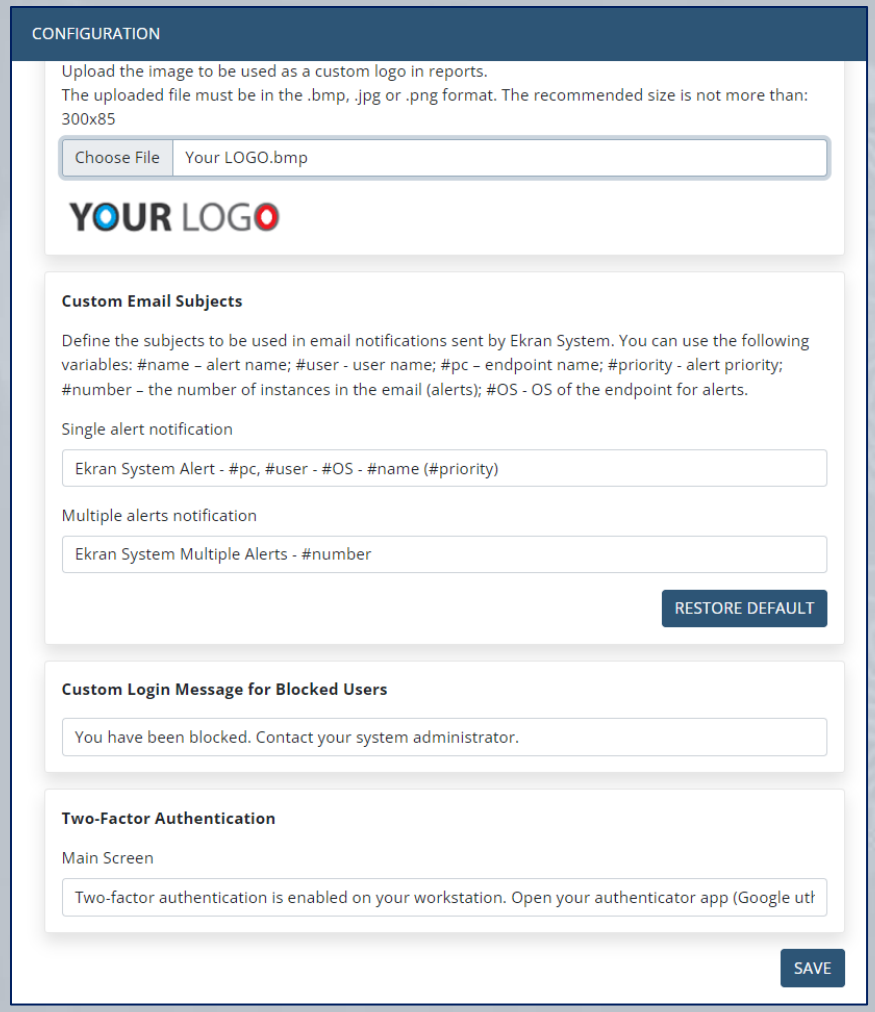
Customizing Reports

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.



Customizing Email Subjects and Messages

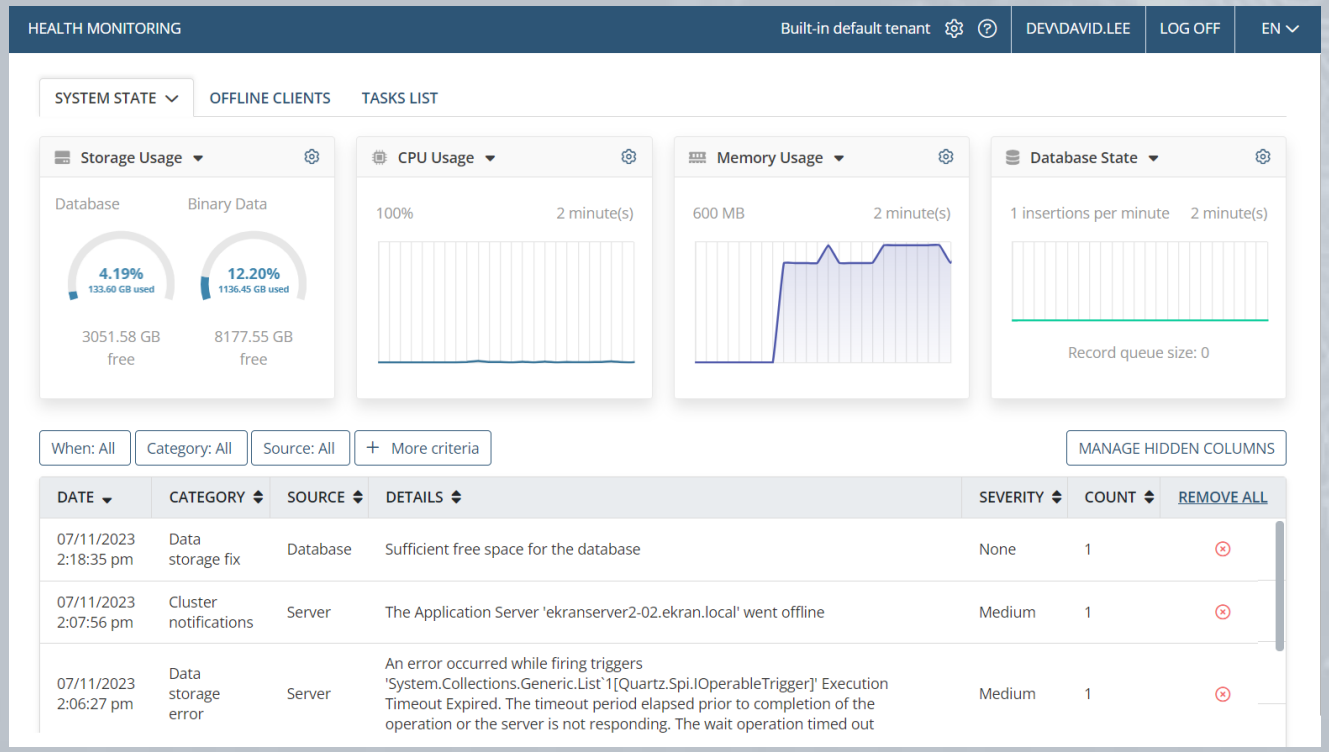
Custom settings allow you to **specify** the **subjects** to be used in **email notifications**, and other various messages, sent by Ekran System.



Health Monitoring

System Health Monitoring

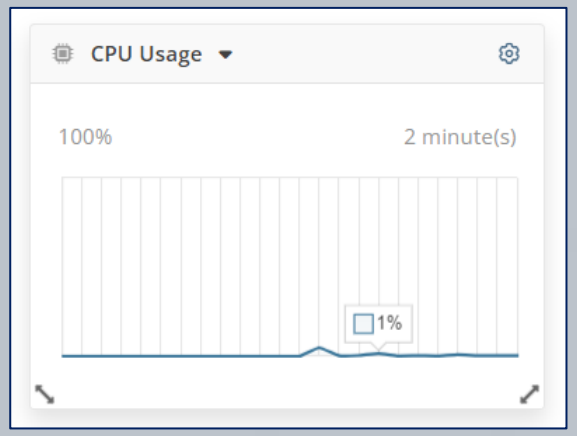
System Health Monitoring allows you to get detailed information about e.g. **database storage usage** and any system **errors** and **warnings** to assist you in monitoring the system “health” and **reacting** to any issues in a **timely** manner.

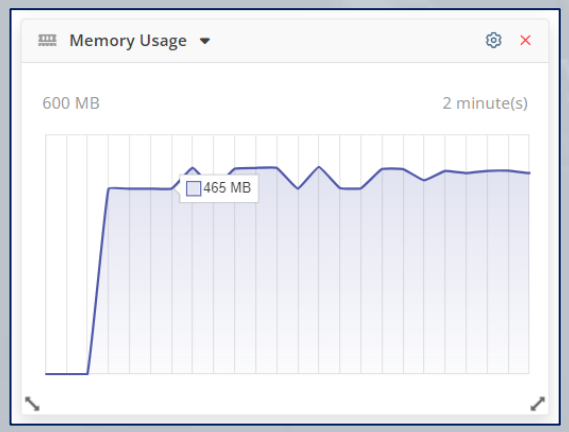


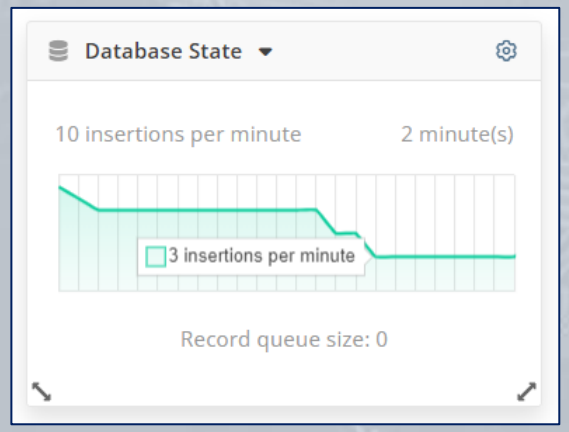
Server Resource Monitoring

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**

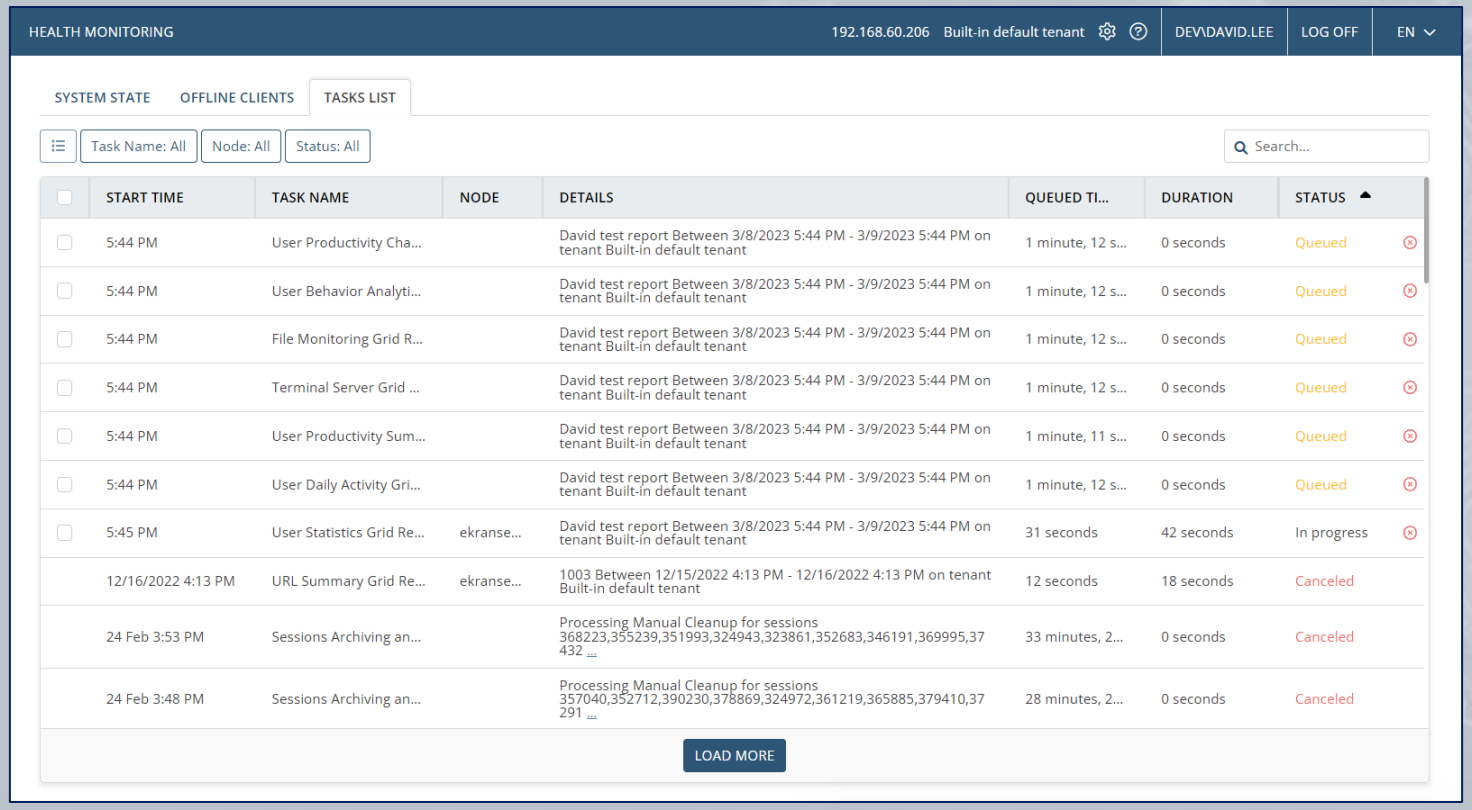






The Tasks List

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).



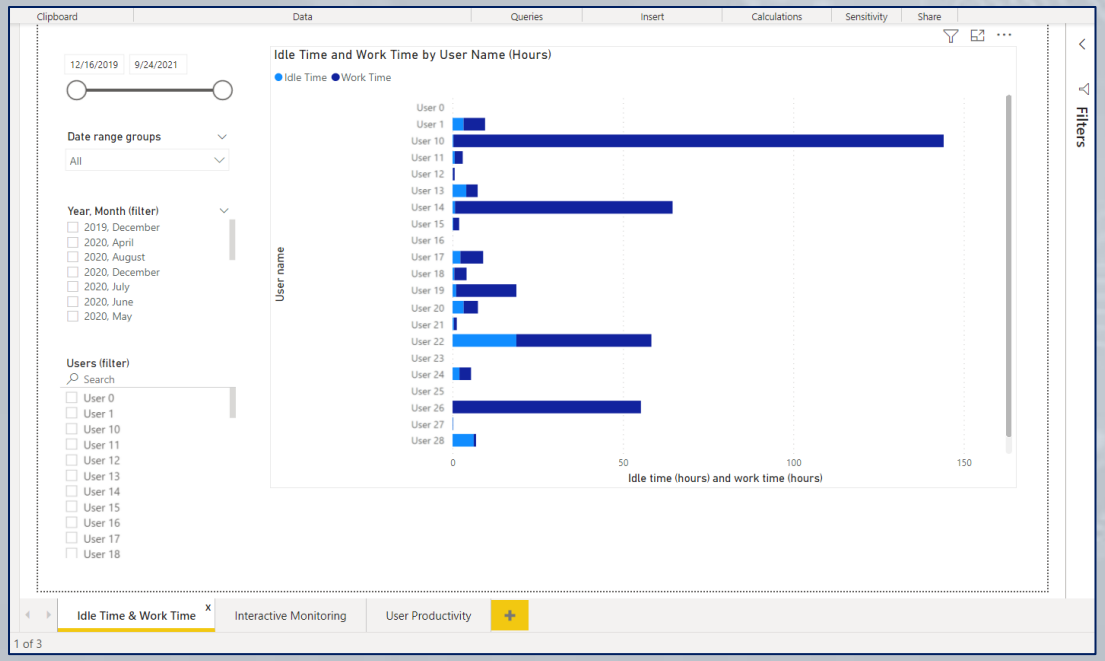
Ekran System API
(& Integration with e.g. Power BI)

Ekran System Data Connector

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**.

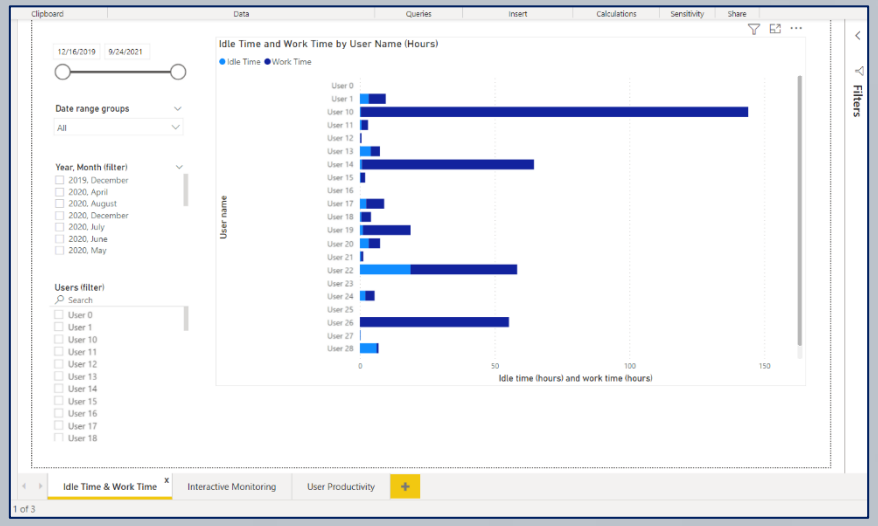
Idle Time & Work Time Report



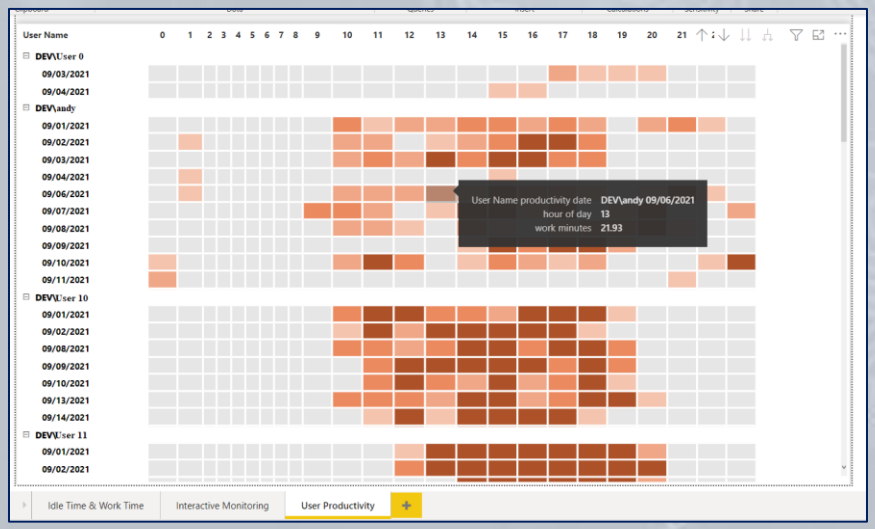
Ekran System Data Connector

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



Ekran

Visit us online:

www.ekransystem.com