Syteca

# Full Feature Presentation

**Syteca**
Enterprise Cybersecurity Platform

# Contents

# System Overview

# About the System

Syteca

## A Privileged Access Management (PAM) & User Activity Monitoring (UAM) Solution

### Privileged Activity Monitoring

Syteca 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/Unix** 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 **detect and control** the use of **sensitive data**?

### Privileged Access and Session Management

Syteca 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

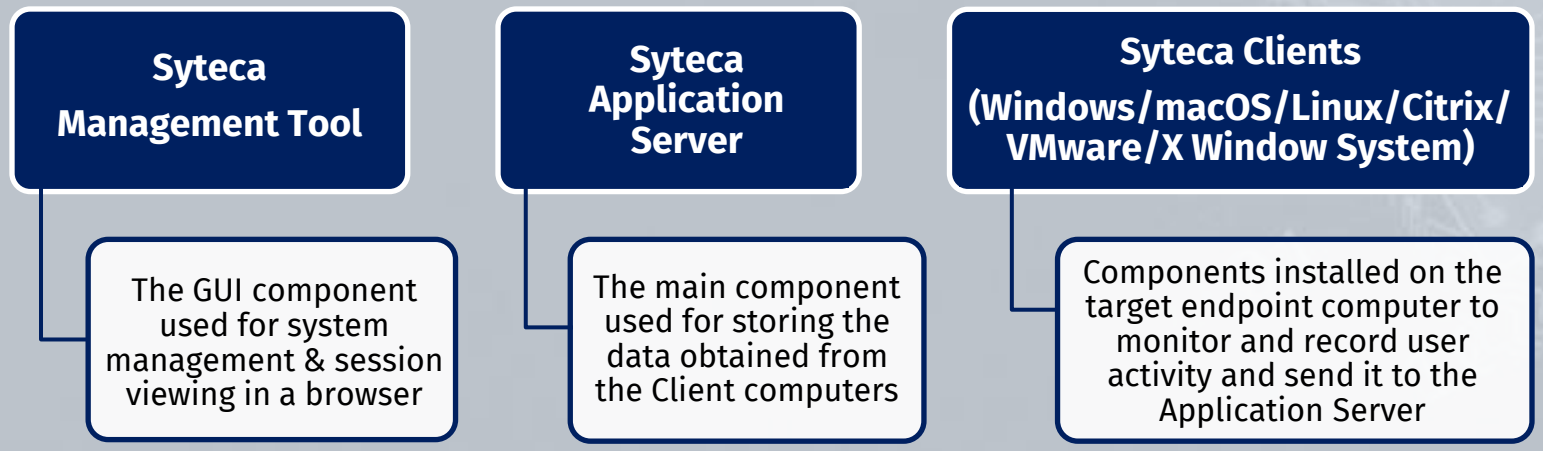
Syteca supports the **widest range of platforms and infrastructure** configurations on the market, delivering reliable **deployments of any size**, from piloting dozens to tens of thousands of endpoints. **Flexible licensing** helps to fit it into your budget and address project changes.

# About the System

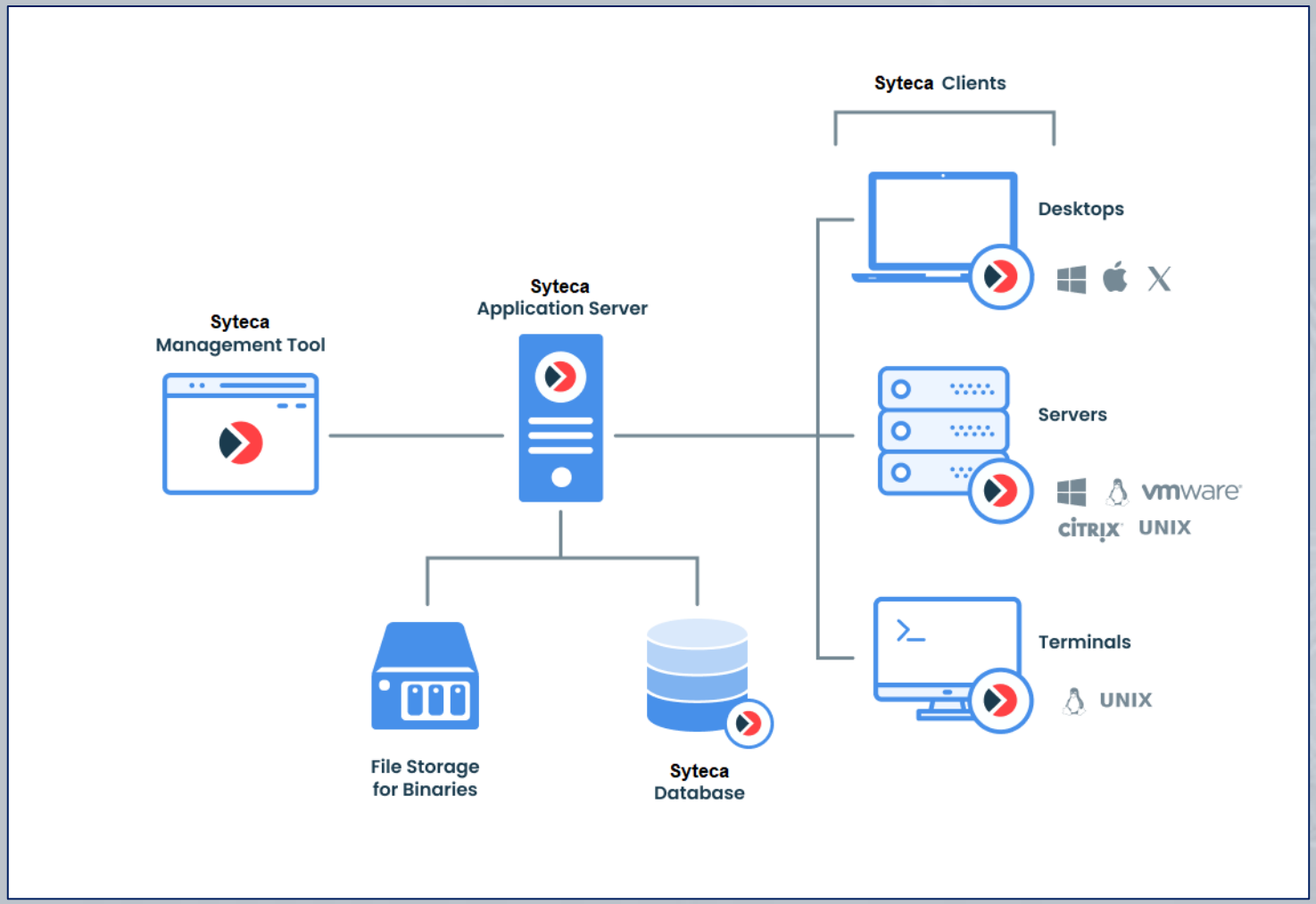
**Syteca** (formerly **Ekran System**) is an enterprise-level **cybersecurity platform** software solution featuring **privileged access management (PAM)** and **user activity monitoring (UAM)**. It is used to **protect** your corporate IT infrastructure from **internal risks**, as well as to assist you in meeting **compliance requirements** (e.g. GDPR), manage **privileged user access (PAM)**, immediately respond to potential incidents, and much more.

You can **record** all terminal, remote, and local **user sessions**, and **alert** security personnel to suspicious events, and Syteca is available in both **on-premises** and **SaaS deployments** for **monitoring user activity** on **Windows**, **macOS** and **Linux** (incl. **SELinux**, **Solaris**, Ubuntu using **Wayland**, etc.) Client computers.

## The Main Components of Syteca



# The Basic Deployment Scheme

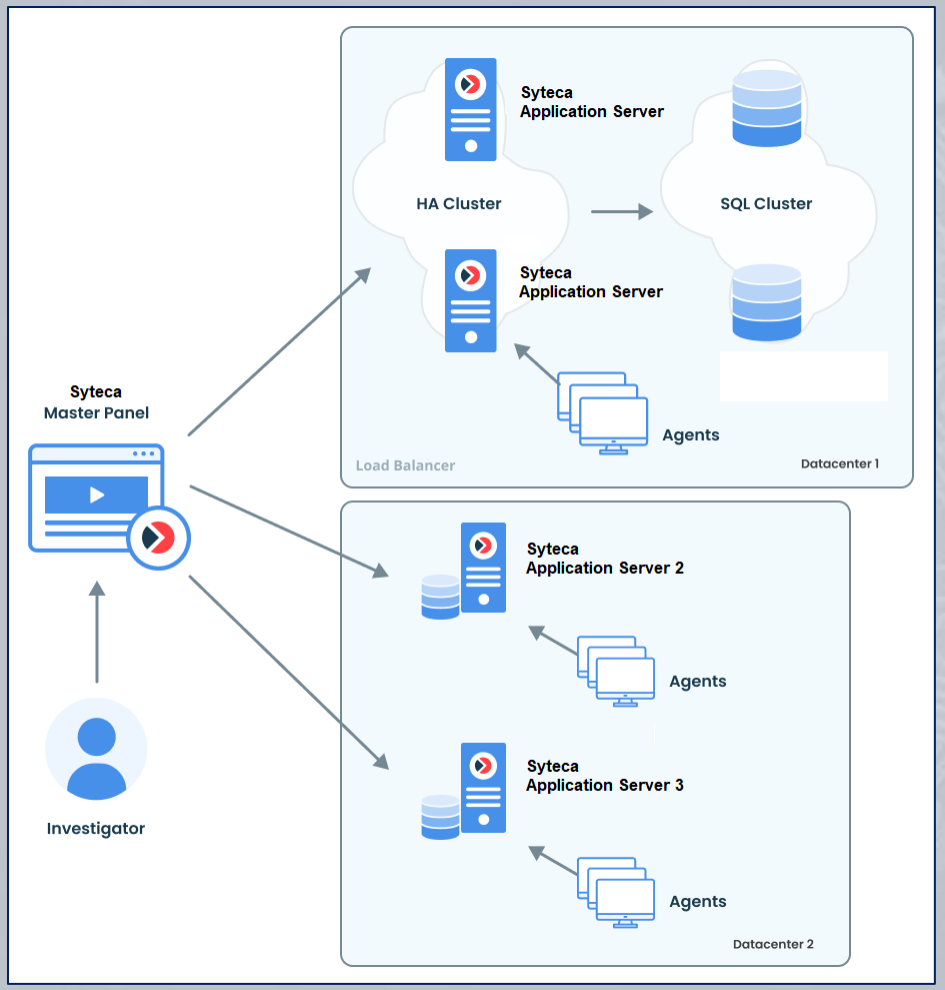


# Large-Scale Deployments

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.

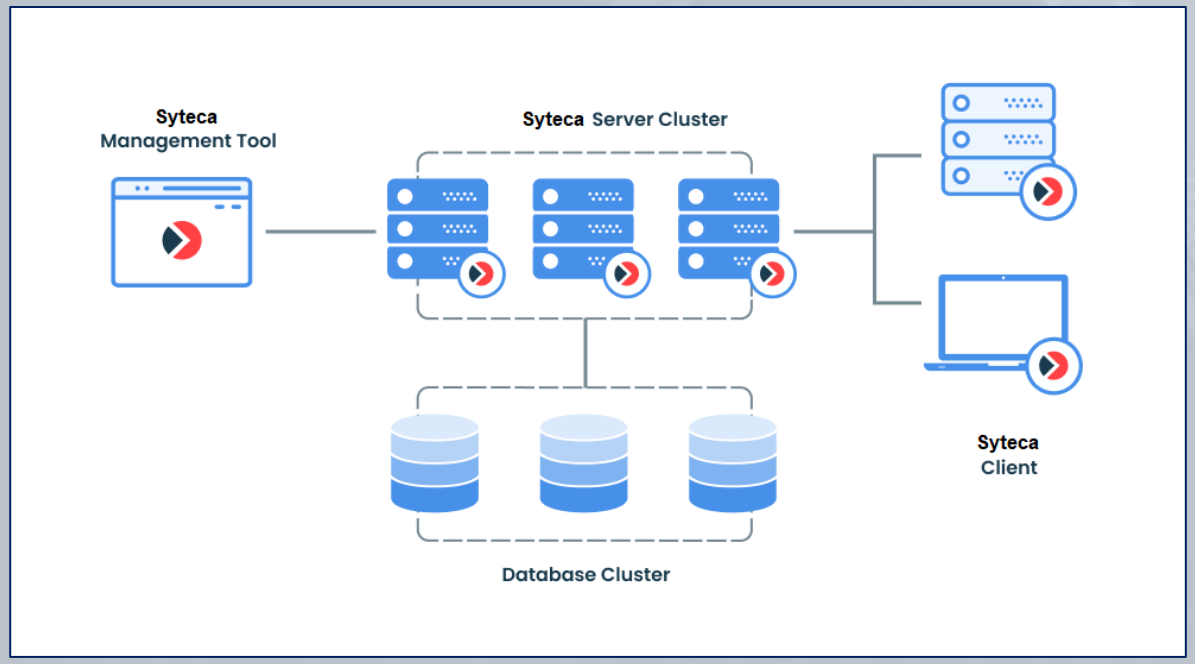
For complex deployments, Syteca also offers **high availability & disaster recovery**, and **multi-tenant** mode, as well as supports the use of third-party **load balancing** software.

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



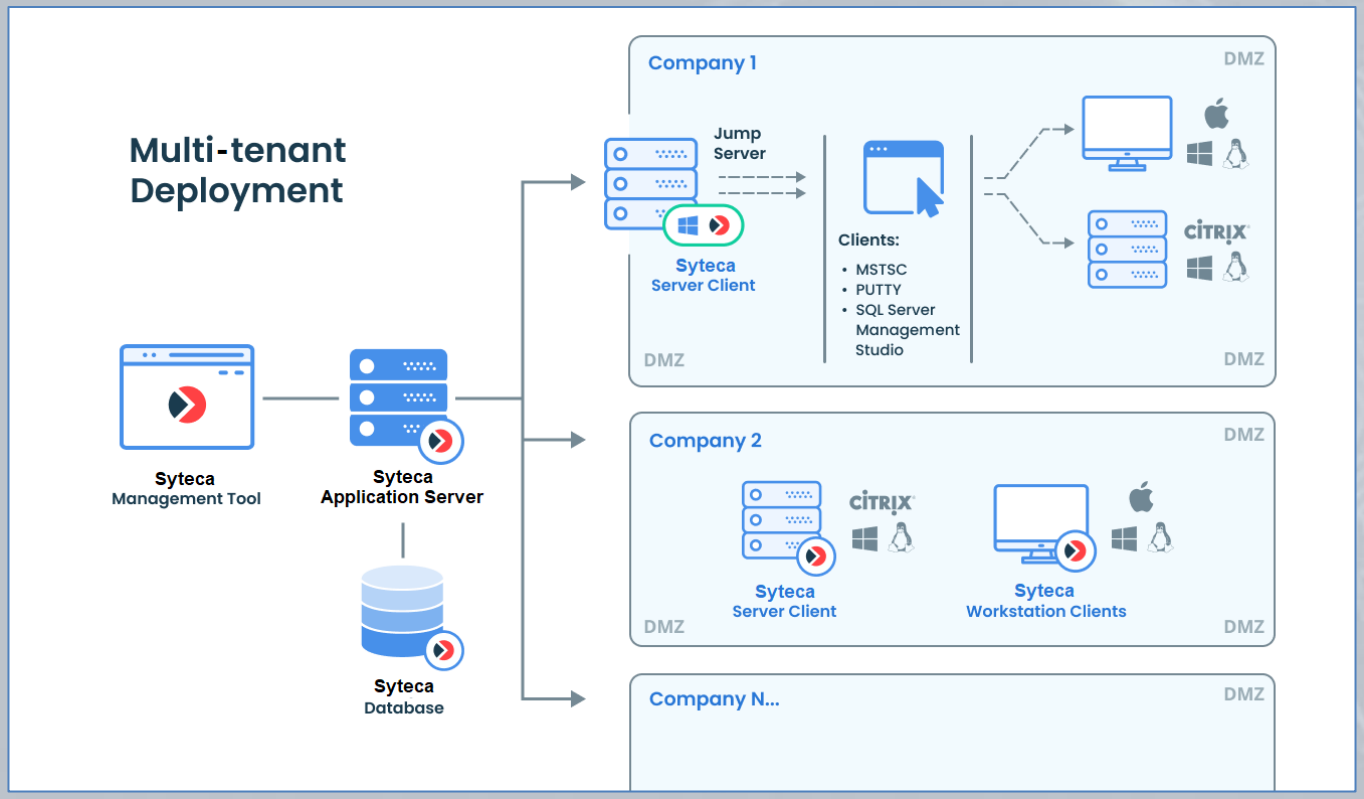
# High Availability Mode

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



# Multi-Tenant Mode

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

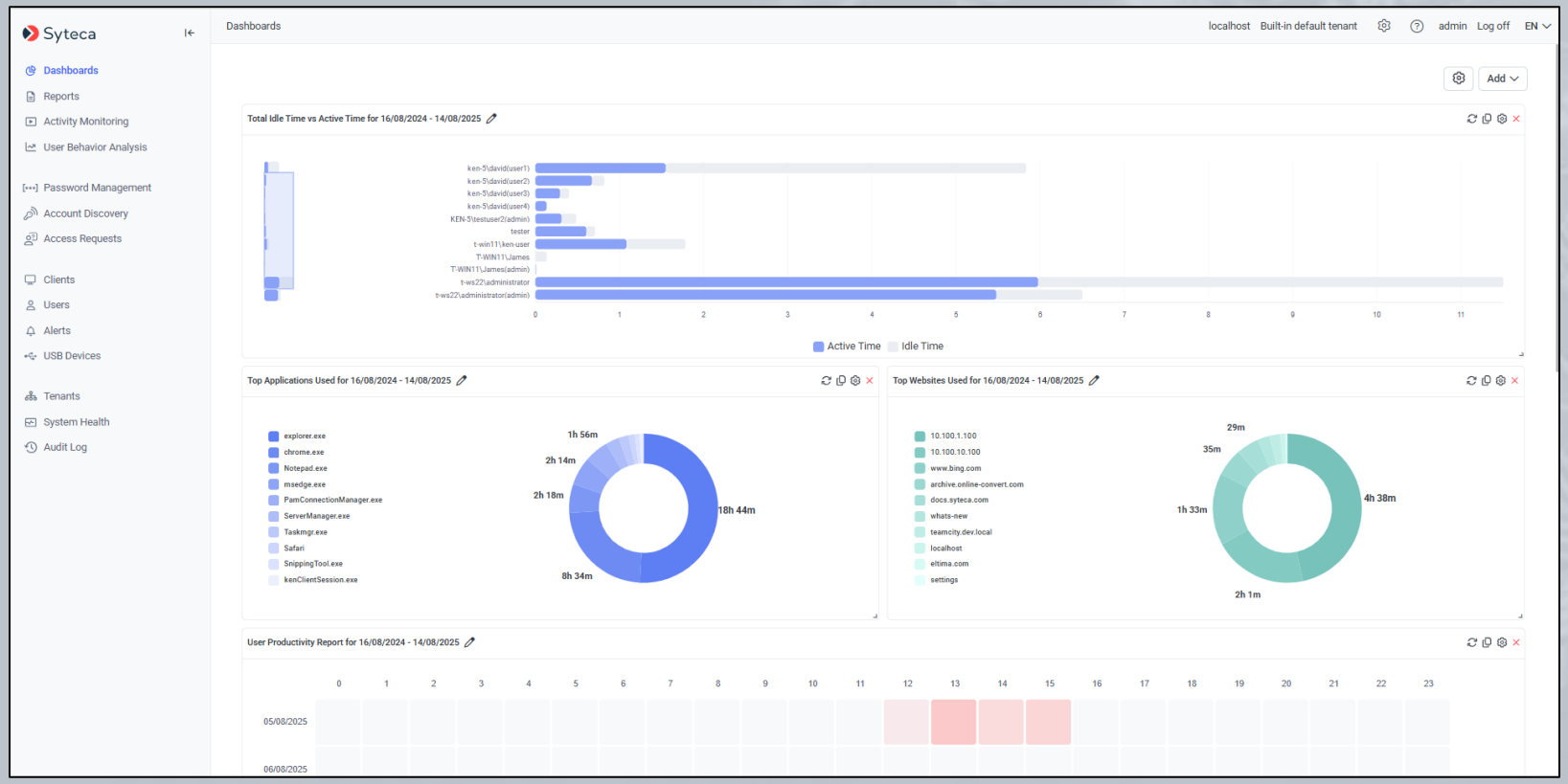


# Syteca Application Server & the Management Tool

(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.



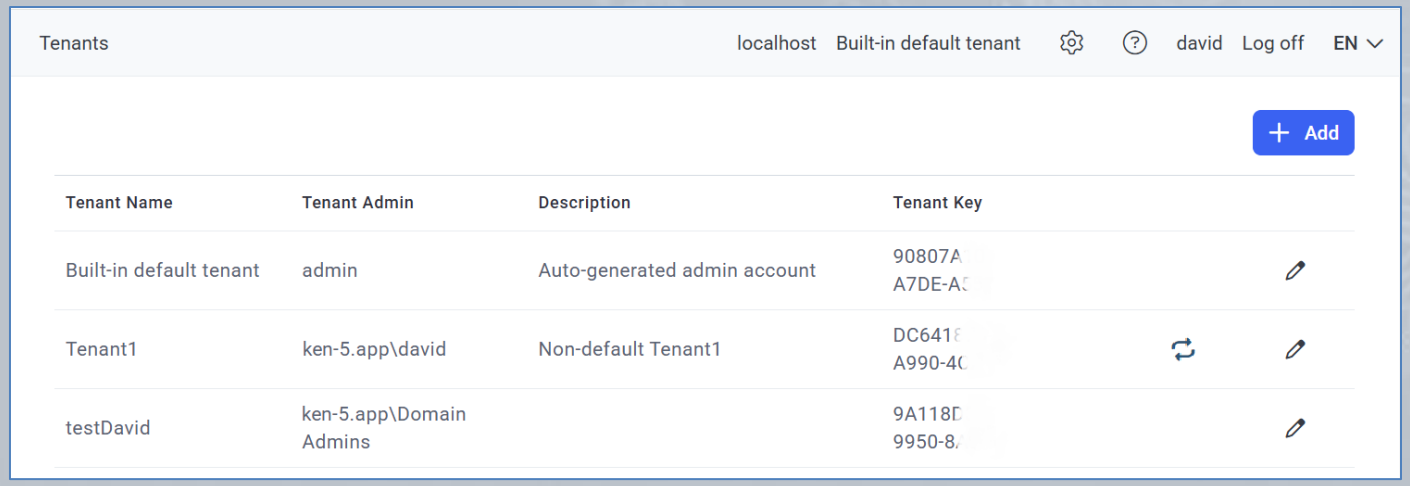
# Tenants

Syteca 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**.

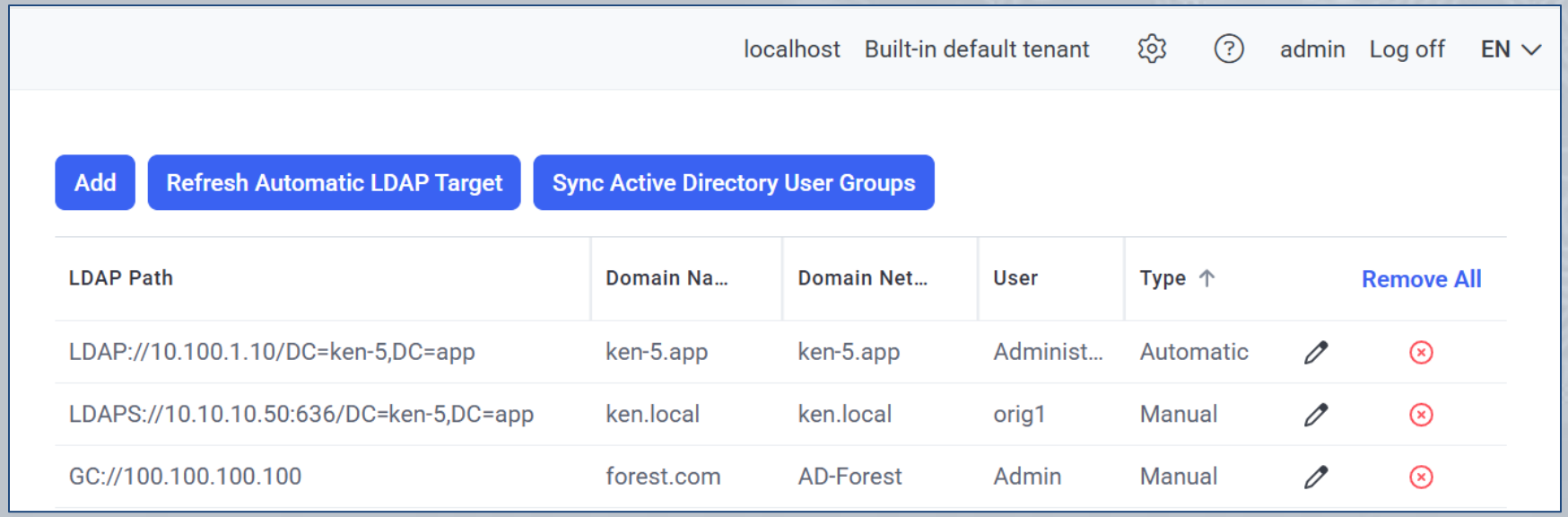


# Active Directory Integration

Syteca

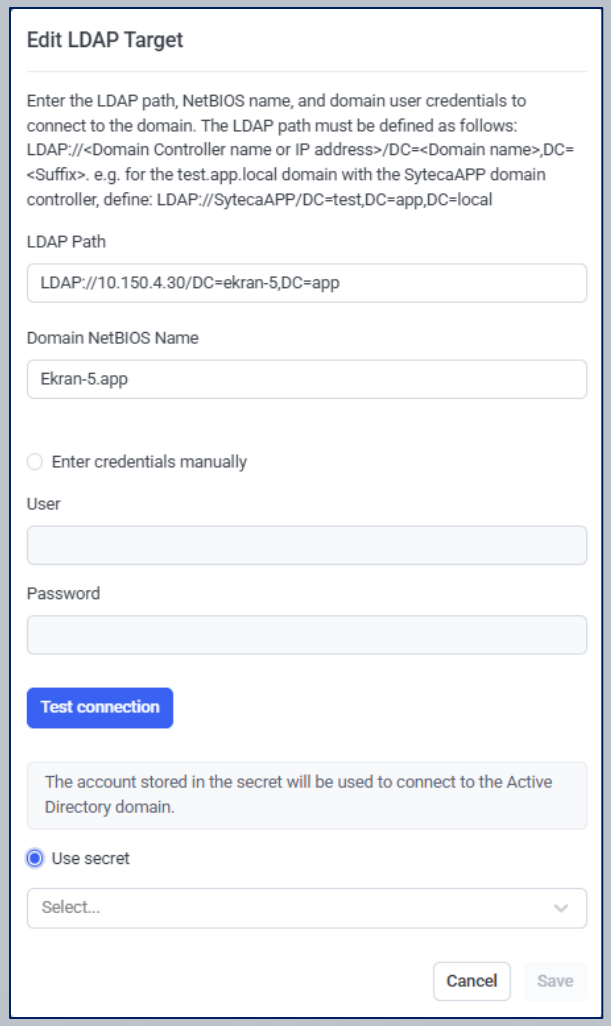
Integration with Active Directory (AD) allows you to establish domain trusts with **multiple domain** controllers by adding **LDAP targets**.

An **AD global catalog** can also by added as a single LDAP target to add **all the domains (and subdomains) in an AD forest** (without needing to add each domain in the AD forest as a separate LDAP target).

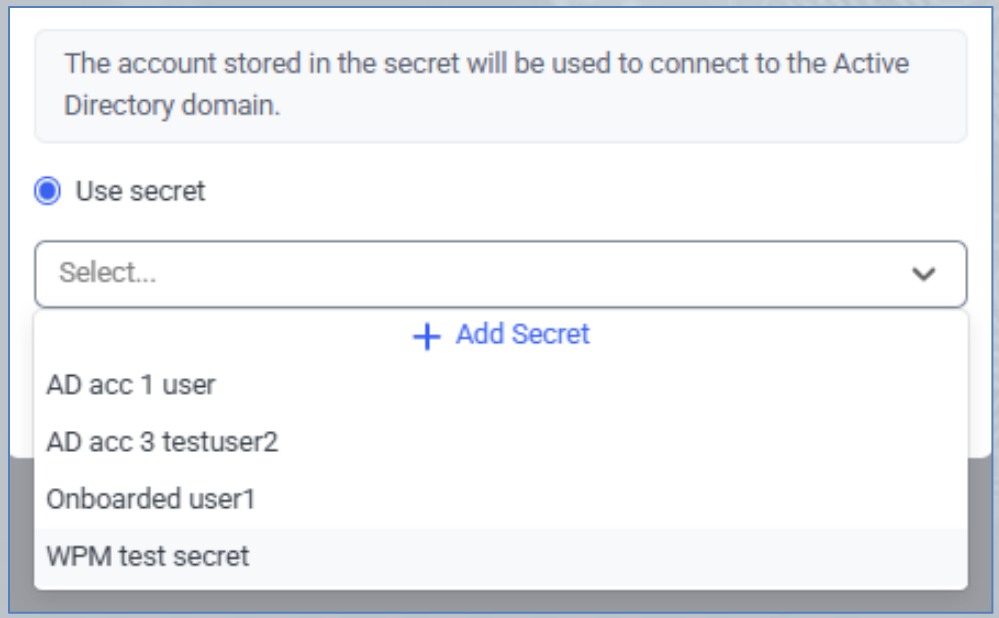


# Active Directory Integration

Syteca




The **account** used in an LDAP target can optionally be **stored in a secret** (e.g. for security reasons).

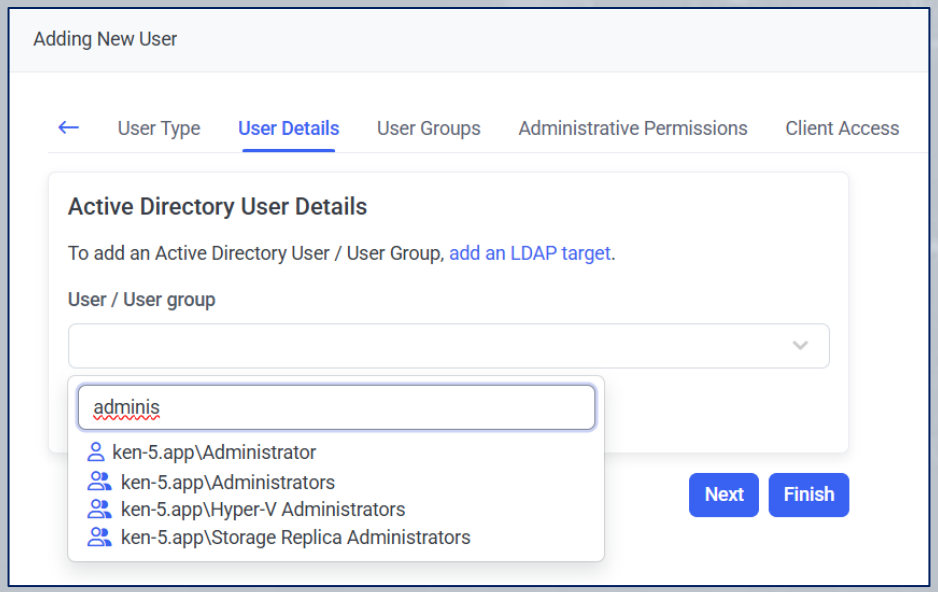


# Active Directory Integration

Syteca

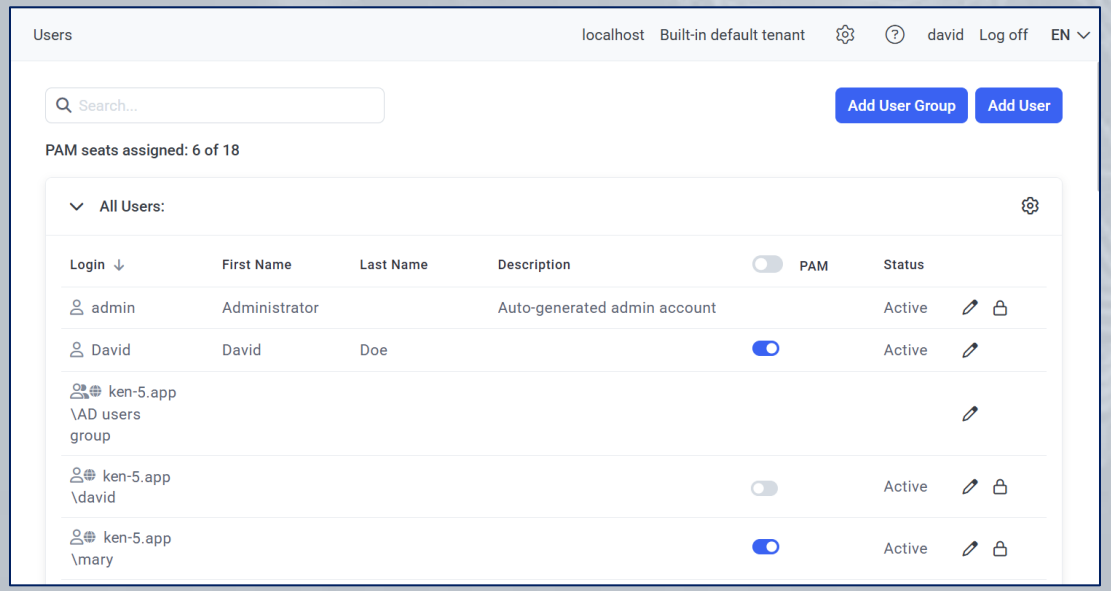
Integration with Active Directory allows you to do the following:

- 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.



# User Management & Permissions

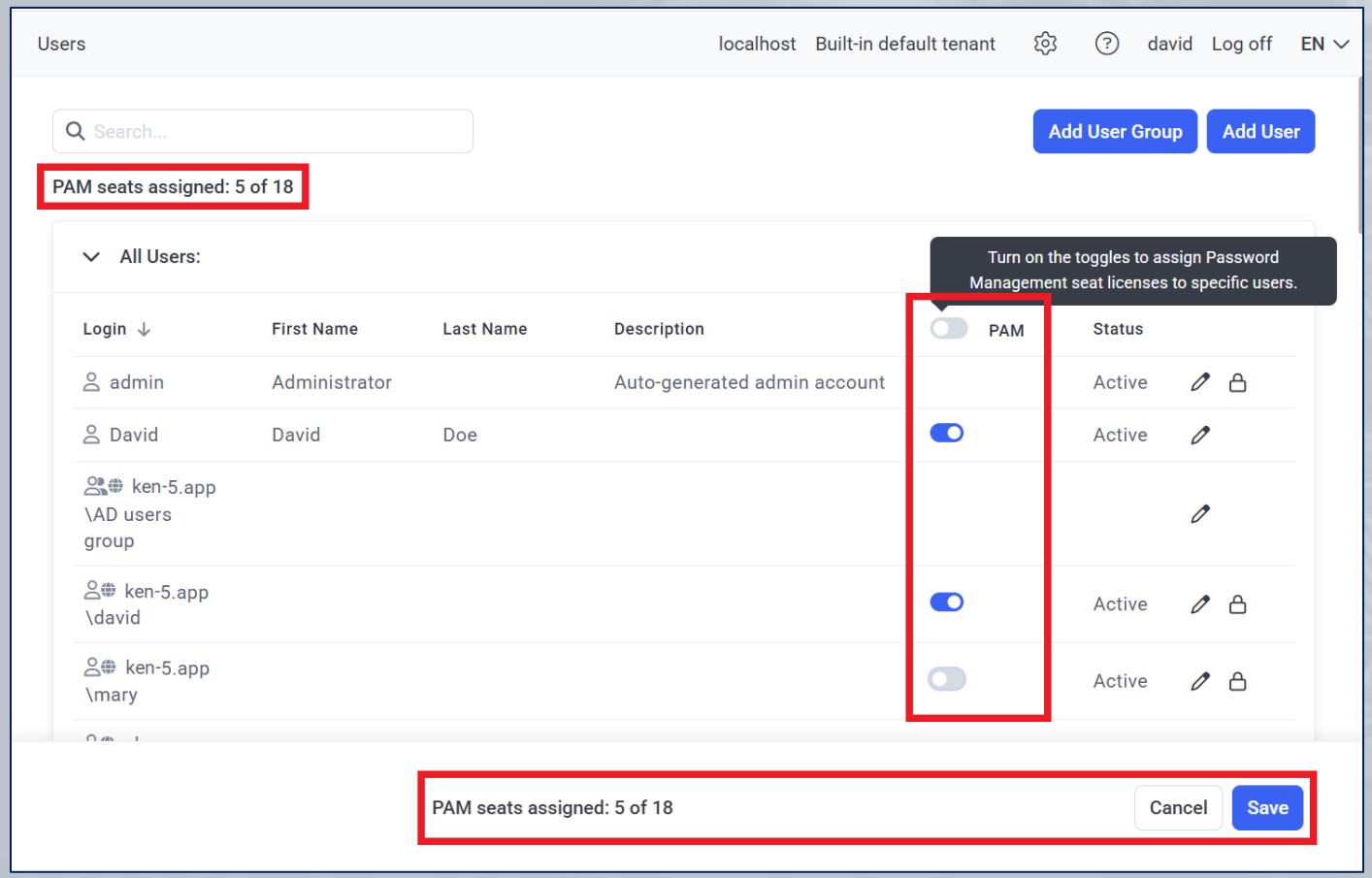
- Create **3 types of users**: Internal, Active Directory (Windows/macOS domain users/groups) or application accounts.
- Use **groups** for easier management of users, and define **permissions** for users/groups.
- The built-in default **“admin” user** of the system can be **disabled** for security reasons (if required).



# Assign PAM Licenses to Users

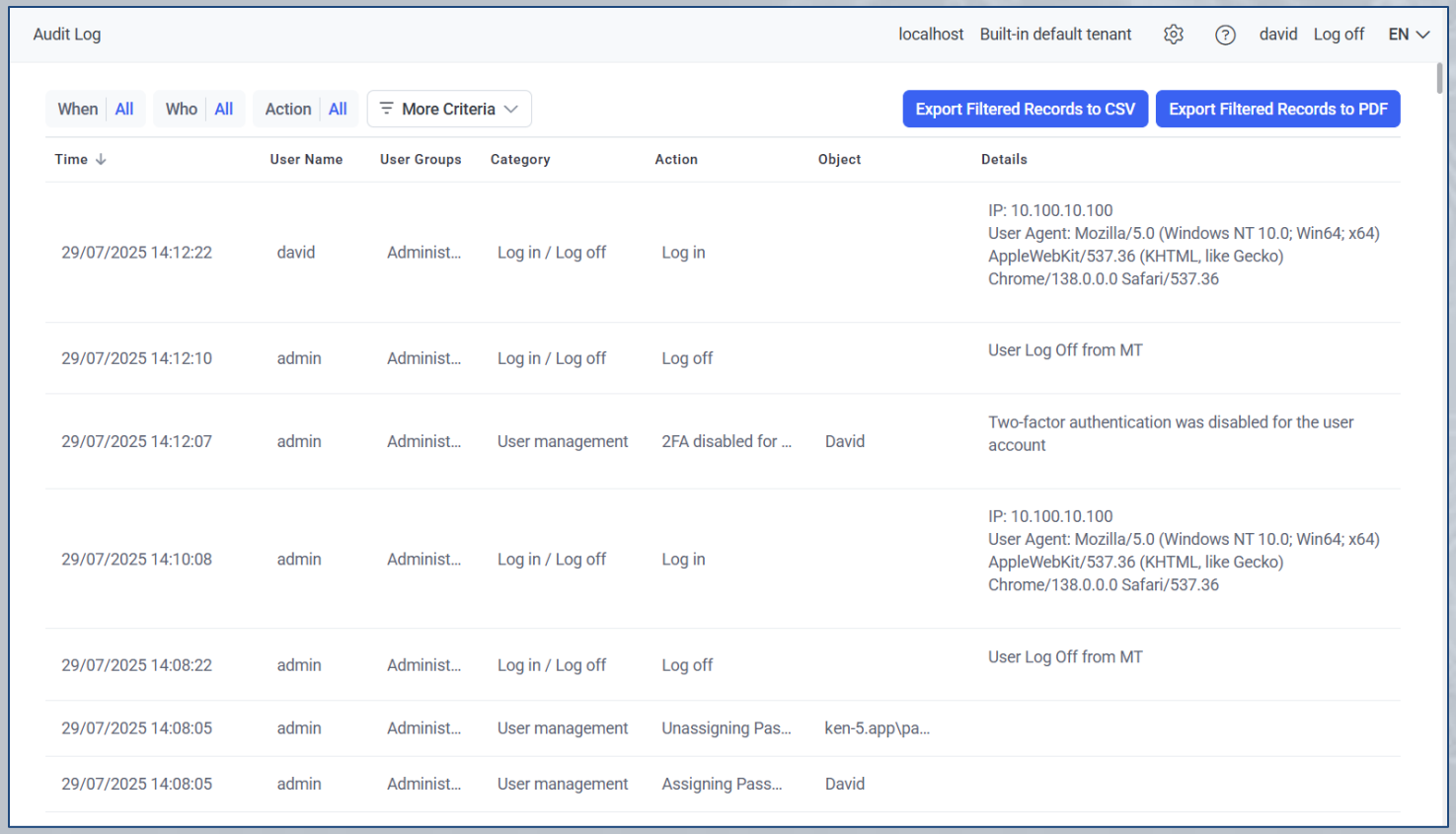
Syteca

- Assign **PAM seat licenses** to Privileged Access Management (PAM) users.



# The Audit Log

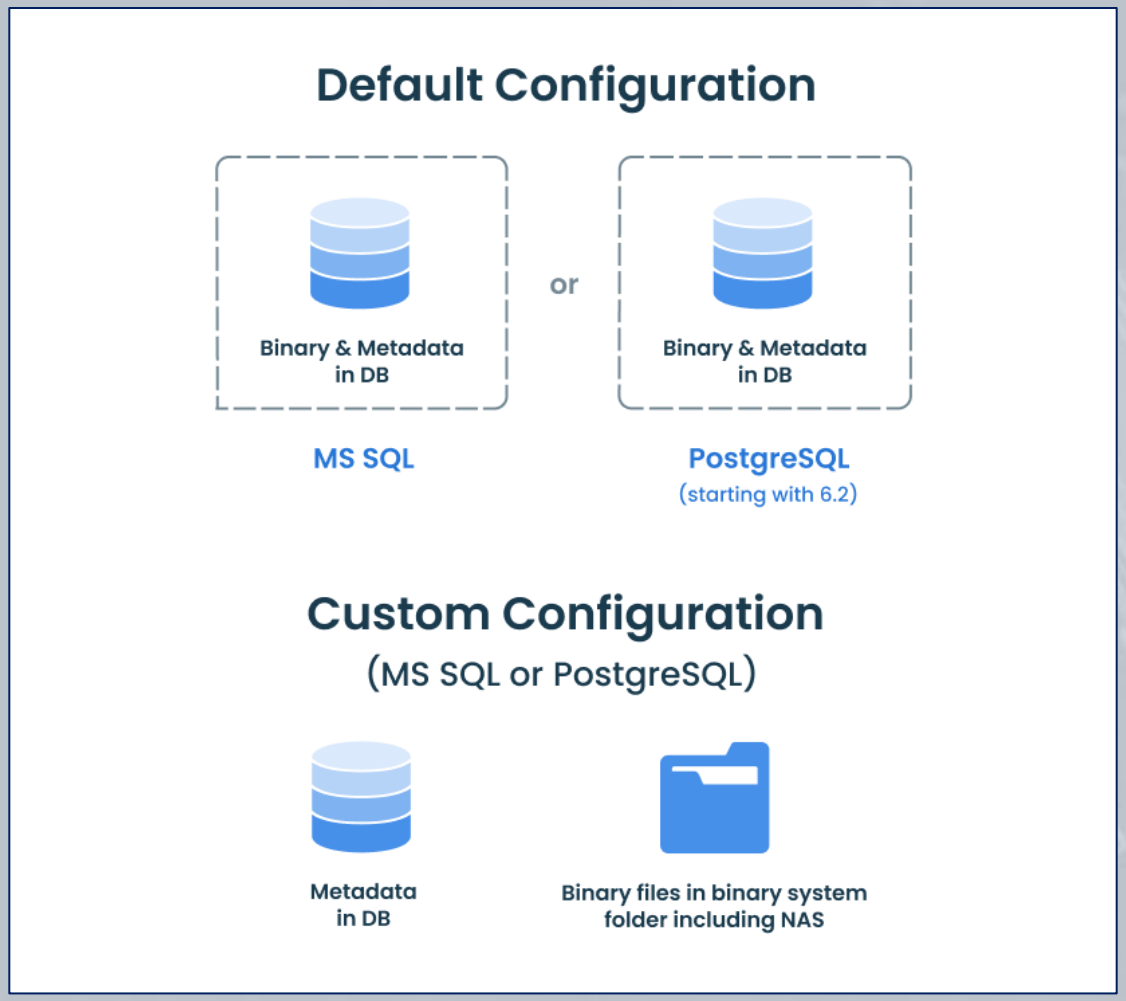
Audit all **user activities** performed in the Management Tool via the Audit log which contains detailed information on **all changes**.



# Database Management

# Database Configuration

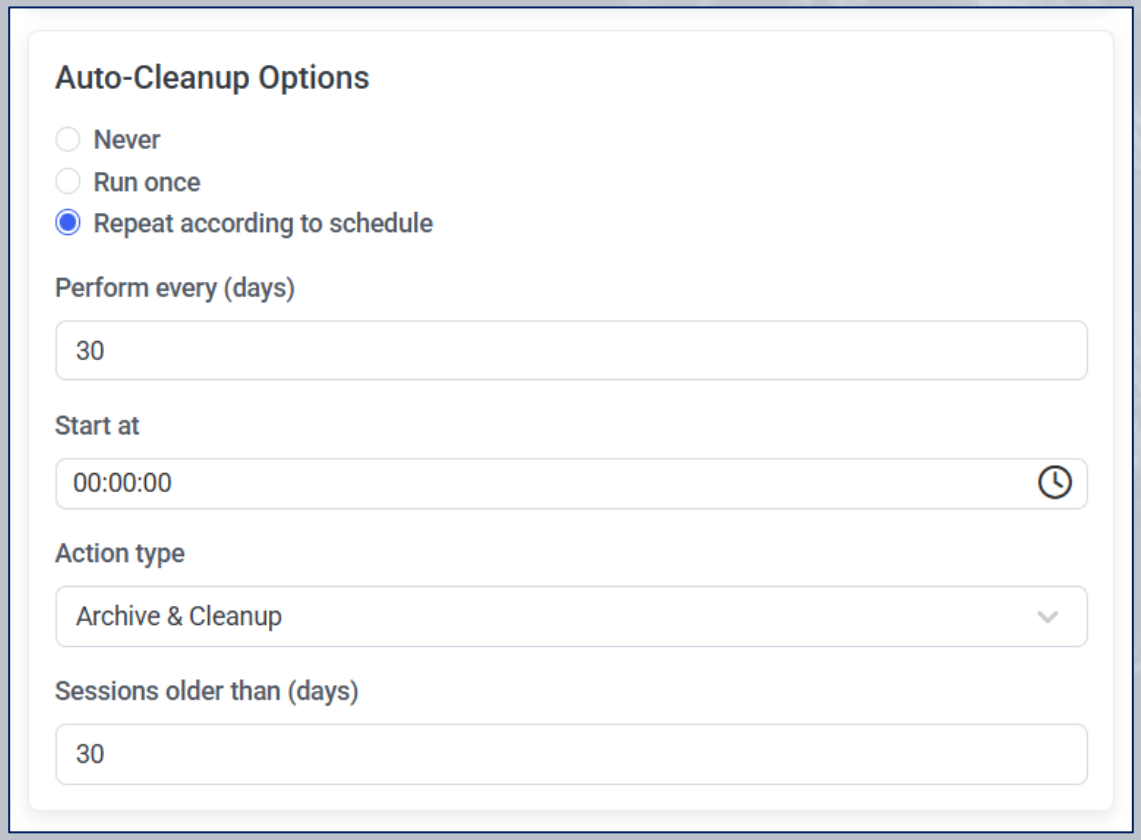
Syteca



# Database Cleanup

Syteca

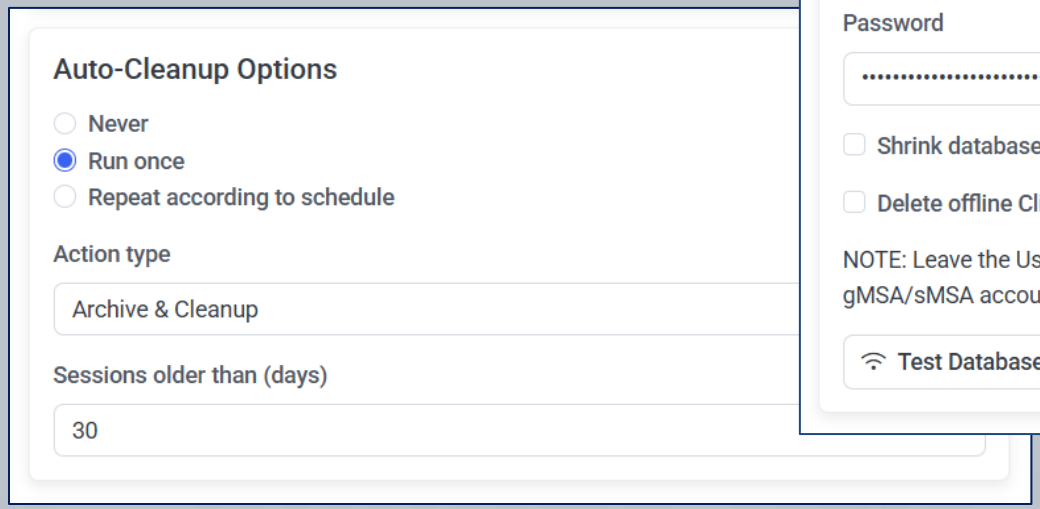
You can configure a **Cleanup** (or **Archive & Cleanup**) operation that can be applied to either a specific **Client** or a specific **Client group**.

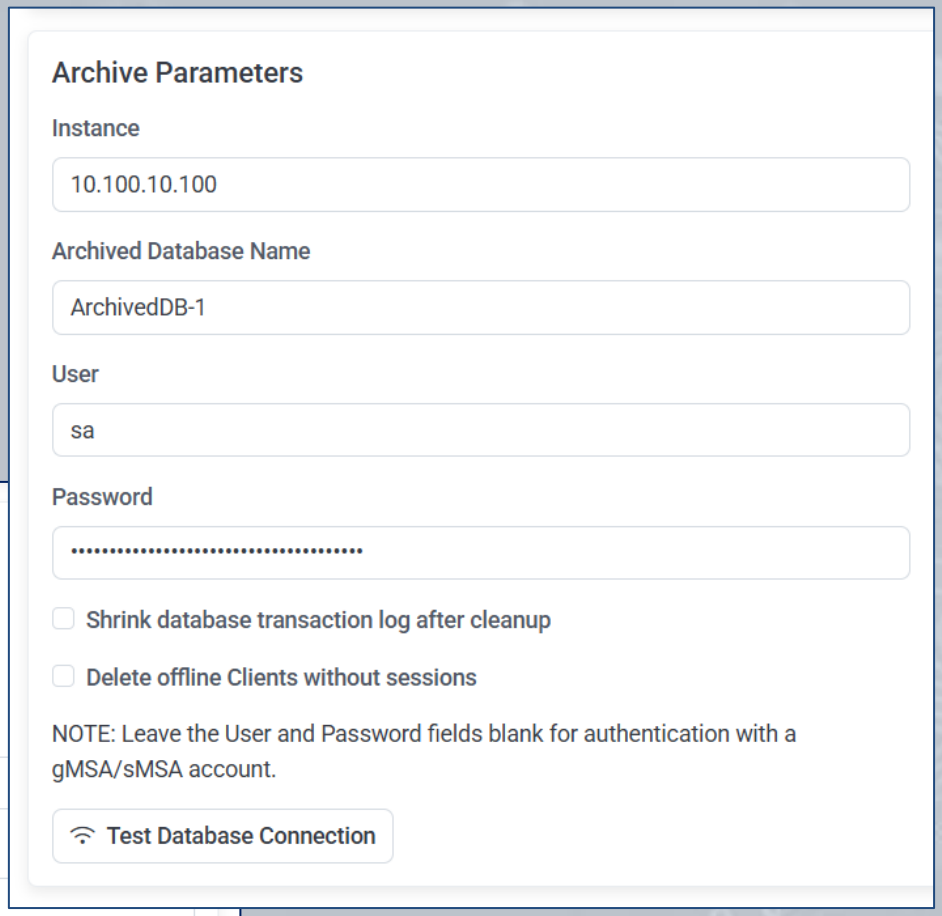


# Database Archiving

Syteca

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**.

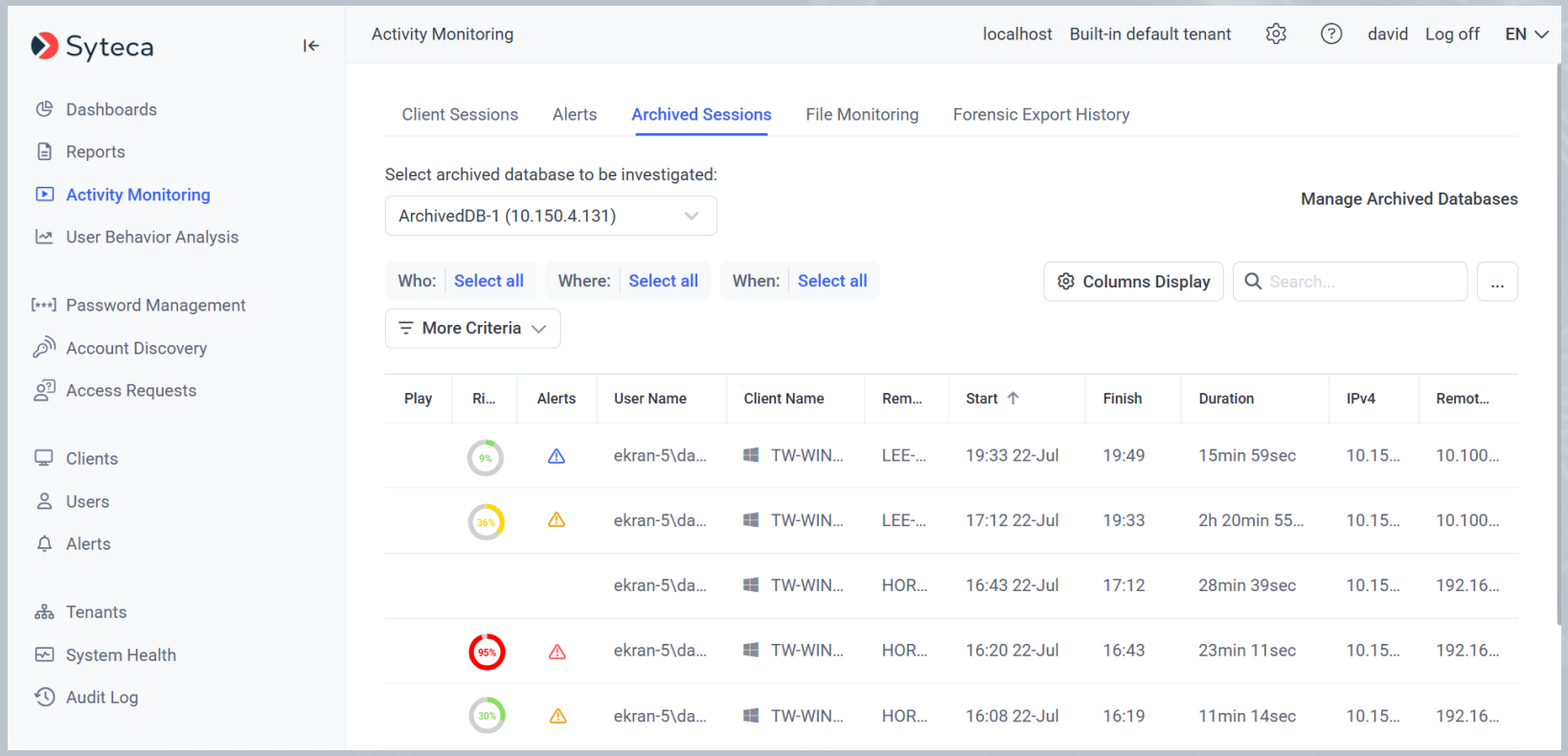


# Database Archiving

Syteca

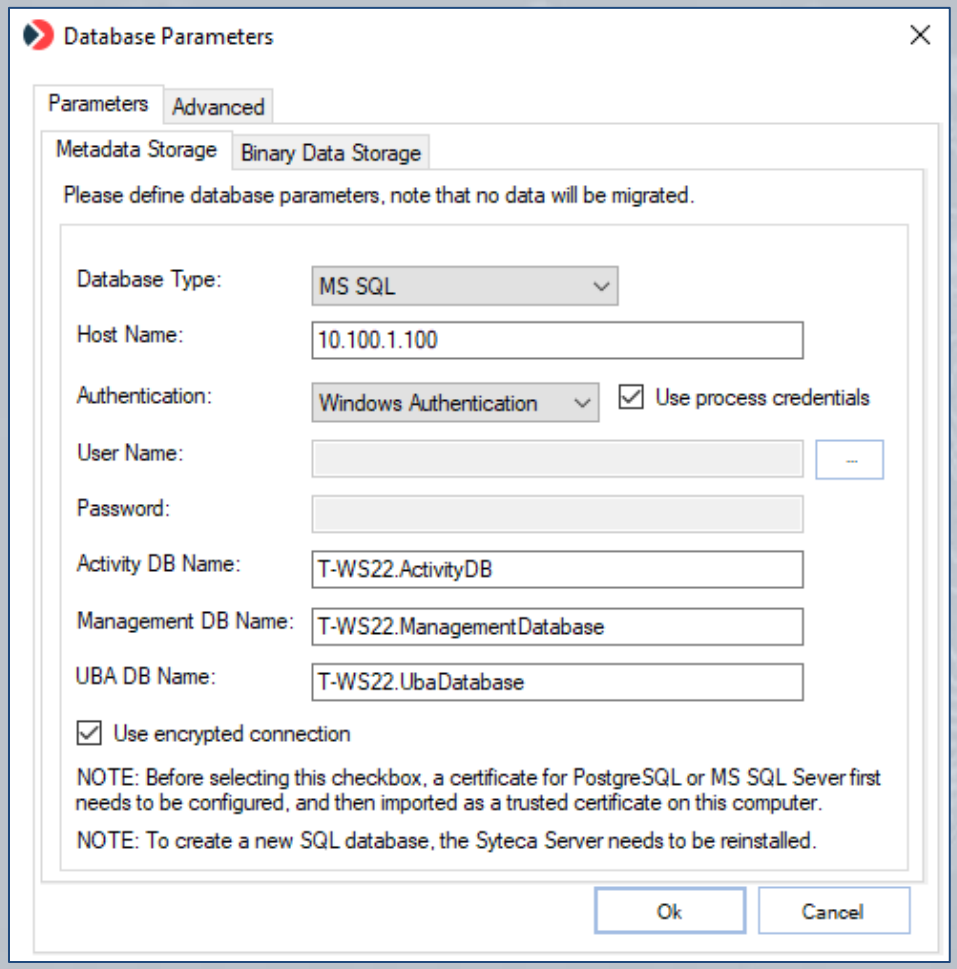
**Archived sessions** in any archived database **can be viewed** in the Session Viewer, and **searches** can be performed on the data, in the usual way at **any time**.



# Database Parameters

If the **database credentials** defined during installation of the Application Server need to be changed, you can easily **edit them** without reinstalling the Application Server.

**SSL encryption** can also be enabled, and a **gMSA/sMSA** account can be used (with the MS SQL Server database), for the connection between the Application Server and the database.

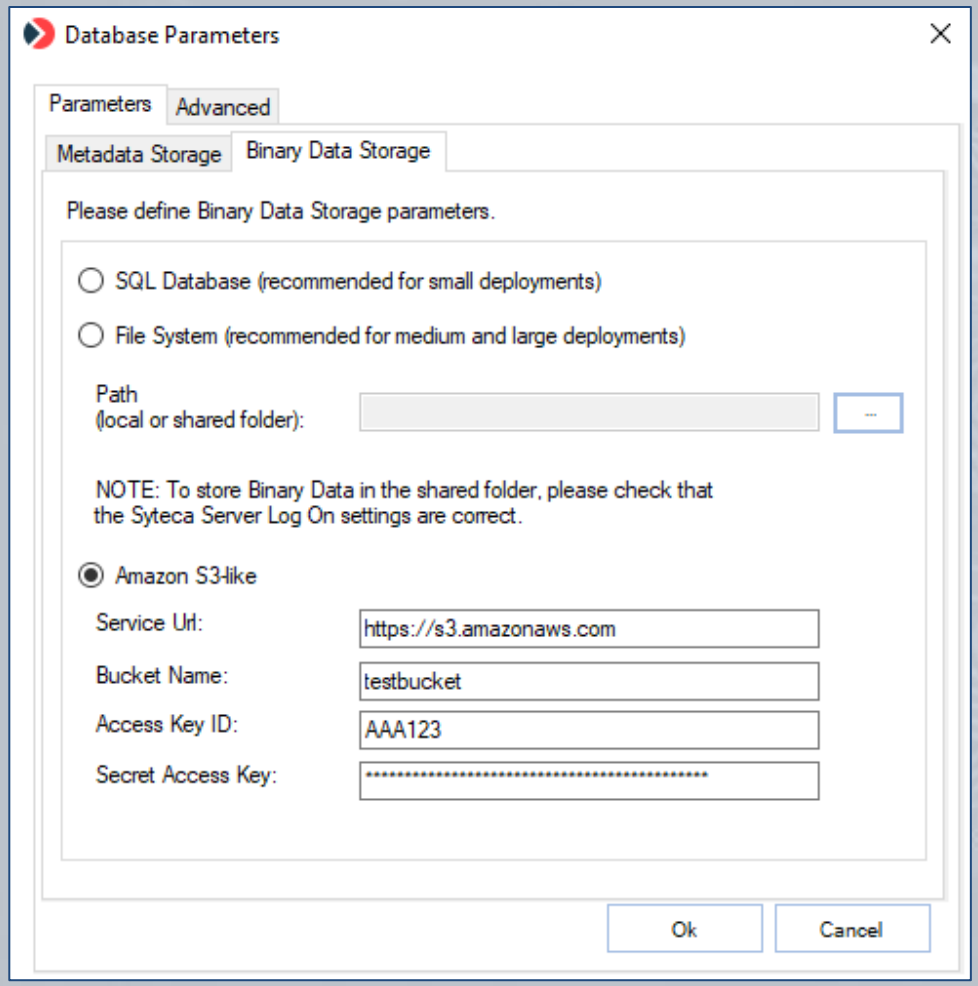


# Database Parameters (for Binary Data Storage)

Syteca

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

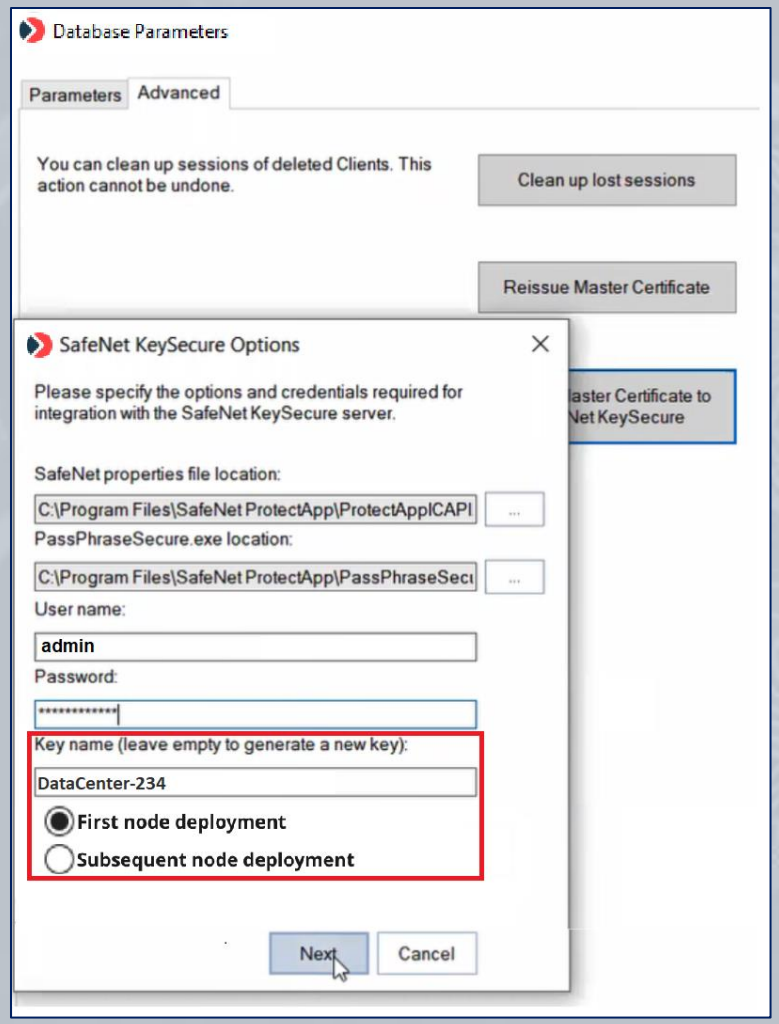
**Network-Attached Storage (NAS)** can also be used (by using the **File System** option).



# Database Parameters (Hardware Security Module)

Syteca

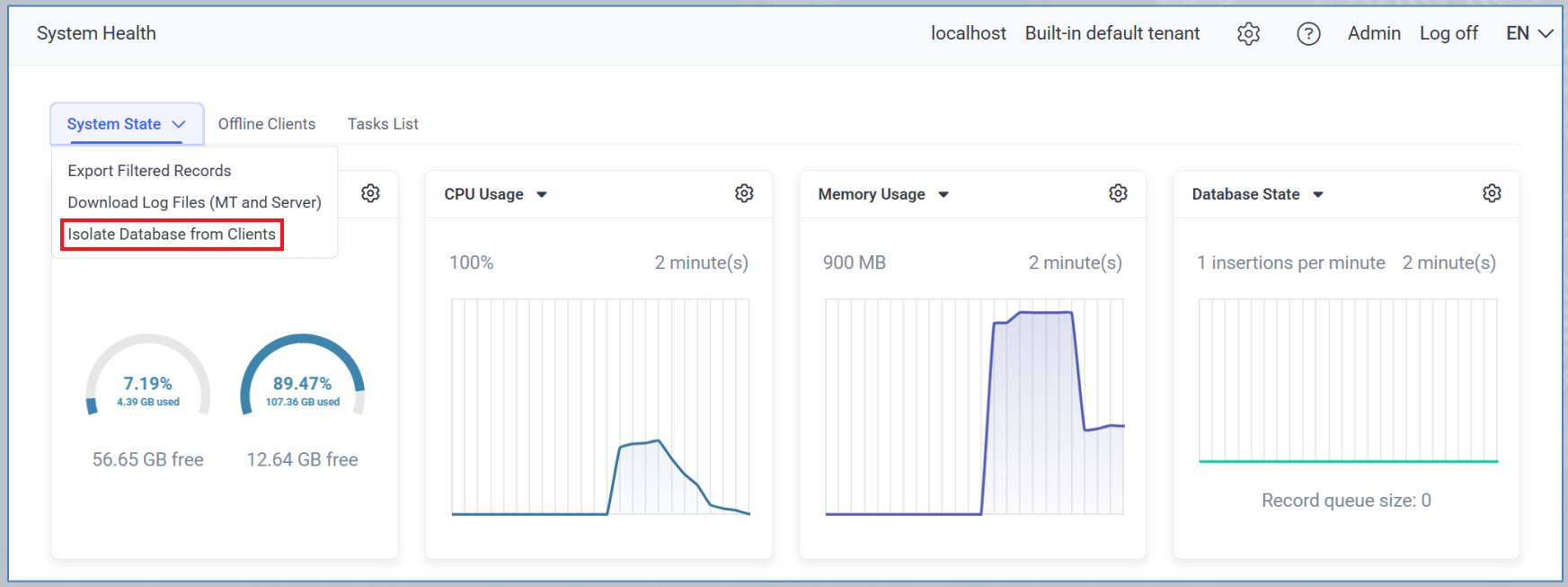
To further enhance security, the RSA-2048 encrypted Syteca **Master Certificate** can also be **moved** to a Hardware Security Module **(HSM)** device by using the integrated **Thales SafeNet KeySecure** with **SafeNet ProtectApp**.



# Isolating the Database from Clients

Syteca

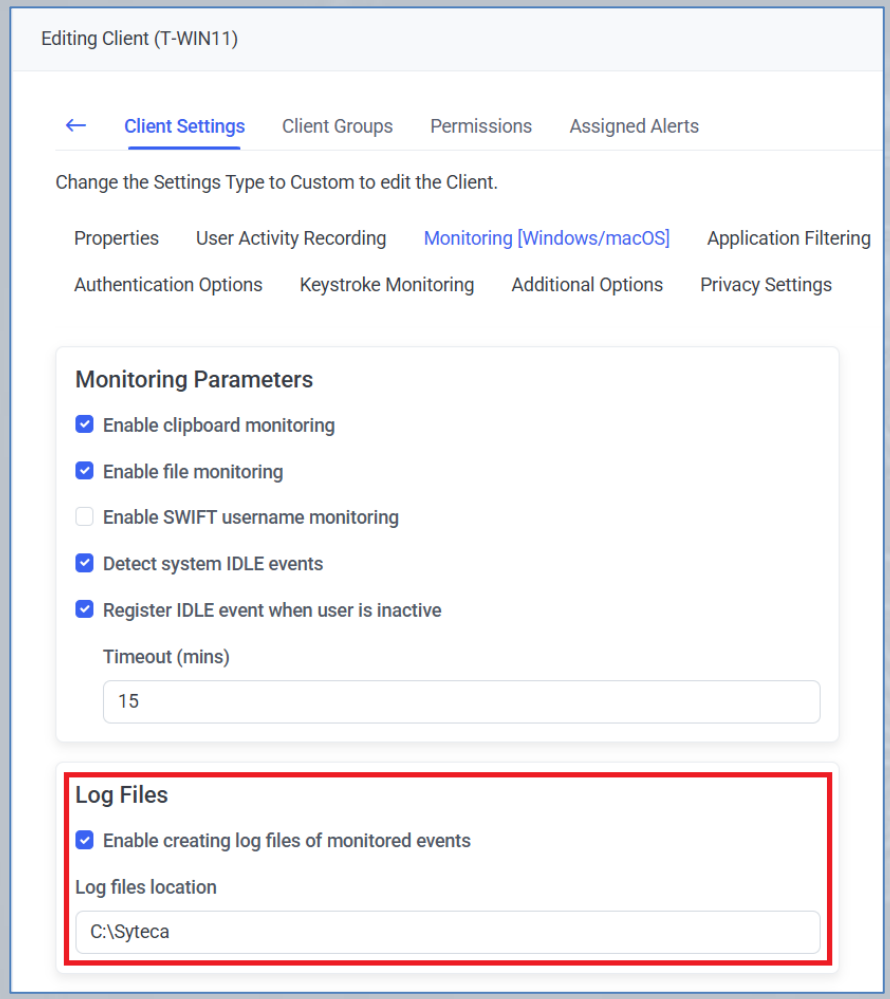
You can **disconnect all Clients** from the **database** to make them go offline, so as to **fix any issues** with the database, and perform database **cleanup and maintenance** without stopping Syteca Application Server. Once database operation is restored, you can bring all Clients **back online in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



# SIEM Integration

Syteca

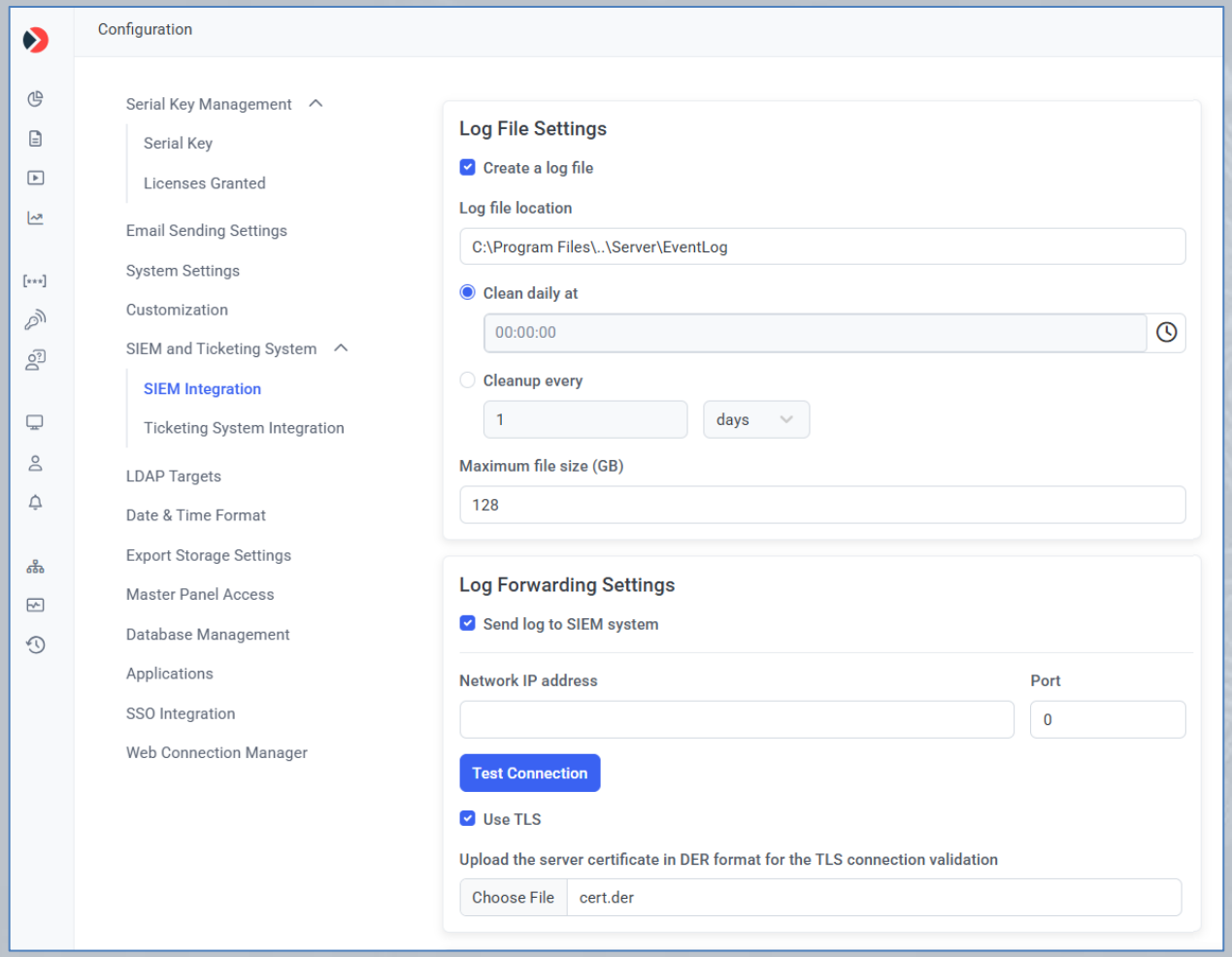
Syteca **integrates with your SIEM system** by using the log files of monitored events.



# SIEM Integration

Syteca

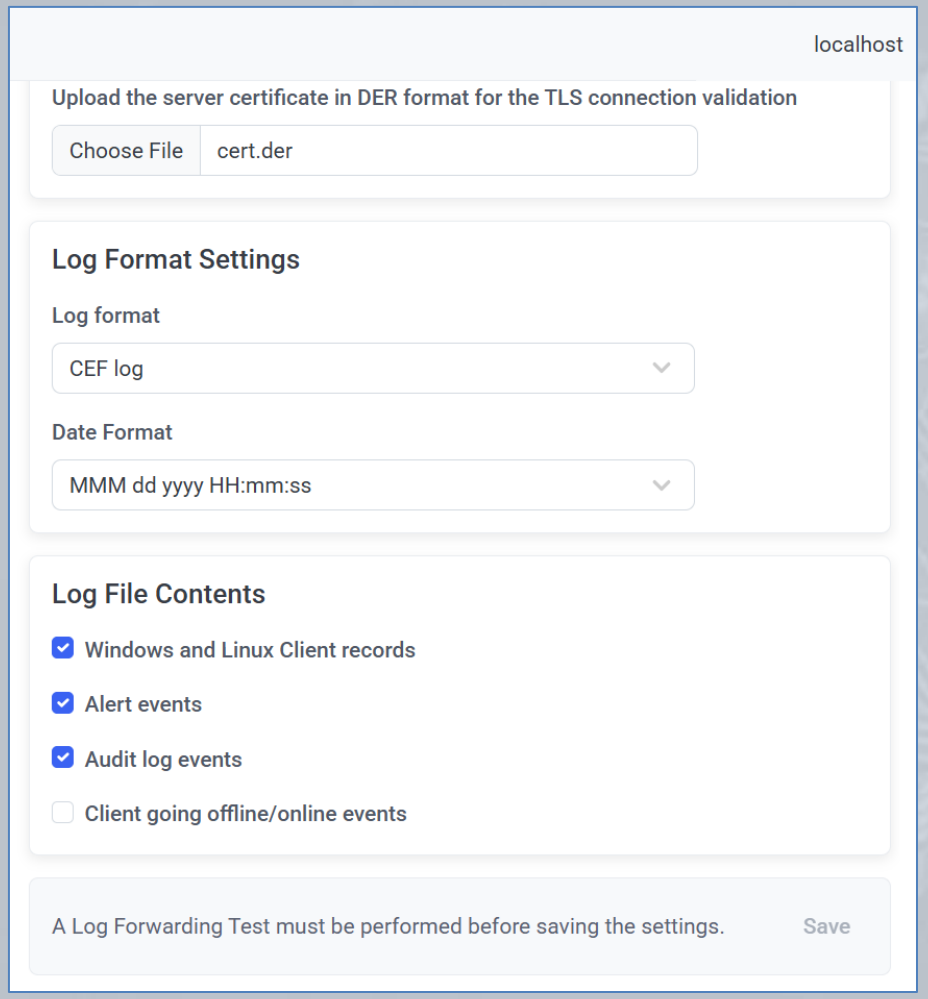
Syteca allows the **sending** of records about alert events and monitored data **directly to SIEM systems** such as Splunk, ArcSight, and IBM QRadar, where an encrypted **TLS connection** can also be used to forward the records securely.



# SIEM Integration

Get access to Syteca 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)

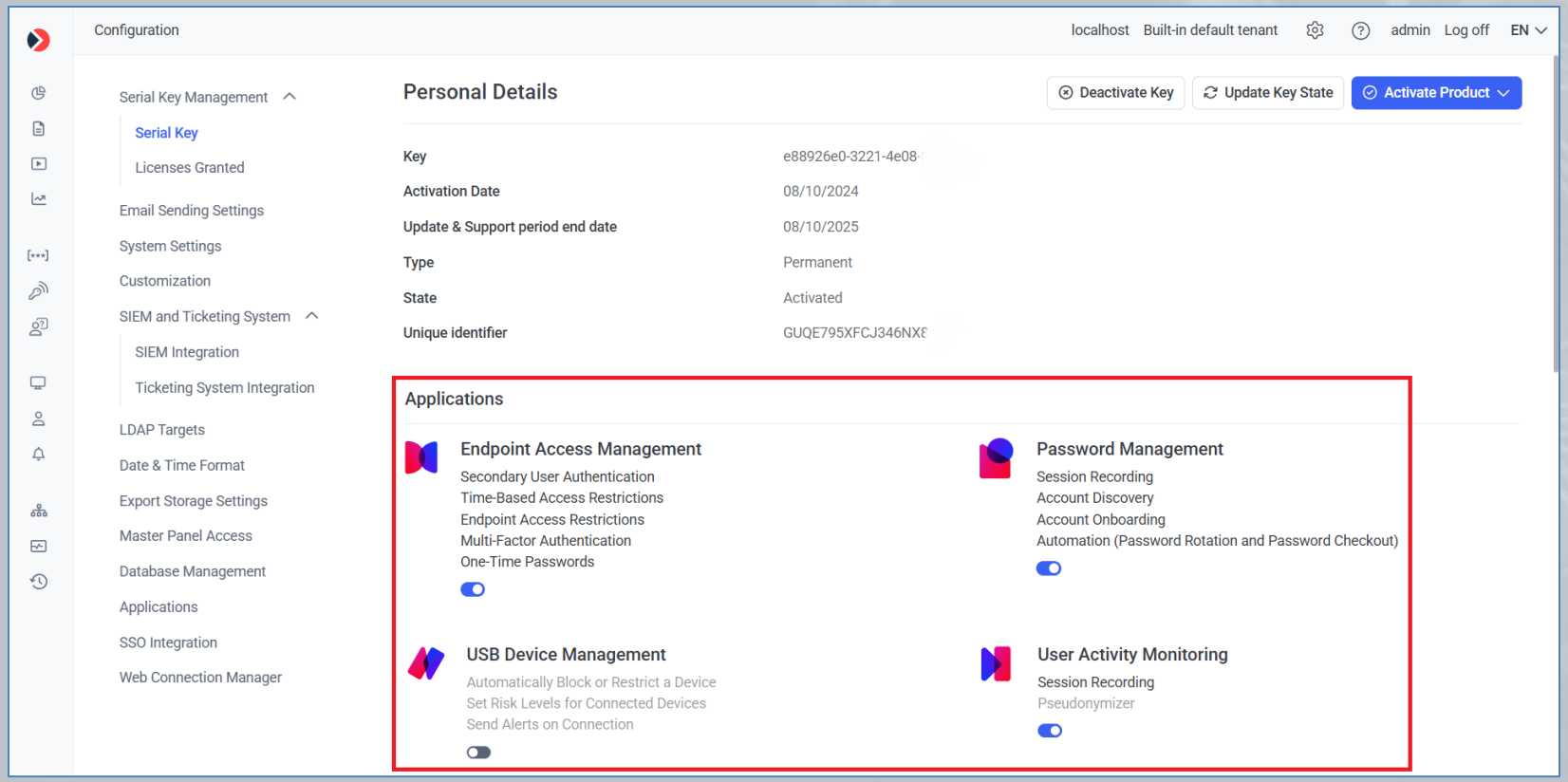


# Licensing

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

# Licensing

A Syteca **product license serial key** contains the **applications** that are enabled, and the **features** they include (as purchased).

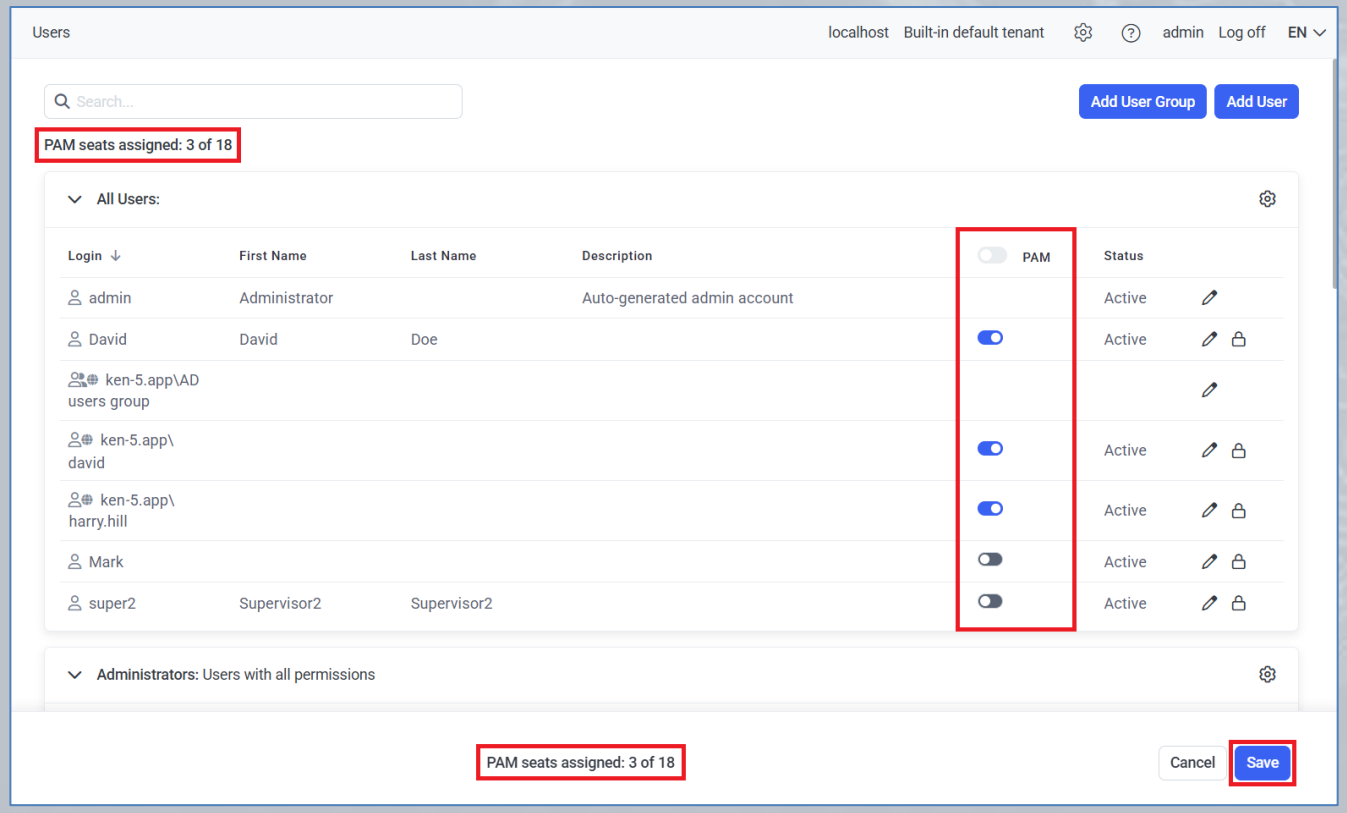


# PAM Seat Licenses (for PAM Users)

Syteca

To start using the applications and features enabled in the activated serial key, the **various license types** it contains **need to be assigned.**

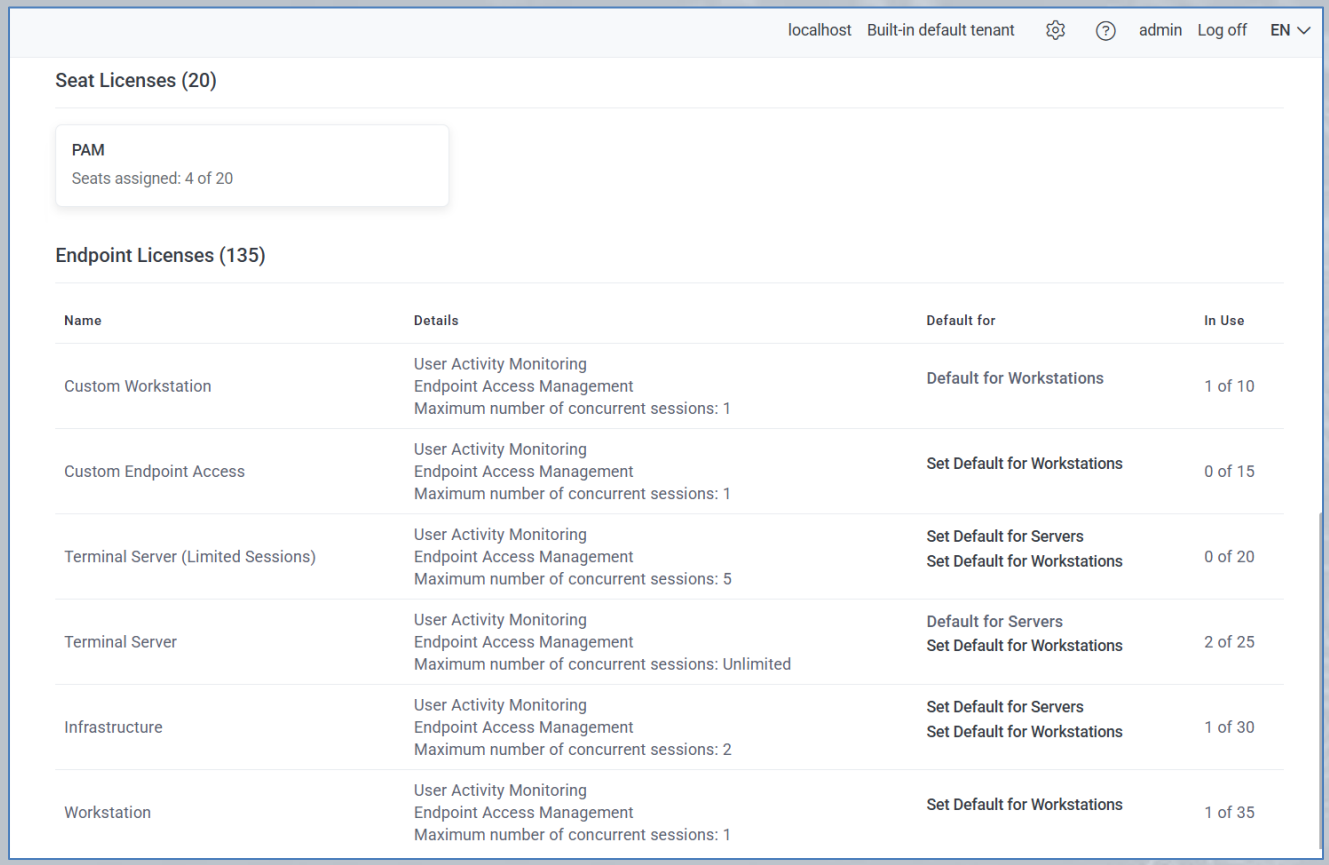
- **PAM seat licenses** for the **Password Management (PAM)** application only.



# Endpoint Licenses (for Client Computers)

Syteca

- **Endpoint licenses** of various (custom) types for the **User Activity Monitoring (UAM)**, **USB Device Management**, and **Endpoint Access Management** applications.



# Types of Serial Keys

Syteca

A limited **Trial product license serial key** for Syteca can be requested and used for an **evaluation period**, to deploy the system and review its features, as well as **update** the product during this period.

To use Syteca for a **longer period**, and get a **greater number of licensed PAM users and endpoints**, the product needs to be **licensed** by **activating a purchased serial key** on the computer where Syteca Application Server is installed.

You can purchase either a **Permanent** (aka **Perpetual**), **Subscription**, or **SaaS** serial key.

# Floating Endpoint Licensing

Syteca

Syteca is currently the **only such product on the market** to offer floating endpoint licensing (along with automatic endpoint license assignment).

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 number of the appropriate types of Syteca **endpoint 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 endpoint licenses automatically (e.g. after a database cleanup).
  - **Using a golden image** (for VMware/Citrix desktop monitoring): Dynamically assigns endpoint licenses to **virtual desktops** whenever new Windows-based desktops are created, and unassigns them whenever Client computers are shut down.

# Installing & Updating Clients

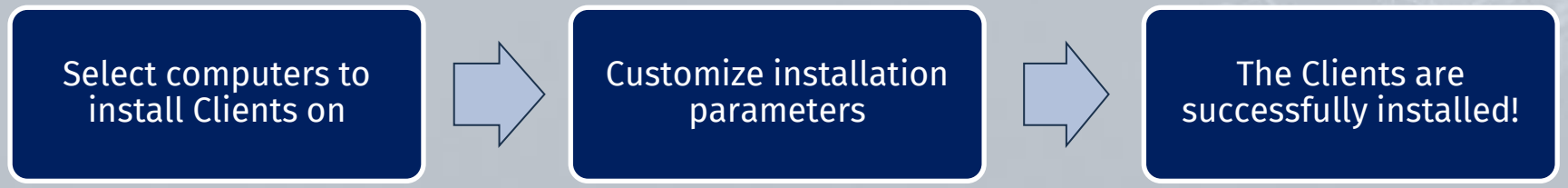
# Installing Syteca Clients

Syteca

Convenient Syteca Client installation:

- **Locally**:
  - Windows Clients:
    - using the installation file with **default parameters**.
    - using a package generated with **customized parameters**.
  - macOS or **macOS Hidden/Stealth** Clients (using a tar.gz file).
  - Linux, incl. **SELinux**, **Solaris**, etc (using a tar.gz file).
- **Remotely:**
  - for Windows Clients.
  - for macOS or **macOS Hidden/Stealth** Clients (**mass deployment**).

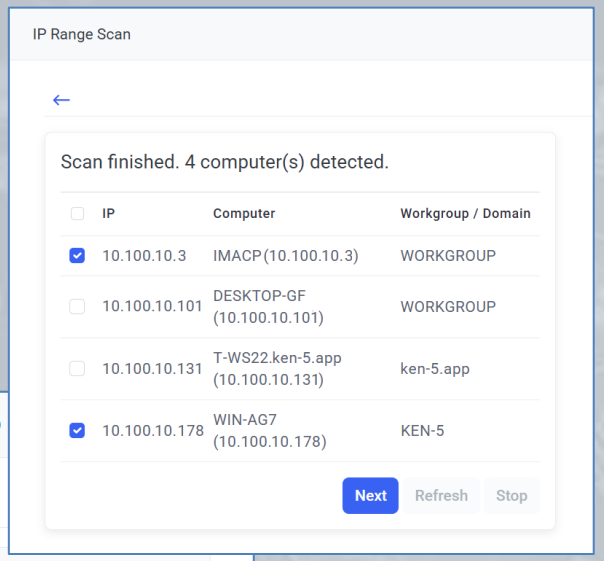
## Remote Installation

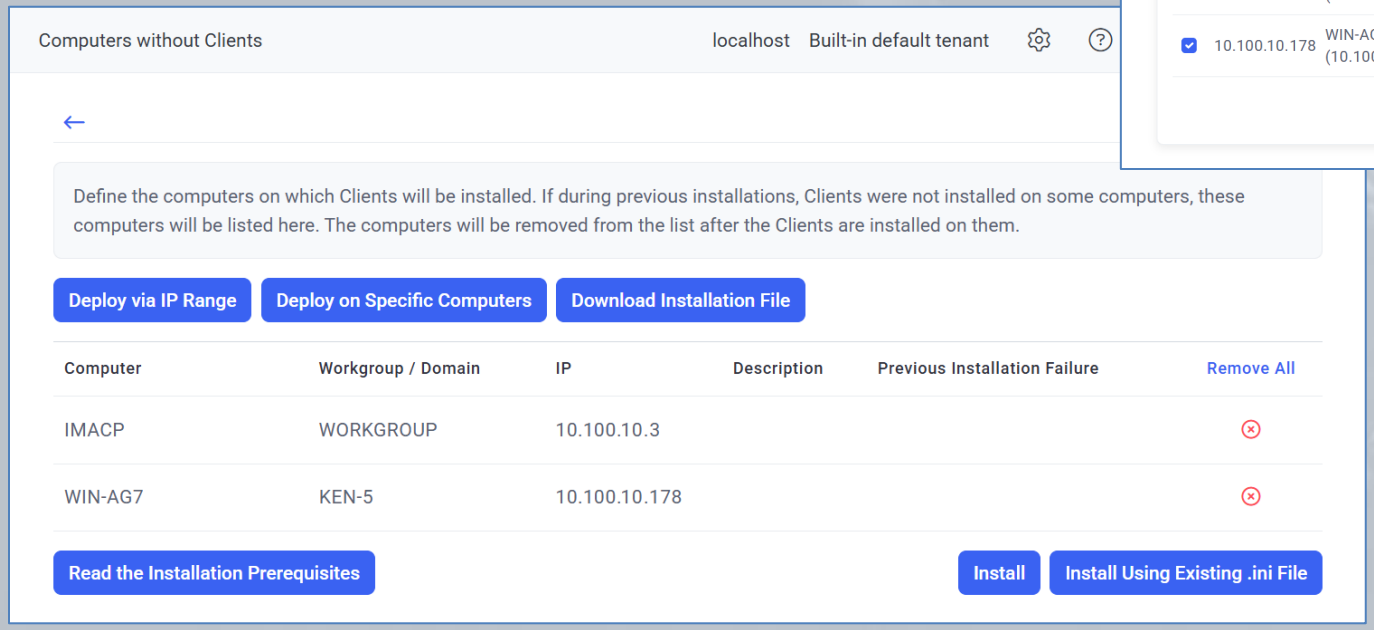


# Target Computers for Remote Installation

Syteca

- **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**

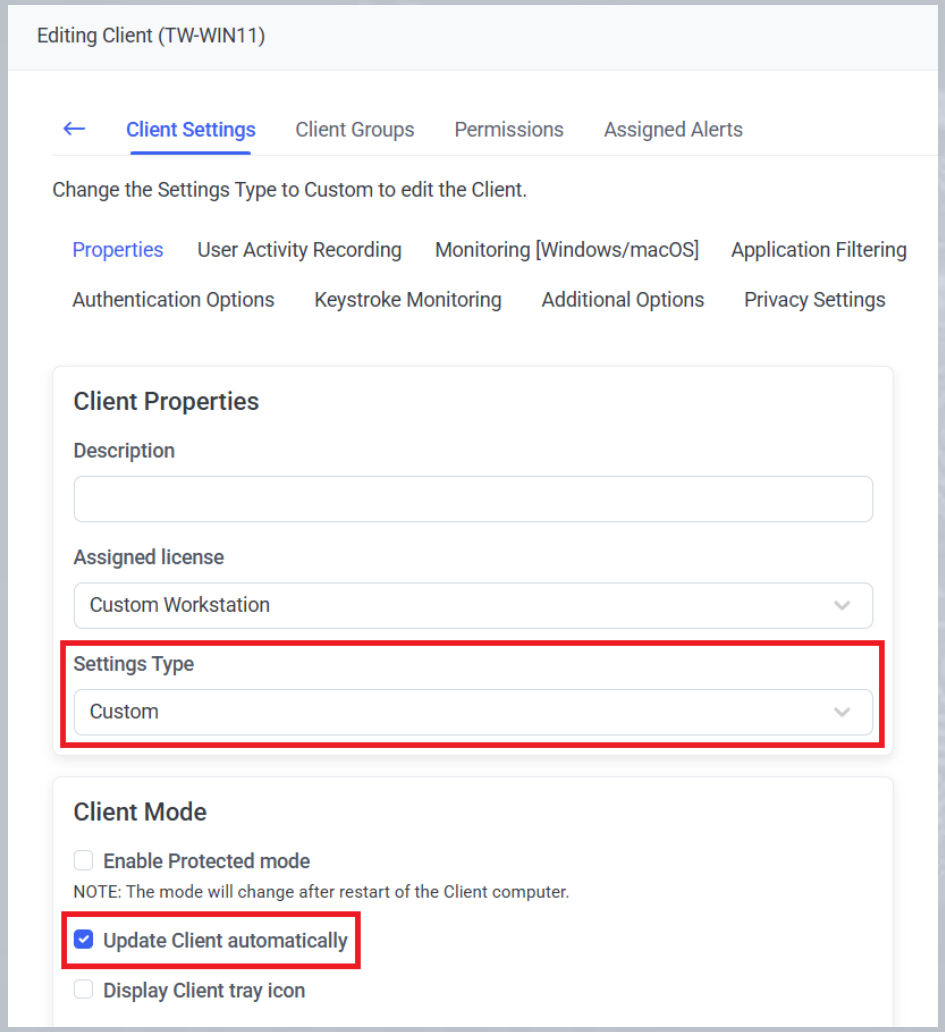


# Updating Syteca Clients

After Syteca 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

Syteca

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.

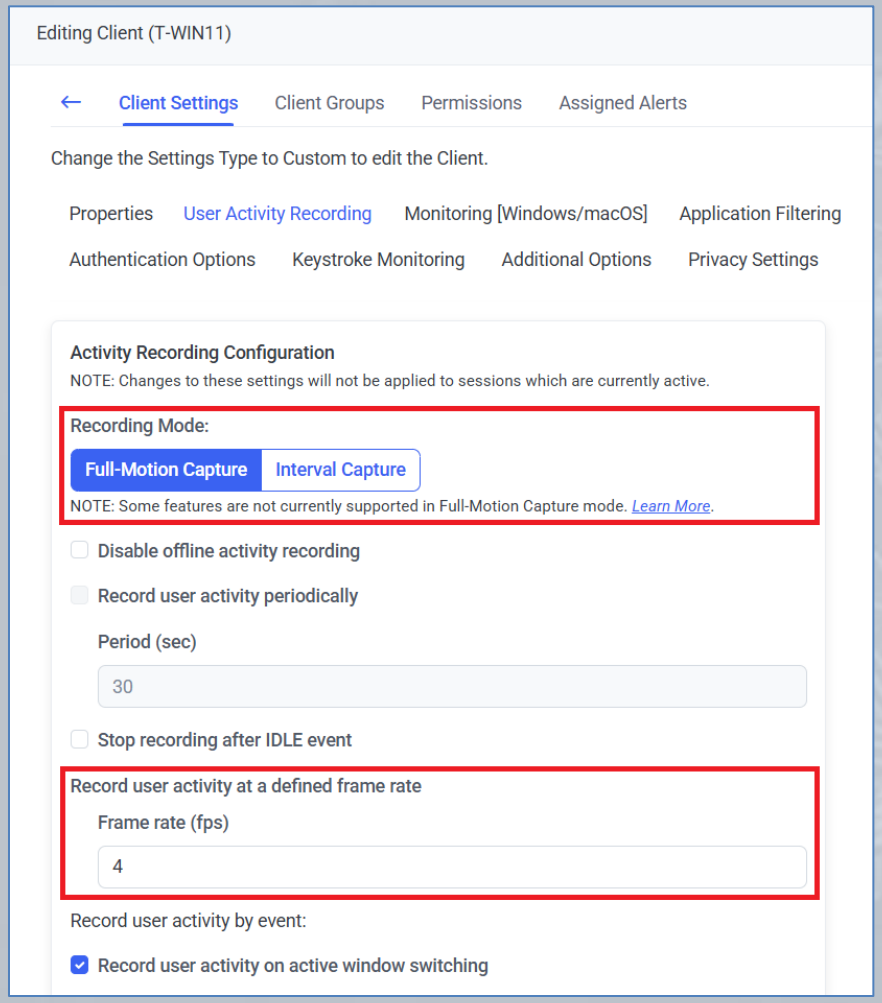
The information recorded is saved in an easy-to-review and easy-to-search form, including:

- Names of **applications** launched.
- Titles of **active windows**.
- **URLs** entered into browsers.
- 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

The **Recording Mode** toggle allows either:

- **Full-Motion Capture** mode for **video** to be **recorded continuously**, and at the defined **frame rate** (for Windows Clients).
- **Interval Capture** mode for **screen captures** to be recorded **at intervals** and/or only **when triggered** by events.

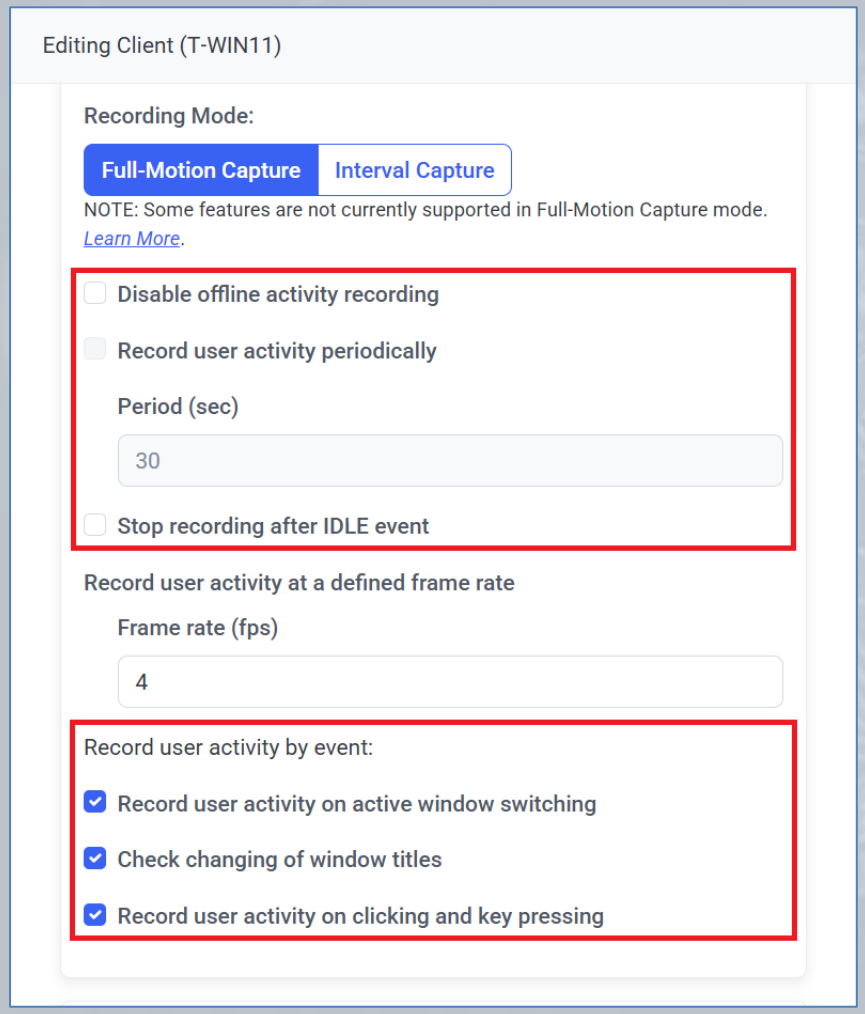


# User Activity Recording

Syteca

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

You can easily **configure** exactly **when and what** Windows, macOS, and Linux Clients **will record**.

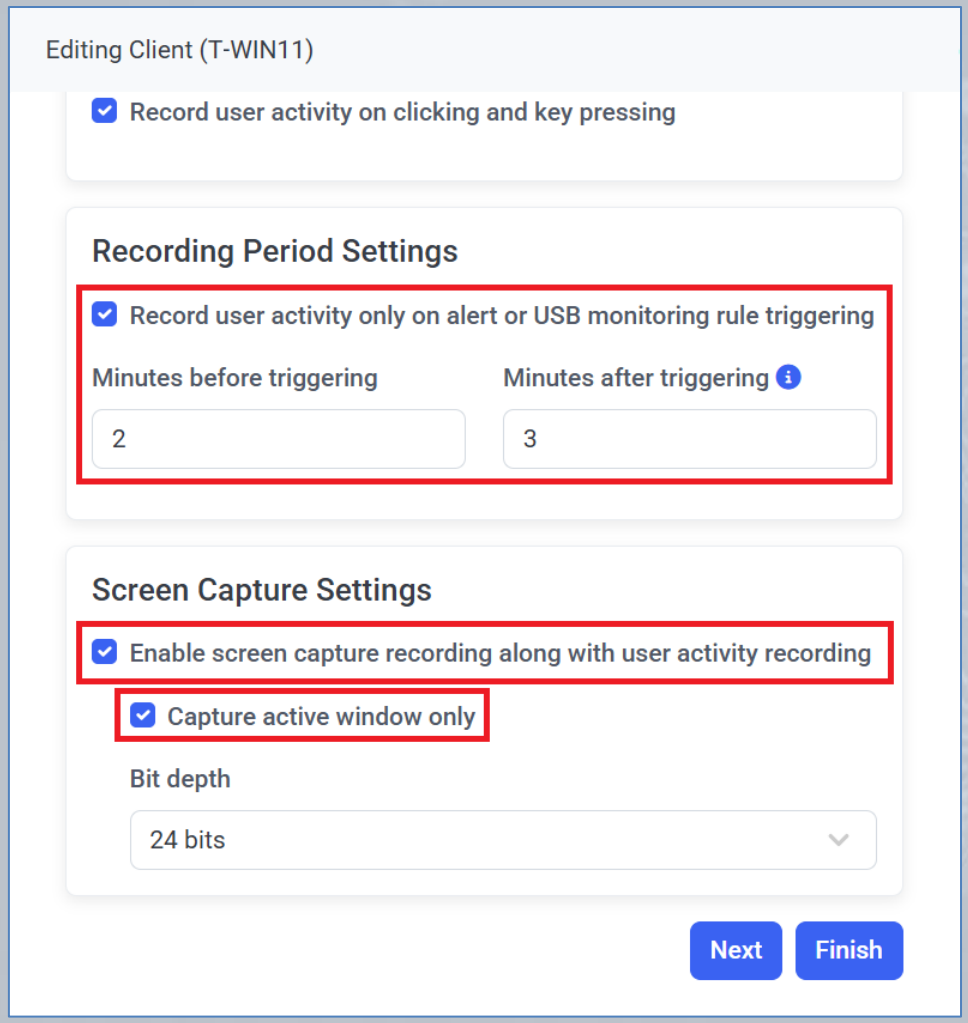


# User Activity Recording

Syteca

For example, you can configure a Client (or the Clients in a Client group) to:

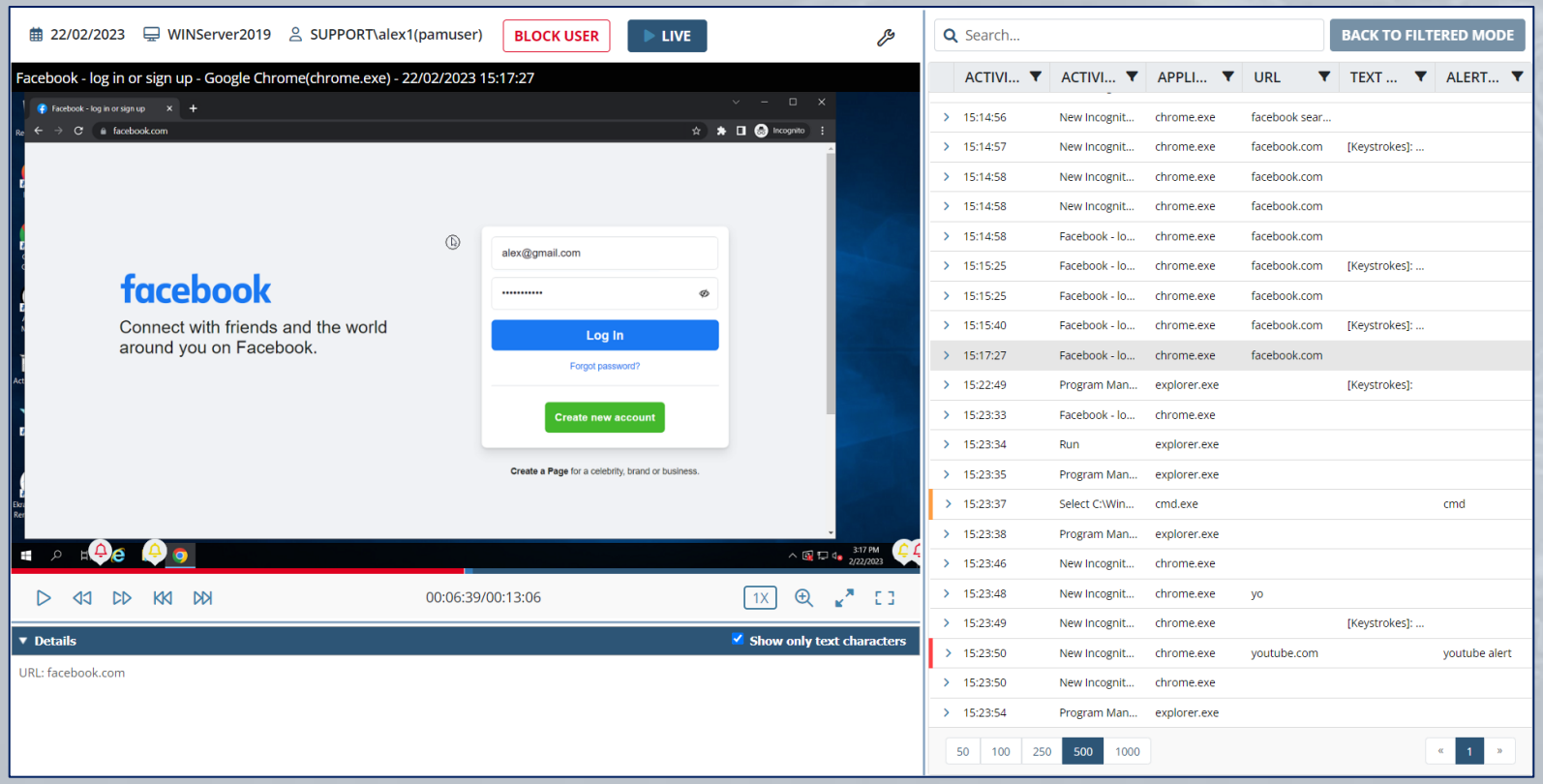
- **Only record** user activity **when an alert** (or USB monitoring) rule **is triggered** (on Windows and macOS Clients).
- Only record user activity **without recording screen captures**.
- Only record the **active window**.



# URL Monitoring

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

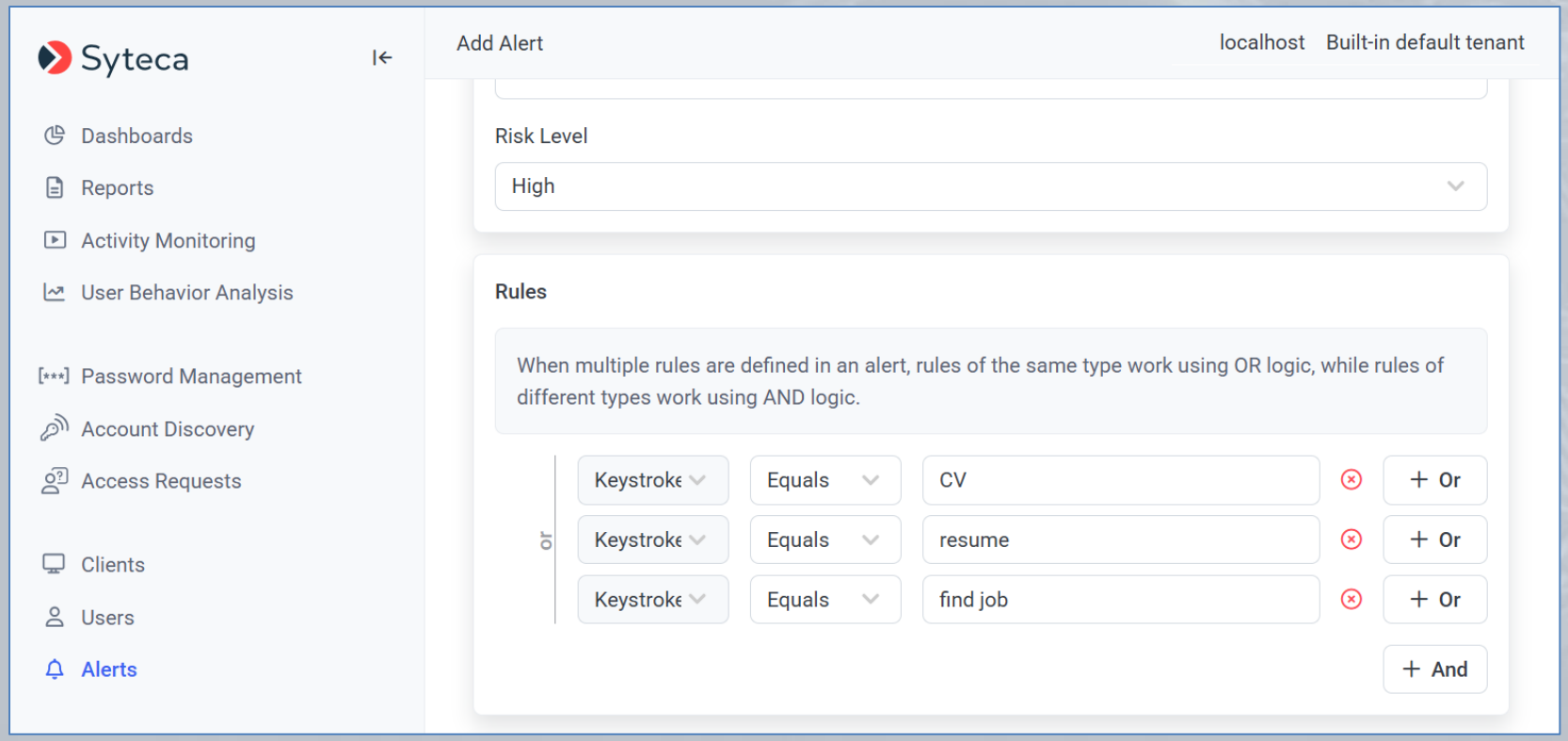
You can configure the Client to monitor either full URLs or top and second level domain names only.



# Keystroke Logging

Syteca

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.

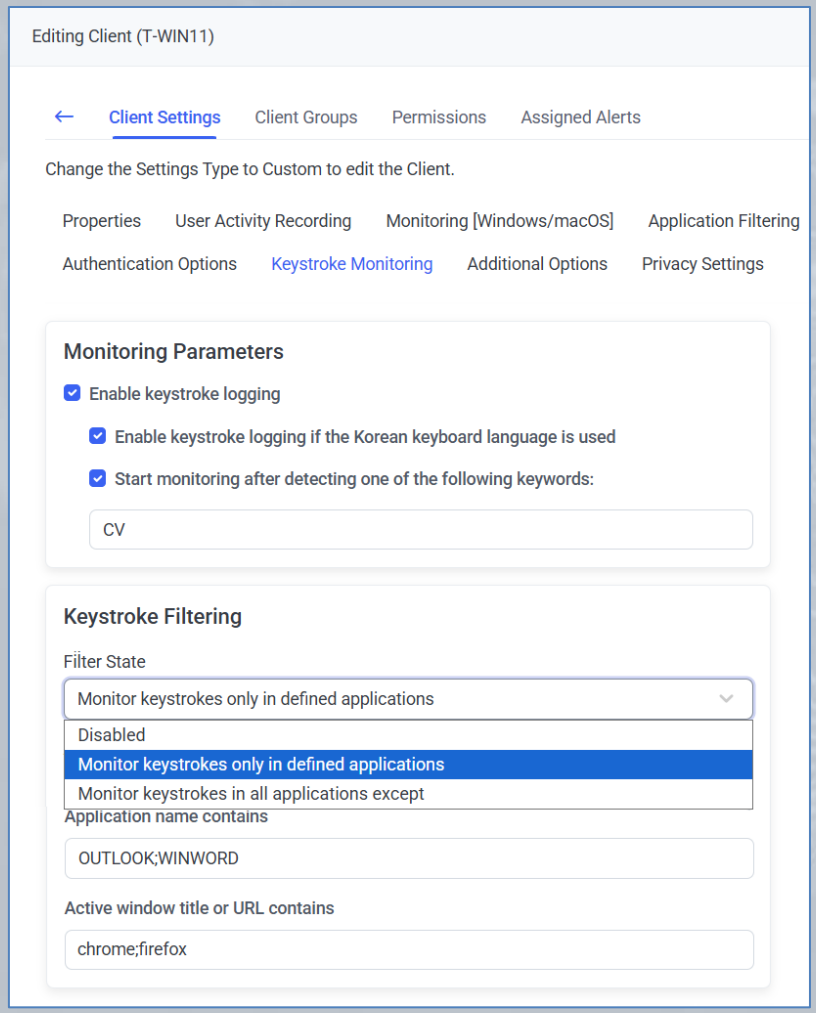


# Keyword-Triggered Monitoring

Syteca

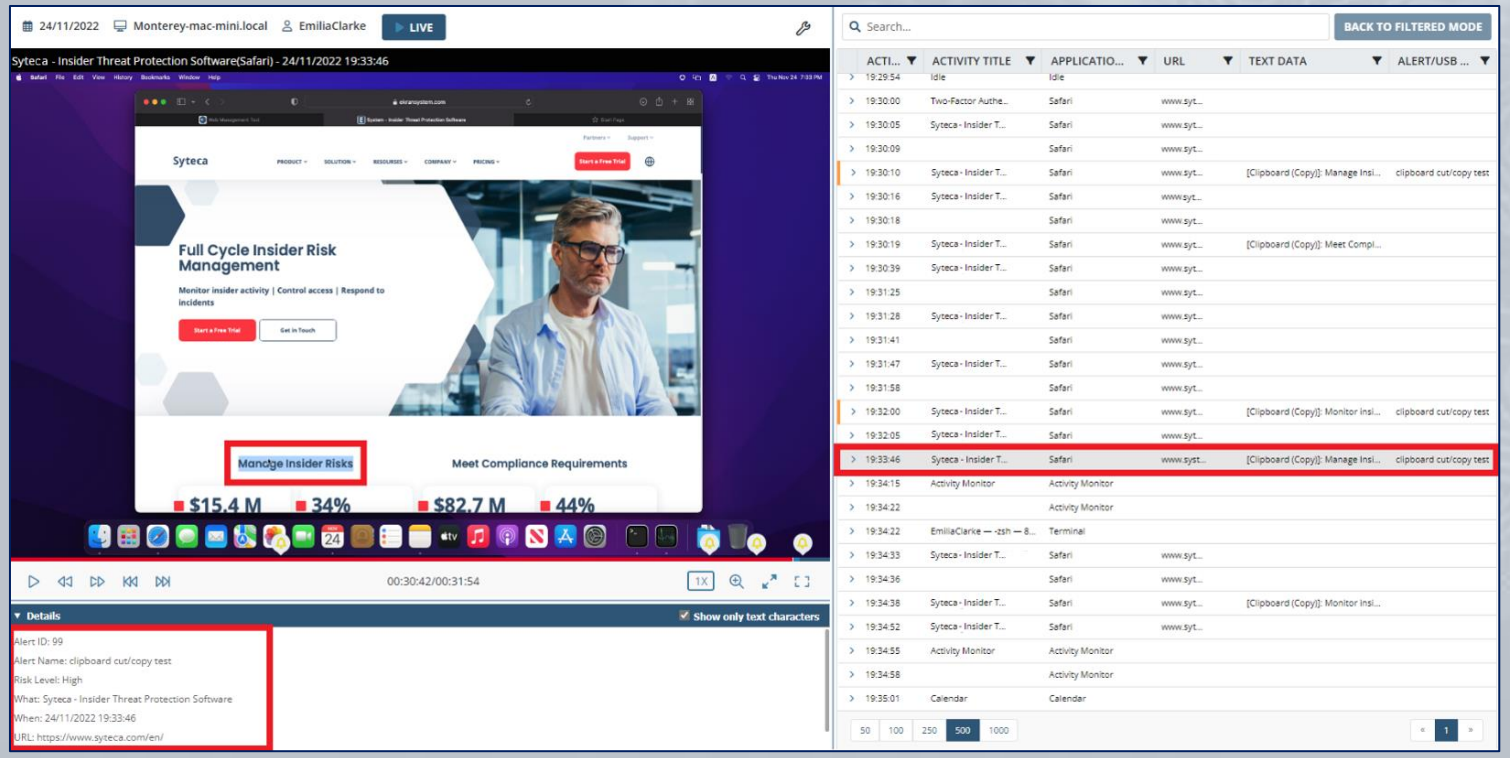
You can configure Syteca Clients to start monitoring and recording screen captures/ video only after they **detect** defined **keywords** entered by the user in **specified applications**.

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



# Clipboard Monitoring

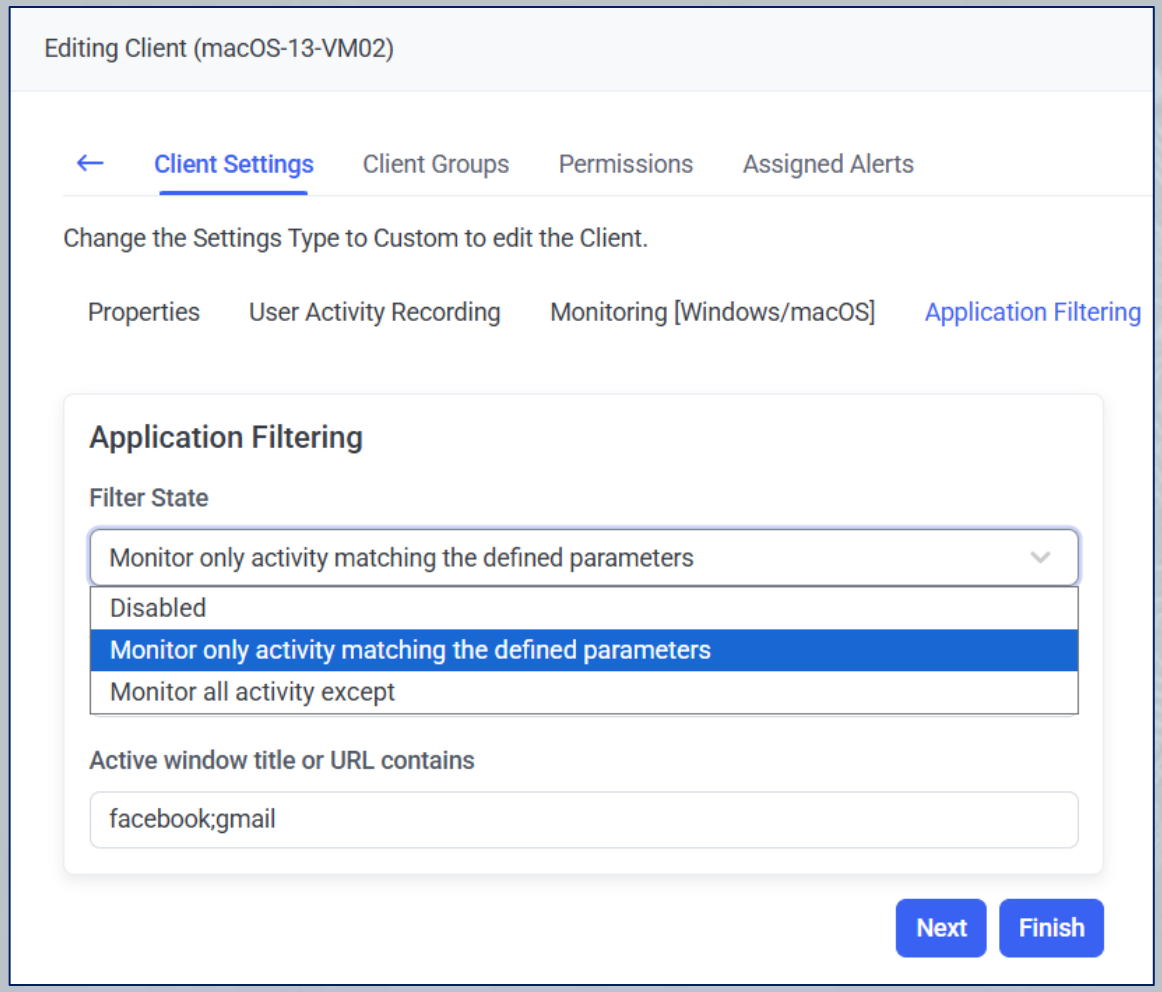
The Syteca Client can **capture all text data** that is **copied/cut** from, or **pasted** into documents, files, applications, the browser address bar, etc, on Windows and macOS Client computers. **Alerts** can also be added to **be triggered** by these clipboard operations.



# Application Filtering

Syteca

Syteca 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**.

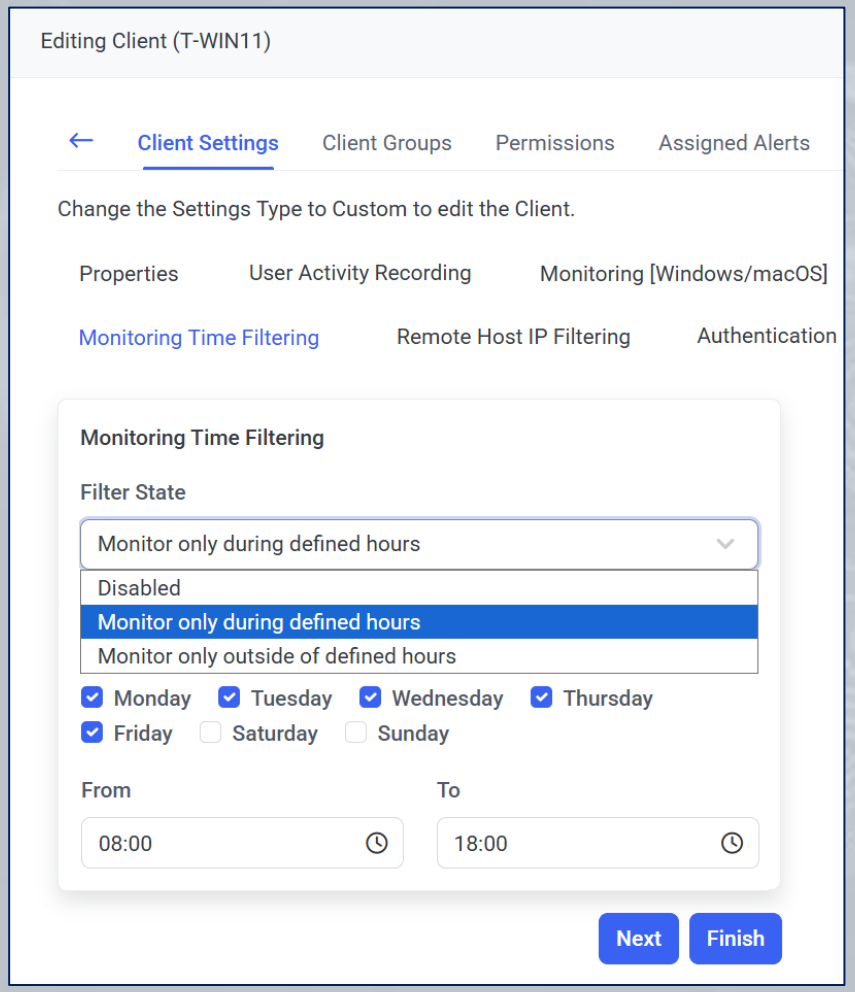


# Monitoring Time Filtering

Syteca

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

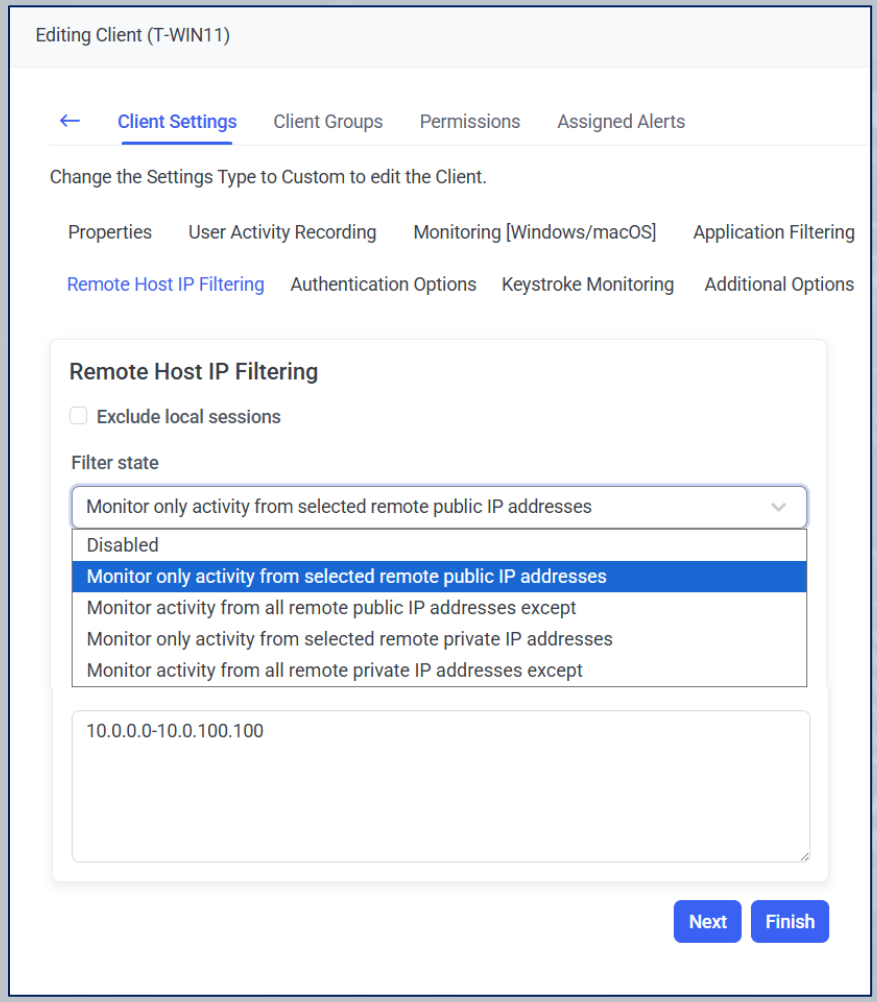
By selecting certain **days of the week** and defining **specific hours**, you can establish bounds within which Syteca Clients will record all user activity.



# Remote Host IP Filtering

Syteca

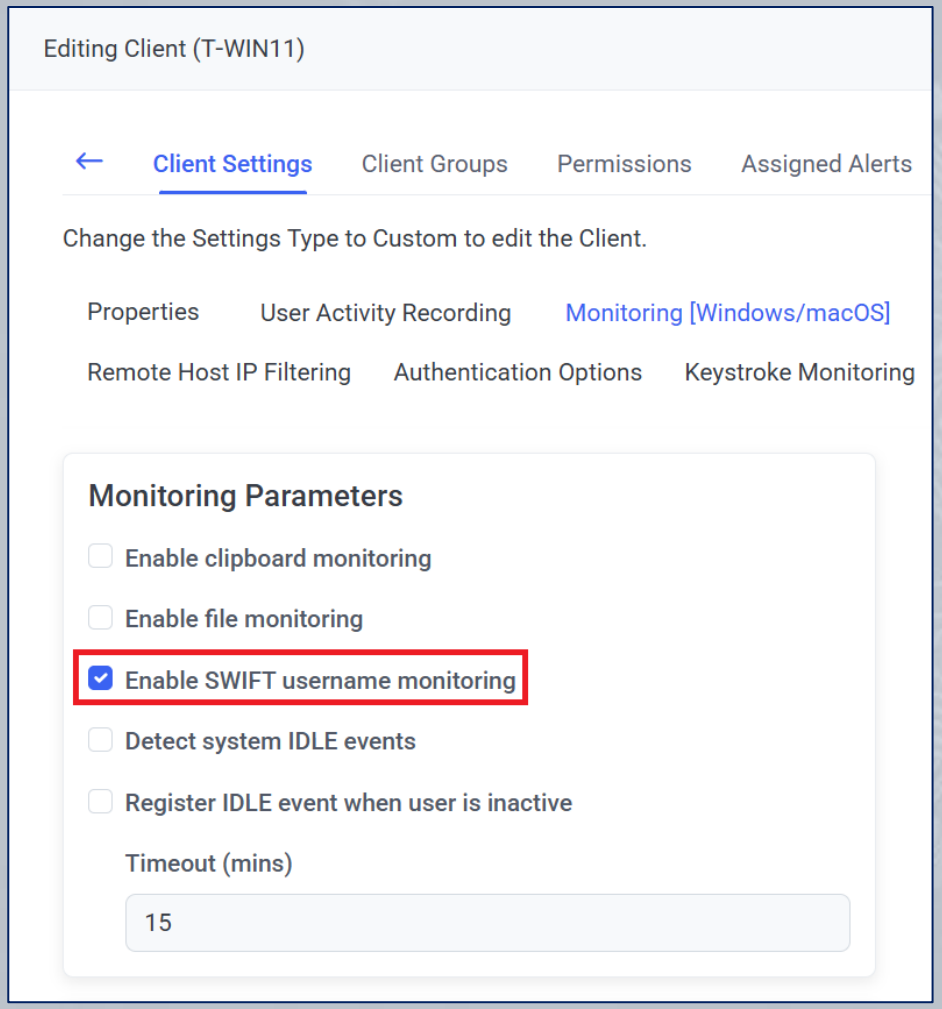
Additionally, you can **filter** sessions from **certain remote** (public or private) **IP addresses**, or only monitor sessions from certain IP addresses.



# SWIFT Username Monitoring

Syteca

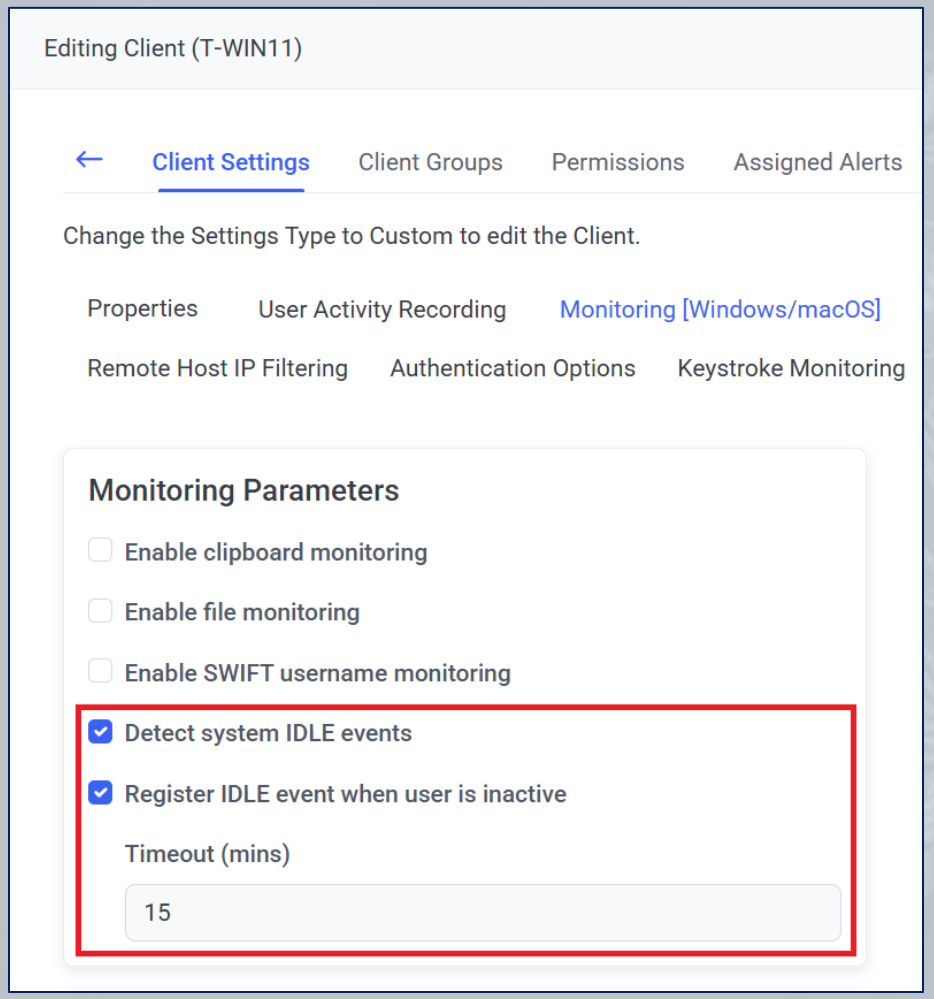
Syteca allows the **username** used when logging in to the **SWIFT** network to be recorded, so that you can easily identify such users.



# Idle Events Monitoring

**Idle events** can be **detected,** when:

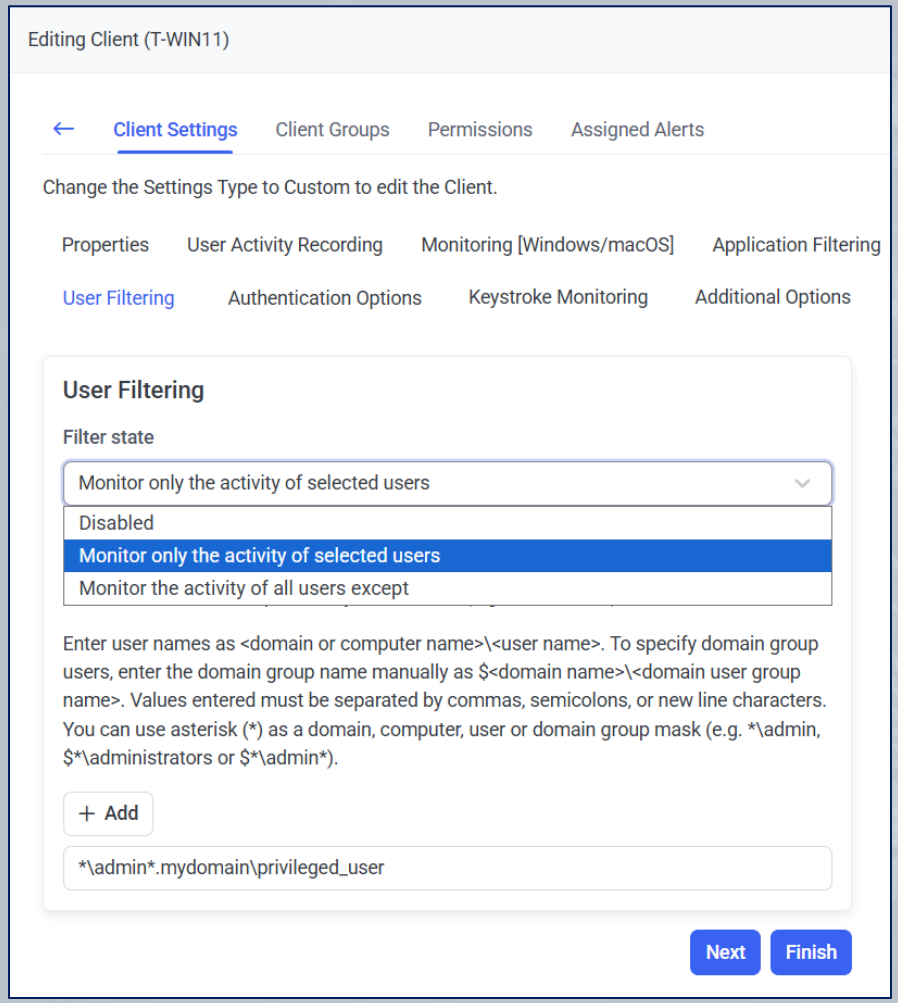
- The Client computer goes into **sleep** or hibernation mode, or the **screen turns off** automatically.
- The **user is inactive** for longer than a **specified period**.



# Privileged User Monitoring

Syteca

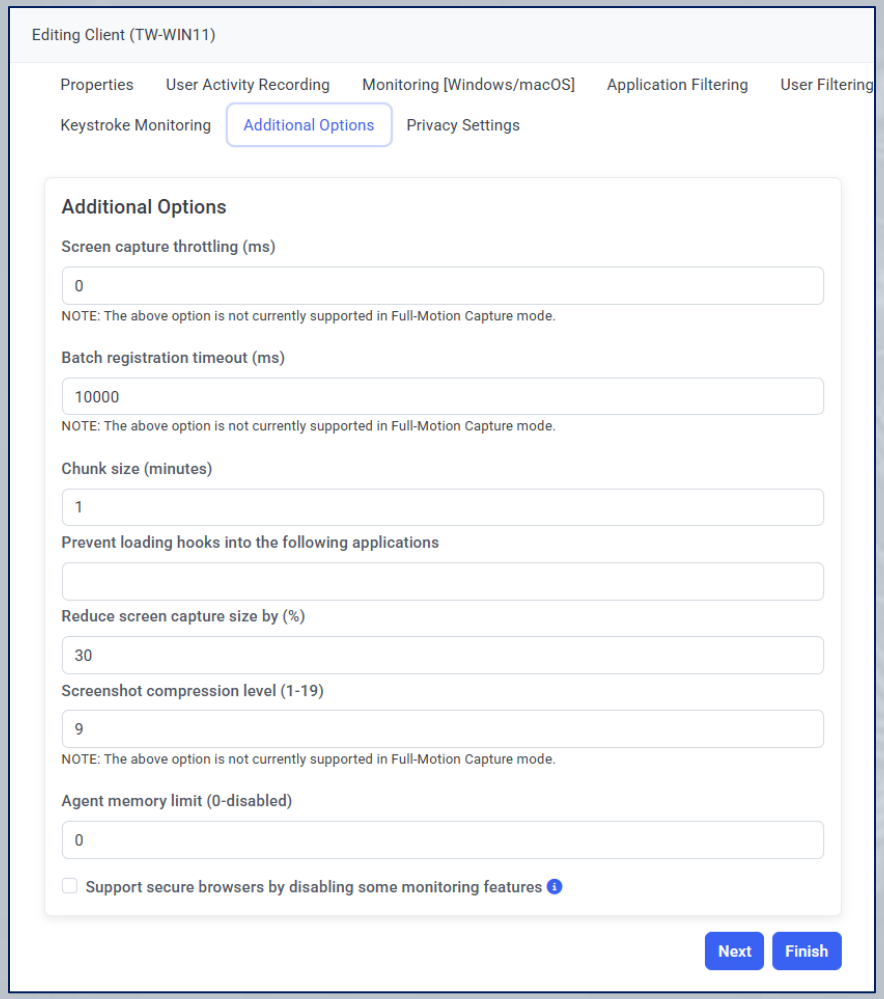
You can also monitor the activity of users logging in under **privileged access accounts**.



# Bandwidth Usage Reduction

Syteca

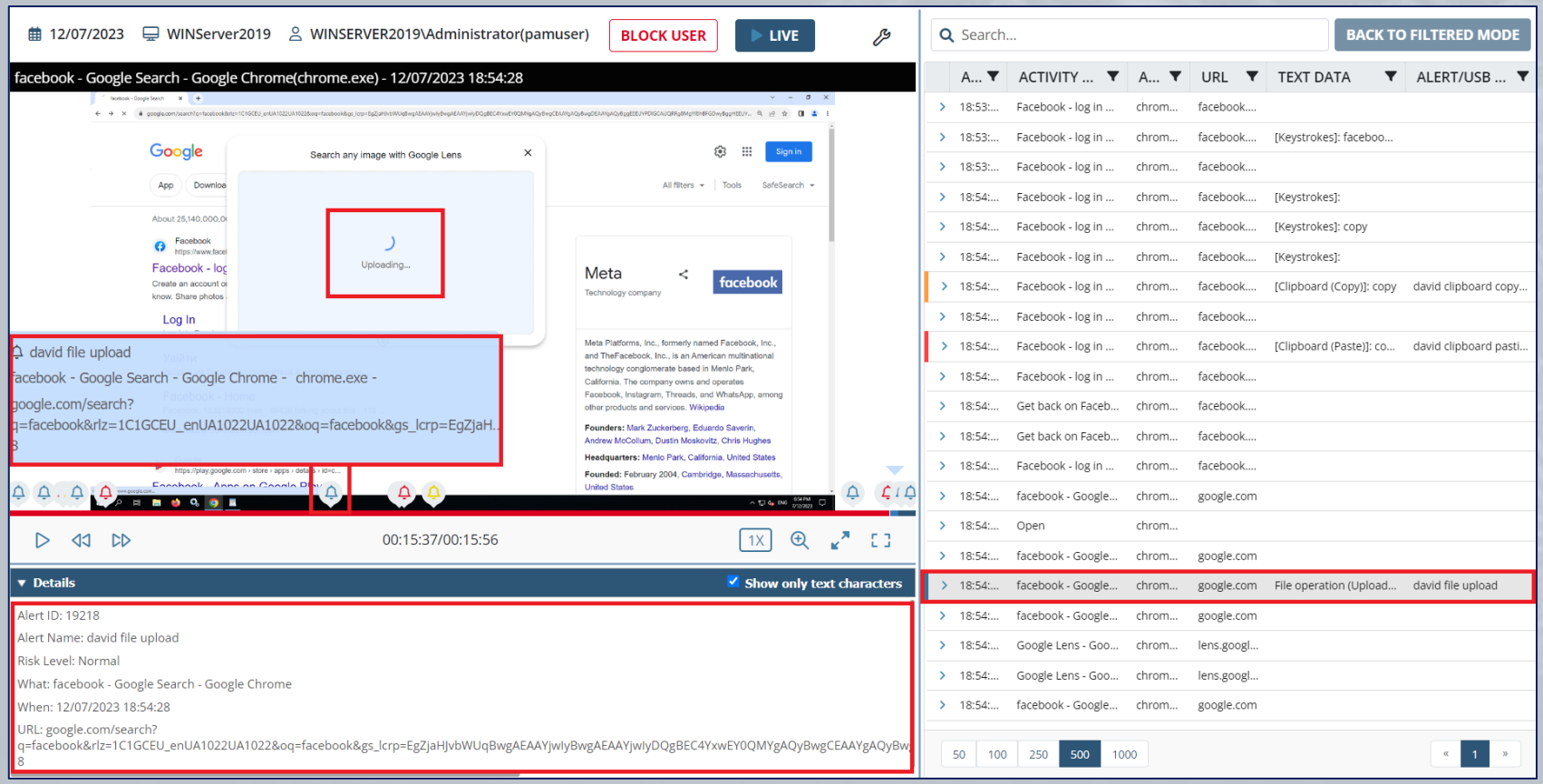
Syteca allows you to configure various other options, including **bandwidth usage reduction** parameters to manage the **volume of traffic** from the Client to Syteca Application Server, and the **chunk size for video** segments recorded, and to **prevent loading hooks** from specified applications.



# File Monitoring

Syteca

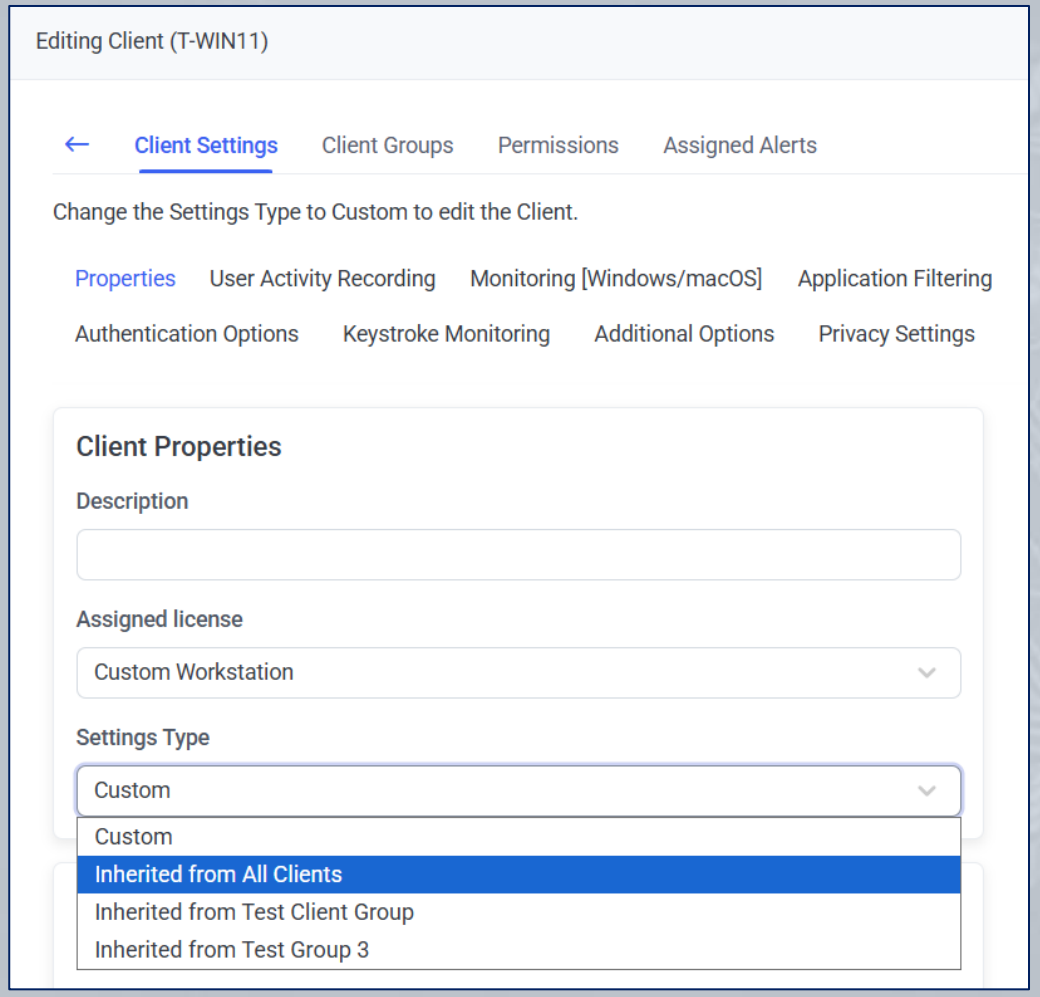
File monitoring operations (e.g. **file upload**) can be detected, including in many applications such as common browsers and messaging apps.



# Client Group Settings

Syteca

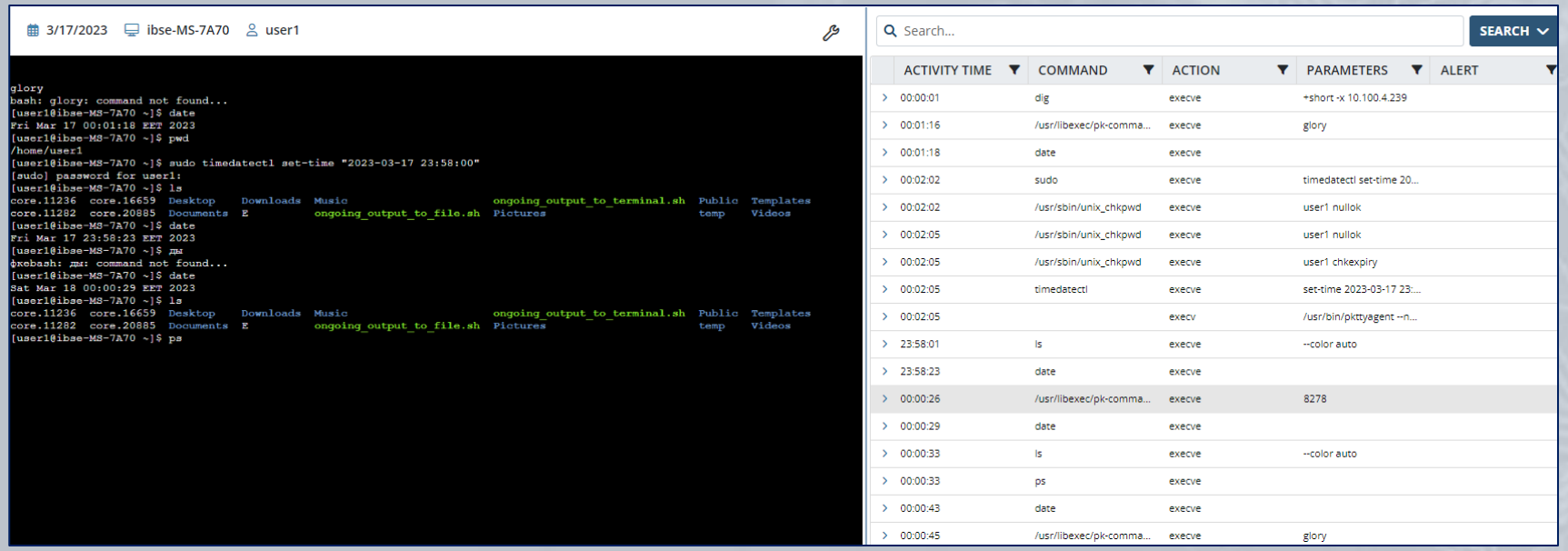
You can define the settings for a Client group, and then **apply them to Clients** in the group by inheritance, so as to save time.



# Monitoring Linux Clients

Syteca

Syteca **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.



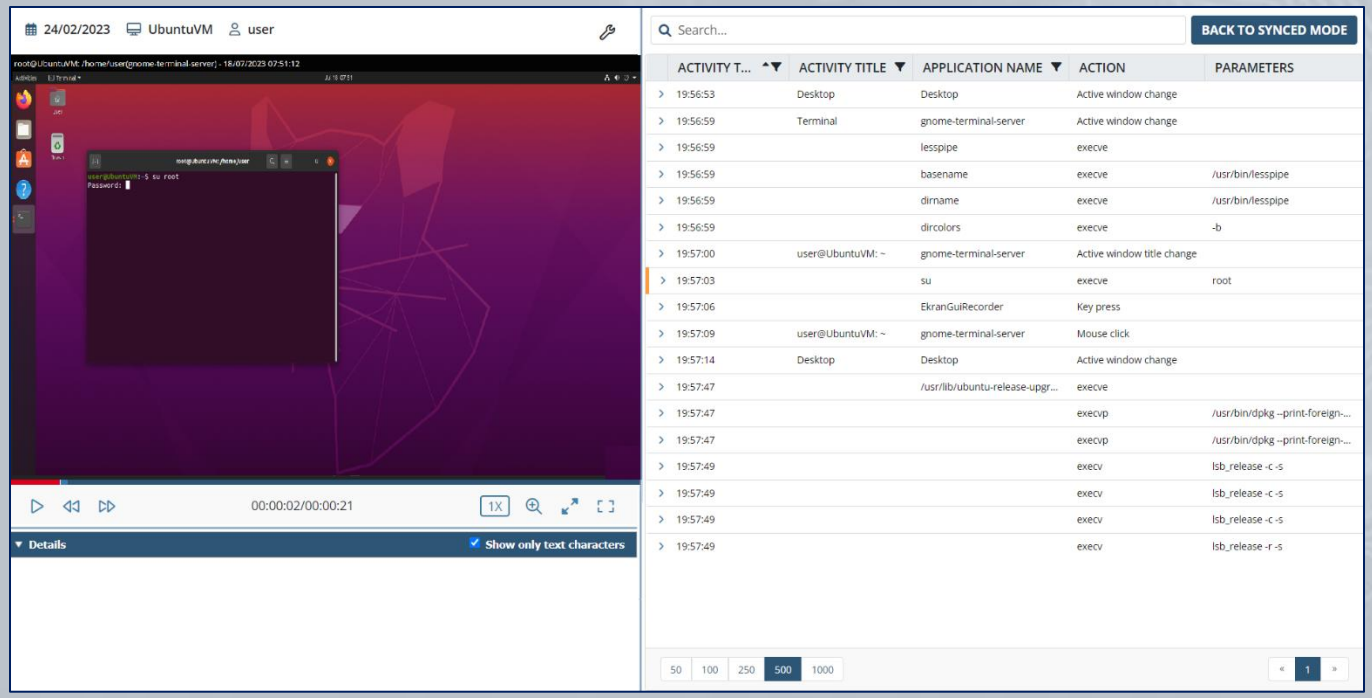

Monitoring of Linux **sessions started locally** via the GUI (**X11**) is also supported.

# Monitoring Linux Clients (Local Sessions)

Syteca

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

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

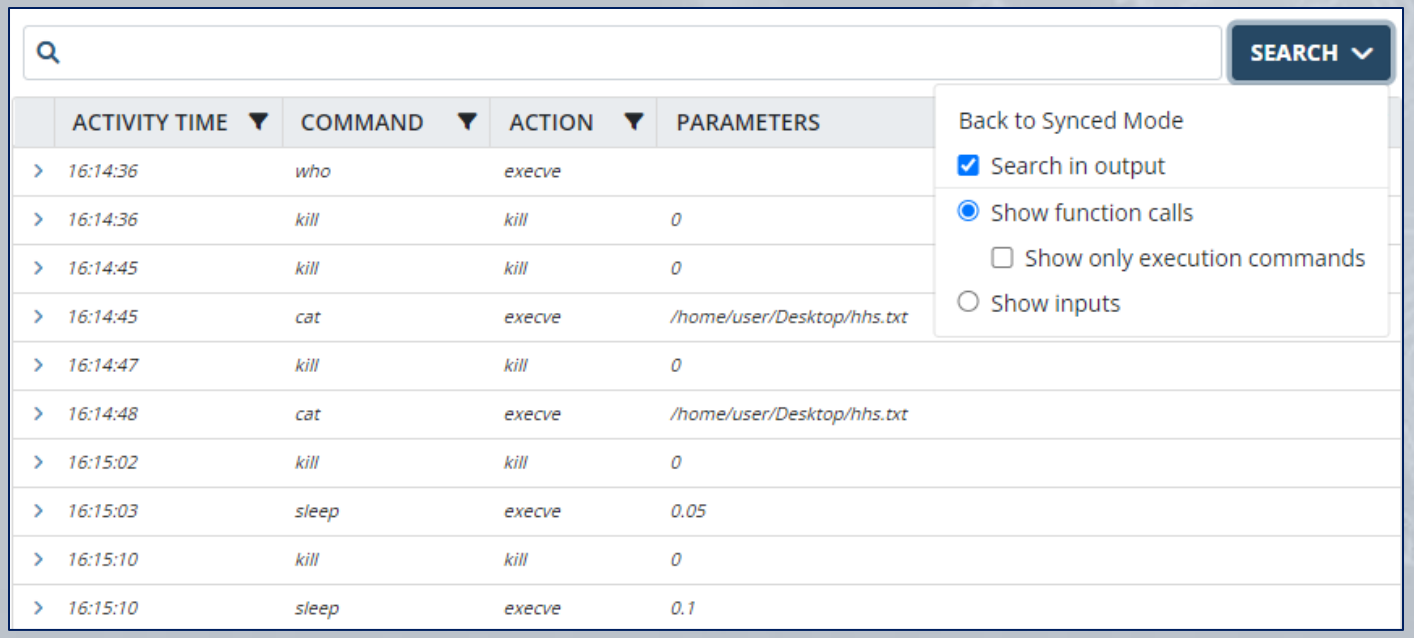


# Monitoring Linux Clients (Remote SSH Sessions)

Syteca

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

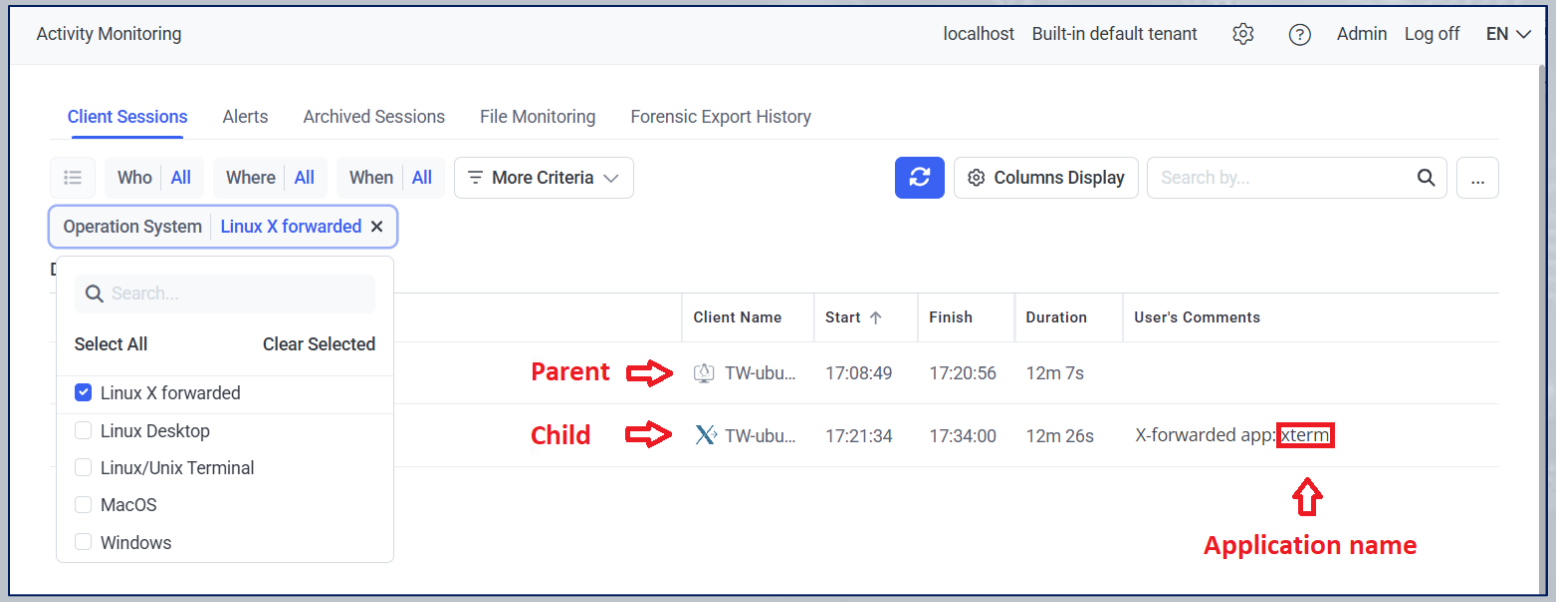
- **User actions** (keystrokes and commands & parameters **input**), and responses **output** from a terminal.
- System **function calls**.
- **Commands** executed in scripts run.



# Monitoring Linux Clients (X-Forwarded Sessions)

Syteca

- **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.



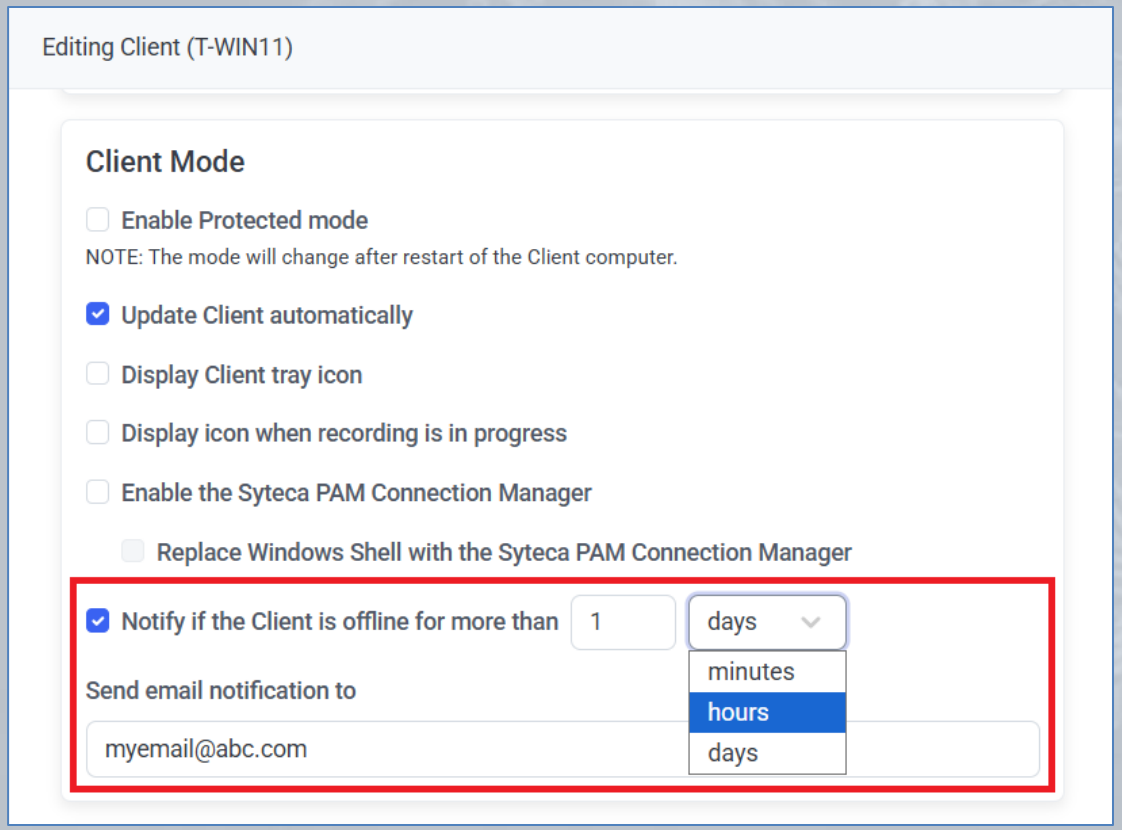
# Detection of Disconnected Clients

# Detection of Disconnected Clients

Syteca

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

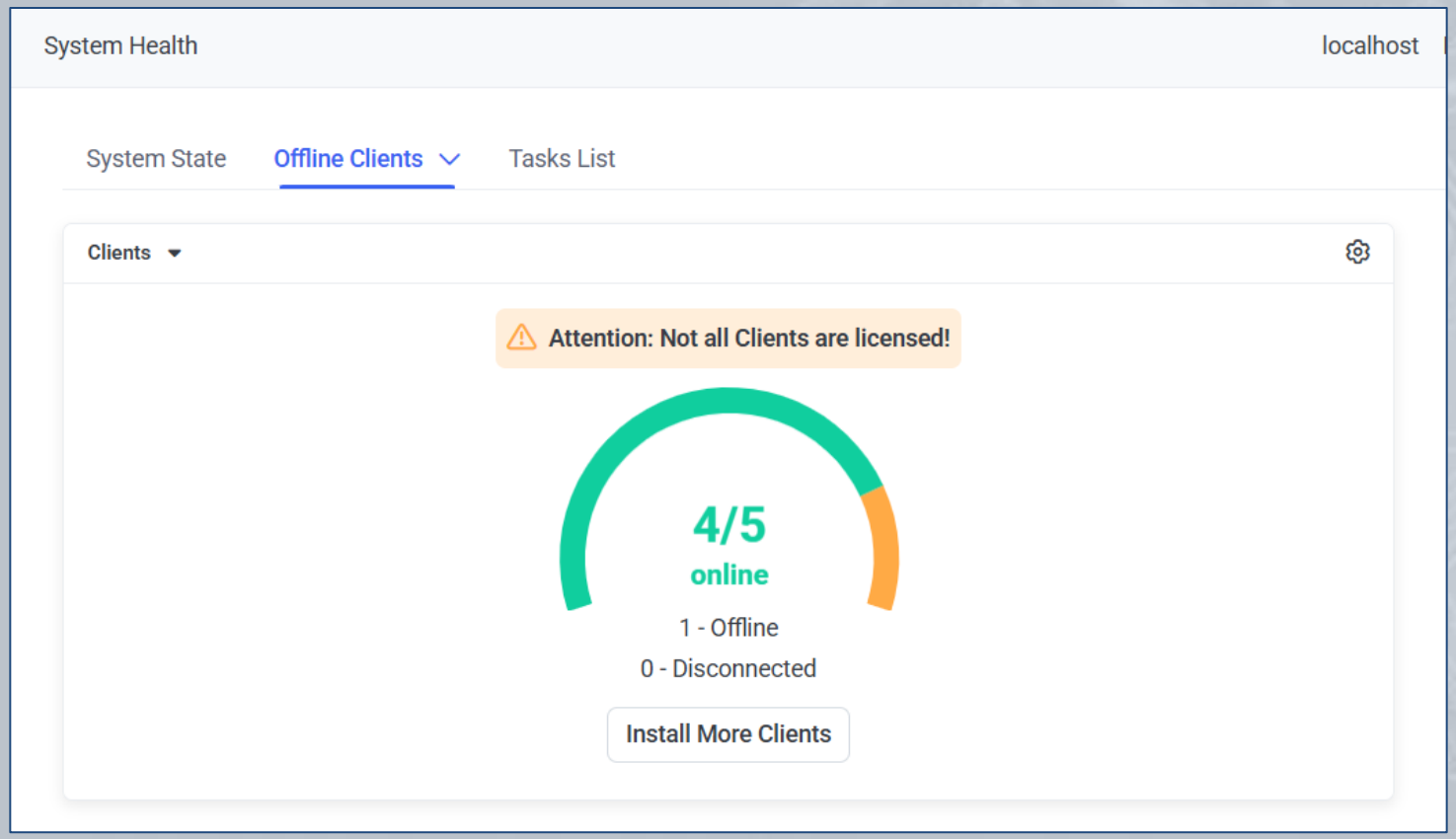
Just **define the time period** after which offline Clients will be considered as disconnected, and **get notified** about such incidents.



# Viewing Disconnected Clients

Syteca

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



# Client Protection

# Protected Mode

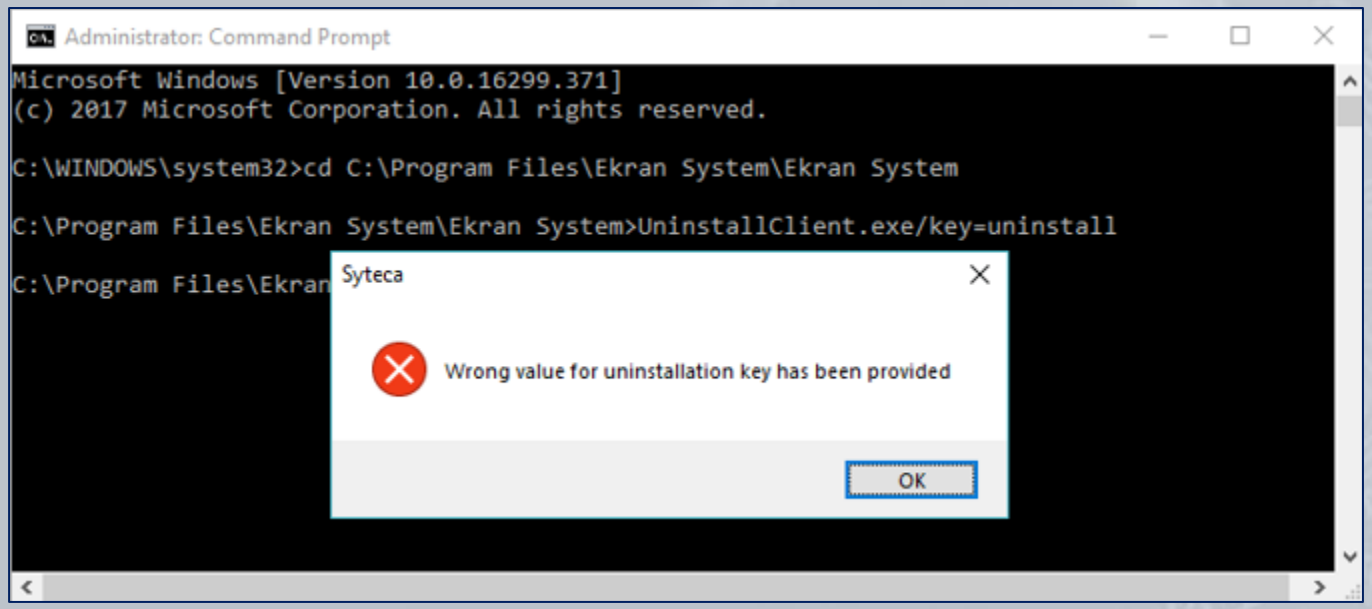
Syteca allows you to **protect Windows Clients** and their **data** by enabling Protected mode.

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

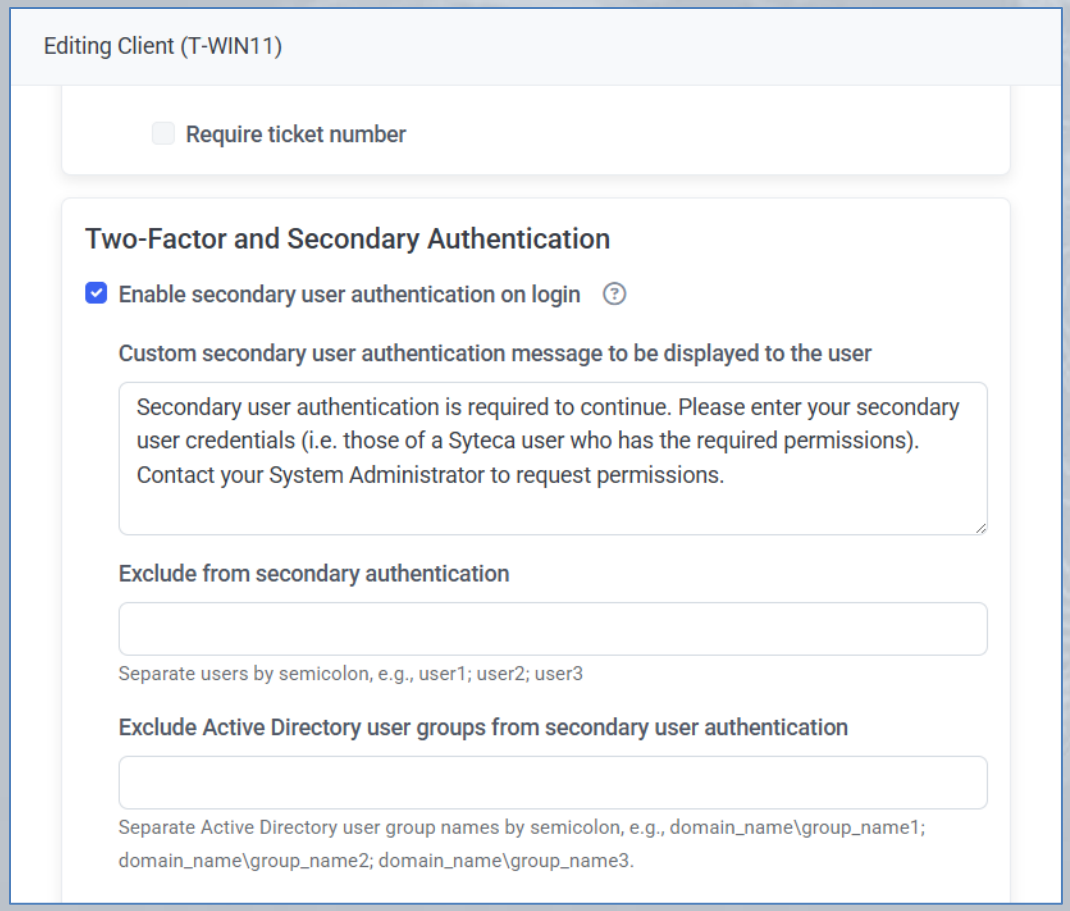
# Secondary User Authentication

# Secondary User Authentication (Windows/Linux)

Syteca

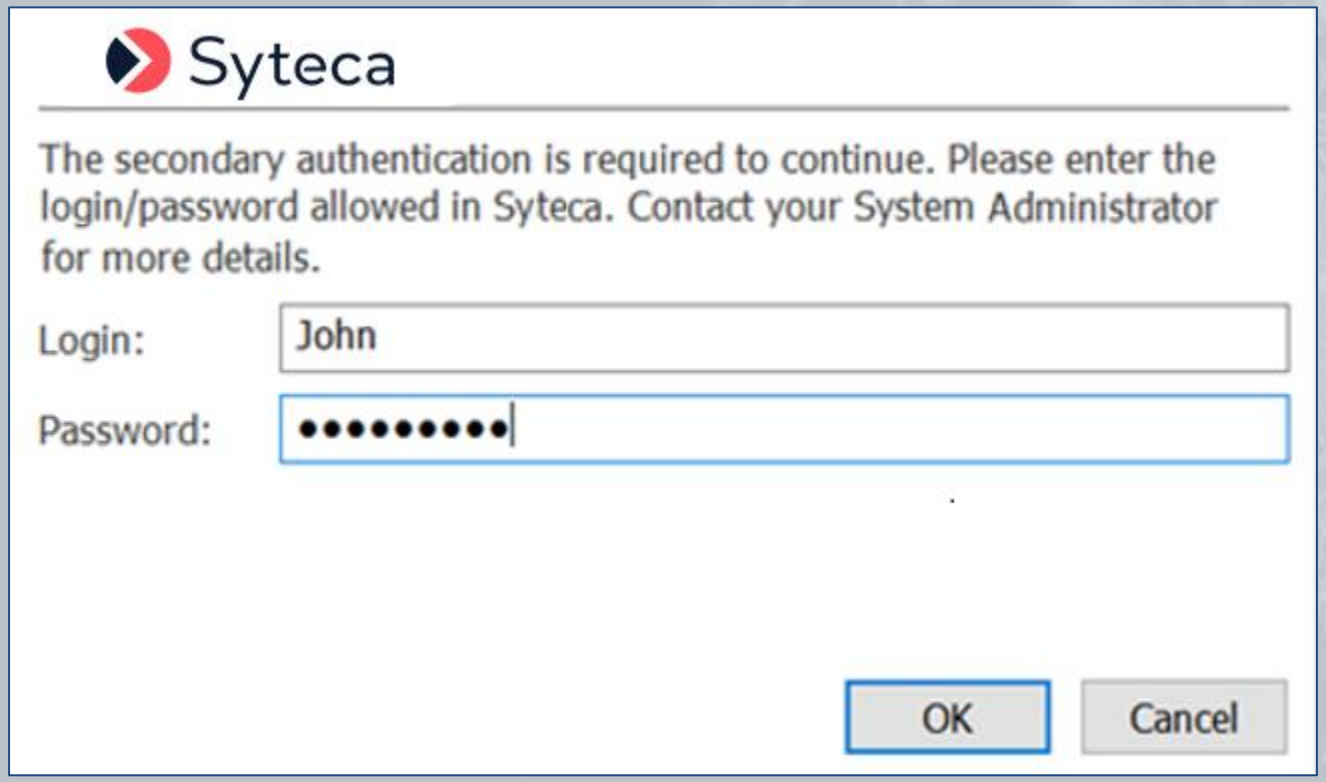
Secondary user authentication allows you to achieve **two goals**:

- 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)

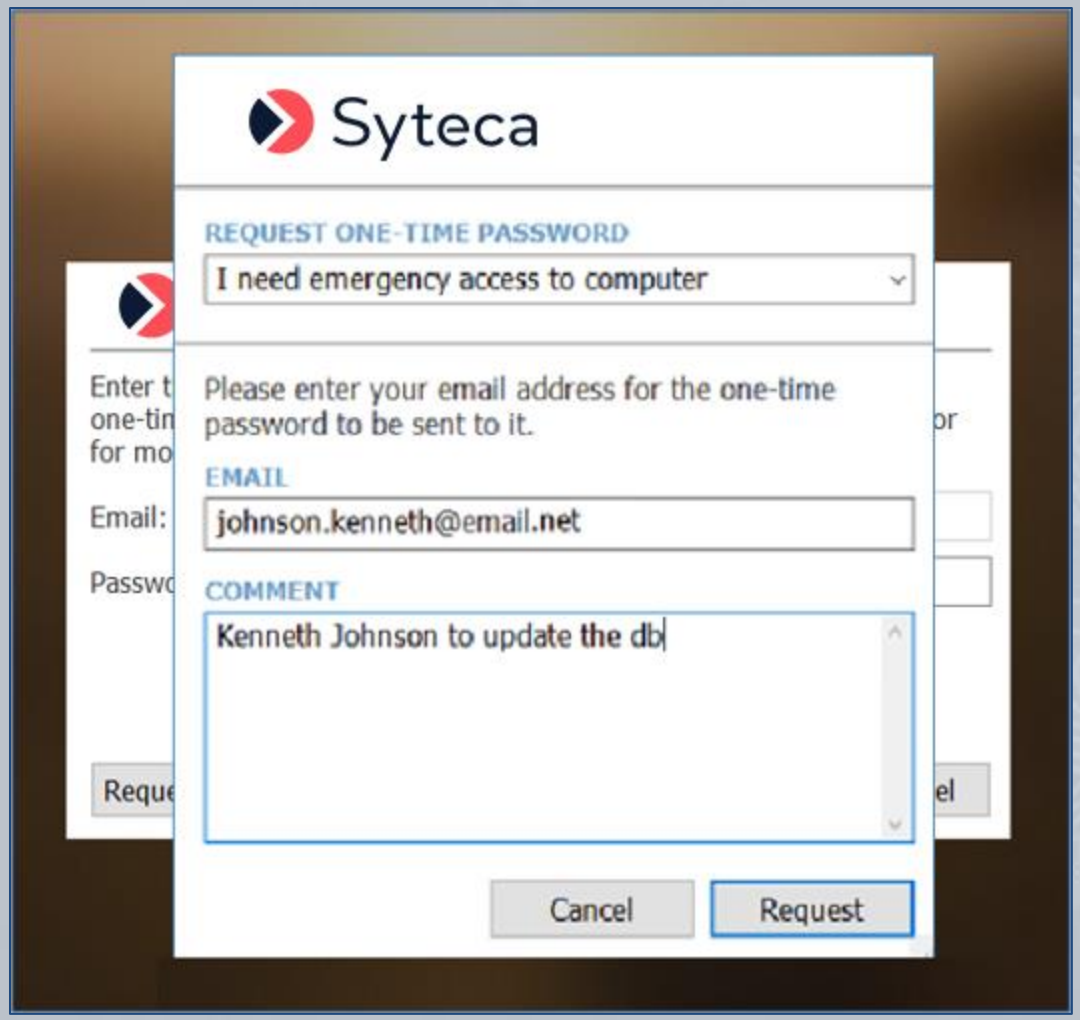
The Syteca Client requests **credentials** to be entered **before** allowing a user to **access** the Windows operating system.



# One-Time Passwords (Windows Clients)

Syteca provides the **administrator** with the unique **capability** to protect Client computers with one-time passwords.

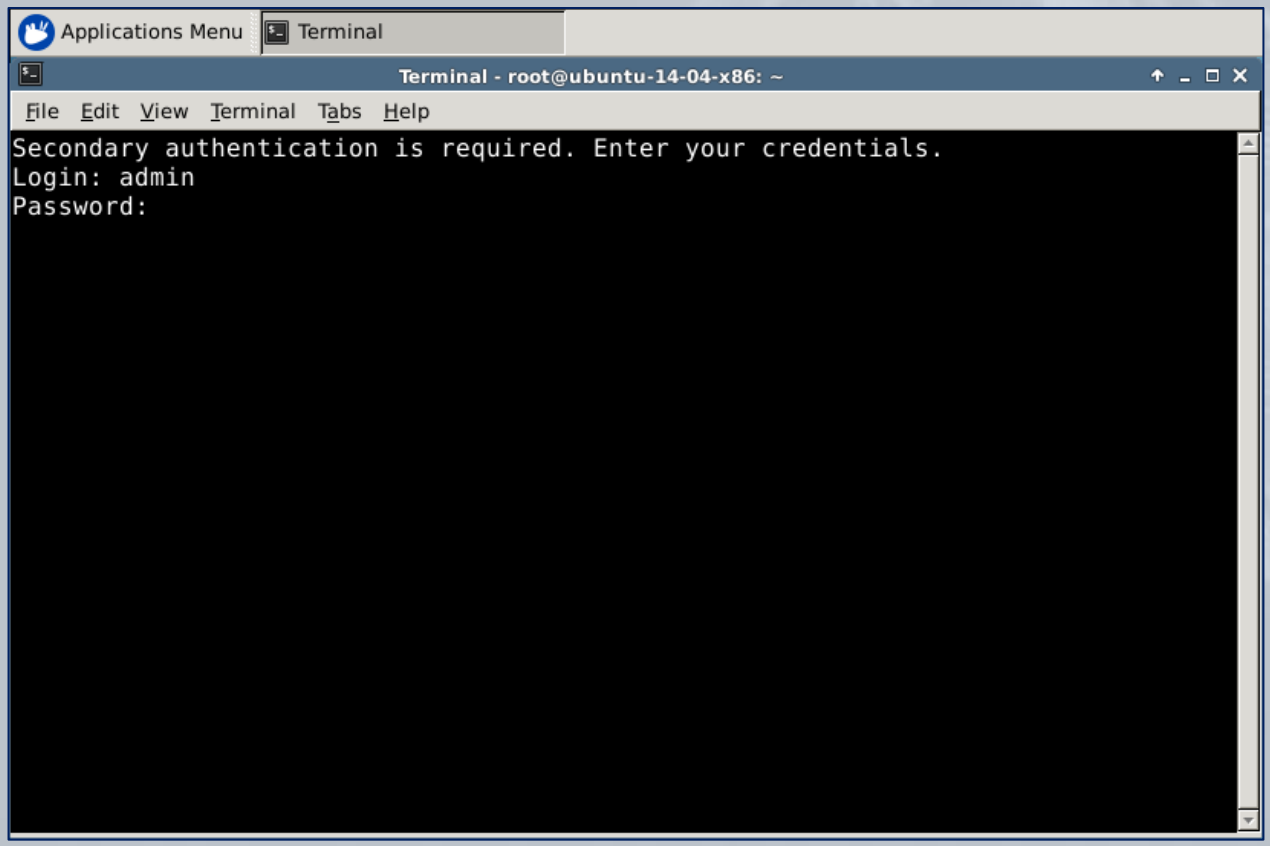
The **user** can **request** a **one-time password** directly **from** the secondary user authentication **window** displayed **during login** to the Windows OS.



# Secondary User Authentication (Linux Clients)

Syteca

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

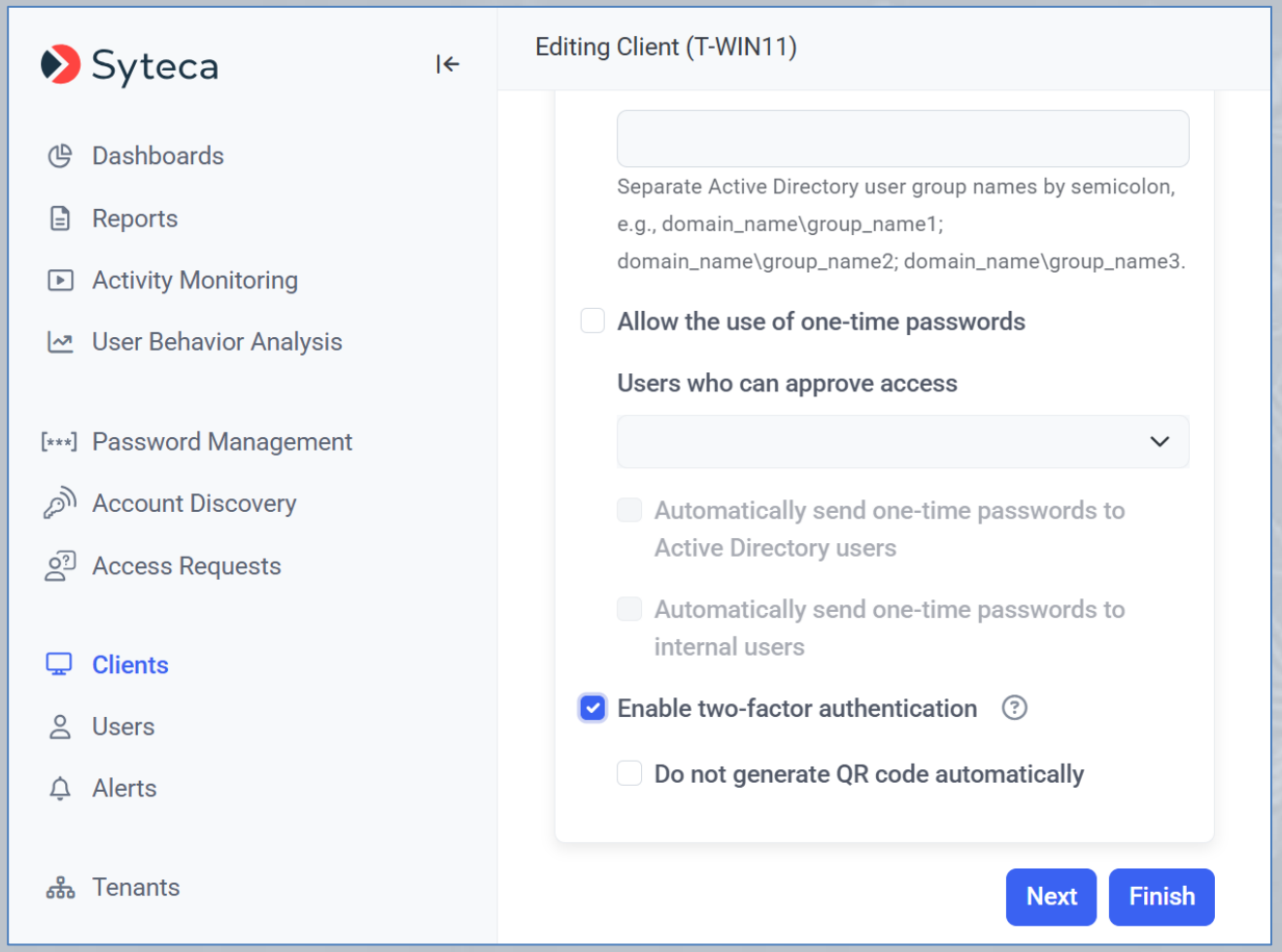


# Two-Factor Authentication

# Two-Factor Authentication (Windows/Linux)

Syteca

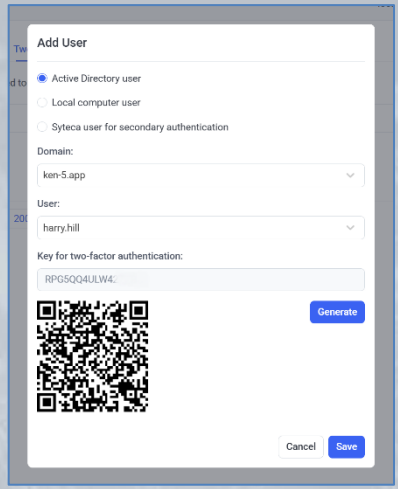
Two-factor authentication allows you to enable an **extra layer of security** to better protect the critical endpoints in your network.

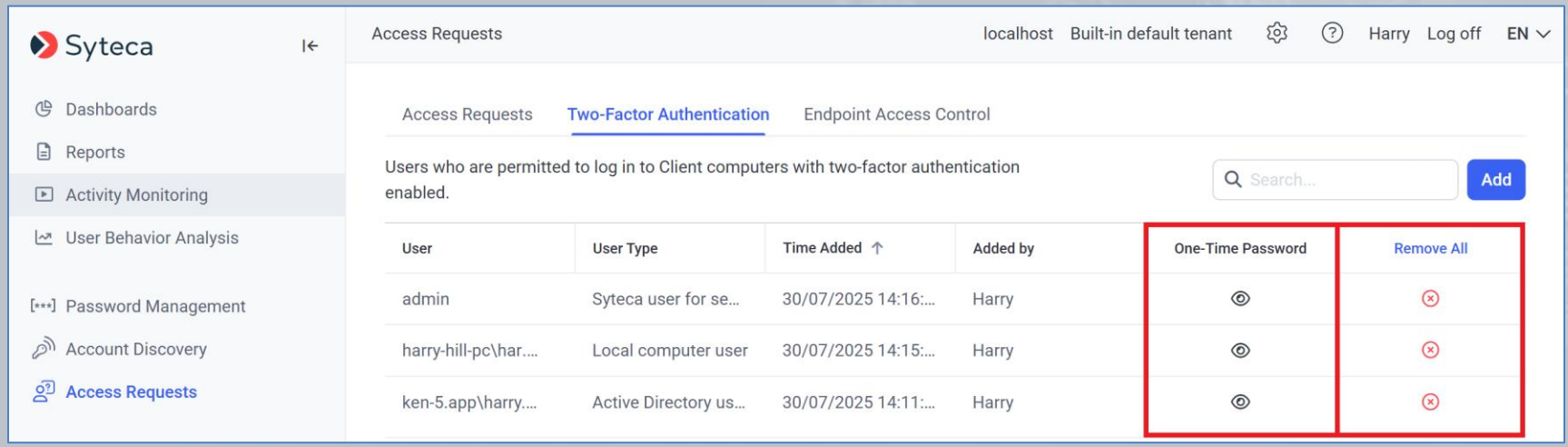


# Two-Factor Authentication (Windows/Linux)

Syteca

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.

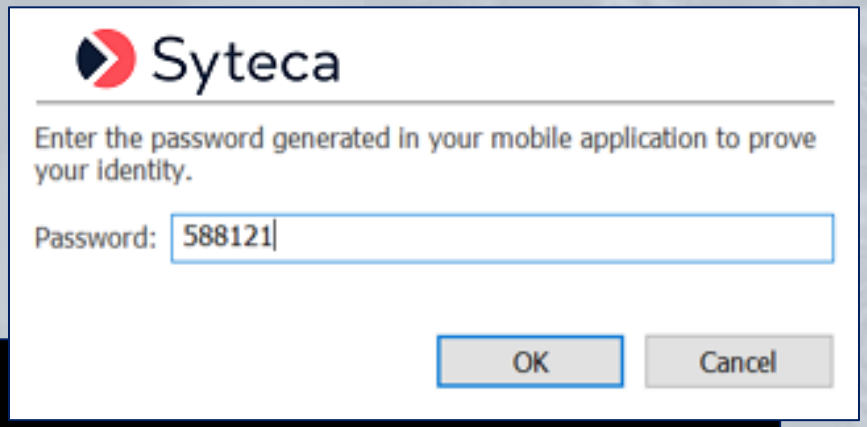


# Two-Factor Authentication (Windows/Linux)

Syteca

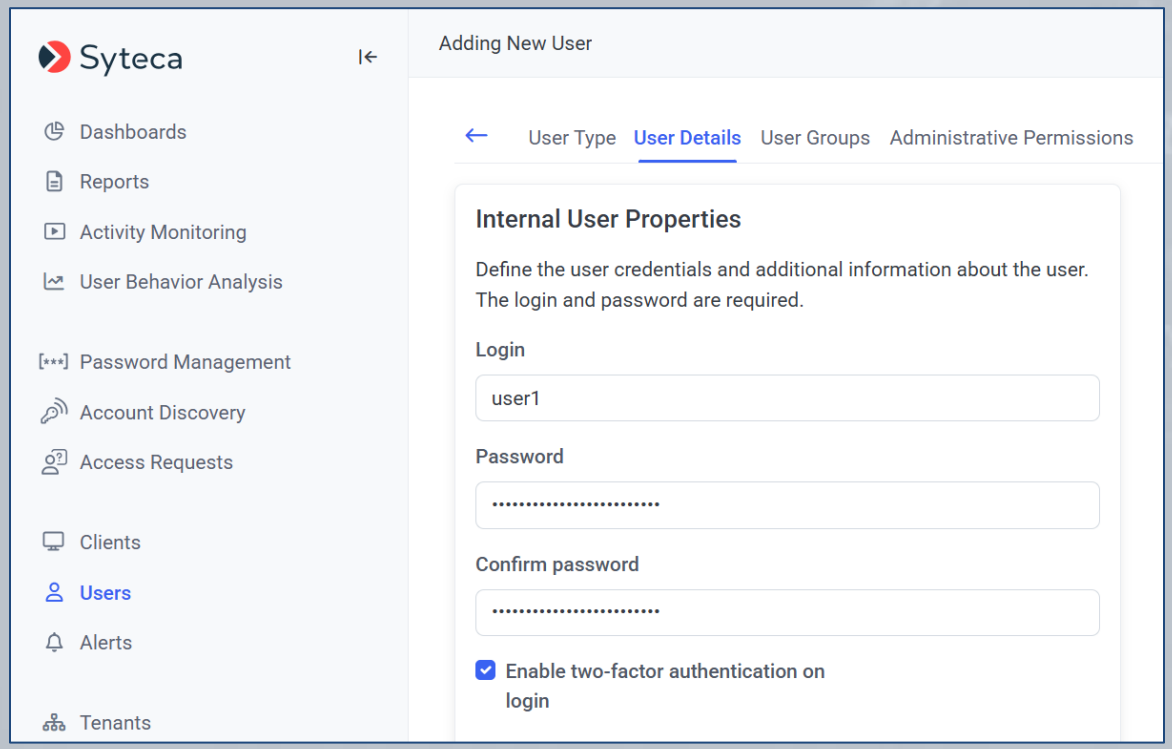
The Syteca Client **prompts the user to enter a TOTP** to access the system.

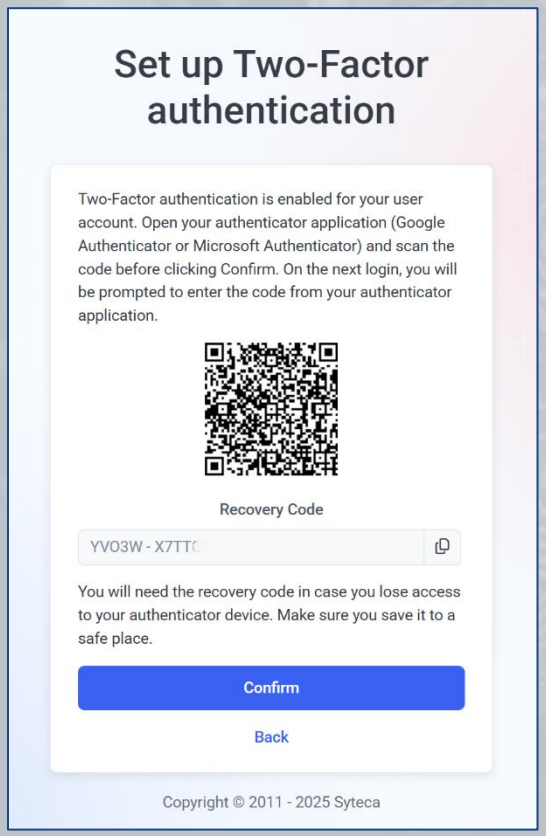



```
Ubuntu 16.04.2 LTS ubuntu tty2

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 Syteca **Management Tool users**.



# Password Management (PAM)

# Password Management

Syteca

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

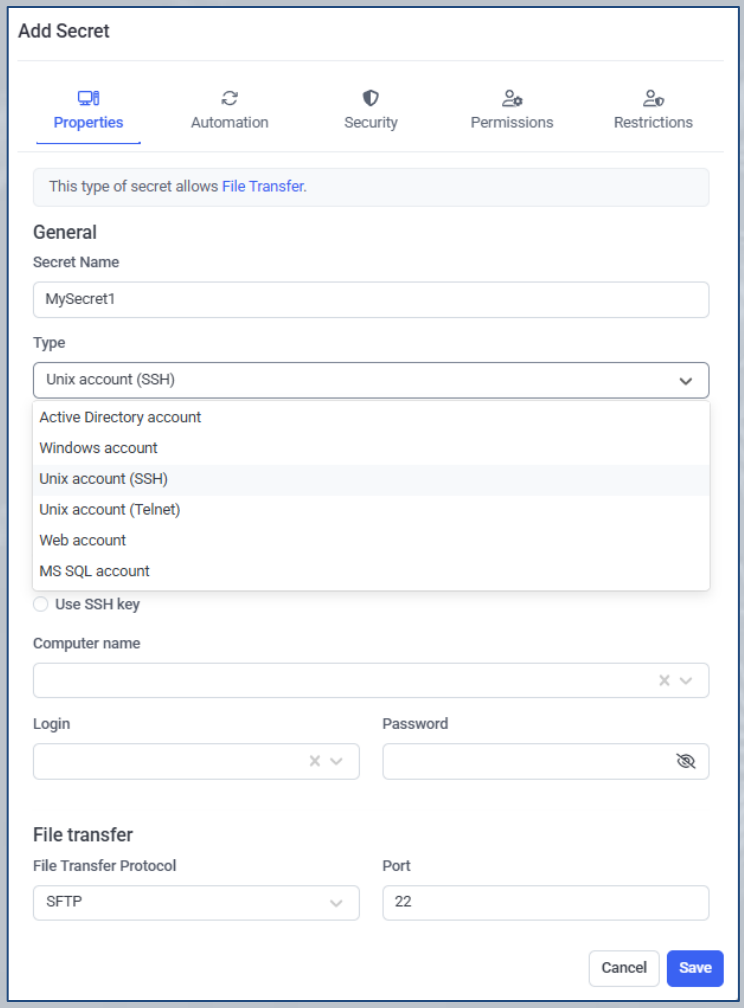
With Syteca, you can:

- 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, or **audit** any secret (to see when it was managed and used).
- Allow users to **view/copy a secret's password**, or **transfer files using WinSCP**.
- **Create** (and manage) **your own private Workforce Password Management (WPM) secrets**, which are **hidden from other users** (unless specifically shared with them).

# Adding a Secret

Add a secret manually by specifying:

- a **privileged account** to connect to
- the account **credentials**
- and **users / user groups** to give access to
- and much more!

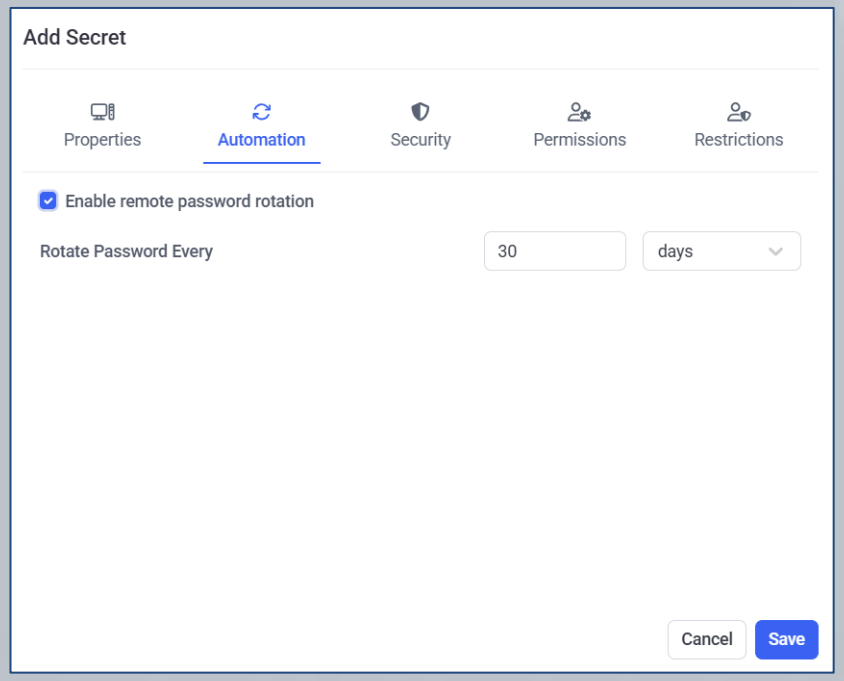


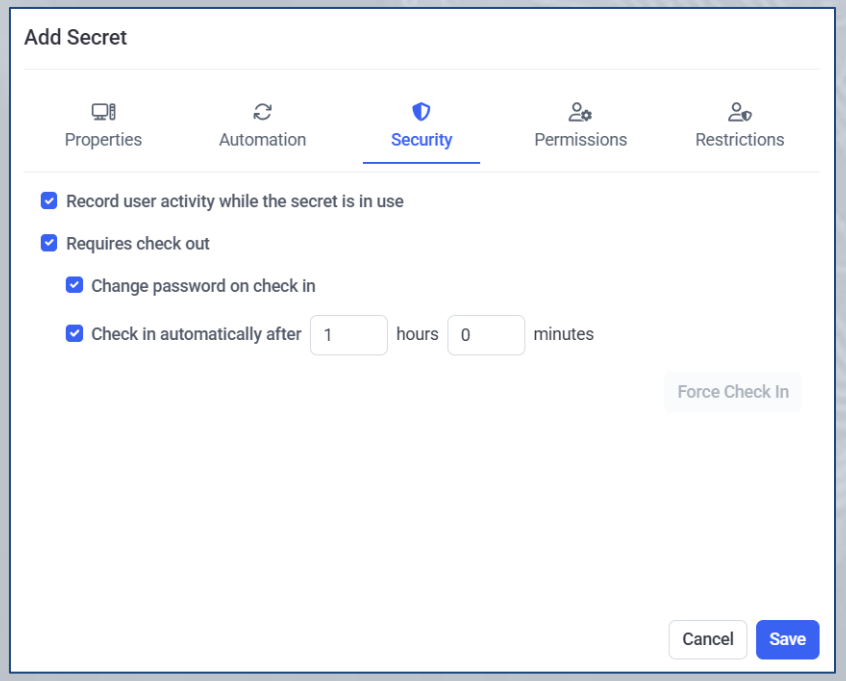
# Adding a Secret (Enhanced Security Options)

Syteca

To enhance security further, optionally for the secret:

- enable **remote password rotation**
- **Record user activity only** while a **user is accessing** the secret
- require **password checkout**



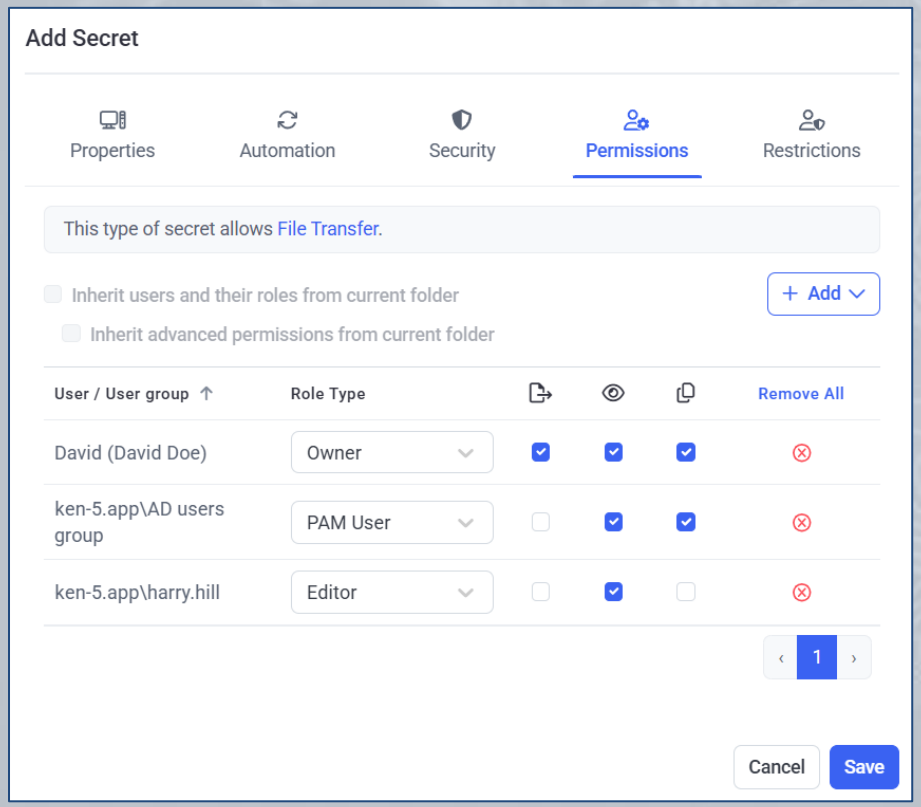



# Adding a Secret (Users & Permissions)

Syteca

To define users' access to a secret:

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

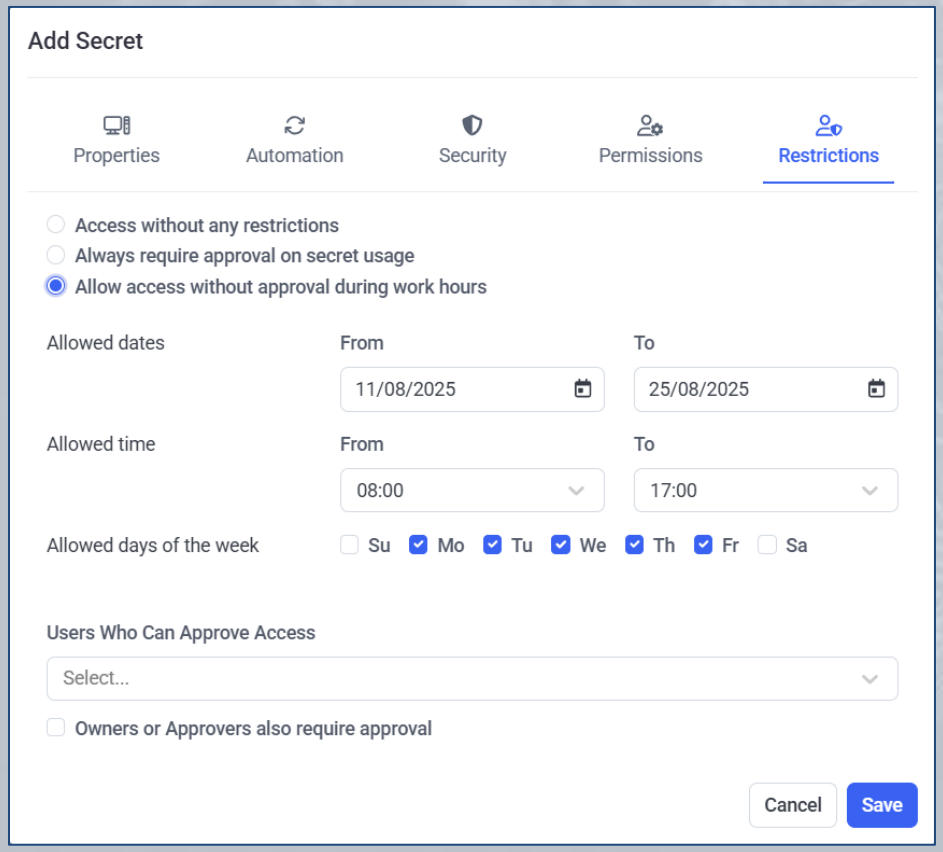


# Adding a Secret (Access Restrictions)

Syteca

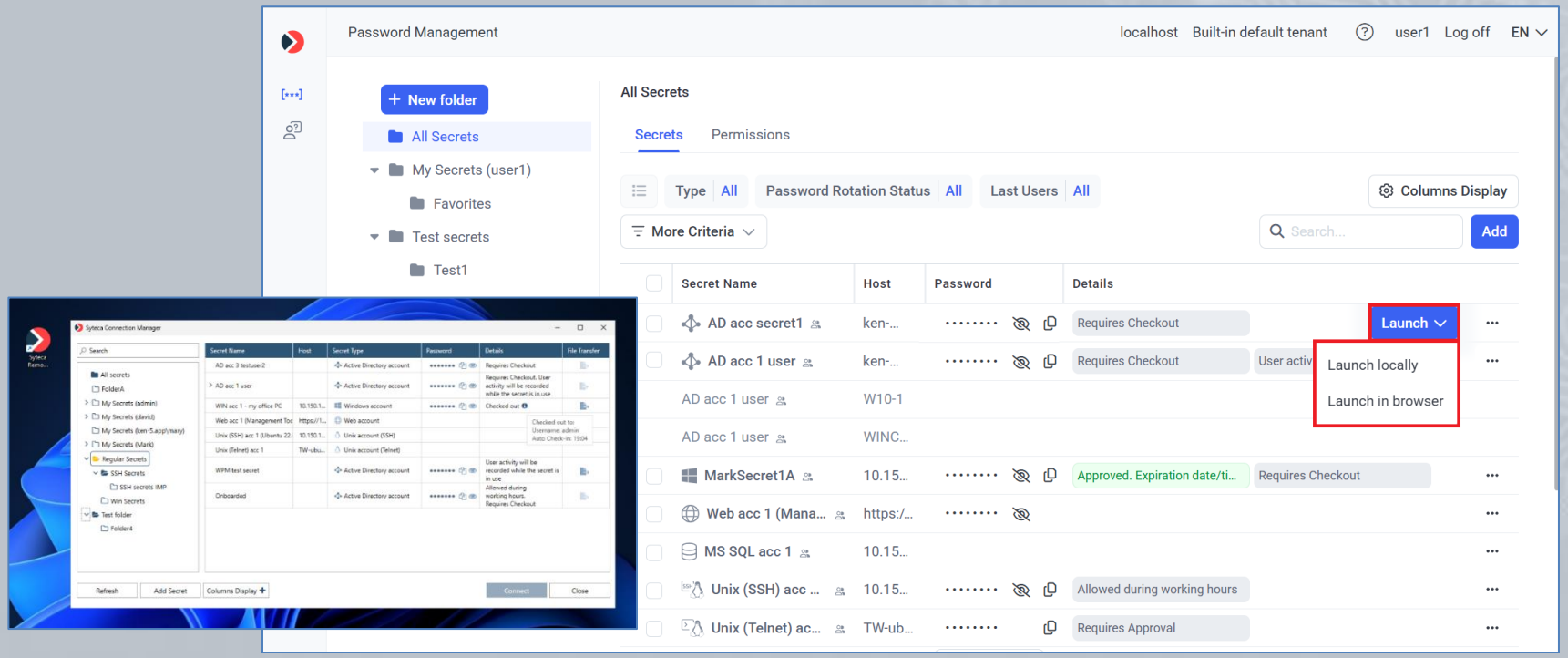
To enhance security still further, **restrict access** to the secret **by requiring approval** from a supervisor:

- on **secret usage**
- or only **outside of** specific:
  - (work) **hours**
  - and **days** of the week.



# Using a Secret

A **privileged user can access a critical endpoint via a secret** by using either the **Web** (incl. **agentless PAM**) or **Desktop** version of **Syteca Connection Manager**. The secrets are stored in a granular **Tree-View folder structure** and have **user permissions** for both folders and secrets.

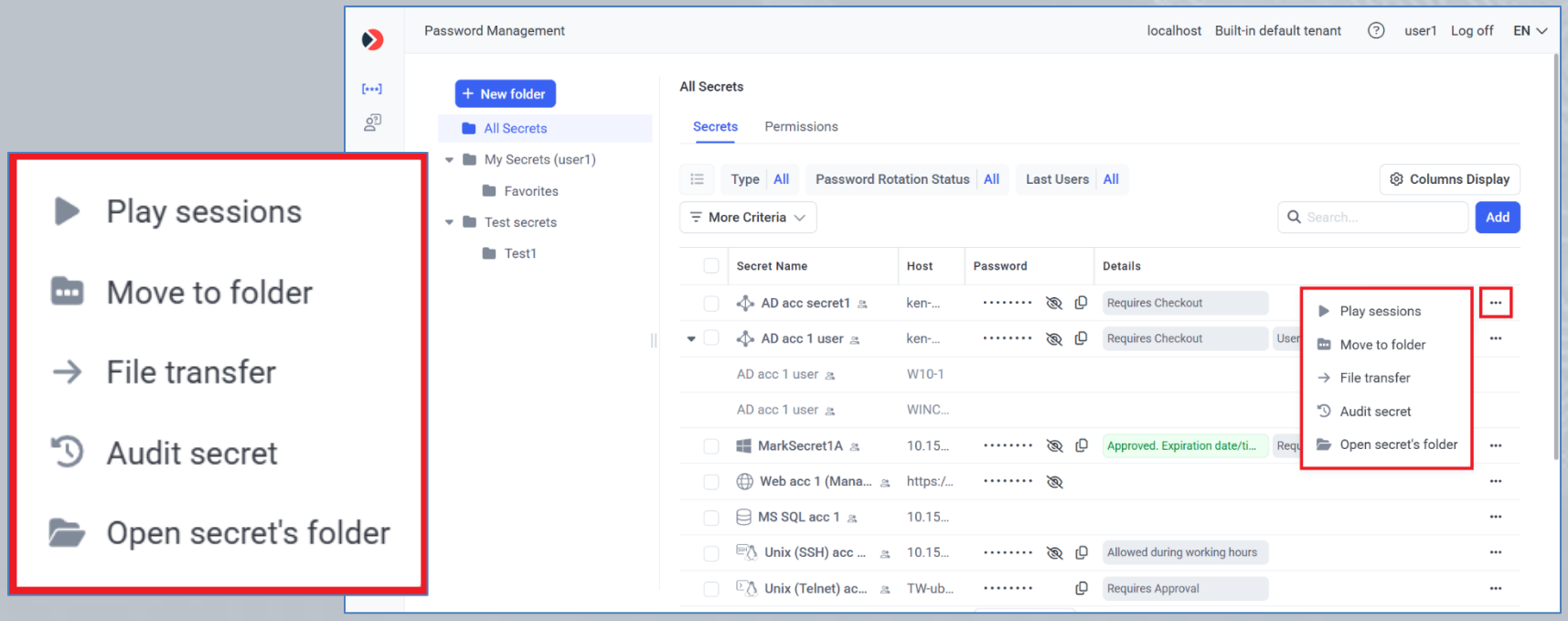


# Viewing Secrets in Sessions

Syteca

You can click **Play sessions** in a specific secret (in any folder) **to open the list of sessions that it was used in** (and the **secret data is highlighted** when playing the session in the Session Viewer).

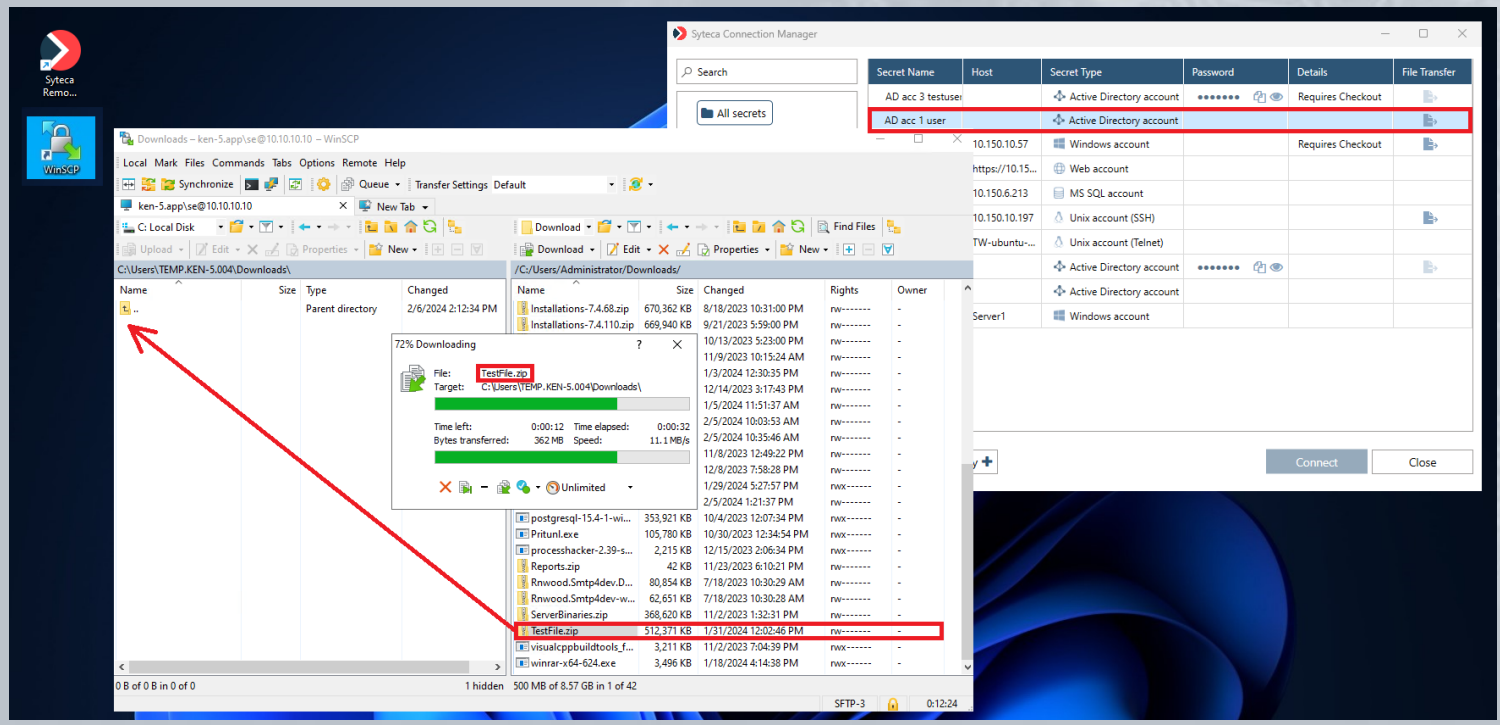
You can also click e.g. **Audit secret** to see when a secret was **managed and used** (to open the Audit Log page), etc.



# Transferring Files Using WinSCP

Syteca

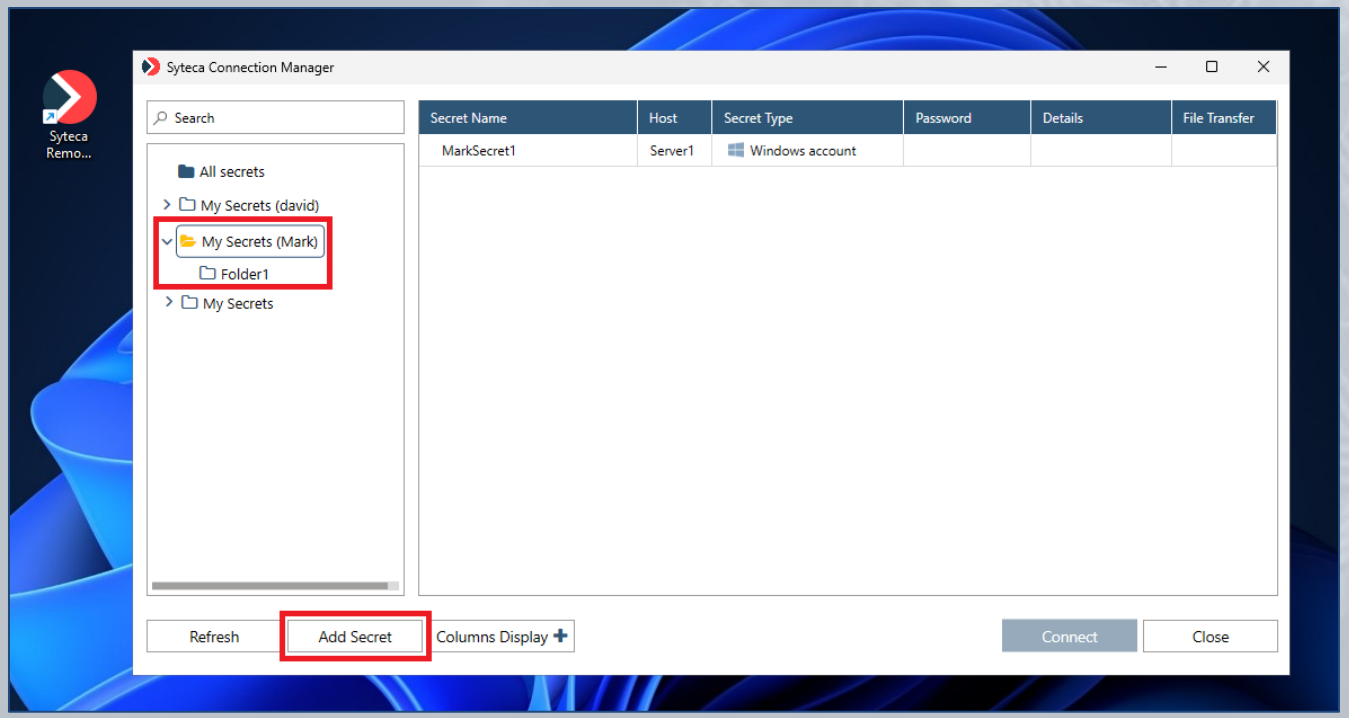
The **File Transfer** functionality allows users of secrets to transfer files **between the computer** with Syteca Connection Manager **and the remote computers** (which are accessed via the secrets) by using **the WinSCP application**.



# Workforce Password Management (WPM)

Syteca

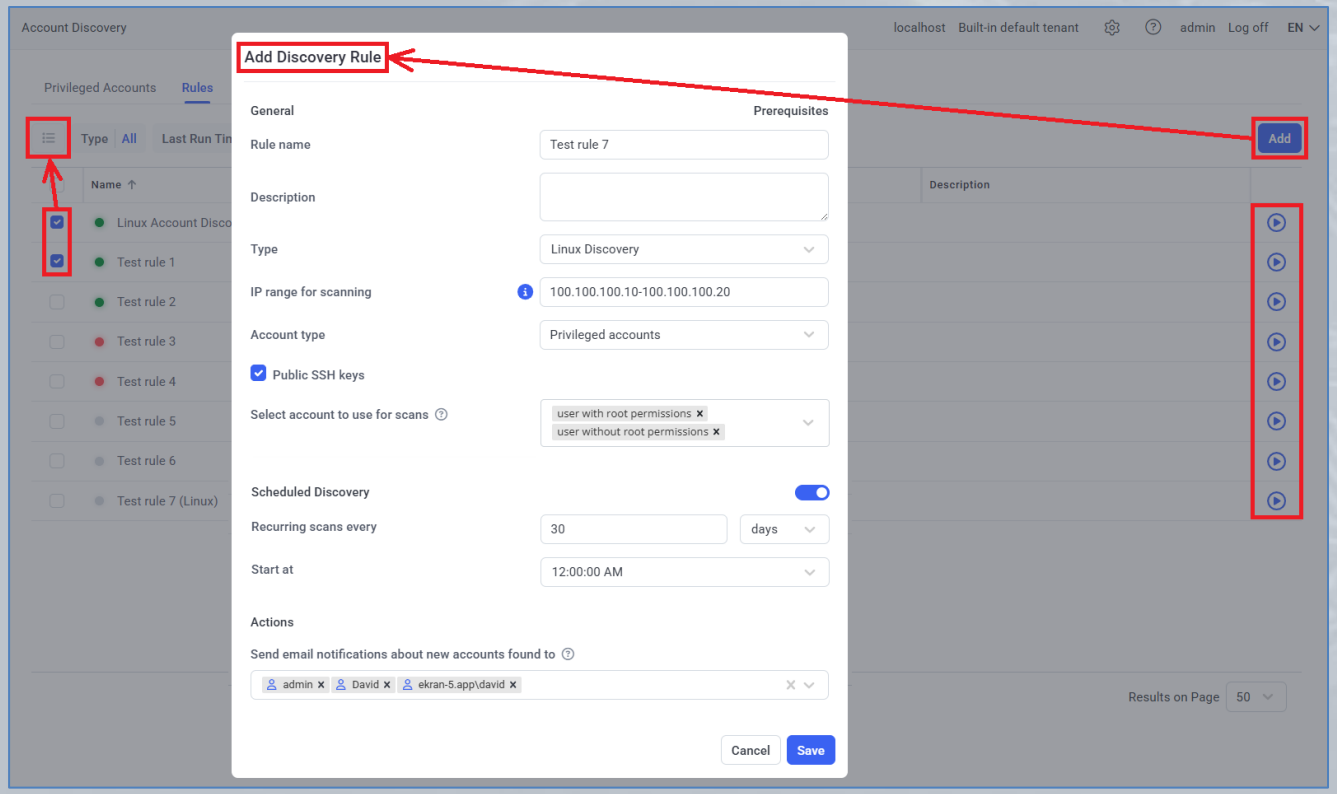
The WPM functionality enables PAM users (i.e. any **users of Syteca Connection Manager**) to **create (and manage) their own private** Workforce Password Management **(WPM) secrets**, which are **hidden from other users** (unless specifically shared with them).



# Account Discovery and Onboarding (PAM)

# Account Discovery

Account Discovery (PAM) allows **privileged** (and other) **accounts** to be **discovered** (by performing **network scans**), and then **onboarded into secrets**, by first **adding and running** account discovery **rules**.

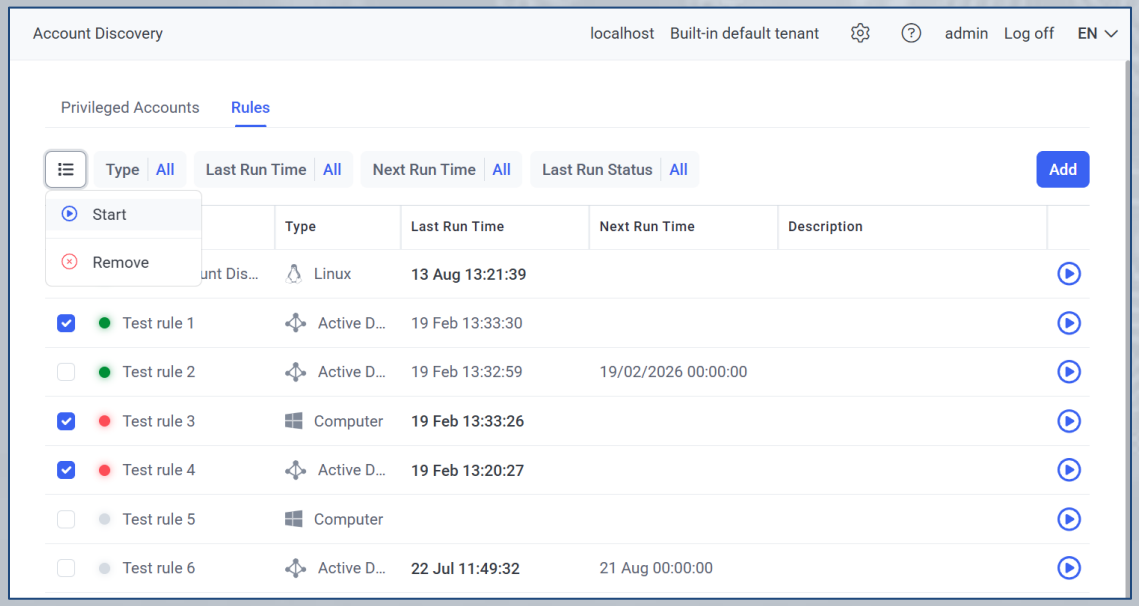


# Account Discovery

Syteca

Various **types** of **discovery rules** can be added:

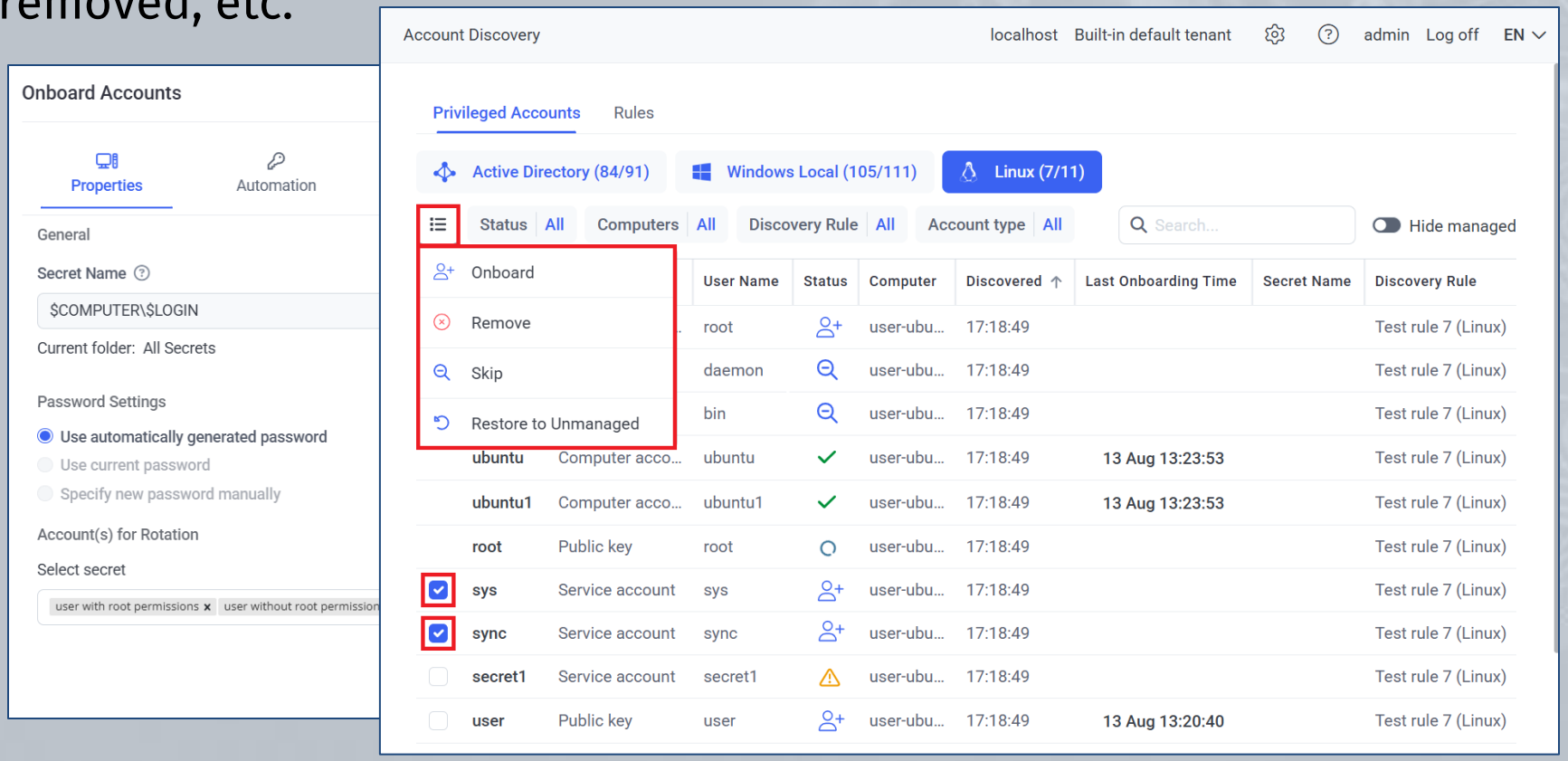
- **Active Directory** (for privileged **AD domain** accounts).
- **Computer** (for privileged **Window local** accounts).
- **Linux** (for privileged, **service**, and **application** accounts, including accounts with **public SSH keys**).



# Account Onboarding

Syteca

The accounts discovered can then be selectively **onboarded** into **new secrets** (either individually, or by using **Bulk Action**) or skipped, removed, etc.



# User and Entity Behavior Analytics (UEBA)

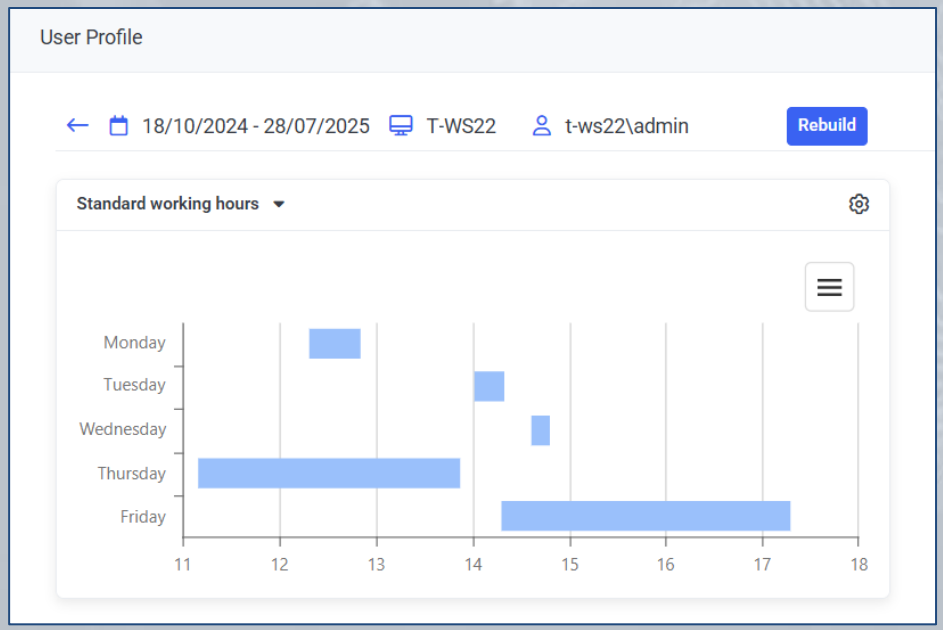
# User and Entity Behavior Analytics (UEBA)

Syteca

Syteca 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:

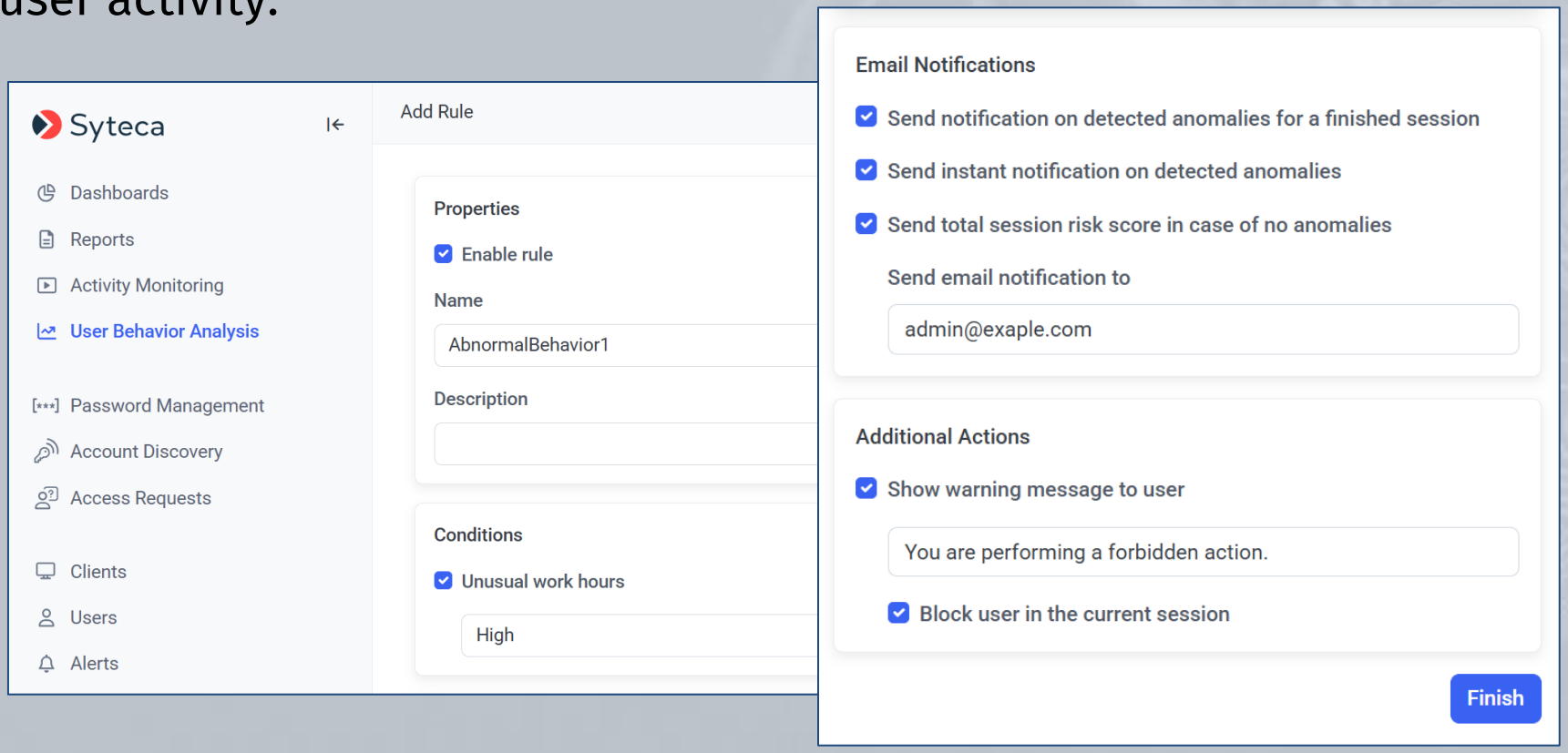
- **Analysis** of user **behavior patterns** and establishment of a baseline for **normal behavior**.
- Automatic **detection** of behavioral **anomalies** & **deviations**.
- Timely **notification** of potential **insider threats**.



# User and Entity Behavior Analytics

Syteca

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

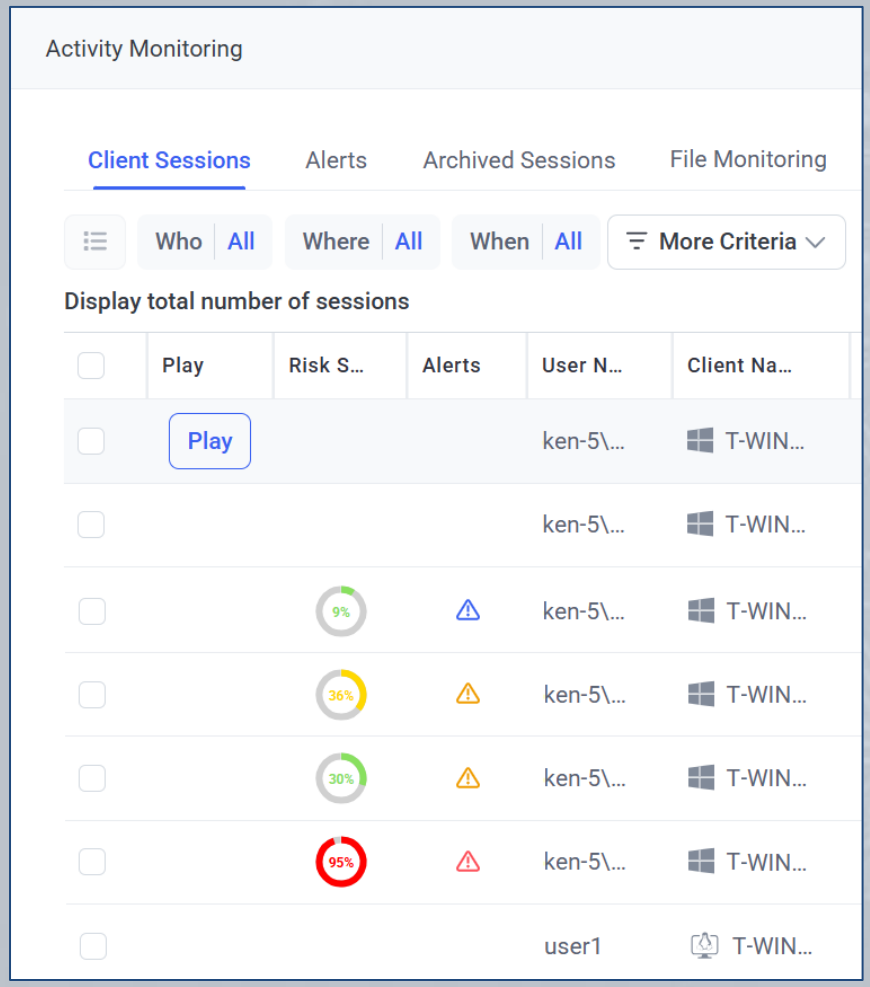


# User and Entity Behavior Analytics

Syteca

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 during activity monitoring.

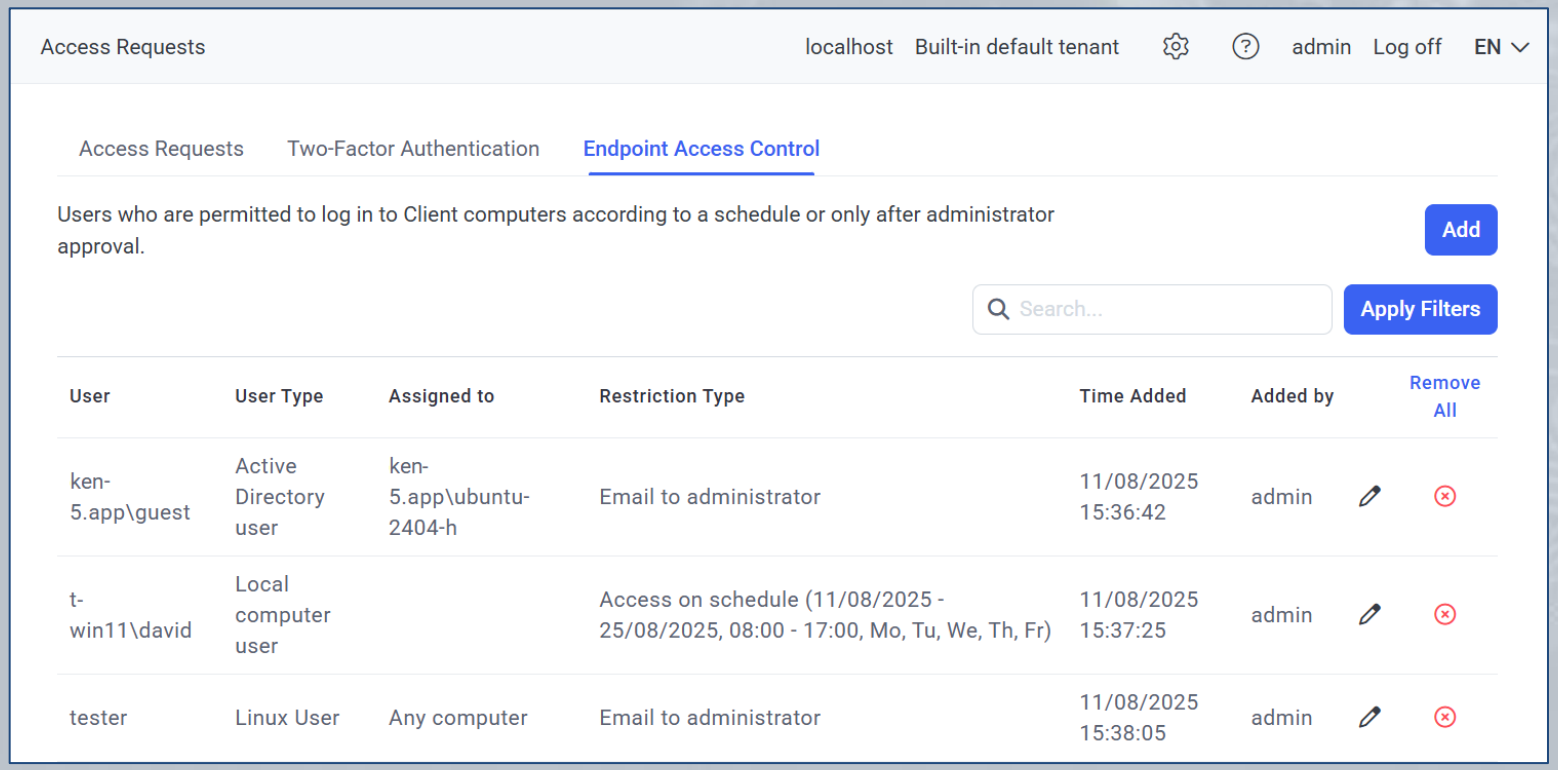


# Access Requests and Approval Workflow

# Access Requests and Approval Workflow

Syteca

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

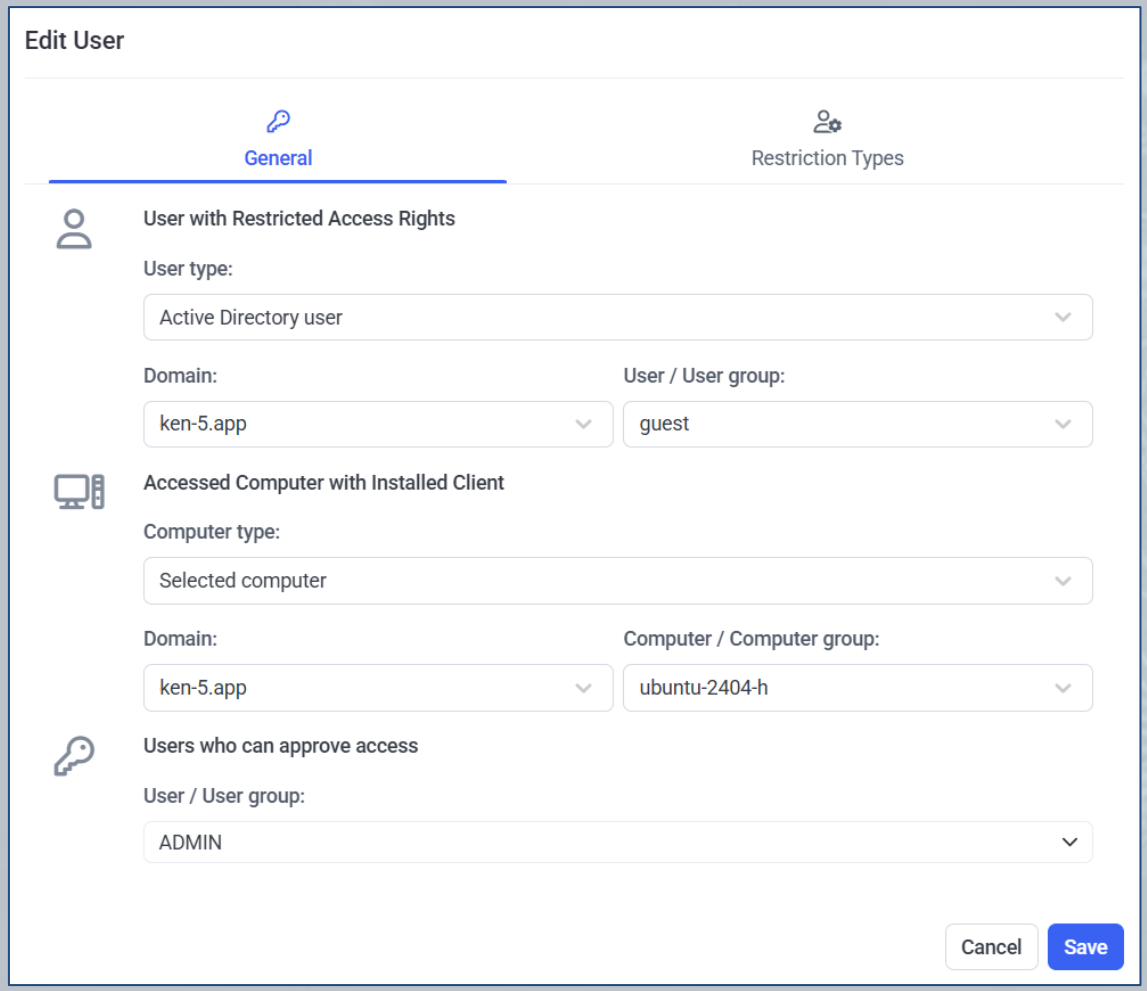


# Access Requests and Approval Workflow

Syteca

You can **add users** whose **access** to Client computers needs to be **restricted**, by using:

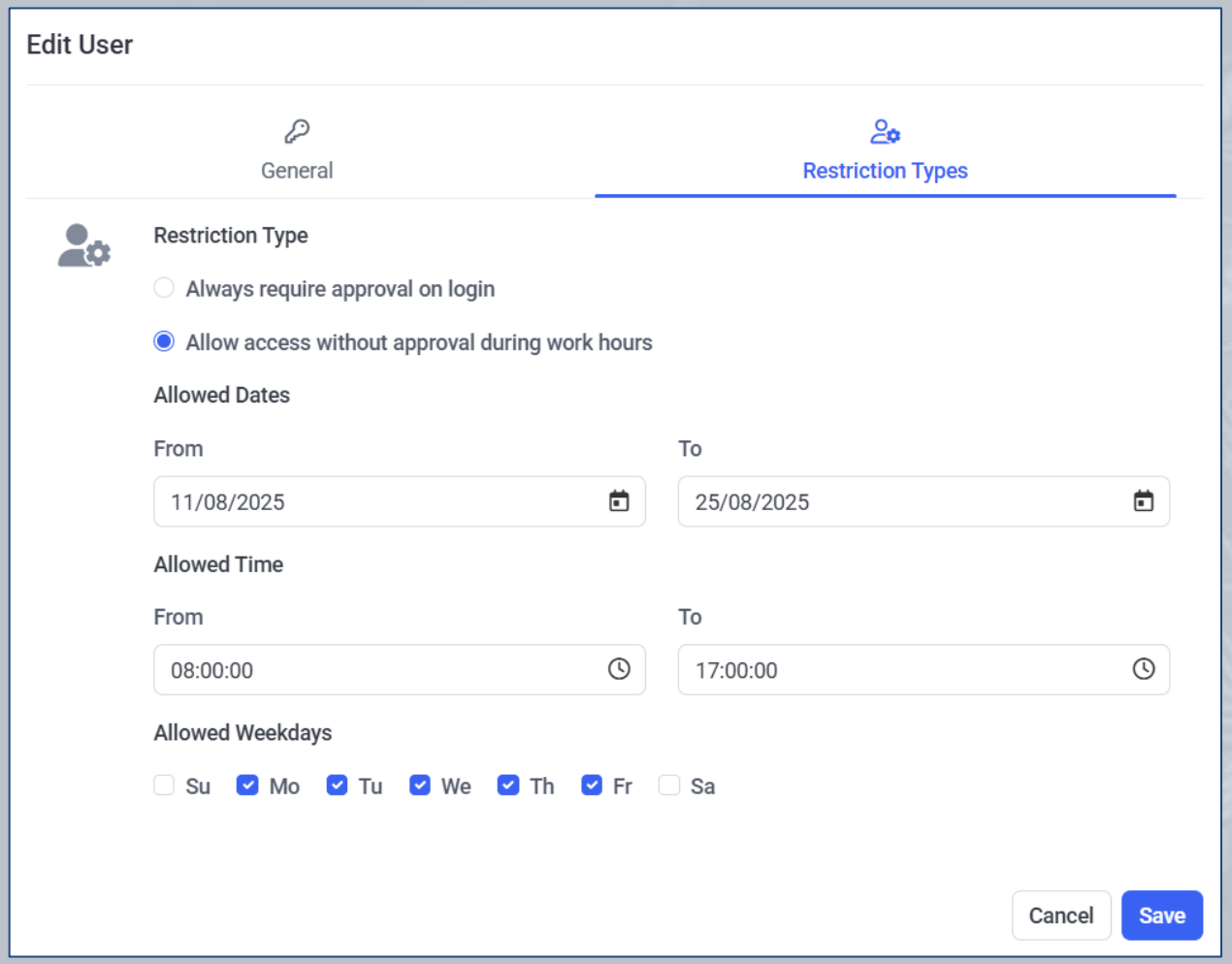
- **Manual access approval** by an administrator to determine who can access what and when.



# Access Requests and Approval Workflow

Syteca

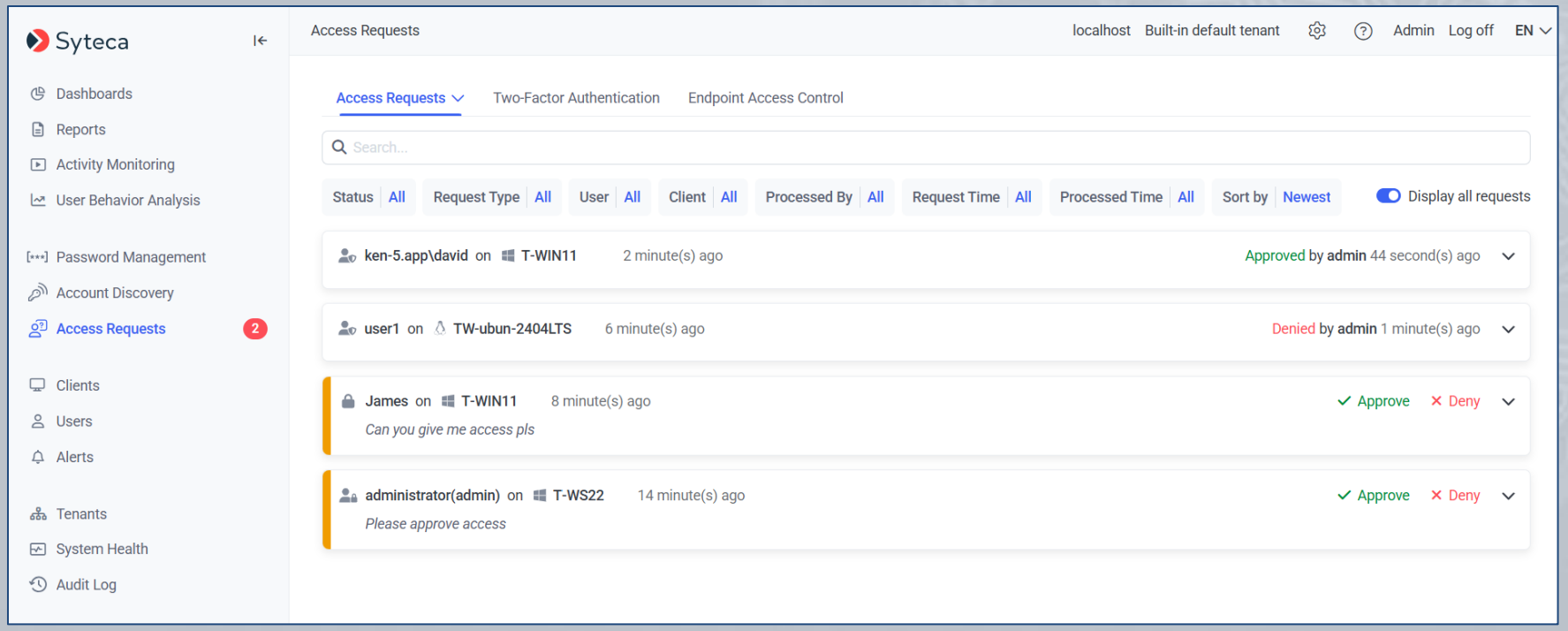
- Or **Time-based user access restriction** to enhance the protection of critical data and systems.



# Administrator Approval on Login

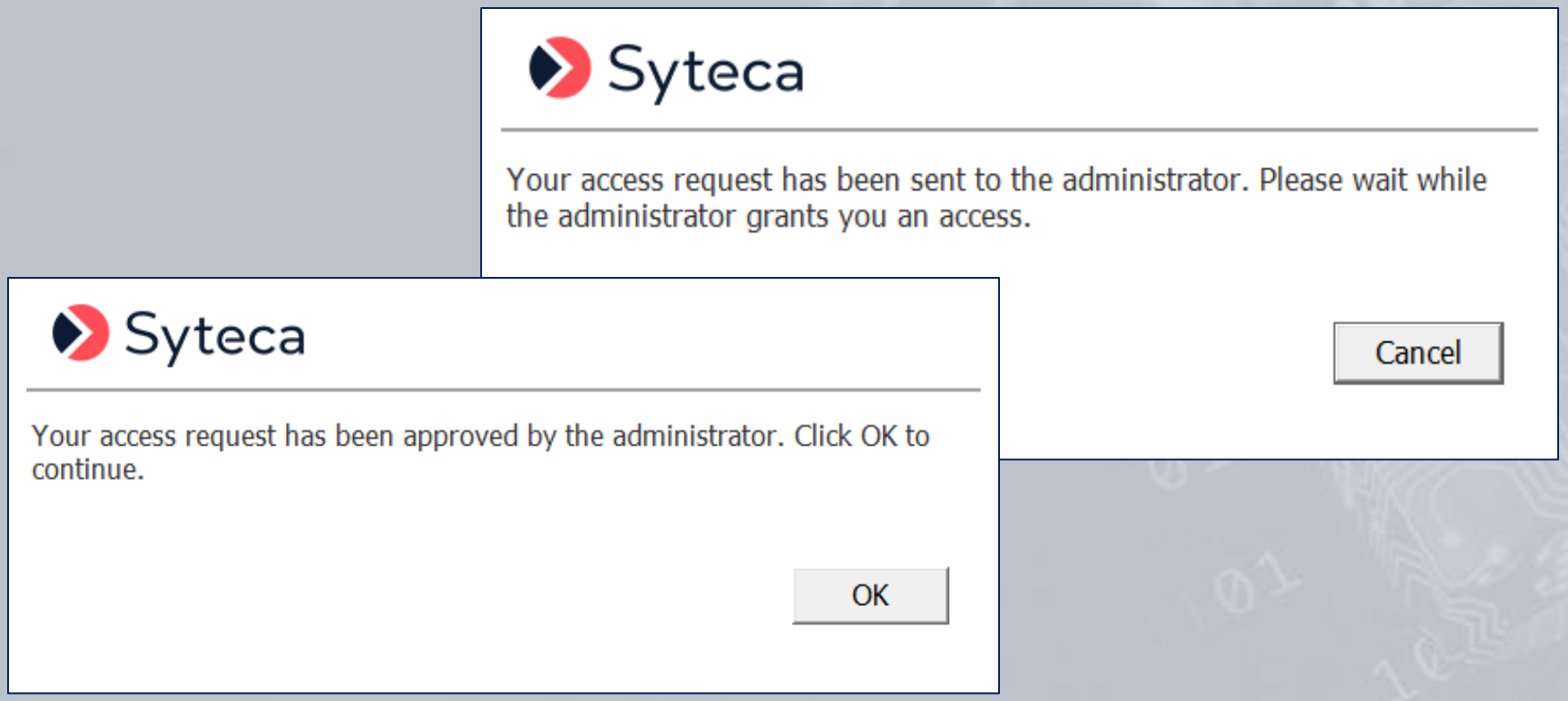
Syteca

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).



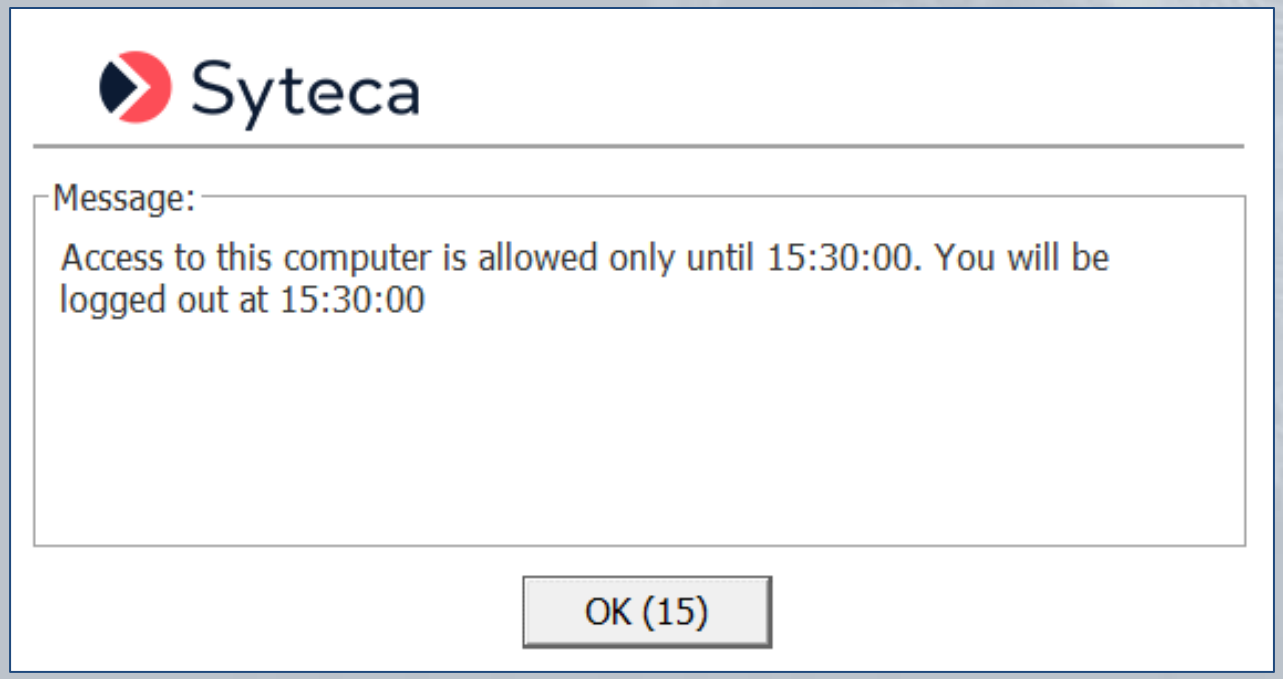
# Administrator Approval on Login

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



# Access Requests 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**.

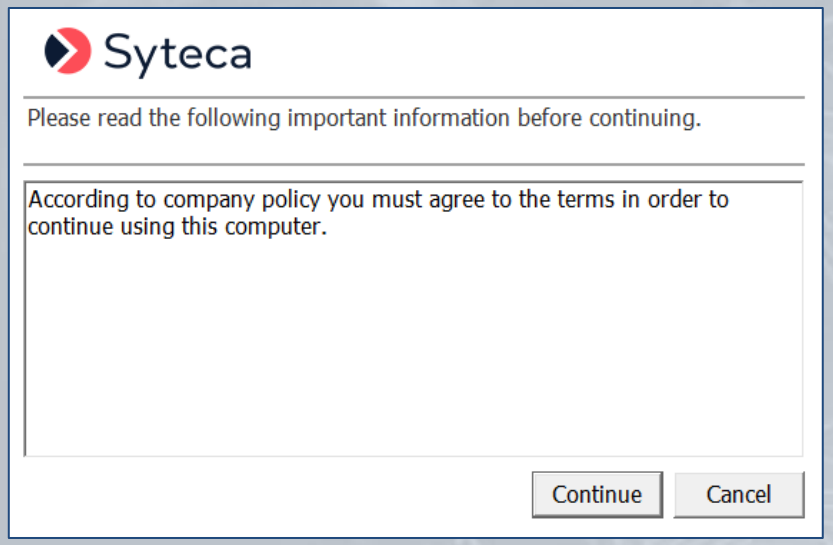


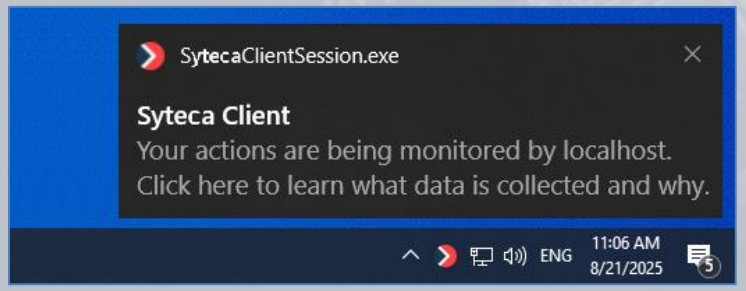
# Notifying Users About Being Monitored

# 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.

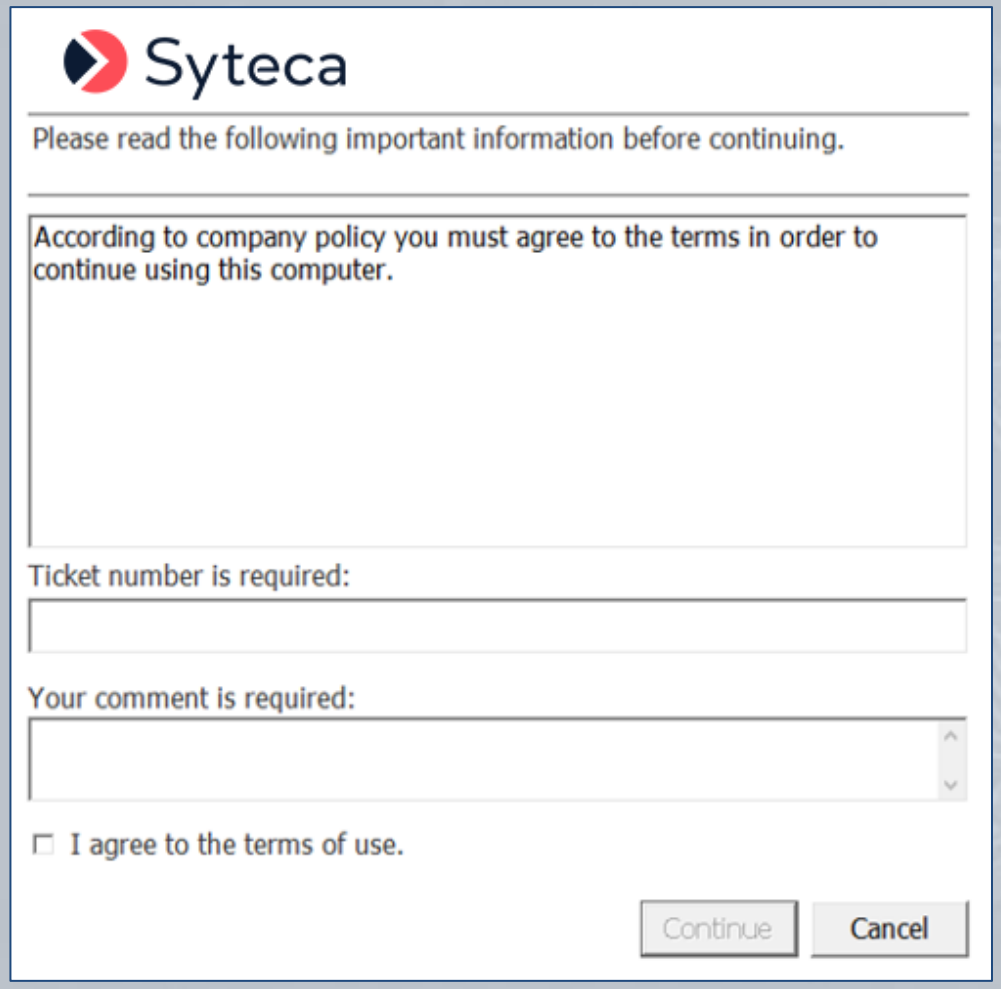


# Notifying Users about Being Monitored

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

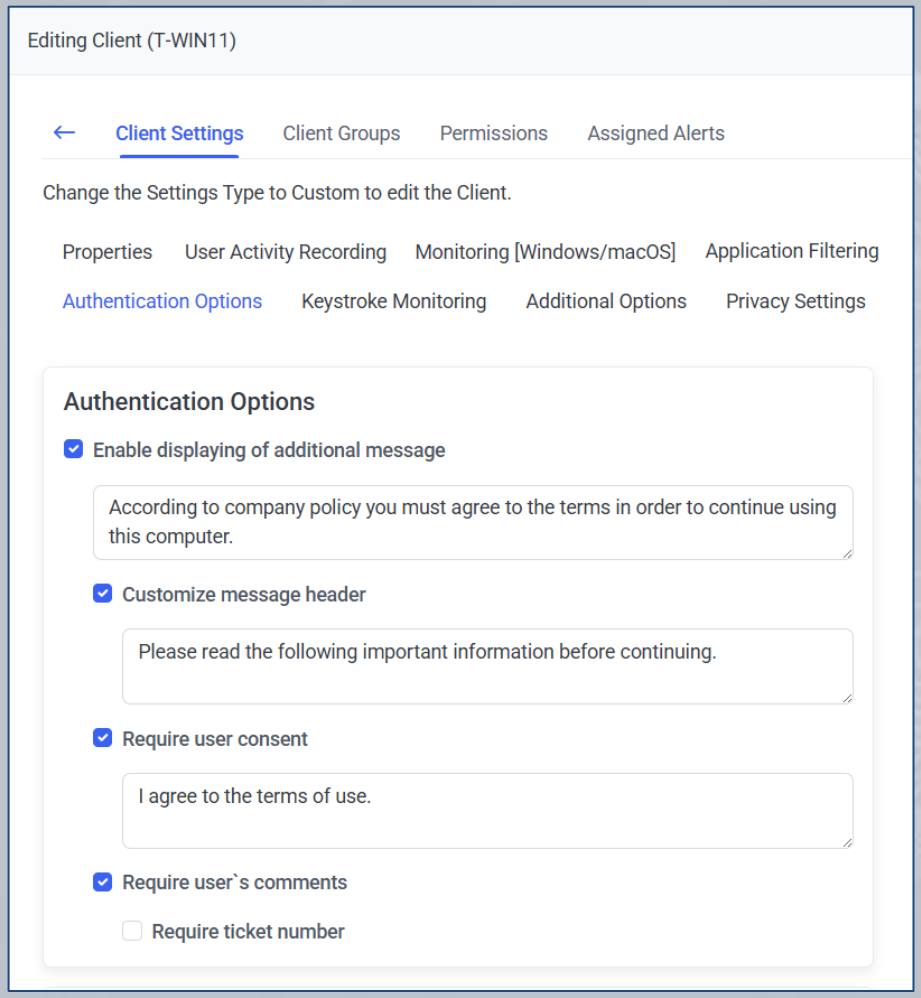
- **Enter** a valid **ticket number**, created in an **integrated ticketing system**.
- **Explain** their **reason for** needing **access**, in a comment.
- **Agree** to the **terms of use**.



# Notifying Users about Being Monitored

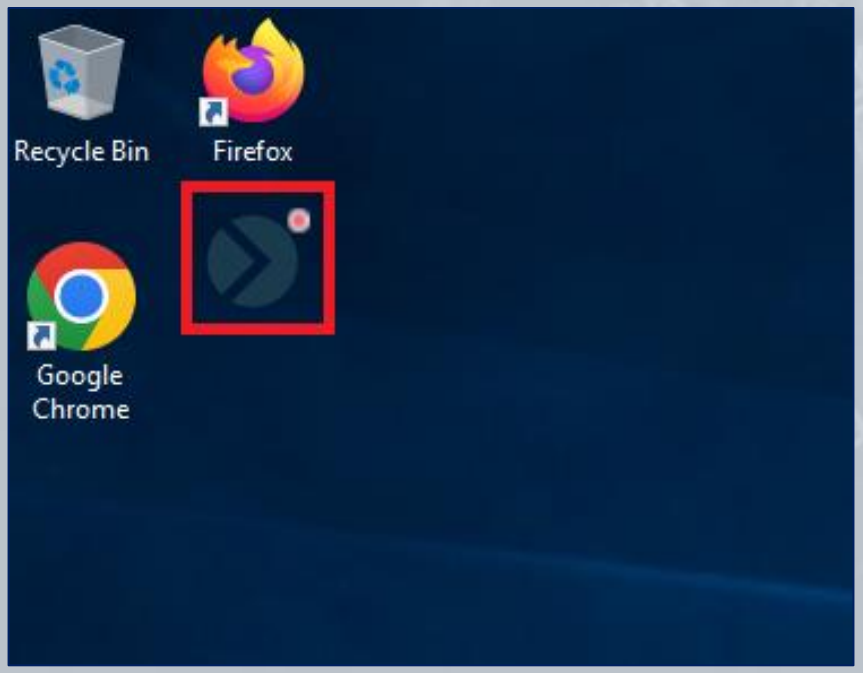
Syteca

When enabling the **options** to be displayed to users in the **additional message**, the message texts can be **customized** and **user consent** or **user's comment**, and **ticket number** can be **required**.



# 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**.



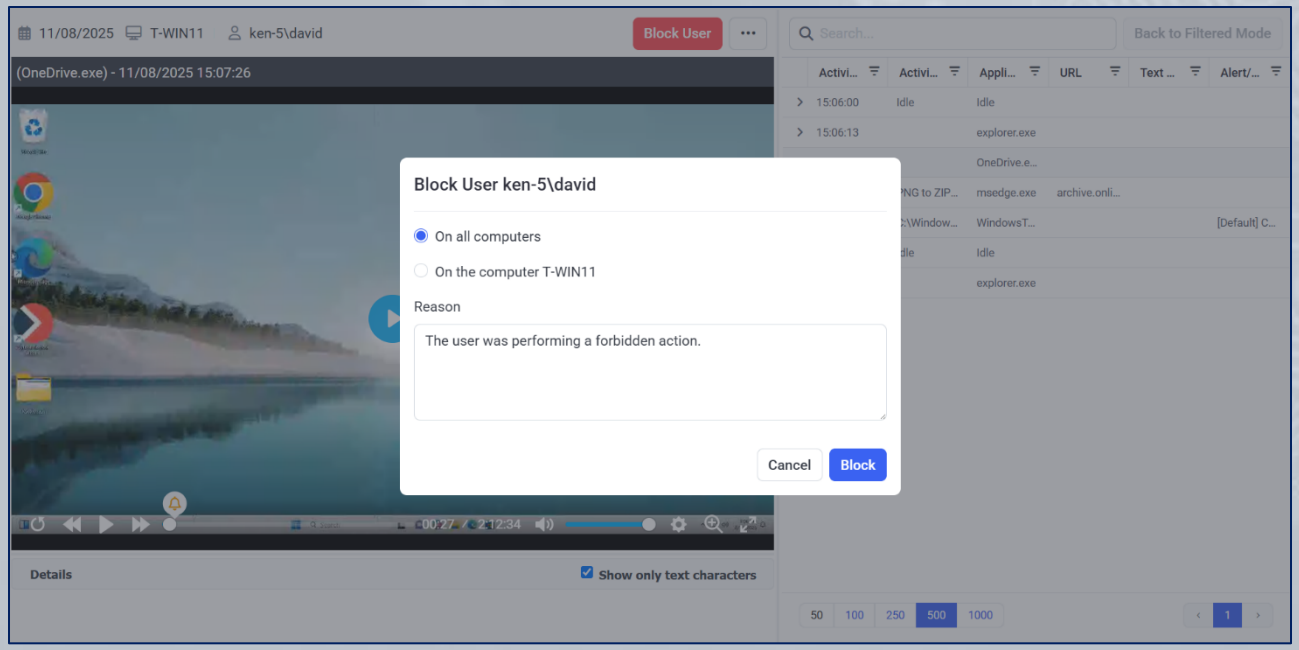
# Blocking Users

# Blocking Users Overview

Syteca

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

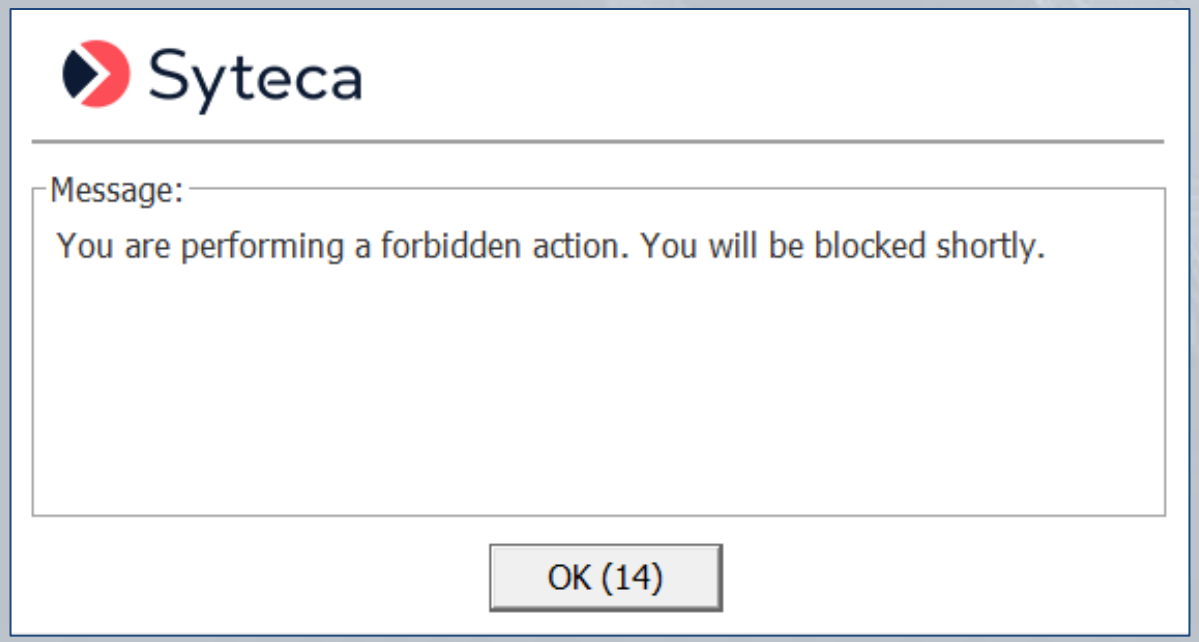
Users can be **blocked manually** from both **Live** and **Finished** sessions, or **automatically** when they perform an action that **triggers a specific alert**.



# 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.

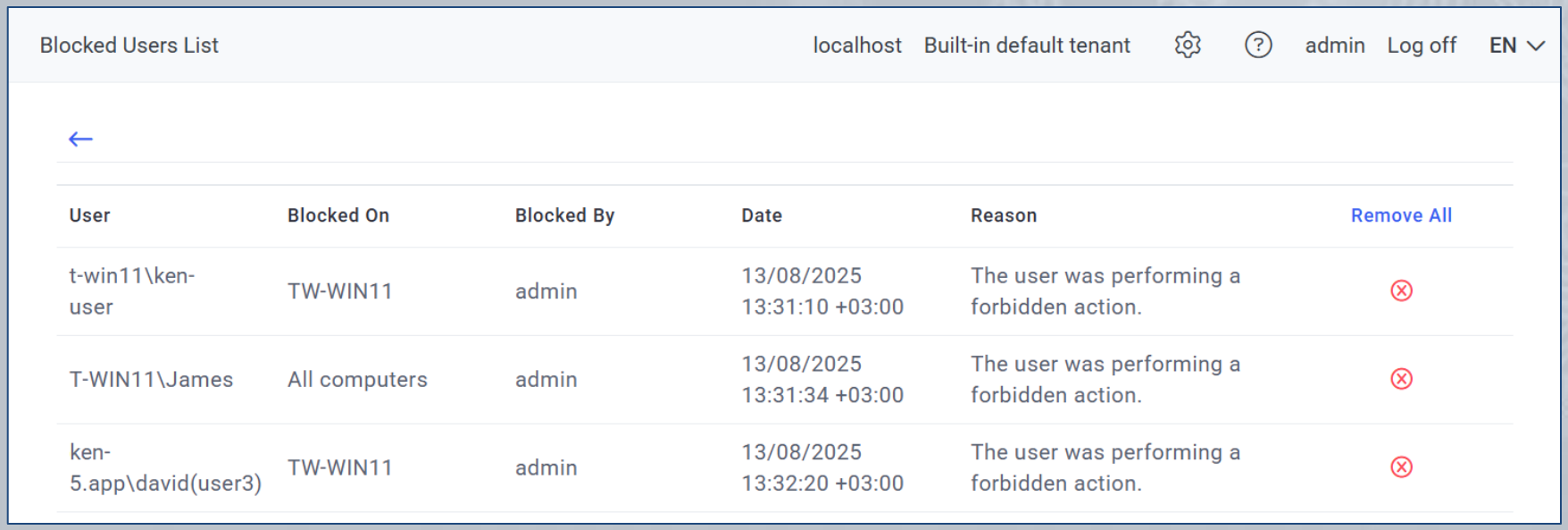


# Viewing the Blocked Users List

Syteca

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

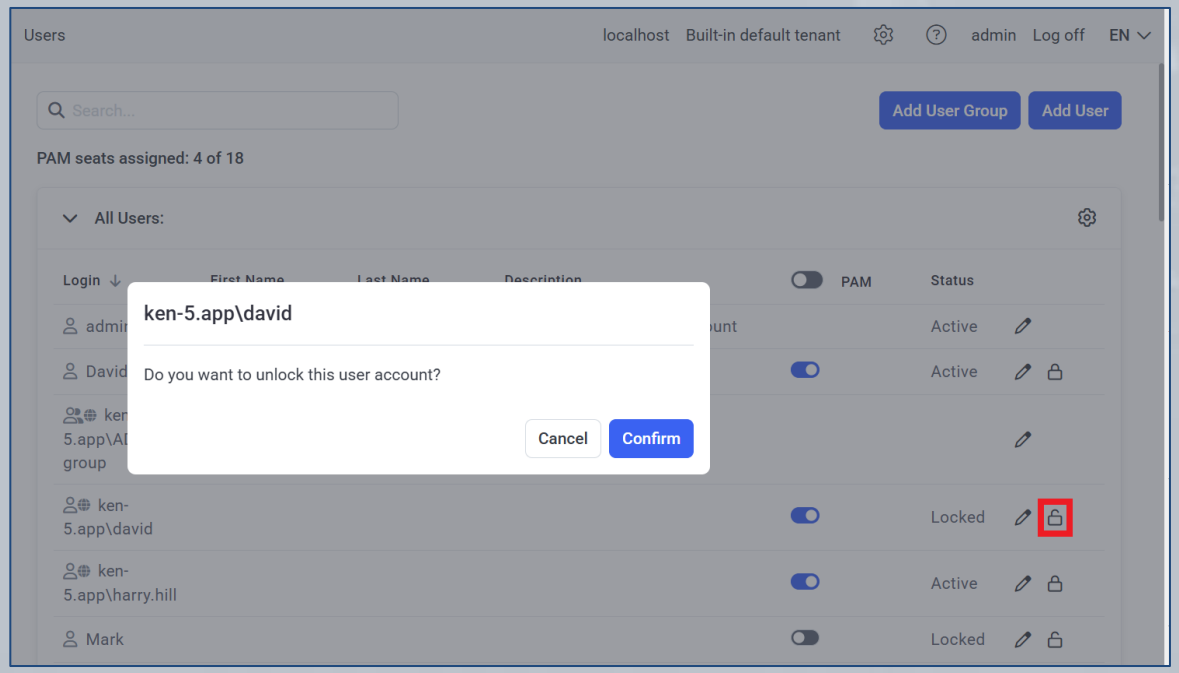
To **allow** users to **access** Client computers again, simply remove them from the list.

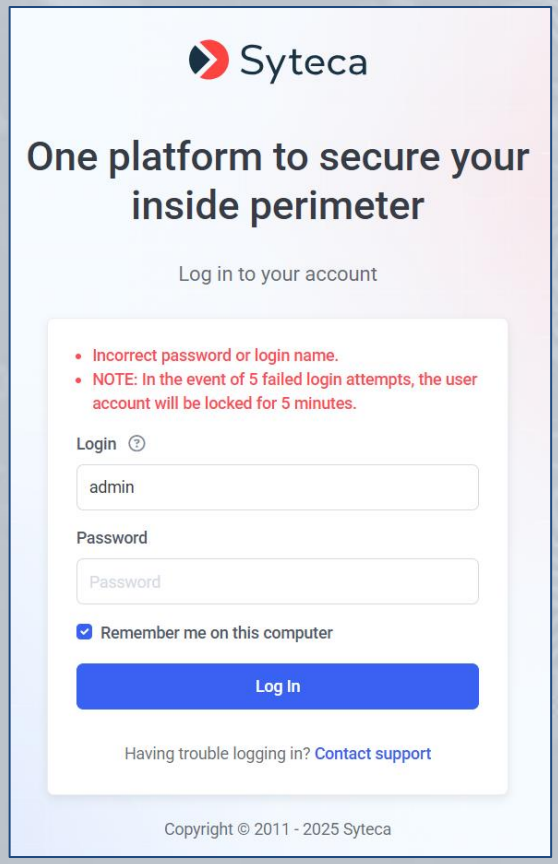


# Locking Management Tool User Accounts

The accounts of Syteca **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**.



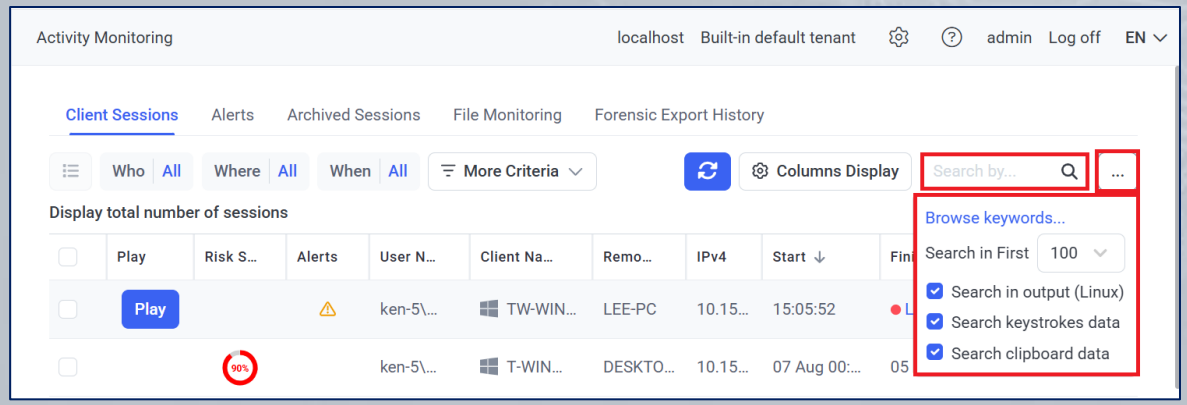



# Viewing Client Sessions

# Searching the Data in the Client Sessions List

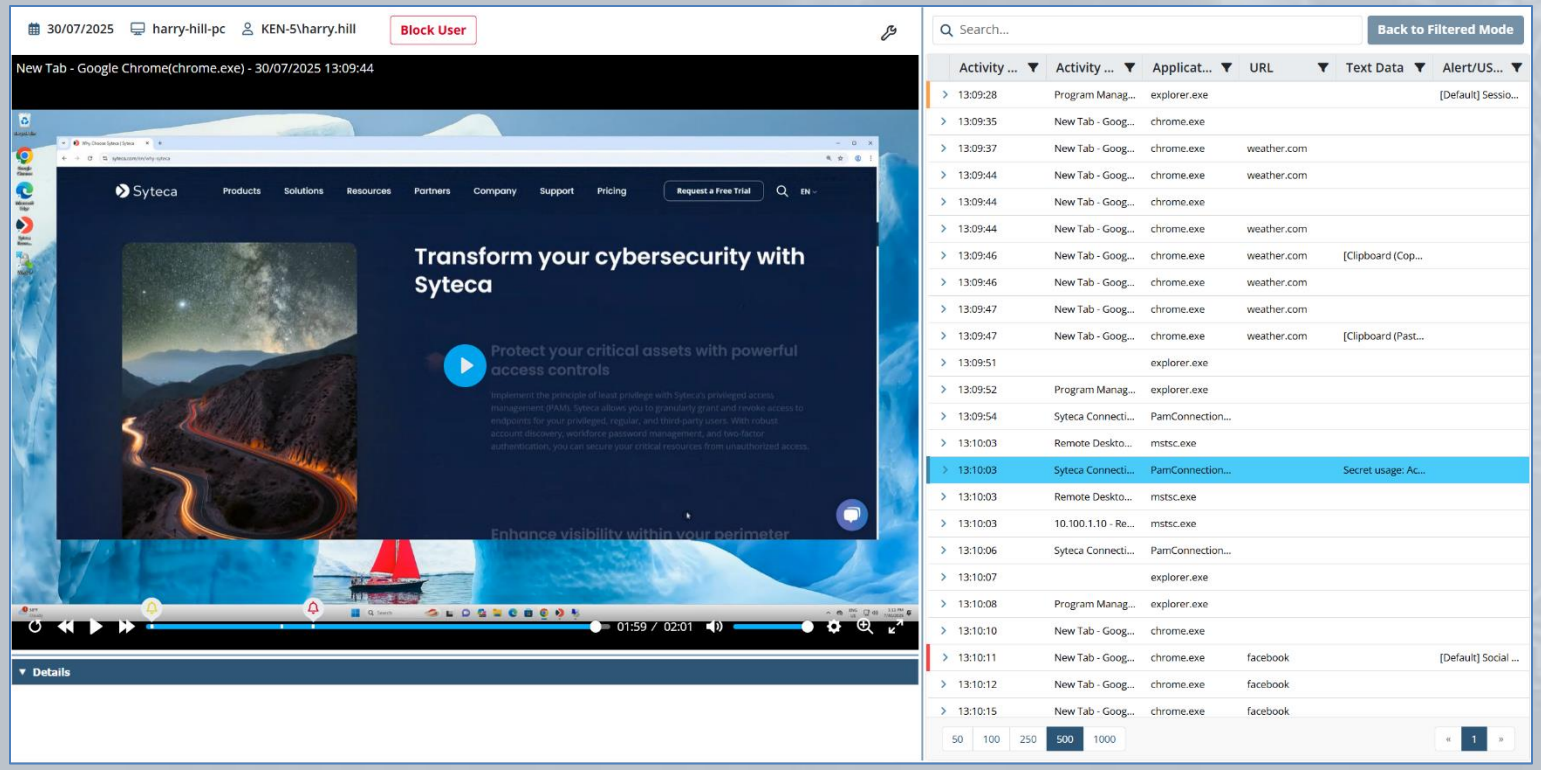
The Syteca Management Tool allows searching within the monitored sessions that are recorded by various parameters:

- **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 / video and metadata** recorded in the session, and can be **played back** with **alerts highlighted and color-coded**.

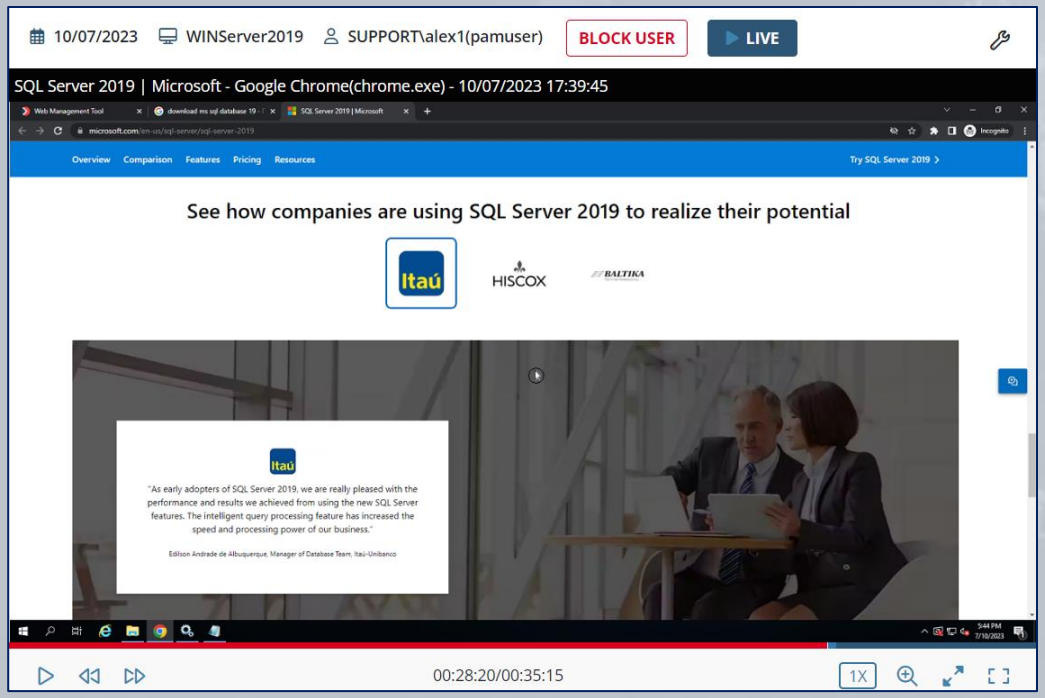


# Viewing Live Sessions

Syteca

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

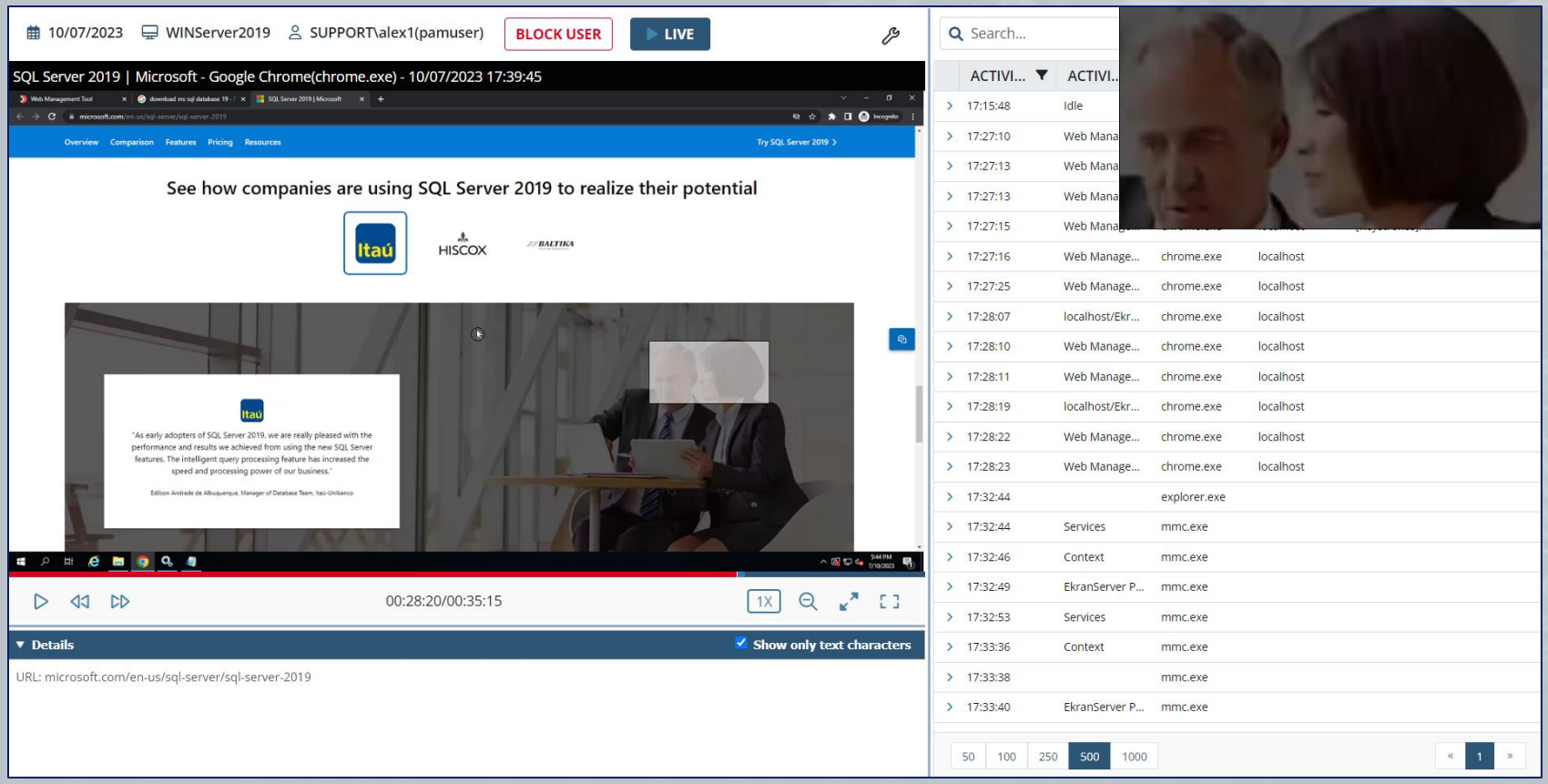
You can connect to a **Live** session and observe the activities a user is performing at any given moment (and **block the user** if required).



# The Magnifying Glass

Syteca

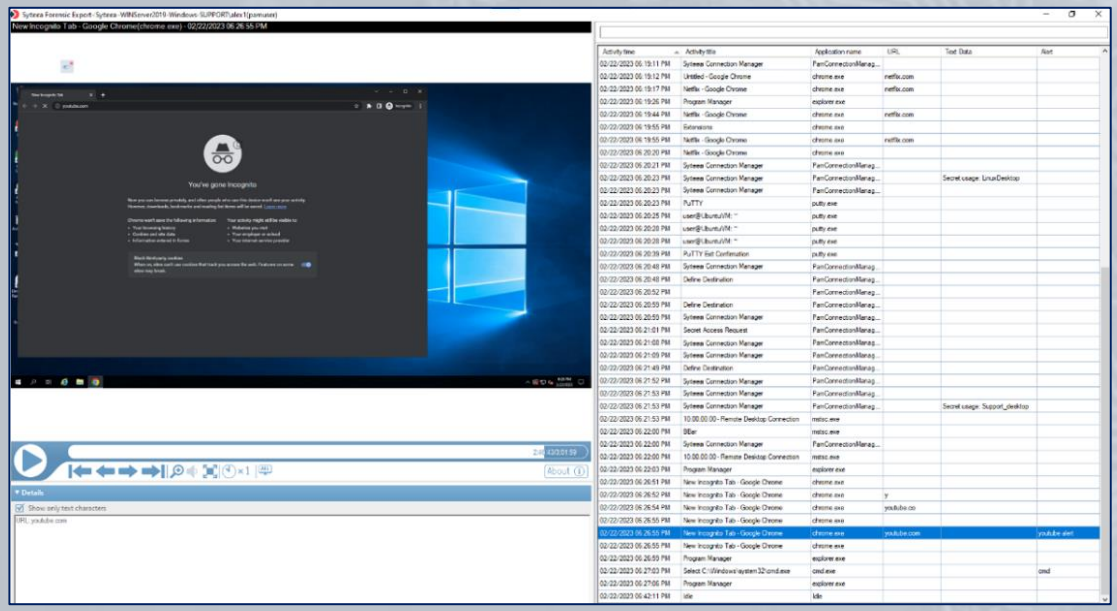
You can also enlarge any area of the video in the Session Player pane by using the **Magnifying Glass**.



# Forensic Export

With Syteca **Forensic Export**, you can:

- **Export** selected **monitored sessions** (or all or part of one) to a securely **encrypted** file, and **verify its integrity** (and to **MP4** format for **video**).
- **Investigate** the user activity **data recorded** by using the offline Syteca Forensic Player.
- Present **evidence** in a **forensic format** to third parties.



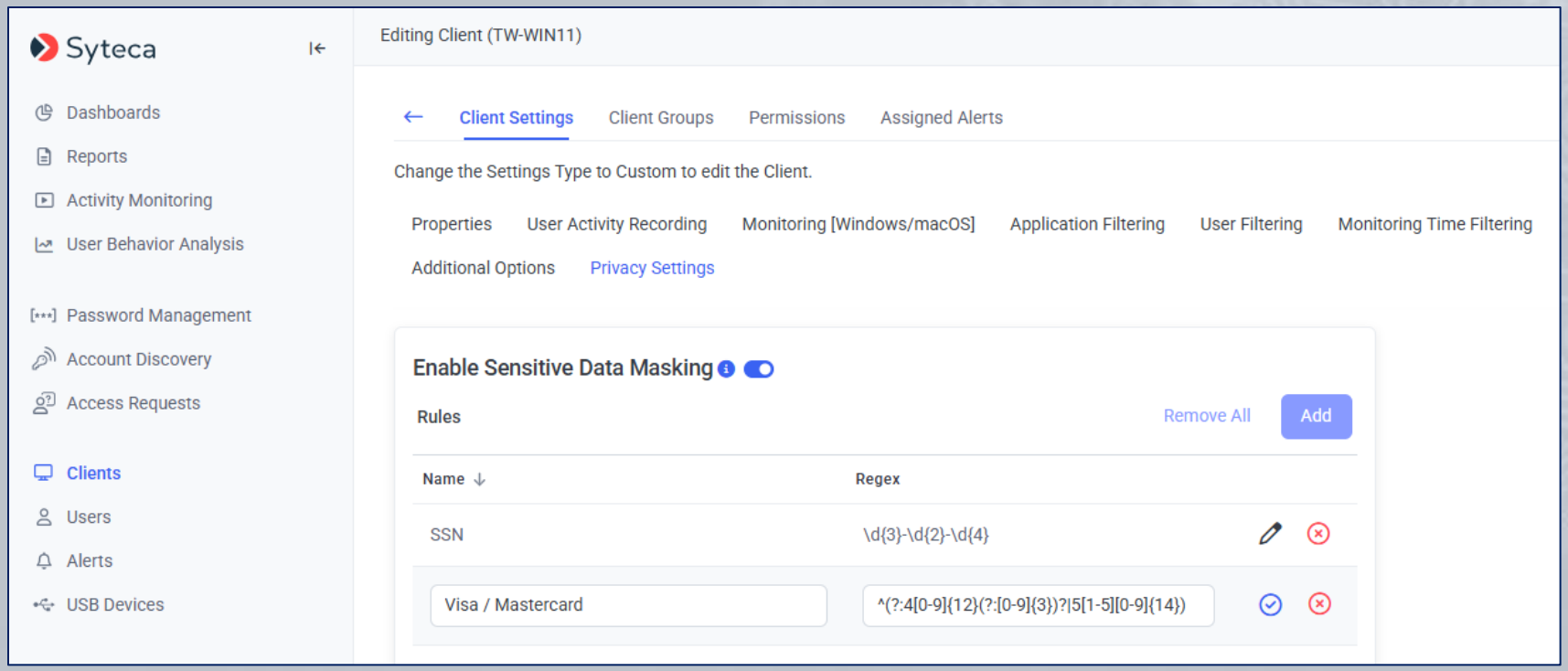
# Sensitive Data Masking

(for GDPR, PCI DSS, HIPAA compliance, etc.)

# Sensitive Data Masking

Syteca

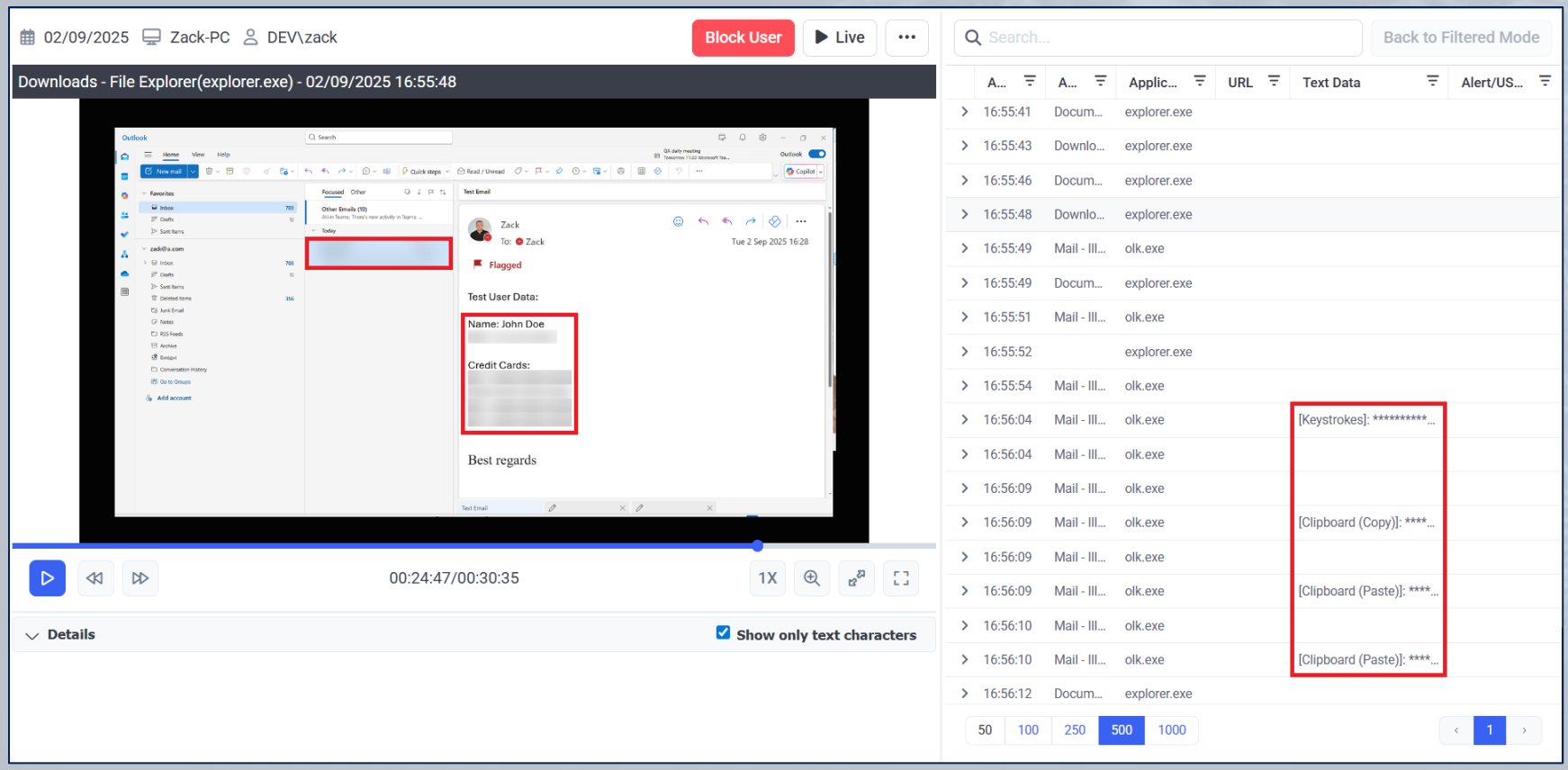
The **Sensitive Data Masking** feature allows custom **regex** values to be defined **to detect** sensitive **clear text data** (e.g. **passwords**, **SSNs, credit card numbers**, etc.) on Windows Client computers, including in **keystrokes** typed and **clipboard** operations performed by users.



# Sensitive Data Masking

Syteca

The sensitive data detected is **masked in real-time** when **played back** in the **Sessions Viewer**, as well as **encrypted** in the database.



# Pseudonymizer

(for GDPR compliance, etc.)

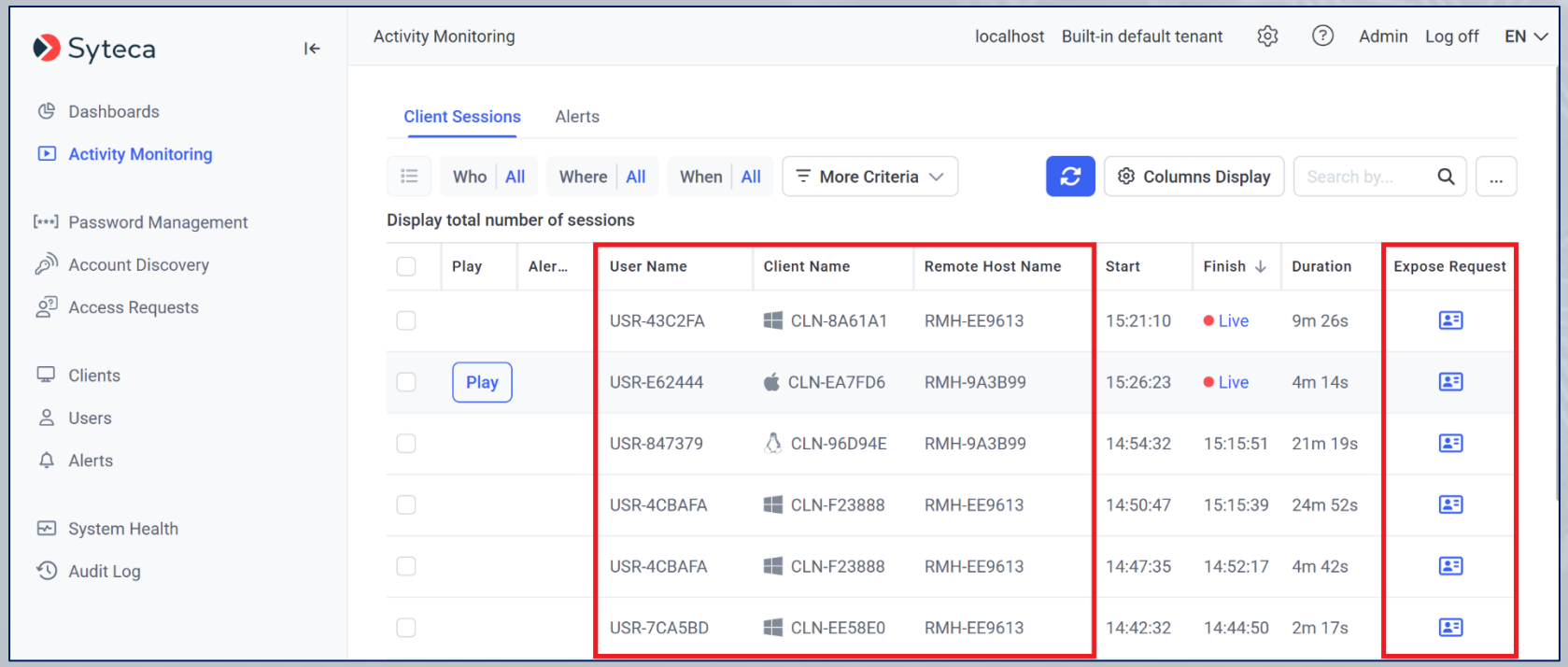
# Pseudonymizer

**Pseudonymizer** (also known as **Monitored Data Pseudonymization**) 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 **personally identifiable information (PPI)** of endpoint users, that is recorded during monitoring of their activities by Syteca, is achieved by the system **pseudonymizing** this data (i.e. hiding and replacing it with **randomized values** when viewed).

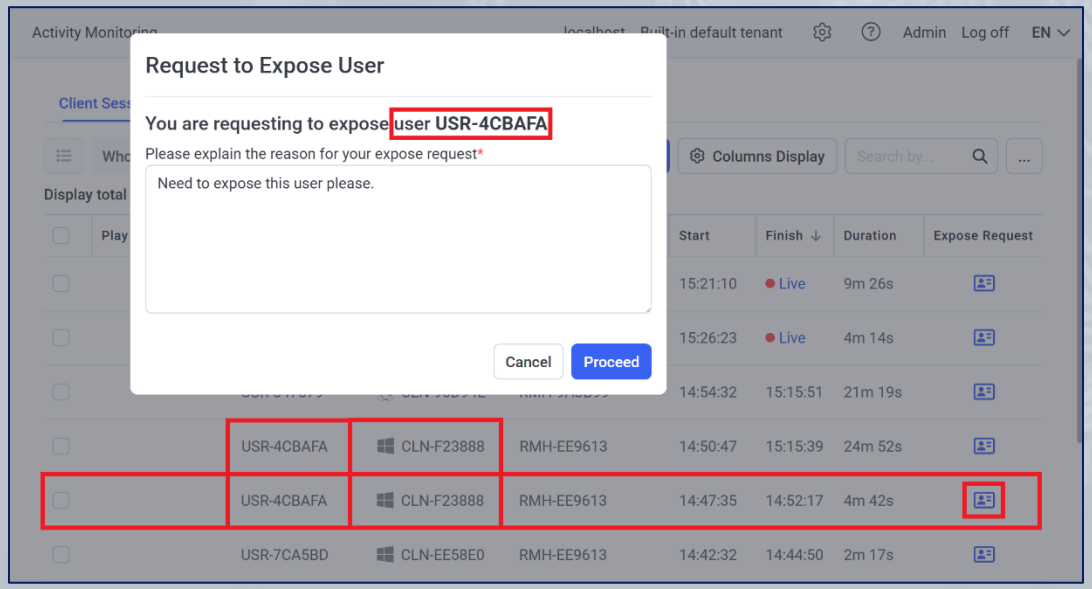


# Requesting De-Anonymization of PPI Data

Syteca

In **Pseudonymized 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 an **Expose 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).

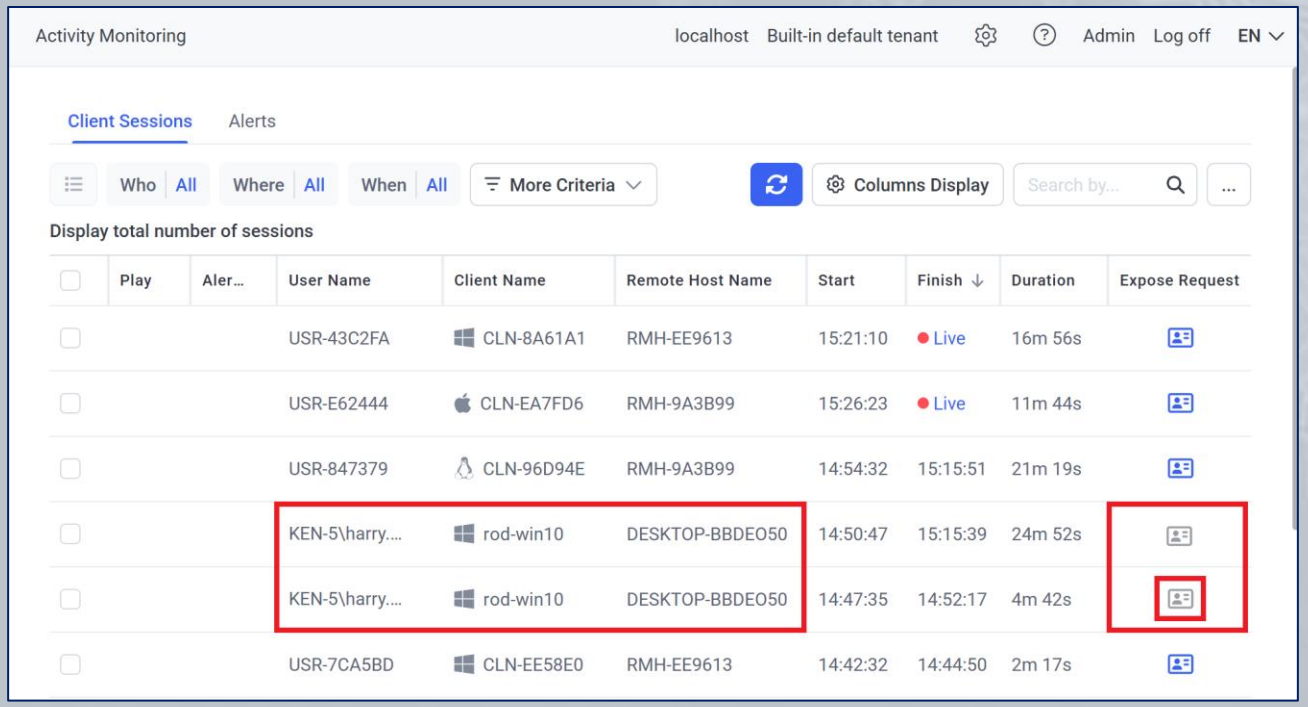
At the same time, **supervisors** do **<u>not</u> have permission** to open and **view the sessions** of endpoint users.



# Temporarily De-Anonymizing PII Data

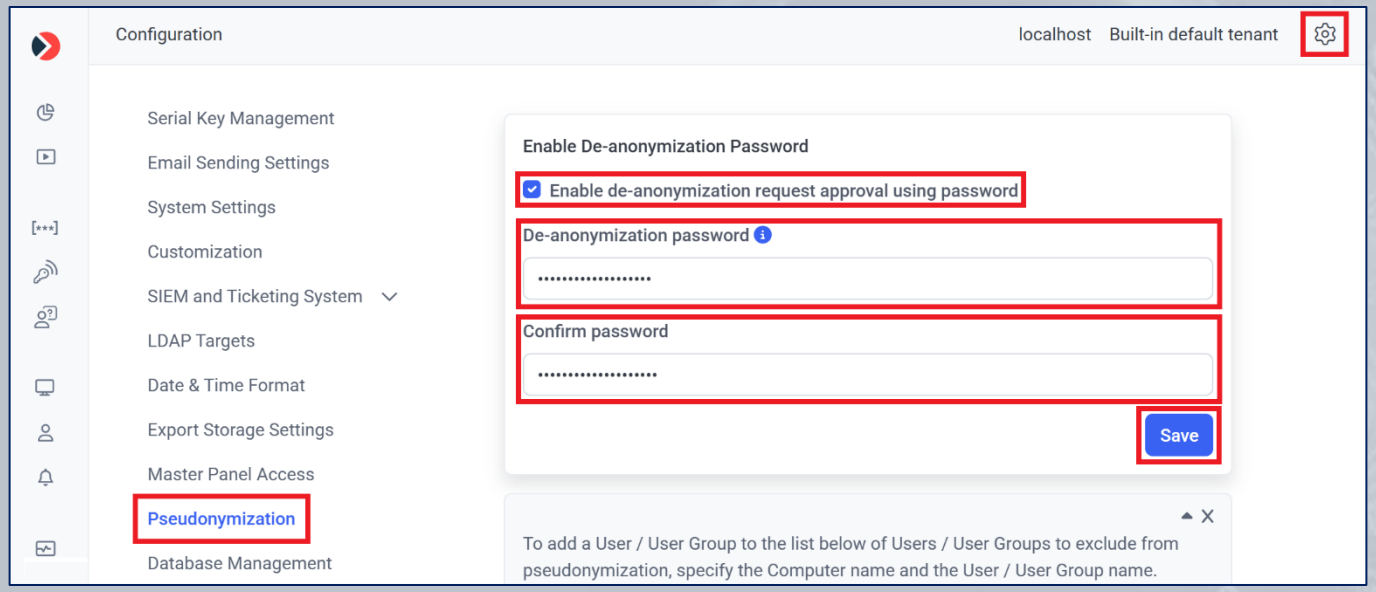
Syteca

If an **investigator's Expose 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 de-anonymized** for **that investigator to view**.



# De-Anonymization Password

A **de-anonymization password** can also **be required** for Supervisor users **to approve Expose requests**, in order to e.g. improve security (or comply with corporate policies and contracts).

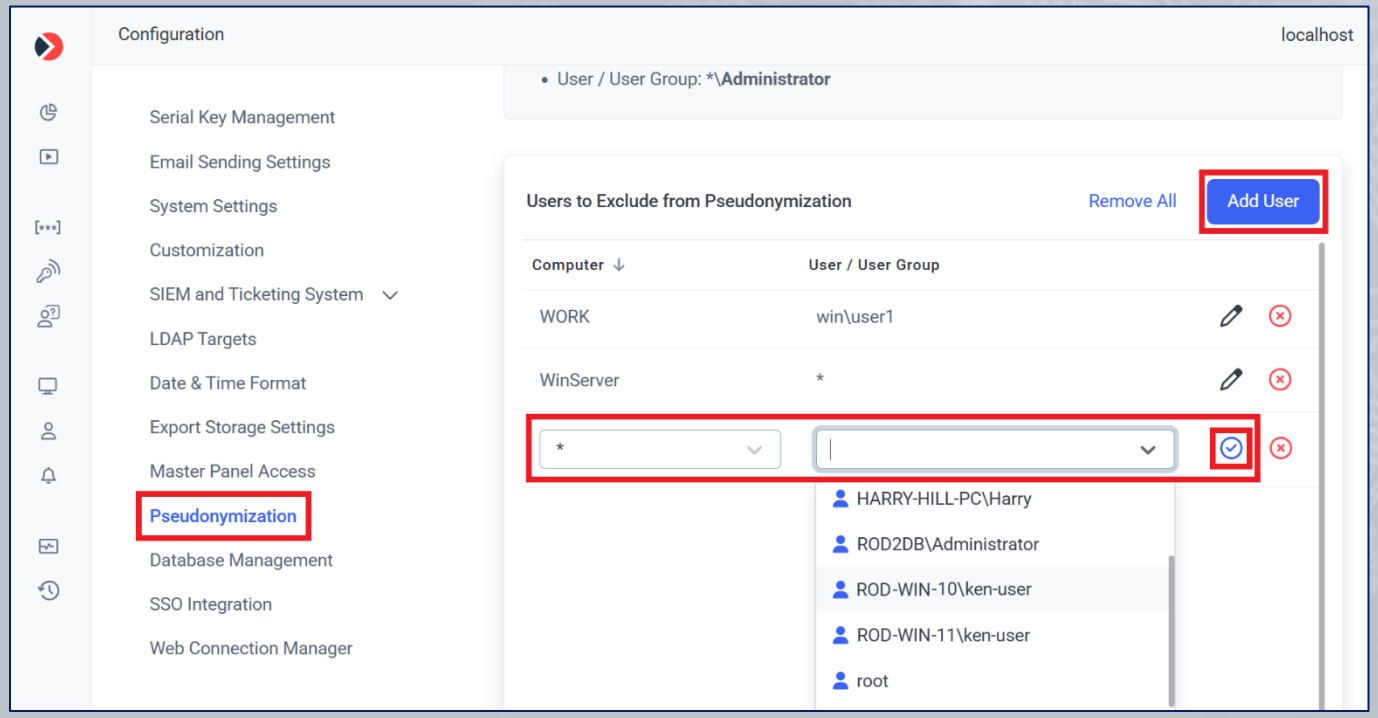



**Only** the built-in default "**admin**" user of Syteca can **set** (**or change**) the **de-anonymization password**.

# Excluding User from Pseudonymization

Syteca

Any Management Tool users in the default "**Supervisors**" group **can add specific endpoint users** to the **"Users to Exclude from Pseudonymization" list**, so that all **Supervisors** can view the de-anonymized data of these endpoint users.



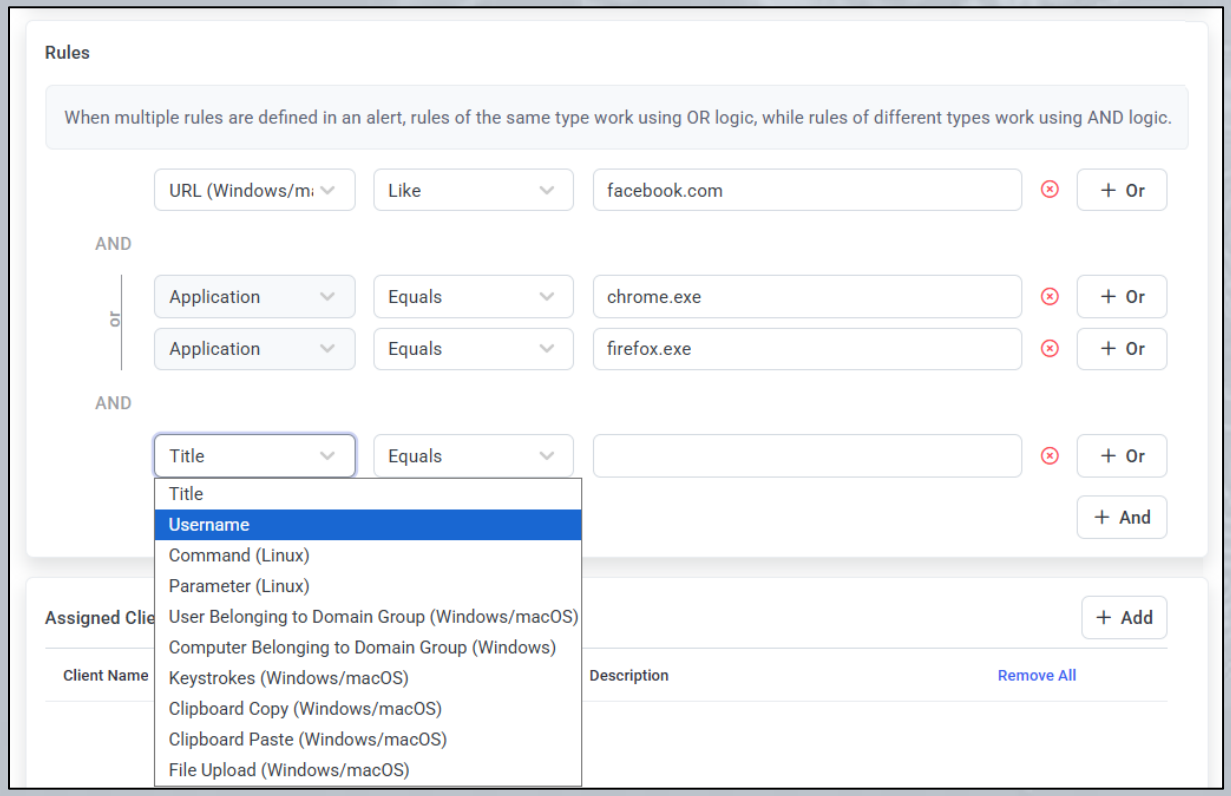
# Alerts

# Adding Alerts

Syteca

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

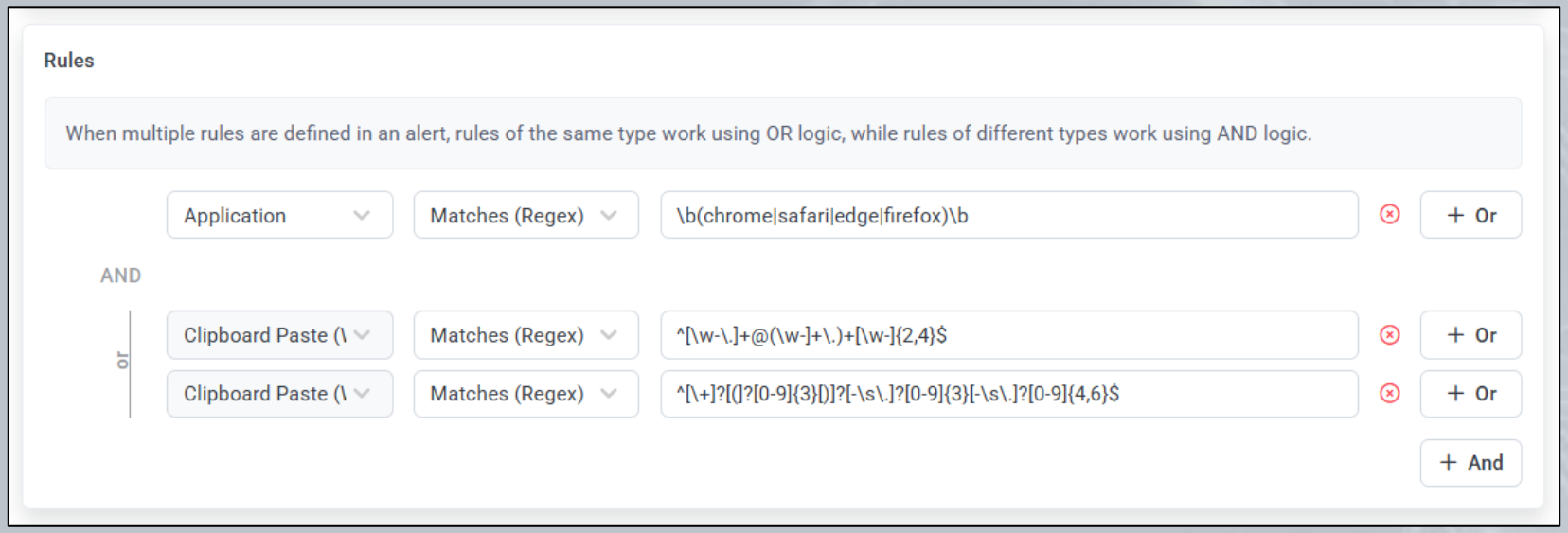
- **Add alert rules** to detect specific suspicious user activity on Client computers.
- Specify individuals to receive instant **alert notifications** via **email** and **tray** notifications.



# Using Regular Expressions (regex)

Syteca

Regular expressions (also known as **regex** or **regexp**) based on ECMAScript language grammar can be used to allow **more flexibility** when **defining alert rules** for Windows and Linux Client computers.



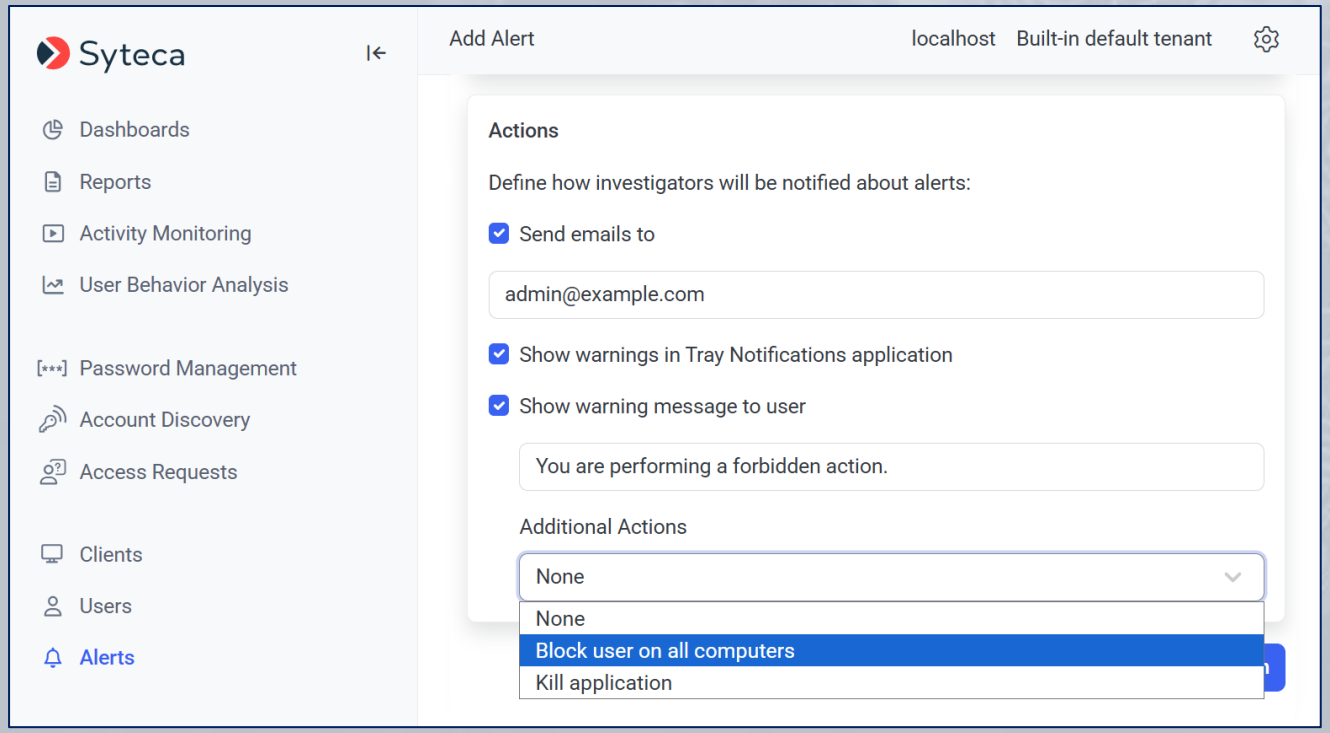

e.g. the **combination of alert rules** shown above triggers the alert if an **email address** or **phone number** is pasted into any of 4 browsers (which may indicate **sensitive data** being **pasted into an email** being composed).

# Alert Actions

Syteca

You can also set an alert to:

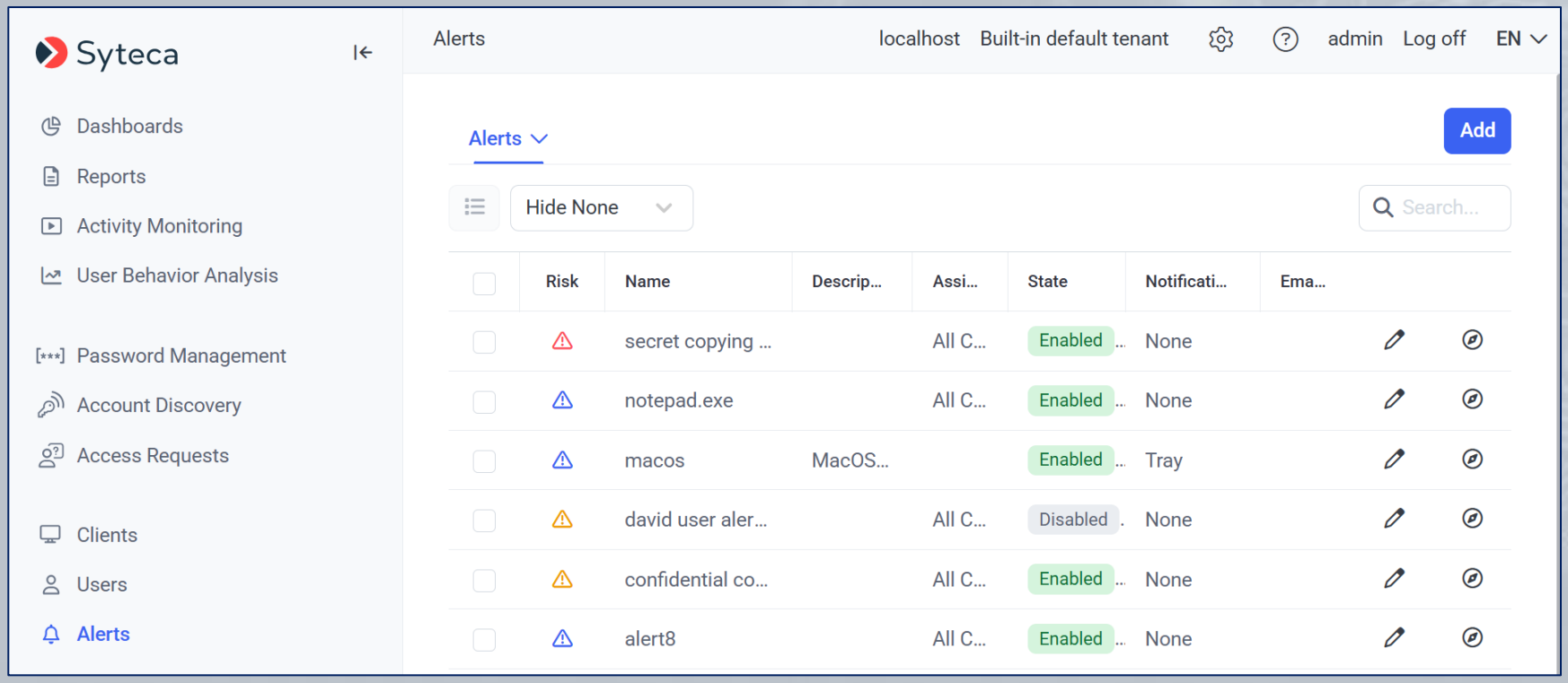
- Display a **warning message** to the **user** when the alert is triggered (the message can be edited).
- **Block** the **user**.
- Forcibly **stop the application**.



# Default Alerts

Syteca

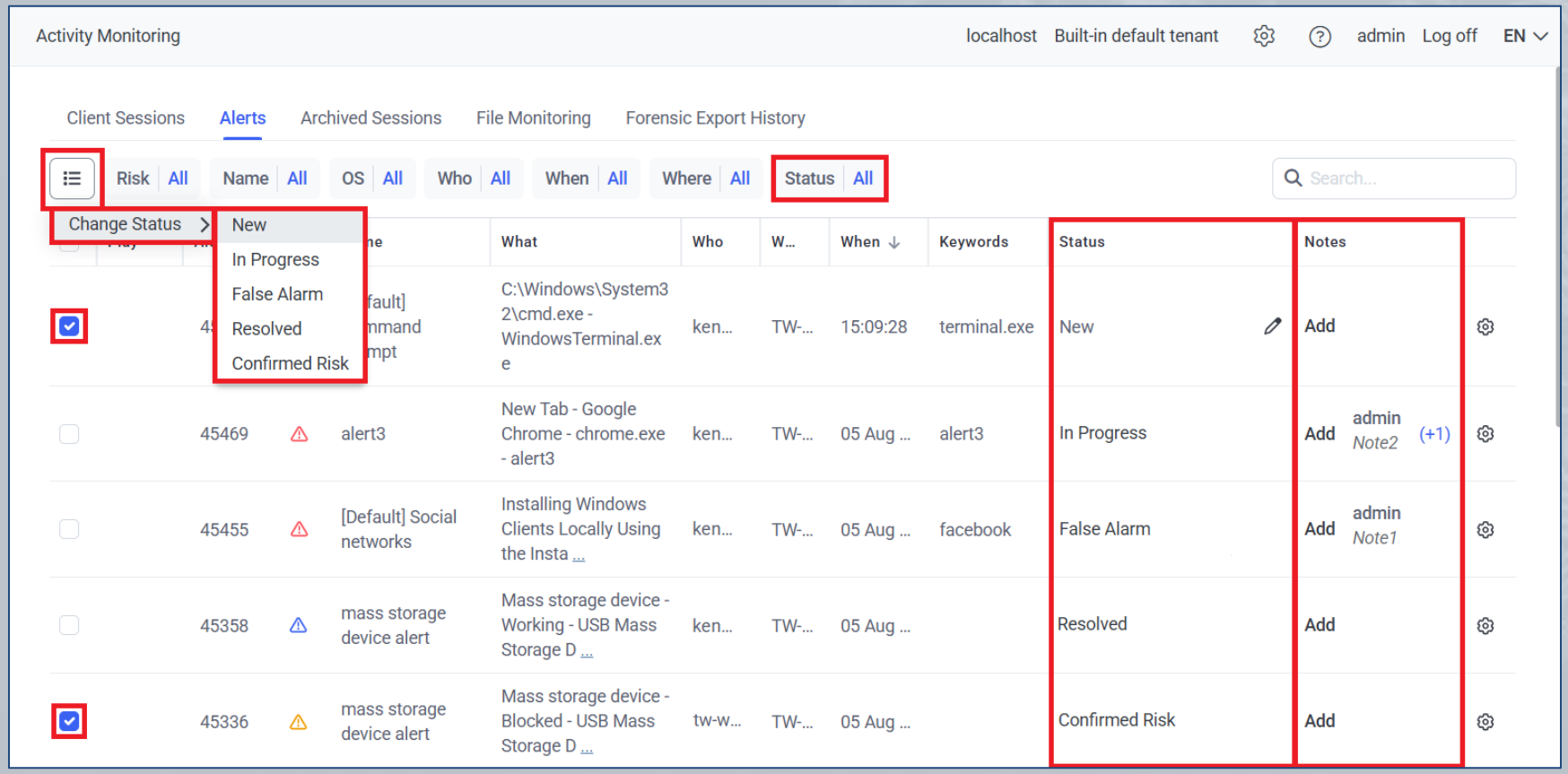
Syteca contains a set of default alerts prepared by the vendor's security experts. They will inform you about **data leakage** or potentially **fraudulent**, **illicit**, or **non-work-related** activities.



# Viewing Alert Events

Syteca

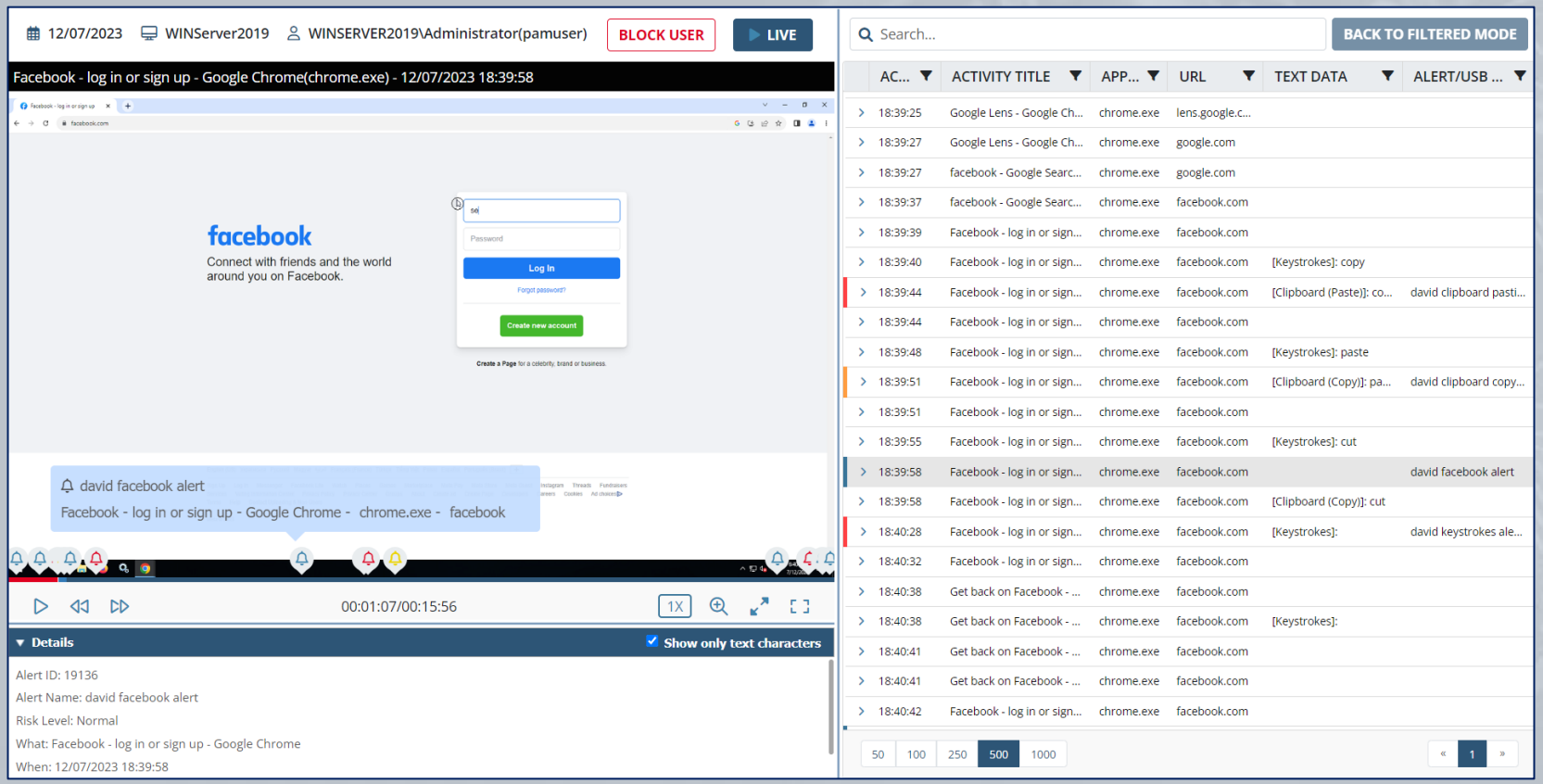
The list of alerts triggered can be **viewed and managed** on the **Alerts tab**, where the **Status can be changed** and **Notes added**.



# Viewing Alert Events in the Session Viewer

Syteca

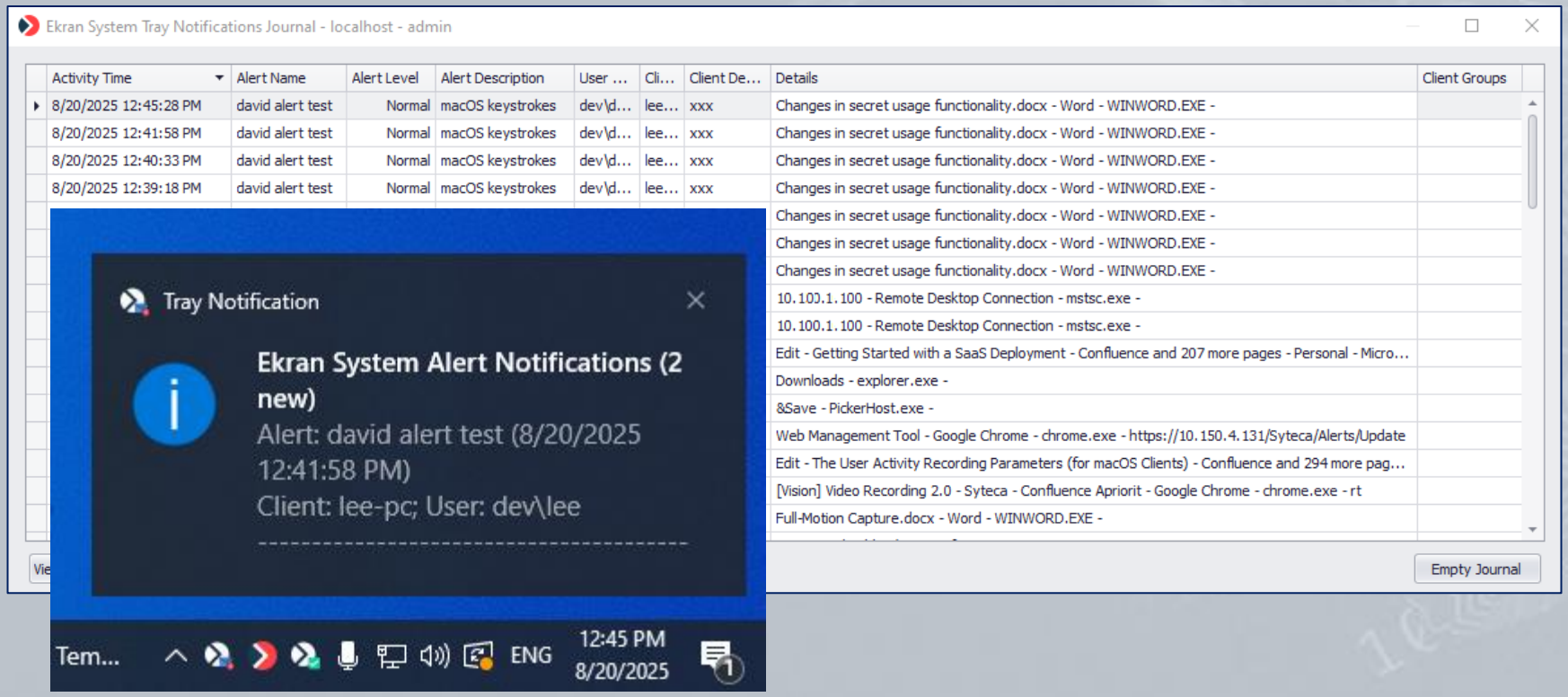
Monitored data associated with alert events is **highlighted** in the Session Viewer (in different **colors** depending on the **alert risk level**).



# Receiving Alert Notifications

Syteca

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



# USB Device Monitoring

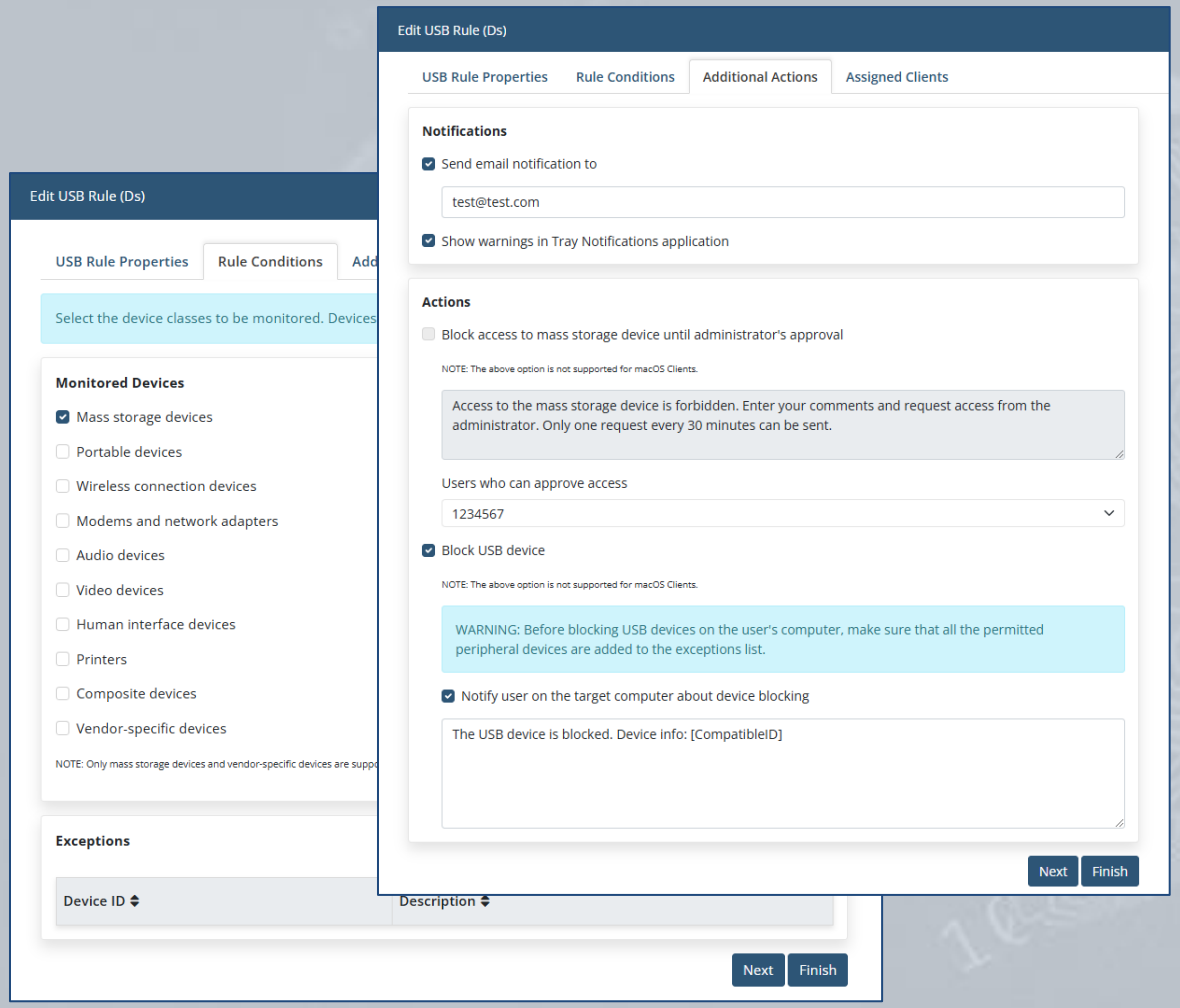
# USB Device Monitoring

Syteca 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

Syteca 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.

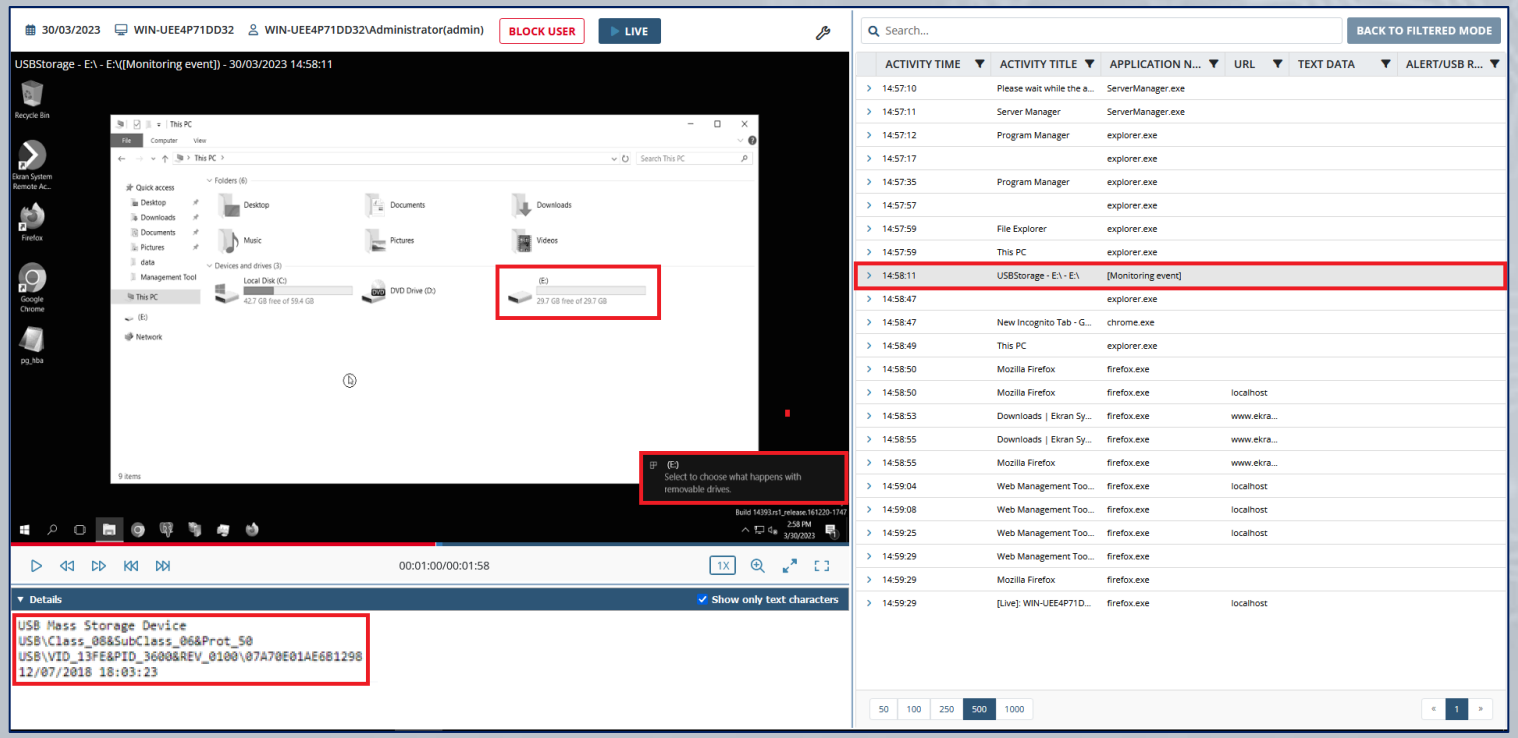


# Automatic USB Device Monitoring

Syteca

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.



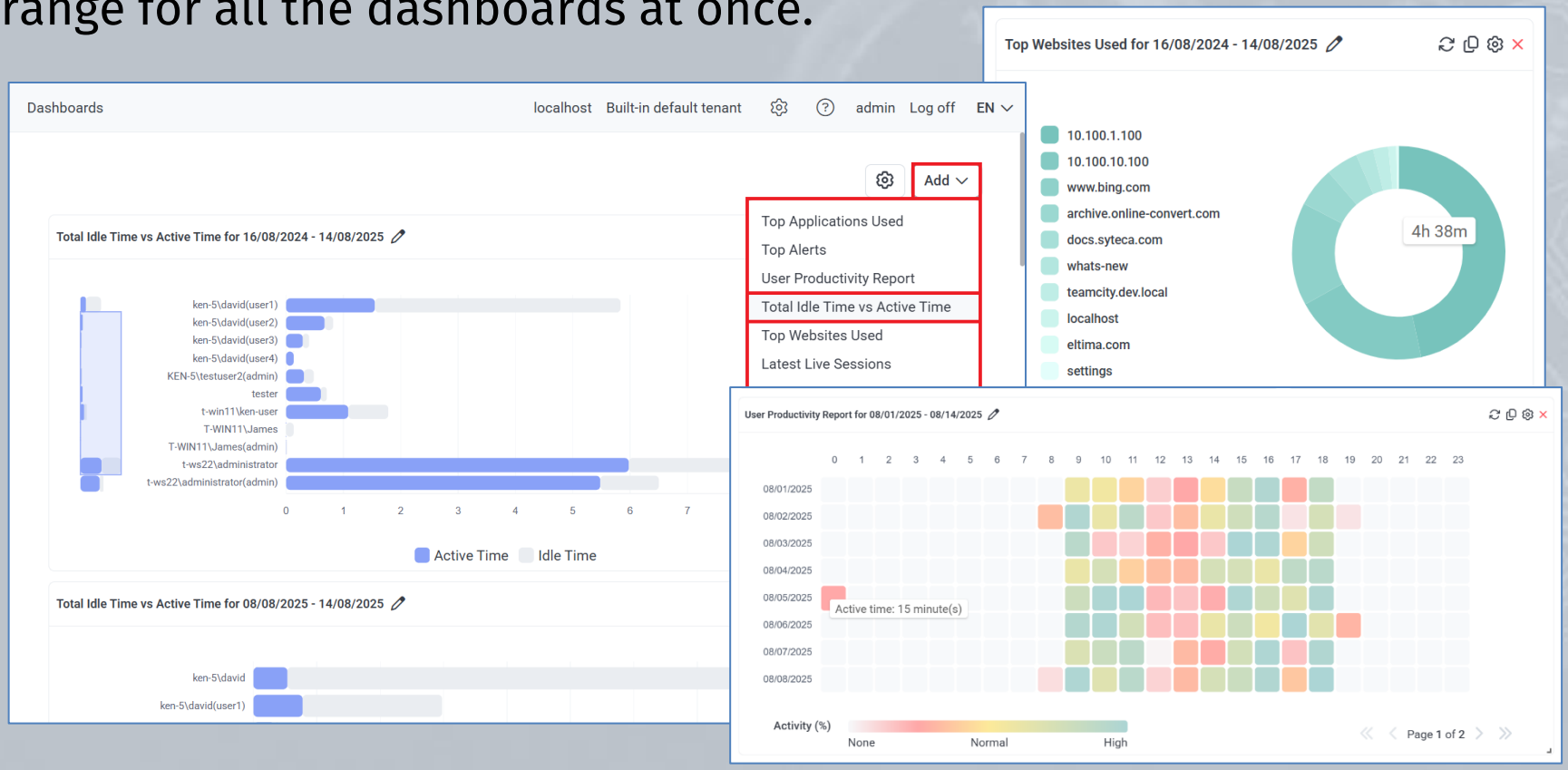
# Dashboards

(on the **Dashboards** and **System Health** pages)

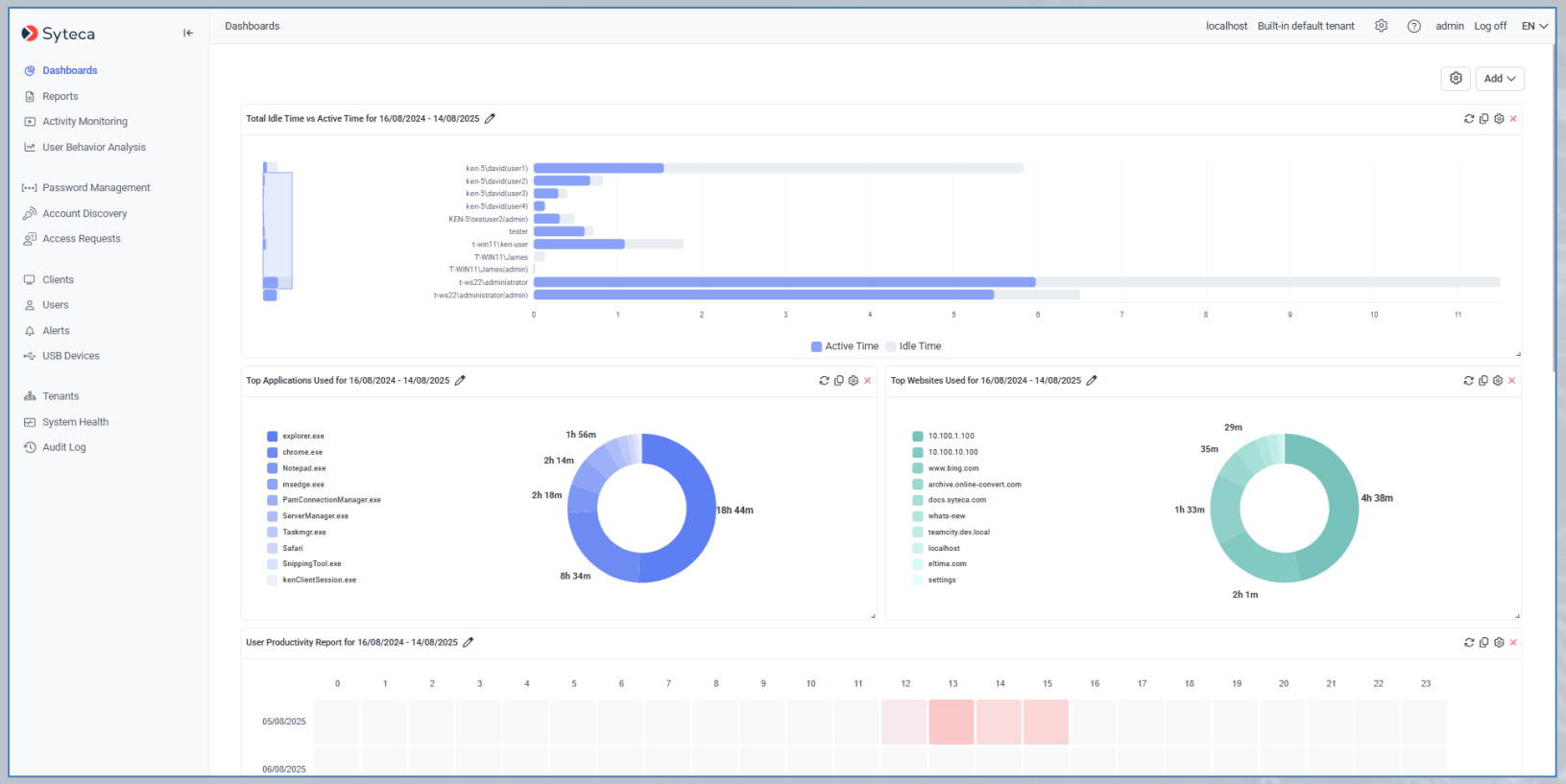
# Generating Dashboards

Syteca

Various types of **user productivity** and other dashboards can be generated (on the **Dashboards** page) by specifying a global data range for all the dashboards at once.



# Viewing Dashboards

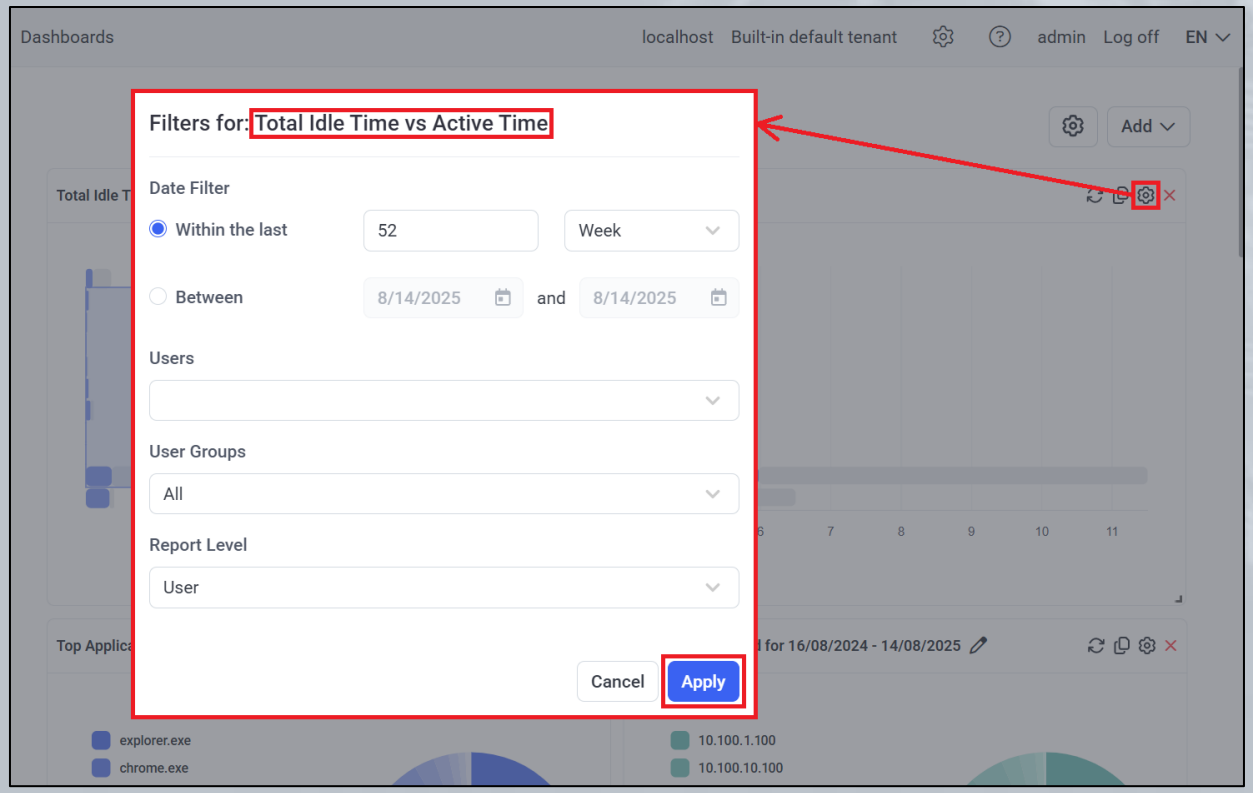



Some of these dashboards are **similar** to when **importing data** from Syteca **into Power BI** report templates by using **Syteca API Data Connector**, but are **much simpler to generate** and **customize**.

# Customizing Dashboards

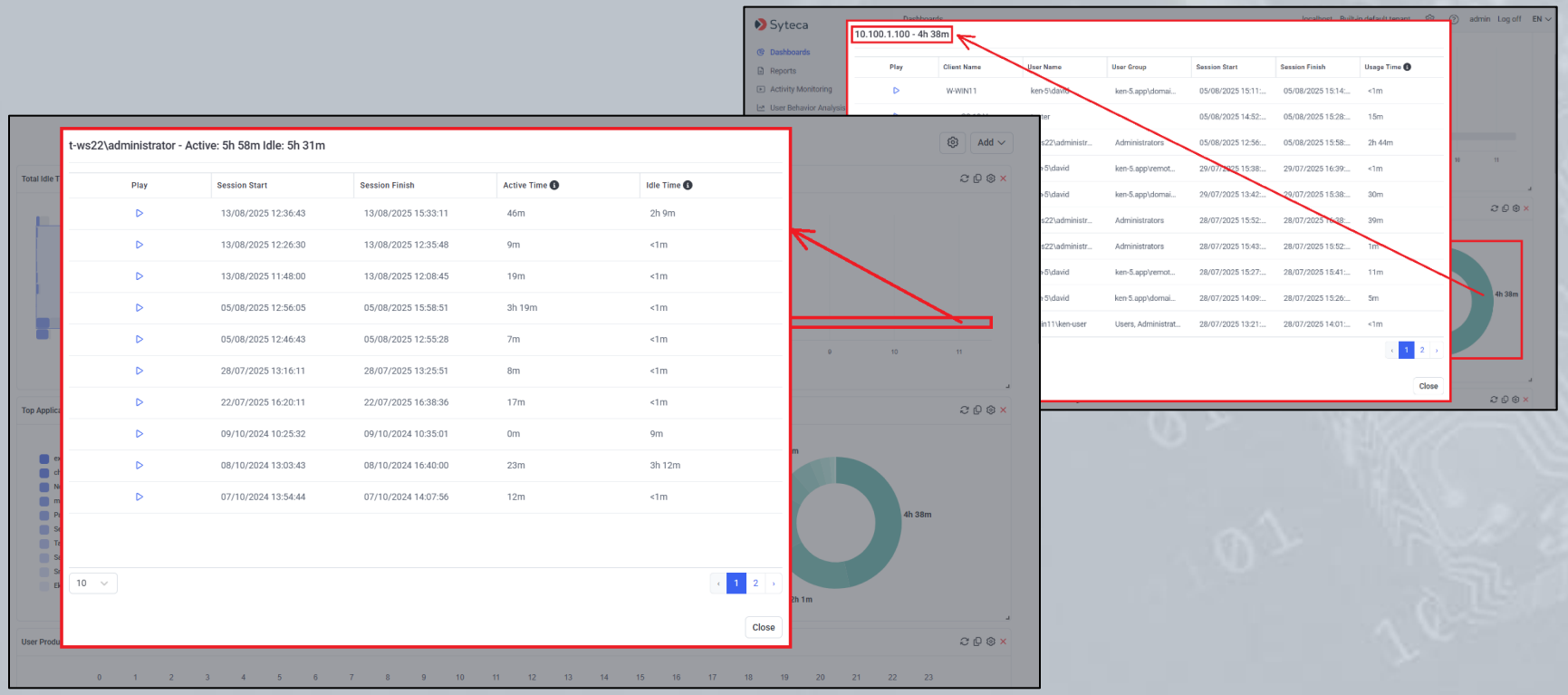
Syteca

**Each dashboard** can be **individually customized** to change the range of data specified in it (by using the different **Filter** options).



# Viewing Detailed Information

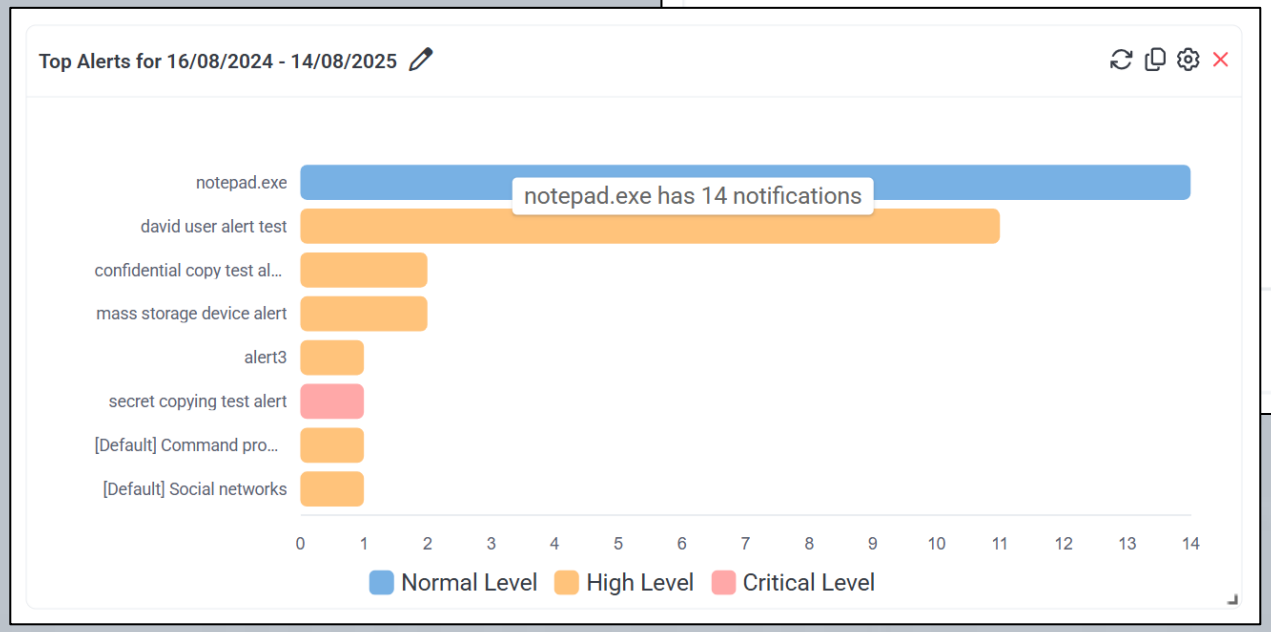
**Detailed information** about all the **sessions** that the data in the **charts contains** can then be viewed by **drilling down** (and the sessions can be **played** in the **Session Viewer**).

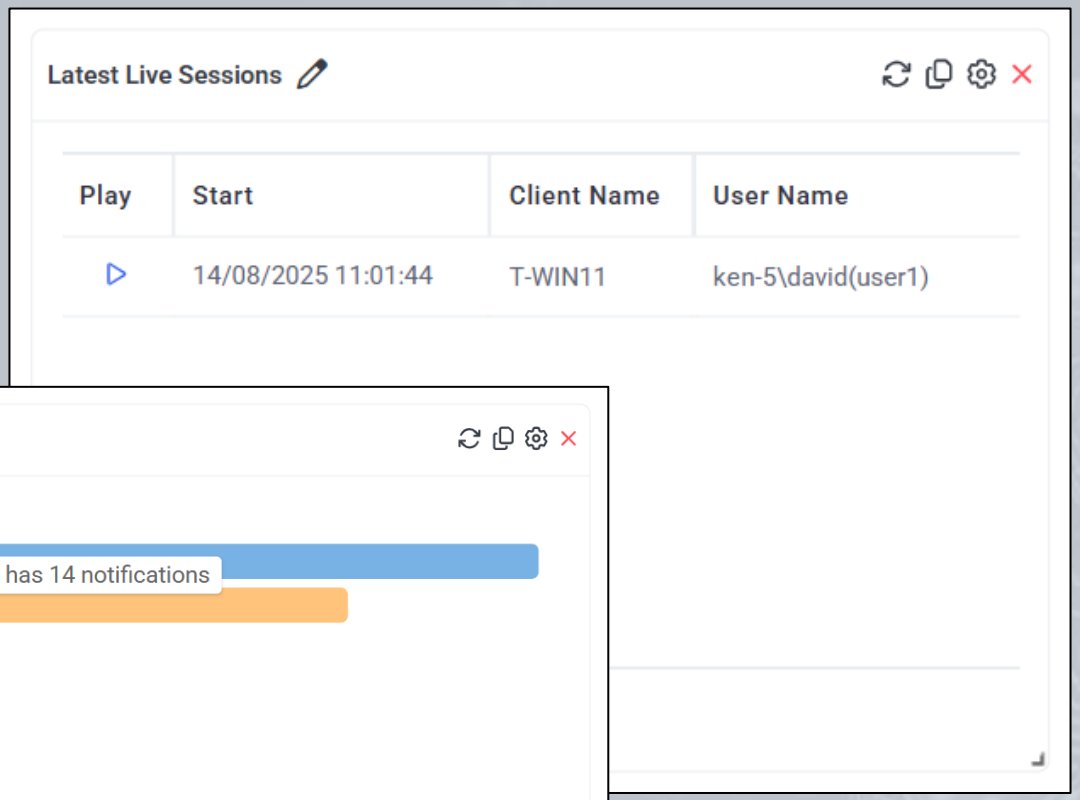


# Monitoring Dashboards

Syteca

## Top Alerts




## Latest Live Sessions

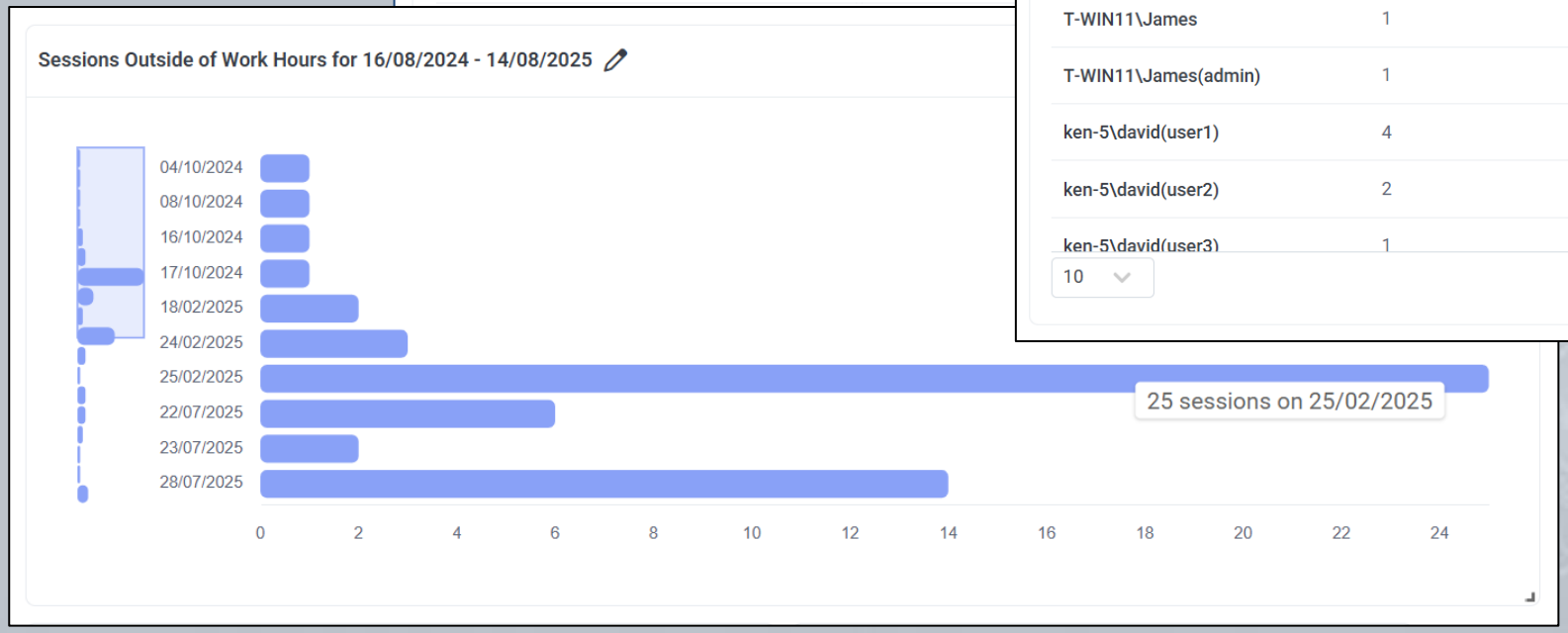
# Threat Detection Dashboards

Syteca

## Rarely Used Computers

## Rarely Used Logins

## Sessions Outside of Work Hours

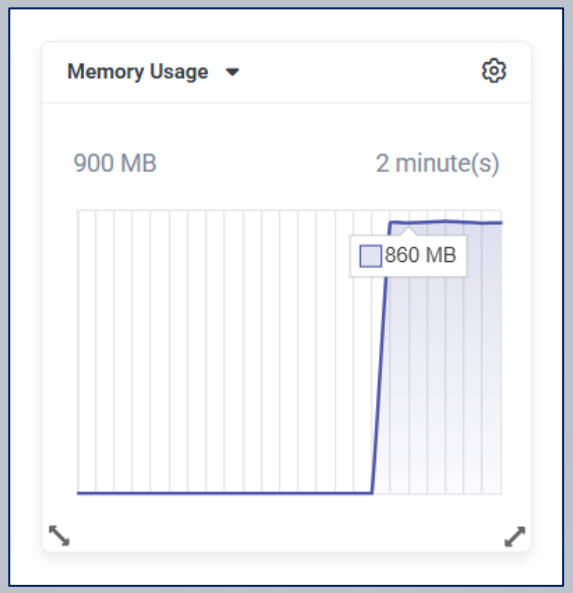


# Server Resource Monitoring Dashboards

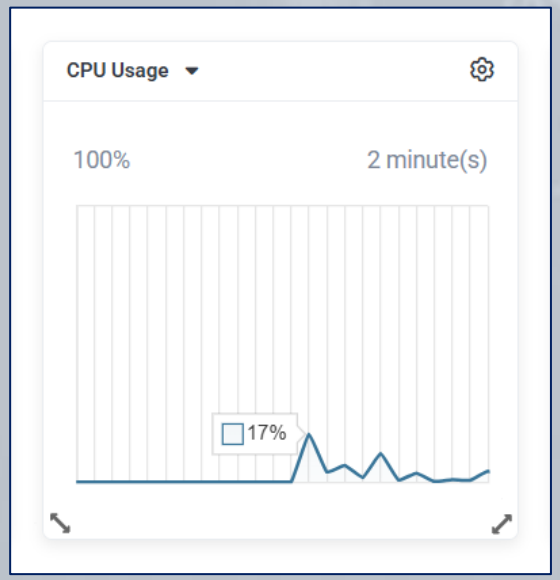
Syteca

Other dashboards (on the **System Health** page) provide real-time **resource monitoring** information about the Application Server computer and the database.

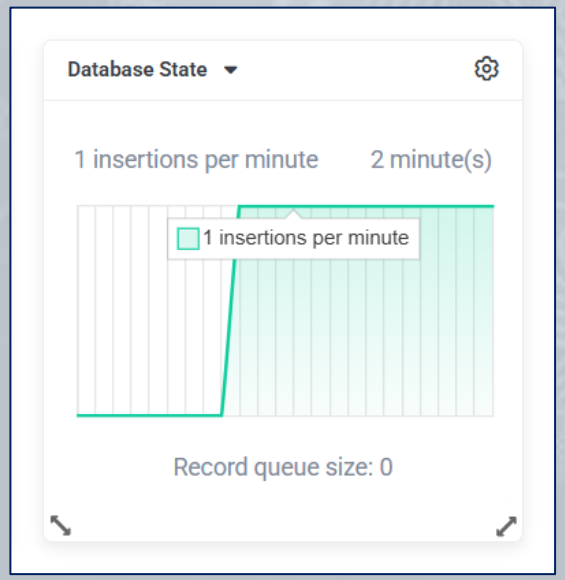
## Memory Usage




## CPU Usage




## Database State

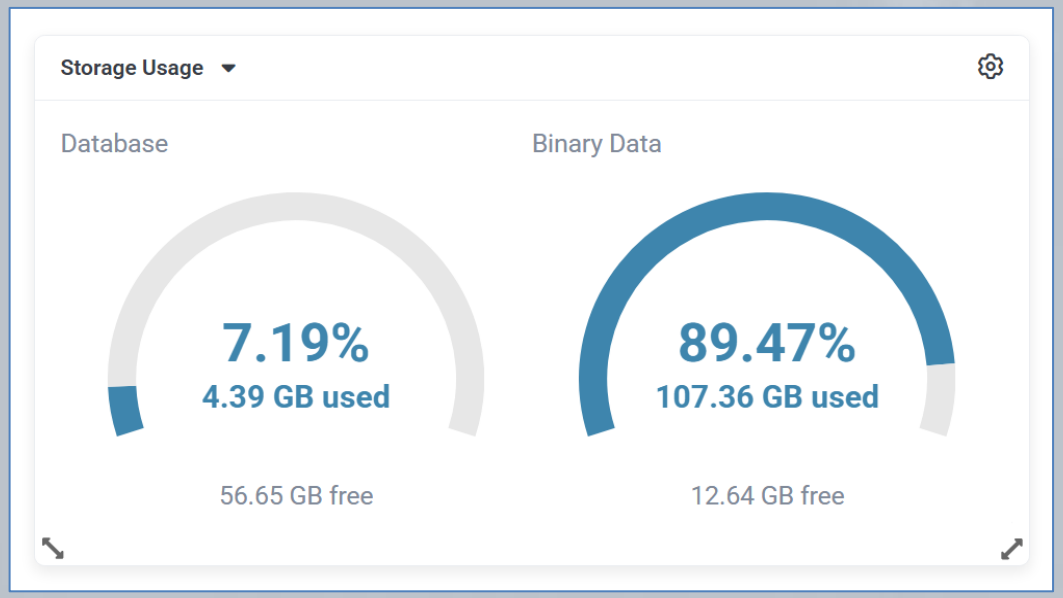


# System State Dashboards

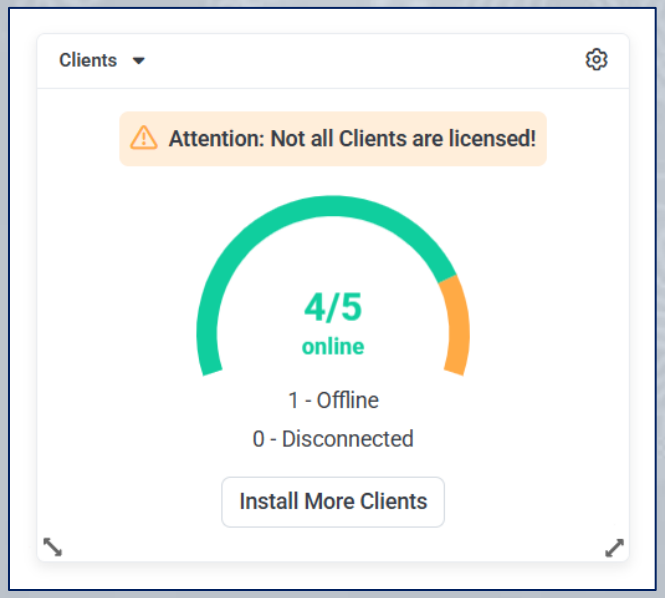
Syteca

The **Storage Usage** and **Clients** dashboards (on the **System Health** page) provide information about the system state in real time.

## Storage Usage




## Clients



# Reports

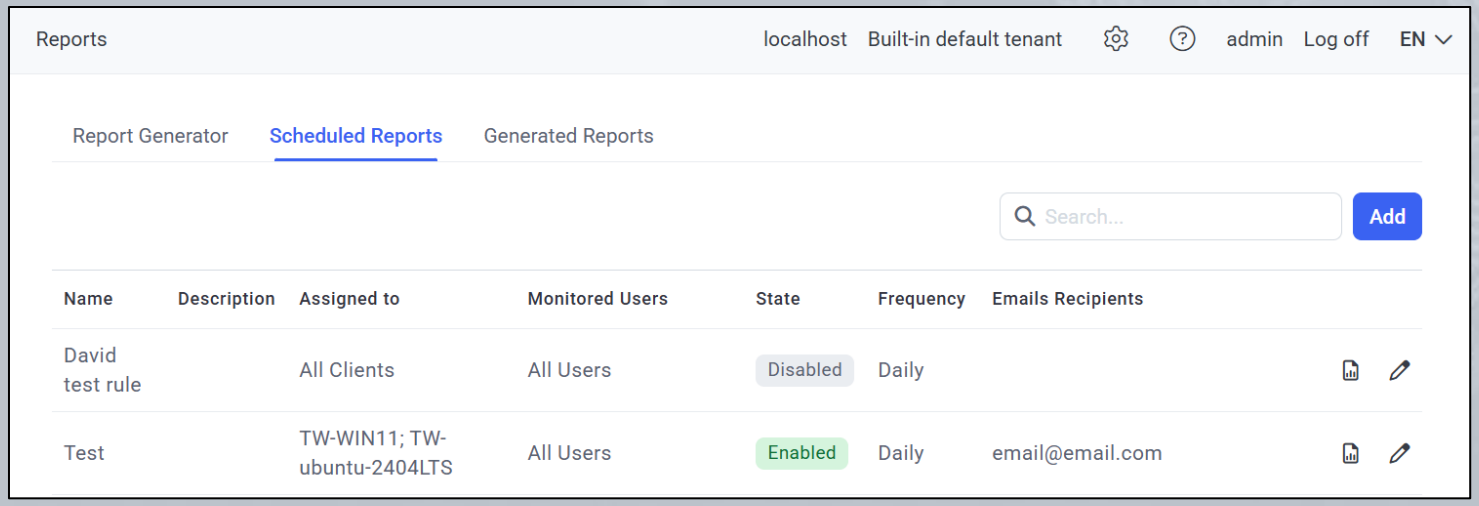
# Reports & Statistics

Syteca

You can generate **30+ types** of highly **customizable** reports 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, **Linux commands** executed, etc, and is available in a variety of **file formats**.

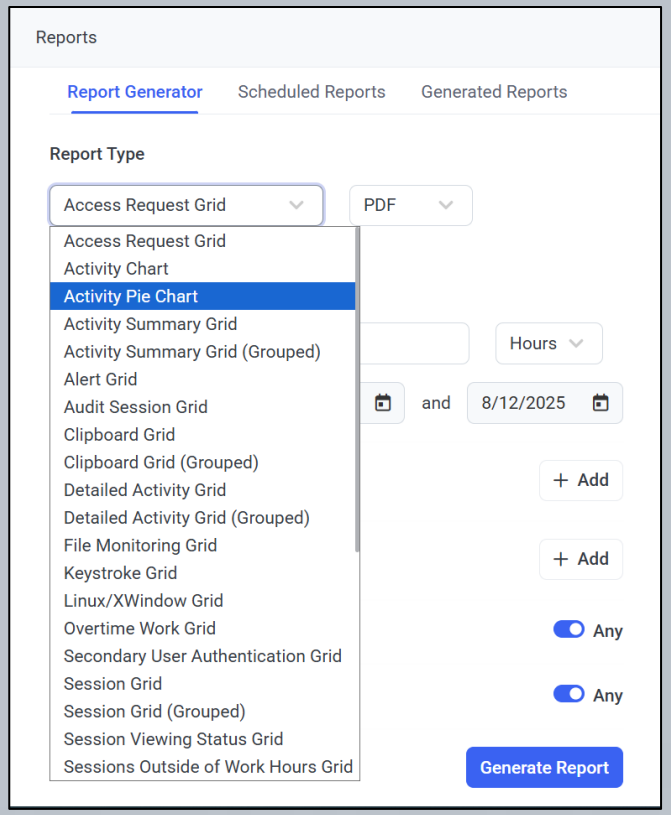
**Scheduled Reports**

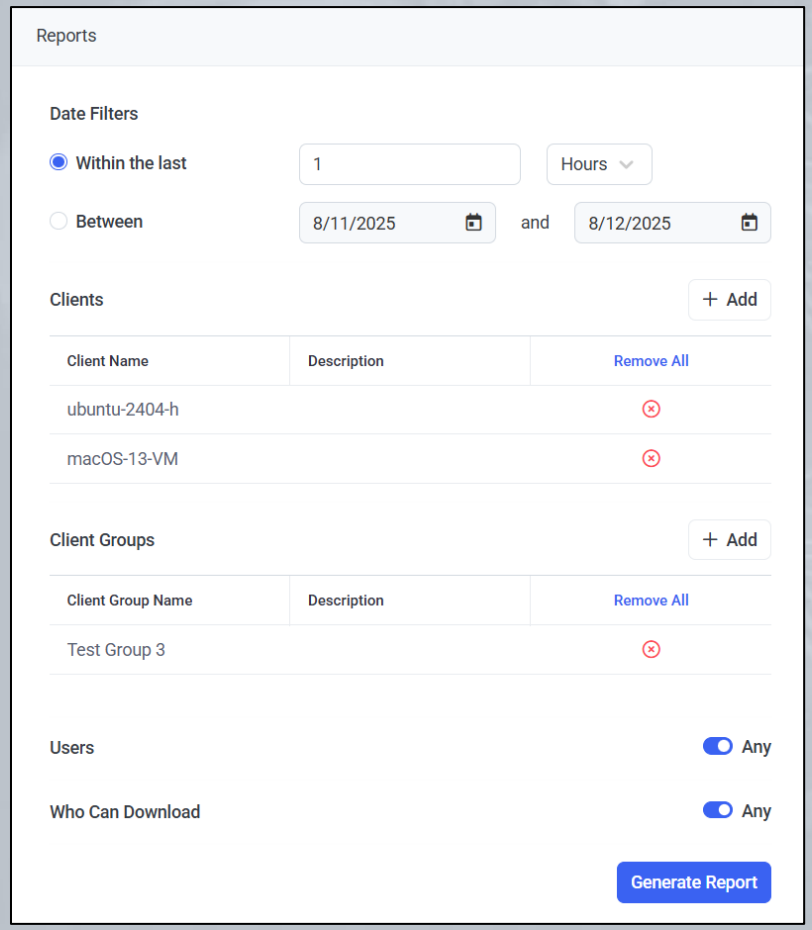


Syteca

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

## Manual Report Generation



# Examples of Report Types

Syteca

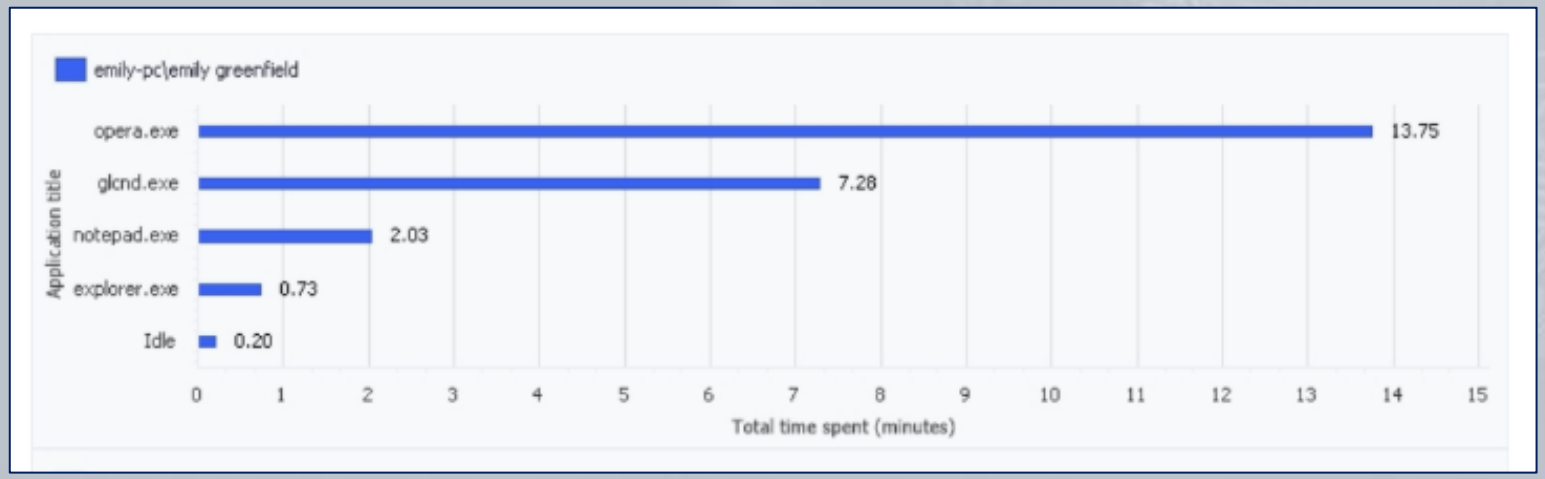
## Activity Summary Grid Report

| | |
|---|---|
| **Client name** | emily-pc |
| **Client description** | |
| **User name** | emily-pc\carol looney |
| **Total time** | 24 minutes |
| **Active time** | 23 minutes, 31 seconds |

| Application name | % | Time spent |
|---|---|---|
| opera.exe | 43.54 | 10 minutes, 27 seconds |
| WINWORD.EXE | 20.35 | 4 minutes, 53 seconds |

## Activity Pie Chart Report


## Activity Chart Report



# Examples of Report Types

Syteca

## Access Requests Grid Report

| Client Name | User Name | Request Type | Requested At | Status | Proccessed At | Proccessed By | Expired At |
|---|---|---|---|---|---|---|---|
| emily-pc | emily-pc\carol looney | Endpoint Access | 08/18/2024 03:59:46 PM | Expired | | | 08/17/2024 03:59:46 PM |
| emily-pc | emily-pc\emily greenfield | Endpoint Access | 08/19/2024 11:59:46 AM | Denied | 08/19/2024 12:59:46 PM | admin | |
| emily-pc | emily-pc\paul johnson | Endpoint Access | 08/21/2024 12:59:46 PM | Pending | | | |
| emily-pc | emily-pc\tom green | Endpoint Access | 08/20/2024 12:59:46 PM | Approved | 08/20/2024 01:59:46 PM | admin | |
| leslie-pc | leslie-pc\leslie howell | Endpoint Access | 12/08/2023 04:54:56 PM | Expired | | | |
| leslie-pc | leslie-pc\randy mccreed | Endpoint Access | 12/08/2023 04:43:34 PM | Denied | 12/08/2023 04:57:29 PM | admin | |

## Sessions Outside of Work Hours Grid Report

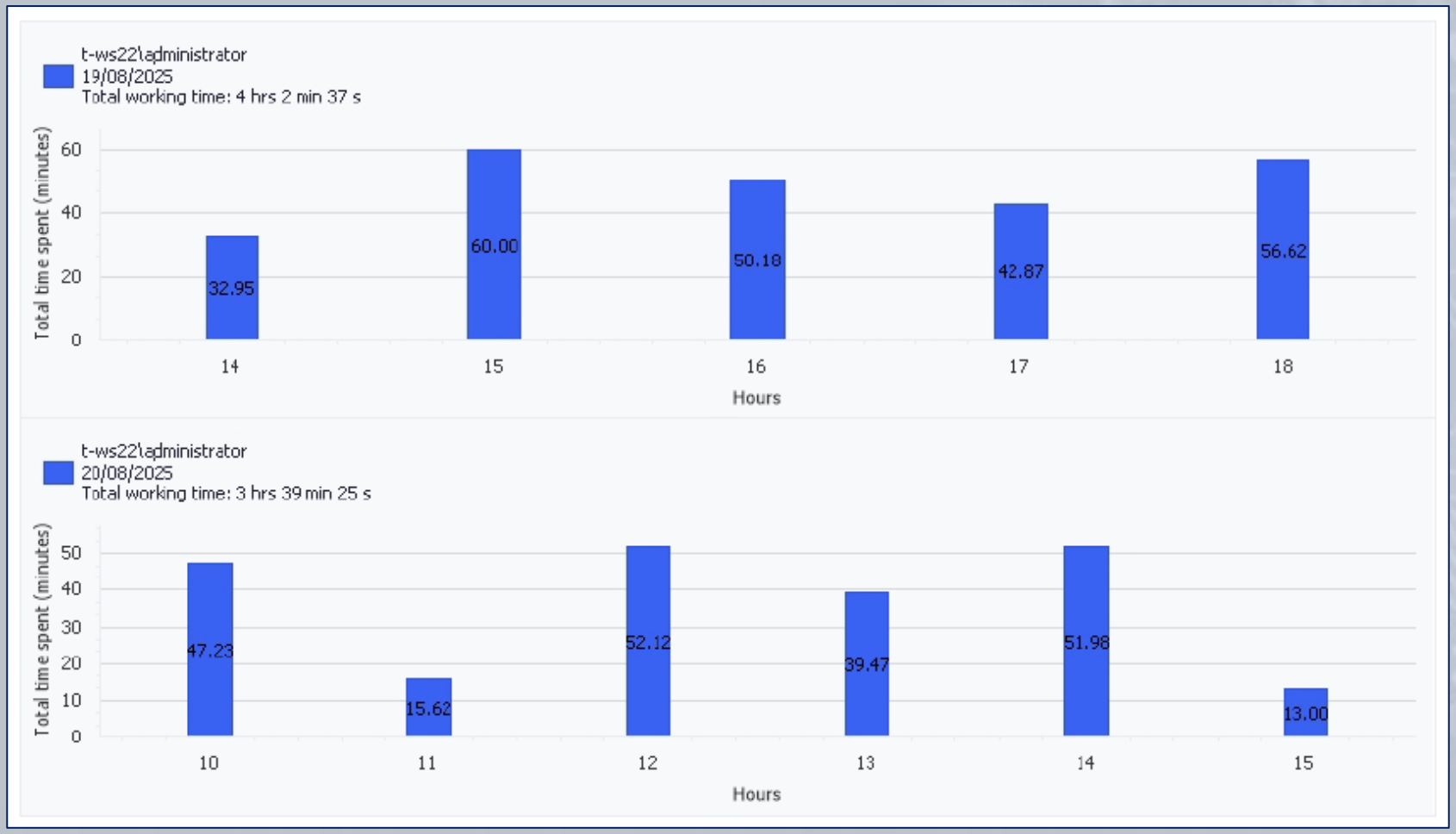
| | |
|---|---|
| Client name | aids-Mac-mini-3.local |
| Client description | |
| Total out of work hours | 20m 32s |

| User name | Total time spent | Active out of work hours | Session start time | Last activity time | Remote IP | Remote Public IP | Session URL |
|---|---|---|---|---|---|---|---|
| derricksmith | 11m 23s | 11m 23s | 01/19/2024 04:17:43 PM | 01/19/2024 04:29:06 PM | 10.200.0.194 | None | Open Session |
| richardstone | 9m 9s | 9m 9s | 01/19/2024 04:38:16 PM | 01/19/2024 04:47:25 PM | 10.200.0.194 | None | Open Session |

# Examples of Report Types

Syteca

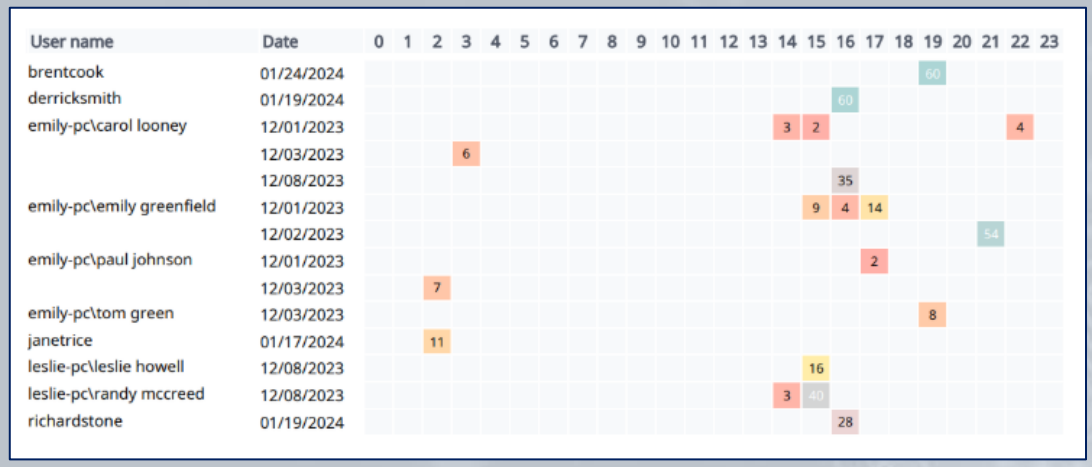
## User Productivity Chart Report



# Examples of Report Types

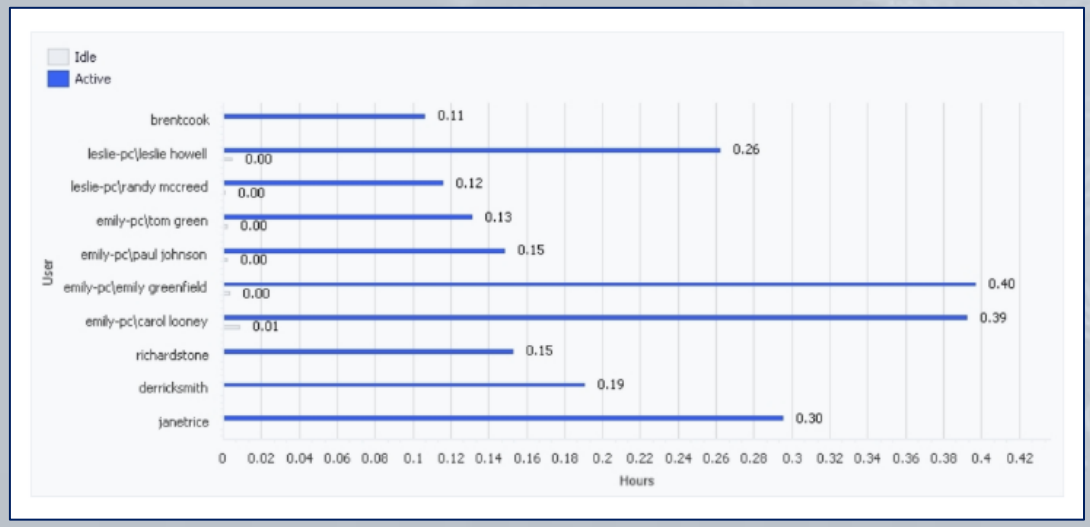
Syteca

## User Productivity Heatmap Report



| User name | Date | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| brentcook | 01/24/2024 | | | | | | | | | | | | | | | | | | | | 60 | | | | |
| derricksmith | 01/19/2024 | | | | | | | | | | | | | | | | | 60 | | | | | | | |
| emily-pc\carol looney | 12/01/2023 | | | | | | | | | | | | | | | 3 | 2 | | | | | | | 4 | |
| | 12/03/2023 | | | | 6 | | | | | | | | | | | | | | | | | | | | |
| | 12/08/2023 | | | | | | | | | | | | | | | | | 35 | | | | | | | |
| emily-pc\emily greenfield | 12/01/2023 | | | | | | | | | | | | | | | | 9 | 4 | 14 | | | | | | |
| | 12/02/2023 | | | | | | | | | | | | | | | | | | | | | | 54 | | |
| emily-pc\paul johnson | 12/01/2023 | | | | | | | | | | | | | | | | | | 2 | | | | | | |
| | 12/03/2023 | | | 7 | | | | | | | | | | | | | | | | | | | | | |
| emily-pc\tom green | 12/03/2023 | | | | | | | | | | | | | | | | | | | | 8 | | | | |
| janetrice | 01/17/2024 | | | 11 | | | | | | | | | | | | | | | | | | | | | |
| leslie-pc\leslie howell | 12/08/2023 | | | | | | | | | | | | | | | | 16 | | | | | | | | |
| leslie-pc\randy mccreed | 12/08/2023 | | | | | | | | | | | | | | | 3 | 40 | | | | | | | | |
| richardstone | 01/19/2024 | | | | | | | | | | | | | | | | | 28 | | | | | | | |

## User Active Time and Idle Time Chart Report



# Report Types: Examples

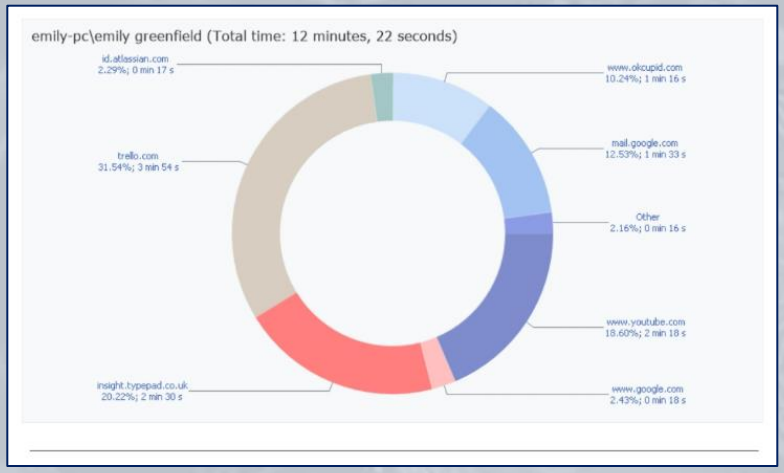
Syteca

## URL Summary Grid Report

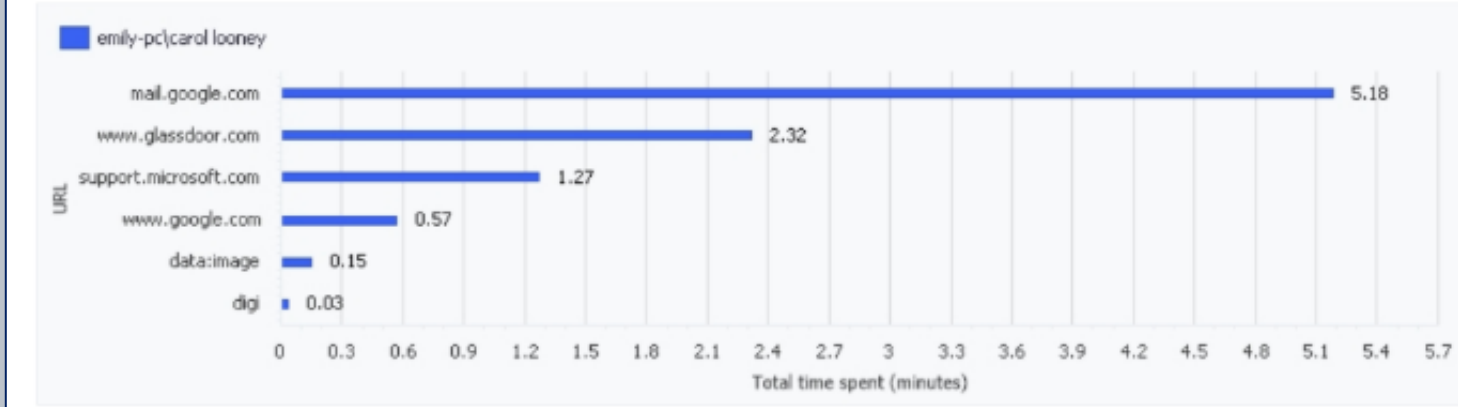
| | |
|---|---|
| **Client name** | emily-pc |
| **Client description** | |
| **User name** | emily-pc\carol looney |
| **Total time** | 9 minutes, 31 seconds |

| URL | % | Time spent |
|---|---|---|
| mail.google.com | 54.47 | 5 minutes, 11 seconds |
| www.glassdoor.com | 24.34 | 2 minutes, 19 seconds |
| support.microsoft.com | 13.31 | 1 minute, 16 seconds |
| www.google.com | 5.95 | 34 seconds |
| data:image | 1.58 | 9 seconds |
| digi | 0.35 | 2 seconds |

## URL Pie Chart Report




## URL Chart Report



# Examples of Report Types

Syteca

## USB Storage Grid Report

| | |
|---|---|
| Client name | emily-pc |
| Client description | |
| User name | emily-pc\carol looney |

| Time | Details |
|---|---|
| 09/01/2023 01:49:41 AM | Connected Microphone USB |
| 09/01/2023 01:49:41 AM | Connected Microphone USB |
| 09/07/2023 02:02:00 PM | Connected Keyboard USB |
| 09/07/2023 02:02:00 PM | Connected Keyboard USB |
| 09/14/2023 12:10:15 PM | Connected Mouse USB |

## USB Alert Grid Report

| | |
|---|---|
| Client name | emily-pc |
| Client description | |
| User name | emily-pc\carol looney |

| Time | Rule Name | Action | Risk Level | Device Class | Device Details |
|---|---|---|---|---|---|
| 12/08/2023 04:20:31 PM | | Allowed | | Camera | RZR Device; RZR Device\RZR-00225002198 |
| 12/08/2023 04:20:31 PM | | Blocked | | Microphone | RZR Device; RZR Device\RZR-000054324321 |

# Report Types : Examples

Syteca

## Terminal Server Grid Report

| Date | 09/01/2024 | | | |
|---|---|---|---|---|
| **Client name** | **Number of users** | **User name** | **Number of connections** | **Total time** |
| Terminal-Server-US | 2 | terminal-server-us\taskrunner | 1 | 12h 0m 0s |
| | | terminal-server-eu\genericuser | 1 | 12h 0m 0s |

| Date | 09/02/2024 | | | |
|---|---|---|---|---|
| **Client name** | **Number of users** | **User name** | **Number of connections** | **Total time** |
| Terminal-Server-EU | 1 | terminal-server-eu\genericuser | 1 | 12h 0m 0s |

| Date | 09/03/2024 | | | |
|---|---|---|---|---|
| **Client name** | **Number of users** | **User name** | **Number of connections** | **Total time** |
| Terminal-Server-US | 2 | terminal-server-eu\systemuser | 1 | 12h 0m 0s |
| | | terminal-server-us\serviceaccount | 1 | 12h 0m 0s |
| Terminal-Server-TR | 1 | terminal-server-tr\logprocessor | 1 | 12h 0m 0s |

# Report Types: Examples

Syteca

The Audit Session Grid Report is a **special** report type, 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 |
|---|---|---|---|---|---|
| 11/30/2023 12:33:13 AM | | Viewed session | | emily-pc | |
| 11/30/2023 12:50:25 AM | | Viewed session | | emily-pc | |
| 11/30/2023 12:54:57 AM | | Viewed session | | emily-pc | |
| 11/30/2023 12:55:23 AM | | Viewed session | | emily-pc | |
| 11/30/2023 12:55:33 AM | | Viewed session | | emily-pc | |
| 11/30/2023 12:57:42 AM | | Viewed session | | emily-pc | |
| 11/30/2023 01:04:54 AM | | Viewed session | | emily-pc | |
| 11/30/2023 03:33:19 PM | | Viewed session | | emily-pc | |
| 11/30/2023 03:45:38 PM | | Viewed session | | emily-pc | |
| 12/01/2023 02:53:29 PM | | Viewed session | | emily-pc | |

# Report Types

Syteca

The Session Viewing Status Grid Report is a **special** report type that allows **whether all Client sessions have been viewed** (by at least one user) to be **conveniently checked** (as well as **who** has viewed each session, and **when**).

## Session Viewing Status Grid Report

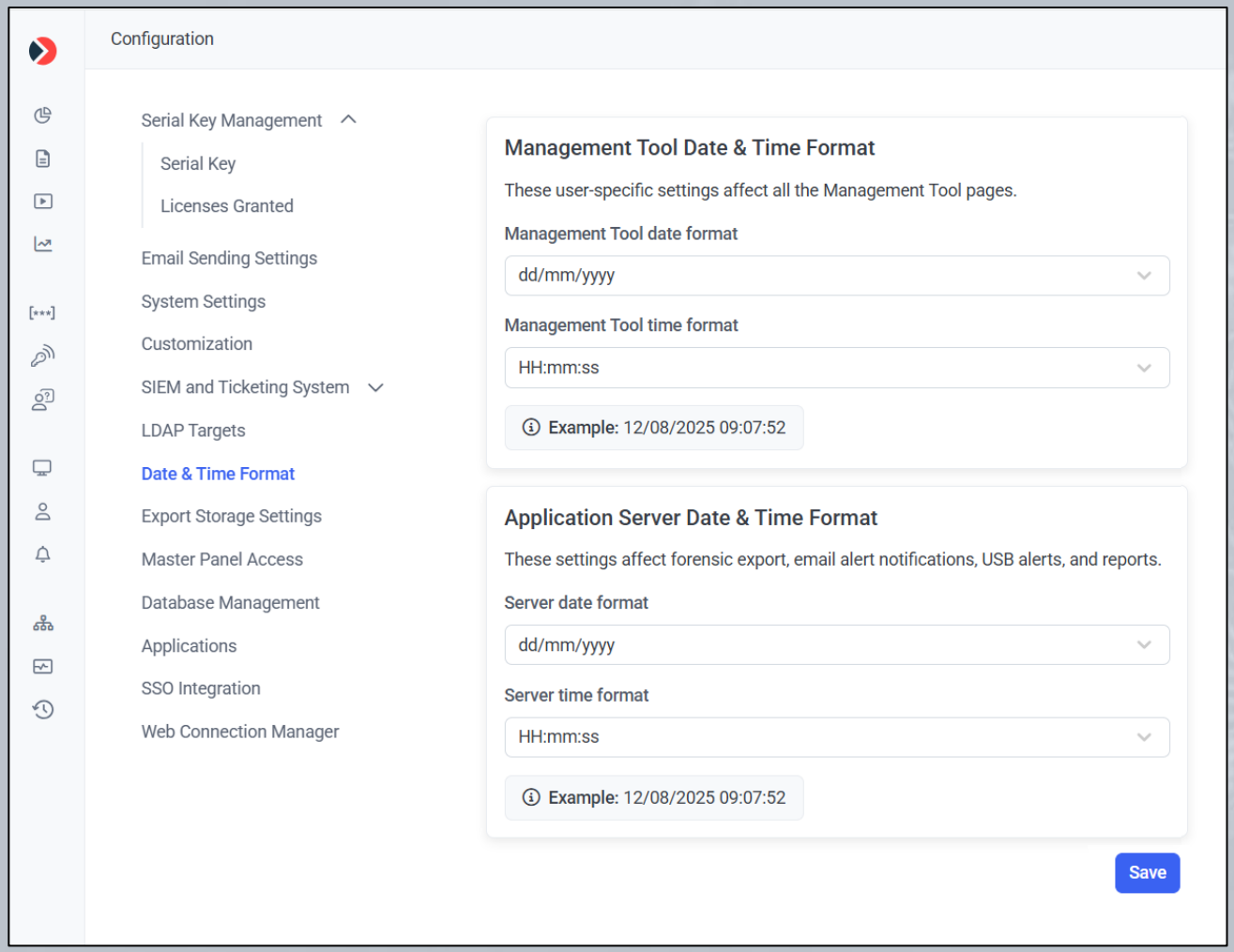
| Session ID | User name | Client name | Session start | Last activity | Remote IP | Remote Public IP | Session URL | Is viewed | Viewer user name | Date and time |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | emily-pc | emily-pc\user | 06/18/2025 01:09:57 PM | 06/18/2025 02:09:57 PM | 192.168.100.2 | 203.0.114.2 | Open Session | No | | |
| 2 | emily-pc | emily-pc\user | 06/18/2023 02:09:57 PM | 06/18/2023 02:09:57 PM | 192.168.100.2 | 203.0.114.2 | Open Session | No | | |
| 3 | emily-pc | emily-pc\user | 06/18/2023 02:09:57 PM | 06/18/2023 02:09:57 PM | 192.168.100.2 | 203.0.114.2 | Open Session | Yes | emily-pc | 06/18/2023 02:09:57 PM |
| 3 | leslie-pc | leslie-pc | 06/18/2023 02:09:57 PM | 06/18/2023 02:09:57 PM | 192.168.100.3 | 203.0.114.3 | Open Session | Yes | leslie-pc | 06/18/2023 02:09:57 PM |
| 3 | leslie-pc | leslie-pc | 06/18/2023 02:09:57 PM | 06/18/2023 02:09:57 PM | 192.168.100.3 | 203.0.114.3 | Open Session | No | leslie-pc | 06/18/2023 02:09:57 PM |
| 3 | leslie-pc | leslie-pc | 06/18/2023 02:09:57 PM | 06/18/2023 02:09:57 PM | 192.168.100.3 | 203.0.114.3 | Open Session | No | leslie-pc | 06/18/2023 02:09:57 PM |
| 3 | emily-pc | emily-pc | 06/18/2023 02:09:57 PM | 06/18/2023 02:09:57 PM | 192.168.100.3 | 203.0.114.3 | Open Session | Yes | emily-pc | 06/18/2025 01:09:57 PM |
| 3 | emily-pc | emily-pc | 06/18/2023 02:09:57 PM | 06/18/2023 02:09:57 PM | 192.168.100.3 | 203.0.114.3 | Open Session | Yes | emily-pc | 06/18/2023 02:09:57 PM |

# System Customization

# Setting the Date & Time Format

Syteca

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



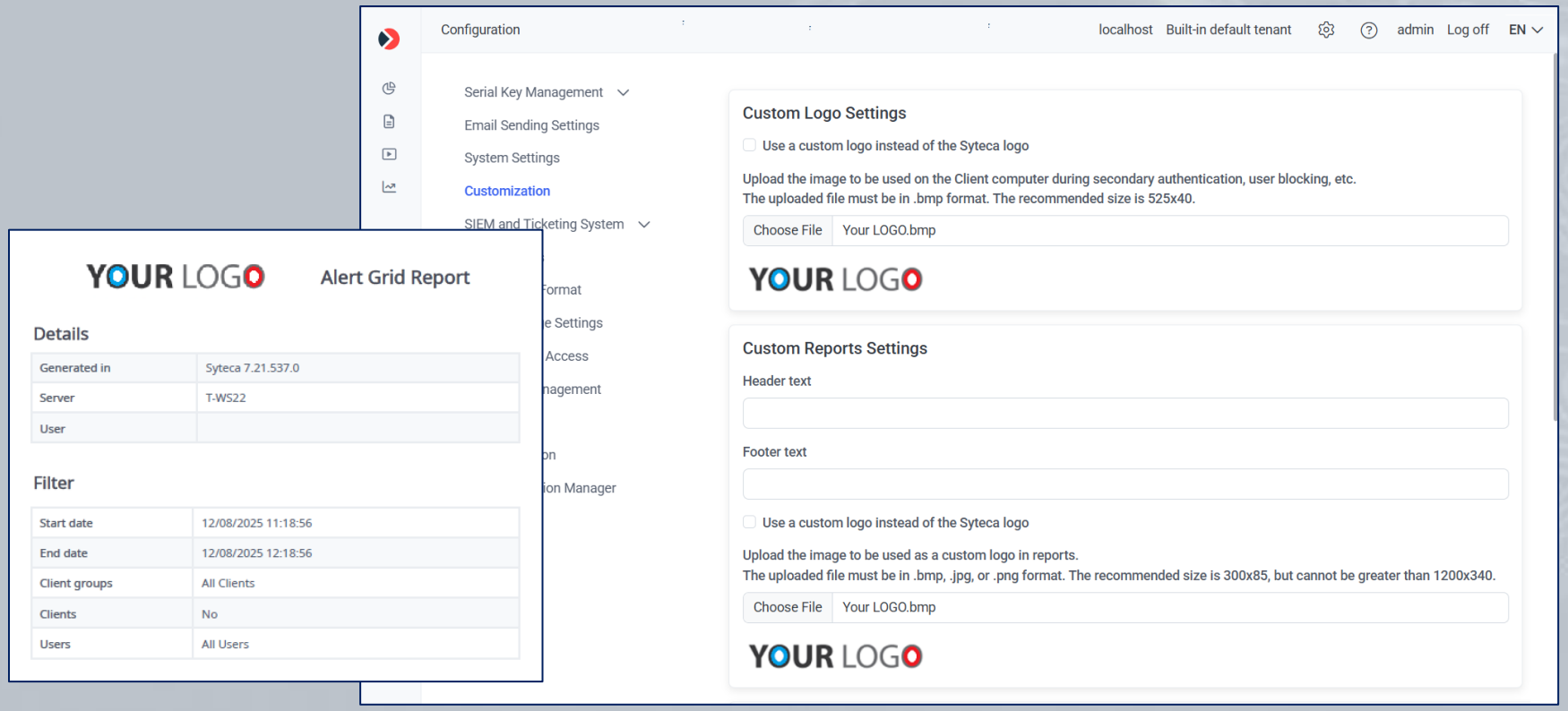
# Customizing the Logo on Client Notifications

Syteca

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.

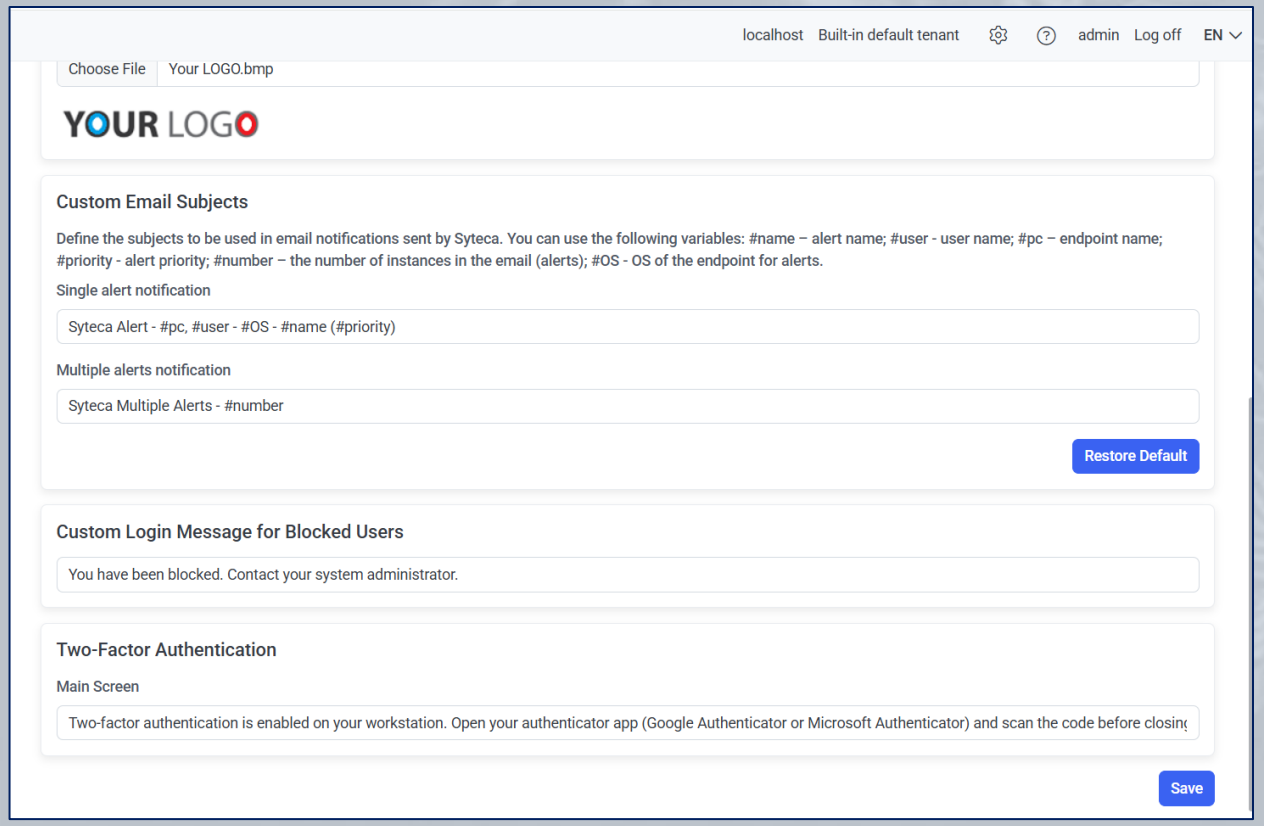
# Customizing Reports

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 Syteca.

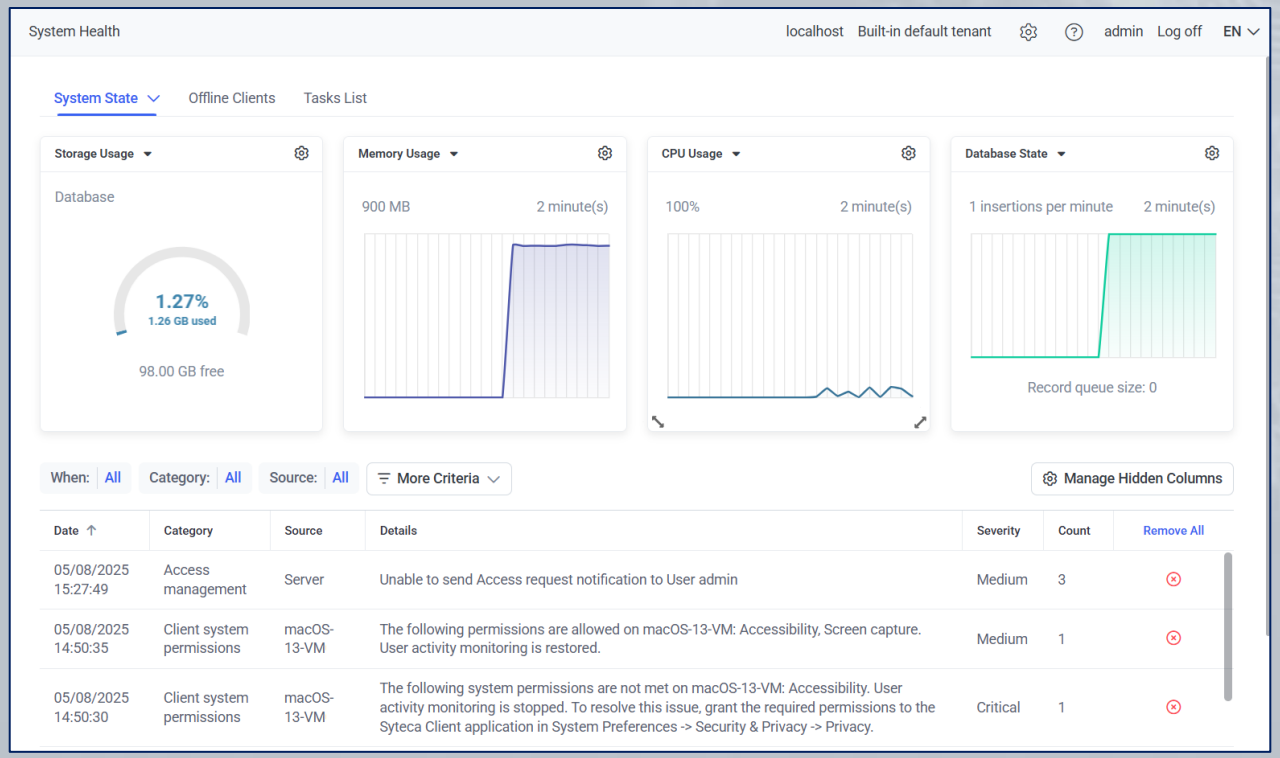


# System Health Monitoring

# System Health Monitoring

Syteca

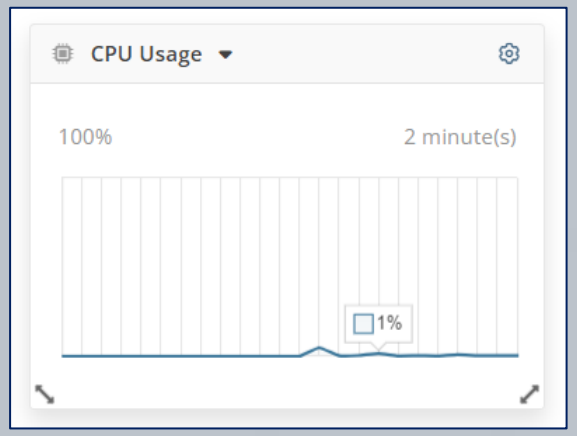
System Health monitoring allows you view the Application Server and database resources in real-time and get detailed information about any system **errors** with **warnings** to assist you in **reacting** to any issues in a **timely** manner.

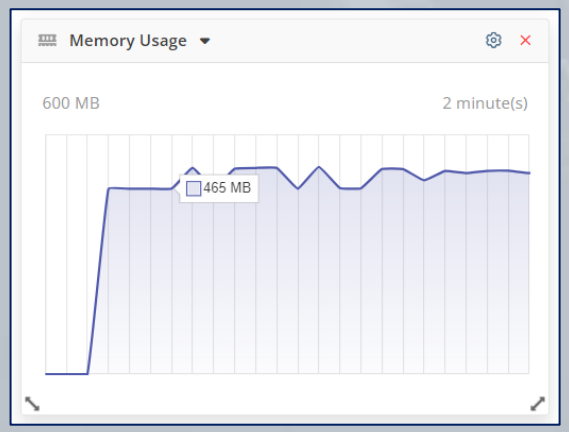


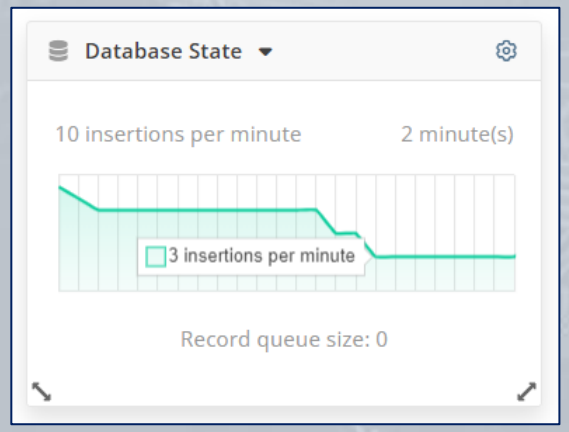
# Server Resource Monitoring

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

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

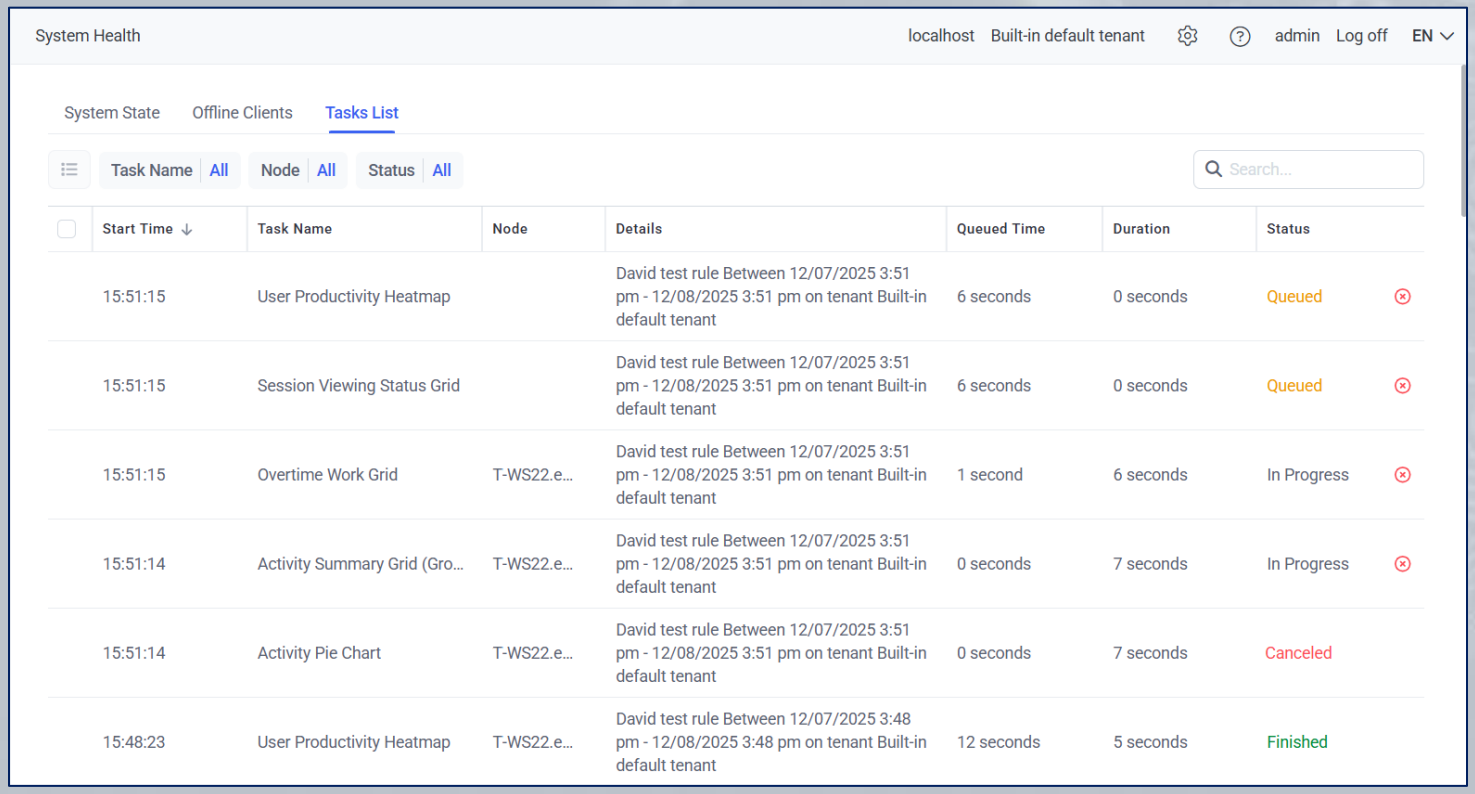


# The Tasks List

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



# Syteca SDK, APIs and Integrations

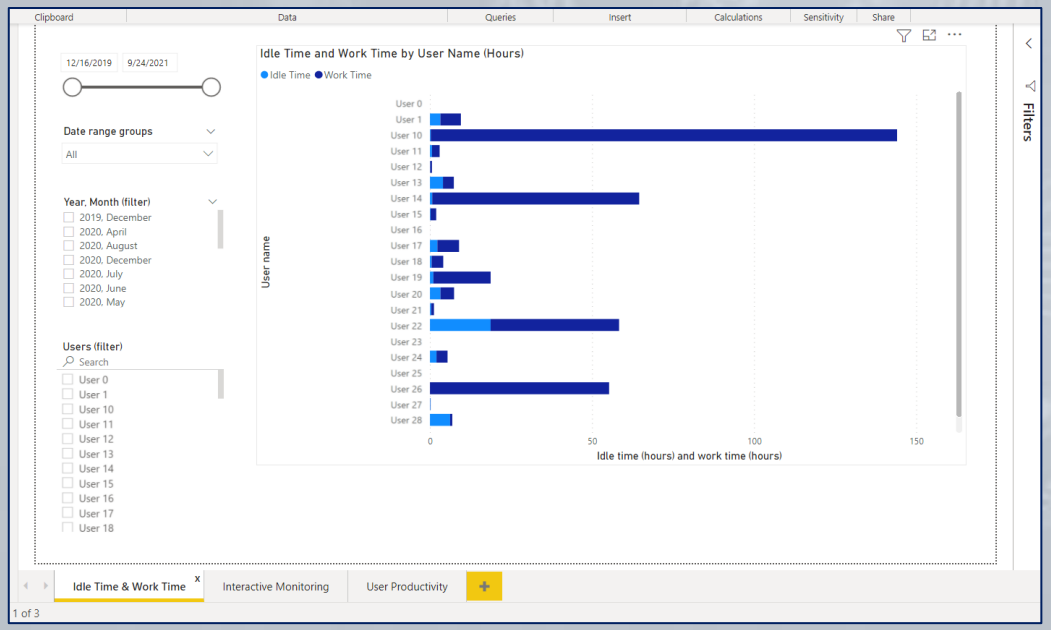
(e.g. with Power BI, Venn, SSO providers, etc.)

# Syteca API Data Connector

Syteca provides several APIs (for developers), e.g. **Syteca API Data Connector** is a stand-alone component of Syteca that is used for **integrating a customer's IT system** via Syteca API.

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

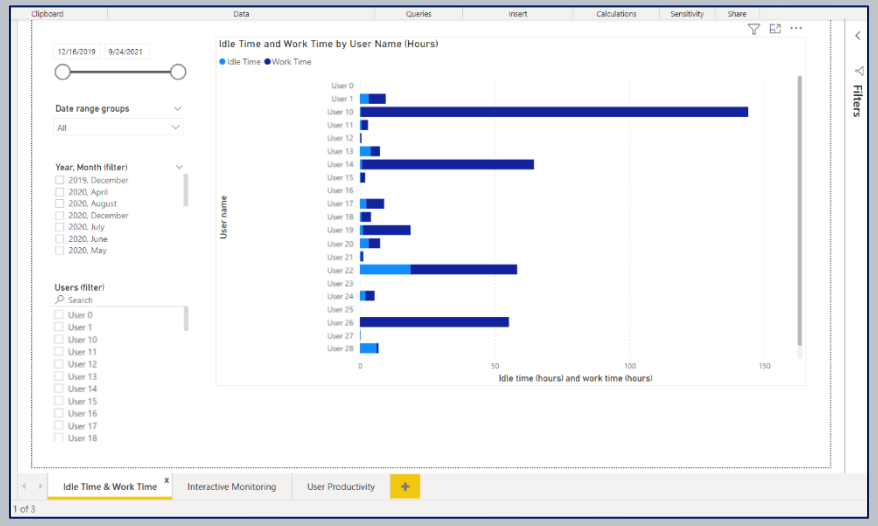
**Idle Time & Work Time Report**



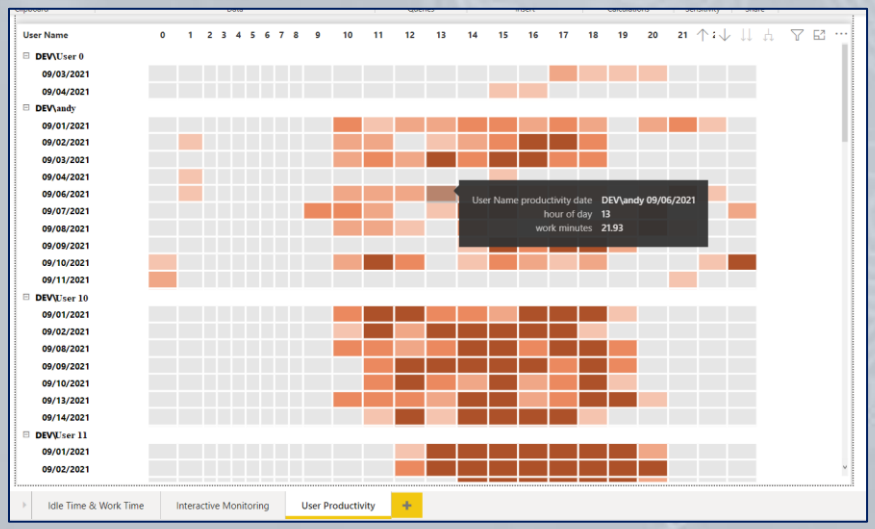
# Syteca Data Connector with Power BI

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



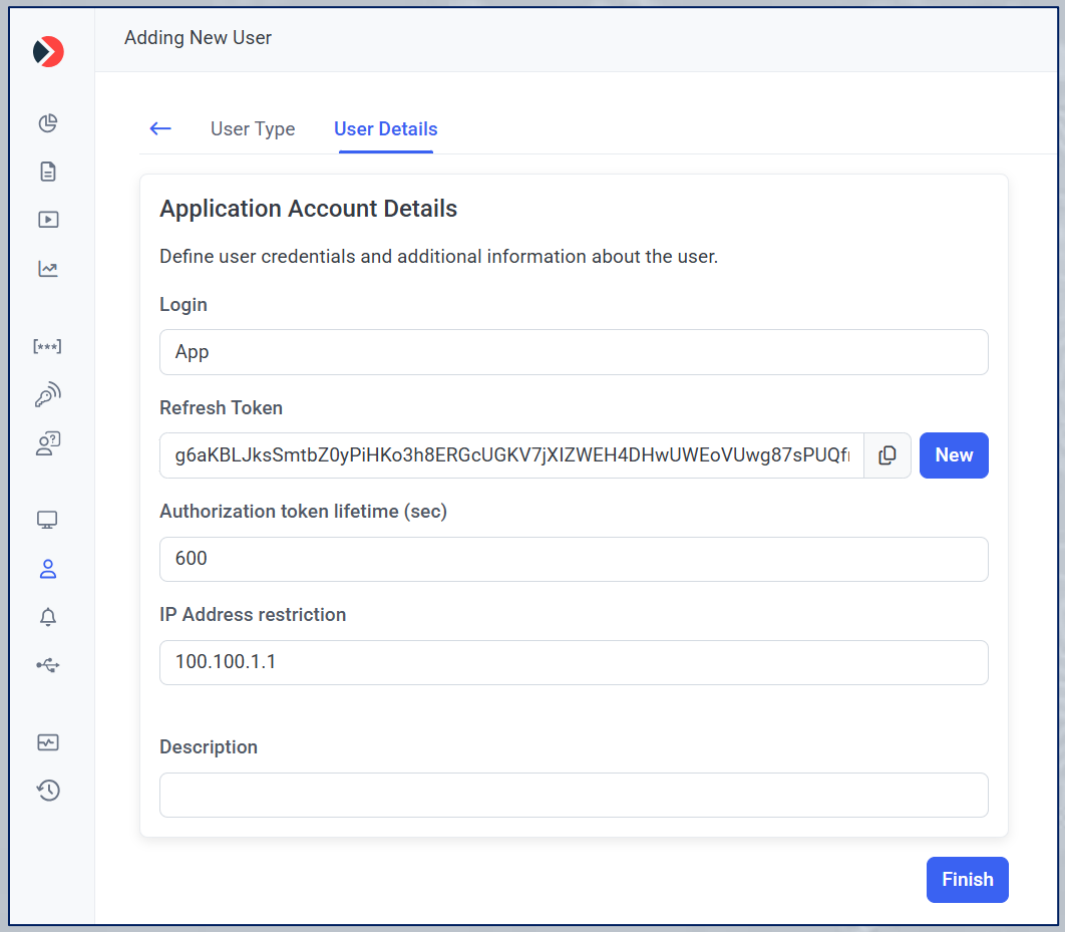

## User Productivity Report



# Syteca Application Credentials Broker (ACB)

Syteca **Application Credentials Broker (ACB)** is a stand-alone component of Syteca that is used for **integrating a customer's IT system with Syteca**.

This application is designed to allow customers to **get** Syteca **secrets' data via the ACB API**, to use it for their own business purposes.

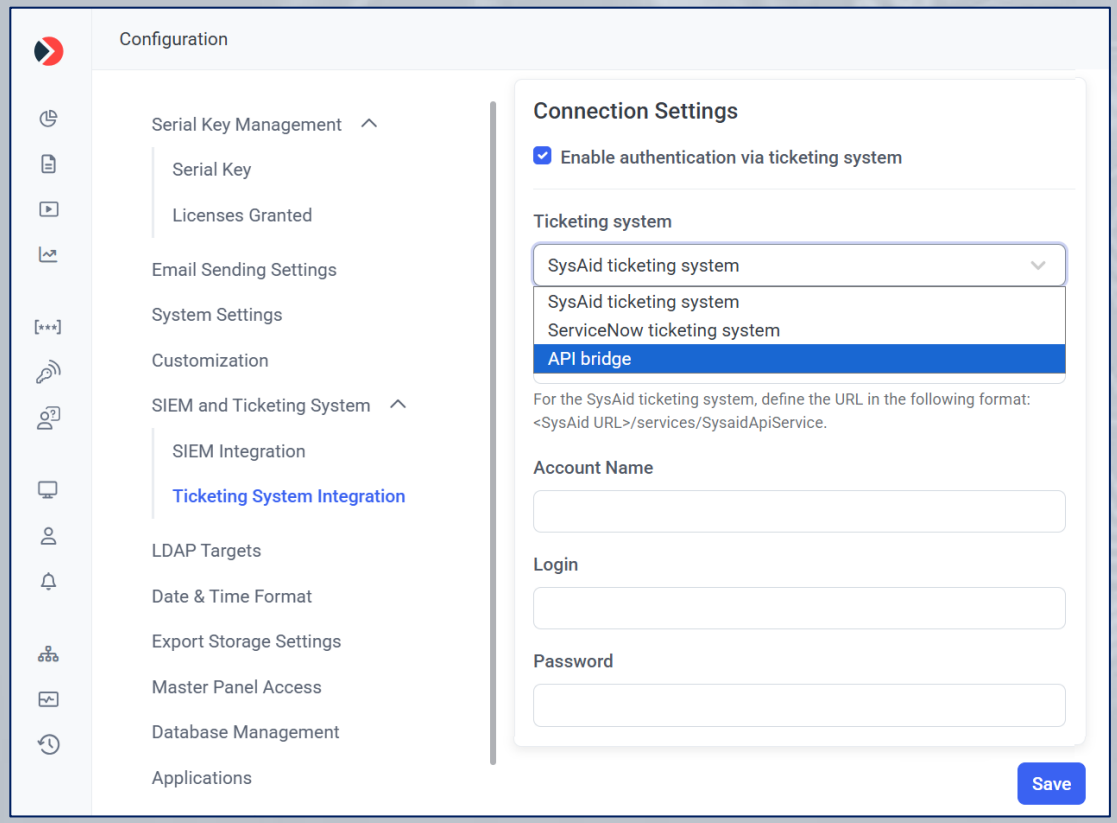


# Syteca API Bridge (for Ticketing Systems)

Syteca

Ticketing system integration allows you to **require users to provide ticket numbers to log in** to Client computers.

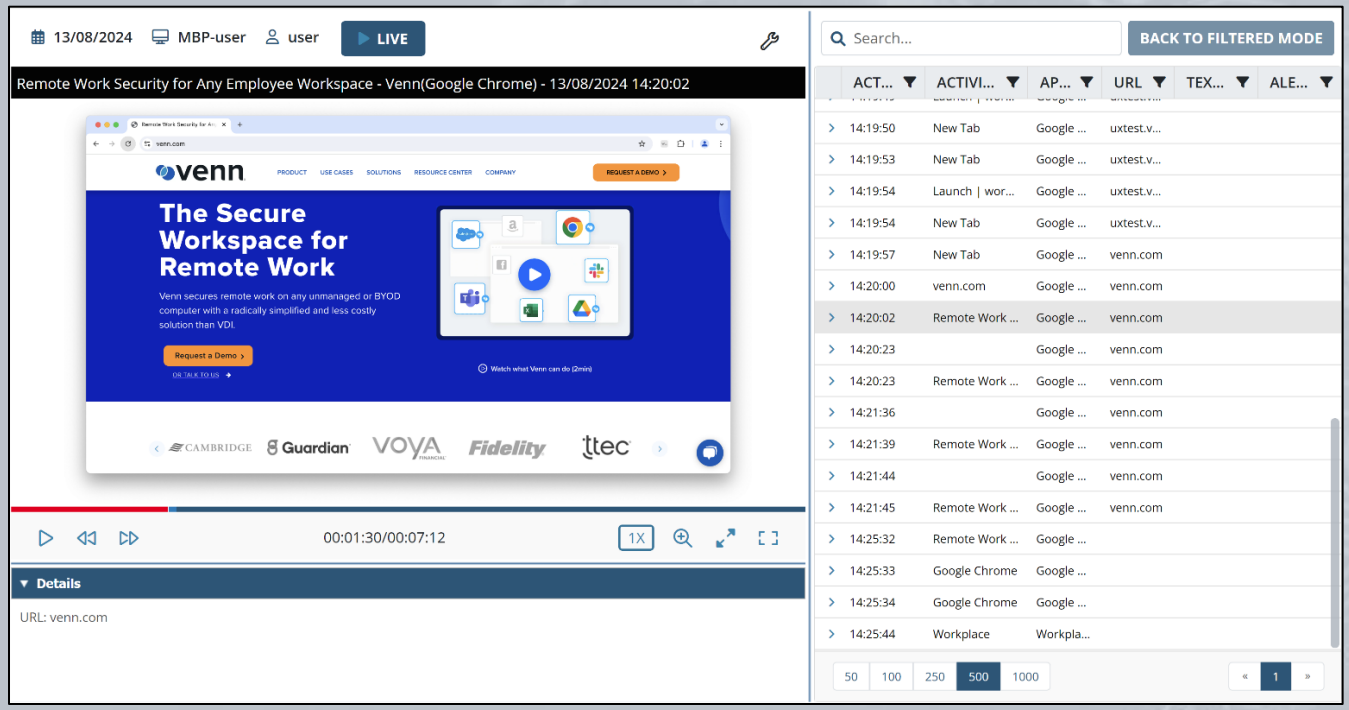
Syteca **API Bridge** is a REST-based HTTP application that allows **integration** with different **ticketing systems**, where the **SysAid** and **ServiceNow** ticketing systems are already currently supported.



# Integration with the Venn App Launcher

Syteca is **integrated with**, and **can be configured** for use with, a variety of third-party products.

For example, Syteca is **integrated with the Venn** app launcher, and can **monitor user activity only** in **applications opened** by users in a **Venn workspace.**

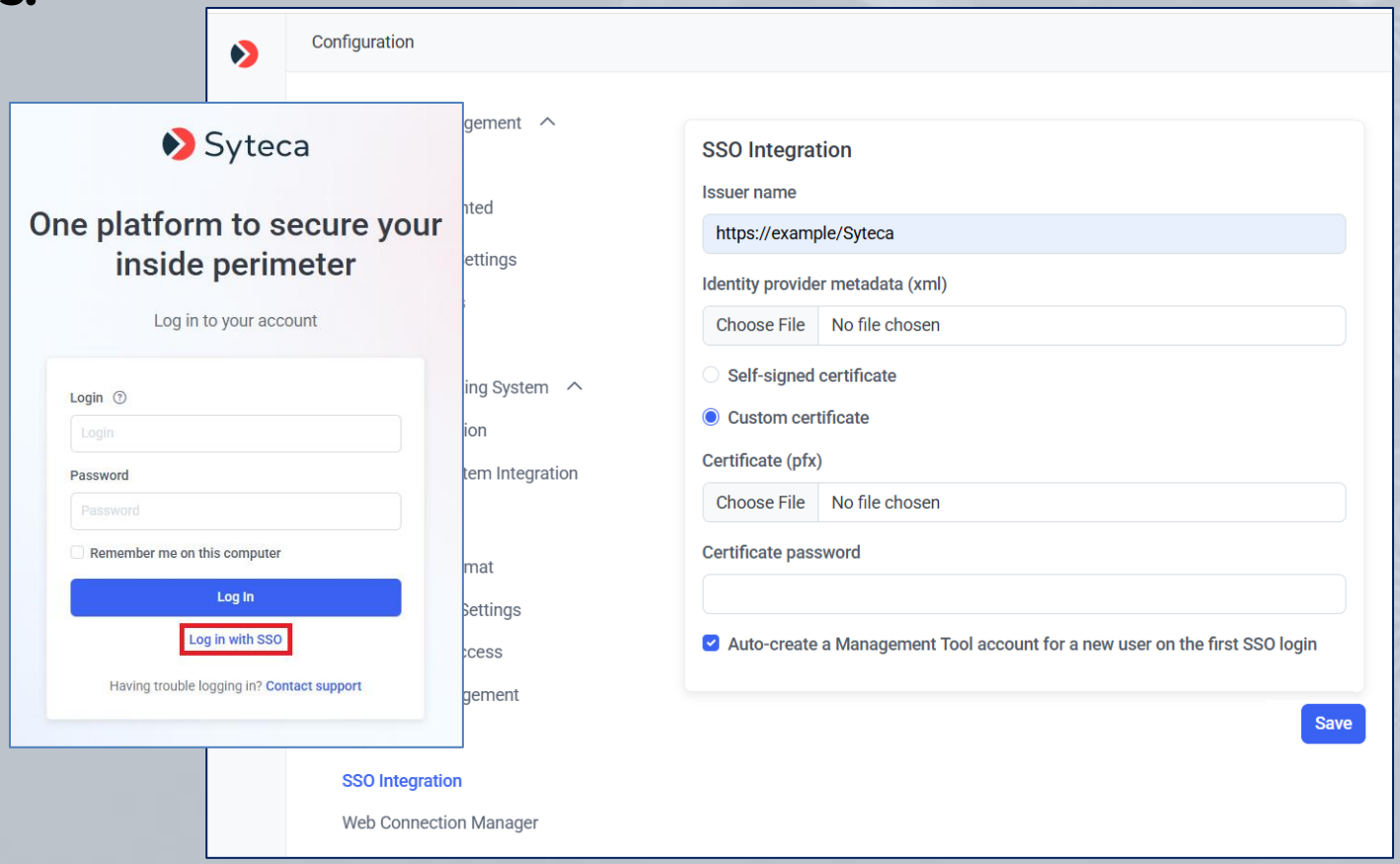


# Single Sign-On (SSO) Integrations

Syteca

Syteca is **integrated with**, and **can be configured** for use with, several **SSO providers.**

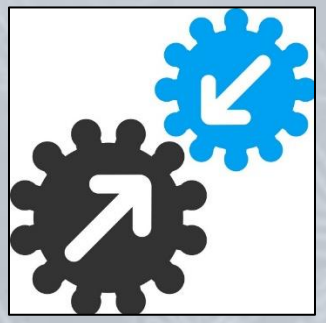
Syteca is currently integrated with **ForgeRock SSO**, **Azure SSO**, and **Okta SSO**, etc.



# Other Products Supported

A wide-range of other **third-party products and services**, etc. are used, **supported** and/or can be **configured for use** with Syteca, such as:

- **Databases** (PostgreSQL / MS SQL Server).
- Data communication and **encryption protocols** (SSL, TLS, AES-256, SHA-256, RSA-2048, etc).
- **Storage** mediums & services (HSM, NAS, Amazon S3, etc).
- **Load balancers**.
- etc.



**NOTE: Some of these third-party products are described in more detail in other sections of this presentation.**


Visit us online:

**www.syteca.com**