



Full Feature Presentation



Table of Contents

- [System Overview](#)
- [Syteca Application Server & Management Tool](#)
- [Database Management](#)
- [Licensing](#)
- [Installing & Updating Clients](#)
- [Monitoring Parameters](#)
- [Detection of Disconnected Clients](#)
- [Client Protection](#)
- [Secondary User Authentication](#)
- [Two-Factor Authentication](#)
- [Password Management \(PAM\)](#)
- [Account Discovery \(PAM\)](#)
- [User Behavior Analytics \(UEBA\)](#)
- [Access Requests and Approval Workflow](#)
- [Notifying Users about Being Monitored](#)
- [Blocking Users](#)
- [Viewing Client Sessions](#)
- [Sensitive Data Masking](#)
- [Pseudonymizer](#)
- [Alerts](#)
- [USB Device Monitoring](#)
- [Dashboards](#)
- [Reports](#)
- [System Customization](#)
- [System Health Monitoring](#)
- [Syteca SDK, APIs and Integrations](#)

System Overview

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.

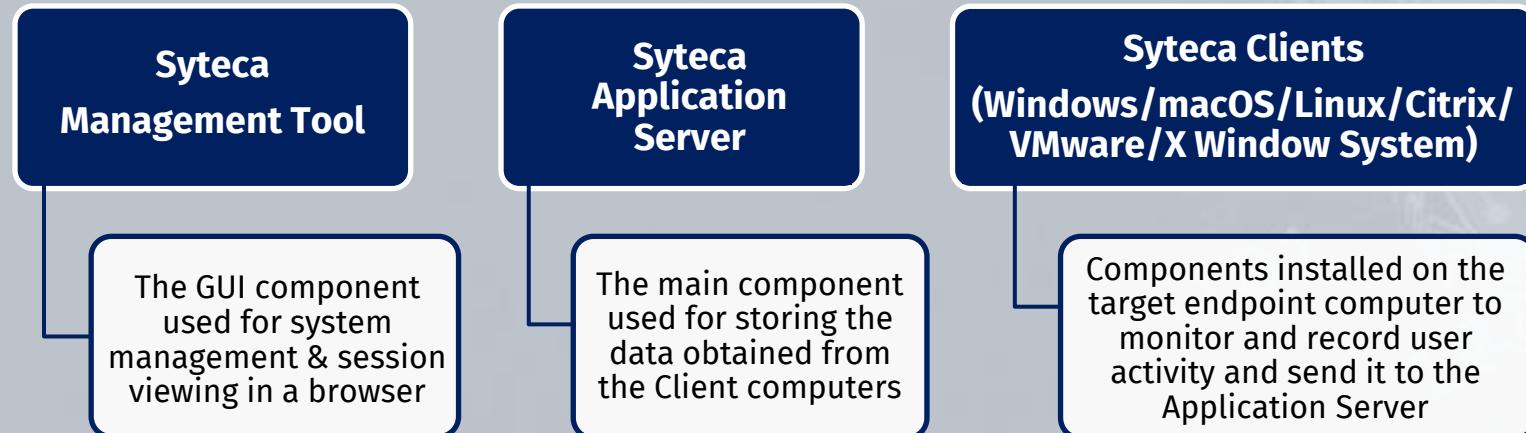
Flexible Deployment and Licensing

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.

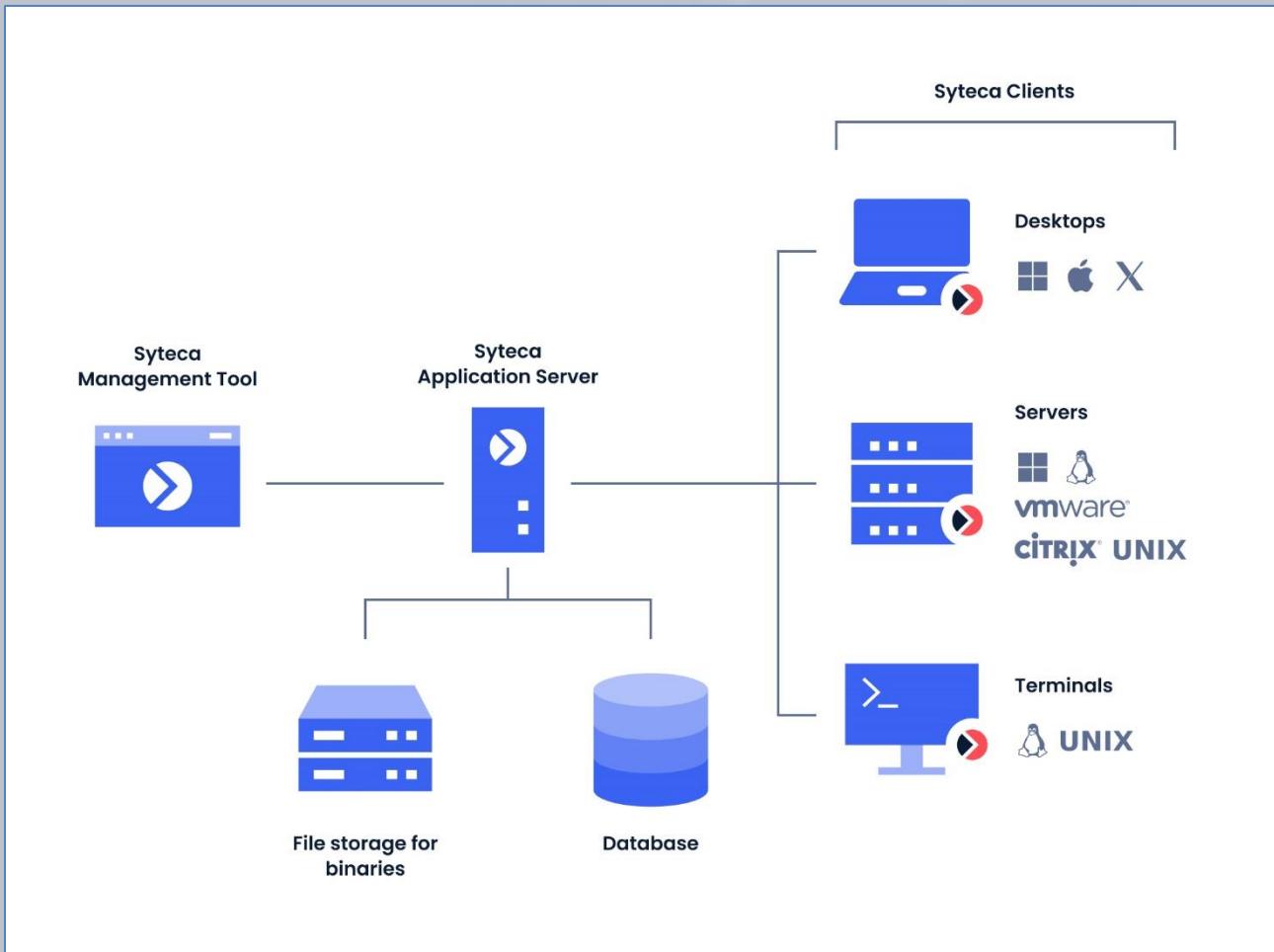
Syteca is an enterprise-level **cybersecurity platform** software solution featuring **privileged access management (PAM)** and **user activity monitoring (UAM)**. It is used to **protect** your corporate IT infrastructure from **internal risks**, as well as to assist you in meeting **compliance requirements** (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

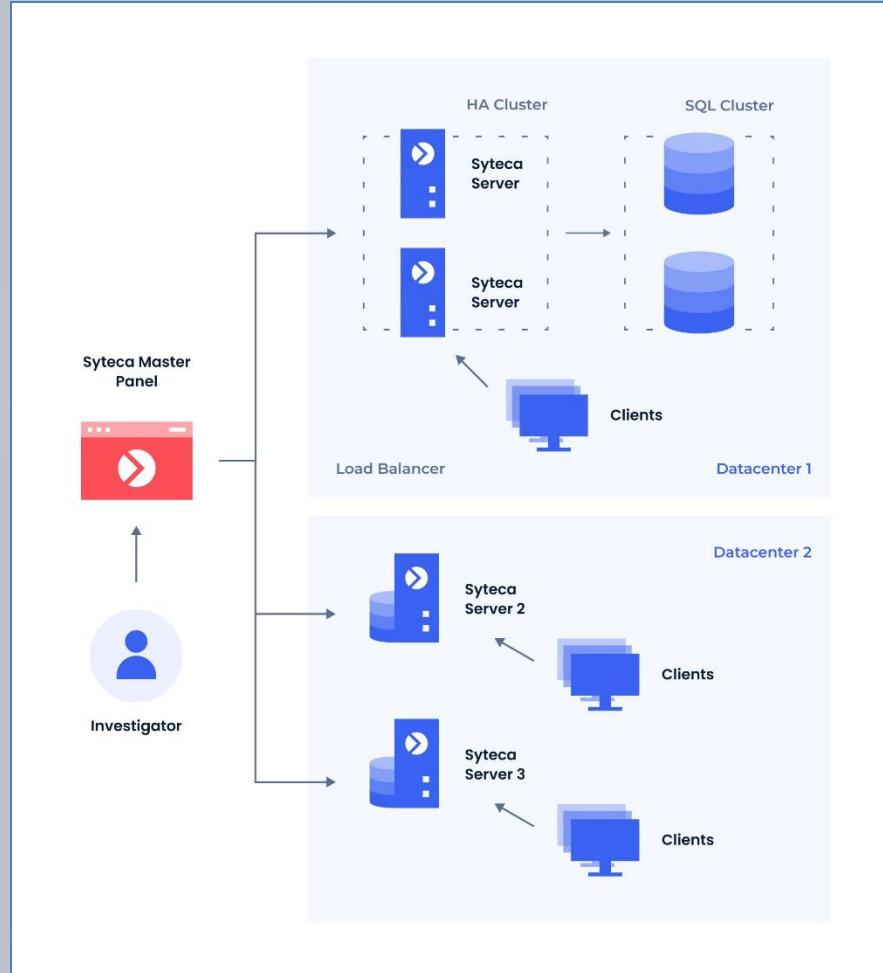


Large-Scale Deployments

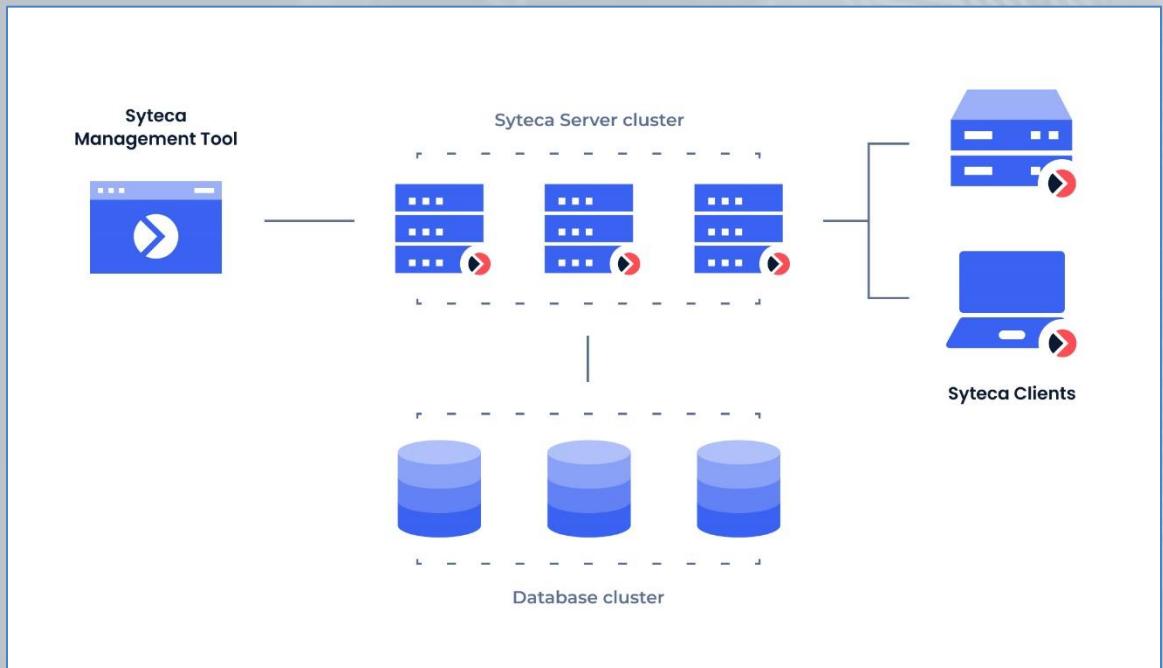
In terms of scalability, and for large organizations which may have several geographically isolated data centers, **multiple connected** instances of the **Application Server** can be deployed.

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.

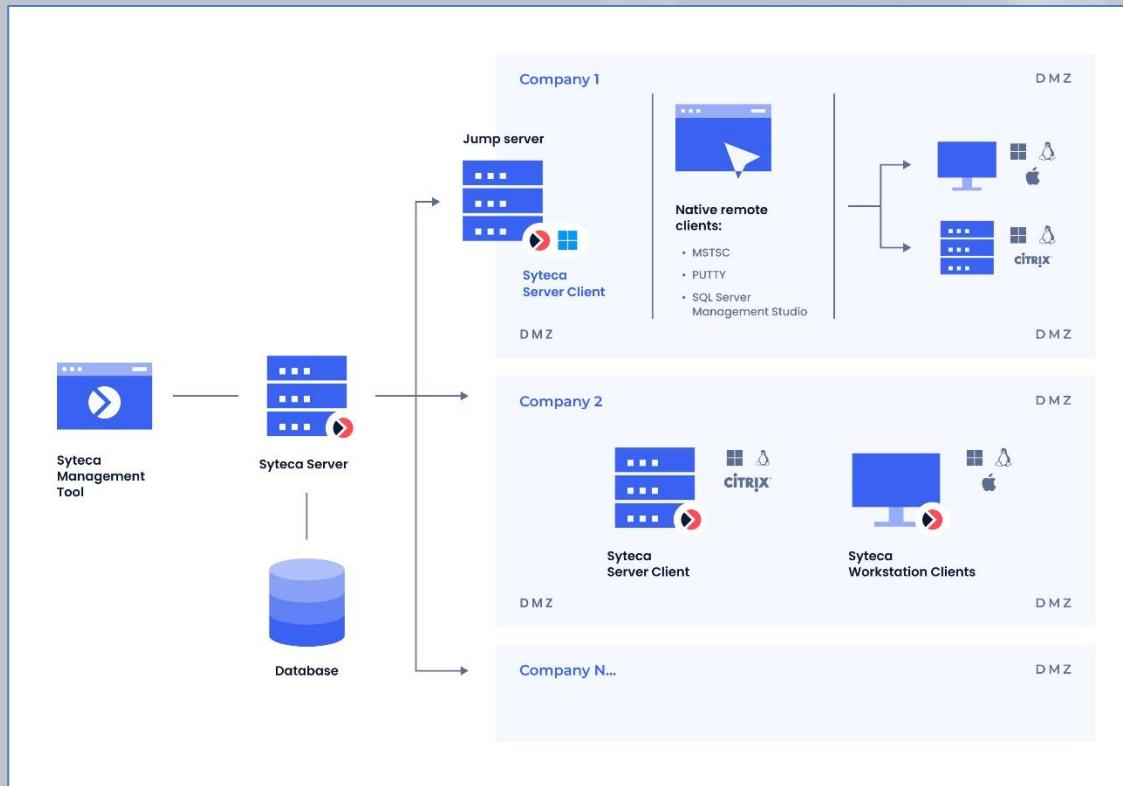
The **Master Panel**, which is an additional stand-alone component of Syteca, **combines the data** recorded by all Syteca Applications Servers in multiple locations, allowing the data to be **viewed and managed in a single user interface**.



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



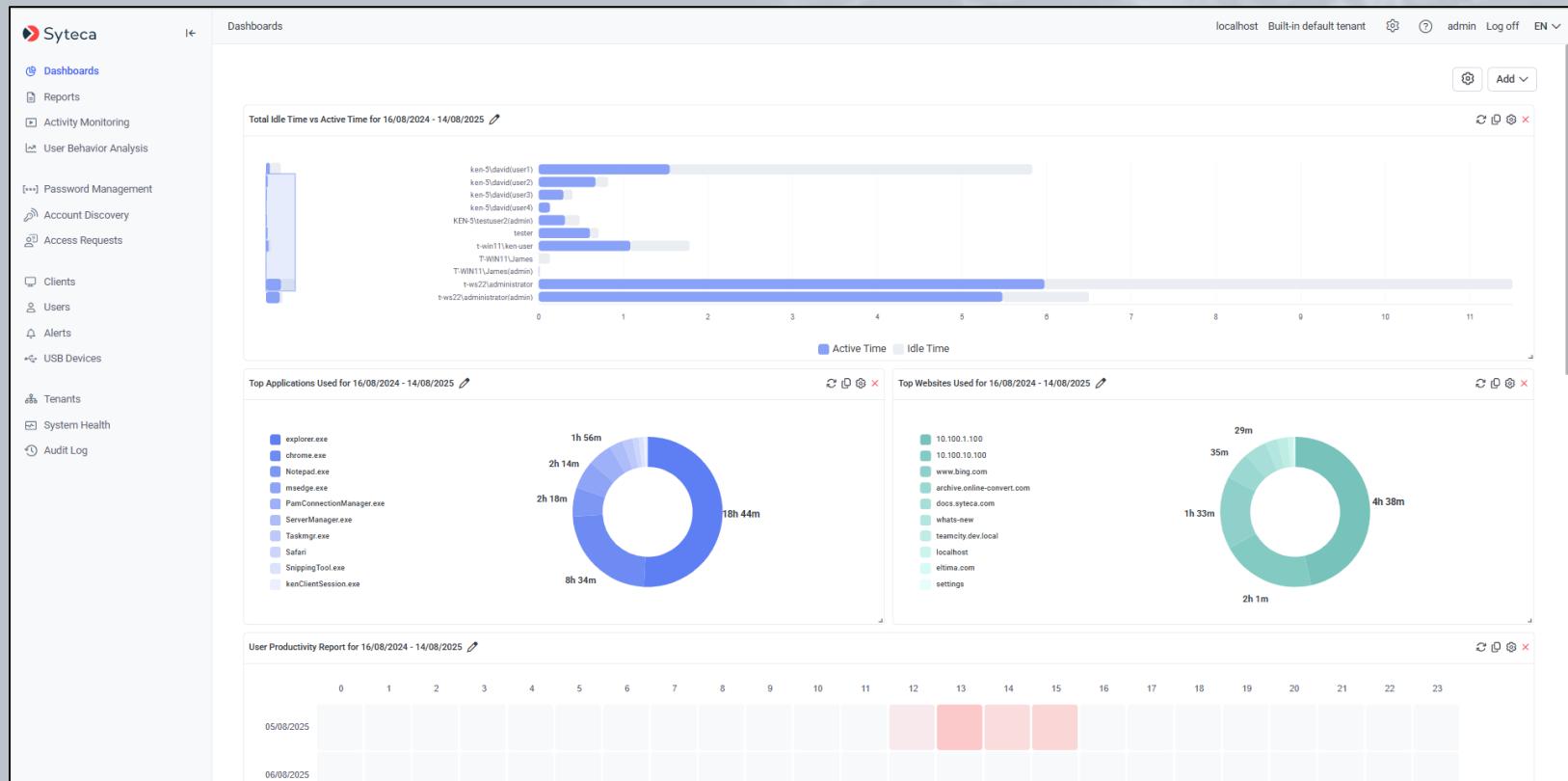
Syteca Application Server & the Management Tool

(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.



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.

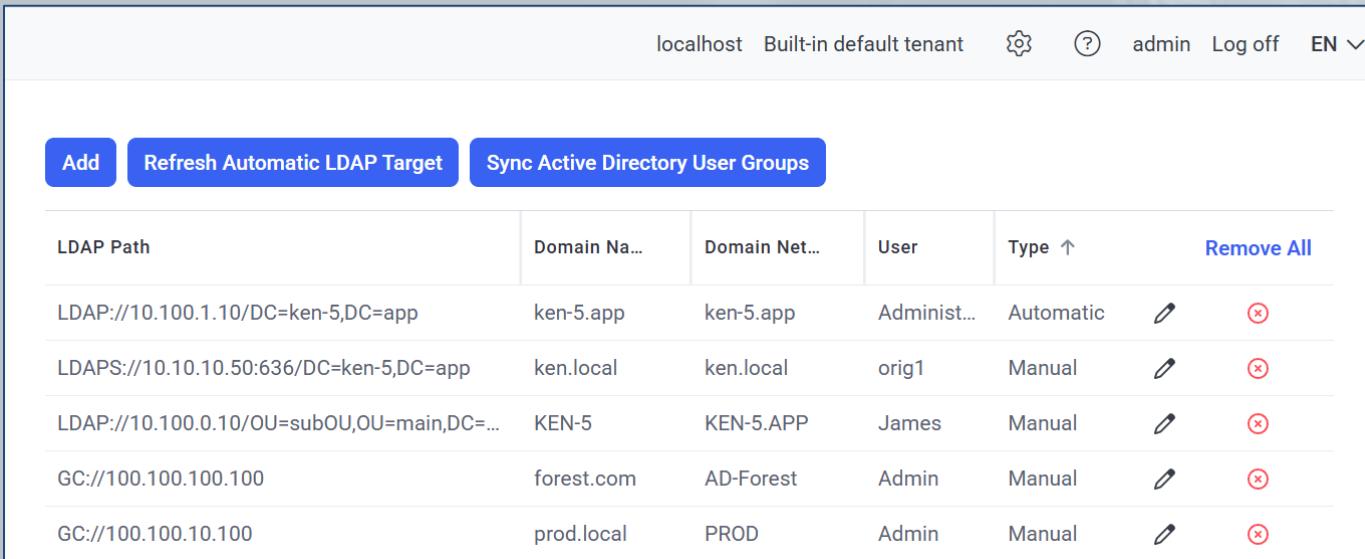
In Multi-Tenant mode, all tenant **users** have access to their tenant Clients, but **do not have access to other tenants' Clients, configurations, alerts, reports, etc.**

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

Tenants				localhost	Built-in default tenant			david	Log off	EN
Tenant Name	Tenant Admin	Description	Tenant Key							
Built-in default tenant	admin	Auto-generated admin account	90807A A7DE-AC							
Tenant1	ken-5.app\david	Non-default Tenant1	DC641E A990-4C							
testDavid	ken-5.app\Domain Admins		9A118E 9950-8,							

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 be 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), as well as **Organizational Units (OUs)** and **LDAP over SSL (LDAPS)**.



LDAP Path	Domain Na...	Domain Net...	User	Type	Remove All
LDAP://10.100.1.10/DC=ken-5,DC=app	ken-5.app	ken-5.app	Administrist...	Automatic	 
LDAPS://10.10.10.50:636/DC=ken-5,DC=app	ken.local	ken.local	orig1	Manual	 
LDAP://10.100.0.10/OU=subOU,OU=main,DC=...	KEN-5	KEN-5.APP	James	Manual	 
GC://100.100.100.100	forest.com	AD-Forest	Admin	Manual	 
GC://100.100.10.100	prod.local	PROD	Admin	Manual	 

Edit LDAP Target

Enter the LDAP path, NetBIOS name, and domain user credentials to connect to the domain. The LDAP path must be defined as follows: LDAP://<Domain Controller name or IP address>/DC=<Domain name>,DC=<Suffix>. e.g. for the test.app.local domain with the SytecaAPP domain controller, define: LDAP://SytecaAPP/DC=test,DC=app,DC=local

LDAP Path

Domain NetBIOS Name

Enter credentials manually

User

Password

Test connection

The account stored in the secret will be used to connect to the Active Directory domain.

Use secret

Select...

Cancel Save

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

The account stored in the secret will be used to connect to the Active Directory domain.

Use secret

Select...

+ Add Secret

- AD acc 1 user
- AD acc 3 testuser2
- Onboarded user1
- WPM test secret

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.

Adding New User

User Type **User Details** User Groups Administrative Permissions Client Access

Active Directory User Details

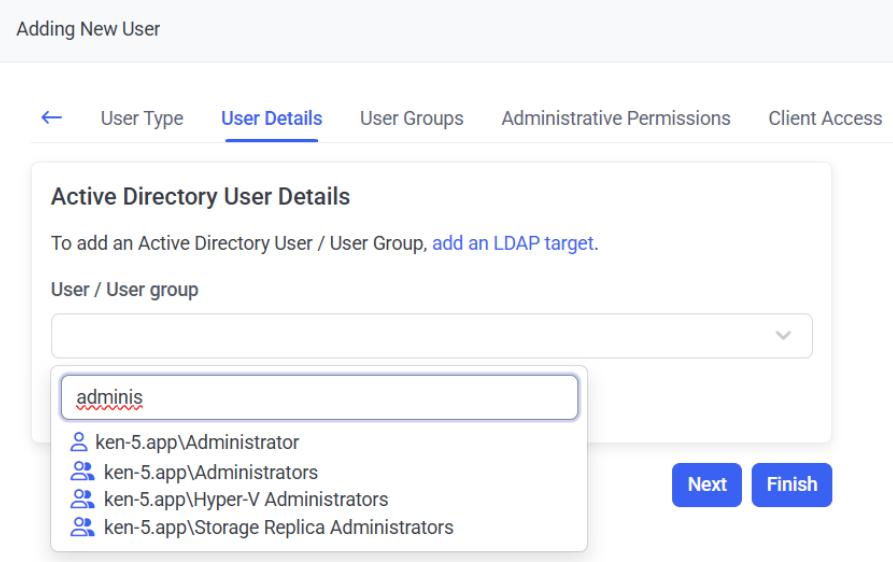
To add an Active Directory User / User Group, [add an LDAP target](#).

User / User group

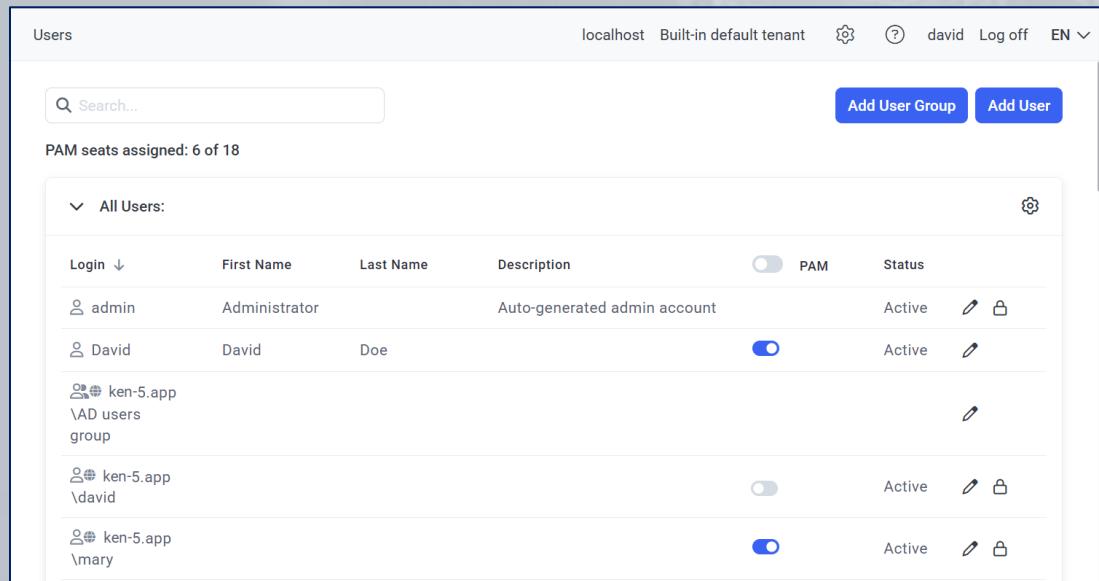
adminis

ken-5.app\Administrator
ken-5.app\Administrators
ken-5.app\Hyper-V Administrators
ken-5.app\Storage Replica Administrators

Next Finish



- 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).

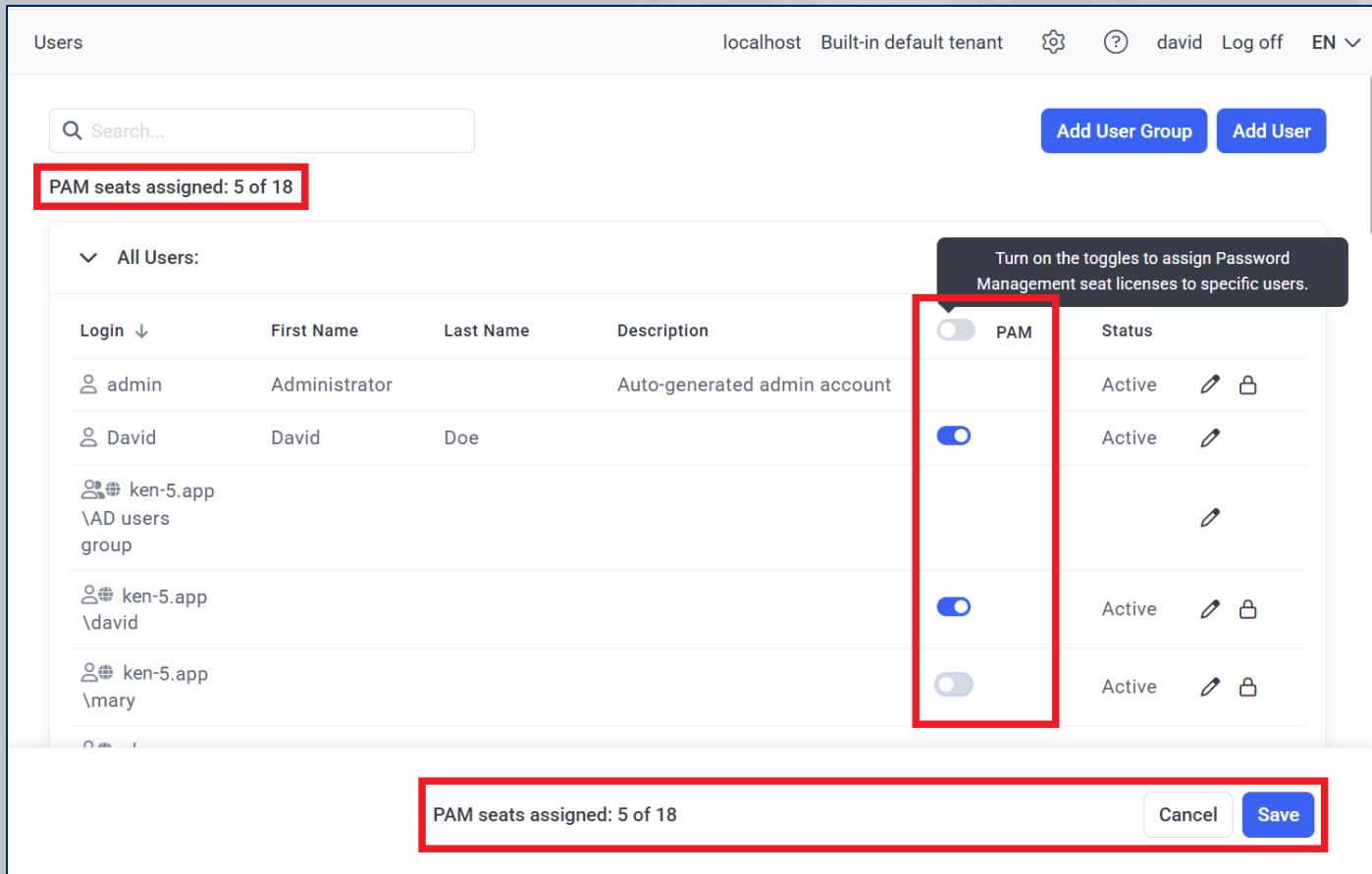


The screenshot shows the Syteca User Management interface. At the top, there is a header with the title 'Users', the URL 'localhost', the tenant name 'Built-in default tenant', and various navigation links. Below the header, there is a search bar with the placeholder 'Search...' and two buttons: 'Add User Group' and 'Add User'. The main content area displays a table of users and groups. The table has columns for 'Login', 'First Name', 'Last Name', 'Description', 'PAM' (a toggle switch), and 'Status'. There are also edit and delete icons for each row. The data in the table is as follows:

Login	First Name	Last Name	Description	PAM	Status
admin	Administrator		Auto-generated admin account	<input type="checkbox"/>	Active
David	David	Doe		<input checked="" type="checkbox"/>	Active
ken-5.app\\AD users group				<input type="checkbox"/>	
ken-5.app\\david				<input type="checkbox"/>	Active
ken-5.app\\mary				<input checked="" type="checkbox"/>	Active

Assign PAM Licenses to Users

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



The screenshot shows the Syteca 'Users' page. At the top, there is a search bar and buttons for 'Add User Group' and 'Add User'. A message 'PAM seats assigned: 5 of 18' is displayed. Below this, a section titled 'All Users:' lists several users with their details: Login, First Name, Last Name, and Description. To the right of the list, a modal window is open, titled 'Turn on the toggles to assign Password Management seat licenses to specific users.' It contains a table with columns 'PAM' (with a toggle switch), 'Status' (Active), and edit/cancel icons. The 'PAM' column for the first four users is highlighted with a red box. At the bottom of the modal, the message 'PAM seats assigned: 5 of 18' is shown again, along with 'Cancel' and 'Save' buttons.

PAM	Status
<input checked="" type="checkbox"/>	Active
<input checked="" type="checkbox"/>	Active
<input checked="" type="checkbox"/>	Active
<input type="checkbox"/>	Active

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

Audit Log						
						localhost Built-in default tenant   david Log off EN 
When  All	Who  All	Action  All	More Criteria 		 Export Filtered Records to CSV  Export Filtered Records to PDF	
Time 	User Name	User Groups	Category	Action	Object	Details
29/07/2025 14:12:22	david	Administ...	Log in / Log off	Log in		IP: 10.100.10.100 User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36
29/07/2025 14:12:10	admin	Administ...	Log in / Log off	Log off		User Log Off from MT
29/07/2025 14:12:07	admin	Administ...	User management	2FA disabled for ...	David	Two-factor authentication was disabled for the user account
29/07/2025 14:10:08	admin	Administ...	Log in / Log off	Log in		IP: 10.100.10.100 User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36
29/07/2025 14:08:22	admin	Administ...	Log in / Log off	Log off		User Log Off from MT
29/07/2025 14:08:05	admin	Administ...	User management	Unassigning Pas...	ken-5.app\pa...	
29/07/2025 14:08:05	admin	Administ...	User management	Assigning Pass...	David	

Database Management

Default Configuration



Binary &
metadata in DB

MS SQL



Binary &
metadata in DB

PostgreSQL
Starting with 6.3



Metadata
in DB



Binary files
in the same folder

Firebird (free)

Custom Configuration

(Firebird, MS SQL, or PostgreSQL)



Metadata
in DB



Binary files in a binary
system folder including
NAS

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

Auto-Cleanup Options

Never
 Run once
 Repeat according to schedule

Perform every (days)
30

Start at
00:00:00 

Action type
Archive & Cleanup 

Sessions older than (days)
30

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

Auto-Cleanup Options

Never
 Run once
 Repeat according to schedule

Action type
 Archive & Cleanup

Sessions older than (days)
30

Archive Parameters

Instance
10.100.10.100

Archived Database Name
ArchivedDB-1

User
sa

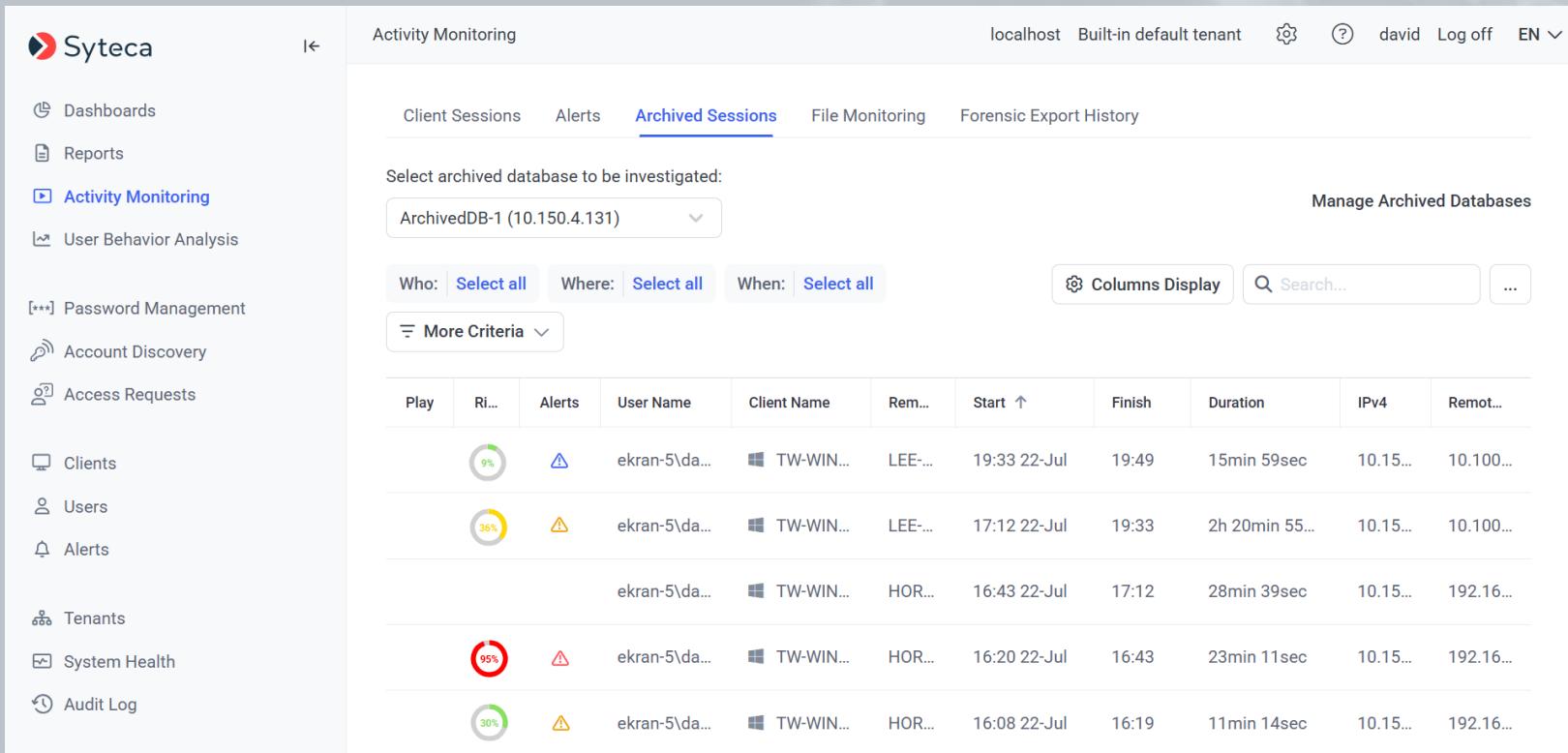
Password
.....

Shrink database transaction log after cleanup
 Delete offline Clients without sessions

NOTE: Leave the User and Password fields blank for authentication with a gMSA/sMSA account.



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**.

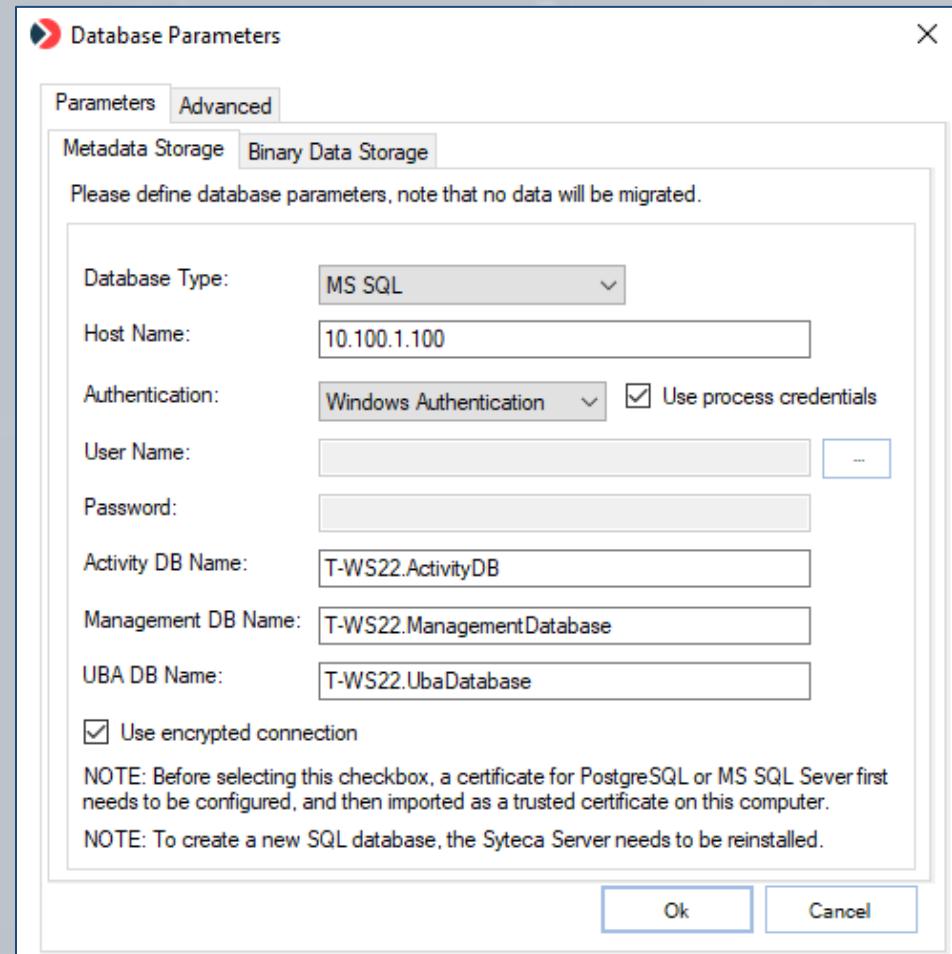


The screenshot shows the Syteca Activity Monitoring interface. The left sidebar contains navigation links: Dashboards, Reports, Activity Monitoring (which is selected and highlighted in blue), User Behavior Analysis, Password Management, Account Discovery, Access Requests, Clients, Users, Alerts, Tenants, System Health, and Audit Log. The main content area is titled 'Activity Monitoring' and shows 'Archived Sessions' as the active tab. It includes tabs for Client Sessions, Alerts, Archived Sessions, File Monitoring, and Forensic Export History. A dropdown menu 'Select archived database to be investigated' is set to 'ArchivedDB-1 (10.150.4.131)'. A 'Manage Archived Databases' button is available. Below these are filters for 'Who', 'Where', and 'When', and buttons for 'Columns Display' and 'Search...'. A 'More Criteria' button is also present. The main table lists sessions with columns: Play, Ri..., Alerts, User Name, Client Name, Rem..., Start ↑, Finish, Duration, IPv4, and Remot... (partially visible). The table contains five rows of session data, each with a progress bar icon and a status icon (green, yellow, or red).

Play	Ri...	Alerts	User Name	Client Name	Rem...	Start ↑	Finish	Duration	IPv4	Remot...
9%	▲	ekran-5\da...	TW-WIN...	LEE...	19:33 22-Jul	19:49	15min 59sec	10.15...	10.100...	
36%	⚠	ekran-5\da...	TW-WIN...	LEE...	17:12 22-Jul	19:33	2h 20min 55...	10.15...	10.100...	
		ekran-5\da...	TW-WIN...	HOR...	16:43 22-Jul	17:12	28min 39sec	10.15...	192.16...	
95%	⚠	ekran-5\da...	TW-WIN...	HOR...	16:20 22-Jul	16:43	23min 11sec	10.15...	192.16...	
30%	⚠	ekran-5\da...	TW-WIN...	HOR...	16:08 22-Jul	16:19	11min 14sec	10.15...	192.16...	

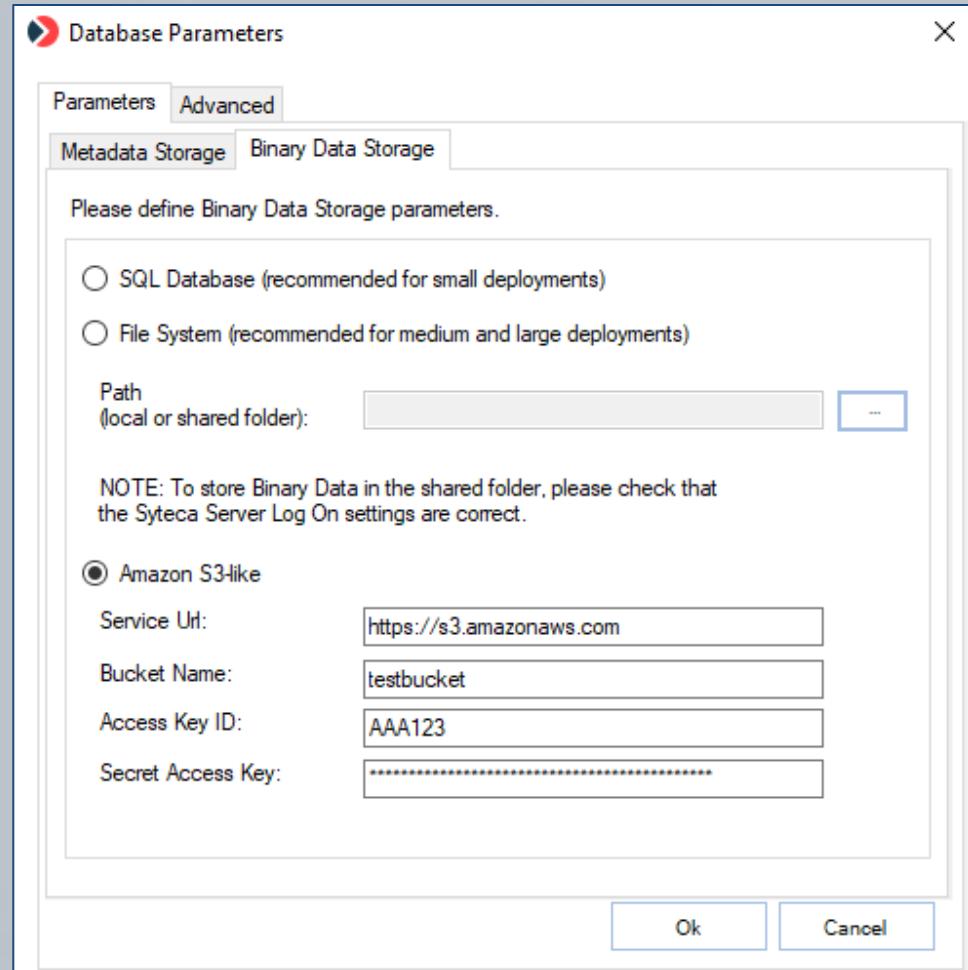
If the **database credentials** defined during installation of the Application Server need to be changed, you can easily **edit them** without reinstalling the Application Server.

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.

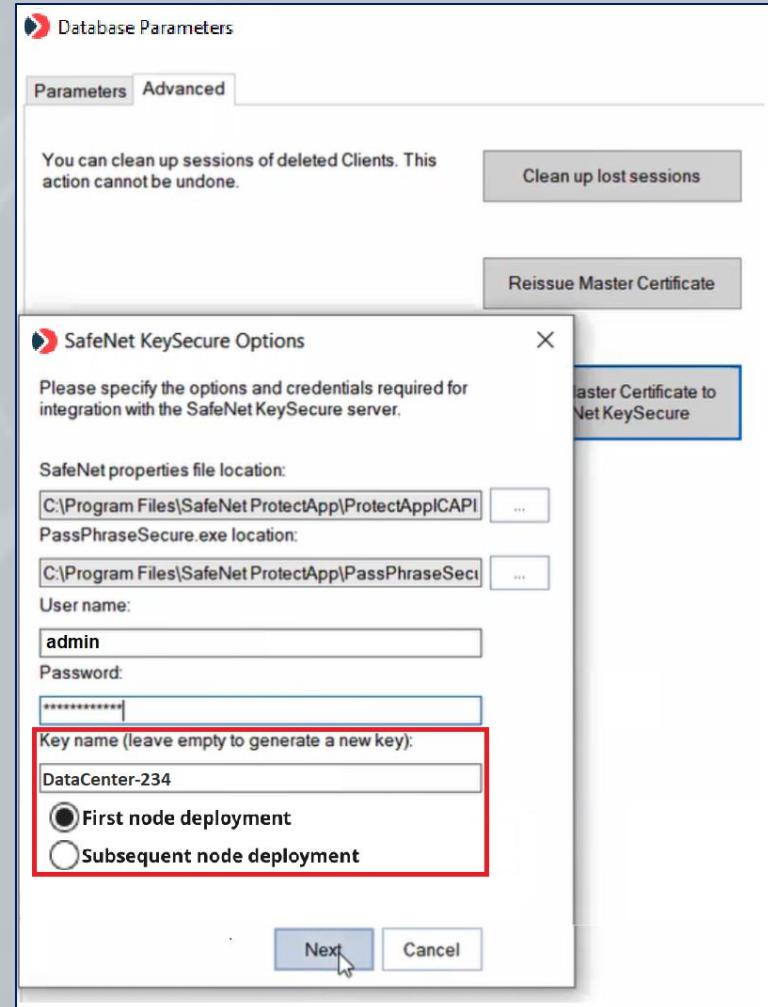


A **new location** (e.g. **Amazon S3** storage) can alternatively be used to **store the binary data** (i.e. screen captures) recorded during monitoring.

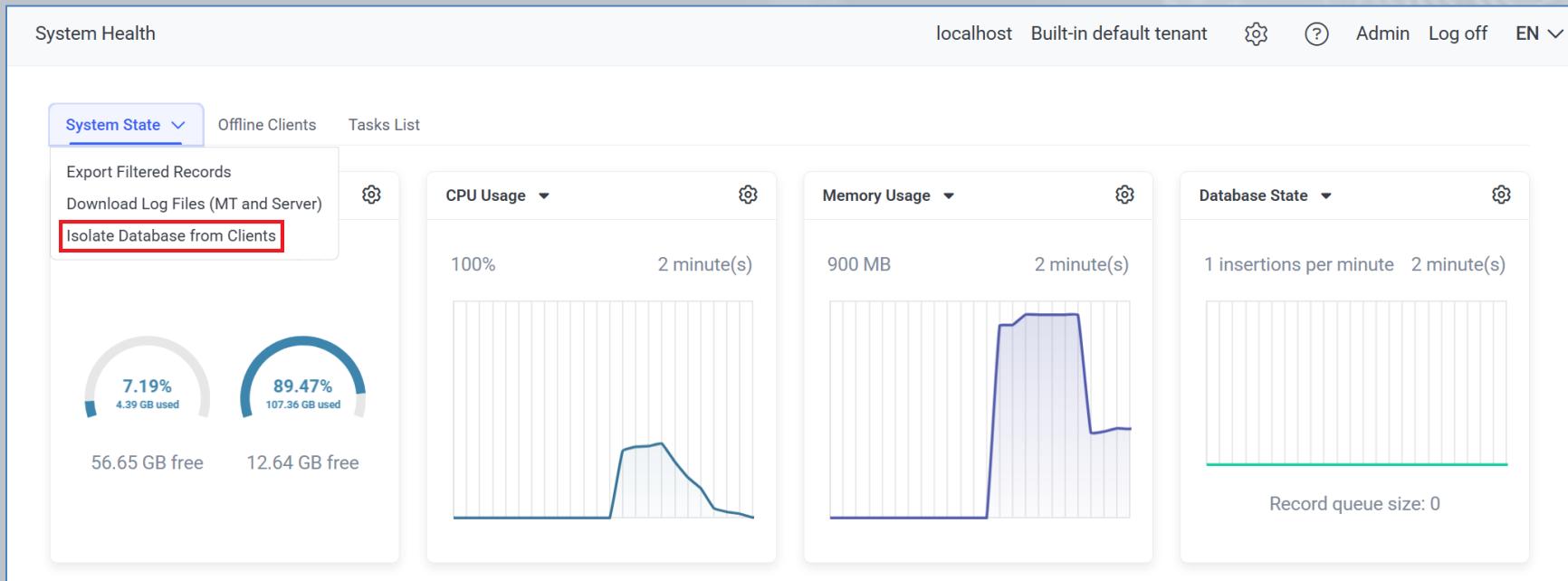
Network-Attached Storage (NAS) can also be used (by using the **File System** option).



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**.



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**.



The screenshot shows the Syteca System Health dashboard. At the top, there are navigation links: 'localhost', 'Built-in default tenant', a gear icon, a question mark icon, 'Admin', 'Log off', and a language selector 'EN'. Below the navigation, there are four main monitoring panels: 'System State', 'CPU Usage', 'Memory Usage', and 'Database State'. The 'System State' panel has a sub-menu with options: 'Export Filtered Records', 'Download Log Files (MT and Server)', and 'Isolate Database from Clients', with the last option highlighted by a red box. Below this are two disk usage charts: one for '7.19%' (4.39 GB used) and one for '89.47%' (107.36 GB used). The 'CPU Usage' panel shows 100% usage over a 2-minute period. The 'Memory Usage' panel shows 900 MB usage over a 2-minute period. The 'Database State' panel shows 1 insertion per minute over a 2-minute period and a 'Record queue size: 0' status.

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

Editing Client (T-WIN11)

← Client Settings Client Groups Permissions Assigned Alerts

Change the Settings Type to Custom to edit the Client.

Properties User Activity Recording Monitoring [Windows/macOS] Application Filtering
Authentication Options Keystroke Monitoring Additional Options Privacy Settings

Monitoring Parameters

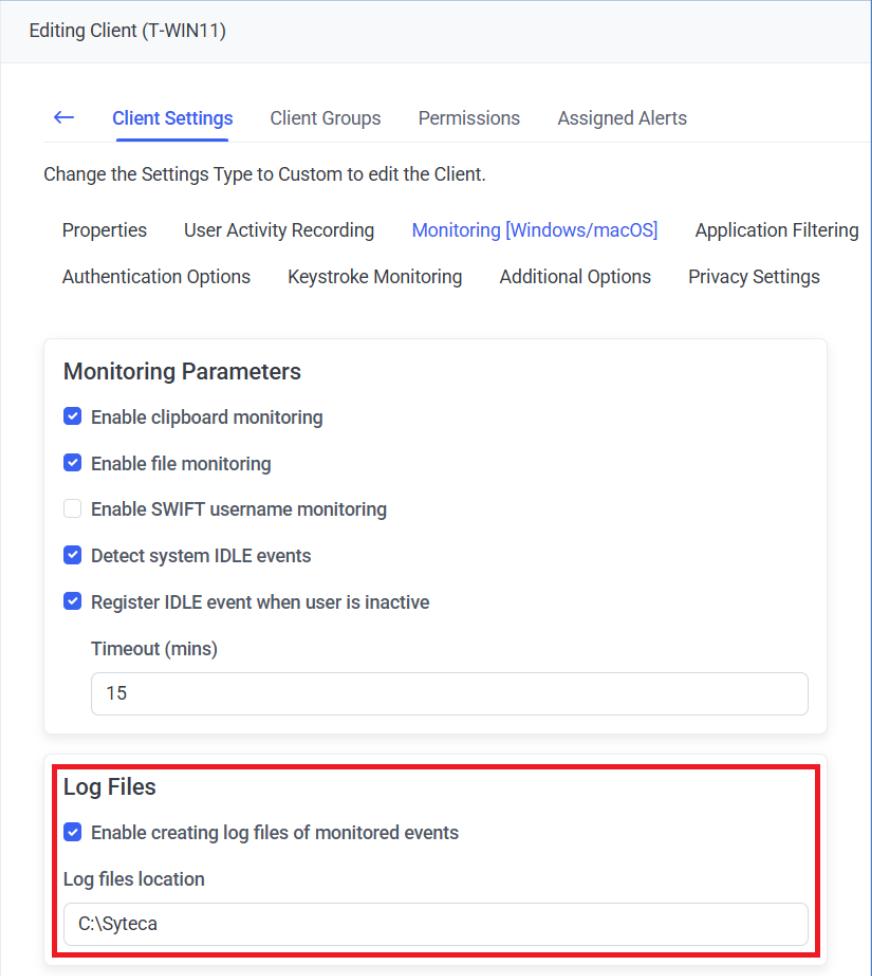
Enable clipboard monitoring
 Enable file monitoring
 Enable SWIFT username monitoring
 Detect system IDLE events
 Register IDLE event when user is inactive

Timeout (mins)
15

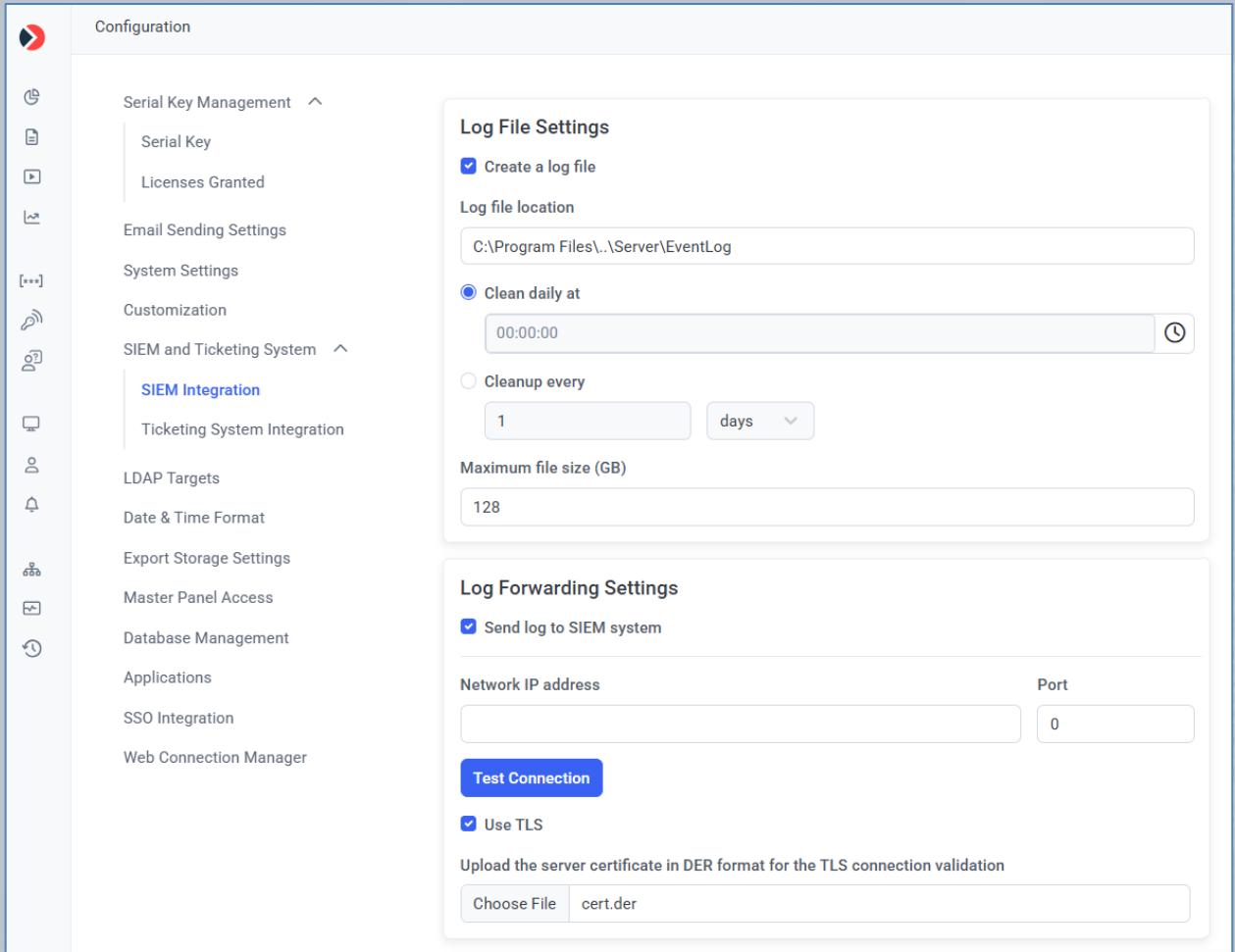
Log Files

Enable creating log files of monitored events

Log files location
C:\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.



The screenshot shows the Syteca Configuration interface with the following details:

- Left Sidebar:** Shows various configuration categories: Serial Key Management (Serial Key, Licenses Granted), Email Sending Settings, System Settings, Customization, SIEM and Ticketing System (SIEM Integration, Ticketing System Integration), LDAP Targets, Date & Time Format, Export Storage Settings, Master Panel Access, Database Management, Applications, SSO Integration, and Web Connection Manager.
- Right Panel - Log File Settings:**
 - Create a log file
 - Log file location: C:\Program Files\..\\Server\EventLog
 - Clean daily at: 00:00:00
 - Cleanup every: 1 days
 - Maximum file size (GB): 128
- Right Panel - Log Forwarding Settings:**
 - Send log to SIEM system
 - Network IP address: (empty)
 - Port: 0
 - Test Connection** button
 - Use TLS
 - Upload the server certificate in DER format for the TLS connection validation:
 - Choose File: cert.der

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)

localhost

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

Choose File cert.der

Log Format Settings

Log format

CEF log

Date Format

MMM dd yyyy HH:mm:ss

Log File Contents

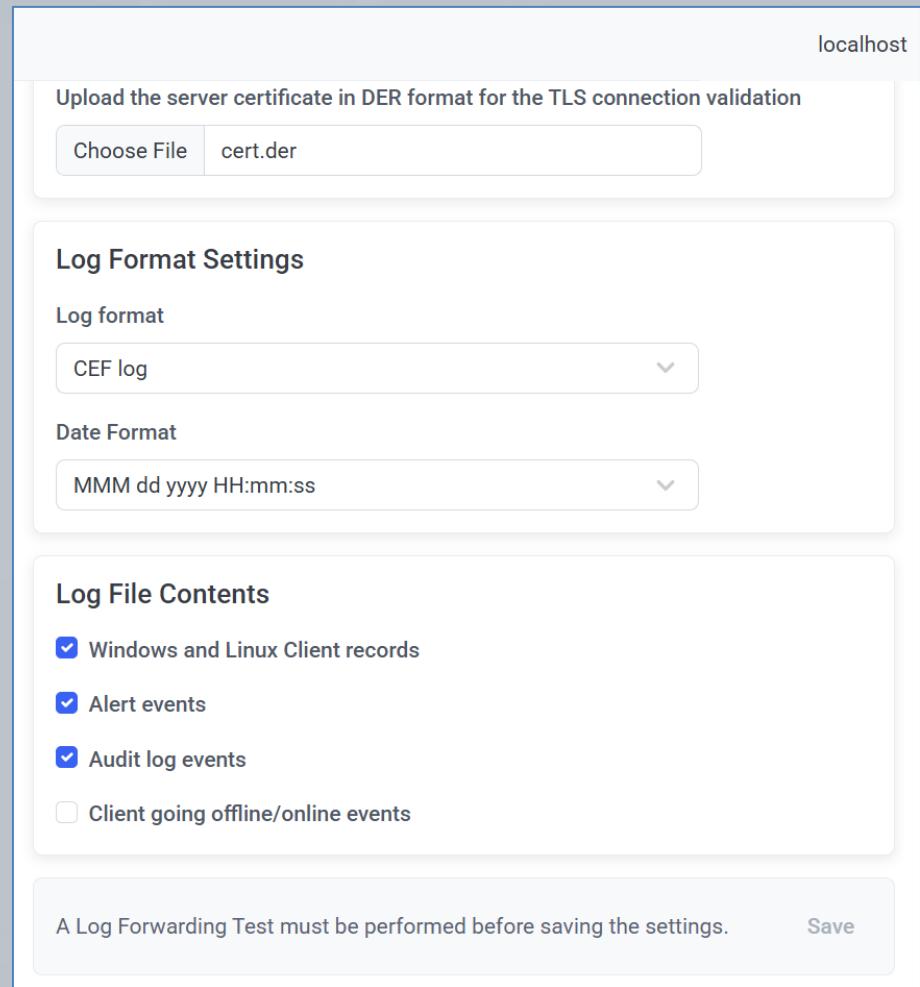
Windows and Linux Client records

Alert events

Audit log events

Client going offline/online events

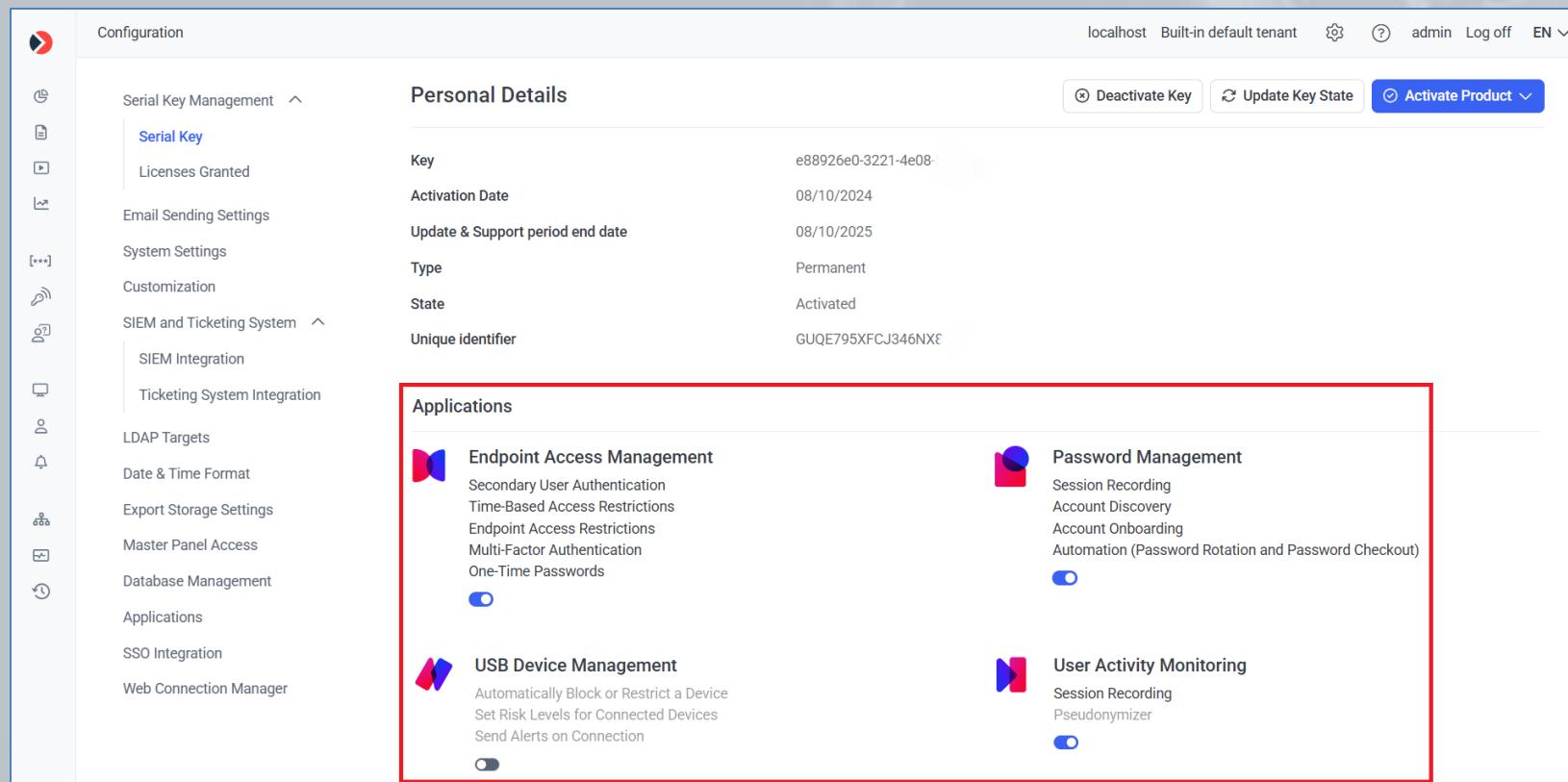
A Log Forwarding Test must be performed before saving the settings. Save



Licensing

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

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



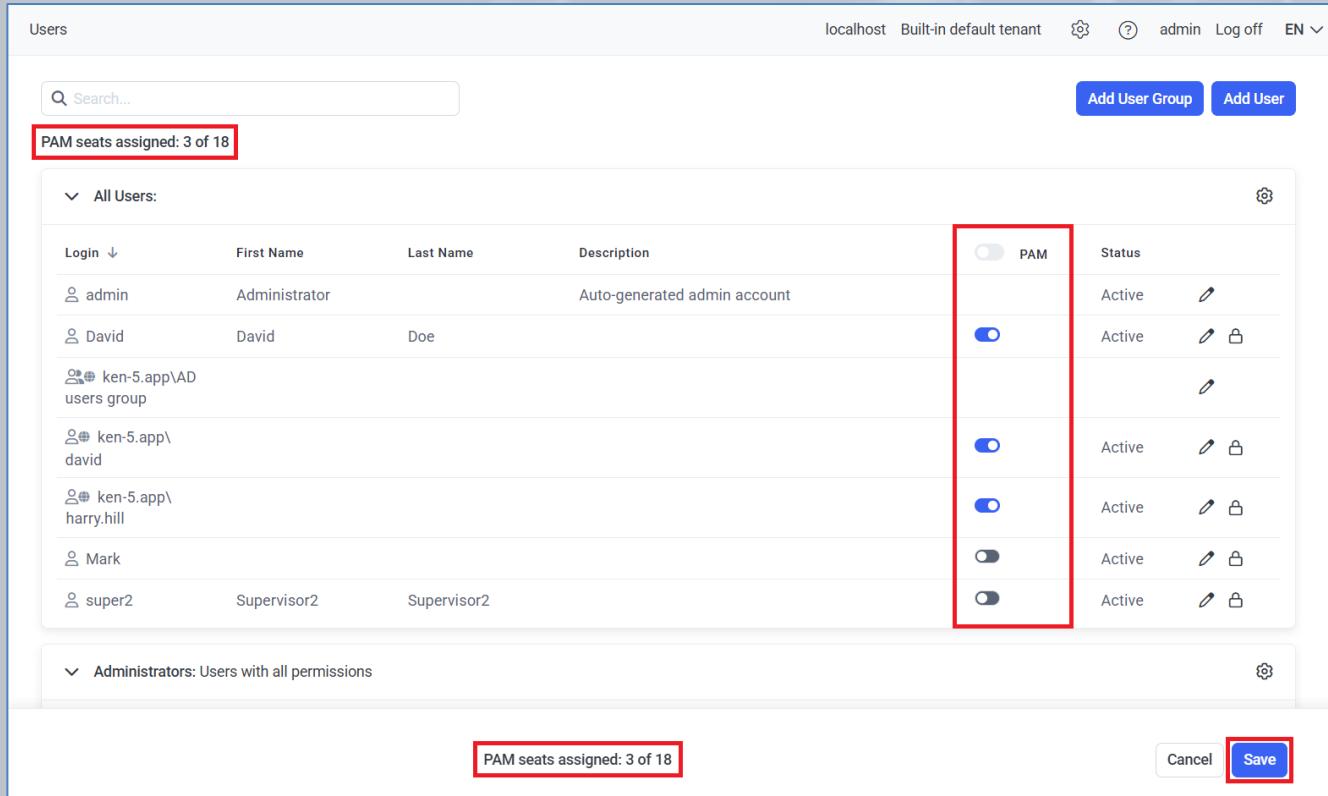
The screenshot shows the Syteca Configuration interface. On the left is a sidebar with various icons and menu items. The main area is titled "Personal Details" and shows a table of key information. Below this is a section titled "Applications" which is highlighted with a red box. The "Applications" section contains four items, each with a icon and a list of features. The items are: "Endpoint Access Management" (with icons for a user and a lock), "USB Device Management" (with icons for a drive and a device), "Password Management" (with icons for a lock and a user), and "User Activity Monitoring" (with icons for a play button and a user). Each application section has a toggle switch at the bottom.

Personal Details	
Key	e88926e0-3221-4e08-
Activation Date	08/10/2024
Update & Support period end date	08/10/2025
Type	Permanent
State	Activated
Unique identifier	GUQE795XFCJ346NXE

Applications	
 Endpoint Access Management	 Secondary User Authentication Time-Based Access Restrictions Endpoint Access Restrictions Multi-Factor Authentication One-Time Passwords <input checked="" type="checkbox"/>
 USB Device Management	 Automatically Block or Restrict a Device Set Risk Levels for Connected Devices Send Alerts on Connection <input checked="" type="checkbox"/>
 Password Management	 Session Recording Account Discovery Account Onboarding Automation (Password Rotation and Password Checkout) <input checked="" type="checkbox"/>
 User Activity Monitoring	 Session Recording Pseudonymizer <input checked="" type="checkbox"/>

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.



The screenshot shows the Syteca web interface for managing users. The top navigation bar includes 'localhost', 'Built-in default tenant', a gear icon, 'admin', 'Log off', and language 'EN'. Below the navigation is a search bar and buttons for 'Add User Group' and 'Add User'.

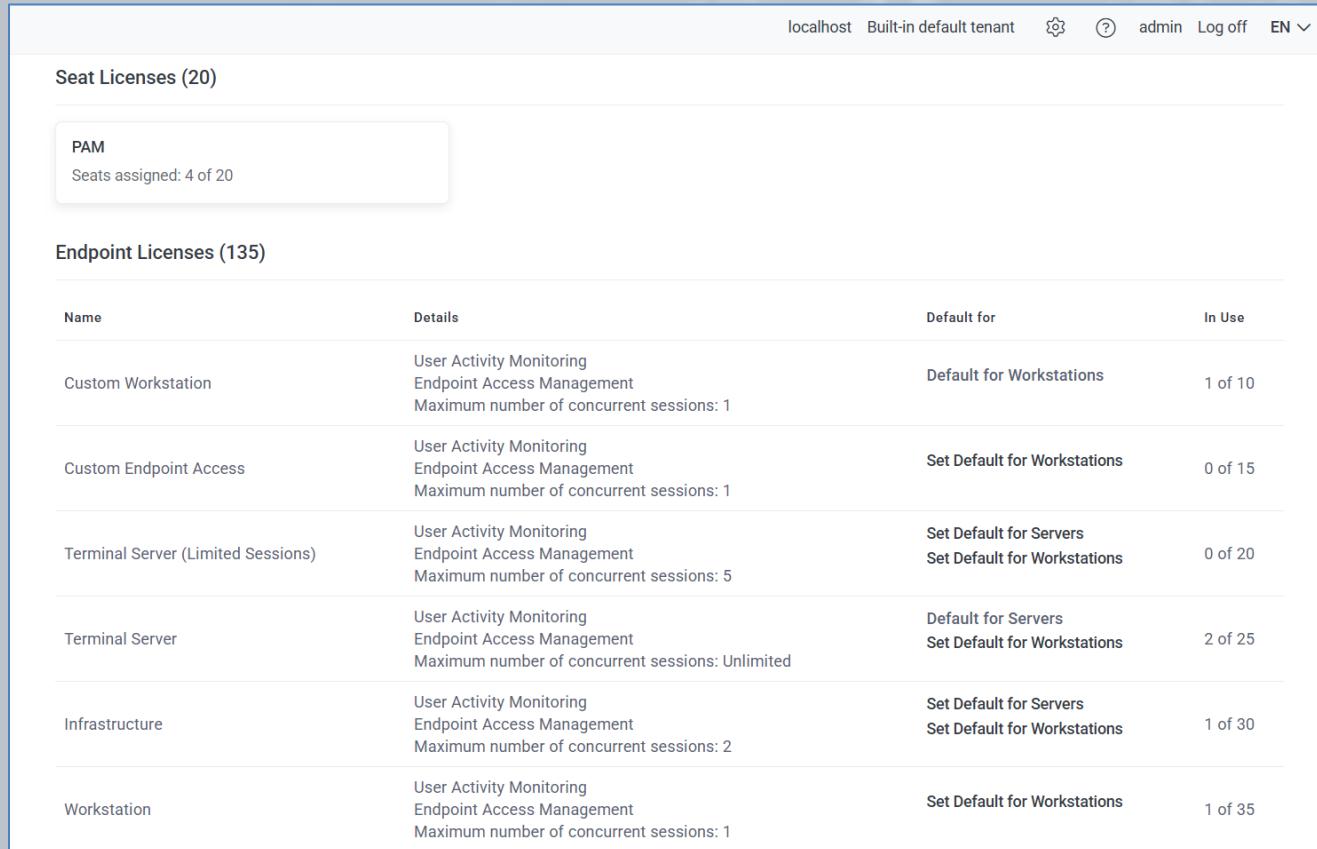
The main content area is titled 'Users' and shows a table of users. The table has columns: Login, First Name, Last Name, Description, and Status. The 'Status' column includes edit and delete icons. To the left of the table, a dropdown menu shows 'All Users' and 'Administrators: Users with all permissions'. A red box highlights the status column.

A message 'PAM seats assigned: 3 of 18' is displayed above the user table. A red box highlights this message. The user table shows the following data:

Login	First Name	Last Name	Description	Status
admin	Administrator		Auto-generated admin account	Active
David	David	Doe		Active
ken-5.app\AD users group				
ken-5.app\david				
ken-5.app\harry.hill				
Mark				
super2	Supervisor2	Supervisor2		

Below the user table, another message 'PAM seats assigned: 3 of 18' is highlighted with a red box. At the bottom right are 'Cancel' and 'Save' buttons, with 'Save' highlighted by a red box.

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



The screenshot shows the Syteca interface with the following navigation bar: localhost, Built-in default tenant, 🌐, 🎪, admin, Log off, EN. The main content area displays two sections: 'Seat Licenses (20)' and 'Endpoint Licenses (135)'.

Name	Details	Default for	In Use
Custom Workstation	User Activity Monitoring Endpoint Access Management Maximum number of concurrent sessions: 1	Default for Workstations	1 of 10
Custom Endpoint Access	User Activity Monitoring Endpoint Access Management Maximum number of concurrent sessions: 1	Set Default for Workstations	0 of 15
Terminal Server (Limited Sessions)	User Activity Monitoring Endpoint Access Management Maximum number of concurrent sessions: 5	Set Default for Servers Set Default for Workstations	0 of 20
Terminal Server	User Activity Monitoring Endpoint Access Management Maximum number of concurrent sessions: Unlimited	Default for Servers Set Default for Workstations	2 of 25
Infrastructure	User Activity Monitoring Endpoint Access Management Maximum number of concurrent sessions: 2	Set Default for Servers Set Default for Workstations	1 of 30
Workstation	User Activity Monitoring Endpoint Access Management Maximum number of concurrent sessions: 1	Set Default for Workstations	1 of 35

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.

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.

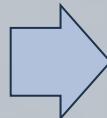
Installing & Updating Clients

Convenient Syteca Client installation:

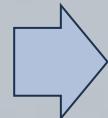
- **Locally:**
 - Windows Clients:
 - using the installation file with **default parameters**.
 - using a package generated with **customized parameters**.
 - macOS or **macOS Hidden/Stealth** Clients (using a tar.gz file).
 - Linux, incl. **SELinux**, **Solaris**, etc (using a tar.gz file).
- **Remotely:**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

Remote Installation

Select computers to install Clients on



Customize installation parameters



The Clients are successfully installed!

Target Computers for Remote Installation



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

Computers without Clients localhost Built-in default tenant

←

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

[Deploy via IP Range](#) [Deploy on Specific Computers](#) [Download Installation File](#)

Computer	Workgroup / Domain	IP	Description	Previous Installation Failure	Remove All
IMACP	WORKGROUP	10.100.10.3			
WIN-AG7	KEN-5	10.100.10.178			

[Read the Installation Prerequisites](#)

[Install](#) [Install Using Existing .ini File](#)

IP Range Scan

Scan finished. 4 computer(s) detected.

IP	Computer	Workgroup / Domain
<input type="checkbox"/> 10.100.10.3	IMACP (10.100.10.3)	WORKGROUP
<input type="checkbox"/> 10.100.10.101	DESKTOP-GF (10.100.10.101)	WORKGROUP
<input type="checkbox"/> 10.100.10.131	T-WS22.ken-5.app (10.100.10.131)	ken-5.app
<input checked="" type="checkbox"/> 10.100.10.178	WIN-AG7 (10.100.10.178)	KEN-5

[Next](#) [Refresh](#) [Stop](#)

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.

Editing Client (TW-WIN11)

← Client Settings Client Groups Permissions Assigned Alerts

Change the Settings Type to Custom to edit the Client.

Properties User Activity Recording Monitoring [Windows/macOS] Application Filtering
Authentication Options Keystroke Monitoring Additional Options Privacy Settings

Client Properties

Description

Assigned license

Custom Workstation

Settings Type

Custom

Client Mode

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

Update Client automatically

Display Client tray icon

A screenshot of the Syteca Client Settings interface. The top navigation bar shows 'Client Settings' is selected. Below it, a note says 'Change the Settings Type to Custom to edit the Client.' There are several tabs: Properties (selected), User Activity Recording, Monitoring [Windows/macOS], Application Filtering, Authentication Options, Keystroke Monitoring, Additional Options, and Privacy Settings. The 'Client Properties' section has a 'Description' field and an 'Assigned license' dropdown set to 'Custom Workstation'. The 'Settings Type' dropdown is set to 'Custom' and is highlighted with a red box. The 'Client Mode' section contains three checkboxes: 'Enable Protected mode', 'Update Client automatically' (which is checked and highlighted with a red box), and 'Display Client tray icon'. A note below 'Enable Protected mode' says 'NOTE: The mode will change after restart of the Client computer.'

Monitoring Parameters

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

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

- 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 upload** monitoring operations.
- **Alerts** triggered (on various user activities).

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.

Editing Client (T-WIN11)

← Client Settings Client Groups Permissions Assigned Alerts

Change the Settings Type to Custom to edit the Client.

Properties User Activity Recording Monitoring [Windows/macOS] Application Filtering
Authentication Options Keystroke Monitoring Additional Options Privacy Settings

Activity Recording Configuration
NOTE: Changes to these settings will not be applied to sessions which are currently active.

Recording Mode:

Full-Motion Capture Interval Capture

NOTE: Some features are not currently supported in Full-Motion Capture mode. [Learn More](#).

Disable offline activity recording

Record user activity periodically

Period (sec)
30

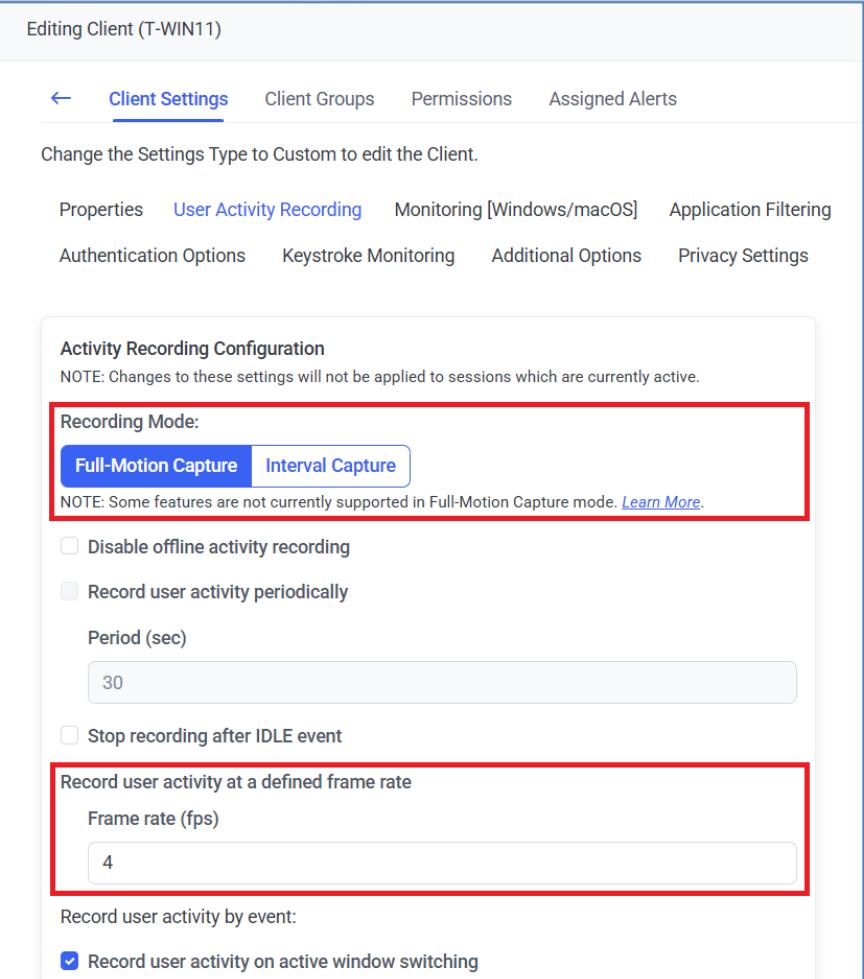
Stop recording after IDLE event

Record user activity at a defined frame rate

Frame rate (fps)
4

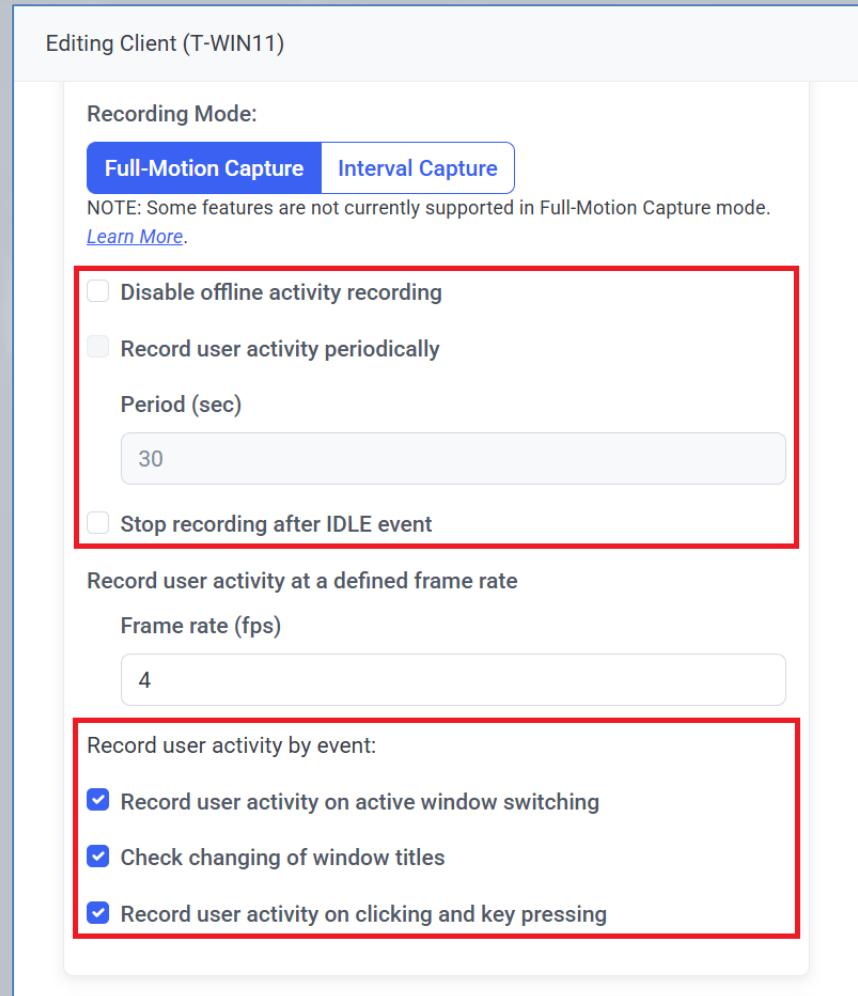
Record user activity by event:

Record user activity on active window switching



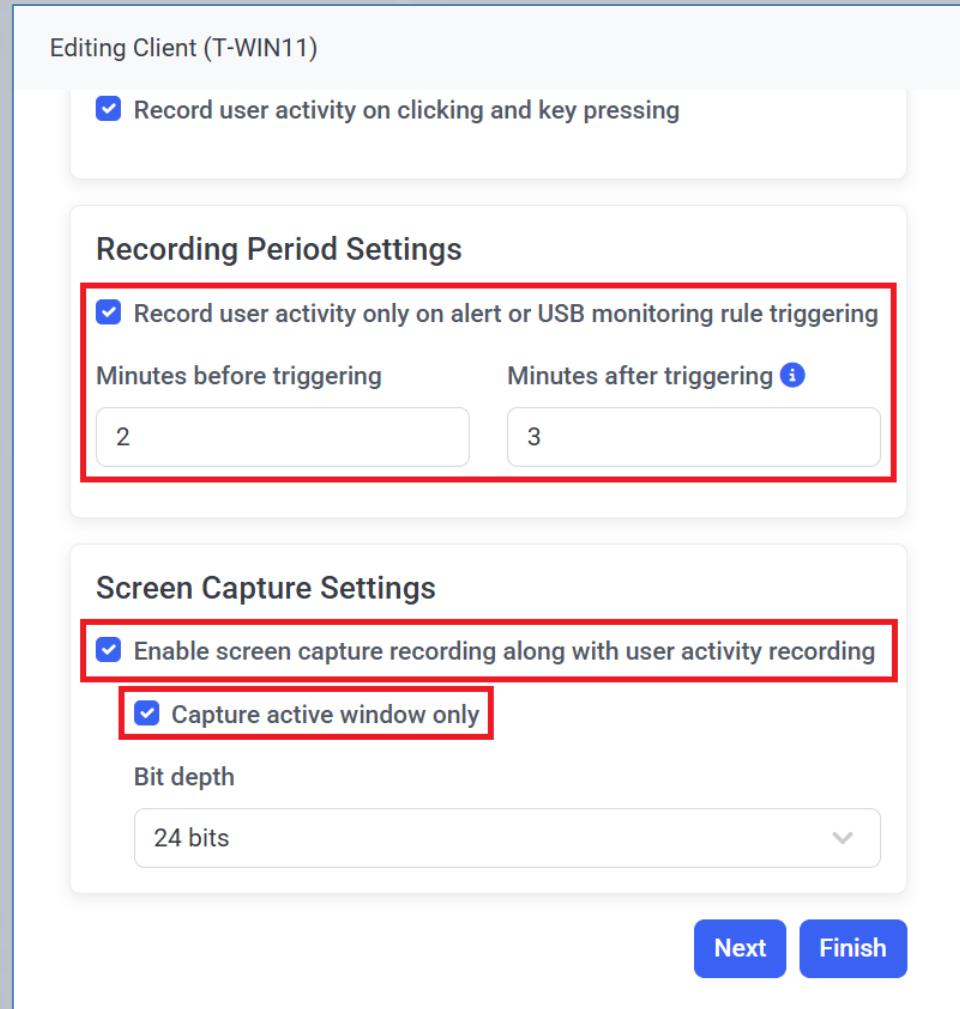
Syteca Client user activity recording is **event-triggered** by default.

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



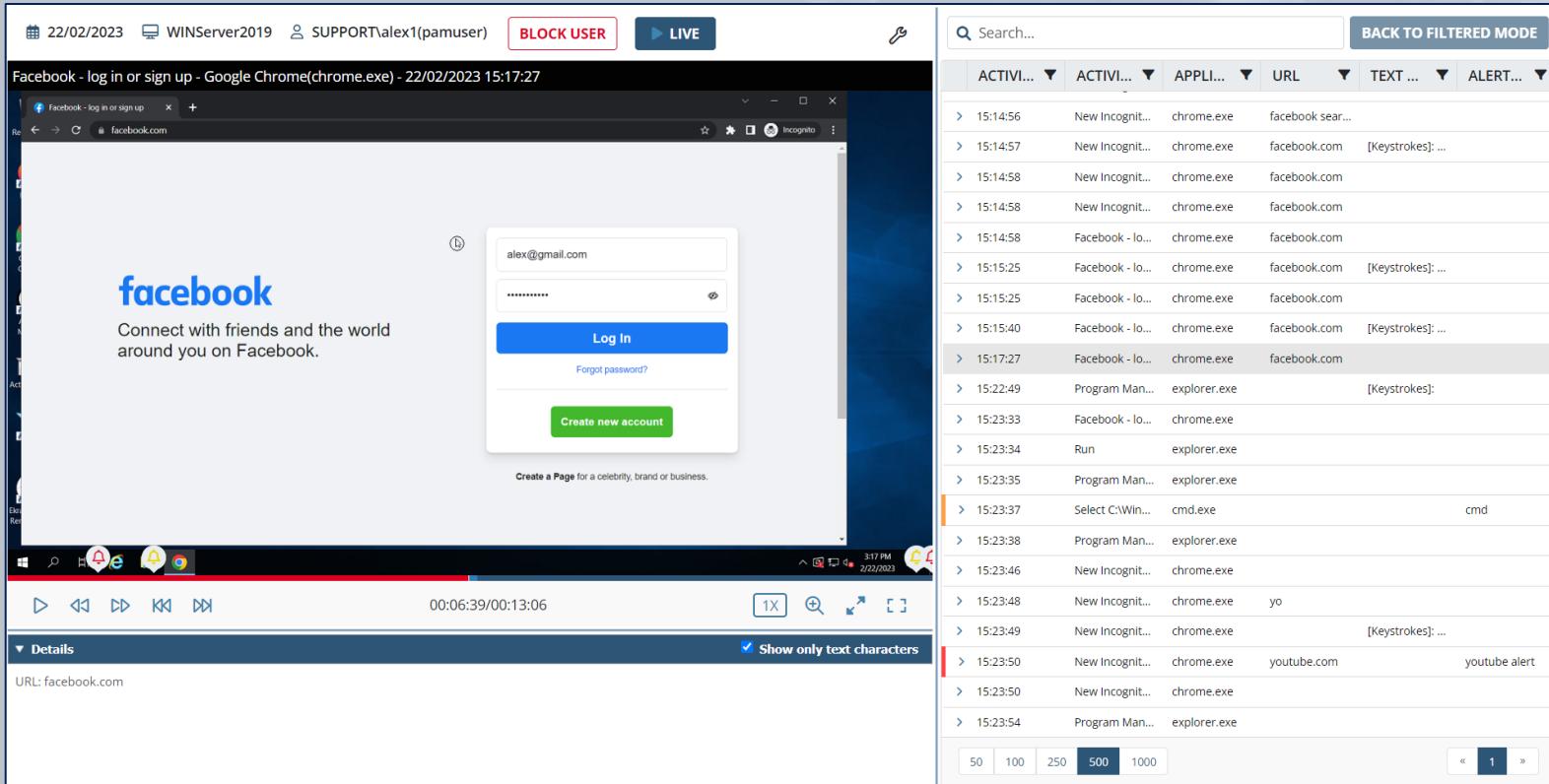
For example, you can configure a Client (or the Clients in a Client group) to:

- **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.**



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

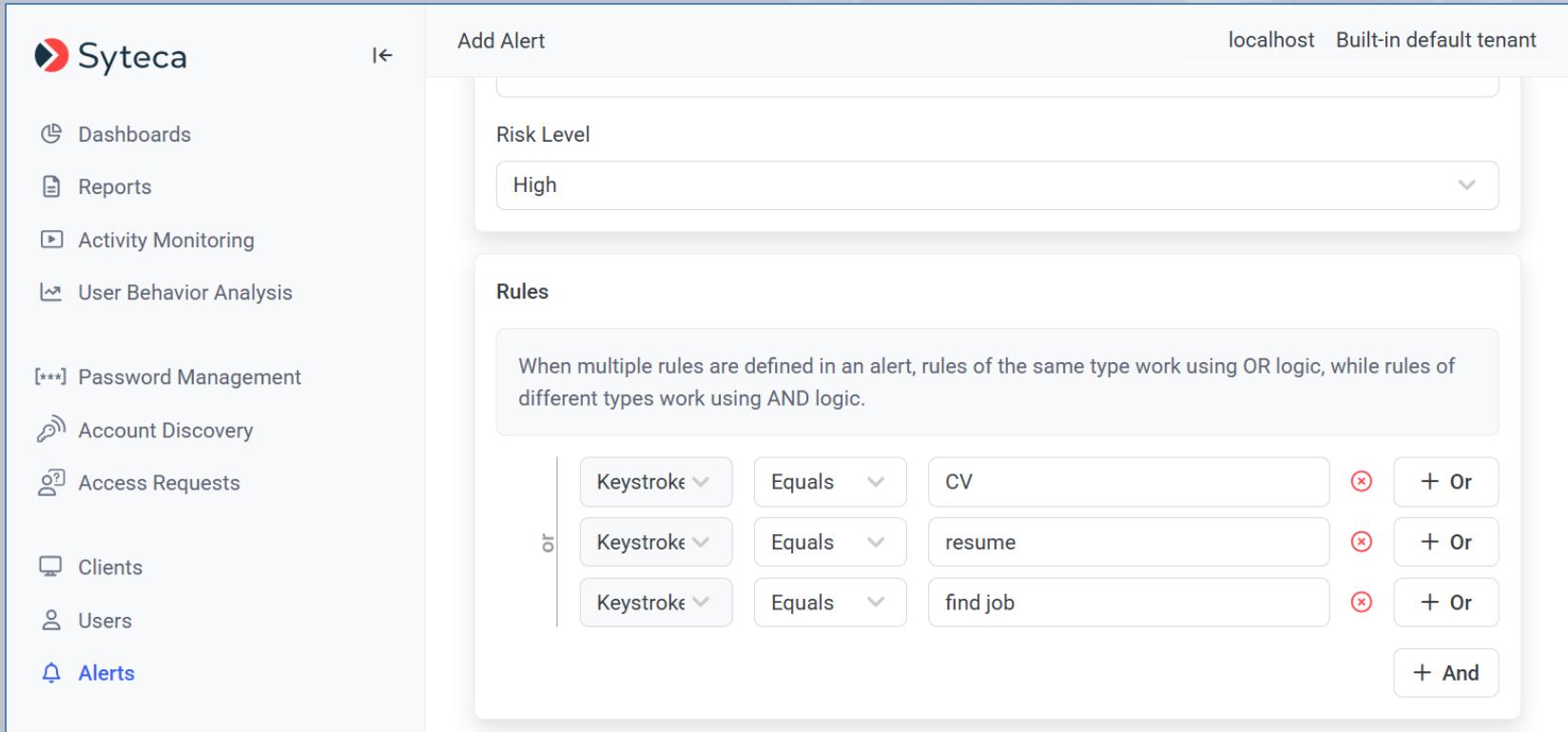
You can configure the Client to monitor either full URLs or top and second level domain names only.



The screenshot shows the Syteca Client interface with the following components:

- Top Bar:** Displays the date (22/02/2023), computer name (WINServer2019), user (SUPPORT\alex1(pamuser)), and a red **BLOCK USER** button.
- Live Monitoring Window:** Shows a screenshot of a Google Chrome browser window displaying the Facebook login page. The URL is `facebook.com`. The Syteca interface overlays a red **LIVE** button and a key icon.
- Log Table:** A detailed log of monitored activities. The columns are: ACTIVI..., ACTIVI..., APPLI..., URL, TEXT ..., and ALERT The log entries include:
 - 15:14:56 New Incognit... chrome.exe facebook.sear...
 - 15:14:57 New Incognit... chrome.exe facebook.com [Keystrokes]: ...
 - 15:14:58 New Incognit... chrome.exe facebook.com
 - 15:14:58 Facebook - lo... chrome.exe facebook.com
 - 15:15:25 Facebook - lo... chrome.exe facebook.com [Keystrokes]: ...
 - 15:15:25 Facebook - lo... chrome.exe facebook.com
 - 15:15:40 Facebook - lo... chrome.exe facebook.com [Keystrokes]: ...
 - 15:17:27 Facebook - lo... chrome.exe facebook.com
 - 15:22:49 Program Man... explorer.exe [Keystrokes]: ...
 - 15:23:33 Facebook - lo... chrome.exe
 - 15:23:34 Run explorer.exe
 - 15:23:35 Program Man... explorer.exe
 - 15:23:37 Select C:\Win... cmd.exe cmd
 - 15:23:38 Program Man... explorer.exe
 - 15:23:46 New Incognit... chrome.exe
 - 15:23:48 New Incognit... chrome.exe yo
 - 15:23:49 New Incognit... chrome.exe [Keystrokes]: ...
 - 15:23:50 New Incognit... chrome.exe youtube.com youtube alert
 - 15:23:50 New Incognit... chrome.exe
 - 15:23:54 Program Man... explorer.exe
- Bottom Panel:** Includes a "Details" section showing the URL `facebook.com` and a checkbox for "Show only text characters". It also features a toolbar with various icons and a page navigation bar with buttons for 50, 100, 250, 500, and 1000.

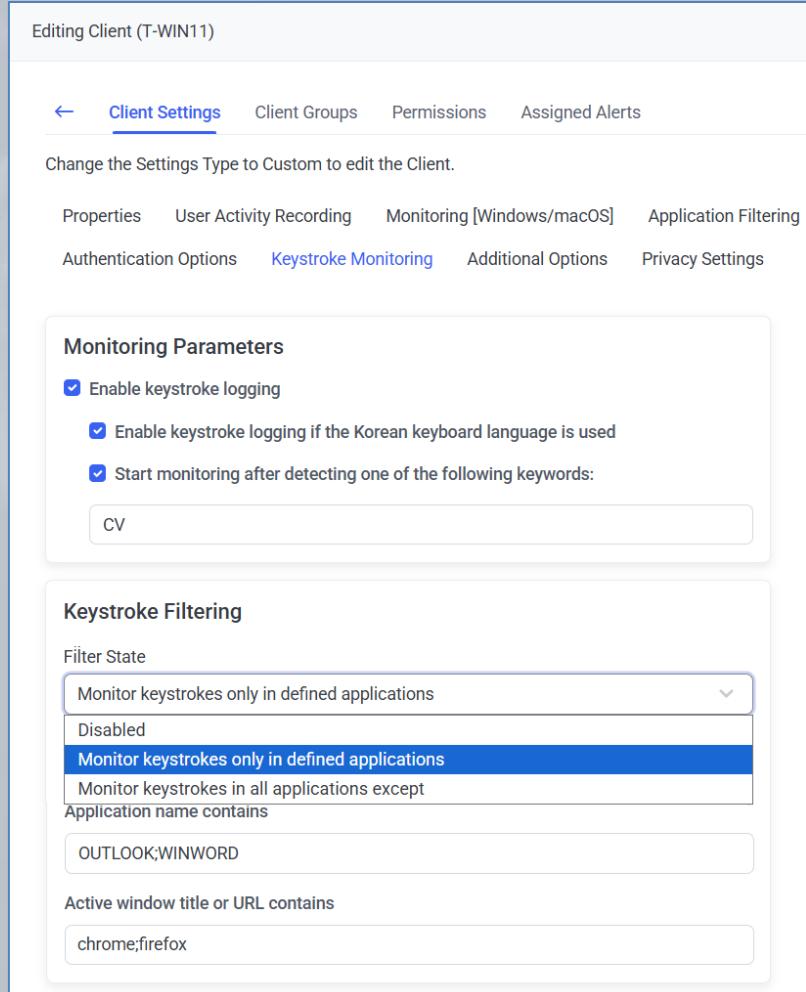
To ensure **compliance** (e.g. with GDPR), **all keystrokes logged are hidden**, but you can **perform searches** on them and **create alerts** to be triggered when specific keywords are typed.



The screenshot shows the Syteca interface for creating a new alert. The left sidebar contains navigation links: Dashboards, Reports, Activity Monitoring, User Behavior Analysis, Password Management, Account Discovery, Access Requests, Clients, Users, and Alerts (which is the active tab). The main 'Add Alert' page has a 'Risk Level' set to 'High'. The 'Rules' section contains a note about rule logic: 'When multiple rules are defined in an alert, rules of the same type work using OR logic, while rules of different types work using AND logic.' Below this, there are three 'Keystroke Equals CV' rules separated by 'Or' operators. Each rule has a 'Delete' (X) and an 'Or' button. A 'And' button is located at the bottom right of the rule section. The top right of the page shows 'localhost' and 'Built-in default tenant'.

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.

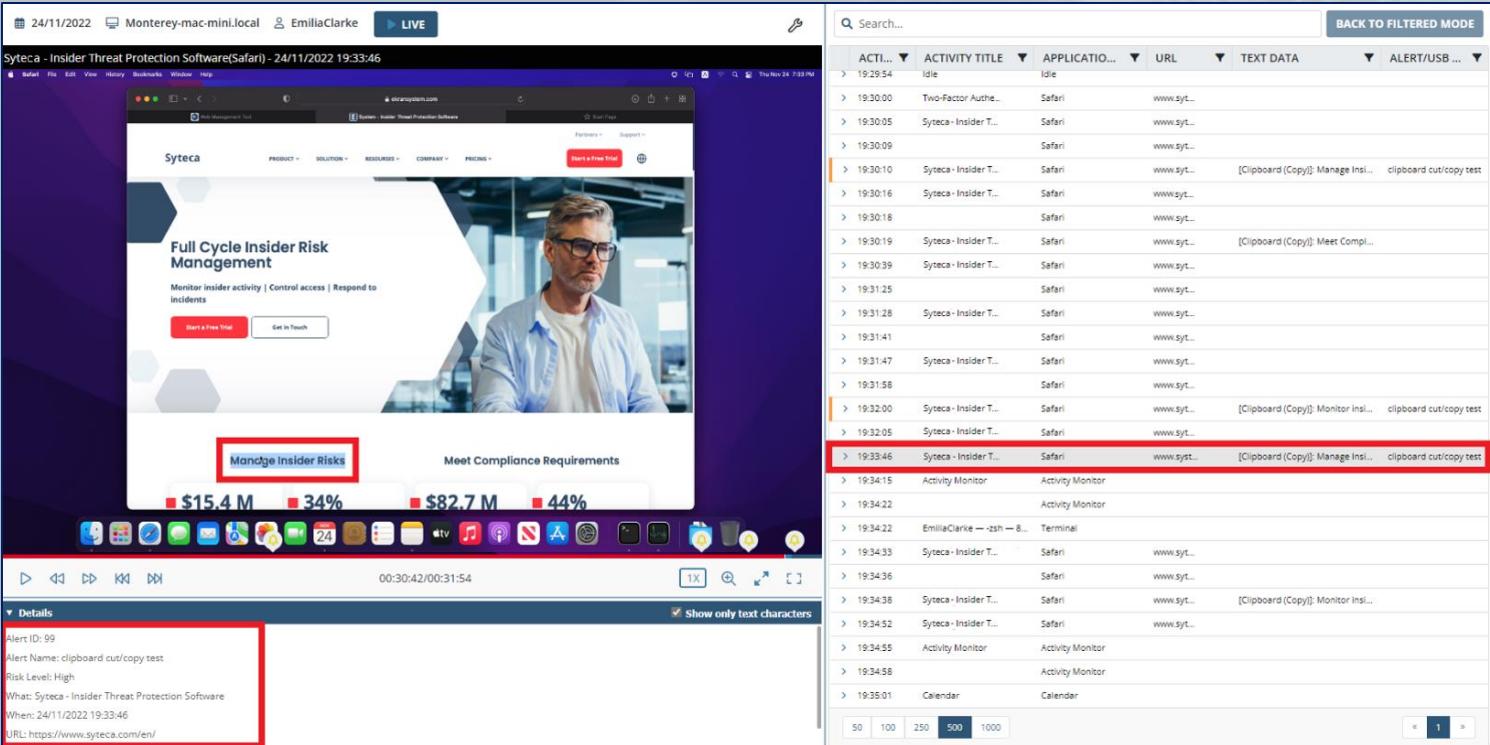


The screenshot shows the 'Editing Client (T-WIN11)' interface in the Syteca web application. The 'Client Settings' tab is selected. The 'Keystroke Monitoring' section is active, with the following configuration:

- Enable keystroke logging
- Enable keystroke logging if the Korean keyboard language is used
- Start monitoring after detecting one of the following keywords:
CV

The 'Keystroke Filtering' section shows the 'Filter State' dropdown set to 'Monitor keystrokes only in defined applications', which is highlighted in blue. Other options in the dropdown are 'Disabled' and 'Monitor keystrokes in all applications except'. Below the dropdown are two text input fields: 'Application name contains' with 'OUTLOOK;WINWORD' and 'Active window title or URL contains' with 'chrome;firefox'.

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.



The screenshot displays the Syteca Client interface on a macOS desktop. On the left, a browser window shows the Syteca website with a prominent 'Manage Insider Risks' button highlighted with a red box. On the right, a detailed log table lists clipboard activities. The log table has columns for ACTI..., ACTIVITY TITLE, APPLICATION, URL, TEXT DATA, and ALERT/USB ...

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

Details pane (highlighted with a red box):

- Alert ID: 99
- Alert Name: clipboard cut/copy test
- Risk Level: High
- What: Syteca - Insider Threat Protection Software
- When: 24/11/2022 19:33:46
- URL: <https://www.syteca.com/en/>

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**.

Editing Client (macOS-13-VM02)

← Client Settings Client Groups Permissions Assigned Alerts

Change the Settings Type to Custom to edit the Client.

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

Application Filtering

Filter State

Monitor only activity matching the defined parameters

Disabled

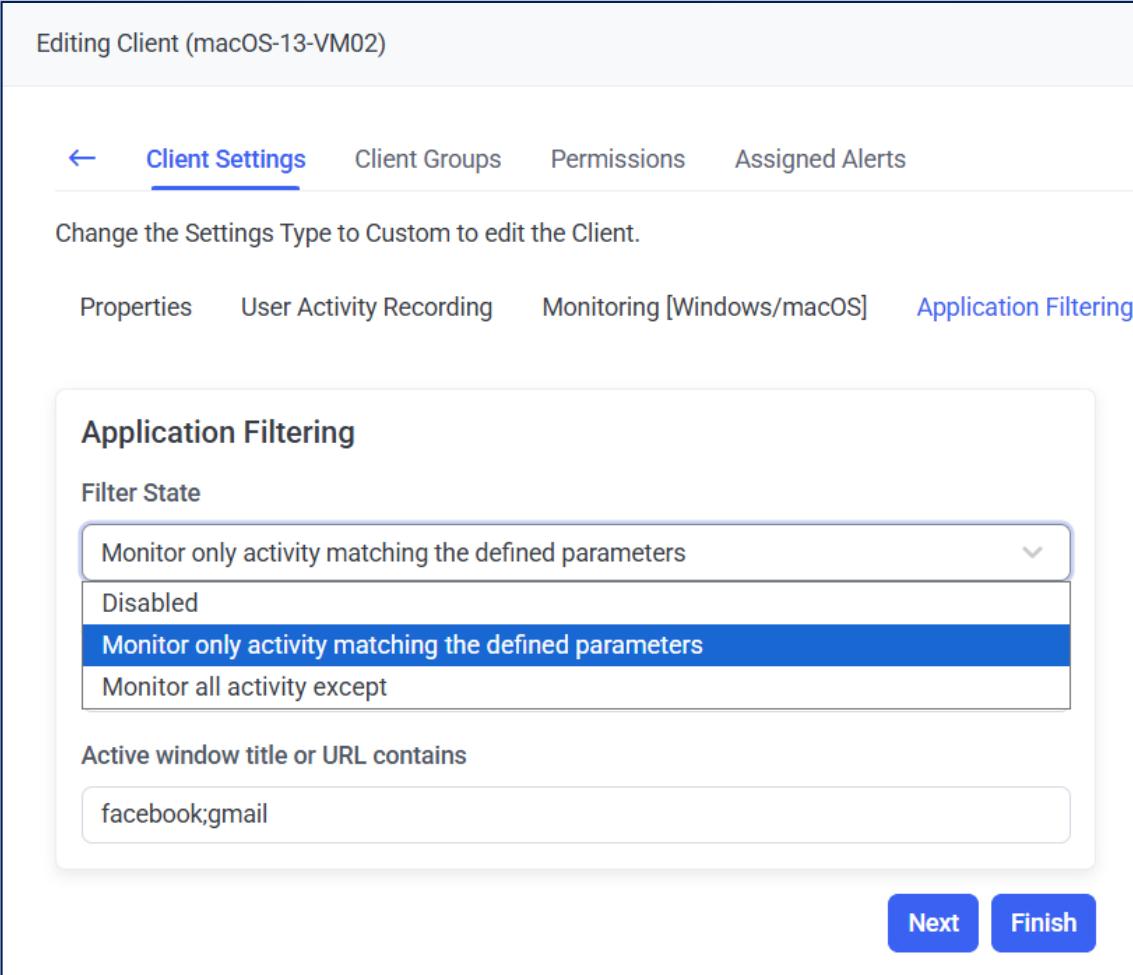
Monitor only activity matching the defined parameters

Monitor all activity except

Active window title or URL contains

facebook;gmail

Next Finish



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.

Editing Client (T-WIN11)

← Client Settings Client Groups Permissions Assigned Alerts

Change the Settings Type to Custom to edit the Client.

Properties User Activity Recording Monitoring [Windows/macOS]

Monitoring Time Filtering Remote Host IP Filtering Authentication

Monitoring Time Filtering

Filter State

Monitor only during defined hours

Disabled

Monitor only during defined hours

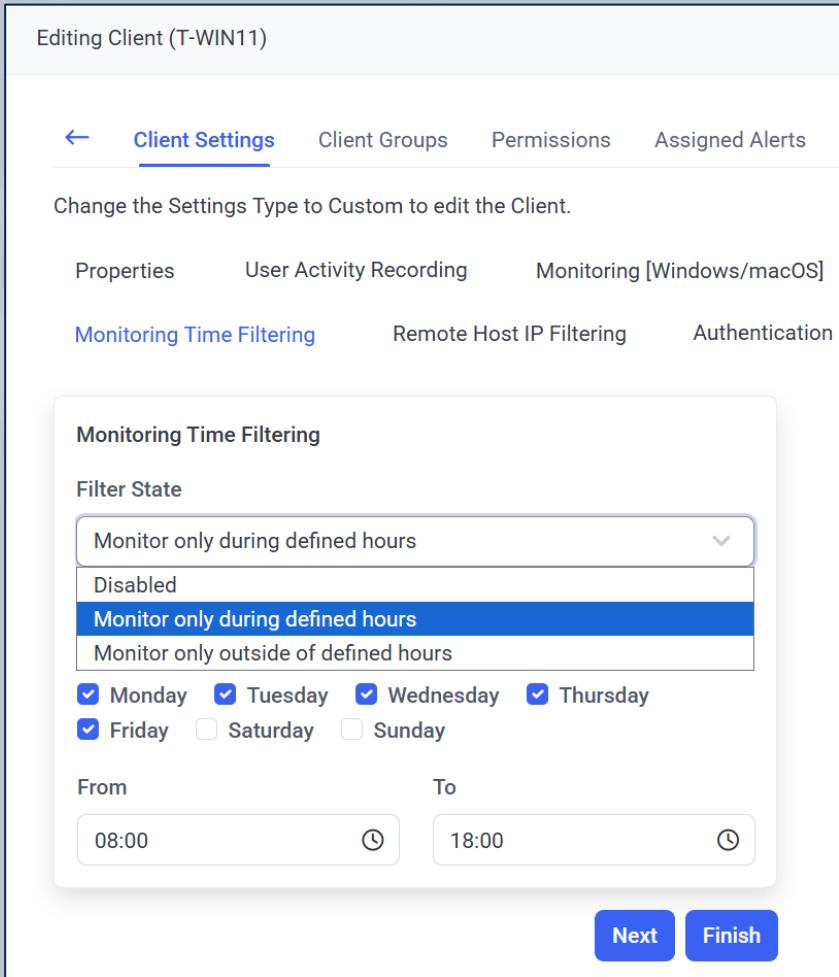
Monitor only outside of defined hours

Monday Tuesday Wednesday Thursday
 Friday Saturday Sunday

From To

08:00 18:00

Next Finish



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

Editing Client (T-WIN11)

← Client Settings Client Groups Permissions Assigned Alerts

Change the Settings Type to Custom to edit the Client.

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

Remote Host IP Filtering Authentication Options Keystroke Monitoring Additional Options

Remote Host IP Filtering

Exclude local sessions

Filter state

Monitor only activity from selected remote public IP addresses

Disabled

Monitor only activity from selected remote public IP addresses

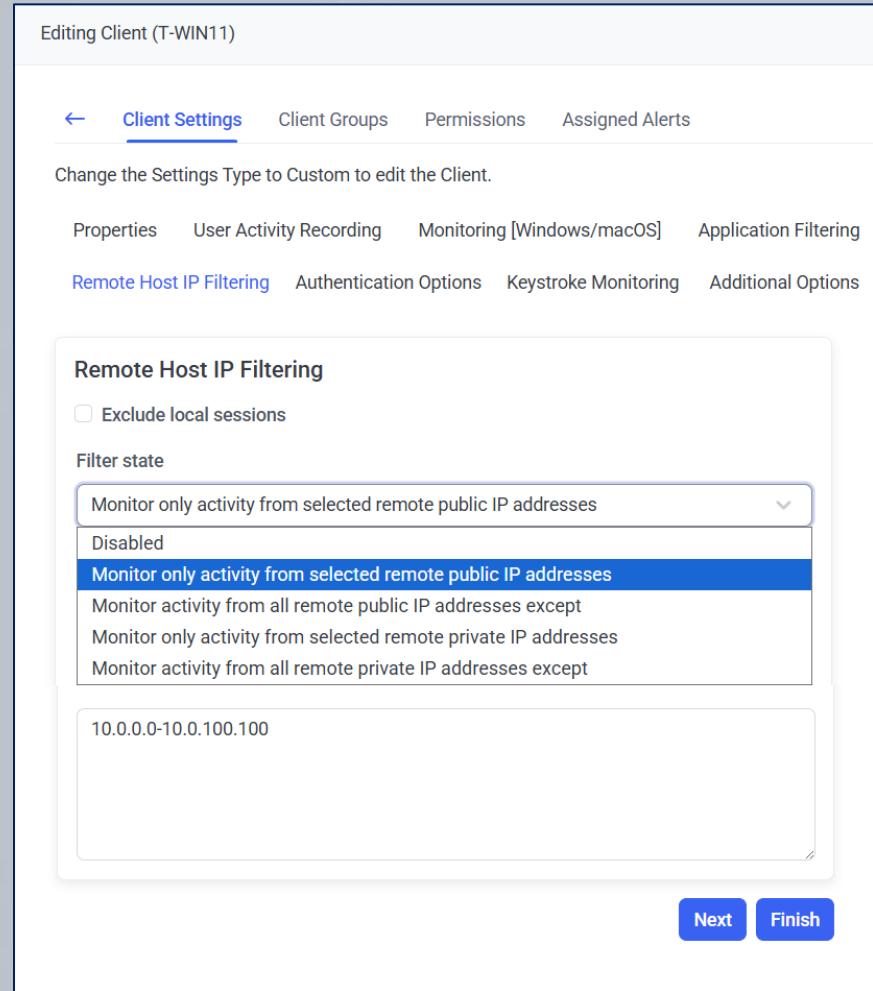
Monitor activity from all remote public IP addresses except

Monitor only activity from selected remote private IP addresses

Monitor activity from all remote private IP addresses except

10.0.0.0-10.0.100.100

Next Finish



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

Editing Client (T-WIN11)

← Client Settings Client Groups Permissions Assigned Alerts

Change the Settings Type to Custom to edit the Client.

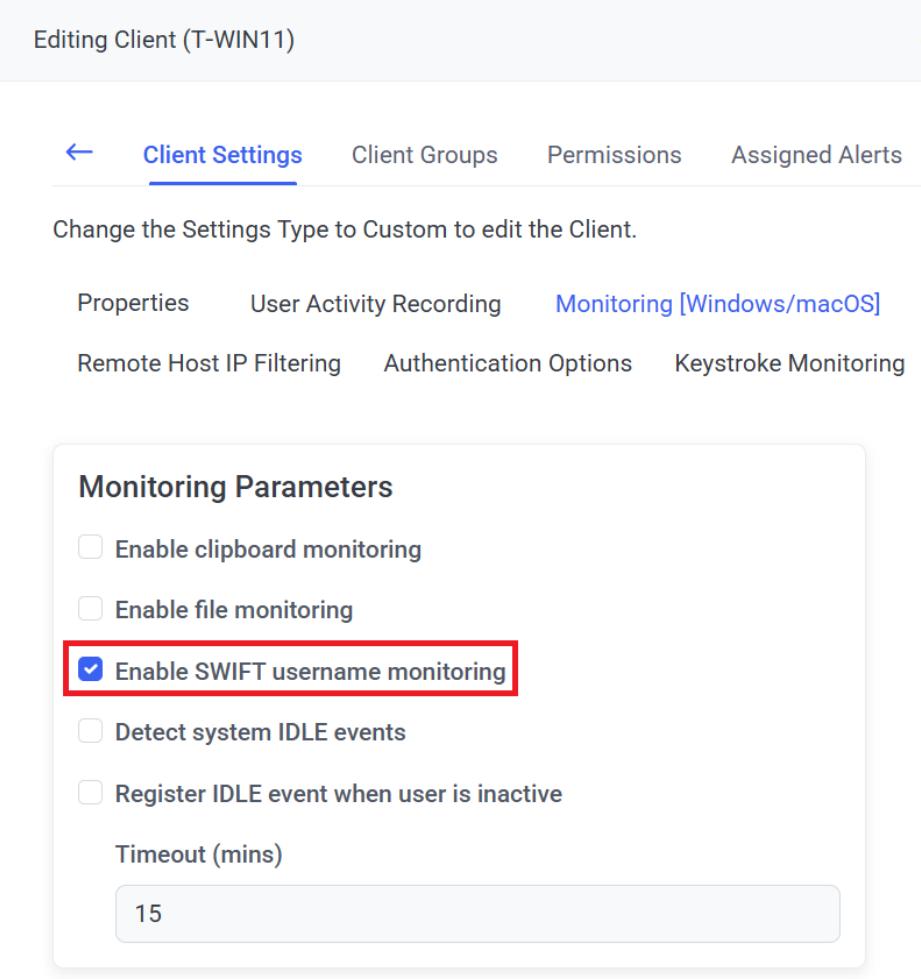
Properties User Activity Recording Monitoring [Windows/macOS]
Remote Host IP Filtering Authentication Options Keystroke Monitoring

Monitoring Parameters

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

Timeout (mins)

15



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**.

Editing Client (T-WIN11)

← Client Settings Client Groups Permissions Assigned Alerts

Change the Settings Type to Custom to edit the Client.

Properties User Activity Recording Monitoring [Windows/macOS]
Remote Host IP Filtering Authentication Options Keystroke Monitoring

Monitoring Parameters

Enable clipboard monitoring

Enable file monitoring

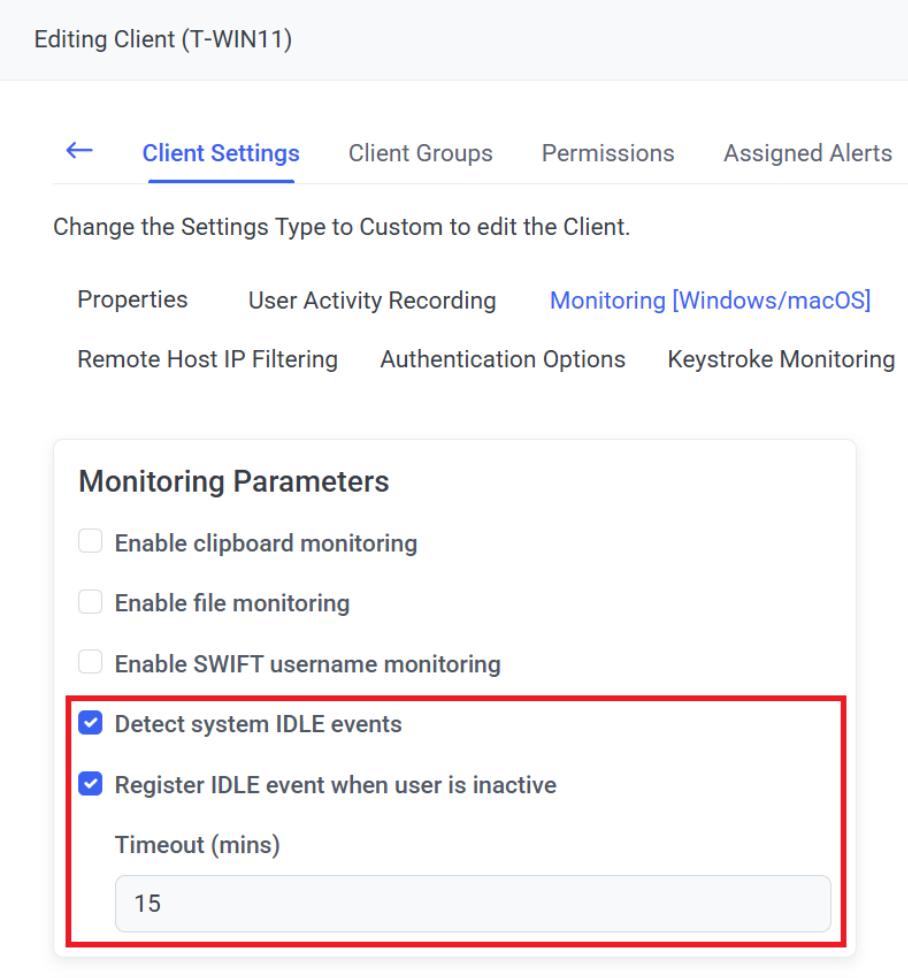
Enable SWIFT username monitoring

Detect system IDLE events

Register IDLE event when user is inactive

Timeout (mins)

15



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

Editing Client (T-WIN11)

← Client Settings Client Groups Permissions Assigned Alerts

Change the Settings Type to Custom to edit the Client.

Properties User Activity Recording Monitoring [Windows/macOS] Application Filtering
User Filtering Authentication Options Keystroke Monitoring Additional Options

User Filtering

Filter state

Monitor only the activity of selected users

Disabled

Monitor only the activity of selected users

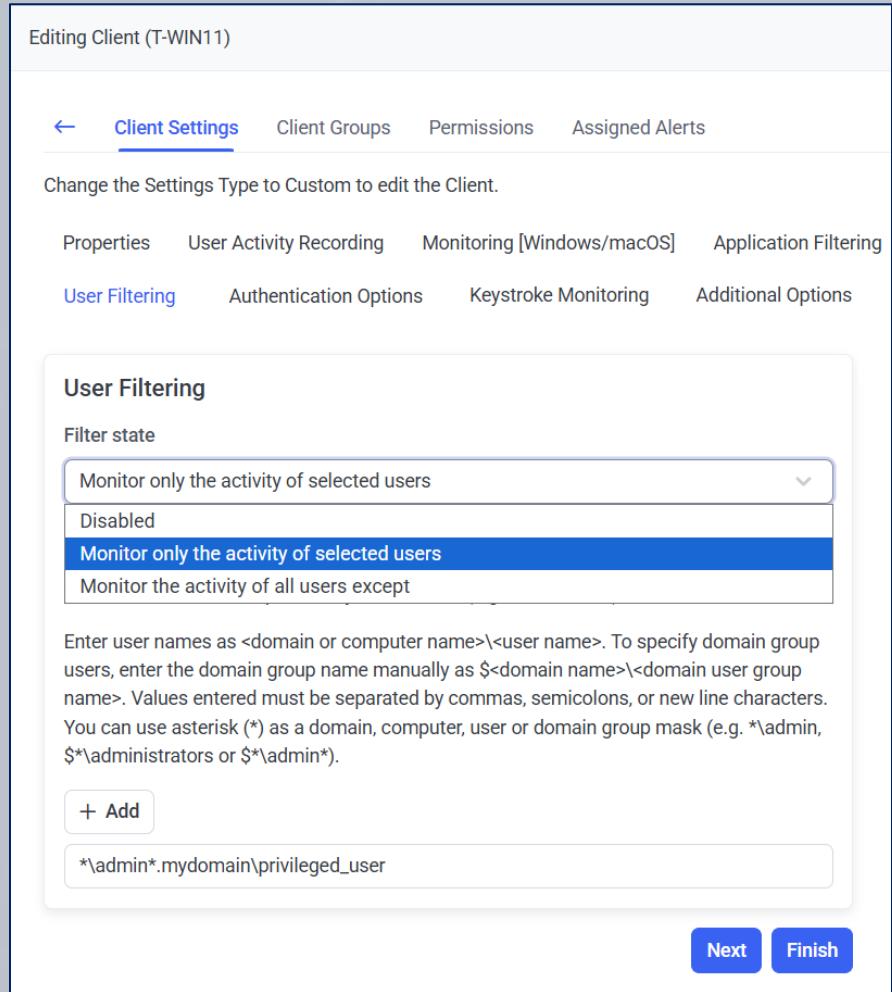
Monitor the activity of all users except

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

+ Add

\admin.mydomain\privileged_user

Next Finish



Bandwidth Usage Reduction



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.

Editing Client (TW-WIN11)

Properties User Activity Recording Monitoring [Windows/macOS] Application Filtering User Filtering
Keystroke Monitoring Additional Options Privacy Settings

Additional Options

Screen capture throttling (ms)
0
NOTE: The above option is not currently supported in Full-Motion Capture mode.

Batch registration timeout (ms)
10000
NOTE: The above option is not currently supported in Full-Motion Capture mode.

Chunk size (minutes)
1

Prevent loading hooks into the following applications

Reduce screen capture size by (%)
30

Screenshot compression level (1-19)
9
NOTE: The above option is not currently supported in Full-Motion Capture mode.

Agent memory limit (0-disabled)
0

Support secure browsers by disabling some monitoring features ?

Next Finish

File Upload Monitoring



File upload monitoring operations can be detected, including in many applications such as common browsers and messaging apps.

The screenshot illustrates a file upload monitoring feature. On the left, a Google Chrome window shows a search for 'facebook' and an image upload progress bar. On the right, a log table displays a list of detected activities, with the last entry highlighting a file upload operation.

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

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.

Editing Client (T-WIN11)

← Client Settings Client Groups Permissions Assigned Alerts

Change the Settings Type to Custom to edit the Client.

Properties User Activity Recording Monitoring [Windows/macOS] Application Filtering
Authentication Options Keystroke Monitoring Additional Options Privacy Settings

Client Properties

Description

Assigned license

Custom Workstation

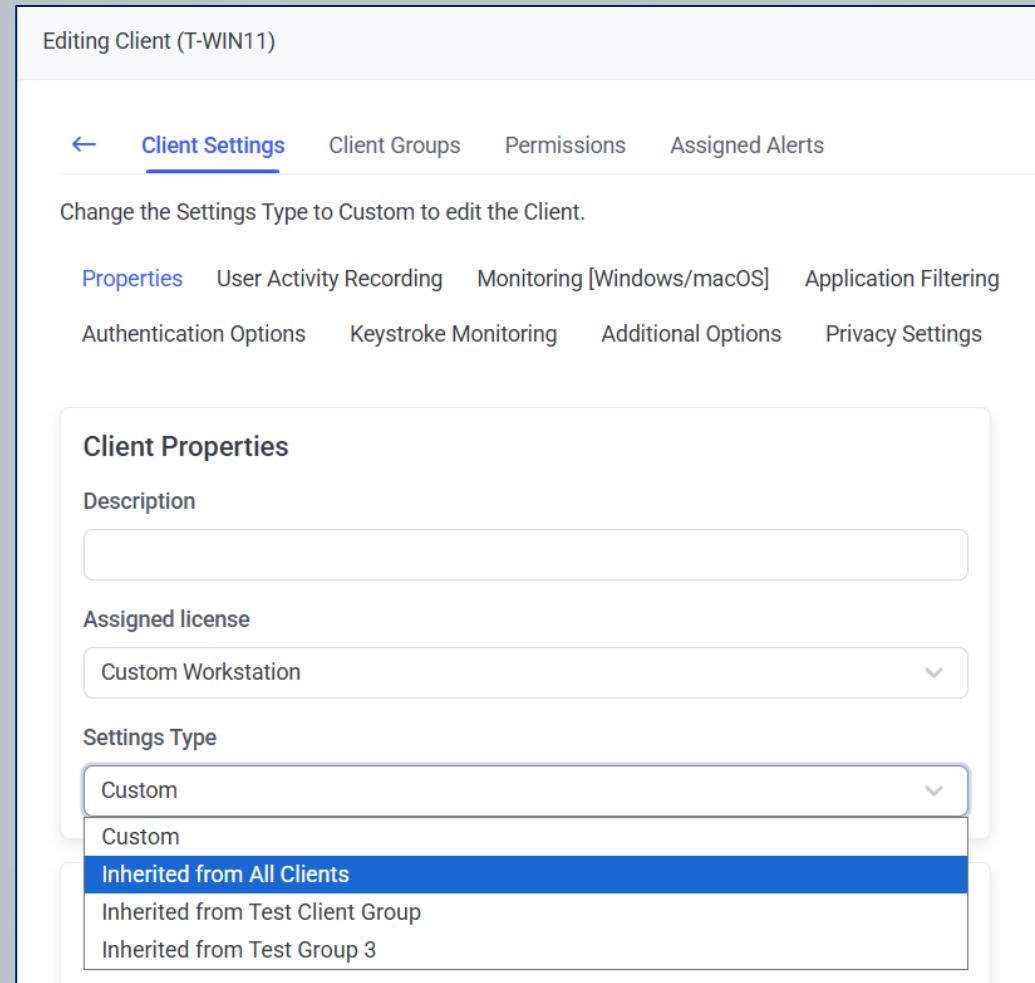
Settings Type

Custom

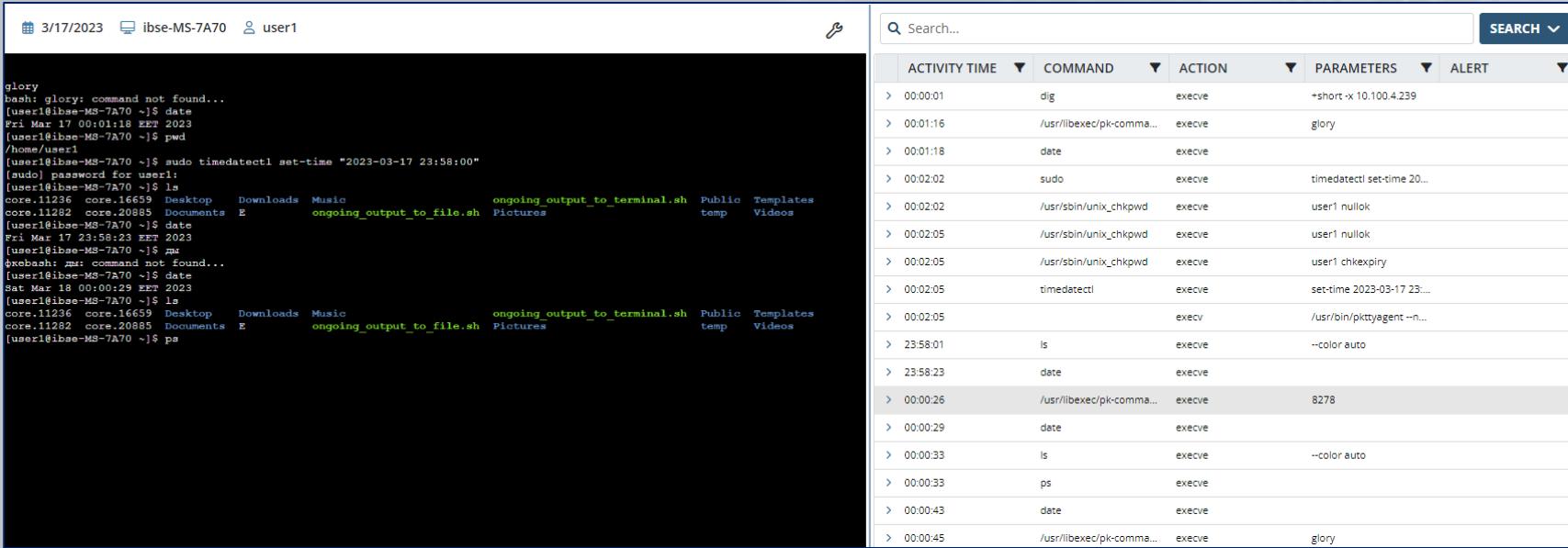
Inherited from All Clients

Inherited from Test Client Group

Inherited from Test Group 3



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.



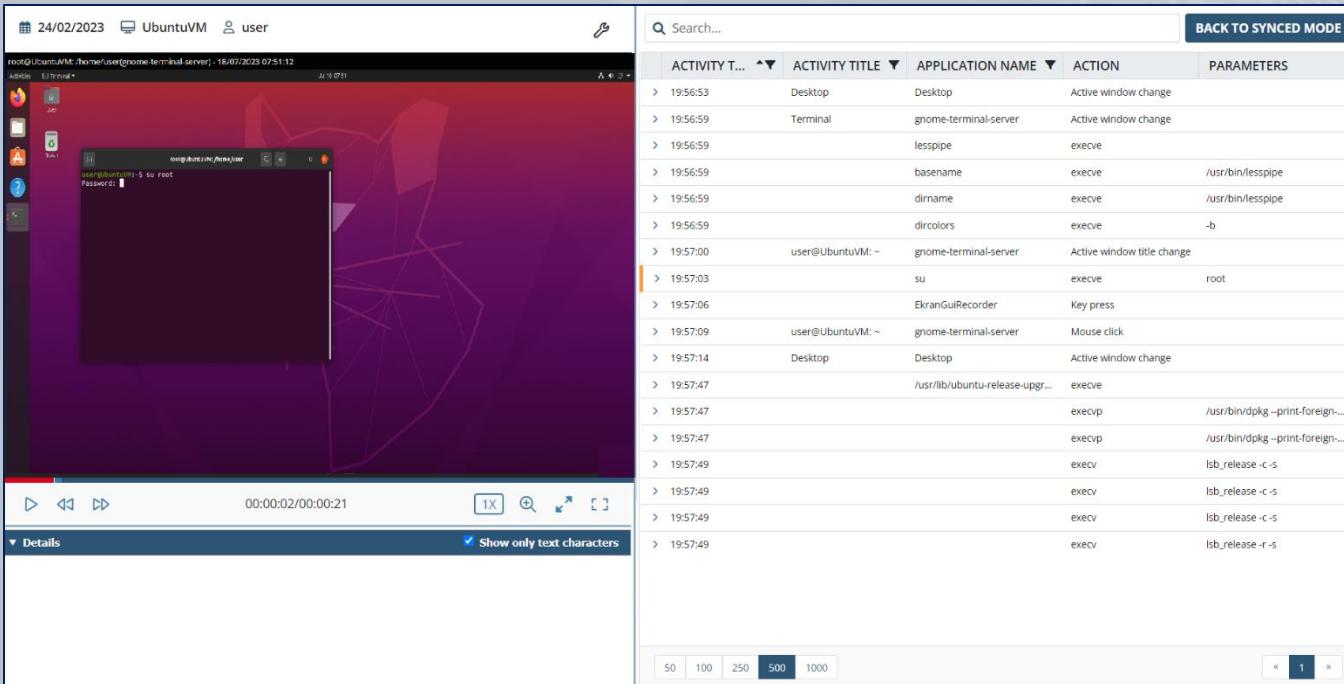
The screenshot shows a dual-pane interface. The left pane is a terminal window titled '3/17/2023 ibse-MS-7A70 user1'. It displays a user's session with various commands like 'date', 'ls', 'sudo', and 'ps'. The right pane is a table titled 'ACTIVITY TIME' showing a log of system events. The table has columns for ACTIVITY TIME, COMMAND, ACTION, PARAMETERS, and ALERT. The log includes entries for 'dig', 'date', 'sudo', and 'timedatectl' commands, along with file operations like 'ls' and 'ps'.

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

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

A **local Linux Client session for X Window System (X11)** includes:

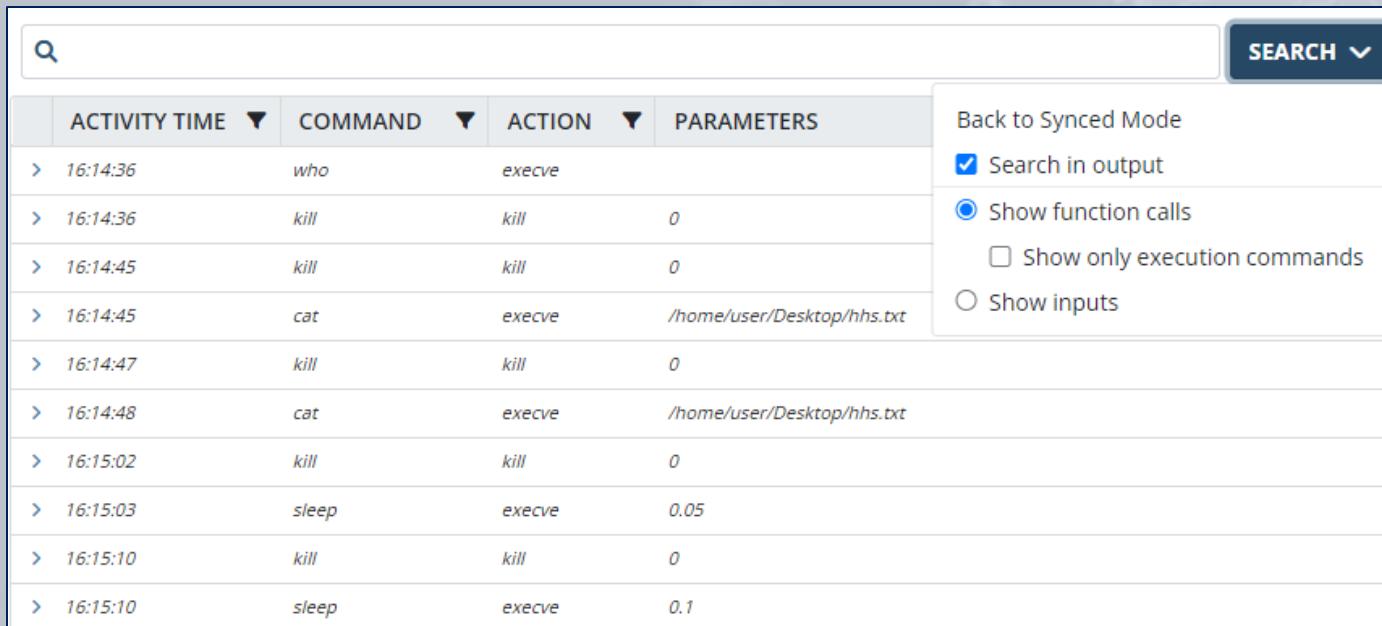
- Screen captures
- Activity times
- Activity titles
- Application names / Commands
- Actions / System function calls
- Parameters



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

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

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



The screenshot shows a monitoring interface with a table of system activities and a sidebar with search filters.

Table Headers: ACTIVITY TIME, COMMAND, ACTION, PARAMETERS

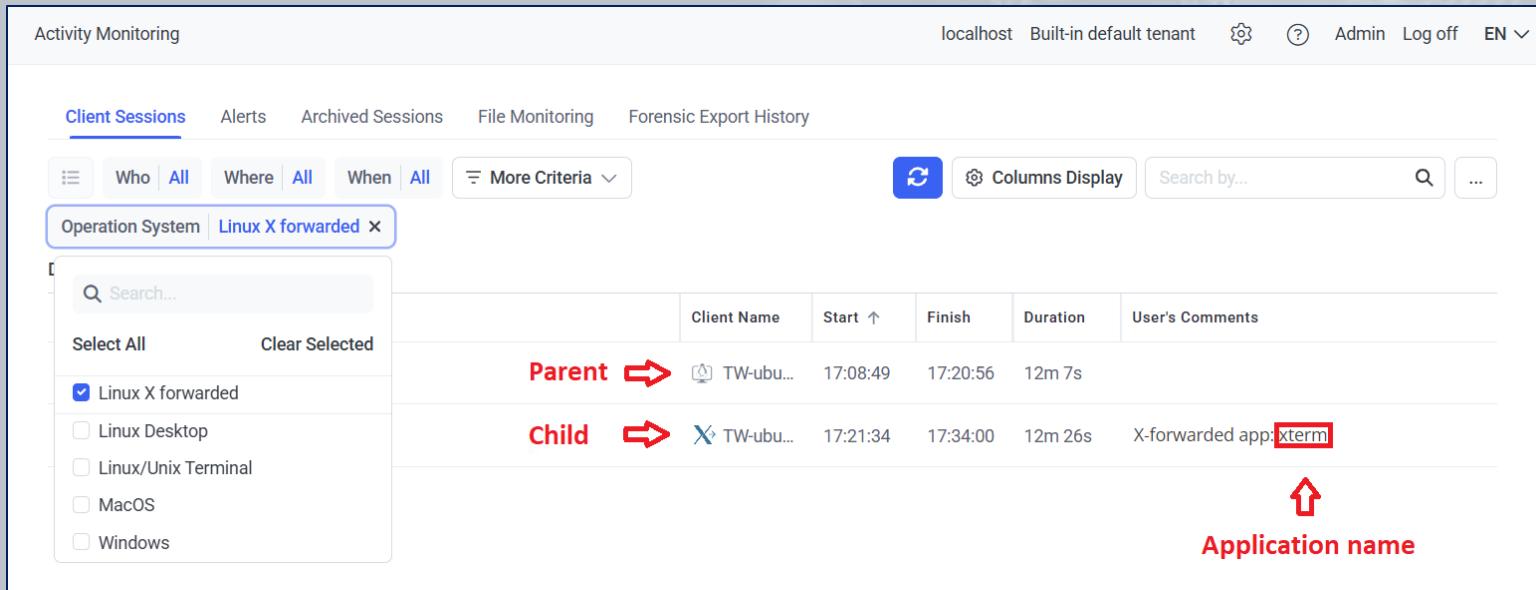
Table Data:

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

Search Filter Sidebar:

- Search in output
- Show function calls
- Show only execution commands
- Show inputs

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



Activity Monitoring

localhost Built-in default tenant   Admin Log off EN 

Client Sessions Alerts Archived Sessions File Monitoring Forensic Export History

Who | All Where | All When | All More Criteria   Columns Display Search by... 

Operation System | Linux X forwarded 

Search...
Select All Clear Selected
 Linux X forwarded
 Linux Desktop
 Linux/Unix Terminal
 MacOS
 Windows

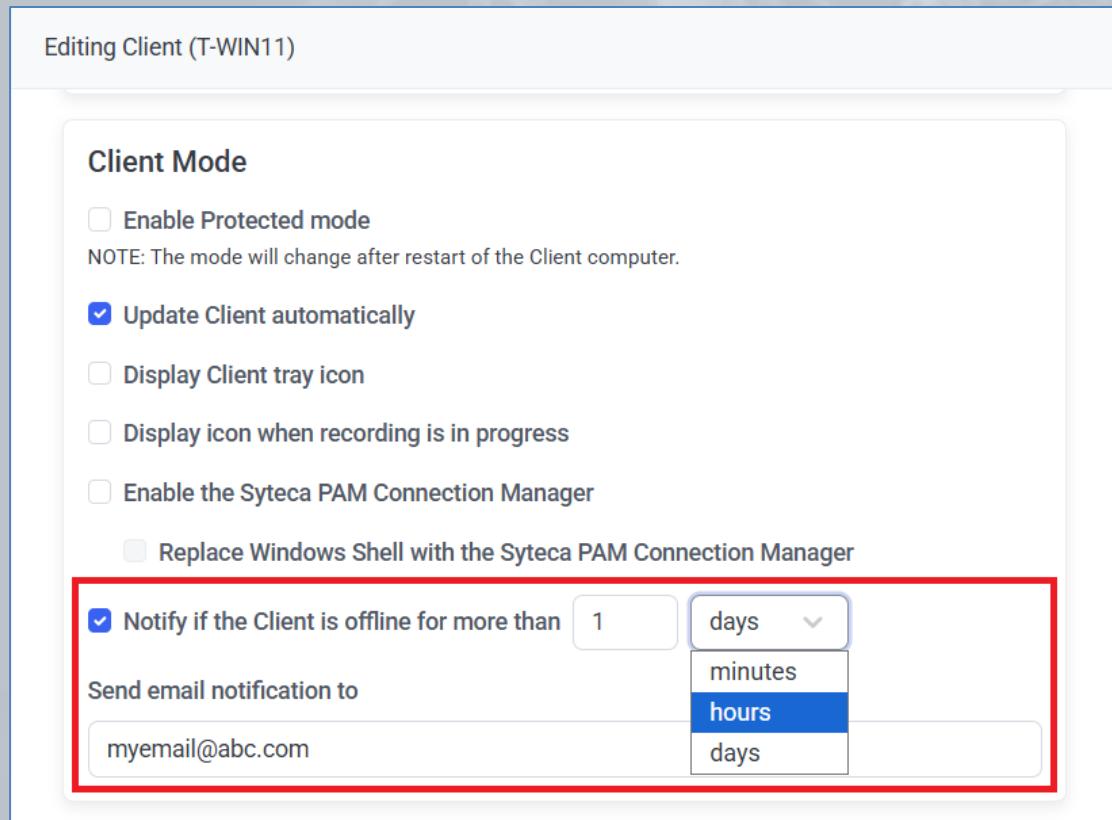
	Client Name	Start ↑	Finish	Duration	User's Comments
Parent 	 TW-ubu...	17:08:49	17:20:56	12m 7s	
Child 	 TW-ubu...	17:21:34	17:34:00	12m 26s	X-forwarded app:  xterm

 Application name

Detection of Disconnected Clients

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

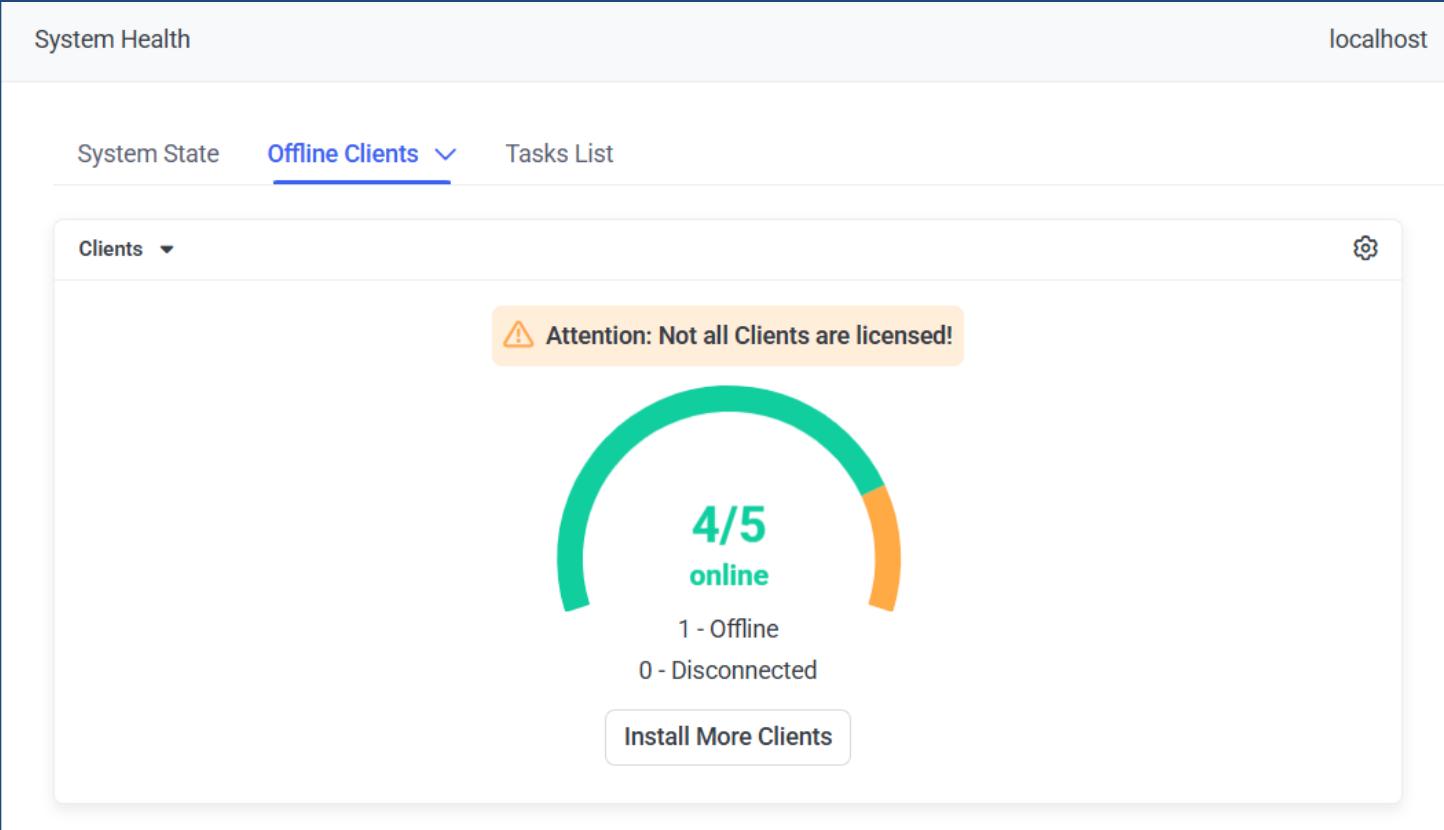
Just **define the time period** after which offline Clients will be considered as disconnected, and **get notified** about such incidents.



Viewing Disconnected Clients



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



The screenshot shows the Syteca System Health interface with the following details:

- System Health** header with **localhost** on the right.
- System State** dropdown.
- Offline Clients** dropdown (underlined in blue, indicating the active view).
- Tasks List** link.
- Clients** dropdown.
- Attention:** Not all Clients are licensed! (Warning message).
- 4/5 online** (Status summary).
- 1 - Offline** (Count of offline clients).
- 0 - Disconnected** (Count of disconnected clients).
- Install More Clients** button.

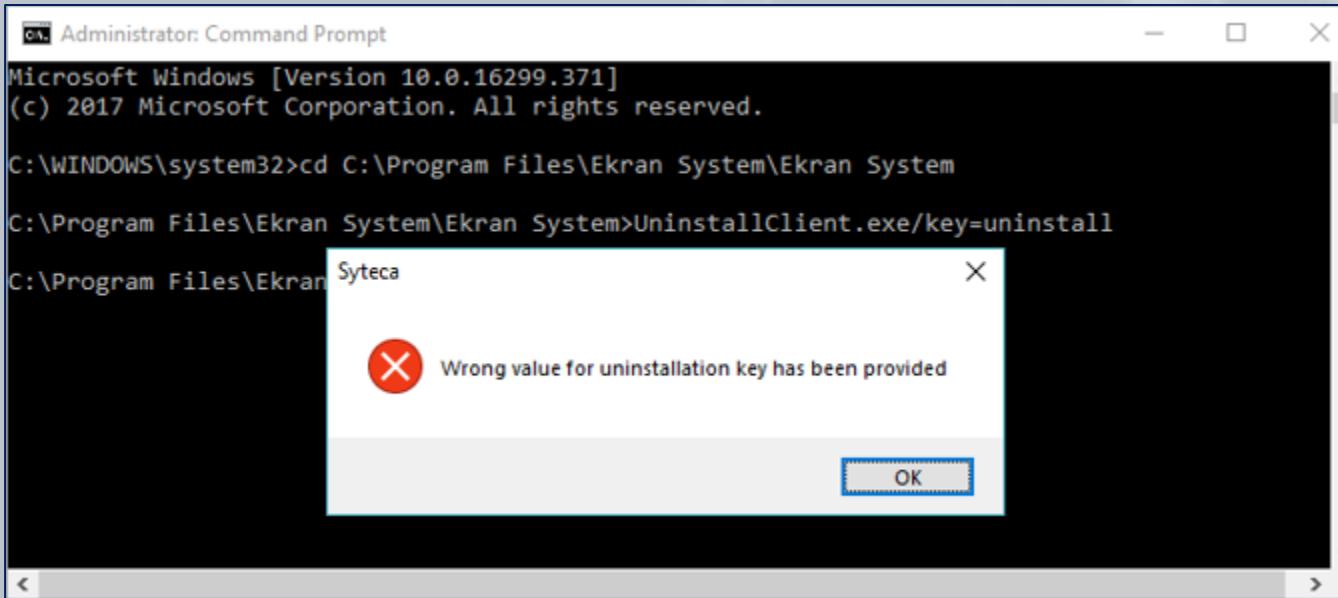
Client Protection

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**.

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

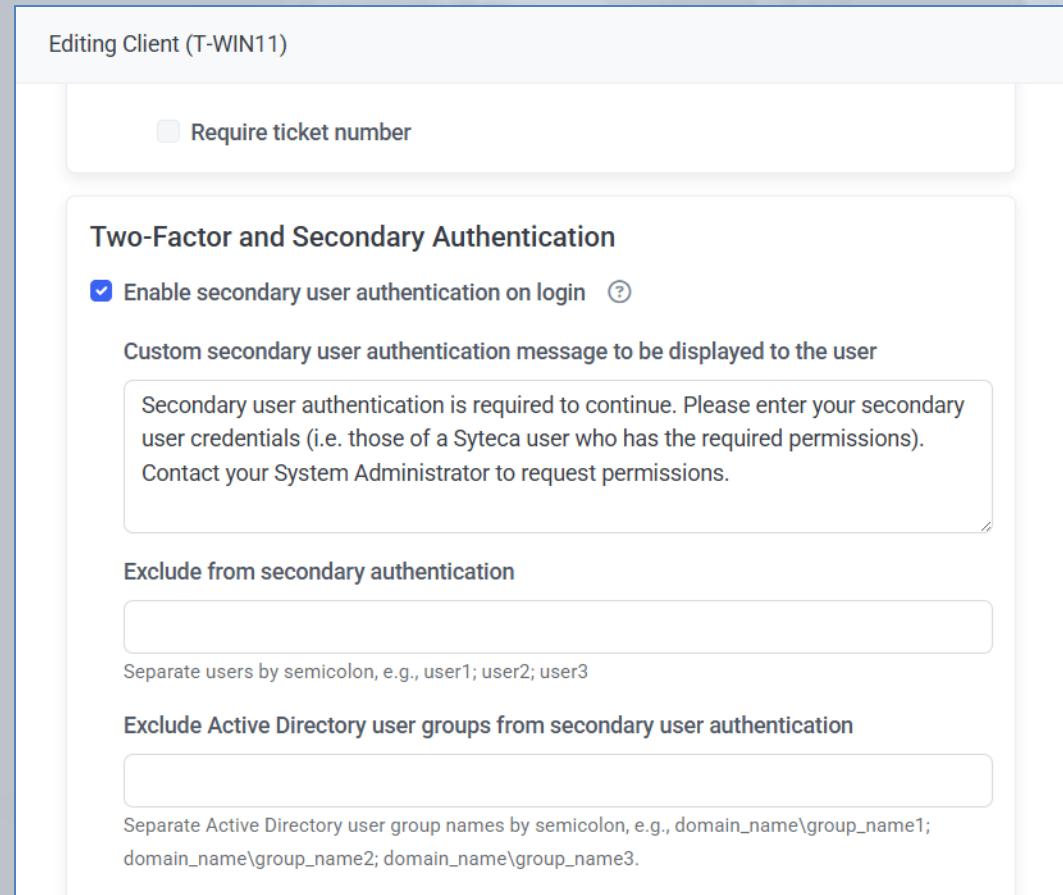


Only the **Syteca administrator knows the Uninstallation key** defined prior to Client installation, and which is required for local removal.

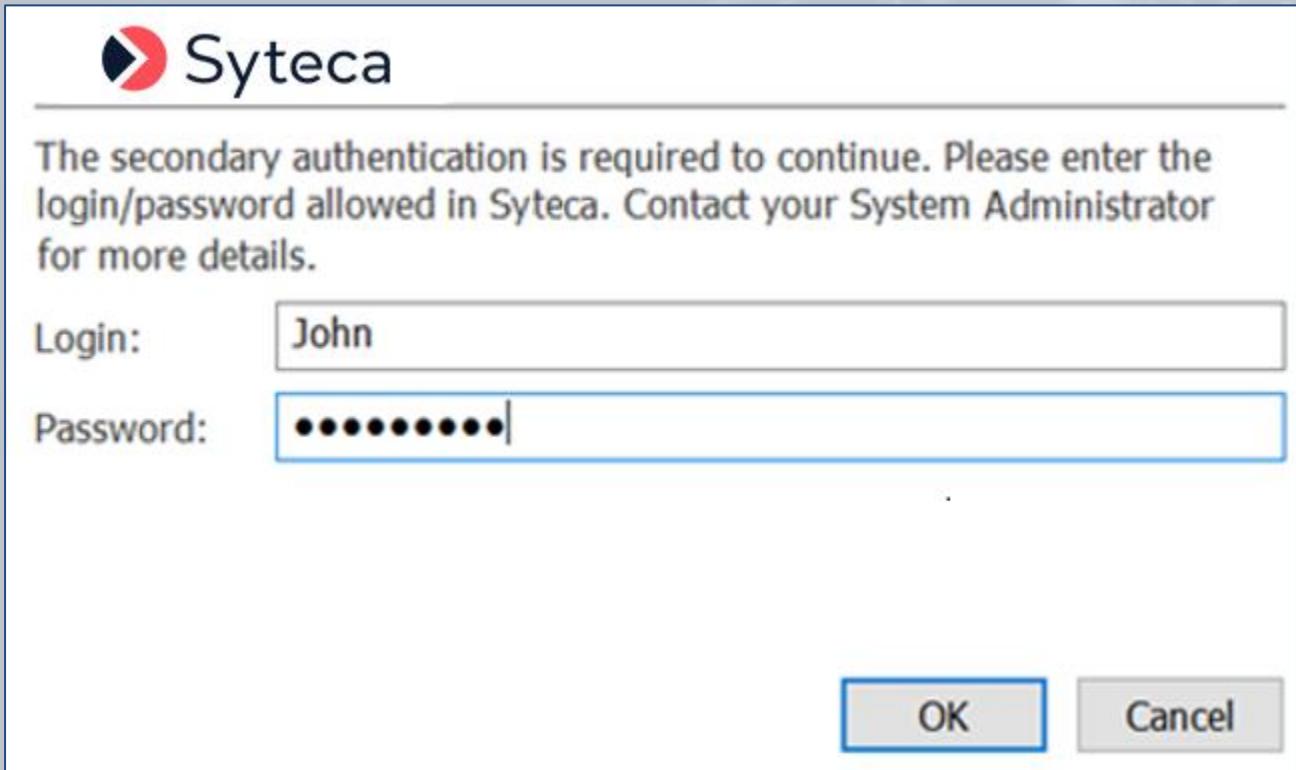
Secondary User Authentication

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

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

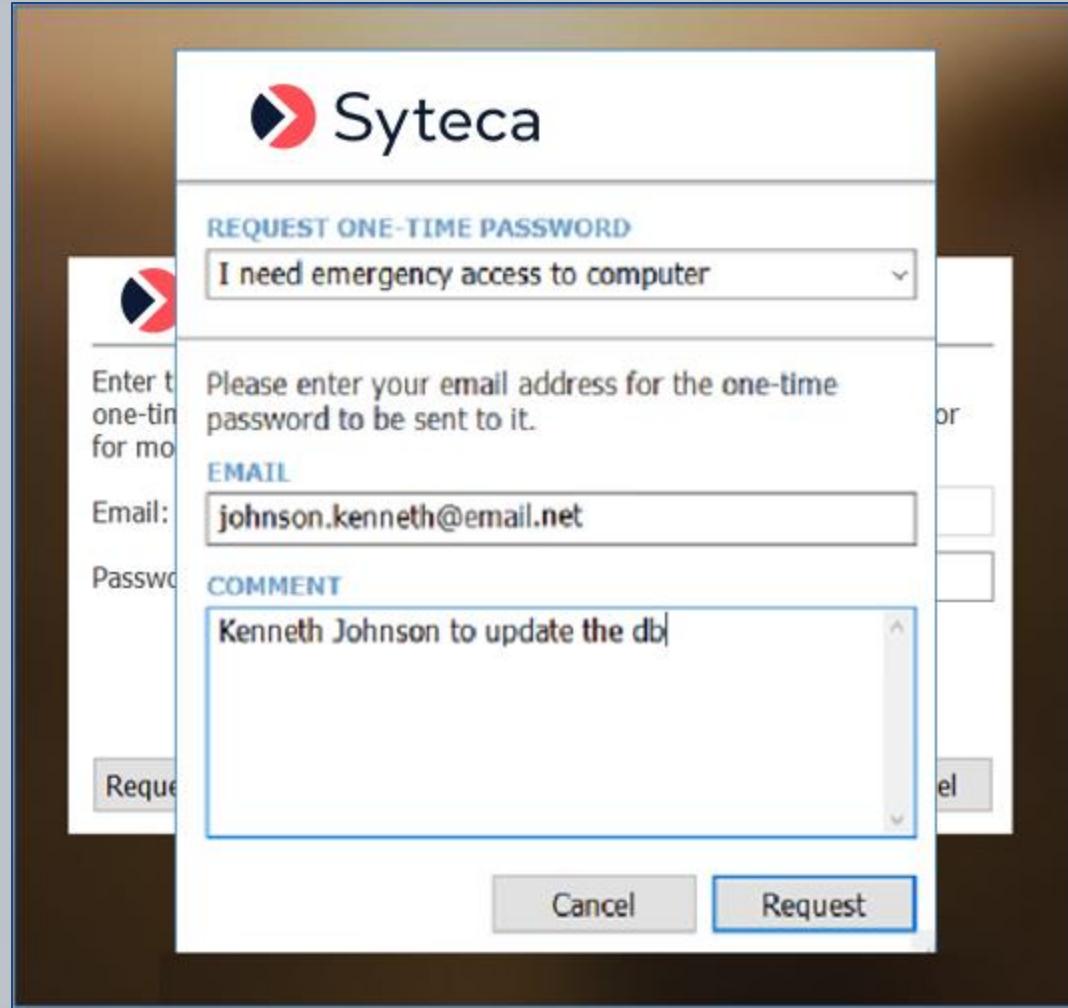


The Syteca Client requests **credentials** to be entered **before** allowing a user to **access** the Windows operating system.

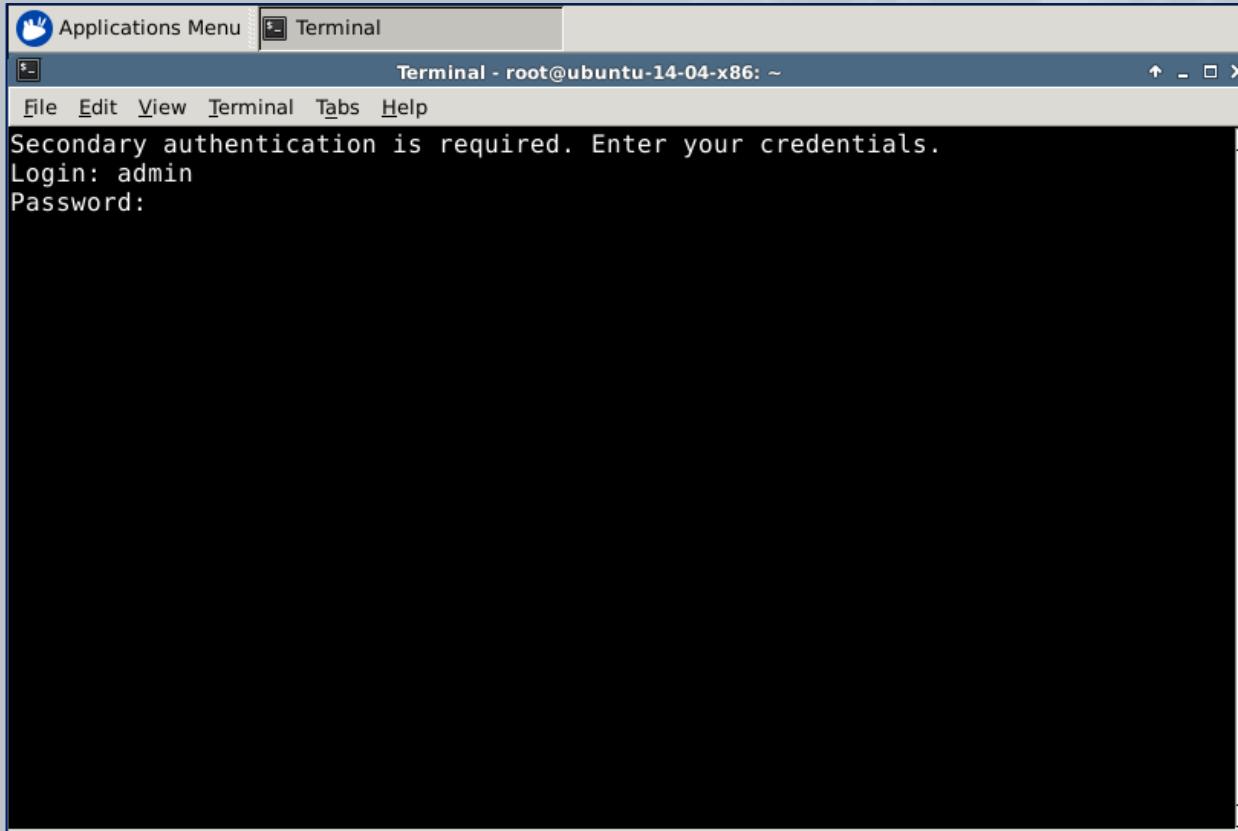


Syteca provides the **administrator** with the unique **capability** to protect Client computers with one-time passwords.

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

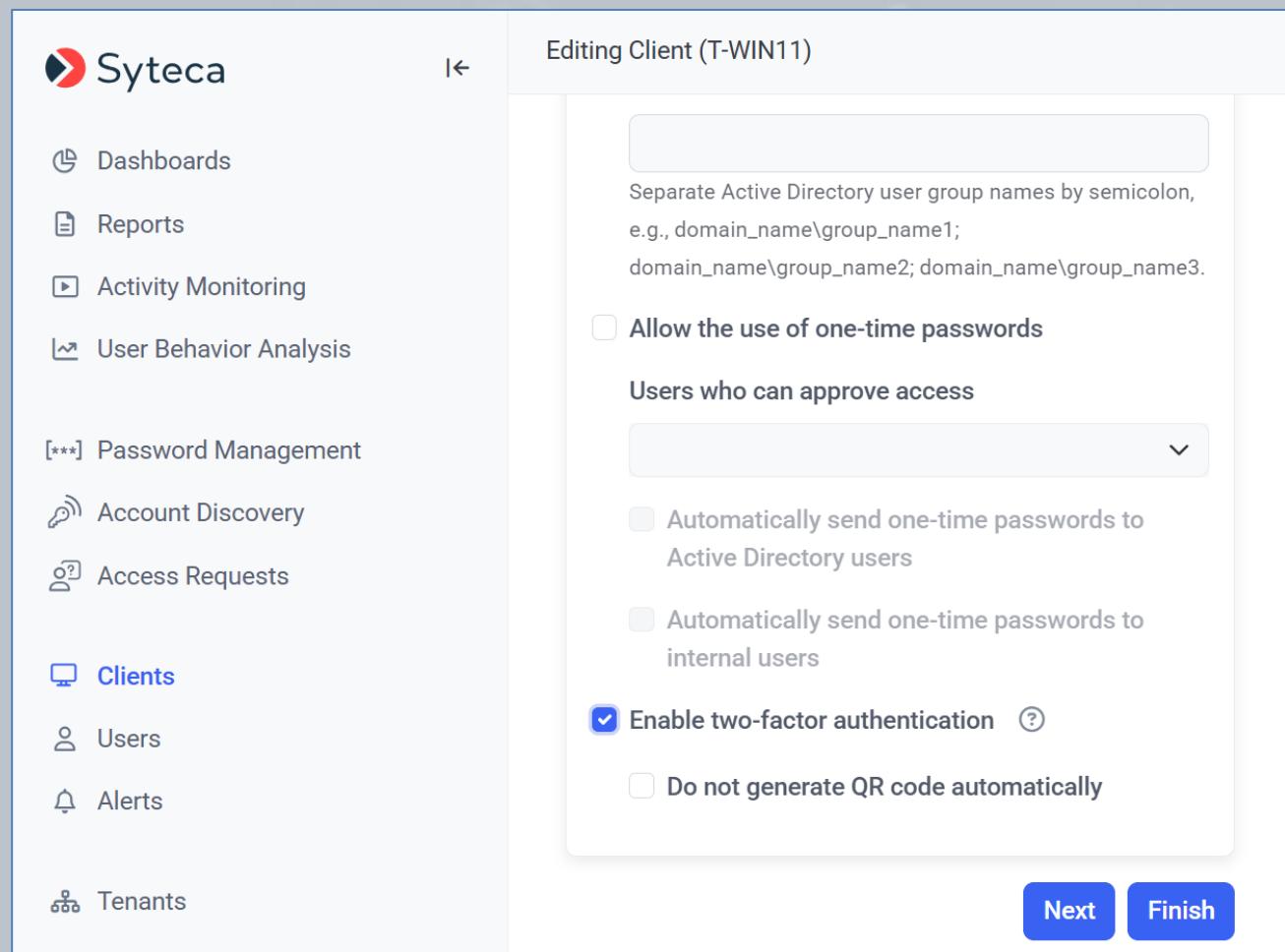


The Syteca Client requests **credentials** to be entered to allow a user to **log on to the terminal** on **Linux** Client computers.



Two-Factor Authentication

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



Editing Client (T-WIN11)

Separate Active Directory user group names by semicolon, e.g., domain_name\group_name1; domain_name\group_name2; domain_name\group_name3.

Allow the use of one-time passwords

Users who can approve access

Automatically send one-time passwords to Active Directory users

Automatically send one-time passwords to internal users

Enable two-factor authentication ?

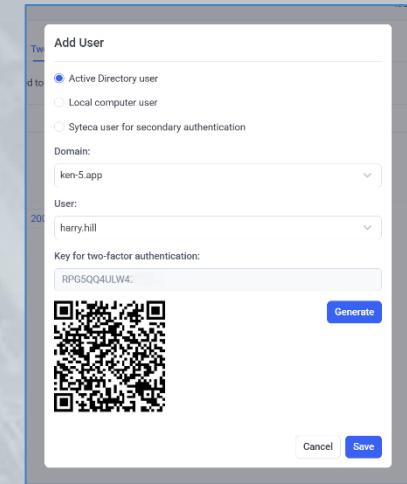
Do not generate QR code automatically

Next Finish

Two-Factor Authentication (Windows/Linux)

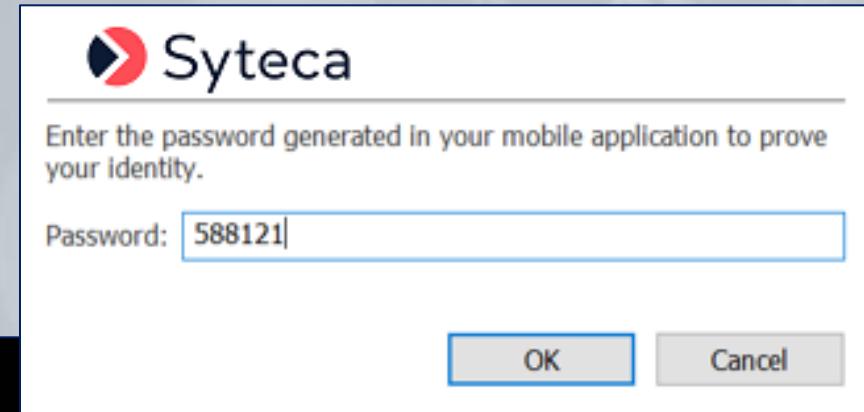


You can either enable this feature for all Windows Client computers, or manually add only users who you want to be allowed to log in to Windows and Linux Client computers, using **time-based one-time passwords** (TOTP) generated by way of a mobile authenticator application.



User	User Type	Time Added	Added by	One-Time Password	Remove All
admin	Syteca user for se...	30/07/2025 14:16:...	Harry		
harry-hill-pc\har...	Local computer user	30/07/2025 14:15:...	Harry		
ken-5.app\harry....	Active Directory us...	30/07/2025 14:11:...	Harry		

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)
```

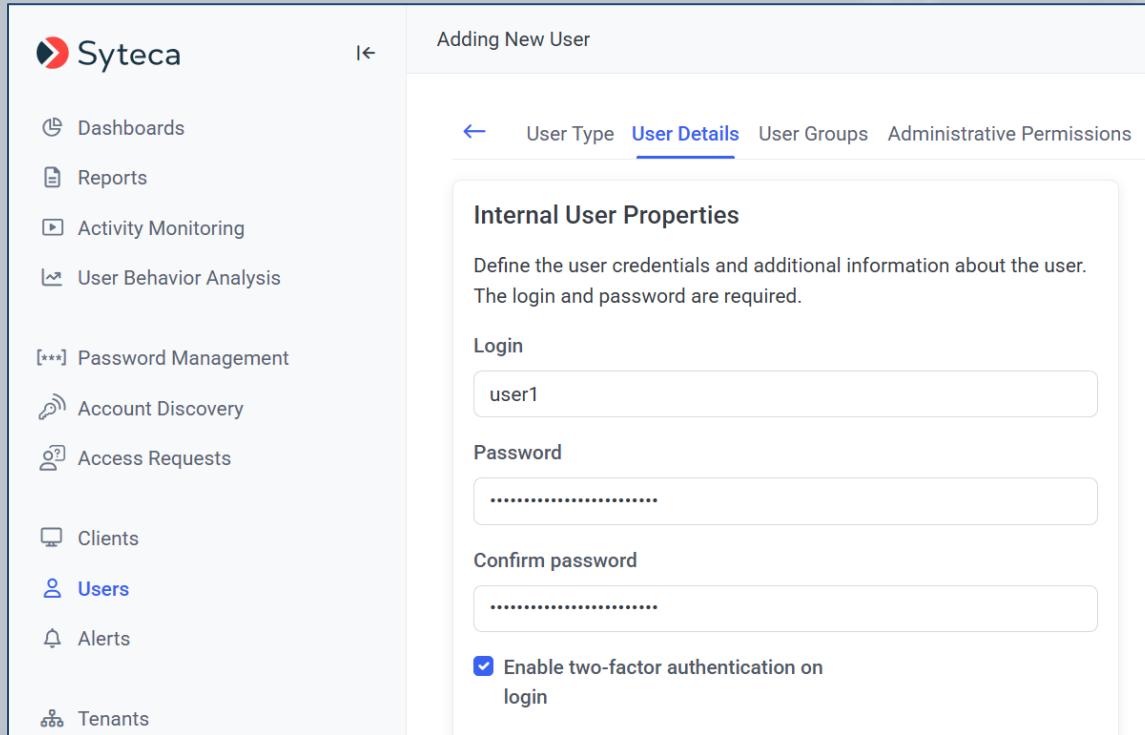
```
* Documentation: https://help.ubuntu.com
```

```
* Management: https://landscape.canonical.com
```

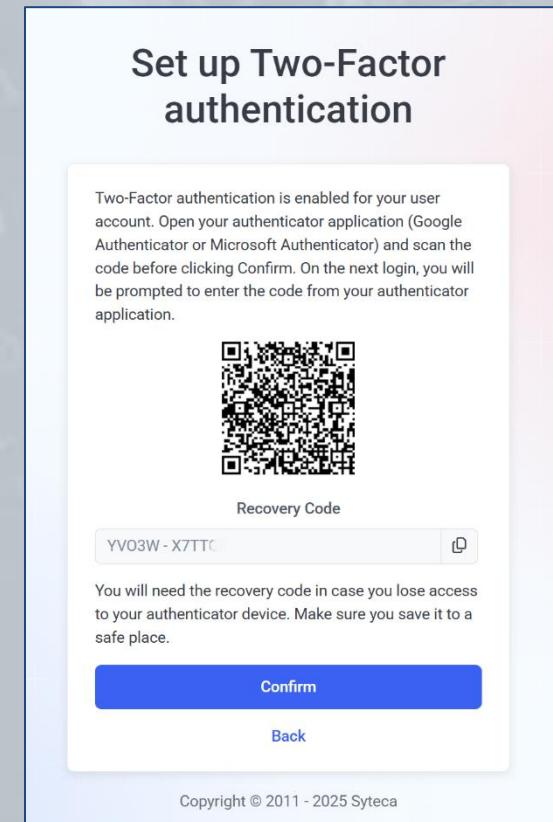
```
* Support: https://ubuntu.com/advantage
```

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

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



The screenshot shows the Syteca Management Tool's user management interface. On the left is a sidebar with various navigation options: Dashboards, Reports, Activity Monitoring, User Behavior Analysis, Password Management, Account Discovery, Access Requests, Clients, Users (which is the active tab), Alerts, and Tenants. The main content area is titled 'Adding New User' and shows the 'User Details' tab selected. It includes sections for 'Internal User Properties' (with a note that login and password are required), 'Login' (with fields for 'user1' and a password placeholder), 'Password' (with a password placeholder), 'Confirm password' (with a password placeholder), and a checkbox for 'Enable two-factor authentication on login' which is checked. The URL in the browser is <https://app.syteca.com/auth/realms/syteca/protocol/openid-connect/userinfo>.



The screenshot shows a modal window titled 'Set up Two-Factor authentication'. It contains instructions: 'Two-Factor authentication is enabled for your user account. Open your authenticator application (Google Authenticator or Microsoft Authenticator) and scan the code before clicking Confirm. On the next login, you will be prompted to enter the code from your authenticator application.' Below the instructions is a QR code for scanning. A text input field shows a recovery code: 'YV03W - X7TTC'. At the bottom are 'Confirm' and 'Back' buttons. The URL in the browser is <https://app.syteca.com/auth/realms/syteca/protocol/openid-connect/userinfo>.

Password Management (PAM)

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).

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!

Add Secret

Properties Automation Security Permissions Restrictions

This type of secret allows [File Transfer](#).

General

Secret Name: MySecret1

Type: Unix account (SSH)

Active Directory account
Windows account
Unix account (SSH)
Unix account (Telnet)
Web account
MS SQL account

Use SSH key

Computer name:

Login: Password:

File transfer

File Transfer Protocol: SFTP Port: 22

Adding a Secret (Enhanced Security Options)



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**

Add Secret

Properties Automation Security Permissions Restrictions

Enable remote password rotation

Rotate Password Every days

Add Secret

Properties Automation Security Permissions Restrictions

Record user activity while the secret is in use

Requires check out

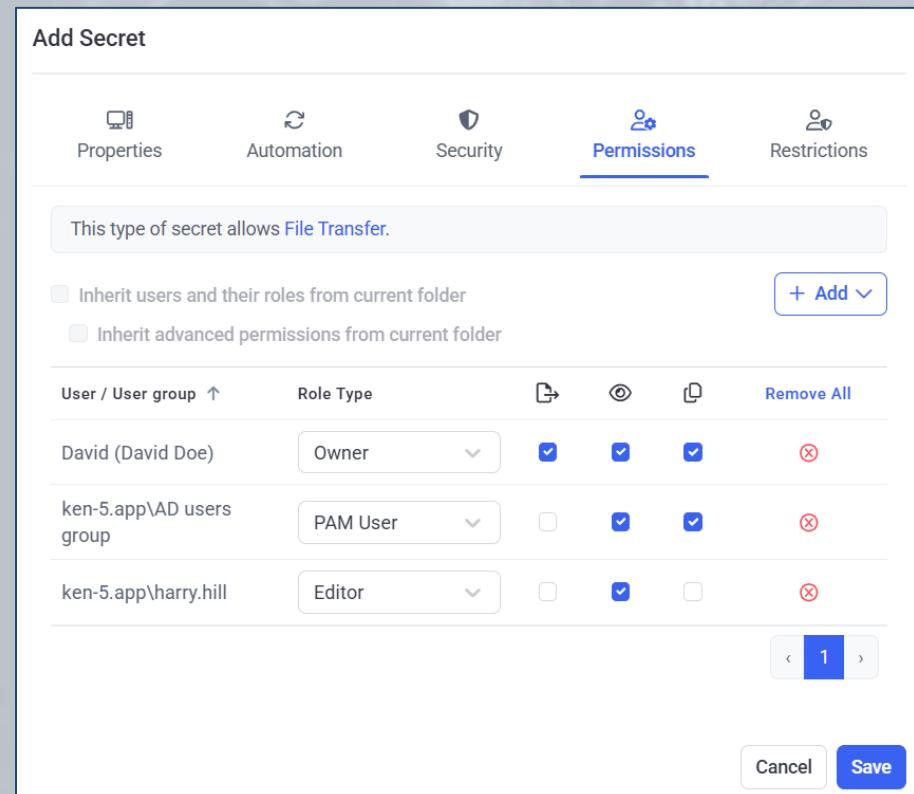
Change password on check in

Check in automatically after hours minutes

Force Check In

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



User / User group	Role Type	File Transfer	View Password	Copy Password	Remove
David (David Doe)	Owner	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ken-5.app\AD users group	PAM User	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ken-5.app\harry.hill	Editor	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

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**.

Add Secret

Properties Automation Security Permissions **Restrictions**

Access without any restrictions
 Always require approval on secret usage
 Allow access without approval during work hours

Allowed dates From: 11/08/2025 To: 25/08/2025

Allowed time From: 08:00 To: 17:00

Allowed days of the week Su Mo Tu We Th Fr Sa

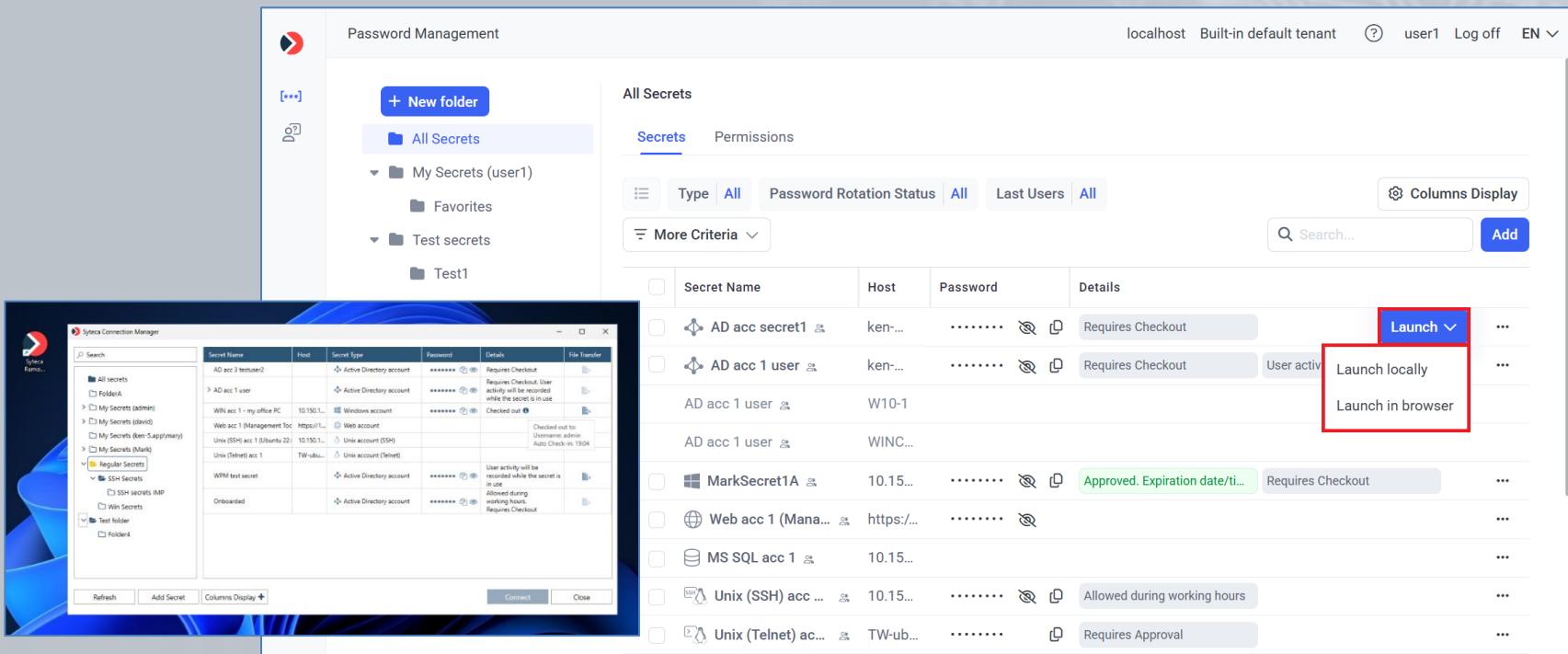
Users Who Can Approve Access

Select...

Owners or Approvers also require approval

Cancel **Save**

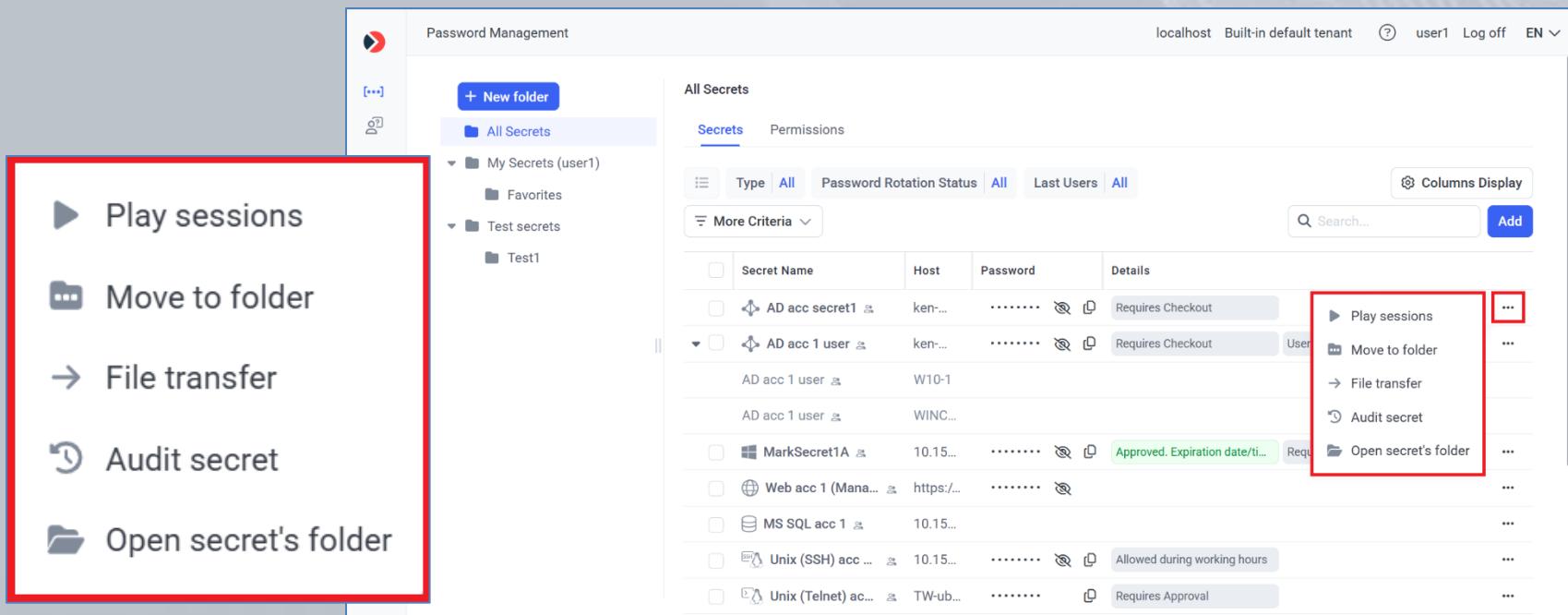
A privileged user can access a critical endpoint via a secret by using either the Web (incl. agentless PAM) or Desktop version of Syteca Connection Manager. The secrets are stored in a granular Tree-View folder structure and have user permissions for both folders and secrets.



The screenshot displays the Syteca Password Management interface. On the left, a sidebar shows a tree-view structure of secrets, including 'All secrets', 'My Secrets (user1)', 'Favorites', 'Test secrets', and 'Test1'. A 'New folder' button is also present. The main area is titled 'All Secrets' and contains a table with columns: Secret Name, Host, Secret Type, Password, Details, and File Transfer. The 'Details' column shows various secret types like Active Directory account, Web account, Unix account (SSH), and Unix account (Telnet). A 'Launch' button with a dropdown menu is highlighted, showing options: 'Launch locally' and 'Launch in browser'. A red box surrounds this dropdown. In the bottom-left corner, a smaller window titled 'Syteca Connection Manager' is open, showing a list of secrets with columns: Secret Name, Host, Secret Type, Password, Details, and File Transfer. The 'Details' column for the 'AD acc 1 user' secret shows a tooltip: 'User activity will be recorded while the secret is in use. Allowed during working hours. Requires Approval'.

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.

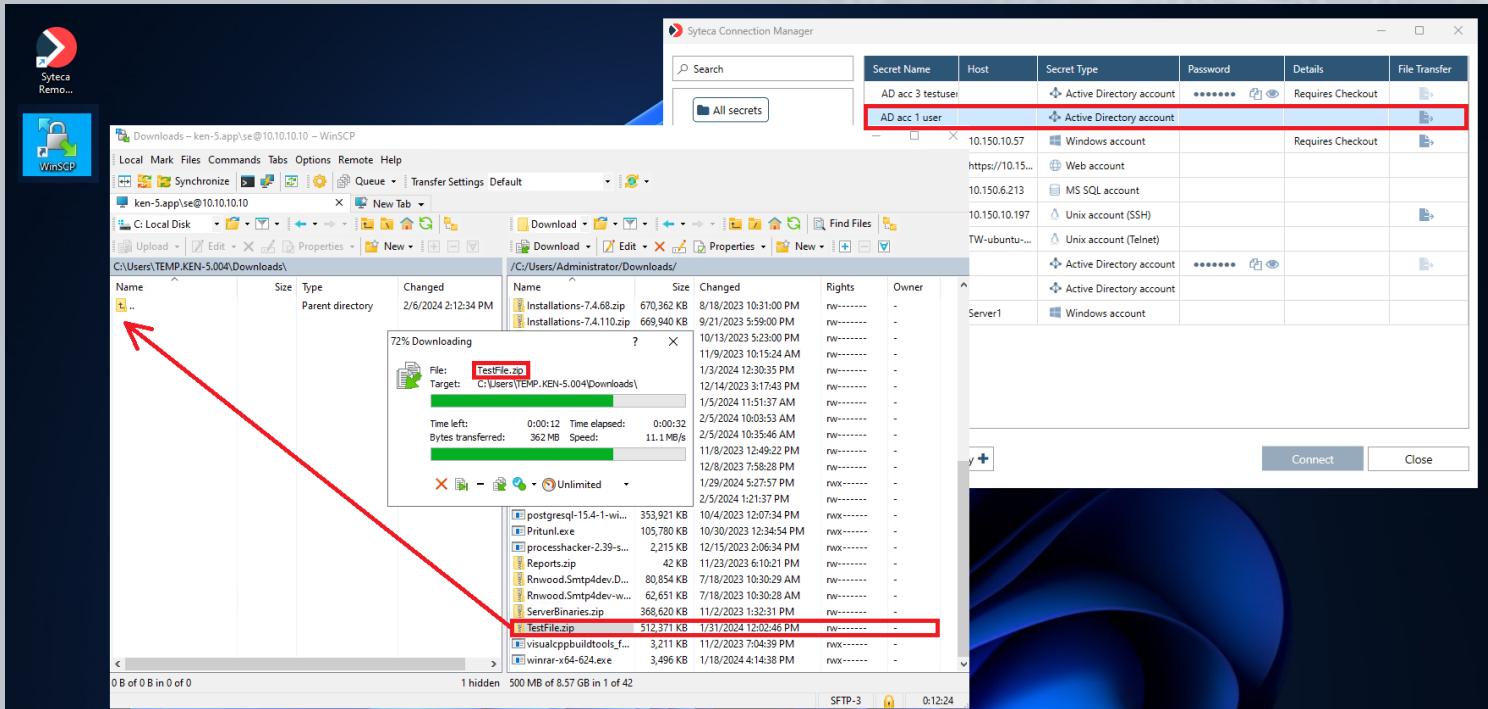


The screenshot shows the Syteca Password Management interface. On the left, a sidebar lists navigation options: 'Play sessions', 'Move to folder', 'File transfer', 'Audit secret', and 'Open secret's folder'. The main area displays a table of 'All Secrets' with columns for Secret Name, Host, Password, and Details. A specific row for 'AD acc 1 user' is selected. On the right, a context menu for this secret is open, showing options: 'Play sessions', 'Move to folder', 'File transfer', 'Audit secret', and 'Open secret's folder'. The 'Audit secret' option is highlighted with a red box.

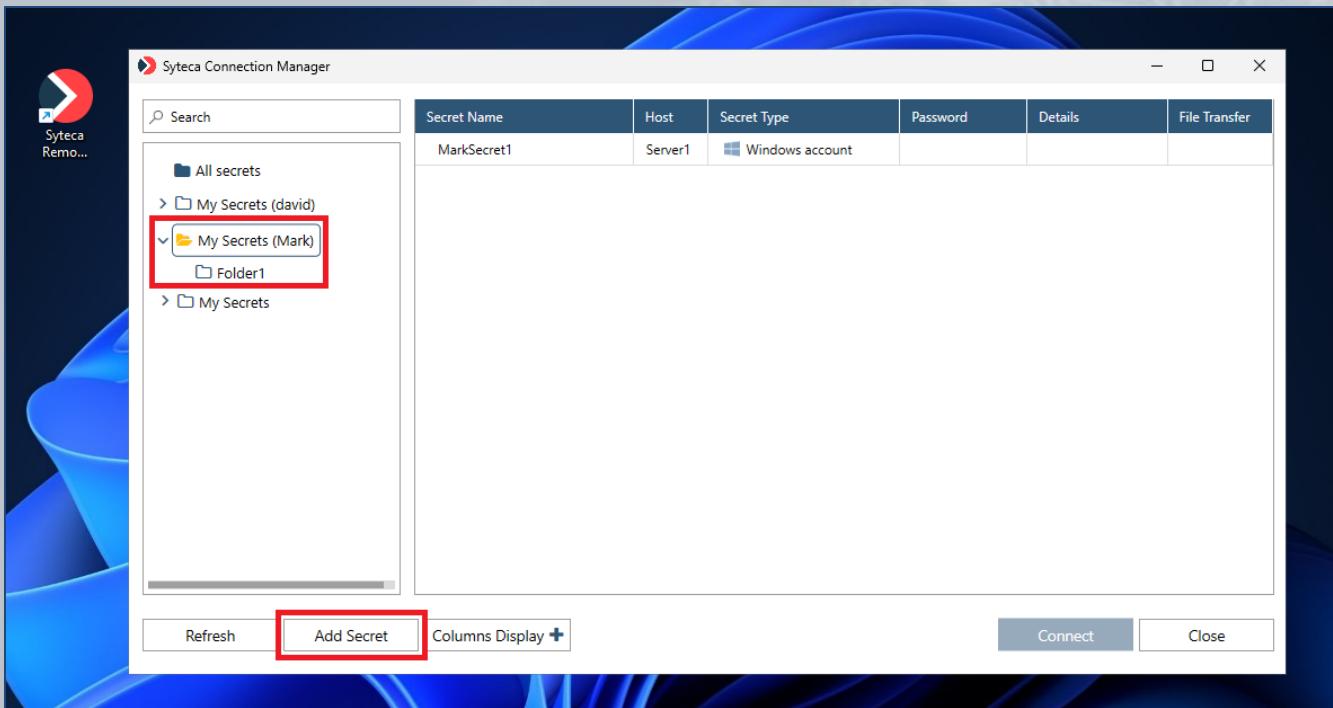
Secret Name	Host	Password	Details
AD acc 1 user	ken...	Requires Checkout
AD acc 1 user	W10-1		
AD acc 1 user	WINC...		
MarkSecret1A	10.15...	Approved. Expiration date/ti...
Web acc 1 (Manag...	https://...	
MS SQL acc 1	10.15...		
Unix (SSH) acc ...	10.15...	Allowed during working hours
Unix (Telnet) ac...	TW-ub...	Requires Approval

Transferring Files Using WinSCP

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**.

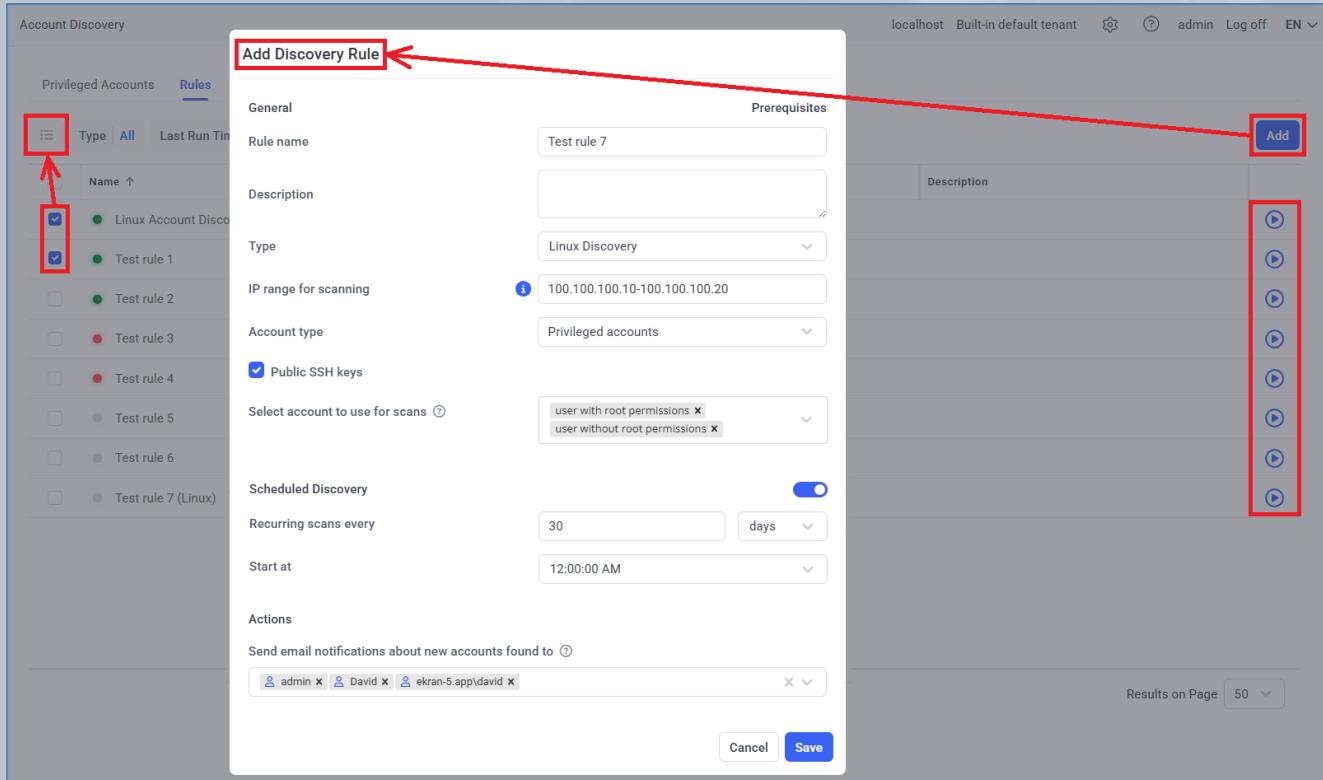


The WPM functionality enables PAM users (i.e. any **users of Syteca Connection Manager**) to **create (and manage) their own private** Workforce Password Management (**WPM**) **secrets**, which are **hidden from other users** (unless specifically shared with them).



Account Discovery and Onboarding (PAM)

Account Discovery (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**.



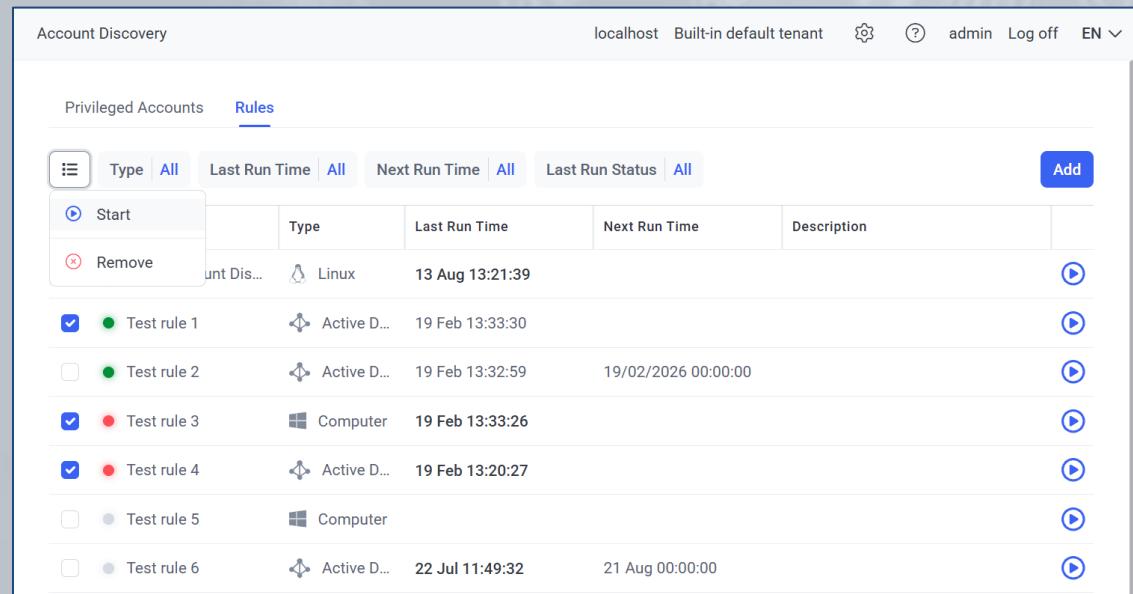
The screenshot shows the Syteca Account Discovery interface. On the left, a sidebar lists 'Privileged Accounts' and 'Rules'. The 'Rules' tab is selected, showing a table with columns for 'Name', 'Type', and 'Last Run Time'. Several rules are listed, including 'Linux Account Discovery' (green), 'Test rule 1' (green), 'Test rule 2' (grey), 'Test rule 3' (red), 'Test rule 4' (grey), 'Test rule 5' (grey), 'Test rule 6' (grey), and 'Test rule 7 (Linux)' (grey). A red box highlights the 'Add' button in the top right of the sidebar. A red arrow points from the 'Add Discovery Rule' button in the central dialog to the 'Add' button in the sidebar. The central dialog is titled 'Add Discovery Rule' and contains the following fields:

- General**
 - Rule name: Test rule 7
 - Description: (empty)
 - Type: Linux Discovery
 - IP range for scanning: 100.100.100.10-100.100.100.20
 - Account type: Privileged accounts
 - Public SSH keys
 - Select account to use for scans: user with root permissions (selected), user without root permissions
- Scheduled Discovery**
 - Recurring scans every: 30 days
 - Start at: 12:00:00 AM
- Actions**
 - Send email notifications about new accounts found to: admin, David, ekran-5.app\david

At the bottom of the dialog are 'Cancel' and 'Save' buttons. The right side of the interface shows a list of rules with a red box highlighting the 'Actions' column, which contains a series of circular icons with arrows.

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**).



The screenshot shows the 'Account Discovery' interface with the 'Rules' tab selected. The top navigation bar includes 'localhost', 'Built-in default tenant', a gear icon, 'admin', 'Log off', and 'EN'. The main area has a table titled 'Privileged Accounts' with columns: Start, Type, Last Run Time, Next Run Time, and Description. The table lists the following rules:

Start	Type	Last Run Time	Next Run Time	Description
Start				
Remove	unt Dis...	Linux	13 Aug 13:21:39	
<input checked="" type="checkbox"/>	Test rule 1	Active D...	19 Feb 13:33:30	
<input type="checkbox"/>	Test rule 2	Active D...	19 Feb 13:32:59	19/02/2026 00:00:00
<input checked="" type="checkbox"/>	Test rule 3	Computer	19 Feb 13:33:26	
<input checked="" type="checkbox"/>	Test rule 4	Active D...	19 Feb 13:20:27	
<input type="checkbox"/>	Test rule 5	Computer		
<input type="checkbox"/>	Test rule 6	Active D...	22 Jul 11:49:32	21 Aug 00:00:00

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

Onboard Accounts

 Properties  Automation

General

Secret Name 

Current folder: All Secrets

Password Settings

Use automatically generated password

Use current password

Specify new password manually

Account(s) for Rotation

Select secret

user with root permissions user without root permission

Account Discovery localhost Built-in default tenant   admin Log off EN 

Privileged Accounts Rules

 Active Directory (84/91)  Windows Local (105/111)  Linux (7/11)

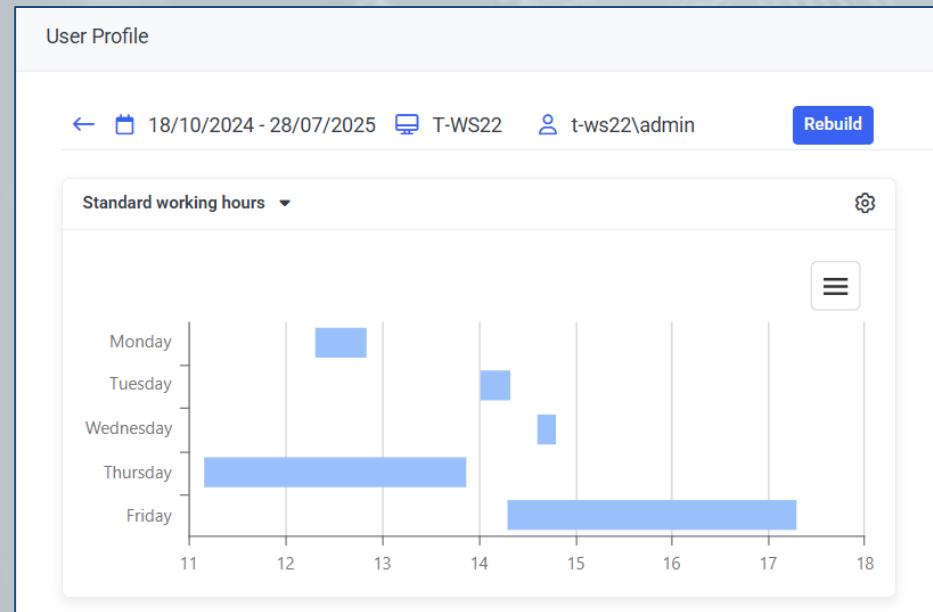
 Status	All	Computers	All	Discovery Rule	All	Account type	All	 Search...	 Hide managed
 Onboard									
 Remove									
 Skip									
 Restore to Unmanaged									
ubuntu	Computer acco...	ubuntu							
ubuntu1	Computer acco...	ubuntu1							
root	Public key	root							
<input checked="" type="checkbox"/> sys	Service account	sys							
<input checked="" type="checkbox"/> sync	Service account	sync							
<input type="checkbox"/> secret1	Service account	secret1							
<input type="checkbox"/> user	Public key	user							

User and Entity Behavior Analytics (UEBA)

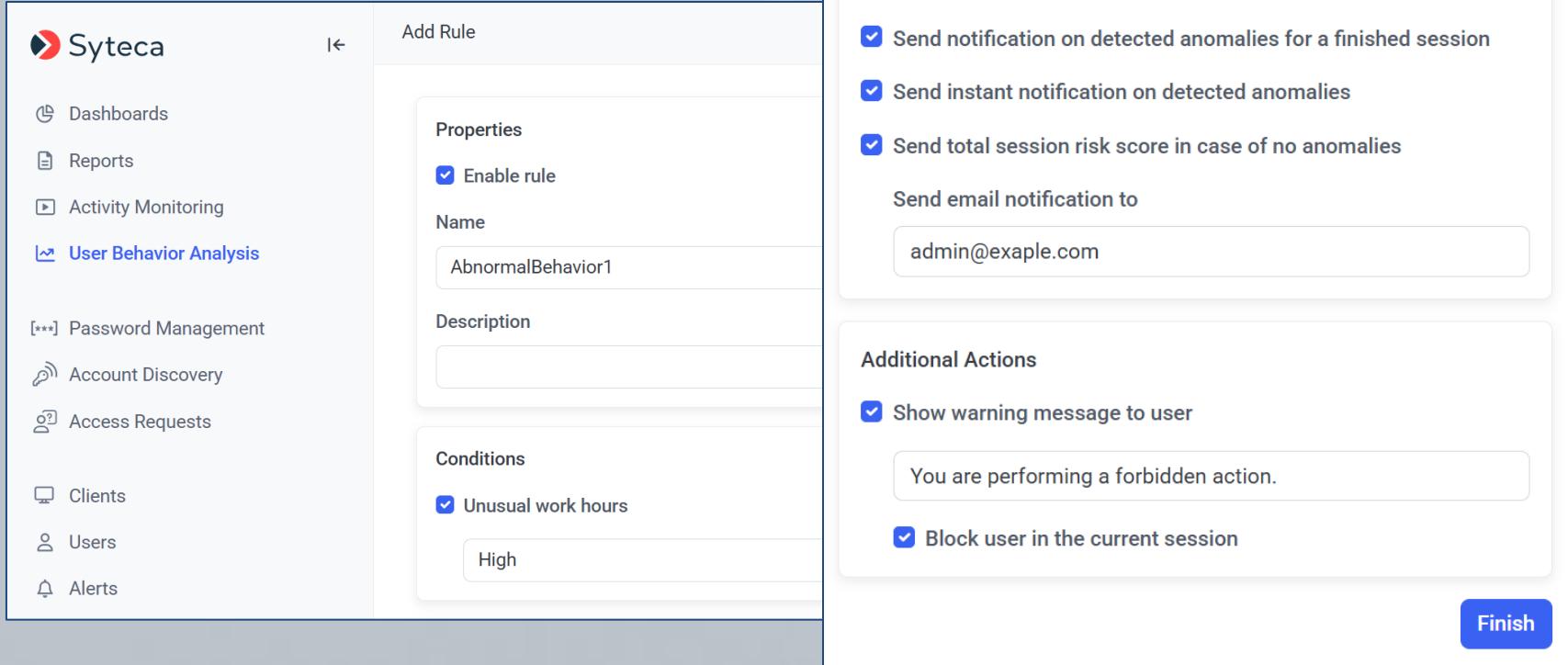
Syteca User & Entity Behavior Analytics (UEBA) allows you to **better protect your system** from malicious and illicit insiders.

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**.



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



The image shows a screenshot of the Syteca platform interface. On the left, there is a sidebar with various navigation options: Dashboards, Reports, Activity Monitoring, User Behavior Analysis (which is selected and highlighted in blue), Password Management, Account Discovery, Access Requests, Clients, Users, and Alerts. The main content area is titled 'Add Rule' and contains several configuration sections:

- Properties**:
 - Enable rule
 - Name**: AbnormalBehavior1
 - Description**: (empty text input field)
- Conditions**:
 - Unusual work hours
 - High (radio button selection)
- Email Notifications**:
 - Send notification on detected anomalies for a finished session
 - Send instant notification on detected anomalies
 - Send total session risk score in case of no anomalies

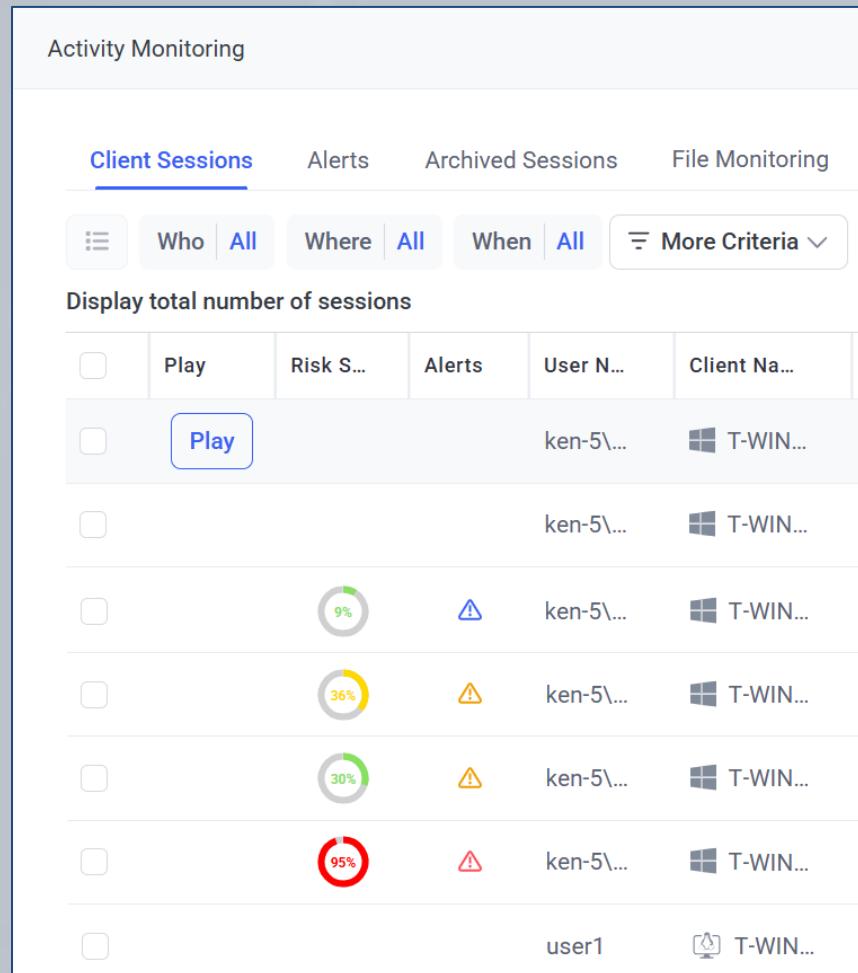
Send email notification to: admin@example.com
- Additional Actions**:
 - Show warning message to user

You are performing a forbidden action.
 - Block user in the current session

At the bottom right of the configuration window is a blue 'Finish' button.

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

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

Access Requests

localhost Built-in default tenant   admin Log off EN ▾

Access Requests Two-Factor Authentication Endpoint Access Control

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

User	User Type	Assigned to	Restriction Type	Time Added	Added by	
ken-5.app\guest	Active Directory user	ken-5.app\ubuntu-2404-h	Email to administrator	11/08/2025 15:36:42	admin  	
t-win11\david	Local computer user		Access on schedule (11/08/2025 - 25/08/2025, 08:00 - 17:00, Mo, Tu, We, Th, Fr)	11/08/2025 15:37:25	admin  	
tester	Linux User	Any computer	Email to administrator	11/08/2025 15:38:05	admin  	

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.

Edit User

 General  Restriction Types

Do User with Restricted Access Rights

User type: Active Directory user

Domain: ken-5.app User / User group: guest

 Accessed Computer with Installed Client

Computer type: Selected computer

Domain: ken-5.app Computer / Computer group: ubuntu-2404-h

 Users who can approve access

User / User group: ADMIN

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

Edit User

 General  **Restriction Types**

 **Restriction Type**

Always require approval on login

Allow access without approval during work hours

Allowed Dates

From:  To: 

Allowed Time

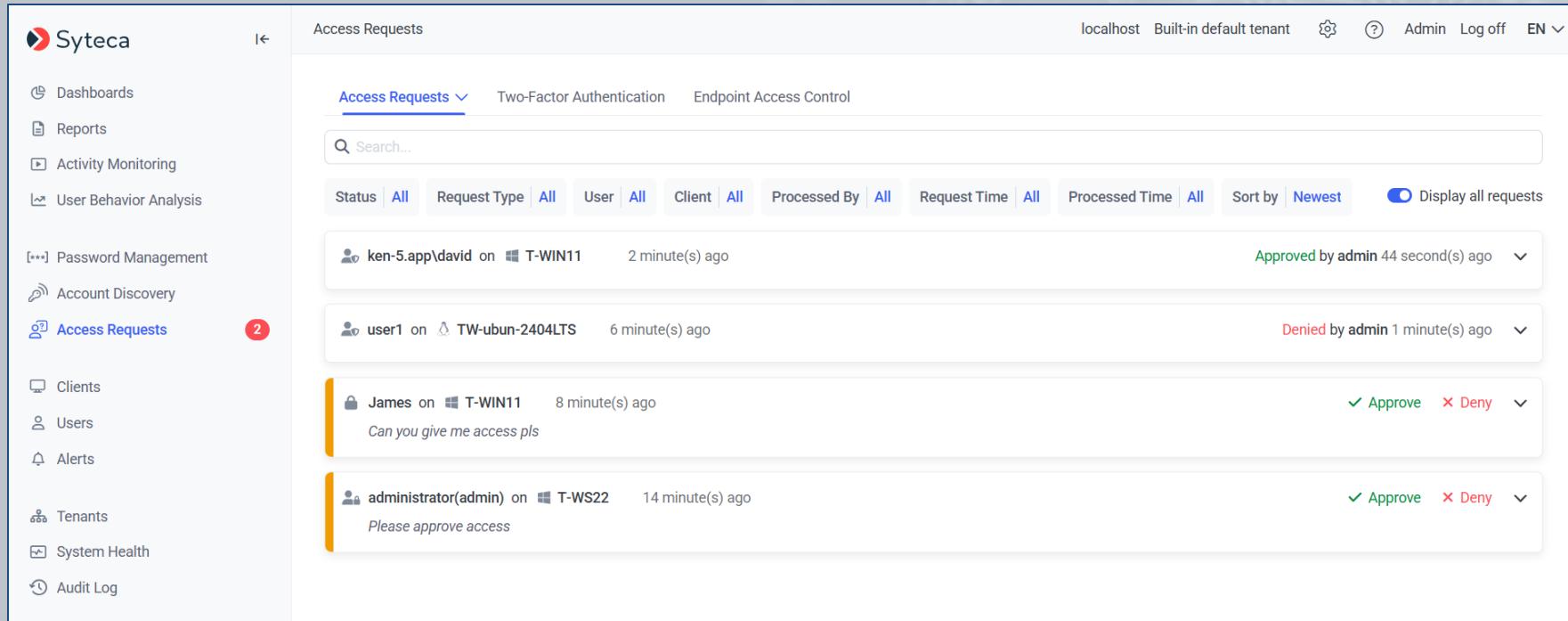
From:  To: 

Allowed Weekdays

Su Mo Tu We Th Fr Sa

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).



The screenshot shows the Syteca interface with the 'Access Requests' tab selected. The main area displays a list of pending access requests:

User	Client	Time Ago	Status	Action
ken-5.app\david	T-WIN11	2 minute(s) ago	Approved	Approved by admin 44 second(s) ago
user1	TW-ubun-2404LTS	6 minute(s) ago	Denied	Denied by admin 1 minute(s) ago
James	T-WIN11	8 minute(s) ago		✓ Approve ✖ Deny
administrator(admin)	T-WS22	14 minute(s) ago		✓ Approve ✖ Deny

The 'Access Requests' tab has a red notification badge with the number '2'.

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



Your access request has been sent to the administrator. Please wait while the administrator grants you an access.

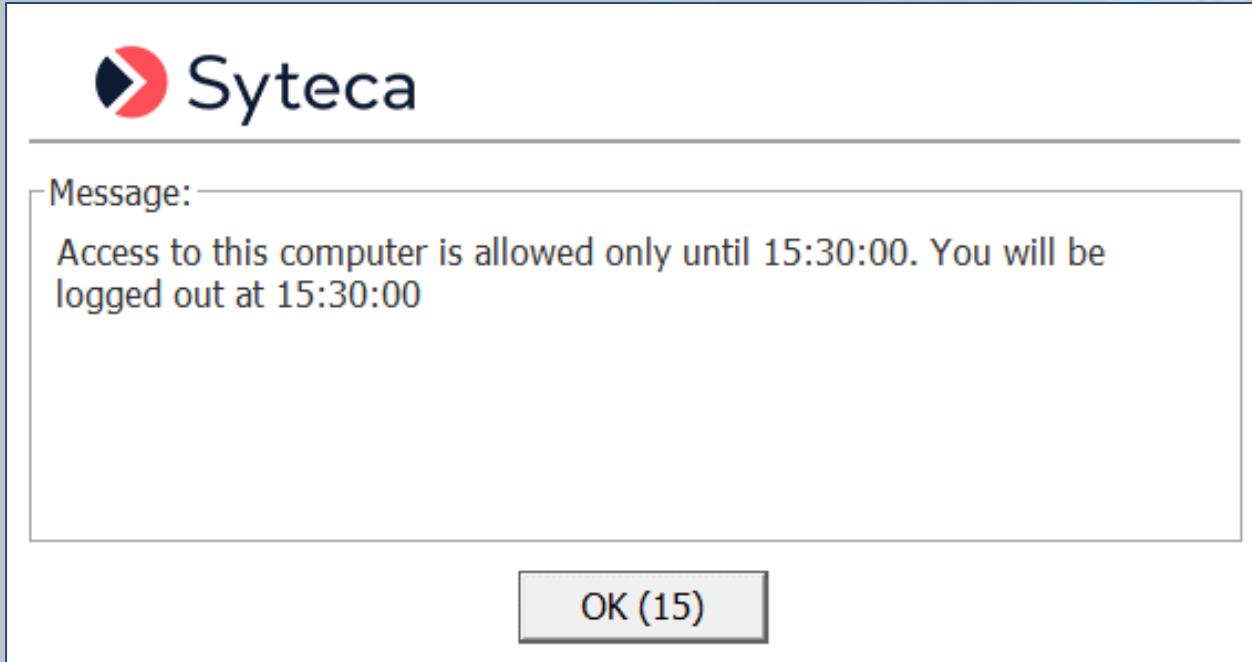


Your access request has been approved by the administrator. Click OK to continue.

OK

Cancel

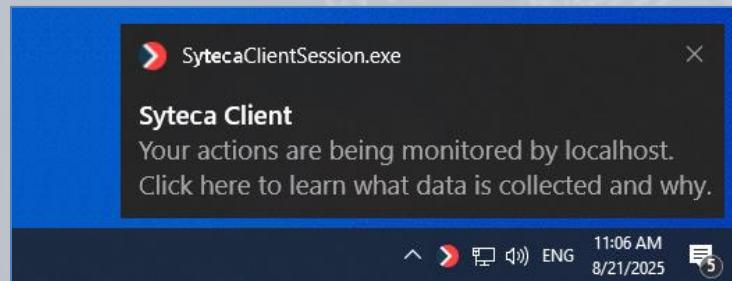
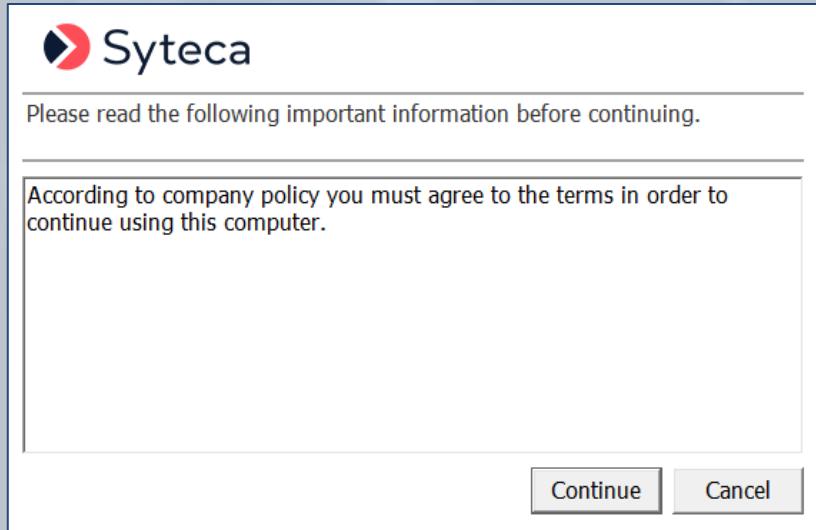
Restricted users will be able to **log in** to Client computers **only during the defined time period**, and will need **additional approval** to log in **outside of this period**.



Notifying Users About Being Monitored

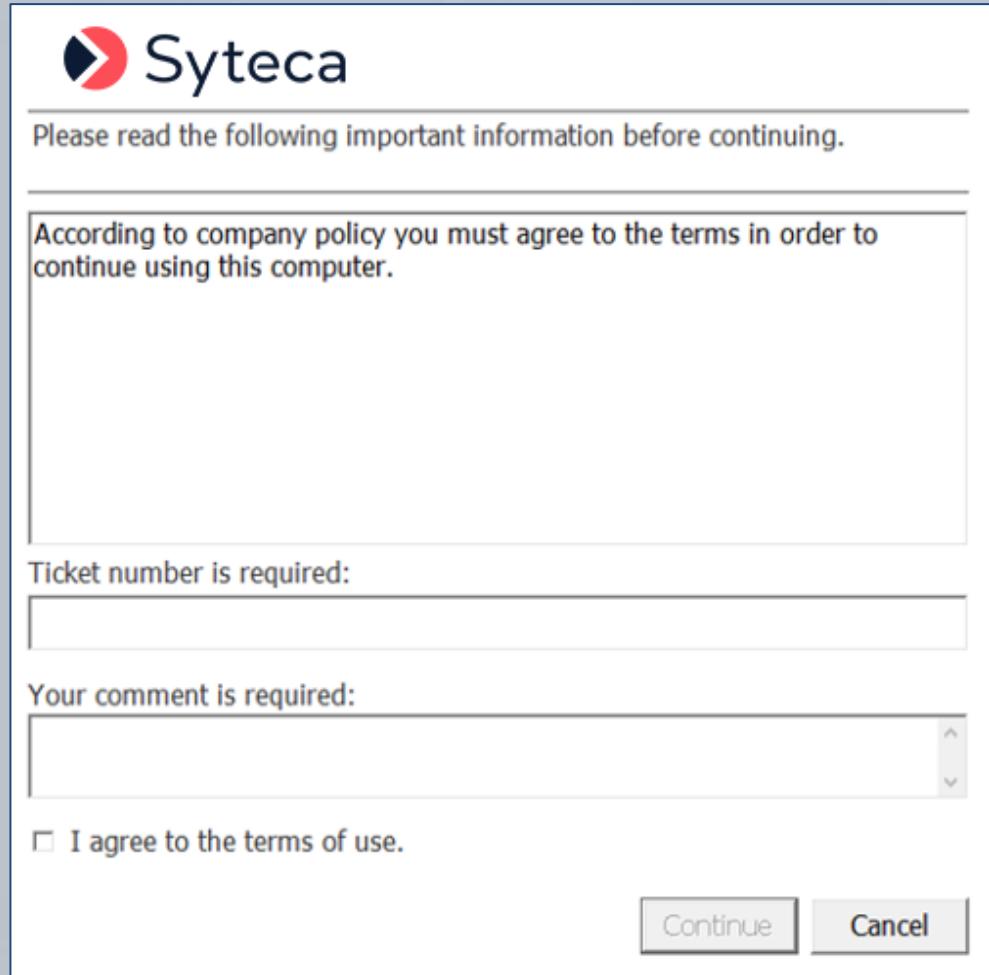
To adhere to the **security policy** of your company or your **country regulations**, you can:

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



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

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



The image shows a screenshot of a web-based application interface. At the top, the Syteca logo is displayed. Below it, a message reads: "Please read the following important information before continuing." A text box contains the message: "According to company policy you must agree to the terms in order to continue using this computer." Below this, there are two input fields: one for a "Ticket number" and one for a "Your comment". At the bottom, there is a checkbox labeled "I agree to the terms of use." and two buttons: "Continue" and "Cancel".

Notifying Users about Being Monitored



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

Editing Client (T-WIN11)

← Client Settings Client Groups Permissions Assigned Alerts

Change the Settings Type to Custom to edit the Client.

Properties User Activity Recording Monitoring [Windows/macOS] Application Filtering User Filtering
Keystroke Monitoring Additional Options Privacy Settings

Authentication Options

Enable displaying of additional message
According to company policy you must agree to the terms in order to continue using this computer.

Customize message header
Please read the following important information before continuing.

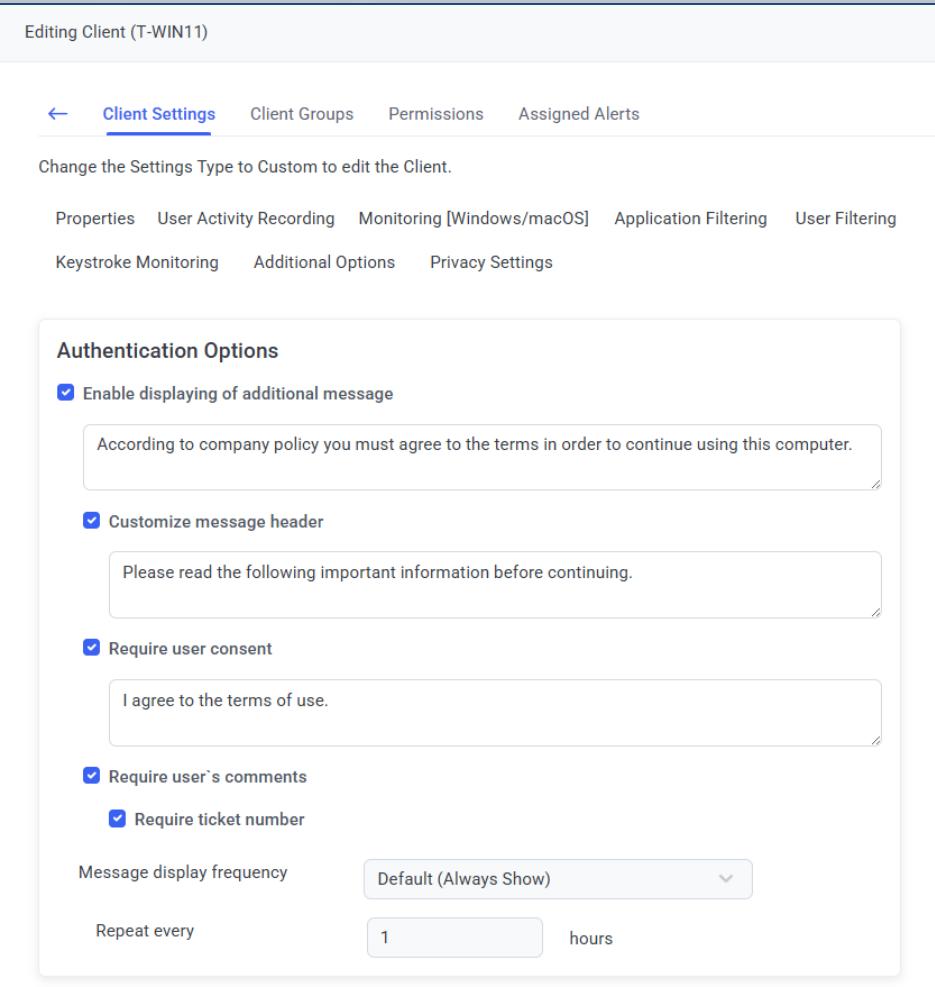
Require user consent
I agree to the terms of use.

Require user's comments

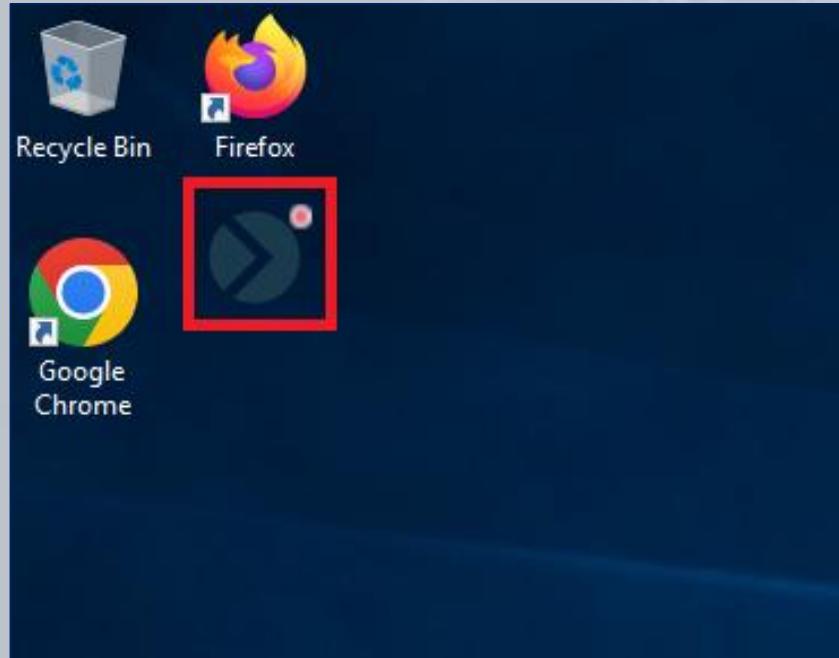
Require ticket number

Message display frequency: Default (Always Show)

Repeat every: 1 hours



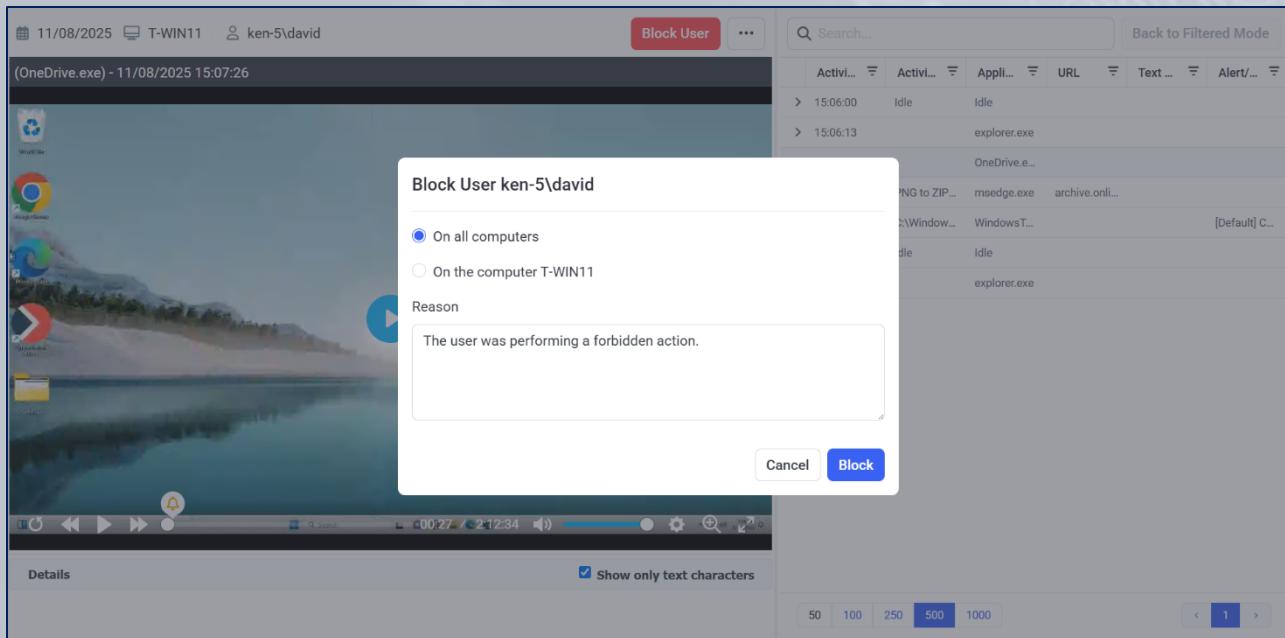
- A movable **icon** can also be displayed on the desktop (that is always on top of all applications opened) to **inform users** that **their actions** are currently **being monitored and recorded**.



Blocking Users

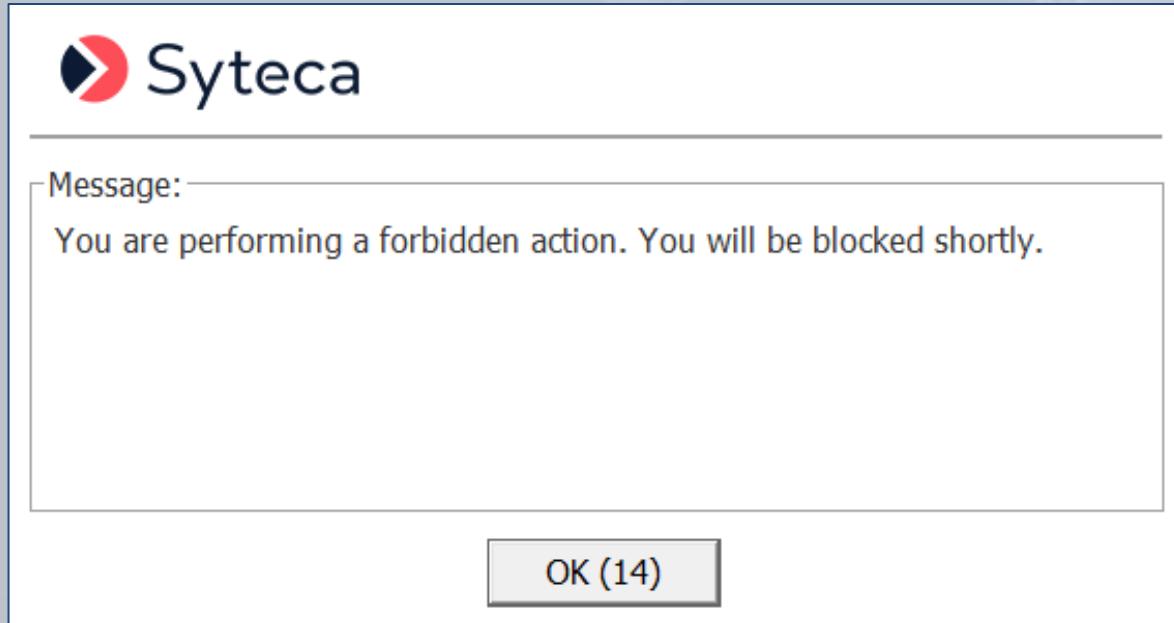
Syteca allows you to **block endpoint users** from performing potentially harmful and forbidden actions on computers running Windows OS with Syteca Clients installed on them.

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



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.



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

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

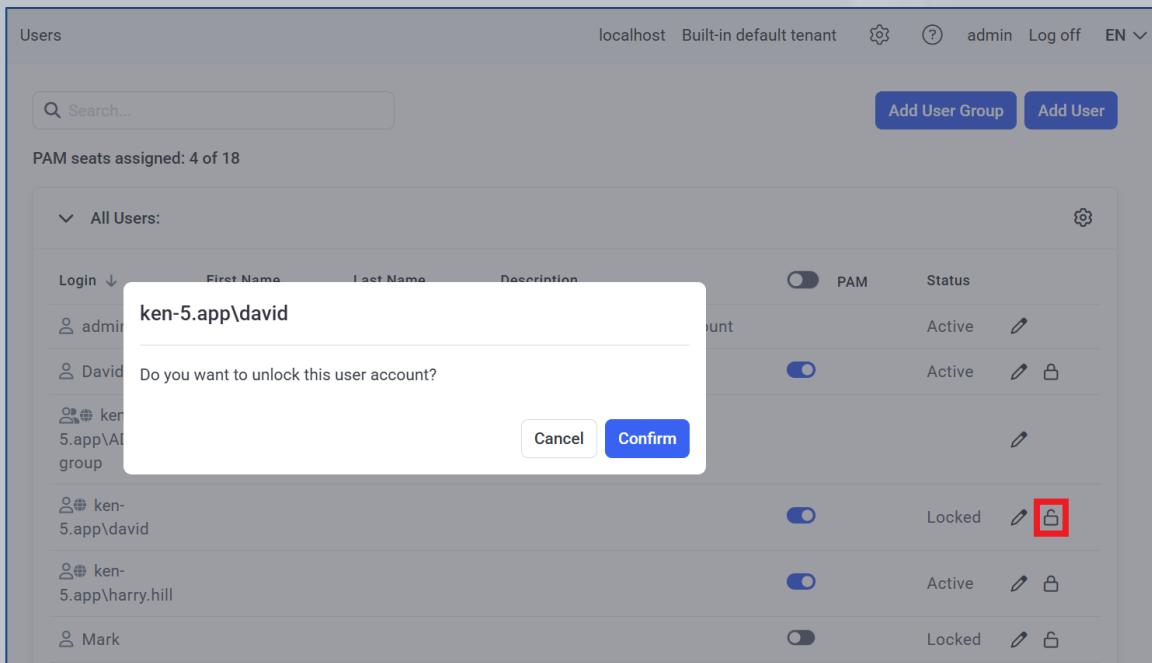
Blocked Users List					
		localhost		Built-in default tenant	
User	Blocked On	Blocked By	Date	Reason	Remove All
t-win11\ken-user	TW-WIN11	admin	13/08/2025 13:31:10 +03:00	The user was performing a forbidden action.	
T-WIN11\James	All computers	admin	13/08/2025 13:31:34 +03:00	The user was performing a forbidden action.	
ken-5.app\david(user3)	TW-WIN11	admin	13/08/2025 13:32:20 +03:00	The user was performing a forbidden action.	

Locking Management Tool User Accounts

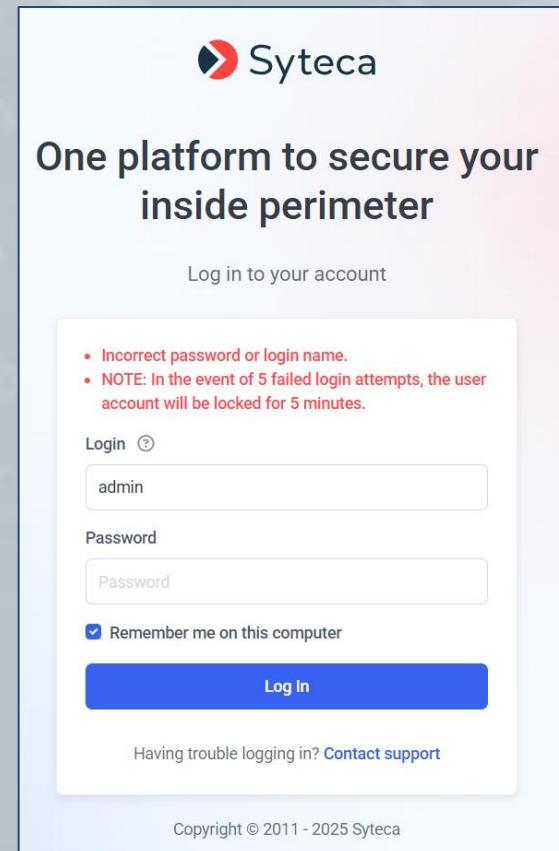


The accounts of Syteca **Management Tool users** can also be **automatically locked** (for a specific duration) if they **enter incorrect login credentials multiple times**.

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



The screenshot shows the Syteca Management Tool's user management interface. A modal window is open for the user 'ken-5.app\david'. The modal asks, 'Do you want to unlock this user account?' with 'Cancel' and 'Confirm' buttons. In the background, the user list shows several other users, including 'admin', 'David', and 'Mark'. Some users have their accounts locked, indicated by a red lock icon in the 'Status' column.

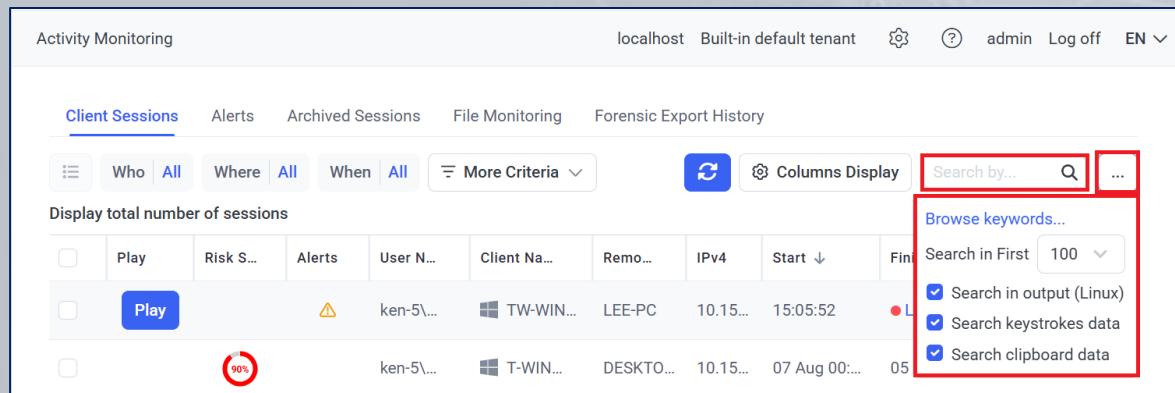


The screenshot shows the Syteca login page. It features a note: 'One platform to secure your inside perimeter' and a 'Log in to your account' button. Below the button, a note states: 'Incorrect password or login name. NOTE: In the event of 5 failed login attempts, the user account will be locked for 5 minutes.' The login form includes fields for 'Login' (with 'admin' entered), 'Password', and a 'Remember me on this computer' checkbox, followed by a 'Log In' button. At the bottom, there's a link 'Having trouble logging in? Contact support' and a copyright notice 'Copyright © 2011 - 2025 Syteca'.

Viewing Client Sessions

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

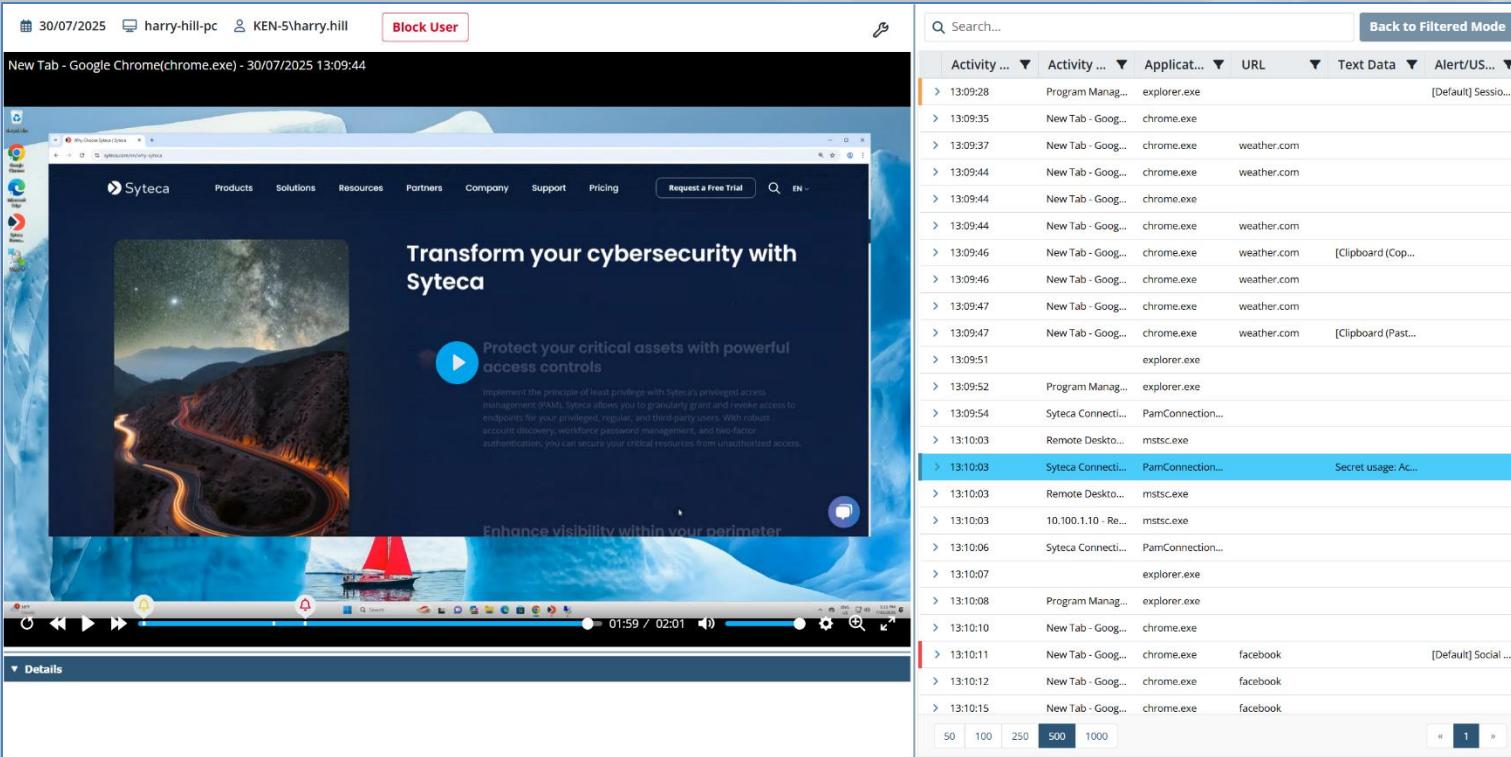
- **For Windows Clients:** active window title, application name, user name, Client name, URL visited, keystrokes, clipboard data, user's comment in additional message, ticket number, USB device info, etc.
- **For macOS Clients:** active window title, application name, user name, Client name, URL visited,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



The screenshot shows the 'Activity Monitoring' interface of the Syteca Management Tool. The 'Client Sessions' tab is selected. At the top, there are filters for 'Who' (All), 'Where' (All), and 'When' (All), along with a 'More Criteria' dropdown. To the right of these filters are buttons for 'Columns Display' and a search bar labeled 'Search by...'. A red box highlights the search bar and the 'Columns Display' button. Below the filters, a table displays session data with columns for session ID, Play button, Risk Score, Alerts, User Name, Client Name, Remote IP, Start Date, and End Date. The first row shows a session for 'Play' with a risk score of 90%. A red box highlights the 'Play' button in this row. To the right of the table, there is a 'Browse keywords...' dropdown menu with several search options, also highlighted with a red box. The options include 'Search in First' (set to 100), 'Search in output (Linux)', 'Search keystrokes data', and 'Search clipboard data'. The bottom right corner of the interface shows the number '05'.

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**.

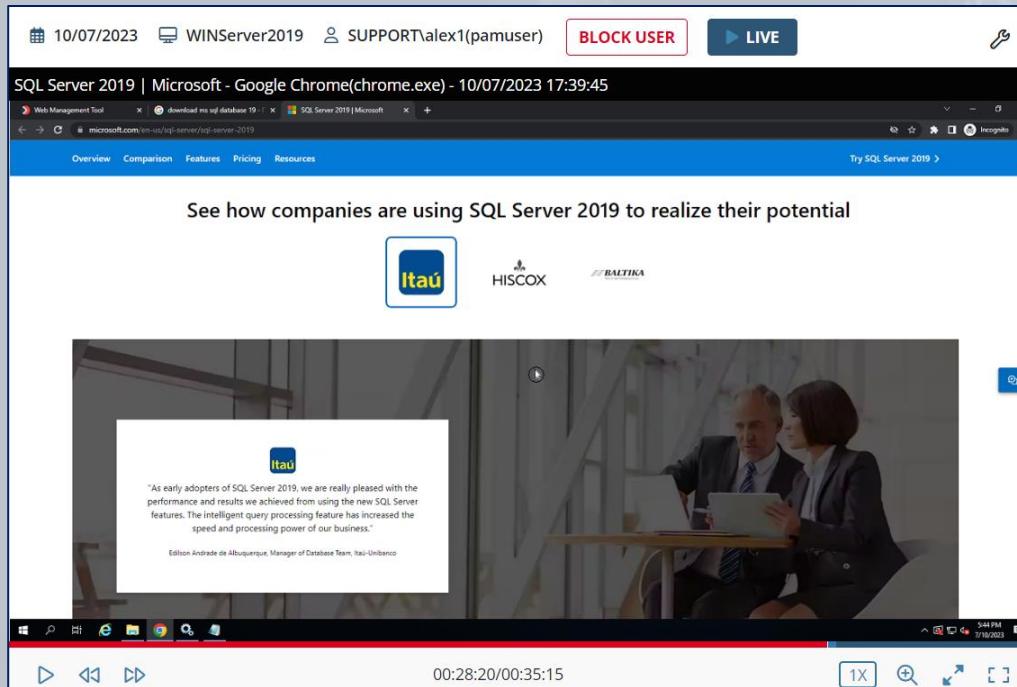


The image shows the Syteca Session Viewer interface. On the left, a video player displays a recorded session of a user interacting with a Syteca website. The video player has a timestamp of 01:59 / 02:01. On the right, a timeline table lists system events with columns for Activity, Application, URL, and Text Data. A specific event at 13:10:03 is highlighted in blue, indicating a 'Secret usage' alert.

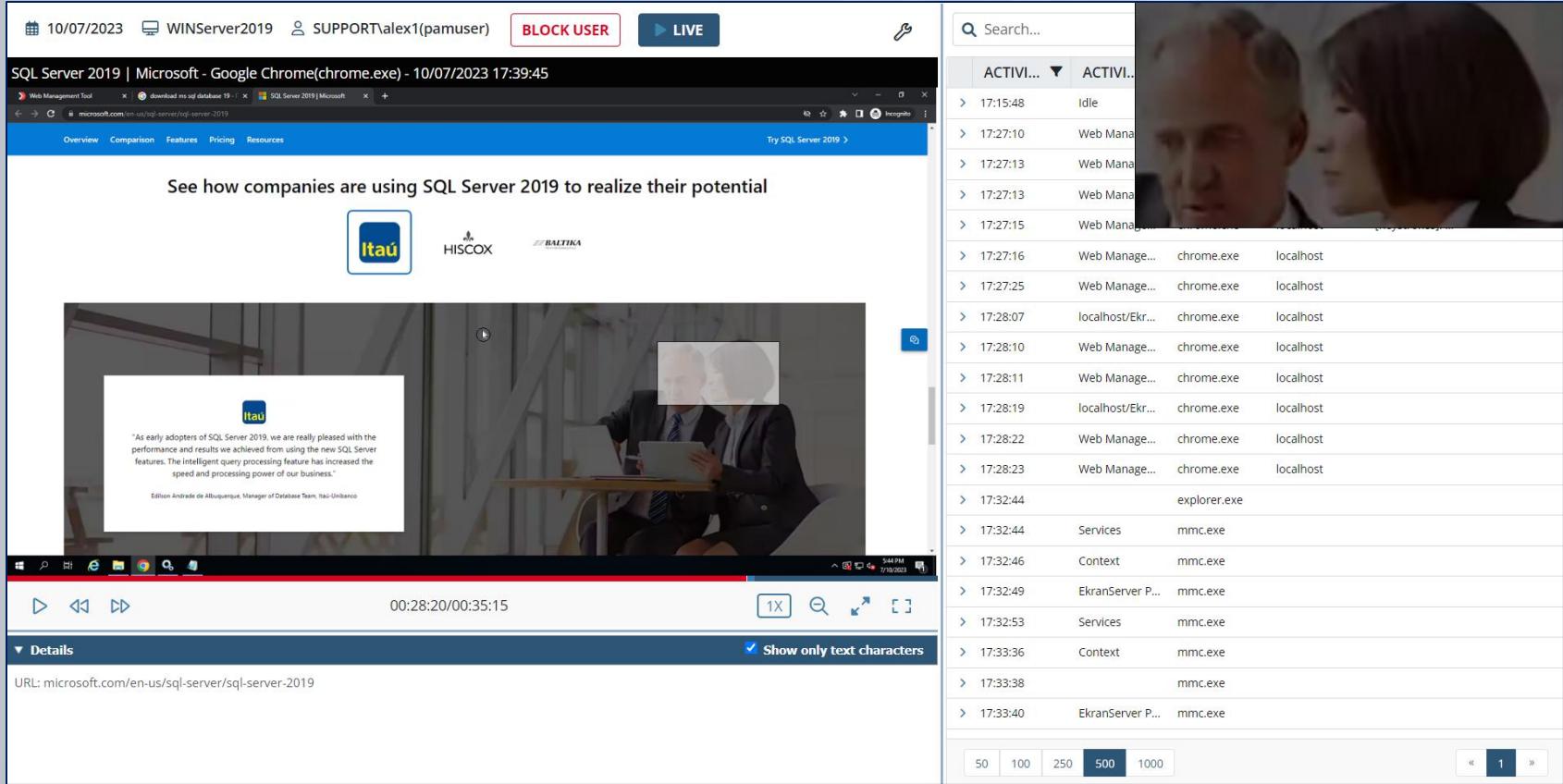
Activity ...	Application ...	URL	Text Data	Alert/US...
13:09:28	Program Manager	explorer.exe		[Default] Session
13:09:35	New Tab - Google Chrome	chrome.exe		
13:09:37	New Tab - Google Chrome	chrome.exe	weather.com	
13:09:44	New Tab - Google Chrome	chrome.exe	weather.com	
13:09:44	New Tab - Google Chrome	chrome.exe	weather.com	
13:09:44	New Tab - Google Chrome	chrome.exe	weather.com	
13:09:46	New Tab - Google Chrome	chrome.exe	weather.com	[Clipboard (Copy)]
13:09:46	New Tab - Google Chrome	chrome.exe	weather.com	
13:09:47	New Tab - Google Chrome	chrome.exe	weather.com	
13:09:47	New Tab - Google Chrome	chrome.exe	weather.com	[Clipboard (Paste)]
13:09:51		explorer.exe		
13:09:52	Program Manager	explorer.exe		
13:09:54	Syteca Connect	PamConnection...		
13:10:03	Remote Desktop	mstsc.exe		
13:10:03	Syteca Connect	PamConnection...	Secret usage: Ac...	
13:10:03	Remote Desktop	mstsc.exe		
13:10:03	10.100.1.10 - Remote Desktop	mstsc.exe		
13:10:06	Syteca Connect	PamConnection...		
13:10:07		explorer.exe		
13:10:08	Program Manager	explorer.exe		
13:10:10	New Tab - Google Chrome	chrome.exe		
13:10:11	New Tab - Google Chrome	chrome.exe	facebook	[Default] Social
13:10:12	New Tab - Google Chrome	chrome.exe	facebook	
13:10:15	New Tab - Google Chrome	chrome.exe	facebook	

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).



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

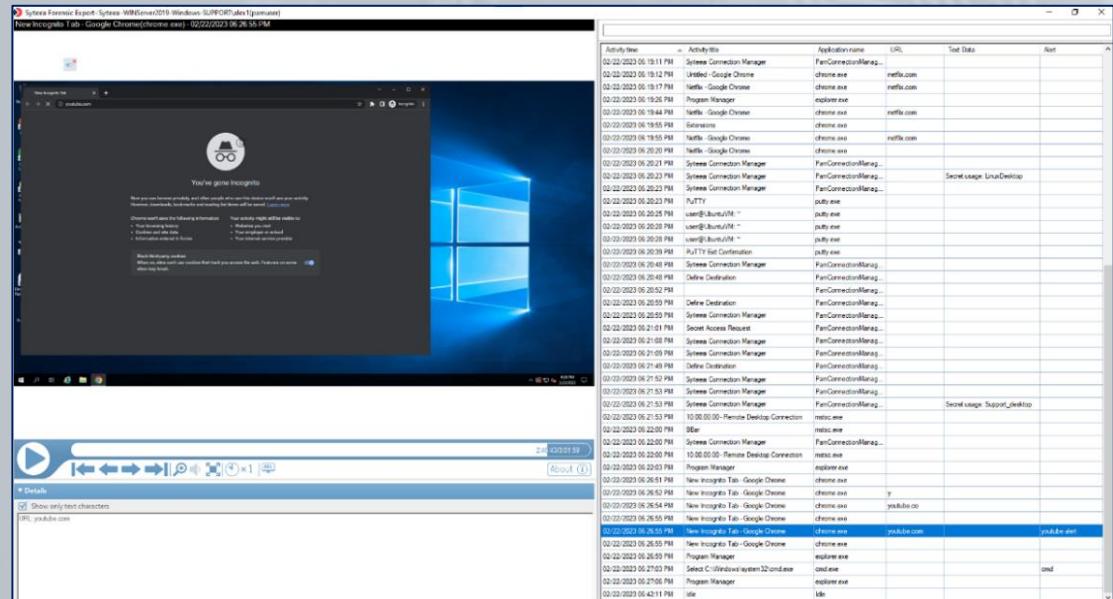


The screenshot shows the Syteca Session Player interface. On the left, a video player displays a scene from a video. A magnifying glass icon is overlaid on the video, indicating an enlarged view of a specific area. The video content shows two people in a professional setting. The timeline pane on the right lists system events with timestamps, file paths, and process names. The timeline shows activity from 17:15:48 to 17:33:40, with most entries being "Web Manage..." events for chrome.exe on localhost. The interface includes a search bar, a "BLOCK USER" button, and a "LIVE" button at the top.

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

Forensic Export

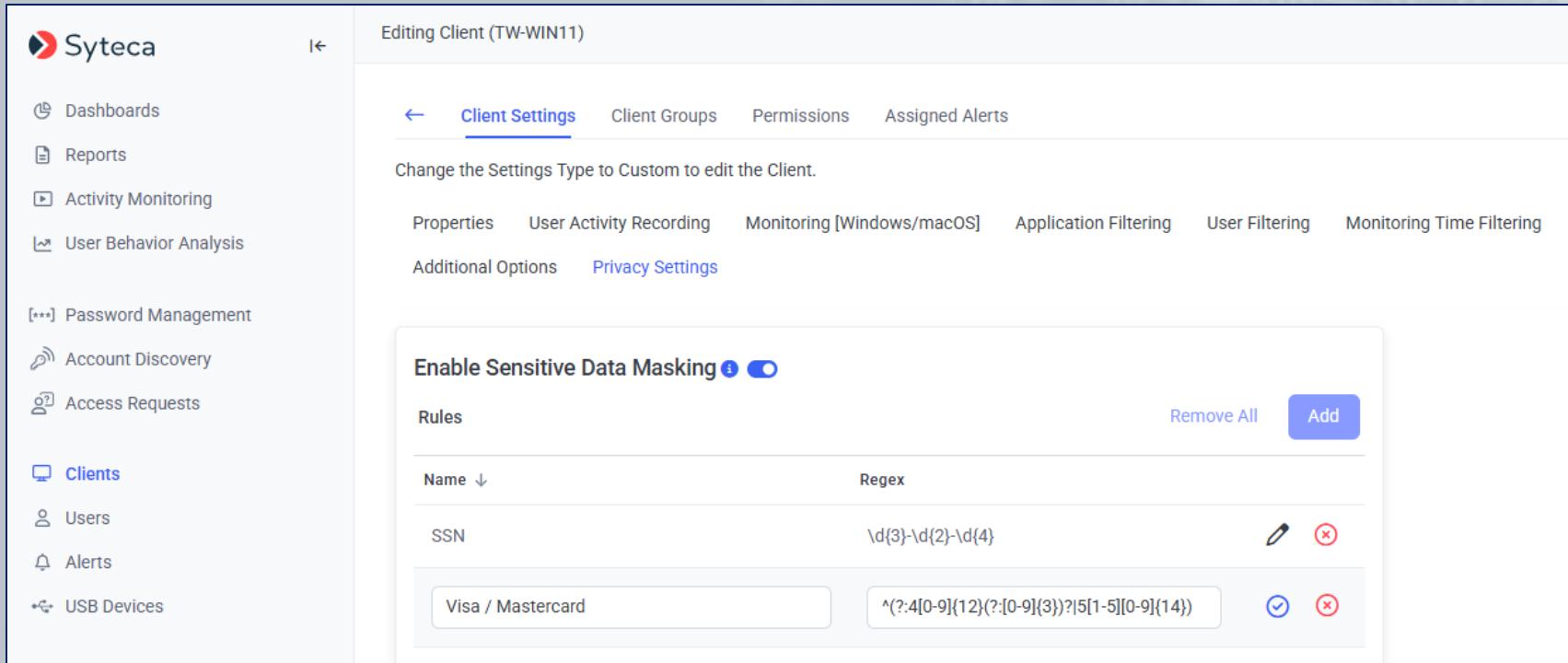
With Syteca **Forensic Export**, you can:



Sensitive Data Masking

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

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.



Editing Client (TW-WIN11)

Client Settings Client Groups Permissions Assigned Alerts

Change the Settings Type to Custom to edit the Client.

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

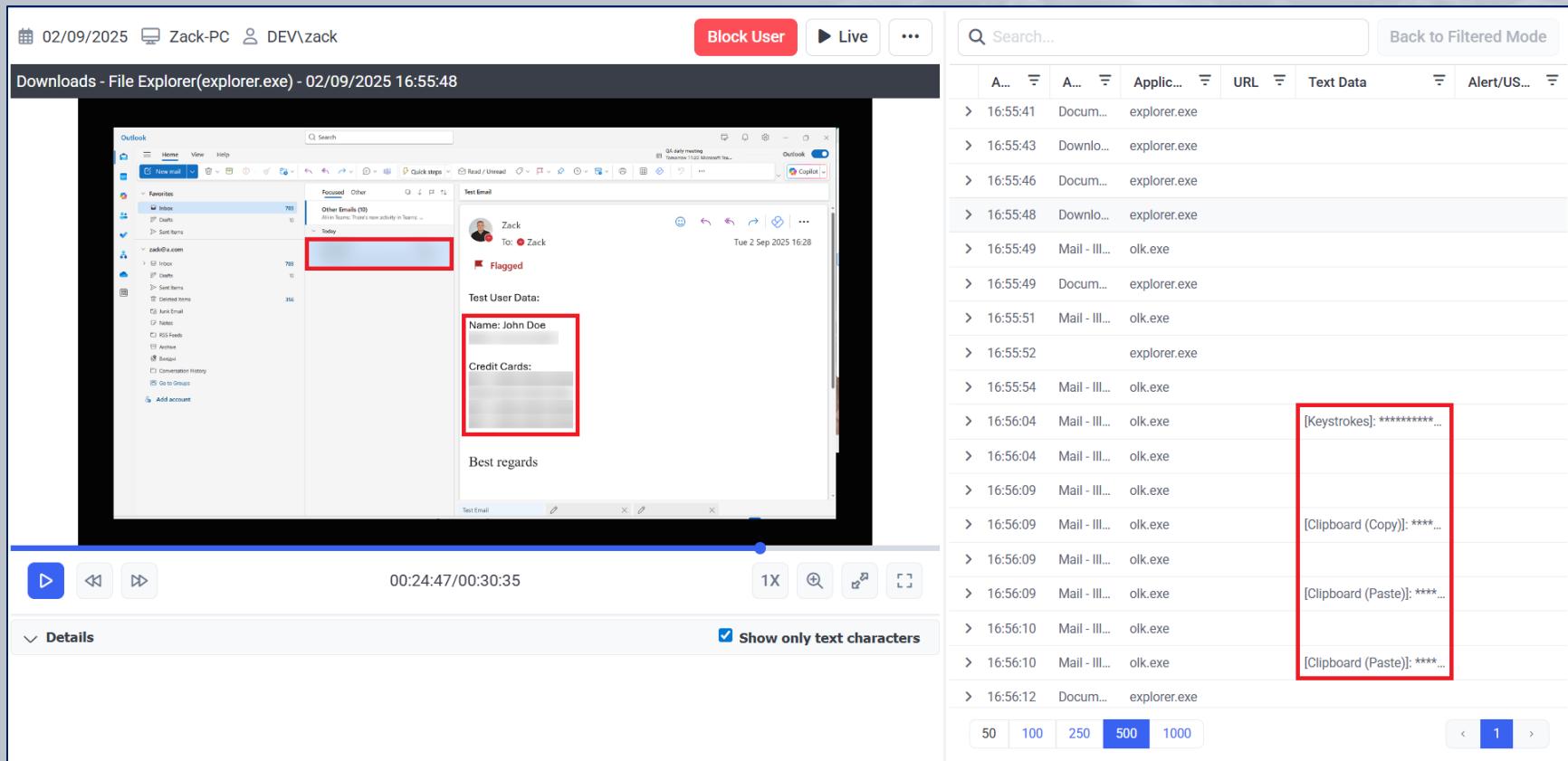
Additional Options Privacy Settings

Enable Sensitive Data Masking

Name	Regex	Actions
SSN	\d{3}-\d{2}-\d{4}	 
Visa / Mastercard	^(?>4[0-9]{12}(?:[0-9]{3})? 5[1-5][0-9]{14})	 

Sensitive Data Masking

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



02/09/2025 Zack-PC DEV\zack

Block User Live ...

Search... Back to Filtered Mode

Downloads - File Explorer(explorer.exe) - 02/09/2025 16:55:48

Outlook

Focused Other

Test Email

Zack To: Zack

Flagged

Tue 2 Sep 2025 16:28

Test User Data:

Name: John Doe

Credit Cards:

Best regards

00:24:47/00:30:35 1X

Details Show only text characters

A... A... Applic... URL Text Data Alert/US...

16:55:41 Docum... explorer.exe

16:55:43 Downlo... explorer.exe

16:55:46 Docum... explorer.exe

16:55:48 Downlo... explorer.exe

16:55:49 Mail - III... olk.exe

16:55:49 Docum... explorer.exe

16:55:51 Mail - III... olk.exe

16:55:52 explorer.exe

16:55:54 Mail - III... olk.exe

16:56:04 Mail - III... olk.exe

16:56:04 Mail - III... olk.exe

16:56:09 Mail - III... olk.exe

16:56:09 Mail - III... olk.exe

16:56:09 Mail - III... olk.exe

16:56:10 Mail - III... olk.exe

16:56:10 Mail - III... olk.exe

16:56:12 Docum... explorer.exe

[Keystrokes]: *****

[Clipboard (Copy)]: ****

[Clipboard (Paste)]: ****

[Clipboard (Paste)]: ****

50 100 250 500 1000 1 >

Pseudonymizer

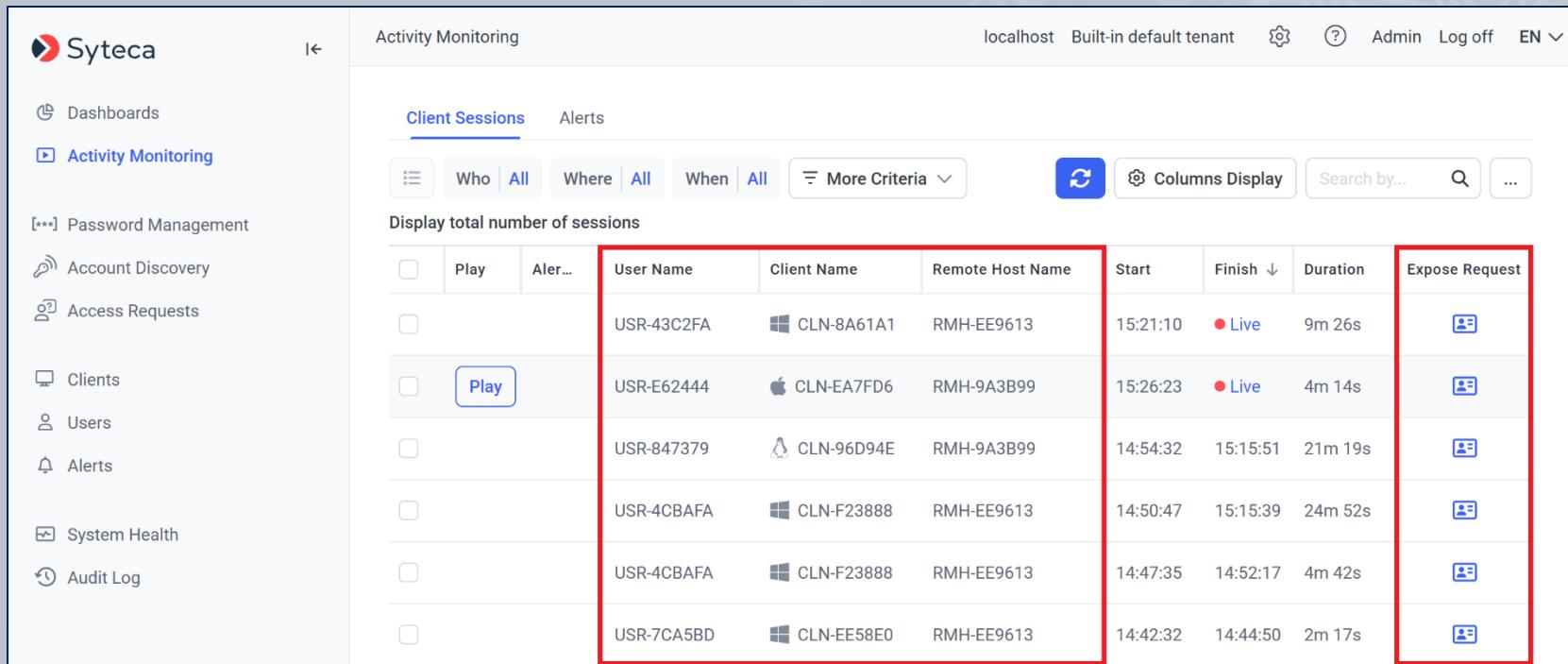
(for GDPR compliance, etc.)

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.



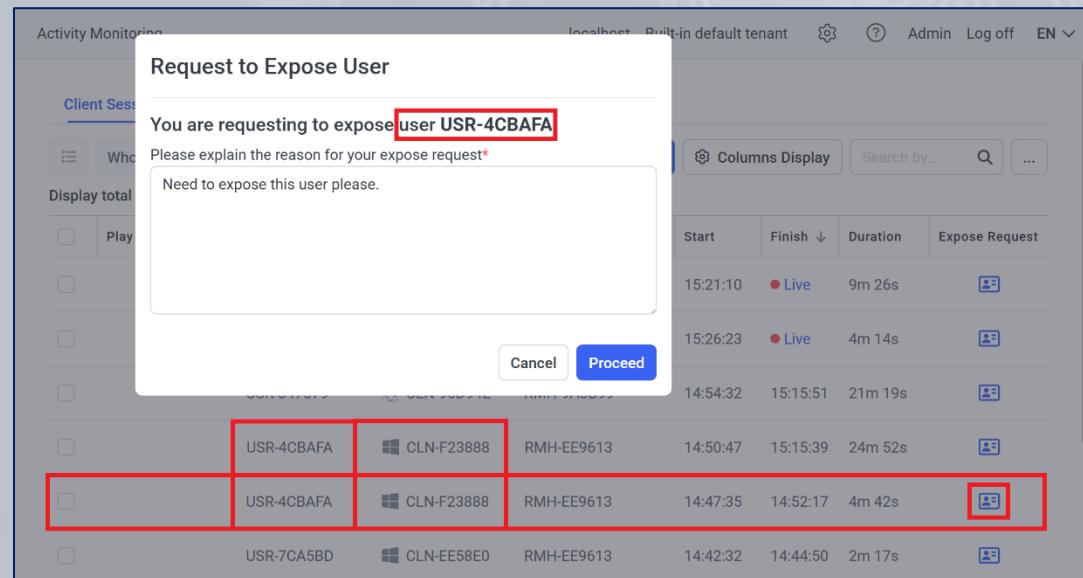
Protection of the **personally identifiable information (PPI)** of endpoint users, that is recorded during monitoring of their activities by Syteca, is achieved by the system **pseudonymizing** this data (i.e. hiding and replacing it with **randomized values** when viewed).



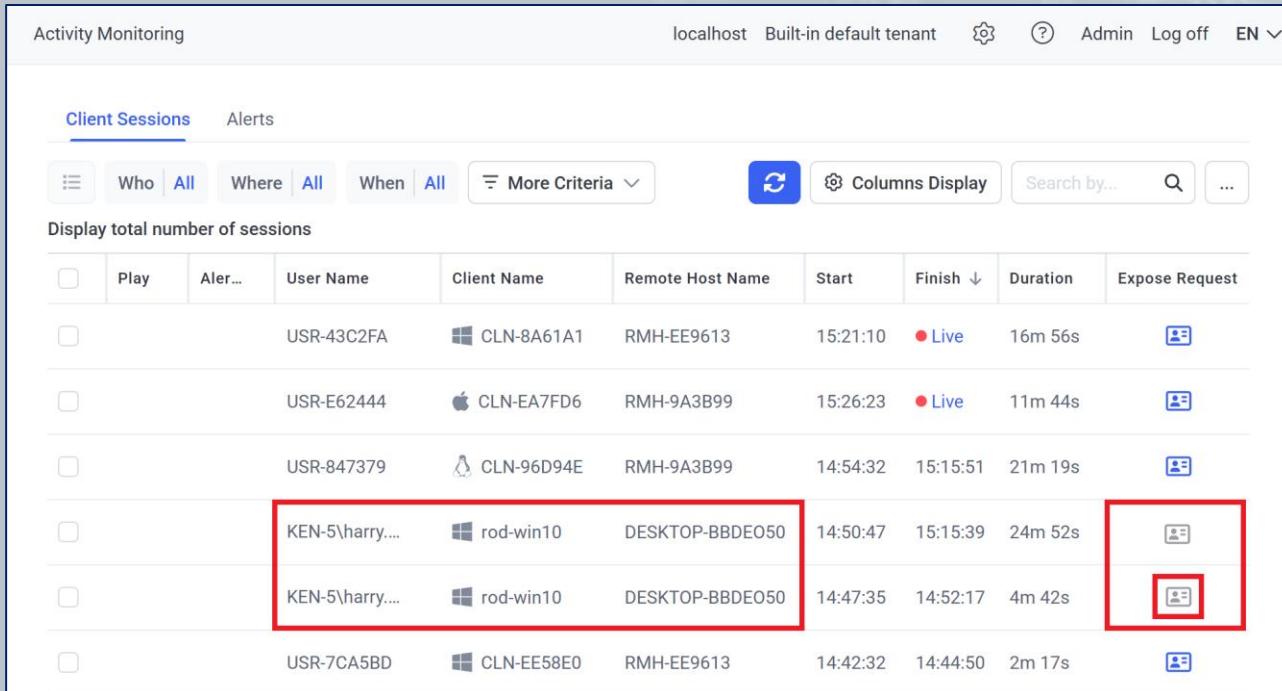
	Play	Aler...	User Name	Client Name	Remote Host Name	Start	Finish	Duration	Expose Request
<input type="checkbox"/>	Play		USR-43C2FA	CLN-8A61A1	RMH-EE9613	15:21:10	● Live	9m 26s	
<input type="checkbox"/>			USR-E62444	CLN-EA7FD6	RMH-9A3B99	15:26:23	● Live	4m 14s	
<input type="checkbox"/>			USR-847379	CLN-96D94E	RMH-9A3B99	14:54:32	15:15:51	21m 19s	
<input type="checkbox"/>			USR-4CBAFA	CLN-F23888	RMH-EE9613	14:50:47	15:15:39	24m 52s	
<input type="checkbox"/>			USR-4CBAFA	CLN-F23888	RMH-EE9613	14:47:35	14:52:17	4m 42s	
<input type="checkbox"/>			USR-7CA5BD	CLN-EE58E0	RMH-EE9613	14:42:32	14:44:50	2m 17s	

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 **not have permission** to open and **view the sessions** of endpoint users.



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**.



Activity Monitoring

localhost Built-in default tenant   Admin Log off EN

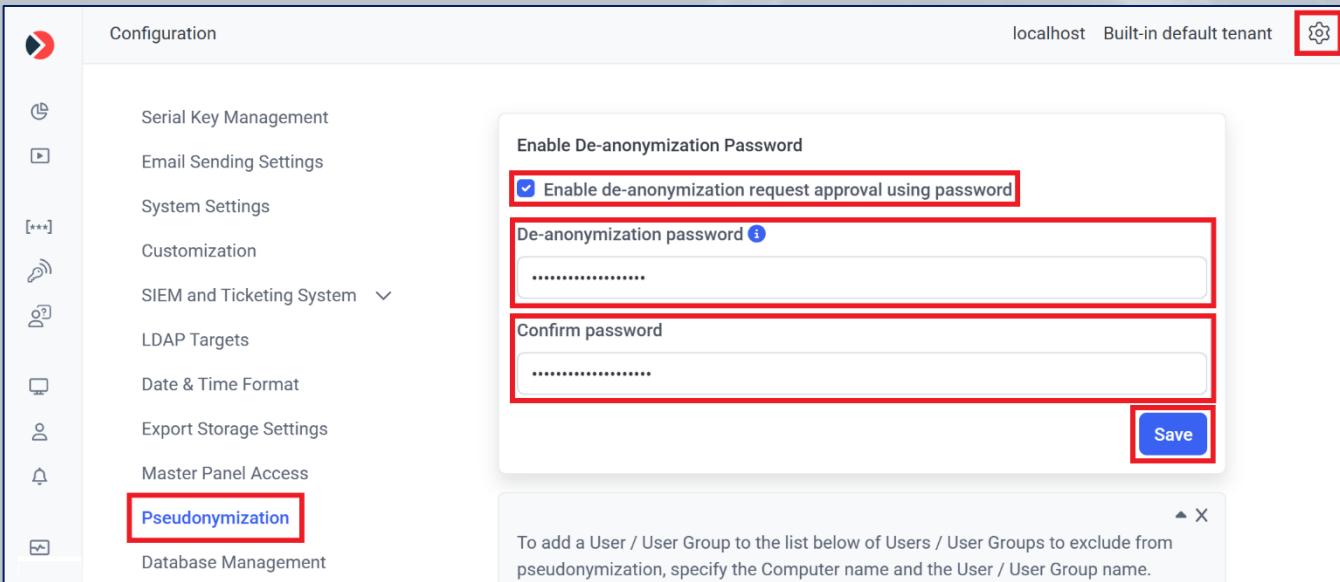
Client Sessions Alerts

Who All Where All When All More Criteria   Columns Display Search by...  ...

Display total number of sessions

<input type="checkbox"/>	Play	Aler...	User Name	Client Name	Remote Host Name	Start	Finish	Duration	Expose Request
<input type="checkbox"/>			USR-43C2FA	 CLN-8A61A1	RMH-EE9613	15:21:10	 Live	16m 56s	
<input type="checkbox"/>			USR-E62444	 CLN-EA7FD6	RMH-9A3B99	15:26:23	 Live	11m 44s	
<input type="checkbox"/>			USR-847379	 CLN-96D94E	RMH-9A3B99	14:54:32	15:15:51	21m 19s	
<input type="checkbox"/>			KEN-5\harry....	 rod-win10	DESKTOP-BBDE050	14:50:47	15:15:39	24m 52s	
<input type="checkbox"/>			KEN-5\harry....	 rod-win10	DESKTOP-BBDE050	14:47:35	14:52:17	4m 42s	
<input type="checkbox"/>			USR-7CA5BD	 CLN-EE9613	RMH-EE9613	14:42:32	14:44:50	2m 17s	

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).



Configuration

localhost Built-in default tenant 

Serial Key Management

Email Sending Settings

System Settings

Customization

SIEM and Ticketing System

LDAP Targets

Date & Time Format

Export Storage Settings

Master Panel Access

Pseudonymization

Database Management

Enable De-anonymization Password

Enable de-anonymization request approval using password

De-anonymization password 

.....

Confirm password

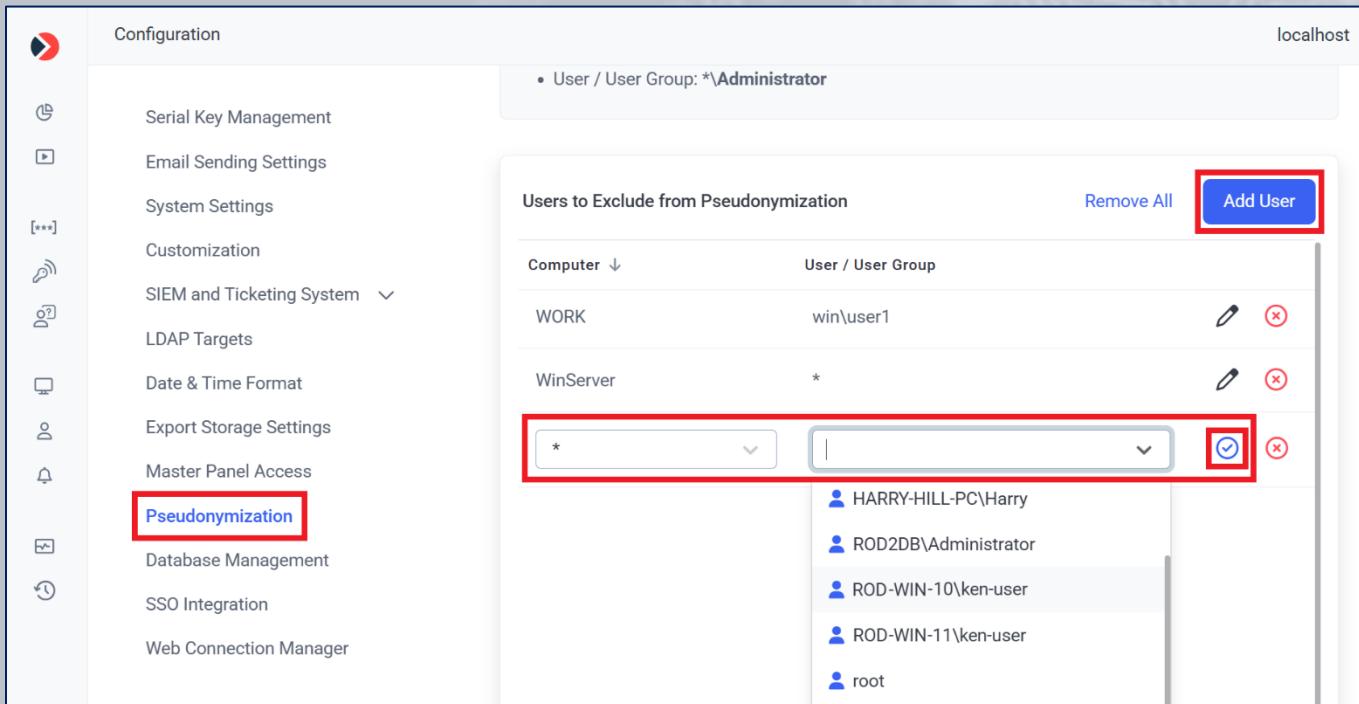
.....

Save

To add a User / User Group to the list below of Users / User Groups to exclude from pseudonymization, specify the Computer name and the User / User Group name.

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

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.

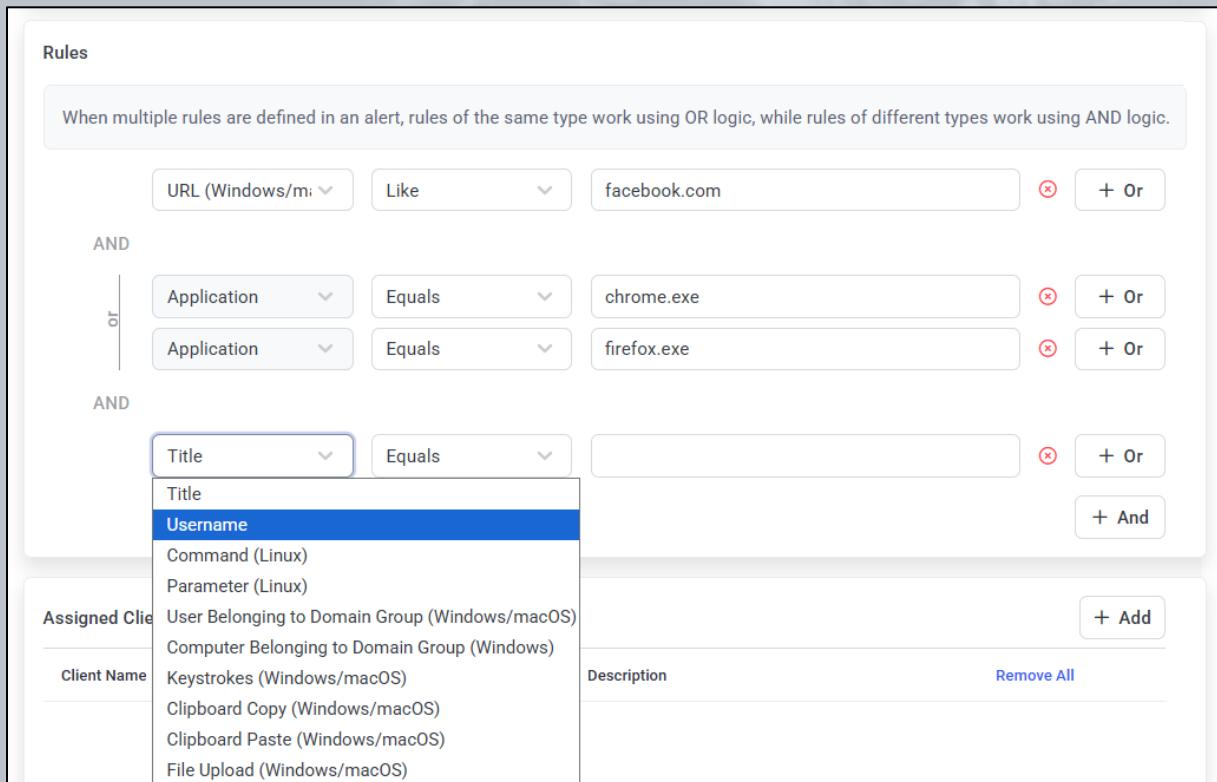


The screenshot shows the Syteca Management Tool interface. On the left, a sidebar lists various configuration options: Serial Key Management, Email Sending Settings, System Settings, Customization, SIEM and Ticketing System (with a dropdown arrow), LDAP Targets, Date & Time Format, Export Storage Settings, Master Panel Access, **Pseudonymization** (which is highlighted with a red box), Database Management, SSO Integration, and Web Connection Manager. The main panel is titled 'Configuration' and shows a section for 'User / User Group: *\\Administrator'. Below this, there is a table titled 'Users to Exclude from Pseudonymization' with columns for 'Computer' and 'User / User Group'. The table contains two entries: 'WORK' with 'User / User Group: win\\user1' and 'WinServer' with 'User / User Group: *'. A red box highlights the search bar and the 'Add User' button. A list of users is shown at the bottom of the table, including 'HARRY-HILL-PC\\Harry', 'ROD2DB\\Administrator', 'ROD-WIN-10\\ken-user', 'ROD-WIN-11\\ken-user', and 'root'. A red box highlights the search bar and the 'Add User' button.

Alerts

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**.



The screenshot shows the Syteca alert configuration interface. At the top, a header reads "Rules" and includes a note: "When multiple rules are defined in an alert, rules of the same type work using OR logic, while rules of different types work using AND logic." Below this, there are three main sections: "AND", "or", and "AND". Each section contains a row of three dropdown menus: "Condition", "Operator", and "Value". The first row under "AND" has "URL (Windows/macOS)" as the condition, "Like" as the operator, and "facebook.com" as the value. The second row under "or" has "Application" as the condition, "Equals" as the operator, and "chrome.exe" as the value. The third row under "or" has "Application" as the condition, "Equals" as the operator, and "firefox.exe" as the value. The fourth row under "AND" has "Title" as the condition, "Equals" as the operator, and an empty value field. To the right of these rows are "Remove" and "Or" buttons. Below the rows, there is a "And" button. On the left side of the interface, there is a vertical list of alert types under "Assigned Client" and "Client Name". The "Username" option is highlighted with a blue selection bar. At the bottom right, there is a "Remove All" button and a "+ Add" button.

Using Regular Expressions (regex)

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.

Rules

When multiple rules are defined in an alert, rules of the same type work using OR logic, while rules of different types work using AND logic.

Application Matches (Regex) `\b(chrome|safari|edge|firefox)\b` + Or

AND

Clipboard Paste Matches (Regex) `^[\w-\.]+@[\\w-]+\.\w-[2,4]$` + Or

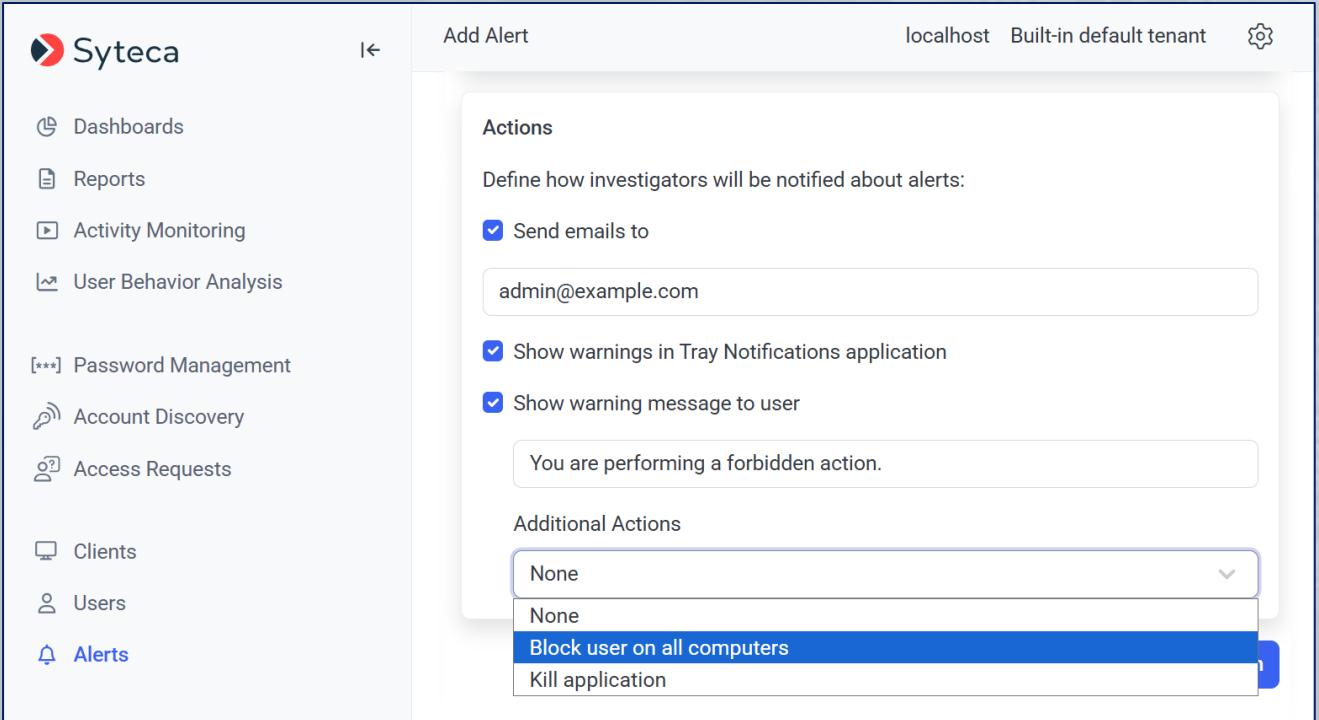
Clipboard Paste Matches (Regex) `^[(+)?([)]?0-9){3}[)]?[-\s.]{2-4}[0-9]{3}[-\s.]{2-4}[0-9]{4,6}$` + Or

+ And

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).

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.**



The screenshot shows the Syteca web interface with a sidebar on the left and a main configuration panel on the right.

Left Sidebar (Syteca Navigation):

- Dashboard
- Reports
- Activity Monitoring
- User Behavior Analysis
- >Password Management
- Account Discovery
- Access Requests
- Clients
- Users
- Alerts

Main Panel (Add Alert):

Top right: localhost, Built-in default tenant, gear icon.

Actions Section:

Define how investigators will be notified about alerts:

- Send emails to
- Show warnings in Tray Notifications application
- Show warning message to user

Additional Actions Section:

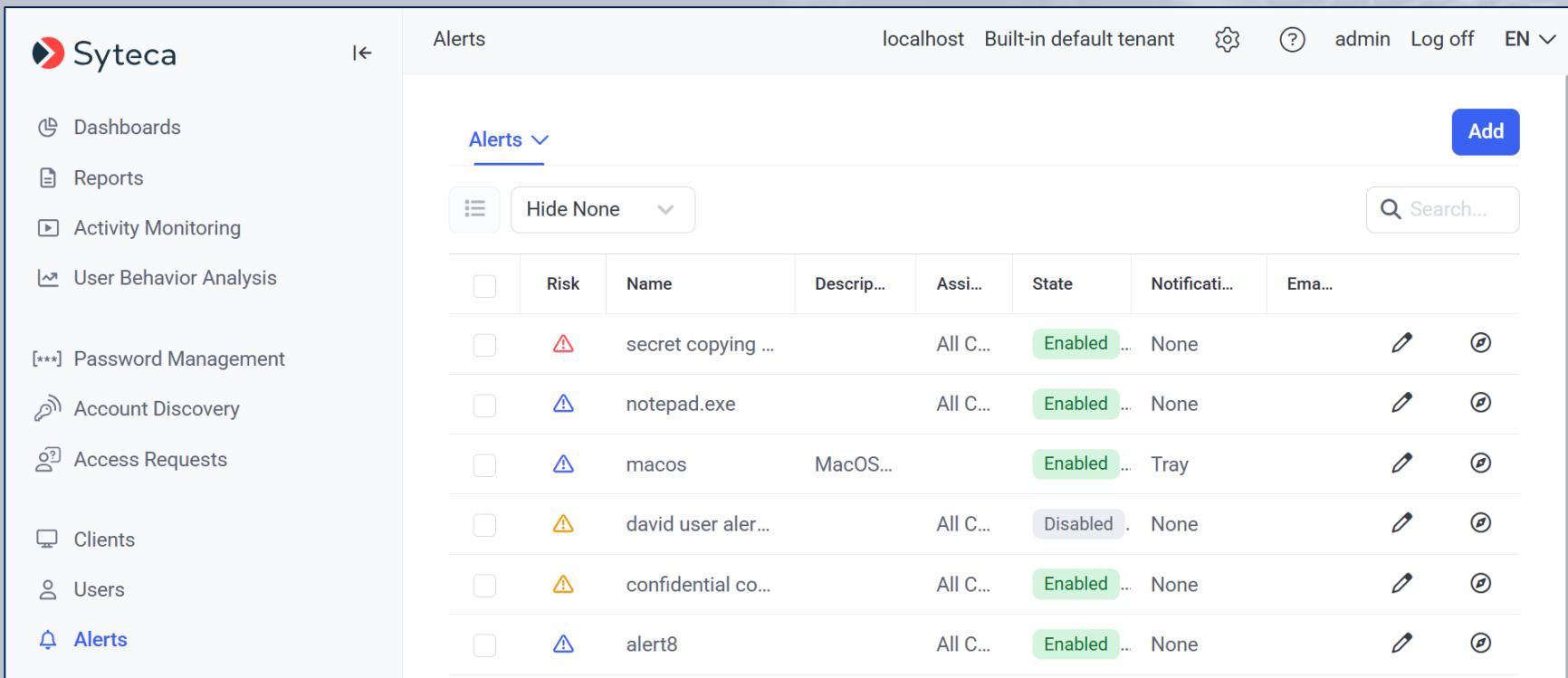
None

None

Block user on all computers (highlighted in blue)

Kill application

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.



The screenshot shows the Syteca interface with the 'Alerts' page selected. The left sidebar includes links for Dashboards, Reports, Activity Monitoring, User Behavior Analysis, Password Management, Account Discovery, Access Requests, Clients, Users, and Alerts. The main content area is titled 'Alerts' and displays a table of default alerts. The table columns are: Risk, Name, Description..., Assigned..., State, Notifications..., and Email... (partially visible). The alerts listed are:

Risk	Name	Description...	Assigned...	State	Notifications...	Email...
⚠️	secret copying ...	All C...	Enabled	None		
⚠️	notepad.exe	All C...	Enabled	None		
⚠️	macos	MacOS...	Enabled	Tray		
⚠️	david user aler...	All C...	Disabled	None		
⚠️	confidential co...	All C...	Enabled	None		
⚠️	alert8	All C...	Enabled	None		

Viewing Alert Events

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

Viewing Alert Events in the Session Viewer



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

The screenshot displays the Syteca Session Viewer interface. On the left, a browser window shows a Facebook login page. A blue callout box highlights an 'alert' event: 'david facebook alert' (Alert ID: 19136) for the action 'Facebook - log in or sign up - Google Chrome - chrome.exe - facebook'. On the right, a log table lists activity events. Several rows are highlighted in different colors (light blue, orange, red, grey) corresponding to the alert risk levels. The log includes columns for timestamp, activity title, application, URL, text data, and alert/USB information. The bottom of the log shows pagination and a search bar.

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

Receiving Alert Notifications



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

The screenshot shows the Syteca System Tray Notifications Journal window and a corresponding tray notification. The journal table lists multiple alerts, all named 'david alert test', occurring between 12:41:58 PM and 12:45:28 PM on 8/20/2025. Each alert is of 'Normal' level and involves 'macOS keystrokes' from 'dev\lee...' to 'lee...'. The 'Details' column provides a brief description of the activity, such as 'Changes in secret usage functionality.docx - Word - WINWORD.EXE -' and '10.100.1.100 - Remote Desktop Connection - mstsc.exe -'. A tray notification window titled 'Tray Notification' is overlaid on the journal, showing 'Ekran System Alert Notifications (2 new)' and the specific alert details: 'Alert: david alert test (8/20/2025 12:41:58 PM) Client: lee-PC; User: dev\lee'. The tray also shows standard system icons and the date/time.

Activity Time	Alert Name	Alert Level	Alert Description	User ...	Cli...	Client De...	Details	Client Groups
8/20/2025 12:45:28 PM	david alert test	Normal	macOS keystrokes	dev\lee...	lee...	xxx	Changes in secret usage functionality.docx - Word - WINWORD.EXE -	
8/20/2025 12:41:58 PM	david alert test	Normal	macOS keystrokes	dev\lee...	lee...	xxx	Changes in secret usage functionality.docx - Word - WINWORD.EXE -	
8/20/2025 12:40:33 PM	david alert test	Normal	macOS keystrokes	dev\lee...	lee...	xxx	Changes in secret usage functionality.docx - Word - WINWORD.EXE -	
8/20/2025 12:39:18 PM	david alert test	Normal	macOS keystrokes	dev\lee...	lee...	xxx	Changes in secret usage functionality.docx - Word - WINWORD.EXE -	
8/20/2025 12:35:01 PM	david alert test	Normal	macOS keystrokes	dev\lee...	lee...	xxx	Changes in secret usage functionality.docx - Word - WINWORD.EXE -	
8/20/2025 12:32:24 PM	david alert test	Normal	macOS keystrokes	dev\lee...	lee...	xxx	Changes in secret usage functionality.docx - Word - WINWORD.EXE -	
8/20/2025 12:23:59 PM	david alert test	Normal	macOS keystrokes	dev\lee...	lee...	xxx	Changes in secret usage functionality.docx - Word - WINWORD.EXE -	

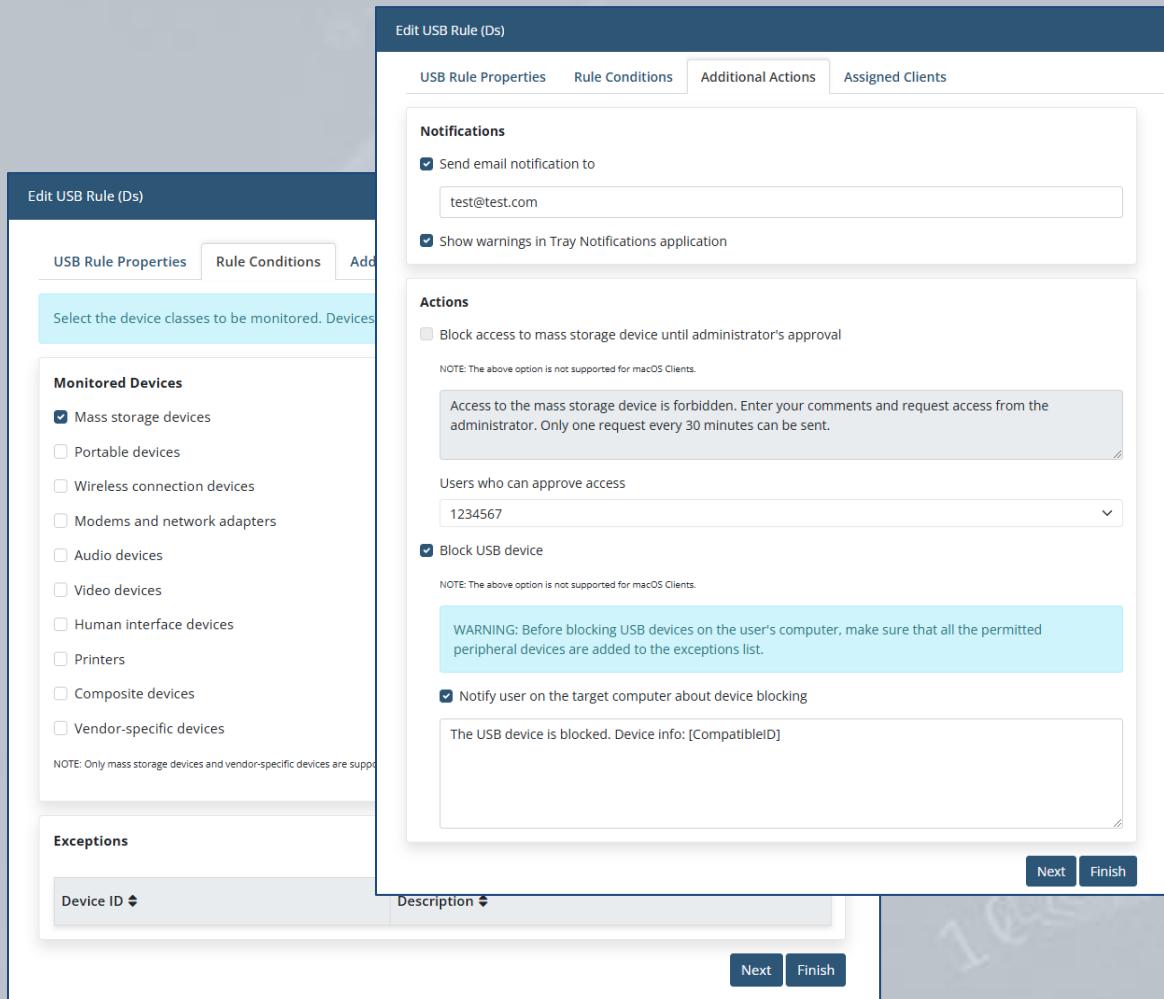
USB Device Monitoring

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

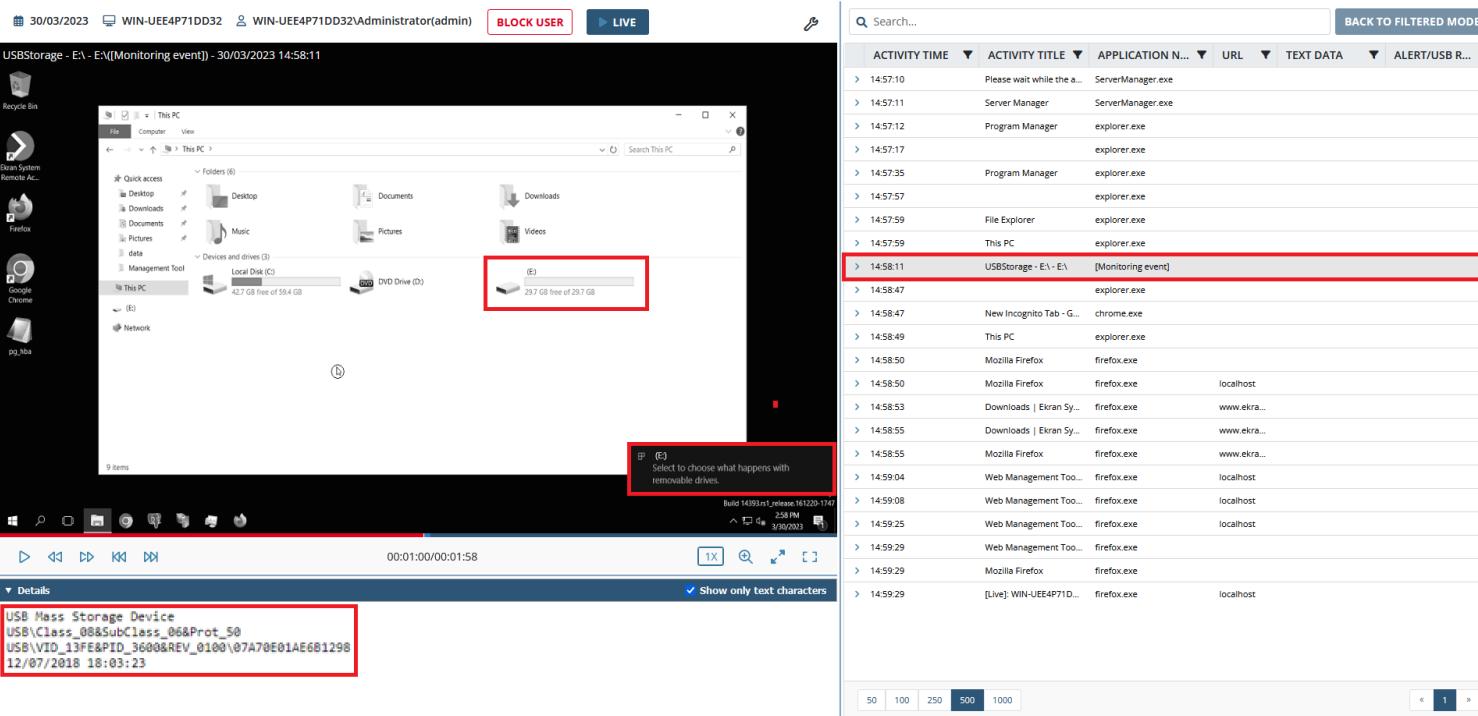
Syteca can **detect** USB devices connected to a computer, **alert** you when a device is plugged in, and block their usage or **forbid** access to them until **administrator approval** (either for all devices of a certain class, or all devices except permitted ones) on a Client computer.



Automatic USB Device Monitoring

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.



The screenshot shows the Syteca Session Viewer interface. On the left, a file explorer window is open, showing the 'This PC' view. A red box highlights the USB storage device (E:) which is listed under 'Devices and drives'. On the right, a log table displays activity events. A red box highlights the event for 'USBStorage - E\ - E\ [Monitoring event]' at 14:58:11. The log table includes columns for Activity Time, Activity Title, Application Name, URL, Text Data, and Alert/USB R...

Activity Time	Activity Title	Application Name	URL	Text Data	Alert/USB R...
14:57:10	Please wait while the a...	ServerManager.exe			
14:57:11	Server Manager	ServerManager.exe			
14:57:12	Program Manager	explorer.exe			
14:57:17		explorer.exe			
14:57:35	Program Manager	explorer.exe			
14:57:57		explorer.exe			
14:57:59	File Explorer	explorer.exe			
14:57:59	This PC	explorer.exe			
14:58:11	USBStorage - E\ - E\ [Monitoring event]				
14:58:47		explorer.exe			
14:58:47	New Incognito Tab G...	chrome.exe			
14:58:49	This PC	explorer.exe			
14:58:50	Mozilla Firefox	firefox.exe			
14:58:50	Mozilla Firefox	firefox.exe	localhost		
14:58:53	Downloads Ecran Sy...	firefox.exe	www.ekra...		
14:58:55	Downloads Ecran Sy...	firefox.exe	www.ekra...		
14:58:55	Mozilla Firefox	firefox.exe	www.ekra...		
14:59:04	Web Management Too...	firefox.exe	localhost		
14:59:08	Web Management Too...	firefox.exe	localhost		
14:59:25	Web Management Too...	firefox.exe	localhost		
14:59:29	Web Management Too...	firefox.exe			
14:59:29	Mozilla Firefox	firefox.exe			
14:59:29	[Live] WIN-UEE4P71D...	firefox.exe	localhost		

Dashboards

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

Generating Dashboards



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.

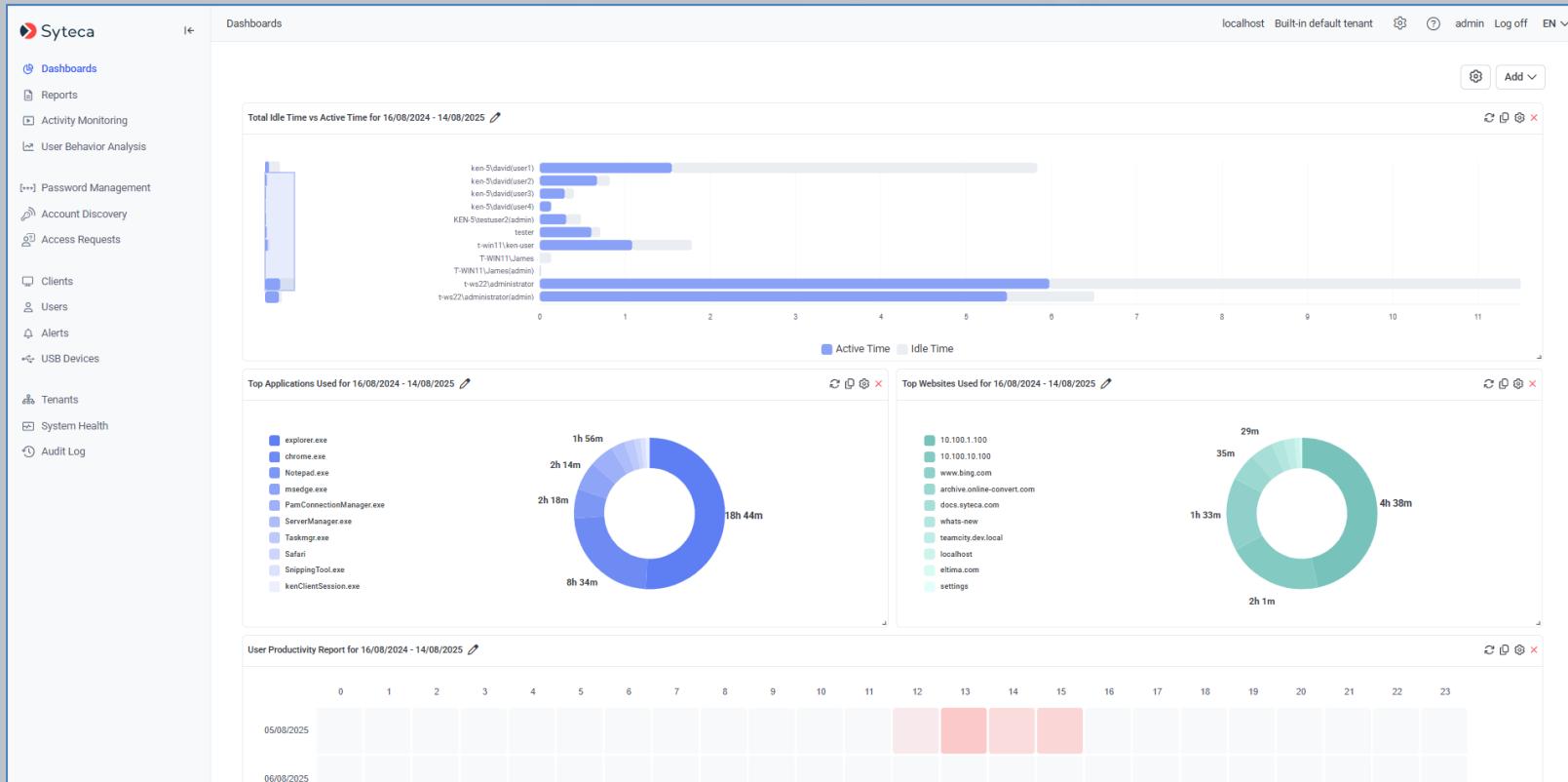
The screenshot shows the Syteca Dashboards page with three generated dashboards:

- Total Idle Time vs Active Time for 16/08/2024 - 14/08/2025**: A horizontal bar chart comparing active and idle time for various users. The x-axis ranges from 0 to 8. The legend indicates blue for Active Time and grey for Idle Time. The chart shows significant idle time for most users, with t-ws22\administrator having the highest active time.
- Top Websites Used for 16/08/2024 - 14/08/2025**: A donut chart showing the total time spent on different websites. The total is 4h 38m. The legend lists websites: 10.100.1.100, 10.100.10.100, www.bing.com, archive.online-convert.com, docs.syteca.com, whats-new, teamcity.dev.local, localhost, eltima.com, and settings.
- User Productivity Report for 27/09/2024 - 25/09/2025**: A heatmap showing activity levels over a 24-hour period for multiple days. The x-axis represents hours from 0 to 23. The y-axis represents dates from 04/09/2025 to 12/09/2025. A color scale at the bottom indicates activity levels from None (red) to High (green). A tooltip for a cell on 10/09/2025 shows "Active time: 34 minute(s)".

A red box highlights the "Add" button and the list of dashboard options in the sidebar, which includes:

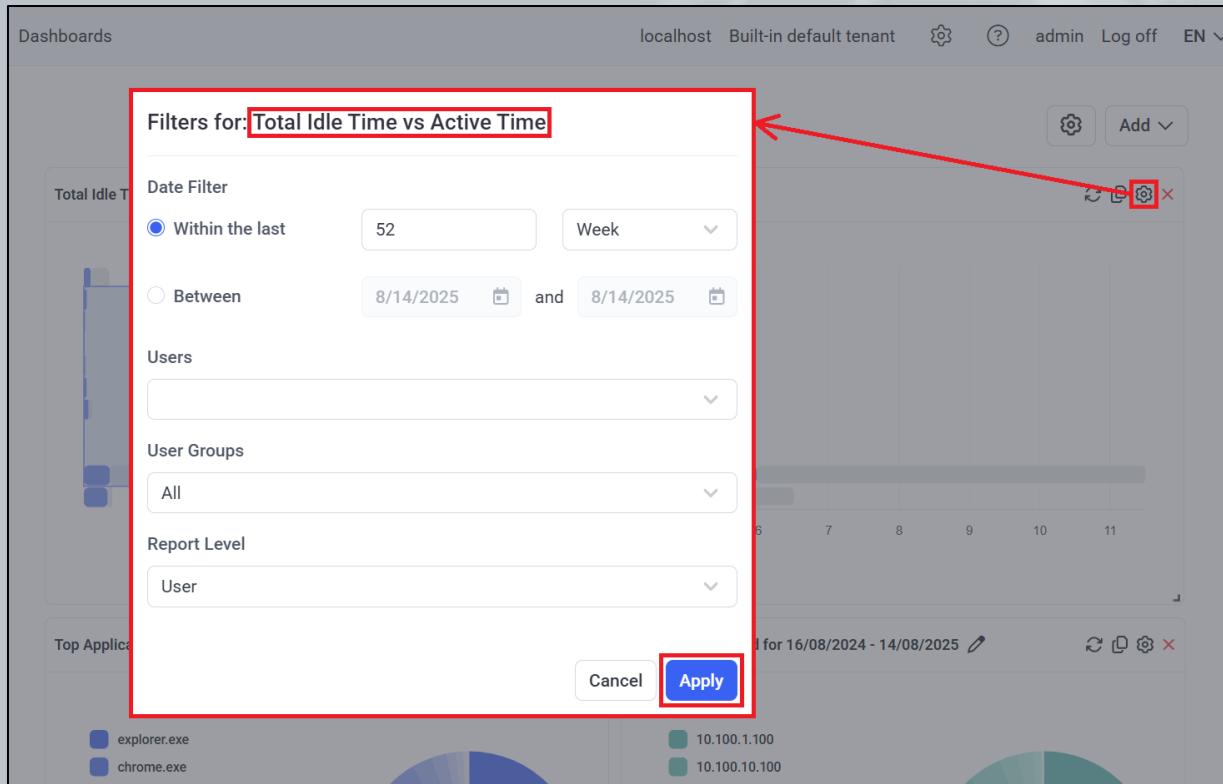
- Top Applications Used
- Top Alerts
- User Productivity Report
- Total Idle Time vs Active Time
- Top Websites Used
- Latest Live Sessions
- Sessions Outside of Work Hours

Viewing Dashboards



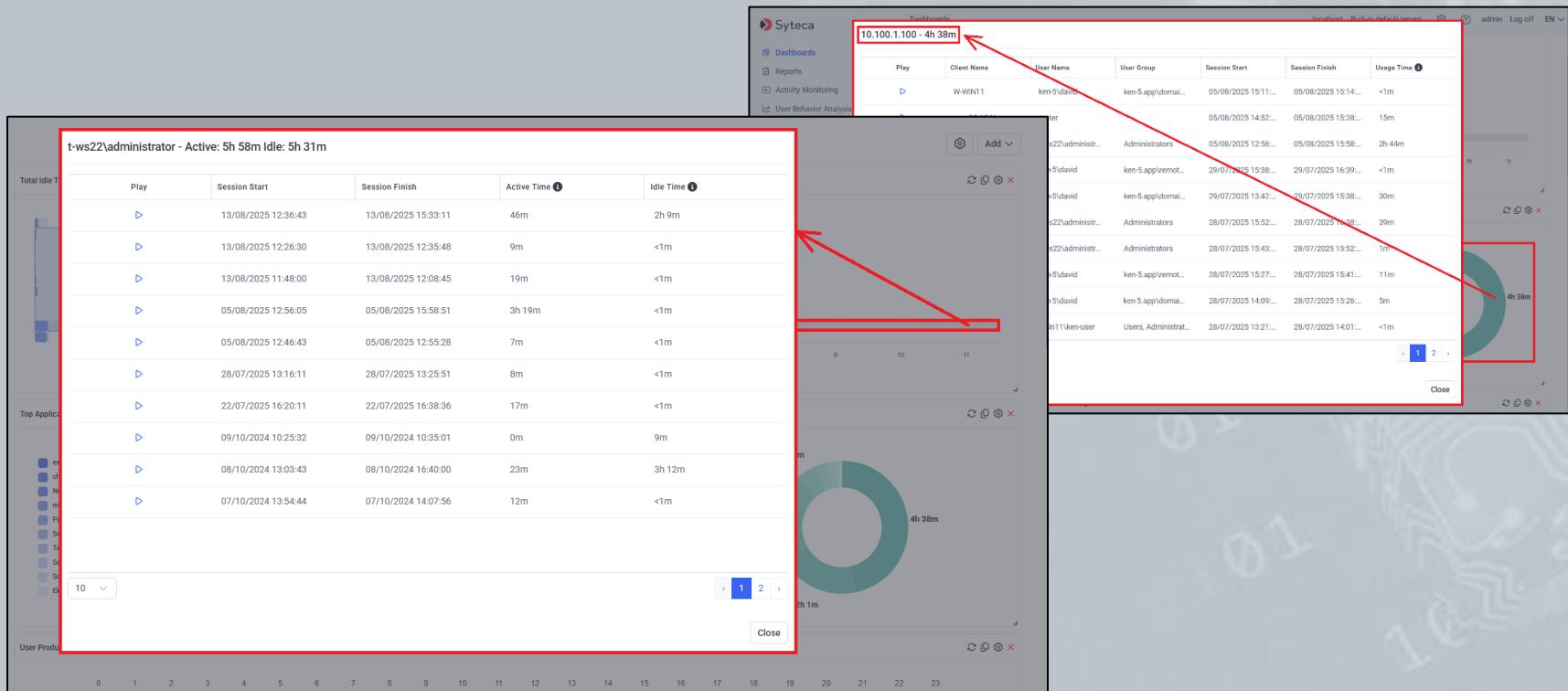
Some of these dashboards are **similar** to when **importing data from Syteca into Power BI** report templates by using **Syteca API Data Connector**, but are **much simpler to generate and customize**.

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**).



Latest Live Sessions

Play	Start	Client Name	User Name
	14/08/2025 11:01:44	T-WIN11	ken-5\david(user1)

Top Alerts

Top Alerts for 16/08/2024 - 14/08/2025

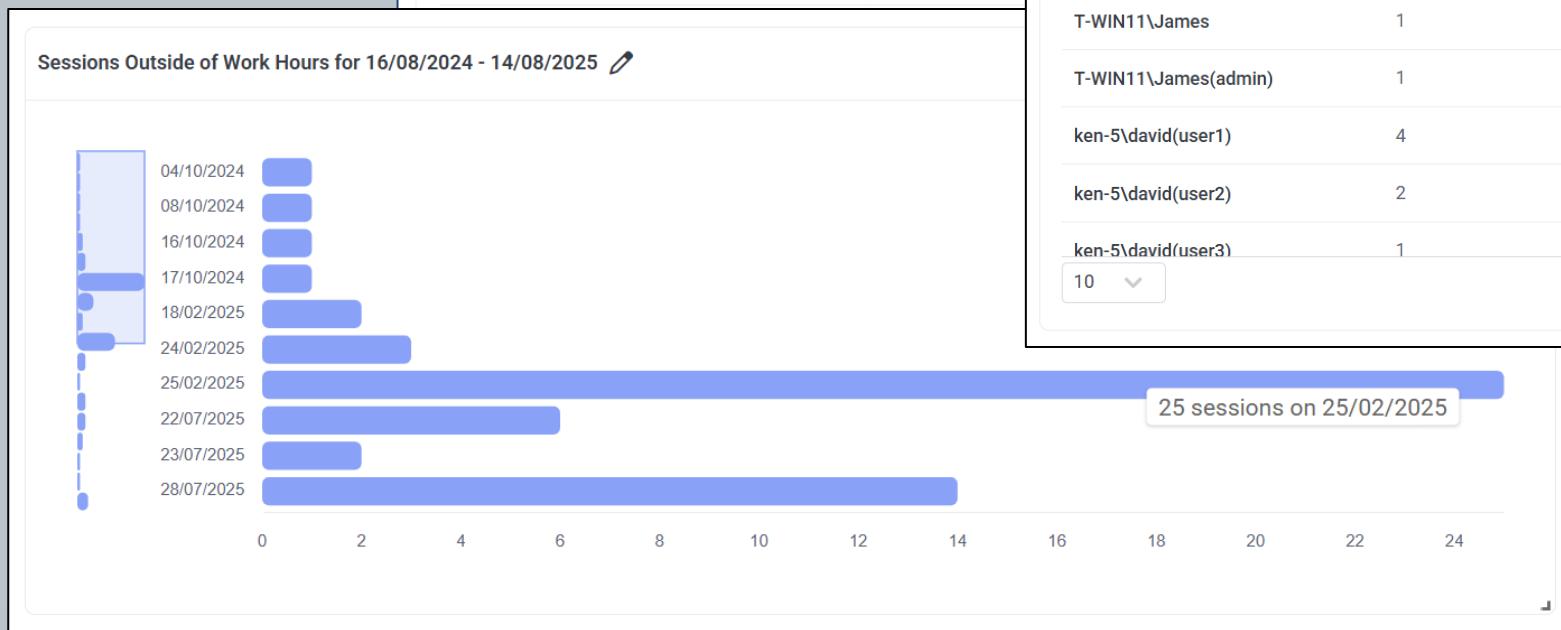


Alert Name	Notification Count	Level
notepad.exe	14	Normal Level
david user alert test	11	High Level
confidential copy test al...	2	High Level
mass storage device alert	2	High Level
alert3	1	High Level
secret copying test alert	1	Critical Level
[Default] Command pro...	1	High Level
[Default] Social networks	1	High Level

Legend: Normal Level High Level Critical Level

Latest
Live
Sessions

Sessions Outside of Work Hours



Rarely Used Computers

Rarely Used Computers for 22/08/2024 - 20/08/2025

Client Name ↓	Sessions
rzone1	1
rodii-ws22	2

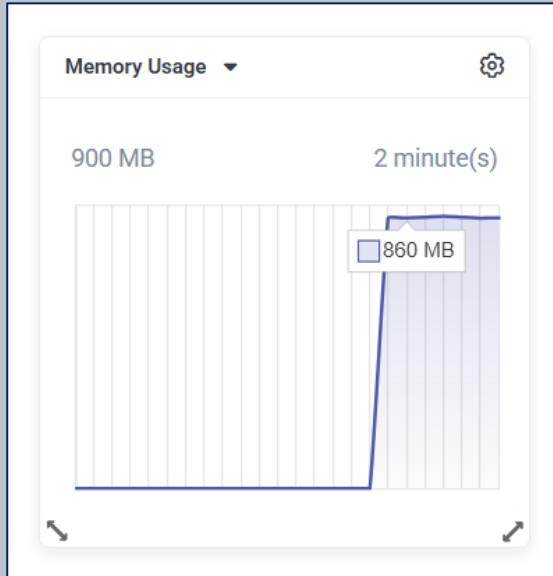
Rarely Used Logins

Rarely Used Logins for 16/08/2024 - 14/08/2025

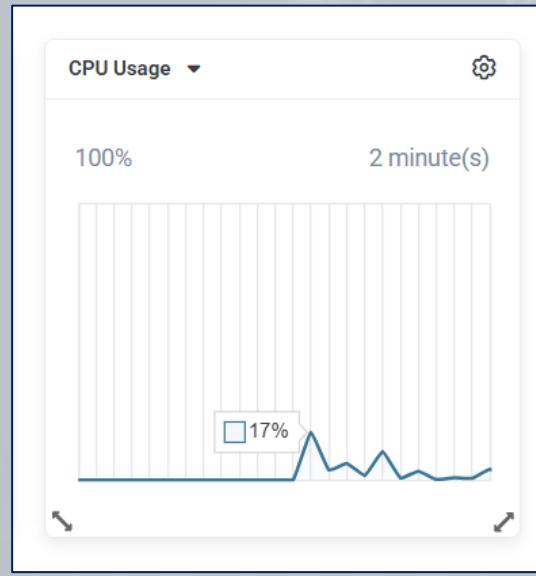
User Name ↑	Sessions
EKRAN-5\testuser2(admin)	2
T-WIN11\James	1
T-WIN11\James(admin)	1
ken-5\david(user1)	4
ken-5\david(user2)	2
ken-5\david(user3)	1

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

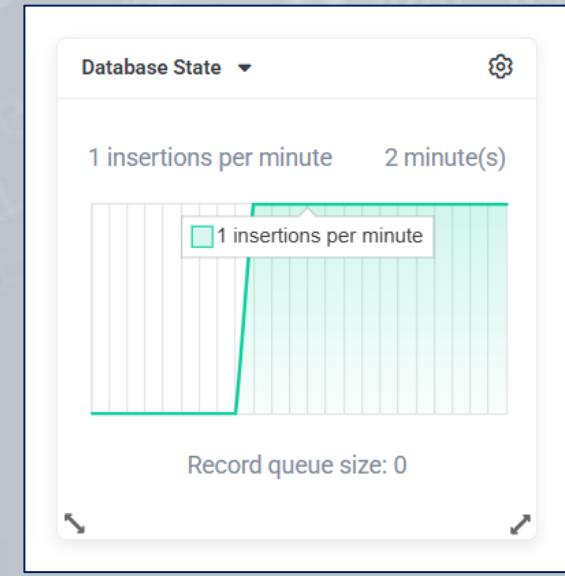
Memory Usage



CPU Usage

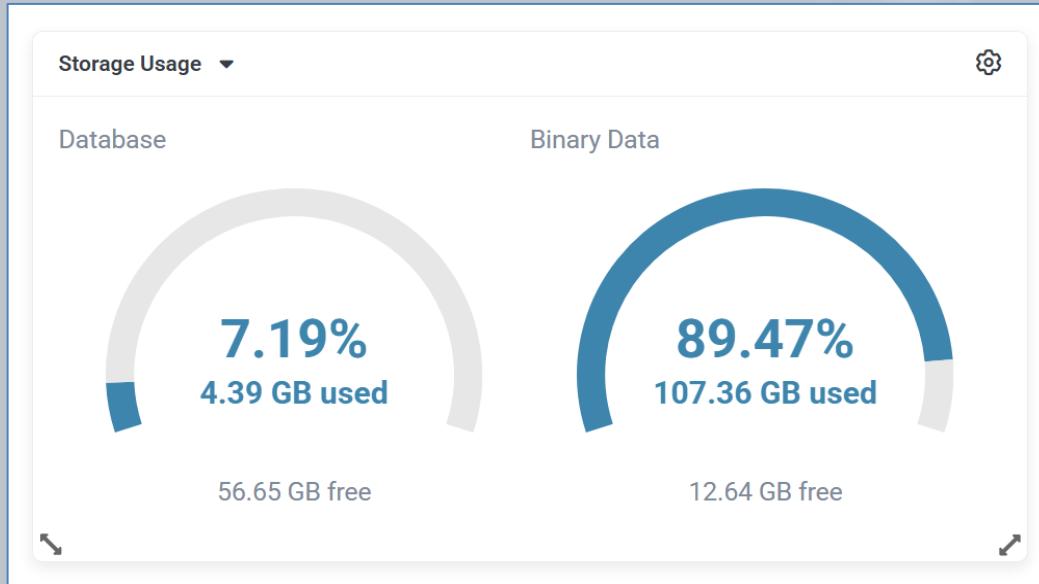


Database State

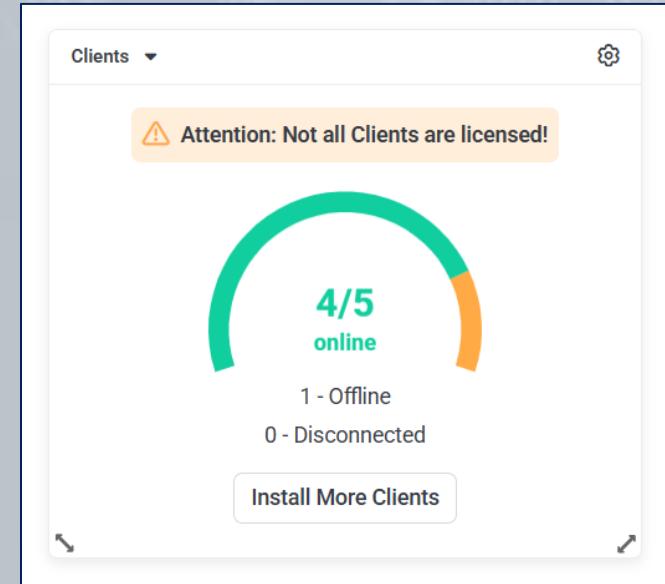


The **Storage Usage** and **Clients** dashboards (on the **System Health** page) provide information about the system state in real time.

Storage Usage



Clients

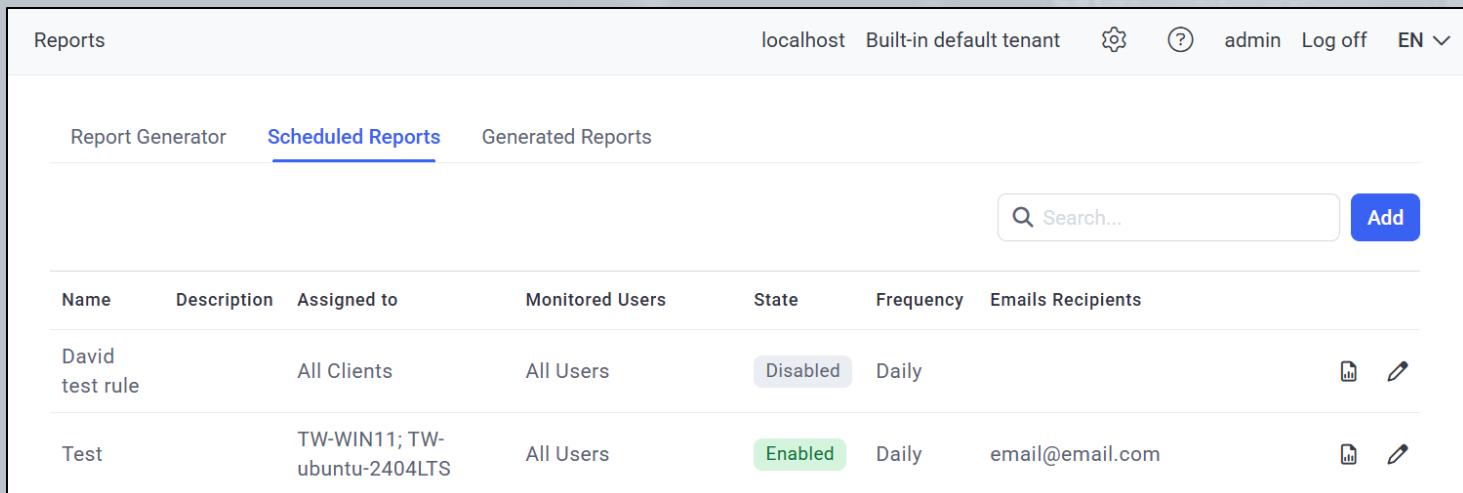


Reports

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



Name	Description	Assigned to	Monitored Users	State	Frequency	Emails Recipients	Actions
David test rule		All Clients	All Users	Disabled	Daily		 
Test		TW-WIN11; TW-ubuntu-2404LTS	All Users	Enabled	Daily	email@email.com	 

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

Manual Report Generation

Reports

Report Generator Scheduled Reports Generated Reports

Report Type

Access Request Grid PDF

Activity Pie Chart

Activity Summary Grid

Activity Summary Grid (Grouped)

Alert Grid

Audit Session Grid

Clipboard Grid

Clipboard Grid (Grouped)

Detailed Activity Grid

Detailed Activity Grid (Grouped)

File Monitoring Grid

Keystroke Grid

Linux/XWindow Grid

Overtime Work Grid

Secondary User Authentication Grid

Session Grid

Session Grid (Grouped)

Session Viewing Status Grid

Sessions Outside of Work Hours Grid

Generate Report

Reports

Date Filters

Within the last 1 Hours

Between 8/11/2025 and 8/12/2025

Clients

+ Add

Client Name	Description	Remove All
ubuntu-2404-h		
macOS-13-VM		

Client Groups

+ Add

Client Group Name	Description	Remove All
Test Group 3		

Users

Who Can Download

Any

Generate Report

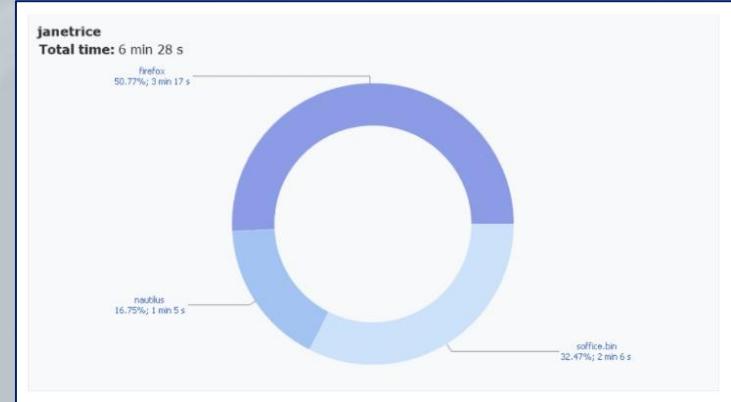
Examples of Report Types



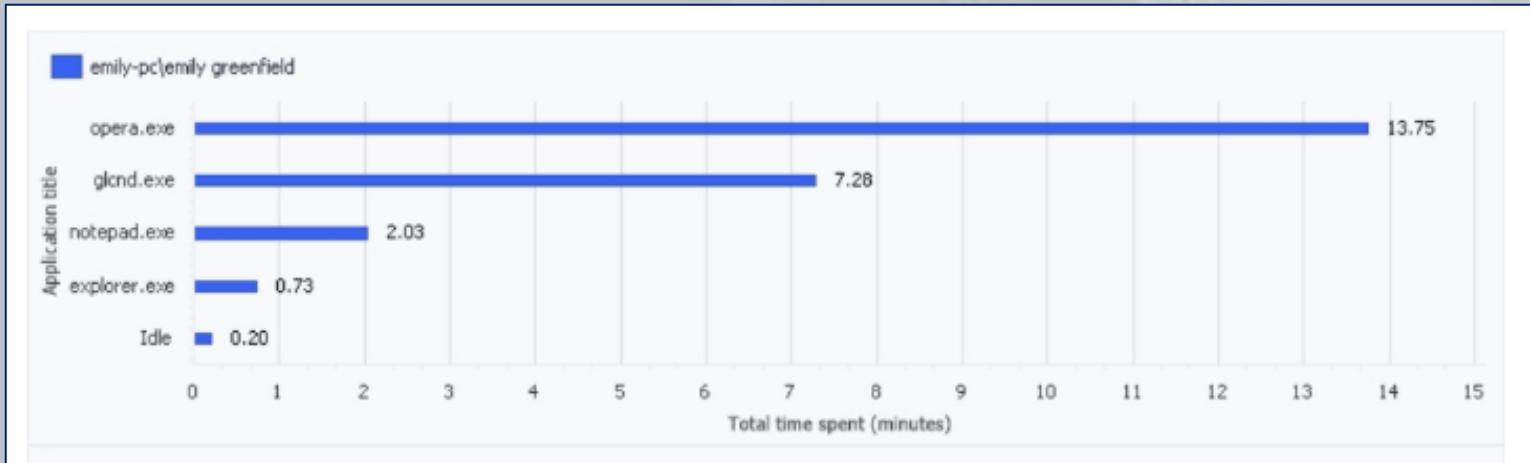
Activity Summary Grid Report

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



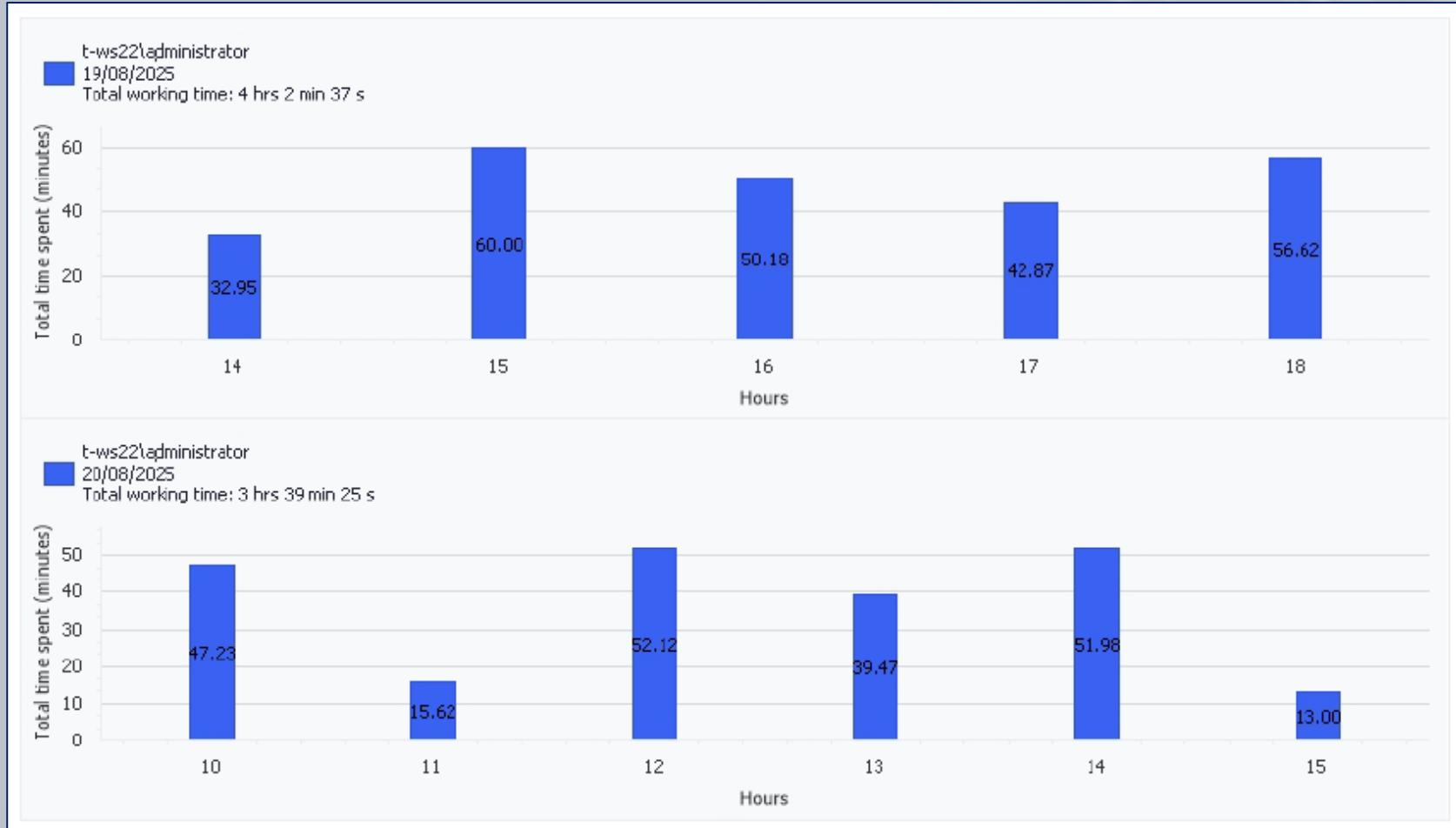
Access Requests Grid Report

Client Name	User Name	Request Type	Requested At	Status	Processed At	Processed 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						
<hr/>							
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

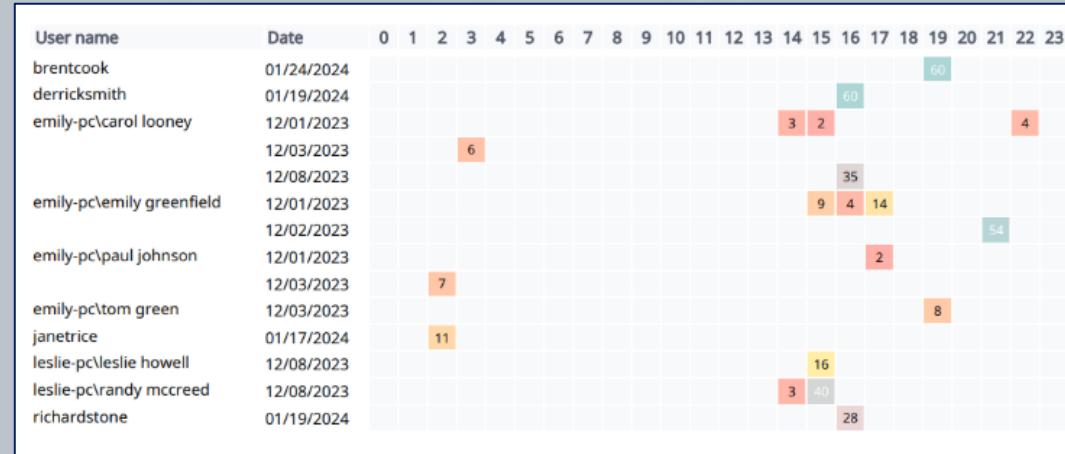
User Productivity Chart Report



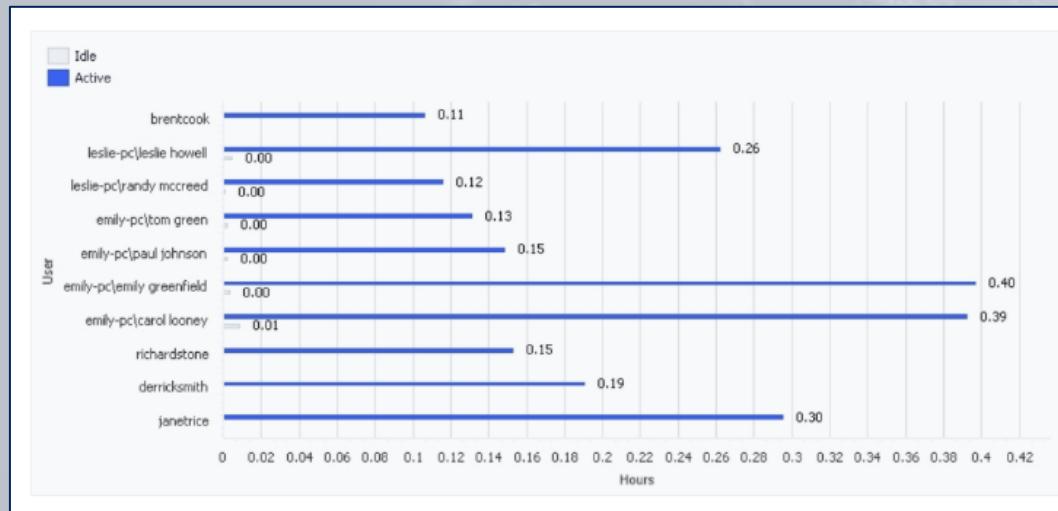
Examples of Report Types



User Productivity Heatmap Report



User Active Time and Idle Time Chart Report



Report Types: Examples



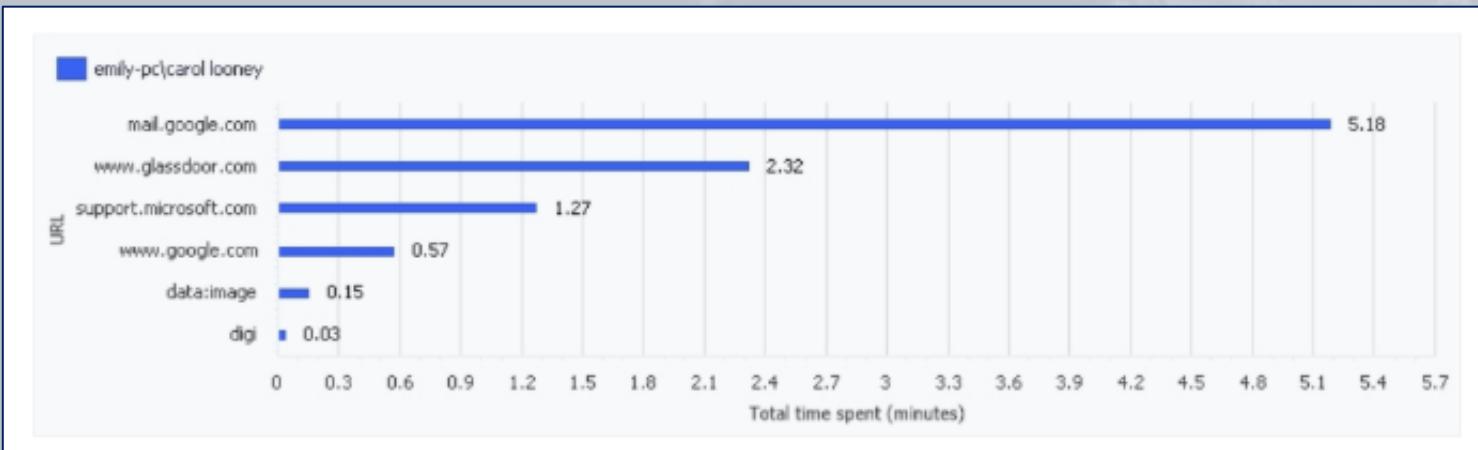
URL Summary Grid Report

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



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				
<hr/>					
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

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

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	

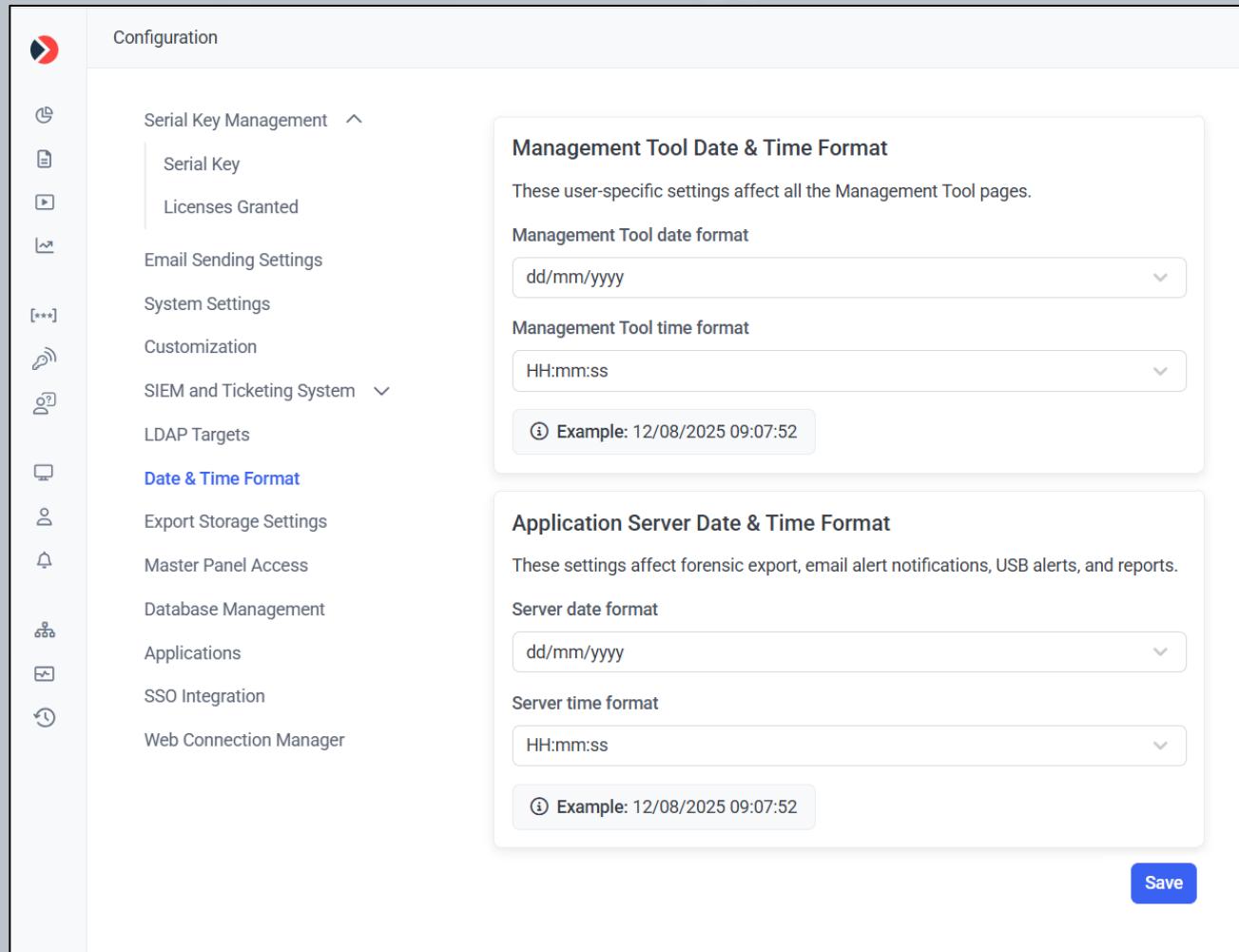
The Session Viewing Status Grid Report is a **special** report type that allows **whether all Client sessions have been viewed** (by at least one user) to be **conveniently checked** (as well as **who** has viewed each session, and **when**).

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

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

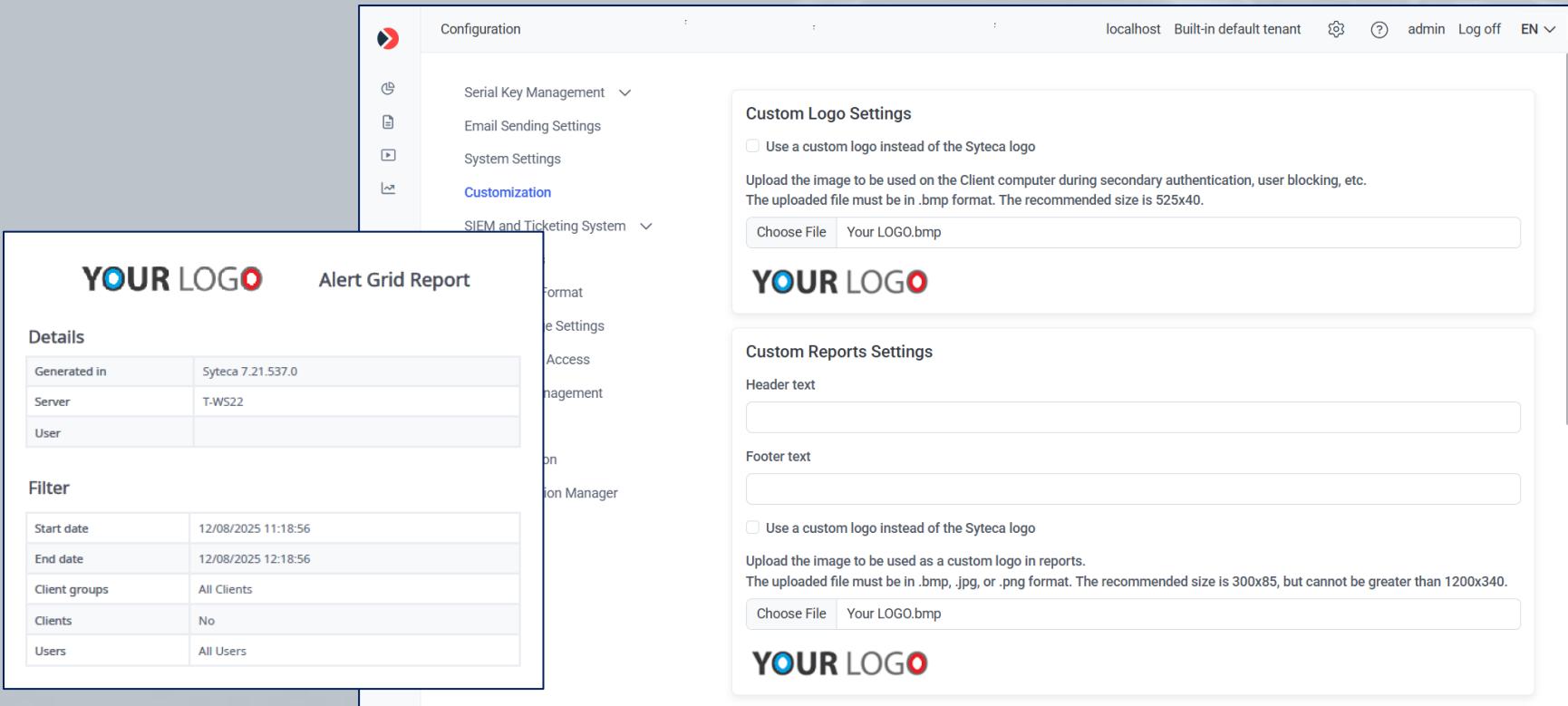


The screenshot shows the Syteca Configuration interface. The left sidebar contains icons for various management tools and settings. The main menu under 'Configuration' includes 'Serial Key Management', 'Email Sending Settings', 'System Settings', 'Customization', 'SIEM and Ticketing System', 'LDAP Targets', 'Date & Time Format' (which is highlighted in blue), 'Export Storage Settings', 'Master Panel Access', 'Database Management', 'Applications', 'SSO Integration', and 'Web Connection Manager'. The 'Date & Time Format' section is expanded, showing two main sections: 'Management Tool Date & Time Format' and 'Application Server Date & Time Format'. Each section has dropdown menus for 'Management Tool date format' (set to 'dd/mm/yyyy') and 'Management Tool time format' (set to 'HH:mm:ss'). Below these dropdowns is a placeholder text 'Example: 12/08/2025 09:07:52'. At the bottom right of the configuration area is a 'Save' button.

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.



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.



The screenshot shows the Syteca Configuration interface. On the left, there's a navigation sidebar with icons for Serial Key Management, Email Sending Settings, System Settings, and **Customization** (which is highlighted). Below that is a dropdown for SIEM and Ticketing System. The main content area has two sections: **Custom Logo Settings** and **Custom Reports Settings**.

Custom Logo Settings:

- Use a custom logo instead of the Syteca logo
- Upload the image to be used on the Client computer during secondary authentication, user blocking, etc.
- The uploaded file must be in .bmp format. The recommended size is 525x40.
- Choose File: Your LOGO.bmp

Custom Reports Settings:

- Header text:** (Text input field)
- Footer text:** (Text input field)
- Use a custom logo instead of the Syteca logo
- Upload the image to be used as a custom logo in reports.
- The uploaded file must be in .bmp, .jpg, or .png format. The recommended size is 300x85, but cannot be greater than 1200x340.
- Choose File: Your LOGO.bmp

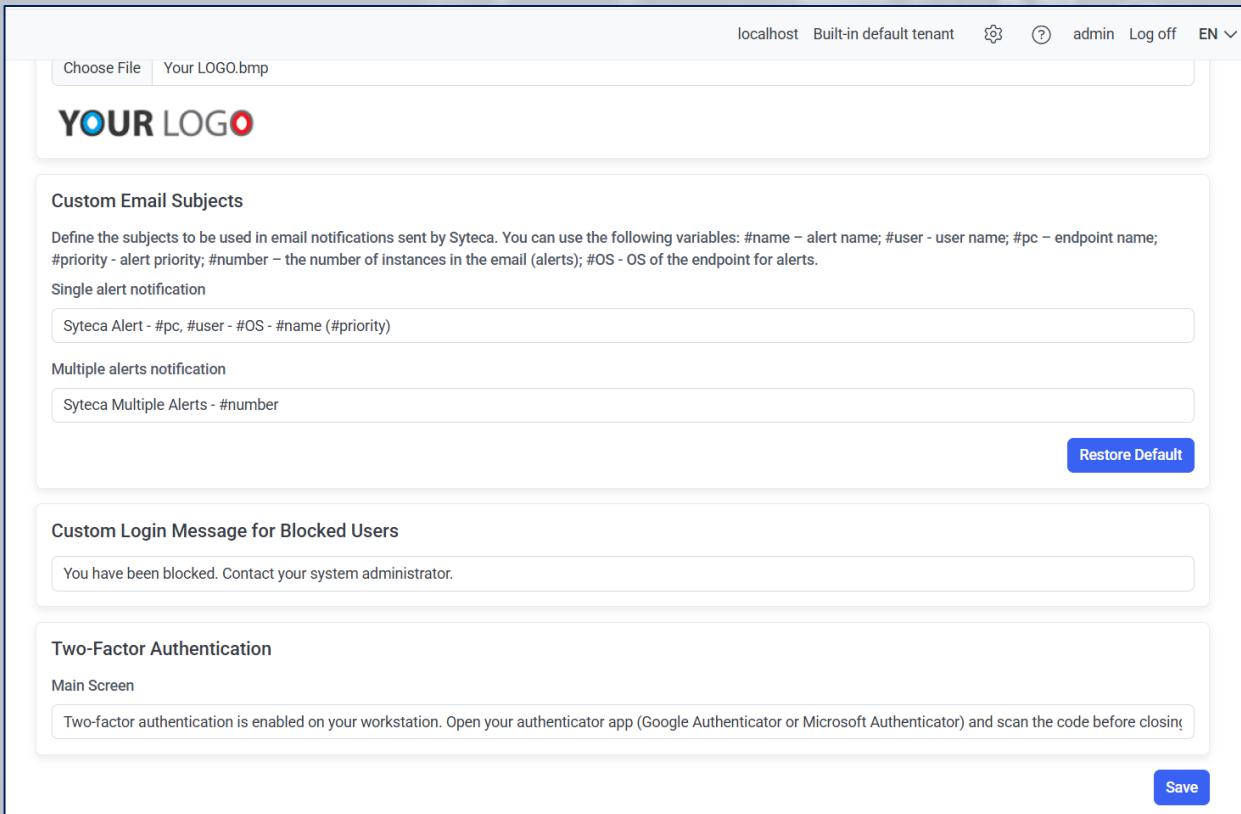
Report Preview: On the left, there's a preview of an "Alert Grid Report" with a placeholder logo. The report details section shows:

Generated in	Syteca 7.21.537.0
Server	T-WS22
User	

The filter section shows:

Start date	12/08/2025 11:18:56
End date	12/08/2025 12:18:56
Client groups	All Clients
Clients	No
Users	All Users

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



The screenshot shows the Syteca custom settings interface. At the top, there is a logo upload section with a placeholder 'YOUR LOGO'. Below it, the 'Custom Email Subjects' section contains two text input fields: 'Single alert notification' with the placeholder 'Syteca Alert - #pc, #user - #OS - #name (#priority)' and 'Multiple alerts notification' with the placeholder 'Syteca Multiple Alerts - #number'. A 'Restore Default' button is located to the right of these fields. The 'Custom Login Message for Blocked Users' section contains a single text input field with the placeholder 'You have been blocked. Contact your system administrator.' The 'Two-Factor Authentication' section contains a 'Main Screen' text input field with the placeholder 'Two-factor authentication is enabled on your workstation. Open your authenticator app (Google Authenticator or Microsoft Authenticator) and scan the code before closing'. At the bottom right of the interface is a 'Save' button.

System Health Monitoring

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.

System Health

localhost Built-in default tenant   admin Log off EN 

System State  Offline Clients Tasks List

Storage Usage 

Database

1.27%  1.26 GB used

98.00 GB free

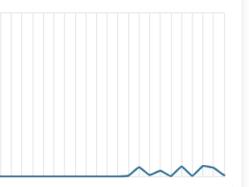
Memory Usage 

900 MB 2 minute(s)



CPU Usage 

100% 2 minute(s)



Database State 

1 insertions per minute 2 minute(s)



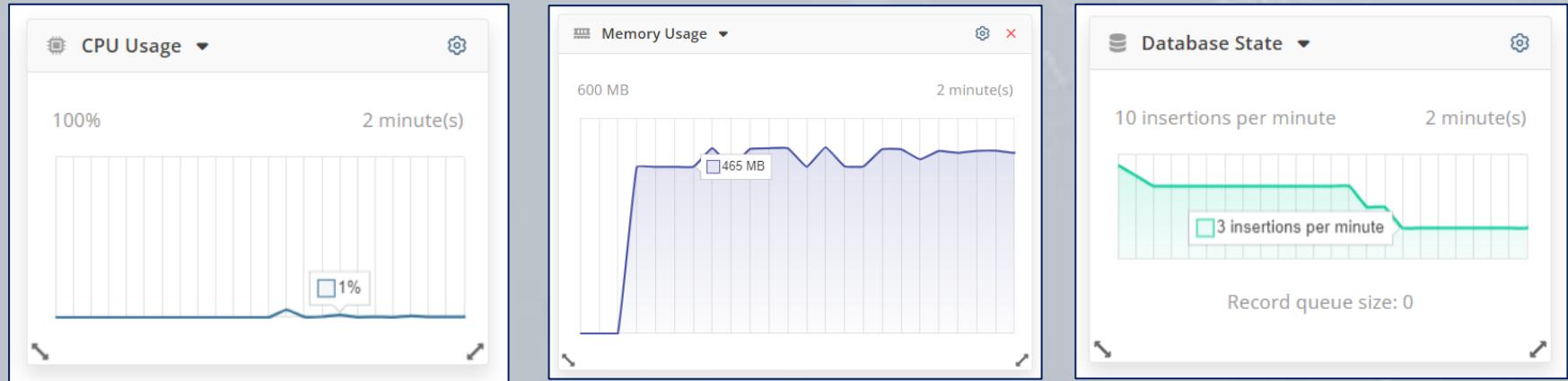
Record queue size: 0

When: All Category: All Source: All  Manage Hidden Columns

Date ↑	Category	Source	Details	Severity	Count	Remove All
05/08/2025 15:27:49	Access management	Server	Unable to send Access request notification to User admin	Medium	3	
05/08/2025 14:50:35	Client system permissions	macOS-13-VM	The following permissions are allowed on macOS-13-VM: Accessibility, Screen capture. User activity monitoring is restored.	Medium	1	
05/08/2025 14:50:30	Client system permissions	macOS-13-VM	The following system permissions are not met on macOS-13-VM: Accessibility. User activity monitoring is stopped. To resolve this issue, grant the required permissions to the Syteca Client application in System Preferences -> Security & Privacy -> Privacy.	Critical	1	

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



	Start Time	Task Name	Node	Details	Queued Time	Duration	Status
	15:51:15	User Productivity Heatmap		David test rule Between 12/07/2025 3:51 pm - 12/08/2025 3:51 pm on tenant Built-in default tenant	6 seconds	0 seconds	Queued
	15:51:15	Session Viewing Status Grid		David test rule Between 12/07/2025 3:51 pm - 12/08/2025 3:51 pm on tenant Built-in default tenant	6 seconds	0 seconds	Queued
	15:51:15	Overtime Work Grid	T-WS22.e...	David test rule Between 12/07/2025 3:51 pm - 12/08/2025 3:51 pm on tenant Built-in default tenant	1 second	6 seconds	In Progress
	15:51:14	Activity Summary Grid (Gro...	T-WS22.e...	David test rule Between 12/07/2025 3:51 pm - 12/08/2025 3:51 pm on tenant Built-in default tenant	0 seconds	7 seconds	In Progress
	15:51:14	Activity Pie Chart	T-WS22.e...	David test rule Between 12/07/2025 3:51 pm - 12/08/2025 3:51 pm on tenant Built-in default tenant	0 seconds	7 seconds	Canceled
	15:48:23	User Productivity Heatmap	T-WS22.e...	David test rule Between 12/07/2025 3:48 pm - 12/08/2025 3:48 pm on tenant Built-in default tenant	12 seconds	5 seconds	Finished

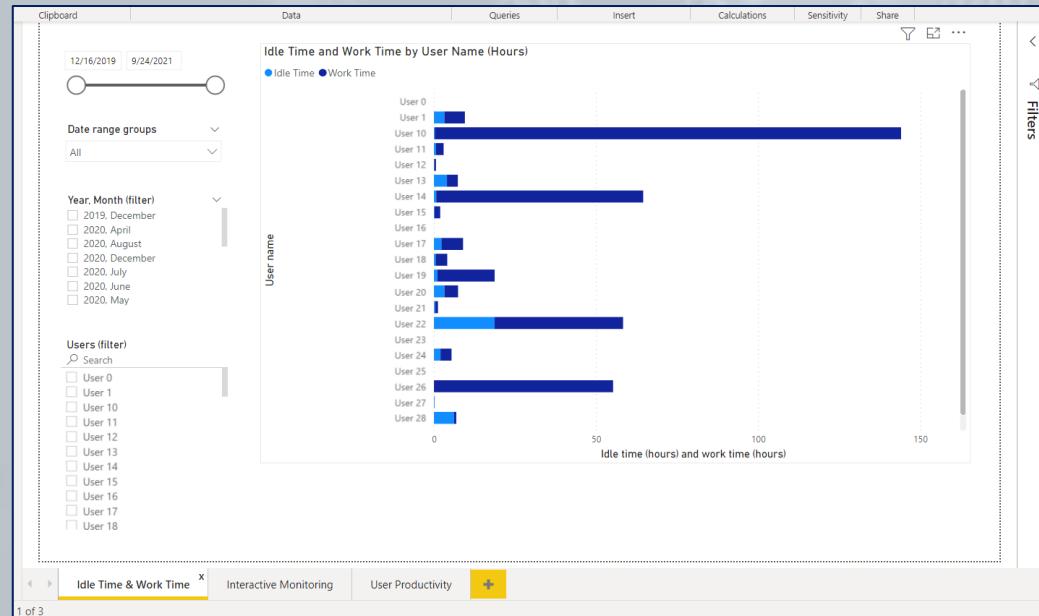
Syteca SDK, APIs and Integrations

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

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.

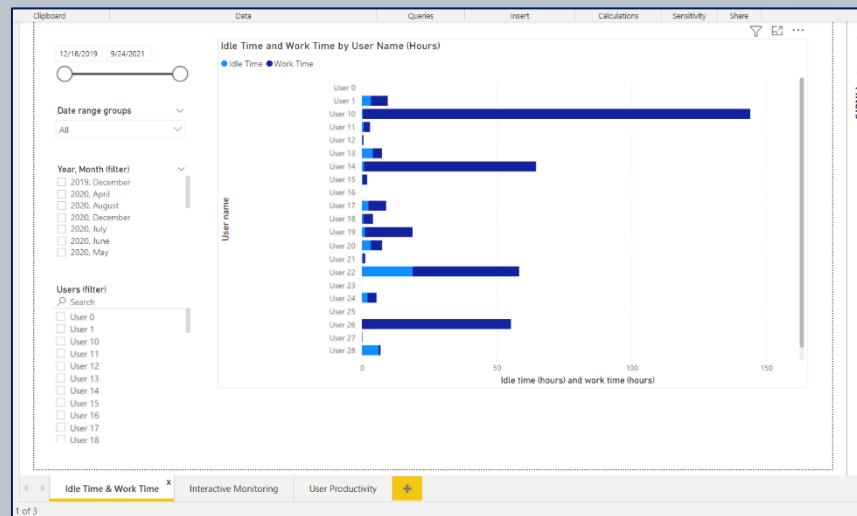
This application is designed to **allow customers to get Syteca monitoring data** via the API in order to **use for their own business purposes**.

Idle Time & Work Time Report

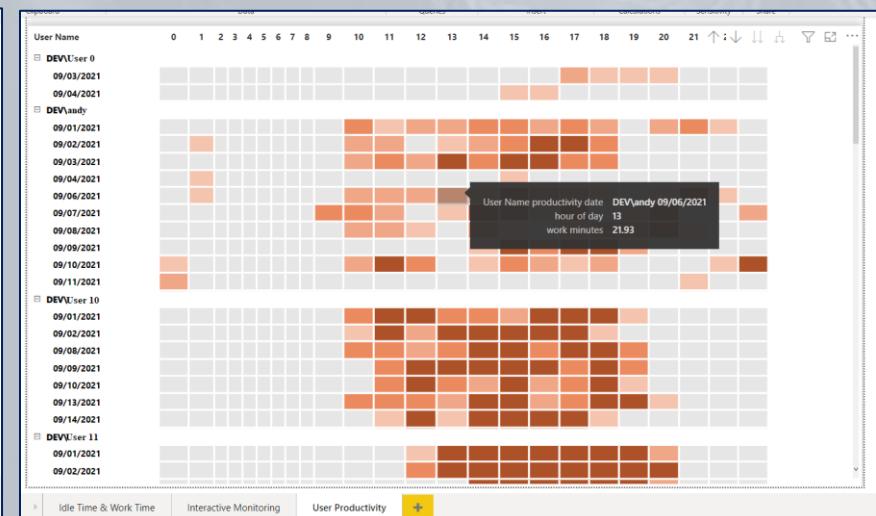


For example, **Client session records** containing **user productivity data** (such as **productivity time**, **idle time**, **duration**, etc.) can be used to build BI (business intelligence) reports in **Microsoft Power BI**.

Interactive Monitoring Report



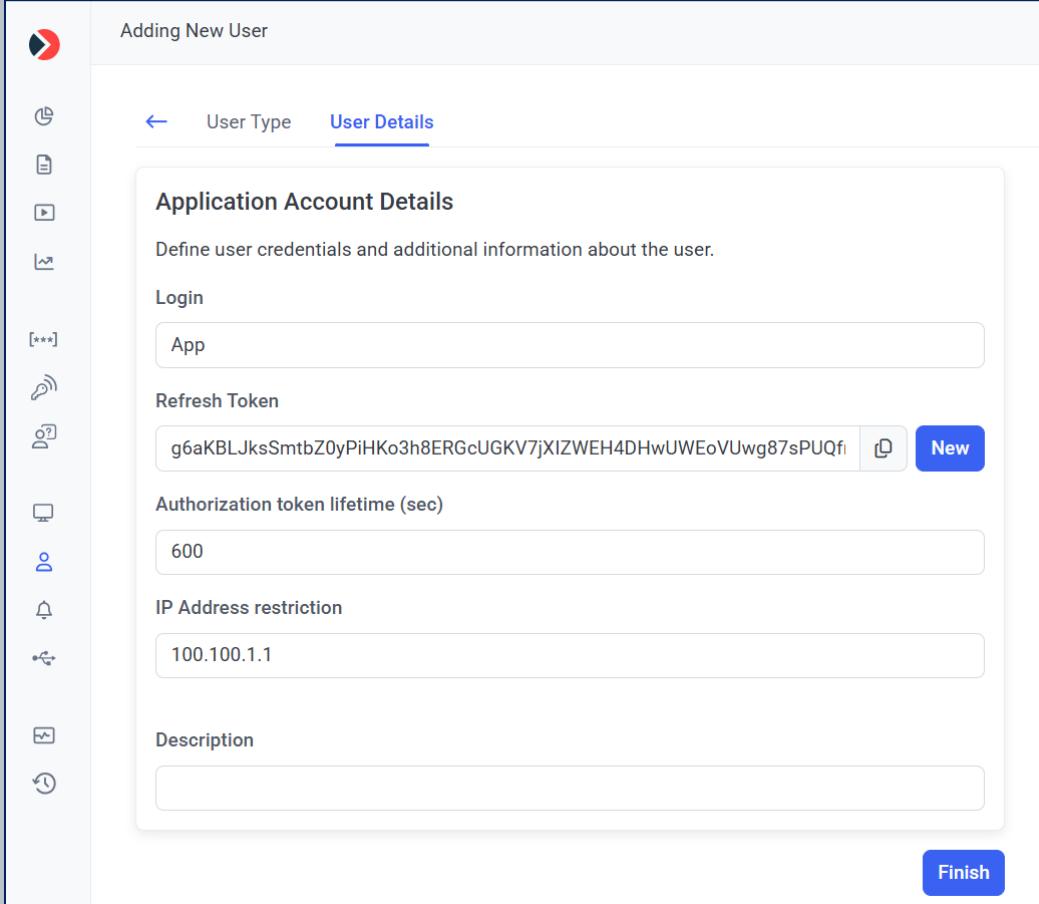
User Productivity Report



Syteca Application Credentials Broker (ACB) 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, add, and manage Syteca secrets' data via the ACB API**, to use it for their own business purposes.

ACB can also be used to **rotate the password of the default "admin" user** of Syteca via an external application.



Adding New User

User Type [User Details](#)

Application Account Details

Define user credentials and additional information about the user.

Login: App

Refresh Token: g6aKBLJksSmtbZ0yPiHKo3h8ERGcUGKV7jXIZWEH4DHwUWEoVUwg87sPUQfi [New](#)

Authorization token lifetime (sec): 600

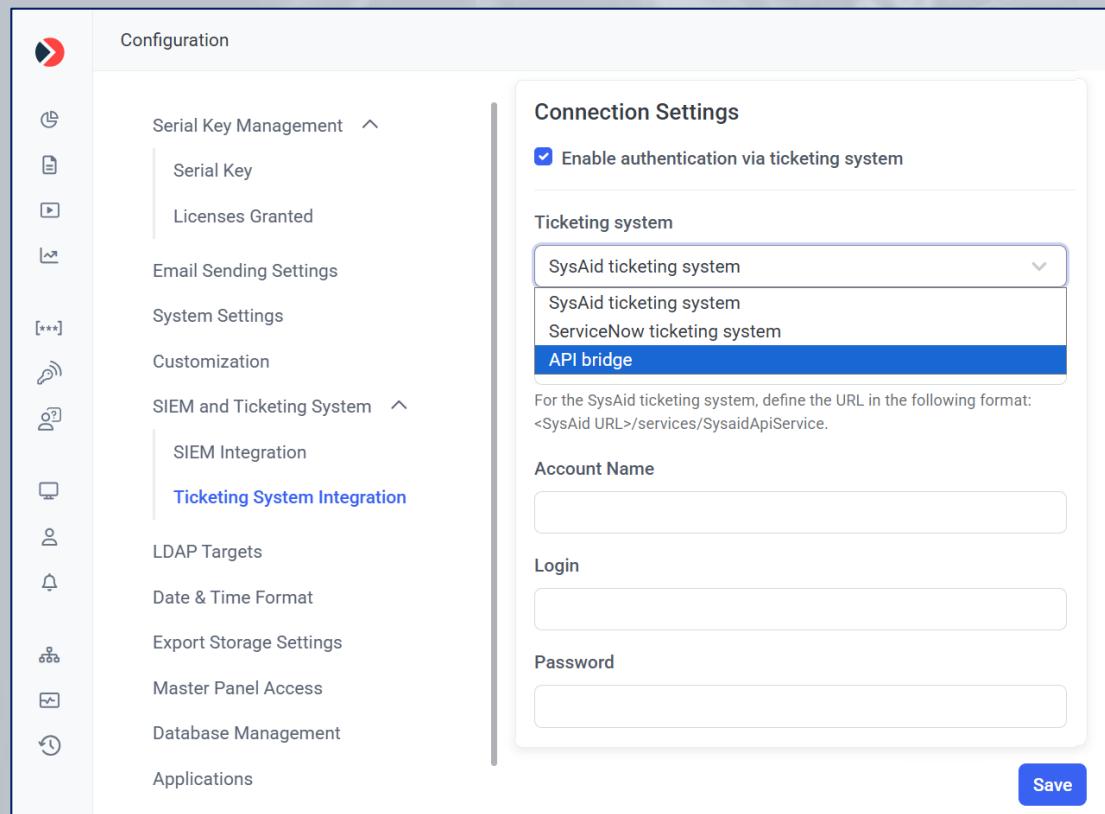
IP Address restriction: 100.100.1.1

Description:

Finish

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.



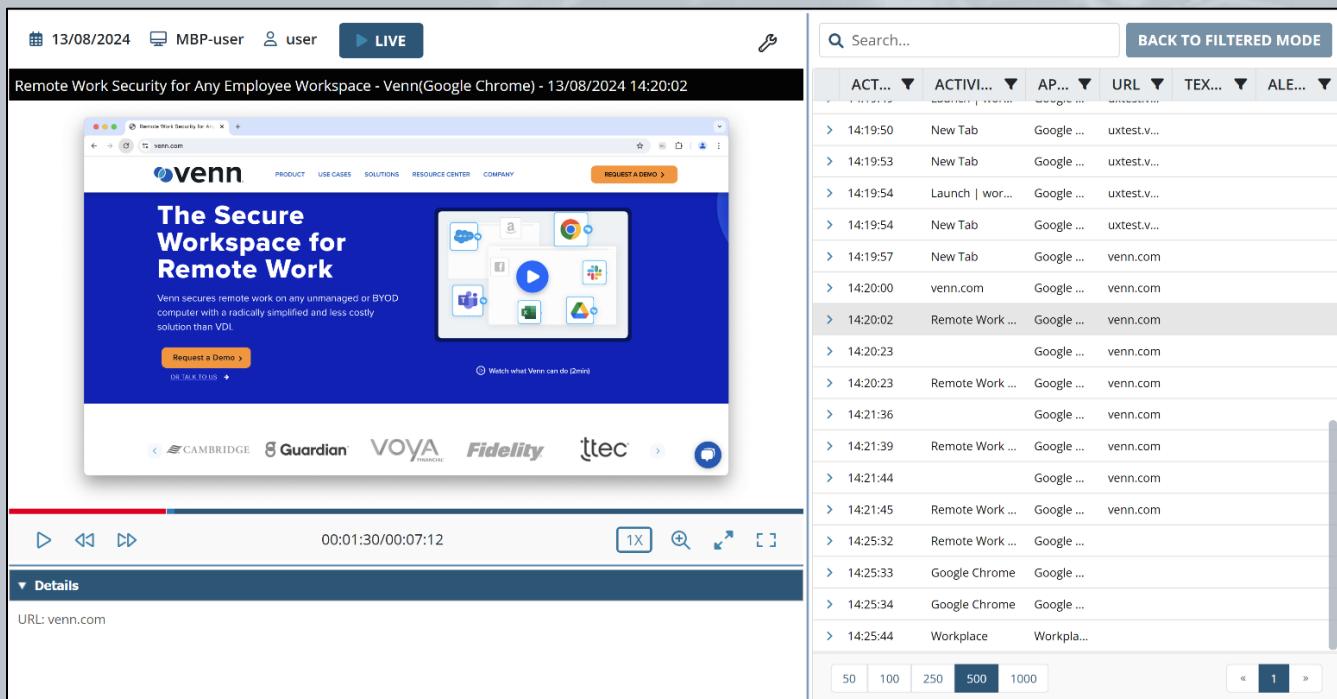
The screenshot shows the Syteca API Bridge configuration interface. The left sidebar has a red circular icon and a list of settings: Serial Key Management (Serial Key, Licenses Granted), System Settings, Customization, SIEM and Ticketing System (SIEM Integration, **Ticketing System Integration**), LDAP Targets, Date & Time Format, Export Storage Settings, Master Panel Access, Database Management, and Applications. The main panel is titled 'Configuration' and shows 'Connection Settings' with a checked checkbox for 'Enable authentication via ticketing system'. Under 'Ticketing system', 'SysAid ticketing system' is selected in a dropdown menu, with 'SysAid ticketing system', 'ServiceNow ticketing system', and 'API bridge' as options. Below the dropdown, a note says: 'For the SysAid ticketing system, define the URL in the following format: <SysAid URL>/services/Sysaid ApiService.' There are fields for 'Account Name', 'Login', and 'Password', and a 'Save' button at the bottom right.

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.



The screenshot displays the Syteca platform interface. On the left, a video player shows a screen recording of a Venn workspace. The workspace features a blue header with the Venn logo and the text 'The Secure Workspace for Remote Work'. Below the header, there's a section with icons for various applications like Google Chrome, Microsoft Word, and Microsoft Excel. On the right, a log table lists user activities. The columns include ACT..., ACTIVI..., AP..., URL, TEX..., and ALE... (partially visible). The log shows multiple entries for 'New Tab' and 'Launch' events, all associated with the URL 'venn.com'. The log table also includes a search bar at the top and pagination controls at the bottom.

ACT...	ACTIVI...	AP...	URL	TEX...	ALE...
> 14:19:50	New Tab	Google ...	uxtest.v...		
> 14:19:53	New Tab	Google ...	uxtest.v...		
> 14:19:54	Launch wor...	Google ...	uxtest.v...		
> 14:19:54	New Tab	Google ...	uxtest.v...		
> 14:19:57	New Tab	Google ...	venn.com		
> 14:20:00	venn.com	Google ...	venn.com		
> 14:20:02	Remote Work ...	Google ...	venn.com		
> 14:20:23		Google ...	venn.com		
> 14:20:23	Remote Work ...	Google ...	venn.com		
> 14:21:36		Google ...	venn.com		
> 14:21:39	Remote Work ...	Google ...	venn.com		
> 14:21:44		Google ...	venn.com		
> 14:21:45	Remote Work ...	Google ...	venn.com		
> 14:25:32	Remote Work ...	Google ...	venn.com		
> 14:25:33	Google Chrome	Google ...			
> 14:25:34	Google Chrome	Google ...			
> 14:25:44	Workplace	Workpla...			

Single Sign-On (SSO) Integrations



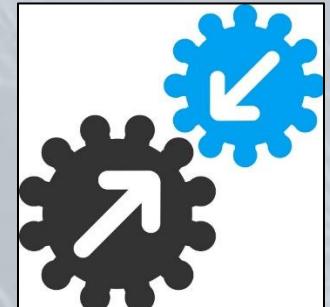
Syteca is **integrated with**, and **can be configured** for use with, several **SSO providers**.

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

A screenshot showing the Syteca management interface. On the left, a login page for 'One platform to secure your inside perimeter' is displayed, featuring fields for 'Login' and 'Password', a 'Remember me on this computer' checkbox, and 'Log In' and 'Log in with SSO' buttons. The 'Log in with SSO' button is highlighted with a red box. On the right, a configuration panel titled 'SSO Integration' is open, showing fields for 'Issuer name' (set to 'https://example/Syteca'), 'Identity provider metadata (xml)' (a file input field showing 'No file chosen'), and 'Certificate (pfx)' (a file input field showing 'No file chosen'). It also includes a 'Certificate password' field and a checked checkbox for 'Auto-create a Management Tool account for a new user on the first SSO login'. A 'Save' button is at the bottom right of the configuration panel. The Syteca logo is visible in the top right corner of the slide.

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-4096, 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.

For More Information...



Visit us online:
www.syteca.com