



Full Feature Presentation

Syteca

Enterprise Cybersecurity Platform

- [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.

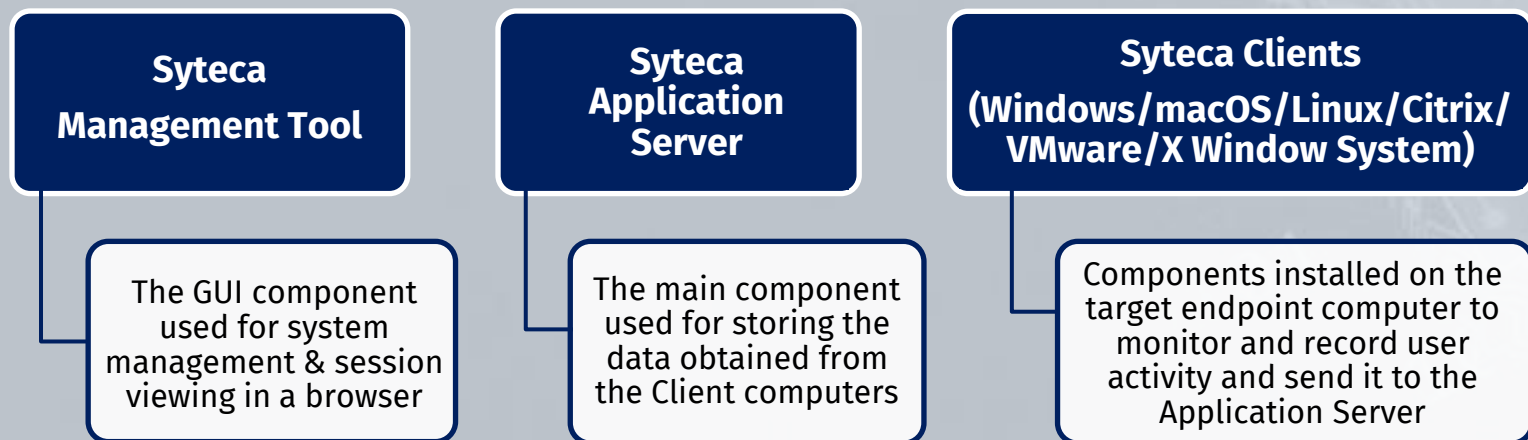
Flexible Deployment and Licensing

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.

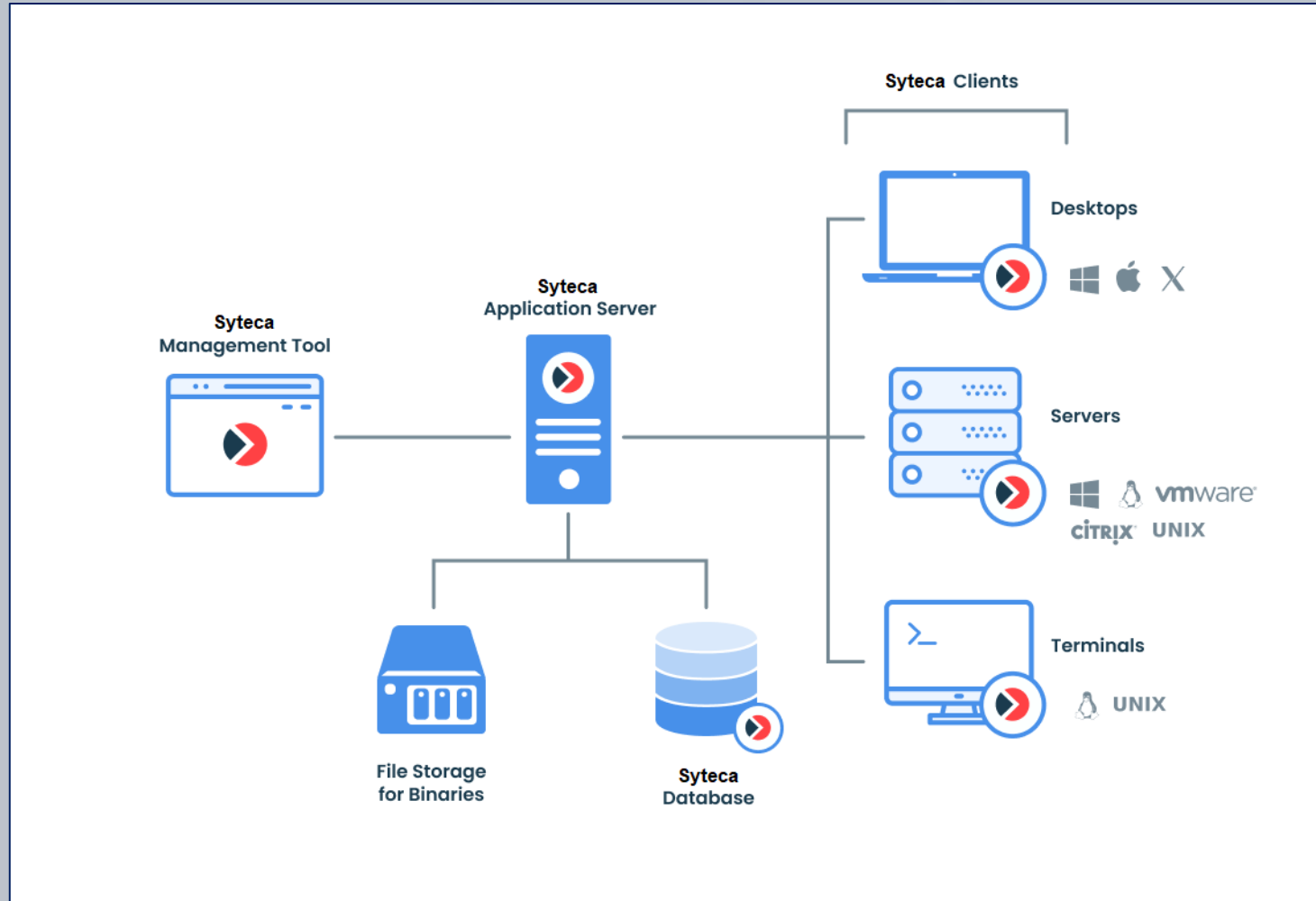
Syteca (formerly **Ekrans System**) is an enterprise-level **cybersecurity platform** software solution featuring **privileged access management (PAM)** and **user activity monitoring (UAM)**. It is used to **protect** your corporate IT infrastructure from **internal risks**, as well as to assist you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

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

The Main Components of Syteca



The Basic Deployment Scheme

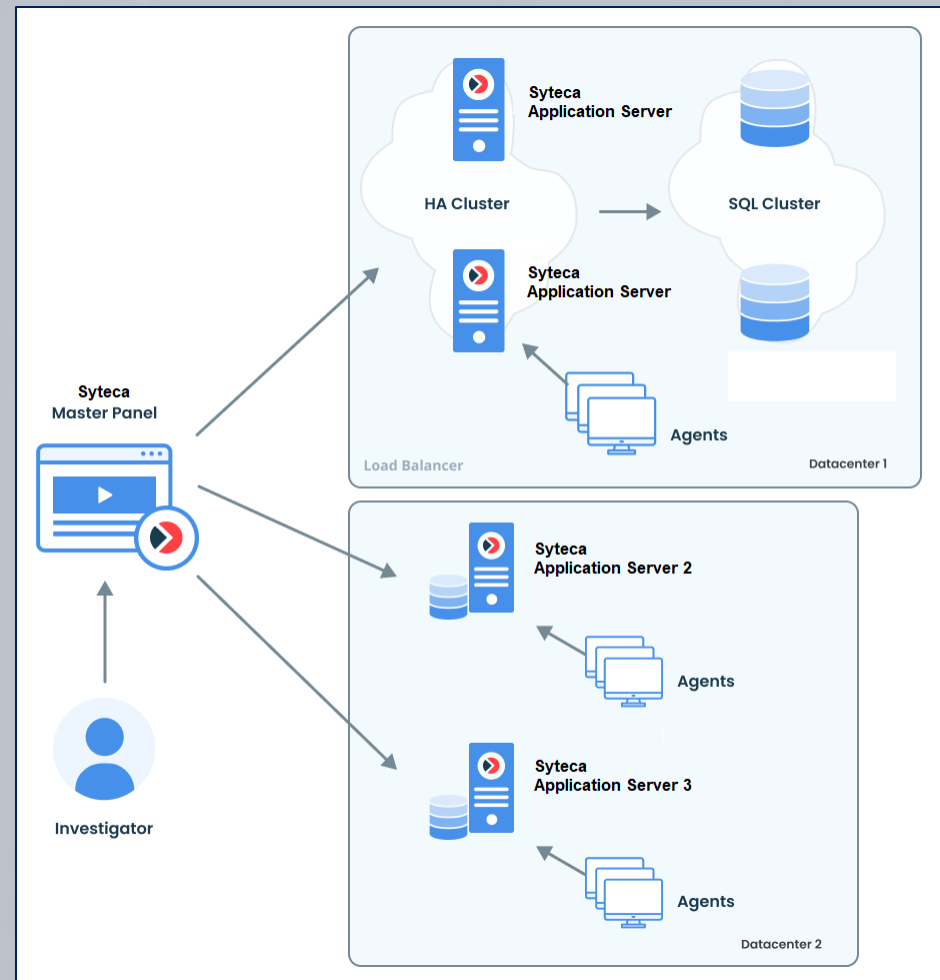


Large-Scale Deployments

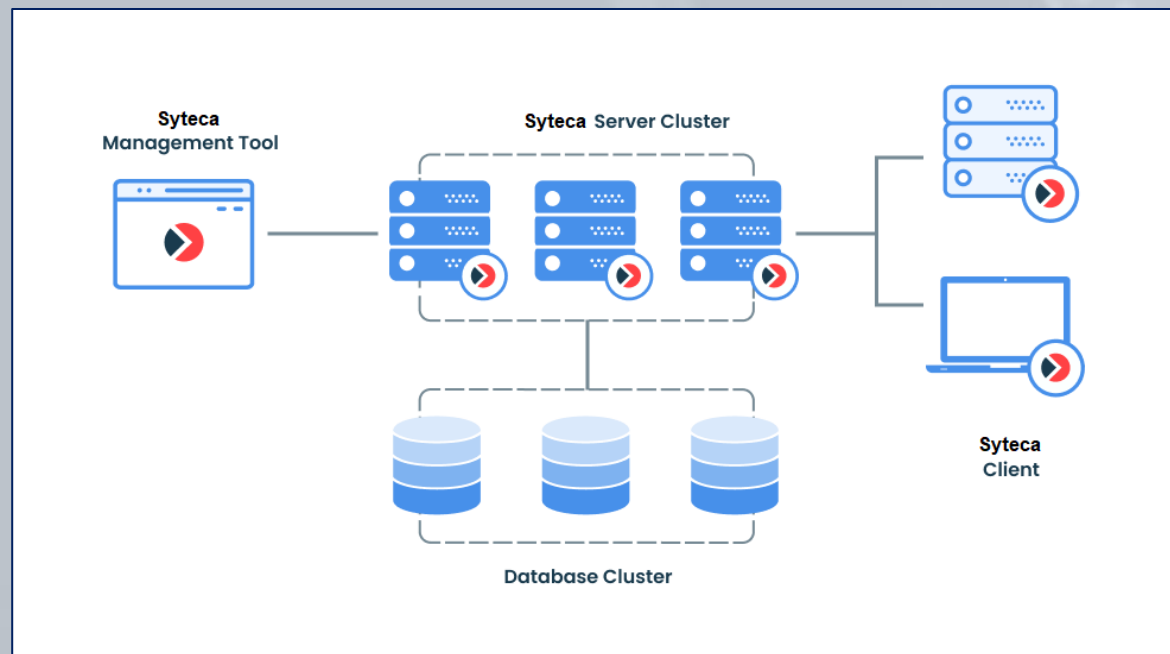
In terms of scalability, and for large organizations which may have several geographically isolated data centers, **multiple connected** instances of the **Application Server** can be deployed.

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

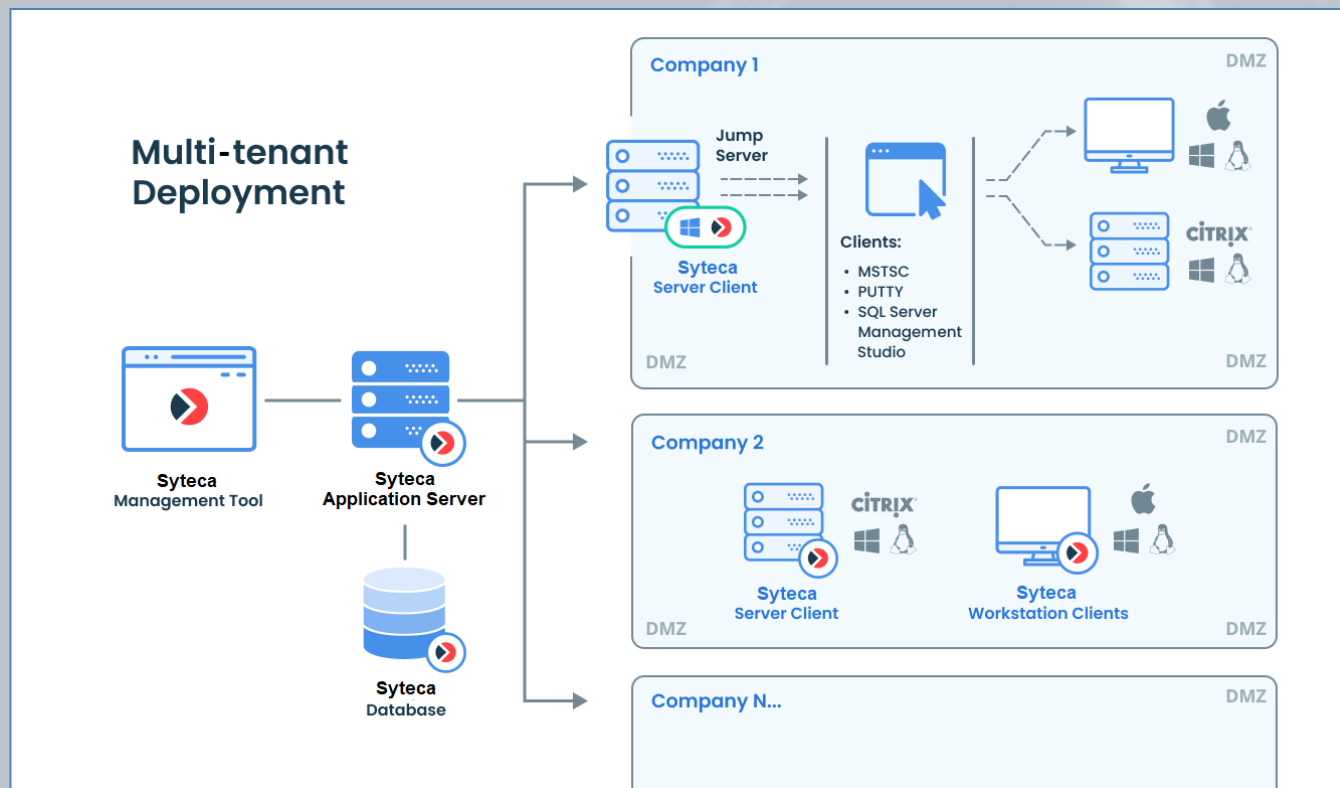
The **Master Panel**, which is an additional stand-alone component of Syteca, **combines the data** recorded by all Syteca Applications Servers in multiple locations, allowing the data to be **viewed and managed in a single user interface**.



High Availability mode 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.



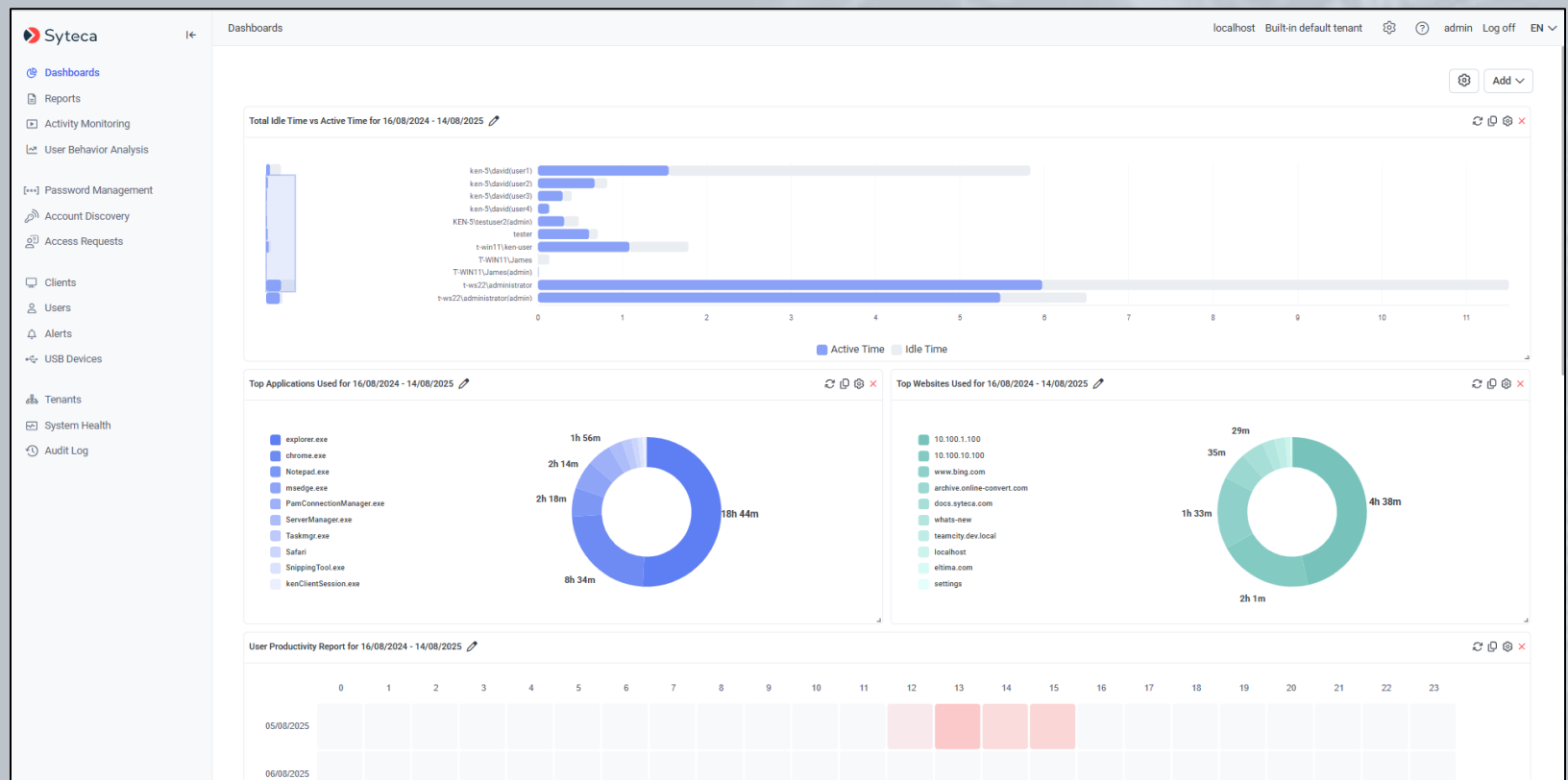
Syteca Application Server & the Management Tool

(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.

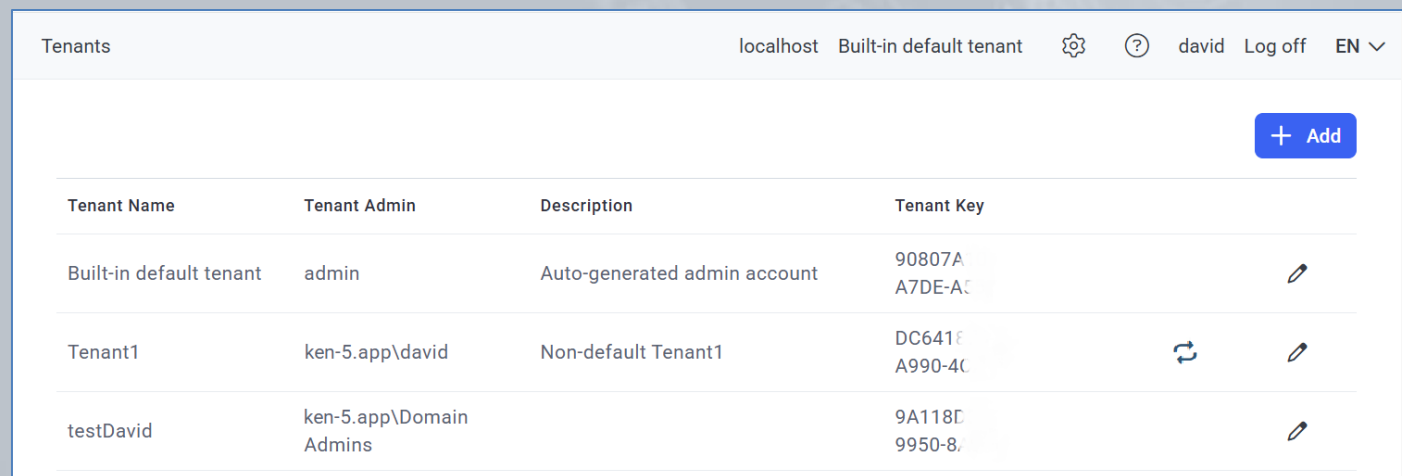


Syteca can operate in Single-Tenant or **Multi-Tenant mode**.

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**.



The screenshot shows the 'Tenants' management page in the Syteca interface. At the top, there's a header with 'Tenants' on the left and user information 'localhost Built-in default tenant david Log off EN' on the right. A blue '+ Add' button is in the top right corner. Below is a table with four columns: 'Tenant Name', 'Tenant Admin', 'Description', and 'Tenant Key'. There are three rows of tenants. Each row has an edit icon (pencil) on the right. The 'Tenant1' row also has a refresh icon (circular arrows).

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	DC641F A990-4C
testDavid	ken-5.app\Domain Admins		9A118D 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).

localhost Built-in default tenant   admin Log off EN 

Add Refresh Automatic LDAP Target Sync Active Directory User Groups

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	Administ...	Automatic		
LDAPS://10.10.10.50:636/DC=ken-5,DC=app	ken.local	ken.local	orig1	Manual		
GC://100.100.100.100	forest.com	AD-Forest	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

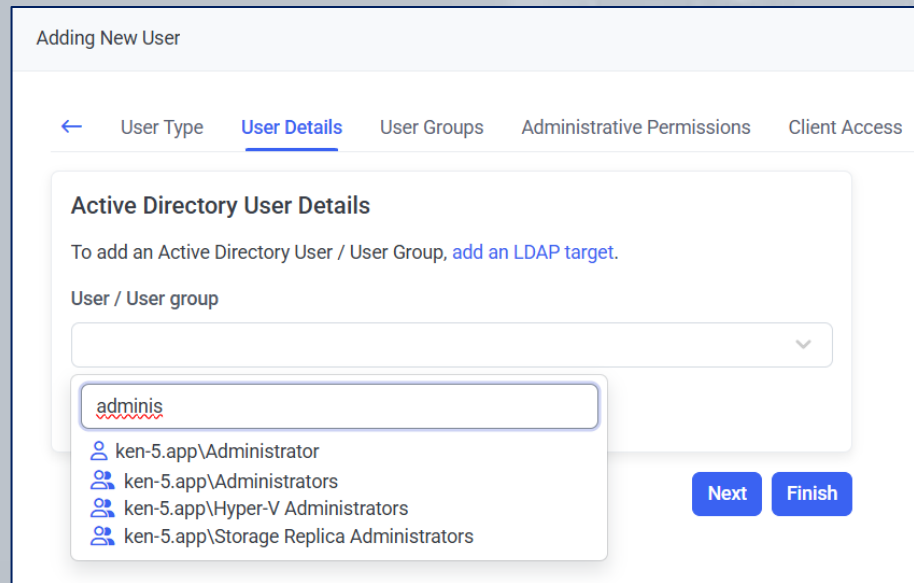
AD acc 3 testuser2

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](#).

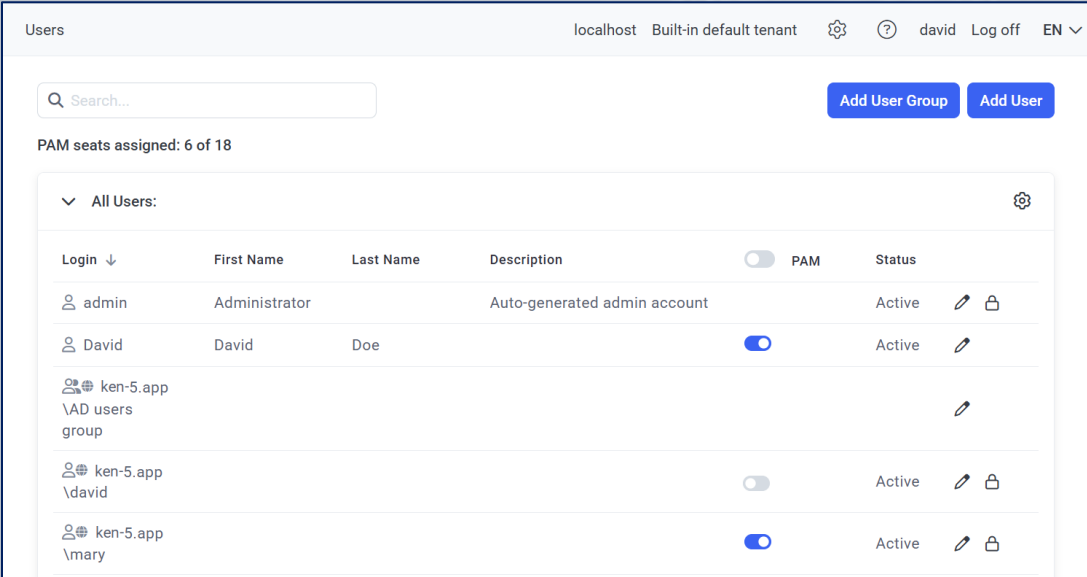
User / User group

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).

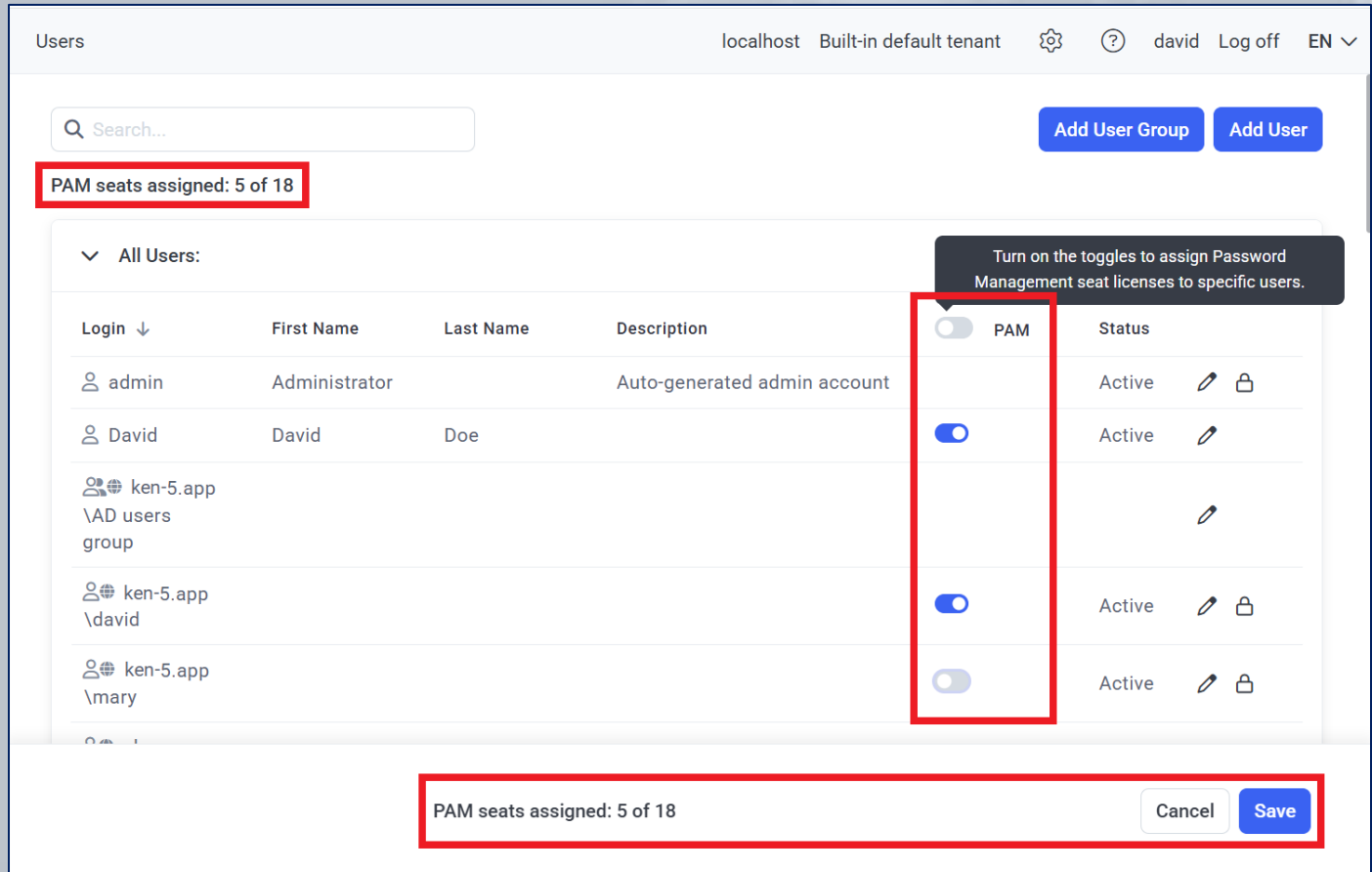


The screenshot shows the 'Users' management page in the Syteca interface. At the top, there's a header with 'localhost', 'Built-in default tenant', and user information 'david'. Below the header is a search bar and two buttons: 'Add User Group' and 'Add User'. A status message indicates 'PAM seats assigned: 6 of 18'. The main section is titled 'All Users:' and contains a table of users.

Login ↓	First Name	Last Name	Description	PAM	Status
admin	Administrator		Auto-generated admin account	☐	Active
David	David	Doe		☒	Active
ken-5.app VAD users group					
ken-5.app \david				☐	Active
ken-5.app \mary				☒	Active

Assign PAM Licenses to Users

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



The screenshot displays the 'Users' management interface. At the top, there's a search bar and buttons for 'Add User Group' and 'Add User'. A red box highlights the text 'PAM seats assigned: 5 of 18' in the top left. Below this, a table lists users with columns for 'Login', 'First Name', 'Last Name', 'Description', 'PAM' (toggle), and 'Status'. A red box highlights the 'PAM' toggle column, showing that David Doe and ken-5.app \david have their toggles turned on. A tooltip above the toggles reads: 'Turn on the toggles to assign Password Management seat licenses to specific users.' At the bottom, another red box highlights the 'PAM seats assigned: 5 of 18' text and 'Cancel'/'Save' buttons.

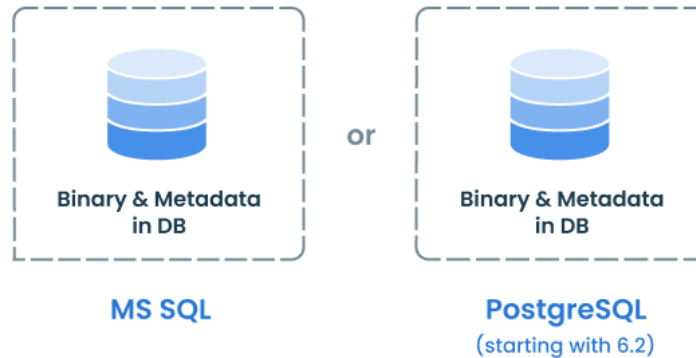
Login ↓	First Name	Last Name	Description	PAM	Status
admin	Administrator		Auto-generated admin account	☐	Active  
David	David	Doe		☒	Active 
ken-5.app \AD users group				☐	
ken-5.app \david				☒	Active  
ken-5.app \mary				☐	Active  

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

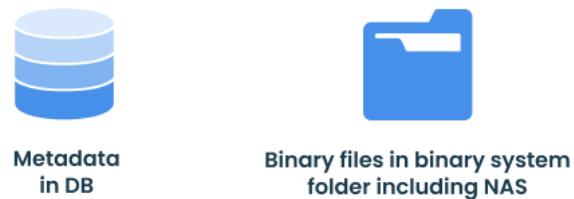
Audit Log						
localhost Built-in default tenant david Log off EN						
When	All	Who	All	Action	All	More Criteria
Export Filtered Records to CSV Export Filtered Records to PDF						
Time ↓	User Name	User Groups	Category	Action	Object	Details
29/07/2025 14:12:22	david	Administ...	Log in / Log off	Log 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



Custom Configuration (MS SQL or PostgreSQL)



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

Auto-Cleanup Options

☐ Never
☐ Run once
☒ Repeat according to schedule

Perform every (days)

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

.....

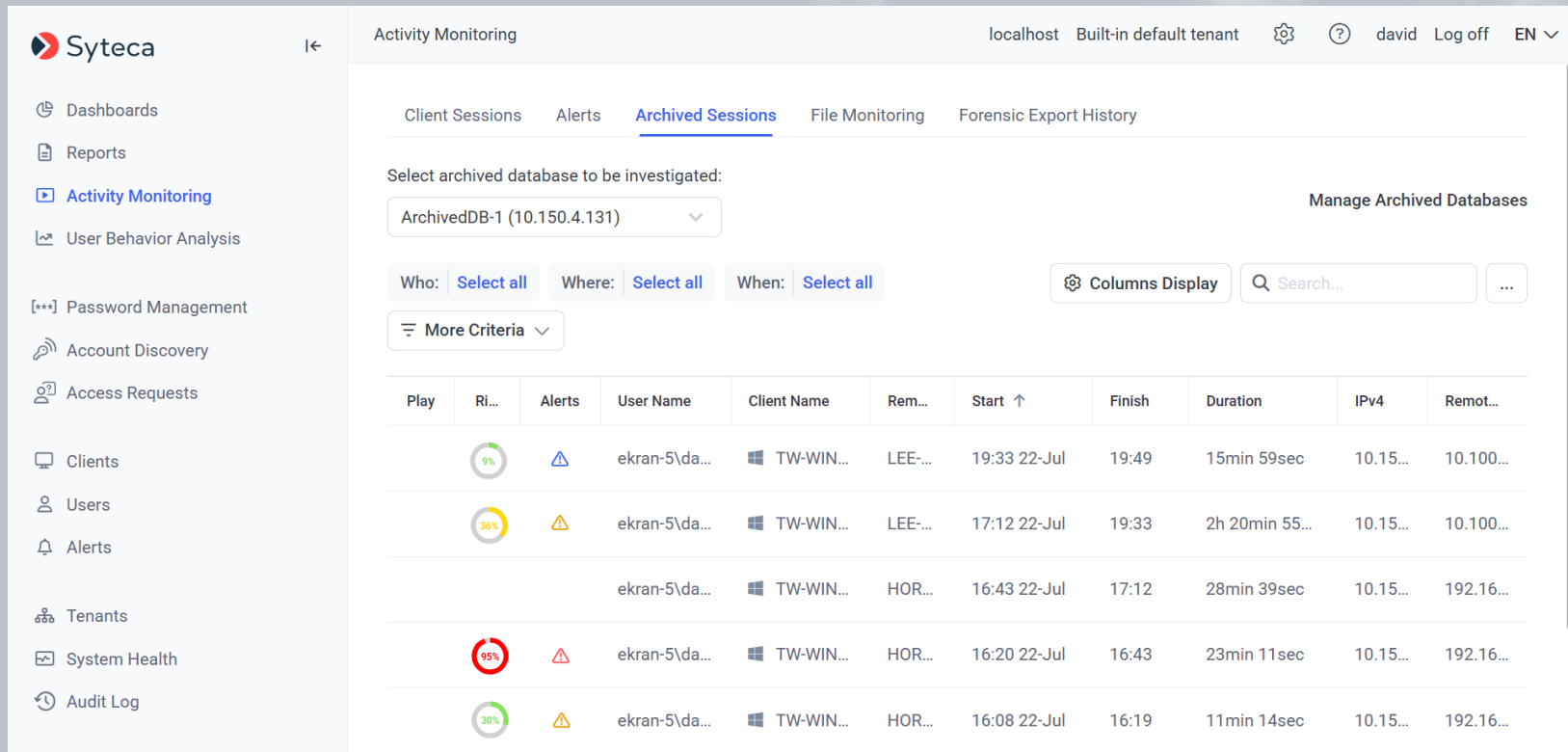
☐ Shrink database transaction log after cleanup

☐ Delete offline Clients without sessions

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

 Test Database Connection

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

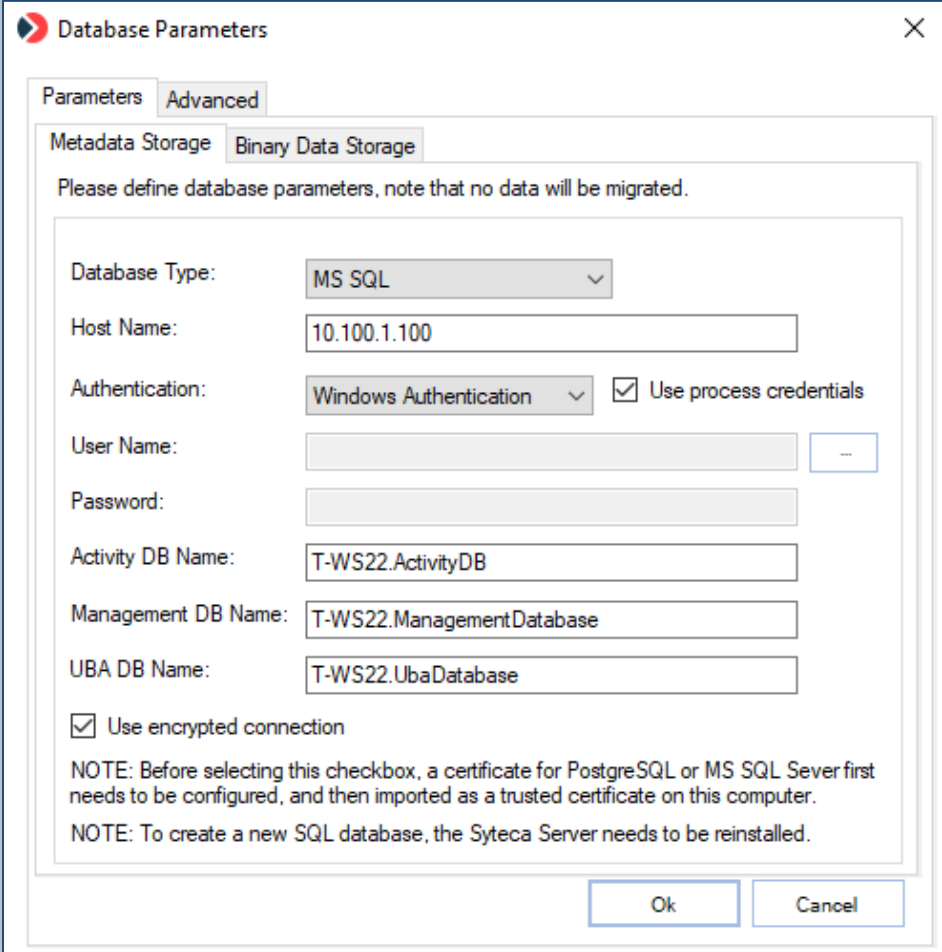


The screenshot displays the Syteca Activity Monitoring interface. The left sidebar contains navigation links: Dashboards, Reports, Activity Monitoring (selected), User Behavior Analysis, Password Management, Account Discovery, Access Requests, Clients, Users, Alerts, Tenants, System Health, and Audit Log. The main content area is titled 'Activity Monitoring' and includes tabs for Client Sessions, Alerts, Archived Sessions (selected), File Monitoring, and Forensic Export History. A dropdown menu allows selecting the archived database to be investigated, currently set to 'ArchivedDB-1 (10.150.4.131)'. Below this, filters for 'Who', 'Where', and 'When' are set to 'Select all'. A 'Columns Display' button and a search bar are also present. The table below lists archived sessions with columns for Play, Ri..., Alerts, User Name, Client Name, Rem..., Start, Finish, Duration, IPv4, and Remot....

Play	Ri...	Alerts	User Name	Client Name	Rem...	Start	Finish	Duration	IPv4	Remot...
			ekran-5\da...	TW-WIN...	LEE...	19:33 22-Jul	19:49	15min 59sec	10.15...	10.100...
			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...
			ekran-5\da...	TW-WIN...	HOR...	16:20 22-Jul	16:43	23min 11sec	10.15...	192.16...
			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.



The screenshot shows the 'Database Parameters' dialog box with the 'Advanced' tab selected. The 'Metadata Storage' and 'Binary Data Storage' sub-tabs are also visible. The main instruction reads: 'Please define database parameters, note that no data will be migrated.' The configuration fields are as follows:

- Database Type: MS SQL (dropdown)
- Host Name: 10.100.1.100 (text box)
- Authentication: Windows Authentication (dropdown) with a checked 'Use process credentials' checkbox.
- User Name: (text box) with a browse button ('...').
- Password: (password text box).
- Activity DB Name: T-WS22.ActivityDB (text box)
- Management DB Name: T-WS22.ManagementDatabase (text box)
- UBA DB Name: T-WS22.UbaDatabase (text box)
- A checked 'Use encrypted connection' checkbox.

Two notes are provided at the bottom of the configuration area:

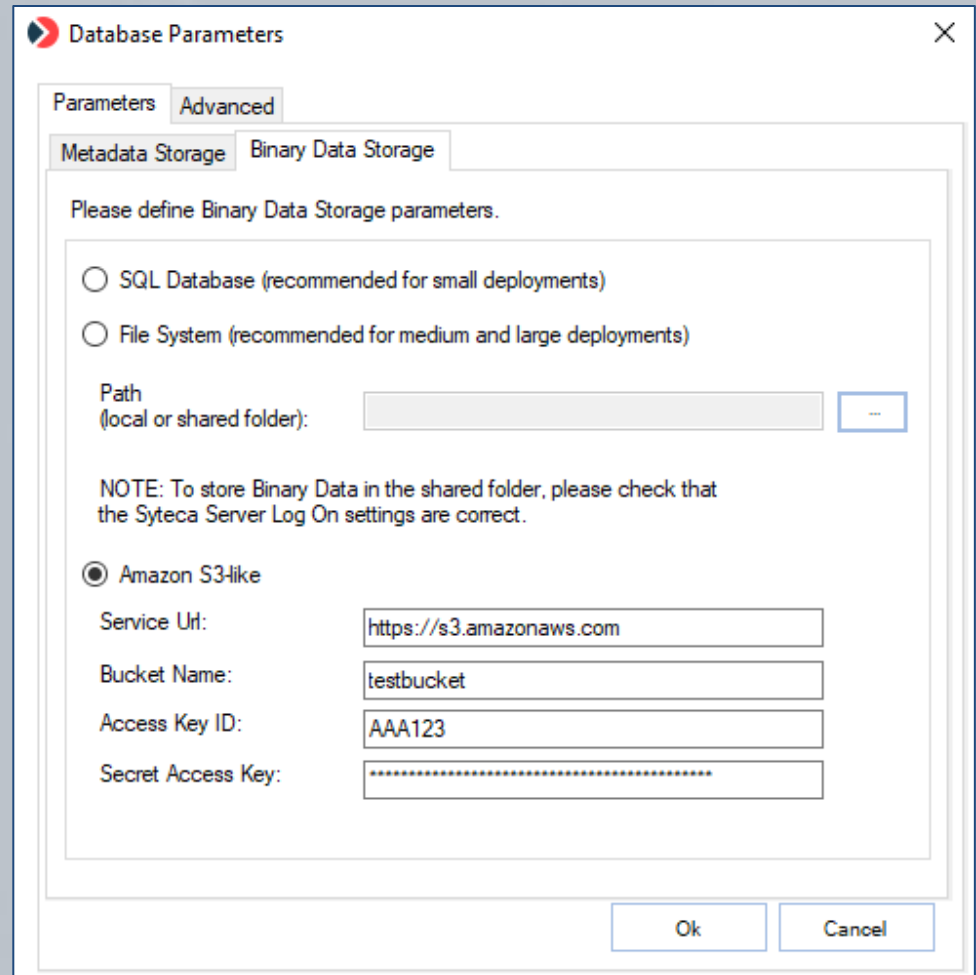
- NOTE: Before selecting this checkbox, a certificate for PostgreSQL or MS SQL Sever first needs to be configured, and then imported as a trusted certificate on this computer.
- NOTE: To create a new SQL database, the Syteca Server needs to be reinstalled.

'Ok' and 'Cancel' buttons are located at the bottom right of the dialog.

Database Parameters (for Binary Data Storage)

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

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



The screenshot shows a 'Database Parameters' dialog box with a close button (X) in the top right corner. It has two tabs: 'Parameters' and 'Advanced'. The 'Advanced' tab is active, and within it, there are two sub-tabs: 'Metadata Storage' and 'Binary Data Storage'. The 'Binary Data Storage' sub-tab is selected. The text 'Please define Binary Data Storage parameters.' is displayed. There are two radio button options: 'SQL Database (recommended for small deployments)' and 'File System (recommended for medium and large deployments)'. Below these is a 'Path (local or shared folder):' label followed by a text input field and a browse button (three dots). A note states: 'NOTE: To store Binary Data in the shared folder, please check that the Syteca Server Log On settings are correct.' The 'Amazon S3-like' option is selected with a radio button. Below it are four text input fields: 'Service Uri:' with the value 'https://s3.amazonaws.com', 'Bucket Name:' with the value 'testbucket', 'Access Key ID:' with the value 'AAA123', and 'Secret Access Key:' with a masked value represented by dots. At the bottom right are 'Ok' and 'Cancel' buttons.

Database Parameters

Parameters Advanced

Metadata Storage Binary Data Storage

Please define Binary Data Storage parameters.

☐ SQL Database (recommended for small deployments)

☐ File System (recommended for medium and large deployments)

Path
(local or shared folder):

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

☒ Amazon S3-like

Service Uri:

Bucket Name:

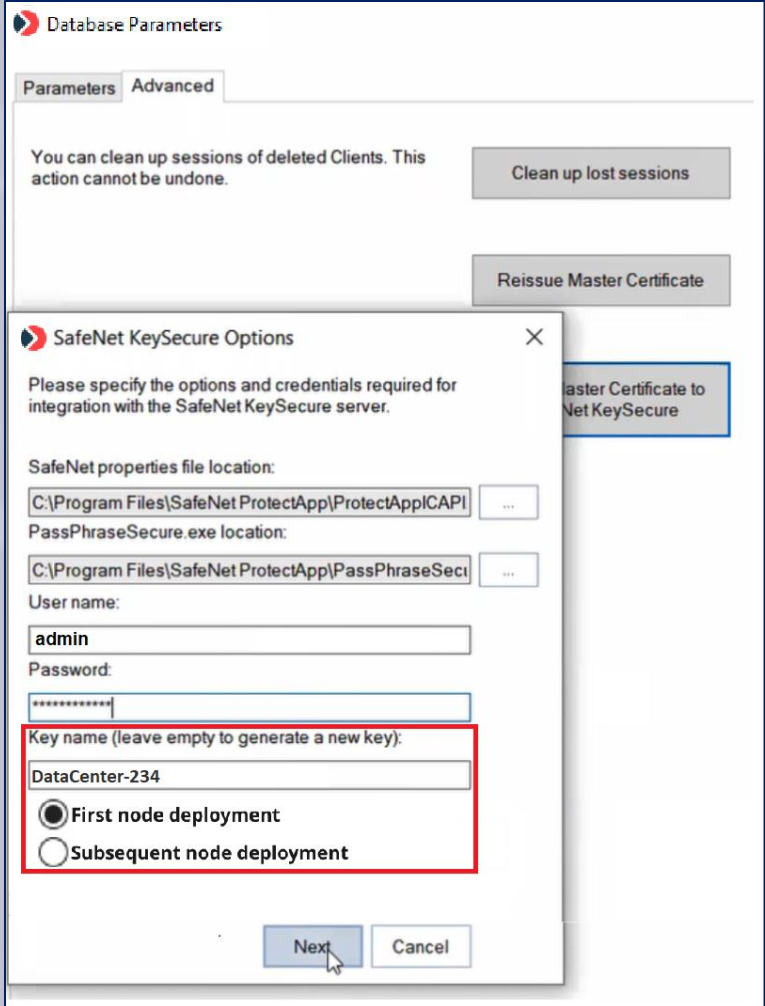
Access Key ID:

Secret Access Key:

Ok Cancel

Database Parameters (Hardware Security Module) Syteca

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



The screenshot shows the 'Database Parameters' dialog box with the 'Advanced' tab selected. The 'Parameters' tab is also visible. The 'Advanced' tab contains two buttons: 'Clean up lost sessions' and 'Reissue Master Certificate'. The 'SafeNet KeySecure Options' sub-dialog box is open, displaying the following fields and options:

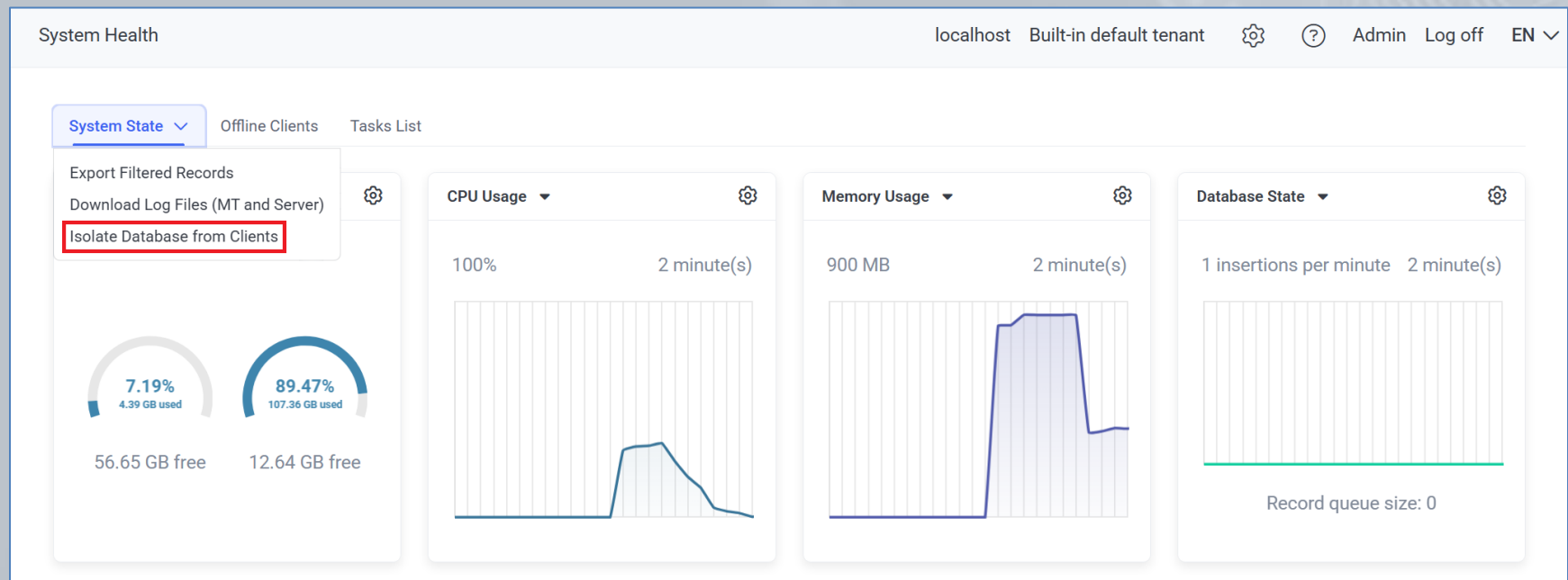
- SafeNet properties file location: C:\Program Files\SafeNet ProtectApp\ProtectApp\CAPI\ ...
- PassPhraseSecure.exe location: C:\Program Files\SafeNet ProtectApp\PassPhraseSeci ...
- User name: admin
- Password: [masked]
- Key name (leave empty to generate a new key): DataCenter-234
- Deployment options: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

The 'Next' button is highlighted with a mouse cursor.

Isolating the Database from Clients



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



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

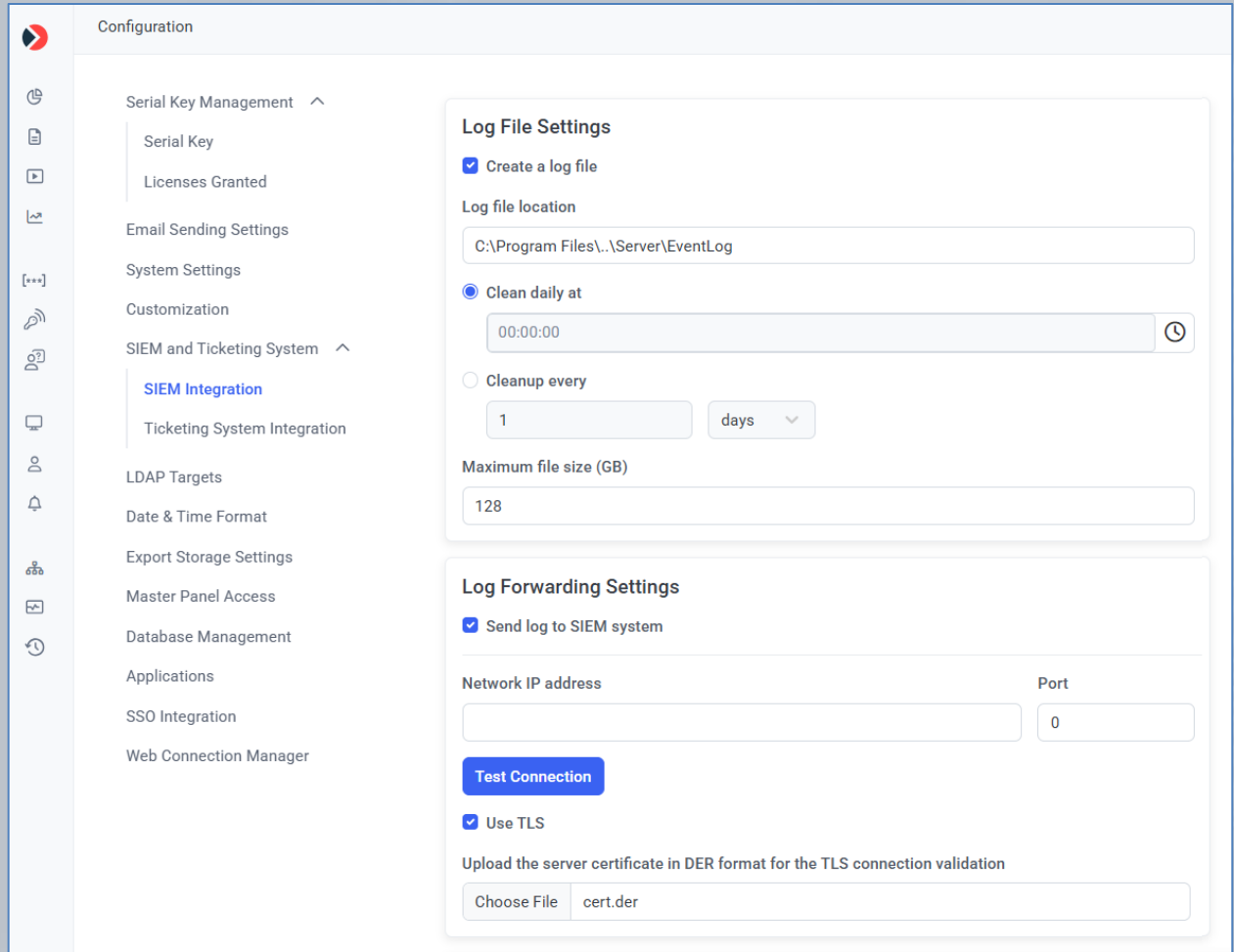
Log Files

- ☒ 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 displays the Syteca Configuration interface. On the left is a sidebar with icons and a menu. The main area is titled 'Configuration' and contains a list of settings categories on the left and two configuration panels on the right.

Configuration Menu (Left):

- 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
- Web Connection Manager

Log File Settings (Right Panel):

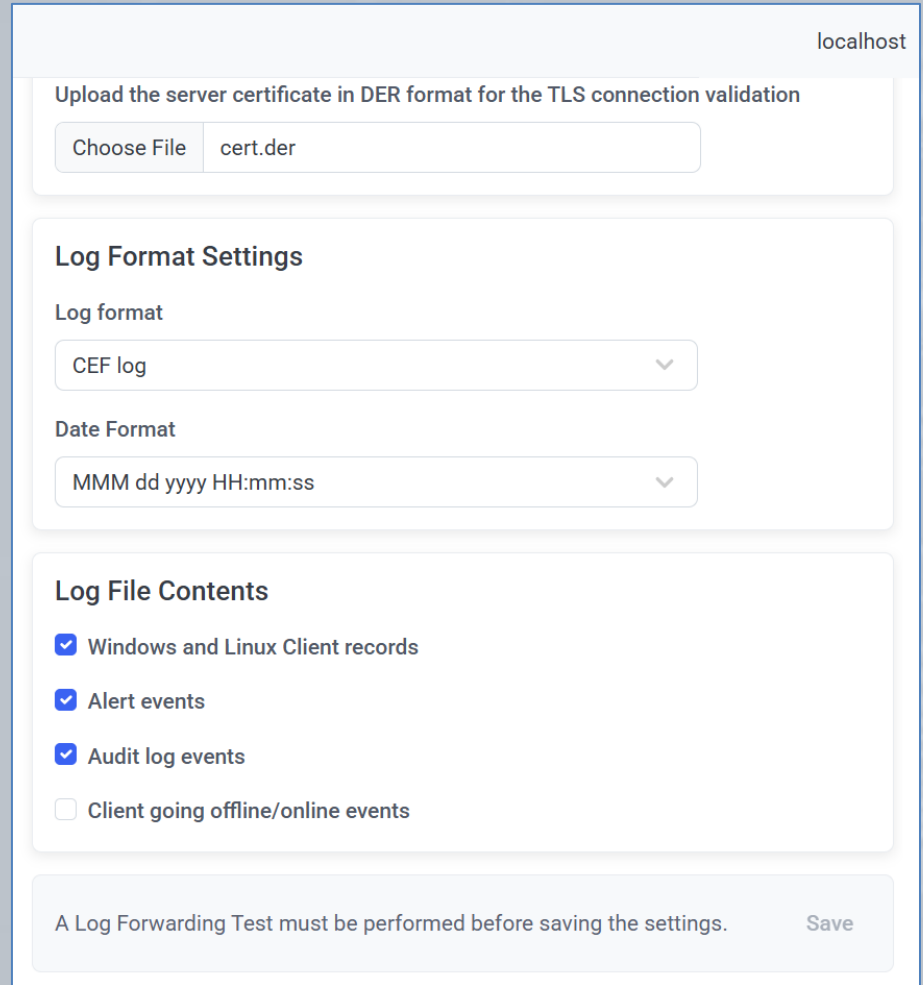
- ☒ Create a log file
- Log file location:
- ☒ Clean daily at:
- ☐ Cleanup every: days
- Maximum file size (GB):

Log Forwarding Settings (Right Panel):

- ☒ Send log to SIEM system
- Network IP address:
- Port:
-
- ☒ Use TLS
- Upload the server certificate in DER format for the TLS connection validation:

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)



The screenshot shows a web-based configuration interface for Syteca SIEM integration. The interface is titled 'localhost' in the top right corner. It contains three main sections: 1. 'Upload the server certificate in DER format for the TLS connection validation' with a 'Choose File' button and a text input field containing 'cert.der'. 2. 'Log Format Settings' with two dropdown menus: 'Log format' set to 'CEF log' and 'Date Format' set to 'MMM dd yyyy HH:mm:ss'. 3. 'Log File Contents' with four checkboxes: 'Windows and Linux Client records' (checked), 'Alert events' (checked), 'Audit log events' (checked), and 'Client going offline/online events' (unchecked). At the bottom, there is a message: 'A Log Forwarding Test must be performed before saving the settings.' and a 'Save' button.

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

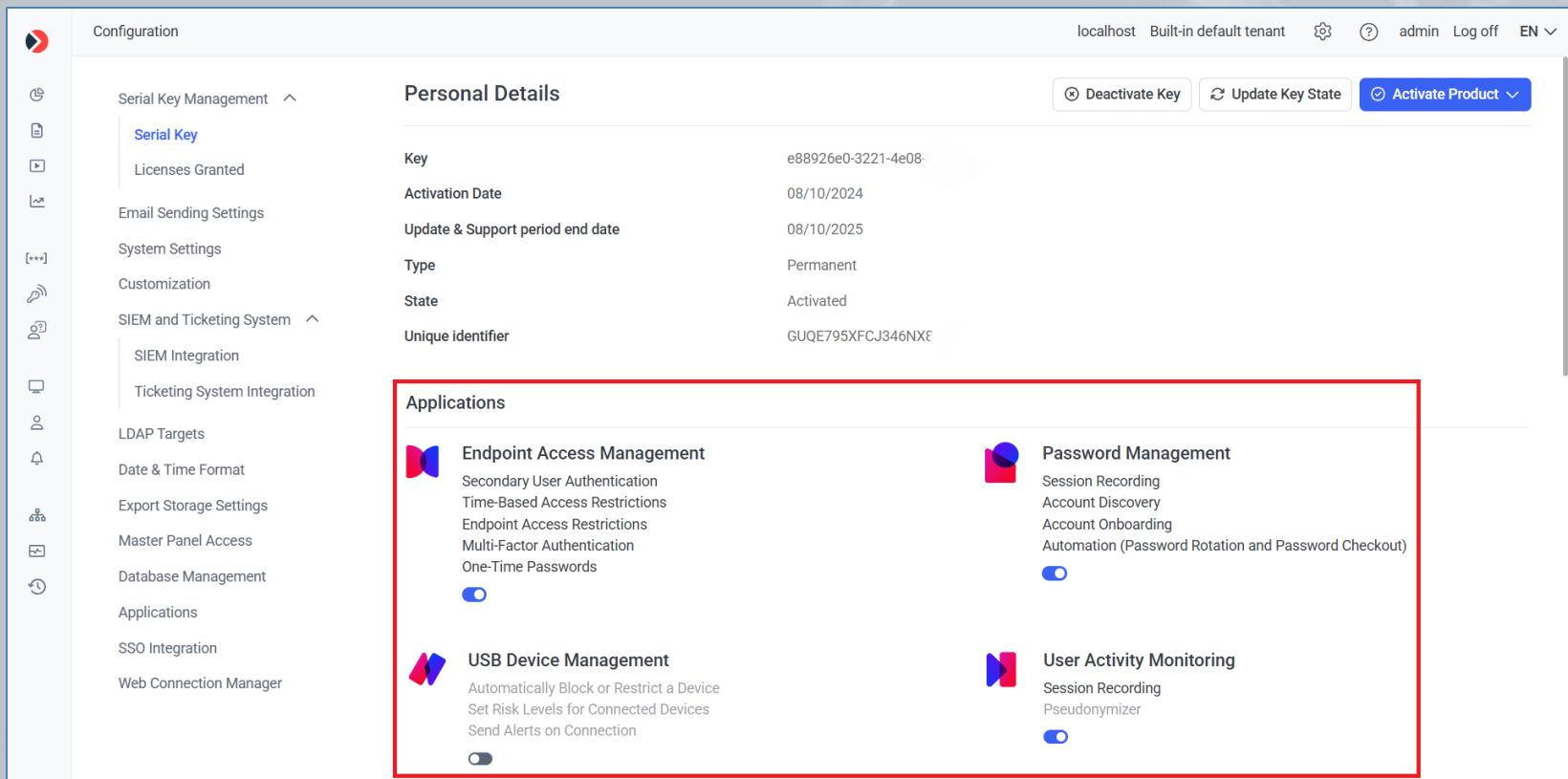
☐ Client going offline/online events

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 displays the Syteca Configuration interface. The left sidebar lists various configuration categories, including Serial Key Management, Email Sending Settings, System Settings, Customization, SIEM and Ticketing System, LDAP Targets, Date & Time Format, Export Storage Settings, Master Panel Access, Database Management, Applications, SSO Integration, and Web Connection Manager. The main content area is titled 'Configuration' and shows the 'Serial Key Management' section. The 'Personal Details' table lists the following information:

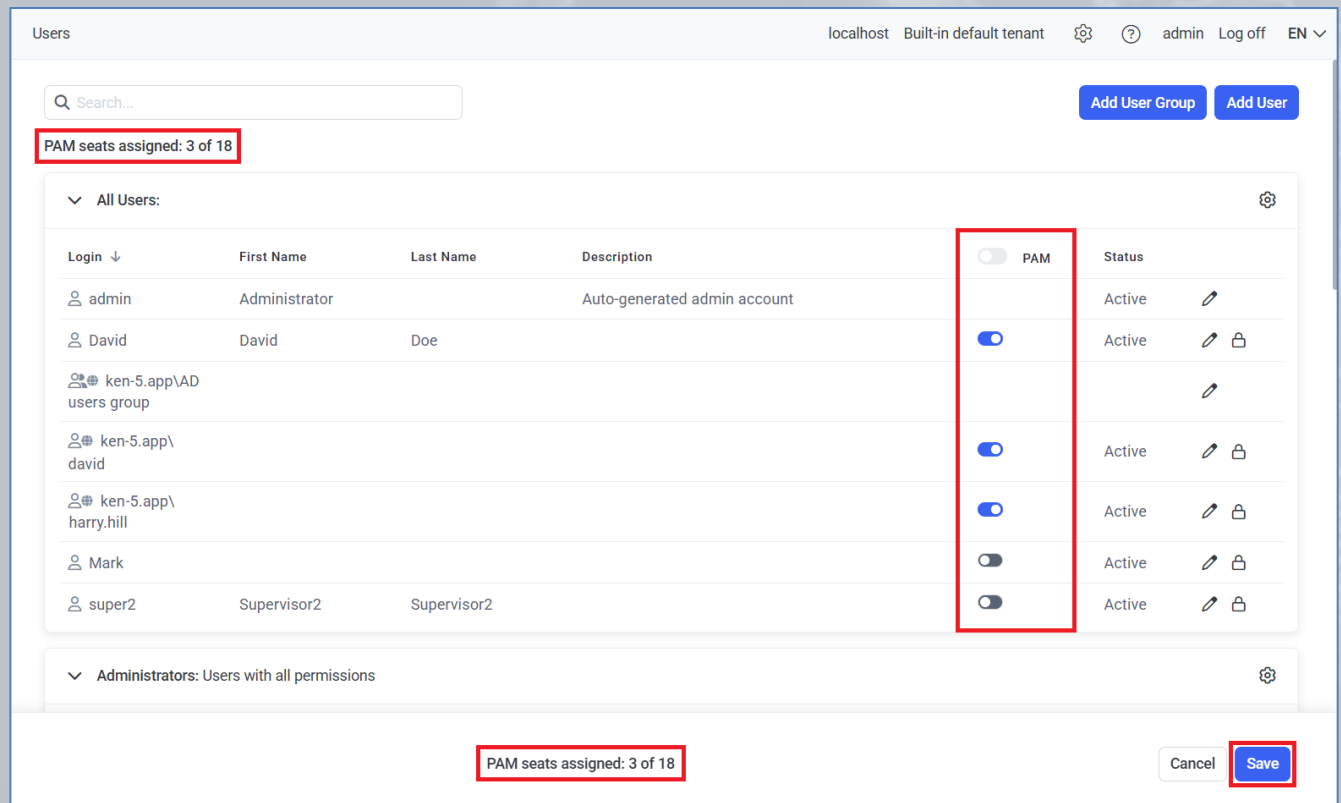
Field	Value
Key	e88926e0-3221-4e08
Activation Date	08/10/2024
Update & Support period end date	08/10/2025
Type	Permanent
State	Activated
Unique Identifier	GUQE795XFCJ346NXE

Below the table, the 'Applications' section is highlighted with a red box. It contains four applications, each with a list of features and a toggle switch:

- Endpoint Access Management**
 - Secondary User Authentication
 - Time-Based Access Restrictions
 - Endpoint Access Restrictions
 - Multi-Factor Authentication
 - One-Time Passwords
 - Toggle: ☒
- Password Management**
 - Session Recording
 - Account Discovery
 - Account Onboarding
 - Automation (Password Rotation and Password Checkout)
 - Toggle: ☒
- USB Device Management**
 - Automatically Block or Restrict a Device
 - Set Risk Levels for Connected Devices
 - Send Alerts on Connection
 - Toggle: ☒
- User Activity Monitoring**
 - Session Recording
 - Pseudonymizer
 - Toggle: ☒

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 displays the 'Users' management page in the Syteca interface. At the top, it shows 'localhost Built-in default tenant' and user 'admin' with a 'Log off' button. A search bar is present, and buttons for 'Add User Group' and 'Add User' are on the right. A red box highlights the text 'PAM seats assigned: 3 of 18' below the search bar. The main section is titled 'All Users:' and contains a table with columns: Login, First Name, Last Name, Description, PAM (toggle), and Status. The table lists several users, including 'admin', 'David', and a group 'ken-5.app\AD users group'. A red box highlights the 'PAM' toggle column, showing that three users have the toggle turned on. At the bottom, another red box highlights 'PAM seats assigned: 3 of 18' and 'Cancel' and 'Save' buttons are visible.

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

Endpoint Licenses (for Client Computers)



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

localhost Built-in default tenant ? admin Log off EN ▾			
Seat Licenses (20)			
PAM Seats assigned: 4 of 20			
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**.

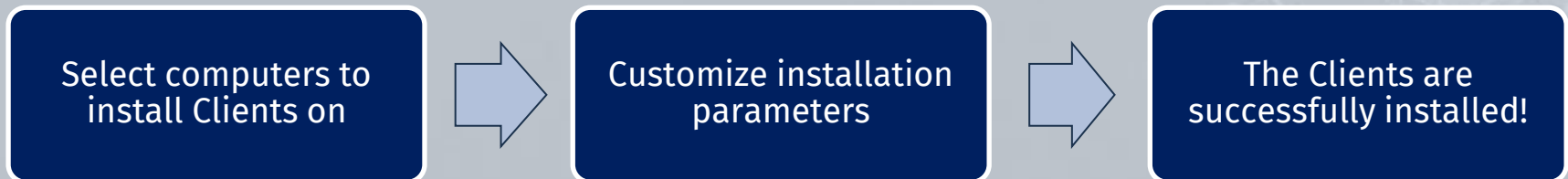
- **Manual** reassignment: Can be done **at any time**, in just a **couple of clicks**.
- **Automatic** reassignment:
 - **Delete offline Clients without sessions**: This option allows the licenses of Clients, whenever they do not have sessions stored, to be returned to the pool of available endpoint 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



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**

IP Range Scan

←

Scan finished. 4 computer(s) detected.

☐	IP	Computer	Workgroup / Domain
☒	10.100.10.3	IMACP(10.100.10.3)	WORKGROUP
☐	10.100.10.101	DESKTOP-GF (10.100.10.101)	WORKGROUP
☐	10.100.10.131	T-WS22.ken-5.app (10.100.10.131)	ken-5.app
☒	10.100.10.178	WIN-AG7 (10.100.10.178)	KEN-5

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

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](#)

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

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 monitoring operations (e.g. **file upload**).
- **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**.

Editing Client (T-WIN11)

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

☒ Check changing of window titles

☒ Record user activity on clicking and key pressing

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**.

Editing Client (T-WIN11)

☒ Record user activity on clicking and key pressing

Recording Period Settings

☒ Record user activity only on alert or USB monitoring rule triggering

Minutes before triggering Minutes after triggering

Screen Capture Settings

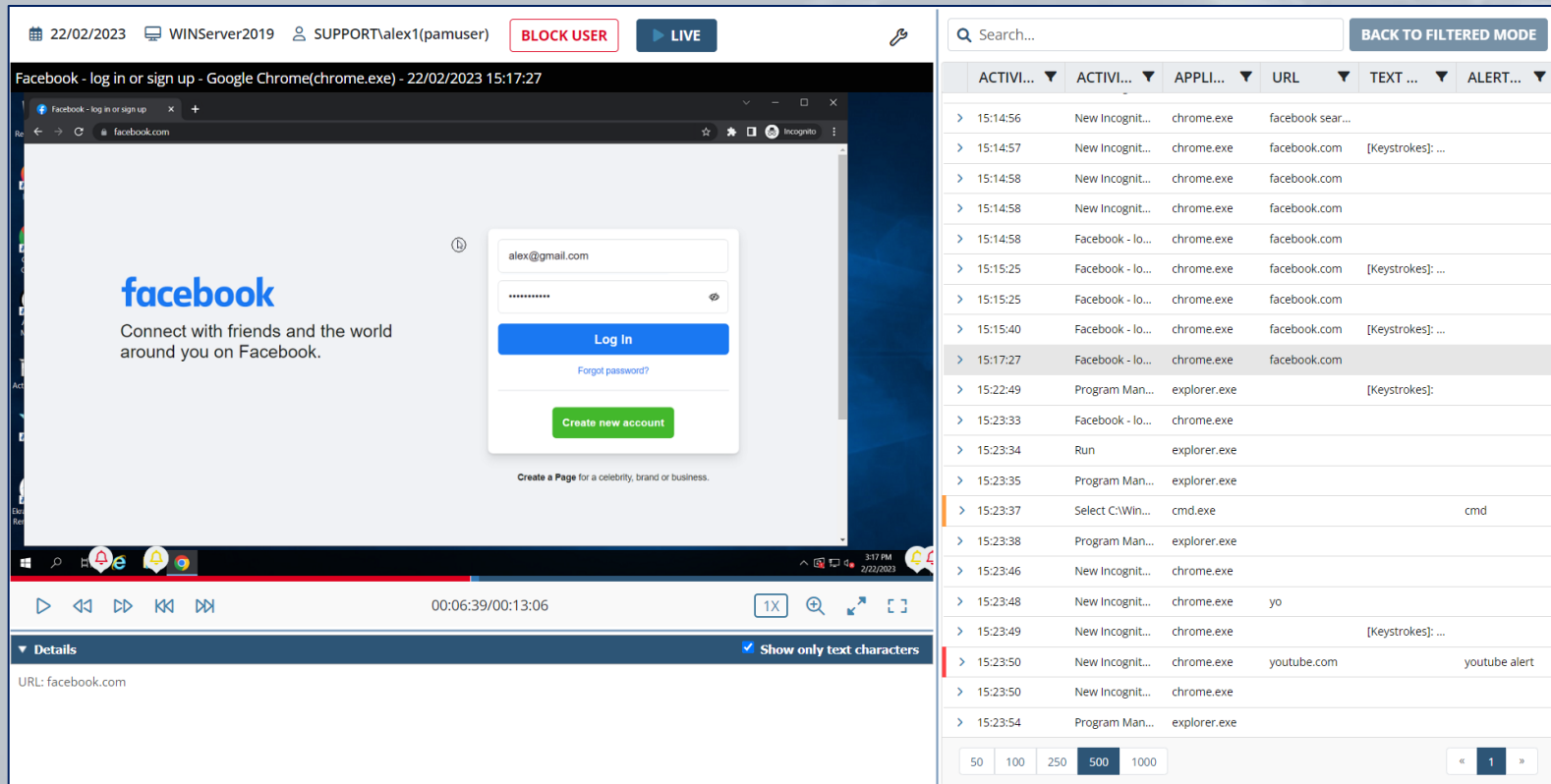
☒ Enable screen capture recording along with user activity recording

☒ Capture active window only

Bit depth

[Next](#) [Finish](#)

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.

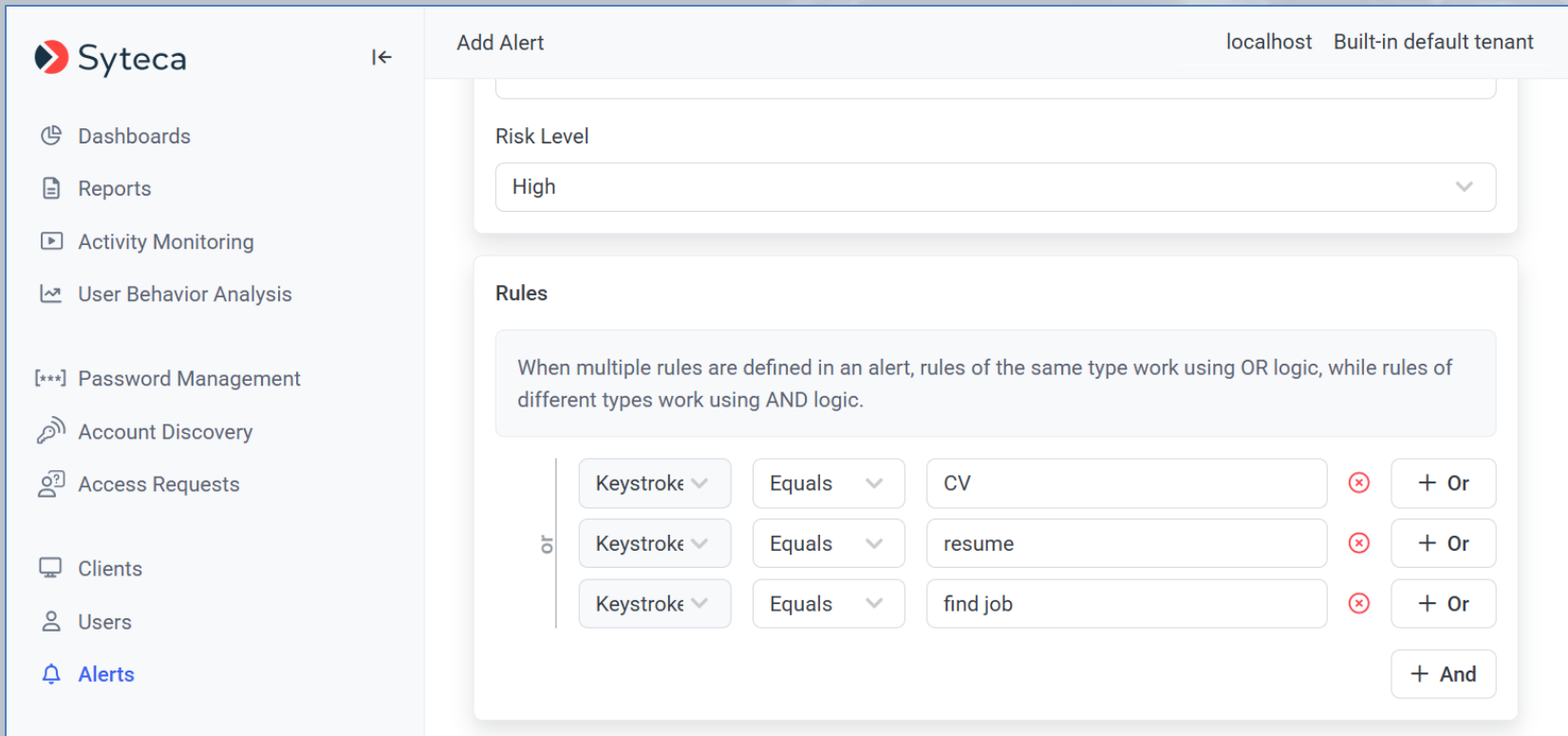


The screenshot displays the Syteca Client interface. The top bar shows the date 22/02/2023, the system name WINServer2019, the user SUPPORT\alex1(pamuser), and buttons for BLOCK USER and LIVE. The main window shows a Google Chrome browser window with the Facebook login page. The URL bar shows facebook.com. The bottom bar shows the URL: facebook.com. On the right side, there is a table of monitored URLs.

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

At the bottom of the table, there are filters for 50, 100, 250, 500, and 1000. The 500 filter is selected. There is also a button for BACK TO FILTERED MODE.

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.



Syteca | Add Alert | localhost | Built-in default tenant

←

Risk Level

High

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.

or

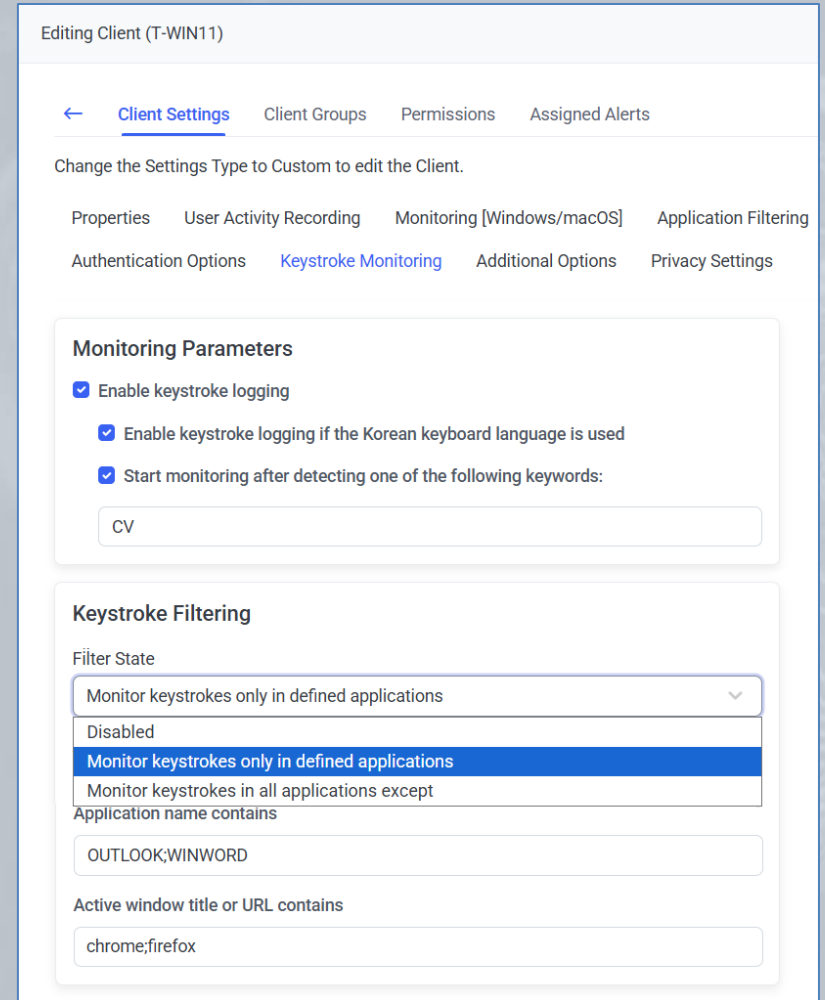
Keystroke	Equals	CV	✗	+ Or
Keystroke	Equals	resume	✗	+ Or
Keystroke	Equals	find job	✗	+ Or

+ And

Keyword-Triggered Monitoring

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. The 'Client Settings' tab is active, with sub-tabs for Properties, User Activity Recording, Monitoring [Windows/macOS], Application Filtering, Authentication Options, Keystroke Monitoring, Additional Options, and Privacy Settings. The 'Keystroke Monitoring' sub-tab is selected. The 'Monitoring Parameters' section includes three checked options: 'Enable keystroke logging', 'Enable keystroke logging if the Korean keyboard language is used', and 'Start monitoring after detecting one of the following keywords:'. A text input field below contains the keyword 'CV'. The 'Keystroke Filtering' section has a 'Filter State' dropdown menu with four options: 'Monitor keystrokes only in defined applications' (selected), 'Disabled', 'Monitor keystrokes only in defined applications' (highlighted in blue), and 'Monitor keystrokes in all applications except'. Below this is a text input field for 'Application name contains' with the value 'OUTLOOK;WINWORD'. At the bottom, there is a text input field for 'Active window title or URL contains' with the value 'chrome;firefox'.

Clipboard Monitoring



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

The screenshot displays the Syteca Insider Threat Protection Software interface. The main window shows a browser with the Syteca website. A red box highlights the 'Manage Insider Risks' button on the website. Below the browser window, a 'Details' panel shows alert information for a clipboard cut/copy test. To the right, a table lists recent clipboard activity.

Details Panel:

- 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/

Clipboard Activity Table:

ACTI...	ACTIVITY TITLE	APPLICATION...	URL	TEXT DATA	ALERT/USB ...
19:29:54	Idle	Idle			
19:30:00	Two-Factor Auth...	Safari	www.syt...		
19:30:05	Syteca - Insider T...	Safari	www.syt...		
19:30:09	Syteca - Insider T...	Safari	www.syt...		
19:30:10	Syteca - Insider T...	Safari	www.syt...	[Clipboard (Copy): Manage Insi...	clipboard cut/copy test
19:30:16	Syteca - Insider T...	Safari	www.syt...		
19:30:18	Syteca - Insider T...	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	Syteca - Insider T...	Safari	www.syt...		
19:31:28	Syteca - Insider T...	Safari	www.syt...		
19:31:41	Syteca - Insider T...	Safari	www.syt...		
19:31:47	Syteca - Insider T...	Safari	www.syt...		
19:31:58	Syteca - Insider T...	Safari	www.syt...		
19:32:00	Syteca - Insider T...	Safari	www.syt...	[Clipboard (Copy): Monitor Insi...	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 Insi...	clipboard cut/copy test
19:34:15	Activity Monitor	Activity Monitor			
19:34:22	Activity Monitor	Activity Monitor			
19:34:22	EmiliaClarke - ssh - 8...	Terminal			
19:34:33	Syteca - Insider T...	Safari	www.syt...		
19:34:36	Syteca - Insider T...	Safari	www.syt...		
19:34:38	Syteca - Insider T...	Safari	www.syt...	[Clipboard (Copy): Monitor Insi...	
19:34:52	Syteca - Insider T...	Safari	www.syt...		
19:34:55	Activity Monitor	Activity Monitor			
19:34:58	Activity Monitor	Activity Monitor			
19:35:01	Calendar	Calendar			

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

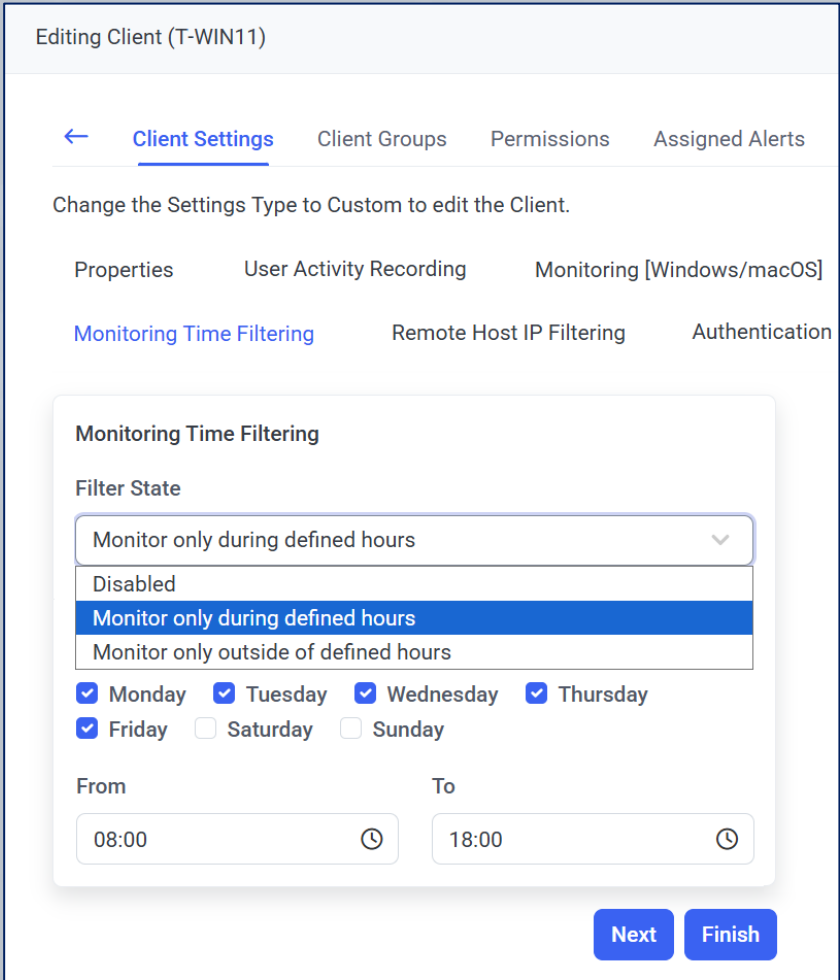
facebook;gmail

[Next](#) [Finish](#)

Monitoring Time Filtering

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

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



The screenshot shows the 'Editing Client (T-WIN11)' interface. At the top, there are tabs for 'Client Settings', 'Client Groups', 'Permissions', and 'Assigned Alerts'. Below these, a message states: 'Change the Settings Type to Custom to edit the Client.' Underneath, there are three main sections: 'Properties', 'User Activity Recording', and 'Monitoring [Windows/macOS]'. The 'Monitoring [Windows/macOS]' section is expanded, showing three sub-sections: 'Monitoring Time Filtering' (which is selected), 'Remote Host IP Filtering', and 'Authentication'. The 'Monitoring Time Filtering' section contains a 'Filter State' dropdown menu with four options: 'Monitor only during defined hours' (selected), 'Disabled', 'Monitor only during defined hours' (highlighted in blue), and 'Monitor only outside of defined hours'. Below the dropdown, there are checkboxes for the days of the week: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. The 'From' and 'To' time fields are set to 08:00 and 18:00 respectively. At the bottom right, there are 'Next' and 'Finish' buttons.

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

Remote Host IP Filtering

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

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)

NOTE: The above option is not currently supported in Full-Motion Capture mode.

Batch registration timeout (ms)

NOTE: The above option is not currently supported in Full-Motion Capture mode.

Chunk size (minutes)

Prevent loading hooks into the following applications

Reduce screen capture size by (%)

Screenshot compression level (1-19)

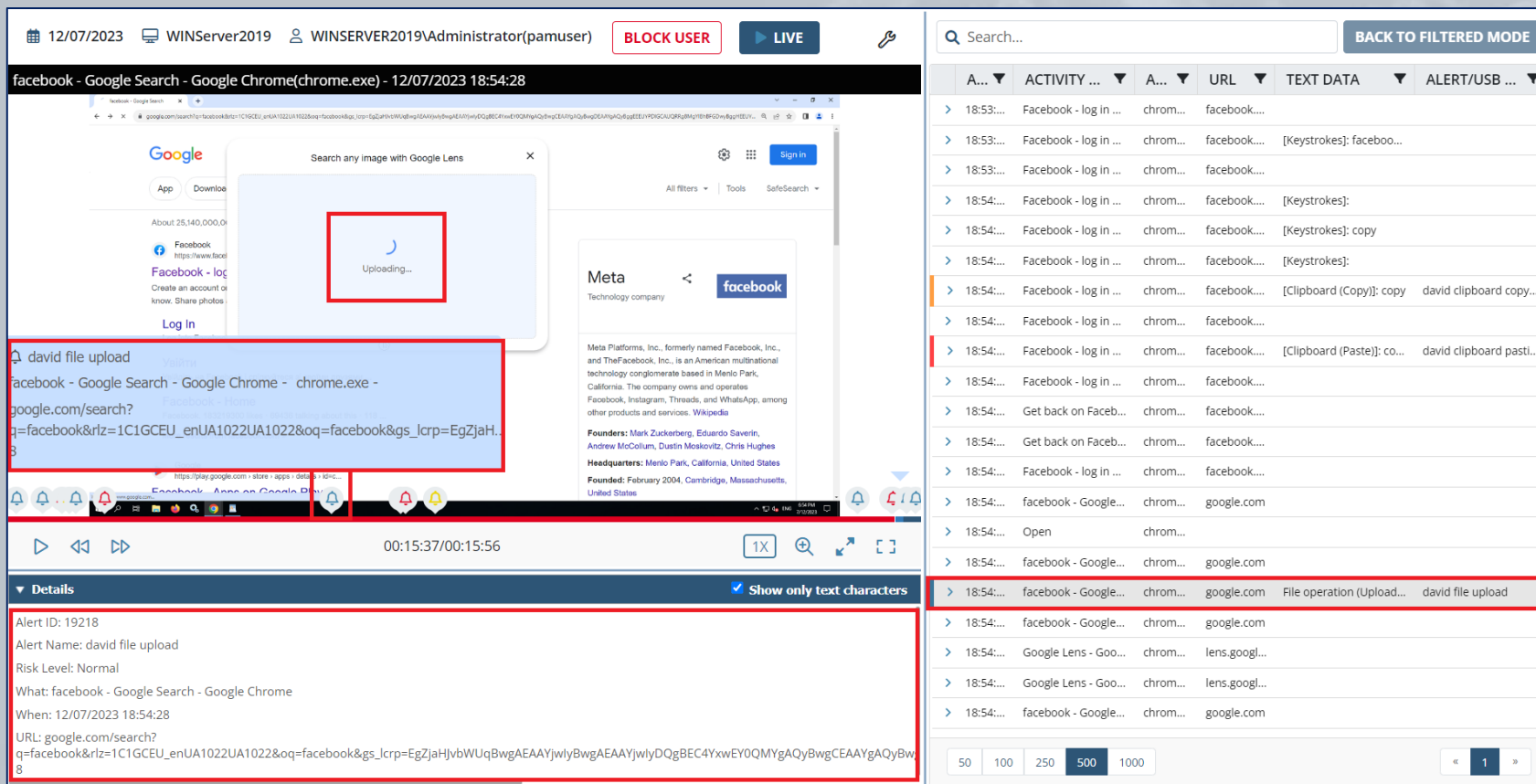
NOTE: The above option is not currently supported in Full-Motion Capture mode.

Agent memory limit (0-disabled)

☐ Support secure browsers by disabling some monitoring features ⓘ

Next Finish

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



The screenshot displays the Syteca File Monitoring interface. The top bar shows the date and time (12/07/2023 18:54:28), the user (WINServer2019\Administrator(pamuser)), and buttons for 'BLOCK USER' and 'LIVE'. The main window shows a Google search for 'facebook' in Google Chrome. A red box highlights the 'Uploading...' status in the Google search results. Below the browser window, a 'Details' panel shows the alert information:

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

On the right, a table lists the activity:

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

You can define the settings for a Client group, and then **apply them to Clients** 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

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.

3/17/2023 ibse-MS-7A70 user1

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

Search...

SEARCH

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

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

A local Linux Client session for X Window System includes:

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

📅 24/02/2023
💻 UbuntuVM
👤 user
🔧

The screenshot shows a terminal window titled "user@ubuntuvm: ~". The prompt is "user@ubuntuvm:~\$". The user has entered "su" and is prompted for a password. The background is a dark red Ubuntu desktop environment.

Search Activity...

ACTIVITY TITLE ▼	ACTIVITY TITLE ▼	APPLICATION NAME ▼	ACTION	PARAMETERS
>	19:56:53	Desktop	Desktop	Active window change
>	19:56:59	Terminal	gnome-terminal-server	Active window change
>	19:56:59		lesspipe	execve
>	19:56:59		basename	execve /usr/bin/lesspipe
>	19:56:59		dirname	execve /usr/bin/lesspipe
>	19:56:59		dircolors	execve -b
>	19:57:00	user@UbuntuVM: ~	gnome-terminal-server	Active window title change
>	19:57:03		su	execve root
>	19:57:06		EkransGörüntü Kaydedici	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

50 100 250 500 1000
« 1 »

▶ ◀ ▶▶
00:00:02/00:00:21
1X 🔍 ↗ 🖨️

▾ Details ☒ Show only text characters

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.

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

Back to Synced Mode

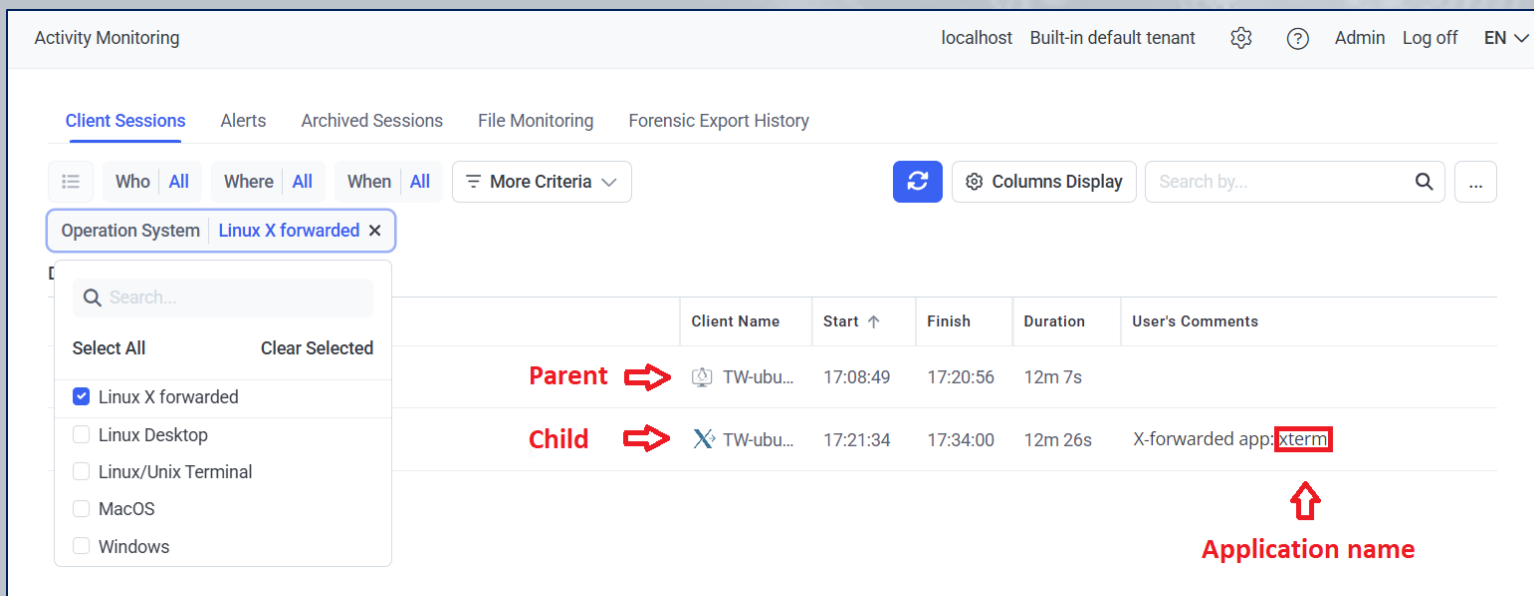
☒ Search in output

☒ Show function calls

☐ Show only execution commands

☐ Show inputs

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



The screenshot displays the 'Activity Monitoring' dashboard. At the top, it shows 'localhost Built-in default tenant' and user controls for 'Admin', 'Log off', and 'EN'. The main navigation bar includes 'Client Sessions' (active), 'Alerts', 'Archived Sessions', 'File Monitoring', and 'Forensic Export History'. Below this, there are filters for 'Who', 'Where', and 'When', all set to 'All'. A 'More Criteria' dropdown is also present. A 'Columns Display' button and a search bar are on the right. The 'Operation System' filter is set to 'Linux X forwarded'. A dropdown menu is open, showing options: 'Linux X forwarded' (checked), 'Linux Desktop', 'Linux/Unix Terminal', 'MacOS', and 'Windows'. The main table lists sessions with columns: 'Client Name', 'Start', 'Finish', 'Duration', and 'User's Comments'. Two sessions are shown: a 'Parent' session (TW-ubu...) and a 'Child' session (TW-ubu...). The 'Child' session's 'User's Comments' field contains 'X-forwarded app: xterm', where 'xterm' is highlighted with a red box. A red arrow points from the text 'Application name' below to this box.

	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

Detection of Disconnected Clients

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

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

Editing Client (T-WIN11)

Client Mode

- ☐ Enable Protected mode
NOTE: The mode will change after restart of the Client computer.
- ☒ Update Client automatically
- ☐ Display Client tray icon
- ☐ Display icon when recording is in progress
- ☐ Enable the Syteca PAM Connection Manager
- ☐ Replace Windows Shell with the Syteca PAM Connection Manager

☒ Notify if the Client is offline for more than

days

minutes

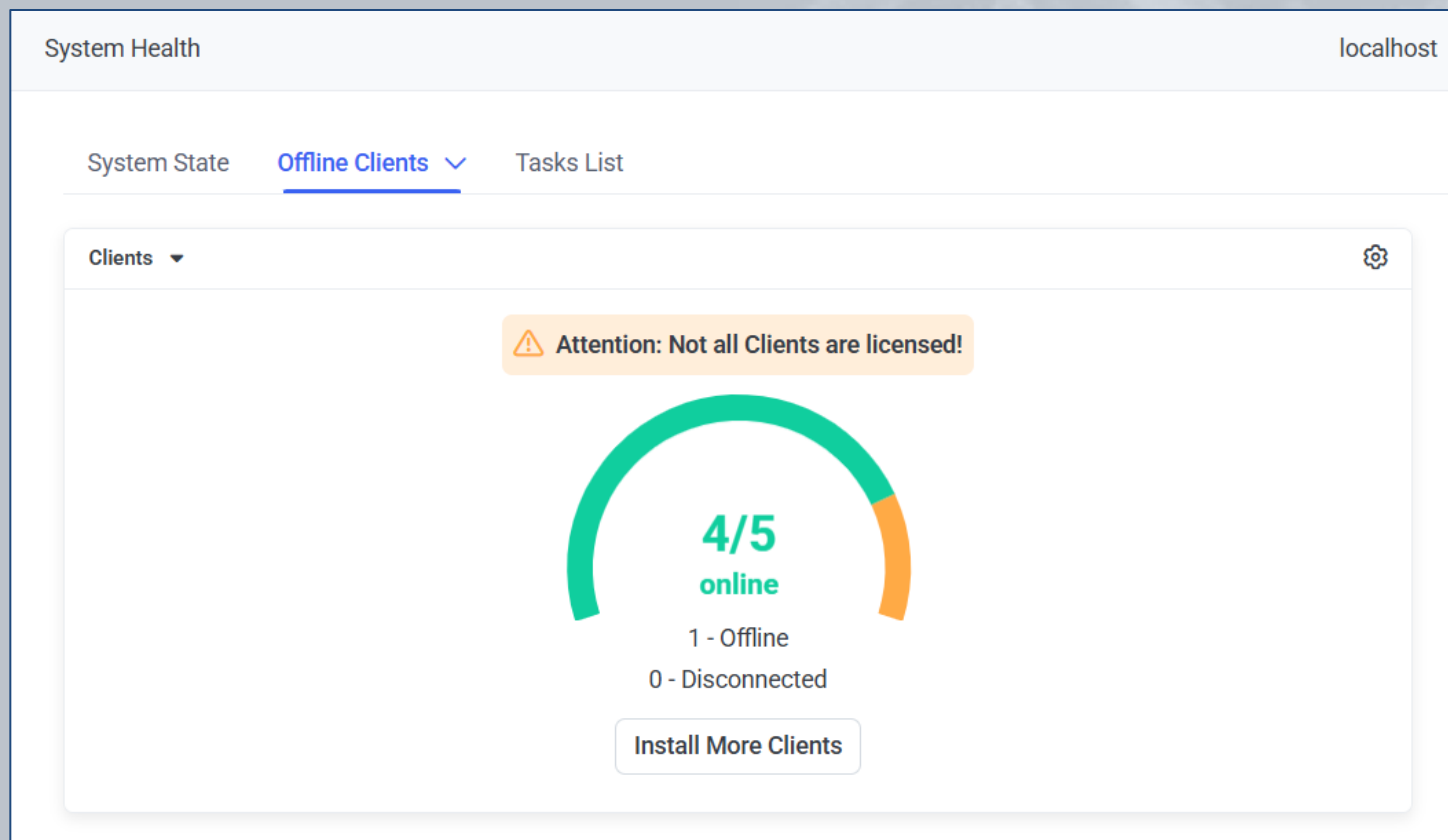
hours

days

Send email notification to

Viewing Disconnected Clients

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



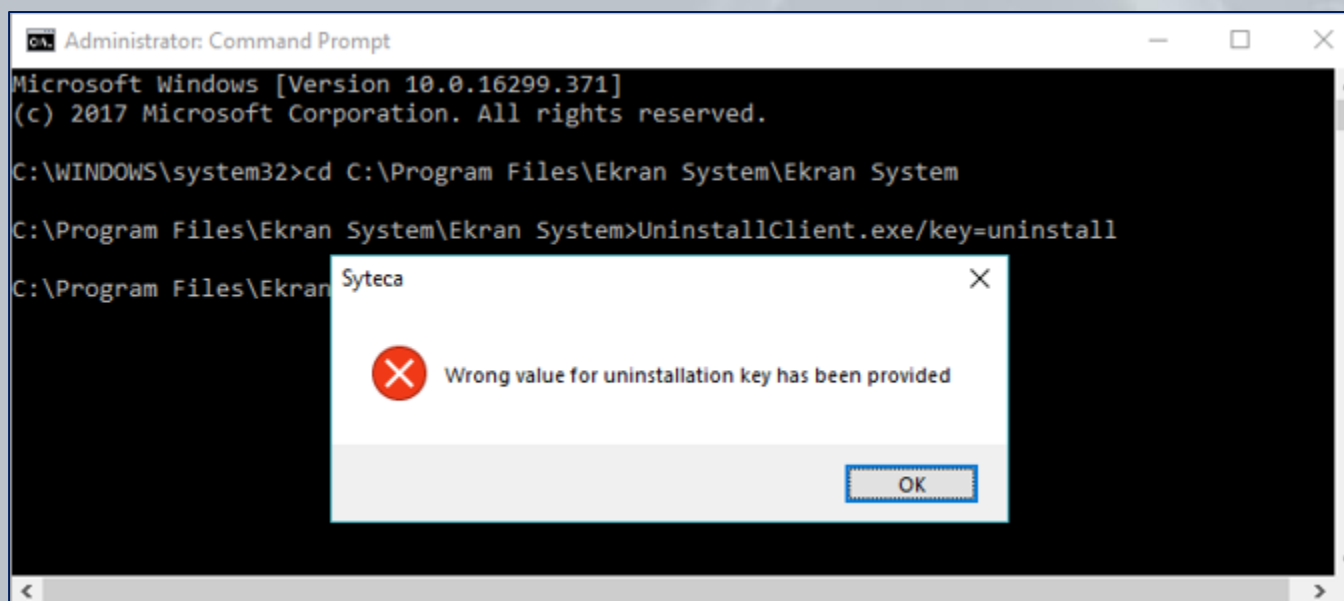
Client Protection

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.

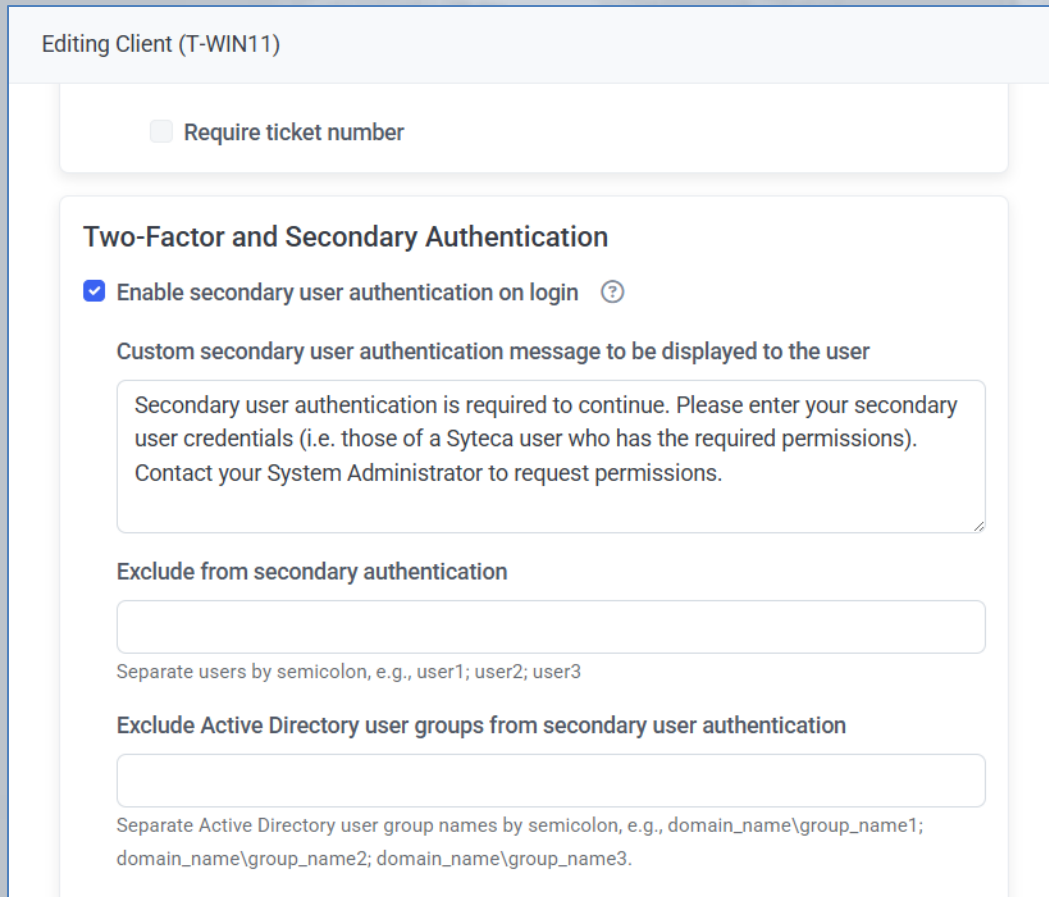


Only the **Syteca administrator** knows the **Uninstallation key** defined prior to Client installation, and which is required for local removal.

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**.



Editing Client (T-WIN11)

☐ Require ticket number

Two-Factor and Secondary Authentication

☒ Enable secondary user authentication on login [?](#)

Custom secondary user authentication message to be displayed to the user

Secondary user authentication is required to continue. Please enter your secondary user credentials (i.e. those of a Syteca user who has the required permissions). Contact your System Administrator to request permissions.

Exclude from secondary authentication

Separate users by semicolon, e.g., user1; user2; user3

Exclude Active Directory user groups from secondary user authentication

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

Secondary User Authentication (Windows)



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

A screenshot of a Windows-style dialog box for Syteca secondary authentication. The dialog has a title bar with the Syteca logo and name. The main text reads: "The secondary authentication is required to continue. Please enter the login/password allowed in Syteca. Contact your System Administrator for more details." Below this, there are two input fields. The first is labeled "Login:" and contains the text "John". The second is labeled "Password:" and contains ten black dots, indicating a masked password. At the bottom right, there are two buttons: "OK" and "Cancel".

 Syteca

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

Login:

Password:

One-Time Passwords (Windows Clients)



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

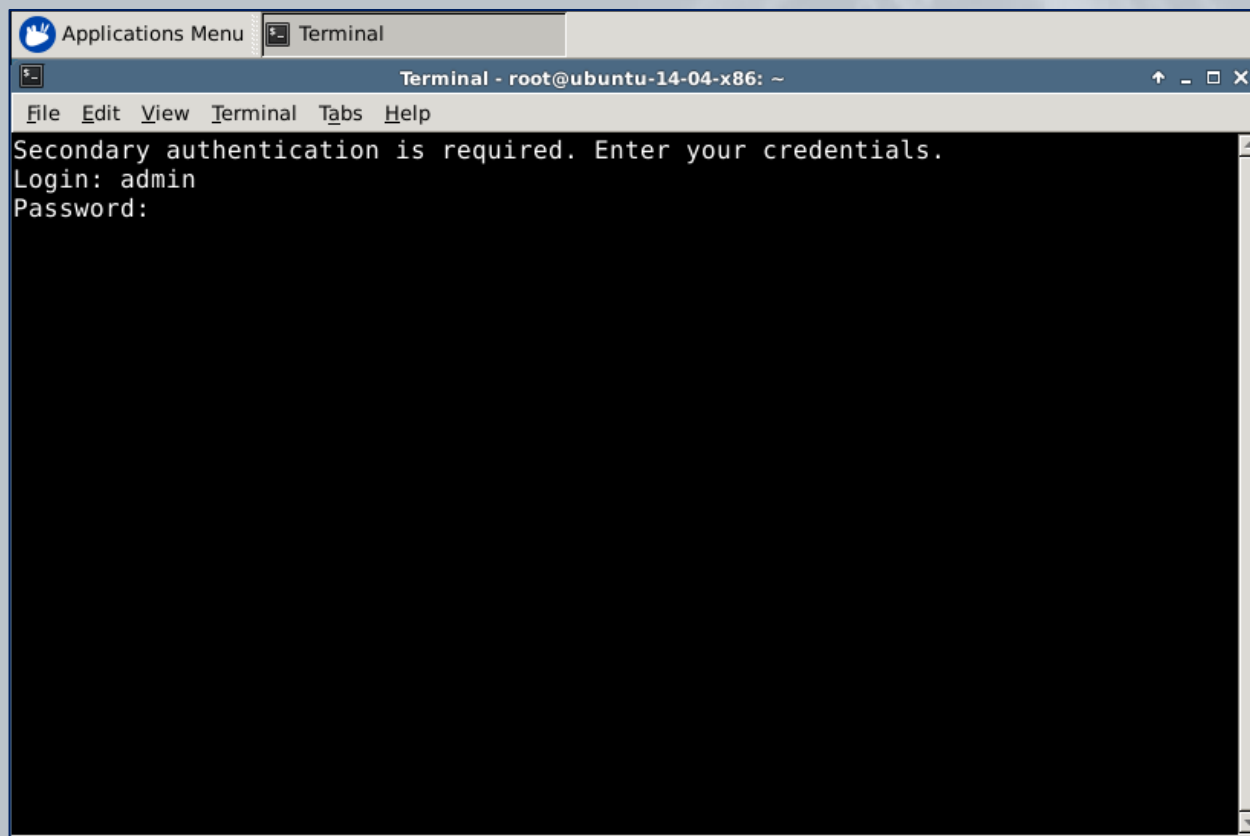
The **user** can **request** a **one-time password** directly **from** the secondary user authentication **window** displayed **during login** to the Windows OS.

A screenshot of a Windows-style dialog box titled "Syteca". The dialog has a white background with a blue border. At the top, the Syteca logo is on the left and the title "Syteca" is on the right. Below the title bar, the text "REQUEST ONE-TIME PASSWORD" is displayed in blue. A dropdown menu shows "I need emergency access to computer". Below this, a message says "Please enter your email address for the one-time password to be sent to it." There are three input fields: "EMAIL" with the text "johnson.kenneth@email.net", "COMMENT" with the text "Kenneth Johnson to update the db", and a third empty field. At the bottom, there are "Cancel" and "Request" buttons. The dialog is overlaid on a blurred background of a Windows login screen.

Secondary User Authentication (Linux Clients)

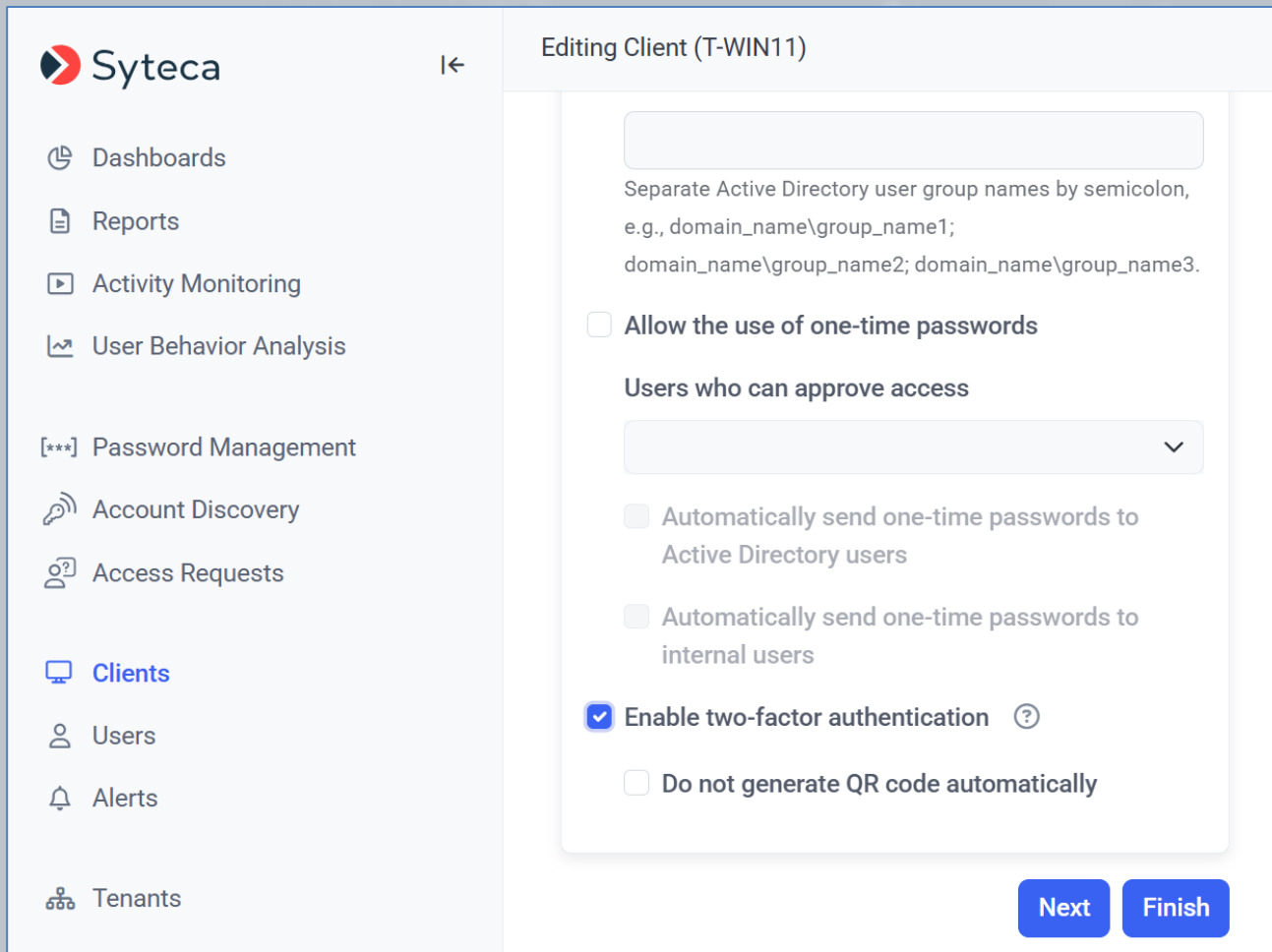


The Syteca Client requests **credentials** to be entered to allow a user to **log on to the terminal** on **Linux** Client computers.



Two-Factor Authentication

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



Syteca |← Editing Client (T-WIN11)

 Dashboards

 Reports

 Activity Monitoring

 User Behavior Analysis

 Password Management

 Account Discovery

 Access Requests

 **Clients**

 Users

 Alerts

 Tenants

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

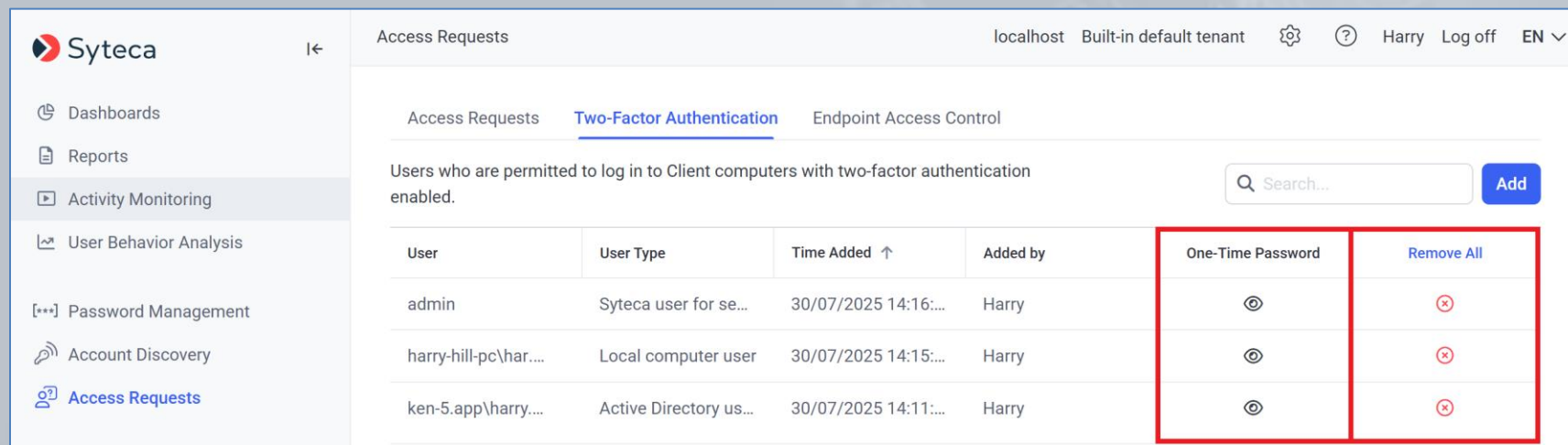
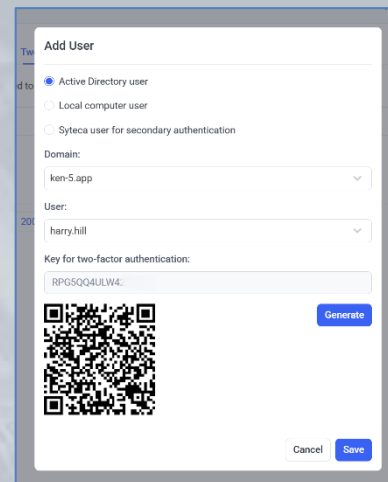
☒ Enable two-factor authentication ?

☐ Do not generate QR code automatically

Next **Finish**

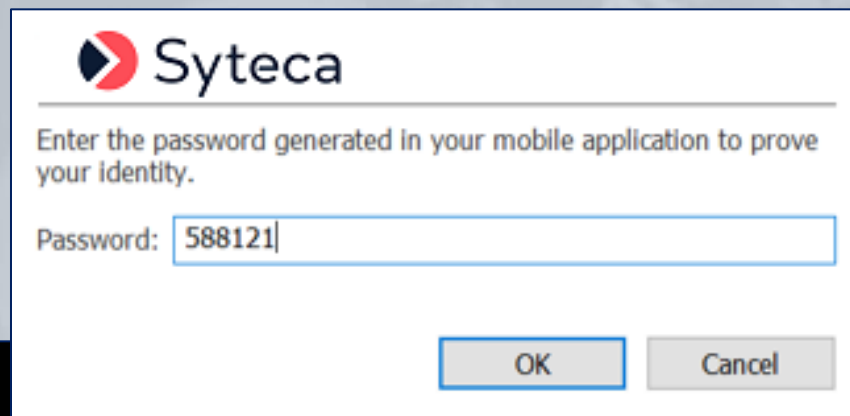
Two-Factor Authentication (Windows/Linux)

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.



A screenshot of a Syteca authentication dialog box. The dialog has a title bar with the Syteca logo and name. Below the title bar, it says "Enter the password generated in your mobile application to prove your identity." There is a text input field labeled "Password:" containing the value "588121". At the bottom right, there are two buttons: "OK" and "Cancel".

```
Ubuntu 16.04.2 LTS ubuntu tty2
```

```
ubuntu login: May
```

```
Password:
```

```
Last login: Fri May 3 01:45:16 PDT 2019 on tty2
```

```
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic x86_64)
```

```
* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage
```

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

```
Enter pin: _
```

Two-Factor Authentication (for MT users)



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

Syteca

Adding New User

User Type **User Details** User Groups Administrative Permissions

Internal User Properties

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

Login

user1

Password

.....

Confirm password

.....

☒ Enable two-factor authentication on login

Set up Two-Factor authentication

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

Recovery Code

YV03W - X7TTC

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

Confirm

[Back](#)

Copyright © 2011 - 2025 Syteca

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**.

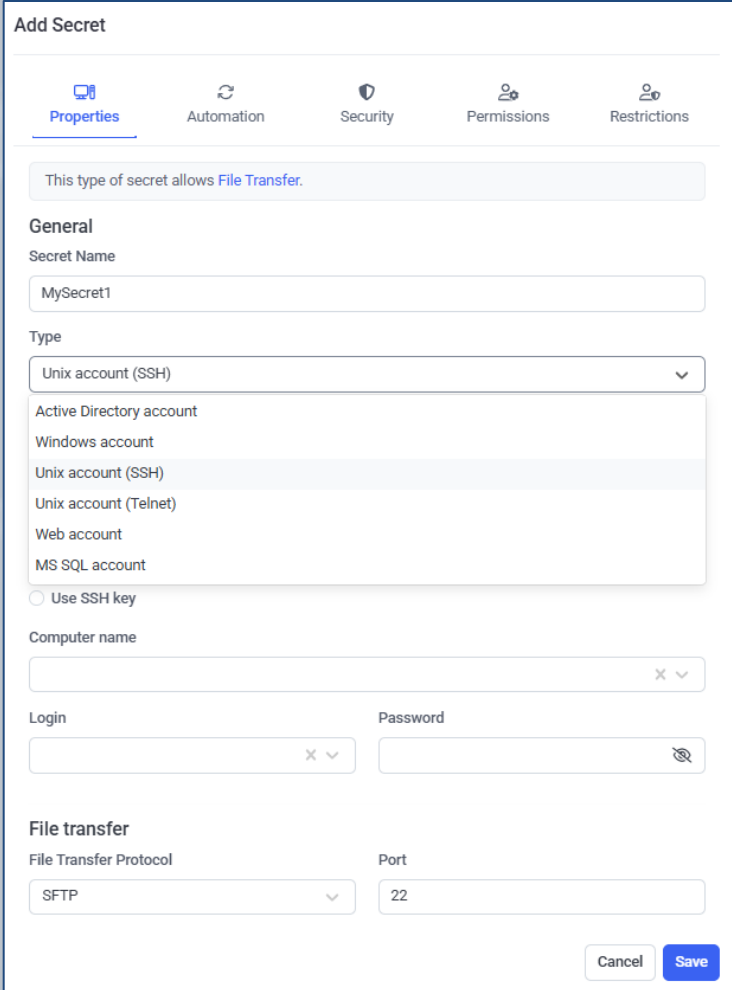
With Syteca, you can:

- 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).

Adding a Secret

Add a secret manually by specifying:

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



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 Port

SFTP 22

Cancel Save

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

30

days

Cancel

Save

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

1

hours

0

minutes

Force Check In

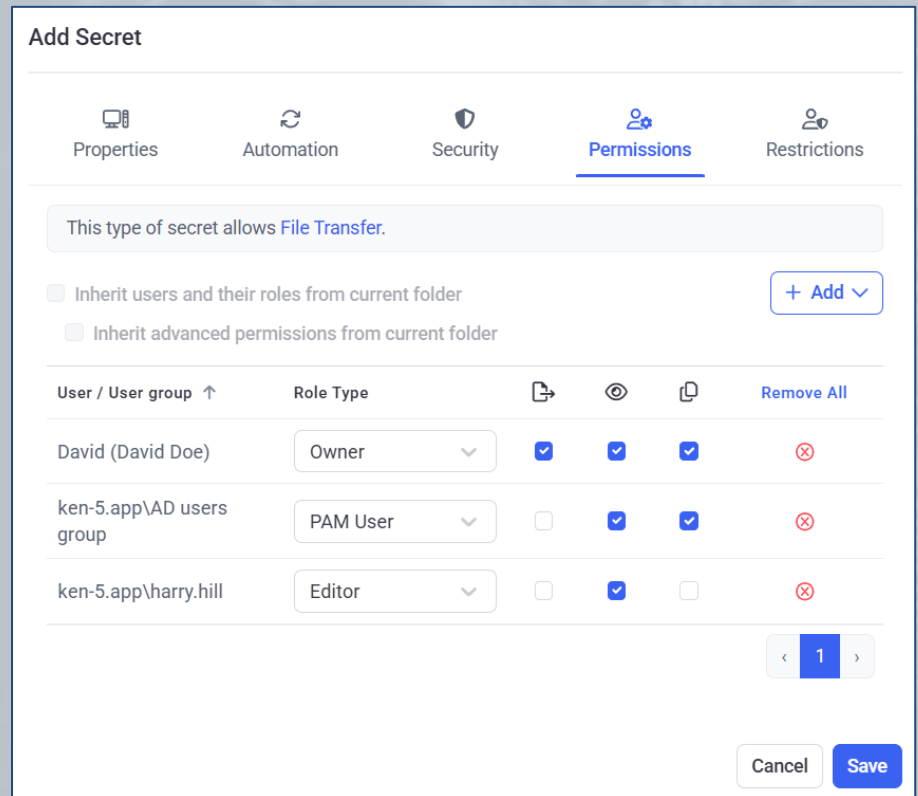
Cancel

Save

Adding a Secret (Users & Permissions)

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



The screenshot shows the 'Add Secret' dialog box with the 'Permissions' tab selected. The dialog has tabs for Properties, Automation, Security, Permissions, and Restrictions. A message states: 'This type of secret allows File Transfer.' Below this are two unchecked checkboxes: 'Inherit users and their roles from current folder' and 'Inherit advanced permissions from current folder'. A '+ Add v' button is to the right. A table lists users and their permissions:

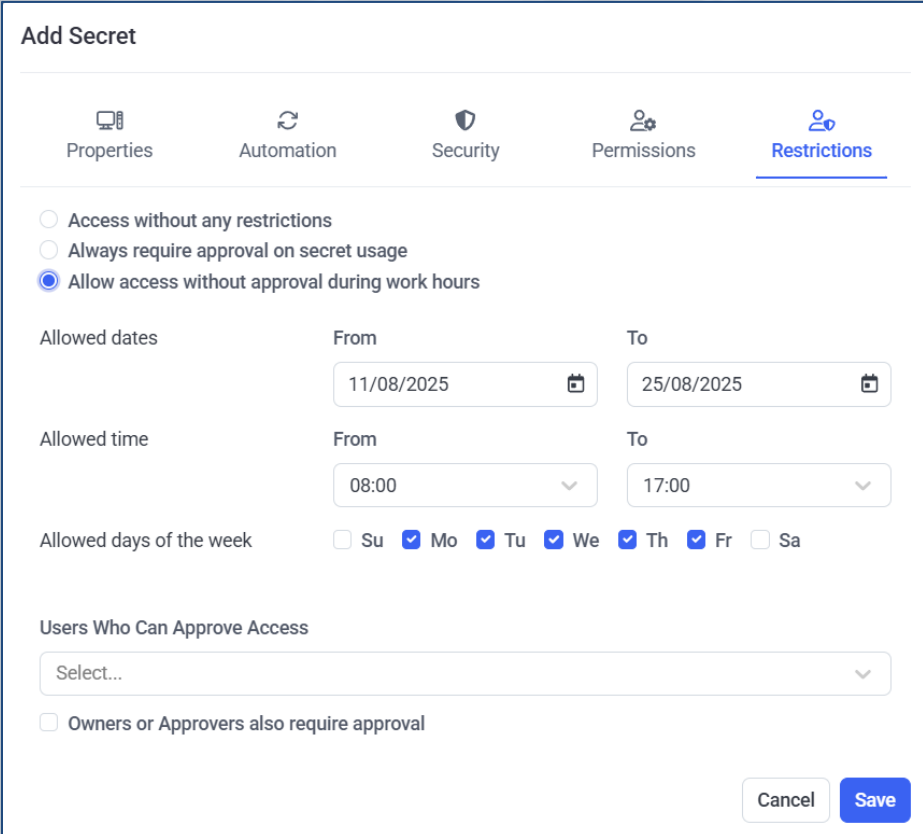
User / User group ↑	Role Type	File Transfer	View Password	Copy Password	Remove
David (David Doe)	Owner	☒	☒	☒	☒
ken-5.app\AD users group	PAM User	☐	☒	☒	☒
ken-5.app\harry.hill	Editor	☐	☒	☐	☒

At the bottom right, there is a 'Cancel' button and a 'Save' button. A pagination control shows '< 1 >'.

Adding a Secret (Access Restrictions)

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.



The screenshot shows the 'Add Secret' dialog box with the 'Restrictions' tab selected. The dialog has five tabs: Properties, Automation, Security, Permissions, and Restrictions. Under the 'Restrictions' tab, there are three radio button options: 'Access without any restrictions', 'Always require approval on secret usage', and 'Allow access without approval during work hours'. The third option is selected. Below these options, there are fields for 'Allowed dates' (From: 11/08/2025, To: 25/08/2025), 'Allowed time' (From: 08:00, To: 17:00), and 'Allowed days of the week' (Su: unchecked, Mo: checked, Tu: checked, We: checked, Th: checked, Fr: checked, Sa: unchecked). There is also a dropdown menu for 'Users Who Can Approve Access' with the text 'Select...'. At the bottom, there is a checkbox for 'Owners or Approvers also require approval' which is unchecked. The dialog has 'Cancel' and 'Save' buttons at the bottom right.

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 To
11/08/2025 25/08/2025

Allowed time From To
08:00 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

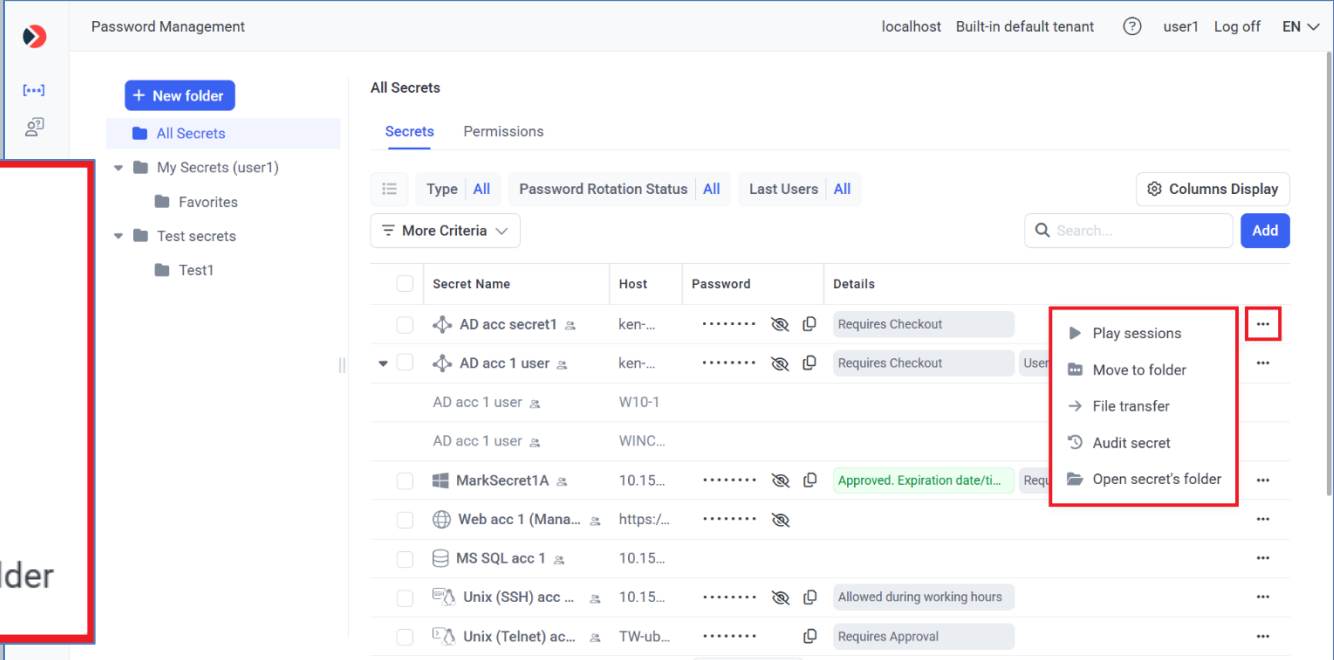
A **privileged user** can access a critical endpoint via a **secret** by using either the **Web** (incl. **agentless PAM**) or **Desktop** version of **Syteca Connection Manager**. The secrets are stored in a granular **Tree-View folder structure** and have **user permissions** for both folders and secrets.

[illegible]

Viewing Secrets in Sessions

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.

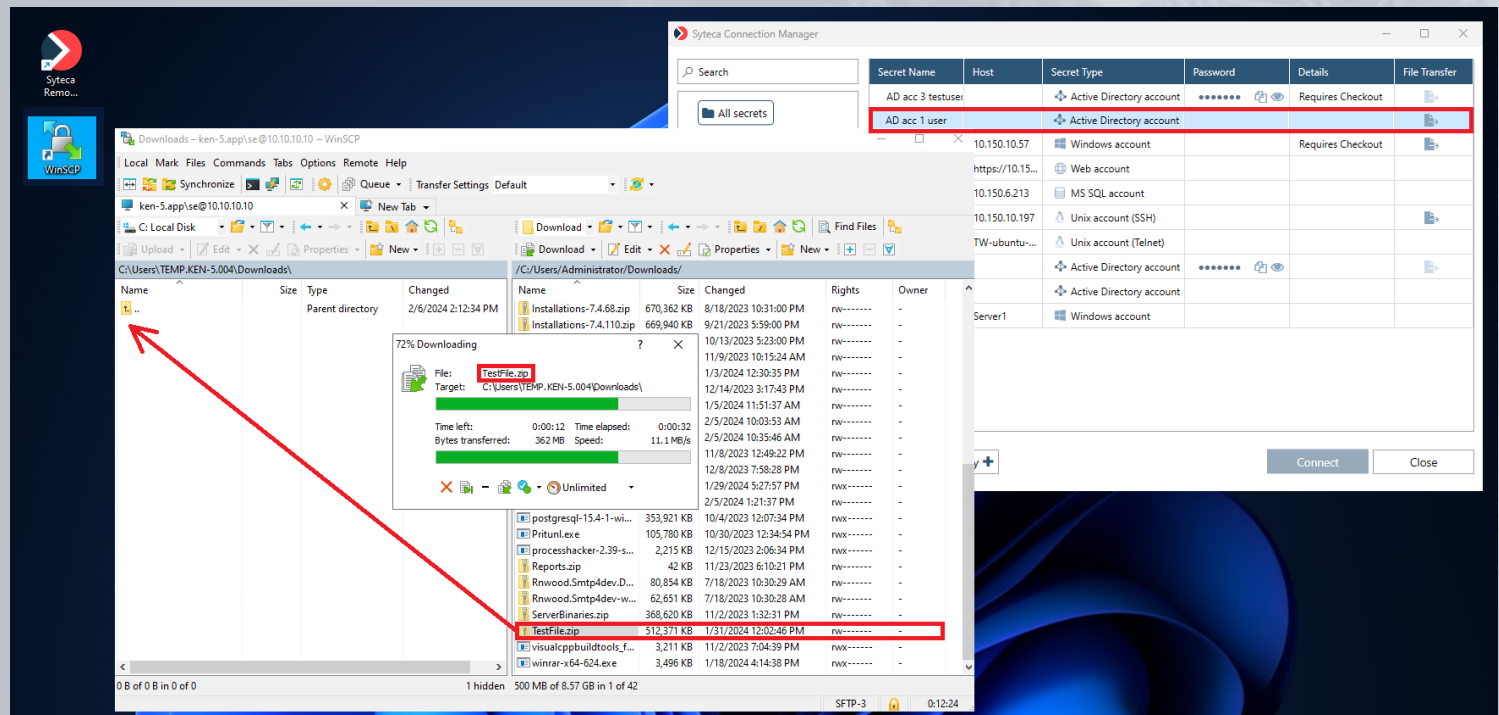


The screenshot displays the Password Management interface. On the left, a sidebar shows a folder structure: 'All Secrets', 'My Secrets (user1)', 'Favorites', 'Test secrets', and 'Test1'. The main area, titled 'All Secrets', shows a table of secrets. A context menu is open over the 'AD acc 1 user' secret, listing actions: 'Play sessions', 'Move to folder', 'File transfer', 'Audit secret', and 'Open secret's folder'. The 'Play sessions' option is highlighted.

Secret Name	Host	Password	Details
AD acc secret1	ken...		Requires Checkout
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 (Mana...	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

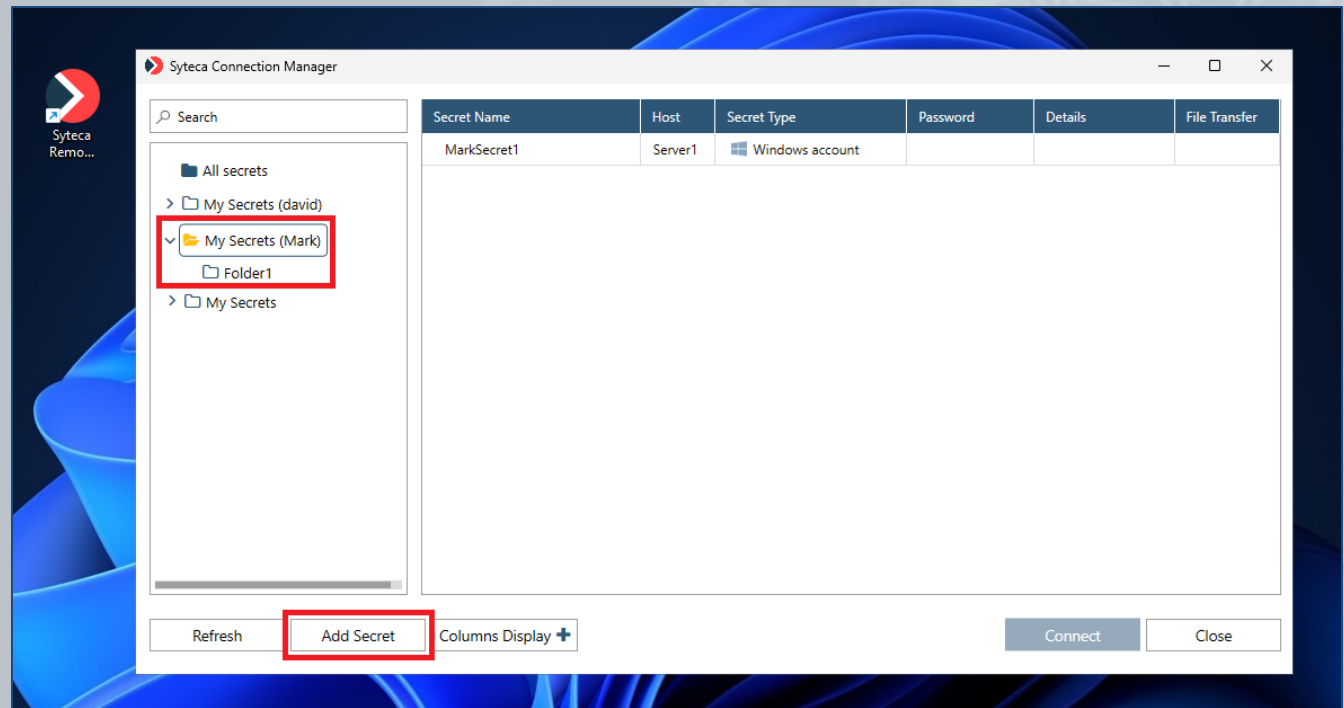
The **File Transfer** functionality allows users of secrets to transfer files **between the computer** with Syteca Connection Manager **and the remote computers** (which are accessed via the secrets) by using the **WinSCP** application.



Workforce Password Management (WPM)

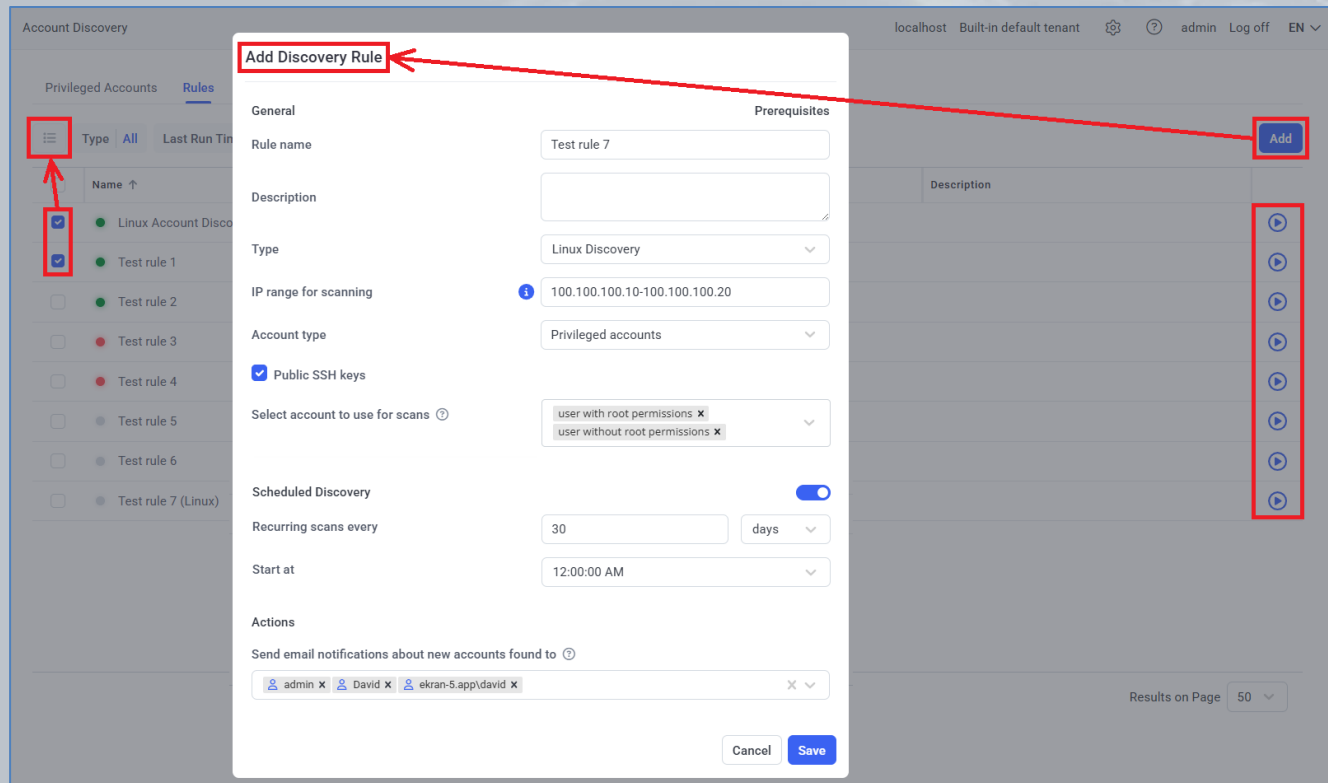


The WPM functionality enables PAM users (i.e. any **users of Syteca Connection Manager**) to **create (and manage) their own private Workforce Password Management (WPM) secrets**, which are **hidden from other users** (unless specifically shared with them).



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 displays the Syteca Account Discovery interface. A modal window titled "Add Discovery Rule" is open, showing various configuration options. The modal is divided into sections: General, Prerequisites, Scheduled Discovery, and Actions. The "General" section includes fields for Rule name, Description, Type, IP range for scanning, Account type, and a checkbox for Public SSH keys. The "Prerequisites" section includes a dropdown for Select account to use for scans. The "Scheduled Discovery" section includes a toggle for Scheduled Discovery, a field for Recurring scans every, and a dropdown for Start at. The "Actions" section includes a checkbox for Send email notifications about new accounts found to and a list of email addresses. The modal is annotated with red boxes and arrows: a box around the "Add Discovery Rule" title, a box around the "Add" button in the top right, a box around the "Add" button in the bottom right, and a box around the "Add" button in the bottom right. A red arrow points from the "Add" button in the top right to the "Add Discovery Rule" title. Another red arrow points from the "Add" button in the bottom right to the "Add" button in the bottom right. A third red arrow points from the "Add" button in the bottom right to the "Add" button in the bottom right.

Account Discovery

Privileged Accounts Rules

Type All Last Run Time

Name ↑

- ☒ Linux Account Discovery
- ☒ Test rule 1
- ☐ Test rule 2
- ☐ Test rule 3
- ☐ Test rule 4
- ☐ Test rule 5
- ☐ Test rule 6
- ☐ Test rule 7 (Linux)

Add Discovery Rule

General

Rule name Test rule 7

Description

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 X

user without root permissions X

Scheduled Discovery

Recurring scans every 30 days

Start at 12:00:00 AM

Actions

Send email notifications about new accounts found to

admin X David X ekran-5.app\david X

Cancel Save

localhost Built-in default tenant admin Log off EN

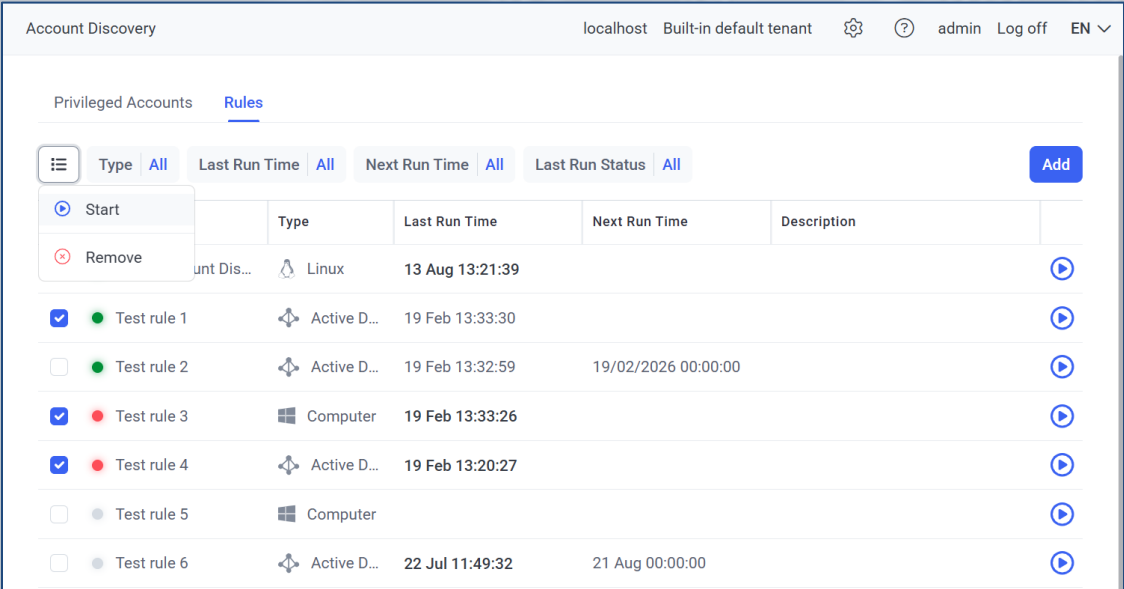
Add

Description

Results on Page 50

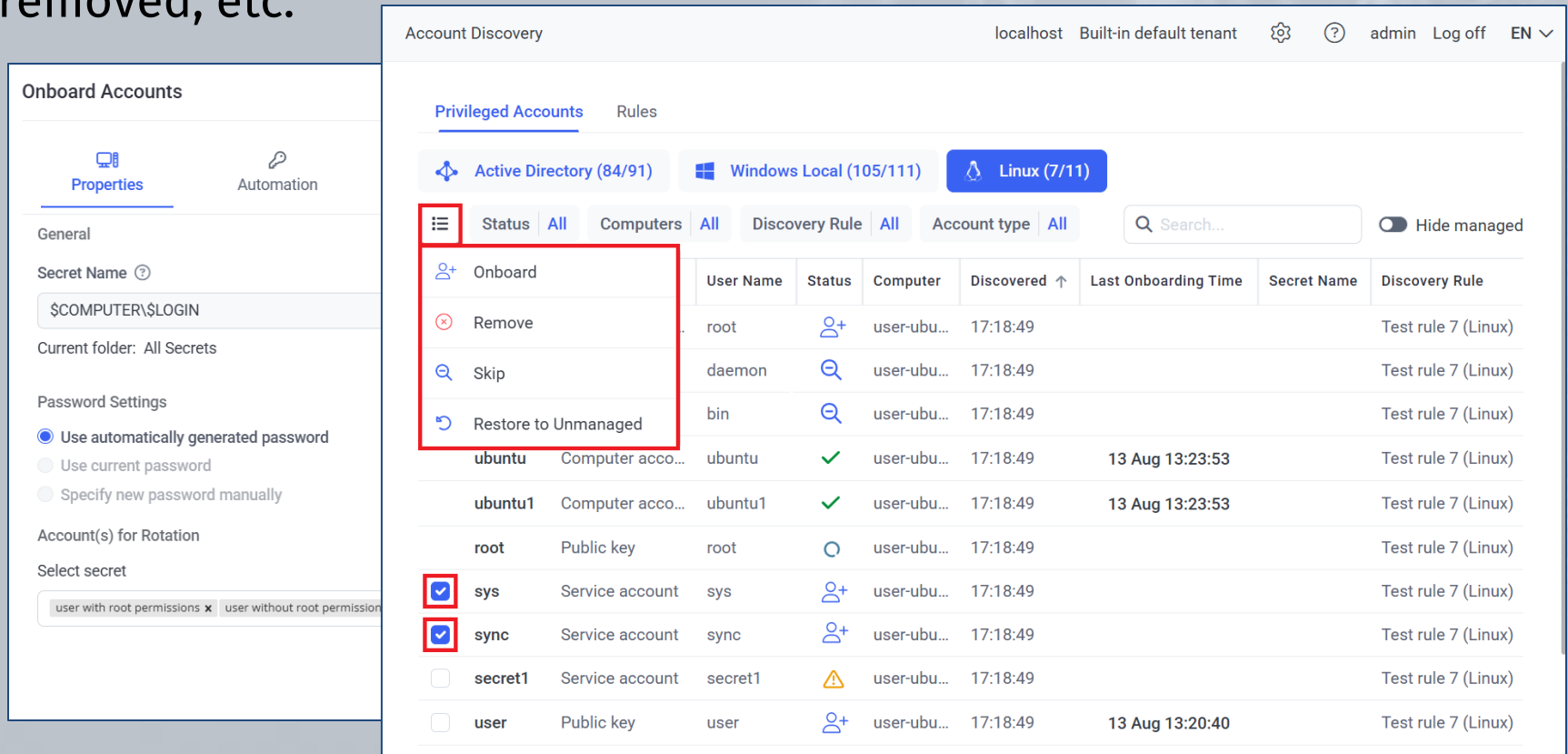
Various **types** of **discovery rules** can be added:

- **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**).



Type	Last Run Time	Next Run Time	Description
Linux	13 Aug 13:21:39		
Active D...	19 Feb 13:33:30		
Active D...	19 Feb 13:32:59	19/02/2026 00:00:00	
Computer	19 Feb 13:33:26		
Active D...	19 Feb 13:20:27		
Computer			
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.



The screenshot displays the Syteca Account Onboarding interface. On the left, the 'Onboard Accounts' sidebar is visible, showing the 'Properties' tab. The 'Secret Name' is set to '\$COMPUTER\$LOGIN'. The 'Current folder' is 'All Secrets'. Under 'Password Settings', the 'Use automatically generated password' option is selected. The 'Account(s) for Rotation' section shows 'Select secret' with a dropdown menu containing 'user with root permissions x' and 'user without root permission'. The main area, titled 'Account Discovery', shows the 'Privileged Accounts' tab. It includes filters for 'Active Directory (84/91)', 'Windows Local (105/111)', and 'Linux (7/11)'. A table of accounts is displayed with columns: User Name, Status, Computer, Discovered, Last Onboarding Time, Secret Name, and Discovery Rule. A red box highlights the 'Onboard', 'Remove', 'Skip', and 'Restore to Unmanaged' actions in the table's header. The table lists several accounts, including 'ubuntu', 'ubuntu1', 'root', 'sys', 'sync', 'secret1', and 'user'. The 'sys' and 'sync' accounts are marked with a checkmark in the 'Status' column, indicating they are onboarded.

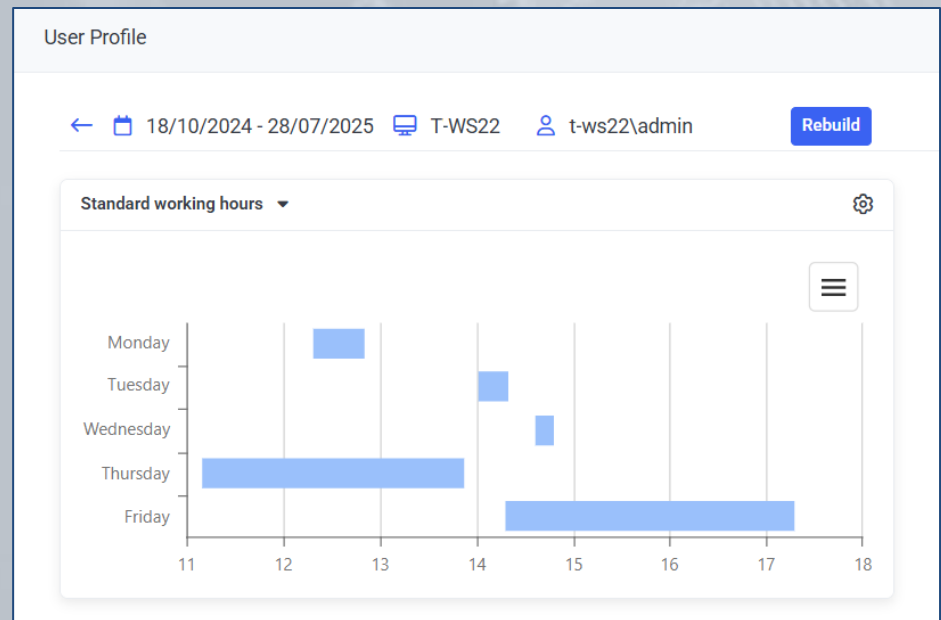
User Name	Status	Computer	Discovered	Last Onboarding Time	Secret Name	Discovery Rule
root	Onboard	user-ubu...	17:18:49			Test rule 7 (Linux)
daemon	Onboard	user-ubu...	17:18:49			Test rule 7 (Linux)
bin	Onboard	user-ubu...	17:18:49			Test rule 7 (Linux)
ubuntu	Computer acco...	ubuntu	17:18:49	13 Aug 13:23:53		Test rule 7 (Linux)
ubuntu1	Computer acco...	ubuntu1	17:18:49	13 Aug 13:23:53		Test rule 7 (Linux)
root	Public key	root	17:18:49			Test rule 7 (Linux)
sys	Service account	sys	17:18:49			Test rule 7 (Linux)
sync	Service account	sync	17:18:49			Test rule 7 (Linux)
secret1	Service account	secret1	17:18:49			Test rule 7 (Linux)
user	Public key	user	17:18:49	13 Aug 13:20:40		Test rule 7 (Linux)

User and Entity Behavior Analytics (UEBA)

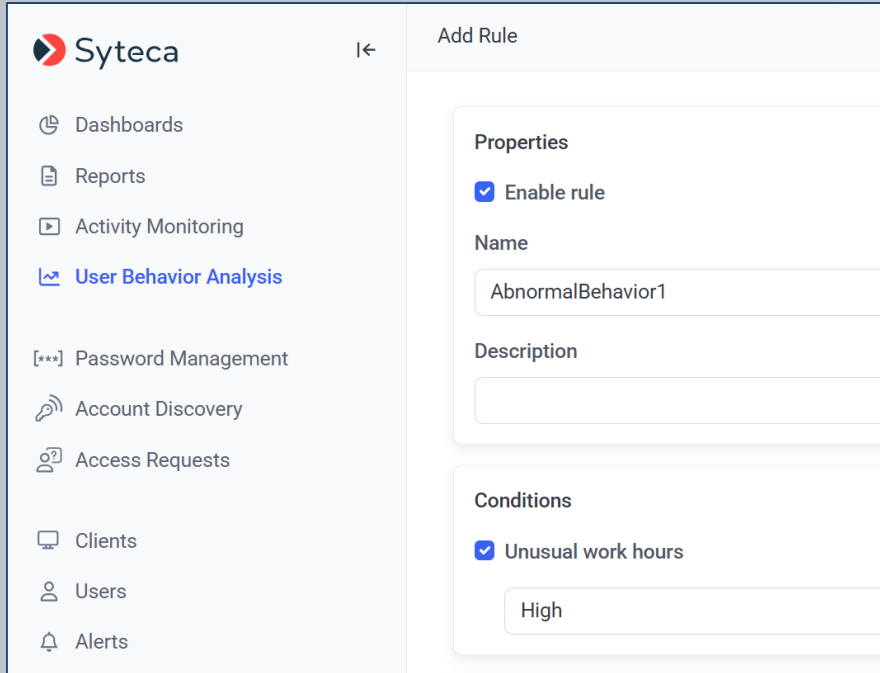
Syteca User & Entity Behavior Analytics (UEBA) allows you to **better protect your system** from malicious and illicit insiders.

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 the Syteca User Behavior Analysis configuration interface. On the left is a sidebar with navigation links: Dashboards, Reports, Activity Monitoring, User Behavior Analysis (highlighted), Password Management, Account Discovery, Access Requests, Clients, Users, and Alerts. The main area is titled 'Add Rule' and contains three sections: Properties, Name, and Description. The Properties section has a checked 'Enable rule' checkbox. The Name section has a text input field containing 'AbnormalBehavior1'. The Description section has an empty text input field. Below these is a 'Conditions' section with a checked 'Unusual work hours' checkbox and a text input field containing 'High'.

Syteca

← Add Rule

Properties

☒ Enable rule

Name

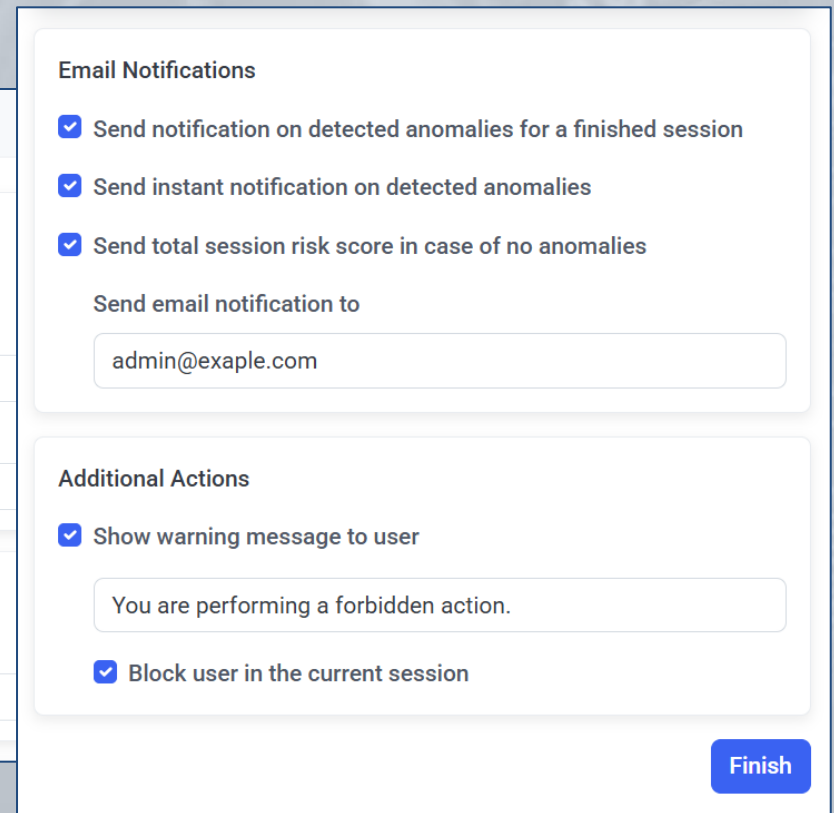
AbnormalBehavior1

Description

Conditions

☒ Unusual work hours

High



The image shows the configuration interface for email notifications and additional actions. The 'Email Notifications' section has three checked checkboxes: 'Send notification on detected anomalies for a finished session', 'Send instant notification on detected anomalies', and 'Send total session risk score in case of no anomalies'. Below these is a text input field for 'Send email notification to' containing 'admin@exaple.com'. The 'Additional Actions' section has a checked checkbox for 'Show warning message to user' and a text input field containing 'You are performing a forbidden action.'. Below this is another checked checkbox for 'Block user in the current session'. A blue 'Finish' button is at the bottom right.

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@exaple.com

Additional Actions

☒ Show warning message to user

You are performing a forbidden action.

☒ Block user in the current session

Finish

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 RequestslocalhostBuilt-in default tenant⚙️🔍adminLog offEN ▼

Access RequestsTwo-Factor AuthenticationEndpoint Access Control

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

Add

🔍 Search...

Apply Filters

User	User Type	Assigned to	Restriction Type	Time Added	Added by	Remove All	
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**

**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

Cancel

Save

- 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

11/08/2025

25/08/2025

Allowed Time

From

To

08:00:00

17:00:00

Allowed Weekdays

☐ Su ☒ Mo ☒ Tu ☒ We ☒ Th ☒ Fr ☐ Sa

Cancel

Save

Administrator Approval on Login



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

The screenshot displays the Syteca web interface. On the left is a sidebar with navigation links: Dashboards, Reports, Activity Monitoring, User Behavior Analysis, Password Management, Account Discovery, Access Requests (highlighted with a red badge '2'), Clients, Users, Alerts, Tenants, System Health, and Audit Log. The main content area is titled 'Access Requests' and includes tabs for 'Access Requests' (selected), 'Two-Factor Authentication', and 'Endpoint Access Control'. Below the tabs is a search bar and a set of filters: Status (All), Request Type (All), User (All), Client (All), Processed By (All), Request Time (All), Processed Time (All), Sort by (Newest), and a toggle for 'Display all requests'. The list of requests contains four entries:

User	Client	Time Ago	Status	Action
ken-5.app\david	T-WIN11	2 minute(s) ago	Approved by admin	44 second(s) ago
user1	TW-ubun-2404LTS	6 minute(s) ago	Denied by admin	1 minute(s) ago
James	T-WIN11	8 minute(s) ago	Pending	Can you give me access pls
administrator(admin)	T-WS22	14 minute(s) ago	Pending	Please approve access

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.

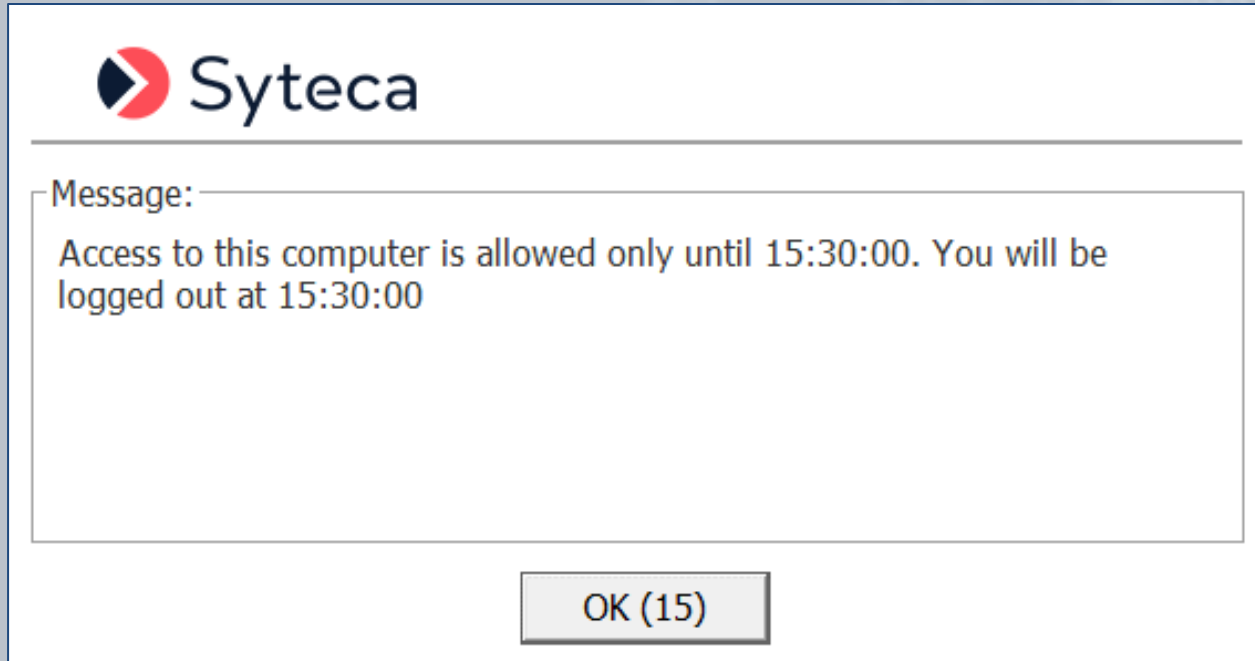
Cancel



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

OK

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

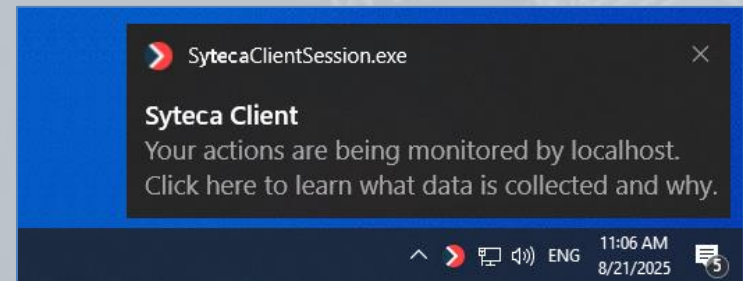
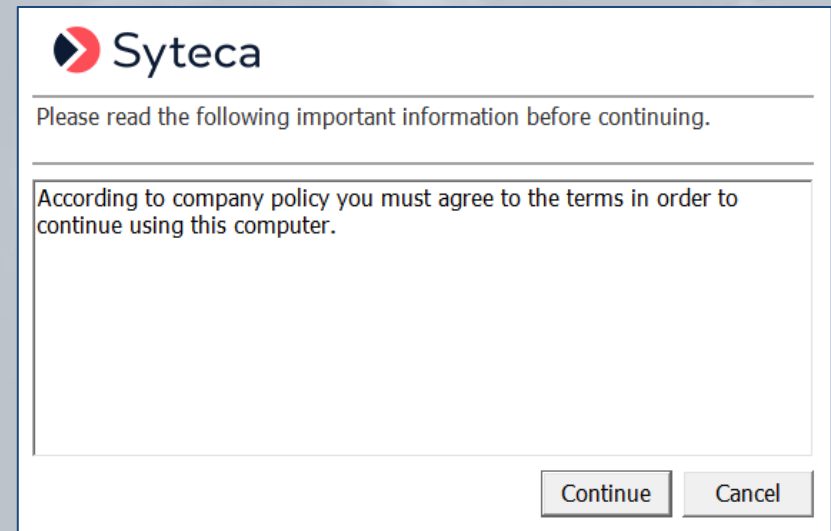


Notifying Users About Being Monitored

Notifying Users about Being Monitored

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

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



Notifying Users about Being Monitored



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

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

A screenshot of a Syteca login form. At the top is the Syteca logo. Below it is a horizontal line, followed by the text "Please read the following important information before continuing." Another horizontal line follows. Below that is a large rectangular box containing the text "According to company policy you must agree to the terms in order to continue using this computer." Below this box is the label "Ticket number is required:" followed by a text input field. Below that is the label "Your comment is required:" followed by a text area with up and down arrow buttons on the right. Below the text area is a checkbox with the text "I agree to the terms of use." At the bottom right are two buttons: "Continue" and "Cancel".

Syteca

Please read the following important information before continuing.

According to company policy you must agree to the terms in order to continue using this computer.

Ticket number is required:

Your comment is required:

☐ I agree to the terms of use.

Notifying Users about Being Monitored

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

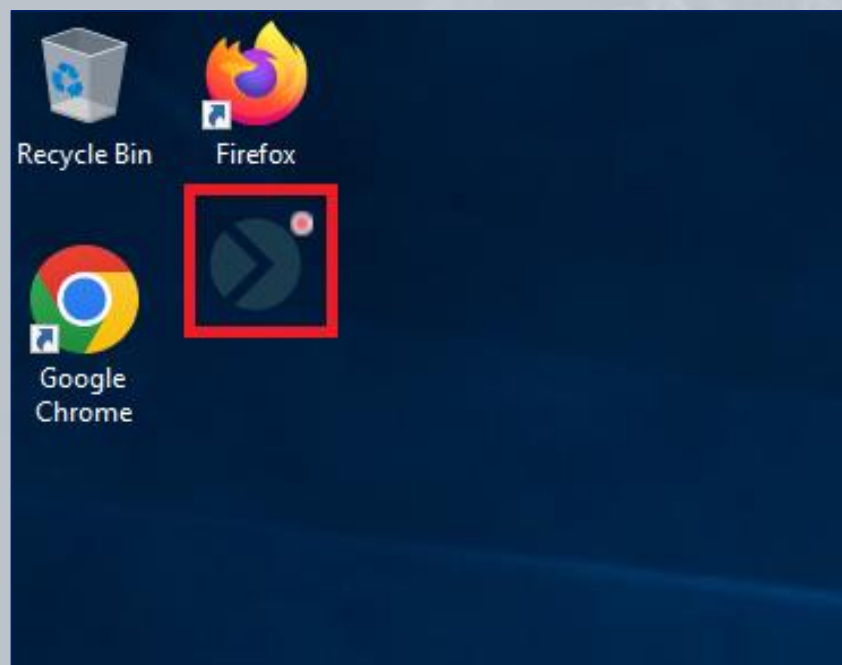
Properties User Activity Recording Monitoring [Windows/macOS] Application Filtering
Authentication Options Keystroke Monitoring Additional Options Privacy Settings

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

Notifying Users about Being Monitored

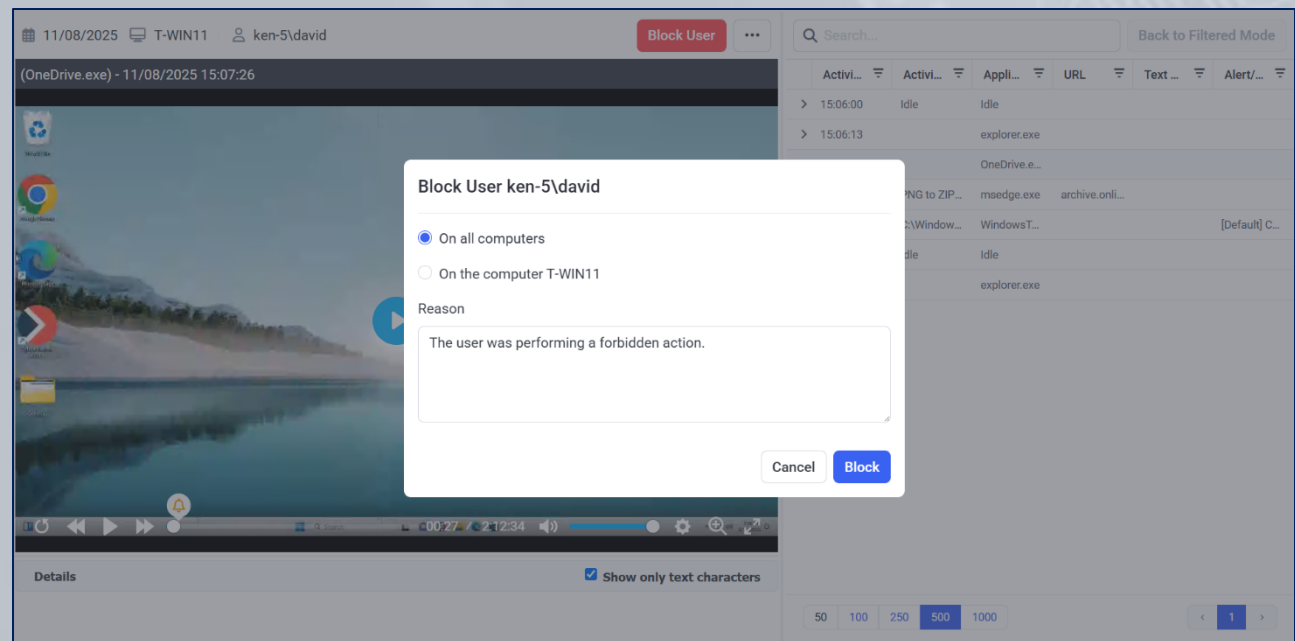
- An **icon** can also be displayed on the desktop (that is always on top of all applications opened) to **inform users** that **their actions** are currently **being monitored and recorded**.



Blocking Users

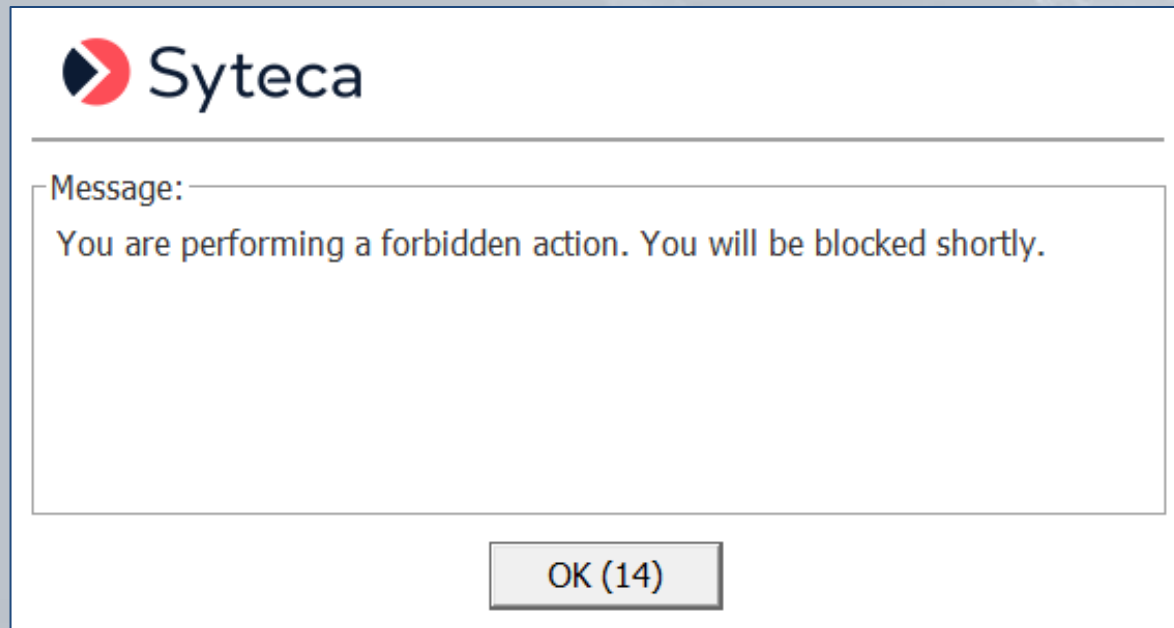
Syteca allows you to **block endpoint users** from performing potentially harmful and forbidden actions on computers running Windows OS with Syteca Clients installed on them.

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.



Viewing the Blocked Users List

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

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

Blocked Users List

localhostBuilt-in default tenant

admin

Log off

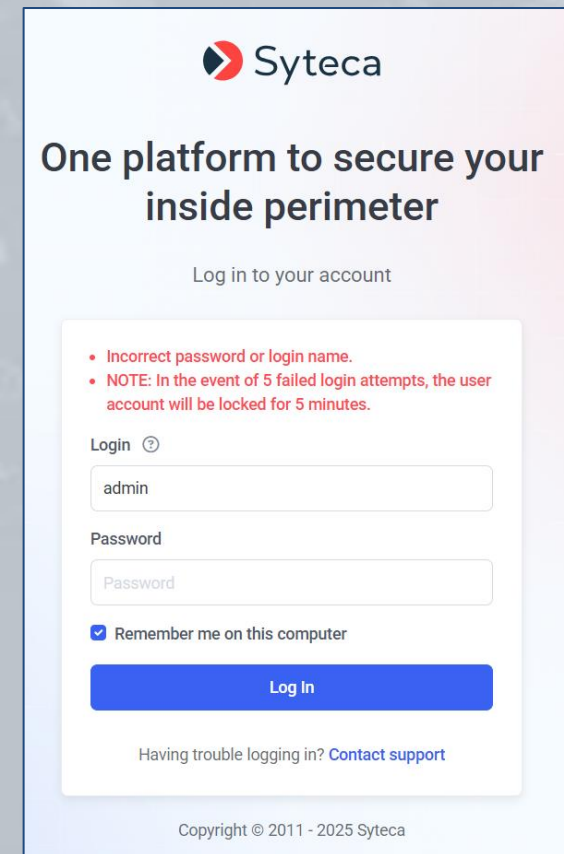
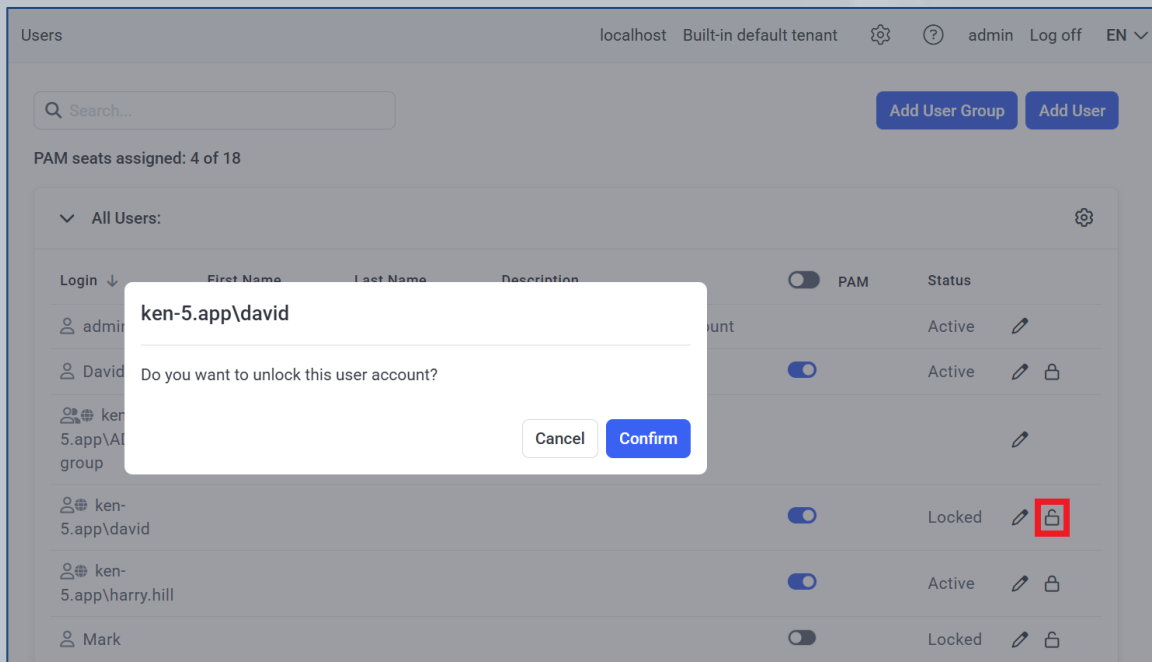
EN

Locking Management Tool User Accounts



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

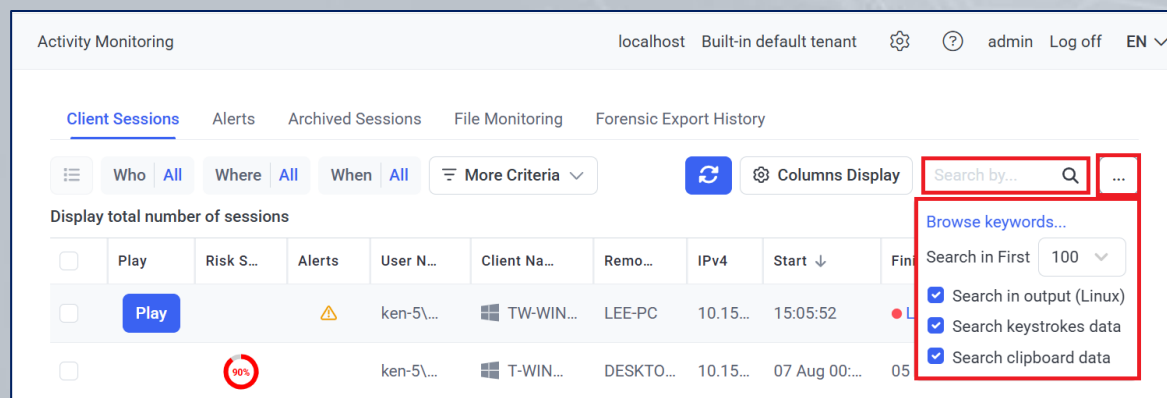
Administrators can also **lock** and **unlock** a user account **at any time**.



Viewing Client Sessions

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

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



Viewing a Session



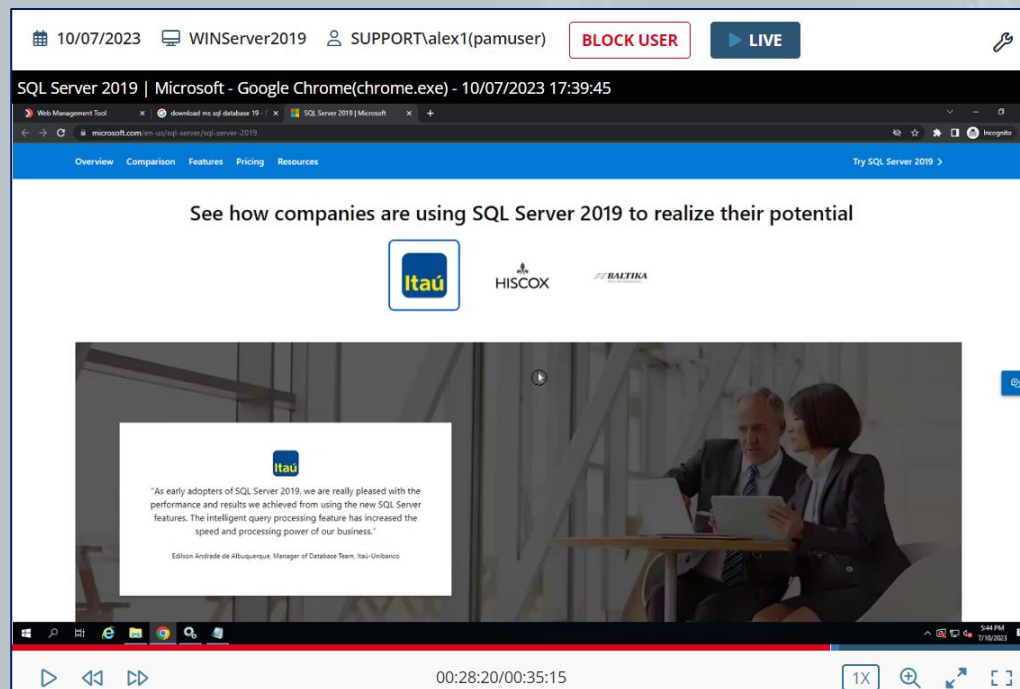
The panes in the Session Viewer display the **screen captures / video** and **metadata** recorded in the session, and can be **played back** with **alerts highlighted and color-coded**.

The screenshot displays the Syteca Session Viewer interface. The top bar shows the date 30/07/2025, the user harry-hill-pc, and the session ID KEN-5\harry.hill, along with a 'Block User' button. The main area is split into two panes. The left pane shows a video playback of a website with the Syteca logo and the text 'Transform your cybersecurity with Syteca'. The right pane shows a table of session activity.

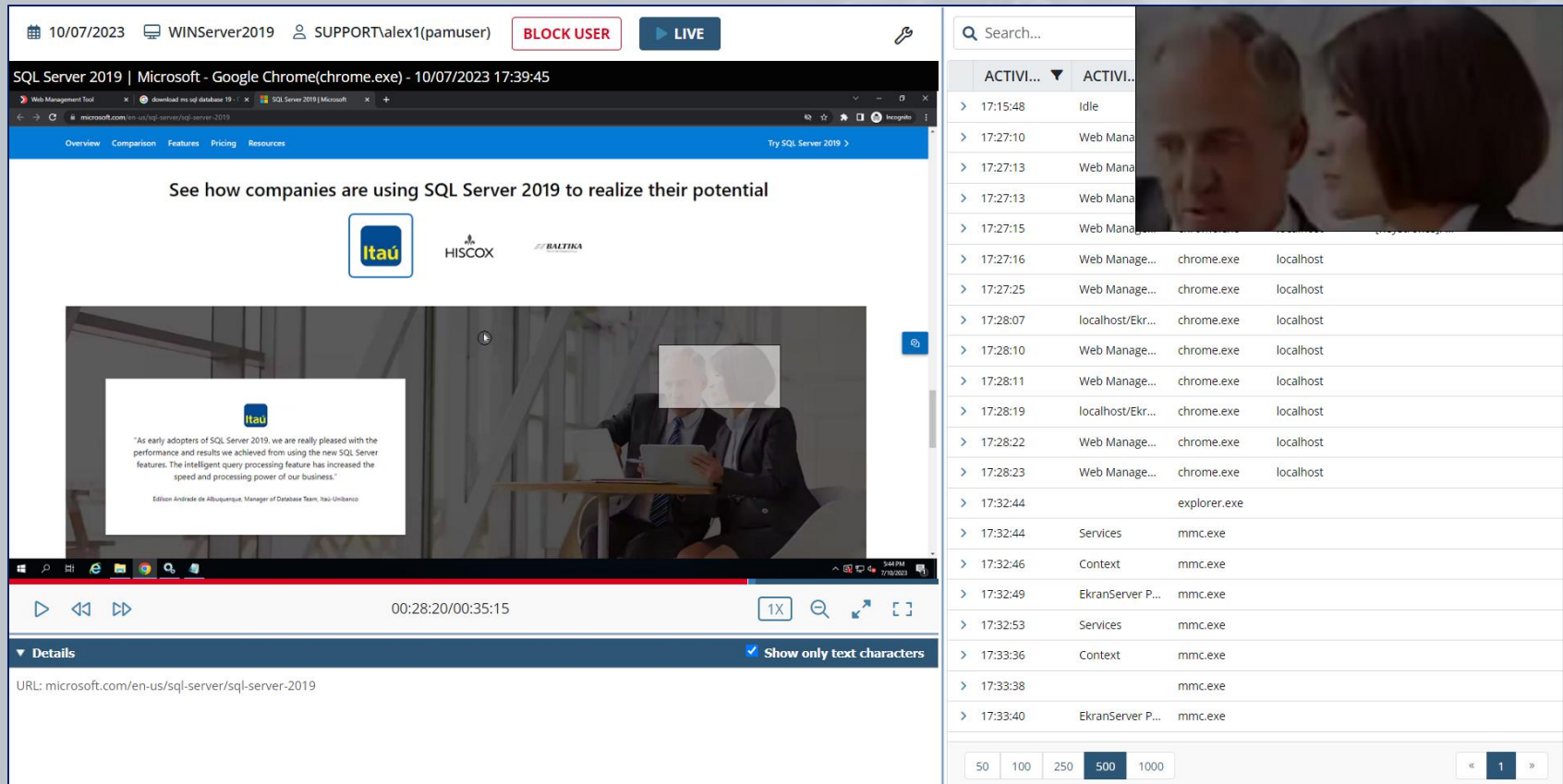
Activity ...	Activity ...	Applicat...	URL	Text Data	Alert/US...
> 13:09:28	Program Manag...	explorer.exe			[Default] Sessio...
> 13:09:35	New Tab - Goog...	chrome.exe			
> 13:09:37	New Tab - Goog...	chrome.exe	weather.com		
> 13:09:44	New Tab - Goog...	chrome.exe	weather.com		
> 13:09:44	New Tab - Goog...	chrome.exe			
> 13:09:44	New Tab - Goog...	chrome.exe	weather.com		
> 13:09:46	New Tab - Goog...	chrome.exe	weather.com	[Clipboard (Cop...	
> 13:09:46	New Tab - Goog...	chrome.exe	weather.com		
> 13:09:47	New Tab - Goog...	chrome.exe	weather.com		
> 13:09:47	New Tab - Goog...	chrome.exe	weather.com	[Clipboard (Past...	
> 13:09:51		explorer.exe			
> 13:09:52	Program Manag...	explorer.exe			
> 13:09:54	Syteca Connecti...	PamConnection...			
> 13:10:03	Remote Desko...	mstsc.exe			
> 13:10:03	Syteca Connecti...	PamConnection...		Secret usage: Ac...	
> 13:10:03	Remote Desko...	mstsc.exe			
> 13:10:03	10.100.1.10 - Re...	mstsc.exe			
> 13:10:06	Syteca Connecti...	PamConnection...			
> 13:10:07		explorer.exe			
> 13:10:08	Program Manag...	explorer.exe			
> 13:10:10	New Tab - Goog...	chrome.exe			
> 13:10:11	New Tab - Goog...	chrome.exe	facebook		[Default] Social ...
> 13:10:12	New Tab - Goog...	chrome.exe	facebook		
> 13:10:15	New Tab - Goog...	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**.



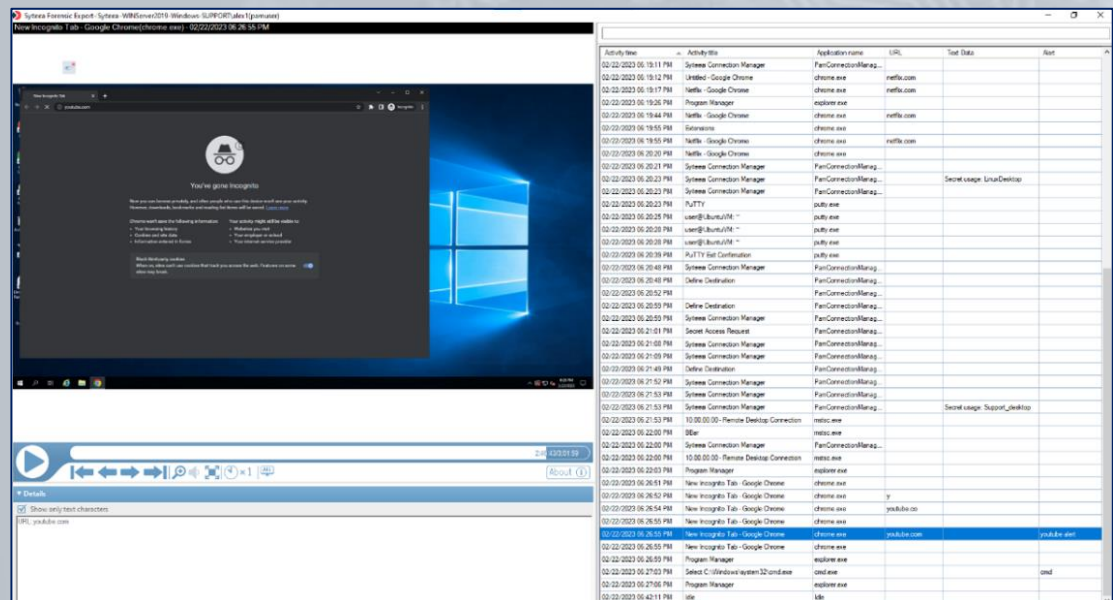
The screenshot displays the Syteca Session Player interface. The main pane shows a video of the Microsoft SQL Server 2019 website. The video player includes a magnifying glass icon in the bottom right corner. The details pane at the bottom left shows the URL: `microsoft.com/en-us/sql-server/sql-server-2019`. The right pane displays a list of active processes.

Search...	ACTIVI...	ACTIVI...
> 17:15:48	Idle	
> 17:27:10	Web Mana	
> 17:27:13	Web Mana	
> 17:27:13	Web Mana	
> 17:27:15	Web Mana	
> 17:27:16	Web Manage...	chrome.exe localhost
> 17:27:25	Web Manage...	chrome.exe localhost
> 17:28:07	localhost/Ekr...	chrome.exe localhost
> 17:28:10	Web Manage...	chrome.exe localhost
> 17:28:11	Web Manage...	chrome.exe localhost
> 17:28:19	localhost/Ekr...	chrome.exe localhost
> 17:28:22	Web Manage...	chrome.exe localhost
> 17:28:23	Web Manage...	chrome.exe localhost
> 17:32:44		explorer.exe
> 17:32:44	Services	mmc.exe
> 17:32:46	Context	mmc.exe
> 17:32:49	Ekranserver P...	mmc.exe
> 17:32:53	Services	mmc.exe
> 17:33:36	Context	mmc.exe
> 17:33:38		mmc.exe
> 17:33:40	Ekranserver P...	mmc.exe

At the bottom of the right pane, there are filters for 50, 100, 250, 500, and 1000, with 500 selected. A page indicator shows 1 of 1.

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

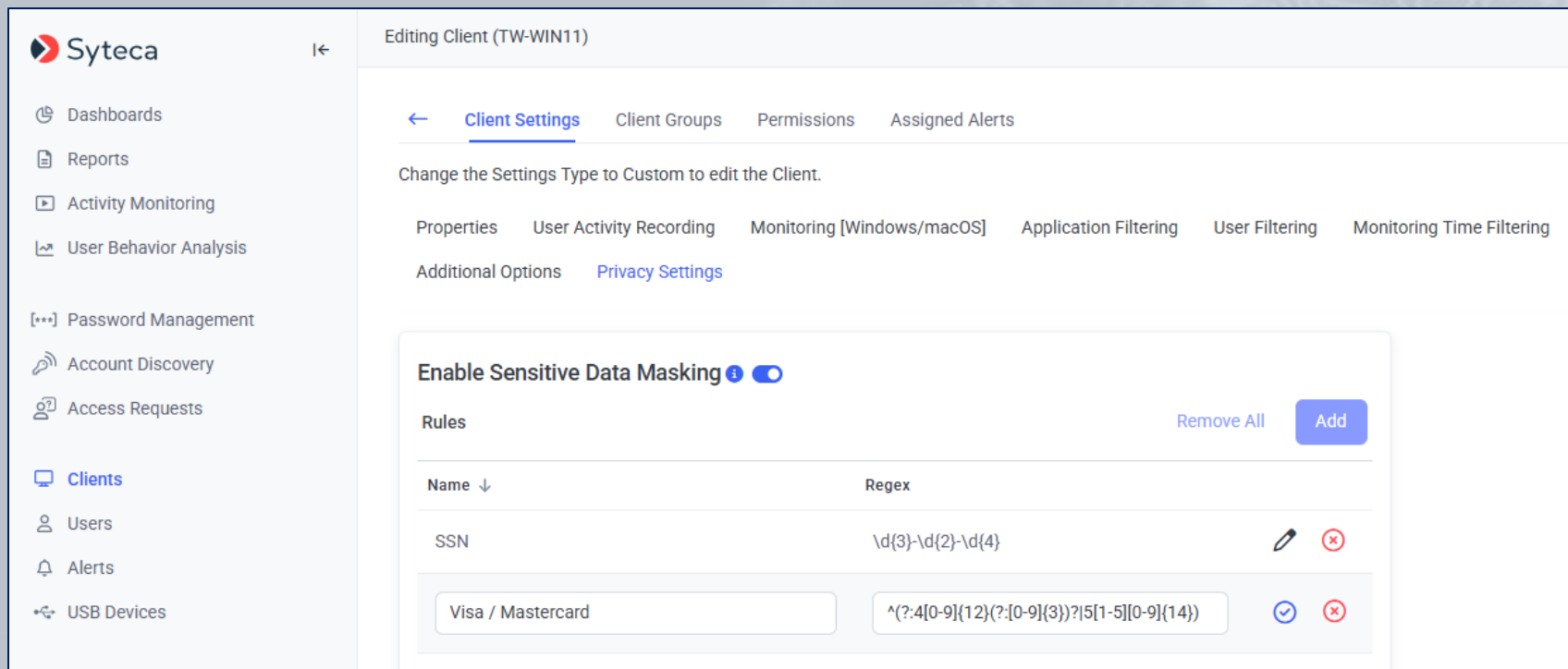
- **Export** selected **monitored sessions** (or all or part of one) to a securely **encrypted** file, and **verify its integrity** (and to **MP4** format for **video**).
- **Investigate** the user activity **data recorded** by using the offline Syteca Forensic Player.
- Present **evidence** in a **forensic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



Sensitive Data Masking

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

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.



Syteca | 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

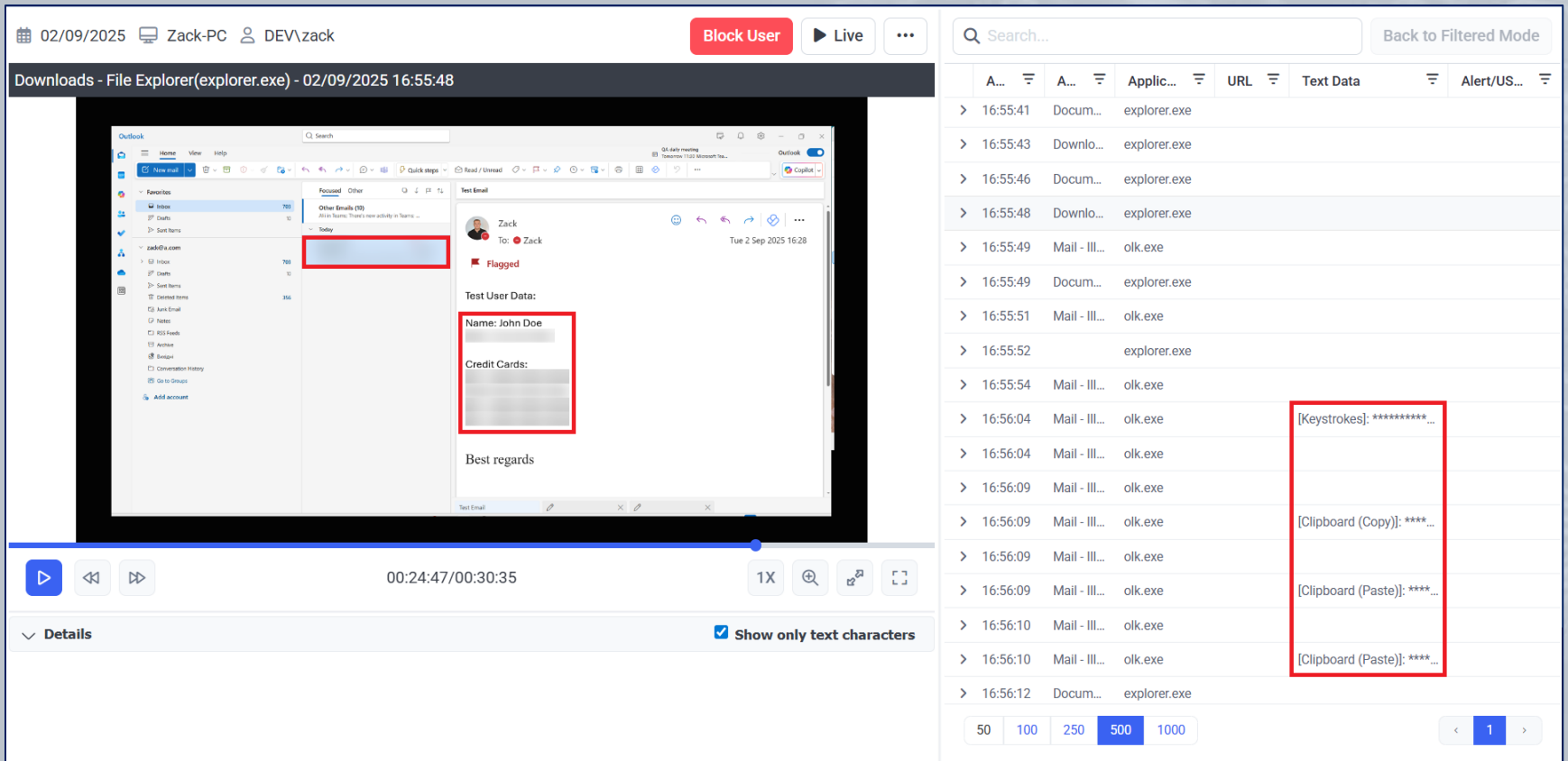
Additional Options | **Privacy Settings**

Enable Sensitive Data Masking 

Rules Remove All Add

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

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



The screenshot displays the Syteca Sessions Viewer interface. The top bar shows the date 02/09/2025, the user Zack-PC, and the session ID DEV\zack. A red 'Block User' button and a 'Live' button are visible. The main area is divided into two panes. The left pane shows a file explorer window titled 'Downloads - File Explorer(explorer.exe) - 02/09/2025 16:55:48'. The right pane shows a list of sessions with columns for time, application, URL, text data, and alert/US. The 'Text Data' column contains masked sensitive information, including 'Name: John Doe', 'Credit Cards:', and '[Keystrokes]: *****'. The 'Clipboard (Copy): ****...' and 'Clipboard (Paste): ****...' entries are also visible. A red box highlights the masked data in the 'Text Data' column. The bottom of the interface shows a 'Details' section with a 'Show only text characters' checkbox and a progress bar.

	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		[Keystrokes]: *****	
>	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		[Clipboard (Copy)]: ****...	
>	16:56:09	Mail - III...	olk.exe			
>	16:56:09	Mail - III...	olk.exe		[Clipboard (Paste)]: ****...	
>	16:56:10	Mail - III...	olk.exe			
>	16:56:10	Mail - III...	olk.exe			
>	16:56:10	Mail - III...	olk.exe			
>	16:56:12	Docum...	explorer.exe			

Pseudonymizer

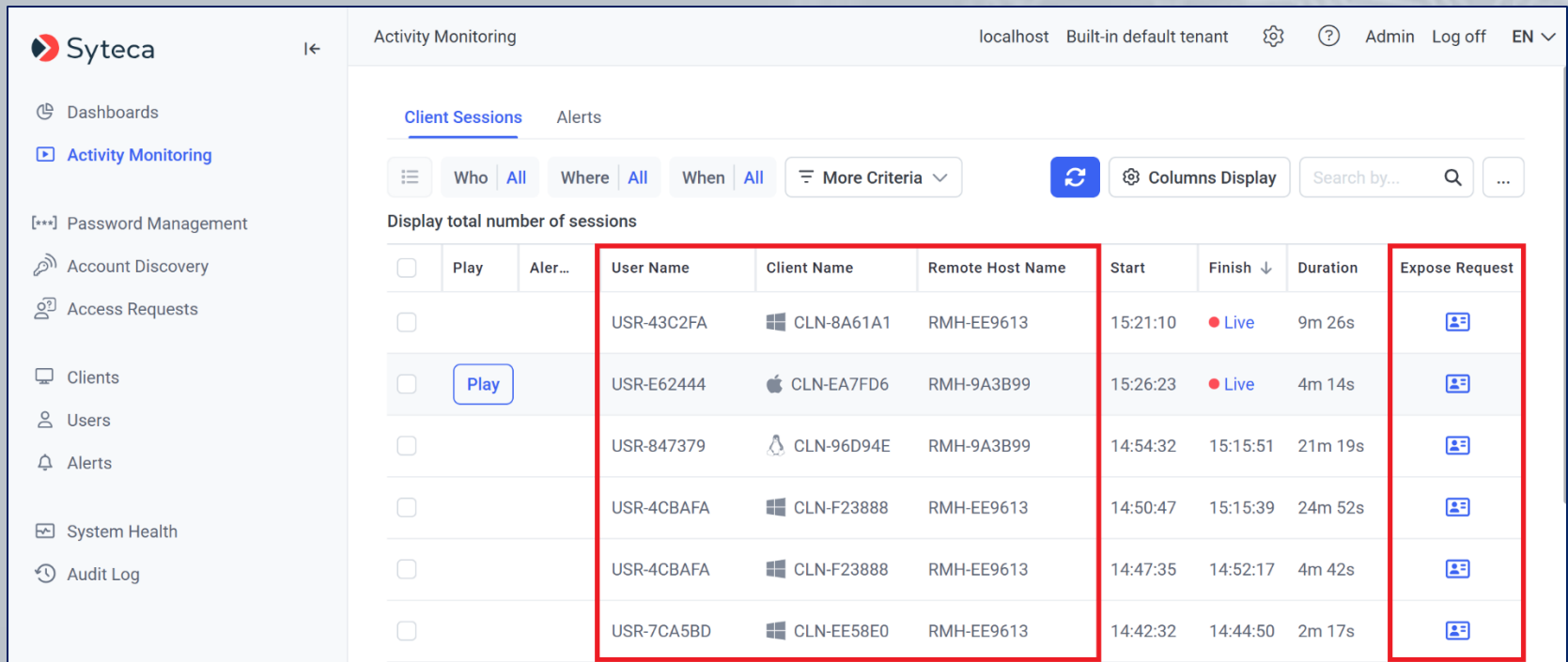
(for GDPR compliance, etc.)

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 (PII)** 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).

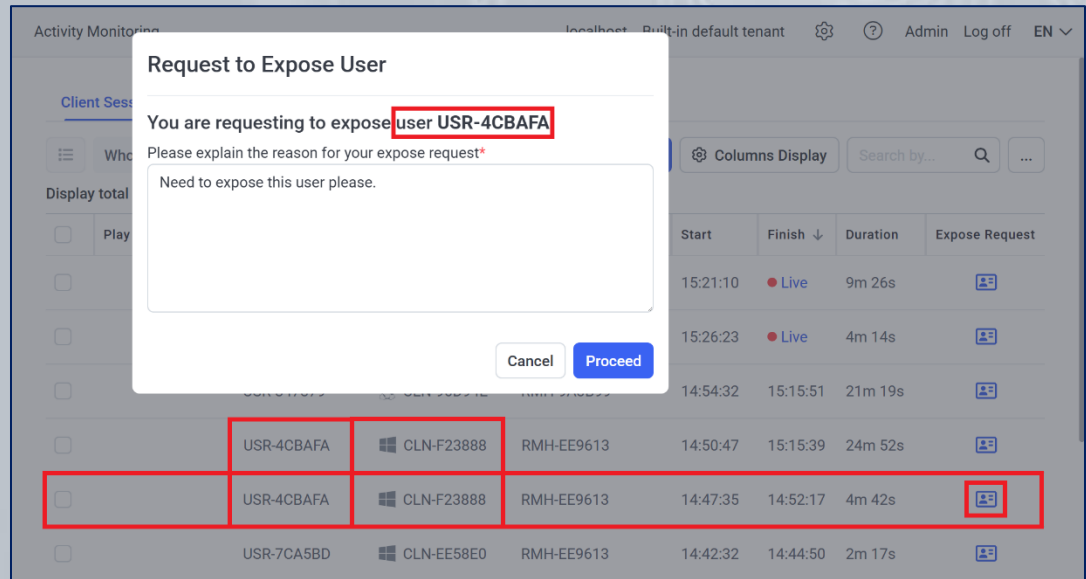


The screenshot displays the Syteca Activity Monitoring interface. The left sidebar contains navigation links: Dashboards, Activity Monitoring (selected), Password Management, Account Discovery, Access Requests, Clients, Users, Alerts, System Health, and Audit Log. The main panel is titled 'Activity Monitoring' and shows 'Client Sessions' and 'Alerts' tabs. Below the tabs are filters for 'Who', 'Where', and 'When', all set to 'All'. A 'More Criteria' dropdown and a 'Columns Display' button are also present. A search bar is located on the right. The table below shows a list of sessions, with a red box highlighting the 'User Name', 'Client Name', 'Remote Host Name', and 'Expose Request' columns. The 'Expose Request' column contains a red icon representing a user profile.

	Play	Aler...	User Name	Client Name	Remote Host Name	Start	Finish ↓	Duration	Expose Request
☐			USR-43C2FA	CLN-8A61A1	RMH-EE9613	15:21:10	● Live	9m 26s	
☐	Play		USR-E62444	CLN-EA7FD6	RMH-9A3B99	15:26:23	● Live	4m 14s	
☐			USR-847379	CLN-96D94E	RMH-9A3B99	14:54:32	15:15:51	21m 19s	
☐			USR-4CBAFA	CLN-F23888	RMH-EE9613	14:50:47	15:15:39	24m 52s	
☐			USR-4CBAFA	CLN-F23888	RMH-EE9613	14:47:35	14:52:17	4m 42s	
☐			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.**



The screenshot displays the 'Activity Monitoring' interface. A modal dialog titled 'Request to Expose User' is open, showing a confirmation message: 'You are requesting to expose user USR-4CBAFA'. Below this, there is a text input field with the placeholder 'Please explain the reason for your expose request*' and a pre-filled text 'Need to expose this user please.'. The dialog has 'Cancel' and 'Proceed' buttons. In the background, a table lists activity sessions. The row for user 'USR-4CBAFA' on client 'CLN-F23888' is highlighted with a red box. The table columns include 'Start', 'Finish', 'Duration', and 'Expose Request'.

Start	Finish	Duration	Expose Request
15:21:10	Live	9m 26s	
15:26:23	Live	4m 14s	
14:54:32	15:15:51	21m 19s	
14:50:47	15:15:39	24m 52s	
14:47:35	14:52:17	4m 42s	
14:42:32	14:44:50	2m 17s	

Temporarily De-Anonymizing PII Data



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

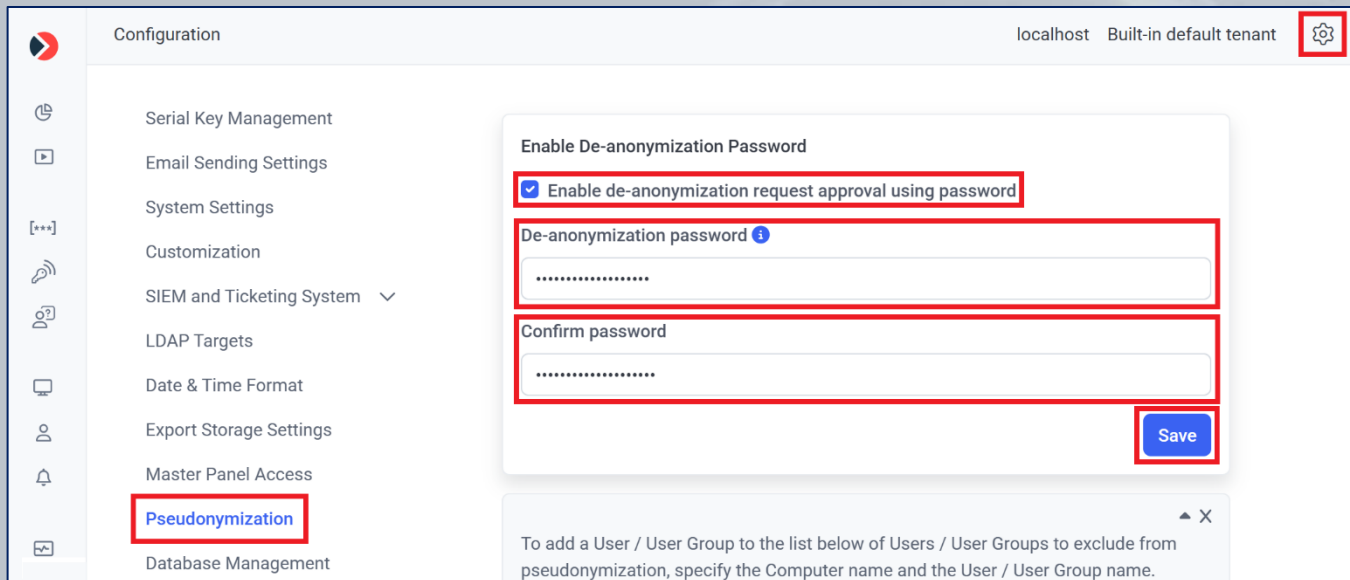
[Client Sessions](#) [Alerts](#)

☐ Who [All](#) Where [All](#) When [All](#) [More Criteria](#) [Columns Display](#)

Display total number of sessions

☐	Play	Aler...	User Name	Client Name	Remote Host Name	Start	Finish ↓	Duration	Expose Request
☐			USR-43C2FA	CLN-8A61A1	RMH-EE9613	15:21:10	● Live	16m 56s	
☐			USR-E62444	CLN-EA7FD6	RMH-9A3B99	15:26:23	● Live	11m 44s	
☐			USR-847379	CLN-96D94E	RMH-9A3B99	14:54:32	15:15:51	21m 19s	
☐			KEN-5\harry....	rod-win10	DESKTOP-BBDE050	14:50:47	15:15:39	24m 52s	
☐			KEN-5\harry....	rod-win10	DESKTOP-BBDE050	14:47:35	14:52:17	4m 42s	
☐			USR-7CA5BD	CLN-EE58E0	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

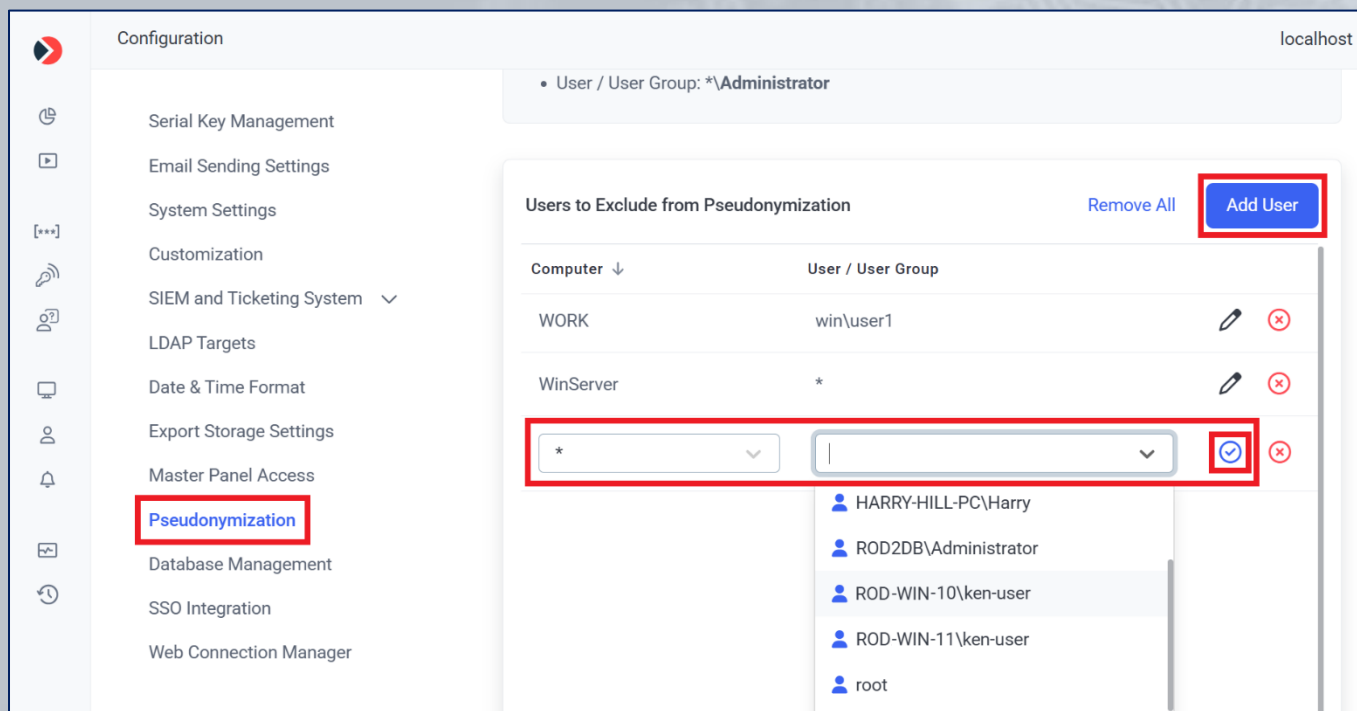
Save

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**.

Excluding User from Pseudonymization

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 Configuration interface. The left sidebar contains a menu with the following items: 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** (highlighted with a red box), Database Management, SSO Integration, and Web Connection Manager. The main content area is titled 'Configuration' and shows the 'User / User Group: *\Administrator' selection. Below this, the 'Users to Exclude from Pseudonymization' section is visible, with a 'Remove All' button and an 'Add User' button (highlighted with a red box). The table below shows the list of users to be excluded:

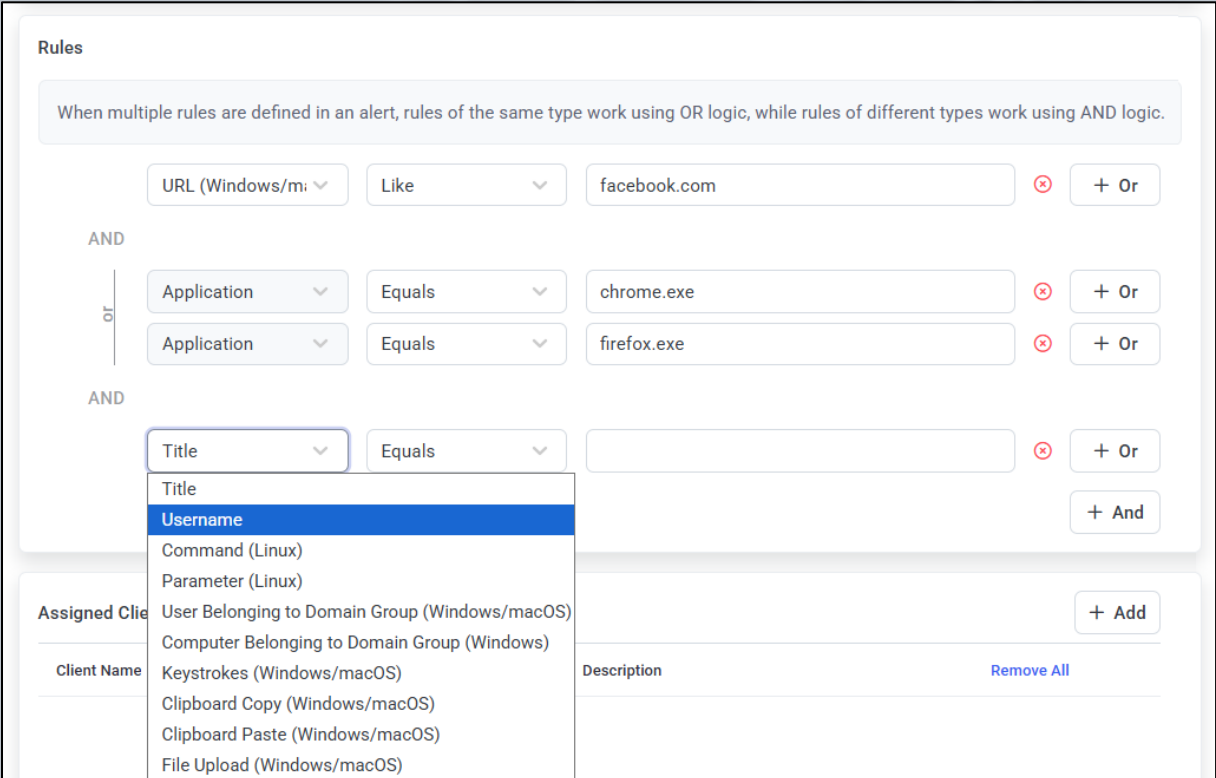
Computer ↓	User / User Group	
WORK	win\user1	 
WinServer	*	 
*		 

The dropdown menu for the 'Add User' button is open, showing a list of users: HARRY-HILL-PC\Harry, ROD2DB\Administrator, ROD-WIN-10\ken-user, ROD-WIN-11\ken-user, and root. The 'Add' button (highlighted with a red box) is visible in the dropdown menu.

Alerts

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

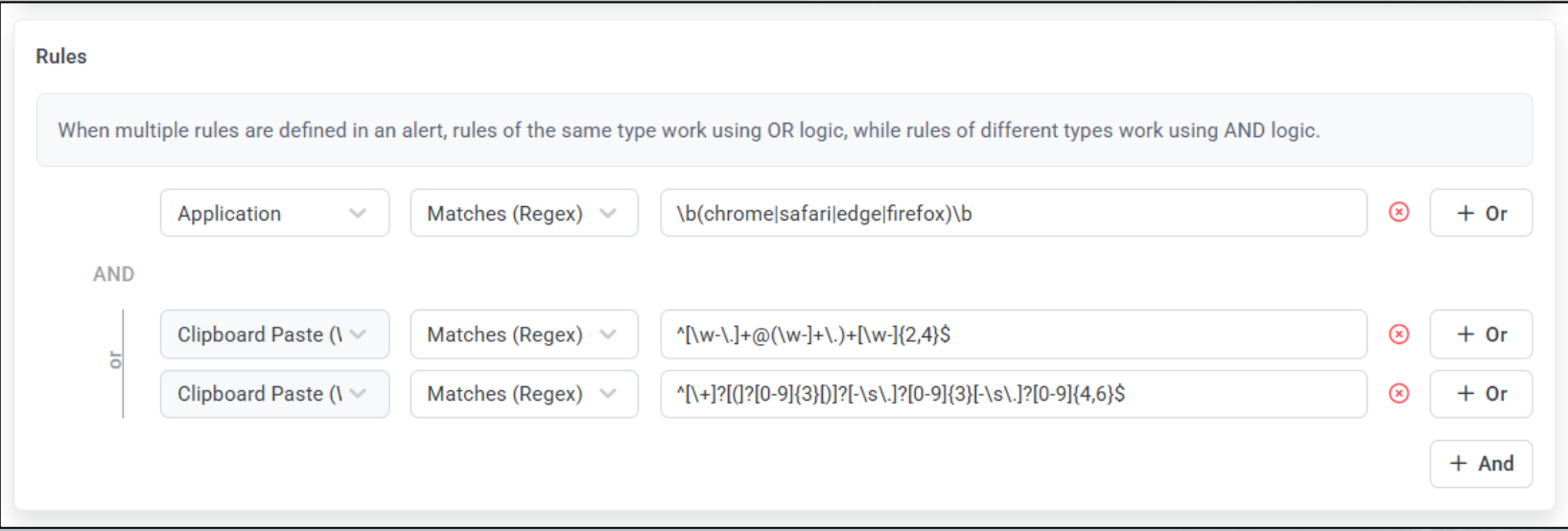
- **Add alert rules** to detect specific suspicious user activity on Client computers.
- Specify individuals to receive instant **alert notifications** via **email** and **tray** notifications.



The screenshot shows the 'Rules' configuration page in the Syteca interface. At the top, a note states: 'When multiple rules are defined in an alert, rules of the same type work using OR logic, while rules of different types work using AND logic.' Below this, there are three rule groups. The first group is connected by an 'Or' operator and contains one rule: 'URL (Windows/m:)' with the value 'facebook.com'. The second group is connected by an 'And' operator and contains two rules: 'Application' with the value 'chrome.exe' and 'Application' with the value 'firefox.exe'. The third group is also connected by an 'And' operator and contains one rule: 'Title' with the value 'Equals'. A dropdown menu is open for the 'Title' rule, showing a list of fields: 'Title', 'Username' (highlighted), 'Command (Linux)', 'Parameter (Linux)', 'User Belonging to Domain Group (Windows/macOS)', 'Computer Belonging to Domain Group (Windows)', 'Keystrokes (Windows/macOS)', 'Clipboard Copy (Windows/macOS)', 'Clipboard Paste (Windows/macOS)', and 'File Upload (Windows/macOS)'. At the bottom, there are sections for 'Assigned Client' (with a 'Client Name' field), 'Description' (with a 'Remove All' link), 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.



The screenshot shows the 'Rules' configuration interface. At the top, a note states: 'When multiple rules are defined in an alert, rules of the same type work using OR logic, while rules of different types work using AND logic.' Below this, the rules are organized into two main sections. The first section contains a single rule: 'Application' (dropdown) 'Matches (Regex)' (dropdown) with the regex '\b(chrome|safari|edge|firefox)\b'. The second section, labeled 'AND' on the left, contains two rules of the same type: 'Clipboard Paste (\)' (dropdown) 'Matches (Regex)' (dropdown). The first rule in this section has the regex '^[\\w-\\.]+@([\\w-]+\\.){2,4}\$' and the second has '^[\\+]?([0-9]{3})?[-\\s\\.]?[0-9]{3}[-\\s\\.]?[0-9]{4,6}\$'. Each rule has a red 'x' icon and a '+ Or' button. At the bottom right of the second section is a '+ And' button.

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

AND

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

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

+ Or

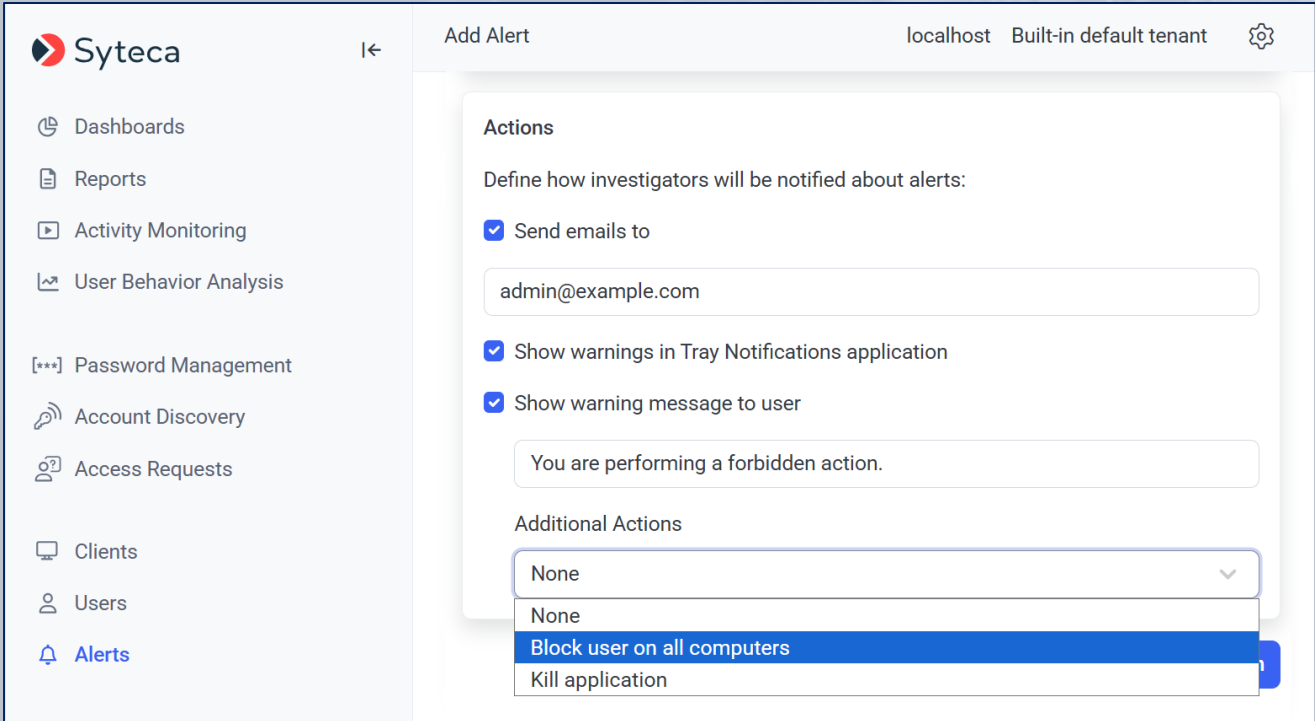
+ Or

+ 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.**



Syteca | Add Alert | localhost | Built-in default tenant

Actions

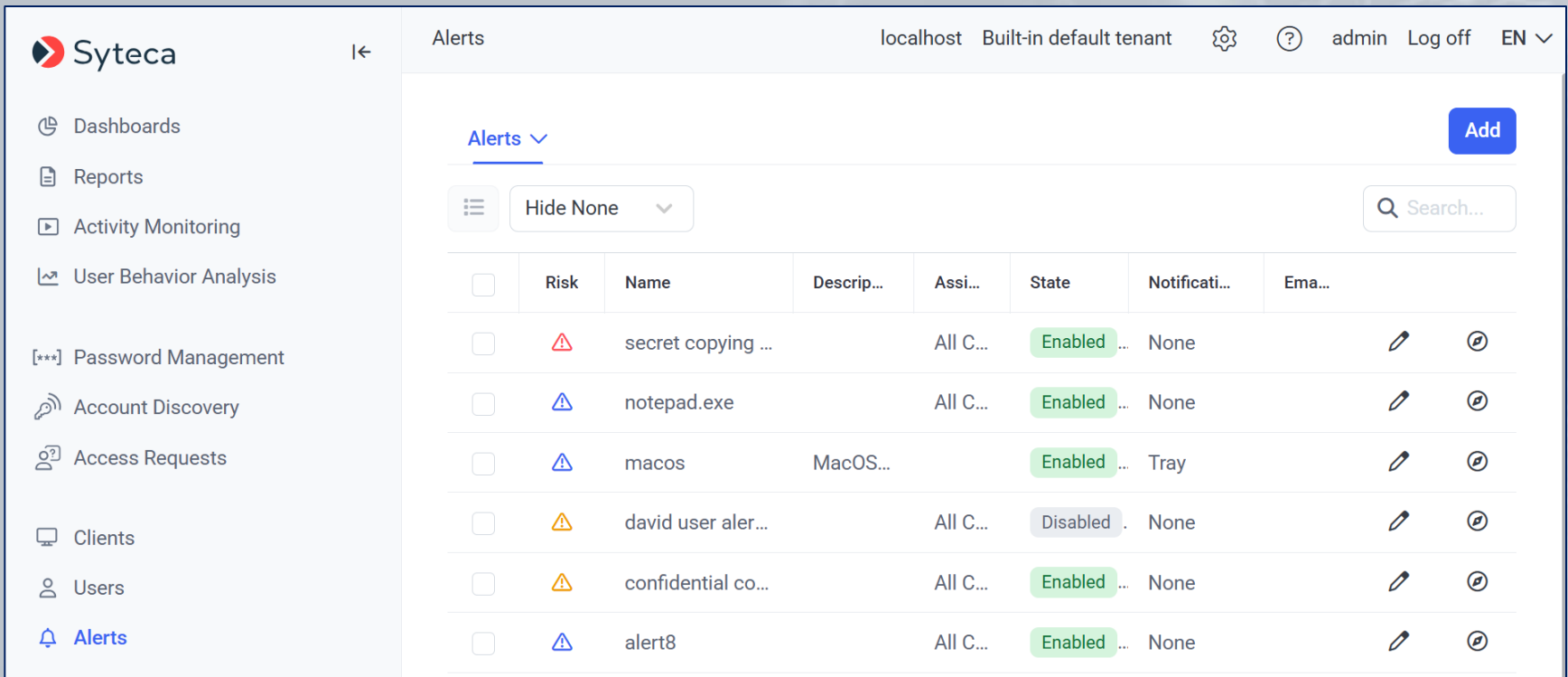
Define how investigators will be notified about alerts:

- ☒ Send emails to
admin@example.com
- ☒ Show warnings in Tray Notifications application
- ☒ Show warning message to user
You are performing a forbidden action.

Additional Actions

- None
- Block user on all computers**
- 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 Alerts management interface. On the left is a sidebar with navigation links: Dashboards, Reports, Activity Monitoring, User Behavior Analysis, Password Management, Account Discovery, Access Requests, Clients, Users, and Alerts (highlighted). The main content area is titled 'Alerts' and includes a top bar with 'localhost Built-in default tenant', user 'admin', and 'Log off' button. Below the title bar, there's a search bar and a table of alerts. The table has columns: Risk, Name, Descrip..., Assi..., State, Notificati..., and Ema... (Email). The table lists seven default alerts with their respective risk levels, names, descriptions, associations, states, and notification settings.

	Risk	Name	Descrip...	Assi...	State	Notificati...	Ema...
☐	High	secret copying ...		All C...	Enabled	None	 
☐	Medium	notepad.exe		All C...	Enabled	None	 
☐	Medium	macos	MacOS...		Enabled	Tray	 
☐	Low	david user aler...		All C...	Disabled	None	 
☐	Low	confidential co...		All C...	Enabled	None	 
☐	Medium	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.

Activity Monitoring localhost Built-in default tenant admin Log off EN

Client Sessions **Alerts** Archived Sessions File Monitoring Forensic Export History

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

☒ **Change Status** > **New**
In Progress
False Alarm
Resolved
Confirmed Risk

				What	Who	W...	When ↓	Keywords	Status	Notes
☒	45469	⚠	alert3	C:\Windows\System32\cmd.exe - WindowsTerminal.exe	ken...	TW...	15:09:28	terminal.exe	New	Add
☐	45469	⚠	alert3	New Tab - Google Chrome - chrome.exe - alert3	ken...	TW...	05 Aug ...	alert3	In Progress	Add admin Note2 (+1)
☐	45455	⚠	[Default] Social networks	Installing Windows Clients Locally Using the Insta ...	ken...	TW...	05 Aug ...	facebook	False Alarm	Add admin Note1
☐	45358	⚠	mass storage device alert	Mass storage device - Working - USB Mass Storage D ...	ken...	TW...	05 Aug ...		Resolved	Add
☒	45336	⚠	mass storage device alert	Mass storage device - Blocked - USB Mass Storage D ...	tw-w...	TW...	05 Aug ...		Confirmed Risk	Add

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**).

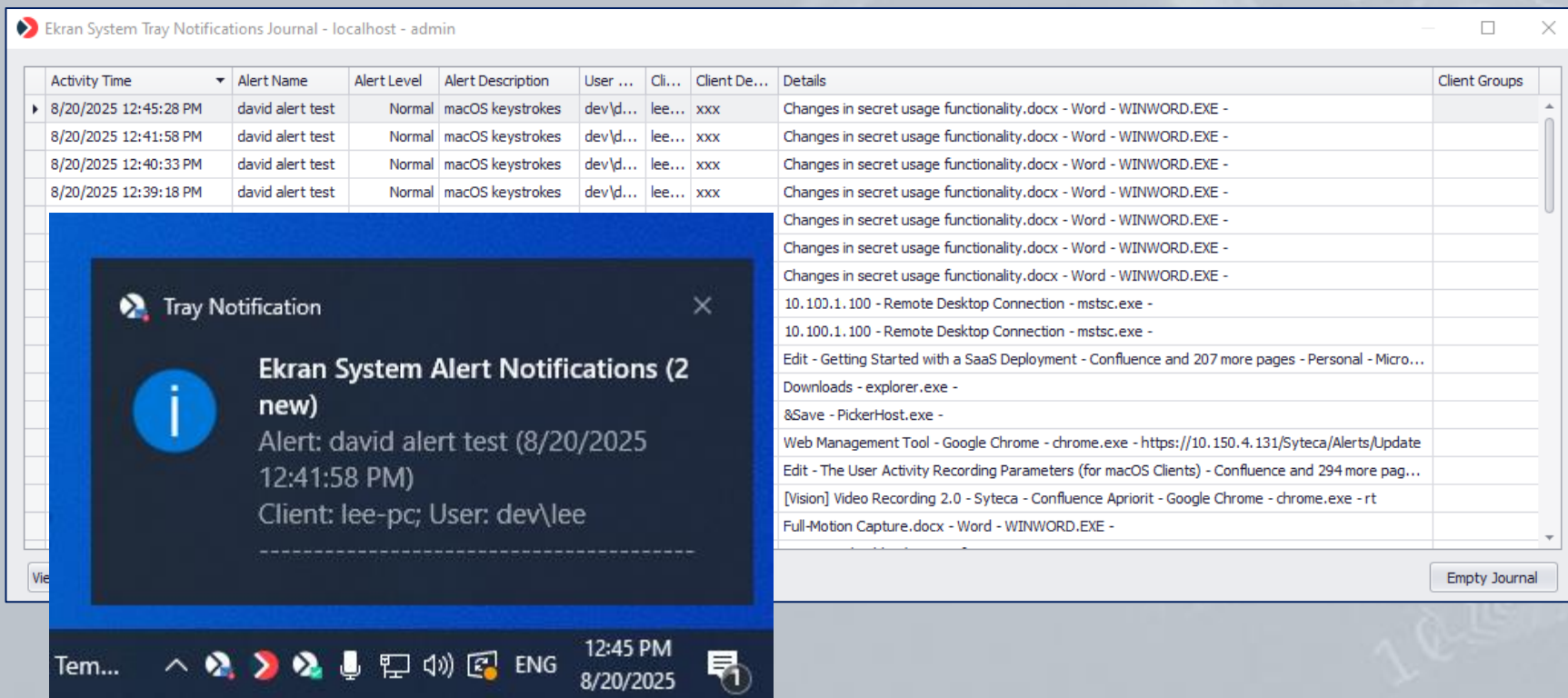
The screenshot displays the Syteca Session Viewer interface. The top bar shows the date 12/07/2023, the session name WINServer2019, the user WINSERVER2019\Administrator(pamuser), and buttons for BLOCK USER and LIVE. The main window shows a Facebook login page in Google Chrome. A blue alert bubble at the bottom left indicates a 'david facebook alert'. The right sidebar contains a search bar and a table of alert events.

AC...	ACTIVITY TITLE	APP...	URL	TEXT DATA	ALERT/USB ...
>	18:39:25	Google Lens - Google Ch...	chrome.exe	lens.google.c...	
>	18:39:27	Google Lens - Google Ch...	chrome.exe	google.com	
>	18:39:27	facebook - Google 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	

Details: Alert ID: 19136, Alert Name: david facebook alert, Risk Level: Normal, What: Facebook - log in or sign up - Google Chrome, When: 12/07/2023 18:39:58

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 displays the 'Ekran System Tray Notifications Journal - localhost - admin' window. It features a table with columns: Activity Time, Alert Name, Alert Level, Alert Description, User, Client, and Details. The table lists several alerts, all with 'Normal' levels and 'macOS keystrokes' descriptions. A blue tray notification popup is overlaid on the table, titled 'Ekran System Alert Notifications (2 new)', showing the alert name 'david alert test', time '8/20/2025 12:41:58 PM', and client/user information 'Client: lee-pc; User: dev\lee'. The Windows taskbar at the bottom shows the time as 12:45 PM on 8/20/2025.

Activity Time	Alert Name	Alert Level	Alert Description	User	Client	Details
8/20/2025 12:45:28 PM	david alert test	Normal	macOS keystrokes	dev\d...	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\d...	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\d...	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\d...	lee... xxx	Changes in secret usage functionality.docx - Word - WINWORD.EXE -
						Changes in secret usage functionality.docx - Word - WINWORD.EXE -
						Changes in secret usage functionality.docx - Word - WINWORD.EXE -
						Changes in secret usage functionality.docx - Word - WINWORD.EXE -
						10.100.1.100 - Remote Desktop Connection - mstsc.exe -
						10.100.1.100 - Remote Desktop Connection - mstsc.exe -
						Edit - Getting Started with a SaaS Deployment - Confluence and 207 more pages - Personal - Micro...
						Downloads - explorer.exe -
						&Save - PickerHost.exe -
						Web Management Tool - Google Chrome - chrome.exe - https://10.150.4.131/Syteca/Alerts/Update
						Edit - The User Activity Recording Parameters (for macOS Clients) - Confluence and 294 more pag...
						[Vision] Video Recording 2.0 - Syteca - Confluence Apriorit - Google Chrome - chrome.exe - rt
						Full-Motion Capture.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.

The image displays two overlapping screenshots of the Syteca USB monitoring rule configuration interface.

Left Screenshot: Edit USB Rule (Ds) - USB Rule Properties

- Select the device classes to be monitored. Devices**
- Monitored Devices**
 - ☒ Mass storage devices
 - ☐ Portable devices
 - ☐ Wireless connection devices
 - ☐ Modems and network adapters
 - ☐ Audio devices
 - ☐ Video devices
 - ☐ Human interface devices
 - ☐ Printers
 - ☐ Composite devices
 - ☐ Vendor-specific devices
- NOTE: Only mass storage devices and vendor-specific devices are supported.
- Exceptions**
 - Device ID

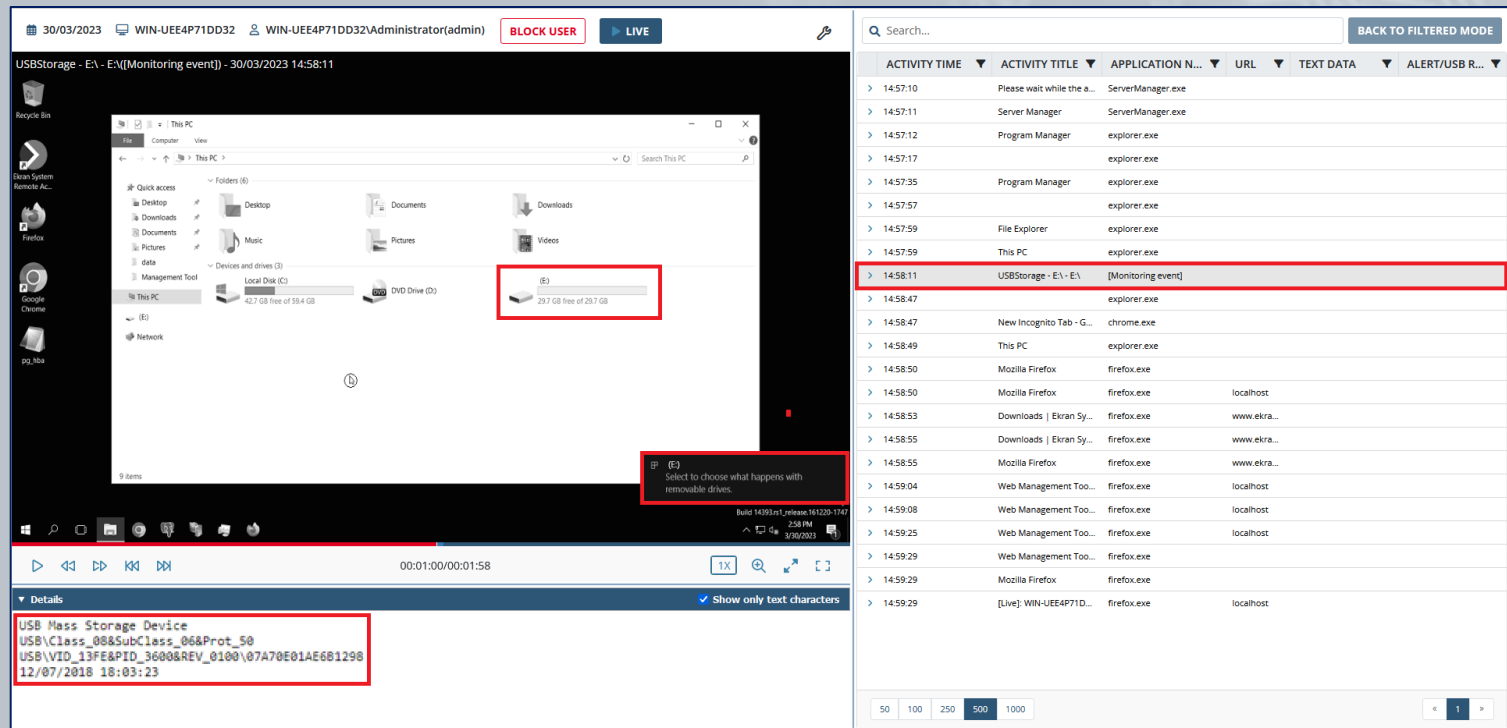
Right Screenshot: Edit USB Rule (Ds) - Additional Actions

- Notifications**
 - ☒ Send email notification to
 - test@test.com
 - ☒ Show warnings in Tray Notifications application
- Actions**
 - ☐ Block access to mass storage device until administrator's approval
 - NOTE: The above option is not supported for macOS Clients.
 - Access to the mass storage device is forbidden. Enter your comments and request access from the administrator. Only one request every 30 minutes can be sent.
 - Users who can approve access
 - 1234567
 - ☒ Block USB device
 - NOTE: The above option is not supported for macOS Clients.
 - WARNING:** Before blocking USB devices on the user's computer, make sure that all the permitted peripheral devices are added to the exceptions list.
 - ☒ Notify user on the target computer about device blocking
 - The USB device is blocked. Device info: [CompatibleID]

Buttons: Next, Finish

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.



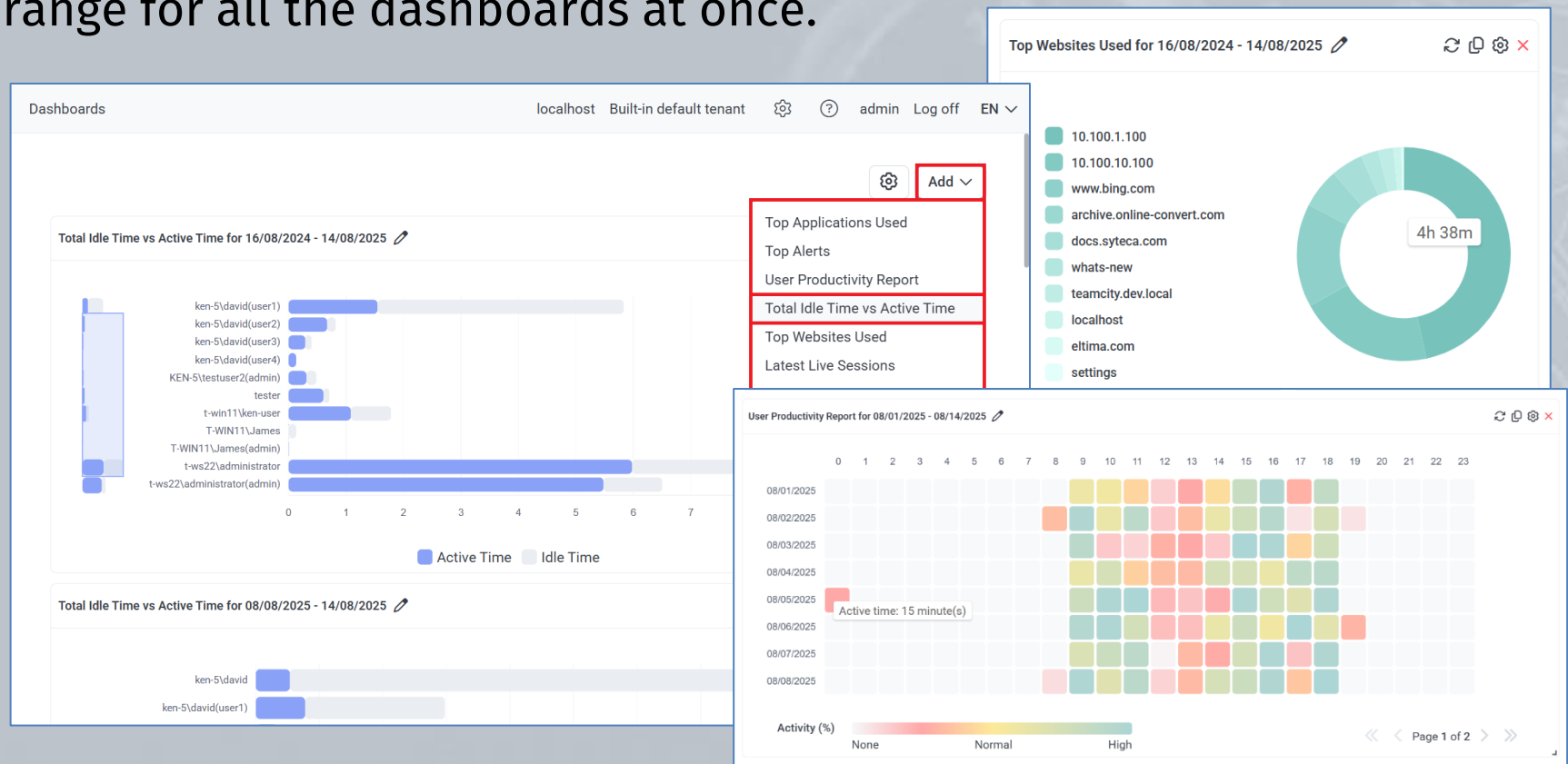
The screenshot displays the Syteca Session Viewer interface. The top bar shows the session date (30/03/2023), session ID (WIN-UEE4P71DD32), and user (Administrator(admin)). It includes buttons for 'BLOCK USER' and 'LIVE'. The main area is split into two panes. The left pane shows a Windows File Explorer window titled 'USBStorage - E:\ - EV((Monitoring event)) - 30/03/2023 14:58:11'. The window displays the 'This PC' view with various folders and drives. A red box highlights the 'E:' drive, which is labeled '29.7 GB free of 29.7 GB'. A tooltip for the 'E:' drive is visible, stating 'Select to choose what happens with removable drives.' The right pane shows an activity log table with columns: 'ACTIVITY TIME', 'ACTIVITY TITLE', 'APPLICATION N...', 'URL', 'TEXT DATA', and 'ALERT/USB R...'. The table lists various system events and application activities. A red box highlights the entry at 14:58:11, which is titled 'USBStorage - E:\ - EV' and has the text '[Monitoring event]'. Below the main view, there is a 'Details' section with a checkbox 'Show only text characters'. It contains the following text: 'USB Mass Storage Device', 'USB\Class_08&SubClass_06&Prot_50', 'USB\VID_13FE&PID_3600&REV_0100\07A70E01AE681298', and '12/07/2018 18:03:23'.

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

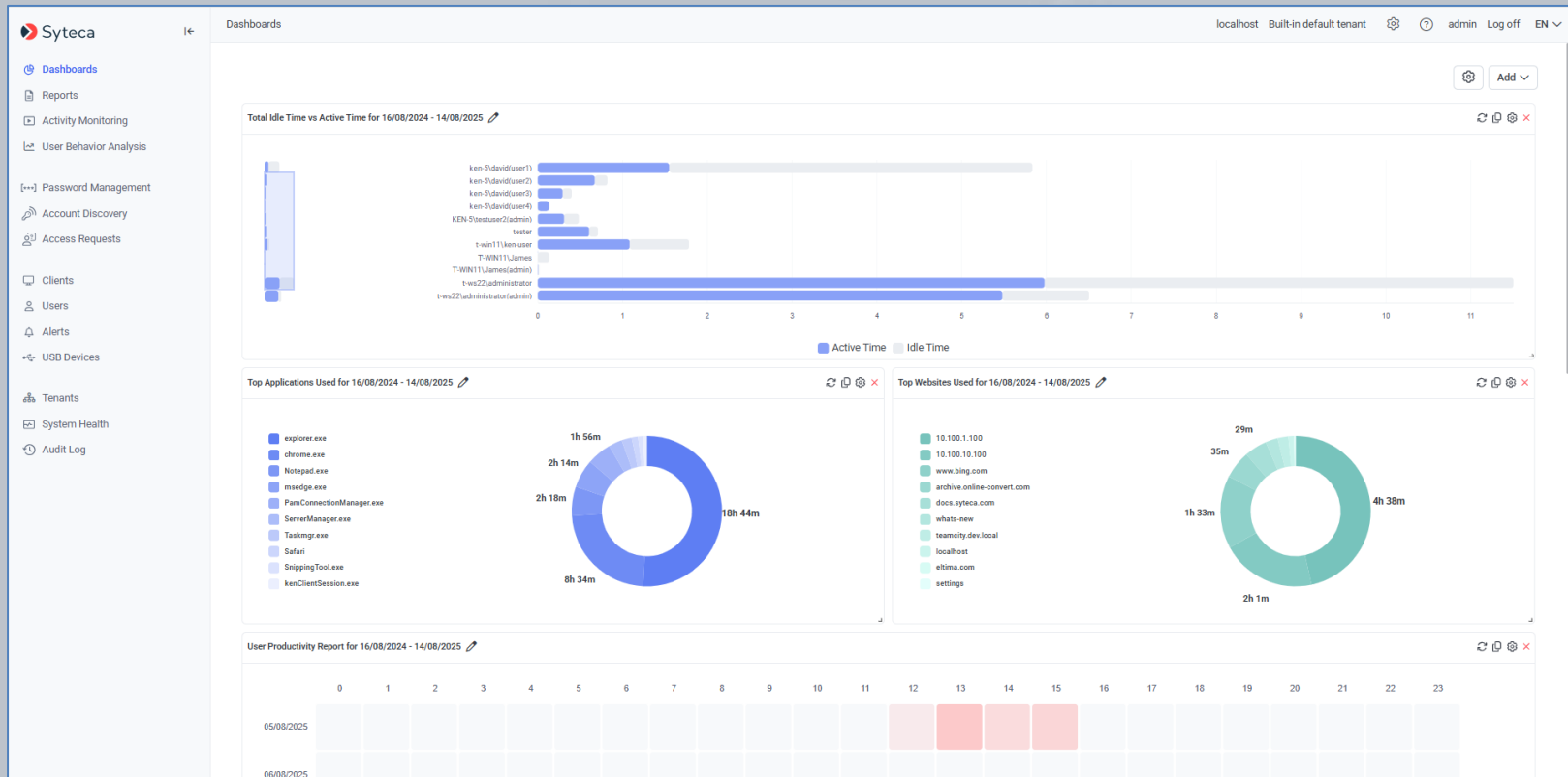
Dashboards

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

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

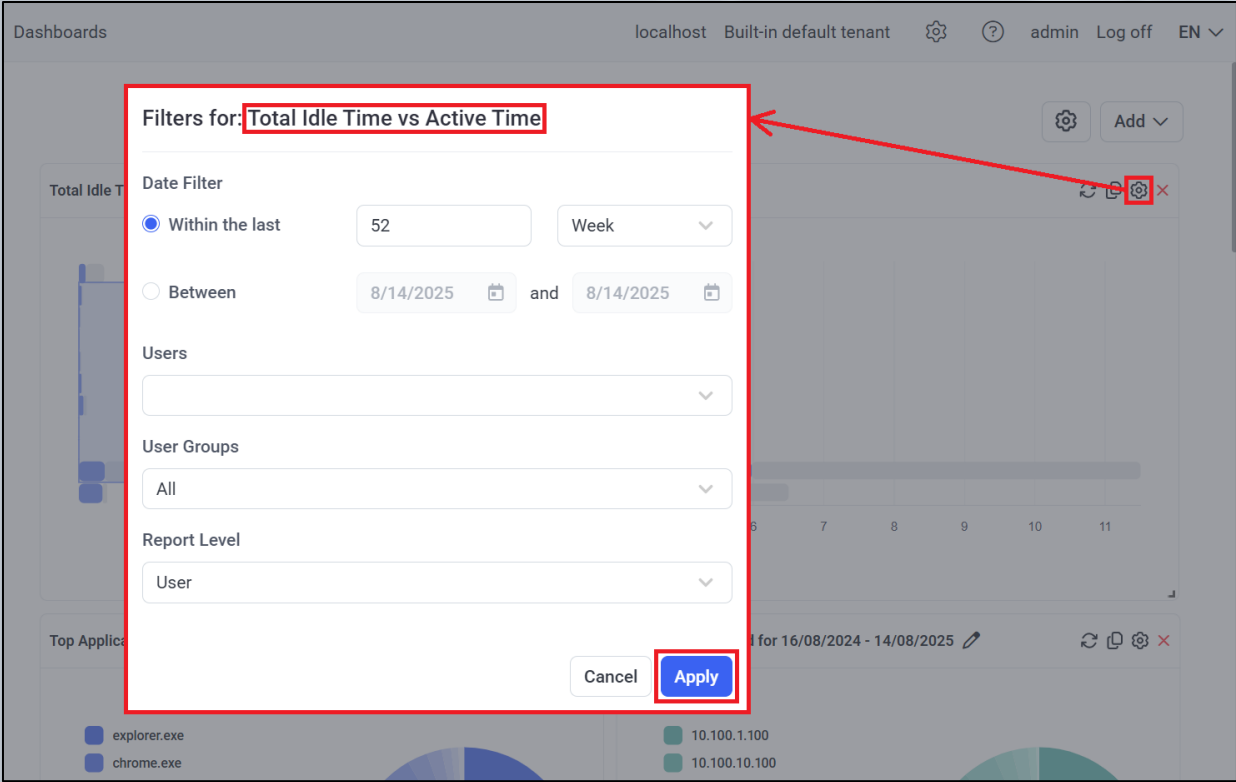


Viewing Dashboards



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

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



The screenshot shows the Syteca dashboard interface. At the top, there's a header with 'localhost Built-in default tenant' and user information 'admin Log off EN'. A modal window titled 'Filters for: Total Idle Time vs Active Time' is open, allowing customization of the dashboard. The modal includes sections for 'Date Filter' (with options 'Within the last' and 'Between'), 'Users', 'User Groups', and 'Report Level'. The 'Within the last' option is selected with a value of '52' and a unit of 'Week'. The 'Between' option shows dates '8/14/2025' and '8/14/2025'. The 'Users' section has a dropdown menu. The 'User Groups' section has a dropdown menu set to 'All'. The 'Report Level' section has a dropdown menu set to 'User'. At the bottom of the modal are 'Cancel' and 'Apply' buttons. A red box highlights the modal, and a red arrow points to the settings icon in the top right of the dashboard.

Filters for: **Total Idle Time vs Active Time**

Date Filter

☒ Within the last 52 Week

☐ Between 8/14/2025 and 8/14/2025

Users

User Groups

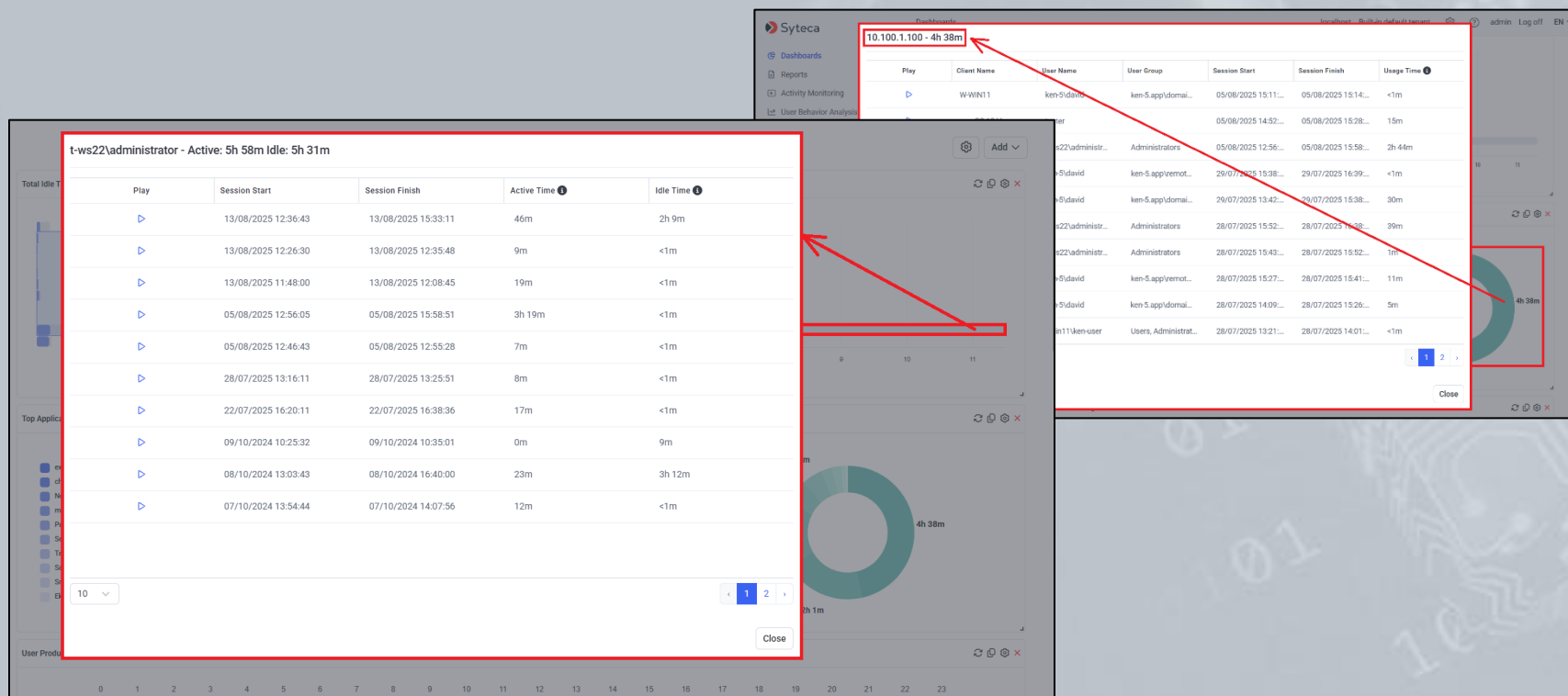
All

Report Level

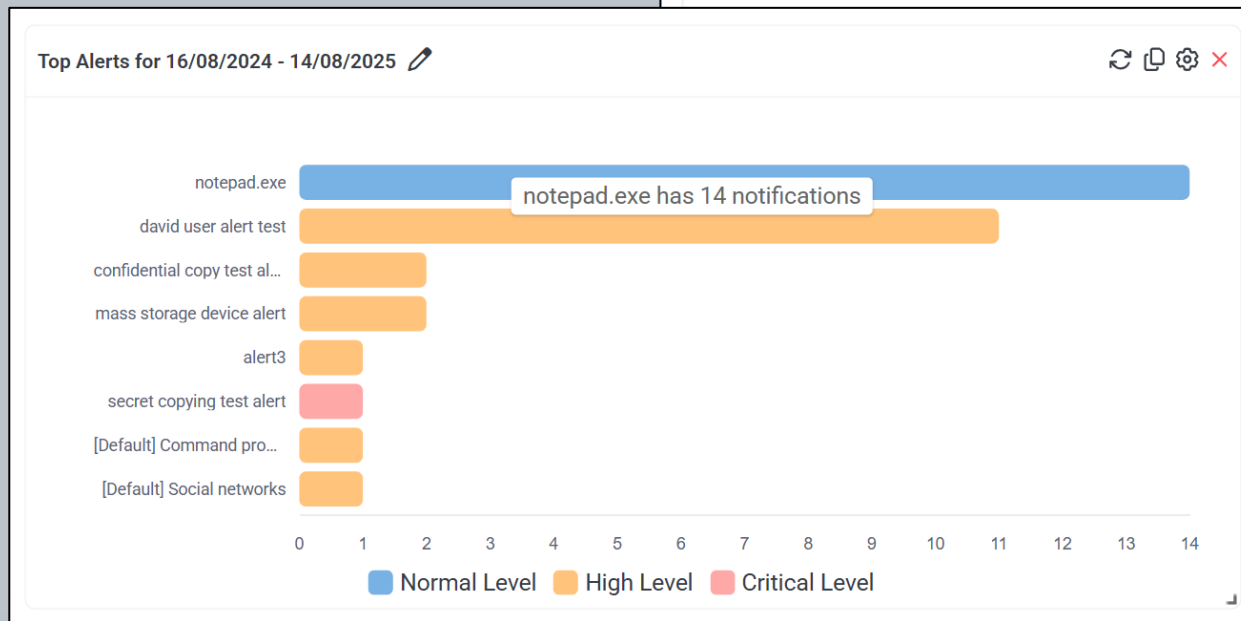
User

Cancel Apply

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**).



Top Alerts



Latest Live Sessions 

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

**Latest
Live
Sessions**

Sessions Outside of Work Hours

Rarely Used Computers

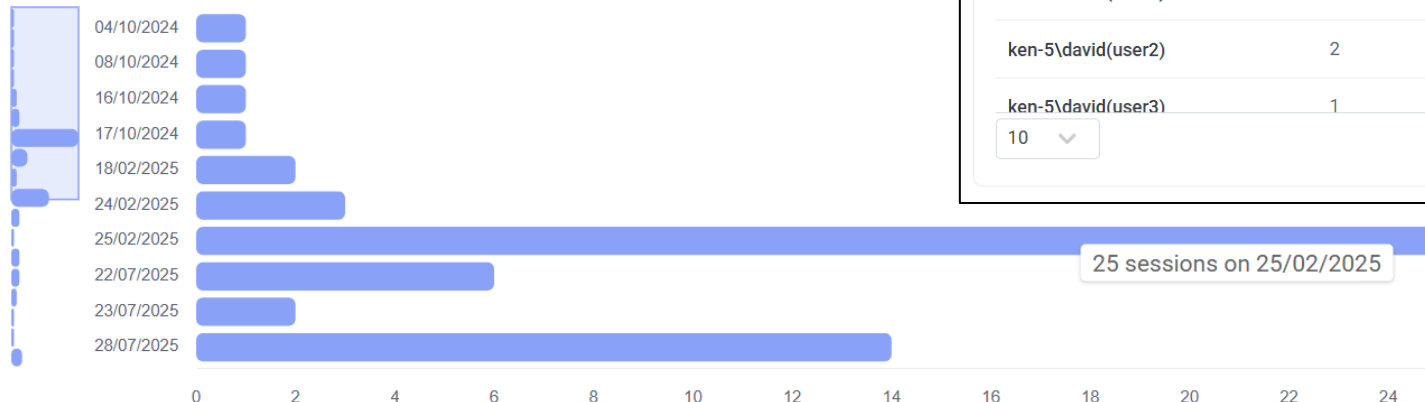
Rarely Used Logins

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



Client Name ↓	Sessions
rzone1	1
rodii-ws22	2

Sessions Outside of Work Hours for 16/08/2024 - 14/08/2025 



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

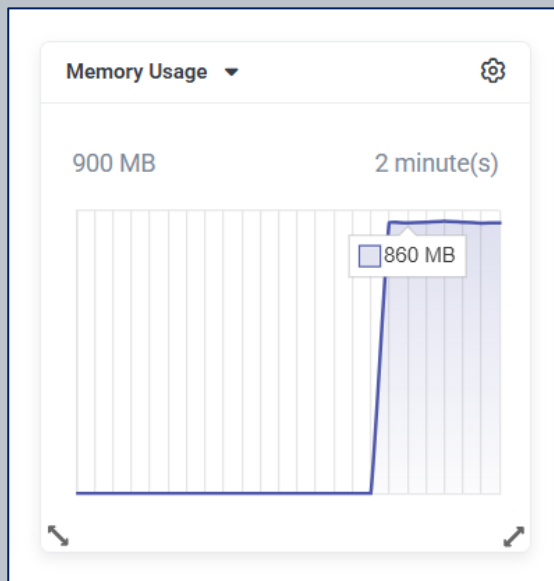


User Name ↑	Sessions
EKRAN-5\testuser2(admin)	2
T-WIN11\James	1
T-WIN11\James(admin)	1
ken-5\david(user1)	4
ken-5\david(user2)	2
ken-5\david(user3)	1

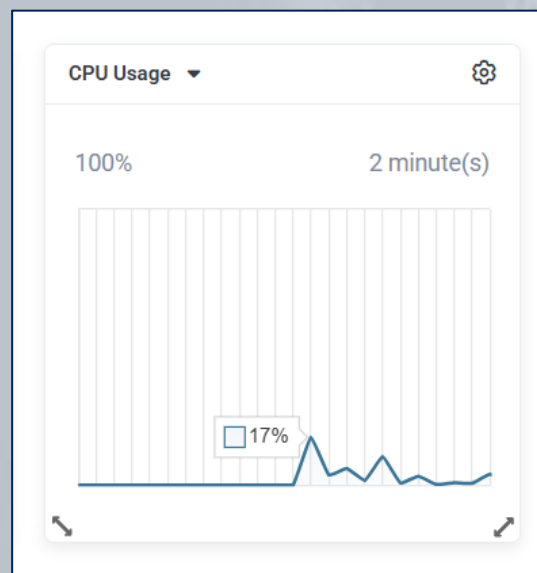
10 

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

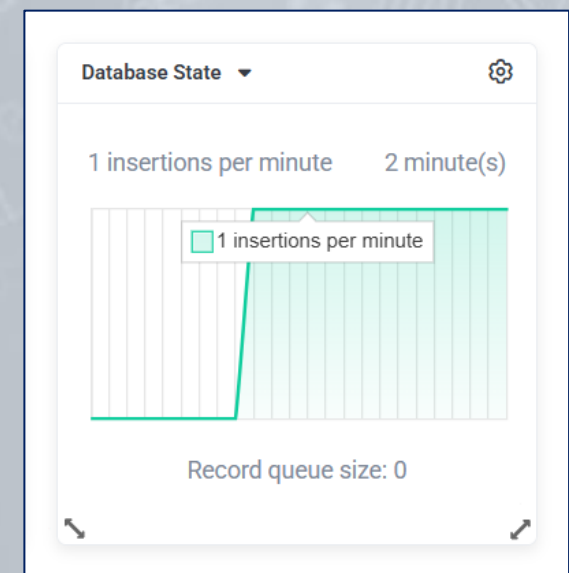
Memory Usage



CPU Usage

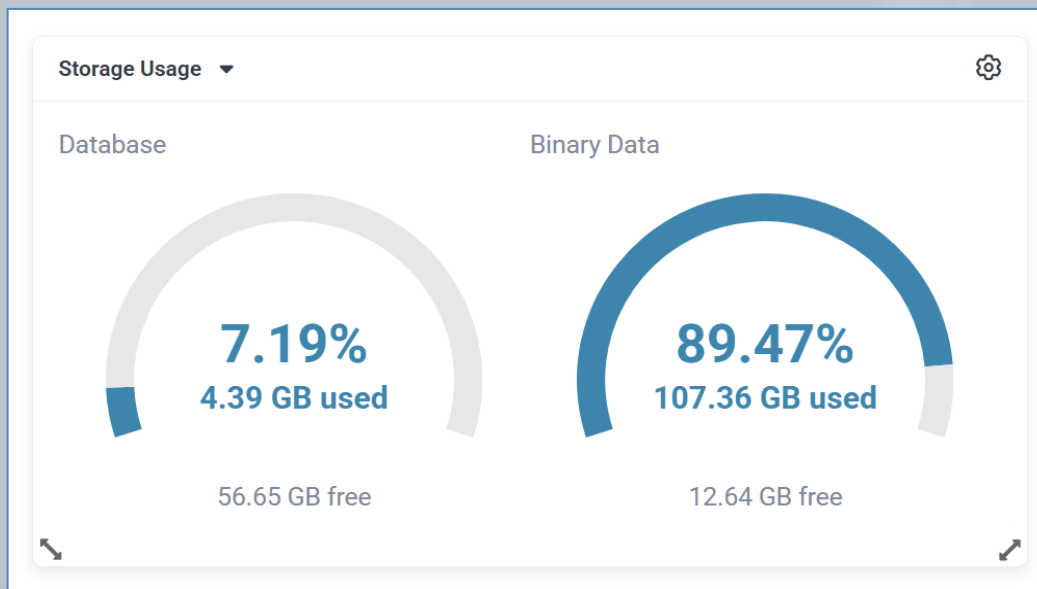


Database State

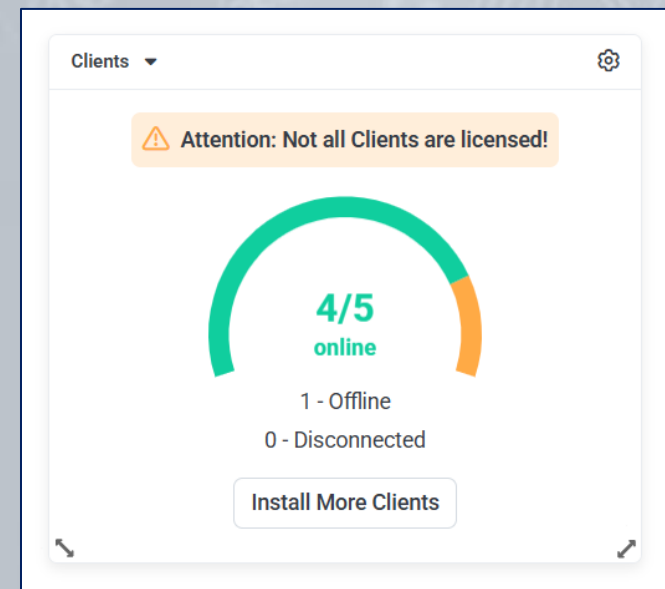


The **Storage Usage** and **Clients** dashboards (on the **System Health** page) provide information about the system state in real time.

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

Reports

localhostBuilt-in default tenant⚙️🔍adminLog offEN ▾

Report Generator

Scheduled Reports

Generated Reports

🔍 Search...

Add

Name	Description	Assigned to	Monitored Users	State	Frequency	Emails Recipients
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

- Access Request Grid
- Activity Chart
- 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

Hours + Add

8/12/2025 + Add

Generate Report

Reports

Date Filters

☒ Within the last Hours

☐ Between and

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 Any

Who Can Download Any

Generate Report

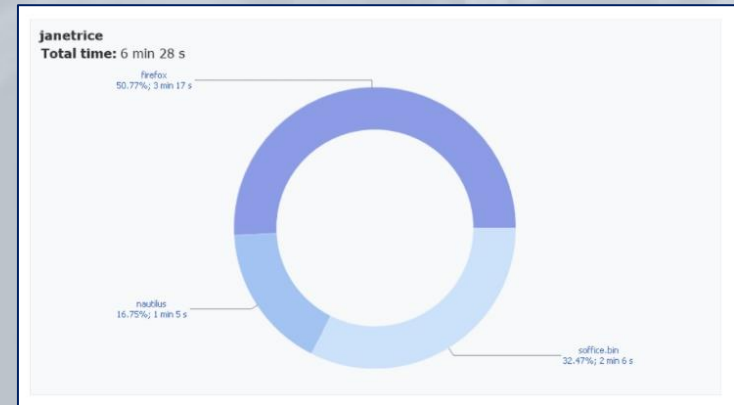
Examples of Report Types

Activity Summary Grid Report

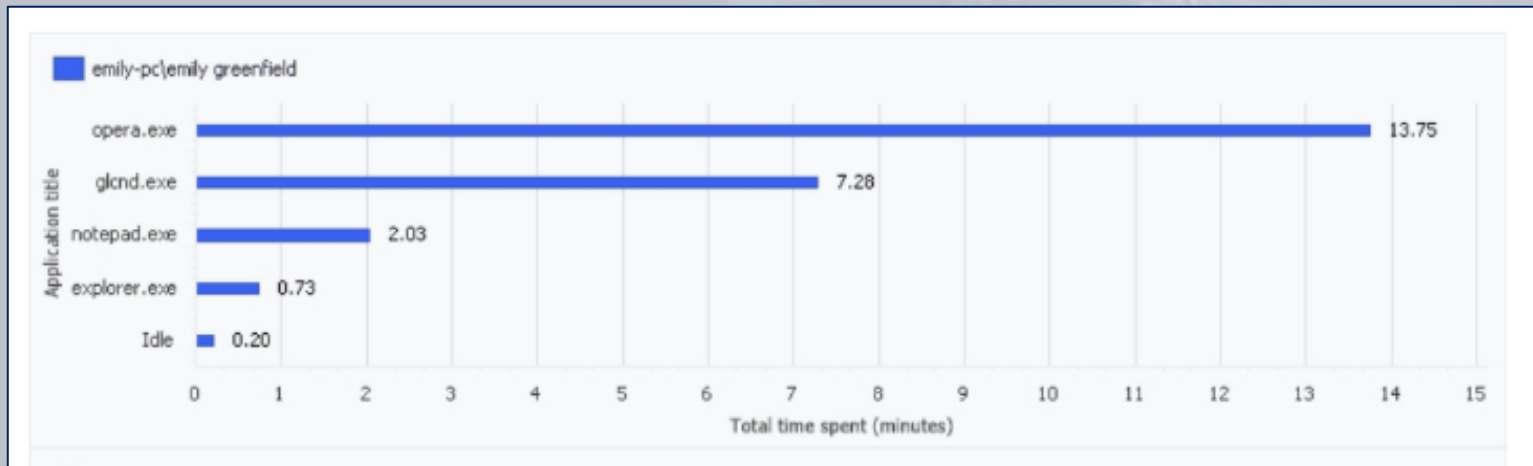
Client name	emily-pc		
Client description			
User name	emily-pc\carol looney		
Total time	24 minutes		
Active time	23 minutes, 31 seconds		

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

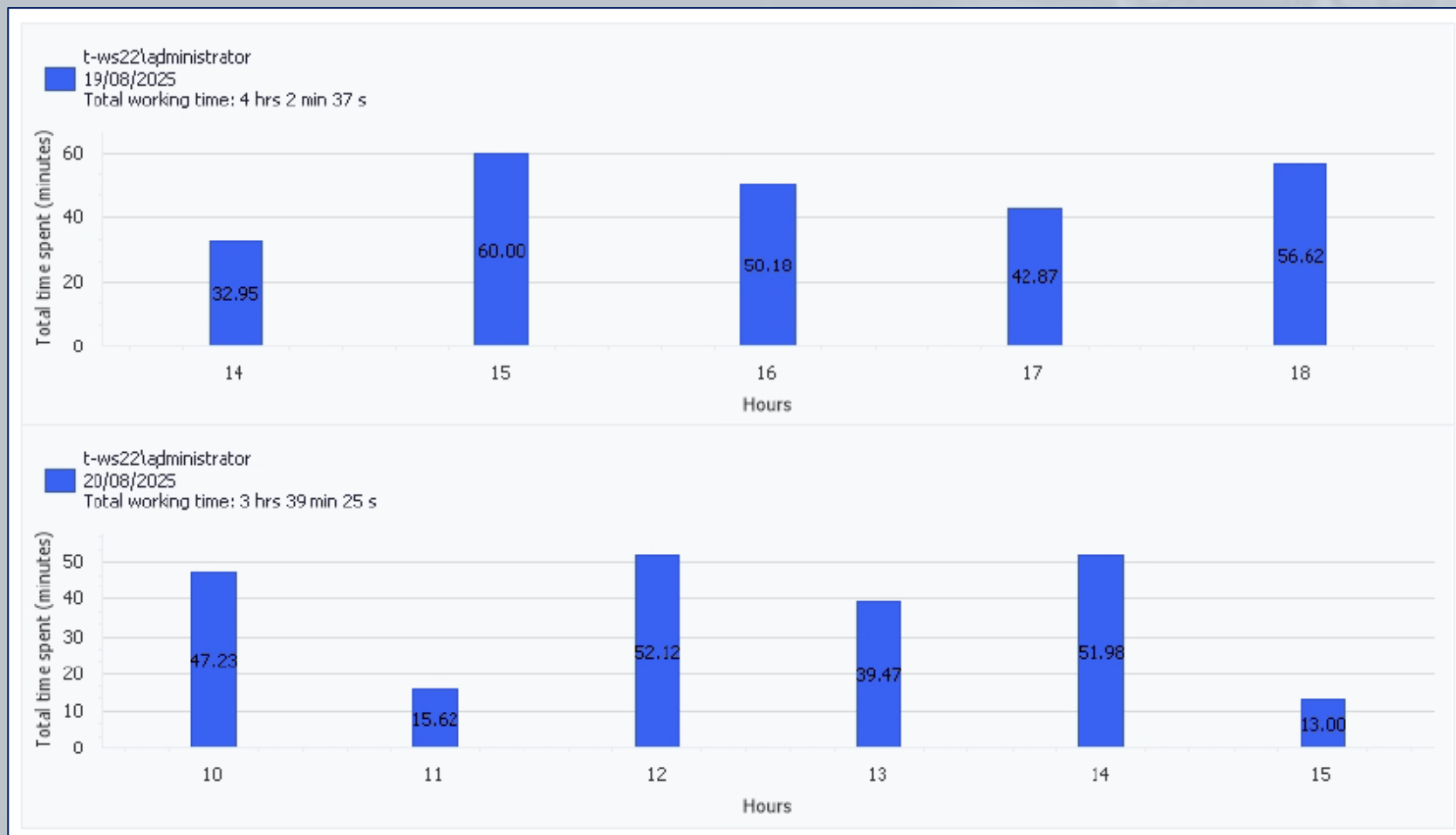
Access Requests Grid Report

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 mcreed	Endpoint Access	12/08/2023 04:43:34 PM	Denied	12/08/2023 04:57:29 PM	admin	

Sessions Outside of Work Hours Grid Report

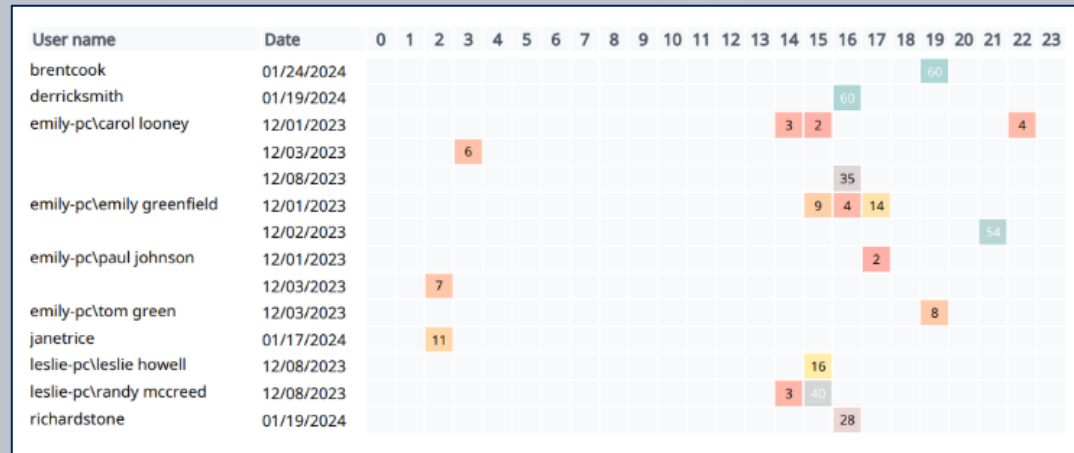
Client name	aids-Mac-mini-3.local						
Client description							
Total out of work hours	20m 32s						
User name	Total time spent	Active out of work hours	Session start time	Last activity time	Remote IP	Remote Public IP	Session URL
derricksmith	11m 23s	11m 23s	01/19/2024 04:17:43 PM	01/19/2024 04:29:06 PM	10.200.0.194	None	Open Session
richardstone	9m 9s	9m 9s	01/19/2024 04:38:16 PM	01/19/2024 04:47:25 PM	10.200.0.194	None	Open Session

User Productivity Chart Report

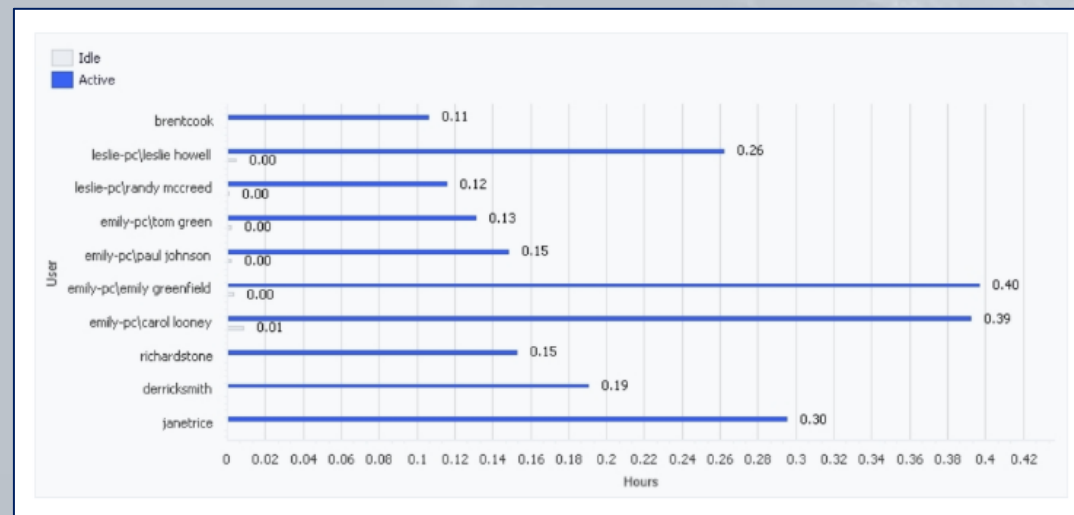


Examples of Report Types

User Productivity Heatmap Report



User Active Time and Idle Time Chart Report



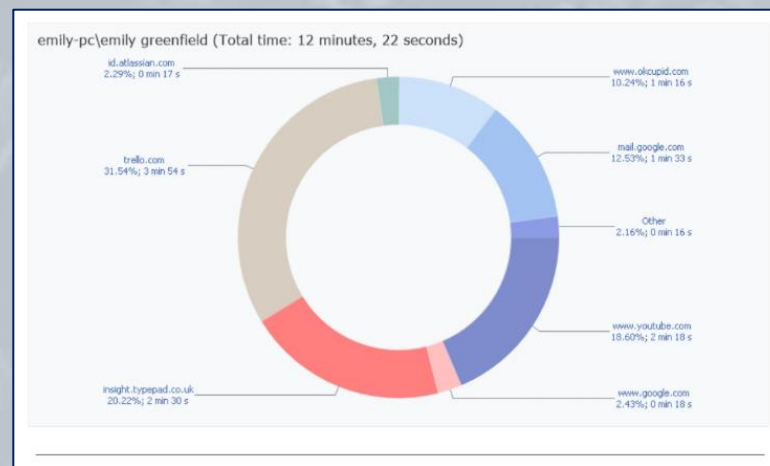
Report Types: Examples

URL Summary Grid Report

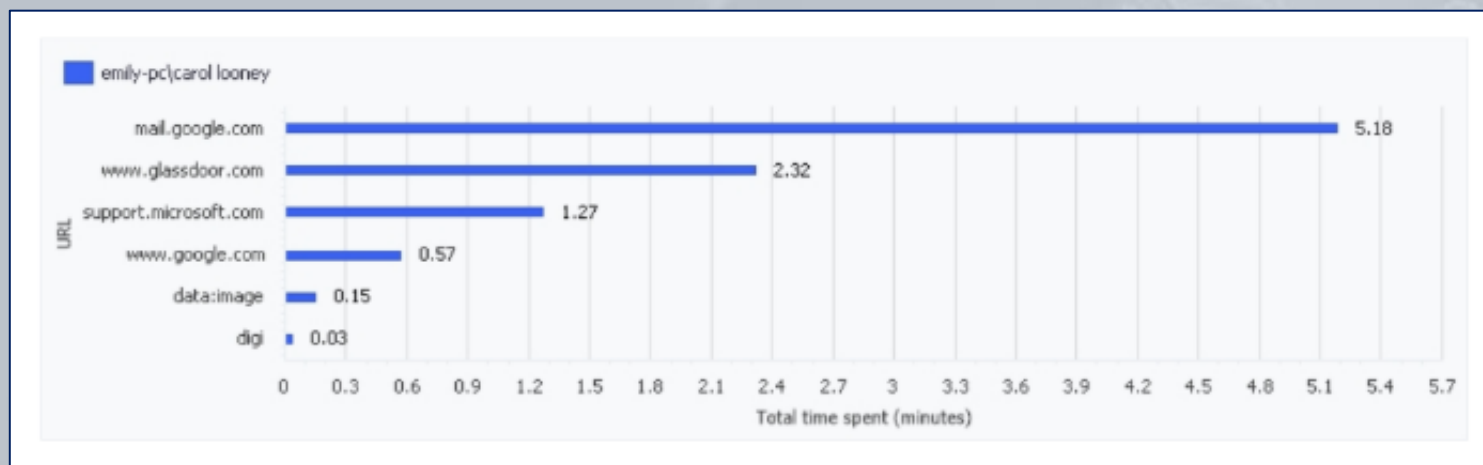
Client name	emily-pc
Client description	
User name	emily-pc\carol looney
Total time	9 minutes, 31 seconds

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

URL Pie Chart Report



URL Chart Report



Examples of Report Types

USB Storage Grid Report

Client name	emily-pc
Client description	
User name	emily-pc\carol looney
Time	Details
09/01/2023 01:49:41 AM	Connected Microphone USB
09/01/2023 01:49:41 AM	Connected Microphone USB
09/07/2023 02:02:00 PM	Connected Keyboard USB
09/07/2023 02:02:00 PM	Connected Keyboard USB
09/14/2023 12:10:15 PM	Connected Mouse USB

USB Alert Grid Report

Client name	emily-pc				
Client description					
User name	emily-pc\carol looney				
Time	Rule Name	Action	Risk Level	Device Class	Device Details
12/08/2023 04:20:31 PM		Allowed		Camera	RZR Device; RZR Device\RZR-00225002198
12/08/2023 04:20:31 PM		Blocked		Microphone	RZR Device; RZR Device\RZR-000054324321

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**).

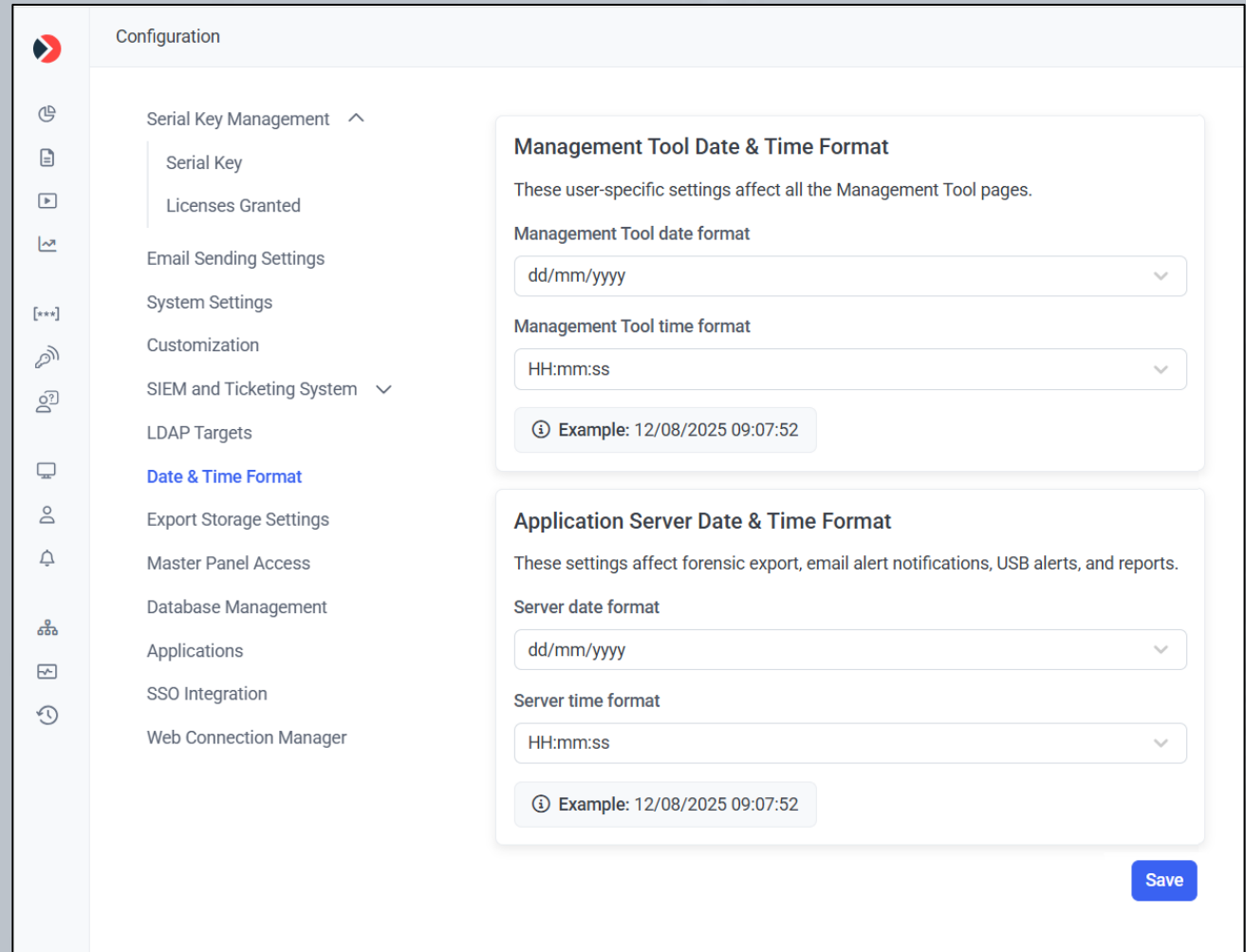
Session Viewing Status Grid Report

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

Setting the Date & Time Format

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



The screenshot displays the 'Configuration' page in the Syteca interface. On the left is a sidebar with various settings categories, including 'Serial Key Management', 'Email Sending Settings', 'System Settings', 'Customization', 'SIEM and Ticketing System', 'LDAP Targets', 'Date & Time Format' (highlighted in blue), 'Export Storage Settings', 'Master Panel Access', 'Database Management', 'Applications', 'SSO Integration', and 'Web Connection Manager'. The main content area is titled 'Configuration' and contains two sections: 'Management Tool Date & Time Format' and 'Application Server Date & Time Format'. Each section includes a description of the settings' scope and dropdown menus for selecting date and time formats. An example of the resulting format is provided for each. A 'Save' button is located at the bottom right of the configuration area.

Configuration

Serial Key Management ^

- Serial Key
- Licenses Granted

Email Sending Settings

System Settings

Customization

SIEM and Ticketing System v

LDAP Targets

Date & Time Format

Export Storage Settings

Master Panel Access

Database Management

Applications

SSO Integration

Web Connection Manager

Management Tool Date & Time Format

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

Management Tool date format

dd/mm/yyyy

Management Tool time format

HH:mm:ss

Example: 12/08/2025 09:07:52

Application Server Date & Time Format

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

Server date format

dd/mm/yyyy

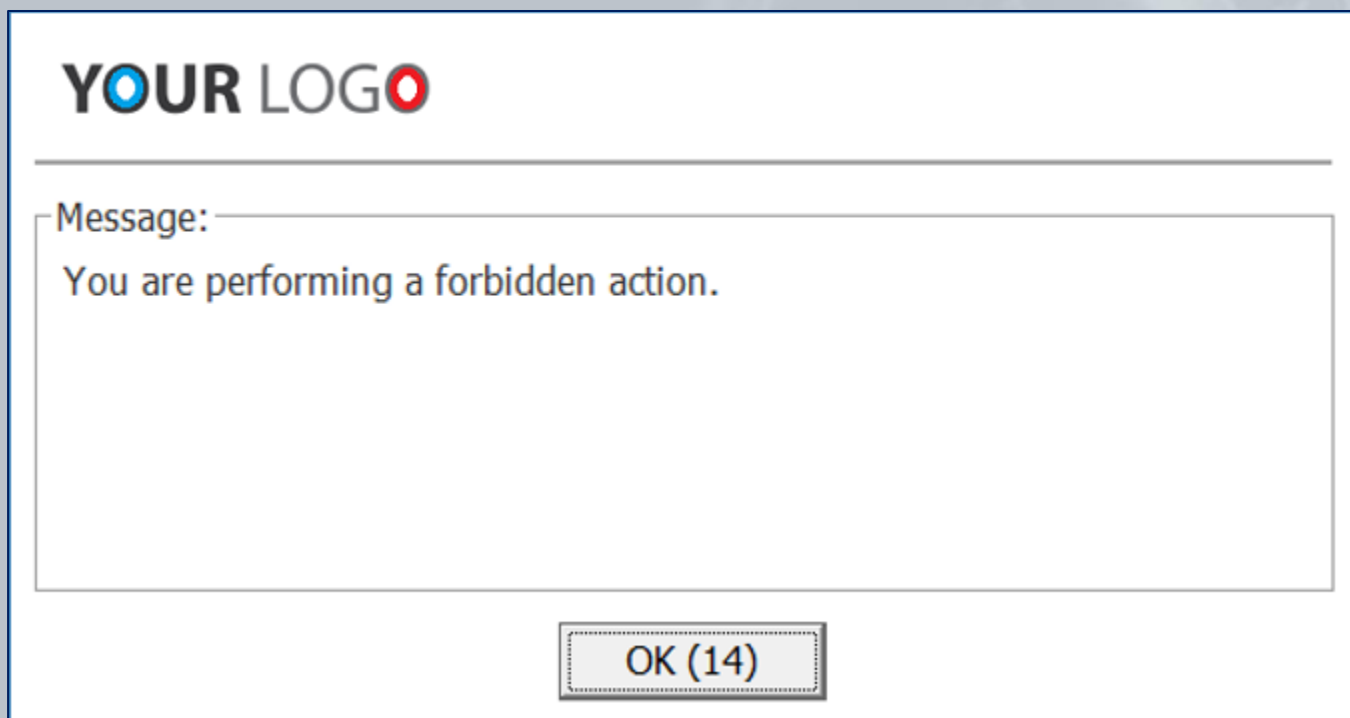
Server time format

HH:mm:ss

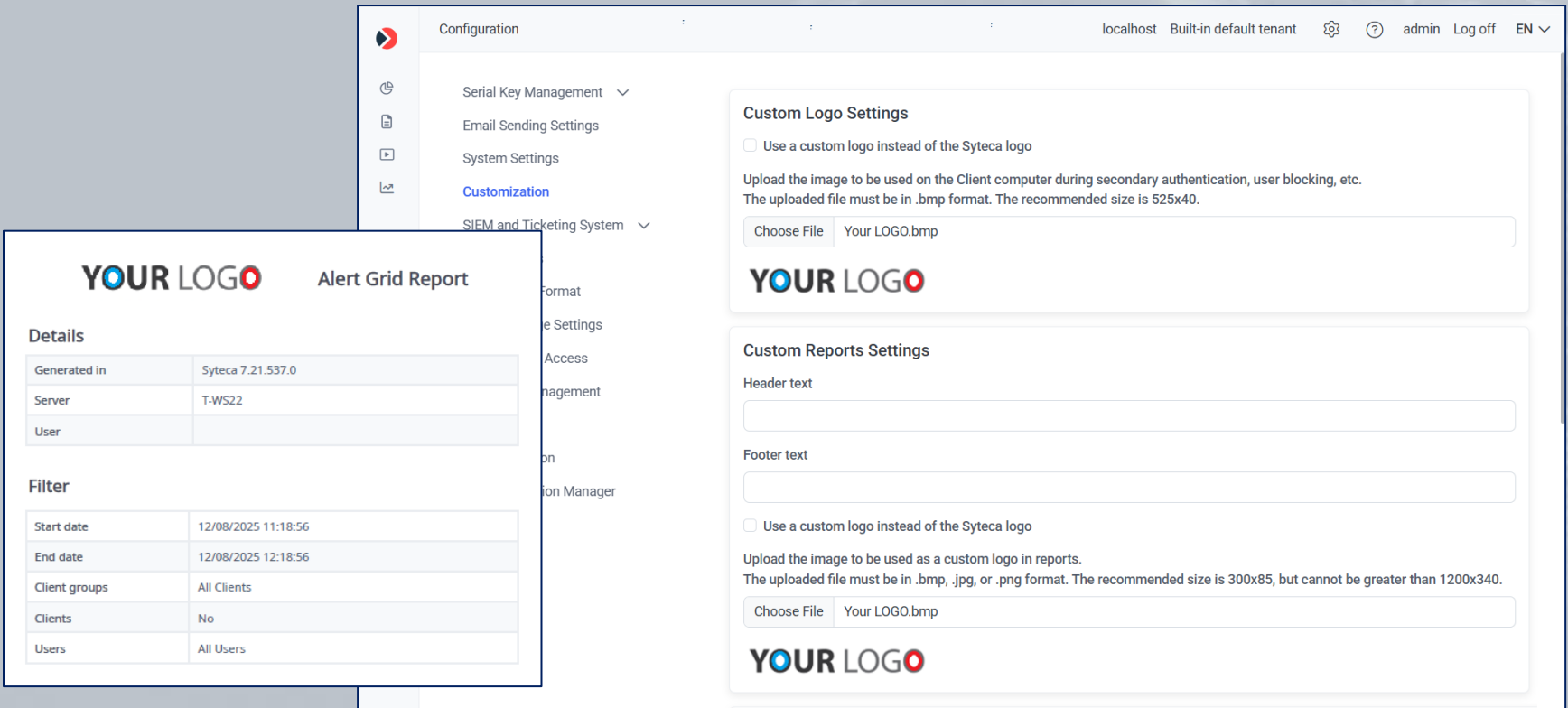
Example: 12/08/2025 09:07:52

Save

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



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 displays the Syteca Configuration interface. The left sidebar lists various settings categories, with 'Customization' selected. The main content area is divided into 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
- Footer text
- ☐ 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 (Alert Grid Report)

YOUR LOGO Alert Grid Report

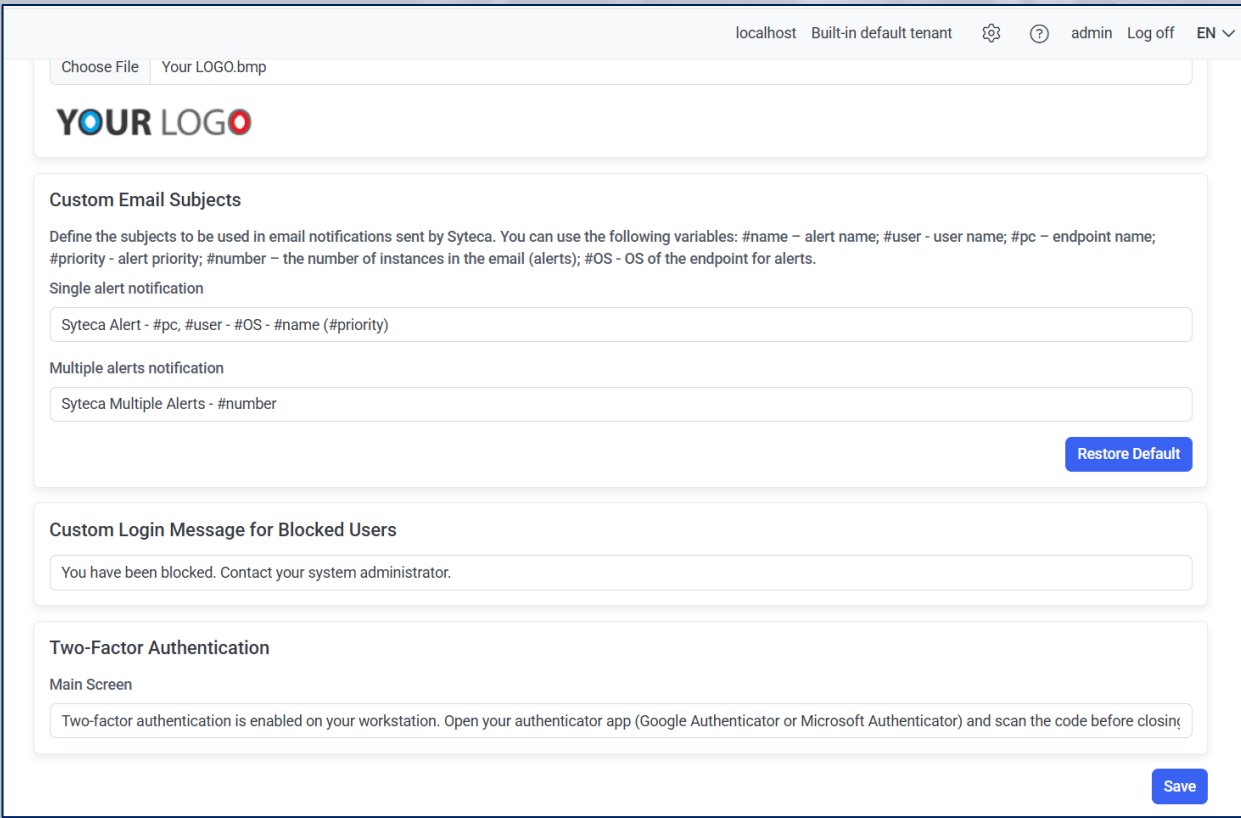
Details

Generated in	Syteca 7.21.537.0
Server	T-WS22
User	

Filter

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

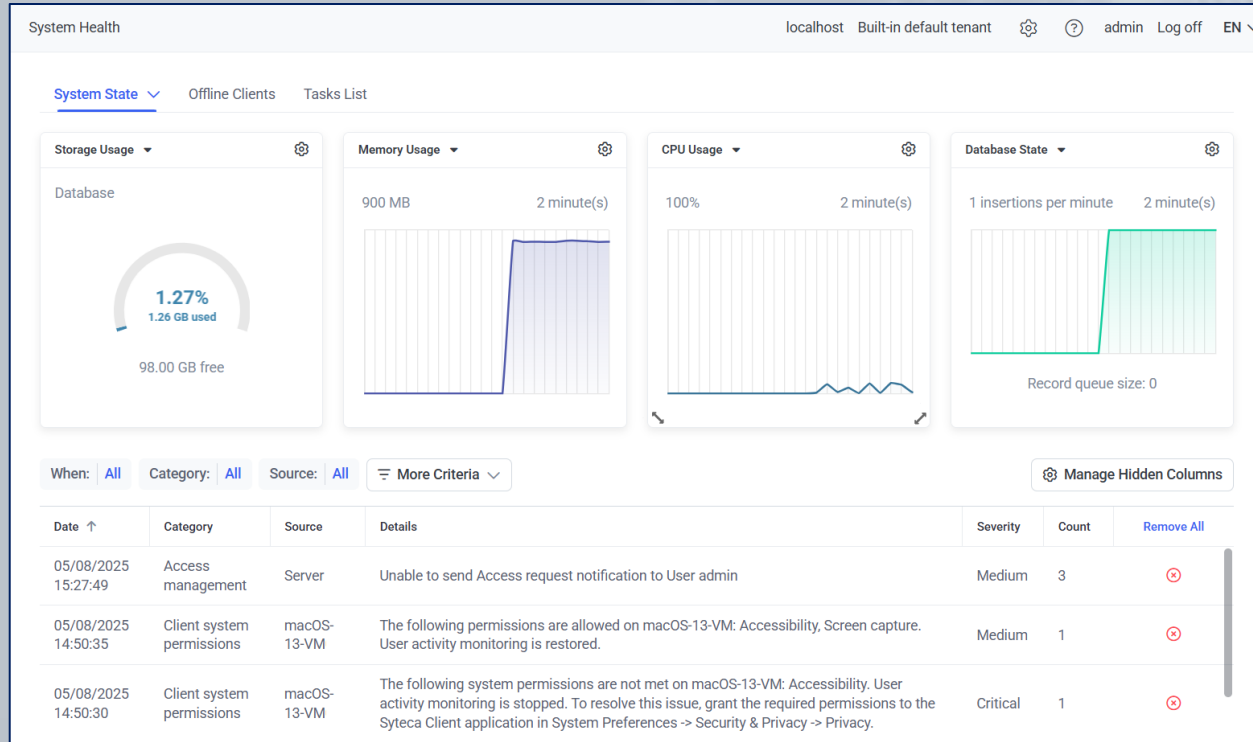
Custom settings allow you to **specify** the **subjects** to be used in **email notifications**, and other various messages, sent by Syteca.



The screenshot shows the Syteca configuration interface. At the top right, there is a navigation bar with the text "localhost Built-in default tenant" followed by icons for settings and help, and the text "admin Log off EN". Below this, there is a "Choose File" button and a text input field containing "Your LOGO.bmp". The main content area is divided into sections. The first section is titled "YOUR LOGO" and contains a placeholder for a logo. The second section is titled "Custom Email Subjects" and contains a description: "Define the subjects to be used in email notifications sent by Syteca. You can use the following variables: #name - alert name; #user - user name; #pc - endpoint name; #priority - alert priority; #number - the number of instances in the email (alerts); #OS - OS of the endpoint for alerts." Below this, there are two sub-sections: "Single alert notification" and "Multiple alerts notification". The "Single alert notification" section has a text input field containing "Syteca Alert - #pc, #user - #OS - #name (#priority)". The "Multiple alerts notification" section has a text input field containing "Syteca Multiple Alerts - #number". To the right of the "Multiple alerts notification" section is a blue button labeled "Restore Default". The third section is titled "Custom Login Message for Blocked Users" and has a text input field containing "You have been blocked. Contact your system administrator." The fourth section is titled "Two-Factor Authentication" and has a sub-section "Main Screen" with a text input field containing "Two-factor authentication is enabled on your workstation. Open your authenticator app (Google Authenticator or Microsoft Authenticator) and scan the code before closing". To the right of the "Main Screen" section is a blue button labeled "Save".

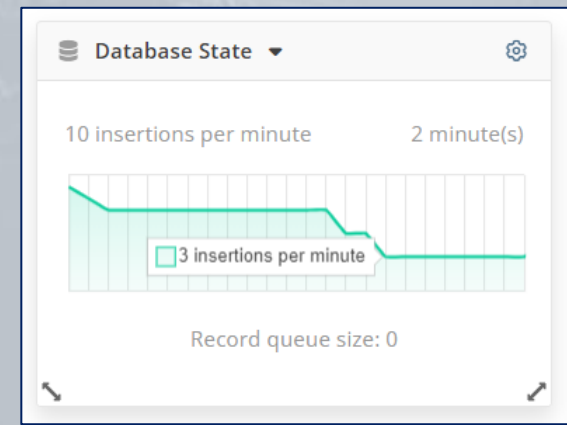
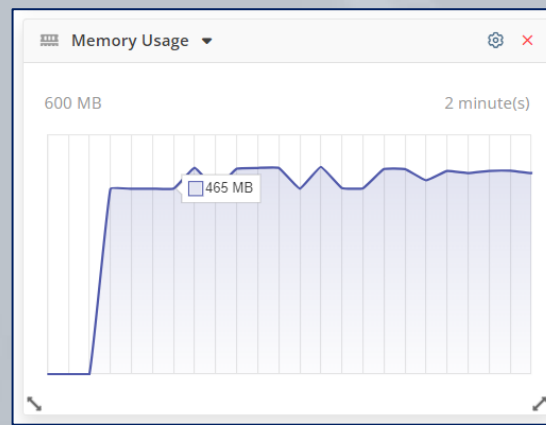
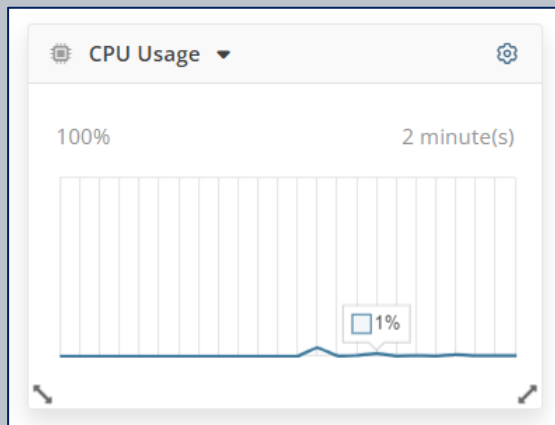
System Health Monitoring

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.



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).

System Health

localhost Built-in default tenant

admin

Log off

EN

System State

Offline Clients

Tasks List

Task Name

All

Node

All

Status

All

Q

Search...

☐	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.

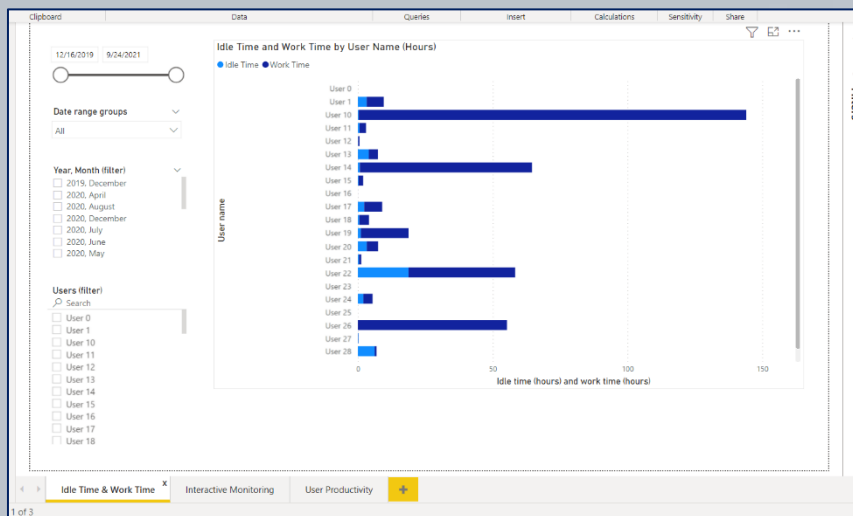
This application is designed to **allow customers to get Syteca monitoring data** via the API in order to **use for their own business purposes**.

Idle Time & Work Time Report

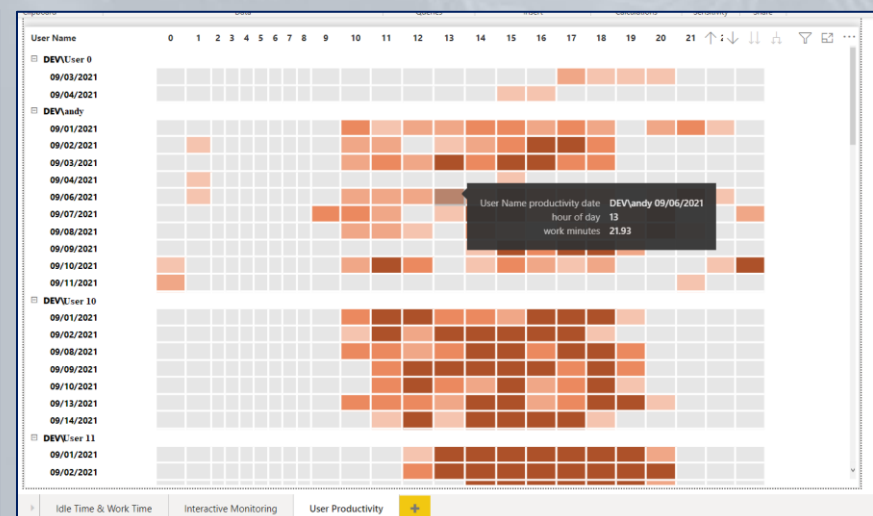


For example, **Client session records** containing **user productivity data** (such as **productivity time, idle time, duration**, etc.) can be used to build BI (business intelligence) reports in **Microsoft Power BI**.

Interactive Monitoring Report

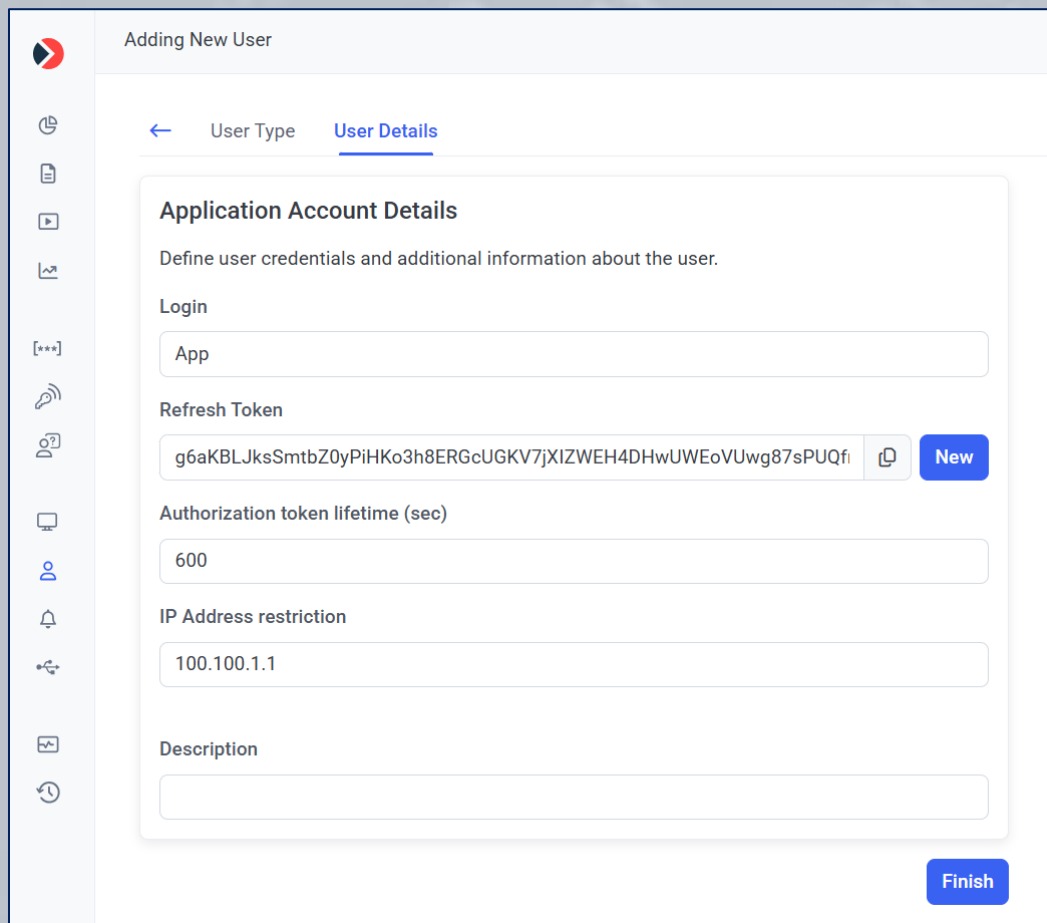


User Productivity Report



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 Syteca secrets' data via the ACB API**, to use it for their own business purposes.



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

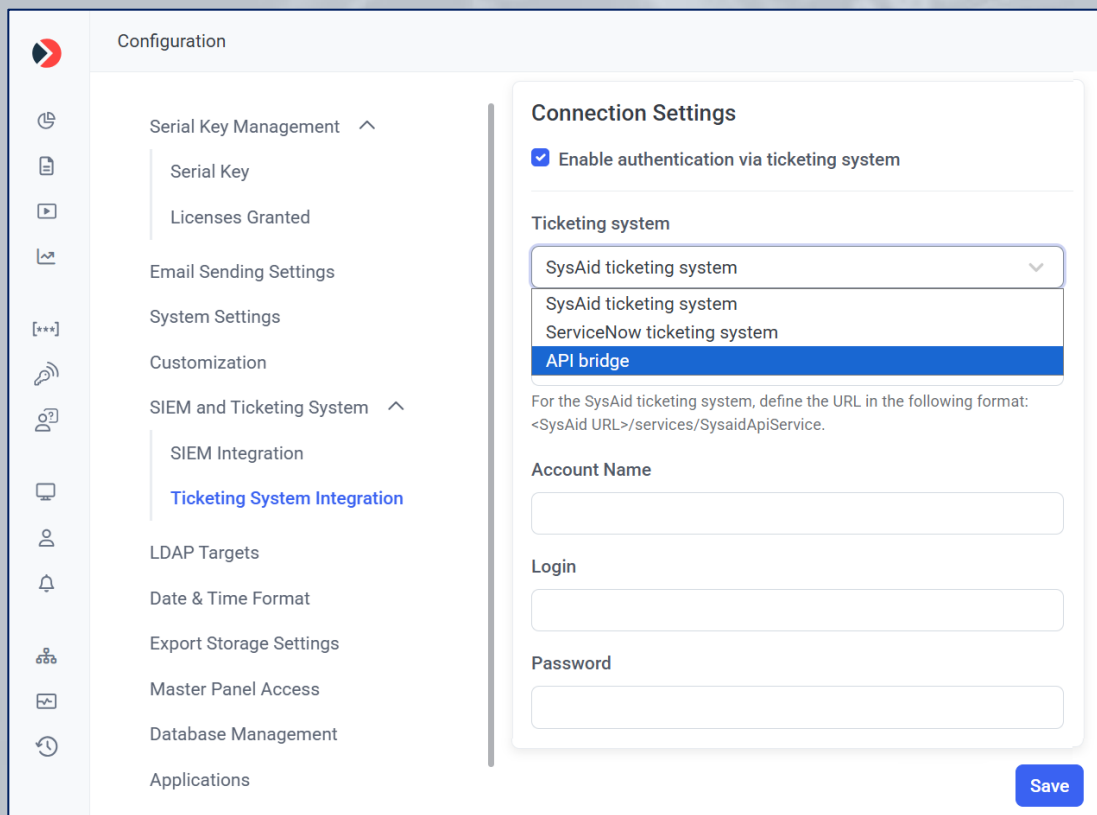
100.100.1.1

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 displays the 'Configuration' page of the Syteca API Bridge. The left sidebar contains a navigation menu with icons for various settings. The main content area is titled 'Configuration' and lists several categories: Serial Key Management, Email Sending Settings, System Settings, Customization, SIEM and Ticketing System, LDAP Targets, Date & Time Format, Export Storage Settings, Master Panel Access, Database Management, and Applications. Under 'SIEM and Ticketing System', the 'Ticketing System Integration' option is highlighted. The right panel shows the 'Connection Settings' for the selected system. It includes a checkbox to 'Enable authentication via ticketing system', which is checked. Below this, a dropdown menu for 'Ticketing system' is open, showing options: 'SysAid ticketing system', 'ServiceNow ticketing system', and 'API bridge'. The 'API bridge' option is selected. A note below the dropdown states: 'For the SysAid ticketing system, define the URL in the following format: <SysAid URL>/services/SysaidApiService.' Below the note are input fields for 'Account Name', 'Login', and 'Password'. A 'Save' button is located at the bottom right of the settings panel.

Configuration

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

Connection Settings

☒ Enable authentication via ticketing system

Ticketing system

SysAid ticketing system

SysAid ticketing system

ServiceNow ticketing system

API bridge

For the SysAid ticketing system, define the URL in the following format:
<SysAid URL>/services/SysaidApiService.

Account Name

Login

Password

Save

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 Venn app launcher interface. The main content area shows a video player with the title "Remote Work Security for Any Employee Workspace - Venn(Google Chrome) - 13/08/2024 14:20:02". The video player shows a webpage for Venn, titled "The Secure Workspace for Remote Work", which describes Venn's secure remote work solution. Below the video player, there is a "Details" section showing the URL: "venn.com".

On the right side of the interface, there is a table listing activities. The table has columns for "ACT...", "ACTIVI...", "AP...", "URL", "TEX...", and "ALE...". The table contains a list of activities, including "New Tab", "Launch | wor...", "Remote Work ...", and "Google Chrome". The table is filtered to show 500 items.

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 ...		
>	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.

The image shows a screenshot of the Syteca Configuration page. On the left, there is a login overlay with the Syteca logo and the text "One platform to secure your inside perimeter". Below this, it says "Log in to your account". There are fields for "Login" and "Password", a "Remember me on this computer" checkbox, and a "Log in" button. A "Log in with SSO" button is highlighted with a red box. At the bottom of the overlay, it says "Having trouble logging in? [Contact support](#)".

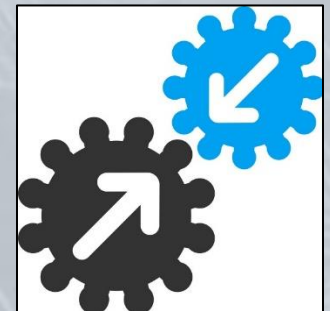
The main configuration page is titled "Configuration" and has a sidebar with options like "Management", "Settings", "Integration System", "System Integration", "Format", "Settings", "Access", and "Management". The "SSO Integration" section is active, showing the following fields:

- Issuer name:**
- Identity provider metadata (xml):** No file chosen
- Certificate type:** ☐ Self-signed certificate, ☒ Custom certificate
- Certificate (pfx):** No file chosen
- Certificate password:**
- Auto-create a Management Tool account for a new user on the first SSO login:** ☒

A "Save" button is located at the bottom right of the SSO Integration section.

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

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



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

For More Information...



Visit us online:
www.syteca.com