



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](#)
- [Pseudonymizer \(for e.g. GDPR Compliance\)](#)
- [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 **control** the use of **sensitive information**?

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.

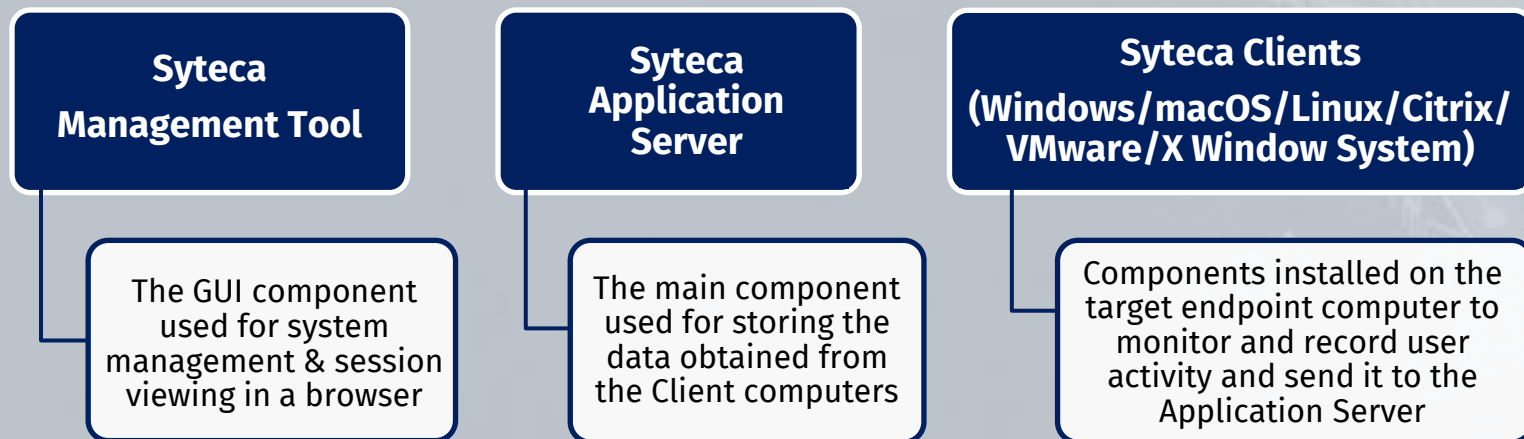
Flexible Deployment and Licensing

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.

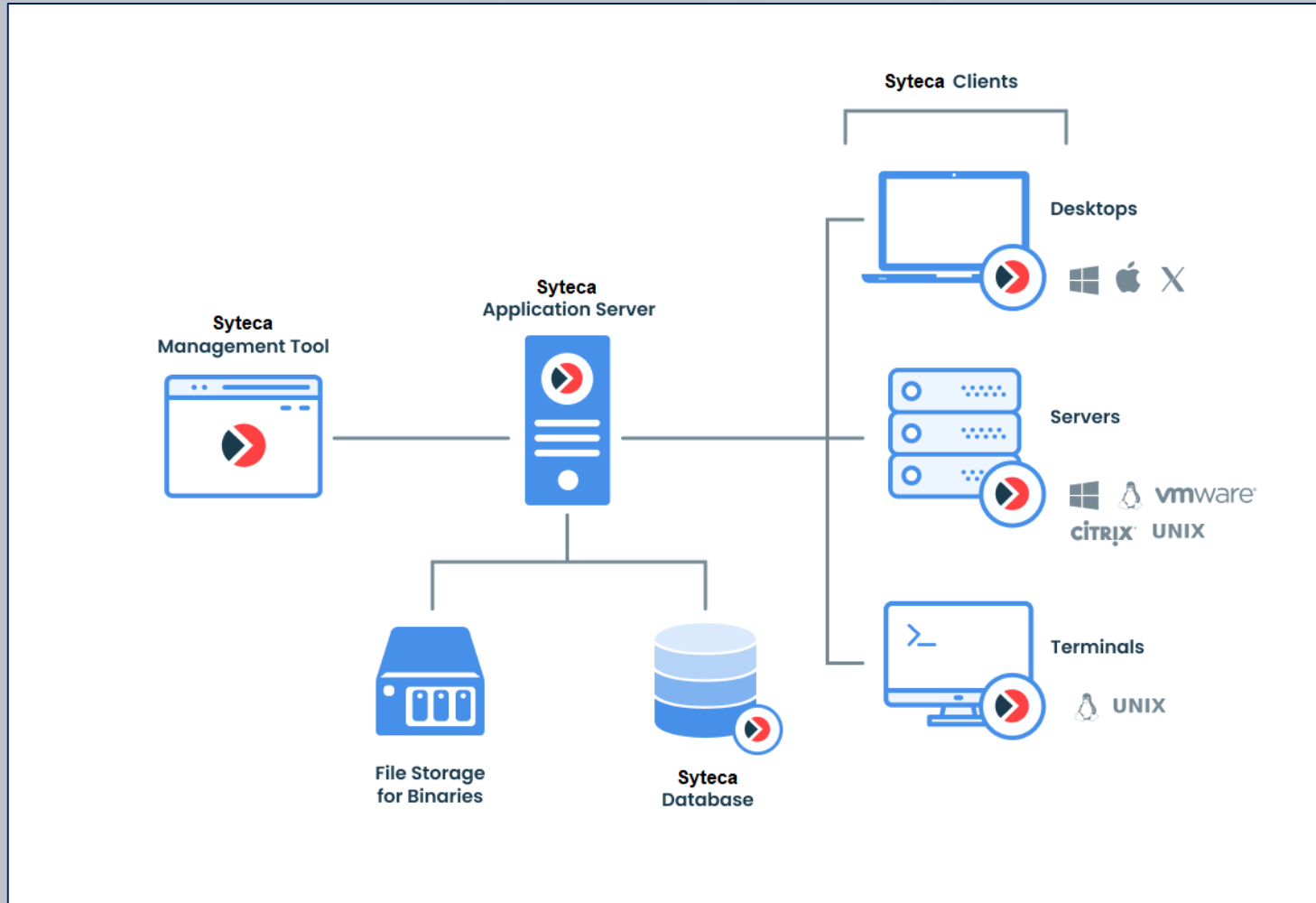
Syteca (formerly **Ekrans System**) is an enterprise-level **cybersecurity platform** software solution featuring **privileged access management (PAM)** and **user activity monitoring (UAM)**. It is used to **protect** your corporate IT infrastructure from **internal risks**, as well as to assist you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

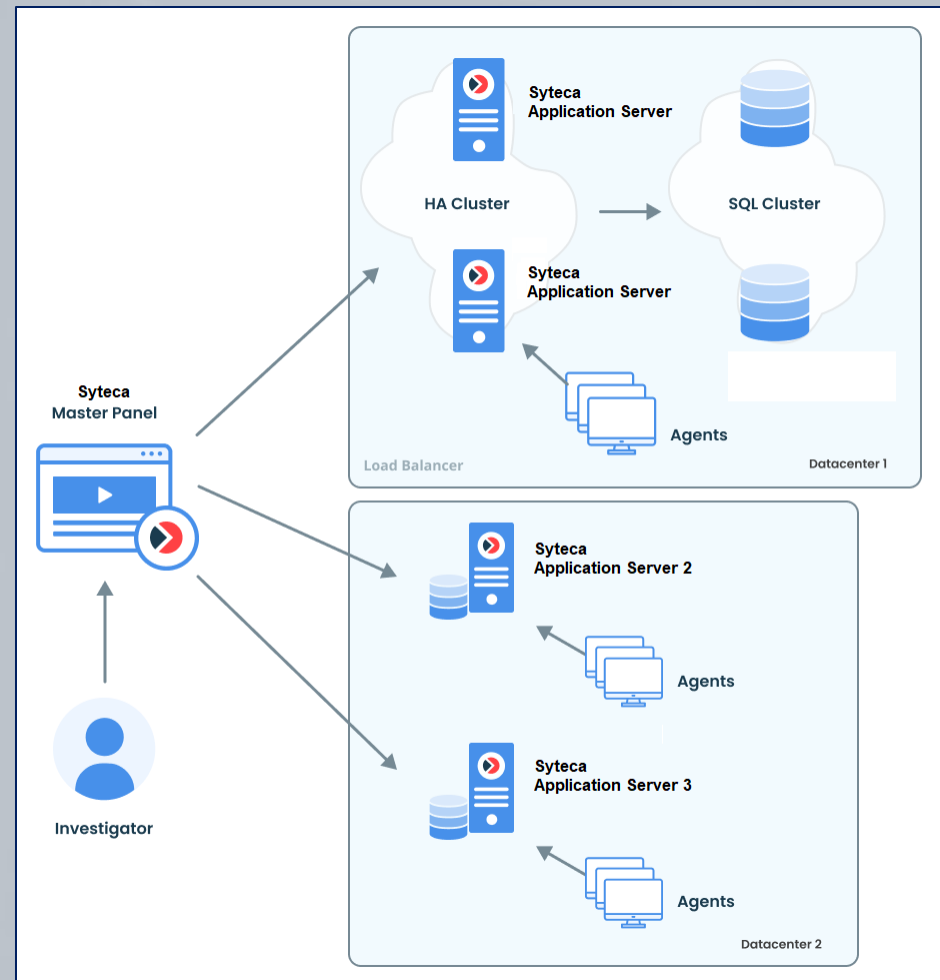


Large-Scale Deployments

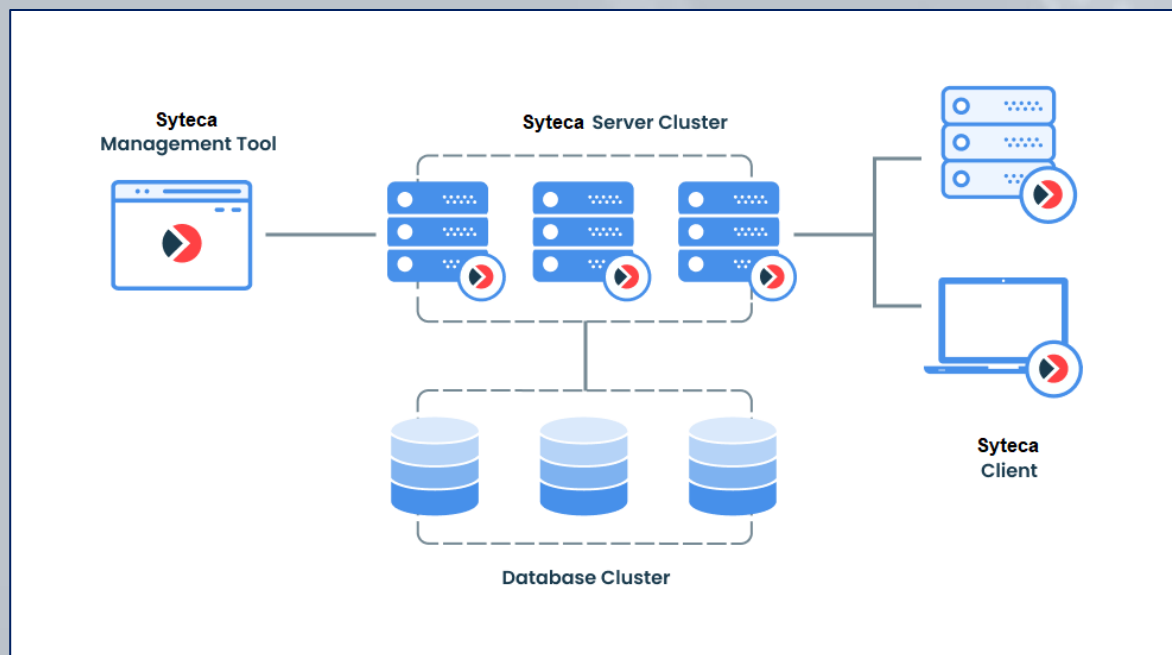
In terms of scalability, and for large organizations which may have several geographically isolated data centers, **multiple connected** instances of the **Application Server** can be deployed.

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.

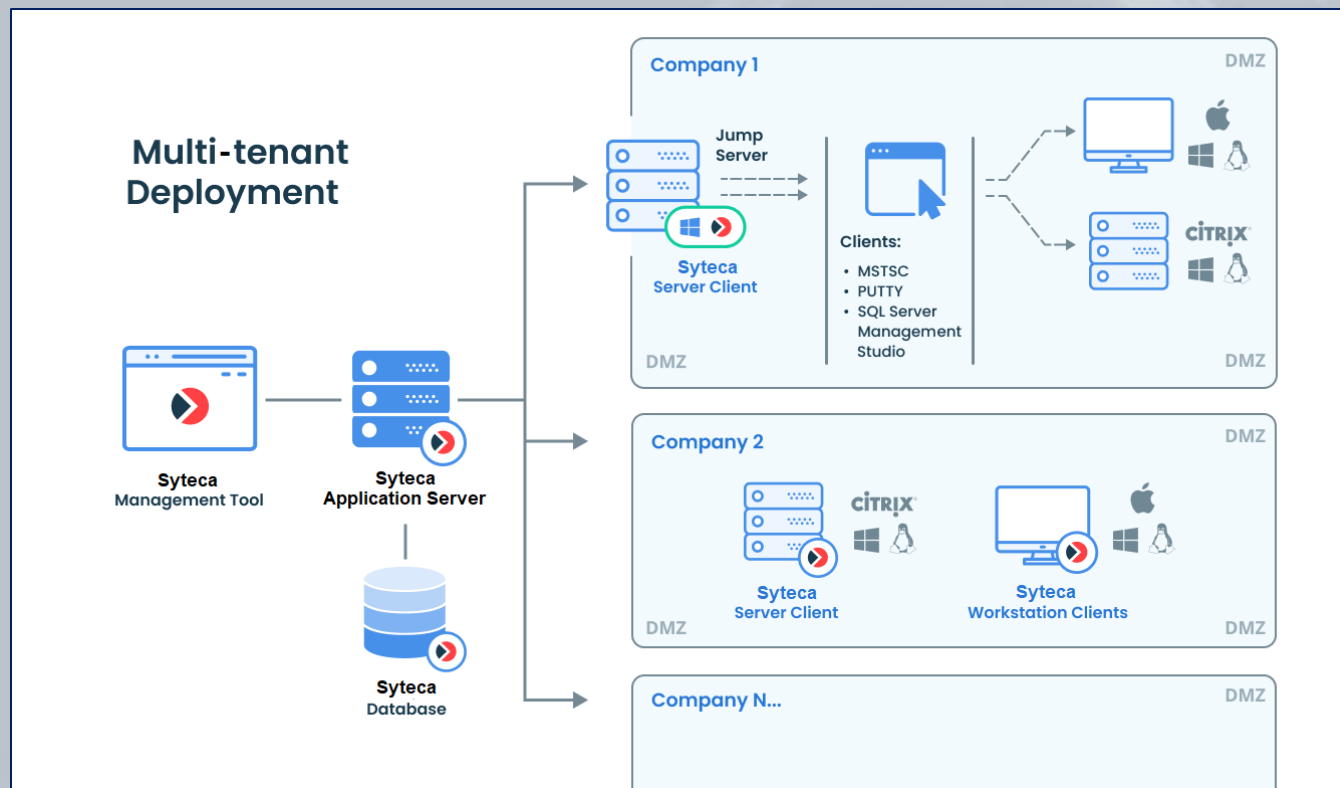
The **Master Panel**, which is an additional stand-alone component of Syteca, **combines the data** recorded by all Syteca Applications Servers in multiple locations, allowing the data to be **viewed and managed in a single user interface**.



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**.



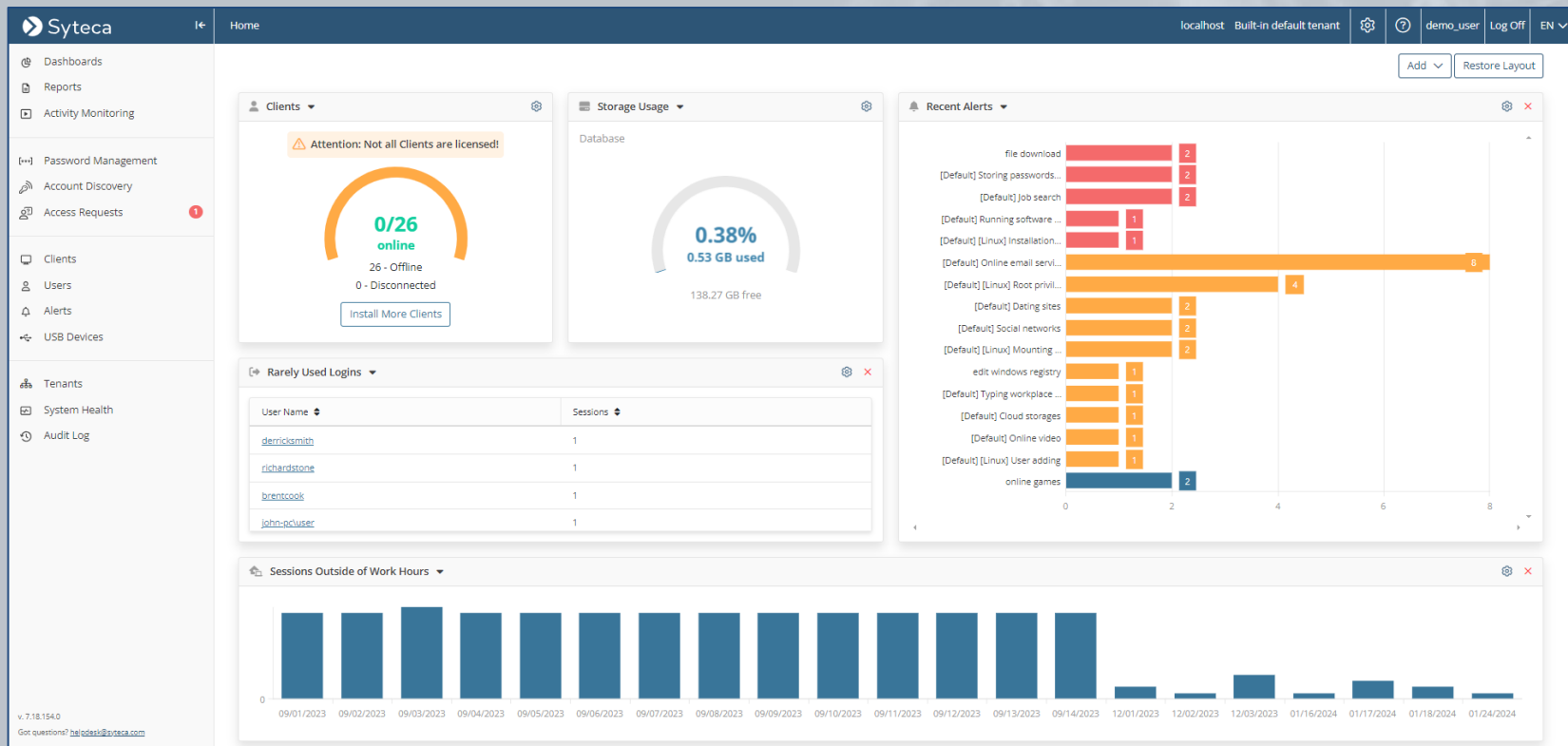
Multi-Tenant mode allows **multiple** completely **isolated tenants** to operate in the Syteca environment. The **data** in each tenant is **independent** and not accessible to other tenants.



Syteca Application Server & the Management Tool

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

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

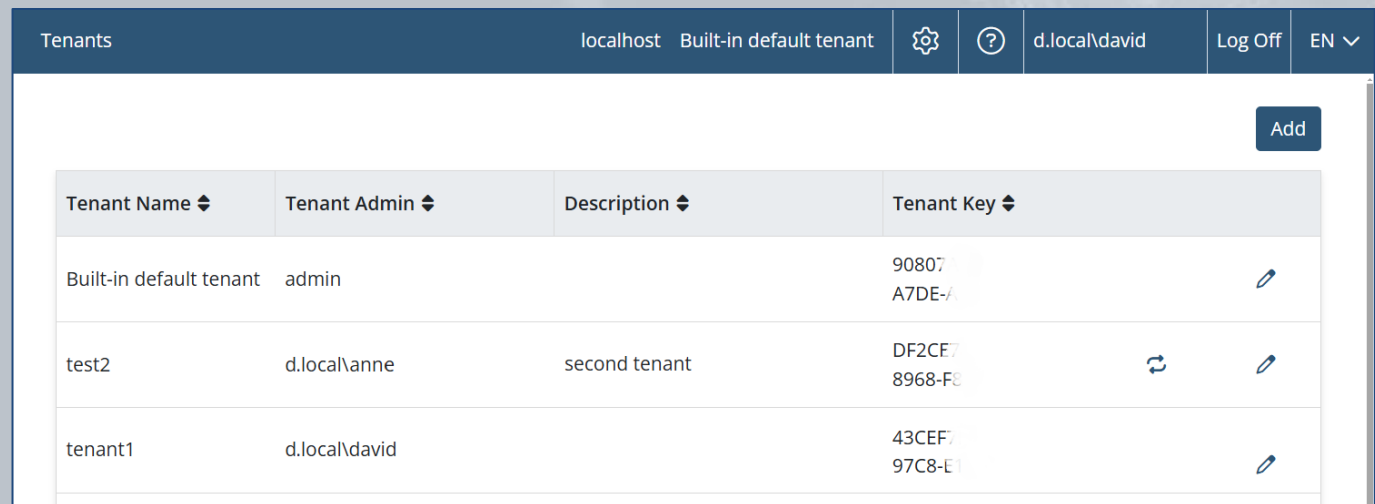


Syteca can operate in Single-Tenant or **Multi-Tenant mode**.





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.

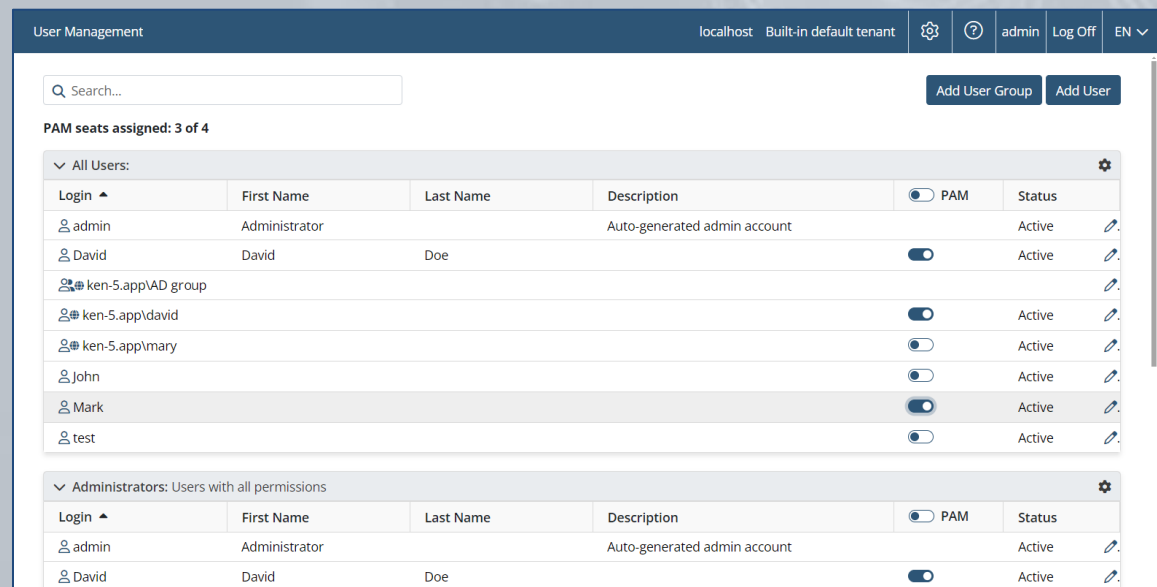
You can **switch** to Multi-Tenant mode **at any time**.



The screenshot shows the 'Tenants' management page in the Syteca interface. The top navigation bar includes the 'Tenants' title, a dropdown for 'localhost', a dropdown for 'Built-in default tenant', a settings gear icon, a help icon, a user profile 'd.local\david', a 'Log Off' button, and a language dropdown 'EN'. An 'Add' button is located in the top right corner of the table area. The table has four columns: 'Tenant Name', 'Tenant Admin', 'Description', and 'Tenant Key'. It lists three tenants: 'Built-in default tenant' (admin), 'test2' (d.local\anne), and 'tenant1' (d.local\david). Each row has an edit icon in the 'Tenant Key' column. The 'test2' row also features a refresh icon.

Tenant Name	Tenant Admin	Description	Tenant Key
Built-in default tenant	admin		90807A7DE- A7DE- 
test2	d.local\anne	second tenant	DF2CE78968-F8  
tenant1	d.local\david		43CE797C8-E1 

- 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).



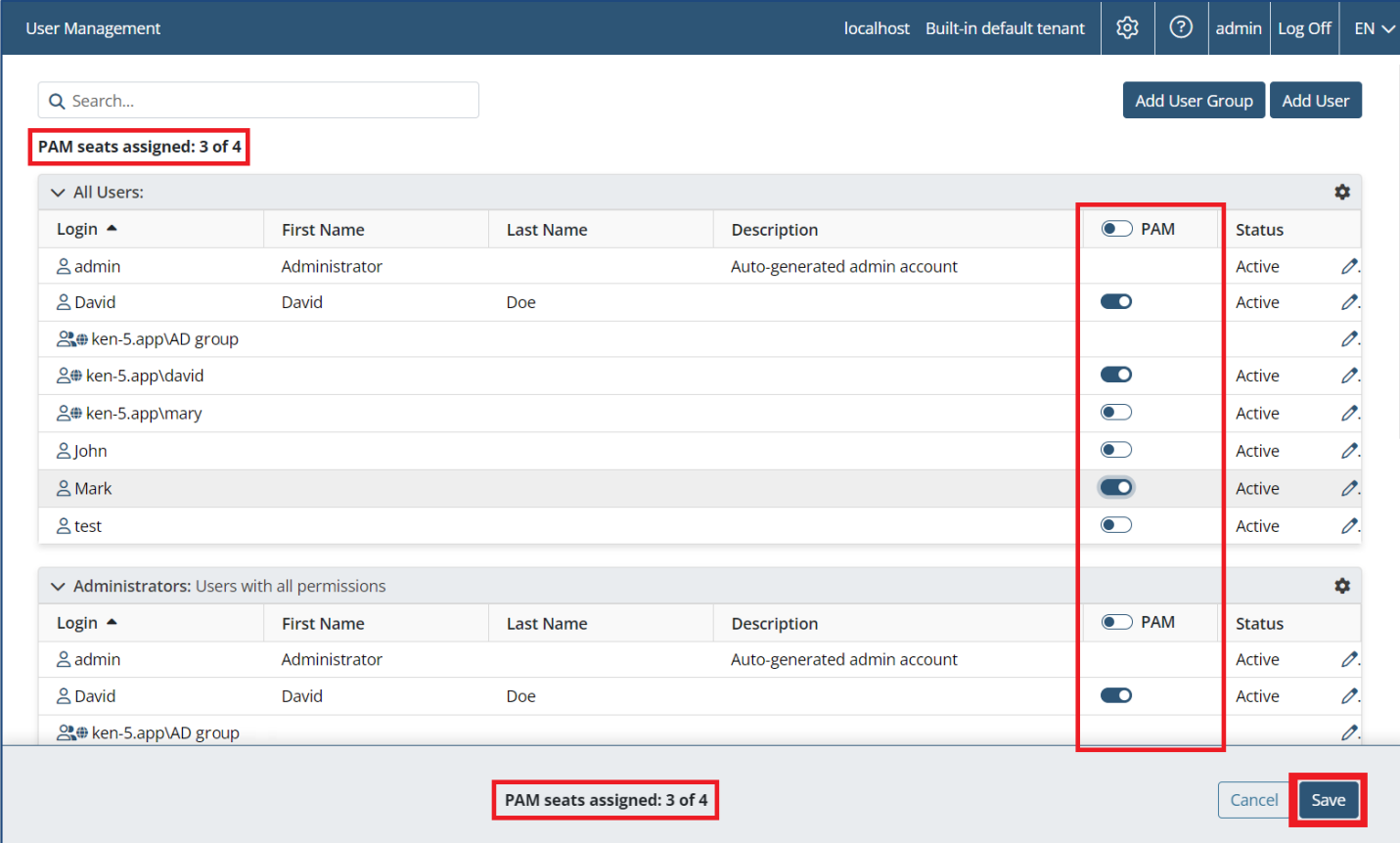
The screenshot shows the 'User Management' interface. At the top, there's a header with 'localhost Built-in default tenant' and user controls for 'admin', 'Log Off', and 'EN'. Below the header is a search bar and buttons for 'Add User Group' and 'Add User'. A status bar indicates 'PAM seats assigned: 3 of 4'. The main content area is divided into two sections: 'All Users' and 'Administrators: Users with all permissions'. Each section contains a table with columns for 'Login', 'First Name', 'Last Name', 'Description', 'PAM' (toggle), and 'Status'. The 'All Users' section lists 8 users, including 'admin', 'David', and several 'ken-5.app' users. The 'Administrators' section lists 2 users, 'admin' and 'David'.

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

Administrators: Users with all permissions					
Login	First Name	Last Name	Description	PAM	Status
admin	Administrator		Auto-generated admin account	<input checked="" type="checkbox"/>	Active
David	David	Doe		<input type="checkbox"/>	Active

Assign PAM Licenses to Users

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



The screenshot displays the 'User Management' interface. At the top, there's a navigation bar with 'localhost', 'Built-in default tenant', and user controls. Below this is a search bar and buttons for 'Add User Group' and 'Add User'. A red box highlights the text 'PAM seats assigned: 3 of 4' in the top left. The main content area shows two tables: 'All Users' and 'Administrators: Users with all permissions'. Both tables have columns for 'Login', 'First Name', 'Last Name', 'Description', 'PAM' (with a toggle switch), and 'Status'. A red box highlights the 'PAM' toggle column for both tables. At the bottom, another red box highlights 'PAM seats assigned: 3 of 4', and there are 'Cancel' and 'Save' buttons.


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


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

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

Configuration

localhost Built-in default tenant





d.local\david

Log Off

EN ▾

Serial Key Management

Email Sending Settings

System Settings

Customization

SIEM Integration

Ticketing System Integration

LDAP Targets

Date & Time Format

Export Storage Settings

Master Panel Access

Database Management

Embedding Settings

Applications













SSO Integration

Cluster Settings

Add

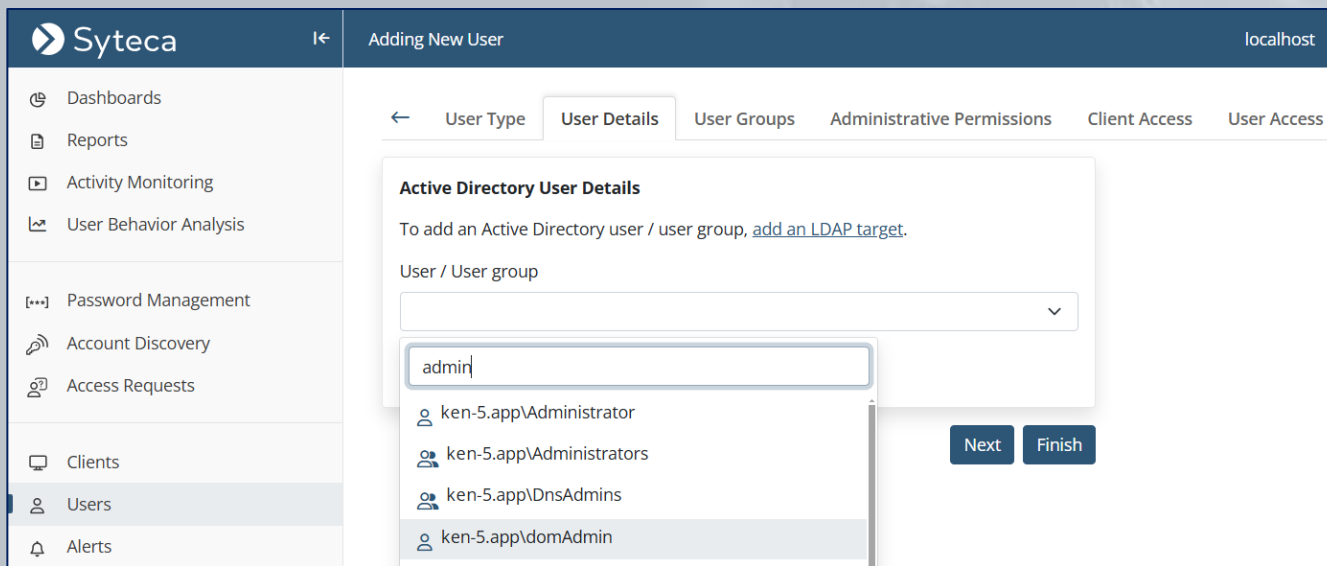
Refresh Automatic LDAP Target

Sync Active Directory User Groups

LDAP Path	Domain Name	Domain NetBIOS Name	User	Type		Remove All
LDAP://ken.local/DC=ek...	ken.local	KEN	all.tea...	Manual		
LDAP://100.100.10.100/D...	ken-2.app	KEN-2-APP	orig1	Manual		
GC://100.100.100.100	forest.com	AD-Forest	Admi...	Manual		
GC://100.100.10.100	prod.local	PROD	Adm ...	Manual		
LDAP://10.100.0.1/DC=de...	d.local	DEV	kenni...	Manual		
LDAP://ken.local/DC=ek...	ken.local	KEN	samk...	Auto...		



Integration with Active Directory allows you to do the following:

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



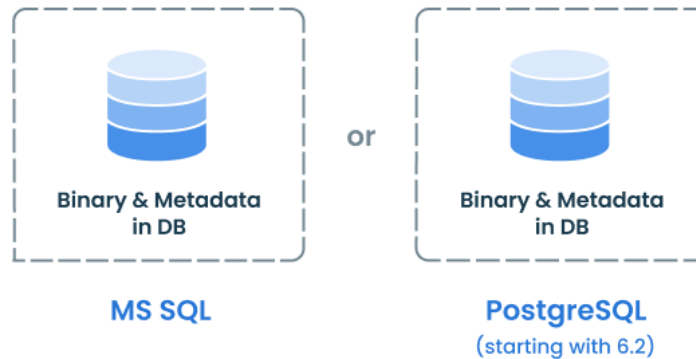
The screenshot shows the Syteca web interface for adding a new user. The left sidebar contains navigation links: Dashboards, Reports, Activity Monitoring, User Behavior Analysis, Password Management, Account Discovery, Access Requests, Clients, Users (selected), and Alerts. The main content area is titled 'Adding New User' and includes a breadcrumb trail: User Type > User Details > User Groups > Administrative Permissions > Client Access > User Access. The 'User Details' tab is active, displaying the 'Active Directory User Details' section. This section contains the instruction 'To add an Active Directory user / user group, [add an LDAP target](#).' Below this is a 'User / User group' dropdown menu. A search input field contains the text 'admin', and a list of suggestions is shown: ken-5.app\Administrator, ken-5.app\Administrators, ken-5.app\DnsAdmins, and ken-5.app\domAdmin. At the bottom right of the form are 'Next' and 'Finish' buttons.

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

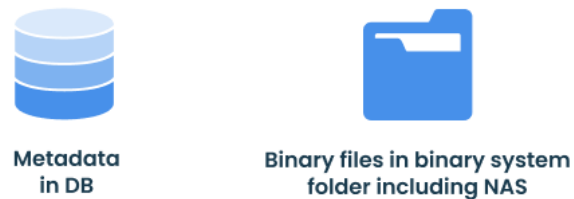
Audit Log							localhost	Built-in default tenant			ADMIN	LOG OFF	EN ▾
When: All Who: All Action: All + More criteria							EXPORT FILTERED RECORDS TO CSV EXPORT FILTERED RECORDS TO PDF						
TIME ▾	USER NAME ▾	USER GROUPS ▾	CATEGORY ▾	ACTION ▾	OBJECT ▾	DETAILS							
02/15/2023 11:40...	admin	Administrators	Session viewing	Viewing	WIN10	User: SUPPORT\alex1 Time: 14/12/2022 13:00:49-14/12/2022 13:16:39 View							
02/15/2023 11:40...	admin	Administrators	Session viewing	Viewing	WINServer2019	User: WIN-4D\Administrator(pamuser) Time: 20/09/2022 10:57:04-20/09/2022 17:43:07 View							
02/15/2023 11:39...	admin	Administrators	Client group editing	Editing settings	Jump Servers	Jump Server mode: No							
02/15/2023 11:38...	Pamuser		Secret manager	Using Secret	Support_desktop	Jump Server Name: WINServer2019 Remote IP: 10.1							
02/15/2023 11:38...	admin	Administrators	Access management	Granting access	WINServer2019	Approved by: admin Comments: Secret Name: Support_desktop Secret Type: Active Directory account Requested by: support\alex1 (pamuser)							
02/15/2023 11:33...	Pamuser		Secret manager	Using Secret	DesktopWin10	Jump Server Name: WINServer2019							
02/15/2023 11:31...	Pamuser		Secret manager	Using Secret	WebAccount	Jump Server Name: WINServer2019							
02/15/2023 11:31...	Pamuser		Secret manager	Using Secret	WebAccount	Jump Server Name: WINServer2019							
02/15/2023 11:31...	Pamuser		Secret manager	Using Secret	DesktopWin10	Jump Server Name: WINServer2019							
10 50 100 200							« 1 2 3 4 5 6 »						

Database Management

Default Configuration



Custom Configuration (MS SQL or PostgreSQL)



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

Auto-Cleanup options

☐ Never


☐ Run once

☒ Repeat according to schedule


Perform every (days)

30

Start at

12:00:00 AM 

Action type

Archive & Cleanup 

Sessions older than (days)

0

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

Auto-Cleanup options

☐ Never

☒ Run once

☐ Repeat according to schedule

Action type

Archive & Cleanup ▼

Sessions older than (days)

30

Configuration

Archive Parameters

Instance

db1.ken.local,50000

Archived database name

ArchiveDB

User

sa

Password

.....

Binary data location

\\DC-ABC\ArchiveDB

☒ Archive and clean up the database without archiving and deleting the binary data

☐ Use separate credentials to access binary storage

User

Password

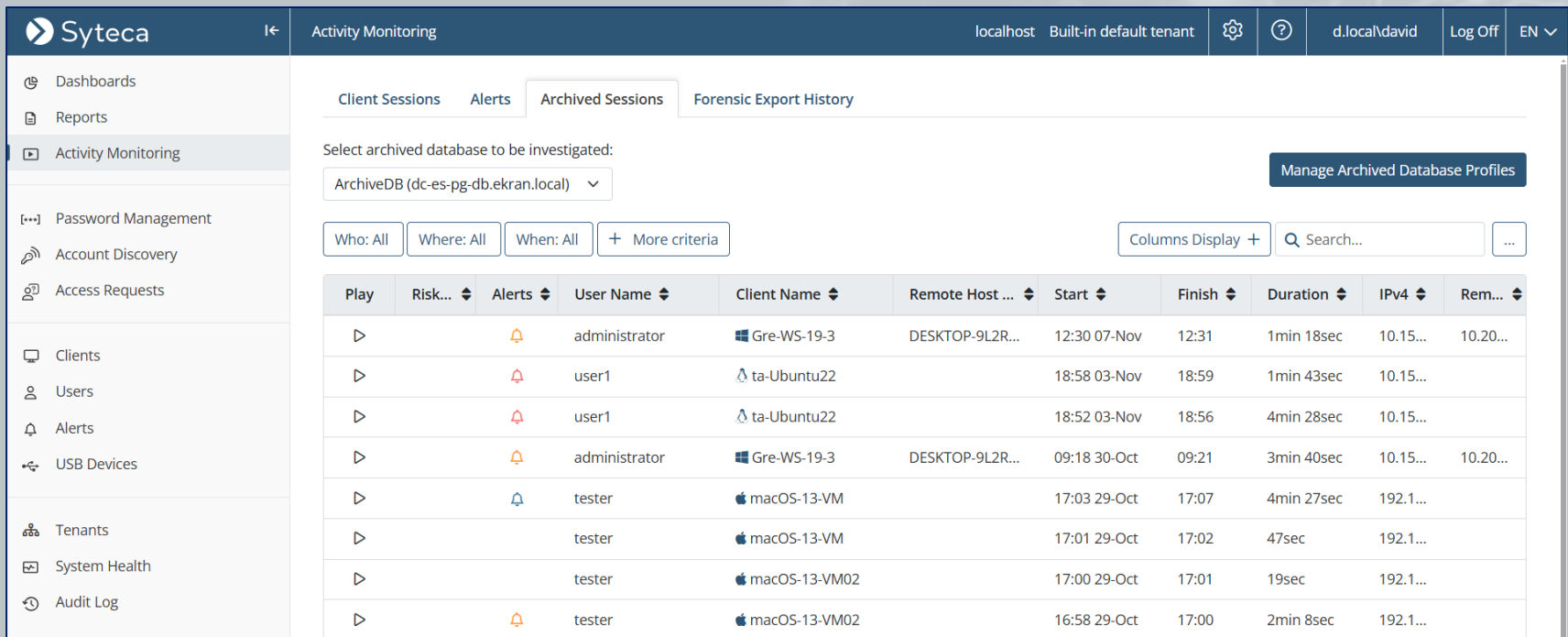
☐ Shrink database transaction log after cleanup

☐ Delete offline Clients without sessions

Test Database Connection

Shrink transaction log Update statistics Save

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**.

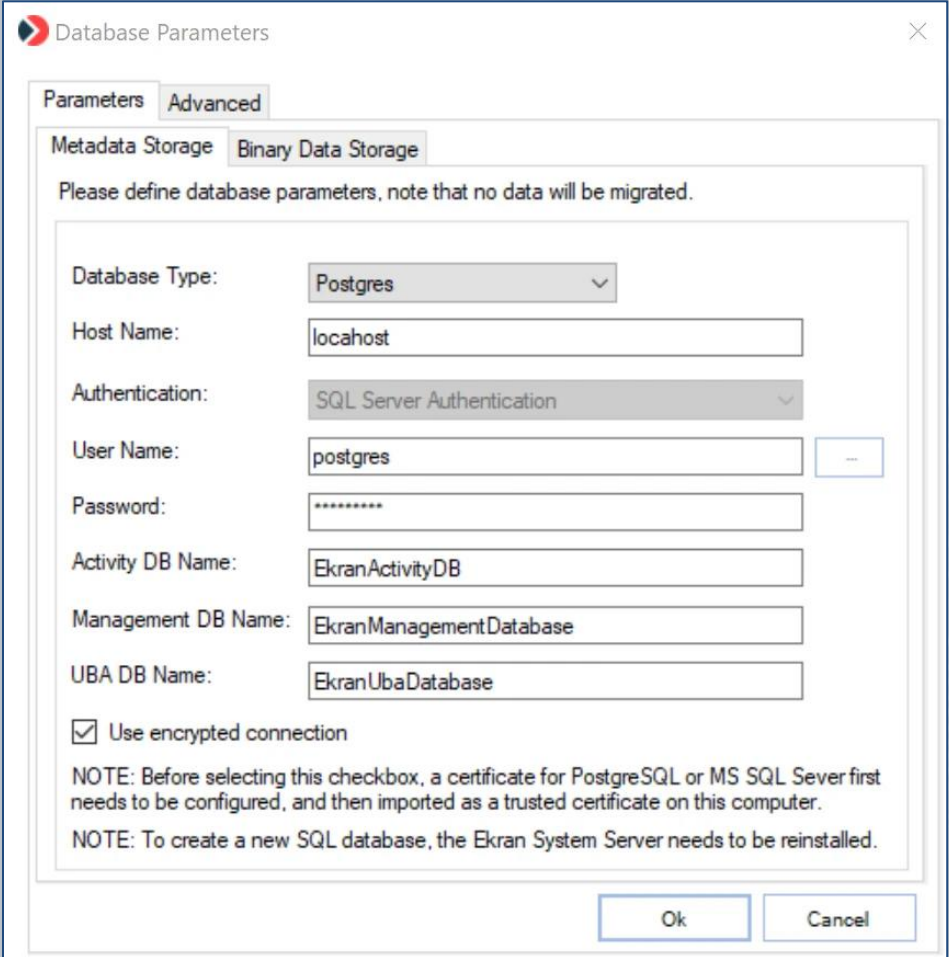


The screenshot displays the Syteca Activity Monitoring interface. The left sidebar contains navigation links: Dashboards, Reports, Activity Monitoring (selected), Password Management, Account Discovery, Access Requests, Clients, Users, Alerts, USB Devices, Tenants, System Health, and Audit Log. The main content area is titled 'Activity Monitoring' and includes tabs for Client Sessions, Alerts, Archived Sessions (selected), and Forensic Export History. A dropdown menu shows 'ArchiveDB (dc-es-pg-db.ekran.local)' as the selected database. Below this are filters for 'Who: All', 'Where: All', 'When: All', and a '+ More criteria' button. A 'Manage Archived Database Profiles' button is also present. A table displays session data with columns: Play, Risk..., Alerts, User Name, Client Name, Remote Host, Start, Finish, Duration, IPv4, and Rem... The table contains 10 rows of session data.

Play	Risk...	Alerts	User Name	Client Name	Remote Host ...	Start	Finish	Duration	IPv4	Rem...
▶		🔔	administrator	Gre-WS-19-3	DESKTOP-9L2R...	12:30 07-Nov	12:31	1min 18sec	10.15...	10.20...
▶		🔔	user1	ta-Ubuntu22		18:58 03-Nov	18:59	1min 43sec	10.15...	
▶		🔔	user1	ta-Ubuntu22		18:52 03-Nov	18:56	4min 28sec	10.15...	
▶		🔔	administrator	Gre-WS-19-3	DESKTOP-9L2R...	09:18 30-Oct	09:21	3min 40sec	10.15...	10.20...
▶		🔔	tester	macOS-13-VM		17:03 29-Oct	17:07	4min 27sec	192.1...	
▶			tester	macOS-13-VM		17:01 29-Oct	17:02	47sec	192.1...	
▶			tester	macOS-13-VM02		17:00 29-Oct	17:01	19sec	192.1...	
▶		🔔	tester	macOS-13-VM02		16:58 29-Oct	17:00	2min 8sec	192.1...	

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

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



Database Parameters

Parameters Advanced

Metadata Storage Binary Data Storage

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

Database Type: Postgres

Host Name: localhost

Authentication: SQL Server Authentication

User Name: postgres

Password: *****

Activity DB Name: EkranActivityDB

Management DB Name: EkranManagementDatabase

UBA DB Name: EkranUbaDatabase

☒ Use encrypted connection

NOTE: Before selecting this checkbox, a certificate for PostgreSQL or MS SQL Server first needs to be configured, and then imported as a trusted certificate on this computer.

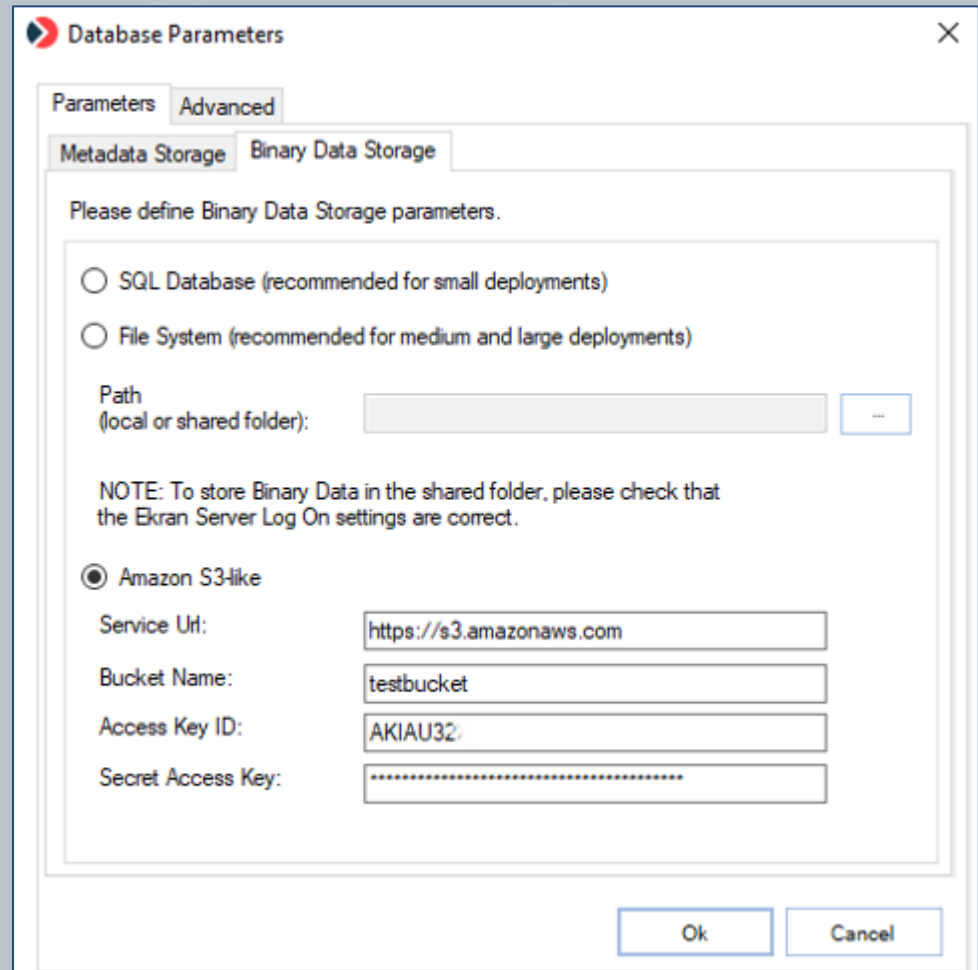
NOTE: To create a new SQL database, the Ekran System Server needs to be reinstalled.

Ok Cancel

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.

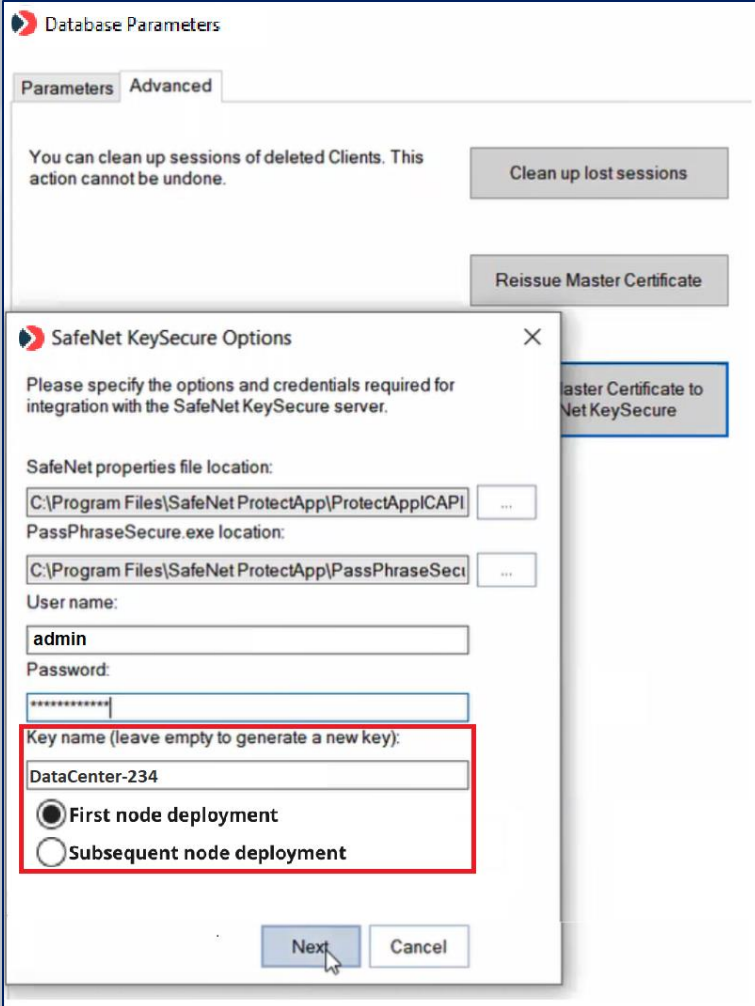
Network-Attached Storage (NAS) can also be used (by using the **File System** option).



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 main text inside the dialog says 'Please define Binary Data Storage parameters.' Below this, there are two radio button options: 'SQL Database (recommended for small deployments)' and 'File System (recommended for medium and large deployments)'. The 'File System' option is currently selected. Below these options is a text field labeled 'Path (local or shared folder):' followed by a browse button (three dots). A note below the path field states: 'NOTE: To store Binary Data in the shared folder, please check that the Ekran Server Log On settings are correct.' Below the note, the 'Amazon S3-like' option is selected with a radio button. This option has 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 'AKIAU32', and 'Secret Access Key:' with a masked value represented by dots. At the bottom right of the dialog are 'Ok' and 'Cancel' buttons.

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**.

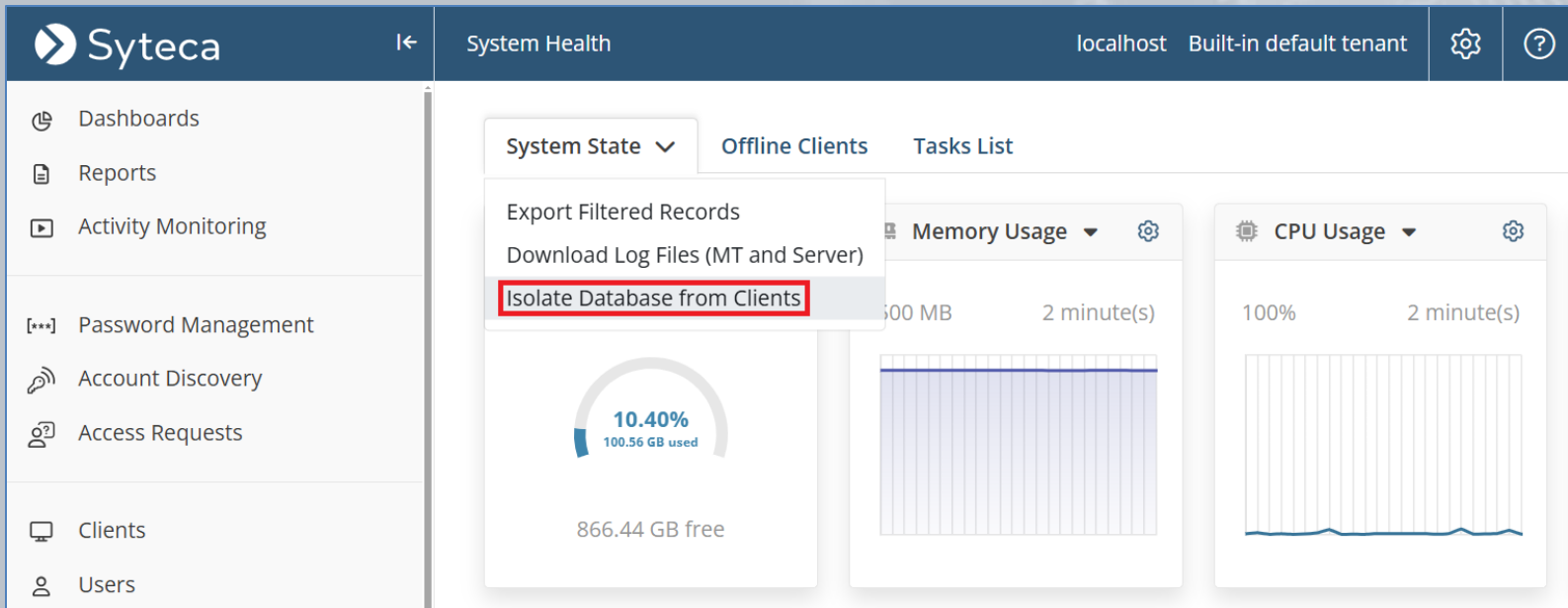


The screenshot shows the 'Database Parameters' dialog box with the 'Advanced' tab selected. The 'Parameters' tab is also visible. The 'Advanced' tab contains two buttons: 'Clean up lost sessions' and 'Reissue Master Certificate'. The 'SafeNet KeySecure Options' sub-dialog box is open, displaying the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

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



The screenshot displays the Syteca System Health dashboard. The left sidebar contains navigation links: Dashboards, Reports, Activity Monitoring, Password Management, Account Discovery, Access Requests, Clients, and Users. The main content area shows the 'System Health' status for 'localhost' and 'Built-in default tenant'. A dropdown menu for 'System State' is open, highlighting the 'Isolate Database from Clients' option. Below the menu, three performance metrics are visible: a disk usage gauge showing 10.40% (100.56 GB used) and 866.44 GB free; a 'Memory Usage' bar chart; and a 'CPU Usage' line chart. All charts indicate a 2-minute refresh interval.

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

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

Monitoring Parameters

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

Timeout (min)

15

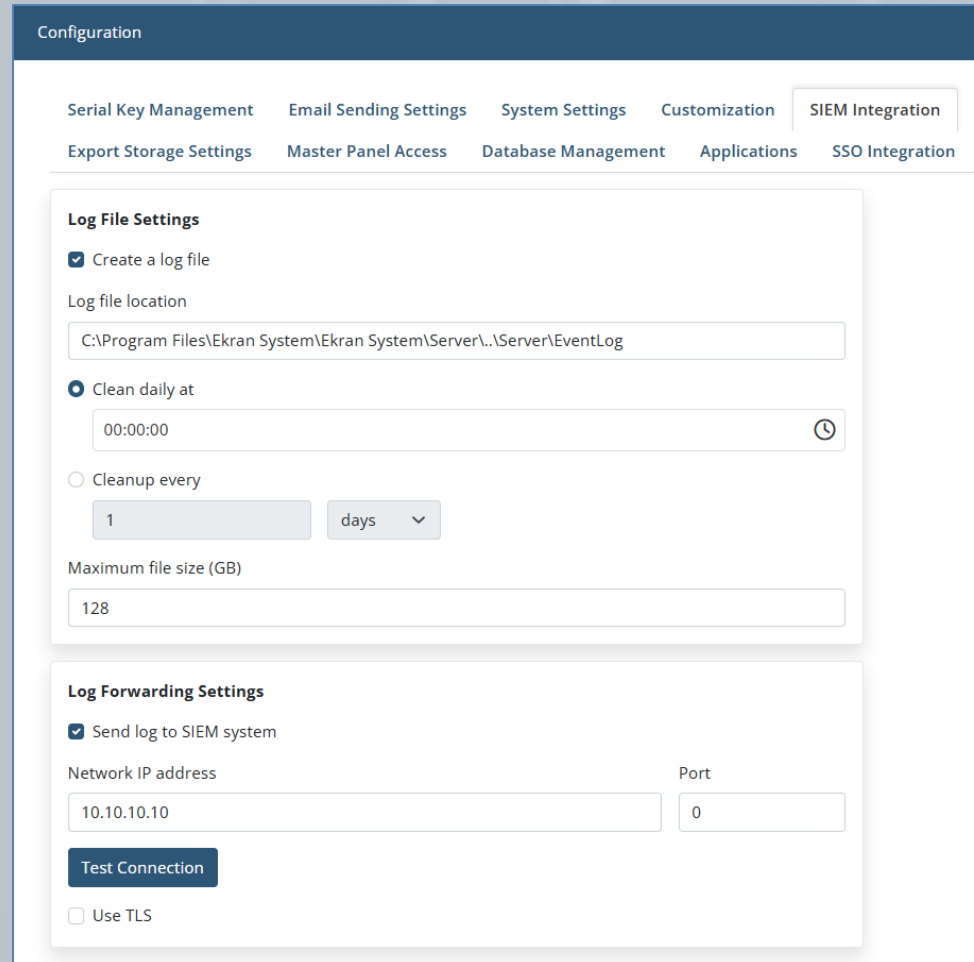
Log Files

- ☒ Enable creating log files of monitored events

Log files location



C:\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 'Configuration' page of the Syteca interface. The 'SIEM Integration' tab is selected in the top navigation bar. Below the navigation bar, there are two main sections: 'Log File Settings' and 'Log Forwarding Settings'.

Log File Settings:

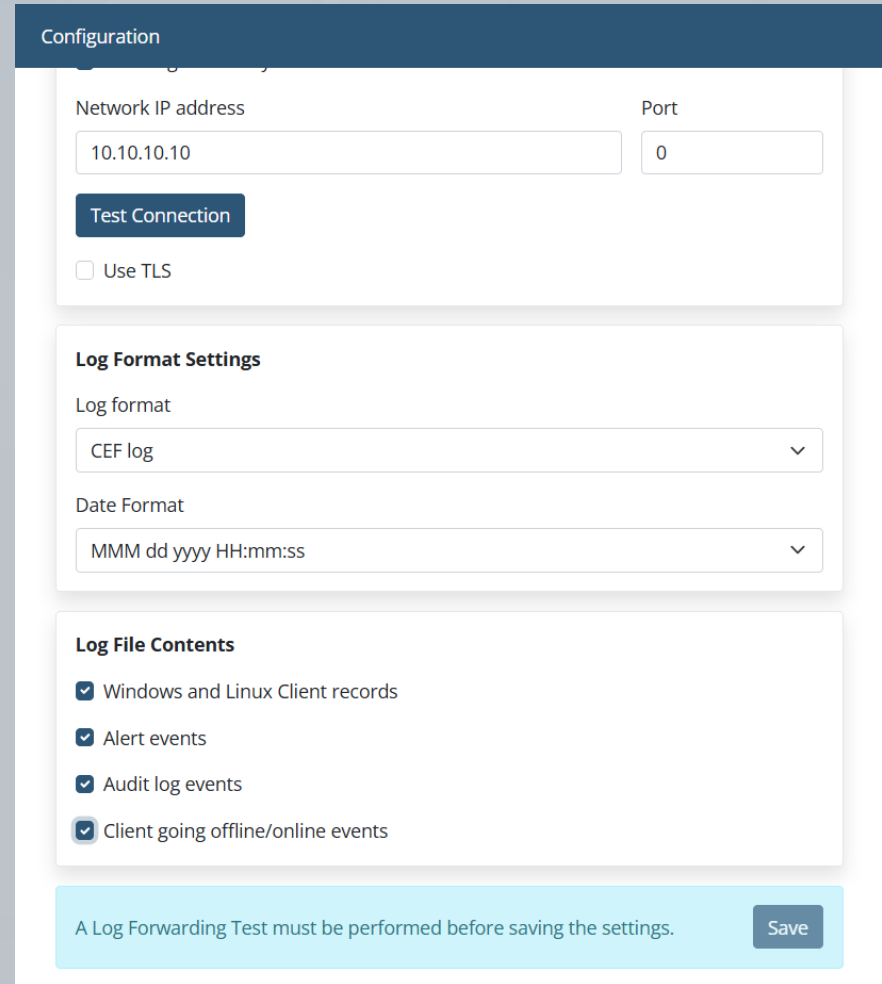
- ☒ Create a log file
- Log file location:
- ☒ Clean daily at: 
- ☐ Cleanup every: days 
- Maximum file size (GB):

Log Forwarding Settings:

- ☒ Send log to SIEM system
- Network IP address:
- Port:
-
- ☐ Use TLS

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 image shows a web-based configuration interface for Syteca SIEM integration. The interface is titled "Configuration" and is divided into three main sections: Network Settings, Log Format Settings, and Log File Contents. In the Network Settings section, the "Network IP address" is set to "10.10.10.10" and the "Port" is set to "0". There is a "Test Connection" button and an unchecked checkbox for "Use TLS". The Log Format Settings section has a "Log format" dropdown set to "CEF log" and a "Date Format" dropdown set to "MMM dd yyyy HH:mm:ss". The Log File Contents section has four checked checkboxes: "Windows and Linux Client records", "Alert events", "Audit log events", and "Client going offline/online events". At the bottom, a light blue banner contains the text "A Log Forwarding Test must be performed before saving the settings." and a "Save" button.

Configuration

Network IP address: 10.10.10.10 Port: 0

Test Connection

☐ Use TLS

Log Format Settings

Log format: CEF log

Date Format: MMM dd yyyy HH:mm:ss

Log File Contents

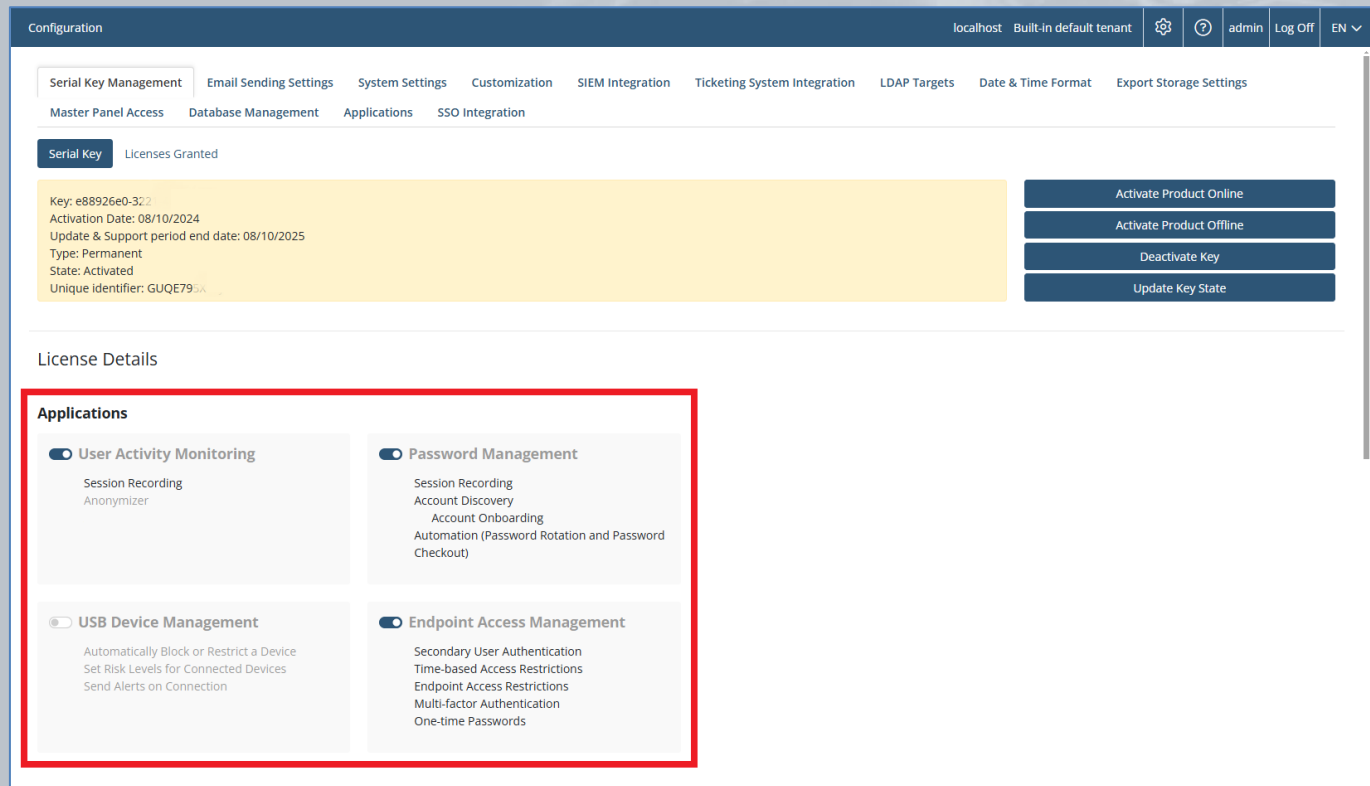
- ☒ Windows and Linux Client records
- ☒ Alert events
- ☒ Audit log events
- ☒ Client going offline/online events

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).

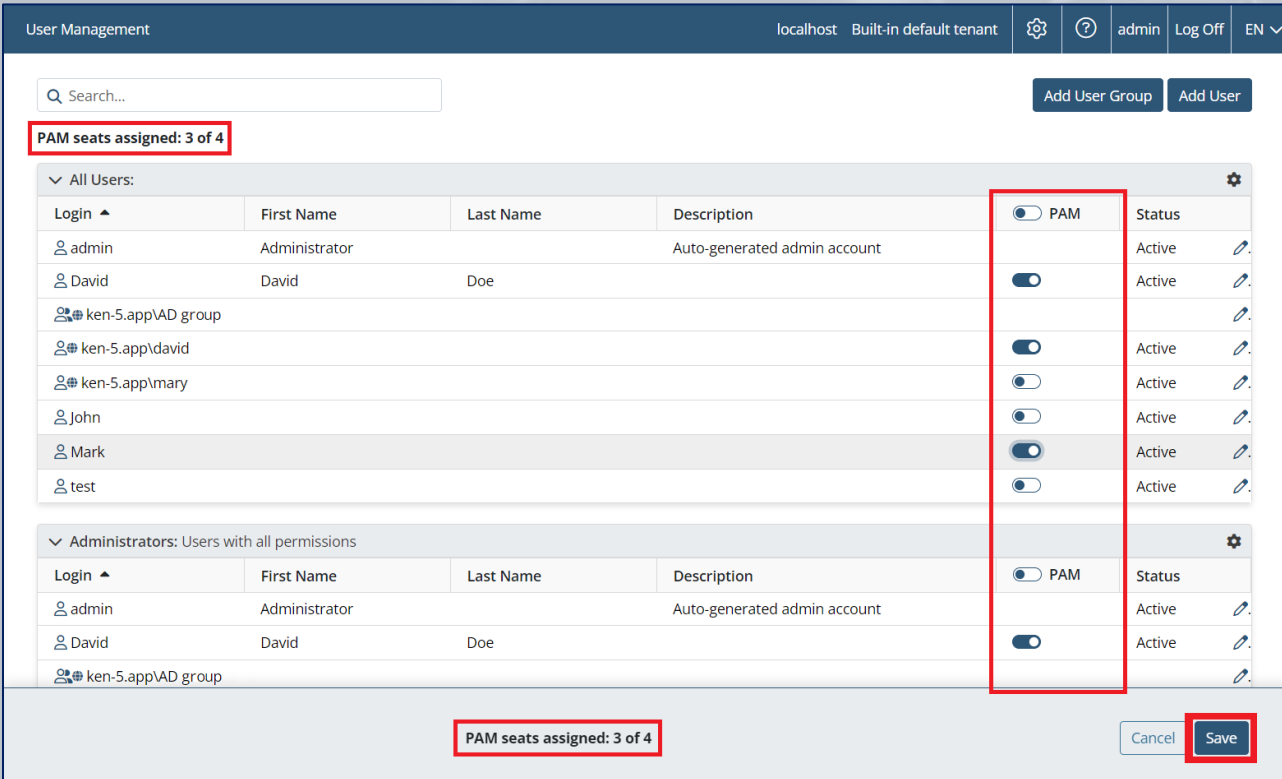


The screenshot displays the Syteca Configuration interface. The top navigation bar includes 'localhost Built-in default tenant', a settings icon, a help icon, 'admin', 'Log Off', and a language dropdown 'EN'. Below this is a sub-navigation bar with tabs: 'Serial Key Management', 'Email Sending Settings', 'System Settings', 'Customization', 'SIEM Integration', 'Ticketing System Integration', 'LDAP Targets', 'Date & Time Format', and 'Export Storage Settings'. Under 'Serial Key Management', there are sub-tabs for 'Serial Key' and 'Licenses Granted'. The 'Serial Key' tab is active, showing a yellow box with the following details: Key: e88926e0-322, Activation Date: 08/10/2024, Update & Support period end date: 08/10/2025, Type: Permanent, State: Activated, and Unique Identifier: GUQE79. To the right of this box are four buttons: 'Activate Product Online', 'Activate Product Offline', 'Deactivate Key', and 'Update Key State'. Below the license details is the 'License Details' section, which contains a red-bordered box titled 'Applications'. This box lists four enabled applications with their respective features:

- User Activity Monitoring** (enabled): Session Recording, Anonymizer.
- Password Management** (enabled): Session Recording, Account Discovery, Account Onboarding, Automation (Password Rotation and Password Checkout).
- USB Device Management** (disabled): Automatically Block or Restrict a Device, Set Risk Levels for Connected Devices, Send Alerts on Connection.
- Endpoint Access Management** (enabled): Secondary User Authentication, Time-based Access Restrictions, Endpoint Access Restrictions, Multi-factor Authentication, One-time Passwords.

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 'User Management' interface. At the top, a navigation bar includes 'localhost Built-in default tenant', settings, help, and user options ('admin', 'Log Off', 'EN'). Below the navigation bar is a search bar and buttons for 'Add User Group' and 'Add User'. A red box highlights the text 'PAM seats assigned: 3 of 4' in the top left. The main content area shows two sections: 'All Users' and 'Administrators: Users with all permissions'. Each section contains a table with columns for 'Login', 'First Name', 'Last Name', 'Description', 'PAM' (toggle), and 'Status'. A red box highlights the 'PAM' toggle column for all users. At the bottom, another red box highlights the text 'PAM seats assigned: 3 of 4' and a 'Save' button.

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

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

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.

Configuration localhost

Seat Licenses (5)

PAM
Seats assigned: 2 of 5

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	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	1 of 25
Infrastructure	User Activity Monitoring Maximum number of concurrent sessions: Unlimited	Set Default for Servers Set Default for Workstations	1 of 30
Workstation	User Activity Monitoring 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**.

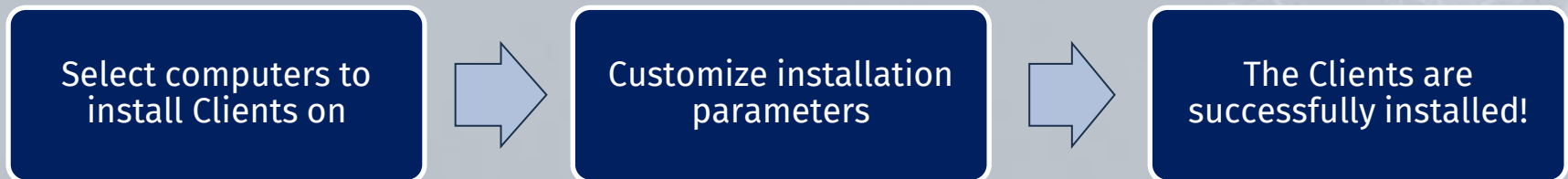
- **Manual** reassignment: Can be done **at any time**, in just a **couple of clicks**.
- **Automatic** reassignment:
 - **Delete offline Clients without sessions**: This option allows the licenses of Clients, whenever they do not have sessions stored, to be returned to the pool of available endpoint 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. 2 computer(s) detected.

<input type="checkbox"/>	IP ↕	Computer ↕	Workgroup / Domain ↕
<input checked="" type="checkbox"/>	10.10.10.10	lee.d.local (10.10.10.10)	d.local
<input type="checkbox"/>	10.10.10.100	kody.d.local (10.10.10.100)	d.local

Next Refresh Stop

Computers Without Clients

localhost Built-in default tenant ⚙️ ⓘ admin Log Off EN ▼

←

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

Deploy via IP Range Deploy on specific computers Download installation file

Computer ↕	Workgroup / Domain ↕	IP ↕	Description ↕	Previous Installation Failure ↕	Remove All
lee.d.local	d.local	10.10.10.10			⊗

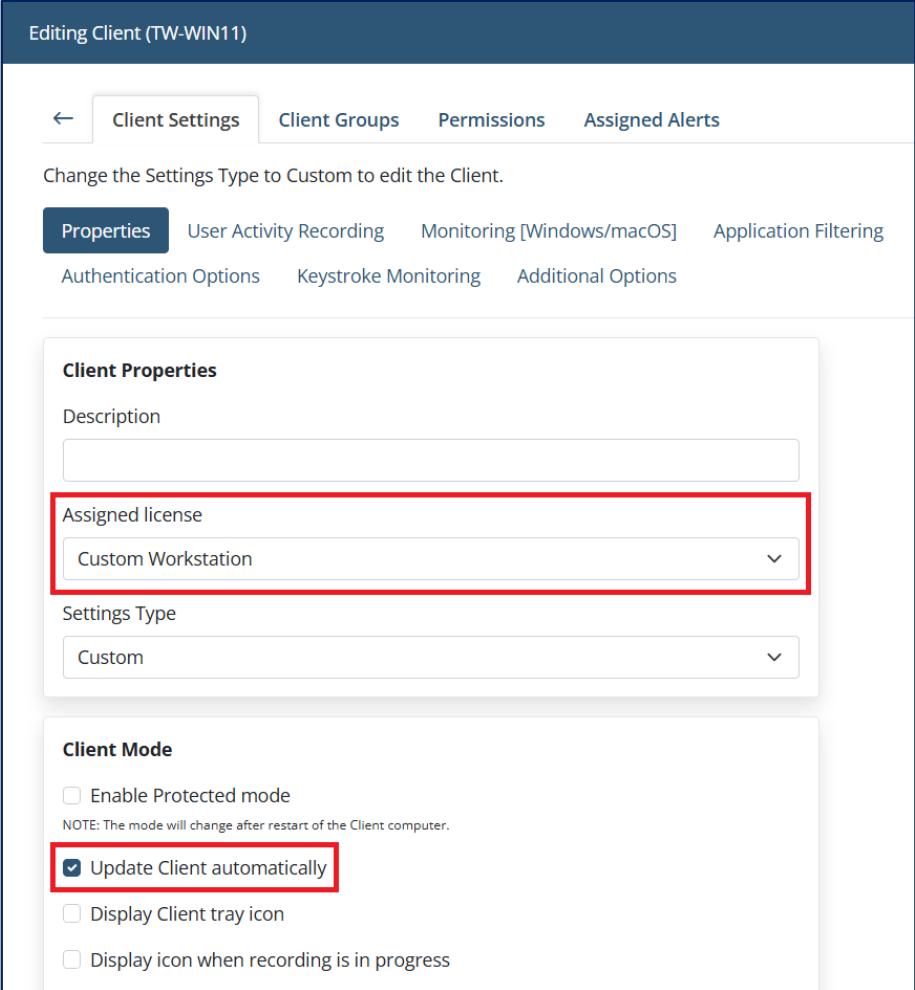
Read the installation prerequisites

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

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

☐ Display icon when recording is in progress

Monitoring Parameters

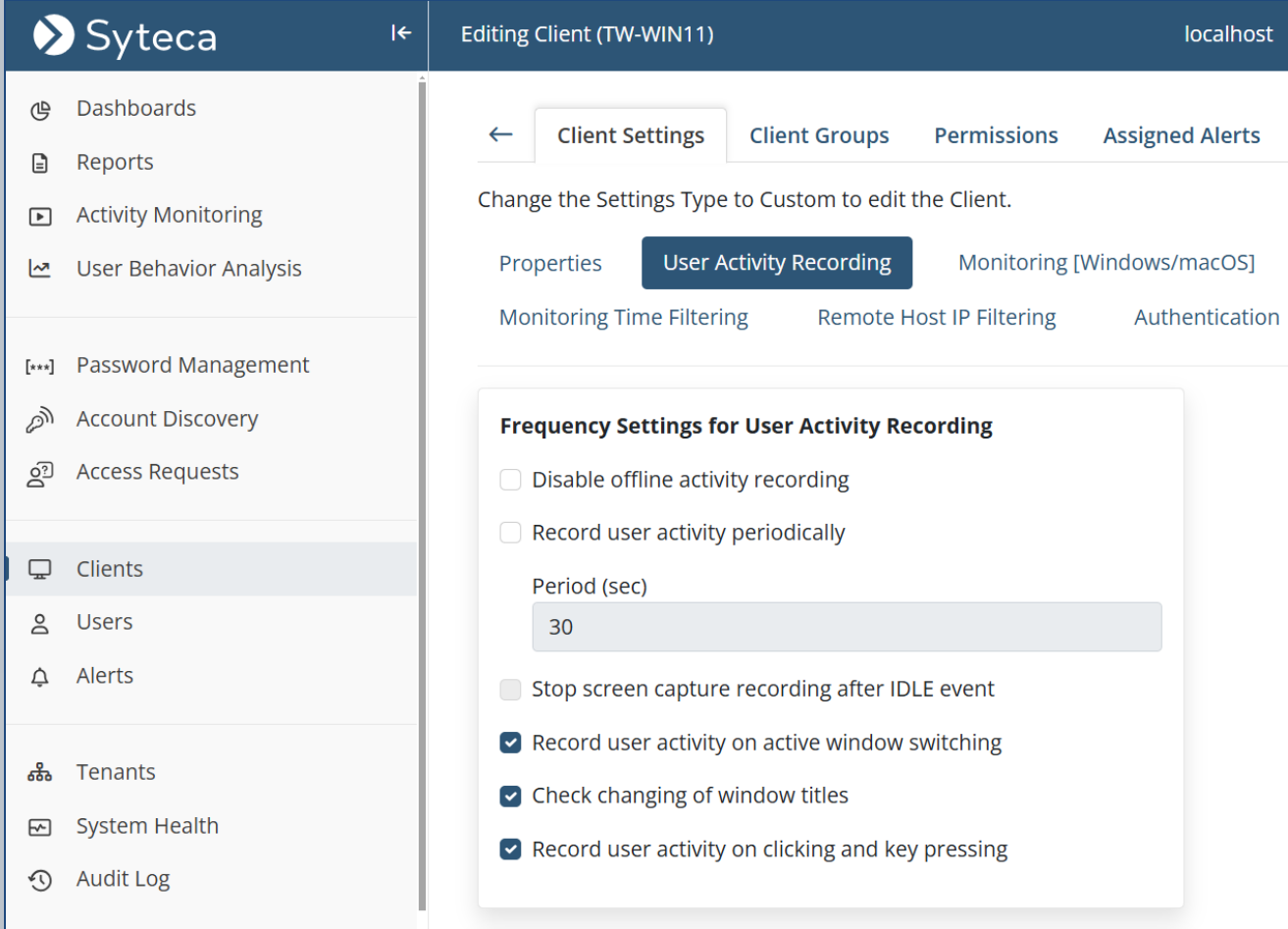
The **screen captures** that the Client sends are stored in the form of deltas (i.e. the differences between a newer recorded screen capture and an older one) to minimize the storage space used.

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).

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**.



Syteca | Editing Client (TW-WIN11) | localhost

← Client Settings | Client Groups | Permissions | Assigned Alerts

Change the Settings Type to Custom to edit the Client.

Properties | **User Activity Recording** | Monitoring [Windows/macOS]

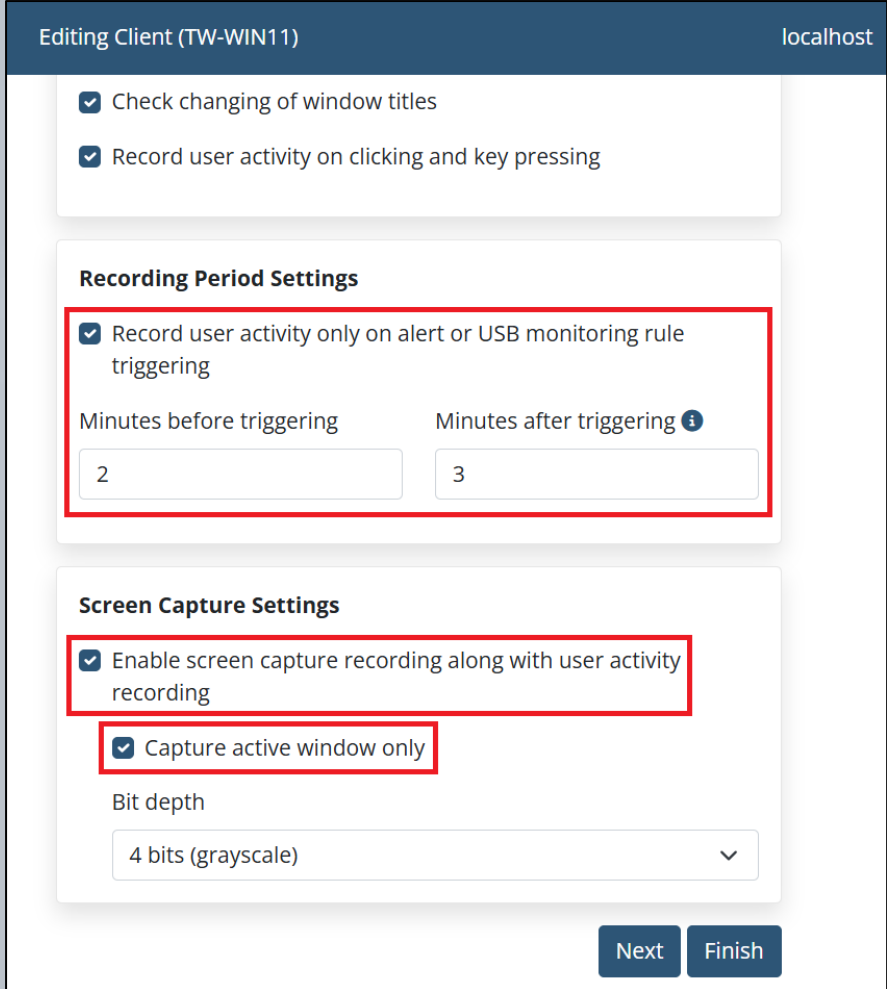
Monitoring Time Filtering | Remote Host IP Filtering | Authentication

Frequency Settings for User Activity Recording

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

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 (TW-WIN11) localhost

- ☒ Check changing of window titles
- ☒ 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: 2 Minutes after triggering: 3 ⓘ

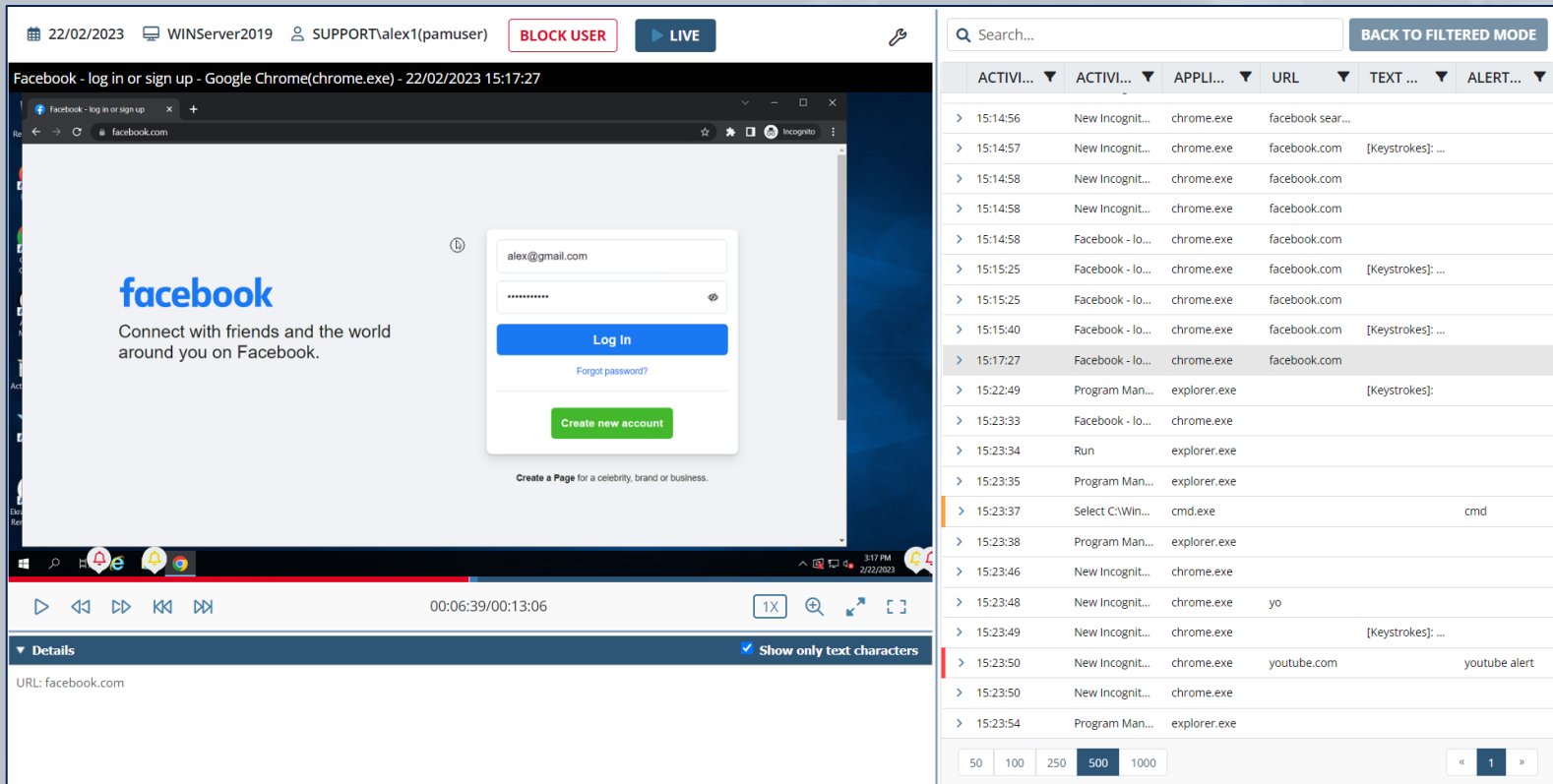
Screen Capture Settings

- ☒ Enable screen capture recording along with user activity recording
- ☒ Capture active window only

Bit depth: 4 bits (grayscale) ▼

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.

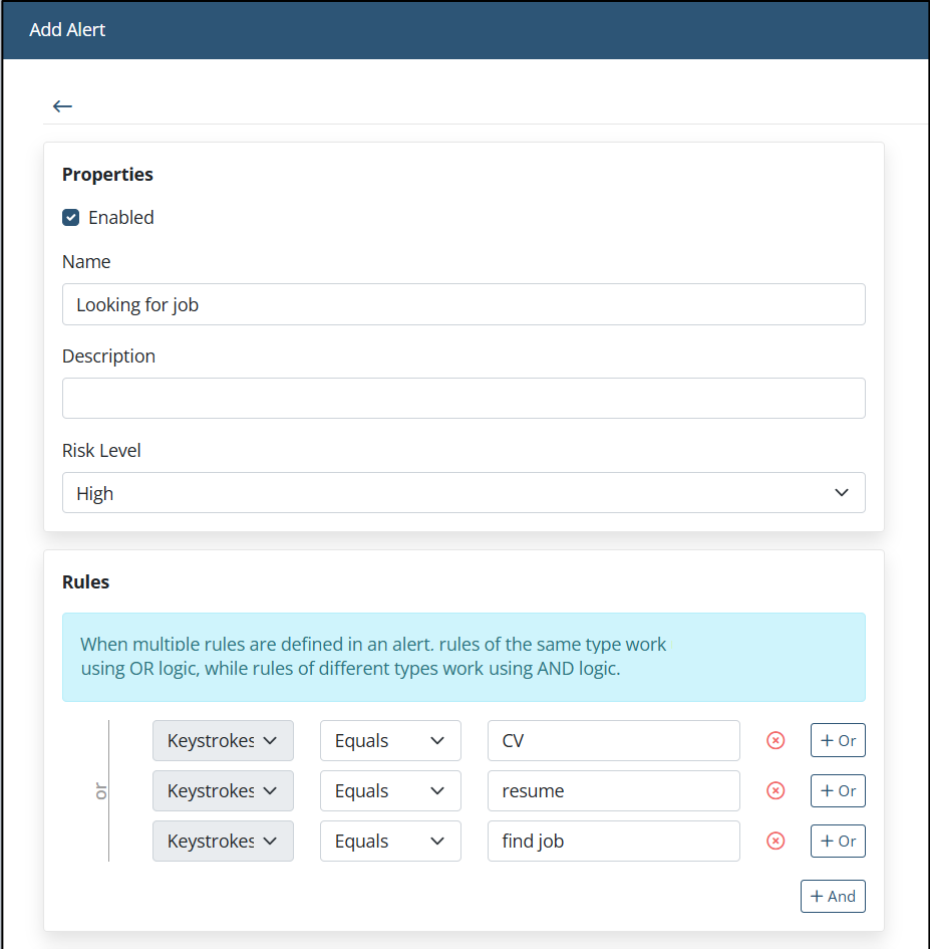


The screenshot displays the Syteca Client interface. The top bar shows the date 22/02/2023, the system name WINServer2019, the user SUPPORT\alex1(pamuser), and buttons for BLOCK USER and LIVE. The main window shows a Google Chrome browser window with the Facebook login page. The URL bar shows facebook.com. The bottom bar shows the URL: facebook.com. The right panel displays a list of monitored URLs with columns for ACTIVI..., ACTIVI..., APPLI..., URL, TEXT ..., and ALERT... The list includes various activities such as New Incognit..., Facebook - lo..., Program Man..., Run, Select C:\Win..., and youtube.com. The bottom of the right panel shows a filter for 500 items.

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

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

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



The screenshot shows the 'Add Alert' configuration page. It has a dark blue header with the title 'Add Alert'. Below the header is a back arrow icon. The main content area is divided into two sections: 'Properties' and 'Rules'.

Properties Section:

- Enabled:** A checkbox that is checked.
- Name:** A text input field containing 'Looking for job'.
- Description:** An empty text input field.
- Risk Level:** A dropdown menu currently set to 'High'.

Rules Section:

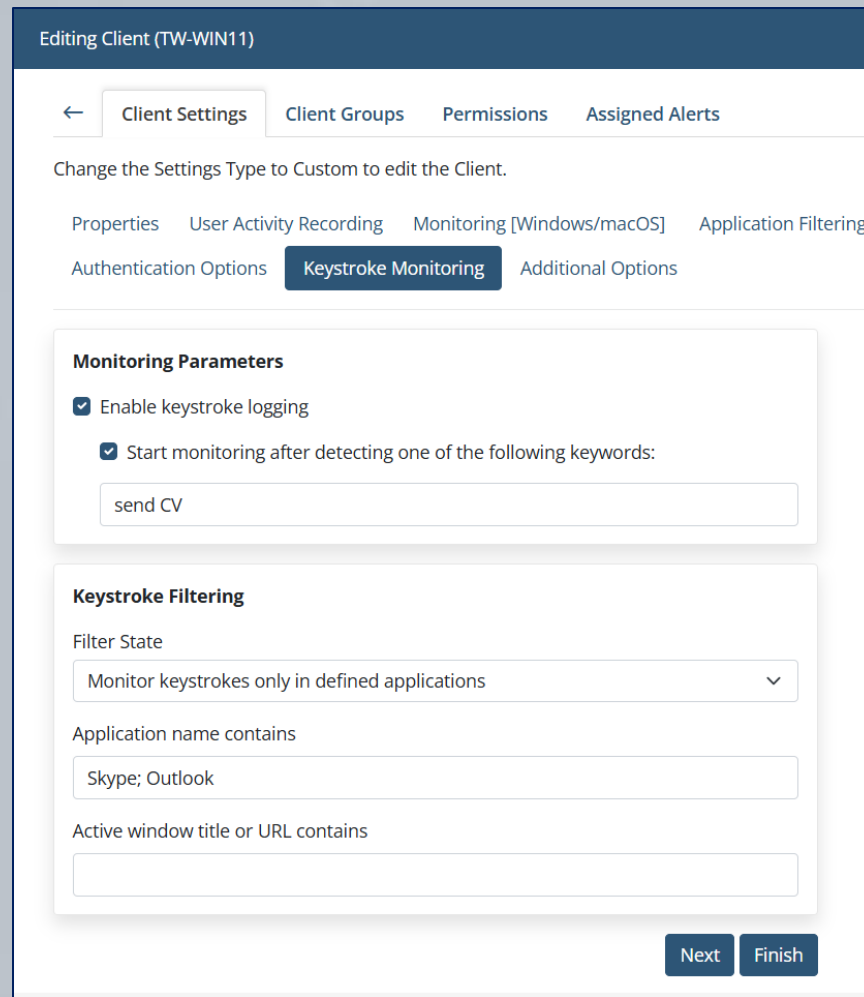
A light blue informational box states: 'When multiple rules are defined in an alert, rules of the same type work using OR logic, while rules of different types work using AND logic.'

Below this box, there are three rules defined, each with a 'Keystrokes' dropdown, an 'Equals' dropdown, and a text input field. To the left of these rules is a vertical line with a '10' icon. Each rule has a red 'X' icon and a '+ Or' button. At the bottom right of the rules section is a '+ And' button.

Rule	Keystrokes	Equals	Value	Action
1	Keystrokes	Equals	CV	+ Or
2	Keystrokes	Equals	resume	+ Or
3	Keystrokes	Equals	find job	+ Or

Keyword-Triggered Monitoring

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



The screenshot shows the 'Editing Client (TW-WIN11)' interface. At the top, there are tabs for 'Client Settings', 'Client Groups', 'Permissions', and 'Assigned Alerts'. Below the tabs, a message states: 'Change the Settings Type to Custom to edit the Client.' Underneath, there are sub-tabs: 'Properties', 'User Activity Recording', 'Monitoring [Windows/macOS]', 'Application Filtering', 'Authentication Options', 'Keystroke Monitoring' (which is selected), and 'Additional Options'.

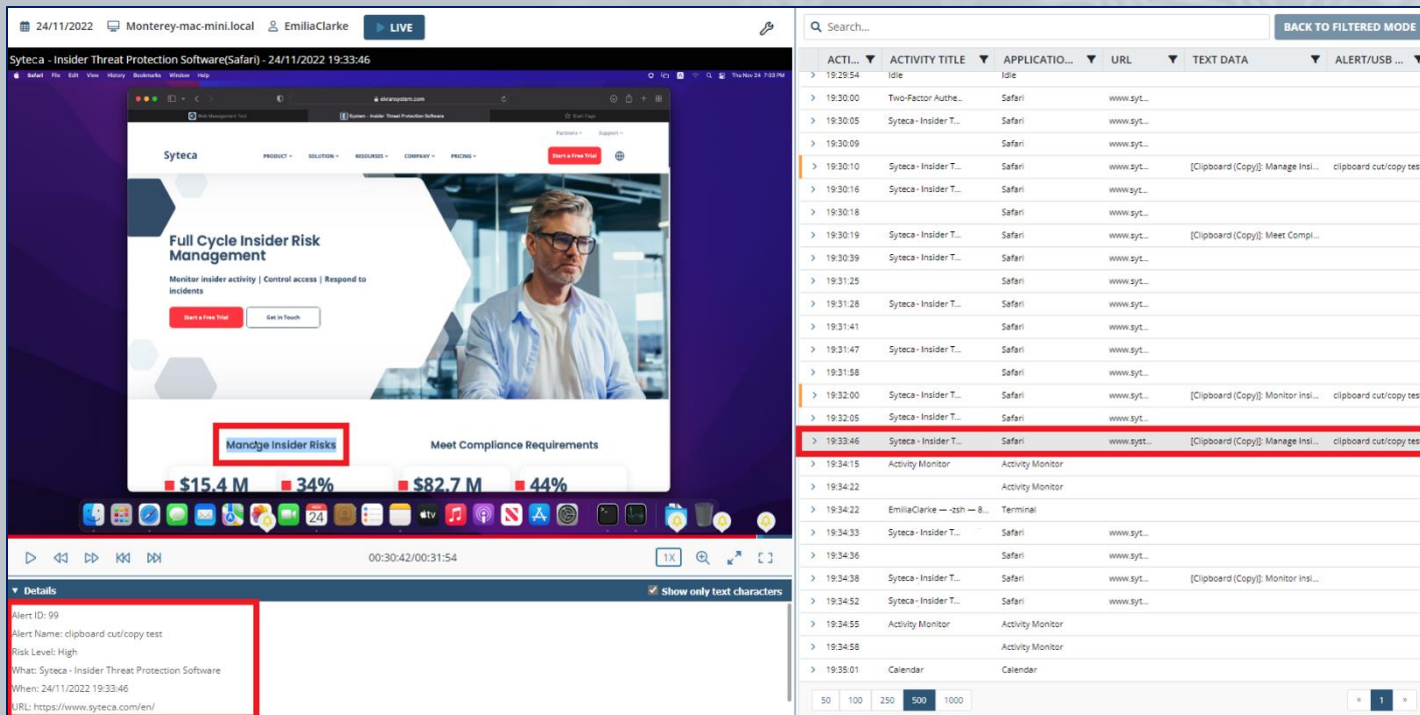
The 'Keystroke Monitoring' section contains two main parts:

- Monitoring Parameters:**
 - ☒ Enable keystroke logging
 - ☒ Start monitoring after detecting one of the following keywords:
 - Text input field: send CV
- Keystroke Filtering:**
 - Filter State: Monitor keystrokes only in defined applications (dropdown menu)
 - Application name contains: Skype; Outlook (text input field)
 - Active window title or URL contains: (empty text input field)

At the bottom right, there are 'Next' and 'Finish' buttons.

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

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



The screenshot displays the Syteca Insider Threat Protection Software interface. The main window shows the Syteca website with a red box highlighting the "Manage Insider Risks" button. Below the website, a red box highlights the "Details" section of an alert. The alert details are as follows:

- 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/

On the right side, a table lists recent activity. The table has columns: ACTI..., ACTIVITY TITLE, APPLICATION..., URL, TEXT DATA, and ALERT/USB... The table shows a list of activities, with the row for "Clipboard (Copy): Manage Ins..." highlighted in red.

ACTI...	ACTIVITY TITLE	APPLICATION...	URL	TEXT DATA	ALERT/USB...
> 19:29:54	Idle	Idle			
> 19:30:00	Two-Factor Authe...	Safari	www.syt...		
> 19:30:05	Syteca - Insider T...	Safari	www.syt...		
> 19:30:09	Safari	Safari	www.syt...		
> 19:30:10	Syteca - Insider T...	Safari	www.syt...	[Clipboard (Copy): Manage Ins...	clipboard cut/copy test
> 19:30:16	Syteca - Insider T...	Safari	www.syt...		
> 19:30:18	Safari	Safari	www.syt...		
> 19:30:19	Syteca - Insider T...	Safari	www.syt...	[Clipboard (Copy): Meet Compl...	
> 19:30:39	Syteca - Insider T...	Safari	www.syt...		
> 19:31:25	Safari	Safari	www.syt...		
> 19:31:28	Syteca - Insider T...	Safari	www.syt...		
> 19:31:41	Safari	Safari	www.syt...		
> 19:31:47	Syteca - Insider T...	Safari	www.syt...		
> 19:31:58	Safari	Safari	www.syt...		
> 19:32:00	Syteca - Insider T...	Safari	www.syt...	[Clipboard (Copy): Monitor ins...	clipboard cut/copy test
> 19:32:05	Syteca - Insider T...	Safari	www.syt...		
> 19:33:46	Syteca - Insider T...	Safari	www.syt...	[Clipboard (Copy): Manage Ins...	clipboard cut/copy test
> 19:34:15	Activity Monitor	Activity Monitor			
> 19:34:22	Activity Monitor	Activity Monitor			
> 19:34:22	EmiliaClarke -- ssh -- 8...	Terminal			
> 19:34:33	Syteca - Insider T...	Safari	www.syt...		
> 19:34:36	Safari	Safari	www.syt...		
> 19:34:38	Syteca - Insider T...	Safari	www.syt...	[Clipboard (Copy): Monitor ins...	
> 19:34:52	Syteca - Insider T...	Safari	www.syt...		
> 19:34:55	Activity Monitor	Activity Monitor			
> 19:34:58	Activity Monitor	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 (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

Application Filtering

Filter State

Monitor all activity except

Application name contains

chrome; edge; firefox

Active window title or URL contains

facebook, twitter

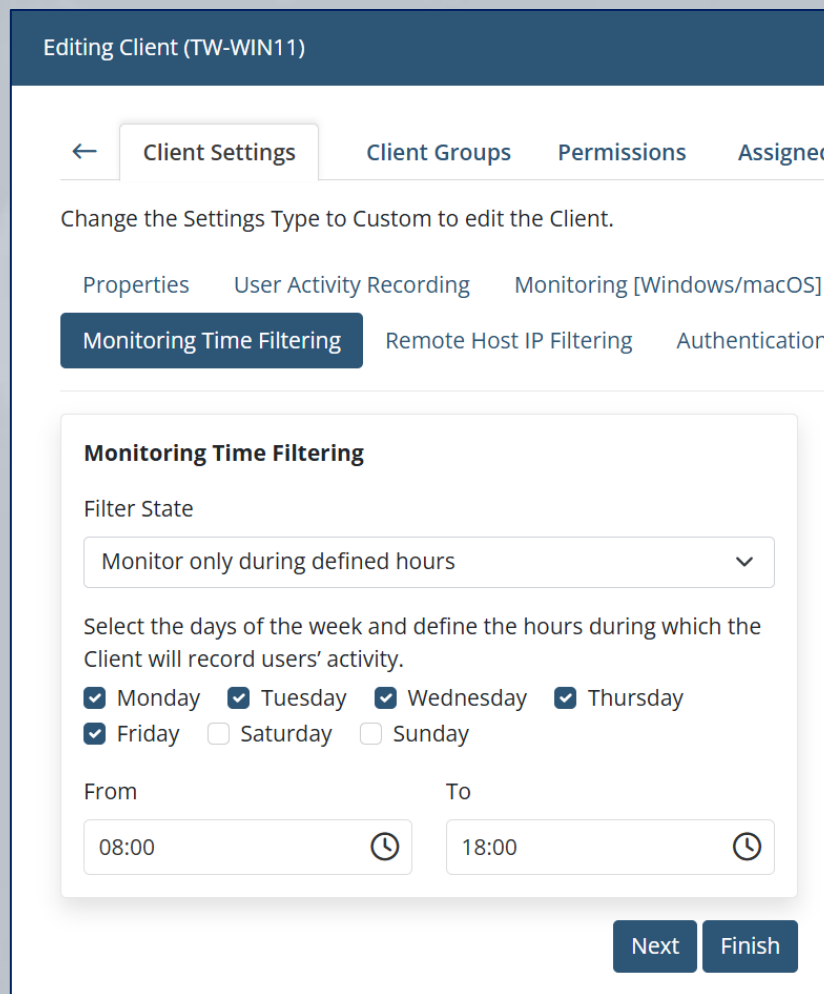
Next

Finish

Monitoring Time Filtering

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

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



The screenshot shows the 'Editing Client (TW-WIN11)' interface. At the top, there are tabs: '←', 'Client Settings' (active), 'Client Groups', 'Permissions', and 'Assigned'. Below the tabs, a message states: 'Change the Settings Type to Custom to edit the Client.' Underneath, there are sub-tabs: 'Properties', 'User Activity Recording', 'Monitoring [Windows/macOS]' (active), 'Monitoring Time Filtering' (active), 'Remote Host IP Filtering', and 'Authentication'. The 'Monitoring Time Filtering' section contains a 'Filter State' dropdown menu set to 'Monitor only during defined hours'. Below this, a text prompt says: 'Select the days of the week and define the hours during which the Client will record users' activity.' There are checkboxes for days of the week: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. Monday through Friday are checked. Below the checkboxes are two time input fields: 'From' (08:00) and 'To' (18:00), each with a clock icon. At the bottom right, there are 'Next' and 'Finish' buttons.

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

Editing Client (TW-WIN11)

←

Client Settings

Client Groups

Permissions

Assigned

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

Remote Host IP Filtering

☐ Exclude local sessions

Filter state

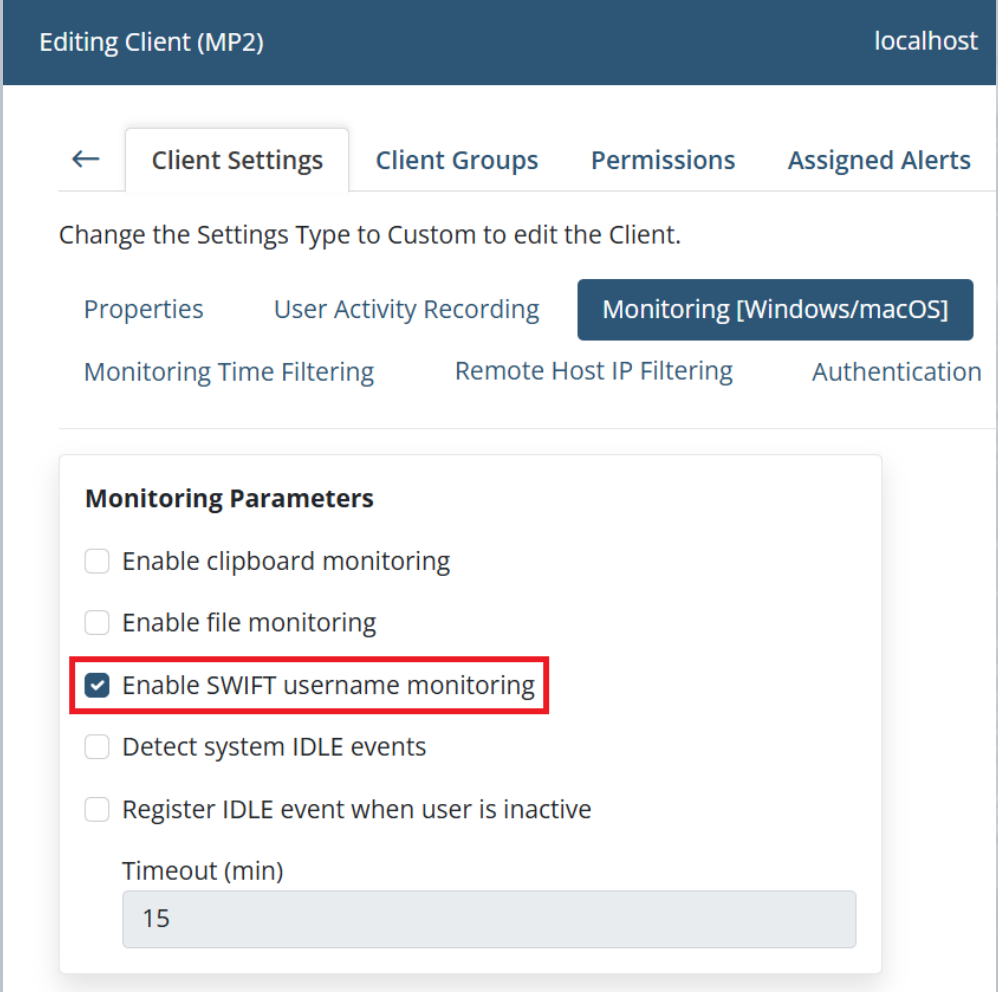
Monitor only activity from selected remote public IP address ▾

Using this feature, you can reduce the amount of information received from the Client by defining remote host IP addresses for which remote sessions will not be monitored.

Enter IP addresses or IP-address ranges in the IPv4 or IPv6 formats separated by commas, semicolons, or new line characters. You can also use asterisk as a mask. For example, 10.100.0.1-10.100.2.255; 2001:0db8:85a3:0000:0000:8a2e:0370:7334; 10.200.*.*

10.0.0.0-10-255.255.255

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



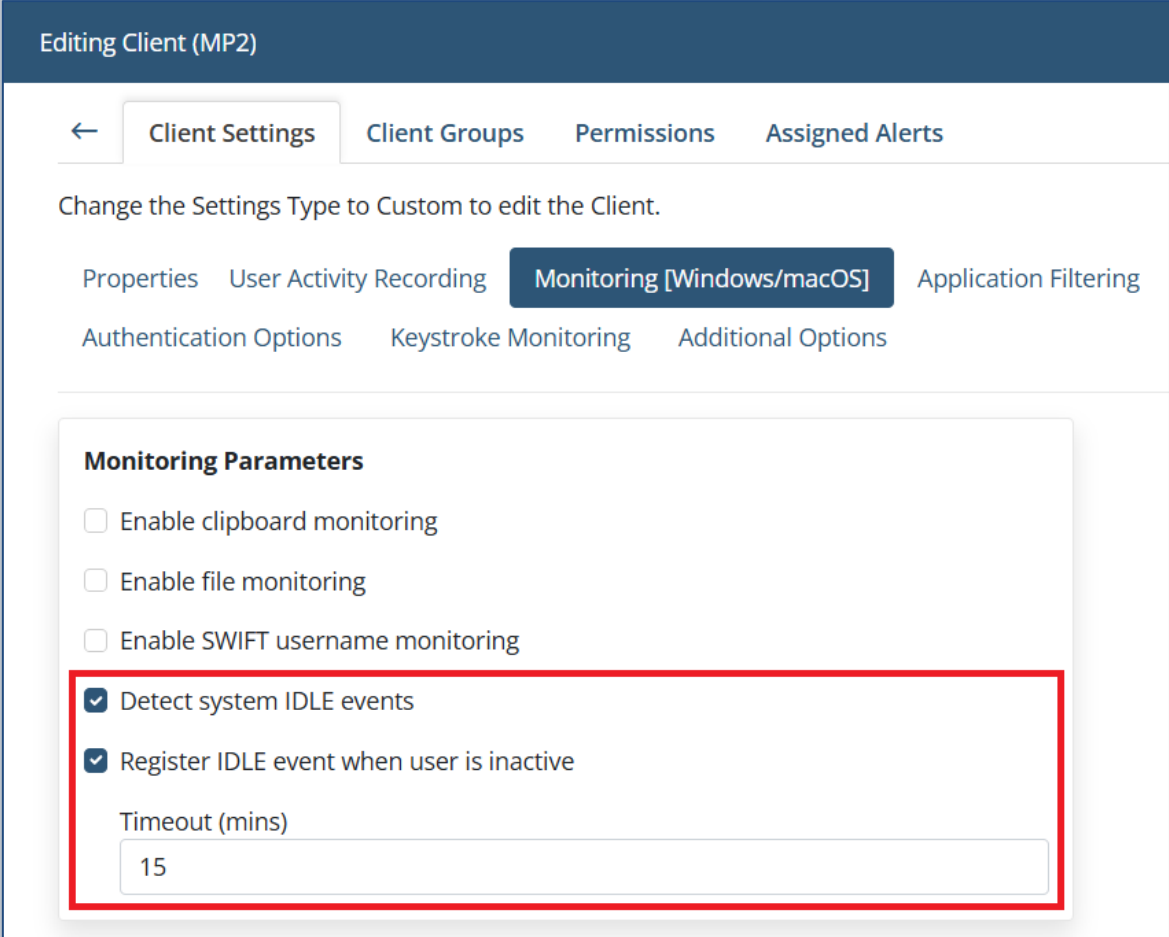
The screenshot shows the 'Editing Client (MP2)' interface for a client named 'localhost'. The 'Client Settings' tab is active, displaying a navigation bar with 'Client Settings', 'Client Groups', 'Permissions', and 'Assigned Alerts'. Below the navigation bar, a message states: 'Change the Settings Type to Custom to edit the Client.' The 'Monitoring [Windows/macOS]' tab is selected, showing sub-tabs for 'Properties', 'User Activity Recording', 'Monitoring [Windows/macOS]', 'Monitoring Time Filtering', 'Remote Host IP Filtering', and 'Authentication'. The 'Monitoring Parameters' section contains the following options:

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

Below these options is a 'Timeout (min)' input field with the value '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 (MP2)

← Client Settings Client Groups Permissions Assigned Alerts

Change the Settings Type to Custom to edit the Client.

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

Authentication Options Keystroke Monitoring Additional Options

Monitoring Parameters

- ☐ Enable clipboard monitoring
- ☐ Enable file monitoring
- ☐ 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 (TW-WS22)

localhost

← Client Settings Client Groups Permissions Assigned Alerts

Change the Settings Type to Custom to edit the Client.

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

Authentication Options Keystroke Monitoring Additional Options

User Filtering

Filter state

Monitor only the activity of selected users

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

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

+ Add

\admin,mydomain\privileged_user

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.

Editing Client (MP2)

← Client Settings Client Groups Permissions Assigned Alerts

Change the Settings Type to Custom to edit the Client.

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

Additional Options

Screen capture throttling (ms)
2000

Batch registration timeout (ms)
10000

Prevent loading hooks into the following applications
WINWORD;EXCEL

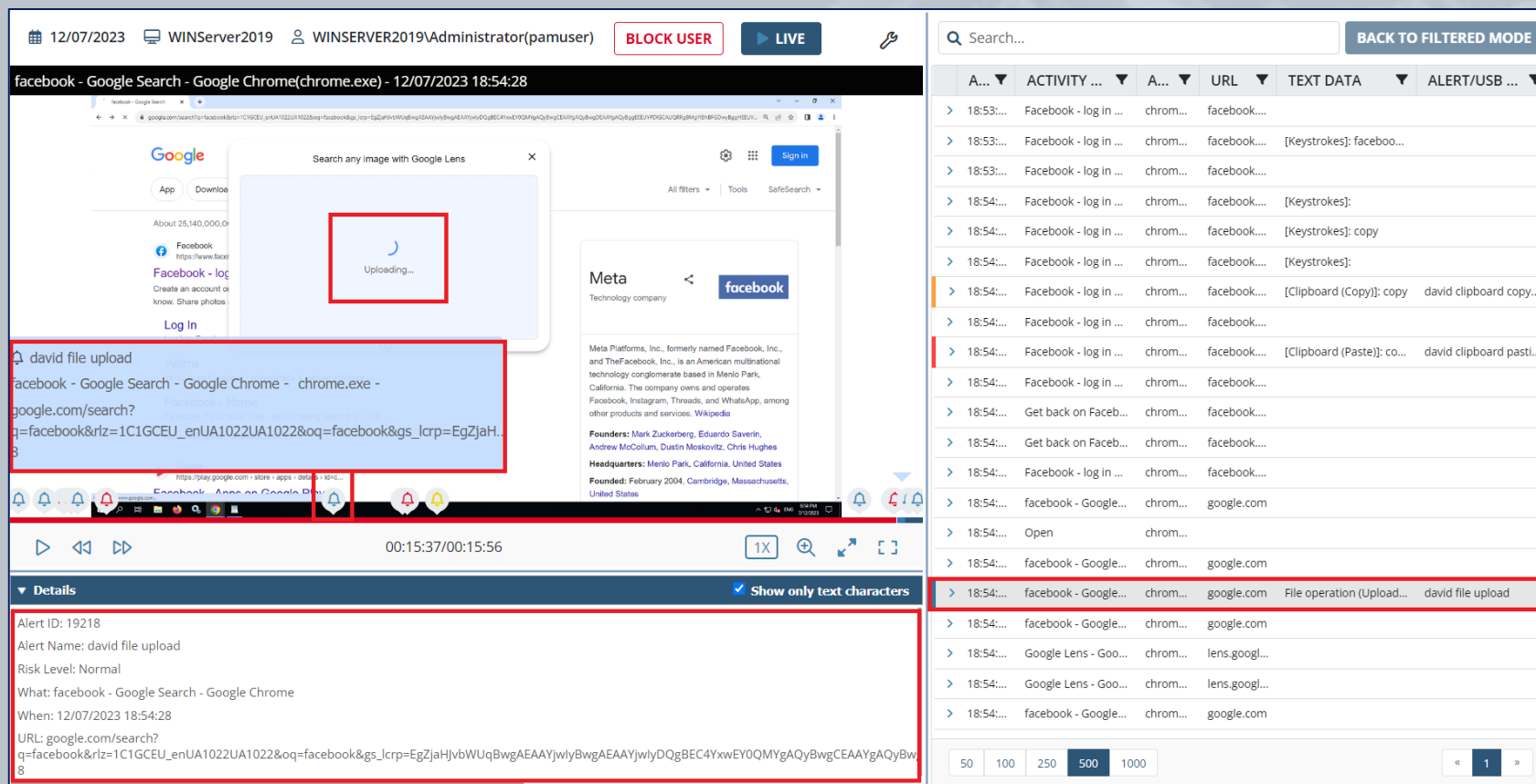
Reduce screen capture size by (%)
30

Screenshot compression level (1-19)
9

Agent memory limit (0-disabled)
0

Next Finish

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



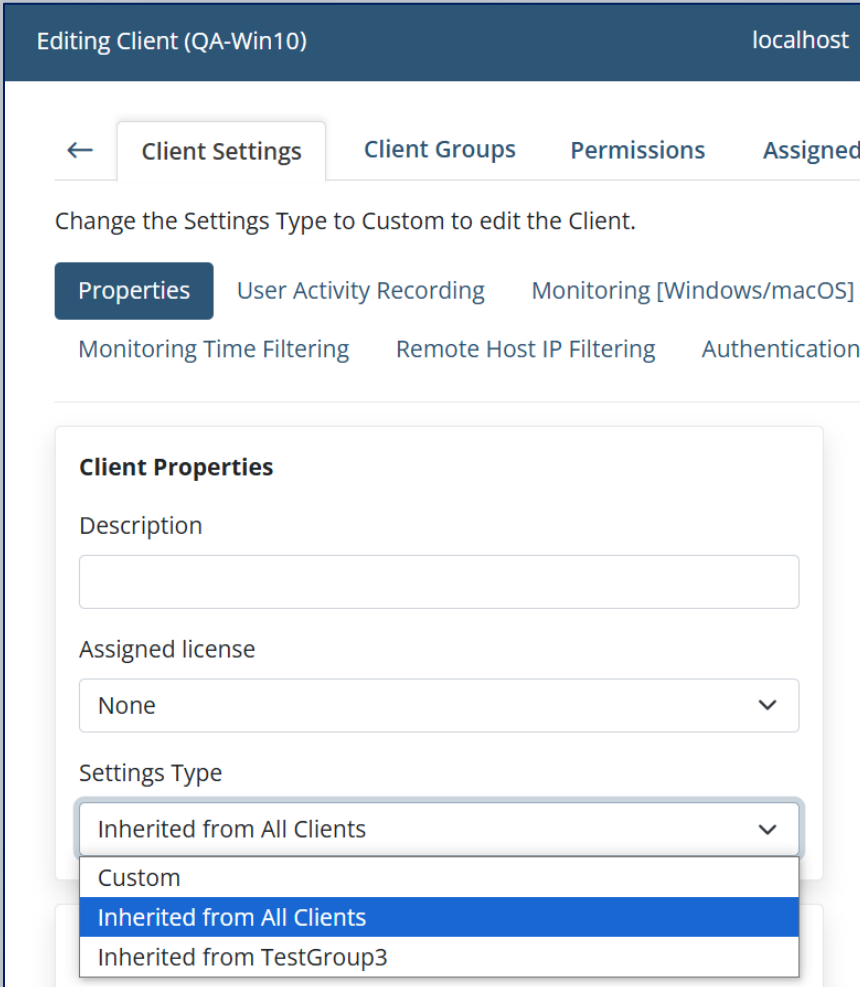
The screenshot displays the Syteca File Monitoring interface. The top bar shows the date and time (12/07/2023 18:54:28), the user (WINServer2019\Administrator(pamuser)), and buttons for 'BLOCK USER' and 'LIVE'. The main window shows a Google search for 'facebook' in Google Chrome. A red box highlights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

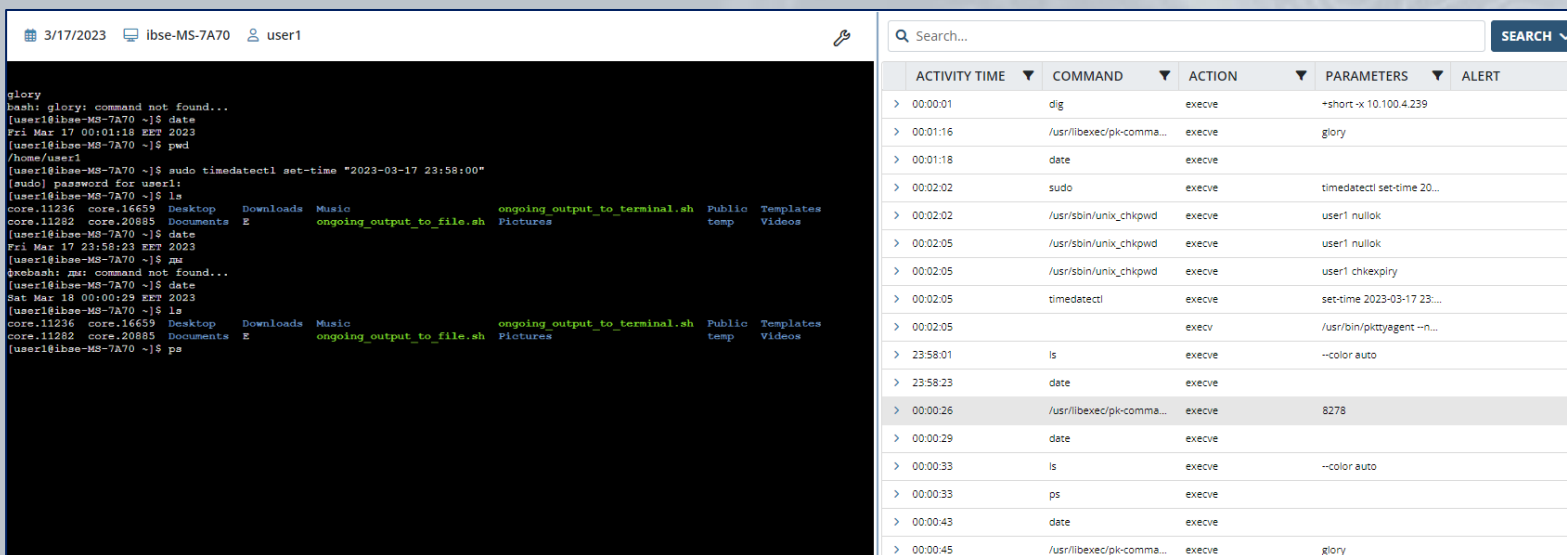
A...	ACTIVITY ...	A...	URL	TEXT DATA	ALERT/USB ...
> 18:53:...	Facebook - log in ...	chrom...	facebook...		
> 18:53:...	Facebook - log in ...	chrom...	facebook...	[Keystrokes]: faceboo...	
> 18:53:...	Facebook - log in ...	chrom...	facebook...		
> 18:54:...	Facebook - log in ...	chrom...	facebook...	[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.



The screenshot shows the 'Editing Client (QA-Win10)' interface on a 'localhost' environment. The top navigation bar includes a back arrow, 'Client Settings' (active), 'Client Groups', 'Permissions', and 'Assigned'. Below the navigation, a message states: 'Change the Settings Type to Custom to edit the Client.' The 'Properties' tab is selected, with other tabs for 'User Activity Recording', 'Monitoring [Windows/macOS]', 'Monitoring Time Filtering', 'Remote Host IP Filtering', and 'Authentication'. The 'Client Properties' section contains a 'Description' text field, an 'Assigned license' dropdown menu (currently set to 'None'), and a 'Settings Type' dropdown menu. The 'Settings Type' dropdown is open, showing four options: 'Inherited from All Clients' (selected), 'Custom', 'Inherited from All Clients', and 'Inherited from TestGroup3'.

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.

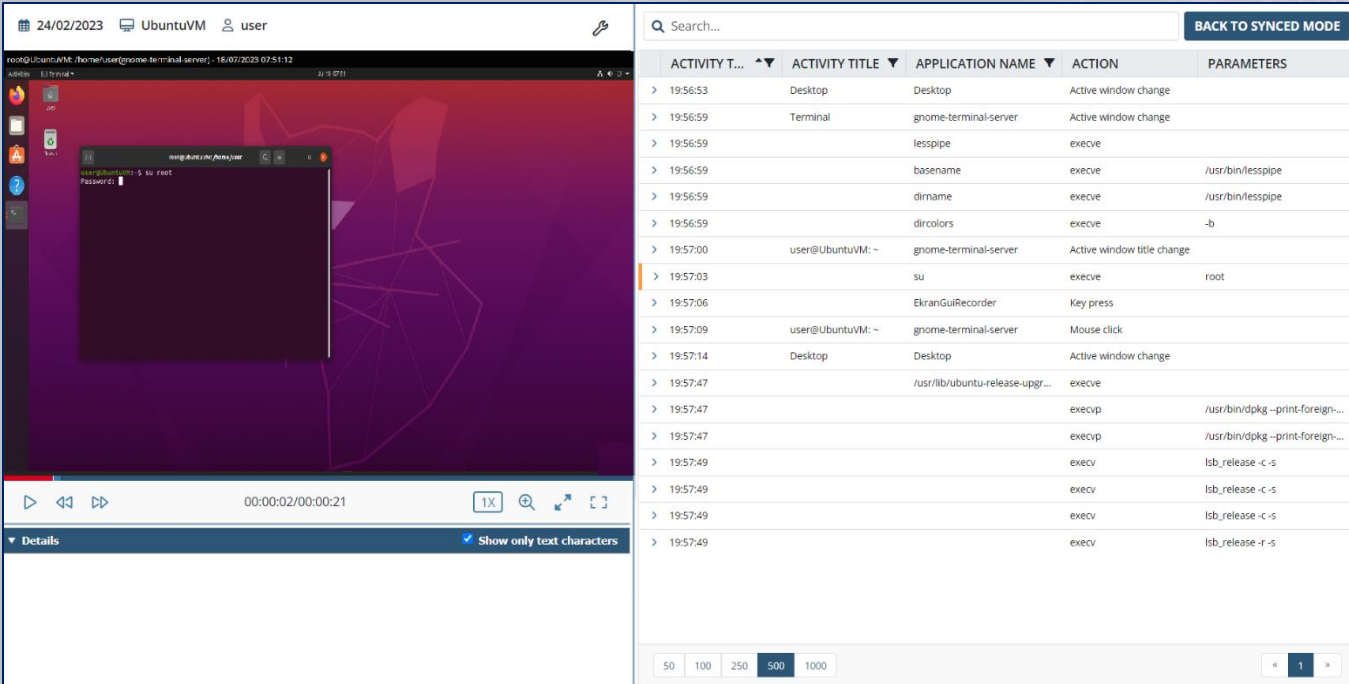


ACTIVITY TIME	COMMAND	ACTION	PARAMETERS	ALERT
> 00:00:01	dig	execve	+short -x 10.100.4.239	
> 00:01:16	/usr/libexec/pk-comm...	execve	glory	
> 00:01:18	date	execve		
> 00:02:02	sudo	execve	timedatectl set-time 20...	
> 00:02:02	/usr/sbin/unix_chkpwd	execve	user1 nullok	
> 00:02:05	/usr/sbin/unix_chkpwd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

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

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





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



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

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

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

<input type="text" value="SEARCH"/> 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

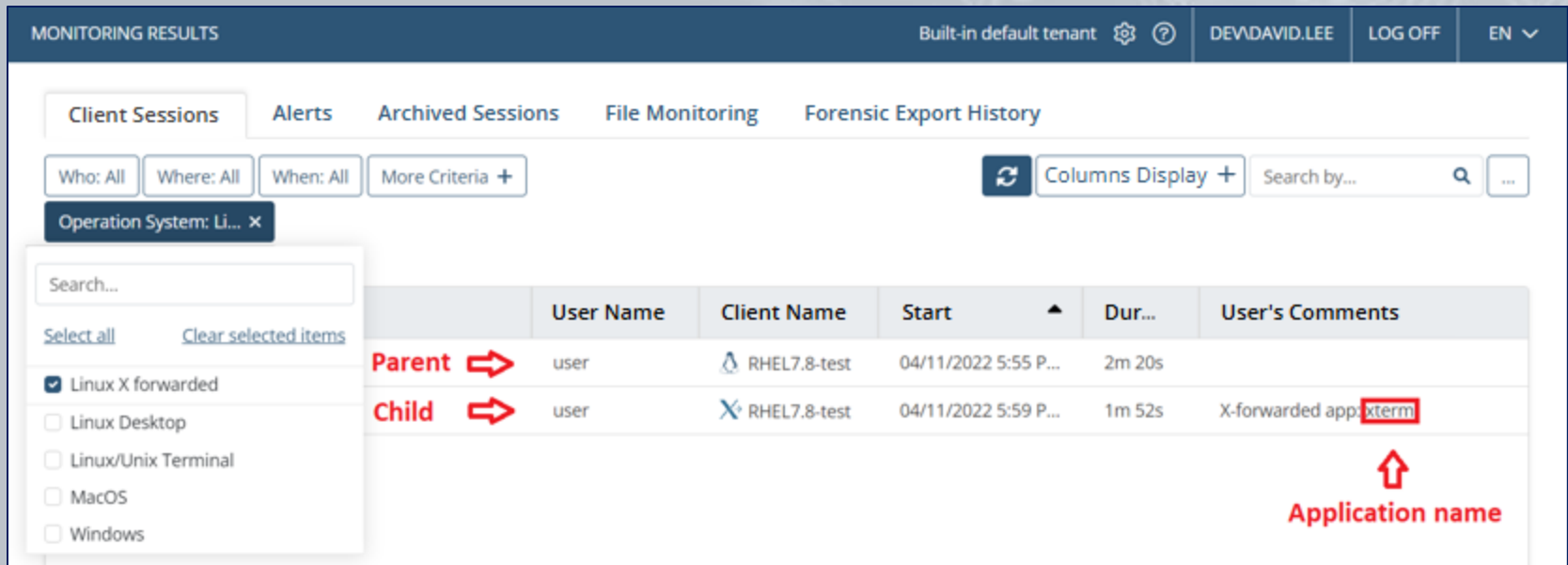
☒ Search in output

☒ 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.



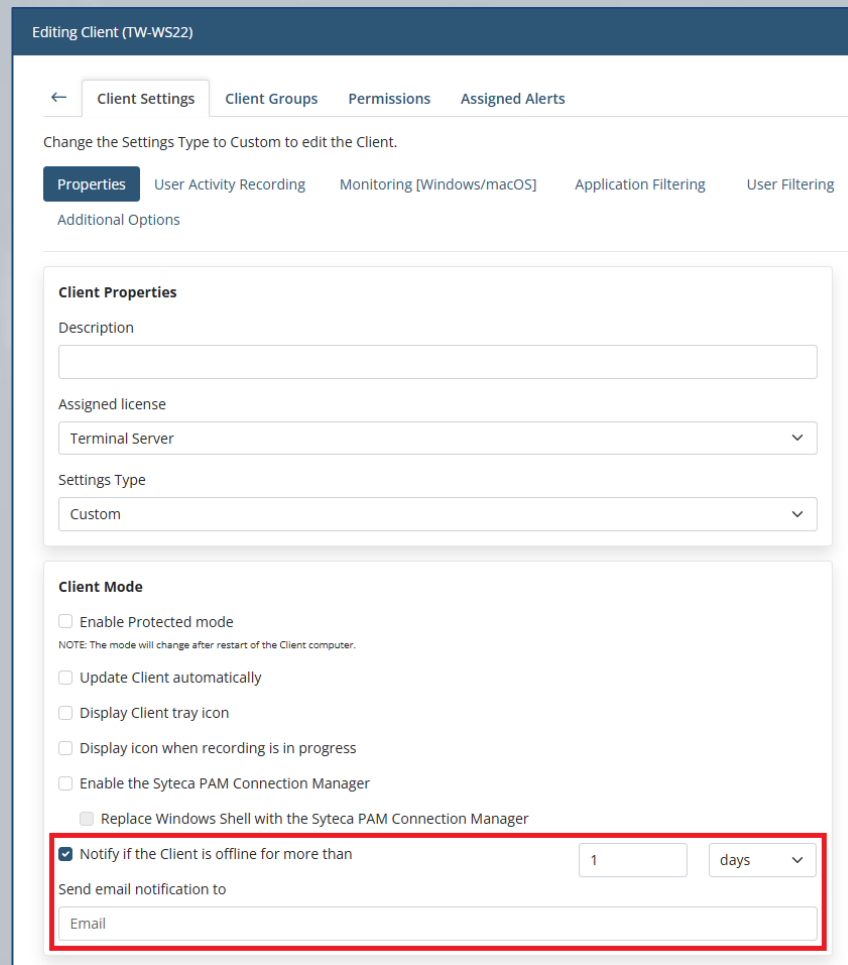
The screenshot displays the 'MONITORING RESULTS' dashboard. At the top, there's a navigation bar with 'Built-in default tenant', user 'DEVDAVID.LEE', and a 'LOG OFF' button. Below this, a tabbed interface shows 'Client Sessions' as the active tab, with other tabs for 'Alerts', 'Archived Sessions', 'File Monitoring', and 'Forensic Export History'. A search bar includes filters for 'Who: All', 'Where: All', 'When: All', and 'More Criteria +'. A 'Columns Display +' button and a 'Search by...' dropdown are also present. A filter for 'Operation System: Li...' is expanded, showing a list of operating systems: Linux X forwarded (checked), Linux Desktop, Linux/Unix Terminal, MacOS, and Windows. The main table lists sessions with columns: 'User Name', 'Client Name', 'Start', 'Dur...', and 'User's Comments'. It shows a 'Parent' session (user, RHEL7.8-test) and a 'Child' session (user, RHEL7.8-test) which is an X-forwarded application named 'xterm'. A red arrow points from the 'xterm' application name to a label 'Application name'.

	User Name	Client Name	Start	Dur...	User's Comments
Parent	user	RHEL7.8-test	04/11/2022 5:55 P...	2m 20s	
Child	user	RHEL7.8-test	04/11/2022 5:59 P...	1m 52s	X-forwarded app: xterm

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 (TW-WS22)

← 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

Additional Options

Client Properties

Description

Assigned license

Terminal Server

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

☐ Display icon when recording is in progress

☐ Enable the Syteca PAM Connection Manager

☐ Replace Windows Shell with the Syteca PAM Connection Manager

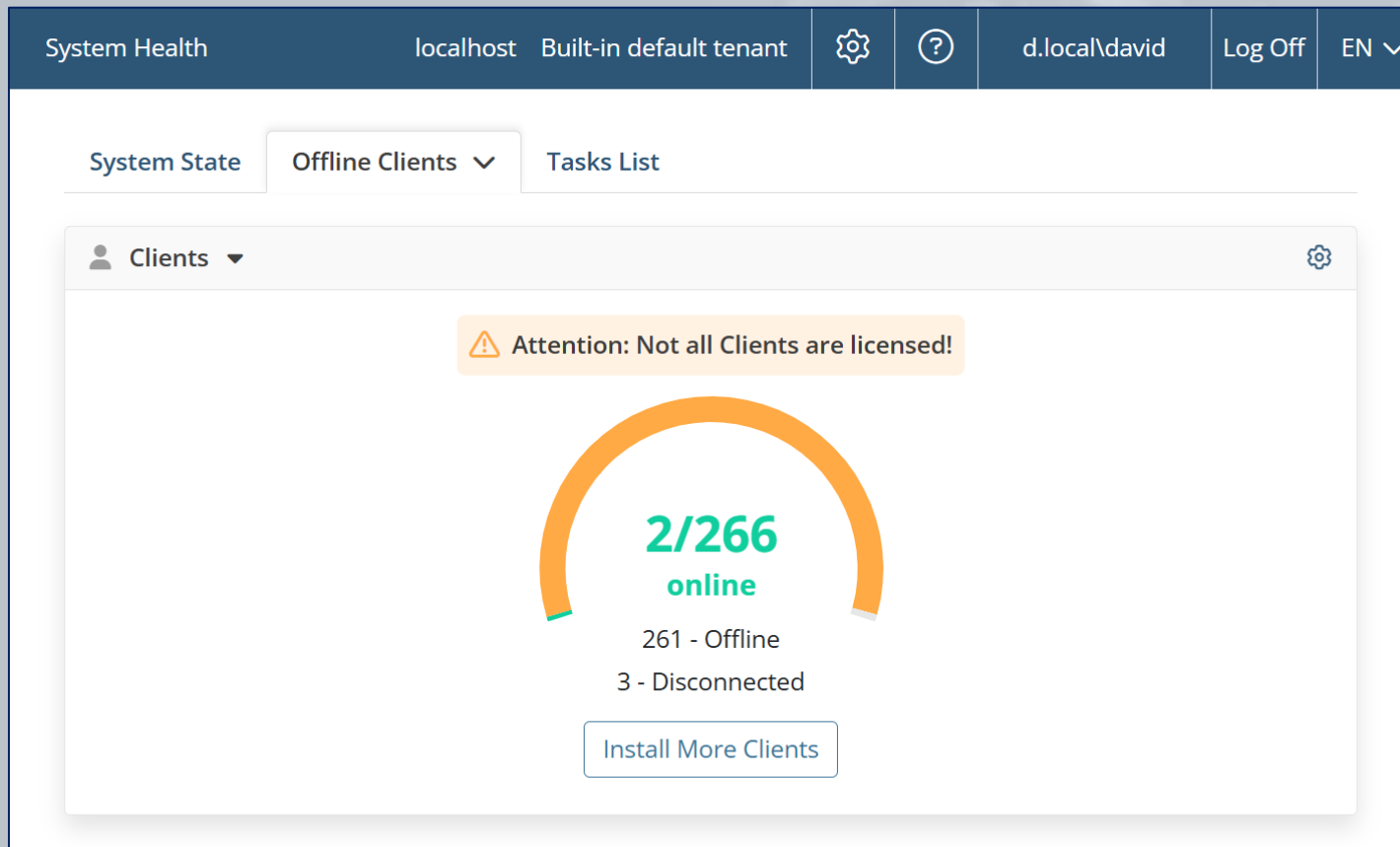
☒ Notify if the Client is offline for more than 1 days

Send email notification to

Email

Viewing Disconnected Clients

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



The screenshot displays the Syteca Enterprise Cybersecurity Platform interface. The top navigation bar includes 'System Health', 'localhost', 'Built-in default tenant', a settings icon, a help icon, the user 'd.local\david', 'Log Off', and 'EN'. Below this, the 'Offline Clients' tab is selected among 'System State' and 'Tasks List'. The main content area shows a 'Clients' section with a warning message: 'Attention: Not all Clients are licensed!'. A large orange arc indicates the client status: 2/266 online, 261 - Offline, and 3 - Disconnected. An 'Install More Clients' button is visible at the bottom.

Status	Count
Online	2
Offline	261
Disconnected	3

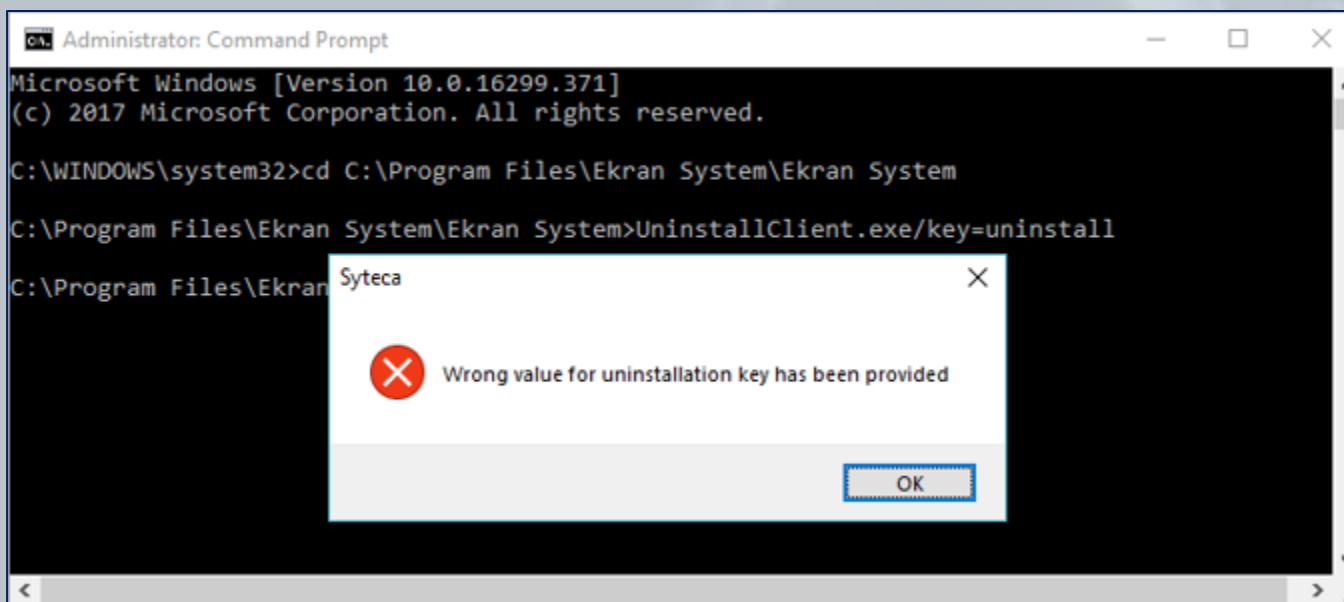
Client Protection

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.

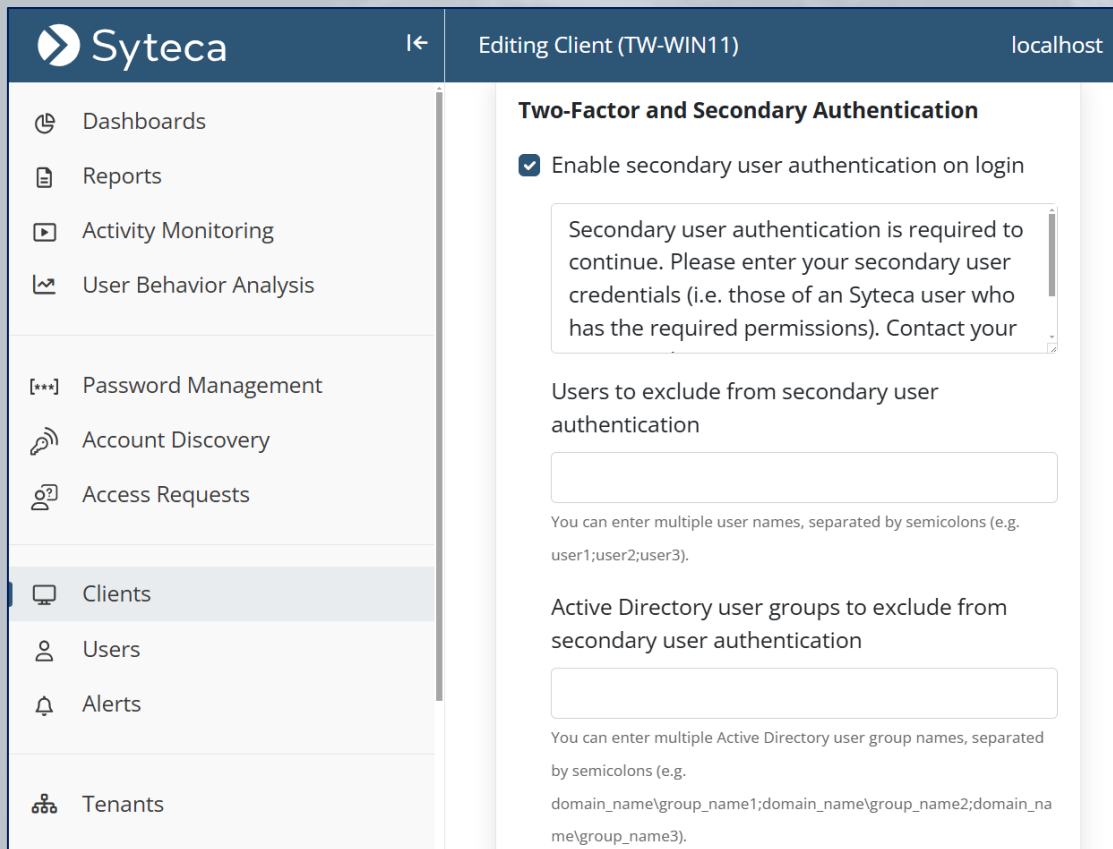


Only the **Syteca administrator** knows the **Uninstallation key** defined prior to Client installation, and which is required for local removal.

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**.



Syteca | Editing Client (TW-WIN11) | localhost

Two-Factor and Secondary Authentication

☒ Enable secondary user authentication on login

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

Users to exclude from secondary user authentication

You can enter multiple user names, separated by semicolons (e.g. user1;user2;user3).

Active Directory user groups to exclude from secondary user authentication


You can enter multiple Active Directory user group names, separated by semicolons (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.

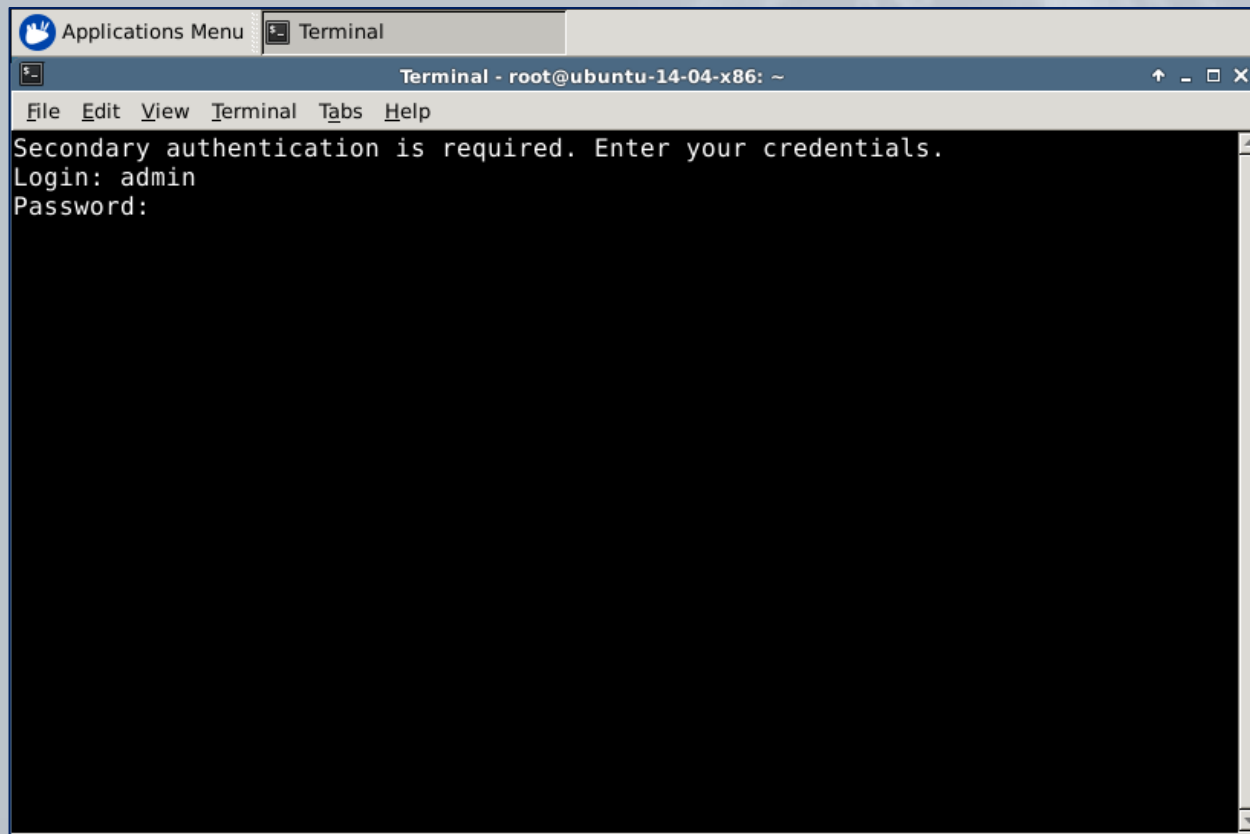
The **user** can **request** a **one-time password** directly **from** the secondary user authentication **window** displayed **during login** to the Windows OS.

A screenshot of the Syteca "REQUEST ONE-TIME PASSWORD" dialog box. The dialog has a white background with a Syteca logo at the top. Below the title bar, there is a dropdown menu with the text "I need emergency access to computer". Below this, a text prompt says "Please enter your email address for the one-time password to be sent to it." followed by an "EMAIL" label and a text input field containing "johnson.kenneth@email.net". Below the email field is a "COMMENT" label and a text area containing "Kenneth Johnson to update the db". At the bottom right, there are two buttons: "Cancel" and "Request". The dialog is overlaid on a blurred background of a Windows login screen.

Secondary User Authentication (Linux Clients)

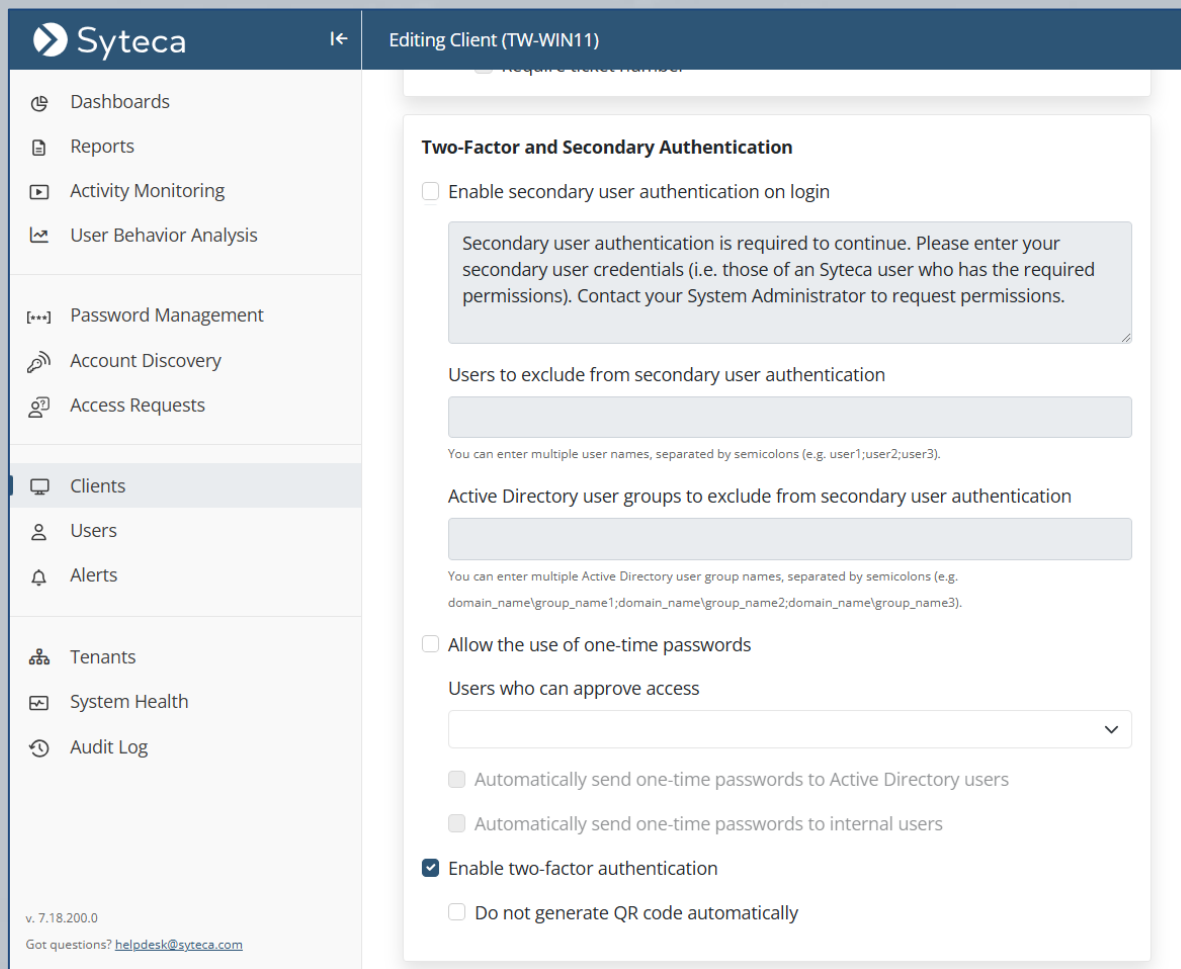


The Syteca Client requests **credentials** to be entered to allow a user to **log on to the terminal** on **Linux** Client computers.



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 (TW-WIN11)

Two-Factor and Secondary Authentication

☐ Enable secondary user authentication on login

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

Users to exclude from secondary user authentication

You can enter multiple user names, separated by semicolons (e.g. user1;user2;user3).

Active Directory user groups to exclude from secondary user authentication

You can enter multiple Active Directory user group names, separated by semicolons (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

v. 7.18.200.0
Got questions? helpdesk@syteca.com

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.

ADD USER

☒ Active Directory user
☐ Local computer user
☐ Syteca user for secondary authentication

Domain:
support.local

User:
Administrator

Key for two-factor authentication:
2AFJG3ICM1

GENERATE

CANCEL SAVE

Syteca

Access Requests

localhost Built-in default tenant admin Log Off EN

Access Requests Two-Factor Authentication Endpoint Access Control

Users who are permitted to log in to Client computers with two-factor authentication enabled.

Search...

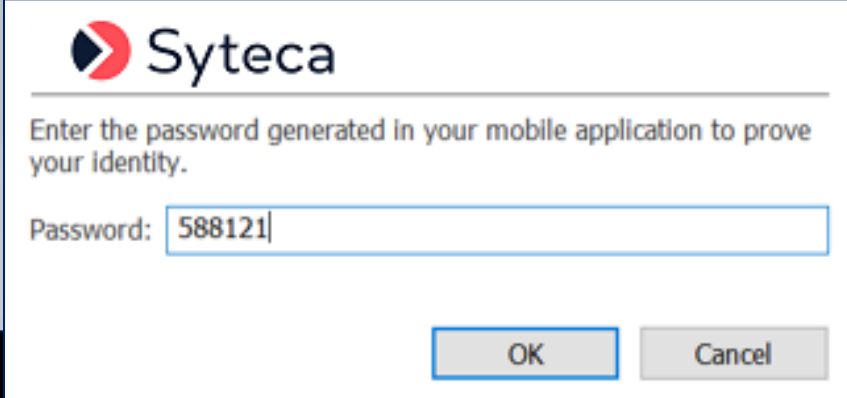
Add

User	User Type	Time Added	Added By	OneTime password	Remove All
Nick	Syteca user for secundar...	02/07/2023 3:07:34 pm	admin		
WIN10\Administrator	Local computer user	02/07/2023 3:06:16 pm	admin		
support.local\alex1	Active Directory user	02/07/2023 3:05:44 pm	admin		

10 30 100 200 500

1

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



The image shows a Syteca authentication dialog box. It features the Syteca logo at the top left. Below the logo, the text reads: "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**.

Editing User (David)

[←](#) [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
David

Password
.....


Confirm password
.....


☒ Enable two-factor authentication on login [RESET 2FA](#)

First name
David

SET UP TWO-FACTOR AUTHENTICATION

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



RECOVERY CODE
PSU52 - DHHBE - QNEFK - VMMSW 

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

[BACK](#) [CONFIRM](#)

Password Management (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**.

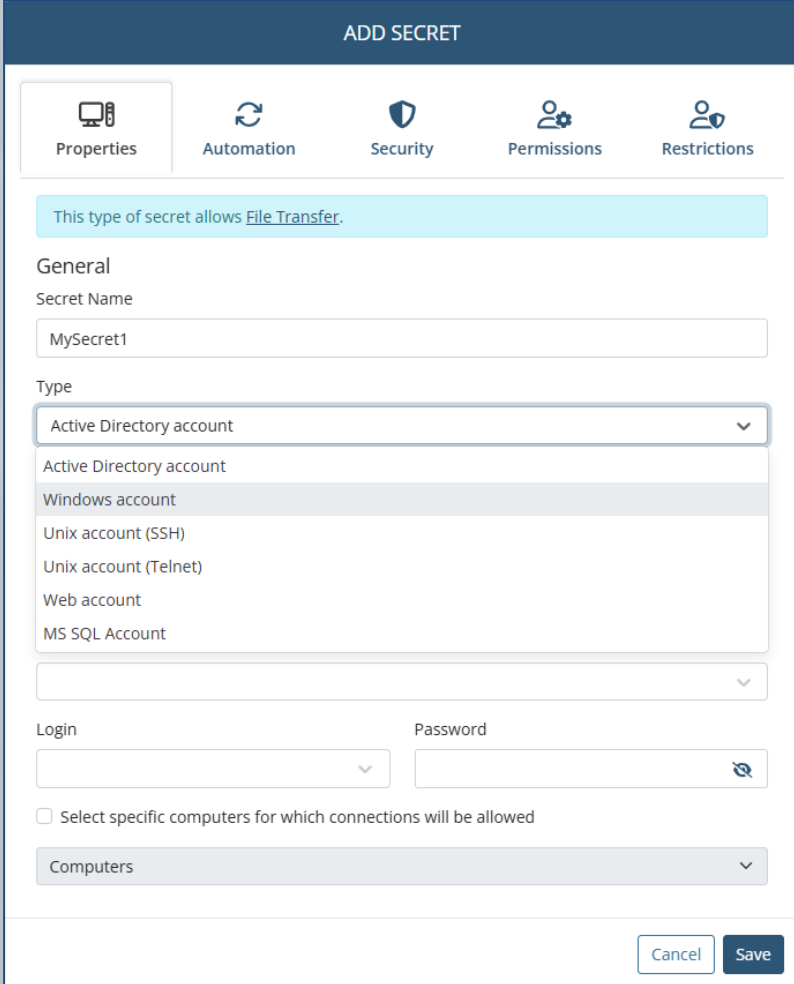
With Syteca, you can:

- 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!



The screenshot shows the 'ADD SECRET' form in the Syteca interface. The form has a dark blue header with the title 'ADD SECRET'. Below the header is a navigation bar with five tabs: 'Properties' (selected), 'Automation', 'Security', 'Permissions', and 'Restrictions'. A light blue banner below the tabs states: 'This type of secret allows [File Transfer](#).' The form is divided into sections: 'General' with a 'Secret Name' field containing 'MySecret1'; 'Type' with a dropdown menu showing 'Active Directory account' and a list of other options: 'Active Directory account', 'Windows account', 'Unix account (SSH)', 'Unix account (Telnet)', 'Web account', and 'MS SQL Account'; 'Login' and 'Password' fields; a checkbox for 'Select specific computers for which connections will be allowed'; and a 'Computers' dropdown menu. At the bottom right are 'Cancel' and 'Save' buttons.

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

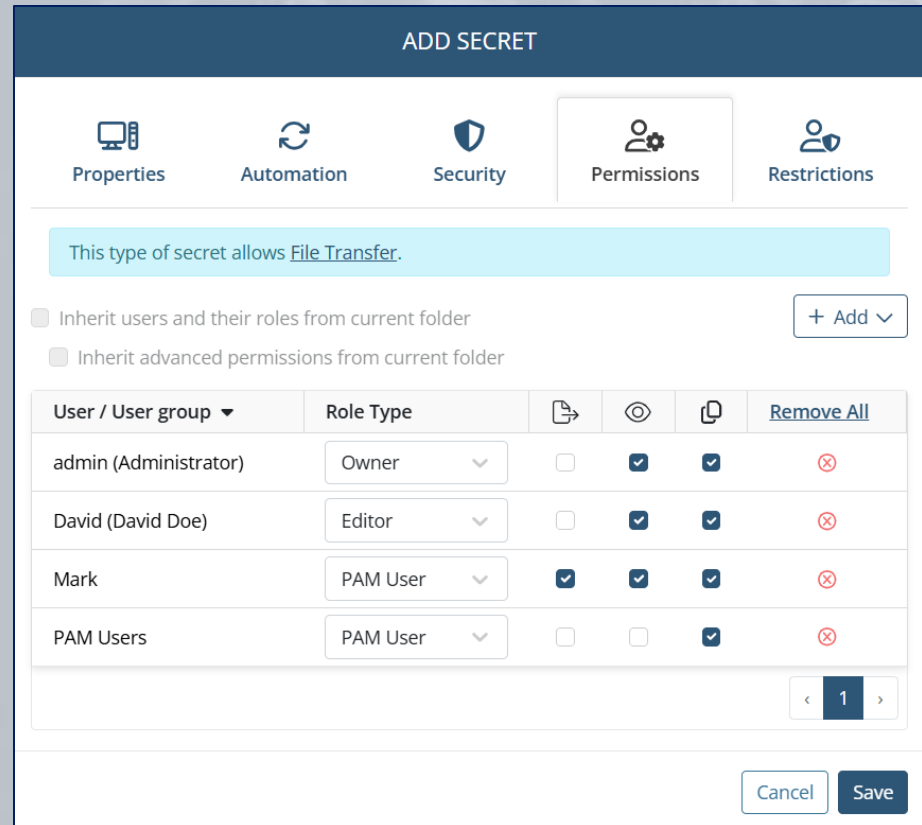
Cancel

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










ADD SECRET

Properties Automation Security **Permissions** Restrictions

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

☐ Inherit users and their roles from current folder + Add ▾

☐ Inherit advanced permissions from current folder

User / User group ▾	Role Type				Remove All
admin (Administrator)	Owner ▾	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
David (David Doe)	Editor ▾	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Mark	PAM User ▾	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
PAM Users	PAM User ▾	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

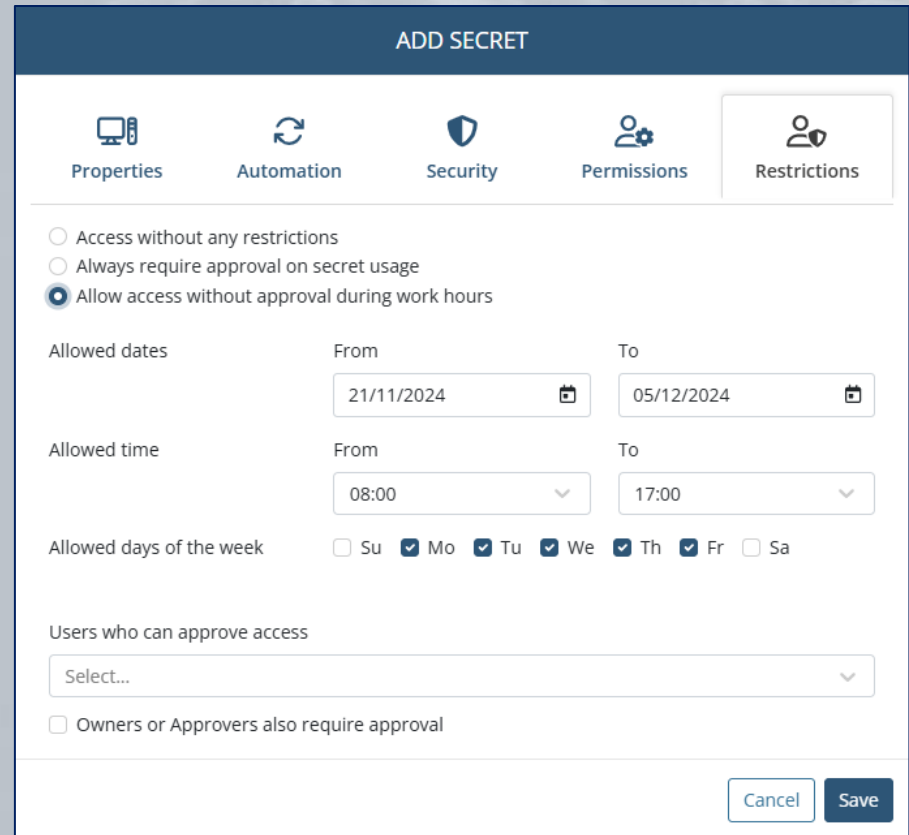
< 1 >

Cancel Save

Adding a Secret (Access Restrictions)

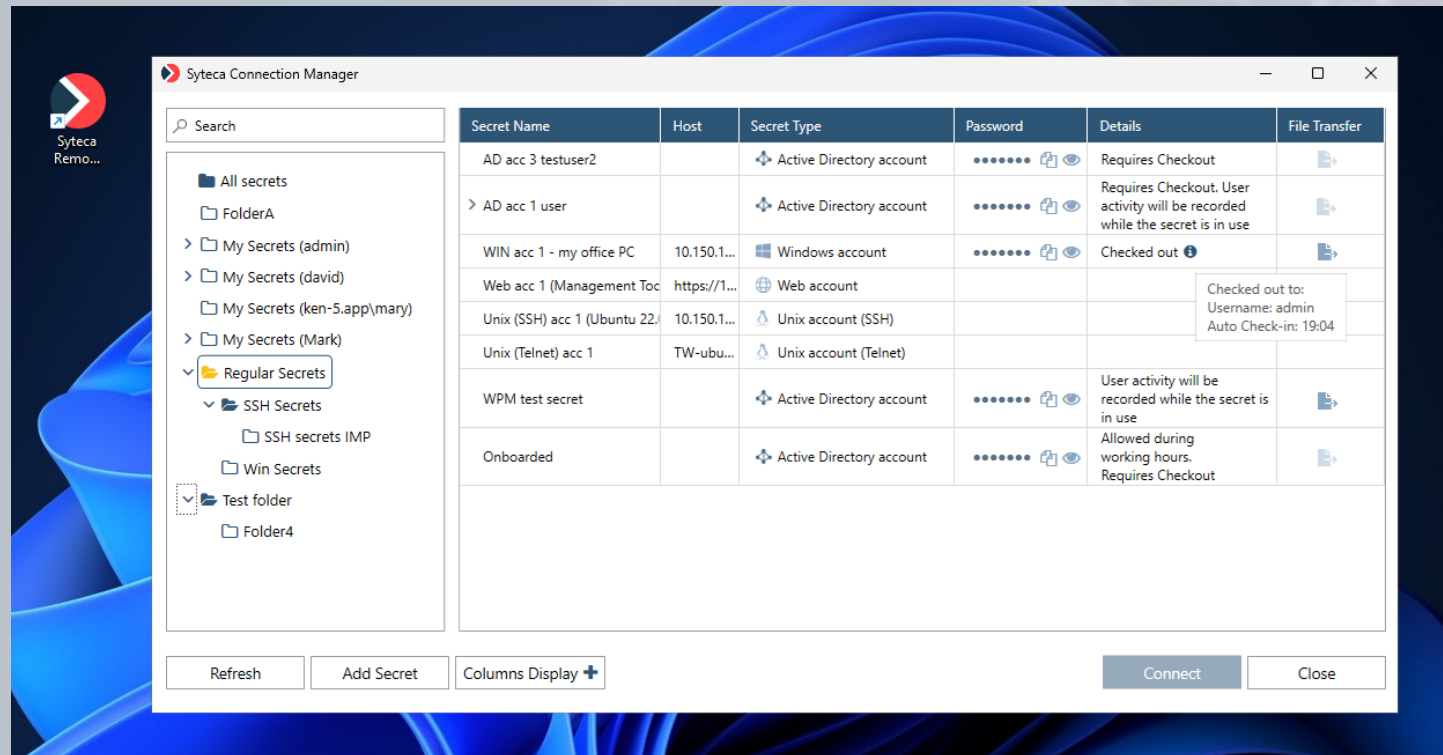
To enhance security still further, **restrict access** to the secret **by requiring approval** from a supervisor:

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



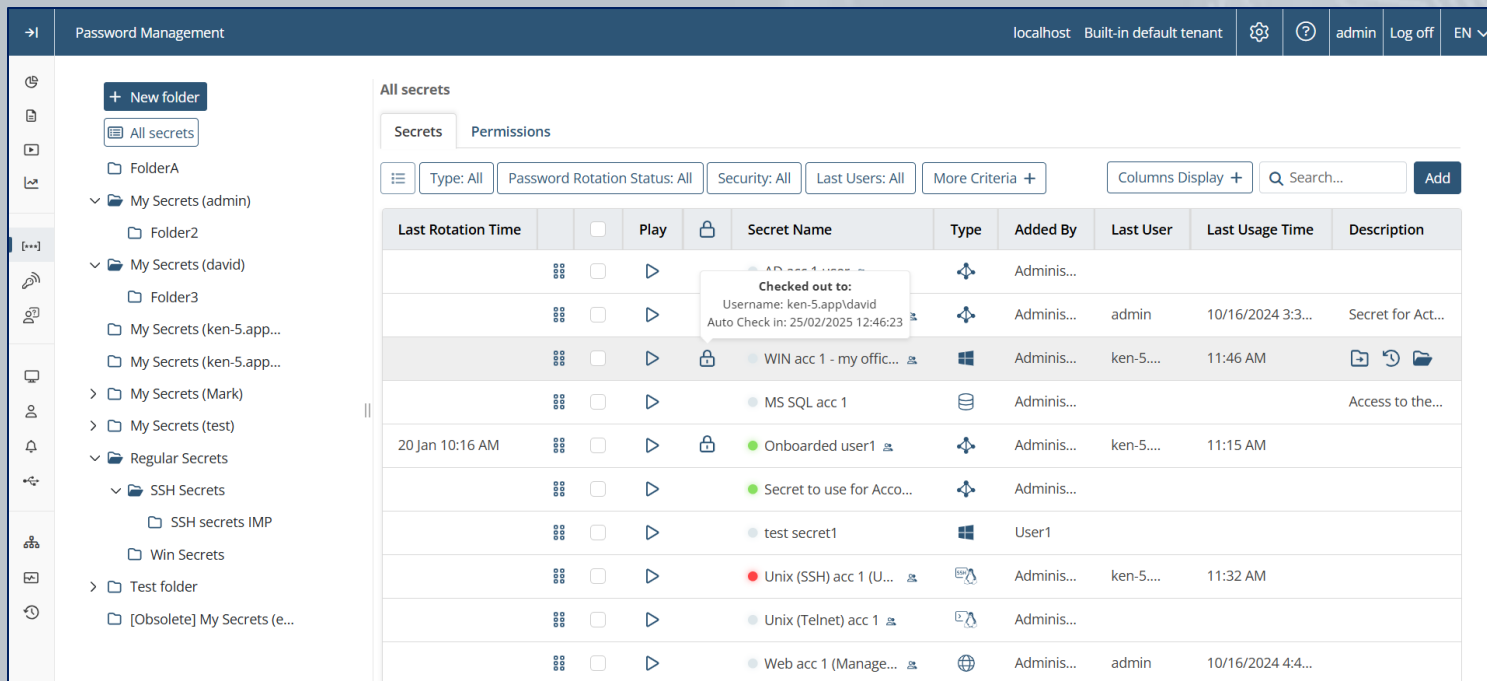
The screenshot shows the 'ADD SECRET' dialog box with the 'Restrictions' tab selected. The dialog has five tabs: Properties, Automation, Security, Permissions, and Restrictions. Under the Restrictions tab, there are three radio button options: 'Access without any restrictions', 'Always require approval on secret usage', and 'Allow access without approval during work hours' (which is selected). Below these are fields for 'Allowed dates' (From: 21/11/2024, To: 05/12/2024), '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 a dropdown menu for 'Users who can approve access' with 'Select...' as the current selection. At the bottom, there is an unchecked checkbox for 'Owners or Approvers also require approval' and two buttons: 'Cancel' and 'Save'.

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



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

You can also **click** e.g. the **Audit** icon (🕒) to see when a secret was **managed and used** (on the Audit Log page).

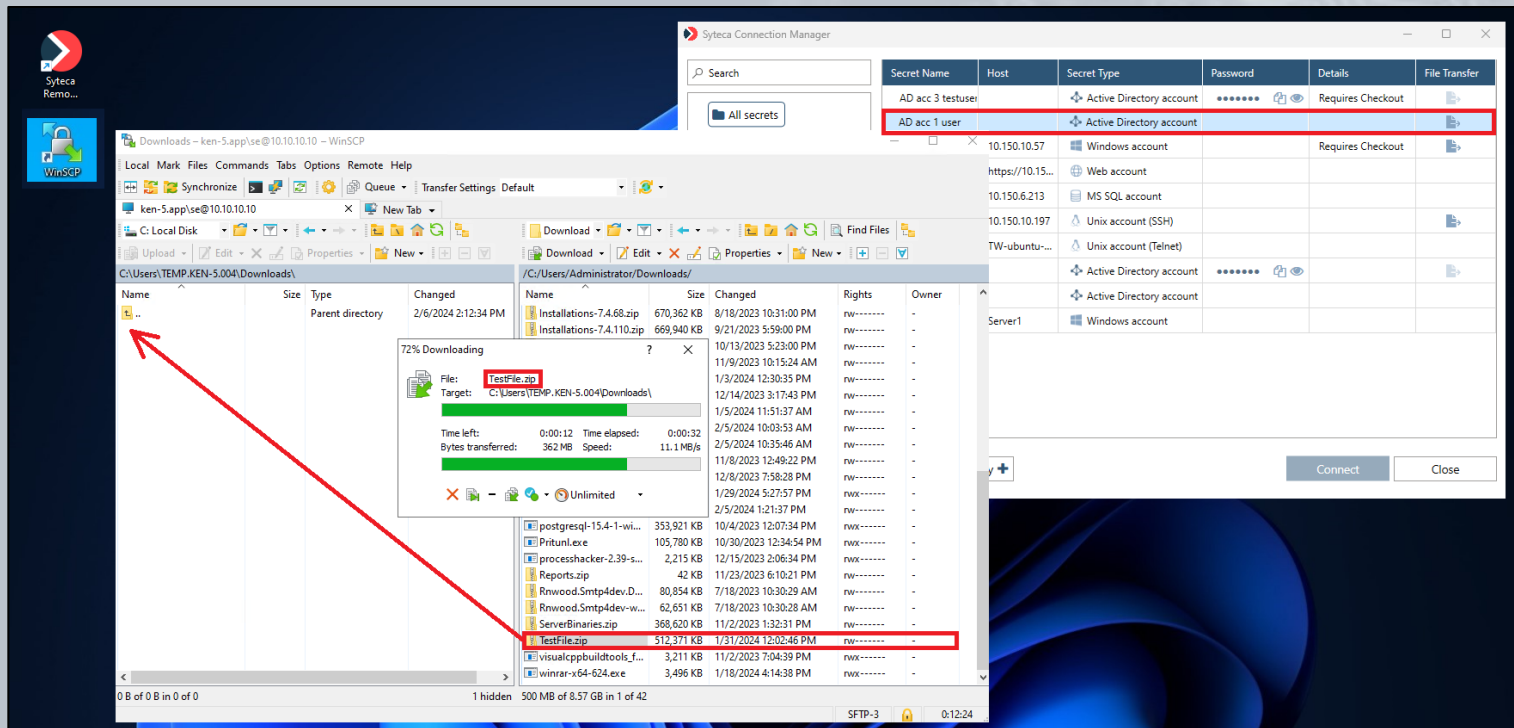


The screenshot displays the Password Management interface. On the left, a sidebar shows a tree view of folders and secrets, including 'My Secrets (admin)', 'My Secrets (david)', 'My Secrets (ken-5.app...)', 'My Secrets (ken-5.app...)', 'My Secrets (Mark)', 'My Secrets (test)', 'Regular Secrets', 'SSH Secrets', 'SSH secrets IMP', 'Win Secrets', 'Test folder', and '[Obsolete] My Secrets (e...'. The main area shows a table of secrets with columns: Last Rotation Time, Play, Secret Name, Type, Added By, Last User, Last Usage Time, and Description. A tooltip is visible over the 'Play' button for the secret 'WIN acc 1 - my offic...'. The tooltip text reads: 'Checked out to: Username: ken-5.app\david, Auto Check in: 25/02/2025 12:46:23'.

Last Rotation Time	Play	Secret Name	Type	Added By	Last User	Last Usage Time	Description
		WIN acc 1 - my offic...	Windows	Adminis...	ken-5....	11:46 AM	
		MS SQL acc 1	Database	Adminis...			Access to the...
20 Jan 10:16 AM		Onboarded user1	User	Adminis...	ken-5....	11:15 AM	
		Secret to use for Acco...	Secret	Adminis...			
		test secret1	Secret	User1			
		Unix (SSH) acc 1 (U...	SSH	Adminis...	ken-5....	11:32 AM	
		Unix (Telnet) acc 1	Telnet	Adminis...			
		Web acc 1 (Manage...	Web	Adminis...	admin	10/16/2024 4:4...	

Transferring Files Using WinSCP

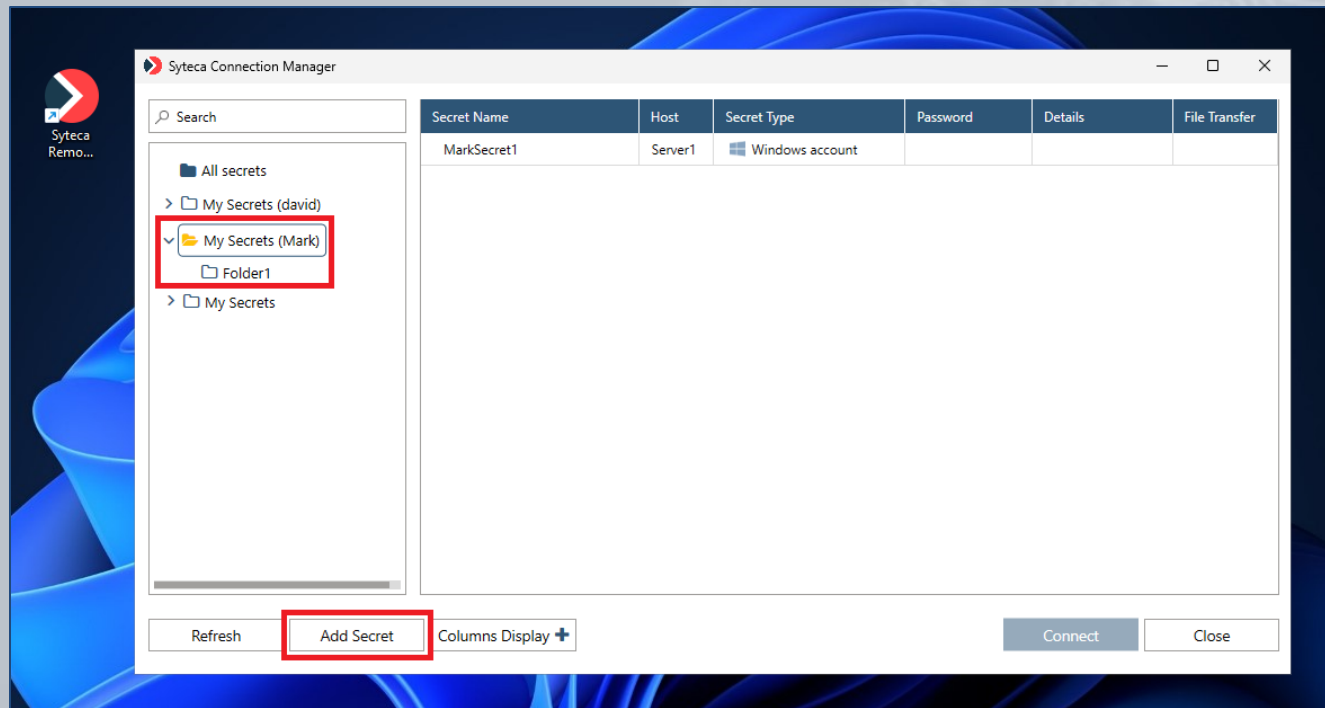
The **File Transfer** functionality allows users of secrets to transfer files **between the computer** with the Syteca Connection Manager and **the remote computers** (which are accessed via the secrets) by using the **WinSCP** application.



Workforce Password Management (WPM)



The WPM functionality enables PAM users (i.e. any **users of the 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).

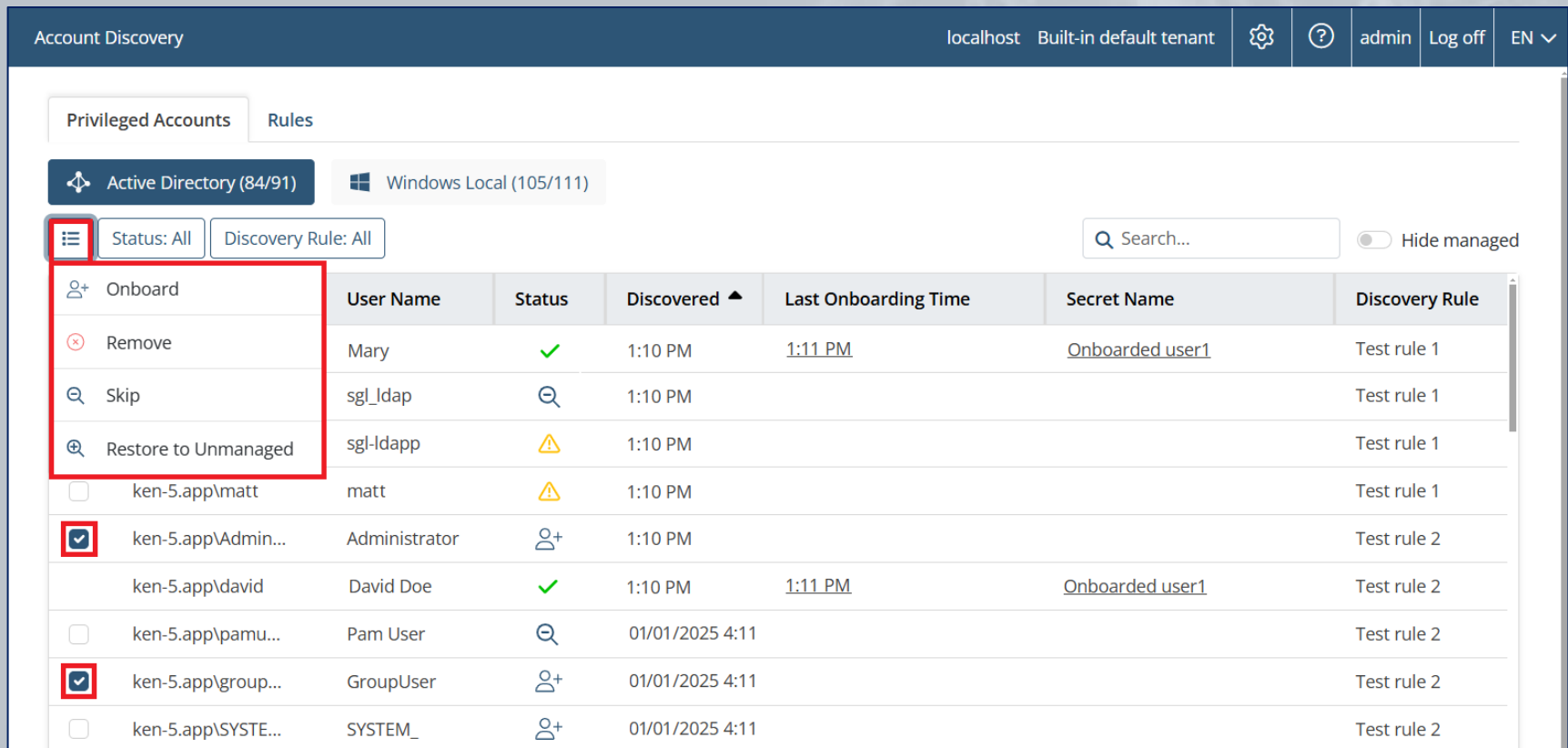


Account Discovery and Onboarding (PAM)

Account Discovery (PAM) allows Active Directory and Window local **accounts to be discovered** by performing a **network scan**, and then **onboarded them into secrets**, by first **adding and running** account discovery **rules**.

[illegible]

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



Account Discovery

localhost Built-in default tenant admin Log off EN

Privileged Accounts Rules

Active Directory (84/91) Windows Local (105/111)

Status: All Discovery Rule: All Search... Hide managed

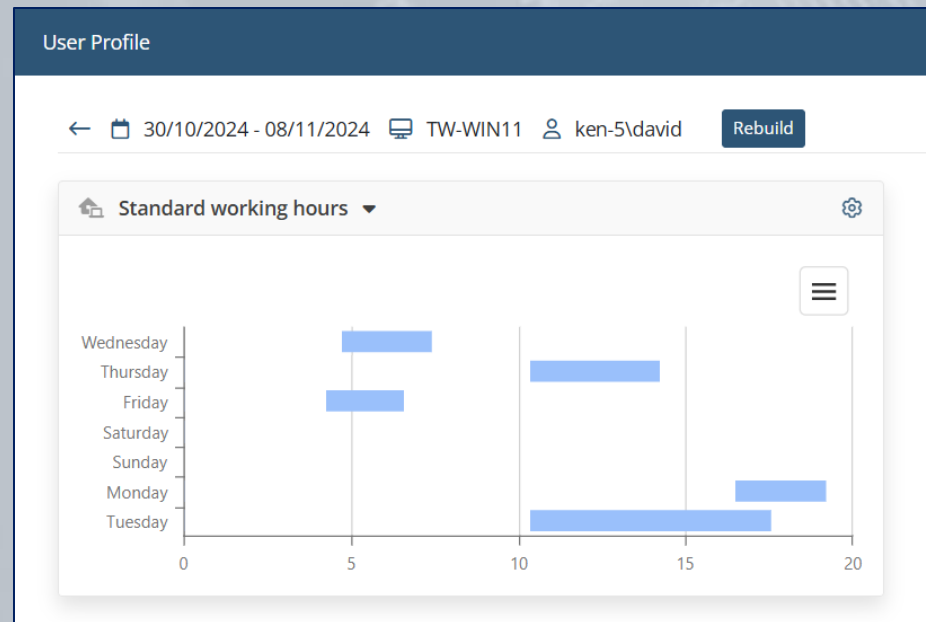
	User Name	Status	Discovered	Last Onboarding Time	Secret Name	Discovery Rule
<input type="checkbox"/>	Mary	✓	1:10 PM	1:11 PM	Onboarded user1	Test rule 1
<input type="checkbox"/>	sgl_ldap	🔍	1:10 PM			Test rule 1
<input type="checkbox"/>	sgl-ldapp	⚠️	1:10 PM			Test rule 1
<input type="checkbox"/>	ken-5.app\matt	⚠️	1:10 PM			Test rule 1
<input checked="" type="checkbox"/>	ken-5.app\Administrator	👤+	1:10 PM			Test rule 2
<input type="checkbox"/>	ken-5.app\david	✓	1:10 PM	1:11 PM	Onboarded user1	Test rule 2
<input type="checkbox"/>	ken-5.app\pamu...	🔍	01/01/2025 4:11			Test rule 2
<input checked="" type="checkbox"/>	ken-5.app\group...	👤+	01/01/2025 4:11			Test rule 2
<input type="checkbox"/>	ken-5.app\SYSTEM_	👤+	01/01/2025 4:11			Test rule 2

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.

Add Rule

Properties

☒ Enable rule

Name

Abnormal behavior1

Description

Conditions

☒ Unusual work hours

High

Email Notifications

☒ Send notification on detected anomalies for a finished session

☐ Send instant notification on detected anomalies

☒ Send total session risk score in case of no anomalies

Send email notification to

admin@example.com

Additional Actions

☒ Show warning message to user

You are performing a forbidden action.

☐ Block user in the current session

FINISH

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

The **risk score** indicates the **severity level** of the session and is calculated according to the risk level of the abnormal user behavior **patterns and alerts** detected during activity monitoring.

Activity Monitoring

Client SessionsAlertsArchived SessionsFile Monitoring

Who: AllWhere: AllWhen: AllMore Criteria +

Total number of sessions: 82

Play	Risk Score	Alerts	User Name	Client Name
			SUPPORT\alex...	WIN-4D1MTM6US...
			WIN-4D1MTM...	WIN-4D1MTM6US...
			WIN-4D1MTM...	WIN-4D1MTM6US...
			WIN-4D1MTM...	WIN-4D1MTM6US...
			WIN-4D1MTM...	WIN-4D1MTM6US...
			WIN-4D1MTM...	WIN-4D1MTM6US...
			WIN-4D1MTM...	WIN-4D1MTM6US...

Access Requests and Approval Workflow

Access Requests and Approval Workflow




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


Access Requests							localhost	Built-in default tenant			d.local\david	Log Off	EN ▾
Access Requests							Two-Factor Authentication						
Endpoint Access Control													
Users who are permitted to log in to Client computers according to a schedule or only after administrator approval.							Add						
							<input type="text" value="Search..."/>						
							Apply Filters						
User ▾	User Type ▾	Assigned To ▾	Restriction Type ▾		Time Added ▾	Added By ▾	Remove All						
ken-2.app\1604	Active Directory user	ken-2.app\pma1604-node1	Email to administrator		02/03/2022 18:36:33	d.lvmatt							
ken-5.app\1604	Active Directory user	ken-5.app\gmkw10	Email to administrator		10/09/2024 13:36:44	anne							
d.local\hal	Syteca user for secondary authentication	ken-5.app\win19-ta	Email to administrator		01/11/2024 15:54:06	dev.local\hal							
ken-5.app\om	Active Directory user	ken-5.app\ompwin11	Access on schedule (14/11/2024 - 28/11/2024, 00:30 - 23:30,)		14/11/2024 19:22:49	dev.local\o.matt							


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.

ADD USER

GENERAL

RESTRICTION TYPES

 **User with Restricted Access Rights**

User type:


Active Directory user

Domain:

ekran-2.app

User / User group:

test


 **Accessed Computer with Installed Client**

Computer Type:

Computers from Client Group

Client group

test

 **Users Who Can Approve Access**

User / User group:

ADMINISTRATORS


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


CANCEL


SAVE



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



ADD USER


GENERAL


RESTRICTION TYPES

**Restriction Type**
☐ Always require approval on login
☒ Allow access without approval during work hours

Allowed dates
From  To 

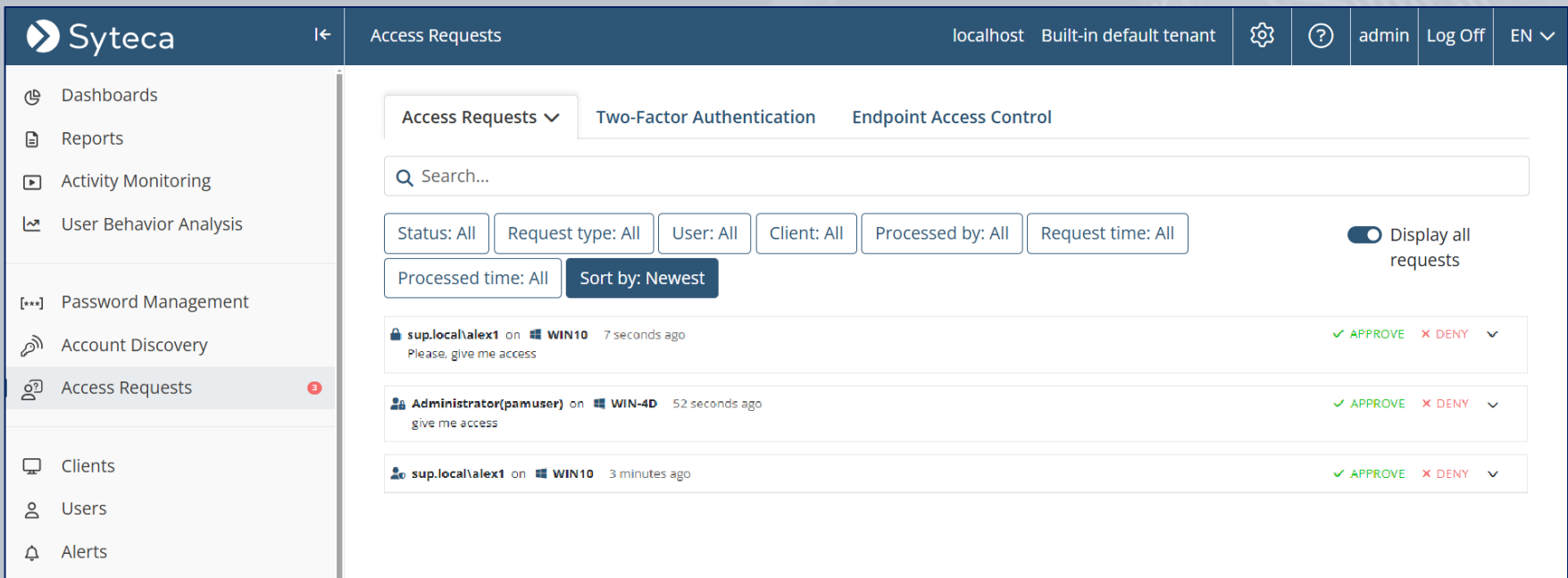
Allowed time
From  To 

Allowed weekdays
☐ Su ☒ Mo ☒ Tu ☒ We ☒ Th ☒ Fr ☐ Sa

CANCEL

SAVE

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



The screenshot shows the Syteca web interface for managing access requests. The left sidebar contains navigation links: Dashboards, Reports, Activity Monitoring, User Behavior Analysis, Password Management, Account Discovery, Access Requests (highlighted with a red notification badge), Clients, Users, and Alerts. The main content area is titled 'Access Requests' and includes tabs for 'Access Requests', 'Two-Factor Authentication', and 'Endpoint Access Control'. A search bar is present above a set of filters: Status: All, Request type: All, User: All, Client: All, Processed by: All, Request time: All, and Processed time: All. A 'Sort by: Newest' button is also available. A toggle switch for 'Display all requests' is on the right. The table below lists three requests:

User	Client	Time	Action
sup.local\alex1	WIN10	7 seconds ago	APPROVE DENY
Administrator(pamuser)	WIN-4D	52 seconds ago	APPROVE DENY
sup.local\alex1	WIN10	3 minutes ago	APPROVE DENY

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.

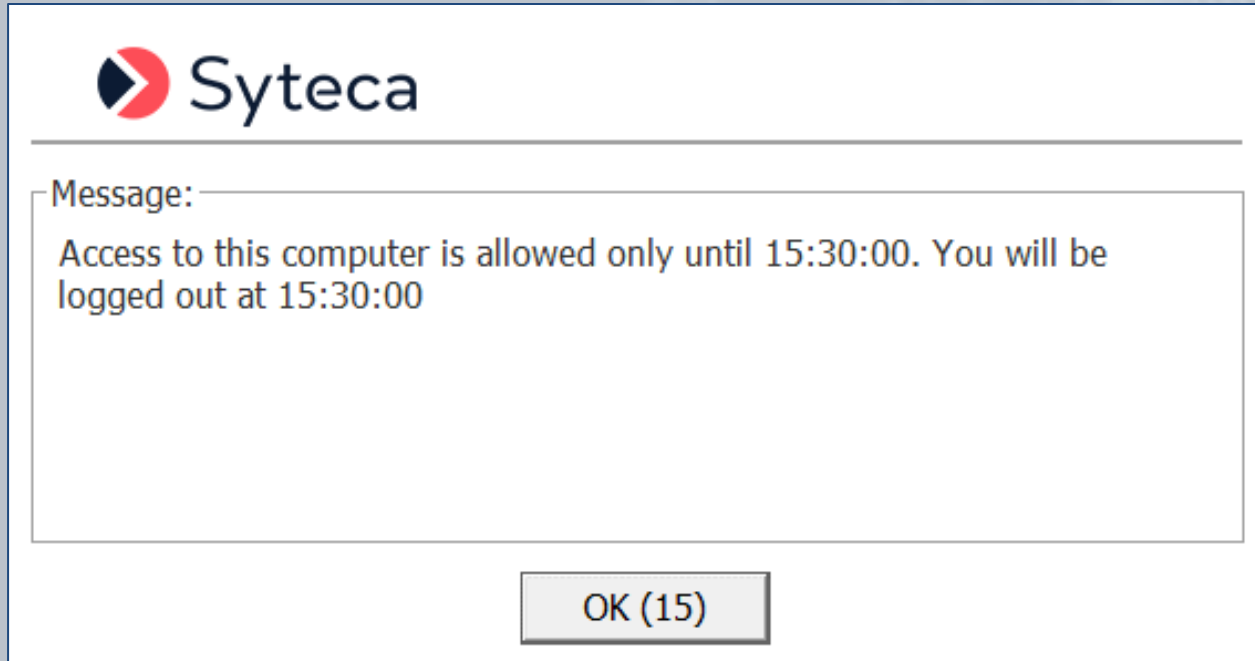
Cancel



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**.

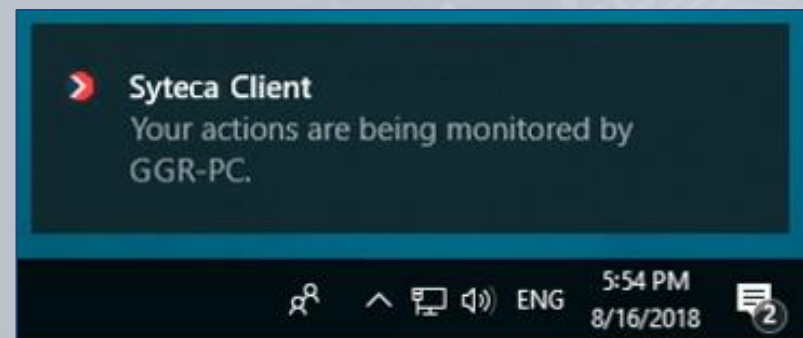
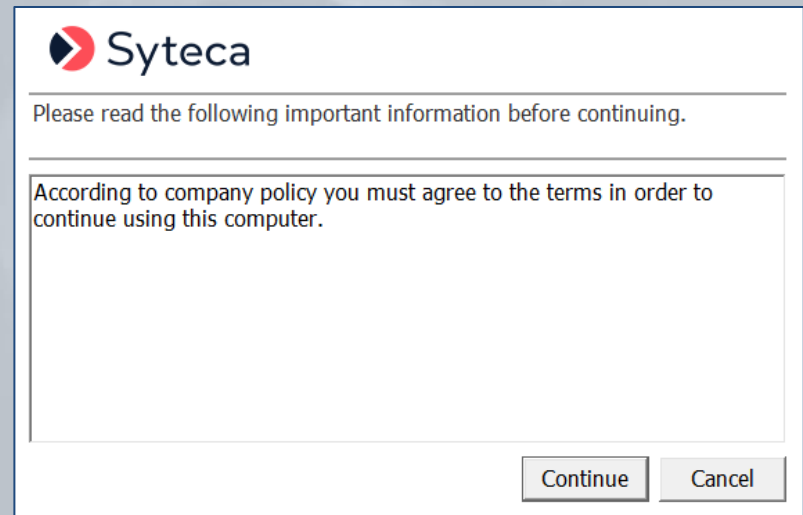


Notifying Users About Being Monitored

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 larger text area with up and down arrow icons on the right side. 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.

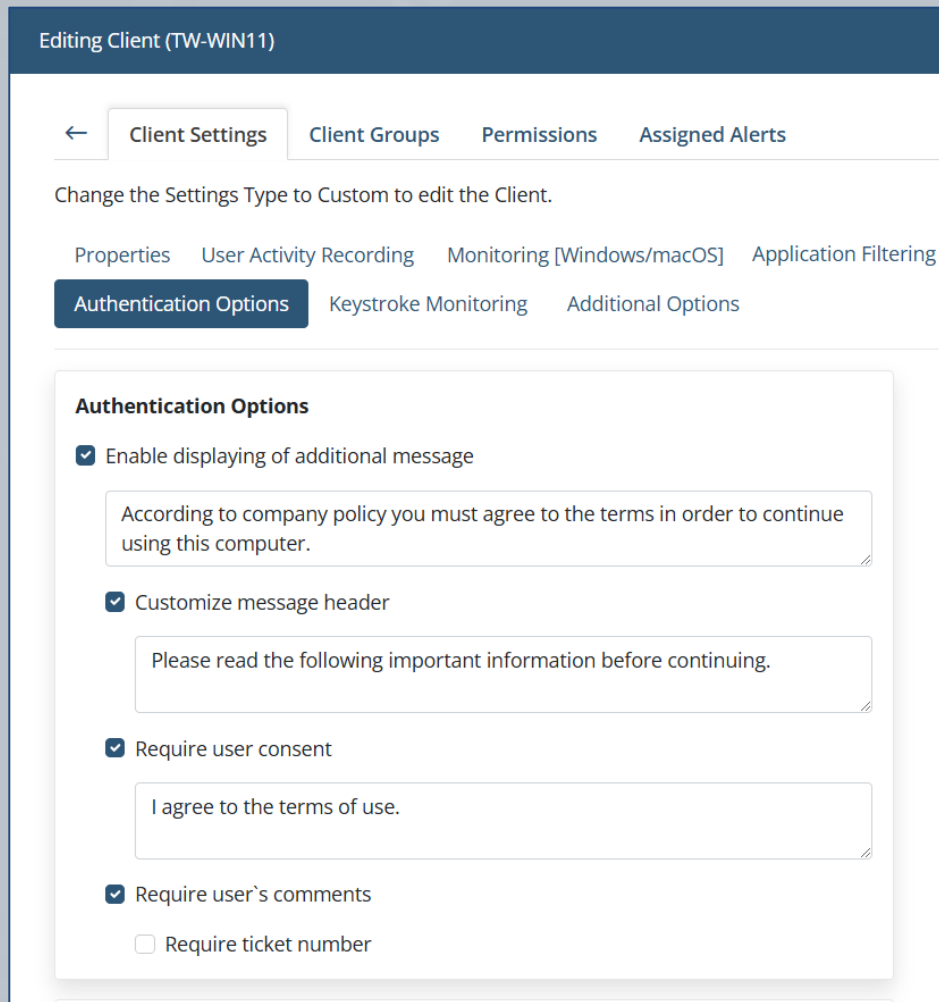
Ticket number is required:

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**.



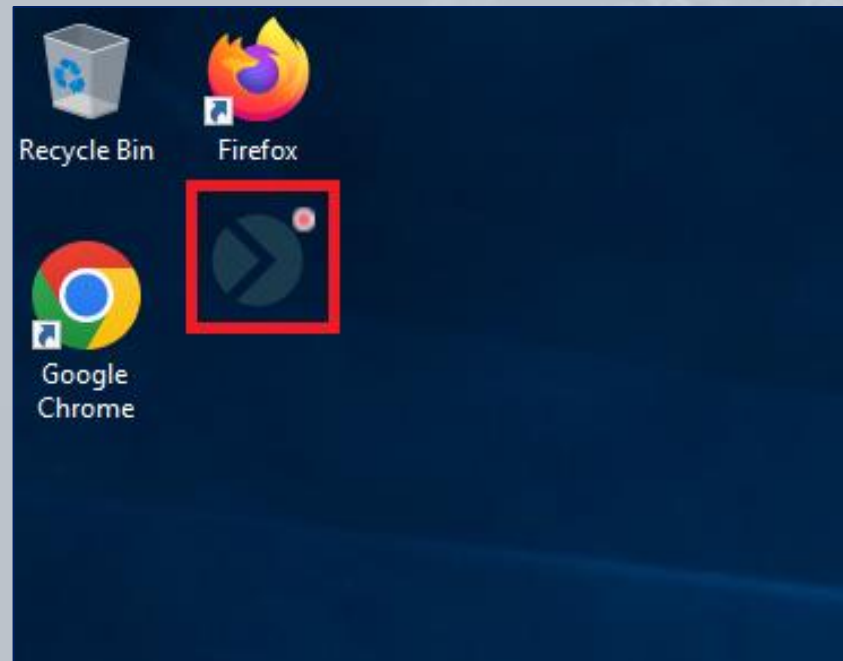
The screenshot shows the 'Editing Client (TW-WIN11)' interface. At the top, there are tabs: 'Client Settings' (selected), 'Client Groups', 'Permissions', and 'Assigned Alerts'. Below the tabs, a message states: 'Change the Settings Type to Custom to edit the Client.' Underneath, there are sub-tabs: 'Properties', 'User Activity Recording', 'Monitoring [Windows/macOS]', 'Application Filtering', 'Authentication Options' (selected), 'Keystroke Monitoring', and 'Additional Options'.

The 'Authentication Options' section contains the following settings:

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

Notifying Users about Being Monitored

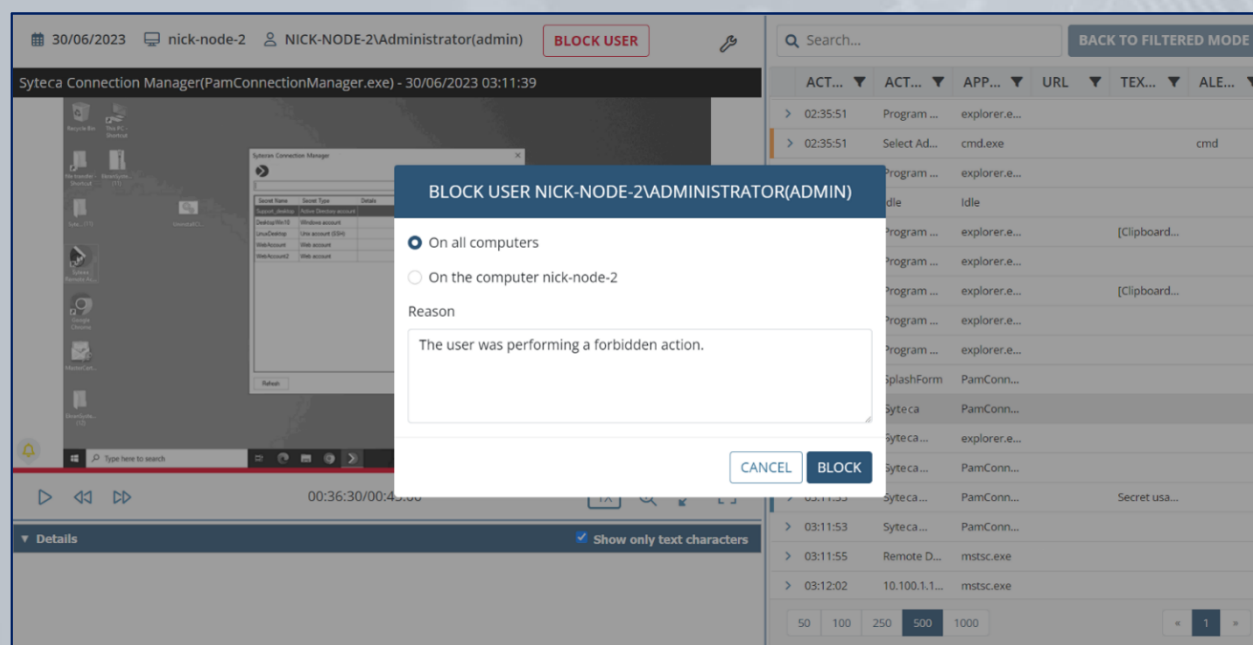
- An **icon** can also be displayed on the desktop (that is always on top of all applications opened) to **inform users** that **their actions** are currently **being monitored and recorded**.



Blocking Users

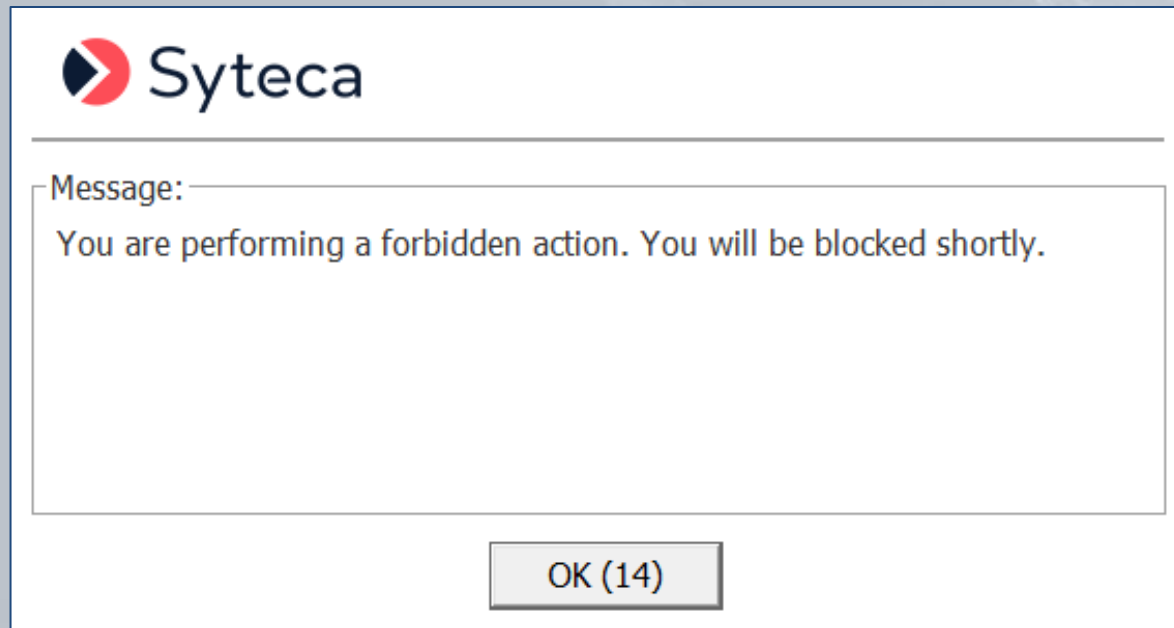
Syteca allows you to **block endpoint users** from performing potentially harmful and forbidden actions on computers running Windows OS with Syteca Clients installed on them.

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					
localhost Built-in default tenant			admin	Log Off	EN
User	Blocked On	Blocked By	Date	Reason	Remove All
WINSERVER2019\Administrator(pamuser)	WINServer2019	admin	13/07/2023 14:07:14 +03:00	The user was performing a forbidden action.	⊗
NICK-NODE-2\Administrator	nick-node-2	admin	13/07/2023 14:08:02 +03:00	The user was performing a forbidden action.	⊗

The accounts of 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**.

LOG IN

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

Use an internal or domain account to log in.

Login

Password

☐ Remember me on this computer

Log in

Users

Search...

ALL USERS:

LOGIN	FIRST NAME	LAST NAME
admin	Administrator	
user1	John	Doe

ADMINISTRATORS: Users with all permissions

LOGIN	FIRST NAME	LAST NAME
admin	Administrator	
user1	John	Doe

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

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

PAM USERS: Group does not have permission to access

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

APPLICATION ACCOUNTS:

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

USER1

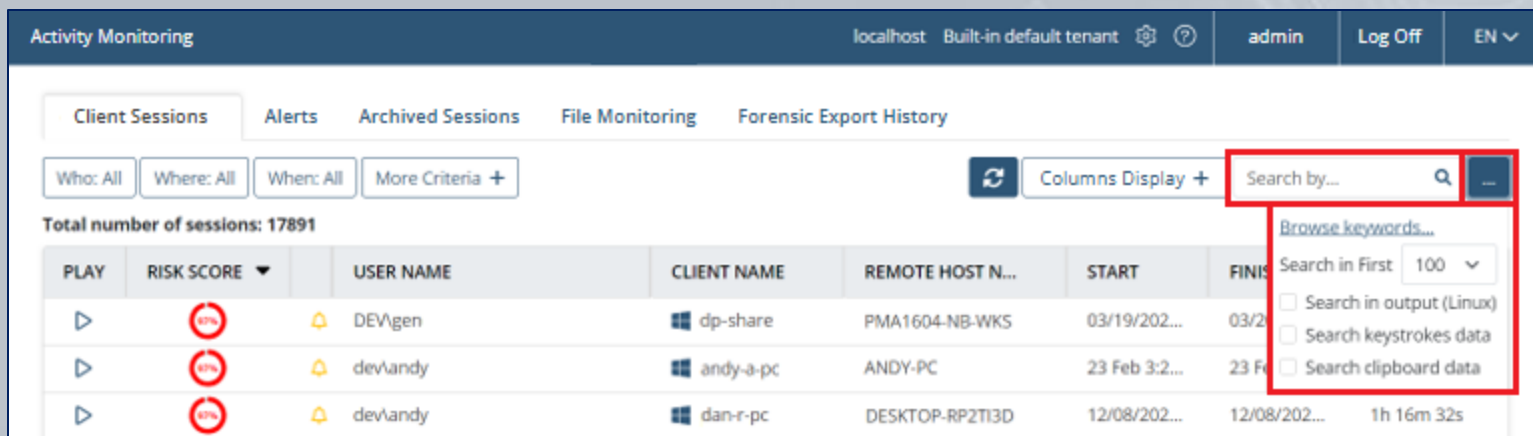
Do you want to unlock this user account?

CANCEL CONFIRM

Viewing Client Sessions

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

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

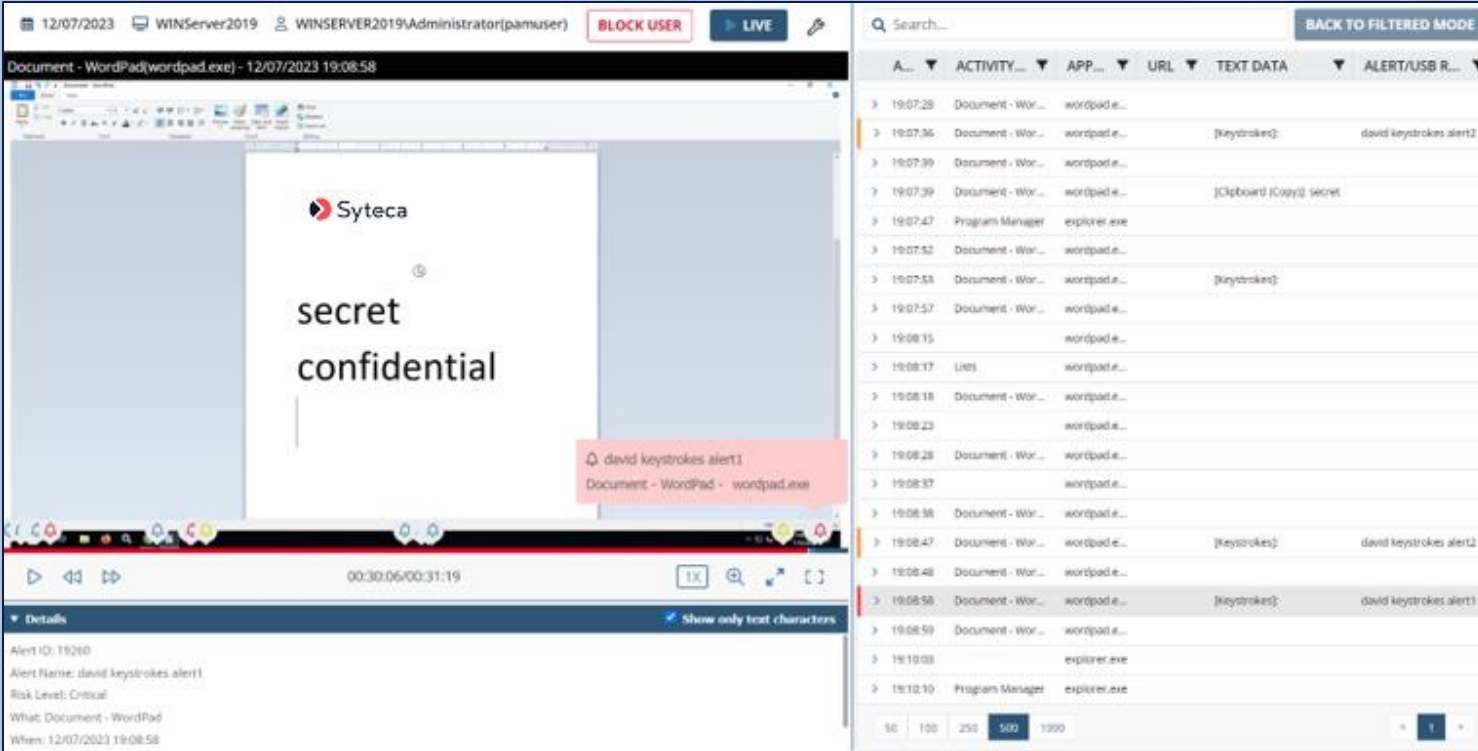


The screenshot displays the Syteca Management Tool interface. At the top, there's a navigation bar with "Activity Monitoring" and user information. Below it, a tabbed interface shows "Client Sessions" selected. A search bar is present with a dropdown menu open, showing options to "Search by..." and "Browse keywords...". The search dropdown includes checkboxes for "Search in output (Linux)", "Search keystrokes data", and "Search clipboard data". The main table lists sessions with columns: PLAY, RISK SCORE, USER NAME, CLIENT NAME, REMOTE HOST N..., START, and FINIS. The first three rows show sessions with a risk score of 57% and user names DEV\gen, dev\andy, and dev\andy.

PLAY	RISK SCORE	USER NAME	CLIENT NAME	REMOTE HOST N...	START	FINIS
▶	57%	DEV\gen	dp-share	PMA1604-NB-WKS	03/19/202...	03/2...
▶	57%	dev\andy	andy-a-pc	ANDY-PC	23 Feb 3:2...	23 Fe...
▶	57%	dev\andy	dan-r-pc	DESKTOP-RP2T13D	12/08/202...	12/08/202... 1h 16m 32s

Viewing a Session

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



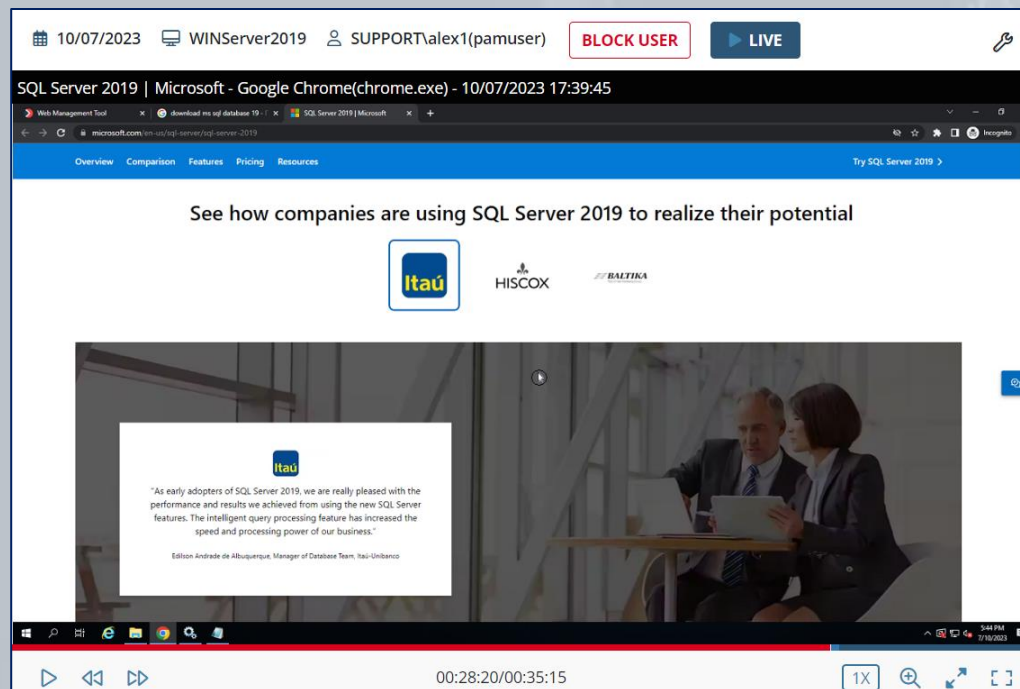
The screenshot displays the Syteca Session Viewer interface. The main pane shows a video capture of a Windows desktop. A WordPad window is open, displaying the text "secret" and "confidential". A red alert box is overlaid on the video, indicating "david keystrokes alert1" for the application "Document - WordPad - wordpad.exe". The video player controls at the bottom show a timestamp of 00:30:06/00:31:19.

The right pane displays a list of alerts. The table has columns for time, activity, application, URL, text data, and alert/USB R... The alerts are color-coded: red for critical alerts and yellow for informational alerts.

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

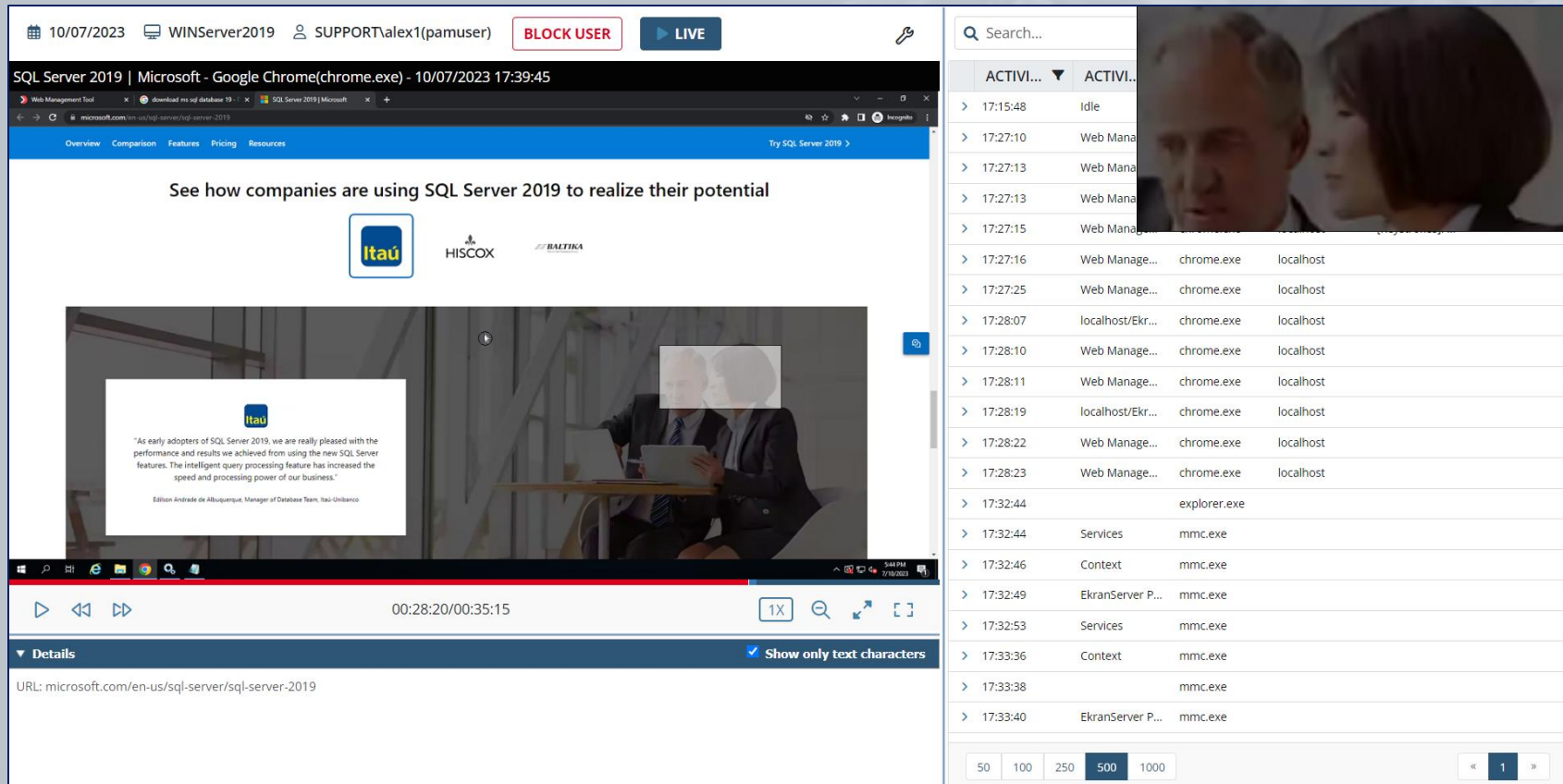
Syteca allows you to perform **monitoring** of user activity on Clients computer **in real time**.

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



The Magnifying Glass

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



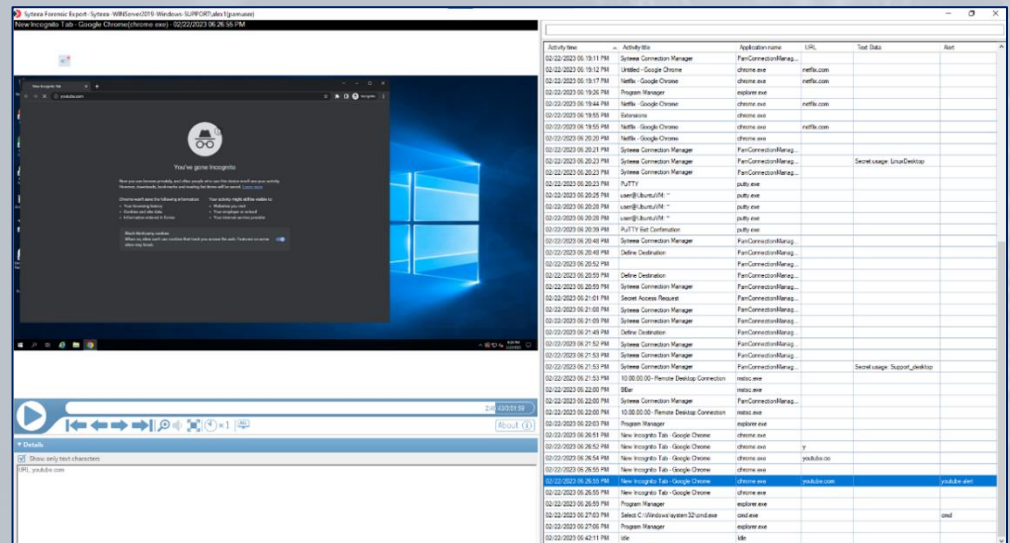
The screenshot displays the Syteca Session Player interface. The main video pane shows a Microsoft website for SQL Server 2019. A magnifying glass is active over a video frame showing two men in business suits. The interface includes a top navigation bar with user information and a 'BLOCK USER' button. The right sidebar contains an 'ACTIVITIES' table and a video thumbnail. The bottom section shows video controls and details.

TIME	ACTIVITY	PROCESS	HOST
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	

Details: microsoft.com/en-us/sql-server/sql-server-2019

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**.
- **Investigate** the user activity **data recorded** by using the offline Syteca Forensic Player.
- Present **evidence** in a **forensic format** to third parties.



Pseudonymizer

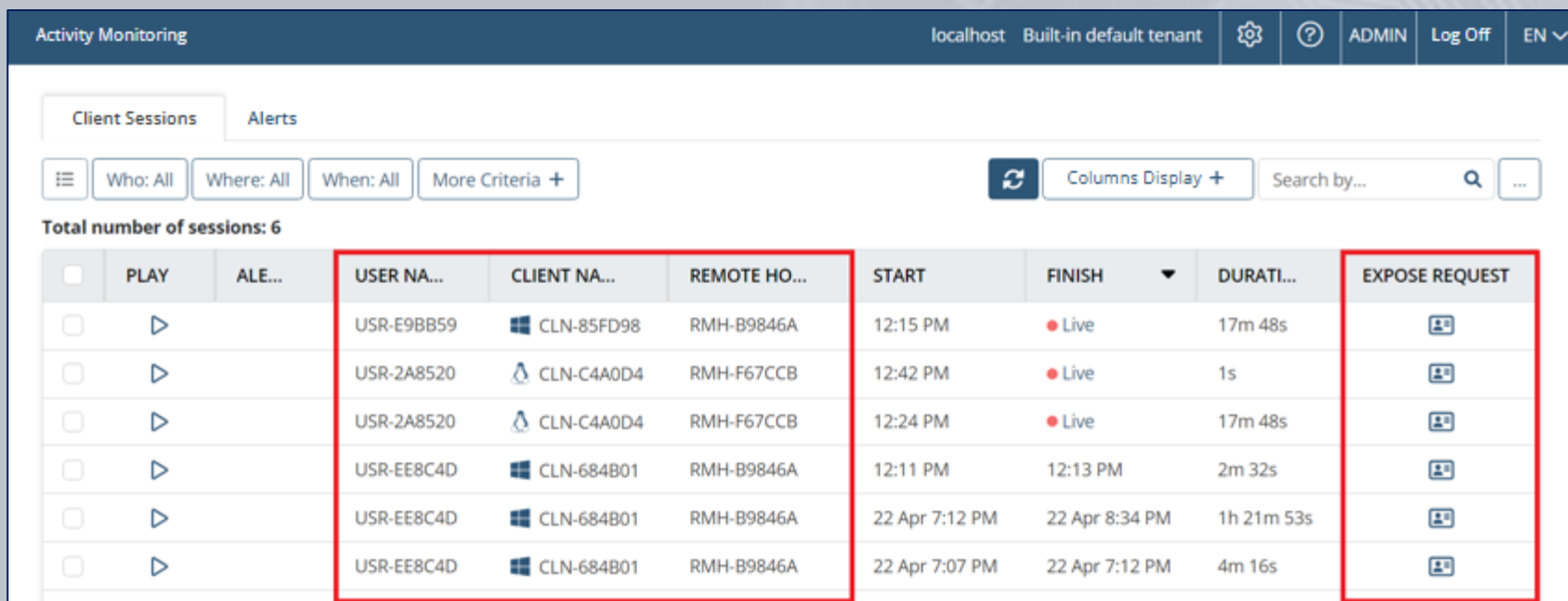
(for GDPR compliance, etc.)

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 'Activity Monitoring' interface. At the top, there's a navigation bar with 'localhost', 'Built-in default tenant', and user controls like 'ADMIN', 'Log Off', and 'EN'. Below this, a tabbed interface shows 'Client Sessions' and 'Alerts'. A filter bar includes 'Who: All', 'Where: All', 'When: All', and 'More Criteria +'. A 'Columns Display +' button and a search bar are also present. The main content area shows 'Total number of sessions: 6'. A table lists sessions with columns: PLAY, ALE..., USER NA..., CLIENT NA..., REMOTE HO..., START, FINISH, DURATI..., and EXPOSE REQUEST. The USER NA, CLIENT NA, and REMOTE HO columns are highlighted with a red box, indicating pseudonymized data. The EXPOSE REQUEST column is also highlighted with a red box, showing icons for each session.

	PLAY	ALE...	USER NA...	CLIENT NA...	REMOTE HO...	START	FINISH	DURATI...	EXPOSE REQUEST
<input type="checkbox"/>	▶		USR-E9BB59	CLN-85FD98	RMH-B9846A	12:15 PM	● Live	17m 48s	
<input type="checkbox"/>	▶		USR-2A8520	CLN-C4A0D4	RMH-F67CCB	12:42 PM	● Live	1s	
<input type="checkbox"/>	▶		USR-2A8520	CLN-C4A0D4	RMH-F67CCB	12:24 PM	● Live	17m 48s	
<input type="checkbox"/>	▶		USR-EE8C4D	CLN-684B01	RMH-B9846A	12:11 PM	12:13 PM	2m 32s	
<input type="checkbox"/>	▶		USR-EE8C4D	CLN-684B01	RMH-B9846A	22 Apr 7:12 PM	22 Apr 8:34 PM	1h 21m 53s	
<input type="checkbox"/>	▶		USR-EE8C4D	CLN-684B01	RMH-B9846A	22 Apr 7:07 PM	22 Apr 7:12 PM	4m 16s	

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

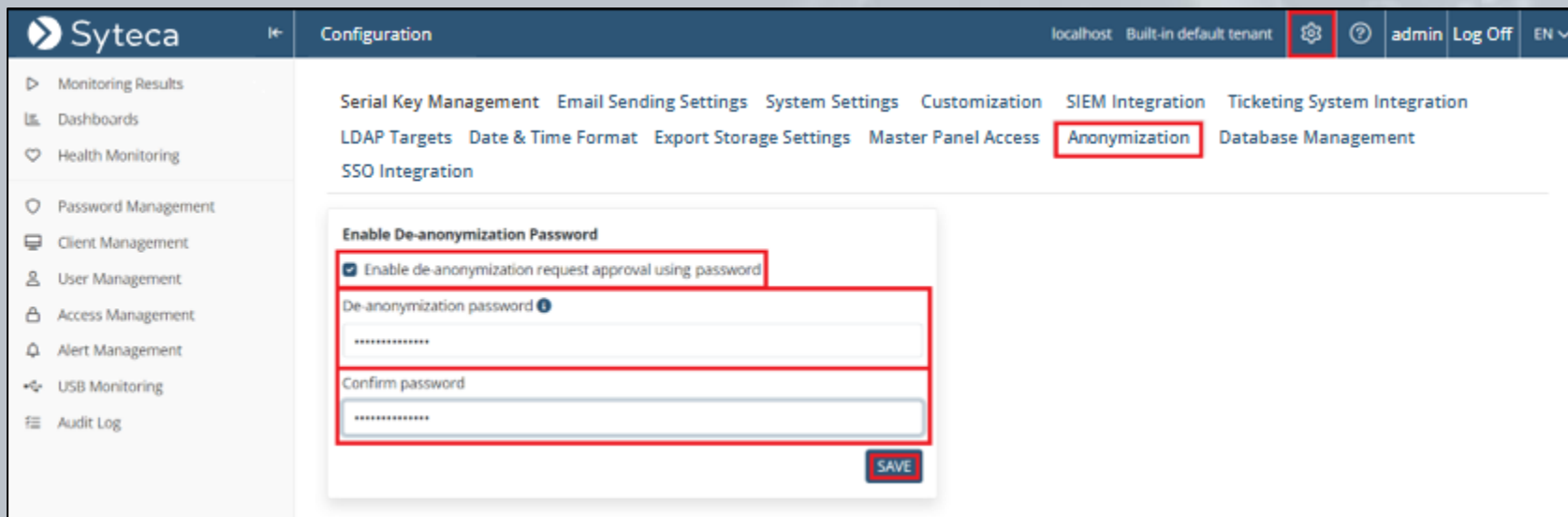
Client Sessions Alerts

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

Total number of sessions: 6

	PLAY	ALE...	USER NA...	CLIENT NA...	REMOTE HO...	START	FINISH	DURATI...	EXPOSE REQUEST
<input type="checkbox"/>	▶		USR-E9BB59	CLN-85FD98	RMH-EBD6BB	12:15 PM	1:05 PM	49m 41s	
<input type="checkbox"/>	▶		USR-A3EA2D	CLN-55D7C2	RMH-52825E	12:24 PM	12:42 PM	17m 48s	
<input type="checkbox"/>	▶		USR-A3EA2D	CLN-55D7C2	RMH-52825E	12:42 PM	12:42 PM	1s	
<input type="checkbox"/>	▶		andy-termw...	andy-term...	ANDY-LAPTOP	12:11 PM	12:13 PM	2m 32s	
<input type="checkbox"/>	▶		andy-termw...	andy-term...	ANDY-LAPTOP	22 Apr 7:12 PM	22 Apr 8:34 PM	1h 21m 53s	
<input type="checkbox"/>	▶		andy-termw...	andy-term...	ANDY-LAPTOP	22 Apr 7:07 PM	22 Apr 7:12 PM	4m 16s	

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).

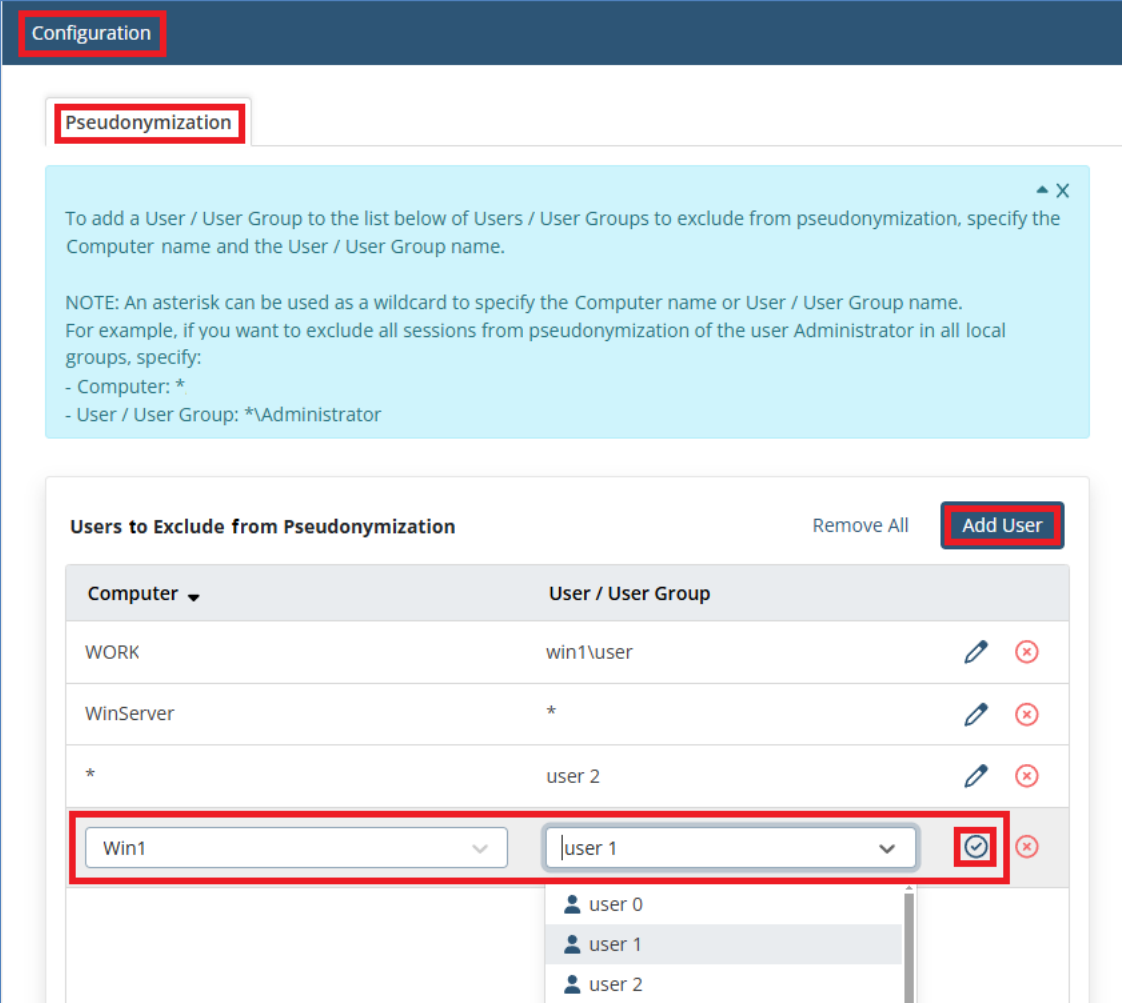


The screenshot shows the Syteca Configuration page. The top navigation bar includes the Syteca logo, a back arrow, the title 'Configuration', and user information: 'localhost Built-in default tenant', a settings gear icon, a help icon, 'admin', 'Log Off', and 'EN'. The left sidebar lists various management options. The main content area shows a list of configuration categories, with 'Anonymization' highlighted in a red box. Below this, the 'Enable De-anonymization Password' section is also highlighted in a red box. It contains a checked checkbox 'Enable de-anonymization request approval using password', followed by two password input fields: 'De-anonymization password' and 'Confirm password', both filled with asterisks. A 'SAVE' button is located at the bottom right of this section.

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.



Configuration









Pseudonymization

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.

NOTE: An asterisk can be used as a wildcard to specify the Computer name or User / User Group name.
For example, if you want to exclude all sessions from pseudonymization of the user Administrator in all local groups, specify:

- Computer: *
- User / User Group: *\Administrator

Users to Exclude from Pseudonymization Remove All **Add User**

Computer ▼	User / User Group	
WORK	win1\user	 
WinServer	*	 
*	user 2	 
Win1	user 1	 

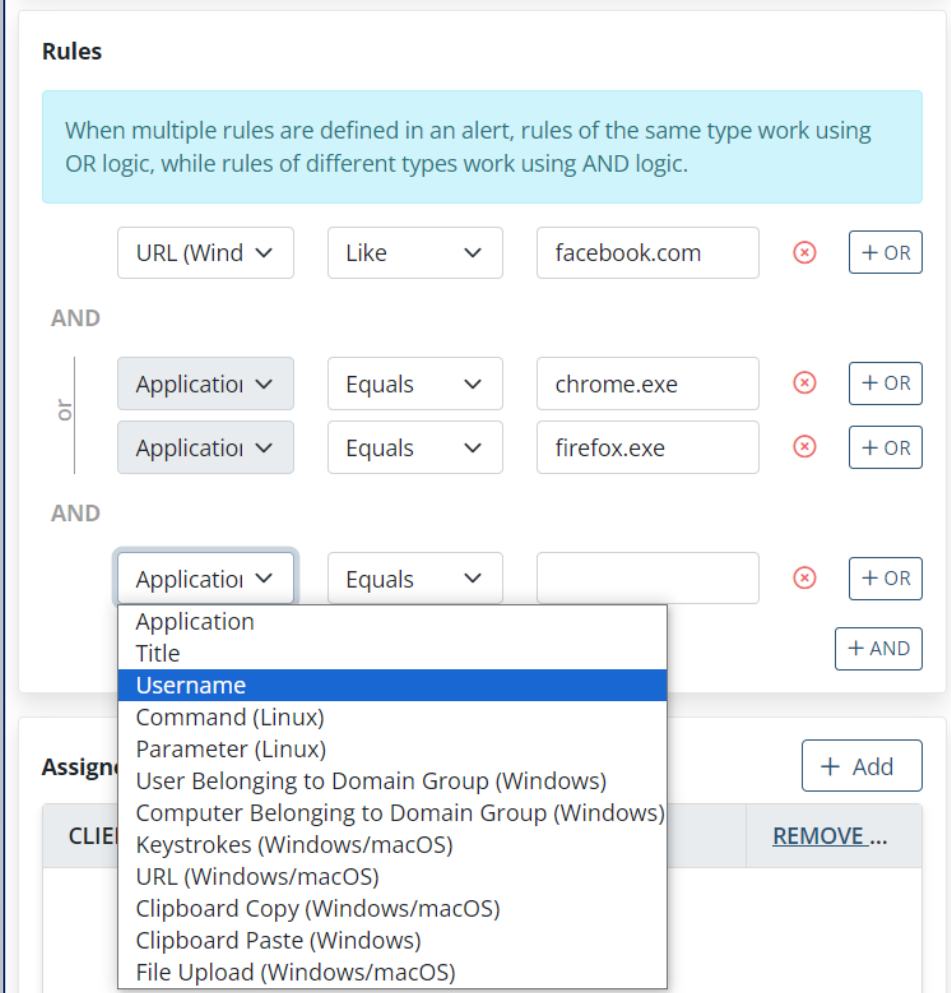
user 0
user 1
user 2

Alerts

Adding 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 light blue box contains the text: '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 interface is divided into sections for adding rules. The first section has a single rule: 'URL (Wind)' with the operator 'Like' and the value 'facebook.com'. The second section, labeled 'AND', contains two rules: 'Application' with operator 'Equals' and value 'chrome.exe', and 'Application' with operator 'Equals' and value 'firefox.exe'. The third section, also labeled 'AND', has one rule: 'Application' with operator 'Equals' and an empty value field. A dropdown menu is open for the 'Application' field in the third section, showing a list of options: 'Application', 'Title', 'Username' (highlighted), 'Command (Linux)', 'Parameter (Linux)', 'User Belonging to Domain Group (Windows)', 'Computer Belonging to Domain Group (Windows)', 'Keystrokes (Windows/macOS)', 'URL (Windows/macOS)', 'Clipboard Copy (Windows/macOS)', 'Clipboard Paste (Windows)', and 'File Upload (Windows/macOS)'. To the right of the rules, there are buttons for '+ OR', '+ AND', '+ Add', and 'REMOVE...'. The 'Assign' and 'CLIENT' sections are partially visible at the bottom.

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

Rules

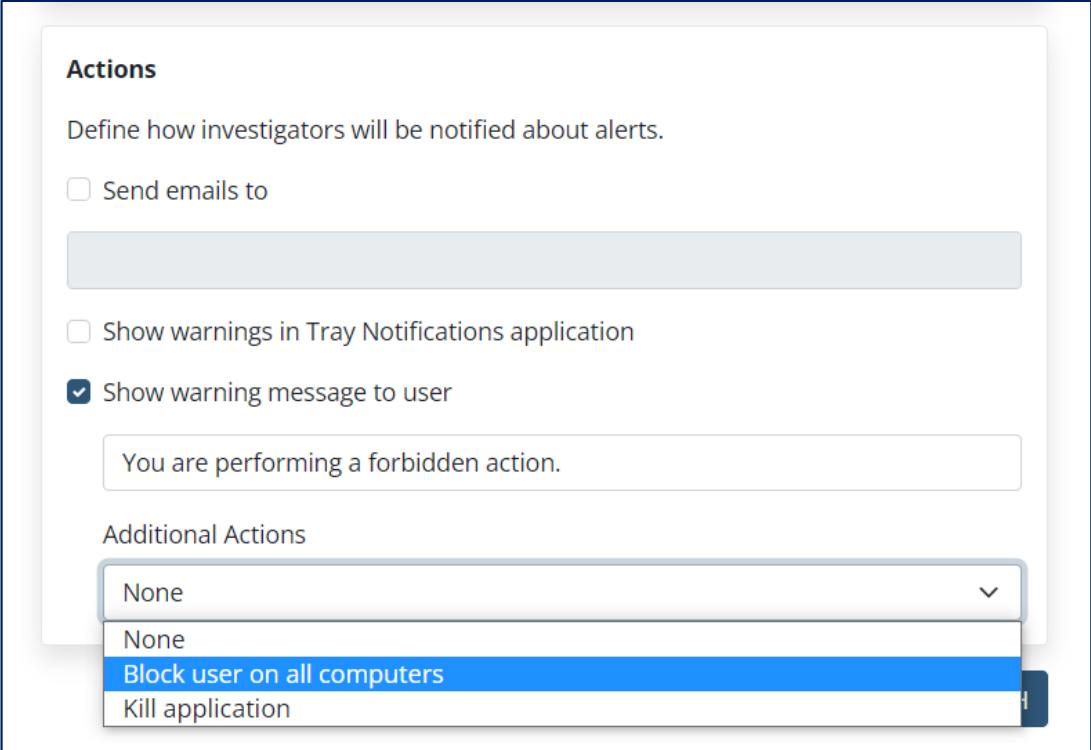
When multiple rules are defined in an alert, rules of the same type work using OR logic, while rules of different types work using AND logic.

	Application	Matches (Regex)	\b(chrome safari edge firefox)\b	✖	+ OR
AND or	Clipboard Paste (Windows/m	Matches (Regex)	^[w-\.]+\@[([w-]+\.)+[w-]{2,4}\$	✖	+ OR
	Clipboard Paste (Windows/m	Matches (Regex)	^[+]?([0-9]{3})?[-\s\.]?[0-9]{3}[-\s\.]?[0-9]{4,6}\$	✖	+ OR
					+ AND

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

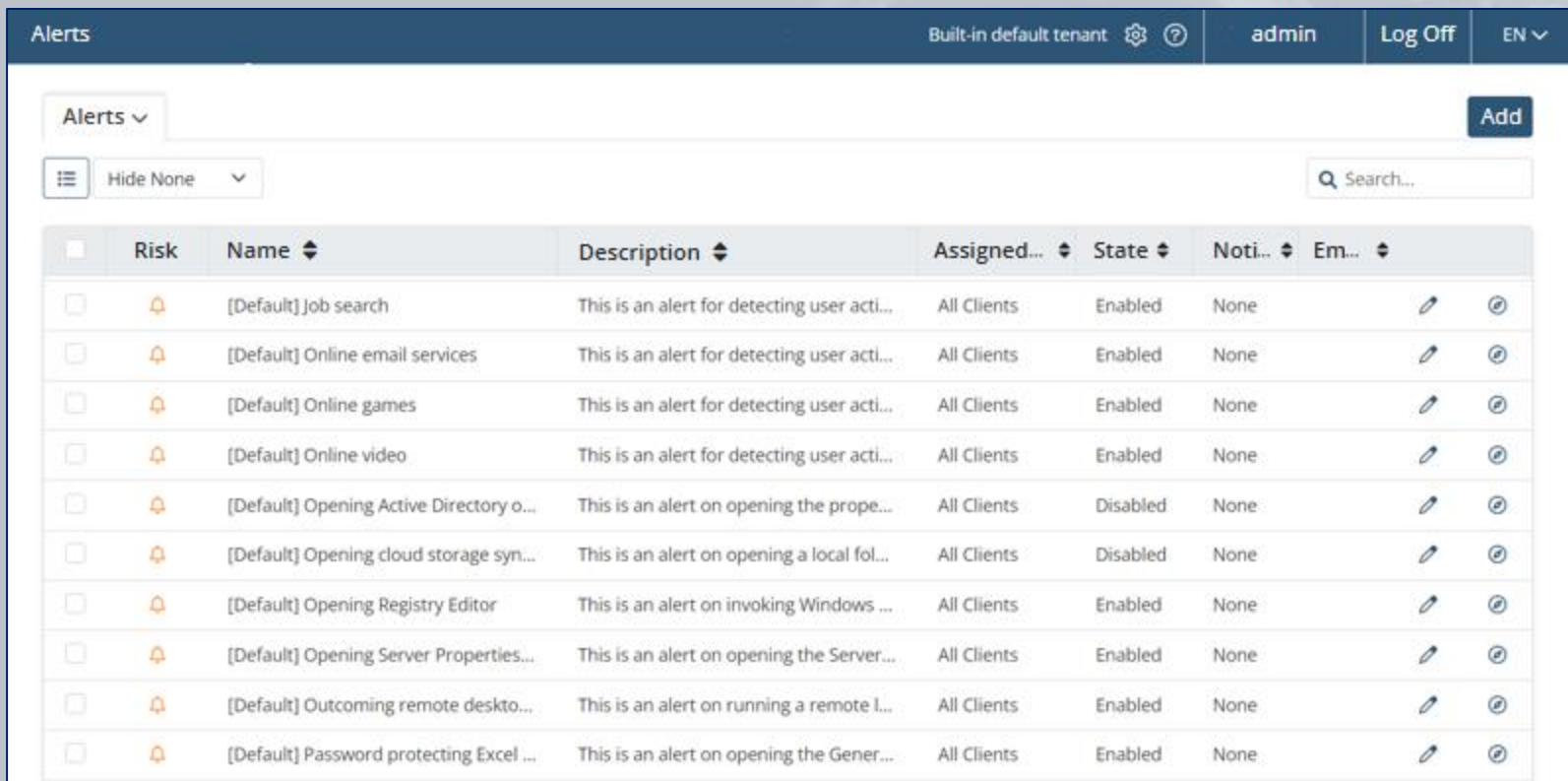
You can also set an alert to:

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























The screenshot shows the 'Alert Actions' configuration window. It has a title bar 'Actions' and a subtitle 'Define how investigators will be notified about alerts.' Below this, there are three checkboxes: 'Send emails to' (unchecked), 'Show warnings in Tray Notifications application' (unchecked), and 'Show warning message to user' (checked). Under the checked option, there is a text input field containing the message 'You are performing a forbidden action.' Below this, there is a section titled 'Additional Actions' with a dropdown menu. The dropdown is currently open, showing four options: 'None', 'None', 'Block user on all computers' (which is highlighted in blue), and '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 'Alerts' management interface. At the top, there's a header bar with 'Alerts', 'Built-in default tenant', user 'admin', 'Log Off', and a language dropdown 'EN'. Below the header, there's a section with 'Alerts' and an 'Add' button. A 'Hide None' dropdown and a search bar are also present. The main area contains a table of default alerts.

<input type="checkbox"/>	Risk	Name	Description	Assigned...	State	Noti...	Em...
<input type="checkbox"/>	🔔	[Default] Job search	This is an alert for detecting user acti...	All Clients	Enabled	None	 
<input type="checkbox"/>	🔔	[Default] Online email services	This is an alert for detecting user acti...	All Clients	Enabled	None	 
<input type="checkbox"/>	🔔	[Default] Online games	This is an alert for detecting user acti...	All Clients	Enabled	None	 
<input type="checkbox"/>	🔔	[Default] Online video	This is an alert for detecting user acti...	All Clients	Enabled	None	 
<input type="checkbox"/>	🔔	[Default] Opening Active Directory o...	This is an alert on opening the prope...	All Clients	Disabled	None	 
<input type="checkbox"/>	🔔	[Default] Opening cloud storage syn...	This is an alert on opening a local fol...	All Clients	Disabled	None	 
<input type="checkbox"/>	🔔	[Default] Opening Registry Editor	This is an alert on invoking Windows ...	All Clients	Enabled	None	 
<input type="checkbox"/>	🔔	[Default] Opening Server Properties...	This is an alert on opening the Server...	All Clients	Enabled	None	 
<input type="checkbox"/>	🔔	[Default] Outcoming remote deskto...	This is an alert on running a remote I...	All Clients	Enabled	None	 
<input type="checkbox"/>	🔔	[Default] Password protecting Excel ...	This is an alert on opening the Gener...	All Clients	Enabled	None	 

Viewing Alert Events

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

Activity Monitoring 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**

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

[Select all](#) [Clear selected items](#)
☐ Confirmed Risk
☐ False Alarm
☐ In Progress
☐ New
☐ Resolved

Viewing Alert Events in the Session Viewer



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

The screenshot displays the 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 bottom left panel shows details for Alert ID: 19136, Alert Name: david facebook alert, Risk Level: Normal, What: Facebook - log in or sign up - Google Chrome, and When: 12/07/2023 18:39:58. The right panel shows a list of alert events with columns for AC..., ACTIVITY TITLE, APP..., URL, TEXT DATA, and ALERT/USB ...

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

Receiving Alert Notifications



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

The screenshot displays the 'Syteca Tray Notifications Journal' window for user 'admin' on 'ginger-pc'. It contains a table of alerts with columns: Activity Time, Alert Name, Alert Level, Alert Description, User Name, Client Name, Client Description, Details, and Client Groups. A notification popup is overlaid on the right, showing a new alert: '[Default] Editing Windows Registry (8/17/2018 4:46:49 PM)' for client 'win2012_BA' and user 'WIN20_BA\Administrator'. The popup also includes a 'Tray Notification' button. At the bottom of the journal window, there are buttons for 'View in Web-Player' and 'Empty Journal'.

Activity Time	Alert Name	Alert Level	Alert Description	User Name	Client Name	Client Description	Details	Client Groups
8/17/2018 4:52...	[Default] Instan...	Normal	This is an alert o...	DEV\cathy	cathy-pc		Skype [1] - Sky...	
8/17/2018 4:51...	[Default] Online...	Critical	This is an alert f...	DEV\cathy	cathy-pc		Facebook - Goo...	
8/17/2018 4:51...	[Default] Social ...	Normal	This is an alert f...	DEV\cathy	cathy-pc		Facebook - Goo...	
8/17/2018 4:51...	[Default] Instan...	Normal	This is an alert o...	DEV\cathy	cathy-pc		Skype - Skype.e...	
8/17/2018 4:51...	[Default] Online...	Critical	This is an alert f...	DEV\cathy	cathy-pc		New Tab - Goog...	
8/17/2018 4:51...	[Default] Date a...	High	This is an Alert ...	DEV\alice	alice-pc			
8/17/2018 4:51...	[Default] Social ...	Normal	This is an alert f...	DEV\cathy	cathy-pc			
8/17/2018 4:50...	[Default] Instan...	Normal	This is an alert o...	DEV\cathy	cathy-pc			
8/17/2018 4:50...	[Default] Comm...	High	This is an alert o...	WIN2012_BA\A...	win2012_BA			
8/17/2018 4:50...	[Default] Remot...	High	This is an Alert ...	DEV\alice	alice-pc			
8/17/2018 4:50...	[Default] Cloud ...	Critical	This is an alert o...	DEV\alice	alice-pc			
8/17/2018 4:50...	File downloading	Normal	This is an alert o...	DEV\alice	alice-pc			
8/17/2018 4:49...	[Default] Social ...	Normal	This is an alert f...	DEV\alice	alice-pc			
8/17/2018 4:48...	[Default] Comm...	High	This is an alert o...	WIN2012_BA\A...	win2012_BA			
8/17/2018 4:48...	[Default] Editing...	Critical	This is an alert o...	WIN2012_BA\A...	win2012_BA		Edit String - reg...	
8/17/2018 4:46...	[Default] Editing...	Critical	This is an alert o...	WIN2012_BA\A...	win2012_BA		Edit String - reg...	

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 screenshots of the Syteca USB monitoring rule configuration interface. The left screenshot shows the 'Edit USB Rule (Ds)' window with the 'USB Rule Properties' tab selected. Under 'Monitored Devices', 'Mass storage devices' is checked. The right screenshot shows the 'Edit USB Rule (Ds)' window with the 'Additional Actions' tab selected. Under 'Actions', 'Block USB device' is checked. A warning message is displayed: 'WARNING: Before blocking USB devices on the user's computer, make sure that all the permitted peripheral devices are added to the exceptions list.' Below the warning, there is a checkbox for 'Notify user on the target computer about device blocking' which is also checked. The notification text is 'The USB device is blocked. Device info: [CompatibleID]'. Both screenshots have 'Next' and 'Finish' buttons at the bottom right.

Automatic USB Device Monitoring



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

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

The screenshot displays the Syteca Session Viewer interface. The top bar shows the session date (30/03/2023), user (WIN-UEE4P71DD32\Administrator(admin)), and status (BLOCK USER, LIVE). The main window is a Windows File Explorer showing the 'This PC' view. A red box highlights the 'E:' drive, which is a USB Storage device. A tooltip for the 'E:' drive is visible, stating 'Select to choose what happens with removable drives.' Below the File Explorer, a 'Details' panel shows the following information:

```
USB Mass Storage Device
USB\Class_08&SubClass_06&Prot_50
USB\VID_13FE&PID_3600&REV_0100\07A70E01AE681298
12/07/2018 18:03:23
```

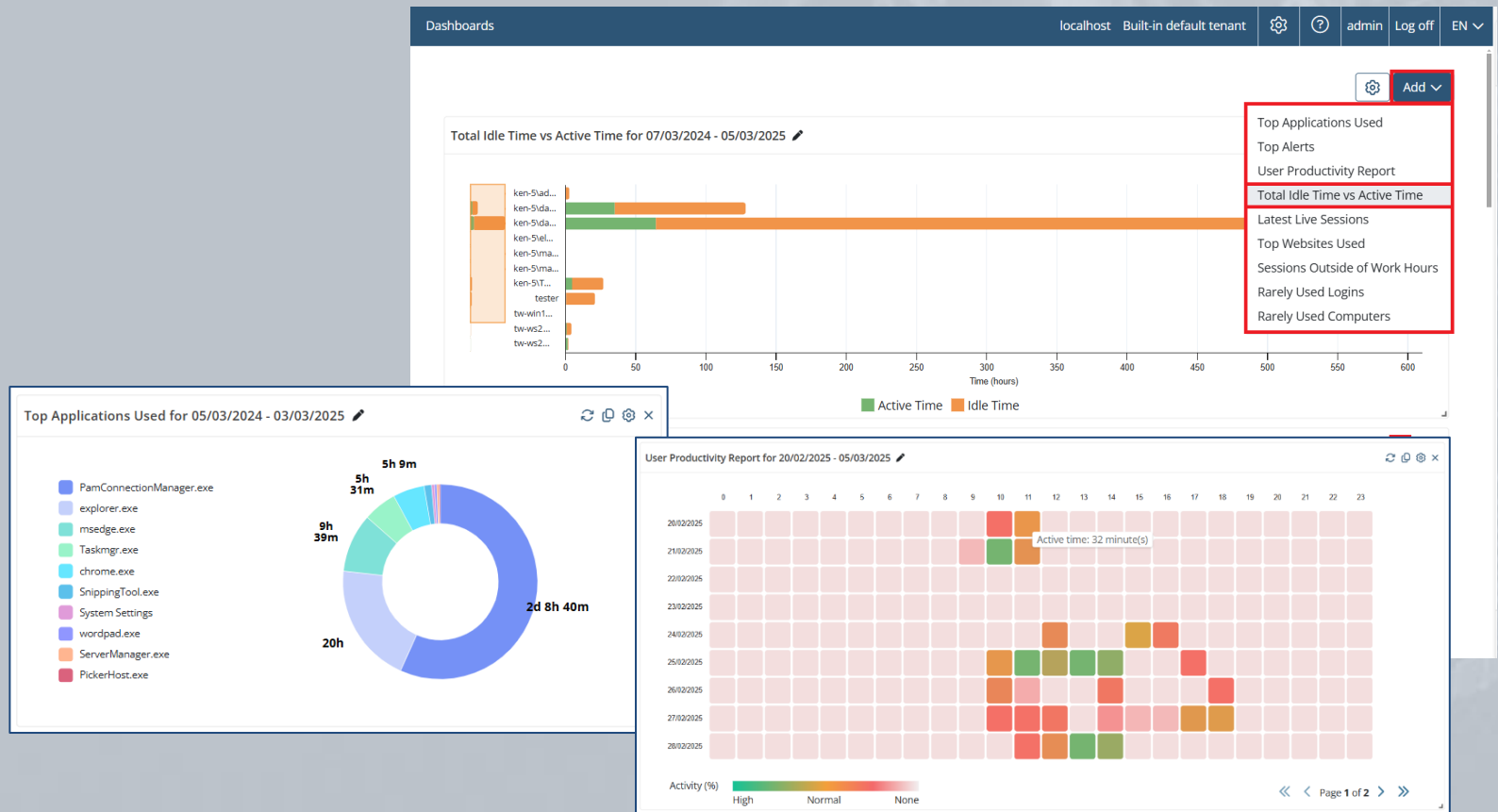
On the right side, an activity log table lists various events. The event at 14:58:11 is highlighted with a red box:

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:\- E\	[Monitoring event]			
14:58:47		explorer.exe			
14:58:47	New Incognito Tab - G...	chrome.exe			
14:58:49	This PC	explorer.exe			
14:58:50	Mozilla Firefox	firefox.exe			
14:58:50	Mozilla Firefox	firefox.exe	localhost		
14:58:53	Downloads 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		

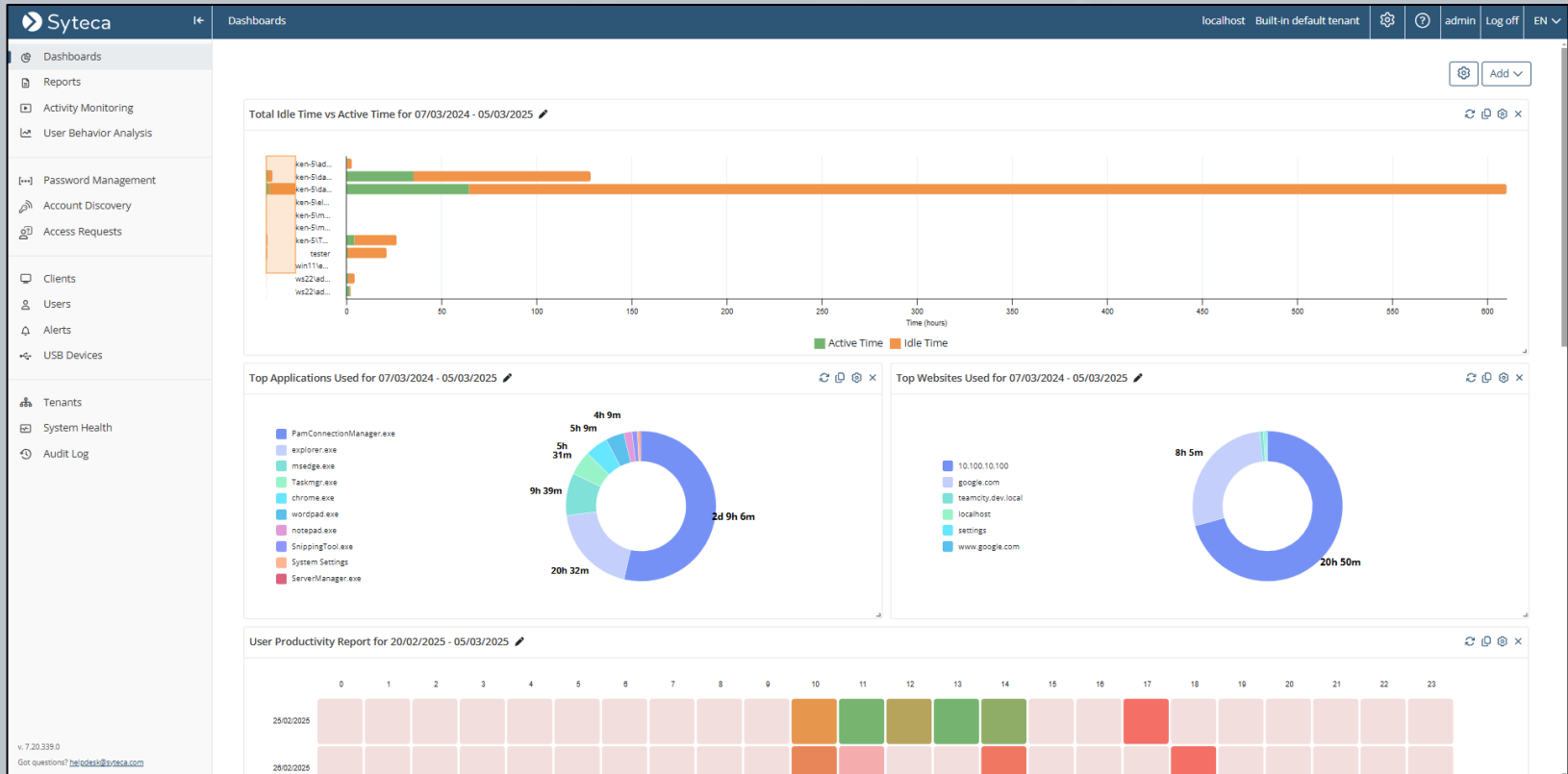
Dashboards

(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 range of data.

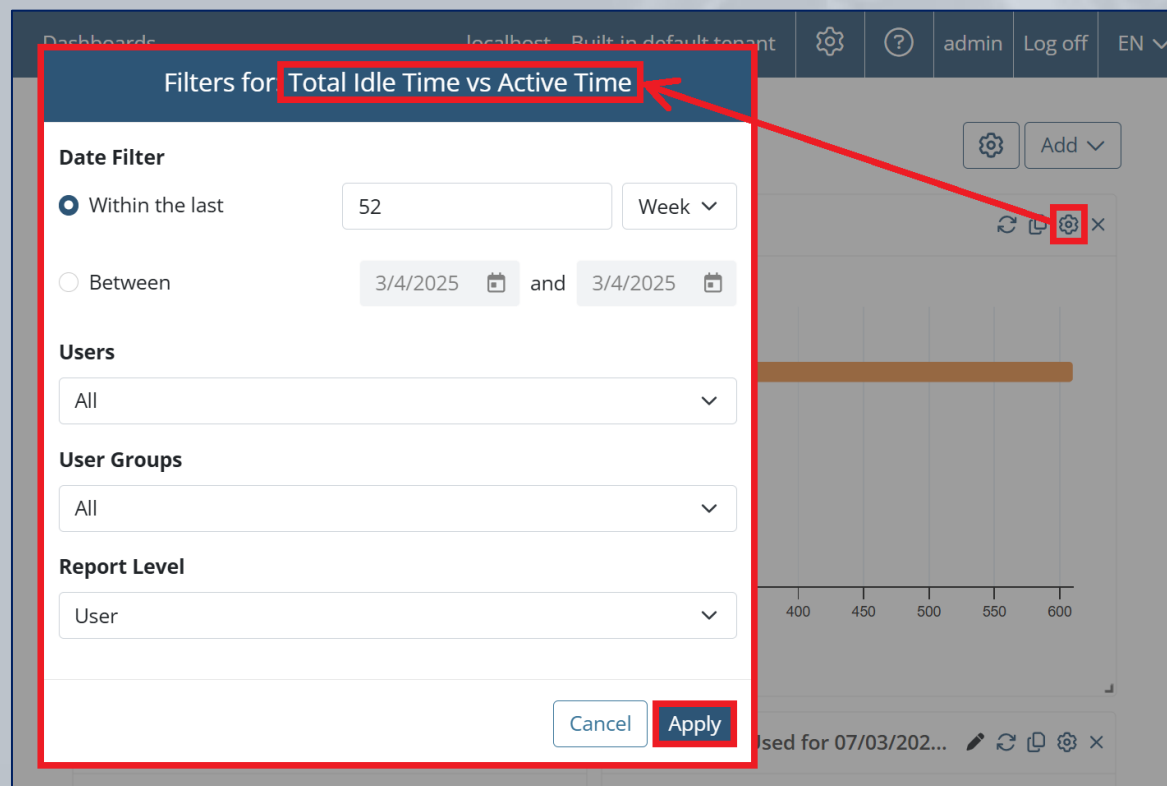


Viewing Dashboards

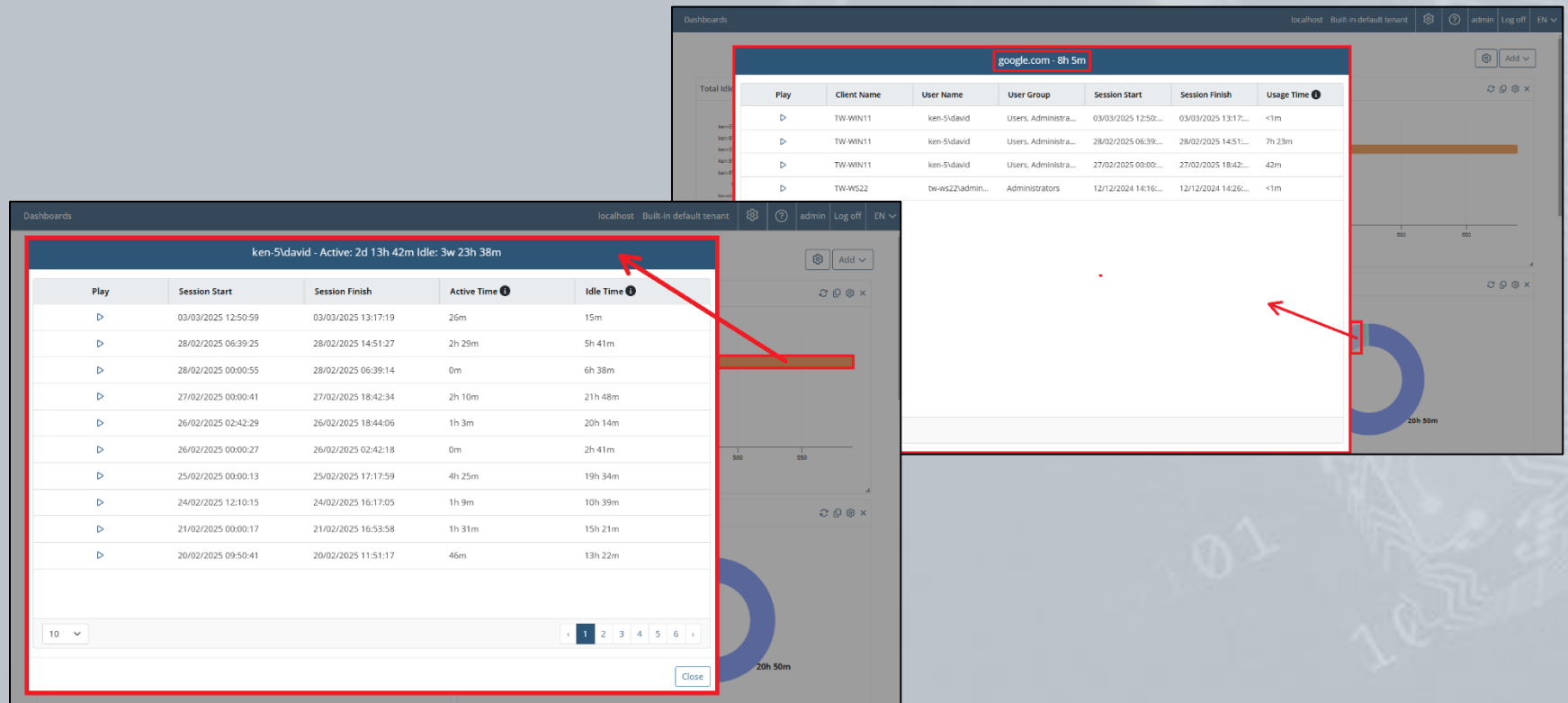


Some of these dashboards are **similar** to when **importing data** from Syteca **into Power BI** report templates by using **Syteca API Data Connector**, but are **much simpler to generate** and **customize**.




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



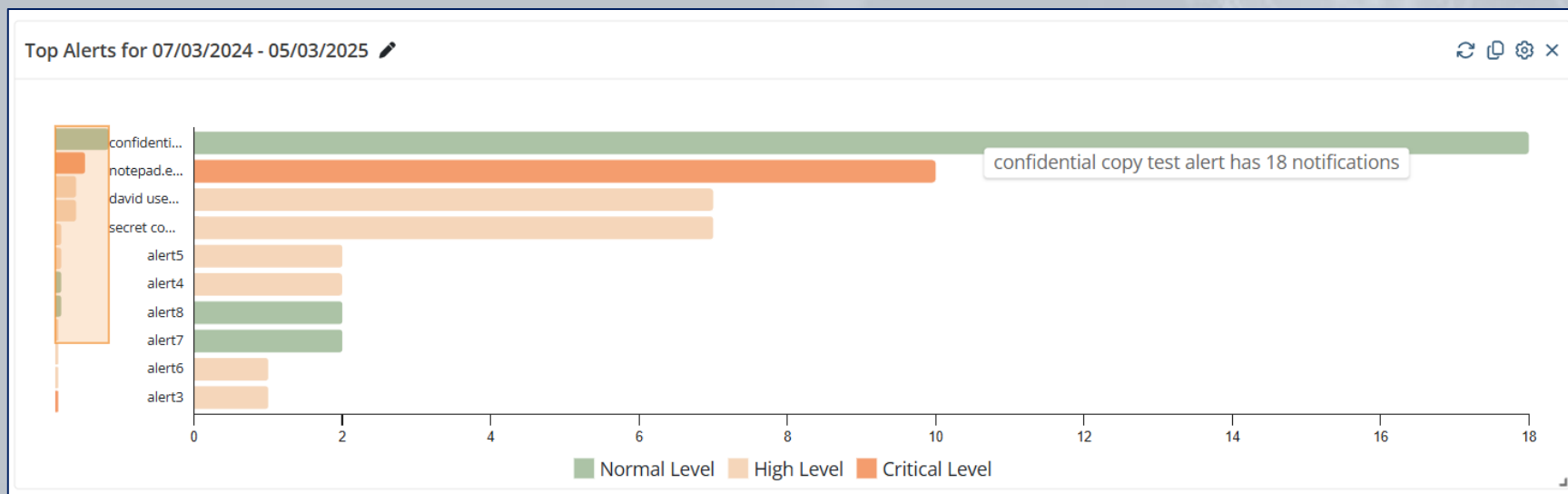
Detailed information about all the **sessions** that the data in the **charts contains** can then be viewed by **drilling down** (and can be played in the **Session Viewer**).



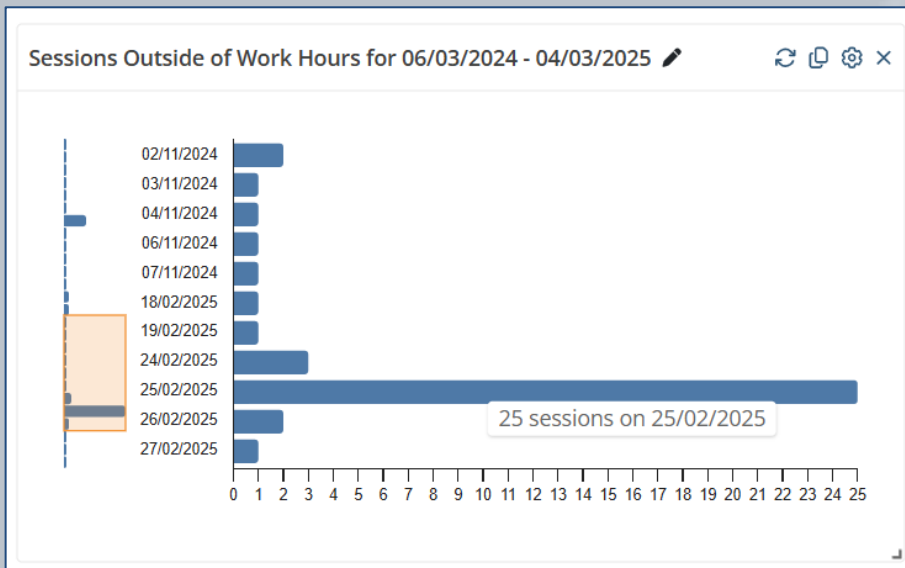
Latest Live Sessions

Latest Live Sessions 			
Play	Start	Client Name	User Name
	03/03/2025...	TW-WIN11	ken-5\david
<div></div>			
<div>10 </div>			

Top Alerts



Sessions Outside of Work Hours



Rarely Used Logins

Rarely Used Logins for 05/03/2024 - 03/03/2025

User Name	Sessions
user2	5
tw-ws22\administrator	3
tw-win11\ekran-user	1
tester	3
ken-5\mary(admin)	1
ken-5\mary	1

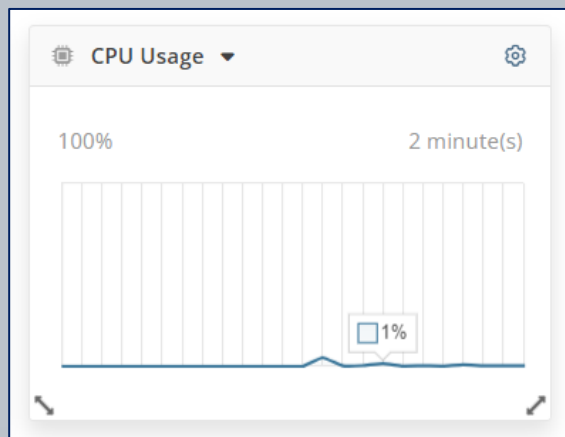
Rarely Used Computers

Rarely Used Computers for 05/03/2024 - 03/03/2025

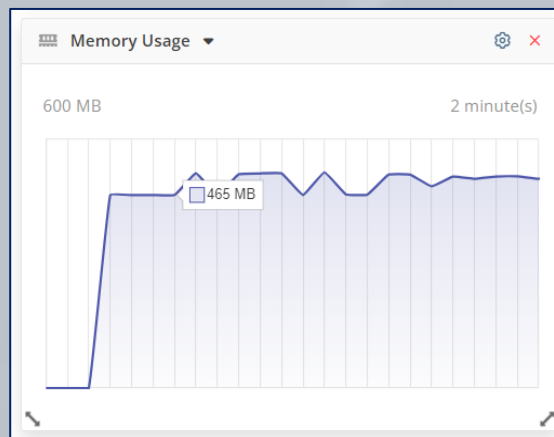
Client Name	Sessions
macOS-13-VM02	3
TW:WS22	15

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

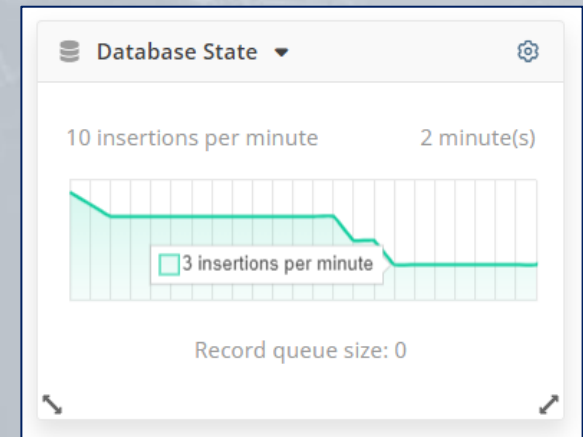
CPU Usage



Memory Usage

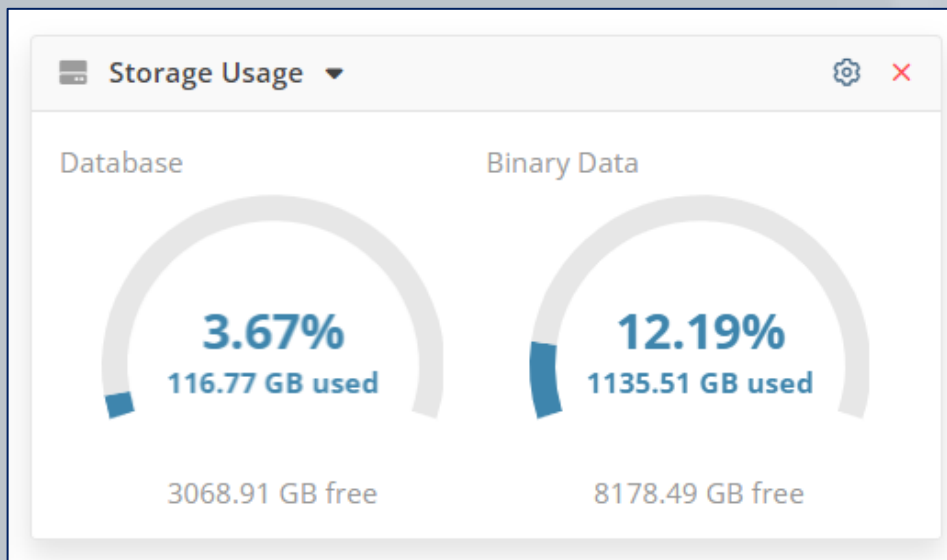


Database State

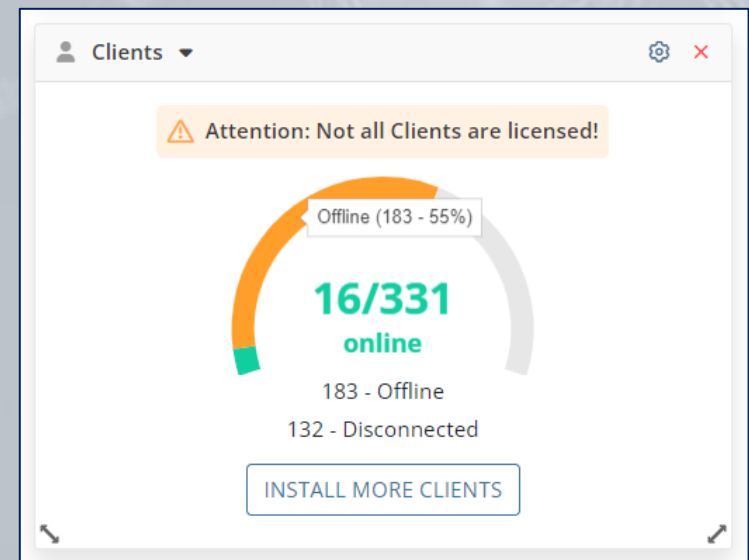


The **Storage Usage** and **Clients** dashboards (on the **System Health** page) provide information about the system state in real time.

Storage Usage



Clients



Reports

You can generate 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

ReportslocalhostBuilt-in default tenant⚙️🔍adminLog OffEN ▼

Report Generator

Scheduled Reports

Generated Reports

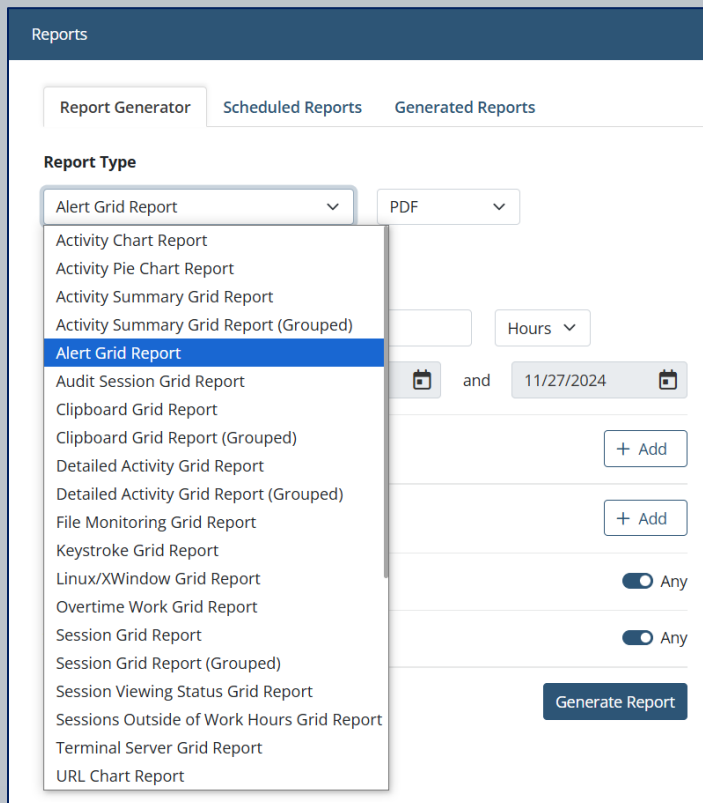
🔍 Search...

Add

Name ⚙️	Description ⚙️	Assigned To ⚙️	Monitored Users ⚙️	State ⚙️	Frequency ⚙️	Emails Recipients ⚙️
David test rule		All Clients	All Users	Disabled	Daily	<div>📄✎</div>
Test		ubuntu-2404LTS; macOS-13-VM	All Users	Enabled	Daily	<div>📄✎email@email.com</div>

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

Manual Report Generation



The screenshot shows the 'Reports' section with tabs for 'Report Generator', 'Scheduled Reports', and 'Generated Reports'. The 'Report Generator' tab is active. Under 'Report Type', a dropdown menu is open, listing various report types. 'Alert Grid Report' is selected and highlighted. To the right of the dropdown is a 'PDF' format selector. Below these are date filters: 'Within the last' with a value of '1' and 'Hours' as the unit, and 'Between' with dates '11/26/2024' and '11/27/2024'. There are 'Add' buttons for each filter. At the bottom is a 'Generate Report' button.

Reports

Report Generator Scheduled Reports Generated Reports

Report Type

Alert Grid Report PDF

Activity Chart Report

Activity Pie Chart Report

Activity Summary Grid Report

Activity Summary Grid Report (Grouped)

Alert Grid Report

Audit Session Grid Report

Clipboard Grid Report

Clipboard Grid Report (Grouped)

Detailed Activity Grid Report

Detailed Activity Grid Report (Grouped)

File Monitoring Grid Report

Keystroke Grid Report

Linux/XWindow Grid Report

Overtime Work Grid Report

Session Grid Report

Session Grid Report (Grouped)

Session Viewing Status Grid Report

Sessions Outside of Work Hours Grid Report

Terminal Server Grid Report

URL Chart Report

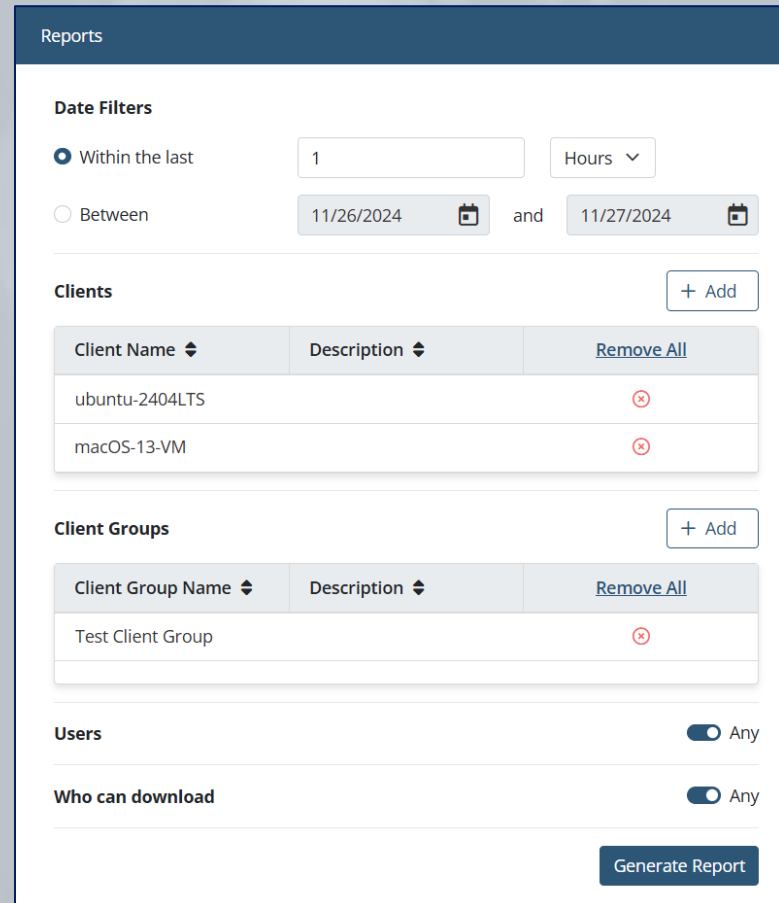
Hours

11/27/2024

+ Add

+ Add

Generate Report



The screenshot shows the 'Reports' section with various filters. 'Date Filters' include 'Within the last' (1 Hours) and 'Between' (11/26/2024 and 11/27/2024). 'Clients' and 'Client Groups' are listed in tables with 'Remove All' links. 'Users' and 'Who can download' have toggle switches set to 'Any'. A 'Generate Report' button is at the bottom.

Reports

Date Filters

Within the last 1 Hours

Between 11/26/2024 and 11/27/2024

Clients + Add

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

Client Groups + Add

Client Group Name	Description	Remove All
Test Client Group		

Users Any

Who can download Any

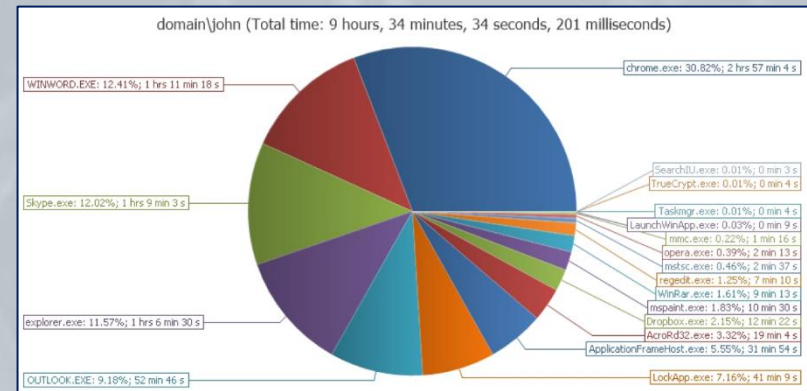
Generate Report

Activity Summary Grid Report

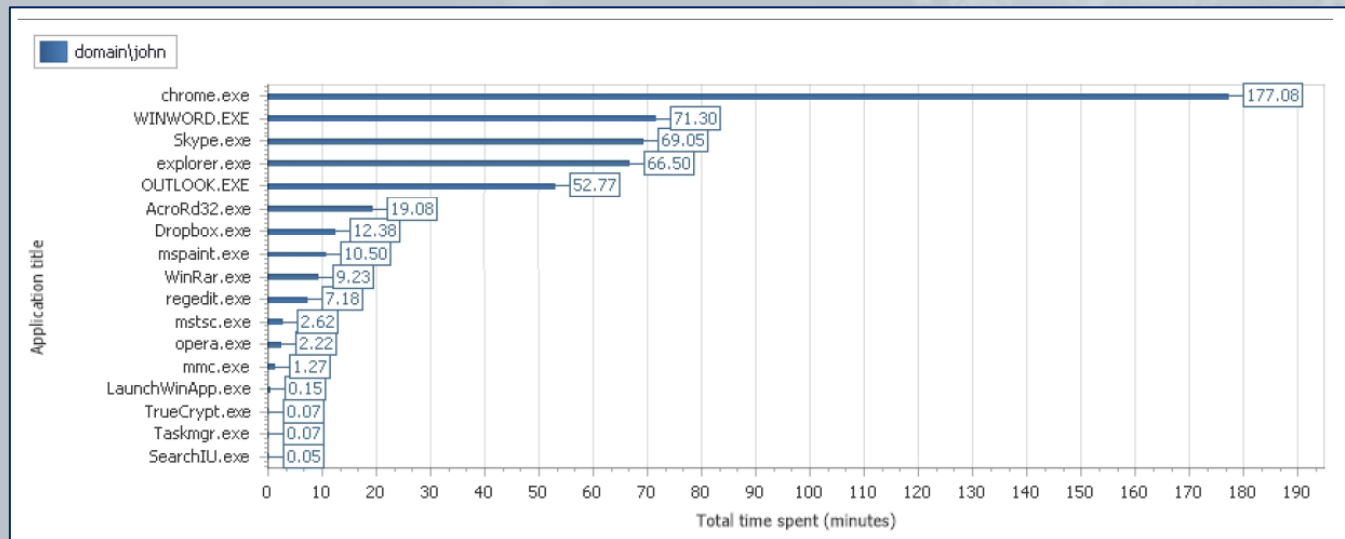
Client name	johnsmith-pc
Client description	Security AS group
User name	domain\john
Total time	6 hours, 42 minutes, 5 seconds
Active time	6 hours, 20 minutes

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

Activity Pie Chart Report



Activity Chart Report



User Statistics Report

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

Clipboard Grid Report

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

Access Requests Grid Report

Client Name	User Name	Request Type	Requested At	Status	Processed At	Processed By	Expired At
kirk-pc	kirk-pc\albert catsfield	One Time Password	10/04/2024 12:48:54 PM	Expired			10/04/2024 01:19:32 PM
kirk-pc	kirk-pc\albert catsfield	One Time Password	10/10/2024 06:07:16 PM	Denied	10/10/2024 06:17:37 PM	admin	
kirk-pc	kirk-pc\emily duck	Protected User	10/04/2024 12:44:53 PM	Denied	10/04/2024 12:45:10 PM	admin	
kirk-pc	kirk-pc\emily duck	One Time Password	10/10/2024 05:05:39 PM	Expired			10/10/2024 05:36:51 PM
kirk-pc	kirk-pc\kirk wallace	Protected User	10/04/2024 12:34:08 PM	Approved	10/04/2024 12:34:25 PM	admin	

Secondary User Authentication Grid Report

Client Name	IP Address	User Name	Secondary Auth Login	Login Time	Remote IPv4	Remote Host Name
kirk-pc	10.150.11.91	KIRK-PC\ALBERT CATSFIELD	albertcatsfield	10/11/2024 11:54:28 AM	192.168.237.165	ADMIN
kirk-pc	10.150.11.91	KIRK-PC\ALBERT CATSFIELD	alicecooper	10/11/2024 01:59:25 PM	192.168.237.165	ADMIN
kirk-pc	10.150.11.91	KIRK-PC\EMILY DUCK	emilyduck	10/11/2024 11:31:11 AM	192.168.237.165	ADMIN
kirk-pc	10.150.11.91	KIRK-PC\EMILY DUCK	emilyduck	10/11/2024 01:04:25 PM	192.168.237.165	ADMIN

Session Grid Report

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

Sessions Outside of Work Hours Grid Report

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

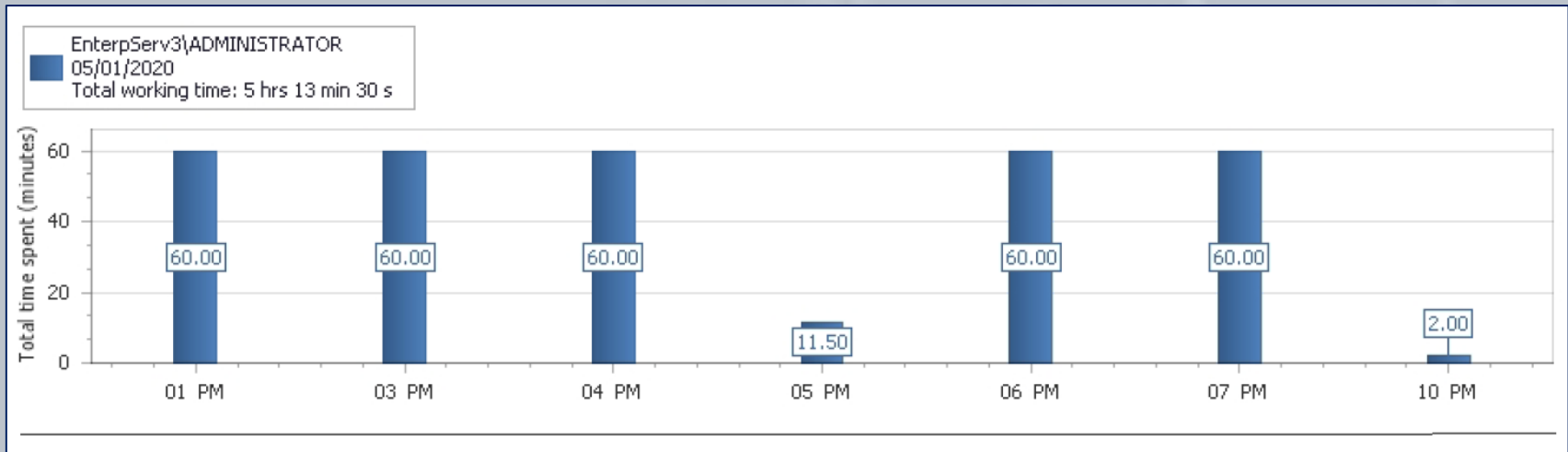
Detailed Activity Grid Report

Client name		alice-pc			
Client description		Loading Sensitive Data to a Flash Drive			
User name		ALICE-PC\Alice			
Activity time	Activity title	Application name	URL	Text data	
07/10/2018 08:53:01 AM	My Drive - Google Drive - Google Chrome	chrome.exe	https://drive.google.com/drive/my-drive?ogsrc=32		
07/10/2018 08:53:01 AM	My Drive - Google Drive - Google Chrome	chrome.exe	https://drive.google.com/drive/my-drive?ogsrc=32		
07/10/2018 08:53:01 AM	My Drive - Google Drive - Google Chrome	chrome.exe	https://drive.google.com/drive/my-drive?ogsrc=32	[Clipboard (Paste)]: https://drive.google.com/file/d/19TprsVorHH8GcdL0xnHmQ8HKh7ww/view?usp=har...	
07/10/2018 08:53:08 AM	My Drive - Google Drive - Google Chrome	chrome.exe	https://mail.google.com/mail/u/0/#inbox		
07/10/2018 08:53:08 AM	Inbox (6) - helenapeterson.hr@gmail.com - Gmail - Google Chrome	chrome.exe	https://mail.google.com/mail/u/0/#inbox		

User Daily Activity Grid Report

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

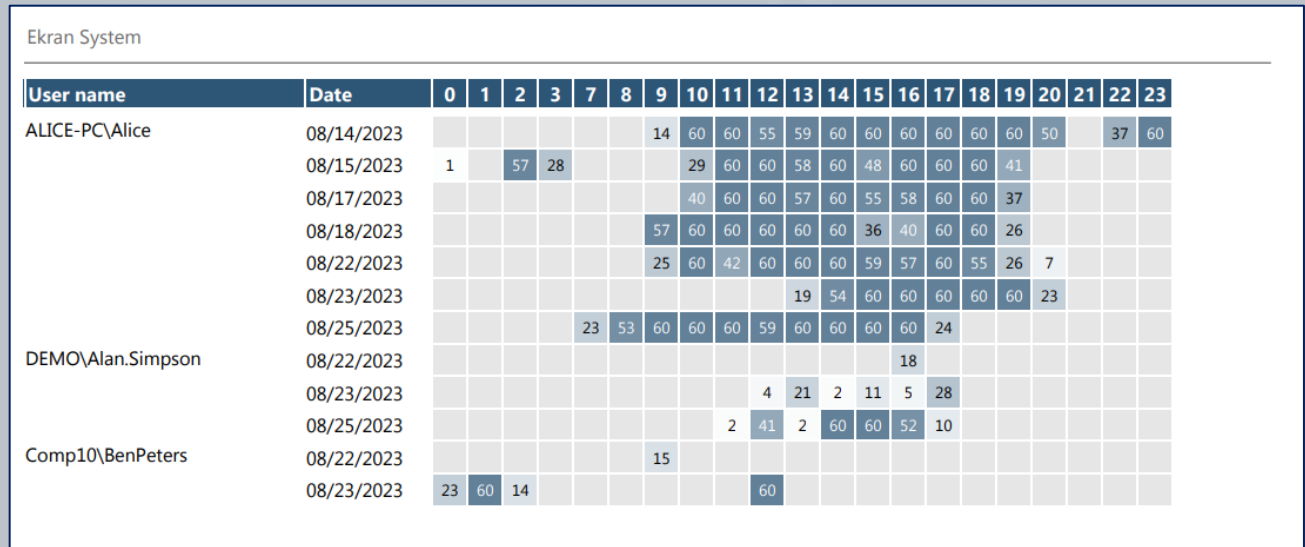
User Productivity Chart Report



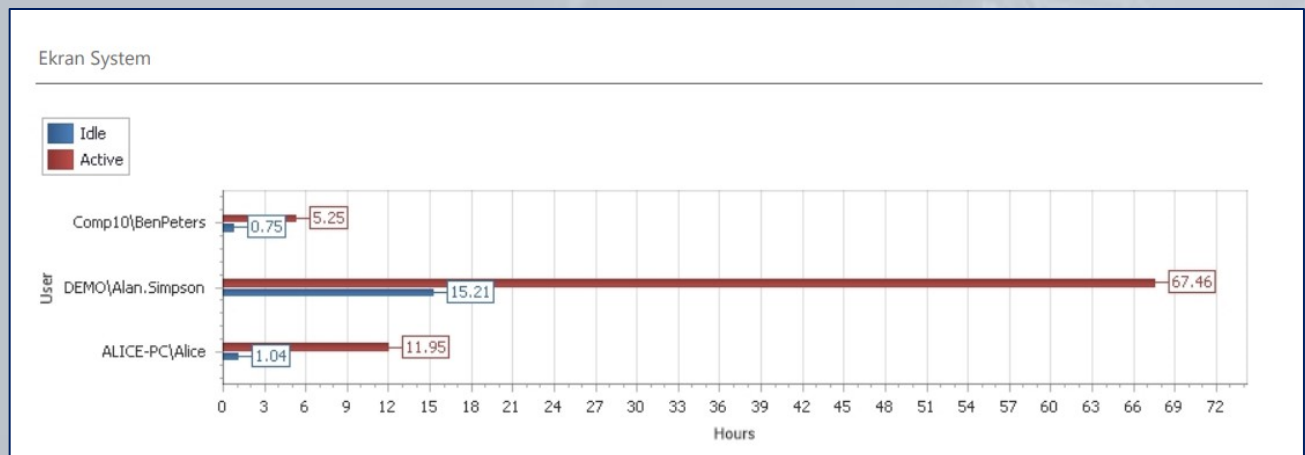
User Productivity Summary Grid Report

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

User Productivity Heatmap Report



User Active Time and Idle Time Chart Report



Alert Grid Report

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

User Behavior Analytics Report

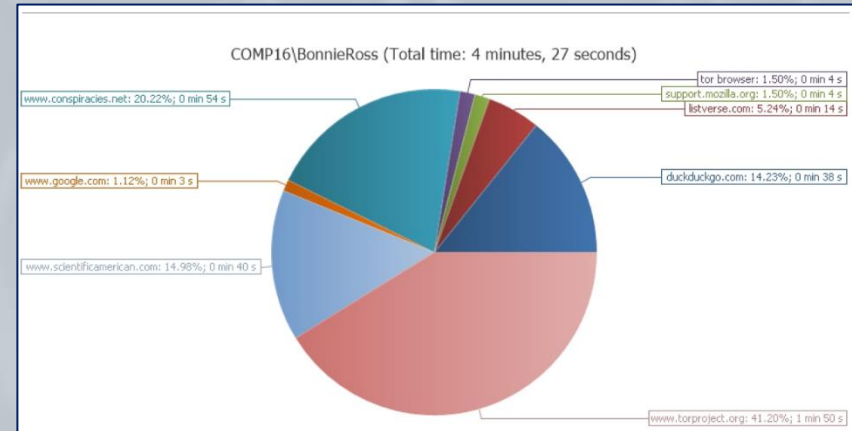
Risk Level	Normal				
Risk Score, %	50 - 1				
Session number	3				
Who	Where	When	Details	Session Score	Session URL
ALICE-PC\Alice	alice-pc	07/12/2018 06:01:48 PM - 07/12/2018 06:04:08 PM	WorkingHours: normal	9%	Open Session
COMP11\SusieWade	Comp11	07/10/2018 11:08:30 AM - 07/10/2018 11:11:01 AM	WorkingHours: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

URL Summary Grid Report

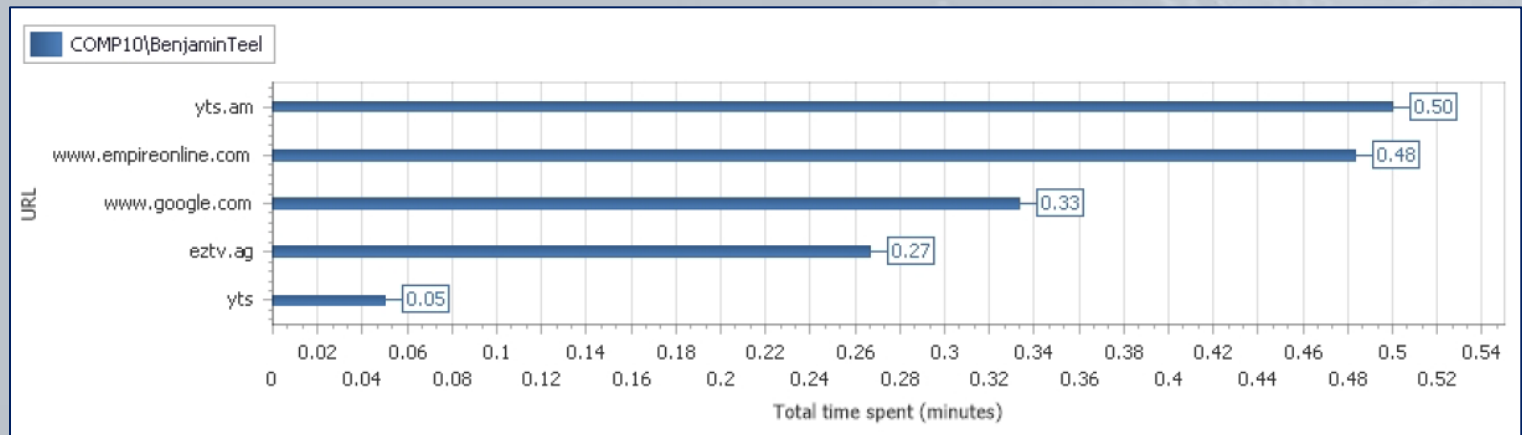
Client name	Comp15
Client description	Exporting HR Data
User name	COMP15\HelenPeterson
Total time	4 minutes, 33 seconds

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

URL Pie Chart Report



URL Chart Report



USB Storage Grid Report

Client name	alice-pc
Client description	Loading Sensitive Data to a Flash Drive
User name	ALICE-PC\Alice
Time	Details
07/12/2018 06:02:55 PM	USBStorage - (Standard MTP Device) - MTP USB Device
07/12/2018 06:03:26 PM	USBStorage - E:\ - JULIETTE

USB Alert Grid Report

Client name	juliet-pc				
Client description	USB device blocking				
User name	JULIET-PC\Julia()				
Time	Rule Name	Action	Risk Level	Device Class	Device Details
07/12/2018 04:23:12 PM	usb device blocking	Blocked	Critical	USB Mass Storage Device	USB\Class_08&SubClass_06&Prot_50; USB\VID_13FE&PID_3600&REV_0100\07A70E01AE6 B1298
07/12/2018 04:23:38 PM	usb device blocking	Blocked	Critical	USB Mass Storage Device	USB\Class_08&SubClass_06&Prot_50; USB\VID_13FE&PID_3600&REV_0100\07A70E01AE6 B1298

Terminal Server Grid Report

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

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

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

Linux/XWindow Grid Report

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

The Audit Session Grid Report is a special 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
04/27/2023 03:32:47 PM	admin/Administrators	Viewed session	ubuntu	Ubuntu-20.04	04/27/2023 03:18:33 PM - 04/27/2023 03:18:47 PM
04/27/2023 03:40:49 PM	admin/Administrators	Viewed session	root	Ubuntu-20.04	04/27/2023 03:18:33 PM - 04/27/2023 03:18:47 PM
04/27/2023 03:41:01 PM	admin/Administrators	Viewed session	tester	macos-11-vm1	04/27/2023 03:18:54 PM - 04/27/2023 03:19:00 PM

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**).

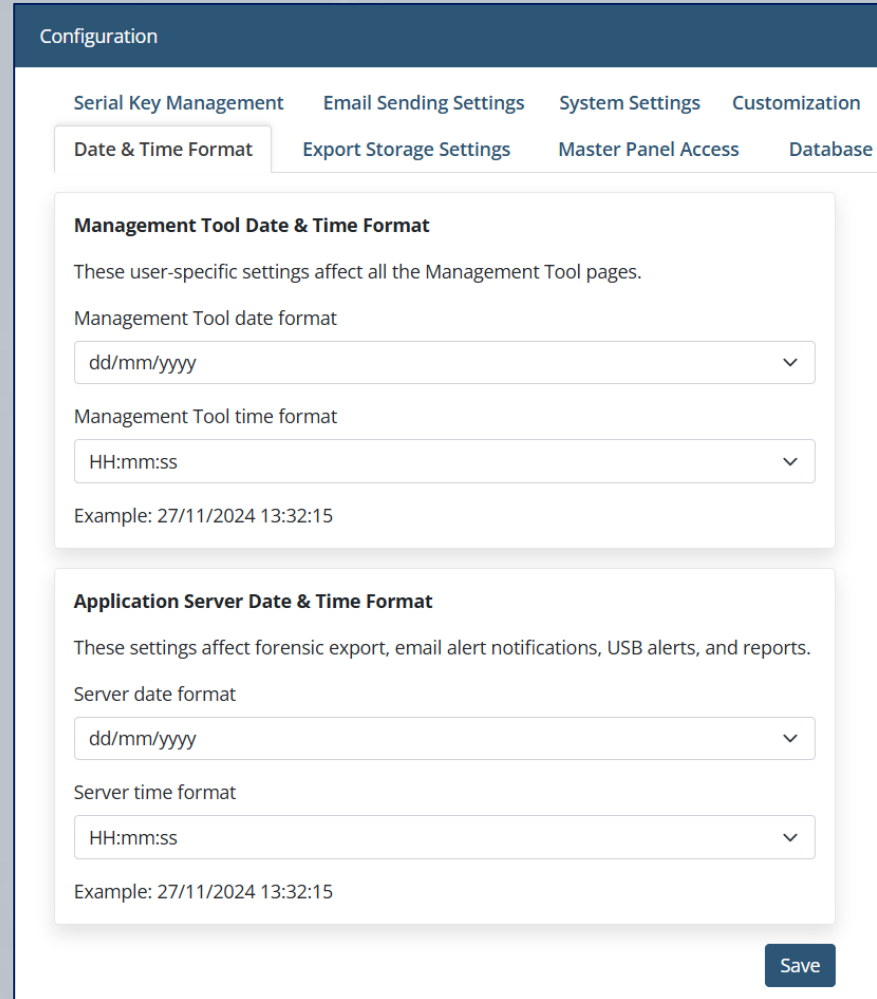
Session Viewing Status Grid Report

Ekran System 7.11.34.0										
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
8	w11testpc\user	w11testPC	03/13/2024 02:00:49 PM	03/13/2024 02:01:50 PM	None	None	Open Session	Yes	admin	03/13/2024 02:02:02 PM
10	desktop-msaqs4k\user	DESKTOP-MSAQS4K	03/13/2024 02:02:22 PM	03/13/2024 02:16:30 PM	None	None	Open Session	Yes	admin	03/13/2024 02:03:07 PM
10	desktop-msaqs4k\user	DESKTOP-MSAQS4K	03/13/2024 02:02:22 PM	03/13/2024 02:16:30 PM	None	None	Open Session	Yes	user2	03/13/2024 02:03:36 PM
11	desktop-msaqs4k\user	DESKTOP-MSAQS4K	03/13/2024 02:16:45 PM	03/13/2024 02:18:09 PM	None	None	Open Session	No		
15	desktop-msaqs4k\user	DESKTOP-MSAQS4K	03/13/2024 02:22:12 PM	03/13/2024 02:22:42 PM	None	None	Open Session	No		
16	w11testpc\user	w11testPC	03/13/2024 02:23:07 PM	03/13/2024 02:24:01 PM	None	None	Open Session	Yes	admin	03/13/2024 02:23:26 PM
16	w11testpc\user	w11testPC	03/13/2024 02:23:07 PM	03/13/2024 02:24:01 PM	None	None	Open Session	Yes	admin	03/13/2024 02:23:49 PM
Wednesday, 13 March 2024										
										2

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 with a navigation bar containing 'Serial Key Management', 'Email Sending Settings', 'System Settings', and 'Customization'. Under 'Customization', there are tabs for 'Date & Time Format', 'Export Storage Settings', 'Master Panel Access', and 'Database'. The 'Date & Time Format' tab is active, showing two sections: 'Management Tool Date & Time Format' and 'Application Server Date & Time Format'. Each section includes a description, a 'Server date format' dropdown (set to 'dd/mm/yyyy'), a 'Server time format' dropdown (set to 'HH:mm:ss'), and an example of the combined format: '27/11/2024 13:32:15'. A 'Save' button is located at the bottom right of the configuration area.

Configuration

Serial Key Management Email Sending Settings System Settings Customization

Date & Time Format Export Storage Settings Master Panel Access Database

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: 27/11/2024 13:32:15

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: 27/11/2024 13:32:15

Save

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



Customizing Reports

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



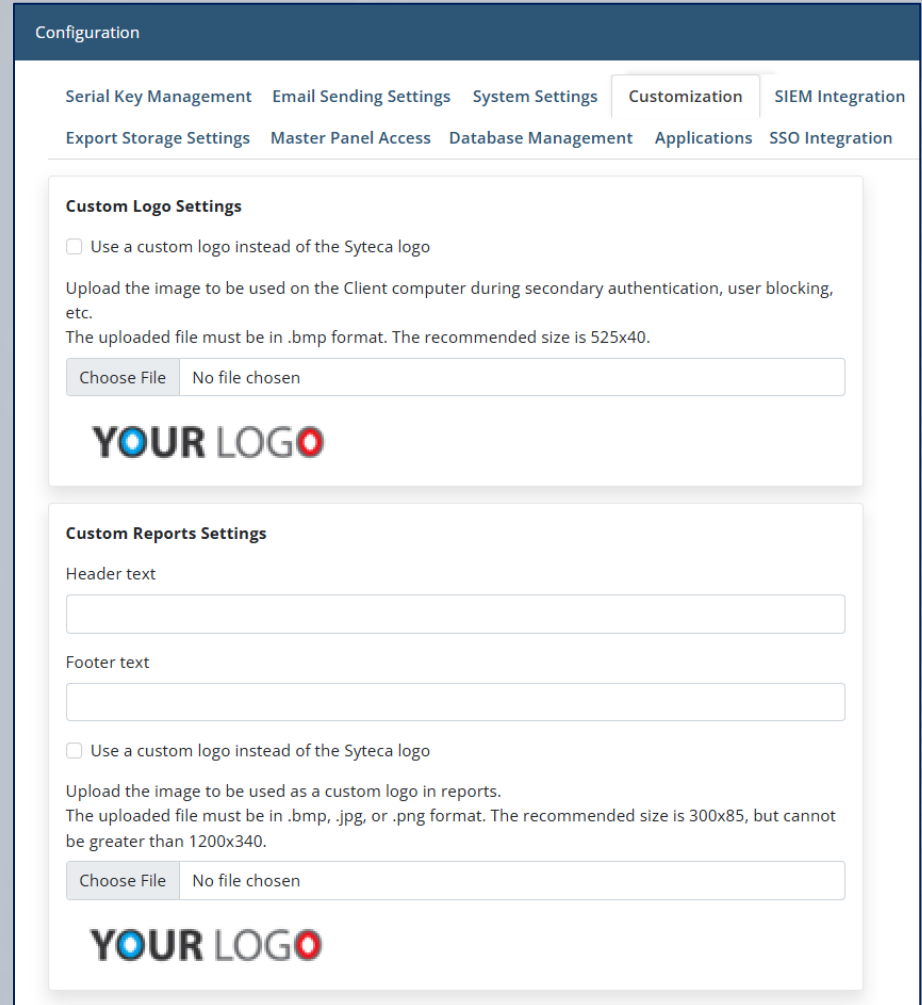
YOUR LOGO Activity Pie Chart Report

Details

Generated in	Ekran System
Server	WEB-DEMO
User	

Filter

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



Configuration

Serial Key Management Email Sending Settings System Settings **Customization** SIEM Integration

Export Storage Settings Master Panel Access Database Management Applications SSO Integration

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 No file chosen

YOUR LOGO

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 No file chosen

YOUR LOGO

Customizing Email Subjects and Messages



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

Configuration

be greater than 1200x340.

Choose File

No file chosen

Custom Email Subjects

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.

Single alert notification

Syteca Alert - #pc, #user - #OS - #name (#priority)

Multiple alerts notification

Syteca Multiple Alerts - #number

Restore Default

Custom Login Message for Blocked Users

You have been blocked. Contact your system administrator.

Two-Factor Authentication

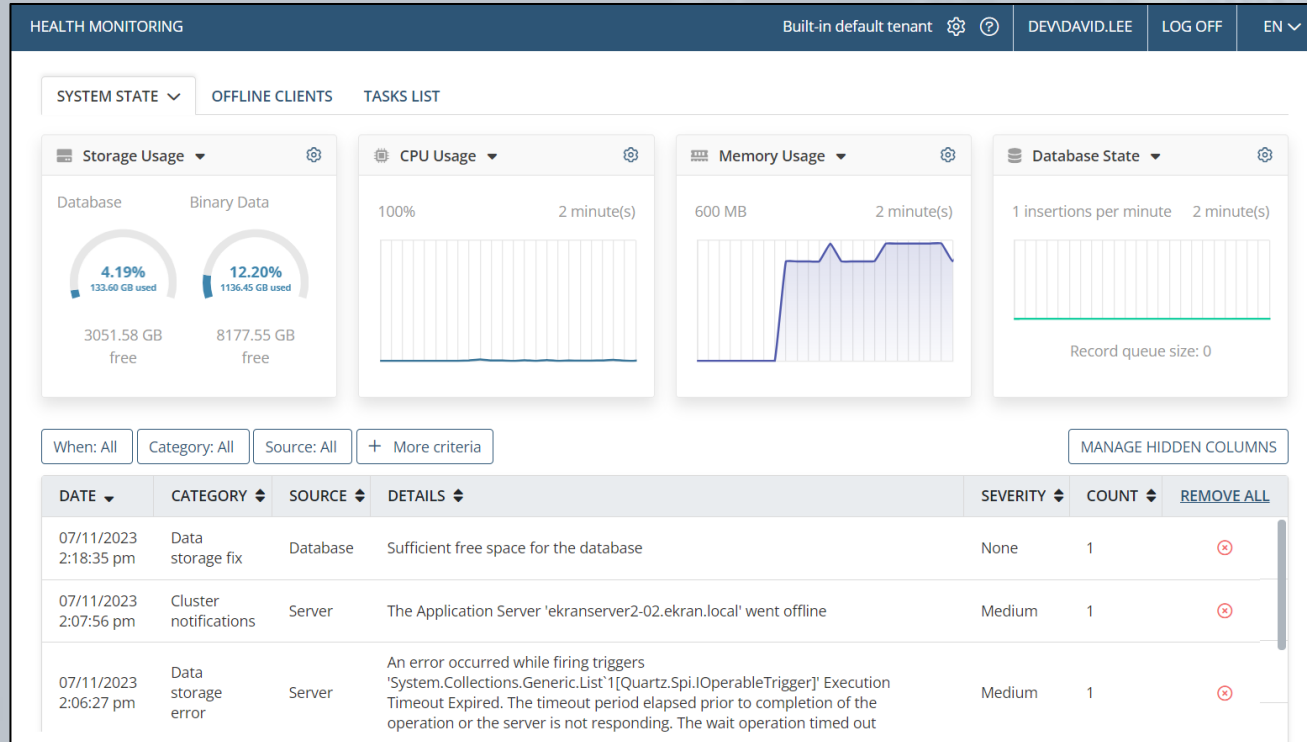
Main Screen

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

Save

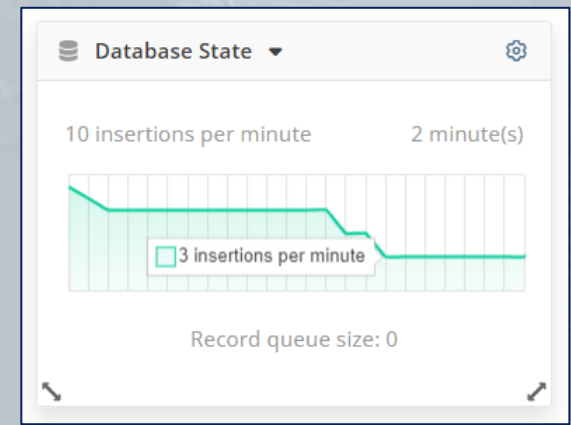
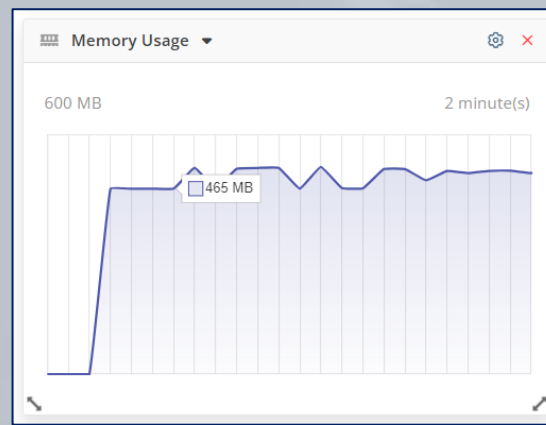
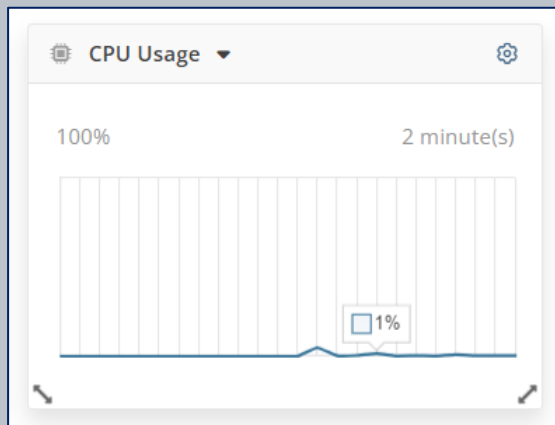
System Health Monitoring

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.

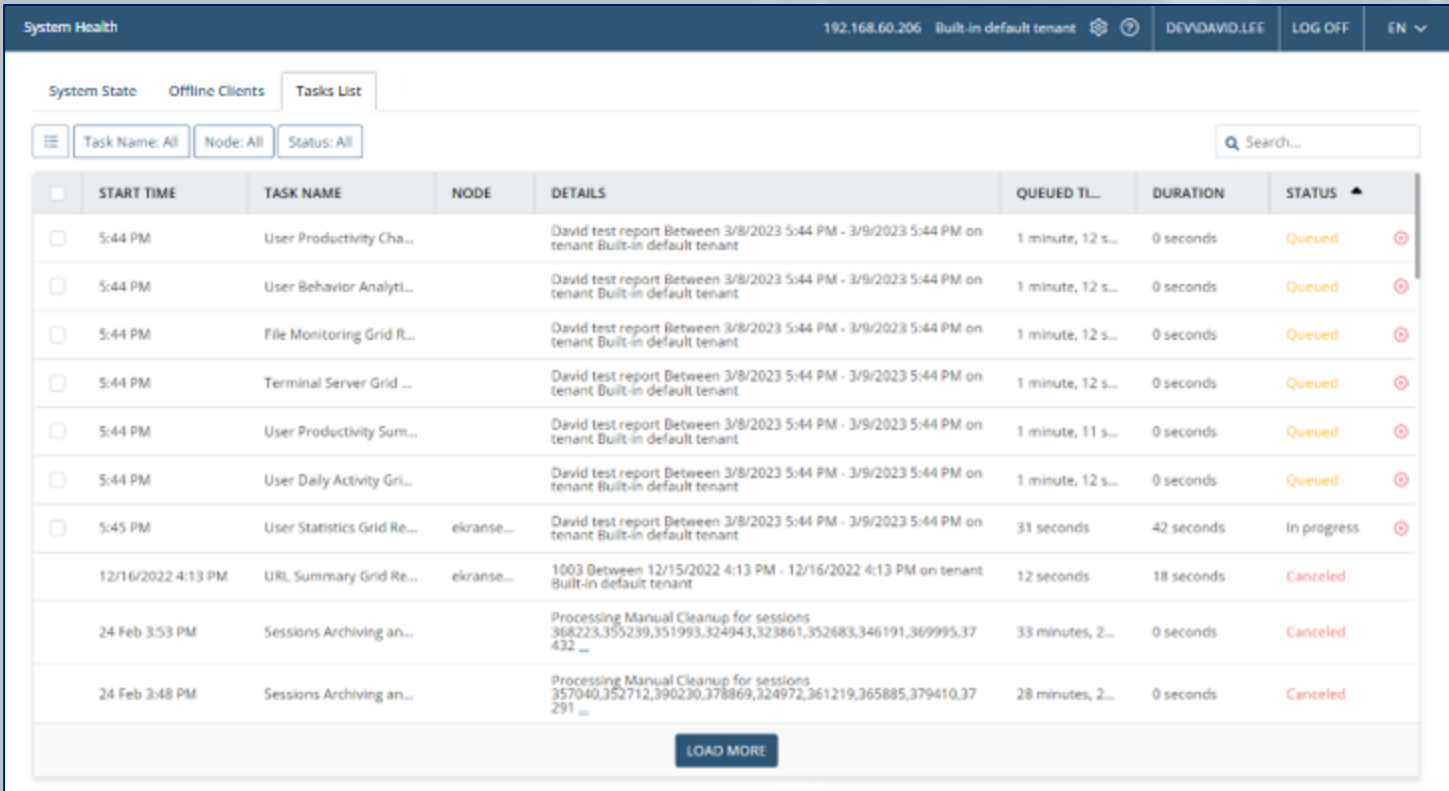


Resource monitoring allows you to view the **current resource usage** by the Syteca Application Server process:

- **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).



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

LOAD MORE

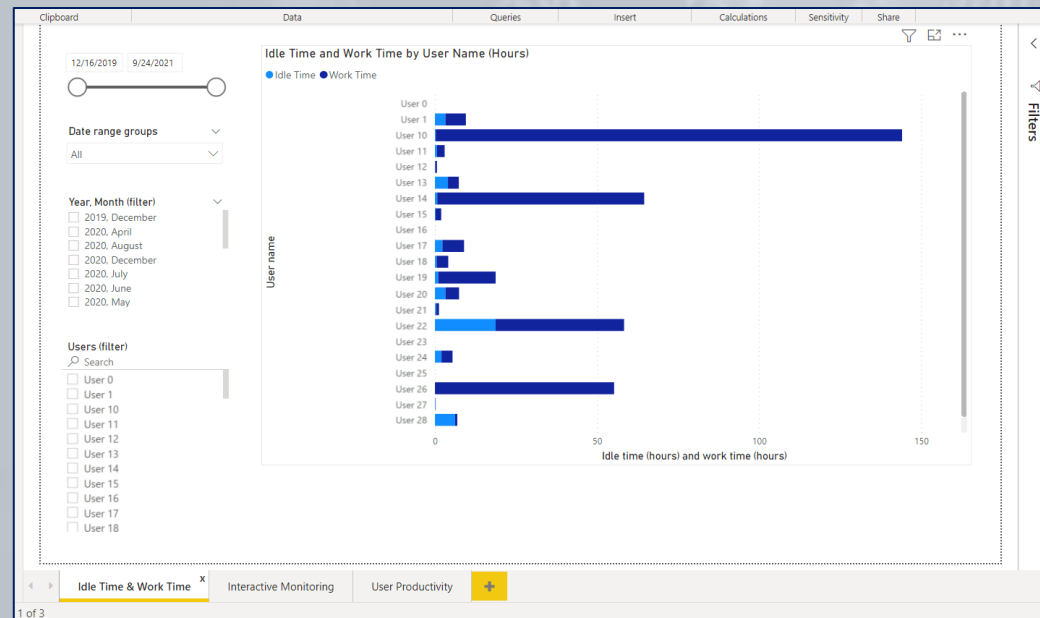
Syteca SDK, APIs and Integrations

(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.

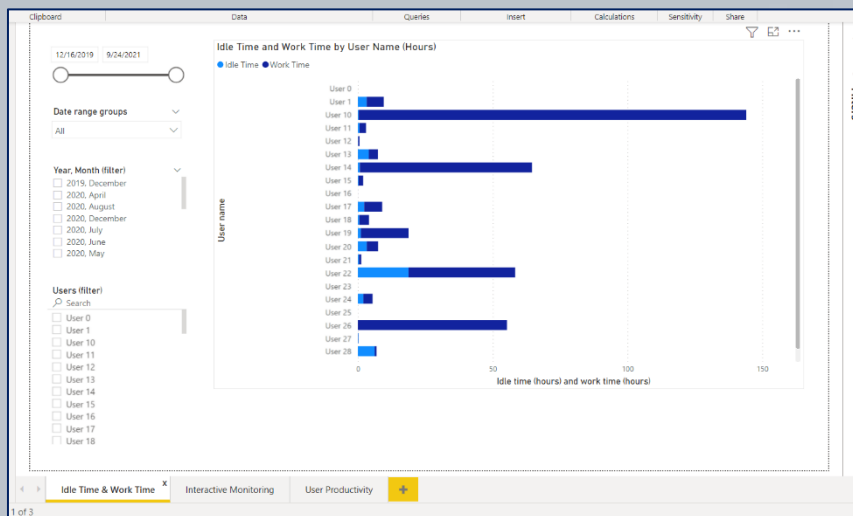
This application is designed to **allow customers to get Syteca monitoring data** via the API in order to **use for their own business purposes**.

Idle Time & Work Time Report

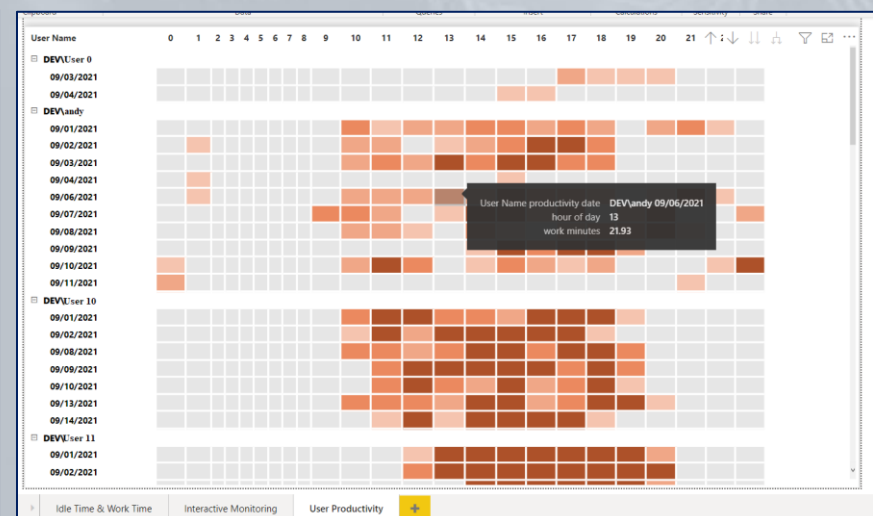


For example, **Client session records** containing **user productivity data** (such as **productivity time, idle time, duration**, etc.) can be used to build BI (business intelligence) reports in **Microsoft Power BI**.

Interactive Monitoring Report

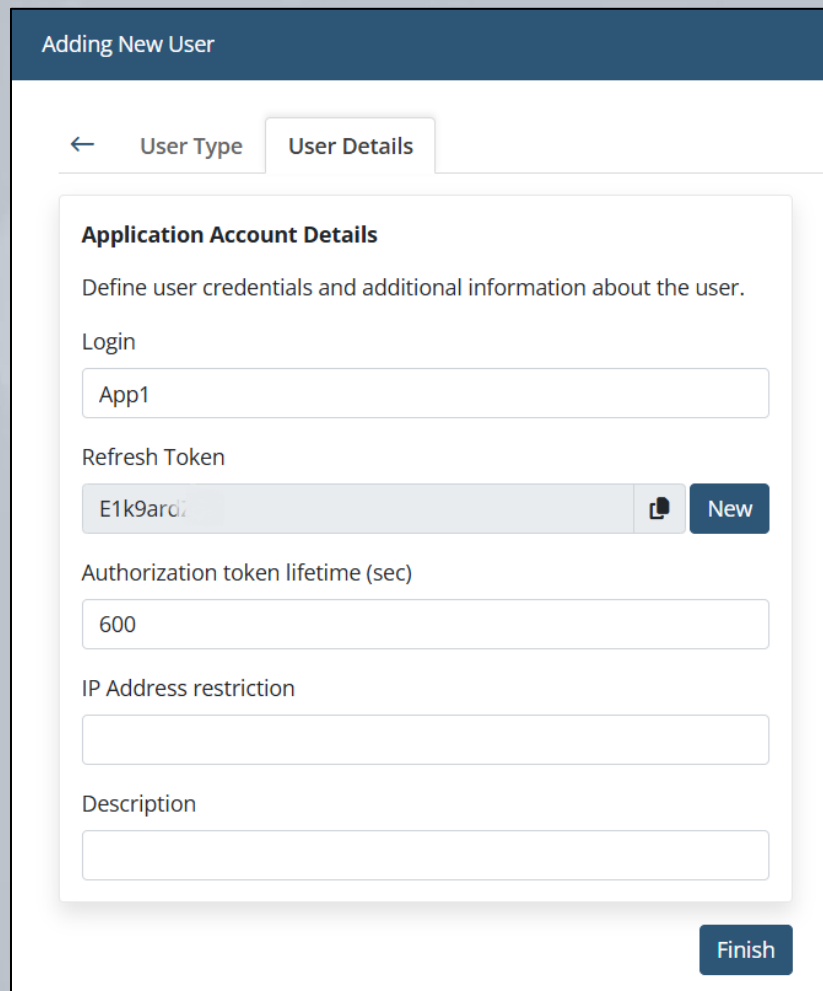


User Productivity Report



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

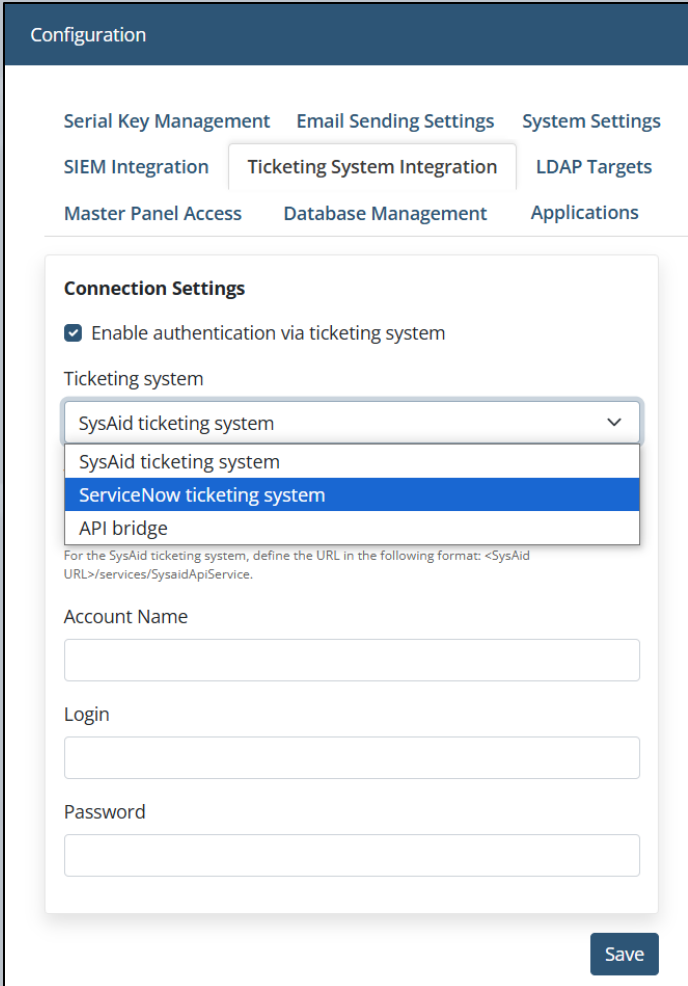
This application is designed to allow customers to **get Syteca secrets' data via the ACB API**, to use it for their own business purposes.



The screenshot displays the 'Adding New User' interface. At the top, a dark blue header bar contains the text 'Adding New User'. Below this, there are two tabs: 'User Type' and 'User Details', with 'User Details' being the active tab. The main content area is titled 'Application Account Details' and includes a subtitle 'Define user credentials and additional information about the user.' The form contains several input fields: 'Login' with the value 'App1', 'Refresh Token' with the value 'E1k9ard' and a 'New' button, 'Authorization token lifetime (sec)' with the value '600', 'IP Address restriction' (empty), and 'Description' (empty). A 'Finish' button is located at the bottom right of the form.

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 'Ticketing System Integration' tab is selected. Under 'Connection Settings', the checkbox 'Enable authentication via ticketing system' is checked. The 'Ticketing system' dropdown menu is open, showing options: 'SysAid ticketing system', 'ServiceNow ticketing system' (highlighted), and 'API bridge'. Below the dropdown, a note specifies the URL format for SysAid: '<SysAid URL>/services/SysaidApiService.'. There are input fields for 'Account Name', 'Login', and 'Password'. A 'Save' button is located at the bottom right.

Configuration

Serial Key Management Email Sending Settings System Settings

SIEM Integration **Ticketing System Integration** LDAP Targets

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 top bar shows the date 13/08/2024, user MBP-user, and a LIVE status. The main content area features a video player showing the Venn website, which promotes 'The Secure Workspace for Remote Work'. Below the video, there is a list of applications and their activity. The table below represents the data shown in the application list.

ACT...	ACTIV...	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...		

The interface also includes a search bar, a 'BACK TO FILTERED MODE' button, and a pagination control at the bottom right showing 50, 100, 250, 500, and 1000 items, with 1 item currently displayed.

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.

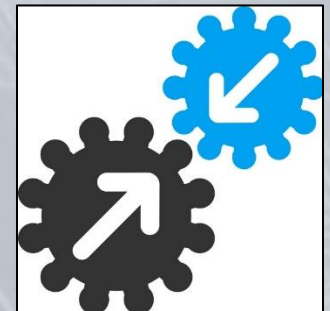
The login interface features a 'LOG IN' header and a sub-header 'Use an internal or domain account to log in.' Below this are input fields for 'Login' and 'Password'. A 'Remember me on this computer' checkbox is located below the password field. A 'Log in' button is positioned to the right of the password field. A red-bordered button labeled 'Log in with SSO' is located at the bottom right of the login form.

The configuration interface is titled 'Configuration' and shows 'localhost' in the top right corner. A navigation bar contains several menu items: 'Serial Key Management', 'Email Sending Settings', 'System Settings', 'Customization', 'SIEM Integration', 'Ticketing System Integration', 'Export Storage Settings', 'Master Panel Access', 'Database Management', 'Embedding Settings', 'Applications', and 'SSO Integration' (which is highlighted with a red border). The main content area is for SSO configuration and includes the following fields and options:

- 'Issuer name' with a text input field containing 'https://example/ES'.
- 'Identity provider metadata (xml)' with a 'Choose File' button and 'No file chosen' text.
- Radio buttons for 'Self-signed certificate' and 'Custom certificate' (the latter is selected).
- 'Certificate (pfx)' with a 'Choose File' button and 'No file chosen' text.
- 'Certificate password' with a password input field.
- A checked checkbox for 'Auto-create a Management Tool account for a new user on the first SSO login'.
- A 'Save' button at the bottom right.

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