



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](#)
- [Anonymizer \(for e.g. GDPR Compliance\)](#)
- [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 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.

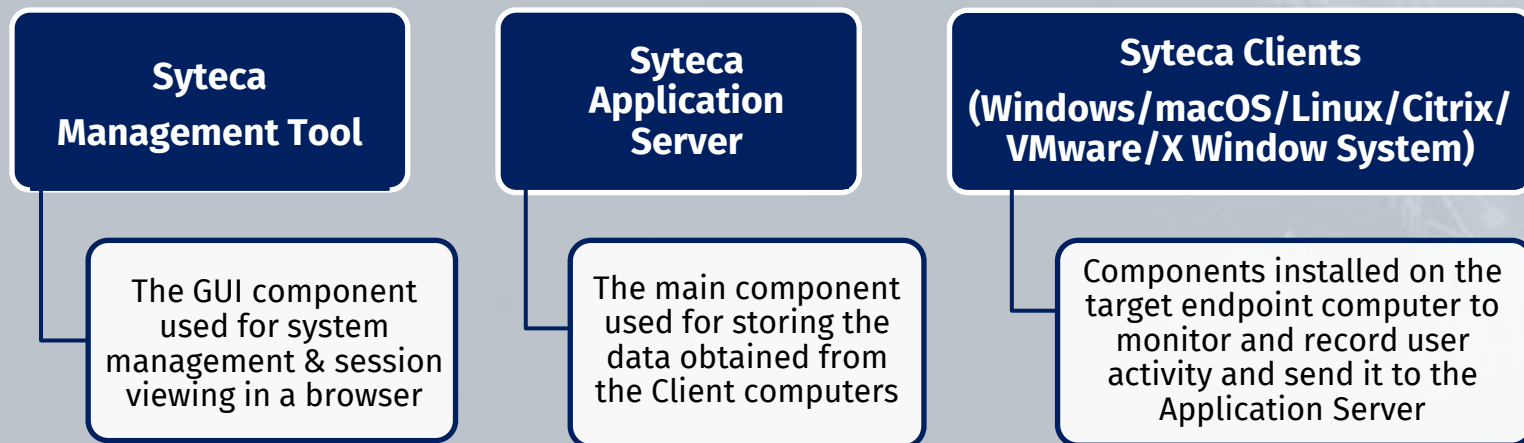
Flexible Deployment and Licensing

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.

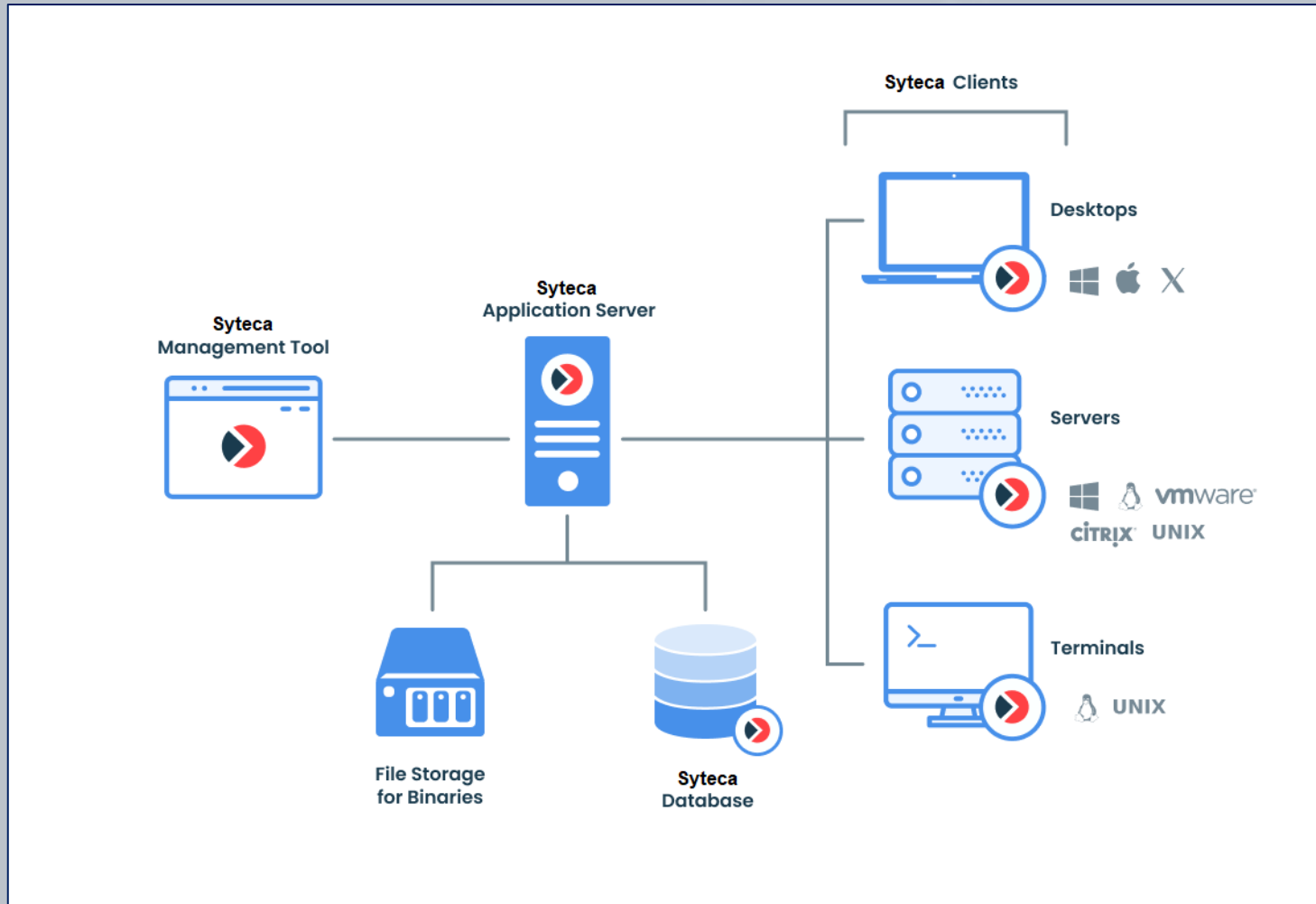
Syteca (formerly **Ekran System**) is an enterprise-level **cybersecurity platform** software solution featuring **privileged access management (PAM)** and **user activity monitoring (UAM)**. It is used to **protect** your corporate IT infrastructure from **internal risks**, as well as to assist you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

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

The Main Components of Syteca



The Basic Deployment Scheme

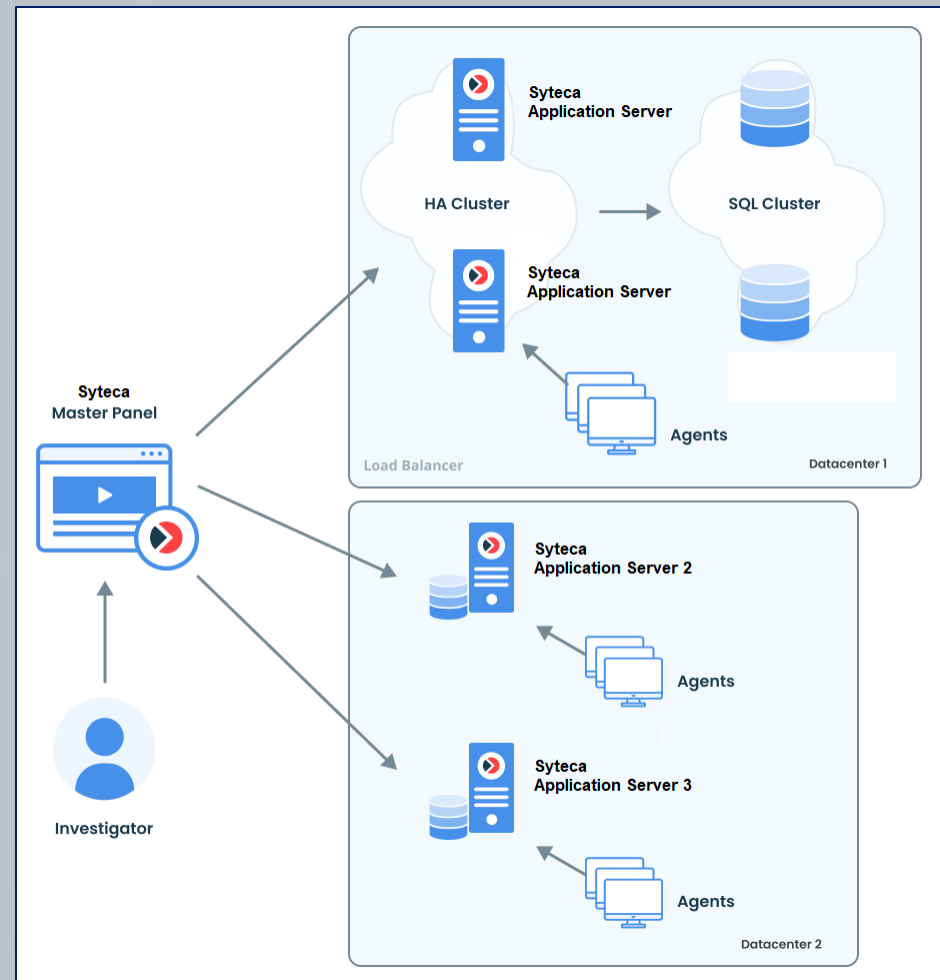


Large-Scale Deployments

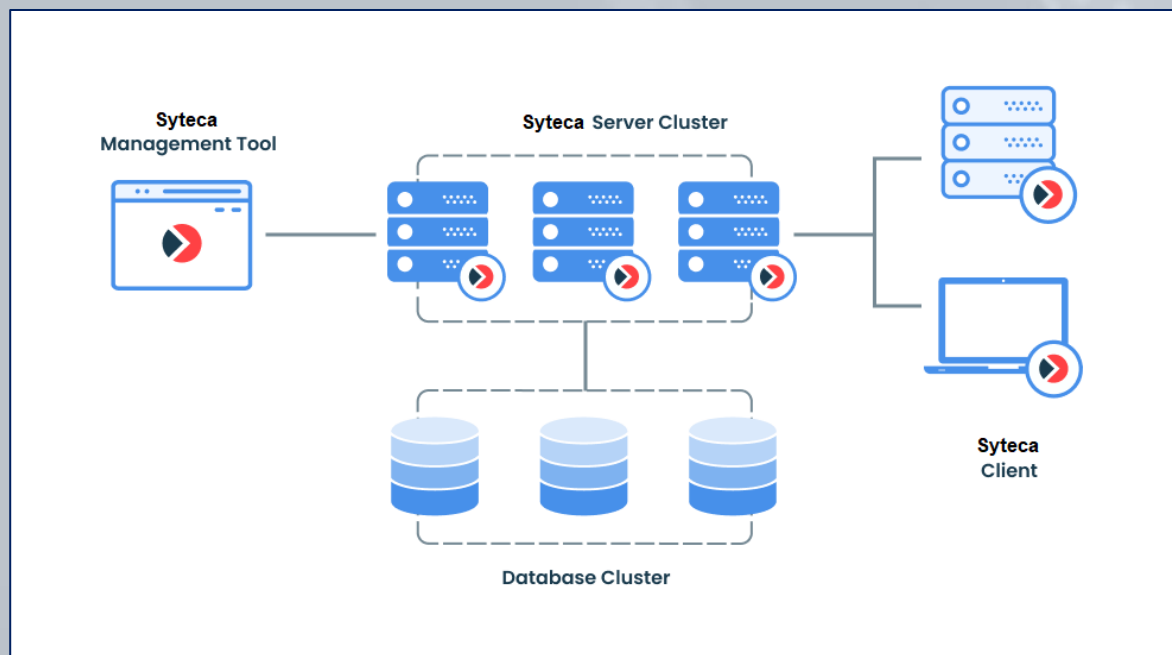
In terms of scalability, and for large organizations which may have several geographically isolated data centers, **multiple connected** instances of the **Application Server** can be deployed.

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.

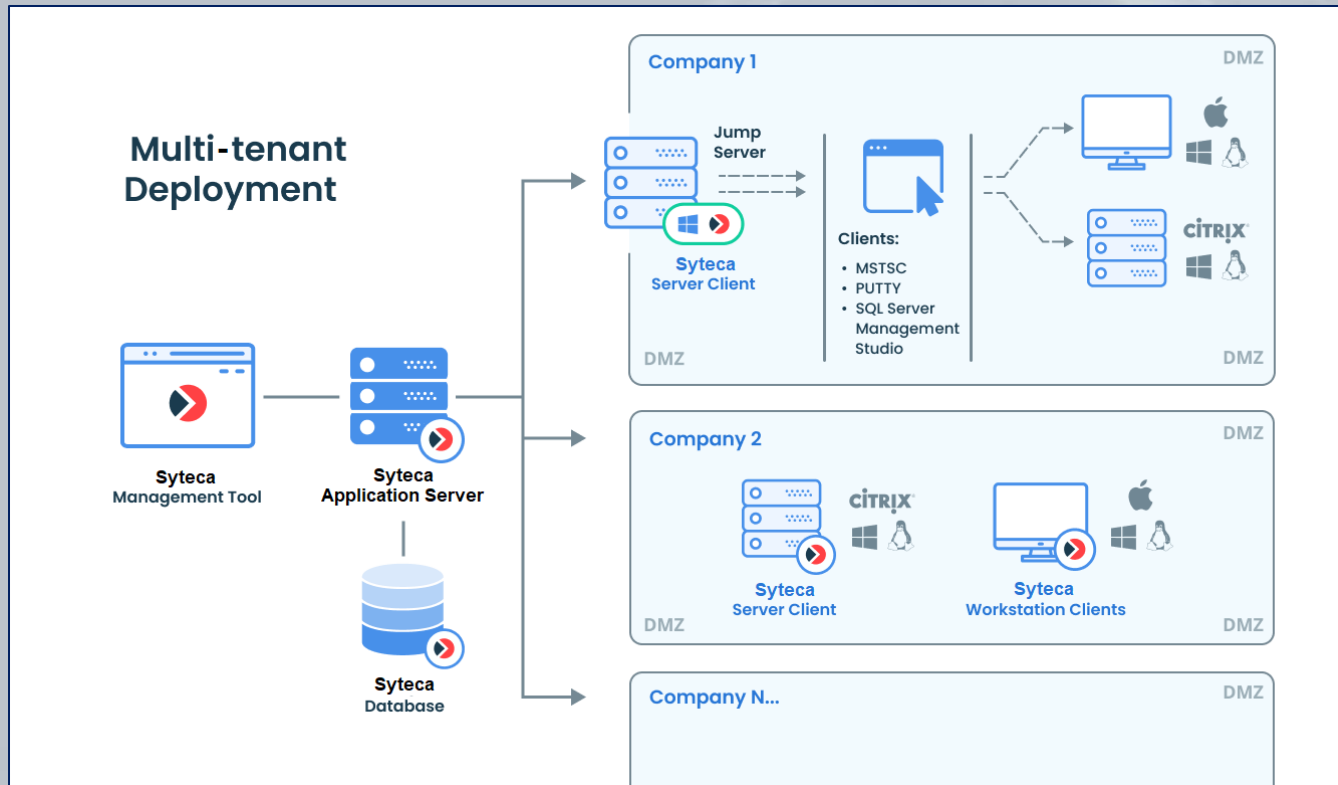
The **Master Panel**, which is an additional stand-alone component of Syteca, **combines the data** recorded by all Syteca Applications Servers in multiple locations, allowing the data to be **viewed and managed in a single user interface**.



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**.



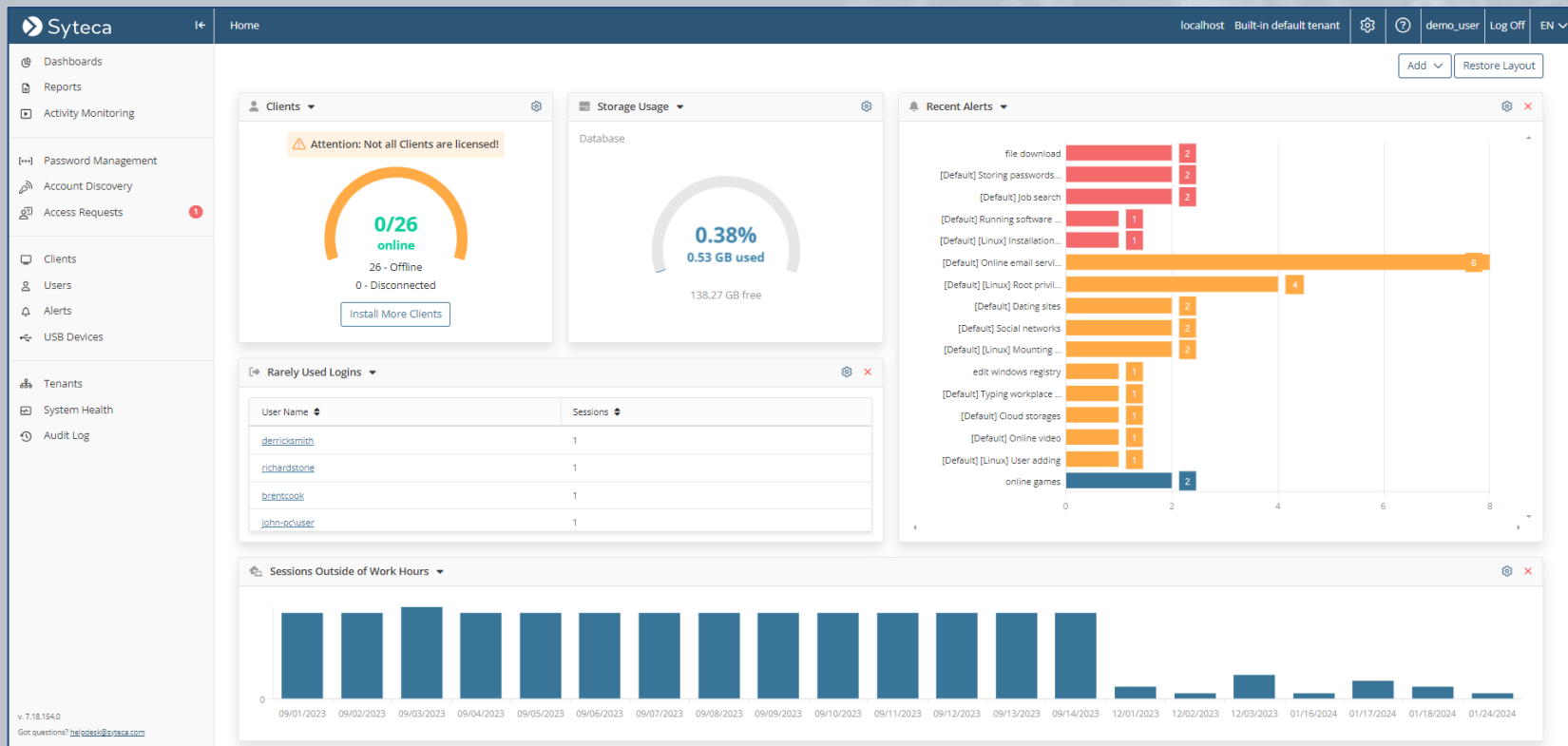
Multi-Tenant mode allows **multiple** completely **isolated tenants** to operate in the Syteca environment. The **data** in each tenant is **independent** and not accessible to other tenants.



The 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.

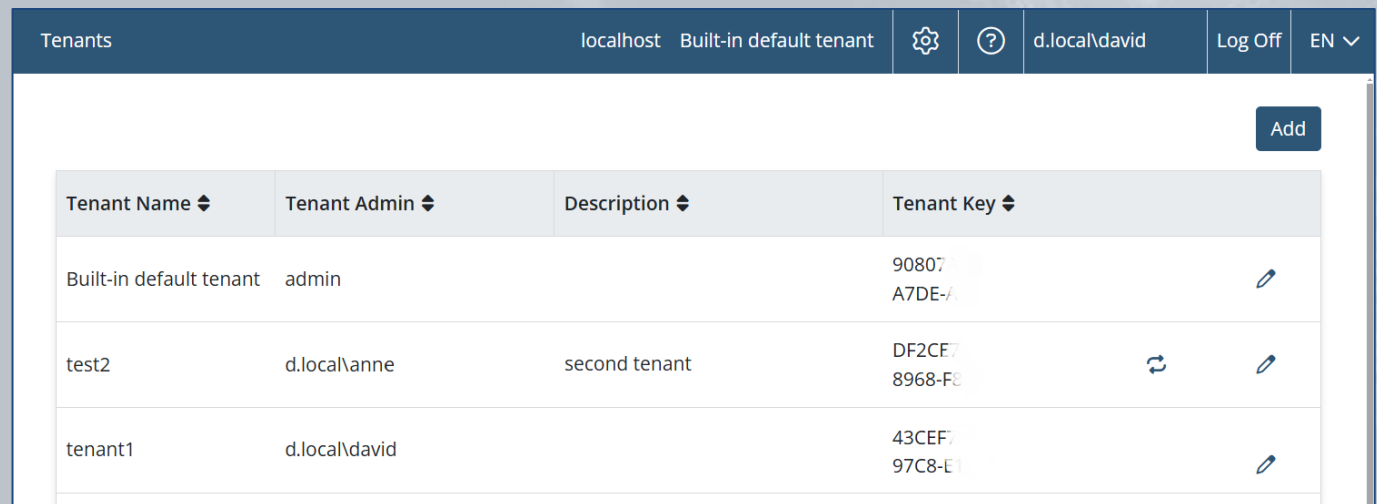






Syteca can operate in Single-Tenant or **Multi-Tenant mode**.

Single-Tenant mode is selected by default. In this mode, **all users have access to all Clients and settings** according to their permissions.

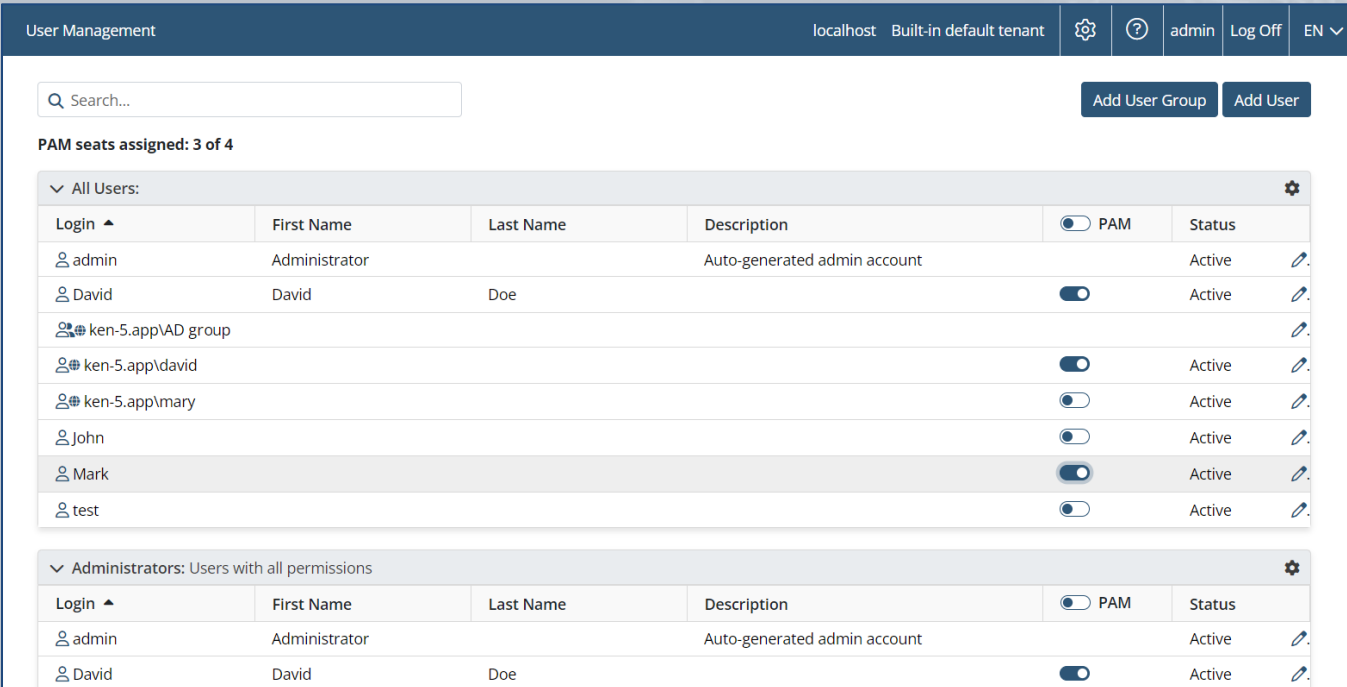
In Multi-Tenant mode, all tenant **users** have access to their tenant Clients, but **do not have access to other tenants'** Clients, configurations, alerts, reports, etc.

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



Tenant Name	Tenant Admin	Description	Tenant Key	
Built-in default tenant	admin		90807 A7DE-7	
test2	d.local\anne	second tenant	DF2CE7 8968-F8	 
tenant1	d.local\david		43CE7 97C8-E1	

- Create **3 types of users**: Internal, Active Directory (Windows/macOS domain users/groups) or application accounts.
- Use **groups** for easier management of users.
- Define **permissions** for users/groups.



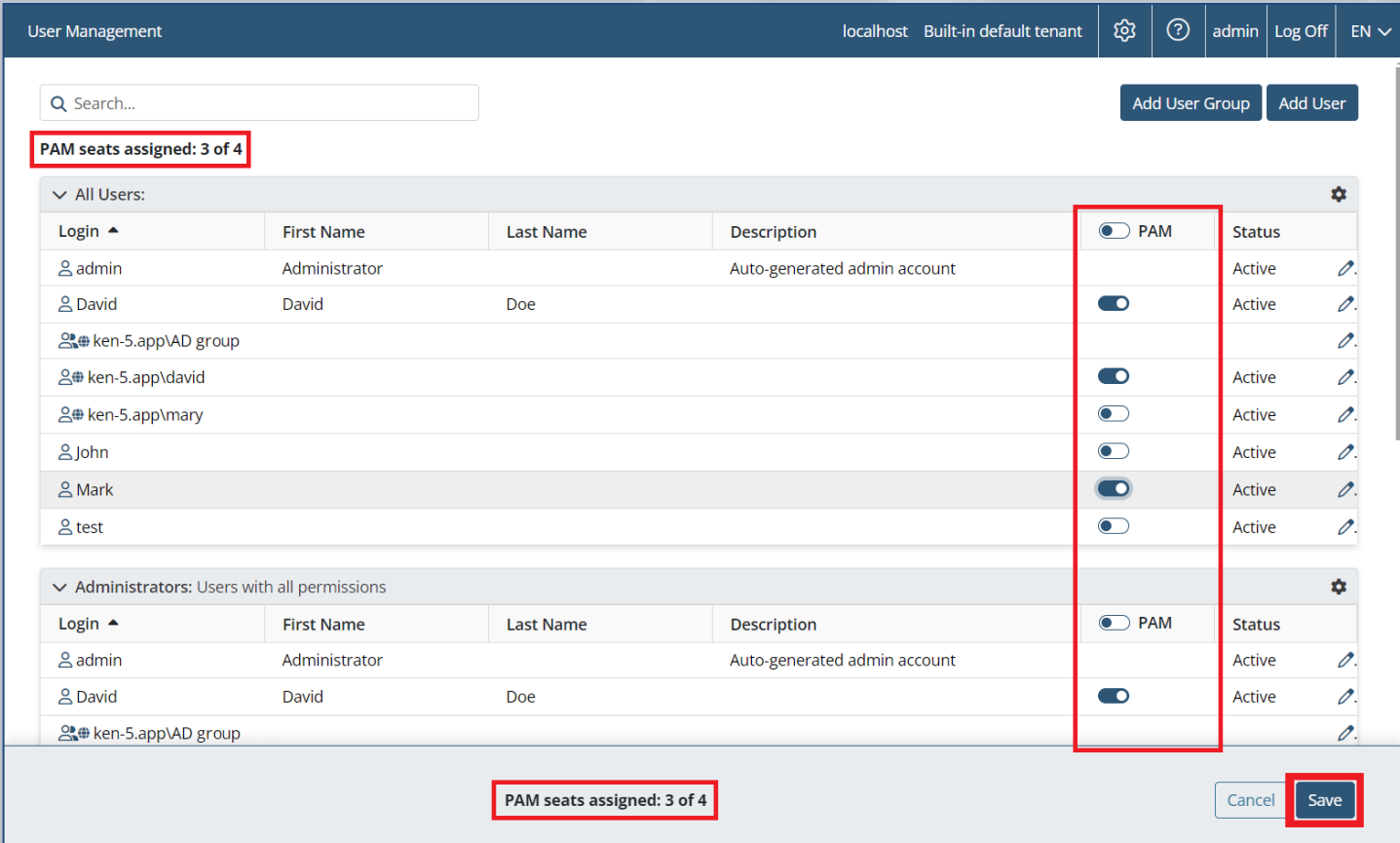
The screenshot displays the 'User Management' interface. At the top, there is a navigation bar with 'localhost Built-in default tenant' and user 'admin'. A search bar is present with the text 'Search...'. Below the search bar, there are two buttons: 'Add User Group' and 'Add User'. A status indicator shows '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 users like 'admin', 'David', and 'ken-5.app\david', along with a group 'ken-5.app\VAD group'. The 'Administrators' section lists 'admin' and 'David'.

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

Assign PAM Licenses to Users

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

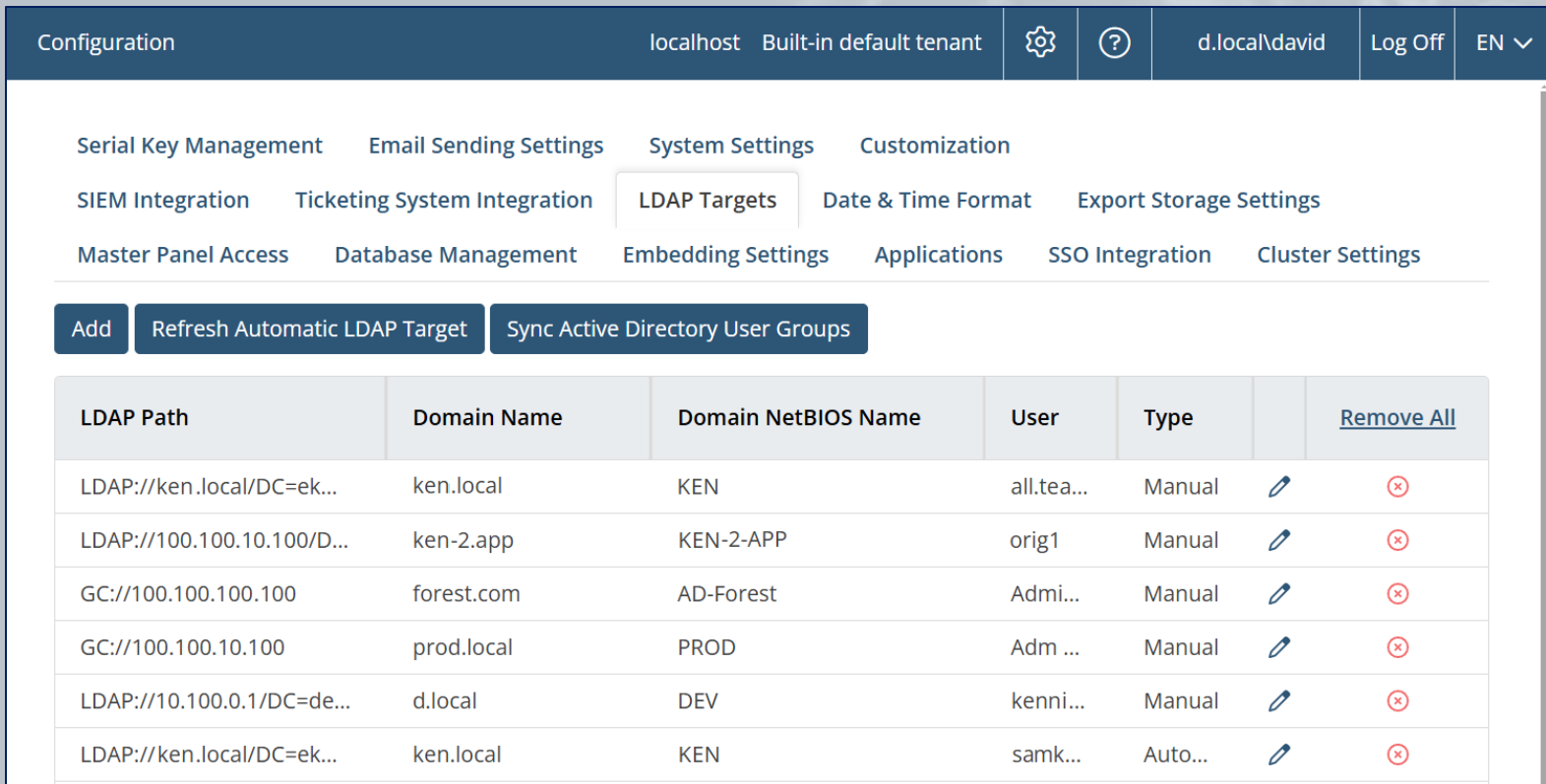


The screenshot shows the 'User Management' interface. At the top, there is a search bar and buttons for 'Add User Group' and 'Add User'. A red box highlights the text 'PAM seats assigned: 3 of 4' in the top left. Below this, there are two tables. The first table, 'All Users', lists users with columns for Login, First Name, Last Name, Description, PAM (toggle), and Status. The second table, 'Administrators: Users with all permissions', lists administrators with similar columns. A red box highlights the PAM toggle for the 'David' user in both tables. At the bottom, another red box highlights '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 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**.



The screenshot shows the Syteca configuration interface. At the top, there is a navigation bar with "Configuration", "localhost", "Built-in default tenant", a settings icon, a help icon, "d.local\david", "Log Off", and "EN". Below this, there are several tabs for configuration: "Serial Key Management", "Email Sending Settings", "System Settings", "Customization", "SIEM Integration", "Ticketing System Integration", "LDAP Targets" (which is selected), "Date & Time Format", "Export Storage Settings", "Master Panel Access", "Database Management", "Embedding Settings", "Applications", "SSO Integration", and "Cluster Settings".

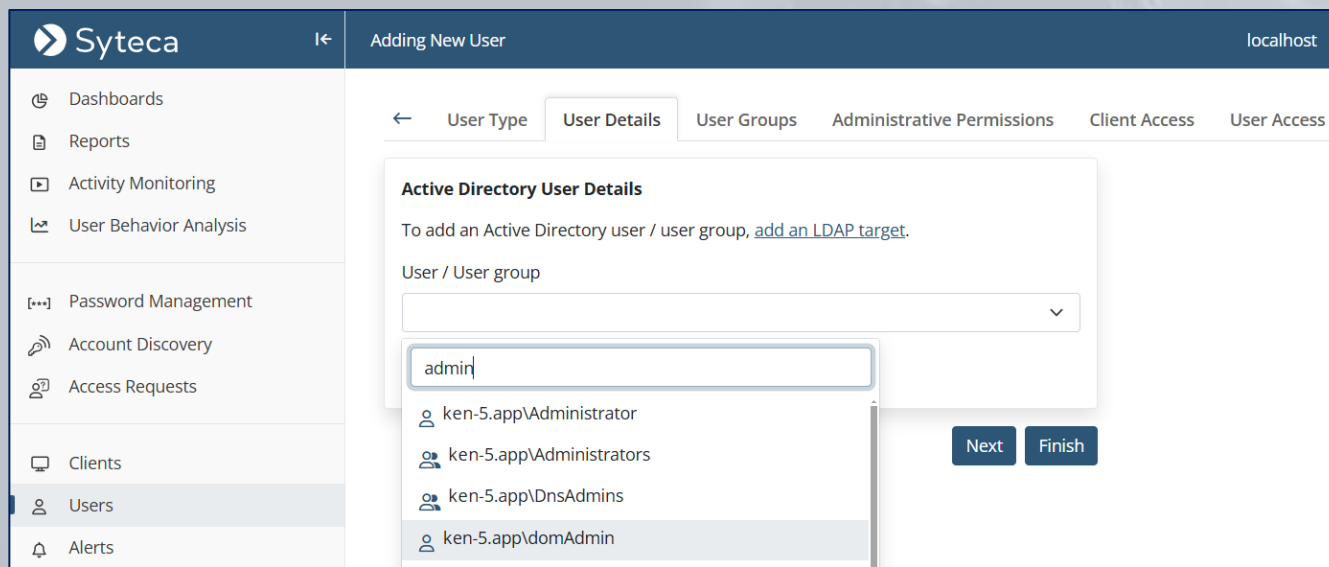
Below the tabs, there are three buttons: "Add", "Refresh Automatic LDAP Target", and "Sync Active Directory User Groups".

The main content area displays a table of LDAP Targets. The table has the following columns: "LDAP Path", "Domain Name", "Domain NetBIOS Name", "User", "Type", and "Remove All".

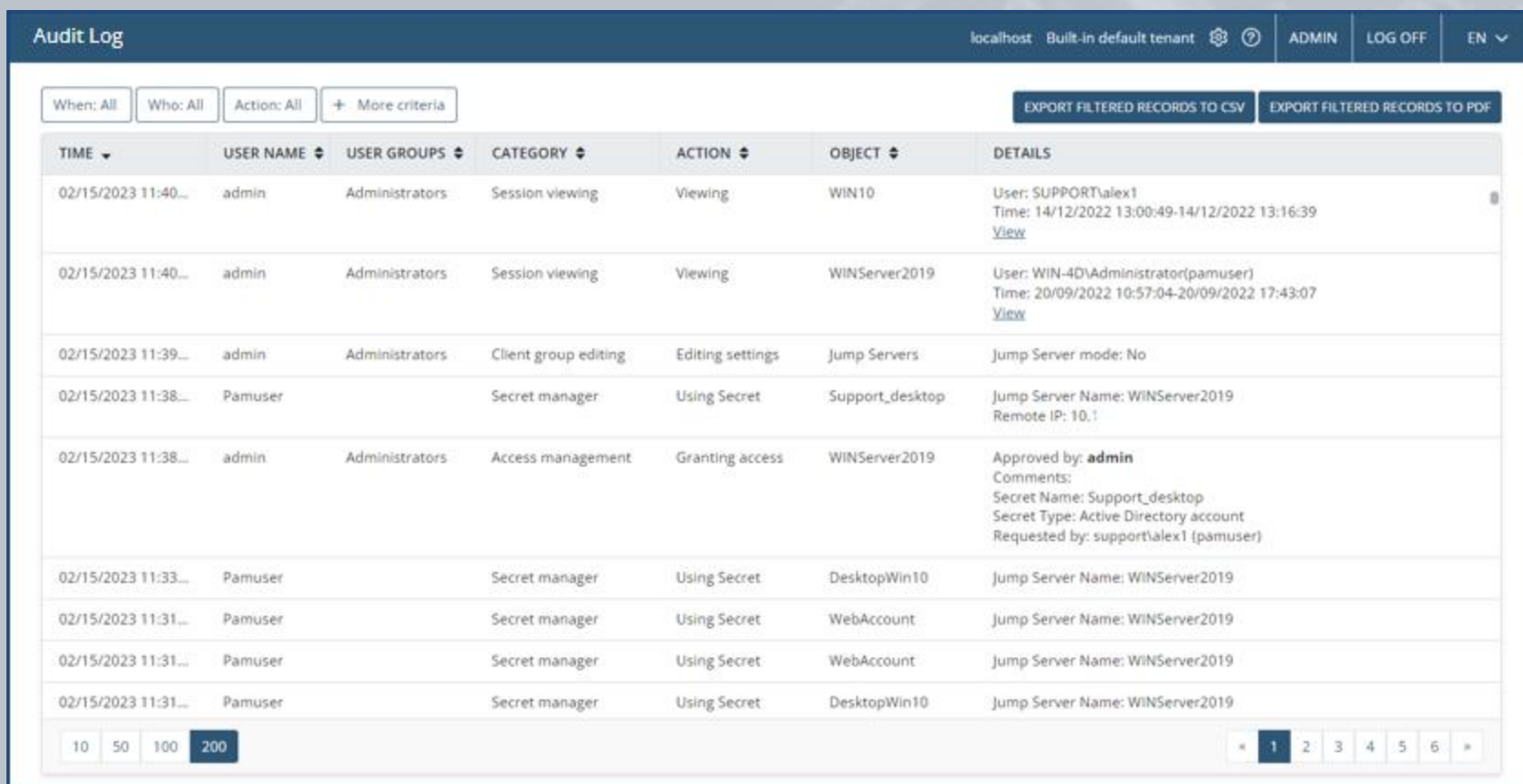
LDAP Path	Domain Name	Domain NetBIOS Name	User	Type	Remove All
LDAP://ken.local/DC=ek...	ken.local	KEN	all.tea...	Manual	 
LDAP://100.100.10.100/D...	ken-2.app	KEN-2-APP	orig1	Manual	 
GC://100.100.100.100	forest.com	AD-Forest	Admi...	Manual	 
GC://100.100.10.100	prod.local	PROD	Adm ...	Manual	 
LDAP://10.100.0.1/DC=de...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



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

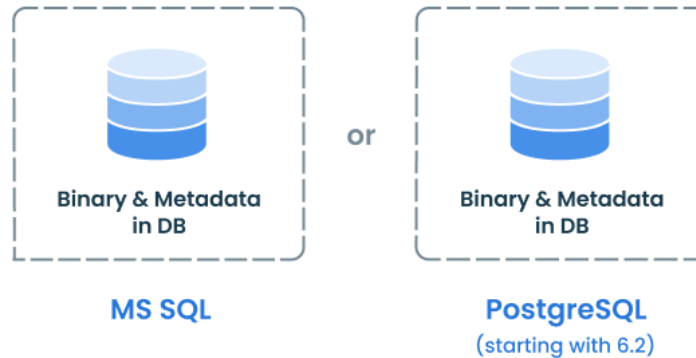


The screenshot displays the 'Audit Log' interface. At the top, there are navigation links for 'localhost', 'Built-in default tenant', 'ADMIN', 'LOG OFF', and 'EN'. Below the navigation, there are filter buttons for 'When: All', 'Who: All', 'Action: All', and '+ More criteria'. On the right, there are buttons for 'EXPORT FILTERED RECORDS TO CSV' and 'EXPORT FILTERED RECORDS TO PDF'. The main content is a table with the following columns: TIME, USER NAME, USER GROUPS, CATEGORY, ACTION, OBJECT, and DETAILS. The table contains several rows of activity logs, including session viewing, client group editing, secret manager usage, and access management. At the bottom, there are pagination controls showing '10', '50', '100', and '200' records per page, and a page number '1'.

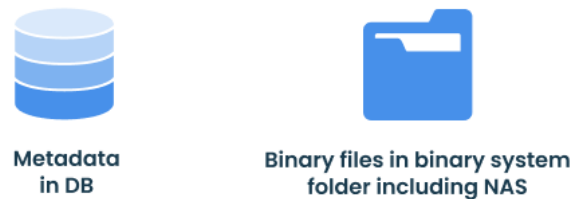
TIME	USER NAME	USER GROUPS	CATEGORY	ACTION	OBJECT	DETAILS
02/15/2023 11:40...	admin	Administrators	Session viewing	Viewing	WIN10	User: SUPPORT\alex1 Time: 14/12/2022 13:00:49-14/12/2022 13:16:39 View
02/15/2023 11:40...	admin	Administrators	Session viewing	Viewing	WINServer2019	User: WIN-4D\Administrator(pamuser) 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

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)

Start at

Action type

Sessions older than (days)

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

.....

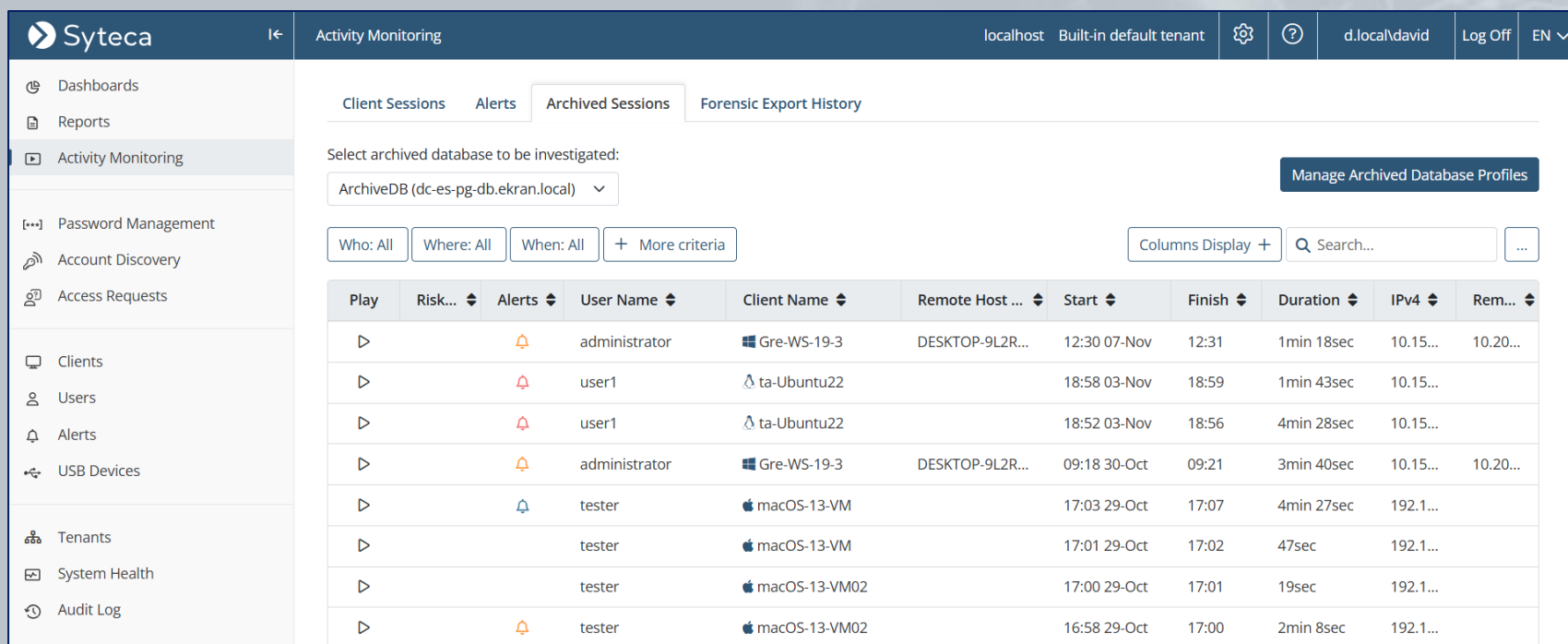
Shrink database transaction log after cleanup

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**.

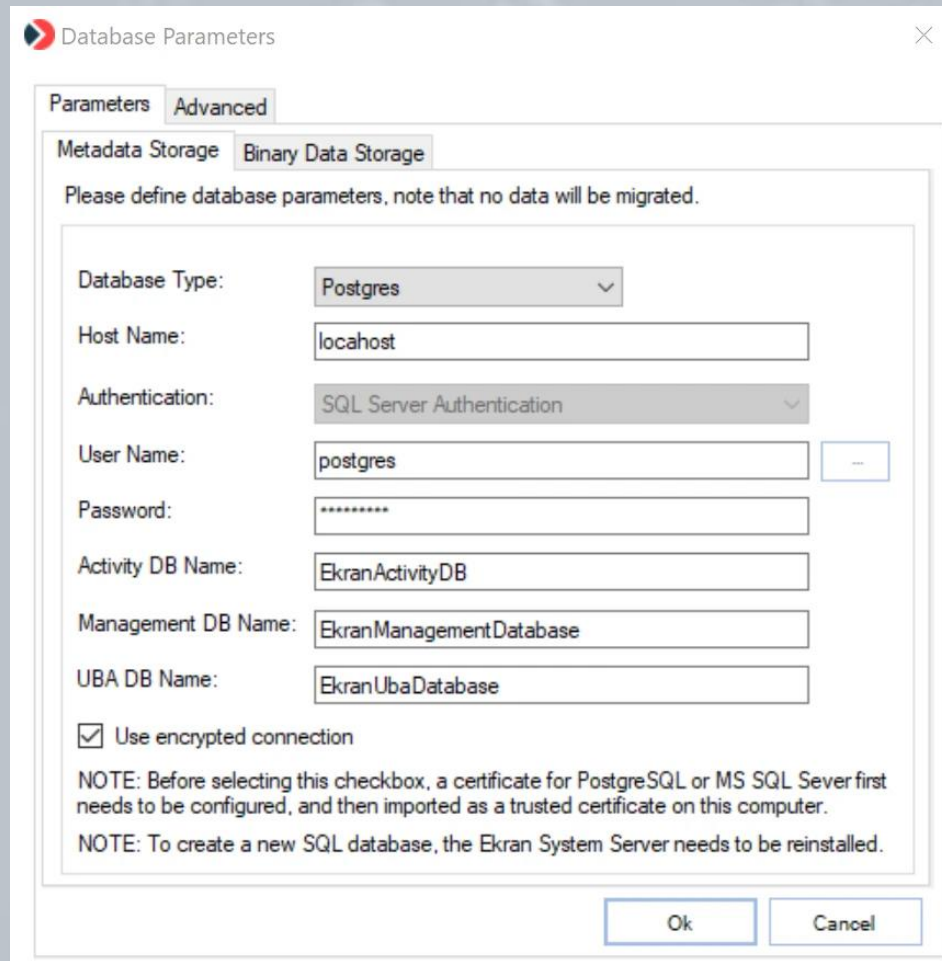


The screenshot displays the Syteca Activity Monitoring interface. The top navigation bar includes the Syteca logo, a back arrow, the title 'Activity Monitoring', and user information: 'localhost Built-in default tenant', a settings gear, a help icon, 'd.local\ david', 'Log Off', and 'EN'. The left sidebar contains a menu with items: 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 has tabs for 'Client Sessions', 'Alerts', 'Archived Sessions' (active), and 'Forensic Export History'. Below the tabs, there is a dropdown menu for 'Select archived database to be investigated:' with 'ArchiveDB (dc-es-pg-db.ekran.local)' selected. A 'Manage Archived Database Profiles' button is to the right. Below this are filter buttons: 'Who: All', 'Where: All', 'When: All', and '+ More criteria'. To the right of these are 'Columns Display +' and a search box with 'Search...' and a dropdown arrow. The main area contains a table of archived sessions.

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 for the connection between the Application and the Database (if it was not enabled during installation).



The screenshot shows the 'Database Parameters' dialog box with the 'Advanced' tab selected. The 'Binary Data Storage' sub-tab is active. The dialog contains the following fields and options:

- Database Type: Postgres (dropdown)
- Host Name: localhost (text input)
- Authentication: SQL Server Authentication (dropdown)
- User Name: postgres (text input)
- Password: ***** (password input)
- Activity DB Name: EkranActivityDB (text input)
- Management DB Name: EkranManagementDatabase (text input)
- UBA DB Name: EkranUbaDatabase (text input)
- Use encrypted connection

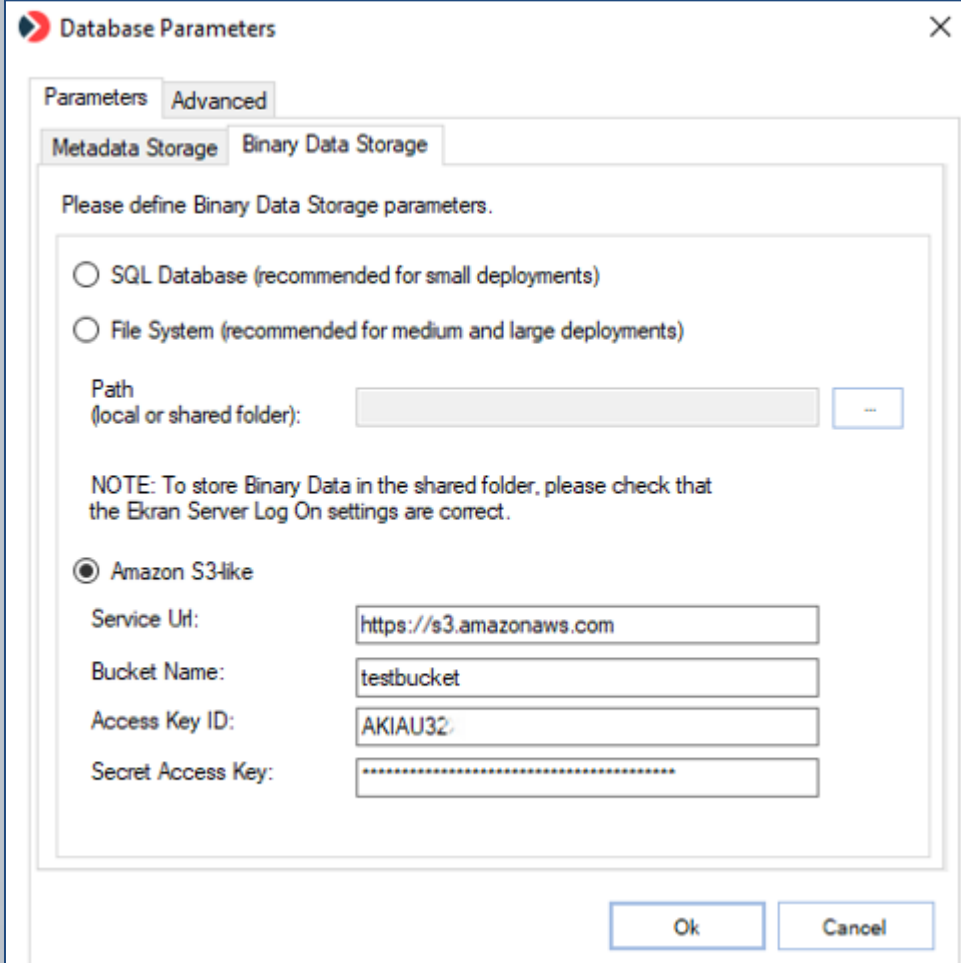
Two notes are displayed at the bottom of the dialog:

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

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

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 dialog box titled "Database Parameters" 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 content area contains the text "Please define Binary Data Storage parameters." followed by two radio button options: "SQL Database (recommended for small deployments)" and "File System (recommended for medium and large deployments)". Below these is a "Path (local or shared folder):" label with a text input field and a browse button ("..."). A note states: "NOTE: To store Binary Data in the shared folder, please check that the Ekran Server Log On settings are correct." The "Amazon S3-like" option is selected with a radio button. Below it are four text input fields: "Service Url:" (containing "https://s3.amazonaws.com"), "Bucket Name:" (containing "testbucket"), "Access Key ID:" (containing "AKIAU32"), and "Secret Access Key:" (containing a series of dots). At the bottom right, there are "Ok" and "Cancel" buttons.

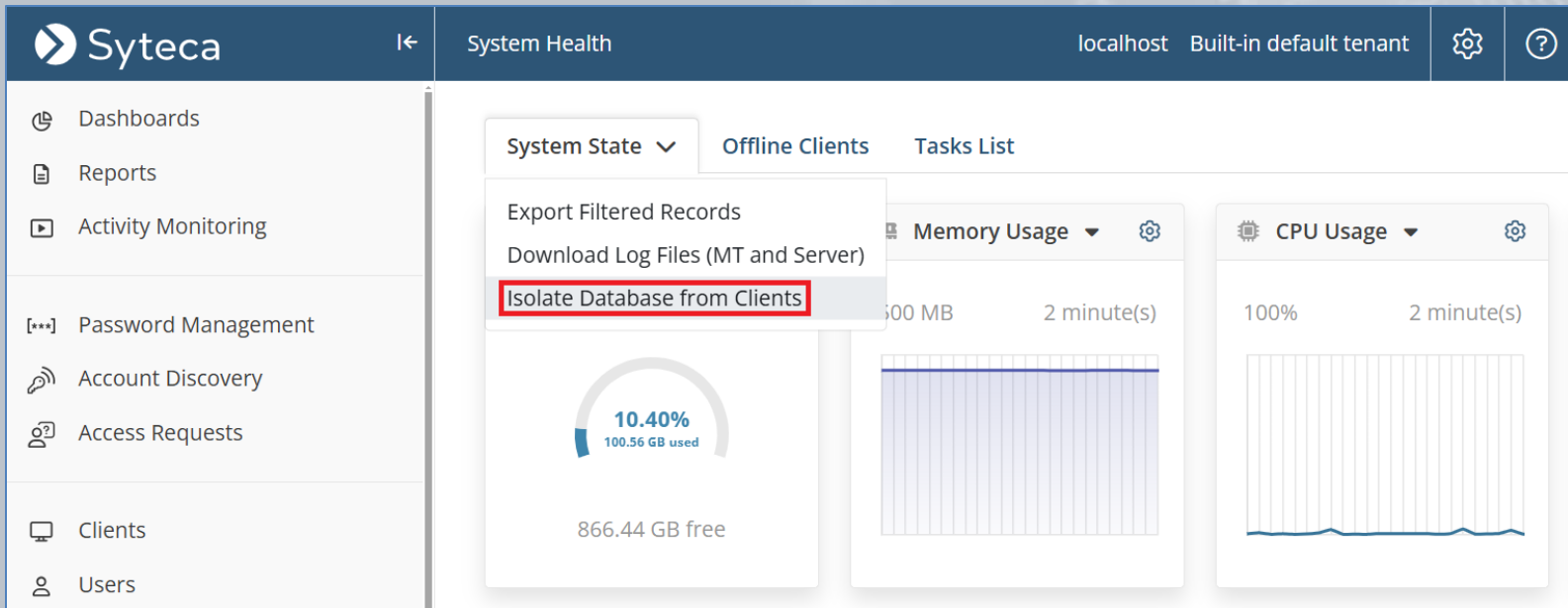
Database Parameters (Hardware Security Module) Syteca

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 image shows two overlapping dialog boxes. The background dialog is titled "Database Parameters" and has tabs for "Parameters" and "Advanced". It contains a warning message: "You can clean up sessions of deleted Clients. This action cannot be undone." with a "Clean up lost sessions" button. Below it is a "Reissue Master Certificate" button. The foreground dialog is titled "SafeNet KeySecure Options" and contains the following fields and options:

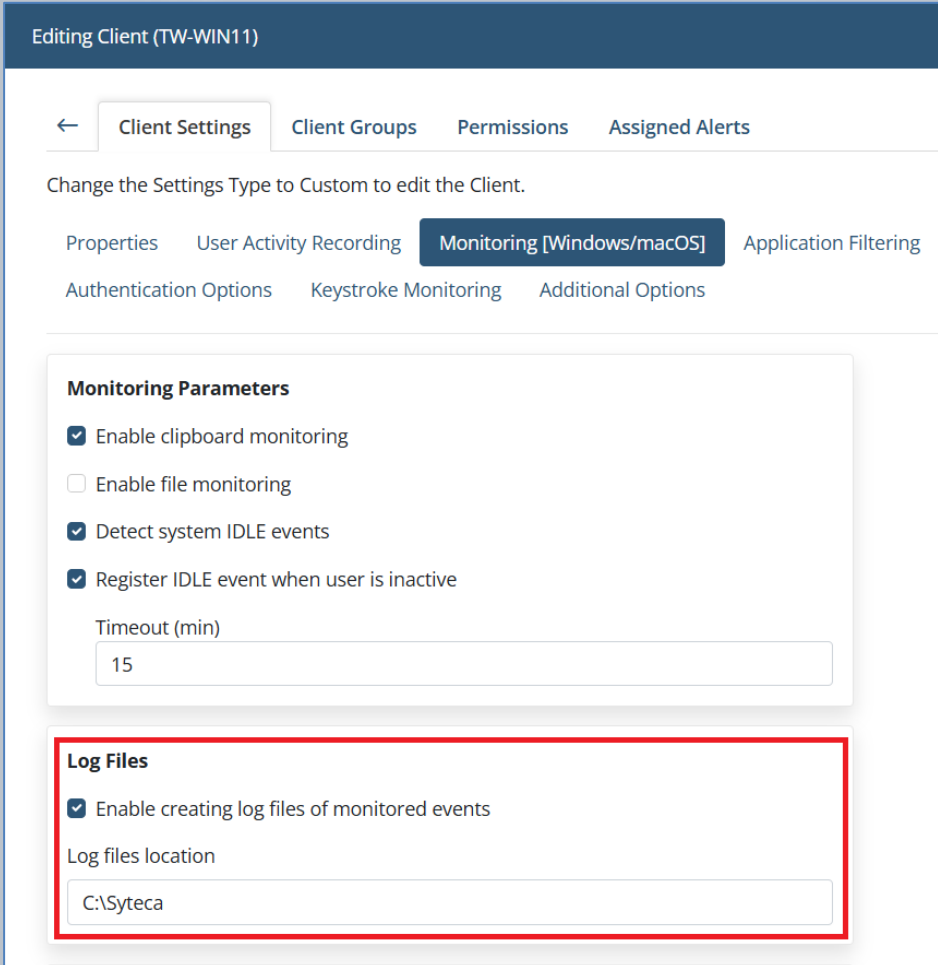
- SafeNet properties file location: C:\Program Files\SafeNet ProtectApp\ProtectApp\CAP\...
- PassPhraseSecure.exe location: C:\Program Files\SafeNet ProtectApp\PassPhraseSeci\...
- User name: admin
- Password: [masked]
- Key name (leave empty to generate a new key): DataCenter-234
- Deployment options: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

You can **disconnect all Clients** from the **database** to make them go offline, so as to **fix any issues** with the database, and perform database **cleanup and maintenance** without stopping the 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 top navigation bar includes the Syteca logo, a back arrow, 'System Health', and user information 'localhost Built-in default tenant'. A left sidebar lists navigation options: Dashboards, Reports, Activity Monitoring, Password Management, Account Discovery, Access Requests, Clients, and Users. The main content area has tabs for 'System State', 'Offline Clients', and 'Tasks List'. A dropdown menu is open under 'System State', with 'Isolate Database from Clients' highlighted in red. Below the menu, three performance metrics are shown: a disk usage gauge at 10.40% (100.56 GB used, 866.44 GB free), a 'Memory Usage' bar chart (2 minute(s)), and a 'CPU Usage' line chart (2 minute(s)).

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

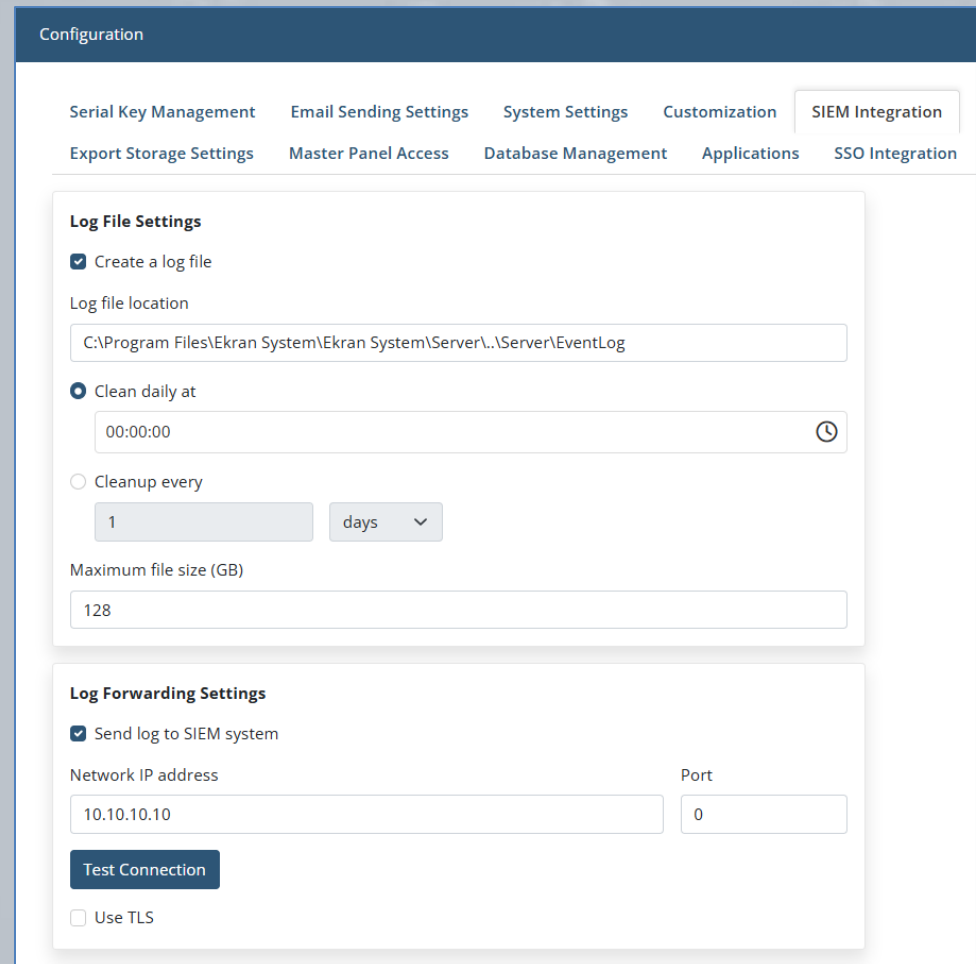
Log Files

- 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 in the Syteca interface, specifically the 'SIEM Integration' tab. The page is organized into two main sections: 'Log File Settings' and 'Log Forwarding Settings'.

Log File Settings:

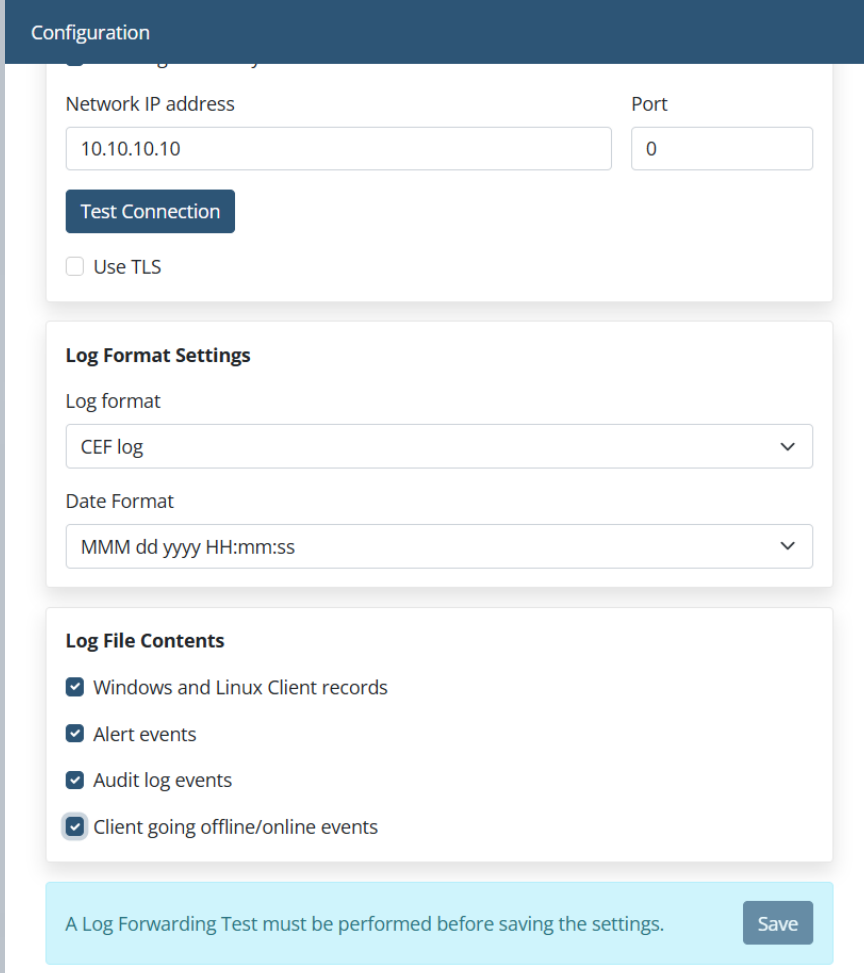
- Create a log file
- Log file location:
- Clean daily at: (clock icon)
- Cleanup every: days
- Maximum file size (GB):

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 screenshot shows a configuration page titled "Configuration" with the following sections:

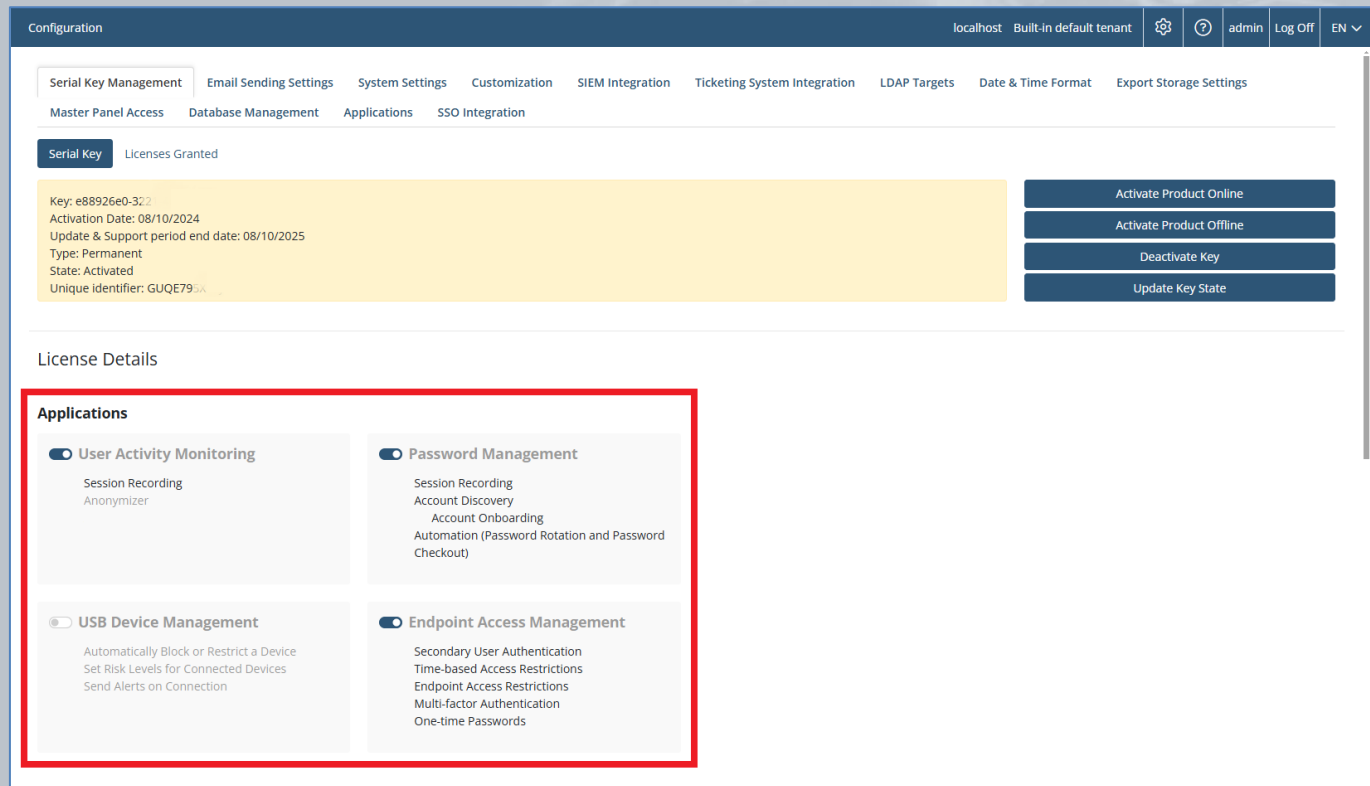
- Network IP address**: Input field containing "10.10.10.10".
- Port**: Input field containing "0".
- Test Connection**: A blue button.
- Use TLS
- Log Format Settings**:
 - Log format**: Dropdown menu set to "CEF log".
 - Date Format**: Dropdown menu set to "MMM dd yyyy HH:mm:ss".
- Log File Contents**:
 - Windows and Linux Client records
 - Alert events
 - Audit log events
 - Client going offline/online events

A light blue banner at the bottom contains the message: "A Log Forwarding Test must be performed before saving the settings." and a "Save" button.

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).

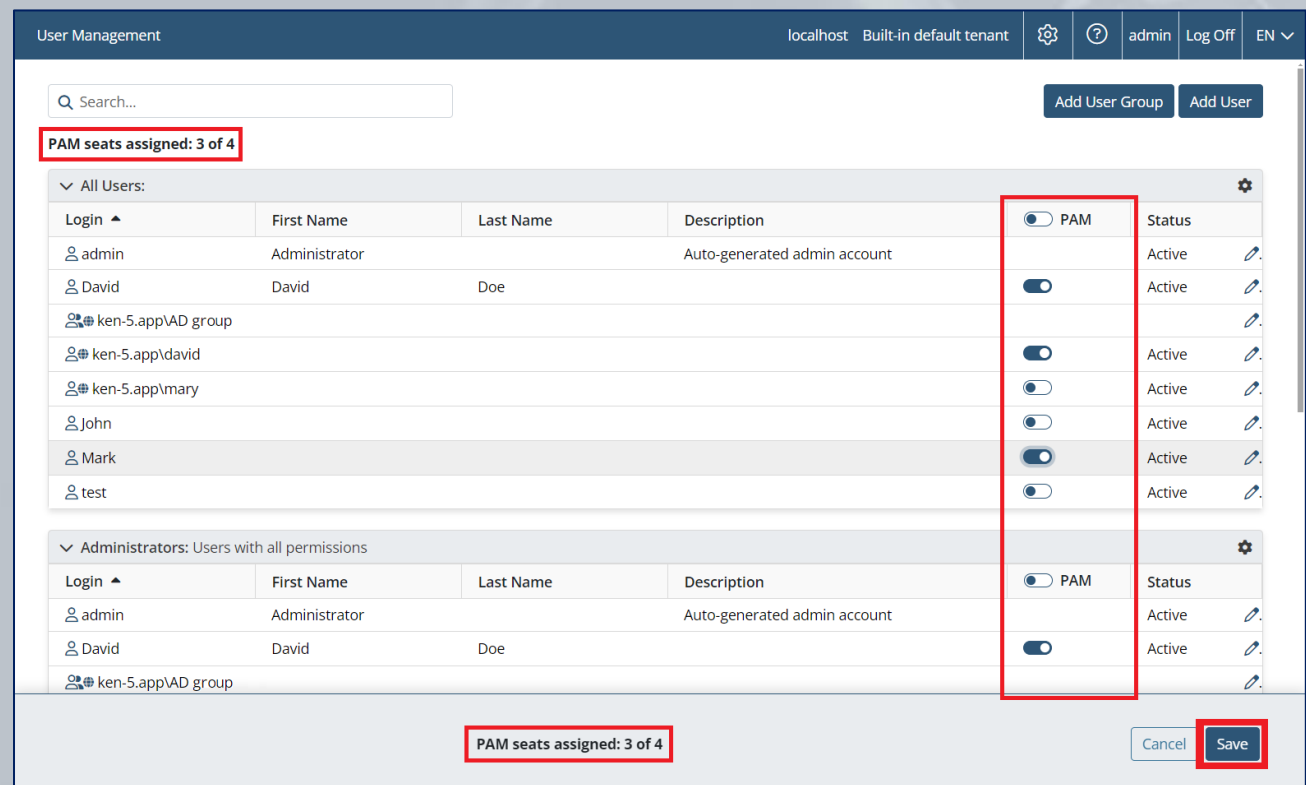


The screenshot displays the Syteca Configuration interface. The top navigation bar includes 'localhost Built-in default tenant', user 'admin', and 'Log Off'. The main menu contains various settings categories, with 'Serial Key Management' selected. The 'Serial Key' section shows a license key: 'Key: e88926e0-322', 'Activation Date: 08/10/2024', 'Update & Support period end date: 08/10/2025', 'Type: Permanent', 'State: Activated', and 'Unique Identifier: GUQE79'. Action buttons include 'Activate Product Online', 'Activate Product Offline', 'Deactivate Key', and 'Update Key State'. The 'License Details' section is titled 'Applications' and lists four enabled 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 shows the 'User Management' interface. At the top, there 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. Below this, there are two tables of users. The first table, 'All Users', lists users with columns for Login, First Name, Last Name, Description, PAM status (toggle), and Status. The second table, 'Administrators: Users with all permissions', lists administrators with similar columns. A red box highlights the PAM status toggle for the 'David' user in both tables. 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 type="checkbox"/>	Active
David	David	Doe		<input checked="" 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

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

- **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**, get access to the **full set of features** required, and have a **greater number of licensed PAM users and endpoints**, the product needs to be **licensed** by **activating a purchased serial key** on the computer with the Syteca Application Server 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**.

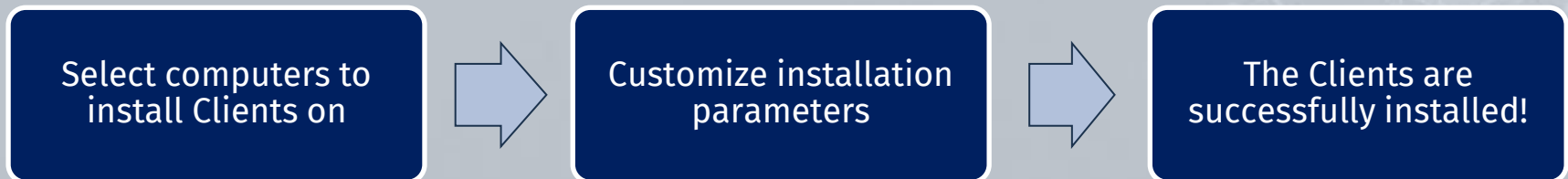
- **Manual** reassignment: Can be done **at any time**, in just a **couple of clicks**.
- **Automatic** reassignment:
 - **Delete offline Clients without sessions**: This option allows the licenses of Clients, whenever they do not have sessions stored, to be returned to the pool of available endpoint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

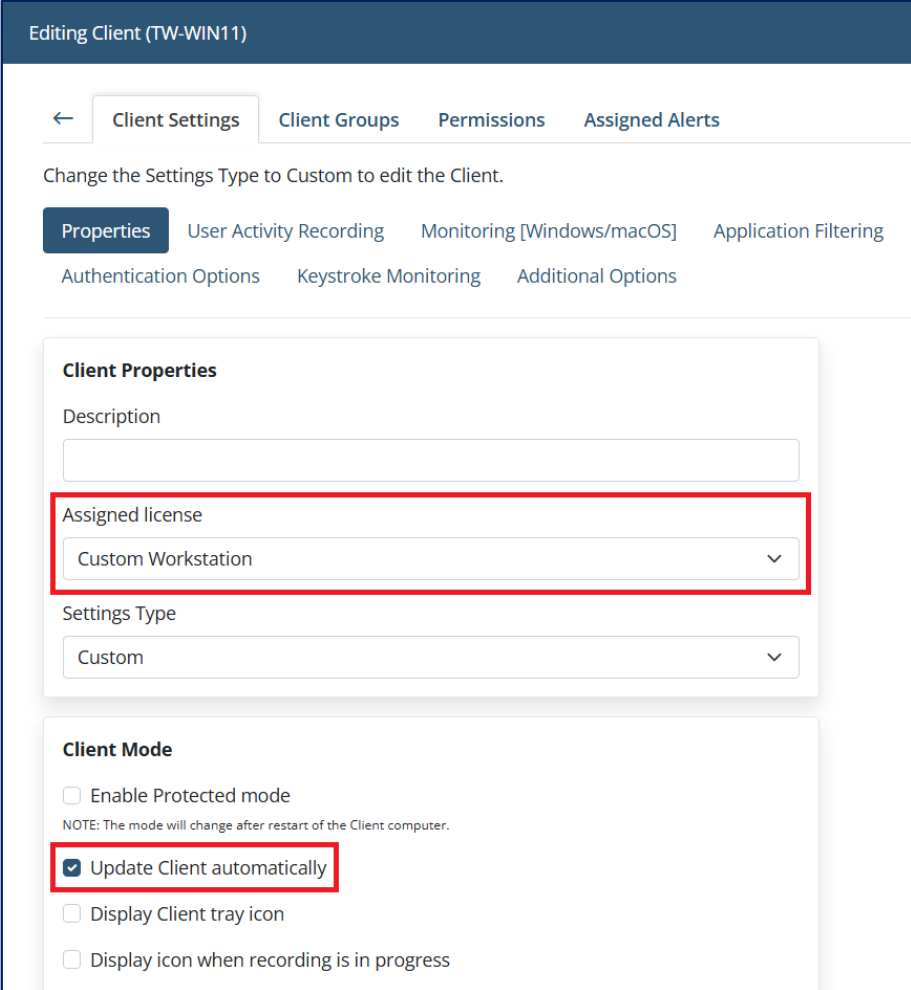
Computer ↕	Workgroup / Domain ↕	IP ↕	Description ↕	Previous Installation Failure ↕	Remove All
lee.d.local	d.local	10.10.10.10			

Read the installation prerequisites

Install Install using existing .ini file

After the 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.



The screenshot shows the 'Editing Client (TW-WIN11)' interface. At the top, there are navigation 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.' There are two rows of sub-tabs: the first row contains 'Properties' (selected), 'User Activity Recording', 'Monitoring [Windows/macOS]', and 'Application Filtering'; the second row contains 'Authentication Options', 'Keystroke Monitoring', and 'Additional Options'. The main content area is divided into two sections: 'Client Properties' and 'Client Mode'. In the 'Client Properties' section, the 'Assigned license' dropdown menu is highlighted with a red box and set to 'Custom Workstation'. Below it, the 'Settings Type' dropdown is set to 'Custom'. In the 'Client Mode' section, the 'Update Client automatically' checkbox is checked and highlighted with a red box. Other options include 'Enable Protected mode', 'Display Client tray icon', and 'Display icon when recording is in progress'. A note below the 'Enable Protected mode' checkbox reads: 'NOTE: The mode will change after restart of the Client computer.'

Monitoring Parameters

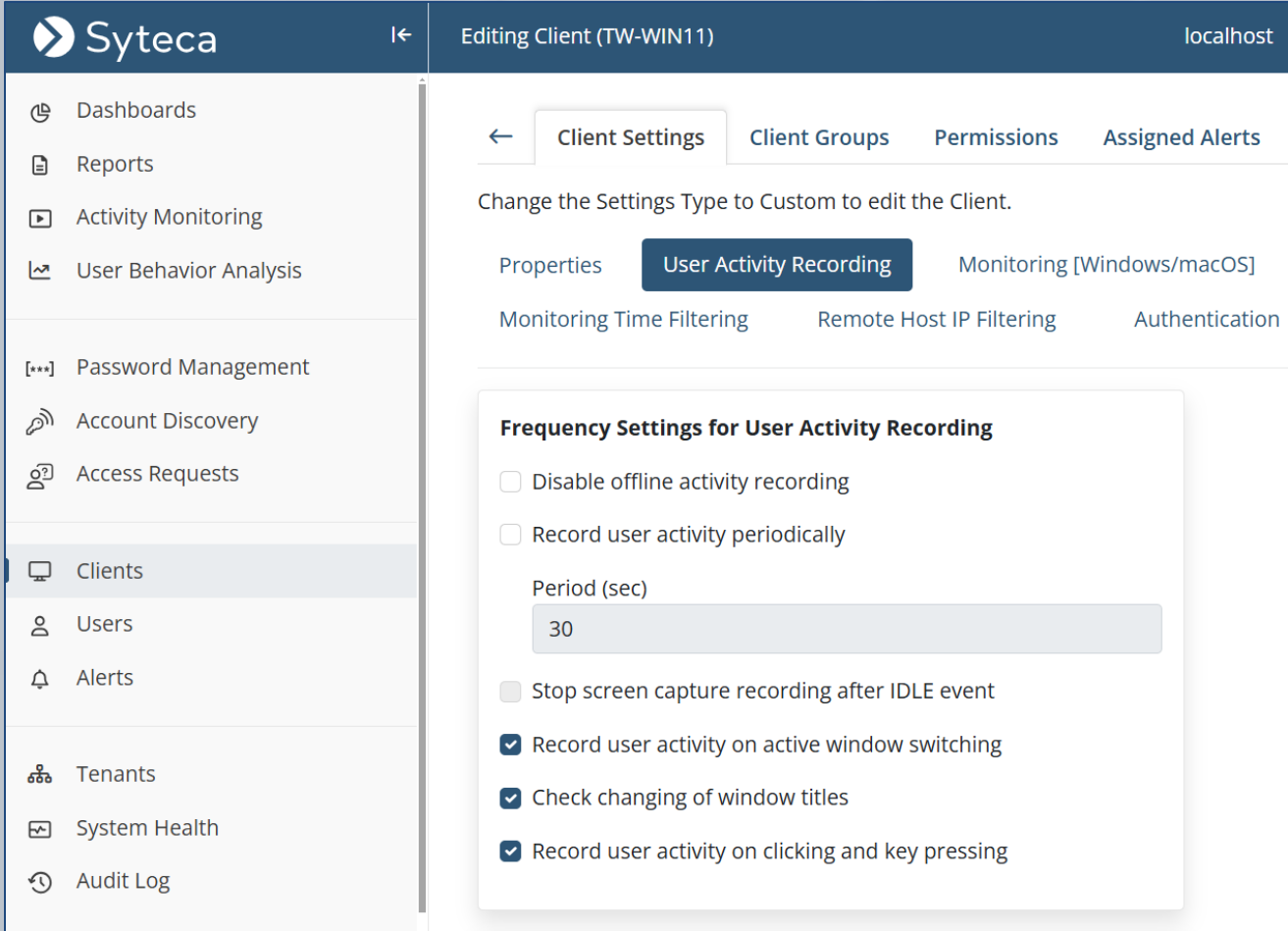
The **screen captures** that the Client sends are stored in the form of deltas (i.e. the differences between a newer recorded screen capture and an older one) to minimize the storage space used.

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

- The names of **applications** launched.
- The titles of **active windows**.
- The **URLs** entered.
- Text entered via the user's keyboard (i.e. **keystrokes**).
- **Clipboard** text data (copied/cut or pasted).
- **Commands** executed using **Linux** (from both user input & scripts run) and **responses** output.
- **USB devices** plugged-in.
- File monitoring operations (e.g. **file upload**).
- **Alerts** triggered (on various user activities).

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**.

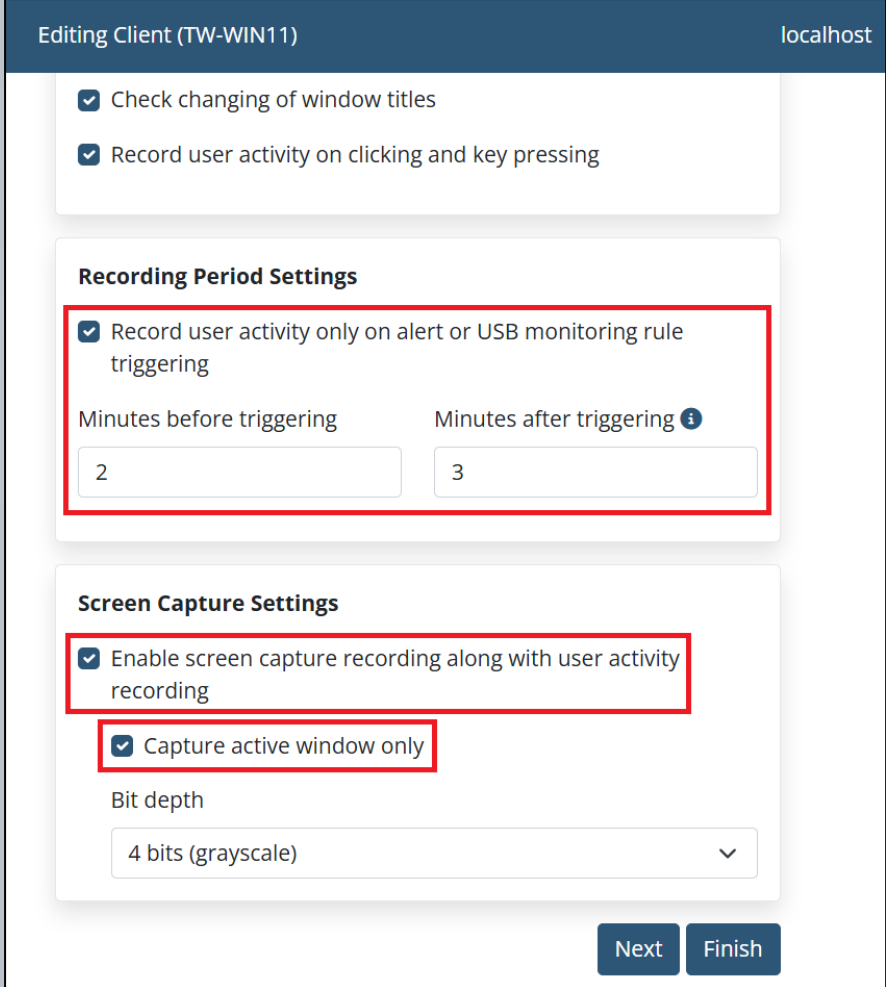


The screenshot displays the Syteca web interface for editing a client named 'TW-WIN11'. The left sidebar contains a navigation menu with options: Dashboards, Reports, Activity Monitoring, User Behavior Analysis, Password Management, Account Discovery, Access Requests, Clients (highlighted), Users, Alerts, Tenants, System Health, and Audit Log. The main content area is titled 'Editing Client (TW-WIN11)' and includes tabs for Client Settings, Client Groups, Permissions, and Assigned Alerts. Below the tabs, there is a message: 'Change the Settings Type to Custom to edit the Client.' The 'User Activity Recording' tab is active, showing a 'Properties' section with a 'Monitoring [Windows/macOS]' dropdown. Below this, there are settings for 'Monitoring Time Filtering', 'Remote Host IP Filtering', and 'Authentication'. A modal window titled 'Frequency Settings for User Activity Recording' is open, containing the following options:

- 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** (Windows Clients only).
- 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

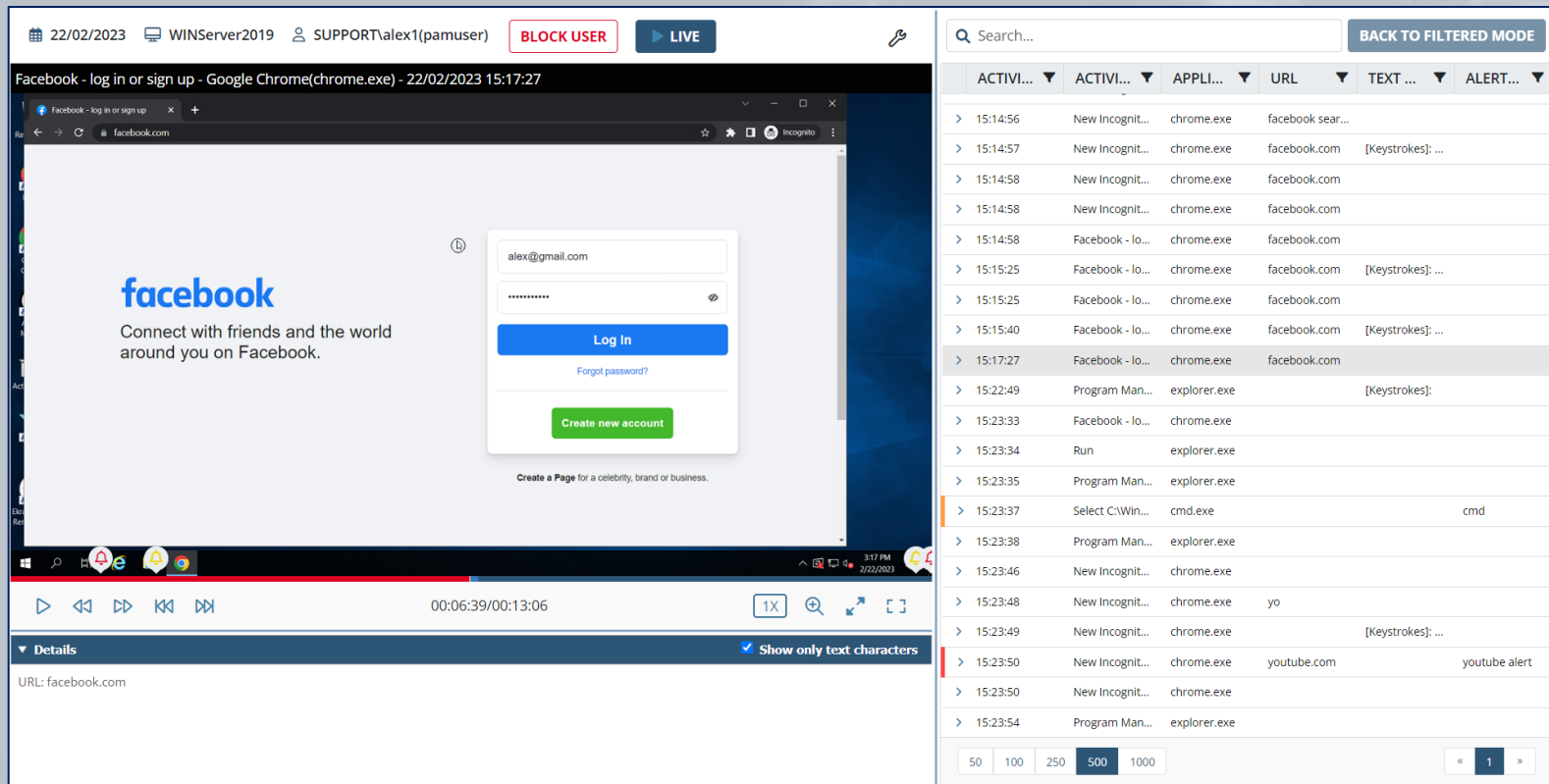
Screen Capture Settings

- 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.

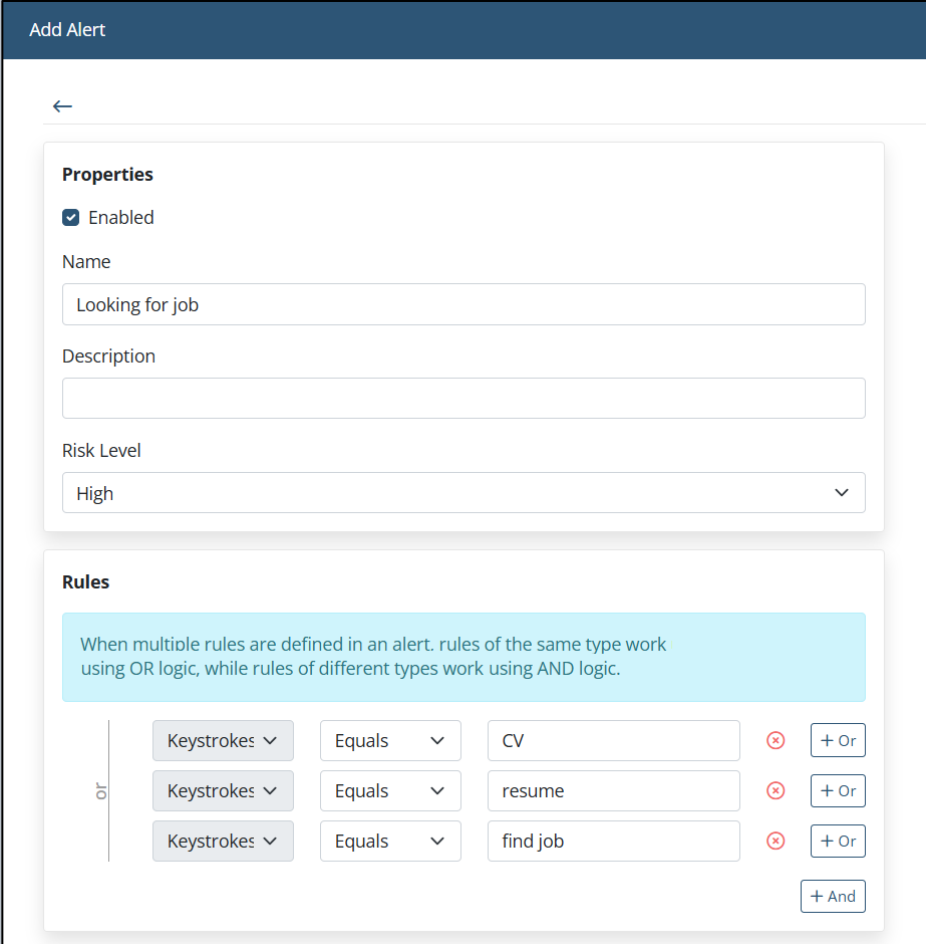


The screenshot displays the Syteca Client interface. On the left, a browser window shows the Facebook login page with the email 'alex@gmail.com' entered. The top of the interface includes a status bar with the date '22/02/2023', system name 'WINServer2019', user 'SUPPORT\alex1(pamuser)', and buttons for 'BLOCK USER' and 'LIVE'. Below the browser window is a 'Details' section showing the URL 'facebook.com'. On the right, a table lists monitored activities with columns for time, application, URL, and alert type.

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.



Add Alert

←

Properties

Enabled

Name
Looking for job

Description

Risk Level
High

Rules

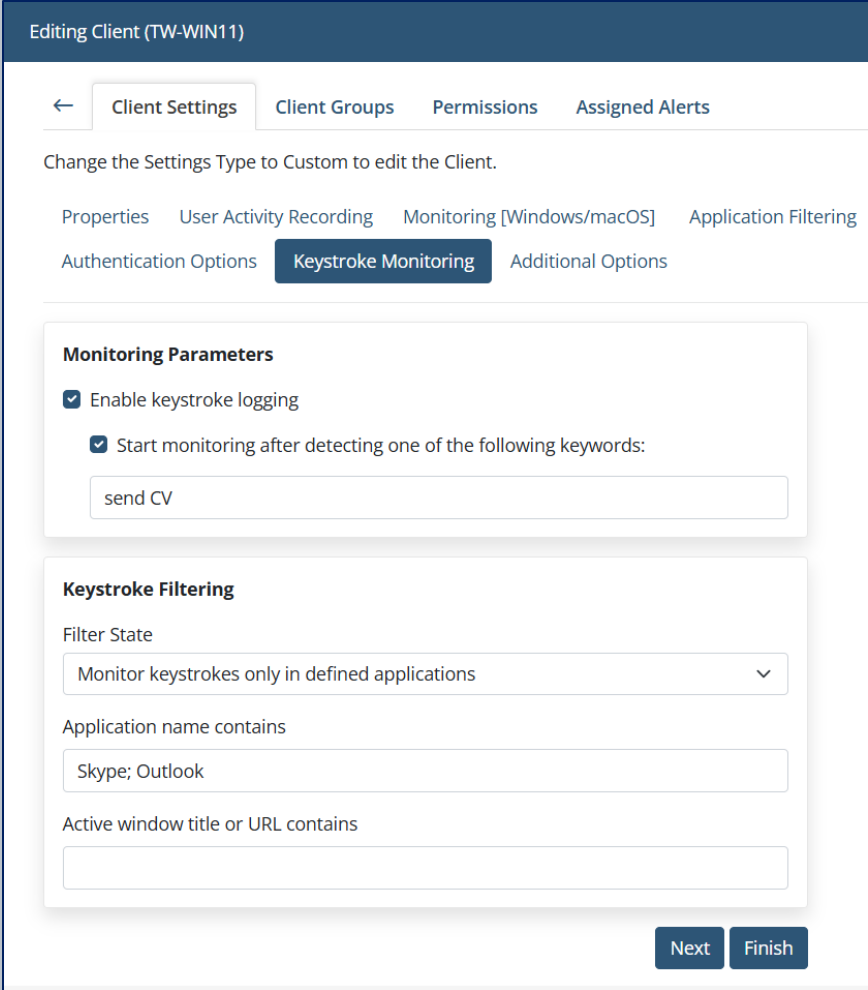
When multiple rules are defined in an alert, rules of the same type work using OR logic, while rules of different types work using AND logic.

or

Keystrokes	Equals	CV	⊗	+ Or
Keystrokes	Equals	resume	⊗	+ Or
Keystrokes	Equals	find job	⊗	+ Or

+ And

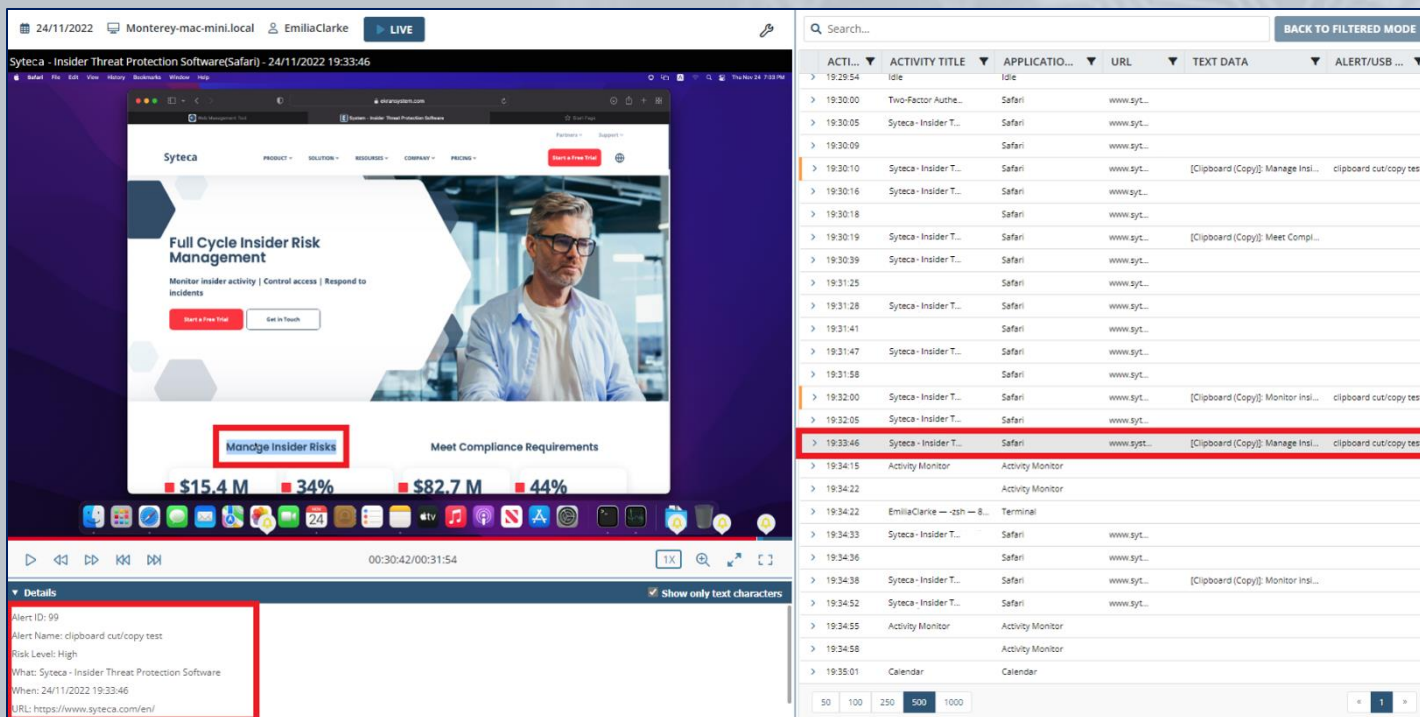
You can configure Syteca Clients to start monitoring and recording screen captures only after they **detect** defined **keywords** entered by the user in **specified applications**.



The screenshot shows the 'Editing Client (TW-WIN11)' configuration page. The 'Client Settings' tab is active, and the 'Keystroke Monitoring' sub-tab is selected. The interface includes a breadcrumb trail: Client Settings > Client Groups > Permissions > Assigned Alerts. A message states: 'Change the Settings Type to Custom to edit the Client.' Below this are several tabs: Properties, User Activity Recording, Monitoring [Windows/macOS], Application Filtering, Authentication Options, Keystroke Monitoring (selected), and Additional Options. The 'Monitoring Parameters' section contains two checked checkboxes: 'Enable keystroke logging' and 'Start monitoring after detecting one of the following keywords:'. A text input field below contains 'send CV'. The 'Keystroke Filtering' section includes a 'Filter State' dropdown menu set to 'Monitor keystrokes only in defined applications', an 'Application name contains' text input field with 'Skype; Outlook', and an 'Active window title or URL contains' text input field. At the bottom right 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 a live monitoring dashboard with a search bar, a table of activity logs, and a details panel for a selected alert.

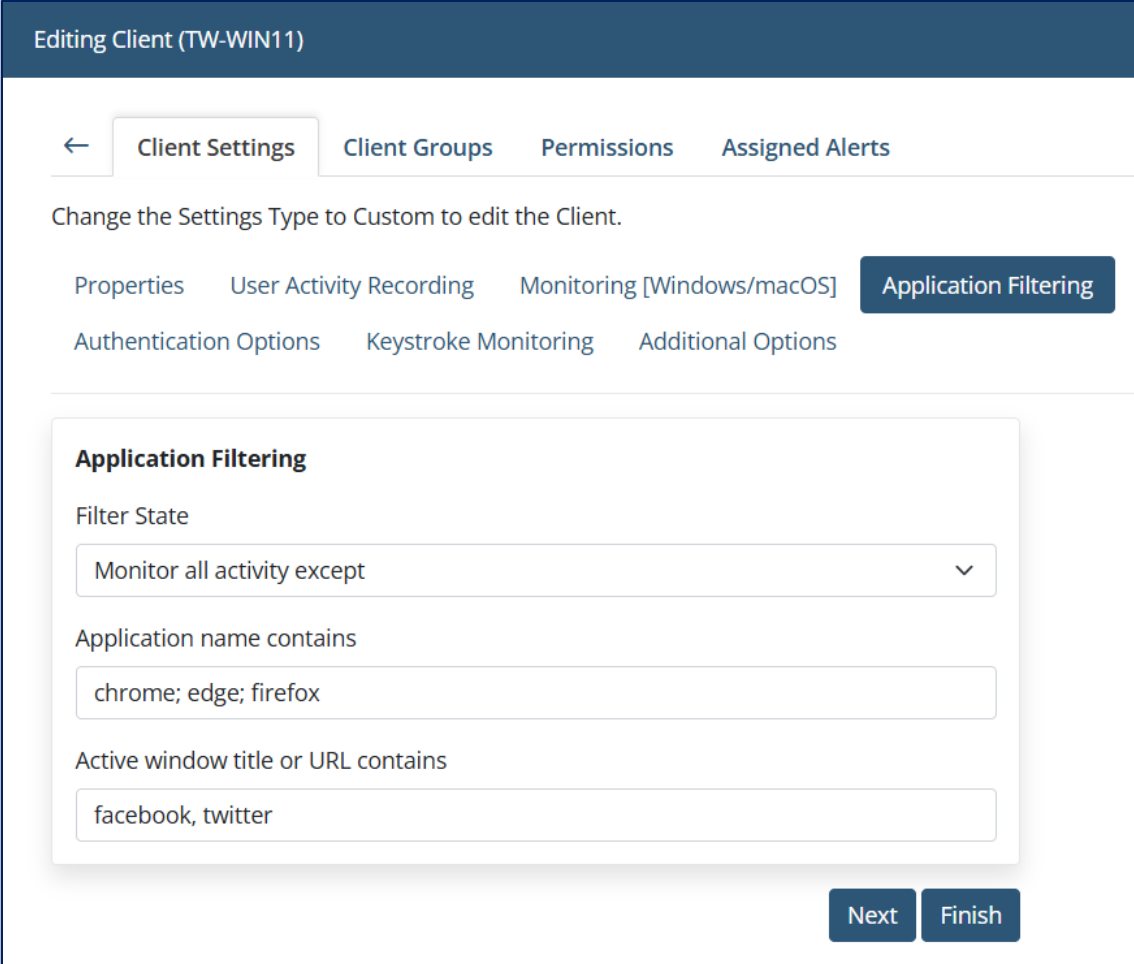
Activity Log Table:

ACTI...	ACTIVITY TITLE	APPLICATIO...	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	Syteca - Insider T...	Safari	www.syt...		
19:30:10	Syteca - Insider T...	Safari	www.syt...	[Clipboard (Copy): Manage Insi...	clipboard cut/copy test
19:30:16	Syteca - Insider T...	Safari	www.syt...		
19:30:18	Syteca - Insider T...	Safari	www.syt...		
19:30:19	Syteca - Insider T...	Safari	www.syt...	[Clipboard (Copy): Meet Compl...	
19:30:39	Syteca - Insider T...	Safari	www.syt...		
19:31:25	Syteca - Insider T...	Safari	www.syt...		
19:31:28	Syteca - Insider T...	Safari	www.syt...		
19:31:41	Syteca - Insider T...	Safari	www.syt...		
19:31:47	Syteca - Insider T...	Safari	www.syt...		
19:31:58	Syteca - Insider T...	Safari	www.syt...		
19:32:00	Syteca - Insider T...	Safari	www.syt...	[Clipboard (Copy): Monitor Insi...	clipboard cut/copy test
19:32:05	Syteca - Insider T...	Safari	www.syt...		
19:33:46	Syteca - Insider T...	Safari	www.syt...	[Clipboard (Copy): Manage Insi...	clipboard cut/copy test
19:34:15	Activity Monitor	Activity Monitor			
19:34:22	Activity Monitor	Activity Monitor			
19:34:22	EmiliaClarke -- zsh -- 8...	Terminal			
19:34:33	Syteca - Insider T...	Safari	www.syt...		
19:34:36	Syteca - Insider T...	Safari	www.syt...		
19:34:38	Syteca - Insider T...	Safari	www.syt...	[Clipboard (Copy): Monitor Insi...	
19:34:52	Syteca - Insider T...	Safari	www.syt...		
19:34:55	Activity Monitor	Activity Monitor			
19:34:58	Activity Monitor	Activity Monitor			
19:35:01	Calendar	Calendar			

Alert Details Panel:

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

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-WIN1)

← 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

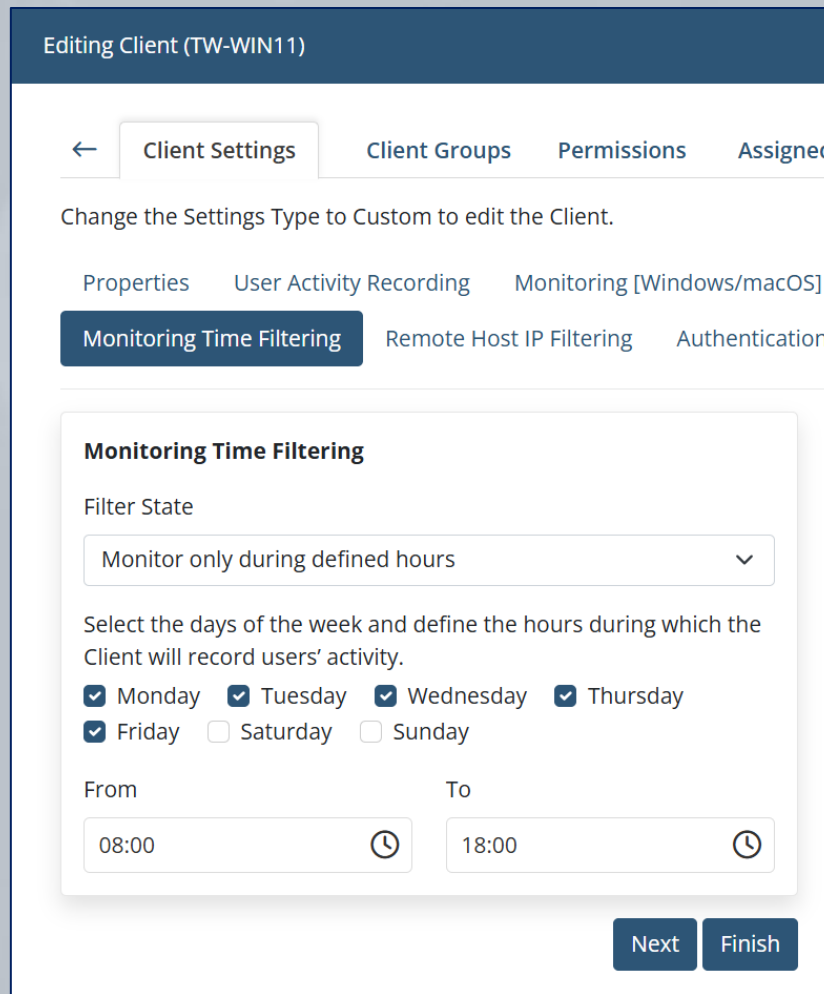
Active window title or URL contains

facebook, twitter

Next Finish

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

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



Editing Client (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

Monitoring Time Filtering

Filter State

Monitor only during defined hours

Select the days of the week and define the hours during which the Client will record users' activity.

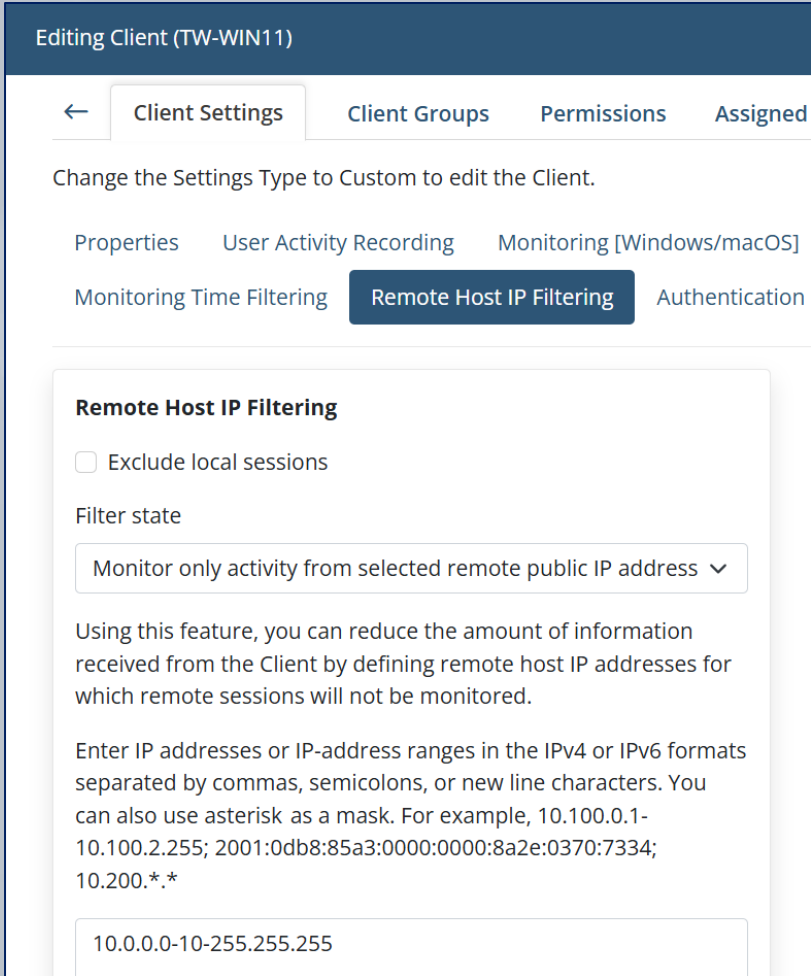
Monday Tuesday Wednesday Thursday
 Friday Saturday Sunday

From To

08:00 18:00

Next Finish

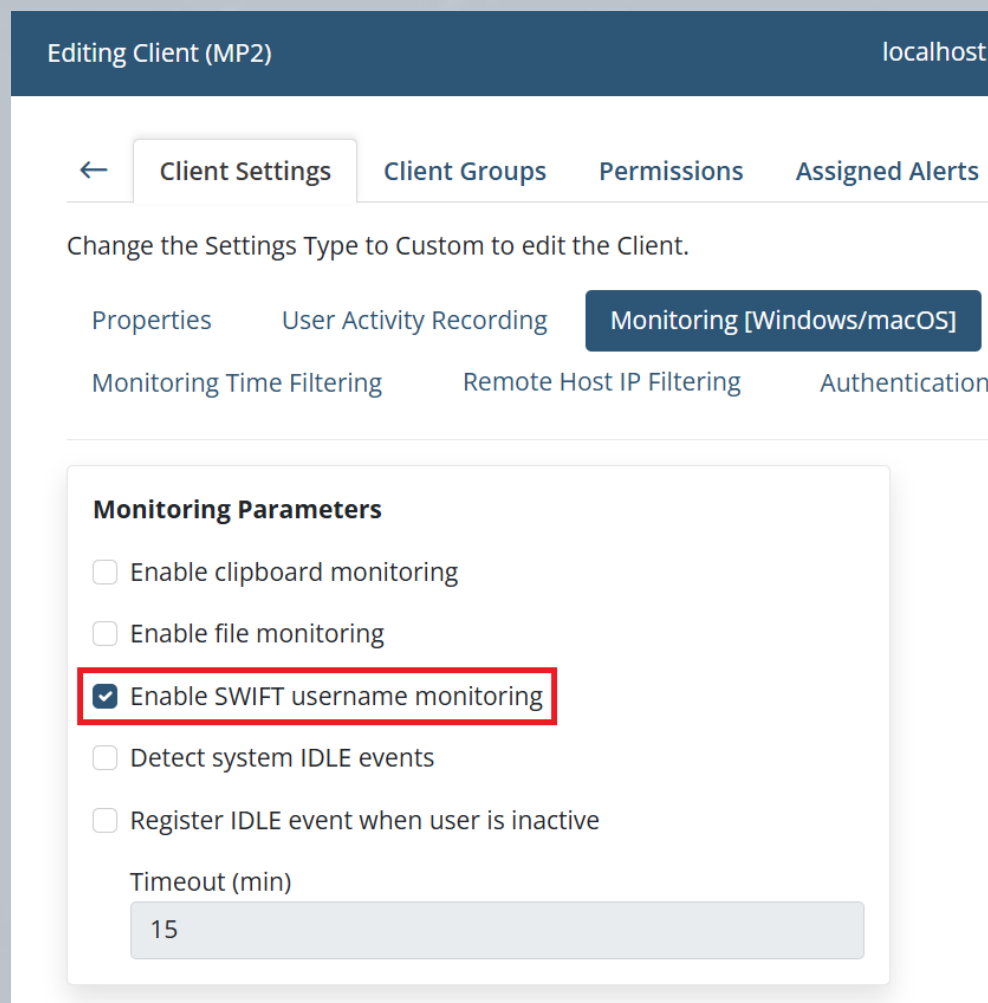
Additionally, you can **filter** sessions from **certain remote IP addresses**, or only monitor sessions from certain IP addresses.



The screenshot shows the 'Editing Client (TW-WIN11)' interface. At the top, there are tabs for 'Client Settings', 'Client Groups', 'Permissions', and 'Assigned'. Below the tabs, a message states: 'Change the Settings Type to Custom to edit the Client.' A row of settings tabs includes 'Properties', 'User Activity Recording', 'Monitoring [Windows/macOS]', 'Monitoring Time Filtering', 'Remote Host IP Filtering' (which is highlighted), and 'Authentication'. The 'Remote Host IP Filtering' section contains the following elements:

- An unchecked checkbox labeled 'Exclude local sessions'.
- A 'Filter state' dropdown menu currently set to 'Monitor only activity from selected remote public IP address'.
- Explanatory text: '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.'
- Instructions: '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.*.*'
- A text input field containing the IP range '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.



Editing Client (MP2) 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

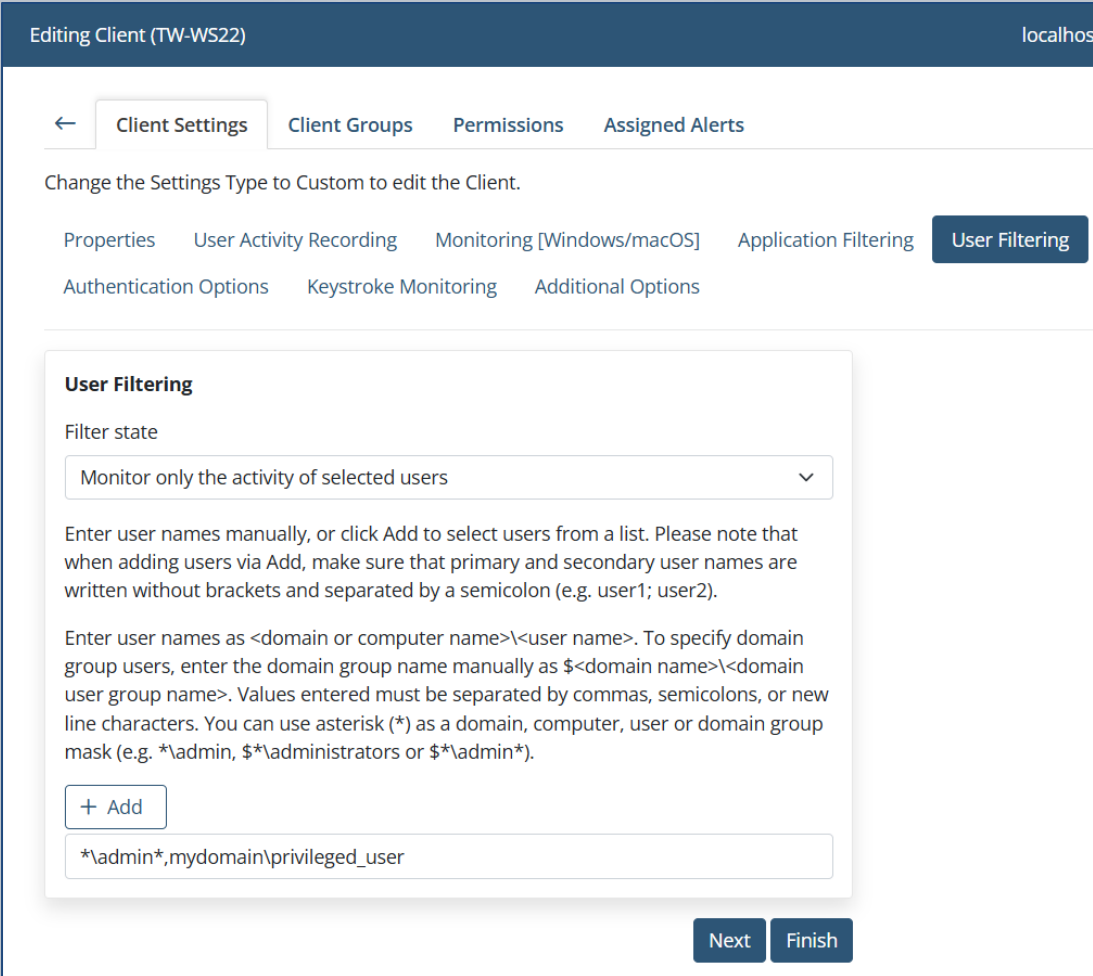
Monitoring Parameters

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

Timeout (min)

15

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



The screenshot shows the 'Editing Client (TW-WS22)' interface on a 'localhost' environment. The main navigation bar includes 'Client Settings', 'Client Groups', 'Permissions', and 'Assigned Alerts'. Below this, a breadcrumb trail shows 'Properties', 'User Activity Recording', 'Monitoring [Windows/macOS]', 'Application Filtering', and 'User Filtering' (which is highlighted). A secondary row of options includes 'Authentication Options', 'Keystroke Monitoring', and 'Additional Options'. The 'User Filtering' section is expanded, showing a 'Filter state' dropdown menu set to 'Monitor only the activity of selected users'. Below the dropdown, there is instructional text: '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*).' A '+ Add' button is present above a text input field containing '*\admin*,mydomain\privileged_user'. At the bottom right of the configuration area are 'Next' and 'Finish' buttons.

Syteca allows you to configure various **bandwidth usage reduction** parameters to manage the **traffic volume** from the Client to the Syteca Application Server.

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
Authentication Options Keystroke Monitoring **Additional Options**

Additional Options

Screen capture throttling (ms)

Batch registration timeout (ms)

Prevent loading hooks into the following applications

Reduce screen capture size by (%)

Screenshot compression level (1-9)

Agent memory limit (0-disabled)

Next Finish

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

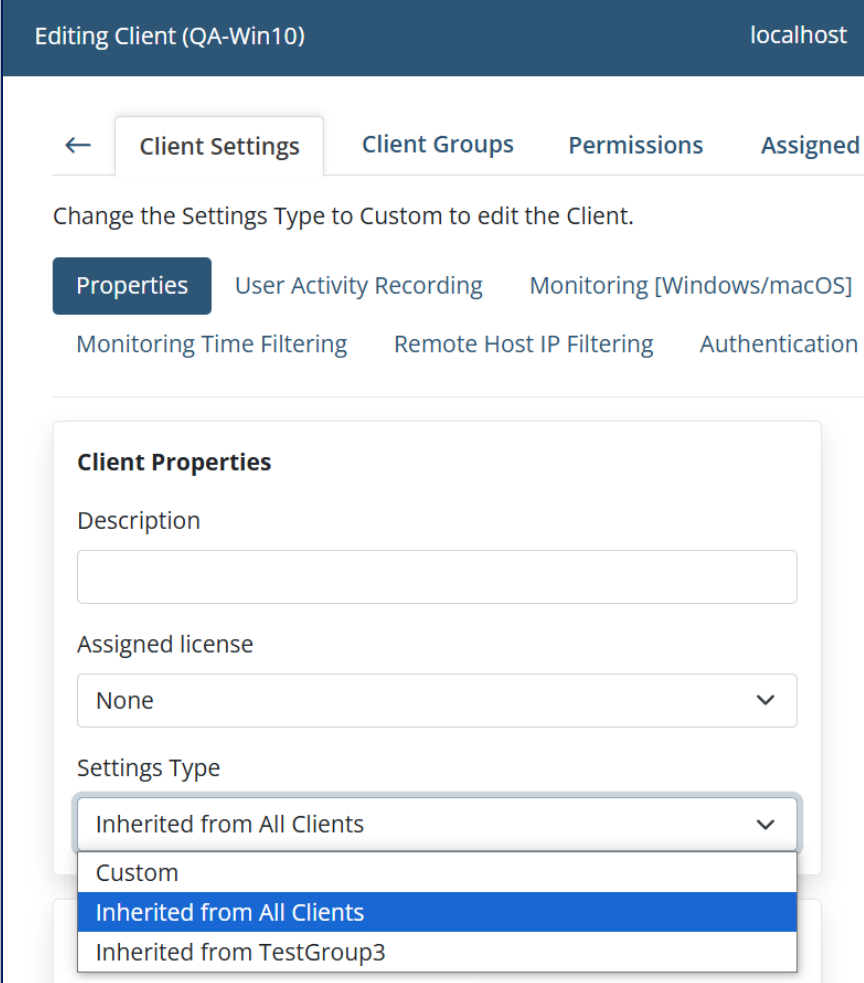
The screenshot displays a security monitoring interface. At the top, it shows the date and time (12/07/2023 18:54:28) and the user (WINSERVER2019\Administrator(pamuser)). A red box highlights the 'BLOCK USER' button and a 'LIVE' indicator. Below this, a browser window is shown with a Google search page. A red box highlights the 'Uploading...' progress bar in the browser's address bar. A red box highlights the 'david file upload' alert in the browser's address bar. Below the browser window, a 'Details' section is shown with a red box highlighting 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=EgZjaHJvWUqBwgAEEAYjwlyBwgAEEAYjwlyDQgBEC4YxwEY0QMgAQyBwgCEAAyAQyBw...

On the right side of the interface, there is a table of activity logs. The table has columns for 'A...', 'ACTIVITY ...', 'A...', 'URL', 'TEXT DATA', and 'ALERT/USB ...'. The table contains multiple rows of activity logs, with one row highlighted in red:

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 Faceb...	chrom...	facebook...		
> 18:54:...	Get back on Faceb...	chrom...	facebook...		
> 18:54:...	Facebook - log in ...	chrom...	facebook...		
> 18:54:...	facebook - Google...	chrom...	google.com		
> 18:54:...	Open	chrom...			
> 18:54:...	facebook - Google...	chrom...	google.com		
> 18:54:...	facebook - Google...	chrom...	google.com	File operation (Upload...	david file upload
> 18:54:...	facebook - Google...	chrom...	google.com		
> 18:54:...	Google Lens - Goo...	chrom...	lens.google...		
> 18:54:...	Google Lens - Goo...	chrom...	lens.google...		
> 18:54:...	facebook - Google...	chrom...	google.com		

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



Editing Client (QA-Win10) localhost

← 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

Client Properties

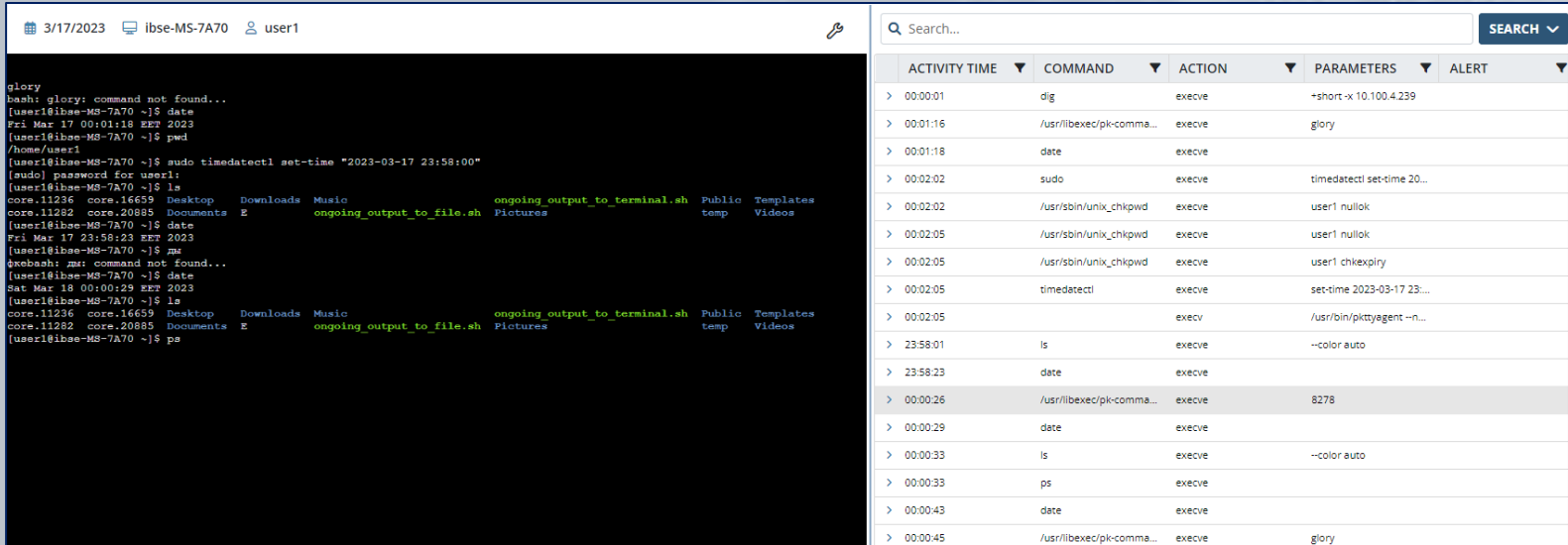
Description

Assigned license
None

Settings Type

- Inherited from All Clients
- Custom
- Inherited from All Clients
- 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.



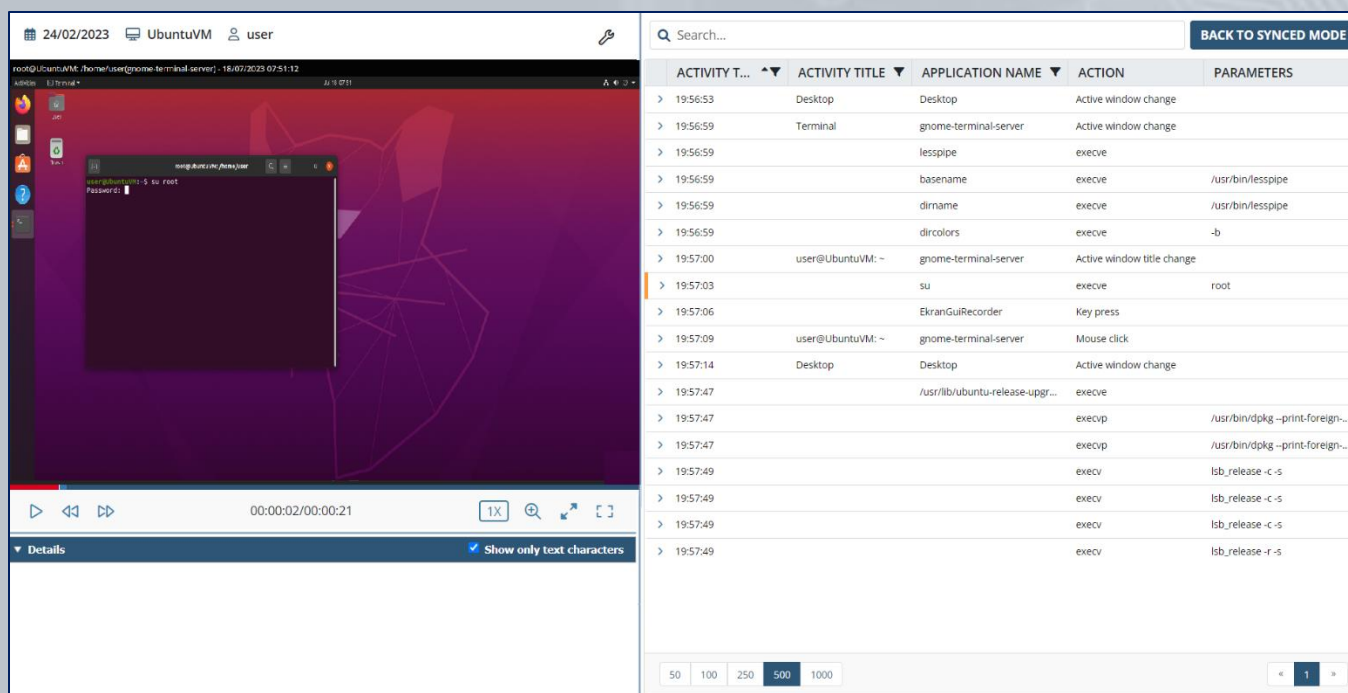
The screenshot displays the Syteca remote SSH session monitoring interface. On the left, a terminal window shows a user's session on a host named 'ibse-MS-7A70'. The user 'user1' enters the command 'glory', which is not found. They then run 'date', 'pwd', and 'sudo timedatectl set-time "2023-03-17 23:58:00"'. The terminal also shows the user's desktop environment with icons for Desktop, Downloads, Music, Pictures, Public, Templates, and Videos. On the right, an activity log table tracks the session's actions.

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	/usr/bin/pktyagent --n...	execv		
> 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:

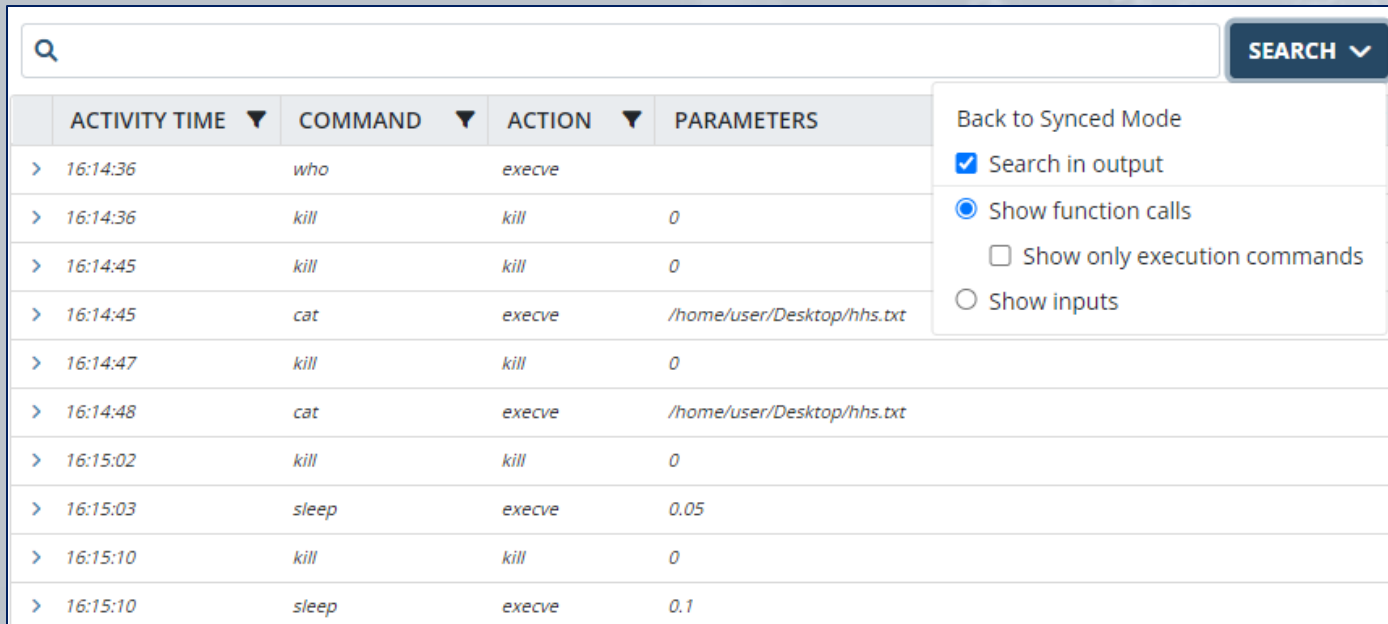
- Screen captures
- Activity times
- Activity titles
- Application names / Commands
- Actions / System function calls
- Parameters



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	execvp	/usr/bin/dpkg --print-foreign...
> 19:57:47		execvp	execvp	/usr/bin/dpkg --print-foreign...
> 19:57:49		execv	execv	lbb_release -c -s
> 19:57:49		execv	execv	lbb_release -c -s
> 19:57:49		execv	execv	lbb_release -c -s
> 19:57:49		execv	execv	lbb_release -r -s

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

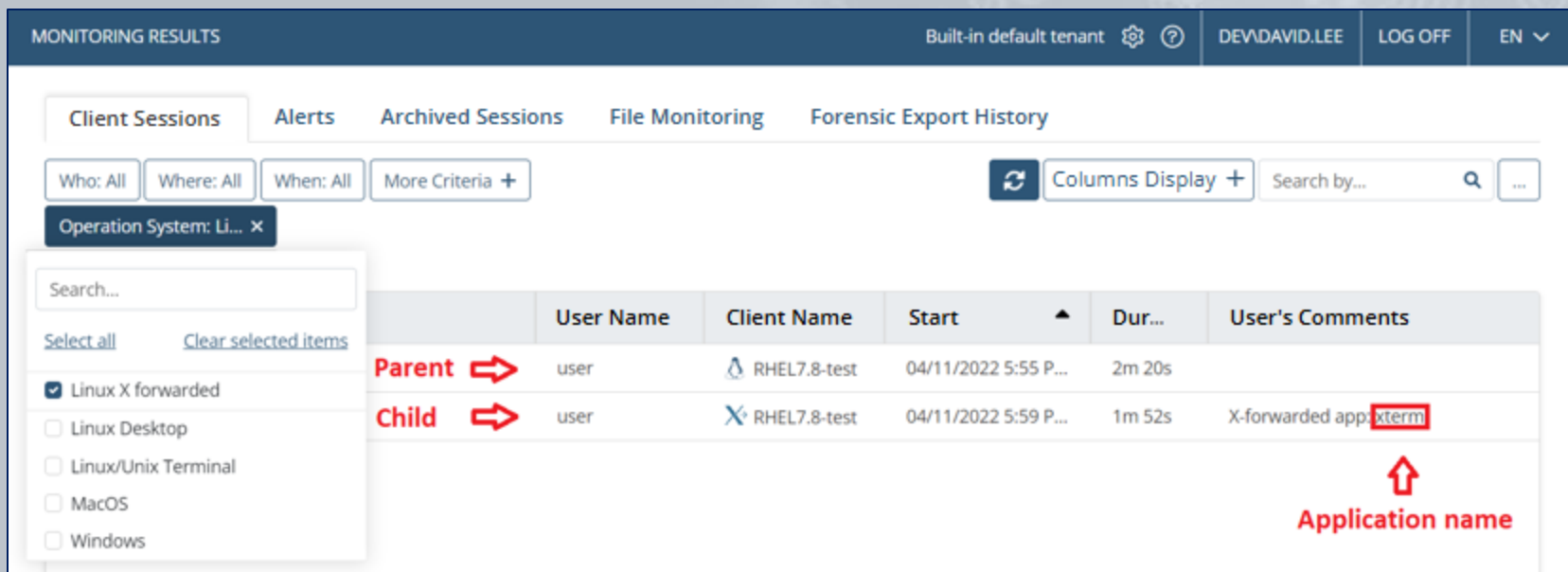
- **User actions** (keystrokes and commands & parameters **input**), and responses **output** from a terminal.
- System **function calls**.
- **Commands** executed in scripts run.



The screenshot shows a monitoring interface with a search bar at the top right containing a magnifying glass icon and a 'SEARCH' button with a dropdown arrow. Below the search bar is a table with the following columns: 'ACTIVITY TIME', 'COMMAND', 'ACTION', and 'PARAMETERS'. The table contains 10 rows of activity logs. A filter menu is open on the right side of the table, showing options: 'Back to Synced Mode', 'Search in output' (checked), 'Show function calls' (selected with a radio button), 'Show only execution commands' (unchecked), and 'Show inputs' (unchecked).

	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

- **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.



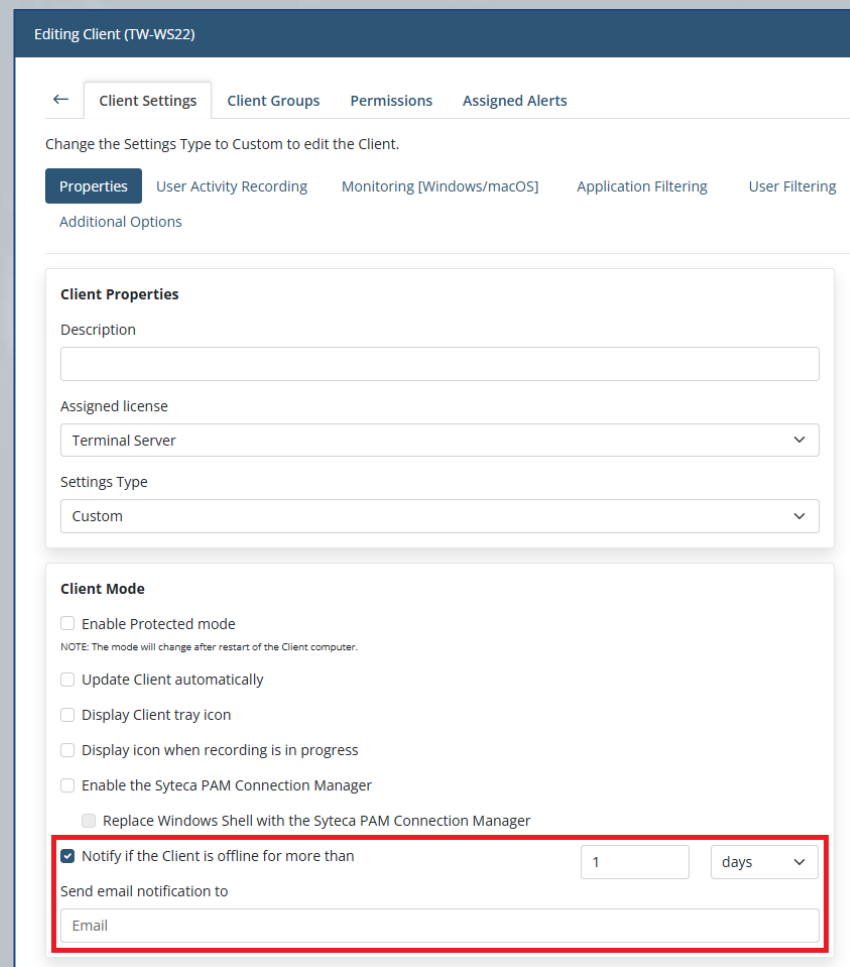
The screenshot displays the 'MONITORING RESULTS' page in the Syteca interface. The top navigation bar includes 'Built-in default tenant', 'DEVDAVID.LEE', 'LOG OFF', and 'EN'. Below the navigation, there are tabs for 'Client Sessions', 'Alerts', 'Archived Sessions', 'File Monitoring', and 'Forensic Export History'. The 'Client Sessions' tab is active, showing a search bar with filters for 'Who: All', 'Where: All', 'When: All', and 'More Criteria +'. A search bar is also present with a 'Columns Display +' button and a search icon. A filter for 'Operation System: Li...' is visible. The main content area shows a table of sessions with columns for 'User Name', 'Client Name', 'Start', 'Dur...', and 'User's Comments'. Two sessions are listed: a 'Parent' session and a 'Child' session. The 'Child' session is highlighted with a red box around the application name 'xterm' in the 'User's Comments' column. A red arrow points to the 'xterm' application name, with the text 'Application name' below it.

	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

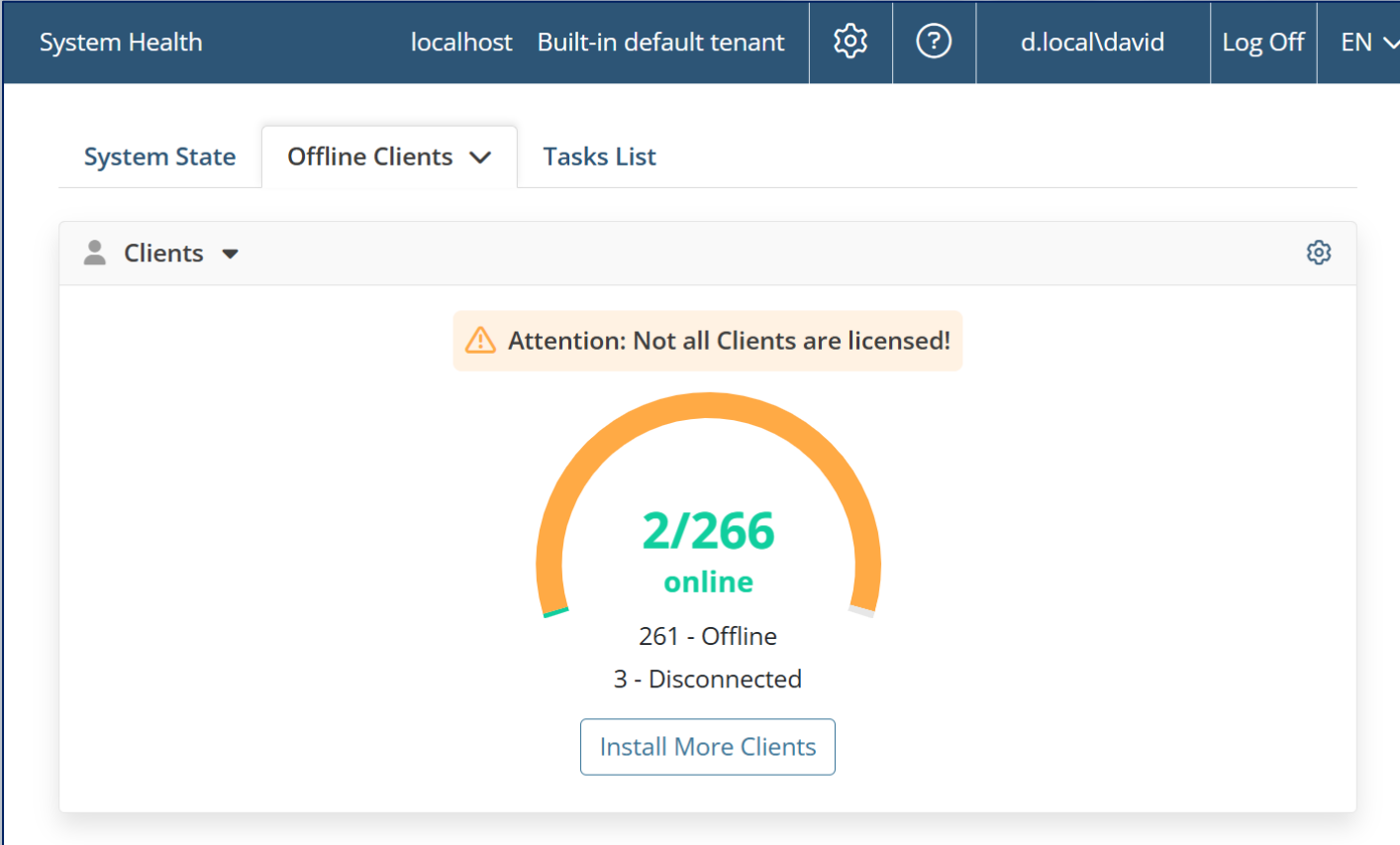
Replace Windows Shell with the Syteca PAM Connection Manager

Notify if the Client is offline for more than 1 days

Send email notification to

Email

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



The screenshot shows the Syteca management console interface. At the top, there is a navigation bar with "System Health", "localhost Built-in default tenant", a settings icon, a help icon, the user "d.local\david", "Log Off", and "EN". Below this, there are tabs for "System State", "Offline Clients" (selected), and "Tasks List". The main content area is titled "Clients" and features a warning message: "Attention: Not all Clients are licensed!". A large orange arc indicates the client status, with "2/266 online" in green text. Below this, it shows "261 - Offline" and "3 - Disconnected". A button labeled "Install More Clients" is positioned at the bottom of the client status summary.

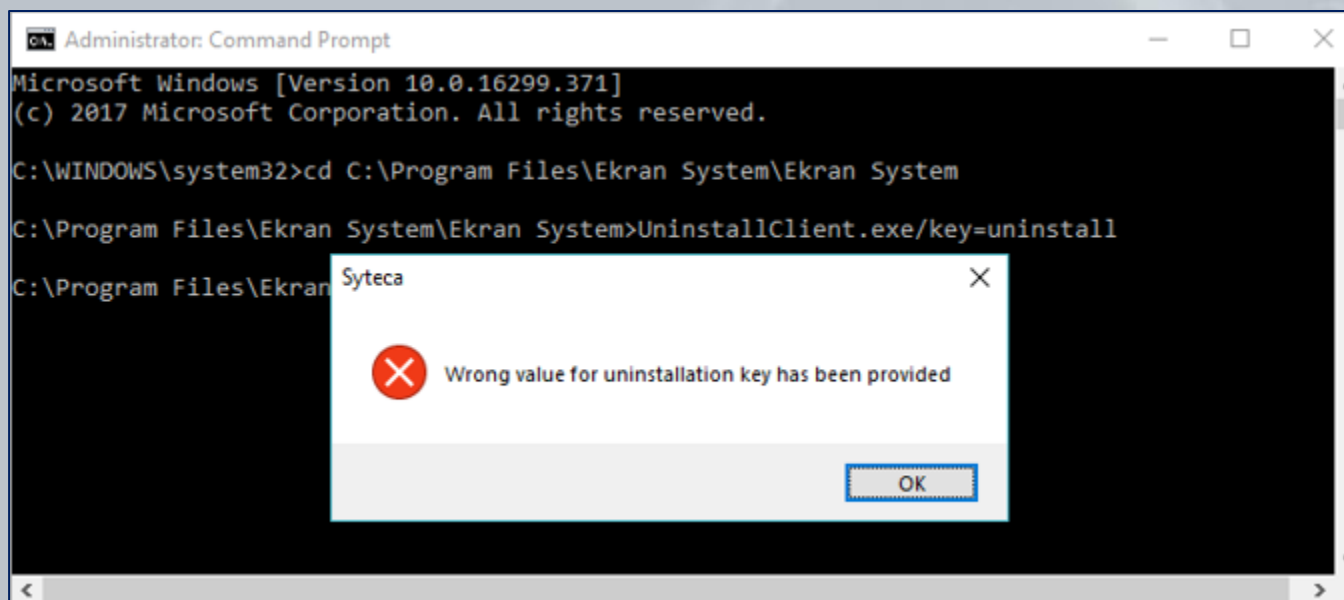
Client Protection

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

The use of Protected mode has the following **advantages**:

- Prevention of Client **uninstallation**.
- Prevention of **stopping** Client **processes**.
- Prevention of **editing** Client **system files and logs**.
- Prevention of **editing** Client **settings** in the **registry** of the Client computer.
- Prevention of **modification, removal, and renaming** of Client **files**.

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

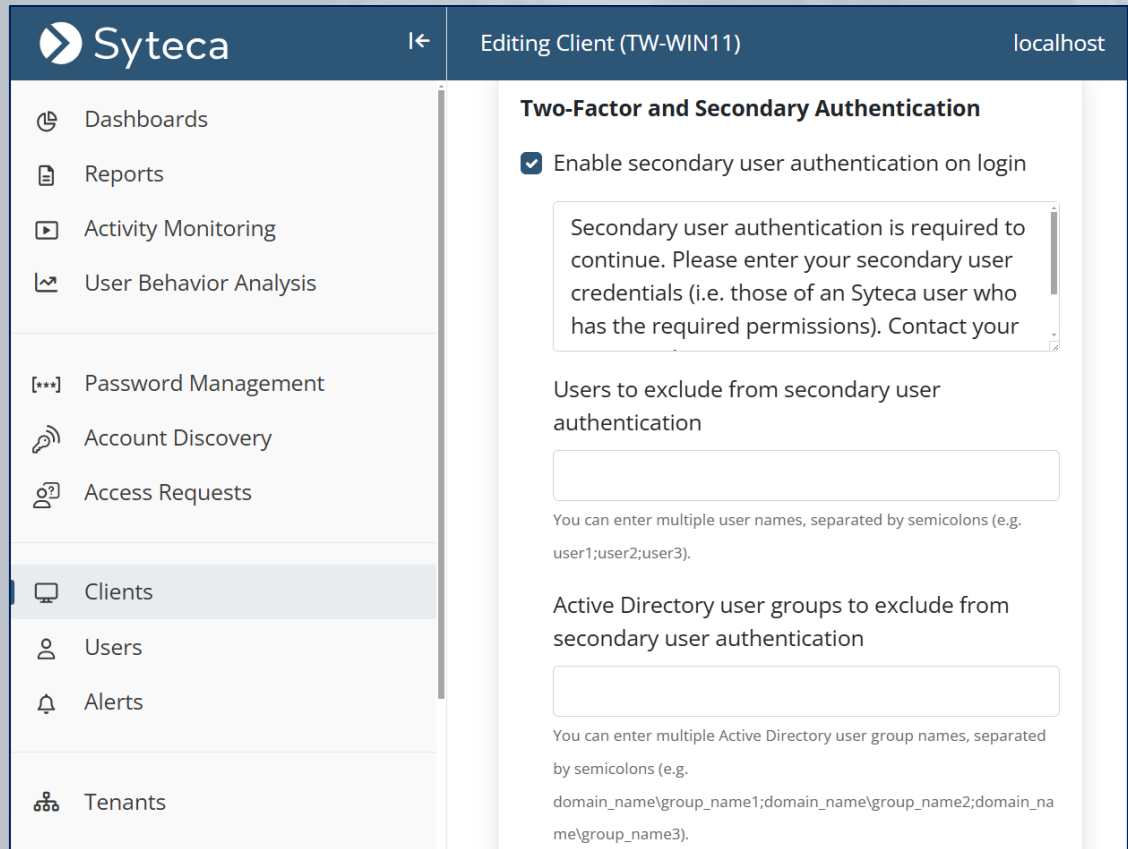


Only the **Syteca administrator** knows the **Uninstallation key** defined prior to Client installation, and which is required for local removal.

Secondary User Authentication

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

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



The screenshot shows the Syteca web interface. The left sidebar contains a navigation menu with the following items: Dashboards, Reports, Activity Monitoring, User Behavior Analysis, Password Management, Account Discovery, Access Requests, Clients (highlighted), Users, Alerts, and Tenants. The main content area is titled "Editing Client (TW-WIN11)" and shows the configuration for "Two-Factor and Secondary Authentication". The "Enable secondary user authentication on login" checkbox is checked. Below this, a text box explains that secondary user authentication is required to continue and provides instructions on how to enter credentials. Further down, there are two text input fields for "Users to exclude from secondary user authentication" and "Active Directory user groups to exclude from secondary user authentication". Both fields have placeholder text explaining the format for multiple entries, separated by semicolons.

Secondary User Authentication (Windows)



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

The image shows a secondary authentication dialog box for Syteca. At the top left is the Syteca logo. Below it, a horizontal line separates the header from the main text. 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 text 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 of the dialog box are two buttons: "OK" and "Cancel".

One-Time Passwords (Windows Clients)



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

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

A screenshot of a Windows-style dialog box titled "Syteca" with the subtitle "REQUEST ONE-TIME PASSWORD". The dialog box is overlaid on a blurred background of a login window. It contains a dropdown menu with the selected option "I need emergency access to computer". Below this is a text field for "EMAIL" containing "johnson.kenneth@email.net". Underneath is a text area for "COMMENT" containing "Kenneth Johnson to update the db". At the bottom are "Cancel" and "Request" buttons.

Syteca

REQUEST ONE-TIME PASSWORD

I need emergency access to computer

Please enter your email address for the one-time password to be sent to it.

EMAIL

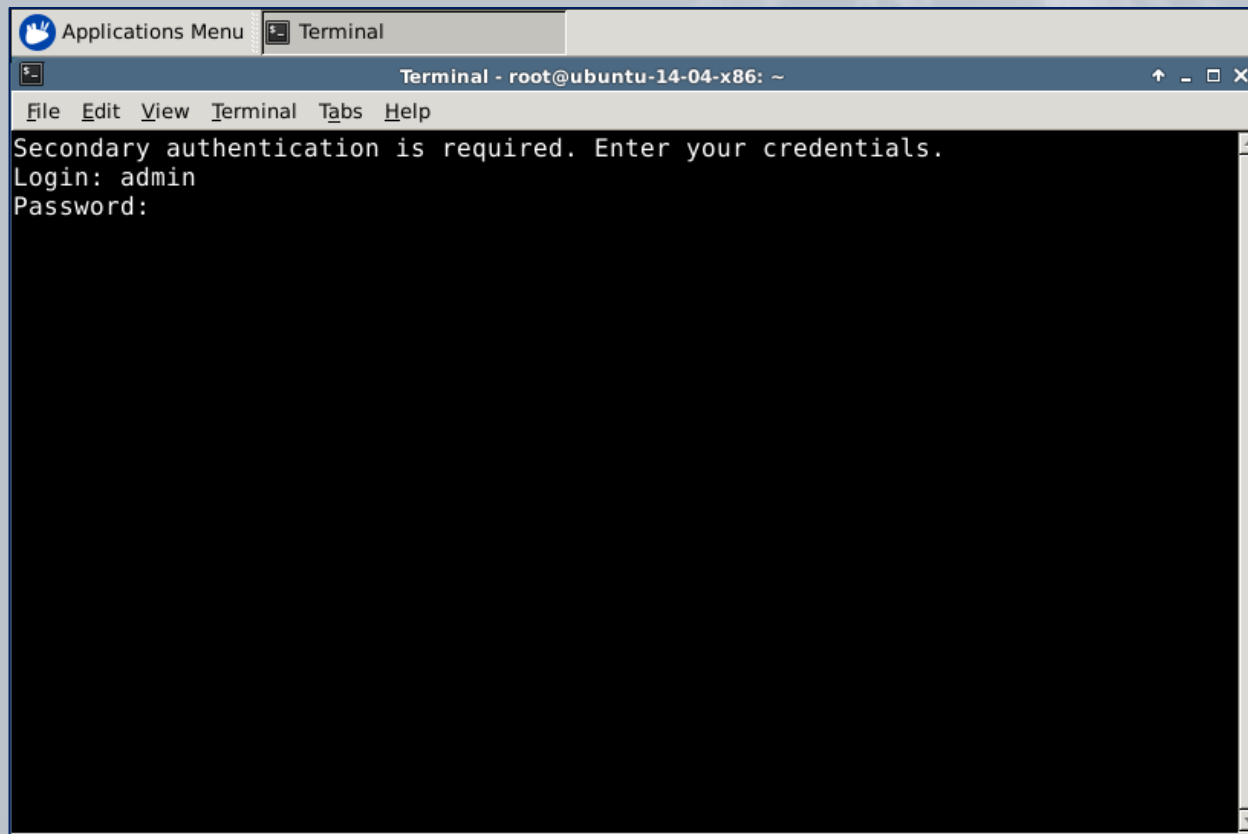
Email: johnson.kenneth@email.net

COMMENT

Kenneth Johnson to update the db

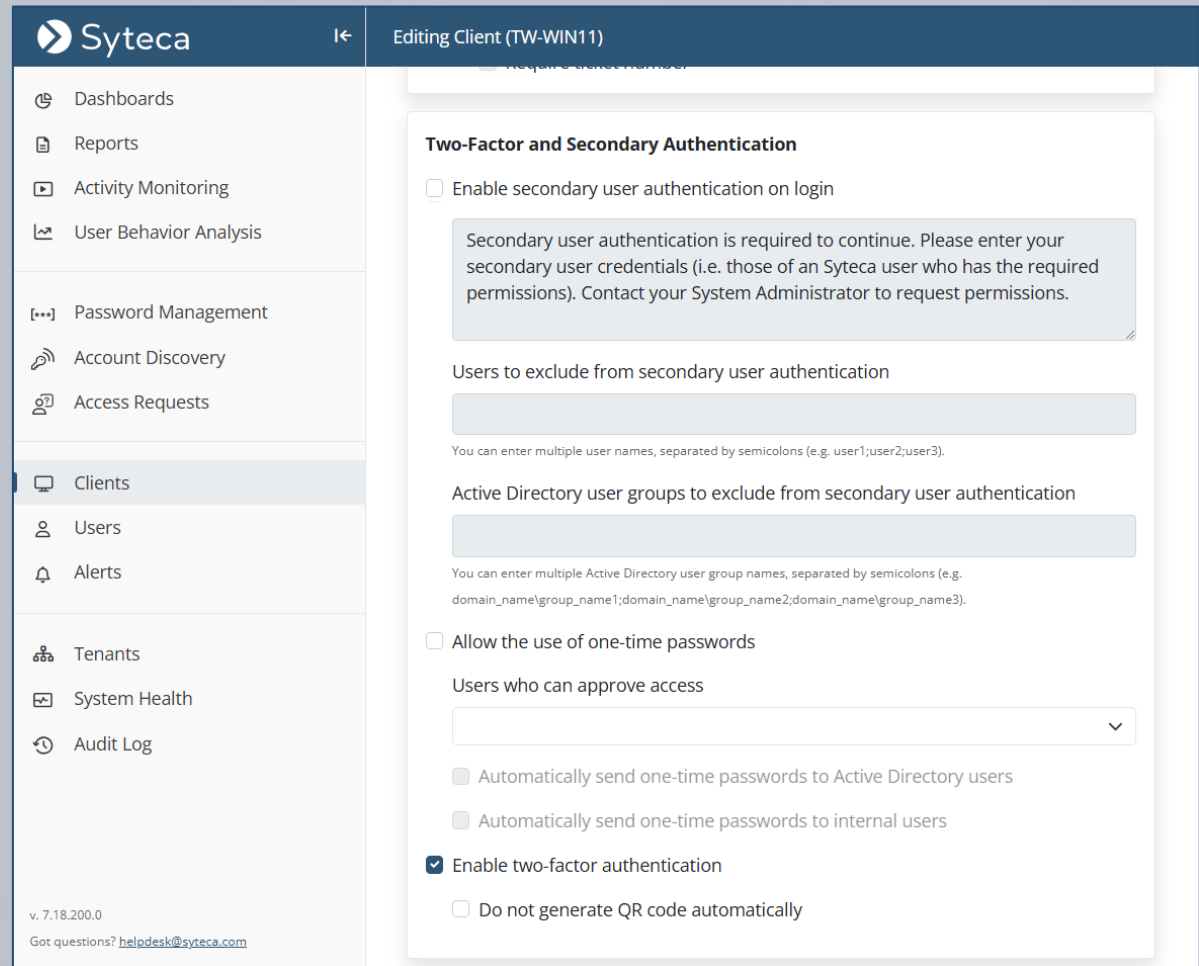
Cancel Request

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.



The screenshot shows the Syteca management console interface. The left sidebar contains a navigation menu with the following items: Dashboards, Reports, Activity Monitoring, User Behavior Analysis, Password Management, Account Discovery, Access Requests, Clients (highlighted), Users, Alerts, Tenants, System Health, and Audit Log. The main content area is titled "Editing Client (TW-WIN11)" and displays the "Two-Factor and Secondary Authentication" settings. The settings include:

- Enable secondary user authentication on login
- A text box containing: "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 (text input field)
- Active Directory user groups to exclude from secondary user authentication (text input field)
- Allow the use of one-time passwords
- Users who can approve access (dropdown menu)
- 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

At the bottom left of the console, it shows version "v. 7.18.200.0" and a link for "Got questions? helpdesk@syteca.com".

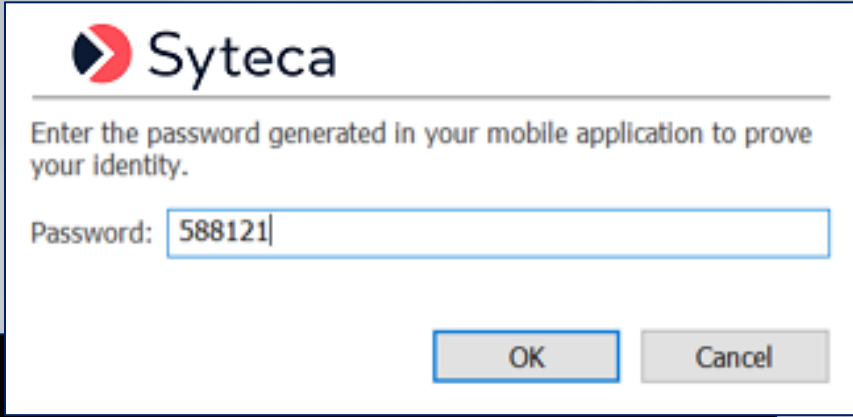
Two-Factor Authentication (Windows/Linux)



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.

User	User Type	Time Added	Added By	One-Time password	Remove All
Nick	Syteca user for secondar...	02/07/2023 2:07:34 pm	admin	👁	🗑
WIN10Administrator	Local computer user	02/07/2023 2:06:16 pm	admin	👁	🗑
support.local\alex1	Active Directory user	02/07/2023 2:05:44 pm	admin	👁	🗑

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



The dialog box 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." A text input field is positioned below this text, containing the value "588121". At the bottom right of the dialog, 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: _
```

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

Password


Confirm password

Enable two-factor authentication on login RESET 2FA

First name

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**.

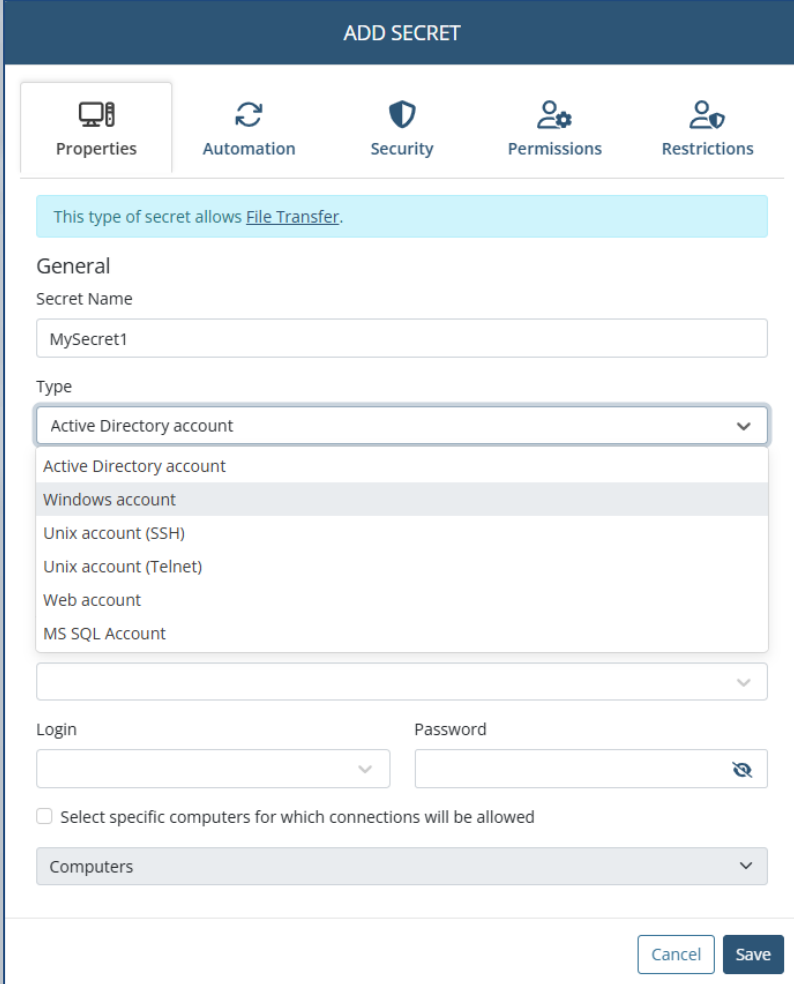
With Syteca, you can:

- 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:

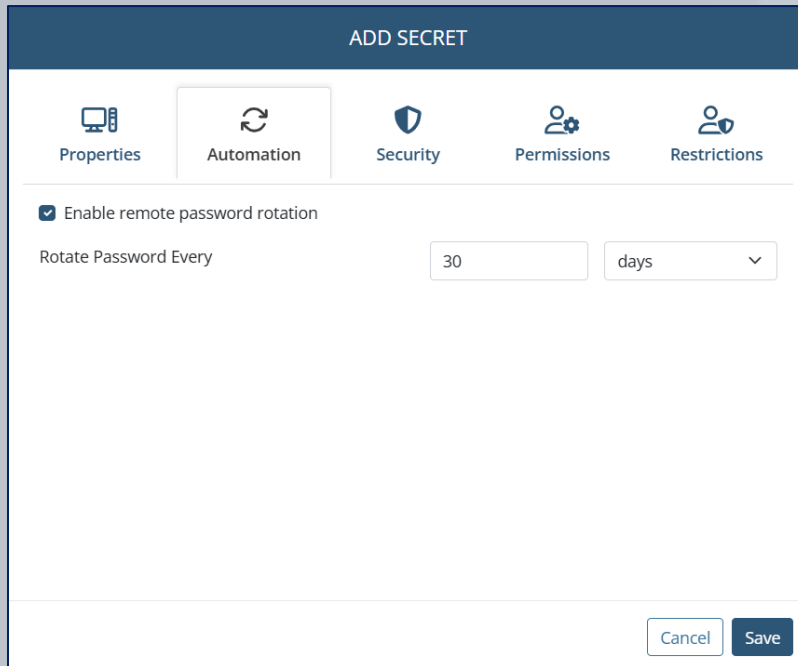
- a **privileged account** to connect to
- the account **credentials**
- and **users / user groups** to give access to
- and much more!



The screenshot shows the 'ADD SECRET' configuration page. At the top, there are navigation tabs: Properties, Automation, Security, Permissions, and Restrictions. A light blue banner states: 'This type of secret allows [File Transfer](#).' Below this, the 'General' section contains a 'Secret Name' field with the value 'MySecret1'. The 'Type' section features a dropdown menu currently set to 'Active Directory account', with a list of other options: 'Active Directory account', 'Windows account', 'Unix account (SSH)', 'Unix account (Telnet)', 'Web account', and 'MS SQL Account'. Below the dropdown is another empty dropdown menu. The 'Login' and 'Password' fields are present, with the password field having an eye icon for visibility. A checkbox labeled 'Select specific computers for which connections will be allowed' is checked, and a dropdown menu below it is set to 'Computers'. At the bottom right, there are 'Cancel' and 'Save' buttons.

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**



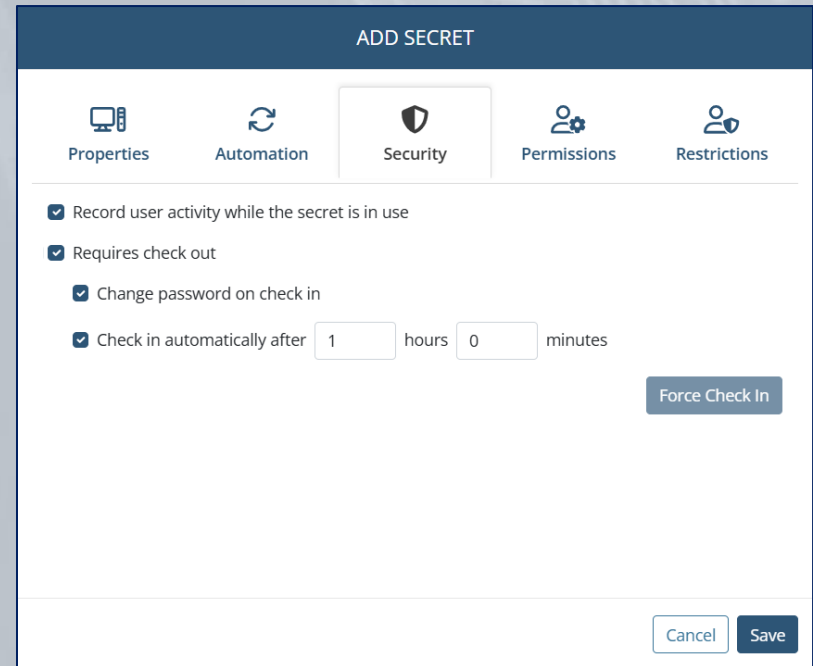
ADD SECRET

Properties Automation **Security** Permissions Restrictions

Enable remote password rotation

Rotate Password Every

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 hours 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 v

Inherit advanced permissions from current folder

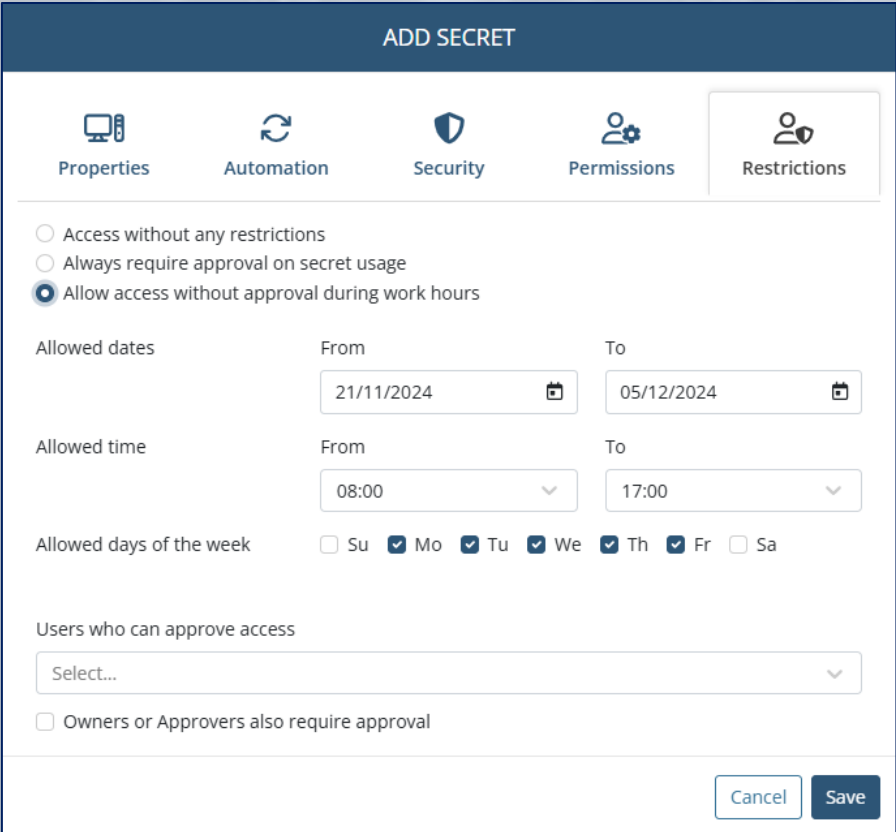
User / User group ▼	Role Type				Remove All
admin (Administrator)	Owner ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
David (David Doe)	Editor ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input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

< 1 >

Cancel Save

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

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



ADD SECRET

Properties Automation Security Permissions **Restrictions**

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

Allowed dates From 21/11/2024 To 05/12/2024

Allowed time From 08:00 To 17:00

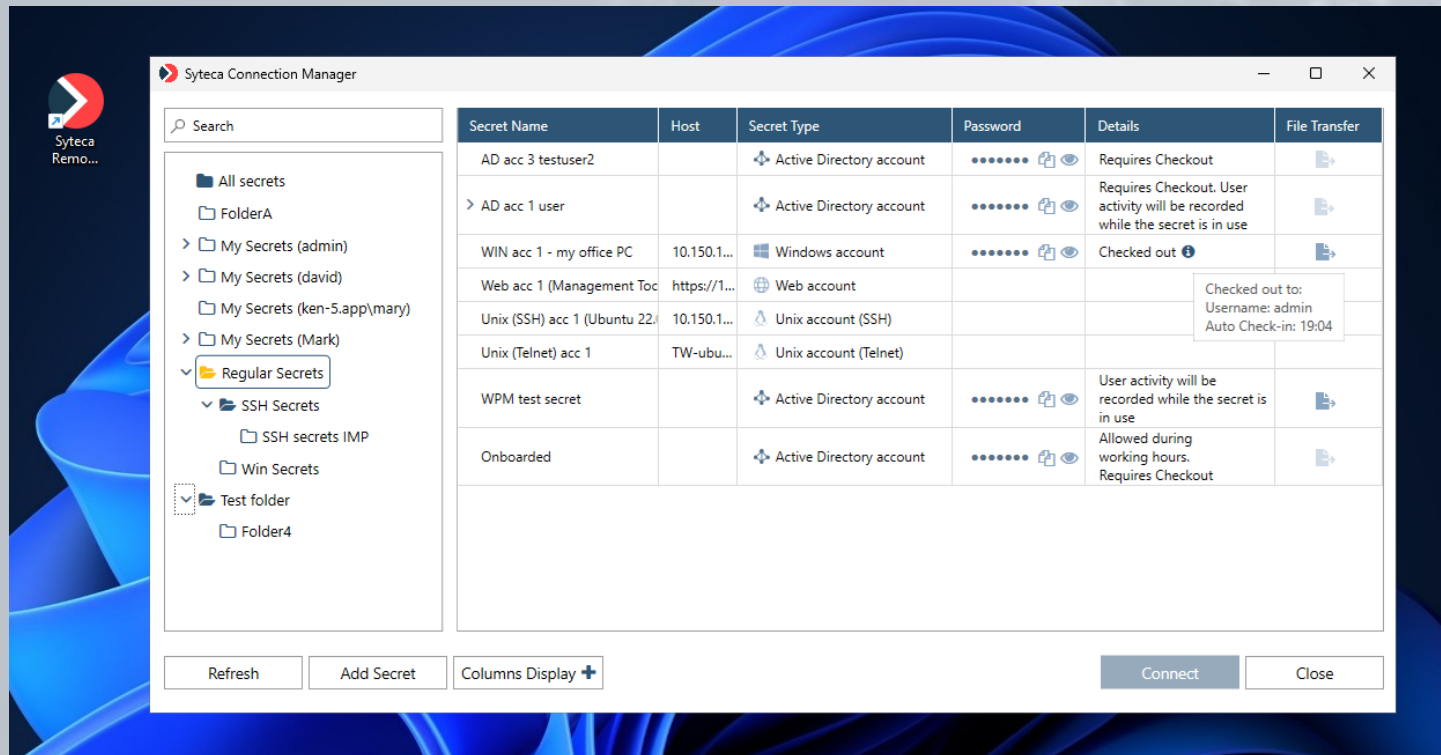
Allowed days of the week Su Mo Tu We Th Fr Sa

Users who can approve access
Select...

Owners or Approvers also require approval

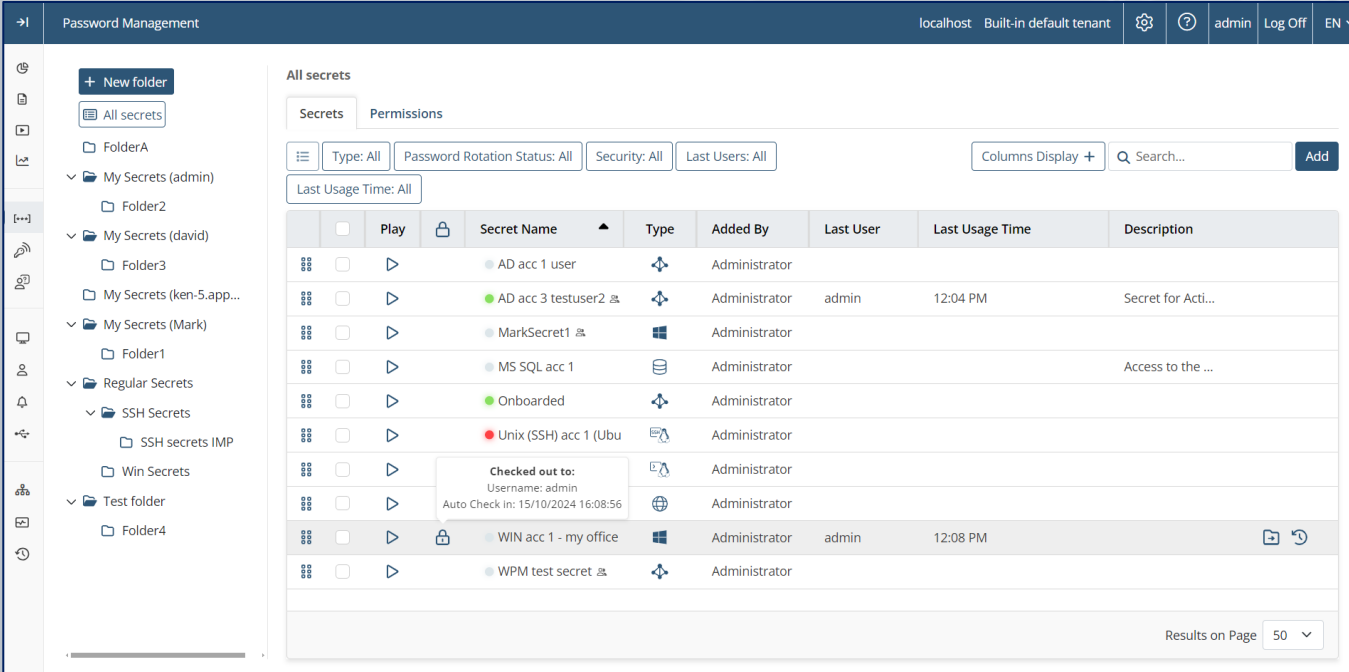
Cancel Save

A **privileged user can access a critical endpoint via a secret** by using 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** on a specific secret (in any folder) **to open the list of sessions which it was used in**. The **secret data is highlighted** when playing the session in the Session Viewer.

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

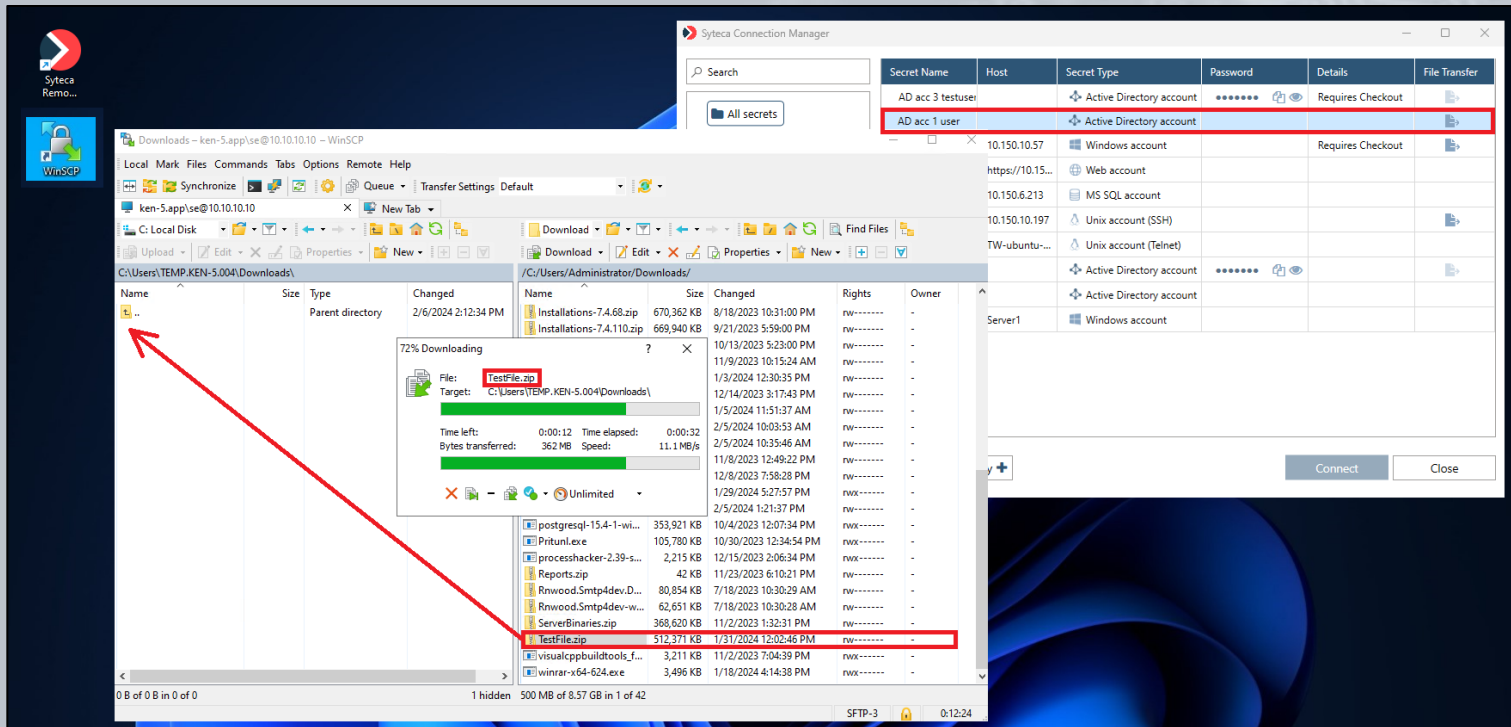


The screenshot displays the Password Management interface. On the left, a sidebar shows a folder tree with 'Test folder' selected. The main area shows a table of secrets with columns for 'Secret Name', 'Type', 'Added By', 'Last User', 'Last Usage Time', and 'Description'. The 'WIN acc 1 - my office' secret is highlighted, and its 'Last Usage Time' is 12:08 PM. Below the table, there is a 'Results on Page' dropdown set to 50.

	Play	Secret Name	Type	Added By	Last User	Last Usage Time	Description
		AD acc 1 user	Administrator	Administrator			
		AD acc 3 testuser2	Administrator	Administrator	admin	12:04 PM	Secret for Acti...
		MarkSecret1	Administrator	Administrator			
		MS SQL acc 1	Administrator	Administrator			Access to the ...
		Onboarded	Administrator	Administrator			
		Unix (SSH) acc 1 (Ubu)	Administrator	Administrator			
		Checked out to: Username: admin Auto Check in: 15/10/2024 16:08:56	Administrator	Administrator			
		WIN acc 1 - my office	Administrator	Administrator	admin	12:08 PM	
		WPM test secret	Administrator	Administrator			

Transferring Files Using WinSCP

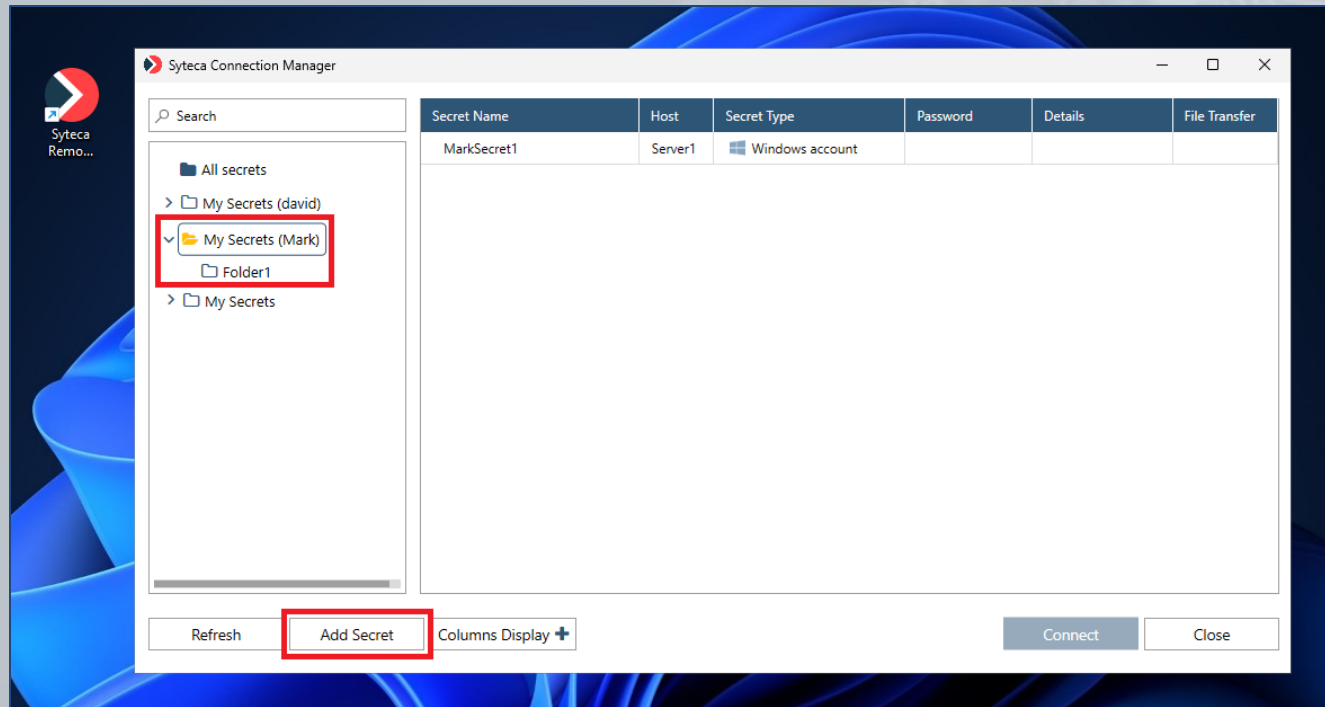
The **File Transfer** functionality allows users of secrets to transfer files **between the computer** with the Syteca Connection Manager and **the remote computers** (which are accessed via the secrets) by using the **WinSCP application**.



The screenshot displays the WinSCP application interface and the Syteca Connection Manager. The WinSCP window shows a file transfer progress dialog for 'TestFile.zip' from 'ken-5.app@10.10.10' to 'C:\Users\ADMINISTRATOR\Downloads\'. The Syteca Connection Manager window shows a list of secrets, with 'AD acc 1 user' highlighted in red. A red arrow points from the 'TestFile.zip' entry in the WinSCP file list to the 'TestFile.zip' entry in the Syteca Connection Manager secrets list.

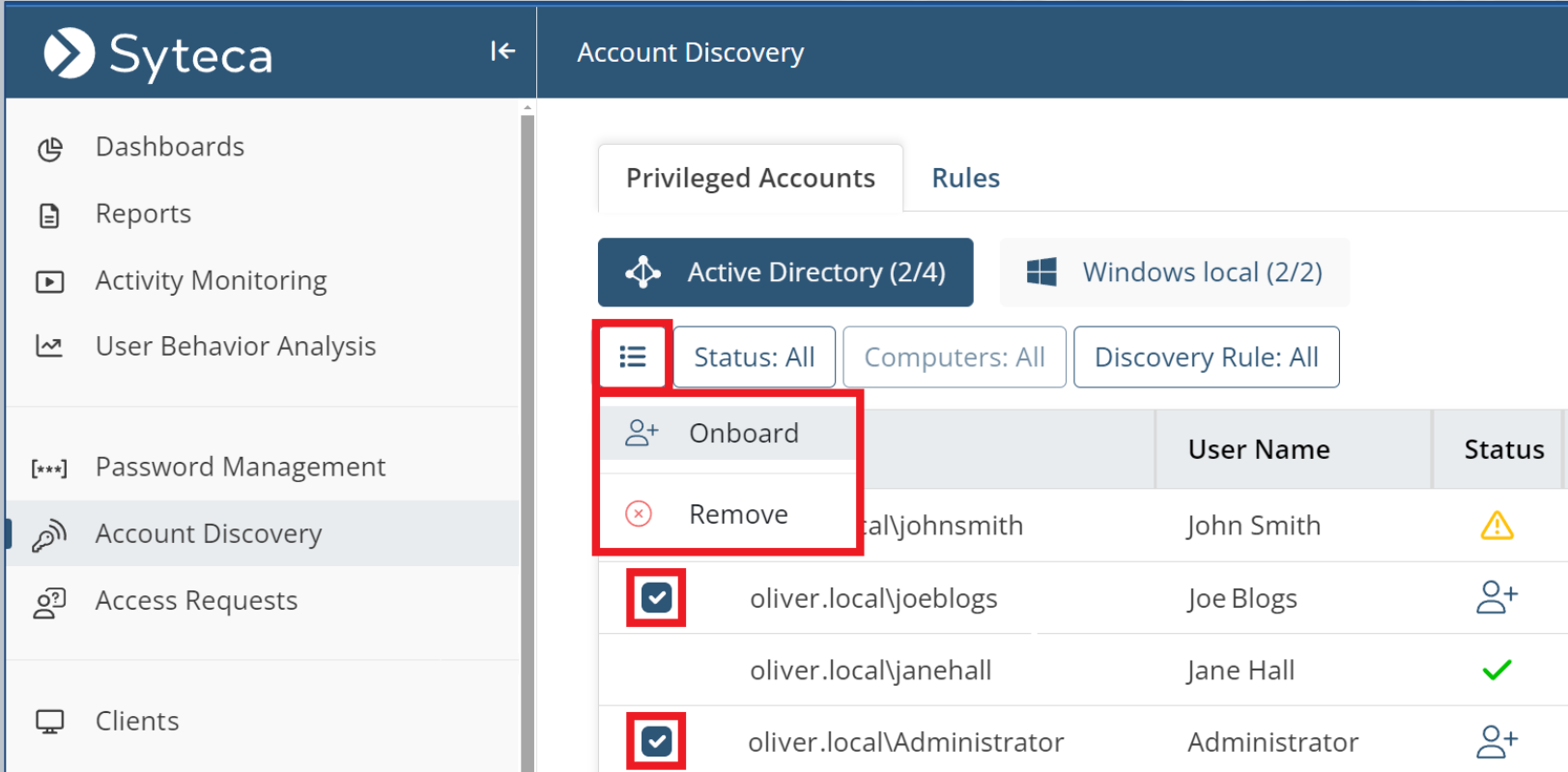
Secret Name	Host	Secret Type	Password	Details	File Transfer
AD acc 3 testuser		Active Directory account	*****	Requires Checkout	
AD acc 1 user		Active Directory account			
	10.150.10.57	Windows account		Requires Checkout	
	https://10.15...	Web account			
	10.150.6.213	MS SQL account			
	10.150.10.197	Unix account (SSH)			
	TW-ubuntu-...	Unix account (Telnet)			
		Active Directory account	*****		
		Active Directory account			
Server1		Windows account			

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)

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



The screenshot shows the Syteca Account Discovery interface. The left sidebar contains navigation options: Dashboards, Reports, Activity Monitoring, User Behavior Analysis, Password Management, Account Discovery (highlighted), Access Requests, and Clients. The main content area is titled 'Account Discovery' and features tabs for 'Privileged Accounts' and 'Rules'. Below these are filters for 'Active Directory (2/4)' and 'Windows local (2/2)'. There are also filter buttons for 'Status: All', 'Computers: All', and 'Discovery Rule: All'. A table of discovered accounts is shown with columns for 'User Name' and 'Status'. The 'Remove' button in the bulk actions menu is highlighted with a red box, as are the 'Onboard' and 'Remove' buttons in the row actions for the 'oliver.local\johsmith' account. The 'oliver.local\johsmith' account has a yellow warning icon, while 'oliver.local\joeblogs' and 'oliver.local\janehall' have a plus icon and a green checkmark, respectively. The 'oliver.local\Administrator' account has a plus icon and a blue checkmark.

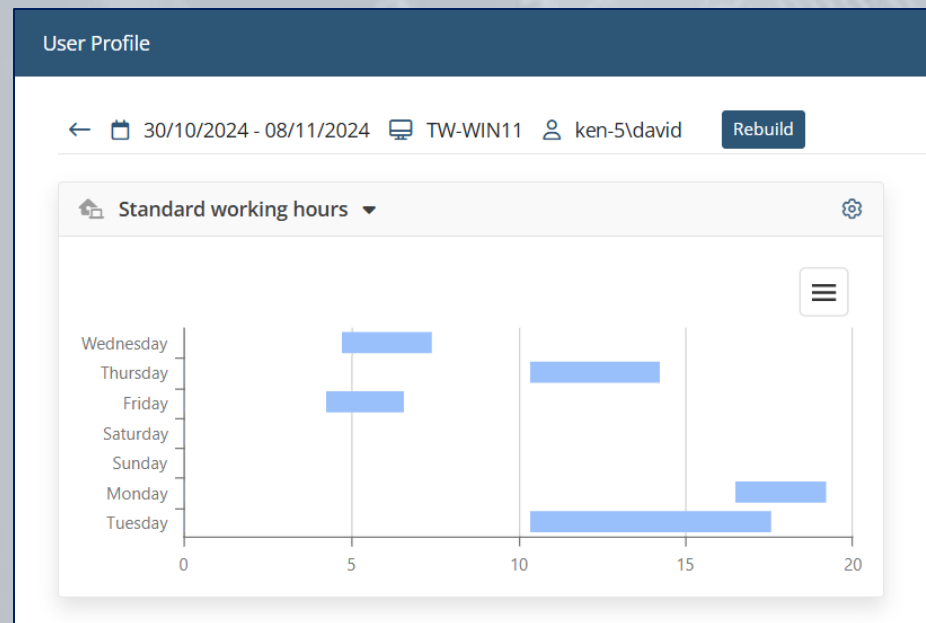
	User Name	Status
<input type="checkbox"/>	oliver.local\johsmith	John Smith 
<input checked="" type="checkbox"/>	oliver.local\joeblogs	Joe Blogs 
<input type="checkbox"/>	oliver.local\janehall	Jane Hall 
<input checked="" type="checkbox"/>	oliver.local\Administrator	Administrator 

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:
- Description:

Conditions

- Unusual work hours
-

Email Notifications

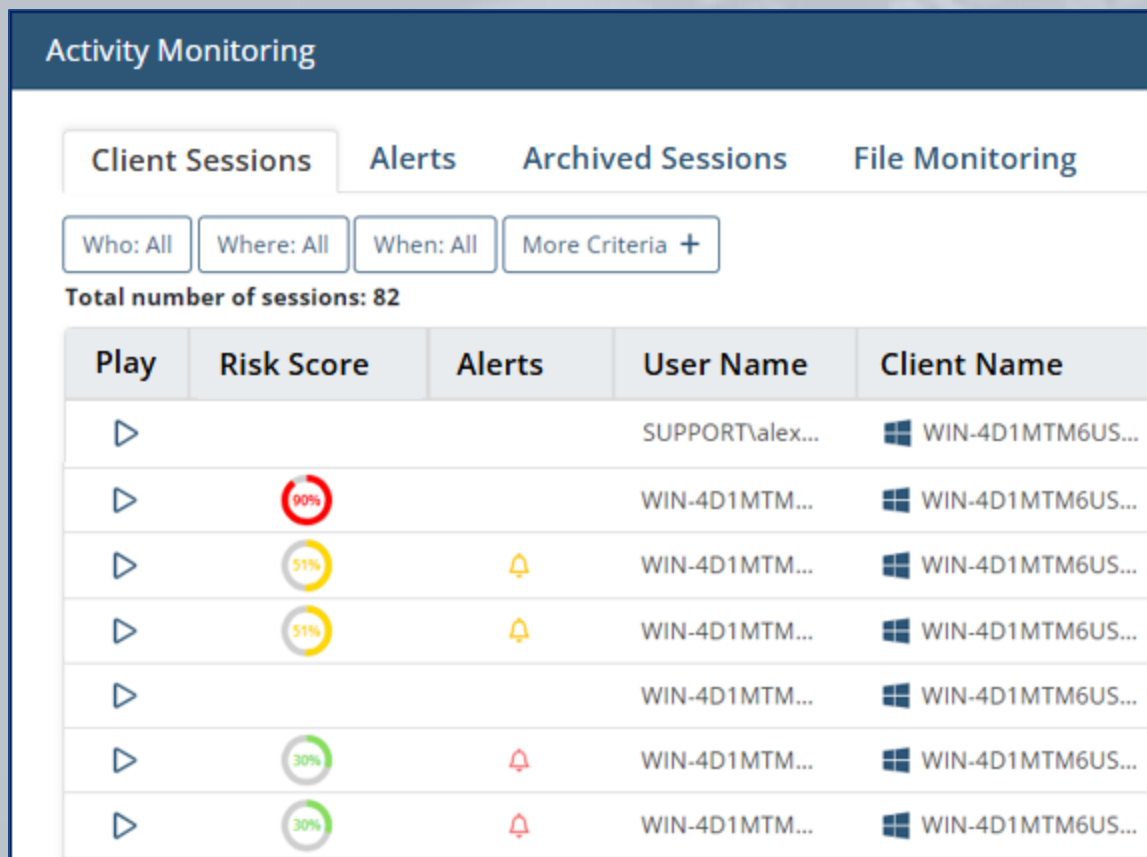
- Send notification on detected anomalies for a finished session
- Send instant notification on detected anomalies
- Send total session risk score in case of no anomalies
- Send email notification to:

Additional Actions

- Show warning message to user
-
- Block user in the current session

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.

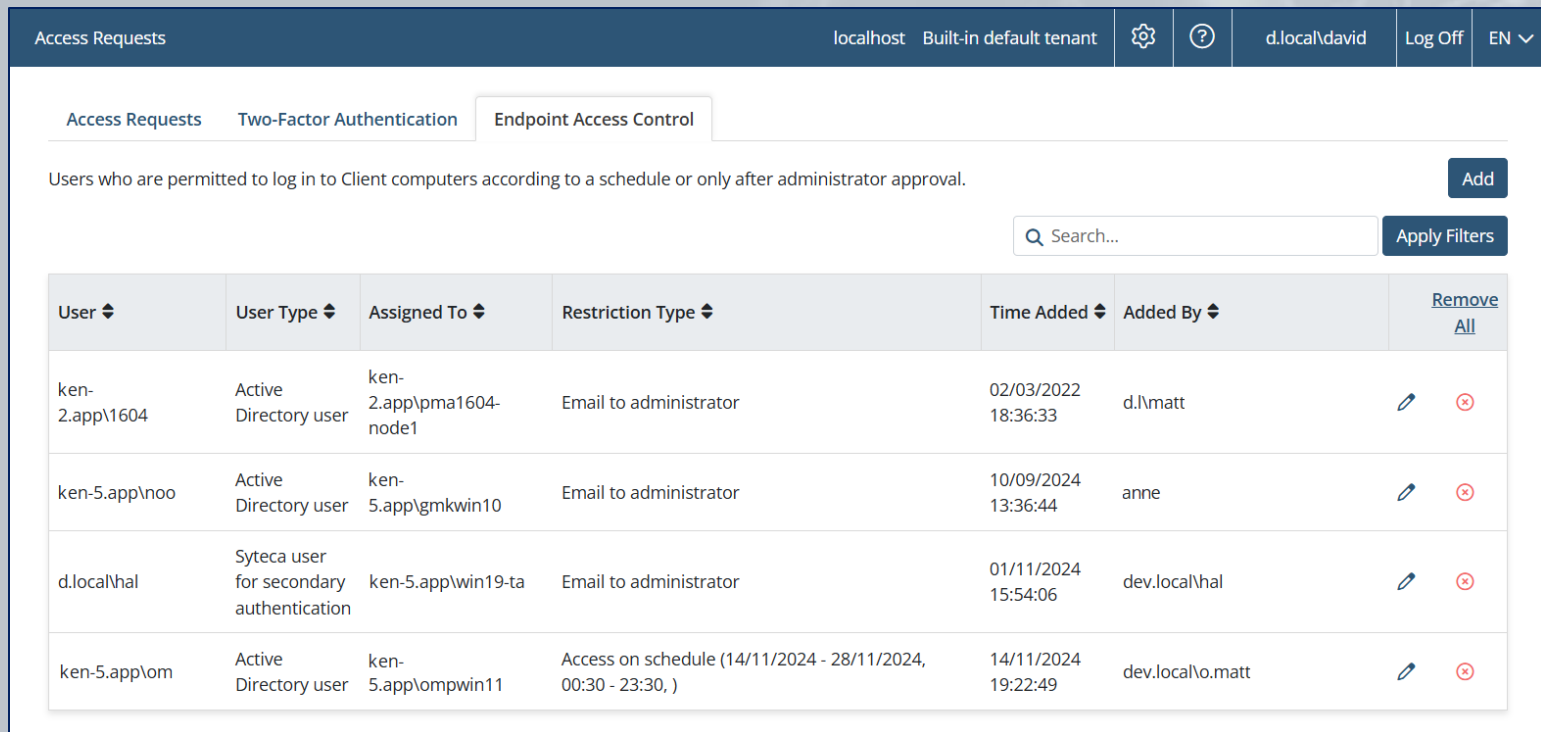


The screenshot displays the 'Activity Monitoring' interface. It features a navigation bar with tabs for 'Client Sessions', 'Alerts', 'Archived Sessions', and 'File Monitoring'. Below the navigation bar are filter controls for 'Who: All', 'Where: All', 'When: All', and 'More Criteria +'. A summary line indicates 'Total number of sessions: 82'. The main content is a table with the following columns: 'Play', 'Risk Score', 'Alerts', 'User Name', and 'Client Name'. The table lists several sessions, with risk scores represented by circular progress indicators (90%, 51%, 51%, 30%, 30%) and alerts indicated by bell icons.









Play	Risk Score	Alerts	User Name	Client Name
▶			SUPPORT\alex...	WIN-4D1MTM6US...
▶	90%		WIN-4D1MTM...	WIN-4D1MTM6US...
▶	51%	🔔	WIN-4D1MTM...	WIN-4D1MTM6US...
▶	51%	🔔	WIN-4D1MTM...	WIN-4D1MTM6US...
▶			WIN-4D1MTM...	WIN-4D1MTM6US...
▶	30%	🔔	WIN-4D1MTM...	WIN-4D1MTM6US...
▶	30%	🔔	WIN-4D1MTM...	WIN-4D1MTM6US...

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.



The screenshot displays the 'Access Requests' management interface. At the top, there are navigation tabs for 'Access Requests', 'Two-Factor Authentication', and 'Endpoint Access Control'. Below the tabs, a descriptive text states: 'Users who are permitted to log in to Client computers according to a schedule or only after administrator approval.' To the right of this text is an 'Add' button. Below the text is a search bar with the placeholder 'Search...' and an 'Apply Filters' button. The main content is a table with the following columns: 'User', 'User Type', 'Assigned To', 'Restriction Type', 'Time Added', 'Added By', and 'Remove All'. The table contains four rows of data.

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.\lmatt	 
ken-5.app\noo	Active Directory user	ken-5.app\gmkwin10	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 

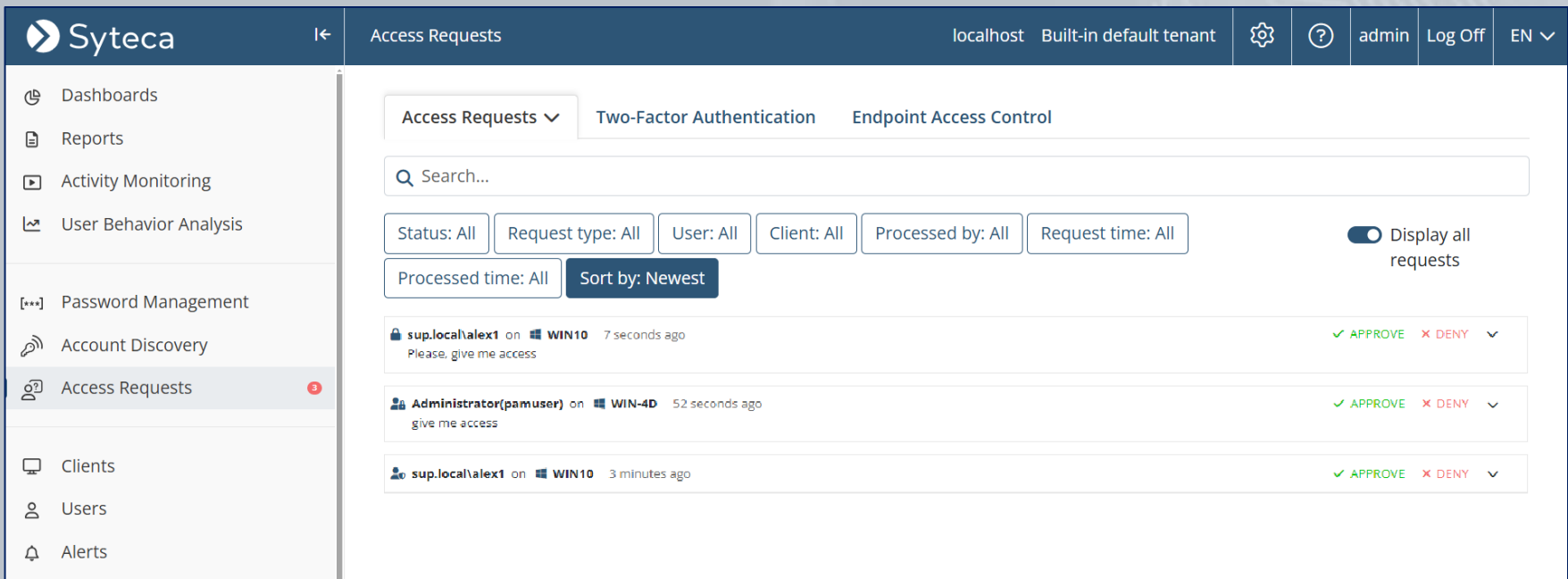
Allowed time

From  To 

Allowed weekdays

Su Mo Tu We Th Fr Sa

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 top navigation bar includes the Syteca logo, a back arrow, the page title "Access Requests", and user information: "localhost Built-in default tenant", "admin", "Log Off", and "EN". A left sidebar contains navigation options: 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 features tabs for "Access Requests", "Two-Factor Authentication", and "Endpoint Access Control". Below the tabs is a search bar and a set of filter buttons: "Status: All", "Request type: All", "User: All", "Client: All", "Processed by: All", and "Request time: All". There is also a "Sort by: Newest" button and a "Display all requests" toggle switch.

The list of access requests is as follows:

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.

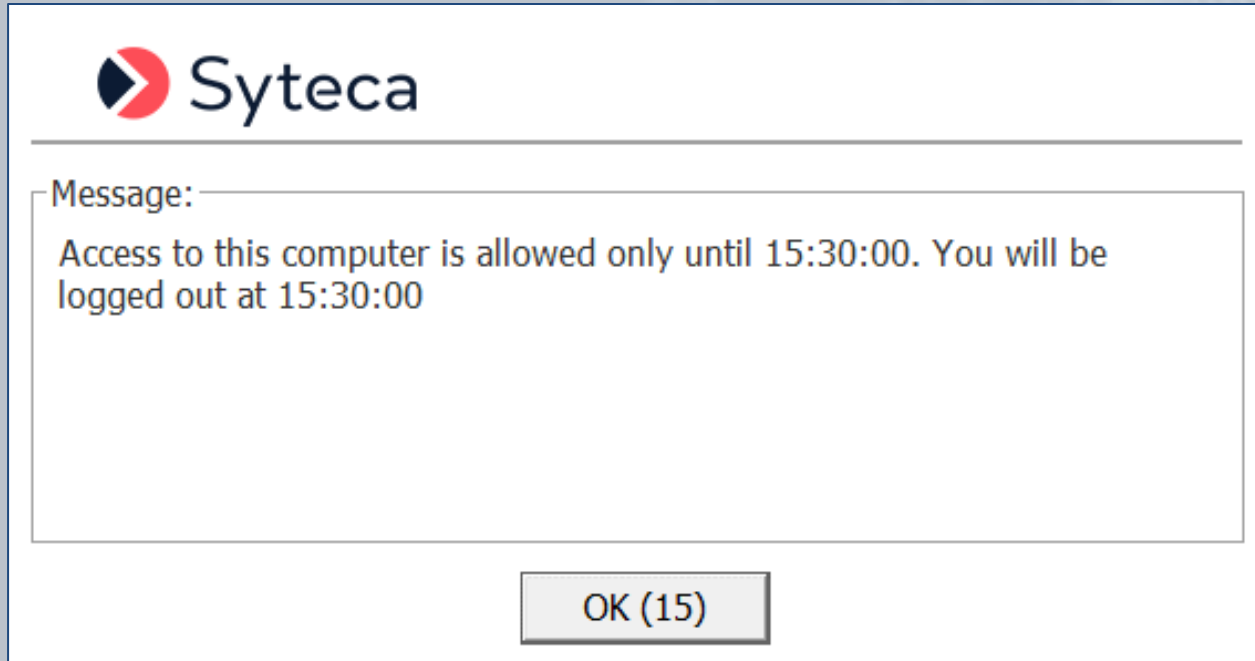
Cancel



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

OK

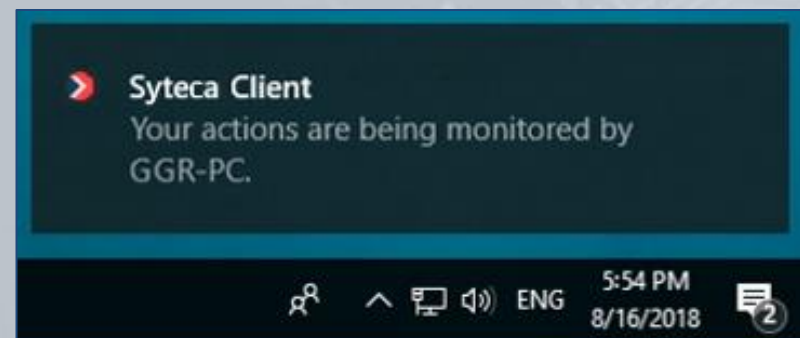
Restricted users will be able to **log in** to Client computers **only during the defined time period**, and will need **additional approval** to log in **outside of this period**.



Notifying Users About Being Monitored

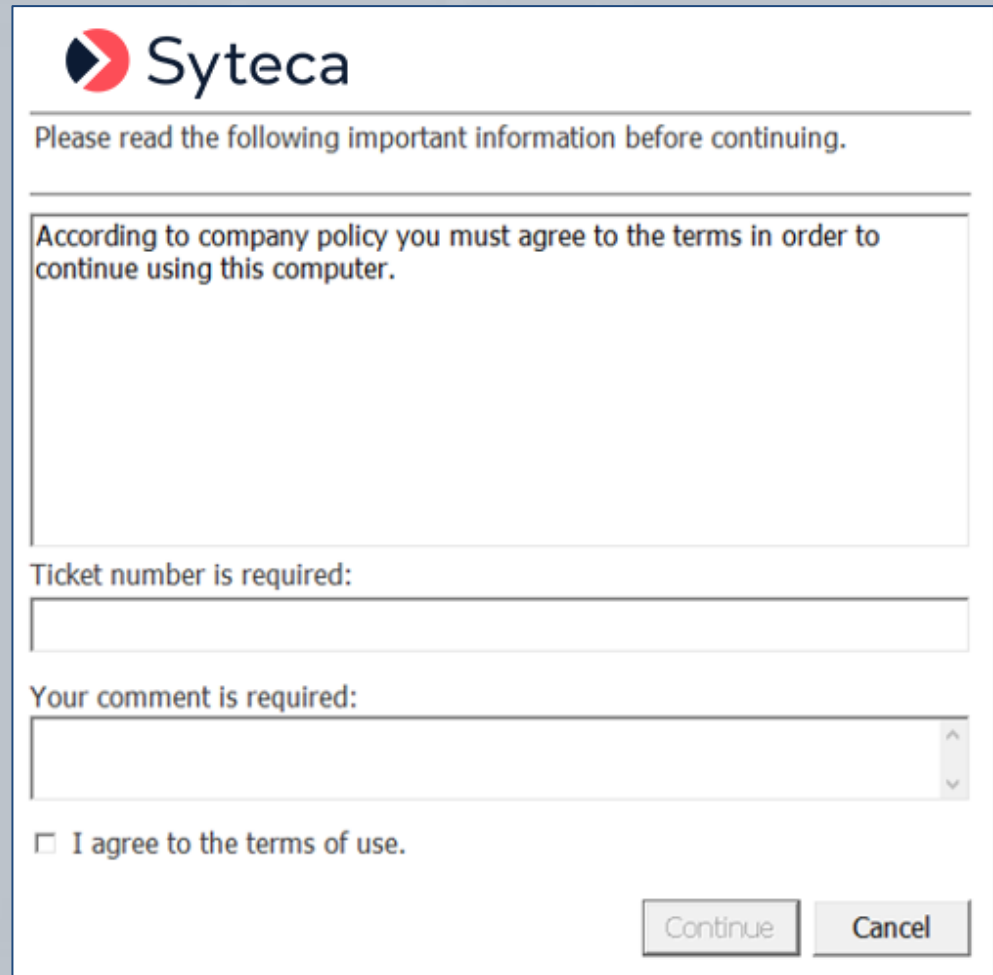
To adhere to the **security policy** of your company or your **country regulations**, you can:

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



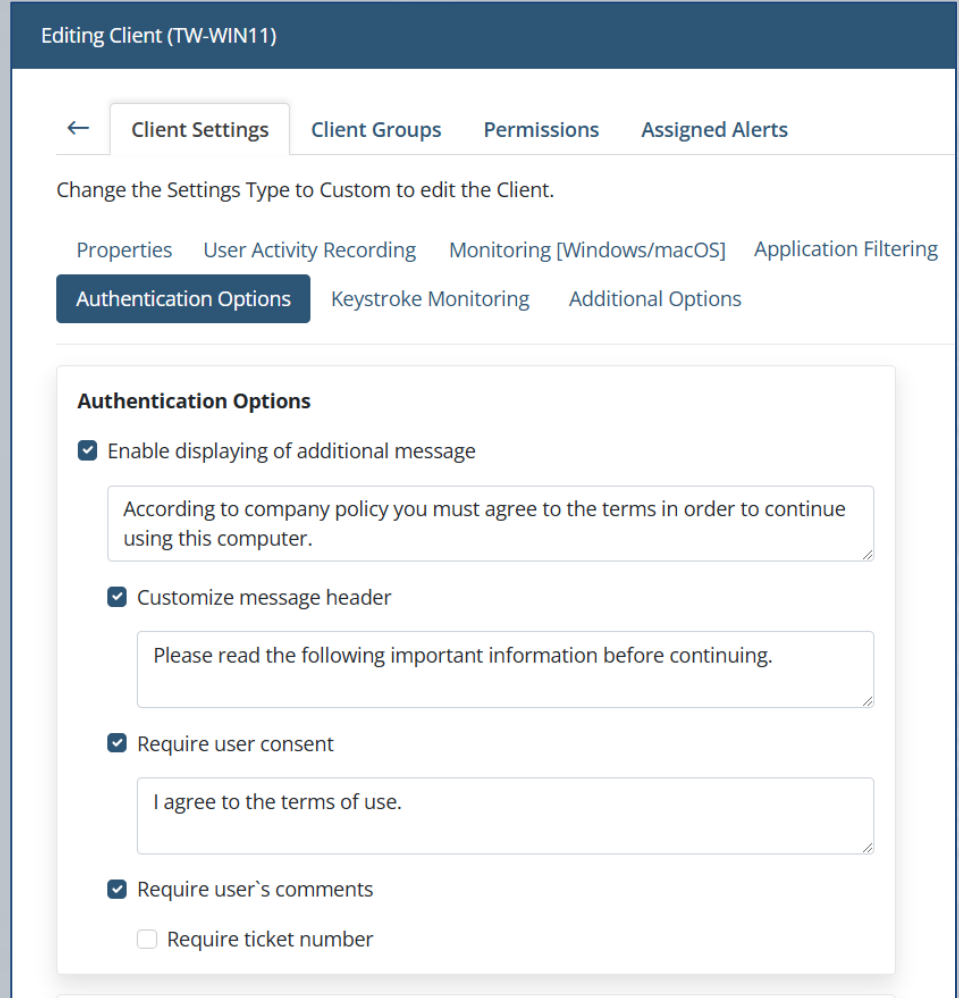
Before being allowed to log in to the Client computer, users can also be **required to:**

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



The screenshot shows a web form with the Syteca logo at the top. Below the logo, a message reads: "Please read the following important information before continuing." This is followed by a large text box containing the text: "According to company policy you must agree to the terms in order to continue using this computer." Below this text box are three input fields: "Ticket number is required:" (a text box), "Your comment is required:" (a text area), and a checkbox labeled "I agree to the terms of use." At the bottom right of the form are two buttons: "Continue" and "Cancel".

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. The 'Client Settings' tab is active, and the 'Authentication Options' sub-tab is selected. The 'Enable displaying of additional message' checkbox is checked. Below it, a text area contains the message: 'According to company policy you must agree to the terms in order to continue using this computer.' The 'Customize message header' checkbox is also checked, with a text area containing: 'Please read the following important information before continuing.' The 'Require user consent' checkbox is checked, with a text area containing: 'I agree to the terms of use.' The 'Require user's comments' checkbox is checked, and the 'Require ticket number' checkbox is unchecked.

Editing Client (TW-WIN11)

← Client Settings Client Groups Permissions Assigned Alerts

Change the Settings Type to Custom to edit the Client.

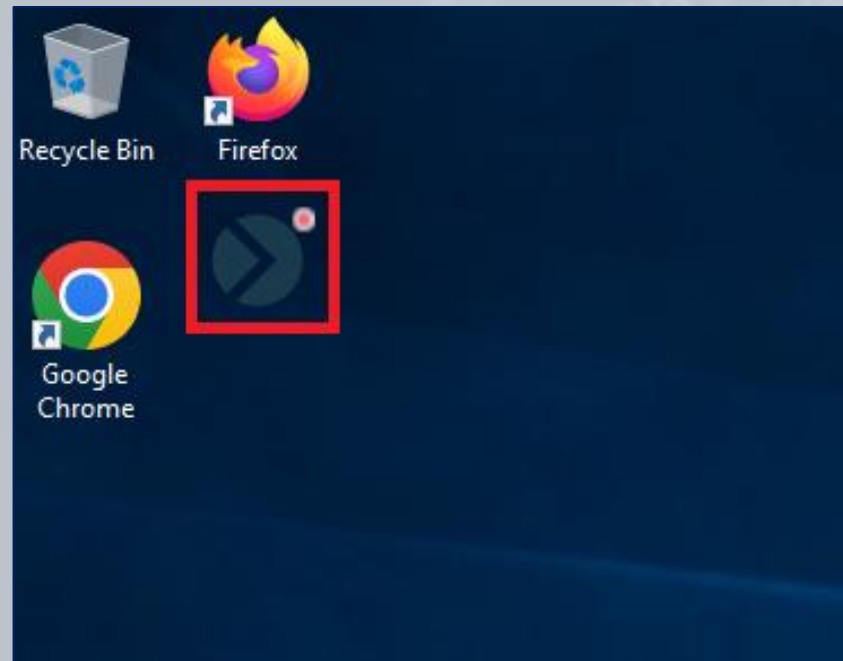
Properties User Activity Recording Monitoring [Windows/macOS] Application Filtering

Authentication Options Keystroke Monitoring Additional Options

Authentication Options

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

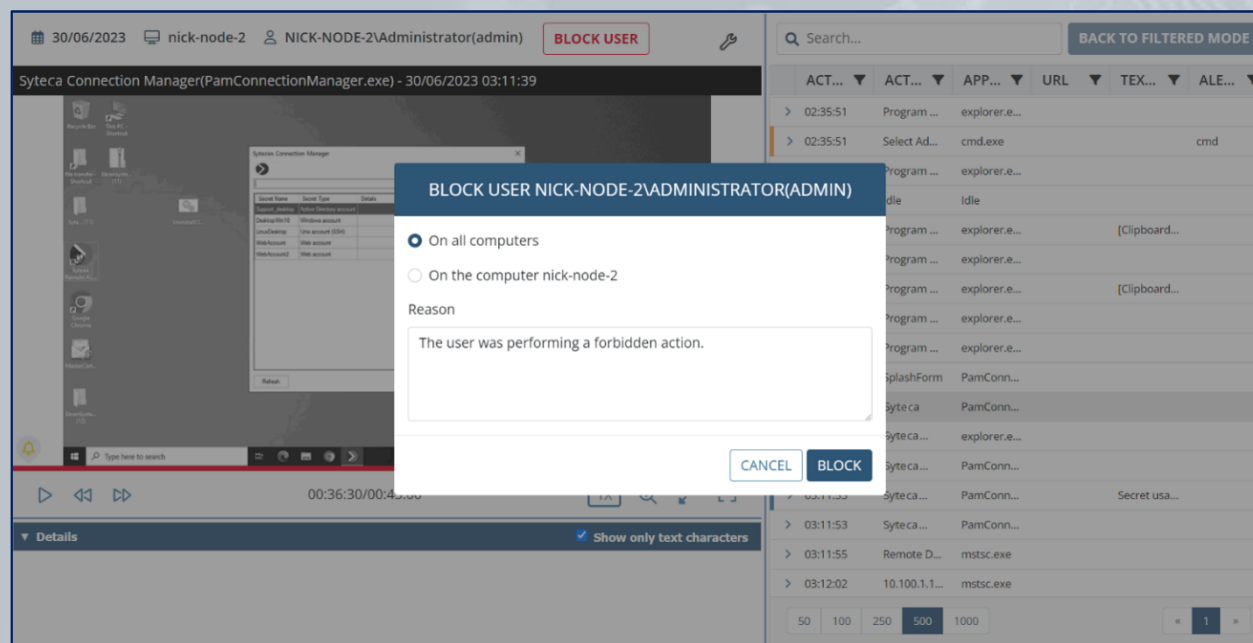
- An **icon** can also be displayed on the desktop (that is always on top of all applications opened) to **inform users** that **their actions** are currently **being monitored and recorded**.



Blocking Users

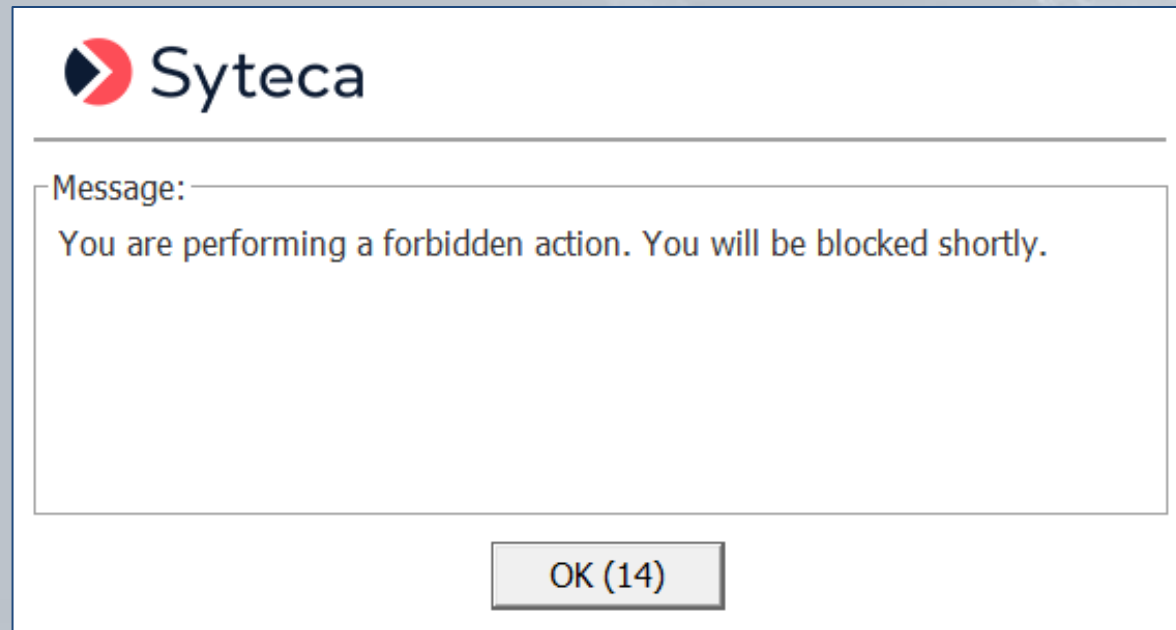
Syteca allows you to **block endpoint users** from performing potentially harmful and forbidden actions on computers running Windows OS with Syteca Clients installed on them.

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



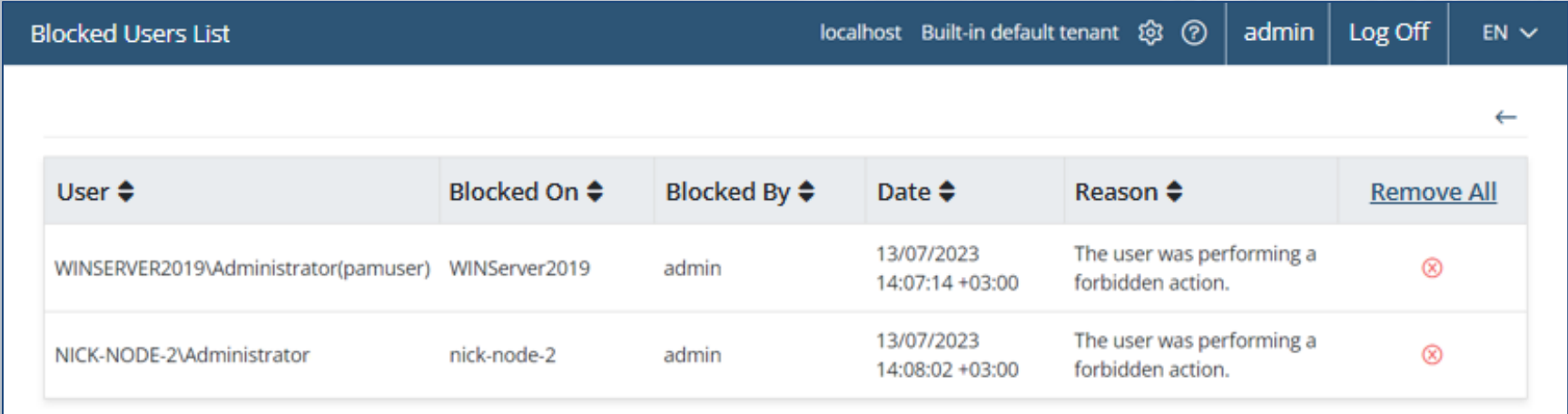
The endpoint user's **desktop is blocked**, and after a defined time interval the user is **forcibly logged out**.

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



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.



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

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
user1	John	Doe

PAM USERS: Group does not have permission to access

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

APPLICATION ACCOUNTS:

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

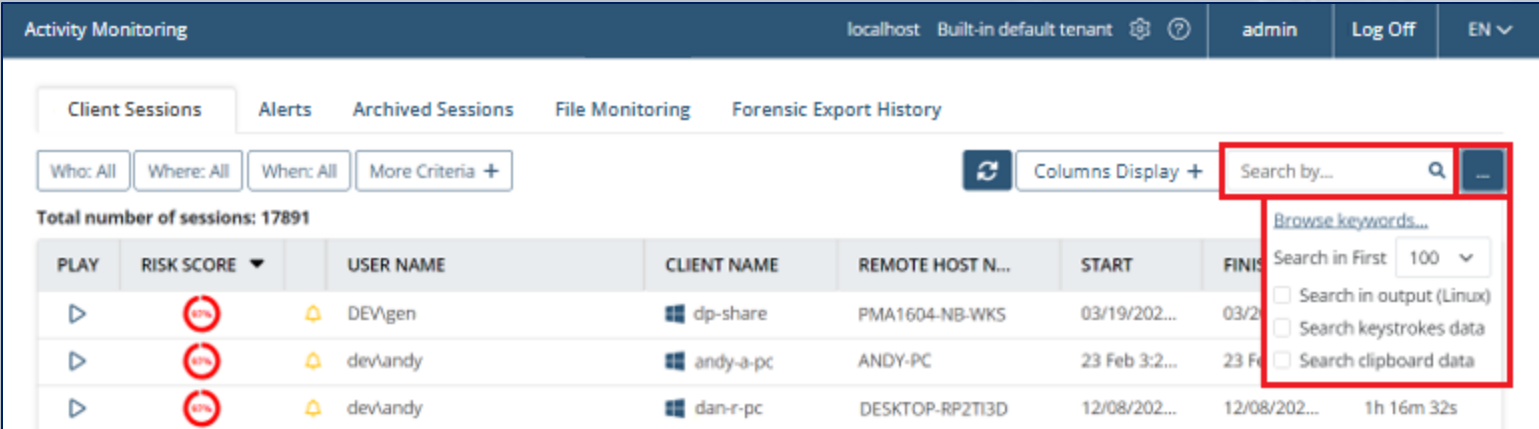
USER1

Do you want to unlock this user account?

Viewing Client Sessions

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

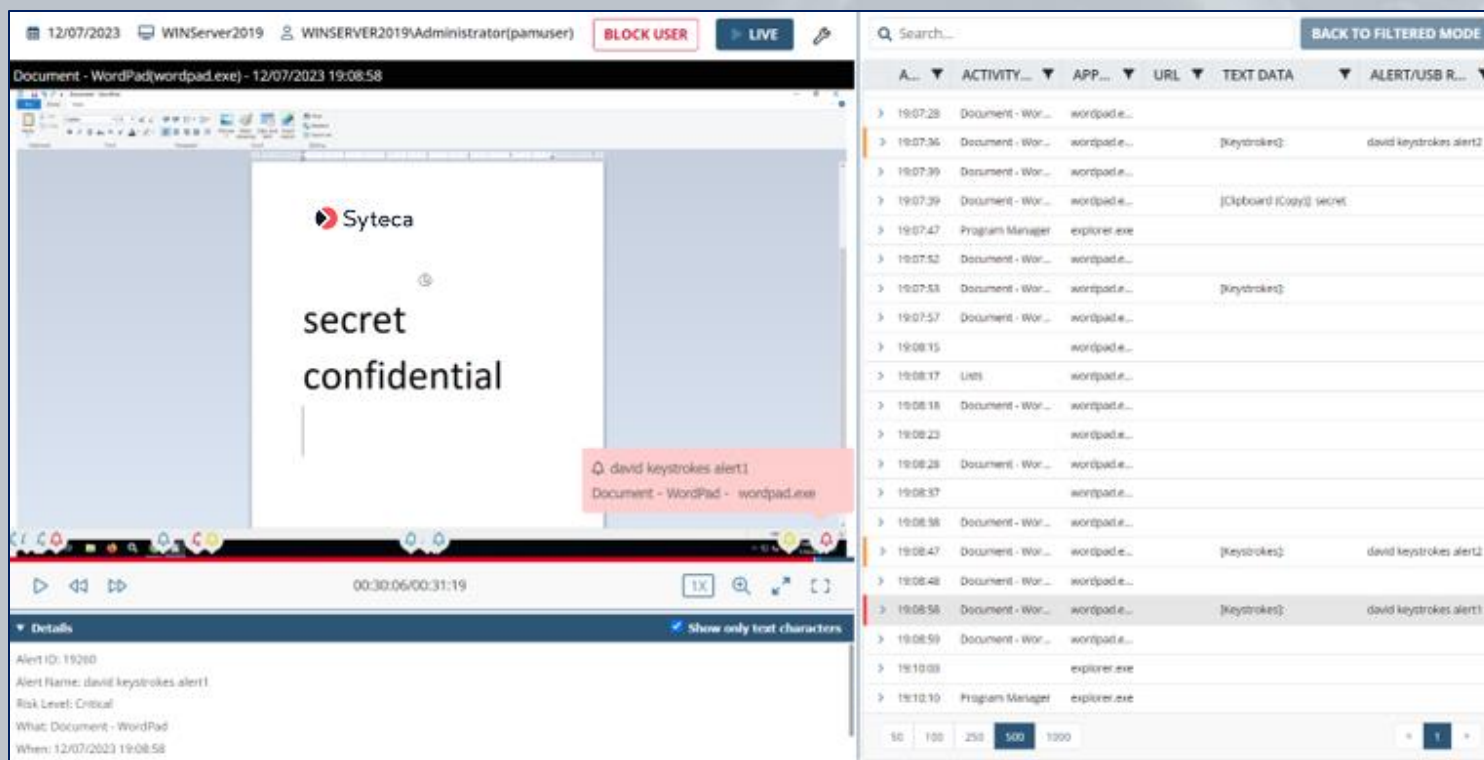
- **For Windows Clients:** active window title, application name, user name, Client name, URL visited, keystrokes, clipboard data, user's comment in additional message, ticket number, USB device info, etc.
- **For macOS Clients:** active window title, application name, user name, Client name, URL visited, 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 'Activity Monitoring' dashboard. At the top, it shows 'localhost Built-in default tenant' and user 'admin'. Below the navigation tabs (Client Sessions, Alerts, Archived Sessions, File Monitoring, Forensic Export History), there are filter buttons for 'Who: All', 'Where: All', and 'When: All'. A search bar is highlighted with a red box, containing a 'Search by...' dropdown menu. The dropdown menu is also highlighted with a red box and lists search options: 'Browse keywords...', 'Search in First 100', 'Search in output (Linux)', 'Search keystrokes data', and 'Search clipboard data'. Below the search bar, a table lists client sessions with columns for PLAY, RISK SCORE, USER NAME, CLIENT NAME, REMOTE HOST N..., START, and FINIS. The first three rows show sessions for users 'DEV\gen', 'devVandy', and 'devVandy' with a risk score of 50%.

PLAY	RISK SCORE	USER NAME	CLIENT NAME	REMOTE HOST N...	START	FINIS
▶	50%	DEV\gen	dp-share	PMA1604-NB-WKS	03/19/202...	03/2
▶	50%	devVandy	andy-a-pc	ANDY-PC	23 Feb 3:2...	23 F
▶	50%	devVandy	dan-r-pc	DESKTOP-RP2T3D	12/08/202...	12/08/202... 1h 16m 32s

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**.



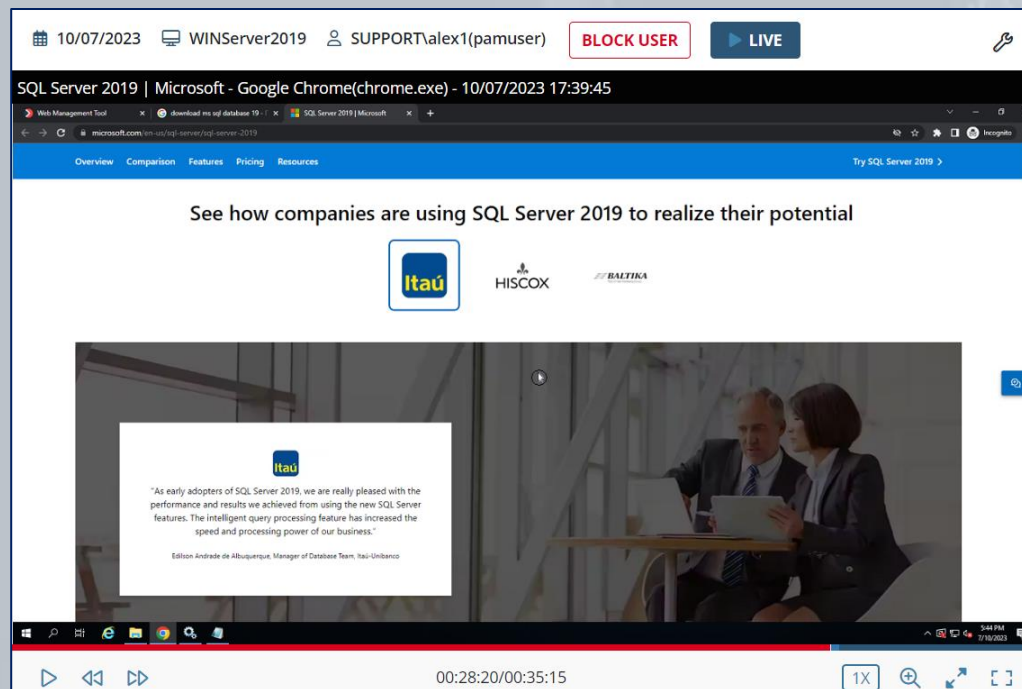
The screenshot displays the Syteca Session Viewer interface. The left pane shows a video player with a screen capture of a WordPad window. The window title is "Document - WordPad[wordpad.exe] - 12/07/2023 19:08:58". The content of the window shows the Syteca logo and the text "secret confidential". A red alert box is overlaid on the video, indicating "david keystrokes alert1" for "Document - WordPad - wordpad.exe". The video player controls show a progress bar at 00:30:06/00:31:19 and a 1X zoom level.

The right pane displays a table of session metadata. The table has columns for time, activity, application, URL, text data, and alert/USB R... The table is filtered to show only text characters. The following table represents the data shown in the screenshot:

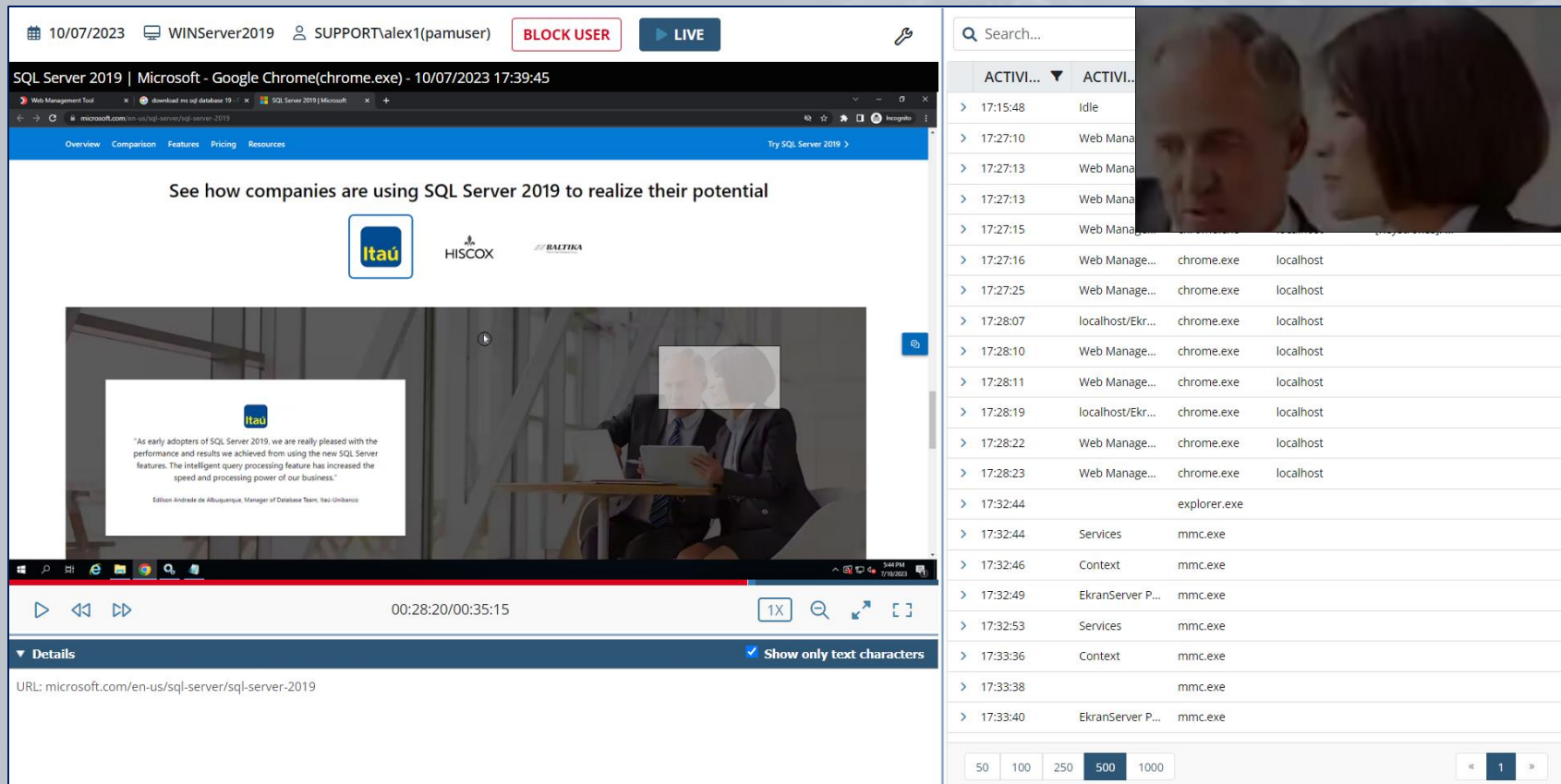
Time	Activity	App	URL	Text Data	Alert/USB R...
19:07:28	Document - Wor...	wordpad.e...			
19:07:36	Document - Wor...	wordpad.e...		[Keystrokes]	david keystrokes alert2
19:07:39	Document - Wor...	wordpad.e...			
19:07:39	Document - Wor...	wordpad.e...		[Clipboard (Copy)]	secret
19:07:47	Program Manager	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	LNBS	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...			
19:08:58	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...			
19:10:03		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).



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

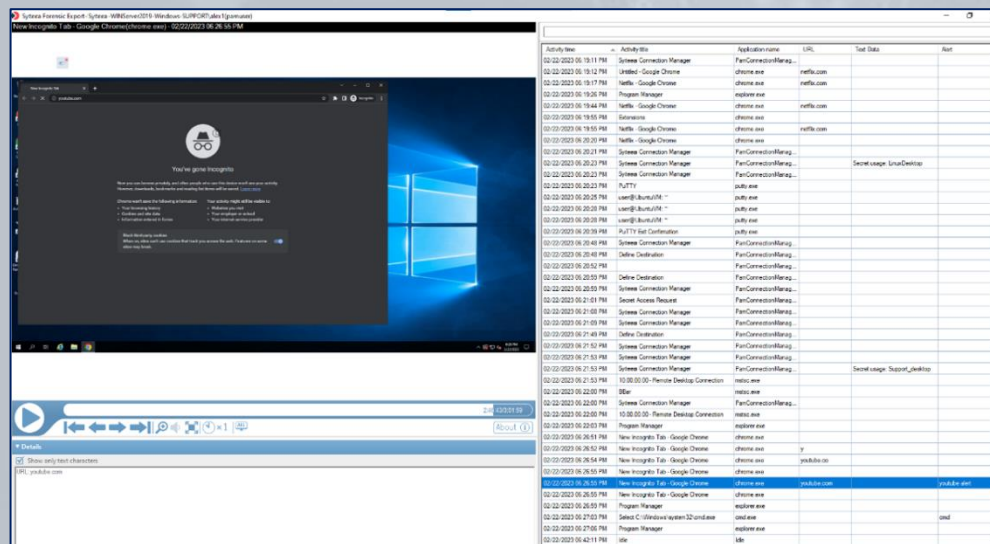


The screenshot displays the Syteca Session Player interface. The main window shows a Microsoft website for SQL Server 2019. A magnifying glass is applied to a video player on the page, showing a testimonial from Edilson Andrade de Albuquerque, Manager of Database Team at Itaú. The video player controls show a timestamp of 00:28:20/00:35:15 and a 1X magnification level. On the right side, there is a search bar and a list of active processes. The process list includes various applications like chrome.exe, mmc.exe, and explorer.exe, along with their parent processes and local host addresses.

Time	Process Name	Parent Process	Local 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	

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.



Anonymizer

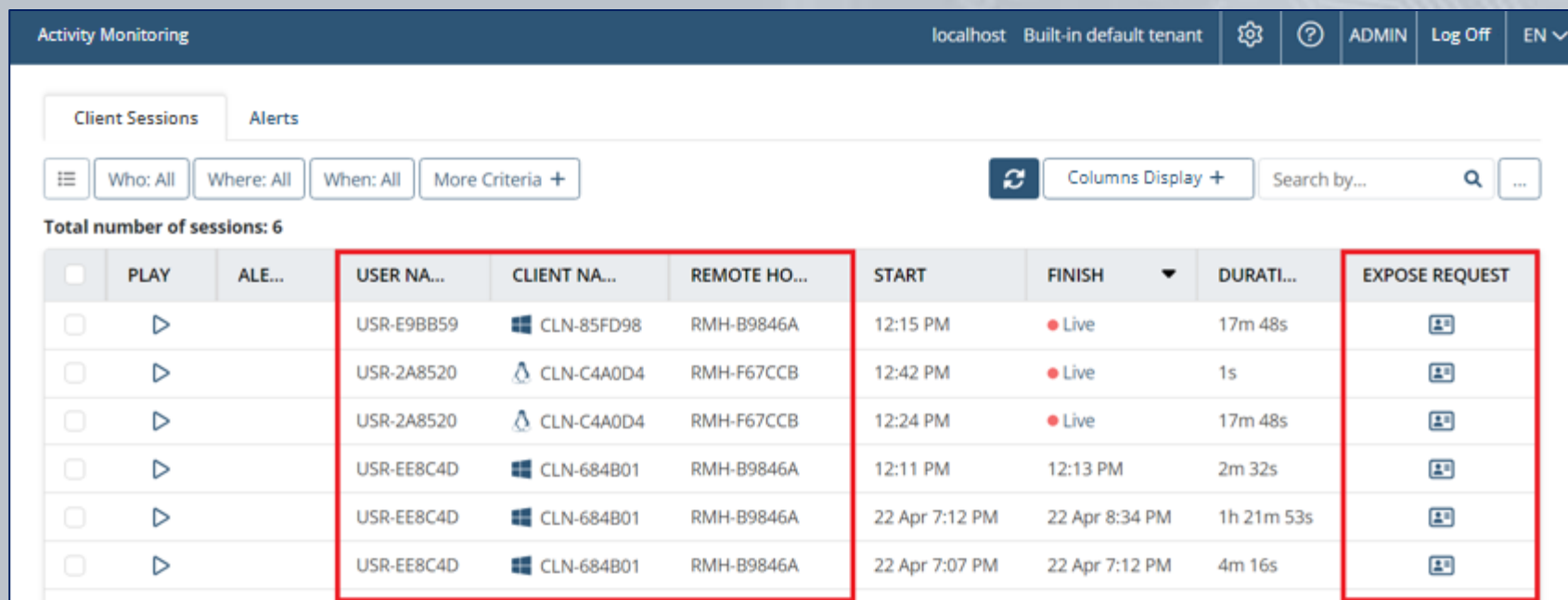
(for GDPR compliance, etc.)

The **Anonymizer** (also known as **Pseudonymizer** or **Monitored Data Anonymization**) feature allows **compliance with data protection and privacy laws**, standards and regulations, such as the European Union's General Data Protection Regulation (**GDPR**) law in relation to protecting personally identifiable information (PII).







PII means any **personal data** that can directly identify an individual person.



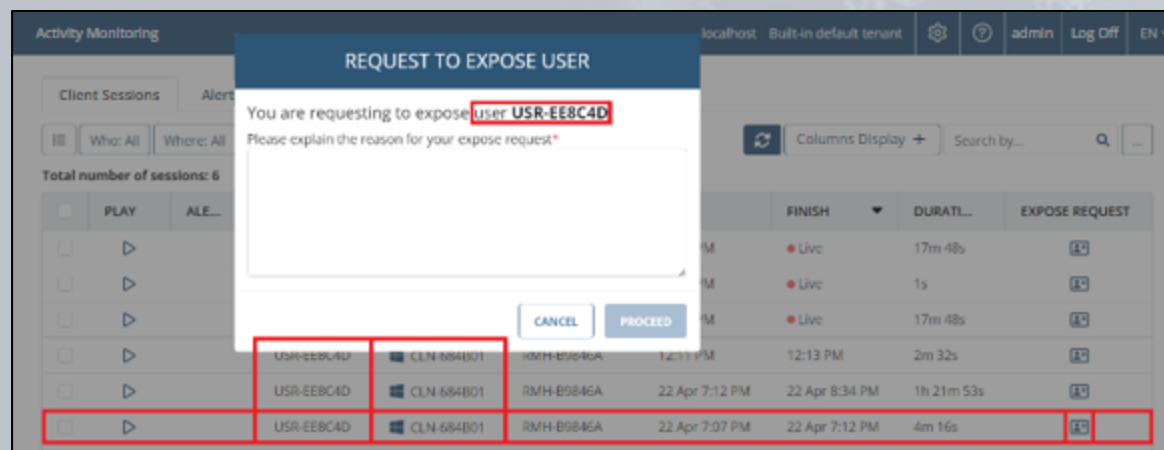
Protection of the **personally identifiable information (PII)** of endpoint users, that is recorded during monitoring of their activities by Syteca, is achieved by the system **pseudonymizing** this data (i.e. hiding and replacing it with **randomized values** when viewed).



The screenshot shows the 'Activity Monitoring' interface. At the top, there's a navigation bar with 'localhost Built-in default tenant', a settings gear, a help icon, 'ADMIN', 'Log Off', and 'EN'. Below this, there are tabs for 'Client Sessions' and 'Alerts'. A search bar contains 'Who: All', 'Where: All', 'When: All', and 'More Criteria +'. To the right, there are buttons for 'Columns Display +', 'Search by...', and a search icon. Below the search bar, it says 'Total number of sessions: 6'. The main table has columns: 'PLAY', 'ALE...', 'USER NA...', 'CLIENT NA...', 'REMOTE HO...', 'START', 'FINISH', 'DURATI...', and 'EXPOSE REQUEST'. The 'USER NA...', 'CLIENT NA...', and 'EXPOSE REQUEST' columns are highlighted with a red border. The 'EXPOSE REQUEST' column contains icons representing user profiles.

	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	

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



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

If an **investigator's request is approved** (by a supervisor) to **de-anonymize** the PII data of a specific endpoint user (on a specific Client computer), **that user's data is temporarily deanonymized for that investigator only to view.**

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

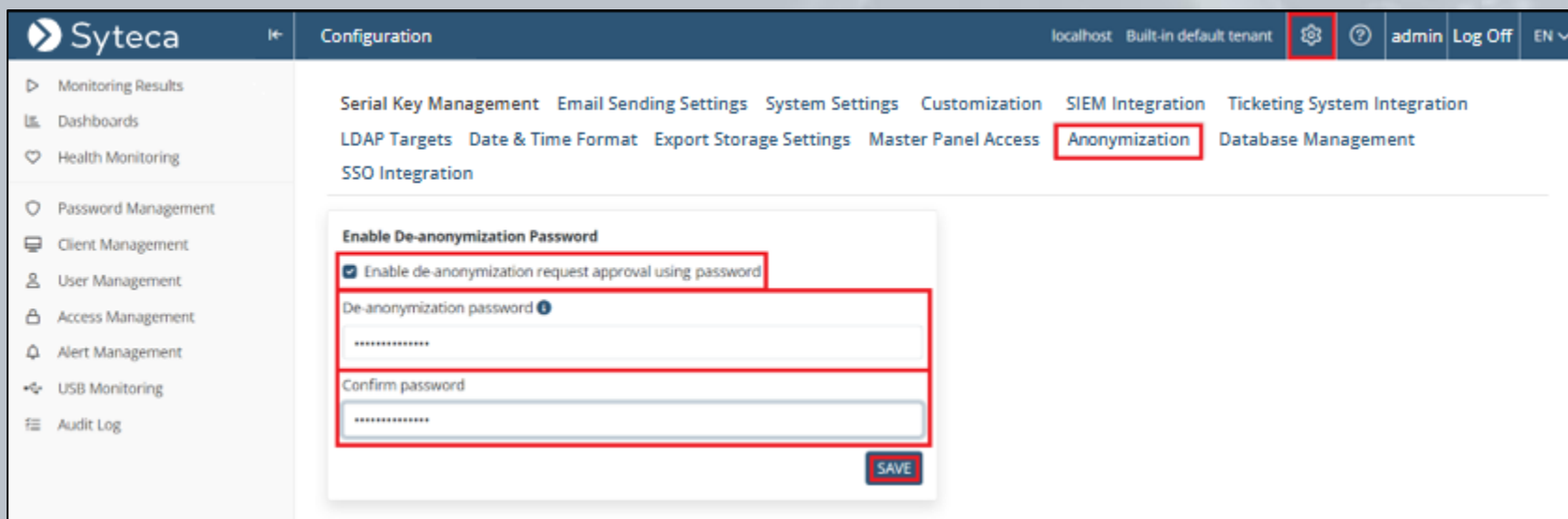
Client Sessions Alerts

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).



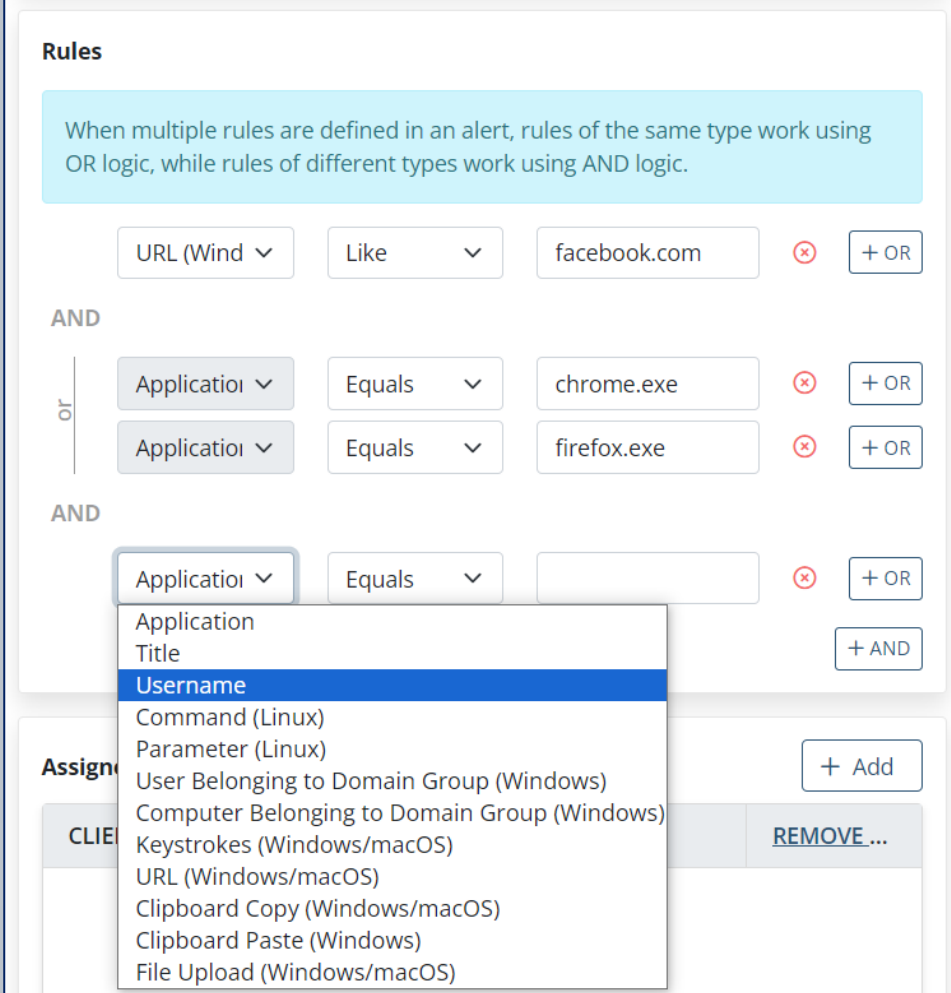
The screenshot shows the Syteca Configuration page. The top navigation bar includes the Syteca logo, a back arrow, the title 'Configuration', and user information: 'localhost Built-in default tenant', a settings gear icon, a help icon, 'admin', 'Log Off', and 'EN'. The left sidebar lists various system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

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

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 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.'

The interface displays a rule configuration with the following elements:

- Rule 1:** 'URL (Wind)' dropdown, 'Like' dropdown, 'facebook.com' text input, a red 'x' icon, and a '+ OR' button.
- AND Logic:** A vertical line with 'AND' text and 'or' text indicates the relationship between rules.
- Rule 2:** 'Application' dropdown, 'Equals' dropdown, 'chrome.exe' text input, a red 'x' icon, and a '+ OR' button.
- Rule 3:** 'Application' dropdown, 'Equals' dropdown, 'firefox.exe' text input, a red 'x' icon, and a '+ OR' button.
- Rule 4:** 'Application' dropdown, 'Equals' dropdown, an empty text input, a red 'x' icon, and a '+ OR' button.
- Buttons:** '+ AND' and '+ Add' buttons are visible at the bottom right.
- Dropdown Menu:** A dropdown menu is open for the 'Application' dropdown in Rule 4, showing the following options: Application, Title, Username (highlighted in blue), 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).
- Other Elements:** 'Assign' and 'CLIENT' labels are partially visible on the left, and a 'REMOVE...' button is visible on the right.

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 Client computers.

Rules

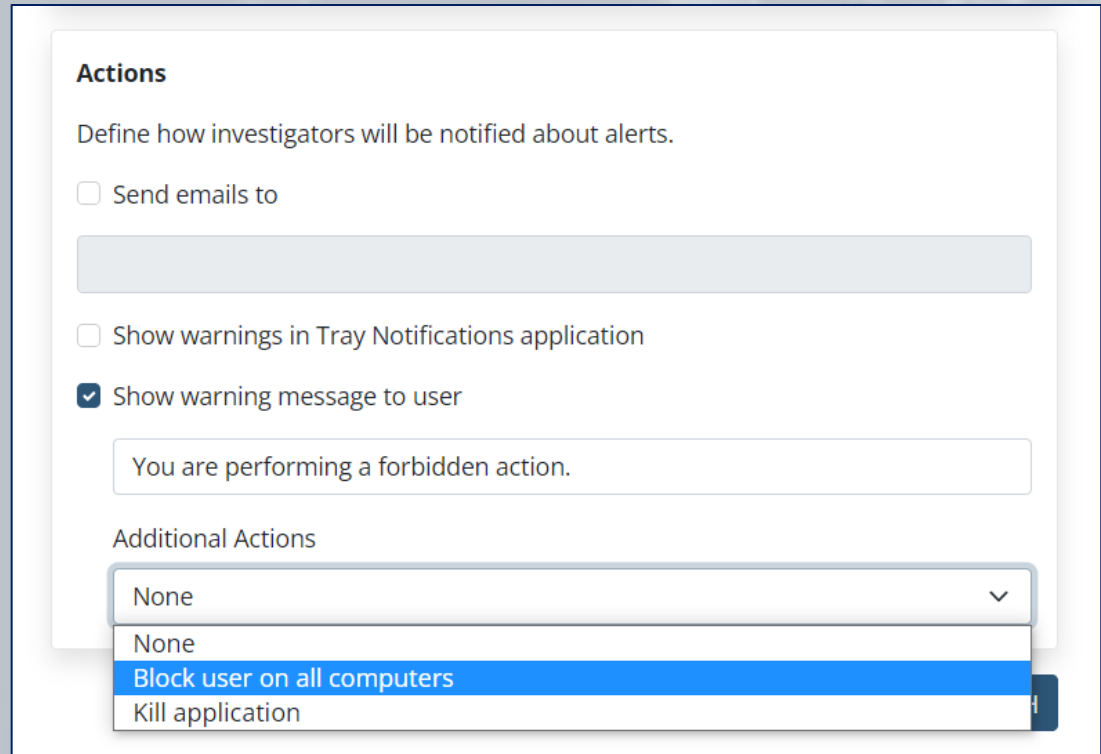
When multiple rules are defined in an alert, rules of the same type work using OR logic, while rules of different types work using AND logic.

	Application	Matches (Regex)	\b(chrome safari edge firefox)\b	✕	+ OR
AND	Clipboard Paste (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).

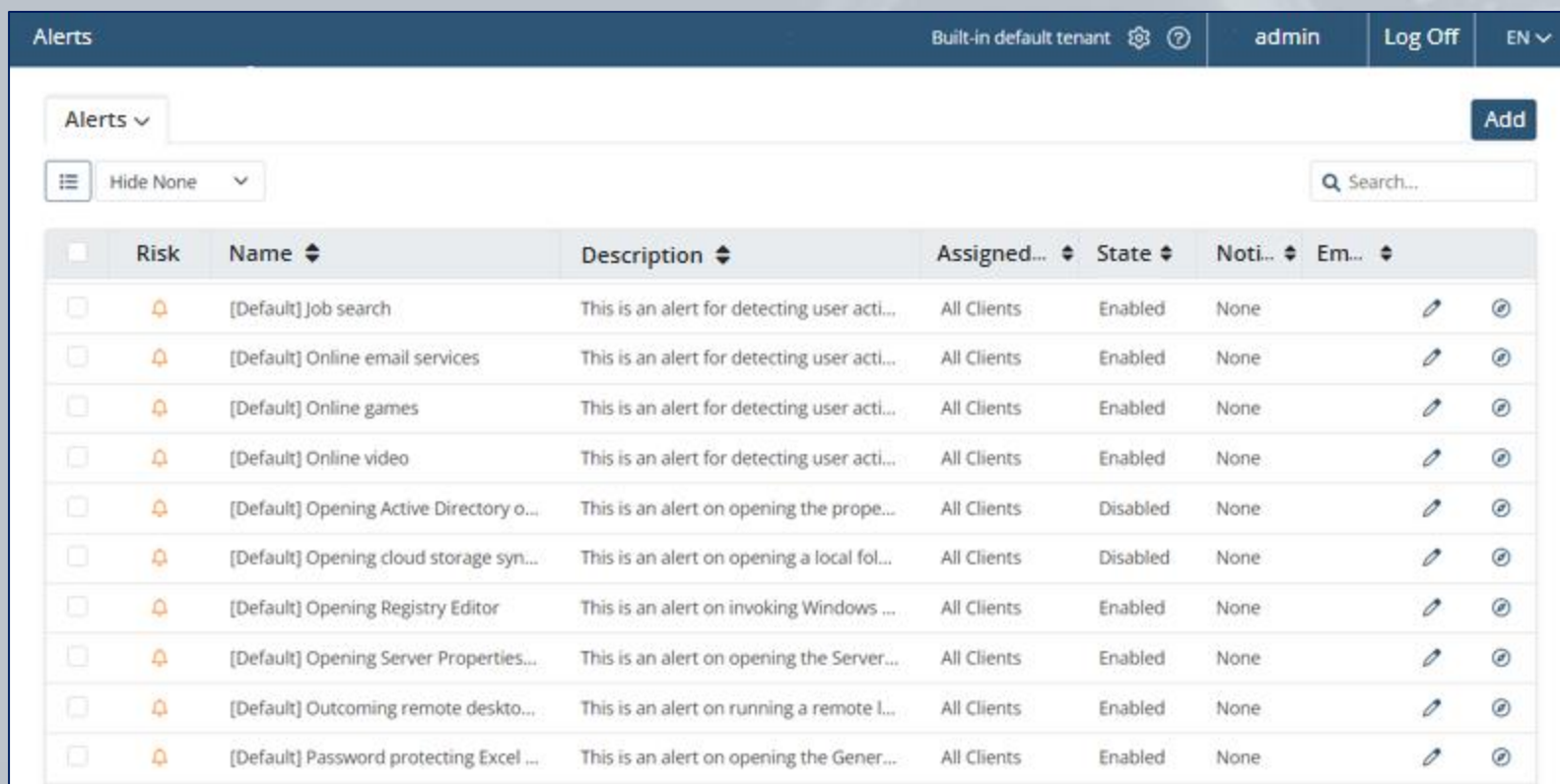
You can also set an alert to:

- 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 a configuration window titled "Actions" with the subtitle "Define how investigators will be notified about alerts." It contains three checkboxes: "Send emails to" (unchecked), "Show warnings in Tray Notifications application" (unchecked), and "Show warning message to user" (checked). Below the checked option is a text input field containing "You are performing a forbidden action." Underneath is a section titled "Additional Actions" with a dropdown menu. The dropdown is open, showing four options: "None", "None", "Block user on all computers" (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.

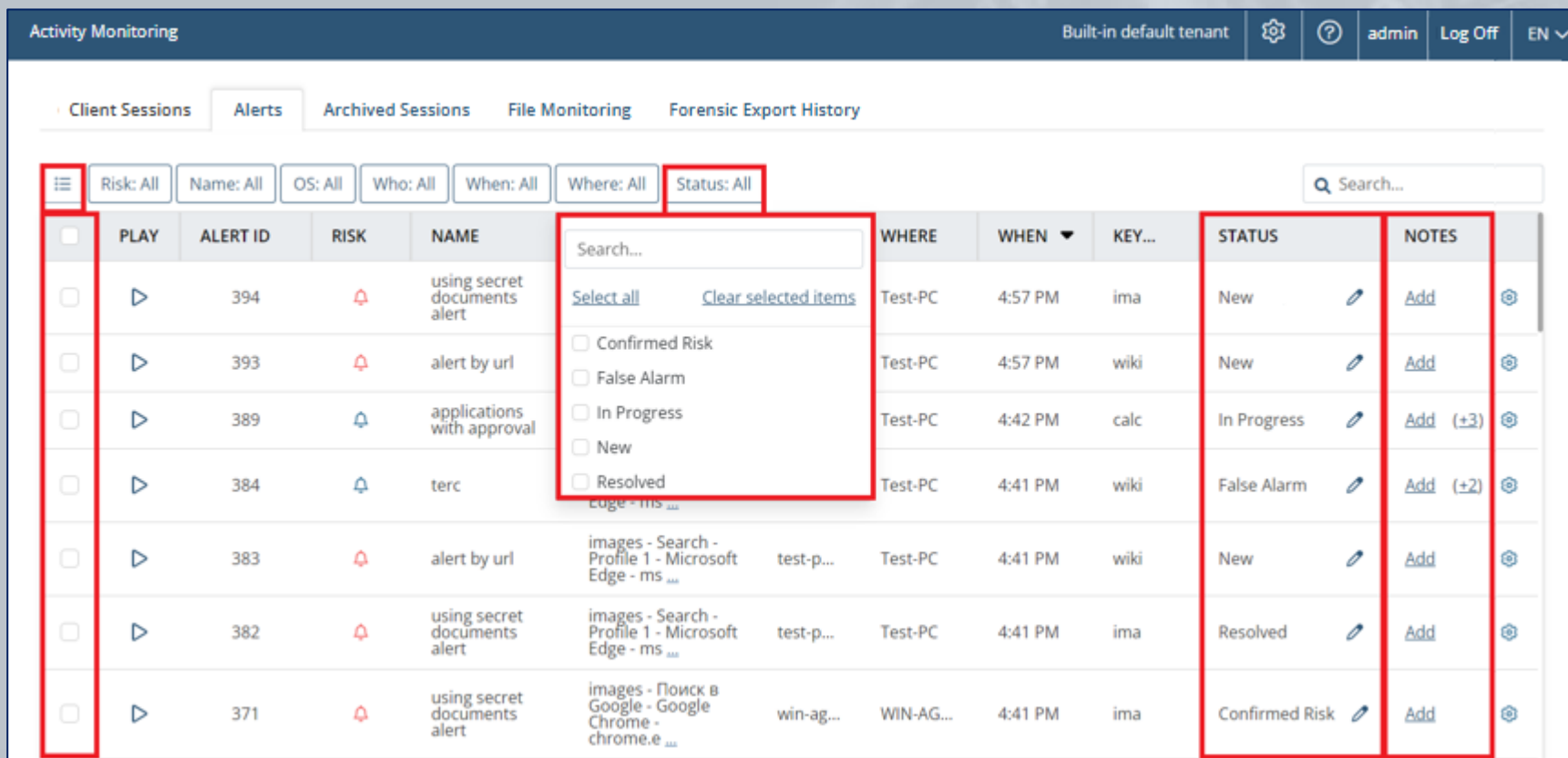


The screenshot shows the 'Alerts' management page in the Syteca interface. The page header includes 'Alerts', 'Built-in default tenant', 'admin', 'Log Off', and 'EN'. Below the header, there is a search bar and a table of alerts. The table has columns for Risk, Name, Description, Assigned..., State, Noti..., and Em... Each row represents a default alert with a checkbox, a bell icon, and edit/delete icons.

<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

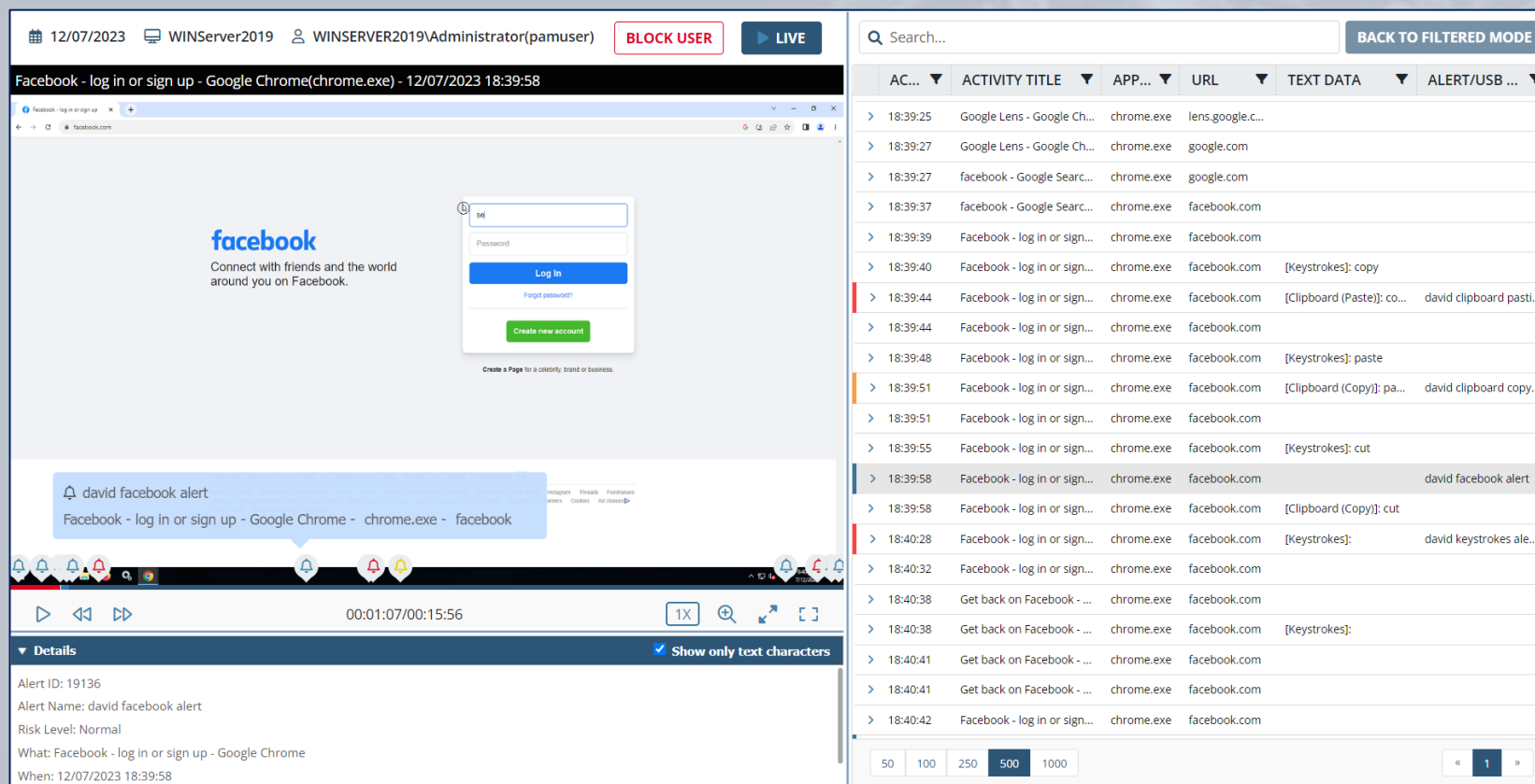
Client Sessions Alerts Archived Sessions File Monitoring Forensic Export History

Risk: All Name: All OS: All Who: All When: All Where: All Status: All Search...

	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

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 Session Viewer interface. The top bar shows the date (12/07/2023), system name (WINServer2019), user (WINSERVER2019\Administrator(pamuser)), and buttons for 'BLOCK USER' and 'LIVE'. The main window shows a Facebook login page with a search bar containing 'david'. A blue alert notification is overlaid on the page, stating 'david facebook alert' and 'Facebook - log in or sign up - Google Chrome - chrome.exe - facebook'. The bottom of the window shows a playback control bar with a timestamp of 00:01:07/00:15:56 and a 'Details' section.

The 'Details' section contains the following information:

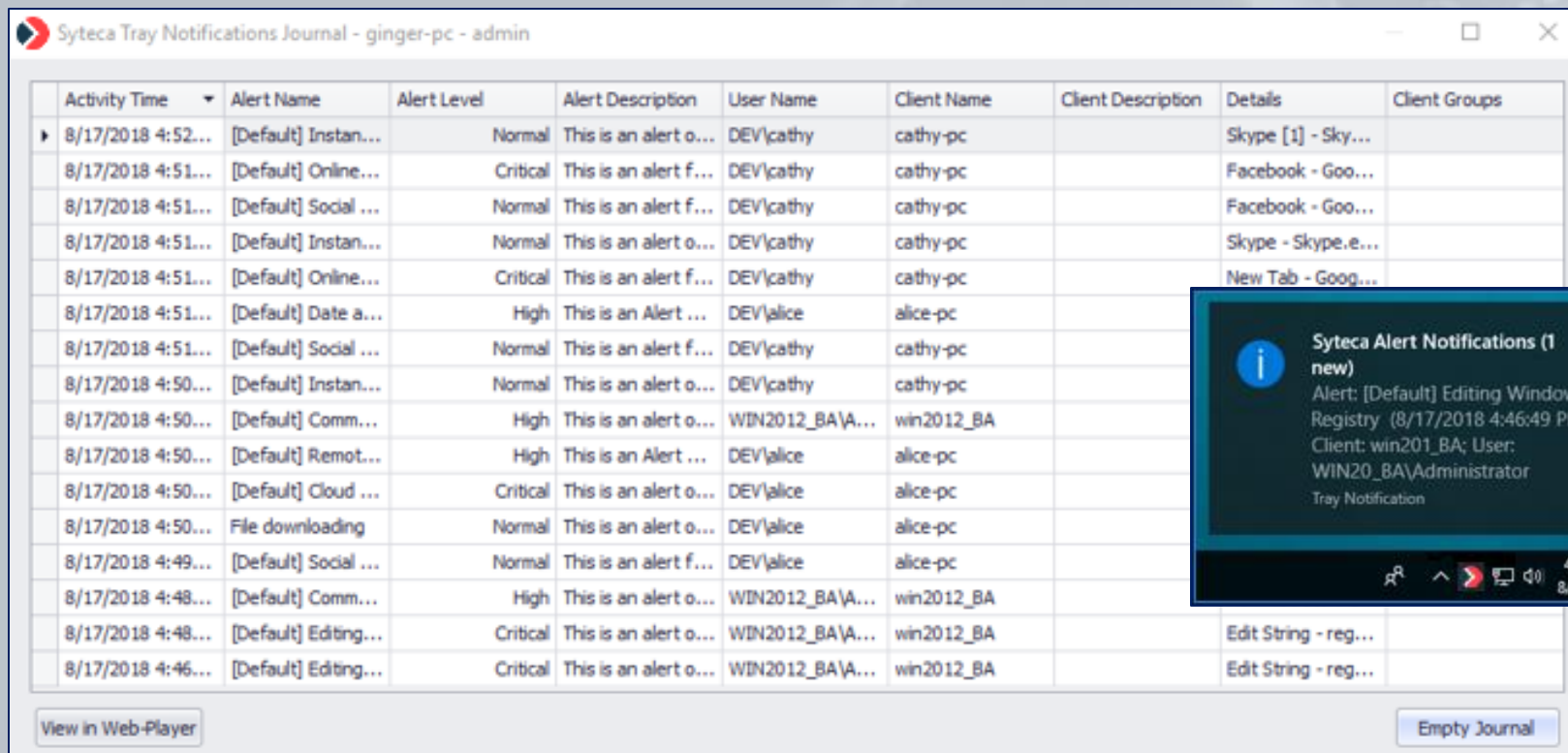
- Alert ID: 19136
- Alert Name: david facebook alert
- Risk Level: Normal
- What: Facebook - log in or sign up - Google Chrome
- When: 12/07/2023 18:39:58

On the right side, there is a table of alert events. The table has columns for 'AC...', 'ACTIVITY TITLE', 'APP...', 'URL', 'TEXT DATA', and 'ALERT/USB ...'. The events are listed with timestamps and details. The event at 18:39:58 is highlighted in blue, corresponding to the alert shown in the main window.

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 Sear...	chrome.exe	google.com	
>	18:39:37	facebook - Google Sear...	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. It contains a table with the following columns: Activity Time, Alert Name, Alert Level, Alert Description, User Name, Client Name, Client Description, Details, and Client Groups. The table lists various alerts from 8/17/2018 4:46 to 4:52. A tray notification popup is visible in the bottom right corner, showing a new alert: 'Alert: [Default] Editing Windows Registry (8/17/2018 4:46:49 PM) Client: win201_BA; User: WIN20_BA\Administrator'. The popup also includes a 'Tray Notification' label and a notification icon in the system tray.

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] Edting...	Critical	This is an alert o...	WIN2012_BA\A...	win2012_BA		Edit String - reg...	

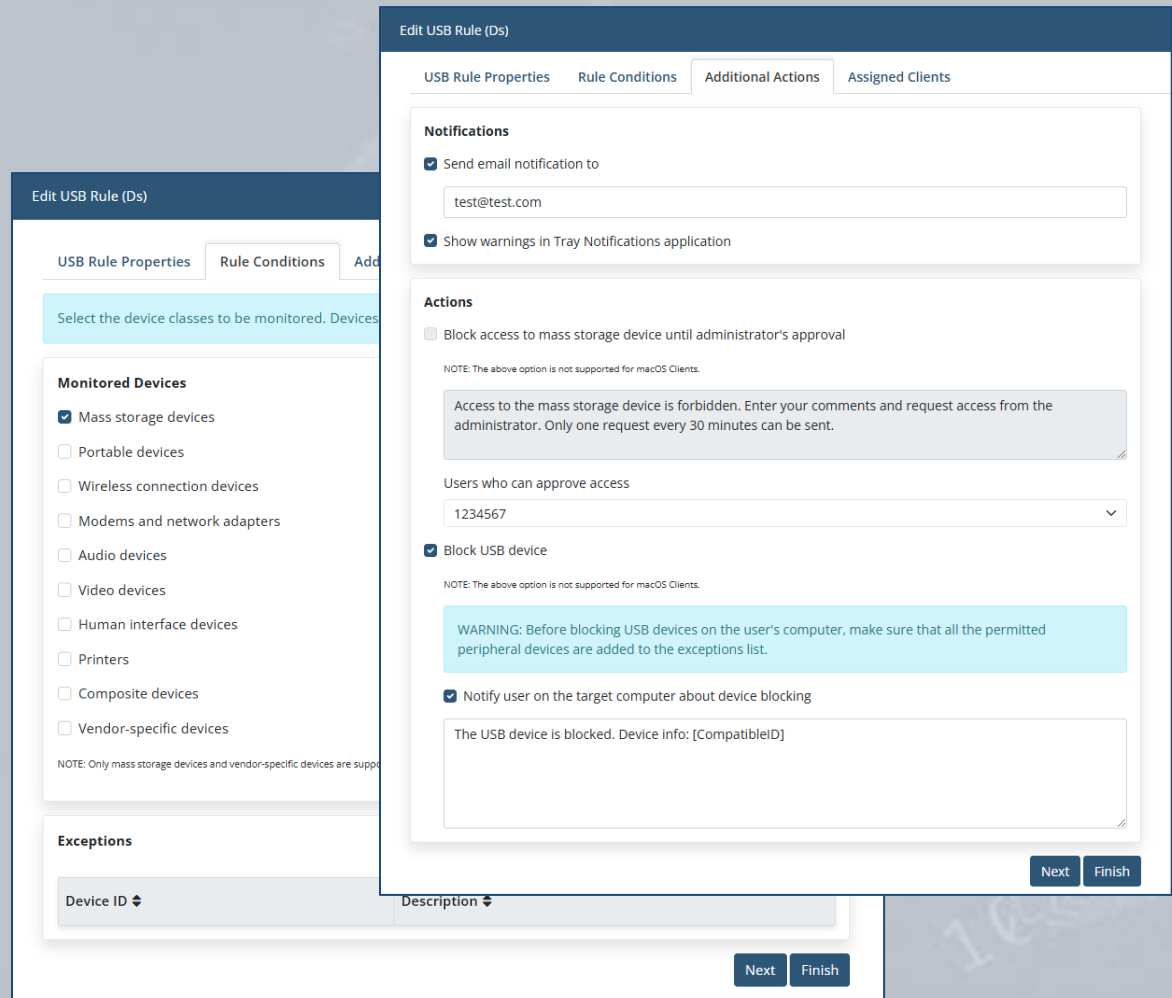
USB Device Monitoring

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.



Edit USB Rule (Ds)

USB Rule Properties | Rule Conditions | Additional Actions | Assigned Clients

Select the device classes to be monitored. Devices

Monitored Devices

- Mass storage devices
- Portable devices
- Wireless connection devices
- Modems and network adapters
- Audio devices
- Video devices
- Human interface devices
- Printers
- Composite devices
- Vendor-specific devices

NOTE: Only mass storage devices and vendor-specific devices are supported.

Exceptions

Device ID	Description

Notifications

- Send email notification to
test@test.com
- Show warnings in Tray Notifications application

Actions

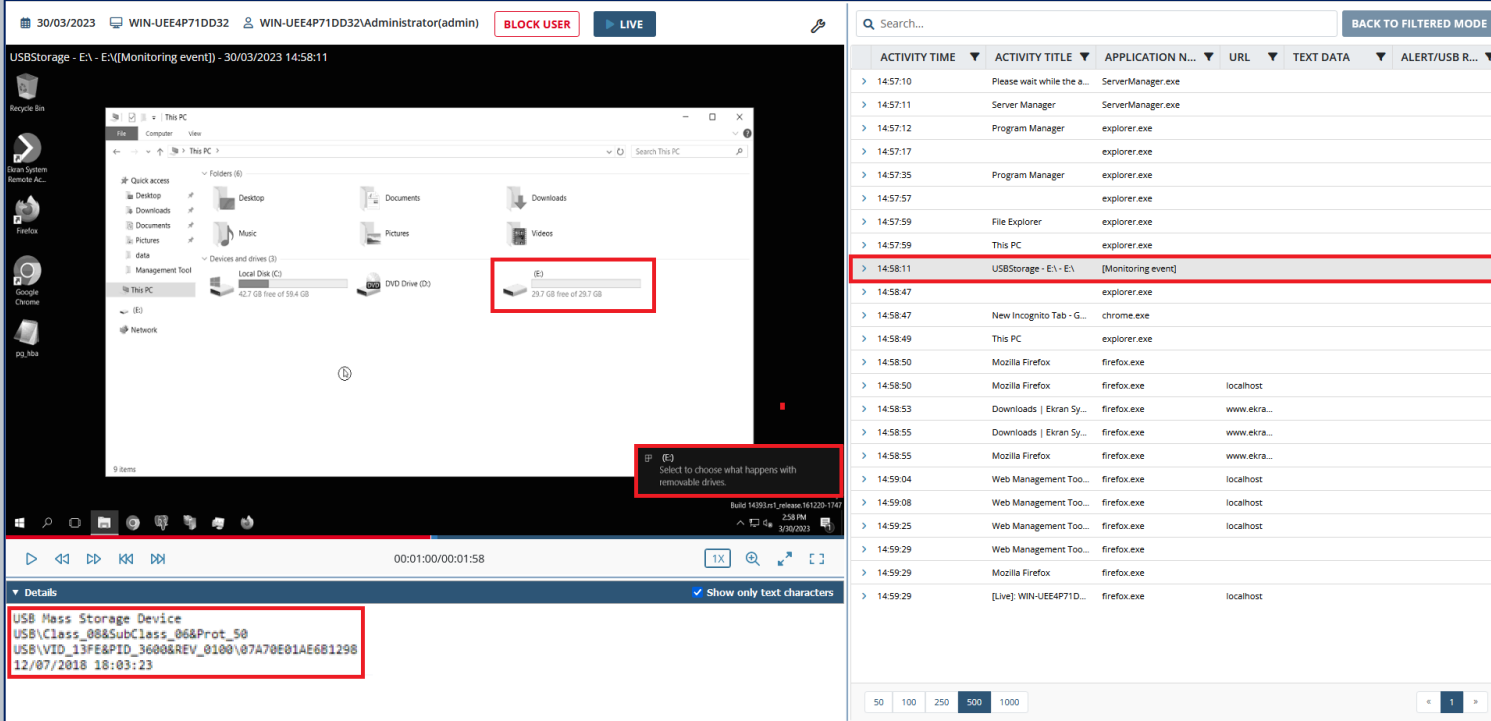
- Block access to mass storage device until administrator's approval
NOTE: The above option is not supported for macOS Clients.
Access to the mass storage device is forbidden. Enter your comments and request access from the administrator. Only one request every 30 minutes can be sent.
Users who can approve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

Next Finish

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.



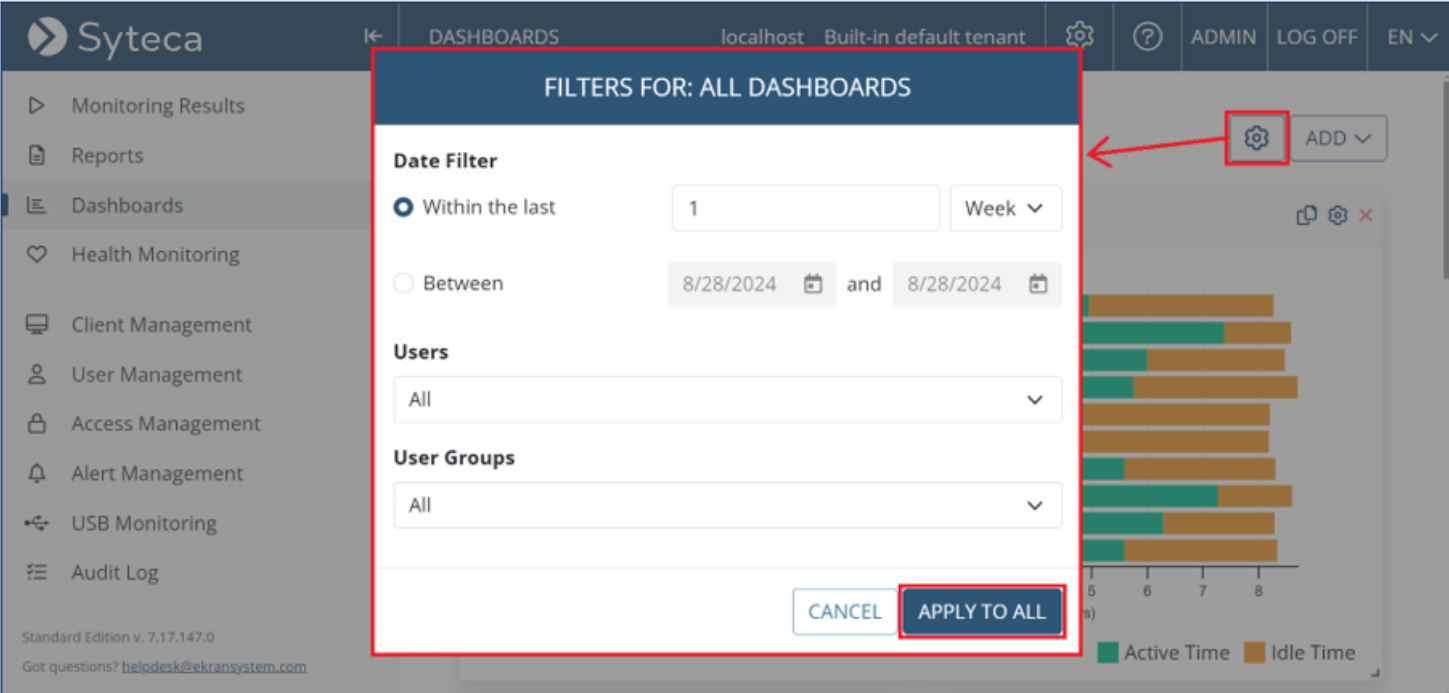
The screenshot displays the Syteca Session Viewer interface. At the top, it shows the session ID '30/03/2023 WIN-UEE4P71DD32' and the user 'WIN-UEE4P71DD32\Administrator(admin)'. A red 'BLOCK USER' button and a blue 'LIVE' button are visible. The main window is split into two panes. The left pane shows a Windows File Explorer window titled 'USBStorage - E:\ - EV((Monitoring event)) - 30/03/2023 14:58:11'. The File Explorer shows the 'This PC' view with a red box highlighting the 'E:' drive, which is labeled '29.7 GB free of 29.7 GB'. A tooltip for the 'E:' drive is visible, stating 'Select to choose what happens with removable drives.' The right pane is an activity log table with columns for 'ACTIVITY TIME', 'ACTIVITY TITLE', 'APPLICATION N...', 'URL', 'TEXT DATA', and 'ALERT/USB R...'. The log shows various system events, with the entry at 14:58:11, 'USBStorage - E:\ - EV', '[Monitoring event]', highlighted in red. Below the log, a 'Details' pane shows the following information:

```
USB Mass Storage Device
USB\Class_08&SubClass_06&Prot_50
USB\VID_13FE&PID_3600&REV_0100\07A70E01AE601298
12/07/2018 18:03:23
```

Dashboards

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

Four types of BI (business intelligence) productivity dashboards can be **customized** (on the **Dashboards** page), which contain **statistics on various measures of user productivity** displayed in the form of convenient, interactive and individually-customizable charts.

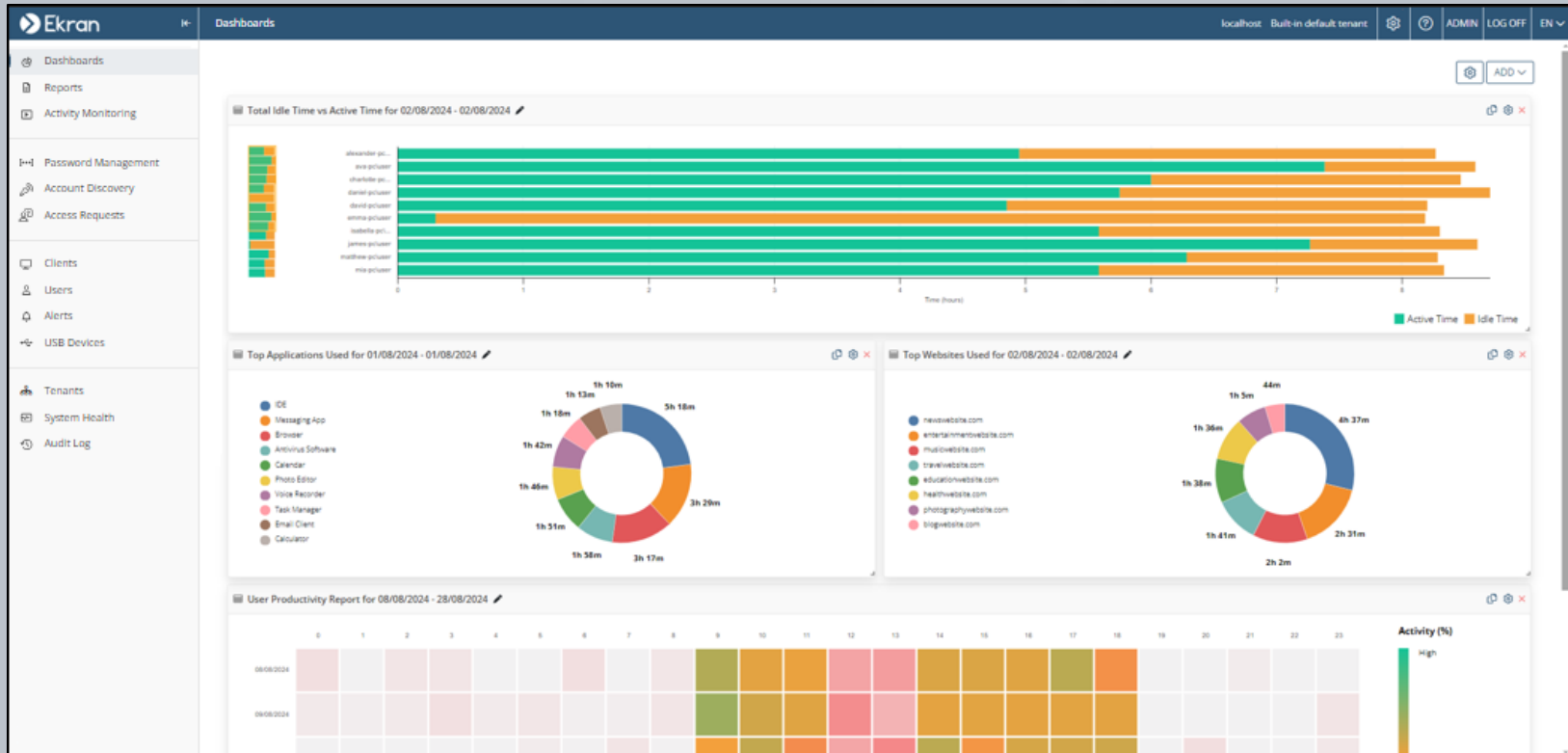


The screenshot displays the Syteca Dashboards interface. A modal window titled "FILTERS FOR: ALL DASHBOARDS" is overlaid on the dashboard content. The modal contains the following sections:

- Date Filter:** Includes radio buttons for "Within the last" (selected) and "Between". The "Within the last" section has a text input field with "1" and a dropdown menu set to "Week". The "Between" section has two date pickers, both showing "8/28/2024".
- Users:** A dropdown menu currently set to "All".
- User Groups:** A dropdown menu currently set to "All".

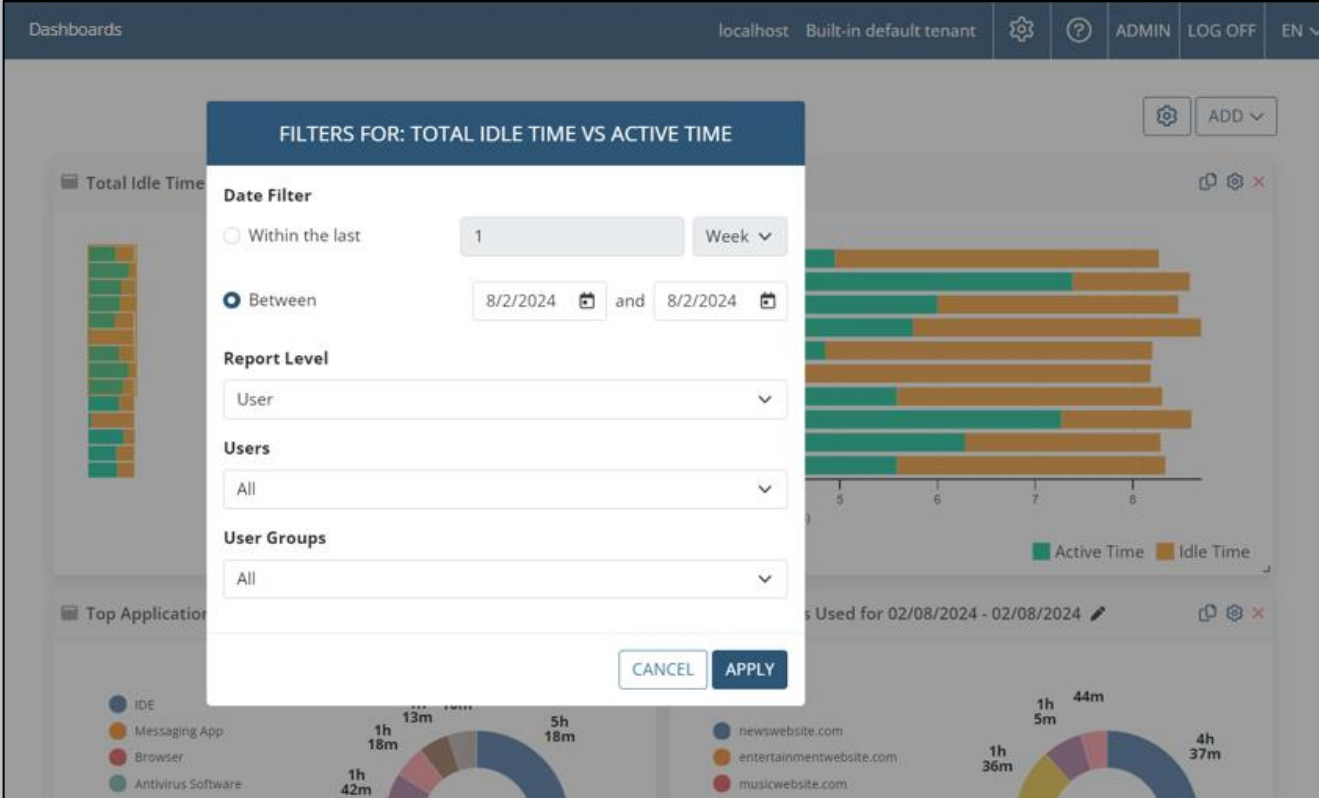
At the bottom of the modal are two buttons: "CANCEL" and "APPLY TO ALL". A red box highlights the "APPLY TO ALL" button. A red arrow points from the "APPLY TO ALL" button to a gear icon in the top right corner of the dashboard, which is also highlighted with a red box. The background dashboard shows a horizontal bar chart with a legend for "Active Time" (green) and "Idle Time" (orange). The chart has an x-axis labeled "1 5 6 7 8" and a y-axis with a label "s)".

Viewing Productivity Dashboards



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

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



The screenshot shows a productivity dashboard interface with a modal window titled "FILTERS FOR: TOTAL IDLE TIME VS ACTIVE TIME". The modal contains the following sections:

- Date Filter:** Two options are shown: "Within the last" (set to 1 Week) and "Between" (set to 8/2/2024 and 8/2/2024).
- Report Level:** A dropdown menu currently set to "User".
- Users:** A dropdown menu currently set to "All".
- User Groups:** A dropdown menu currently set to "All".

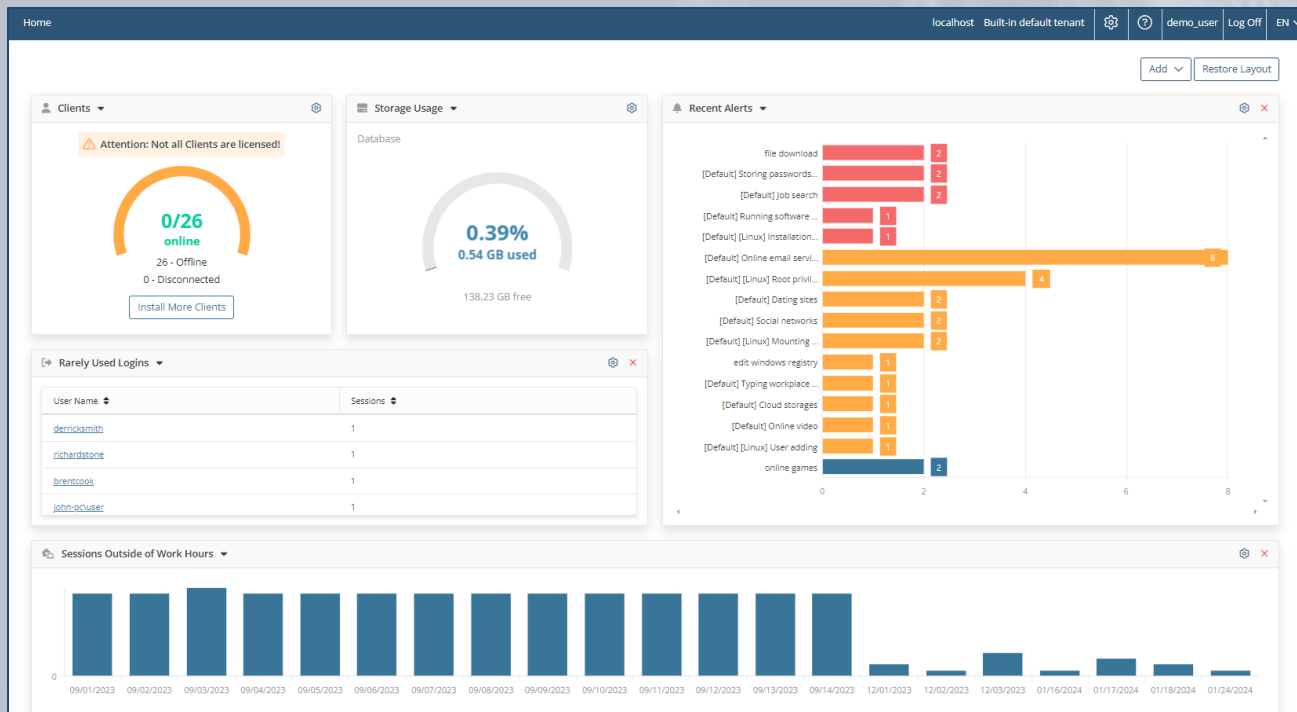
At the bottom of the modal are "CANCEL" and "APPLY" buttons. The background dashboard shows a bar chart for "Total Idle Time" and "Top Application" usage, with a legend for "Active Time" (green) and "Idle Time" (orange).

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**).

The screenshot displays the Syteca interface with several components:

- Session Viewer (Top Right):** A table showing session details for MATTHEW-PCUSER. The table has columns for PLAY, SESSION START, SESSION FINISH, ACTIVE TIME, and IDLE TIME. Two sessions are listed, both with an active time of 6h 17m. A red arrow points from the 'ACTIVE TIME' column to the 'Session Viewer' window.
- Session List (Middle Left):** A table with columns: PLAY, CLIENT NAME, USER NAME, USER GROUP, SESSION START, and SESSION FINISH. It lists sessions for David-PC and Charlotte-PC. A red box highlights 'BLOGWEBSITE.COM - 44M' and a red arrow points to the 'USER GROUP' column.
- Activity Charts (Bottom Left):** Two donut charts showing activity distribution. The first chart shows activity for various applications like Antivirus Software, To-Do List App, Video Player, PDF Viewer, VPN Client, and Photo Editor. The second chart shows activity for websites like entertainmentwebsite.com, blogwebsite.com, musicwebsite.com, healthwebsite.com, and travelwebsite.com. A red box highlights 'blogwebsite.com' and a red arrow points to the 'Session Viewer' window.
- Activity Heatmap (Bottom Right):** A heatmap titled 'Report for 01/08/2024 - 28/08/2024' showing activity levels over time. The x-axis represents hours (2-23) and the y-axis represents dates from 07/08/2024 to 13/08/2024. A legend indicates activity levels: High (green), Normal (yellow), and None (pink). A tooltip shows 'Active time: 37 minute(s)'. A red arrow points from the 'Session Viewer' window to the heatmap.

Other dashboards (on the **Home** and **System Health** pages) also offer a **convenient real-time view** of the **most useful data** grouped together in **one place**, and can be **customized** by adjusting their **appearance and settings**.



Apart from productivity dashboards (on the **Dashboards** page), there are also **four main types** of Syteca dashboards (on the **Home** and **System Health** pages):

System State Dashboards:

- Licenses
- Clients
- Database Storage Usage

Threat Detection Dashboards:

- Sessions Outside of Work Hours
- Rarely Used Computers
- Rarely Used Logins

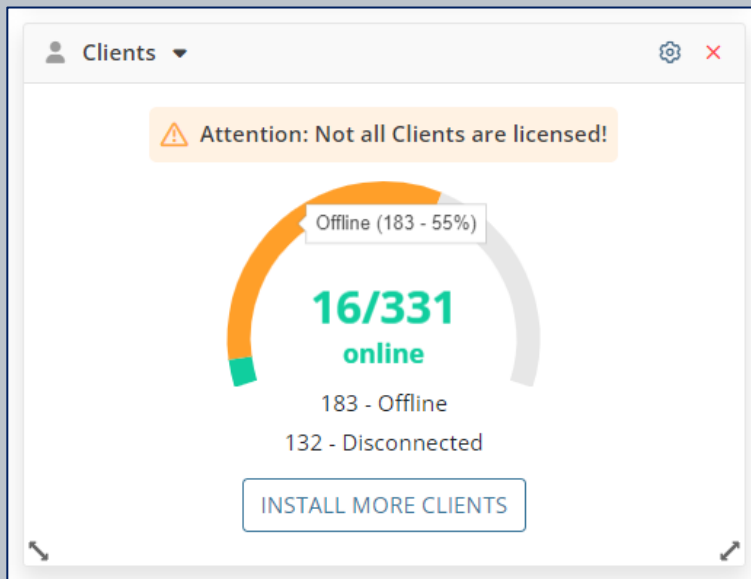
Monitoring Dashboards:

- Recent Alerts
- Latest Live Sessions

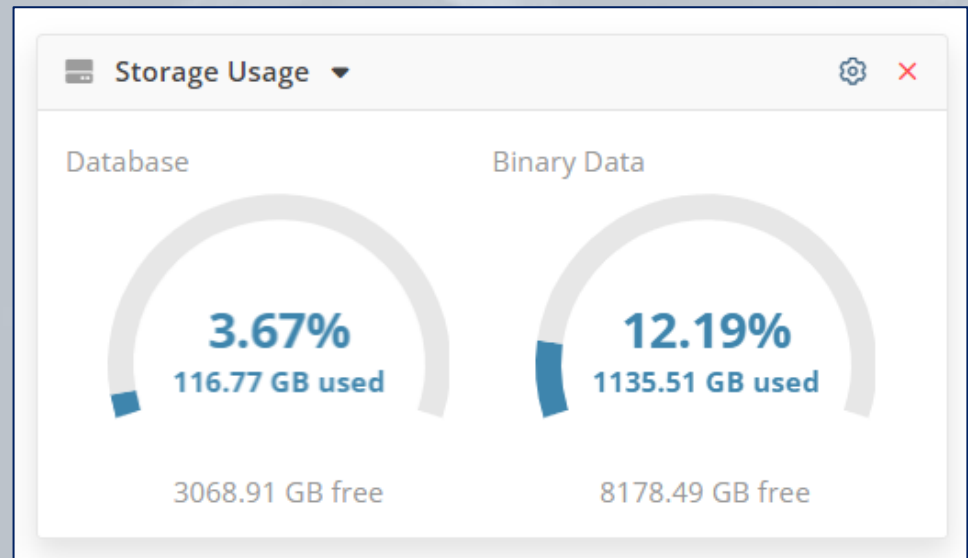
Server Resource Monitoring Dashboards:

- CPU Usage
- Memory Usage
- Database State

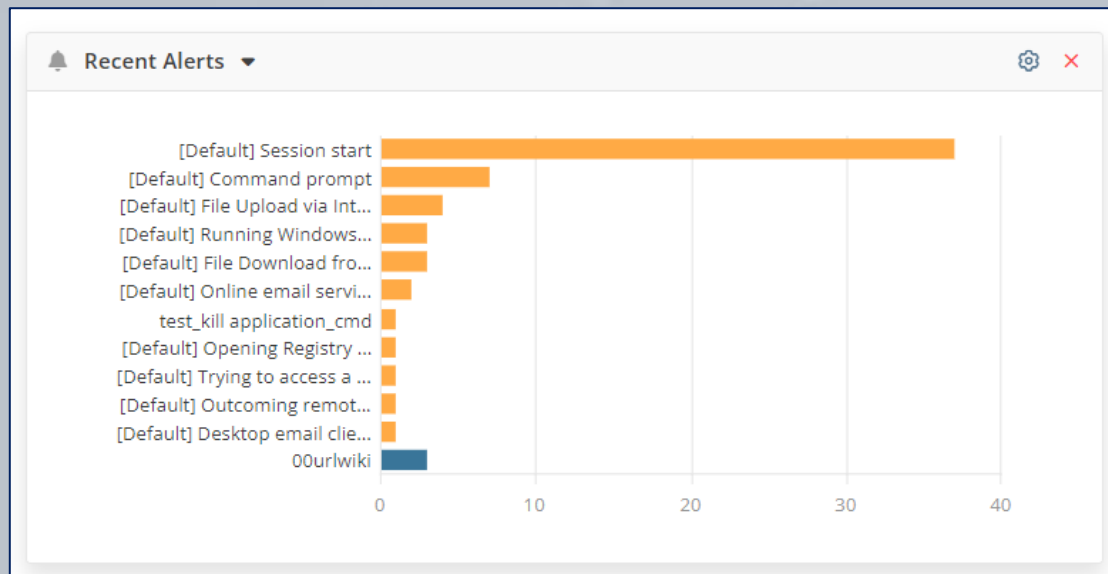
Clients



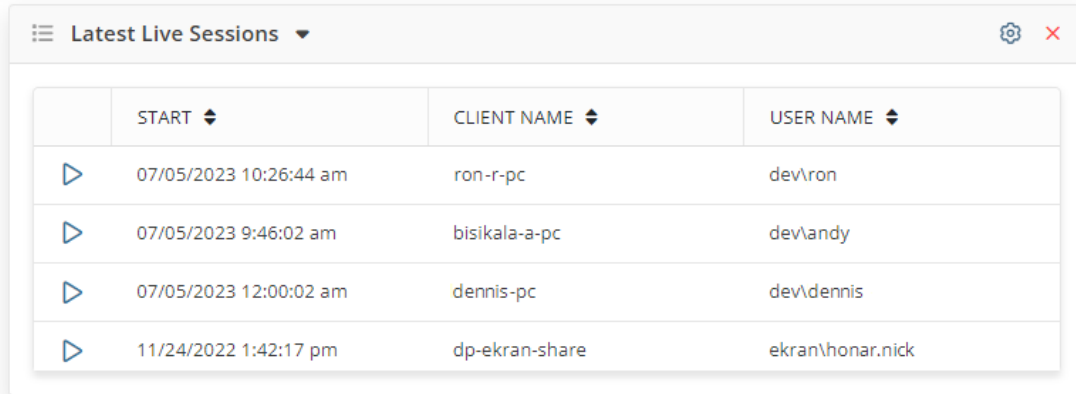
Storage Usage



Recent Alerts



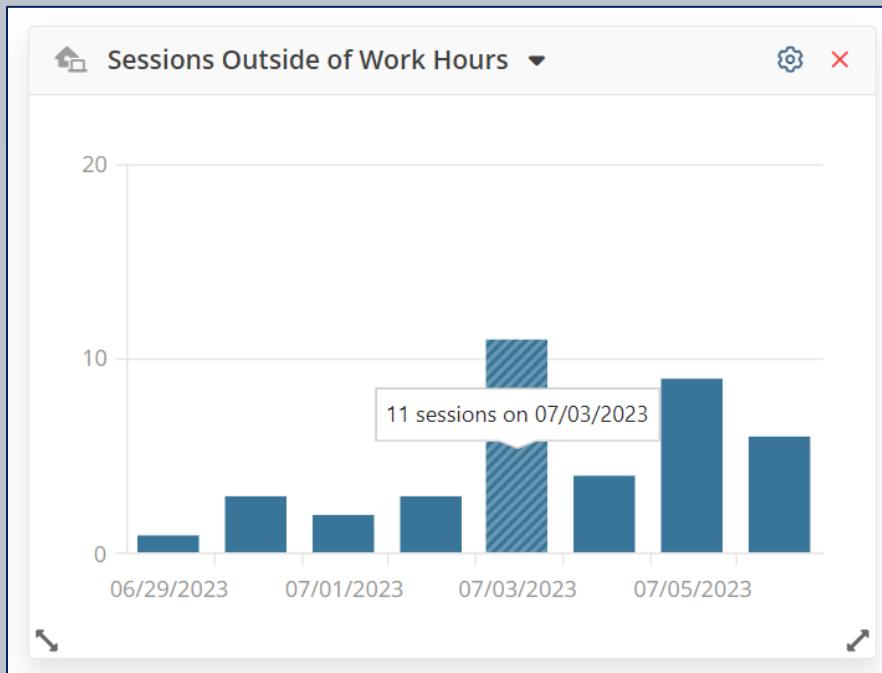
Latest Live Sessions



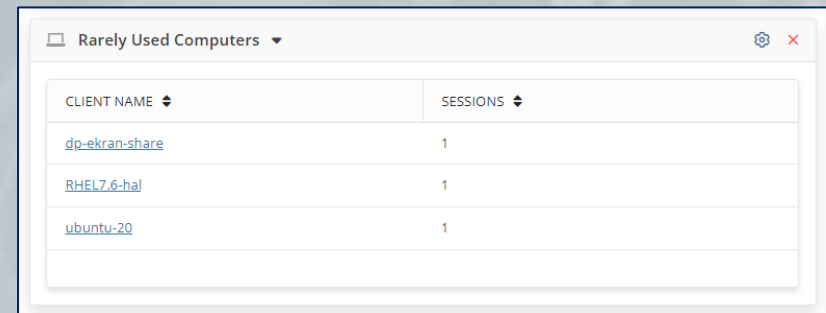
The 'Latest Live Sessions' dashboard displays a table with the following data:

	START	CLIENT NAME	USER NAME
▶	07/05/2023 10:26:44 am	ron-r-pc	dev\ron
▶	07/05/2023 9:46:02 am	bisikala-a-pc	dev\andy
▶	07/05/2023 12:00:02 am	dennis-pc	dev\dennis
▶	11/24/2022 1:42:17 pm	dp-ekran-share	ekran\honar.nick

Sessions Outside of Work Hours



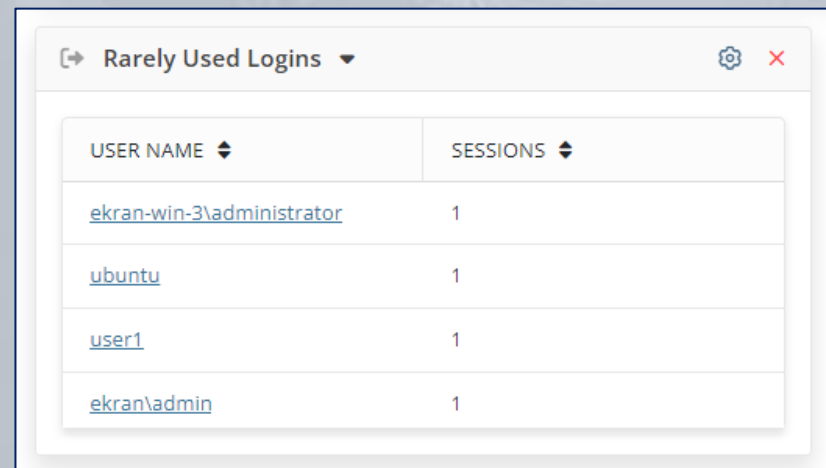
Rarely Used Logins



A screenshot of a dashboard titled "Rarely Used Computers". It displays a table with two columns: "CLIENT NAME" and "SESSIONS".

CLIENT NAME	SESSIONS
dp-ekran-share	1
RHEL7.6-hal	1
ubuntu-20	1

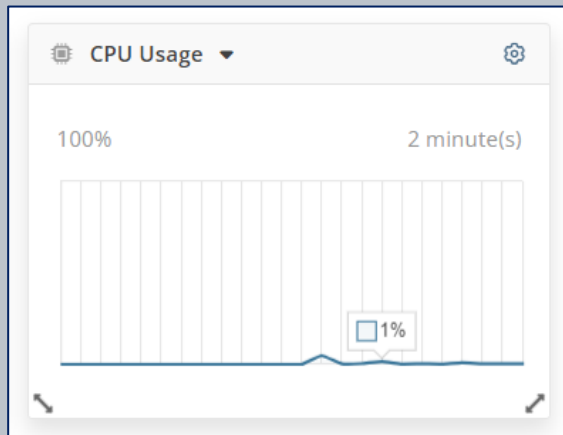
Rarely Used Computers



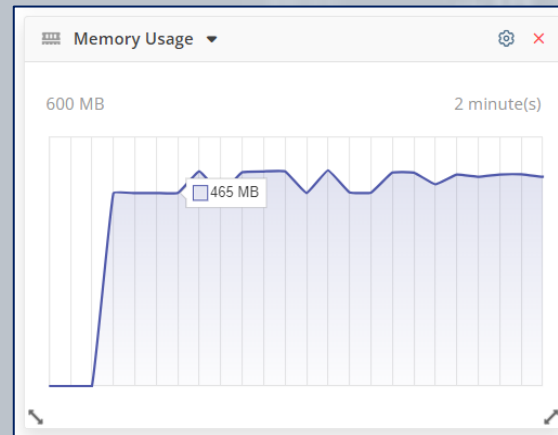
A screenshot of a dashboard titled "Rarely Used Logins". It displays a table with two columns: "USER NAME" and "SESSIONS".

USER NAME	SESSIONS
ekran-win-3\administrator	1
ubuntu	1
user1	1
ekran\admin	1

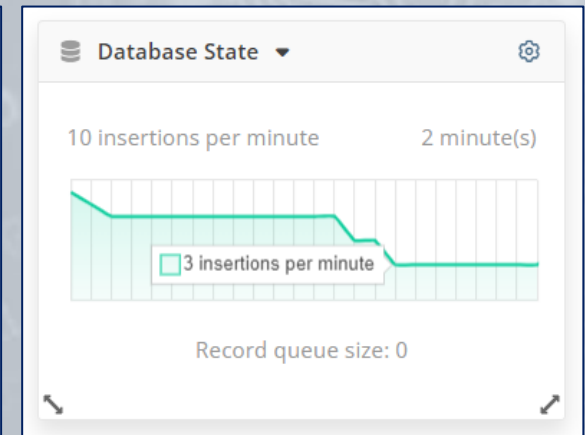
CPU Usage



Memory Usage



Database State

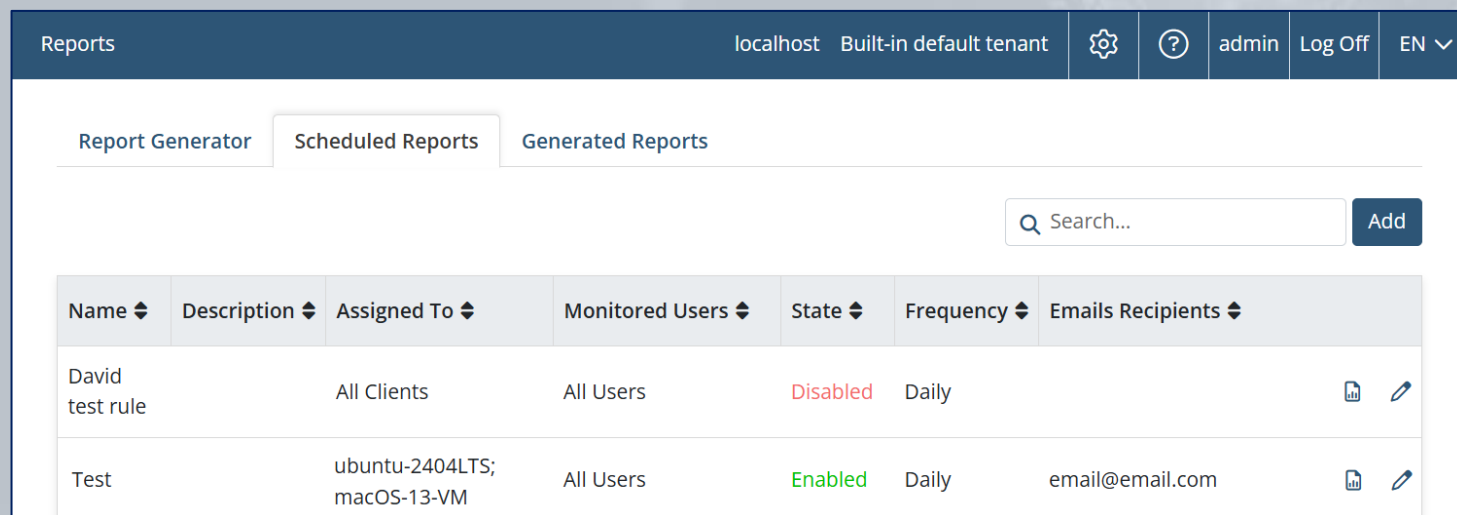


Reports

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**.

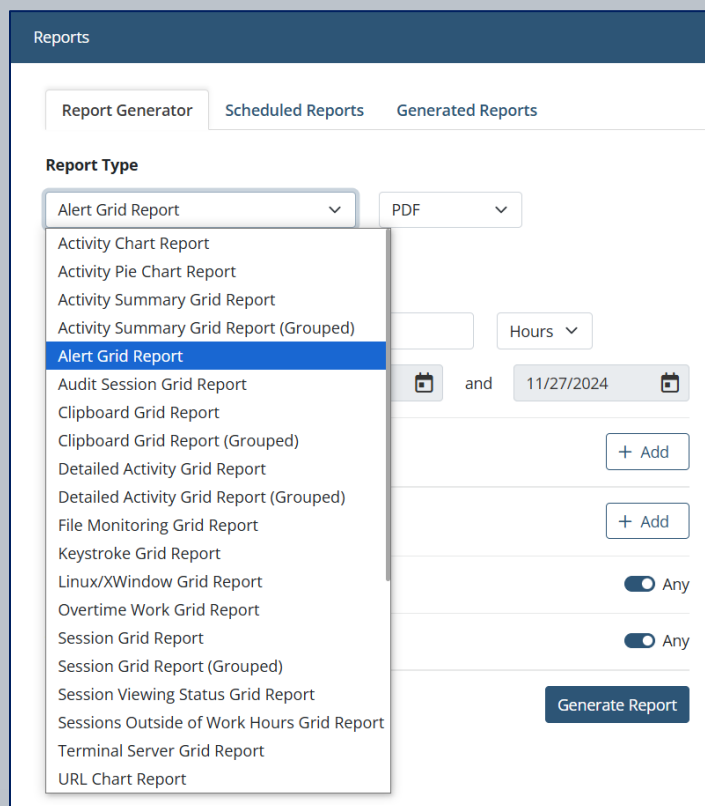
Scheduled Reports



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

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

Manual Report Generation



Reports

Report Generator | Scheduled Reports | Generated Reports

Report Type

Alert Grid Report (selected) | 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)

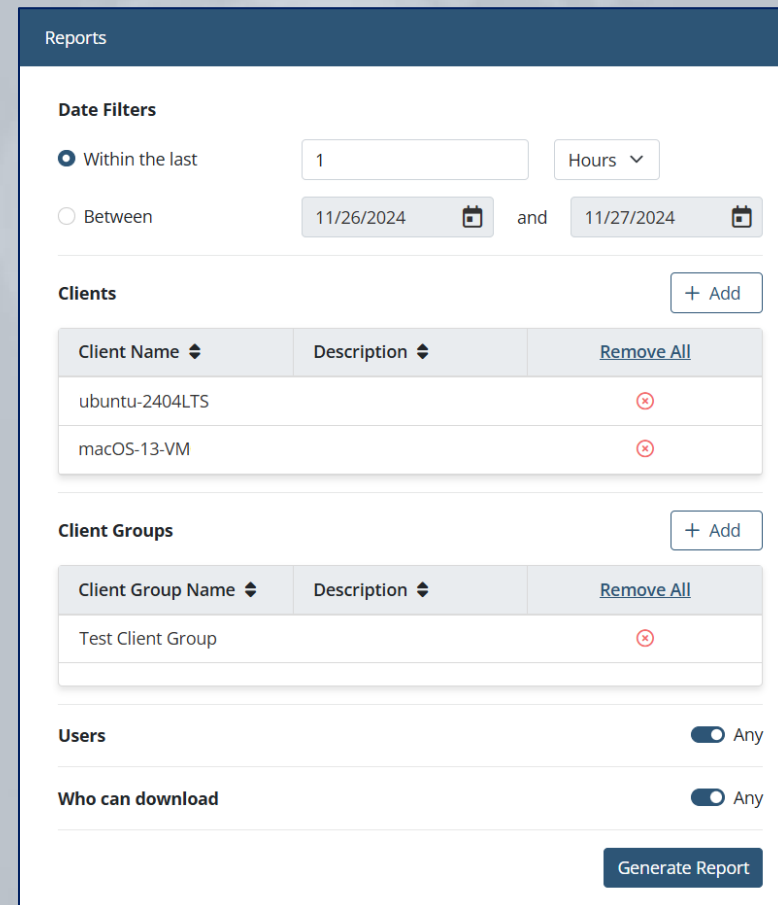
Session Viewing Status Grid Report

Sessions Outside of Work Hours Grid Report

Terminal Server Grid Report

URL Chart Report

Generate Report



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

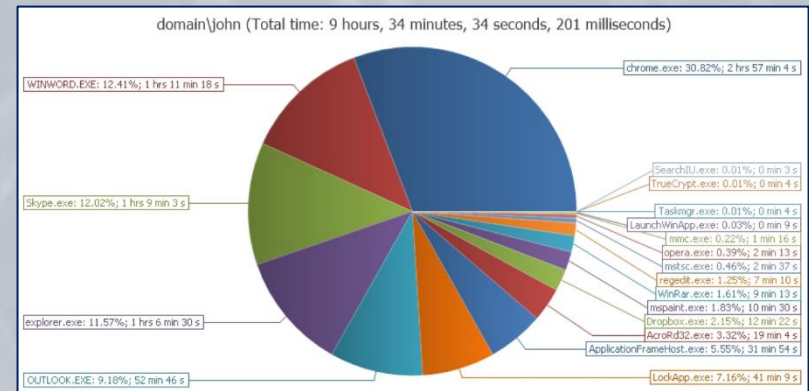
Who can download | Any

Generate Report

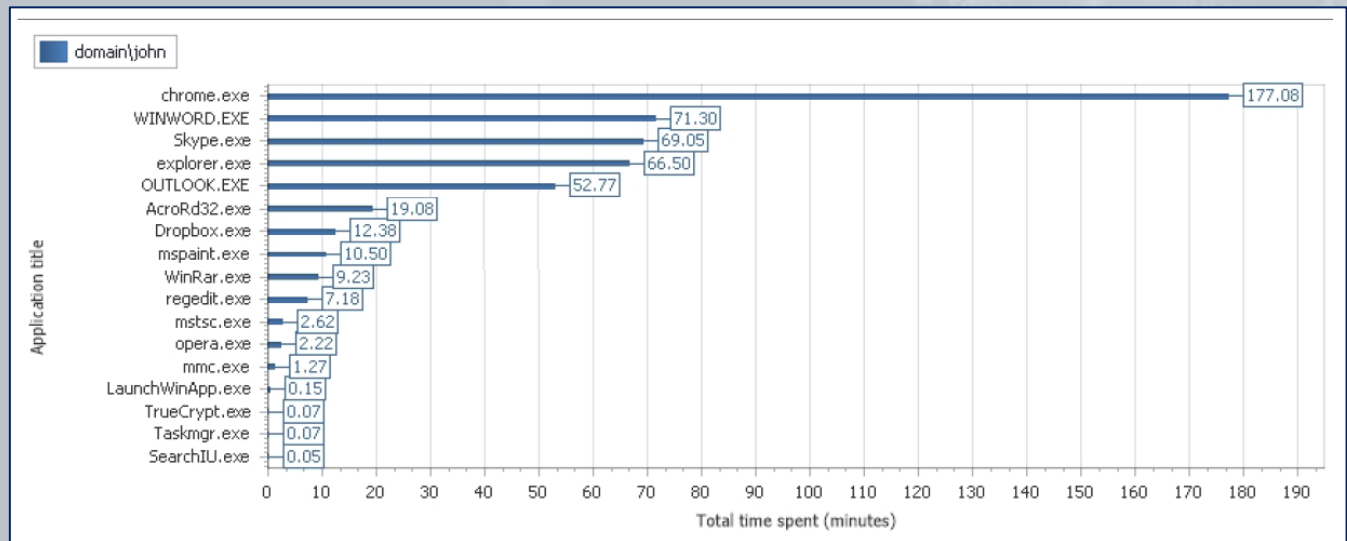
Activity Summary Grid Report

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

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

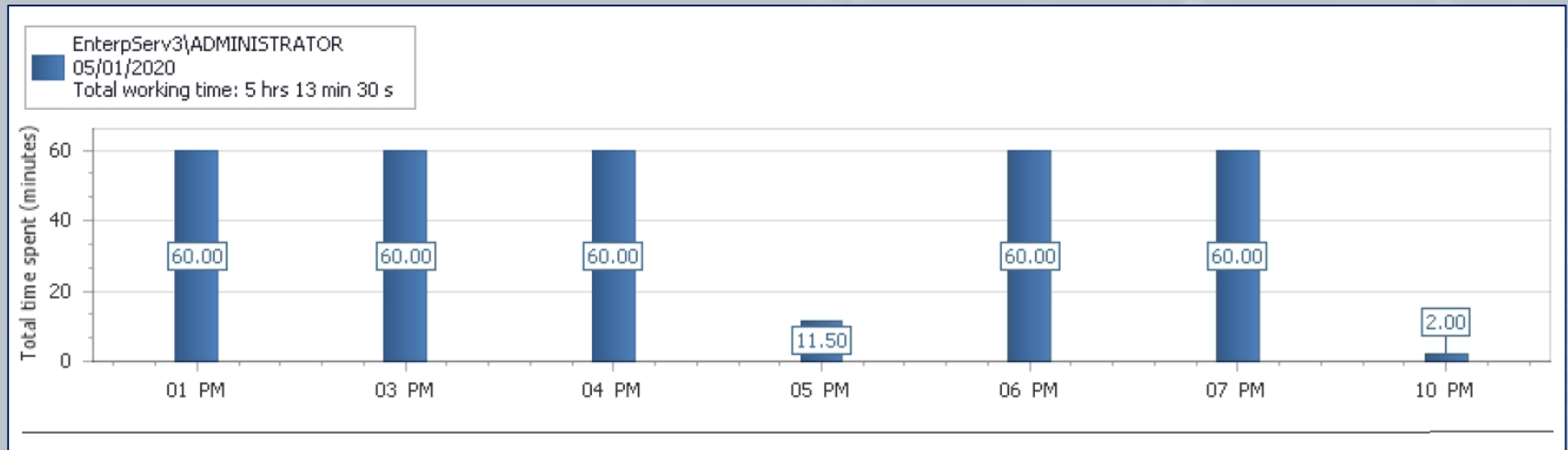
Detailed Activity Grid Report

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/19TprsVorHH8GodL0xnHmO8HKh7ww/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

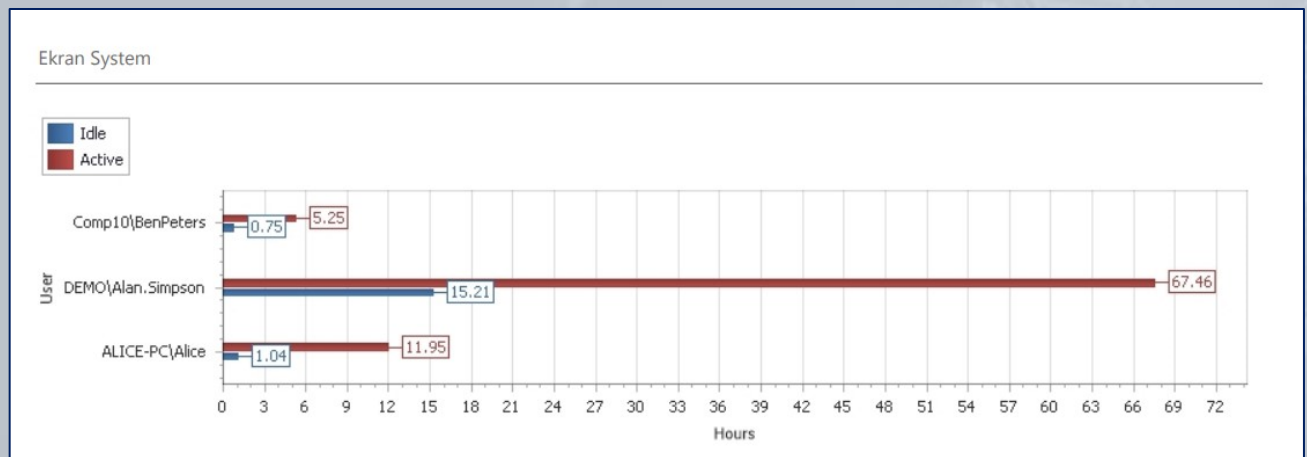
User Name	Date	Total Time Spent	Active Time	First Activity Time	Last Activity Time	Idle Time	Top 10 Applications	Top 10 URLs
COMP8\RobertO akley	07/06/2018	4m	4m	04:37:50 PM	04:42:37 PM	-	chrome.exe 3m EXCEL.EXE 1m explorer.exe 34s	bustle.com 5m mail.google.com 1m personalcreate.com 22s

User Productivity Heatmap Report

Ekran System

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

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

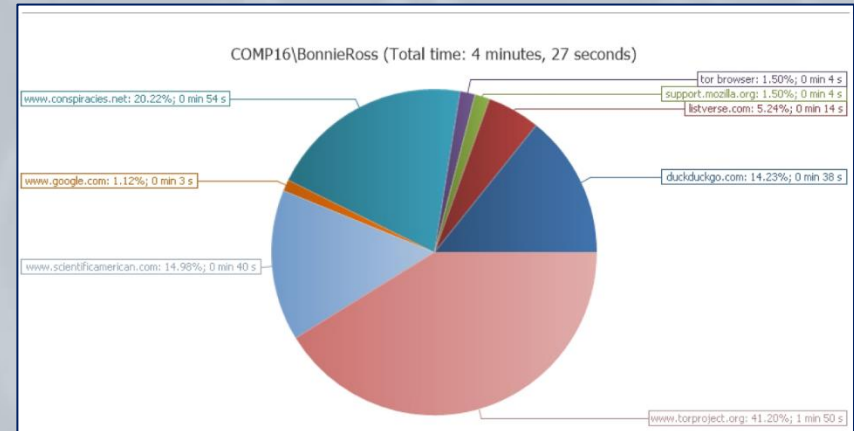
Who	Where	When	Details	Session Score	Session URL
ALICE-PC\Alice	alice-pc	07/12/2018 06:01:48 PM - 07/12/2018 06:04:08 PM	WorkingHours: normal	9%	Open Session
COMP11\SusieWade	Comp11	07/10/2018 11:08:30 AM - 07/10/2018 11:11:01 AM	WorkingHours: normal	30%	Open Session
COMP13\KylieKey	Comp13	07/09/2018 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

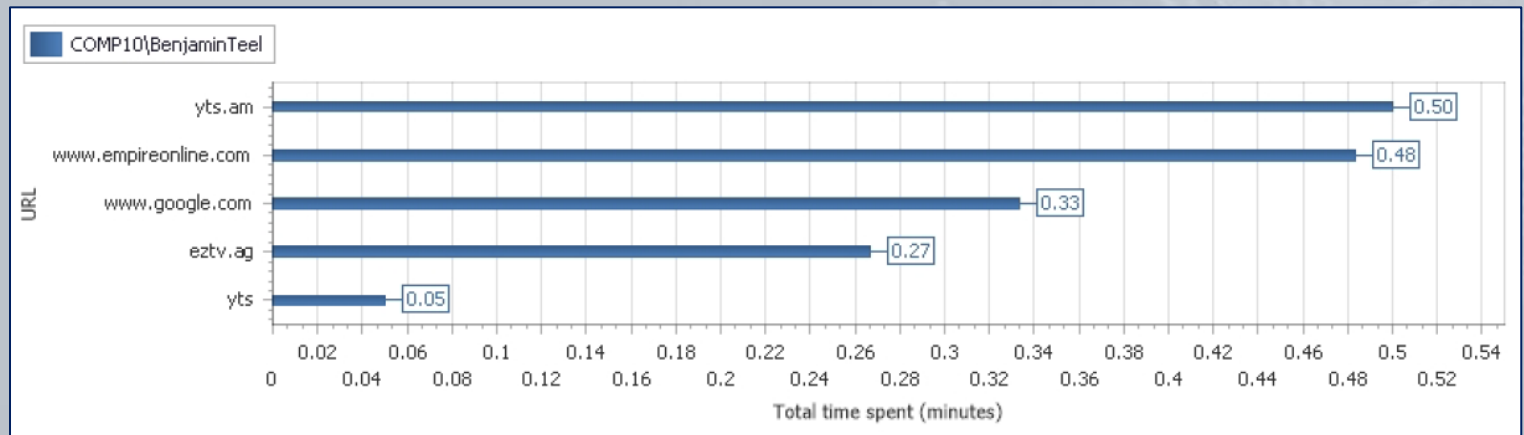
Client name	Comp15
Client description	Exporting HR Data
User name	COMP15\HelenPeterson
Total time	4 minutes, 33 seconds

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

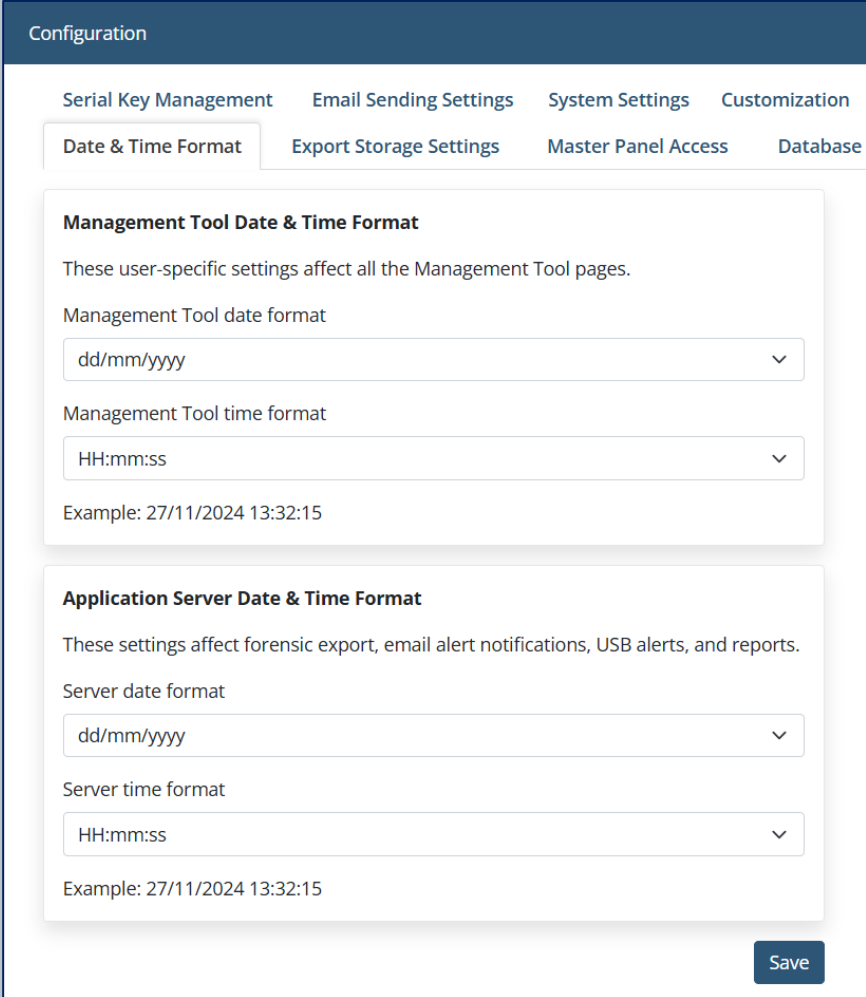
Session ID	User name	Client name	Session start	Last activity	Remote IP	Remote Public IP	Session URL	Is viewed	Viewer user name	Date and time
8	w11testpc\user	w11testPC	03/13/2024 02:00:49 PM	03/13/2024 02:01:50 PM	None	None	Open Session	Yes	admin	03/13/2024 02:02:02 PM
10	desktop-msaqs4k\user	DESKTOP-MSAQS4K	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 shows the 'Configuration' page with a navigation menu. The 'Date & Time Format' tab is selected. The page is divided into two main sections: 'Management Tool Date & Time Format' and 'Application Server Date & Time Format'. Each section contains a description of the settings, two dropdown menus for date and time formats, and an example of the resulting format. 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

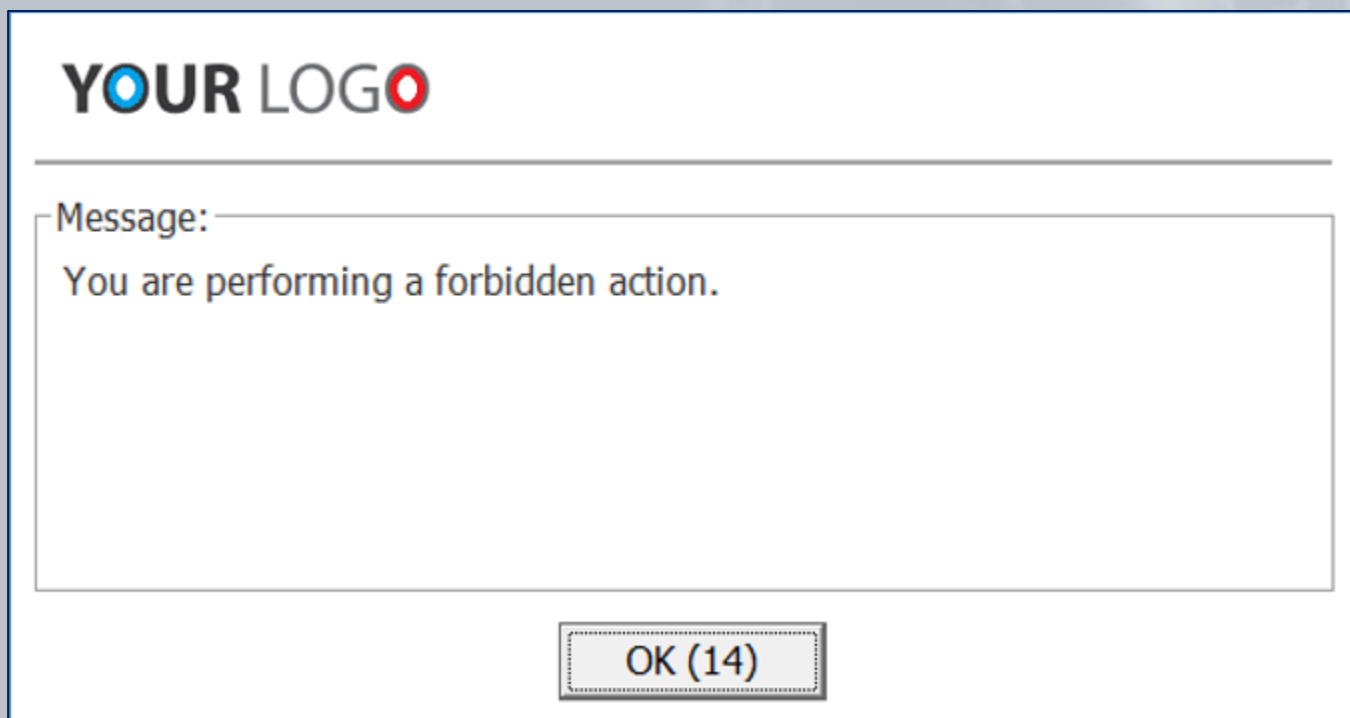
Server time format

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.



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.



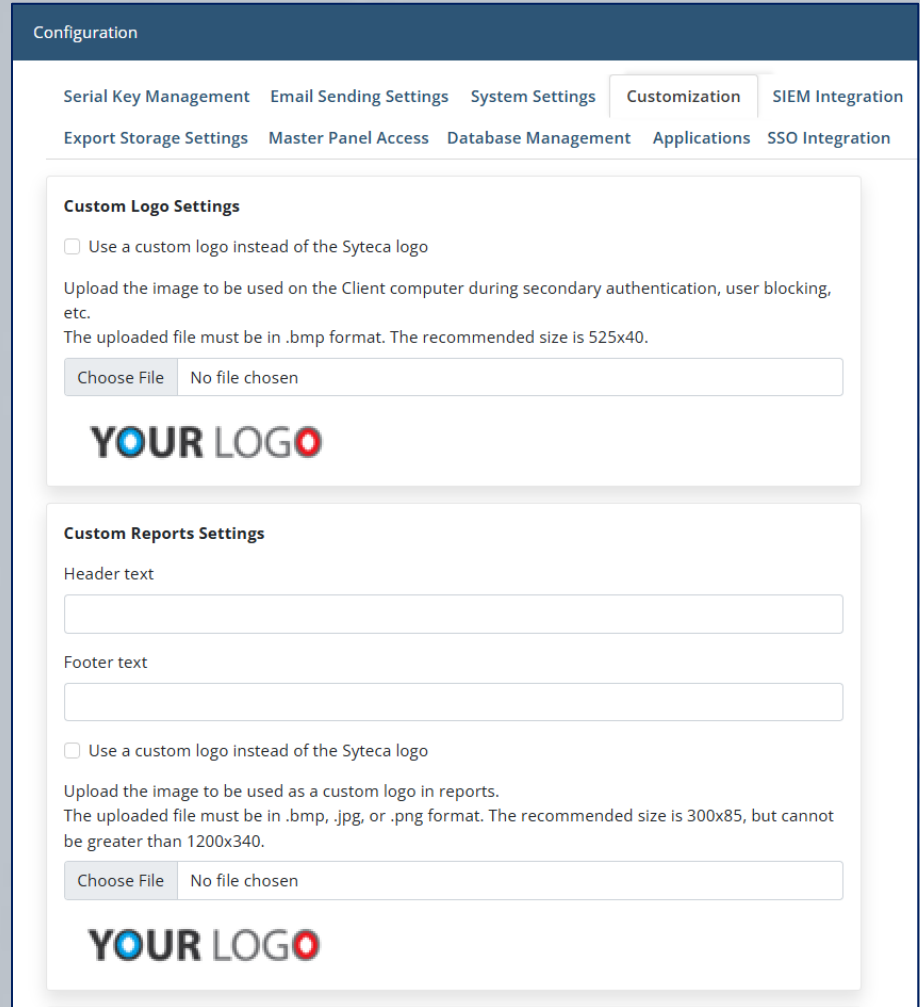
YOUR LOGO Activity Pie Chart Report

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

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

YOUR LOGO

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

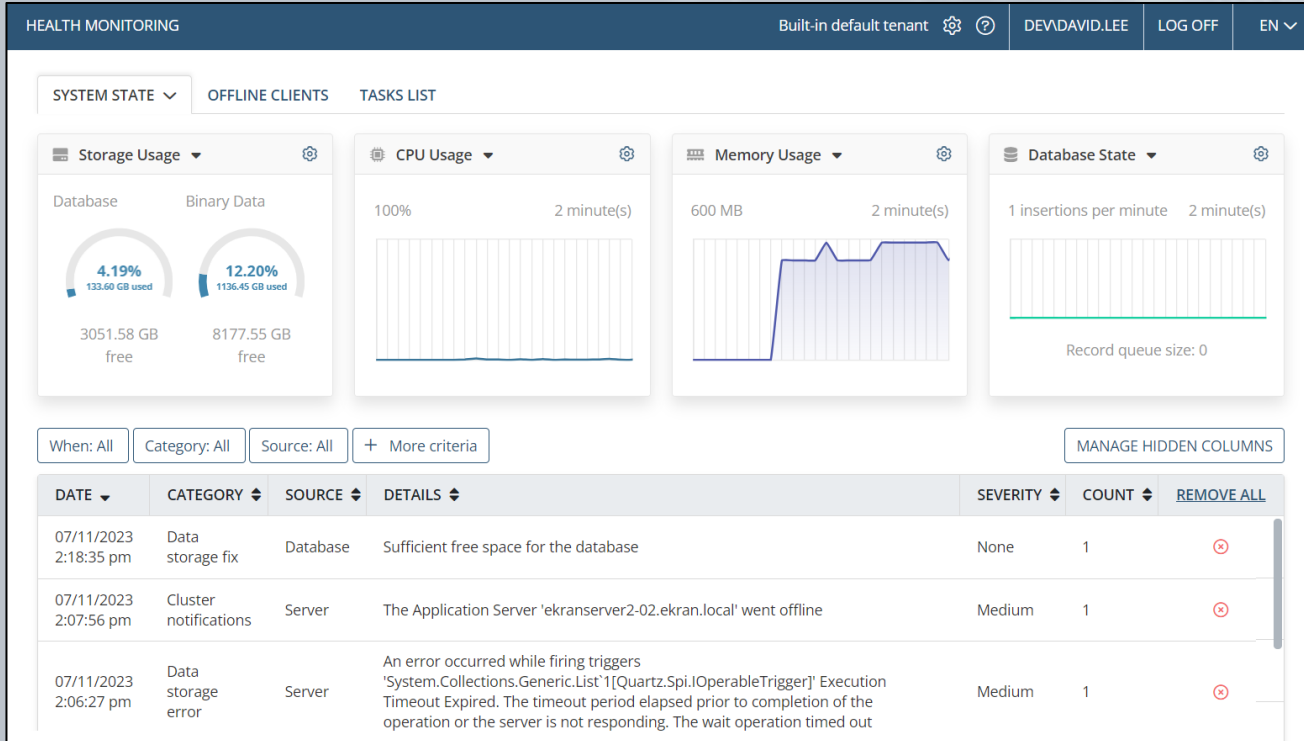
Main Screen

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

Save

System Health Monitoring

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



The dashboard displays the following metrics:

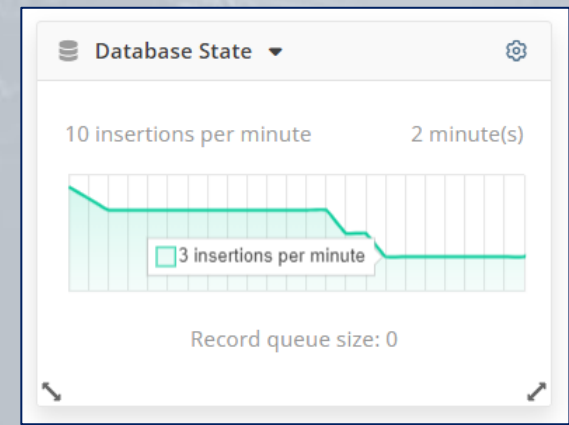
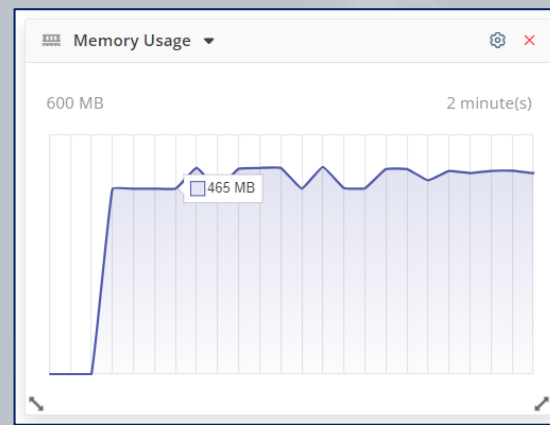
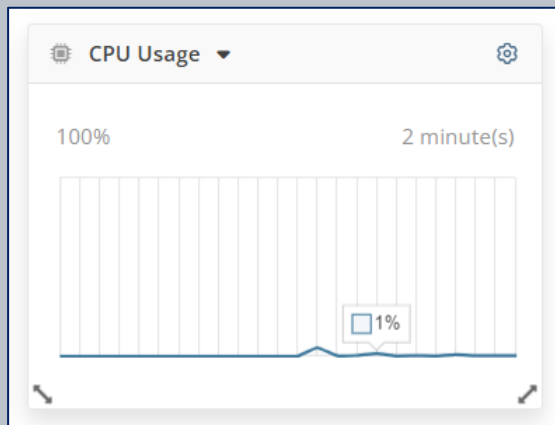
- Storage Usage:** Database (4.19% used, 133.60 GB used, 3051.58 GB free), Binary Data (12.20% used, 1136.45 GB used, 8177.55 GB free).
- CPU Usage:** 100% (2 minute(s)).
- Memory Usage:** 600 MB (2 minute(s)).
- Database State:** 1 insertions per minute (2 minute(s)), Record queue size: 0.

Filter criteria: When: All, Category: All, Source: All, + More criteria. [MANAGE HIDDEN COLUMNS](#)

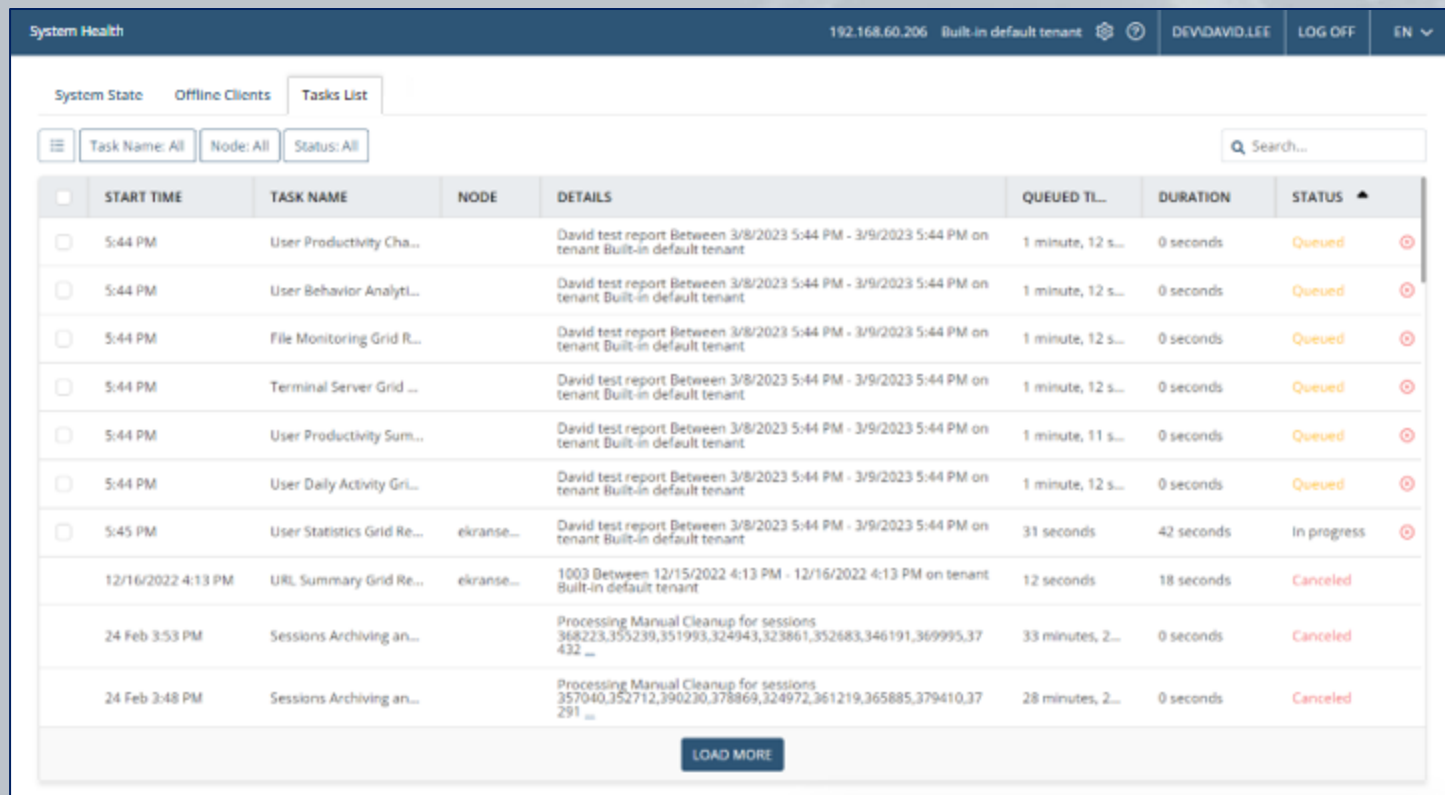
DATE	CATEGORY	SOURCE	DETAILS	SEVERITY	COUNT	REMOVE ALL
07/11/2023 2:18:35 pm	Data storage fix	Database	Sufficient free space for the database	None	1	
07/11/2023 2:07:56 pm	Cluster notifications	Server	The Application Server 'ekranserver2-02.ekran.local' went offline	Medium	1	
07/11/2023 2:06:27 pm	Data storage error	Server	An error occurred while firing triggers 'System.Collections.Generic.List`1[Quartz.Spi.IOperableTrigger]' Execution Timeout Expired. The timeout period elapsed prior to completion of the operation or the server is not responding. The wait operation timed out	Medium	1	

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

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



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



The screenshot shows the 'System Health' page with the 'Tasks List' tab selected. The interface includes a search bar and filter buttons for 'Task Name: All', 'Node: All', and 'Status: All'. The table below lists various tasks with their start times, names, nodes, details, and statuses.

START TIME	TASK NAME	NODE	DETAILS	QUEUED TL...	DURATION	STATUS
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
5:44 PM	User Behavior Analyti...		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
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
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
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
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
5:45 PM	User Statistics Grid Re...	eikranse...	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...	eikranse...	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

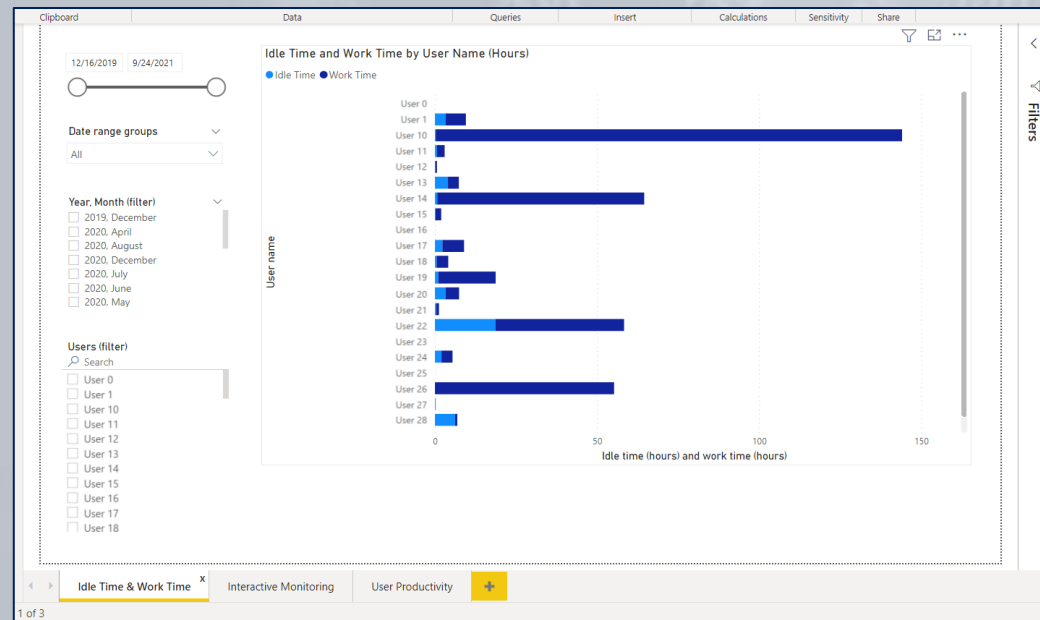
Syteca SDK, APIs and Integrations

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

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

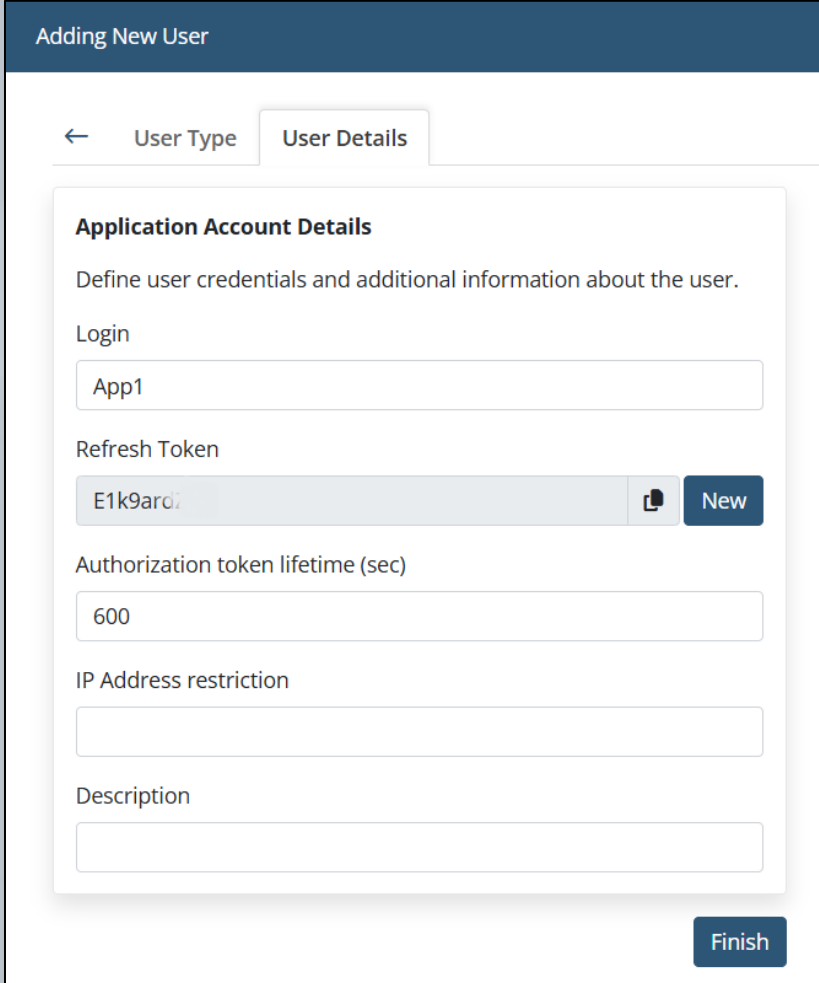
This application is designed to **allow customers to get Syteca monitoring data** via the API in order to **use for their own business purposes**.

Idle Time & Work Time Report



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

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



Adding New User

← User Type User Details


Application Account Details

Define user credentials and additional information about the user.

Login

App1

Refresh Token

E1k9ard:  **New**

Authorization token lifetime (sec)

600

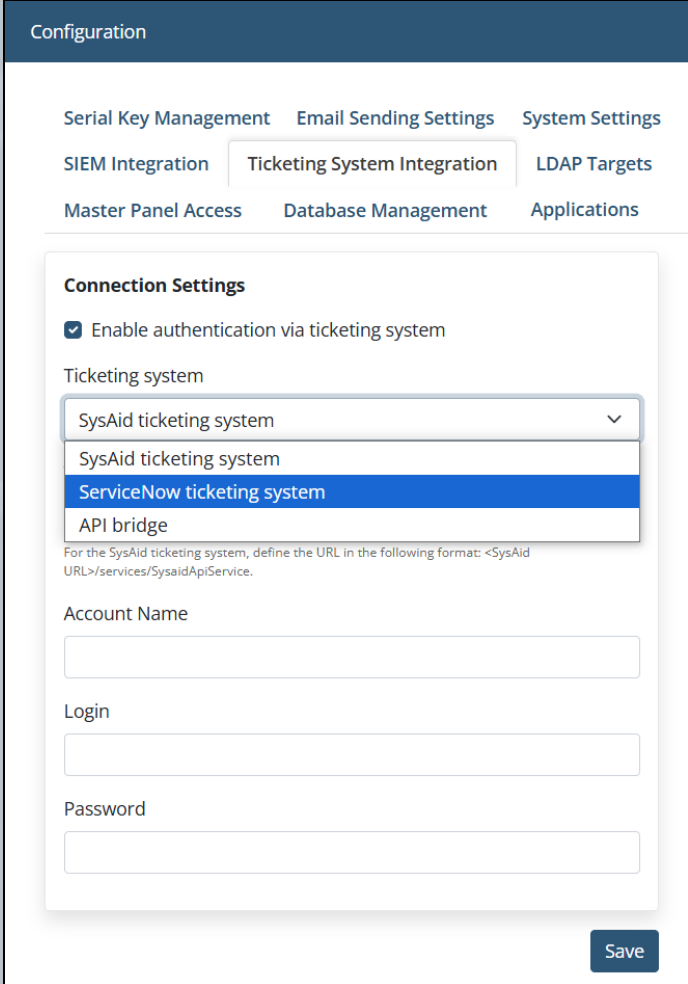
IP Address restriction

Description

Finish

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

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

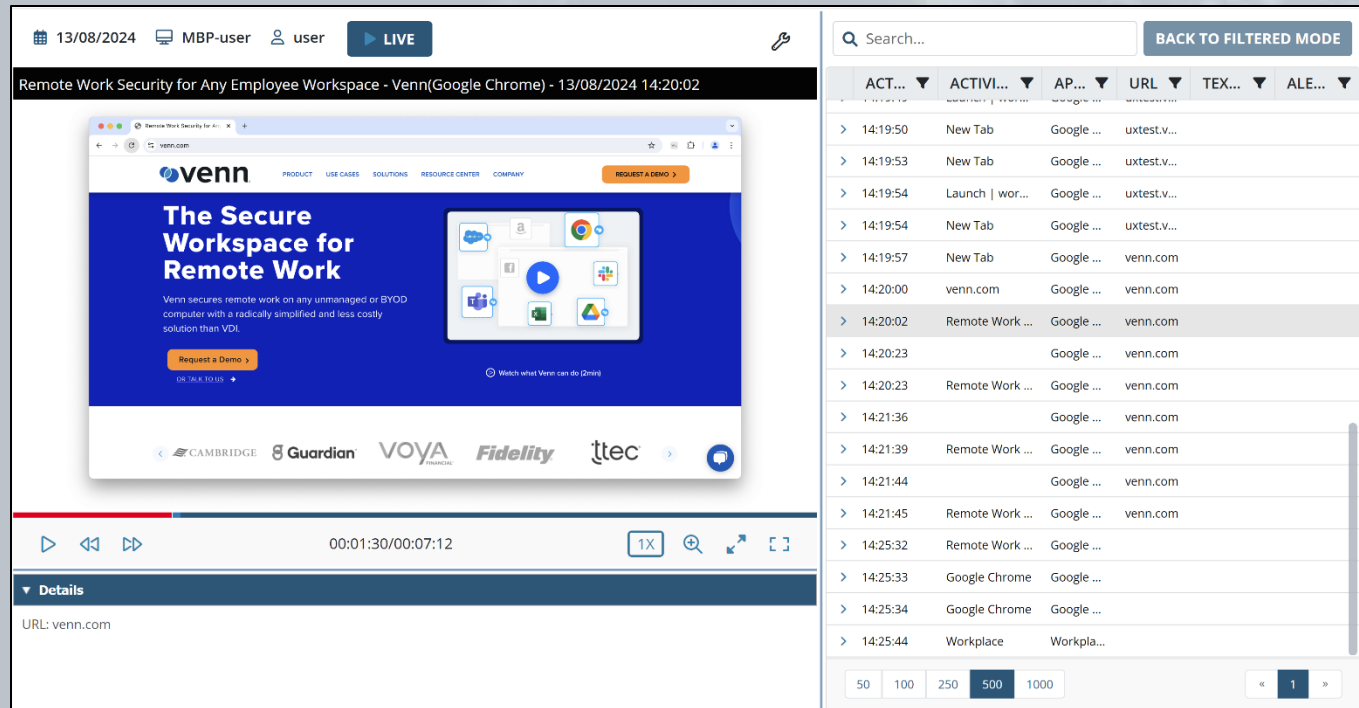


The screenshot shows the 'Configuration' page for 'Ticketing System Integration'. The page has a dark blue header with the title 'Configuration'. Below the header, there are several tabs: 'Serial Key Management', 'Email Sending Settings', 'System Settings', 'SIEM Integration', 'Ticketing System Integration' (which is active), and 'LDAP Targets'. Below these tabs, there are more options: 'Master Panel Access', 'Database Management', and 'Applications'. The main content area is titled 'Connection Settings' and contains a checkbox labeled 'Enable authentication via ticketing system' which is checked. Below this is a dropdown menu for 'Ticketing system' with three options: 'SysAid ticketing system', 'ServiceNow ticketing system' (which is selected and highlighted in blue), and 'API bridge'. Below the dropdown, there is a note: 'For the SysAid ticketing system, define the URL in the following format: <SysAid URL>/services/SysaidApiService.' Below this note are three input fields: 'Account Name', 'Login', and 'Password'. At the bottom right of the form is a 'Save' button.

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.**



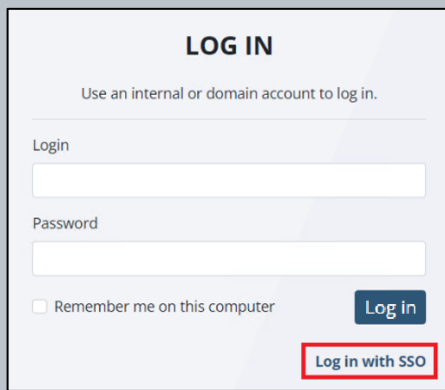
The screenshot displays a Venn workspace interface. At the top, it shows the date 13/08/2024, user information (MBP-user, user), and a LIVE indicator. Below this is a video player showing a Venn website page titled "Remote Work Security for Any Employee Workspace". The video player includes a progress bar at 00:01:30/00:07:12 and a details panel showing the URL: venn.com.

To the right of the video player is a filtered activity log table. The table has columns for ACT..., ACTIVI..., AP..., URL, TEX..., and ALE... The log shows a list of activities with timestamps and details. The following table represents the data visible in the screenshot:

Timestamp	Activity	Source	Destination
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...	

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**.



LOG IN

Use an internal or domain account to log in.

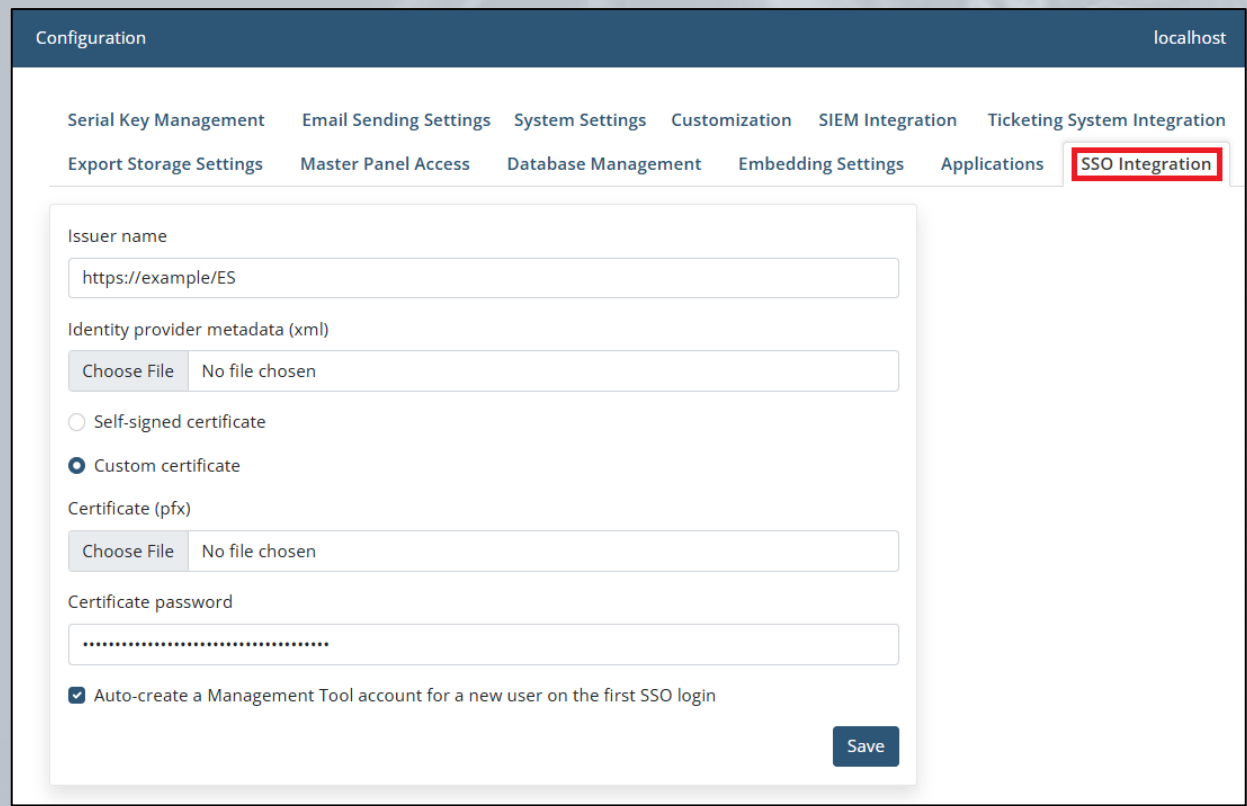
Login

Password

Remember me on this computer

Log in

Log in with SSO



Configuration localhost

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 **SSO Integration**

Issuer name

Identity provider metadata (xml)

Choose File No file chosen

Self-signed certificate

Custom certificate

Certificate (pfx)

Choose File No file chosen

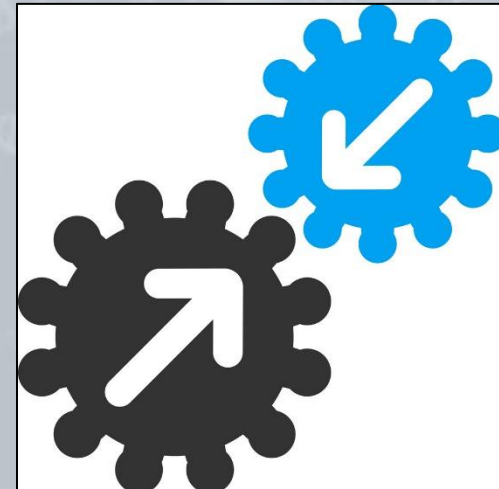
Certificate password

Auto-create a Management Tool account for a new user on the first SSO login

Save

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

- Databases (PostgreSQL / MS SQL Server)
- Data encryption protocols
- Storage mediums & services
- Load balancers
- etc.



NOTE: Some of these third-party products are referred to in other sections of this presentation.

For More Information...



Visit us online:
www.syteca.com