



User Manual

Viasecurity Control Center **V1.2.0**



Зміст

Розділ 1 Вступ до роботи з Viasecurity Control Center.....	6
1.1 Рекомендоване середовище роботи.....	7
1.2 Відмінності у функціях та можливостях: безкоштовна та повна версії.....	8
1.3 Технічні характеристики обладнання та показники максимальної продуктивності.	14
1.4 Можливості декодування.....	18
Розділ 2 Початок роботи.....	21
2.1 Активація ліцензії.....	21
2.1.1 Метод онлайн-активації.....	21
2.1.2 Спосіб офлайн-активації.....	22
2.2 Додавання пристроїв.....	24
2.2.1 Додавання сервера та управління даними.....	28
2.3 Локальна конфігурація.....	29
2.3.1 Події та сигнали тривоги.....	30
2.3.2 Розширені налаштування системи.....	31
2.3.3 Налаштування відображення відео.....	32
Розділ 3 Відеоспостереження.....	34
3.1 Налаштування та підготовка системи.....	34
3.1.1 Додавання пристроїв кодування.....	34
3.1.2 Налаштування обладнання.....	35
3.2 Основні інструменти спостереження.....	38
3.2.1 Операції з відео в реальному часі та відтворенням.....	38
3.2.2 Управління PTZ у реальному часі.....	41
3.2.3 Моніторинг за допомогою камер на карті.....	41
3.3 Порівняння зображень облич та виявлення людських тіл.....	45
3.3.1 Додавання бібліотек зображень облич та зображень облич.....	45
3.3.2 Перегляд відео, пов'язаних із розпізнаванням обличчя та людського тіла.....	47
3.3.3 Пошук розпізнаних зображень обличчя та зображень людського тіла.....	49
3.3.4 Пошук Об'єктів за Зображенням.....	50
3.4 Операції з транспортними засобами.....	51

3.4.1	Додавання списків транспортних засобів та номерів.....	51
3.4.2	Перегляд відео, пов'язаного з моніторингом транспортних засобів.....	52
3.4.3	Пошук та експорт подій ANPR.....	53
3.5	Функції інтелектуального пошуку.....	55
3.5.1	Смарт-пошук / VCA.....	56
3.5.2	TargetTrace та Object Search.....	58
3.5.3	Аналітика та звіти щодо підрахунку людей.....	60
Розділ 4 Системи контролю доступу та відеодомофонія.....		62
4.1	Підготовка.....	63
4.1.1	Додавання пристроїв.....	63
4.1.2	Переглянути детальну інформацію про пристрій.....	64
4.1.3	Переглянути детальну інформацію про двері.....	65
4.2	Додати відділи та осіб.....	66
4.2.1	Налаштування Облікових Даних.....	68
4.2.2	Захист зображень профілю.....	69
4.3	Управління рівнями доступу.....	70
4.4	Додати сигнал тривоги.....	72
4.5	Моніторинг Дверей у Режимі Реального Часу.....	73
4.5.1	Моніторинг дверей та контроль їхнього стану.....	75
4.5.2	Відображення та керування дверима на карті.....	76
4.6	Налаштування та робота відеодомофона.....	78
4.7	Управління подіями, пошук та аналітика.....	79
4.7.1	Пошук та експорт журналів подій.....	79
4.7.2	Імпорт відсутніх журналів автентифікації.....	82
4.7.3	Статистика даних та інформаційні панелі.....	83
Розділ 5 Управління сховищем.....		85
5.1	Підготовка.....	85
5.2	Розташування сховища та розподіл ємності.....	86
5.3	Налаштування графіка зберігання.....	87
5.4	Відтворення відео та пошук VCA.....	89
5.5	Життєвий цикл зберігання даних.....	90

5.6 Розширене управління сховищем даних.....	90
5.6.1 Завдання щодо мережевого інтерфейсного контролера (NIC).....	91
5.6.2 Відновити індекс.....	91
5.6.3 Обслуговування.....	91
Розділ 6 Інтерфейс моніторингу Viasecurity Control Center.....	93
Розділ 7 Пошук.....	97
7.1 Пошук транспортних засобів або осіб, виявлених камерами/дверима.....	97
7.2 Пошук виявлених осіб або транспортних засобів у зонах VCA.....	100
Розділ 8 Управління подіями та сигналами тривоги.....	101
8.1 Підтримувані події, що запускають дію.....	101
8.3 Додавання сигналу тривоги.....	115
8.4 Підтримувані дії взаємодії.....	116
8.5 Управління налаштованими сигналами тривоги.....	118
8.6 Моніторинг, пошук та експорт сповіщень.....	118
Розділ 9 Доступ до системи та управління обліковими записами.....	120
9.1 Управління користувачами та системними ролями.....	120
9.1.1 Додати користувача.....	120
9.1.2 Управління та ведення списку користувачів.....	121
9.1.3 Налаштування системних ролей.....	121
9.2 Безпека облікового запису та відновлення облікових даних.....	126
9.2.1 Налаштування безпеки облікових записів.....	126
9.2.2 Скидання пароля для входу.....	127
Розділ 10 Конфігурація системи.....	128
10.1 Налаштування параметрів електронної пошти.....	128
10.2 Управління графіками вихідних днів.....	129
10.3 Управління налаштуваннями мережі.....	129
10.3.1 Налаштування синхронізації часу через Інтернет.....	129
10.3.2 Налаштування протоколу доступу до пристроїв.....	130
10.3.3 Налаштування доступу до глобальної мережі (WAN).....	130
10.3.4 Налаштування NIC.....	131
10.3.5 Скидання мережевих налаштувань.....	131

10.4 Захист HTTPS-з'єднань за допомогою сертифікатів SSL/TLS.....	131
10.4.1 Управління сертифікатами.....	131
10.4.2. Отримання сертифіката SSL/TLS.....	132
10.5 Налаштування сертифіката компонента служби.....	134
10.6 Приватність та безпека.....	135
Розділ 11 Технічне обслуговування.....	136
11.1 Створення та відображення звіту про технічне обслуговування.....	136
11.2 Пошук повідомлень.....	140
11.3 Пошук системних журналів.....	141
А. Обмеження щодо використання продукту: сценарії та рекомендації.....	143

Розділ 1 Вступ до роботи з Viasecurity Control Center

Viasecurity Control Center — це оптимізована система управління відео, спроектована з урахуванням мінімального споживання системних ресурсів для забезпечення максимально зручного користувацького досвіду. Ця платформа централізує функції додатків та налаштувань у різних сферах, зокрема у відеоспостереженні, автоматичному розпізнаванні номерних знаків (ANPR), відеодомофоні та контролі доступу.

Завдяки інтуїтивно зрозумілому інтерфейсу користувача та наявності чітких вбудованих підказок, оператори можуть швидко розгорнути систему та вільно в ній орієнтуватися з мінімальними витратами часу на навчання. Крім того, програмне забезпечення підтримує широку сумісність із різноманітним обладнанням сторонніх виробників. Для дистанційного керування передбачено мобільний клієнт, який надає такі функції, як моніторинг тривоги, відтворення відео та перегляд у реальному часі.

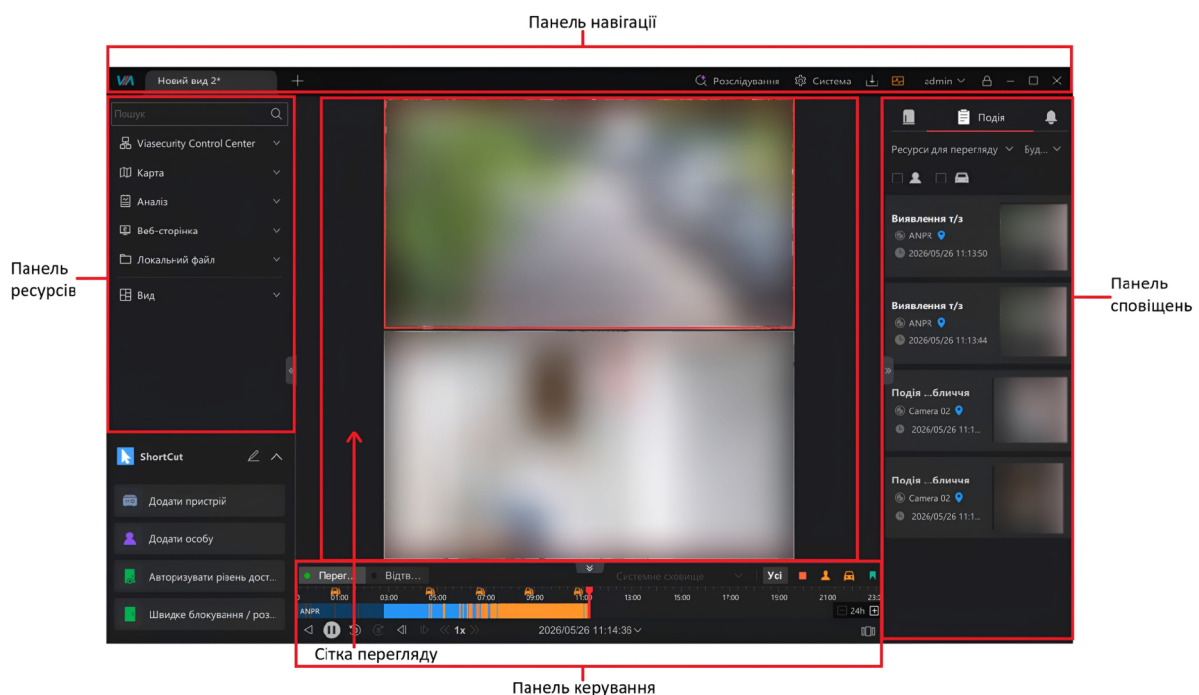


Рисунок 1.1 Головна сторінка

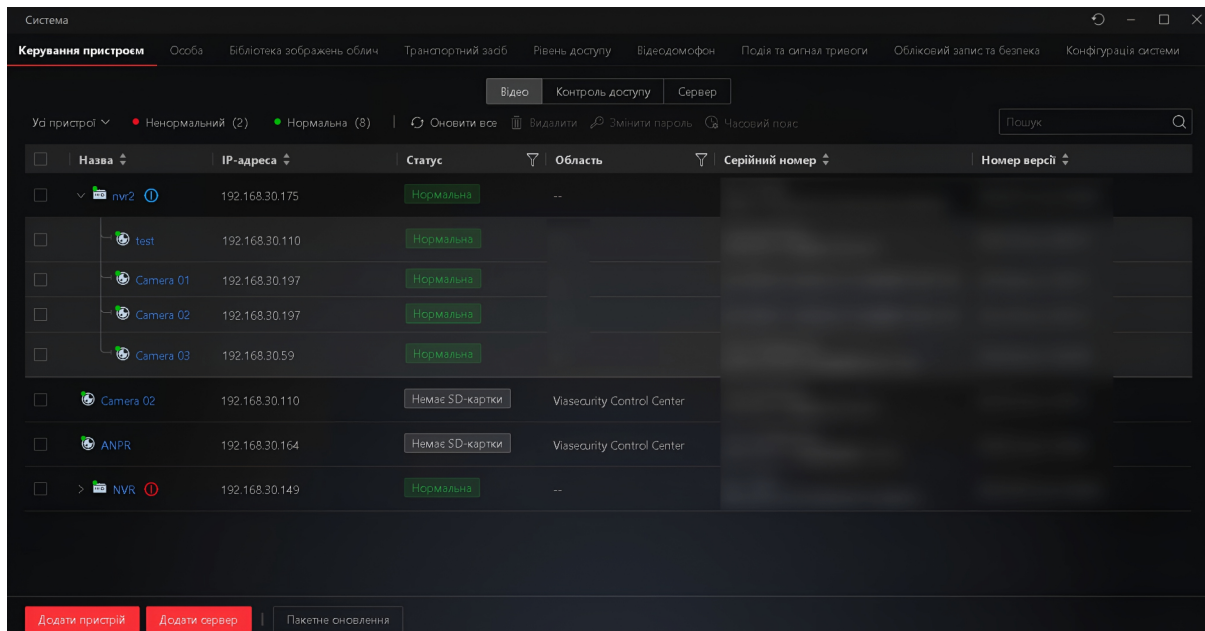


Рисунок 1.2 Вікно системи

1.1 Рекомендоване середовище роботи

Таблиця 1.1 Рекомендоване середовище роботи

Платформа	ОС
Сервер	- Microsoft® Windows Server 2025 - Microsoft® Windows Server 2022 - Microsoft® Windows Server 2019 64-bit - Microsoft® Windows Server 2016 64-bit - Microsoft® Windows 11 64-bit - Microsoft® Windows 10 64-bit
Настільний ПК	- Microsoft® Windows Server 2025 - Microsoft® Windows Server 2022 - Microsoft® Windows Server 2019 64-bit - Microsoft® Windows Server 2016 64-bit - Microsoft® Windows 11 64-bit - Microsoft® Windows 10 64-bit
Мобільний клієнт	- iOS 14.0+ - Android 8.0+

1.2 Відмінності у функціях та можливостях: безкоштовна та повна версії

У цьому розділі описано основні функціональні відмінності та максимальні можливості безкоштовної та повної версій Viasecurity Control Center.

Максимальна продуктивність

Таблиця 1.2 Ресурси, що підлягають управлінню

Продуктивність	Повна версія	Безкоштовна версія
Загальна кількість каналів	128 *Включає кількість камер TargetTrace, камер ANPR, камер для підрахунку людей, камер для порівняння зображень обличчя та розпізнавання фігури, а також камер сторонніх виробників	16
Камери для підрахунку людей	128	0
Камери TargetTrace	128	0
Камери ANPR	8	0
Камери для порівняння зображень обличчя та розпізнавання фігури	16	0
Камери сторонніх виробників	128	0
Двері	32	2
Зовнішні сервери потокового передавання	64	64

Таблиця 1.3 Інше

Продуктивність	Повна версія	Безкоштовна версія
Транспортні засоби	2,000	0

Таблиця 1.4 Контроль доступу

Продуктивність	Повна версія	Безкоштовна версія
Особи	500	500
Облікові дані	Картки: 1,000 Фотографії обличчя: 500 Відбитки пальців: 1,000	Картки: 1,000 Фотографії обличчя: 500 Відбитки пальців: 1,000

Таблиця 1.5 Користувачі

Продуктивність	Повна версія	Безкоштовна версія
Локальні користувачі	128	128
Ролі	64	64
Користувачі, що одночасно увійшли через настільний ПК	64	3
Користувачів, що одночасно увійшли через мобільний клієнт	64	3

Основні функції

Наступні функції доступні **лише у повній версії**.

Звіт про підрахунок відвідувачів

- Доступ до вичерпних звітів про підрахунок відвідувачів

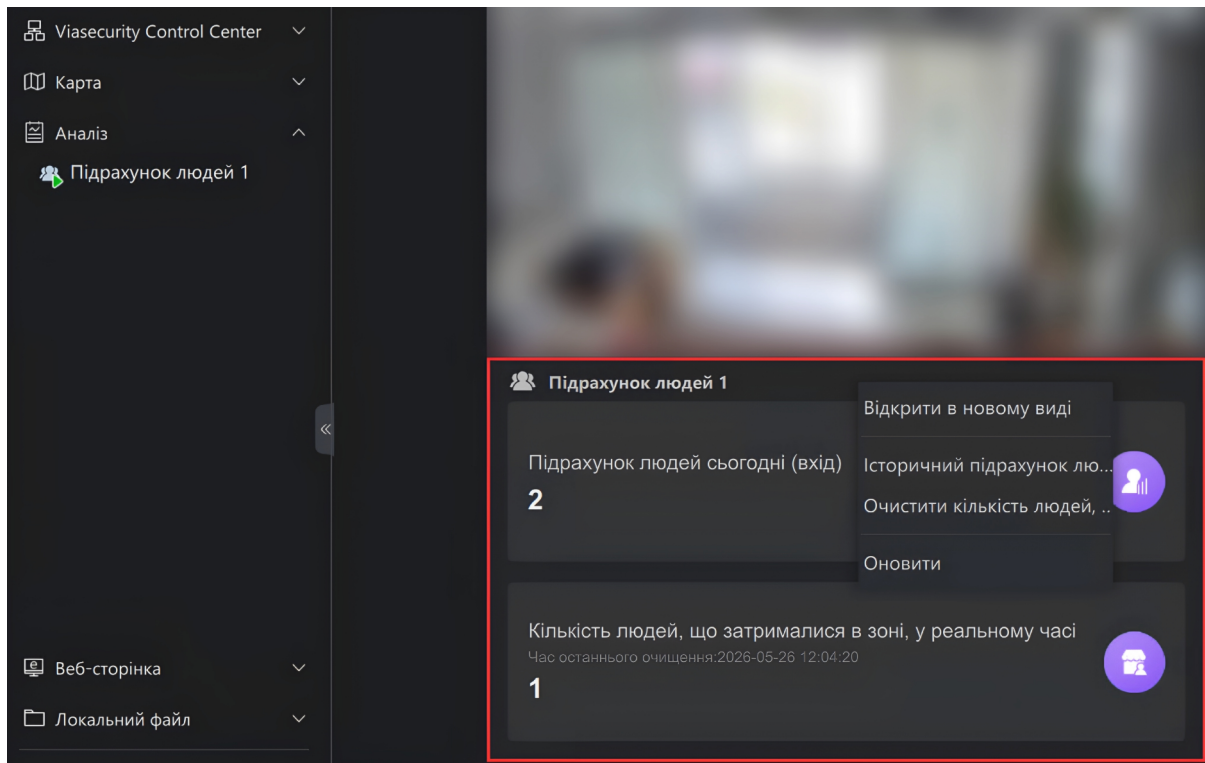


Рисунок 1.4 Звіт про підрахунок відвідувачів

Пошук транспортних засобів

- Користувачі можуть фільтрувати та шукати конкретні транспортні засоби на основі ідентифікаційних характеристик, перейшовши до меню Пошук → Подія проїзду транспортного засобу

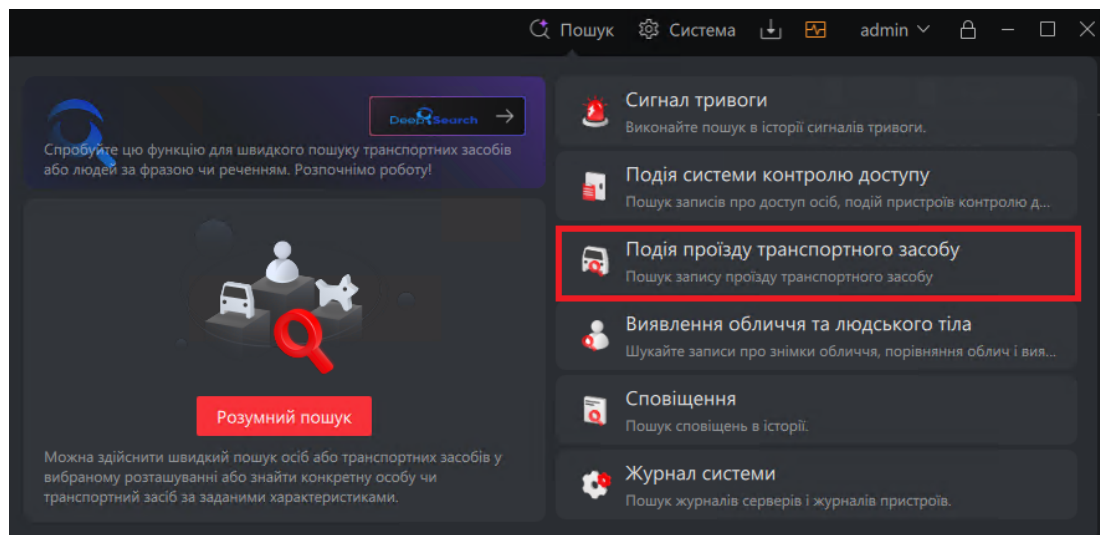


Рисунок 1.5 Подія проїзду транспортного засобу

- або Пошук → Розумний пошук

The screenshot shows a search form with the following fields and options:

- Ціль (Target):**
 - Особа (Person)
 - Автомобіль (Car)** (highlighted with a red border)

Якщо ви виберете «Людина в системі», пошук за характеристиками транспортного засобу буде заборонено.
- Країна/регіон (Country/Region):**

Уведіть ім'я країни / регіону для пошуку.
- Номерний знак (License Plate):**
 - ☐ З номерним знаком
 - ☐ Відсутній номерний знак
- Власник транспортного засобу (Vehicle Owner):**

Введіть ім'я власника транспортного засобу.
- Тип (Type):**

Уведіть тип транспортного засобу для пошуку.
- Марка (Brand):**

Уведіть назву бренду для пошуку.
- Колір (Color):**

Buttons: **OK** (red), **Скасувати** (grey).

Рисунок 1.6 Пошук транспортних засобів за ознаками

- Крім того, система дозволяє керувати списками номерних знаків та транспортних засобів при інтеграції з камерами ANPR.

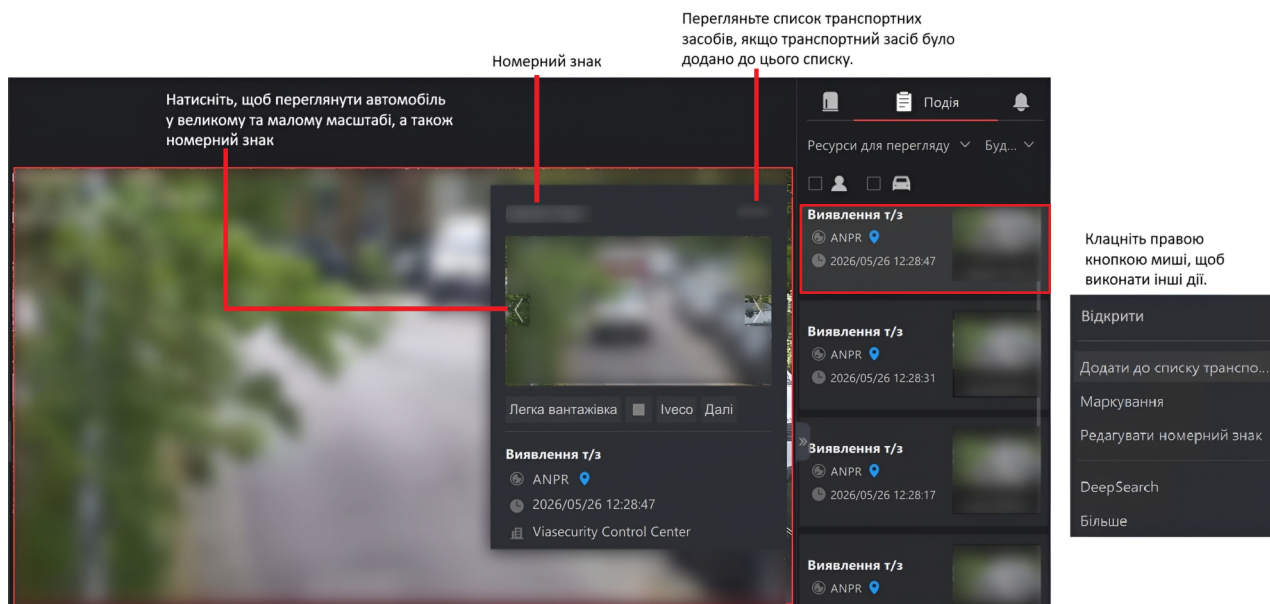


Рисунок 1.7 Камера ANPR

Порівняння зображень облич

- Програмне забезпечення дозволяє здійснювати пошук персоналу за конкретними ознаками через меню **Пошук → Виявлення обличчя та людського тіла**

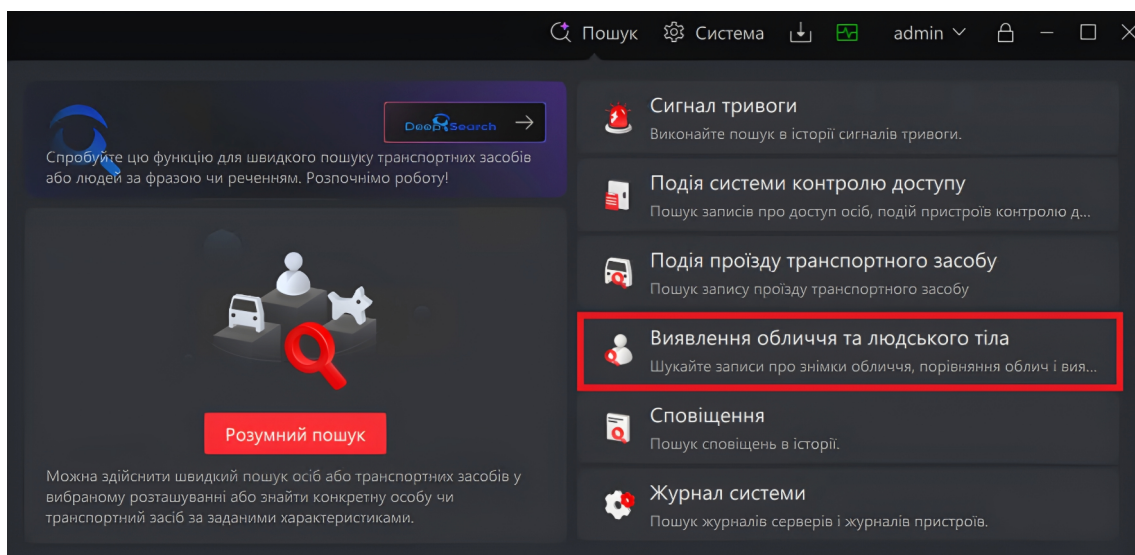


Рисунок 1.8 Виявлення обличчя та людського тіла

- та Пошук → Розумний пошук

Ціль

Особа

Автомобіль

Якщо ви виберете «Людина в системі», пошук за характеристиками транспортного засобу буде заборонено.

Характеристика Особи

Стать

Чоловік Жінка

Вікова група

Підлітки Молода людина Людина середнього віку Літні люди

Немовля Дитина Юнак Дорослий

Люди середнього віку та літні люди

Аксесуари

В окулярах Без окулярів У сонячних окулярах У масці

Без маски Із рюкзаком Без рюкзака

Зачіска

Довге волосся Коротке волосся

Тип верхнього одягу

Особа в системі

OK

Скасувати

Рисунок 1.9 Пошук осіб за ознаками

- Порівняння зображень облич повністю підтримується при використанні TargetTrace та спеціальних камер розпізнавання облич

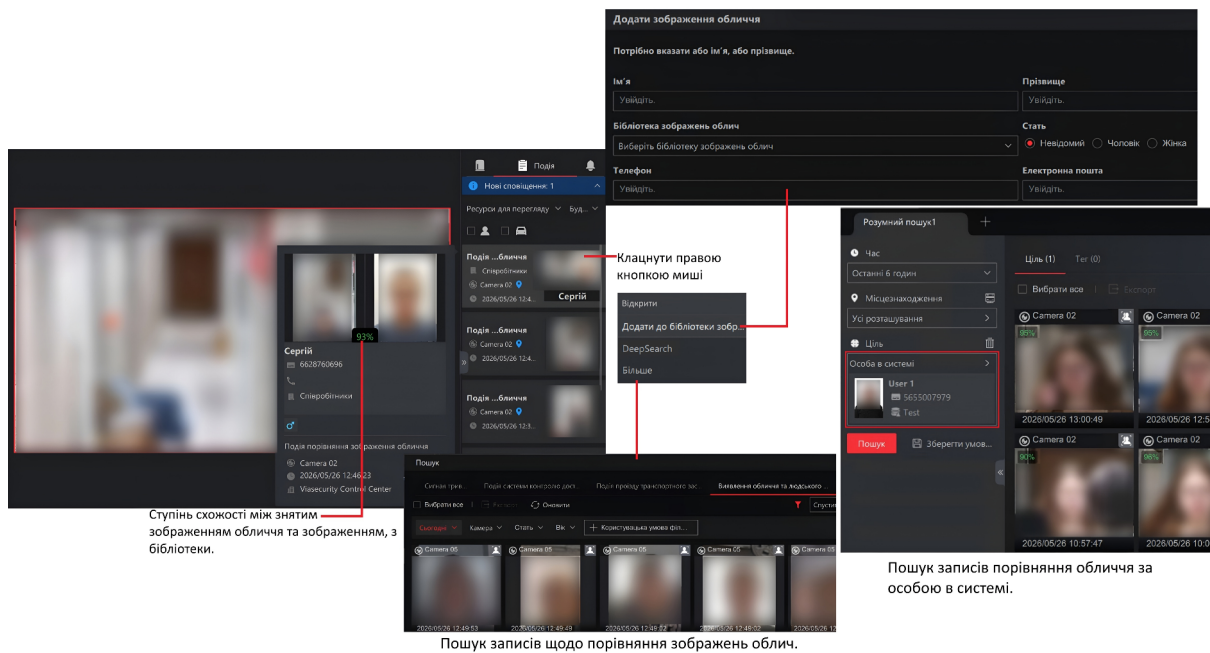


Рисунок 1.10 Камера для порівняння зображень обличчя

Пошук за зображеннями обличчя/тіл

Оператори можуть завантажувати еталонні зображення та визначати конкретні параметри для пошуку відповідних зображень обличчя або тіла. Клацнувши правою кнопкою миші на будь-якому результаті пошуку, можна також швидко знайти візуально схожі зображення.

Дискове сховище сервера

- Повна версія дозволяє здійснювати прямий запис відео на дискове сховище сервера.

(Примітка: Безкоштовна версія обмежена лише зберіганням файлів та статичних зображень.)

Розширена інтеграція з продуктами сторонніх виробників

- Забезпечено широкую сумісність з пристроями, що використовують протоколи ONVIF, а також з пристроями від Hikvision, Dahua, Axis та Hanwha.

Мобільний клієнт / Настільний ПК

- Кількість одночасних підключень збільшено до 64 одночасних входів через настільні та мобільні клієнти.

(Примітка: у безкоштовній версії обмеження становить 3 одночасних підключення. Мобільний доступ надається автоматично після активації базової ліцензії, що усуває необхідність у окремій мобільній ліцензії.)

1.3 Технічні характеристики обладнання та показники максимальної продуктивності

Експлуатаційні обмеження Viasecurity Control Center були протестовані з використанням конкретних апаратних середовищ. У таблиці 1.6 наведено детальну інформацію про дві основні конфігурації, що використовувалися для визначення цих базових можливостей.

Конфігурації системи

Таблиця 1.6 Апаратні середовища

Характеристика	Конфігурація 1	Конфігурація 2
Процесор	Intel® Core™ i5-12500	Intel® Core™ i7-12700
Оперативна пам'ять	2*8 ГБ	2*8 ГБ
Мережева карта	Мережева карта 1 Гбіт/с	Мережева карта 1 Гбіт/с
SSD для ОС	SSD корпоративного класу	SSD корпоративного класу
HDD для зберігання відео	HDD корпоративного класу або високопродуктивний мережевий HDD. Він повинен підтримувати швидкість запису або читання 10 МБ/с.	HDD корпоративного класу або високопродуктивний мережевий HDD. Він повинен підтримувати швидкість запису або читання 20 МБ/с.
Ємність SSD для бази даних	Не менше 500 ГБ	Не менше 500 ГБ
ОС	Microsoft® Windows 10 64-біт або пізніша версія	Microsoft® Windows 10 64-біт або пізніша версія

У наступних підрозділах наведено абсолютні максимальні системні можливості, які можна досягти за цих перевірених умов.

Ресурсні можливості

Таблиця 1.7 Ресурсні можливості

Тип ресурсу	Конфігурація 1	Конфігурація 2
Камери (включно з камерами, до яких здійснюється доступ за протоколом ONVIF та камери сторонніх виробників)	128 (Допускається не більше 8 камер ANPR та 16 камер для порівняння зображень облич.)	128 (Допускається не більше 8 камер ANPR та 16 камер для порівняння зображень облич.)
Двері	32	32
Зовнішні сервери потокового передавання	64	

Обмеження щодо обробки відео

Вбудований сервер потокового передавання системи обмежений обробкою максимум 200 внутрішніх каналів із загальною пропускнуою здатністю входу/виходу 400 Мбіт/с.

Контроль доступу

Таблиця 1.8 Параметри контролю доступу

Параметр	Конфігурація 1	Конфігурація 2
Особи	500	500
Картки	1,500	1,500
Фотографії профілю	500	500

Порогові значення панелі моніторингу та керування

У таблиці 1.9 визначено відображення та управління пороговими значеннями в інтерфейсі моніторингу.

Таблиця 1.9 Можливості інтерфейсу моніторингу

Паметр	Конфігурація 1	Конфігурація 2
Ресурси в одному вікні	64	64
Ресурси в дукількох вікнах	256	256
Області	256	256
Карти	Загальна кількість статичних карт: 16 Карт в одному вікні: 4	Загальна кількість статичних карт: 16 Карт в одному вікні: 4

Таблиця 1.10 Параметри інтерфейсу користувача, незалежні від апаратного забезпечення

Параметр	Продуктивність
Нові вікна	4
Види	64
Рівні області	5
Ресурси на GIS-карті або на кожній статичній карті	256

Користувачі, ролі та дозволи

Таблиця 1.11 Показники користувачів та ролей

Параметр	Конфігурація 1	Конфігурація 2
Локальні користувачі	128	128
Ролі	64	64

Користувачі, що перебувають у мережі на настільних комп'ютерах	64	64
Користувачі, що перебувають у мережі на мобільних клієнтах	64	64

Події та сигнали тривоги

Таблиця 1.12 Продуктивність параметрів подій та тривог

Параметр	Конфігурація 1	Конфігурація 2
Отримання подій	20/с	20/с
Кількість правил сигналів тривоги	1000	1000
Швидкість передачі тривог/подій/повідомлень із сервера до одного клієнта	20/с	20/с

Обмеження щодо архівування та зберігання даних

Таблиця 1.13 Параметри продуктивності зберігання

Параметр	Конфігурація 1	Конфігурація 2
Пропускна здатність сховища відео	480 Мбіт/с	600 Мбіт/с
Період зберігання зафіксованих облич, записів ANPR, подій, даних інтелектуального аналізу, записів доступу та системних журналів	3 роки	3 роки
Ємність сховища (включно із зафіксованими обличчями, записами ANPR, подіями, даними)	10 мільйонів	10 мільйонів

інтелектуального аналізу, записами доступу та системними журналами)		
---	--	--

1.4 Можливості декодування

Можливості декодування клієнта, описані в цьому розділі, були оцінені в рамках спеціальної конфігурації апаратного забезпечення клієнта. У таблиці 1.14 наведено конкретну конфігурацію тестування, яка використовувалася для встановлення цих обмежень.

Таблиця 1.14 Конфігурація апаратного забезпечення для декодування на стороні клієнта

Характеристика	Конфігурація
Процесор	Intel® Core™ i5-12500 3.0.0 ГГц
Оперативна пам'ять	16 (8+8) ГБ
Мережева карта	Intel® Ethernet Connection (17) I219-LM
Відеокарта	Intel® UHD Graphics 770
ОС	Microsoft® Windows 10 (64-біт)

У наведених нижче таблицях наведено максимальну кількість одночасних потоків прямого перегляду, що можна досягти за допомогою апаратного та програмного декодування, з поділом за форматами стиснення H.264 та H.265.

H.264

Таблиця 1.15 Тести продуктивності апаратного декодування для H.264

Частота кадрів (кадрів/с)	Швидкість передачі даних (Мбіт/с)	Роздільна здатність	Макс. кількість каналів Live View
30	6	1080p	35
30	12	8 MP	10
25	6	1080p	42

25	12	8 MP	12
----	----	------	----

Таблиця 1.16. Тести продуктивності програмного декодування H.264

Частота кадрів (кадрів/с)	Швидкість передачі даних (Мбіт/с)	Роздільна здатність	Макс. кількість каналів Live View
30	6	1080p	15
30	12	8 MP	5
25	6	1080p	17
25	12	8 MP	6

H.265

Таблиця 1.17 Тести продуктивності апаратного декодування для H.265

Частота кадрів (кадрів/с)	Швидкість передачі даних (Мбіт/с)	Роздільна здатність	Макс. кількість каналів Live View
30	3	1080p	41
30	6	8 MP	11
25	3	1080p	45
25	6	8 MP	15

Таблиця 1.18 Тести продуктивності програмного декодування для H.265

Частота кадрів (кадрів/с)	Швидкість передачі даних (Мбіт/с)	Роздільна здатність	Макс. кількість каналів Live View
30	3	1080p	13
30	6	8 MP	4
25	3	1080p	15

25	6	8 MP	5
----	---	------	---

Розділ 2 Початок роботи

Цей розділ є основним посібником з розгортання та налаштування програмного забезпечення. Він містить необхідні інструкції, які допоможуть вам швидко виконати початкове налаштування та ознайомитися з основними операціями.

2.1 Активація ліцензії

Після початкової інсталяції клієнтське програмне забезпечення працює за тимчасовою ліцензією, яка обмежує загальну кількість пристроїв, що підлягають управлінню, та певні системні функції. Щоб розкрити повний потенціал платформи, включаючи розширені можливості пристроїв та додаткові функції, необхідно зареєструвати свій сервер.

(Примітка: активація на цьому етапі є необов'язковою і, за бажанням, її можна відкласти на пізніше).

Важливі зауваження:

- Активація системи, оновлення ліцензій та деактивація доступні виключно для облікових записів з правами адміністратора.
- Якщо під час циклу дії ліцензії виникнуть будь-які помилки, будь ласка, експортуйте журнали сервера та надішліть їх нашій команді технічної підтримки для отримання допомоги.
- Перейдіть до меню Огляд ліцензій, щоб призначити доступні ліцензійні ресурси конкретно для камер ANPR, розпізнавання облич або розпізнавання людських тіл.

Щоб розпочати процедуру активації:

1. На головній панелі інструментів (домашній сторінці) натисніть на свій профіль/ім'я користувача, розташоване у верхньому правому куті.
2. Виберіть **Керування ліцензіями** у спадному меню, щоб відкрити спеціальну панель.
3. Натисніть кнопку **Активувати ліцензію**, розташовану в нижньому лівому куті інтерфейсу.

2.1. Метод онлайн-активації

Якщо ваш комп'ютер має активне підключення до Інтернету, реєстрація через мережу є найпростішим методом.

Процедура:

1. У вікні активації виберіть **Активация онлайн** як бажаний метод.
2. Введіть унікальний ключ активації, наданий під час придбання програмного забезпечення. Якщо у вас є кілька ключів, скористайтесь кнопкою **Додати**, щоб ввести додаткові коди.
 - а) Переконайтеся, що ключ активації складається саме з 32 буквено-цифрових символів (крім тире), у форматі: XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX
3. Ознайомтеся з обов'язковими юридичними документами. Ви повинні поставити галочки, підтверджуючи свою згоду як з *Ліцензійною угодою користувача програмного забезпечення Viasecurity*, так і з *Заявою про захист даних*. Натисніть **ОК**, щоб продовжити.
4. Завершіть процес, натиснувши **Активувати**.

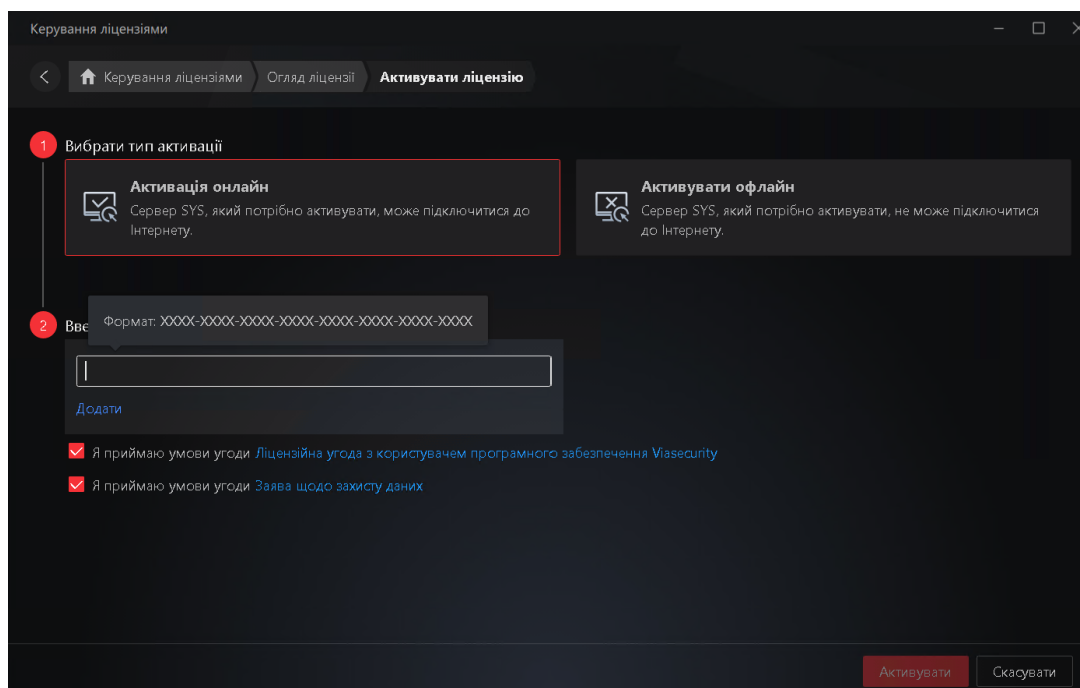


Рисунок 2.1 Активация ліцензії в режимі онлайн

2.1.2 Спосіб офлайн-активації

Для захищених середовищ без прямого доступу до Інтернету система підтримує локалізовану процедуру офлайн активації, що вимагає використання окремого пристрою, підключеного до Інтернету.

Процедура:

1. У меню активації виберіть метод **Активувати офлайн**.
2. Введіть придбаний ключ активації. Кілька ключів можна додати, натиснувши кнопку **Додати**.
 - а) Переконайтеся, що ключ активації складається саме з 32 буквено-цифрових символів (крім тире) у форматі: XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX.
3. Ознайомтеся з обов'язковими юридичними документами. Ви повинні поставити галочки, підтверджуючи свою згоду як з *Ліцензійною угодою користувача програмного забезпечення Viasecurity*, так і з *Заявою про захист даних*. Натисніть **ОК**, щоб продовжити.
4. Натисніть **Згенерувати файл запиту**. Ця дія створює файл із назвою *ActivationRequestFile.bin*. Виберіть **Переглянути файл**, щоб знайти місце розташування файлу та перенести його наприклад, на портативний USB-накопичувач, або перевірте свої записи про завантаження на головній сторінці.
5. Перенесіть цей створений файл на іншу робочу станцію, яка має активний доступ до Інтернету.
6. На підключеній робочій станції перейдіть на офіційний портал ліцензування через веб-браузер: <https://kms.fc-solution.com/active#/active>

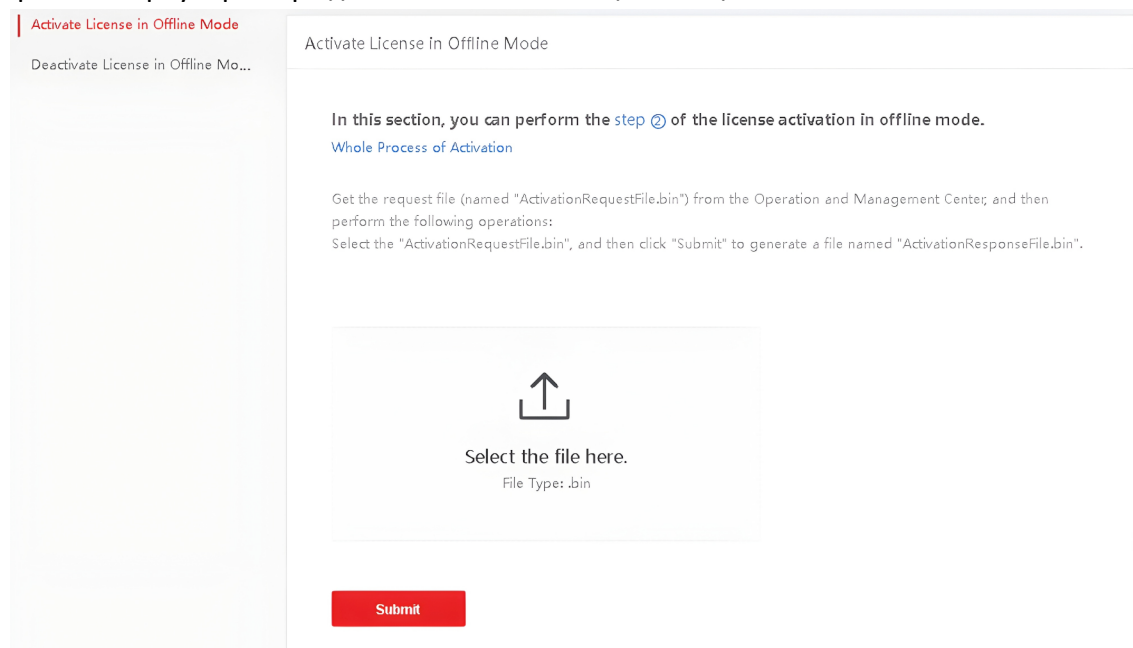


Рисунок 2.2 Активувати ліцензію в офлайн-режимі

7. Завантажте файл *ActivationRequestFile.bin* на веб-портал і натисніть **Надіслати**.
8. Портал згенерує файл *ActivationResponseFile.bin*. Завантажте та надійно збережіть цей файл на свій портативний USB-накопичувач.

9. Поверніться до вашої автономної робочої станції Viasecurity Control Center. На екрані **Активувати ліцензію** натисніть, щоб переглянути файл *ActivationResponseFile.bin*, або перетягніть файл безпосередньо у визначену область.
10. Завершіть налаштування, натиснувши **Активувати**.

2.2 Додавання пристроїв

Система дозволяє інтегрувати різноманітне обладнання, включаючи пристрої систем відеоспостереження, відеодомофони та обладнання контролю доступу. Ви можете підключити їх трьома основними способами: автовиявлення, груповий імпорт або ручне додавання.

Додати пристрій

Перейдіть з головної панелі управління до **Система → Керування пристроєм → Додати пристрій**. Звідси виберіть бажаний метод додавання (Автовиявлення, груповий імпорт, або ручне додавання). Крім того, ви можете додати нове обладнання, скориставшись призначеним ярликом або клацнувши правою кнопкою миші безпосередньо в певній області інтерфейсу.

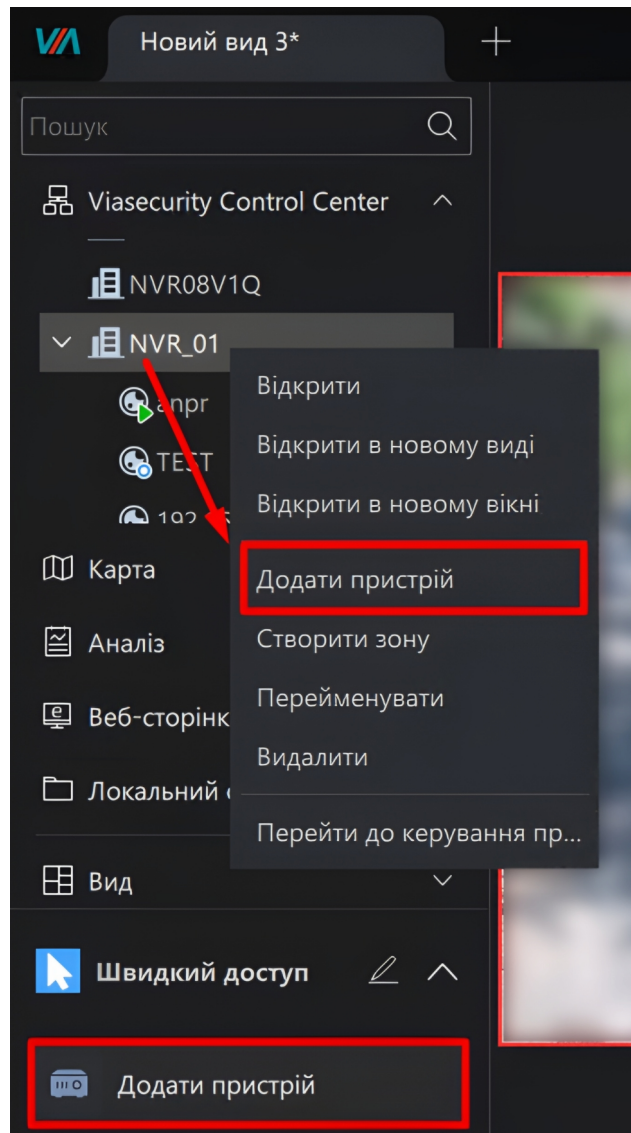


Рисунок 2.3 Інші способи додавання пристроїв

Таблиця 2.1 Додавання пристрою

Режим	Опис
Автовиявлення	Виберіть цей варіант, щоб знайти обладнання, яке використовує ту саму локальну мережу (LAN), що й ваш клієнт або сервер. Доступні дії: Використовуйте функцію Вказати діапазон IP-адрес, щоб сканувати всі мережі, до яких має доступ клієнт, навіть у різних підмережах. (Примітка: для роботи потрібно увімкнути службу ONVIF.) Натисніть «  », щоб редагувати IP-адресу пристрою та номер порту.

	Натисніть «  », щоб скинути пароль. Натисніть «  », щоб відфільтрувати за статусом Активовано або Неактивовано, а також за типом пристрою. Якщо апаратне забезпечення відображає статус неактивовано, натисніть Активувати, щоб ініціалізувати його перед додаванням до системи. Налаштуйте часовий пояс пристрою. За замовчуванням він відображає місцевий час сервера. Узгодження часових поясів пристрою та сервера дозволяє здійснювати запис відео як на апаратному забезпеченні, так і на сервері запису; невідповідність часових поясів обмежує зберігання даних виключно самим пристроєм. Ручні налаштування часового поясу автоматично синхронізуються з підключеними пристроями кожні 24 години (за винятком обладнання, підключеного через ONVIF).
Груповий імпорт	Використовуйте цей метод для ефективної реєстрації декількох пристроїв одночасно, якщо їхні мережеві дані (IP-адреса, номер порту, ідентифікатор та секретний ключ) вже відомі, що дозволяє швидко додавати їх без перевірки дійсності. - Цей підхід рекомендується для обладнання, яке наразі не підключене до мережі або знаходиться в мережі, відмінній від мережі сервера чи клієнта. - Встановіть часовий пояс пристрою, який за замовчуванням відповідає конфігурації сервера. Синхронізовані часові пояси дозволяють використовувати подвійне зберігання (на сервері та пристрої), тоді як розбіжні налаштування обмежують записи локальним сховищем пристрою. - Налаштування користувацьких часових поясів оновлюються на всьому обладнанні кожні 24 години (за винятком пристроїв, що використовують протоколи ONVIF або сторонні SDK).
Додати вручну	Виберіть цей варіант, щоб окремо зареєструвати пристрій, використовуючи його конкретні дані (IP-адресу, порт, ім'я користувача та пароль).

	• Ви повинні вказати відповідний протокол зв'язку та надати необхідні дані про обладнання. Підтримувані базові протоколи включають: протокол VIA Security, приватний протокол Hikvision, приватний протокол Dahua, протокол ONVIF, протокол Hanwha SDK та Протокол Axis SDK. (Примітка: з міркувань безпеки перед використанням протоколу ONVIF необхідно вручну його увімкнути. Крім того, обладнання, інтегроване через ONVIF або сторонні SDK, вимагає ретельного ручного налаштування часового поясу.
--	--

Після успішного додавання обладнання клацніть правою кнопкою миші на будь-якому записі у списку пристроїв, щоб відкрити додаткові параметри керування. Система також підтримує відображення версій прошивки та серійних номерів для камер, підключених через NVR.

Налаштування часових поясів

Виділіть потрібні пристрої та натисніть **Часовий пояс**, щоб змінити їхні налаштування часу. Встановіть прапорець **Установити часовий пояс вручну**, якщо ви хочете самостійно визначити часовий пояс; якщо прапорець не встановлено, програмне забезпечення автоматично синхронізується з існуючим часовим поясом обладнання.

(Примітка: налаштування часового поясу можна застосувати лише до пристроїв, які наразі підключені до мережі.)

Віддалене налаштування пристрою

Щоб дистанційно налаштувати параметри пристрою, наведіть курсор на його запис, клацніть правою кнопкою миші та виберіть **Віддалена конфігурація пристрою**.

Ручна синхронізація налаштувань обладнання контролю доступу

Коли обладнання не підключено до мережі, зміни конфігурації зберігаються в кеші платформи. Після відновлення з'єднання ці параметри, що знаходяться в черзі, необхідно вручну синхронізувати з пристроєм. Крім того, ручне застосування правил контролю доступу платформи (таких як блокування декількох дверей, Багаторазова автентифікація або постійні стани блокування/розблокування) необхідне щоразу, коли ви виконуєте заводське скидання налаштувань пристрою, відновлюєте системну базу даних або встановлюєте двері в стан залишатись заблокованими/розблокованими. Щоб це виконати, перейдіть до інтерфейсу **Контроль доступу** та виберіть **Застосувати вручну**.

(Примітка: Якщо пристрої налаштовані на зйомку зображень як відповідь на взаємодію, ці візуальні матеріали можуть передаватися на сервер через HTTP.)

2.2.1 Додавання сервера та управління даними

Для ефективного розподілу медіа в режимі реального часу між різними пристроями та клієнтами ви можете підключити зовнішній сервер потокового передавання до своєї інфраструктури. Впровадження цієї архітектури оптимізує обробку відеоданих, гарантуючи оперативний доступ до медіапотоків у разі потреби.

Додати сервер

На головній сторінці перейдіть до **Система → Керування пристроями → Сервер**.

Сервер призначений для перегляду в реальному часі, відтворення, відеодомофона тощо. Макс. канал потокового передавання — це максимальна кількість каналів потокового передавання, яку може підтримувати сервер.

Після додавання серверів ви можете виконувати подальші операції зі списком серверів.

Перегляд налаштування сигналу тривоги

Наведіть курсор на один із серверів, клацніть правою кнопкою миші та виберіть **Переглянути налаштування сигналу тривоги**, щоб переглянути та редагувати конфігурації тривоги відповідного сервера.

Дистанційне налаштування

Наведіть курсор на один із серверів, клацніть правою кнопкою миші та виберіть **Віддалена конфігурація пристрою**, щоб відкрити веб-сторінку налаштувань пристрою.

Перегляд інформації про сервер

Щоб отримати детальну інформацію про операційні показники сервера, наведіть курсор на сервер, клацніть правою кнопкою миші та виберіть **Перегляд подробиць**.

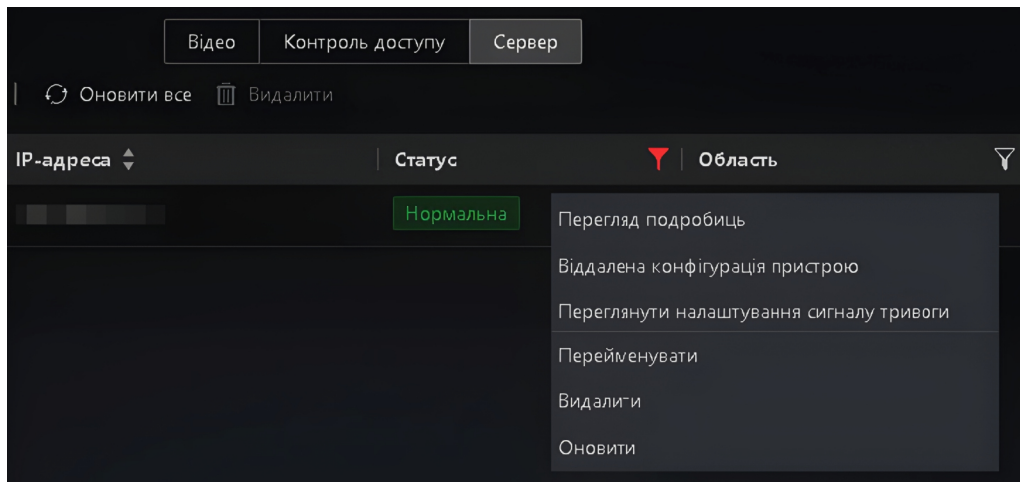


Рисунок 2.4 Перегляд деталей сервера

У цьому вікні доступні такі дії:

- Моніторинг робочого стану (як нормального, так і аномального) безпосередньо під назвою сервера. За замовчуванням інтерфейс надає пріоритет відображенню аномальних станів. Розгорніть вікно, натиснувши Більше, щоб переглянути повний журнал стану.
- Змінити параметри базової конфігурації сервера.

2.3 Локальна конфігурація

У цьому розділі описано, як налаштувати параметри, специфічні для клієнта, зокрема параметри відтворення відео, сповіщення та загальну поведінку програми.

Щоб змінити ці налаштування, натисніть своє **ім'я користувача** у верхньому правому куті інтерфейсу та перейдіть до розділу **Локальна конфігурація**.

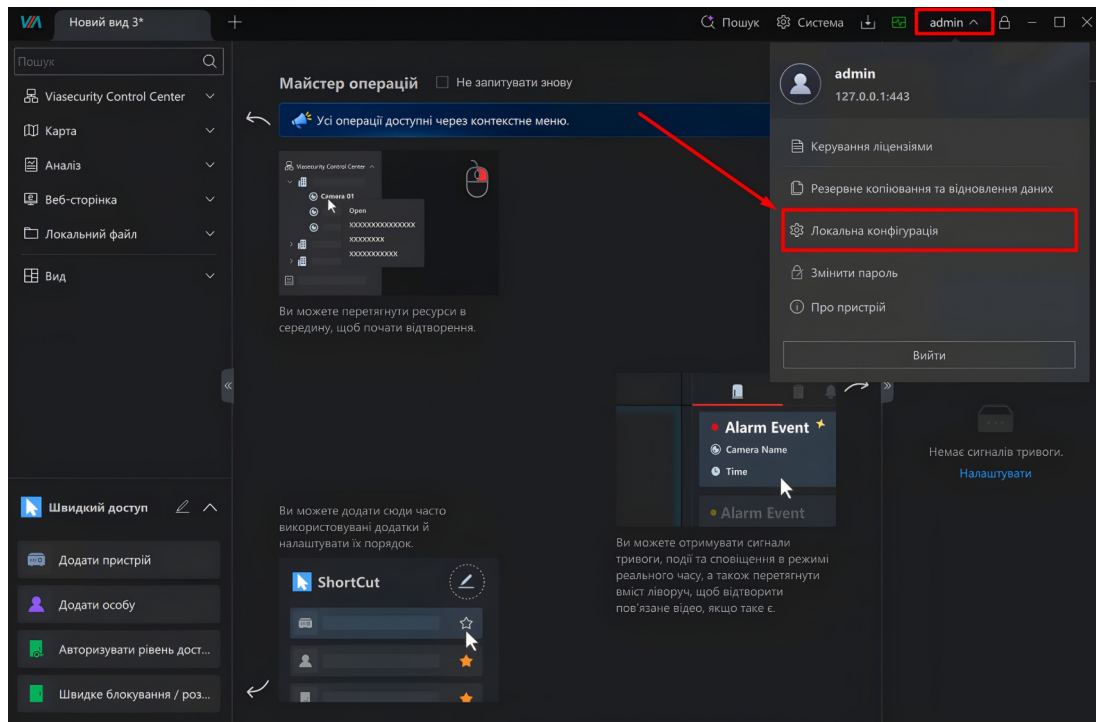


Рисунок 2.5 Локальна конфігурація

2.3.1 Події та сигнали тривоги

Відображення

- **Аудіо:** увімкнення або вимкнення всіх звукових сповіщень (таких як сирени або звукові сигнали) для поточного клієнта.
- **Спливаюче вікно:** увімкнення або вимкнення візуальних вікон сповіщень. За замовчуванням ці вікна з'являються в центрі екрана, але система збереже будь-які ручні налаштування їхнього положення для майбутніх сеансів.

(Примітка: якщо звук або спливаючі вікна вимкнені, пов'язані з ними дії все одно будуть запускатися, але не будуть помітні для користувача.)

Звук сигналу тривоги

- **Голосова підтримка(потрібна підтримка ОС):** Використовує можливості перетворення тексту в мову операційної системи для озвучування описів сповіщень.
- **Локальні аудіофайли:** запускає відтворення завантажених користувачем файлів. Налаштований голосовий текст не матиме значення.

Налаштування циклу відтворення

- **Повторювати відтворення аудіо:** Увімкніть цей перемикач, якщо хочете, щоб вибраний звук сигналу тривоги відтворювався повторно, а не лише один раз.

- **Кількість відтворень:** Якщо увімкнено функцію повторного відтворення, скористайтесь цим списком, щоб встановити точну кількість разів, скільки система має відтворити аудіофайл.

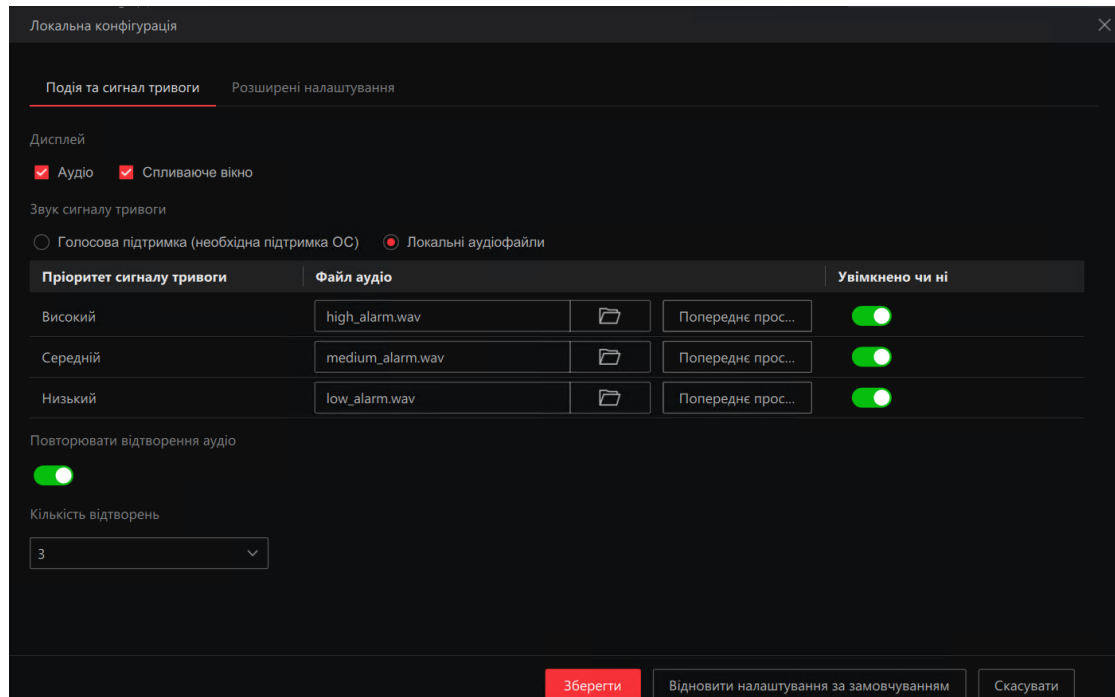


Рисунок 2.6 Налаштування подій та сигналів тривоги

2.3.2 Розширені налаштування системи

Шлях збереження файлів

- Виберіть папку призначення для експортованих медіафайлів, включаючи зображення, завантажені відео та записи, зроблені вручну.

Режим доступу до трансляції

Визначте спосіб доступу до всіх доданих пристроїв кодування та декодування.

- **Автоматична оцінка:** система вибирає найефективніший шлях на основі мережевих доменів. Прямі потоки використовуються, якщо клієнт і пристрій мають спільний домен; в іншому випадку дані маршрутизуються через сервер потокового передавання.
- **Прямий доступ:** коли вибрано цей параметр, програмне забезпечення клієнта встановлює з'єднання та отримує відеопотік безпосередньо з кінцевого пристрою, повністю оминаючи проміжний сервер потокового передавання. Використання цього режиму рекомендується, коли необхідно зменшити навантаження на центральний сервер, за умови, що робоча станція клієнта має стабільний прямий мережевий доступ до пристрою.
- **Через сервер потокової передачі:** Доступ до всіх даних здійснюється через сервер потокового передавання, щоб мінімізувати навантаження на апаратне

забезпечення, особливо в середовищах з великою кількістю активних клієнтів.

2.3.3 Налаштування відображення відео

Щоб отримати доступ до цих налаштувань, клацніть правою кнопкою миші на будь-якій вільній ділянці головної панелі керування.

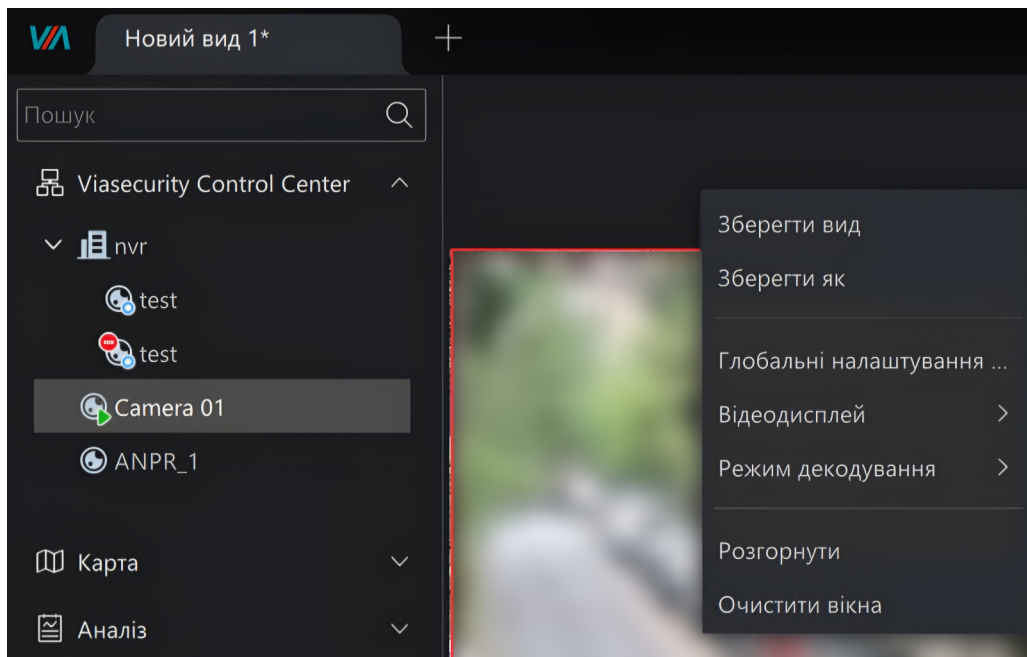


Рисунок 2.7 Доступ до основних налаштувань відео

Глобальна конфігурація потоку

- Якщо ви встановите прапорець **Потокова адаптація**, програмне забезпечення автоматично перемикатиметься між основним і допоміжним потоками залежно від роздільної здатності вікна перегляду.
- **Ручне налаштування роздільної здатності:** Ви можете вибрати бажану роздільну здатність (від «Дуже велика» до «Мала»), щоб збалансувати якість відео та навантаження на мережу.
- **Фіксований режим:** Якщо адаптація вимкнена, програма використовує конкретний вибраний основний або допоміжний потік.

Масштаб перегляду (Відеодисплей)

- **Оригінальна роздільна здатність:** відображає відео у фактичних розмірах (що може призвести до появи чорних рамок).
- **Повнекранный режим у межах вікна:** розширює відео, щоб заповнити всю область перегляду.

Режим декодування

- Апаратне декодування здійснюється на базі графічного процесора (GPU), тоді як програмне декодування — на базі центрального процесора (CPU). Оберіть режим декодування відповідно до продуктивності вашого графічного процесора (GPU) та центрального процесора (CPU).

Розділ 3 Відеоспостереження

Моніторинг відео є основним компонентом безпеки Viasecurity Control Center. Цей модуль надає операторам можливість візуального нагляду за захищеними середовищами в режимі реального часу, миттєвих сповіщень про спрацювання сигналів тривоги або подій, а також комплексного відстеження різних цільових типів на всій території об'єкта.

- Налаштування та підготовка системи
 - Додавання пристроїв кодування
 - Налаштування обладнання
- Основні інструменти спостереження
 - Операції з відео в реальному часі та відтворенням
 - Управління PTZ у реальному часі
 - Моніторинг за допомогою камер на карті
- Порівняння зображень облич та виявлення людських тіл
 - Додавання бібліотек зображень облич та зображень облич
 - Перегляд відео, пов'язаних із розпізнаванням обличчя та людського тіла
 - Пошук розпізнаних зображень обличчя та зображень людського тіла
 - Пошук об'єктів за зображенням
- Операції з транспортними засобами
 - Додавання списків транспортних засобів та транспортних засобів
 - Перегляд відео, пов'язаного з моніторингом транспортних засобів
 - Пошук та експорт подій ANPR
- Функції інтелектуального пошуку
 - Смарт-пошук / VCA
 - Targettrace та object search
- Аналітика та звіти щодо підрахунку людей

3.1 Налаштування та підготовка системи

3.1.1 Додавання пристроїв кодування

Перш ніж використовувати такі основні функції, як пряма трансляція, зберігання відео або тригери подій, оператори повинні спочатку підключити до платформи все фізичне обладнання для кодування, включаючи IP-камери та мережеві відеореєстратори (NVR).

- У головному інтерфейсі робочої області перейдіть до **Система → Керування пристроями → Додати пристрій**, щоб зареєструвати нове обладнання. (Див.

розділ 2.2 Додавання пристроїв для отримання вичерпних інструкцій щодо сполучення.)

3.1.2 Налаштування обладнання

Після підключення обладнання адміністратори можуть налаштувати робочі параметри. Доступні опції інтерфейсу, такі як графіки запису, ресурси вводу-виводу, можливості аналітики та розширені налаштування мережі або PTZ, динамічно коригуватимуться залежно від конкретної моделі, протоколу підключення та методу інтеграції.

- Перейдіть до **Система → Керування пристроями**, щоб переглянути перелік обладнання. Клацніть безпосередньо на назві певного обладнання, щоб відкрити його панель налаштувань.

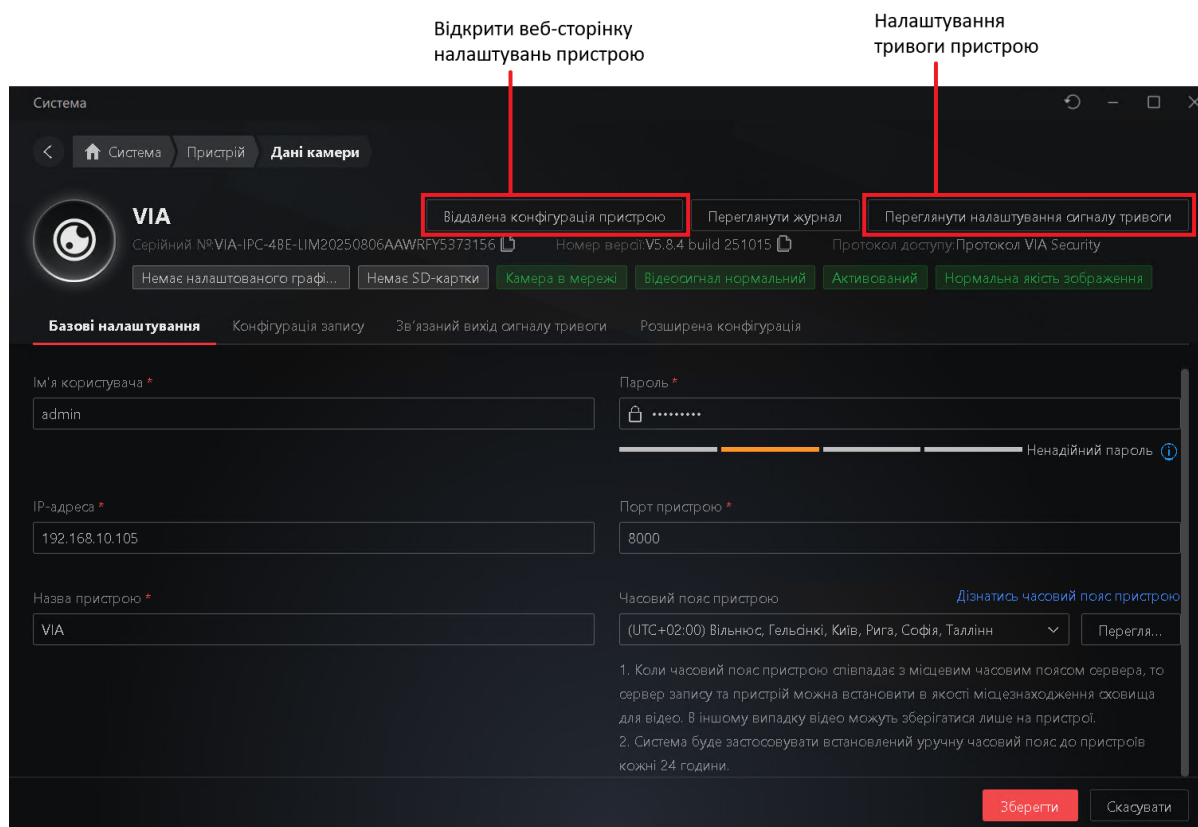
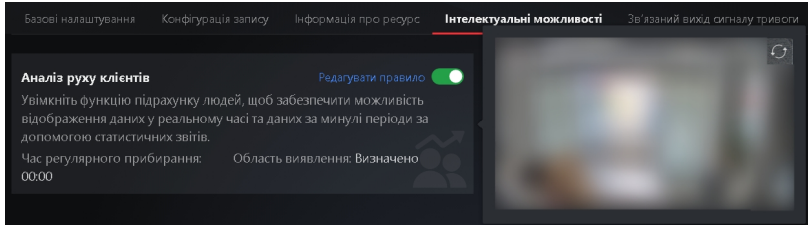


Рисунок 3.1. Деталі камери

(Примітка: Деталі пристрою залежать від типу пристрою, протоколу доступу та методу додавання пристрою. Налаштування повинні відповідати фактичній ситуації.)

Таблиця 3.1 Вступ до вкладки «Деталі пристрою»

Назва вкладки	Опис
Конфігурація запису	Виключно для апаратного забезпечення камери, використовується для визначення правил зберігання.

Інформація про ресурс	Відображає всі периферійні компоненти, підключені до обладнання, такі як входи/виходи сигналізації та підключені камери. Оператори можуть клацнути правою кнопкою миші на будь-якому ресурсі зі списку, щоб виконати певні команди, наприклад, запустити вбудований веб-портал обладнання, переглянути журнали, керувати сигналами тривоги або видалити елемент.
Інтелектуальні можливості	Виділяє доступні інструменти інтелектуальних функцій (наприклад, TargetTrace, ANPR, розпізнавання обличчя), пов'язані з обчислювальною потужністю обладнання та активною ліцензією. Оператори повинні увімкнути ці функції, перш ніж їх можна буде застосувати глобально. На цій вкладці також здійснюється управління клонуванням та редагуванням правил. 
Зв'язаний вихід сигналу тривоги	Виключно для камер, що дозволяє користувачам відображати фізичні виходи тривоги безпосередньо на макеті прямої трансляції.
Розширена конфігурація	Використовується для призначення протоколів мережевої передачі та визначення профілів медіа та увімкнення шифрування сигналу. Якщо система не може автоматично розпізнати функції панорамування, нахилу та зуму (PTZ) камери, адміністратори можуть вручну примусово встановити класифікацію PTZ тут, щоб увімкнути пряме керування через інтерфейс.

Визначення параметрів зберігання та запису

Коли додається нова камера, Viasecurity Control Center автоматично імпортує її існуючий графік запису. За замовчуванням система буде записувати у форматі подвійного потоку, якщо це дозволяє апаратне забезпечення, надаючи операторам можливість гнучко перемикає якість відео під час відтворення архівних записів. Переведіть перемикач **Запис** у положення **увімкнено**, щоб отримати доступ до таких параметрів:

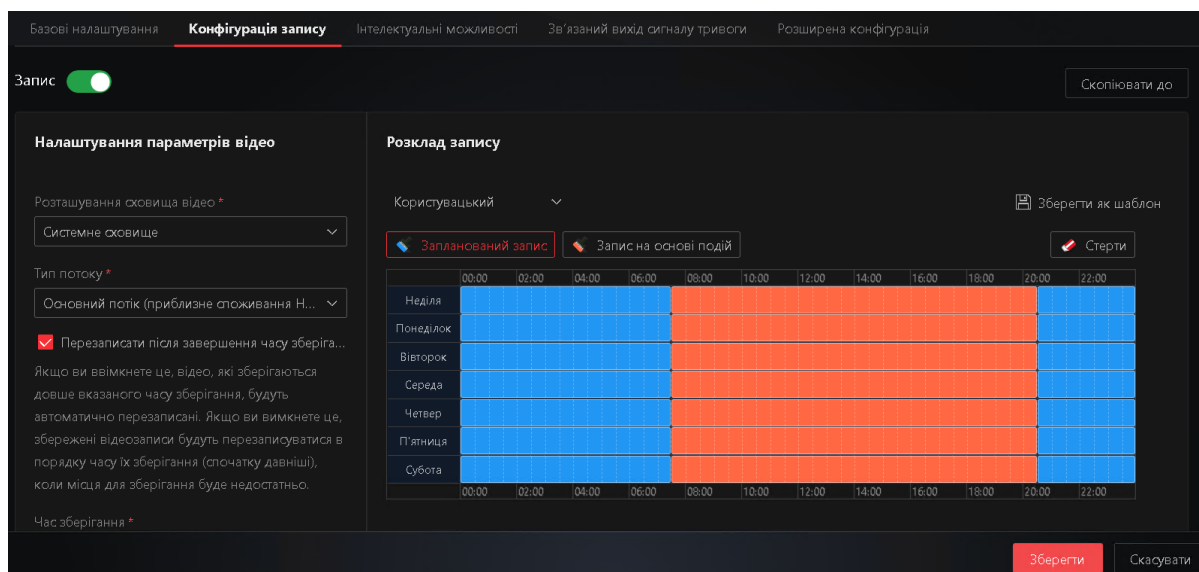


Рисунок 3.2 Конфігурація запису

Місце зберігання відео

- Визначте, чи зберігатимуться архівні записи на центральних серверах системи чи на локальних дисках пристроїв.

(Примітка: якщо ви використовуєте системне сховище разом із шифруванням потоку, ви повинні суворо контролювати свої ключі шифрування. Оновлення ключа шифрування без збереження попереднього зробить усі історичні записи, зашифровані за допомогою старого ключа, назавжди недоступними для читання.)

Тип потоку

Виберіть **Основний потік**, **Додатковий потік** або **Подвійний потік** залежно від пропускної здатності мережі та бажаної роздільної здатності відтворення.

Зберігання даних

Увімкніть функцію **Перезаписати після закінчення терміну зберігання**, щоб автоматично видаляти записи, коли вони перевищують визначений термін зберігання. Якщо ця функція вимкнена, система просто перезапише найстаріші доступні блоки відео, коли ємність сховища буде вичерпана.

Автоматичне зворотне копіювання

Механізм відмовостійкості, який зберігає відео локально на пристрої під час збою мережі. Після відновлення з'єднання записи передаються на основний накопичувач. (Примітка: ця функція працює лише тоді, коли тип потоку встановлено на «Основний потік», і вимагає сумісних камер виробництва Viasecurity або Hikvision.)

Розклад запису

Визначте, коли камера має записувати. Оператори можуть призначати готові шаблони або створювати власні вікна, розрізняючи безперервний запис 24/7 та запис, що запускається подіями.

Створити резервну копію відео

Увімкніть резервне зберігання. Це створює вторинний архів на резервному пристрої, забезпечуючи доступ до відеозаписів навіть у разі пошкодження основного сховища або втрати даних.

Скопіювати до

Використовуйте цю дію, щоб швидко застосувати ваші налаштування запису до інших сумісних камер у вашій мережі.

3.2 Основні інструменти спостереження

Viasecurity Control Center надає операторам основні можливості для активного спостереження за об'єктом. Ці базові функції включають потокову передачу відео в реальному часі, пошук записів з архіву, точне керування панорамуванням, нахилом і зумом (PTZ), а також просторове відстеження за допомогою інтерактивних планів поверхів і карт.

3.2.1 Операції з відео в реальному часі та відтворенням

Оператори можуть безперешкодно запускати та керувати відеопотоками для окремих або об'єднаних у кластер апаратних одиниць.

Моніторинг окремого пристрою

- Щоб запустити трансляцію в режимі реального часу, просто двічі клацніть на потрібному пристрої у списку обладнання, перетягніть його піктограму на матрицю перегляду або клацніть правою кнопкою миші на елементі та виберіть **Відкрити**.

Перегляд архівних записів

- Під час активного моніторингу потоку оператори можуть перейти до архівних відеозаписів, перетягнувши хронологічну шкалу в зворотному напрямку або натиснувши піктограму **Відтворення**, розташовану в нижньому лівому куті панелі перегляду.

Моніторинг декількох пристроїв

- Щоб одночасно переглядати кілька потоків, утримуйте клавішу Ctrl і клацніть, щоб вибрати кілька камер. Потім їх можна перетягнути на матрицю перегляду разом або відкрити через контекстне меню.

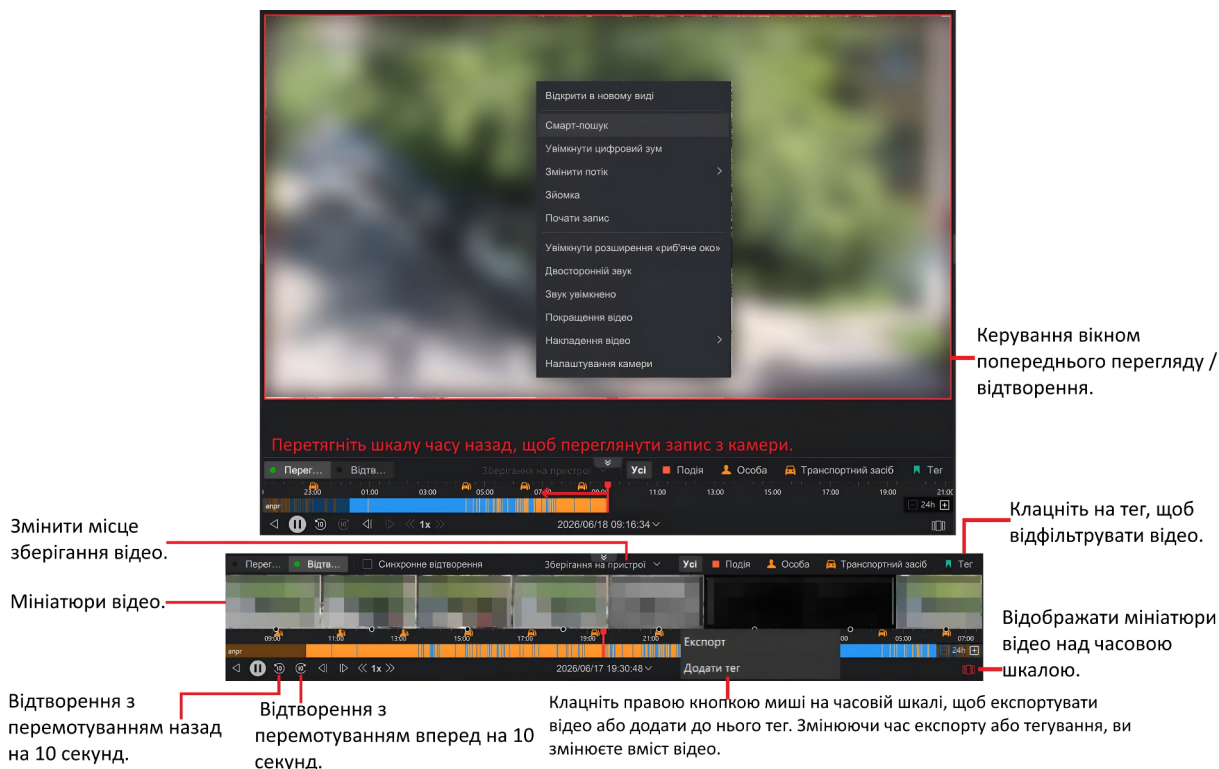


Рисунок 3.4 Запуск прямого перегляду / відтворення однієї камери

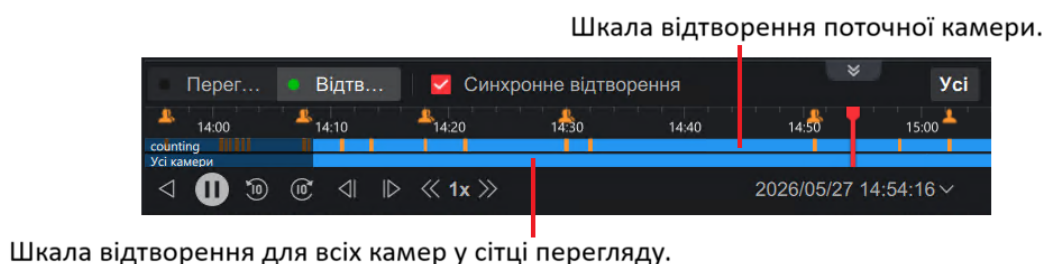


Рисунок 3.5 Синхронне відтворення

Операції з потоком

Клацнувши правою кнопкою миші на панелі перегляду або скориставшись іконками керування в правому нижньому куті, ви відкриєте набір інструментів для роботи як з прямими, так і з архівними потоками:

- Відкрити в новому виді:** відкрийте поточний канал у окремому вікні перегляду.
- Смарт-пошук / пошук VCA:** намалюйте власні обмежувальні рамки безпосередньо на відеозаписі, щоб запустити виявлення людей, транспортних

засобів або аномальних рухів у цій зоні. Результати відображаються на бічній панелі для швидкого перегляду або детального аналізу.

- **TargetTrace / Пошук об'єктів:** виділіть конкретні профілі людей або транспортних засобів, щоб просканувати зняті зображення на наявність відповідних цілей.
- **Увімкнути цифровий зум:** збільшуйте певні зони, натискаючи на піктограму лупи, малюючи визначений кадр над областю, що вас цікавить, або прокручуючи коліщатко миші.
- **Змінити потік:** перемикайтеся між профілями потоку «Основний», «Додатковий», «Четвертий» або «Плавний» залежно від доступної пропускної здатності мережі.
- **Зйомка:** знімайте миттєві знімки з потоку або експортуйте конкретні сегменти відео під час відтворення.
- **Почати запис:** змусьте систему зробити локальний запис під час активного спостереження в реальному часі.
- **Модифікації об'єктива та виду:** активуйте «Риб'яче око» для розширення, щоб виправити спотворення ультраширокої перспективи, налаштуйте візуальні параметри, такі як яскравість і насиченість, або накладіть важливі метадані безпосередньо на потік.
- **Активне стримування та аудіо:** ініціюйте двосторонній голосовий зв'язок, вмикайте або вимикайте прослуховування аудіо або вручну запускайте сигнальні вогні камери.

(Примітка: апаратне забезпечення повинно підтримувати ці функції.)

Теги: людина/транспортний засіб

Щоб система могла успішно позначати блоки відеозаписів тегами «Людина» або «Транспортний засіб», необхідно виконати кілька попередніх умов:

- На підключеному обладнанні повинні бути активно налаштовані правила VCA (наприклад, перетин лінії, вторгнення в область).
- Виявлення людей та/або транспортних засобів має бути увімкнено.
- Відповідна підписка на події повинна бути активною в Viasecurity Control Center.
- Відео, записані до додавання пристрою на платформу, не будуть позначені.

Комбінації клавіш для відтворення

Оператори можуть пришвидшити перегляд відеозаписів за допомогою стандартних комбінацій клавіш.

Таблиця 3.2 Комбінації клавіш

Клавіша	Функція
Пробіл	Відтворення / Пауза
↑	Перемотка вперед

↓	Перемотка назад
←	Відтворення з відмотуванням по одному кадру
→	Швидке перемотування вперед по кадрах
[	Відтворення у зворотному напрямку
]	Звичайне відтворення

3.2.2 Управління PTZ у реальному часі

Ви можете керувати PTZ камерами під час перегляду в режимі реального часу.

Після запуску камери з підтримкою PTZ у сітку перегляду (двічі клацнувши, перетягнувши або клацнувши правою кнопкою миші) знайдіть і клацніть на відповідну піктограму PTZ  у правому нижньому куті панелі. Ця дія відкриває спеціальну накладку керування у правій частині екрана, що дозволяє персоналу служби безпеки вручну керувати об'єктивом, регулювати рівні оптичного зуму та налаштовувати автоматичні маршрути патрулювання або фіксовані попередньо встановлені кути огляду.

Два способи керування напрямком повороту камери PTZ:

- Натисніть кнопку посередині, а потім перетягніть стрілку в потрібному напрямку. Швидкість повороту камери PTZ збільшується, якщо відсунути стрілку далі від центральної кнопки.
- Клацніть на зображенні відео, щоб камера PTZ повернула в бік місця, де було зроблено клік мишею.

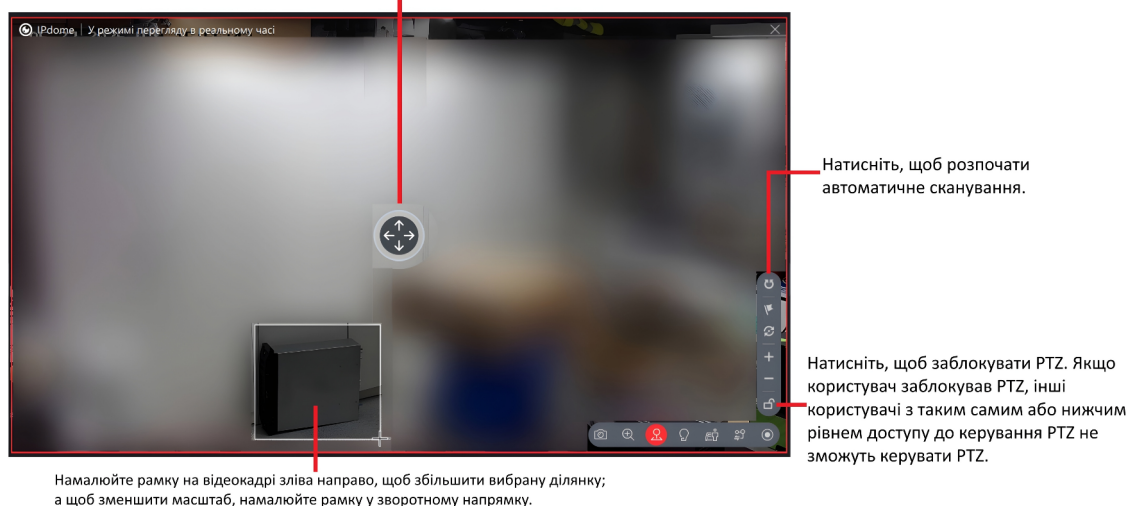


Рисунок 3.6 Управління PTZ

3.2.3 Моніторинг за допомогою камер на карті

Інтеграція карт в платформу надає просторовий контекст мережі спостереження, дозволяючи операторам моніторити активність та стан пристроїв на основі фізичних розташувань.

Щоб отримати доступ до карти об'єкта, перейдіть до модуля **Карта** та відкрийте потрібну схему, двічі клацнувши на ній, перетягнувши її у праве вікно або скориставшись контекстним меню. Інтерфейс працює у двох різних середовищах:

1. Режим налаштування

Використовується адміністраторами для нанесення координат камер, визначення географічних «гарячих» зон та налаштування типів маркерів ресурсів, що відображаються на карті.

2. Режим моніторингу

Призначений для активного спостереження. Оператори можуть натиснути на будь-яку піктограму камери, закріплену на карті, щоб миттєво створити спливаюче вікно з прямим переглядом цього пристрою.

Додати карту

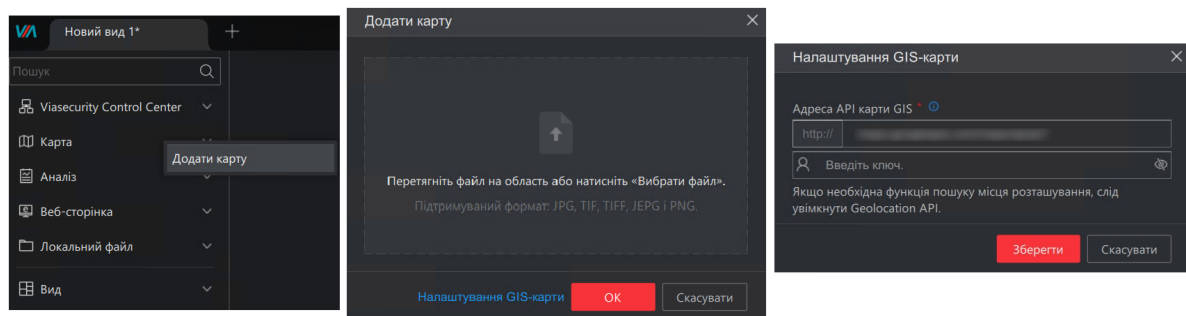


Рисунок 3.7 Додати GIS-карту

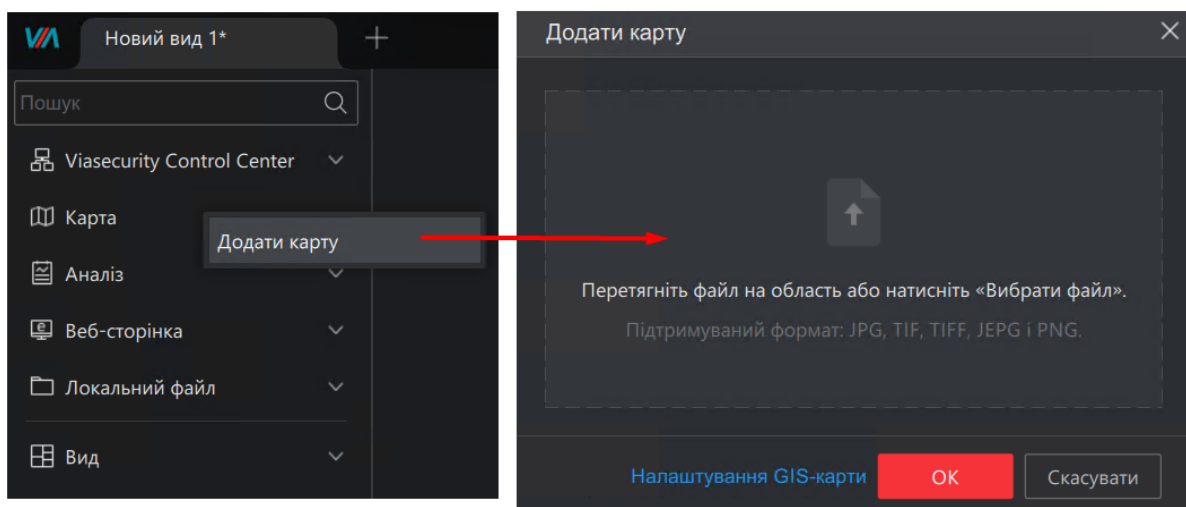


Рисунок 3.8 Додати статичну карту

Режим налаштування

На статичній карті після налаштування масштабу клацніть правою кнопкою миші на камері, щоб налаштувати її кут огляду. Для камер із функцією PTZ кут огляду відображається автоматично.

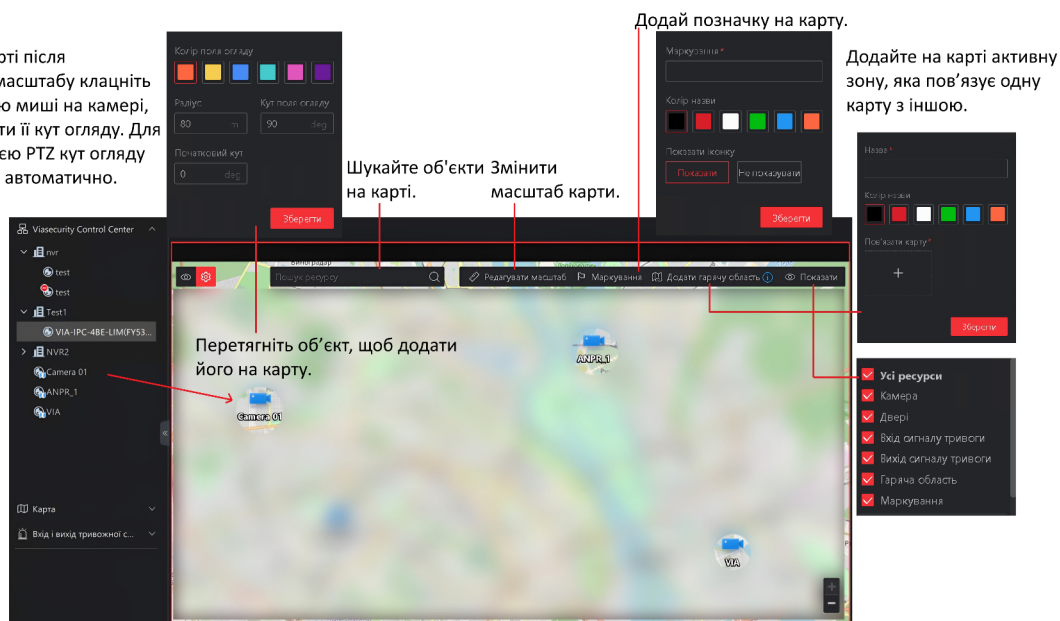


Рисунок 3.9 Підтримувані операції з картою в режимі конфігурації

Режим моніторингу

Ви можете здійснювати моніторинг за допомогою камер на карті.

- Клацніть на камеру, щоб переглянути пряму трансляцію з камери на карті.

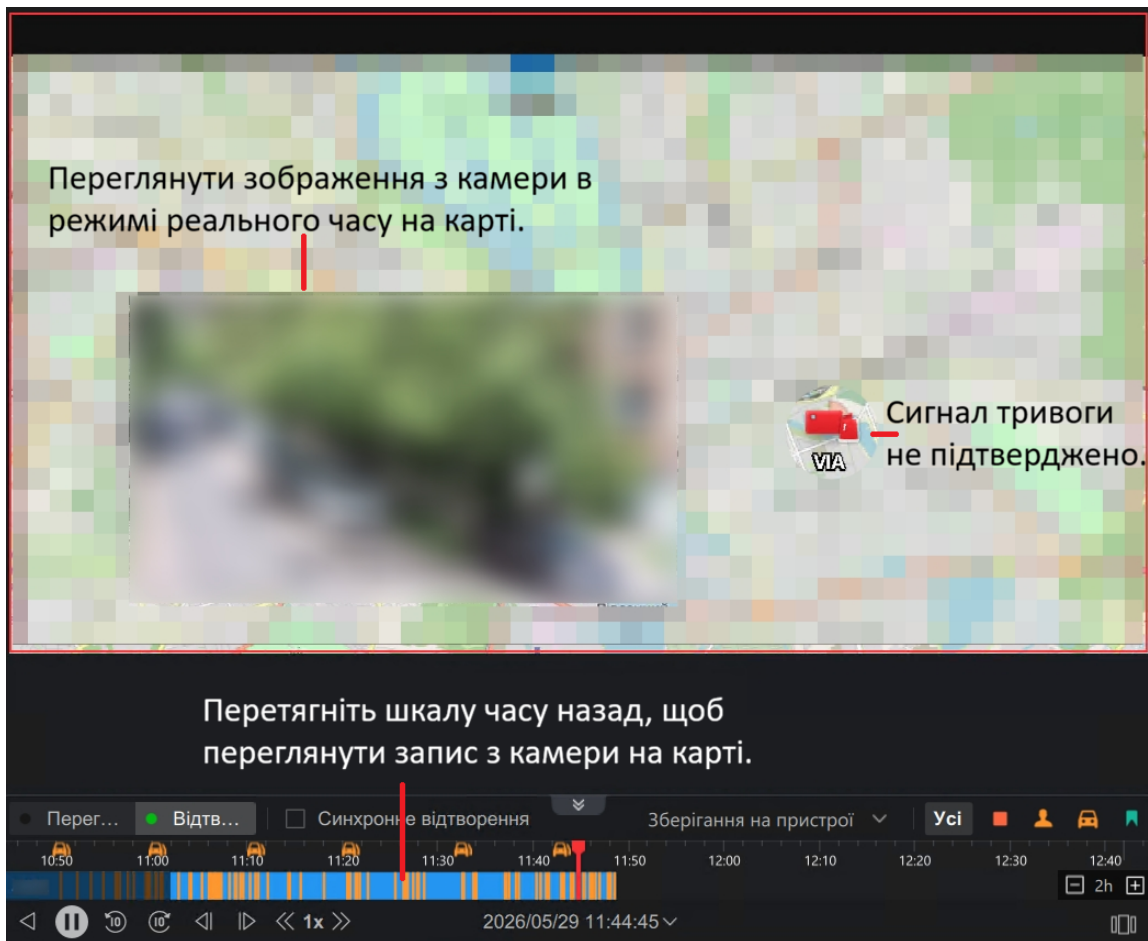


Рисунок 3.10 Перегляд прямого ефіру та відтворення запису з камери на карті

Щоб ефективно оглянути весь сектор, скористайтесь інструментом **Груповий вибір**, щоб накреслити периметр навколо групи камер на карті, а потім натисніть **Групове відтворення**, щоб одночасно транслявати всі вибрані пристрої. Крім того, оператори можуть утримувати клавішу Ctrl, щоб вибрати кілька піктограм на карті, і перетягнути їх у стандартні вікна перегляду поза межами області карти для постійного спостереження.

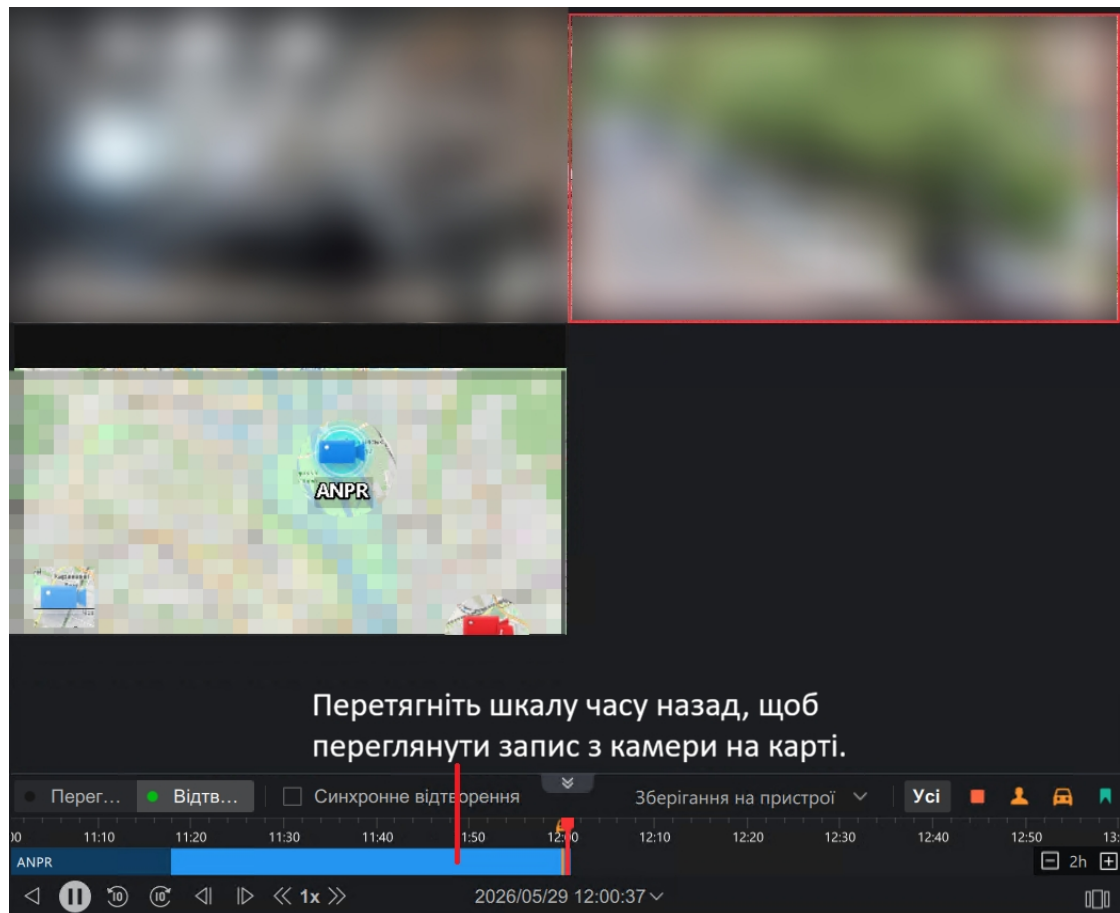


Рисунок 3.11 Пакетний перегляд прямого ефіру та відтворення з камер

3.3 Порівняння зображень облич та виявлення людських тіл

Порівняння облич оцінює знятий об'єкт у порівнянні з встановленими профілями для підтвердження збігу ідентичності, тоді як виявлення людської фігури ідентифікує осіб у різних фізичних середовищах. Ці інструменти є основою для проактивних заходів безпеки та широко застосовуються в роздрібній торгівлі та корпоративних середовищах.

Вимоги до обладнання

- Для використання цих функцій оператори повинні застосовувати сумісні камери розпізнавання облич або мережеві відеореєстратори (NVR). Зверніться до служби технічної підтримки, щоб отримати повний перелік підтримуваних моделей обладнання.

3.3.1 Додавання бібліотек зображень облич та зображень облич

Для ефективного використання функції розпізнавання облич адміністратори повинні створити бази даних, відомі як бібліотеки зображень облич, які містять базові зображення, що використовуються для зіставлення з активно знятим зображенням обличчя. Ці репозиторії дозволяють службам безпеки групувати дані про обличчя (наприклад, створюючи спеціальну бібліотеку для «Чорного списку»).

Перейдіть до Система → Бібліотека зображень облич, щоб отримати доступ до панелі управління даними про обличчя.

Створення бібліотеки зображень облич:

1. Знайдіть і натисніть кнопку **Додати бібліотеку зображень облич**, розташовану в нижньому лівому куті інтерфейсу.
2. Щоб прив'язати створену бібліотеку зображень облич з відповідною налаштованою камерою для розпізнавання облич, потрібно перейти в пункт **Дані камери → Інтелектуальні можливості** та натиснути кнопку **Редагувати правило**, після вибрати потрібні бібліотеки зображень облич (для роботи цієї функції мають бути активовані відповідні ліцензії).
3. Після створення бібліотеки та її прив'язки до конкретного обладнання для запису в інтерфейсі безпосередньо під назвою бібліотеки відобразиться загальна кількість та відповідні назви пов'язаних камер.

Додавання зображення обличчя:

1. Натисніть **Додати зображення обличчя** у нижньому лівому куті, щоб вручну зареєструвати профіль однієї особи.
2. Для масових операцій або альтернативних методів імпорту даних скористайтеся меню **Імпорт**, яке пропонує такі функції:
3. **Додати з наявних осіб**: витягніть еталонні зображення з профілів користувачів, які вже зареєстровані в системі.
4. **Імпорт інформації про обличчя через Excel**: Використовуйте стандартизований шаблон електронної таблиці для одночасного завантаження великого обсягу даних про обличчя.
5. **Імпорт зображень обличчя**: завантажте пакет файлів зображень, підготовлений вручну.
6. **Імпортувати бібліотеку зображень облич з пристрою**: синхронізуйте та витягніть існуючі бази даних облич, що зберігаються локально на підключених периферійних пристроях.

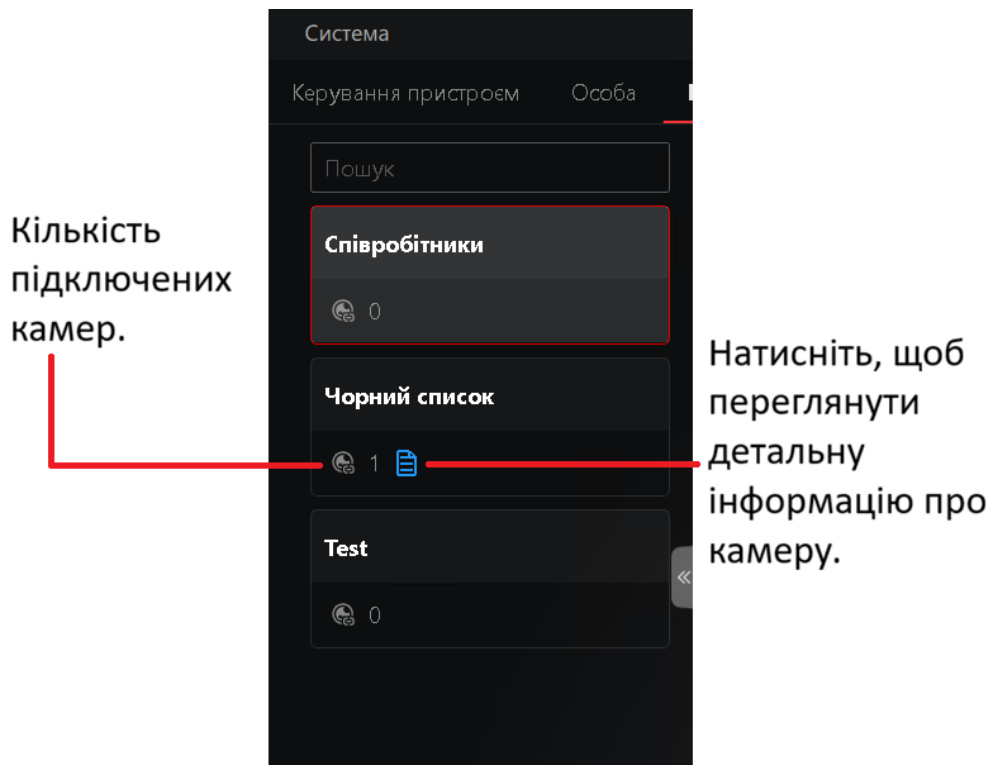


Рисунок 3.12 Камери, пов'язані з бібліотеками зображень облич

3.3.2 Перегляд відео, пов'язаних із розпізнаванням обличчя та людського тіла

Перегляд біометричних відеозаписів

Після налаштування камер розпізнавання облич та людських тіл оператори можуть переглядати прямі трансляції, доповнені біометричною аналітикою. Система безперервно відображає пов'язані події виявлення в режимі реального часу поряд з активною відеопотоком.

(Примітка: Переконайтеся, що інтегровано сумісні камери розпізнавання та що відповідні ліцензії на канали активно виділено, перейшовши до Керування ліцензіями → Огляд ліцензій).

Аналітика збігів у реальному часі

Миттєво переглядайте відсотки схожості збігів та ідентифікуйте конкретне сховище облич, пов'язане із зафіксованим об'єктом.

Швидкі взаємодії

Наведіть курсор на будь-яку активну подію, щоб відобразити короткий звіт даних, або клацніть правою кнопкою миші на події, щоб отримати доступ до додаткових дій, таких як запуск цільового пошуку пов'язаних знімків.

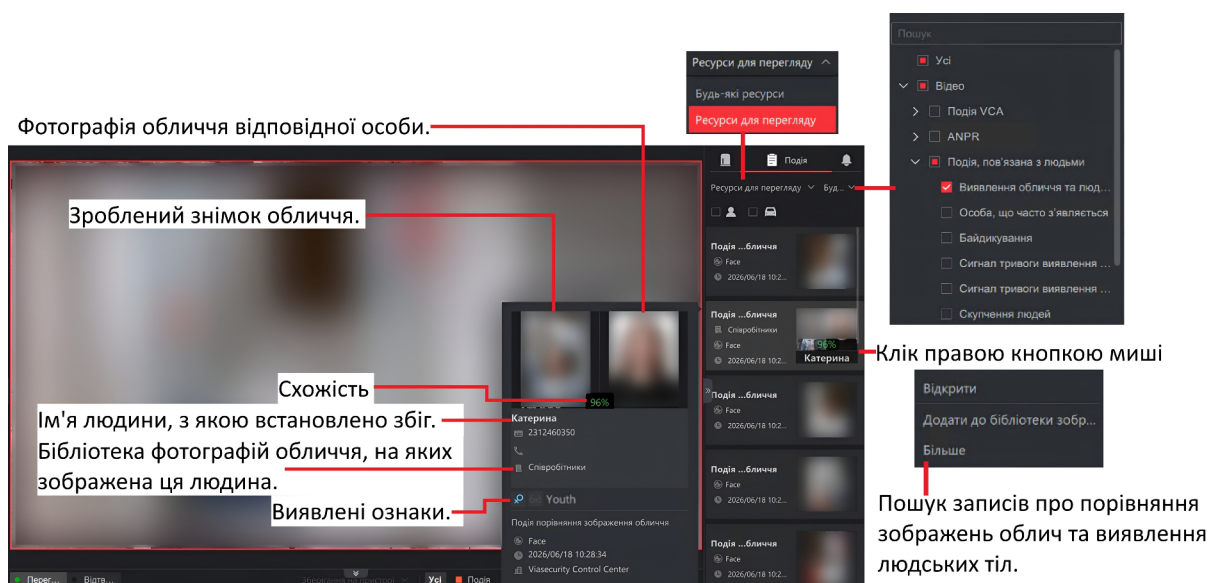


Рисунок 3.13 Деталі порівняння зображень облич

Візуальна перевірка

Відкрийте вікно **Деталі тривоги** під час збігу подій, щоб збільшити як знімок, зроблений у реальному часі, так і еталонне зображення з бази даних для точного візуального порівняння.

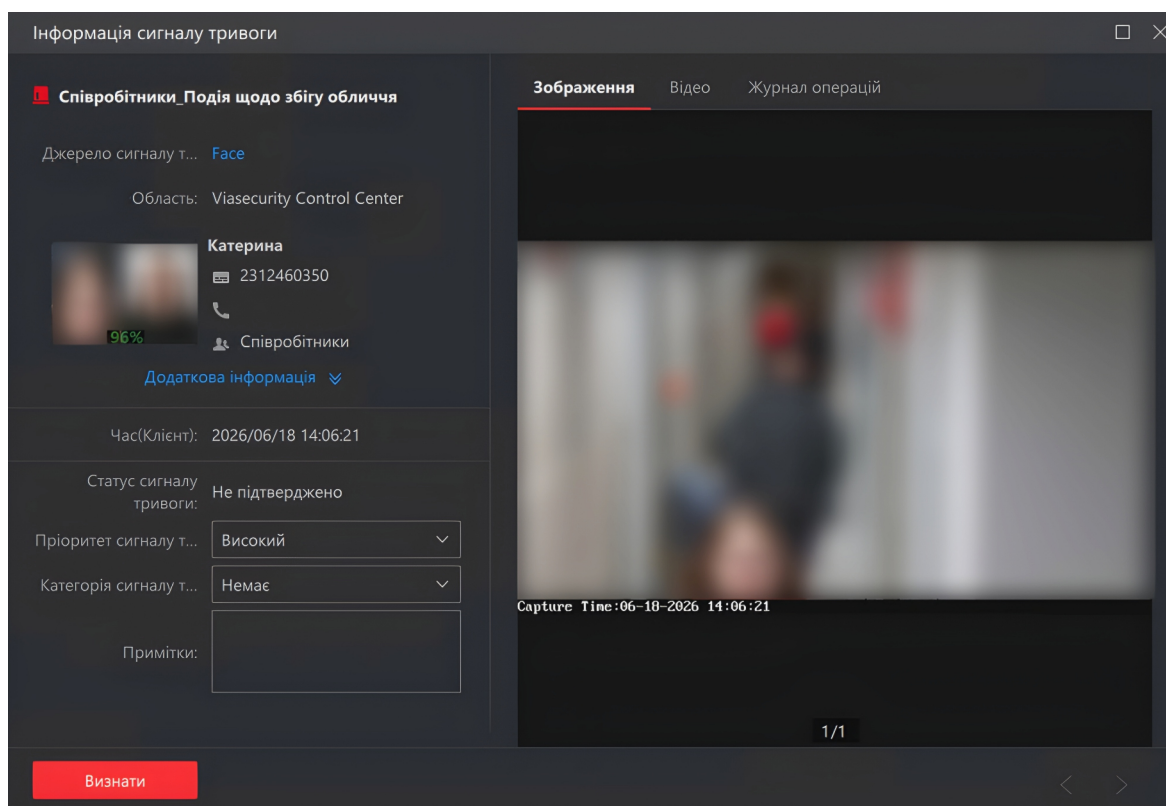


Рисунок 3.14 Деталі тривоги

3.3.3 Пошук розпізнаних зображень обличчя та зображень людського тіла

Оператори можуть ефективно отримувати журнали, застосовуючи конкретні фільтри пошуку. Цей механізм запитів охоплює стандартні знімки обличчя, записи порівняння, що відповідають критеріям, та події виявлення тіла людини.

Пошук розпізнаних зображень обличчя та зображень людського тіла:

1. Перейдіть до **Пошук → Виявлення обличчя та людського тіла**, щоб отримати доступ до панелі запитів.
2. Визначте параметри пошуку, щоб відфільтрувати та знайти необхідні записи біометричних знімків.

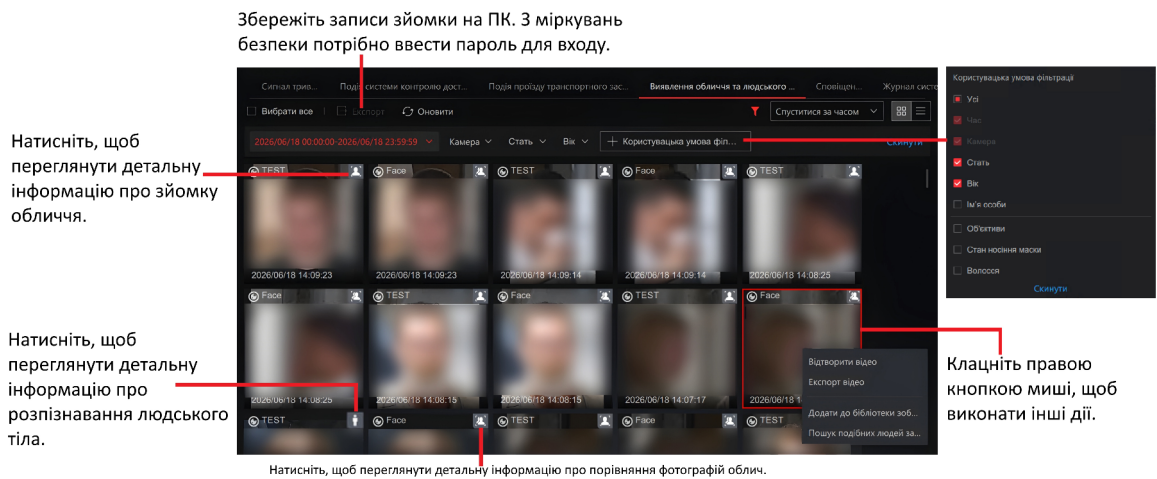


Рисунок 3.15 Виявлення обличчя та людського тіла

3. Виберіть будь-який окремий запис із отриманих результатів, щоб переглянути його детальну інформацію.
4. Використовуйте функцію експорту, щоб зберегти журнали знімків об'єктів локально для зовнішньої звітності або управління доказами.

Обличчя Виявлення людського тіла										
Базова інформація										
Експорт часу:	18.06.2026 15:49									
Оператор:	admin									
Експортувати вміст:	Дані		Захват	Відео						
Час звіту:	2026/06/18 00:00:00 - 2026/06/18 23:59:59									
№	Тип зйомки	Час	Камера	Подібність	Вікова група	Стать	У масці	Окуляри	Група порівнян	Ім'я особи
1	Захоплення зображення обличчя	18.06.2026 15:49	TEST	Не підтримується.	Невідомий	Невідомий	Невідомий	Невідомий	Невідомий	Невідомий
2	Порівняння облич	18.06.2026 15:49	Face	97%	Молодий	Жінка	Невідомий	Невідомий	Співробітники	Катерина
3	Захоплення зображення обличчя	18.06.2026 15:48	TEST	Не підтримується.	Невідомий	Невідомий	Невідомий	Невідомий	Невідомий	Невідомий
4	Порівняння облич	18.06.2026 15:48	Face	Не підтримується.	Невідомий	Невідомий	Невідомий	Невідомий	Невідомий	Невідомий

Рисунок 3.16 Експорт записів знімків

(Примітка: Ця функція пошуку в історії залежить від апаратного забезпечення і повинна підтримуватися підключеними пристроями.)

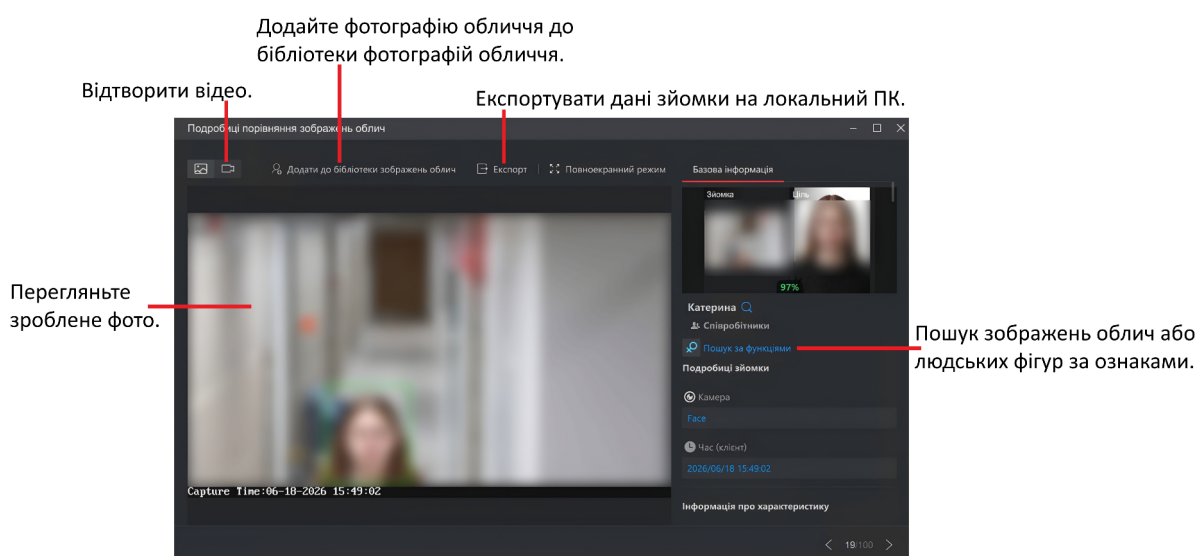


Рисунок 3.17 Підтримувані операції на сторінці деталей знімків обличчя

3.3.4 Пошук Об'єктів за Зображенням

Оператори можуть виконувати зворотний пошук за зображенням, завантажуючи еталонне фото, щоб швидко знайти відповідні профілі обличчя, силуети людей або транспортні засоби в архівах записаних відео.

Інструкції:

1. Перейдіть до меню **Пошук → Розумний пошук → Завантажити зображення**.
2. Імпортуйте зразкове зображення з вашої локальної робочої станції, вибравши його за допомогою файлового браузера або перетягнувши безпосередньо в інтерфейс.
3. Якщо завантажене зображення містить лише один розпізнаваний об'єкт, система автоматично виконає запит і відобразить результати.
4. Якщо зображення містить натовп або кілька об'єктів, вручну виберіть конкретне обличчя, фігуру людини або транспортний засіб, які ви хочете виділити та знайти.

На панелі згенерованих результатів оператори можуть переглянути точні деталі знімка та запустити відтворення відповідного відеоматеріалу.

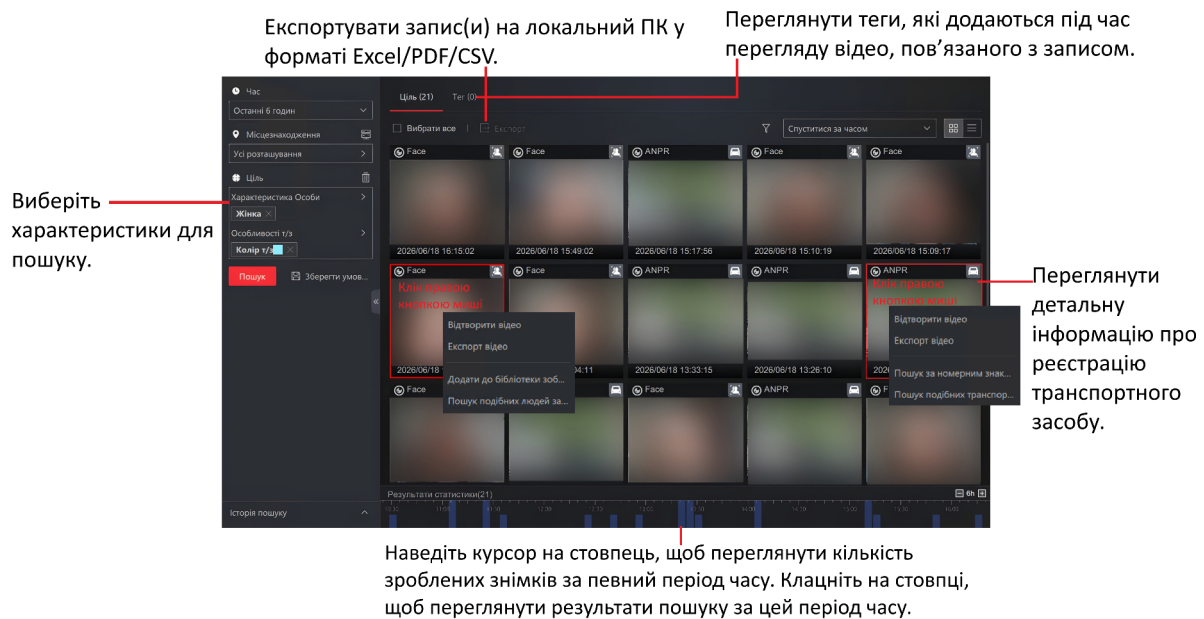


Рисунок 3.18 Умови пошуку та підтримувані операції на сторінці результатів пошуку

3.4 Операції з транспортними засобами

Viasecurity Control Center забезпечує комплексне відстеження транспортних засобів, дозволяючи операторам контролювати потоки дорожнього руху в режимі реального часу, керувати категоризованими реєстрами транспортних засобів та здійснювати пошук по історії проїздів.

(Примітка: Моніторинг транспортних засобів здійснюється виключно за допомогою пристроїв, сумісних з ANPR. Зверніться до служби технічної підтримки, щоб отримати перевірений перелік підтримуваних моделей камер.)

3.4.1 Додавання списків транспортних засобів та номерів

Для ефективної категоризації та моніторингу транспортного руху адміністратори повинні створювати та підтримувати спеціальні списки транспортних засобів. Цей модуль дозволяє здійснювати масове управління, переносити дані між списками та витягувати дані.

Списки транспортних засобів:

- Перейдіть до **Система** → **Транспортний засіб**, щоб отримати доступ до централізованої панелі управління транспортними засобами.

- Натисніть на назву транспортного засобу, щоб редагувати його.

Співробітники						
Базова інформація						
Час	2026/06/19 09:44:15					
Оператор	admin					
Усього записів	5					
Правило (уведіть відповідну інформацію про транспортний засіб згідно з такими номерами)						
Марка	0=Інше 1=Volkswagen 2=Buick 3=BMW 4=Honda 5=Peugeot 6=Toyota 7=Ford 8=Nissan 9=Audi 10=Mazda 11=Chevrolet 12=Citroen 13=Hyundai 14=Chery 15=KIA 16=Renault 17=Volvo 18=Ford 19=Vauxhall 20=Subaru 21=Honda 22=Toyota 23=Ford 24=Nissan 25=Dongfeng 26=BYD 27=Suzuki 28=Jinbei 29=Haima 30=SGMW 31=JAC 32=Subaru 33=Englon 34=GWM 35=Hafei 36=Qingling/Isuzu 37=SOUEAST 38=Changan 39=Ford 40=Changan 41=Changan 42=Changan 43=Changan 44=Changan 45=Changan 46=Changan 47=Changan 48=Changan 49=Changan 50=Kama 51=Zotye 52=Changhe 53=Xiamen Jinlong/Jinlqv 54=Shanghai Huizhong 55=Suzhou Jinglong 56=Higer 57=Yutong 58=CNHTC 59=Вантажівка Beiben/транс. засіб 60=BMW MINI 101=Toyota MAROX 102=Haval 103=Acura 104=Venucia 105=BYD Style 2 106=Benz SMART 107=Beijing Vehicle Manufacture/BAW 108=Luxgen 109=Mustang 110=Ford 121=Lotus 123=Nanjun 124=Shuanghuan Motor 125=Hafei Saibao 126=Huatai 127=Yongyuan Feidie 128=Yongyuan Motor 129=Fu Long Ma 130=Hyundai 131=MG 132=MG 133=MG 134=MG 135=MG 136=MG 137=MG 138=MG 139=MG 140=MG 141=MG 142=MG 143=MG 144=MG 145=MG 146=MG 147=MG 148=MG 149=MG 150=GMC 151=SAIC Maxus 152=Beiqi Yinyixiang 153=New Qirui 154=Mudan 155=Dayun Motor 156=Dongwo Motor 157=Union Motor 158=Автобус Chunchun 159=Sany He 160=Maserati 201=Автобус Shuchi 202=Автобус Shili 203=Zhongke Huabei 204=SAIC Yizheng 205=Chunlan Motor 206=Dafa Motor 207=Shenye Motor 208=Ferrari 209=Ford 210=AC Schnitzer 1026=ALFA ROMEO 1027=ASTON MARTIN 1029=LA JOYA 1041=BRABUS 1042=BUGATTI 1047=Changfeng Liebao 1049=Changan Saloon 1055=DETROIT 1056=DETROIT 1057=DETROIT 1058=DETROIT 1059=DETROIT 1060=DETROIT 1061=DETROIT 1062=DETROIT 1063=DETROIT 1064=DETROIT 1065=DETROIT 1066=DETROIT 1067=DETROIT 1068=DETROIT 1069=DETROIT 1070=DETROIT 1071=DETROIT 1072=DETROIT 1073=DETROIT 1074=DETROIT 1075=DETROIT 1076=DETROIT 1077=DETROIT 1078=DETROIT 1079=DETROIT 1080=DETROIT 1081=DETROIT 1082=DETROIT 1083=DETROIT 1084=DETROIT 1085=DETROIT 1086=DETROIT 1087=DETROIT 1088=DETROIT 1089=DETROIT 1090=DETROIT 1091=KANDI 1092=KOENIGSEGG 1095=Rolls-Royce 1096=LINCOLN 1099=LANCIA 1100=LOTUS NVO 1101=Meiya 1110=Max/Ipelon 1111=МАЙБЕХ 1113=MORGAN 1115=Mercedes 1116=Mercedes 1117=Mercedes 1118=Mercedes 1119=Mercedes 1120=Mercedes 1121=Mercedes 1122=Mercedes 1123=Mercedes 1124=Mercedes 1125=Mercedes 1126=Mercedes 1127=Mercedes 1128=Mercedes 1129=Mercedes 1130=Mercedes 1131=Mercedes 1132=Mercedes 1133=Mercedes 1134=Mercedes 1135=Mercedes 1136=Mercedes 1137=Mercedes 1138=Mercedes 1139=Mercedes 1140=Mercedes 1141=Mercedes 1142=Mercedes 1143=Mercedes 1144=Mercedes 1145=Mercedes 1146=Mercedes 1147=Mercedes 1148=Mercedes 1149=Mercedes 1150=Mercedes 1151=Mercedes 1152=Mercedes 1153=Mercedes 1154=Mercedes 1155=Mercedes 1156=Mercedes 1157=Mercedes 1158=Mercedes 1159=Mercedes 1160=Mercedes 1161=Mercedes 1162=Mercedes 1163=Mercedes 1164=Mercedes 1165=Mercedes 1166=Mercedes 1167=Mercedes 1168=Mercedes 1169=Mercedes 1170=Mercedes 1171=Mercedes 1172=Mercedes 1173=Mercedes 1174=Mercedes 1175=Mercedes 1176=Mercedes 1177=Mercedes 1178=Mercedes 1179=Mercedes 1180=Mercedes 1181=Mercedes 1182=Mercedes 1183=Mercedes 1184=Mercedes 1185=Mercedes 1186=Mercedes 1187=Mercedes 1188=Mercedes 1189=Mercedes 1190=Mercedes 1191=Mercedes 1192=Mercedes 1193=Mercedes 1194=Mercedes 1195=Mercedes 1196=Mercedes 1197=Mercedes 1198=Mercedes 1199=Mercedes 1200=Mercedes 1201=Mercedes 1202=Mercedes 1203=Mercedes 1204=Mercedes 1205=Mercedes 1206=Mercedes 1207=Mercedes 1208=Mercedes 1209=Mercedes 1210=Mercedes 1211=Mercedes 1212=Mercedes 1213=Mercedes 1214=Mercedes 1215=Mercedes 1216=Mercedes 1217=Mercedes 1218=Mercedes 1219=Mercedes 1220=Mercedes 1221=Mercedes 1222=Mercedes 1223=Mercedes 1224=Mercedes 1225=Mercedes 1226=Mercedes 1227=Mercedes 1228=Mercedes 1229=Mercedes 1230=Mercedes 1231=Mercedes 1232=Mercedes 1233=Mercedes 1234=Mercedes 1235=Mercedes 1236=Mercedes 1237=Mercedes 1238=Mercedes 1239=Mercedes 1240=Mercedes 1241=Mercedes 1242=Mercedes 1243=Mercedes 1244=Mercedes 1245=Mercedes 1246=Mercedes 1247=Mercedes 1248=Mercedes 1249=Mercedes 1250=Mercedes 1251=Mercedes 1252=Mercedes 1253=Mercedes 1254=Mercedes 1255=Mercedes 1256=Mercedes 1257=Mercedes 1258=Mercedes 1259=Mercedes 1260=Mercedes 1261=Mercedes 1262=Mercedes 1263=Mercedes 1264=Mercedes 1265=Mercedes 1266=Mercedes 1267=Mercedes 1268=Mercedes 1269=Mercedes 1270=Mercedes 1271=Mercedes 1272=Mercedes 1273=Mercedes 1274=Mercedes 1275=Mercedes 1276=Mercedes 1277=Mercedes 1278=Mercedes 1279=Mercedes 1280=Mercedes 1281=Mercedes 1282=Mercedes 1283=Mercedes 1284=Mercedes 1285=Mercedes 1286=Mercedes 1287=Mercedes 1288=Mercedes 1289=Mercedes 1290=Mercedes 1291=Mercedes 1292=Mercedes 1293=Mercedes 1294=Mercedes 1295=Mercedes 1296=Mercedes 1297=Mercedes 1298=Mercedes 1299=Mercedes 1300=Mercedes 1301=Mercedes 1302=Mercedes 1303=Mercedes 1304=Mercedes 1305=Mercedes 1306=Mercedes 1307=Mercedes 1308=Mercedes 1309=Mercedes 1310=Mercedes 1311=Mercedes 1312=Mercedes 1313=Mercedes 1314=Mercedes 1315=Mercedes 1316=Mercedes 1317=Mercedes 1318=Mercedes 1319=Mercedes 1320=Mercedes 1321=Mercedes 1322=Mercedes 1323=Mercedes 1324=Mercedes 1325=Mercedes 1326=Mercedes 1327=Mercedes 1328=Mercedes 1329=Mercedes 1330=Mercedes 1331=Mercedes 1332=Mercedes 1333=Mercedes 1334=Mercedes 1335=Mercedes 1336=Mercedes 1337=Mercedes 1338=Mercedes 1339=Mercedes 1340=Mercedes 1341=Mercedes 1342=Mercedes 1343=Mercedes 1344=Mercedes 1345=Mercedes 1346=Mercedes 1347=Mercedes 1348=Mercedes 1349=Mercedes 1350=Mercedes 1351=Mercedes 1352=Mercedes 1353=Mercedes 1354=Mercedes 1355=Mercedes 1356=Mercedes 1357=Mercedes 1358=Mercedes 1359=Mercedes 1360=Mercedes 1361=Mercedes 1362=Mercedes 1363=Mercedes 1364=Mercedes 1365=Mercedes 1366=Mercedes 1367=Mercedes 1368=Mercedes 1369=Mercedes 1370=Mercedes 1371=Mercedes 1372=Mercedes 1373=Mercedes 1374=Mercedes 1375=Mercedes 1376=Mercedes 1377=Mercedes 1378=Mercedes 1379=Mercedes 1380=Mercedes 1381=Mercedes 1382=Mercedes 1383=Mercedes 1384=Mercedes 1385=Mercedes 1386=Mercedes 1387=Mercedes 1388=Mercedes 1389=Mercedes 1390=Mercedes 1391=Mercedes 1392=Mercedes 1393=Mercedes 1394=Mercedes 1395=Mercedes 1396=Mercedes 1397=Mercedes 1398=Mercedes 1399=Mercedes 1400=Mercedes 1401=Mercedes 1402=Mercedes 1403=Mercedes 1404=Mercedes 1405=Mercedes 1406=Mercedes 1407=Mercedes 1408=Mercedes 1409=Mercedes 1410=Mercedes 1411=Mercedes 1412=Mercedes 1413=Mercedes 1414=Mercedes 1415=Mercedes 1416=Mercedes 1417=Mercedes 1418=Mercedes 1419=Mercedes 1420=Mercedes 1421=Mercedes 1422=Mercedes 1423=Mercedes 1424=Mercedes 1425=Mercedes 1426=Mercedes 1427=Mercedes 1428=Mercedes 1429=Mercedes 1430=Mercedes 1431=Mercedes 1432=Mercedes 1433=Mercedes 1434=Mercedes 1435=Mercedes 1436=Mercedes 1437=Mercedes 1438=Mercedes 1439=Mercedes 1440=Mercedes 1441=Mercedes					

3.4.2 Перегляд відео, пов'язаного з моніторингом транспортних засобів

Оператори можуть стежити за дорожнім рухом у режимі реального часу та відстежувати проїзд транспортних засобів за допомогою потоків відео з підключених камер ANPR. Під час виявлення транспортних засобів система миттєво зіставляє зняті кадри зі списком активних транспортних засобів, відображаючи дані про розпізнаного власника та збіги зі списком безпосередньо поруч із відеопотоком.

Основні взаємодії:

- Наведіть курсор на будь-яку активну подію, пов'язану з транспортним засобом, щоб миттєво переглянути зведення про виявлення.
- Клацніть правою кнопкою миші на події, щоб виконати негайні адміністративні дії, наприклад, вручну виправити неправильно зчитаний номерний знак або безпосередньо віднести розпізнаний транспортний засіб до конкретного списку.

Необхідна умова: Перед тим, як почати використовувати моніторинг ANPR у режимі реального часу, переконайтеся, що всі необхідні камери розпізнавання повністю інтегровані та що відповідні канали мають ліцензії. Присвойте ці ліцензії, перейшовши в розділ **Керування ліцензіями → Огляд ліцензій**.

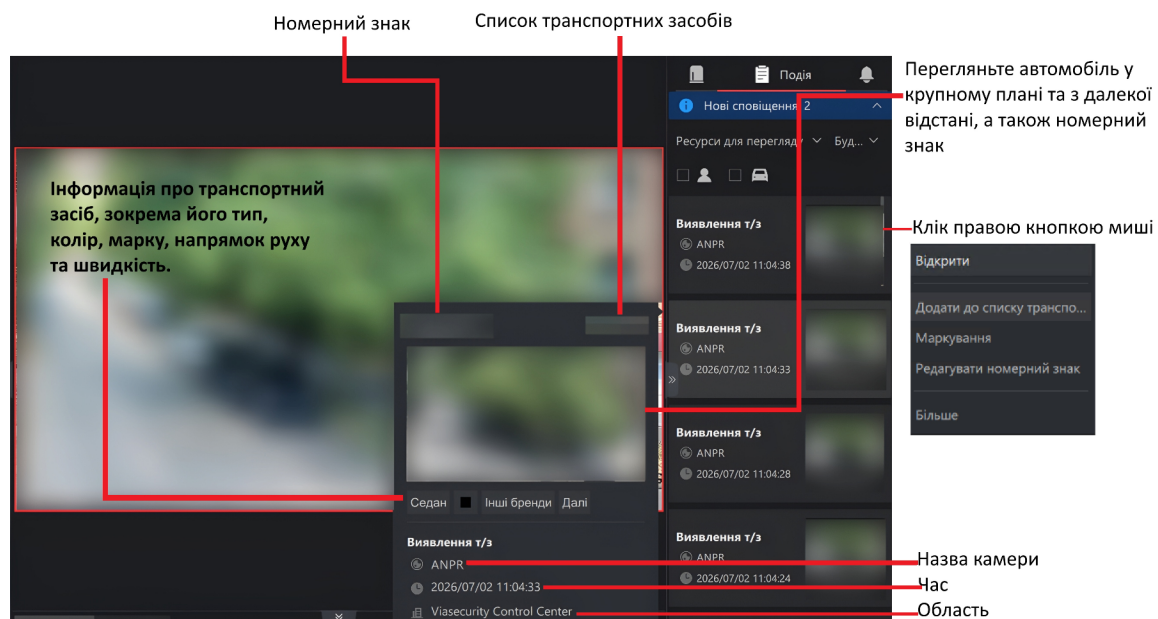


Рисунок 3.21 Деталі події ANPR

3.4.3 Пошук та експорт подій ANPR

Viasecurity Control Center веде вичерпний архів усіх випадків проїзду транспортних засобів із можливістю пошуку, що дозволяє співробітникам служби безпеки ефективно знаходити та витягувати історичні дані про рух транспорту.

Інструкції:

1. Перейдіть до **Пошук → Подія проїзду транспортного засобу**, щоб отримати доступ до інтерфейсу запитів за історією ANPR.
2. Застосуйте точні фільтри пошуку — зокрема діапазони дати та часу, конкретні джерела камер, списки цільових транспортних засобів або точні номерні знаки — щоб виділити необхідні записи.
3. Щоб детально переглянути дані про виявлення конкретного транспортного засобу, клацніть безпосередньо на текст у стовпці **Номерний знак**, щоб відкрити повну інформацію про знімок.
4. Щоб витягти ці записи для зовнішнього аудиту або складання звітів, натисніть кнопку **Експорт**, щоб завантажити відфільтровані результати на свій комп'ютер у форматі Excel, PDF або CSV.

1	Записи отримання ANPR											
2	SYS:											
3	Експорт часу: 2026/06/19 09:27:51											
4	Сумарна кількість: 17,											
5												
6	Номерний знак	Час (клієнт)	Камера	Список транспортных засобів	Власник	№ телефону	Країна/region	Вид т/з	Марка	Колір	Швидкість руху	Напрямок руху
7		2026/06/19 05:38:29	ANPR	Співробітники	--	--	Україна	Кросовер/MPV	Jeep	Чорний	--	Далі
8		2026/06/19 05:38:25	ANPR	--	--	--	Україна	Мінівен	Volkswagen	Білий	--	Далі
9		2026/06/19 05:32:22	ANPR	Співробітники	--	--	Україна	Седан	Toyota	Сірий	--	Далі
10		2026/06/19 05:25:10	ANPR	Співробітники	--	--	Україна	Седан	Toyota	Білий	--	Далі
11		2026/06/19 05:24:07	ANPR	Співробітники	--	--	Україна	Кросовер/MPV	Toyota	Сірий	--	Далі
12		2026/06/19 05:23:27	ANPR	Співробітники	--	--	Україна	Мінівен	Mitsubishi	Білий	--	Далі
13		2026/06/19 05:11:22	ANPR	Співробітники	--	--	Україна	Седан	Skoda	Сірий	--	Далі
14		2026/06/19 05:10:55	ANPR	--	--	--	Україна	Кросовер/MPV	Jeep	Чорний	--	Далі
15		2026/06/19 05:10:52	ANPR	--	--	--	Україна	Мінівен	Інші бренди	Білий	--	Далі
16		2026/06/19 05:02:14	ANPR	Співробітники	--	--	Україна	Вантажівка	Volvo	Сірий	--	Далі
17		2026/06/19 04:49:37	ANPR	Співробітники	--	--	Україна	Седан	Інші бренди	Інші кольори	--	Далі
18		2026/06/19 04:47:35	ANPR	--	--	--	Україна	Кросовер/MPV	Renault	Білий	--	Далі
19		2026/06/19 02:47:29	ANPR	Співробітники	--	--	Україна	Седан	Suzuki	Чорний	--	Далі
20		2026/06/19 01:20:11	ANPR	--	--	--	Україна	Седан	Hyundai	Білий	--	Далі
21		2026/06/19 01:04:37	ANPR	Співробітники	--	--	Україна	Мінівен	JAC	Білий	--	Далі
22		2026/06/19 00:04:18	ANPR	Співробітники	--	--	Україна	Кросовер/MPV	Land Rover	Сірий	--	Далі
23		2026/06/19 00:00:02	ANPR	Співробітники	--	--	Україна	Седан	Ora	Чорний	--	Далі

Рисунок 3.22. Експорт даних про проїзду транспортних засобів у форматі Excel

Інформація про проїзд транспортних засобів

Базова інформація

Час пошуку: 2026/06/19 09:38:55

Критерій пошуку: admin

Час: 2026/06/19 00:00:00 - 2026/06/19 06:00:59

Сукупна кількість: 17

Номерний знак	Подобиці зйомки	Інформація про транспортний засіб	Інформація про власника	Мініатюри
	ANPR 2026/06/19 05:38:29	Україна Кросовер/MPV Jeep Чорний Далі	-- --	
	ANPR 2026/06/19 05:38:25	Україна Мінівен Volkswagen Білий Далі	-- --	
	ANPR 2026/06/19 05:32:22	Україна Седан Toyota Сірий Далі	-- --	
	ANPR 2026/06/19 05:25:10	Україна Седан Toyota Білий Далі	-- --	
	ANPR 2026/06/19 05:24:07	Україна Кросовер/MPV Toyota Сірий Далі	-- --	

Рисунок 3.23 Експорт даних про проїзду транспортних засобів у форматі PDF

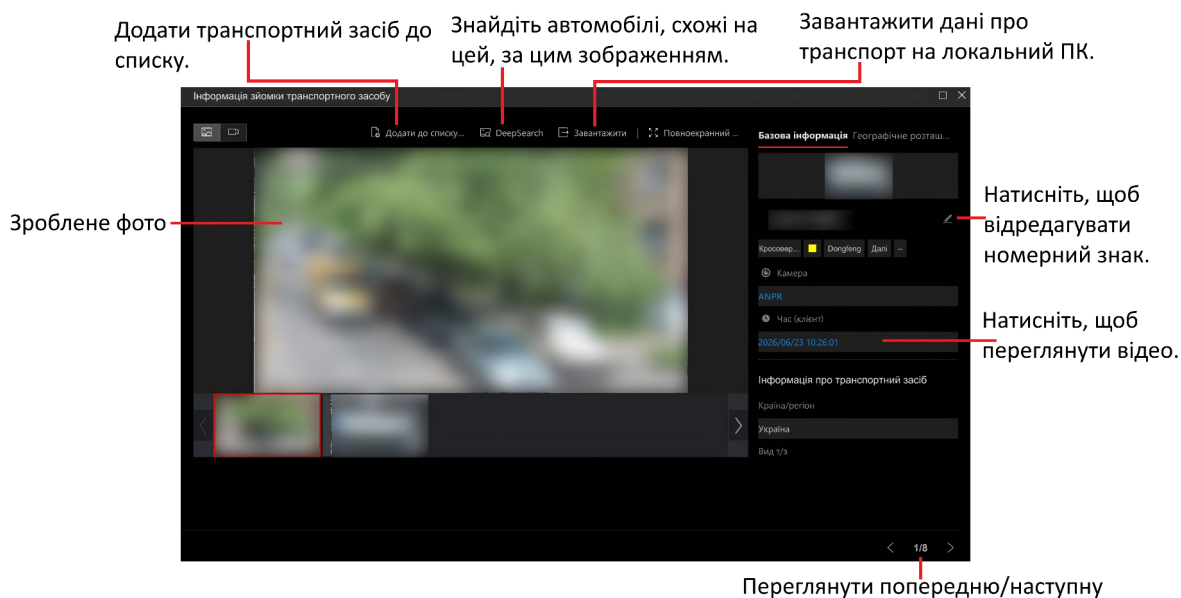


Рисунок 3.24 Детальна інформація про проїзд транспортного засобу

3.5 Функції інтелектуального пошуку

Цей модуль надає розширені інструменти для ефективного пошуку конкретних об'єктів та аналізу записаних відеоматеріалів. Ви можете використовувати функцію Смарт-пошук або VCA-пошук залежно від того, чи підтримують підключені пристрої відповідні функції. Перед використанням цих функцій переконайтеся, що розклади запису для відповідних мережевих камер налаштовані належним чином.

3.5.1 Смарт-пошук / VCA

Налаштування мережевого відеореєстратора (NVR) та мережевої камери

Щоб скористатися функціями Смарт-пошук або VCA, переконайтеся, що для ваших мережевих камер налаштовано активні графіки запису та що ваше обладнання NVR підтримує ці функції. Процедури налаштування залежать від конкретної конфігурації вашого обладнання:

- **Для мережевих відеореєстраторів (NVR) з прошивкою версії V5.01 або вище:** Увійдіть у веб-інтерфейс NVR. Перейдіть до розділу **Керування зберіганням** → **Розширена конфігурація** та увімкніть функцію **Зберегти дані інтелектуального аналізу камери**.

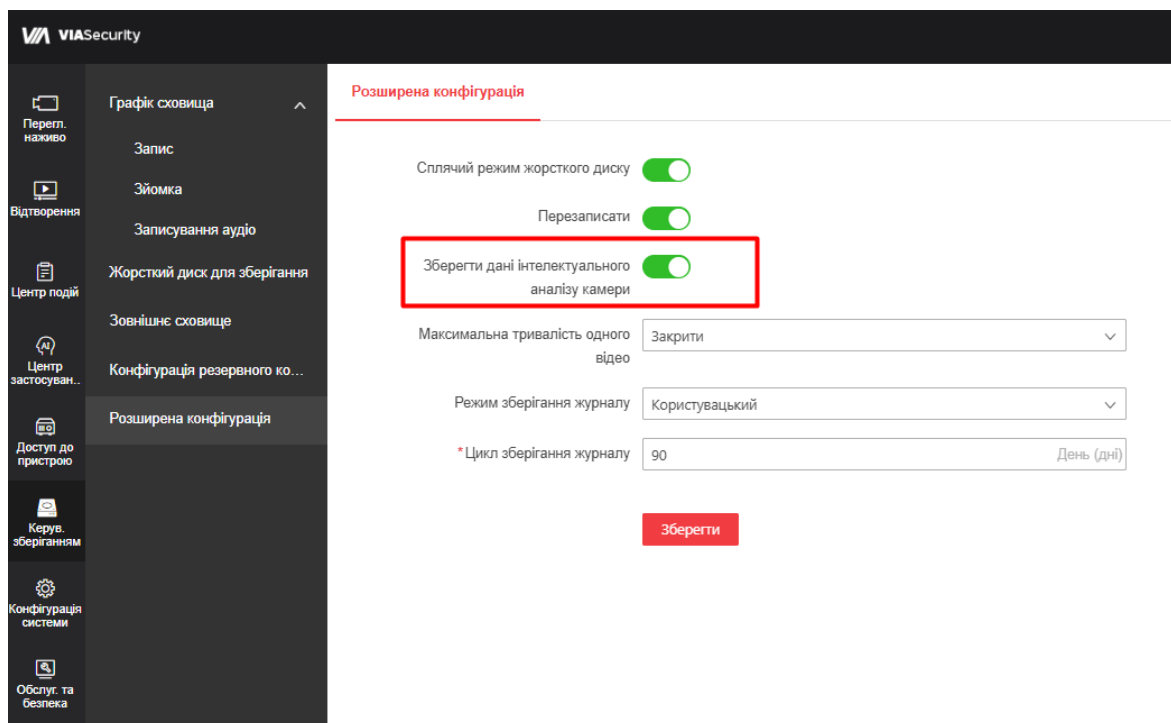


Рисунок 3.24 Зберегти дані інтелектуального аналізу камери

- **Для NVR із версією прошивки нижче V5.01:** Увійдіть у веб-інтерфейс NVR і увімкніть функцію Dual-VCA для відповідної мережевої камери. Переконайтеся, що встановлено галочки як біля пункту Увімкнути виявлення перетину лінії, так і

біля пункту Увімкнути виявлення вторгнення. Після цього натисніть Зберегти дані VCA камери та збережіть налаштування.

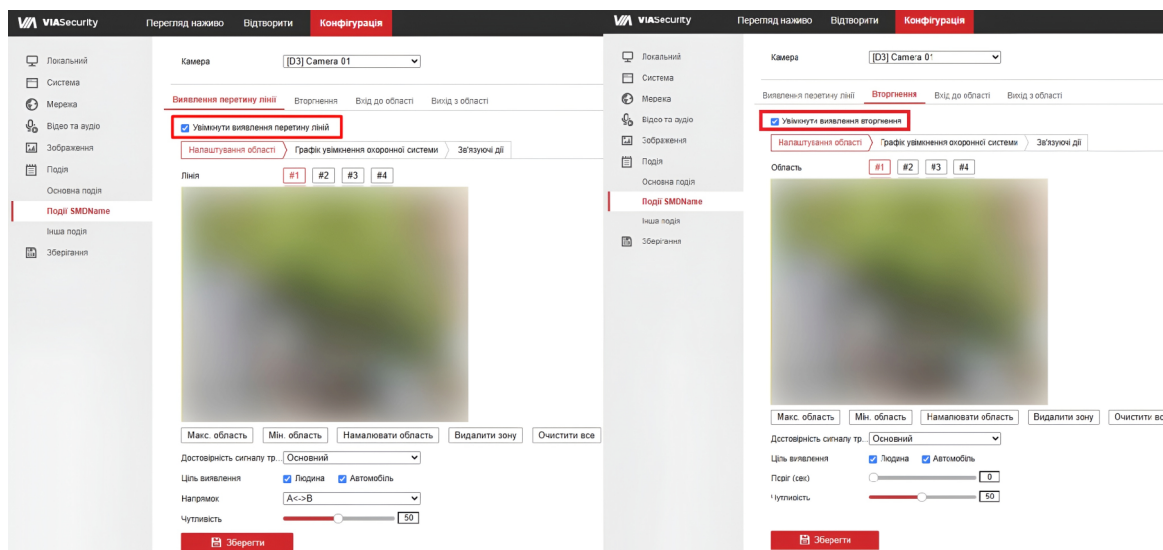


Рисунок 3.25 Увімкнути виявлення перетину лінії та увімкнути виявлення вторгнення

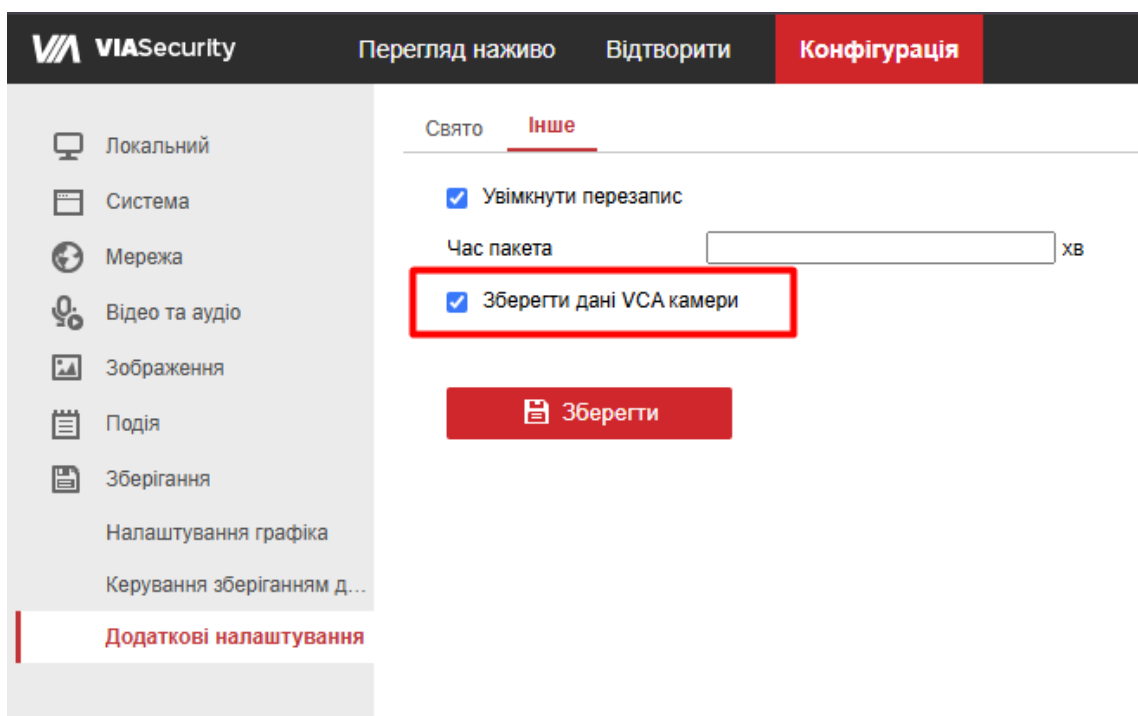


Рисунок 3.26 Зберегти дані VCA з камери

- Для камер, доданих самостійно до Viasecurity Control Center або через NVR без підтримки VCA: Увійдіть у веб-інтерфейс камери та увімкніть подвійний VCA. Після цього перейдіть на сторінку Дані камери у Viasecurity Control Center та встановіть місце зберігання відеозаписів як Системне сховище.

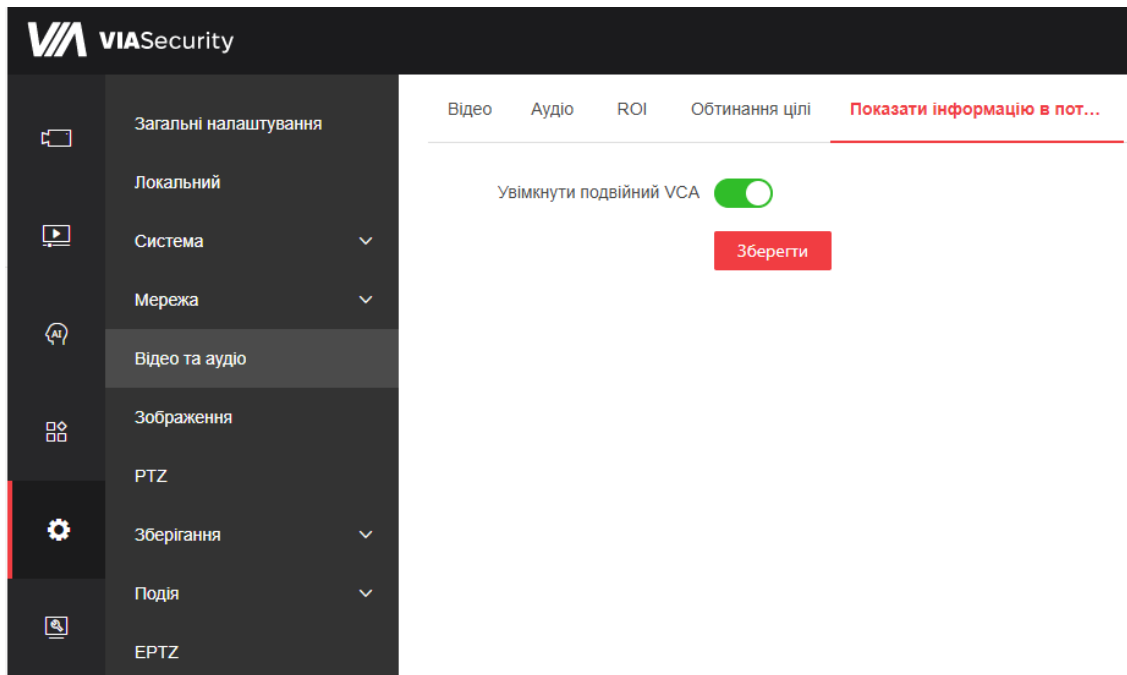


Рисунок 3.27 Увімкнути подвійний VCA

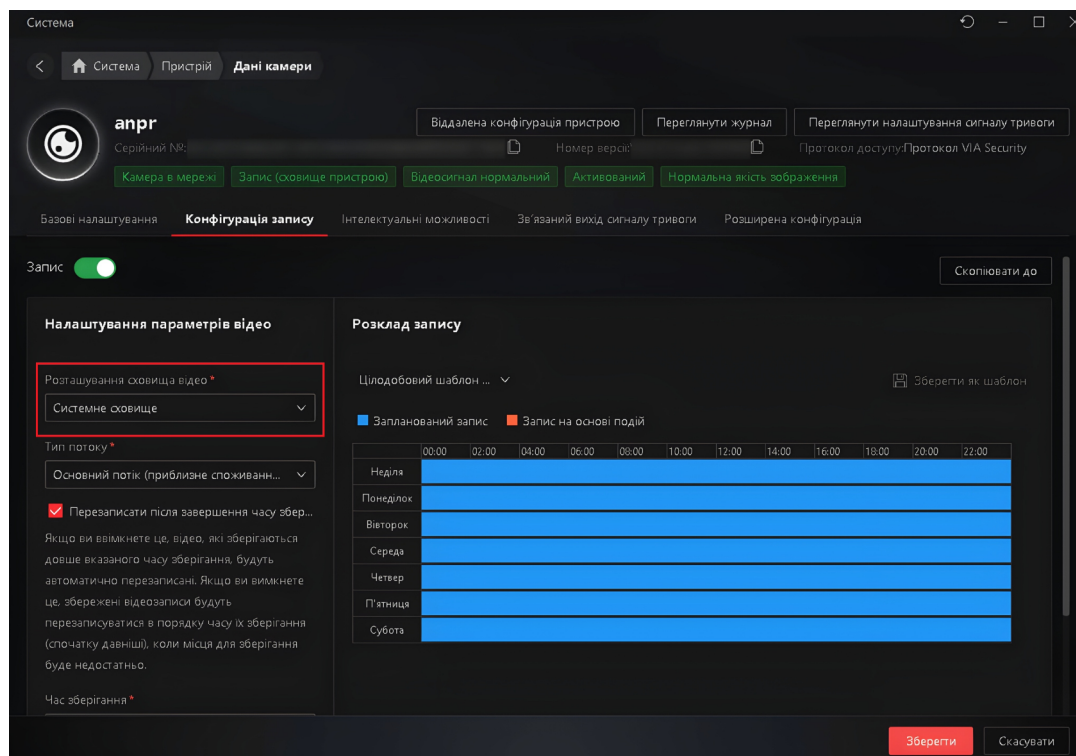


Рисунок 3.28 Налаштування місця зберігання відео

3.5.2 TargetTrace та Object Search

Ця функція автоматизує виокремлення та порівняння зображень людей або транспортних засобів із поточкових трансляцій та записаних відео, що дозволяє операторам швидко відстежувати конкретні цілі в мережі відеоспостереження. Інтерфейс динамічно позначає кнопку активації як «TargetTrace» або «Object Search» залежно від того, чи підключене обладнання безпосередньо підтримує розширений пошук об'єктів. Цю функцію необхідно увімкнути в меню «Деталі камери».

Ми настійно рекомендуємо оновити всі пристрої системи до найновіших версій прошивки, щоб забезпечити повну сумісність.

Перш ніж почати

Перш ніж скористатися цією функцією, переконайтеся, що ви увімкнули її на сторінці **Дані камери**.

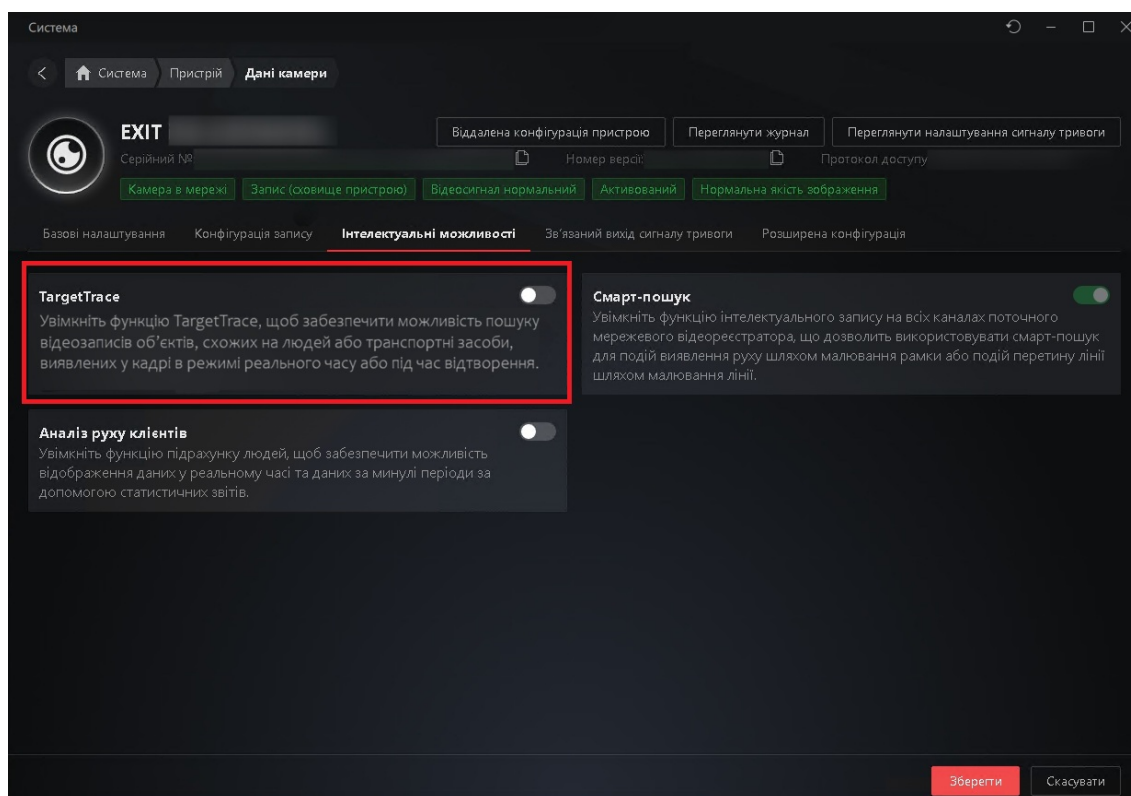


Рисунок 3.29 Дані камери

Виконання за допомогою інтелектуального пошуку

Під час перегляду результатів пошуку клацніть правою кнопкою миші на мініатюрі відео та виберіть опцію «TargetTrace / Object Search», щоб запустити сканування всієї системи на наявність подібних об'єктів у записаних відеоматеріалах.

Виконання за допомогою режиму Live View або відтворення

Натисніть на спеціальну піктограму «TargetTrace / Пошук об'єкта» безпосередньо у вікні перегляду. Відповідні результати автоматично з'являться у правій панелі.

3.5.3 Аналітика та звіти щодо підрахунку людей

Створюйте детальні візуальні звіти, що містять інформацію про записи в режимі реального часу, поточне заповнення приміщення (кількість присутніх) та історичні показники відвідуваності.

(Примітка: Перед створенням звіту необхідно придбати та активувати спеціальну ліцензію для підрахунку людей.)

Використання

Панель «Підрахунок людей у реальному часі» відстежує конкретні події входу та поточну кількість відвідувачів, що перебувають у приміщенні, тоді як панель «Історичний підрахунок відвідувачів» фіксує загальну кількість відвідувачів, що входять та виходять. Усі звіти з історичними даними можна завантажити безпосередньо на локальний ПК для подальшого аналізу.

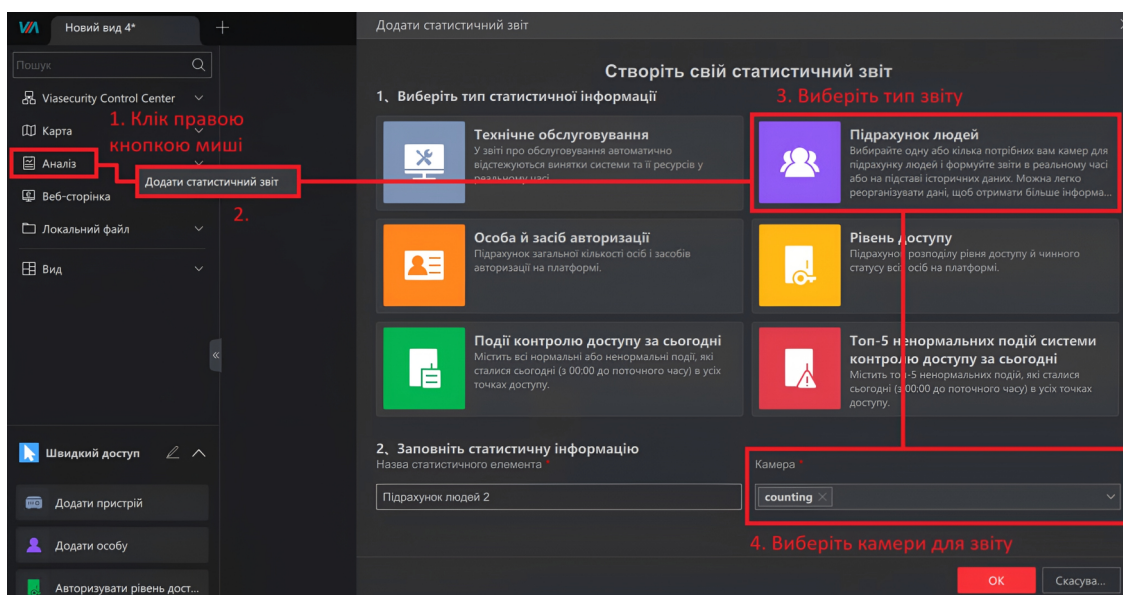


Рисунок 3.39 Створити звіт про підрахунок людей

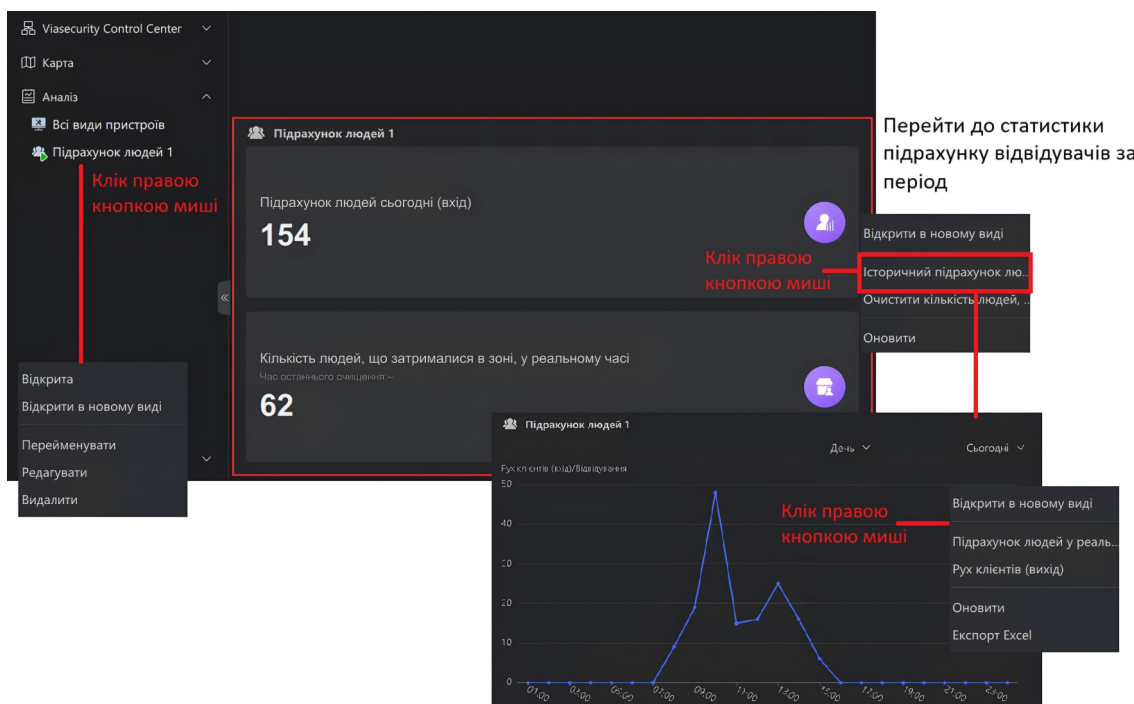


Рисунок 3.40 Переглянути згенерований звіт про підрахунок людей

Історичний підрахунок людей

Базова інформація					
Час експорту	2026/06/23 14:21:00				
Оператор	admin				
Назва статистики	Підрахунок людей 1				
Джерело даних	counting				
Тип даних	Рух клієнтів (вихід)&Рух клієнтів (вихід)				
Період часу дані:	2026/06/23 00:00:00 - 2026/06/23 23:59:59				
Загальна кількість	158(Відвідування)				
Загальний підрахунок людей					
№	Дата	Час	Загальна кількість людей (вихід)(Відвідування)		Загальний підрахунок людей (вихід)
1	2026/06/23	00:00-00:59	0		0
2	2026/06/23	01:00-01:59	0		0
3	2026/06/23	02:00-02:59	0		0
4	2026/06/23	03:00-03:59	0		0
5	2026/06/23	04:00-04:59	0		0
6	2026/06/23	05:00-05:59	0		0
7	2026/06/23	06:00-06:59	0		0
8	2026/06/23	07:00-07:59	9		5
9	2026/06/23	08:00-08:59	19		4
10	2026/06/23	09:00-09:59	48		17
11	2026/06/23	10:00-10:59	15		10
12	2026/06/23	11:00-11:59	16		13
13	2026/06/23	12:00-12:59	25		30
14	2026/06/23	13:00-13:59	16		23
15	2026/06/23	14:00-14:59	10		9
16	2026/06/23	15:00-15:59	0		0
17	2026/06/23	16:00-16:59	0		0
18	2026/06/23	17:00-17:59	0		0
19	2026/06/23	18:00-18:59	0		0
20	2026/06/23	19:00-19:59	0		0
21	2026/06/23	20:00-20:59	0		0
22	2026/06/23	21:00-21:59	0		0
23	2026/06/23	22:00-22:59	0		0
24	2026/06/23	23:00-23:59	0		0
Подробиці					
№	Дата	Час	counting		
			Рух клієнтів (вихід) Рух клієнтів (вихід)(Відвідування)		
1	2026/06/23	00:00-00:59	0		0
2	2026/06/23	01:00-01:59	0		0
3	2026/06/23	02:00-02:59	0		0

Рисунок 3.41 Завантажені звіти

Розділ 4 Системи контролю доступу та відеодомофонія

У цьому розділі описано можливості системи щодо управління пристроями доступу, даними про персонал та функціями зв'язку, що забезпечують комплексний моніторинг об'єкта. Програмне забезпечення пропонує низку інструментів для відстеження облікових даних, аналізу статистики подій та забезпечення фізичної безпеки в режимі реального часу.

Огляд системи контролю доступу

Функції контролю доступу забезпечують оптимізований підхід до управління інфраструктурою фізичної безпеки вашого об'єкта. Адміністратори можуть легко інтегрувати апаратне забезпечення контролю доступу в систему, налаштовувати основні параметри мережі та переглядати детальний стан роботи пристроїв. Для підтримки впорядкованої бази даних програмне забезпечення дозволяє операторам групувати користувачів за відділами, керувати індивідуальними профілями та налаштовувати необхідні набори ідентифікаційних даних для пристроїв.

Для регулювання входу на об'єкт оператори служби безпеки можуть визначати конкретні графіки допуску. Ці рівні доступу можна призначати як цілим відділам, так і окремим користувачам, точно визначаючи, хто саме може відчиняти конкретні двері та в який час. Під час щоденної експлуатації система пропонує надійні можливості моніторингу в режимі реального часу. Оператори можуть переглядати прямі трансляції з камер, пов'язаних із конкретними дверима, динамічно змінювати стан замків на ходу та візуально контролювати кілька точок входу за допомогою інтерактивних карт системи.

Крім того, система забезпечує комплексне відстеження даних та формування звітів. Оператори можуть здійснювати пошук у історії подій контролю доступу або створювати детальні статистичні огляди, що охоплюють діяльність персоналу та системи. Для гарантування цілісності даних програмне забезпечення також підтримує ручне імпортування офлайн-журналів автентифікації осіб безпосередньо з апаратного обладнання.

Можливості відеодомофонії

Модуль відеодомофона забезпечує всебічну взаємодію між пристроями та центральним клієнтським програмним забезпеченням, надаючи операторам можливість детального контролю за взаємодією з відвідувачами. За допомогою

панелі сповіщень оператори можуть легко відстежувати пропущені дзвінки з пристроїв та безперешкодно ініціювати зворотні дзвінки безпосередньо з інтерфейсу. Крім того, співробітники служби охорони мають можливість у будь-який час вручну запустити двосторонній аудіопотік у режимі реального часу з будь-яким підключеним пристроєм.

Для оптимізації робочих процесів адміністратори можуть налаштувати конкретні правила маршрутизації аудіо та дзвінків для поточного клієнта. Програмне забезпечення дозволяє встановлювати точні часові обмеження, наприклад «Час автоматичного завершення дзвінка у разі відсутності відповіді», що автоматично припиняє дзвінки з пристроїв, на які не було відповіді, після закінчення заданого часу очікування. Ви також можете встановити «Максимальну тривалість дзвінка», щоб обмежити тривалість будь-якої активної розмови. Крім того, система підтримує індивідуальну маршрутизацію дзвінків, що дозволяє пов'язувати конкретні апаратні пристрої з визначеними користувачами-клієнтами. Це гарантує, що запити на зв'язок з різних місць завжди спрямовуються до відповідного персоналу.

4.1 Підготовка

4.1.1 Додавання пристроїв

Система підтримує підключення пристроїв контролю доступу, дверних станцій та шлагбаумів.

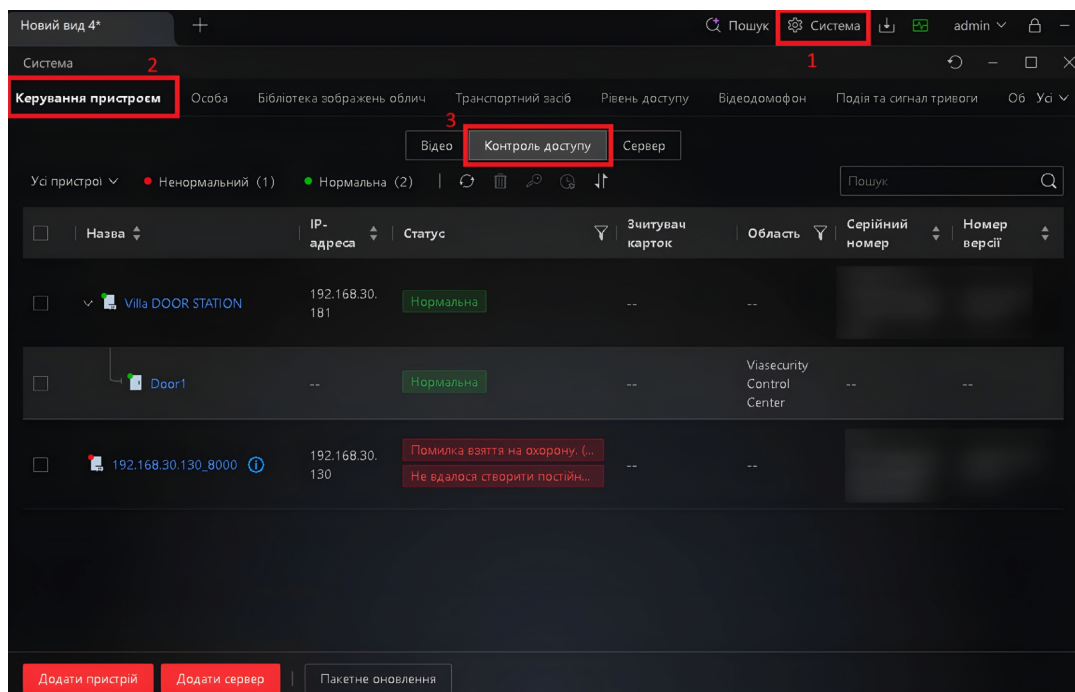


Рисунок 4.1 Список пристроїв

Детальніше див. розділ 2.2 Додавання Пристрою.

4.1.2 Переглянути детальну інформацію про пристрій

Щоб перевірити поточний стан або змінити налаштування певного обладнання, перейдіть до списку пристроїв. Відкрити інтерфейс налаштувань можна, натиснувши безпосередньо на назву пристрою або клацнувши правою кнопкою миші на пристрої чи дверях і вибравши пункт **Перегляд подробиць**.

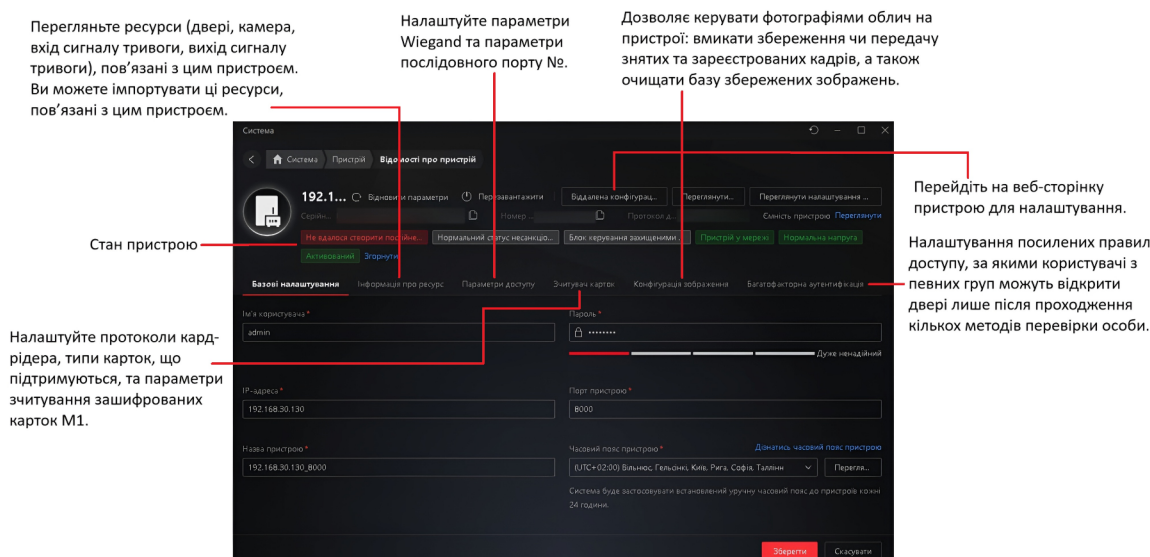


Рисунок 4.2 Детальна інформація про пристрій контролю доступу

На сторінці детальної інформації оператори можуть керувати такими основними функціями:

Управління ресурсами

Перегляд та налаштування підключених апаратних ресурсів. Для додаткової зручності входи та виходи сигналізації також можна імпортувати масово безпосередньо через головний список пристроїв.

Інтервал багатфакторної автентифікації

Встановіть максимально допустимий проміжок часу між кожним етапом перевірки. Якщо цей проміжок часу (наприклад, 5 секунд) закінчиться до того, як буде надано наступні облікові дані, спроба буде визнана недейсною, і користувач повинен буде розпочати всю процедуру автентифікації спочатку.

Пароль автентифікації

Увімкніть додаткову перевірку пароля. Зверніть увагу, що для роботи цієї функції необхідне сумісне обладнання. Крім того, адміністратор або оператор, який налаштовує цей параметр, повинен мати право **Налаштування паролю автентифікації**, присвоєне його ролі користувача.

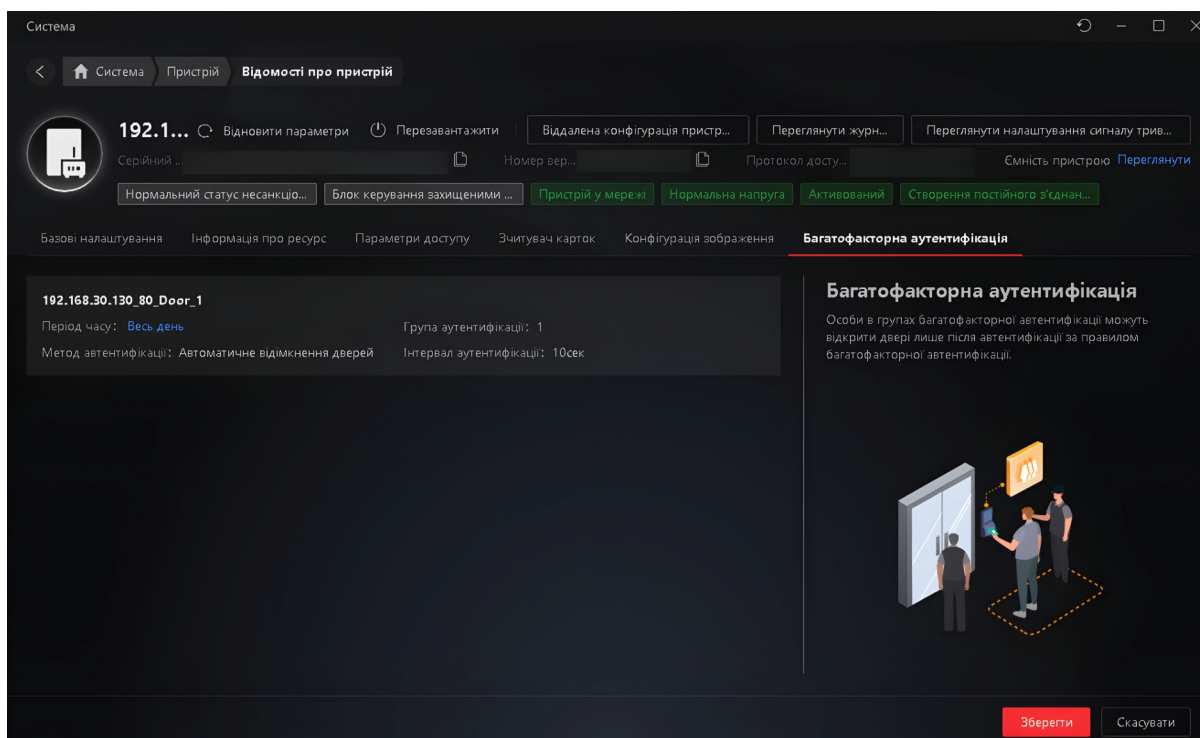


Рисунок 4.3 Налаштування багатофакторної автентифікації

4.1.3 Переглянути детальну інформацію про двері

У списку пристроїв клацніть на назві дверей або клацніть на них правою кнопкою миші, а потім виберіть **Перегляд подробиць**.

Увімкніть два зчитувачі карток та налаштуйте такі параметри: назву зчитувача, інтервал зчитування карток, виявлення несанкціонованого втручання, сигналізацію про шаблони несправних карток та режим автентифікації зчитувача.

Увімкніть опцію «Залишилися незамкненими та залишилися замкненими» для дверей та виберіть шаблони розкладу для цих двох станів. Натисніть «Скопіювати до», щоб скопіювати налаштування на інші двері.

Увімкніть режим «Відчинення дверей першою особою», виберіть правило та "першу особу".

Налаштуйте параметри, зокрема назву дверей, тривалість розблокування дверей, автоматичне блокування, код дії під примусом та суперпароль.

Підключіть камери до дверей, переглядайте пряму трансляцію з підключених камер.

Якщо ви встановите цей прапорець, камера зробить знімок, щойно на дверях відбудеться будь-яка подія. Знімок відобразиться у вікні деталей події пристрою контролю доступу та на панелі подій.

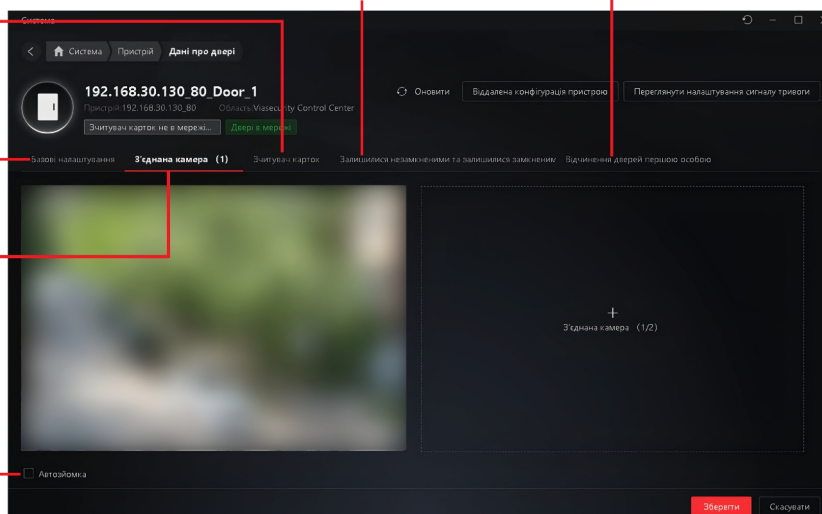


Рисунок 4.4 Дані про двері

4.2 Додати відділи та осіб

Сторінка **Особа** дозволяє операторам керувати профілями користувачів, організовувати організаційні структури та експортувати дані про персонал на локальний ПК.

Додати відділи

Щоб створити організаційну ієрархію, клацніть правою кнопкою миші на кореневому вузлі або будь-якій існуючій папці, щоб додати **підвідділ** або **відділ того самого рівня**. Ви можете легко змінити рівень відділу, перетягнувши його в межах дерева відділів.

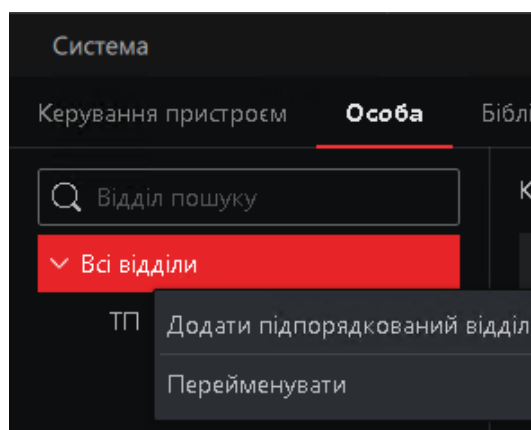


Рисунок 4.5 Структура відділів

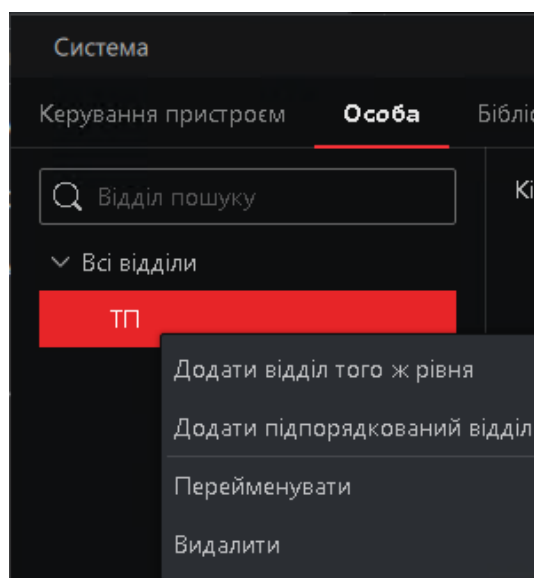


Рисунок 4.6 Структура відділів

Додати осіб

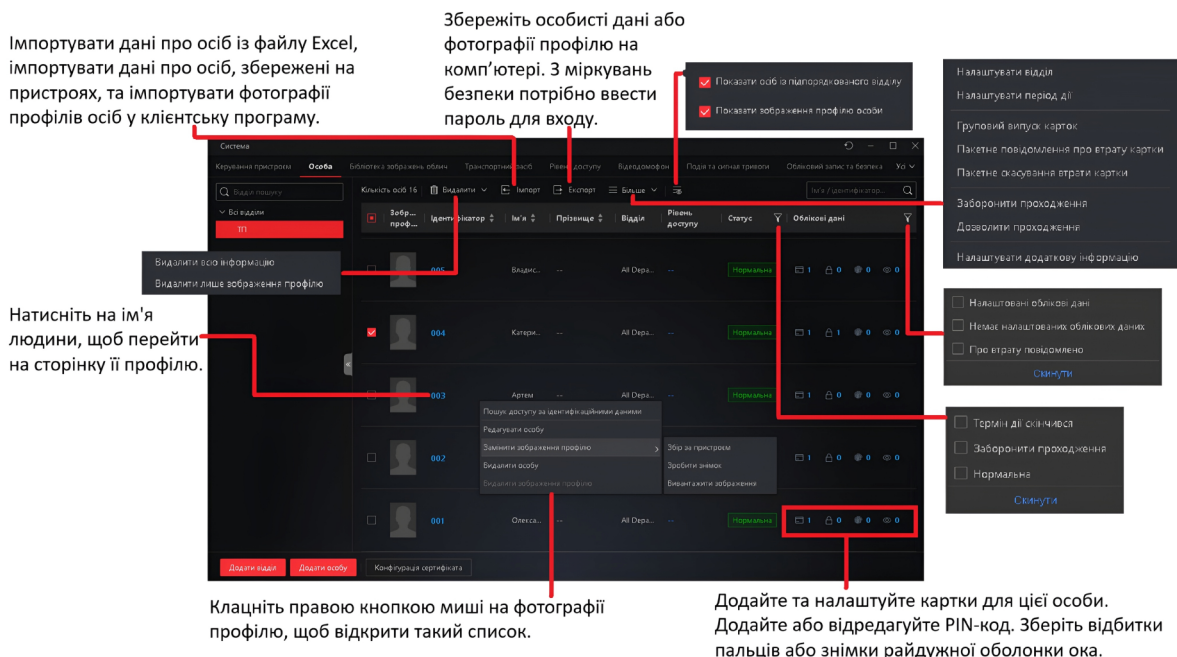


Рисунок 4.7 Список осіб

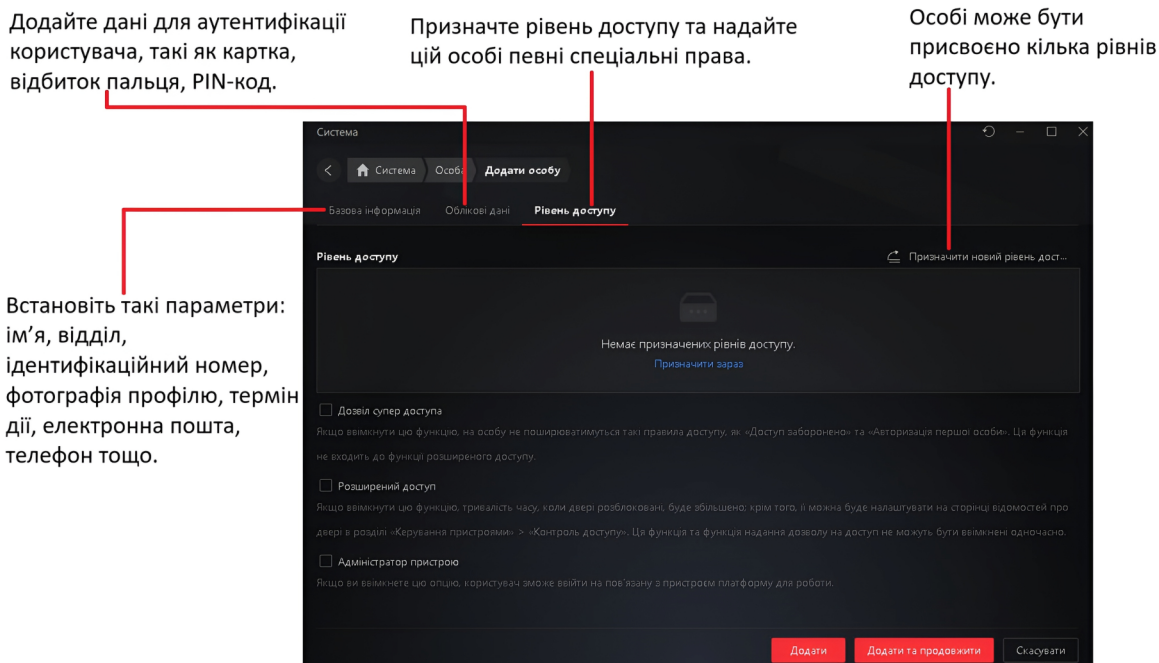


Рисунок 4.8 Додати сторінку особи

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Шаблон інформації про особу												
2	Правило												
3	1.Потрібно вказати принаймні ім'я або прізвище.												
4	2.Після налаштування ідентифікатора не можна змінити. Підтвердіть правило ідентифікатора, перш ніж встановлювати ідентифікатор.												
5	3.НЕ змінюйте макет та заголовок стовпця у цьому шаблонному файлі. Інакше це може призвести до збою імпортування.												
6	4.Ви можете додавати осіб до існуючих відділів. Назви відділів мають розділятися /. Наприклад, імпортувати осіб у Відділ А в Усіх відділах. Формат: All Departments/Відділ А.												
7	5.Час початку періоду дії / час закінчення періоду дії: Період дії особи для контролю доступу та час доступу. Формат: yyyy/mm/dd HH:MM:SS.												
8	6.Для кожної особи можна застосувати до 3 карток. Розділяйте декілька номерів карток крапкою (;), наприклад 01;02;03.												
9	7.Розширений доступ та супер-користувач: неможливо ввімкнути одночасно.												
10	Ідентифікатор	Ім'я	Прізвище	Відділ	Час початку періоду дії	Час завершення періоду дії	Картка	Стать	Електронна пошта	Телефон	Суперкористувач	Розширений доступ	Адміністратор пристрою
11													
12													

Рисунок 4.9 Шаблон для імпорту даних про осіб

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Інформація особи_20260625112545													
2	Правило													
3	1.Потрібно вказати праймні ім'я або прізвище.													
4	2.Після налаштування ідентифікатор не можна змінити. Підтвердіть правило ідентифікатора, перш ніж встановлювати ідентифікатор.													
5	3.НЕ змінюйте макет та заголовки стовпця у цьому шаблонному файлі. Інакше це може призвести до збою імпортування.													
6	4.Ви можете додавати осіб до існуючих відділів. Назви відділів мають розділятися /. Наприклад, імпортувати осіб у Відділ А в Усіх відділах. Формат: Усі відділи/Відділ А.													
7	5.Час початку періоду дії / час закінчення періоду дії: Період дії особи для контролю доступу та час доступу. Формат: yyyy/mm/dd HH:MM:SS.													
8	6.Для кожної особи можна застосувати до 3 карток. Розділяйте декілька номерів карток крапкою з комою (;), наприклад 01;02;03.													
9	7.Розширений доступ та супер-користувач: неможливо вимкнути одночасно.													
10	Ідентифікатор	Прізвище	Відділ	Час початку періоду дії	Час закінчення періоду дії	Карт	Стать	Електронна пошта	Телефон	Суперкористувач	Розширений доступ	Адміністратор пристрою	Рівень доступу	
11	016	Ярослав	All Departments/ТП	2026/06/18 16:41:22	2036/06/18 23:59:59	5672	Чоловік			Вимкнути	Вимкнути	Вимкнути	test-Шаблон на весь день	
12	015	Богдан	All Departments/ТП	2026/06/18 16:41:22	2036/06/18 23:59:59	5672	Чоловік			Вимкнути	Вимкнути	Вимкнути	test-Шаблон на весь день	
13	014	Володимир	All Departments/ТП	2026/06/18 16:41:22	2036/06/18 23:59:59	5672	Чоловік			Вимкнути	Вимкнути	Вимкнути	test-Шаблон на весь день	
14	013	Ілля	All Departments/ТП	2026/06/18 16:41:22	2036/06/18 23:59:59	5672	Чоловік			Вимкнути	Вимкнути	Вимкнути	test-Шаблон на весь день	
15	012	Вікторія	All Departments/ТП	2026/06/18 16:41:22	2036/06/18 23:59:59	5672	Жінка			Вимкнути	Вимкнути	Вимкнути	test-Шаблон на весь день	
16	011	Марк	All Departments/ТП	2026/06/18 16:41:22	2036/06/18 23:59:59	5672	Чоловік			Вимкнути	Вимкнути	Вимкнути	test-Шаблон на весь день	
17	010	Олександра	All Departments/ТП	2026/06/18 16:41:22	2036/06/18 23:59:59	5672	Жінка			Вимкнути	Вимкнути	Вимкнути	test-Шаблон на весь день	
18	009	Матвій	All Departments/ТП	2026/06/18 16:41:22	2036/06/18 23:59:59	5672	Чоловік			Вимкнути	Вимкнути	Вимкнути	test-Шаблон на весь день	
19	008	Дмитро	All Departments/ТП	2026/06/18 16:41:22	2036/06/18 23:59:59	5672	Чоловік			Вимкнути	Вимкнути	Вимкнути	test-Шаблон на весь день	
20	007	Юлія	All Departments/ТП	2026/06/18 16:41:22	2036/06/18 23:59:59	5672	Жінка			Вимкнути	Вимкнути	Вимкнути	test-Шаблон на весь день	
21	006	Данило	All Departments/ТП	2026/06/18 16:41:22	2036/06/18 23:59:59	5672	Чоловік			Вимкнути	Вимкнути	Вимкнути	test-Шаблон на весь день	
22	005	Владислав	All Departments/ТП	2026/06/18 16:41:22	2036/06/18 23:59:59	5672	Чоловік			Вимкнути	Вимкнути	Вимкнути	test-Шаблон на весь день	
23	004	Катерина	All Departments/ТП	2026/06/18 16:41:22	2036/06/18 23:59:59	5672	Жінка			Вимкнути	Вимкнути	Вимкнути	test-Шаблон на весь день	
24	003	Артем	All Departments/ТП	2026/06/18 16:41:22	2036/06/18 23:59:59	5672	Чоловік			Вимкнути	Вимкнути	Вимкнути	test-Шаблон на весь день	
25	002	Максим	All Departments/ТП	2026/06/18 16:41:22	2036/06/18 23:59:59	5672	Чоловік			Вимкнути	Вимкнути	Вимкнути	test-Шаблон на весь день	

Рисунок 4.10 Інформація про експортованих осіб

Управління персоналом та його експорт

Ви можете додавати нові профілі співробітників різними способами. Під час завантаження шаблонів для імпорту користувачів усі додаткові системні поля будуть автоматично включені. Якщо вам потрібно експортувати фотографії профілів користувачів на свій ПК, спочатку необхідно увімкнути відповідний дозвіл, перейшовши в меню **Система → Конфігурація системи → Безпека → Конфіденційність і безпека → Зберегти дані моделі тільки для зображення профілю**.

Зберігання видалених даних користувачів

Коли особу видаляють із системи, її основні дані (включно з ім'ям, ідентифікаційним номером, терміном дії та обліковими даними) тимчасово архівуються, а не видаляються одразу. Щоб налаштувати, скільки саме часу ця інформація зберігатиметься перед остаточним видаленням, перейдіть до розділу **Система → Конфігурація системи → Зберігання → Період зберігання даних → Видалені особи**.

4.2.1 Налаштування Облікових Даних

Переконайтеся, що вибрано правильний режим збору даних та правильно налаштовано пристрій збору.

На сторінці «Особа» натисніть **Конфігурація сертифіката**. Виберіть режим збору даних відповідно до наведеної нижче таблиці.

Таблиця 4.1 Сценарії, що застосовуються для різних режимів збору даних

Пристрій збору даних	Сценарій
- Станція реєстрації карток - Пристрій для	Ідеально підходить для мобільних операцій з реєстрації, під час яких адміністраторам доводиться виїжджати в різні місця для фізичного зчитування карток, фотографування

зчитування відбитків пальців	обличчя та зняття відбитків пальців на місці.
• USB-камера	
Пристрій контролю доступу	Призначений для віддаленого зчитування даних про посвідчення за допомогою стаціонарно встановленого обладнання. Пристрій повинен підтримувати цю функцію та бути попередньо доданим до системи. (Примітка: Якщо система не може зчитати номер картки, перейдіть на сторінку «Деталі дверей», щоб переконатися, що ці двері наразі перебувають у режимі охоронної сигналізації.)
Пункт реєстрації	Універсальні портативні пристрої, що підключаються через USB або мережу для зчитування зображень обличчя, карток та відбитків пальців. Ці станції дають змогу зберігати зібрані ідентифікаційні дані локально, безпосередньо на самому пристрої.

4.2.2 Захист зображень профілю

Ознайомтеся з цією темою, якщо вам потрібно захистити свої фотографії профілю.

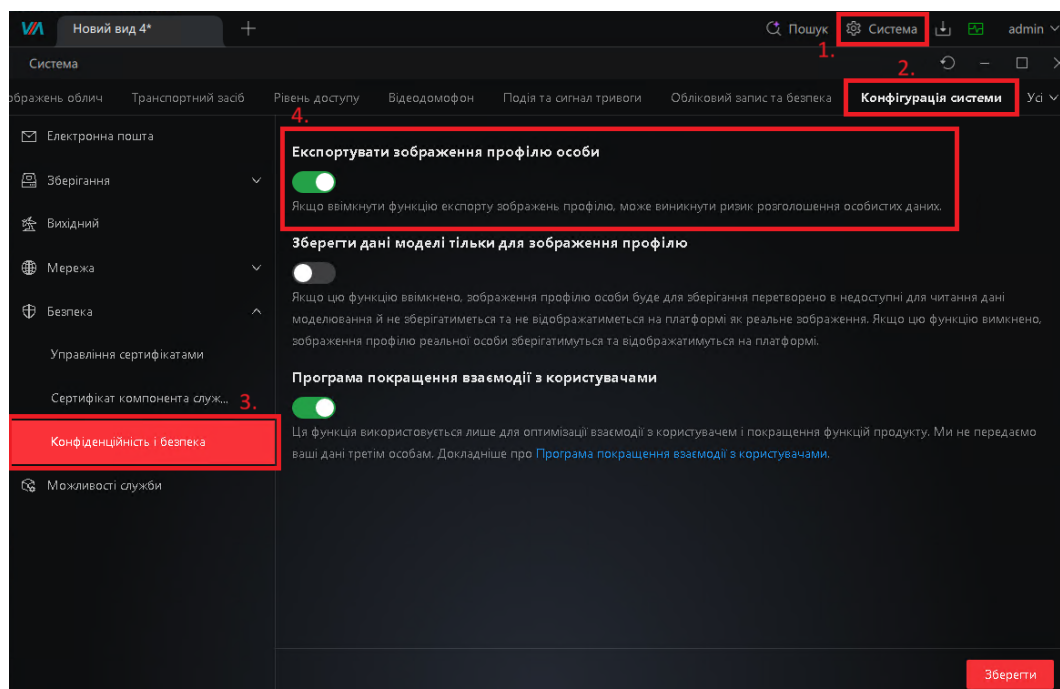


Рисунок 4.11 Увімкнення функції експорту зображень профілю особи

Експортувати фотографію профілю особи

Якщо ви увімкнете цю функцію, ви зможете експортувати фотографії профілів користувачів на ПК.

(Примітка: увімкнути цю функцію може лише адміністратор.)

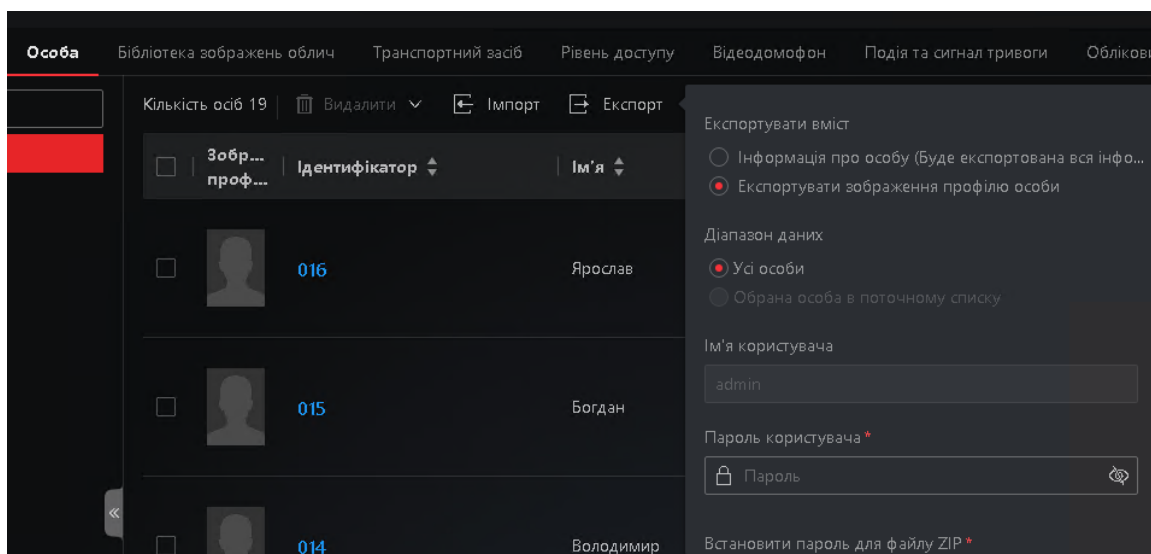


Рисунок 4.12 Введення експорту зображень профілю

4.3 Управління рівнями доступу

Рівень доступу об'єднує певні двері з визначеним графіком, точно визначаючи, хто саме може відчиняти які двері та коли. Ви можете оптимізувати управління безпекою, застосовуючи ці правила як до окремих співробітників, так і до цілих відділів.

Будьте обережні при використанні цієї функції, оскільки рівні доступу, збережені в пристроях, будуть скинуті і їх неможливо буде відновити!

Огляд рівнів доступу

Клацніть правою кнопкою миші на відділі, щоб призначити новий рівень доступу або скасувати рівні доступу для співробітників.

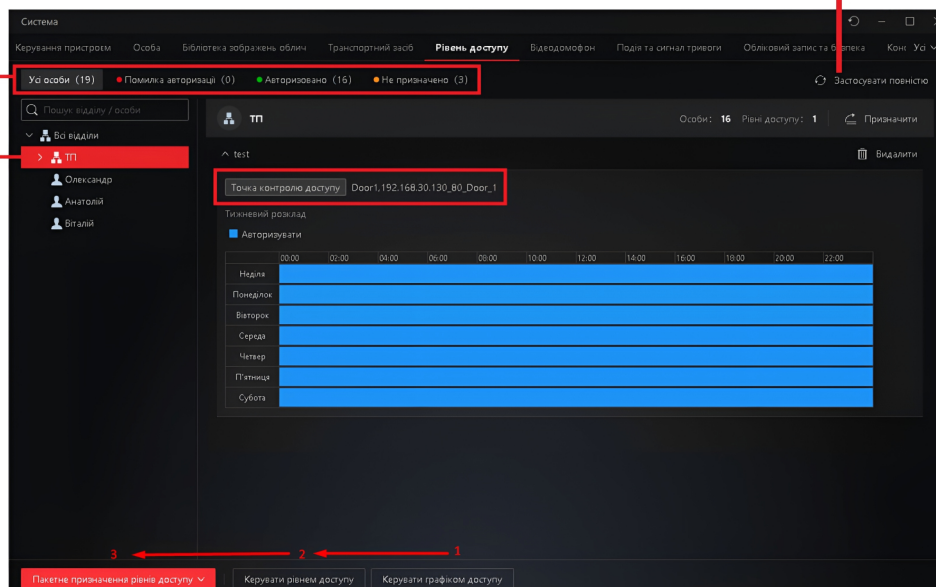


Рисунок 4.13 Сторінка рівнів доступу

Додати графік доступу

Графіки визначають, коли дозволено вхід. Ви можете скористатися трьома наданими шаблонами («Цілий день», «Робочий день» та «Вихідні») або створити власні параметри. Натисніть **«Авторизувати»** і перетягніть курсор по часовій шкалі, щоб позначити дозволені періоди часу. Для точного налаштування наведіть курсор на синій блок з дозволом доступу, щоб вручну ввести або скоригувати точний час.

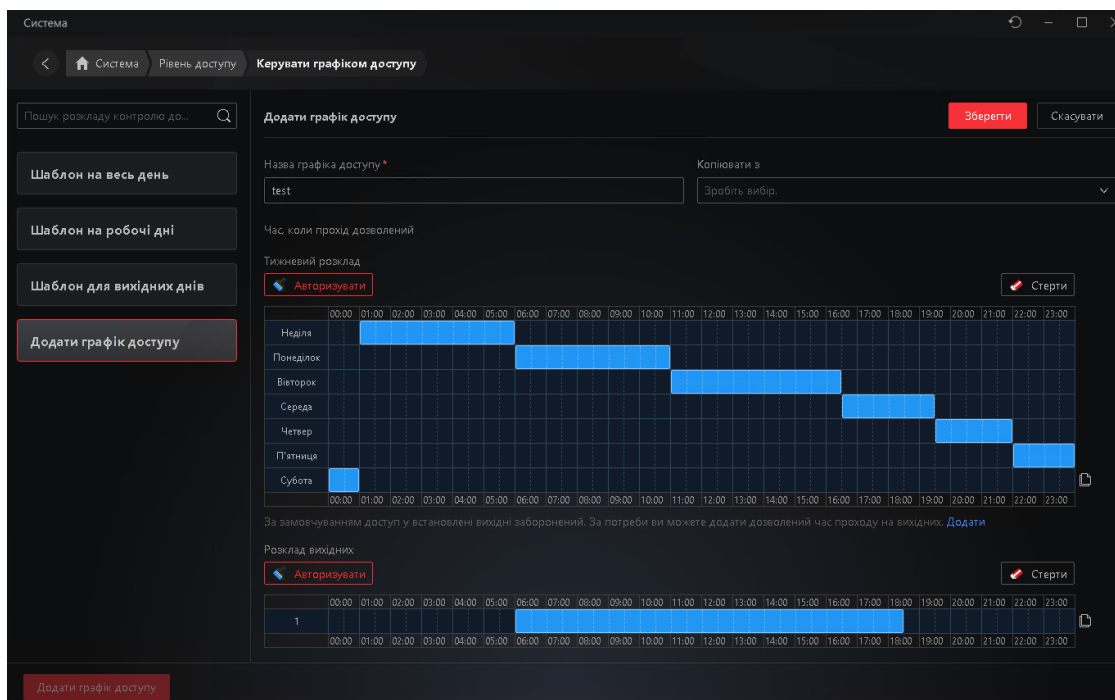


Рисунок 4.14 Додати графік доступу

Додати рівень доступу

Після встановлення розкладу виберіть відповідні двері, щоб остаточно визначити рівень доступу. Зверніть увагу, що одні й ті самі двері можуть одночасно входити до складу кількох різних рівнів доступу.

Присвоєння прав доступу:

1. **За відділом:** Рекомендується для надання стандартного доступу до певних приміщень, таких як загальні офісні зони. Будь-який новий співробітник, доданий до цього відділу, автоматично отримає відповідні рівні доступу.
2. **За особою:** Ідеально підходить для надання окремого користувачеві тимчасових дозволів або вузькоспеціалізованого доступу до дверей з обмеженим доступом.

Апаратна синхронізація

Рівні доступу, призначені за допомогою клієнтського програмного забезпечення, автоматично передаються на фізичне обладнання. Якщо призначення не вдалося

застосувати, переконайтеся, що цільовий пристрій не перебуває в автономному режимі та що мережеве з'єднання залишається стабільним.

4.4 Додати сигнал тривоги

Ви можете додати сповіщення для певного пристрою або для всіх ресурсів у системі.

Сповіщення можуть ініціювати як двері, так і пристрої контролю доступу та відеодомофони. Перейти на сторінку **Налаштування сигналу тривоги** можна зі сторінки детальної інформації про пристрій або з модуля **Події та сигнал тривоги**.

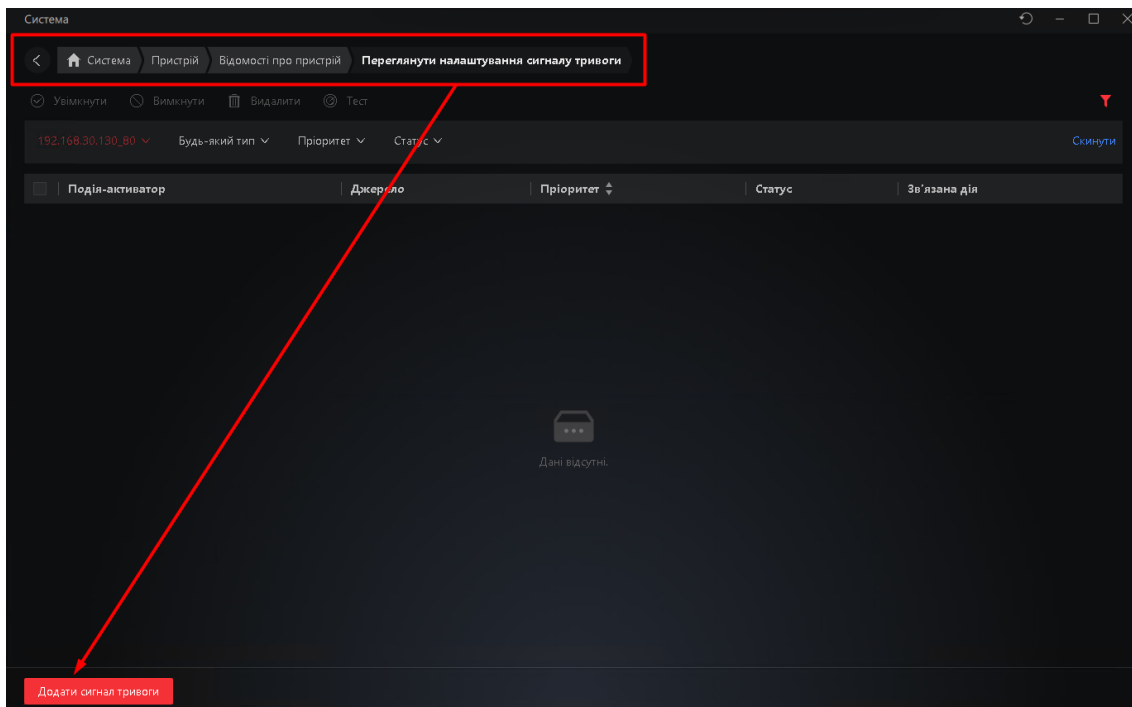


Рисунок 4.15 Сторінка налаштування сигналу тривоги

Джерела, що можуть викликати спрацьовування сигналізації	Категорія сигналізації
Двері	- Звичайне зчитування картки - Нестандартне зчитування картки - Інші події, пов'язані з дверима
Пристрій контролю доступу/відеодомофон	- Безпека пристрою - Мережа пристрою - Акумулятор пристрою

	• Звітність щодо записів пристрою • Диск/жорсткий диск пристрою • Зв'язок між компонентами пристрою • Локальне керування пристроєм • Дистанційно через платформу
Вхід сигналізації	• Спрацьовування сигнального входу • Відновлення сигнального входу
Особа	• Подія, пов'язана з ідентифікацією особи • Подія, пов'язана з номером картки

4.5 Моніторинг Дверей у Режимі Реального Часу

Ви можете відстежувати стан дверей та керувати ним у режимі реального часу. Пояснення наведено в таблиці нижче.

Таблиця 4.2 Пояснення щодо стану дверей, стану дверного контакту, стану дверного замка та керування станом дверей

Статус	Піктограма	Пояснення
Статус дверей		Двері заблоковані Замок дверей заблоковано

		Двері заблоковані Замок дверей залишається заблокованим
		Двері заблоковані Замок дверей розблоковано
		Двері заблоковані Замок дверей залишається розблокованим
		Двері відчинені Дверний замок заблоковано
		Двері відчинені Замок дверей залишається заблокованим
		Двері відчинені Замок дверей відчинено
		Двері відчинені Замок дверей залишається розблокованим
		Невідомо
Стан дверного контакту		Контакт дверей розблоковано
		Контакт дверей заблоковано
Стан дверного замка		Замок дверей розблоковано
		Замок дверей заблоковано
Контроль стану		Закрити двері

дверей		Відкрити двері
		Установити, щоб двері залишалися заблокованими
		Встановити, щоб двері залишалися відчиненими

4.5.1 Моніторинг дверей та контроль їхнього стану

Після налаштування дверей оператори можуть керувати станом замків та переглядати відео в режимі реального часу (якщо двері оснащені камерою або підключені до неї).

Управління окремими дверима

Двічі клацніть на дверях або перетягніть їх у сітку перегляду. Клацніть правою кнопкою миші на елементі або скористайтеся піктограмами в правому нижньому куті, щоб змінити стан замка.

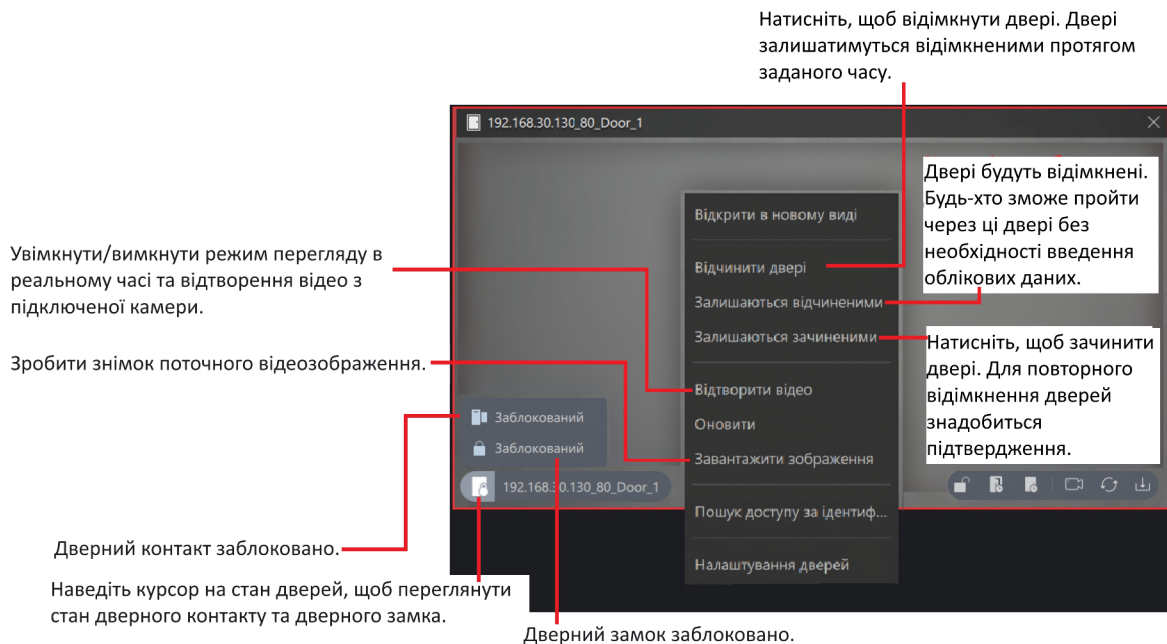


Рисунок 4.16 Підтримувані операції для керування одними дверима

Функції камери

Для дверей із підключеною відеосистемою доступні додаткові опції безпосередньо в вікні перегляду: запуск/зупинка прямої трансляції, зйомка знімків, запис відео та двосторонній аудіозв'язок.

Управління декількома дверима

- **Поточний вигляд:** Намалюйте рамку виділення навколо декількох дверей у сітці, а потім клацніть правою кнопкою миші, щоб застосувати масові команди. Крім

того, використовуйте верхні піктограми стану для пакетного керування всіма дверима, що наразі видно.

- **Глобальне керування:** перейдіть до області **Ярлики** та скористайтесь функцією «Швидке блокування/розблокування», щоб миттєво глобально заблокувати, розблокувати або захистити всі двері системи.

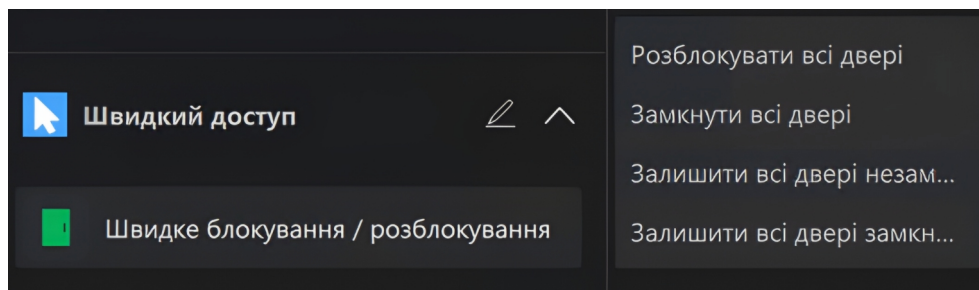


Рисунок 4.17 Вхід для керування всіма дверима

Усунення несправностей у виняткових ситуаціях

Якщо система повідомляє про невідповідність між магнітним контактом дверей та їхнім станом блокування, це зазвичай вказує на фізичну перешкоду, що заважає правильному закриттю. Необхідно негайно провести фізичний огляд обладнання.

4.5.2 Відображення та керування дверима на карті

Модуль **Карта** надає географічний інтерфейс для управління точками входу та потоковим відео з камер, включаючи термінали розпізнавання обличчя та двері, пов'язані з камерами.

Доступ до карт

Перейдіть до модуля **Карта**. Відкрийте карту, двічі клацнувши по ній, перетягнувши її до головного вікна перегляду або клацнувши правою кнопкою миші та вибравши пункт **Відкрити**.

Додати карту

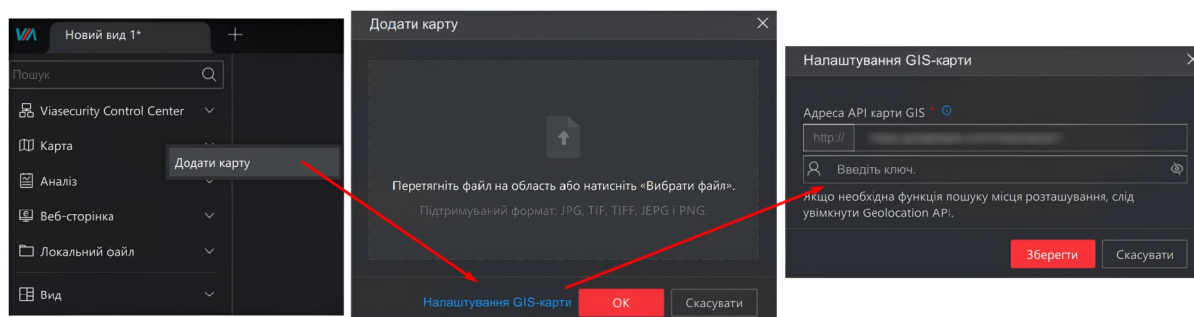


Рисунок 4.18 Додати GIS карту

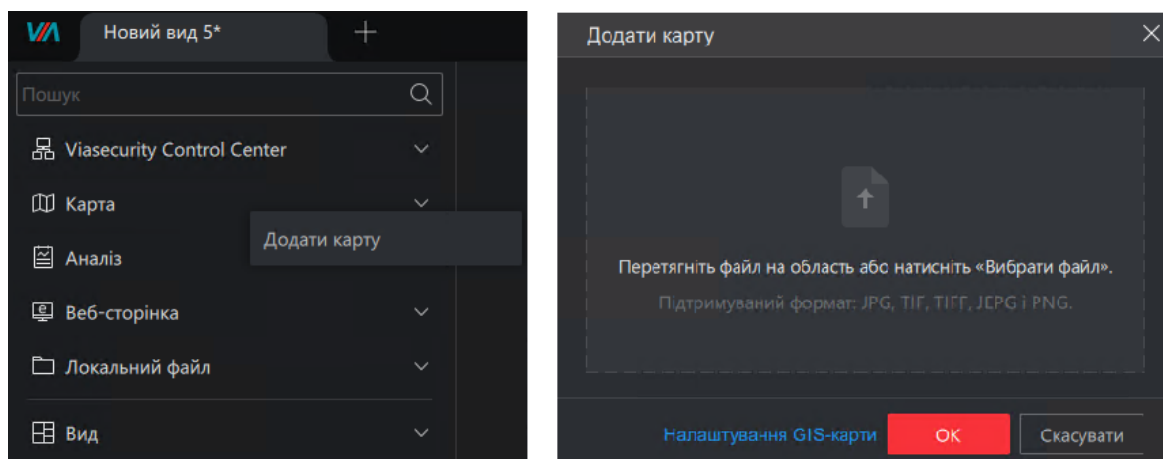


Рисунок 4.19 Додати статичну карту

Режими роботи

Інтерфейс карти використовує два окремі режими для відокремлення налаштувань від повсякденних операцій:

Режим конфігурації

Використовуйте цей режим для створення макета. Ви можете додавати двері, розміщувати маркери, визначати активні зони та вибирати, які ресурси відображатимуться на карті.

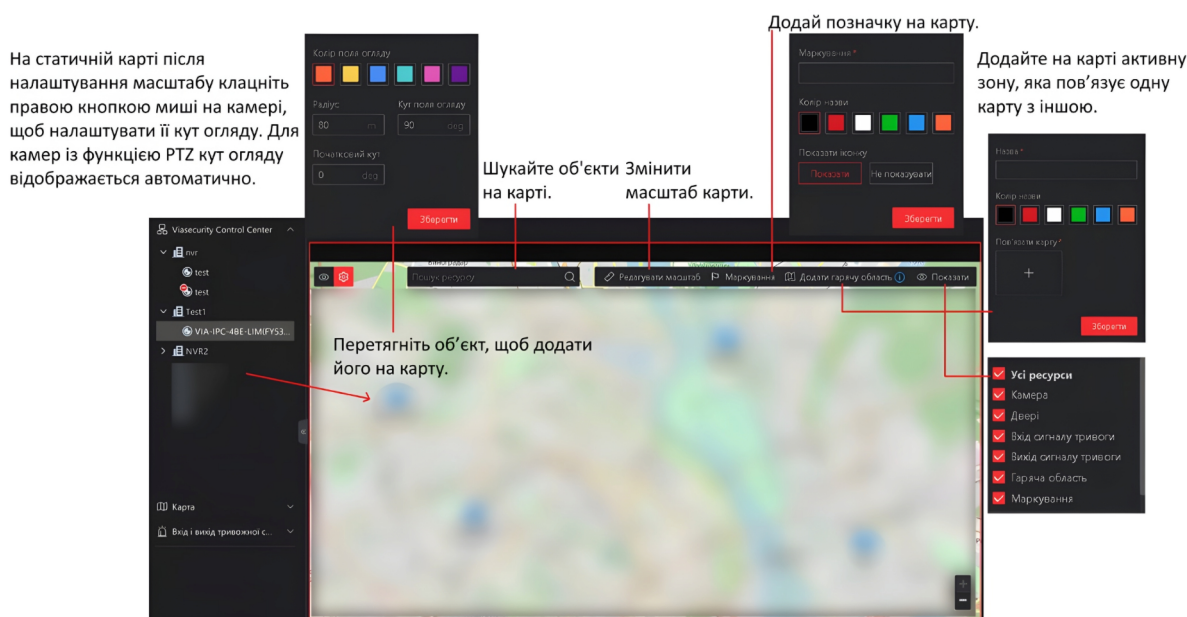


Рисунок 4.20 Підтримувані операції в режимі конфігурації

Режим моніторингу

Використовуйте цей режим для активних операцій безпеки, перегляду в режимі реального часу та керування дверима.

Дії в режимі моніторингу

- **Операції з окремими дверима:** клацніть на піктограму дверей, щоб негайно запустити пряму трансляцію з підключеної камери. Щоб змінити стан замка, просто клацніть правою кнопкою миші на дверях.
- **Операції з групою:** щоб переглядати кілька трансляцій одночасно, натисніть **Вибрати групу**, обведіть виділеною областю цільові двері на карті та натисніть **Відтворити групу**, щоб одночасно відкрити всі пов'язані трансляції в реальному часі.

4.6 Налаштування та робота відеодомофона

Люди можуть дзвонити користувачам системи через пристрої контролю доступу та відеодомофони, а користувачі також можуть дзвонити на пристрій через клієнт.

Параметри конфігурації

Перед використанням домофона адміністратори повинні визначити правила маршрутизації дзвінків та часові обмеження:

- **Одержувачі дзвінків:** Ви можете призначити конкретні апаратні пристрої для дзвінків на певних операторів клієнта, гарантуючи, що дзвінки надходять до відповідного персоналу.
- **Час автоматичного завершення дзвінка після відсутності відповіді:** встановіть тривалість автоматичного завершення дзвінка; якщо оператор не відповість на вхідний дзвінок з пристрою протягом цього часу, система автоматично завершить його.
- **Макс. тривалість дзвінка:** Застосуйте суворий максимальний часовий ліміт для будь-якої активної, триваючої розмови між польовим пристроєм та клієнтським програмним забезпеченням.

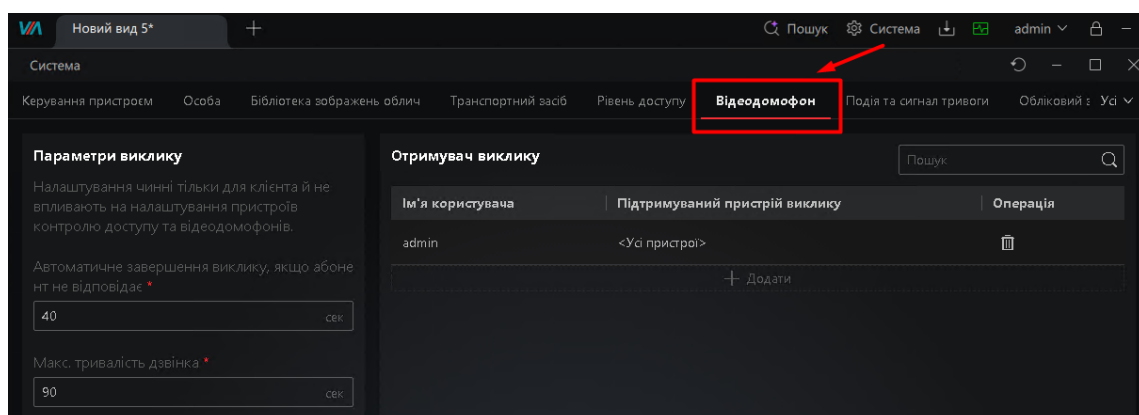


Рисунок 4.21 Вхід у відеодомофон

Дзвінок через відеодомофон

Оператори клієнта можуть ініціювати зв'язок з апаратними пристроями двома основними способами:

- **Через сповіщення про пропущені дзвінки:** якщо відвідувач намагається зателефонувати клієнту, а оператор пропускає дзвінок, у панелі сповіщень з'являється сповіщення. Клацніть правою кнопкою миші на цьому сповіщенні, перейдіть до **Переглянути деталі** та виберіть **Зворотний виклик**, щоб миттєво набрати номер пристрою.

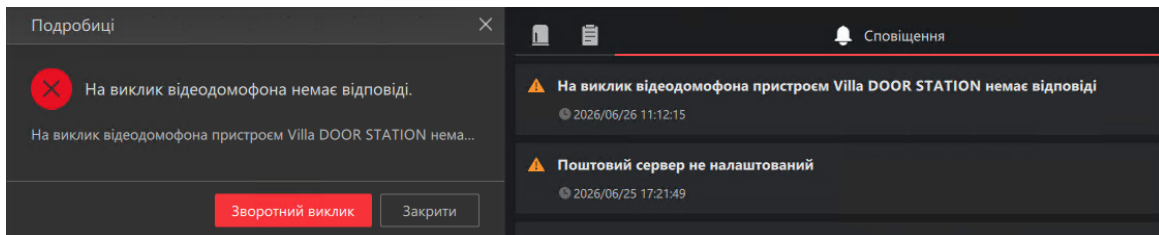


Рисунок 4.22 Дзвінок на пристрій

- **Через прямий перегляд:** під час активного перегляду прямої трансляції з камери, пов'язаної з дверима, клацніть на відповідну піктограму домофона на інтерфейсі, щоб відкрити двосторонній аудіоканал.

4.7 Управління подіями, пошук та аналітика

У цьому розділі зібрано всі інструменти, необхідні для відстеження активності об'єкта, відновлення офлайн-журналів та візуалізації даних системи.

4.7.1 Пошук та експорт журналів подій

Оператори можуть досліджувати історію активності системи, перейшовши до меню **Пошук → Події системи контролю доступу**. Ви можете фільтрувати пошук за трьома основними категоріями:

- **Подія автентифікації особи:** перегляньте історію як успішних (нормальних), так і невдалих (аномальних) сканувань облікових даних.

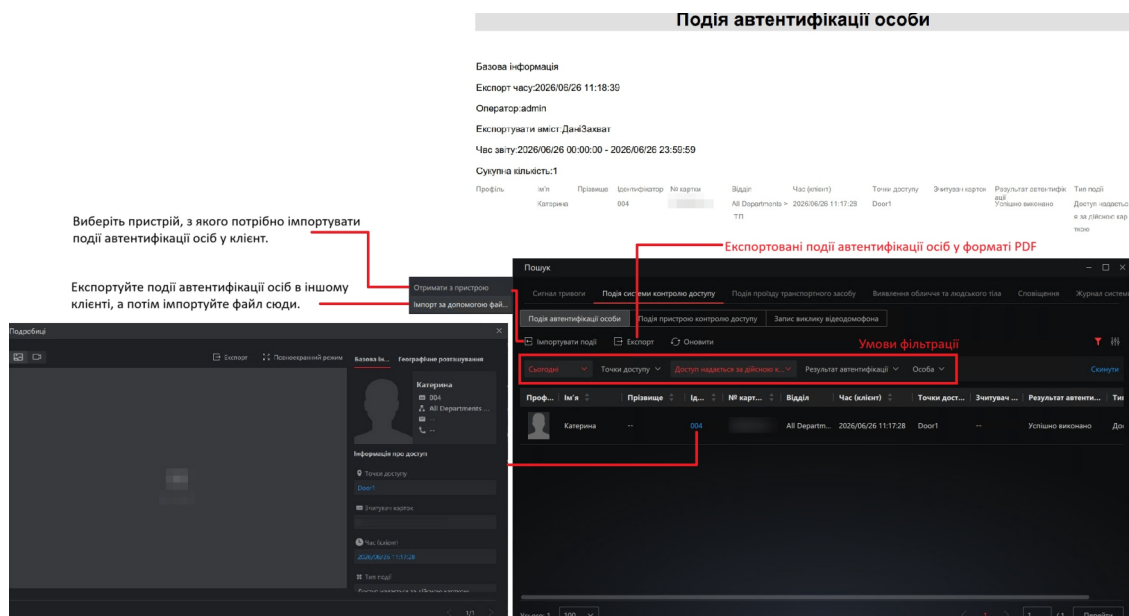


Рисунок 4.23 Подія автентифікації особи

- **Подія пристрою контролю доступу:** відстежуйте події на рівні апаратного забезпечення, такі як стан розблокованих дверей або загальні тригери пристрою.

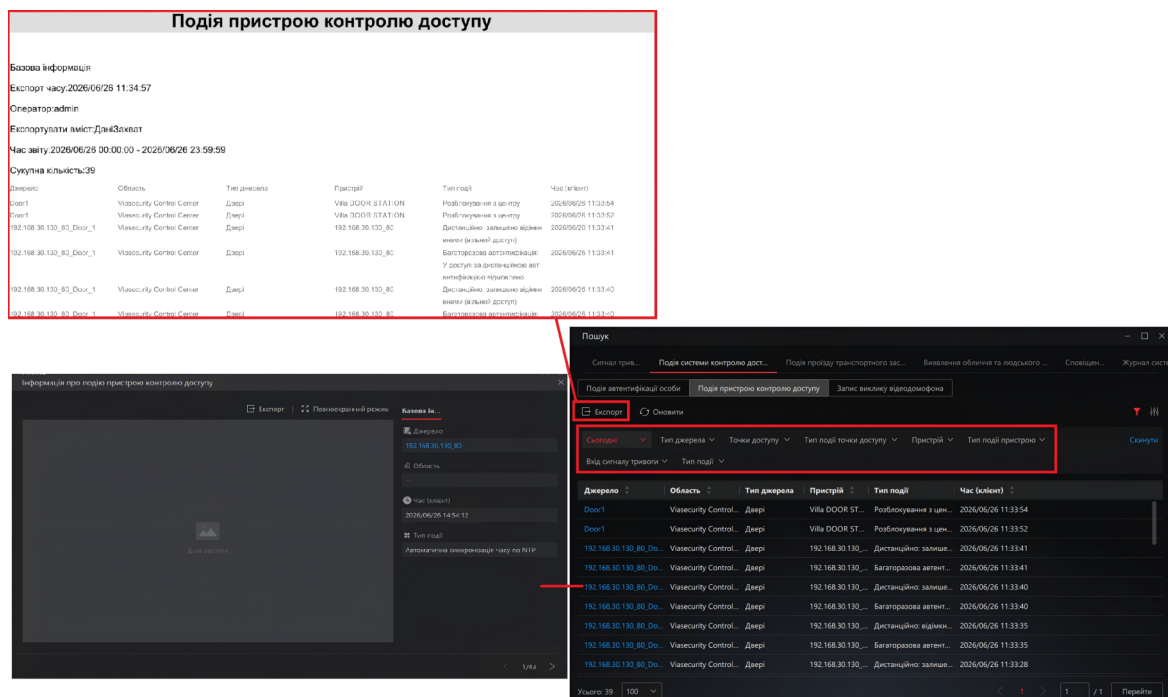


Рисунок 4.24 Подія пристрою контролю доступу

- **Запис виклику відеодомофона:** доступ до повного історичного запису всіх дзвінків, ініційованих з польових пристроїв до клієнта.

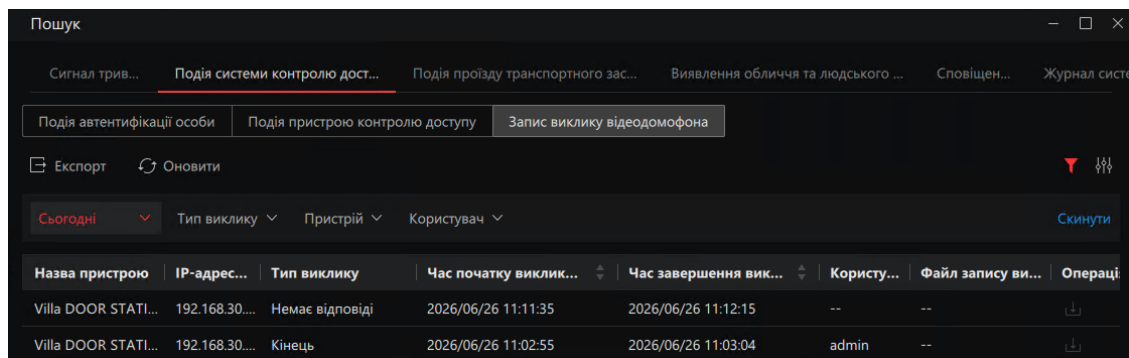


Рисунок 4.25 Записи дзвінків відеодомофона

Запис виклику відеодомофона

Базова інформація

Експорт часу: 2026/06/26 15:13:36

Оператор: admin

Експортувати вміст: Дані

Час звіту: 2026/06/26 00:00:00 - 2026/06/26 23:59:59

Сукупна кількість: 2

Назва пристрою	IP-адреса пристрою	Тип виклику	Час початку виклику (клієнт)	Час завершення виклику (клієнт)	Корист. Файл запису виклику
Villa DOOR STATION	192.168.30.181	Немає відпові	2026/06/26 11:11:35	2026/06/26 11:12:15	увач
Villa DOOR STATION	192.168.30.181	Кінець	2026/06/26 11:02:55	2026/06/26 11:03:04	admin

P

исунок 4.26 Експортовані записи дзвінків відеодомофона

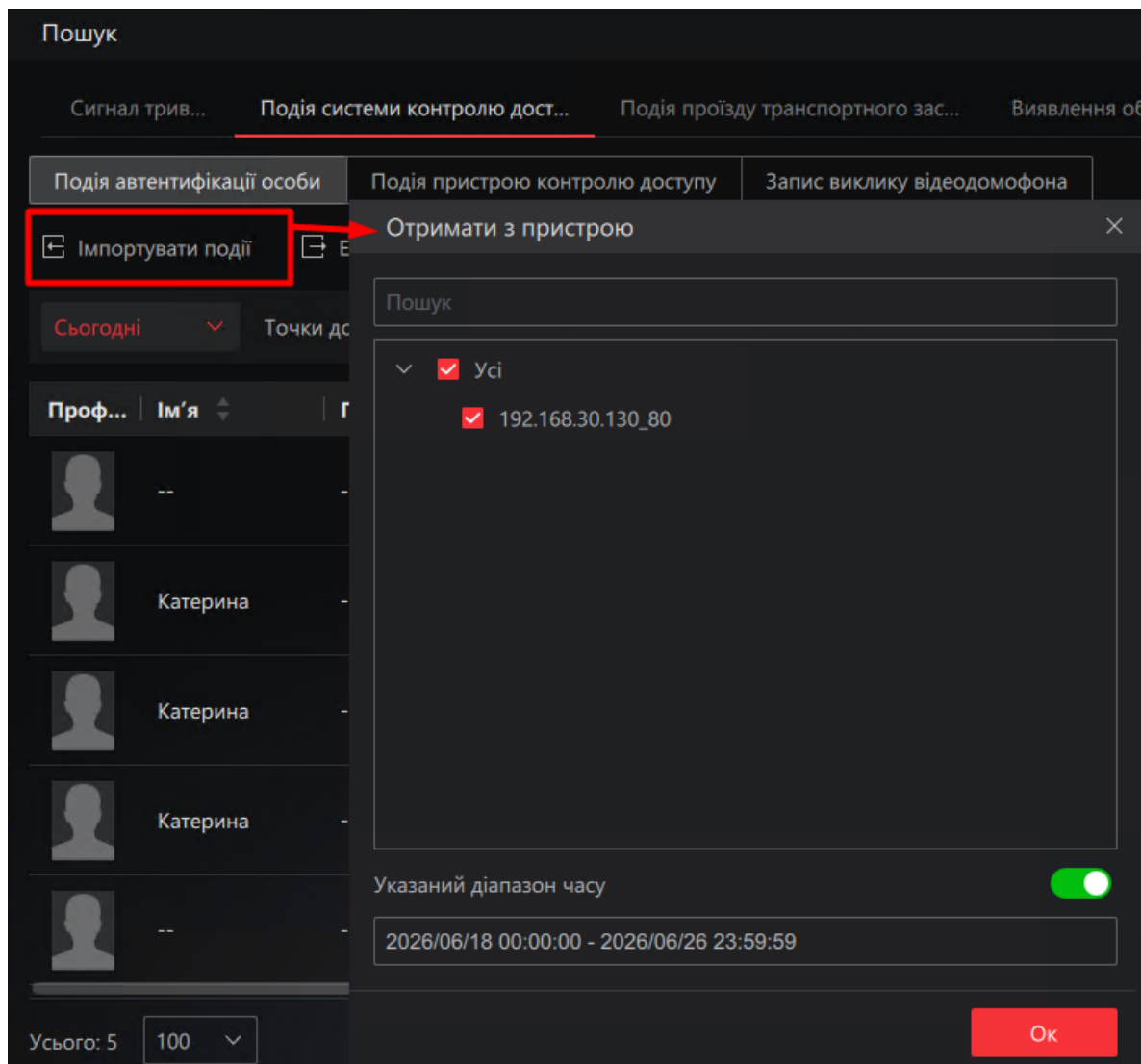


Рисунок 4.27 Отримання подій з пристрою

4.7.2 Імпорт відсутніх журналів автентифікації

Якщо через перебої в роботі мережі клієнт пропустив події доступу в режимі реального часу, ви можете вручну синхронізувати ці записи з апаратним забезпеченням.

Перейдіть до **Пошук** → **Подія системи контролю доступу** → **Подія автентифікації особи**.

- **Отримати з пристрою (онлайн-пристрої):** виберіть цільове обладнання, вкажіть відповідний часовий проміжок і завантажте збережені події безпосередньо через мережу.
- **Імпорт за допомогою файлу (пристрої в автономному режимі):** для обладнання, повністю відключеного від мережі, вставте USB-накопичувач безпосередньо в пристрій та експортуйте записи. Перенесіть накопичувач на ПК клієнта та імпортуйте файл CSV.

(Примітка: система приймає лише зашифровані файли. Крім того, імпортований файл повинен відповідати суворим правилам іменування: recordlist_ [Серійний номер пристрою] (наприклад, recordlist_FC2922753).)

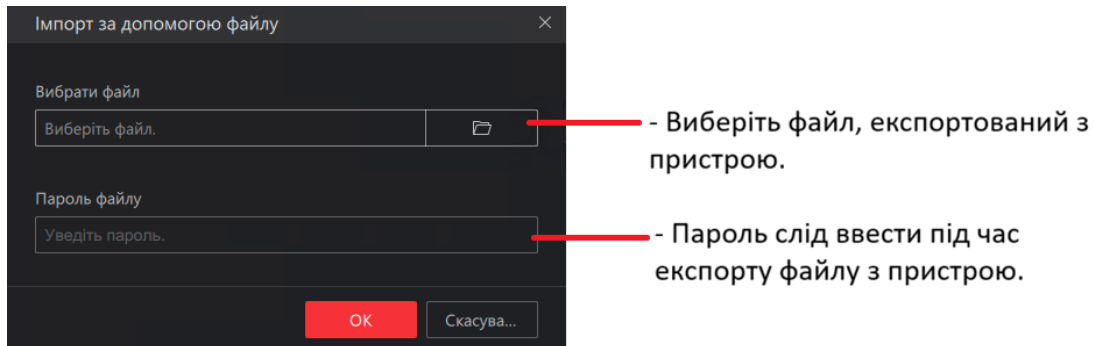


Рисунок 4.28 Імпорт подій через файл

4.7.3 Статистика даних та інформаційні панелі

Програмне забезпечення надає вичерпний візуальний огляд вашого середовища фізичної безпеки, детально показуючи активний персонал, зареєстровані облікові дані, налаштовані рівні доступу та щоденні обсяги подій.

Щоденна аналітика

Швидко перегляньте сьогоднішні показники доступу, зокрема загальну кількість успішних входів («Звичайний доступ за допомогою аутентифікації») та відхилених спроб («Доступ заборонено»).

Інтерактивне управління

Панель управління повністю інтерактивна. Натиснувши на статистичний показник, ви перейдете безпосередньо на відповідну сторінку налаштувань, де зможете внести зміни в режимі реального часу.

Звітність

Клацніть правою кнопкою миші на будь-якому статистичному звіті, щоб відкрити його в окремому вікні перегляду, оновити потік даних або експортувати візуальний звіт у форматі PDF.

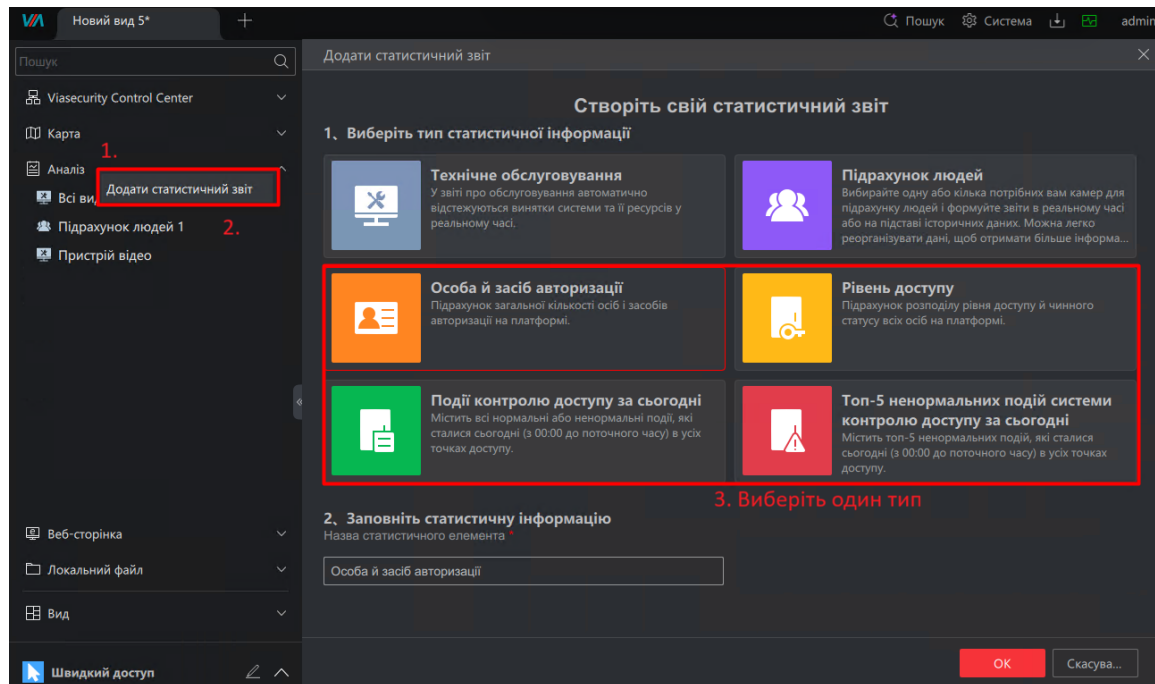


Рисунок 4.29 Додати звіт зі статистикою

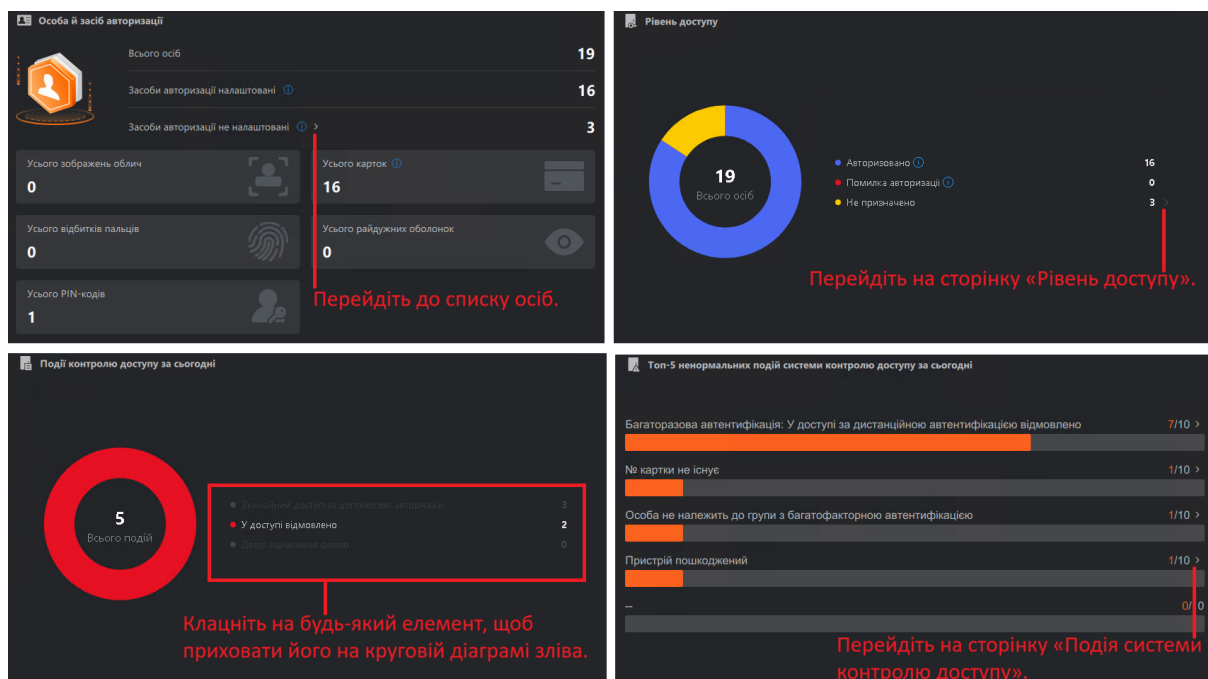


Рисунок 4.30 Статистика

Розділ 5 Управління сховищем

Viasecurity Control Center забезпечує централізований механізм зберігання на сервері для архівування відеопотоків, знятих зображень та пов'язаних файлів. Цей модуль дозволяє адміністраторам виділяти певний дисковий простір, встановлювати графіки запису з камер та визначати чіткі терміни зберігання системних даних, включаючи журнали та події.

Відео

Зберігає відеозаписи з камер, що ведуть безперервний запис за часом або запускаються за подіями, відповідно до встановлених графіків.

Зображення та файли

Зберігає ручні знімки, знімки, пов'язані з тривогами, та аудіофайли, створені відеодомофонами.

Щоб налаштувати ці параметри, натисніть **Система → Конфігурація системи → Зберігання → Системне сховище / Період зберігання даних** у правому верхньому куті робочого столу.

(Примітка: Нові користувачі можуть активувати 30-денну пробну ліцензію, яка підтримує збереження відеозаписів з максимум 4 каналів. Якщо ви подасте заявку на отримання офіційної ліцензії під час дії пробної версії, система збереже пробні функції до закінчення початкового 30-денного терміну.)

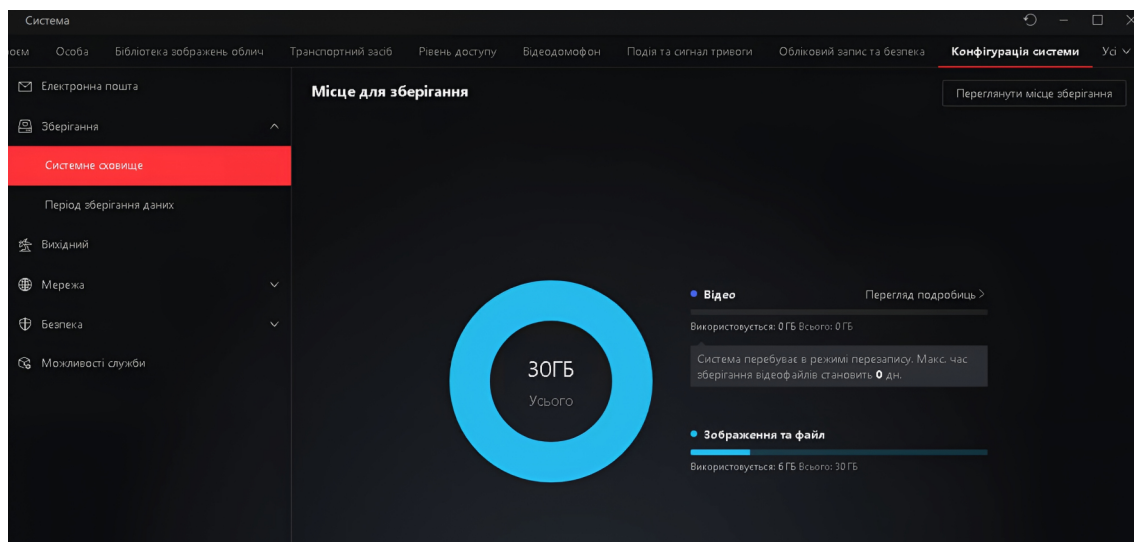


Рисунок 5.1 Налаштування сховища

5.1 Підготовка

Перед ініціалізацією місць зберігання переконайтеся, що виконано такі системні вимоги:

- Функція зберігання відео стає доступною лише після активації пробної ліцензії або офіційно придбаної ліцензії.
- Ви повинні додати системний процес зберігання даних до списку дозволених процесів брандмауера вашого сервера. Якщо цей процес не буде додано до списку дозволених, необхідні мережеві порти будуть заблоковані, що призведе до перевищення часу очікування під час з'єднання або до відмови у з'єднанні. Якщо брандмауер заблокує службу зберігання даних, у панелі **Сповіщення** на головній панелі з'явиться попередження про виняток.

5.2 Розташування сховища та розподіл ємності

У цьому розділі описано, як визначити місце збереження даних та як розподілити доступний простір на диску між відеоархівами та статичними мультимедійними даними (зображеннями та файлами).

Визначення шляху до сховища

Щоб керувати дисками для зберігання даних, натисніть **Переглянути місце зберігання** у правому верхньому куті інтерфейсу.

1. Система автоматично надає пріоритет диску з найбільшим вільним об'ємом. За замовчуванням увімкнено циклічне перезаписування, що забезпечує безперебійну роботу завдяки автоматичній заміні найстаріших файлів, коли диск заповнюється.
2. Натисніть на піктограму повзунка, щоб ініціалізувати додаткові диски для зберігання даних. Зверніть увагу, що використання динамічних дисків та дисків, відформатованих у форматі, відмінному від NTFS, суворо заборонено.

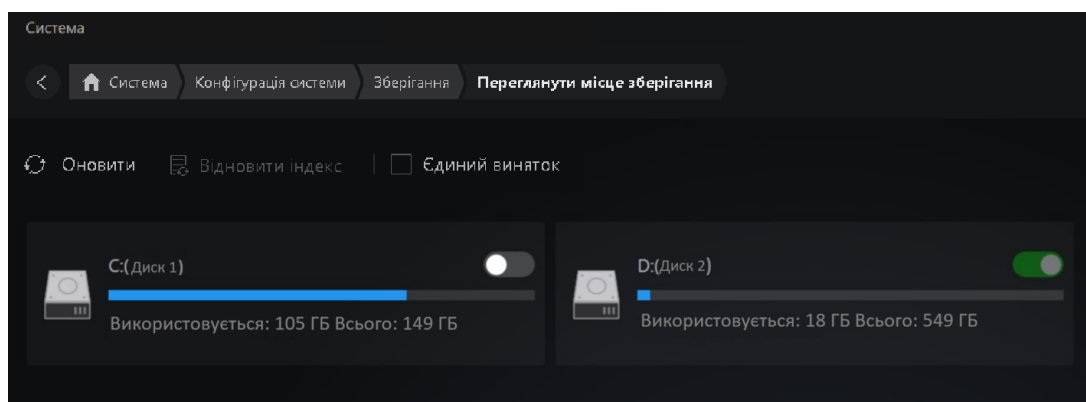


Рисунок 5.2 Місце зберігання

Рекомендації щодо обслуговування та заміни дисків

Ручне видалення файлів безпосередньо з диска або переведення диска в автономний режим призведе до остаточного знищення важливих записів. У такому випадку система видасть попередження.

Перед заміною диска завжди спочатку створюйте резервну копію наявних даних. Переконайтеся, що ємність нового диска дорівнює або перевищує ємність старого.

Покрокові інструкції щодо заміни: Спочатку вимкніть активний логічний диск і видаліть пов'язані з ним файли. Далі створіть нову літеру диска спеціально для цього місця зберігання даних і перевірте його робочий стан. Не змінюйте літеру диска в операційній системі, оскільки це може спричинити збої в роботі.

Налаштування простору для зберігання даних

Ви повинні розподілити загальний обсяг сховища між відеопотоками та іншими медіаформатами (такими як зображення та аудіо).

- Натисніть «Налаштувати простір для зберігання» у меню вгорі праворуч.
- Перетягніть  на круговій діаграмі, щоб визначити співвідношення розподілу. Або введіть вручну числове значення для однієї категорії, і система автоматично розрахує баланс для іншої.

5.3 Налаштування графіка зберігання

Ви можете створити графіки запису для окремих камер або застосувати налаштування до декількох пристроїв одночасно. Перейдіть до налаштувань, натиснувши **Система → Конфігурація системи → Зберігання → Перегляд подробиць**, у вас відкриється сторінка **Інформація сховища відеофайлів**. Натисніть **Додати**, щоб створити новий графік запису. Існуючі графіки можна редагувати безпосередньо у списку камер. Перш ніж продовжувати, завжди переконайтеся, що у вашій системі є достатньо вільного місця на диску.

Режими запису та налаштування потоку

Тип розкладу

Виберіть: застосувати готовий шаблон розкладу або створити власний графік. Вам потрібно вибрати між безперервним записом за розкладом протягом заданого періоду часу або записом, що запускається за подією, який активується лише під час спрацьовування сигналу тривоги.

Вибір потоку

Виберіть «Головний потік», «Додатковий потік» або «Подвійний потік» відповідно до ваших вимог щодо якості відтворення та енергоспоживання. При використанні «Додаткового потоку» можна увімкнути опцію **Використовувати основний потік для запису відео, запущеного подією**. Ця функція автоматично здійснює запис відео з

високою роздільною здатністю при виникненні події, а під час відтворення події система надаватиме пріоритет саме цьому матеріалу з основного потоку.

Політики зберігання та перезапису даних

Час зберігання

Увімкніть опцію **Перезаписати після завершення часу зберігання**, щоб відео автоматично видалялися після закінчення визначеного вами терміну зберігання. Якщо залишити цю опцію вимкненою, система перейде на стандартний алгоритм «першим прийшов — першим пішов», перезаписуючи найстаріші збережені відео лише тоді, коли місце на диску буде вичерпано.

Міграція локальних пристроїв

Якщо ви перенесете камеру з активного локального розкладу (де місце зберігання було встановлено як «Локальний пристрій») до системного сховища, система автоматично увімкне функцію перезапису даних та встановить стандартний 30-денний термін зберігання.

Планування потужностей

Під час налаштування система аналізує загальний обсяг місця на диску та забезпечує встановлення відповідних термінів зберігання. Встановлення надмірно тривалих термінів зберігання для однієї камери може негативно вплинути на обсяг місця, необхідний іншим пристроям у мережі.

Удосконалення мережі та безпеки

Автоматичне зворотне копіювання

Увімкніть цю функцію захисту на випадок збою, щоб тимчасово зберігати відеодані в кеші на пристрої у разі втрати мережевого з'єднання. Після відновлення з'єднання відео з кешу автоматично переноситься на основний пристрій зберігання даних.

Маршрутизація на сервері потокового передавання

Вибір призначеного сервера для потокового передавання дозволяє оптимізувати використання пропускної здатності мережі та заощадити її.

Інструкції з налаштування пакетної обробки

Щоб одночасно налаштувати параметри для декількох камер, виберіть потрібні камери зі списку та натисніть **Налаштувати параметри запису**.

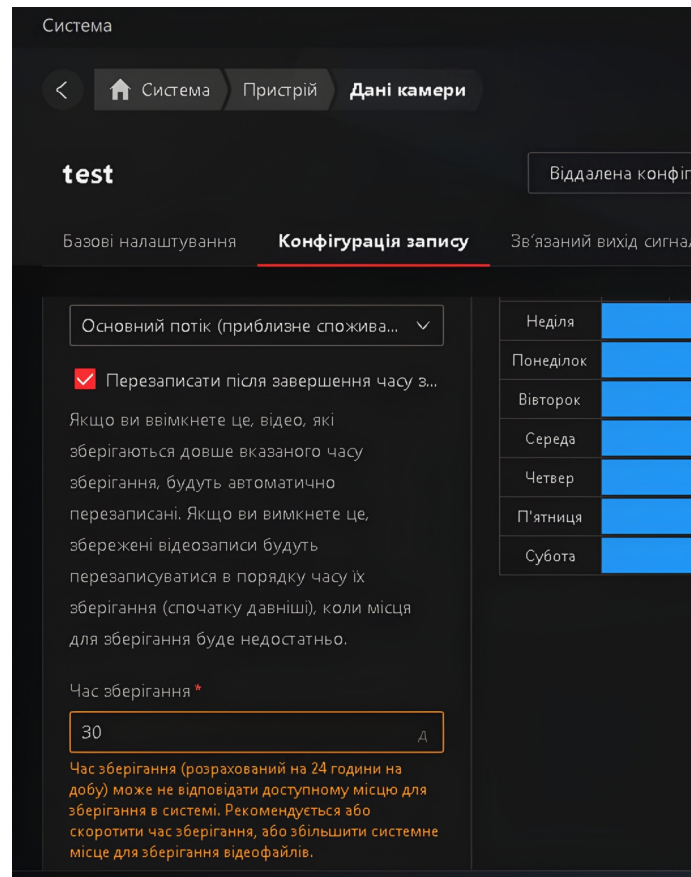


Рисунок 5.3 Налаштування запису для камери

5.4 Відтворення відео та пошук VCA

Viasecurity Control Center забезпечує безперебійне відтворення всіх відеозаписів, що зберігаються в системі зберігання даних. Крім того, оператори можуть використовувати функцію аналізу відеоконтенту (VCA) для ефективного пошуку конкретних подій. Система дозволяє здійснювати цільову фільтрацію, виділяючи людей, транспортні засоби або поєднання обох об'єктів.

Детальні інструкції наведено в розділі [3.5.1 Смарт-пошук / VCA](#).

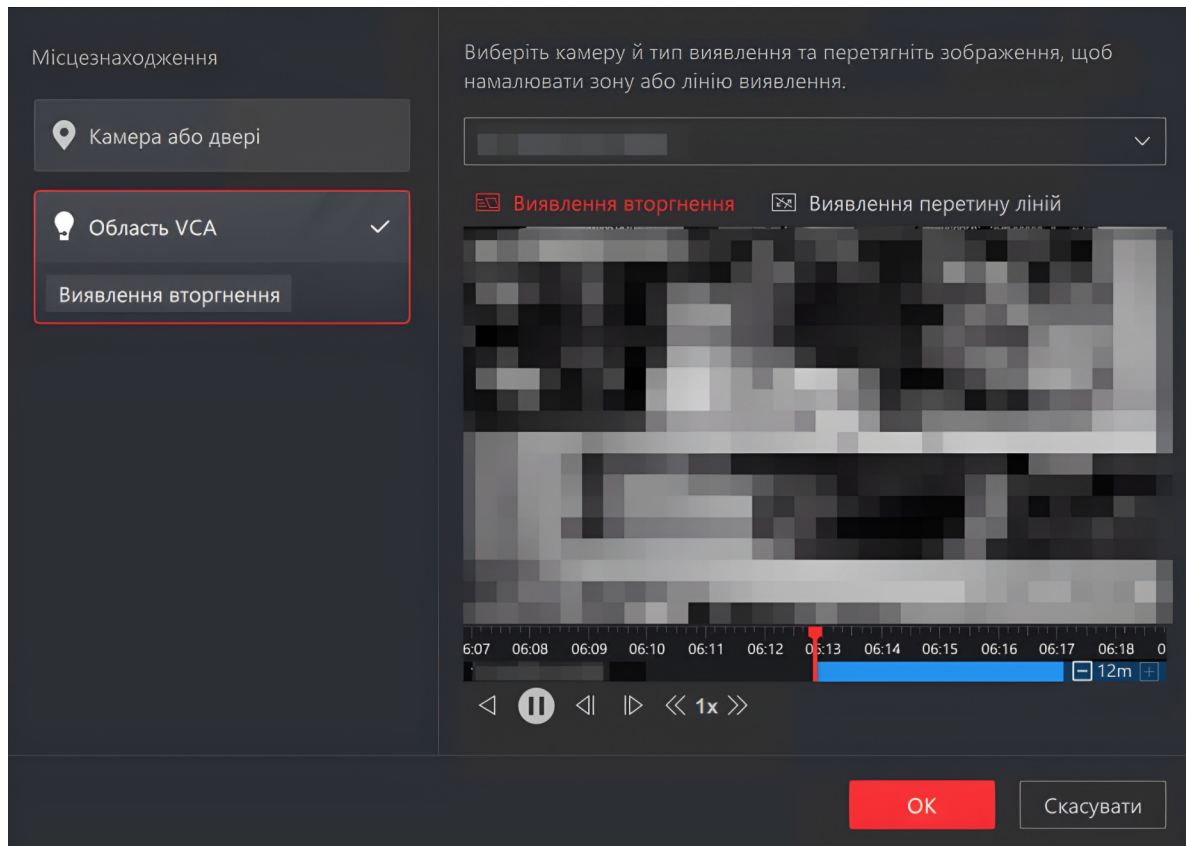


Рисунок 5.4 VCA пошук

5.5 Життєвий цикл зберігання даних

З метою оптимізації потужності сервера адміністраторам рекомендується налаштувати автоматичні графіки видалення архівних записів. Після досягнення встановленого терміну зберігання система остаточно видалить відповідні відеозаписи, журнали контролю доступу та загальні системні дані.

Етапи налаштування:

1. Перейдіть до розділу **Зберігання** → **Період зберігання даних**.
2. Вкажіть бажаний термін зберігання для кожної відповідної категорії даних

5.6 Розширене управління сховищем даних

У цьому розділі описано спеціалізовані адміністративні інструменти, призначені для налаштування мережевих інтерфейсів, усунення аномалій у базах даних та моніторингу загального стану системи.

5.6.1 Завдання щодо мережевого інтерфейсного контролера (NIC)

Для забезпечення оптимального потоку даних служба системного сховища може бути прив'язана до виділеного мережевого адаптера. Адміністратори мають можливість призначити окремий мережевий адаптер виключно для системного сховища або використовувати один мережевий адаптер спільно з центральною службою SYS. Під час розгортання в мережі WAN служби сховища та SYS можуть використовувати одну й ту саму IP-адресу або працювати з різними IP-адресами.

5.6.2 Відновити індекс

У разі пошкодження бази даних, виникнення виняткових ситуацій із зберіганням даних або зниження швидкості реагування під час пошуку настійно рекомендується виконати перебудову системного індексу для відновлення оптимальної продуктивності запитів.

- **Важливе попередження:** Будь ласка, переконайтеся, що система не вимкнена і залишається повністю працездатною протягом усієї процедури, щоб уникнути подальших збоїв.

Етапи налаштування:

1. Перейдіть до **Системне сховище** → **Переглянути місце зберігання**.
2. Виберіть **Відновити індекс**.

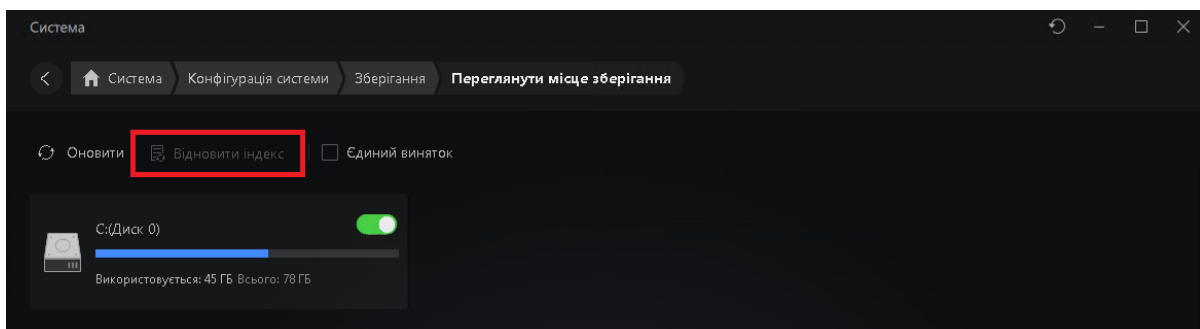


Рисунок 5.5 Відновити індекс

5.6.3 Обслуговування

Viasecurity Control Center забезпечує комплексний діагностичний контроль інфраструктури зберігання даних. За допомогою інтерфейсу «Звіт про технічне обслуговування» адміністратори можуть переглядати статистичні дані в режимі реального часу щодо пропускну здатності мережевої карти сервера запису, стану фізичних дисків, активних шляхів до сховища та загального стану відеоархіву.

(Примітка: щоб ознайомитися з детальними можливостями формування звітів, перегляньте [11.1 Створення та відображення звіту про технічне обслуговування](#).)

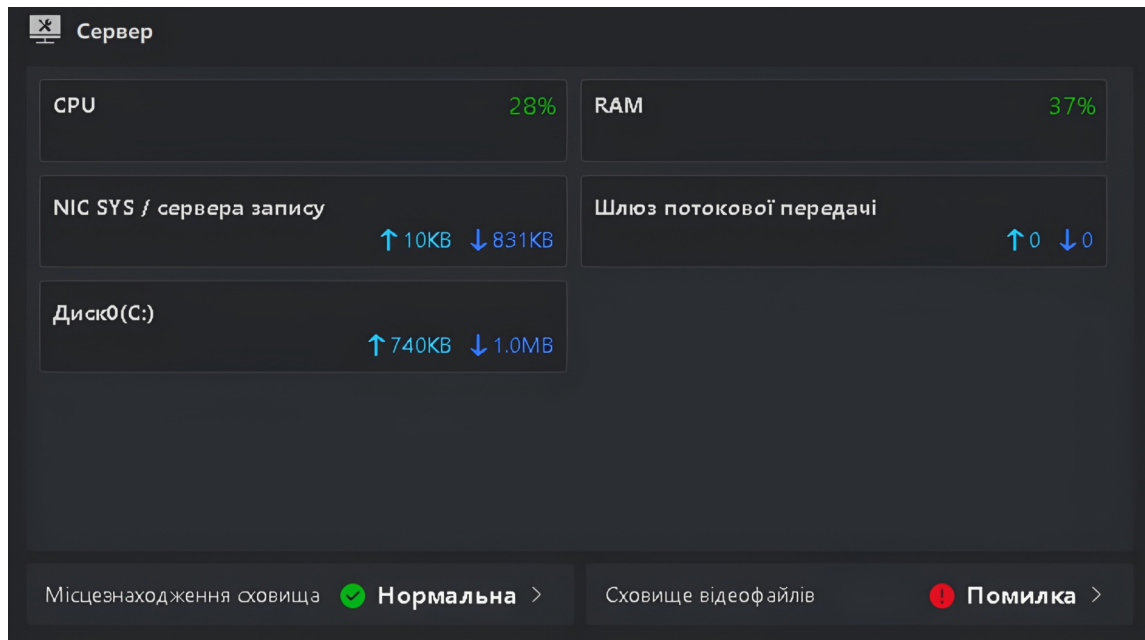


Рисунок 5.6 Статистика сервера

Розділ 6 Інтерфейс моніторингу Viasecurity Control Center

У цьому розділі наведено вичерпний огляд головної панелі моніторингу та керування, де детально описано, як орієнтуватися в інтерфейсі, керувати компонуванням відеокадрів та використовувати аналітику в режимі реального часу.

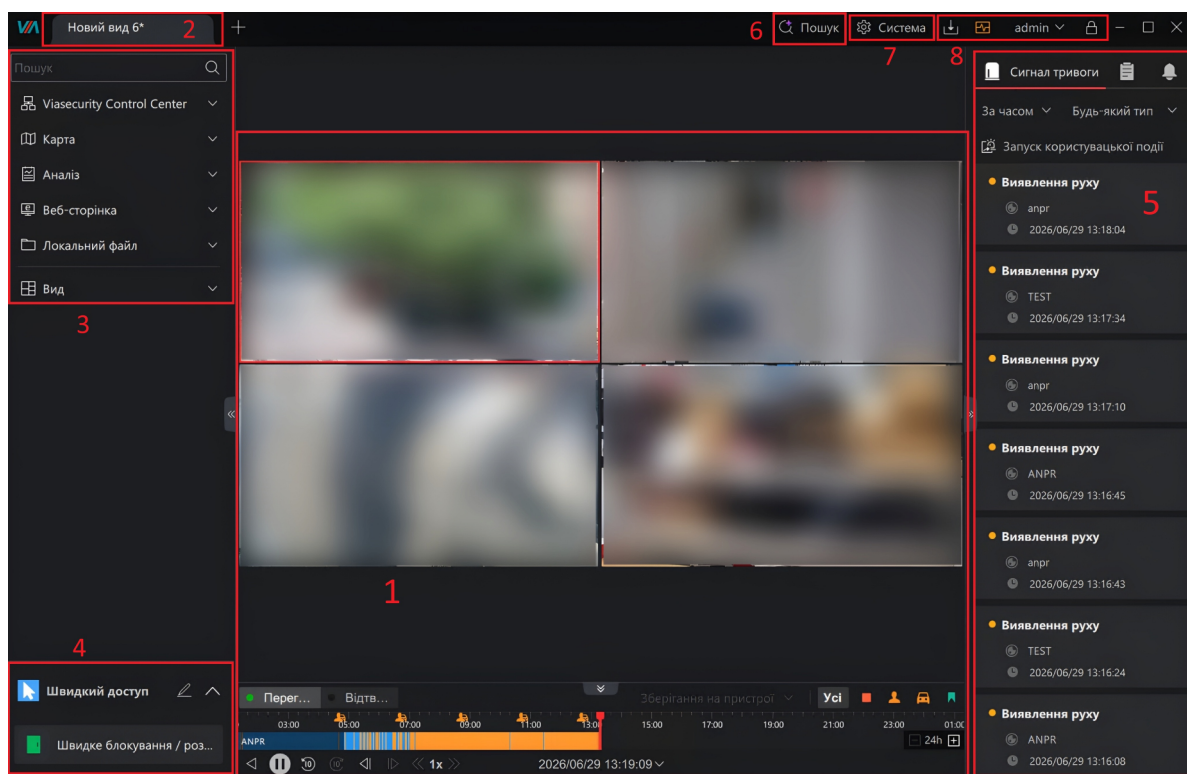


Рисунок 6.1 Головна панель моніторингу та управління

Таблиця 6.1 Огляд головної панелі

№	Функція
1	Сітка перегляду — це центральна робоча область для відображення відео в реальному часі, карт, локальних медіафайлів, веб-сторінок та статистичних звітів. Заповнення сітки Перетягуйте ресурси безпосередньо з вашого локального ПК або з браузера ресурсів у комірки сітки. Локальні медіафайли включають записані відео та зроблені знімки. Управління вікнами Змінюйте розташування робочої області, перетягуючи вікна вгору або вниз. Щоб від'єднати вікно перегляду, клацніть на ньому правою

	кнопкою миші та виберіть Відкрити в новому виді. Контекстне меню сітки Клацніть правою кнопкою миші на будь-якій порожній ділянці сітки, щоб отримати доступ до розширених елементів керування відображенням: - Управління макетом: збережіть поточний макет як нове вікно перегляду, очистіть усі активні вікна або розгорніть поточне вибране зображення на весь екран. Налаштування потоку: застосуйте загальні налаштування потоку до всієї сітки. - Масштаб вікна: Визначте, як відео вписується в комірку. Виберіть Повноекранний екран, щоб розтягнути зображення так, щоб воно заповнило вікно, або Оригінальна роздільна здатність, щоб зберегти справжній розмір відео (що може призвести до появи чорних рамок, якщо розмір не відповідає розмірам вікна). - Режим декодування: Оптимізуйте продуктивність відтворення. Виберіть Апаратне декодування, щоб використовувати графічний процесор (GPU) вашої системи, або Програмне декодування, щоб використовувати центральний процесор (CPU), залежно від апаратних можливостей вашої робочої станції.
2	Перетягніть вікно вгору або вниз, або клацніть правою кнопкою миші на вікні та виберіть пункт Відкрити в новому вікні, щоб відкрити поточне вікно в новому вікні.
3	Цей каталог, розташований на лівій панелі, упорядковує ієрархію вашої системи, включаючи камери, зони, веб-сторінки та збережені види. Навігація Двічі клацніть на будь-якому ресурсі, щоб миттєво відобразити його в сітці перегляду. Управління Клацніть правою кнопкою миші в межах каталогу, щоб додати нові ресурси, карти або групи видів. Швидке фільтрування

	Щоб виділити конкретне обладнання, клацніть правою кнопкою миші на зоні та виберіть Перейти до керування пристроями . Це автоматично відфільтрує список пристроїв, щоб показати лише обладнання, призначене для цієї локації.
4	Налаштуйте швидкий доступ для максимальної ефективності. • Натисніть на іконку головного меню зліва внизу  , щоб відкрити всі модулі клієнта. • Натисніть на іконку додавання  поруч із часто використовуваними модулями, щоб закріпити їх на панелі Швидкого доступу. • Перетягніть закріплені іконки швидкого доступу, щоб змінити їхній порядок.
5	Права панель забезпечує миттєвий огляд активності системи, автоматичне відстеження та активні тривоги. Вкладка Сигнал тривоги Відстежує до 100 тривог у режимі реального часу. Ви можете сортувати список за пріоритетом або часом виникнення, а також фільтрувати за типом події. Наведіть курсор на тривогу, щоб переглянути детальну інформацію, або перетягніть її в сітку перегляду, щоб відтворити відповідне відео. Клацніть правою кнопкою миші на тривозі, щоб підтвердити її, експортувати дані або налаштувати параметри. Використовуйте кнопку Налаштувати, щоб створити нові правила тривог. Вкладка Події Відображає налаштовані системні події для «поточного перегляду» або «усіх ресурсів». Як і у випадку з тривогами, ви можете навести курсор для перегляду деталей або перетягнути для відтворення відео. Опції правого кліка залежать від конкретного типу події. Вкладка Повідомлення Реєструє загальні статуси роботи системи та програмні повідомлення. VCA / Смарт-пошук Відображає результати аналізу відеоконтенту. Фільтруйте результати за часом і клацайте на будь-якій мініатюрі, щоб переглянути конкретний момент у відео.

	Пошук об'єктів / TargetTrace Відстежує конкретні об'єкти в мережі. Фільтруйте за часом та відсотком схожості, щоб зіставити виявлені об'єкти із зображеннями з бази даних.
6	Спеціалізований портал для пошуку історичних даних, таких як минулі сигнали тривоги, журнали доступу осіб та записи про проїзд транспортних засобів.
7	Центральна платформа для адміністрування програмного забезпечення. У цьому розділі можна додавати пристрої, керувати рівнями доступу користувачів, створювати бібліотеки фотографій облич та налаштовувати загальні параметри безпеки.
8	 : Увійти до Центру завантажень.  : Переглянути показники продуктивності ПК, на якому встановлено клієнт.  : Переглянути інформацію про користувача, що увійшов у систему, керувати ліцензіями, створювати резервні копії даних, змінювати пароль тощо.  : Заблокувати клієнт.

Розділ 7 Пошук

Viasecurity Control Center оснащений комплексним модулем розслідувань, призначеним для пошуку широкого спектру системних записів та подій. Перейшовши у верхню частину інтерфейсу робочого столу та натиснувши **Пошук**, адміністратори можуть легко знайти важливі дані, зокрема сигнали тривоги, журнали контролю доступу, записи ANPR (автоматичного розпізнавання номерних знаків), знімки облич та тіл людей, системні сповіщення та журнали роботи. Крім того, платформа має розширені можливості «розумного запиту», що дозволяють точно зіставляти відеопотоки з конкретними параметрами щодо осіб, транспортних засобів та аналізу відеоконтенту (VCA).

7.1 Пошук транспортних засобів або осіб, виявлених камерами/дверима

Цей модуль полегшує пошук відеоархівів та даних про події, пов'язаних із конкретними кінцевими пристроями системи, такими як камери або двері з системою контролю доступу.

Камери

Отримуйте доступ до стандартних відеозаписів, журналів руху транспортних засобів, зроблених знімків обличчя та метаданих, що генеруються під час відтворення або через тригери сигналізації.

Двері

Отримати синхронізовані відеопотоки, матеріали з функцією розпізнавання облич та вичерпні записи про аутентифікацію за допомогою облікових даних та карток.

Пошук транспортних засобів за камерами

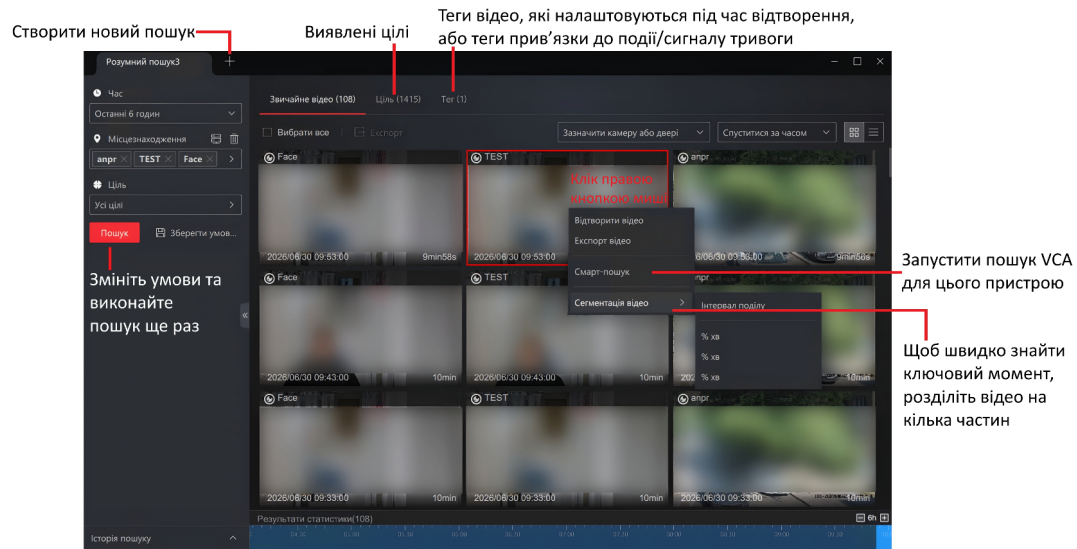


Рисунок 7.1 Результати пошуку відео

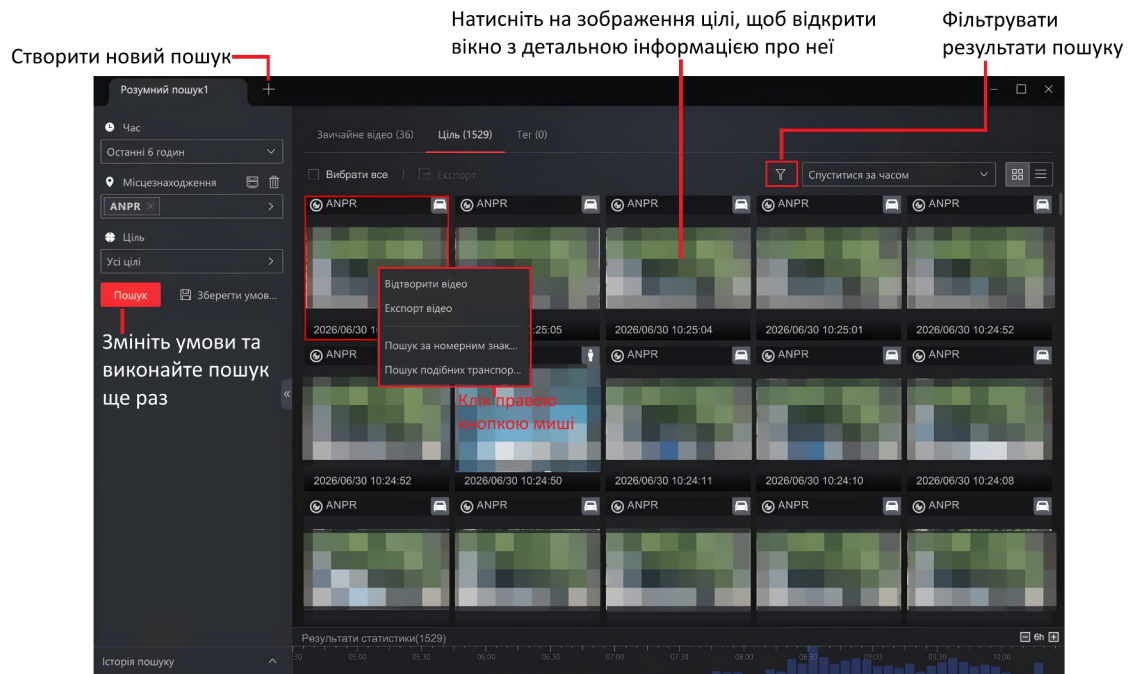


Рисунок 7.2 Результати пошуку транспортних засобів

Пошук осіб за допомогою камер

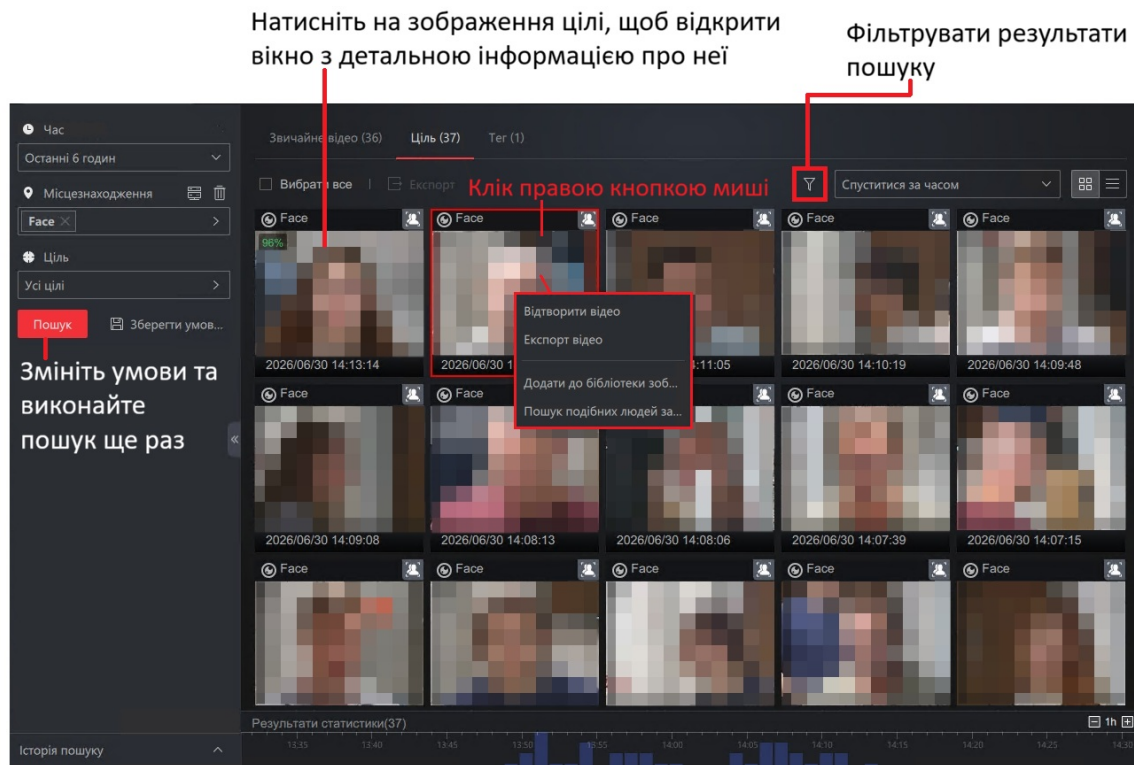


Рисунок 7.3 Пошук осіб за допомогою камер

Аналіз результатів

Щоб переглянути конкретний запис, двічі клацніть або клацніть правою кнопкою миші на файлі, щоб відкрити інтерфейс відтворення. Оператори можуть регулювати швидкість відтворення або перейти безпосередньо на сторінку з детальною інформацією про ресурс для подальшого аналізу.

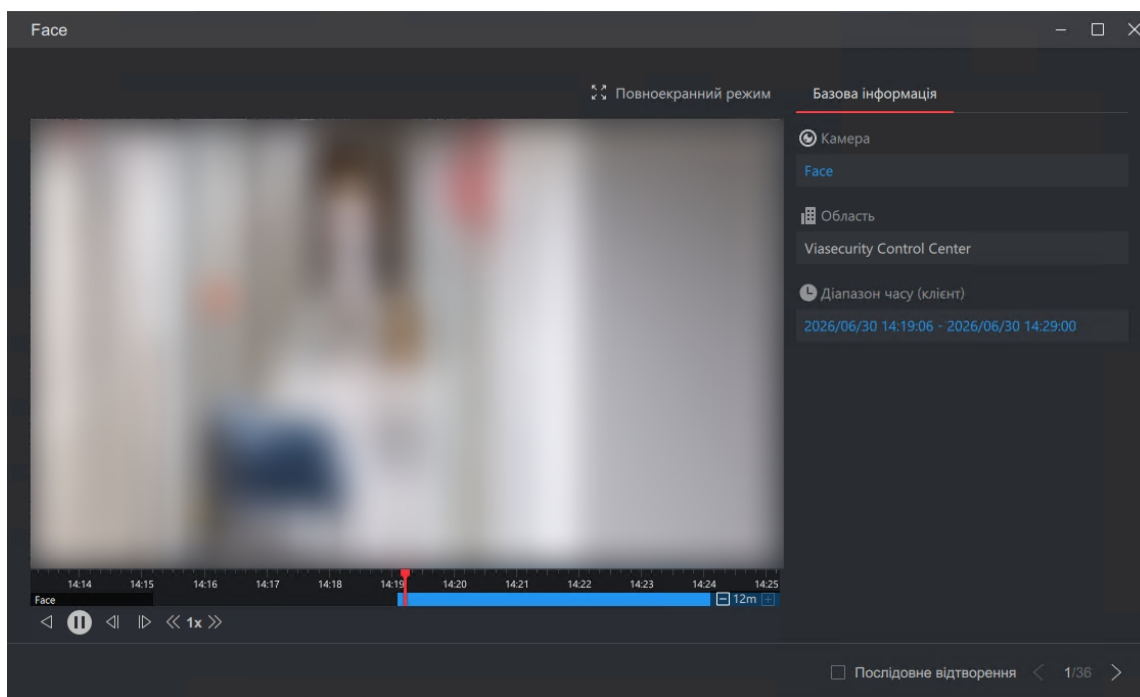


Рисунок 7.4 Відтворення відео

7.2 Пошук виявлених осіб або транспортних засобів у зонах VCA

Використовуйте цю функцію для виділення об'єктів (осіб або транспортних засобів), які викликали спрацювання певних правил аналізу відеоконтенту (VCA). Система спеціально фільтрує події **Виявлення вторгнення** та **Виявлення перетину лінії**.

(Примітка: Перед початком пошуку переконайтеся, що функції VCA увімкнені на відповідному обладнанні.)

Етапи налаштувань:

1. Перейдіть до інтерфейсу **Розумний пошук** і вкажіть часовий діапазон розслідування.
2. Встановіть для параметра **Місцезнаходження** значення **Області VCA**.
3. Вкажіть цільову **камеру** для запиту.
4. Виберіть потрібний режим роботи (**Виявлення вторгнення** або **Виявлення перетину лінії**) та інтерактивно накресліть зону або лінію виявлення безпосередньо на екрані попереднього перегляду відео.
5. Виконайте команду **Пошук**.

Теги на відео, які налаштовуються під час відтворення, або теги прив'язки до події/сигналу тривоги.

Підтримується перехід на сторінку з інформацією про поточну камеру.

Клік правою кнопкою миші

Відтворити відео
Експорт відео
Смарт-пошук
Сегментація відео >

Змініть умови та виконайте пошук ще раз.

Клацніть на стовпці, щоб переглянути результати пошуку за вибраним часовим діапазоном. Під час перегляду детальної інформації про один із результатів пошуку ви можете перемкнути стовпець, щоб переглянути результати пошуку за іншим часовим діапазоном.

Рисунок 7.5 VCA пошук

Розділ 8 Управління подіями та сигналами тривоги

Модуль **Управління подіями та тривогами** слугує централізованим інтерфейсом для адміністрування системних тригерів, моніторингу сповіщень у режимі реального часу та експорту даних для аналізу. У цьому розділі оператори можуть визначати складні протоколи тривоги, керувати підписками на події та переглядати журнали інцидентів.

Доступ до цих налаштувань можна отримати через: **Система → Події та сигнал тривоги**.

8.1 Підтримувані події, що запускають дію

Щоб визначити конкретні тригери, доступні для налаштування сповіщень, виконайте такі дії:

1. Перейдіть до розділу **Конфігурація сигналу тривоги** та виберіть **Додати сигнал тривоги**.
2. Скористайтесь випадаючим меню **Подія-активатор**, щоб переглянути повний перелік сумісних системних сигналів.

Сигнал тривоги системи відеонагляду

Таблиця 8.1 Відео

Категорія	Конкретна подія
Основні й інтелектуальні події	Виявлення руху
	Вторгнення в область
	Перетин лінії
	Швидкий рух
	Видалення об'єкта
	Об'єкт викинуто з будівлі
	Вхід до області
	Вихід з області
	Сигнал тривоги щодо входу людей з іншого напрямку
	Залишений багаж

ANPR	Подія щодо збігу ТЗ
	Подія щодо відсутності збігу ТЗ
	Подія збігу типу транспортного засобу
	Відсутній номерний знак
Подія, пов'язана з людьми	Подія щодо збігу обличчя
	Подія щодо відсутності збігу обличчя
	Багатоцільове визначення
	Особа, що часто з'являється
	Байдикування
	Виявлення обличчя
	Захоплення обличчя
	Виявлення черги людей
	Визначення часу очікування
	Скупчення людей
	Щільність людей
Вхід сигналу тривоги	Введення сигналу тривоги запущено

Сигнал тривоги системи контролю доступу

Таблиця 8.2 Двері

Категорія	Конкретна подія
Доступ надано	Доступ надано за допомогою картки та відбитка пальця
	Доступ надано за допомогою картки, відбитка пальця та PIN-коду
	Доступ надано за допомогою картки та PIN-коду
	Доступ надано за допомогою дійсної картки
	Доступ надано за відбитком пальця
	Доступ надано за відбитком пальця та PIN-кодом
	Сигнал тривоги

	Доступ надано за допомогою розпізнавання обличчя та відбитка пальця
	Доступ надано за обличчям та PIN-кодом
	Доступ надано за обличчям та картою
	Доступ надано за обличчям, PIN-кодом та відбитком пальця
	Доступ надано за допомогою розпізнавання обличчя, картки та відбитка пальця
	Доступ надано за допомогою розпізнавання обличчя
	Доступ надано за ідентифікаційним номером співробітника та відбитком пальця
	Доступ надано за ідентифікаційним номером співробітника, відбитком пальця та PIN-кодом
	Доступ надано за ідентифікаційним номером співробітника та обличчям
	Доступ надано за ідентифікаційним номером співробітника та PIN-кодом
	Доступ надано за допомогою комбінованих режимів аутентифікації
	Доступ надано за PIN-кодом
У доступі відмовлено	Помилка перевірки шифрування картки
	Макс. кількість невдалих спроб доступу за картою
	Строк дії № картки скінчився
	Вийшов час очікування для аутентифікації за допомогою картки та PIN-коду
	У доступі відмовлено (двері залишились замкненими або неактивними)
	У доступі відмовлено: Першу особу не авторизовано

	У доступі за картою та PIN-кодом відмовлено
	Вийшов час очікування аутентифікації за допомогою картки + відбитка пальця + PIN-коду
	У доступі за допомогою картки, відбитка пальця та PIN-коду відмовлено
	У доступі за допомогою картки та відбитка пальця відмовлено
	Вийшов час очікування аутентифікації за допомогою картки + відбитка пальця
	Не призначено рівень доступу
	Номер картки не існує
	Недопустимий період часу
	Відбиток пальця не існує
	У доступі за відбитком пальця відмовлено
	У доступі за відбитком пальця та PIN-кодом відмовлено
	Вийшов час очікування для аутентифікації за відбитком пальця + PIN-кодом
	У доступі за обличчям та відбитком пальця відмовлено
	Вийшов час очікування аутентифікації за допомогою обличчя та відбитка пальця
	У доступі за обличчям та PIN-кодом відмовлено
	Вийшов час очікування аутентифікації за допомогою обличчя та PIN-коду
	У доступі за обличчям та картою відмовлено
	Вийшов час очікування аутентифікації за обличчям та картою
	У доступі за обличчям, PIN-кодом та відбитком пальця відмовлено

	Вийшов час очікування аутентифікації за допомогою обличчя + PIN-коду + відбитка пальця
	У доступі за обличчям, картою та відбитком пальця відмовлено
	Вийшов час очікування аутентифікації за допомогою обличчя + картки + відбитка пальця
	У доступі за обличчям відмовлено
	Не вдалось захопити обличчя
	Двері для блокування не зачинено
	У доступі за посвідченням співробітника та відбитком пальця відмовлено
	Вийшов час очікування аутентифікації за посвідченням співробітника + відбитком пальця
	У доступі за посвідченням співробітника, відбитком пальця та PIN-кодом відмовлено
	Вийшов час очікування аутентифікації за посвідченням співробітника + відбитком пальця + PIN-кодом
	У доступі за посвідченням співробітника та обличчям відмовлено
	Вийшов час очікування аутентифікації за посвідченням співробітника та обличчям
	У доступі за посвідченням співробітника та PIN-кодом відмовлено
	Вийшов час очікування автентифікації за посвідченням співробітника + PIN-кодом
	Особа не належить до групи з багатофакторною автентифікацією
	Особа поза часовим періодом багатофакторної автентифікації

	Таймаут комбінованої аутентифікації
	У доступі за недійсною картою M1 відмовлено
	Помилка перевірки шифрування картки CPU
	У доступі відмовлено (вимкнено зчитування картки NFC)
	Зчитування картки EM не ввімкнено
	Зчитування картки M1 не ввімкнено
	Зчитування картки CPU вимкнено
	Невідповідність режиму аутентифікації
	Втрачену картку автентифіковано
	Перевищено обмеження спроб аутентифікації за картою + PIN-кодом
	Паролі не збігаються
	Посвідчення співробітника не існує
	Сигнал тривоги після невдалих спроб введення паролю
	Помилка перевірки шифрування картки DESFire
	Зчитування картки DESFire вимкнено
	Помилка аутентифікації через аномальні характеристики
	Помилка виявлення підробки райдужної оболонки ока
Інші події дверей	Двері розблоковано (дверний замок)
	Двері заблоковано (дверний замок)
	Кнопка виходу натиснена
	Кнопка виходу відпущена
	Сигнал тривоги втручання в зчитувач карток
	Двері відчинено з помилками (контакт дверей)

	Дистанційно: відімкнені двері
	Дистанційно: замкнені двері
	Продзвенів дверний дзвінок
	Дистанційно: залишено відімкненими (вільний доступ)
	Дистанційно: залишено замкненими (помилка авторизації)
	Початок стану "Вільний прохід"
	Завершення стану "Вільний прохід"
	Початок стану "Доступ заборонено"
	Закінчення стану "Доступ заборонено"
	Вхід першої особи запущено
	Вхід для першої особи було зупинено
	Авторизацію першої особи розпочато
	Авторизацію першої особи зупинено
	Двері відчинено (контакт дверей)
	Двері зачинено (контакт дверей)
	Таймаут розблокування
	Термінал розпізнавання обличчя в мережі
	Термінал розпізнавання обличчя не в мережі
	Проходження впритул
	Проходження у зворотному напрямку
	Примусовий доступ
	Перелазіння через шлагбаум
	Таймаут проходження

	Сигнал тривоги про вторгнення
	Помилка доступу під час вільного проходження
	Шлагбаум заблоковано
	Роботу шлагбаума відновлено
	Багаторазова автентифікація: у доступі за супер-паролем відмовлено
	Багаторазова автентифікація: доступ відхилено через віддалену автентифікацію
	Багаторазова автентифікація: доступ надано
	Багаторазова автентифікація: Дистанційне відчинення дверей
	Багаторазова автентифікація: доступ надано за супер-паролем
	Багаторазова автентифікація: повторна автентифікація
	Таймаут багатофакторної автентифікації
	Пошкодження зчитувача карток усунено
	Сигнал тривоги зламу блока керування захищеними дверима відновлено
	Ввести код анулювання
	Реле сигналу тривоги пожежі залишає двері відкритими
	Реле сигналу тривоги пожежі відновлене і двері відновлені
	Подія у списку блокування
	Не вдалося відкрити двері кнопкою виходу у режимі "двері залишаються зачиненими" або у режимі сну
	Не вдалося відкрити двері через з'єднання в режимі "двері залишаються зачиненими" або у режимі сну

	Надмірна затримка
	Розблокування центром
	Двері не відчинені
	Двері не зачинені
	Блок керування захищеними дверима відключено
	Блок керування захищеними дверима підключено
	Виявлення руху

Таблиця 8.3 Пристрій контролю доступу

Категорія	Конкретна подія
Безпека пристрою	Сигнал тривоги пошкодження блока керування відеодомофона захищених дверей
	Пристрій пошкоджений
	Сигнал тривоги про пошкодження контролера смуги руху
	Сигнал пошкодження пристрою відновлено
Локальна операція на пристрої	Локально: вхід заблоковано
	Локальний: вхід розблоковано
	Локальний: Увійти
	Локально: Вийти
	Локально: Оновити
	Автоматична синхронізація часу по NTP
	Локальний: Відновлено стандартні налаштування
	Редагувати конфігурацію мережевого центру
	Змінити параметри GPRS
	Редагування конфігурації центральної групи
	Імпортувати звичайний файл конфігурації
	Експортувати звичайний файл конфігурації
	Імпортувати параметри дозволу картки

	Експортувати параметри дозволу карт
	Локально: Оновити прошивку пристрою через накопичувач USB
	Локально: Помилка оновлення
Зв'язок між компонентами пристрою	Сигнал тривоги пожежного входу контролера смуги
	Зависока температура основи
	Помилка зв'язку зі світловою панеллю
	Індикатор вимкнено
	Контролер смуги відключений
	Контролер смуги підключено
	Шину CAN відновлено
	Пожежний вхід контролера смуги руху відновлено
	Зв'язок з ІЧ адаптером відновлений
	Активний інфрачервоний детектор вторгнення відновлений
	Модуль розширення офлайн
	Модуль розширення онлайн
Диск / жорсткий диск пристрою	Сигналізація нестачі пам'яті для подій, про які не звітується
	Карта пам'яті заповнена
	Бракує місця в пам'яті для автономного зберігання подій
	Помилка читання/запису з флеш-пам'яті
Акумулятор пристрою	Живлення змінного струму ввімкнено
	Напруга батареї відновлена
	Напругу батареї відновлено
	Увімкнення пристрою
	Вимкнення пристрою
Створення звіту про записи пристрою	Пристрій контролю доступу встановлено в режим охорони
	Увімкнено охорону відеодомофона

Мережа пристрою	Пристрій контролю доступу в мережі
	Пристрій контролю доступу не в мережі
Віддалена операція на платформі	Дистанційно: Увійти
	Дистанційно: Вийти
	Дистанційно: Взяття на охорону
	Дистанційно: Вимикання охорони
	Дистанційно: Перезапустити
	Дистанційно: Оновити
	Дистанційно: Експортувати файл конфігурації
	Дистанційно: Імпортувати файл конфігурації
	Вихід сигналу тривоги увімкнений
	Вихід сигналу тривоги вимкнено
	Дистанційно: Синхронізація часу вручну
	Дистанційно: Очистити № картки
	Дистанційно: Відновлені стандартні параметри
	Дистанційно: Зйомка
	Дистанційно: Помилка оновлення
	Дистанційно: Модуль розширення оновлено
	Дистанційне керування: Помилка оновлення модуля розширення
	Дистанційно: Модуль відбитків пальців оновлено
	Дистанційно: Помилка оновлення модуля відбитків пальців
	SOS

Таблиця 8.4 Вхід сигналу тривоги

Конкретна подія	Опис
Введення сигналу тривоги запущено	Відбувається, коли на вході сигналу тривоги пристрою виявлено ненормальний сигнал (наприклад, концентрація, виміряна датчиком диму, перевищує поріг), що активує сигнал тривоги. Ця подія вказує на

	початок стану тривоги.
Тривожний вхід відновлено	Відбувається, коли аномальний сигнал припиняється, і стан тривоги повертається до нормального. Ця подія означає закінчення стану тривоги.

Таблиця 8.5 Особа

Конкретна подія
Подія збігу особи
Подія збігу номеру картки

Сигнали тривог про технічне обслуговування
Таблиця 8.6 Служба

Категорія	Конкретна подія
Сервер потокової передачі	Сервер потокової передачі не в мережі
Сервер зберігання даних	Вийняток сховища
Служба керування системою	Помилка центрального процесора
	Попередження щодо центрального процесора
	Помилка оперативної пам'яті
	Попередження щодо оперативної пам'яті
	Системну службу зупинено з помилками

Таблиця 8.7 Технічне обслуговування пристрою контролю доступу

Конкретна подія
Пристрій пошкоджений
Сигнал тривоги про втручання в контролер смуги руху
Сигнал тривоги зламу блока управління захищеними дверима
Пристрій контролю доступу не в мережі
Відеодомофон не в мережі
Вимкнення живлення змінного струму
Пристрій вимкнено

Низька напруга батареї
Напруга батареї відновлена
Низька напруга батареї сховища
Не вдалося встановити пристрій на охорону
Не вдалось встановити відеодомофон у режим охорони
Картка пам'яті заповнена
Помилка читання /запису флеш-пам'яті
Помилка мотора або датчика
Помилка шини CAN
Помилка активного інфрачервоного детектора вторгнення
Помилка зв'язку з ІЧ адаптером
Індикатор увімкнено
Контролер смуги руху відключено
Контролер смуги руху підключено
Модуль розширення офлайн
Кол-центр (пристрій контролю доступу)
Кол-центр (відеодомофон)

Таблиця 8.8 Камера

Конкретна подія
Камера в мережі
Камера не в мережі
Канал установлено в режим охорони
Не вдалось встановити канал у режим охорони
Виявлення розфокусування
Втрата відео
Виняток під час запису камери
Відновлення запису з камери
Подія винятку зображення
Виявлення втручання у відео

Виявлення зміни сцени
Сигнал тривоги про виявлення вібрації
Виявлення виняткових ситуацій в аудіо
Виняток транскодування відеопотоку

Таблиця 8.9 Пристрій кодування

Конкретна подія
Виявлено зв'єднання з пристроєм
Пристрій не в мережі
Жорсткий диск заповнений
Перегрівання жорсткого диска
Удар по жорсткому диску
Серйозна несправність жорсткого диска
Збій жорсткого диска під час читання/запису
Помилка масиву
Несанкціонований вхід
Пристрій увімкнено
Не вдалось встановити пристрій на охорону

Сигнали тривоги для користувацьких подій
Таблиця 8.10 Настроювана подія

Категорія	Конкретна подія
Користувацька подія	Подія, визначена користувачем
Звичайна подія	Загальна подія

8.2 Підписка на події

У Viasecurity Control Center підписка на події гарантує, що вони активно реєструються, їх можна шукати в системі, а також вони відображаються на головній панелі моніторингу.

Основні аспекти, на які слід звернути увагу:

- Ви й надалі отримуватимете сповіщення про спрацювання тривоги, навіть якщо ви не підписані на відповідну подію.
- Якщо підписка на подію скасована, вона не з'являтиметься в модулі «Пошук» і не відображатиметься на головній панелі моніторингу.

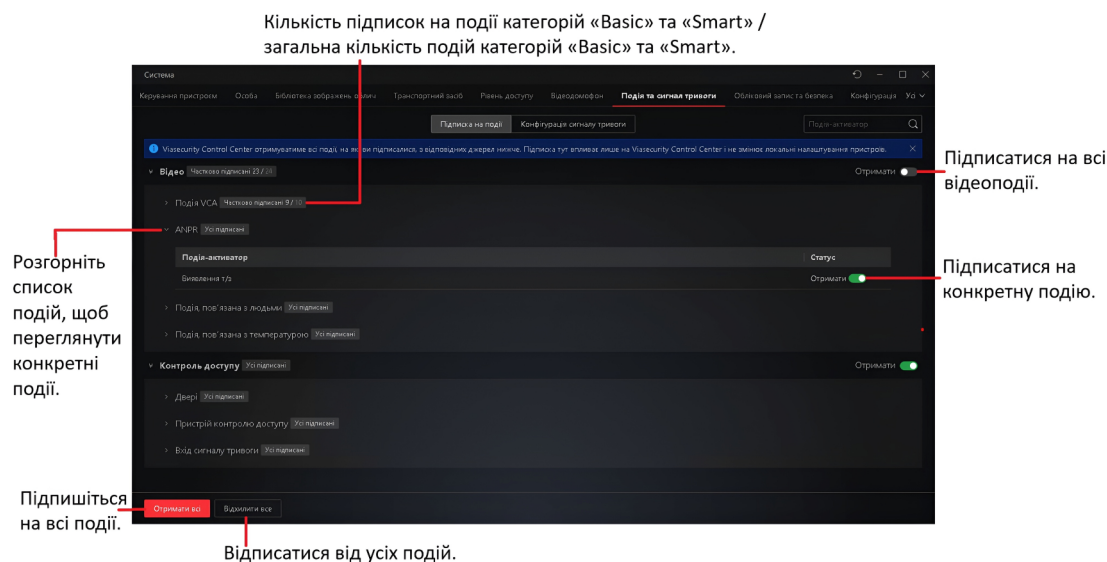


Рисунок 8.1 Підписка на події

Управління підписками:

- **Цільовий вибір:** Розгорніть категорії подій, щоб вручну увімкнути або вимкнути підписку на конкретні події.
- **Вибір категорії:** Ви можете підписатися на цілі групи подій одночасно (наприклад, увімкнути всі події, пов'язані з відео).

8.3 Додавання сигналу тривоги

Ця платформа дозволяє створювати індивідуальні правила сповіщення, пов'язуючи конкретні виявлення системи з автоматичними реакціями та сповіщеннями.

Етапи налаштування:

1. Перейдіть до модуля **Події та сигнал тривоги**.
2. Перейдіть до розділу **Конфігурація сигналу тривоги** та натисніть кнопку **Додати сигнал тривоги**.
3. Виберіть потрібну подію, що викликає тривогу, та вкажіть конкретні апаратні джерела, які будуть її відстежувати.
4. Призначте рівень пріоритету тривоги, а потім натисніть **Далі**.

5. Визначте розклад активного прийому для цієї тривоги, а потім натисніть **Далі**.
(Примітка: якщо потрібно врахувати вихідні/святкові дні, налаштуйте їх у розділі «Вихідний»).
6. Виберіть систему для користувачів або груп, які повинні отримувати це сповіщення про тривогу, а потім натисніть **Далі**.
7. Призначте автоматичні системні реакції (наприклад, початок запису, зняття знімка, спливаюче вікно), які будуть виконуватися при спрацьовуванні тривоги.
8. Натисніть **Готово**, щоб зберегти та активувати правило тривоги.

8.4 Підтримувані дії взаємодії

Платформа Viasecurity Control Center дозволяє налаштовувати автоматичні реакції системи, відомі як «пов'язані дії», які виконуються негайно після спрацьовування певної тривоги.

(Примітка: Якщо ви застосовуєте візуальні дії (запис, зняття знімка або створення мітки) до дверей системи контролю доступу, до цих дверей має бути підключена камера. Якщо камера не підключена, система дозволить налаштування, але дія не буде виконана.)

Посилання на відео та зображення

Запис за пусковою подією

Накажіть камерам записати подію тривоги. Ви можете використати **Камеру-джерело** (камеру, яка виявила подію) та визначити місце її збереження (Основне сховище, Додаткове сховище або Не зберігати), або вибрати **Зазначену камеру** для запису з додаткових ракурсів.

- Запис починається за 3 секунди до події та закінчується через 15 секунд після неї.
- Файли зберігаються щонайменше 7 днів, після чого підлягають стандартному циклу перезапису пристрою.

Захоплення зображення

Дає команду камері-джерелу або вручну вказаним камерам зробити один знімок під час події. З кожної камери знімається лише одне зображення.

Створення мітки

Додає закладки з можливістю пошуку до відеозаписів тривоги.

- Для використання цієї функції необхідно увімкнути опцію «Запуск запису».

- Теги застосовуються до 3-секундного періоду до спрацювання тривоги та 15-секундного періоду після спрацювання тривоги. Ви можете ввести власний текст або використати системні змінні (\$Назва події, \$Час події або \$джерело події).

Активувати PTZ-камеру

Система вибрала камери PTZ для миттєвого переходу до певної попередньо заданої позиції, маршруту патрулювання або схеми руху.

Зв'язок між апаратним забезпеченням та системою контролю доступу

Поєднати точку контролю доступу

Автоматично змінювати фізичний стан вибраних дверей (наприклад, «Заблокувати», «Розблокувати», «Залишити заблокованими» або «Залишити розблокованими») для забезпечення безпеки зони під час спрацювання сигналізації.

Поєднати тривожний вихід

Увімкніть підключені фізичні периферійні пристрої, такі як зовнішні сигнальні гучномовці.

(Примітка: ці пристрої виводу потрібно спочатку імпортувати в систему, перш ніж їх можна буде вибрати тут.)

Взаємодія між системою та повідомленнями оператора

Активувати спливаюче вікно

Негайно відображає на екрані оператора інтерфейс, у якому показуються деталі критичної тривоги разом із потоковим відео та опціями миттєвого відтворення.

Активувати звуковий сигнал тривоги

Відтворює синтезоване голосове сповіщення з ПК оператора, щоб привернути його увагу. *Необхідна умова: аудіосистема повинна бути увімкнена, а голосовий модуль має бути призначений як звук сигналізації.*

Надіслати електронний лист

Надсилає автоматичне сповіщення електронною поштою із детальною інформацією про подію вказаним одержувачам.

Запуск користувацької події

Перш ніж додати цю дію зв'язку, слід спочатку налаштувати тривоги для подій, визначених користувачем. Оскільки події, визначені користувачем, не можна виявити автоматично, їх потрібно запускати вручну, натиснувши **Запуск користувацької події** на панелі сповіщень головної сторінки або додати як дію зв'язку для іншої тривоги.

8.5 Управління налаштованими сигналами тривоги

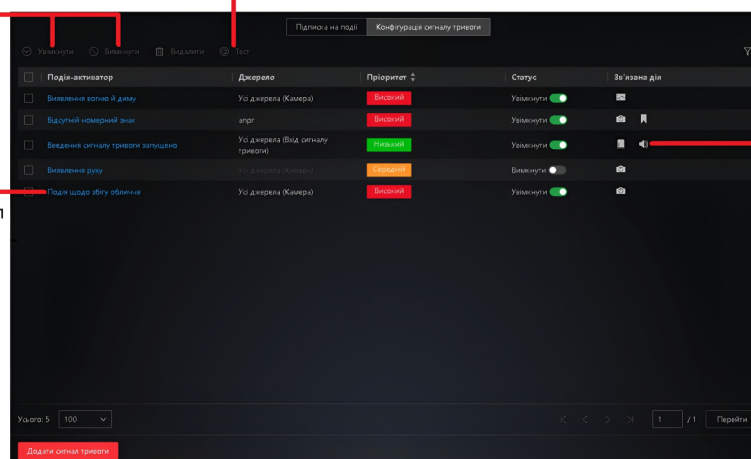
Після створення правила сповіщень активуються автоматично. Ви можете керувати налаштованими сповіщеннями безпосередньо з головного списку:

- Вручну вмикайте або вимикайте сповіщення. Вимкнення сповіщення запобігає його спрацьовуванню та зупиняє всі пов'язані з ним дії.
- Клацніть безпосередньо на назві події, щоб змінити її поточні параметри.
- Виберіть конкретні сповіщення та скористайтесь функцією тестового спрацьовування, щоб перевірити свою конфігурацію.

Після налаштування сигналу тривоги він увімкнений за замовчуванням. Ви можете вручну вимкнути сигнал тривоги, щоб він не спрацьовував і відповідні дії не виконувалися.

Виконайте тестове спрацьовування вибраних сигналів тривоги, щоб перевірити, чи правильно вони налаштовані. Сигнал тривоги спрацює та відобразиться у списку спрацьованих сигналів тривоги (**Пошук > Сигнал тривоги**).

Натисніть на назву події, щоб відредагувати сигнал тривоги.



Наведіть курсор на дію зв'язку, щоб переглянути її деталі

Рисунок 8.2 Список налаштованих сигналів тривог

8.6 Моніторинг, пошук та експорт сповіщень

Ознайомитися з повною історією спрацьованих подій можна, перейшовши в розділ **Пошук → Сигнал тривоги**. Цей модуль дозволяє операторам переглядати, керувати та витягувати дані про події.

Деталі події та додавання до закладок

Натисніть на будь-який конкретний сигнал тривоги, щоб переглянути вичерпну інформацію, включаючи джерело спрацьовування, пов'язане відео та операційні записи. Ви також можете вручну позначити критичні сигнали тривоги як важливі для швидкого доступу.

Налаштування списку

Оптимізуйте вигляд списку, налаштувавши його так, щоб найновіші події або тривоги з найвищим пріоритетом завжди відображалися у верхній частині.

Можливості експорту

Оператори можуть експортувати окремий запис про тривогу або виконати пакетний експорт усіх зареєстрованих тривог для зовнішньої звітності.

Спливаючі сповіщення

У спливаючих вікнах у режимі реального часу критичні сповіщення відображаються у хронологічному порядку. Ви можете перемикатися між активними спливаючими вікнами або повністю вимкнути їх для локального клієнта.

Позначте сигнал тривоги як важливий.

Натисніть, щоб переглянути деталі сигналу тривоги (джерело сигналу, пристрій, зона, відео, запис операції тощо).

Експортуйте всі сигнали тривоги.

Експортувати певну тривогу.

Журнал сигналів тривоги й подій

Базова інформація

Час пошуку: 2025/07/01 15:08:21
Хто виконав пошук: admin
Тригери події: Виявлення руху, Відсутній номерний знак, worklet_Подія щодо збігу обличчя
Час: 2025/07/01 00:00:00 - 2025/07/01 23:59:59
Суккупна кількість: 15

Маркування	Тригери події	Джерело	Область	Час	Пріоритет	Категорія	Визначити	Більше
НІ	Виявлення руху	aprr	NVR_01	2025/07/01 15:08:12	Середній	Не підтверджено		
НІ	Відсутній номерний знак	aprr	NVR_01	2025/07/01 15:07:52	Високий	Не підтверджено		
НІ	Виявлення руху	aprr	NVR_01	2025/07/01 15:07:28	Середній	Не підтверджено		
НІ	Виявлення руху	102.168.30.188.8	NVR_01	2025/07/01 15:06:51	Середній	Не підтверджено		
НІ	worklet_Подія щодо збігу обличчя	Face	Viasecurity Control Center	2025/07/01 15:06:50	Високий	Не підтверджено		
НІ	Виявлення руху	EXIT	NVR_01	2025/07/01 15:06:48	Середній	Не підтверджено		
НІ	Виявлення руху	7a26	Viasecurity Control Center	2025/07/01 15:06:45	Середній	Не підтверджено		

Рисунок 8.3 Список спрацьовувань сигналів тривоги

Завжди відображати найновіше сповіщення зверху.

Сповіщення з вищим пріоритетом завжди закріплюються зверху, причому нові повідомлення того ж рівня їх не витісняють.

Пріоритет відображення останнього с...

Пріоритетизувати відображення тривог з...

Визначити

Пріоритет відображення останнього с...

Звук сповіщення сигналу тривоги

Увімкнути/вимкнути всі звукові сигнали, пов'язані з тривогою, для поточного клієнта.

Зніміть прапорець, щоб вимкнути всі спливаючі попередження для цього клієнта (дія збережеться в налаштуваннях).

Перемикання спливаючих сповіщень. Спливаючі сповіщення впорядковані за часом.

Рисунок 8.4 Спливаюче вікно з попередженням

Розділ 9 Доступ до системи та управління обліковими записами

Модуль Облікові записи та безпека надає необхідні інструменти для налаштування облікових даних користувачів, визначення груп дозволів та забезпечення дотримання загальних протоколів автентифікації. Щоб отримати доступ до цих налаштувань та керувати ними, перейдіть до Система → Обліковий запис та безпека.

9.1 Управління користувачами та системними ролями

Розділ «Управління користувачами та системними ролями» містить інструменти, необхідні для управління доступом до платформи та її безпекою. Цей модуль дозволяє адміністраторам створювати та налаштовувати локальні облікові записи користувачів, керувати існуючою базою даних користувачів, а також визначати конкретні набори прав шляхом створення та призначення системних ролей. Ефективно використовуючи ці функції, ви можете забезпечити, щоб кожен користувач мав відповідний рівень повноважень, необхідний для виконання його конкретних робочих завдань.

9.1.1 Додати користувача

Ви можете додавати звичайних користувачів та призначати їм ролі для доступу до системи. Звичайні користувачі — це всі користувачі, крім суперкористувача.

Щоб створити та налаштувати новий профіль:

1. Перейдіть до інтерфейсу створення користувача та введіть необхідні базові облікові дані.
2. Перемкніть статус доступу. Встановлення профілю в стан «Неактивний» ефективно запобігає авторизації цього облікового запису в системі.
3. Присвойте числове значення, щоб визначити ієрархію управління PTZ оператора.
4. Користувачі, яким присвоєно вищий числовий пріоритет, можуть переривати та замінювати активні команди PTZ, ініційовані персоналом нижчого рівня.
5. Під час активної роботи з потоковим зображенням PTZ користувач може заблокувати камеру. Ця дія блокує будь-які команди PTZ від інших операторів, які мають рівний або нижчий рівень пріоритету.
6. Прив'яжіть до нового профілю відповідні попередньо визначені групи дозволів. Щоб перевірити точну систему прав, пов'язаних із конкретною роллю, перед її

призначенням наведіть курсор на назву ролі у списку та клацніть, щоб переглянути детальні дозволи.

9.1.2 Управління та ведення списку користувачів

Модуль «Облікові записи та безпека» надає повний огляд усіх зареєстрованих профілів. З цього головного вікна адміністратори можуть швидко знаходити конкретних співробітників та виконувати стандартні завдання з управління життєвим циклом на основі списку користувачів, наприклад, змінювати облікові дані або коригувати права доступу.

Тільки користувачі, яким присвоєно роль адміністратора, можуть деактивувати або активувати користувача. Якщо користувач деактивовано, вхід за допомогою його облікового запису заборонено.

Примусово вийти з системи для користувача, що перебуває в мережі.

Натисніть на ім'я користувача, щоб переглянути та редагувати його налаштування.

Отримати актуальний статус усіх користувачів.

Введіть ключове слово або ім'я користувача, щоб знайти потрібних користувачів.

Користувачам, облікові записи яких заблоковано через надмірну кількість невдалих спроб входу, користувачі з роллю «Адміністратор» можуть розблокувати облікові записи для входу.

Ім'я користувача	Роль	Номер підключення	Статус входу	Статус користувача	Час завершення сесії
Admin	Адміністратор	1 >	Online	Активний	2019/12/01 23:55:55
User 15	Оператор	0 >	Не в мережі	Активний	2019/12/01 23:55:55

Рисунок 9.1 Список користувачів

9.1.3 Налаштування системних ролей

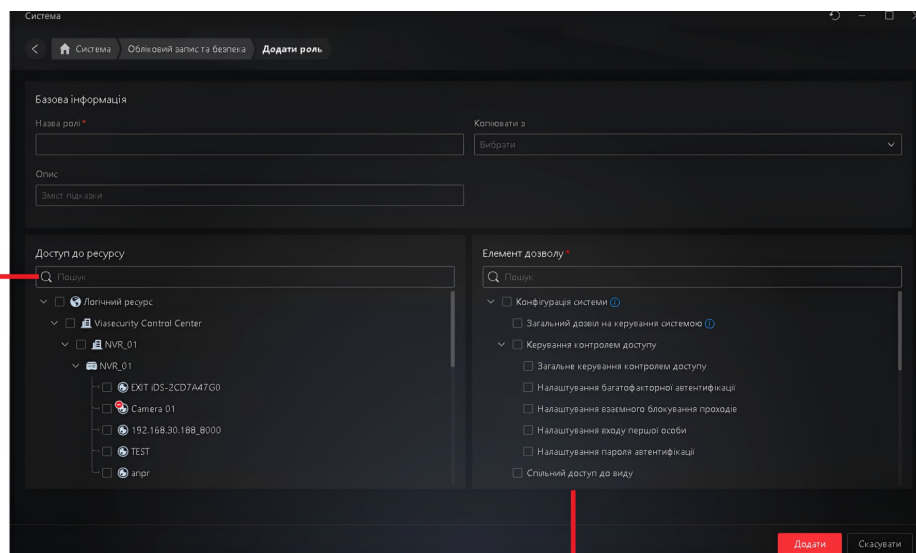
У Viasecurity Control Center ролі виконують функцію шаблонів дозволів, які визначають, які дії користувач має право виконувати. Групуючи конкретні привілеї платформи у власні ролі, ви можете ефективно розподіляти рівні доступу користувачів та керувати ними в системі.

Вбудовані системні профілі

Платформа містить дві обов'язкові ролі за замовчуванням. З міркувань безпеки та стабільності ці вбудовані профілі не можна редагувати чи видаляти:

1. **Адміністратор:** Цей профіль має абсолютний контроль і володіє всіма доступними правами доступу та налаштуваннями в межах усієї платформи.
2. **Оператор:** Цей профіль призначений для щоденного моніторингу та експлуатації; він надає повні повноваження для взаємодії з оперативними ресурсами та додатками без зміни основних системних налаштувань.

Виберіть ресурс(и),
до яких слід
застосувати
елемент(и) дозволу.



Виберіть один або кілька елементів дозволів. Наприклад, якщо встановлено прапорець «Управління пристроями», ви отримаєте дозвіл на налаштування та управління всіма доступними пристроями (тобто додавання, редагування та видалення пристроїв, а також пошук журналів).

Рисунок 9.2 Додавання ролей

Таблиця 9.1 Елементи дозволу

Категорія	Підкатегорія	Конкретний дозвіл
Конфігурація системи	Загальний дозвіл на керування системою	Дозвіл на налаштування системи, управління зображеннями облич та фігурами людей, систему автоматичного розпізнавання номерних знаків (ANPR), особами, управління подіями та сигналами тривоги, управління користувачами та ролями, права на перегляд, налаштування параметрів безпеки, а також додавання/видалення/редагування прав доступу до карт.

	Керування контролем доступу	Загальне керування контролем доступу: Доступ до модуля «Рівні доступу» в розділі Система: застосування рівнів доступу за підрозділами/особами; доступ до управління графіками доступу та налаштування графіків; доступ до управління рівнями доступу та налаштування рівнів доступу; повторне застосування рівня доступу у разі невдалого застосування; статистика та детальна інформація за статусом рівня доступу. Для отримання цього дозволу необхідний дозвіл на доступ до ресурсу для підрозділу(-ів) та осіб у межах підрозділу, а конкретні елементи дозволу призначаються відповідно до ресурсу.
--	-----------------------------	--

		Налаштування багатофакторної автентифікації: Увійдіть у меню налаштувань багатофакторної автентифікації та налаштуйте її. Для цього дозволу необхідний дозвіл на доступ до дверей, а конкретні елементи дозволу призначаються відповідно до ресурсу.
		Налаштування взаємного блокування проходів: Увійдіть у конфігурацію блокування декількох дверей та налаштуйте блокування декількох дверей. Для цього дозволу необхідний дозвіл на доступ до дверей, а конкретні елементи дозволу призначаються відповідно до ресурсу.
		Налаштування входу першої особи: Вхід до налаштувань «Відчинення дверей першою особою» та налаштування цієї функції. Для цього дозволу необхідний дозвіл на доступ до дверей, а конкретні елементи дозволу призначаються відповідно до ресурсу.
		Налаштування пароля автентифікації: Перейдіть до розділу Пароль автентифікації та налаштуйте пароль автентифікації на пристрої. Для цього дозволу необхідний дозвіл на доступ до дверей, а конкретні елементи дозволу призначаються відповідно до ресурсу.

	Спільний доступ до виду	Дозвіл на обмін переглядами з іншими користувачами та перегляд списку обмінів.
Керування пристроєм	Дозвіл на додавання/видалення/редагування всіх доступних пристроїв контролю доступу та відеодомофонів, моніторинг стану ресурсів у режимі реального часу, перевірку максимальної місткості та поточної кількості осіб, карток, відбитків пальців, знімків обличчя та подій, пов'язаних із пристроєм, редагування конфігурації пристрою, імпорт ресурсів вхідних/вихідних сигналів тривоги, управління зонами та ресурсами в межах зон, налаштування ієрархії зон та належних їм ресурсів, а також пошук журналів пристроїв.	
Дозвіл на операцію	Дозвіл на загальне спостереження	- Дозвіл на керування виходами сигналізації: необхідний дозвіл на доступ до ресурсів відповідних пристроїв, а конкретні елементи дозволу призначаються відповідно до ресурсу. - Дозвіл на доступ та керування всіма картами. - Дозвіл на створення/перегляд/експорт статистики та звітів щодо системи контролю доступу та відеодомофонної служби: необхідний дозвіл на доступ до ресурсів відповідних звітів, а конкретні елементи дозволу призначаються відповідно до ресурсу. - Дозвіл на отримання та обробку подій і сигналів тривоги: необхідний дозвіл на відповідні ресурси та сигнали тривоги, а конкретні елементи дозволу призначаються відповідно до ресурсу.

	Дозвіл на пошук	
	Операція з відео	Відтворення
		Експорт відео
		Керування тегами
	Операції з контролю доступу	Дистанційно: Відчинити двері
		Дистанційно: Замкнути двері
		Дистанційно: Залишити відімкненими
		Дистанційно: Залишити замкненими

9.2 Безпека облікового запису та відновлення облікових даних

У цьому розділі описано протоколи забезпечення цілісності облікових записів та управління даними доступу в Viasecurity Control Center. Тут наведено докладні інструкції щодо налаштування захисних правил безпеки.

9.2.1 Налаштування безпеки облікових записів

Щоб захистити систему від несанкціонованого доступу, можна встановити суворі параметри входу та опції відновлення. Щоб застосувати ці параметри, перейдіть до модуля **Обліковий запис та безпека** і виберіть **Налаштування безпеки**.

Параметри захисту входу

Макс. кількість невдалих спроб до блокування

Встановіть максимальну кількість послідовних спроб введення неправильного пароля, що допускаються. *(Зверніть увагу, що цей поріг враховує лише невдалі спроби введення пароля та ігнорує невдалі спроби введення коду підтвердження.)*

Після перевищення цього ліміту система миттєво заблокує відповідний обліковий запис для поточної IP-адреси.

Тривалість блокування

Вкажіть точну тривалість, протягом якої обліковий запис залишатиметься заблокованим після досягнення ліміту невдалих спроб.

Налаштування контрольних питань

Налаштуйте контрольні питання, призначені спеціально для облікового запису суперкористувача (адміністратора).

Ці питання слугують резервним методом для адміністратора, щоб підтвердити свою особу та відновити забутий пароль. Під час налаштування та процесу відновлення у всіх наданих відповідях не враховується реєстр.

9.2.2 Скидання пароля для входу

Користувачі мають можливість або змінити свій поточний пароль під час входу в систему, або скинути його, якщо забули.

Зміна пароля під час активної сесії

- Знайдіть та натисніть на ім'я вашого облікового запису у верхньому правому куті інтерфейсу.
- Виберіть **Змінити пароль** у меню, щоб встановити нові облікові дані.

Відновлення забутого пароля

Щоб розпочати процес відновлення, натисніть кнопку **Забули пароль** безпосередньо на головному екрані входу. Доступні методи відновлення суворо залежать від рівня привілеїв користувача:

Методи відновлення для суперкористувача (адміністратора):

- Контрольні запитання: Успішно дайте відповіді на заздалегідь налаштовані контрольні запитання, щоб відновити доступ.
- Перевірка коду ліцензії: Якщо ліцензія системи активна, введіть код активації, зазначений у вашому файлі ліцензії, щоб відновити пароль.
- Перевірка електронної пошти: Якщо ліцензія не активована, система надішле код підтвердження для відновлення на вказану електронну адресу адміністратора.

Способи відновлення для звичайних користувачів:

- Перевірка електронної пошти: Відновіть доступ за допомогою коду підтвердження, надісланого на вказану електронну адресу користувача.
- Допомога адміністратора: Зверніться з проханням про скидання пароля до користувача з вищим рівнем привілеїв. Користувачі без прав адміністратора можуть звернутися до адміністратора, тоді як адміністратори можуть звернутися за допомогою безпосередньо до головного адміністратора.

Розділ 10 Конфігурація системи

Ви можете керувати основними робочими параметрами Центру управління Viasecurity за допомогою модуля **Конфігурація системи**. Щоб отримати доступ до цих опцій, перейдіть у правий верхній кут інтерфейсу робочого столу та виберіть **Система → Конфігурація системи**.

Цей розділ управління дозволяє адміністраторам:

- Підключити поштові сервери для надсилання сповіщень.
- Встановлювати квоти на зберігання даних та правила їхнього зберігання.
- Визначати графіки святкових днів.
- Налаштовувати властивості мережі, зокрема синхронізацію NTP, налаштування WAN та протоколи доступу до пристроїв.
- Керувати безпекою облікових записів та сертифікатами SSL/TLS.
- Змінювати основні можливості системи.

10.1 Налаштування параметрів електронної пошти

Підключення облікового запису електронної пошти дозволяє системі надсилати автоматичні сповіщення про події та коди підтвердження для відновлення пароля до облікового запису.

Етапи налаштування:

1. Перейдіть до розділу **Система → Конфігурація системи → Електронна пошта**.
2. Вкажіть необхідні параметри підключення відповідно до вимог вашого поштового провайдера:
3. **Адреса SMTP-сервера:** Введіть ім'я хосту або IP-адресу вашого поштового провайдера (наприклад, smtp.gmail.com).
4. **Криптографічний протокол:** Оберіть необхідний метод шифрування для захисту вихідної пошти відповідно до вимог вашого SMTP-сервера.
5. **Аутентифікація на сервері:** Встановіть цей прапорець, якщо ваш поштовий сервер вимагає введення облікових даних для надсилання повідомлень.
6. Натисніть **Тест**, щоб переконатися, що програма може успішно зв'язуватися з поштовим сервером.
7. Натисніть **Зберегти**, щоб застосувати та завершити налаштування.

(Примітка: Якщо ви використовуєте обліковий запис Google Workspace або Gmail, спочатку потрібно увімкнути двоступеневу автентифікацію в налаштуваннях безпеки Google, згенерувати спеціальний пароль для додатка та ввести його тут для автентифікації.)

10.2 Управління графіками вихідних днів

Шаблони святкових/вихідних днів дають змогу визначити конкретні дати, які мають пріоритет над стандартними графіками щодо контролю доступу, спрацьовування сигналізації та послуг, що залежать від подій.

Створення запису про святковий день:

1. У меню **Конфігурація системи** виберіть вкладку **Вихідний**.
2. Натисніть **Додати**, присвойте унікальну назву та вкажіть **Тип вихідного дня**:
3. **Фіксована дата (регулярний святковий день)**: використовуйте цей варіант для святкових днів, які припадають на одну й ту саму календарну дату щороку, наприклад, Різдво (25 грудня).
4. **Рухомий (нерегулярне свято)**: використовуйте цей варіант для свят, що припадають на певні дні тижня, дата яких щороку змінюється, наприклад, День матері (друга неділя травня).

Редагування існуючих свят

Щоб оновити існуючий запис, знайдіть його у списку та натисніть безпосередньо на параметр, який бажаєте редагувати.

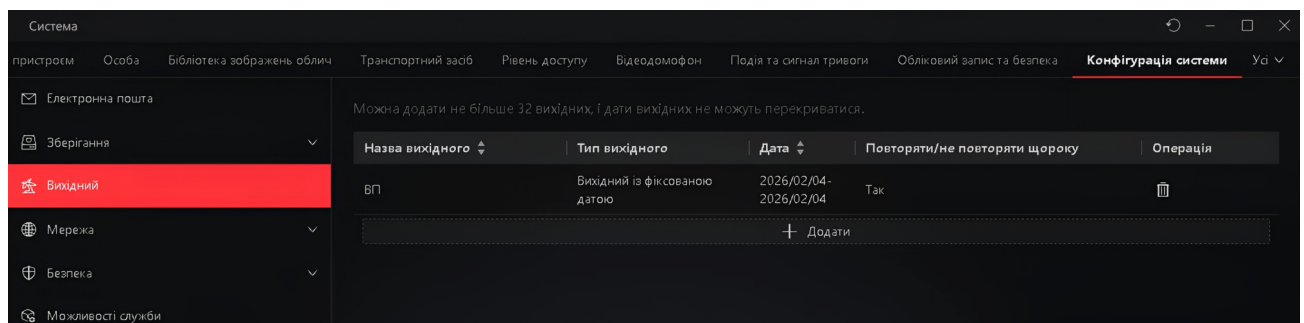


Рисунок 10.1 Редагування параметрів свята

10.3 Управління налаштуваннями мережі

Усі налаштування, пов'язані з мережею, можна виконати, перейшовши з головної сторінки до розділу **Система → Конфігурація системи → Мережа**.

10.3.1 Налаштування синхронізації часу через Інтернет

Ви можете налаштувати параметри NTP для синхронізації часу між ресурсами, що управляються на платформі, та сервером NTP. Підтримуються три режими синхронізації системного часу. Детальнішу інформацію дивіться в таблиці нижче.

Налаштування синхронізації часу

Щоб гарантувати точний час на всьому підключеному обладнанні, система пропонує три методи синхронізації:

1. Режим **Синхронізація часу операційної системи** використовує налаштування годинника вашого хост-комп'ютера та за замовчуванням синхронізує пристрої кожні 60 хвилин.
2. Якщо ви використовуєте виключно пристрої Viasecurity, можна вибрати опцію **Синхронізація часу з локальним сервером**, яка за замовчуванням також має інтервал у 60 хвилин.
3. Для ширшої сумісності режим **Синхронізація часу за NTP** дозволяє вказати власну адресу NTP-сервера, порт NTP та інтервал синхронізації. Якщо для вашого розгортання потрібні зовнішні сервери часу, цей режим підтримує увімкнення функції **Налаштування зіставлення WAN**. Ви завжди можете перевірити з'єднання з обраним сервером часу, натиснувши кнопку **Тест**.

10.3.2 Налаштування протоколу доступу до пристроїв

Перед інтеграцією обладнання відеоспостереження необхідно увімкнути відповідний протокол зв'язку. У налаштуваннях протоколу доступу до пристроїв можна активувати доступ через протокол ONVIF.

10.3.3 Налаштування доступу до глобальної мережі (WAN)

Для складних топологій, що вимагають зовнішнього підключення, необхідно активувати функцію доступу до глобальної мережі (WAN Access), щоб встановити статичну IP-адресу, доменне ім'я та конкретні порти для зв'язку в глобальній мережі. Залежно від вашої апаратної інфраструктури, вам потрібно буде призначити відповідні мережеві адреси. У середовищі з одним мережевим адаптером (NIC) визначте єдину системну мережеву адресу (SYS / System Storage Network Address) для обслуговування як доступу до системної мережі, так і служб зберігання даних.

Для високопродуктивних розгортань із використанням середовища з двома мережевими адаптерами (NIC) можна розділити трафік, визначивши мережеву адресу SYS для системних служб та окрему мережеву адресу системного сховища для операцій зі сховищем. Під час роботи з двома мережевими адаптерами переконайтеся, що як мережева адреса SYS, так і мережева адреса сервера запису, а

також відповідні мережеві адаптери, знаходяться в одному мережевому домені, щоб запобігти збоям у зв'язку.

Потім можна вибрати необхідні сценарії застосування та скористатися функцією «Налаштувати порт зіставлення», щоб призначити номер порту для передачі даних. Ви можете зберегти конфігурацію або експортувати повні дані зіставлення портів WAN, включаючи інформацію про LAN, WAN та протоколи, безпосередньо у файл Excel. Зверніть увагу, що будь-які подальші зміни порту LAN вимагатимуть відповідних коригувань у конфігурації зіставлення портів вашого маршрутизатора.

10.3.4 Налаштування NIC

Цей розділ дозволяє призначити конкретні мережеві адаптери поточного сервера для управління різними типами мережевого трафіку. Ви можете явно призначити мережевий адаптер SYS для прийому інформації про тривоги від обладнання, підключеного за протоколом ONVIF. Крім того, ви можете виділити окремий мережевий адаптер для системного сховища виключно для обробки інтенсивного обміну даними, необхідного під час архівування відеозаписів, зображень та робочих файлів.

10.3.5 Скидання мережевих налаштувань

Якщо у вашій системі відбудеться зміна мережевого домену, наприклад, під час міграції сервера, попередні конфігурації пристроїв стануть недійсними, що призведе до перебоїв у відтворенні медіа. Щоб адаптувати підключені пристрої до нового середовища, перейдіть до пункту **Скинути інформацію про мережу** та застосуйте команду **Скинути**.

10.4 Захист HTTPS-з'єднань за допомогою сертифікатів SSL/TLS

Щоб гарантувати, що клієнт взаємодіє виключно з перевіреними та безпечними серверами, Viasecurity Control Center забезпечує перевірку сертифікатів серверів, що захищає канал зв'язку шляхом блокування з'єднань із неперевіреними адресами.

10.4.1 Управління сертифікатами

Програмне забезпечення передбачає три окремі рівні перевірки сертифікатів для забезпечення відповідності різним політикам безпеки:

1. На рівні **Високий** система приймає виключно відкриті сертифікати, видані визнаним центром сертифікації (CA), або сертифікати PKI, створені

користувачем, активно відхиляючи будь-які самопідписані варіанти для забезпечення максимального рівня автентифікації. У цьому суворому режимі користувачі отримуватимуть попереджувальне повідомлення, якщо спробують підключитися до системи, використовуючи недійсний сертифікат або невідповідне ім'я хосту.

2. **Середній (рекомендований)** рівень дозволяє серверу працювати з самопідписаними сертифікатами за умови, що всі підключення за доменними іменами явно зареєстровані як користувацькі сервери.
3. **Базовий** рівень повністю обходить будь-яку перевірку сертифікатів, дозволяючи прямі підключення без будь-яких попереджувальних повідомлень. Не рекомендується використовувати цей стан з вимкненою перевіркою, оскільки активна перевірка сертифікатів є фундаментальним компонентом зміцнення безпеки системи.

10.4.2. Отримання сертифіката SSL/TLS

Отримання надійного сертифіката SSL/TLS передбачає придбання цифрового сертифіката у надійного центру сертифікації (CA) для забезпечення безпеки передачі даних та підтвердження ідентичності сервера. Цей придбаний сертифікат забезпечує значно вищий рівень безпеки порівняно зі стандартним сертифікатом платформи.

Спочатку необхідно вибрати надійний центр сертифікації та сформулювати запит на підписання сертифіката (CSR) разом із приватним ключем, використовуючи стандартні методи, такі як Microsoft IIS, OpenSSL або надійні веб-сайти. Надішліть сформований запит CSR до обраного центру сертифікації, щоб отримати авторизований сертифікат SSL/TLS, а потім завантажте його на свій локальний ПК. Дуже важливо переконатися, що завантажений файл сертифіката має саме формат PEM, використовуючи для цього інструменти конвертації або, за необхідності, редагуючи розширення файлу.

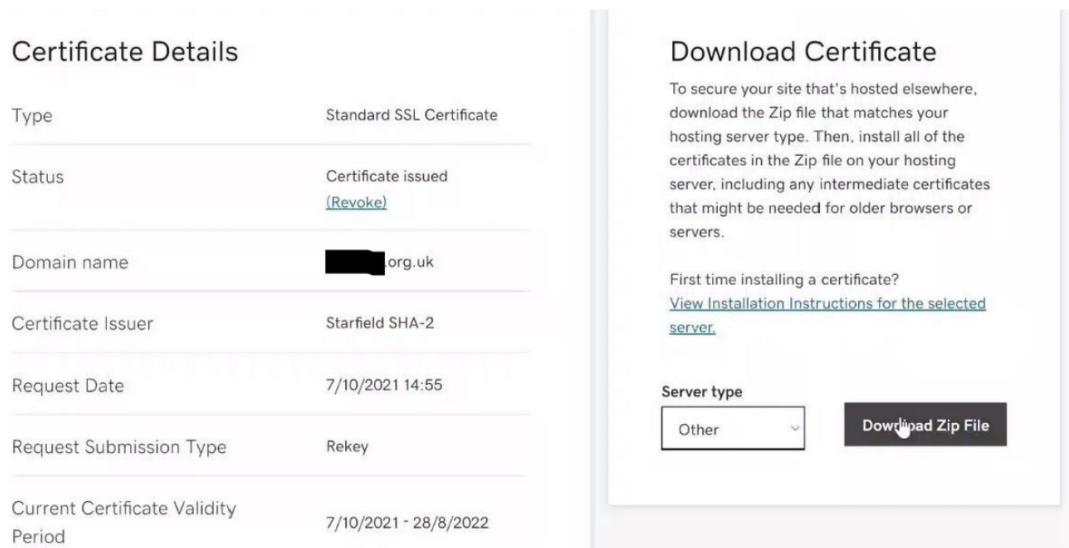


Рисунок 10.2 Приклад сертифіката SSL/TLS

10.4.3 Завантажте свій сертифікат SSL/TLS у систему

Щоб інтегрувати виданий сертифікат у систему, необхідно об'єднати його компоненти — зазвичай це файл сертифіката у форматі PEM, приватний ключ, згенерований за допомогою CSR, та ланцюжок сертифікатів у форматі PEM. Об'єднайте саме ці елементи в один файл PEM із кодуванням UTF-8 у суворій послідовності: спочатку файл сертифіката, потім приватний ключ, а наостанок — ланцюжок сертифікатів.

Далі перейдіть до **Система → Конфігурація системи → Безпека → Управління сертифікатами** у верхній частині інтерфейсу Desktop. Встановіть значення «Високий» у полі «Рівень безпеки сертифіката» та скористайтесь областю «Завантажити сертифікат», щоб завантажити щойно об'єднаний файл. Зверніть увагу, що після успішного завантаження програма Desktop автоматично перезапуститься. Крім того, якщо недійсний або неповний ланцюжок сертифікатів операційної системи спричиняє помилки перевірки, ви можете скористатися розділом «Сертифікат верхнього рівня», щоб додати ланцюжок безпосередньо на сервер. У таких випадках користувачі також мають можливість завантажити ланцюжок сертифікатів, перетворити його у формат CRT та встановити локально на своїх ПК.

```
-----BEGIN CERTIFICATE-----
MIIGbzCCBVeGAWIBAgIMUit4TG0LEB4xyfNBMA0GCSqGSIb3DQEBCwUAMFAxCzAJ
tAqm/TgWlV8dwimlwc6t525+Hrl3lOnHA3FF78cwWML5x5dNKhwf632dxMQz4IpB
8XMkRHge9AIdnlVmp2HUB7iOZW3K4Cv9O/YCwuHsnnFCibwWpXZUY2KSi52lRxBJ
0/gC3Cr/WyI5fRzHqnrXnHmEqQ==
-----END CERTIFICATE-----

-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEApg3HSjp4zoyFCii+Ct2f7501VmzdnYdxEVqBdQtMie27pJk6
G4e5YQKBgCE/n8nqGm9spvRz6GW59tboV8eByZePkyn+8ydv4VeSgL9q5uTbHKTQ
N9VTTuYxmAyUQ46EDWKHAU5445uEUFSbY6X+77zPEvuNpqUsdEsOjm9s4XmpibK
ptsahzxpzPKCKalnN2nnGpvJ60ailfEMYzP5zMNiEQPbtEZ734yR
-----END RSA PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
MIIHAgCCBOqgAWIBAgIQBeEL6xHDBPMqVc/6KaEeljANBqkqhkiG9w0BAQsFADBx
MQswCQYDVQQGEwJVUzErMCKGA1UEChMl0YWx3Z3XJrcyBjb3Rlcm5ldCBTb2x1
0y3ryvnrPxtYleAljYaHoa08klpIbWlOUZHL5T4DTFj6ko0Jl5MjGSTOanrvme52
oVOgwRlGPAUBRQyqbNA/N5PgYvnbYnP+3zLjV2fcsTQd9Ryk7ulSbK5ZTjds3PCC
Z/aCk1NiNiygUKZmFSniwaFMpojLdiBmKZjgepFJxMTiITr8ZqBG+lkJSZB88POf
AAyK5ka+CpCndiSV/gQnsMagCmeyhw==
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIF4DCCBMigAWIBAgIQAtzIUa9xYrr53z9VlROxXjANBqkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGAlUEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
FrgGtfxlRKPst8yZpX6jBLHy5eUUGJmG3VCGWRDrri1lWSajBC6RffzR7vzb0/wB
QOXi74AB8YHtYlzmjGGA7IY5Mjdur4CgcUWPlpqn4lgPvzRdRDvD0lg3rvpF/ma
ySyHlhO/+GHWldxQRb0QdhxyF4g=
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIDjjCCANagAWIBAgIQAzrx5qcRqaC7KGSxHQn65TANBqkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGAlUEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZ3RlbnRlcuY29tMSAwHgyYDVQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBH
Fdtom/DzMNU+MeKNhJ7jitrAlj41E6Vf8PlwUHBHQRFXGU7Aj64GxJUTFY8bJZ91
8rGOMAfvE7FBcf6IKshPECBV1/MURexGRPTqh5Uykw7+U0b6LJ3/iYK5S9kJRaTe
pLiaWN0bfVKfjllDiIGknibVb63dDcy3fe0Dkhvld1927jyNxFlWW6LZ2m6zNTfl
MrY=
-----END CERTIFICATE-----
```

Рисунок 10.3 Приклад об'єднаного сертифіката

10.5 Налаштування сертифіката компонента служби

Щоб забезпечити належний рівень безпеки даних, перед інтеграцією сервера потокового передавання необхідно синхронізувати сертифікати між головним сервером та новим компонентом. Цей процес передбачає використання функції **Сертифікат між службами в системі**, яку можна знайти на головній сторінці, перейшовши за наступним шляхом: **Система → Конфігурація системи → Безпека → Сертифікат компонента служби**.

У цьому меню ви можете переглянути існуючий сертифікат, скопіювати його для налаштування або створити новий, дотримуючись підказок системи; зверніть увагу, що для будь-яких дій, пов'язаних із сертифікатом, необхідно ввести пароль адміністратора. Лише після того, як дані сертифіката на обох серверах стануть ідентичними, ви зможете продовжити додавання апаратного забезпечення. Крім того,

якщо ваша конфігурація передбачає використання додаткового сервера для міжмашинного резервного копіювання та відновлення, вам потрібно буде створити **підпис автентифікації системного сховища AK/SK**. Оновлення або створення цього підпису також вимагає підтвердження паролем адміністратора.

10.6 Приватність та безпека

Ви можете самостійно керувати налаштуваннями приватності, перейшовши до **Система → Конфігурація системи → Безпека → Конфіденційність та безпека**.

У цьому вікні ви можете налаштувати **Програму покращення взаємодії з користувачами**, яка дозволяє системі надсилати звіти про операційні журнали та показники використання програмного забезпечення з метою вдосконалення продукту. Якщо ваша політика безпеки не дозволяє надавати таку інформацію, ви можете будь-коли вимкнути цю функцію у відповідному меню налаштувань.

Розділ 11 Технічне обслуговування

У цьому розділі розглядається моніторинг стану серверів та пристроїв у режимі реального часу з метою забезпечення оптимальної роботи систем безпеки. Тут ви знайдете інструкції щодо формування звітів про стан, отримання сповіщень та пошуку в системних журналах.

11.1 Створення та відображення звіту про технічне обслуговування

Viasecurity Control Center постійно відстежує систему та підключені ресурси на предмет будь-яких відхилень у роботі. Ви можете налаштовувати та переглядати ці зведені дані про стан серверів, апаратного забезпечення контролю доступу та відеопристроїв.

Створити звіт про технічне обслуговування

Щоб створити новий звіт, перейдіть на головну сторінку, клацніть правою кнопкою миші на **Статистика** у панелі ресурсів і виберіть **Додати звіт про статистику**. Виберіть «Технічне обслуговування» як тип статистики, вкажіть власну назву звіту та вкажіть бажаний тип пристрою.

Додати статистичний звіт

Створіть свій статистичний звіт

1. Виберіть тип статистичної інформації

Технічне обслуговування
У звіті про обслуговування автоматично відстежуються винятки системи та її ресурсів у реальному часі.

Підрахунок людей
Вибирайте одну або кілька потрібних вам камер для підрахунку людей і формуйте звіти в реальному часі або на підставі історичних даних. Можна легко реорганізувати дані, щоб отримати більше інформації...

Особа й засіб авторизації
Підрахунок загальної кількості осіб і засобів авторизації на платформі.

Рівень доступу
Підрахунок розподілу рівня доступу й чинного статусу всіх осіб на платформі.

Події контролю доступу за сьогодні
Містить всі нормальні або ненормальні події, які сталися сьогодні (з 00:00 до поточного часу) в усіх точках доступу.

Топ-5 ненормальних подій системи контролю доступу за сьогодні
Містить топ-5 ненормальних подій, які сталися сьогодні (з 00:00 до поточного часу) в усіх точках доступу.

2. Заповніть статистичну інформацію

Назва статистичного елемента *

Тип пристрою *

Пристрій контролю доступу

Контроль доступу

OK Скасува...

Рисунок 11.1 Створити звіт про технічне обслуговування

Перегляд звіту про технічне обслуговування

Після створення натисніть на піктограму , щоб перейти до зібраних статистичних даних, і двічі клацніть на конкретному звіті, щоб переглянути його детальні дані. Зверніть увагу, що візуальне оформлення цих статистичних даних залежить від обраної вами категорії обладнання.

Для отримання точних показників щодо сховища відео, місця зберігання, диска та мережевої карти (NIC) попередньо необхідно перезапустити систему SYS. Крім того, дані для диска C не можуть відображатися під час роботи у середовищі віртуальної машини. Якщо статистичні дані не відображаються, спочатку перегляньте системні журнали, щоб виявити можливі повідомлення про помилки, пов'язані з диском.

Усі види пристроїв

На цій сторінці наведено кількість випадків як зі статусом  **Нормальний**, так і зі статусом  **Виянок**, що охоплює всі типи пристроїв, включаючи відеопристрої, пристрої контролю доступу та сервери.

Всі види пристроїв		
Тип	Нормальна	Помилка
Відео	 8	 4 >
Контроль доступу	 4	 0 >
Сервер потокового мультимедіа	 0	 0 >
SYS	 Нормальна >	
Сервер запису	 Нормальна >	

Рисунок 11.2 Усі види пристроїв

Ви можете натиснути на піктограму , щоб переглянути детальну інформацію про сервер та пристрій у звичайному або аварійному стані.

- Для SYS можна перевірити завантаження процесора, використання оперативної пам'яті, трафік мережевої карти та обсяг передачі даних через шлюз потокового передавання.

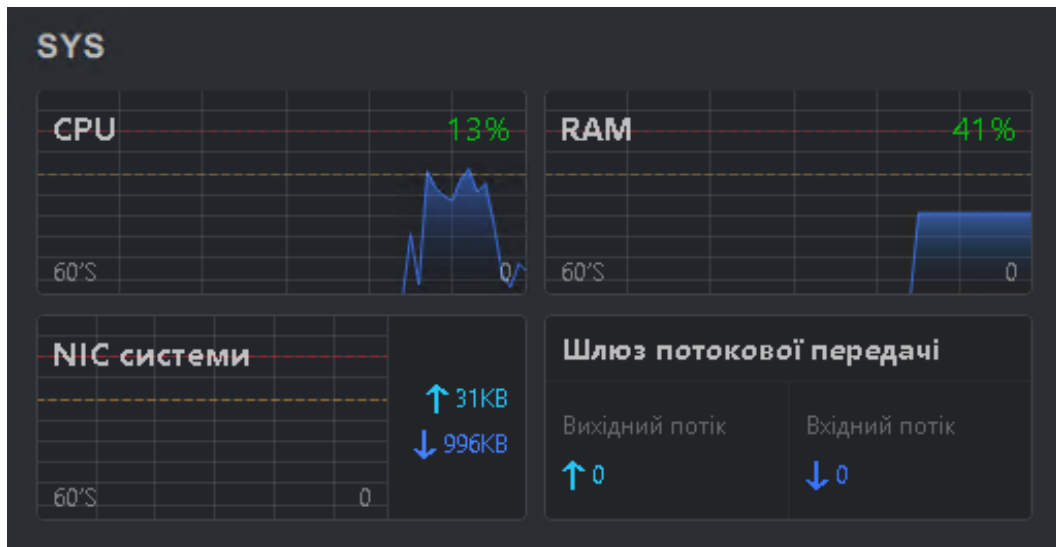


Рисунок 11.3 SYS

- Для сервера запису можна перевірити трафік мережевої карти, операції вводу-виводу на диск, місце зберігання даних та обсяг сховища відеозаписів.

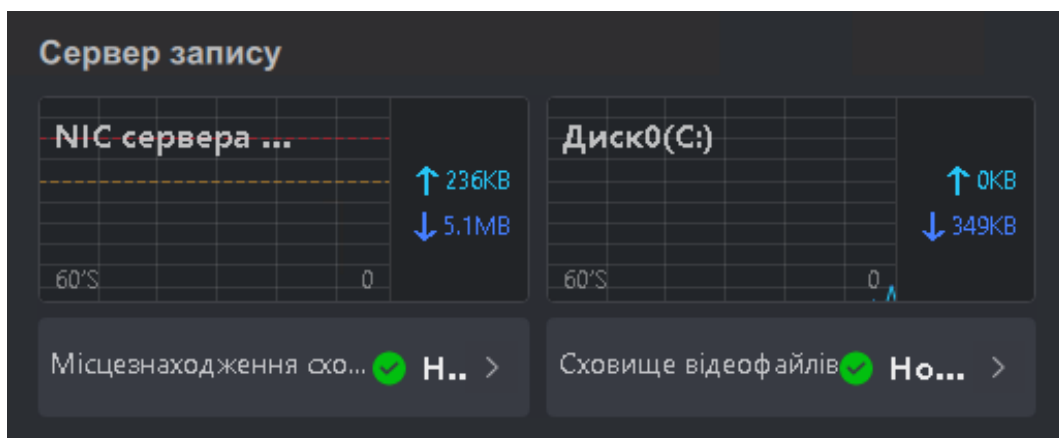


Рисунок 11.4 Сервер запису

- Щодо пристроїв, ви будете перенаправлені на сторінку **Керування пристроями**, де зможете переглянути деталі винятків.

Відео

- Натисніть на піктограму поруч із числом, щоб перейти на сторінку управління пристроями. Тут ви можете переглянути детальну інформацію про відеопристрої, які перебувають у стані втрати відеосигналу, винятку запису або винятку зображення.
- Наведіть курсор на кругову діаграму, щоб переглянути кількість пристроїв, що працюють у нормальному режимі, або тих, у яких виникла виняткова ситуація.

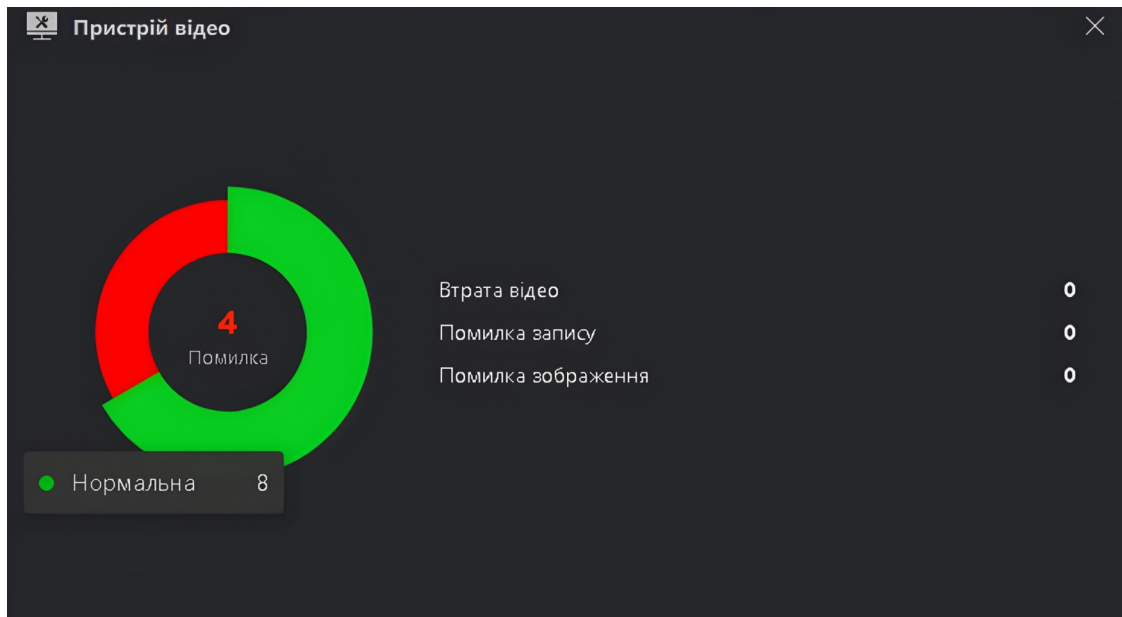


Рисунок 11.5 Статистика відео

Контроль доступу

- Натисніть на піктограму поруч із числом, щоб перейти на сторінку управління пристроями. Тут ви можете переглянути детальну інформацію про пристрої контролю доступу, які перебувають у стані винятку щодо безпеки пристрою, винятку щодо мережі пристрою, винятку щодо звітності записів пристрою або винятку щодо заряду акумулятора пристрою.
- Наведіть курсор на кругову діаграму, щоб переглянути кількість пристроїв, що працюють у нормальному режимі, або тих, що перебувають у стані винятку.

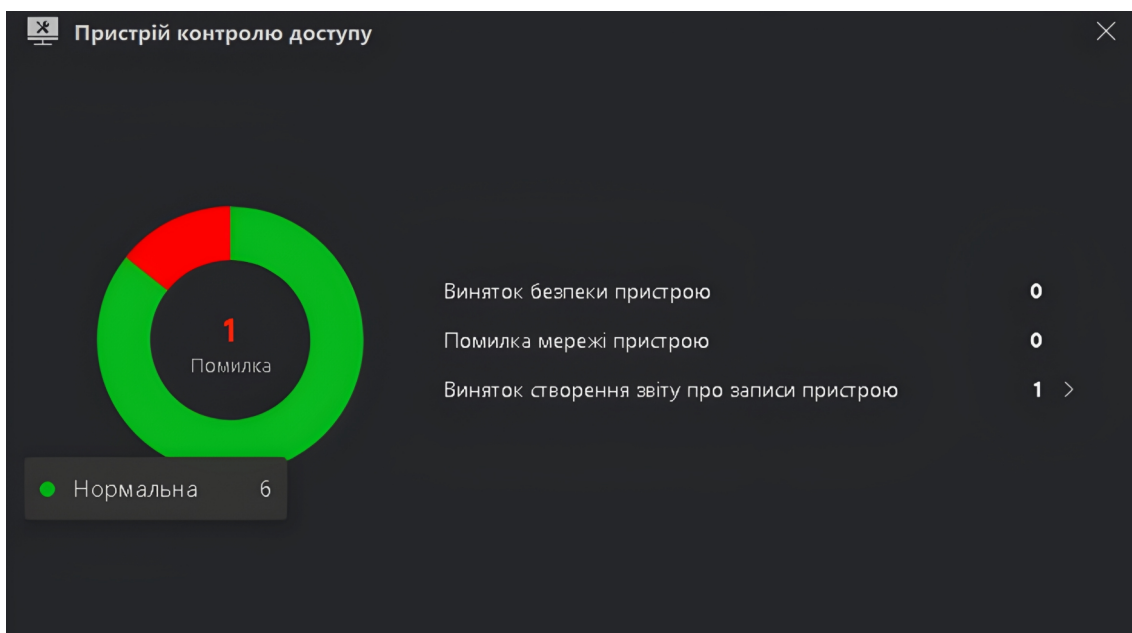


Рисунок 11.6 Статистика контролю доступу

Сервер

Надає загальну інформацію про SYS та сервер запису, включаючи завантаження процесора, трафік мережевої карти, операції вводу-виводу на диск тощо.

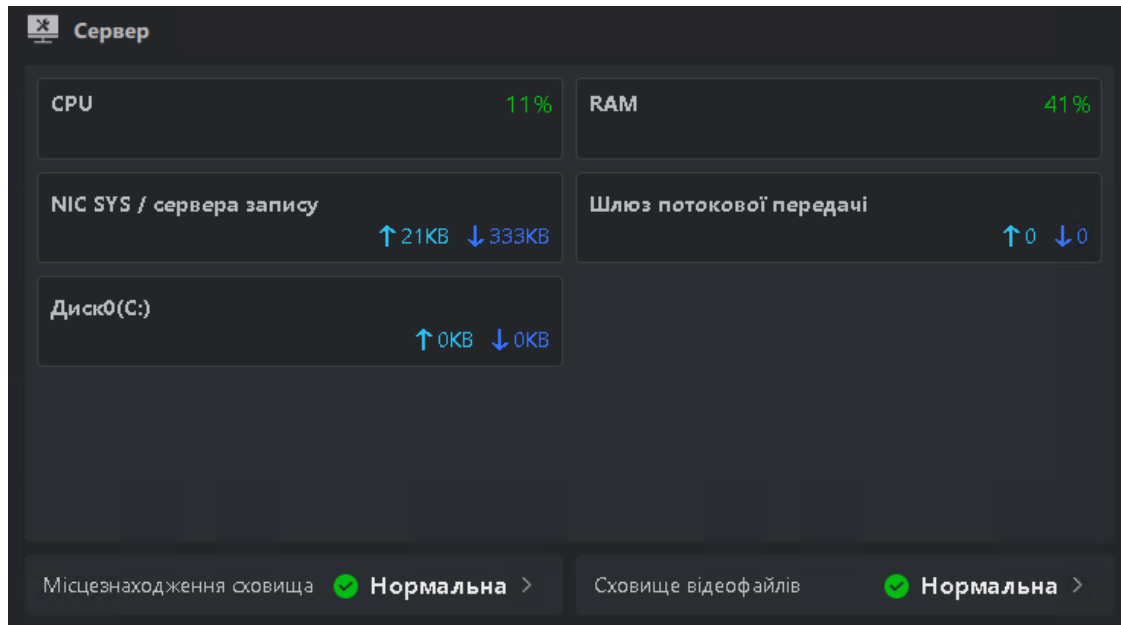


Рисунок 11.7 Статистика сервера

11.2 Пошук повідомлень

Користувачі можуть переглядати історію сповіщень, щоб виявляти оновлення системи або події безпеки та реагувати на них.

Щоб здійснити пошук сповіщень:

1. Перейдіть до **Головна** → **Пошук** → **Сповіщення**.
2. Скористайтесь фільтрами, щоб вибрати конкретну **Дату** та **Тип сповіщення**.
3. До зареєстрованих сповіщень належать:
4. **Системні сповіщення**: критичні проблеми, наприклад «тип пристрою не підтримується».
5. **Дії користувачів**: функціональні повідомлення, наприклад «не відповіли на дзвінок по відеодомофону».
6. Щоб витягти дані, натисніть **Експорт** (у верхньому лівому куті), щоб зберегти поточний вигляд у вигляді файлу **Excel**, **PDF** або **CSV**.

Записи сповіщень			
SVS: 127.0.0.1			
Експорт часу: 2026/07/01 16:37:34			
Сукупна кількість: 511			
Назва	Час (клієнт)	Тип	Опис
Поштовий сервер не налаштований	2026/06/30 17:21:58	Система	Поштовий сервер не налаштовано.
Дисковий простір для встановлення п. 2026/06/30 09:09:42	2026/06/30 09:09:42	Система	Вільне місце на диску, на якому встановлена платформа (C:), скоро закінчиться.
Вільне місце на диску скоро закінчиться 2026/06/30 09:09:42	2026/06/30 09:09:42	Система	Вільне місце на диску (C:) скоро закінчиться.
Дисковий простір для встановлення п. 2026/06/30 08:59:13	2026/06/30 08:59:13	Система	Вільне місце на диску, на якому встановлена платформа (C:), скоро закінчиться.
Вільне місце на диску скоро закінчиться 2026/06/30 08:59:13	2026/06/30 08:59:13	Система	Вільне місце на диску (C:) скоро закінчиться.
Дисковий простір для встановлення п. 2026/06/30 08:48:44	2026/06/30 08:48:44	Система	Вільне місце на диску, на якому встановлена платформа (C:), скоро закінчиться.
Вільне місце на диску скоро закінчиться 2026/06/30 08:48:44	2026/06/30 08:48:44	Система	Вільне місце на диску (C:) скоро закінчиться.
Дисковий простір для встановлення п. 2026/06/30 08:38:14	2026/06/30 08:38:14	Система	Вільне місце на диску, на якому встановлена платформа (C:), скоро закінчиться.
Вільне місце на диску скоро закінчиться 2026/06/30 08:38:14	2026/06/30 08:38:14	Система	Вільне місце на диску (C:) скоро закінчиться.
Дисковий простір для встановлення п. 2026/06/30 08:27:45	2026/06/30 08:27:45	Система	Вільне місце на диску, на якому встановлена платформа (C:), скоро закінчиться.
Вільне місце на диску скоро закінчиться 2026/06/30 08:27:45	2026/06/30 08:27:45	Система	Вільне місце на диску (C:) скоро закінчиться.
Дисковий простір для встановлення п. 2026/06/30 08:17:15	2026/06/30 08:17:15	Система	Вільне місце на диску, на якому встановлена платформа (C:), скоро закінчиться.
Вільне місце на диску скоро закінчиться 2026/06/30 08:17:15	2026/06/30 08:17:15	Система	Вільне місце на диску (C:) скоро закінчиться.
Дисковий простір для встановлення п. 2026/06/30 08:06:46	2026/06/30 08:06:46	Система	Вільне місце на диску, на якому встановлена платформа (C:), скоро закінчиться.

Рисунок 11.8 Шаблон Excel для витягання повідомлень

11.3 Пошук системних журналів

Для забезпечення цілісності системи та прискорення вирішення проблем Viasecurity Control Center дає змогу отримувати та аналізувати журнали як на стороні сервера, так і на рівні апаратного забезпечення.

Доступ до системних журналів

Журнали поділяються на **журнали сервера**, які ведуться на центральному сервері, та **журнали пристроїв**, які зберігаються безпосередньо на апаратному забезпеченні.

Централізований пошук

Щоб здійснити пошук за обома типами журналів з єдиного інтерфейсу, перейдіть до **Головна → Пошук → Журнал системи**.

Прямий доступ до журналів пристроїв

Якщо апаратне забезпечення підтримує цю функцію, ви можете отримати доступ до локальних записів за допомогою таких методів:

- **Управління пристроями:** Перейдіть до **Головна → Система → Керування пристроєм**, клацніть правою кнопкою миші на конкретному пристрої та виберіть **Переглянути журнал**.
- **Детальний перегляд:** На сторінці **Деталі пристрою** клацніть правою кнопкою миші на пристрої, виберіть **Перегляд подробиць** та натисніть **Переглянути журнал** у правому верхньому куті.

Аналіз журналів та експорт даних

Фільтрування журналів сервера

Звузьте перелік подій, вибравши рівні серйозності: **Інформація**, **Сигнал тривоги**, **Операція** або **Помилка**. Ви також можете скористатися полем **Назва ресурсу**, щоб швидко виділити конкретні записи.

Витяг даних

Щоб зберегти записи для зовнішнього аналізу, натисніть **Експорт** у верхньому лівому куті, щоб завантажити журнали у форматі **Excel** або **CSV**.

Журнал сервера							
Базова інформація							
Експорт часу:	01.07.2026 16:40						
Оператор:	admin						
Експортувати вміст:	Дані						
Час звіту:	2026/07/01 00:00:00 - 2026/07/01 23:59:59						
Сукупна кількість:	51						
Рівень	Час (клієнт)	Джерело	Подія	Назва рес	Область	Адреса	Опис
Інформація	01.07.2026 16:40	admin	Експорт журналу			127.0.0.1	
Інформація	01.07.2026 16:40	admin	Експорт журналу			127.0.0.1	
Інформація	01.07.2026 16:40	admin	Пошук у журналі			127.0.0.1	
Інформація	01.07.2026 16:40	admin	Пошук у журналі			127.0.0.1	
Інформація	01.07.2026 16:40	admin	Пошук у журналі			127.0.0.1	
Інформація	01.07.2026 16:39	admin	Пошук у журналі			127.0.0.1	
Інформація	01.07.2026 16:39	admin	Пошук у журналі			127.0.0.1	
Інформація	01.07.2026 16:39	admin	Пошук у журналі			127.0.0.1	
Інформація	01.07.2026 16:39	admin	Пошук у журналі			127.0.0.1	
Інформація	01.07.2026 16:39	admin	Пошук запису про сповіщення			127.0.0.1	
Інформація	01.07.2026 16:37	admin	Експортувати запис про спові			127.0.0.1	
Інформація	01.07.2026 16:37	admin	Пошук запису про сповіщення			127.0.0.1	
Інформація	01.07.2026 16:37	admin	Пошук запису про сповіщення			127.0.0.1	
Інформація	01.07.2026 16:37	admin	Пошук запису про сповіщення			127.0.0.1	
Інформація	01.07.2026 16:34	admin	Додати ст Пристрій контролю			127.0.0.1	

Рисунок 11.9 Шаблон Excel для журналу сервера

А. Обмеження щодо використання продукту: сценарії та рекомендації

У цьому розділі наведено сценарії, в яких діють обмеження, щоб допомогти користувачам уникнути ненавмисного неправильного використання. Він слугує коротким довідником для перевірки дозволених дій у конкретних випадках використання.

Система

- Якщо запустити клієнт з правами адміністратора, імпорту даних у систему може завершитися невдачею.
- Для перегляду експортованих файлів Excel необхідно встановити Microsoft Office.
- Не перетягуйте клієнт між екранами з різними налаштуваннями DPI, оскільки це може призвести до небажаних проблем зі масштабуванням інтерфейсу користувача.
- Переконайтеся, що вільного місця на диску не менше 10 ГБ, щоб уникнути збою під час встановлення сервера.

Управління пристроями

- Камери, у назвах яких містяться спеціальні символи, зокрема \ / : * ? " < > | , не можна імпортувати.
- Під час редагування пароля пристрою на веб-сторінці зупиніть прямий перегляд та відтворення на всіх клієнтах і якнайшвидше змініть пароль у списку пристроїв. Спробуйте змінити пароль пристрою через систему, а не через веб-сторінку.

Відеоспостереження

- Під час використання TargetTrace / пошуку об'єктів, якщо з'являється неправильне повідомлення, ви можете перевірити, чи увімкнено цю функцію на сторінці налаштувань пристрою.
- Не змінюйте безпідставно налаштування щодо шифрування потоку пристрою або конкретні ключі шифрування.
- Не використовуйте одночасно функцію «плавного потоку» та шифрування потоку.
- Для пристроїв, налаштованих на запис із двома потоками, під час відтворення відео буде використовуватися основний потік.
- Ручний запуск запису не підтримується під час перегляду в режимі реального часу через «плавний потік».

- Якщо підключені пристрої не підтримують час за UTC, під час використання функцій пошуку (пошук відео / «Смарт-пошук» / усі пошуки через NVR) у період переходу на літній час (DST) система не може розрізнити дубльовані часові проміжки (наприклад, час 01:30, що з'являється двічі після закінчення літнього часу). Усі результати пошуку відображатимуться за місцевим часом пристрою без коригування зсуву щодо UTC. Для подій та тривог у реальному часі (пошук у журналі тривог), що базуються на пристроях без підтримки UTC, під час періодів виходу з переходу на літній час можуть з'являтися дубльовані часові мітки (наприклад, два записи з позначкою «01:30»).
- Для перегляду в реальному часі та відтворення через пристрої Axis та Hanwha переконайтеся, що вибрано формат кодування H.264.
- Зворотне відтворення відео, збережених на пристроях Axis, Dahua або Hanwha, не підтримується.
- Одночасне синхронізоване відтворення підтримується не більше ніж для 12 вікон перегляду.
- Щоб збільшити зображення, розширене за допомогою ефекту «риб'яче око», двічі клацніть на зображенні перед увімкненням розширення «риб'яче око».
- Двосторонній аудіозв'язок через канали DVR не підтримується.
- Під час малювання зон виявлення для підрахунку людей підтримуються лише прямокутні зони.
- Для камер, що керуються через NVR/DVR, система не може отримати їхні попередні налаштування.
- Відео у форматі AVI можуть не відтворюватися програвачами, що входять до складу Windows, тому рекомендується використовувати безкоштовні програвачі, які підтримують усі відеоформати.

Контроль доступу та відеодомофон

- Під час імпортування ZIP-файлу з профільними фотографіями переконайтеся, що мова системи на ПК, з якого здійснюється стиснення профільних фотографій, збігається з мовою системи сервера.

Системне сховище

- Для зберігання відео підтримується до 128 камер.
- Якщо ліцензія на зберігання відео не активована, у системі можна зберігати лише зображення та файли.
- Для встановлення Viasecurity Control Center із системним сховищем переконайтеся, що диск відповідає таким мінімальним вимогам щодо ємності; інакше його не можна буде використовувати для системного сховища.

- 34 ГБ (якщо ємність диска ≤ 2 ТБ)
- 74 ГБ (якщо ємність диска > 2 ТБ)
- Ініціалізація диска займає 90 % вільного місця на диску.
- Оскільки відео, зображення та файли зберігаються на системному диску, перехід системи в режим глибокого сну або сплячого режиму може призвести до відключення живлення диска, що потенційно може спричинити винятки у зберіганні. Рекомендується вимкнути режим глибокого сну або сплячого режиму.
- Мінімальний обсяг місця, необхідний для кожного типу файлів, становить 4 ГБ (наприклад, 4 ГБ для відео, 4 ГБ для зображень і 4 ГБ для файлів), що включає файли, необхідні для управління зберіганням.
- Відновлення індексу може тимчасово вплинути на функціональність пошуку та відтворення, але це не призведе до втрати даних.
- Підтримується 6 варіантів перезапису даних.
- У середовищі віртуальної машини продуктивність диска C не відображатиметься у звіті про технічне обслуговування. Див. 11.1 Створення та відображення звіту про технічне обслуговування для отримання додаткової інформації.

Юридична інформація

Про цей документ

- Цей документ містить інструкції щодо використання та управління Продуктом. Ілюстрації, діаграми, зображення та вся інша інформація, наведена нижче, мають виключно описовий та пояснювальний характер.
- Інформація, що міститься в цьому документі, може змінюватися без попередження у зв'язку з оновленнями прошивки або з інших причин. Останню версію документа можна знайти на веб-сайті Viasecurity (<https://viasecurity.ua>). Якщо інше не погоджено, компанія Viasecurity LLC або її афілійовані особи (далі — «Viasecurity») не надають жодних гарантій, явних чи припущених.
- Будь ласка, користуйтеся цим документом під керівництвом та за допомогою фахівців, які пройшли навчання з технічної підтримки даного продукту.

Про цей продукт

Цей продукт може отримувати післяпродажне обслуговування лише в тій країні або регіоні, де було здійснено його придбання.

Визнання прав інтелектуальної власності

- Компанія Viasecurity володіє авторськими правами та/або патентами, пов'язаними з технологією, втіленою в Продуктах, описаних у цьому Документі, що може включати ліцензії, отримані від третіх осіб.
- Будь-яка частина цього Документа, включаючи текст, зображення, графіку тощо, належить компанії Viasecurity. Жодна частина цього Документа не може бути витягнута, скопійована, перекладена або змінена повністю чи частково будь-якими засобами без письмового дозволу.
- Viasecurity та інші торговельні марки й логотипи Viasecurity є власністю компанії Viasecurity у різних юрисдикціях.
- Інші згадані торговельні марки та логотипи є власністю відповідних власників.

ЮРИДИЧНЕ ЗАСТЕРЕЖЕННЯ

- У МАКСИМАЛЬНО ДОЗВОЛЕНИХ ЧИННИМ ЗАКОНОДАВСТВОМ МЕЖАХ ЦЕЙ ДОКУМЕНТ ТА ОПИСАНИЙ ПРОДУКТ, ВКЛЮЧАЮЧИ ЙОГО АПАРАТНЕ, ПРОГРАМНЕ ТА ВБУДОВАНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, НАДАЮТЬСЯ «ЯК Є» ТА «З УСІМА НЕДОЛІКАМИ ТА ПОМИЛКАМИ». VIASECURITY НЕ НАДАЄ ЖОДНИХ ЯВНИХ АБО ПРИПУЩЕНИХ ГАРАНТІЙ, ВКЛЮЧАЮЧИ, БЕЗ ОБМЕЖЕНЬ, ГАРАНТІЇ ПРИДАТНОСТІ ДЛЯ ПРОДАЖУ, ЗАДОВІЛЬНОЇ ЯКОСТІ АБО ПРИДАТНОСТІ ДЛЯ КОНКРЕТНОЇ МЕТИ.

ВИ КОРИСТУЄТЕСЯ ЦИМ ПРОДУКТОМ НА ВЛАСНИЙ РИЗИК. У ЖОДНОМУ ВИПАДКУ VIASECURITY НЕ НЕСЕ ПЕРЕД ВАМИ ВІДПОВІДАЛЬНОСТІ ЗА БУДЬ-ЯКІ ОСОБЛИВІ, НАСЛІДКОВІ, ВИПАДКОВІ АБО НЕПРЯМІ ЗБИТКИ, ВКЛЮЧАЮЧИ, СЕРЕД ІНШОГО, ЗБИТКИ ВІД ВТРАТИ КОМЕРЦІЙНОГО ПРИБУТКУ, ПЕРЕРИВАННЯ ДІЯЛЬНОСТІ АБО ВТРАТИ ДАНИХ, ПОШКОДЖЕННЯ СИСТЕМ АБО ВТРАТУ ДОКУМЕНТАЦІЇ, НЕЗАЛЕЖНО ВІД ТОГО, ЧИ ВОНИ ВИНИКАЮТЬ НА ОСНОВІ ПОРУШЕННЯ ДОГОВОРУ, ПРАВОПОРУШЕННЯ (ВКЛЮЧАЮЧИ НЕДБАЛИСТЬ), ВІДПОВІДАЛЬНОСТІ ЗА ПРОДУКЦІЮ АБО ІНШИХ ПІДСТАВ, У ЗВ'ЯЗКУ З ВИКОРИСТАННЯМ ПРОДУКТУ, НАВІТЬ ЯКЩО КОМПАНІЯ VIASECURITY БУЛА ПОПЕРЕДЖЕНА ПРО МОЖЛИВІСТЬ ТАКИХ ЗБИТКІВ АБО ВТРАТ

- ВИ ВИЗНАЄТЕ, ЩО ХАРАКТЕР ІНТЕРНЕТУ ПЕРЕДБАЧАЄ ВЛАСНІ РИЗИКИ БЕЗПЕКИ, І VIASECURITY НЕ НЕСЕ ЖОДНОЇ ВІДПОВІДАЛЬНОСТІ ЗА НЕНОРМАЛЬНУ РОБОТУ, ВИТОК ПЕРСОНАЛЬНИХ ДАНИХ АБО ІНШІ ЗБИТКИ, ЩО ВИНИКАЮТЬ ВНАСЛІДОК КІБЕРАТАКИ, ХАКЕРСЬКОЇ АТАКИ, ЗАРАЖЕННЯ ВІРУСАМИ АБО ІНШИХ РИЗИКІВ, ПОВ'ЯЗАНИХ З БЕЗПЕКОЮ В ІНТЕРНЕТІ; ПРОТЕ, У РАЗІ НЕОБХІДНОСТІ, VIASECURITY НАДАСТЬ СВОЄЧАСНУ ТЕХНІЧНУ ПІДТРИМКУ.
- ВИ ПОГОДЖУЄТЕСЯ ВИКОРИСТОВУВАТИ ЦЕЙ ПРОДУКТ У ВІДПОВІДНОСТІ ДО ВСІХ ЧИННИХ ЗАКОНІВ, І ВИ НЕСЕТЕ ВИКЛЮЧНУ ВІДПОВІДАЛЬНІСТЬ ЗА ЗАБЕЗПЕЧЕННЯ ТОГО, ЩОБ ВАШЕ ВИКОРИСТАННЯ ВІДПОВІДАЛО ЧИННОМУ ЗАКОНОДАВСТВУ. ЗОКРЕМА, ВИ НЕСЕТЕ ВІДПОВІДАЛЬНІСТЬ ЗА ВИКОРИСТАННЯ ЦЬОГО ПРОДУКТУ ТАКИМ ЧИНОМ, ЩОБ НЕ ПОРУШУВАТИ ПРАВА ТРЕТЬОЇ СТОРОНИ, ВКЛЮЧАЮЧИ, БЕЗ ОБМЕЖЕНЬ, ПРАВА НА ПУБЛІЧНІСТЬ, ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ, А ТАКОЖ ПРАВА НА ЗАХИСТ ДАНИХ ТА ІНШІ ПРАВА НА ПРИВАТНІСТЬ. ВИ НЕ МАЄТЕ ПРАВА ВИКОРИСТОВУВАТИ ЦЕЙ ПРОДУКТ ДЛЯ БУДЬ-ЯКИХ ЗАБОРОНЕНИХ ЦІЛЕЙ, ВКЛЮЧАЮЧИ РОЗРОБКУ АБО ВИРОБНИЦТВО ЗБРОЇ МАСОВОГО ЗНИЩЕННЯ, РОЗРОБКУ АБО ВИРОБНИЦТВО ХІМІЧНОЇ АБО БІОЛОГІЧНОЇ ЗБРОЇ, БУДЬ-ЯКИХ ДІЙ, ПОВ'ЯЗАНИХ З ЯДЕРНИМИ ВИБУХОВИМИ ПРИСТРОЯМИ АБО НЕБЕЗПЕЧНИМ ЯДЕРНИМ ПАЛИВНИМ ЦИКЛОМ, А ТАКОЖ ДІЙ, ЩО СПРИЯЮТЬ ПОРУШЕННЮ ПРАВ ЛЮДИНИ.
- У РАЗІ ВИНИКНЕННЯ СУПЕРЕЧНОСТЕЙ МІЖ ЦИМ ДОКУМЕНТОМ ТА ЧИННИМ ЗАКОНОДАВСТВОМ, ПРІОРИТЕТ МАЄ ОСТАННЄ.