



## MAZi – zdalny dostęp do rejestratorów i kamer przez chmurę

wersja 1.2

Instrukcja opisuje jak skonfigurować rejestrator lub kamerę by było możliwe połączenie z nimi przez Internet za pomocą przez chmurę (np. połączenie przez sieci 3G/LTE ).

### Ważne informacje:

- ze względu na specyfikę połączenia przez sieci komórkowe 3G/LTE jego prędkość może się znacznie zmieniać w czasie, co może powodować problemy z jakością połączenia, jego stabilnością itp. które nie są związane z jakością pracy serwera chmury czy rejestratora
- należy pamiętać że połączenie przez chmurę jest realizowane przez serwery pośredniczące których obciążenie może się zmieniać w czasie
- wymaganą przeglądarką jest Internet Explorer w wersji 8.0 lub wyższej
- na jakość połączenia z rejestratorem ma wpływ jakość (m. in. szybkość uploadu w miejscu podłączenia rejestratora) połączenia przez Internet
- usługa dostępu przez chmurę Hicloudcam oraz usługa DDNS GuardingVision to dwie różne usługi
- usługi Hicloudcam oraz GuardingVision korzystają z tego samego klienta włączanego w *MENU* → *Ustawienia* → *Siec* → *Extranet* lub *Dostęp do platformy* o nazwie GuardingVision
- należy zwrócić uwagę że zależnie od wersji firmware'u może być konieczne nadanie kodu weryfikacyjnego
- należy zawsze stosować najnowszą dostępną wersję firmware'u oraz programu *Guarding Vision* które znajdziesz na <http://materialy.gde.pl/do-pobrania>

Wszelkie uwagi i poprawki prosimy zgłaszać na adres: [cctv@gde.pl](mailto:cctv@gde.pl)

### 1. Zdalny dostęp do rejestratorów i kamer MAZi przez chmurę

Dzięki chmurze zdalny dostęp do rejestratora z przeglądarki oraz klienta mobilnego jest bardzo prosty, a co najważniejsze, pozwala na zdalny dostęp przez sieci LTE oraz 3G, gdzie tradycyjne sposoby połączenia z rejestratorem nie działają.

Połączenie przez chmurę działa gdy nie mamy routowalnego adresu IP albo gdy dostawca internetu blokuje połączenia przychodzące.

Należy pamiętać że jest niezbędne prawidłowe skonfigurowanie ustawień sieciowych w rejestratorze: prawidłowo wpisane adresy serwerów DNS, adres IP i maska rejestratora

Nie potrzebujemy przekierowania portów na routerze czy routowalnego adresu.

### 2. Bezpieczeństwo rejestratora lub kamery

Niezależnie od metody dostępu należy stosować podstawowe zasady bezpieczeństwa. Niestosowanie się do nich może skutkować przejęciem rejestratora przez nieuprawnione osoby.

- stosowanie skomplikowanych haseł, absolutne minimum to
  - 8 znaków oraz zastosowanie równocześnie
  - duże litery
  - małe litery
  - cyfry
  - symboli specjalnych
- porty
  - zmiana portów ze standardowych na inne, koniecznie powyżej 1024
  - nie należy używać portów o numerach kojarzącymi się z portami standardowymi np. 80 do 90, 8080, 4554
- nie udostępniamy urządzeń poprzez umieszczeniu w DMZ

- nie należy wyłączać blokowania po nieudanym logowaniu lub kilku kolejnych nieudanych logowaniach. Następną próbą logowania możliwa jest dopiero po określonym czasie, zazwyczaj 20 minut
- należy zaktualizować firmware do najnowszej dostępnej wersji

### 3. Konfiguracja połączenia za pomocą chmury Hicloudcam – przez smartfon

**Założenie konta możliwe jest przez przeglądarkę lub smartfon, możliwe jest również szybkie nawiązanie połączenia przez zeskanowanie kodu QR.**

W obu przypadkach musimy skonfigurować połączenie sieciowe w rejestratorze (punkt 3.1) oraz klienta chmury (punkt 3.2).

Kod weryfikacyjny jest także kodem szyfrowania.

#### 3.1. Konfiguracja połączenia sieciowego w rejestratorze

Konfiguracja ustawień sieci w rejestratorze jak w punkcie 5.1 *Poszczególne etapy konfiguracji - konfiguracja rejestratora*

- **w przypadku połączenia przez chmurę dla uproszczenia można włączyć klienta DHCP, wtedy pozostałe podpunkty pomijamy, sprawdzamy tylko czy router przydzielił rejestratorowi adres IP oraz serwery DNS i wykonujemy od razu**
  - punkt 3.3 – jeśli chcemy dokonać szybkiej konfiguracji za pomocą smartfona
  - punkt 3.4 – gdy chcemy założyć konto o pełnej funkcjonalności i logować się na nie z wielu urządzeń
- rejestrator musi mieć prawidłowy adres IP oraz maskę, zgodne z adresacją stosowanej w sieci do której podłączony jest rejestrator
- bezpośrednio w rejestratorze wybieramy Menu → Ustawienia → Sieć – Ogólne
- wpisujemy prawidłowy adres IPv4 oraz maskę sieci IPv4, zgodne z adresacją stosowaną w sieci do której podłączony jest rejestrator
- adres bramy domyślnej IPv4 (czyli adres portu LAN routera udostępniającego internet)
- adresy serwerów DNS preferowanego oraz alternatywnego (nie mylimy z DDNS), można wykorzystać serwery DNS Googla (8.8.8.8, 8.8.4.4), Orange (194.204.159.1, 194.204.152.34) itp.

The screenshot shows the network configuration page for a device. The left sidebar contains navigation options: Lokalnie, System, Sieć, Ustawienia podstawowe (highlighted), and Ustawienia zaawansowane. The main content area is titled 'Konfiguracja' and has sub-tabs for TCP/IP, DDNS, PPPoE, Port, and NAT. The 'TCP/IP' sub-tab is selected, and the 'Lan 1' interface is chosen. The configuration fields are as follows:

Parameter	Value
Typ NIC	10M/100M/1000M Auto
DHCP	<input type="checkbox"/>
Adres IPv4	192.168.0.206
Maska sieci IPv4	255.255.255.0
Brama dom. IPv4	192.168.0.199
Adres IPv6	fe80::bead:28ff:feae:658f
Brama IPv6	
Adres MAC	bc:ad:28:ae:65:8f
MTU	1500

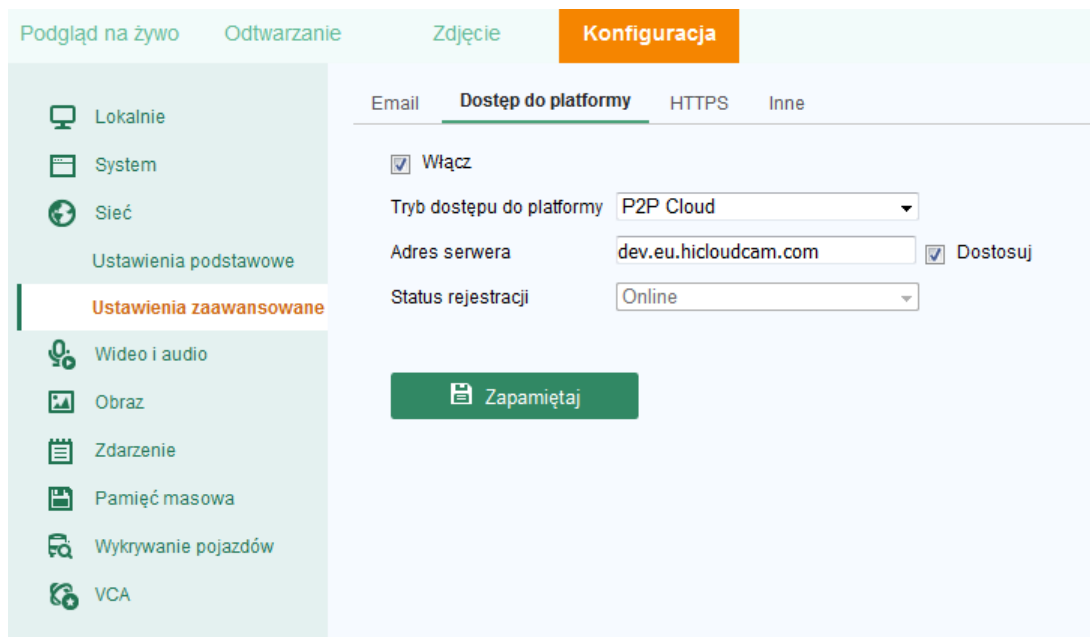
Under the 'Serwer DNS' section:

Parameter	Value
Preferowany DNS	8.8.8.8
Alternatywny DNS	

A green 'Zapamiętaj' button is located at the bottom of the configuration area.

### 3.2. Konfiguracja klienta chmury w rejestratorze

Standardowo wystarcza włączenie dostępu do platformy, zaakceptowanie polityki prywatności, nadanie kodu weryfikacyjnego oraz sprawdzenie czy w polu *Status* ma komunikat *Online*.



Konfiguracja rejestratora.

- *MENU* → *Ustawienia* → *Sieć* → *Extranet* lub *Dostęp do platformy* – menu lokalne rejestratora lub *Konfiguracja* → *Sieć* → *Ustawienia zaawansowane* → *Dostęp do platformy* – menu przez przeglądarkę
- Włączamy chmurę. Pojawić się prośba o zaakceptowanie polityki prywatności oraz nadanie kodu weryfikacyjnego
- Tryb dostępu do platformy *P2P Cloud* lub *Guarding Vision*
- Adres serwera: pozostawiamy domyślny
- Zatwierdzamy klikając *Zapamiętaj*
- Sprawdzamy w polu *Status* czy mamy komunikat *Online*

Standardowe ustawienia:

- *Ustawienia* -> *Sieć* -> *Dostęp do platformy*
- Dostęp do platformy: *włącz*
- Typ dostępu: *P2P cloud* lub *Guarding Vision*
- Adres serwer: *dev.hicloudcam.com* lub *dev.eu.hicloudcam.com*. W nowszych firmware'ach domyślne wybrany jest serwer *dev.guardingvision.com*, *dev.eu.guardingvision.com* lub *lite.dev.eu.guardingvision.com* – nie zalecamy zmiany domyślnych ustawień
- Użytkownika: odznaczone
- Włącz szyfrowanie strumienia: odznaczone (w niektórych wersja może być włączone, można wyłączyć)

### 3.3. Konfiguracja połączenia za pomocą chmury Hicloudcam – przez smartfon w trybie gościa za pomocą kodu QR

**Najprostsza opcja to tryb gościa** – możemy dodać rejestratory, bez konieczności zakładania konta – pomijamy wtedy punkt 3.4 (Utworzenie konta na serwerze Hicloudcam oraz dodanie rejestratora). W razie potrzebny konto podstawowe można przekształcić do konta z rejestracją za pomocą e-maila lub numeru telefonu.

**W przypadku konta gościa nie ma możliwości zalogowania się na to konto z innego urządzenia, za to możliwe jest udostępnienie urządzeń innym użytkownikom – do ich własnych kont.**

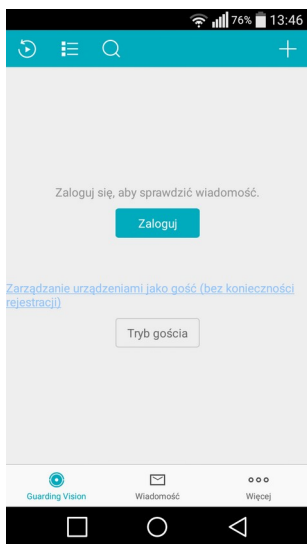
Konfiguracja smartfona:

- pobierz z program *Guarding Vision* dla *Android* lub *iOS*
- wybierz opcję *Tryb gościa*

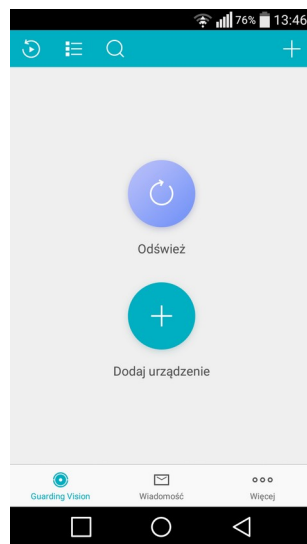
- wybierz *Dodaj urządzenie*
- zeskanuj kod QR w rejestratorze *Menu* → *Ustawienia* → *Sieć* → *Dostęp do platformy* → *kod QR* lub jeśli dany firmware nie ma opcji QR kodu to:
- w prawym górnym rogu wybierz *ikonę ołówka* i podaj numer seryjny (najprościej odczytać z dołu lub boku obudowy) oraz wprowadź kod weryfikacyjny odczytany z *Menu rejestratora* (ten który nadaliśmy podczas włączenia usługi chmury)
- zatwierdź *Dodaj*
- dodawanie zostało zakończone
- wybierz *Dalej*,
- teraz możesz nadać rejestratorowi własną nazwę
- wybierz *Zapisz*

Zostało utworzone konto gościa pozwalające na podgląd i przeglądanie nagrań. Rejestrator został do niego dodany i ze względów bezpieczeństwa (zachowanie prywatności) nie można go dodać do innego konta. Konto jest powiązane z telefonem. Jeśli chcemy przypisać rejestrator do innego konta to należy usunąć go z konta gościa.

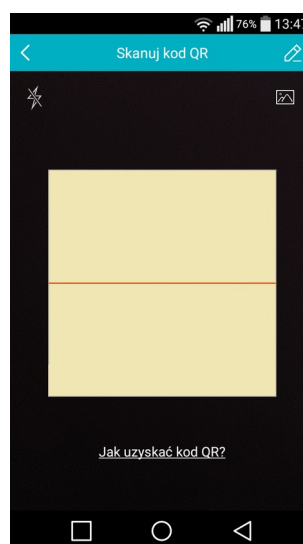
Poniżej znajdują się screeny z poszczególnych etapów dodawania rejestratora przez kod QR.



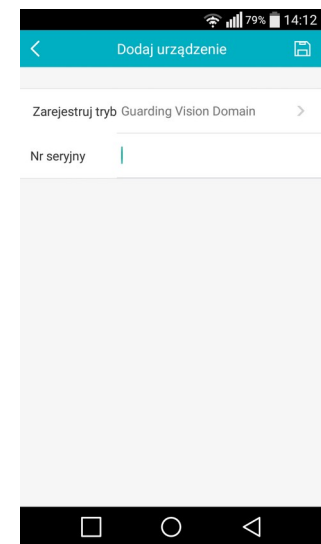
tryb gościa



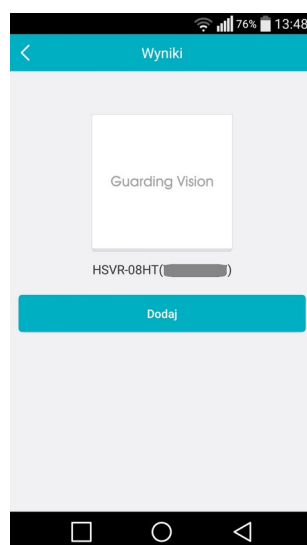
dodaj urządzenie



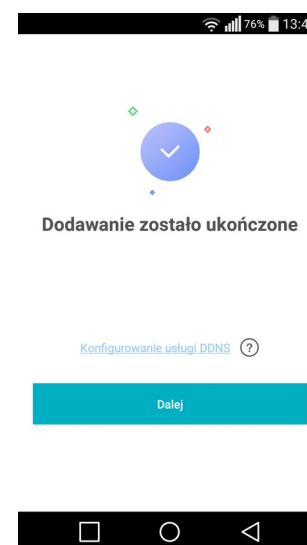
zeskanuj kod



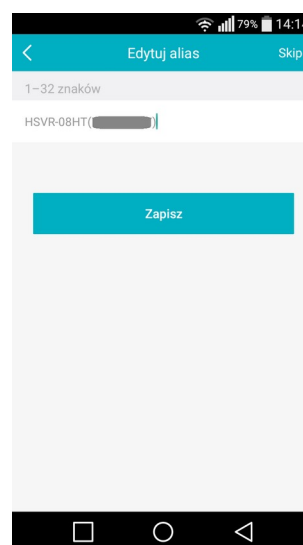
lub wpisz numer seryjny.



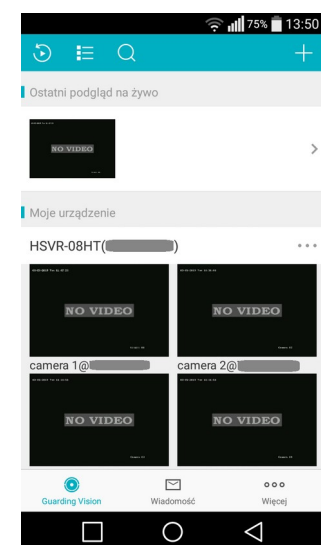
zatwierdź



zatwierdź ponownie



nadać nazwę



oglądaj

### Przekształcenie w konto pełne.

Posiadając pełne konto można logować się do niego z różnych urządzeń za pomocą loginu oraz hasła, tak

samo jak w przypadku gdy konto utworzyliśmy na komputerze przez przeglądarkę. Po rejestracji urządzenia dodane do konta gościa będą przepisane do nowego konta i będzie można nimi zarządzać z poziomu tego konta.

#### **Udostępnienie urządzeń innym użytkownikom.**

Istnieje możliwość udostępnienia urządzeń innym użytkownikom wraz przydzieleniem praw do konkretnej kamery i czynności np. przeglądania nagrań.

### **3.4. Utworzenie konta na serwerze Hicloudcam oraz dodanie rejestratora**

Dostęp i zarządzanie chmurą przez przeglądarkę Internet Explorer dla Windows wymaga wtyczki <http://www.hicloudcam.com/assets/deps/PCPlayer.exe>.

Wtyczka dostępna jest także dla komputerów z MacOS <http://hicloudcam.com/assets/deps/PCPlayer.zip>.

Założenie konta możliwe jest także z poziomu programu *Guarding Vision* na PC, Android oraz iOS (iPhone, iPad).

- Na stronie głównej <http://www.hicloudcam.com> tworzymy konto klikając w opcję *Register*
  - Możliwe jest także utworzenie konta przez program *Guarding Vision* na PC, Android oraz iOS
- Podajemy
  - User Name (nazwę użytkownika)
  - Password (hasło)
  - Confirm Password (potwierdzenie hasła)
  - Country (kraj)
  - E-mail – adres e-mail na który zostanie wysłany mail z kodem aktywacyjnym
  - Verification Code (tzw. captcha) – kod weryfikacyjny, ciąg literowo-cyfrowy widoczny po prawej stronie pola
- Po wpisaniu kodu weryfikacyjnego captcha, klikamy na dole formularza w *Next*, pojawia się okno aktywacji konta
- Sprawdzamy mail'a w poszukiwaniu maila z kodem weryfikacyjnym
- Odebrany na maila 4-cyfrowy kod aktywacyjny (ważny przez pół godziny) podajemy w oknie aktywacji konta
- W kolejnym kroku dodajemy rejestrator *Homepage* → *Quick Add* i klikamy *Add now*. Można go dodać go automatycznie przez *Add Automatically* (jeśli jesteśmy w tej samej sieci LAN co rejestrator) albo ręcznie przez *Add by Serial No.* (jeśli jesteśmy pracujemy zdalnie) – wtedy należy podać numer seryjny rejestratora z naklejki na rejestratorze.
- Kolejny etap to podanie sześcioliterowego kodu weryfikacyjnego z *Menu* → *Sieć* → *Extranet* względnie *Menu* → *Konserwacja* → *Info o systemie* → *Dane urządzenia*. Odczyt kodu możliwy jest tylko bezpośrednio na rejestratorze a w przypadku najnowszych firmware'ów także z poziomu przeglądarki *Sieć* → *Ustawienia zaawansowane* → *Dostęp do platformy*.
- W przypadku braku kodu (dotyczy kamer) należy użyć kodu ABCDEF lub AAAAAA

Mając dodany rejestrator w zakładce Video Library wybieramy kamery do podglądu.

**Uwaga: Rejestrator może być przypisany tylko do jednego konta.**

## **4. Dostępne oprogramowanie**

**Uwaga: Gdy pojawi się żądanie kodu szyfrowania**

- w rejestratorze *MENU* → *Ustawienia* → *Sieć* → *Dostęp do platformy* możemy wyłączyć szyfrowanie jeśli na szyfrowaniu wideo na nie zależy
- podgląd przez przeglądarkę w opcji *Konfiguracja* → *Lokalnie* → *Klucz szyfrowania* podajemy kod weryfikacyjny
- podgląd przez aplikację *Guarding Vision* – zostaniemy poproszeni o podanie kodu
- program *Guarding Vision* na PC: pojawi się monit o podanie kodu weryfikacyjnego, można go także podać w panelu *Zarządzanie urządzeniami*, zakładka *Grupa*, gdzie zaznaczamy wybraną kamerę i klikamy *Edytuj*, w polu *Klucz kodowania* wpisujemy kod weryfikacyjny

### **4.1. Urządzenia mobilne**

Dostępne oprogramowanie pozwala na zdalny monitoring za pomocą rejestratorów analogowych HD, rejestratorów IP, kamer IP stacjonarnych a także obrotowych. Możliwe jest odtwarzanie nagrań, lokalne



nagrywanie, wykonywanie zrzutów, sterowanie kamerami PTZ oraz wyjściami alarmowymi. W przypadku braku płynności połączenia należy zmniejszyć rozdzielczość, liczbę klatek i bitrate w kamerze lub zmniejszyć jakość obrazu. Jakość i płynność połączenia zdalnego zależy od jakości łącza sieciowego i wydajności telefonu.

### **Program Guarding Vision na smartfon**

Program pozwala na połączenia przez adres IP, DDNS, DDNS Guarding Vision, MAZi DDNS a zwłaszcza przez chmurę.

Łączymy się z rejestratorem podając nazwę konta Guarding Vision i wybierając z listy urządzenie z którym chcemy się łączyć.

Wybieramy opcję Zaloguj i logujemy się danymi jak do konta Hicloudcam

Wybieramy *Zaloguj*, wpisujemy login i hasło. Opcja *Zarejestruj konto* pozwala na założenie konta Guarding Vision / Hicloudcam z poziomu programu Guarding Vision. Wybieramy rejestrator i rozpoczynamy podgląd. Po zalogowaniu możliwe jest także dodawanie urządzeń do chmury przyciskiem + na środku ekranu.

Klikając w + w prawym górnym rogu ekranu możemy dodać rejestrator zarówno wśród urządzeń on-line (muszą znajdować się w sieci lokalnej), skanując QR kod, jak i podając ich adres IP/domenowy.

Możliwe jest zeskanowanie QR kodu z ekranu rejestratora (*MENU* → *Ustawienia* → *Sieć* → *Extranet* lub *Dostęp do platformy*) lub przez wpisanie numeru seryjnego odczytanego z obudowy rejestratora. W obu przypadkach konieczne jest także wpisanie kodu weryfikacyjnego rejestratora.

Guarding Vision dostępny jest na urządzenia z systemem Android jak i iOS. Służy do łączenia za pośrednictwem usługi GuardingVision.

Można go znaleźć w Apple Store (<https://itunes.apple.com/us/app/guarding-vision/id1101697283?mt=8>) oraz w Google Play (<https://play.google.com/store/apps/details?id=com.mcu.guardingvision&hl=pl>)

### **4.2. Połączenie przez przeglądarkę**

Wymagana jest przeglądarka Internet Explorer – przez zalogowanie się na stronie <http://www.hicloudcam.com>.

- Łączymy się ze stroną <http://www.hicloudcam.com>
- Pozwalamy zainstalować wtyczki ActiveX
  - Znajdujemy się na stronie logowania gdzie podajemy login i hasło do konta które utworzyliśmy w punkcie 3.4.
  - *Homepage* – widok podstawowy
  - *Gallery* – podgląd obrazów z maksymalnie 4 kamer oraz przeglądanie nagrań
  - *Messages* – przeglądanie wiadomości alarmowych np. wywołanych detekcją ruchu
  - *System Management* – zarządzanie urządzeniami oraz udostępnianie innym użytkownikom usługi Hicloudcam naszych urządzeń.

W razie problemów z dostępem do usługi przez przeglądarkę Internet Explorer sprawdzamy (Narzędzia → Zarządzaj dodatkami) czy następujące dodatki są włączone: UpdateActiveX Control, SP7WebVideoActiveX Control oraz SafePWSBox Control.

### **4.3. Program Guarding Vision na PC**

Funkcje Guarding Vision:

- wyszukiwanie i zmianę adresów IP wszystkich urządzeń MAZi
- podgląd na żywo
- przeglądanie nagrań
- konfigurację wszystkich urządzeń MAZi
- wielopoziomowa - mapa
- praca wielomonitrowa
- tworzenie wirtualnych urządzeń składających się z wielu różnych urządzeń fizycznych
- program umożliwia połączenie z rejestratorem przez adres IP, adres domenowy, z użyciem DDNS a także przez chmurę

Łączymy się z rejestratorem podając:

- nazwę konta Guarding Vision i wybierając z listy urządzenie z którym chcemy się łączyć
- po zalogowaniu widzimy wszystkie urządzenia dodane do naszego konta, można także dodawać kolejne oraz je usuwać

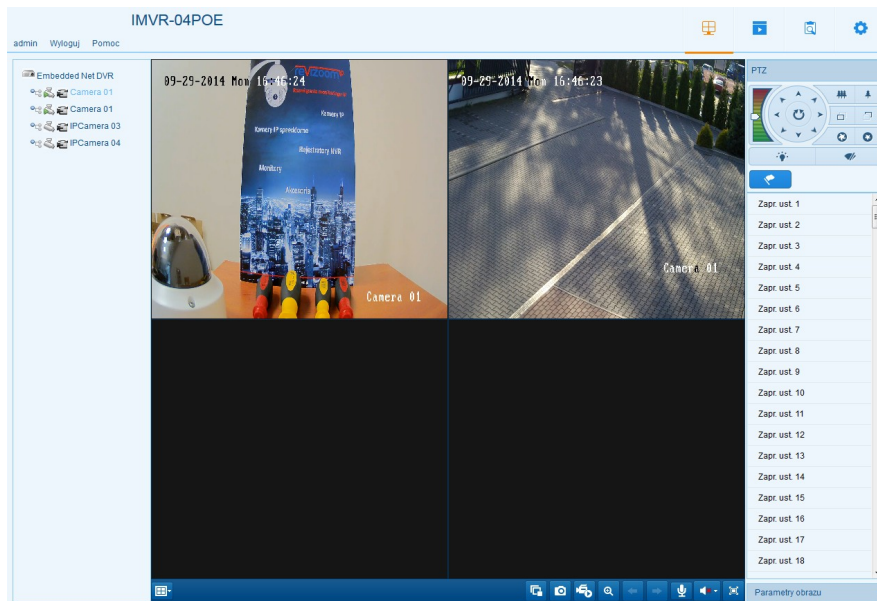
- szczególną cechą programu Guarding Vision jest opcja *Zdalna konfiguracja* pozwalająca na zarządzanie ustawieniami rejestratora poprzez chmurę
- opcja Rejestruj pozwala na założenie konta Hicloudcam z poziomu programu

## 5. Najczęściej spotykane pytania i problemy

### Dostęp przez przeglądarki

Wymaganą przeglądarką jest Internet Explorer na Windows oraz Safari na MacOS.

W systemie Windows wymagane jest zainstalowanie wtyczki WebComponents (połączenie lokalne przez adres IP) oraz UpdateActiveX Control, SP7WebVideoActiveX Control oraz SafePWSBox Control (połączenie przez chmurę) – powinno nastąpić to automatycznie w chwili pierwszego połączenia z rejestratorem.



W przypadku systemu MacOS i przeglądarki Safari wtyczkę należy zainstalować ręcznie, można ją pobrać z [http://www.gde.pl/Do\\_pobrania/](http://www.gde.pl/Do_pobrania/) - dział Rozwiązania IP MAZi.

Łączymy się z rejestratorem podając adres i port HTTP np. <http://192.0.0.64:80>

### Najczęściej spotykane problemy związane z dostępem przez przeglądarkę Internet Explorer

Omyłkowe używanie przeglądarki Edge zamiast Internet Explorer spowodowane podobną ikoną.

Brak podglądu lub ciągle żądanie instalacji kontrolki

- wejść w *Narzędzia -> Opcje internetowe -> zakładka Zabezpieczenia*
- wybieramy *Internet* (opcjonalnie możemy zrobić to dla *Intranetu* jeśli tam jest rejestrator, albo dodać go do *Zaufanych witryn* i tam zmodyfikować ustawienia)
- klikamy w *Poziom niestandardowy*
- tylko IE9, IE10 i wyższe – *Zezwalaj na Filtrowanie ActiveX* – wyłącz
- Wszystkie IE:
- *inicjowanie i wykonywanie skryptów kontrolek ActiveX niezaznaczonych jako bezpieczne do wykonywania* – monituj
- *pobieranie niepodpisanych kontrolek ActiveX* – monituj
- *pobieranie podpisanych kontrolek ActiveX* – monituj
- *uruchamianie kontrolek ActiveX i wtyczek* - włącz
- zapisz modyfikacje klikając OK i wyjdź z menu Zabezpieczeń.
- czasem może być potrzebne przeładowanie komputera a zawsze ponowne uruchomienie przeglądarki

Czasem może być konieczne dodanie rejestratora do Widoku zgodności. Zazwyczaj dotyczy to IE10 i wyższe.

- wejść w *Narzędzia* a następnie w *Ustawienia widoku zgodności*
- dodajemy rejestrator wpisując jego adres o ile sam się nie pojawił
- warto także zaznaczyć *Wyświetlaj witryny intranetu w widoku zgodności*
- zamykamy okno
- ponownie uruchamiamy przeglądarkę

Jeśli w dalszym ciągu nie działa podgląd w albo mamy inne problemy.

Sprawdzamy (*Narzędzia* → *Zarządzaj dodatkami*) czy następujące dodatki są włączone: *WebVideoActiveX Control* lub *HCWPWebVideoActiveX Control* (w przypadku rejestratorów IMVR-xxA oraz ADVR-xx). Łącząc się przez chmurę za pomocą serwisu <http://www.hicloudcam.com> należy mieć zainstalowane wtyczki: *UpdataActiveX Control*, *SP7WebVideoActiveX Control* oraz *SafePWSBox Control*.

Przy pierwszym uruchomieniu może pojawić się monit czy uruchomić – wybieramy *Zawsze dla wszystkich witryn*.

### Gdzie zapisują się nagrania i screeny dokonywane przez przeglądarkę?

Jeśli po dokonaniu nagrań czy archiwizacji we wskazanych katalogach nic nie ma albo wręcz nie ma samych katalogów, oznacza to że, ze względu na ustawienia zabezpieczeń, przeglądarka korzysta z wirtualnego systemu plików. Pliki w tym katalogu zazwyczaj są usuwane po zamknięciu przeglądarki.

Najprostszą metodą jest uruchamianie przeglądarki z prawami administratora (choć obniża to poziom bezpieczeństwa przeglądarki) lub wyłączenie trybu chronionego dla danej strefy Internetowej.

Można także zlokalizować ścieżkę do naszych katalogów w wirtualnym systemie plików i utworzyć do nich link np. na Pulpicie. Po wykonaniu nagrań klikamy w link i kopiujemy pliku do zwykłego katalogu np. na Pulpit.

Katalogów należy szukać w:

`C:\Users\nazwa_użytkownika\AppData\Local\Microsoft\Windows\Temporary Internet Files\Virtualized\ C:\Users\nazwa_użytkownika\katalog`

gdzie:

nazwa\_użytkownika - nasza nazwa użytkownika

katalog - jest to katalog taki jak wybraliśmy do zapisu nagrań

Ze względu na politykę bezpieczeństwa systemu Windows 10 w celu dostępu do katalogu wirtualnego nie można użyć systemowego Exploratora plików, należy zastosować inny manager plików.

### Instalacja wtyczki w MacOS

W systemie MacOS wtyczkę należy zainstalować ręcznie

- wyłączyć przeglądarkę Safari
- pobrać wtyczkę z naszej strony z działu Do pobrania
- zainstalować wtyczkę – uruchamiany pobrany plik np. `WebVideoPlugin_IMAC_V3.0.5.43_build_20160118.pkg`
- uruchamiamy przeglądarkę
- w Safari - Preferences – Security sprawdzamy czy są włączone wtyczki
- w Help - Installed Plug-ins sprawdzamy czy mamy zainstalowany webvideo-plugin
- łączymy się z rejestratorem

### W opcjach chmury Status wyświetla się jako Niepołączony

Sprawdzamy kolejno:

- czy adres rejestratora jest zgodny z pulą adresową stosowaną w sieci LAN w której on pracuje
- czy wpisano poprawny adres routera (brama domyślna, gateway) a także adresy DNS

W następnym kroku sprawdzamy połączenie rejestratora z routerem - najprostszą metodą by to sprawdzić polecenie ping.

### Komenda Ping z poziomu rejestratora:

*Konserwacja* → *Test sieci* → *Diagnostyka sieci*

W polu Adres sieciowy wpisujemy adres routera i klikamy *Test*.

W przypadku gdy połączenie jest prawidłowe wyświetla się informacja: Średnie opóźnienie 1ms, Zagubionych pakietów 0%. W przypadku łącza radiowego opóźnienie może być nieco większe rzędu kilkunastu ms.

W ten sposób możemy także sprawdzić czy istnieje połączenie rejestratora np. z kamerami IP czy routerem nawet gdy nie posiadamy dostępu do komputera.