



MAZi – zdalny dostęp do rejestratorów i kamer



wersja 2.9

Instrukcja opisuje jak skonfigurować rejestrator lub kamerę by było możliwe połączenie z nimi przez Internet za pomocą chmury lub przez adres IP/domenowy.

Ważne informacje:

- **połączenie przez chmurę Hicloudcam (połączenie przez sieci 3G/LTE) – patrz punkt 6, dostępna także możliwość szybkiego nawiązania połączenia przez kod QR**
 - należy pamiętać że połączenie przez chmurę jest realizowane przez serwer pośredniczący którego obciążenie może się zmieniać w czasie
 - 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
- **połączenie bezpośrednio przez adres IP, domenowy lub DDNS (większość dostawców stacjonarnych) – patrz punkt 5**
 - wymagany jest adres routowalny IPv4
 - w pewnych sytuacjach pomimo iż dostawca przydzielił nam adres nieroutowalny możliwe jest połączenie bezpośrednie przez przekierowanie portów na jego routerze
 - czasem dostawca przydziela adres IPv6, w takim przypadku musimy poprosić o zmianę na adres IPv4, jeśli jest to niemożliwe należy zastosować połączenie przez chmurę Hicloudcam
 - połączenie jest możliwe zarówno gdy mamy do dyspozycji adres przydzielony na stałe lub adres przydzielany dynamicznie
 - w niektórych przypadkach może być konieczne przekierowanie portów nie tylko na routerze do którego podłączony jest rejestrator, ale także i na routerze dostawcy
 - jeśli tylko jest to możliwe należy zawsze stosować połączenie bezpośrednio rejestratorem
- zalecaną przeglądarką jest Internet Explorer w wersji 8.0 lub wyższej, możliwa jest również obsługa za pomocą przeglądarki Firefox 52 ESR (wyłącznie 32-bity)
- nie jest możliwa obsługa za pomocą przeglądarek Chrome, Opera i innych
- 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, jednakże konto założone w Hicloudcam jest automatycznie aktywne także w GuardingVision i odwrotnie
- usługi Hicloudcam oraz GuardingVision korzystają z tego samego klienta włączanego w *MENU* → *Ustawienia* → *Sieć* → *Extranet* lub *Dostęp do platformy* o nazwie GuardingVision
- usługa połączenia przez chmurę dostępna jest dla następujących rejestratorów: HTVR-xx, HAVR-xx, HSVR-xx, INVR-xxAL, INVR-xxB, INVR-xxKL, INVR-xxAxx, INVR-xxK, IMVR-xxQxx oraz IMVR-xxAxx
- w przypadku rejestratorów HTVR-xx oraz IMVR-xxA może być wymagana aktualizacja firmware'u
 - po aktualizacji wymagane jest przywrócenie urządzenia do ustawień fabrycznych, po czym ponowne skonfigurowanie
 - nie należy przywracać ustawień z kopii wykonanej na starej wersji firmware'u.
- 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 VMS-A1 które znajdziesz na <http://materialy.gde.pl/do-pobrania>

Spis treści

1. Zdalny dostęp do rejestratorów MAZi
2. Wymagania by zdalny dostęp do rejestratora lub kamery był możliwy
3. Bezpieczeństwo rejestratora lub kamery
4. Konfiguracja połączenia bezpośredniego przez DDNS
5. Konfiguracja połączenia za pomocą chmury Hicloudcam
6. Najczęściej spotykane pytania i problemy

Wszelkie uwagi i poprawki prosimy zgłaszać na adres: cctv@gde.pl

1. Zdalny dostęp do rejestratorów i kamer MAZi

Dostęp do rejestratorów MAZi poprzez Internet możliwy jest na dwa sposoby.

1.1. Połączenie bezpośrednio przez adres IP, adres domenowy lub DDNS

Łączymy się podając adres IP (np. 198.122.90.2) lub adres domenowy (np. rejestrator.gde.pl).

- połączenie za pomocą adresu IP stosujemy gdy mamy do dyspozycji stały i routowalny adres IP, lub
- połączenie za pomocą adresu domenowego stosujemy gdy mamy do dyspozycji routowalny adres IP, lecz jest on przydzielany dynamicznie. Taką sytuację mamy np. w Orange przy dostępie przewodowym czy Netii. Wymaga to wykorzystania usługi DDNS świadczonej odpłatnie np. no-ip.org czy dyn.com. Dla ułatwienia rejestratory MAZi pozwalają także skorzystać z własnego darmowego serwera DDNS – HiDDNS, Guarding Vision oraz MAZi Dynamic DNS.

W obu przypadkach możemy się łączyć za pomocą

- przeglądarki (np. Internet Explorer, Firefox)
- za pomocą programu VMS-A1 (Windows, MacOS)
- klienta na urządzenia mobilne Guarding Vision (Android, iOS) – zalecany, aplikacja obecnie rozwijana, obsługująca wszystkie generacje rejestratorów, serwis Guarding Vision oraz chmurę
- klienta na urządzenia mobilne CCTV Viewer lub CCTV Viewer HD (Android, iOS) – aplikacja już nie rozwijana, kompatybilna ze starszymi rejestratorami, serwisem HiDDNS oraz chmurą

1.2. Połączenie za pomocą chmury

Usługa chmury dostępna jest dla rejestratorów INVR-xxAL, INVR-xxB, INVR-xxKL, INVR-xxK, IMVR-xxQxx, IMVR-xxAxx, HTVR-xx, HAVR-xx oraz HSVR-xx.

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, to zastosowanie chmury

Należy pamiętać że jest niezbędne prawidłowe skonfigurowanie ustawień sieciowych w rejestratorze, lecz nie potrzebujemy przekierowania portów na routerze czy routowalnego adresu.

2. Wymagania by zdalny dostęp do rejestratora lub kamery był możliwy

- prawidłowo wpisane adresy serwerów DNS, adres IP i maska rejestratora
- oraz w przypadku połączenia przez adres IP lub domenowy
- przekierowane w routerze porty HTTP, HTTPS, RTSP oraz SDK
 - prawidłowo skonfigurowany firewall w routerze, połączenia do rejestratora nie są blokowane
 - wyłączona usługa UPnP na routerze jak i w rejestratorze o ile nie korzystamy z niej świadomie
 - wyłączona funkcja DMZ w routerze
 - router musi posiadać routowalny (zewnętrzny) stały lub dynamiczny adres IP
 - jako DDNS można wykorzystać serwis www.hiddns.com lub eudev.hiddns.com dostępny bezpłatnie dla użytkowników urządzeń MAZi
 - brak blokowania połączeń przychodzących przez dostawcę internetu

3. Bezpieczeństwo rejestratora lub kamery

Niezależenie od metody dostępu należy stosować podstawowe zasady bezpieczeństwa. Niestosowanie się do nich zazwyczaj skutkuje 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 przypadkowych numerach, nie kojarzącymi się z portami standardowymi np. 80 do 90, 8080, 4554
- nie udostępnianiu urządzeń poprzez umieszczeniu w DMZ
- przekierowywanie tylko niezbędnych portów
- jeśli urządzenie posiada taką funkcję (np. nowe urządzenia MAZi) to włączamy blokowanie po nieudanym logowaniu lub kilku kolejnych nieudanych logowaniach. Następną próbą logowania możliwa jest dopiero po określonym czasie, zazwyczaj 20 minut
- aktualizacja firmware'u do najnowszej dostępnej wersji

4. Dostępne oprogramowanie

4.1. Program VMS-A1

Funkcje VMS-A1:

- wyszukiwanie i zmianę adresów IP wszystkich urządzeń MAZi
- podgląd na żywo
- przeglądanie nagrań
- konfigurację wszystkich urządzeń MAZi
- wielopoziomowa -mapa
- praca wielomonitorowa
- tworzenie wirtualnych urządzeń składających się z wielu różnych urządzeń fizycznych

Łączymy się z rejestratorem podając:

- adres IP, port SDK
- adres domenowy, port SDK
- adres domenowy DDNS, port SDK (np. MAZi DDNS)
- nazwę domeny w HiDDNS, tu nie musimy podawać portu SDK
- nazwę konta Guarding Vision i wybierając z listy urządzenie z którym chcemy się łączyć
- szczególną cechą programu VMS-A1 jest opcja *Zdalna konfiguracja* pozwalająca na zarządzanie ustawieniami rejestratora poprzez chmurę.

4.2. Urządzenia mobilne

dostępne oprogramowanie pozwala na zdalny monitoring za pomocą rejestratorów analogowych, rejestratorów IP, kamer IP stacjonarnych a także obrotowych. Możliwe jest odtwarzanie nagrań, lokalne nagrywanie, wykonywanie zrzutów, sterowanie kamerami PTZ oraz wyjściami alarmowymi. Dostęp do urządzeń jest możliwy przez sieć Wi-Fi lub 3G. Wymaga prawidłowo skonfigurowanych urządzeń sieciowych do których podłączone są urządzenia z którymi się łączymy. W przypadku braku płynność 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.

Łączymy się z rejestratorem podając:

- adres IP, port SDK
- adres domenowy, port SDK
- adres domenowy DDNS, port SDK (np. MAZi DDNS)
- nazwę domeny w HiDDNS, tu nie musimy podawać portu SDK
- nazwę konta Guarding Vision i wybierając z listy urządzenie z którym chcemy się łączyć

Program Guarding Vision

Zalecana, obecnie rozwijana, aplikacja obsługująca wszystkie generacje rejestratorów, serwis Guarding Vision oraz chmurę. Program pozwala na połączenia przez adrs IP, DDNS, DDNS Guarding Vision, MAZi DDNS, brak możliwości połączenia przez nierozwijany HiDDNS.

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>)

CCTV Viewer oraz CCTV Viewer HD

Aplikacja już nie rozwijana, kompatybilna ze rejestratorami starszymi rejestratorami, serwisem HiDDNS oraz chmurę. Brak możliwości połączenia przez usługę Guarding Vision.

CCTV Viewer – wersja dla telefonów.

Można go znaleźć w Apple Store (<https://itunes.apple.com/us/app/cctv-viewer/id680436764?mt=8>) oraz na naszej stronie <https://www.gde.pl/do-pobrania> w dziale *MAZi Security (firmware'y, oprogramowanie)*.

CCTV Viewer HD – wersja zoptymalizowana dla tabletów dostępna w Apple Store (<https://itunes.apple.com/us/app/cctv-viewer-hd/id680437675?mt=8>) oraz na naszej stronie <https://www.gde.pl/do-pobrania> w dziale *MAZi Security (firmware'y, oprogramowanie)*.

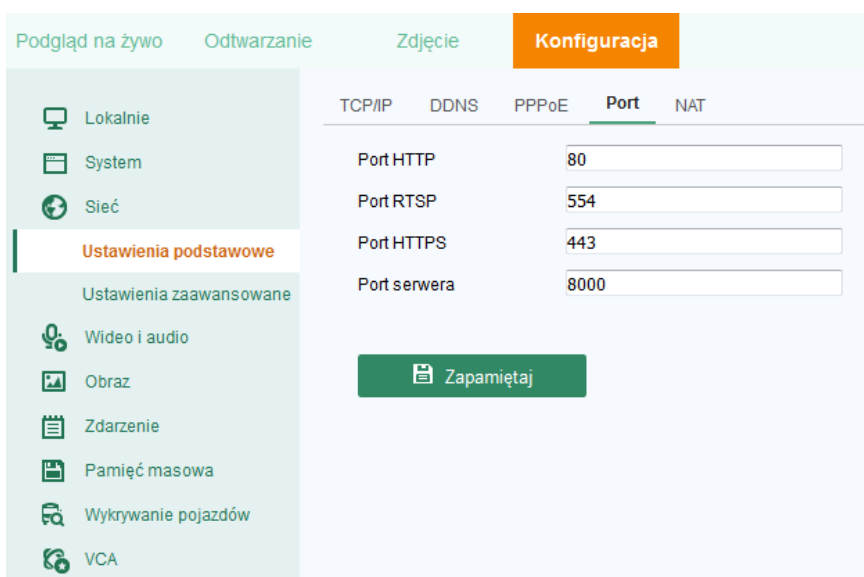
CCTV Viewer jest dostępny dla systemu iOS (iPhone, iPad) w wersji iOS 4.3 lub wyższej a także dla systemu Android (smartfony, tablety) w wersji 2.3.3 lub wyższej. Obsługiwana rozdzielczość 480*800, 480*854, 960*540, 1280*720, 800*1280 or 1920*1080.

5. Konfiguracja połączenia bezpośredniego przez DDNS

Punkt 5.1 wykonujemy zawsze, niezależnie od wybranego rodzaju połączenia przez adres IP lub adres domenowy.

5.1. Poszczególne etapy konfiguracji:

- konfiguracja rejestratora
 - łącząc się przez przeglądarkę, wchodzimy w zakładkę *Konfiguracja* → *Sieć* → *Ustawienia podstawowe* → *TCP/IP* lub
 - 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.
 - jeśli mamy adres dostępowy do Internetu przydzielany dynamicznie to włączamy klienta DDNS w *Konfiguracja* → *Sieć* → *Ustawienia podstawowe* → *DDNS* (przez przeglądarkę) lub *Menu* → *Ustawienia* → *Sieć* → *Ogólne*
 - konfigurujemy klienta zgodnie z opisem w kolejnych punktach



- jako DDNS można wykorzystać usługi:
 - www.hiddns.com lub eudev.hiddns.com dostępne bezpłatnie dla użytkowników urządzeń MAZI
 - maziddns.com dostępny bezpłatnie (w okresie promocyjnym) dla użytkowników urządzeń MAZI
 - guardingvision.com
- następnie konfigurujemy router
 - przekierowujemy na routerze porty HTTP, HTTPS, RTSP oraz SDK
 - domyślne wartości portów HTTP – 80, HTTPS – 443, RTSP – 554 oraz SDK – 8000
 - zalecamy ich zmianę na niestandardowe w ustawieniach rejestratora (przez przeglądarkę *Konfiguracja* → *Sieć* → *Ustawienia podstawowe* → *Port* lub bezpośrednio *Menu* → *Ustawienia* → *Sieć* → *Więcej ustawień*) albo możemy zrobić translację portów w regułach przekierowania tworzonych na routerze
 - sprawdzamy czy firewall w routerze jest prawidłowo skonfigurowany i pozwala na połączenia przychodzące
 - sprawdzamy czy wyłączona jest usługa UPnP na routerze jak i w rejestratorze (*Konfiguracja* → *Sieć* → *Ustawienia podstawowe* → *NAT*) o ile nie korzystamy z niej świadomie
- sprawdzamy czy wyłączona jest funkcja DMZ w routerze
- router musi posiadać routowalny (zewnętrzny) stały lub dynamiczny adres IP
- sprawdzamy czy nasz rejestrator ma odblokowany dostęp do Internetu na routerze – bywa że administrator routera domyślnie blokuje dostęp do Internetu
- sprawdzamy u dostawcy Internetu czy nie blokuje połączeń przychodzących

The screenshot shows the 'Konfiguracja' (Configuration) tab in the MAZi interface. The left sidebar contains navigation options: 'Lokalnie', 'System', 'Sieć', 'Ustawienia podstawowe' (highlighted), 'Ustawienia zaawansowane', 'Wideo i audio', 'Obraz', 'Zdarzenie', 'Pamięć masowa', 'Wykrywanie pojazdów', and 'VCA'. The main area is titled 'Konfiguracja' and has sub-tabs for 'TCP/IP', 'DDNS', 'PPPoE', 'Port', and 'NAT'. Under 'TCP/IP', 'Lan 1' is selected. The configuration fields are as follows:

Typ NIC	10M/100M/1000M Auto
<input type="checkbox"/> DHCP	
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

Below these fields is a 'Serwer DNS' section with the following settings:

Preferowany DNS	8.8.8.8
Alternatywny DNS	

A 'Zapamiętaj' (Save) button is located at the bottom of the configuration area.

5.2. Konfiguracja usługi MAZi Dynamic DNS

Używając MAZi DDNS łączy się z rejestratorem tak jak za pomocą adresu domenowego.

Zarządzanie kontem MAZi DDNS.

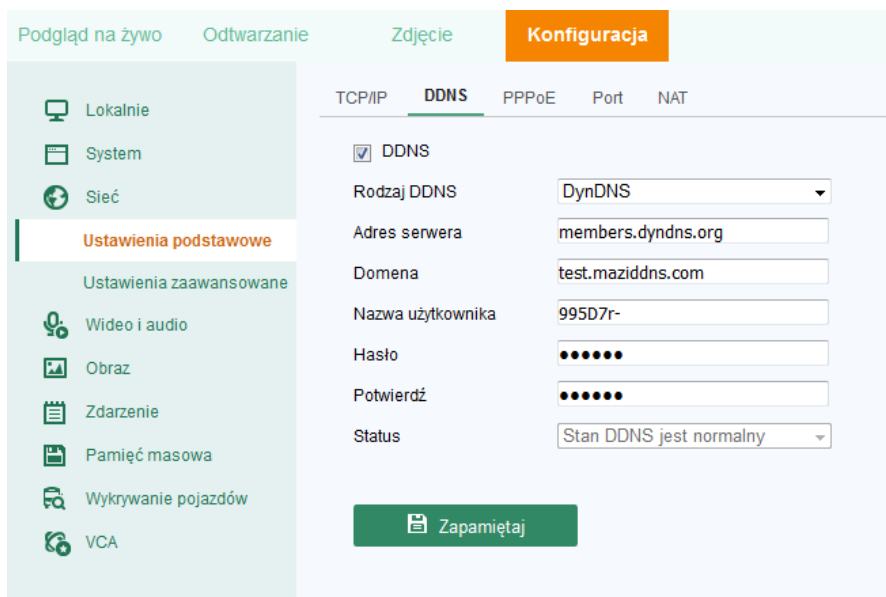
- W pierwszej kolejności należy założyć konto w serwisie www.maziddns.com
- Następnie dodajemy domenę podając jej nazwę (*Domain*), adres IP (*Ip Address*) rejestratora – adres odczytany np. za pomocą strony www.myip.com, port HTTP (*HTTP Port*) rejestratora – port musi być przekierowany na routerze, nazwę użytkownika (*Username*) oraz dwa razy podajemy hasło (*Password*) które musi mieć co najmniej 8 znaków, muszą wystąpić łącznie litery małe i duże, liczby
- Zatwierdzamy
- Dane domeny wykorzystujemy podczas konfiguracji DDNS w rejestratorze

Podawany adres IP potrzebny jest do sprawdzenia czy urządzenie które będzie korzystało z usług jest urządzeniem MAZi. Jeśli urządzenie MAZi nie zostanie wykryte, nie będzie się dało zapisać ustawień.

Konfiguracja rejestratora.

- *MENU* -> *Ustawienia* -> *Sieć* -> *DDNS* – menu lokalne rejestratora lub *Konfiguracja* → *Sieć* → *Ustawienia podstawowe* → *DDNS* – menu przez przeglądarkę
- Włączmy DDNS
- Wybieramy Rodzaj DDNS: DynDNS
- Adres serwera: members.dyndns.org
- Nazwa domeny DVR: domena.maziddns.com
- Nazwa użytkownika: jak podane przy dodawaniu domeny w panelu zarządzania na stronie maziddns.com
- Hasło: jak podane przy dodawaniu domeny w panelu zarządzania na stronie maziddns.com

Uwaga: login i hasło hosta to nie to samo co login i hasło logowania do panelu zarządzania maziddns.com.



Połączenie przez przeglądarkę

Jeśli stworzono host o nazwie "gde.maziddns.com" to przez przeglądarkę łączymy się wpisując http://gde.maziddns.com:port_http.

Połączenie przez CCTV Viewer

W przypadku CCTV Viewer dodajemy *Urządzenie* → *Dodaj urządzenie* → *Ręczne dodawanie* → wybieramy *IP/Domain* i podajemy adres "gde.maziddns.com" oraz port SDK np. 8000.

Połączenie przez VMS-A1

W przypadku programu VMS-A1 – przez *Zarządzanie urządzeniami* → *Serwer* → *Dodanie urządzenia* → *IP/Domena* oraz port SDK np. 8000.

Połączenie przez Guarding Vision

W programie klikamy w + w prawym górnym rogu ekranu możemy dodać rejestrator wśród urządzeń on-line (muszą znajdować się w sieci lokalnej), jak i podając ich adres IP/domenowy.

5.3. Usługa GuardingVision

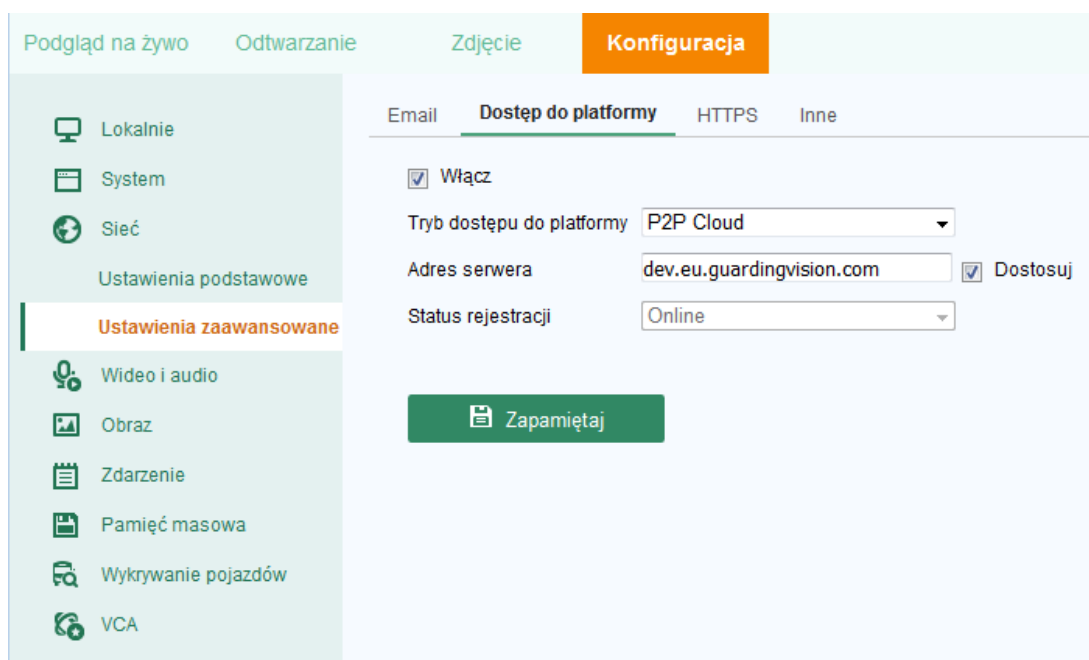
GuardingVision to usługa DDNS. Jeśli szukasz dostępu przez chmurę – patrz punkt 6 chmura Hicloudcam.

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. Może pojawić się prośba o nadanie kodu weryfikacyjnego.
- Tryb dostępu: P2P Cloud lub Guarding Vision
- Adres serwera: pozostawiamy domyślny adres dev.guardingvision.com lub dev.eu.guardingvision.com
- 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.guardingvision.com
- Użytkownika: odznaczone
- Włącz szyfrowanie strumienia: odznaczone



Następny krok to utworzenie konta.

- Jeśli mamy utworzone konto w usłudze Hicloudcam możemy wykorzystać istniejące konto i dane logowania. W przeciwnym przypadku musimy utworzyć nowe konto
- Tworzymy konto przez opcję *Register* na stronie głównej <https://www.guardingvision.com>.
- Podajemy adres e-mail na który zostanie wysłany mail z kodem aktywacyjnym.
- Po wpisaniu kodu weryfikacyjnego na dole formularza klikamy *Next*
- Odebrany na maila 4-cyfrowy kod aktywacyjny (ważny przez pół godziny) podajemy w oknie aktywacji konta, które wyświetla się po kliknięciu *Next*. Kod musimy wprowadzić w ciągu pół godziny
- W kolejnym kroku dodajemy rejestrator. Można dodać go przez *Add* – należy podać numer seryjny rejestratora z naklejki na rejestratorze oraz sześcioliterowy kod weryfikacyjny z *Menu* → *Sieć* → *Extranet* lub *Dostęp do Platformy* 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*.
- Rejestrator ma domyślną nazwę domenową taką samą jak numer seryjny rejestratora, którą przyciskiem *Edit* można zmienić
- Zalecamy opcję UPnP Mode zmienić na *Manual*, i wtedy ustawić port HTTP oraz SDK rejestratora (taki jaki jest przekierowany na routerze)

Należy pamiętać że jest niezbędne prawidłowe skonfigurowanie ustawień sieciowych rejestratora.

Połączenie przez przeglądarkę

Logujemy się na stronie <https://www.guardingvision.com>, w zakładce *Device Management*

- klikamy w pole IP/port by połączyć się z rejestratorem
- adres możemy także skopiować adres klikając w ikonę *Copy* (po prawej stronie na liście rejestratorów) i wklejając go w pole adresowe przeglądarki, adres tworzony jest wg schematu: <https://www.guardingvision.com/domena>, może pojawić się strona logowania do serwisu Guarding Vision, logujemy się do niego, po czym automatycznie pojawi się strona logowania naszego urządzenia

Połączenie przez VMS-A1

Za pomocą programu VMS-A1 (Windows) – przez *Zarządzanie urządzeniami* → *Serwer* → *Dodaj nowy typ urządzenia* → *P2P CloudUrząd.* Następnie logujemy się danymi do konta GuardingVision

Połączenie przez Guarding Vision

Wybieramy opcję *Zaloguj* i logujemy się danymi jak do konta GuardingVision. Wybierając opcję *GuardingVision* (pasek menu na dole) uzyskujemy dostęp do rejestratora za pośrednictwem chmury i przekierowane portów nie jest konieczne. Klikając w + w prawym górnym rogu ekranu możemy dodać kolejny rejestrator zarówno wśród urządzeń on-line (muszą znajdować się w sieci lokalnej), skanując QR kod jak i wpisując numer seryjny.

Uwaga: Rejestrator może być przypisany tylko do jednego konta, lecz jest możliwość udostępniania go innym

użytkownikom – ikona *Share* (po prawej stronie na liście rejestratorów).

Uwaga: W przypadku połączenia za pomocą przeglądarki możemy uzyskać błąd szyfrowania.

W takiej sytuacji bezpośrednio w rejestratorze *MENU* → *Ustawienia* → *Sieć* → *Dostęp do platformy* wyłączamy szyfrowanie lub przez przeglądarkę *Konfiguracja* → *Lokalnie* → *Klucz szyfrowania* podajemy kod weryfikacyjny.

6. Konfiguracja połączenia za pomocą chmury Hicloudcam

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 6.1) oraz klienta chmury (punkt 6.2).

Kod weryfikacyjny jest także kodem szyfrowania.

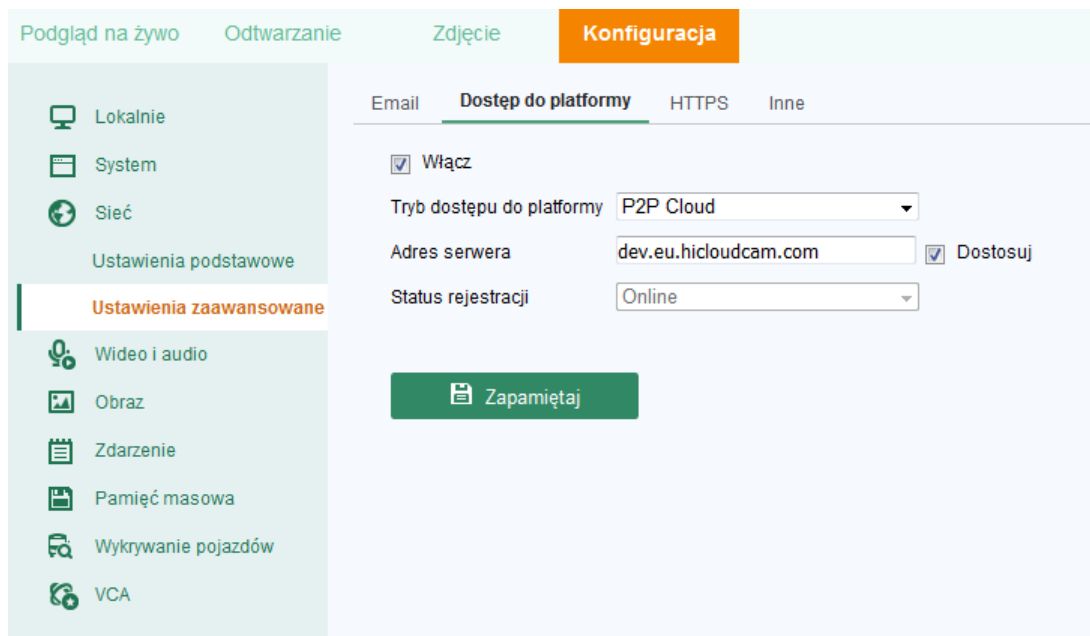
6.1. Konfiguracja połączenia sieciowego w rejestratorze

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 punkty pomijamy, sprawdzamy tylko czy router przydzielił rejestratorowi adres IP oraz serwery DNS
- rejestrator musi mieć prawidłowy adres IP oraz maskę, zgodne z adresacją stosowanej w sieci do której podłączony jest rejestrator
- podany adres bramy sieciowej (portu LAN routera udostępniającego internet)
- prawidłowo wpisane adresy serwerów DNS (nie mylimy z DDNS) dostarczone przez dostawcę Internetu, można także wykorzystać serwery DNS Googla (8.8.8.8, 8.8.4.4), Orange (194.204.159.1, 194.204.152.34) i inne
- sprawdzamy czy nasz rejestrator ma odblokowany dostęp do Internetu na routerze – bywa że administrator routera domyślnie blokuje dostęp do Internetu

6.2. Konfiguracja klienta chmury w rejestratorze

Zazwyczaj 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. Może pojawić się prośba o nadanie kodu weryfikacyjnego.
- Tryb dostępu do platformy *P2P Cloud* lub *Guarding Vision*
- Adres serwera: pozostawiamy domyślny adres *dev.hicloudcam.com* lub *dev.eu.hicloudcam.com*. W nowszych firmware'ach domyślne wybrany jest serwer *dev.guardingvision.com* lub *dev.eu.guardingvision.com*

- 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.guardingvision.com*
- Użytkownika: odznaczone
- Włącz szyfrowanie strumienia: odznaczone (w niektórych wersja może być włączone)

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

Najprostsza opcja to tryb gościa – w tym trybie używamy podstawowego konta do którego możemy dodać rejestratory, bez konieczności rejestracji – pomijamy wtedy punkt 6.4.

W razie potrzeby konto podstawowe można przekształcić do konta z rejestracją za pomocą e-maila lub numeru telefonu. Nie ma możliwości zalogowania się na to konto z innego urządzenia, za to możliwe jest udostępnienie urządzeń innym użytkownikom.

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 otwórka* i podaj numer seryjny (najprościej odczytać z dołu lub boku obudowy) oraz wprowadź kod weryfikacyjny odczytany z *Menu rejestratora*
- zatwierdź *Dodaj*
- dodawanie zostało zakończone
- wybierz *Dalej*,
- teraz możesz nadać rejestratorowi własną nazwę
- wybierz *Zapisz*

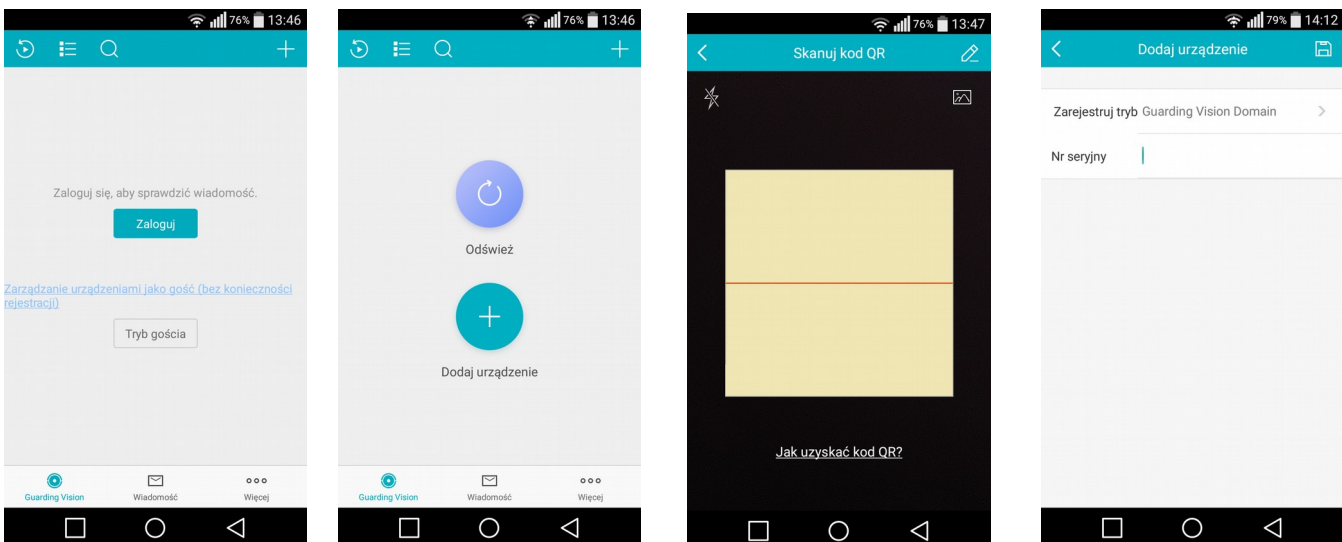
Zostało utworzone uproszczone konto pozwalające na podgląd i przeglądanie nagrań. Rejestrator został do niego dodany i nie można go dodać do innego konta.

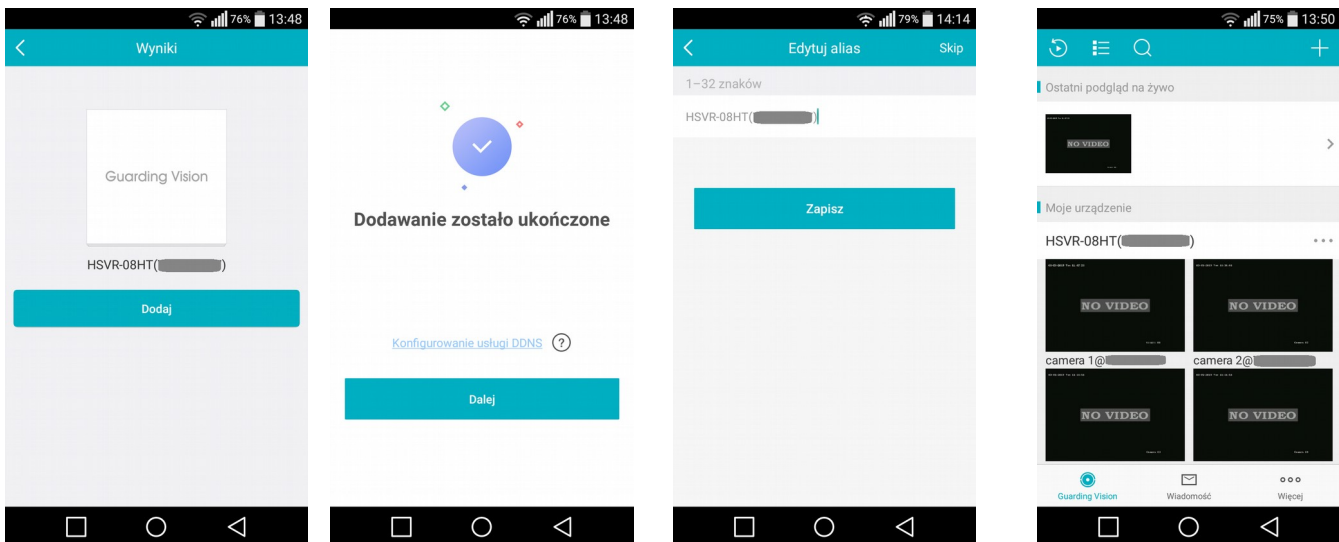
Konto jest powiązane z telefonem. Jeśli chcemy przypisać rejestrator do innego konta to należy usunąć go z konta gościa.

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.

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





Udostępnienie urządzeń innym użytkownikom.

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

6.4. Utworzenie konta na serwerze Hicloudcam

Dostęp i zarządzanie chmurą przez przeglądarkę Firefox oraz 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>.

- Na stronie głównej <http://www.hicloudcam.com> tworzymy konto klikając w opcję *Register*
 - Opcjonalnie możliwe jest także utworzenie konta przez program CCTV Viewer oraz VMS-A1.
- 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.

W przypadku gdy nie wiemy do jakiego konta jest on przypisany należy skontaktować z GDE Polska.

Uwaga: W przypadku połączenia za pomocą przeglądarki możemy uzyskać błąd szyfrowania.

W takiej sytuacji bezpośrednio w rejestratorze *MENU* → *Ustawienia* → *Sieć* → *Dostęp do platformy* możemy wyłączyć szyfrowanie lub gdy łączymy się przez przeglądarkę w opcji *Konfiguracja* → *Lokalnie* → *Klucz szyfrowania* podajemy kod weryfikacyjny, przez aplikację Guarding Vision – zostaniemy poproszeni o podanie kodu, w przypadku programu VMS-A1 także 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.

6.5. Dostępne metody połączenie przez chmurę

Połączenie przez przeglądarkę

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

Łączymy się ze stroną <http://www.hicloudcam.com>.

Znajdujemy się na stronie logowania gdzie podajemy login i hasło do konta które utworzyliśmy w punkcie 6.2.

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.

W przypadku Firefox'a (obsługa do wersji 52ESR 32-bity) należy sprawdzić czy następujące wtyczki są zaznaczone (opcja Narzędzi → Dodatki) jako Zawsze aktywuj: Web Update, Web Safe Box oraz ShiPin7 Web Player.

Połączenie przez CCTV Viewer

Wybieramy opcję Cloud P2P i logujemy się danymi jak do konta Hicloudcam.

Wybieramy w menu opcję *Cloud P2P*, wpisujemy login i hasło. Opcja *Rejestruj* pozwala na założenie konta Hicloudcam z poziomu programu CCTV Viewer. Wybieramy rejestrator i rozpoczynamy podgląd. Po zalogowaniu możliwe jest także dodawanie urządzeń do chmury przyciskiem +. 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. Przełączenie trybu wprowadzania następuje przyciskiem w prawym górnym rogu ekranu lub przez powrót wstecz z okna wpisywania numeru seryjnego i powtórne kliknięcie przycisku +.

Połączenie przez VMS-A1

Wymaga to zalogowania do konta w chmurze: *Zarządzanie urządzeniami* → *Serwer* → *Dodaj nowy typ urządzenia* → *P2P CloudUrządź* lub *Guarding VisionUrządź* (zależnie od wersji programu). Następnie logujemy się danymi do konta Hicloudcam.

Otwieramy zakładkę *Zarządzanie urządzeniami* → *Urządź* → *Dodaj nowy typ urządzenia*, wybieramy *Guarding VisionUrządź* i zatwierdzamy. Następnie klikamy w *Guarding VisionUrządź* i logujemy się do naszego konta. Opcja *Rejestruj* pozwala na założenie konta Hicloudcam z poziomu programu VMS-A1. Po zalogowaniu widzimy wszystkie urządzenia, możemy także dodać kolejne korzystając z opcji *Dodanie urządź.*, które jest możliwe po podaniu numeru seryjnego oraz kodu weryfikacyjnego.

Szczególną cechą programu VMS-A1 jest opcja *Zdalna konfigur.* pozwalająca na zarządzanie ustawieniami rejestratora poprzez chmurę.

Połączenie przez Guarding Vision

klienta na urządzenia mobilne Guarding Vision (Android, iOS) – 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.

7. Najczęściej spotykane pytania i problemy

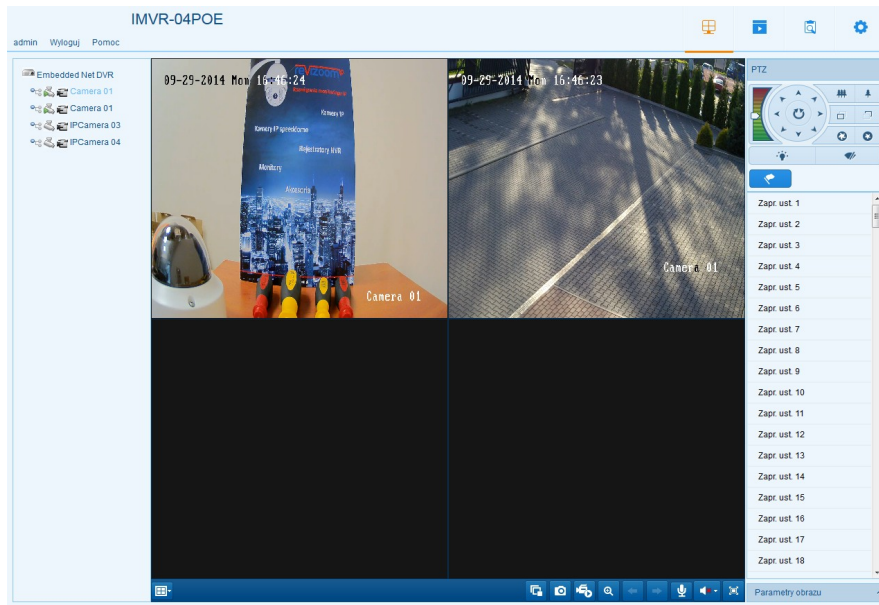
Dostęp przez przeglądarki

Zalecana przeglądarką jest Internet Explorer na Windows oraz Safari na MacOS. Z ograniczeniami konfiguracja rejestratora oraz podgląd możliwy jest także przez Mozilla Firefox.

W systemie Windows wymagane jest zainstalowanie wtyczki WebComponents – powinno nastąpić to automatycznie w chwili pierwszego połączenia z rejestratorem.

Microsoft Edge, Google Chrome i Opera nie obsługują zarówno wtyczek NPAPI jak i kontrolek ActiveX, dlatego nie można

ich wykorzystywać do konfiguracji rejestratora oraz podglądu.



Wtyczki NPAPI nie działają w Chrome w wersji 42 lub nowszej. W przypadku Chrome do wersji 45 można włączyć obsługę NPAPI. Włączamy Chrome, na pasku adresu wpisujemy `chrome://flags/#enable-npapi`, a następnie klikamy link *Włącz interfejs NPAPI*. Teraz klikamy przycisk *Uruchom ponownie teraz*.

W przypadku systemu MacOS i przeglądarki Safari wtyczkę należy zainstalować ręcznie, można ją pobrać z 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>

Firefox od wersji 52 – koniec obsługi wtyczek NPAPI

Wraz tą wersją zaprzestano obsługi wtyczek NPAPI. Wtyczki NPAPI (poza Adobe Flash, wymaganą przez rejestratory MAZI serii S oraz kamery ReviZOOM) przestały działać.

Nie działają WebComponent, HCWPWebComponent (wymagane przez kamery IDH, IWH, IBH, IMH, IFH, ICH oraz rejestratory MAZI z wyjątkiem serii S).

Rozwiązanie 1:

Zainstalować Firefoxa 52 ESR w wersji 32-bitowej <https://download.mozilla.org/?product=firefox-52.0esr-SSL&os=win&lang=pl>.

Instalacja przejmuje ustawienia z istniejącej wersji. Wersja 32-bitowa działa z Windows 32-bity oraz 64-bity. Wersja 64-bitowa ma możliwość pracy z tylko Adobe Flash oraz Microsoft Silverlight, inne są zablokowane i dlatego nie można jej zastosować.

Firefox 52 ESR pozwoli na korzystanie z istniejących wtyczek do początku 2018 roku. Jeśli po zainstalowaniu Firefoxa 52 ESR wtyczki dalej nie działają, należy usunąć cały profil użytkownika, uprzednio eksportując zakładki i inne ustawienia.

Rozwiązanie 2:

Istnieje możliwość włączenia obsługi wtyczek innych niż Adobe Flash także w Firefox 52. Ta opcja może być w każdej chwili zablokowana przez deweloperów Firefoxa. Jeśli nie zadziała należy usunąć profil użytkownika programu Firefox (`C:\Users\NazwaUzytkownika\AppData\Roaming\Mozilla\Firefox\Profiles`) i zainstalować wersję ESR.

- w nowej zakładce wpisujemy: `about:config`
- klikamy prawym klawiszem myszy, wybieramy opcję *Dodaj ustawienie typu*, a następnie *Wartość logiczna (Boolean)*
- pojawi się okno w którym wpisujemy `plugin.load_flash_only`
- pojawi się kolejne okno w którym ustawiamy wartość `false`

Firefox w wersji podstawowej, ze względu na utrzymaną obsługę wtyczki Adobe Flash, działa dalej z rejestratorami serii S (INVR-xxS, IMVR-xxS) oraz kamerami ReviZOOM.

Najczęściej spotykane problemy związane z dostępem przez przeglądarkę Firefox

Brak podglądu lub ciągle żądanie instalacji lub uruchomienia wtyczki.

W razie problemów z dostępem do usługi przez przeglądarkę, w przypadku Firefox'a należy sprawdzić czy następujące wtyczki są zaznaczone (opcja *Narzędzi* -> *Dodatki*) jako *Zawsze aktywuj: Web Components* – wszystkie obecnie sprzedawane rejestratory. W przypadku rejestratorów ADVR-xxxx oraz IMVR/INVR-04/08A może to być wtyczka *HCWP Web Components*.

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* – wszystkie obecnie sprzedawane rejestratory. W przypadku rejestratorów ADVR-xxxx oraz IMVR/INVR-04/08A może to być wtyczka *HCWPWebVideoActiveX Control*.

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

Usunięcie wtyczki w Windows

W razie dalszych problemów można usunąć wtyczkę ręcznie i ją ponownie zainstalować.

- wyłączyć wszystkie przeglądarki np. Firefox, Internet Explorer
- skasować *C:\Program Files\Web Components* lub w przypadku starszych rejestratorów *C:\Program Files\HCWP Web Components*
- włączyć przeglądarkę, połączyć się rejestratorem, pobrać wtyczkę
- wyłączyć przeglądarki
- zainstalować wtyczkę, opcjonalnie zainstalować wtyczkę z załącznika bez pobierania z rejestratora
- włączyć przeglądarki

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).

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 Pulpicie.

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)

W następnym kroku sprawdzamy połączenie rejestratora z routerem.

Najprostszą metodą by to sprawdzić polecenie ping.

Brak połączenia z rejestratorem pomimo przekierowanych portów

Sprawdzamy kolejno:

- czy nasz router nie blokuje połączeń przychodzących ze względu na ustawienia funkcji *Firewall*
- czy dostawca nie blokuje portów
- czy nie jest konieczne przekierowanie portów na jego routerze, prosimy o przekierowanie tych samych portów co na naszym
- czy router nie pracuje z adresacją IPv6, prosimy o przełączenie naszego routera na adresację IPv4

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

Przykład konfiguracji ustawień sieciowych w rejestratorze

Chcemy prawidłowo skonfigurować ustawienia sieciowe w rejestratorze MAZi. W instrukcji „MAZi – zdalny dostęp przez DDNS i chmurę v1.1 PL” w punkcie 4.1 opisano gdzie wpisujemy dane sieci.

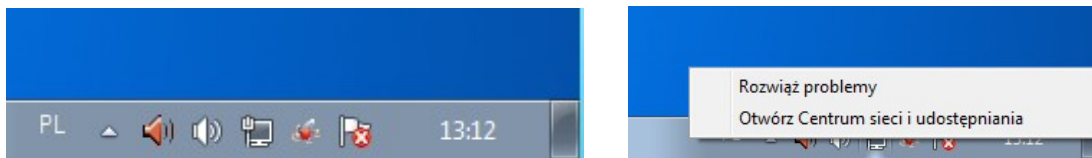
Co musimy znać:

- adres IPv4 jaki planujemy przydzielić rejestratorowi
- maskę sieci IPv4 rejestratorach
- adres bramy domyślnej IPv4 (czyli adres portu LAN routera udostępniającego internet)
- adresy serwerów DNS preferowanego oraz alternatywnego

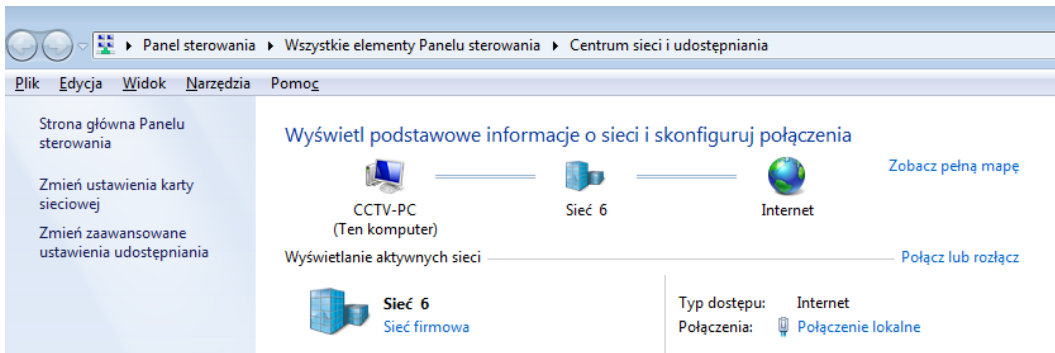
Serwery DNS - można wykorzystać serwery DNS Googla (8.8.8.8, 8.8.4.4), Orange (194.204.159.1, 194.204.152.34), naszego dostawcy Internetu albo adresy używane w naszej sieci LAN.

Przydzieleniu ustawień sieciowych rejestratora dokonuje administrator sieci. Możemy także dokonać tego sami. Aby przydzielić adres, maskę i poznać adres routera najprościej sprawdzić ustawienia dowolnego komputera pracującego w naszej sieci.

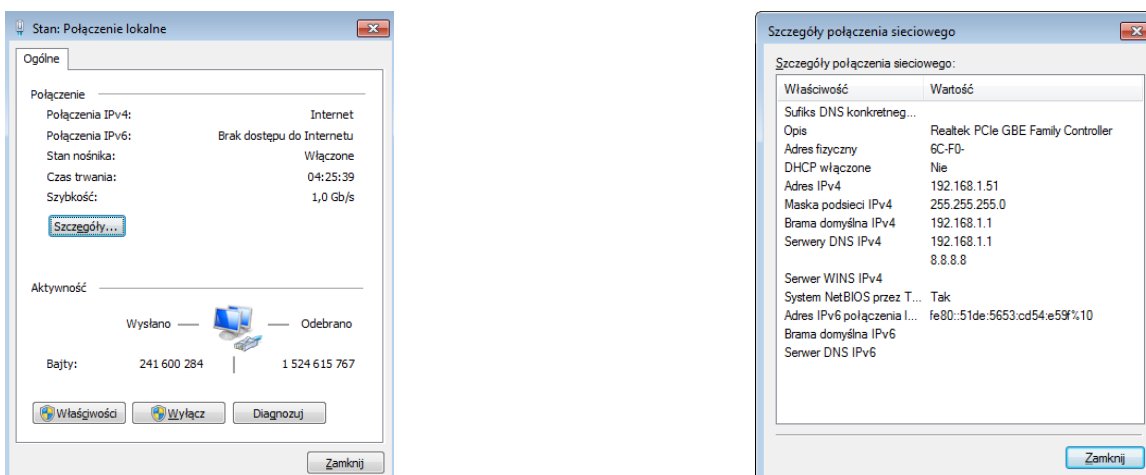
Na pasku zadań, w zasobniku systemowym (koło zegara) klikamy prawym klawiszem myszy w ikonę sieci a następnie Otwórz Centrum sieci i udostępniania.



Następnie klikamy Połączenie lokalne – może to nazywać się nieco inaczej np. Połączenie bezprzewodowe.



Następnie klikamy w Szczegóły.



W oknie Szczegóły połączenia sieciowego widzimy jakie są ustawienia naszego komputera;

- adres IPv4 – 192.168.1.51
- maska – 255.255.255.0
- adres bramy domyślnej czyli routera w naszej sieci – 192.168.1.1
- adresy serwerów DNS – 192.168.1.1 oraz 8.8.8.8

Na tej podstawie w ustawieniach sieci w rejestratorze wpisujemy:

- adres IPv4 – musimy wybrać adres z tej samej puli jaka jest używana w naszej sieci, tu mamy 192.168.1.xxx (xxx adresu urządzeń od 1 do 254), i przydzielamy wolny adres np. np. 192.168.1.90.
- sprawdzamy komendą ping czy jest wolny
 - klikamy w ikonę Windows / Start w lewym dolnym rogu ekranu, w polu Wyszukaj programy i pliki wpisujemy cmd
 - pojawia się okno linii komend
 - wpisujemy ping 192.168.1.90 (adres który chcemy przydzielić rejestratorowi)
 - powinniśmy otrzymać komunikat „Host docelowy jest nieosiągalny” oznaczający że adres jest wolny
 - inne komunikaty sugerują że adres może być zajęty, należy spróbować inny
- maskę sieci IPv4 – taką samą jak w komputerze czyli 255.255.255.0
- adres bramy domyślnej IPv4 – taki sam jak w komputerze czyli 192.168.1.1
- adresy serwerów DNS preferowanego oraz alternatywnego - takie same jak w komputerze – 192.168.1.1 oraz 8.8.8.8

Zakończyliśmy konfigurację ustawień sieciowych rejestratora. Możemy teraz np. przez przeglądarkę sprawdzić czy możemy się połączyć z rejestratorem, a także czy po włączeniu dostępu do chmury: (Konfiguracja → Sieć → Ustawienia zaawansowane → Dostęp do platformy) mamy Status Online.