MAZi – zdalny dostęp do rejestratorów i kamer

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

Ważne informacje:

- zalecaną przeglądarką jest Internet Explorer w wersji 8.0 lub wyższej, możliwa jest również obsługa za pomocą przeglądarki Firefox 52 ESR
- nie jest możliwa obsługa za pomocą przeglądarek Chrome, Opre i innych
- połączenie przez adres IP lub domenowy DDNS (większość dostawców stacjonarnych) – patrz punkt 5
  - 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 bezpośrednie rejestratorem
- połączenie przez chmurę Hicloudcam (połączenie przez sieci 3G/LTE) – patrz punkt 6
  - 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
- 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-xxK oraz IMVR-xxA
- w przypadku rejestratorów HTVR-xx oraz IMVR-xx 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 firmeware'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

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

- Możemy łączyć się bezpośrednio za pomocą adresu IP albo domenowego – wymagany jest routowalny adres IP.
- Druga możliwość, gdy nie mamy routowalnego adresu IP albo gdy dostawca internetu blokuje połączenia przychodzące, to zastosowanie chmury.

1.1. Połączenie bezpośrednie przez adres IP lub adres domenowy

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)
- klienta na urządzenia mobilne CCTV Viewer lub CCTV Viewer HD (Android, iOS)
- za pomocą programu VMS-A1 (Windows, MacOS)
- klienta na urządzenia mobilne Guarding Vision (Android, iOS)

1.2. Połączenie za pomocą chmury

Usługa chmury dostępna jest dla rejestratorów INVR-xxAL, INVR-xxB, INVR-xxKL, INVR-xxK, 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.
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. Zmiany w funkcjonowaniu usługi HiDDNS

Od dnia 16 kwietnia 2017 nie będzie możliwe rejestrowanie nowych urządzeń na serwerze HiDDNS.
Dotychczas zarejestrowane urządzenia będą działać bez zmian.

W przypadku urządzeń gdzie w opcjach DDNS w dalszym ciągu jest dostępna na liście wyboru usługa HiDDNS warunkowo będzie możliwe rejestrowanie urządzenia po 16 kwietnia 2017.

W związku z rozwojem technologii została uruchomiona nowa darmowa usługa GuardingVision która zastępuje usługę HiDDNS.

Dodatkowo uruchomiono serwis MAZi DDNS. Serwis przeznaczony jest wyłącznie dla urządzeń MAZi i do końca 2017 roku (okres promocyjny) korzystanie jest bezpłatne. Po zakończeniu okresu promocyjnego korzystanie z usługi może wymagać wykupienia symbolicznego abonamentu.

HiDDNS nie jest już dostępna w rejestratorach INVR-xxAL od firmware'u 3.4.92_170411, HAVR MT/LT/HT od 3.4.81_170418 i 3.4.81_170315 oraz HAVR-xx72H1 od V3.4.81_170406 – zastąpiły je nowe usługi Guarding Vision oraz MAZi DDNS.

4. Bezpieczeństwo rejestratora lub kamery

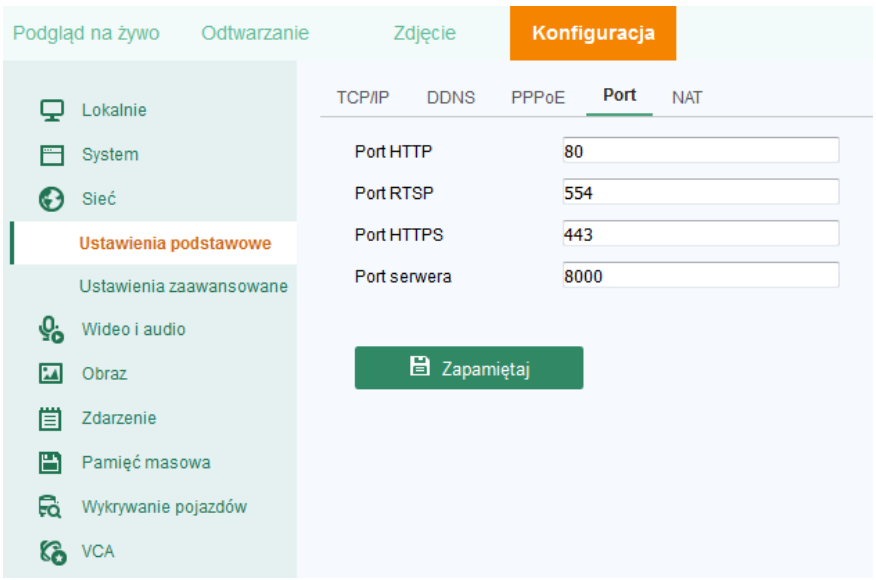
Niezależenie od metody dostępu należy stosować podstawowe zasady bezpieczeństwa. Niestosowanie się do nich zazwyczaj skutkuje przejęciem rejestratora przez nieuprawnione osoby.

- 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 umieszczaniu 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. Następna próba logowania możliwa jest dopiero po określonym czasie, zazwyczaj 20 minut
- aktualizacja firmware'u do najnowszej dostępnej wersji

5. Konfiguracja połączenia bezpośredniego przez adres IP lub adres domenowy

5.1. Poszczególne etapy konfiguracji:

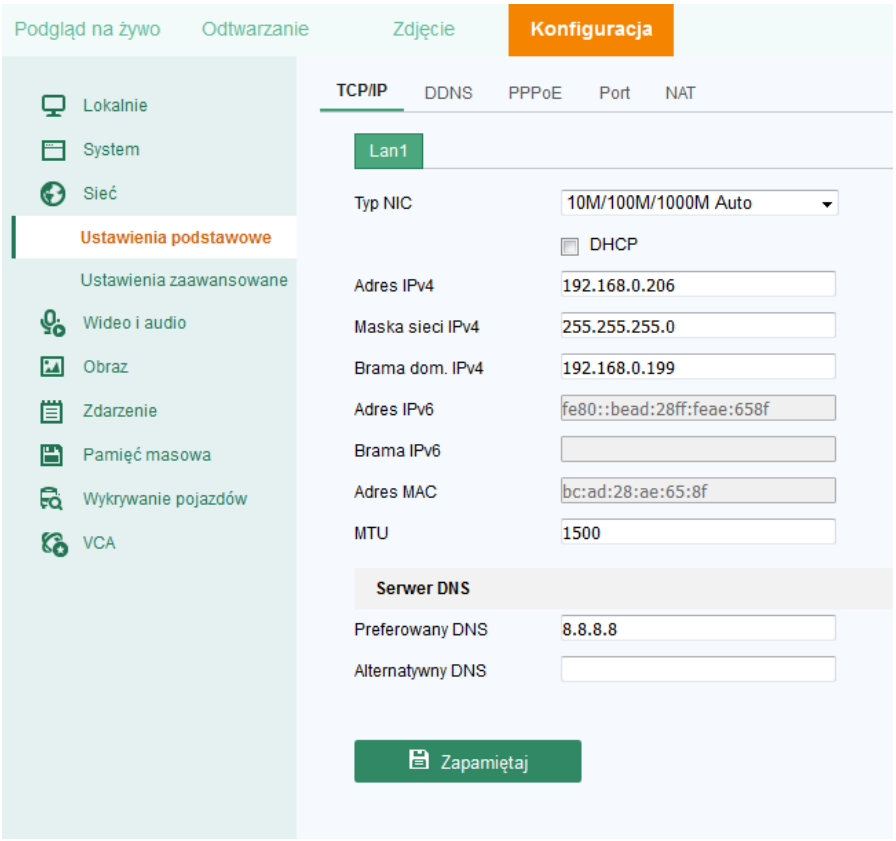
- konfiguracja rejestratora
  - łącząc się przez przeglądarkę, wchodzimy w zakładkę *Konfiguracja → Sieć → Ustawienia podstawowe → TCP/IP* lub
  - bezpośrednio w rejestratorze wybieramy *Menu → Ustawienia → Sieć - Ogólne*
  - wpisujemy prawidłowy adres IPv4 oraz maskę sieci IPv4, zgodne z adresacją stosowaną 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 ustawianiach 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 rejestratora ma odblokowany dostęp do Internetu na routerze – bywa ze administrator routera domyślnie blokuje dostęp do Internetu
- sprawdzamy u dostawcy Internetu czy nie blokuje połączeń przychodzących



5.2. Konfiguracja usługi HiDDNS

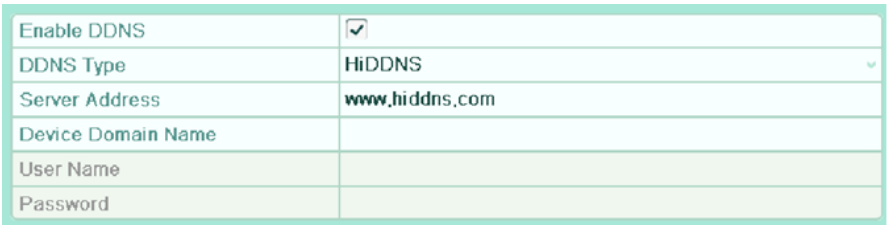
Usługa pozwala na dodawanie nowych domen do 15 kwietnia 2017. Po tej dacie można będzie używać już istniejących domen.

Ustawienia DDNS

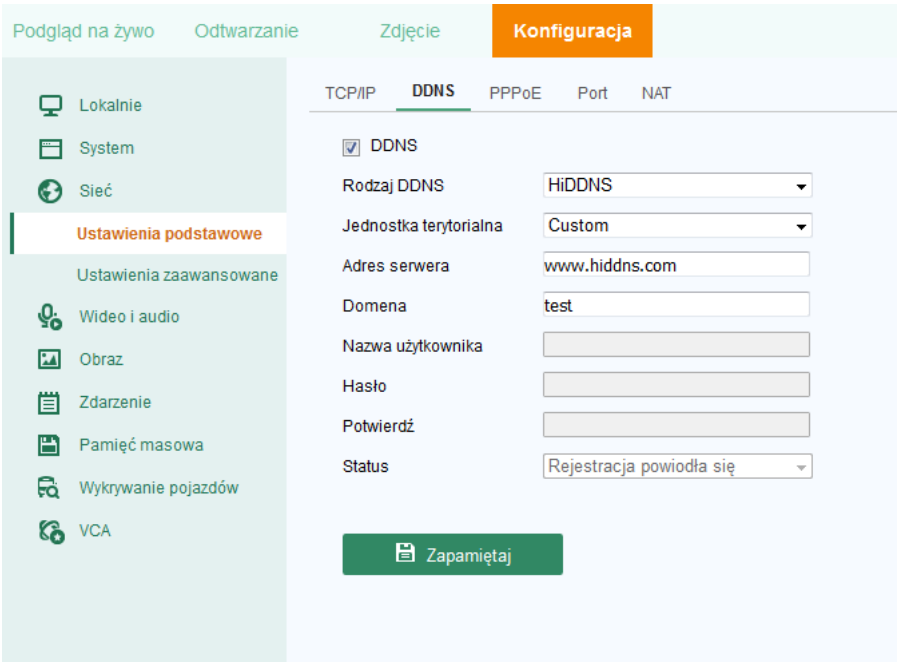
- włączamy usługę
- wybieramy opcję *HiDDNS*
- zostawiamy parametr jednostka terytorialna jako *Custom*
- adres serwera to *www.hiddns.com*, alternatywnie można wykorzystać serwer *eudev.hiddns.com*
- wpisujemy unikalną nazwę naszej domeny czyli alias i ją zatwierdzamy klikając *Zapamiętaj*. W przypadku kolizji z istniejącą domeną o takiej samej nazwie zostanie wyświetlony komunikat.
- Sprawdzamy w polu *Status* czy mamy komunikat *Stan DDNS jest normalny*

W obecnie dostępnych urządzeniach nie jest wymagane tworzenie konta na serwerze HiDDNS.

Niektóre najwcześniejsze wersje firmware'ów wymagają wcześniejszego utworzenia konta w serwisie HiDDNS, zarejestrowania urządzenia podając jego numer seryjny odczytany w menu rejestratora *Manu - Maintenance / Konserwacja – System info*. Następnie należy podać login i hasło w ustawieniach logowania rejestratora do serwisu HiDDNS.



ustawienia DDNS bezpośrednio w rejestratorze



ustawienia DDNS przez przeglądarkę

Połączenie przez przeglądarkę
Adres naszego rejestratora to *http://www.hiddns.com/alias* lub *http://alias.hiddns.com*. Standardowo serwer sam podstawia numer portu i jego podawanie nie jest konieczne. Tylko w przypadku najstarszych urządzeń gdy nie udało się uzyskać numeru portu automatycznie, należy podać port *http://www.hiddns.com/alias:port* (port HTTP na którym działa rejestrator).
Połączenie przez CCTV Viewer i VMS-A1
W przypadku CCTV Viewer wybieramy *Urządzenie → Dodaj urządzenie → Ręczne dodawanie → wybieramy HiDDNS* i podajemy nazwę domeny. Nie jest konieczne podawanie portów.
W przypadku programu VMS-A1 – przez *Zarządzanie urządzeniami → Serwer → Dodanie urządzenia →* HiDDNS oraz port SDK np. 8000. Nie jest konieczne podawanie portów.

5.3. Konfiguracja usługi MAZi Dynamic DNS

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

Zarządzanie kontem MAZi DDNS.

- W pierwszej kolejności należy założyć konto w serwisie *maziddns.com*
- Następnie dodajemy domenę podając jej nazwę (*Domain*), adres IP (*Ip Address*), port HTTP (*HTTP Port*), nazwę użytkownika (*Username*) oraz dwa razy podajemy hasło (*Password*)
- Zatwierdzamy
- Dane domeny wykorzystujemy podczas konfiguracji DDNS w rejestratorze

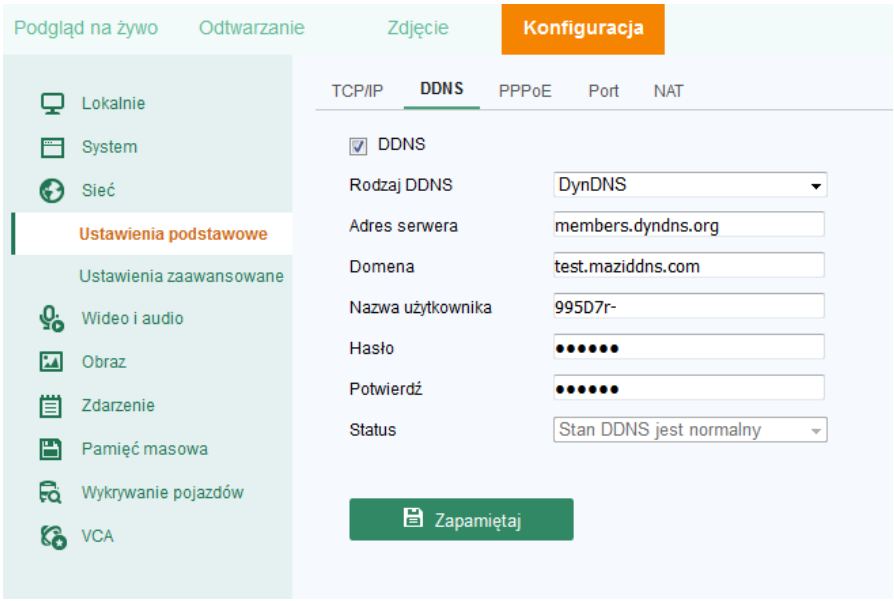
Podawany adres IP potrzebny jest do sprawdzenia czy urządzenie które będzie korzystać z usług jest urządzeniem MAZi. Jeśli urządzenie MAZi nie zostanie wykryte, nie będzie się dało zapisać ustawień.

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 i VMS-A1
W przypadku CCTV Viewer dodajemy *Urządzenie → Dodaj urządzenie → Ręczne dodawanie → wybieramy IP/Domain* i podajemy adres "*gde.maziddns.com*" oraz port SDK np. 8000.
W przypadku programu VMS-A1 – przez *Zarządzanie urządzeniami → Serwer → Dodanie urządzenia → IP/Domena* oraz port SDK np. 8000.

5.4. Usługa GuardingVision

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

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 kodu weryfikacyjnego 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
- Należy także ustawić port HTTP oraz SDK rejestratora

Należy pamiętać że jest niezbędne prawidłowe skonfigurowanie ustawień sieciowych rejestratora.

Możemy się łączyć za pomocą:

- Logujemy się na stronie *https://www.guardingvision.com*,w zakładce *Device Managament*
  - 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, znając adres możemy łączyć się bez potrzeby ponownego logowania do serwisu Guarding Vision
- klienta na urządzenia mobilne 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 rejestrator zarówno wśród urządzeń on-line (muszą znajdować się w sieci lokalnej) jak i podając ich adres IP/domenowy
- za pomocą programu VMS-A1 (Windows) – przez *Zarządzanie urządzeniami → Serwer → Dodaj nowy typ urządzenia → P2P CloudUrzadz*. Następnie logujemy się danymi do konta GuardingVision

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.

5.5. Zdalny dostęp przez 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.

5.6. Zdalny dostęp z urządzeń mobilnych

Pozwala na zdalny monitoring za pomocą rejestratorów analogowych, rejestratorów IP, kamer IP stacjonarnych, obrotowych a także enkoderów marki MAZi. 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

CCTV Viewer oraz CCTV Viewer HD

CCTV Viewer – obsługuje DVR, NVR, kamery IP oraz enkodery.
Można go znaleźć w Apple Store (https://itunes.apple.com/us/app/cctv-viewer/id680436764?mt=8) oraz w Google Play (https://play.google.com/store/apps/details?id=com.europe1.iVMS)

CCTV Viewer HD – wersja zoptymalizowana dla tabletów dostępna w Apple Store (https://itunes.apple.com/us/app/cctv-viewer-hd/id680437675?mt=8) oraz w Google Play (https://play.google.com/store/apps/details?id=com.europe1.iVMSHD&hl=pl).

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.

Program Guarding Vision

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)

6. Konfiguracja połączenia za pomocą chmury Hicloudcam

6.1. Konfiguracja połączenia sieciowego w rejestratorze

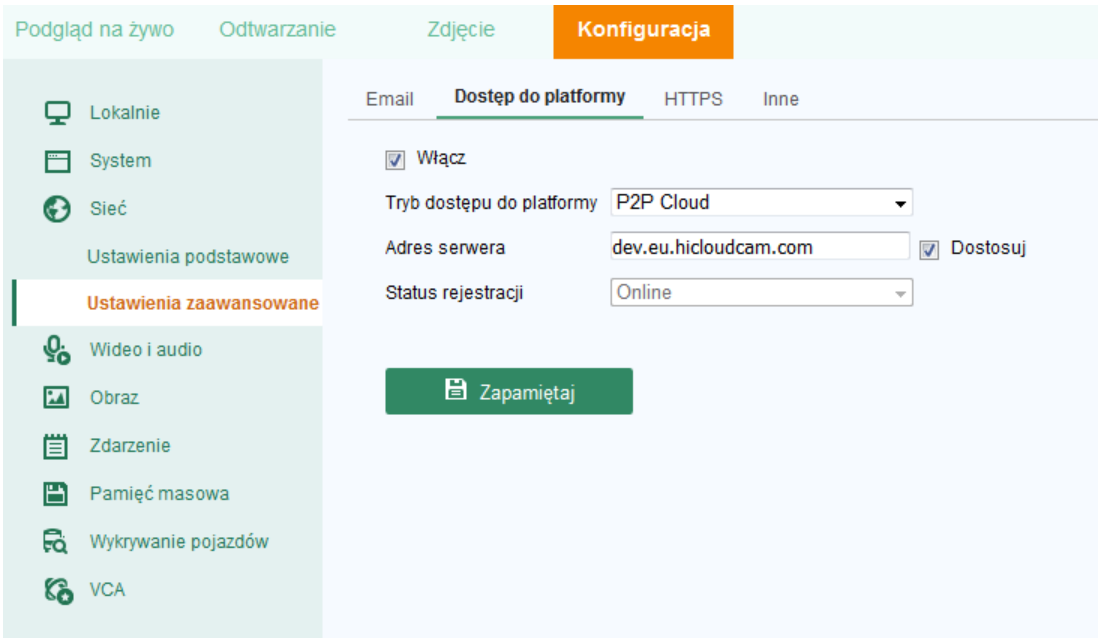
- rejestrator musi mieć prawidłowy adres IP oraz maskę, zgodne z adresacją stosowanej w sieci do której podłączony jest rejestrator
- podany adres bramy sieciowej (portu LAN routera udostępniającego internet)

- 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 ze administrator routera domyślnie blokuje dostęp do Internetu

6.2. Konfiguracja klienta chmury w rejestratorze

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 G*uarding 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 G*uarding Vision*
- Adres serwer: *dev.hicloudcam.com* lub *dev.guardingvision.com*
- Użytkownika: odznaczone
- Włącz szyfrowanie strumienia: odznaczone

6.3. 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
  - Veryfication 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 wyłączamy szyfrowanie lub w przypadku gdy łączymy się przez przeglądarkę w opcji Konfiguracja → Lokalnie → podajemy kod weryfikacyjny.

6.4. Dostępne metody połączenie przez chmurę

Możemy się łączyć za pomocą:

- przeglądarki (np. Internet Explorer, Firefox) – przez zalogowanie się na stronie *http://www.hicloudcam.com*
- klienta na urządzenia mobilne CCTV Viewer lub CCTV Viewer HD (Android, iOS) – wybieramy opcję Cloud P2P i logujemy się danymi jak do konta Hicloudcam
- za pomocą programu VMS-A1 (Windows) – przez *Zarządzanie urządzeniami → Serwer → Dodaj nowy typ urządzenia → P2P CloudUrzadz* lub *Guarding VisionUrzadz (zależnie od wersji programu).* Następnie logujemy się danymi do konta Hicloudcam

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 Update, Web Safe Box oraz ShiPin7 Web Player. W przypadku Internet Explorera sprawdzamy (Narzędzia –> Zarządzaj dodatkami) czy następujące dodatki są włączone: UpdataActiveX Control, SP7WebVideoActiveX Control oraz SafePWSBox Control.

6.5. Nawiązywanie połączenia

Przeglądarka:
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 Managament – zarządzanie urządzeniami oraz udostępnianie innym użytkownikom usługi Hicloudcam naszych urządzeń.

CCTV Viewer:
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 ekrany 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 następuję przyciskiem w prawym górnym rogu ekrany lub przez powrót wstecz z okna wpisywania numeru seryjnego i powtórne kliknięcie przycisku +.

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

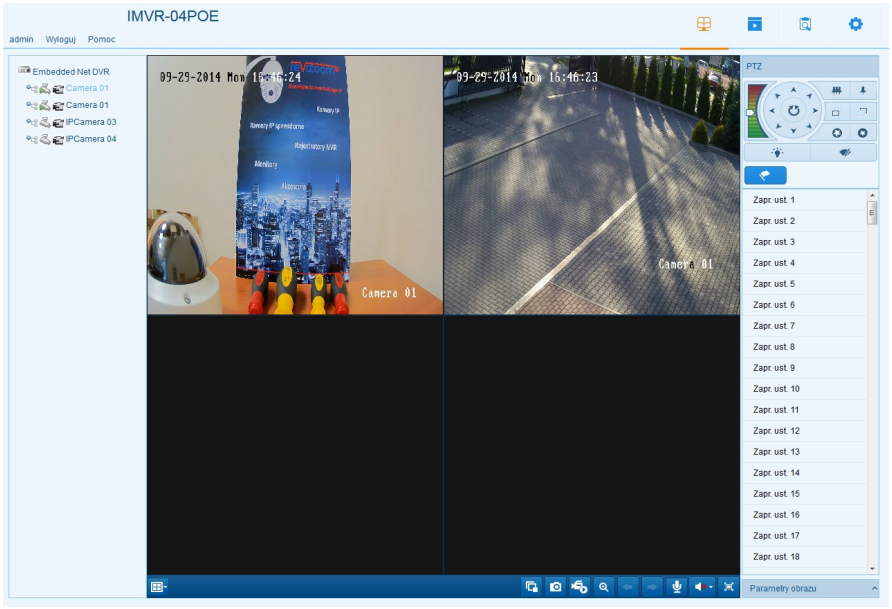
Szczególną cechą programu VMS-A1 jest opcja *Zdalna konfigur*. pozwalająca na zarządzanie ustawieniami rejestratora poprzez chmurę.

7. Najczęściej spotykane pytania i problemy

Dostęp przez przeglądarki

Konfiguracja rejestratora oraz podgląd możliwy jest przez następujące przeglądarki: Mozilla Firefox, Internet Explorer, Apple Safari. 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\Nazwaużytkownika\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 ciągłe 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 ciągłe 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 niepodpisanych kontrolek ActiveX* – monituj
- zapisz modyfikacje klikając OK i wyjdź z menu Zabezpieczeń.
- czasem może być potrzebne przeładowanie komputera a zawsze ponowne uruchomienie przeglądarki

Czasem może być koniecznie 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*
- zamykany 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*

Usuniecie wtyczki w Windows

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

- wyłączyć wszystkie przeglądarki np. Firefox, Internet Expolorer
- 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

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

Problemy z połączeniem sieciowym

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.

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

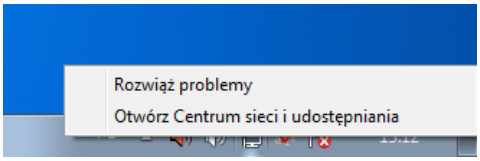
Chcemy prawidłowo skonfigurować ustawienia sieciowe w rejestratorze MAZi. W instrukcji „MAZi – zdalny dostęp przez DDNS i chmurę v1.1 PL” w punkcie 4.1 opisano gdzie wpisujemy dane sieci.

Co musimy znać:

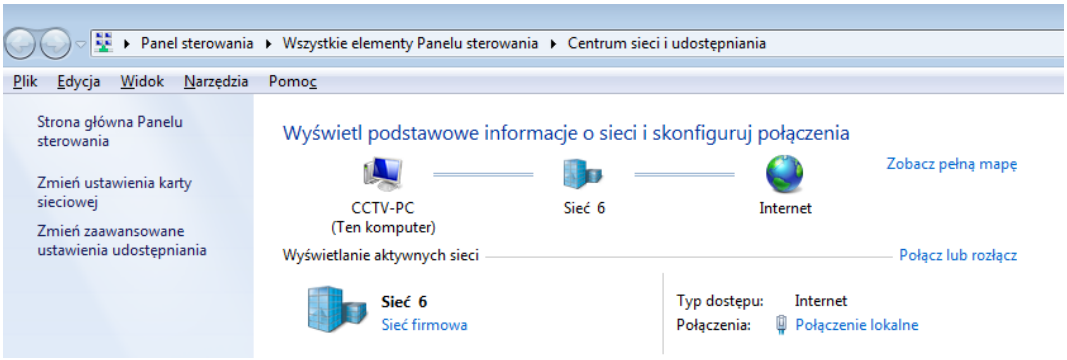
- adres IPv4 jaki planujemy przydzielić rejestratorowi
- maskę sieci IPv4 rejestratorach
- adres bramy domyślnej IPv4 (czyli adres portu LAN routera udostępniającego internet)
- adresy serwerów DNS preferowanego oraz alternatywnego

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.
Przydziału 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.

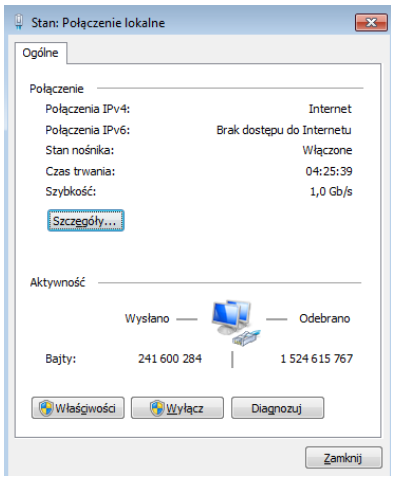
Na pasku zadań, w zasobniku systemowym (koło zegara) klikamy prawym klawiszem myszy w ikonę sieci a następnie Otwórz Centrum sieci i udostępniania.

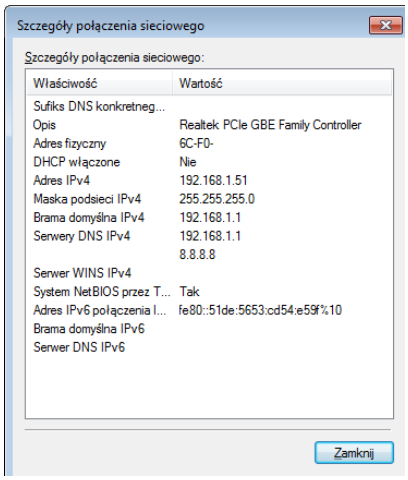


Następnie klikamy Połączenie lokalne – może to nazywać się nieco inaczej np. Połączenie bezprzewodowe.



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 wpisujmy:

- 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 ekrany, 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.

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