MAZi – zdalny dostęp do rejestratorów i kamer przez chmurę

wersja 2.5

Instrukcja opisuje jak skonfigurować rejestrator lub kamerę by było możliwe połączenie z nimi przez Internet za pomocą chmury. Ten rodzaj zdalnego dostępu jest zalecany gdy nasze urządzenie podłączone jest do Internetu za pomocą sieci 3G/4G/5G lub gdy nie mamy dostępu do routera i równocześnie ma on wyłączoną funkcje UPnP.
W przypadku gdy mamy dostęp do Internetu posiadający adres IP publiczny (stały lub przydzielany dynamicznie) zalecamy skorzystać z połączenia bezpośredniego przez adres IP, DNS lub DDNS.
Postępowanie w przypadku dodawania kamer bezpośrednio do chmury, procedura jest identyczna jak w przypadku rejestratora. Jeśli kamery są dodane do rejestratora to jest wystarczające by w chmurze pracował tylko rejestrator.
Ta instrukcja dotyczy rejestratorów MAZi z wyłączeniem serii S oraz kamer MAZi serii H (np. IVH-xx, IWH-xx). Kamery serii N (np. IVN-xx, IWN-xx) posiadają własną i odrębną usługę chmury.

Ważne informacje:
ze względu na specyfikę połączenia przez sieci komórkowe 3G/4G/5G 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

- producent ani dystrybutor nie odpowiadają za możliwość, jakość i ciągłość zdalnego dostępu przez sieć
- należy pamiętać że połączenie przez chmurę jest realizowane przez serwery pośredniczące których obciążenie może się zmieniać w czasie
- na jakość połączenia ma wpływ jakość połączenia przez Internet (m. in. szybkość uploadu w miejscu podłączenia urządzenia)
- usługa dostępu przez chmurę oraz usługa DDNS to dwie różne usługi
- usługa chmury oraz DDNS korzystają z tego samego klienta włączanego w opcji *Dostęp do platformy*
- należy zwrócić uwagę że konieczne jest nadanie kodu weryfikacyjnego, który jest równocześnie kluczem szyfrowania
- usługi sieciowe MAZi takie jak dostęp przez chmurę czy DDNS są usługami niegwarantowanymi, świadczonymi w miarę możliwości technicznych i organizacyjnych i jako takie nie są objęte gwarancją
- należy zawsze stosować najnowszą dostępną wersję firmware'u urządzenia oraz programów na PC oraz urządzenia mobilne które znajdziesz na http://materialy.gde.pl/do-pobrania

Wszelkie uwagi i poprawki prosimy zgłaszać na adres: 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 mogą nie działać.
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, w tym prawidłowo wpisane adresy serwerów DNS, adres IP i maska sieci.
Nie potrzebujemy przekierowania portów na routerze czy routowalnego adresu.

2. Bezpieczeństwo rejestratora lub kamery

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

- stosowanie skomplikowanych haseł i kodów, 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 umieszczaniu w DMZ
- nie należy wyłączać blokowania po nieudanym logowaniu lub kilku kolejnych nieudanych logowaniach, następna próba logowania możliwa jest dopiero po określonym czasie, zazwyczaj 30 minut
- należy zaktualizować firmware do najnowszej dostępnej wersji

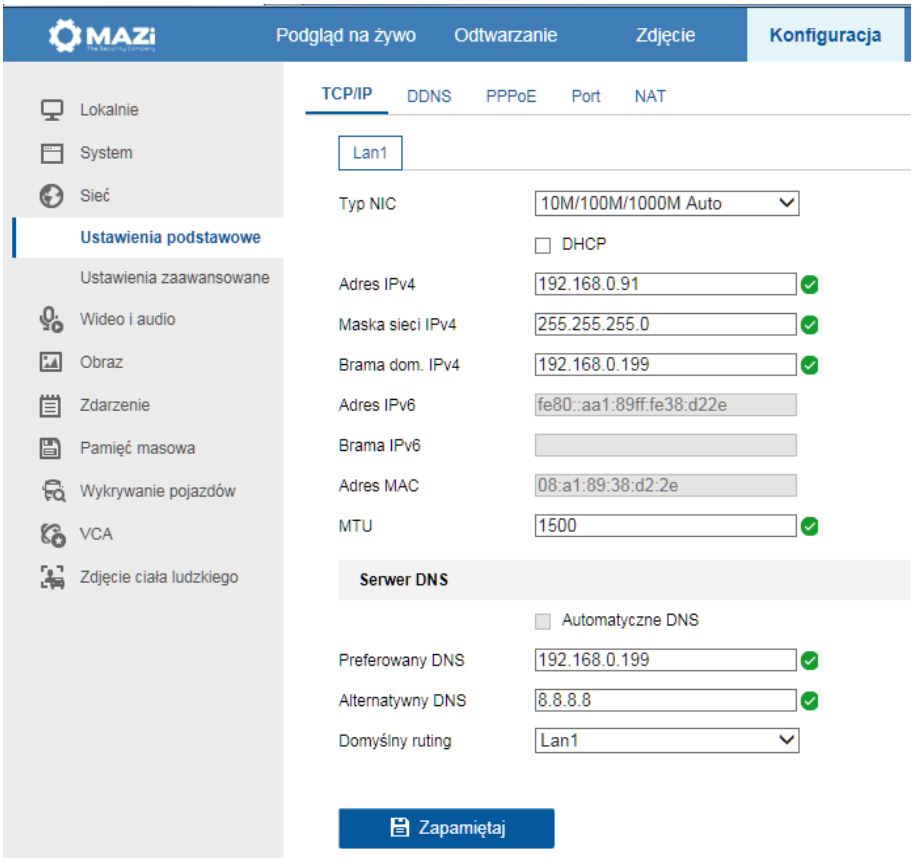
3. Konfiguracja połączenia

Konfiguracja składa się z kilku kroków:

- skonfigurowanie połączenia sieciowego w urządzeniu (punkt 3.1)
- włącznie klienta chmury (punkt 3.2) i nadanie kodu weryfikacyjnego, kod weryfikacyjny jest także kodem szyfrowania i jego podanie jest wymagane na każdym urządzeniu z którego logujemy się do konta w chmurze
- utworzenie konta chmurze (punk 3.3)
- dodanie urządzenia (punkt 3.4)

3.1. Konfiguracja połączenia sieciowego w rejestratorze

Konfiguracji ustawień sieci w rejestratorze dokonujemy tak jak w każdym innym urządzeniu sieciowym.

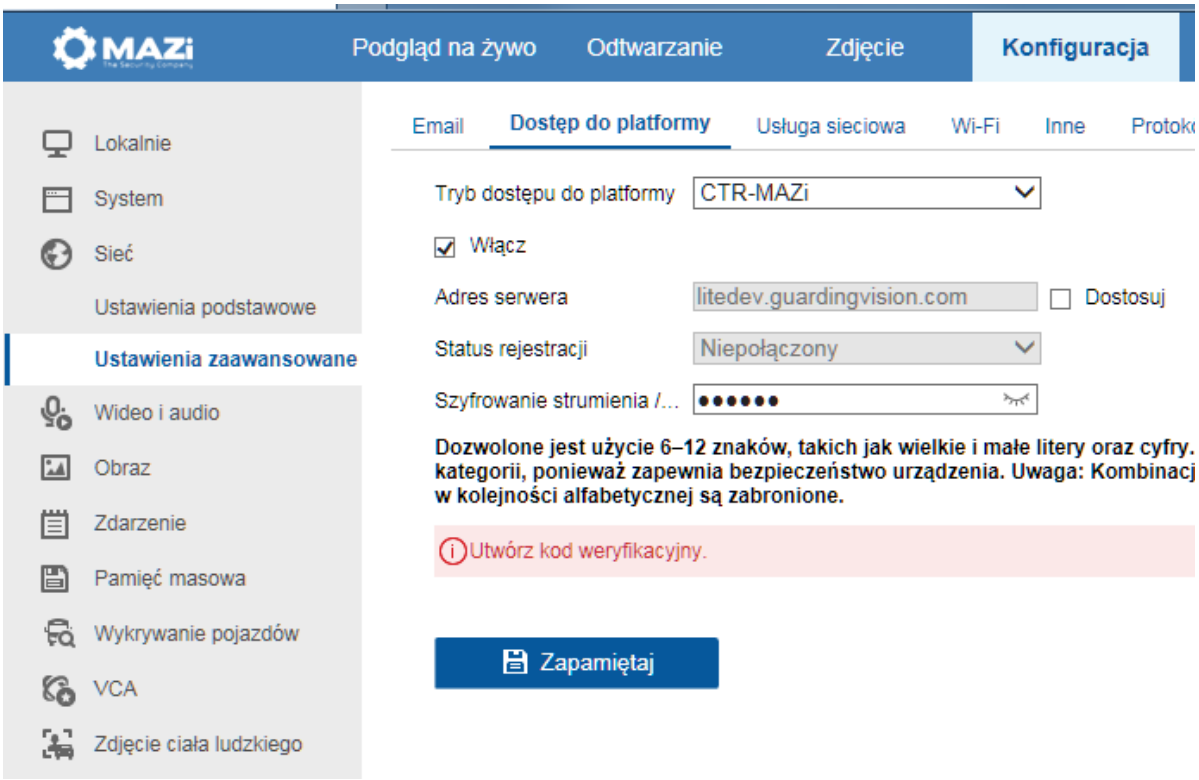


Zalecamy przydzielenie rejestratorowi stałego adresu IP i dokonanie samodzielnej konfiguracji ustawień sieciowych. Jednakże w przypadku połączenia przez chmurę dopuszczalna jest konfiguracja z wykorzystaniem klienta DHCP. Wtedy pozostałe podpunkty pomijamy, sprawdzamy tylko czy router przydzielił rejestratorowi adres IP oraz serwery DNS i wykonujemy punkt 3.2 i kolejne – zakładamy konto w chmurze.

- Wybieramy czy adresacji dokonujemy samodzielnie zgodnie z opisem poniżej czy też włączamy kienta DHCP i korzystamy z autokonfiguracji.
- rejestrator musi mieć prawidłowy adres IP oraz maskę, zgodne z adresacją stosowanej w sieci do której podłączony jest rejestrator
- bezpośrednio w rejestratorze wybieramy *Menu → System → Sieć → Protokół TCP/IP → Protokół TCP/IP*, można także połączyć się przez przeglądarkę i wtedy mamy *Konfiguracja → Sieć → Ustawienia podstawowe → TCP/IP*
- 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.
- gdy korzystamy z usługi DHCP i rejestrator sam konfiguruje ustawienia sieci na podstawie danych otrzymanych z router'a to zalecamy wyłączenie funkcji *automatyczny DNS* i ręczne wpisanie adresów serwerów DNS

3.2. Włączenie 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.*
Rejestrator: *Menu → System → Sieć → Zaawansowane → Dostęp do platformy*
Przeglądarka: *Konfiguracja → Sieć → Ustawienia zaawansowane → Dostęp do platformy*



Konfiguracja rejestratora

- Włączamy chmurę. Pojawi się prośba o zaakceptowanie polityki prywatności oraz nadanie kodu weryfikacyjnego

- Tryb dostępu do platformy ustawiamy jako *CTR-MAZi*
- Adres serwera: pozostawiamy domyślny - *litedev.guardingvision.com*
- Zatwierdzamy klikając *Zapamiętaj*
- Sprawdzamy w polu *Status* czy mamy komunikat *Online*. Gdy pojawia się komunikat *Niepołączony* to należy odświeżyć stronę, w następnej kolejności zrestartować rejestrator poprzez menu *Konfiguracja* a jeśli dalej mamy status niepołączony to należy sprawdzić prawidłowość konfiguracji zakładki *Konfiguracja → Sieć → Ustawienia podstawowe → TCP/IP.*
- Dokonując konfiguracji bezpośrednio na rejestratorze mamy dodatkowe opcje
  - *Włącz szyfrowanie*, można włączać i wyłączać szyfrowanie strumienia audio/video, zalecamy zostawić ją włączoną
  - Gdy szyfrowanie jest włączone to podgląd przez przeglądarkę możliwy jest przez Internet Explorer (wymagana instalacja wtyczki WebComponents) oraz przez przeglądarki Firefox, Edge, Chrome (wymagana instalacja wtyczki LocalServiceComponents – dotyczy wybranych rejestratorów)
  - *Stan konta CTR-MAZi* pojawi się status *Niepowiązany* (rejestrator nie jest dodany do konta w chmurze) lub *Powiązany* (rejestrator jest już dodany do konta w chmurze)
  - *Anuluj powiązanie* – pozwala na usunięcie rejestratora z konta nawet gdy nie wiemy co to za konto lub nie znamy nazwy użytkownika i hasła, wymagana jest znajomość hasła administratora do rejestratora

Standardowe ustawienia:

- Dostęp do platformy: *włącz*
- Typ dostępu: *CTR-MAZi*
- Adres serwer: *litedev.eu.guardingvision.com* – nie zmieniamy
- Włącz szyfrowanie strumienia: *włączone*

3.3. Utworzenie konta w chmurze

Założenie konta możliwe jest z poziomu programu CTR-MAZi na Android oraz iOS (iPhone, iPad) oraz *CMS-MAZi* na PC.

- pobierz z program *CTR-MAZi* dla *Android* lub *iOS*
- Opcja *Zarejestruj*
- Zaakceptuj regulaminy
- Opcja *Wybierz region* – wybieramy Polska
- Wybieramy *Zaloguj* / *Zarejestruj*
- Teraz możemy wybrać czy do założenia konta użyjemy e-maila czy numeru telefonu, te dane są potrzebny by dokonać aktywacji konta
- Podajemy
  - *Adres E-mail* – adres e-mail na który zostanie wysłany mail z kodem aktywacyjnym
  - *Hasło* – hasło
- Wybieramy *Pobierz kod zabezpieczający*
- Wprowadź kod weryfikacyjny – tzw. *captch'a* i czekaj na mail z kodem z zabezpieczającym
- Sprawdzamy mail'a w poszukiwaniu maila z kodem zabezpieczającym
- Odebrany na maila 4-cyfrowy kod aktywacyjny (ważny przez pół godziny) podajemy w oknie aktywacji konta

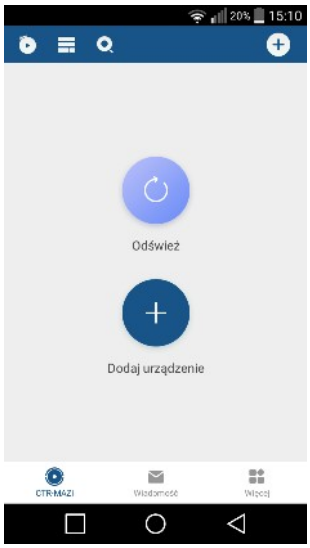
3.4. Dodanie rejestratora do konta

Uwaga: Rejestrator może być przypisany tylko do jednego konta, ale może być udostępniony wielu innym kontom. Jest to warunkowane względami bezpieczeństwa (zachowanie prywatności).

- wybierz *Dodaj urządzenie*
- zeskanuj kod QR w rejestratorze : *Menu → System → Sieć → Zaawansowane → Dostęp do platformy*, lub przez przeglądarkę: *Konfiguracja → Sieć → Ustawienia zaawansowane → Dostęp do platformy* lub jeśli dany firmware nie ma opcji QR kodu to:

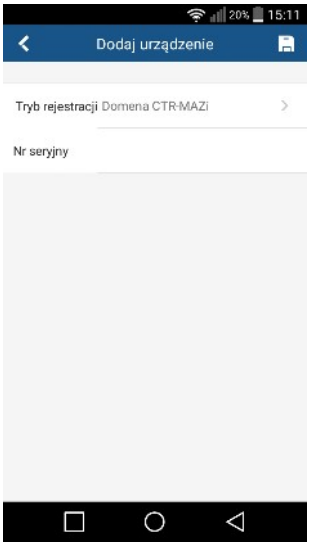
- opcjonalnie: w prawym górnym roku wybierz *ikonę ołówka* i podaj numer seryjny (najprościej odczytać z dołu lub boku obudowy) oraz wprowadź kod weryfikacyjny odczytany z *Menu rejestratora* (ten który nadaliśmy podczas włączenia usługi chmury)
- zatwierdź *Dodaj*
- dodawanie zostało zakończone
- wybierz *Dalej*,
- teraz możesz nadać rejestratorowi własną nazwę
- wybierz *Zapisz*

Poniżej znajdują się screeny z poszczególnych etapów dodawania rejestratora do konta w chmurze



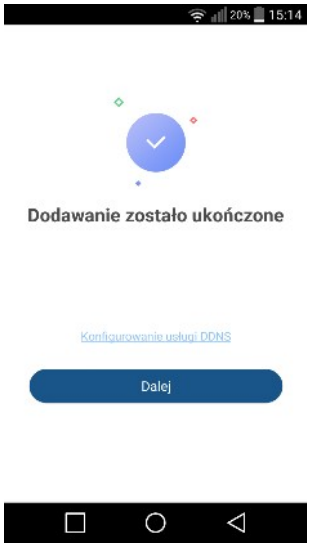
dodaj urządzenie

zeskanuj kod

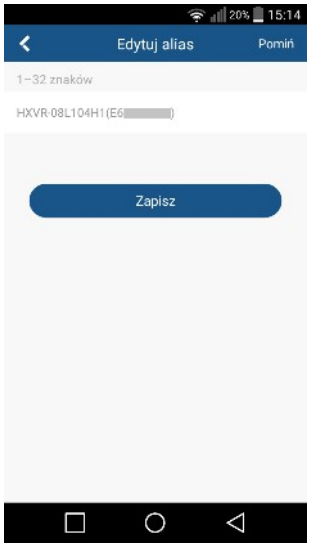


lub wpisz numer seryjny

zatwierdź

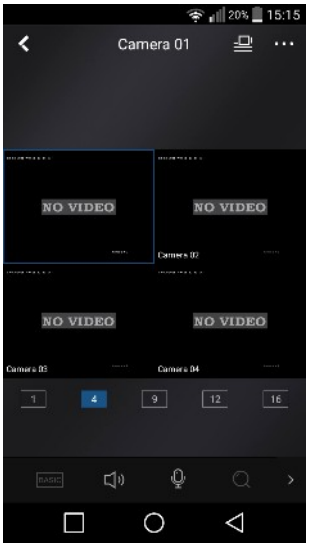


zatwierdź ponownie



nadaj nazwę

lista urządzeń



podgląd

Gdzie znaleźć kod weryfikacyjny:

- Rejestrator: *Menu → System → Sieć → Zaawansowane → Dostęp do platformy*,
- Przeglądarka: *Konfiguracja → Sieć → Ustawienia zaawansowane → Dostęp do platformy*

Możliwe jest kilkukrotne zalogowanie z użyciem danych jednego użytkownika.

Udostępnienie urządzeń innym użytkownikom.
Istnieje możliwość udostępnia urządzeń innym użytkownikom posiadającym własne konta w chmurze wraz

przydzieleniem praw do konkretnej kamery i czynności np. przeglądania nagrań.

4. Dostępne oprogramowanie

4.1. Urządzenia mobilne - program CTR-MAZi na smartfon/tablet

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.
Jakość i płynność połączenia zdalnego zależy od jakości łącza sieciowego i wydajności telefonu. W przypadku braku płynność połączenia należy przełączyć w strumień pomocniczy (basic) lub zmniejszyć rozdzielczość, liczbę klatek i bitrate w kamerze – ma to wpływ na jakość nagrania.
Program pozwala na połączenia przez adres IP, adres DNS, serwisy DDNS oraz przez chmurę.
Łączymy się z rejestratorem logując się do konta w chmurze i wybierając z listy urządzenie z którym chcemy się łączyć.
Wybieramy opcję *Zaloguj* i logujemy się danymi do konta chmurze
Wybieramy rejestrator i rozpoczynamy podgląd. Bezpośrednio po zalogowaniu do konta możliwe jest także dodawanie urządzeń do chmury przyciskiem + na środku ekranu.

CTR-MAZi dostępny jest na urządzenia z systemem Android jak i iOS. Można go znaleźć w Apple Store oraz w Google Play.

Uwaga: Gdy pojawi się żądanie kodu szyfrowania

- podgląd przez aplikację *CTR-MAZi* – zostaniemy poproszeni o podanie kodu weryfikacyjnego
- program *CMS-MAZi* na PC: przy pierwszej próbie podglądu pojawi się monit o podanie kodu weryfikacyjnego,

W obu przypadkach wpisujemy kod weryfikacyjny (klucz szyfrowania), rozłączamy się i ponownie włączamy podgląd. Kod wystarczy podać dla jednej z kamer danego rejestratora.

4.2. Program CMS-MAZi na PC

Funkcje CMS-MAZi:

- 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
- program umożliwia połączenie z rejestratorem przez adres IP, adres domenowy, z użyciem DDNS a także przez chmurę

Łączymy się z rejestratorem w chmurze podając:

- nazwę konta w chmurze 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 CMS-MAZi jest opcja *Zdalna konfiguracja* pozwalająca na zarządzanie ustawieniami rejestratora poprzez chmurę
- opcja *Rejestruj* pozwala na założenie konta w chmurze z poziomu programu, możliwe jest także dodawanie urządzeń do chmury

5. Najczęściej spotykane pytania i problemy

Dostęp przez przeglądarki – połączenie przez adres IP/DNS/DDNS

W przypadku rejestratorów wyposażonych menu i firmware w wersji co najmniej 4.0 oraz niektóre w wersji 3.4.xx możliwe jest połączenie za pomocą przeglądarek Firefox, Edge, Chrome, IE i innych. W przypadku

starszych firmware'ów wymaganą przeglądarką jest Internet Explorer na Windows lub EDGE w trybie Internet Explorer oraz Safari na MacOS. Połączenie przez przeglądarkę możliwe jest przez adres IP, DNS lub DDNS. Nie ma możliwości połączenia z rejestratorem przez chmurę za pomocą przeglądarki. Łączymy się z rejestratorem podając adres i port HTTP np. http://192.0.0.64:80

W systemie Windows wymagane jest zainstalowanie wtyczki WebComponents (dotyczy IE) lub LocalServiceComponents oraz HTML5 (Firefox, Edge itp. - obsługa przez wtyczkę lub HTML5 zależy od wersji firmware'u) – 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/* - dział Rozwiązania IP MAZi. W razie potrzebny można także pobrać wtyczki dla Windows.

Najczęściej spotykane problemy związane z dostępem przez przeglądarkę Internet Explorer

– Brak włączonego trybu Internet Explorer w przeglądarce Edge

- uruchamiamy EDGE, klikamy trzy kropki w prawym górnym rogu, a następnie klikamy w *Ustawienia*
- w menu po lewej stronie wchodzimy w opcję *Przeglądarka domyślna*, następnie włączamy przełącznik *Zezwalaj na ponowne ładowanie witryn w trybie programu Internet Explorer*.
- wymagane jest ponowne uruchomienie przeglądarki
- następnie należy ponownie załadować witrynę w trybie IE. Należy wpisać adres urządzenia, wywołać stronę, gdy się załaduje to klikamy w trzy kropki w prawym górnym rogu, a następnie klikamy w *Załaduj ponownie w trybie Internet Explorer*

– 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 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 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 to sprawdzamy (*Narzędzia –> Zarządzaj dodatkami*) czy następujące dodatki są włączone: *WebVideoActiveX Control* lub *HCWPWebVideoActiveX Control* (w przypadku rejestratorów IMVR-xxA oraz ADVR-xx).

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 np. Free Commander.

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 – najprościej używając polecenia 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.

W czasie dodawania urządzenia do chmury pojawia się komunikat *Urządzenie zostało dodane do konta ab**@cd****.efgh* i nie można go dodać do naszego konta**

Jest to informacja że urządzenie jest dodane do innego konta wraz z zanonizowanym mail'em który był wykorzystany do założenia konta w chmurze do którego dodany jest rejestrator. Mail może nam pomóc w przypomnieniu sobie konta do którego daliśmy rejestrator. Jeśli to jest niemożliwe, to klikamy *Anuluj powiązanie urządzenia*, podajemy hasło administratora oraz kod captcha i klikamy zatwierdź. Urządzenie zostanie wyrejestrowane, można je dodać ponownie do nowego konta. Wymagane jest by nasz telefon był w tej samej sieci LAN w której znajduje się urządzenie.

Ważna uwaga

Pomimo iż producent dokłada wszelkich starań to usługi i funkcje sieciowe (np. dostęp przez chmurę, DDNS itp., połączenie za pomocą urządzeń mobilnych, komputerów i innych urządzeń) nie są w żaden gwarantowane. Ich dostępność i jakość zależy od wielu czynników (w tym od czynników niezależnych od producenta) np. jakość łącza internetowego, sieci LAN, konfiguracji sieci, zastosowanych rozwiązań technicznych. Zmiany protokołów i standardów, w tym systemów operacyjnych mogą mieć wpływ na funkcjonowanie urządzenia i dostarczonego z nim oprogramowania. Na te zmiany producent i dystrybutor nie mają wpływu a utrata funkcji związana z tymi zmianami nie jest objęta gwarancją. Dostępność i funkcje bezpłatnych usług – np. chmury oraz DDNS – których operatorem jest producent, nie są w żaden sposób gwarantowane.