

Bosch IP video products



Spis treści

1	Cel dokumentu i docelowi odbiorcy	5
2	Koncepcja i względy bezpieczeństwa	6
3	Bezpieczna instalacja	7
3.1	Serwery i urządzenia pamięci masowej	7
3.2	Kamery i urządzenia brzegowe	7
4	Bezpieczna konfiguracja	8
4.1	Przypisywanie adresów IP	8
4.1.1	Zarządzanie DHCP	10
4.2	Konta i hasła użytkowników	10
4.2.1	Przypisywanie haseł	11
4.2.2	Przypisywanie haseł za pomocą strony internetowej urządzenia wizyjnego	12
4.2.3	Przypisywanie haseł za pomocą programu Configuration Manager	13
4.2.4	Przypisywanie haseł dla autonomicznej instalacji VRM	14
4.2.5	Przypisywanie haseł za pomocą BVMS (na DIVAR IP lub w rozwiązaniu autonomicznym)	16
4.3	Wzmacnianie dostępu do urządzenia	17
4.3.1	Ogólne wykorzystanie portów sieciowych i transmisja sygnału wizyjnego	17
4.3.2	Minimalna wersja protokołu TLS	18
4.3.3	Stosowanie portu HTTP, HTTPS i portu wizyjnego	18
4.3.4	Oprogramowanie wideo i wybór portu	19
4.3.5	Tunelowanie SSH	19
4.3.6	Dostęp Telnet	20
4.3.7	RTSP: Protokół transmisji strumieniowej w czasie rzeczywistym	20
4.3.8	UPnP: Universal Plug and Play	21
4.3.9	Multicasting	22
4.3.10	Filtrowanie IPv4	23
4.3.11	SNMP	24
4.3.12	Bezpieczne ramy czasowe	25
4.3.13	Usługi chmurowe	25
4.4	Wzmacnianie kamer IP	26
4.4.1	Poziomy wzmacniania	26
4.4.2	Przegląd wzmacniania	26
4.4.3	Opis funkcji i zalecenia dotyczące wzmacniania	28
4.4.4	Głęboka obrona	31
4.5	Wzmacnianie pamięci	32
4.5.1	Ustawianie hasła CHAP na urządzeniach iSCSI	32
4.6	Wzmacnianie serwerów	33
4.6.1	Zalecane ustawienia sprzętowe serwera	33
4.6.2	Zalecane ustawienia zabezpieczeń systemu operacyjnego Windows	33
4.6.3	Aktualizacje systemu Windows	33
4.6.4	Instalacja oprogramowania antywirusowego	33
4.6.5	Zalecane ustawienia systemu operacyjnego Windows	34
4.6.6	Uaktywnianie kontroli konta użytkownika na serwerze	34
4.6.7	Dezaktywacja autoodtworzenia	35
4.6.8	Urządzenia zewnętrzne	35
4.6.9	Konfiguracja przypisania praw użytkownika	35
4.6.10	Wygaszacz ekranu	36
4.6.11	Aktywacja ustawień zasad dotyczących haseł	36
4.6.12	Wyłączyć usługi nieistotne dla systemu Windows	37

4.6.13	Konta użytkowników systemu operacyjnego Windows	37
4.6.14	Włączyć zaporę na serwerze	38
4.7	Wzmacnianie klientów Windows	38
4.7.1	Stacje robocze Windows	38
4.7.2	Zalecane ustawienia sprzętowe stacji roboczych systemu Windows	38
4.7.3	Zalecane ustawienia zabezpieczeń systemu operacyjnego Windows	39
4.7.4	Zalecane ustawienia systemu operacyjnego Windows	39
4.7.5	Uaktywnianie kontroli konta użytkownika na serwerze	39
4.7.6	Dezaktywacja autoodtworzenia	40
4.7.7	Urządzenia zewnętrzne	40
4.7.8	Konfiguracja przypisania praw użytkownika	40
4.7.9	Wygaszacz ekranu	41
4.7.10	Aktywacja ustawień zasad dotyczących haseł	42
4.7.11	Wyłączyć usługi nieistotne dla systemu Windows	42
4.7.12	Konta użytkowników systemu operacyjnego Windows	43
4.7.13	Włączyć zaporę na stacji roboczej	43
4.8	Ochrona dostępu do sieci	43
4.8.1	VLAN: wirtualna sieć LAN	44
4.8.2	VPN: wirtualna sieć prywatna	44
4.8.3	Wyłączanie niewykorzystanych portów przełączników	45
4.8.4	Sieci chronione 802.1x	45
5	Bezpieczne działanie	46
5.1	Separacja sieci	46
5.2	Bezpieczne przechowywanie kluczy w skarbcu sprzętowym	46
5.3	Unikatowe certyfikaty urządzeń	46
5.4	Sprawdzanie plików dziennika	47
5.5	System SIEM	47
5.6	PKI	48
5.7	AD FS	48
5.8	Bezpieczna praca kamer IP	48
5.8.1	Tworzenie zaufania przy użyciu certyfikatów	48
5.8.2	Uwierzytelnianie materiału wizyjnego	49
6	Zarządzanie aktualizacjami zabezpieczeń	52
7	Monitorowanie bezpieczeństwa	53
8	Bezpieczne usuwanie i wycofywanie z eksploatacji	54
9	Informacje dodatkowe	55
	Słowniczek	56

1 Cel dokumentu i docelowi odbiorcy

Technologia rozwija się z czasem zapierającą dech w piersiach szybkością. Szybki postęp w dziedzinie sztucznej inteligencji (AI) i Internetu Rzeczy (IoT) oraz ich masowe wykorzystanie (AIoT) zmienia profil zagrożenia w produktach i usługach. Ze względu na lepszą łączność zamierzone złośliwe ataki stają się bardziej wykonalne oraz bardziej prawdopodobne. Celem Bosch jest dostarczanie klientom bezpiecznych oraz niezawodnych produktów i usług.

Niniejszy podręcznik powstał, aby pomóc wzmocnić produkty wizyjne IP firmy Bosch w celu lepszego dostosowania się do istniejących już zasad i procedur dotyczących bezpieczeństwa sieci.

Przewodnik ten będzie obejmował:

- Najważniejsze informacje o funkcjach i podstawach urządzeń wizyjnych IP firmy Bosch
- Określone funkcje, które mogą zostać zmienione lub wyłączone
- Określone funkcje, które mogą stać się aktywne i wykorzystane
- Najlepsze procedury odnoszące się do systemów wizyjnych oraz bezpieczeństwa

Ten przewodnik koncentruje się przede wszystkim na wykorzystaniu aplikacji Configuration Manager do wprowadzenia omówionych konfiguracji. W większości przypadków konfiguracje mogą być wykonywane przy użyciu narzędzi BVMS Configuration Client, Configuration Manager oraz wbudowanego interfejsu internetowego urządzenia wizyjnego.

2 Koncepcja i względy bezpieczeństwa

Produkty wizyjne IP stały się powszechne w dzisiejszym środowisku sieciowym i tak jak w przypadku każdego urządzenia IP umieszczonego w sieci, administratorzy IT i menedżerowie ds. bezpieczeństwa mają prawo znać pełen zakres funkcji i możliwości zestawu.

Podczas stosowania urządzeń wizyjnych IP firmy Bosch pierwsza linia zabezpieczeń to te właśnie urządzenia. Nadajniki i kamery firmy Bosch produkowane są w kontrolowanym i bezpiecznym środowisku, które jest ciągle sprawdzane. Urządzenia można zapisywać tylko poprzez wykorzystanie ważnego oprogramowania układowego określonego dla danej serii sprzętu i chipsetu.

Większość urządzeń wizyjnych IP firmy Bosch wyposażonych jest w wbudowany układ zabezpieczeń zapewniający funkcjonalność podobną do inteligentnej karty kryptograficznej SmartCards oraz tzw. Trusted Platform Module bądź w skrócie TPM. Ten czip działa jak sejf dla danych krytycznych, chroniąc certyfikaty, klucze, licencje itd. przed nieautoryzowanym dostępem, nawet jeśli kamera została otwarta w celu uzyskania dostępu.

Urządzenia wizyjne IP firmy Bosch zostały poddane ponad trzydziestu tysiącom testów dotyczących wrażliwości i możliwości przedostania się, przeprowadzonych przez niezależnych dostawców zabezpieczeń. Do tej pory nie powiódł się żaden atak cybernetyczny na odpowiednio zabezpieczone urządzenie.

3 Bezpieczna instalacja

3.1 Serwery i urządzenia pamięci masowej

Wszystkie komponenty serwera (np. serwer BVMS Management Server i Video Recording Manager) oraz urządzenia pamięci masowej powinny być zainstalowane w bezpiecznym miejscu. Dostęp do bezpiecznego obszaru zapewnia się za pomocą systemu kontroli dostępu i powinien on być monitorowany. Grupa użytkowników, która ma dostęp do centralnego serwera, powinna zostać ograniczona do małej grupy osób. Choć serwery i urządzenia pamięci masowej są instalowane w bezpiecznym miejscu, to muszą być chronione przed nieautoryzowanym dostępem.

Patrz

- *Wzmacnianie serwerów, Strona 33*
- *Wzmacnianie pamięci, Strona 32*

3.2 Kamery i urządzenia brzegowe

W przypadku montażu kamer i urządzeń brzegowych należy wybrać bezpiecznie miejsce instalacji i pozycję montażu urządzenia. Idealne miejsce to takie, w którym praca kamery nie może zostać zakłócona w umyślny lub przypadkowy sposób.

4 Bezpieczna konfiguracja

4.1 Przypisywanie adresów IP

Wszystkie urządzenia wizyjne IP firmy Bosch są obecnie fabrycznie skonfigurowane do zaakceptowania adresu IP przesyłanego przez protokół DHCP.

Jeśli w aktywnej sieci, w której zainstalowane jest urządzenie, nie ma żadnego serwera DHCP automatycznie zastosuje ono — jeśli jest uruchomione oprogramowanie układowe w wersji 6.32 lub wyższej — łącze adresu lokalnego w zakresie od 169.254.1.0 do 169.254.254.255 lub 169.254.0.0/16.

Przy oprogramowaniu układowym we wcześniejszych wersjach urządzenie przypisze sobie domyślny adres IP 192.168.0.1.

Istnieje kilka narzędzi, które można wykorzystać do przydzielania adresów IP do urządzeń wizyjnych IP firmy Bosch, np.:

- Bosch Configuration Manager
- BVMS Configuration Client
- BVMS Configuration Wizard

Wszystkie narzędzia programowe umożliwiają równoczesne przypisanie pojedynczego adresu statycznego IPv4 oraz wielu adresów IPv4 do wielu urządzeń. Obejmuje to maskę podsieci i adresowanie bramy domyślnej.

Wszystkie adresy IPv4 i wartości maski podsieci muszą zostać wprowadzone przy użyciu tzw. zapisu dziesiętnego z segmentami oddzielanymi kropkami.

Uwaga!



Jednym z pierwszych etapów ograniczania możliwości wewnętrznych ataków cybernetycznych w sieci wykonywanych przez nieupoważnione podłączone lokalnie urządzenia sieciowe jest ograniczenie dostępnych niewykorzystanych adresów IP. Wykonuje się to przy użyciu protokołu IPAM (IP **A**dress **M**anagement) w połączeniu z podsiecią zakresu używanego adresu IP.

Podsieciowanie jest czynnością wypożyczania bitów z części hosta adresu IP w celu podzielenia dużej sieci na kilka mniejszych. Im więcej wypożyczonych bitów, tym więcej sieci można stworzyć, ale każda sieć będzie obsługiwać mniej adresów hostów.

Sufiks	Hosty	CIDR	Wypożyczone	Kod binarny
.255	1	/32	0	.11111111
.254	2	/31	1	.1111111 0
.252	4	/30	2	.111111 00
.248	8	/29	3	.11111 000
.240	16	/28	4	.1111 0000
.224	32	/27	5	.111 00000
.192	64	/26	6	.11 000000
.128	128	/25	7	. 10000000

W 1993 r. organizacja Internet Engineering Task Force (IETF) wprowadziła nową koncepcję przydzielania bloków adresów IPv4 w sposób bardziej elastyczny niż dotychczas używane adresowanie architektury za pomocą przypisywania do klas. Nowa metoda nazywana jest bezklasową metodą przydzielania adresów IP (Classless Inter-Domain Routing, CIDR) i jest też używana z adresami IPv6.

Sieci klasowe IPv4 są przypisane do klasy A, B i C, z 8, 16 i 24 bitami numerów sieci oraz klasy D, która używana jest do adresowania w trybie Multicast.

Przykład:

Jako łatwy do zrozumienia przykład zostanie użyty scenariusz adresowania klasy C. Domyślna maska podsieci adresu klasy C to 255.255.255.0. Technicznie rzecz biorąc, w przypadku tej nie zostało wykonane podsieciowanie, więc cały ostatni oktet jest dostępny do poprawnego adresowania hosta. Ponieważ pożyczamy bity z adresu hosta, w ostatnim okciecie opcje maski są następujące:

.128, .192, .224, .240, .248 oraz .252.

Podczas korzystania z maski podsieci 255.255.255.240 (4 bity) zostanie utworzonych 16 małych sieci obsługujących 14 adresów hostów w każdej podsieci.

- Identyfikator podsieci 0:
zakres adresu hosta od 192.168.1.1 do 192.168.1.14. Transmitowany adres 192.168.1.15
- Identyfikator podsieci 16:
zakres adresu hosta od 192.168.1.17 do 192.168.1.30. Transmitowany adres 192.168.1.31
- Identyfikatory podsieci :32, 64, 96 itd.

W przypadku większych sieci niezbędna może okazać się większa sieć klasy B lub odpowiednio zdefiniowany blok CIDR.

Przykład:

Przed wdrożeniem wizyjnej sieci zabezpieczeń należy wykonać proste obliczenia, ile urządzeń IP będzie potrzebnych w sieci, aby uwzględnić miejsce na zwiększenie ich liczby w przyszłości:

- 20 wizyjnych stacji roboczych
- 1 serwer centralny
- 1 serwer VRM
- 15 macierzy dyskowych iSCSI
- 305 kamer IP

Łącznie potrzebne są 342 adresy IP

Biorąc pod uwagę obliczoną liczbę 342 adresów IP, będzie potrzebny co najmniej schemat adresów klasy B, aby uwzględnić taką liczbę adresów IP. Użycie domyślnej maski podsieci klasy B 255.255.0.0 umożliwi dostęp do 65 534 dostępnych adresów IP w sieci.

Sieć może być również planowana przy użyciu bloku CIDR z 23 bitami używanymi jako prefiks, zapewniając w ten sposób przestrzeń 512 adresów oraz odpowiednio 510 hostów.

To ryzyko można zmniejszyć przez dzielenie dużej sieci na mniejsze części, czyli tworzenie podsieci, lub określenie bloku CIDR.

Przykład:

	Domyślne	Podsieci
Zakres adresu IP	172.16.0.0 - 172.16.255.255	172.16.8.0 - 172.16.9.255
Maska podsieci	255.255.0.0	255.255.254.0
Zapis CIDR	172.16.0.0/16	172.16.8.0/23
Liczba podsieci	1	128
Liczba hostów	65.534	510
Nadmiar adresów	65.192	168

4.1.1**Zarządzanie DHCP**

IPAM może wykorzystywać DHCP jako potężne narzędzie do kontroli i użytkowania adresów IP w środowisku sieciowym. DHCP można skonfigurować tak, aby wykorzystywać określony zakres adresów IP. Może być również skonfigurowany tak, aby wykluczać zakres adresów.

Podczas korzystania z DHCP najlepsze byłoby skonfigurowanie podczas rozmieszczania urządzeń wizyjnych niewygasających rezerw adresów na podstawie adresu MAC każdego urządzenia.

Uwaga!

Przed użyciem IP Address Management do śledzenia adresów IP najlepszą metodą zarządzania siecią jest ograniczenie dostępu do sieci przez zabezpieczenie portów na przełącznikach krawędziowych, na przykład tylko określony adres MAC może uzyskać dostęp za pośrednictwem określonego portu.

4.2**Konta i hasła użytkowników**

Wszystkie kamery i kodery IP firmy Bosch dysponują trzema wbudowanymi kontami użytkowników:

– **live**

To standardowe konto użytkownika umożliwia dostęp tylko do strumieniowego przesyłania obrazu na żywo.

- **user**
To bardziej zaawansowane konto użytkownika pozwala na dostęp do filmów nagranych i nadawanych na żywo oraz funkcji sterowania kamerami, takich jak sterowanie PTZ. To konto nie pozwala na dostęp do ustawień konfiguracyjnych.
- **service**
To konto administratora zapewnia dostęp do wszystkich menu urządzenia oraz do ustawień konfiguracyjnych.

Do każdego z kont należy przypisać hasło.

Przypisanie hasła jest kluczowym krokiem w ochronie dowolnego urządzenia sieciowego.

Zaleca się, aby hasła były przypisywane do wszystkich zainstalowanych sieciowych urządzeń wizyjnych.



Uwaga!

Dzięki oprogramowaniu układowemu w wersji 6.30 zarządzanie użytkownikami zostało ulepszone, aby zezwalać na logowanie innych użytkowników za pomocą nazw użytkowników z własnymi hasłami. Wcześniejsze poziomy konta odpowiadają teraz poziomom grup użytkowników.

W wersji oprogramowania układowego 6.32 wprowadzono bardziej restrykcyjną politykę dotyczącą haseł (więcej informacji można znaleźć tu: *Przypisywanie haseł za pomocą strony internetowej urządzenia wizyjnego, Strona 12*).

4.2.1

Przypisywanie haseł

Hasła mogą być przypisywane na kilka sposobów, w zależności od rozmiaru systemu dozoru wizyjnego i oprogramowania. W mniejszych instalacjach składających się tylko z kilku kamer hasła można ustawiać przy użyciu strony internetowej urządzenia lub za pomocą programu Bosch Configuration Manager, ponieważ jest przyjazny dla użytkownika dzięki konfiguracji wielu urządzeń oraz kreatora konfiguracji.



Uwaga!

Jak wspomniano wcześniej, ochrona haseł ma kluczowe znaczenie przy zabezpieczeniu danych przed możliwymi atakami cybernetycznymi. Dotyczy to wszystkich urządzeń sieciowych w całej infrastrukturze zabezpieczeń. Większość przedsiębiorstw posiada już zasady dotyczące silnych haseł, ale podczas pracy nad nową instalacją bez żadnych istniejących zasad, należy przestrzegać najlepszych procedur dotyczących ochrony haseł wymienionych poniżej:

- Hasła powinny składać się z 8–12 znaków.
- Hasła powinny zawierać zarówno duże, jak i małe litery.
- Hasła powinny zawierać co najmniej jeden znak specjalny.
- Hasła powinny zawierać co najmniej jedną cyfrę.

Przykład:

Zastosowanie tekstu szyfrującego „to be or not to be” (być albo nie być) oraz podstawowych zasad tworzenia hasła.

- 2be0rnOt!t0Be



Uwaga!

Istnieją pewne ograniczenia dotyczące używania znaków specjalnych: '@', '&', '<', '>', '!' w hasłach ze względu na ich dedykowane znaczenie w XML i innych językach znaczników. Choć interfejs sieciowy je zaakceptuje, inne oprogramowanie do zarządzania i konfiguracji może odmówić akceptacji.

4.2.2

Przypisywanie haseł za pomocą strony internetowej urządzenia wizyjnego

1. Na stronie internetowej urządzenia przejść na stronę **Konfiguracja** .
2. Wybrać menu **Ogólne** i podmenu **Zarządzanie przez użytkownika** (Uwaga: w wersjach oprogramowania układowego wcześniejszych niż 6.30 podmenu **Zarządzanie przez użytkownika** było nazywane **Hasło**).

Podczas pierwszego uruchomienia strony internetowej kamery użytkownik zostanie poproszony o przypisanie haseł w celu zapewnienia minimalnej ochrony.

Dopóki nie zostanie ustawione hasło, monit będzie powtarzany przy każdym ponownym załadowaniu strony internetowej kamery. Kliknięcie **OK** automatycznie przenosi do menu **Zarządzanie przez użytkownika** .

W oprogramowaniu układowym 6.30 istniała możliwość aktywacji pola wyboru **Nie pokazuj...**. Ta opcja została usunięta w wersji 6.32 oprogramowania układowego, aby uniknąć zagrożeń związanych z bezpieczeństwem.

1. Wybrać menu **Zarządzanie przez użytkownika** i wprowadzić oraz potwierdzić żądane hasło dla każdego z trzech kont.
Należy zauważyć, że:
 - Hasła muszą zostać najpierw przypisane na najwyższym poziomie dostępu (**Hasło „service”**).
 - Począwszy od wersji oprogramowania układowego 6.20, nowy wskaźnik o nazwie „miernik siły hasła” podaje wskazówki dotyczące potencjalnej siły hasła. Jest to tylko narzędzie pomocnicze i nie gwarantuje, że hasło odpowiada wymaganiam bezpieczeństwa instalacji.
2. Kliknąć **Ustaw** , aby zapisać zmiany.

Password

Password 'service'	<input type="password" value="••••••••••"/>	Strong
Confirm password	<input type="password"/>	
Password 'user'	<input type="password" value="••••••••••"/>	Medium
Confirm password	<input type="password"/>	
Password 'live'	<input type="password" value="•••••"/>	Weak
Confirm password	<input type="password"/>	
		Set

Wprowadzona z wersją oprogramowania układowego 6.30 funkcja **Zarządzanie przez użytkownika** zapewnia większą elastyczność w tworzeniu nazw użytkowników oraz haseł. Wcześniejsze poziomy konta odpowiadają teraz poziomom grup użytkowników.



User Management

 Please make sure that all users are password protected.

User name	Group	Type	
service	service	Password	 
user	user	Password	 
live	live	Password	 



Dawniejsi użytkownicy nadal używają haseł, które zostały im przypisane przez wcześniejsze oprogramowanie układowe i nie mogą zostać usunięci ani nie zmienia się ich poziom grupy użytkowników.

Hasła można przypisać lub zmienić, klikając na  lub .

W przypadku, gdy nie wszyscy użytkownicy korzystają z ochrony haseł, zostanie wyświetlony komunikat ostrzegawczy.

1. W celu dodania nowego użytkownika kliknąć **Dodaj**.
Pojawi się okno podręczne.
2. Wprowadzić nowe dane uwierzytelniające i przypisać grupę użytkowników.
3. Kliknąć **Ustaw**, aby zapisać zmiany.




Uwaga!

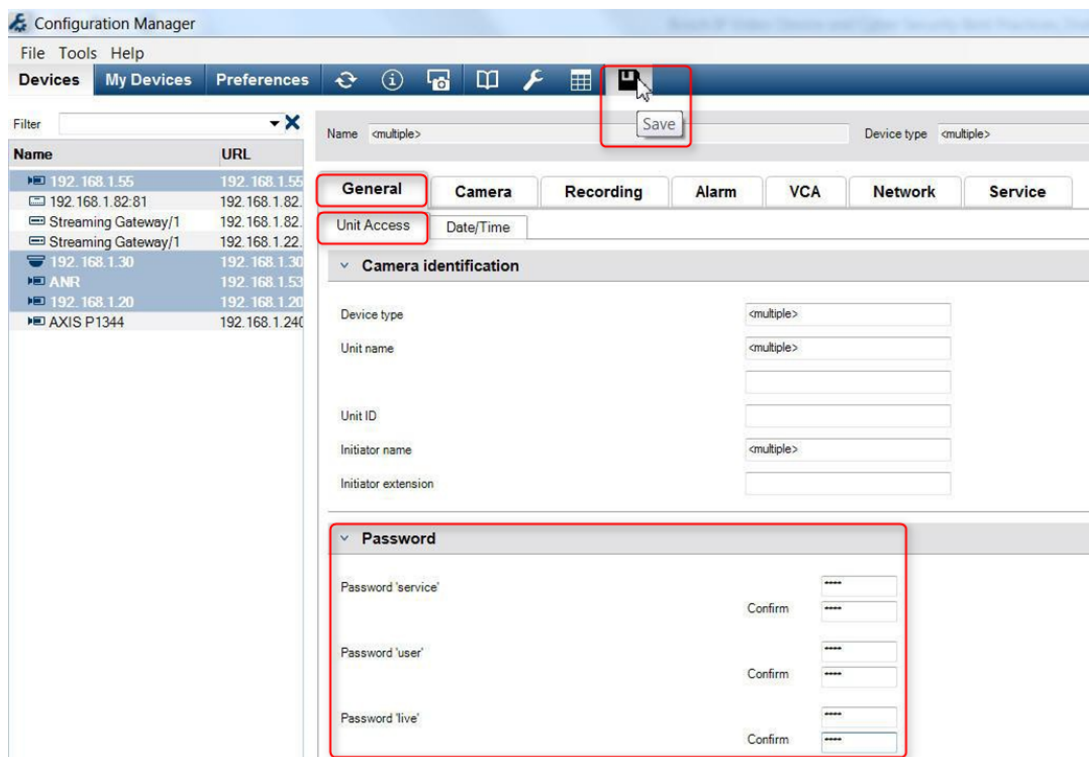
W wersji oprogramowania układowego 6.32 zastosowano także surowszą politykę dotyczącą haseł.
Hasła wymagają teraz co najmniej 8 znaków.

4.2.3

Przypisywanie haseł za pomocą programu Configuration Manager

Korzystając z Bosch Configuration Manager, hasła można łatwo przypisać zarówno do pojedynczych, jak i wielu urządzeń jednocześnie.

1. W programie Configuration Manager wybrać jedno lub więcej urządzeń.
2. Wybrać kartę **Ogólne**, a następnie **Dostęp do urządzenia**.
3. W menu **Hasło** wprowadzić i potwierdzić żądane hasło dla każdego z trzech kont (**Hasło „service”**, **Hasło „user”** oraz **Hasło „live”**).
4. Kliknąć , aby zapisać zmiany.



W większych instalacjach, które są zarządzane przez system BVMS lub Video Recording Manager zainstalowane w rozwiązaniach służących do zapisu, globalne hasła mogą być stosowane do wszystkich urządzeń wizyjnych IP dołączanych do systemu. Pozwala to na łatwe zarządzanie i zapewnia standardowy poziom bezpieczeństwa w całym sieciowym systemie wizyjnym.

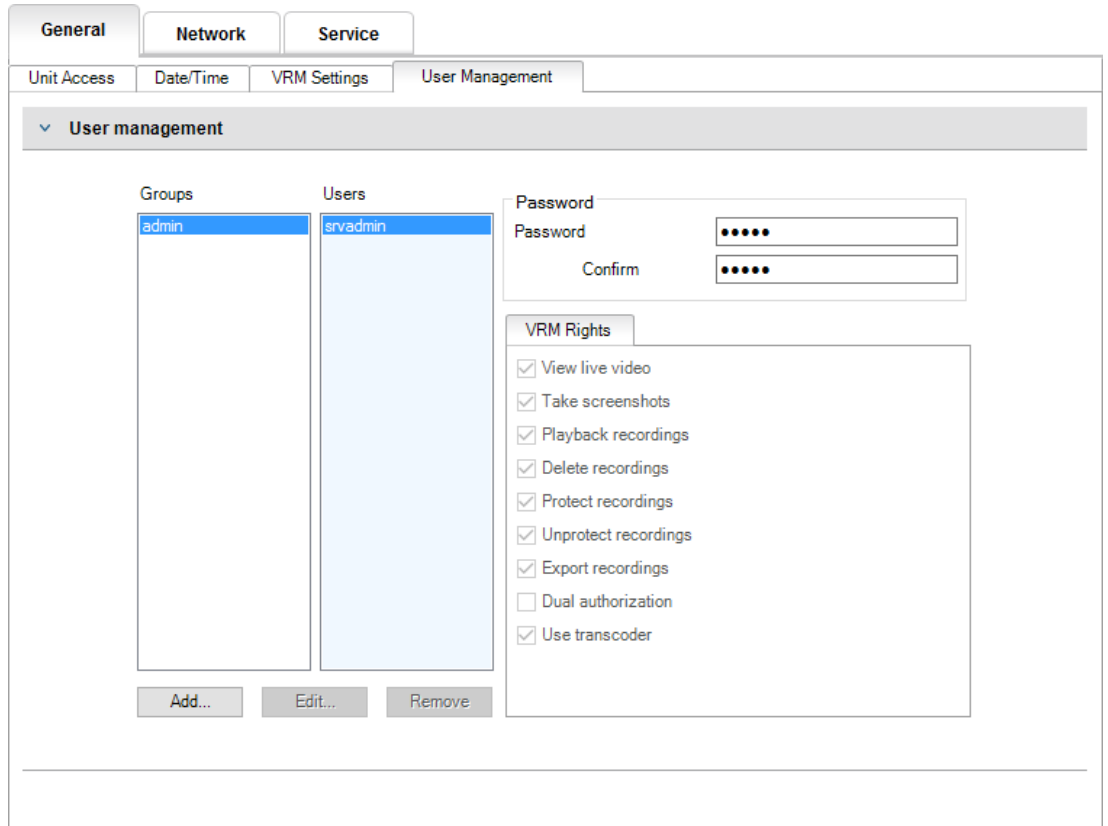
4.2.4

Przypisywanie haseł dla autonomicznej instalacji VRM

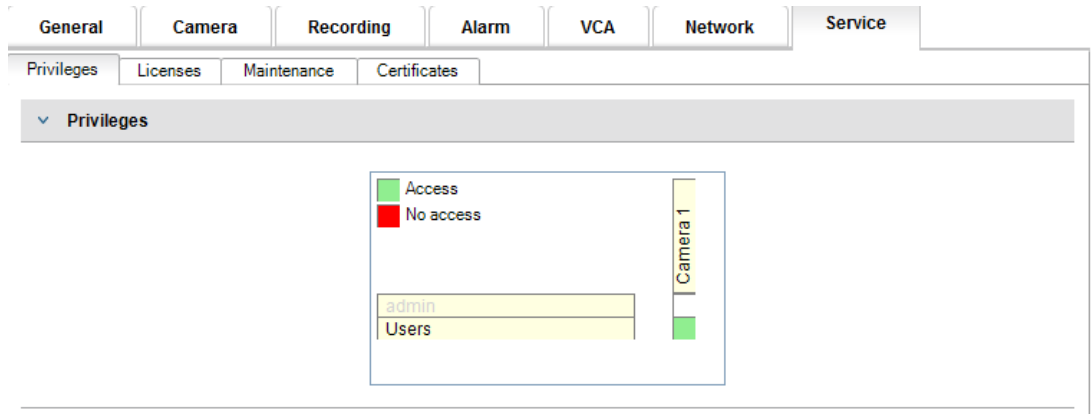
Program Video Recording Manager umożliwia zarządzanie użytkownikami w celu zwiększenia elastyczności i bezpieczeństwa.

Domyślnie nie ma haseł przypisanych do któregoś z kont użytkowników. Przypisanie hasła jest kluczowym krokiem w ochronie dowolnego urządzenia sieciowego. Zalecane jest przypisanie haseł do wszystkich zainstalowanych sieciowych urządzeń wizyjnych.

To samo dotyczy się użytkowników programu Video Recording Manager.



Ponadto członkowie grupy użytkowników mogą mieć dostęp do określonych kamer i uprawnień. Można zatem uzyskać szczegółowe zarządzanie użytkownikami.



4.2.5 Przypisywanie haseł za pomocą BVMS (na DIVAR IP lub w rozwiązaniu autonomicznym)

Ochrona hasła urządzenia

Kamery i nadajniki zarządzane przez rozwiązanie BVMS mogą być zabezpieczone hasłem przed nieautoryzowanym dostępem.

Hasła dla wbudowanych kont użytkowników nadajników/kamer można skonfigurować za pomocą BVMS Configuration Client.

Aby ustawić hasło dla wbudowanych kont użytkowników w systemie BVMS Configuration Client:

1. W drzewie urządzeń wybrać żądany nadajnik.
2. Kliknąć prawym przyciskiem myszy na nadajnik **Zmień hasło....**
3. Wprowadzić hasło dla trzech wbudowanych kont użytkowników live, user i service.

Domyślna ochrona hasłem

Wersja 5.0 i nowsze systemu BVMS zapewniają możliwość wdrożenia globalnych haseł na wszystkich urządzeniach w systemie wizyjnym obejmującym do 2000 kamer IP. Ta funkcja może być dostępna zarówno za pośrednictwem systemu BVMS Configuration Wizard pracującego z rozwiązaniami zapisu DIVAR IP 3000 lub DIVAR IP 7000, albo za pośrednictwem systemu BVMS Configuration Client w dowolnym systemie.

Aby uzyskać dostęp do menu globalnych haseł w systemie BVMS Configuration Client:

1. W menu **Urządzenie** kliknąć **Ochrona urządzeń przy użyciu hasła domyślnego...**
2. W polu **Globalne hasło domyślne** wprowadź hasło i wybierz polecenie **Wymuś ochronę hasłem przy aktywacji**.

Po zapisaniu zmian i aktywacji systemu wprowadzone hasło zostanie przypisane do konta live, user i service wszystkich urządzeń, w tym konta administratora programu Video Recording Manager.



Uwaga!

Jeśli urządzenia mają już hasła zapisane na dowolnym z kont, nie zostaną one zastąpione. Na przykład jeśli hasło jest ustawione dla service, ale nie dla live i user, hasła globalne zostaną skonfigurowane tylko dla kont live i user.

Konfiguracja rozwiązania BVMS i ustawienia VRM

Domyślnie rozwiązanie BVMS System korzysta z wbudowanego konta administracyjnego **srvadmin**, aby połączyć się z programem Video Recording Manager z wykorzystaniem ochrony za pomocą hasła. Aby uniknąć nieupoważnionego dostępu do programu Video Recording Manager, konto administracyjne **srvadmin** jest chronione hasłem złożonym.

W celu zmiany hasła konta **srvadmin** w BVMS Configuration Client:

1. W drzewie urządzeń wybrać urządzenie VRM.
2. Kliknąć prawym przyciskiem myszy na urządzenie VRM, a następnie kliknąć **Zmień hasło systemu VRM**.
Zostanie wyświetlone okno dialogowe **Zmień hasło....**
3. Wprowadzić nowe hasło dla konta **srvadmin** i kliknąć **OK**.

Szyfrowanie komunikacji wychodzącej do kamer

Począwszy od wersji 7.0 BVMS obraz na żywo i kontrola komunikacji pomiędzy kamerą a BVMS Operator Client, Configuration Client, Management Server i Video Recording Manager mogą być szyfrowane.

Po włączeniu bezpiecznego połączenia w oknie dialogowym **Edytuj nadajnik** serwer BVMS program Operator Client i Video Recording Manager będą używać bezpiecznego połączenia HTTPS w celu łączenia się z kamerą lub nadajnikiem.

Ten używany wewnętrznie ciąg połączenia BVMS zmieni się z rcpp://a.b.c.d (zwykłe połączenie RCP + z portem 1756) na https://a.b.c.d. (połączenie HTTPS z portem 443).

W starszych urządzeniach, które nie obsługują HTTPS, ciąg połączeń pozostaje niezmieniony (RCP+).

Przy wybraniu komunikacji HTTPS komunikacja będzie wykorzystywać HTTPS (TLS) w celu szyfrowania całej komunikacji sterującej oraz obrazu za pośrednictwem mechanizmu szyfrowania w urządzeniu. Podczas korzystania z TLS każde sterowanie komunikacją i obrazem HTTPS jest szyfrowane kluczem szyfrującym AES o długości do 256 bitów.

Aby umożliwić szyfrowaną komunikację w BVMS Configuration Client:

1. W drzewie urządzeń wybrać żądany nadajnik/kamerę.
2. Kliknąć prawym przyciskiem myszy na nadajnik/kamerę i kliknąć **Edytuj nadajnik**.
3. W oknie dialogowym **Edytuj nadajnik** włączyć **Zabezpiecz połączenie**.
4. Zapisać i uaktywnić konfigurację.

Po włączeniu bezpiecznego połączenia z nadajnikiem inne protokoły mogą zostać wyłączone (patrz *Ogólne wykorzystanie portów sieciowych i transmisja sygnału wizyjnego, Strona 17*).



Uwaga!

BVMS domyślnie obsługuje tylko port 443 HTTPS. Użycie innych portów nie jest możliwe.

4.3

Wzmacnianie dostępu do urządzenia

Wszystkie urządzenia wizyjne IP firmy Bosch wyposażone są we wbudowane wielofunkcyjne strony internetowe. Strony internetowe specyficzne dla danego urządzenia obsługują zarówno funkcję odtwarzania, jak i oglądania na żywo, a także określone ustawienia konfiguracyjne, których nie można uzyskać za pośrednictwem systemu zarządzania sygnałem wizyjnym.

Wbudowane konta użytkowników działają jako dostęp do różnych sekcji dedykowanych stron internetowych. Choć dostęp do strony internetowej nie może być całkowicie wyłączony za pośrednictwem samej tej strony — może zostać do tego użyty program Configuration Manager — istnieje kilka metod maskowania obecności urządzenia, ograniczenia dostępu i zarządzania portami wizyjnymi.

4.3.1

Ogólne wykorzystanie portów sieciowych i transmisja sygnału wizyjnego

Wszystkie urządzenia wizyjne IP firmy Bosch do wykrywania, sterowania i komunikacji wykorzystują protokół Remote Control Protocol Plus (RCP+). RCP+ to zastrzeżony protokół firmy Bosch wykorzystujący określone porty statyczne do wykrywania i komunikacji z urządzeniami wizyjnymi IP firmy Bosch — 1756, 1757 i 1758. Podczas pracy z rozwiązaniem BVMS lub systemem zarządzania sygnałem wizyjnym innych firm zintegrowanym z urządzeniami wizyjnymi IP firmy Bosch za pośrednictwem pakietu Bosch VideoSDK wymienione porty muszą być dostępne w sieci, aby urządzenia wizyjne IP działały poprawnie.

Sygnał wizyjny można przesyłać strumieniowo z urządzeń na kilka sposobów: UDP (dynamiczny), HTTP (80) lub HTTPS (443).

Można modyfikować protokół HTTP oraz użycie portu HTTPS (zobacz *Stosowanie portu HTTP, HTTPS i portu wizyjnego*, Strona 18). Przed dokonaniem jakichkolwiek modyfikacji portów należy skonfigurować żadaną formę komunikacji z urządzeniem. Dostęp do menu komunikacji można uzyskać za pomocą programu Configuration Manager.

1. W programie Configuration Manager wybrać żądane urządzenie.
2. Wybrać kartę **Ogólne**, a następnie **Dostęp do urządzenia**.
3. Zlokalizować część **Dostęp do urządzenia** strony.



4. Z listy **Protokół** wybrać żądany protokół:
 - RCP+
 - HTTP (domyślny)
 - HTTPS

Jeśli wybrano komunikację HTTPS, komunikacja pomiędzy Configuration Manager i urządzenia wizyjnymi będzie korzystać z HTTPS (TLS) do zaszyfrowania ładunku z kluczem szyfrującym AES o długości do 256 bitów. Jest to darmowa podstawowa cecha. Podczas korzystania z TLS każda komunikacja kontrolna HTTPS oraz obraz są szyfrowane za pomocą mechanizmu szyfrowania w urządzeniu.



Uwaga!

Szyfrowanie jest specyficzne dla „ścieżki transmisji”. Po odebraniu obrazu przez oprogramowanie dekodujące bądź dekodier strumień zostaje odszyfrowany na stałe.

4.3.2

Minimalna wersja protokołu TLS

Niektóre starsze wersje klientów mogą wymagać użycia starszych i mniej bezpiecznych wersji protokołu TLS. Jeśli to możliwe, zdefiniuj minimalną wymaganą wersję protokołu TLS tak, aby klienci nie zmuszali urządzenia do przejścia w mniej bezpieczny tryb dostępu.

Wybierz jako wersję minimalną najwyższą możliwą wersję protokołu TLS.



Uwaga!

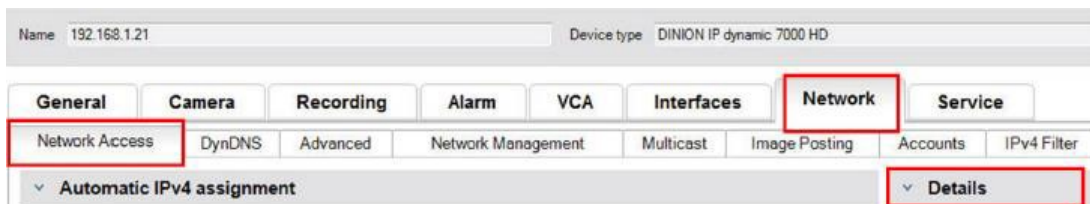
Określając minimalny poziom bezpieczeństwa dostępu do urządzeń z oprogramowania klienta, należy upewnić się, że wszystkie porty i protokoły, które pozwalają na niższy poziom dostępu, są wyłączone lub zablokowane na urządzeniach.

4.3.3

Stosowanie portu HTTP, HTTPS i portu wizyjnego

Stosowanie portu HTTP i HTTPS na wszystkich urządzeniach może zostać zmienione lub wyłączone. Szyfrowana komunikacja może być wymuszona przez wyłączenie portu RCP +, a także portu HTTP, co wymusi szyfrowanie na całej komunikacji. Jeśli używanie portu HTTP jest wyłączone, port HTTPS pozostanie niezmieniony, a wszelkie próby wyłączenia nie powiodą się.

1. W programie Configuration Manager wybrać żądane urządzenie.
2. Wybrać kartę **Sieć**, a następnie **Dostęp do sieci**.
3. Zlokalizować dział **Szczegóły** na stronie.



4. W dziale **Szczegóły** zmienić porty wyszukiwarki HTTP i HTTPS oraz port RCP+, używając menu rozwijanego:
 - Modyfikacja portu przeglądarki HTTP: 80 lub porty 10000 do 10100
 - HTTPS modyfikacja portu przeglądarki: 443 lub porty od 10443 do 10543
 - Port RCP+ 1756: **Włączony** lub **Wyłączony**

Uwaga!

Jeśli w wersji oprogramowania układowego 6.1x port HTTP jest wyłączony, a zostanie podjęta próba uzyskania dostępu do strony sieciowej urządzenia, żądanie zostanie skierowane do portu HTTPS, który jest obecnie zdefiniowany.

Funkcja przekierowania została pominięta w wersji oprogramowania układowego 6.20 i wyższych. Jeśli port HTTP jest wyłączony, a port HTTPS został zmodyfikowany, aby korzystać z portu innego niż 443, dostęp do stron internetowych można uzyskać tylko przez nawigację do adresu IP urządzenia oraz przypisanego portu.



Przykład:

https://192.168.1.21:10443. Wszelkie próby nawiązania połączenia z domyślnym adresem nie powiodą się.

4.3.4

Oprogramowanie wideo i wybór portu

Dostosowanie tych ustawień będzie miało również wpływ na to, jaki port jest wykorzystywany do transmisji sygnału wizyjnego podczas korzystania z oprogramowania do zarządzania sygnałem wizyjnym w sieci LAN.

Jeśli wszystkie urządzenia wizyjne IP ustawione są na przykład na port HTTP 10000, a system BVMS Operator Client jest skonfigurowany do tunelowania protokołu TCP, wówczas wszystkie transmisje sygnału wizyjnego w sieci będą realizowane na porcie HTTP 10000.



Uwaga!

Zmiany ustawień portów w urządzeniach muszą odpowiadać ustawieniom w systemie zarządzania i jego elementach, jak również w klientach.



Uwaga!

Najlepsze procedury mogą się różnić w zależności od scenariusza wdrażania i celów związanych z bezpieczeństwem instalacji. Wyłączenie i przekierowanie stosowania protokołu HTTP lub HTTPS ma swoje zalety. Zmiana portu w obu protokołach może pomóc w uniknięciu dostarczania informacji do narzędzi sieciowych, takich jak NMAP (Network Mapper, darmowy skaner zabezpieczeń). Aplikacje, takie jak NMAP, są zazwyczaj używane jako narzędzia rozpoznawcze w celu wykrywania słabych punktów w dowolnym urządzeniu w sieci. Ta technika w połączeniu z implementacją silnego hasła zwiększa całkowite bezpieczeństwo systemu.

4.3.5

Tunelowanie SSH

W przypadku zdalnego dostępu do urządzenia za pomocą programu BVMS Operator Client przez sieci publiczne, rozwiązanie BVMS umożliwia zabezpieczenie (zaszyfrowanie) komunikacji poprzez wykorzystanie tunelowania Secure Shell (SSH).

Tunelowanie SSH tworzy zaszyfrowany tunel ustanowiony przez połączenia gniazda protokołu SSH. Takiego zaszyfrowanego tunelu można używać do transportu zarówno ruchu szyfrowanego, jak i niezaszyfrowanego. Implementacja protokołu SSH firmy Bosch również korzysta z protokołu Omni-Path będącego wysoko wydajnym protokołem komunikacyjnym o małym opóźnieniu opracowanym przez firmę Intel.

Więcej informacji na temat konfiguracji usługi SSH w rozwiązaniu BVMS można znaleźć w dokumentacji rozwiązania BVMS.

Więcej informacji na temat konfiguracji systemu DIVAR IP pod kątem bezpiecznego zdalnego dostępu z rozwiązaniem BVMS Operator Client można znaleźć w dokumentacji systemu DIVAR IP.

4.3.6

Dostęp Telnet

Telnet to protokół warstwy aplikacji, który zapewnia komunikację z urządzeniami za pośrednictwem wirtualnej sesji terminalowej do celów konserwacji i rozwiązywania problemów. Wszystkie urządzenia wizyjne IP firmy Bosch są zgodne ze standardami Telnet, a obsługa protokołu Telnet jest włączona domyślnie w wersjach oprogramowania układowego do 6.1x. Począwszy od wersji oprogramowania układowego 6.20, port Telnet jest domyślnie wyłączony.



Uwaga!

Od 2011 roku wzrosła liczba ataków cybernetycznych przy użyciu protokołu Telnet. Zgodnie z aktualną praktyką należy wyłączyć obsługę protokołu Telnet na wszystkich urządzeniach, dopóki nie zajdzie potrzeba konserwacji czy rozwiązywania problemów.

1. W programie Configuration Manager wybrać żądane urządzenie.
2. Wybrać kartę **Sieć**, a następnie **Dostęp do sieci**.
3. Zlokalizować dział **Szczegóły** na stronie.



4. W dziale **Szczegóły** wybrać **Obsługa Telnet Włączony** lub **Wyłączony**, używając menu rozwijanego.



Uwaga!

Począwszy od wersji oprogramowania układowego 6.20, protokół Telnet jest obsługiwany przez tak zwane gniazda sieciowe, które używają bezpiecznych połączeń HTTPS. Gniazda sieciowe nie korzystają ze standardowego portu Telnet i zapewniają bezpieczny sposób dostępu do interfejsu wiersza polecenia urządzeń IP, jeśli jest to wymagane.

4.3.7

RTSP: Protokół transmisji strumieniowej w czasie rzeczywistym

Protokół transmisji strumieniowej w czasie rzeczywistym (RTSP) jest podstawowym składnikiem sygnału wizyjnego wykorzystywanym przez protokół ONVIF w celu przesyłania strumienia wizyjnego, jak również sterowania urządzeniami systemów zgodnych z ONVIF. RTSP jest wykorzystywany również przez zastosowania z zakresu monitoringu innych firm do

podstawowych funkcji transmisji strumieniowej, a w niektórych przypadkach może być używany do rozwiązywania problemów z urządzeniami i siecią. Wszystkie urządzenia wizyjne IP firmy Bosch mogą dostarczać strumienie za pomocą protokołu RTSP.

Usługi RTSP można łatwo modyfikować za pomocą programu Configuration Manager.

1. W programie Configuration Manager wybrać żądane urządzenie.
2. Wybrać kartę **Sieć**, a następnie **Zaawansowane**.



3. Zlokalizować na stronie dział **RTSP**.
4. W menu rozwijanym **Złącze RTSP** wyłączyć lub zmodyfikować usługę RSTP:
 - Domyślny port RTSP: 554
 - Zmiana portu RTSP: 10554 do 10664

Uwaga!

Odnotowano niedawne doniesienia o cyberatakach wykorzystujących bufor przepełnienia stosu RTSP. Ataki zostały specjalnie skierowane na konkretne urządzenia dostawców. Najlepszym rozwiązaniem byłoby wyłączenie usługi, jeśli nie jest ona wykorzystywana przez zgodny system zarządzania sygnałem wizyjnym ONVIF lub przesyłanie strumieniowe w czasie rzeczywistym.

Alternatywnie oraz gdy klient odbierający to umożliwia, komunikacja RTSP może być tunelowana przy użyciu połączenia HTTPS, co jest jedynym sposobem na przesyłanie zaszyfrowanych danych RTSP.



Uwaga!

Więcej szczegółów na temat protokołu RTSP można znaleźć w dokumencie Uwaga dotycząca aplikacji *Korzystanie z RTSP za pomocą urządzeń VIP firmy Bosch* w internetowym katalogu produktów firmy Bosch Security Systems dostępnym pod następującym adresem: https://resources-boschsecurity-cdn.azureedge.net/public/documents/RTSP_VIP_Application_note_enUS_9007200806939915.pdf



4.3.8

UPnP: Universal Plug and Play

Urządzenia wizyjne IP firmy Bosch są w stanie komunikować się z urządzeniami sieciowymi za pośrednictwem **UPnP**. Funkcja ta jest wykorzystywana przede wszystkim w mniejszych systemach z kilkoma kamerami, w których kamery pojawiają się automatycznie w katalogu sieciowym komputera, dzięki czemu można je łatwo znaleźć. Tak robią dla każdego urządzenia w sieci.

UPnP może zostać wyłączony przy użyciu Configuration Manager.

1. W programie Configuration Manager wybrać żądane urządzenie.
2. Wybrać kartę **Sieć**, a następnie **Zarządzanie siecią**.



3. Zlokalizować na stronie dział **UPnP**.
4. W menu rozwijanym **UPnP** wybrać **Wyłącz**, aby dezaktywować **UPnP**.

**Uwaga!**

Zaleca się nie używać **UPnP** w dużych instalacjach z uwagi na dużą liczbę zgłoszeń do rejestracji oraz potencjalne ryzyko niepożądanego dostępu lub ataku.

4.3.9**Multicasting**

Wszystkie urządzenia wizyjne IP firmy Bosch są w stanie dostarczyć zarówno sygnał wizyjny typu Multicast on Demand (Na żądanie), jak i Multicast Streaming (Na żywo). Jeżeli transmisja obrazu w trybie Unicast jest bazą docelową, to transmisja w trybie Multicast jest oparta na źródłach i może powodować problemy związane z bezpieczeństwem na poziomie sieci, w tym dotyczące kontroli dostępu grupowego, zaufania centrum grupy i zaufania routera. Mimo że kwestia konfiguracji routera przekracza zakres tego przewodnika, istnieje rozwiązanie zabezpieczające, które można wdrożyć z samego urządzenia wizyjnego IP.

Określanie zakresu czasowego TTL (czas życia) określa, gdzie i jak daleko ruch w trybie Multicast może przepływać w obrębie sieci, przy czym każdy z nich zmniejsza TTL o jeden. Podczas konfigurowania urządzeń wizyjnych IP do używania funkcji Multicast pakiet TTL urządzenia może zostać modyfikowany.

1. W programie Configuration Manager wybrać żądane urządzenie.
2. Wybrać kartę **Sieć**, a następnie **Multicast**.
3. Zlokalizować na stronie dział **Czas przesyłania w trybie multicastingu**.
4. Dostosować ustawienia **Czas przesyłania pakietu** przy użyciu następujących wartości TTL i limitu zakresu:
 - Wartość TTL 0 = ograniczona do hosta lokalnego
 - Wartość TTL 1 = ograniczona do tej samej podsieci
 - Wartość TTL 15 = ograniczona do tej samej witryny
 - Wartość TTL 64 (domyślna) = ograniczona do tego samego regionu
 - Wartość TTL 127 = na całym świecie
 - Wartość TTL 191 = na całym świecie z ograniczoną szerokością pasma
 - Wartość TTL 255 = dane nieograniczone

General	Camera	Recording	Alarm	VCA	Interfaces	Network	Service	
Network Access	DynDNS	Advanced	Network Management	Multicast	Image Posting	Accounts	IPv4 Filter	Encryption
Multicast Stream 1								
Enable		Multicast Address	Port	Streaming				
Video 1 <input type="checkbox"/>		0.0.0.0	60010	<input type="checkbox"/>				
Multicast Stream 2								
Enable		Multicast Address	Port	Streaming				
Video 1 <input checked="" type="checkbox"/>		226.3.209.201	60020	<input type="checkbox"/>				
Multicast TTL								
Packet TTL		64						

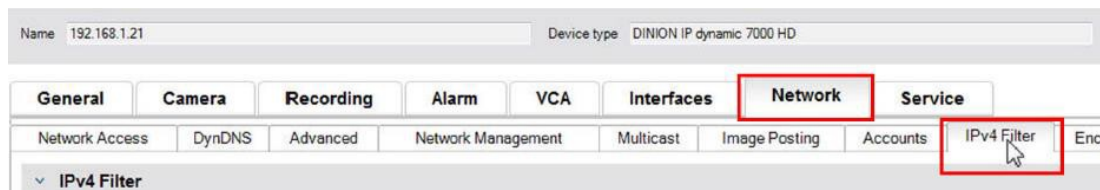
**Uwaga!**

W przypadku danych nadzoru wizyjnego najlepszą praktyką byłoby poziom ustawień TTL 15 ograniczonych do tej samej witryny. Jeśli natomiast znana jest dokładna maksymalna liczba przeskoków, można użyć jej jako wartości TTL.

4.3.10 Filtrowanie IPv4

Można ograniczyć dostęp do dowolnego urządzenia wizyjnego IP firmy Bosch za pomocą funkcji zwanej filtrowanie IPv4. Filtrowanie IPv4 wykorzystuje podstawowe zasady sieci w celu zdefiniowania maksymalnie dwóch dozwolonych zakresów adresów IP. Po zdefiniowaniu blokuje dostęp z dowolnego adresu IP poza tymi zakresami.

1. W programie Configuration Manager wybrać żądane urządzenie.
2. Wybrać kartę **Sieć**, a następnie **Filtr IPv4**.



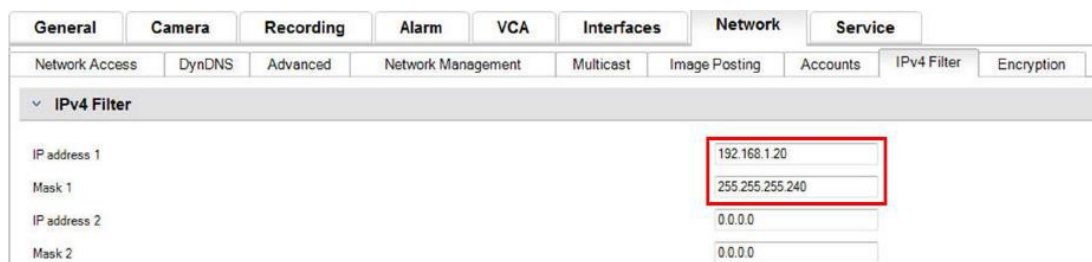
Uwaga!



Aby pomyślnie skonfigurować tę funkcję, należy dysponować podstawową wiedzą na temat sieci lub uzyskać dostęp do kalkulatora sieci. Niepoprawne ustawienie może ograniczyć dostęp do samego urządzenia i w celu odzyskania dostępu może być konieczne przywrócenie ustawień fabrycznych.

3. Aby dodać regułę filtru, należy wykonać dwa wpisy:
 - Wprowadzić podstawowy adres IP, który należy do utworzonej reguły sieci. Podstawowy adres IP określa, która sieć ma być dozwolona i musi mieścić się w wymaganym zakresie.
 - Wpisać maskę sieci definiującą adresy IP, komunikację z którymi zaakceptuje urządzenie wizyjne IP.

W poniższym przykładzie został wprowadzony **Adres IP 1** 192.168.1.20 oraz **Maska 1** 255.255.255.240. To ustawienie ogranicza dostęp urządzeniom mieszczącym się w zdefiniowanym zakresie adresów IP od 192.168.1.1 do 192.168.1.31.



Podczas korzystania z **Filtr IPv4** przyszłe urządzenia będą skanowane za pośrednictwem protokołu RCP+, ale dostęp do ustawień konfiguracji i sygnału wizyjnego nie jest możliwy za pośrednictwem klientów nienależących do dozwolonego zakresu adresów IP. Obejmuje to dostęp za pośrednictwem przeglądarki internetowej.

Urządzenie wizyjne IP nie musi znajdować się w dopuszczalnym zakresie adresów.

Uwaga!



Na podstawie konfiguracji systemu korzystanie z opcji **Filtr IPv4** może zmniejszyć niepożądaną widoczność urządzeń w sieci. Podczas włączania tej funkcji, upewnij się, że ustawienia zostały zapisane do późniejszego wykorzystania.

Należy uwzględnić, że urządzenie będzie nadal dostępne za pośrednictwem IPv6, więc filtrowanie IPv4 ma sens jedynie w sieciach opartych wyłącznie na IPv4.

4.3.11

SNMP

Protokół SNMP (Simple Network Management Protocol) jest powszechnie stosowany do monitorowania stanu systemu. Taki system monitorowania zazwyczaj posiada centralny serwer zarządzania, który gromadzi wszystkie dane ze zgodnych komponentów i urządzeń systemu. SNMP udostępnia dwie metody uzyskania stanu systemu:

- Serwer zarządzania siecią może sprawdzać stan urządzenia przy użyciu żądań SNMP.
- Urządzenia mogą aktywnie powiadamiać serwer zarządzania siecią o stanie systemu w przypadku błędu lub warunków alarmowych, wysyłając pułapki SNMP do serwera SNMP. Takie pułapki muszą być skonfigurowane wewnątrz urządzenia.

SNMP umożliwia także konfigurację niektórych zmiennych wewnątrz urządzeń i komponentów. Informacje, które wiadomości obsługuje urządzenie oraz które pułapki może wysłać, pochodzą z Management Information Base, tak zwanego pliku MIB dostarczanego wraz z produktem, który ułatwia integrację z systemem monitorowania sieci.

Istnieją trzy różne wersje protokołu SNMP:

- SNMP wersja 1
SNMP wersja 1 (SNMPv1) to początkowa implementacja protokołu SNMP. Jest powszechnie używany i stał się standardowym protokołem do monitorowania i zarządzania siecią.
Ale SNMPv1 jest zagrożony ze względu na brak zabezpieczeń. Używa tylko *ciąg znaków wspólnoty* jako rodzaju haseł, które są przekazywane za pomocą zwykłego tekstu. Tak więc SNMPv1 jest używany tylko wtedy, gdy można mieć pewność, że sieć jest fizycznie chroniona przed nieautoryzowanym dostępem.
- SNMP wersja 2
SNMP wersja 2 (SNMPv2) obejmowała między innymi poprawę bezpieczeństwa i poufności, a także wprowadziła zbiorcze pobieranie dużych ilości danych w pojedynczym żądaniu. Jednak takie podejście do bezpieczeństwa zostało uznane za zbyt złożone, co utrudnia jego odbiór.
Dlatego wkrótce został on zastąpiony wersją SNMPv2c, która odpowiada protokołowi SNMPv2, ale bez jego kontrowersyjnego modelu zabezpieczeń, zamiast tego wracając do metody wspólnotowej z protokołu SNMPv1 i co za tym idzie z brakiem bezpieczeństwa.
- SNMP wersja 3
SNMP wersja 3 (SNMPv3) przede wszystkim zwiększa bezpieczeństwo oraz zdalne ulepszanie konfiguracji. Obejmują one ulepszenia dotyczące poufności dzięki szyfrowaniu pakietów, integralności wiadomości i uwierzytelnianiu.
Odnosi się również do wdrażania protokołu SNMP na szeroką skalę.

Uwaga!

Zarówno SNMPv1, jak i SNMPv2c są podatne na zagrożenia ze względu na brak zabezpieczeń. Używają tylko ciągu znaków wspólnoty jako rodzaju haseł, które są przekazywane za pomocą zwykłego tekstu.

Tak więc SNMPv1 lub SNMPv2c powinny być używane tylko wtedy, gdy można mieć pewność, że sieć jest fizycznie chroniona przed nieautoryzowanym dostępem.

Kamery firmy Bosch obsługują obecnie tylko SNMPv1. Należy upewnić się, że funkcja SNMP jest wyłączona, jeśli jej nie używasz.



4.3.12

Bezpieczne ramy czasowe

Dodatkowo do protokołu czasowego i protokołu SNTP, które są protokołami niezabezpieczonymi, został wprowadzony trzeci tryb dla klienta Timeserver z oprogramowaniem układowym 6.20, przy użyciu protokołu TLS. Ta metoda jest również powszechnie znana jako *TLS-Date*.

W tym trybie dowolny serwer HTTPS może zostać użyty jako serwer czasowy. Wartość czasu jest pochodną efektu ubocznego, zwanego procesem uzgadniania HTTPS. Transmisja jest zabezpieczona przez TLS. Opcjonalny certyfikat główny dla serwera HTTPS można załadować do magazynu certyfikatów kamery w celu uwierzytelnienia serwera.



Uwaga!

Należy upewnić się, że wprowadzony adres IP serwera czasu ma stabilną i niezawodną bazę.

4.3.13

Usługi chmurowe

Wszystkie urządzenia wizyjne IP firmy Bosch mogą komunikować się z usługami Bosch opartymi na chmurze, takimi jak np. Remote Portal. W zależności od regionu wdrożenia umożliwi to urządzeniom wizyjnym IP używanie usług, takich jak Remote Device Management lub Cloud VMS, w celu przesyłania alarmów i innych danych do stacji centralnej.

Więcej informacji można znaleźć w bazie wiedzy Bosch Building Technologies:

<https://community.boschsecurity.com>.

Istnieją trzy tryby działania usług w chmurze:

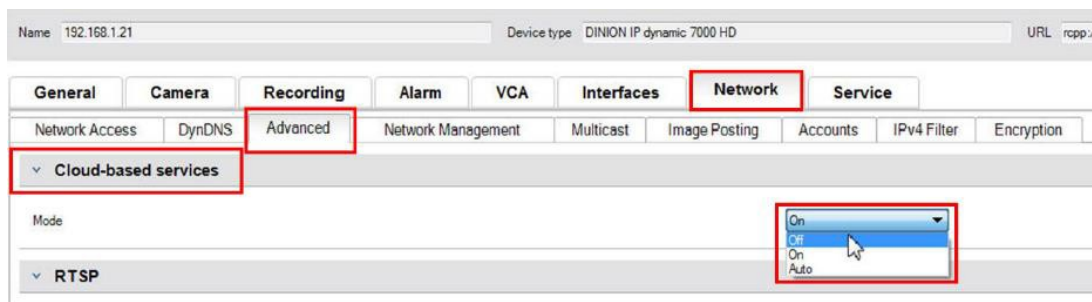
- **Włączone:**
Urządzenie wizyjne będzie stale wyszukiwać serwer chmury.
- **Automatyczne** (domyślny):
Urządzenie wizyjne będzie próbowało kilka razy połączyć się z serwerem chmury i w przypadku niepowodzenia przestanie podejmować próby połączenia z serwerem.

– **Wyłączone:**

Nie będą podejmowane próby wyszukiwania.

Usługi w chmurze można łatwo wyłączyć w programie Configuration Manager.

1. W programie Configuration Manager wybrać żądane urządzenie.
2. Wybierz obszar **Sieć**, a następnie wybierz kartę **Zaawansowane**.
3. Zlokalizuj sekcję **Usługa chmurowa** i wybierz z listy opcję **Off** (Wyłącz).



Uwaga!

W przypadku korzystania z usług chmurowych firmy Bosch należy zachować konfigurację domyślną.

We wszystkich innych przypadkach przełączyć tryb usług w chmurze na **Off** (Wyłącz).

4.4

Wzmacnianie kamer IP

Kamery IP Bosch są dostarczane z domyślną konfiguracją, która umożliwi łatwą integrację z różnymi środowiskami.

W pewnych środowiskach docelowych o ustalonym poziomie bezpieczeństwa może być konieczna zmiana niektórych ustawień kamery w celu zwiększenia bezpieczeństwa cybernetycznego oraz ochrony danych.

Mogą jednak zachodzić ograniczenia środowiska operacyjnego, które nakażą wybranie określonego protokołu lub określonej funkcji, która jest mniej bezpieczna (np. SNMPv1).

4.4.1

Poziomy wzmacniania

Zdefiniowane są dwa poziomy wzmacniania: *podwyższone* i *ściśle*.

Ścisły poziom wzmacniania to najbezpieczniejszy sposób skonfigurowania urządzenia. Może jednak ograniczać możliwości korzystania z urządzenia — takie funkcje jak automatyczne wykrywanie urządzenia są wówczas wyłączone. Dla każdej funkcji należy oddzielnie ustalić, czy można zastosować zabezpieczenie *podwyższone* lub *ściśle*.

4.4.2

Przegląd wzmacniania

Sieć - Usługi sieciowe	Domyślne	Podwyższone	Ścisłe
HTTP	Włączone	Wyłączone	Wyłączone
HTTPS	Włączone	Włączone	Włączone
RTSP	Włączone	Opcjonalnie	Wyłączone
RCP	Włączone	Wyłączone	Wyłączone
SNMPv1	Wyłączone	Wyłączone	Wyłączone
SNMPv3	Wyłączone	Włączone	Włączone
iSCSI	Włączone	Opcjonalnie	Wyłączone

Sieć - Usługi sieciowe	Domyślne	Podwyższone	Ścisłe
UPnP	Wyłączone	Wyłączone	Wyłączone
Serwer NTP	Wyłączone	Wyłączone	Wyłączone
Discovery	Włączone	Włączone	Wyłączone
ONVIF Discovery	Włączone	Włączone	Wyłączone
GBT/28181	Wyłączone	Wyłączone	Wyłączone
Mechanizm resetowania hasła	Włączone	Wyłączone	Wyłączone
Odpowiedź na polecenie ping	Włączone	Włączone	Wyłączone
RTSPS	Włączone	Włączone	Włączone
HTTP	Włączone	Wyłączone	Wyłączone

Sieć - Dostęp do sieci	Domyślne	Podwyższone	Ścisłe
Minimalna wersja protokołu TLS	1.0	1.2	1.2
HSTS	Wyłączone	Włączone	Włączone

Sieć - Zaawansowane	Domyślne	Podwyższone	Ścisłe
802.1x	Wyłączone	Opcjonalnie	Włączone
Syslog	Wyłączone	TCP	TLS

Sieć - Zarządzanie siecią	Domyślne	Podwyższone	Ścisłe
Tryb SNMPv3	Wyłączone	SHA1 / AES	SHA1 / AES

Sieć - Filtr IPv4	Domyślne	Podwyższone	Ścisłe
Filtr IPv4	Wyłączone	Włączone	Włączone

Ogólne - Data / godzina	Domyślne	Podwyższone	Ścisłe
Data/godzina (klient NTP)	Wyłączone	Data SNTP/TLS	Data TLS

Łączność - Usługi chmurowe	Domyślne	Podwyższone	Ścisłe
Remote Portal	Wyłączone	Włączone	Włączone

Serwis - Logowanie	Domyślne	Podwyższone	Ścisłe
Ochrona oprogramowania	Wyłączone	Włączone	Włączone

4.4.3

Opis funkcji i zalecenia dotyczące wzmacniania

HTTP

Protokół HTTP jest domyślnie włączony bez szyfrowania. Oznacza to, że dane uwierzytelniające lub ustawienia są przesyłane niezaszyfrowane.

Zalecenie: protokół HTTP powinien być zastąpiony protokołem HTTPS, zwłaszcza jeśli sieć jest niezauwana.

HTTPS

Protokół HTTPS zawiera szyfrowanie i powinien być domyślnym wyborem przy otwieraniu interfejsu internetowego lub dostępu do API RCP przez Internet. Zalecane jest korzystanie z własnej infrastruktury klucza publicznego i certyfikatów.

Zalecenie: HTTPS to domyślny chroniony protokół używany do konfiguracji. Powinien pozostać włączony.

RTSP

Do przesyłania strumieniowego używany jest protokół RTSP. Zazwyczaj jest nieszyfrowany. Jeśli oprogramowanie odbierające strumień wideo jest w stanie używać protokołu RTSPS, zalecamy wyłączenie RTSP. W przypadku stosowania innych komponentów firmy Bosch (np. dekodery/BVMS/VRM/DIVAR IP) można włączyć szyfrowanie protokołu RTSP opracowane przez firmę Bosch. Zapewnia ono bezpieczeństwo transmisji.

Zalecenie: przyjęcie podejścia opartego na ryzyku, jeśli obraz może być przesyłany w postaci niezaszyfrowanej lub za pomocą szyfrowania firmy Bosch. Jeśli to możliwe, należy używać szyfrowanego protokołu RTSPS.

RCP

Opracowany przez firmę Bosch protokół Remote Control Protocol plus to protokół konfiguracyjny kamer sieciowych firmy Bosch. Zwykły protokół RCP jest nieszyfrowany, więc i ustawienia są przesyłane nieszyfrowane. Wszystkie narzędzia Bosch wykorzystują od pewnego czasu protokół RCP przesyłany przy użyciu protokołu HTTPS. Takie rozwiązanie może być jednak potrzebne w przypadku narzędzi integracyjnych innych firm lub narzędzi skryptowych, które nadal opierają się na prostszym protokole.

Zalecenie: wyłączenie protokołu RCP, jeśli nie jest używany przez narzędzia innych firm lub starsze systemy.

SNMPv1

SNMP jest popularnym protokołem monitorowania stanu sieci używanym do pozyskiwania informacji o stanie urządzenia lub wysyłania sygnałów do zdalnego odbiorcy. Nie jest on szyfrowany.

Zalecenie: pozostawienie tego protokołu wyłączonego, jeśli nie jest wymagane monitorowanie stanu sieci lub nie jest to potrzebne z przyczyn kompatybilności. Jeśli to możliwe, należy używać szyfrowanego protokołu SNMPv3.

SNMPv3

SNMPv3 to następca SNMPv1 i może być również używany z szyfrowaniem.

Zalecenie: zalecany wybór w sytuacji konieczności realizacji monitoringu SNMP.

iSCSI

Wyłącza wewnętrzny serwer iSCSI, który służy do udostępniania nagrań wewnętrznych w kamerze przez protokół iSCSI. iSCSI jest protokołem nieszyfrowanym.

Zalecenie: wyłączenie serwera iSCSI, jeśli nie jest używany w kamerze.

UPnP

Umożliwienie wykrycia kamery za pomocą protokołu UPnP.

Zalecenie: wyłączenie protokołu UPnP, jeśli nie jest potrzebny.

Serwer NTP

Włącz w kamerze serwer NTP, aby umożliwić innym urządzeniom lub kamerom synchronizację czasu. Jeśli to możliwe, czas w sieci kamer powinien być przesyłany przez inne urządzenie, umożliwiając rozdzielanie usług. Jeśli nie ma innego urządzenia, czas może podawać kamera.

Zalecenie: wyłączenie serwera NTP, jeśli nie jest potrzebny.

Discovery

Wykorzystanie mechanizmu opracowanego przez firmę Bosch do umożliwienia wykrywania kamer przez oprogramowanie firmy Bosch, np Configuration Manager.

Zalecenie: przy pracy z dynamicznymi adresami IP ta funkcja powinna pozostać włączona. Podczas pracy w środowisku ze stałymi adresami IP można wyłączyć tę funkcję.

ONVIF Discovery

Obsługuje wykrywanie kamer za pomocą protokołu ONVIF Discovery

Zalecenie: przy pracy z dynamicznymi adresami IP i narzędziami zgodnymi z protokołem ONVIF ta funkcja powinna pozostać włączona. Podczas pracy w środowisku ze stałymi adresami IP można wyłączyć tę funkcję.

GBT/28181

GBT/28181 to chiński standard zapewniający interoperacyjność między różnymi urządzeniami.

Zalecenie: pozostawienie tego protokołu wyłączonego, jeśli nie jest wymagany.

Mechanizm resetowania hasła

Kamery IP mogą być montowane w bardzo odległych miejscach, co utrudnia wykonanie prac konserwacyjnych lub przywrócenie ustawień fabrycznych w przypadku zablokowania dostępu do kamery. Firma Bosch oferuje możliwość zresetowania hasła kamery za pomocą mechanizmu wyzwanie–odpowiedź opartego na bezpiecznym mechanizmie klucza publicznego/prywatnego.

Zalecenie: jeśli ta funkcja nie jest potrzebna, zalecamy jej wyłączenie.

Odpowiedź na polecenie ping

Konfiguruje, czy kamera ma odpowiadać na otrzymywane przez sieć żądania ping. Może to pomóc przy rozwiązywaniu problemów. W sieci o wysokim stopniu zabezpieczeń można to wyłączyć, aby uniknąć wyliczania urządzeń za pomocą polecenia ping sweep — chociaż istnieje kilka innych sposobów wykrywania urządzeń, z których atakujący może skorzystać.

Zalecenie: podejście oparte na ryzyku, można wyłączyć w przypadku sieci o wysokim poziomie bezpieczeństwa.

RTSPS

RTSPS to zaszyfrowana wersja protokołu RTSP, używana do strumieniowego przesyłania wideo. Jeśli protokół RTSPS jest obsługiwany przez oprogramowanie odbierające, należy go zawsze wybrać zamiast zwykłego protokołu RTSP. Ponieważ jednak wielu klientów RTSP nie obsługuje wariantu bezpiecznego, RTSP jest nadal włączony przy zabezpieczeniach poziomu 1.

Zalecenie: jeśli to możliwe, należy używać szyfrowanego protokołu RTSPS.

Minimalna wersja protokołu TLS

Kamery IP nie pozwalają na niezabezpieczone protokoły SSLv3 lub starsze. Protokół TLS w wersji 1.0 i 1.1 został wycofany IETF. Znane są też potencjalne problemy z jego zabezpieczeniami (BEAST, FREAK).

Kamery CPP4, CPP6, CPP7 i CPP7.3 obsługują bezpieczną wersję protokołu TLS 1.2, którą należy ustawić jako minimalną wymaganą wersję.

Kamery CPP13 i CPP14 nie obsługują wersji protokołu TLS starszych niż 1.2. Obsługują one również nowszą specyfikację TLS 1.3.

Zalecenie: ustawienie minimalnej wersji protokołu TLS na 1.2.

HSTS

HTTP Strict Transport Security (HSTS) to polityka ustalona przez stronę internetową w celu ochrony przed atakami typu man-in-the-middle oraz atakami typu „protocol downgrade”. Pozwala stronie internetowej na poinformowanie przeglądarki, aby zezwalała tylko na połączenie przy użyciu protokołu HTTPS i blokowała nieszyfrowane połączenia HTTP.

Zalecenie: włącz w kamerze opcję HSTS.

802.1x

802.1x jest standardem dla protokołu Network Access Control (NAC). Pozwala urządzeniom uwierzytelniać się w sieci i przyznawać dostęp tylko uwierzytelnionym urządzeniom. Kamery sieciowe firmy Bosch obsługują uwierzytelnianie 802.1x za pomocą hasła lub certyfikatu, przy czym preferowaną metodą jest uwierzytelnianie za pomocą certyfikatu. Aby użyć standardu 802.1x, musi go obsługiwać przełącznik sieciowy. Potrzebny jest też serwer uwierzytelniający.

Zalecenie: jeśli infrastruktura sieciowa na to pozwala, użyj uwierzytelniania sieciowego z wykorzystaniem standardu 802.1x.

Syslog

Ponieważ kamera ma ograniczoną przestrzeń na komunikaty dziennika, powinny być one wysyłane do centralnej lokalizacji i tam analizowane pod kątem ataków lub błędów.

Zalecenie: wykorzystanie protokołu TCP Syslog w celu uniknięcia utraty komunikatów z powodu strat pakietów. Używaj Syslog z TLS do szyfrowania i uwierzytelniania wiadomości.

Tryb SNMPv3

Protokół SNMPv3 jest następcą protokołu SNMPv1. Pozwala on na bezpieczne uwierzytelnianie i przesyłanie informacji.

Zalecenie: po włączeniu SNMPv3 użyj protokołu SHA1 do uwierzytelniania i AES do ochrony prywatności (jeśli jest obsługiwany).

Filtr adresów IP

W filtrze adresów IP można zdefiniować kilka adresów IP (pojedynczych hostów lub podsiaci), które będą miały dostęp do kamery. Zalecamy zdefiniowanie w tym miejscu komputerów lub sieci mających dostęp do kamery.

Zalecenie: zalecamy użycie filtra IP do zdefiniowania dozwolonych hostów lub sieci.

Data/godzina

Aby w dziennikach i danych wideo był wprowadzony prawidłowy znacznik czasu, zalecamy synchronizację czasu z centralnym serwerem. Można do tego użyć daty z protokołów SNTP i TLS. Zaletą protokołu SNTP jest bardziej precyzyjna synchronizacja czasu. Z kolei zaletą protokołu TLS jest możliwość sprawdzenia poprawności certyfikatu, co czyni to rozwiązanie bardziej bezpiecznym.

Zalecenie: użycie bezpiecznego sposobu synchronizacji czasu, albo za pomocą daty w protokole SNTP, albo TLS.

Usługi chmurowe

Firma Bosch oferuje własne usługi do zarządzania kamerami za pośrednictwem chmury Bosch (Remote Portal). Usługi w chmurze nie łączą się automatycznie z narzędziem Remote Portal i są domyślnie wyłączone. Każda kamera przed użyciem musi najpierw zostać podłączona do narzędzia Remote Portal. Podjęto wszelkie środki ostrożności, aby zabezpieczyć połączenie między narzędziem Remote Portal i kamerą. W razie potrzeby narzędzie Remote Portal może być użyte w każdym środowisku.

Zalecenie: narzędzie Remote Portal może być użyte stosownie do tego, czy używane jest rozwiązanie chmurowe.

Ochrona oprogramowania

Po zakończonej konfiguracji kamery IP ustawienia urządzenia nie powinny być zmieniane. Można włączyć ochronę oprogramowania — czyli funkcję powiadamiającą o zmianach w konfiguracji urządzenia.

Zalecenie: włączenie ochrony oprogramowania, jeśli nie ma oczekujących zmian w konfiguracji.

4.4.4

Głęboka obrona

Głęboka obrona odnosi się do warstwowego podejścia do bezpieczeństwa, w którym żaden jeden środek nie jest samodzielnie odpowiedzialny za bezpieczeństwo produktu — zamiast tego jest wiele warstw, które atakujący musi złamać. Przy każdej nowej wersji oceniamy, czy potrzebne są nowe funkcje do uniknięcia nowych ataków lub zwiększenia ogólnego bezpieczeństwa produktu.

Oto przegląd głównych funkcji bezpieczeństwa kamer IP.

– Podpisywanie oprogramowania sprzętowego

Każdy plik z aktualizacją oprogramowania sprzętowego jest zaszyfrowany i podpisany certyfikatem firmy Bosch. W kamerach można instalować tylko aktualizacje opublikowane przez firmę Bosch. Pozwala to uniknąć instalacji szkodliwego oprogramowania sprzętowego.

– Secure Boot

Kamery CPP13, CPP14 i nowsze mają mechanizm Secure Boot. Secure Boot sprawdza integralność całego systemu, począwszy od bootloadera, a skończywszy na samym

- oprogramowaniu sprzętowym w kamerach. Każdy procesu rozruchu weryfikuje następny, aż od samego niemodyfikowalnego sprzętowego źródła zaufania. Uniemożliwia to napastnikowi modyfikację bootloadera lub oprogramowania sprzętowego urządzenia.
- **Zapora firewall przed loginem**
Aby zabezpieczyć się przed zgadywaniem haseł, ale jednocześnie umożliwić administratorom logowanie się i ochronę przed atakami typu DoS (Denial of Service), zapora firewall przed loginem sprawdza próby logowania na podstawie analizy behawioralnej i dynamicznie blokuje dostęp lub go dopuszcza na podstawie adresów IP.
 - **Uwierzytelnianie kamery**
Aby jednoznacznie zidentyfikować i uwierzytelnić kamerę, podczas produkcji każdej kamery jest w niej tworzony certyfikat urządzenia firmy Bosch. Za pomocą tego certyfikatu można sprawdzić, czy prowadzona jest komunikacja z autentycznym urządzeniem firmy Bosch. Ponadto do kamery można przesłać lub można w niej utworzyć niestandardowe certyfikaty, które zapewnią integrację ze środowiskiem PKI w celu ochrony przed atakami typu man-in-the-middle.

4.5 Wzmacnianie pamięci

Ponieważ kamery cyfrowe i nadajniki firmy Bosch są w stanie ustanowić sesję iSCSI bezpośrednio do napędu iSCSI i zapisać dane sygnału wizyjnego w napędzie iSCSI, jednostki iSCSI muszą być podłączone do tej samej sieci LAN lub WAN co urządzenia peryferyjne firmy Bosch.

Aby uniknąć nieupoważnionego dostępu do zapisanych danych wizyjnych, należy chronić jednostki iSCSI przed nieautoryzowanym dostępem:

- Użyć uwierzytelniania haseł przez CHAP, aby upewnić się, że tylko znane urządzenia będą miały dostęp do obiektów iSCSI. Skonfigurować hasło CHAP w obiekcie iSCSI i wprowadzić je do konfiguracji VRM. Hasło CHAP obowiązuje dla VRM i jest wysyłane automatycznie do wszystkich urządzeń. Jeśli hasło CHAP jest używane w środowisku BVMS VRM, wszystkie systemy pamięci masowej muszą być skonfigurowane do używania tego samego hasła.
- Usunąć wszystkie domyślne nazwy użytkowników i hasła z obiektu iSCSI.
- Użyć silnego hasła do administrowania kontami użytkowników obiektów iSCSI.
- Wyłączyć dostęp administracyjny przez telnet do obiektów iSCSI. Zamiast tego użyć dostępu przez SSH.
- Zabezpieczyć dostęp konsoli do obiektów iSCSI za pomocą mocnego hasła.
- Wyłączyć niewykorzystane karty interfejsu sieciowego.
- Monitorować stan systemu magazynów iSCSI za pomocą narzędzi innych firm, aby zidentyfikować nieprawidłowości.

4.5.1 Ustawianie hasła CHAP na urządzeniach iSCSI

Po ustawieniu globalnego hasła CHAP w narzędziu BVMS Configuration Client hasło to jest automatycznie przesyłane do wszystkich koderów, dekoderów i urządzeń VSG.

W przypadku niektórych urządzeń iSCSI ta funkcja nie jest obsługiwana. Na tych urządzeniach należy ręcznie ustawić hasło CHAP.



Uwaga!

Przed dodaniem urządzeń iSCSI do środowiska BVMS należy ustawić w nich globalne hasło CHAP.

Urządzeń iSCSI nie można dodać do konfiguracji BVMS, w której globalne hasło CHAP jest już aktywowane.

Aby ręcznie ustawić hasło CHAP na urządzeniu iSCSI (na przykład DIVAR IP), które jest oparte na najnowszej wersji systemu operacyjnego Microsoft Windows Server:

1. Otwórz obszar **Server Manager** (Menedżer serwera) i przejdź do obszaru **File and Storage Services > iSCSI** (Plik i usługi pamięci masowej > iSCSI).
2. Na liście **iSCSI TARGETS** (OBIEKTY iSCSI) kliknij prawym przyciskiem myszy żądany obiekt iSCSI i kliknij polecenie **Properties** (Właściwości).
Pojawi się okno dialogowe **Properties** (Właściwości).
3. W oknie dialogowym **Properties** (Właściwości) kliknij pozycję **Security** (Zabezpieczenia), a następnie zaznacz pole wyboru **Enable CHAP** (Włącz CHAP).
4. Wprowadź następujące dane:
 - **User name** (Nazwa użytkownika): user
 - **Password** (Hasło): wprowadź globalne hasło CHAP podane w programie BVMS Configuration Client (w menu **Hardware > Protect iSCSI storages with CHAP password...**) (Sprzęt > Chroń pamięć iSCSI hasłem CHAP...).
5. Kliknij przycisk **OK**.
Hasło CHAP zostanie przypisane do obiektu iSCSI.

4.6 Wzmacnianie serwerów

4.6.1 Zalecane ustawienia sprzętowe serwera

- Serwer BIOS oferuje możliwość ustawiania hasła niższego poziomu.
Te hasła pozwalają ograniczyć możliwość uruchamiania komputera, uruchamiania przy użyciu urządzeń wymiennych oraz zmiany ustawień BIOS lub UEFI (Unified Extensible Firmware Interface) bez wcześniejszej zgody.
- Aby uniknąć przesyłania danych do serwera, porty USB i napęd CD/DVD powinny być wyłączone.
Ponadto nieużywane porty NIC powinny zostać również wyłączone, a porty zarządzania, takie jak interfejs HP ILO (HP Integrated Lights Out) lub porty konsoli, powinny być chronione hasłem albo tak jak reszta wyłączone.

4.6.2 Zalecane ustawienia zabezpieczeń systemu operacyjnego Windows

Serwery powinny być częścią domeny Windows.

Wraz z integracją serwerów do domeny Windows uprawnienia użytkownika są przypisywane do użytkowników sieci zarządzanych przez centralny serwer.. Ponieważ te konta użytkowników często wdrażają reguły dotyczące hasła i wygaśnięcia hasła, taka integracja może poprawić bezpieczeństwo kont lokalnych, które nie mają tych ograniczeń.

4.6.3 Aktualizacje systemu Windows

Poprawki i aktualizacje oprogramowania Windows powinny być instalowane i zawsze aktualne. Aktualizacje Windows często zawierają poprawki do nowo odkrytych luk w zabezpieczeniach, takich jak luka w zabezpieczeniach związana z protokołem Heartbleed SSL, która dotyczy milionów komputerów na całym świecie. Należy instalować poprawki dotyczące tych istotnych kwestii.

4.6.4 Instalacja oprogramowania antywirusowego

Zainstalować oprogramowanie antywirusowe i antyspygowskie oraz aktualizować je.

4.6.5 Zalecane ustawienia systemu operacyjnego Windows

Następujące Lokalne ustawienia zasad grupy są zalecanymi ustawieniami grupy w systemie operacyjnym Windows Server. Aby zmienić domyślne lokalne zasady grupowe (LCP), użyj edytora lokalnych zasad grupy.

Edytor lokalnych zasad grupy można otworzyć za pomocą wiersza polecenia lub za pomocą konsoli MMC (Microsoft Management Console).

Aby otworzyć edytor lokalnych zasad grupy z wiersza polecenia:

- ▶ Kliknąć **Start**, w polu wyszukiwania **Start** wpisać **gpedit.msc**, po czym nacisnąć Enter.

Aby otworzyć edytor lokalnych zasad grupy jako przystawkę MMC:

1. Kliknąć **Start**, w polu wyszukiwania **Start** wpisać **mmc**, po czym nacisnąć Enter.
2. W oknie dialogowym **Dodaj lub usuń przystawki** kliknąć **Edytor obiektów zasad grupy**, a następnie **Dodaj**.
3. W oknie dialogowym **Wybierz obiekt zasad grupy** kliknąć **Przeglądaj**.
4. Kliknąć **Ten komputer**, aby edytować Obiekt zasad grupy lokalnej lub **Użytkownicy**, aby edytować Administratorów, osoby niebędące administratorami lub użytkowników obiektów zasad grupy lokalnej.
5. Kliknąć **Zakończ**.

4.6.6 Uaktywnianie kontroli konta użytkownika na serwerze

Zasady komputera lokalnego -> Konfiguracja komputera -> Ustawienia systemu Windows -> Ustawienia zabezpieczeń -> Zasady lokalne -> Opcje zabezpieczeń

Kontrola konta użytkownika: tryb zatwierdzania przez administratora dla wbudowanego konta administratora	Włączone
Kontrola konta użytkownika: zezwalaj aplikacjom UIAccess na monit o podwyższenie bez użycia bezpiecznego pulpitu	Wyłączone
Kontrola konta użytkownika: zachowanie progu podwyższenia dla administratorów w trybie zatwierdzania przez administratora	Pytaj o zgodę
Kontrola konta użytkownika: zachowanie monitu o podniesienie standardu dla standardowych użytkowników	Pytaj o poświadczenia na bezpiecznym pulpicie
Kontrola konta użytkownika: wykrywanie instalacji aplikacji i monitowanie o podniesienie	Włączone
Kontrola konta użytkownika: należy podnieść uprawnienia tylko plikom wykonywalnym, które są podpisane i zatwierdzone	Wyłączone
Kontrola konta użytkownika: uruchamianie wszystkich administratorów w trybie zatwierdzania przez administratora	Włączone
Kontrola konta użytkownika: po wyświetleniu monitu o podwyższenie uprawnień przełączanie na bezpieczny pulpit	Włączone
Kontrola konta użytkownika: wirtualizowanie plików i błędów zapisu rejestru do lokalizacji użytkowników	Włączone

Zasady komputera lokalnego -> Konfiguracja komputera -> Szablony administracyjne -> Składniki systemu Windows -> Interfejs użytkownika poświadczeń

Wylicza konta administratorów do podwyższenia	Wyłączone
---	-----------

4.6.7

Dezaktywacja autoodtworzenia

Zasady komputera lokalnego -> Konfiguracja komputera -> Szablony administracyjne -> Składniki systemu Windows -> Zasady autoodtworzenia

Wyłączanie autoodtworzenia	Włączyć wszystkie dyski
Domyślne zachowanie dla procesu automatycznego uruchamiania	Włączone, nie uruchamiać żadnych poleceń AutoRun
Wyłączanie funkcji autoodtworzenia dla urządzeń innych producentów	Włączone

4.6.8

Urządzenia zewnętrzne

Zasady komputera lokalnego -> Konfiguracja komputera -> Ustawienia systemu Windows -> Ustawienia zabezpieczeń -> Zasady lokalne -> Opcje zabezpieczeń

Urządzenia: zezwalanie na otwieranie bez logowania	Wyłączone
Urządzenia: zezwalanie na formatowanie i wysunięcie nośników wymiennych	Administratorzy
Urządzenia: uniemożliwianie użytkownikom instalowanie sterowników drukarki	Włączone
Urządzenia: ograniczenie dostępu do dysku CD-ROM tylko do lokalnie zalogowanego użytkownika	Włączone
Urządzenia: ograniczenie dostępu do stacji dyskietek tylko do lokalnie zalogowanych użytkowników	Włączone

4.6.9

Konfiguracja przypisania praw użytkownika

Zasady komputera lokalnego -> Konfiguracja komputera -> Ustawienia systemu Windows -> Ustawienia zabezpieczeń -> Zasady lokalne -> Przypisanie praw użytkownika

Uzyskiwanie dostęp do menedżera poświadczeń jako zaufany rozmówca	Nikt
Uzyskiwanie dostępu do tego komputera z sieci	Uwierzytlenieni użytkownicy
Działanie jako część systemu operacyjnego	Nikt
Dodawanie stacji roboczych do domeny	Nikt
Zezwalanie na logowanie za pośrednictwem usług pulpitu zdalnego	Administratorzy, użytkownicy pulpitu zdalnego
Zmiana czasu systemowego	Administratorzy
Zmiana strefy czasowej	Administratorzy, usługa lokalna

Tworzenie pliku strony	Administratorzy
Tworzenie obiektu tokenu	Nikt
Tworzenie trwałych udostępnionych obiektów	Nikt
Odmowa dostępu do tego komputera z sieci	Logowanie anonimowe, gość
Ignorowanie logowania jako zadanie wsadowe	Logowanie anonimowe, gość
Ignorowanie logowania jako usługa	Nikt
Ignorowanie logowania lokalnego	Logowanie anonimowe, gość
Ignorowanie logowania za pośrednictwem usług pulpitu zdalnego	Logowanie anonimowe, gość
Aktywowanie komputera i konta użytkowników jako zaufane do delegowania	Nikt
Wymuszenie zamknięcia przez system zdalny	Administratorzy
Generowanie audytów bezpieczeństwa	Serwis lokalny, usługa sieciowa
Zwiększenie priorytetu planowania	Administratorzy
Załadowanie i usunięcie sterowników urządzeń	Administratorzy
Zmiana etykiety obiektu	Nikt
Zmiana wartości środowiska oprogramowania układowego	Administratorzy
Wykonanie zadań związanych z utrzymaniem wolumenu	Administratorzy
Profil pojedynczego procesu	Administratorzy
Wyjmowanie komputera ze stacji dokującej	Administratorzy
Przywracanie plików i katalogów	Administratorzy
Zamykanie systemu	Administratorzy
Synchronizowanie danych usługi katalogowej	Nikt
Przejmowanie prawa własności do plików lub innych obiektów	Administratorzy

4.6.10

Wygaszacz ekranu

- Uaktywnij wygaszacz ekranu chroniony hasłem i określ limitu czasu:
Zasady komputera lokalnego -> Konfiguracja użytkownika -> Szablony administracyjne -> Panel sterowania -> Personalizacja

Włączanie wygaszacza ekranu	Włączone
Zabezpieczenie wygaszacza ekranu hasłem	Włączone
Wygaśnięcie limitu czasu wygaszacza ekranu	1800 sekund

4.6.11

Aktywacja ustawień zasad dotyczących haseł

- Włączenie ustawień zasad dotyczących haseł zapewnia, że hasła użytkowników spełniają minimalne wymagania dotyczące hasła

Zasady komputera lokalnego -> Ustawienia systemu Windows -> Ustawienia zabezpieczeń -> Zasady kont -> Zasady haseł

Wymuszenie historii haseł	10 zapamiętanych haseł
Maksymalny wiek hasła	90 dni
Minimalny wiek hasła	1 dzień
Minimalna długość hasła	10 znaków
Hasło musi spełniać wymagania dotyczące złożoności	Włączone
Przechowywać hasła przy użyciu odwracalnego szyfrowania dla wszystkich użytkowników domeny	Wyłączone

4.6.12 Wyłączyć usługi nieistotne dla systemu Windows

- Wyłączenie innych niż istotne usługi systemu Windows umożliwia wyższy poziom zabezpieczeń i minimalizuje punkty ataków.

Usługa bramy warstwy aplikacji	Wyłączone
Zarządzanie aplikacją	Wyłączone
Przeglądarka komputerowa	Wyłączone
Klient śledzenia łączy rozproszonych	Wyłączone
Host dostawcy wykrywania funkcji	Wyłączone
Funkcja wykrywania zasobów publikacji	Wyłączone
Dostęp do urządzeń interfejsu	Wyłączone
Udostępnianie połączenia internetowego (ICS)	Wyłączone
Mapper topologii warstwy łącza	Wyłączone
Harmonogram zajęć multimedialnych	Wyłączone
Pliki trybu offline	Wyłączone
Menedżer połączeń automatycznych zdalnego dostępu	Wyłączone
Menedżer połączeń zdalnego dostępu	Wyłączone
Routing i dostęp zdalny	Wyłączone
Wykrywanie sprzętu powłokowego	Wyłączone
Administracja specjalna pomocnika konsoli	Wyłączone
Wykrywanie SSDP	Wyłączone

4.6.13 Konta użytkowników systemu operacyjnego Windows

Konta użytkowników systemu operacyjnego Windows muszą być chronione hasłami złożonymi. Serwery są zazwyczaj zarządzane i obsługiwane za pomocą kont administratora Windows, dzięki czemu administratorzy mogą używać silnych haseł.

Hasła muszą zawierać znaki z trzech następujących kategorii:

- Wielkie litery języków europejskich (od A do Z, ze znakami diakrytycznymi, litery greckie i cyrylica)
- Małe litery języków europejskich (a do z, ostre s, znaki diakrytyczne, litery greckie i cyrylica)
- 10 cyfr podstawowych (od 0 do 9)
- Znaki inne niż alfanumeryczne: ~!@#\$%^&* _+=` \ () { } [] ; " ' < > , . ? /
- Dowolny znak Unicode, który jest sklasyfikowany jako alfabetyczny, ale nie wielka lub mała litera. Obejmuje to znaki Unicode z języków azjatyckich.

Użyć blokady konta systemu Windows, aby utrudnić ataki na hasła.

Zalecaną podstawą bezpieczeństwa dla Windows 8.1 jest 10/15/15:

- 10 niepowodzeń
- Czas blokady 15 minut
- Po 15 minutach reset licznika

Zasady komputera lokalnego -> Konfiguracja komputera -> Ustawienia systemu Windows -> Ustawienia zabezpieczeń -> Zasady kont -> Zasady blokowania konta

Czas blokady konta	Czas blokady konta
15 minut próg blokady konta 10 nieudanych prób logowania	15 minut próg blokady konta 10 nieudanych prób logowania
Resetowanie licznika blokady kont	Resetowanie licznika blokady kont

- Należy się upewnić, że wszystkie domyślne hasła serwera i systemu operacyjnego Windows zostały zastąpione nowymi silnymi hasłami.

4.6.14

Włączyć zapórę na serwerze

- ▶ Włączyć komunikację portu standardowego BVMS zgodnie z portami BVMS.



Uwaga!

Informacje na temat odpowiednich ustawień i sposobu użytkowania portu znajdują się w dokumentacji instalacyjnej i użytkownika rozwiązania BVMS. Należy pamiętać, aby ponownie sprawdzić ustawienia aktualizacji oprogramowania układowego lub oprogramowania.

4.7

Wzmacnianie klientów Windows

4.7.1

Stacje robocze Windows

Systemy operacyjne Windows dla komputerów stacjonarnych, stosowane w aplikacjach BVMS Client, takich jak BVMS Operator Client lub Configuration Client, zostaną zainstalowane poza bezpiecznym obszarem. Stacje robocze muszą zostać wzmocnione, aby chronić dane wizyjne, dokumenty i inne aplikacje przed nieautoryzowanym dostępem.

Należy zastosować lub sprawdzić następujące ustawienia.

4.7.2

Zalecane ustawienia sprzętowe stacji roboczych systemu Windows

- Ustawić hasło BIOS/UEFI, aby ograniczyć możliwości uruchamiania innych systemów operacyjnych.
- Aby zapobiec przesyłaniu danych do klienta, porty USB i napęd CD/DVD powinny zostać wyłączone. Ponadto powinny zostać wyłączone wszystkie niewykorzystane porty NIC.

4.7.3 Zalecane ustawienia zabezpieczeń systemu operacyjnego Windows

- Stacja robocza powinna być częścią domeny Windows.
Integracja stacji roboczej z domeną Windows, ustawieniami zabezpieczeń można zarządzać centralnie.
- Aktualizacje Windows
Należy na bieżąco śledzić poprawki i aktualizacje systemu Windows.
- Instalacja oprogramowania antywirusowego
Zainstalować oprogramowanie antywirusowe i antyszpiegowskie oraz aktualizować je.

4.7.4 Zalecane ustawienia systemu operacyjnego Windows

Następujące Lokalne ustawienia zasad grupy są zalecanymi ustawieniami grupy w systemie operacyjnym Windows Server. Aby zmienić domyślne lokalne zasady grupowe (LCP), użyj edytora lokalnych zasad grupy.

Edytor lokalnych zasad grupy można otworzyć za pomocą wiersza polecenia lub za pomocą konsoli MMC (Microsoft Management Console).

Aby otworzyć edytor lokalnych zasad grupy z wiersza polecenia:

- ▶ Kliknąć **Start**, w polu wyszukiwania **Start** wpisać **gpedit.msc**, po czym nacisnąć Enter.

Aby otworzyć edytor lokalnych zasad grupy jako przystawkę MMC:

1. Kliknąć **Start**, w polu wyszukiwania **Start** wpisać **mmc**, po czym nacisnąć Enter.
2. W oknie dialogowym **Dodaj lub usuń przystawki** kliknąć **Edytor obiektów zasad grupy**, a następnie **Dodaj**.
3. W oknie dialogowym **Wybierz obiekt zasad grupy** kliknąć **Przeglądaj**.
4. Kliknąć **Ten komputer**, aby edytować Obiekt zasad grupy lokalnej lub **Użytkownicy**, aby edytować Administratorów, osoby niebędące administratorami lub użytkowników obiektów zasad grupy lokalnej.
5. Kliknąć **Zakończ**.

4.7.5 Uaktywnianie kontroli konta użytkownika na serwerze

Zasady komputera lokalnego -> Konfiguracja komputera -> Ustawienia systemu Windows -> Ustawienia zabezpieczeń -> Zasady lokalne -> Opcje zabezpieczeń

Kontrola konta użytkownika: tryb zatwierdzania przez administratora dla wbudowanego konta administratora	Włączone
Kontrola konta użytkownika: zezwalaj aplikacjom UIAccess na monit o podwyższenie bez użycia bezpiecznego pulpitu	Wyłączone
Kontrola konta użytkownika: zachowanie progu podwyższenia dla administratorów w trybie zatwierdzania przez administratora	Pytaj o zgodę
Kontrola konta użytkownika: zachowanie monitu o podniesienie standardu dla standardowych użytkowników	Pytaj o poświadczenia na bezpiecznym pulpicie
Kontrola konta użytkownika: wykrywanie instalacji aplikacji i monitowanie o podniesienie	Włączone
Kontrola konta użytkownika: należy podnieść uprawnienia tylko plikom wykonywalnym, które są podpisane i zatwierdzone	Wyłączone

Kontrola konta użytkownika: uruchamianie wszystkich administratorów w trybie zatwierdzania przez administratora	Włączone
Kontrola konta użytkownika: po wyświetleniu monitu o podwyższenie uprawnień przełączanie na bezpieczny pulpit	Włączone
Kontrola konta użytkownika: wirtualizowanie plików i błędów zapisu rejestru do lokalizacji użytkowników	Włączone

Zasady komputera lokalnego -> Konfiguracja komputera -> Szablony administracyjne -> Składniki systemu Windows -> Interfejs użytkownika poświadczeń

Wylicza konta administratorów do podwyższenia	Wyłączone
---	-----------

4.7.6

Dezaktywacja autoodtworzenia

Zasady komputera lokalnego -> Konfiguracja komputera -> Szablony administracyjne -> Składniki systemu Windows -> Zasady autoodtworzenia

Wyłączanie autoodtworzenia	Włączyć wszystkie dyski
Domyślne zachowanie dla procesu automatycznego uruchamiania	Włączone, nie uruchamiać żadnych poleceń AutoRun
Wyłączanie funkcji autoodtworzenia dla urządzeń innych producentów	Włączone

4.7.7

Urządzenia zewnętrzne

Zasady komputera lokalnego -> Konfiguracja komputera -> Ustawienia systemu Windows -> Ustawienia zabezpieczeń -> Zasady lokalne -> Opcje zabezpieczeń

Urządzenia: zezwalanie na otwieranie bez logowania	Wyłączone
Urządzenia: zezwalanie na formatowanie i wysunięcie nośników wymiennych	Administratorzy
Urządzenia: uniemożliwianie użytkownikom instalowanie sterowników drukarki	Włączone
Urządzenia: ograniczenie dostępu do dysku CD-ROM tylko do lokalnie zalogowanego użytkownika	Włączone
Urządzenia: ograniczenie dostępu do stacji dyskiety tylko do lokalnie zalogowanych użytkowników	Włączone

4.7.8

Konfiguracja przypisania praw użytkownika

Zasady komputera lokalnego -> Konfiguracja komputera -> Ustawienia systemu Windows -> Ustawienia zabezpieczeń -> Zasady lokalne -> Przypisanie praw użytkownika

Uzyskiwanie dostęp do menedżera poświadczeń jako zaufany rozmówca	Nikt
Uzyskiwanie dostępu do tego komputera z sieci	Uwierzytelnieni użytkownicy
Działanie jako część systemu operacyjnego	Nikt

Dodawanie stacji roboczych do domeny	Nikt
Zezwalanie na logowanie za pośrednictwem usług pulpitu zdalnego	Administratorzy, użytkownicy pulpitu zdalnego
Zmiana czasu systemowego	Administratorzy
Zmiana strefy czasowej	Administratorzy, usługa lokalna
Tworzenie pliku strony	Administratorzy
Tworzenie obiektu tokenu	Nikt
Tworzenie trwałych udostępnionych obiektów	Nikt
Odmowa dostępu do tego komputera z sieci	Logowanie anonimowe, gość
Ignorowanie logowania jako zadanie wsadowe	Logowanie anonimowe, gość
Ignorowanie logowania jako usługa	Nikt
Ignorowanie logowania lokalnego	Logowanie anonimowe, gość
Ignorowanie logowania za pośrednictwem usług pulpitu zdalnego	Logowanie anonimowe, gość
Aktywowanie komputera i konta użytkowników jako zaufane do delegowania	Nikt
Wymuszenie zamknięcia przez system zdalny	Administratorzy
Generowanie audytów bezpieczeństwa	Serwis lokalny, usługa sieciowa
Zwiększenie priorytetu planowania	Administratorzy
Załadowanie i usunięcie sterowników urządzeń	Administratorzy
Zmiana etykiety obiektu	Nikt
Zmiana wartości środowiska oprogramowania układowego	Administratorzy
Wykonanie zadań związanych z utrzymaniem wolumenu	Administratorzy
Profil pojedynczego procesu	Administratorzy
Wyjmowanie komputera ze stacji dokującej	Administratorzy
Przywracanie plików i katalogów	Administratorzy
Zamykanie systemu	Administratorzy
Synchronizowanie danych usługi katalogowej	Nikt
Przejmowanie prawa własności do plików lub innych obiektów	Administratorzy

4.7.9

Wygaszacz ekranu

- Uaktywnij wygaszacz ekranu chroniony hasłem i określ limitu czasu:

Zasady komputera lokalnego -> Konfiguracja użytkownika -> Szablony administracyjne -> Panel sterowania -> Personalizacja

Włączanie wygaszacza ekranu	Włączone
Zabezpieczenie wygaszacza ekranu hasłem	Włączone
Wygaśnięcie limitu czasu wygaszacza ekranu	1800 sekund

4.7.10

Aktywacja ustawień zasad dotyczących haseł

- Włączenie ustawień zasad dotyczących haseł zapewnia, że hasła użytkowników spełniają minimalne wymagania dotyczące hasła

Zasady komputera lokalnego -> Ustawienia systemu Windows -> Ustawienia zabezpieczeń -> Zasady kont -> Zasady haseł

Wymuszenie historii haseł	10 zapamiętanych haseł
Maksymalny wiek hasła	90 dni
Minimalny wiek hasła	1 dzień
Minimalna długość hasła	10 znaków
Hasło musi spełniać wymagania dotyczące złożoności	Włączone
Przechowywać hasła przy użyciu odwracalnego szyfrowania dla wszystkich użytkowników domeny	Wyłączone

4.7.11

Wyłączyć usługi nieistotne dla systemu Windows

- Wyłączenie innych niż istotne usługi systemu Windows umożliwia wyższy poziom zabezpieczeń i minimalizuje punkty ataków.

Usługa bramy warstwy aplikacji	Wyłączone
Zarządzanie aplikacją	Wyłączone
Przeglądarka komputerowa	Wyłączone
Klient śledzenia łączy rozproszonych	Wyłączone
Host dostawcy wykrywania funkcji	Wyłączone
Funkcja wykrywania zasobów publikacji	Wyłączone
Dostęp do urządzeń interfejsu	Wyłączone
Udostępnianie połączenia internetowego (ICS)	Wyłączone
Mapper topologii warstwy łącza	Wyłączone
Harmonogram zajęć multimedialnych	Wyłączone
Pliki trybu offline	Wyłączone
Menedżer połączeń automatycznych zdalnego dostępu	Wyłączone
Menedżer połączeń zdalnego dostępu	Wyłączone
Routing i dostęp zdalny	Wyłączone
Wykrywanie sprzętu powłokowego	Wyłączone
Administracja specjalna pomocnika konsoli	Wyłączone

Wykrywanie SSDP	Wyłączone
-----------------	-----------

4.7.12

Konta użytkowników systemu operacyjnego Windows

Konta użytkowników systemu operacyjnego Windows muszą być chronione hasłami złożonymi. Serwery są zazwyczaj zarządzane i obsługiwane za pomocą kont administratora Windows, dzięki czemu administratorzy mogą używać silnych haseł.

Hasła muszą zawierać znaki z trzech następujących kategorii:

- Wielkie litery języków europejskich (od A do Z, ze znakami diakrytycznymi, litery greckie i cyrylica)
- Małe litery języków europejskich (a do z, ostre s, znaki diakrytyczne, litery greckie i cyrylica)
- 10 cyfr podstawowych (od 0 do 9)
- Znaki inne niż alfanumeryczne: ~!@#\$%^&* _+= ` | \ () { } [] ; : " ' < > , . ? /
- Dowolny znak Unicode, który jest sklasyfikowany jako alfabetyczny, ale nie wielka lub mała litera. Obejmuje to znaki Unicode z języków azjatyckich.

Użyć blokady konta systemu Windows, aby utrudnić ataki na hasła.

Zalecaną podstawą bezpieczeństwa dla Windows 8.1 jest 10/15/15:

- 10 niepowodzeń
- Czas blokady 15 minut
- Po 15 minutach reset licznika

Zasady komputera lokalnego -> Konfiguracja komputera -> Ustawienia systemu Windows -> Ustawienia zabezpieczeń -> Zasady kont -> Zasady blokowania konta

Czas blokady konta	Czas blokady konta
15 minut próg blokady konta 10 nieudanych prób logowania	15 minut próg blokady konta 10 nieudanych prób logowania
Resetowanie licznika blokady kont	Resetowanie licznika blokady kont

- Należy się upewnić, że wszystkie domyślne hasła serwera i systemu operacyjnego Windows zostały zastąpione nowymi silnymi hasłami.
- Wyłączyć niewykorzystane konta systemu operacyjnego Windows.
- Wyłączyć dostęp do pulpitu zdalnego do stacji roboczej klienta.
- Uruchomić stację roboczą z prawami nieadministracyjnymi, aby uniknąć zmiany ustawień systemu przez standardowego użytkownika.

4.7.13

Włączyć zaporę na stacji roboczej

- ▶ Włączyć komunikację portu standardowego BVMS zgodnie z portami BVMS.



Uwaga!

Informacje na temat odpowiednich ustawień i sposobu użytkowania portu znajdują się w dokumentacji instalacyjnej i użytkownika rozwiązania BVMS. Należy pamiętać, aby ponownie sprawdzić ustawienia aktualizacji oprogramowania układowego lub oprogramowania.

4.8

Ochrona dostępu do sieci

Obecnie wiele małych i średnich systemów dozoru wizyjnego IP jest rozmieszczonych w istniejącej infrastrukturze sieciowej klienta jako inna aplikacja IT.

Pomimo że ma to zalety pod względem kosztów i utrzymania, tego rodzaju wdrożenie naraża system zabezpieczeń na niepożądane zagrożenia, w tym wewnętrzne. Należy zastosować odpowiednie środki, aby uniknąć sytuacji, takich jak, wyciek do danych Internetu czy portali społecznościowych. Takie zdarzenia nie tylko naruszają prywatność, ale mogą zaszkodzić firmie.

Istnieją dwie główne technologie umożliwiające tworzenie sieci w sieci. To, która z nich zostanie wybrana przez architektów infrastruktury informatycznej, zależy w dużej mierze od istniejącej infrastruktury sieciowej, wdrożonych urządzeń sieciowych oraz wymaganych możliwości i topologii sieci.

4.8.1

VLAN: wirtualna sieć LAN

Wirtualna sieć LAN jest tworzona przez dzielenie LAN na wiele segmentów. Segmentacja sieci odbywa się poprzez konfigurację przełącznika sieciowego lub routera. Sieć VLAN ma taką zaletę, że potrzeby zasobów można rozwiązać bez konieczności ponownego podłączania połączeń sieciowych urządzeń.

Systemy jakości usług stosowane do konkretnych segmentów, takich jak dozór wizyjny, mogą pomóc nie tylko poprawić bezpieczeństwo, ale również wydajność.

VLAN są implementowane na warstwie łącza danych (warstwa OSI 2) i zapewniają analogię do podsieci IP (zobacz *Przypisywanie adresów IP, Strona 8*), która jest podobna do warstwy sieciowej (warstwa OSI 3).

4.8.2

VPN: wirtualna sieć prywatna

Sieć prywatna VPN to oddzielona (prywatna) sieć, która często rozciąga się na sieciach publicznych lub w Internecie. Do utworzenia sieci VPN wykorzystywane są różne protokoły, zazwyczaj jest to tunel prowadzący ruch chroniony. Wirtualne sieci prywatne mogą być zaprojektowane jako tunele bezpośrednie, połączenia dowolne lub wielopunktowe. Sieci VPN mogą być rozmieszczane przy użyciu szyfrowanej komunikacji lub polegać na bezpiecznej komunikacji wewnątrz samej sieci VPN.

Sieci VPN mogą być wykorzystywane do łączenia odległych miejsc przez połączenia sieci rozległej (WAN), a jednocześnie chronią prywatność i zwiększają bezpieczeństwo w sieci lokalnej (LAN). Ponieważ sieć VPN działa jako oddzielna sieć, wszystkie urządzenia dodane do sieci VPN będą pracować bez zakłóceń, tak jakby znajdowały się w typowej sieci. Sieć VPN nie tylko dodaje dodatkową warstwę ochrony systemu dozoru, ale także zapewnia dodatkową korzyść z segmentowania sieci produkcyjnych ruchu biznesowego i danych wizyjnych.



Uwaga!

W stosownych przypadkach sieć VLAN lub VPN zwiększa poziom bezpieczeństwa systemu nadzoru połączonego z istniejącą infrastrukturą informatyczną.

Poza ochroną systemu nadzoru przed nieupoważnionym dostępem do wspólnej infrastruktury IT należy zwrócić uwagę na osoby, które mogą łączyć się z siecią.

4.8.3 Wyłączanie niewykorzystanych portów przełączników

Wyłączenie nieużytych portów sieciowych zapewnia, że nieautoryzowane urządzenia nie mają dostępu do sieci. Zmniejsza to ryzyko uzyskania dostępu do podsieci zabezpieczającej za pomocą podłączenia urządzenia do przełącznika lub nieużywanego gniazda sieciowego. Opcja wyłączenia określonych portów jest wspólną opcją w zarządzanych przełącznikach, zarówno tych niedrogich, jak i klasy „enterprise”.

4.8.4 Sieci chronione 802.1x

Wszystkie urządzenia wizyjne IP firmy Bosch mogą zostać skonfigurowane jako klienci 802.1x. Pozwala to na uwierzytelnianie przez serwer RADIUS i uczestniczenie w zabezpieczonej sieci. Przed umieszczeniem urządzeń wizyjnych w zabezpieczonej sieci konieczne jest bezpośrednie połączenie urządzenia z laptopem technika w celu wprowadzenia ważnych poświadczeń, co szczegółowo opisano poniżej.

Usługę 802.1x można łatwo skonfigurować za pomocą Configuration Manager.

1. W programie Configuration Manager wybrać żądane urządzenie.
2. Wybrać kartę **Sieć**, a następnie **Zaawansowane**.



3. Zlokalizować na stronie dział **802.1x**.
4. W menu rozwijanym **802.1x** wybrać **Włącz**.
5. Wprowadzić poprawne **Identyfikacja i Hasło**.
6. Zapisać zmiany.
7. Odłączyć i umieścić urządzenia w zabezpieczonej sieci.



Uwaga!

802.1x nie zapewnia bezpiecznej komunikacji między serwerem aplikującym a serwerem uwierzytelniającym.

W rezultacie nazwa użytkownika i hasło mogą zostać zidentyfikowane w sieci. 802.1x może używać protokołu EAP-TLS w celu zapewnienia bezpiecznej komunikacji.

Rozszerzony protokół uwierzytelniania — Transport Layer Security

Rozszerzony protokół uwierzytelniania (EAP) umożliwi obsługę wielu metod uwierzytelniania. Zabezpieczenie warstwy transportowej (TLS) zapewnia wzajemne uwierzytelnianie, negocjacje dotyczące szyfrowanych pakietów zabezpieczonych integralnością oraz zmianę kluczy między dwoma punktami końcowymi. EAP-TLS obejmuje obsługę certyfikatów opartych na wzajemnym uwierzytelnianiu oraz kluczach źródłowych. Innymi słowy, protokół EAP-TLS obejmuje proces, w którym zarówno serwer, jak i klient wysyłają sobie certyfikat.



Uwaga!

Należy zapoznać się z raportem technicznym *Uwierzytelnianie sieciowe — 802.1x — zabezpieczanie krańców sieci* dostępnym online w katalogu produktów Bosch Security Systems pod adresem:

http://resource.boschsecurity.com/documents/WP_802.1x_Special_enUS_22335867275.pdf.

5 Bezpieczne działanie

5.1 Separacja sieci

Jeśli to możliwe, w celu ograniczenia ruchu rozgłoszeniowego i ochrony urządzenia przed atakami sieciowymi urządzenie powinno pracować w oddzielnej sieci (na przykład z wykorzystaniem sieci VLAN) z ograniczeniami dostępu.

5.2 Bezpieczne przechowywanie kluczy w skarbcu sprzętowym

Klucze prywatne do certyfikatów są najlepiej chronione, gdy są bezpiecznie przechowywane w komponencie sprzętowym lub w skarbcu sprzętowym. Takie układy zapewniają ochronę przed nieautoryzowanym dostępem do kluczy prywatnych nawet wtedy, gdy urządzenie w celu uzyskania dostępu zostanie fizycznie otwarte.

W kamerach Bosch takie klucze są przechowywane w oddzielnym krypto-koprocesorze lub bezpiecznym elemencie (SE). Oba zapewniają bezpieczne przechowywanie. Mają także funkcje kryptograficzne, które nigdy nie ujawniają kluczy prywatnych w lokalizacjach lub pamięci, w których mogłyby zostać potencjalnie odczytane.

W stacjach roboczych i serwerach zazwyczaj dostępny jest układ TPM (Trusted Platform Module). Biblioteki i funkcje kryptograficzne należy konfigurować tak, aby w miarę możliwości korzystały z magazynu modułu TPM.

5.3 Unikatowe certyfikaty urządzeń

Choć domyślny samopodpisany certyfikat jest zazwyczaj dostępny w każdym urządzeniu obsługującym TLS lub HTTPS, nie należy go uważać za wystarczający wyłącznie do uwierzytelniania — nie chroni on przed atakiem typu "man-in-the-middle" (MITM).

Jeśli urządzenia są rozmieszczone w środowisku, w którym wymagane są dodatkowe kroki w celu potwierdzenia tożsamości każdego pojedynczego urządzenia wizyjnego IP, można utworzyć i załadować nowe certyfikaty i klucze prywatne do urządzeń wizyjnych. Nowe certyfikaty można uzyskać od urzędu certyfikacji (CA) lub można je utworzyć, używając np. pakietu narzędzi OpenSSL.

Jeśli urządzenia są używane w sieciach publicznych, zaleca się uzyskiwanie certyfikatów z publicznego urzędu certyfikacji lub posiadanie własnego certyfikatu podpisanego przez użytkownika, który jest również w stanie weryfikować pochodzenie i ważność, czyli zaufanie do certyfikatu urządzenia.

Od lat wszystkie kamery firmy Bosch mają zainstalowany fabrycznie unikatowy certyfikat urządzenia oraz klucz prywatny pochodzący z certyfikatu głównego Bosch, zainstalowany w bezpiecznym środowisku produkcyjnym oraz potwierdzający, że kamera jest „oryginalnym produktem” Bosch. Certyfikat jest używany do automatycznych połączeń HTTPS i może być użyty do identyfikacji i uwierzytelnienia urządzenia poprzez weryfikację łańcucha certyfikatów aż do certyfikatu głównego Bosch.



Uwaga!

Certyfikaty powinny być używane do uwierzytelnienia jednego urządzenia. Zaleca się utworzenie określonego certyfikatu dla każdego urządzenia pochodzącego z certyfikatu głównego.

Najbezpieczniejszym wariantem wdrożenia certyfikatu jest wygenerowanie żądania podpisania certyfikatu (CSR) na urządzeniu i zażądanie certyfikatu od wewnętrznego lub zewnętrznego urzędu certyfikacji.

W przypadku żądania podpisania certyfikatu urządzenie przechowuje klucz prywatny wewnątrz, i udostępnia jedynie resztę certyfikatu do podpisania przez urząd certyfikacji. Klucz prywatny jest przechowywany bezpiecznie w elemencie chronionym (SE) kamery lub np. w module Trusted Platform Module (TPM) urządzenia.

Dlatego gdy urządzenie udostępnia funkcję CSR, powinien to być preferowany sposób tworzenia certyfikatu.

Certyfikaty można przysyłać do urządzenia za pomocą jego strony internetowej lub narzędzia Configuration Manager.

Przesyłanie certyfikatów za pomocą strony internetowej urządzenia wizyjnego

Certyfikaty można przysyłać za pomocą strony internetowej urządzenia wizyjnego.

Na stronie internetowej urządzenia wizyjnego, w obszarze **Certyfikaty** można dodawać oraz usuwać nowe certyfikaty i definiować ich wykorzystanie.

Przesyłanie certyfikatów za pomocą programu Configuration Manager

W programie Configuration Manager certyfikaty mogą zostać przesłane do jednego lub wielu urządzeń jednocześnie.

Aby przesłać certyfikaty:

1. W programie Configuration Manager wybierz jedno lub więcej urządzeń.
2. Kliknąć prawym przyciskiem myszy **Przesyłanie pliku**, a następnie **Certyfikat SSL....**
Zostanie otwarte okno Windows Explorer do zlokalizowania certyfikatu do przesłania.

W przypadku mniejszych systemów program Configuration Manager udostępnia funkcję pomocniczą o nazwie **MicroCA**, która pozwala na utworzenie lub wykorzystanie głównego urzędu certyfikacyjnego i wyprowadzenie z niego certyfikatów urządzeń lub wykorzystanie go do realizacji żądań podpisania certyfikatów urządzeń także dla wielu urządzeń jednocześnie. Więcej informacji można znaleźć w instrukcji obsługi programu Configuration Manager.

Patrz

– *Tworzenie zaufania przy użyciu certyfikatów, Strona 48*

5.4 Sprawdzanie plików dziennika

Monitorowanie plików dziennika jest ważną częścią analizy bezpieczeństwa lub działań konserwacyjnych. Regularne przeglądanie plików dziennika może ujawnić problemy z konfiguracją lub bezpieczeństwem, takie jak przypadku fałszywego logowania.

Aby analizować pliki dziennika i przechowywać je przez dłuższy czas, zalecamy wysyłanie ich z urządzenia do serwera syslog lub systemu SIEM. Kamera ma zarezerwowaną stałą ilość miejsca na dzienniki, ale po jego zapełnieniu nadpisuje najstarsze dzienniki.

5.5 System SIEM

System Security Information and Event Management (SIEM) to system, który służy do zbierania i analizowania informacji z różnych urządzeń i systemów. Urządzenia mogą być integrowane z systemem SIEM poprzez wysyłanie logów za pomocą protokołu syslog. Analiza tych logów może pomóc w przeprowadzeniu konserwacji oraz w wykryciu błędów w konfiguracji lub ataków na urządzenie (na przykład fałszywych logowań).

5.6 PKI

Infrastruktura klucza publicznego (PKI) oznacza systemy potrzebne do generowania certyfikatów cyfrowych i zarządzania nimi. W przypadku protokołu HTTPS i uwierzytelniania sieciowego za pomocą standardu 802.1x, uwierzytelniania użytkownika za pomocą certyfikatów i innych funkcji szyfrowania, na urządzeniu można zainstalować niestandardowe certyfikaty.

5.7 AD FS

Active Directory Federation Services (AD FS) to usługa oferowana przez firmę Microsoft, która umożliwia uwierzytelnianie do lokalnego rozwiązania Active Directory (przy użyciu serwera AD FS) lub do chmury Azure. Oprócz lokalnego uwierzytelniania użytkowników za pomocą hasła lub uwierzytelniania opartego na certyfikatach możliwa jest integracja urządzeń z domeną Active Directory za pomocą AD FS w celu centralnego uwierzytelniania i zarządzania dostępem użytkowników.

5.8 Bezpieczna praca kamer IP

5.8.1 Tworzenie zaufania przy użyciu certyfikatów

Wszystkie kamery IP firmy Bosch używają FW 6.10 lub nowszego magazynu certyfikatów, który jest dostępny w menu **Serwis** konfiguracji kamery.

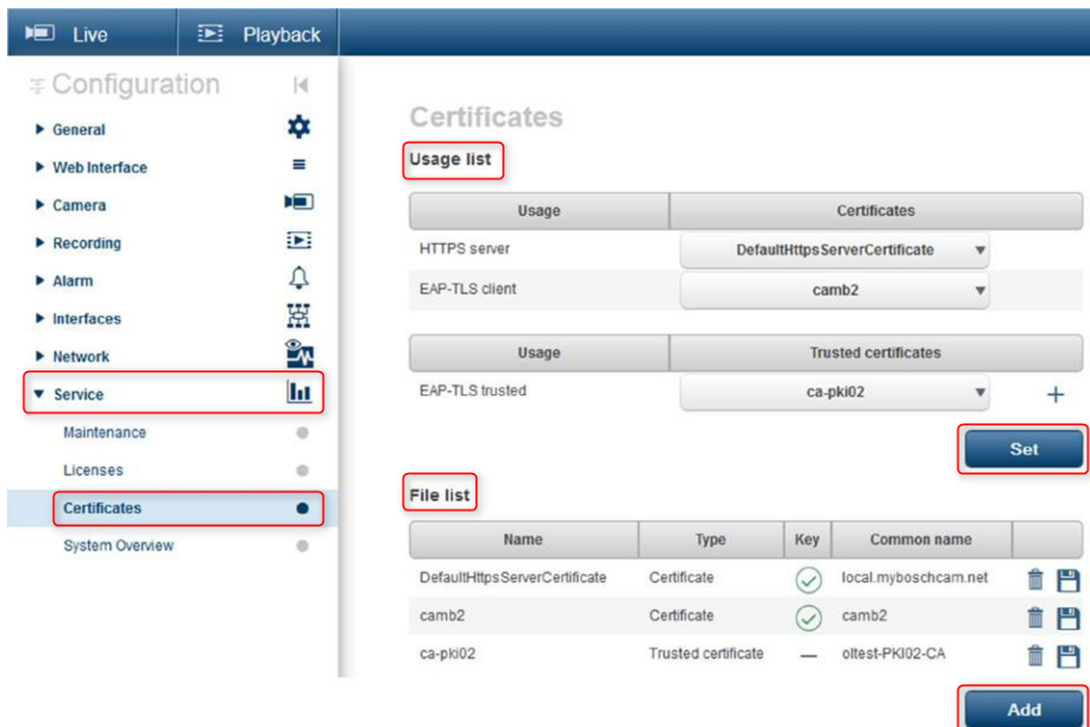
Możliwe jest dodanie do magazynu certyfikatów serwera, certyfikatów klientów oraz zaufanych certyfikatów.

W celu dodania certyfikatu do magazynu:

1. Na stronie internetowej urządzenia przejść na stronę **Konfiguracja**.
2. Wybrać menu **Serwis** oraz podmenu **Certyfikaty**.
3. W sekcji **Lista plików** kliknąć **Dodaj**.
4. Załadować wymagane certyfikaty.

Po zakończeniu przesyłania certyfikaty pojawiają się na liście w sekcji **Lista użycia**.

5. W sekcji **Lista użycia** wybrać żądany certyfikat.
6. Aby aktywować użycie certyfikatów, należy ponownie uruchomić kamerę. Aby ponownie uruchomić kamerę, kliknąć **Ustaw**.



Rysunek 5.1: Przykład: certyfikaty EAP/TLS przechowywane w kamerze Bosch (FW6.11)

Certyfikaty są akceptowane w formacie *.pem, *.cer lub *.crt i muszą być kodowane w formacie base64. Można je przesłać jako jeden połączony plik lub podzielić na certyfikaty i kluczowe części i przesłać w tej kolejności jako osobne pliki, które mają zostać automatycznie ponownie połączone.

Począwszy od wersji oprogramowania układowego 6.20, obsługiwane są chronione hasłem prywatne klucze PKCS # 8 (z szyfrowaniem AES), które muszą być przesyłane w formacie base64 *.pem.

5.8.2

Uwierzytelnianie materiału wizyjnego

Gdy urządzenia w systemie są chronione i poprawnie uwierzytelniane, warto zwrócić uwagę na dostarczane przez nie dane wizyjne. Metoda ta nazywana jest uwierzytelnianiem materiału wizyjnego.

Uwierzytelnianie materiału wizyjnego dotyczy wyłącznie metod sprawdzania autentyczności obrazu. Uwierzytelnianie materiału wizyjnego nie dotyczy w żaden sposób jego przesyłania ani samych danych.

Przed wydaniem wersji oprogramowania układowego 5.9 dodano znak wodny, używając prostego algorytmu sum kontrolnych nad strumieniem wizyjnym. W przypadku podstawowego znaku wodnego nie ma certyfikatów ani szyfrowania. Suma kontrolna to podstawowy pomiar dokładności danych pliku, który sprawdza jego integralność.

Aby skonfigurować uwierzytelnianie materiału wizyjnego na przykład w przeglądarce internetowej:

1. Przejść do menu **Ogólne** i wybrać **Wyświetlanie informacji**.
2. W menu rozwijanym **Uwierzytelnianie wideo** wybrać żadaną opcję: wersje oprogramowania układowego 5.9 i nowsze udostępniają trzy opcje uwierzytelniania materiału wizyjnego oprócz klasycznego znaku wodnego:
 - MD5: Message-digest, który generuje wartość skrótu 128-bitowego.

- SHA-1: zaprojektowany przez Agencję Bezpieczeństwa Narodowego Stanów Zjednoczonych, jest amerykańskim federalnym standardem przetwarzania informacji opublikowanym przez NIST Stanów Zjednoczonych. SHA-1 generuje wartość skrótu 160-bitowego.
- SHA-256: algorytm SHA-256 generuje mieszankę praktycznie niepowtarzalną, o stałej wielkości 256-bitowej (32-bajtowej).

Display Stamping

Camera name stamping

Logo

Logo position

Time stamping

Display milliseconds

Alarm mode stamping

Alarm message (max. 31 characters)

Transparent background

Video authentication

Signature Interval [s]



Uwaga!

Znacznik jest funkcją jednokierunkową — nie można jej odszyfrować.

Podczas korzystania z uwierzytelniania materiału wizyjnego każdy pakiet strumienia wizyjnego jest mieszany. Są one osadzone w strumieniu wizyjnym i mieszają się razem z danymi wizyjnymi. To zapewnia integralność zawartości strumienia.

Znaczniki są podpisywane w regularnych odstępach czasu definiowanych przez interwał podpisu przy użyciu klucza prywatnego przechowywanego certyfikatu w obrębie modułu TPM urządzenia. Zapisy alarmowe i zmiany blokowe w zapisach iSCSI są zamykane podpisem w celu zapewnienia ciągłej autentyczności obrazu.



Uwaga!

Obliczanie cyfrowego podpisu wymaga mocy obliczeniowej, która może mieć wpływ na ogólną wydajność kamery, jeśli jest wykonywane zbyt często. Dlatego należy wybrać odpowiedni odstęp czasowy.

Znaczniki i podpisy cyfrowe osadzone w strumieniu wizyjnym będą również przechowywane w nagraniu, co pozwala na uwierzytelnianie materiału wizyjnego również w celu odtwarzania i eksportowania.

6 Zarządzanie aktualizacjami zabezpieczeń

Przed pierwszym rozpoczęciem obsługi urządzenia należy upewnić się, że jest instalowana najnowsza dostępna wersja oprogramowania. Aby zapewnić spójność działania, zgodność, wydajność i bezpieczeństwo, oprogramowanie należy regularnie aktualizować przez cały okres eksploatacji urządzenia. Należy postępować zgodnie z instrukcjami podanymi w dokumentacji produktu w zakresie aktualizacji oprogramowania.

Więcej informacji można znaleźć w następujących miejscach:

- Informacje ogólne: <https://www.boschsecurity.com/xc/en/support/product-security/>
- Forum bezpieczeństwa, czyli lista rozpoznanych zagrożeń i proponowanych rozwiązań: <https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html>

Firma Bosch nie ponosi odpowiedzialności za szkody spowodowane korzystaniem ze starej wersji oprogramowania.

Najnowsze wersje oprogramowania sprzętowego i naszych programów oprogramowania można znaleźć w sklepie z plikami do pobrania Bosch Security and Safety Systems: <https://downloadstore.boschsecurity.com/>

W przypadku urządzeń podłączonych do programu Remote Portal użytkownicy mogą za pośrednictwem usługi Remote Alert otrzymywać powiadomienia e-mail o dostępnych aktualizacjach oprogramowania sprzętowego.

Bardziej kompleksowe pakiety do pobrania są dystrybuowane poprzez katalog produktów Bosch Security and Safety Systems:

<https://www.boschsecurity.com>

7 Monitorowanie bezpieczeństwa

Ponieważ wymagania stale się zmieniają, zagwarantowanie pełnego bezpieczeństwa nie jest możliwe. Dlatego w firmie Bosch zbudowano ustrukturyzowany proces zarządzania słabymi punktami i incydentami w celu profesjonalnego zarządzania bezpieczeństwem produktów.

Bardzo ważna jest dla nas profesjonalna, systematyczna obsługa zgłoszonych luk bezpieczeństwa oraz transparentność wobec klientów. Dlatego sprawdzamy wszystkie zgłoszenia luk w zabezpieczeniach. Ocenę podatności produktów na zagrożenia bezpieczeństwa przeprowadzamy zgodnie ze standardem CVSS (Common Vulnerability Scoring System). CVSS to darmowy, otwarty standard branżowy oceny dotkliwości luk w bezpieczeństwie systemów komputerowych. Wyniki są obliczane na podstawie wzoru, który zależy od kilku wskaźników przybliżających łatwość wykorzystania luki i wpływ jej wykorzystania. Wyniki wahają się od 0 do 10, z oceną 10 oznaczającą najpoważniejszy problem.

W przypadku potwierdzonej luki informujemy klientów o zidentyfikowanej luce w produkcji lub rozwiązaniu i sposobie jej usunięcia poprzez opublikowanie komunikatu dotyczącego bezpieczeństwa. Wszystkie komunikaty dotyczące bezpieczeństwa zawierają:

- Opis luki z odniesieniem do katalogu Common Vulnerabilities and Exposures (CVE) i z wynikiem CVSS.
- Nazwy znanych produktów i wersji oprogramowania/sprzętu, których dotyczy problem.
- Informacje o czynnikach łagodzących i obejściach.
- Harmonogram i lokalizację dostępnych poprawek lub innych środków zaradczych.

Lista opublikowanych komunikatów dotyczących bezpieczeństwa jest dostępna na naszej stronie internetowej: <https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html>.

Jeśli sądzić, że udało Ci się zidentyfikować lukę w zabezpieczeniach lub inny problem bezpieczeństwa związany z produktem lub usługą firmy Bosch, skontaktuj się z zespołem Bosch Product Security Incident Response Team (PSIRT): <https://psirt.bosch.com>.

8 Bezpieczne usuwanie i wycofywanie z eksploatacji

W pewnym momencie cyklu życia produktu lub systemu może zaistnieć konieczność wymiany lub wycofania z eksploatacji całego urządzenia lub jakiejś jego części. Ponieważ urządzenie lub część mogą zawierać dane wrażliwe, takie jak dane uwierzytelniające lub certyfikaty, należy upewnić się, że dane te zostaną uprzednio bezpiecznie usunięte.

Większość urządzeń można ustawić na domyślne ustawienia fabryczne.

W przypadku większości kamer IP i enkoderów można do tego celu użyć przycisku resetowania. W przypadku tych urządzeń, które nie mają przycisku resetowania, przed odłączeniem ich od sieci użyj funkcji przywrócenia ustawień fabrycznych dostępnej w interfejsie internetowym urządzenia.

Wszyscy użytkownicy i ich hasła zostaną usunięte, a ustawienia zostaną przywrócone do domyślnych ustawień fabrycznych. Wszystkie certyfikaty i odpowiednie klucze, które były przechowywane w TPM lub elemencie SE, również zostaną usunięte.

Różne urządzenia mogą mieć różnie nazwaną opcję przywrócenia ustawień fabrycznych. Aby uzyskać informacje na temat prawidłowych procedur utylizacji, zapoznaj się z instrukcjami w odpowiedniej dokumentacji użytkownika.

Certyfikaty i poświadczenia mogą być również przechowywane przez serwery i stacje robocze. Należy użyć odpowiednich narzędzi i metod, aby upewnić się, że dane te zostaną bezpiecznie usunięte przed wycofywaniem z eksploatacji lub utylizacją.

Zalecamy przywrócenie ustawień fabrycznych również w przypadku konieczności przeniesienia urządzenia do innej instalacji, w której mogą być używane inne dane uwierzytelniające lub certyfikaty.



Uwaga!

Aby uzyskać informacje na temat prawidłowych procedur utylizacji, zapoznaj się z instrukcjami w odpowiedniej dokumentacji użytkownika.

9 Informacje dodatkowe

Więcej informacji, dokumentację i oprogramowanie do pobrania można znaleźć na stronie danego produktu w katalogu produktów:

<http://www.boschsecurity.com>

Słowniczek

802.1x

Standard IEEE 802.1x to podstawowa metoda uwierzytelniania i autoryzacji w sieciach IEEE-802. Autoryzacja jest dokonywana przez specjalny moduł (authenticator), który sprawdza przesłane informacje, używając serwera uwierzytelniania (patrz serwer RADIUS) i zezwala lub nie zezwala na dostęp do oferowanych usług (LAN, VLAN lub WLAN).

Adres IPv4

Niepowtarzalny numer składający się z 4 bajtów, służący do identyfikacji każdego urządzenia w sieci Internet. Zwykle zapisywany w postaci dziesiętnej z segmentami oddzielonymi kropkami, np. „209.130.2.193”.

DHCP

Skrót od „Dynamic Host Configuration Protocol”. Protokół, dzięki któremu odpowiedni serwer dynamicznie przypisuje adres IP i parametry konfiguracyjne komputerom w sieci (Internecie lub sieci LAN)

Grupa użytkowników

Grupy użytkowników służą do definiowania wspólnych atrybutów użytkownika, takich jak pozwolenia, uprawnienia oraz priorytet funkcji PTZ. Stając się członkiem grupy, użytkownik automatycznie nabywa wszystkie atrybuty grupy.

HTTP

Skrót od „Hypertext Transfer Protocol”. Jest to protokół transmisji danych w sieci

LAN

Local Area Network – Sieć lokalna. Jest to sieć łącząca urządzenia w obrębie ograniczonego obszaru geograficznego.

Net mask (Maska sieci)

Maska służy do określenia, która część adresu IP jest adresem sieciowym, a która adresem hosta. Zwykle zapisywany w postaci dziesiętnej z segmentami oddzielonymi kropkami, np. „255.255.255.192”.

ONVIF

Open Network Video Interface Forum. Globalny standard sieciowych urządzeń wizyjnych. Urządzenia zgodne z normą ONVIF mogą

wymieniać bieżący obraz, dźwięk, metadane i sygnały sterujące. Ponadto użytkownik zyskuje gwarancję, że będą one automatycznie wykrywane i podłączane do aplikacji sieciowych, takich jak systemy zarządzania sygnałem wizyjnym.

Protokół HTTPS

Skrót od „Hypertext Transfer Protocol Secure”. Protokół, który służy do szyfrowania i uwierzytelniania komunikacji między serwerem WWW a przeglądarką

RCP+

Protokół zdalnego sterowania: zastrzeżony protokół firmy Bosch, który wykorzystuje określone porty statyczne do wykrywania i komunikacji z urządzeniami wizyjnymi IP firmy Bosch

RTSP

Skrót od „Real Time Streaming Protocol”. Protokół sieciowy umożliwiający kontrolę nad ciągłą transmisją dźwięku i obrazu lub oprogramowania w sieciach IP.

Serwer RADIUS

Skrót od „Remote Authentication Dial-in User Service”. Protokół klient-serwer służący do uwierzytelniania, autoryzacji i obciążania użytkowników opłatami w połączeniach modemowych w sieciach komputerowych. Serwer RADIUS stanowi w zasadzie standard scentralizowanego uwierzytelniania przyłączeniowego za pomocą modemu, ISDN, wirtualnych sieci prywatnych, sieci bezprzewodowej (p. 802.1x) i DSL.

SNMP

Simple Network Management Protocol – protokół do zarządzania siecią, zarządzania i monitorowania komponentów sieciowych

SSL

Skrót od „Secure Sockets Layer”. Nieaktualny protokół szyfrujący do transmisji danych w sieciach IP (patrz TLS).

TCP

Skrót od „Transmission Control Protocol” (nazwa protokołu komunikacyjnego). Protokół połączeń komunikacyjnych używany do przesyłania danych przez sieć IP. Zapewnia niezawodne i uporządkowane przesyłanie danych.

Telnet

Protokół, za pomocą którego użytkownicy mogą uzyskać dostęp do zdalnego komputera przez Internet

TLS

Transport Layer Security. Wersje 1.0 i 1.1 protokołu TLS są ustandaryzowanymi zaawansowanymi rozszerzeniami protokołu SSL 3.0 (patrz SSL). Nowoczesne urządzenia używają protokołu TLS w wersji 1.2 lub 1.3

Tryb Multicast

Komunikacja w sieci pomiędzy jednym nadajnikiem/odbiornikiem a kilkoma odbiornikami, polegająca na dystrybucji jednego strumienia danych do kilku odbiorników w zdefiniowanej grupie. Do pracy w trybie multicastingu jest wymagana zgodna sieć z obsługą protokołu UDP i IGMP.

TTL

Skrót od „Time-To-Live” – czas pozostawiania pakietów danych w sieci podczas transmisji między stacjami

UDP

User Datagram Protocol. Protokół bezpołączeniowy używany do wymiany danych przez sieć IP. Protokół UDP jest bardziej wydajny od protokołu TCP przy transmisji obrazu ze względu na mniejszą nadmiarowość.

urządzenie

Komponent sprzętowy taki jak kamera, koder/ dekodek, NVR, DiBos, matryca analogowa lub most ATM/POS.

uwierzytelnianie

Proces weryfikacji autentyczności strumienia sygnału wizyjnego. Użytkownik może uruchomić proces uwierzytelniania. Jeśli pojawią się nieautentyczne dane, wyświetlany jest odpowiedni komunikat.

VPN

Wirtualna sieć prywatna (VPN) wykonuje sieć prywatną w sieci publicznej, takiej jak Internet. Ruch sieciowy w sieci VPN jest szyfrowany, dzięki czemu jest chroniony przed podsłuchiowaniem.

Wide Area Network (Sieć rozległa)

Sieć komputerowa o dużym zasięgu rozbudowująca lub łącząca odległe sieci lokalne

wzmacnianie

Proces zwiększania bezpieczeństwa systemu poprzez używanie tylko dedykowanego oprogramowania, które jest niezbędne do działania systemów, stosowanie określonych ustawień oraz usuwanie oprogramowania, które nie jest wymagane.

Bosch Sicherheitssysteme GmbH

Robert-Bosch-Ring 5

85630 Grasbrunn

Germany

www.boschsecurity.com

© Bosch Sicherheitssysteme GmbH, 2023

Building solutions for a better life.

202302091957