nVision 10

axence®

Podręcznik użytkownika

axence®

Axence nVision Help

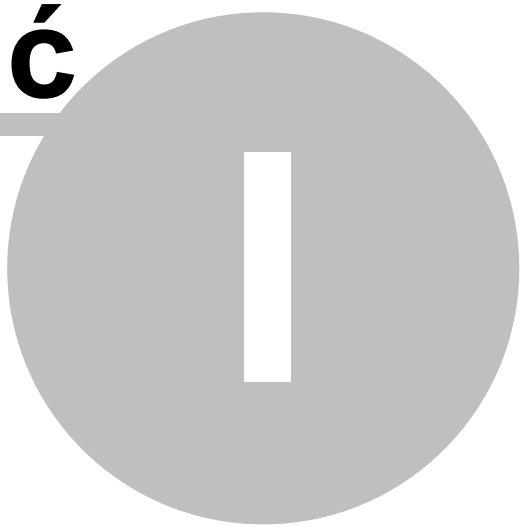
Wizualizacja i zarządzanie siecią

Axence nVision daje Ci wszystko, czego potrzebujesz do skutecznego i efektywnego zarządzania siecią.
Aplikacja składa się z 5 modułów: proaktywnego monitorowania i wizualizacji sieci, inwentaryzacji sprzętu i oprogramowania, monitorowania aktywności użytkowników, zdalnego wsparcia technicznego i ochrony danych przed wyciekiem.

Axence nVision Help

Spis treści

Część



1 Wprowadzenie

1.1 Funkcjonalność Axence nVision

Axence nVision® - monitorowanie sieci, aplikacji i pracowników, inwentaryzacja sprzętu i oprogramowania

Axence nVision® składa się z 5 modułów funkcjonalnych, które można instalować w dowolnych kombinacjach i zarządzać nimi w jednej konsoli.

Proaktywne monitorowanie i wizualizacja sieci	**Network**	Moduł Network monitoruje serwery pocztowe i adresy WWW, serwisy TCP/IP i Windows, stan i działanie aplikacji oraz switche i routery (mapowanie portów, ruch sieciowy, monitorowanie SNMP). Sieć jest wykrywana automatycznie i prezentowana interaktywnie na mapach.
Inwentaryzacja sprzętu i oprogramowania	**Inventory**	Moduł Inventory automatycznie zbiera informacje o sprzęcie i oprogramowaniu komputerów Windows. Umożliwia audyt i weryfikację użytkowania licencji oraz informuje o zainstalowaniu programu lub zmianie konfiguracji.
Zaawansowane monitorowanie użytkowników	**Users**	Moduł Users monitoruje i raportuje aktywność użytkowników pracujących na komputerach Windows: faktyczny czas aktywności (pracy), użytkowanie programów, odwiedzane strony WWW oraz transfer sieciowy.
Zdalna pomoc techniczna dla użytkowników	**HelpDesk**	Moduł HelpDesk umożliwia udzielanie pomocy technicznej użytkownikom poprzez zdalny dostęp do stacji roboczych. Pomaga szybko i skutecznie rozwiązywać zgłaszane problemy.
Ochrona danych przed kradzieżą	**DataGuard**	Moduł DataGuard zarządza prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, przez które użytkownik może skopiować pliki z komputera firmowego lub uruchomić na nim program zewnętrzny.
Alarmowanie i zdarzenia		Możesz zdefiniować szeroki zakres zdarzeń, które uruchamiają alarmy. Zdarzenia mogą być definiowane dla każdego monitorowanego parametru i serwisu, np. gdy komputer lub serwis nie działa, zmieni się zawartość strony, serwer pocztowy ma problemy lub parametry serwera MS SQL są poza zakresem itp. Każde zdarzenie może uruchomić jedną lub więcej akcji powiadamiających lub korekcyjnych, takich jak wiadomość na ekranie, email, SMS i ICQ, uruchomienie programu, zapis do pliku. Alarmy są zachowywane w logu, aby umożliwić ich późniejszą analizę.

1.2 Wersje Axence nVision

Spis wersji programu wraz z funkcjami i usprawnieniami, które wprowadzają, znajduje się na stronie http://www.axence.net/pl/lista-zmian-w-oprogramowaniu/.

1.3 Funkcjonalność modułów

Tabela poniżej porównuje funkcjonalność modułów nVision. Wszystkie moduły mogą być zamawiane niezależnie.

Funkcje	Network	Inventory	Users	HelpDesk	DataGuard
Wykrywanie i wizualizacja sieci					
Serwer nVision: skanowanie i monitorowanie sieci, wykrywanie urządzeń i serwisów TCP/IP, dostęp zdalny przez przeglądarkę oraz automatyczna kopia zapasowa	–	–	–	–	–
Konsola nVision: dynamiczne mapy sieci, mapy użytkownika, oddziały, mapy inteligentne, zestaw narzędzi z możliwoscią dodawania własnych	✓	✓	✓	✓	✓
Konsola nVision: jednoczesna praca wielu administratorów, zarządzanie uprawnieniami użytkowników, dziennik dostępu administratorów	–	–	–	–	–
Monitorowanie sieci					
Serwisy TCP/IP: poprawność i czas odpowiedzi, statystyka ilości odebranych/utraconych pakietów (PING, SMB, HTTP, POP3, SNMP, IMAP, SQL itp.)	–	–	–	–	–
Liczniki WMI: obciążenie procesora, zajętość pamięci, zajętość dysków, transfer sieciowy itp.	✓	–	–	–	–
Działanie Windows: zmiana stanu usług (uruchomienie, zatrzymanie, restart), wpisy dziennika zdarzeń	–	–	–	–	–
Liczniki SNMP v1/2/3 (transfer sieciowy, temperatura, wilgotność, napięcie zasilania, poziom tonera itp.),	✓	–	–	–	–
Obsługa komunikatów syslog	–	–	–	–	–
Pułapki SNMP	–	–	–	–	–
Routery i switche: mapowanie portów i monitoring ruchu sieciowego	–	–	–	–	–

Funkcje	Network	Inventory	Users	HelpDesk	DataGuard
Dystrybucja plików z wykorzystaniem WMI	✓	–	–	–	–
Kompilator plików MIB	–	–	–	–	–
Alarmowanie i raporty					
Alarmy zdarzenie-akcja (np. gdy ważne parametry znajdą się poza zakresem zdefiniowanym przez użytkownika)	–	–	–	–	–
Powiadomienia (pulpitowe, e-mail, SMS) oraz akcje korekcyjne (uruchomienie programu, restart komputera itp.)	✓	✓	✓	✓	✓
Raporty (dla użytkownika, grupy, urządzenia, mapy urządzeń lub całego atlasu)	–	–	–	–	–
Inwentaryzacja sprzętu i oprogramowania					
Lista aplikacji oraz aktualizacji Windows na stacji roboczej (na podstawie rejestru systemowego oraz skanowania dysku)	–	–	–	–	–
Numery seryjne (klucze) oprogramowania	–	–	–	–	–
Informacje o plikach wykonywalnych i wpisach rejestru na stacji roboczej	–	✓	–	–	–
Informacje o plikach multimedialnych (mp3, avi itp.) oraz archiwach zip i ich metadanych (tytuł i autor utworu, zawartość pliku zip)	–	–	–	–	–
Ogólne informacje o sprzęcie na stacji roboczej	–	✓	–	–	–
Szczegółowe informacje o konfiguracji sprzętowej stacji roboczej (model, płyta, procesor, pamięć, napędy, karty itp.)	–	–	–	–	–
Informacje systemowe (komendy startowe, konta użytkowników, foldery udostępnione, informacje SMART, monitorowanie harmonogramu zadań Windows itp.)	–	✓	–	–	–
Audyt inwentaryzacji sprzętu i oprogramowania	–	–	–	–	–
Możliwość dystrybucji i deinstalacji oprogramowania przez paczki MSI	–	–	–	–	–
Zarządzanie instalacjami/deinstalacjami oprogramowania w oparciu o menedżer pakietów MSI	–	–	–	–	–

Funkcje	Network	Inventory	Users	HelpDesk	DataGuard
Baza wzorców oprogramowania	–	✓	–	–	–
Zarządzanie licencjami	–	–	–	–	–
Historia zmian sprzętu i oprogramowania	–	✓	–	–	–
Środki Trwałe: baza ewidencji majątku IT (definiowanie własnych typów środków, ich atrybutów oraz wartości, załączniki, import danych z pliku CSV)	–	–	–	–	–
Alarmy: instalacja oprogramowania, zmiana w zasobach sprzętowych oraz systemowych	–	✓	–	–	–
Skaner inwentaryzacji offline	–	–	–	–	–
Skanowanie i drukowanie kodów kreskowych oraz QR	–	✓	–	–	–
Aplikacja dla systemu Android umożliwiająca "spis z natury" na bazie kodów kreskowych (możliwość archiwizacji i porównywania audytów środków trwałych)	–	✓	–	–	–
Skanowanie plików użytkownika i możliwosć ich podglądnięcia	–	–	–	–	–
Monitorowanie aktywności użytkowników					
Ogólne informacje o aktywności użytkownika	–	–	–	–	–
Szczegółowy czas pracy (godzina rozpoczęcia i zakończenia aktywności oraz przerwy)	–	–	✓	–	–
Użytkowane aplikacje (aktywnie i nieaktywnie czyli całkowity czas działania aplikacji, czas faktycznego używania jej przez użytkownika oraz informacja o procesach z podwyższonymi uprawnieniami)	–	–	–	–	–
Blokowanie uruchamianych aplikacji	–	–	✓	–	–
Odwiedzane strony WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt)	–	–	–	–	–
Blokowanie stron WWW	–	–	✓	–	–
Wydruki: audyt (per: drukarka, użytkownik, komputer), koszty wydruków	–	–	–	–	–
Wysłane i odebrane wiadomości e-mail (nagłówki)	–	–	✓	–	–
Użycie łącza: generowany przez	–	–	–	–	–

Funkcje	Network	Inventory	Users	HelpDesk	DataGuard
użytkowników ruch sieciowy (wchodzący i wychodzący, lokalny i internetowy)					
Statyczny zdalny podgląd pulpitu użytkownika (bez dostępu)	-	-	✓	✓	-
Zrzuty ekranowe (historia pracy użytkownika "ekran po ekranie")	-	-	-	-	-
Pomoc użytkownikom sieci					
Baza zgłoszeń serwisowych w przeglądarce internetowej	-	-	-	-	-
Tworzenie zgłoszeń i zarządzanie zgłoszeniami (przypisywanie do administratorów z powiadamianiem e-mail)	-	-	-	✓	-
Komentarze, załączniki, zrzuty ekranowe w zgłoszeniach	-	-	-	-	-
Wewnętrzny komunikator (czat)	-	-	-	✓	-
Komunikaty wysyłane do użytkowników/ komputerów z możliwym obowiązkowym potwierdzeniem odczytu	-	-	-	-	-
Statyczny zdalny podgląd pulpitu użytkownika (bez dostępu)	-	-	✓	✓	-
Zdalny dostęp do komputerów (pracownik jak i administrator widzą ten sam ekran) z możliwym pytaniem użytkownika o zgodę oraz opcjonalnym blokowaniem myszy i klawiatury	-	-	-	-	-
Zadania dystrybucji oraz uruchamiania plików (jeśli komputer jest wyłączony podczas uruchamiania dystrybucji, dojdzie ona do skutku po jego uruchomieniu)	-	-	-	✓	-
Integracja bazy użytkowników z Active Directory	-	-	-	-	-
Przypisywanie pracowników helpdesk do kategorii zgłoszeń	-	-	-	-	-
Procesowanie zgłoszeń z wiadomości e-mail	-	-	-	-	-
Baza wiedzy	-	-	-	-	-
Zdalne wykonywanie poleceń(możliwosć wysłania komend wiersza poleceń do stacji	-	-	-	-	-

Funkcje	Network	Inventory	Users	HelpDesk	DataGuard
roboczych)					
Metryki SLA, czyli obsługa umów o gwarantowanym poziomie świadczenia usług	–	–	–	–	–
Kontrola dostępu do urządzeń i nośników danych					
Urządzenia podłączone do danego komputera	–	–	–	–	–
Lista wszystkich urządzeń podłączonych do komputerów w sieci	–	–	–	–	✓
Audyt (historia) podłączeń oraz operacji na urządzeniach przenośnych oraz na udziałach sieciowych	–	–	–	–	–
Zarządzanie prawami dostępu (zapis, uruchomienie, odczyt) dla urządzeń, komputerów i użytkowników (np. autoryzowanie firmowych szyfrowanych pendrive'ów a blokowanie pendrive'ów prywatnych pracowników)	–	–	–	–	✓
Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci, dla wybranych map sieci oraz dla grup i użytkowników Active Directory	–	–	–	–	–
Integracja bazy użytkowników i grup z Active Directory	–	–	–	–	–
Alarmy: podłączono/odłączono urządzenie mobilne, operacja na plikach na urządzeniu mobilnym	–	–	–	–	–
Inne					
Ochrona Agenta przed usunięciem	–	–	–	–	–
Axence netTools	✓	–	–	–	–
Agent na Windows	–	–	–	–	–
Agent i skaner offline na Linux Ubuntu / OS X	–	✓	–	–	–
Agent na Android	–	–	–	–	–

1.4 Konto Axence

1.4.1 Opis

W ramach aktualizacji programu Axence nVision® do wersji 7.5, dla wygody naszych Użytkowników, wprowadziliśmy Konto Axence, na którym możesz zarządzać posiadanymi licencjami.

- Począwszy od wersji 7.5 licencja Axence nVision® nie ma postaci klucza licencyjnego w formie pliku .ALS (stare typ kluczy obowiązuje jedynie do starszych wersji np. 7.1, 6, itp.).
- Obecnie **licencja ma postać kodu aktywacyjnego**, który można wkleić ręcznie do programu lub może zostać pobrany z Konta Axence. (Jak aktywować pełną wersję Axence nVision®?)
- Wygenerowany przez Axence kod aktywacyjny zostaje automatycznie wysłany bezpośrednio do przypisanego użytkownika Konta Axence (przy zakupie pierwszorazowym informacje o licencji administrator otrzymuje również mailowo).
- **Kto powinien mieć założone konto Axence?**

Każda licencja jest powiązana z Kontem Axence, które powinno zostać utworzone dla wskazanego użytkownika – najlepiej administratora, który w danej firmie będzie odpowiadać za Axence nVision®. (Wejdź na konto Axence >>) Dzięki temu program Axence nVision® będzie automatycznie pobierał wszystkie aktualizacje lub zmiany licencji.

- **Kto może założyć Konto Axence?**

Konto może zostać założone samodzielnie przez użytkownika lub przez Axence (na życzenie użytkownika).

- **Jakie dane są potrzebne do utworzenia Konta Axence?**

Aby utworzyć Konto Axence wymagane są następujące informacje:

- Imię i nazwisko administratora (lub innego wskazanego użytkownika, który będzie odpowiadać za Axence nVision® w firmie/instytucji)

- Adres email

- Nazwa firmy/instytucji, która jest właścicielem licencji.

- W przypadku, gdy użytkownik ma już założone Konto Axence, informacje te pozwolą na wyszukanie go w bazie użytkowników i połączenie jego konta z nową licencją.

- **Czy w przypadku licencji testowych muszę posiadać Konto Axence?**

Tak, wymóg utworzenia Konta Axence dotyczy wszystkich typów licencji: testowych, czasowych i bezterminowych.

- **Jeśli jesteś już naszym Klientem**:

Utworzyliśmy już dla Ciebie Konto Axence oraz wygenerowaliśmy licencję do wersji 7.5. Prosimy o sprawdzenie maila i postępowanie zgodnie z instrukcją. W razie braku informacji, prosimy o kontakt z naszym Działem Sprzedaży pod adresem email: sprzedaz@axence.net.

- Każda zmiana licencji, czyli m.in.: rozszerzenie licencji, zmiana długości Umowy Serwisowej, wydłużenie okresu ważności licencji, odbywa się poprzez Konto Axence, a Klient nie otrzymuje już dodatkowego/nowego kodu. Automatycznie zmodyfikowana licencja zostaje przesyłana do programu Axence nVision®.

1.4.2 Rejestracja

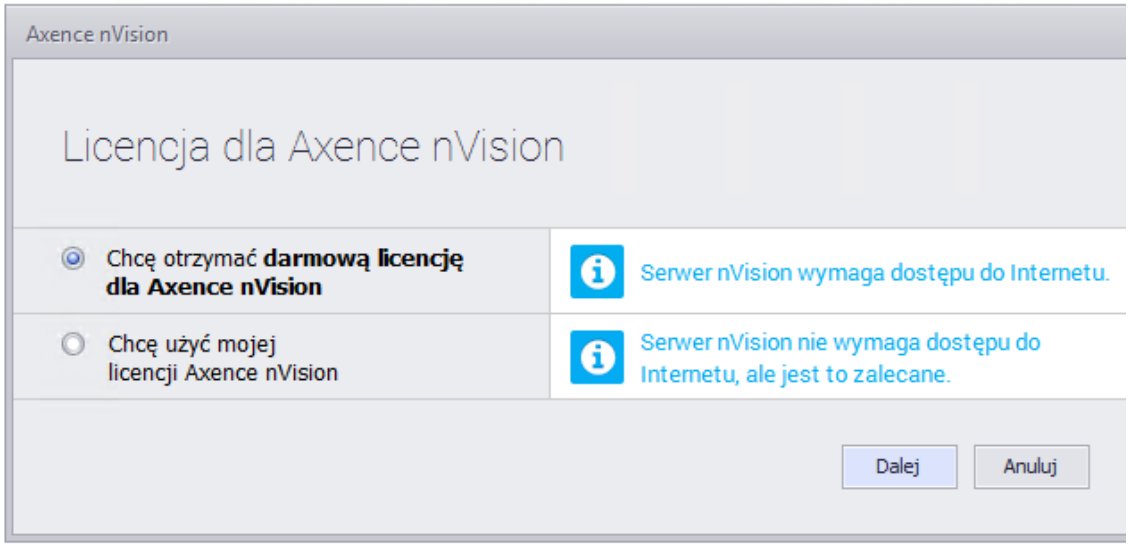
W wersji 7.5 nVision, wprowadzona została integracja z kontem Axence. Konto umożliwia zakup oraz łatwe zarządzanie licencjami - zarówno darmowymi jak i zakupionymi licencjami Axence nVision®.

Konta Axence są zakładane automatycznie na adres podany w formularzu zamówienia licencji. Dla kont założonych automatycznie, wysyłana jest wiadomość e-mail z linkiem do resetu hasła.

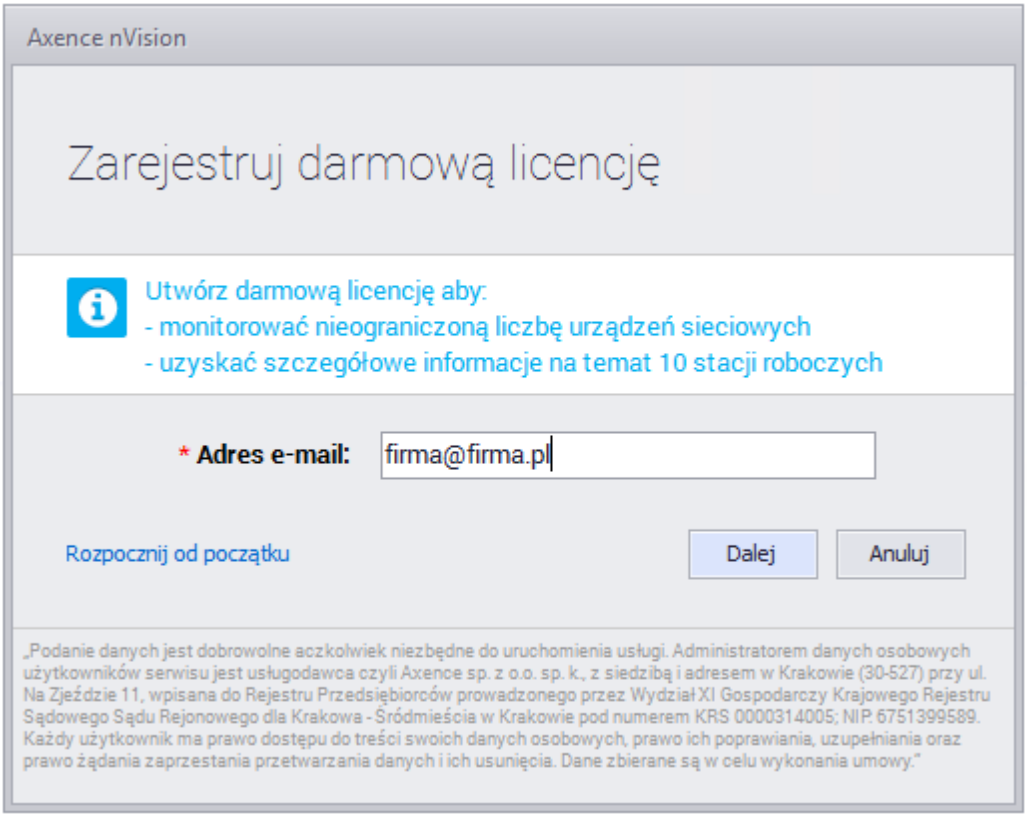
Rejestracji konta Axence można dokonać:

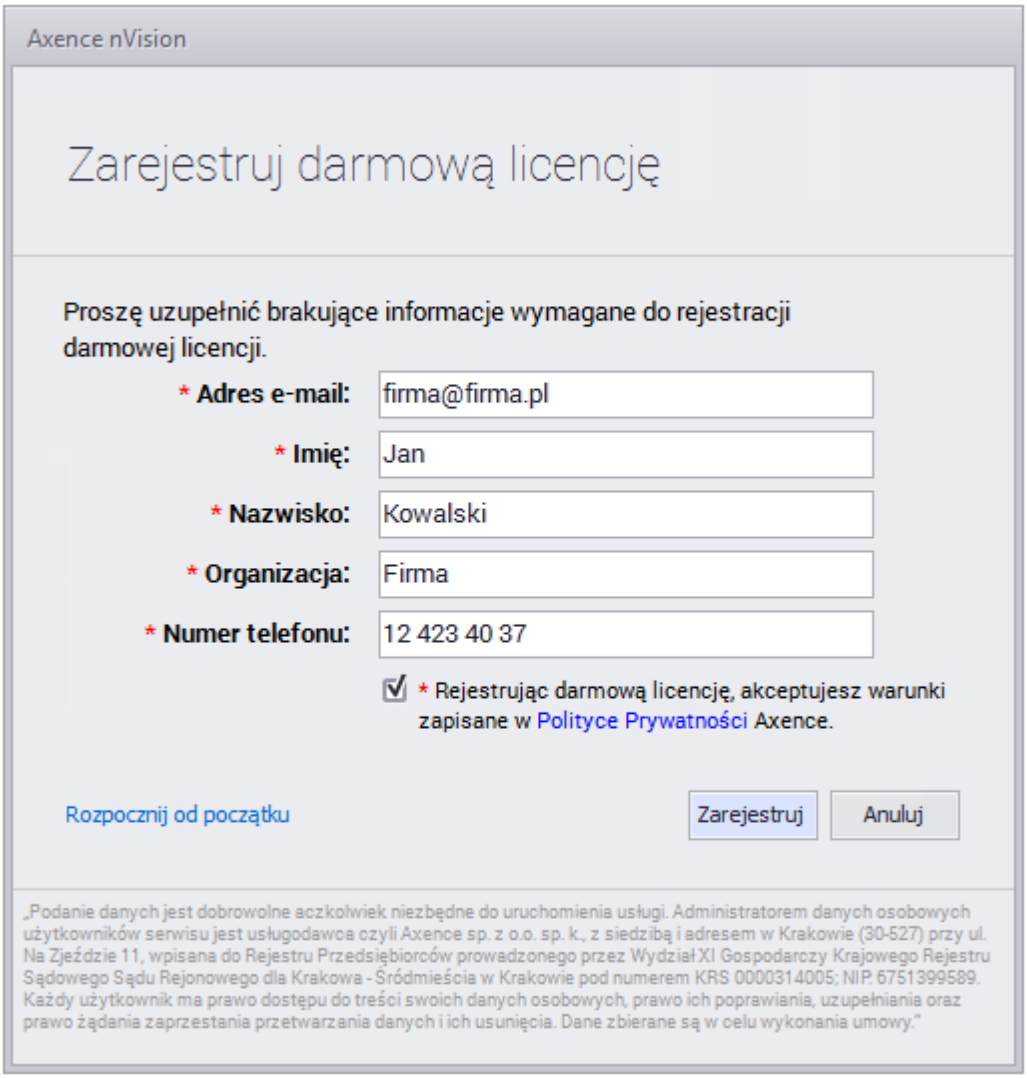
- podczas instalacji Axence nVision® - **podczas rejestracji darmowej licencji dla Axence nVision®** (wymagany dostęp do sieci Internet)

  1. W oknie wyboru licencji zaznacz **Chcę otrzymać darmową licencję dla Axence nVision®** i kliknij przycisk **Dalej**

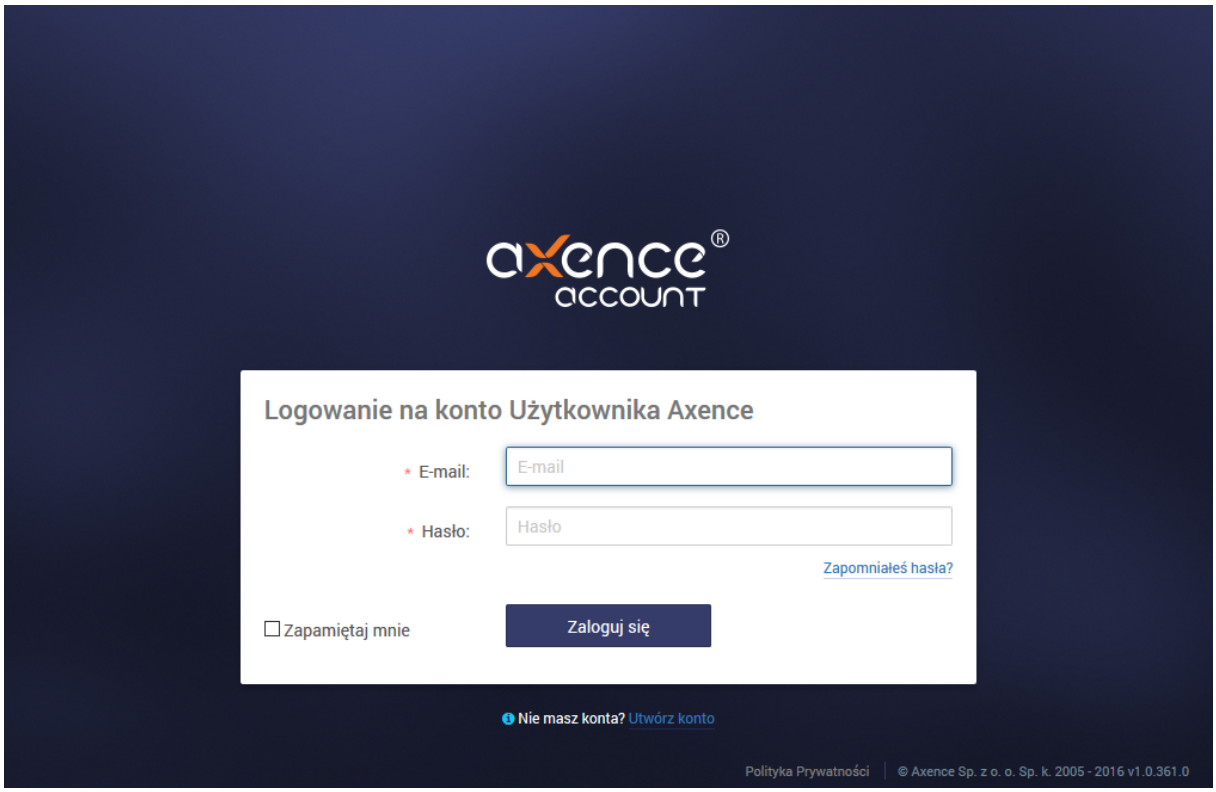


  2. Wprowadź adres e-mail, wypełnij formularz rejestracyjny:



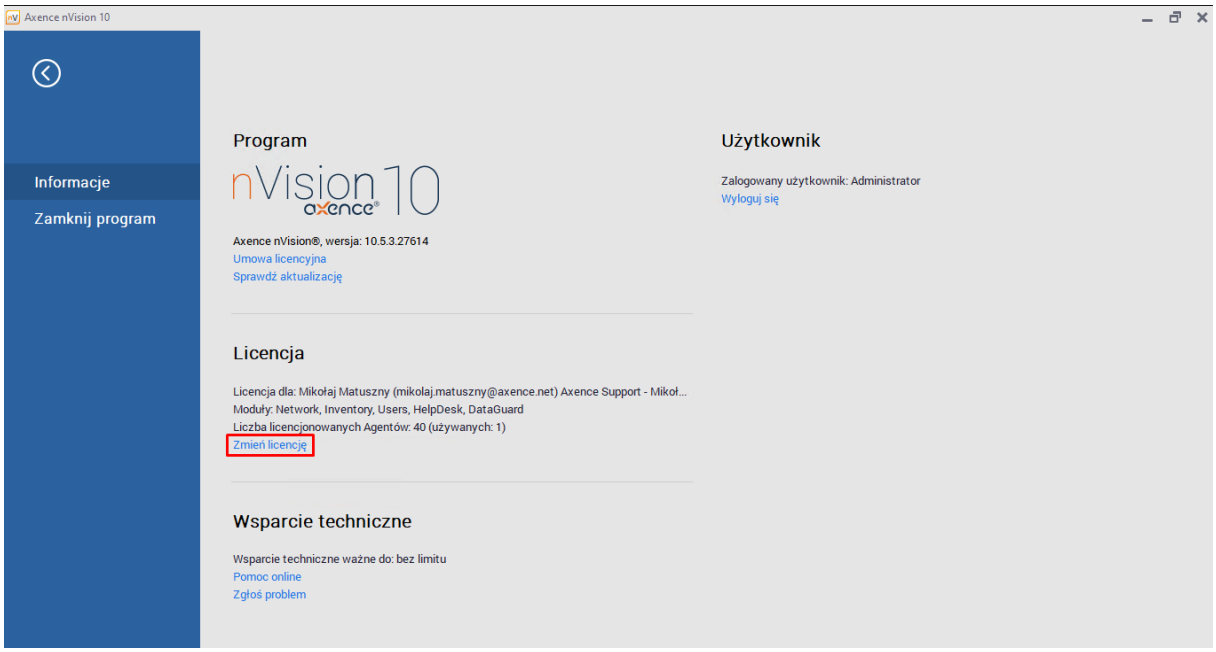


- poprzez przeglądarkę internetową, na stronie: https://account.axence.net/

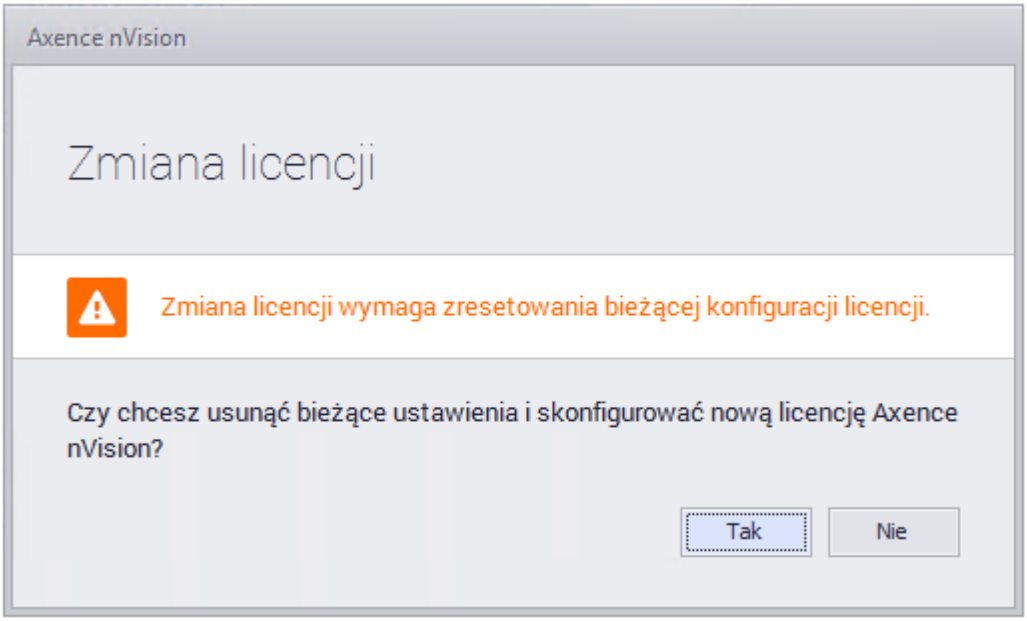


1.4.3 Logowanie

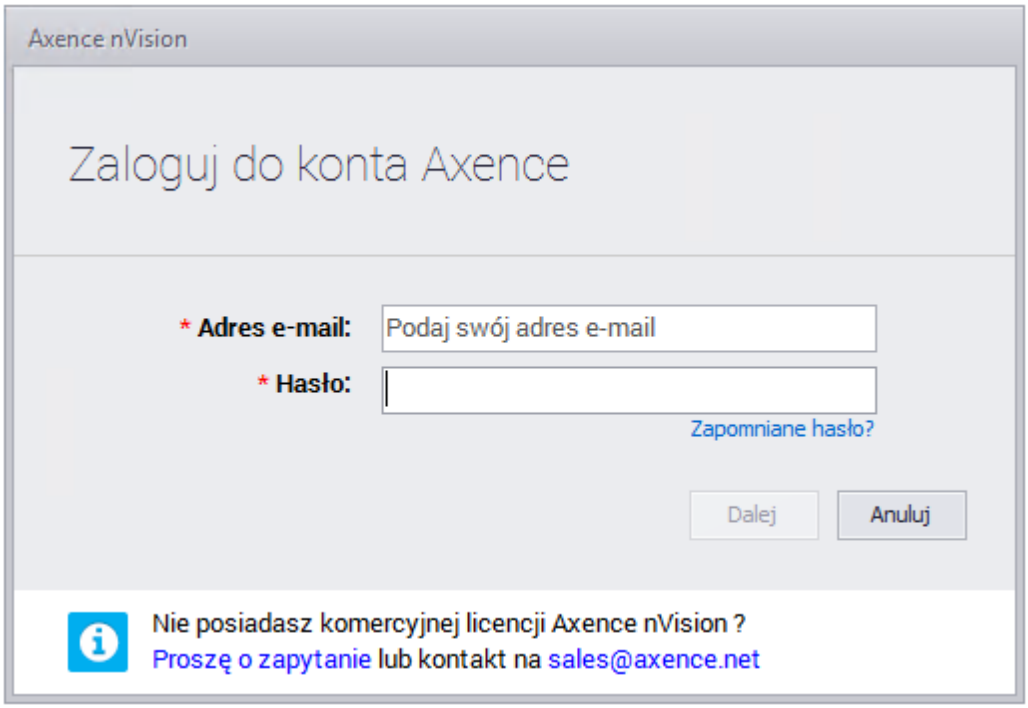
Aby zalogować się w programie do konta Axence, należy w lewym górym rogu ekranu wybrać zakładkę **Axence nVision** a następnie w sekcji **Licencja** kliknąć przycisk **Zmień licencję.**



Następnie zostanie wyswietlone okno:

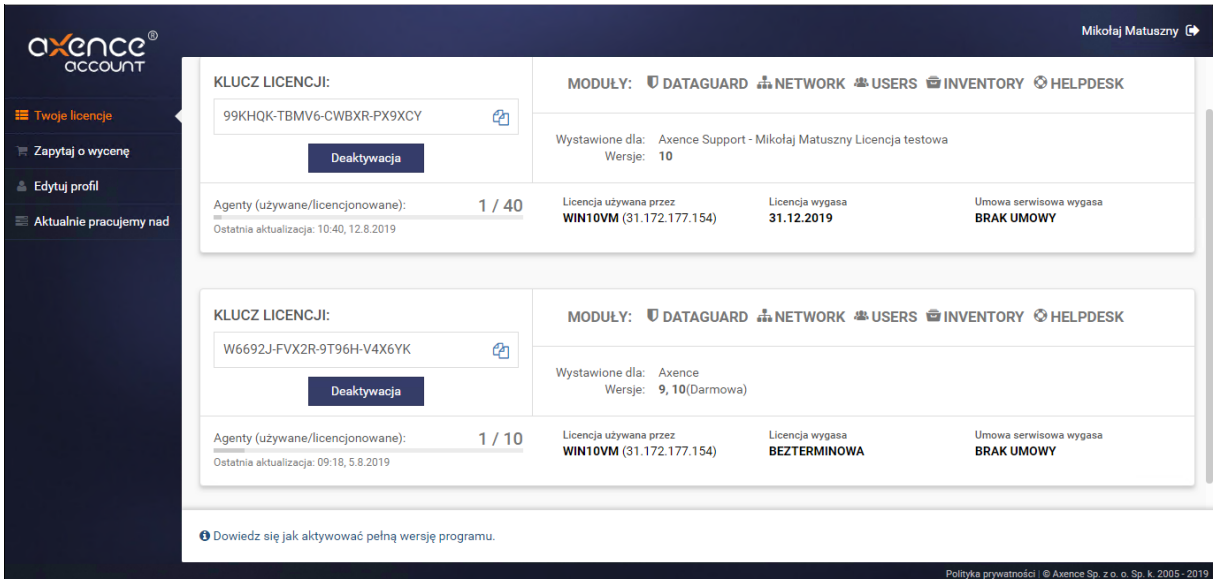


Kliknięcie przycisku **Tak** spowoduje odpięcie licencji i wyświetlenie okna logowania do konta Axence *(zebrane w monitoringu dane oraz konfiguracja programu zostaną zachowane)*.
Następnie należy wprowadzić adres e-mail oraz hasło zarejestrowanego konta powiązanego z licencją:



1.4.4 Zarządzanie kontem

Zarządzanie kontem Axence, możliwe jest po zalogowaniu na stronie: https://account.axence.net



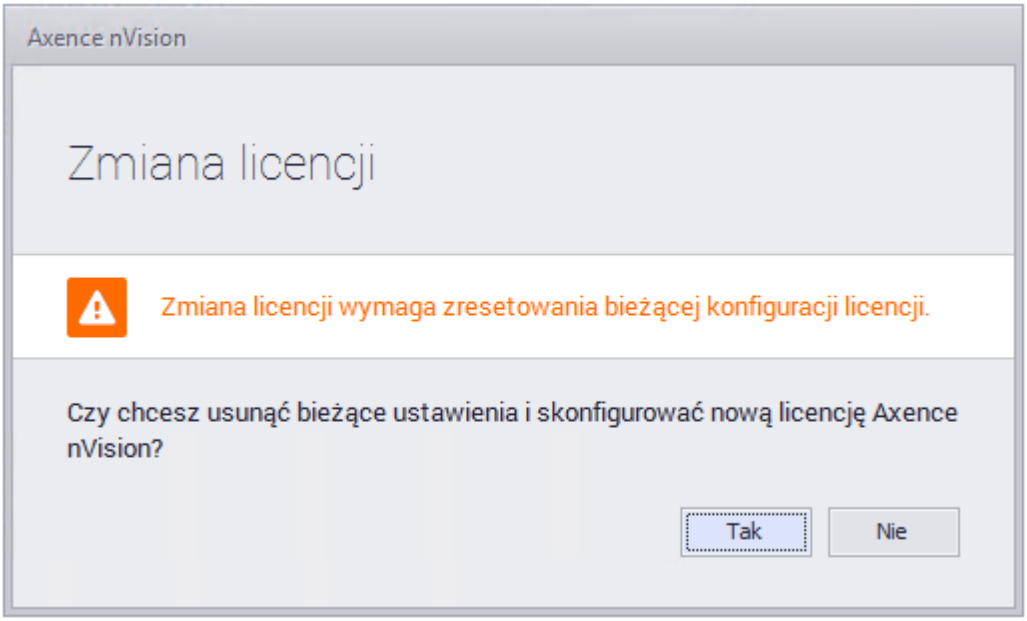
W wyglądzie strony głównej konta Axence wyróżnić można panel administracyjny znajdujący się w lewej części okna. Panel zawiera łącza do podstron:

Menu	Opis
Twoje licencje	Pozwala na podgląd informacji dotyczących zakupionych licencji.
Zapytaj o wycenę	Pozwala na kontakt z działem handlowym Axence w celu wyceny
Edytuj profil	Podgląd podstawowych informacji o koncie wraz z możliwością ich edycji.
Aktualnie pracujemy nad	Prezentuje listę funkcji, nad którymi aktualnie trwają prace programistyczne

1.4.5 Aktywacja programu

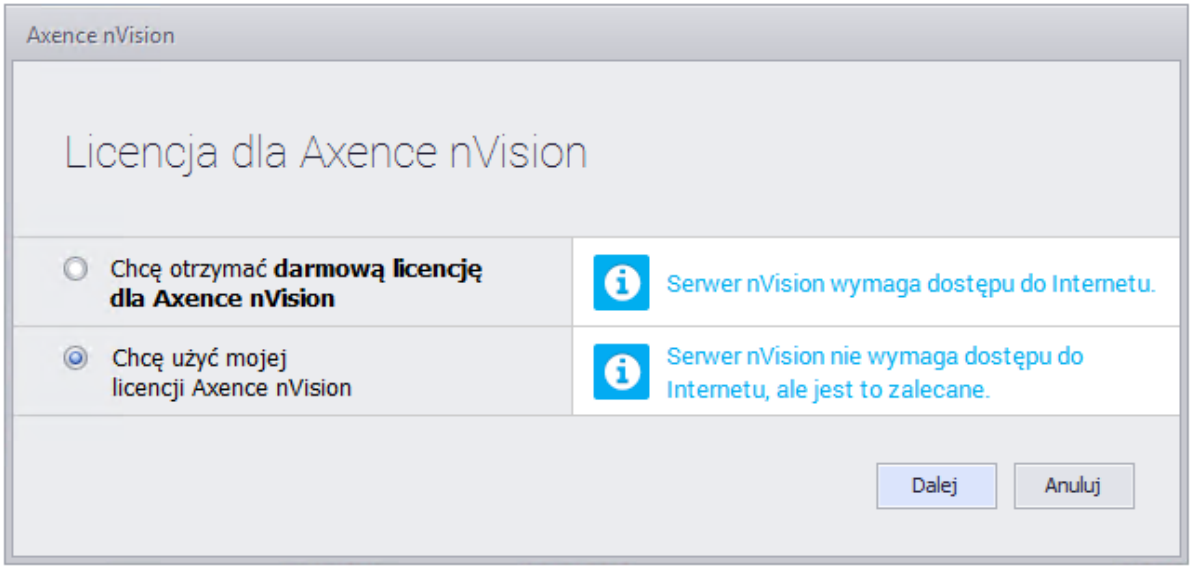
Informacja o używanej licencji wyświetlana jest po kliknięciu na wstążce karty **Axence nVision**.

W celu wprowadzenia posiadanej licencji należy wybrać **Zmień licencję**.Wyświetlone zostanie okno:



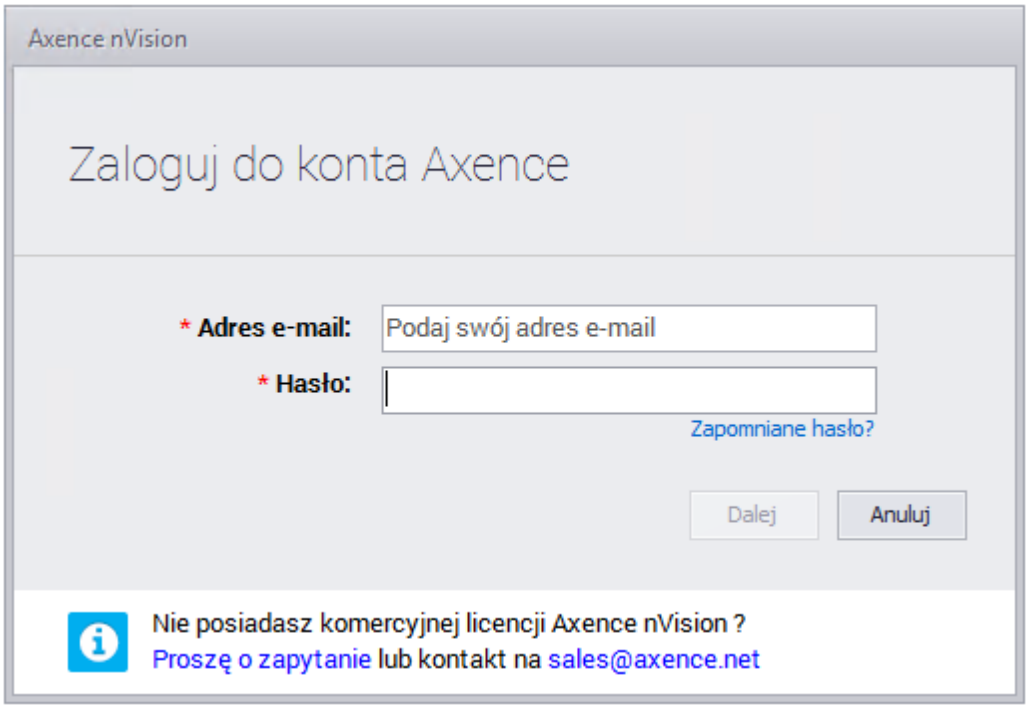
Kliknięcie przycisku **Tak** spowoduje odpięcie licencji i wyświetlenie okna logowania do konta Axence *(zebrane w monitoringu dane oraz konfiguracja programu zostaną zachowane)*.

W oknie wyboru licencji wybierz zaznacz opcję **Chcę użyć mojej licencji Axence nVision®** i kliknij przycisk **Dalej:**

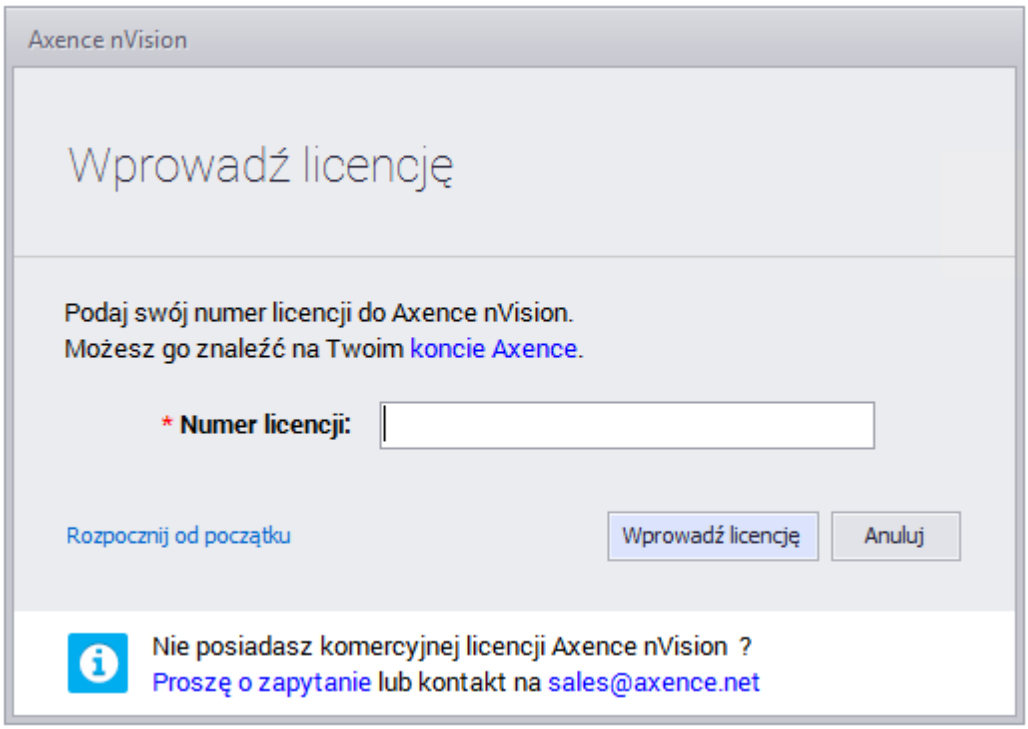


Aktywacja online

1. Wprowadź adres e-mail oraz hasło zarejestrowanego konta powiązanego z licencją. Kliknij przycisk **Dalej:**



2. W wyświetlonym oknie **Wprowadź licencję** wpisz (lub wklej) kod licencji, który został przesłany we wiadomości e-mail lub skopiuj go strony konta Axence.

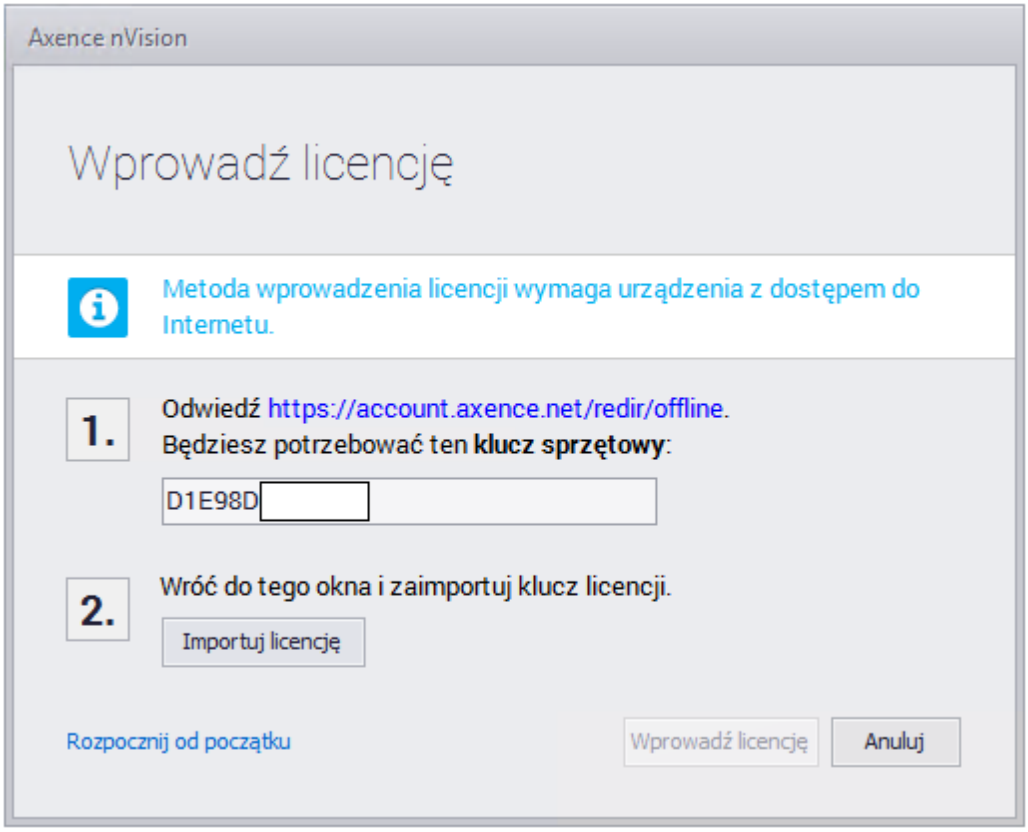


3. Po kliknięciu przycisku **Wprowadź licencję** program zostanie aktywowany.

W przypadku gdy Serwer nVision (usługa **Axence nVision**) podczas uruchamiania nie uzyska połączenia z Internetem, postępuj zgodnie ze wskazówkami wyświetlonymi na ekranie.

Aktywacja offline

Postępuj zgodnie z wyświetlonymi wskazówkami:



1. Na komputerze z dostępem do Internetu otwórz stronę https://account.axence.net/#/offline
2. W formularzu generowania licencji offline wypełnij pola:

   Nazwa komputera: *(dowolna nazwa komputera)*

   Klucz licencji: *(numer licencji skopiowany ze strony https://account.axence.net/licenses np.: 4B4MC9-MG4PQ-XYZXY-XYZXY)*

   Klucz komputera: *(12-znakowy klucz komputera widoczny w oknie **Wprowadź licencję** w punkcie 1.)*

3. W formularzu generowania licencji offline kliknij przycisk **Pobierz klucz licencyjny offline** a następnie **Zapisz do pliku.**
4. Przenieś zapisany plik licencji offline **AxenceOfflineKey.txt** na dysk twardy Serwera nVision, kliknij przycisk **Importuj licencję** i wskaż zapisany plik. Kliknij przycisk **Wprowadź licencję.**

Aktywacja wersji darmowej:

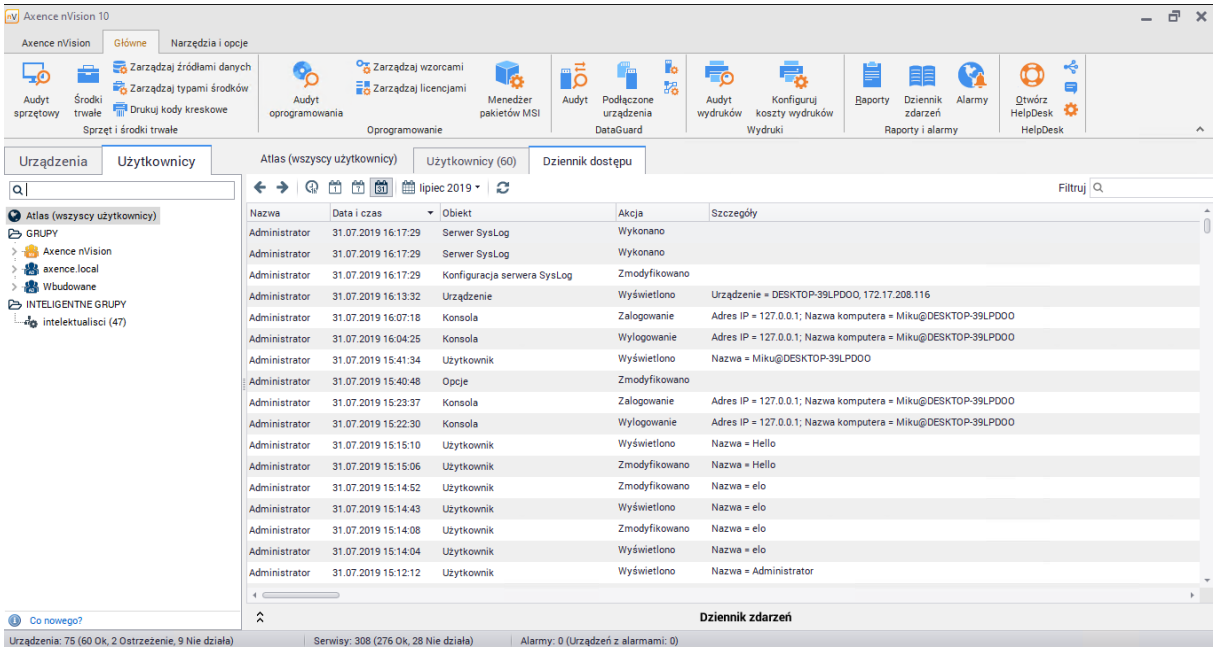
W celu aktywacji darmowej wersji nVision, należy zaznaczyć opcję **Chcę otrzymać darmową licencję dla Axence nVision®** nawet w przypadku, gdy licencja darmowa została uprzednio utworzona.

1.5 Dziennik dostępu Administratorów

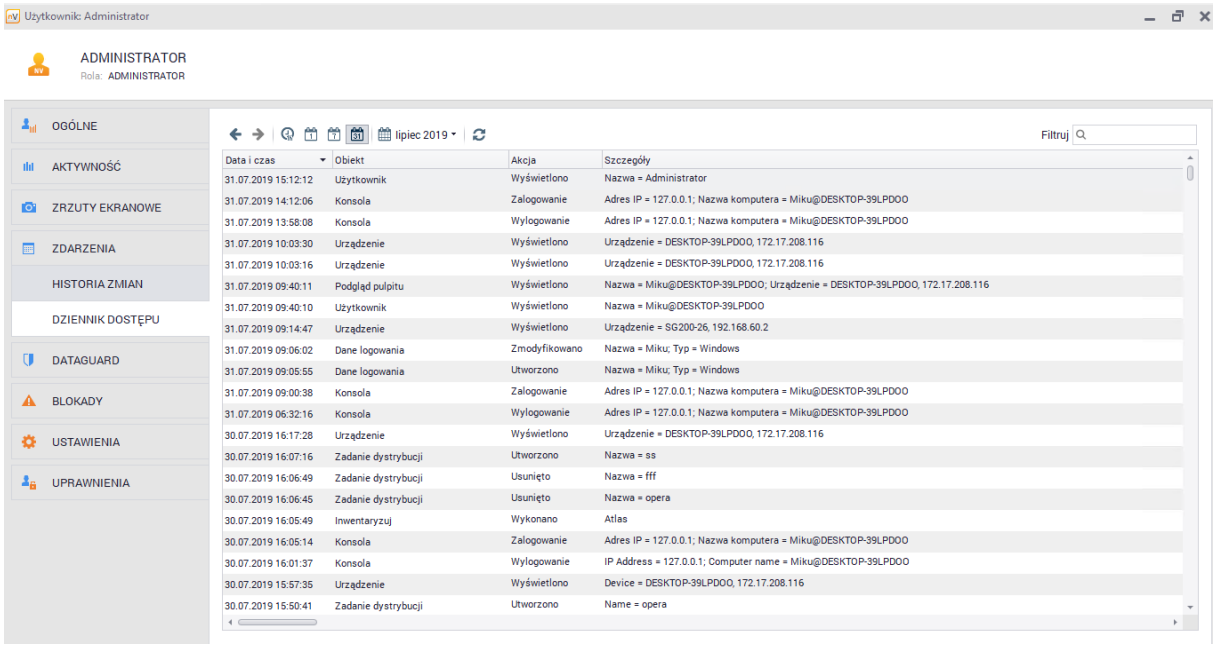
nVision umożliwia przeglądanie Dziennika Dostępu Administratorów.

Aby przejść do Dziennika dostępu należy wybrać z panelu map kartę **Użytkownicy** a następnie zakładkę **Dziennik dostępu**. Wyświetlone zostaną informacje o czynnościach wykonanych przez wszystkich Administratorów wraz z datą i dokładnym czasem ich wykonania.

Ikony zegara i kartek kalendarza umożliwiają wyświetlenie informacji z ostatniej godziny/dnia/tygodnia/ miesiąca. Ikona kalendarza umożliwia wyświetlenie informacji z wybranego dnia.



Aby wyświetlić **Dziennik dostępu** dla konkretnego administratora, należy dwukrotnie kliknąć lewym przyciskiem myszy na nazwie jego konta a następnie przejść do zakładki **Zdarzenia** a następnie **Dziennik dostępu.**



Powiązane tematy

Uprawnienia Adminstratorów

Jak zainstalować zdalną konsolę nVision?

1.6 Uprawnienia Administratorów

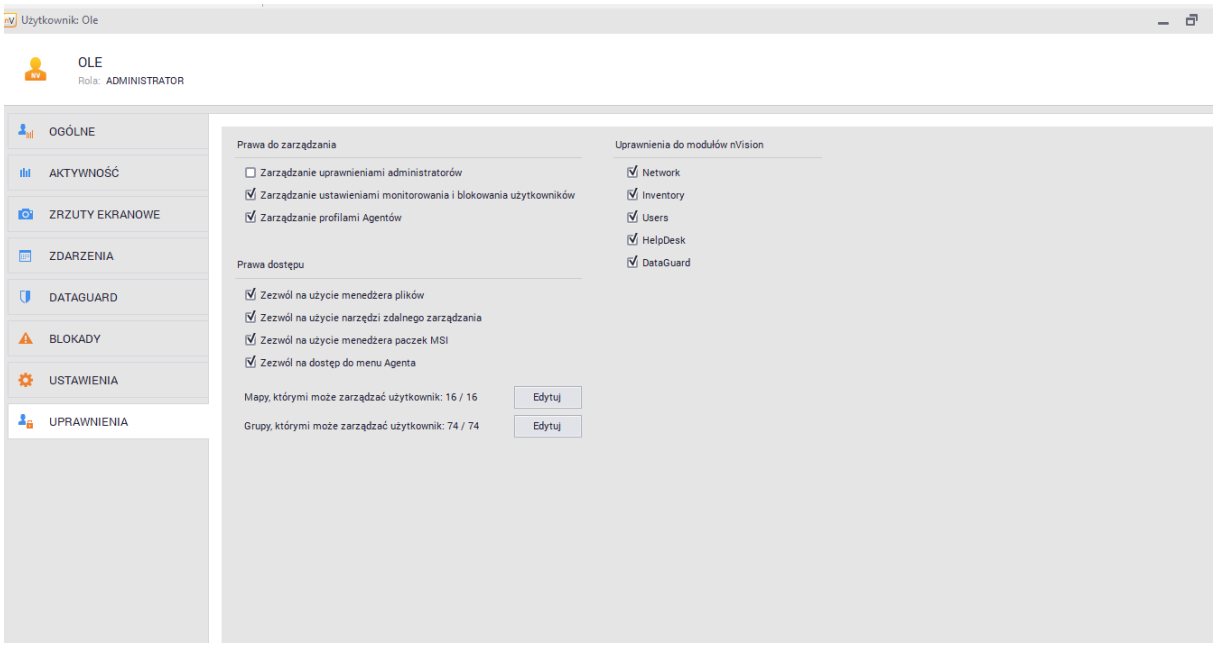
nVision umożliwia konfigurowanie uprawnień administratorów.

Aby przejść do zarządzania uprawnieniami Administratorów należy zalogować się na wbudowane konto Administrator a następnie wybrać z panelu map kartę **Użytkownicy** i dwukrotnie kliknąć lewym przyciskiem myszy na nazwie konta wybranego użytkownika administracyjnego, po czym przejść do zakładki **Uprawnienia.**

Wyświetlone zostaną informacje dotyczące zarządzania prawami dostępu do map i grup użytkowników oraz wykonywania czynności w ramach wybranych modułów funkcjonalnych programu.

Zaznaczając pole **Zarządzanie uprawnieniami administratorów** można zezwolić danemu administratorowi na dostęp do zakładki **Uprawnienia** we właściwościach konta innego administratora.

Uwaga: Nie można zmienić praw dostępu do modułów dla wbudowanego konta Administrator Axence nVision (Administratora, którego konto zostało utworzone podczas pierwszego uruchomienia nVision).



Powiązane tematy

- Dziennik dostępu Administratorów
- Jak zainstalować zdalną konsolę nVision?

Część II

2 Wymagania i konfiguracja

2.1 Wymagania

System operacyjny (zainstalowany aktualny Service Pack)	Serwer nVision*	Konsola nVision	Agent nVision
Windows XP	✗	✓**	✓**
Windows Server 2003	✗	✓**	✓**
Windows Vista	✗	✓**	✓**
Windows Server 2008	✓	✓	✓
Windows 7	✓	✓	✓
Windows Server 2008 R2	✓	✓	✓
Windows 8	✓	✓	✓
Windows Server 2012	✓	✓	✓
Windows 8.1	✓	✓	✓
Windows Server 2012 R2	✓	✓	✓
Windows 10	✓	✓	✓
Windows Server 2016	✓	✓	✓***

**Produkcyjnie Serwer nVision powinien być używany jedynie na serwerowych edycjach Windows, ze względu na treść zapisów licencyjnych Microsoft, które nie zezwalają na hostowanie aplikacji na klienckich edycjach Windows.*

***Instalacja jest możliwa, ale dla tej wersji systemu program nie jest już wspierany.*
Proszę jednocześnie pamiętać, iż w przypadku problemów technicznych może okazać się, że nie będziemy w stanie znaleźć dla nich rozwiązania. Stąd gorąco zalecamy aktualizację systemu (dla którego istnieje wsparcie producenta).
https://support.microsoft.com/en-us/help/22882/windows-vista-end-of-support

**** Na tej wersji systemu Windows, przy włączonym SecureBoot, może nie działać filtrowanie sieci, monitorowanie e-mail oraz DataGuard.*

HelpDesk oraz czat (są testowane oraz) działają poprawnie w najnowszych wersjach przeglądarek internetowych.

Serwer nVision musi działać na statycznym adresie IP.

Serwer nVision:

- 2 rdzenie CPU,
- 4 GB RAM,
- 10 GB wolnego miejsca na dysku,
- system operacyjny Windows Server w wersji 2008 lub nowszy.

Zalecane dla monitorowania powyżej 1000 Agentów:

- nVision na dedykowanej maszynie fizycznej (nie wirtualnej),
- 64-bitowy system operacyjny,
- procesor czterordzeniowy,
- minimum 8GB RAM (dla każdego dodatkowego 1000 Agentów kolejne 8GB RAM),
- szybki dysk twardy.

Wymagana szybkość procesora, wielkość dysku oraz zajętość pamięci są zależne od liczby monitorowanych urządzeń i zakresu monitorowanych danych.

Aby dowiedzieć się więcej o konfiguracji przy monitorowaniu dużej liczby Agentów (powyżej 250), przejdź do rozdziału Wydajność nVision.

Konsola nVision:

- 2 rdzenie CPU,
- 2 GB RAM,
- 400 MB wolnego miejsca na dysku,
- Windows XP lub nowszy,
- Połączenie do Serwera nVision w sieci LAN na port TCP 4436,
- Do poprawnego generowania raportów wymagana jest przeglądarka Internet Explorer w wersji min. 8.0 (zalecana najnowsza dostępna wersja).

Agent nVision:

- 1 rdzeń CPU,
- 128 MB RAM,
- 100 MB wolnego miejsca na dysku,
- Windows XP lub nowszy,
- Połączenie do Serwera nVision na port TCP 4436.

Celem prawidłowej pracy Serwera nVision, Konsol nVision, Agentów nVision oraz netTools należy na każdym komputerze dodać katalog instalacji

(przykładowo: „C:\Program Files (x86)\Axence") do wykluczeń oprogramowania antywirusowego - przykłady:

- http://kb.eset.com/esetkb/index?page=content&id=SOLN2153&viewlocale=pl_PL
- http://support.kaspersky.com/pl/10017
- http://www.avg.com/pl-pl/faq.num-5187

Po dodaniu wykluczenia należy zrestartować tak skonfigurowane komputery.

Przeglądarki monitorowane przez nVision:

- Internet Explorer,
- Microsoft Edge,
- Mozilla Firefox,
- Google Chrome.

2.2 Porty

Aby możliwa była komunikacja między Agentami a nVision, konieczne jest otwarcie określonych portów na urządzeniach z Agentami i na urządzeniu z uruchomionym nVision. Agenty i nVision otwierają wymagane porty w zaporze Windows automatycznie. Jeśli jednak masz jeszcze jakąś inną zaporę, musisz otworzyć je ręcznie. Porty te muszą być także otwarte na ruterze, jeśli Agenty działają poza siecią lokalną komputera z nVision.

Porty otwarte na urządzeniu z nVision

Port TCP	Opis
4434	Informacje diagnostyczne
4436	Komunikacja z Agentami (stałe połączenie).
8080*	WebAccess - dostęp do nVision przez przeglądarkę. * Wartość konfigurowalna. Może być zmieniona w nVision **Narzędzia | Opcje | Zdalny dostęp**.

Porty otwarte na zdalnych urządzeniach

W przypadku, gdy porty na urządzeniu z Agentem są zamknięte, Agent wciąż będzie zbierał monitorowane dane i przesyłał je do nVision, ale niektóre operacje wykonane w nVision nie będą miały natychmiastowego skutku w Agencie.

Port TCP	Opis
4433	linformacje diagnostyczne
135,139, 445, 593	WMI, m.in. monitorowanie liczników Windows (Monitorowanie i zarządzanie Windows przez WMI). Uwaga: liczniki i usługi Windows mogą być także monitorowane przez Agenta (zobacz Monitorowanie usług Windows).

Dodatkowo, przy monitorowaniu serwisów TCP/IP należy otworzyć na zdalnym urządzeniu odpowiednie porty w zależności od monitorowanej usługi, np. TCP 80 dla HTTP.

Aby dowiedzieć się więcej o komunikacji Agentów z nVision, przejdź do rozdziału Komunikacja między Agentem a nVision.

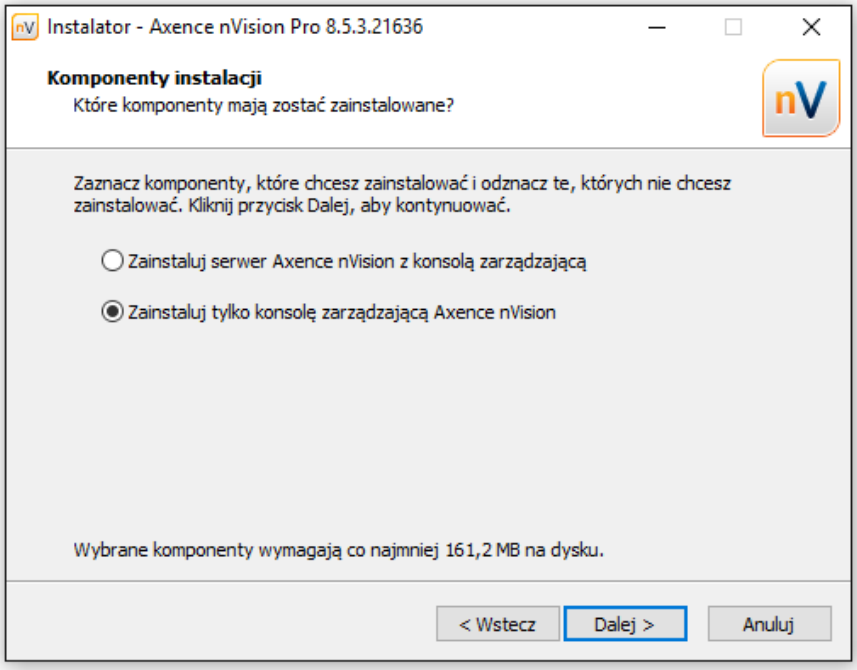
Aby dowiedzieć się więcej o zdalnym dostępie oraz o stałym połączeniu Agenta i nVision, przejdź do rozdziału Zdalny dostęp.

Aby dowiedzieć się więcej o konfigurowaniu Agentów na komputerach mobilnych, przejdź do rozdziału Konfiguracja połączenia Agentów zainstalowanych na komputerach mobilnych.

2.3 Zdalna konsola nVision

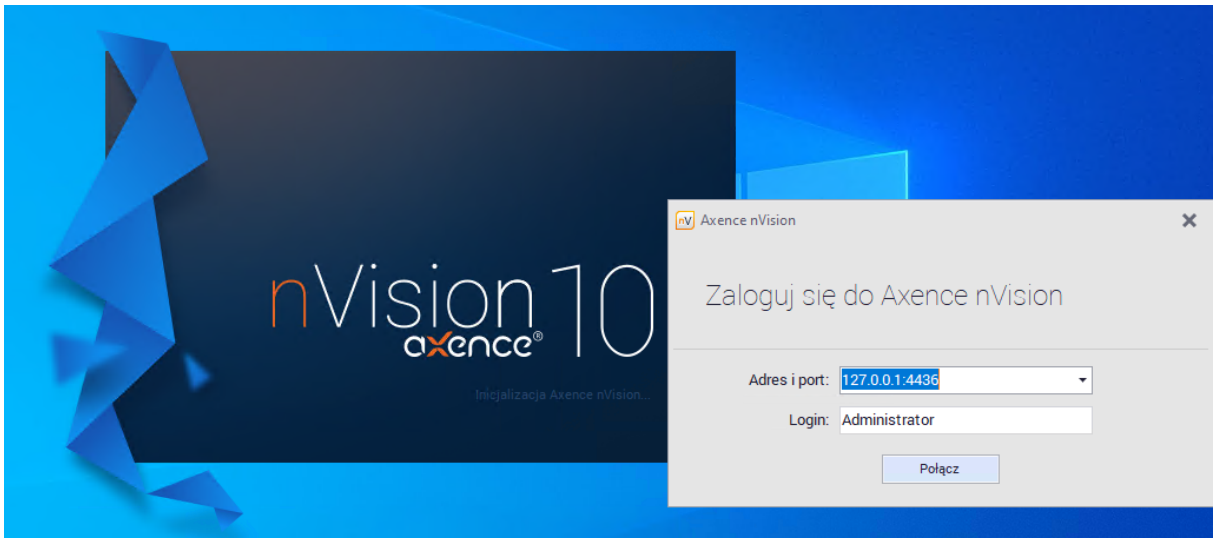
Wersja 7 nVision wprowadziła możliwość rozdzielenia instalacji Konsoli nVision od Serwera. Instalacja zdalnej Konsoli pozwala na jednoczesną pracę kilku Adminstratorów z programem.

Aby zainstalować wyłącznie Konsolę zarządzania nVision należy użyć tego samego pliku instalatora co w przypadku podstawowej instalacji Serwera. Instalator umożliwi wybór komponentów do zainstalowania - należy wybrać opcję "Zainstaluj tylko konsolę zarządzającą" tak jak przedstawiono na rys. poniżej:



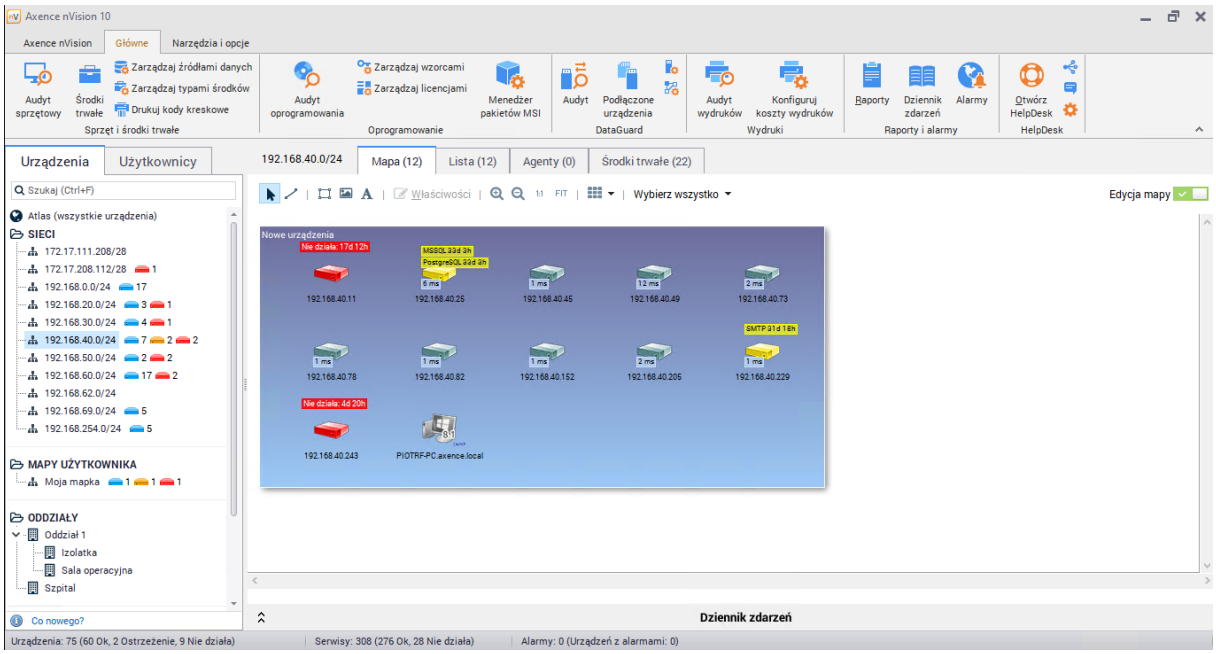
Po zainstalowaniu Konsoli i dodaniu wykluczeń skanowania w oprogramowaniu antywirusowym na katalog instalacji nVision, można uruchomić program.

W oknie logowania należy podać login i hasło Administratora nVision oraz adres IP i port zdalnego komputera, na którym zainstalowany jest serwer nVision:



2.4 Układ okna

Układ okna nVision jest intuicyjny i prosty w użyciu.



Wstążka
Funkcje programu zostały pogrupowane i umieszczone na wstążce w 3 kartach:

Karta "Axence nVision"

Karta prezentuje informacje o wersji nVision, zalogowanym użytkowniku, wprowadzonej licencji oraz dacie wygaśnięcia umowy serwisowej.

Karta "Główne"

Grupa	Funkcje	Opis

Sprzęt i środki trwałe	Audyt sprzętowy	Prezentuje szczegółowe dane dotyczące konfiguracji sprzętowej na komputerach z zainstalowanymi Agentami.
	Środki trwałe	Prezentuje listę wszystkich środków trwałych przypisanych do urządzeń.
	Zarządzaj źródłami danych	Pozwala zaimportować środki trwałe ze spisu w postaci pliku .CSV.
	Zarządzaj typami środków	Pozwala zarządzać szablonami typów środków trwałych.
	Drukuj kody kreskowe	Okno zarządzania wydrukami etykiety (naklejek) dla środków trwałych.
Oprogramowanie	Audyt oprogramowania	Prezentuje listę aplikacji wykrytych na komputerach z Agentami.
	Zarządzaj wzorcami	Pozwala zarządzać wzorcami wykorzystywanami do identyfikowania aplikacji, sterowników i systemów operacyjnych.
	Zarządzaj licencjami	Pozwala zarządzać licencjami wykorzystywanymi w audycie oprogramowania.
	Menedżer pakietów MSI	Pozwala zarządzać instalacjami oprogramowania w postaci przygotowanych paczek instalatorów.
DataGuard	Audyt	Umożliwia przeglądnięcie historii podłączeń i operacji na plikach an zewnętrznych nośnikach.
	Podłączone urządzenia	Pokazuje listę urządzeń podłączonych do Agentów.
	Zarządzaj urządzeniami	Umożliwia skonfigurowanie praw dostępu do urządzeń podłączonych do Agentów.
	Zarządzaj zaufanymi jednostkami	Umożliwia skonfigurowanie praw dostępu do nośników dla użytkowników.
Wydruki	Audyt wydruków	Pozwala wyświetlić listę wykonanych przez użytkowników wydruków.
	Konfiguruj koszty wydruków	Pozwala skonfigurować koszty wydruków.
Raporty i alarmy	Raporty	Umożliwia przygotowanie szablonów i wygenerowanie raportów.
	Dziennik zdarzeń	Wyświetla wszystkie wygenerowane alarmy.
	Alarmy	Konfiguracja alarmów dla Atlasu.
HelpDesk	Otwórz HelpDesk	Otwiera interfejs WWW HelpDesku.
	Zadania dystrybucji	Pozwala na zdalne przesyłanie i wykonywanie plików na Agentach.
	Komunikaty	Umożliwia łatwe przekazywanie informacji do użytkowników z zainstalowanym Agentem.
	Konfiguracja	Otwiera okno ustawień HelpDesku.

Karta "Narzędzia i opcje"

Grupa	Funkcje	Opis
Urządzenia i użytkownicy	Dodaj użytkownika	Tworzy konto nowego użytkownika.
	Dodaj grupę	Tworzy nową grupę.
	Dodaj urządzenie	Pozwala dodać ikonę nowego urządzenia (np. niewykrywalnego przez skanowanie ping).
	Pokaż duplikaty urządzeń	Pokazuje listę urządzeń ze zduplikowanymi adresami IP/MAC lub nazwami DNS.
	Utwórz licznik dla urządzeń	Pozwala utworzyć liicznik wydajności na wielu urządzeniach.
Narzędzia	Uruchom netTools	Uruchamia program netTools.
	Wykryj nową sieć	Uruchamia kreator skanowania sieci.
	Dystrybuuj plik przez WMI	Uruchamia menu dystrybucji przez WMI
SNMP i Syslog	Serwer Pułapek SNMP	Konfiguracja serwera oraz przeglądanie zebranych pułapek SNMP.
	Serwer Syslog	Konfiguracja serwera oraz przeglądanie zebranych komunikatów Syslog.
	Kompilator MIB	Pozwala zaimportować pliki MIB.
Agenty	Zainstaluj Agenta nVision	Pozwala przygotować plik instalatora Agenta w postaci paczki MSI.
	Odinstaluj Agenta nVision	Umożliwia zdalną deinstlację Agentów, które łaczą się z Serwerem.
	Importuj skany inwentaryzacji	Umożliwia inwentaryzację komputerów bez zainstalowanego Agenta.
	Propaguj nowy adres Atlasu	Pozwala przygotować Agenty do przeniesienie instalacji serwera nVision na inną maszynę.
	Zarządzanie profilami Agentów	Zarządzanie konfiguracją Agentów.
	Plik wykonywalny skaner inwentaryzacji	Umożliwia zapisanie pliku skanera inwentaryzacji.
Opcje	Opcje	Pozwala na zmianę opcji działania nVision.
	Właściwości Atlasu	Podstawowe właściwości Atlasu (styl wizaulizacji, ignorowane urządzenia itp.)
	Filtry dla inteligentnych map	Pozwala utworzyć inteligentne mapy, które grupują urządzenia spełniające określone warunki.
	Filtry dla	Pozwala utworzyć inteligentne grupy, które grupują konta

inteligentnych grup	użytkowników spełniające określone warunki.
Zarządzaj	Konfiguracja: zdarzeń i akcji alarmów, stylów wizualizacji ikon, dodatkowych narzędzi, danych logowania oraz oddziałów.

Panel Atlasu

Panel Atlasu jest zlokalizowane jest w lewej części okna i podzielony na dwie zakładki: **Urządzenia** oraz **Użytkownicy**.

Zakładka **Urządzenia** przedstawia listę wszystkich urządzeń pogrupowanych w postaci map. Aby dowiedzieć się więcej o mapach, przejdź do rozdziału Praca z atlasami, mapami i urządzeniami.
Po wybraniu mapy urządzeń w drzewie, jest ona prezentowana w centralnym widoku.

W zakładce **Użytkownicy** prezentowane są konta użytkowników nVision oraz ich grupy. Zarówno konta i grupy są nośnikami ustawień monitorowania oraz blokad.
Zapoznaj się z ustawieniami monitorowania oraz blokowania.

2.5 Konfiguracja

2.5.1 Podstawowa konfiguracja

Planowanie monitorowania

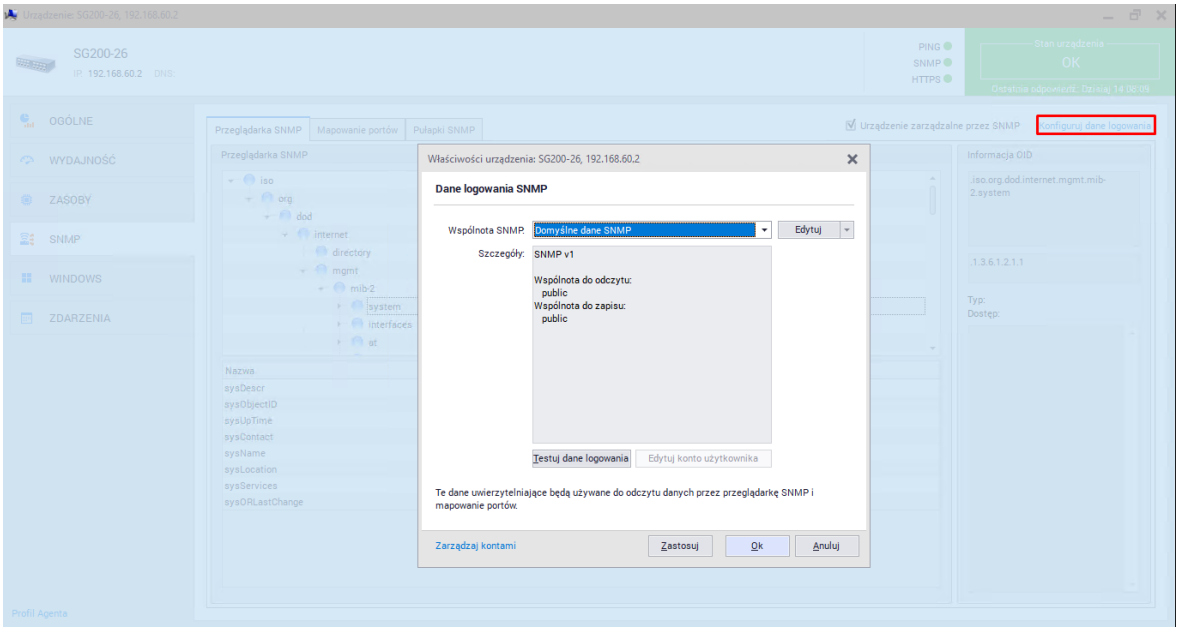
Aby z powodzeniem monitorować wszystkie urządzenia w Twojej sieci, przed uruchomieniem skanera sieci nVision musisz wykonać określone kroki. Oto lista wszystkich czynności, które należy przeprowadzić, aby w pełni wykorzystywać wszystkie funkcje nVision:

Prawidłowe skonfigurowanie urządzeń SNMP

Aby właściwie monitorować wszystkie urządzenia w sieci, konieczne jest wykonanie kilku niezbędnych kroków zanim skaner sieciowy zostanie uruchomiony. Przede wszystkim należy odpowiednio skonfigurować urządzenia SNMP (najważniejsze jest ustawienie właściwego adresu IP i wspólnoty SNMP). Aby dowiedzieć się więcej o konfiguracji urządzeń SNMP, skorzystaj z odpowiedniej dokumentacji urządzenia.

Konfiguracja danych logowania

Aby monitorować SNMP należy podać wspólnotę SNMP. Wspólnotę możesz określić w oknie **Informacje o urządzeniu** w zakładce SNMP.



Wymagania przy monitorowaniu urządzeń SNMP

Monitorowanie	Używany protokół	Wymagania
Liczniki wydajności SNMP	SNMP	• Właściwie ustawione dane logowania. • Urządzenie skonfigurowane jako zarządzalne przez SNMP.
Porty i interfejsy na switch'ach i router'ach		• Przynajmniej jeden interfejs zaznaczony jako wspierający SNMP.
Ruch sieciowy		• SNMP właściwie skonfigurowane na zdalnym urządzeniu. • Dostępność określonych OID-ów i tabel SNMP na urządzeniu.

Poza powyższymi wymaganiami, zapora na zdalnym komputerze musi być właściwie skonfigurowana. Poniższa tabela przedstawia porty, które muszą być otwarte:

Protokół lub monitor	Porty, które muszą być otwarte
SNMP	UDP 161,162

Uruchomienie WMI na wszystkich komputerach Windows

Uruchamianie WMI jest szczegółowo opisane w rozdziale Monitorowanie Windows przez WMI. Aby WMI było w stanie poprawnie działać, należy poprawnie skonfiguwać dane logowania(są to dane logowania do systemu Windows na danej stacji).

Zainstalowanie Agentów nVision

Różne sposoby instalowania Agentów są szczegółowo opisane w rozdziale Instalowanie i odinstalowywanie Agentów.

Otwarcie określonych portów na komputerach zdalnych i na tym, gdzie uruchomione jest nVision

Dodaj folder, w którym zainstalowany jest Agent nVision (domyślnie **C:\Program Files\Axence*** lub **C:\Program Files (x86)\Axence***) do wyjątków w programie antywirusowym.

Agenty i nVision otwierają wymagane porty w zaporze Windows automatycznie. Jeśli jednak masz jeszcze jakąś inną zaporę, musisz otworzyć je ręcznie.

Lista portów znajduje się w temacie Porty.

Powiązane tematy

- Wymagania
- Zdalny dostęp
- Instalowanie i odinstalowywanie Agentów
- Ustawienia Agenta

2.5.2 Monitorowanie i zarządzanie Windows przez WMI

Udostępnianie monitorowania liczników Windows

Protokół WMI (używany przez WinTools, zbieranie informacji o zasobach i monitorowanie liczników wydajności Windows) jest dostępny na Windows 2003 Server. Jednak aby uzyskać informację z komputerów Windows XP Professional, Vista i Windows 7 należy wykonać kilka czynności. Aby je przyśpieszyć przygotowaliśmy program (WMIEnable.exe dostępny w katalogu instalacyjnym serwera nVision), który automatycznie wykona niezbędne operacje. Aby udostępnić WMI, należy uruchomić ten program na zdalnym komputerze. Można uruchomić go ze skryptu logowania, co zapewni dostępność WMI na wszystkich Windows XP, Vista i Windows 7. **Jeśli używasz zapory (firewall) innego producenta na zdalnym komputerze, musisz samodzielnie odblokować następujące porty: TCP 135, 139, 445, 593.**

Aby używać WinTools lub odczytać zasoby z Windows należy pamiętać, że system zdalny musi mieć dokładnie te same dane logowania (nazwę użytkownika i hasło) co użytkownik zalogowany na komputerze gdzie działa netTools i nVision. Wynika to z ograniczeń systemu w wersji Home.

WMIEnable

Program ten udostępnia WMI na Windows XP Professional i Vista. Poniżej znajduje się lista operacji wykonywanych przez program:

1. DCOM jest włączany przez ustawienie klucza rejestru

   ```
   [HKEY_LOCAL_MACHINE\Software\Microsoft\OLE\EnableDCOM]
   ```

   na wartość **"Y".**

2. Zdalny UAC na Windows Vista jest włączany przez ustawienie klucza rejestru

   ```
   [HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system
   \LocalAccountTokenFilterPolicy]
   ```

   na wartość **1.**

3. Porty WMI **(TCP 135,139,445,593)** są otwierane na zaporze Windows przez wykonanie komendy:

   ```
   netsh firewall set service RemotеAdmin
   ```

4. Dostęp do WMI na Windows Vista jest udostępniany przez dodanie wyjątku zapory dla **"Windows Management Instrumentation (WMI)".**

5. Model autoryzacji jest ustawiany na "Local user authorize as themselves" przez ustawienie wartości klucza rejestru

   ```
   [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\forceguest]
   ```

   na wartość **0.**

Zwykle restart systemu nie jest konieczny a WMI będzie dostępne zaraz po wykonaniu programu, można jednak wymusić restart systemu przez uruchomienie programu z parametrem **/restart**. Program nie dokona restartu jeśli ustawienie parametrów systemu się nie powiodło.

Jeśli WMI dalej nie działa

Jeśli WMI nie działa pomimo uruchomienia programu WMIEnable, należy sprawdzić:

1. Uruchom **Local Security Settings** (**secpol.msc /s**) wybierz **Local Policies -> User Rights Assignment -> Access this computer from network**. Sprawdź czy wszystkie właściwe grupy/ użytkownicy są dodani. Przynajmniej grupa Administrators lub Administrator powinni być dodani.
2. Uruchom **Group Policy** (**gpedit.msc**) i wybierz **Windows Settings -> Security Settings -> Local Policies -> Security Options -> Network access: Sharing and security model for local accounts**. Ustaw tą opcję na **"Classic - local user authorize as themselves".**
3. Sprawdź czy WMI działa przez wywołanie komendy "**wbemtest**". WMI działa jeśli program ten działa poprawnie.
4. Sprawdź, czy następujące serwisy są uruchomione:
   COM+ Event System
   Remote Access Auto Connection Manager
   Remote Access Connection Manager
   Remote Procedure Call (RPC)
   Remote Procedure Call (RPC) Locator
   Remote Registry
   Server
   Windows Management Instrumentation
   Windows Management Instrumentation Driver Extensions
   WMI Performance Adapter
   Workstation

Wycieki pamięci przez starą wersję Rpcrt4.dll

W razie monitorowania liczników wydajności Windows, należy upewnić się, że zainstalowana jest najnowsza wersja pliku Rpcrt4.dll. Wszystkie poprzednie wersje powodują poważne wycieki pamięci w

systemie, co może doprowadzić do awarii systemu. Problem ten jest opisany przez Microsoft na stronie http://support.microsoft.com/?kbid=911262.

Plik Rpcrt4.dll powinien być w poniższej wersji (lub wyższej):

System	Wersja	Rozmiar pliku
Windows 2003	5.2.3790.2900	643,072
Windows XP	5.1.2600.2810	582,144

Problem wywołań RPC i wysokich portów

Domyślnie wywołanie RPC używa portów z zakresu portów do jednorazowego użytku (1024-5000) podczas przypisywania portów do aplikacji RPC w celu nasłuchiwania w punkcie końcowym TCP. Takie zachowanie może ograniczyć dostęp do tych portów, co może powodować utrudnienia w pracy z Agentami nVision. Informacje o tym, jak skonfigurować wywołanie RCP w taki sposób, aby używało pewnych portów i jak ułatwić zabezpieczanie tych portów można znaleźć na stronie http://support.microsoft.com/kb/908472.

Podłączenie do innych systemów operacyjnych

Nie ma możliwości podłączenia do komputera pracującego pod kontrolą jednej z poniższych edycji systemu Windows: Starter, Basic lub Home.

Więcej informacji:
http://msdn.microsoft.com/en-us/library/windows/desktop/aa389284%28v=vs.85%29.aspx#failure_to_connect

2.5.3 Monitorowanie i blokady

2.5.3.1 Ustawienia monitorowania

W odróżnieniu do nVision 9 (w której ustawienia były zachowane w postaci zestawu reguł, czyli w profilach Agentów) najnowsza wersja Axence nVision 10, ustawienia monitorowania użytkowników i blokowania stron oraz aplikacji, konfiguruje na grupach użytkowników.

To w ich właściwościach administrator powinien skonfigurować opcje monitorowania, ponieważ konta użytkowników dziedziczą z nich ustawienia. Oczywiście konto każdego z użytkowników może przynależeć do więcej niż jednej grupy – wtedy efektywne ustawienia monitorowania będą stosowane zgodnie z zasadami opisanymi poniżej.

Podstawowymi nośnikami ustawień monitorowania w najnowszej wersji programu są: Atlas, Grupy użytkowników, konto użytkownika.

Atlas – ustawienia domyślne

Atlas jest podstawowym obiektem w nVision 10, który zawiera podstawowe, globalne ustawienia monitorowania. Oznacza to, że konto każdego użytkownika, który nie należy do żadnej z grup, przyjmie ustawienia monitorowania, które przypisane są do Atlasu.

Możliwe konfiguracje:

- Monitorowanie

Ustawienie	Możliwe wartości	Wartość domyślna
Użycie łącza	**monitoruj**/nie monitoruj	monitoruj
Odwiedzone strony WWW	**monitoruj**/nie monitoruj	monitoruj
Użycie aplikacji	**monitoruj**/nie monitoruj	monitoruj
Czas pracy	**monitoruj**/nie monitoruj	monitoruj
Wydruki	**monitoruj**/nie monitoruj	monitoruj
E-maile	monitoruj/**nie monitoruj**	nie monitoruj
Przesyłaj aktywność w czasie	monitoruj/**nie monitoruj**	nie monitoruj
Przerwy w aktywności	**monitoruj**/nie monitoruj	monitoruj
Zapisuj przerwy powyżej ”X” minut	liczba minut	5 minut
Czas monitorowania	Kiedykolwiek | pomiędzy | z wyjątkiem (godziny, dni tygodnia)	kiedykolwiek

- Zdalny dostęp

Ustawienie	Możliwe wartości	Wartość domyślna
Zezwól na podgląd pulpitu	**zezwól**/nie zezwalaj	zezwól
Zezwól na zdalny dostęp	**zezwól**/nie zezwalaj	zezwól
Pokaż powiadomienie	**nie powiadamiaj**/ powiadamiaj	nie powiadamiaj
Pytaj o zgodę użytkownika	nie pytaj/**zapytaj**	zapytaj
Zezwól, jeżeli użytkownik nie odpowiada	**zezwól**/nie zezwalaj	zezwól

- Wyświetlanie Agenta

Ustawienie	Możliwe wartości	Wartość domyślna
Pokaż ikonę Agenta	**pokaż**/nie pokazuj	pokaż
Po zalogowaniu pokaż informację o Agencie	**pokaż**/nie pokazuj	pokaż
Pokaż informację o monitorowaniu aktywności użytkownika	**pokaż**/nie pokazuj	pokaż

Domyślnie Atlas zawiera taki zestaw ustawień monitorowania, aby każdy nowy użytkownik objęty był maksymalnie restrykcyjnym monitorowaniem.

Grupy użytkowników

Grupy użytkowników mogą zawierać dowolną liczbę kont użytkowników oraz podgrup. Jeżeli grupa użytkowników nie jest podgrupą, wtedy jej obiektem nadrzędnym, z którego dziedziczy ustawienia, jest Atlas.

W konfiguracji ustawień grupy (lub podgrupy) można definiować jedynie ustawienia, które są wyjątkami mniej restrykcyjnymi od ustawień nadrzędnych (Atlasu lub grupy, która zawiera daną podgrupę). Np. na poziomie Atlasu włączono monitorowanie

wydruków – zatem na poziomie grupy możliwe jest jedynie wyłączenie monitorowania wydruków.
Takie podejście pozwala na wyłączenie pewnej grupy użytkowników z monitorowania.

Możliwe konfiguracje wyjątków na poziomie grupy:

- Monitorowanie

Ustawienie	Możliwe wartości
Użycie łącza	nie monitoruj
Odwiedzone strony WWW	nie monitoruj
Użycie aplikacji	nie monitoruj
Czas pracy	nie monitoruj
Wydruki	nie monitoruj
E-maile	nie monitoruj
Przesyłaj aktywność w czasie	nie monitoruj
Przerwy w aktywności	nie monitoruj
Czas monitorowania	Czas monitorowania można ustawić tylko w Atlasie lub indywidualnie dla każdego użytkownika.

- Zdalny dostęp

Ustawienie	Możliwe wartości
Zezwól na podgląd pulpitu	nie pozwalaj
Zezwól na zdalny dostęp	nie pozwalaj
Pokaż powiadomienie	powiadom
Pytaj o zgodę użytkownika	zapytaj
Zezwól, jeżeli użytkownik nie odpowiada	nie pozwalaj

- Wyświetlanie Agenta

Ustawienie	Możliwe wartości
Pokazuj ikonę Agenta	nie pokazuj
Po zalogowaniu pokaż informację o Agencie	nie pokazuj
Pokaż informację o monitorowaniu aktywności użytkownika	nie pokazuj

Domyślnie, żadna grupa nie zawiera żadnych wyjątków od ustawień nadrzędnych (Atlasu).

Wyjątki zdefiniowane dla grupy propagowane są również na jej wszystkie podgrupy. Nie można w żaden sposób "wyłączyć" grupy z propagowania ustawień lub wyjątków z bytów nadrzędnych.

Wyjątki zdefiniowane dla grupy wpływają na ustawienia wszystkich użytkowników, którzy do niej należą (z wyjątkiem tych, którzy mają zdefiniowane indywidualne ustawienia). Jeżeli użytkownik znajduje się w więcej niż jednej grupie, to aplikują się do niego wszystkie wyjątki ze wszystkich tych grup.

Użytkownik

Konto użytkownika może podlegać ustawieniom monitorowania, które są wynikiem ustawień Atlasu i grup lub może korzystać z indywidualnych ustawień monitorowania.
Ustawienia monitorowania i blokad użytkownia można skonfigurować w oknie **Informacje o użytkowniku**, które wyświetli się po dwukrotnym kliknięciu nazwy konta użytkownika.

Ustawienia indywidualne umożliwiają konfigurację indywidualnych ustawień monitorowania, które będą miały zastosowanie tylko i wyłącznie dla konta użytkownika, dla które zostały ustawione, niezależnie od ustawień globalnych i wyjątków grup.

Ustawienia wynikowe to ustawienia globalne Atlasu po uwzględnieniu wyjątków ze wszystkich grup, do których należy dane konto użytkownika. Jeśli konto użytkownika przynależy do kilku grup, dla których skonfigurowano różne ustawienia tego samego parametru monitorowania, to wynikowo zastosowane będzie ustawienie mniej restrykcyjne (np. nie monitoruj użycia aplikacji).

Dla każdego z ustawień, administrator może wybrać zastosowanie ustawienia wynikowego lub indywidualnego (np. wynikowym będzie ustawienie czasu pracy a indywidualnie przydzielonym ustawienie użycia aplikacji).

Wprowadzenie nowego modelu ustawień monitorowania pozwala na zastosowanie intuicyjnego sposobu sumowania ustawień, który wynika z faktu przynależenia konta danego użytkownika do wielu grup (konto będzie objęte wszystkimi wyjątkami, wszystkich grup, do których należy).

Zupełnie nowe podejście do zarządzania ustawieniami monitorowania określa, że ustawienia grupy nie mogą być użyte do zwiększenia uprawnień a jedynie do ich ograniczenia. Pozwala to na zastosowanie dobrej praktyki korzystania z Axence nVision 10 – budowania przejrzystych reguł monitorowania sieci.
Przykład: globalne włączenie monitorowania czasu pracy i użycia aplikacji a następnie wyłączanie tego ustawienia w drodze wyjątków na poziomie grup użytkowników.

2.5.3.2 Ustawienia blokowania

Podstawowymi nośnikami ustawień blokowania w najnowszej wersji programu są: Atlas, Grupy użytkowników, konto użytkownika.
W przeciwieństwie do ustawień monitorowania (które mają z góry zdefiniowaną listę możliwych ustawień), ustawienia blokowania opierają się na definiowaniu dowolnie dużej liczby reguł blokowania.
Atlas nie zawiera żadnych domyślnych ustawień blokowania o ile nie zostały one utworzone w wyniku procesu migracji danych z nVision 9.

Blokowanie stron

W nVision 10 usunięta została domyślna akcja blokowania stron: "Zablokuj wszystkie strony oprócz poniższych". W sytuacji, gdy administrator nie skonfigurował żadnych reguł blokad stron, dostęp do wszystkich stron internetowych nadal jest możliwy (program zachowuje się tak, jakby akcja domyślna była zawsze ustawiona na "zezwól na wszystkie strony oprócz poniższych"). W praktyce oznacza to, że każda strona, która nie pasuje do żadnej ze zdefiniowanych reguł, nie jest blokowana.

W programie można zdefiniować dowolnie dużą liczbę reguł blokowania stron.

Każda reguła zawiera swoją nazwę, rodzaj akcji, domenę (lub adres IP) i efektywny czas obowiązywania.

- Akcja reguły to jedna z dwóch opcji: "zezwól" lub "blokuj".
- Domena (lub adres IP) to wzorzec, do którego dopasowywane będą odwiedzane strony. We wzorcu można używać znaku ***** , który oznacza dopasowanie dowolnego ciągu znaków.
- Efektywny czas obowiązywania to wzorzec czasowy w który można wyszczególnić dni tygodnia lub godziny w obrębie dnia.
  Jeżeli czas obowiązywania został zdefiniowany, to poza tym czasem reguła jest ignorowana.

Jeżeli odwiedzona strona pasuje do więcej niż jednej reguły, to:

- Jeżeli wszystkie z tych reguł mają akcję "blokuj", to strona jest blokowana.
- Jeżeli co najmniej jedna z tych reguł ma akcję "zezwól", to strona nie jest blokowana.

Jeżeli odwiedzona strona nie pasuje do żadnej reguły, to również nie jest blokowana.

Blokowanie aplikacji

Analogicznie jak dla blokowania stron, w programie zdefiniować można dowolnie dużą liczbę reguł blokowania aplikacji.

Każda reguła zawiera swoją nazwę, nazwę blokowanego pliku wykonywalnego i efektywny czas obowiązywania.

- Dla reguł blokowania aplikacji nie można zdefiniować akcji "zezwól" (każda z tych reguł jest zawsze z akcją "blokuj").
- We wzorcu nazwy blokowanego pliku wykonywalnego również można używać znaku ***** .

Jeżeli uruchomiona aplikacja nie pasuje do żadnej reguły, to nie jest blokowana.

Blokowanie rozszerzeń pobieranych plików

Analogicznie jak dla blokowania stron, w programie zdefiniować można dowolnie dużą liczbę reguł blokowania rozszerzeń pobieranych plików.

Każda reguła zawiera swoją nazwę i zablokowane rozszerzenie pliku.

- Dla reguł blokowania rozszerzeń pobieranych plików nie można zdefiniować akcji "zezwól" (każda z tych reguł jest zawsze z akcją "blokuj").
- We wzorcu zablokowanego rozszerzenia pliku nie można używać znaku "*".
- Reguły blokowania rozszerzeń pobieranych plików nie mają efektywnego czasu obowiązywania (obowiązują cały czas).

Jeżeli rozszerzenie ściągniętego pliku nie pasuje do żadnej reguły, to nie jest blokowane.

Dziedziczenie ustawień blokowania

Atlas

Atlas jest podstawowym obiektem w nVision 10, który zawiera podstawowe, globalne ustawienia blokowania. Oznacza to, że konto każdego użytkownika, który nie należy do żadnej z grup, przyjmie ustawienia monitorowania, które przypisane są do Atlasu.
Atlas nie dziedziczy ustawień z żadnego innego bytu.

Atlas nie zawiera żadnych domyślnych ustawień blokowania o ile nie zostały one utworzone w wyniku procesu migracji danych z nVision 9.

Grupy użytkowników
Każda grupa użytkowników zawiera wszystkie reguły blokowania Atlasu oraz grup nadrzędnych, do których należy.
Na poziomie grupy nie można w żaden sposób modyfikować reguł odziedziczonych z Atlasu ani z grup nadrzędnych. Nie można ich również usuwać ani wyłączać z dziedziczenia.
Na poziomie grupy można zdefiniować dowolnie dużą liczbę reguł indywidualnych, które zostaną dołączone do zbioru tych odziedziczonych.
Reguły indywidualne zdefiniowane w grupie są dziedziczone przez wszystkie grupy podrzędne, które do niej należą.

Użytkownik
Konto użytkownika korzysta z reguł odziedziczonych z grup (i Atlasu) oraz z reguł indywidualnych.
Dla pojedynczego użytkownika można wyłączyć dziedziczenie reguł blokowania z Atlasu i grup.

Jeżeli użytkownik ma **włączone** dziedziczenie reguł, to obowiązuje go sumaryczna kolekcja:

- reguł odziedziczonych z atlasu (jeżeli nie jest w żadnej grupie),
- reguł odziedziczonych ze wszystkich grup, w których się znajduje,
- reguł indywidualnych zdefiniowanych na poziomie tego użytkownika.

Jeśli konto użytkownika przynależy do kilku grup, dla których skonfigurowano różne reguły blokowania, to wynikowo zastosowane będą reguły blokowania.

Jeżeli użytkownik ma **wyłączone** dziedziczenie reguł, to obowiązują go wyłącznie jego reguły indywidualne.

Podsumowanie

- Jeżeli zablokowano jakąś stronę globalnie, to można określić grupę użytkowników, którzy będą mieć do niej dostęp.
- Jeżeli nie zablokowano jakiejś strony globalnie, to można określić grupę użytkowników, dla których będzie zablokowana.
- Jeżeli użytkownik znajduje się w grupie, która posiada regułę "zezwól" dla jakiejś strony, to nie można jej nadpisać regułą "blokuj" dołączając go do innej grupy.
- Funkcję „białej listy” ("zablokuj wszystkie strony oprócz poniższych") można nadal zrealizować za pomocą reguły "blokuj" dla domeny "*".
- Jeżeli zablokowano globalnie jakąś aplikację lub rozszerzenie pobieranego pliku, to nie można ich odblokować na poziomie grupy.
- Jeżeli nie zablokowano globalnie jakiejś aplikacji lub rozszerzenia pobranego pliku, to można określić grupę użytkowników, dla których te byty będą zablokowane.
- Na poziomie ustawień użytkownika można zawsze można zdefiniować indywidualny zestaw reguł, niezależnie od sposobu działania mechanizmu dziedziczenia.

2.5.4 Migracja ustawień

2.5.4.1 Konta użytkowników

W wyniku migracji danych z nVision 9, do kont użytkowników synchronizowanych z Active Directory zostanie przepisana aktywność z ikon urządzeń ze starszej wersji programu.

Dla każdego konta lokalnego Windows z Agenta nVision 9, na którym ktoś przynajmniej raz się zalogował, utworzone zostanie konto użytkownika w nVision 10.

2.5.4.2 Ustawienia monitorowania

Ustawienia monitorowania dostępne w nVision 9 w profilach Agentów, w nowej wersji nVision 10 przeniesione zostały na użytkowników i grupy.

Ustawienia domyślne

Ustawienia domyślne to ustawienia zmigrowane z nVision 9 i przypisane do Atlasu.
Wyznaczenie domyślnych ustawień monitorowania w nVision 10, sprowadza się do zsumowania wszystkich ustawień zawartych w profilu Agentów z nVision 9, z których korzystało przynajmniej 1 konto użytkownika, przy czym:

- jeżeli wybrana opcja była monitorowana w przynajmniej jednym profilu Agenta w nVision 9, w wyniku migracji danych do nVision 10, jest ona monitorowana w domyślnych ustawieniach,
- jeżeli aktywność w czasie była przesyłana w przynajmniej jednym profilu, to w wyniku migracji jest ona przesyłana w domyślnych ustawieniach,
- jeżeli przerwy w aktywności były wykrywane przynajmniej w jednym profilu, to w wyniku migracji są również wykrywane,
- zmigrowany czas przerwy w domyślnych ustawieniach to minimalny czas wybrany ze wszystkich dotychczasowych profili Agentów,
- zakres czasowy monitorowania w domyślnych ustawieniach to suma wszystkich zakresów występujących w dotychczasowych profilach Agentów:
  - jeżeli zakresy czasowe nie zachodzą na siebie, przy migracji danych wyznaczany jest nowy zakres, za początek którego przyjmowana jest najwcześniejsza a za koniec: najpóźniejsza godzina ze wszystkich dotychczasowych profili (np. zakresy 8:00 – 12:00 oraz 15:00 – 18:00 zostaną zmigrowane na zakres 8:00 – 18:00)
  - przypadek szczególny: jeśli przynajmniej jeden z profili miał ustawiony ciągły czas monitorowania, w wyniku migracji ustawieniem domyślnym będzie również monitorowanie ciągłe,
- jeżeli którykolwiek profil w nVision 9 zezwalał na podgląd pulpitu, dostęp zdalny lub pomijanie zgody użytkownika na zdalny dostęp, w zmigrowanych ustawieniach domyślnych również będą one dozwolone,
- jeżeli którykolwiek profil w nVision 9 zezwalał na wyświetlanie ikony Agenta, w domyślnych ustawieniach również będzie to dozwolone.

Ustawienia grup

W procesie migracji tworzone są grupy użytkowników, które są nośnikiem ustawień monitorowania wynikających z dotychczasowych profili Agentów. Każda grupa zawiera takie ustawienia monitorowania, aby użytkownik, który w niej się znajduje, objęty był takimi ustawieniami monitorowania jak w profilu Agenta w nVision 9.

Podczas migracji danych, tworzona jest nadrzędna grupa „Monitorowanie”, która zawiera 3 podgrupy wbudowane:

- Grupy z profili,
- Grupy z map,
- Grupy z urządzeń.

Zarówno grupa nadrzędna jak i podgrupy wbudowane nie zawierają żadnych ustawień wbudowanych.

W podgrupach wbudowanych zostaną utworzone grupy użytkowników, które przyjmą nazwy:

- profili monitorowania wykorzystywanych w nVision 9,
- map jeśli w nVision 9 korzystały one z indywidualnych ustawień,
- urządzeń, jeśli korzystały one z indywidualnych ustawień (czyli nie korzystały ani z profilu Agenta, ani z ustawień mapy).

Następnie do grup dopisane zostaną konta użytkowników, którzy pracowali na urządzeniach w określonych profilach w nVision 9.

Informacje dodatkowe:

- Nie jest migrowany zakres czasowy monitoringu na poziomie profilu (grupy). W wersji 10 programu nie można ustalać tych zakresów na poziomie grupy. Wszystkie zakresy czasowe ze wszystkich profili są zsumowane wyłącznie do jednego, globalnego zakresu w ustawieniach.
- Żaden z użytkowników nie otrzymuje w procesie migracji ustawień indywidualnych.
- W wyniku migracji, mogą zostać zwiększone efektywne uprawnienia użytkownika pracującego na więcej niż jednym komputerze. Przykładowo, jeżeli w nVision 9 użytkownik pracował na komputerze, na którym monitorowanie było **włączone** i na drugim, gdzie monitorowanie było **wyłączone**, użytkownik po migracji **nie będzie** monitorowany na obu komputerach (ponieważ wyjątek "nie monitoruj" będzie go obowiązywał na obu komputerach).
- Ustawienia monitorowania i blokowania w nVision były związane z ikoną urządzenia i mapą, na której się ono znajdowało. Stąd możliwe było definiowanie różnych polityk bezpieczeństwa dla nowych użytkowników (zależnie od lokalizacji komputera). W nVision 10 jest jeden zestaw domyślnych uprawnień dla każdego nowego użytkownika, zatem administrator musi ręcznie utworzyć grupy z uprawnieniami i każdorazowo przydzielać do nich nowych użytkowników.

2.5.4.3 Ustawienia blokowania

Blokowanie stron

Ustawienia domyślne

Ustawienia domyślne to ustawienia zmigrowane z nVision 9 i przypisane do Atlasu.

Wyznaczenie domyślnych ustawień blokowania stron w nVision 10, sprowadza się do zsumowania wszystkich reguł typu „blokuj” zawartych w profilu Agentów z nVision 9. W ten sposób powstaje domyślny zestaw, który zawiera wszystkie reguły blokowania stron.

Ustawienia grup

W procesie migracji tworzone są grupy użytkowników, które są nośnikiem ustawień blokowania stron.

Podczas migracji danych, tworzona jest nadrzędna grupa „Filtrowanie”, która zawiera 3

podgrupy wbudowane:
- Grupy z profili,
- Grupy z map,
- Grupy z urządzeń.

Zarówno grupa nadrzędna jak i podgrupy wbudowane nie zawierają żadnych ustawień wbudowanych.

W podgrupach wbudowanych zostaną utworzone grupy użytkowników, które przyjmą nazwy:
- profili monitorowania wykorzystywanych w nVision 9,
- map jeśli w nVision 9 korzystały one z indywidualnych ustawień,
- urządzeń, jeśli korzystały one z indywidualnych ustawień (czyli nie korzystały ani z profilu Agenta, ani z ustawień mapy).

Następnie do grup dopisane zostaną konta użytkowników, którzy pracowali na urządzeniach w określonych profilach w nVision 9.

Sposób przeniesienia ustawień:
- Dla Atlasu, każdej z sieci oraz Agentów, które korzystały z indywidualnych reguł blokowania stron, tworzone są grupy ustawień blokowania, które umieszczane są grupie nadrzędnej „Filtrowanie”. Do grup przypisywani są użytkownicy (analogicznie do przeniesienia ustawień monitorowania).
- Każda grupa ustawień blokowania stron zawiera wszystkie reguły filtrowania, które dotychczas były przypisane do profilu. Reguły te są ustawiane jako indywidualne dla każdej z grup.
- Dla każdej reguły typu "blokuj" z ustawień domyślnych, która nie koliduje z żadną indywidualną regułą grupy, tworzona jest przeciwna reguła typu "zezwól" a następnie jest przypisywana jako reguła indywidualna grupy. W wyniku tego działania, odblokowywane są strony, które dotychczas nie były blokowane a w wyniku migracji ustawień mogły zostać zablokowane.
- Po przeniesieniu ustawień wykonywane jest usuwanie reguł nadmiarowych w ustawieniach domyślnych: usuwane są reguły „blokuj”, które zawierają się w innych regułach (np. reguła dla domeny „*.pl” zawiera regułę dla strony „domena.pl”).

Informacje dodatkowe:
- W ramach procesu migracji żaden z użytkowników nie otrzymuje indywidualnych reguł filtrowania stron.
- W wyniku migracji, użytkownik, który pracował na więcej niż jednym komputerze, może mieć mniej stron zablokowanych.
- Jeżeli ustawienia globalne blokują domenę "*" a indywidualne ustawienia grupy blokują tylko domenę "domena.pl", to na poziomie grupy nie zostanie utworzona reguła "zezwól" dla domeny "*.", ponieważ spowodowałoby to bezskuteczność reguły blokowania domeny "domena.pl". Z tego powodu, po migracji część grup może potencjalnie blokować więcej stron niż analogiczne dla nich profile w wersji 9 programu.

Blokowanie aplikacji

Ustawienia domyślne

Domyślne ustawienia blokowania aplikacji tworzone są poprzez zsumowanie wszystkich dotychczasowych reguł blokowania ze wszystkich profili (analogicznie do domyślnych reguł blokowania stron).

Ustawienia grup
Podczas migracji danych, tworzona jest nadrzędna grupa „Blokowanie”, która zawiera 3 podgrupy wbudowane:
- Grupy z profili,
- Grupy z map,
- Grupy z urządzeń.

Zarówno grupa nadrzędna jak i podgrupy wbudowane nie zawierają żadnych ustawień wbudowanych.

W podgrupach wbudowanych zostaną utworzone grupy użytkowników, które przyjmą nazwy:
- profili monitorowania wykorzystywanych w nVision 9,
- map jeśli w nVision 9 korzystały one z indywidualnych ustawień,
- urządzeń, jeśli korzystały one z indywidualnych ustawień (czyli nie korzystały ani z profilu Agenta, ani z ustawień mapy).

Następnie do grup dopisane zostaną konta użytkowników, którzy pracowali na urządzeniach w określonych profilach w nVision 9.

Ustawienia te jednak zawsze będą bezskuteczne, ponieważ ustawienia domyślne zawsze będą tak samo lub bardziej restrykcyjne. Celem tej migracji jest wyłącznie umożliwienie zapoznania się z tym, co te profile zawierały wcześniej.

Blokowanie rozszerzeń pobieranych plików

Ustawienia domyślne
Domyślne ustawienia blokowania rozszerzeń pobieranych plików tworzone są poprzez zsumowanie wszystkich dotychczasowych reguł ze wszystkich profili (analogicznie do domyślnych reguł blokowania stron).

Ustawienia grup
Podobnie jak przy procesie migrowania reguł blokowania aplikacji, ustawienia z profili są przenoszone do odpowiadających im podgrup, które zostały wcześniej utworzone w nadrzędnej grupie "Filtrowanie". Ustawienia te są również bezskuteczne i zostają zachowane tylko w celach informacyjnych.

Informacje dodatkowe:
- Ustawienia blokowania portów nie podlegają migracji, na użytkownika, ponieważ w nVision 10 powiązane są ustawieniami urządzenia.
- Ustawienia ze wszystkich profili blokowania aplikacji i blokowania rozszerzeń pobieranych plików są scalone do jednego bytu ustawień domyślnych i po migracji obowiązują wszystkich użytkowników. Jeżeli korzystałeś z różnych profili na wielu urządzeniach, wymagana będzie ręczna korekta konfiguracji programu po procesie migracji.

2.5.4.4 Powiadomienia o blokadach

W nVision 10, dla każdego z poniższych 4 typów powiadomień o blokowaniu, można skonfigurować **dokładnie jedną wersję**:
- powiadomienia o zablokowaniu strony,
- powiadomienia o zablokowaniu aplikacji,
- powiadomienia o zablokowaniu pliku,

- powiadomienia o blokadzie portów.

W związku z tym, podczas procesu migracji sprawdzona zostanie liczba unikalnych powiadomień o blokadach z wersji 9 a do nowej wersji systemu zostanie przepisane to powiadomienie, które występuje najliczniej (dla każdego z 4 typów powiadomień).

Aby skonfigurować powiadomienia o blokadach:

1. Na wstążce wybierz kartę **Narzędzia i opcje** a następnie **Opcje**.
2. Wybierz zakładkę **Komunikaty i blokady**.

2.5.4.5 Zrzuty ekranowe

Zrzuty ekranowe wykonane w wersji 9 programu na poziomie urządzenia, zostaną przeniesione do użytkownika, w kontekście którego zostały wykonane.
Ustawienie zbierania zrzutów ekranowych na poziomie urządzenia nie jest migrowane. Po procesie migracji należy ręcznie włączyć to ustawienie na poziomie każdego użytkownika, dla którego zrzuty mają być zapisywane.
Z założenia, mechanizm zrzutów ekranowych jest tymczasowy i włączany okresowo, stąd jego ustawienia nie są migrowane.

2.5.4.6 Ustawienia DataGuard

Prawa domyślne
W wyniku migracji ustawień z nVision 9 tworzony jest zbiór praw domyślnych poprzez zsumowanie praw przydzielonych dotychczas do Agentów oraz nadrzędnego bytu Active Directory (najwyższego poziomu „Zaufanych jednostek AD") w taki sposób, aby zawierał on maksymalnie restrykcyjny zbiór uprawnień. W wyniku sumowania bardziej restrykcyjnymi są:

- blokowanie nośnika,
- włączenie audytu operacji na plikach na nośniku.

Ustalenie maksymalnie restrykcyjnego zbioru uprawnień jako "Prawa domyślne" jest niezbędne, aby bezpośrednio po migracji zapewnić ciągłość ochrony danych przed wyciekiem dla każdego nowego użytkownika.

Przeniesienie ustawień DataGuard:

- Utworzona zostanie nadrzędna grupa „Reguły DataGuard", która nie zawiera zdefiniowanych żadnych własnych ustawień.
- Prawa DataGuard przypisane do Atlasu w nVision 9 porównywane są z domyślnymi prawami nVision 10. Następnie jako podgrupa nadrzędnej grupy „Reguły DataGuard" tworzona jest grupa „Grupa z Atlasu", do której przypisywane są wszystkie prawa różniące się od praw domyślnych. Do tej grupy przypisywane są prawa o wartościach takich, jakie poprzednio miał Atlas. Przypisane prawa są prawami indywidualnymi tej grupy.
- Dla każdej mapy tworzona jest grupa o nazwie „Grupa z mapy X", która jest podgrupą grupy Atlasu lub mapy nadrzędnej wynikającej z poprzedniej wersji programu. Do tej grupy, jako prawa indywidualne, przypisywane są wszystkie prawa różniące się od praw grupy mapy nadrzędnej lub Atlasu.
- Dla każdego Agenta, który korzystał z indywidualnych praw DataGuard tworzona jest „Grupa z urządzenia X", do której przypisywani są użytkownicy pracujący na tym Agencie w nVision 9.
- Konto każdego użytkownika niedomenowego umieszczana jest w grupach, które odpowiadają Agentom, na których pracował. Jeżeli użytkownik pracował na więcej niż jednym komputerze, zostanie przypisany do wszystkich grup, które odpowiadają Agentom, na których pracował.

Rezultatem migracji jest odwzorowanie uprawnień wynikających ze struktury Atlasu, map i Agentów z nVision 9 za pomocą maksymalnie uproszczonego schematu grup użytkowników. W ostatecznej strukturze nVision 10 znajdują się tylko grupy, które w jakiś sposób zmieniają uprawnienia. Prawa DataGuard użytkowników domenowych nie ulegają zmianie.

Informacje dodatkowe:

- Po migracji do nVision 10 na każdego nowego użytkownika mogą zostać nałożone większe ograniczenia, nawet jeżeli zostanie utworzony na Agencie, który poprzednio nie miał żadnych blokad w module DataGuard.
- Ponieważ usunięty zostaje nadrzędny byt "Active Directory", który agregował uprawnienia dla wszystkich użytkowników z AD, utracone zostaną ustawienia które zostały w nim zdefiniowane. Pozostałe uprawnienia grup i użytkowników z Active Directory nie są w żaden sposób modyfikowane w trakcie procesu migracji.
- W wyniku migracji może się okazać, że na użytkowników z Active Directory zostaną nałożone większe ograniczenia. Przypadek ten może wystąpić, gdy w nVision 9 nośnik danych był zablokowany na poziomie Atlasu, użytkownik z Active Directory miał do niego dostęp, ponieważ w nadrzędnym bycie "Active Directory" zdefiniowana była dodatkowa reguła dająca dostęp do tego nośnika.
- Program w wersji 10 traci bezpowrotnie możliwość definiowania reguł DataGuard na poziomie hosta. Tym samym nie jest już możliwe blokowanie i audytowanie użytkowników wyłącznie na wskazanych urządzeniach. Każdy użytkownik ma zawsze ten sam zestaw reguł niezależnie od komputera, na którym aktualnie jest zalogowany.

2.5.4.7 Alarmy i raporty

Alarmy

Alarmy nie są w żaden przetwarzane w procesie migracji. W nVision 10, podobnie jak w nVision 9, możliwe jest konfigurowanie alarmów na poziomie ikony urządzenia. Alarmy utworzone w nVision 9 zostaną przeniesione w takiej samej formie na obiekty urządzeń w nowej wersji programu.

Raporty

W wyniku migracji danych do nVision 10 utracone zostaną raporty dotyczące informacji o aktywności użytkowników z określonych map lub na wskazanych urządzeniach. Szablony tych raportów nadal będą widoczne w systemie ale wygenerowany przy ich pomocy raport będzie pusty – wynika to z faktu przeniesienia segmentów dotyczących aktywności użytkowników do sekcji raportów generowanych dla grup.

W związku z tym, przed rozpoczęciem procesu migracji należy wykonać potrzebne raporty dla map i urządzeń wg dotychczasowych szablonów, natomiast po migracji należy odtworzyć ręcznie szablony raportów w kontekście grup.

2.5.4.8 Uprawnienia administratorów

W nVision 10 dane użytkownika zostały przeniesione z bytu w postaci ikony urządzenia na mapach na nowy byt użytkownika w grupach. Ze względu na różnice w działaniu map oraz grup użytkowników, nie jest możliwa migracja ustawień uprawnień administratorów.
W związku z powyższym, jeśli w nVision 9 administrator nie miał uprawnień do wszystkich map, po migracji danych do nVision 10, nie będzie miał uprawnień do żadnej z grup użytkowników.
Niesie to za sobą konieczność ręcznej edycji uprawnień tych administratorów.

2.5.4.9 Powrót do nVision 9

Uruchomienie instalatora Axence nVision 10 automatycznie wykona kopię zapasową bazy danych nVision 9. Kopia zapasowa zawiera zarówno ustawienia programu oraz dane zebrane w monitorowaniu.

Aby przywrócić dane z nVision 9:

- Jeśli instalacja nVision 10 nie powiedzie się (lub nie powiedzie się proces migracji), a Serwer nie uruchomi się w nowej wersji, to Agenty nie zaktualizują się. W takim przypadku należy:
  - zatrzymać usługę „Axence nVision”,
  - usunąć plik **nVision.exe** ze ścieżki instalacji programu na serwerze,
  - pobrać instalator nVision 9 (https://cdn.axence.net/nVision9.zip),
  - zainstalować program,
  - przywrócić kopię zapasową bazy danych poprzez uruchomienie skrótu **DBRestore** (domyślnie: C:\Program Files (x86)\Axence\nVision\Backups).

- Jeśli aktualizacja do nVision 10 powiedzie się a program uruchomi się, Agenty, które podłączyły się do serwera zostaną automatycznie zaktualizowane do najnowszej wersji.
  W tej sytuacji, aby dokonać pełnego downgrade’u do nVision 9 należy:
  - odinstalować Agenty (np. za pomocą polecenia z menu kontekstowego w Konsoli nVision 10),
  - wyłączyć konsolę nVision,
  - zatrzymać usługę „Axence nVision”,
  - usunąć plik **nVision.exe** ze ścieżki instalacji programu na serwerze,
  - pobrać instalator nVision 9 (https://cdn.axence.net/nVision9.zip),
  - zainstalować program,
  - przywrócić kopię zapasową bazy danych poprzez uruchomienie skrótu **DBRestore** (domyślnie: C:\Program Files (x86)\Axence\nVision\Backups),
  - ponownie zainstalować Agenty z instalatora skopiowanego z folderu wskazanego po kliknięciu w Konsoli nVision: [menu] **Agenty \ Zainstaluj Agenty nVision**.

2.5.5 Główne ustawienia programu

Aby zmienić opcje programu:

1. Na wstążce wybierz kartę **Narzędzia i opcje** a następnie **Opcje**.
2. Wybierz odpowiednią zakładkę.
3. Edytuj opcje zgodnie z poniższymi instrukcjami.

Zakładka	Opcje	Opis
Ogólne	**Dodatkowe informacje w drzewie**	Dodatkowe ikony, które wyświetlane są w drzewie map, obok nazwy mapy. Możliwe ustawienia: • stan urządzeń, • alarmy, • oba lub żadne z powyższych.

Zakładka	Opcje	Opis
	Ikona programu w zasobniku [systemowym]	• zawsze, • w przypadku nierozwiązanych alarmów, • tylko jeśli zminimalizowany.
	Automatyczne aktualizacje	Możliwość włączenia automatycznych aktualizacji oraz skonfigurowania częstotliwości sprawdzania dostępności nowych wersji programu.
Monitorowanie	**Serwisy**	Lista usług TCP, które Axence nVision® spróbuje wykryć na każdym urządzeniu. Jeśli chcesz aby jakiś serwis był wykrywany automatycznie przez program, dodaj go do tej listy.
	Wykryj serwisy na każdym interfejsie	Włącz, aby wyskanować serwisy na każdym adresie/ interfejsie. Jeśli opcja jest wyłączona, serwisy zostaną wykryte tylko na podstawowym adresie.
	Rozwiązuj adresy co X minut	Interwał czasowy, zgodnie z którym nVision rozwiązuje adresy IP =>DNS.
	Maksymalna ilość jednoczesnych połączeń przychodzących z Agentów	Parametr określa ile Agentów może jednocześnie przesłać informacje np. o aktywności użytkowników. Uwaga: użyj mniejszych wartości jeżeli obserwujesz zbyt duże obciążenie sieci.
Akcje	Niektóre akcje wymagają konfiguracji, aby działały poprawnie (np. wysłanie wiadomości ICQ wymaga podania danych konta ICQ potrzebnych do zalogowania na serwer). Aby uzyskać więcej informacji przejdź do rozdziału Konfigurowanie akcji.	
Zdalny dostęp	Zdalny dostęp WWW może zostać włączony w tej zakładce. Jeżeli chcesz dowiedzieć się więcej na temat zdalnego dostępu, przejdź do Jak uzyskać dostęp do nVision przez przeglądarkę WWW? oraz Jak utworzyć konta użytkowników Web Access?. W zakładce możesz także zmienić ustawienia serwera API na potrzeby dostępu aplikacji mobilnych. Aby dowiedzieć się więcej, przejdź do rozdziału Aplikacja mobilna.	
	Zdalny dostęp	Zdefiniuj numer portu dla dostępu przez przeglądarkę internetową.
	HelpDesk	Zdefiniuj numer portu, na którym działać będzie HelpDesk. Aby włączyć szyfrowanie komunikacji w helpdesku, należy zainstalować certyfikat dla domeny.
	Serwer API	Zdefiniuj numer portu dla aplikacji Mobilne Środki

Zakładka	Opcje	Opis
		Trwałe dla systemu Android.
Konserwacja	**Wyczyść stare dane z bazy danych**	Ustaw czas, po którym stare dane (określonego typu) będą usuwane z bazy danych programu.
	Kopie bezpieczeństwa	Możesz zarządzać profilami automatycznego tworzenia kopii zapasowych. Aby dowiedzieć się więcej, przejdź do rozdziału Automatyczny backup. Kopia zapasowa poza konfiguracją programu, zawiera również dane zebrane w monitorowaniu sieci, dane o inwentaryzacji oraz dane modułu HelpDesk.
	Restart nVision, jeśli nie odpowiada przez X minut	Axence nVision® jest bardzo stabilnym programem, jednak rozumiemy, że może być używany do monitorowania krytycznych zasobów. Dlatego posiada zabezpieczenie, które automatycznie dokona restartu w razie jakichkolwiek problemów, aby zapewnić nieprzerwane monitorowanie sieci. Zaznacz tę opcję i ustaw czas w minutach jeśli chcesz, aby Axence nVision® było restartowane gdy nie odpowiada.
Komunikaty blokady	W tej zakładce można skonfigurować własne komunikaty, które zostaną wyświetlone w przypadku próby: • wejścia na zablokowaną stronę WWW, • uruchomienia zablokowanej aplikacji, • operacji na zewnętrznym nośniku w ramach DataGuard, • pobrania przez przeglądarkę pliku z zablokowanym rozszerzeniem.	
Aktywność użytkowników	**Aplikacje**	Definicje grup aplikacji. Możesz tworzyć, edytować i usuwać grupy. Nazwa pliku wykonywalnego aplikacji porównywana jest z nazwą uruchamianego przez użytkownika procesu. Wykorzystywane są w module monitorowania aktywności użytkowników (Users).
	Sieci lokalne	Definicje adresacji sieci lokalnych. Lista portów proxy oddzielonych przecinkami. Wykorzystywane są w module monitorowania aktywności użytkowników (Users) do monitorowania użycia łącza i odpowiedniego klasyfikowania ruchu sieciowego (ruch LAN/Internet).
	Wzorce protokołów	Definicje grup wzorców protokołów - wykorzystywane są w module monitorowania aktywności użytkowników (Users) do monitorowania użycia łącza. Możesz tworzyć, edytować i usuwać grupy. Pakiet będzie zaliczony do wybranej grupy, jeśli spełnia co najmniej

Zakładka	Opcje	Opis
		jedno kryterium: nazwa pliku wykonywalnego aplikacji lub porty, na których działa.
	Domeny	Definicje grup domen do oznaczenia odwiedzonych stron. Możesz tworzyć, edytować i usuwać grupy.
Zasoby	Zakładka prezentuje listę katalogów, które **nie są skanowane** podczas monitorowania zasobów. Możesz tworzyć, edytować i usuwać wpisy. W tej zakładce można również utworzyć kategorie rozszerzeń plików, które będą wykrywane przez Agenty.	
HelpDesk	Zakładka umożliwia zarządzanie Kluczowymi ustawieniami oraz przetwarzaniem zgłoszeń w HelpDesku. Pamiętaj aby skonfigurować również port HelpDesku w opcjach nVision, w zakładce **Zdalny dostęp WWW**.	

2.5.6 Informacje dla zaawansowanych

Użycie poniższych funkcji jest zalecane tylko dla zaawansowanych użytkowników.

Wywołania serwisowe z przeglądarki

We wszystkich poniższych wywołaniach jako `IP_*` należy wpisać adres IP komputera, na którym zainstalowany jest Serwer lub Agent nVision.

1. Sprawdzenie informacji o działającym Serwerze:

   `http://IP_SERWERA:4434`

2. Sprawdzenie informacji o działającym Agencie (sprawdzenie identyfikatora komputera - Machine GUID):

   `http://IP_AGENTA:4433`

3. Sprawdzenie listy znanych przez Agenta atlasów:

   `http://IP_AGENTA:4433/atlases`

4. Pobranie pliku instalatora Agenta:

   `http://IP_SERWERA:4436/nVAgentInstall.exe`

5. Pobranie pliku instalatora Zdalnej Konsoli:

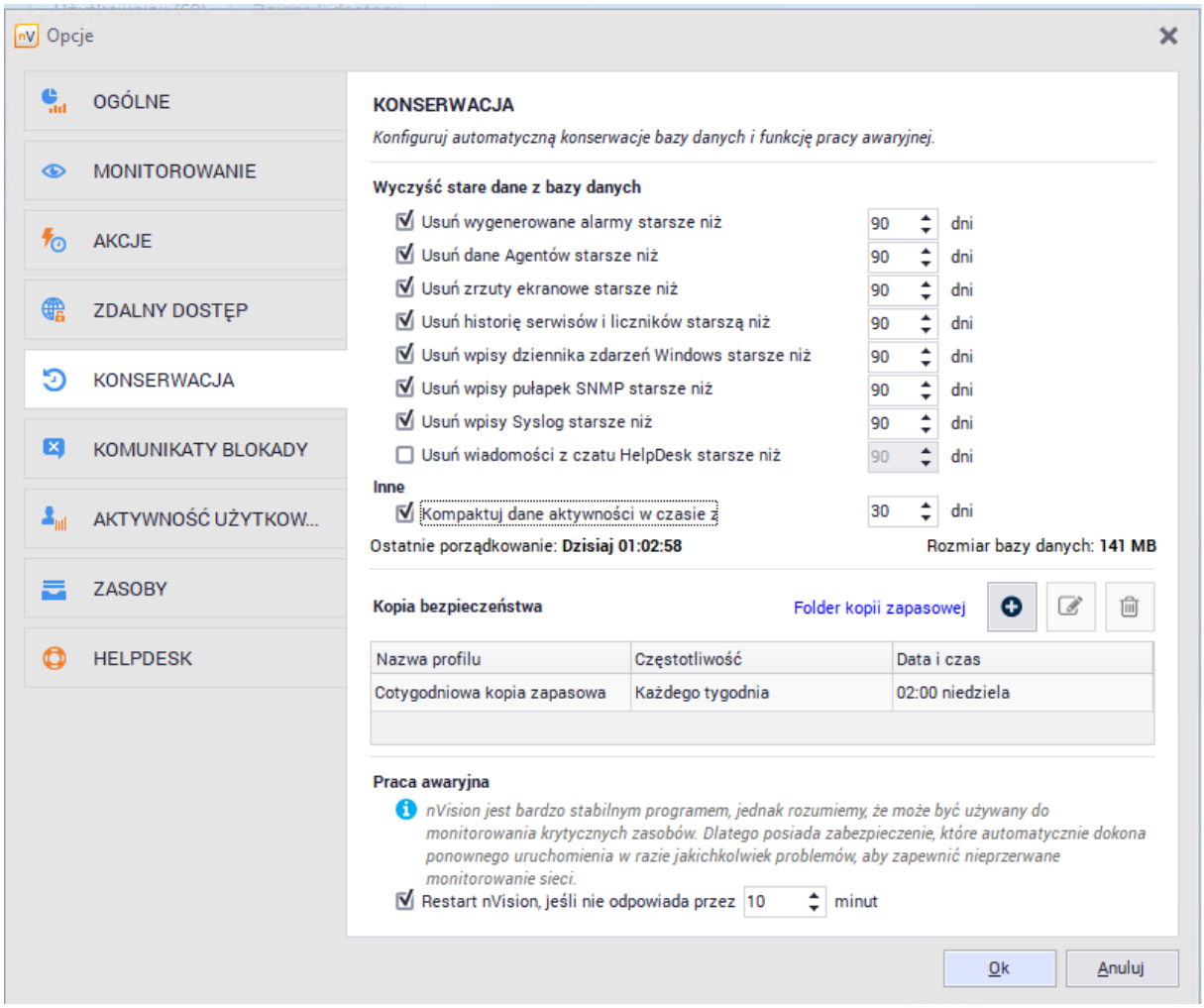
   `http://IP_SERWERA:4436/nVisionSetup.exe`

2.6 Wydajność nVision

W przypadku dużej liczby Agentów przesyłających dane do nVision, wykonaj poniższe akcje dla uzyskania wysokiej wydajności:

Ponad 250 Agentów

1. Przejdź do głównej konfiguracji programu i kliknij w zakładkę **Konserwacja**.
2. Zaznacz opcję **Kompaktuj dane aktywności w czasie z**.



Ponad 1000 Agentów

1. Przejdź do okna **ustawień** Atlasu, grupy lub **okna informacji o użytkowniku**
2. W zakładce **Ustawienia** zmnień opcję **Przesyłaj aktywność w czasie** na **Nie monitoruj**.

Raporty

Dla osiągnięcia pełnej wydajności generowania raportów należy zainstalować Microsoft Core XML Services (MSXML) 6.0:

http://www.microsoft.com/download/en/details.aspx?id=3988.

2.7 Funkcja "Zgłoś problem"

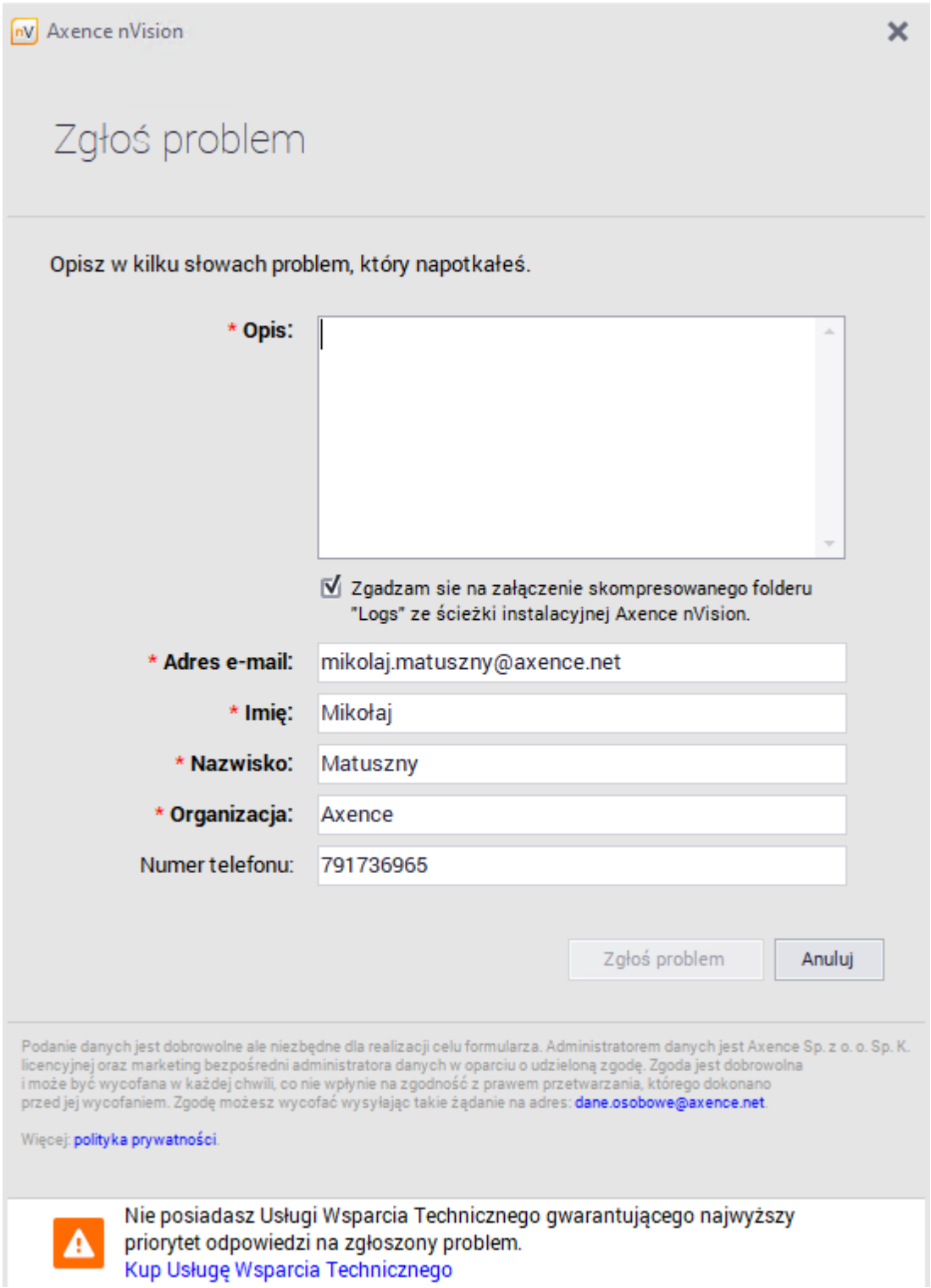
W Axence nVision® 10 wprowadzono uproszczone zgłaszanie problemów dostępne po ze **wstążki** karty **Axence nVision \ Zgłoś problem.** Celem tej funkcji jest ułatwienie Administratorowi zgłaszania napotkanych problemów lub błędów w działaniu programu.

Funkcja wymaga aktywnego połączenia komputera z zainstalowanym Serwerem Axence nVision® z Internetem.

Aby zgłosić problem:

1. Kliknij na wstążce kartę **Axence nVision** a następnie link **Zgłoś problem.**

2. W nowym oknie **Zgłoś problem** wypełnij krótki formularz:



3. Zaznaczenie pola **Zgadzam się na załączenie skompresowanego folderu "Logs" ze ścieżki instalacyjnej Axence nVision®** spowoduje dodanie załącznika zawierającego oczyszone i skompresowane (2MB) archiwum folderu logów Serwera nVision (domyślnie: C:\Program Files (x86) \Axence\nVision\Logs). Przesłanie logów działania programu ułatwia analizę problemu oraz przyśpiesza czas procesowania zgłoszenia.
4. Po kliknięciu przycisku **Zgłoś problem** wysyłana jest wiadomość na adres: pomoc@axence.net

W systemie zgłoszeń Pomocy Technicznej firmy Axence dostępnym pod adresem http://service.axence.net tworzone jest zgłoszenie.
Pierwsza odpowiedź od Pracownika Pomocy Technicznej przesyłana jest w ciągu kilku godzin a najpóźniej następnego dnia roboczego (w przypadku zgłoszeń wymagających wnikliwej analizy logów, czas ten może się wydłużyć).
Administrator może sprawdzić status zgłoszenia logując się w portalu https://service.axence.net/hc/en-us/requests używając adresu e-mail, podanego w formularzu **Zgłoś problem.** Link do ustanowienia hasła do portalu przesyłany jest automatycznie na wspomniany adres e-mail po utworzeniu zgłoszenia. Hasło można również zresetować ręcznie korzystając z formularza na stronie: https://axence.zendesk.com/auth/v2/login/password_reset

2.8 Konfiguracja urządzenia GSM

W nVision możliwe jest ustawienie powiadamiania administratora o alarmach przy użyciu SMS-ów.

Wysyłanie powiadomień przez SMS jest wygodnym sposobem informowania w przypadku zajścia zdefiniowanych wcześniej zdarzeń, na przykład znacznej zmiany treści na stronie WWW (podejrzenie ataku), kopiowania plików na urządzenie mobilne, czy zmiany w zasobach sprzętowych. Wiadomości mogą być wysyłane przez telefony komórkowe podłączone przez USB, sterownik kabla i COM oraz przez modemy GSM (najczęściej też podłączone przez USB). Jest to łatwe, ponieważ wielu operatorów dostarcza karty SIM działające przez długi okres.

Ważne: operatorzy nie dają gwarancji na natychmiastowe dostarczenie SMS-a. W przypadku krytycznych powiadomień nie należy polegać na wiadomościach SMS ani na e-mailach.

Przetestowane urządzenia

Wśród popularnych telefonów i modemów przetestowane zostały poniższe:

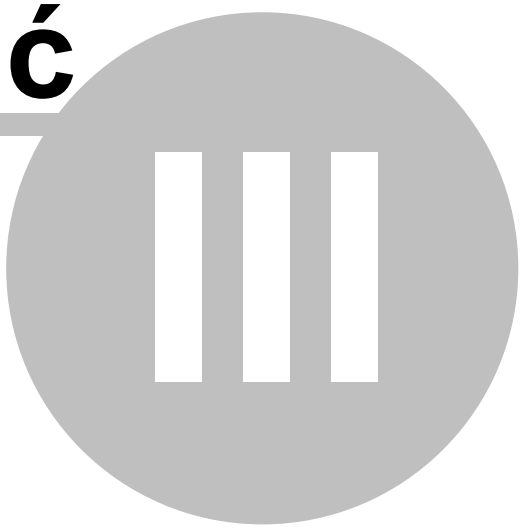
- Falcom: Twist, Swift, Samba 55, Samba 75,
- iTegno: WM1080A, WM1080A1I, WM1080A1E, 3000, 3232E, 3232I, 3898,
- Multitech: MTCBA-G-UF1, MTCBA-G-UF2,
- Nokia: N30, N32, 6100, 6210, 6220, 6310, 6310i, 6820 (Bluetooth), 8910,
- Siemens: TC35, TC35i, TC45, TC65, MC35, MC35i, MC45, MC55, MC65, MC75, A65, AC75, AC45, C35, C45, M35, M45, S35,
- SIMCOM: SIM100S, SIM100T,
- Sony Ericsson: T310, T610, T630, T68, T68i, K310, K320, K500, K510, K600, K700, K750i, K800i, V800, W300, W550, W600, W700, W800i, W810, W900, Z1010, GC75, GC79, GC83, GC85, GC89,
- Teltonika: T-ModemUSB, T-ModemCOM,
- Wavecom: Fastrack M1206B, Fastrack M1306B, Integra, WMOi3.

Oprócz wymienionych powyżej, poprawnie powinna funkcjonować większość modemów USB.

Należy pamiętać o skonfigurowaniu urządzenia oprogramowaniem dostarczonym przez producenta (w szczególności o wprowadzeniu PIN karty SIM).

Jeśli chcesz dowiedzieć się więcej o akcjach notyfikujących, przejdź do rozdziału Definiowanie własności akcji.

Część



3 Wykrywanie i monitorowanie sieci

3.1 Wprowadzenie

Wymagania i planowanie

Przed rozpoczęciem monitorowania sieci należy zapoznać się z rozdziałem Wymagania i konfiguracja. Opisuje on sposób przygotowania urządzeń oraz sieci tak, aby uzyskać wszelkie konieczne informacje.

Wykrywanie sieci

nVision posiada wbudowany, zaawansowany skaner sieciowy który nie tylko wykrywa wszystkie urządzenia w sieci, ale także routery przez które "przechodzi" wykrywając wszystkie sąsiednie sieci. Wykrywa wszystkie urządzenia oraz serwisy na nich działające, takie jak: HTTP, FTP, poczta, serwery bazodanowe, itp.

Do atlasu można dodać dowolną liczbę sieci. Po dodaniu sieci, jest ona skanowana, a więc w pierwszej kolejności należy użyć kreatora skanera sieci, aby zdefiniować opcje wykrywania.

Po ukończeniu procesu skanowania program utworzy mapę sieci lub ich zestaw dla wszystkich wykrytych sieci IP. Sieci zostaną utworzone jako drzewo, które pokazuje zależności pomiędzy nimi.

Aby dowiedzieć się więcej o procesie skanowania, przejdź do rozdziału Wykrywanie sieci.

Monitorowanie urządzeń

nVision może monitorować serwisy sieciowe, liczniki systemowe i SNMP. Nie tylko monitoruje, ale także zapisuje wszelkie informacje i pozwala przeglądać historyczne dane w celu raportowania.

Aby uzyskać więcej informacji, przejdź do rozdziału Monitorowanie.

Stan urządzenia

Stan urządzenia to bardzo ważne pojęcie, której poświęcony został osobny rozdział: Pojęcie stanu urządzenia.

3.2 Pojęcie stanu urządzenia

Stan urządzenia jako wartość wyliczona

Odmiennie niż w przypadku innych produktów, stan urządzenia w nVision może być zmieniony przez zdarzenia. Można zdefiniować warunki, w których urządzenie uzyska stan <Nieznany>, <Działa>, <Nie działa> lub <Ostrzeżenie>. Stan urządzenia zmienia się też w zależności od stanu monitorowanych serwisów.

Automatyczna zmiana stanu

Stan urządzenia początkowo ustawiony jest na <Nieznany>. Zmienia się, gdy nVision rozpoczyna monitorowanie serwisów. Gdy tylko pierwszy serwis zostanie sprawdzony i działa, stan zmieni się na <Działa>. Stan <Ostrzeżenie> oznacza, że istnieją serwisy, które nie działają, ale przynajmniej jeden serwis działa. Stan zmienia się na <Nie działa> jeśli żaden serwis nie działa.

Zmiana stanu przez zdarzenia

Bardzo ważne jest, aby zrozumieć, że nVision określa stan urządzenia także na podstawie aktualnie wygenerowanych alarmów. W tym celu można zdefiniować pole **Zmień stan urządzenia na** w każdym zdarzeniu. Kiedy alarm dla danego zdarzenia jest wygenerowany, wtedy stan urządzenia może zmienić się zgodnie ze zdefiniowaną wartością.

W polu tym można zdefiniować trzy wartości: <Bez zmiany>, <Ostrzeżenie> oraz <Nie działa>. Stan <Nie działa> ma najwyższy priorytet, co oznacza, że jeśli choć jedno zdarzenie ma taki stan, wtedy stan urządzenia również zmieni się na <Nie działa> (niezależnie od stanu monitorowanych serwisów). Jeśli wygenerowanych jest kilka zdarzeń o stanie <Ostrzeżenie> i <Nie działa> wtedy stan urządzenia będzie także <Nie działa>. Jeśli wygenerowane były tylko zdarzenia o stanie <Ostrzeżenie> wtedy stan urządzenia też zmieni się na <Ostrzeżenie> (chyba, że stan już jest <Nie działa> ze względu na niedziałające serwisy - wtedy stan pozostanie <Nie działa>).

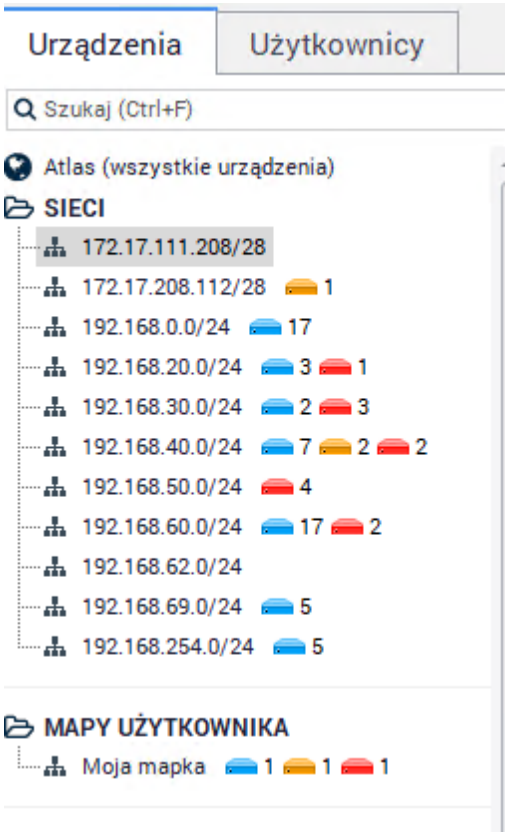
3.3 Wykrywanie sieci

3.3.1 Wykrywanie sieci

Do atlasu można dodać dowolną liczbę sieci. Żeby dodać sieć należy skorzystać ze skanera sieciowego, który wykryje wszystkie urządzenia.

1. Kliknij opcję **Wykryj nową sieć** (na karcie **Narzędzia i opcje)**.
   Otworzy się kreator skanera sieci. Kreator ten pomoże wykryć sieć, wszystkie urządzenia oraz utworzyć mapy sieci.
2. Przejdź przez kolejne kroki kreatora. Informacje dotyczące dostępnych w nim opcji znajdują się w rozdziale Kreator wykrywania sieci.

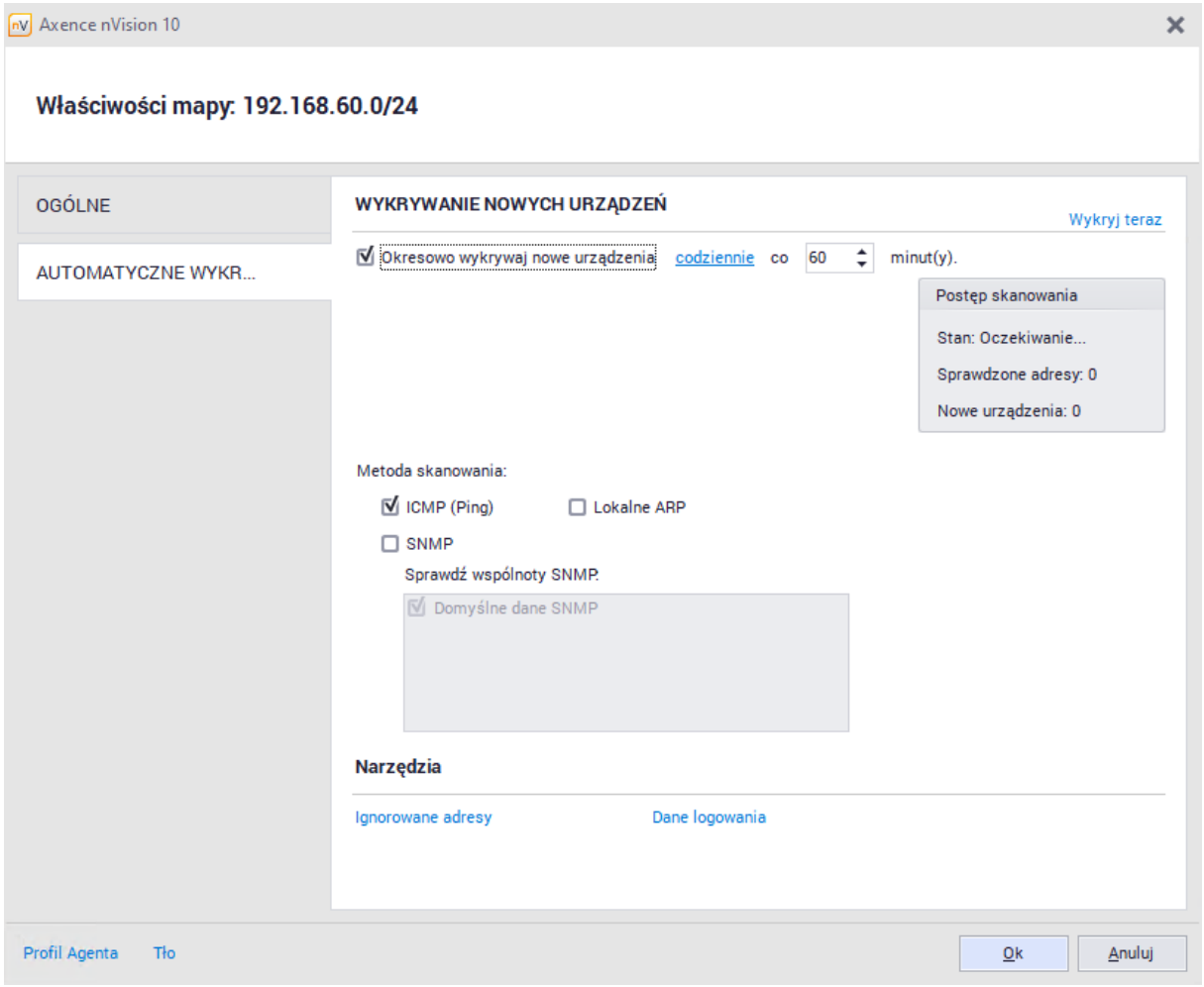
Po zakończeniu procesu skanowania program utworzy mapę wykrytej sieci lub zestaw takich. Sieci będą utworzone jako drzewo pokazujące zależności pomiędzy nimi - sieci utworzone pod określoną mapą są przyłączone właśnie do niej. Prezentuje to poniższy przykład:



Jak można zauważyć sieć 192.168.0.0 jest utworzona pod siecią 89.79.238.106. Oznacza to, że sieci te połączone są przez router. nVision wykrywa wszystkie routery oraz podłączone sieci, co pozwala zobaczyć strukturę logiczną sieci.

nVision może też wykryć urządzenia automatycznie przez wybranie **Wykryj nowe urządzenia** z menu kontekstowego mapy. Proces ten może być wykonywany okresowo:

1. Wybierz mapę, na której chcesz włączyć automatyczne wykrywanie.
2. Otwórz okno **właściwości** mapy i wybierz zakładkę A**utomatyczne wykrywanie**, która pozwala skonfigurować i uruchomić proces wykrywania. Zakładka ta pokazuje też aktualny stan i postęp w belce statusu.
3. Zaznacz opcję **Okresowo wykrywaj nowe urządzenia**
4. Skonfiguruj częstość i czas wykrywania
5. Możesz też uruchomić wykrywanie klikając na przycisku **Wykryj teraz**.



3.3.2 Kreator skanowania sieci

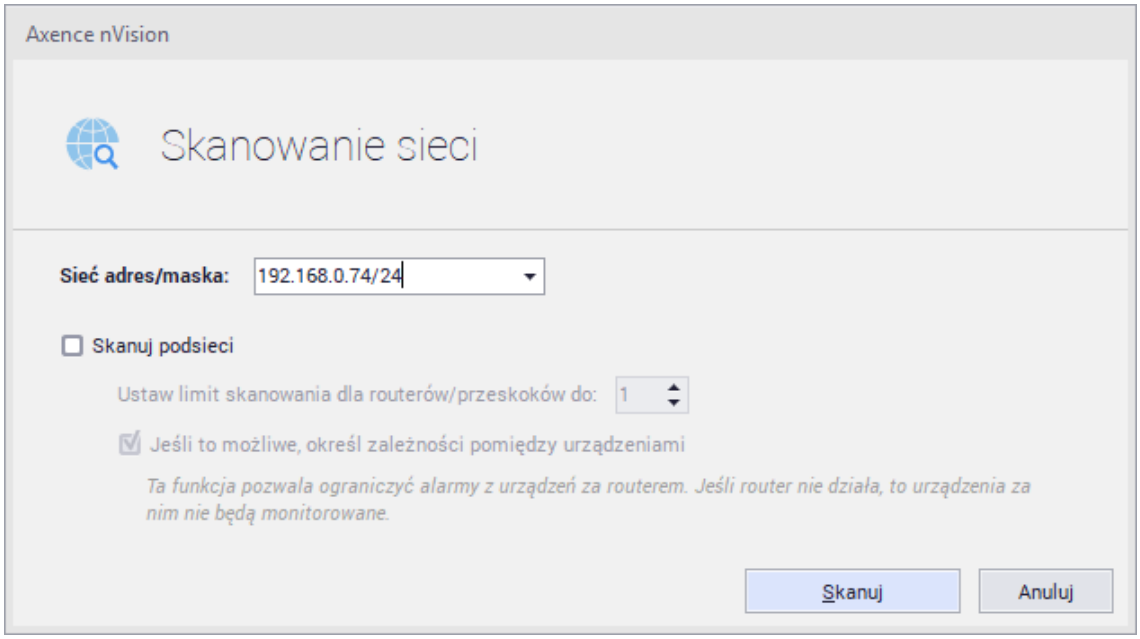
Kreator skanowania sieci pozwala zdefiniować opcje konieczne do przeprowadzenia właściwego skanowania sieci. Uruchamiany jest jeśli chcemy dodać nową sieć i podczas tworzenia Atlasu.

Opcje skanowania nowej sieci

Pozwala zdefiniować jaka sieć i w jaki sposób będzie skanowana.

Właściwość	Opis
Adres	Podaj adres IP/DNS komputera znajdującego się w sieci, która ma być skanowana. Program domyślnie podpowiada lokalny adres, który należy pozostawić, jeśli skanujemy sieć lokalną.
Maska	Maska sieciowa. W większości przypadków nie ma konieczności zmiany domyślnej maski o wartości "255.255.255.0". Zmiana może spowodować bardzo długi czas skanowania.
Skanuj podsieci	Wybierz tą opcję, jeśli w twojej sieci jest router i chcesz także wyskanować sąsiednie sieci, znajdujące się za

Właściwość	Opis
	routerem. nVision może skanować nie tylko podaną sieć, ale potrafi też "przechodzić" routery znajdujące się w tej sieci, aby wyskanować wszystkie podłączone sieci. Funkcja ta wymaga udostępnionego na routerze protokołu SNMP oraz podania wspólnoty SNMP. Program odczyta tabelę routingu i zacznie skanować wszystkie sieci podłączone przez ten router.
Ustaw limit skanowania dla routerów/przeskoków do	Pozwala określić limit hopów (routerów) podczas skanowania.
Jeśli to możliwe, określ zależności pomiędzy urządzeniami	Ta funkcja pozwala ograniczyć alarmy z urządzeń za routerem. Jeśli router nie działa, to urządzenia za nim nie będą monitorowane.



Kliknij przycisk **Skanuj**. Rozpocznie to proces skanowania, który będzie można śledzić. Proces ten można w dowolnej chwili przerwać. W takim przypadku można dodać sieci i urządzenia już wykryte.

Po zakończeniu skanowania, pokaże się okno określające liczbę wykrytych sieci/urządzeń. Kliknij **OK**, aby zamknąć skaner i dodać do Atlasu wykryte sieci i urządzenia.

3.3.3 Dodawanie nowego urządzenia

Opis dodawania nowego urządzenia znajduje się w rozdziale Zarządzanie urządzeniami.

3.4 Monitorowanie

3.4.1 Wprowadzenie do monitorowania

Co może być monitorowane

nVision może monitorować:

- **Stan urządzenia**
  Monitorowany jest dla każdego urządzenia i pozwala uzyskać raporty na temat dostępności urządzeń w czasie.
- **Serwisy**
  - Dostępność: jeśli serwis przestanie odpowiadać nVision pokaże taką informację na mapie i może wygenerować alarm.
  - Wydajność: czas odpowiedzi i procent utraconych pakietów. Można monitorować dowolny serwis TCP/UDP. nVision posiada dużą listę predefiniowanych serwisów takich jak MS SQL Server, Oracle, Notes/Domino, itp.
- **Serwery pocztowe i WWW**
  Specjalne testy serwisów: nVision posiada kilka wbudowanych próbników, które mogą sprawdzać wydajność wysokopoziomowych funkcji pewnych serwisów. Są to następujące próbniki:
  - Czas ładowania strony - mierzy czas załadowania określonej strony.
  - Zmiana treści strony - sprawdza, czy zawartość strony nie uległa zmianie.
  - Czas logowania do POP3 - mierzy czas potrzebny na zalogowanie się do serwera POP3 i sprawdzenia listy dostępnych emaili.
  - Czas wysłania przez SMTP - mierzy czas potrzebny na wysłanie emaila przez serwer SMTP.
- **Routery i switch'e (MRTG)**
  - Interfejsy sieciowe: stan i we/wy ruch sieciowy.
  - Porty switch'a: informacja o stanie portu, adres MAC oraz IP komputerów podłączonych to dowolnego portu oraz ilość przetransmitowanych danych.
  - Ruch sieciowy urządzenia: ruch sieciowy generowany przez urządzenie (monitorowanie przez RMON za pomocą SNMP)
- **Liczniki wydajności**
  - SNMP: można monitorować dowolny licznik SNMP, który zwraca wartość liczbową.
  - Windows: nVision może monitorować liczniki systemu Windows co pozwala monitorować wydajność systemu oraz aplikacji na nim działających. W ten sposób można monitorować liczniki serwisów takich jak serwery MS SQL, Exchange, itp.

Wizualizacja

nVision prezentuje wszystkie monitorowane parametry (zarówno serwisy jak i liczniki) na przejrzystych wykresach. Pokazują one nie tylko raporty zmian wartości w czasie, ale także pozwalają śledzić je w czasie rzeczywistym.

Czas monitorowania

Ustawienie czasu monitorowania we właściwościach urządzenia nie oznacza, że serwisy i liczniki będą monitorowane dokładnie co zadany okres. Jeśli nVision monitoruje dużą sieć z wieloma urządzeniami, okres monitorowania może się wydłużyć, ponieważ nVision może wysłać tylko określoną liczbę żądań na sekundę. W związku z tym, czas monitorowania jest najkrótszym możliwym czasem w jakim serwisy i liczniki mogą być monitorowane. Jeśli urządzeń jest dużo, czas ten może się też znacząco wydłużyć.

Jak dane z monitorowania są przetwarzane

nVision początkowo gromadzi dane z monitorowania w pamięci. Informacja ta zbierana jest w formie kolejnych próbek zapisywanych w momencie każdego sprawdzenia. Można zobaczyć wszystkie próbki tylko na wykresie 15-minutowym. Jeśli zebrane dane przekroczą limit zajętości pamięci, najstarsza próbka jest usuwana za każdym razem, gdy dodawana jest nowa.

Dane z monitorowania zapisywane są do bazy jako 1-minutowe średnie wartości. Dlatego przeglądając wykresy dla dłuższych okresów, dane prezentowane są co najwyżej z rozdzielczością 1-minutową. nVision nie zapisuje wszystkich próbek, ze względu na możliwość monitorowania dużych sieci. W takich sieciach, z dużą liczbą urządzeń, ilość danych gromadzonych codziennie jest znaczna i nie byłoby możliwe ich szybkie przetwarzanie.

3.4.2 Pojęcia

Skaner serwisów i monitor

Po znalezieniu wszystkich urządzeń w sieci nVision wykrywa serwisy na nich działające. Skanowane są tylko wybrane serwisy. Aby uzyskać więcej informacji na temat wyboru skanowanych serwisów, przejdź do rozdziału Opcje programu.

Skaner serwisów nie tylko sprawdza, czy odpowiedni port jest otwarty. Wysyła określone żądanie i sprawdza, czy odpowiedź odpowiada zdefiniowanym kryteriom. Jeśli tak, serwis jest dodawany do urządzenia i nVision rozpoczyna jego monitorowanie.

Monitor serwisów używa tej samem metody co skaner: wysyła żądanie przez TCP/UDP i zapamiętuje czas odpowiedzi oraz procent żądań (pakietów) utraconych. Sprawdza też, czy otrzymana odpowiedź pasuje do ustalonych kryteriów.

Monitor liczników

nVision pozwala monitorować kilka typów liczników wydajności. Poniższa tabela przedstawia dostępne liczniki:

Typ licznika	Opis
Stan urządzenia	Prezentuje stan urządzenia dla każdej minuty. Pozwala raportować dostępność urządzenia.
SNMP	Liczniki SNMP udostępniane są przez protokół SNMP dostępny na routerach i większości serwerów. Pozwalają na monitorowanie takich informacji jak transfery sieciowe, liczbę użytkowników, obciążenie CPU, itp.

Typ licznika	Opis
Windows	nVision może monitorować dowolne liczniki Windows, włączając w to te podawane przez aplikacje nie systemowe, jak serwery MS SQL i Exchange.
Czas ładowania strony	Mierzy czas załadowania określonej strony WWW.
Zmiana strony	Określa zmianę określonej strony WWW.
Czas logowania POP3	Sprawdza czas potrzebny do zalogowania się do serwera POP3 i sprawdzenia listy dostępnych e-maili.
Czas wysłania SMTP	Mierzy czas konieczny do wysłania emaila.

Stan urządzenia

Odmiennie niż w innych, podobnych produktach, stan urządzenia w nVision jest wartością wyliczaną, a nie zakodowaną na stałe. Można więc zdefiniować warunki w których urządzenie ma stan <Nie działa> oraz <Ostrzeżenie>. Aby uzyskać więcej informacji, zapoznaj się z rozdziałem Pojęcie stanu urządzenia.

3.4.3 Monitorowanie serwisów

3.4.3.1 Wykrywanie i monitorowanie serwisów

Jak serwisy są wykrywane i monitorowane

nVision monitoruje serwisy UDP/TCP bazując na predefiniowanych regułach. Nie tylko sprawdza czy określony port jest otwarty, ale wysyła żądanie i czeka na odpowiedź. Potem odpowiedź ta jest sprawdza pod kątem zgodności z określonymi regułami. Tylko takie żądania, gdzie odpowiedź jest poprawna, uznawane są jako świadczące o działaniu serwisu. Ten sam mechanizm wykorzystywany jest do wykrywania serwisów działających na urządzeniach. Zapewni to, że serwisy nie są omyłkowo wykrywane, gdy jakiś serwis działa na porcie przeznaczonym dla innego serwisu. Przykładowo, jeśli FTP będzie działać na porcie 80, nie zostanie wykryty serwis HTTP, jako że odpowiedź nie jest właściwa jako serwisu HTTP.

Serwis nie działa

Gdy serwis nie działa, otrzymuje stan <Nie działa>. Można to zobaczyć jako czerwoną ikonkę w tabeli serwisów dostępnej na zakładce **Serwisy** w oknie **Informacje o urządzeniu**.

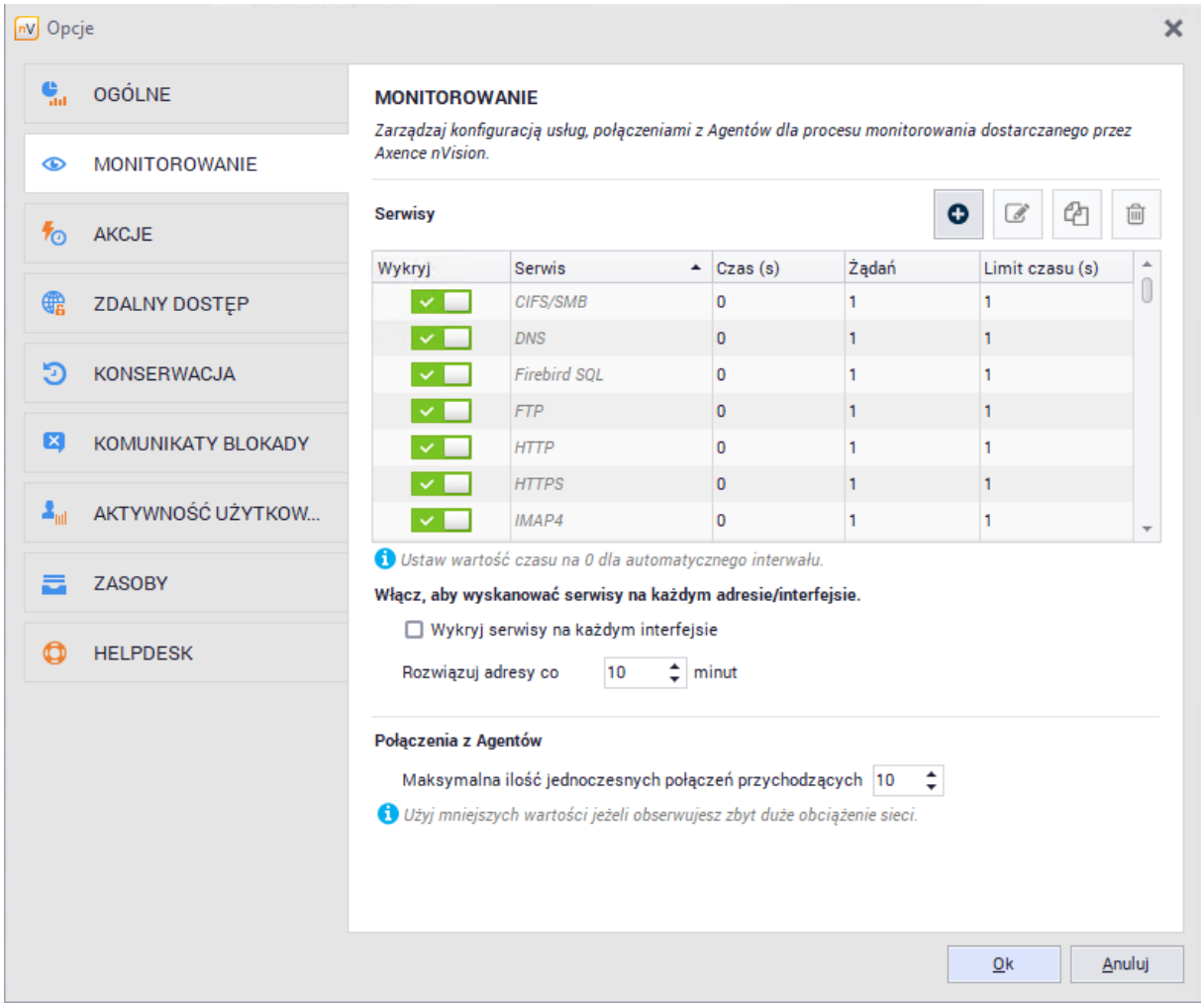
Serwis prowadzący

Dla każdego urządzenia jest zawsze zdefiniowany jeden serwis **prowadzący**. Serwis ten jest oznaczony pogrubioną czcionką w tabeli serwisów w oknie **Informacje o urządzeniu**. Serwis **prowadzący** jest najważniejszym serwisem urządzenia. Czas odpowiedzi tego serwisu może być prezentowany na ikonie urządzenia.

Jak monitorować urządzenia i serwisy?

Po wykryciu urządzeń w sieci nVision automatycznie wykrywa najważniejsze serwisy na nich

działające. Aby więc rozpocząć monitorowanie urządzeń i ich serwisów, nie ma potrzeby wykonywania żadnych dodatkowych działań poza wykrywaniem sieci. Można jednak, manualnie lub przez wywołanie narzędzia wykrywania serwisów, dodać nowy serwis.



Dodawanie serwisów

Aby uzupełnić domyślną listę monitorowanych serwisów:

1. Na wstążce wybierz Opcje (z karty **Narzędzi i opcje**). Przejdź do zakładki **Monitorowanie**.
2. Jeśli chcesz dodać serwis, kliknij w przycisk i wybierz z listy serwis, który ma być monitorowany. Aby zarządzać definicjami serwisów, kliknij w przycisk **Zarządzaj serwisami**.

Serwisy na urządzeniach

Lista monitorowanych serwisów wraz z wykresami reprezentującymi czas odpowiedzi i % utraconych pakietów/żądań, dostępna jest w oknie Stan urządzenia.

Aby uzyskać więcej informacji o serwisach przejdź do rozdziału Zarządzanie urządzeniami.

3.4.3.2 Zarządzanie monitorowanymi serwisami

Rozdział ten opisuje zarządzanie monitorowanymi serwisami.

Otwieranie okna Informacje o urządzeniu na zakładce Serwisy

Za pomocą tego okna można przeglądać, tworzyć, modyfikować i usuwać monitorowane serwisy. Okno nie tylko prezentuje wszystkie serwisy, ale także pokazuje wykresy czasu odpowiedzi w czasie. Wykresy te mogą przedstawiać informację w czasie rzeczywistym.

1. Kliknij podwójnie na ikonie urządzenia lub wybierz **Informacje o urządzeniu** z menu kontekstowego.
2. Wybierz zakładkę **Wydajność \ Serwisy**.

Dodawanie nowych serwisów do monitora lub modyfikowanie istniejącego

1. Otwórz okno **Informacje o urządzeniu** na zakładce **Wydajność \ Serwisy**.
2. Kliknij ikonę aby dodać nowy serwis lub wybierz istniejący serwis i kliknij ikonę aby zmodyfikować jego właściwości.
   Otworzy się okno **Właściwości serwisu**.
3. Skonfiguruj opcje. Poniższa tabela opisuje ich znaczenie.

Właściwość	Opis
Serwis do monitorowania	
Nazwa	Wybierz serwis, który chcesz monitorować. Pole to nie może być zmienione podczas edycji istniejącego serwisu. Aby rozpocząć monitorowanie innego serwisu, należy go stworzyć.
Na interfejsie/IP	Wybierz adres na którym serwis ma być monitorowany.
Parametry monitorowania	
Czas monitorowania	Wybierz **Auto,** aby nVision samo zarządzało czasem monitorowania tak, aby zapewnić jak najczęstsze sprawdzenia (zależnie od liczby monitorowanych urządzeń). Jeśli chcesz ustawić określoną wartość, wybierz **Ustaw** i wpisz tą wartość w polu edycji.
Żądania	Jest to liczba żądań wysyłanych podczas każdego sprawdzenia. Dla serwisów TCP wartość ta powinna być ustawiona na 1, ponieważ protokół ten ma własne mechanizmy chroniące przed utratą żądania (serwisy TCP same powtarzają utracone żądania, więc zwykle podawanie większej wartości nie miałoby sensu). Dla serwisów bazujących na ICMP i UDP warto podać 2-3 aby zagwarantować, iż przypadkowa utrata pakietów nie uruchomi fałszywego alarmu.

Właściwość	Opis
Limit czasu	Czas oczekiwania na odpowiedź. Jeśli nie zostanie otrzymana w tym czasie, żądanie jest uznawane za utracone. Dla serwisów ICMP i UDP wartość 1000 - 2000 ms będzie zwykle odpowiednia. Dla serwisów TCP, ze względu na ich własności, należy podać zdecydowanie wyższą wartość w przedziale 15 000 - 30 000 ms.

Usuwanie serwisu

1. Otwórz okno **Informacje o urządzeniu** na zakładce **Wydajność \ Serwisy**.
2. Wybierz serwis.
3. Kliknij ikonę kosza aby usunąć serwis.

Ponowne wykrywanie serwisów urządzenia

1. Otwórz okno **Informacje o urządzeniu** na zakładce **Wydajność \ Serwisy**.
2. Kliknij opcję **Skanuj ponownie**.
   nVision rozpocznie skanowanie nowych serwisów na wszystkich interfejsach/adresach urządzenia. Po zakończeniu, nowe serwisy zostaną dodane do listy i rozpocznie się ich monitorowanie.

Wybór serwisu wiodącego

Aby uzyskać informacje na temat serwisu wiodącego, przejdź do rozdziału Monitorowanie serwisów.

1. Otwórz okno **Informacje o urządzeniu** na zakładce **Wydajność \ Serwisy**..
2. Zaznacz serwis i wybierz **Ustaw jako wiodący** z menu kontekstowego.
   Serwis wiodący jest wskazywany pogrubioną czcionką.

3.4.3.3 Tworzenie alarmu dla serwisu

Aby zostać powiadomionym w razie problemów z serwisem konieczne jest utworzenie alarmu. Rozdział ten opisuje kolejne kroki niezbędne do wykonania tej czynności.

1. Aby otworzyć okno alarmów, kliknij opcję **Alarmy** znajdującą się na wstążce na karcie **Główne**.
2. Utwórz nowy alarm klikając ikonę **Dodaj alarm** znajdującą się w głównym pasku narzędziowym. Otworzy się okno właściwości alarmu. Za pomocą tego okna można utworzyć zdarzenie inicjujące alarm oraz dodać akcje do wykonania w razie wygenerowania alarmu.
3. Kliknij przycisk **Nowy** znajdujący się po prawej stronie pola zdarzenia. Pozwoli to utworzyć nowe zdarzenie.
   Dla serwisów wybierz typ zdarzenia: **Serwis nie działa** lub **Wydajność serwisu**. Utwórz zdarzenie zgodnie z informacją w rozdziale Właściwości zdarzeń.
4. Kliknij ikonę  i zdefiniuj akcję, która będzie wykonana gdy alarm zostanie wygenerowany.

Możesz wybrać akcję istniejącą lub utworzyć nową. Aby stworzyć nową akcję kliknij przycisk **Nowy** znajdujący się po prawej stronie pola wyboru akcji. Utwórz akcję zgodnie z informacjami dostępnymi w rozdziale Definiowanie własności akcji.

3.4.3.4 Monitorowanie usług Windows

nVision może monitorować serwisy Windows. W razie wystąpienia problemów z serwisem (np. serwis przestaje działać), można skonfigurować akcję alarmową, która uruchomi lub zrestartuje serwis. Monitorowanie serwisów jest wykonywane przez WMI lub przez Agenta.

Aby monitorować przez WMI, konieczne jest właściwe skonfigurowanie danych logowania w oknieinformacji o urządzeniu oraz udostępnienie WMI na zdalnym urządzeniu. Aby uzyskać więcej informacji, przejdź do rozdziału Wymagania i konfiguracja.

Aby monitorować usługi Windows bez otwierania zdalnego dostępu do WMI, należy zainstalować Agenta.

Aby włączyć monitorowanie serwisów Windows

1. Otwórz okno informacji o urządzeniu.
2. Wybierz zakładkę **Windows.**
3. Przejdź do karty **Usługi Windows,** kliknij link **Konfiguruj dane logowania** i wprowadź dane konta, które ma uprawnienia administartora na zdalnym komputerze.

3.4.4 Monitorowanie wydajności urządzenia i systemu

3.4.4.1 Liczniki wydajności i stan urządzenia

nVision może monitorować kilka typów liczników wydajności i stan urządzenia.

Stan urządzenia

Jest to wbudowany licznik, monitorujący i zapisujący stan urządzenia. Licznik ten zapisywany jest co minutę, aby można było śledzić dostępność urządzenia w czasie.

Liczniki Windows i SNMP

nVision może monitorować liczniki Windows za pomocą WMI lub Agenta. Liczniki Windows i SNMP mogą być użyte do monitorowania wydajności systemu Windows, wydajności aplikacji (MS Exchange, IIS, SQL, itp.), switch'ów i routerów (ruch sieciowy, błędy, itp.).

Testy serwisów (monitorowanie serwerów pocztowych i WWW)

Jest to grupa liczników zaprojektowana do monitorowania serwerów pocztowych i WWW. Aby uzyskać więcej informacji, przejdź do rozdziału Monitorowanie serwerów pocztowych i WWW.

3.4.4.2 Typy liczników

Istnieje kilka grup liczników. Poniższa tabela opisuje grupy Dostępność urządzenia oraz Liczniki. Aby uzyskać więcej informacji o grupie Test serwisu, przejdź do rozdziału Monitorowanie serwerów pocztowych i WWW.

Dostępność urządzenia

Stan urządzenia	Licznik ten zapisuje stan urządzenia dla celów raportowych. Jest to licznik wbudowany i nie może być usunięty.
Liczniki	
Liczniki SNMP	Można mierzyć dowolny licznik SNMP o wartości numerycznej. Program może też odczytać całą kolumnę tabeli i zapisać min/max/średnią/sume wartości komórek.
Licznik Windows	Można mierzyć dowolny licznik Windows o wartości numerycznej. Windows udostępnia liczniki systemowe i aplikacyjne. Pozwala to monitorować system oraz programy takie jak SQL Server i Exchange Server.

Liczniki określone dla urządzenia

Niektóre liczniki posiadają pełną informację konieczną do ich sprawdzenia, włączając w to adres urządzenia. Takie liczniki nazywamy Określonymi dla urządzenia. W ogólności wszystkie liczniki typu Testy serwisu są określone dla urządzenia (na przykład licznik **Czas ładowania strony**).

3.4.4.3 Zarządzanie licznikami wydajności

Rozdział ten opisuje zarządzenia licznikami wydajności.

Otwarcie okna Informacje o urządzeniu na zakładce Liczniki wydajności

W tym oknie można zobaczyć, zmodyfikować, tworzyć i usuwać liczniki. Liczniki nie tylko widoczne są w tabeli, ale także można przeglądać ich wartość w czasie na wykresie.

1. Kliknij podwójnie na ikonie urządzenia lub wybierz **Informacje o urządzeniu** z menu kontekstowego.
2. Wybierz zakładkę **Wydajność \ Liczniki wydajności**.

Utworzenie nowego licznika lub modyfikacja istniejącego

1. Otwórz okno **Informacje o urządzeniu** na zakładce **Wydajność \ Liczniki wydajności**.
2. Kliknij ikonę  aby dodać nowy licznik lub wybierz istniejący licznik i kliknij ikonę  aby zmodyfikować jego właściwości.
   Otworzy się okno **Właściwości licznika**.
3. Jeśli tworzysz nowy licznik, wybierz jego typ z listy i kliknij przycisk **Dalej**. Aby dowiedzieć się więcej o typach liczników, przejdź do rozdziału Typy liczników.
4. Skonfiguruj opcje licznika (zależnie od typu licznika jaki wybrałeś). Szczegóły opcji opisane są w rozdziale Definiowanie właściwości liczników.
5. Kliknij przycisk **Zakończ**.

Usuwanie licznika

1. Otwórz okno **Informacje o urządzeniu** na zakładce **Wydajność \ Liczniki wydajności**.

2. Wybierz licznik, który chcesz usunąć.
3. Kliknij ikonę aby usunąć licznik.

3.4.4.4 Tworzenie alarmu dla licznika wydajności

Rozdział ten opisuje sposób utworzenia alarmu na wypadek przekroczenia przez licznik wydajności dopuszczalnego zakresu. Np. alarm, który powiadomi, gdy kolejka pocztowa serwera MS Exchange będzie zbyt długa. Taki licznik wydajnościowy musi być utworzony na każdym serwerze, na którym działa Exchange - następnie tworzymy zdarzenie, które zainicjuje alarm. nVision zapewnia możliwość łatwego utworzenia alarmu i licznika na każdym komputerze, na którym uruchomiony jest MS Exchange.

1. Aby otworzyć okno alarmów, kliknij opcję **Alarmy** znajdującą się na wstążce na karcie **Główne**.
2. Utwórz nowy alarm klikając ikonę **Dodaj alarm** znajdującą się w głównym pasku narzędziowym. Otworzy się okno właściwości alarmu. Za pomocą tego okna można utworzyć zdarzenie inicjujące alarm oraz dodać akcje do wykonania w razie wygenerowania alarmu.
3. Kliknij przycisk **Nowy** znajdujący się po prawej stronie pola zdarzenia. Pozwoli to utworzyć nowe zdarzenie.
   Dla liczników wybierz typ zdarzenia: **Test serwisu** lub **Liczniki**. Utwórz zdarzenie zgodnie z informacją w rozdziale Właściwości zdarzeń.
4. Kliknij ikonę i zdefiniuj akcję, która będzie wykonana gdy alarm zostanie wygenerowany. Możesz wybrać akcję istniejącą lub utworzyć nową. Aby stworzyć nową akcję, kliknij przycisk **Nowy** znajdujący się po prawej stronie pola wyboru akcji.
   Utwórz akcję zgodnie z informacjami dostępnymi w rozdziale Właściwości akcji.

3.4.4.5 Tworzenie licznika na wielu urządzeniach

W wielu przypadkach konieczne jest stworzenie tego samego licznika na wielu urządzeniach. Można to zrobić używając funkcji automatycznego tworzenia liczników. Pozwala ona na stworzenie tego samego licznika Windows lub SNMP na wielu urządzeniach.
Liczniki mogą być stworzone tylko na tych urządzeniach, które wspierają dany licznik - program sprawdzi, czy jest on dostępny na zdalnym urządzeniu.

1. Wybierz **Utwórz licznik dla urządzeń** z karty **Narzędzia i opcje** na wstążce.
   Otworzy się **Kreator definicji licznika**.
2. Wybierz **Windows** lub **SNMP**.
3. Wybierz liczniki i podaj czas monitorowania.
4. Wybierz **Wszystkie** aby utworzyć licznik na wszystkich urządzeniach lub **Wybrane** aby zaznaczyć urządzenia. Aby zaznaczyć kilka urządzeń, użyj Ctrl + klik i Shift + klik.
5. Jeśli chcesz, aby program sprawdził, czy licznik jest dostępny na poszczególnych urządzeniach, włącz **Utwórz tylko jeśli urządzenie wspiera licznik**. Dzięki temu można szybko utworzyć wiele liczników tylko na urządzeniach, które je udostępniają.

3.4.4.6 Definiowanie właściwości liczników

Rozdział ten opisuje właściwości poszczególnych typów liczników w grupie **Liczniki**.

Próg Windows

Właściwość	Opis
Nazwa	Nazwa ta będzie wyświetlona w tabeli.
Licznik	Licznik, który ma być monitorowany. Aby wybrać licznik, kliknij ikonę ··· i wybierz właściwą klasę, licznik i instancję. Może być konieczne ustawienie danych logowania, aby nVision mógł połączyć się ze zdalnym komputerem i pobrać listę liczników.
Interwał monitorowania	Jeśli wybierzesz **Auto** nVision będzie zarządzać czasem monitorowania, tak aby zapewnić odpowiednio częste sprawdzenia (zależnie od liczby monitorowanych urządzeń). Jeśli chcesz ustawić określoną wartość, wybierz **Ustaw** i wpisz ją w polu edycji.

Uwagi

- Program nVision będzie próbował zalogować się do zdalnego komputera za pomocą danych logowania podanych we właściwościach urządzenia.
- Liczniki Windows nie są monitorowane jeśli urządzenie ma stan <Nie działa>.

Próg SNMP

Właściwość	Opis
Nazwa	Nazwa ta będzie wyświetlona w tabeli.
Wybierz licznik SNMP	Licznik, który ma być monitorowany. Aby wybrać licznik, kliknij ikonę ··· i wybierz właściwą właściwy licznik SNMP. Można wybrać odczyt całej kolumny tabeli i zapis wartości min/max/średniej/sumy wartości komórek. Może być konieczne ustawienie Wspólnoty SNMP do odczytu, aby nVision mógł połączyć się ze zdalny urządzeniem i pobrać dane.
Podaj OID licznika SNMP	Licznik, który ma być monitorowany. Jeśli podajesz wartość samodzielnie, jesteś odpowiedzialny za wprowadzenie poprawnej wartości. Jeśli OID nie jest poprawny, nie będzie odczytana żadna wartość.
Absolutna	Program zapisze odczytaną wartość.
Średnia na sek., jednostka	Bazując na kolejno odczytanych wartościach, nVision

Właściwość	Opis
	wyliczy szybkość zmiany na sekundę i zapisze tą wartość. Jest to właściwa opcja jeśli monitorujesz liczbę bajtów wysłanych/odebranych i chcesz monitorować obciążenie łącza. Możesz też wybrać jednostki w jakich wartość będzie zapisana.
Interwał monitorowania	Jeśli wybierzesz **Auto** nVision będzie zarządzać czasem monitorowania tak, aby zapewnić odpowiednio częste sprawdzenia (zależnie od liczby monitorowanych urządzeń). Jeśli chcesz ustawić określoną wartość, wybierz **Ustaw** i wpisz ją w polu edycji.

Uwagi

- Program nVision będzie próbował połączyć się do zdalnego komputera korzystając ze wspólnoty SNMP do odczytu podanej we właściwościach urządzenia.
- Liczniki Windows nie są monitorowane jeśli urządzenie ma stan <Nie działa>.

3.4.5 Monitorowanie serwerów pocztowych i WWW

3.4.5.1 Liczniki do monitorowania serwerów pocztowych i WWW

nVision posiada kilka specjalnych liczników do monitorowania serwerów pocztowych i WWW. Liczniki te nie tylko podłączają się do serwera, ale także wykonują pewne testy, aby sprawdzić, czy serwer funkcjonuje poprawnie: określenie czasu załadowania strony i jej zawartości, sprawdzenie listy przychodzących e-maili i wysłanie testowego emaila. Aby wykonać takie testy, należy utworzyć odpowiedni licznik w zakładce **Liczniki wydajności** okna **Informacje o urządzeniu**. Aby dowiedzieć się więcej o tych licznikach i operacjach testowych, przejdź do rozdziału Typy liczników. Aby uzyskać informację o tworzeniu liczników przejdź do rozdziału Zarządzenie licznikami wydajności.

3.4.5.2 Typy liczników

Poniższa lista opisuje wyłącznie grupę Test serwisu odpowiedzialną za monitorowanie serwerów pocztowych i WWW. Aby uzyskać informacje o innych grupach (Dostępność urządzenia i Liczniki) przejdź do rozdziału Monitorowanie wydajności urządzenia i systemu.

Test serwisu	
Czas ładowania strony	Mierzy czas załadowania określonej strony.
Zmiana tresci strony	Sprawdza zmianę zawartości strony.
Czas zalogowania POP3	Mierzy czas konieczny do zalogowania się do serwera pocztowego.
Czas wysłania emaila	Mierzy czas konieczny do wysłania testowego emaila.
Testuj połączenie HTTPS	Testuje połączenie HTTPS z możliwością podania certyfikatu klienta.

Liczniki określone dla urządzenia

Niektóre liczniki posiadają pełną informację konieczną do ich sprawdzenia, włączając w to adres urządzenia. Takie liczniki nazywamy Określonymi dla urządzenia. W ogólności wszystkie liczniki typu Testy serwisu są określone dla urządzenia (na przykład licznik **Czas ładowania strony**).

3.4.5.3 Definiowanie właściwości liczników

Rozdział ten opisuje właściwości poszczególnych typów liczników w grupie **Test serwisu**.

Czas ładowania strony

Licznik ten mierzy czas załadowania określonej strony.

Właściwość	Opis
Adres	Adres strony, która będzie sprawdzana.
Interwał monitorowania	Jeśli wybierzesz **Auto** nVision będzie zarządzać czasem monitorowania tak, aby zapewnić odpowiednio częste sprawdzenia (zależnie od liczby monitorowanych urządzeń). Jeśli chcesz ustawić określoną wartość, wybierz **Ustaw** i wpisz ją w polu edycji.

Zmiana zawartości strony

Licznik ten określa procent zmiany zawartości strony.

Właściwość	Opis
Adres	Adres strony, która będzie sprawdzana.
Interwał monitorowania	Jeśli wybierzesz **Auto** nVision będzie zarządzać czasem monitorowania tak, aby zapewnić odpowiednio częste sprawdzenia (zależnie od liczby monitorowanych urządzeń). Jeśli chcesz ustawić określoną wartość, wybierz **Ustaw** i wpisz ją w polu edycji.

Czas logowania POP3

Licznik ten monitoruje czas potrzebny do zalogowania się do serwera POP3 i sprawdzenia listy dostępnych e-maili.

Właściwość	Opis
Adres serwera POP3	Adres serwera pocztowego
Użytkownik	Nazwa użytkownika konieczna do zalogowania
Hasło	Hasło konieczne do zalogowania
Interwał monitorowania	Jeśli wybierzesz **Auto** nVision będzie zarządzać czasem

Właściwość	Opis
	monitorowania tak, aby zapewnić odpowiednio częste sprawdzenia (zależnie od liczby monitorowanych urządzeń). Jeśli chcesz ustawić określoną wartość, wybierz **Ustaw** i wpisz ją w polu edycji.

Czas wysłania e-maila

Licznik ten mierzy czas konieczny do wysłania testowego e-maila.

Właściwość	Opis
Adres serwera SMTP	Adres serwera pocztowego.
Wymagana autoryzacja	Włącz tą opcję, jeśli twój serwer wymaga autoryzacji do wysłania e-maila.
Użytkownik	Nazwa użytkownika konieczna do zalogowania
Hasło	Hasło konieczne do zalogowania
Wyślij email do	Adres na który email testowy zostanie wysłany. Zmierzony będzie czas całej operacji.
Adres zwrotny	Jeśli adres ten nie jest właściwie ustawiony, lub pusty, większość serwerów pocztowych odrzuci email. Podaj adres, który będzie zaakceptowany przez serwer (najprawdopodobniej twój adres email).
Interwał monitorowania	Jeśli wybierzesz **Auto** nVision będzie zarządzać czasem monitorowania tak, aby zapewnić odpowiednio częste sprawdzenia (zależnie od liczby monitorowanych urządzeń). Jeśli chcesz ustawić określoną wartość, wybierz **Ustaw** i wpisz ją w polu edycji.

3.4.6 Monitorowanie routerów i switch'y

3.4.6.1 Monitorowanie za pomocą SNMP

Dzięki nVision można monitorować za pomocą SNMP następujące elementy sieci:

- **Interfejsy**: status i aktualny ruch sieciowy. Można także skonfigurować monitorowanie ruchu na wejściu/wyjściu każdego interfejsu. Takie informacje są potem prezentowane w zakładce **Liczniki wydajności**, można także zobaczyć wykresy prezentujące ruch sieciowy.
- **Porty switch'a**: nVision automatycznie odczytuje informacje SNMP dotyczące portów switch'a, jeśli tylko jest to możliwe. Gdy taka informacja jest dostępna, zobaczysz zakładkę **Mapowanie portów** w oknie **Informacje o urządzeniu**. Zakładka ta zawiera informacje o statusie każdego portu, adresach MAC i IP komputerów podłączonych do każdego portu, a także ich całkowity/aktualny ruch sieciowy na wejściu/wyjściu.
- **Ruch sieciowy**: niektóre switch'e i routery zbierają informacje o ruchu sieciowych generowanym

przez każde urządzenie. Takie dane są dostępne w tabelach RMON. nVision automatyzuje proces monitorowania ruchu sieciowego generowanego przez dane urządzenie.

To wszystko umożliwia szeroko zakrojone monitorowanie infrastruktury sieciowej, statusu switch'y, routerów i ruchu sieciowego.

3.4.6.2 Monitorowanie portów switch'a

nVision automatycznie odczytuje informacje o wszystkich portach dla każdego switch'a zarządzalnego przez SNMP. Te informacje są prezentowane graficznie w zakładce w oknie **Informacje o urządzeniu \ SNMP \ Mapowanie portów**. Tabela poniżej przedstawia znaczenie poszczególnych symboli graficznych:

Ikona	Opis
	Port jest aktywny, ale nic nie jest do niego podłączone.
	Port jest aktywny i jest do niego podłączona wtyczka.
	Port jest nieaktywny (uszkodzony) i nic nie jest do niego podłączone.
	Port jest nieaktywny (uszkodzony) i jest do niego podłączona wtyczka.

Zakładka ta może nie być dostępna na początku (po przeskanowaniu sieci). Pokaże się ona automatycznie, gdy tylko nVision odczyta z urządzenia zawartości tabeli "dot1dBasePortTable" (OID: 1.3.6.1.2.1.17.1.4), co może zająć jakiś czas. Jeśli zakładka nie pojawia się przez dłuższy czas, upewnij się, że SNMP jest dostępne na tym urządzeniu i że prawidłowo skonfigurowałeś wspólnotę SNMP we właściwościach urządzenia.

Aby włączyć mapowanie portów na switchu:

1. Przejdź do okna **Informacje o urządzeniu**.
2. W zakładce **Ogólne** zaznacz pole **Włącz monitorowanie** (serwisy, liczniki, SNMP, mapowanie portów, Windows).
3. W zakładce **Snmp \ Przeglądarka SNMP** zaznacz pole **Urządzenie zarządzalne przez SNMP** oraz kliknij link **Konfiguruj dane logowania -** następnie skonfiguruj poprawną wspólnotę SNMP (ustawioną w panelu zarządzania urządzenia). Upewnij się, że dane logowania są poprawne poprzez kliknięcie przycisku **Testuj dane logowania** (test powinien zakończyć się komunikatem "Test wspólnoty SNMP się powiódł").

Zakładka mapowania portów powinna pojawić się po otwarciu okna **Informacje o urządzeniu**.

Jeśli pomimo prawidłowego skonfigurowania powyższych punktów zakładka port mappera nie jest generowana - należy upewnić się, że tabela "dot1dBasePortTable" jest dostępna na danym urządzeniu (odczytując jej zawartość w zakładce "SNMP" według drzewa podanego w łączu poniżej).

http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en&translate=Translate&objectInput=1.3.6.1.2.1.17.1.4#oidContent

3.4.6.3 Monitorowanie ruchu sieciowego

Niektóre switche i routery zbierają informacje o ruchu sieciowym generowanym przez każde urządzenie. Dane te znajdują się w tabelach RMON SNMP. nVision automatyzuje proces monitorowania ruchu

sieciowego generowanego przez dane urządzenie.

Monitorowanie ruchu sieciowego urządzenia

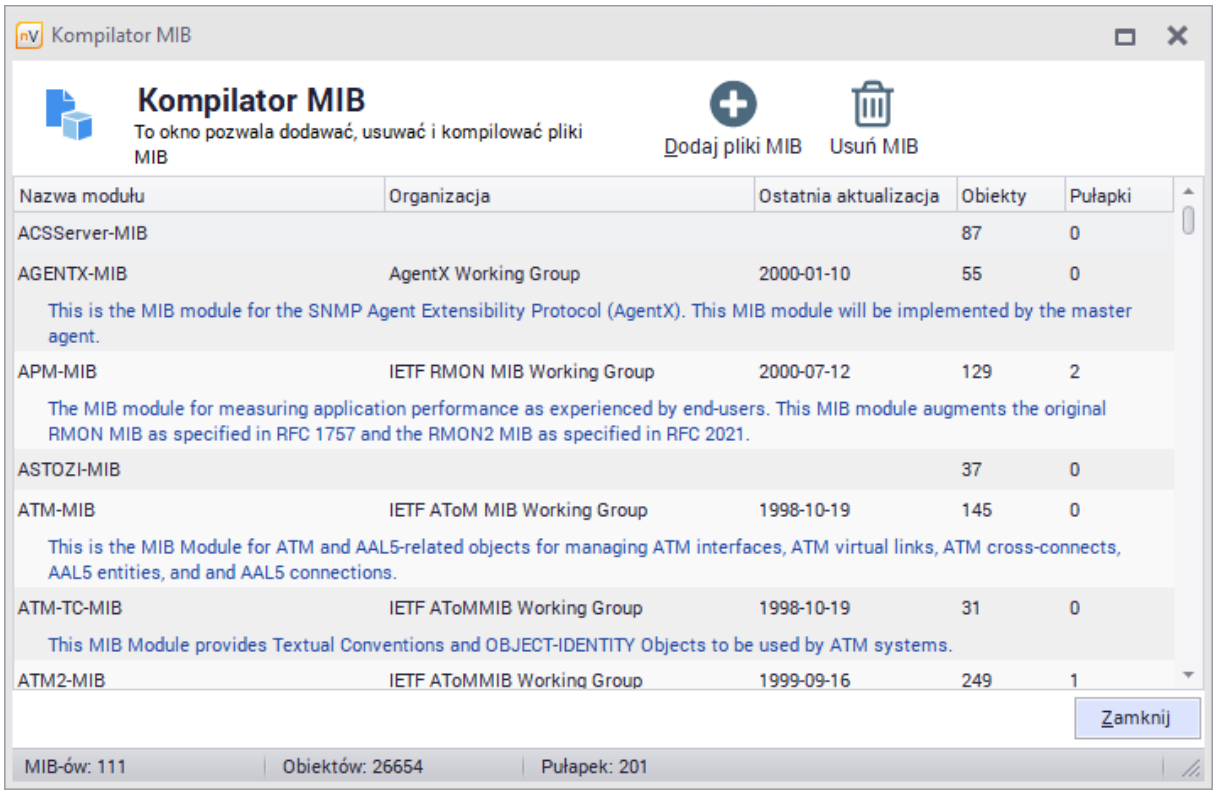
1. Otwórz okno **Informacje o urządzeniu**.
2. Przejdź do zakładki **Mapowanie portów**. Jeśli taka zakładka nie jest dostępna, oznacza to, że nie ma takich danych dla danego urządzenia. Aby uzyskać więcej informacji, przejdź do rozdziału Monitorowanie portów switch'a.
3. Wybierz wiersz, który zawiera informacje o urządzeniu, które chciałbyś monitorować. Wybierz **Monitoruj ruch sieciowy urządzenia** z menu kontekstowego.
   Utworzy to dwa liczniki monitorujące SNMP (dla ruchu sieciowego na wejściu/wyjściu). Liczniki te będą się znajdować w zakładce **Liczniki wydajnościowe**.

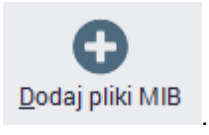
3.4.7 Kompilacja plików MIB

Kompilator plików MIB pozwala na dodawanie nowych plików MIB, ich usuwanie i kompilowanie. Ułatwia gromadzenie informacji ze wszystkich urządzeń sieciowych: przełączników, routerów, drukarek, urządzenia VoIP itp. Program może skutecznie monitorować tysiące różnych urządzeń SNMP.

Aby korzystać z kompilatora MIB:

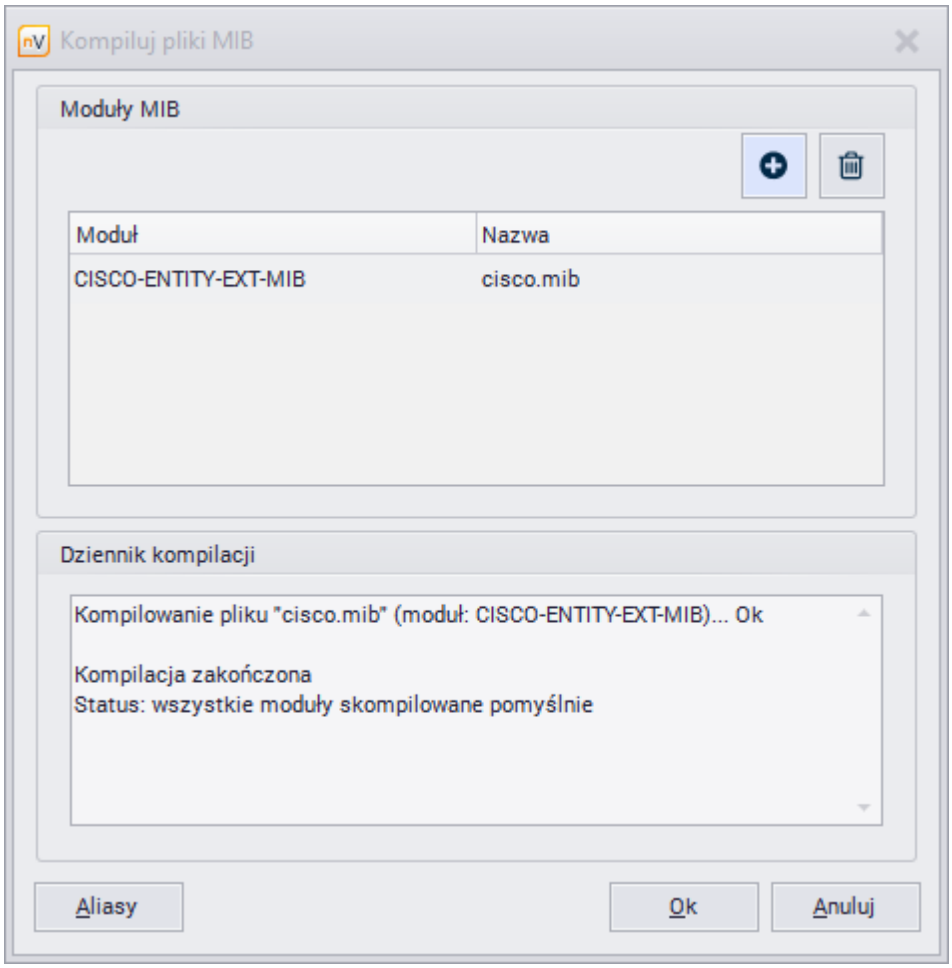
- Wybierz opcję **Kompilator MIB** z karty **Narzędzia i opcje** na wstążce. Okno kompilatora MIB zostanie otwarte.



1. Jeśli chcesz dodać nowy plik, kliknij na przycisk 

.

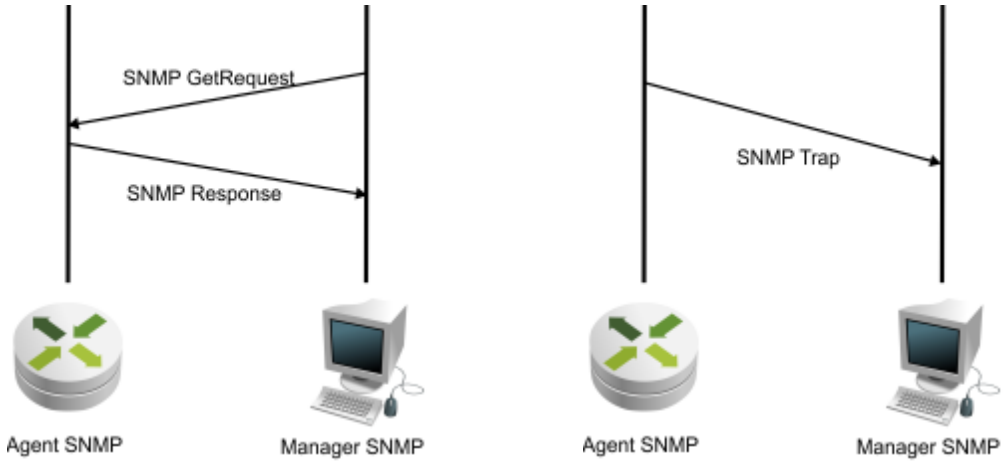
2. Dodaj moduł MIB, klikając na przycisk  i wybierając plik z jego lokalizacji. Dziennik kompilacji pojawia się po kompilacji.



3. Można również zdefiniować aliasy w Edytorze aliasów (przycisk **Aliasy**).

3.4.8 Pułapki SNMP

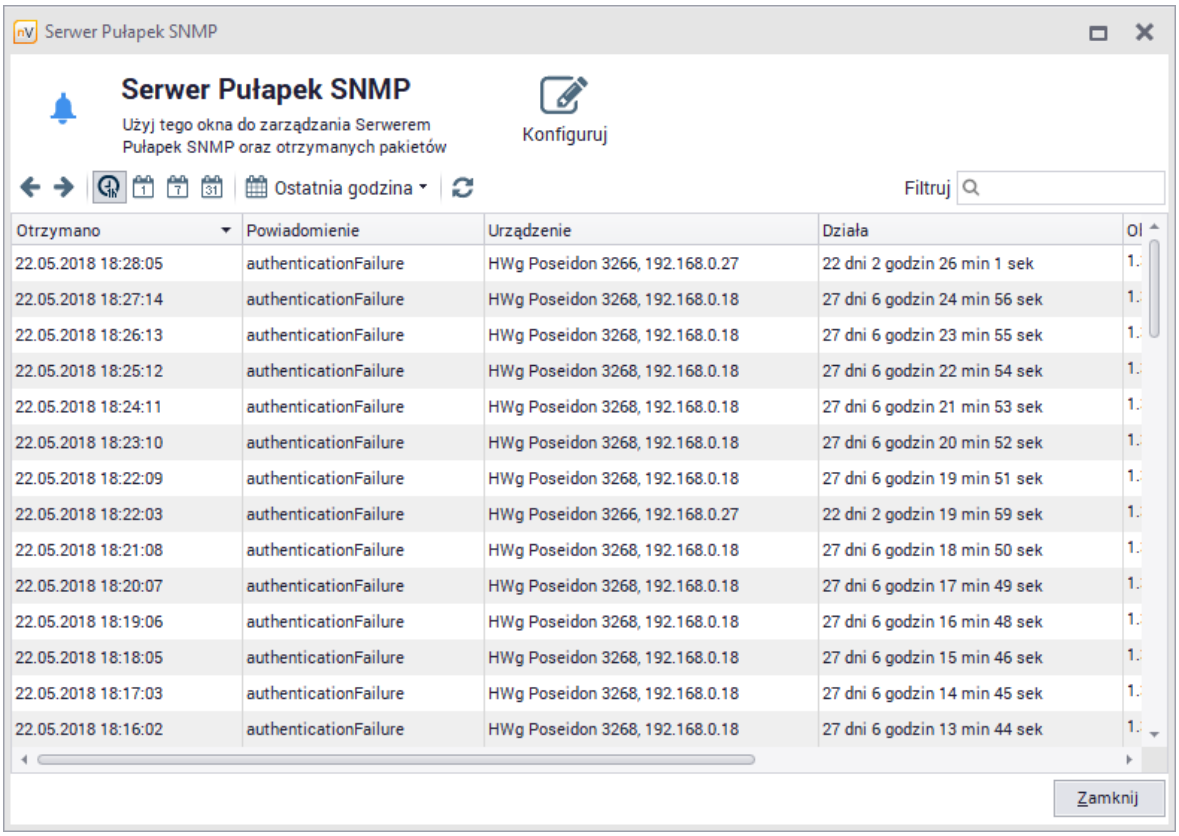
Pułapki SNMP umożliwiają Agentom SNMP powiadamianie managera o zmianie swojego stanu w przypadku zajścia określonego zdarzenia. Na poniższym diagramie przedstawione są różnice pomiędzy kontaktem nawiązywanym przez managera (po lewej) a komunikatem Trap wysyłanym przez Agenta (po prawej).



Serwer Pułapek SNMP

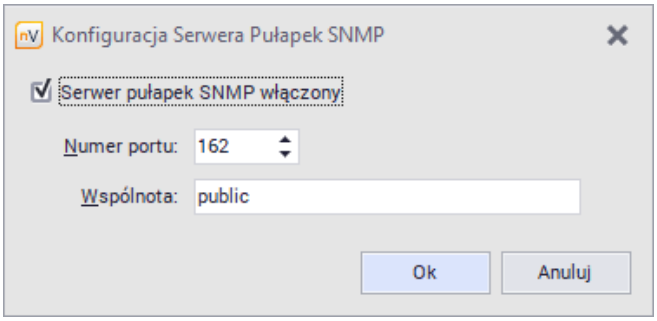
Aby zarządzać serwerem pułapek SNMP:

1. Wybierz **Serwer Pułapek SNMP** z karty **Narzędzia i opcje** na wstążce.
2. W oknie Serwera Pułapek SNMP wyświetlane są pułapki przechwycone przez serwer. Możesz wybrać okres, dla którego mają być pokazane dane (godzina, dzień, tydzień, miesiąc).



3. W celu skonfigurowania serwera kliknij w przycisk **Konfiguruj** znajdujący się w górnej części okna.

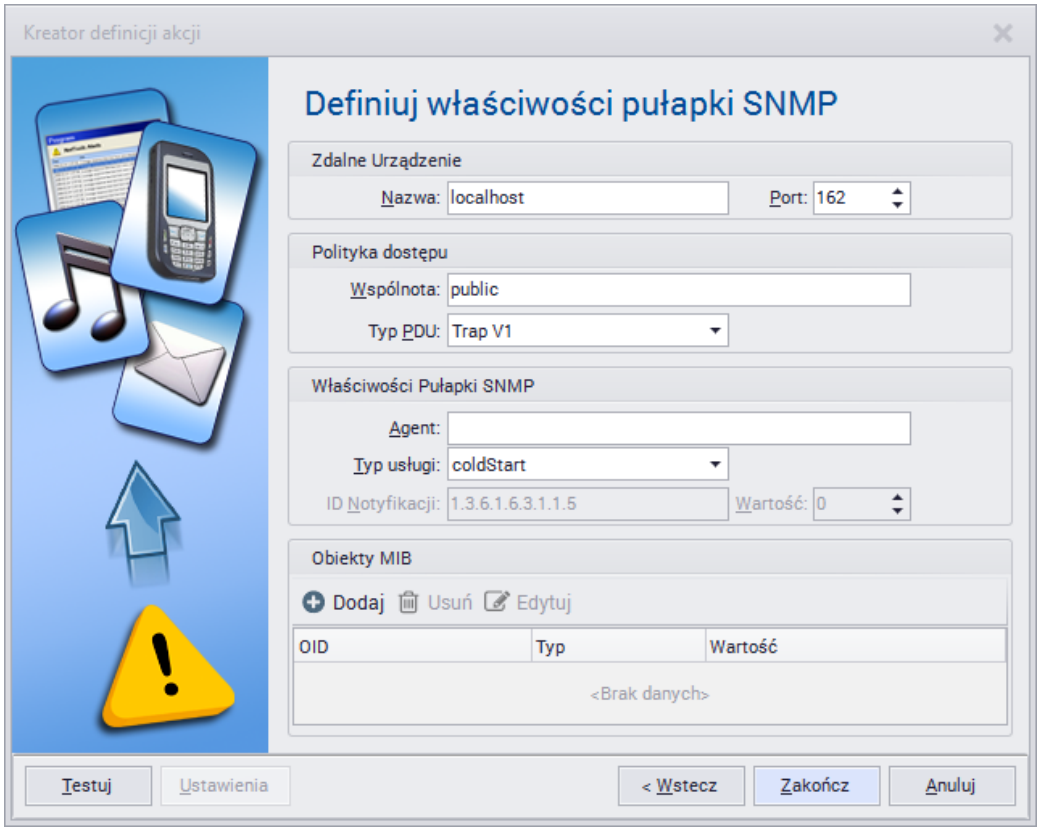
4. Ustaw port nasłuchiwania i opcje polityki dostępu. Zaznacz pole **Autostart serwera**, jeśli ma być on automatycznie uruchamiany przy starcie aplikacji.



Pułapka SNMP jako akcja

Aby zdefiniować pułapkę SNMP jako akcję:

1. Wybierz **Zarządzaj akcjami** z karty **Narzędzia i opcje** na wstążce.
2. W oknie Kreatora definicji akcji wpisz nazwę akcji i wybierz **Wyślij pułapkę SNMP**.
3. Uzupełnij pola **Nazwa**, **Port**, **Wspólnota** i **Typ PDU**.



4. Pole **ID Notyfikacji** jest wymagane, jeśli jako **Typ usługi** wybrano enterpriseSpecific.
5. Zgodnie ze specyfikacją SNMP Trap jest możliwość podania adresu Agenta SNMP, jeśli jest inny niż urządzenie wysyłające, oraz obiektów MIB z dodatkowymi informacjami dotyczącymi notyfikacji.

Powiązane tematy

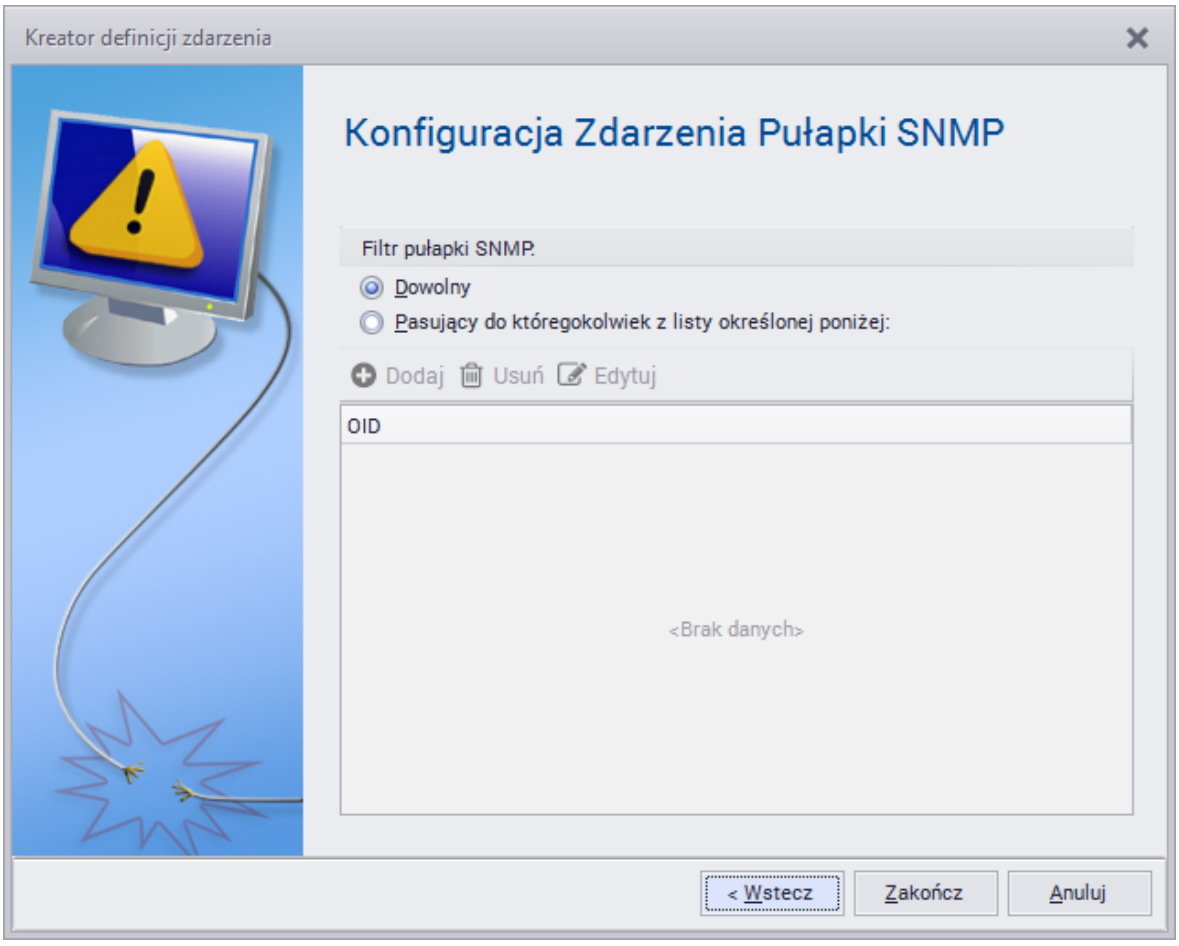
Alarmowanie

Akcje

Pułapka SNMP jako zdarzenie

Aby zdefiniować zdarzenie **Pułapka SNMP**:

1. Wybierz **Zarządzaj zdarzeniami** z karty **Narzędzia i opcje** na wstążce
2. Wpisz nazwę zdarzenia i wybierz typ zdarzenia **Inny | Pułapka SNMP**. Przejdź **Dalej**.
3. W oknie Kreatora definicja zdarzenia ustaw **Filtr MIB**. Jeśli wybrano drugą opcję, należy **Dodać** ID obiektów MIB, które mają być uwzględniane w definiowanym zdarzeniu.



Powiązane tematy

Alarmowanie

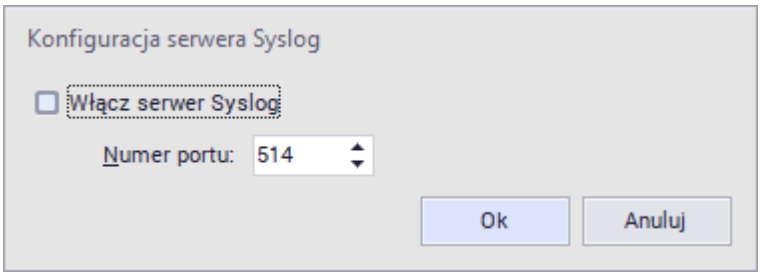
Zdarzenia

3.4.9 Serwer Syslog

Serwer Syslog

Aby zarządzać serwerem Syslog:

1. Wybierz **Serwer Syslog** z karty **Narzędzia i opcje** na wstążce.
2. W oknie Serwera Syslog wyświetlane są zdarzenia systemowe zarejestrowane przez serwer. Możesz wybrać okres, dla którego mają być pokazane dane (godzina, dzień, tydzień, miesiąc).
3. W celu skonfigurowania serwera kliknij w przycisk **Konfiguruj** znajdujący się w górnej części okna.
4. Ustaw port nasłuchiwania. Zaznacz pole **Autostart serwera**, jeśli ma być on automatycznie uruchamiany przy starcie aplikacji.



5. W panelu administracyjnym danego urządzenia podaj adres i port serwera Syslog, do którego będą wysyłane komunikaty, czyli adres serwera nVision wraz ze skonfigurowanym portem.

Wiadomość SysLog jako akcja

Aby zdefiniować wiadomość SysLog jako akcję:

1. Wybierz **Zarządzaj akcjami** z karty **Narzędzia i opcje** na wstążce .
2. W oknie Kreatora definicji akcji wpisz nazwę akcji i wybierz **Wyślij wiadomość SysLog**.
3. Uzupełnij pola **Adres** i **Port serwera** oraz wiadomość SysLog, jaka ma zostać wysłana.

Powiązane tematy

Alarmowanie

Akcje

Wiadomość SysLog jako zdarzenie

Aby zdefiniować zdarzenie **Wiadomość SysLog**:

1. Wybierz **Zarządzaj zdarzeniami** z karty **Narzędzia i opcje** na wstążce.
2. Wpisz nazwę zdarzenia i wybierz typ zdarzenia **Inny | Wiadomość SysLog**. Przejdź **Dalej**.
3. W oknie Kreatora definicja zdarzenia ustaw **Filtr słów kluczowych SysLog**. Zdarzenie może uwzględniać **Dowolne** komunikaty SysLog, lub pasujące do słów kluczowych. Jeśli wybrano drugą opcję, należy **Dodać** słowa kluczowe, które mają być uwzględniane w definiowanym zdarzeniu.

Powiązane tematy

Alarmowanie

Zdarzenia

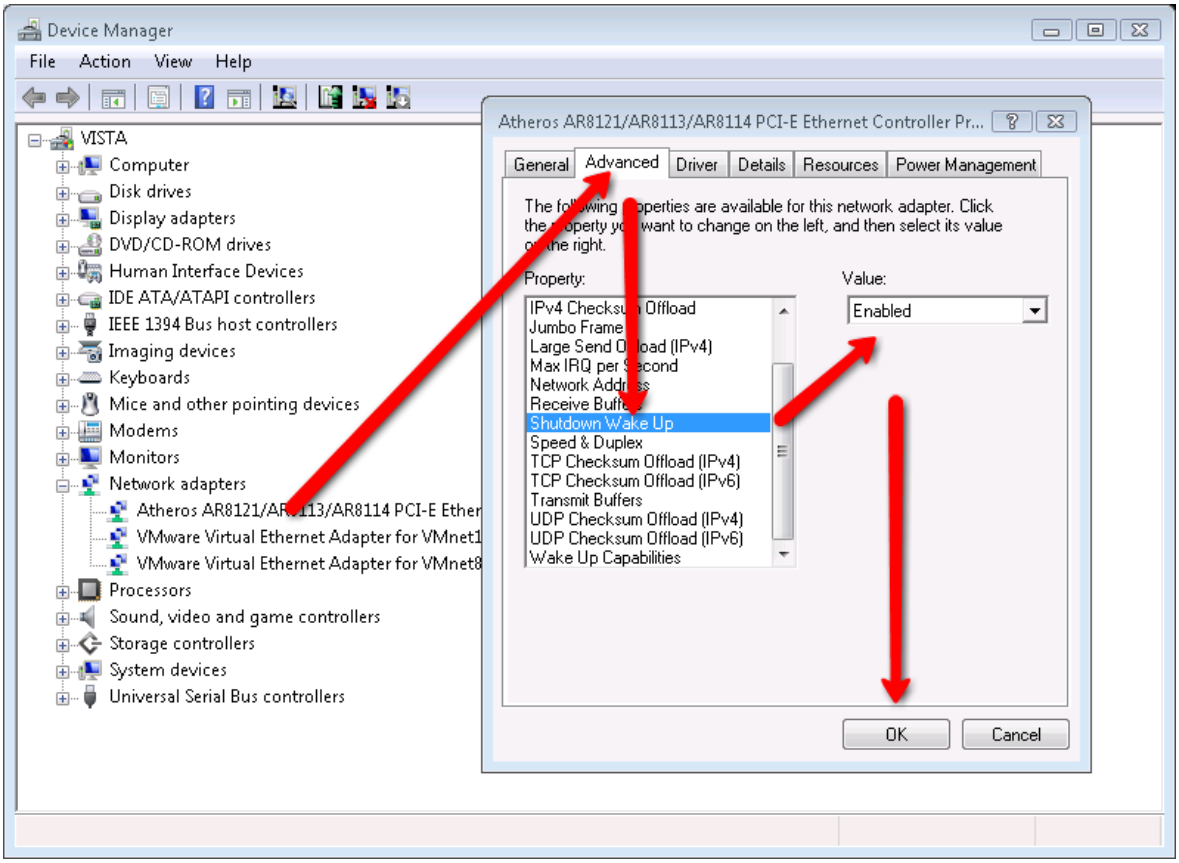
3.4.10 Wake On LAN

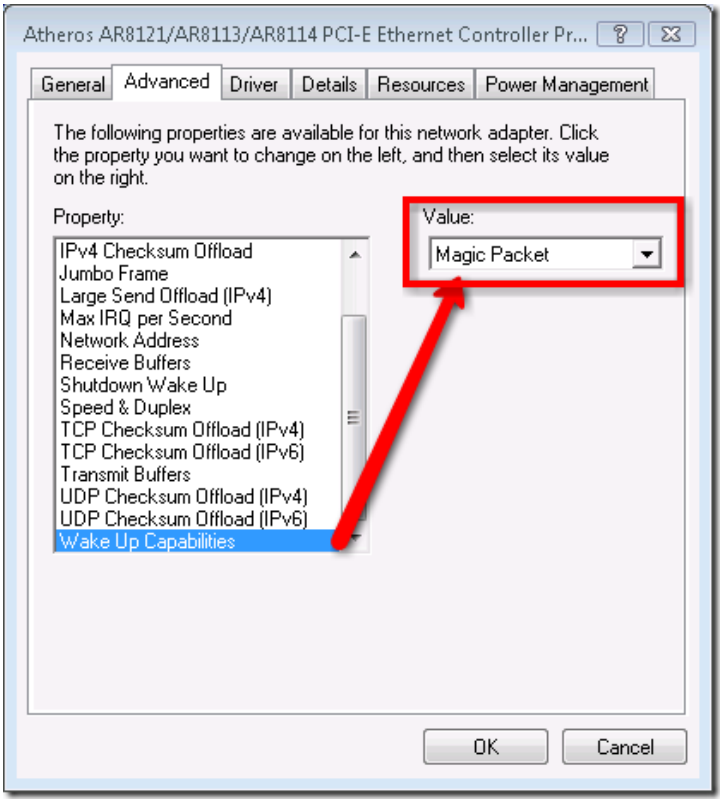
Wake On LAN to metoda zdalnego włączania komputerów. W celu wysłania pakietu potrzebny jest adres MAC urządzenia docelowego (w przypadku błędu pojawia się stosowny komunikat). Oprócz tego, konieczne jest skonfigurowanie urządzenia (opisane poniżej) i ewentualne przekierowanie portu na routerze, jeśli komputer będzie wybudzany w innej podsieci lub spoza NAT.

Ustawienia wybudzanego urządzenia

Konfiguracja zależy od konkretnego urządzenia. Przykładowe wymagania i ustawienia:

1. Aby możliwe było korzystanie z funkcji Wake On LAN, konieczny jest zasilacz ATX, przynajmniej 1A, +5Vsb.
2. Ustawienia BIOS-u:
   w zakładce Power (Management) lub Advanced włącz Wake On LAN - opcja może się różnie nazywać, np. Wake On LAN, MAC Resume From S3/S4, MACPME Power Up Control, Power On By Onboard LAN, Power Up By Onboard LAN, Resume by LAN, Resume By WOL, Resume on LAN, Resume on LAN/PME#, Wake on LAN from S5, Wake Up On LAN, WakeUp by Onboard LAN lub WOL (PME#) From Soft-Off.
3. Ustawienia karty sieciowej:
   a. Przejdź do ustawień karty sieciowej w Windows | Panel sterowania | Menadżer urządzeń.
   b. W zakładce "Zarządzanie energią" ustaw opcje tak, aby możliwe było wybudzanie komputera (nazwy opcji zależą od karty sieciowej, przykładowo "Zezwalaj temu urządzeniu na wyprowadzenie komputera ze stanu wstrzymania").
   c. W zakładce "Zaawansowane" włącz wybudzanie i Wake On LAN - opcje mogą się różnić w zależności od karty sieciowej, przykładowe ustawienia przedstawione są poniżej:

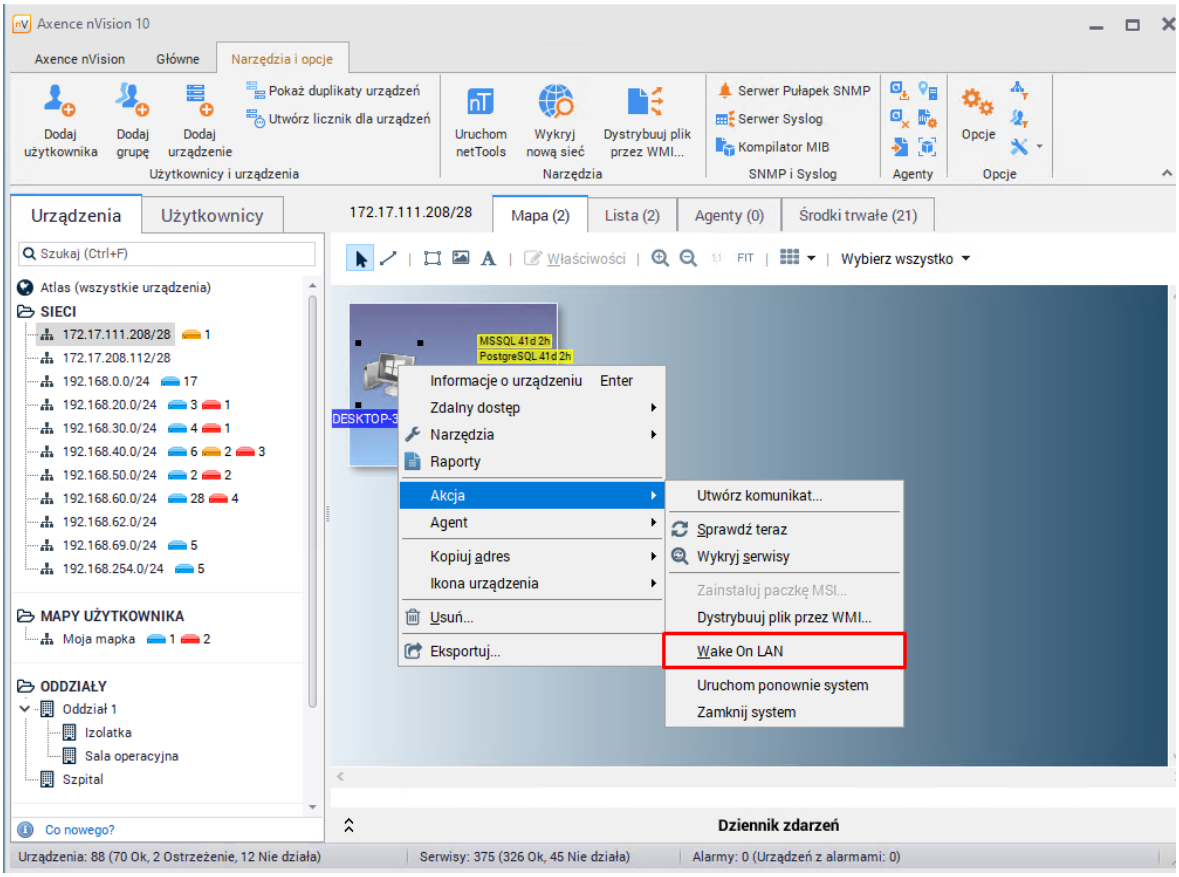




Wybudzanie urządzenia

Aby wybudzić monitorowane urządzenie, wykonaj jedno z poniższych:

1. W widoku mapy lub urządzeń w głównym oknie nVision kliknij prawym przyciskiem myszy na urządzeniu i wybierz opcję **Wake On LAN**.



2. W oknie informacji o urządzeniu, w zakładce **Ogólne**, kliknij prawym przyciskiem myszy na interfejsie, do którego ma być wysłany pakiet i wybierz opcję **Wake On LAN**.

Wake On LAN jako akcja

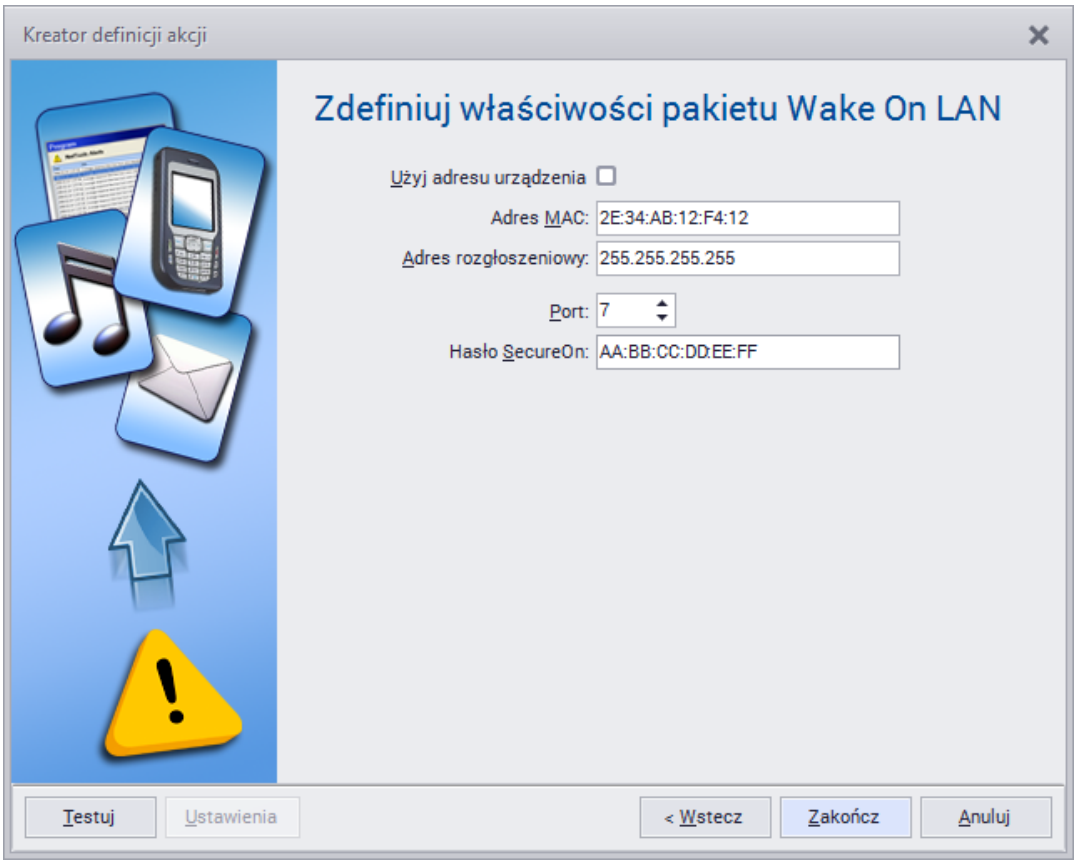
Aby zdefiniować Wake On LAN jako akcję:

1. Wybierz **Zarządzaj akcjami** z karty **Narzędzia i opcje** na wstążce.
2. W oknie Kreatora definicji akcji wpisz nazwę akcji i wybierz typ **Wyślij pakiet Wake On LAN**.
3. Jeśli chcesz użyć adresu hosta, na którym definiujesz akcję, zaznacz pole **Użyj adresu urządzenia** i przejdź do punktu 5. W przeciwnym razie konieczne jest zdefiniowanie hosta (punkt 4).
4. Podaj adres MAC urządzenia oraz jeden z następujących adresów docelowych pakietu Wake On LAN:
   a. adres rozgłoszeniowy: 255.255.255.255 (jeśli urządzenie znajduje się w tej samej sieci LAN),

b. adres rozgłoszeniowy podsieci (jeśli urządzenie znajduje się w innej sieci LAN – np. 192.168.0.255 w przypadku podsieci 192.168.0.1 o masce 255.255.255.0),

c. adres IP routera skonfigurowanego na przekierowanie pakietów (jeśli urządzenie znajduje się poza siecią LAN)

5. Podanie hasła SecureOn nie jest konieczne, jednak wymagają go niektóre karty sieciowe. Format hasła to sześć bajtów w reprezentacji szesnastkowej: AA:BB:CC:DD:EE:FF.



Część IV

4 Praca z atlasami, mapami i urządzeniami

4.1 Wprowadzenie

Atlas

Atlas to zbiór map sieci prezentujących monitorowane urządzenia oraz grupy użytkowników wraz ze zdefiniowanymi alarmami, zdarzeniami, stylami wizualizacji etc.

Drzewo atlasu

Drzewo atlasu przedstawia wszystkie dostępne mapy. Dostępnych jest wiele rodzajów map, które są szczegółowo opisane w rozdziale Rodzaje map. Drzewo atlasu umożliwia wybór mapy, która jest przedstawiona po prawej stronie, ustawienie właściwości danej mapy etc. Można zmieniać kolejność map w drzewie (Aby uzyskać więcej informacji, przejdź do rozdziału Zarządzanie mapami).

Mapy

Mapa to graficzny obraz sieci lub jej części. Mapy wizualizują urządzenia tworzące sieć. Jest wiele rodzajów map. Aby uzyskać więcej informacji, przejdź do rozdziału Rodzaje map.

Style

Wszystkie obiekty na mapie (oprócz tekstu) używają mechanizmu stylów. Styl decyduje o sposobie prezentacji obiektów. Definiuje on np. kolory, czcionki, ramki etc. Aby zmienić wygląd obiektu, podczas definiowania jego właściwości, należy wybrać preferowany styl. Aby uzyskać więcej informacji o stylach, przejdź do rozdziałów Style i Mapy.

Urządzenia

Urządzenie oznacza jakikolwiek rodzaj sprzętu fizycznego podłączonego do sieci. Może ono posiadać wiele adresów IP, a nVision może monitorować wszystkie serwisy na nim uruchomione na jakimkolwiek z jego adresów. Oznacza to, że urządzenie z wieloma adresami IP, takie jak routery lub serwery sieciowe, mogą być przedstawione w nVision jako jedna ikona (obiekt) i wszystkie ich interfejsy, adresy i serwisy będą monitorowane.

4.2 Okno informacji o urządzeniu

Aby zobaczyć informacje o urządzeniu, kliknij dwukrotnie ikonę urządzenia lub wybierz **Informacje o urządzeniu** z jej menu kontekstowego.

Ogólne

Zakładka przedstawia:

- podstawowe informacje o monitorowanym urządzeniu: nazwę, poziom istotności (ważność), oddział, typ,
- pole **Monitoruj tylko jeśli działa:** umożliwia ustawienie urządzenia "nadrzędnego" (urządzenie nie będzie monitorowane, alarmy nie będą generowane jeśli urządzenie "nadrzędne" nie działa),
- dodatkowe informacje w polach **info 1 / info 2**: pobierane są przez Agenta z opisu monitorowanego komputera oraz domeny,

- dodatkowe pole na notatki,
- listę wszystkich adresów i interfejsów dostępnych na danym urządzeniu.

Wydajność

Serwisy

nVision może monitorować serwisy ICMP, TCP i UDP. Możesz zobaczyć wszystkie monitorowane serwisy w tabeli, dostępnej na zakładce Serwisy. Dla każdego serwisu prezentowane są informacje o czasie odpowiedzi i żądaniach wysłanych/przyjętych. Po wybraniu jednego lub więcej serwisów, zobaczysz wykres prezentujący czas odpowiedzi oraz procent utraconych żądań/pakietów (w przypadku, gdy wybrany jest jeden serwis). Dane historyczne można zobaczyć dla wielu różnych okresów (np. z ostatnich 15 minut, godziny, dnia, tygodnia, miesiąca, czy z całego roku). Aby wybrać odpowiedni okres, kliknij odpowiednią ikonę na pasku narzędzi wykresu. Aby przewijać wykres do przodu i do tyłu, użyj ikon ze strzałkami znajdujących się na pasku narzędziowym wykresu. Aby uzyskać więcej informacji o serwisach, przejdź do rozdziału Monitorowanie serwisów.

Liczniki

nVision może monitorować wiele liczników wydajności (aby uzyskać pełną listę dostępnych liczników, przejdź do rozdziału Rodzaje liczników). Możesz zobaczyć wszystkie monitorowane liczniki, wyszczególnione w tabeli dostępnej na zakładce **Liczniki wydajności**. Dla każdego licznika prezentowane są dane o ostatniej i najmniejszej/największej/średniej wartości (oprócz licznika statusu urządzenia, który nie ma min/max/średnich wartości). Po wybraniu licznika, zobaczysz wykres pokazujący jego wartość. Możesz zobaczyć dane historyczne dla wielu okresów czasu (np. z ostatnich 15 minut, godziny, dnia, tygodnia, miesiąca, czy z całego roku). Aby przewijać wykres do tyłu i do przodu, użyj ikon ze strzałkami znajdujących się na pasku narzędziowym wykresu. Aby uzyskać więcej informacji o licznikach, przejdź do rozdziału Monitorowanie wydajności.

Użycie łącza

Zakładka prezentuje użycie łącza przez procesy, które pogrupowane zostały zgodnie z ustawieniami w opcjach nVision. Do monitorowania użycia łącza konieczne jest zainstalowanie Agenta i włączenie tej opcji w ustawieniach Agenta.

Zasoby

Sprzęt

W tej zakłade znajdują się informacje o konfiguracji sprzętowej monitorowanego przez Agenta komputera, lista podłączonych urządzeń oraz historia podłączeń oraz operacji na plikach na zewnętrznych nośnikach danych.

Oprogramowanie

Zakładka ta prezentuje wszystkie aplikacje zainstalowane na komputerach. Aby uzyskać więcej informacji, przejdź do rozdziału Inwentaryzacja sprzętu i oprogramowania.

Środki trwałe

Zakładka przedstawia środki trwałe dla danego urządzenia, umożliwia także zarządzanie wykrytymi

zdarzeniami. Aby dowiedzieć się więcej, przejdź do rozdziału Środki trwałe.

Pliki użytkowników

Prezentuje listę plików w określonym formacie przeskanowanych przez Agenta zgodnie z ustawieniami w profilu Agenta.

Menadżer plików

Pozwala na przenoszenie danych pomiędzy lokalnym komputerem (serwerem nVision), a stacją roboczą, którą zarządzamy

Historia

Zakładka prezentuje historię zmian w konfiguracji sprzętowej i programach zainstalowanych na urządzeniu. Wyświetlane są również informacje o adresie IP, z którego Agent połączył się z serwerem nVision. Jeśli jest to adres publiczny, dwukrotne kliknięcie wiersza otworzy nowe okno przeglądarki ze stroną www przedstawiającą szacunkową geolokalizację adresu.

SNMP

Przeglądarka SNMP

Jeśli urządzenie jest zarządzalne przez SNMP, dostępna będzie zakładka SNMP zawierająca przeglądarkę SNMP. Aby dane były odczytywane, skonfiguruj dane wspólnoty SNMP po kliknięciu linku **Konfiguruj dane logowania** na tej zakładce.

Mapowanie portów

Zakładka mapowanie portów przedstawia listę wszystkich urządzeń podłączonych do portu switch'a. Dane te widoczne są tylko wtedy, gdy nVision jest w stanie odczytać odpowiednie informacje SNMP z urządzenia (które są dostępne głównie na switch'ach)

Pułapki SNMP

Zakładka Pułapki SNMP przedstawia listę wszystkich wygenerowanych przez urządzenie pułapek SNMP.

Windows

Informacje systemowe

Informacje o systemie operacyjnym zebrane w ramach modułu Inwentaryzacji.

Usługi Windows

Prezentuje listę usług sytemu Windows monitorowanych na danym urządzeniu.
Aby monitorować przez WMI, konieczne jest właściwe skonfigurowanie danych logowania w oknieinformacji o urządzeniu oraz udostępnienie WMI na zdalnym urządzeniu. Aby uzyskać więcej informacji, przejdź do rozdziału Wymagania i konfiguracja.

Aby monitorować usługi Windows bez otwierania zdalnego dostępu do WMI, należy zainstalować Agenta.

Dziennik zdarzeń Windows

Pokazuje listę zdarzeń zapisanych w Dzienniku Windows, monitorowanych wg określonych kryteriów na danym urządzeniu.
Aby monitorować przez WMI, konieczne jest właściwe skonfigurowanie danych logowania w oknie informacji o urządzeniu oraz udostępnienie WMI na zdalnym urządzeniu. Aby uzyskać więcej informacji, przejdź do rozdziału Wymagania i konfiguracja. Aby monitorować usługi Windows bez otwierania zdalnego dostępu do WMI, należy zainstalować Agenta.

Procesy

Pokazuje listę aktualnie działających procesach na danym urządzeniu.

Zdalne wykonywanie poleceń

Pozwala na zdalne uruchomienie komendy wiesza poleceń na urządzeniu. Funkcja ta może być zastosowana do kilku urządzeń jednoczesnie.

Zdarzenia

Dziennik zdarzeń

Jest to lista wszystkich zainicjowanych alarmów, wraz z rejestrem akcji wykonanych dla każdego alarmu. Możesz zobaczyć alarmy posortowane według wielu pól, a także przefiltrować je tak, aby zobaczyć jedynie te, które Cię interesują. Kliknięcie linku **Konfiguruj alarmy urządzenia** pozwoli na utworzenie indywidualnych alarmów.

Syslog

Zakładka syslog przedstawia listę wszystkich wygenerowanych przez urządzenie komunikatów Syslog.

4.3 Mapy

4.3.1 Ogólne informacje

Mapa to graficzny obraz sieci lub jej części. Mapy przedstawiają ikony, połączenia pomiędzy nimi i trzy grupy obiektów statycznych: kształty, obrazki i tekst. Pełna lista obiektów jest opisana w rozdziale Obiekty na mapie.

Dostępne są trzy rodzaje map: mapy sieci, mapy inteligentne oraz mapy użytkownika - zagadnienie szerzej opisane w rozdziale Rodzaje map.

Style

Wszystkie obiekty na mapie (oprócz tekstu) używają mechanizmu stylów. Styl decyduje o sposobie prezentacji obiektów. Definiuje on np. kolory, czcionki, ramki etc. Aby zmienić wygląd obiektów, podczas definiowania właściwości obiektów, należy wybrać preferowany styl.

Wszystkie nowe obiekty są tworzone w stylu domyślnym. Styl domyślny oznacza, że obiekty będą wykorzystywały domyślny styl mapy. Ustawionym domyślnym stylem mapy może być dowolny wybrany styl lub domyślny styl atlasu. Atlas ma zawsze ustawiony styl domyślny. Przy pierwszym uruchomieniu programu, wszystkie obiekty użyją domyślnych stylów atlasu. Style te mogą być później zmienione. Aby uzyskać więcej informacji o stylach, przejdź do rozdziału Zarządzanie stylami.

4.3.2 Rodzaje map

W nVision dostępne są 3 rodzaje map. Rozdział ten przedstawia charakterystykę każdego z nich.

Rodzaj mapy	Opis	Możliwe operacje
Mapa sieci	Mapa stworzona przez program jako reprezentacja wykrytej sieci IP. nVision może regularnie skanować taką sieć i dodawać nowe urządzenia.	• Można zmienić nazwę mapy, ale nawet po takiej zmianie mapa w dalszym ciągu przedstawia tą samą sieć. • Usuwanie - usunięcie mapy sieci spowoduje także usunięcie wszystkich urządzeń należących do danej sieci. • Wszelkie inne operacje są dostępne bez ograniczeń.
Mapa użytkownika	Jest to mapa stworzona przez użytkownika. Przedstawia wszelkie urządzenia skopiowane lub przeniesione z jakiejkolwiek innej mapy.	• Wszystkie operacje są dostępne bez ograniczeń.
Mapa inteligentna	Na mapie inteligentnej grupowane są urządzenia, które w danej chwili spełniają określone warunki. Działanie inteligentnych map opiera się na zdefiniowanych przez użytkownika filtrach - **mapa tworzona jest dynamicznie**.	• Można zmienić nazwę mapy, ale nawet po takiej zmianie mapa w dalszym ciągu przedstawia tą samą sieć. • Nie można usuwać ani rozmieszczać ikon urządzeń.

4.3.3 Obiekty mapy

Mapa może zawierać ikony, połączenia pomiędzy nimi i trzy rodzaje obiektów statycznych: kształty, obrazki i teksty. Oto pełna lista obiektów na mapie:

Obiekty mapy	Opis
Ikony	Urządzenia są przedstawiane jako ikony. Ikony pokazują stan urządzenia - aby dowiedzieć się więcej o wizualizacji stanu urządzeń, przejdź do rozdziału Wizualizacja urządzeń.
Linie	Ikony mogą być połączone ze sobą, w celu zobrazowania logicznych lub fizycznych połączeń pomiędzy urządzeniami.
Kształty	Obiekty w tle, wykorzystywane do grupowania ikon.
Obrazy	Podobne do kształtów, ale przedstawiają zawartość określonego pliku graficznego.
Teksty	Teksty można umieszczać w dowolnych miejscach mapy.

Hierarchia obiektów

Obiekty mają swoją hierarchię na mapie. Oznacza to, że pewne obiekty są rysowane na innych. Przykładowo, ikony są zawsze rysowane na innych rodzajach obiektów. Jednak hierarchię obiektów jednego rodzaju można zmienić. Można przenieść dane obiekty do przodu lub do tyłu, co zmienia sposób rysowania obiektów nachodzących na siebie.

4.3.4 Zarządzanie mapami

Rozdział ten opisuje wszystkie aspekty związane z zarządzaniem mapami.

Tworzenie nowej mapy

1. W drzewie atlasu wybierz mapę lub katalog, pod którym chcesz utworzyć nową mapę. Możesz wybrać grupę Map Użytkownika.
2. Wybierz **Nowy \ Mapa** z menu kontekstowego.

Uwaga

- Nowe mapy mogą być utworzone jedynie w grupie Map Użytkownika.

Edytowanie właściwości mapy

1. Wybierz mapę
2. Wybierz **Właściwości** z menu kontekstowego.
3. Ustaw właściwości mapy zgodnie z opisem w tabeli poniżej.
4. Możesz także otworzyć okno zarządzania alarmami dla tej mapy - kliknij link pod nazwą **Zarządzaj alarmami**, znajdujący się na dole okna.

Właściwość	Opis
Nazwa	Nazwa mapy
Sieć	Sieć, którą przedstawia mapa sieci (aby dowiedzieć się, czym jest mapa sieci, przejdź do rozdziału Rodzaje map). Jest to pole tylko do odczytu.
Domyślne style map - decydują o sposobie wizualizacji map i urządzeń. Aby dowiedzieć się więcej o stylach, przejdź do rozdziału Style.	
Wizualizacja urządzeń	Domyślny styl wizualizacji ikon.
Styl kształtów	Domyślny styl kształtów.
Styl linii	Domyślny styl linii.

Usuwanie mapy

1. Wybierz mapę.
2. Wybierz **Usuń** z menu kontekstowego.

4.3.5 Praca z mapą

Rozdział ten opisuje wszystkie narzędzia potrzebne do pracy z mapami.

Narzędzia

Narzędzia są dostępne na pasku narzędziowym mapy, znajdującym się zazwyczaj po lewej stronie okna mapy (pasek narzędziowy mapy może być przesunięty na dowolny brzeg map). Narzędzia pozwalają wybierać obiekty na mapie, łączyć ikony i tworzyć obiekty tła, takie jak kształty, obrazki i teksty.

Narzędzie - zaznaczenie

Zaznaczenie jest narzędziem domyślnym. Pozwala wybierać obiekty na mapie, przesuwać je, porządkować i wykonywać inne określone akcje, takie jak otwieranie okna stanu urządzenia czy właściwości.

Aby użyć narzędzia wyboru, kliknij ikonę  na pasku narzędziowym mapy. Narzędzie to będzie aktywne do czasu wybrania innego narzędzia.

Narzędzie - łączenie ikon

Narzędzie to umożliwia łączenie ikon - np. narysowanie graficznych połączeń pomiędzy ikonami urządzeń na mapie.

1. Aby korzystać z narzędzia łączenia ikon, kliknij ikonę  na pasku narzędziowym mapy. Narzędzie to będzie aktywne do czasu wybrania innego narzędzia.
2. Aby połączyć dwie ikony, po prostu kliknij je kolejno, czyli:
   - Kliknij jedną z ikon, które chcesz połączyć. Pojawi się linia łącząca, wskazując, że teraz możesz kliknąć następną ikonę, którą chcesz połączyć.
   - Kliknij kolejną ikonę. W ten sposób pomiędzy tymi dwoma ikonami pojawi się połączenie.
3. Teraz możesz powtórzyć kroki 2-3, aby łączyć kolejne pary ikon.

Narzędzia - tworzenie kształtów

Narzędzie to umożliwia tworzenie różnych kształtów na mapie (graficznych obiektów w tle - prostokątów, elips, etc.).

1. Kliknij ikonę  na pasku narzędziowym mapy. Narzędzie jest aktywne do momentu utworzenia kształtu. Później aktywne będzie narzędzie wyboru.
2. Kliknij i przytrzymaj lewym przyciskiem myszy miejsce, w którym chcesz otrzymać lewy górny róg danego kształtu, a następnie przeciągnij do miejsca, w którym ma być jego prawy dolny róg. Puść przycisk.

Narzędzia - tworzenie obrazów

Narzędzie to umożliwia tworzenie obrazów na mapie. Po utworzeniu obrazu, należy go ustawić, otwierając okno właściwości i wybierając plik, który powinien być pokazany.

1. Kliknij ikonę  na pasku narzędziowym mapy. Narzędzie jest aktywne do momentu utworzenia obrazu. Później aktywne będzie narzędzie wyboru.
2. Kliknij i przytrzymaj lewym przyciskiem myszy miejsce, w którym chcesz otrzymać lewy górny róg obrazu, a następnie przeciągnij do miejsca, w którym ma być jego prawy dolny róg. Puść przycisk.
3. Pokaże się okno właściwości obrazu. Należy wybrać plik graficzny i ustawić opcje, aby we właściwy sposób utworzyć obraz.

Narzędzia - tworzenie tekstów

Narzędzie to umożliwia tworzenie tekstów na mapie. Po utworzeniu tekstu, należy go zdefiniować, wybierając czcionkę oraz wprowadzając tekst, który ma zostać pokazany.

1. Kliknij ikonę  na pasku narzędziowym mapy. Narzędzie jest aktywne do momentu utworzenia tekstu. Później aktywne będzie narzędzie wyboru.
2. Kliknij w miejscu, w którym chcesz wprowadzić tekst.
3. Pokaże się okno właściwości tekstu. Teraz należy wprowadzić tekst i ustawić opcje, aby we właściwy sposób utworzyć tekst.

Praca na obiektach na mapie

Kopiowanie obiektów na inną mapę

1. Wybierz obiekt lub obiekty.
2. Wybierz **Skopiuj do...** z menu kontekstowego.
   Otworzy się okno wyboru mapy.
3. Wybierz mapę, na którą chcesz skopiować wybrany(e) obiekt(y).

Usuwanie obiektów

1. Wybierz obiekt lub obiekty.
2. Wybierz **Usuń** z menu kontekstowego.

Zmienianie kolejności obiektów (przesuwanie ich na wierzch / na spód)

Możesz zmienić kolejność obiektów tego samego rodzaju - sposób, w jaki są narysowane i w jaki zachodzą na siebie. Kolejność obiektów różnego rodzaju jest stała (Aby uzyskać więcej informacji, przejdź do rozdziału Obiekty na mapie).

- Aby wyświetlić obiekt z przodu, na jakimkolwiek innym obiekcie, wybierz **Pozycja | Na wierzchu** z menu kontekstowego.
- Aby przesunąć dany obiekt pod pozostałe obiekty, wybierz **Pozycja | Na spodzie** z menu kontekstowego.

Inne operacje

Automatyczny układ mapy

Są dwa sposoby, aby automatycznie ułożyć mapę: za pomocą funkcji układu mapy i za pomocą asystenta układu mapy.

Aranżuj wszystko

Funkcję tę najlepiej stosować przy mapie sieci lub mapie użytkownika, szczególnie, gdy urządzenia nie są za sobą połączone. Układa ona ikony w kilka rzędów.

1. Kliknij ikonę  , znajdującą się na pasku narzędziowym mapy i wybierz z menu **Aranżuj wszystko**.
2. Określ, jak ma być mapa ułożona i kliknij OK.

Zaznaczenie opcji **Połączenia z mapowania portów** spowoduje ułożenie ikon urządzeń łącząc je z ikonami switchy, do których są one podłączone (aby ta opcja zadziałała, we właściwościach ikony switcha musi być włączone mapowanie portów.)

Aranżuj połączone ikony

Aby prawidłowo ustawić układ mapy routingu (lub jakiejkolwiek innej mapy, na której wszystkie urządzenia są połączone liniami), ikony nie mogą być ułożone rzędami, gdyż spowodowałoby to nieczytelność mapy - połączenia ikon nakładałyby się na siebie. Dlatego należy użyć Asystenta układu mapy, który ułoży całą mapę tak, aby uniknąć przecinania się połączeń i aby była ona tak czytelna, jak to jest tylko możliwe.

1. Kliknij strzałką ikonę  , znajdującą się na pasku narzędziowym mapy i wybierz z menu opcję **Aranżuj połączone ikony**.
2. Opcja zostanie włączona i rozpocznie się układanie mapy. Można ingerować w proces układania, aby dostosować go do własnych potrzeb. Można przesuwać ikony i dodawać/usuwać połączenia pomiędzy nimi.

Powiększanie - zmienianie skali mapy

Można dostosować skalę, w której jest prezentowana mapa. Domyślna skala to 100% i można ją ustawić w każdej chwili, klikając ikonę **1:1** .

Powiększanie

Aby powiększyć mapę, kliknij ikonę  .

Pomniejszanie

Aby pomniejszyć mapę, kliknij ikonę  .

Dostosowanie do wielkości mapy

Aby skala mapa była automatycznie dostosowana do wielkości mapy, kliknij ikonę opisaną **FIT**. nVision pokaże całą mapę w największej możliwej skali.

Blokowanie mapy

Gdy układanie mapy jest już zakończone i chcesz mieć pewność, że nic nie zostanie zmienione przez pomyłkę, możesz zablokować mapę używając przełącznika **Edycja mapy** w prawym górnym rogu ekranu. Na zablokowanej mapie nie można przesuwać obiektów, ani zmieniać ich rozmiarów, w dalszym ciągu można jednak edytować właściwości urządzeń.

4.3.6 Statyczne obiekty na mapie - właściwości

Rozdział ten poświęcony jest właściwościom statycznych obiektów na mapie. Aby uzyskać więcej informacji o obiektach na mapie, przejdź do rozdziału Obiekty na mapie, a jeśli chcesz się dowiedzieć więcej o tworzeniu obiektów, przejdź do rozdziału Praca z mapą.

Linie

Ikony mogą być ze sobą połączone liniami, aby pokazać logiczne i fizyczne połączenia między urządzeniami.

1. Kliknij dwukrotnie w linię lub wybierz **Właściwości** z jej menu kontekstowego.
2. Ustaw właściwości zgodnie z opisem w tabeli poniżej.

Właściwość	Opis
Opis	Opis, który będzie pokazany nad linią łączącą.
Styl	Styl, w którym będzie narysowana linia. Aby uzyskać więcej informacji o stylach, przejdź do rozdziału Style.

Kształt

Obiekt w tle, używany do grupowania ikon.

1. Kliknij dwukrotnie w kształt lub wybierz **Właściwości** z jego menu kontekstowego.
2. Ustaw właściwości zgodnie z opisem w tabeli poniżej.

Właściwość	Opis
Tekst	Tekst, który pojawi się na kształcie.

Właściwość	Opis
Styl	Styl, w którym będzie narysowany kształt. Aby uzyskać więcej informacji o stylach, przejdź do rozdziału Style.

Obraz

Podobny do kształtu, ale jego treścią jest plik graficzny.

1. Kliknij dwukrotnie w obraz lub wybierz **Właściwości** z jego menu kontekstowego.
2. Ustaw właściwości zgodnie z opisem w tabeli poniżej.

Właściwość	Opis
Nazwa pliku	Nazwa pliku graficznego. Wprowadź ją lub wybierz, klikając ikonę ... .
Widok	Decyduje o rozmiarze obrazu: • Normalny - Rozmiar obrazu nie jest zmieniony, ale przy próbach zmniejszenia, widoczna pozostaje jedynie jego część (jeśli obraz jest większy od obiektu, będzie on przycięty). • Rozciągnięcie - Obraz będzie dopasowany tak, aby odpowiadał rozmiarowi obiektu.. • Sąsiadująco - kopie obrazu w skali 1:1 będą wyświetlane sąsiadująco na całym obszarze.
Rozmiar rzeczywisty	Obraz widoczny w całości, bez możliwości zmiany jego rozmiaru.
Stała proporcja	Podczas zmiany rozmiaru obrazu, współczynnik proporcji jest zachowany.
Transparentność	Zastosuj, jeśli obraz ma warstwę przezroczystości.
Przezroczystość	Decyduje o stopniu przezroczystości całego obrazu.

Tekst

Tekst, który można umieścić w dowolnym miejscu na mapie.

1. Kliknij dwukrotnie w tekst lub wybierz **Właściwości** z jego menu kontekstowego.
2. Ustaw właściwości zgodnie z opisem w tabeli poniżej.

Właściwość	Opis
Tekst	Tekst na mapie.
Nazwa czcionki	Czcionka tekstu.

Właściwość	Opis
Rozmiar	Rozmiar czcionki.
Kolor czcionki	Kolor tekstu.
Pochylenie	Pochylenie tekstu.
Cień	Cieniowanie tekstu.

Tło

1. Wybierz **Tło** z menu kontekstowego.
2. Wybierz rodzaj tła i ustaw jego właściwości zgodnie z opisem w tabeli poniżej.

Właściwość	Opis
Gradient	Wybierz kolor początkowy i końcowy oraz kierunek wypełnienia.
Kolor wypełnienia	Wybierz kolor.
Mapa	Wybierz mapę, która będzie pokazana w tle.
Tekstura	Wybierz teksturę.
Obraz	Wprowadź nazwę pliku graficznego lub wybierz go, klikając ikonę ... . Ustaw tryb położenia obrazu: • Normalny - Obraz znajduje się w lewym górnym rogu. • Do środka - Obraz położony centralne, na środku mapy. • Rozciągnięcie - Obraz będzie dopasowany tak, aby odpowiadał rozmiarowi mapy. • Sąsiadująco - kopie obrazu w skali 1:1 będą wyświetlane sąsiadująco na całej mapie.

4.4 Urządzenia

4.4.1 Ogólne informacje

Urządzenia są przedstawione na mapie za pomocą ikon. To samo urządzenie może być pokazane jako ikona na nieograniczonej liczbie map.

Właściwości urządzenia i informacje o urządzeniu

Istnieją dwa główne okna dotyczące urządzenia: właściwości urządzenia i informacje o urządzeniu. W oknie właściwości urządzenia można ustawić jego właściwości, opcje monitorowania i alarmowania. Okno informacji o urządzeniu prezentuje wszystkie dane zgromadzone poprzez monitorowanie. Znajdują się tam informacje i wykresy oparte na danych SNMP (dla urządzeń zarządzalnych przez SNMP), dotyczące serwisów i liczników wydajności.

Jak znaleźć urządzenie / użytkownika?

Można łatwo znaleźć urządzenie przez wyszukiwarkę znajdującą się na głównym pasku narzędziowym w prawej części głównego okna nVision oraz w oknie **Informacje o urządzeniu**. Poniżej znajduje się lista właściwości branych pod uwagę przy wyszukiwaniu:

- Nazwa
- Adresy IP, DNS i MAC każdego interfejsu
- Info1 i Info2

Podczas wpisywania kolejnych znaków w polu szukania następuje odfiltrowanie wyników zawierających wprowadzany ciąg znaków.

Aby wyszukać urządzenie w którym przynajmniej jedno z wyżej wymienionych pól zawiera:

- ciąg kończący się wpisanymi znakami - należy zakończyć go znakiem | ,
  np.:
  54|
- ciąg zaczynający się od wpisanych znaków - należy poprzedzić go znakiem | ,
  np.:
  |AABBCC
- dokładnie wprowadzony ciąg znaków - należy poprzedzić jak i zakończyć go znakiem | ,
  np.:
  |biuro-pc|

Uwaga: identyfikacja urządzenia po nazwie DNS jest włączona tylko, gdy odpytanie IP - DNS daje ten sam rezultat w obu kierunkach.

4.4.2 Wizualizacja urządzeń

Ikony prezentują wiele informacji dotyczących stanu urządzeń. Dane te pomagają dokonać szybkiej oceny stanu całej sieci i znaleźć problematyczne urządzenia.

Przykład ikon komputera

Ikona komputera prezentuje szeroki zakres informacji, co prezentują poniższe przykłady:

- Typ komputera: Windows XP
- Czas odpowiedzi podstawowego serwisu (zwykle PING) to 10ms
- Status komputera <Ostrzeżenie> (żółta ikona) ze względu na niedziałający od 4min 1s serwis HTTP
- Ten komputer jest zarządzalny przez SNMP

- Typ komputera: serwer Linux

- Status komputera <Nie działa> (czerwona ikona) od 1 dnia 2h
- Aktualnie otwarte są (niezakończone) 3 alarmy.

Opcje wizualizacji

Poniższa tabela wyszczególnia wszystkie informacje, jakie mogą być przedstawione graficznie za pomocą ikony urządzenia.

Nazwa		Opis
Ikona z podpisem, status urządzenia: Działa		Podstawowa forma ikony. Przedstawia rodzaj urządzenia i nazwę lub adres urządzenia w podpisie.
Stan urządzenia: Nie działa		Ikona jest zaznaczona na czerwono, a czas niedziałania urządzenia jest określony na górze ikony. Aby uzyskać więcej informacji o stanie urządzenia, przejdź do rozdziału Zdarzenia.
Status urządzenia: Ostrzeżenie		Ikona jest zaznaczona na żółto. Oznacza to, że co najmniej jeden serwis nie działa lub zainicjowano alarm ostrzegawczy na tym urządzeniu. Aby uzyskać więcej informacji o stanie urządzenia, przejdź do rozdziału Zdarzenia.
Status urządzenia: Archiwalny		Ikona jest zaznaczona na szaro. Oznacza to, że dane Agenta na danym urządzeniu zostały zarchiwizowane. Aby dowiedzieć się więcej, przejdź do rozdziału Archiwizowanie Agentów.
Serwis(y) nie odpowiada(ją)		Na górze ikony wyświetla się nazwa problematycznego serwisu oraz czas trwania usterki.
Czas odpowiedzi wybranego serwisu		Na dole ikony wyświetlony jest ostatni lub średni czas odpowiedzi wybranego serwisu. Zwykle jest to średni czas odpowiedzi PING. Tło napisu zmienia kolor w zależności od wydajności serwisu.
Alarmy		Ikona ta znajduje się po prawej stronie ikony urządzenia: wskazuje niepotwierdzone alarmy zainicjowane na danym urządzeniu.
Zarządzalność przez SNMP		Ikona ta znajduje się po prawej stornie ikony urządzenia i wskazuje, że jest ono zarządzalne przez SNMP.
Wykres wydajności		Można zobaczyć maksymalnie 6 słupków wydajności, które przedstawiają czas odpowiedzi serwisu lub liczniki wydajności.

4.4.3 Zarządzanie urządzeniami

Rozdział ten opisuje różne aspekty zarządzania urządzeniami i ich serwisami.

Ustawianie właściwości urządzeń

1. Wybierz **Informacje o urządzeniu** z menu kontekstowego ikony.

2. Ustaw właściwości urządzenia zgodnie z opisem w rozdziale Okno informacji o urządzeniu.

Dodawanie urządzeń

1. Wybierz **Dodaj urządzeniu** z kart **Narzędzia i opcje** na wstążce.
2. Wprowadź adres DNS lub IP urządzenia i maskę.
3. Można także ustawić rodzaj urządzenia i opcje ważności.

Usuwanie ikon urządzeń

1. Wybierz **Usuń** z menu kontekstowego ikony.
2. Potwierdź usunięcie. Podczas usuwania ostatniej ikony określonego urządzenia, usunięte zostanie całe urządzenie wraz z wszystkimi jego danymi. Można więc bezpiecznie usuwać ikony z map użytkownika, jeśli ikony tych urządzeń w dalszym ciągu znajdują się na mapach sieciowych.

Pokazywanie okna informacji o urządzeniu

1. Wybierz **Informacje o urządzeniu** z menu kontekstowego ikony lub dwukrotnie kliknij ikonę.
2. Zobaczysz okno informacji o urządzeniu - opis informacji prezentowanych w tym oknie znajduje się w rozdziale Okno informacji o urządzeniu.
3. Możesz zostawić to okno na pulpicie i dalej pracować z programem. Informacje przedstawione w tym oknie będą automatycznie odświeżane, aby pokazywać zmiany i stan urządzenia.
4. Można otworzyć nieograniczoną liczbę okien informacji o urządzeniu.

Zarządzanie serwisami i licznikami urządzeń

Zarządzanie serwisami

Aby uzyskać więcej informacji o serwisach, przejdź do rozdziału Monitorowanie serwisów..

Zarządzanie licznikami wydajności

Aby uzyskać więcej informacji o licznikach wydajności, przejdź do rozdziału Monitorowanie wydajności.

4.5 Style

4.5.1 Ogólne informacje

Style definiują sposób wizualizacji map. Rozdział ten opisuje domyślne style i sposób definiowania styli dla różnych obiektów. Aby zapoznać się z informacjami o tworzeniu i modyfikowaniu styli, przejdź do rozdziału Zarządzanie stylami.

Style domyślne

Domyślne style atlasu

Domyślne style atlasu zdefiniowane są we właściwościach atlasu. Style te używane są przez wszystkie nowo utworzone obiekty oraz te, które mają sty zdefiniowany jako <domyślny> (jednak mapa zawierająca te obiekty może nadpisywać styl atlasu). Po utworzeniu mapy jej style oraz styl wszystkich jej obiektów przyjmują wartość <domyślny>, w związku z czym zastosowane będą style zdefiniowane dla atlasu. Zmiana stylu we właściwościach atlasu spowoduje zmianę stylów takich obiektów.

Aby zmienić domyślne style atlasu, użyj okna właściwości atlasu.

Style domyślne mapy

Mapa - podobnie jak atlas - posiada swoje domyślne style. Za ich pomocą można nadpisać style globalne. Jeśli ustawimy styl <domyślny>, wtedy styl zdefiniowany dla atlasu będzie miał zastosowanie.

Styl <domyślny> w tym przypadku oznacza, iż mapa używa stylu zdefiniowanego we właściwościach atlasu. Można to traktować jako referencję do stylu atlasu. Dlatego styl <domyślny> nie może być modyfikowany lub usunięty, ponieważ tylko wskazuje na jakiś inny.

Style obiektu mapy

Styl wizualizacji urządzenia

Za pomocą stylu wizualizacji definiuje się sposób prezentacji urządzenia na mapie. Można wybrać informacje, jakie wyświetlane są na ikonie: czas niedziałania, informacja o niedziałających serwisach, czas ostatniej odpowiedzi, wskaźniki SNMP i alarmów, itp.

Styl kształtu

Styl kształtu określa wygląd obiektu kształt (obiekt tła mapy): ramkę, kolory, itp.

Styl linii

Styl ten definiuje właściwości graficzne linii łączącej dwie ikony.

4.5.2 Definiowanie stylów

Rozdział ten opisuje właściwości poszczególnych typów stylów. Aby zapoznać się z informacjami o tworzeniu i modyfikowaniu styli, przejdź do rozdziału Zarządzanie stylami.

Styl wizualizacji urządzenia

Styl ten definiuje sposób prezentacji ikony urządzenia na mapie. Poniższa tabela opisuje właściwości stylu.

Właściwość	Opis
Nazwa	Nazwa stylu

Właściwość	Opis
Po zmianie stanu migotaj	Czas migania ikony w razie zmiany stanu urządzania. Miganie pozwala na łatwe lokalizowanie tych urządzeń, które zmieniły stan.
Podpis ikony	Definiuje tekst znajdujący się w podpisie ikony.
Podpis przezroczysty	Podpis ikony będzie przezroczysty po włączeniu tej opcji.
Czas niedziałania urządzenia i serwisu	Po włączeniu tej opcji na ikonach urządzeń o stanie <Nie działa> będzie wyświetlony czas trwania takiego stanu. Jeśli urządzenie działa, jednak niektóre serwisy nie odpowiadają, wtedy zobaczysz informację o tych serwisach.
Czas odpowiedzi serwisu wiodącego	Opcja ta określa, czy wyświetlać czas odpowiedzi wiodącego serwisu.
Zarządzalność SNMP	Jeśli urządzenie jest zarządzalne przez SNMP, ikona SNMP wyświetli się po prawej stronie ikony urządzenia.
Ostrzeżenie o alarmie	Jeśli urządzenie ma niepotwierdzone alarmy, wtedy po prawej stronie wyświetli się ikona ⚠ - wraz z liczbą alarmów.
Agent zainstalowany	Jeżeli Agent jest zainstalowany na urządzeniu, to po prawej stronie wyświetlona będzie ikona .

Styl kształtu

Styl kształtu określa wygląd obiektu kształt (obiekt tła mapy): ramkę, kolory, itp.

Właściwość	Opis
Nazwa	Nazwa stylu
Typ	Typ kształtu. Dostępne są 4 typy: prostokąt, prostokąt zaokrąglony, elipsa i gwiazda.
Czcionka	Nazwa czcionki napisu.
Kolor i rozmiar czcionki	Kolor i rozmiar czcionki napisu.
Tło	• Jednolite - tło kształtu ma wybrany kolor. • Gradient - tło to przejście tonalne o określonych kolorach i kierunku.
Ramka	• Kolor - kolor ramki. • Grubość - grubość ramki.
Przezroczystość	Określa przezroczystość kształtu.
Cień	Definiuje rozmiar cienia.

Styl linii

Styl ten definiuje właściwości graficzne linii łączącej dwie ikony.

Właściwość	Opis
Nazwa	Nazwa stylu
Grubość	Grubość linii
Kolor	Kolor linii
Typ	• Prosta - linia prosta • Łamana - linia łamana
Czcionka	Wybierz czcionkę.
Rozmiar i kolor	Rozmiar i kolor czcionki.
Pokaż podpis na linii	Jeżeli opcja jest zaznaczona, podpis będzie pokazywany na linii.

4.5.3 Zarządzanie stylami

Wszystkie obiekty na mapie (oprócz tekstu) używają mechanizmu styli. Determinują one wygląd obiektu. Na przykład określają kolor, czcionkę, ramki, itp. Aby zmienić wygląd obiektu należy zmienić jego styl w oknie właściwości.

Okno zarządzania stylami

1. Wybierz **Zarządzaj stylami** z karty **Narzędzia i opcje** na wstążce.
2. Wybierz typ stylów jakimi chcesz zarządzać (urządzenie, kształt lub linia) w pasku nawigacyjnym po prawej stronie.

Tworzenie nowego stylu

1. Otwórz okno zarządzania stylami
2. Kliknij ikonę  .
3. Zdefiniuj styl zgodnie z informacją dostępną w rozdziale Definiowanie stylów.

Edycja stylów

1. Otwórz okno zarządzania stylami
2. Zaznacz styl i kliknij ikonę  .
3. Zmień właściwości stylu zgodnie z informacją dostępną w rozdziale Definiowanie stylów.

Usuwanie stylu

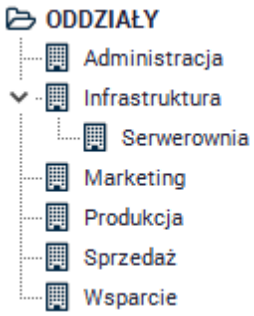
1. Otwórz okno zarządzania stylami.
2. Zaznacz styl i kliknij ikonę .

4.6 Oddziały

4.6.1 Ogólne informacje

Oddziały umożliwiają odzwierciedlenie w nVision rzeczywistej struktury monitorowanej grupy komputerów. Dzięki temu łatwiejsze jest przeglądanie, zarządzanie i tworzenie raportów dotyczących wybranych urządzeń.

Lista oddziałów wyświetlana jest w lewej części okna programu, pod sieciami i mapami użytkownika. Ma ona strukturę hierarchiczną, stąd możliwe jest reprezentowanie relacji zawierania się oddziałów (bycia pododdziałem). Przykładowa hierarchia została przedstawiona na rysunku poniżej.



Powiązane tematy

Tworzenie struktury oddziałów

Dodawanie urządzeń do oddziałów

Raporty

Inteligentne mapy

4.6.2 Tworzenie struktury oddziałów

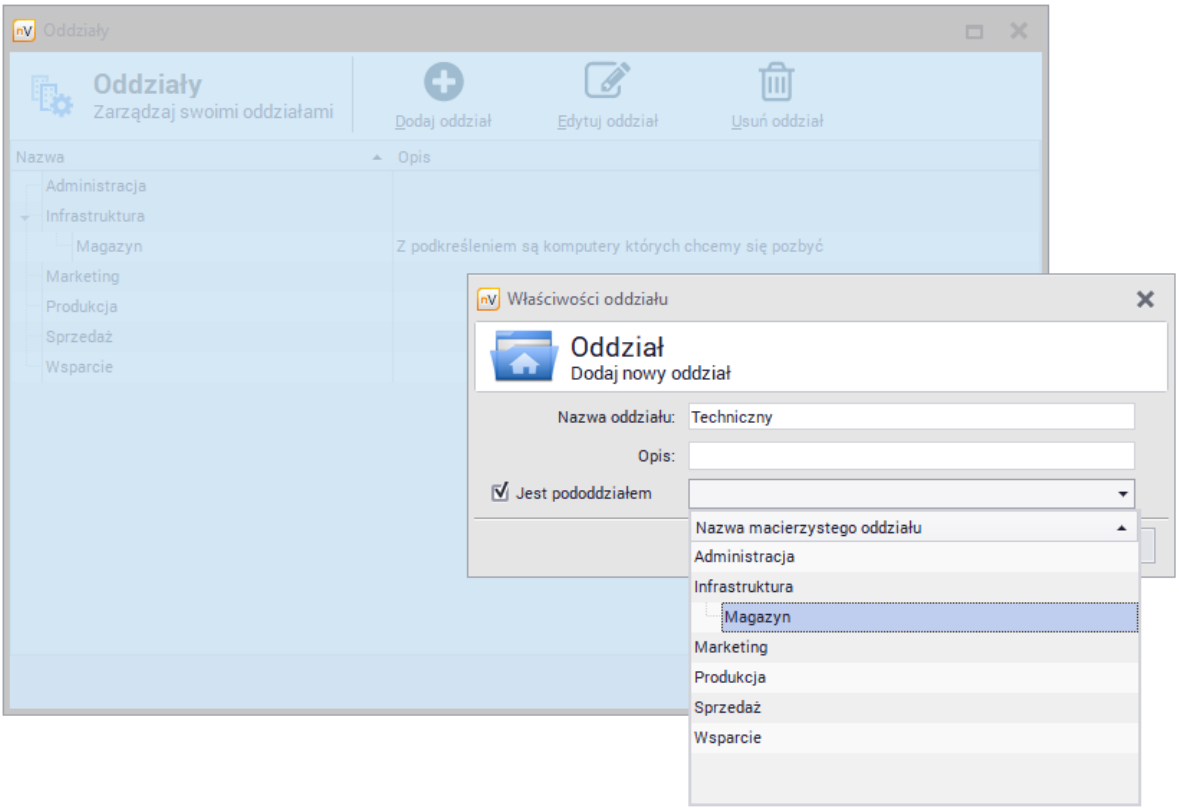
Przy tworzeniu hierarchii oddziałów należy zacząć od najbardziej ogólnych, a w ostatniej kolejności przejść do położonych najniżej w hierarchii pododdziałów. Oddziały pozwalają tylko na graficzne ustalenie zależności, pod kątem działania są one "na tym samym poziomie". Taki postępowanie przyspieszy proces tworzenia, ponieważ nie będzie konieczne wracanie do właściwości pododdziałów i uzupełnianie informacji.

Aby utworzyć strukturę oddziałów:

Wybierz opcję **Zarządzaj oddziałami** z karty **Narzędzia i opcje** na wstążce. Zostanie otwarte okno oddziałów, w którym wyświetlane są wszystkie oddziały zdefiniowane dla atlasu.

1. W celu utworzenia nowego oddziału, kliknij w przycisk **Dodaj oddział**. W oknie właściwości oddziału podaj nazwę tworzonego oddziału i opcjonalnie opis. Jeżeli jest to pododdział, to zaznacz

odpowiednie pole i wybierz z listy oddział nadrzędny.



2. Po zatwierdzeniu wprowadzonych zmian, utworzony oddział pojawi się na liście. Powtarzaj powyższe działania aż do utworzenia wszystkich oddziałów.

3. Jeżeli konieczne jest wprowadzenie poprawek, kliknij w przycisk **Edytuj oddział**.

4.6.3 Dodawanie urządzeń do oddziałów

Aby umieścić urządzenie w utworzonym wcześniej oddziale:

1. Przejdź do okna **Informacje o urządzeniu** do zakładki **Ogólne**.
2. Rozwiń menu znajdujące się przy polu **Oddział** i wybierz oddział z listy. Kliknij **OK** i zamknij okno.

4.6.4 Raporty

Możliwe jest generowanie raportów dla wybranych oddziałów. Aby utworzyć taki raport, kliknij prawym przyciskiem myszy na oddziale, dla którego chcesz utworzyć raport i wybierz opcję **Raporty**. Możesz także wybrać dany oddział bezpośrednio w oknie generowania raportów.

Aby dowiedzieć się więcej na temat tworzenia raportów, przejdź do rozdziału Raporty.

4.7 Inteligentne mapy

4.7.1 Ogólne informacje

Inteligentne mapy różnią się od tradycyjnych map przede wszystkim dynamiką. W skład inteligentnej mapy wchodzą urządzenia, które w danej chwili spełniają podane warunki. Możliwe jest ustawienie

częstotliwości uaktualniania danej mapy oraz zestawu warunków (czyli filtru), które będą sprawdzane.

Działanie inteligentnych map opiera się na zdefiniowanych przez użytkownika filtrach. Aby możliwe było poprawne funkcjonowanie inteligentnej mapy, należy ją połączyć z odpowiednim filtrem.

Powiązane tematy

Filtry

Tworzenie filtru

Tworzenie inteligentnej mapy

Oddziały

4.7.2 Filtry

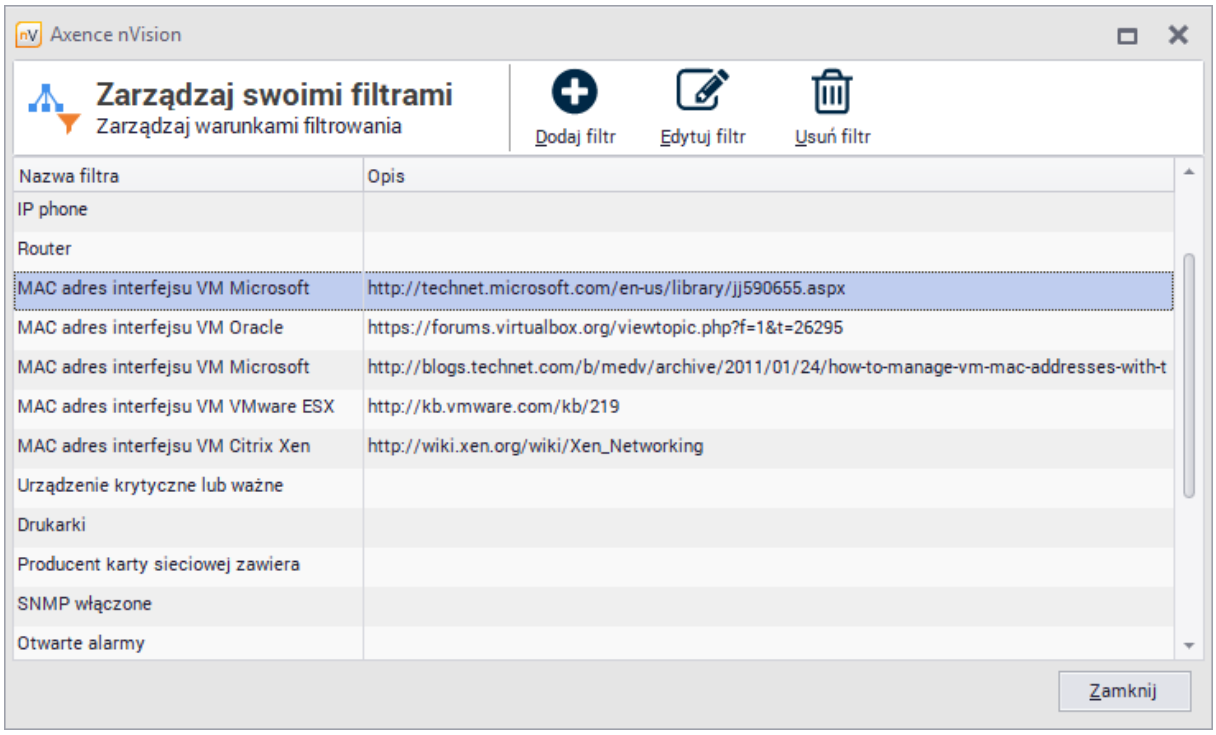
W poniższej tabeli przedstawione są warunki, które mogą zostać wykorzystane przy tworzeniu filtrów:

Grupa	Warunki
Właściwości urządzenia	• Nazwa • Info1 / Info2 • Typ urządzenia • Serwer / Router • Ważność • Status
Monitorowanie serwisów	• Posiadanie serwisu (np. SMTP) • Działanie / Nie działanie
Monitorowanie liczników	• Posiadanie licznika (np. CPU)
Alarmy	• Posiada otwarte alarmy
Agenty	• Posiada Agenta • Agent działa / Nie działa • Wersja Agenta nie jest aktualna
Oddziały	• Nazwa oddziału • Urządzenie bez przypisanego oddziału
Inwentaryzacja oprogramowania	• Posiada zainstalowaną aplikację • Dana aplikacja nie jest zainstalowana

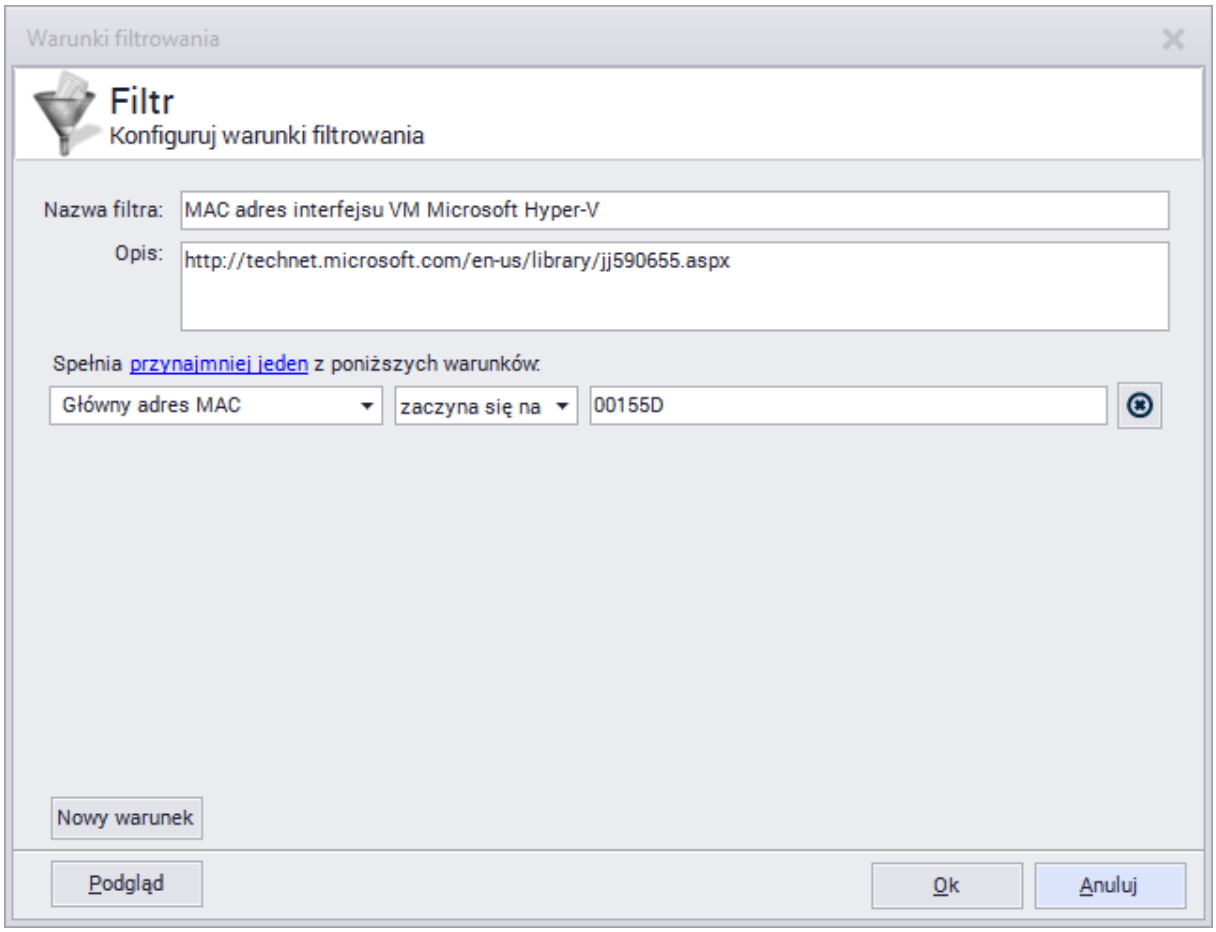
4.7.3 Tworzenie filtru

Aby utworzyć filtr:

1. Wybierz **Filtry dla inteligentnych map** z karty **Narzędzia i opcje** na wstążce. W oknie Zarządzania filtrami kliknij w przycisk **Dodaj filtr**.



2. W oknie Warunków filtrowania podaj **Nazwę filtru** i **Opis**. Następnie ustaw warunki dla filtru. Aby dodać kolejny warunek, kliknij w przycisk **Nowy warunek**. Aby realizować alternatywę zamiast sumy warunków, kliknij w słowo wszystkie - spowoduje to zmianę na przynajmniej jeden. Przykładowy filtr wraz z warunkami przedstawiony jest na poniższym rysunku.

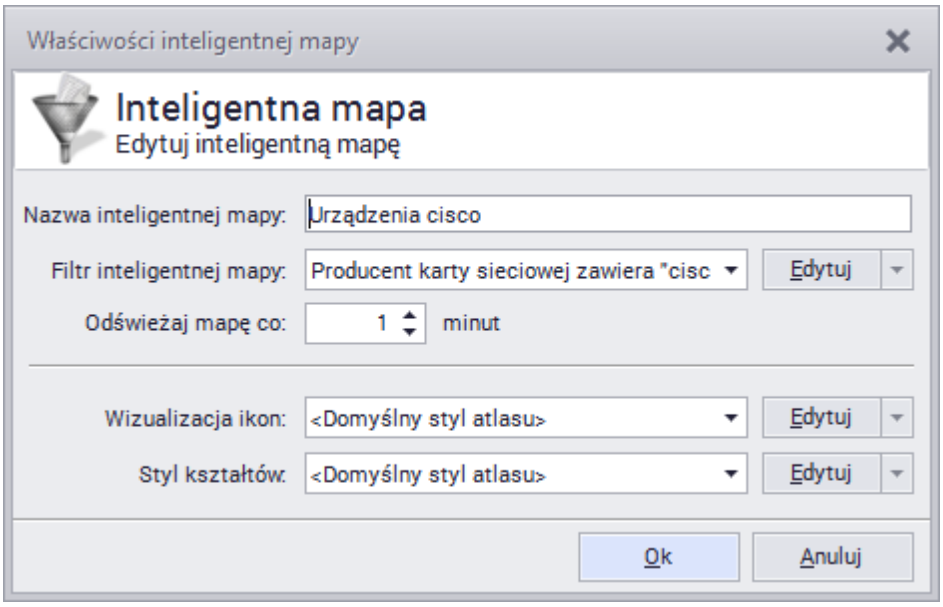


3. Aby przeglądać listę urządzeń spełniających zdefiniowane warunki, kliknij w przycisk **Podgląd**. Po zaakceptowaniu zmian nowo utworzony filtr pojawi się na liście filtrów.

4.7.4 Tworzenie inteligentnej mapy

Aby utworzyć inteligentną mapę:

1. Kliknij prawym przyciskiem myszy w INTELIGENTNE MAPY znajdujące się na liście w lewej części okna nVision. Wybierz opcję **Nowy | Inteligentna mapa**.
2. W oknie Właściwości inteligentnej mapy podaj **Nazwę** i wybierz z listy **Filtr**, który ma być powiązany z tworzoną mapą. Jeśli taki filtr nie został jeszcze utworzony, to rozwiń menu przy przycisku **Edytuj**, wybierz opcję **Utwórz nowy** i postępuj zgodnie z opisem Tworzenie filtru.
3. Ustaw czas odświeżania mapy i style wizualizacji. W przypadku inteligentnych map nie jest możliwe ręczne ustawianie elementów graficznych - inteligentne mapy są tworzone automatycznie.



Część V

5 Agent nVision

5.1 Wprowadzenie

Agenty są programami działającymi na monitorowanych komputerach. Są one niezbędne dla:

- monitorowania aktywności użytkowników,
- inwentaryzacji sprzętu i oprogramowania,
- ochrony danych DataGuard oraz
- zdalnej pomocy technicznej HelpDesk (wybrane funkcje).

Powiązane tematy

Podstawowe informacje o Agentach

Komunikacja między Agentem a nVision

Instalowanie i odinstalowywanie Agentów

Ustawienia Agenta

Wydajność (duża liczba Agentów)

Konfiguracja połączenia Agentów zainstalowanych na komputerach mobilnych

Porty

5.2 Podstawowe informacje o Agentach

Bezpieczeństwo

Komunikacja pomiędzy Agentem a serwerem nVision jest szyfrowana przy pomocy TLS 1.2. Baza danych również jest zabezpieczona, przy pomocy hasła. Aby mieć pewność, że tylko jedna instancja nVision może komunikować się z Agentem, ustaw hasło Agenta w nVision.

Ruch sieciowy generowany przez Agenty

Wszystkie przesyłane dane są pakowane przed wysłaniem i rozpakowywane po dotarciu do nVision. Agenty wysyłają niewielkie pakiety co kilka godzin (można ustawić ten parametr w nVision). Dzienny ruch generowany przez pojedynczego Agenta to ok. 100kB. Pierwszy pakiet wysyłany po instalacji Agenta może być większy (do ok. 500kB). Agent aktualizuje się automatycznie, gdy nowa instalacja nVision zostanie wykryta. Ta operacja może zwiększać ruch w sieci (konieczne jest przesłanie pliku instalacyjnego Agenta). Aby zapobiec znacznemu obciążeniu sieci, można ograniczyć połączenia Agentów z nVision do jednego (Agenty będą uaktualniane po kolei).

Zasoby

Agent przechowuje ok. 30 - 50 MB danych. Zużycie CPU powinno być bardzo niskie (0 - 5%), chwilowo do 15%. Jedynym modułem, który może powodować znaczne obciążenie CPU jest monitorowanie danych przesyłanych przez użytkowników. Jest to spowodowane Windowsowym mechanizmem i może występować na starszych systemach, w których przesyłanych jest bardzo wiele danych (np. serwery

baz danych). Zaleca się wyłączenie monitorowania ruchu sieciowego w profilu Agenta zainstalowanego na tego typu maszynie.

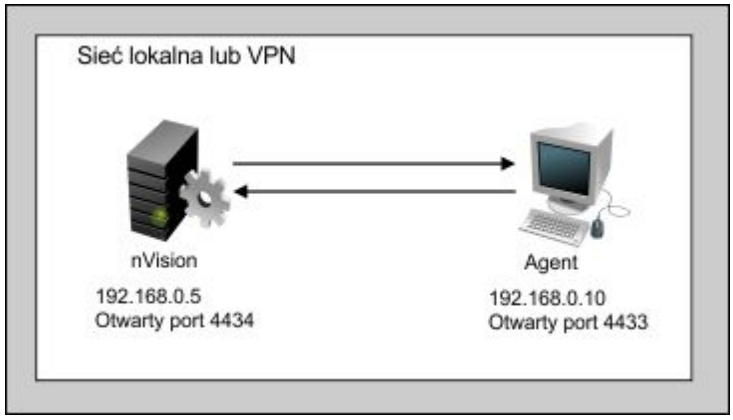
Możliwości

Pliki wykonywalne Agenta muszą być dodane do listy wyjątków programu antywirusowego i listy DEP w Windows. Agent nVision ma funkcję monitorowania maili i blokowania stron www. Te funkcje używają integracji stosu TCP/IP i domyślnie są wyłączone. Jest to spowodowane oprogramowaniem antywirusowym, które nie pozwala na poprawne funkcjonowanie integracji i może skutkować utratą połączenia.

5.3 Komunikacja między Agentem a nVision

Sytuacja 1: Sieć lokalna, bez firewalla

Komputer z nVision oraz komputer z Agentem znajdują się w tej samej sieci lokalnej lub VPN, nie ma firewalla lub jest tylko Windowsowy.

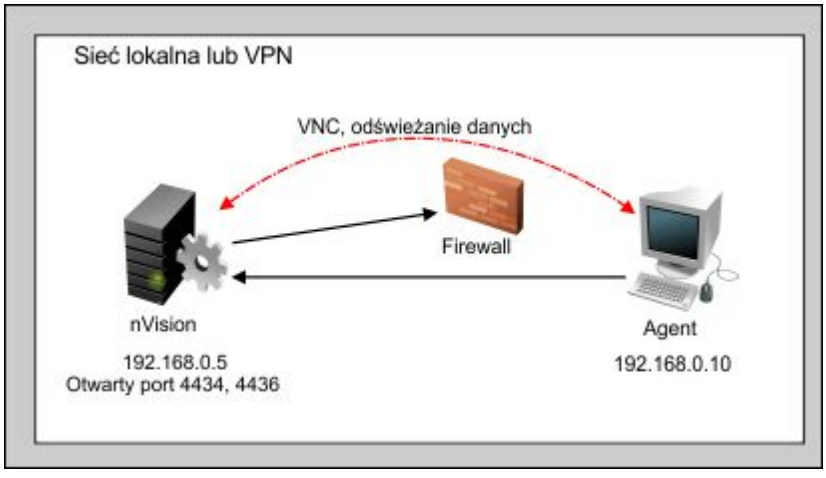


Agent wysyła cykliczne informacje co domyślnie 2 godziny (można ustawić ten czas w profilu Agenta). Z poziomu nVision można wymusić pobranie danych, działa podgląd pulpitu i zdalny dostęp.

Sytuacja 2: Sieć lokalna, firewall

Zablokowany port Agenta:

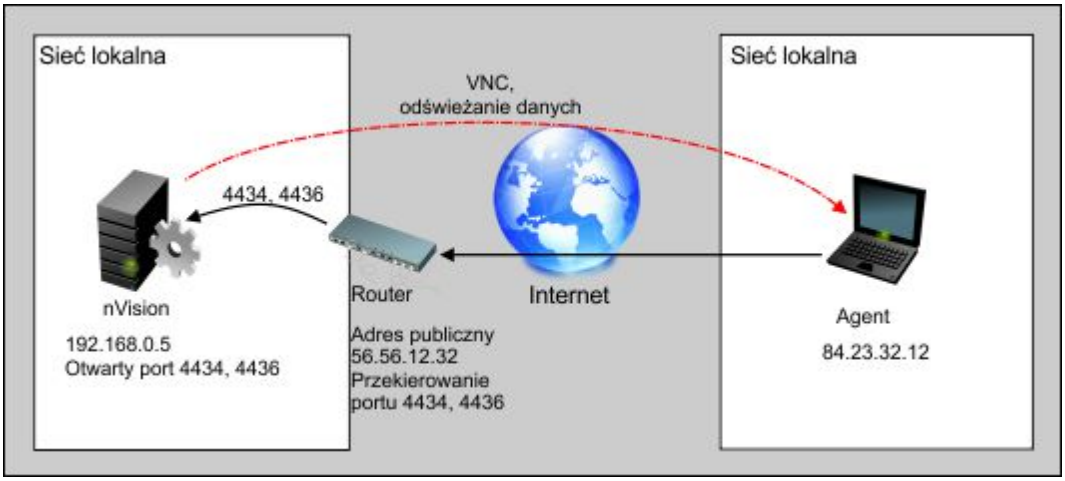
- firewall albo antywirus na komputerze z Agentem lub
- firewall na routerze.



Agent wysyła cykliczne informacje co domyślnie 2 godziny (można ustawić ten czas w profilu Agenta). Z poziomu nVision można wymusić pobranie danych, jest zdalny dostęp. Agent inicjuje komunikację.

Sytuacja 3: Agent w sieci zdalnej

Agent został zainstalowany z podanym adresem publicznym nVision (czyli z publicznym adresem routera).



Sytuacja analogiczna do 2: Agent wysyła cykliczne informacje co domyślnie 2 godziny; z poziomu nVision można wymusić pobranie danych, jest zdalny dostęp.

Powiązane tematy

Aby dowiedzieć się więcej o zdalnym dostępie, przejdź do rozdziału Zdalny dostęp.

Aby dowiedzieć się więcej o instalowaniu Agentów, przejdź do rozdziału Instalowanie i odinstalowywanie Agentów.

Aby zapoznać się z wymaganiami oraz dowiedzieć się, jak prawidłowo skonfigurować nVision i Agenta, przejdź do rozdziałów Konfiguracja oraz Konfiguracja połączenia Agentów zainstalowanych na komputerach mobilnych.

5.4 Instalowanie i odinstalowywanie Agentów

5.4.1 Ogólne informacje

Agenta można zainstalować na kilka sposobów. Wybierz sposób najbardziej odpowiadający Twoim potrzebom:

- Instalacja przez Active Directory (GPO) z zastosowaniem instalatora MSI
- Instalacja zdalna za pomocą konsoli zarządzania oprogramowania antywirusowego
- Instalacja ręczna

Instalowanie nowej wersji Agenta

Agent posiada mechanizm automatycznej aktualizacji. Przy każdym połączeniu z nVision sprawdza on, czy nie ma dostępnej nowej wersji Agenta. Jeśli jest ona dostępna (np. po zainstalowaniu nowej wersji

nVision), Agent automatycznie ją pobierze i ponownie się uruchomi.

Archiwizowanie Agentów

Aby dowiedzieć się, jak odinstalować Agenta i zwolnić jego licencję bez utraty danych o aktywności użytkowników, przejdź do rozdziału Archiwizowanie Agentów.

Odinstalowywanie Agentów

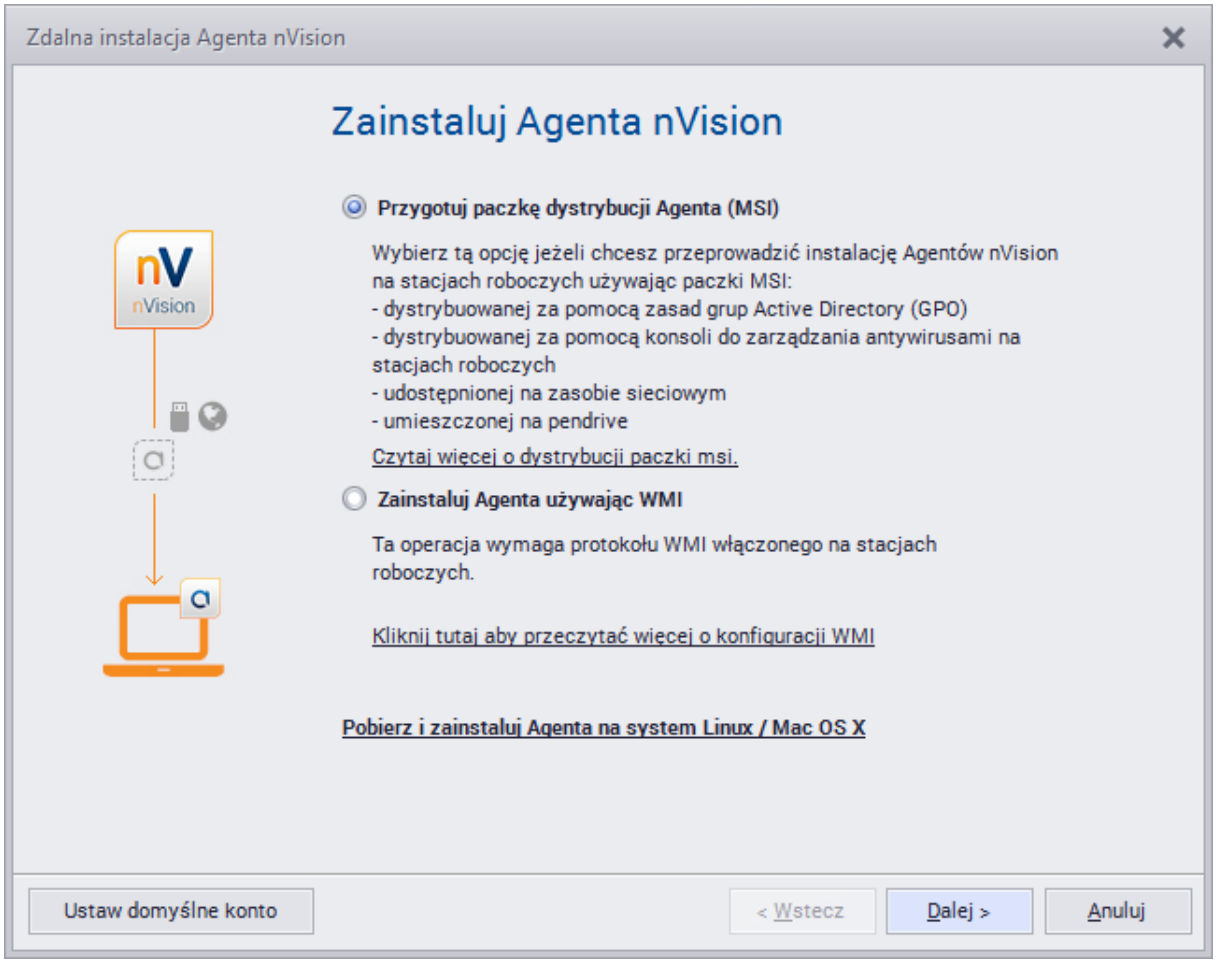
Przejdź do rozdziału Odinstalowywanie Agentów.

5.4.2 Instalacja przez Active Directory (GPO) z zastosowaniem instalatora MSI

Paczka dystrybucji Agenta (MSI)

Poniższy opis wskazuje jak przygotować instalator MSI Agenta. Może on być wykorzystany zarówno do instalacji przez Active Directory, jak i do instalacji ręcznej na poszczególnych komputerach. W takim przypadku należy pamiętać, iż instalator MSI dokonuje instalacji w trybie nieinteraktywnym. Instalator wymaga praw administratora lokalnego komputera w celu zainstalowania serwisu Agenta.

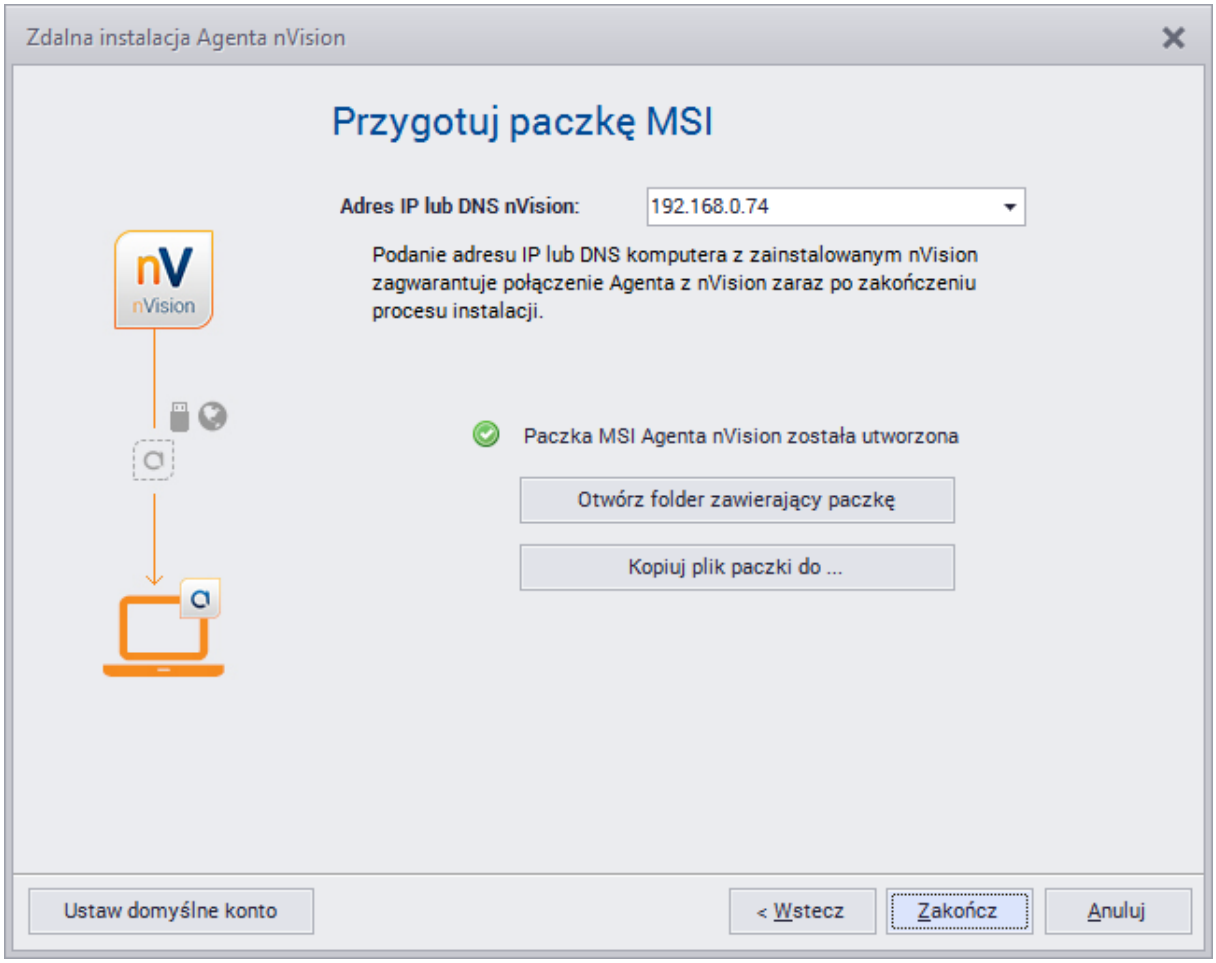
1. Wybierz w menu **Agenty | Zainstaluj Agenta nVision**.
2. Wybierz opcję **Przygotuj paczkę dystrybucji Agenta (MSI)**



3. Podaj adres IP na który Agent będzie wysyłał dane. Domyślnie jest to adres komputera na którym działa nVision. Jeśli jednak chcemy zainstalować Agenta na komputerze pracującym poza

siedzibą firmy, tak aby Agent przesyłał dane przez Internet, w polu tym należy podać publiczny adres IP lub nazwę DNS routera na którym dokonamy przekierowania portu TCP 4434 na komputer z programem nVision. Podany adres zostanie na stałe wpisany do przygotowanej w kolejnym kroku paczki MSI. Aby zmienić ten adres, konieczne jest powtórne przygotowanie paczki.

4. Kliknij odpowiednio jeden z przycisków, aby otworzyć folder z przygotowanym instalatorem MSI, lub skopiować go do podanego katalogu.



Powiązane tematy

Instalacja Agenta przez Active Directory

5.4.3 Instalacja zdalna za pomocą konsoli zarządzania oprogramowania antywirusowego

Wygenerowana paczka instalacyjna Agenta może zostać rozdystrybuowana również przy użyciu konsol zdalnego zarządzania oprogramowania antywirusowego.
Poniżej znajdują się odnośniki do stron producentów najpopularniejszego oprogramowania antywirusowego zawierających instalatory konsol zdalnego zarządzania:

ESET Remote Administrator

pliki do pobrania: http://www.eset.pl/Pobierz/Wersje_pelne,p,1497/ESET_Remote_Administrator

Kaspersky Security Center

pliki do pobrania: http://www.kaspersky.pl/download.html?s=prod_download&prod_id=210

AVG Remote Administration

pliki do pobrania: http://www.avg.com/pl-pl/download.prd-rad

5.4.4 Instalacja ręczna

Aby zainstalować Agenty ręcznie, wykonaj jedną z poniższych akcji:

- Skopiuj na pendrive lub na zasób sieciowy plik nvagentinstall.exe (znajduje się on w podkatalogu "Agents" programu nVision) i uruchom na każdym komputerze, na którym chcesz zainstalować Agenta.
- Możesz także przygotować paczkę dystrybucji MSI i uruchomić ją na każdym komputerze lub dystrybuować przez Active Directory GPO (szczegóły w rozdziale Instalacja przez Active Directory (GPO) z zastosowaniem instalatora MSI).

5.4.5 Archiwizowanie Agentów

Narzędzie archiwizowania Agentów służy do wyłączenia Agentów na urządzeniach, które nie mają być monitorowane bez utraty wszystkich danych zgromadzonych przez Agenta. Skutki zarchiwizowania danych Agenta są następujące:

- odinstalowanie Agenta oraz **zwolnienie** jego licencji,
- **zachowanie** danych aktywności użytkowników,
- **usunięcie** danych inwentaryzacyjnych i środków trwałych,
- **wyłączenie** monitoringu serwisów i liczników.

Archiwizowanie danych Agenta

Aby zarchiwizować dane Agenta:

1. Kliknij prawym przyciskiem myszy na danej ikonie komputera z Agentem w nVision.
2. Wybierz opcję **Agent | Zarchiwizuj**. Kliknij w przycisk **OK**.
3. Po zarchiwizowaniu Agent jest prezentowany ze statusem "Archiwalny".

5.4.6 Deinstalacja Agentów

Aby zdalnie odinstalować Agenty, należy wybrać z menu kontekstowego urządzenia opcję **Agent | Odinstaluj...**. Deinstalacja odbywa się bez udziału WMI, dzięki czemu jest możliwość odinstalowania Agentów niezależnie, czy WMI jest włączone na zdalnym urządzeniu, czy nie. Agenty zostaną odinstalowane automatycznie po uruchomieniu i nawiązaniu połączenia z konsolą.

Można także odinstalować Agenta ręcznie, uruchamiając plik unins000.exe znajdujący się w katalogu Agenta.

5.5 Konfigurowanie Agentów

5.5.1 Hasło Agenta

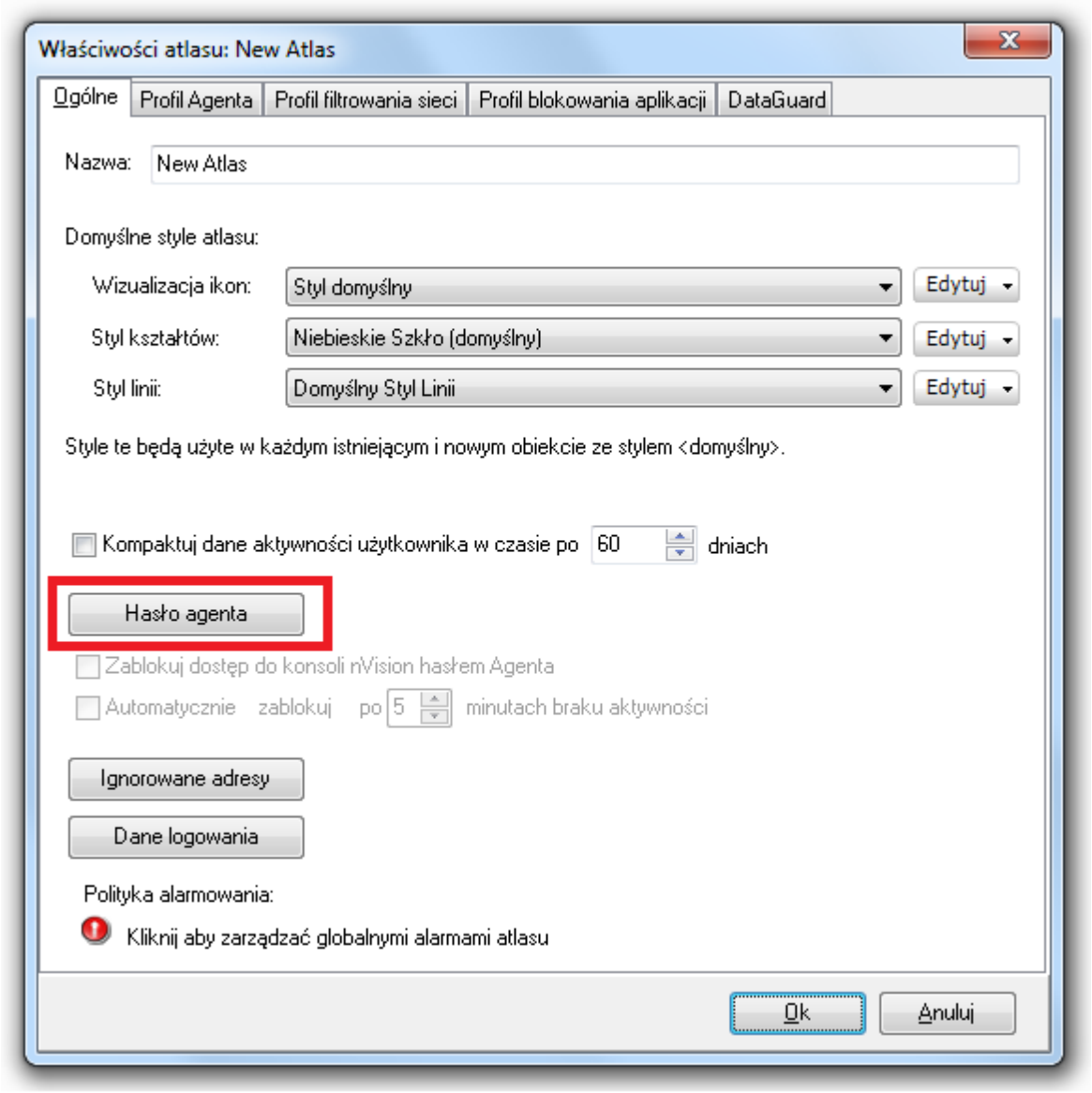
Agent Axence nVision® jest zabezpieczony hasłem przed odinstalowaniem przez użytkownika (nawet posiadającego uprawnienia administratora w systemie Windows).

Hasło zabezpieczające Agenta przed odinstalowaniem jest równocześnie hasłem wbudowanego w nVision **Administratora** (podstawowe konto z loginem **Administrator** - jego nazwa jest pogrubiona w widoku okna **Użytkownicy**). Agent zostaje zabezpieczony hasłem automatycznie po instalacji, przy pierwszym pomyślnym połączeniu z Serwerem nVision.

Hasło Agenta w Axence nVision® w wersjach starszych niż 8.x

Aby zmienić hasło Agenta w danym Atlasie:

1. Wybierz **Atlas | Właściwości**.
2. W oknie Właściwości atlasu kliknij w przycisk **Hasło Agenta**.

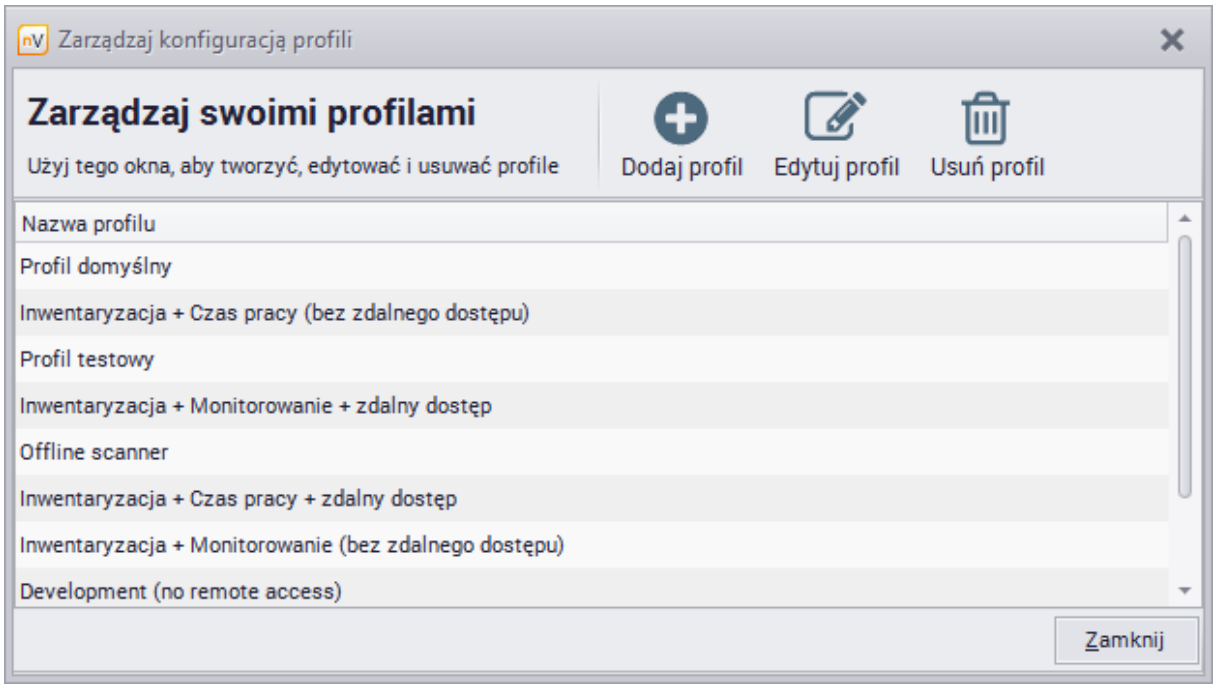


3. Podaj stare i nowe hasło, a następnie wciśnij **OK**.

5.5.2 Zarządzanie profilami

W przypadku definiowania wielu profili Agentów warto skorzystać z możliwości tworzenia i edycji przy użyciu narzędzia zarządzania profilami. W tym celu:

1. Na wstążce wybierz opcję **Zarządzanie profilami Agentów** (z karty **Narzędzia i opcje)**. Zostanie otwarte okno **Zarządzaj konfiguracją profili**.



2. Na liście wyświetlane są zdefiniowane profile. Aby **Dodać**, **Edytować** lub **Usunąć profil**, użyj odpowiedniego przycisku.
3. W przypadku tworzenia nowego profilu należy, po kliknięciu w przycisk **Dodaj profil**, podać w oknie **Konfiguracji Agenta** nazwę tworzonego profilu, a następnie ustawić jego właściwości. Ich opis znajduje się w rozdziale Ustawienia Agenta.

5.5.3 Ustawienia Agenta

Aby zmienić ustawienia profilu Agenta, wybierz na wstążce opcję **Zarządzaj profilami Agentów** (na karcie **Narzędzia i opcje).**

Ustawienia profili Agentów ujęte są w 2 zakładkach:

Ogólne

Ustawienia ogólne umożliwiają:

- włączenie skanowania plików użytkownika wg rozszerzeń.
  Istotnym problemem jest legalność posiadanych przez użytkownika plików. Dlatego też nVision umożliwia monitorowanie plików, których rozszerzenie sugeruje powiązanie z prawami autorskimi. Możliwe jest dodawanie i usuwanie z listy monitorowanych plików użytkownika. W szczególności, aby dodać do listy rozszerzenia najczęściej używanych plików multimedialnych, należy wcisnąć link **dodaj rozszerzenia multimediów.** Aby monitorować inny rodzaj plików, wpisz ich rozszerzenie na liście (oddzielone przecinkami),
- zdefiniowania portów TCP, na których ruch w aplikacjach ma być blokowany przez Agenta.

Kompatybilność

- Monitorowanie użycie łącza
  Pozwala monitorować całkowity transfer wejściowy i wyjściowy z podziałem na lokalny oraz internetowy, a także użycie łącza przez przeglądarki, klienta poczty i inne.

- Integracja blokowania aplikacji

  Pozwala Agentowi na blokowanie aplikacji określonych w konfiguracji nVision.

- Integracja DataGuard
  Włączenie ochrony danych skutkuje monitorowaniem nośników używanych przez użytkownika i pozwala na zarządzanie prawami dostępu.

- Integracja ze stosem TCP/IP
  Odznaczenie tej opcji spowoduje, że blokowanie odwiedzanych stron oraz monitorowanie nagłówków e-maili nie będzie możliwe. Jeśli po właczeniu integracji na komputerze z Agentem występują problemy z działaniem określonych aplikacji lub dostępem do stron internetowych (np. stron bankowości internetowej), należy dodać do wykluczonych nazwy procesów tych aplikacji lub domeny.

5.5.4 Profil filtrowania sieci

W ramach profilu Agenta możliwe jest blokowanie wybranych stron www. Żeby blokowanie się powiodło, konieczne jest zaznaczenie opcji **Integracja ze stosem TCP/IP włączona** w zakładce **Kompatybilność** . Aby dowiedzieć się więcej, przejdź do rozdziału Nie mogę blokować stron www.

Blokowanie stron ma miejsce niezależnie od aplikacji i portu. Strony rozpoznawane są na podstawie prefixu żądania. Blokowanie odbywa się na poziomie:

- adresu IP,
- dokładnej domeny (na poziomie http),
- wyrażeń regularnych dla domeny (także na poziomie http).

Dodawanie reguł filtrowania opisane jest w rozdziale Jak zablokować użytkownikom dostęp do wybranych stron www?.

5.5.5 Integracja ze stosem TCP/IP

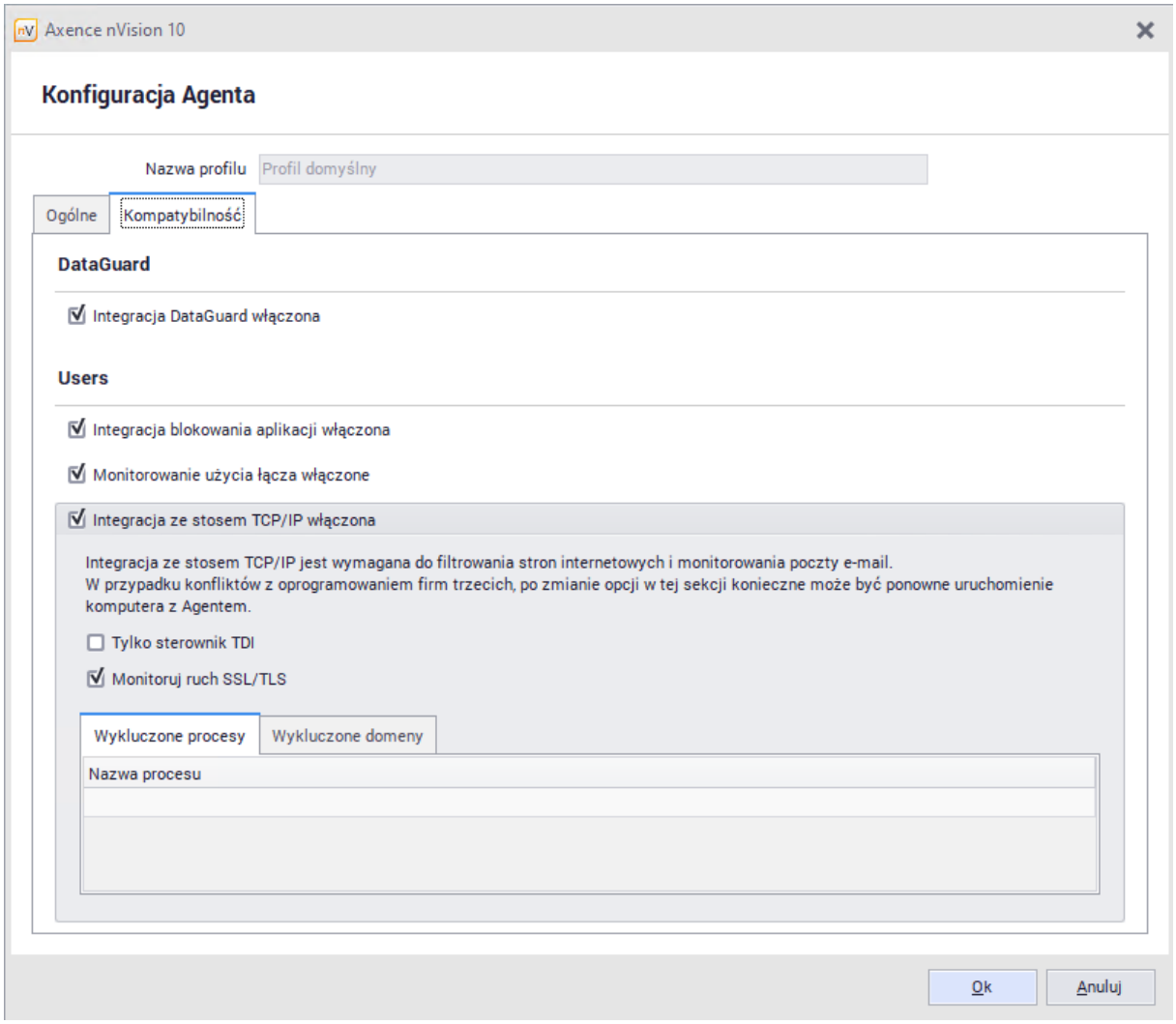
Monitorowanie maili i blokowanie stron WWW możliwe jest tylko dla komputerów z zainstalowanym Agentem i włączoną integracją ze stosem TCP/IP. Aby dowiedzieć się więcej na temat instalowania Agentów, przejdź do rozdziału Instalowanie i odinstalowywanie Agentów.

Obsługiwane są protokoły: HTTP, HTTPS, SMTP:25, SMTP:587, SMTP via SSL, POP3 via SSL i POP3:110. Obecnie nie są obsługiwane: IMAP, MAPI.

Włączanie integracji ze stosem TCP/IP

Jeśli Agent jest zainstalowany, to powodem problemów z monitorowaniem maili i blokowaniem stron WWW może być wyłączona integracja ze stosem TCP/IP. Domyślnie integracja ta jest wyłączona ze względu na konieczność wcześniejszych testów, głównie pod kątem współdziałania z programami antywirusowymi. Aby włączyć integrację ze stosem TCP/IP:

1. Ze wstążki wybierz **Zarządzanie profilami Agentów** (z karty **Narzędzia i opcje).**
2. Utwórz nowy profil lub zaznacz profil, którego używają Agenty a następnie kliknij przycisk **Edytuj profil**.
3. W konfiguracji profilu zaznacz opcję **integracji ze stosem TCP/IP** w zakładce **Kompatybilność**.



4. **Na testowanych komputerach dodaj całą zawartość katalogu `c:\Program Files\Axence \nVision Agent 2\` wraz z podfolderami do wyjątków antywirusa.**
5. Zrestartuj komputery.
6. Jeżeli przez najbliższe kilka restartów systemu nie ma żadnych objaw, np. utrata sieci - oznacza to, że integrację ze stosem TCP/IP można włączyć na reszcie komputerów.

5.6 Instalacja Agenta dla systemu Linux i OS X

Agent dla systemu Linux oraz OS X zbiera informacje o konfiguracji sprzętowej oraz oprogramowaniu zainstalowanym na urządzeniu i przesyła je do Serwera nVision.

Inwentaryzacja domyślnie wykonuje się co 12 godzin, jednak można zmienić ten czas w pliku konfiguracyjnym po czym należy zrestartować Agenta.

Aby zainstalować Agenta:

1. Pobierz plik skryptu instalacyjnego Agenta dla odpowiedniej architektury sprzętowej do folderu *C:\Program Files (x86)\Axence\nVision\Agents*:

OSX:

```
http://cdn.axence.net/linux/osx_agent.run
```

Linux 32-bit:

```
http://cdn.axence.net/linux/linux_agent32bit.run
```

Linux 64-bit:

```
http://cdn.axence.net/linux/linux_agent64bit.run
```

2. Skopiuj plik skryptu instalacyjnego Agenta do systemu Linux/OS X.

3. Do instalacji wymagane są uprawnienia administratora (*root*).
   Przed instalacją Agenta w wersji 2.0 odinstaluj Agenta 1.0.
   Pamiętaj aby nadać atrybuty praw uruchomienia `chmod + x` *dla pliku skryptu instalacyjnego Agenta.*
   W terminalu/konsoli systemu operacyjnego uruchom polecenie:

   ```
   > sudo ./*nazwa_instalatora*.run
   ```

   W przypadku instalacji Agenta na czystym systemie, instalator może poprosić użytkownika o podanie adresu IP Serwera nVision. Wówczas należy podać adres IP komputera, na którym zainstalowany jest Serwer nVision (bez portu).

   Po procesie instalacji, **Agent nie jest uruchamiany od razu.** Należy go uruchomić ręcznie poprzez wydanie odpowiedniego polecenia uruchamiającego usługę ***nvAgent***.
   Najprostszym a zarazem uniwersalnym sposobem na uruchomienie usługi jest wydanie następującej komendy:

   ```
   > /etc/init.d/nvAgent start
   ```

   Należy pamiętać, aby uruchomić usługę należy posiadać uprawnienia administracyjne.

Sterowanie usługą Agenta

Wiele dystrybucji systemu operacyjnego Linux posiada narzędzie ***service***. Narzędzie to odpowiedzialne jest za uruchamianie, zamykanie jak również restart usługi. Jeśli w systemie zainstalowane jest to narzędzie - w celu podejrzenia dostępnych opcji należy użyć polecenia:

```
> service nvAgent
Usage: {start|stop|status|restart}
```

Usługa ***nvAgent*** posiada cztery tryby:

- ***start*** - uruchamia usługę,
- ***stop*** - zamyka usługę,
- ***status*** - informuje użytkownika czy usługa aktualnie działa,
- ***restart*** - zamyka działającą usługę a następnie uruchamia ponownie.

Deinstalacja Agenta

Deinstalacja Agenta w wersji 1.0

W celu usunięcia Agenta w wersji 1.0 należy usunąć plik ***/usr/bin/nVAgent*** oraz katalog ***/var/nVAgent***

Deinstalacja Agenta w wersji 2.0

W celu usunięcia Agenta z systemu, należy wykonać następujące polecenie (na prawach roota):

```
> sudo ./*nazwa_instalatora*.run /uninstall
```

Instalacja nienadzorowana

Podawanie adresu IP serwera nVision na dużej liczbie komputerów może być uciążliwe, dlatego umożliwiono konfigurowanie IP nVision z poziomu parametrów instalatora. W tym celu należy wykonać następujące polecenie:

```
> sudo ./*nazwa_instalatora*.run $IP_Serwera_nVision
```

Jeśli na komputerze nie był zainstalowany Agent, wówczas stworzona zostanie konfiguracja a użytkownik nie będzie proszony o podanie adresu IP serwera nVision.

Hierarchia katalogów, dalsze informacje

Oprogramowanie Agenta instalowane jest w katalogu: */opt/Axence*. Wraz z Agentem instalowane są następujące składniki wymagane do poprawnego działania aplikacji:

- Interpreter node.js: */opt/Axence/node*
- Interpreter perl5: */opt/Axence/perl5*
- Biblioteka FusionInventory: */opt/Axence/fusioninventory*
- Demon forever: */opt/Axence/forever*

Sam Agent jest zainstalowany w: ***/opt/Axence/Axence-agent***

Katalog logów znajduje się w: ***/opt/Axence/Axence-agent/logs***

Pliki konfiguracyjne

Agent posiada dwa pliki konfiguracyjne:

1. /opt/Axence/Axence-agent/agent.config

Odpowiedzialny za konfigurację:

- adresu Serwera nVision,
- portu, na którym Serwer nasłuchuje,
- interwału, po którym będzie sprawdzana aktualizacja
- interwału, po którym przeprowadzony zostanie skan sprzętu i oprogramowania.

Poniżej przedstawiony został przykładowy plik ***agent.config***

```
{
 "nVisionServer": "127.0.0.1",
 "nVisionPort": 4436,
 "updateCheckInterval": 43200000,
 "inventoryInterval": 3600000
}
```

2. /opt/Axence/Axence-agent/common.app.config

Przechowuje:

- ścieżkę do FusionInventory,
- ścieżkę do interpretera Perl,
- ścieżkę do demona Forever,
- ścieżkę do pliku, w którym zapisany jest unikalny identyfikator urządzenia.

Poniżej przedstawiony został przykładowy plik ***common.app.config***

```
{
 "fusionInventoryBin": "/opt/Axence/fusioninventory/bin/
fusioninventory-agent",
 "perlBin": "/opt/Axence/perl5/bin/perl",
 "foreverBin": "/opt/Axence/forever/bin/forever",
 "agentUuidFile": "/opt/Axence/Axence-agent/agent.uuid"
}
```

Należy pamiętać, że każdorazowo po zmianie jakiegokolwiek pliku konfiguracyjnego, należy

zrestartować serwis Agenta.

5.7 Instalacja Agenta dla systemu Android

Agent dla systemu Android zbiera informacje o konfiguracji sprzętowej oraz oprogramowaniu zainstalowanym na urządzeniu i przesyła je do Serwera nVision.

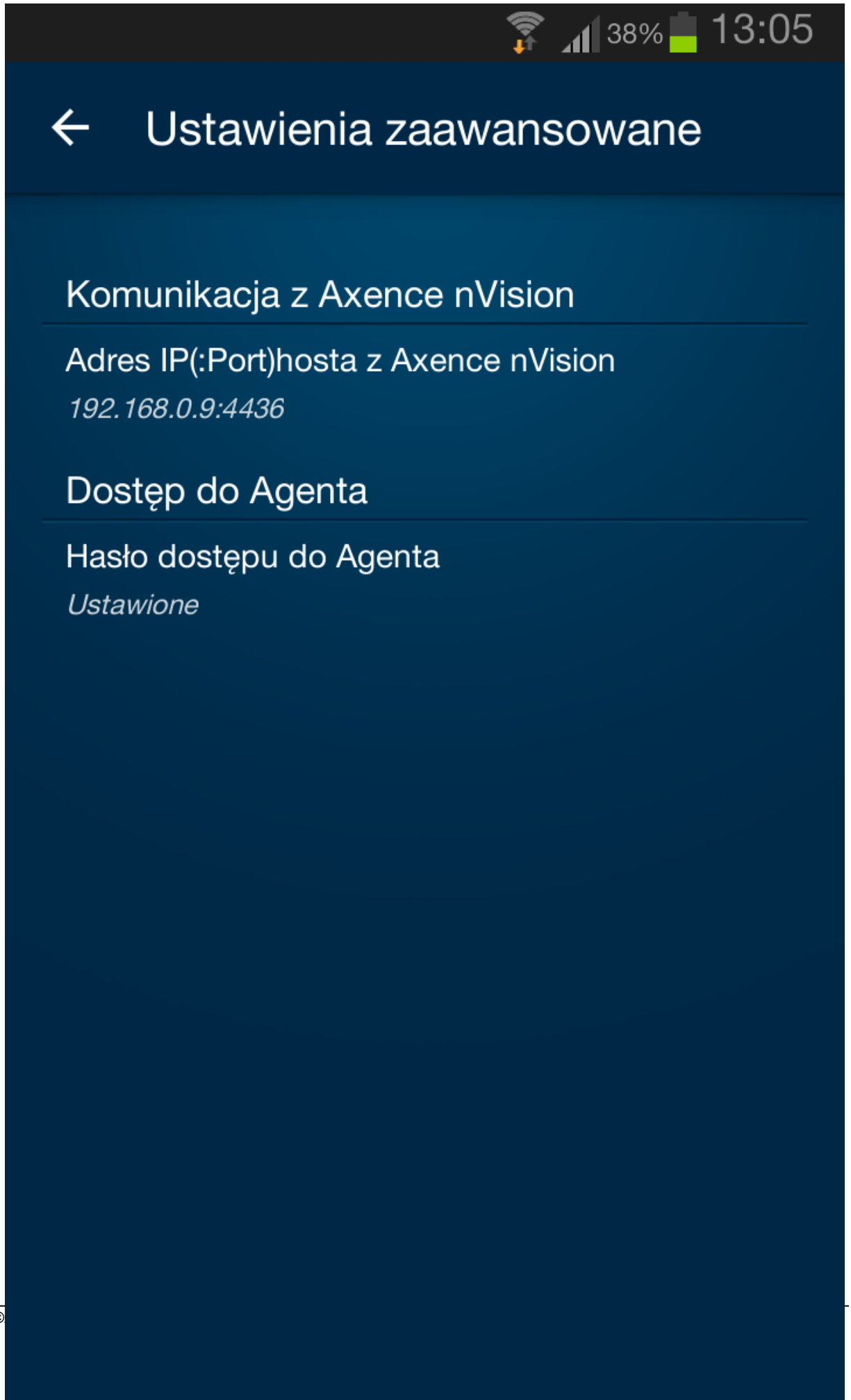
Aktualnie aplikacji nie można jeszcze pobrać za pośrednictwem sklepu Google Play, dlatego plik instalacyjny **"nVAgentInstall.apk"** należy skopiować na urządzenie mobilne (np. za pośrednictwem poczty e-mail albo linku do strony www) i własnoręcznie zainstalować.

Plik instalacyjny znajduje się w katalogu **"Agents"** w ścieżce instalacji Serwera nVision (domyślnie: **'C:\Program Files\Axence\nVision\Agents\'**). Plik instalacyjny może zostać pobrany również bezpośrednio z Serwera nVision:

```
http://IP_SERWERA:4436/nVAgentInstall.apk
```

Aby zainstalować Agenta:

1. Skopiuj plik Agenta **nVAgentInstall.apk** na urządzenie mobilne (np. za pośrednictwem poczty e-mail albo linku do strony www).
2. Zainstaluj aplikację. **Uwaga**: aby instalacja była możliwa konieczne jest włączenie w systemie opcji zezwalającej na instalację aplikacji spoza oficjalnego sklepu Google. Dostęp do tego ustawienia można uzyskać poprzez dłuższe przytrzymanie przycisku Menu, następnie wybranie Settings, Applications i zaznaczenie Unknown sources.
3. Na ekranie startowym aplikacji wprowadź adres komputera, na którym działa nVision, wraz z numerem portu 4436 oraz ustaw nowe hasło wymagane do późniejszej zmiany ustawień aplikacji. (W przypadku pracy poza firmową siecią WiFi konieczne może być dokonanie odpowiedniego przekierowania portu na routerze dostępowym.)

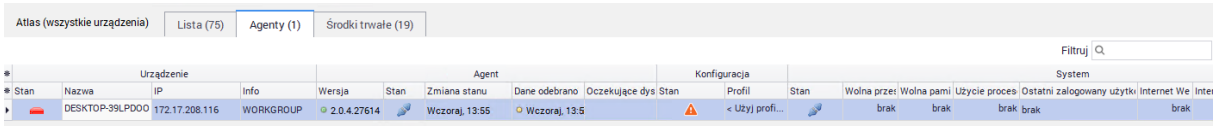

38%
13:05
Ustawienia zaawansowane
Komunikacja z Axence nVision
Adres IP(:Port)hosta z Axence nVision
192.168.0.9:4436
Dostęp do Agenta
Hasło dostępu do Agenta
Ustawione

4. *Ustawienia zaawansowane*: aby przejść do zmiany ustawień wybierz z menu kontekstowego (klawisz telefonu: Menu) "Advanced Settings", a następnie podaj hasło utworzone przy pierwszym uruchomieniu aplikacji.

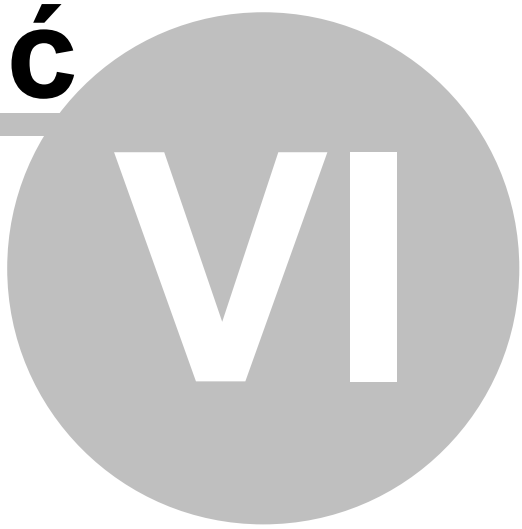
5.8 Widok "Agenty"

Widok "Agenty" w głównym oknie nVision umożliwia szybkie przeglądanie następujących danych:

- stan urządzenia,
- nazwa urządzenia,
- wersja Agenta,
- dostępność Agenta (połączony/odłączony),
- czas ostatniego połączenia,
- ostatnie pobranie danych,
- oczekujące dyspozycje (deinstalacja Agenta, zmiana adresu atlasu, reset danych),
- stan,
- konfiguracja,
- zrzuty ekranowe,
- wolna przestrzeń dyskowa,
- wolna pamięć fizyczna,
- użycie procesora (średnia z ostatniej minuty),
- ostatni zalogowany użytkownik,
- przesyłane dane (z ostatniej godziny)
- i inne.



Część



6 Users - monitorowanie aktywności użytkowników

6.1 Wprowadzenie

Axence nVision® jest wyposażony w Agenty przeznaczone do monitorowania aktywności użytkowników pracujących na komputerach z systemem Windows.
nVision gromadzi następujące informacje:

- Faktyczny czas aktywności (pracy). Nieaktywność (przerwa) to czas, w którym użytkownik nie naciska klawiszy ani nie porusza myszką.
- Czas użytkowania programów - informacje są pogrupowane dla łatwiejszej analizy aktywności użytkowników.
- Lista odwiedzanych stron. Aby otrzymać dane, Agent analizuje informację sieciową niskiego poziomu.
- Zasoby sprzętu i oprogramowania (przejdź do rozdziału Inwentaryzacja sprzętu i oprogramowania).
- Dane na temat wysłanych wiadomości e-mail.
- Informacje o wydrukach.

Agenty automatycznie przesyłają informacje o aktywności użytkownika co 1 godzinę. Skanowanie zasobów sprzętowych wykonywane jest co 24h.

Wymagania związane z monitorowaniem aktywności użytkowników

Aby gromadzić informacje o aktywności użytkowników, należy zainstalować Agenta nVision na zdalnym urządzeniu (co także umożliwi wykonywanie inwentaryzacji). Należy otworzyć port TCP 4436 na komputerze, na którym jest uruchomiony nVision. Aby uzyskać więcej informacji, przejdź do rozdziału Wymagania i konfiguracja.

Należy zauważyć, że cała komunikacja pomiędzy Agentami i nVision wymaga autoryzacji i żadne dane nie zostaną przekazane, jeśli Agenty i nVision nie będą odpowiednio skonfigurowane.

Informacje o aktywności użytkownika

1. Otwórz okno **Informacje o użytkowniku**.
2. Przejdź do zakładki **Aktywność**.
3. Wybierz zakładkę, którą chciałbyś zobaczyć:
   - Podsumowanie,
   - Czas pracy,
   - Aplikacje,
   - Strony internetowe,
   - Wydruki,
   - E-maile,
   - Użycie łącza.
4. Ustaw przedział czasu dla prezentowanych danych.

Możliwe jest uzyskanie informacji o różnych użytkownikach, którzy korzystali z danego komputera poprzez rozwinięcie menu **Użytkownicy** znajdującego się w górnej części okna.

Komputery z przypisanymi adresami DHCP

Jeśli komputer ma nowy adres IP przypisany przez DHCP, będzie on zaktualizowany w bazie danych nVision przy połączeniu Agenta z nVision. Nie trzeba więc robić tego ręcznie.

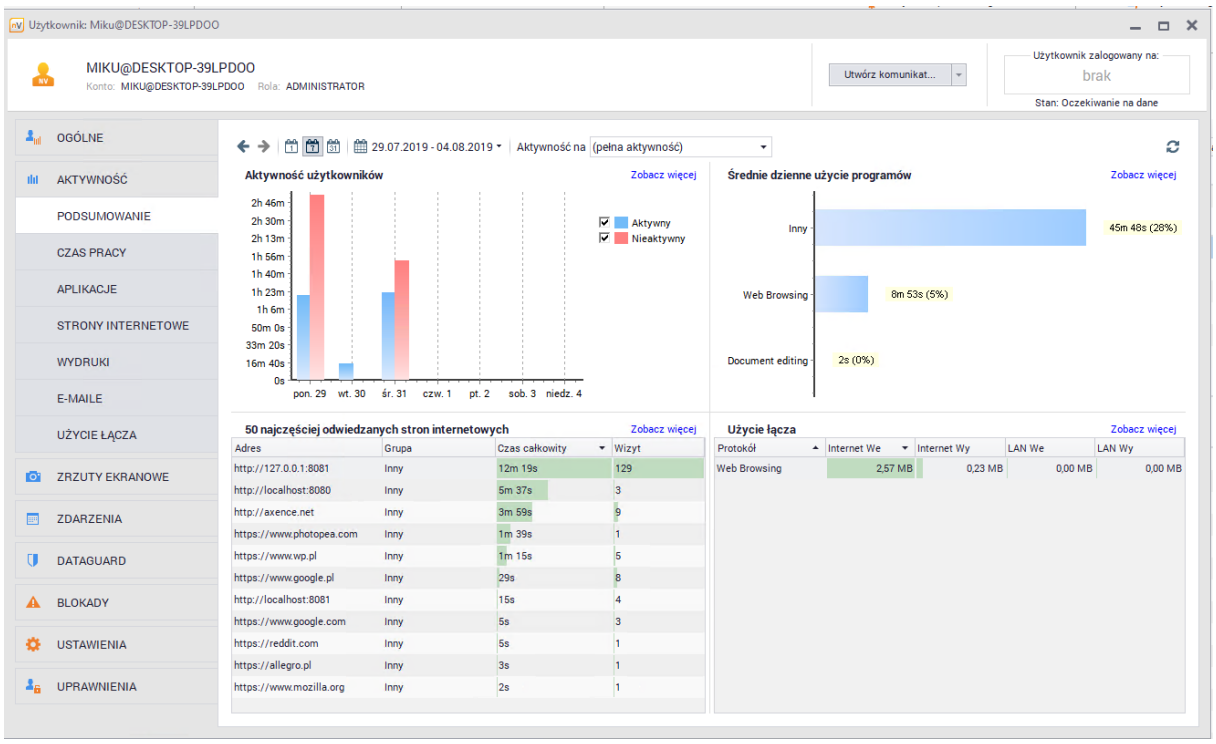
6.2 Ogólne informacje

Aby wyświetlić ogólne informacje na temat aktywności użytkownika przejść do okna **Informacji o użytkowniku** do zakładki **Aktywność \ Podsumowanie**.

Zapoznaj się również z modelem ustawień monitorowania.

Zakładka ta zawiera informacje o:

- aktywności użytkownika (aktywny/nieaktywny),
- średnim dziennym użyciu programów wg grup skonfigurowanych w opcjach nVision,
- 50 najczęściej odwiedzanych stronach internetowych,
- użyciu łącza w sieci lokalnej oraz w Internecie, z podziałem na ruch przychodzący oraz wychodzący.



Więcej szczegółów dotyczących ruchu sieciowego można znaleźć w zakładce **Użycie łącza**.

6.3 Blokowanie dostępu do wybranych aplikacji

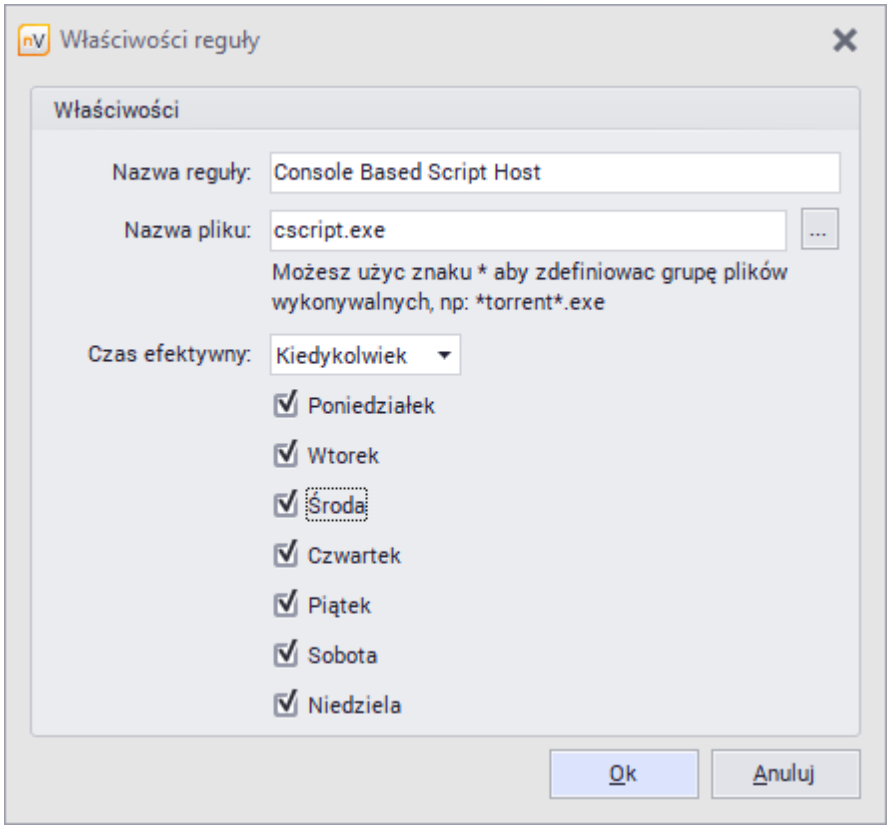
Blokowanie aplikacji jest możliwe na stacjach roboczych z zainstalowanym Agentem nVision poprzez odpowiednie skonfigurowanie Agenta. Domyślnie, wszystkie aplikacje mogą być uruchamiane.

Model ustawień blokowania został przedstawiony w rozdziale Ustawienia blokowania

Blokowanie aplikacji

Aby zablokować aplikację:

1. Przejdź do okna **informacji o Atlasie**, grupie lub **użytkowniku**. Przejdź do zakładki **Blokady.**
2. Otwórz kartę **Blokowanie aplikacji.**
3. Kliknij przycisk **Dodaj regułę**.
4. Podaj nazwę reguły, nazwę pliku wykonywalnego i czas, kiedy blokowanie ma być aktywne. Kliknij **OK**.



W opcjach nVision możesz skonfigurować tekst powiadomienia, które zostanie wyświetlone użytkownikowi gdy spróbuje uruchomić zablokowaną aplikację.

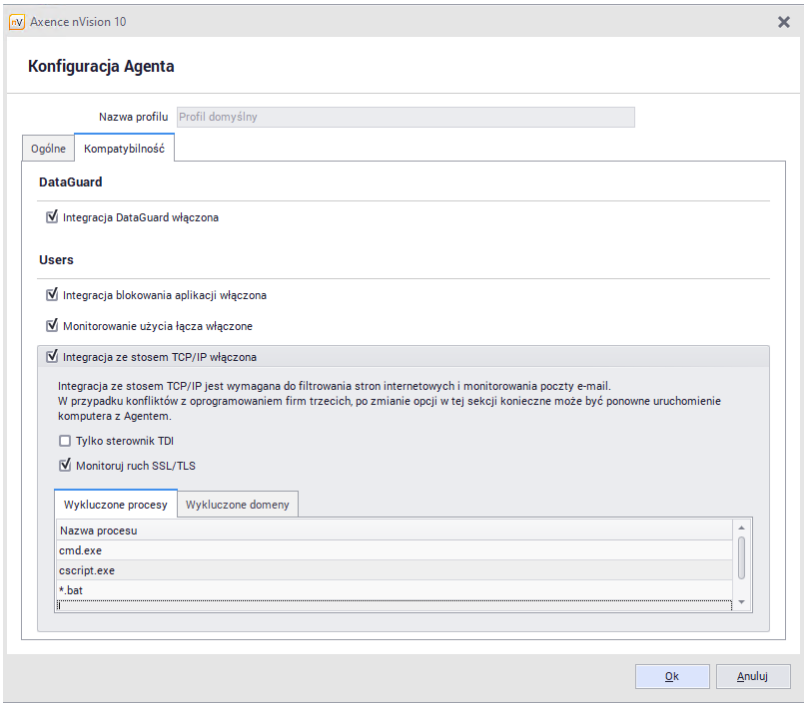
Blokowanie procesów w profilu Agenta

Aby zablokować procesy dla wszystkich urządzeń używających należy odpowiednio skonfigurować profil Agenta.

1. Przejdź do zakładki **Narzędzia i opcje** a następnie do menu **Zarządzaj profilami Agenta**.
2. Wybierz profil Agenta, który chcesz edytować lub stwórz nowy odpowiadający twoim potrzebom.

3. W oknie edycji przejdź do zakładki **Kompatybilność** a następnie do zakładki **Wykluczone procesy**.

4. Dodaj procesy, które chcesz blokować i zatwierdź przyciskiem ok.



6.4 Blokowanie dostępu do wybranych stron WWW

Strony WWW mogą być blokowane dla stacji roboczych z zainstalowanym Agentem nVision przy użyciu profili Agentów. Domyślnie, wszystkie strony mogą być otwierane. Aby możliwe było blokowanie, należy włączyć integrację ze stosem TCP/IP w zakładce **Kompatybilność i wydajność**. Aby dowiedzieć się, jak to zrobić, przejdź do rozdziału Nie mogę blokować stron www.

Obsługiwane są protokoły: HTTP, HTTPS, SMTP:25, SMTP:587, SMTP via SSL, POP3 via SSL i POP3:110. Obecnie nie są obsługiwane: IMAP, MAPI.

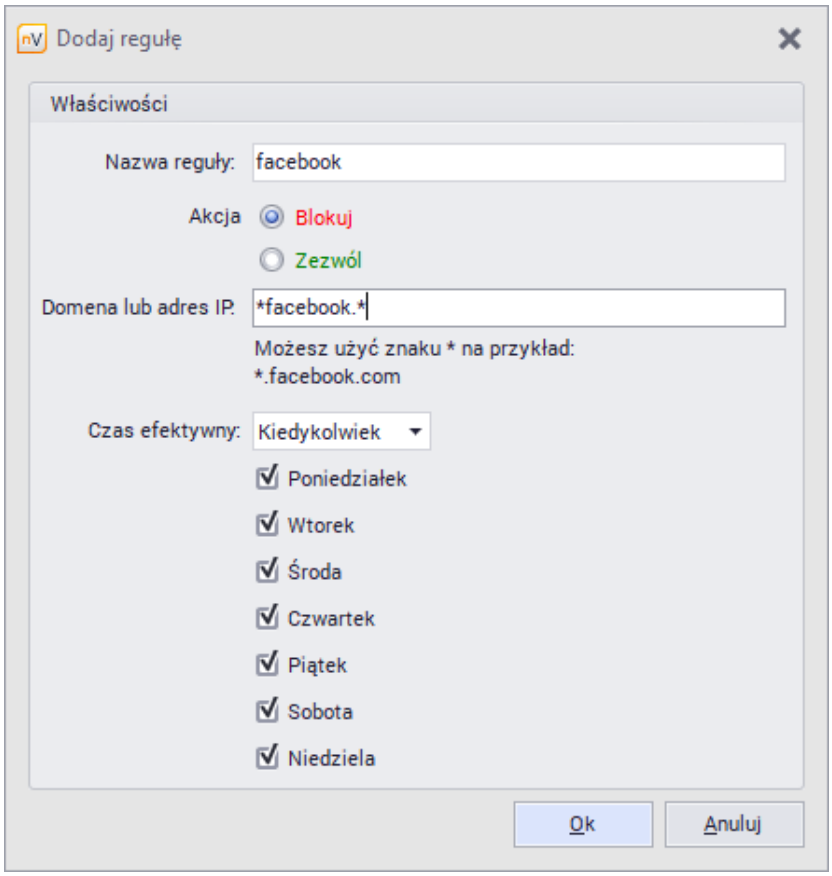
Blokowanie dostępu do stron internetowych

Model ustawień blokowania został przedstawiony w rozdziale Ustawienia blokowania.

Aby zablokować dostęp do strony:

1. Przejdź do okna **informacji o Atlasie**, grupie lub **użytkowniku**. Przejdź do zakładki **Blokady**.
2. Wybierz kartę **Filtrowanie WWW**.
3. Kliknij przycisk **Dodaj regułę**.
4. Podaj nazwę reguły, wybierz akcję **Blokuj** i podaj adres IP lub domenę, którą chcesz zablokować. Przykład reguły pokazany jest na poniższym rysunku.

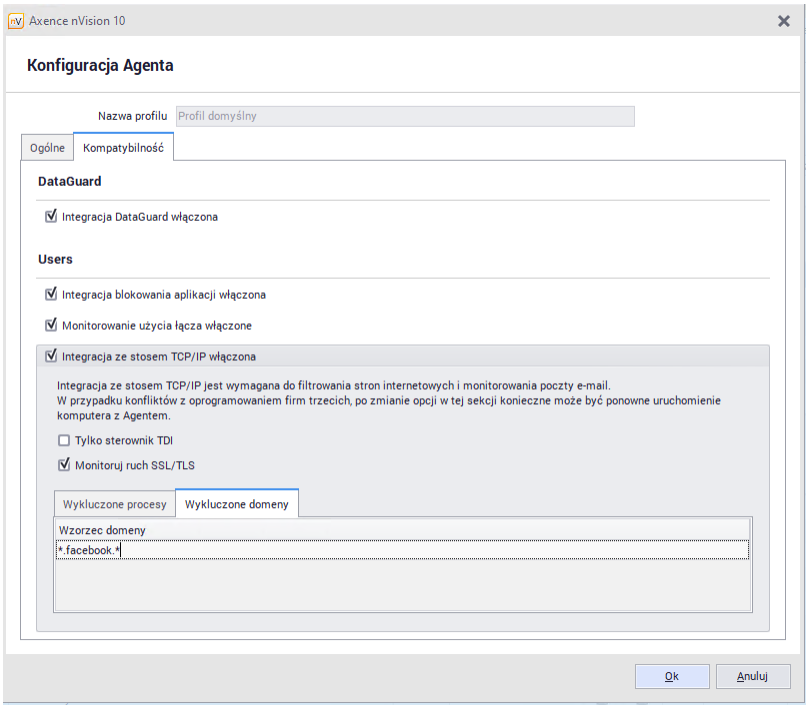
   W opcjach nVision możesz skonfigurować tekst powiadomienia, które zostanie wyświetlone użytkownikowi gdy odwiedzi zablokowaną stronę.



Wykluczanie domen w profilu Agenta

Aby wykluczyć domeny dla wszystkich urządzeń używających należy odpowiednio skonfigurować profil Agenta.

1. Przejdź do zakładki **Narzędzia i opcje** a następnie do menu **Zarządzaj profilami Agenta**.
2. Wybierz profil Agenta, który chcesz edytować lub stwórz nowy odpowiadający twoim potrzebom.
3. W oknie edycji przejdź do zakładki **Kompatybilność** a następnie do zakładki **Wykluczone domeny**.
4. Dodaj domenę, które chcesz blokować i zatwierdź przyciskiem ok.



Zakres czasu

Możliwe jest ustawienie godzin i dni, w których wybrana strona internetowa będzie blokowana. Przykładowo, można zablokować dostęp w dni robocze w godzinach pracy. W ten sposób poza przedziałem czasowym, który należy przeznaczyć na pracę, użytkownik będzie mógł uzyskać dostęp do blokowanej strony internetowej.

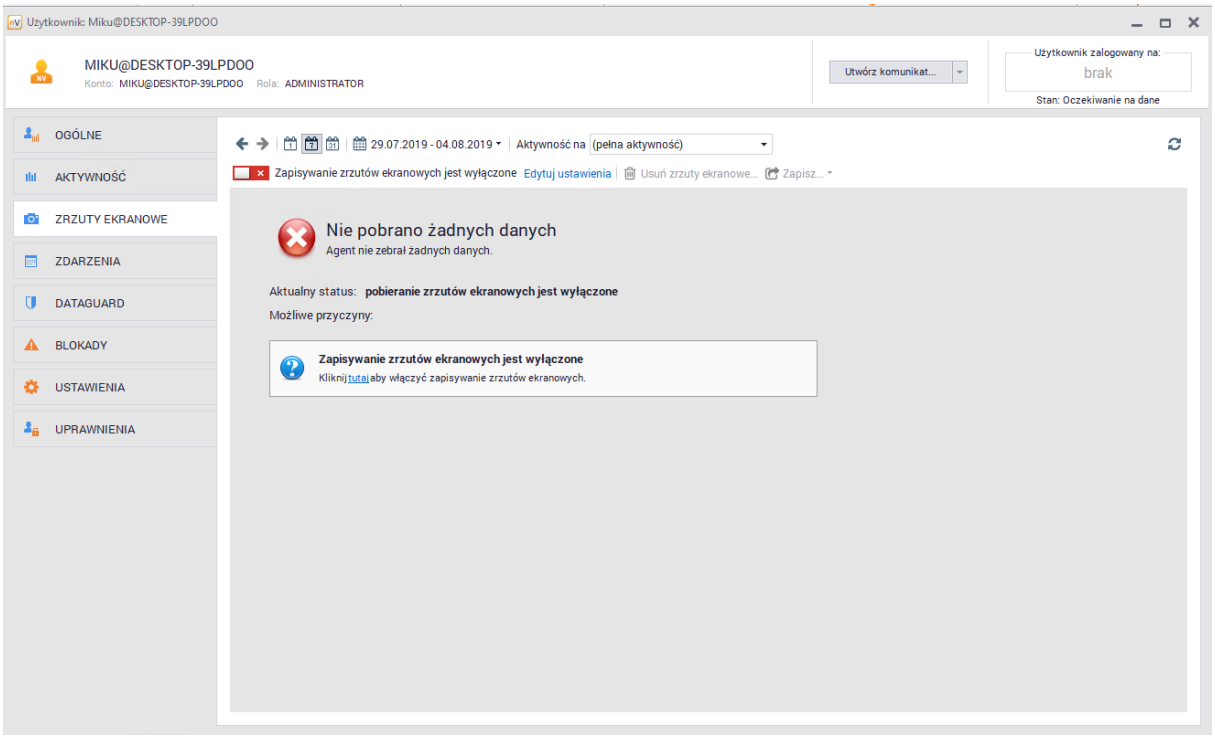
Problemy

Jeśli wystąpiły problemy z blokowaniem stron internetowych, przejdź do rozdziału Nie mogę blokować stron www, aby dowiedzieć się, jak je rozwiązać.

6.5 Zrzuty ekranowe

Zapisywanie zrzutów ekranu jest domyślnie wyłączone. Jeśli chcesz zapisywać zrzuty ekranowe cyklicznie:

1. Przejdź do karty **Zrzuty ekranowe** w oknie **Informacji o użytkowniku**.
2. Jeśli nie pobrano żadnych danych i Agent jest zainstalowany, **Włącz zapisywanie zrzutów ekranowych**.



3. Określ, jak często i do kiedy mają być wykonywane zrzuty ekranowe.
4. Poczekaj, aż Agent wyśle dane lub Odśwież .
5. Możesz przeglądać zrzuty ekranowe i zapisywać je jako pliki *. jpeg.

6.6 E-maile

Jeśli chcesz monitorować e-maile, włącz tę opcję w ustawieniach Agenta (patrz Ustawienia Agenta).

Jeśli masz problemy z monitorowaniem e-maili, przejdź do rozdziału Nie mogę blokować stron WWW i monitorować maili.

Monitorowanie maili możliwe jest tylko dla komputerów z zainstalowanym Agentem i włączoną integracją ze stosem TCP/IP.

Obsługiwane są protokoły:

- *SMTP:25,*
- *SMTP:587,*
- *SMTP via SSL,*
- *POP3 via SSL,*
- *POP3:110.*

Obecnie nie są obsługiwane: IMAP, MAPI.

Uwaga: Monitorowanie obejmuje przychodzącą i wychodzącą pocztę elektroniczną. Nadawca, odbiorca, temat i rozmiar są rejestrowane. Zawartość mail nie jest monitorowana.

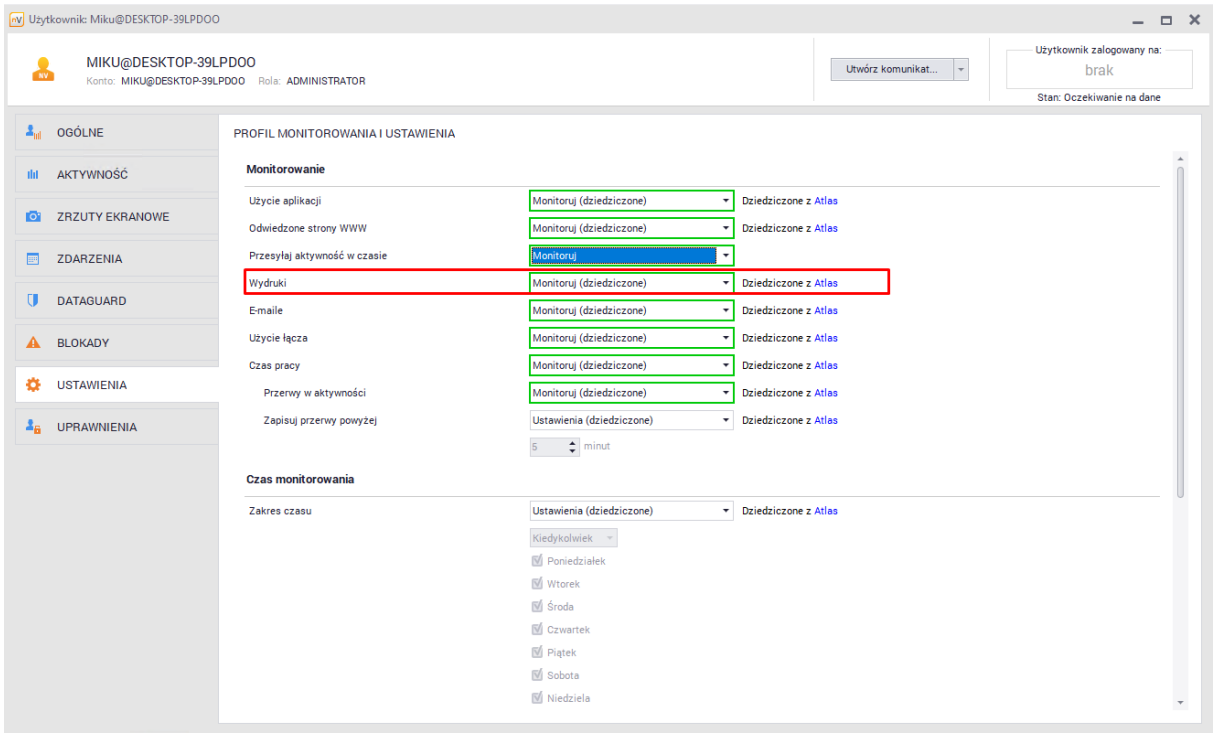
6.7 Wydruki

6.7.1 Monitorowanie wydruków

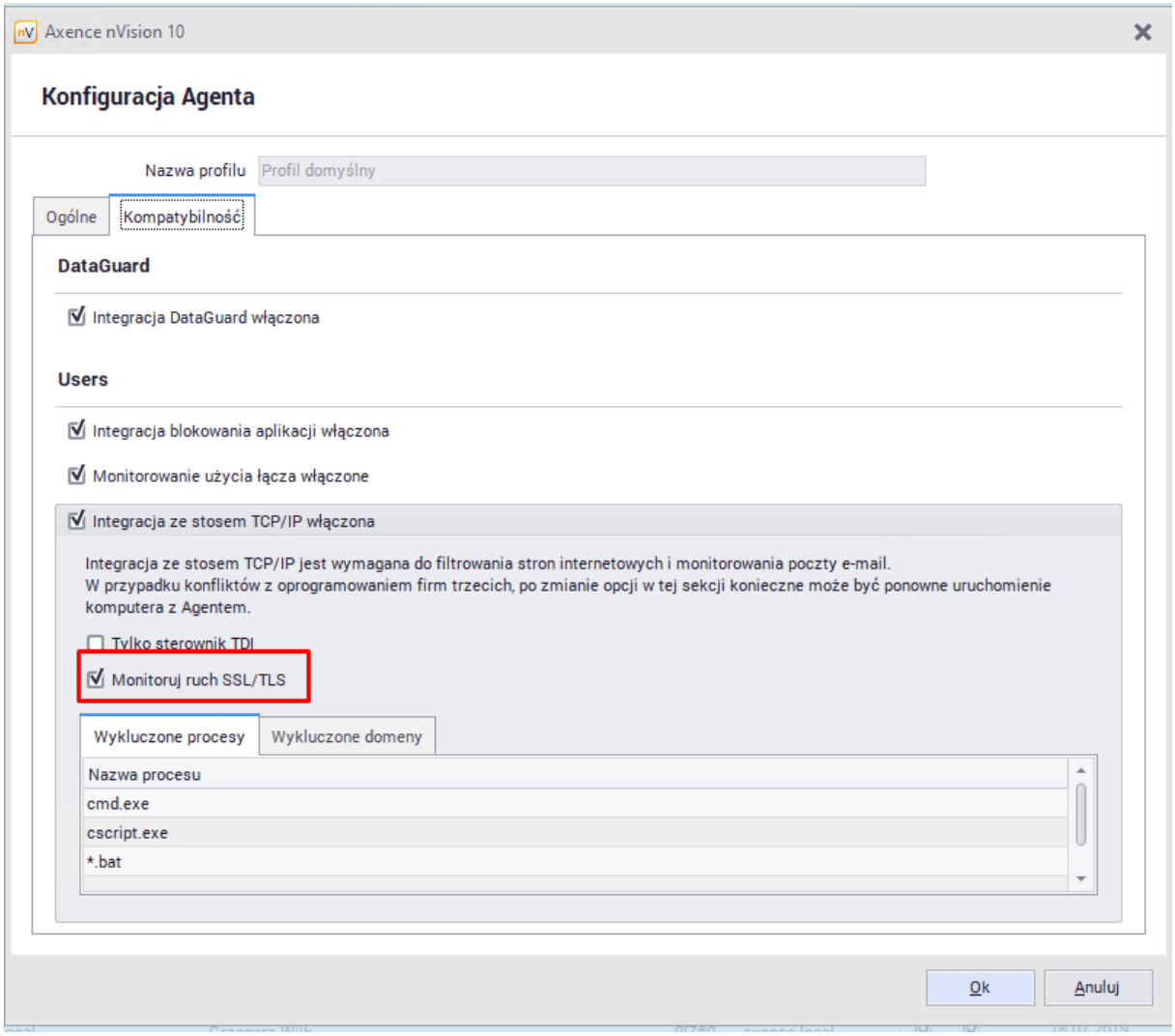
Na komputerach z zainstalowanym Agentem możliwe jest monitorowanie wydruków (po zaznaczeniu odpowiedniej opcji w ustawieniach monitorowania).

Aby włączyć monitorowanie wydruków:

1. Przejdź do okna ustawień Atlasu, grupy lub informacji o użytkowniku.
2. Przejdź do zakładki **Ustawienia.**
3. Dla opcji **Wydruki** wybierz **Monitoruj**.



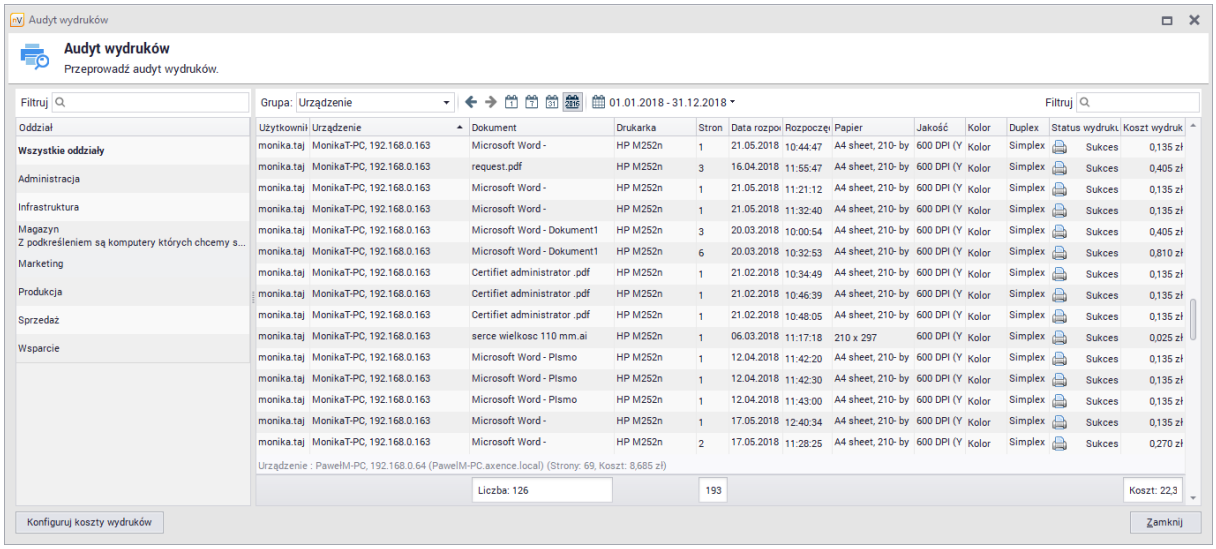
W przypadku gdy poczta używa szyfrowania SSL/TLS, należy w profilu agenta zaznaczyć odpowiednią opcję, aby korespondencja była monitorowana:



6.7.2 Audyt wydruków

Okno audytu wydruków umożliwia przeglądanie historii wydruków w wybranych okresach (dzień, tydzień, miesiąc lub rok). Dane ułożone są w porządku chronologicznym. Aby wyszukiwanie potrzebnych informacji było łatwiejsze, można użyć opcji grupowania - według użytkowników, urządzeń lub drukarek.

Aby przeprowadzić audyt wydruków, kliknij na wstążce **Audyt wydruków** (na karcie **Główne**). Zostanie otwarte okno **Audytu wydruków**.



Jeżeli dane o wydrukach nie są zbierane mimo tego, że komputery z Agentem posiadają aktualna konfigurację z zaznaczoną opcją monitorowania wydruków, zapoznaj się z rozdziałem Wydruki użytkowników nie są monitorowane.

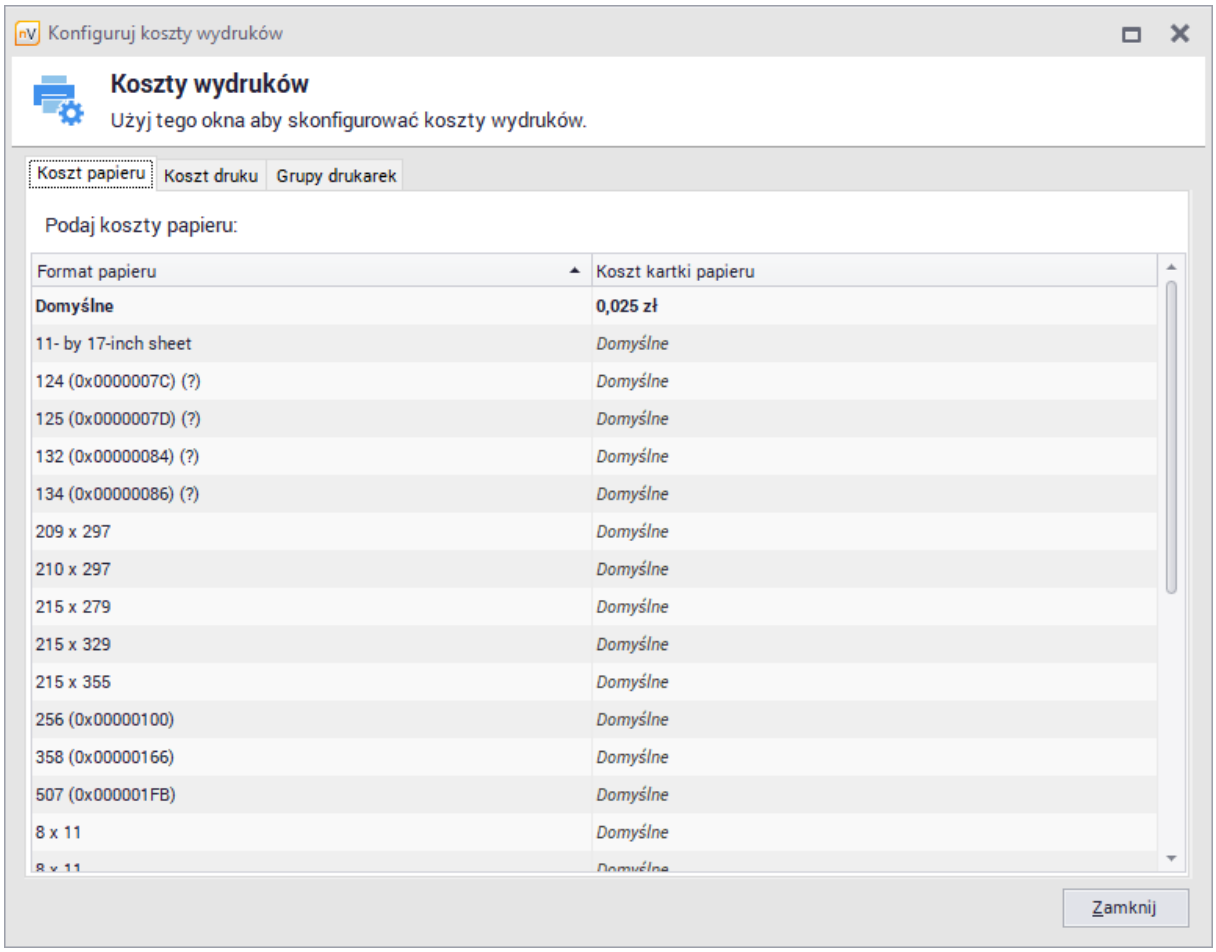
6.7.3 Koszty wydruków

Monitorowanie wydruków daje możliwość poznania kosztów, które zostały poniesione w wyniku drukowania dokumentów. Aby koszty były właściwie oceniane, należy je skonfigurować, z uwzględnieniem kosztów papieru oraz drukowania na poszczególnych drukarkach.

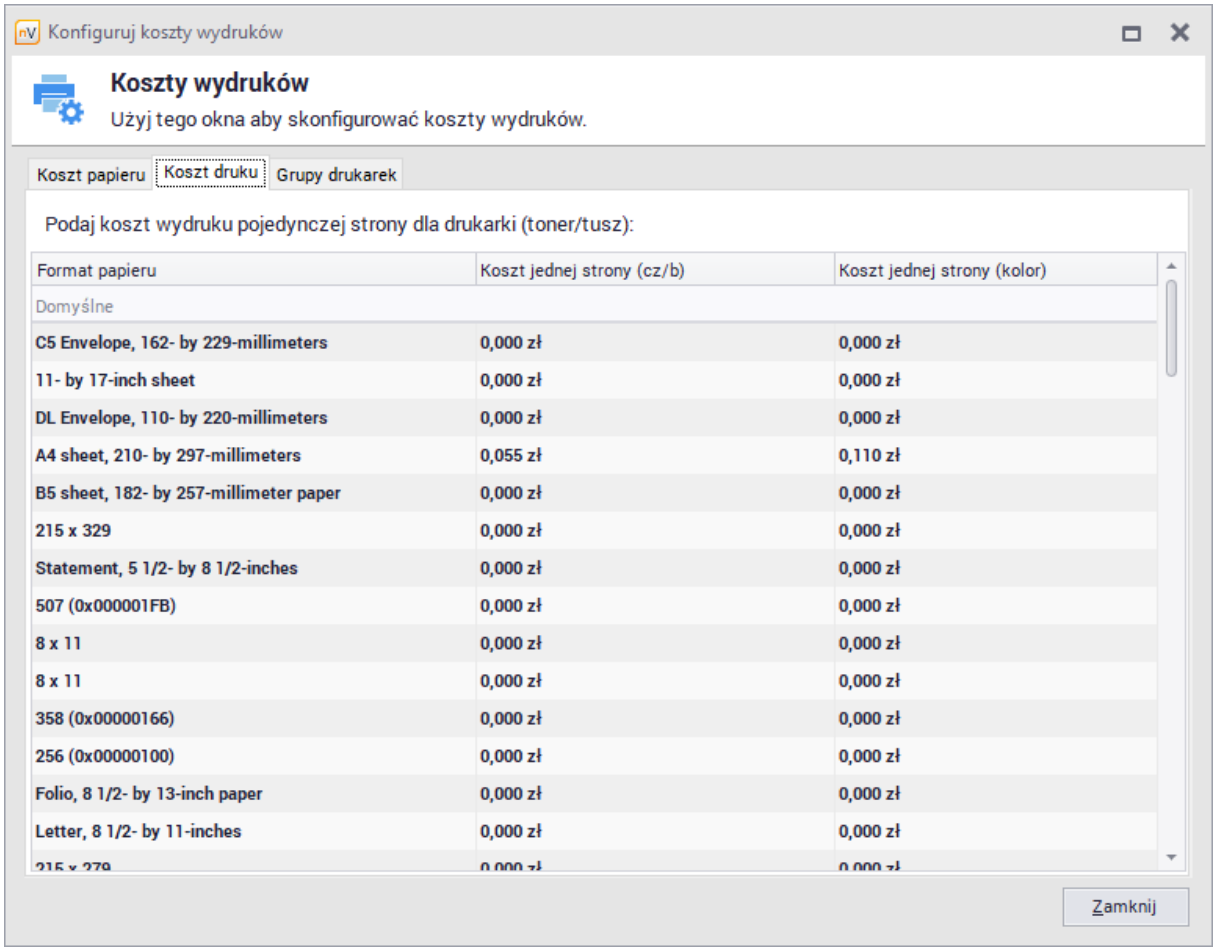
Konfiguracja

Aby skonfigurować koszty wydruków:

1. Wybierz ze wstążki opcję **Konfiguruj koszty wydruków** (na karcie **Główne**). Możesz to zrobić także z poziomu okna **Audytu wydruków**, klikając przycisk **Konfiguruj koszty wydruków**. W obu przypadkach zostanie otwarte okno **Konfiguracji kosztów wydruków**.
2. W zakładce **Koszt papieru** podaj koszty dla poszczególnych formatów papieru (A3, A4, A5, koperta). Koszt podany w komórce **Domyślne** będzie uwzględniany dla wszystkich formatów, dla których koszt nie zostanie wpisany.



3. W zakładce **Koszt druku** podaj koszty druku dla poszczególnych drukarek. Możesz podać różne koszty dla wydruków czarnych i kolorowych, a także wykorzystać wartości domyślne. Jeżeli drukarka nie drukuje w kolorze, można zaznaczyć odpowiednia opcję po kliknięciu prawym przyciskiem myszy.



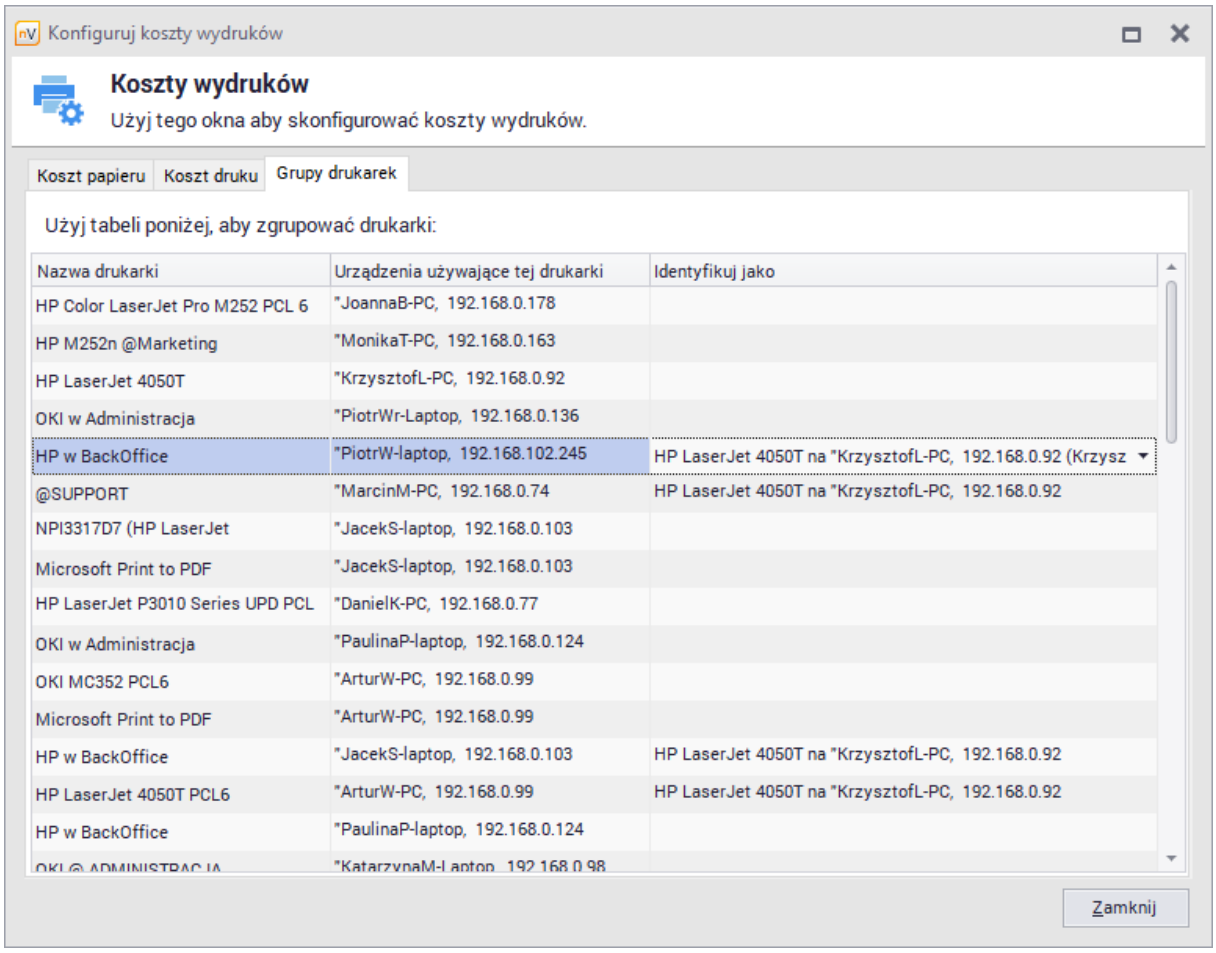
4. W obu zakładkach, jeśli chcesz przywrócić komórce wartość domyślną, kliknij w polu kosztu prawym przyciskiem myszy i wybierz opcję **Ustaw wartość komórki jako domyślną**.

Audyt kosztów wydruku

Koszty wydruków wyświetlane są w ostatniej kolumnie w oknie **Audytu wydruków**. Poniżej podany jest także sumaryczny koszt wydruków z danego okresu.

6.7.4 Grupowanie drukarek

Aby zredukować liczbę wpisów i nie podawać kosztów wydruku dla powtarzających się urządzeń można pogrupować drukarki. Ta funkcja jest dostępna w zakładce **Grupy drukarek** (w oknie **Konfiguruj koszty wydruków**).



Zakładka grupowania drukarek zawiera listę drukarek wraz z informacją o urządzeniach, które wykonywały na nich wydruki. Drukarki identyfikowane jako inne przyjmują ich koszty druku, jednak we wszystkich innych miejscach (Audyt wydruków, raporty) dalej są traktowane jako samodzielne drukarki.

Informacje praktyczne

Przy scalaniu drukarek warto zwrócić uwagę na wpisy oznaczające to samo urządzenie, któremu nadano różne nazwy na danym komputerze, a także urządzenia używane przez wielu użytkowników. Należy także wybrać jeden wpis, na podstawie którego będzie tworzona dana grupa drukarek, gdyż nVision blokuje możliwość tworzenia cyklicznych powiązań.

Aby usunąć powiązanie dla wybranej drukarki, rozwiń menu dla danego wpisu (wciskając prawy przycisk myszy) i wybierz opcję **Wyczyść 'identyfikuj jako'**.

Część VII

7 Inwentaryzacja sprzętu i oprogramowania

7.1 Wprowadzenie

Axence nVision® automatycznie gromadzi informacje o konfiguracji sprzętowej każdego komputera Windows oraz zainstalowanego na nim oprogramowania. Zadanie to jest wykonywane przez Agenta nVision raz na dobę dla każdego komputera. Inwentaryzacja za pomocą Agentów nie wpływa na bezpieczeństwo, ale wymaga zainstalowania Agentów na każdym komputerze.

Jeśli chcesz pobrać informacje dla danego urządzenia lub urządzeń szybciej, wybierz **Agent / Inwentaryzuj** z menu kontekstowego wybranego urządzenia. Można także przeprowadzać inwentaryzację dla całej mapy (wszystkich komputerów) poprzez wybranie **Inwentaryzuj** z menu kontekstowego w drzewie mapy.

Inwentaryzacja wykonywana przez Agenty

Automatyczna inwentaryzacja sprzętu i oprogramowania wymaga zainstalowania na danym komputerze Agenta nVision. Aby uzyskać więcej informacji, przejdź do rozdziału Instalowanie i odinstalowywanie Agentów.

Ręczna inwentaryzacja

Inwentaryzacja sprzętu i oprogramowania może być także wykonana bez instalowania Agentów. W tym celu należy skorzystać ze **skanera inwentaryzacji** opisanego w rozdziale Import skanów inwentaryzacji.

Zakładka Zasoby

Informacje o zasobach można znaleźć w zakładce  **Zasoby** w oknie **Informacje o urządzeniu**. Na samym początku dane te mogą być niedostępne (po przeskanowaniu sieci). Pojawią się one automatycznie, gdy tylko Agenty zakończą skanowanie komputerów i prześlą dane, co może chwilę potrwać. Jeśli dane nie pokazują się po dłuższym czasie, należy się upewnić, czy Agent jest zainstalowany i czy port 4434 na komputerze z nVision jest otwarty.

W historii inwentaryzacji urządzenia (okno **Informacje o urządzeniu / Zasoby / Historia**), po dwukrotnym kliknięciu na wierszu zawierającym publiczny adres IP Agenta otwarta zostanie strona WWW prezentująca geolokalizację adresu.

Audyt

Informacje związane z audytem sprzętu i oprogramowania można znaleźć klikając odpowiednio **Audyt sprzętowy** oraz **Audyt oprogramowania** na głównym pasku narzędziowym programu.

Powiązane tematy

Audyt oprogramowania

Audyt sprzętowy

Audyt wydruków

Import skanów inwentaryzacji

7.2 Oprogramowanie

7.2.1 Inwentaryzacja oprogramowania

Inwentaryzacja oprogramowania jest funkcją umożliwiającą kontrolę aplikacji zainstalowanych na komputerach monitorowanych użytkowników. Pozwala na kontrolę legalności programów oraz plików multimedialnych, a także na zarządzanie posiadanymi licencjami. Aby możliwe było gromadzenie informacji o programach, konieczne jest zainstalowanie Agenta nVision na każdym z komputerów, który ma być monitorowany. Oprócz tego, należy skonfigurować opcje Agenta tak, by uwzględniały skanowanie informacji o oprogramowaniu oraz, jeśli mają być kontrolowane pliki użytkownika, skanowanie plików.

Informacje o oprogramowaniu na pojedynczej stacji roboczej

Aby przeglądać informacje o programach i plikach zainstalowanych na danym komputerze:

1. Wybierz urządzenie i wciśnij Enter, aby przejść do okna **Informacji o urządzeniu**.
2. Przejdź do zakładki **Zasoby / Oprogramowanie**. Z rozwijalnej listy możesz wybrać następujące widoki:

Zakładka	Opis
Aplikacje	Lista aplikacji, systemów operacyjnych, aktualizacji i sterowników wykrytych na danym komputerze. Sposób wykrywania zainstalowanych aplikacji opisany jest w rozdziale Wzorce.
Pliki	Wszystkie pliki wykonywalne znajdujące się na danym komputerze. Nie znajdą się tu pliki uruchamiane np. z pendrive'ów.
Rejestr	Wpisy z rejestru. Między innymi na ich podstawie wykrywane są aplikacje.
Wszystko	Wszystkie wykryte aplikacje.

7.2.2 Wzorce aplikacji

Wzorce służą do identyfikowania aplikacji, sterowników i innych oraz umożliwiają zarządzanie posiadanymi licencjami. Wzorce dzielą się na dwa rodzaje - utworzone ręcznie oraz utworzone automatycznie przez nVision. Wraz z programem nVision dostarczanych jest ok. 600 ręcznie stworzonych wzorców umożliwiających rozpoznanie najczęściej używanych aplikacji. Istotną cechą tego typu wzorców jest znany typ licencji rozpoznawanych aplikacji, co pozwala na kontrolę legalności oprogramowania.

Wyróżnia się następujące typy wzorców:

Aplikacje i systemy operacyjne,

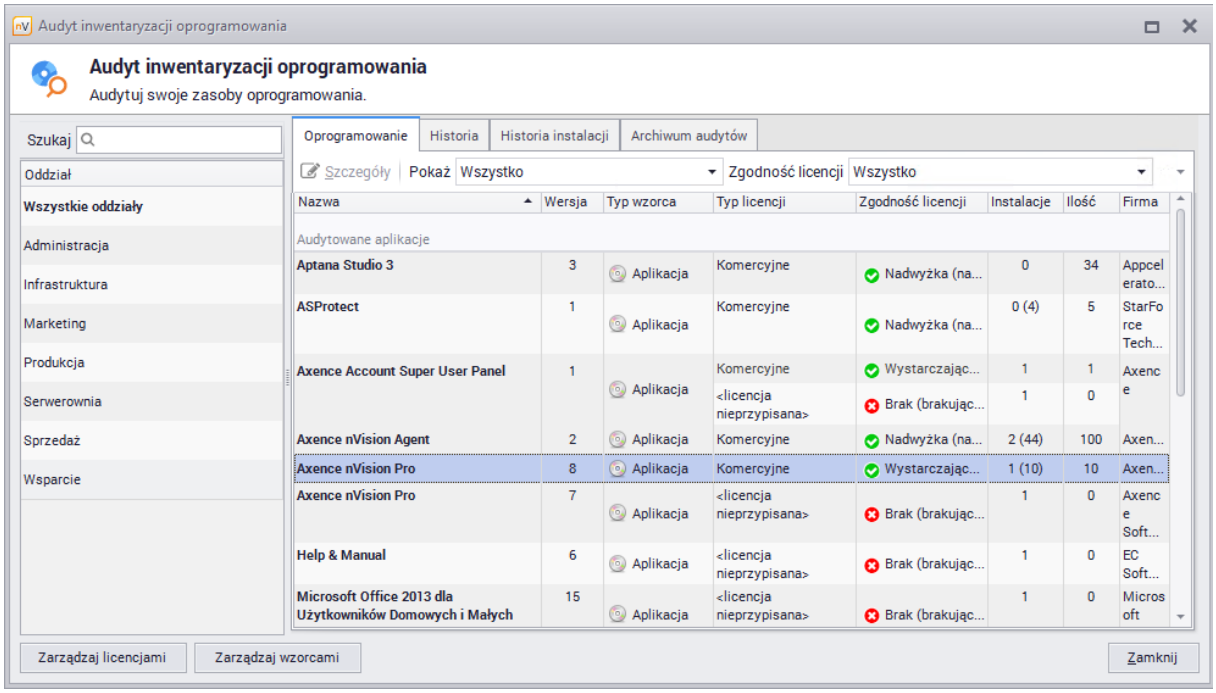
Aktualizacje bezpieczeństwa,

Sterowniki.

W dalszej części rozdziału pod pojęciem aplikacji będą rozumiane wszystkie trzy powyższe typy.

Jak wykrywane są aplikacje?

W pierwszej kolejności sprawdzane są wpisy w rejestrze. Jeśli w rejestrze istnieje wpis o danej aplikacji, to uznaje się, że jest ona zainstalowana na komputerze. Jeśli wpisu nie ma, to przeszukiwane są pliki oznaczone we wzorcach jako identyfikujące (najczęściej jest to plik *.exe umożliwiający uruchomienie programu). Jeżeli zostaną znalezione, to uznaje się, że aplikacja jest na komputerze. W przeciwnym wypadku (brak wpisów w rejestrze i plików identyfikujących) aplikacja nie zostanie wykryta.



Wzorce dostarczane z nVision

Wzorce dostarczone wraz z nVision zostały utworzone ręcznie w oparciu o programy, z których użytkownicy korzystają najczęściej. Aplikacje wykryte na podstawie tego rodzaju wzorców są wyświetlane w pierwszej kolejności, pogrubioną czcionką. Dzielą się one na licencjonowane (jeżeli znany jest typ licencji) i nielicencjonowane. Dla obu tych grup można zmieniać typ licencji oraz tworzyć środki trwałe licencji i przypisywać je do instalacji.

Wzorce utworzone automatycznie

Pozostałe wzorce są tworzone automatycznie przez nVision na podstawie wpisów w rejestrach monitorowanych komputerów. Aplikacje wykryte w ten sposób są wyświetlane w drugiej kolejności, kursywą na liście wykrytych i nieznanych aplikacji i nie jest dla nich znany typ licencji.

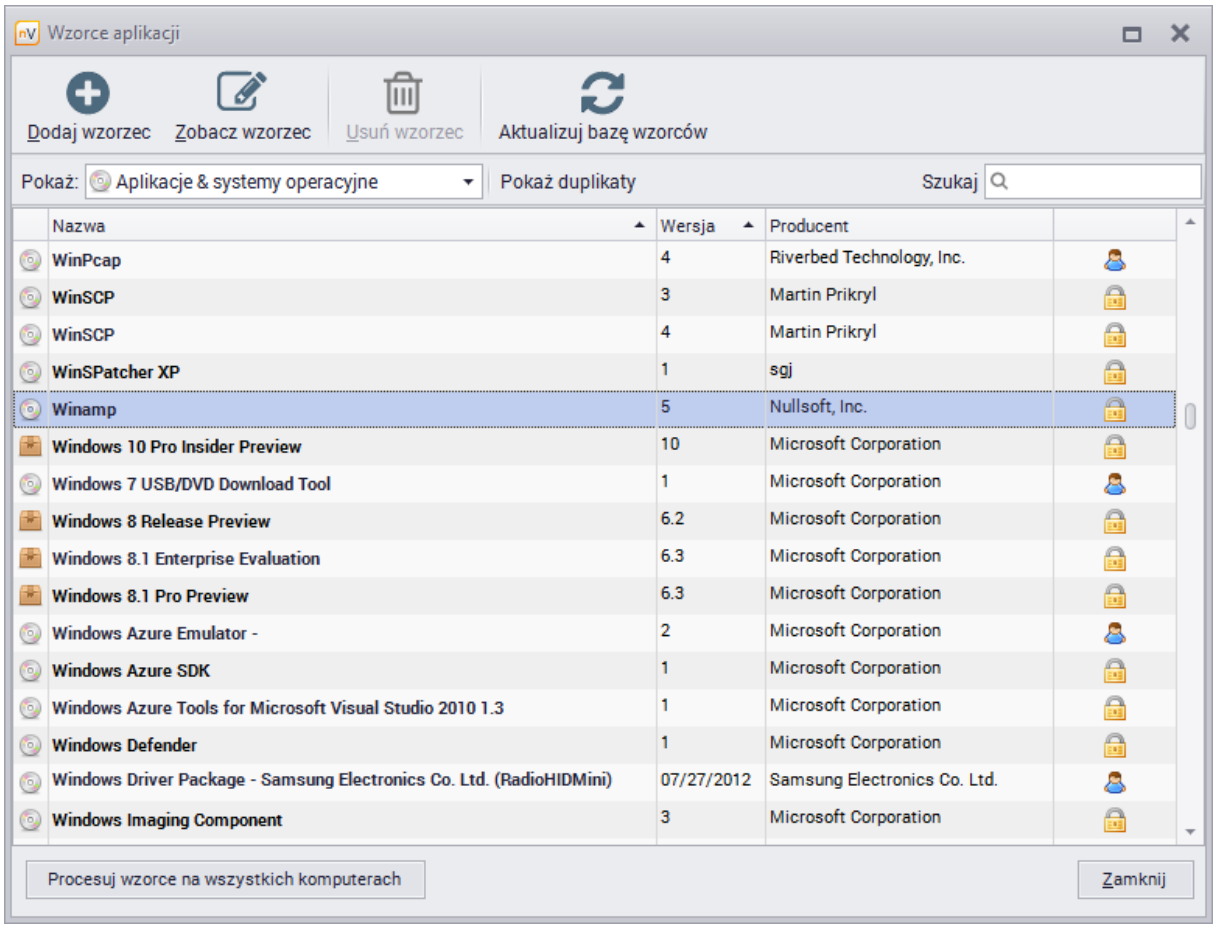
Wzorce mogą być edytowane, można je uzupełniać m. in. o typ licencji i pliki powiązane z daną aplikacją, a także pliki ją identyfikujące. Jeżeli użytkownikowi znana jest aplikacja z listy wykrytych i nieznanych, to zaleca się edycję jej wzorca. Dodanie do wzorca typu licencji powoduje przeniesienie go do grupy wzorców utworzonych ręcznie i skutkuje wykryciem aplikacji na wszystkich komputerach, na których jest zainstalowana.

Powiązane tematy

- Jak utworzyć wzorzec?
- Zarządzanie wzorcami
- Zarządzanie licencjami
- Środki trwałe

7.2.3 Zarządzanie wzorcami

Aby przejść do wzorców należy z głównego menu (sekcja Oprogramowanie) wybrać pozycję **Zarządzaj wzorcami.**



Wzorce oznaczone ikoną zostały utworzone przez Axence i nie można ich zmieniać. Z kolei oznaczone ikoną to wzorce utworzone przez użytkowników lub automatycznie na podstawie wpisów w rejestrze i mogą być edytowane.

Aby dowiedzieć się, w jaki sposób edytuje się wzorce, przejdź do rozdziału Jak utworzyć wzorzec?.

Aktualizacja bazy wzorców

Wybierając funkcję **Aktualizuj bazę wzorców** nVision pobierze najnowsze dostępne wzorce z serwera Axence oraz doda je do nVision.

7.2.4 Tworzenie wzorca

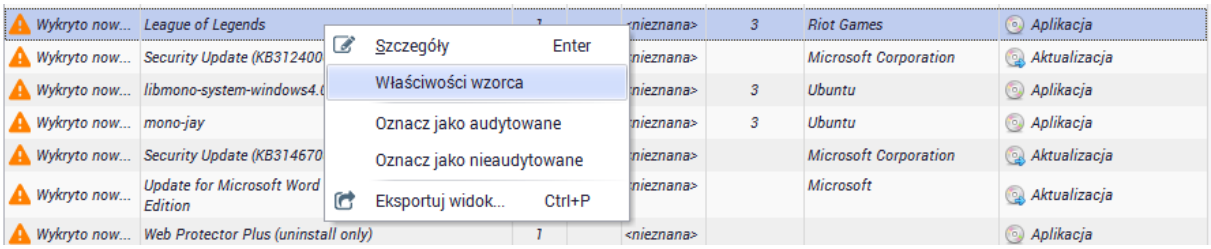
Aby utworzyć kompletny wzorzec należy edytować informacje w oknie wzorca aplikacji. Niektóre wzorce utworzone automatycznie przez nVision powstają na podstawie wpisów w rejestrze i nie zawierają informacji o typie licencji, często także o plikach powiązanych z aplikacją.

Uzupełnianie wzorców

Zmieniane mogą być wyłącznie wzorce aplikacji, które nie są znane przez nVision. Aby uzupełnić wzorzec, należy otworzyć okno wzorca aplikacji. Można to zrobić na kilka sposobów:

1. Z poziomu okna **Audytu oprogramowania**

   Kliknij w przycisk **Audyt oprogramowania** znajdujący się na głównym pasku narzędziowym. Zostanie otwarte okno **Audytu inwentaryzacji oprogramowania**. Wybierz z listy aplikację, której wzorzec chcesz edytować, kliknij na niej prawym przyciskiem myszy i wybierz opcję **Właściwości wzorca**.



2. Z poziomu okna **Informacji o urządzeniu**

   Wybierz urządzenie i przejdź do okna informacji o nim. Następnie przejdź do zakładki **Zasoby / Oprogramowanie**. Następnie wybierz z listy aplikację, której wzorzec chcesz edytować, kliknij na niej prawym przyciskiem myszy i wybierz opcję **Właściwości wzorca**.

3. Z poziomu okna **Zarządzania wzorcami**

   Z głównego paska narzędziowego wybierz opcję **Zarządzaj wzorcami**. Wybierz z listy aplikację, której wzorzec chcesz edytować i kliknij w przycisk **Edytuj wzorzec** .

   Dla wzorców utworzonych przez Axence **wyłączona** jest możliwość edycji - można je jedynie zobaczyć.

Tworzenie nowych wzorców

Aby utworzyć nowy, na razie pusty, wzorzec:

1. Z głównego paska narzędziowego wybierz opcję **Zarządzaj wzorcami.**
2. Kliknij w przycisk **Dodaj wzorzec** . Zostanie otwarte okno **Wzorca aplikacji**, przy czym wszystkie pola będą puste.

Można też utworzyć wzorzec na podstawie plików wykrytych u użytkownika i niepowiązanych z żadnym wpisem w rejestrze. Aby utworzyć wzorzec:

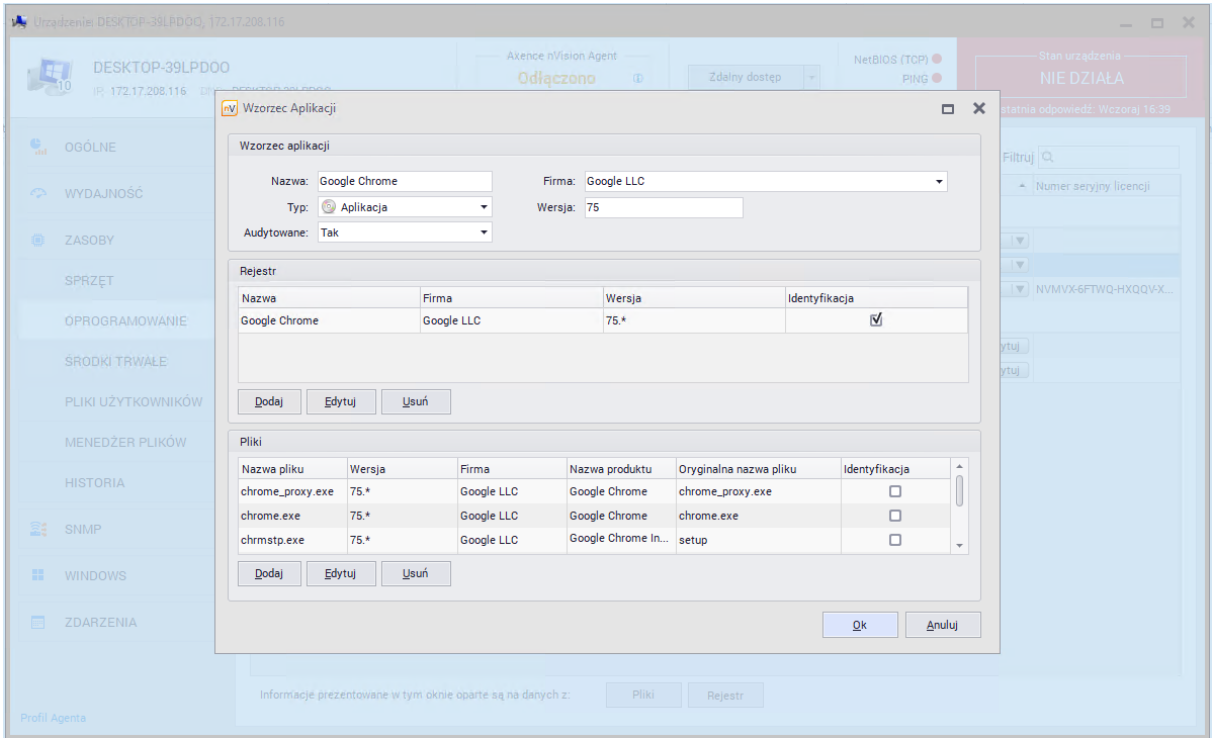
1. Wybierz urządzenie i przejdź do okna informacji o nim. Następnie przejdź do zakładki **Zasoby / Oprogramowanie / Pliki**.

2. Pliki oznaczone ikoną są już przypisane do aplikacji. Pozostałe mogą zostać ręcznie przypisane do istniejących wzorców lub można na ich podstawie utworzyć nowy wzorzec. W tym celu wybierz plik i kliknij na nim prawym przyciskiem myszy. Wybierz z menu opcję **Przypisz do wzorca aplikacji**. Zostanie otwarte okno **Kreatora wzorców**.
3. Jeżeli chcesz dodać plik do istniejącego wzorca, to wybierz opcję **Dodaj zaznaczenie do istniejącego wzorca**, przejdź **Dalej**, wybierz aplikację z listy i **Zakończ** działanie.
4. Aby utworzyć nowy wzorzec, zaznacz opcję **Utwórz nowy wzorzec** i przejdź **Dalej**. Następnie możesz dodać do tworzonego wzorca wpisy z rejestru (jeżeli nie zostały wykryte automatycznie, to można wybrać je z listy). **Zakończ**. Zostanie otwarte okno **Wzorca aplikacji**, opisane w następnym podrozdziale.

Okno Wzorca aplikacji

Aby utworzyć kompletny wzorzec aplikacji, należy uzupełnić pola w oknie tego wzorca. Znajdują się tam następujące pola:

Pole	Opis
Wzorzec aplikacji	Znajdują się tu następujące informacje o aplikacji: • nazwa, • firma, • typ (aplikacja, system operacyjny, aktualizacja lub sterownik), • wersja, • audytowane. Szczególnie istotne jest podanie informacji o licencjonowaniu danej aplikacji, gdy dla nVision jest ona Nieznana.
Rejestr	Lista wpisów w rejestrze powiązanych z daną aplikacją. Aby dodać wpis, kliknij w przycisk **Dodaj**, następnie **Załaduj rejestr** i wybierz z listy stosowny wpis. Jeżeli dany wpis identyfikuje aplikację (jego istnienie oznacza, że aplikacja jest zainstalowana a licencja użyta), to zaznacz pole **Identyfikuje** przy tym wpisie.
Pliki	Lista plików wykonywalnych danej aplikacji. Aby dodać plik, kliknij w przycisk **Dodaj**, następnie **Załaduj plik** i wybierz z listy stosowny wiersz. Jeżeli istnienie danego pliku oznacza, że program może być używany a licencja jest wykorzystana, to zaznacz pole **Identyfikuje** przy tym pliku.



Na powyższym obrazku niektóre pola i przyciski są nieaktywne, ponieważ jest to wzorzec dostarczony wraz z nVision i zablokowana jest możliwość edycji tych pól. Jako identyfikujący oznaczony jest plik pozwalający na uruchomienie aplikacji.

Aby dowiedzieć się więcej o wzorcach, przejdź do rozdziału Wzorce.

Aby dowiedzieć się więcej o przypisywaniu licencji, przejdź do rozdziału Zarządzanie licencjami.

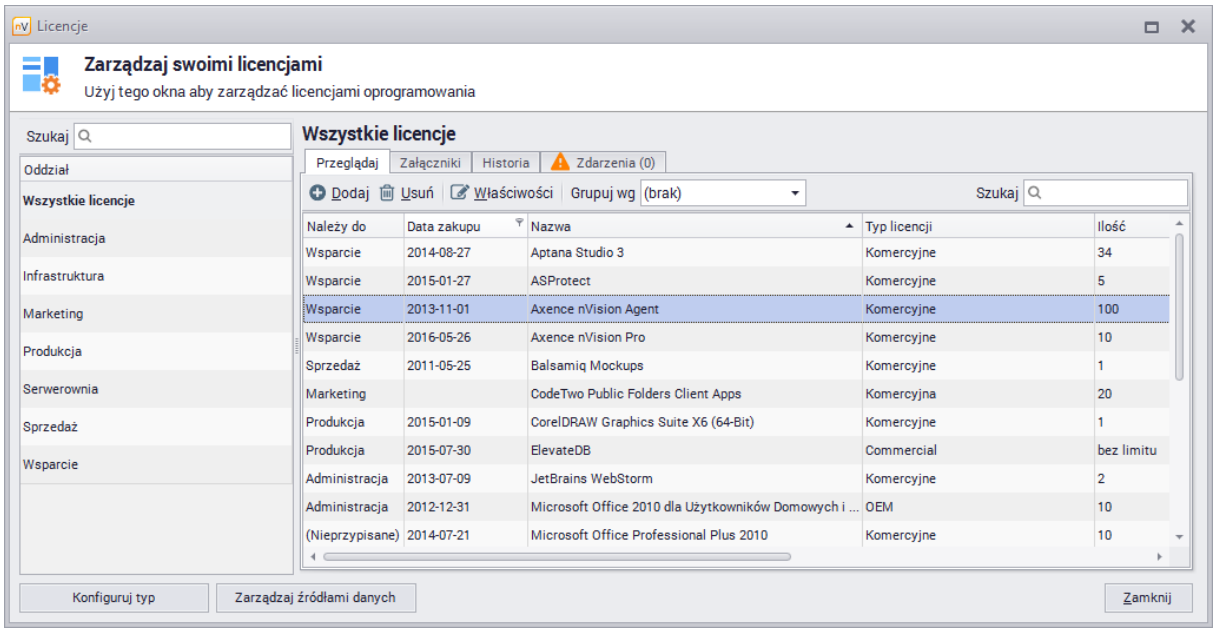
7.2.5 Zarządzanie licencjami

Przy dużej liczbie używanych aplikacji trudna może być kontrola legalności używanego oprogramowania oraz sprawdzanie, czy liczba zainstalowanych kopii programu nie przekracza liczby zakupionych licencji. Zarządzanie licencjami z poziomu nVision ułatwia dokonanie powyższych czynności.

Aby zarządzać licencjami:

1. Z głównego paska narzędziowego wybierz opcję **Zarządzaj licencjami**. Wyświetlana jest lista posiadanych licencji, przy czym kolumna **Instalacje** dotyczy liczby instalacji powiązanych z daną licencją, a kolumna **Ilość** podaje całkowitą liczbę licencji o danej nazwie.

2. W celu dodania licencji kliknij w przycisk **Dodaj**. Następnie, w oknie dodawania licencji, wybierz z listy program, którego dotyczy dodawana licencja. Podaj numer inwentarzowy, ewentualną przynależność do oddziału i szczegóły licencji. Możesz także dodać załączniki (np. skan faktury zakupu). Po zakończeniu uzupełniania pól, kliknij przycisk **OK**.

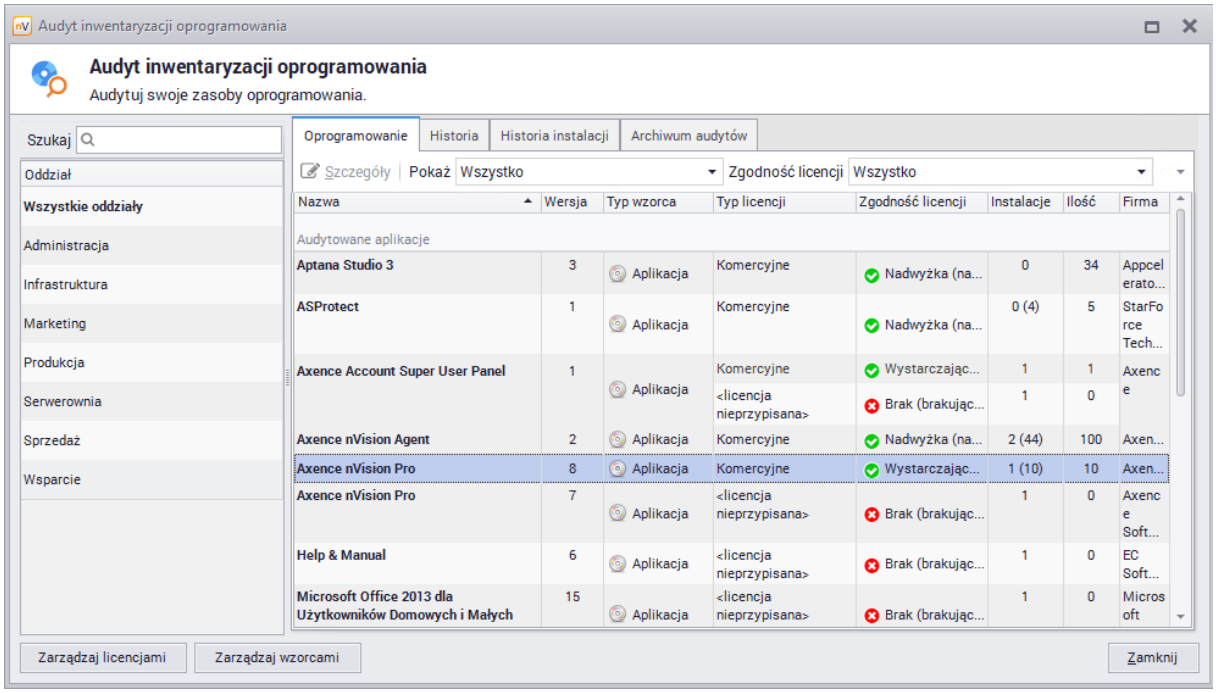


3. Aby edytować licencję kliknij dwukrotnie na wierszu z daną licencją lub zaznacz ją i kliknij w przycisk **właściwości.**

Wprowadzone w powyższy sposób licencje będą uwzględnione w oknie **Audytu inwentaryzacji oprogramowania**. Jeżeli liczba posiadanych licencji jest niewystarczająca, informacja o licencjach dla danej aplikacji zostanie wyświetlona w kolorze czerwonym. W przeciwnym wypadku (gdy liczba instalacji jest mniejsza lub równa liczbie posiadanych licencji) - w zielonym.

7.2.6 Audyt inwentaryzacji oprogramowania

Aby przejść do audytu inwentaryzacji oprogramowania, należy kliknąć w opcję **Audyt oprogramowania** znajdującą się w głównym pasku narzędziowym.

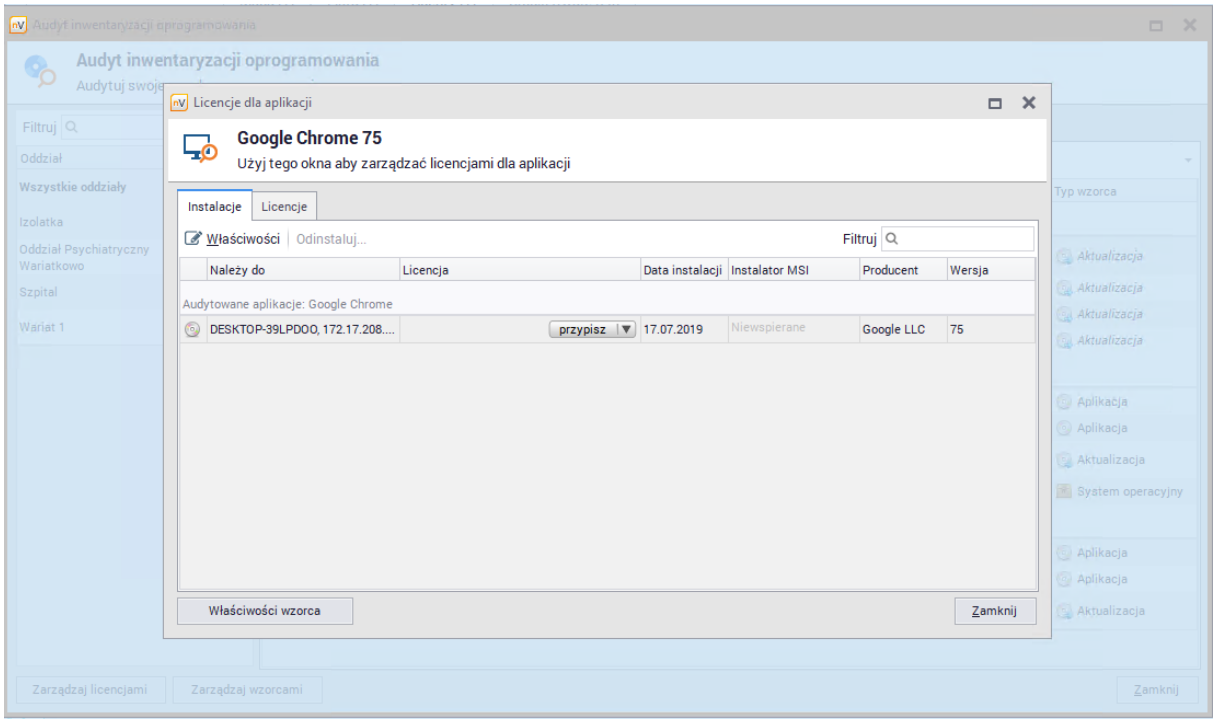


W oknie **Audytu inwentaryzacji oprogramowania** znajduje się lista aplikacji wykrytych na monitorowanych komputerach. W przypadku rozpoznanych programów pojawia się typ licencji oraz liczbę posiadanych licencji w zestawieniu z liczbą wykorzystanych licencji (kolumna Instalacje), czyli liczby stacji roboczych, na których dana aplikacja jest zainstalowana i powiązana z daną licencją.

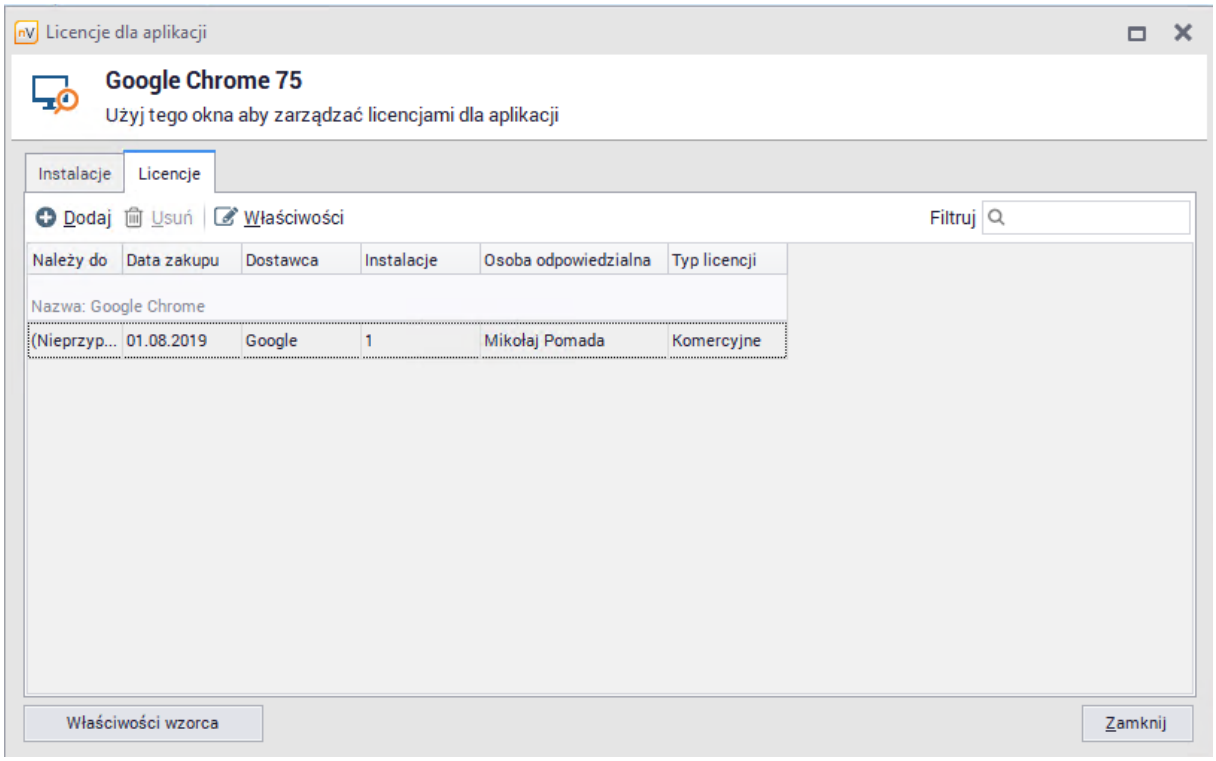
Urządzenia z zainstalowaną aplikacją i licencje

Aby zobaczyć, na których komputerach jest zainstalowana dana aplikacja, należy ją zaznaczyć i kliknąć w przycisk **Szczegóły**.

W zakładce **Instalacje** można przeglądać urządzenia z zainstalowaną aplikacją, **przypisywać** i **edytować** licencje dla wyświetlanych instalacji. Wybranie opcji **Wyczyść licencję** powoduje usunięcie powiązania pomiędzy instalacją a licencją. Aplikacja audytowana, która ma przypisaną licencję będzie widoczna w widoku **Środków trwałych.** Z kolei opcja **Oznacz jako nielicencjonowane** zmienia aplikację na nielicencjonowaną i usuwa ją ze Środków Trwałych.



W zakładce **Licencje** można dodawać, usuwać i edytować licencje dla danej aplikacji. W szczególności, dla pojedynczej aplikacji możliwe jest posiadanie kilku grup licencji, które różnią się np. datą wygaśnięcia (lub dowolnymi innymi szczegółami).



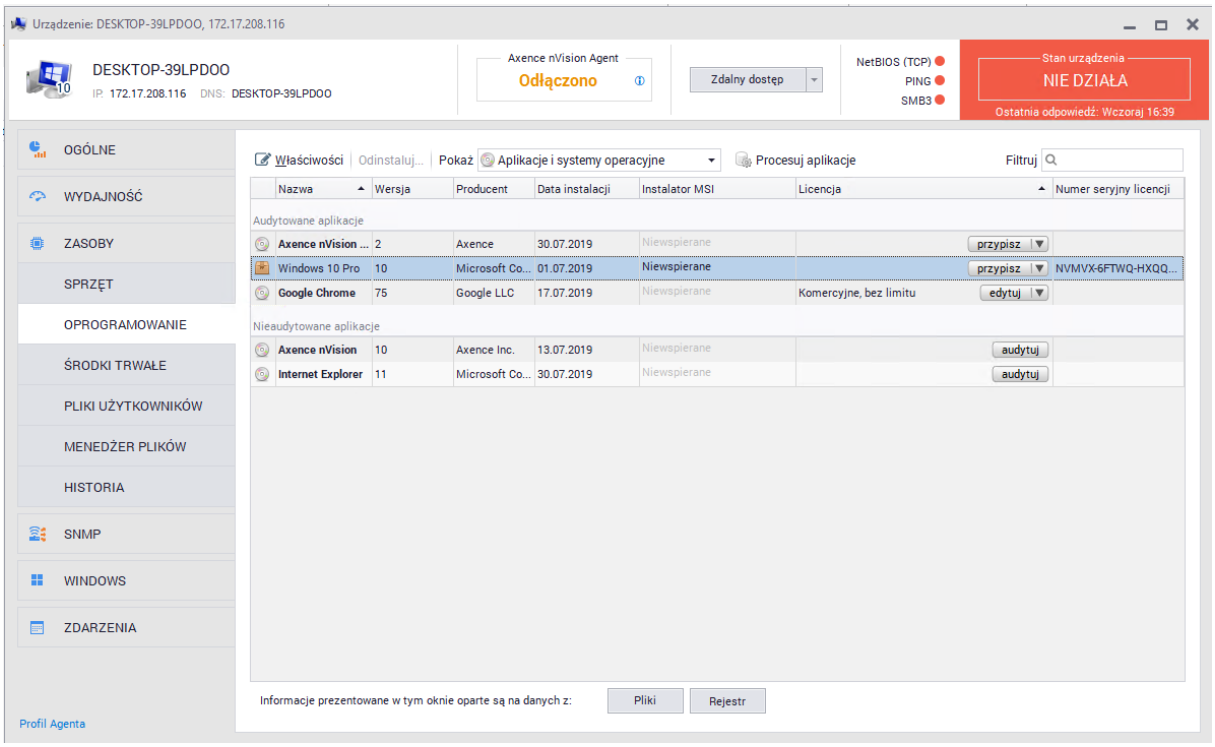
7.2.7 Numery seryjne

Numery seryjne (klucze licencyjne) dla Microsoft SQL Serwer / Windows / Office / VisualStudio odczytywane są razem z listą aplikacji. Użytkownik ma także możliwość dodawania numerów dla innych aplikacji oraz edytowania numerów wykrytych przez Agenta.

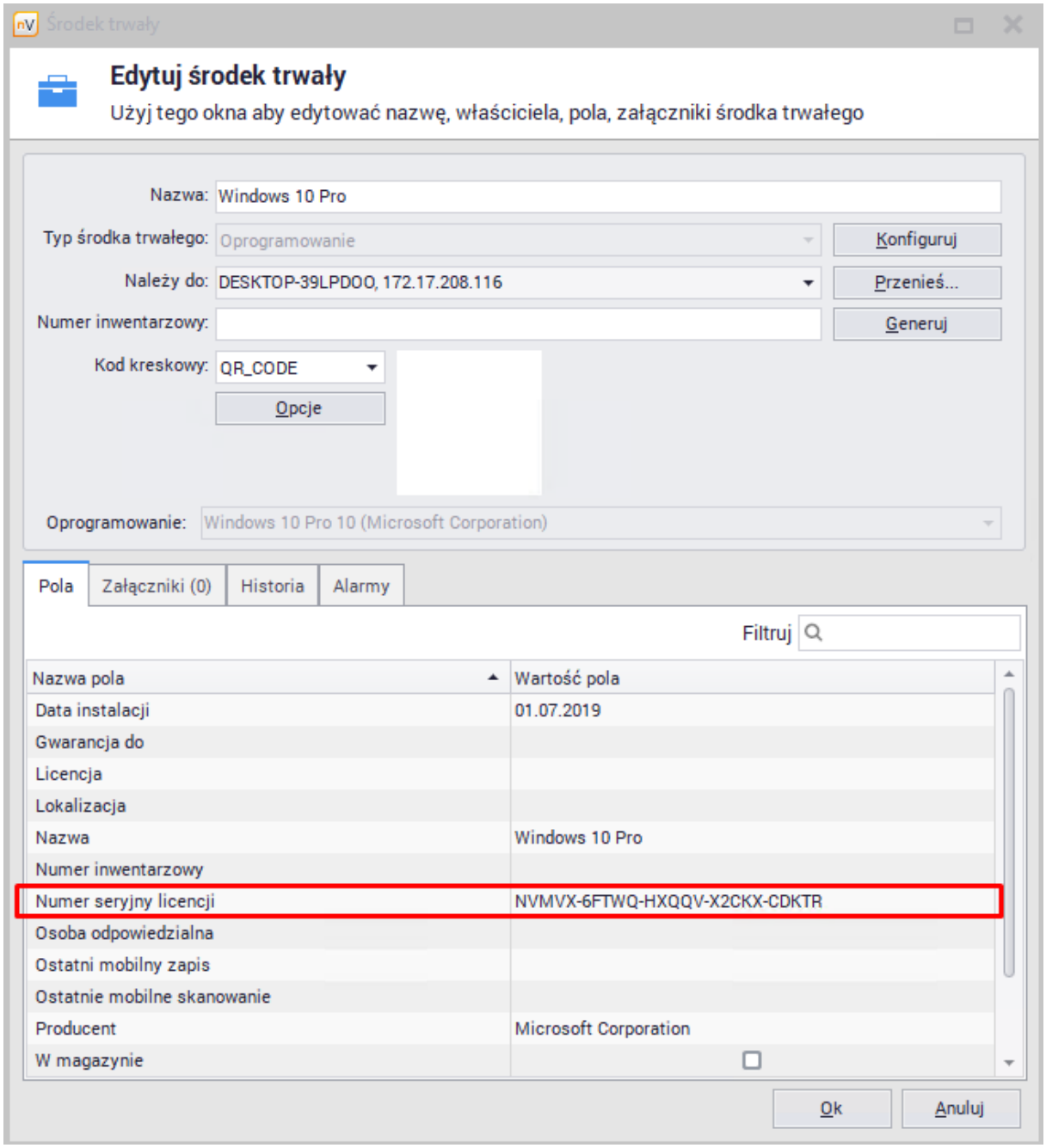
Edycja numerów seryjnych

Aby dodać lub zmienić klucz licencyjny dla aplikacji z poziomu urządzenia:

1. Przejdź do informacji o danym urządzeniu, zakładka **Zasoby / Oprogramowanie**.



2. Wybierz z listy aplikację, dla której chcesz podać numer seryjny i kliknij we **własciwosci**.
3. W oknie **Edycji środka trwałego** uzupełnij pole **Numer seryjny licencji** i kliknij **OK**.



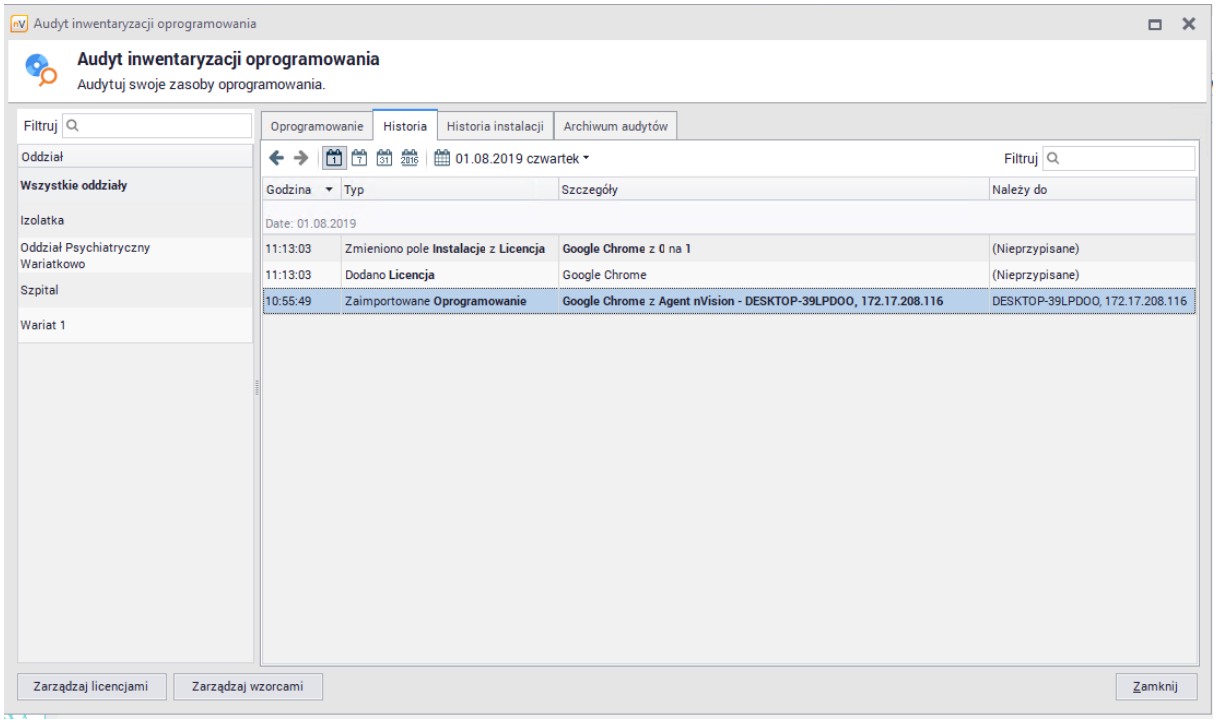
Audyt inwentaryzacji oprogramowania

Klucze licencyjne są widoczne także z poziomu okna **Audytu oprogramowania**. Aby przeglądać klucze licencyjne, wyświetl listę komputerów, na których zainstalowana jest dana aplikacja (kliknij prawym przyciskiem myszy na odpowiednim wierszu na liście programów i wybierz opcję **Szczegóły**). Zostanie wyświetlona lista urządzeń, na których dana aplikacja została wykryta. W ostatniej kolumnie prezentowane są numery seryjne, które, w razie potrzeby, można z tego miejsca uzupełniać.

7.2.8 Historia

Aby przeglądać historię zmian w aplikacjach, ich licencjach i przypisaniu do urządzeń, kliknij w ikonę **Audyt oprogramowania** znajdującą się na głównym pasku narzędziowym i przejdź do zakładki **Historia**.

W zakładce **Historia instalacji** znajduje się historia operacji instalacji i deinstalacji aplikacji na monitorowanych urządzeniach.



7.3 Sprzęt

7.3.1 Inwentaryzacja sprzętu

Inwentaryzacja sprzętu umożliwia kontrolowanie liczby i rodzaju urządzeń w monitorowanych sieciach. Dostarcza szczegółowych informacji na temat podzespołów danego urządzenia oraz wszystkich urządzeń do niego podłączonych. Wymaga zainstalowania Agenta nVision na każdym z komputerów, które mają być monitorowane. Agenta należy też odpowiednio skonfigurować, włączając opcję skanowania informacji o sprzęcie.

Skanowanie informacji o sprzęcie jest zawsze **włączone**. W zakładce **Zasoby / Sprzęt** można zapoznać się z aktualną konfiguracją sprzętową urządzenia.

Inwentaryzacja sprzętu i oprogramowania może być także wykonana bez instalowania Agentów. W tym celu należy skorzystać ze **skanera inwentaryzacji** opisanego w rozdziale Import skanów inwentaryzacji.

7.3.2 Monitorowane informacje o sprzęcie

Zebrane dane dotyczące urządzenia mogą być przeglądane w oknie **Informacji o urządzeniu**. Ze względu na dużą ilość zgromadzonych informacji, zostały one podzielone na dwie zakładki: **Ogólne** oraz **Szczegóły**.

Widok ogólny

W widoku ogólnym zostały zebrane najbardziej istotne informacje dotyczące sprzętu związanego z danym urządzeniem. W szczególności, są to wybrane informacje o komputerze, procesorze, pamięci, systemie operacyjnym, wyświetlaniu i inne.

Nie jest możliwe ręczne uzupełnienie brakujących danych.

Widok szczegółowy

Aby uzyskać dostęp do pełnych informacji o sprzęcie na monitorowanym komputerze, należy przejść do zakładki **Szczegóły**. W widoku szczegółowym można przeglądać dane z podziałem na:

- System operacyjny
- Komputer
- Płytę główną
- BIOS
- Procesory
- Pamięć
- Dyski elastyczne
- Dyski twarde
- Dyski optyczne
- Dyski logiczne
- Monitory
- Karty graficzne
- Urządzenia wejścia
- Urządzenia dźwiękowe
- Urządzenia sieciowe
- Drukarki
- Seryjne porty

7.3.3 Audyt inwentaryzacji sprzętu

Aby przejść do audytu inwentaryzacji sprzętu, należy kliknąć w opcję **Audyt sprzętowy** znajdującą się w głównym pasku narzędziowym.

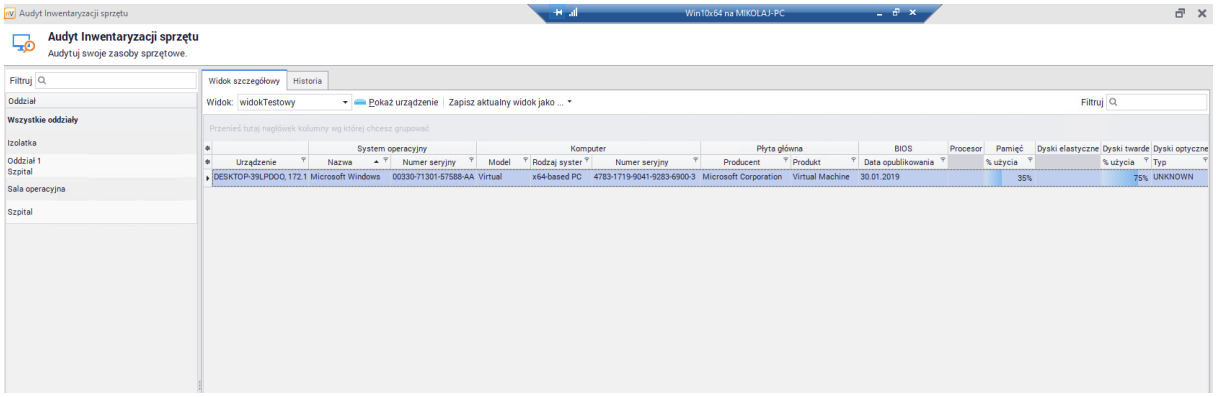
Widok szczegółowy

W widoku szczegółowym można przeglądać wszystkie dane dotyczące sprzętu, jakie zostały wysłane przez Agentów zainstalowanych na monitorowanych komputerach oraz skany sprzętu, które zostały zaimportowane do programu. Dla ułatwienia wprowadzono możliwość grupowania danych przy pomocy widoków. Można skorzystać z jednego z istniejących widoków (np. Wszystkie kolumny, Podstawowy, Multimedia) lub stworzyć własny.

Aby stworzyć własny widok, należy wybrać kolumny, które maja się w nim znaleźć. Najłatwiej to wykonać w następujący sposób:

1. Wybierz widok **Wszystkie kolumny** z listy dostępnych widoków.
2. Kliknij w jeden z przycisków * znajdujących się w lewym górnym rogu tabeli. Górny zawiera listę grup kolumn (wymienione w rozdziale Monitorowane dane), a dolny listę wszystkich kolumn, które mogą być wyświetlane. Zaznacz kolumny, które chcesz wyświetlić.

3. Aby zachować stworzony widok, kliknij w przycisk **Zapisz aktualny widok jako** i wprowadź unikalną nazwę widoku. Od tej pory będzie możliwe wybranie stworzonego widoku z listy.

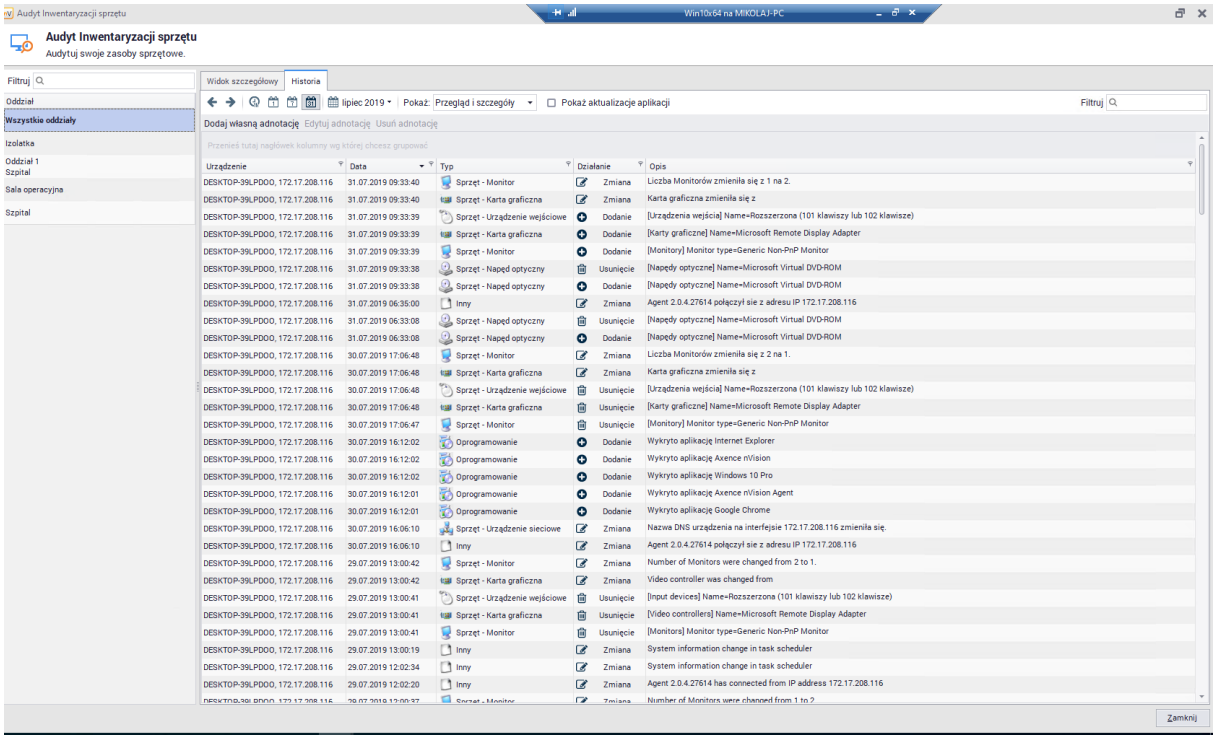


7.3.4 Historia

Zakładka **Historia** umożliwia przeglądanie zmian sprzętu i oprogramowania w wybranym przedziale czasowym dla wszystkich monitorowanych urządzeń należących do danego atlasu.

Aby przeglądać historię zmian w sprzęcie i aplikacjach, kliknij w ikonę **Audyt sprzętowy** znajdującą się na głównym pasku narzędziowym i przejdź do zakładki **Historia**.

Dla wygodnego przeglądania historii można pogrupować informacje względem jednej z kolumn poprzez przeciągnięcie jej nagłówka na niebieskie pole nad listą. Można także dodawać notatki (po kliknięciu w przycisk **Dodaj własną adnotację**) oraz komentarze do wybranych wpisów (prawy przycisk myszy na wybranym wpisie **/ Dodaj komentarz**).

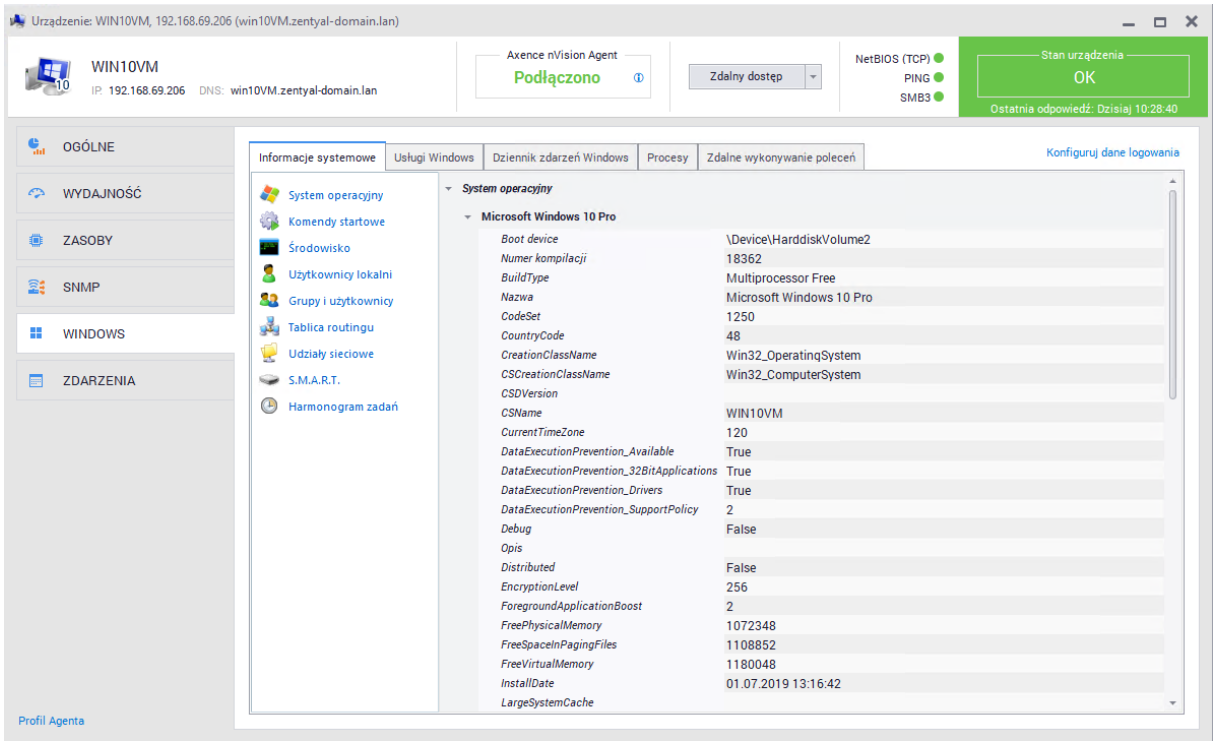


7.4 Informacje systemowe

7.4.1 Informacje systemowe - wprowadzenie

Informacje systemowe są pobierane przez Agenta nVision. Aby gromadzić te dane, należy zainstalować Agenty na wszystkich komputerach, które mają być monitorowane.

Aby przejść do okna informacji systemowych wybierz interesujące Cię urządzenie i przejdź do okna **Informacji o urządzeniu**. Następnie wybierz zakładkę **Windows**.



W tej sekcji znajdziemy zakładki Informacje systemowe, Usługi Windows oraz Dziennik zdarzeń Windows. Są one częścią modułu Inventory.

Zakładki Procesy oraz Zdalne wykonywanie poleceń powiązane są z modułem HelpDesk.

7.4.2 Monitorowane dane

W poniższej tabeli przedstawione są dane systemowe, które mogą być monitorowane.

Dane	Opis
System operacyjny	W tej zakładce znajdują się szczegółowe informacje dotyczące systemu operacyjnego, między innymi nazwa, producent, wersja, numer seryjny i wiele innych.
Komendy startowe	Lista komend startowych, z uwzględnieniem nazwy, komendy, użytkownika oraz lokalizacji wykonywanych plików.
Środowisko	Zakładka zawiera informacje na temat zmiennych środowiskowych.
Użytkownicy lokalni	Dane o użytkownikach lokalnych zawierają nazwę konta, informacje związane z hasłem (czy jest wymagane, czy wygasło), czy dane konto

Dane	Opis
	jest wyłączone i inne.
Grupy i użytkownicy	W tej zakładce znajdują się informacje o grupach użytkowników wraz z opisem tych grup.
Tablica routingu	Tablica routingu danego komputera.
Udziały sieciowe	Zakładka zawiera informacje o zasobach, dyskach i folderach udostępnionych.
S.M.A.R.T.	W zakładce znajdują się informacje zebrane przy użyciu systemu S.M.A.R.T. Aby zmienić napęd, dla którego wyświetlane są informacje, należy wybrać go z menu znajdującego się w górnej części okna. Aby dowiedzieć się więcej o systemie S.M.A.R.T., przejdź do rozdziału S.M.A.R.T.
Harmonogram zadań	Prezentuje informacje o aplikacjach uruchamianych przez Windows wraz z datami zaplanowanych, ostatnich uruchomień oraz wynikiem ostatniego uruchomienia.

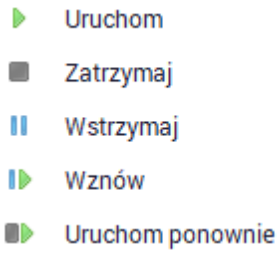
7.4.3 Usługi Windows

Moduł Inventory zawiera funkcję pozwalającą na monitorowanie usług systemu Windows.

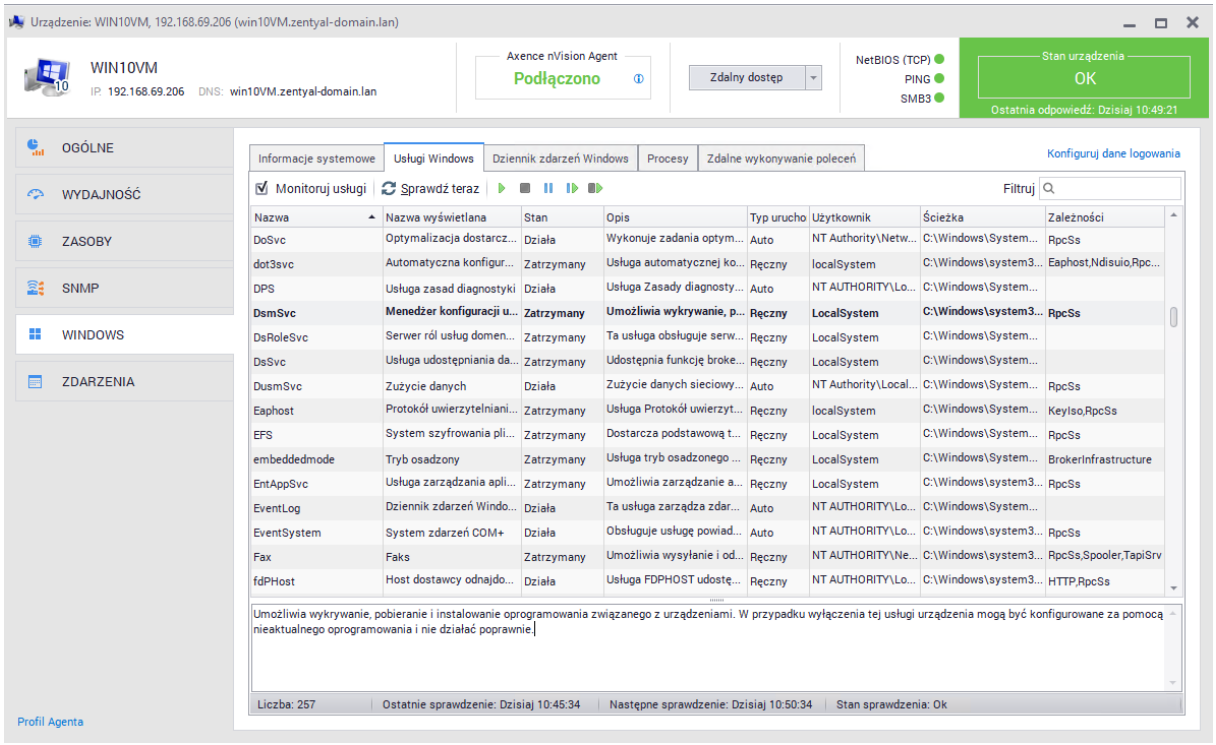
Przechodząc do zakładki **Usługi Windows** możemy zobaczyć wszystkie usługi powiązane z urządzeniem. Zaznaczając okienko **Monitoruj usługi** mamy możliwość włączenia widoczności tej listy.

Widok ten pozwala na uzyskanie dokładnych informacji na temat poszczególnych pozycji w tabeli.

Zakładka usługi Windows daje również możliwość uruchomienia, wstrzymania, zatrzymania czy wznowienia danej usługi. Takie akcje można wykonać używając intuicyjnych przycisków dostępnych na pasku powyżej listy lub w menu kontekstowym danej usługi (prawy klik myszy).

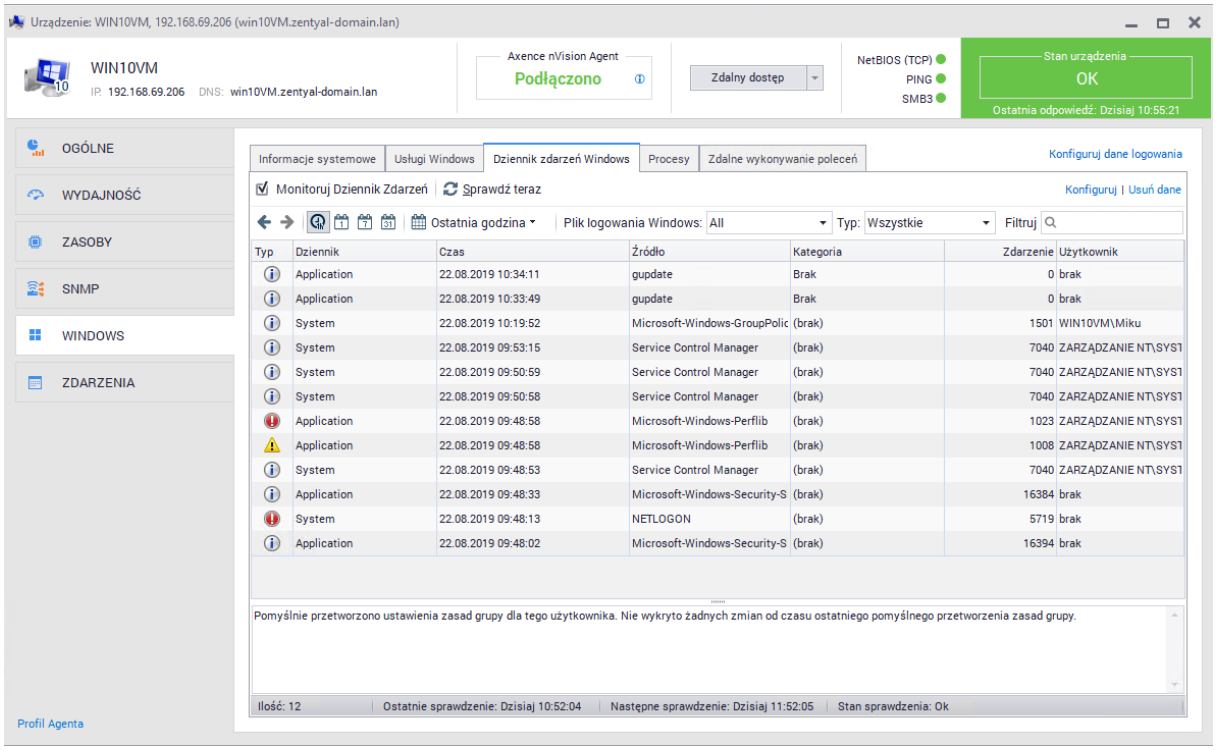


Aby wymusić sprawdzenie aktualnego stanu usług należy użyć przycisku **Sprawdź teraz**.



7.4.4 Dziennik zdarzeń Windows

Moduł Inventory pozwala na monitorowanie dziennika zdarzeń systemu Windows.



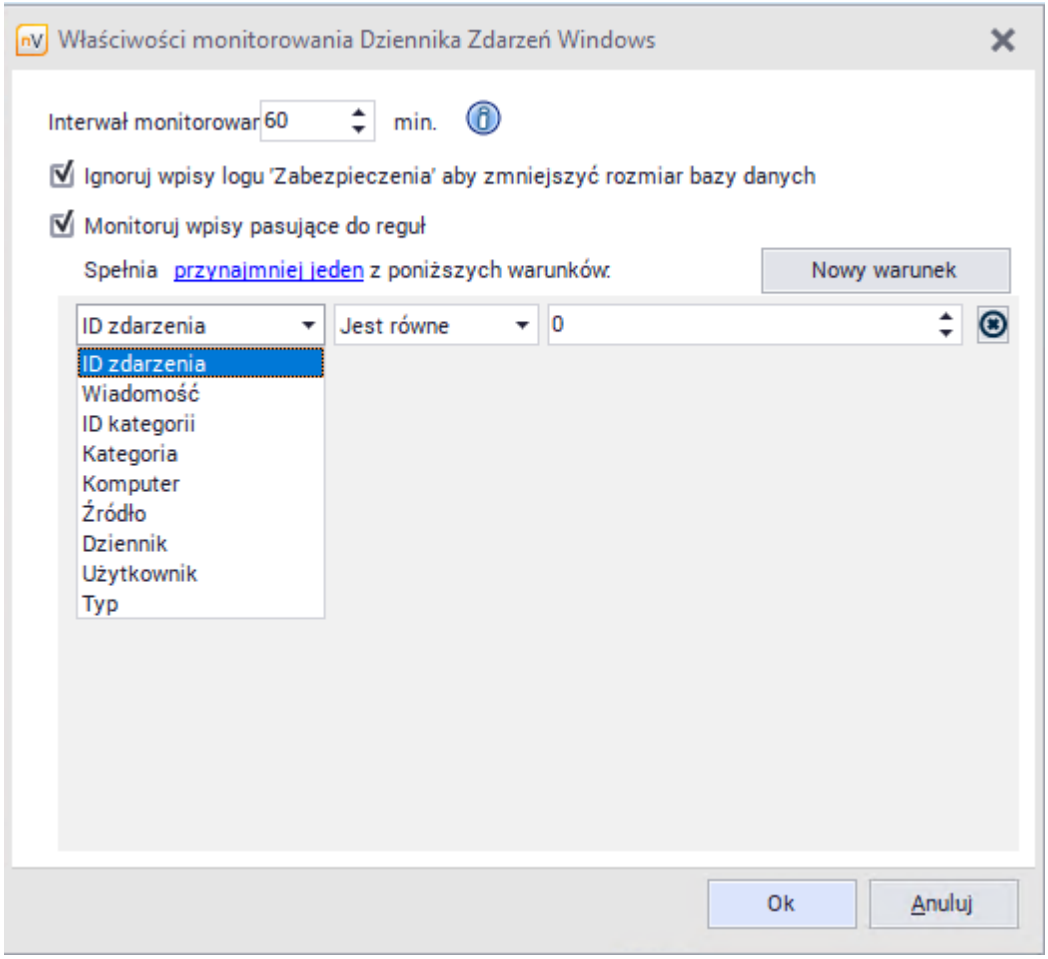
Aby uruchomić funkcję monitorowania dziennika zdarzeń w oknie **Informacje o urządzeniu / Windows** przechodzimy do zakładki **Dziennik zdarzeń Windows** oraz zaznaczamy pole **Monitoruj dziennik zdarzeń**.

UWAGA! Włączenie synchronizacji dziennika zdarzeń dla dużej ilości urządzeń może

znacząco obciążyć sieć i zwiększyć rozmiar bazy danych.

Domyślnie nVision aktualizuje dziennik zdarzeń co godzinę. Przechodząc do opcji **Konfiguruj** możemy zmodyfikować zarówno interwał monitorowania jak i określić dodatkowe reguły. Ustawienie małego interwału monitorowania może skutkować dużym obciążeniem sieci. Domyślny filtr monitorowania dziennika zdarzeń Windows nie zbiera informacji dotyczących logowania się użytkowników.

Aby wymusić natychmiastową synchronizację dziennika zdarzeń należy kliknąć **Sprawdź teraz**.



7.4.5 Procesy Windows

Wgląd w procesy systemowe i zarządzanie nimi jest możliwe dzięki modułowi HelpDesk. Więcej informacji dostępnych jest w rozdziale Procesy Windows.

7.4.6 Zdalne wykonywanie poleceń

Zdalne wykonywanie poleceń jest częścią modułu HelpDesk. Więcej informacji na ten temat można znaleźć w rozdziale Zdalne wykonywanie poleceń.

7.4.7 S.M.A.R.T.

S.M.A.R.T. (ang. Self-Monitoring, Analysis and Reporting Technology) to system monitorowania i powiadamiania o błędach działania dysku twardego służący zwiększeniu bezpieczeństwa składowanych danych. Użycie tego systemu pozwala przewidywać i zapobiegać zbliżającym się awariom (np. poprzez

monitorowanie temperatury, której wzrost może prowadzić do przegrzania).

S.M.A.R.T. monitoruje wiele parametrów dysku twardego, co pozwala mu na bieżąco oceniać stan urządzenia. Monitorowanie obejmuje m.in.:

- liczbę cykli start/stop (Start/Stop Count),
- temperaturę dysku (Temperature Celcius),
- częstotliwość błędów podczas odczytu (Read Error Rate),
- liczbę realokowanych sektorów (Reallocated Sector Count),
- liczbę prób uruchomienia osi dysku (Spin Retry Count).

Analiza błędów, polegająca na przewidywaniu wystąpienia uszkodzeń dysku na podstawie stale monitorowanych parametrów (atrybutów) pozwala na wcześniejsze ostrzeżenie o możliwości wystąpienia potencjalnych problemów.

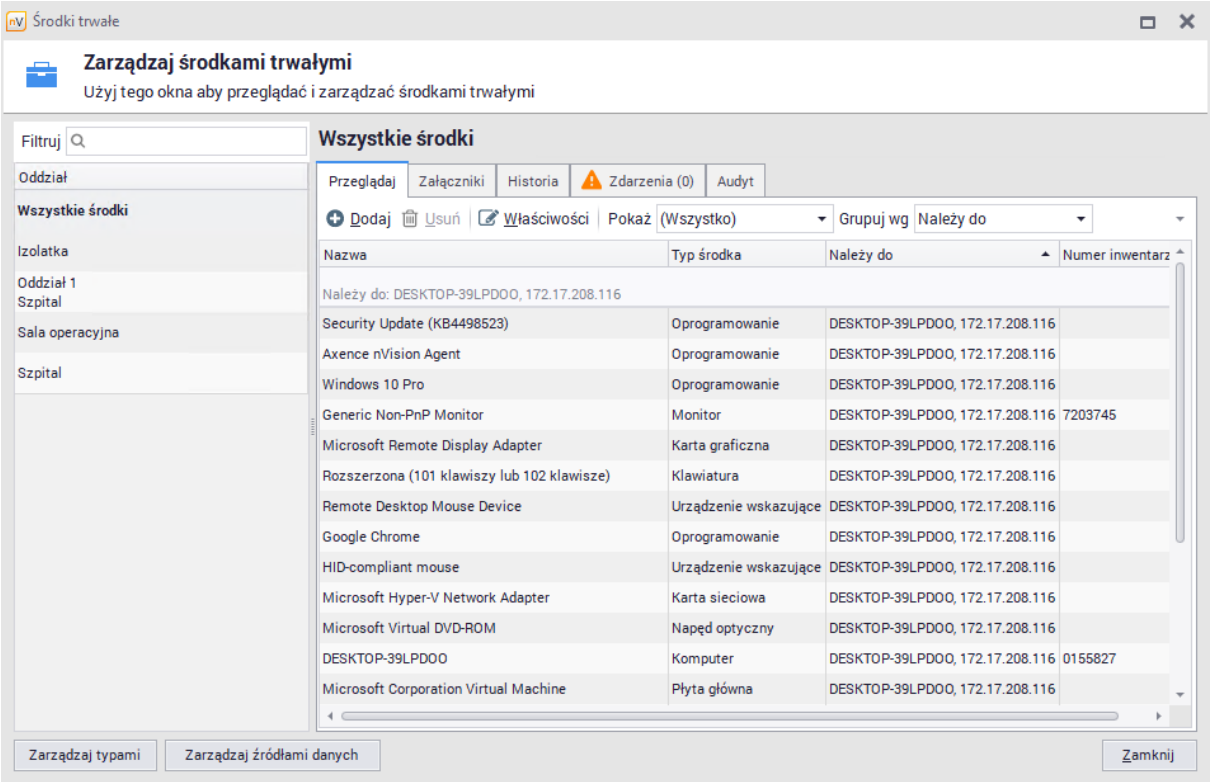
7.5 Środki trwałe

7.5.1 Środki trwałe - wprowadzenie

Moduł administracyjno-rozliczeniowy (tzw. środki trwałe) w module Inwentaryzacji to baza ewidencji majątku IT zintegrowana z informacjami z Agentów dotyczącymi oprogramowania i sprzętu.

Funkcje modułu środków trwałych

- Przechowywanie wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz elastyczne rozszerzanie i aktualizowanie zgromadzonych informacji.
- Możliwość definiowania własnych typów (elementów wyposażenia), ich atrybutów (pól) oraz wartości - dla danego urządzenia lub oprogramowania można podawać dodatkowe informacje, np. numer inwentarzowy, osobę odpowiedzialną, numer i skan faktury zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu i skan gwarancji, termin przeglądu (można podać datę, po której administrator otrzyma powiadomienie o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, inny dowolny plik .DOC, .XLS, skan czy też własny komentarz; możliwość importu danych z zewnętrznego źródła (CSV).
- Możliwość przypisywania środków do oddziałów lub komputerów.
- Specjalny widok audytowy zestawia wszystkie środki trwałe, w tym urządzenia i zainstalowane na nich oprogramowanie.



7.5.2 Typy środków trwałych

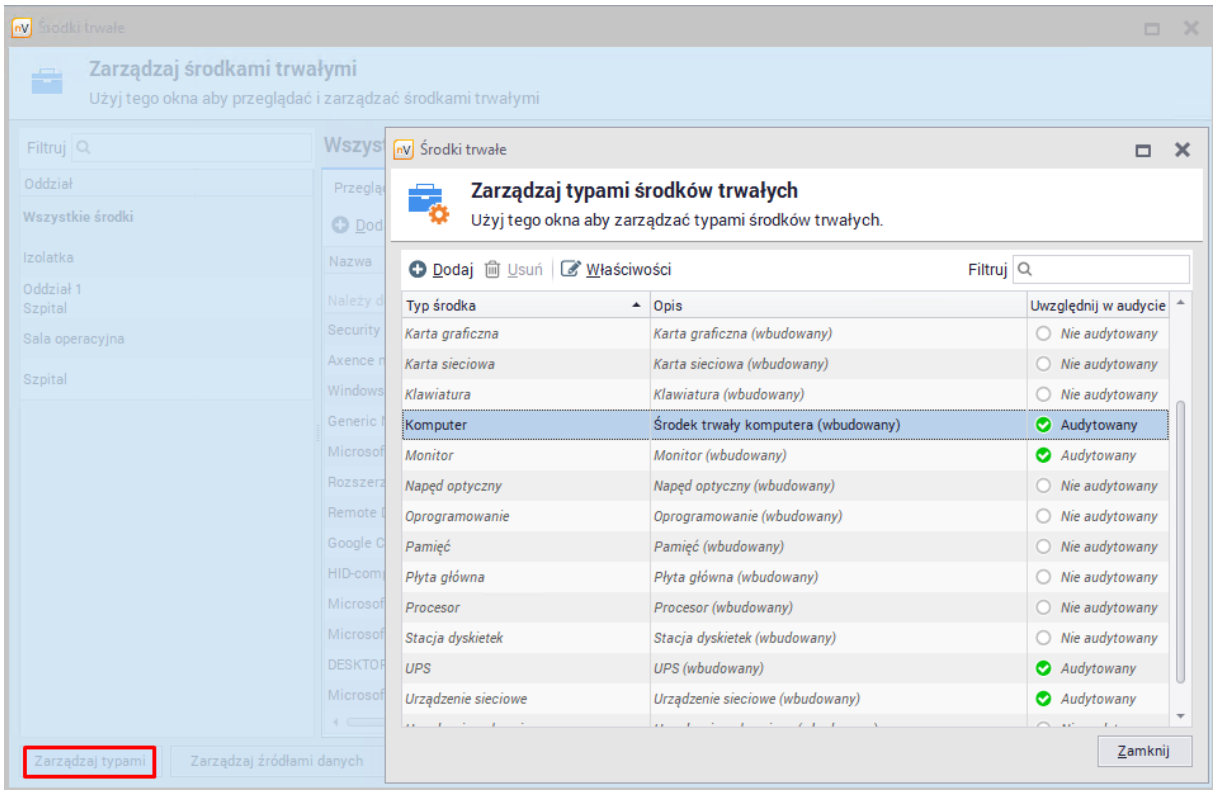
Typy środków trwałych dzielą się na wbudowane oraz zdefiniowane przez użytkownika.

Typy wbudowane

Przykładowe typy wbudowane to:

- Drukarka
- Dysk twardy
- Karta graficzna
- Klawiatura
- Programy
- UPS
- Urządzenie wskazujące

W rzeczywistości zdefiniowanych jest ich więcej i dotyczą środków, które są automatycznie wykrywane przez Agentów. Oznacza to, że na liście środków trwałych pojawi się sprzęt oraz oprogramowanie, których audyt można przeprowadzić w module Inwentaryzacja. Uwaga: w ramach środków trwałych uwzględniane jest wyłącznie oprogramowanie komercyjne (z przypisaną do niego licencją).



Typy wbudowane wyświetlane są w kolorze szarym. Nie można ich usunąć, ale można edytować ich właściwości klikając w menu kontekstowym przycisk **Właściwości** lub wciskając klawisz **Enter**.

Typy zdefiniowane przez użytkownika

Aby dodać własny typ:

1. Będąc w oknie **Środki trwałe** (należy z głównego paska narzędziowego wybrać odpowiednią ikonę) przechodzimy do menu **Zarządzaj typami** znajdującego się w dolnej części ekranu.
2. Kliknij w przycisk **Dodaj**. Zostanie otwarte okno konfiguracji typu środka trwałego.
3. Podaj unikalną **Nazwę** oraz **Opis** typu.
4. Jeśli chcesz, to dodaj własne pola (opisane poniżej) i kliknij **OK**.

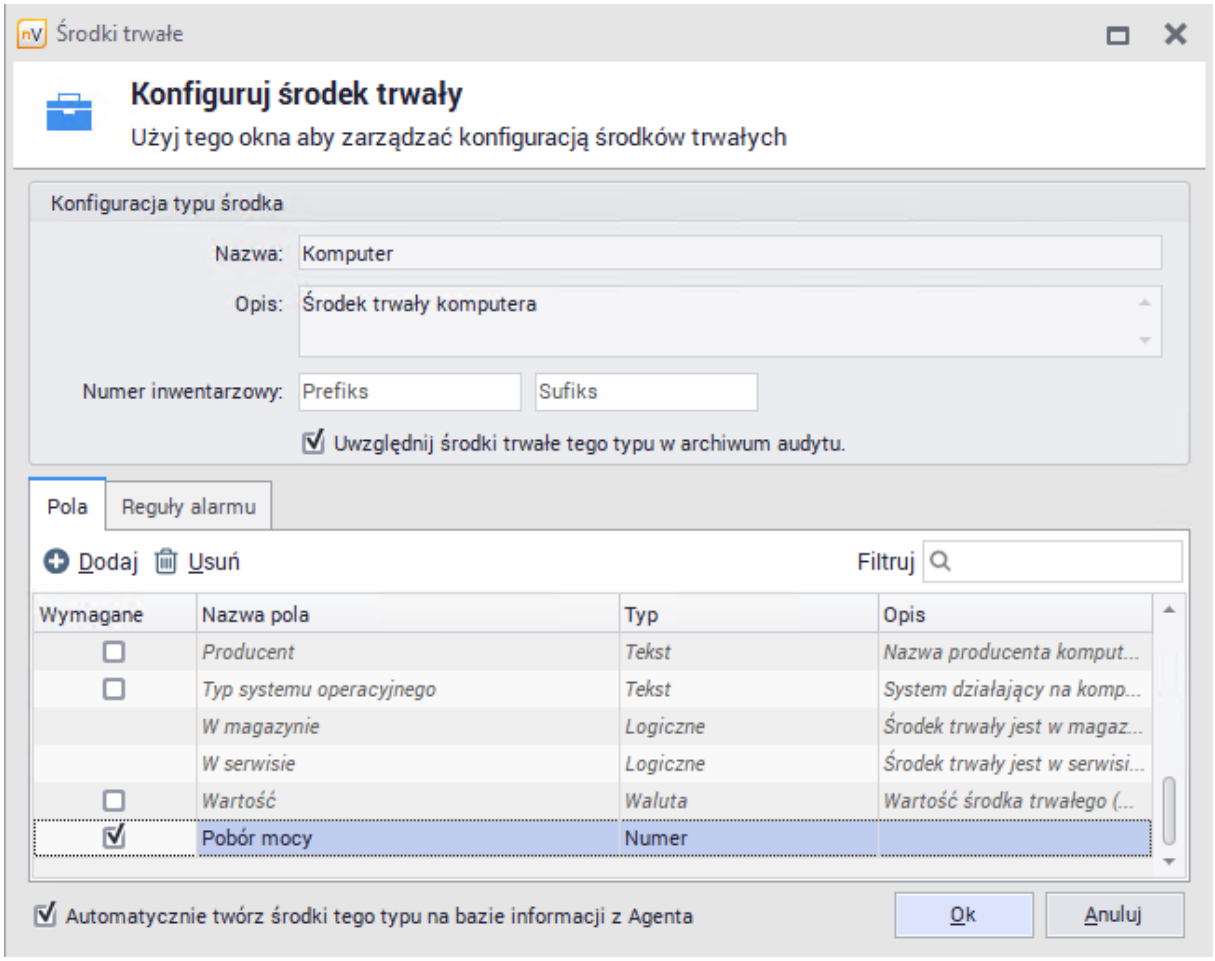
Pola

Każdy typ ma pewne wbudowane pola (np. "wartość", "osoba odpowiedzialna", "w serwisie" i inne). Ich lista zależy od charakterystyki danego typu, np. dla programów wbudowane jest pole "ID rejestracji", a dla monitorów "DPI w poziomie". Do nieusuwalnych wbudowanych pól można dodać własne. Aby to zrobić:

1. Przejdź do **Właściwości** danego typu.
2. Kliknij w przycisk **Dodaj**, wybierz z listy lub podaj własną **Nazwę pola**.
3. Wybierz z listy **Typ** pola (Tekst, Numer, Logiczne, Waluta, Data, Czas, Data i godzina lub Liczba zmiennoprzecinkowa).

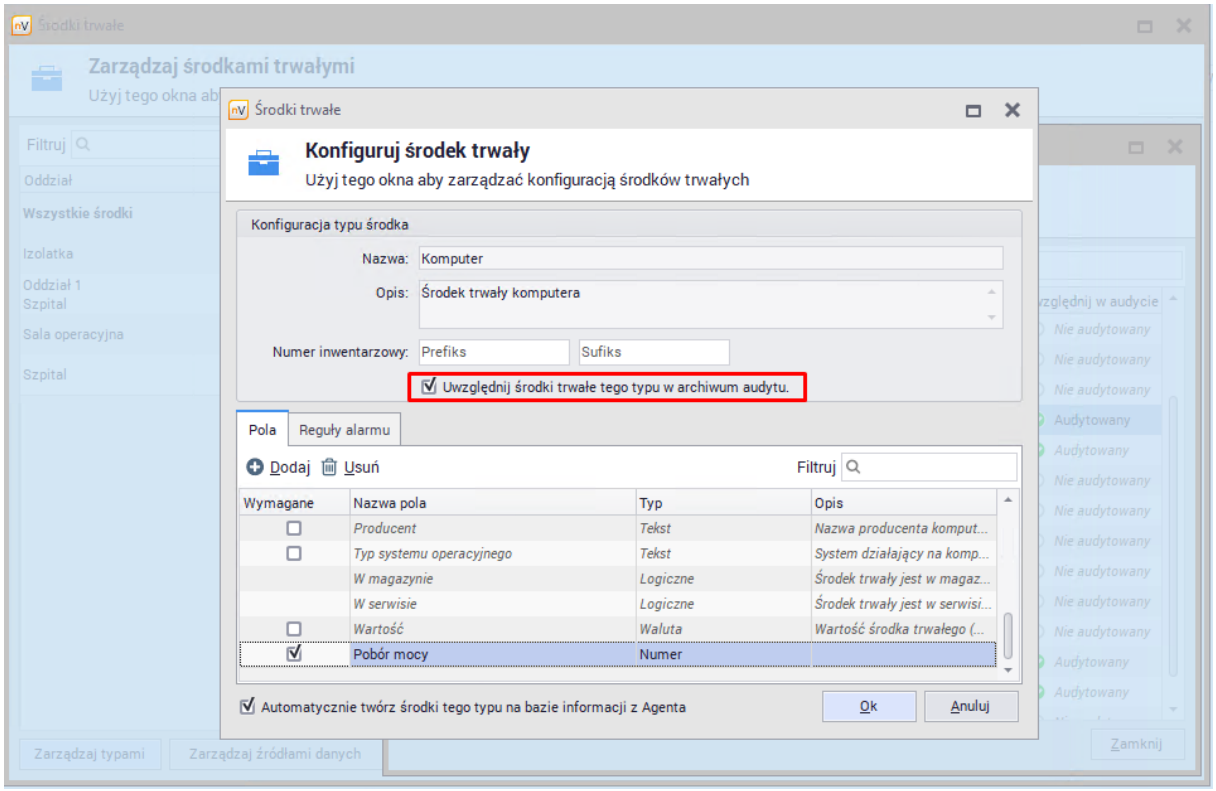
4. Dodaj **Opis** pola i kliknij **OK**.

Dodane przez użytkownika nowe pole wraz z opisem będzie od tej pory wyświetlane na liście pól do wyboru.



Uwzględnianie środków trwałych w archiwum audytu

Aby środki trwałe danego typu były uwzględniane w archiwum audytu, należy zaznaczyć opcję **Uwzględnij środki trwałe tego typu w archiwum audytu**. Brak zaznaczenia tej opcji sprawia, że środki trwałe danego typu nie są archiwizowane w migawce. Ma to na celu ograniczenie ilości gromadzonych danych, co z kolei przekłada się na czas generowania audytu.



Poszczególne typy środków trwałych są porównywane w trakcie audytu, jeżeli w obu porównywanych migawkach zostały zapisane (czyli powyższa opcja była włączona w trakcie wykonywania obu migawek). Wyjątek stanowi wbudowany typ **Programy**, w którego konfiguracji opcja ta nie występuje ze względu na osobny mechanizm migawek i audytów.

Aby dowiedzieć się więcej na temat generowania migawek i audytu, przejdź do rozdziału Audyt środków trwałych.

7.5.3 Właściwości i dodawanie środka trwałego

Aby zobaczyć i edytować właściwości konkretnego środka trwałego kliknij w przycisk **Środki trwałe** i kliknij dwukrotnie na pozycję z tym środkiem. Przy dużej liczbie monitorowanych urządzeń warto skorzystać z pola **Filtruj**.

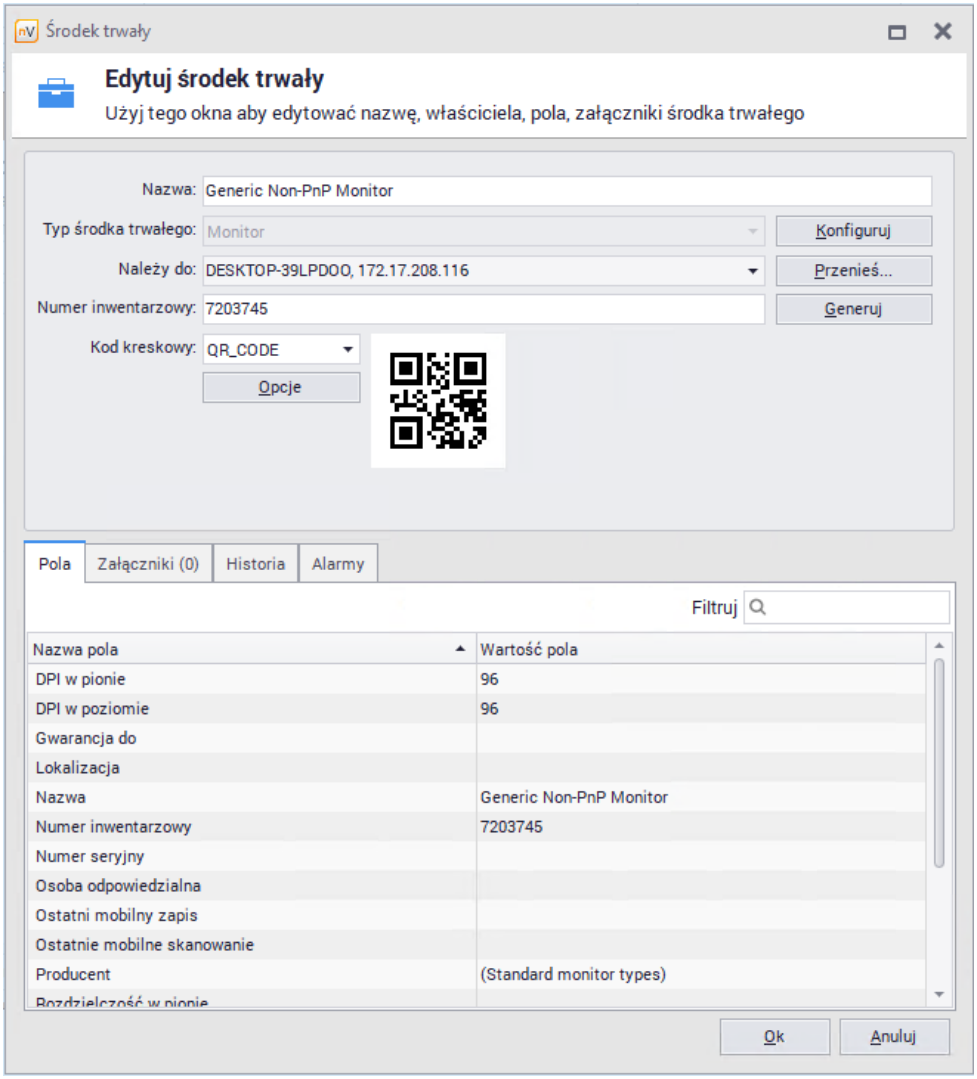
Z poziomu okna środka trwałego można zmienić nazwę i przynależność, ale nie typ. Można za to **Konfigurować** typ, np. dodawać do niego nowe pola.

Przynależność do oddziałów

Środki trwałe mogą przynależeć do oddziałów, urządzeń (komputerów) oraz pozostawać nieprzypisane. Wyjątek stanowią same komputery, które mogą być przypisane albo do oddziału albo wcale.

Możliwe jest przeniesienie danego środka, czyli zmiana jego przynależności, zgodnie z zasadami opisanymi powyżej.

Warto zwrócić uwagę na fakt, że oprócz przynależności można dla danego urządzenia czy przedmiotu zdefiniować osobę za niego odpowiedzialną.



Pola

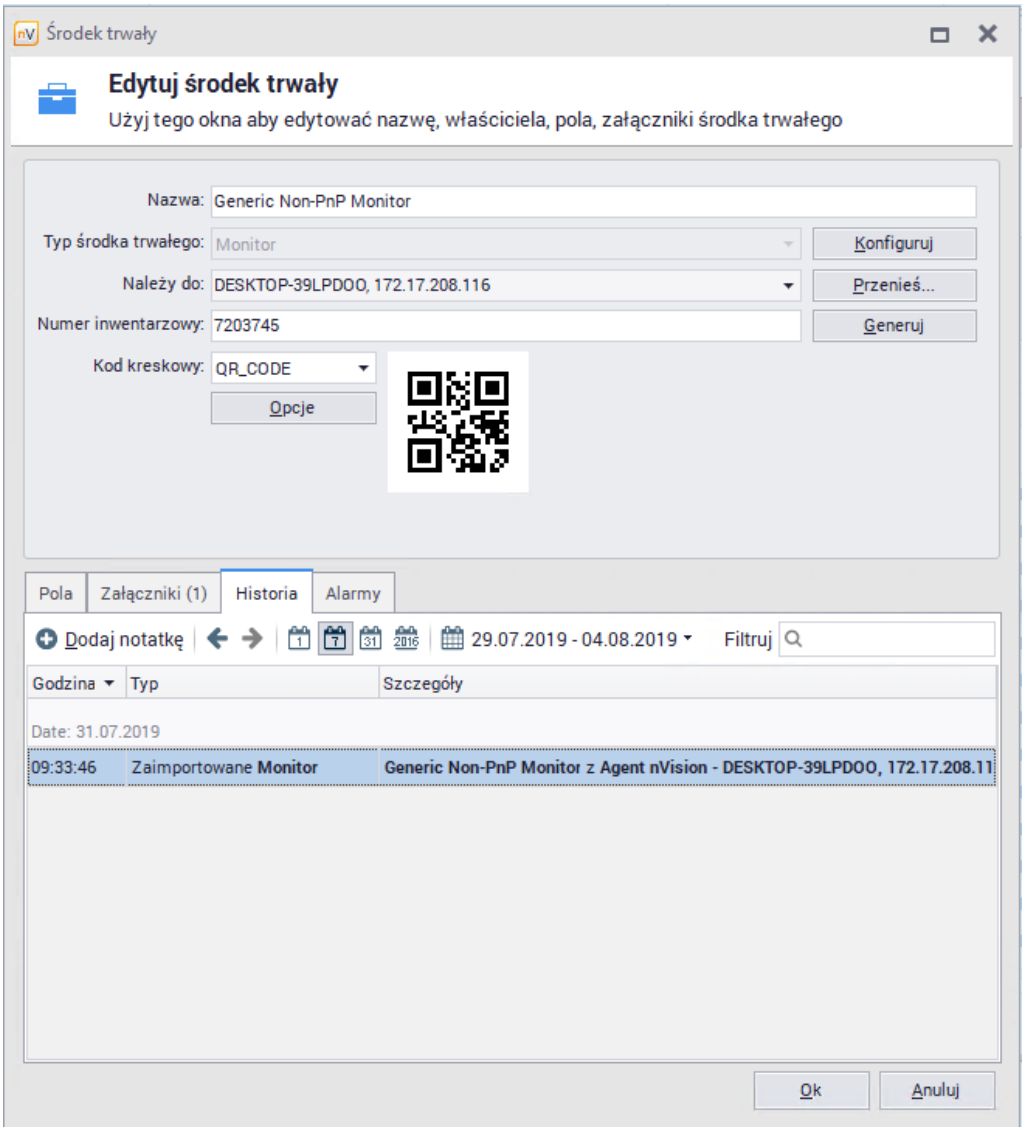
Zależą od typu danego środka trwałego. Można je z tego poziomu edytować, np. podając informację o oddaniu danego urządzenia do serwisu.

Załączniki

Opisane szerzej w rozdziale Załączniki.

Historia

W zakładce **Historia** znajdują się wszystkie informacje dotyczące zmian dokonywanych dla danego środka trwałego. W szczególności, można zobaczyć, kiedy dodano załączniki i je wyświetlić. Można także dodawać własne wpisy klikając w przycisk **Dodaj notatkę**.



Alarmy

Opisane szerzej w rozdziale Alarmy.

Dodawanie środków trwałych

Dodawanie środków trwałych odbywa się z poziomu okna zarządzania środkami, które można otworzyć klikając w ikonę **Środki trwałe** . Aby dodać nowy środek trwały, kliknij w przycisk **Dodaj** znajdujący się w zakładce **Przeglądaj**. W następnej kolejności podaj informacje o danym środku, podaj jego **Typ** i uzupełnij pola. Możesz także dodać załączniki.

7.5.4 Załączniki

Do każdego ze środków trwałych można dodawać załączniki. Przykładowo, może to być skan gwarancji, instrukcja użytkowania lub faktura zakupu.

Importowane pliki dodawane są do bazy danych. Ich kopie znajdują się w folderze z nVision, folder **Database | Numer bazy | FAAttachmentFiles**. W podkatalogach o nazwach oznaczających daty dodania znajdują się kopie plików załączonych w danym dniu.

Można otwierać i edytować pliki bezpośrednio z poziomu nVision. Zmiany zawartości plików są wykrywane - do użytkownika należy decyzja, czy te zmiany będą uwzględnione i pliki zmienione.

Przeglądanie załączników

Lista załączników dla wszystkich środków trwałych jest dostępna po kliknięciu w ikonę **Środki trwałe**, zakładka **Załączniki**. Z tego miejsca można też otwierać i eksportować pliki.

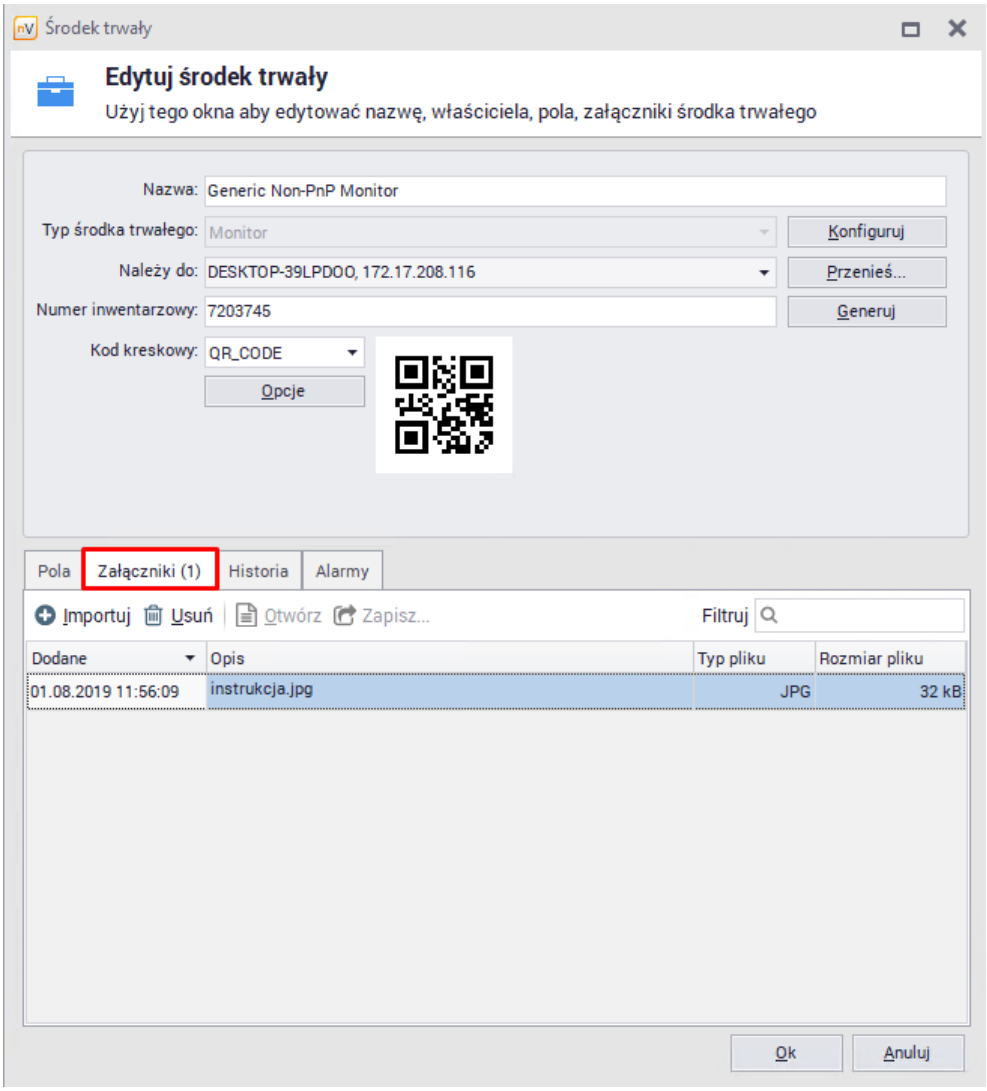
Załączniki dla danego urządzenia wyświetlane są w oknie **Właściwości** tego urządzenia. Aby do niego przejść, w zakładce **Przeglądaj** dwukliknij na danym środku stałym. W zakładce **Załączniki** znajdują się szczegółowe informacje na temat plików dołączonych do środka.

Dodawanie i usuwanie załączników

Aby dodać załącznik:

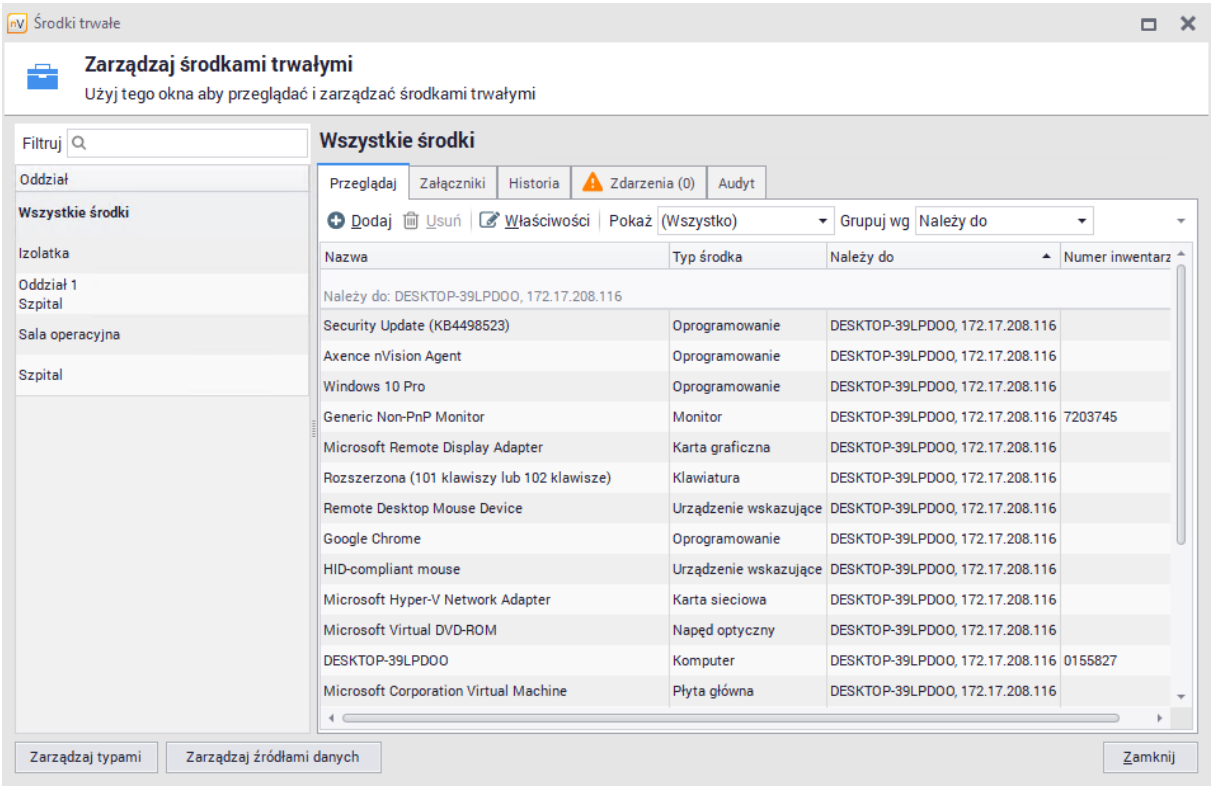
1. Przejdź do okna **Właściwości** środka trwałego, dla którego chcesz dodać załącznik.
2. W zakładce **Załączniki** wciśnij przycisk **Importuj**.
3. Znajdź na dysku plik, który chcesz dodać i wciśnij **Otwórz**.

Aby usunąć plik, w tym samym oknie użyj przycisku **Usuń**.



7.5.5 Widok ogólny

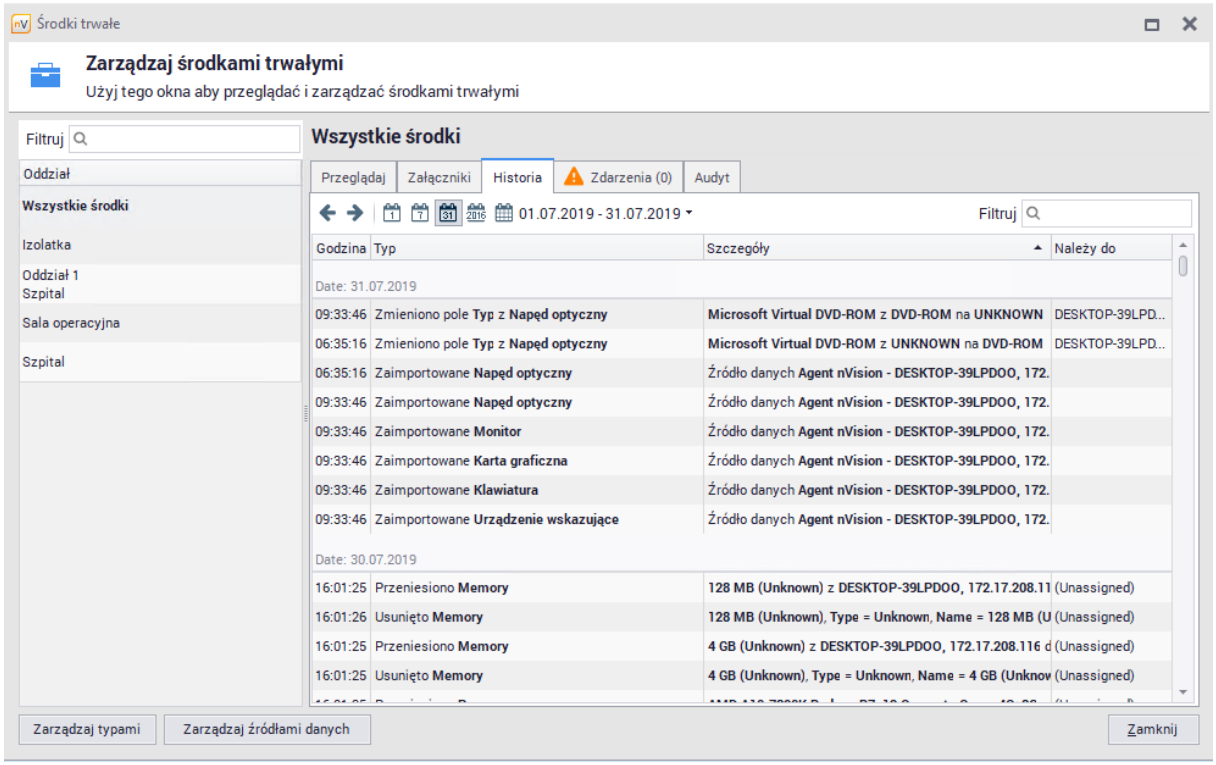
Aby przeglądać środki trwałe wciśnij przycisk **Środki trwałe**. Lista wszystkich środków trwałych znajduje się w zakładce **Przeglądaj**.



Lista wyświetlanych kolumn zależy od wybranych opcji. Można wyświetlić środki należące do danego oddziału lub środki danego typu. Dane można pogrupować wg typu środka, przynależności, nazwy i osoby odpowiedzialnej.

Historia

W zakładce **Historia** znajduje się spis wszystkich zmian, w tym zmian załączników i wartości pól, jakie są dokonywane dla środków trwałych. Możliwe jest przeglądanie historii w okresie dziennym, tygodniowym, miesięcznym bądź rocznym.

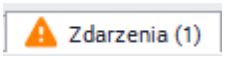


7.5.6 Zdarzenia

W przypadku wykrycia usunięcia bądź zmiany jakiegoś urządzenia lub programu (ogólniej - dowolnego środka trwałego) przez Agenta, nVision nie podejmuje decyzji o usunięciu go z listy bądź zmianie właściwości. Informacja o wystąpieniu tego typu sytuacji wyświetlana jest w zakładce **Zdarzenia**. Należy rozpatrzeć wymienione zdarzenia, wykonując jedną z dostępnych akcji:

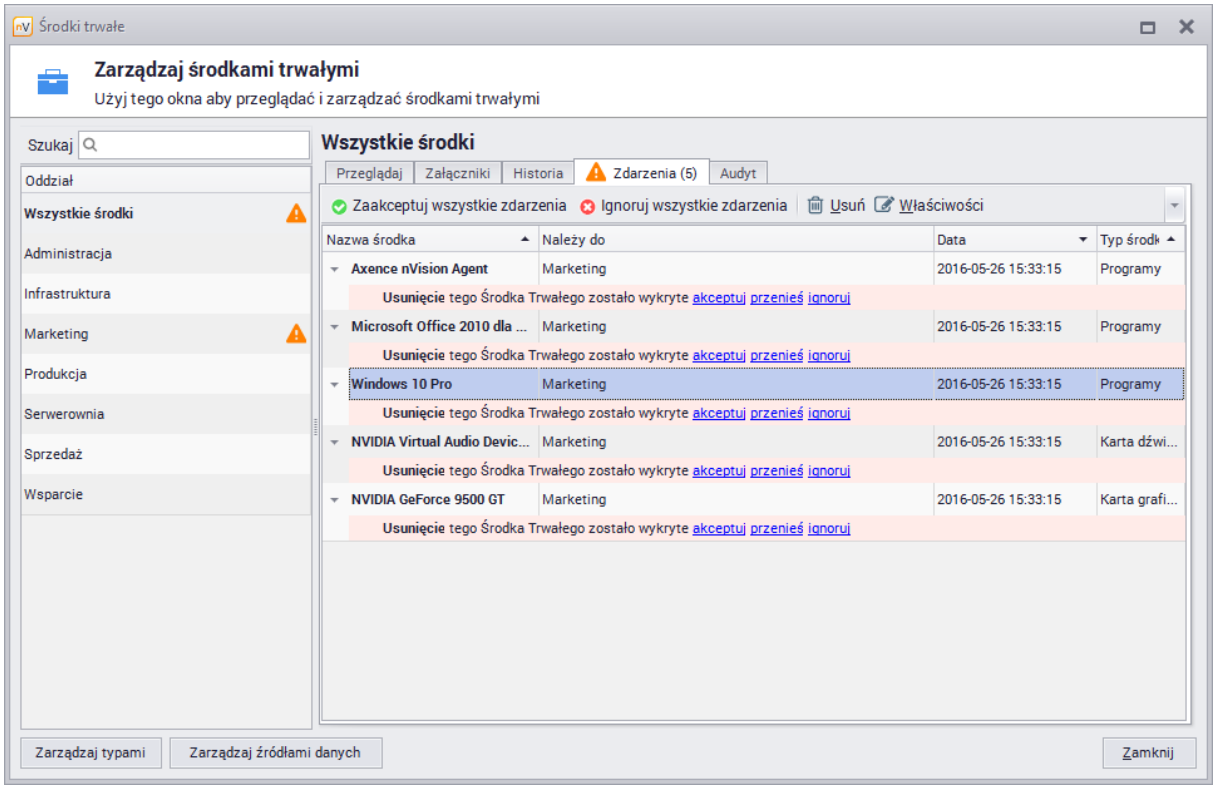
- **Akceptacja** oznacza faktyczne usunięcie środka - zostaje on zutylizowany, nie będzie się już pojawiał na liście środków.
- **Przeniesienie** dotyczy sytuacji odpięcia danego urządzenia od komputera i przeniesienia w inne miejsce, np. przepięcie monitora do innego komputera; należy podać nowe miejsce przynależności.
- **Ignorowanie** nie zmienia stanu rzeczy, dalej jest przypisana w tym samym miejscu; tę akcję dobrze stosować w przypadku urządzeń okresowo podłączanych i odłączanych, jak np. mysz podłączana do laptopa.

Liczba nieobsłużonych zdarzeń wyświetlana jest w nazwie zakładki:



W przypadku dużej liczby podobnych zdarzeń można nie rozpatrywać każdego z nich oddzielnie, lecz skorzystać z przycisku **Akceptacji** lub **Ignorowania** wszystkich zdarzeń. Można także z tego poziomu zarządzać właściwościami danego środka trwałego.

Poniżej przedstawiona jest przykładowa lista zdarzeń. Wykryte zdarzenia dotyczą odłączenia monitora oraz odinstalowania programu.

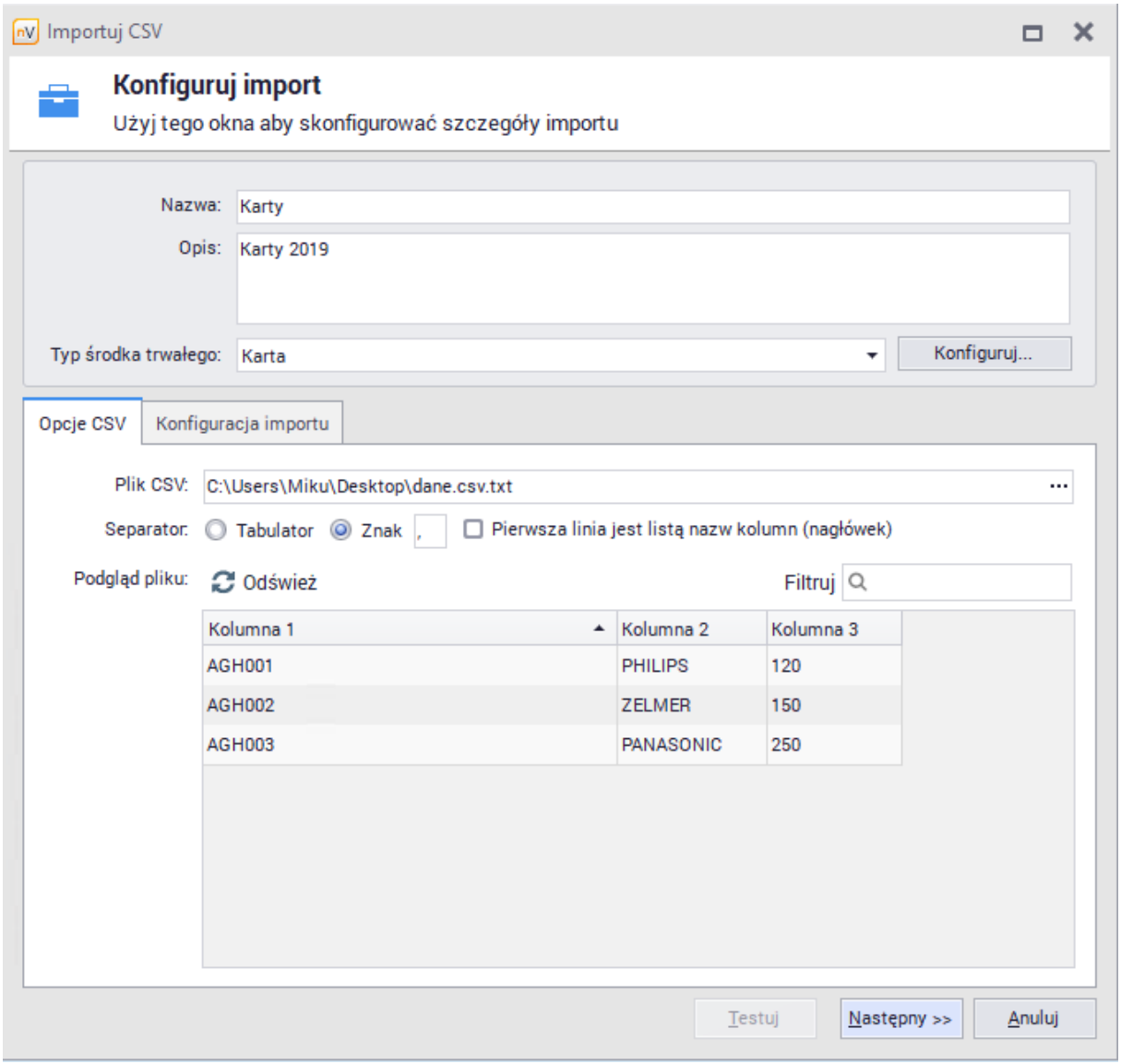


7.5.7 Importowanie danych

Jeżeli już posiadasz spis środków trwałych, to możesz go zaimportować do nVision. Warunkiem udanego importu danych jest umieszczenie ich w pliku *.csv i podzielenie danych tak, aby w jednym pliku znajdowały się środki jednego typu.

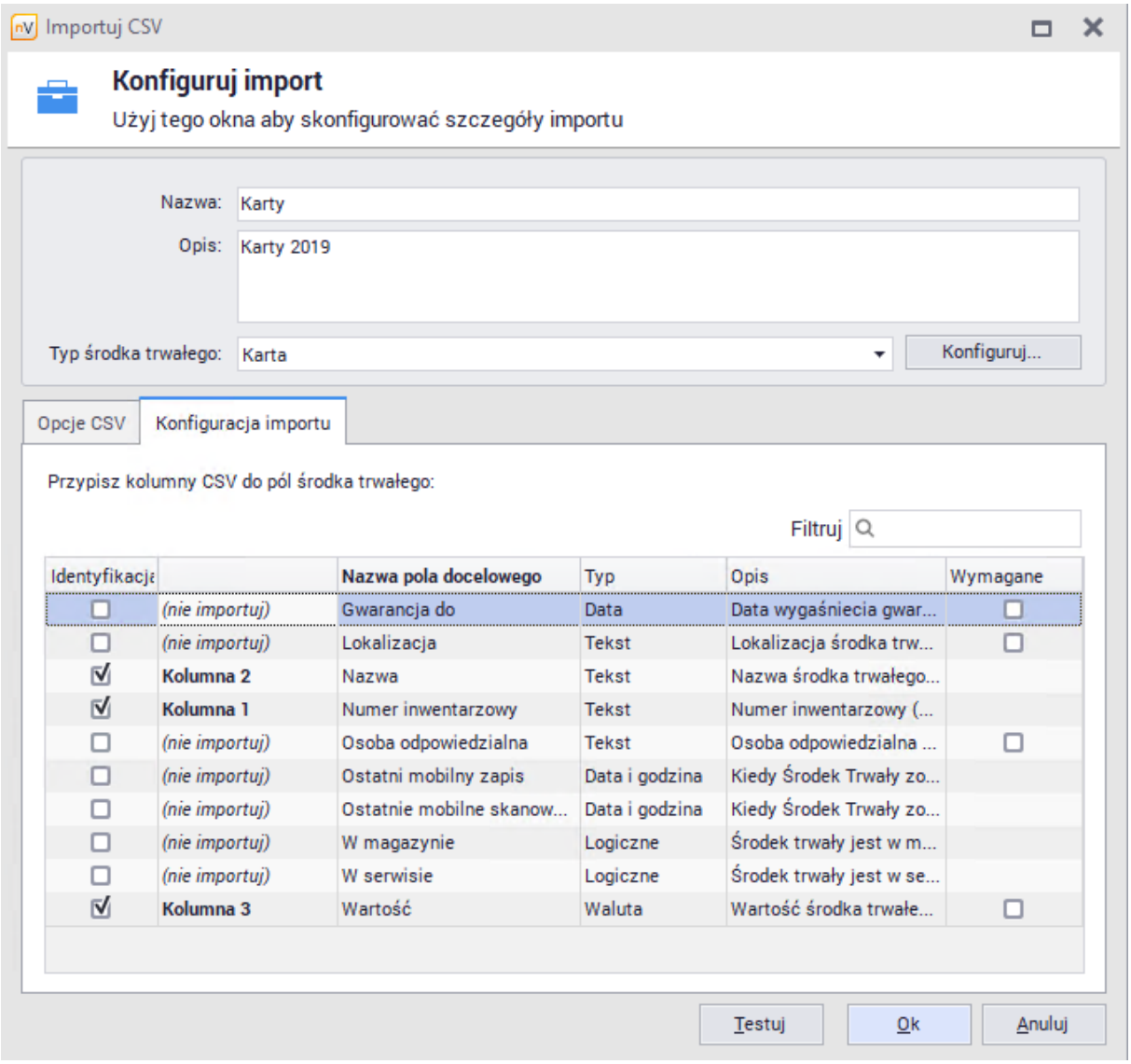
Aby dodać w nVision plik z danymi do importu:

1. Na głównym pasku narzędzi w sekcji **Sprzęt i srodki trwałe** wybierz opcję **Zarządzaj źródłami danych**.
2. Kliknij w przycisk **Dodaj** i wybierz opcję **Import z pliku CSV**.
3. Podaj **Nazwę** i **Opis** zestawu danych, a także **Typ**, który zostanie przypisany do tych danych.
4. W **Opcjach CSV** podaj ścieżkę dostępu do pliku z danymi, określ **Separator** i występowanie nagłówków. Poniżej zostanie pokazany podgląd pliku.

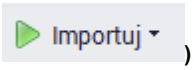


5. W zakładce **Konfiguracja importu** wskaż, która kolumna (bądź zestaw kolumn) źródła identyfikuje środek trwały, czyli jest dla danego przedmiotu unikalna.

6. Powiąż kolumny źródła CSV z nazwami pól docelowych. W razie potrzeby edytuj **Typ środka trwałego** (przycisk **Konfiguruj**) i dodaj do niego nowe pola. W prezentowanym przykładzie dodano pole Numer, aby móc powiązać je z numerem ewidencyjnym z pliku CSV i oznaczyć jako identyfikujące. Połączono także cenę z wartością; nazwy zostały połączone automatycznie przez nVision.

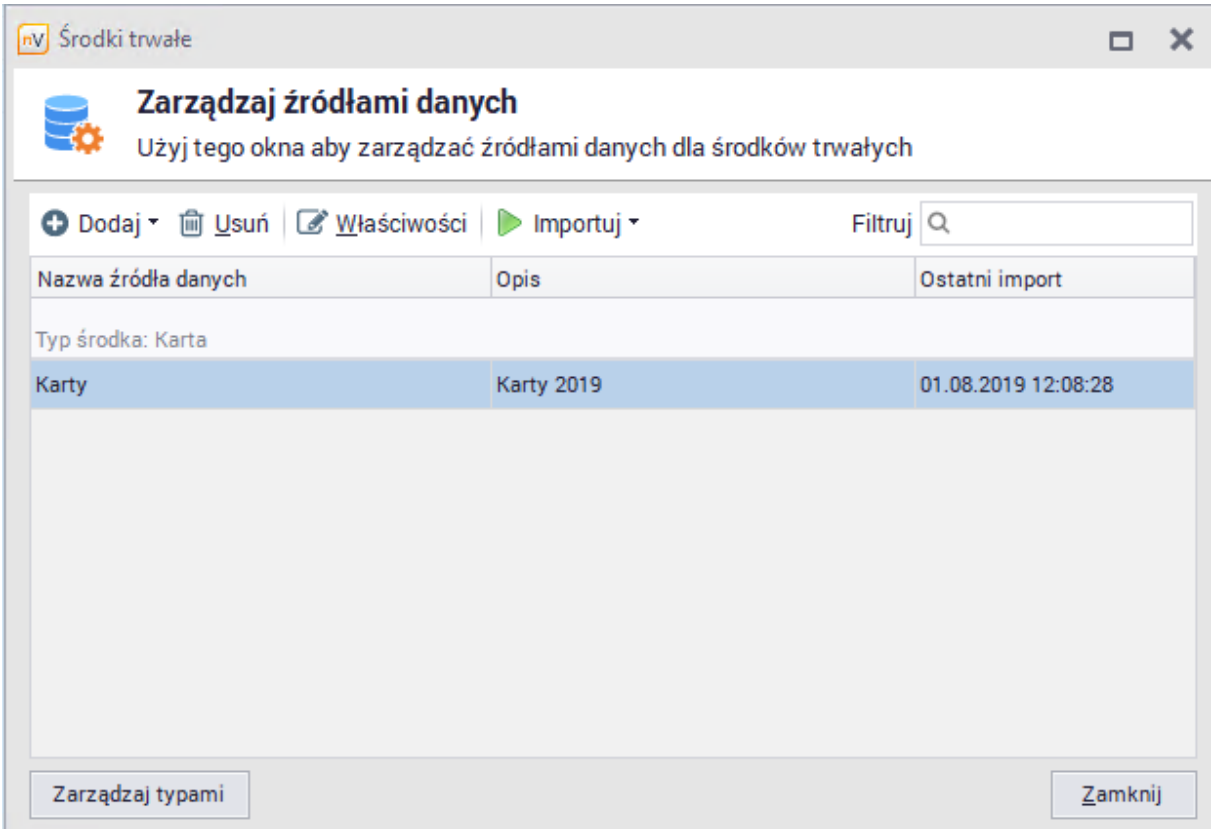


7. Aby przetestować możliwość importu danych, kliknij w przycisk **Testuj**. Aby zaimportować dane, wciśnij **OK**.

Dodany plik pojawi się na liście źródeł danych. Od tej pory można w prosty sposób importować dane z tego pliku, gdy np. zostanie on zmieniony (bez konieczności ponownych ustawień, tylko przycisk 

).

W oknie zarządzania źródłami danych można dodawać źródła danych, usuwać je, zmieniać ich właściwości i importować z nich dane, ale także importować dane z Agentów i przeglądać logi importu.



7.5.8 Kody kreskowe

Wprowadzenie

Aby korzystać z kodów kreskowych w nVision:

1. **Utwórz wszystkie środki trwałe w bazie nVision na jeden z poniższych sposobów:**
   a. automatycznie przy użyciu danych zebranych przez Agenty (zalecane),
   b. samodzielnie w konsoli nVision,
   c. samodzielnie za pośrednictwem aplikacji mobilnej.
2. **Oznakuj urządzenia.**

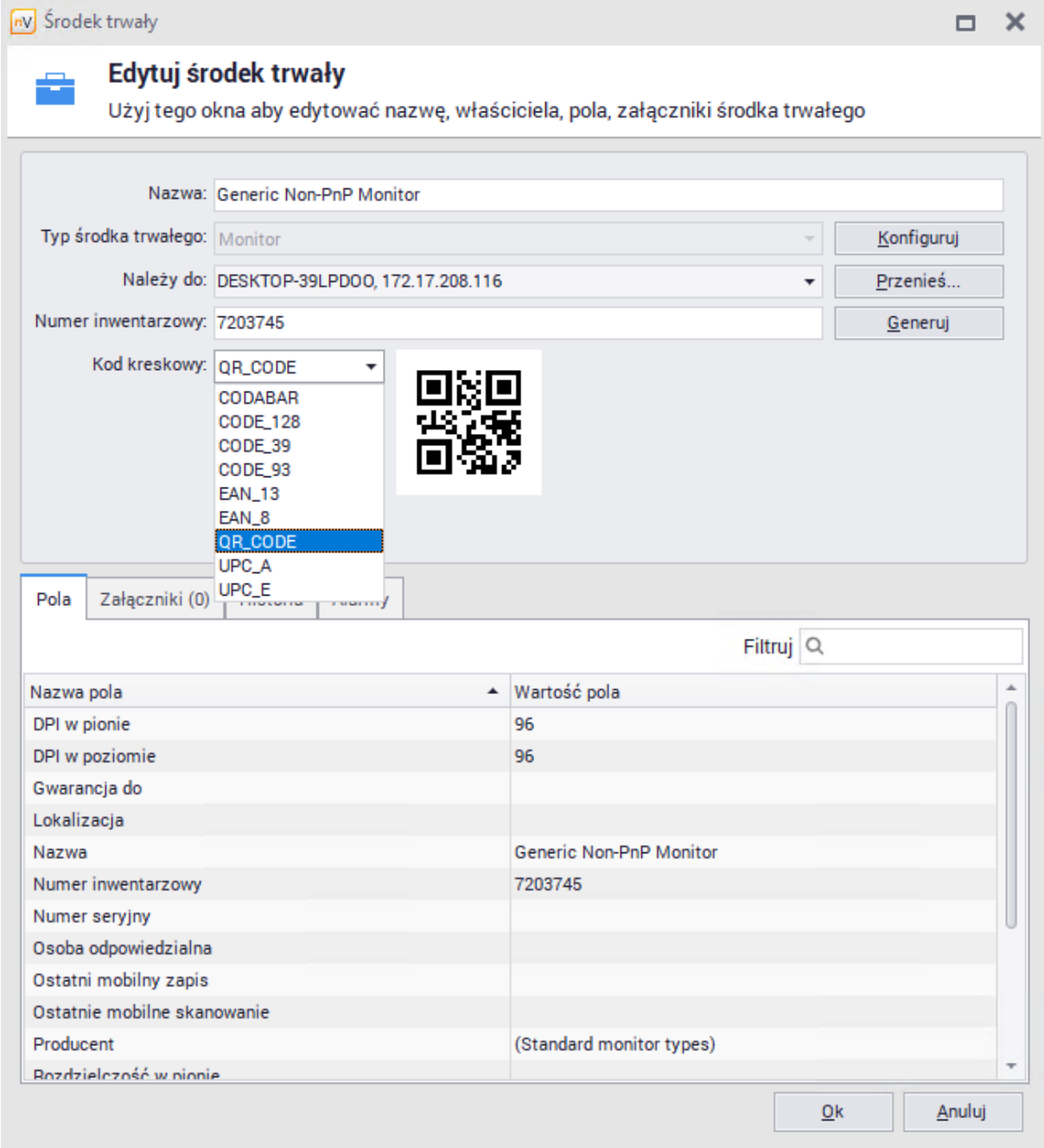
   Środki Trwałe z nVision należy powiązać z rzeczywistymi urządzeniami poprzez naklejanie na nich etykiet z kodem kreskowym. Identyfikator zaszyty w kodzie kreskowym oznacza jednocześnie (unikalny) numer inwentarzowy środka trwałego. Jeśli urządzenia posiadają już swoje unikalne identyfikatory z kodem kreskowym, to istnieje możliwość aktualizacji numeru inwentarzowego za pośrednictwem aplikacji mobilnej.
   Aby dowiedzieć się więcej o drukowaniu etykiet, przejdź do rozdziału Drukowanie etykiet. Aby dowiedzieć się więcej o instalowaniu i korzystaniu z aplikacji mobilnej, przejdź do rozdziału Aplikacja mobilna.
3. **Audytuj środki trwałe.**

   Audyt środków trwałych polega na porównaniu dwóch migawek (ang. *snapshots*), czyli zarchiwizowanych stanów środków trwałych. Porównywać można dwie dowolne migawki lub wybraną migawkę ze stanem bieżącym. Z porównania uzyskujemy informacje o zmianach w inwentarzu, w tym także o brakach.

Aby dowiedzieć się więcej, przejdź do rozdziału Audyt środków trwałych.

Uwaga: Przed rozpoczęciem procesu inwentaryzacji w firmie, należy utworzyć migawkę, a następnie przy użyciu urządzenia mobilnego z zainstalowaną aplikacja mobilną zeskanować kody z etykiet środków trwałych (ewentualnie dodać ręcznie nowe urządzenia).

Podstawowe informacje



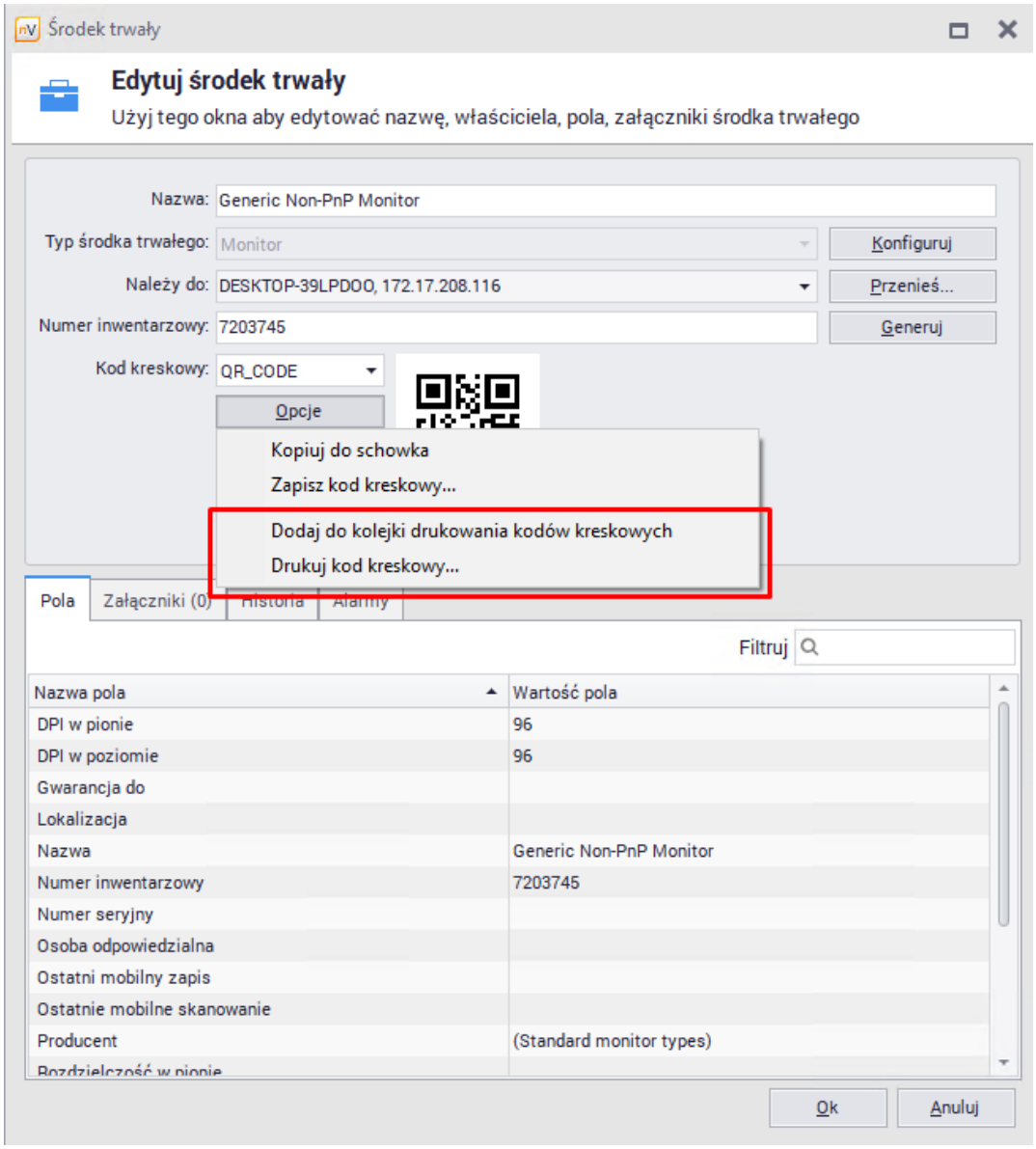
Każdy nowo tworzony środek trwały posiada wygenerowany automatycznie numer inwentarzowy. Standardowo numer taki składa się z 7 cyfr, jest prezentowany w postaci kodu kreskowego QR Code i jest unikalny. Liczbę 7 cyfrową można przedstawić w postaci każdego ze wspieranych rodzajów formatu kodu kreskowego (jednowymiarowe: CODABAR, COD 39, CODE 93, CODE 128, EAN 8, EAN 13, UPC A, UPC E; dwuwymiarowe: QR CODE).

7.5.9 Drukowanie etykiet

Dodawanie do kolejki

Aby wydrukować etykiety dla wybranych środków trwałych, należy użyć opcji **Dodaj do kolejki drukowania kodów kreskowych**. Można to zrobić na trzy sposoby:

1. Z poziomu okna edycji danego środka trwałego (patrz poniższy zrzut ekranowy).
2. Z poziomu okna właściwości danego środka trwałego poprzez kliknięcie prawym przyciskiem myszy na danym środku i wybranie opcji **Dodaj do kolejki drukowania kodów kreskowych**.
3. Z poziomu głównego okna nVision, zakładka **Środki trwałe**, poprzez kliknięcie prawym przyciskiem myszy na danym środku i wybranie opcji **Dodaj do kolejki drukowania kodów kreskowych**.

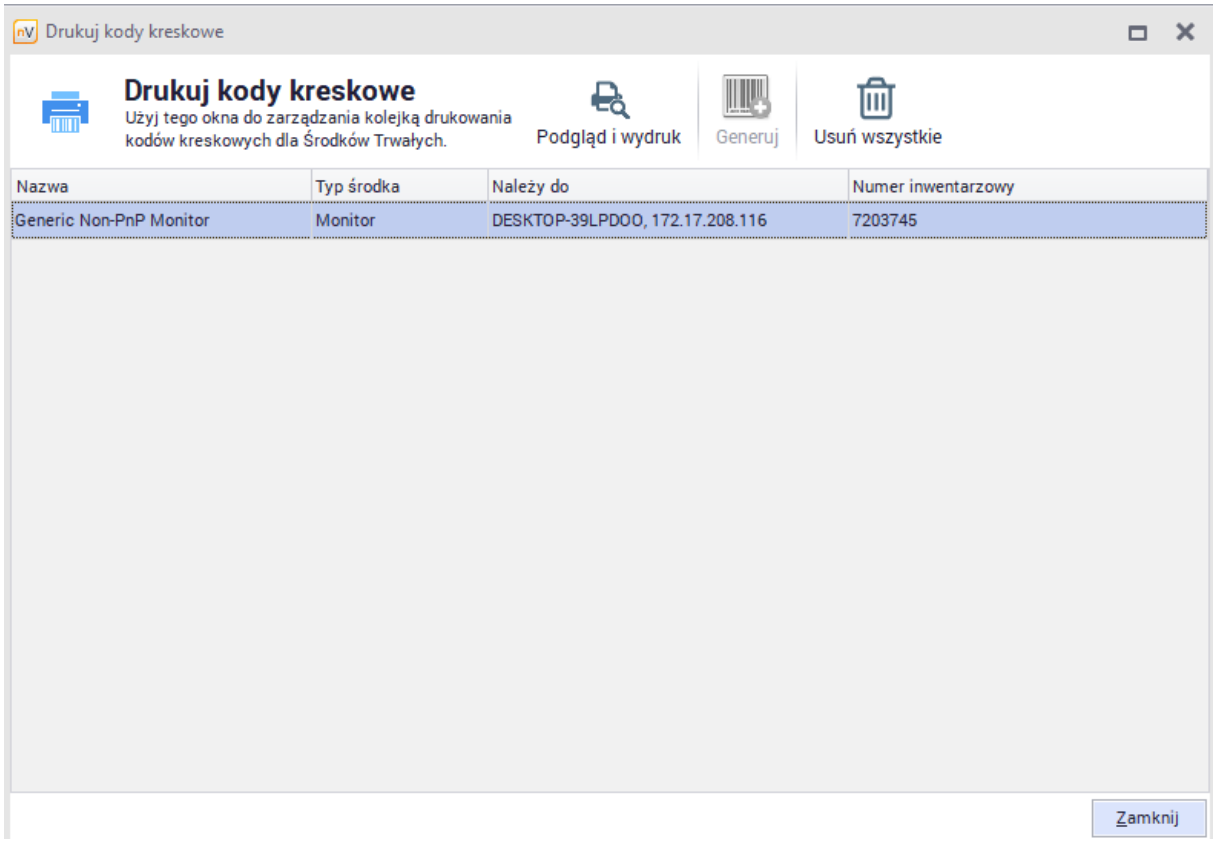


Drukowanie

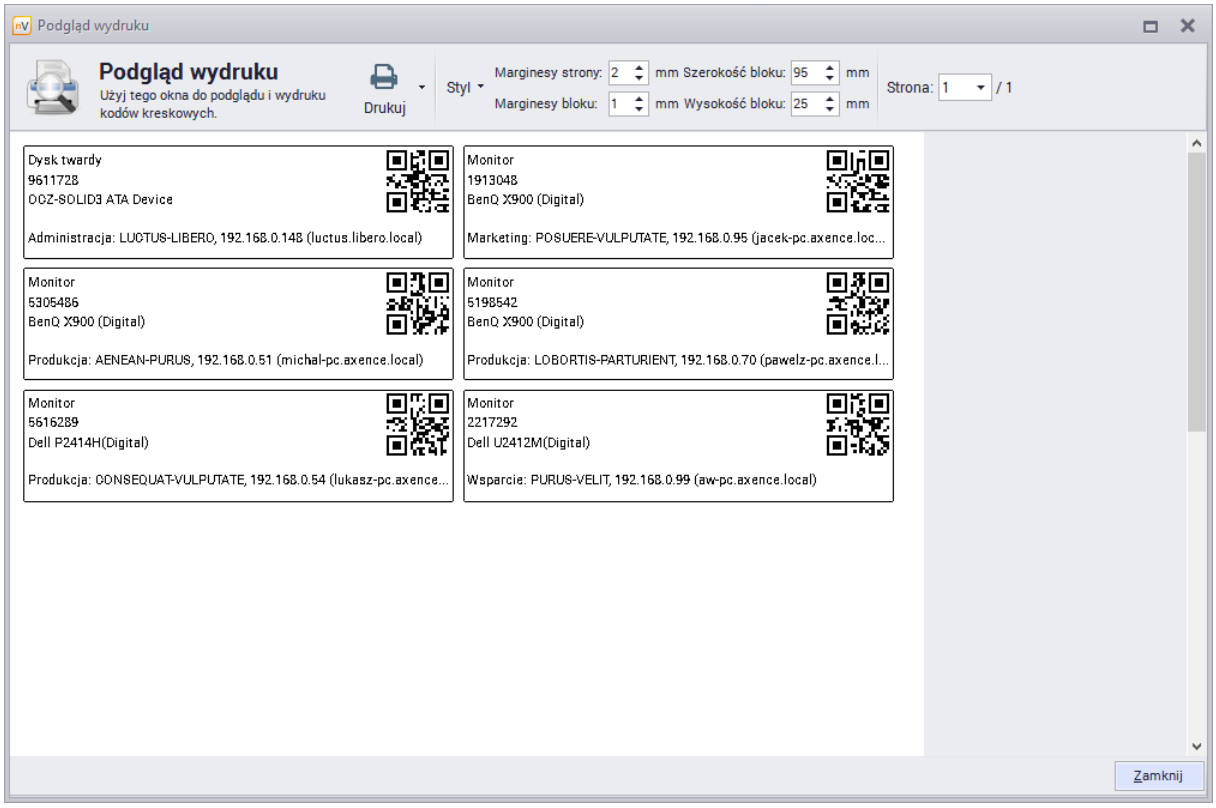
Po dodaniu do kolejki wszystkich środków trwałych, dla których mają być wydrukowane etykiety,

wykonaj następujące działania:

1. W głównym oknie nVision na pasku narzędziowym wybierz opcję **Drukuj kody kreskowe**.
2. W oknie **Drukuj kody kreskowe** są widoczne wszystkie środki trwałe, dla których użyto wspomnianej wcześniej opcji **Dodaj do...**.



3. Jeśli chcesz usunąć z listy dany środek trwały, kliknij na nim prawym przyciskiem i wybierz opcję **Usuń**. Aby wyczyścić listę, użyj opcji **Usuń wszystkie**. Uwaga: powyższe opcje nie usuwają środków trwałych, tylko elementy do drukowania.
4. Jeżeli choć jeden z wybranych środków trwałych nie ma jeszcze przypisanego numeru inwentarzowego, to aktywny jest przycisk , który pozwala na automatyczne uzupełnienie braków.
5. Aby przejść dalej, wciśnij przycisk .
6. Podglądu wydruku odzwierciedla ustawienia wybranej drukarki, a w szczególności rozmiar papieru i orientację strony w skali 1:1. Blok, którego parametry konfigurujemy, to pojedynczy prostokąt z kodem kreskowym i resztą informacji, które zostaną nadrukowane na etykiecie. Ilość bloków na stronie wynika bezpośrednio z ustawionych marginesów i wymiarów. Kody kreskowe są drukowane w taki sposób, aby uzyskać stały wymiar pojedynczego punktu (kreski) w milimetrach niezależnie od rozdzielczości (dokładności) wydruku.
   Na poniższym zrzucie ekranowym jest zaprezentowany typowy podgląd wydruku dla strony A4. W przypadku drukarek przeznaczonych do wydruku etykiet, na podglądzie będzie widoczny tylko jeden bloczek, a liczba stron będzie równa liczbie etykiet do wydrukowania.



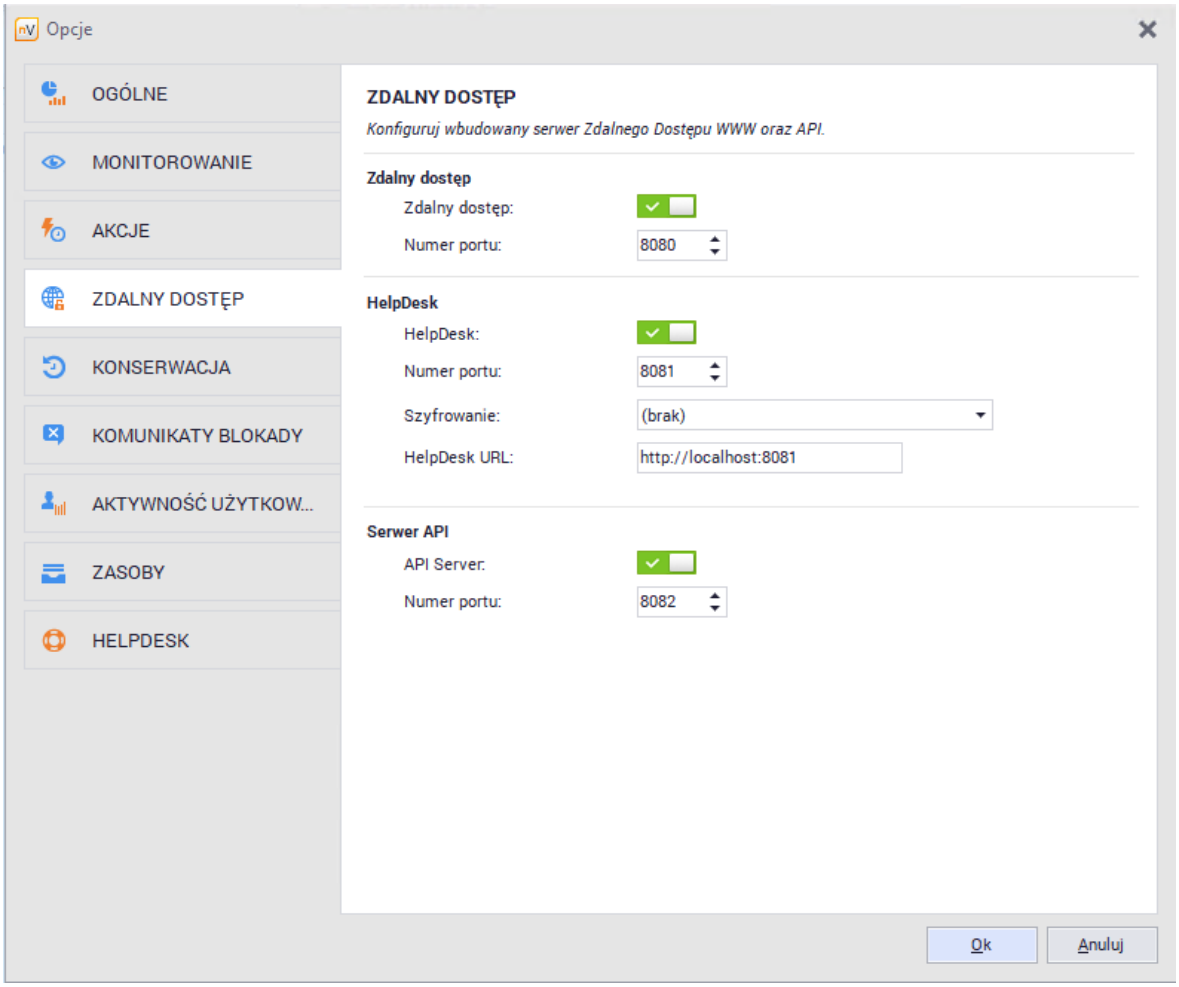
7. Po wybraniu opcji **Drukuj / Drukuj wszystko** następuje drukowanie wszystkich stron. Po zakończeniu nastąpi automatyczne zamknięcie okien **Podglądu wydruku** oraz **Drukuj kody kreskowe**, a lista środków trwałych wybranych do drukowania zostanie wyczyszczona.

7.5.10 Aplikacja mobilna dla systemu Android

Przygotowanie konsoli nVision na potrzeby dostępu aplikacji mobilnych

Konfiguracja serwera API

1. W głównym oknie nVision wybierz **Narzędzia / Opcje / Zdalny dostęp**. Upewnij się, że opcja **Włącz serwer API** jest zaznaczona.
2. Zapamiętaj **numer portu** serwera API, który będzie potrzebny w aplikacji mobilnej lub do przekierowania na routerze. Skonfigurowany port powinien zostać otwarty na zaporze sieciowej.

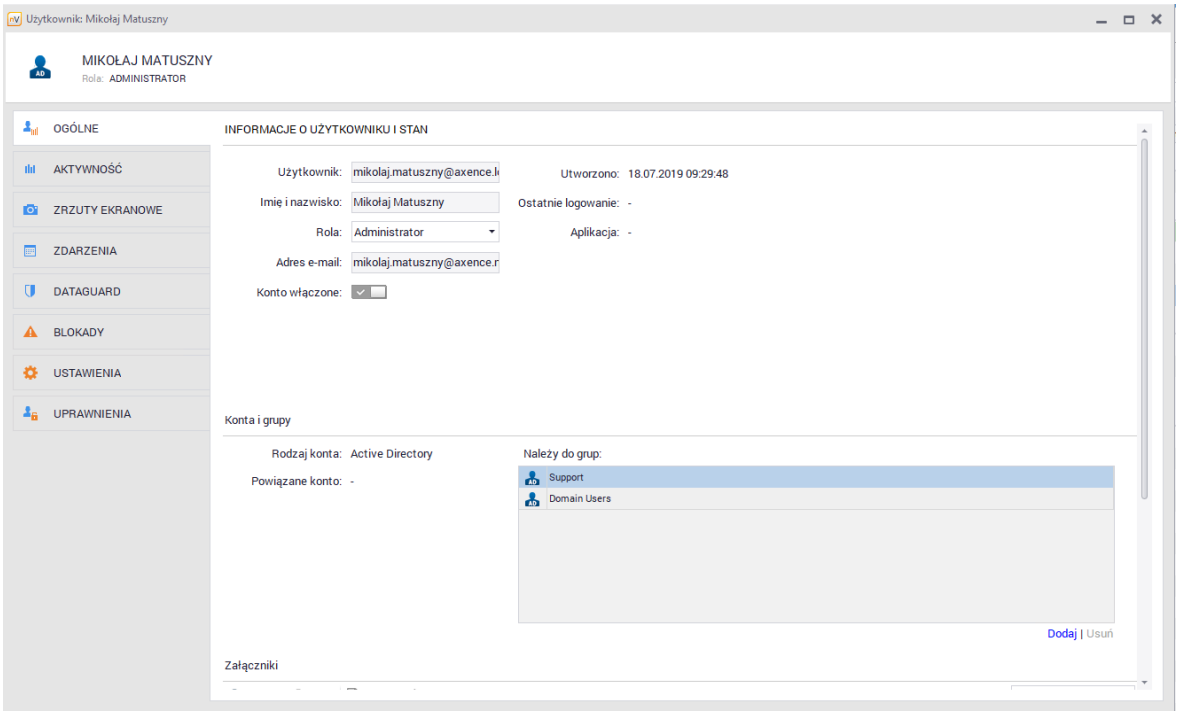


Konto użytkownika

Na potrzeby autoryzacji aplikacji mobilnej niezbędne są dane logowania administratora systemu.

Odpowiednie konto należy utworzyć w oknie **Użytkownicy** wybierając opcję **Dodaj**.

Jeśli konta użytkowników zostały pobrane z usługi Active Directory, to nie ma potrzeby tworzenia dodatkowego konta administratora.



Praca z aplikacją mobilną

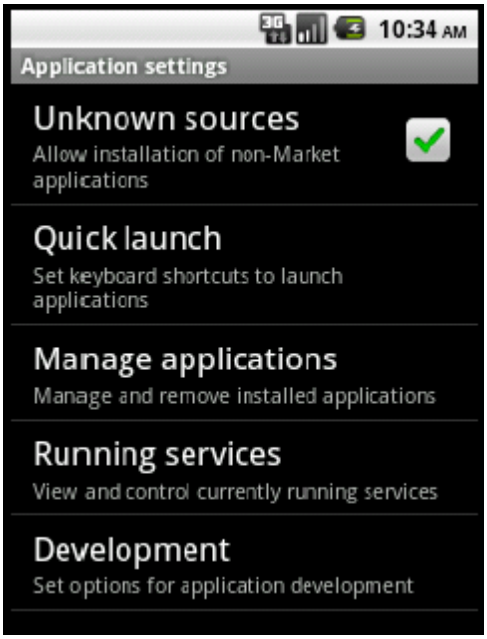
Instalacja

Aktualnie aplikacji nie można jeszcze pobrać za pośrednictwem sklepu Google Play, dlatego plik instalacyjny **"nVFixedAssets.apk"** należy skopiować na urządzenie mobilne (np. za pośrednictwem poczty e-mail albo linku do strony www) i własnoręcznie zainstalować.

Plik instalacyjny znajduje się w katalogu **"Mobile"** w ścieżce instalacji Serwera nVision (domyślnie: **'C:\Program Files\Axence\nVision\Mobile\'**).
Plik instalacyjny może zostać pobrany również bezpośrednio z Serwera nVision:

```
http://IP_SERWERA:4436/nVFixedAssets.apk
```

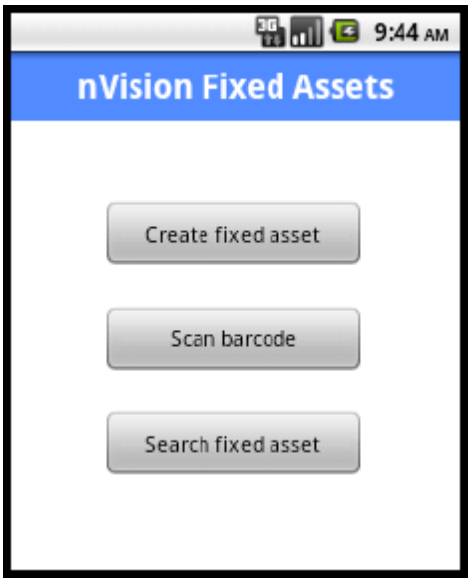
Uwaga: aby instalacja była możliwa, konieczne jest włączenie opcji zezwalającej na instalację aplikacji spoza oficjalnego sklepu Google. Dostęp do tego ustawienia można uzyskać poprzez dłuższe przytrzymanie przycisku **Menu**, następnie wybranie opcji **Settings | Applications** i zaznaczenie **Unknown sources**.



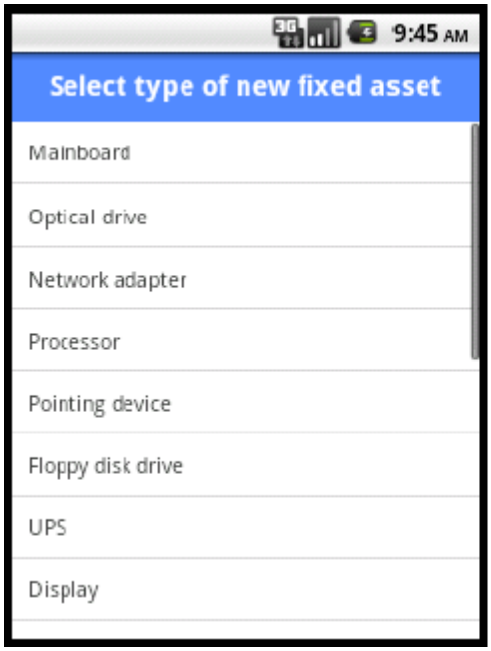
Logowanie

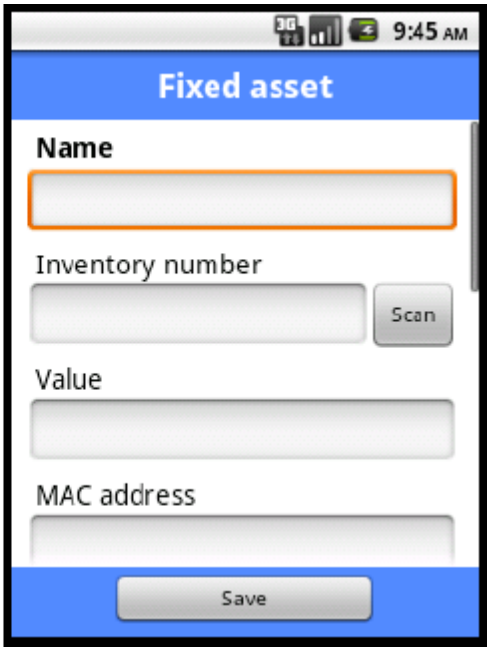
Na ekranie logowania należy wprowadzić adres komputera, na którym pracuje konsola nVision, wraz z numerem portu serwera API. W przypadku pracy poza firmową siecią WiFi konieczne może być dokonanie odpowiedniego przekierowania portu na routerze dostępowym. Zaznaczenie opcji **Remember me** spowoduje, że wprowadzone hasło zostanie zapamiętane i przy następnym uruchomieniu aplikacji automatycznie nastąpi próba połączenia.

Opcje ekranu głównego

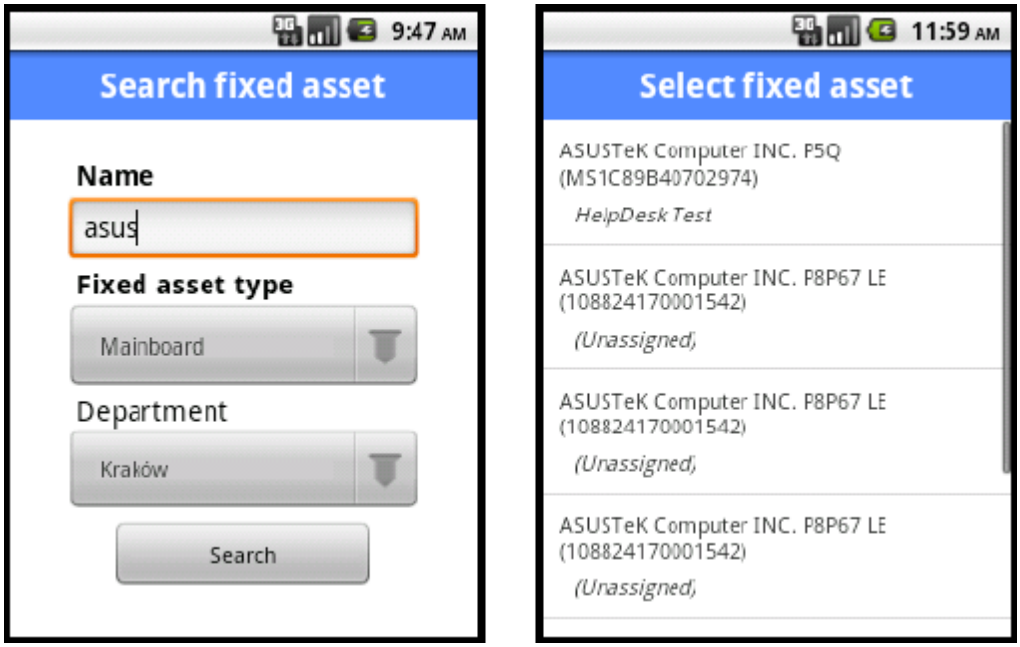


1. **Create fixed asset** - opcja tworzenia nowego środka trwałego. Najpierw należy wprowadzić typ środka trwałego, a następnie pozostałe dane w oknie edycji środka trwałego. Przycisk **Save** zatwierdza wprowadzone zmiany.





2. **Scan barcode** – skanowanie kodu kreskowego. Jeśli w bazie danych istnieje środek trwały z przypisanym kodem to zostanie wyświetlony. Jeśli nie, aplikacja proponuje utworzenie nowego z wprowadzonym kodem jako **Inventory number**.
3. **Search fixed asset** – wyszukiwanie środków trwałych wg nazwy, typu i (opcjonalnie) oddziału (**Department**). Nazwa (**Name**) musi zawierać przynajmniej 3 znaki. Jeśli znaleziono przynajmniej jeden pasujący środek trwały, to zostanie wyświetlona lista z wyborem. Wybranie rekordu z listy otwiera środek trwały w trybie edycji. Wciśnięcie przycisku **Wstecz** skutkuje powrotem do listy znalezionych.

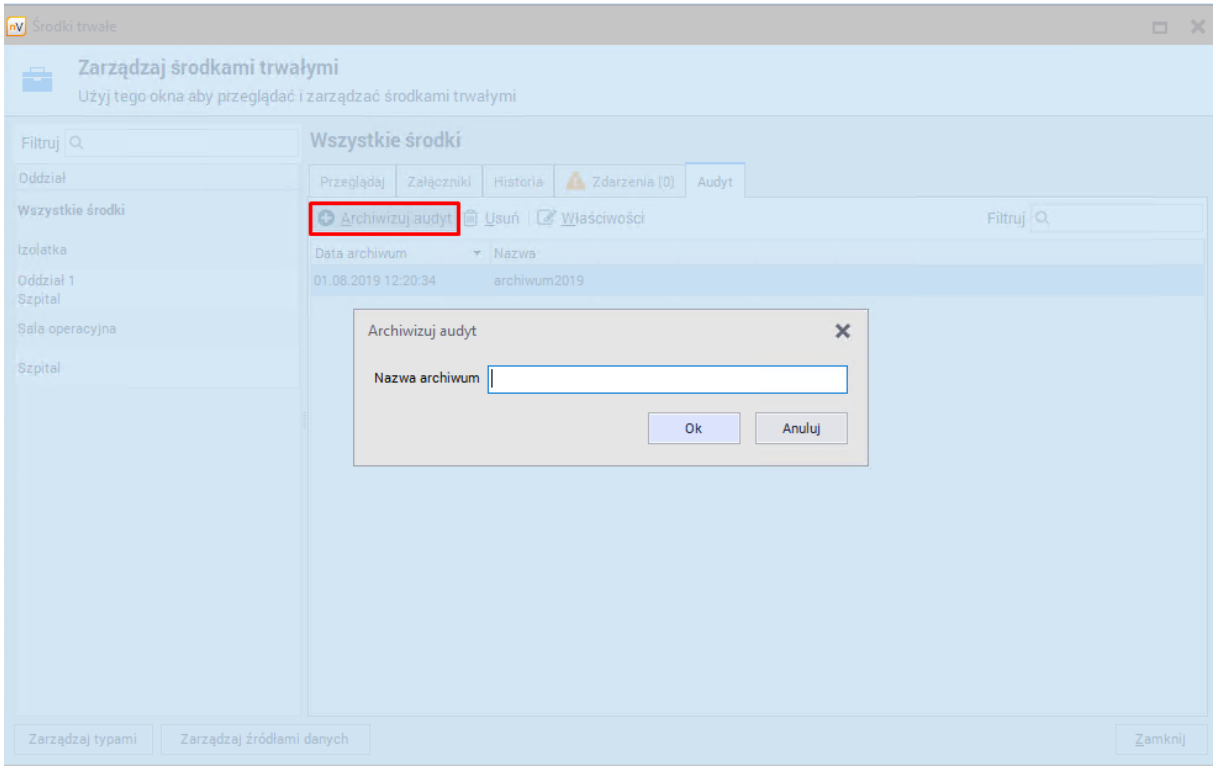


7.5.11 Audyt środków trwałych

Audyt środków trwałych polega na porównaniu dwóch migawek (ang. *snapshots*), czyli zarchiwizowanych stanów środków trwałych. Porównywać można dwie dowolne migawki lub wybraną migawkę ze stanem bieżącym.

Aby dokonać audytu środków trwałych:

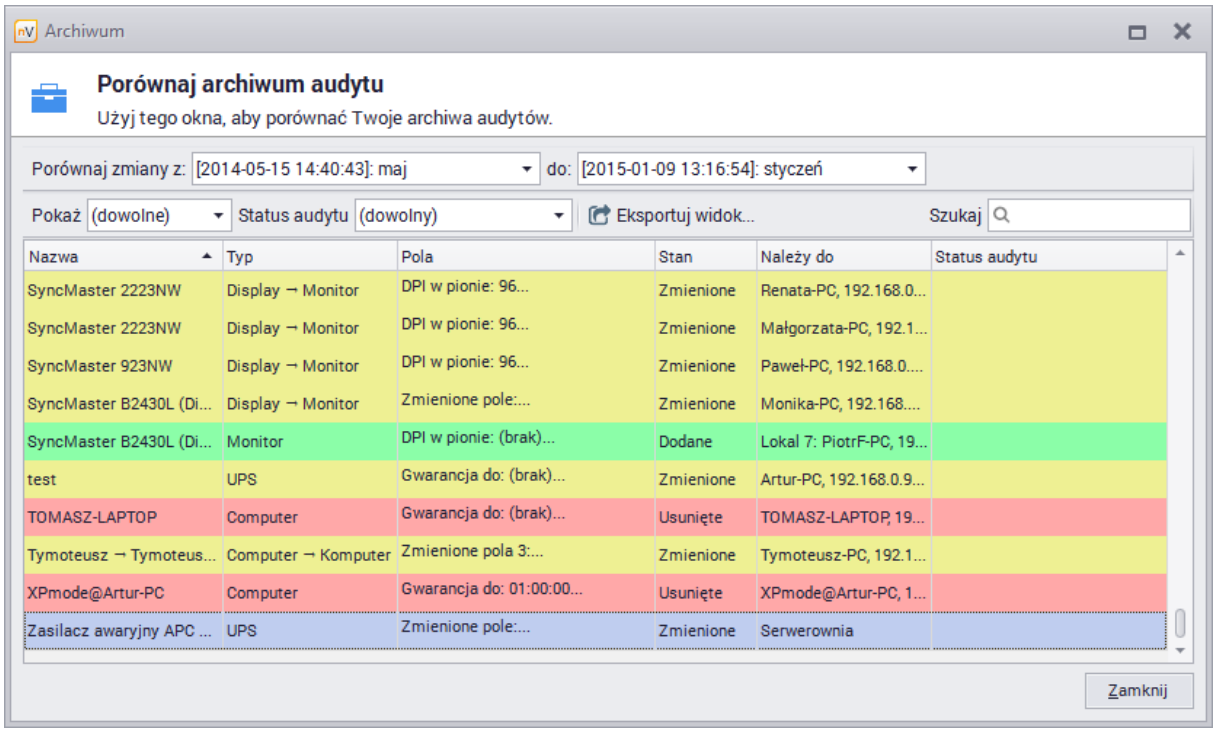
1. W głównym oknie nVision kliknij w przycisk **Środki trwałe**. Przejdź do zakładki **Audyt**.



2. Warunkiem koniecznym do utworzenia migawki jest to, aby ilość zdarzeń oczekujących na

akceptację przez użytkownika była równa zero. Jeśli jest inaczej, przed prośbą o podanie nazwy migawki, pojawi się okno z pytaniem o akceptację wszystkich zdarzeń.

3. Zaznacz archiwum (migawkę), którą chcesz porównywać i przejdź do jej **Właściwości**.
4. Poszczególne typy środków trwałych są porównywane w trakcie audytu pod warunkiem, że w obu porównywanych migawkach zostały zapisane (aby dowiedzieć się więcej, przejdź do rozdziału Typy środków trwałych).
5. W oknie **Porównaj archiwum audytu** należy wybrać archiwa do porównania oraz opcje **Pokaż (stan)** i **Status audytu** (opisane poniżej).



Stan i status audytu

Opcje **Pokaż (stan)** oraz **Status audytu** pozwalają na ograniczenie liczby wyświetlanych rekordów i szybkie dotarcie do najważniejszych informacji. Zależności pomiędzy stanami i statusami są przedstawione w następującej tabeli:

Stan	Możliwy status
Bez zmian	• Zaudytowany • Niezaudytowany
Dodane	• Zaudytowany • Niezaudytowany
Usunięte	• Niezaudytowany
Zmienione	• Zaudytowany • Niezaudytowany

Status **Zaudytowany/Niezaudytowany** jest ściśle powiązany z faktem, czy pomiędzy dwoma migawkami porównywanymi w audycie była używana aplikacja mobilna.

Ważne: jeśli używana jest Aplikacja mobilna, to należy przeskanowć wszystkie urządzenia (kody kreskowe). Te, których nie zeskanowano, zostaną potraktowane jako niezaudytowane i należy traktować je jako brakujące. Przez „użycie aplikacji mobilnej" należy rozumieć wyszukanie środka trwałego za pomocą skanowania kodu kreskowego lub przy użyciu innych parametrów (np. podając fragment z nazwy) i wykonanie opcji zapisu.

7.5.12 Alarmy

Alarmy dla środków trwałych mogą być utworzone dla pojedynczych środków trwałych lub dla wszystkich środków danego typu.

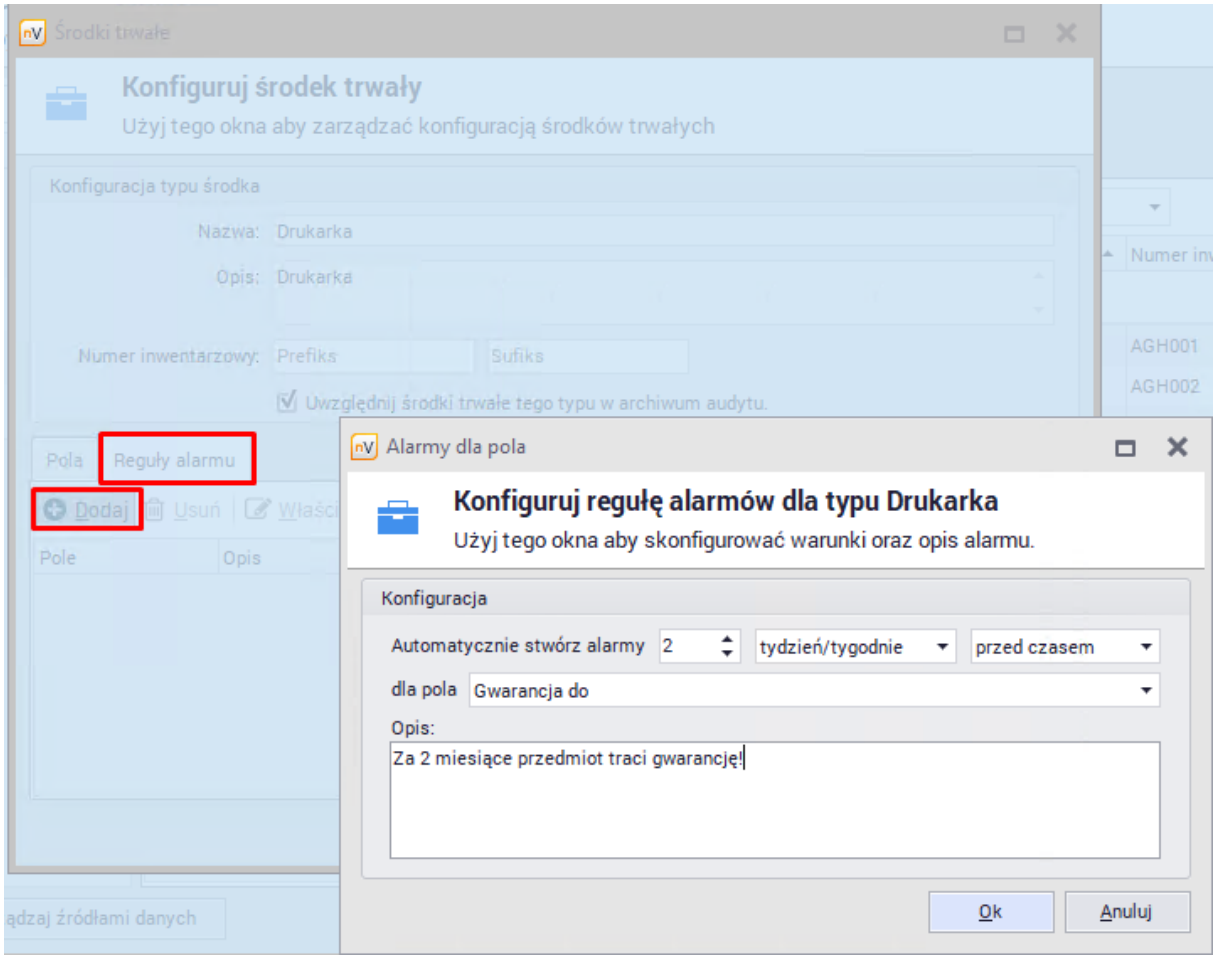
Alarmy dla typu środków trwałych

W poniższej tabeli wymienione są zdarzenia, dla których można zdefiniować alarm:

Nazwa	Opis
Gwarancja do	Data wygaśnięcia gwarancji
Ostatni mobilny zapis	Kiedy środek trwały został zapisany za pośrednictwem aplikacji mobilnej
Ostatnie mobilne skanowanie	Kiedy środek trwały był skanowany za pośrednictwem aplikacji mobilnej

Aby utworzyć alarm dla typu środków trwałych:

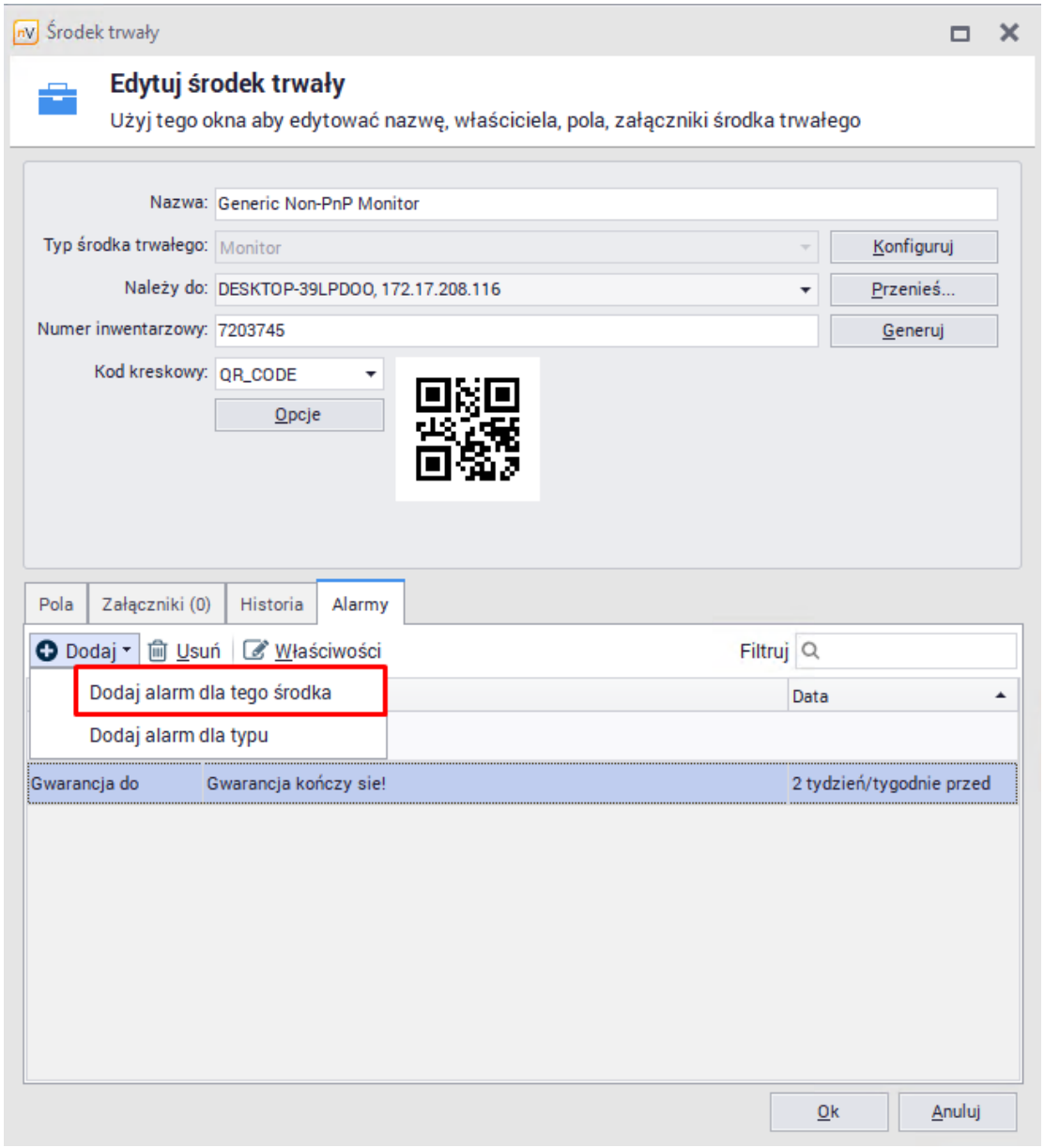
1. W głównym oknie nVision rozwiń menu przy przycisku **Środki trwałe**. Wybierz opcję **Zarządzaj typami.**
2. Zaznacz wybrany typ i przejdź do **Właściwości**.
3. Przejdź do zakładki **Reguły alarmu** i kliknij **Dodaj**.
4. W oknie **Konfigurowania reguły alarmów** wybierz zdarzenie (pole), dla którego chcesz utworzyć alarm i ustaw, kiedy alarm ma być utworzony. Wprowadź opis alarmu i kliknij **OK**.



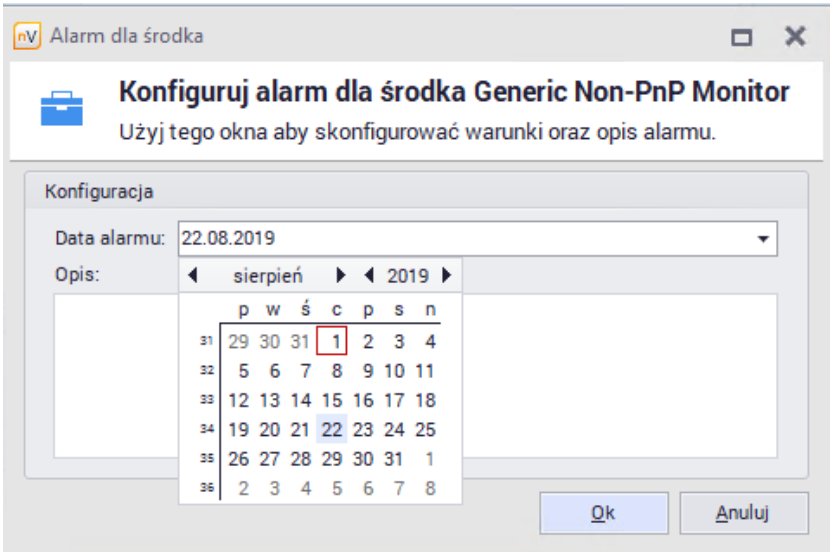
Alarmy dla poszczególnych środków trwałych

Aby utworzyć alarm dla danego środka trwałego:

1. W głównym oknie nVision kliknij w przycisk **Środki trwałe**.
2. W oknie **Zarządzania środkami trwałymi** zaznacz wybrany środek trwały i przejdź do **Właściwości**.
3. Przejdź do zakładki **Alarmy**. Są tu widoczne wszystkie wcześniej zdefiniowane alarmy dotyczące tego środka trwałego (także wynikające z przynależności do typu).



4. Kliknij w przycisk **Dodaj** i wybierz opcję **Dodaj alarm dla tego środka**.
5. Wybierz datę alarmu i podaj opis. Kliknij **OK**.



Z poziomu okna danego środka trwałego można też definiować alarmy dla typu (opcja **Dodaj alarm dla typu**).

Aby dowiedzieć się więcej o alarmach, przejdź do rozdziału Alarmowanie.

7.6 Skaner inwentaryzacji dla systemu Linux i OS X

Skaner inwentaryzacji dla systemu Linux/OS X jest narzędziem przenośnym umożliwiającym zbieranie manualne pobieranie danych o urządzeniu bez instalowania Agenta. Można go użyć także w sytuacji, gdy skanowany komputer nie może być podłączony do sieci.

Aby uruchomić skaner:

1. Pobierz plik skryptu skanera dla odpowiedniej architektury sprzętowej do folderu *C:\Program Files (x86)\Axence\nVision\Agents*:

OSX:

http://cdn.axence.net/linux/osx_scanner.run

Linux 32-bit:

http://cdn.axence.net/linux/linux_scanner32bit.run

Linux 64-bit:

http://cdn.axence.net/linux/linux_scanner64bit.run

2. Skopiuj plik skryptu skanera na pamięć zewnętrzną lub na ogólnodostępny udział sieciowy

3. Do poprawnego uruchomienia wymagane są uprawnienia administratora (*root*).
   Pamiętaj aby nadać atrybuty praw uruchomienia `chmod + x` *dla pliku skryptu skanera inwentaryzacyjnego.*

W terminalu/konsoli Linux/OS X uruchom polecenie:

```
> sudo ./*nazwa_skanera*.run /mnt/scans/
```

Po wykonaniu skanu w katalogu ***/mnt/scans/*** pojawi się przykładowo plik ***{bdf1bf72-8ad4-44b8-b754-e2b934410b50}.zip***, w którym zawarte będą wszystkie dostępne informacje o sprzęcie i oprogramowaniu. ***Uwaga!*** *Podczas następnego skanu z takimi samymi parametrami (katalog docelowy), poprzedni plik ze stanem sprzętowo-programowym zostanie nadpisany.*

Powiązane tematy

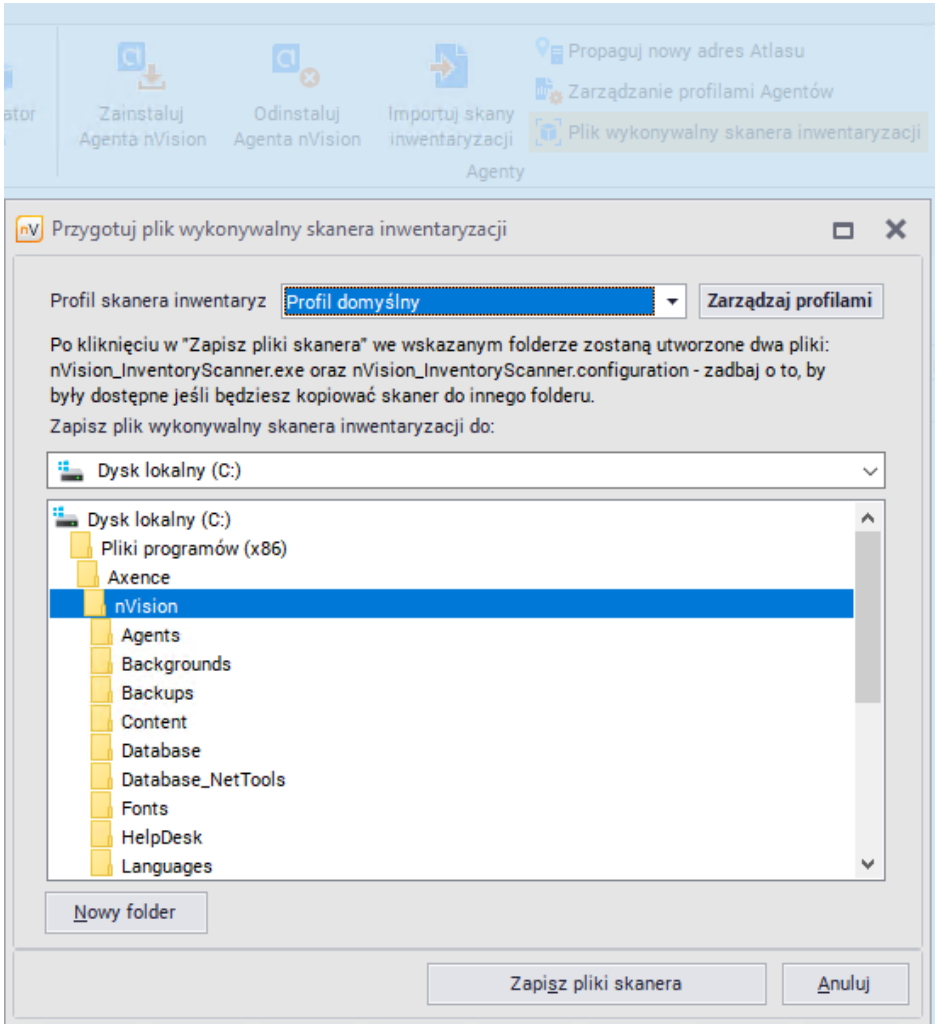
Aby zaimportować wyniki skanu, zapoznaj się z rozdziałem: Import skanów inwentaryzacji.

7.7 Import skanów inwentaryzacji

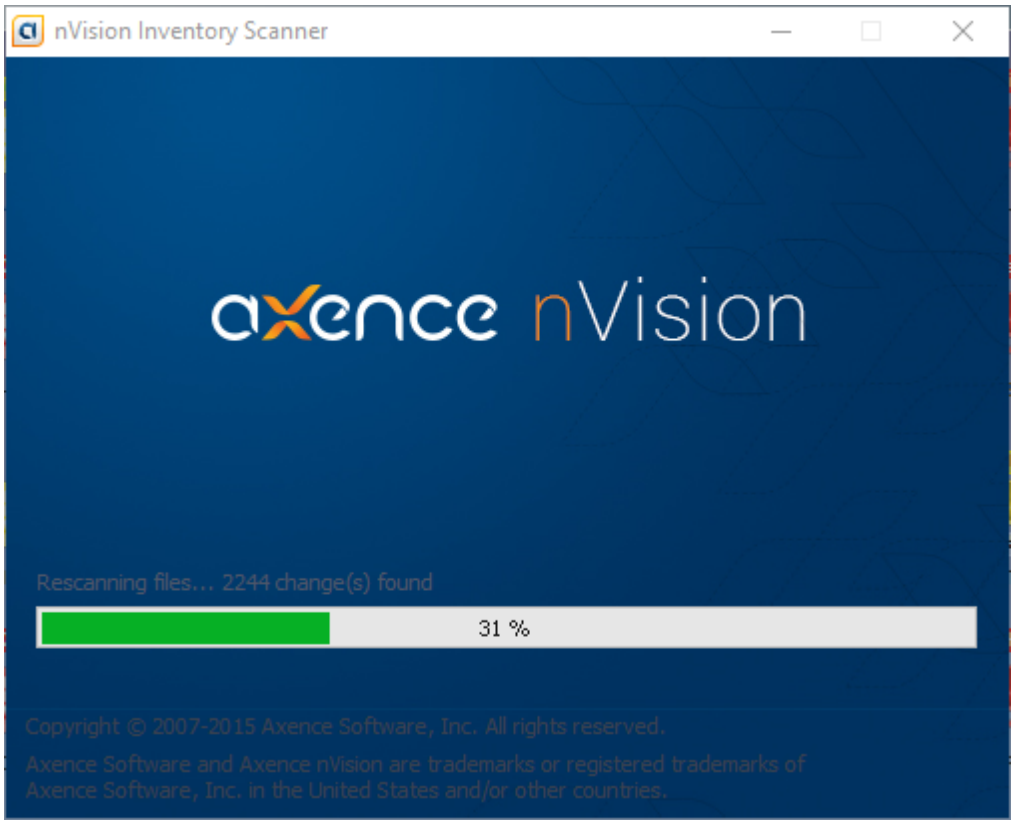
Skaner inwentaryzacji jest narzędziem przenośnym umożliwiającym zebranie danych o urządzeniu bez instalowania Agenta. Można go użyć także w sytuacji, gdy skanowany komputer nie może być podłączony do sieci.

Aby przeprowadzić ręczny import skanów inwentaryzacji, wykonaj następujące kroki:

1. **Przygotuj plik wykonywalny skanera inwentaryzacji**
   a. W tym celu w zakładce Narzędzia i opcje wybierz opcję **Plik wykonywalny skanera inwentaryzacji**.
   b. Wybierz lokalizację, w której mają być utworzone pliki skanera inwentaryzacji (np. pendrive).
   c. Ustaw profil skanera inwentaryzacji, czyli jakie informacje będą zbierane przez skaner. Możesz wybrać istniejący profil z listy, edytować istniejący profil lub utworzyć nowy.
   d. Kliknij w przycisk **Zapisz pliki skanera**.



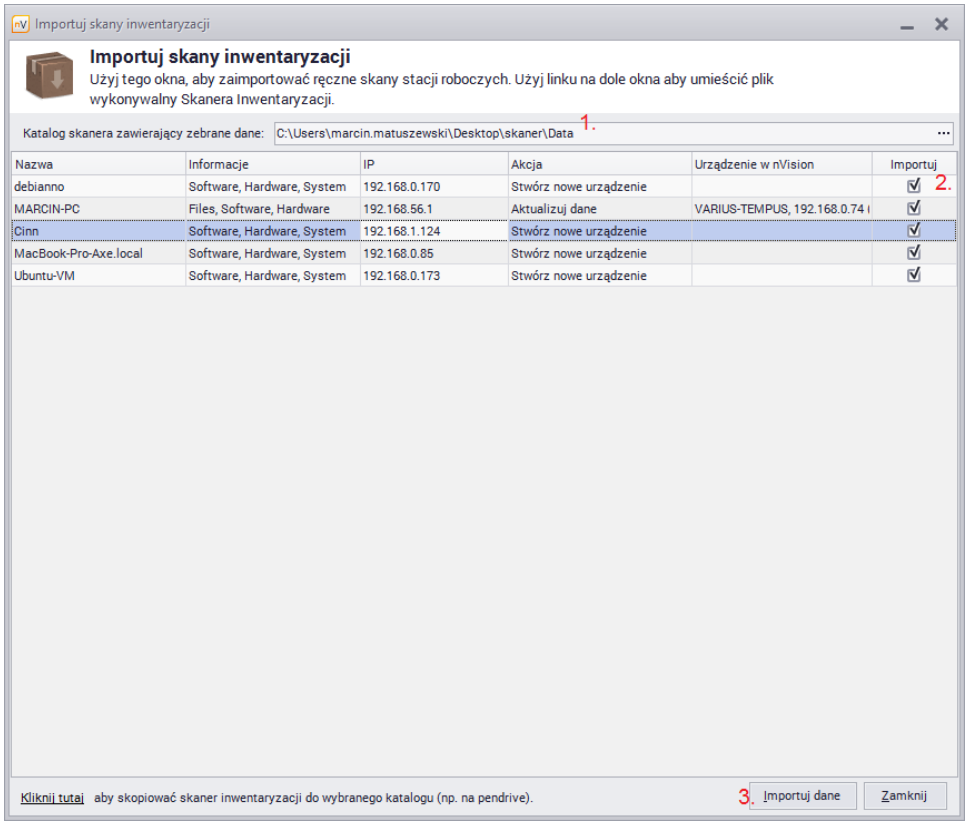
2. **Wykonaj skan inwentaryzacji**. Jeśli będziesz kopiować skaner do innej lokalizacji, to zadbaj o skopiowanie obu plików skanera (nVision_InventoryScanner.exe oraz nVision_InventoryScanner.config). Uruchom plik wykonywalny skanera inwentaryzacji (nVision_InventoryScanner.exe) na komputerze, który ma być skanowany, aby rozpocząć proces skanowania.



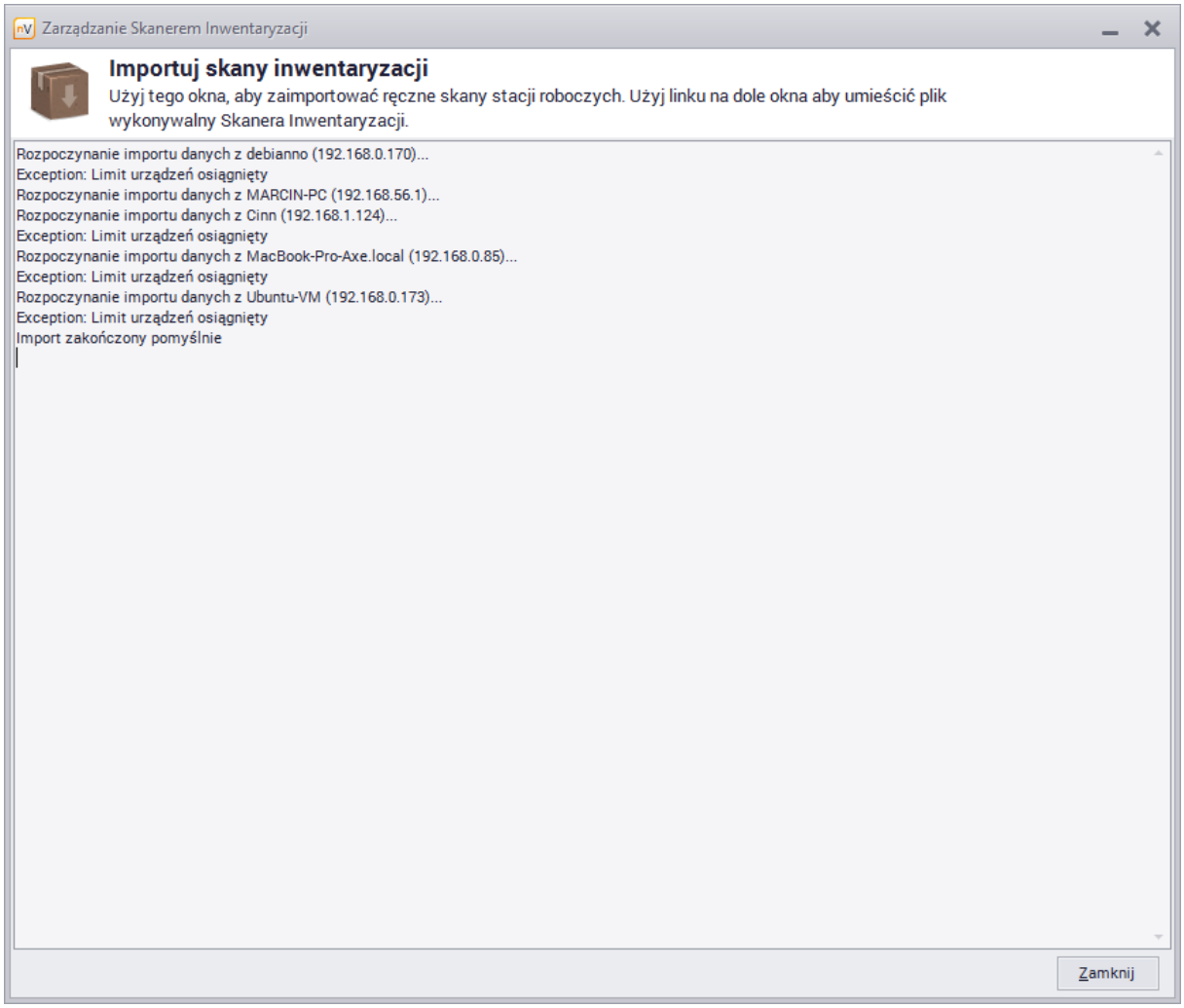
3. **Importuj dane**

   a. Po zakończeniu skanowania, skopiuj utworzone foldery (Data oraz Logs) do lokalizacji, która będzie widoczna z poziomu konsoli nVision.

   b. W oknie importowania skanów inwentaryzacji (**Importuj skany inwentaryzacji** w menu Narzędzia i opcje) wybierz folder, w którym znajdują się skany (czyli skopiowany wcześniej folder Data).



c. Sprawdź, czy zaznaczone jest pole **Importuj** dla skanowanego urządzenia, a następnie kliknij w przycisk **Importuj dane**.



d. Jeżeli import danych został zakończony pomyślnie, to zostanie wyświetlona stosowna informacja (Import zakończony pomyślnie).

Powiązane tematy

Inwentaryzacja sprzętu i oprogramowania

7.8 Menedżer pakietów MSI

Agent nVision umożliwia również zarządzanie instalacjami programów na monitorowanych komputerach poprzez:

- instalację programów wymaganych w firmie,
- deinstalację niautoryzowanych programów.

Zarządzanie instalacjami oprogramowania odbywa się w oparciu o repozytorium paczek (plików) MSI. Paczka MSI to obiekt utworzony na bazie pliku instalacyjnego o rozszerzeniu MSI, który jest zgodny z Windows Installer (https://pl.wikipedia.org/wiki/Windows_Installer). Paczki instalacyjne uznawane są jako unikalne gdy we własnościach pliku MSI różnią się kodem produktu (productCode), wersją produktu

(productVersion), językiem produktu (productLanguage). Działanie Agenta umożliwia również zainstalowanie aktualizacji, nie pozwala jednak na "downgrade" aplikacji.

Schemat działania Agenta

1. Agent instaluje paczki dopiero po pobraniu wszystkich, które dla niego skonfigurowano ponieważ uwzględnia priorytety określone we właściwościach paczek.

2. Działanie Agenta dopuszcza instalację tylko gdy aplikacja nie jest w ogóle zainstalowana albo jest zainstalowana w starszej wersji niż ta, którą otrzymał Agent (aktualizacja).

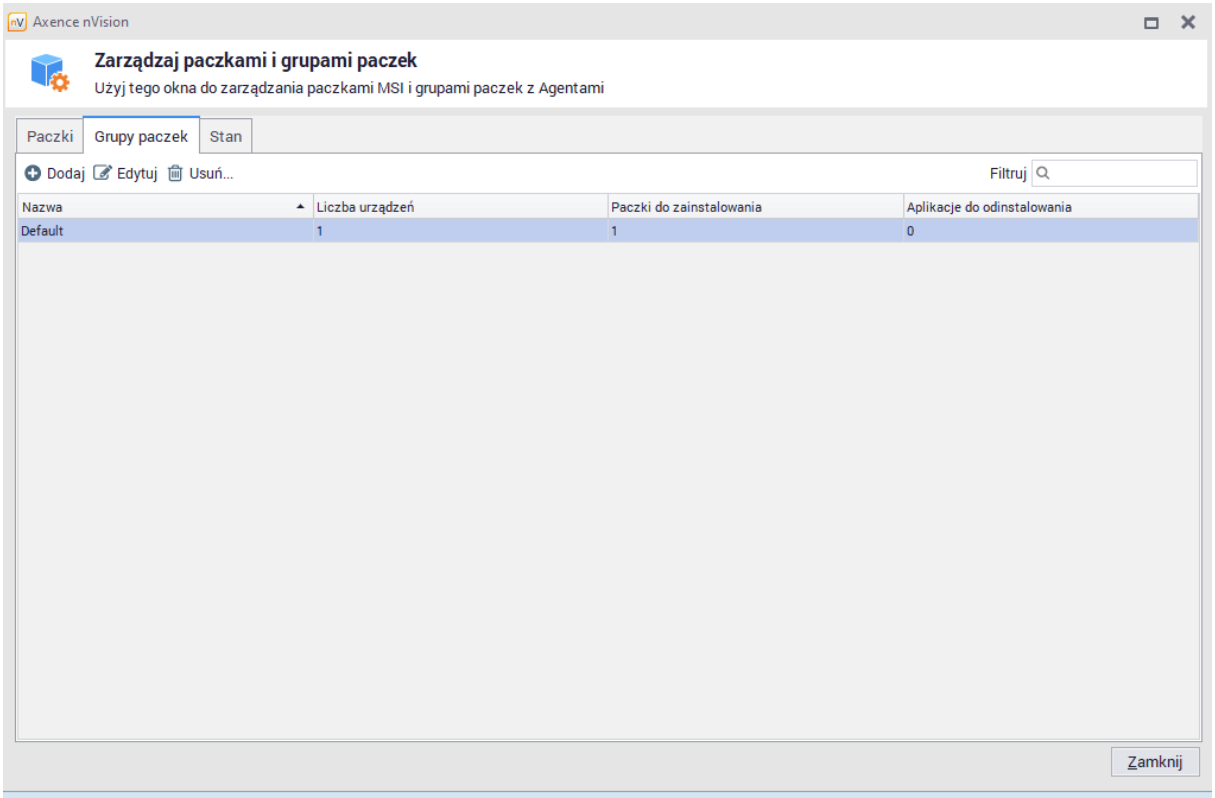
3. Agent cyklicznie sprawdza czy wszystkie aplikacje z paczek przeznaczonych dla niego są zainstalowane - w przypadku wykrycia braków, dokonuje ponownej instalacji. Proces ten odbywa się niezależnie od zaznaczenia w profilu Agenta opcji skanowania informacji o oprogramowaniu.

4. Lista aplikacji (paczek) do odinstalowania generowana jest na podstawie informacji zebranych przez Agenty poprzez monitorowanie wpisów rejestrowych zainstalowanych aplikacji oraz odczytanych informacji o instalacjach z pakietów MSI. Agent cyklicznie sprawdza czy aplikacja zaznaczona do usunięcia została zainstalowana - w przypadku wykrycia, dokonuje ponownej jej deinstalacji.

Aby zarządzać paczkami MSI i grupami paczek poprzez Menedżer pakietów MSI:

1. Wybierz z głównego menu programu **Menedżer pakietów MSI.**

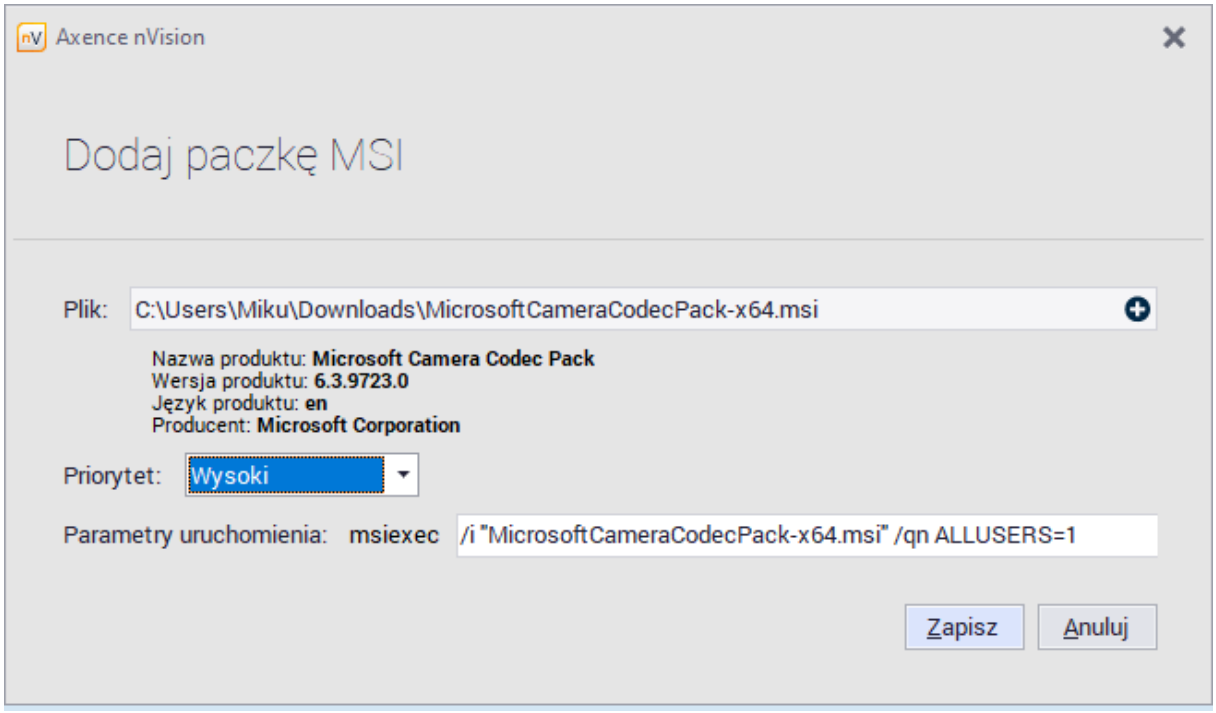
2. W oknie **Zarządzaj paczkami i grupami paczek / Paczki,** kliknij przycisk **Dodaj :**



3. W oknie dialogowym, wskaż plik instalatora MSI.

4. W oknie dodawania paczki, ustaw priorytet instalacji (uwzględniany przy instalacji kilku paczek w

ramach jednej grupy) oraz dodatkowe parametry uruchomienia (skopiowane ze strony producenta instalatora MSI). Kliknij **Zapisz:**

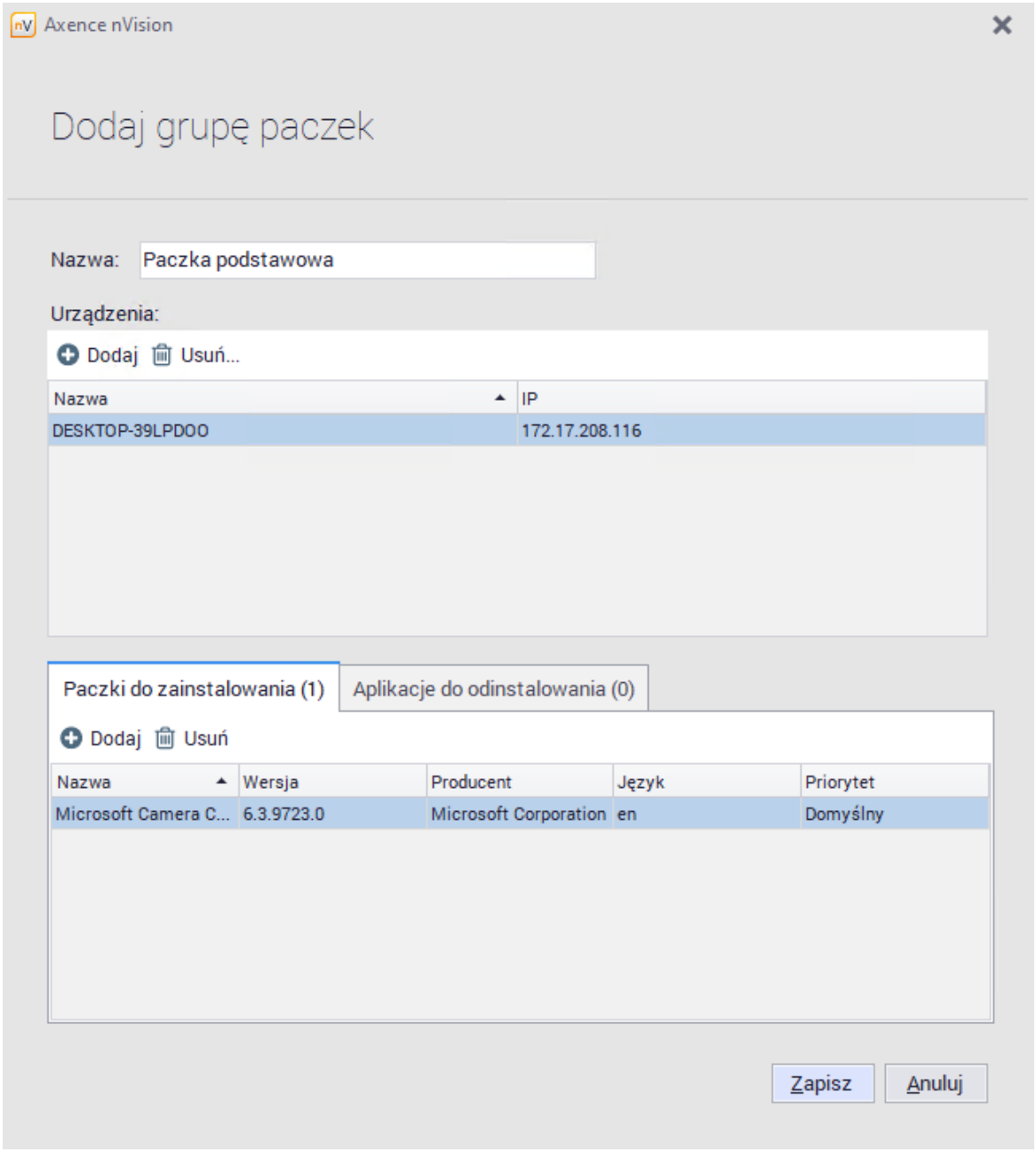


5. Przejdź do zakładki **Grupy paczek,** kliknij przycisk **Dodaj.** Utwórz nową grupę poprzez wskazanie:

a. nazwy grupy

b. urządzeń, na których mają być instalowane lub deinstalowane wskazane aplikacje

c. paczek do zainstalowania (utworzonych w punkcie 4) lub aplikacji do odinstalowania (na podstawie informacji zebranych przez Agenty poprzez monitorowanie wpisów rejestrowych zainstalowanych aplikacji).



6. Kliknij przycisk **Zapisz.** Stan wykonania zadań na urządzeniach, przedstawiony jest w kolejnej zakładce okna **Zarządzaj paczkami i grupami paczek.**
7. Zarówno paczki i grupy paczek mogą być edytowane poprzez 2-krotne kliknięcie lub zaznaczenie i kliknięcie przycisku **Edytuj.**
8. W zakładce stan mamy możliwość sprawdzenia postępu instalacji.

Część VIII

8 DataGuard - ochrona danych

8.1 Wprowadzenie

Axence nVision® DataGuard umożliwia zarządzanie prawami dostępu do danych i ich ochroną. W szczególności, zastosowanie ochrony danych zwiększa bezpieczeństwo firmy, zapobiega zainfekowaniu sieci firmowej wirusami przenoszonymi na pendrive'ach i chroni przed wyciekiem informacji.

Blokowanie urządzeń i nośników

Blokowane mogą być wszystkie urządzenia i nośniki traktowane jako dyski logiczne, między innymi:

- pendrive'y,
- dyski przenośne,
- Wi-Fi, Bluetooth, IrDA,
- aparaty fotograficzne oraz przenośne MP3 działające w trybie *urządzenia multimedialnego* - WPD,
- stacje dyskietek,
- gniazda SD.

Zarządzanie prawami dostępu

Zarządzanie prawami dostępu może odbywać się na różnych poziomach (atlasu, grup i poszczególnych użytkowników). Na każdym z tych poziomów można nadawać użytkownikom odpowiednie prawa związane z korzystaniem z nośników oraz z możliwościami audytu, odczytywania, zapisywania i wykonywania plików. Zarządzanie prawami dostępu przy użyciu nVision ułatwia konfigurację grup komputerów, autoryzowanie firmowych pendrive'ów i dysków oraz blokowanie prywatnych **urządzeń**. Aby dowiedzieć się więcej, przejdź do rozdziału Prawa dostępu.

8.2 Prawa dostępu

8.2.1 Prawa dostępu - wprowadzenie

Wdrażanie

Aby wdrożyć moduł DataGuard należy wybrać jedną z dwóch możliwych koncepcji:

1. **Zablokowanie wszystkich**/większości praw na poziomie atlasu, a następnie zezwalanie na konkretne akcje wraz z przemieszczaniem się w dół hierarchii.
2. **Zezwolenie na wszystkie działania** na poziomie atlasu i ograniczanie dostępu na poziomie map i dla konkretnych stacji roboczych.

Wybór jednej z powyższych strategii zależy od specyfiki systemu, do którego wdrażana jest ochrona danych.

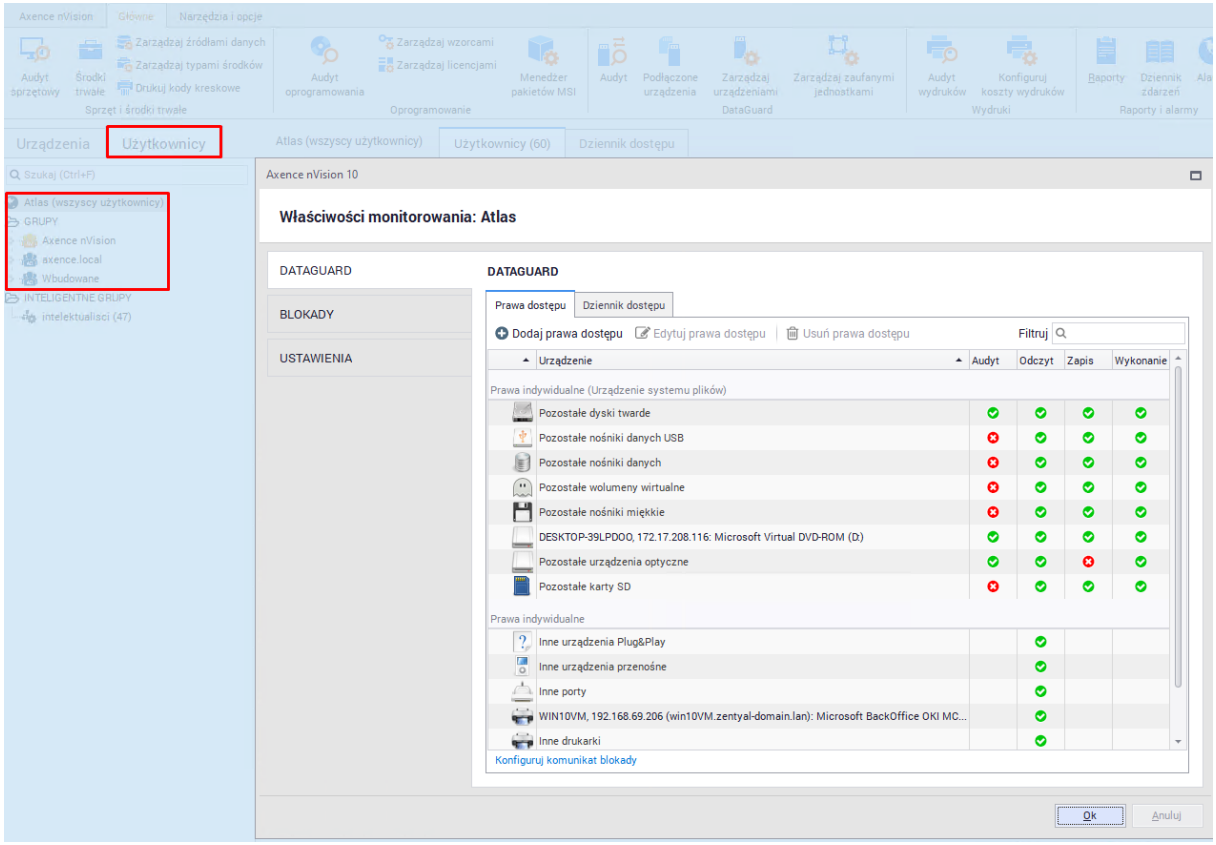
Prawa dostępu mogą być nadawane dla następujących kategorii:

- **Audyt** - określa, czy dostęp do danego urządzenia ma być logowany. Logowaniu podlegają informacje dotyczące zmiany nazwy, tworzenia, kopiowania, usuwania pliku oraz dostępu z zapisem.

- **Odczyt** - możliwość odczytywania informacji z określonego nośnika.
- **Zapis** - możliwość zapisywania informacji na określonym nośniku.
- **Wykonanie** - możliwość uruchamiania programów znajdujących się na określonym nośniku.

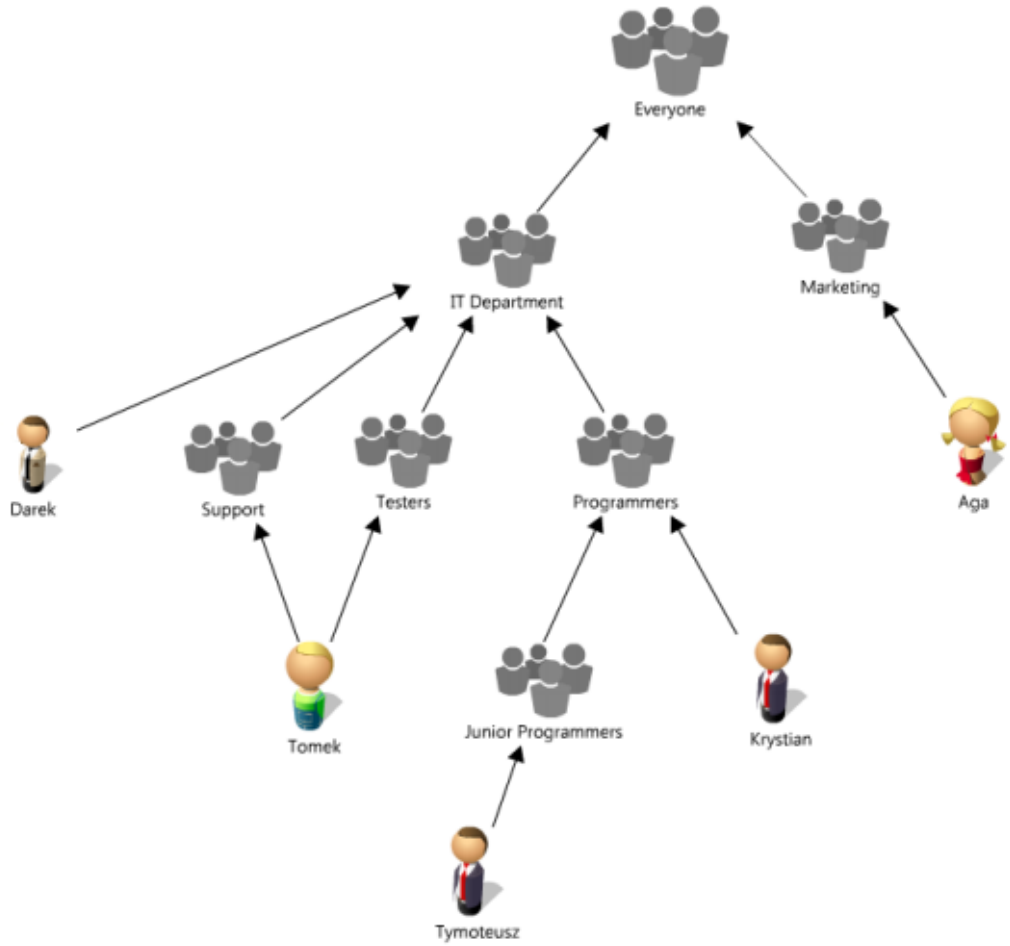
Każda z kategorii (odczyt, zapis, wykonanie) może przyjmować jeden z dwóch stanów: **zezwól** lub **blokuj**. Audyt może być **włączony** lub **wyłączony**. Urządzenia nieposiadające systemu plikowego mają tylko jedną kategorię prawa dostępu. Przyjmuje ona wartość **włączony**, jeśli dopuszczone jest korzystanie z tego urządzenia i **wyłączony** w przeciwnym wypadku.

Aby określić prawa dostępu do nośników należy przejść do właściwości atlasu, grupy lub użytkownika:



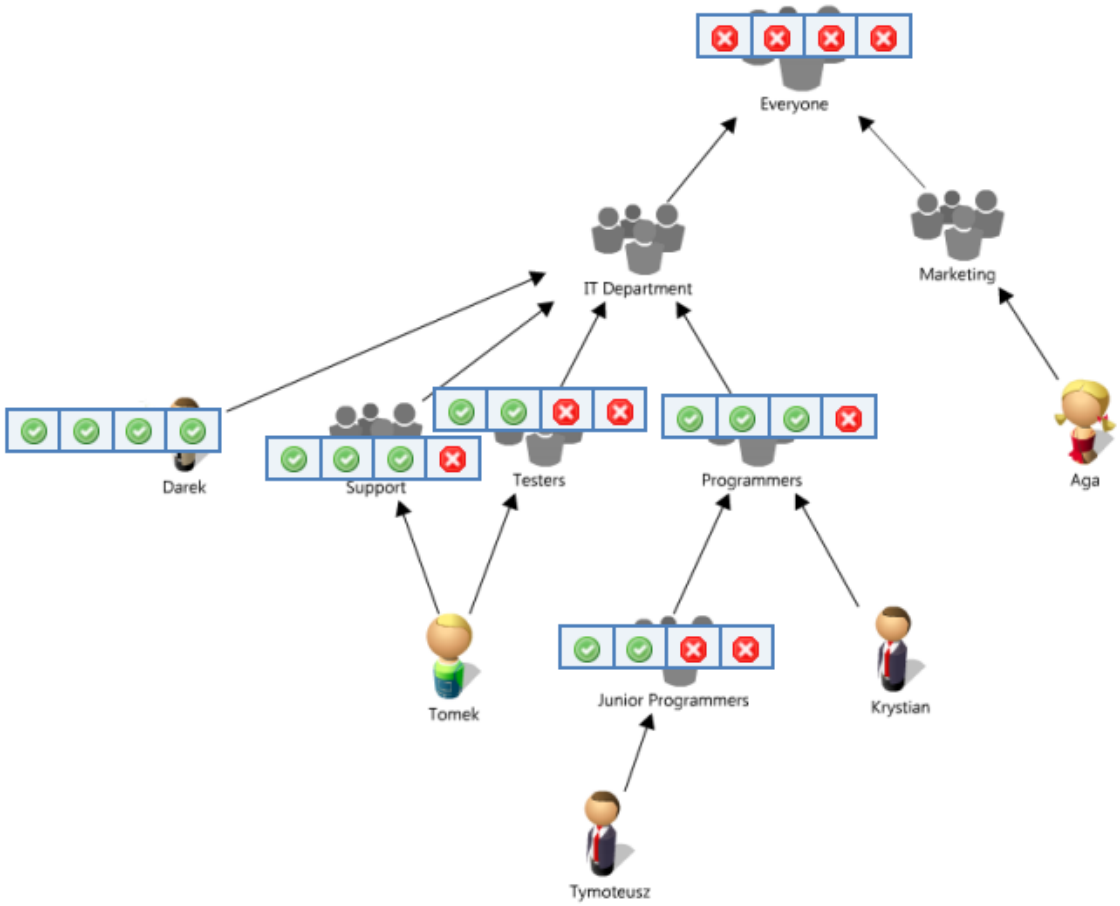
8.2.2 Przykładowa struktura

Poniżej przedstawiona jest przykładowa struktura, na bazie której zostaną omówione zasady definiowania praw w module DataGuard.



Prawa mogą być definiowane na poziomie węzłów wewnętrznych oraz liści. Prawa efektywne dla liści są wyliczane w następujący sposób: przeszukiwane są kolejne węzły od liścia w kierunku korzenia (w prezentowanym przykładzie *Everyone*), aż do znalezienia pierwszego węzła, który ma przypisane prawa. Te prawa są obowiązujące dla liścia.

Warto zwrócić uwagę na fakt, że dany komputer może należeć do kilku różnych map. W prezentowanym przykładzie taka sytuacja ma miejsce dla użytkownika Tomek, którego stacja robocza należy do dwóch map: *Support* i *Testers*. W tym przypadku wyliczane jest prawo efektywne na każdej ze ścieżek do korzenia i jako obowiązująca brana jest suma logiczna wyliczonych praw. Innymi słowy, jeżeli prawo efektywne dla którejkolwiek ze ścieżek będzie zezwalało na akcję w danej kategorii, to dla rozważanego liści ta akcja również będzie dozwolona.



Prawa efektywne dla liści:

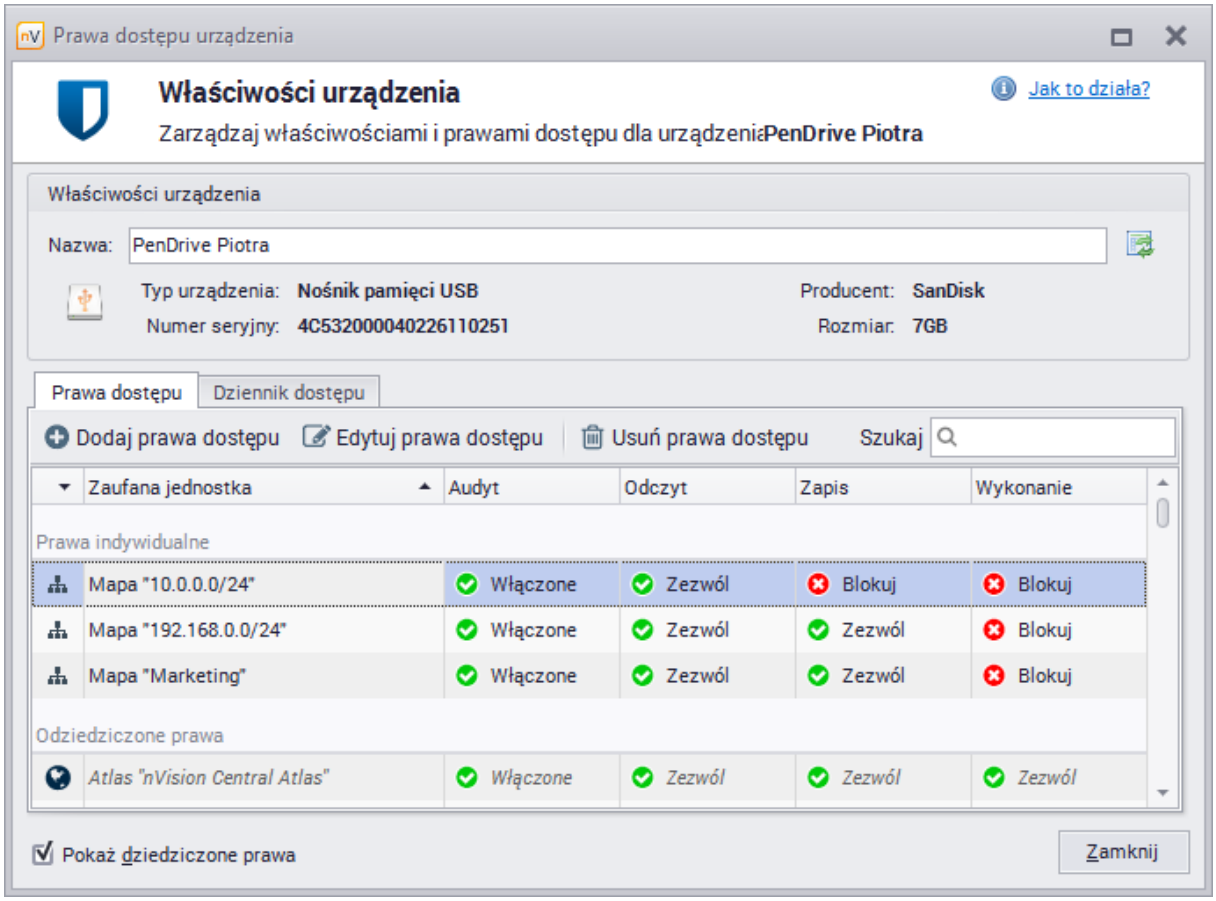
Stacja robocza	Prawa efektywne	Opis
Aga		Brak jakichkolwiek praw. Prawo efektywne wyliczane jest na podstawie przynależności do grupy *Everyone*.
Krystian		Brak prawa do wykonywania plików. Prawa wynikają z przynależności do grupy *Programmers*.
Tymoteusz		Brak praw zapisu oraz uruchamiania. Prawa wynikają z przynależności do grupy *Junior Programmers*.
Tomek		Brak prawa do wykonywania plików. Tomek należy do dwóch grup ze zdefiniowanymi prawami: *Support* i *Testers*. W tym wypadku brana jest pod uwagę suma ich praw.
Darek		Pełne prawa przypisane indywidualnie.

8.2.3 Prawa odziedziczone

Prawa dla danego użytkownika lub grupy mogą być nadane wprost lub odziedziczone z wyższych poziomów. Wyświetlane są w powyższej kolejności, czyli najpierw prawa nadane indywidualnie, a następnie odziedziczone. Oprócz tego, prawa odziedziczone zaznaczone są szarym kolorem i kursywą.

Dzięki temu na pierwszy rzut oka możliwe jest rozróżnienie, które prawa są charakterystyczne dla danej stacji roboczej, a które wynikają z praw nadanych na wyższych poziomach.

W przypadku wielu grup i użytkowników warto skorzystać z możliwości wyłączenia pokazywania odziedziczonych praw przy pomocy pola wyboru **Pokaż dziedziczone prawa** znajdującego się w lewym dolnym rogu okna właściwości urządzenia.



8.3 Urządzenia

8.3.1 Urządzenia i nośniki

Urządzenia i nośniki są podzielone na kilka kategorii. Każda z kategorii oznaczona jest unikalną ikoną.

Urządzenia działające w oparciu o system plikowy

Ikona	Urządzenia systemu plików
	dyski twarde
	urządzenia optyczne
	nośniki danych USB
	wolumeny wirtualne

Ikona	Urządzenia systemu plików
	nośniki danych, karty SD
	nośniki miękkie

Pozostałe urządzenia

Ikona	Typ urządzenia	Przykłady urządzeń
	urządzenia sieciowe lub komunikacyjne	odbiorniki radiowe Bluetooth, urządzenia podczerwieni, karty sieciowe, modemy
	urządzenia przenośne	urządzenia komunikacji bezprzewodowej
	porty	Firewire, wieloportowe karty szeregowe, urządzenia transferu kablowego, karty PCMCIA i wielofunkcyjne, porty COM i LPT
	drukarki	drukarki
	urządzenia PnP	urządzenia do obrazowania, smart cards, pozostałe urządzenia

Nadawanie praw

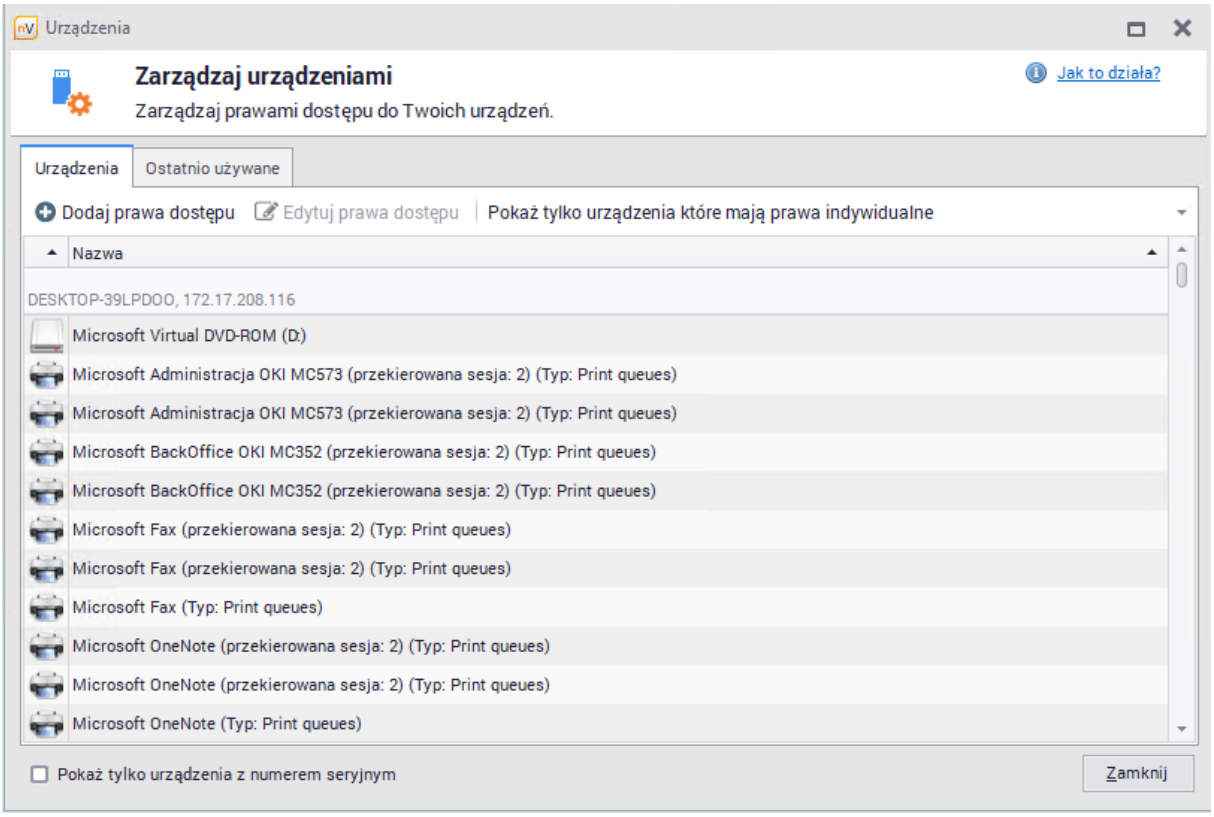
Urządzenia systemu plików mogą mieć nadawane prawa dostępu w każdej z czterech kategorii opisanych w rozdziale Prawa dostępu. Z kolei pozostałe rodzaje urządzeń mają nadawane tylko prawo dotyczące możliwości użytkowania (korzystanie z danego urządzenia może być blokowane lub dozwolone). nVision automatycznie wykrywa podłączone urządzenia oraz nośniki i przyporządkowuje każdemu z nich jedną z powyższych kategorii odpowiednio do rodzaju urządzenia.

8.3.2 Zarządzanie urządzeniami

Aby zarządzać prawami dostępu dla urządzeń, kliknij przycisk **Zarządzaj urządzeniami** znajdujący się na głównym pasku narzędziowym.

Na poniższym obrazku prezentowany jest przykładowy wygląd okna **Urządzenia**. W górnej części listy znajdują się konkretne urządzenia wykryte przez nVision, natomiast jako ostatnia grupa wymienione są **Pozostałe urządzenia**. Znajdują się tu, podzielone na kategorie, wszystkie pozostałe urządzenia, czyli takie, które jeszcze nie zostały zdefiniowane.

Po kliknięciu przycisku **Pokaż tylko urządzenia, które mają prawa indywidualne** wyświetlona zostanie lista urządzeń z indywidualnie przydzielonymi prawami DataGuard. Dwukrotne kliknięcie nazwy urządzenia otworzy okno jego właściwości, w którym wskazane będą konkretne jednostki, dla których ustalone zostały prawa indywidualne.

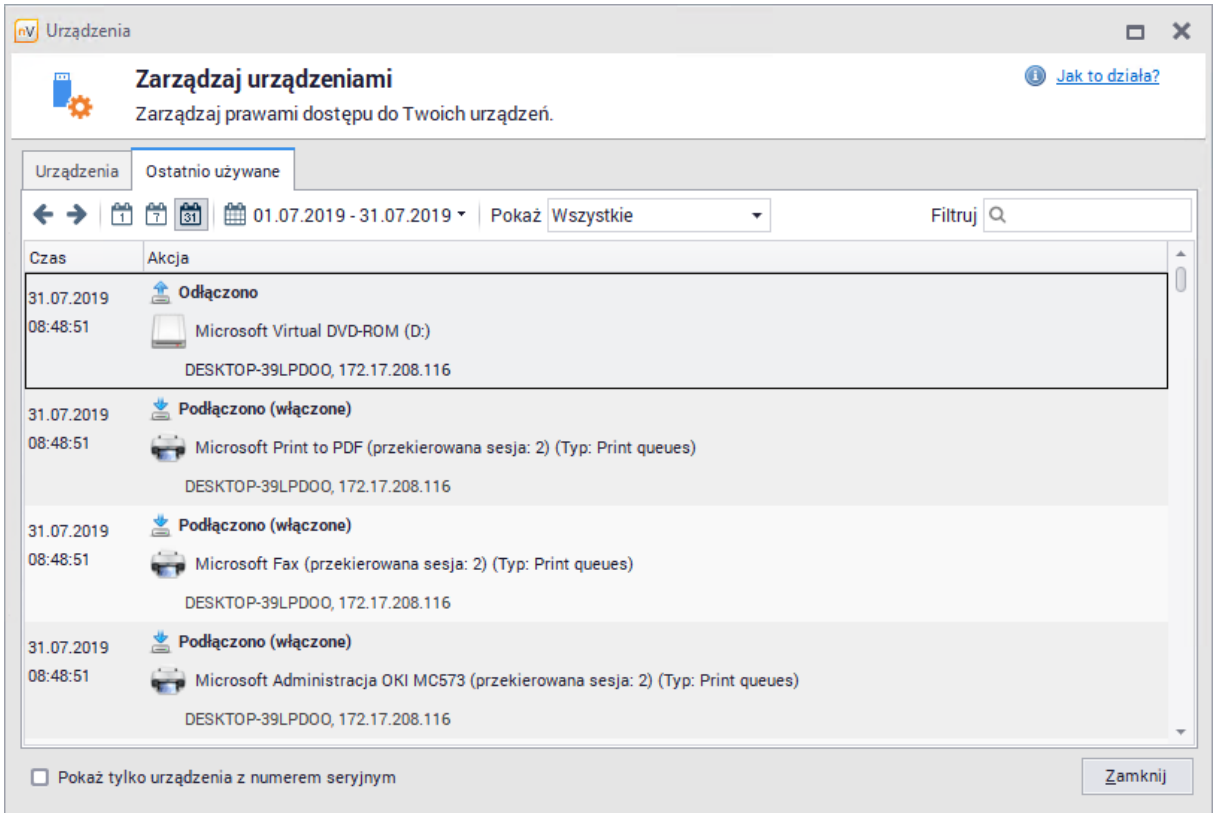


Podpięcie i odłączenie urządzenia monitorowane jest zawsze. Wykryte urządzenia pojawiają się na liście z zachowaniem podziału na kategorie.

Aby dowiedzieć się więcej na temat blokowania pendrive'ów, przejdź do rozdziału Jak ustawić prawa dostępu do nośnika USB?.

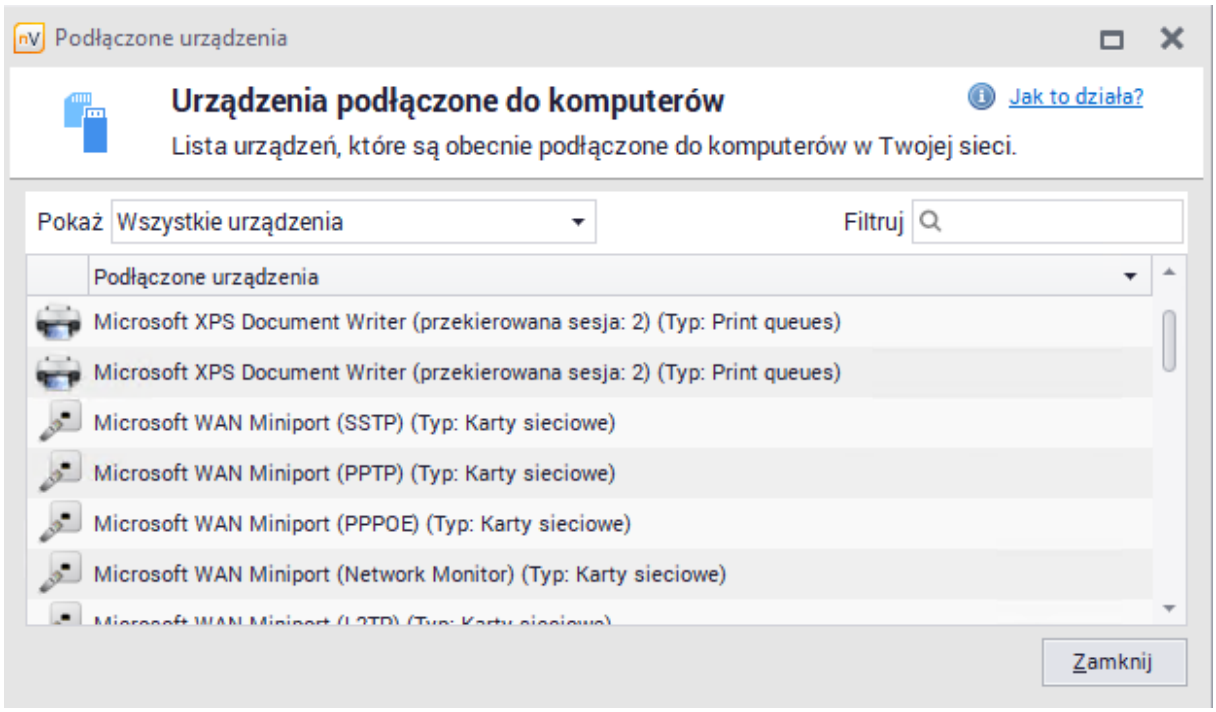
Ostatnio używane urządzenia

W zakładce **Ostatnio używane** w oknie **Urządzeń** wyświetlana jest lista ostatnio używanych urządzeń. Monitorowane są wszelkie zmiany związane z podłączaniem i odłączaniem urządzenia. Aby przeglądać historię używanych urządzeń, wybierz okres (dzień, tydzień lub miesiąc) i w razie potrzeby użyj strzałek, by przeglądać kolejne lub poprzednie okresy. Jeśli danych jest dużo, warto skorzystać z możliwości wyszukania potrzebnych informacji.



8.3.3 Podłączone urządzenia

Aby przeglądać aktualnie podłączone urządzenia, kliknij opcję **Podłączone urządzenia** na głównym pasku narzędziowym.



Przeglądanie urządzeń podłączonych do konkretnego komputera jest też możliwe z poziomu okna

Informacji o tym komputerze, w zakładce **Zasoby / Sprzęt / Podłączone urządzenia**.

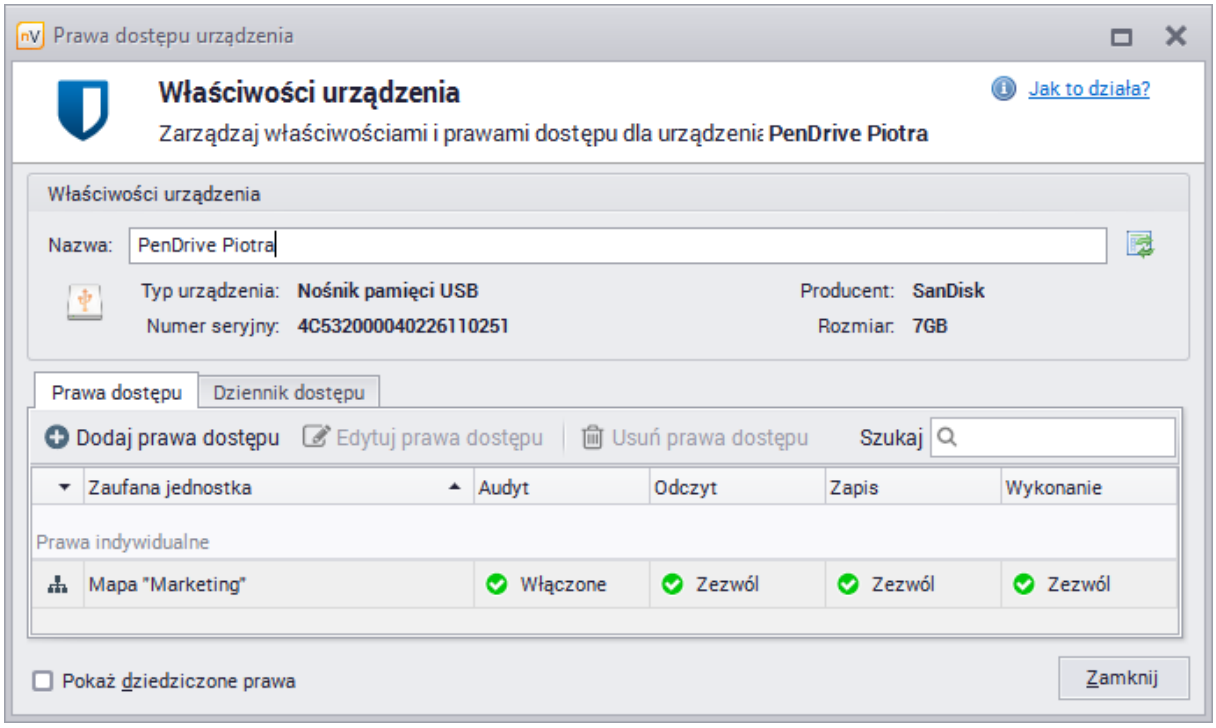
Najbardziej ogólny widok z możliwością przełączania między użytkownikami, grupami i różnymi funkcjonalnościami modułu DataGuard oferuje okno **Zarządzania zaufanymi jednostkami**. Aby dowiedzieć się więcej, przejdź do rozdziału Zarządzanie zaufanymi jednostkami.

8.3.4 Opisywanie urządzeń

Urządzenia podłączone do monitorowanych komputerów mają początkowo domyślne nazwy nadane przez nVision. Możliwa jest dowolna zmiana takiej nazwy, a także powrót do nazwy domyślnej.

Aby zmienić nazwę urządzenia:

1. Przejdź do okna **Właściwości urządzenia** klikając dwa razy na wybranej z listy urządzeń pozycji.
2. Wpisz własną nazwę urządzenia w polu **Nazwa**.



Aby przywrócić domyślną nazwę urządzenia, kliknij w przycisk znajdujący się po prawej stronie pola **Nazwa**.

8.4 Zaufane jednostki

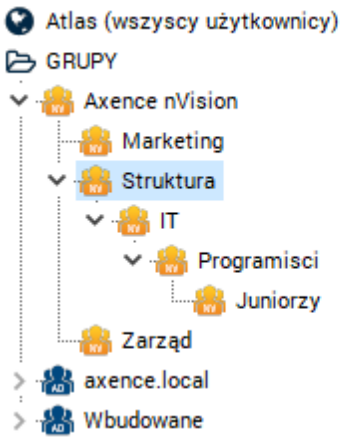
8.4.1 Zaufane jednostki - wprowadzenie

Zaufane jednostki to stacje robocze i grupy komputerów, dla których definiowane są prawa dostępu. W zależności od poziomu zaufania, jednostkom mogą być nadawane różne prawa. Aby dowiedzieć się więcej na temat praw dostępu, przejdź do rozdziału Prawa dostępu.

Grupy użytkowników

Definiowanie praw dostępu dla każdego użytkownika osobno byłoby zajęciem bardzo czasochłonnym. Dlatego też zaleca się umieszczanie poszczególnych użytkowników w grupach utworzonych przez administratora systemu. W przypadku, gdy struktura utworzonych grup odpowiada rzeczywistym

zależnościom między użytkownikami, możliwe jest szybkie ustalenie praw dostępu. Przykładowa struktura grup przedstawiona jest na poniższym rysunku.



Aby dowiedzieć się więcej na temat wyliczania efektywnych praw dostępu dla powyższej struktury map, przejdź do rozdziału Przykładowa struktura.

Zarządzanie prawami dostępu może być realizowane na dwa sposoby:

- Zarządzanie z poziomu właściwości użytkownika, grupy lub atlasu - Zarządzanie poprzez hierarchię użytkowników
- Zarządzanie dzięki funkcji Zarządzanie zaufanymi jednostkami

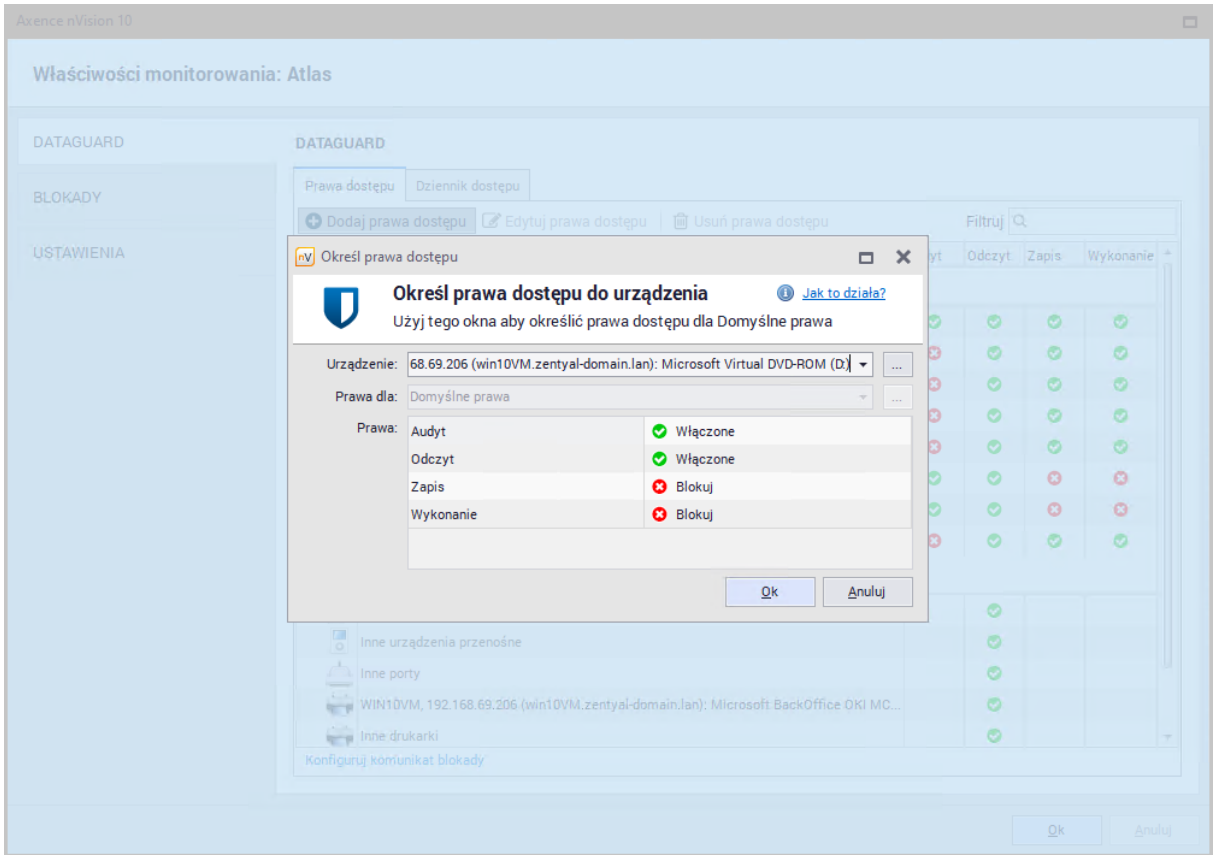
8.4.2 Zarządzanie poprzez hierarchię użytkowników

Aby zarządzać prawami dostępu dla użytkownika, grupy lub atlasu (nazywane dalej jednostkami) należy wykonać następujące kroki:

1. Wybierz jednostkę i klikając prawym przyciskiem myszy przejdź do okna **Informacji o danej jednostce**
2. Przejdź do zakładki DataGuard.
3. Jeśli chcesz zmienić wcześniej zdefiniowaną regułę, dwukrotnie kliknij w wybrany wiersz i przejdź do punktu 5. Aby zdefiniować nową regułę, kliknij w przycisk **Dodaj prawa dostępu**.
4. Wybierz z listy urządzenie, dla którego chcesz nadać prawa.
5. Ustaw prawa dostępu i wciśnij **Enter**.

Aby edytować prawa wybranego urządzenia należy skorzystać z przycisku **Edytuj prawa dostępu**. Natomiast jeżeli chcesz pozbyć się nadanych wcześniej uprawnień użyj przycisku **Usuń prawa dostępu.**

Poniższy zrzut ekranu obrazuje ustalenie indywidualnych praw dla wirtualnej stacji dysków w oknie Informacji o atlasie (prawo domyślne, najważniejsze w hierarchii).

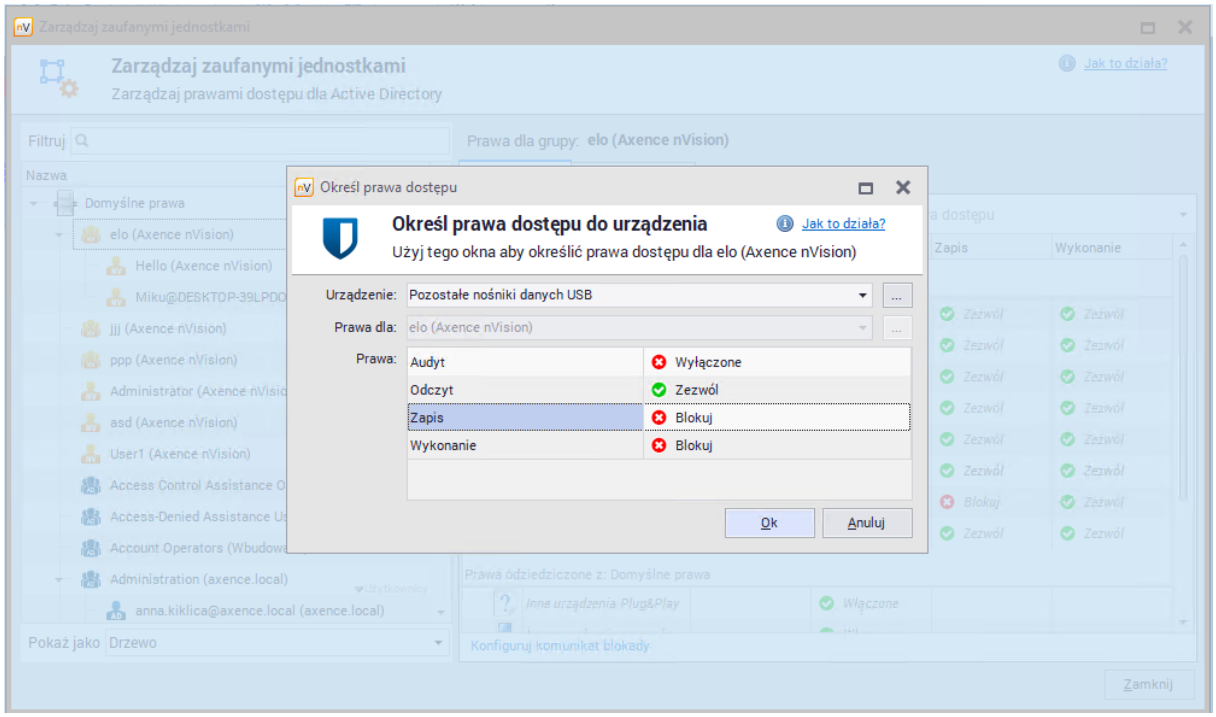


8.4.3 Zarządzanie zaufanymi jednostkami

Aby zarządzać prawami dostępu dla wszystkich jednostek:

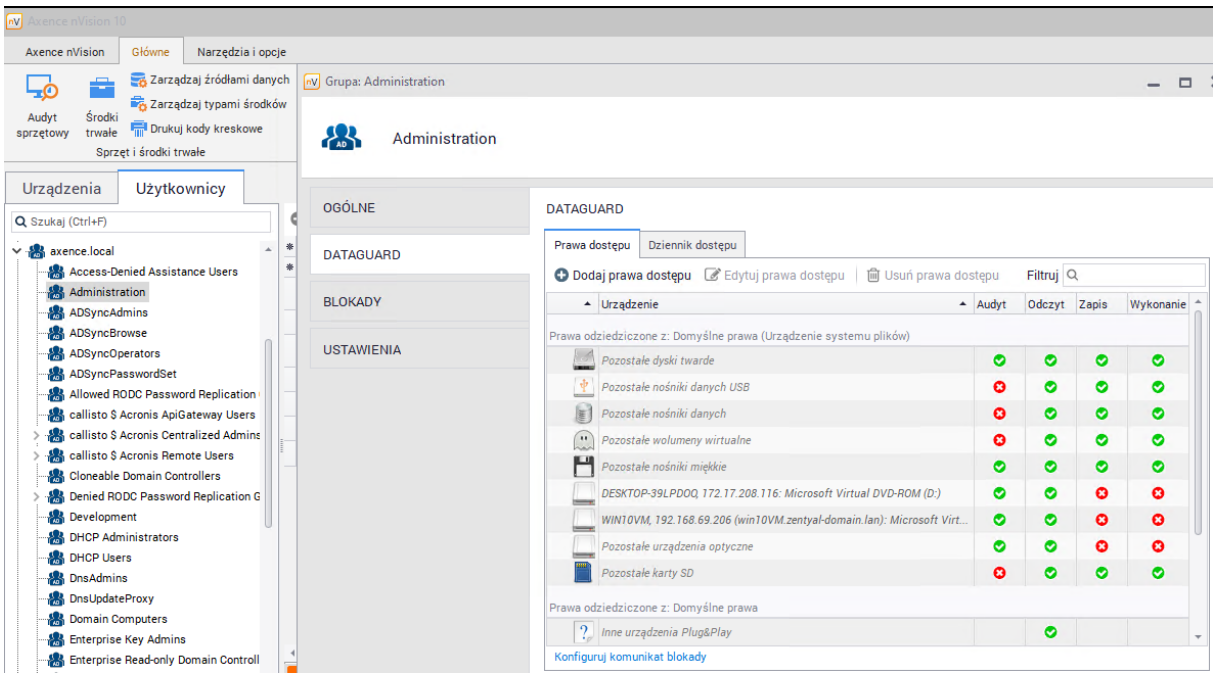
1. Z głównego paska narzędziowego programu w sekcji DataGuard wybierz opcję **Zarządzaj zaufanymi jednostkami**.
2. Wybierz jednostkę organizacyjną z listy znajdującej się po lewej stronie. W razie potrzeby użyj opcji wyszukiwania, by znaleźć właściwy wiersz szybciej.
3. Jeśli chcesz zmienić wcześniej zdefiniowaną regułę, dwukrotnie kliknij w wiersz z wybraną regułą lub wybierz wiersz i kliknij **Edytuj prawa dostępu**. Aby zdefiniować nową regułę, kliknij w przycisk **Dodaj prawa dostępu**.
4. Wybierz z listy urządzenie, dla którego chcesz nadać prawa.
5. Ustaw prawa dostępu i wciśnij **Enter**.

Prawa przydzielone indywidualnie można też edytować bezpośrednio w oknie zarządzania. Aby to zrobić, kliknij na wybranym z praw, a zostanie ono zmienione. Kliknięcie na odziedziczonych prawach dostępu spowoduje otwarcie okna **Określania praw dostępu**.



8.4.4 Użytkownicy Active Directory

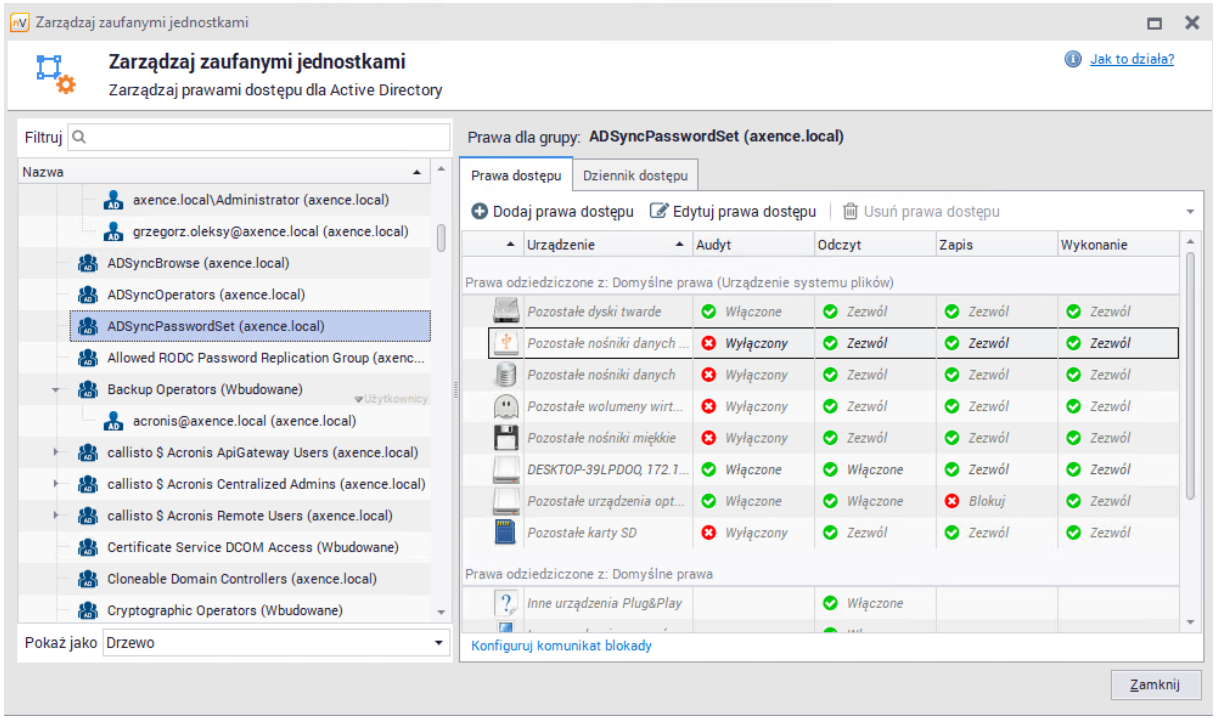
Moduł DataGuard jest zintegrowany z Active Directory. Prawa dostępu mogą być nadawane bezpośrednio użytkownikom AD.



Aby przeglądać i definiować prawa dostępu dla użytkowników AD:

1. Wybierz opcję **Zarządzaj zaufanymi jednostkami** znajdującą się w sekcji DataGuard na głównym pasku narzędziowym.

2. Wybierz grupę lub użytkownika w lewej części okna. Jeśli jest taka potrzeba, użyj opcji wyszukiwania.
3. Aby zmienić wcześniej zdefiniowaną regułę, kliknij dwukrotnie na wiersz z daną regułą w prawej części okna lub kliknij przycisk **Edytuj prawa dostępu**. Aby zdefiniować nową regułę, kliknij w przycisk **Dodaj prawa dostępu**.
4. Wybierz urządzenie, dla którego mają być przypisane prawa.
5. Ustaw prawa dostępu i wciśnij Enter.

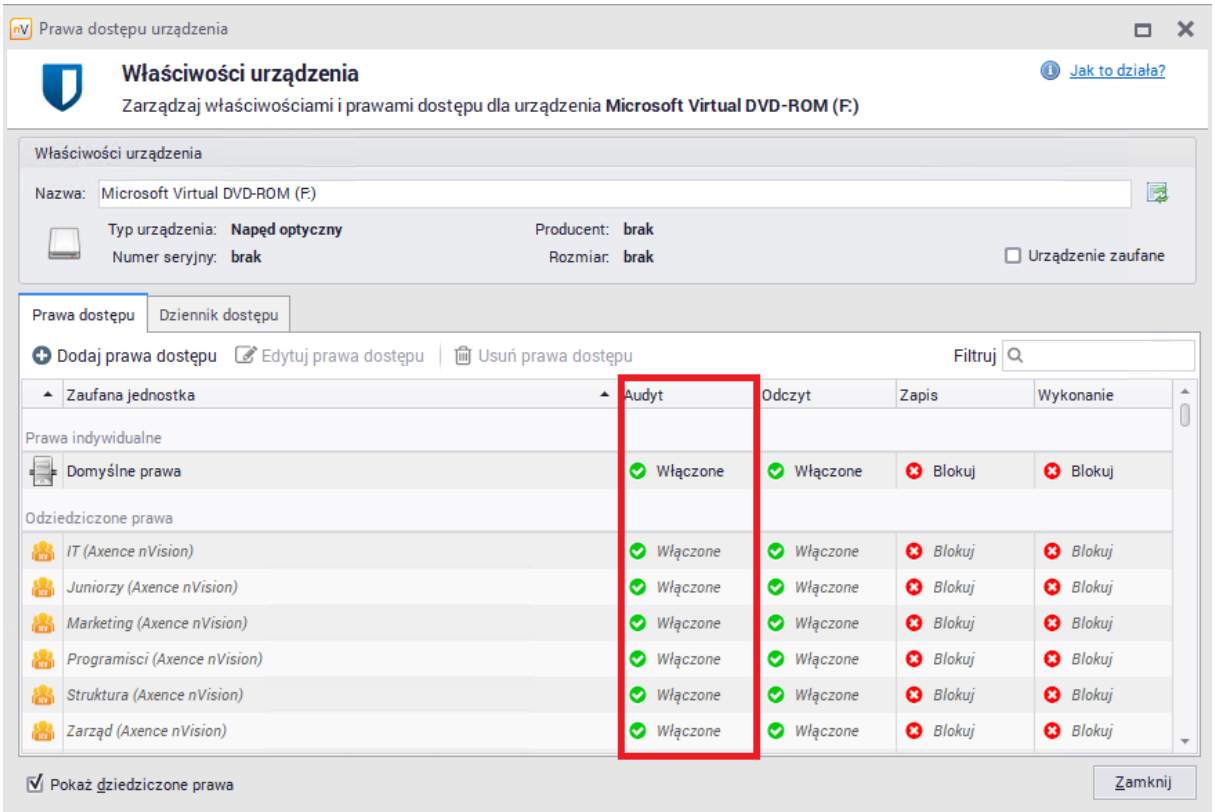


Uwagi

- Prawa dostępu zaufanych jednostek Active Directory mają priorytet względem praw stacji roboczych.
- Prawa dostępu zaufanych jednostek Active Directory mogą być zdefiniowane dla urządzeń z systemem plików i dla urządzeń posiadających numer seryjny.
- Jeśli zostanie wykryta cykliczna zależność pomiędzy jednostkami AD, nVision przerwie każdą zależność w cyklu. Powiadomienie o wystąpieniu tego typu sytuacji zostanie wyświetlone w oknie **Zarządzania zaufanymi jednostkami**.

8.4.5 Dziennik dostępu

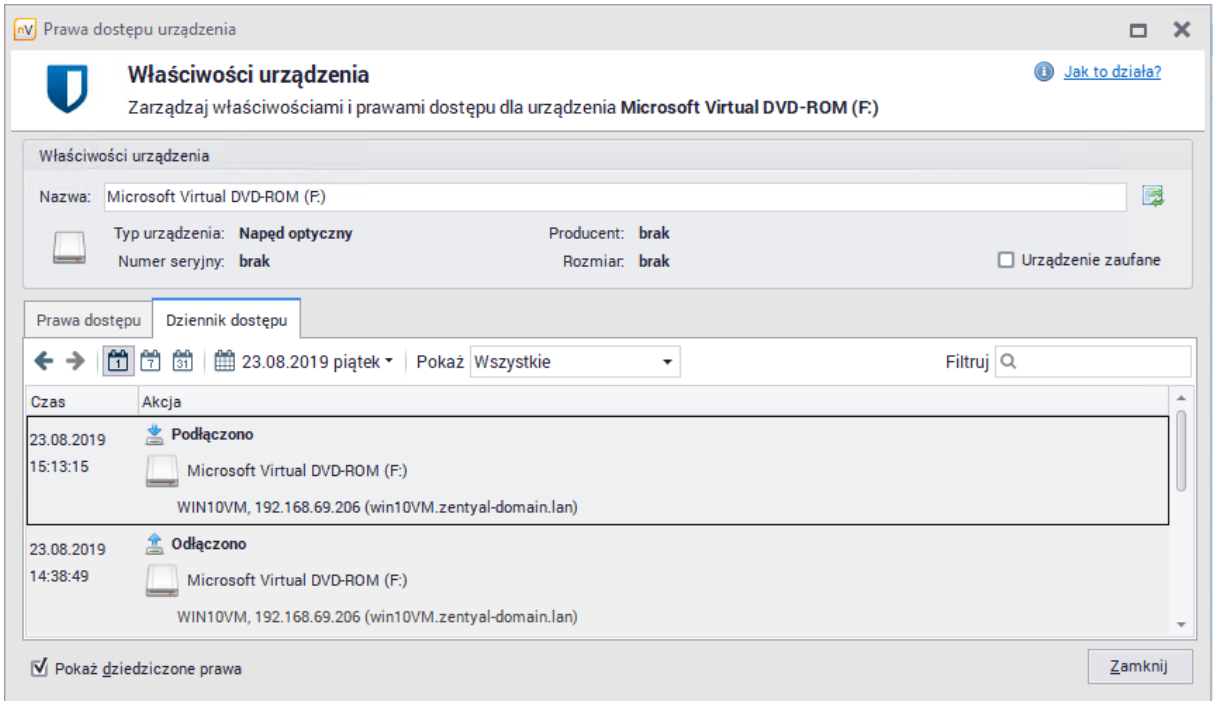
W dzienniku dostępu znajdują się informacje dotyczące dostępu do danych i podłączanych urządzeń. Aby dostęp był monitorowany, należy włączyć audyt dla urządzenia i jednostki (stacji roboczej, mapy, atlasu), które mają być monitorowane. Prawa mogą być zdefiniowane indywidualnie lub odziedziczone (jak na poniższym obrazku).



Podpięcie i odłączenie urządzenia monitorowane jest zawsze. **Przy włączonym audycie monitorowane są także: tworzenie pliku, zmiana nazwy, zapis i usunięcie.**

Aby przeglądać dziennik dostępu:

1. Wybierz opcję **Zarządzaj zaufanymi jednostkami** znajdującą się w sekcji DataGuard na głównym pasku narzędziowym.
2. Przejdź do zakładki **Dziennik dostępu**.
3. Wybierz jednostkę z listy znajdującej się po lewej stronie. W razie potrzeby użyj opcji wyszukiwania, by znaleźć właściwy wiersz szybciej.
4. Wybierz okres, z którego informacje chcesz przeglądać.



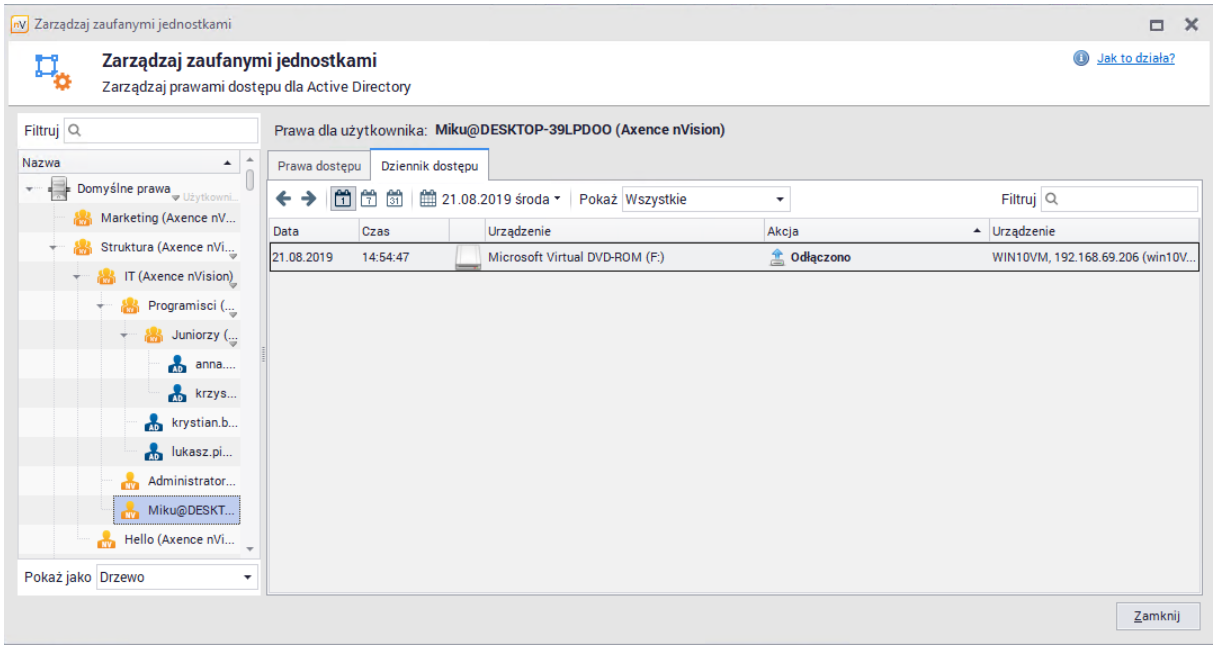
8.4.6 Dziennik dostępu dla użytkowników

Aby przeglądać dziennik dostępu dla użytkowników z poziomu okna **Zarządzania zaufanymi jednostkami**:

1. Wybierz opcję **Zarządzaj zaufanymi jednostkami** znajdującą się w sekcji DataGuard na głównym pasku narzędziowym.
2. Wybierz grupę lub użytkownika w lewej części okna. Jeśli jest taka potrzeba, użyj opcji wyszukiwania.
3. Przejdź do zakładki **dziennik dostępu.**

Widoczne tutaj będą wszystkie dane dotyczące podłączeń oraz odłączeń urządzeń oraz dane dotyczące operacji na plikach (audyt na tych urządzeniach musi być włączony).

Możliwe jest ograniczenie widoku do dnia, tygodnia lub miesiąca. Użyj strzałek nawigacyjnych, aby odczytać dane o interesującym cię okresie.

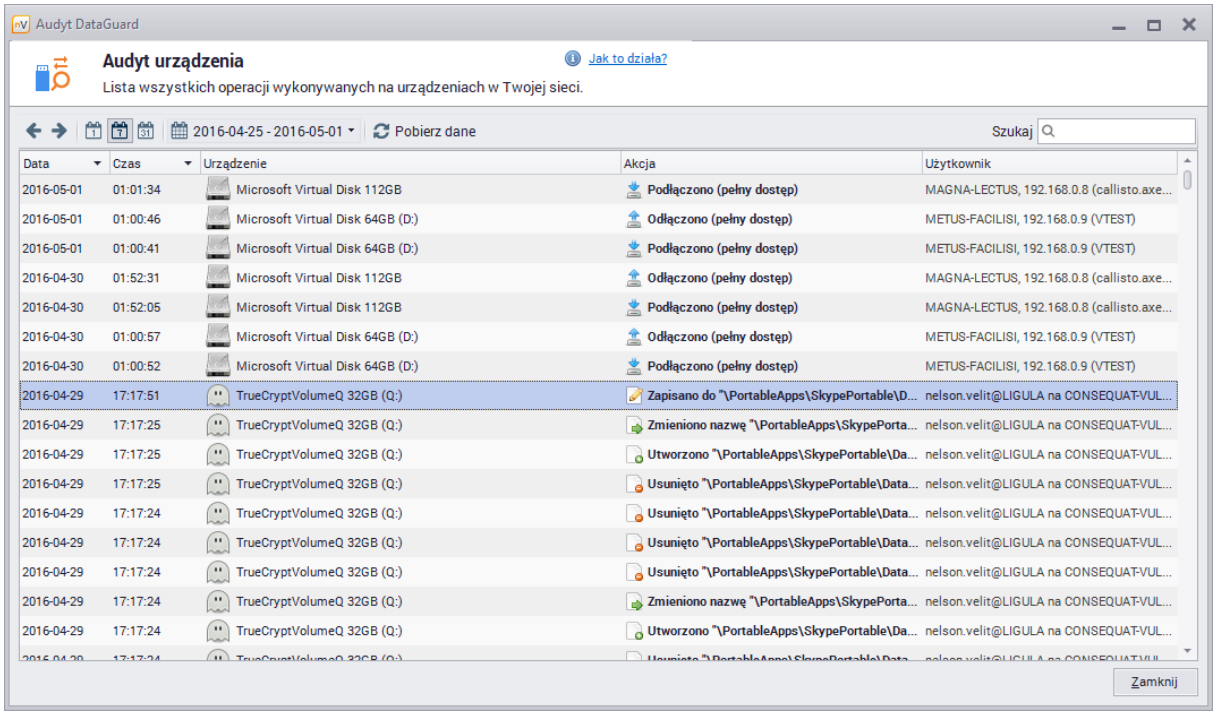


Aby poznać inne sposoby przeglądania podłączonych urządzeń, przejdź do rozdziału Aktualnie podłączone urządzenia.

8.5 Audyt

Aby dokonać audytu urządzeń:

1. Wybierz opcję **Audyt** znajdującą się w sekcji DataGuard na głównym pasku narzędziowym.
2. Wybierz okres, z którego informacje chcesz przeglądać.



Przeglądanie historii dostępu do urządzeń może się odbywać także z poziomu okna **Zarządzania zaufanymi jednostkami**. Aby dowiedzieć się więcej, przejdź do rozdziału Dziennik dostępu.

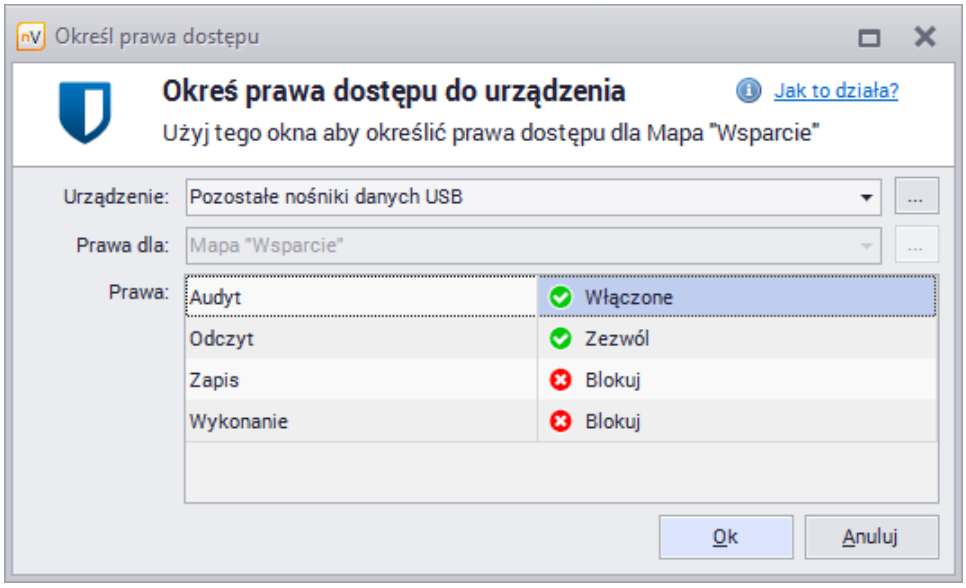
8.6 Szybka pomoc - typowy scenariusz ustalania praw

W tym rozdziale przedstawiony jest scenariusz ustalania praw dla typowej sytuacji: blokowane są operacje na niezdefiniowanych urządzeniach USB (w szczególności zapisywanie oraz uruchamianie plików), natomiast nadaje się większe prawa dla konkretnego urządzenia, którym w tym wypadku jest firmowy pendrive. Firmowy pendrive używany jest przez pewną grupę użytkowników (w poniżej prezentowanym przykładzie - dział reprezentowany przez mapę *Marketing*) i umożliwia przenoszenie danych firmowych między stacjami roboczymi.

Blokowanie praw zapisu i uruchamiania dla niezdefiniowanych urządzeń USB

Aby ustawić prawa dla urządzeń USB:

1. Klikając prawym przyciskiem myszy na Atlasie (zakładka Użytkownicy) przejdź do **Informacji o atlasie**.
2. Przejdź do zakładki **DataGuard** i wybierz grupę urządzeń **Pozostałe nośniki danych USB** oznaczone ikoną  . Wciśnij **Enter** lub kliknij dwukrotnie na wybranym wierszu.
3. Ustaw prawa dostępu jak na poniższym rysunku i wciśnij **Enter**.



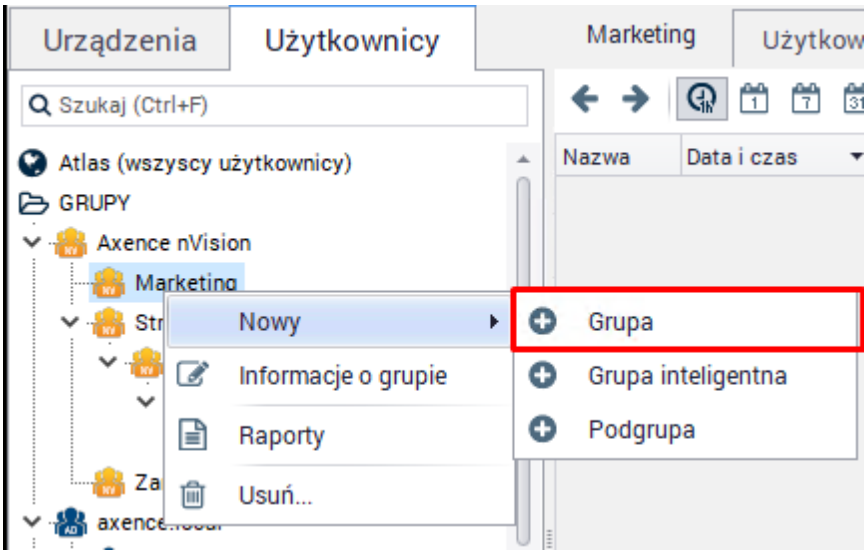
Przy tak ustawionych prawach możliwe jest czytanie plików znajdujących się na nośnikach zewnętrznych, natomiast blokuje się możliwość zapisywania danych oraz uruchamiania plików wykonywalnych. Włączenie audytu skutkuje monitorowaniem działań użytkowników związanych z nośnikami zewnętrznymi, czyli daje informacje o czytanych plikach, a także o próbach zapisu i uruchomienia. Podłączenie i odłączenie urządzenia monitorowane jest zawsze, niezależnie od ustawienia opcji audytu.

Tworzenie grupy użytkowników korzystających z firmowego pendrive'a

Jeśli pendrive firmowy dostępny jest dla pewnego działu lub grupy użytkowników, zaleca się utworzenie grupy umożliwiającej łatwe zarządzanie prawami dostępu dla tych użytkowników.

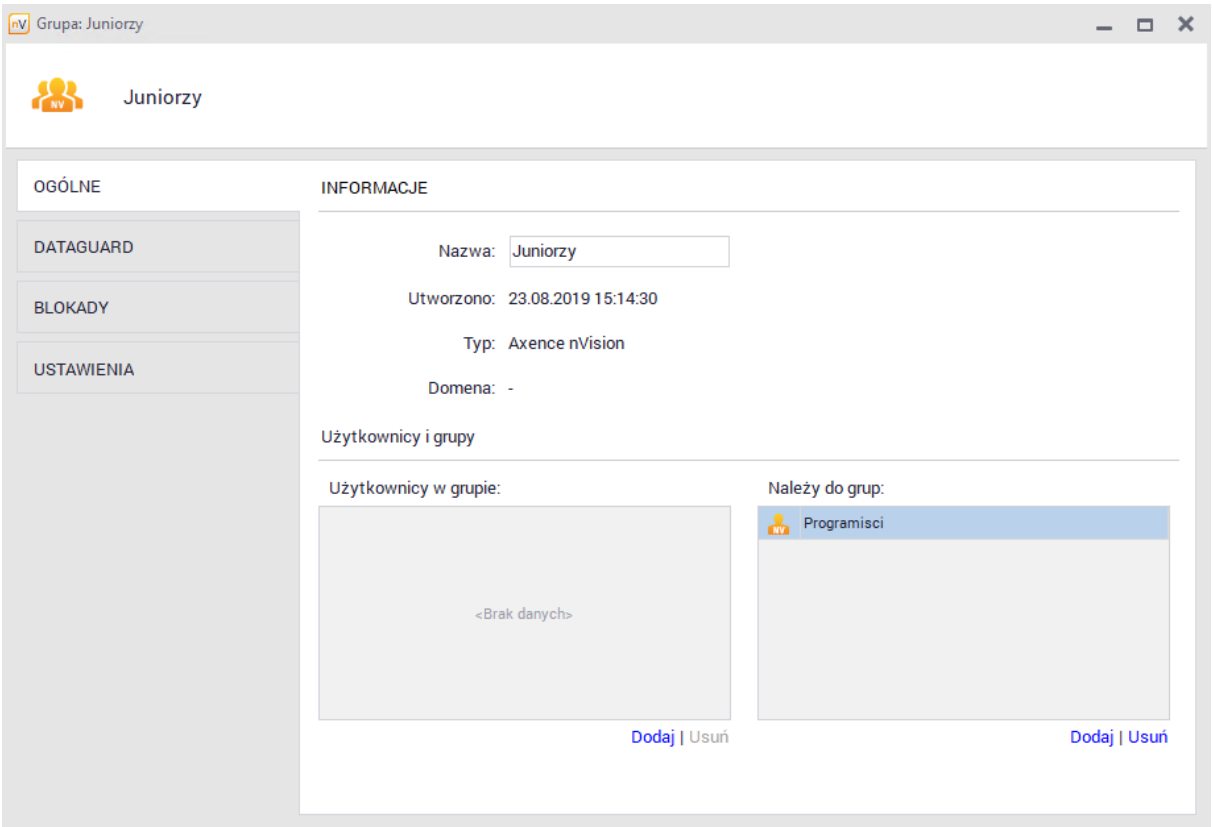
Aby utworzyć grupę:

1. Kliknij na wybranej grupie lub folderze prawym przyciskiem myszy, a następnie wybierz opcje **Nowy | Grupa**.



2. Nadaj utworzonej mapie nazwę klikając na napisie lub poprzez jej **Właściwości**.

Aby dodać grupę do innej grupy (nadrzędnej) należy przejść do jej właściwości:



Następnym krokiem jest przeniesienie odpowiednich użytkowników do utworzonej grupy. Wystarczy zaznaczyć użytkowników i przeciągnąć ich do odpowiedniej grupy.

Ustawianie praw dla firmowego pendrive'a

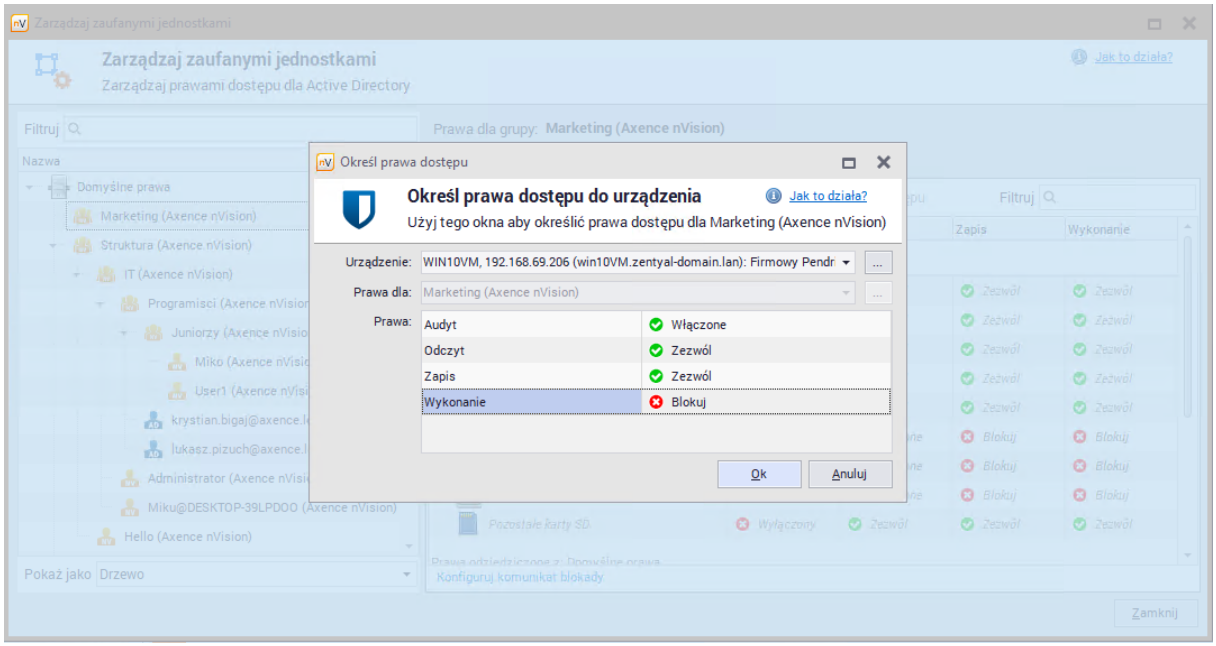
Firmowy pendrive umożliwia przenoszenie danych w obrębie pewnej grupy użytkowników. Stąd dla tego konkretnego urządzenia dozwolone jest czytanie oraz zapisywanie plików. Wciąż zablokowane jest

uruchamianie programów, aby zapobiec przenoszeniu wirusów. Włączony audyt umożliwia monitorowanie wszelkich operacji wykonywanych na danym nośniku USB.

Aby ustawić prawa dostępu dla urządzenia USB:

1. Z głównego paska narzędziowego programu w sekcji DataGuard wybierz opcję **Zarządzaj zaufanymi jednostkami**.
2. Kliknij **Dodaj prawa dostępu** a następnie wybierz odpowiednie urządzenie z listy.
3. Ustaw prawa dostępu jak na poniższym rysunku i wciśnij **Enter**.

Teraz użytkownicy należący do grupy Marketing mogą odczytywać i zapisywać dane z urządzenia "Firmowy Pendrive".

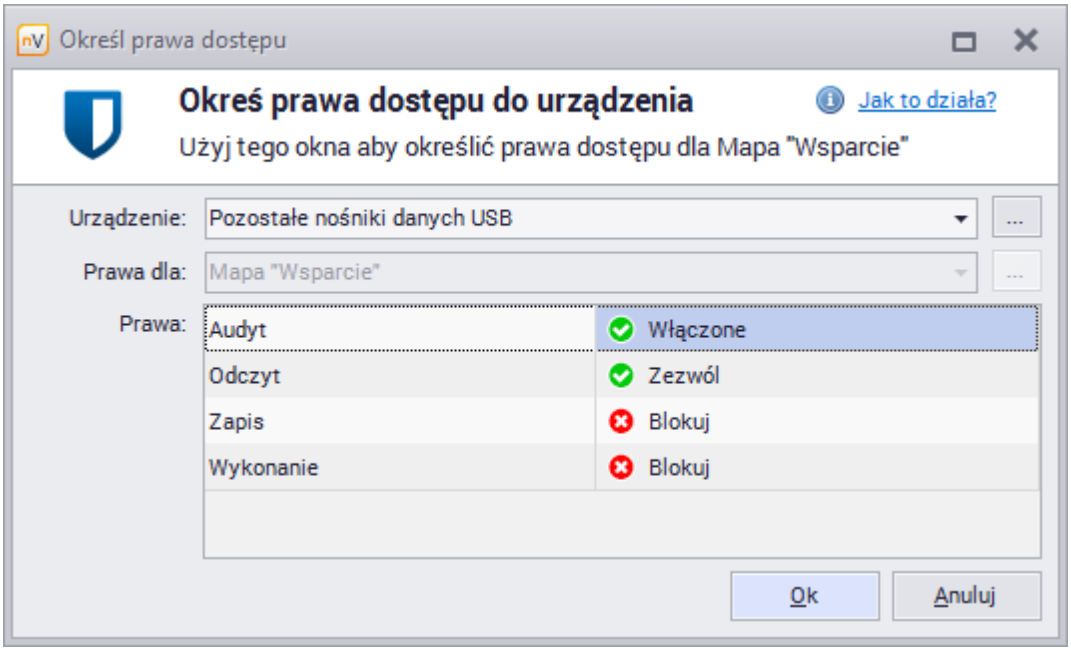


8.7 Szybka pomoc - ustawianie domyślnych praw dostępu do urządzeń USB

Częstą przyczyną zainfekowania komputerów wirusami jest przenoszenie ich za pomocą pendrive'ów. Automatyczne uruchamianie takich urządzeń stwarza możliwość rozprzestrzeniania się szkodliwego oprogramowania. Drugim czynnikiem stwarzającym potencjalne zagrożenie jest możliwość skopiowania poufnych danych i wyniesienia ich poza firmę na nośniku USB. Moduł DataGuard zapewnia ochronę przed powyższymi niebezpieczeństwami.

Aby zablokować możliwość zapisywania i uruchamiania plików ze wszystkich urządzeń USB (poza tymi, dla których prawa zostały zdefiniowane indywidualnie) dla całego atlasu, czyli wszystkich użytkowników:

1. Klikając prawym przyciskiem myszy na Atlasie (zakładka Użytkownicy) przejdź do **Informacji o atlasie**.
2. Przejdź do zakładki **DataGuard** i wybierz grupę urządzeń **Pozostałe nośniki danych USB** oznaczone ikoną  . Wciśnij **Enter** lub kliknij dwukrotnie na wybranym wierszu.
3. Ustaw prawa dostępu jak na poniższym rysunku i wciśnij **Enter**.



Aby ustawić prawa domyślne dla poszczególnych grup oraz użytkowników albo sprawdzić ich ustawienia:

1. Z głównego paska narzędziowego programu w sekcji DataGuard wybierz opcję **Zarządzaj zaufanymi jednostkami**.
2. Wybierz z listy grupę lub użytkownika, dla którego chcesz wprowadzić zmiany.
3. Wybierz grupę urządzeń **Pozostałe nośniki danych USB** oznaczone ikoną . Wciśnij **Enter** lub kliknij dwukrotnie na wybranym wierszu

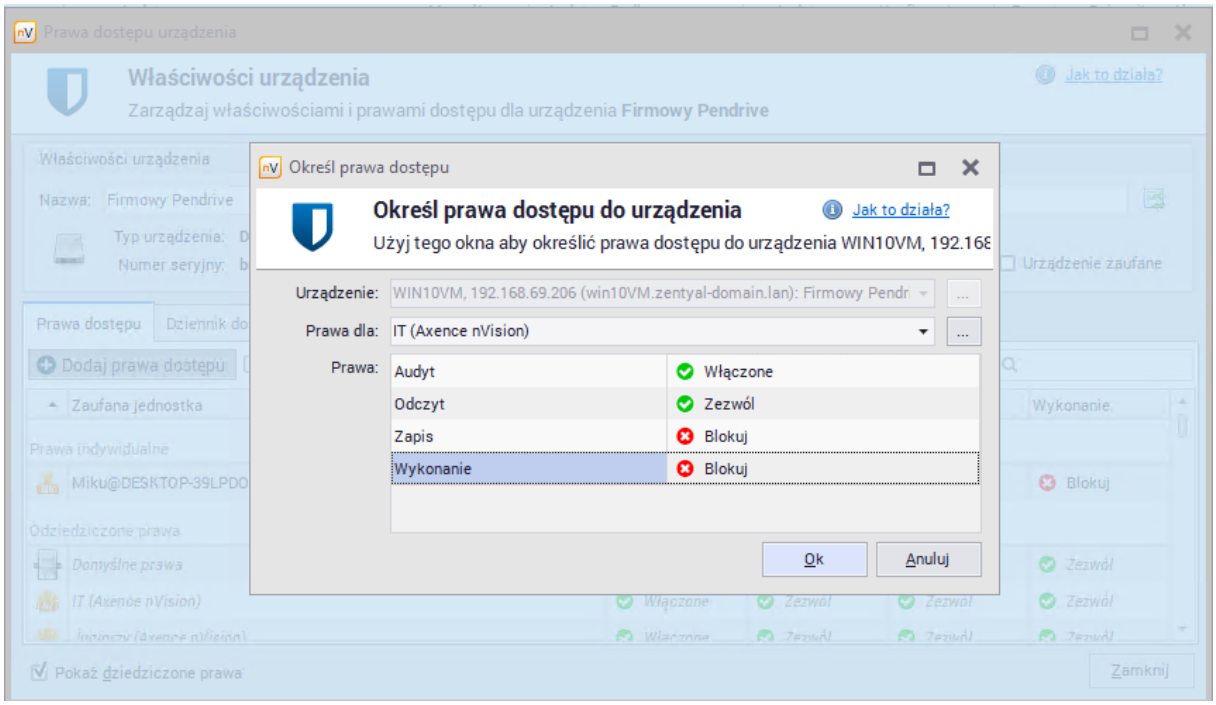
Jeśli użytkownik podłączy blokowane urządzenie, z ikony Agenta zostanie wyświetlona informacja o blokadzie.

Aby dowiedzieć się więcej na temat blokowania pendrive'ów i ustawiania praw dla konkretnych urządzeń wykrytych przez nVision, przejdź do rozdziału Jak ustawić prawa dostępu do nośnika USB?.

8.8 Ustawianie praw dostępu do nośnika USB

Aby zablokować możliwość zapisywania i uruchamiania plików z konkretnego pendrive'a, który został wykryty przez nVision:

1. Kliknij **Podłączone urządzenia** w sekcji DataGuard na głównym pasku narzędziowym.
2. Wybierz z listy wykryte urządzenie, które chcesz zablokować.
3. Kliknij w przycisk **Dodaj prawa dostępu**.
4. Wybierz z listy użytkownika, grupę lub atlas, dla którego chcesz ustawić prawa dostępu i zablokuj je jak na poniższym rysunku. Wciśnij **Enter**.



Aby uzyskać informacje na temat ustawiania domyślnych praw dostępu do urządzeń USB, przejdź do rozdziału Szybka pomoc - ustawianie domyślnych praw dostępu do urządzeń USB.

8.9 Alarmy

8.9.1 Alarmy dla DataGuard

Alarmy dla modułu DataGuard umożliwiają ostrzeganie w przypadku działań wykonywanych na urządzeniach mobilnych i ich podłączania. W szczególności, administrator może być poinformowany o próbie kradzieży poufnych informacji.

Typy zdarzeń

1. Urządzenie mobilne podłączone lub rozłączone
    - Podłączono urządzenie
    - Odłączono urządzenie
2. Operacja na pliku na urządzeniu mobilnym
    - Plik został utworzony
    - Plik został usunięty
    - Nazwa pliku została zmieniona
    - Zapis do istniejącego pliku

    Jako dodatkowy warunek można podać maskę pliku.

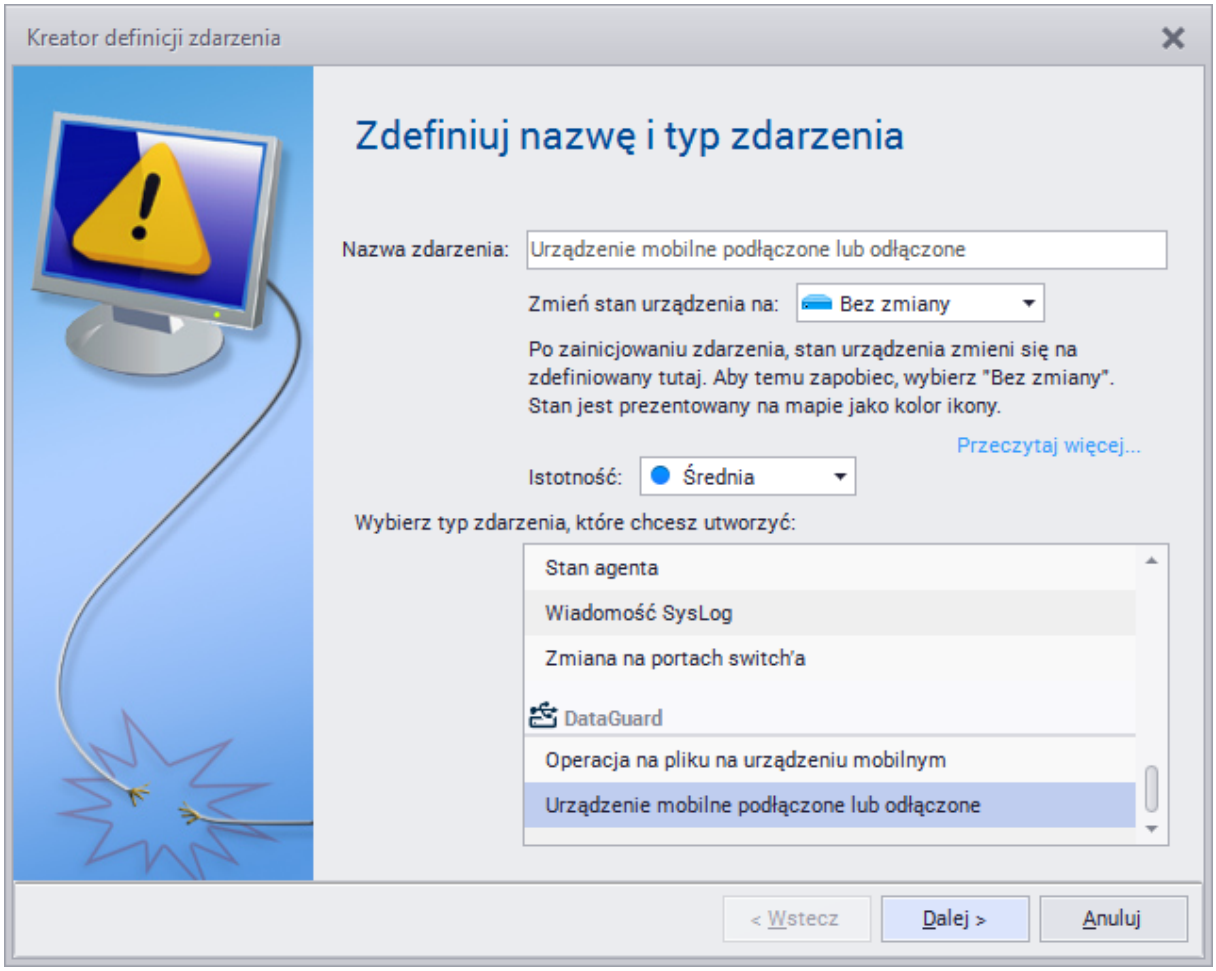
Dla obu powyższych typów zdarzeń możliwe jest generowanie alarmów dla wszystkich urządzeń lub dla określonych, wybieranych z listy.

8.9.2 Tworzenie alarmu

Aby dowiedzieć się więcej o procesie tworzenia alarmów, przejdź do rozdziału Alarmowanie.

Wykrywanie podłączenia urządzenia mobilnego

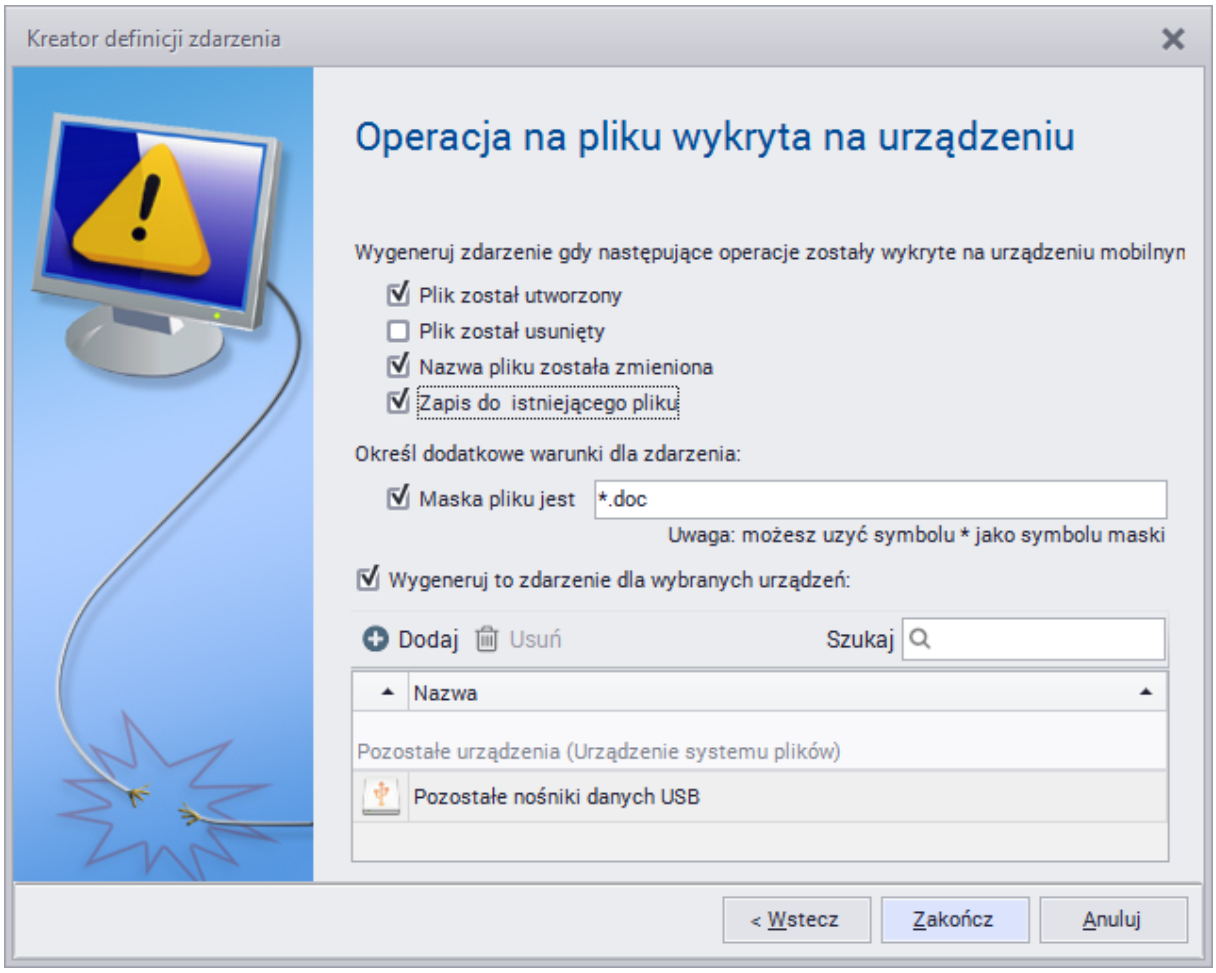
1. Otwórz okno zarządzania alarmami na głównym pasku narzędziowym.
2. Kliknij w przycisk **Dodaj alarm**, aby utworzyć nowy alarm.
3. W oknie definiowania alarmu kliknij w przycisk **Nowy**. Podaj nazwę zdarzenia, a następnie wybierz z listy typ zdarzenia: **Urządzenie mobilne podłączone lub rozłączone**.



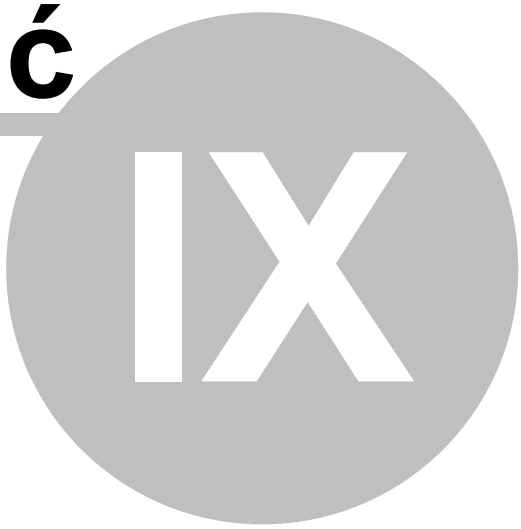
4. Przejdź **Dalej**. Zaznacz pole **Urządzenie jest podłączone** i wybierz z listy **Określone urządzenie**, na przykład **Pozostałe nośniki danych USB**.
5. Następnie, w oknie definiowania alarmów dodaj akcje, które mają być wykonywane w przypadku zaistnienia zdarzenia zdefiniowanego powyżej. Tak utworzony alarm będzie wykrywał sytuacje, w której do monitorowanych komputerów zostanie podłączony nieznany nośnik USB.

Wykrywanie operacji na plikach na urządzeniach mobilnych

Alarm dla operacji na plikach tworzy się w sposób analogiczny, wybierając w punkcie 3. typ zdarzenia: **Operacja na pliku na urządzeniu mobilnym** i oznaczając odpowiednie pola dotyczące tworzenia i zmian plików w punkcie 4. Przykładowe warunki zostały przedstawione na poniższym rysunku.



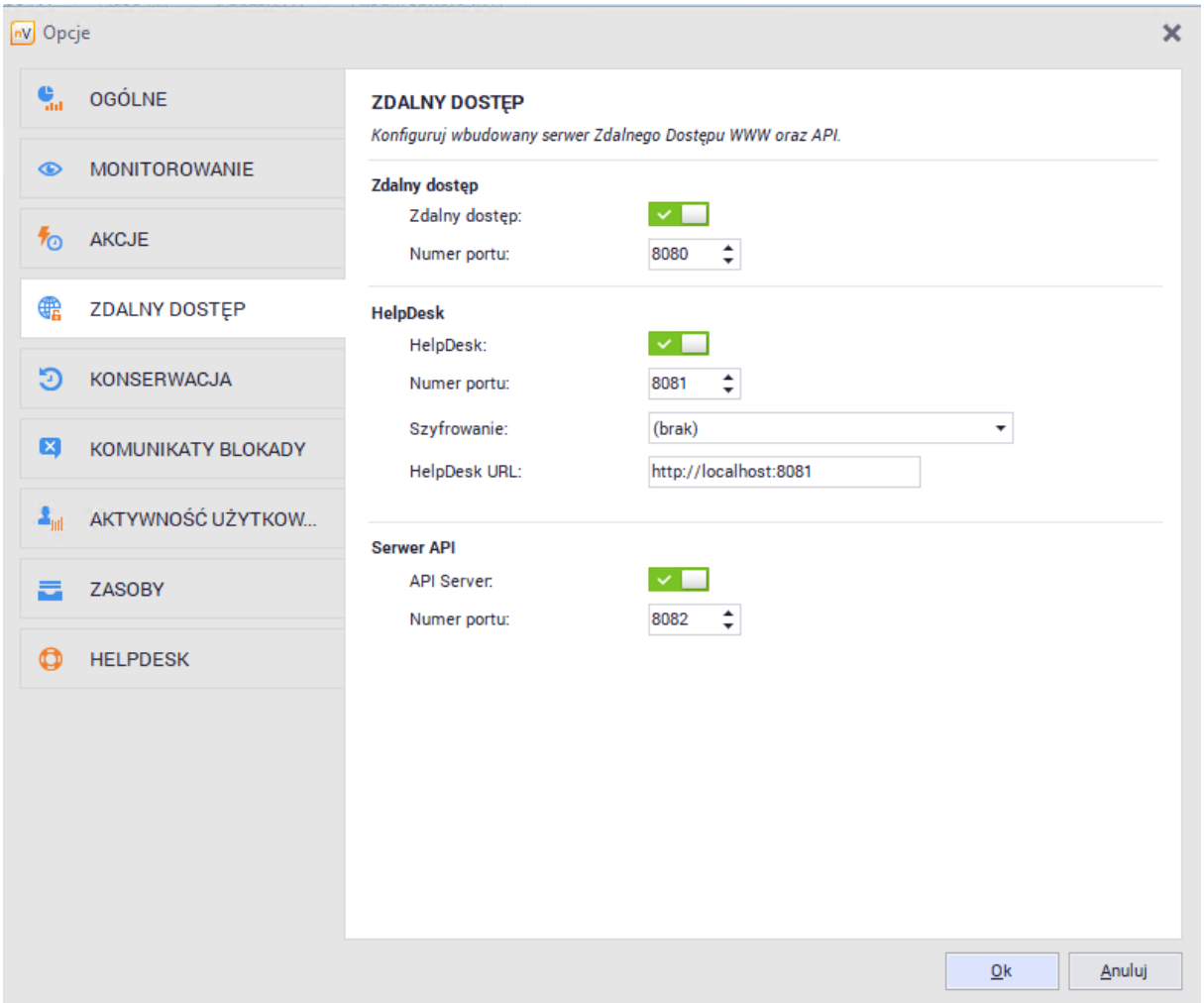
Część



9 Web Access - dostęp przez przeglądarkę WWW

9.1 Jak uzyskać dostęp do nVision przez przeglądarkę WWW?

Aby uzyskać dostęp do nVision przez przeglądarkę (w trybie read-only) należy w pierwszej kolejności włączyć dostęp WWW w nVision:



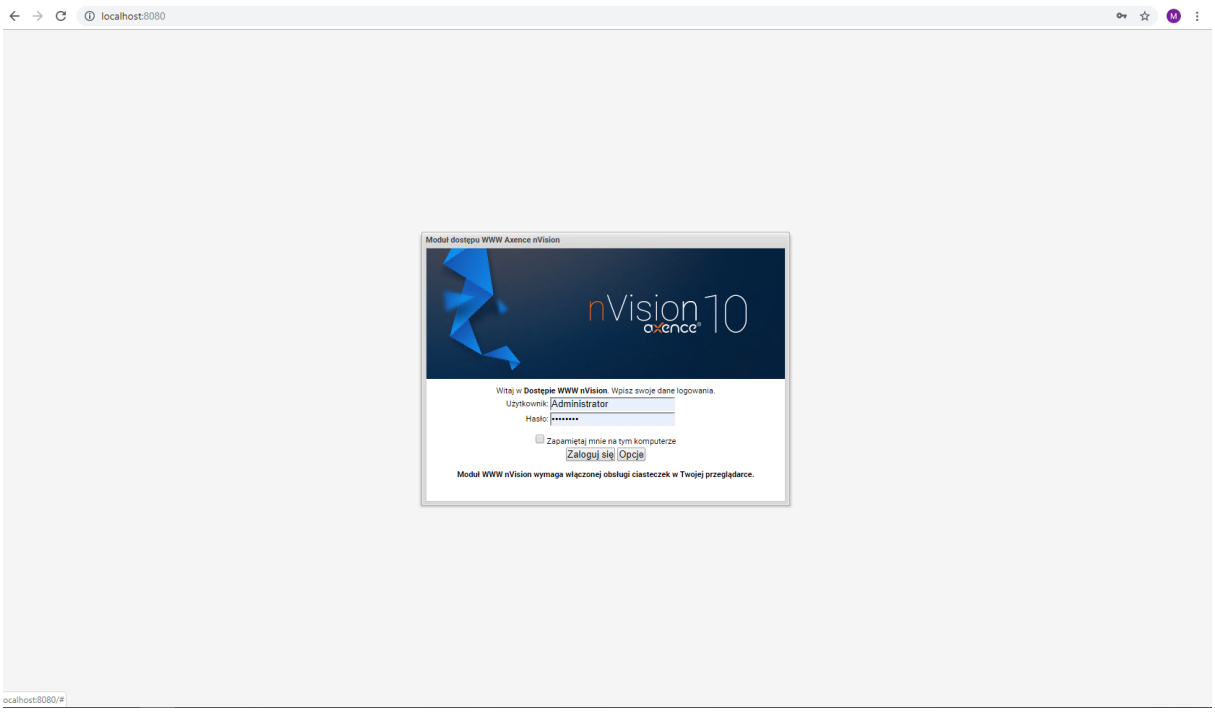
Wybierz opcję **Konfiguracja** z głównego paska narzędziowego programu.

2. Przejdź do zakładki **Zdalny dostęp** a następnie aktywuj zdalny dostęp i wprowadź numer portu, pod którym ma działać zdalny dostęp.

Dostęp przez przeglądarkę

Po włączeniu zdalnego dostępu w sposób opisany powyżej można już korzystać z nVision przez przeglądarkę WWW. W tym celu należy w pasku adresu przeglądarki wpisać adres IP i numer portu komputera, na którym działa nVision, a następnie, po połączeniu się z modułem dostępu, podać nazwę użytkownika oraz hasło i zalogować się do nVision. Uwaga: zdalny dostęp WWW działa w trybie odczytu (read-only), więc nie można za jego pomocą wprowadzać zmian.

Opcja optymalizacji dla wolnych komputerów (okno logowania, przycisk **Opcje**) umożliwia działanie modułu dostępu WWW do nVision na słabszych komputerach, ale zwiększa zużycie łącza.



9.2 Jak utworzyć konta użytkowników Web Access?

Zdalny dostęp do wybranych funkcjonalności nVision przez przeglądarkę może mieć wielu użytkowników. Aby to było możliwe, należy odpowiednio skonfigurować ich konta. Uwaga: zdalny dostęp WWW działa w trybie odczytu (read-only), więc nie można za jego pomocą wprowadzać zmian.

Dostęp przez WWW jest wbudowany dla użytkowników o typie **Administrator** i może zostać włączony dla użytkowników o typie **HelpDesk**. Nie jest możliwe włączenie zdalnego dostępu dla pozostałych typów użytkowników.

Użytkownicy typu Administrator

Administratorzy mają dostęp do wszystkich map, urządzeń, a także do raportów, audytu i dziennika zdarzeń.

Użytkownicy typu HelpDesk

Dla kont użytkowników HelpDesk ustala się prawa dostępu do określonych map:

- Jeżeli dana mapa nie ma zdefiniowanego prawa, to jest dla niej ustawiane prawo domyślne.
- Użytkownicy nie mają dostępu do audytu, raportów i dziennika zdarzeń (ten ostatni widoczny tylko w informacjach o urządzeniu, globalny dziennik zdarzeń nie jest widoczny). Wymienione opcje są ukryte dla użytkowników.
- Mapa, dla której użytkownik nie ma prawa dostępu "Widok mapy", nie jest wyświetlana w drzewie atlasu.

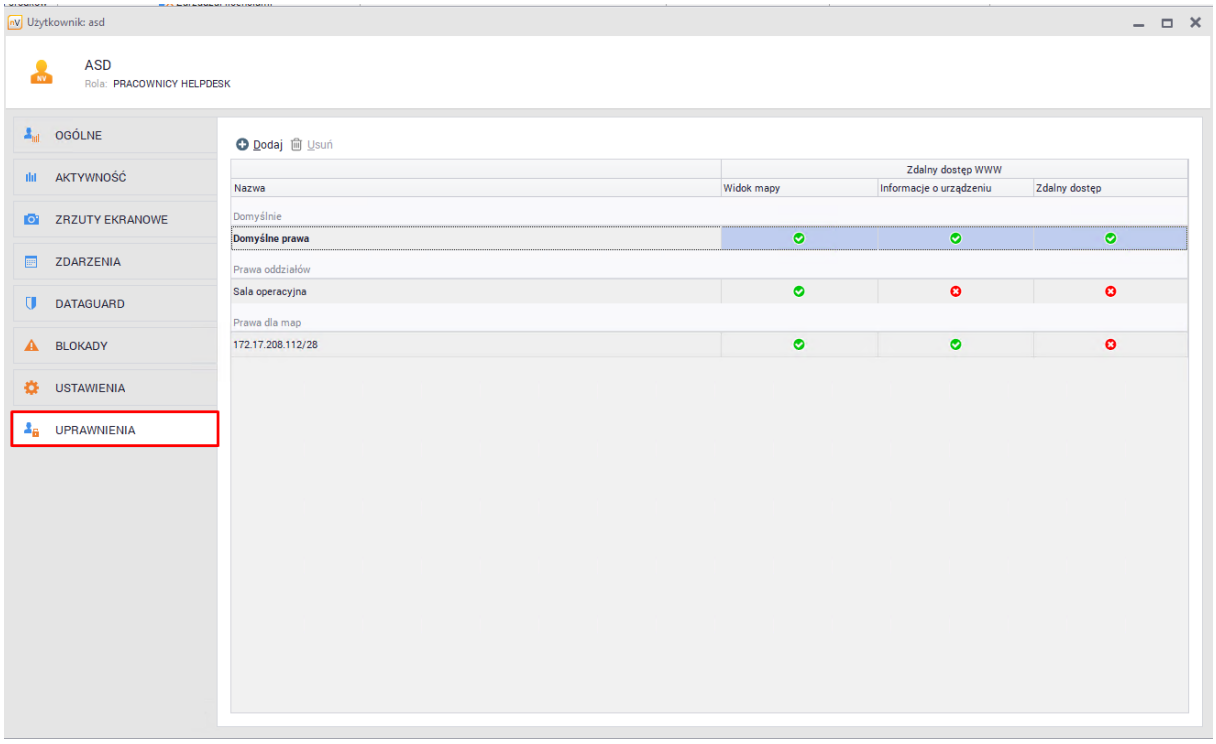
Prawa dostępu

Prawo dostępu	Wymagane prawa	Opis
Widok mapy		Wyświetlanie danej mapy w drzewie atlasu. Daje możliwość zobaczenia wszystkich urządzeń w obrębie tej mapy.
Informacje o urządzeniu (Host Info)	Widok mapy	Dostęp do wszystkich informacji o urządzeniach (serwisy, liczniki, aktywność użytkowników, inwentaryzacja i inne).
Zdalny dostęp		Możliwość uzyskania zdalnego dostępu (VNC) do urządzeń z danej mapy.

Tworzenie kont

Aby utworzyć konto użytkownika Web Access:

1. Dla nowego użytkownika: utwórz konto użytkownika typu HelpDesk. Kliknij w przycisk **Użytkownicy**, następnie **Dodaj** użytkownika; podaj nazwę, rolę (Help-Desk) i hasło. Przejdź do punktu 3.
2. Dla istniejącego użytkownika: kliknij w zakładkę **Użytkownicy**, a następnie klikając prawym przyciskiem na wybrane konto wybieramy opcję **Informacje o użytkowniku.**
3. W zakładce **Uprawnienia** możesz edytować prawa domyślne, a także dodawać prawa dla wybranych oddziałów i map (przycisk **Dodaj**).

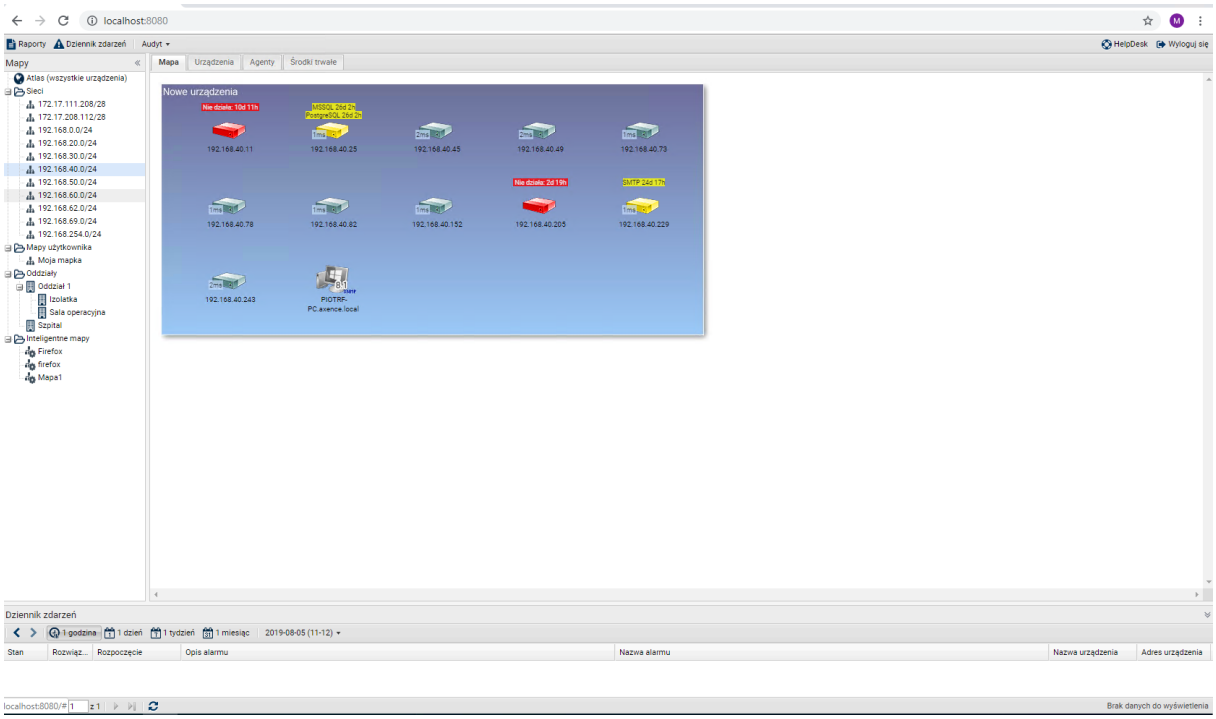


Aby dowiedzieć się więcej o kontach użytkowników, przejdź do rozdziału Zarządzanie użytkownikami.

9.3 Układ okna

Drzewo atlasu

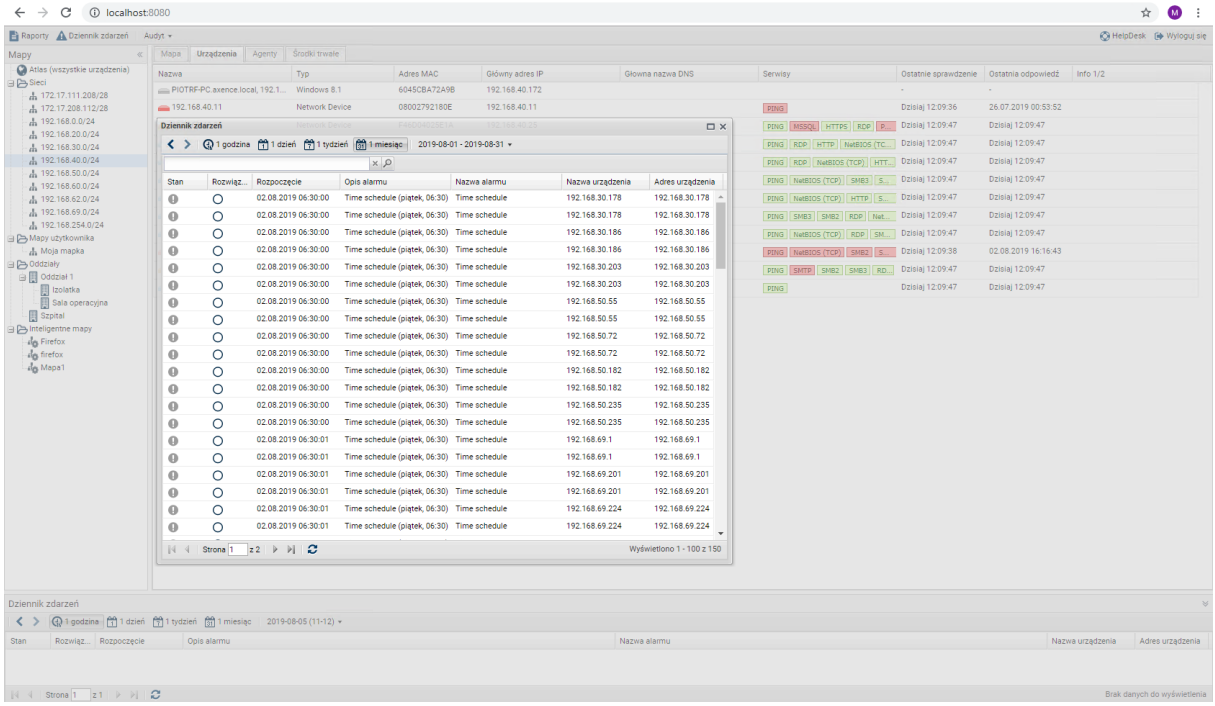
Drzewo atlasu, zlokalizowane w górnej lewej części okna, przedstawia listę wszystkich dostępnych sieci, map użytkownika, oddziałów i inteligentnych map. Po wybraniu mapy w drzewie, jest ona prezentowana po prawej stronie. Można zmieniać szerokość kolumny drzewa atlasu, a także ją zminimalizować.



Dziennik zdarzeń

Pasek dziennika zdarzeń (dolna część okna) pozwala szybko sprawdzić ostatnie alarmy. Można zmieniać rozmiar obszaru, w którym prezentowane są zdarzenia. Aby otworzyć dziennik zdarzeń w oddzielnej ramce, kliknij w przycisk 

znajdujący się w górnej części okna.



Mapa

Ta zakładka prezentuje graficznie mapę wybraną w drzewie atlasu.

Urządzenie

Zakładka prezentuje listę urządzeń należących do wybranej mapy.

Agenty

Zakładka prezentuje listę urządzeń z zainstalowanymi Agentami. Wyświetlane są m.in. podstawowe statystyki i oczekujące instrukcje.

Środki trwałe

Zakładka prezentuje listę wszystkich środków trwałych.

9.4 Audyt

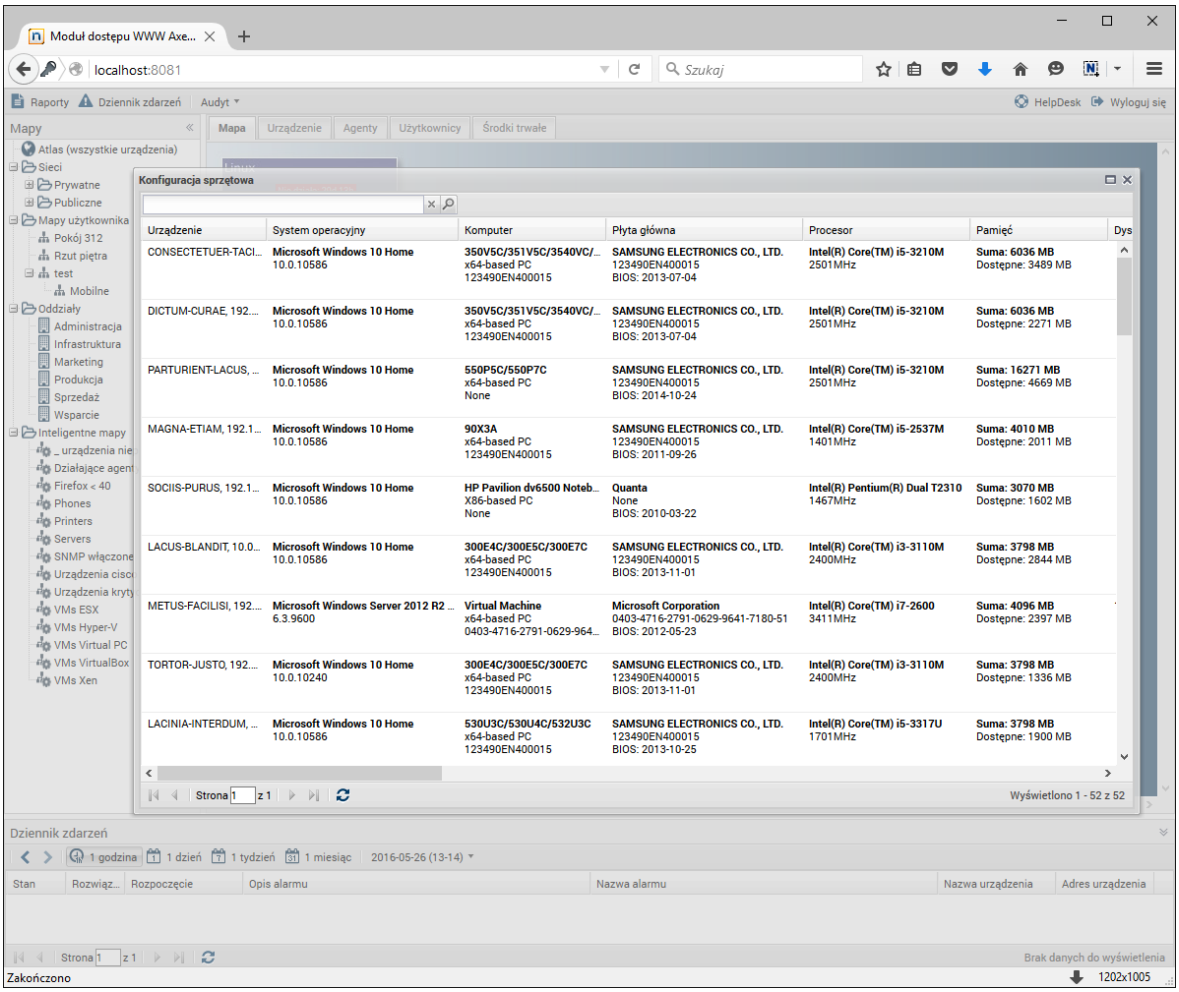
Axence nVision® automatycznie gromadzi informacje o konfiguracji sprzętowej każdego komputera z systemem operacyjnym Windows oraz zainstalowanego na nim oprogramowania.

Sprzęt

Inwentaryzacja sprzętu umożliwia kontrolowanie urządzeń w monitorowanych sieciach. W tym widoku zestawione są informacje dotyczące konfiguracji sprzętowej wszystkich monitorowanych urządzeń – od systemu operacyjnego, przez procesor, monitory i wiele innych aż po lokalne drukarki.

Aby przeglądać konfigurację sprzętową monitorowanych urządzeń:

1. Kliknij w przycisk **Audyt** znajdujący się w górnej części okna.
2. Wybierz opcję Sprzęt.
3. Aby szybciej znaleźć szukane wpisy, użyj opcji wyszukiwania znajdującej się w górnej części okna.
4. Aby zmienić liczbę wyświetlanych kolumn, sposób sortowania lub grupowanie, rozwiń menu przy nagłówkach kolumn.

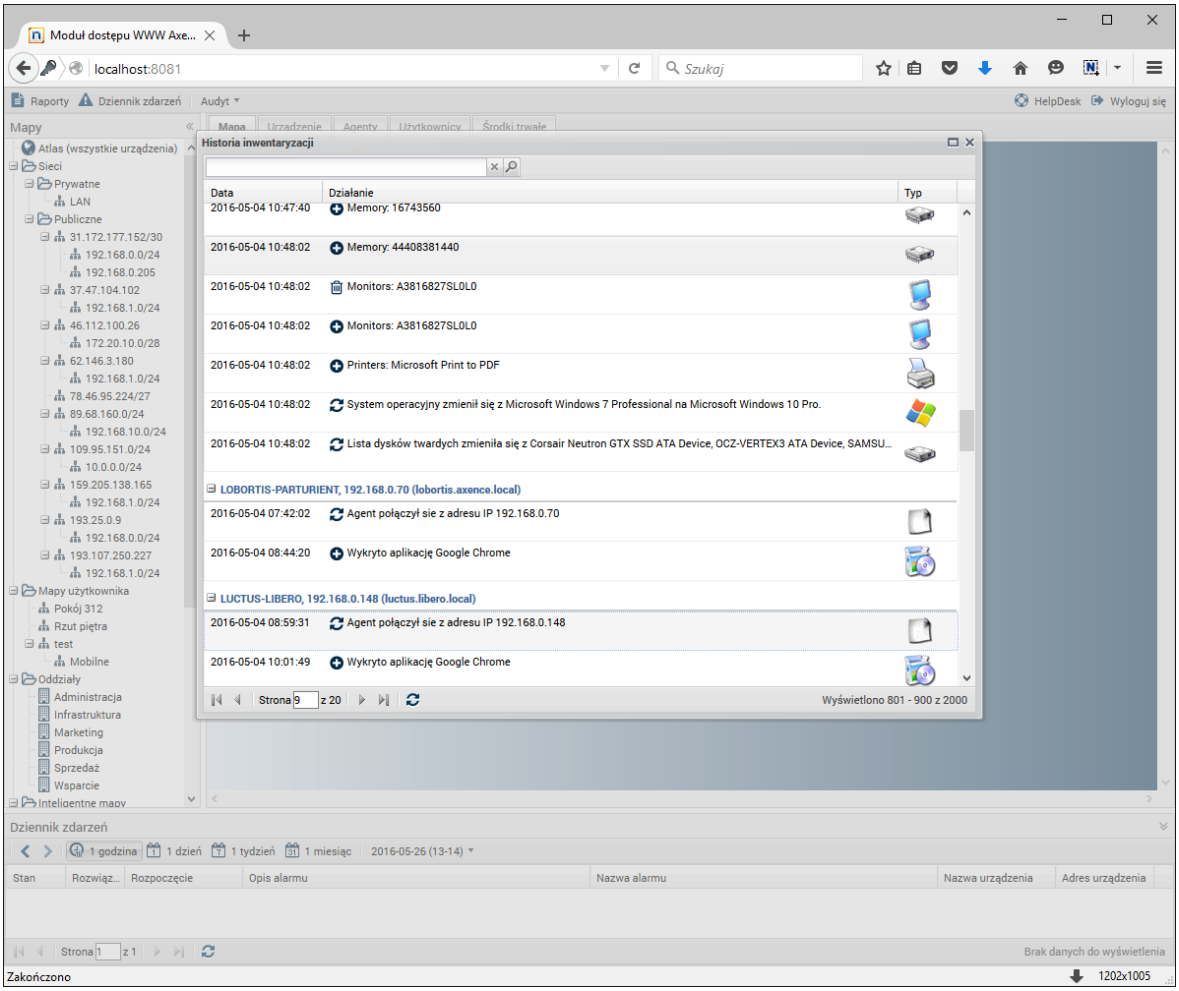


Historia inwentaryzacji

Zakładka zawiera informacje o zmianach sprzętu i oprogramowania na wszystkich monitorowanych urządzeniach.

Aby przeglądać historię inwentaryzacji:

1. Kliknij w przycisk **Audyt** znajdujący się w górnej części okna.
2. Wybierz opcję Historia inwentaryzacji.
3. Aby szybciej znaleźć szukane wpisy, użyj opcji wyszukiwania znajdującej się w górnej części okna.
4. Aby zmienić liczbę wyświetlanych kolumn, sposób sortowania lub grupowanie, rozwiń menu przy nagłówkach kolumn.



Audyt inwentaryzacji oprogramowania

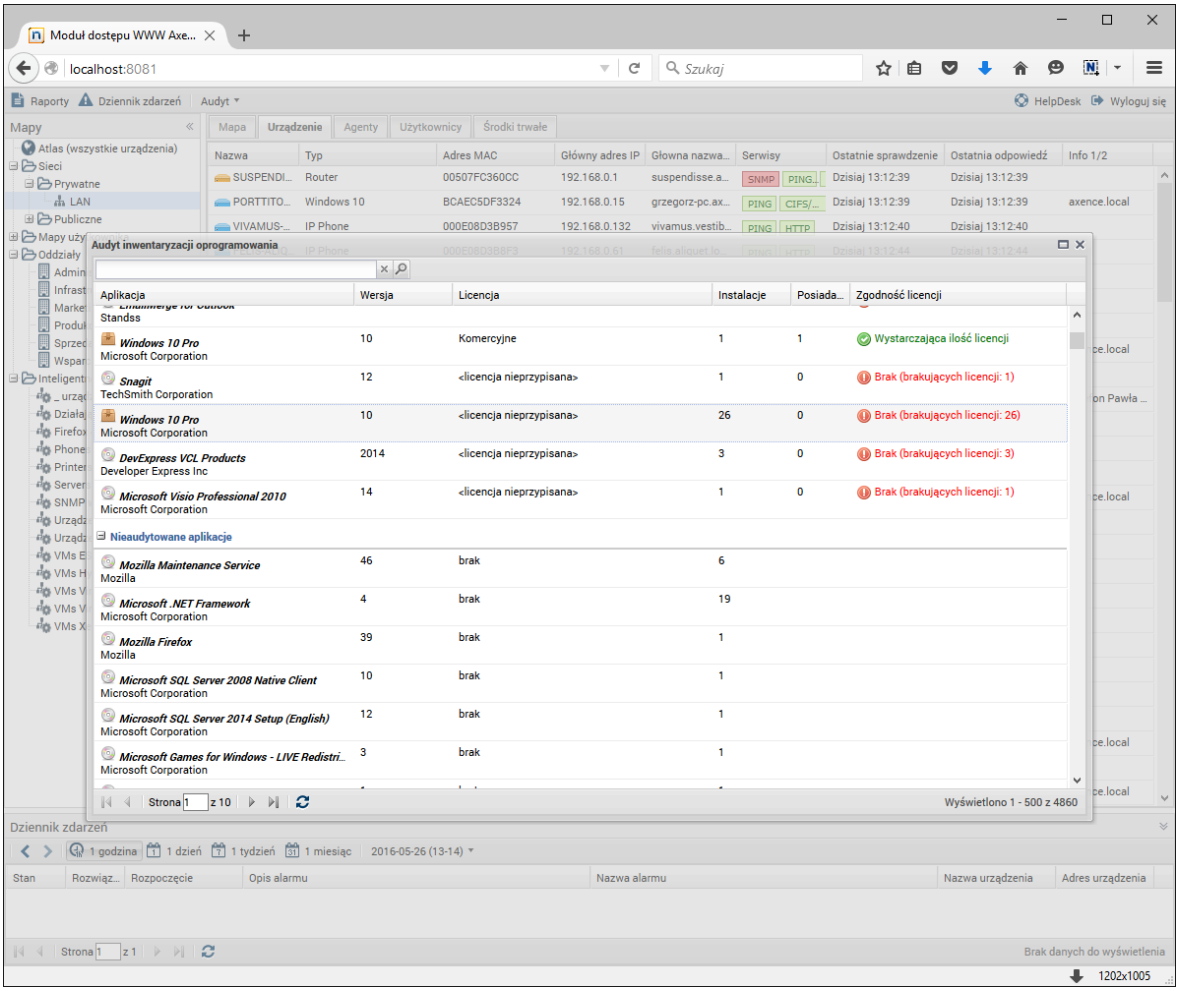
Inwentaryzacja oprogramowania umożliwia kontrolę aplikacji zainstalowanych na komputerach monitorowanych użytkowników. Wpisy podzielone są na trzy kategorie: audytowane aplikacje

(licencjonowane programy rozpoznane przez nVision, podlegające audytowi), nieaudytowane aplikacje (programy rozpoznane przez nVision, niewymagające licencjonowania i niepodlegające audytowi) oraz nieznane aplikacje (wykryte przez nVision ale nieposiadające ustalonego wzorca).

W przypadku audytowanych aplikacji wyświetlana jest informacja o typie licencji, liczbie instalacji w obrębie monitorowanej sieci oraz liczbie posiadanych licencji. Na podstawie tych wartości wyliczana jest zgodność licencji i zostaje ona zaprezentowana w graficzny sposób z wyróżnieniem nadwyżek oraz braków.

Aby przeglądać audyt inwentaryzacji oprogramowania:

1. Kliknij w przycisk **Audyt** znajdujący się w górnej części okna.
2. Wybierz opcję Programy.
3. Aby szybciej znaleźć szukane wpisy, użyj opcji wyszukiwania znajdującej się w górnej części okna.
4. Aby zmienić liczbę wyświetlanych kolumn, sposób sortowania lub grupowanie, rozwiń menu przy nagłówkach kolumn.



Wydruki

Okno audytu wydruków umożliwia przeglądanie historii wydruków w wybranych okresach (dzień,

tydzień lub miesiąc). Dane pogrupowane są według drukarek, a następnie w porządku chronologicznym.

Aby przeglądać audyt wydruków:

1. Kliknij w przycisk **Audyt** znajdujący się w górnej części okna.
2. Wybierz opcję Wydruki.
3. Wybierz okres, dla którego mają być wyświetlone dane.
4. Aby szybciej znaleźć szukane wpisy, użyj opcji wyszukiwania znajdującej się w górnej części okna.
5. Aby zmienić liczbę wyświetlanych kolumn, sposób sortowania lub grupowanie, rozwiń menu przy nagłówkach kolumn.
6. Aby zapoznać się ze szczegółami danego wydruku, rozwiń wpis klikając w ⊞.

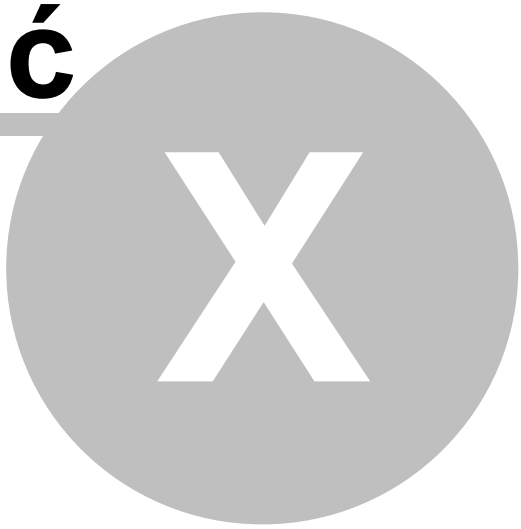
DataGuard

Okno audytu DataGuard umożliwia przeglądanie historii wydruków w wybranych okresach (dzień, tydzień lub miesiąc). Dane pogrupowane są według drukarek, a następnie w porządku chronologicznym.

Aby przeglądać audyt wydruków:

1. Kliknij w przycisk **Audyt** znajdujący się w górnej części okna.
2. Wybierz opcję DataGuard.
3. Wybierz okres, dla którego mają być wyświetlone dane.
4. Aby szybciej znaleźć szukane wpisy, użyj opcji wyszukiwania znajdującej się w górnej części okna.
5. Aby zmienić liczbę wyświetlanych kolumn, sposób sortowania lub grupowanie, rozwiń menu przy nagłówkach kolumn.

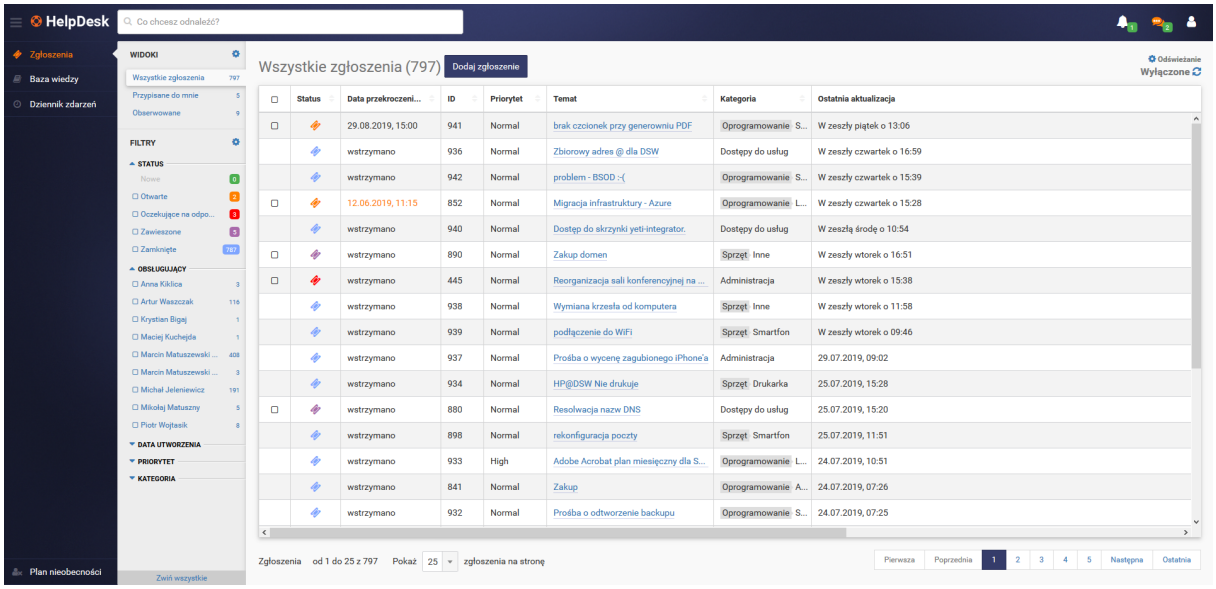
Część



10 HelpDesk - baza zgłoszeń

10.1 Wprowadzenie

Moduł HelpDesk zapewnia interaktywną bazę zgłoszeń dla użytkowników, która ułatwia zgłaszanie i rozwiązywanie problemów. Oprócz tego, wzbogacana na bieżąco kolejnymi zgłoszeniami problemów technicznych i historią ich rozwiązywania, staje się cenną bazą wiedzy zarówno dla użytkowników, jak i pracowników wsparcia technicznego.



Widok listy zgłoszeń - widok użytkownika.

Interfejs HelpDesk

- Baza zgłoszeń umożliwia użytkownikom zgłaszać problemy techniczne za pomocą mechanizmu tworzenia zgłoszeń. Zgłoszenia mogą być tworzone zarówno przez użytkowników z zainstalowanym Agentem, jak i przez pozostałych (po zalogowaniu się lub e-mailem).
- Zgłoszenia są rozwiązywane przez pracowników HelpDesku.
- W części dla Administratorów i pracowników HelpDesk przychodzące zgłoszenia są przetwarzane i przyporządkowywane odpowiednim osobom, które otrzymują powiadomienie o przypisanym im problemie do rozwiązania.
- Użytkownik może monitorować proces rozwiązywania zgłoszonego przez niego problemu i jego aktualnego statusu, jak również wymiany informacji z administratorem za pomocą komentarzy, które mogą być wpisywane i śledzone przez obydwie strony.
- Baza wiedzy to miejsce, w którym Administratorzy i pracownicy HelpDesku mogą umieszczać artykuły opisujące procedury stosowane w danej instytucji oraz najczęściej występujące problemy i ich rozwiązania.

Przykładowy wygląd bazy zgłoszeń z poziomu Administratora prezentowany jest powyżej.

Powiązane tematy

Konfiguracja modułu HelpDesk

- Ustawienia
- Uruchamianie interfejsu HelpDesk
- Widoki główne
- Komunikaty
- Dystrybucja plików

10.2 Zarządzanie i konfiguracja

10.2.1 Konfiguracja

Aby zacząć korzystanie z modułu HelpDesk, należy włączyć i skonfigurować poniższe ustawienia w głównym oknie nVision.

Konfiguracja dostępu do HelpDesku

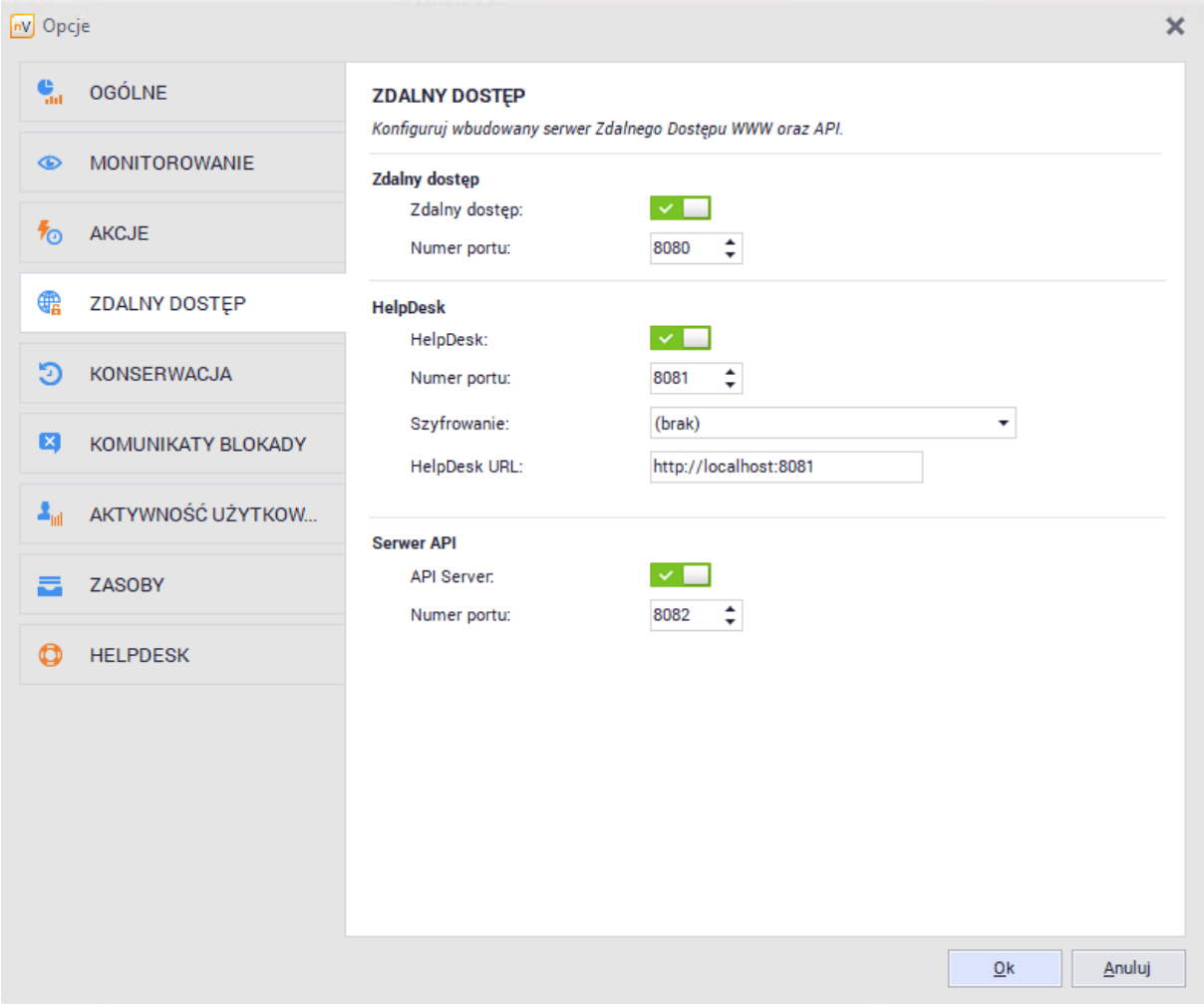
Aby uruchomić funcjonalność HelpDesk, należy w pierwszej kolejności włączyć dostęp do tego modułu w nVision:

1. Wybierz **Narzędzia / Opcje**, zakładka **Zdalny dostęp.**
2. Zaznacz opcję **HelpDesk,** wprowadź numer portu, pod którym ma on działać oraz podaj adres URL wraz z portem, pod którym HelpDesk będzie osiągalny dla Agentów.

   URL to adres IP Serwera nVision, na którym działa HelpDesk. **Ważne**: zamień "localhost" na odpowiedni adres URL Serwera nVision, np. 192.168.0.100:8081 w sieci lokalnej.

Powiązane tematy

- Jak uzyskać dostęp do nVision przez przeglądarkę WWW?

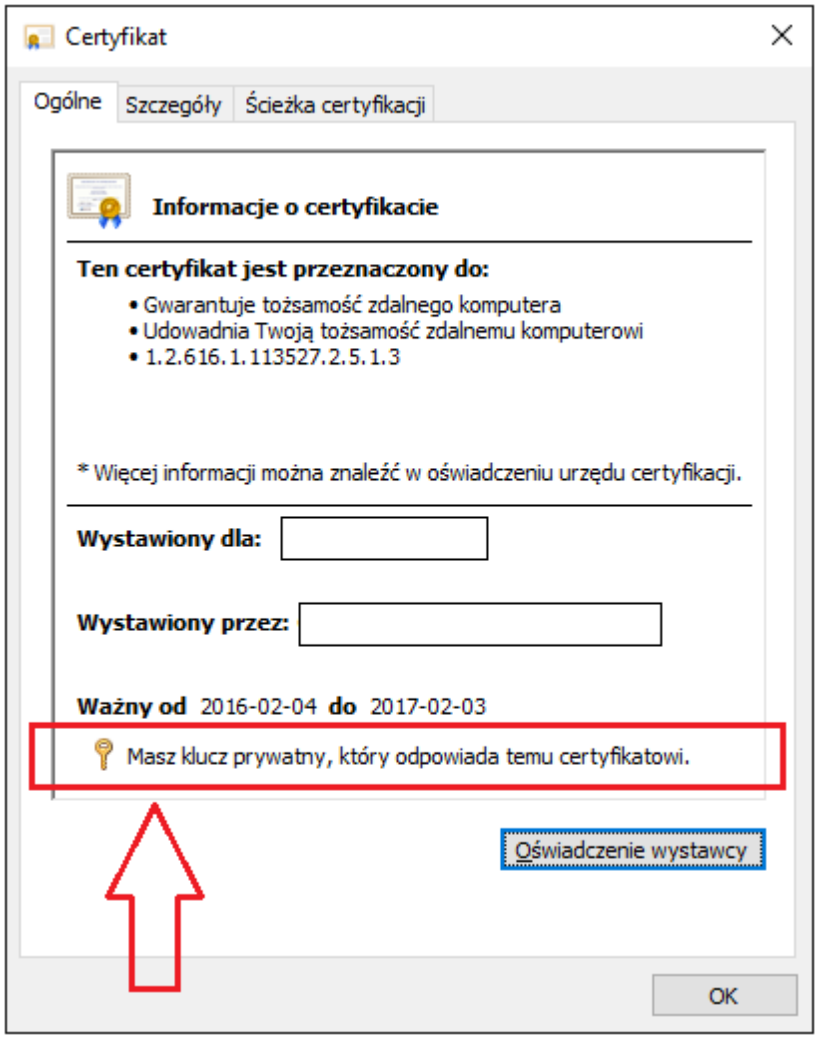


Konfiguracja dostępu do HelpDesku w opcjach nVision.

10.2.2 Dostęp HTTPS

Wymagania:

- Koniecznym warunkiem jest posiadanie aktualnego certyfikatu wystawionego dla domeny, pod którą dostępny będzie HelpDesk.
- Certyfikat musi zawierać klucz prywatny:

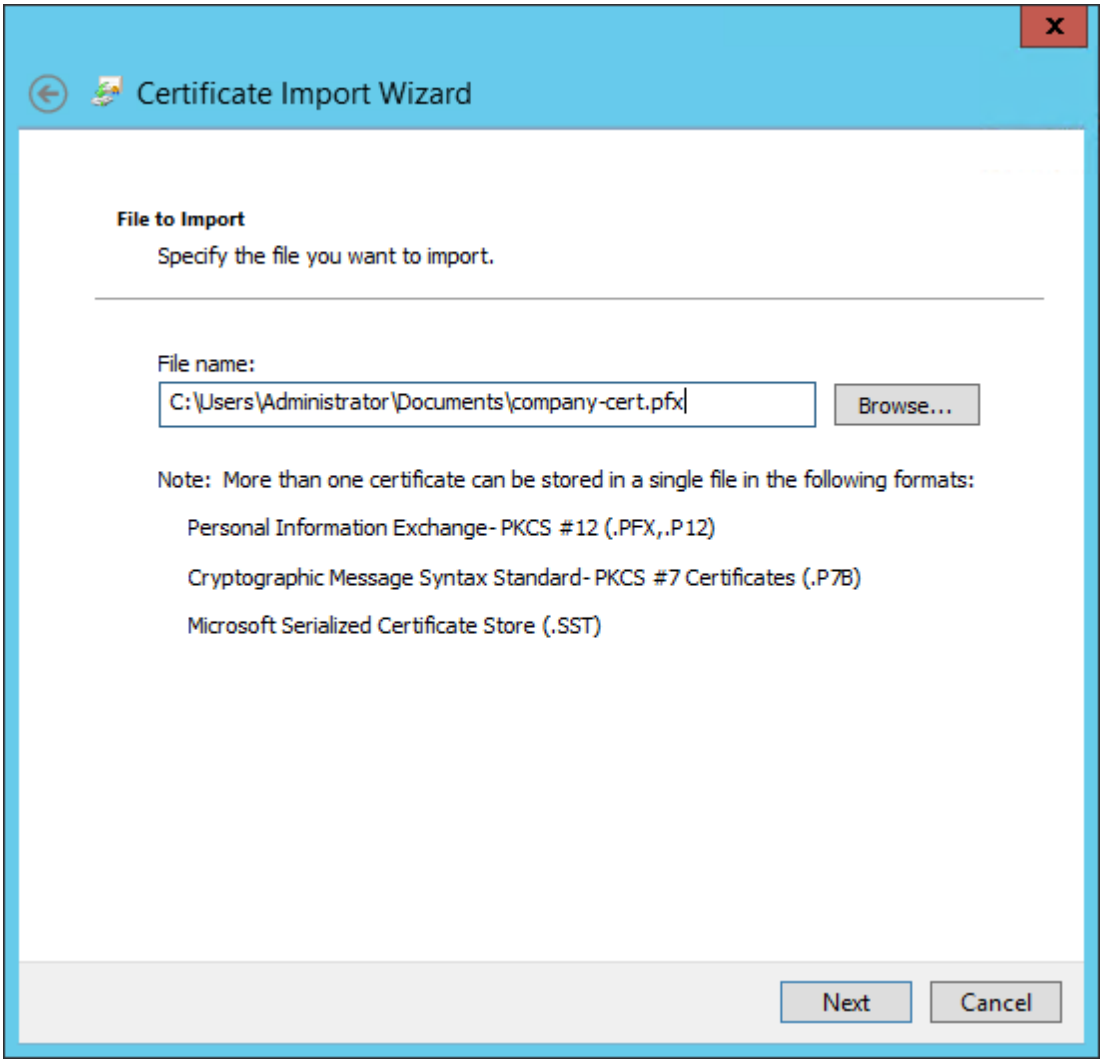


- Certyfikat musi zostać zainstalowany do magazynu osobistych certyfikatów komputera - serwera, na którym zainstalowany jest program Axence nVision® (System Certificate Store \ Local Machine \ Personal). Certyfikat zainstalowany do magazynu użytkownika nie może zostać wykorzystany do konfiguracji szyfrowanego dostępu do helpdesku.

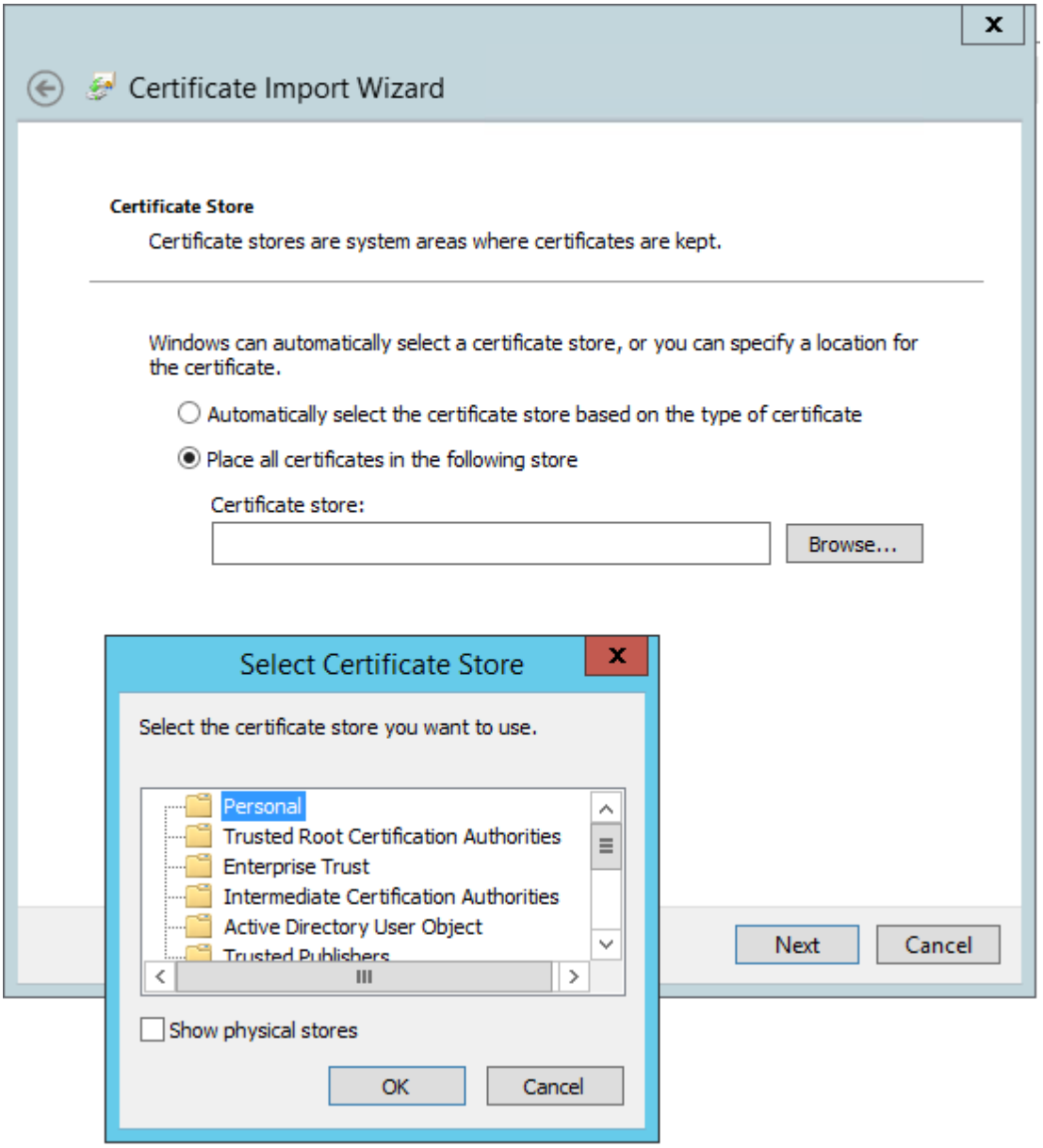
Instalacja certyfikatu

1. Dwukrotnie kliknąć na plik certyfikatu. Otworzy się okno jak poniżej. Wybrać komputer lokalny i kliknąć przycisk **Dalej:**

2. Wskazać ścieżkę do pliku certyfikatu. Kliknąć przycisk **Dalej.**

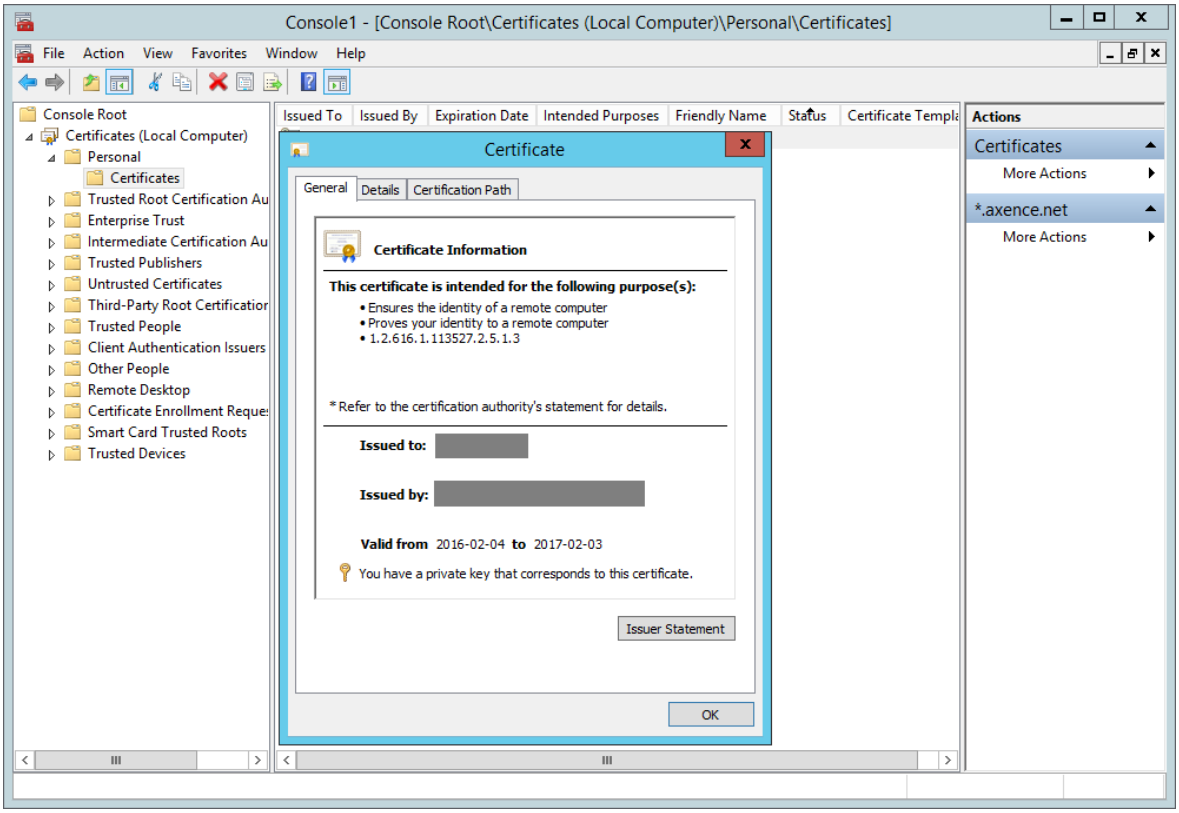


3. Z listy magazynów wskazać magazyn prywatny:

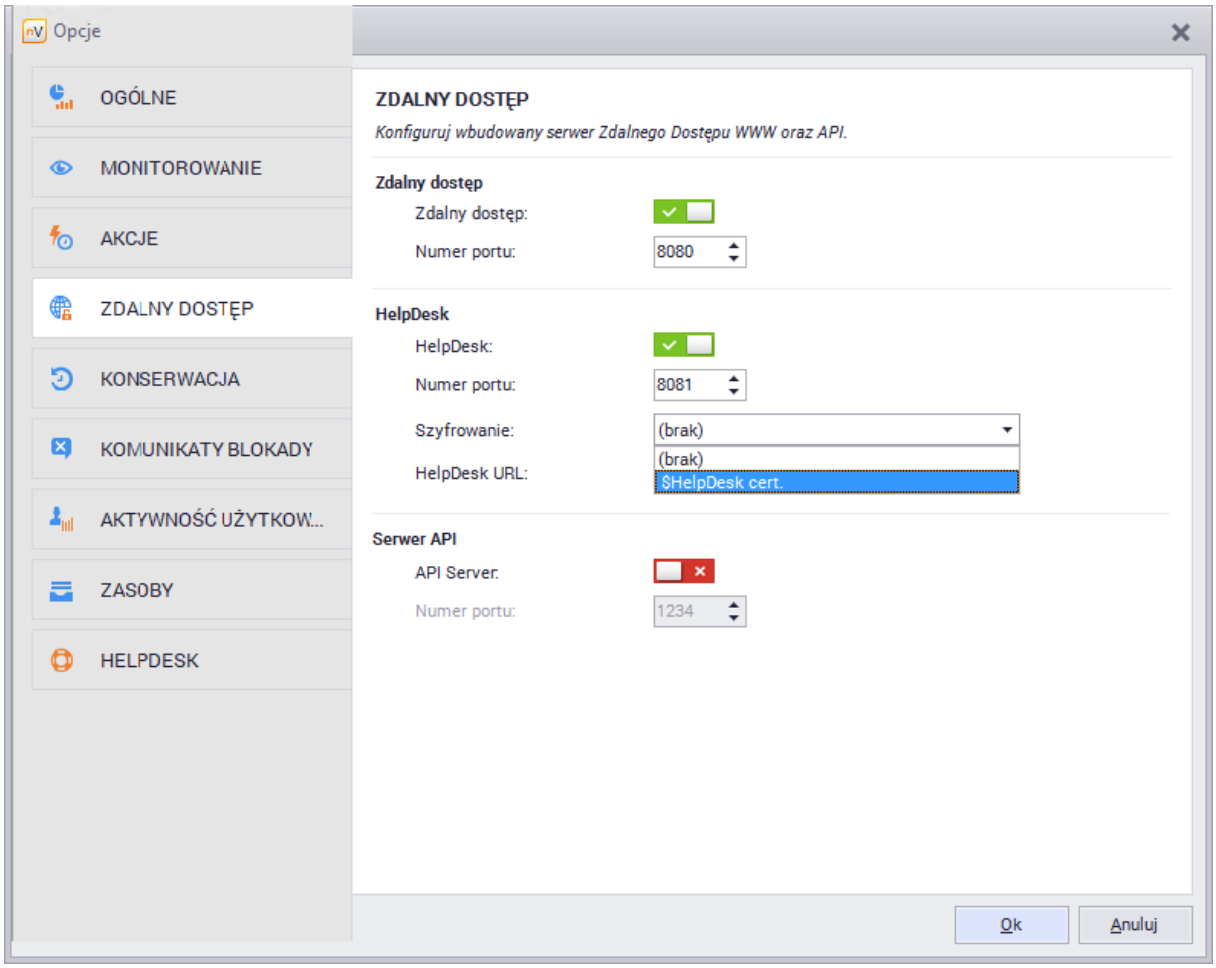


4. Weryfikacja instalacji certyfikatu:

```
uruchom: mmc.exe
File \ Add/Remove snap-in ... \ Certificates \ Add \ Computer account
```



Aby skonfigurować bezpieczny dostęp do helpdesku, przejdź do ustawień nVision i zdalnego dostępu wybierając menu: **Narzędzia \ Opcje \ Zdalny dostęp WWW.**
W sekcji **HelpDesk,** z listy **Szyfrowanie** wybierz zainstalowany na serwerze certyfikat:



Po wskazaniu certyfikatu, adres URL heldesku zostanie automatycznie zmieniony na *https://FQDN:port* - należy dostosować FQDN aby odpowiadał on do faktycznej nazwie DNS (na jaką został wystawiony certyfikat) - najlepiej wówczas skopiować cały URL i sprawdzić czy otwiera się on w przeglądarce. Jeżeli taki test da pozytywny wynik wówczas można zaakceptować okno Opcji klikając przycisk [OK] - wprowadzony URL zostanie rozesłany do Agentów.

10.2.3 Ustawienia

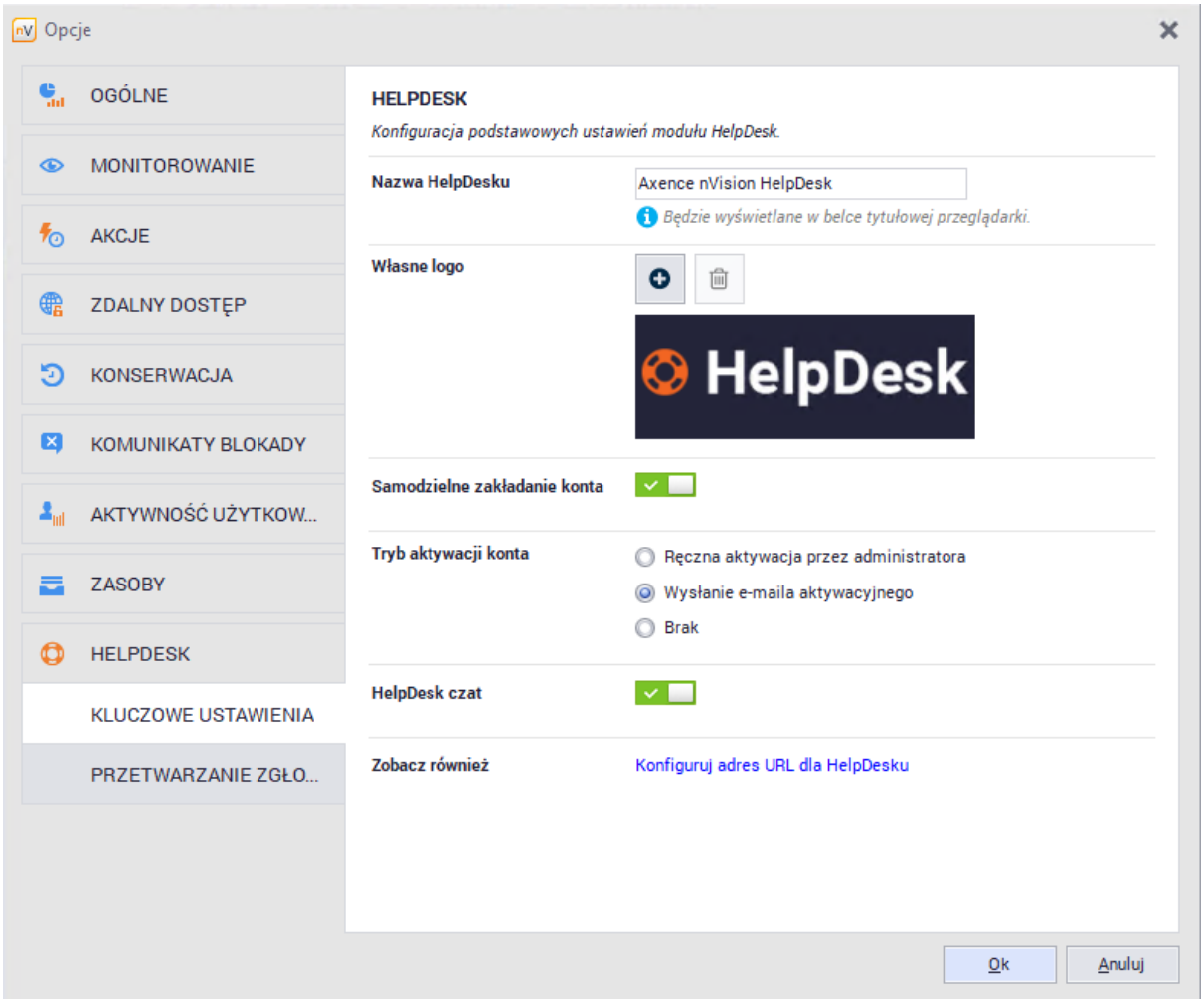
Aby zarządzać ustawieniami HelpDesk, w głównym oknie nVision rozwiń menu i wejdź do **Konfiguracji**, zakładka **HelpDesk**.

Ustawienia znajdują się w dwóch grupach:

- Kluczowe ustawienia
- Przetwarzanie zgłoszeń

Pole	Opis
Nazwa HelpDesku	Podaj tekst, który będzie wyświetlany na ekranie logowania do modułu HelpDesk. Możesz także ustawić logo wybierając obraz znajdujący się na dysku.

Pole	Opis
Własne logo	Umożliwia załadowanie grafiki wyświetlanej jako logo w interfejsie HelpDesku.
Samodzielne zakładanie konta	Zaznaczenie pola umożliwi samodzielne zakładanie kont przez użytkowników, którzy będą używać modułu. Alternatywnie, konta mogą być założone wprost przez administratora.
Tryb aktywacji konta	Pole aktywne w przypadku możliwości samodzielnego zakładania kont przez użytkowników. Aktywacja może mieć miejsce na jeden z poniższych sposobów: • Brak - po założeniu konta przez użytkownika jest ono od razu aktywne. • Wysłanie e-maila aktywacyjnego - do aktywacji wymagane jest kliknięcie w link podany w mailu. Wybranie tej opcji umożliwia weryfikację poprawności adresu mailowego podanego przez użytkownika. • Aktywacja przez administratora - konto musi być aktywowane w nVision pod ikoną **Użytkownicy** poprzez zaznaczenie pola "Konto aktywowane" w odpowiednim wierszu.
HelpDesk czat	Zaznaczenie pola włącza funkcję czatu w nVision HelpDesk.



Konfiguracja kluczowych ustawień HelpDesku w opcjach nVision.

Powiązane tematy

- Zarządzanie i konfiguracja
- Zarządzanie użytkownikami
- Rejestracja użytkownika
- Interfejs HelpDesk

10.2.4 Ustawienia e-mail

Moduł HelpDesk może automatyczne wysyłać wiadomości e-mail o nowych zgłoszeniach oraz o zmianach w zgłoszeniach, a także przetwarzać zgłoszenia użytkowników wysyłane na zdefiniowany adres e-mail.

Powiadomienia przez akcje

Domyślna opcja **Opcje / HelpDesk / Przetwarzanie zgłoszeń / Użyj akcji e-mail nVision do wysyłania powiadomień o zmianach w zgłoszeniach** pozwala na wysyłanie powiadomień e-mail zgodnie z ustawieniami akcji w opcjach nVision.

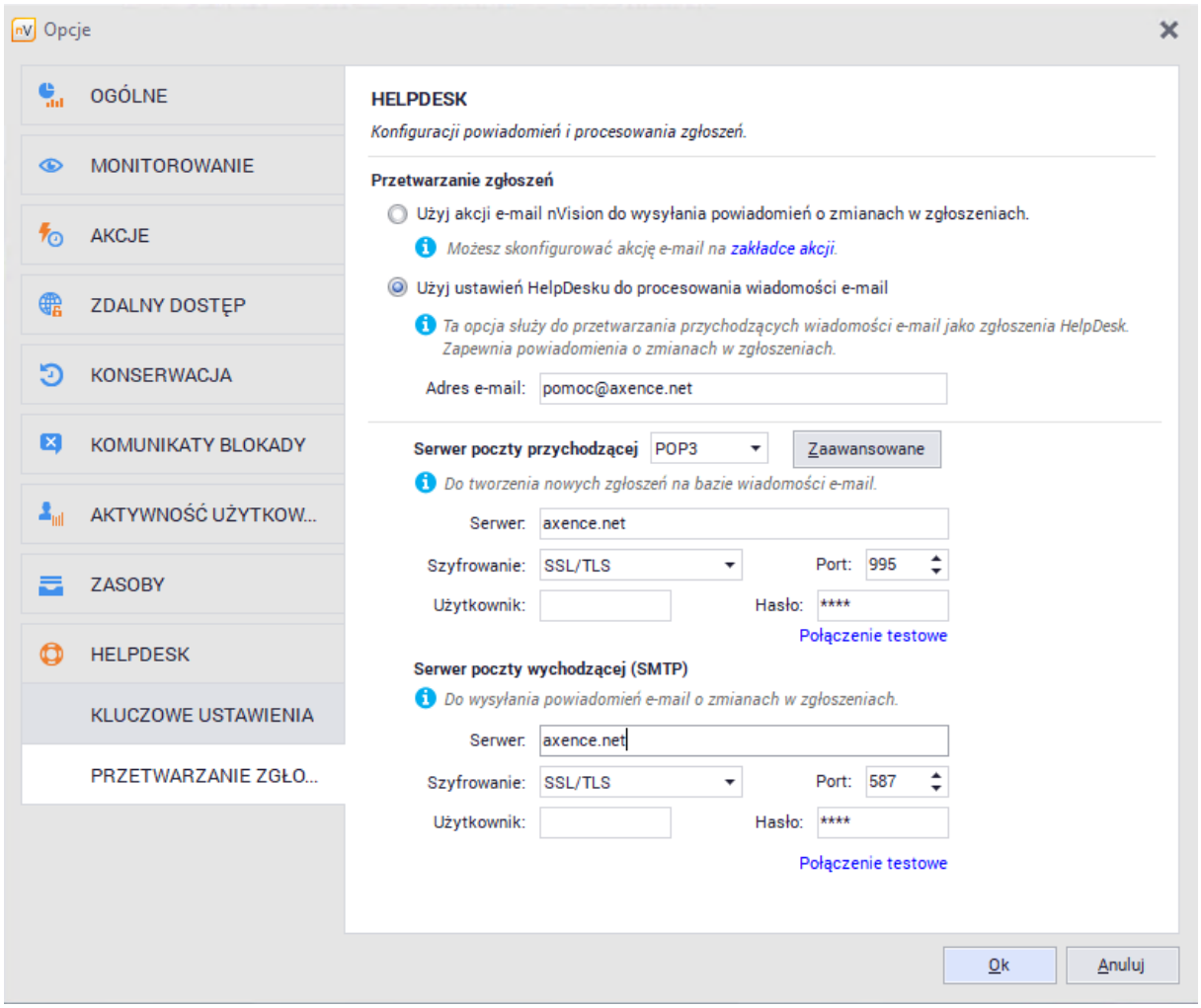
Aby zmienić ustawienia akcji, wejdź w **Narzędzia i opcje / Zarządzaj akcjami**.

Przetwarzanie wiadomości e-mail w HelpDesku

Ta opcja służy do wysyłania powiadomień e-mail o zmianach wprowadzonych w zgłoszeniach oraz do przetwarzania wiadomości e-mail wysyłanych przez użytkowników na zdefiniowany adres e-mail. Dzięki temu możliwe jest tworzenie nowych zgłoszeń przez użytkowników bez dostępu bazy zgłoszeń HelpDesk.

Aby użyć ustawień HelpDesku do przetwarzania e-maili:

1. Wejdź w opcję **Opcje / HelpDesk / Przetwarzanie zgłoszeń**.
2. Wybierz opcję **Użyj ustawień HelpDesku do procesowania wiadomości e-mail**.
3. Zdefiniuj **Adres e-mail**, na który mają być wysyłane zgłoszenia (adres skrzynki, z której nVision HelpDesk będzie przechwytywał wiadomości i na ich podstawie tworzył zgłoszenia).
4. Skonfiguruj ustawienia serwera poczty przychodzącej i wychodzącej. Aby przetestować podane ustawienia, kliknij w przycisk **Połączenie testowe**.



Ustawienia e-mail dla HelpDesku w opcjach nVision.

Uwaga!

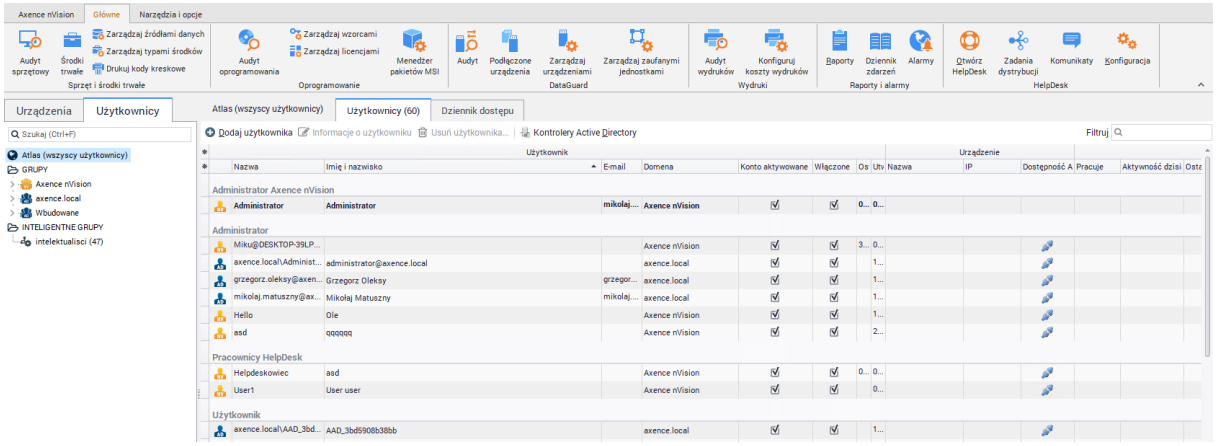
Aby zgłoszenia e-mail były procesowane, zgłaszający musi posiadać konto w nVision z przypisanym **unikalnym** adresem e-mail.

Powiązane tematy

- Akcje
- Zarządzanie i konfiguracja

10.2.5 Zarządzanie użytkownikami

Zarządzanie użytkownikami HelpDesk odbywa się z poziomu okna informacji o użytkownikach.



Zarządzanie kontami użytkowników nVision i HelpDesku.

Typy użytkowników - role w systemie HelpDesk

Rola	Opis
Użytkownik	Może tworzyć oraz aktualizować zgłoszenia. Widzi opublikowane artykuły w bazie wiedzy oraz własne zgłoszenia.
Help-Desk (Pomoc Techniczna)	Osoby zajmujące się udzielaniem pomocy. Oprócz opisanych powyżej, mogą zmieniać status zgłoszenia, delegować zgłoszenia oraz używać opcji zdalnego dostępu do komputera, z którego utworzono zgłoszenie. Mogą także mieć przypisane oddziały, z których zgłoszenia będą im automatycznie przydzielane.
Administrator	Użytkownik tego typu ma najwięcej praw, widzi i może edytować wszystkie zgłoszenia i opcje. Może zarządzać komunikatami i priorytetami i jako jedyny może wysyłać komunikaty (opisane w dziale Komunikaty). Ma także prawa opisane powyżej.

Zakładanie kont

Konta mogą być zakładane na kilka sposobów:

- przez Administratora ręcznie w nVision (wszystkie typy) w zakładce **Użytkownicy** po kliknięciu w przycisk **Dodaj**,
- przez Administratora poprzez pobranie listy kont z kontrolera Active Directory w zakładce **Użytkownicy** po kliknięciu przycisku **Kontrolery Active Directory** i skonfigurowaniu kontrolera domeny,
- samodzielnie przez użytkowników (tylko typ "Użytkownik") bez dodatkowego aktywowania konta lub z aktywacją przez e-mail lub ręcznie przez Administratora.

Aby dowiedzieć się więcej o możliwych scenariuszach zakładania kont użytkowników, przejdź do rozdziału Rejestracja użytkownika.

Zmiana danych użytkownika

Aby zmienić dane użytkownika (np. w celu ustawienia nowego hasła):

1. W zakładce **Użytkownicy** dwukliknij w wiersz użytkownika do edycji.
2. Wprowadź nowe dane użytkownika i zamknij okno.

Uwaga: Nazwy oraz adresy e-mail użytkowników wszystkich typów muszą być unikalne.

Powiązane tematy

Ustawienia

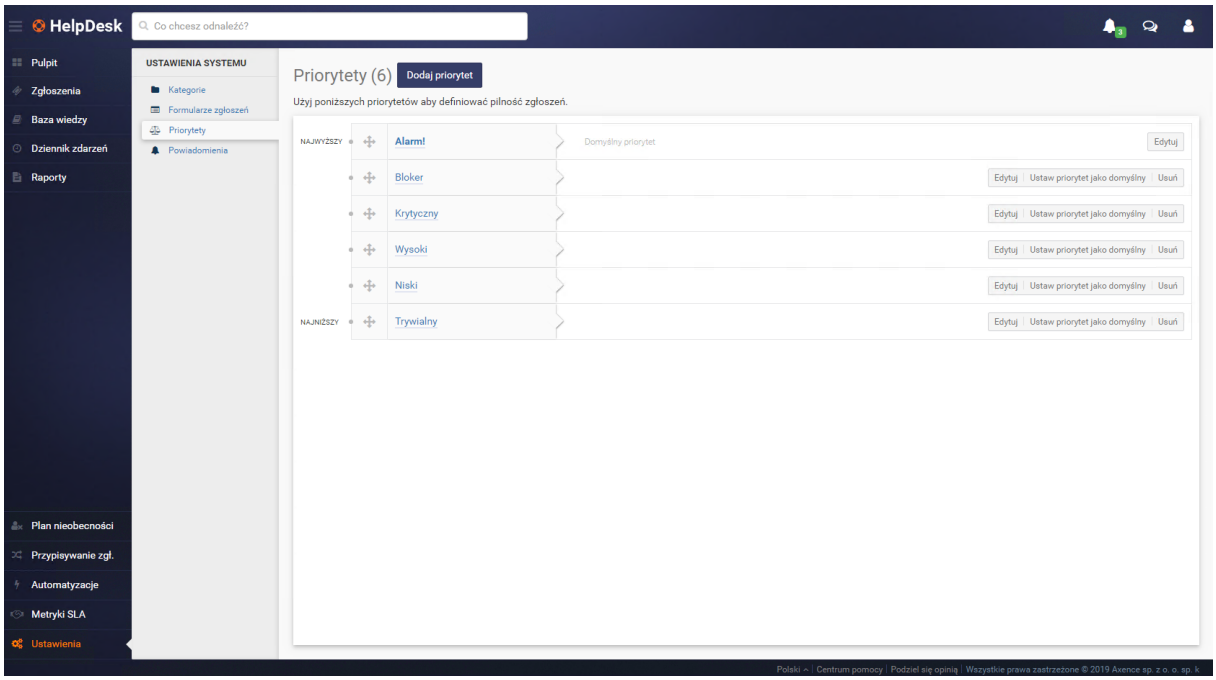
Rejestracja użytkownika

Zarządzanie i konfiguracja

10.2.6 Priorytety

Priorytety pozwalają na określenie ważności zgłaszanego problemu. Użytkownik przy tworzeniu zgłoszenia wybiera z listy priorytet, który najlepiej odpowiada ważności problemu. Administrator może zarządzać istniejącymi priorytetami i dodawać nowe. Zaleca się poprzedzanie nazw cyframi ustawiającymi priorytety w porządku rosnącym lub malejącym, aby po posortowaniu priorytetów alfabetycznie zachowana była czytelność w kolejności ich ważności.

Uwaga: musi istnieć dokładnie jeden domyślny priorytet i nie może on zostać usunięty.



Lista priorytetów.

Zarządzanie priorytetami odbywa się z poziomu interfejsu WWW HelpDesku.

Aby utworzyć nowy priorytet:

1. Przejdź do zakładki **Ustawienia | Priorytety**.

2. Kliknij w przycisk **Dodaj priorytet**.
3. Wpisz nową unikalną nazwę priorytetu i kliknij **Dodaj priorytet**.

Aby edytować priorytet:

1. Przejdź do zakładki **Ustawienia | Priorytety**.
2. Wybierz opcję **Edytuj** dla priorytetu, który chcesz edytować.
3. Wpisz nową nazwę priorytetu i kliknij **Zapisz zmiany**.

Aby zmienić domyślny priorytet:

1. Przejdź do zakładki **Ustawienia | Priorytety**.
2. Wybierz opcję **Ustaw jako domyślną** dla priorytetu, który ma zostać domyślny.
3. Kliknij w przycisk **Ustaw domyślny priorytet**.

Aby usunąć priorytet:

1. Przejdź do zakładki **Ustawienia | Priorytety**.
2. Wybierz opcję **Usuń** dla priorytetu, który chcesz usunąć.
3. Potwierdź usunięcie danego priorytetu klikając **Usuń priorytet**.

Powiązane tematy

HelpDesk

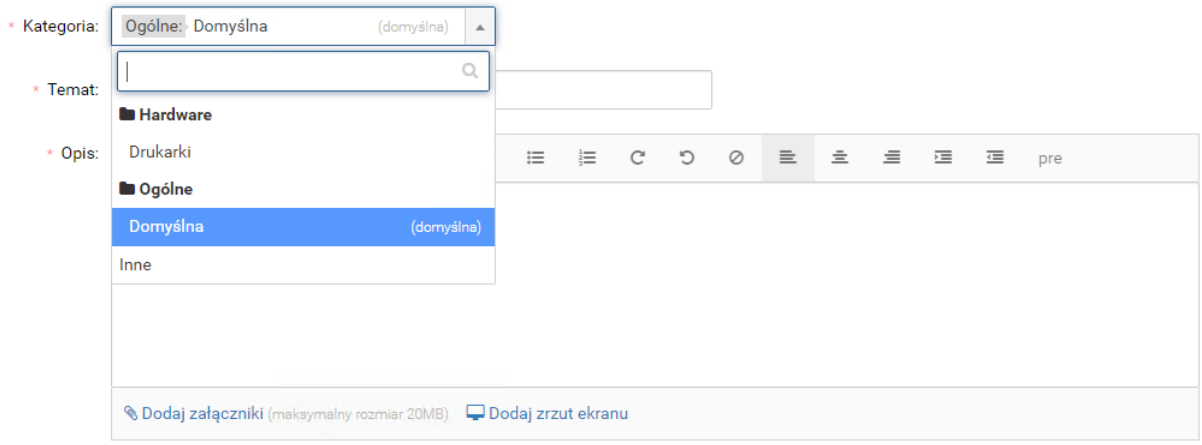
Dodawanie zgłoszenia

10.2.7 Kategorie i etykiety

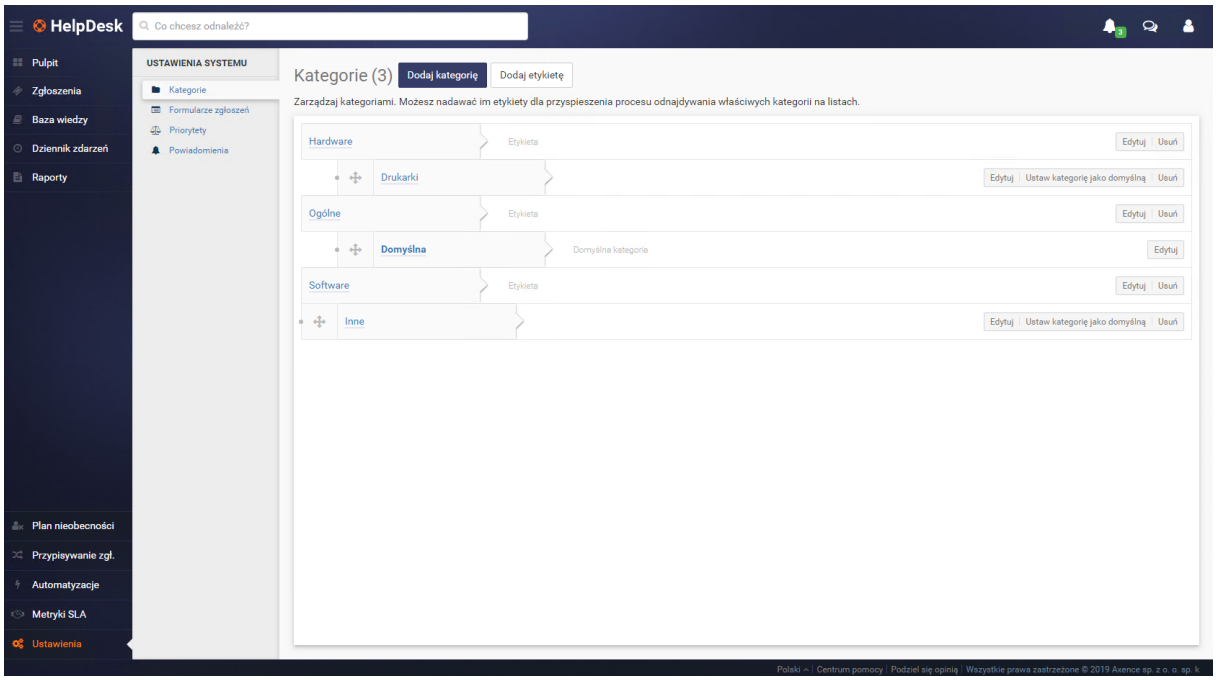
Kategorie oraz etykiety umożliwiają przyporządkowanie zgłoszeń i artykułów do typów problemów, których dotyczą. Przykładowo, Administrator może utworzyć etykietę "Sieć" oraz pod nią kategorie związane z problemami z dostępem do sieci, z oprogramowaniem, ze sprzętem i inne.

Przy tworzeniu zgłoszenia użytkownik wybiera z listy istniejących tę kategorię, która najlepiej pasuje do jego problemu. Początkowo dostępna jest tylko jedna kategoria, **Domyślna**.

Etykiety służą dalszemu kategoryzowaniu zgłoszeń. Pozwalają one na utworzenie wizualnie odseparowanych grup, do których można dodawać kategorie.



Uwaga: musi istnieć dokładnie jedna kategoria domyślna i nie może ona zostać usunięta.



Lista kategorii.

Zarządzanie kategoriami i etykietami odbywa się z poziomu interfejsu WWW HelpDesku.

Aby utworzyć nową kategorię:

1. Przejdź do zakładki **Ustawienia | Kategorie**.
2. Kliknij w przycisk **Dodaj kategorię**.
3. Wpisz nową unikalną nazwę kategorii i kliknij **Dodaj kategorię**.

Aby edytować kategorię:

1. Przejdź do zakładki **Ustawienia | Kategorie**.
2. Wybierz opcję **Edytuj** dla kategorii, którą chcesz edytować.
3. Wpisz nową nazwę kategorii i kliknij **Zapisz zmiany**.

Aby zmienić domyślną kategorię:

1. Przejdź do zakładki **Ustawienia | Kategorie**.
2. Wybierz opcję **Ustaw jako domyślną** dla kategorii, która ma zostać domyślną.
3. Kliknij w przycisk **Ustaw domyślną kategorię**.

Aby usunąć kategorię:

1. Przejdź do zakładki **Ustawienia | Kategorie**.
2. Wybierz opcję **Usuń** dla kategorii, którą chcesz usunąć.
3. Potwierdź usunięcie danej kategorii klikając **Usuń kategorię**.

Postępowanie w przypadku dodawania, edycji lub usuwania etykiety jest analogiczne.

Możliwe jest także przypisanie użytkowników typu HelpDesk lub Administrator do danej kategorii, aby zgłoszenia w tej kategorii były do nich przekazywane automatycznie. Aby dowiedzieć się więcej, przejdź do rozdziału Przypisywanie użytkowników do kategorii.

Powiązane tematy

HelpDesk

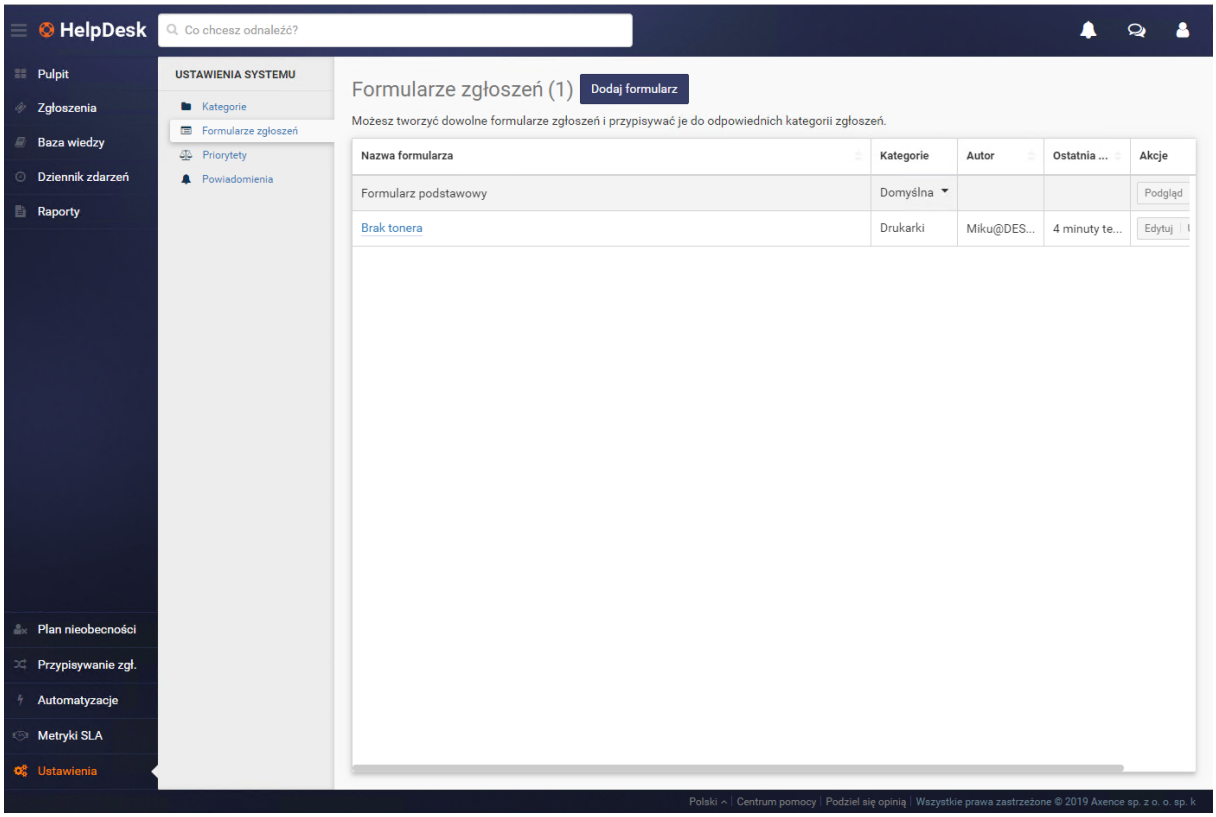
Dodawanie zgłoszenia

Dodawanie artykułu

10.2.8 Formularze zgłoszeń

Formularze pozwalają na skonfigurowanie kilku różnych scenariuszy w momencie tworzenia zgłoszenia. Użytkownik przy tworzeniu zgłoszenia wybiera z listy kategorię, która najlepiej odpowiada ważności problemu. Gdy w systemie dla tej konkretnej kategorii przypisany jest odpowiedni formularz zgłoszenia, strona zostanie zaktualizowana o dodatkowe pola, które usprawnią identyfikację i rozwiązanie problemu. Administrator może zarządzać istniejącymi formularzami i dodawać nowe.

Uwaga: musi istnieć dokładnie jeden domyślny priorytet i nie może on zostać usunięty.



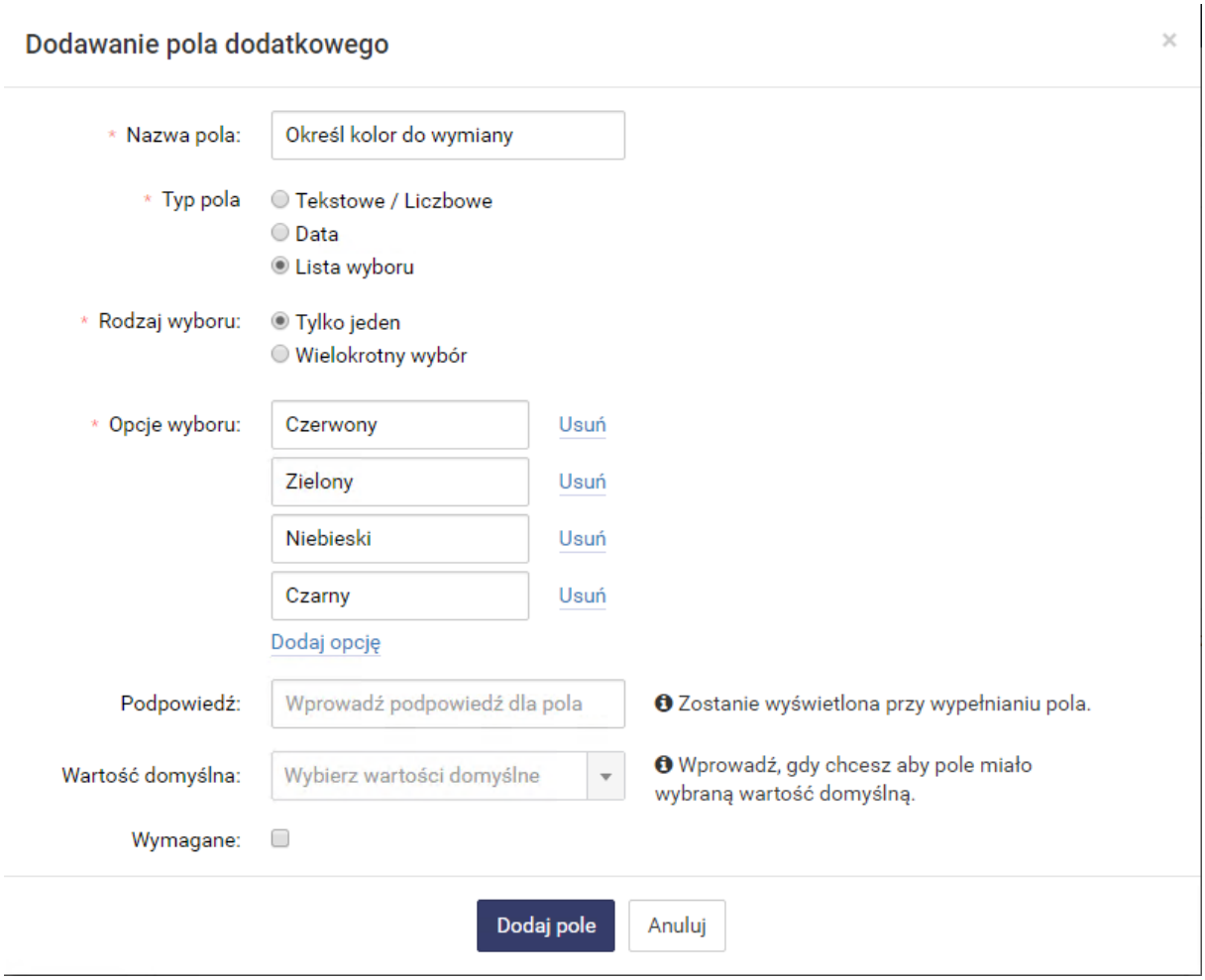
Aby utworzyć nowy formularz zgłoszeń:

1. Przejdź do zakładki **Ustawienia | Formularze zgłoszeń**.
2. Kliknij w przycisk **Dodaj formularz**.
3. Wpisz nową unikalną nazwę formularza oraz okresl dodatkowe pola, które pojawią się w momencie tworzenia zgłoszenia.

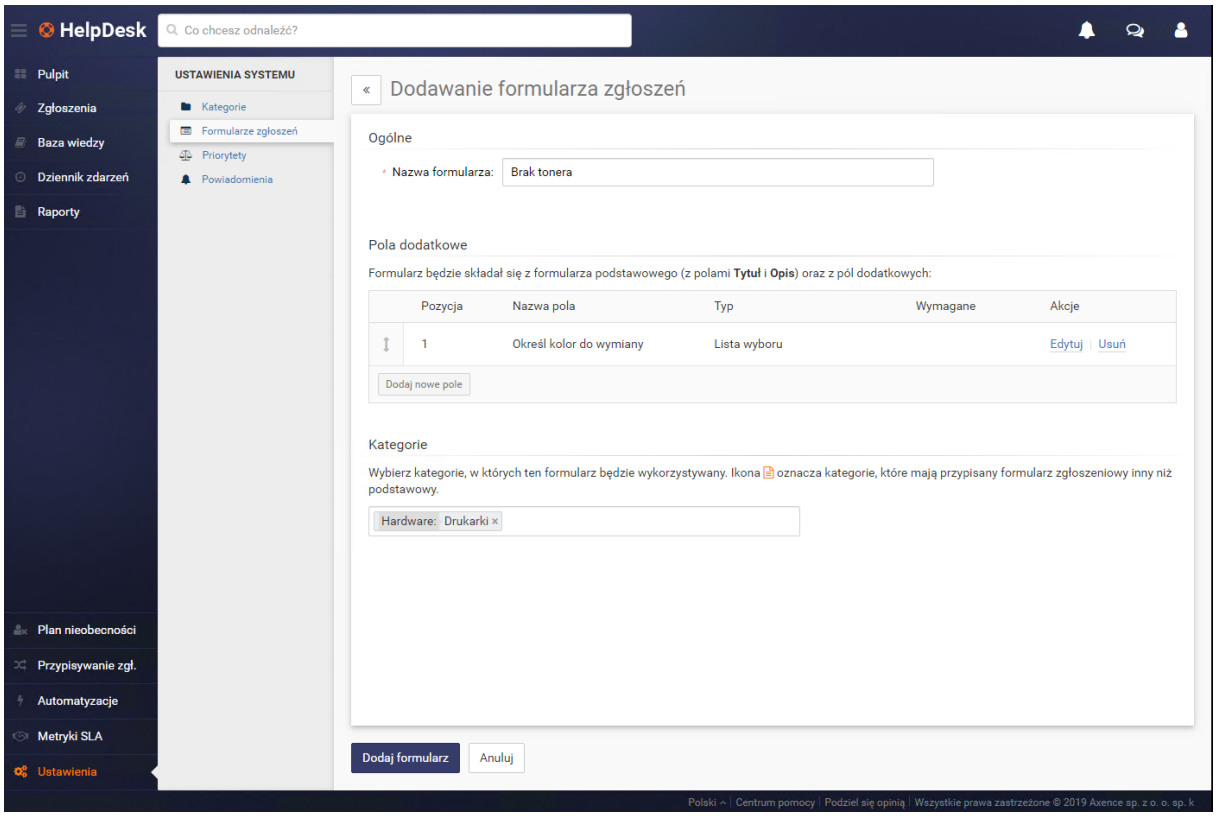
Pola dodatkowe mogą przyjmować różne typy:

- Pole tekstowe/liczbowe,
- Data,
- Lista wyboru (jednokrotnego lub wielokrotnego).

Możliwe jest również okreslenie wartosci domyslnej, podpowiedzi dla użytkownika lub wymaganie konkretnego pola w celu wysłania zgłoszenia.



4. Wybierz kategorie, w których ten formularz będzie wykorzystywany.



5. Kliknij **Dodaj formularz**, aby zakończyć dodawanie nowego formularza.

Aby edytować formularz zgłoszeń:

1. Przejdź do zakładki **Ustawienia | Formularze zgłoszeń**.
2. Wybierz opcję **Edytuj** dla formularza, który chcesz edytować.
3. Wpisz nową nazwę formularza oraz zmodyfikuj pola, które Cię interesują i kliknij **Zapisz zmiany**.

Aby usunąć formularz zgłoszeń:

1. Przejdź do zakładki **Ustawienia | Formularze zgłoszeń**.
2. Wybierz opcję **Usuń** dla formularza, który chcesz usunąć.
3. Potwierdź usunięcie danego formularza klikając **Usuń priorytet**.

10.3 Interfejs HelpDesk

10.3.1 Uruchamianie interfejsu HelpDesk

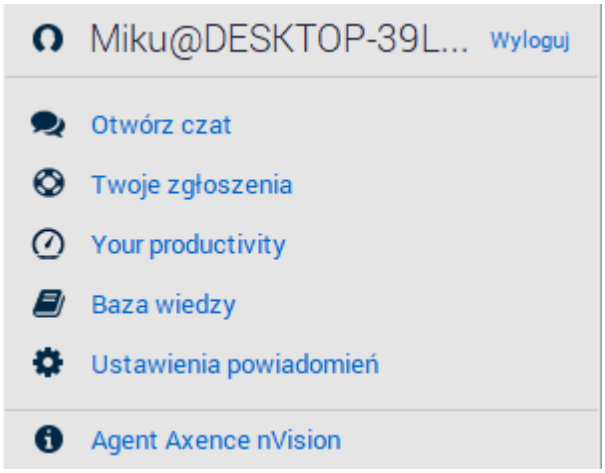
Interfejs HelpDesk można uruchomić na kilka sposobów:

W głównym oknie nVision

Kliknij w **HelpDesk**. W domyślnej przeglądarce zostanie otwarty interfejs HelpDesk.

Przez Agenta

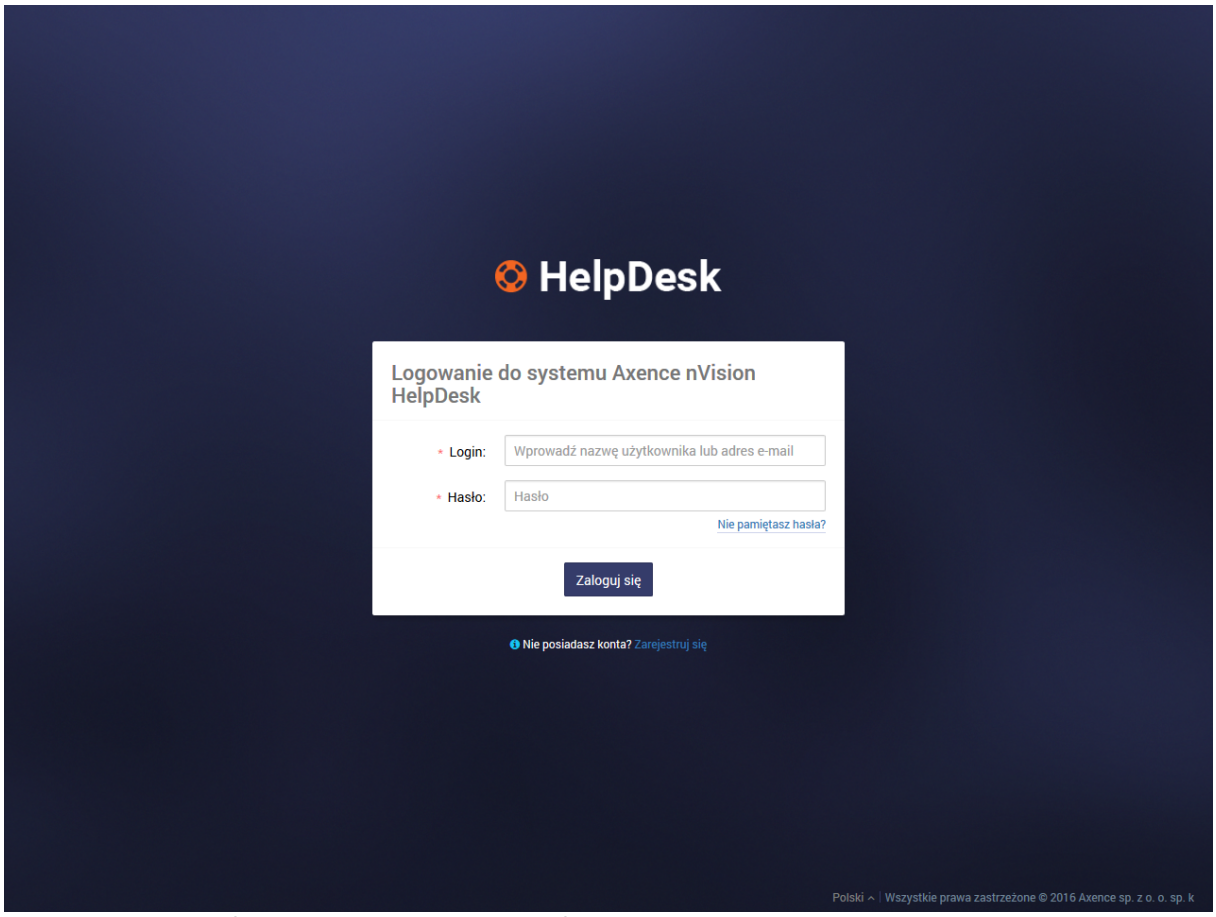
Kliknij prawym przyciskiem myszy na ikonie Agenta na pasku zadań. Zostanie otwarte menu podobne do prezentowanego poniżej. Wyświetlane opcje zależą od ustawień Agenta. Jeśli nie widzisz opcji dotyczących modułu HelpDesk, to znaczy, że należy włączyć HelpDesk w ustawieniach Agenta. Wybierz opcję **Zaloguj do HelpDesku**.



Menu ikony Agenta z zasobnika systemowego.

Bezpośrednio w przeglądarce

Wpisz lub skopiuj adres URL do systemu HelpDesk bezpośrednio w przeglądarce lub kliknij w link (przesłany np. mailem). Adres URL do HelpDesk można znaleźć rozwijając w głównym oknie nVision menu **Narzędzia \ Opcje \ Zdalny dostęp WWW**.



Widok formularza logowania do interfejsu HelpDesk w przeglądarce internetowej.

Powiązane tematy

- Zarządzanie i konfiguracja
- Ustawienia
- Rejestracja użytkownika
- Logowanie

10.3.2 Rejestracja użytkowników

Możliwe scenariusze rejestracji użytkownika

Konta użytkowników typu Administrator i pomoc techniczna HelpDesk mogą być zakładane tylko przez Administratora (również poprzez synchronizację z Active Directory). W przypadku samodzielnej rejestracji przez użytkownika możliwe jest utworzenie wyłącznie konta użytkownika końcowego. Typ konta może być później zmodyfikowany przez Administratora we właściwościach konta).

Przez Administratora

Aby założyć konto użytkownika (wszystkie typy):

1. W głównym oknie nVision przejdź do okna **Użytkownicy**.

2. W zakładce Użytkownicy kliknij w przycisk **Dodaj użytkownika**.
3. Podaj nazwę i hasło dla dodawanego użytkownika.
4. Określ **Rolę** użytkownika (Użytkownik, HelpDesk, Administrator).
5. Ustaw konto jako **włączone**.
6. Możesz uzupełnić szczegóły użytkownika (e-mail, imię i nazwisko), a także inne uprawnienia w zależności od zdefiniowanego typu użytkownika.

Samodzielnie przez użytkowników, aktywacja przez Administratora

Konfiguracja:

1. W głównym oknie nVision rozwiń menu przy przycisku **HelpDesk**, wejdź w opcje **Konfiguracja | Kluczowe ustawienia**.
2. Zaznacz pole **Samodzielne zakładanie konta**.
3. W polu **Tryb aktywacji konta** wybierz opcję **Ręczna aktywacja przez administratora**.

Aby założyć konto użytkownika:

1. Uruchom interfejs HelpDesk. Jeżeli użytkownik nie jest zalogowany, pojawi się okno logowania do interfejsu HelpDesk.
2. Kliknij w przycisk **Zarejestruj się**.
3. W oknie rejestracji użytkownika podaj swój **Adres e-mail**, będący także loginem do interfejsu.
4. Podaj **Hasło** oraz **Imię i nazwisko**.
5. Kliknij w przycisk **Zarejestruj**.
6. Logowanie się do systemu będzie możliwe, gdy administrator aktywuje nowe utworzone konto.

Samodzielnie przez użytkowników, aktywacja przez e-mail

Konfiguracja:

1. W głównym oknie nVision rozwiń menu przy przycisku **HelpDesk**, wejdź w opcje **Konfiguracja | Kluczowe ustawienia**.
2. Zaznacz pole **Samodzielne zakładanie konta**.
3. W polu **Tryb aktywacji konta** wybierz opcję **Wysłanie e-maila aktywacyjnego**.

Aby założyć konto użytkownika:

1. Uruchom interfejs HelpDesk. Jeżeli użytkownik nie jest zalogowany, pojawi się okno logowania do interfejsu HelpDesk.
2. Kliknij w przycisk **Zarejestruj się**.
3. W oknie rejestracji użytkownika podaj swój **Adres e-mail**, będący także loginem do interfejsu.
4. Podaj **Hasło** oraz **Imię i nazwisko**.
5. Kliknij w przycisk **Zarejestruj**.

6. Na podany adres e-mail zostanie wysłany e-mail aktywacyjny. Aby ukończyć proces rejestracji, kliknij w link podany w e-mailu. Możesz teraz zalogować się do interfejsu HelpDesk.

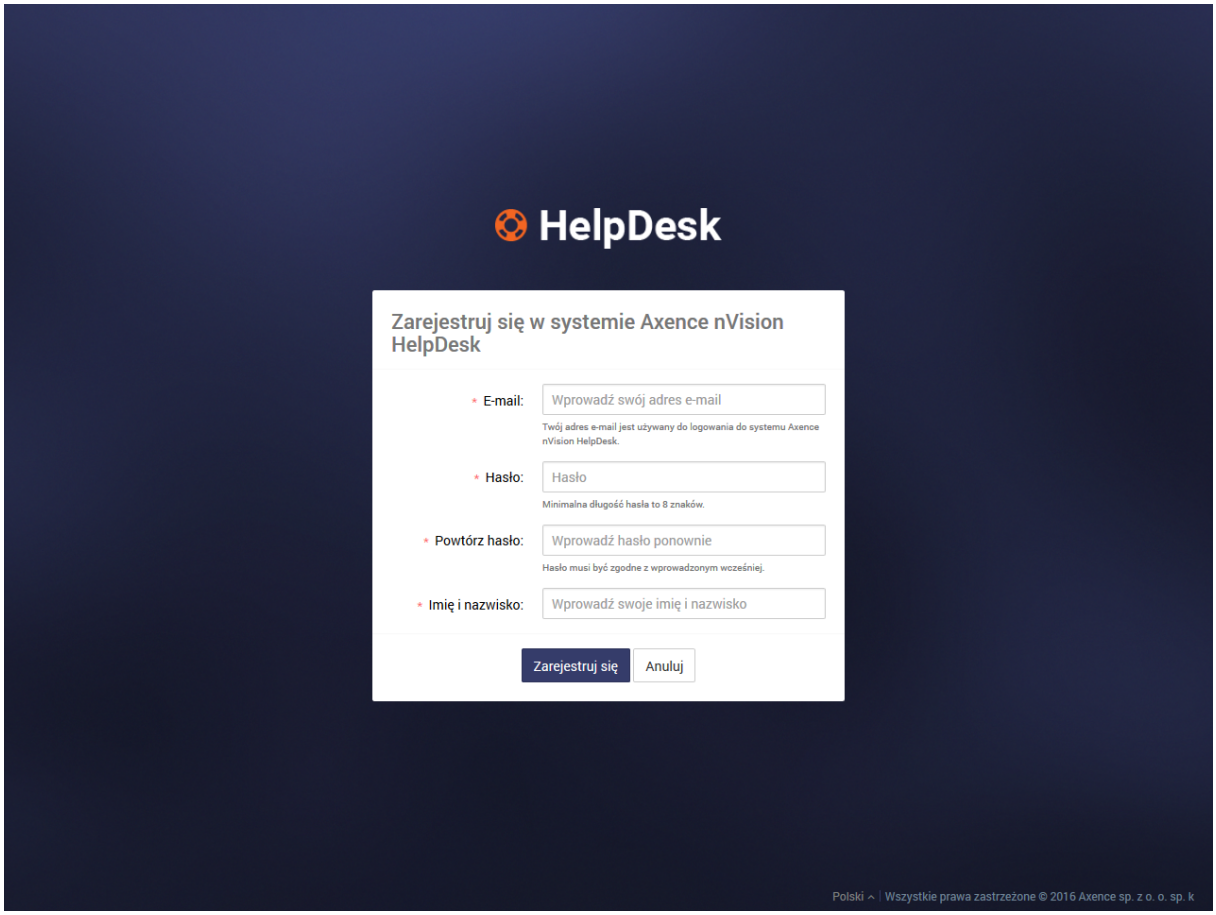
Samodzielnie przez użytkowników, bez aktywacji konta

Konfiguracja:

1. W głównym oknie nVision rozwiń menu przy przycisku **HelpDesk**, wejdź w opcje **Konfiguracja | Kluczowe ustawienia**.
2. Zaznacz pole **Samodzielne zakładanie konta**.
3. W polu **Tryb aktywacji konta** wybierz opcję **Brak**.

Aby założyć konto użytkownika:

1. Uruchom interfejs HelpDesk. Jeżeli użytkownik nie jest zalogowany, pojawi się okno logowania do interfejsu HelpDesk.
2. Kliknij w przycisk **Zarejestruj się**.
3. W oknie rejestracji użytkownika podaj swój **Adres e-mail**, będący także loginem do interfejsu.
4. Podaj **Hasło** oraz **Imię i nazwisko**.
5. Kliknij w przycisk **Zarejestruj**.
6. Po potwierdzeniu poprawności danych (unikalność adresu e-mail oraz długość hasła przynajmniej 8 znaków) zostanie wyświetlony komunikat o zakończeniu rejestracji. Możesz teraz zalogować się do interfejsu HelpDesk.



Formularz samodzielnej rejestracji konta przez użytkownika.

Powiązane tematy

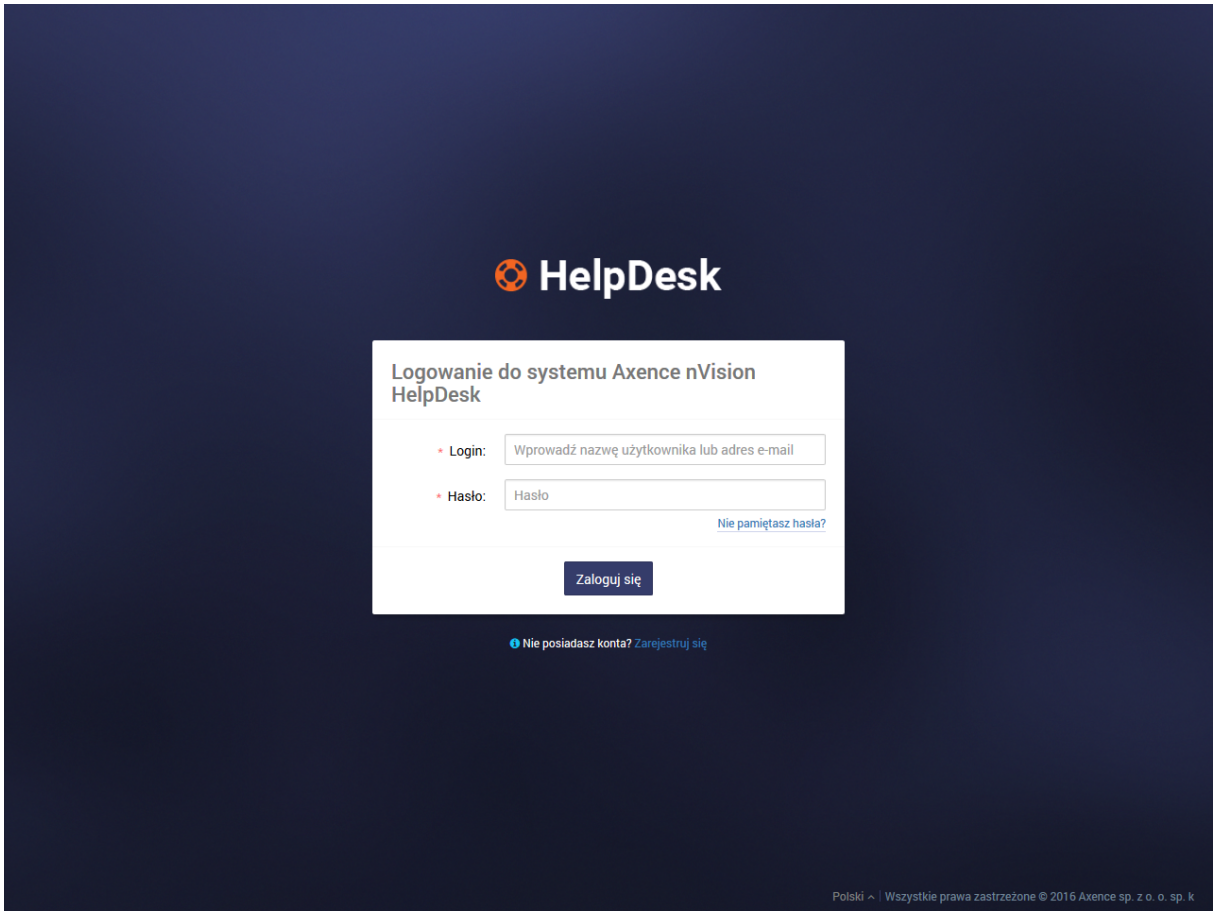
- Uruchamianie interfejsu HelpDesk
- Zarządzanie użytkownikami
- Ustawienia HelpDesk

10.3.3 Logowanie

Logowanie

Aby zalogować się do interfejsu HelpDesk:

1. Uruchom interfejs HelpDesk.
2. Podaj **login** (nazwę użytkownika lub adres e-mail) i **hasło**. (W przypadku wejścia do HelpDesku przez Agenta następuje próba autologowania.)
3. Kliknij w przycisk **Zaloguj**. Jeśli podane dane były poprawne, możesz rozpocząć korzystanie z interfejsu HelpDesk.



Widok formularza logowania do interfejsu HelpDesk.

Wylogowanie

Aby wylogować się z interfejsu HelpDesk:

1. Kliknij w awatar w strefie użytkownika znajdującej się w prawym górnym rogu interfejsu HelpDesk.
2. Z menu kontekstowego wybierz opcję **Wyloguj**.

Powiązane tematy

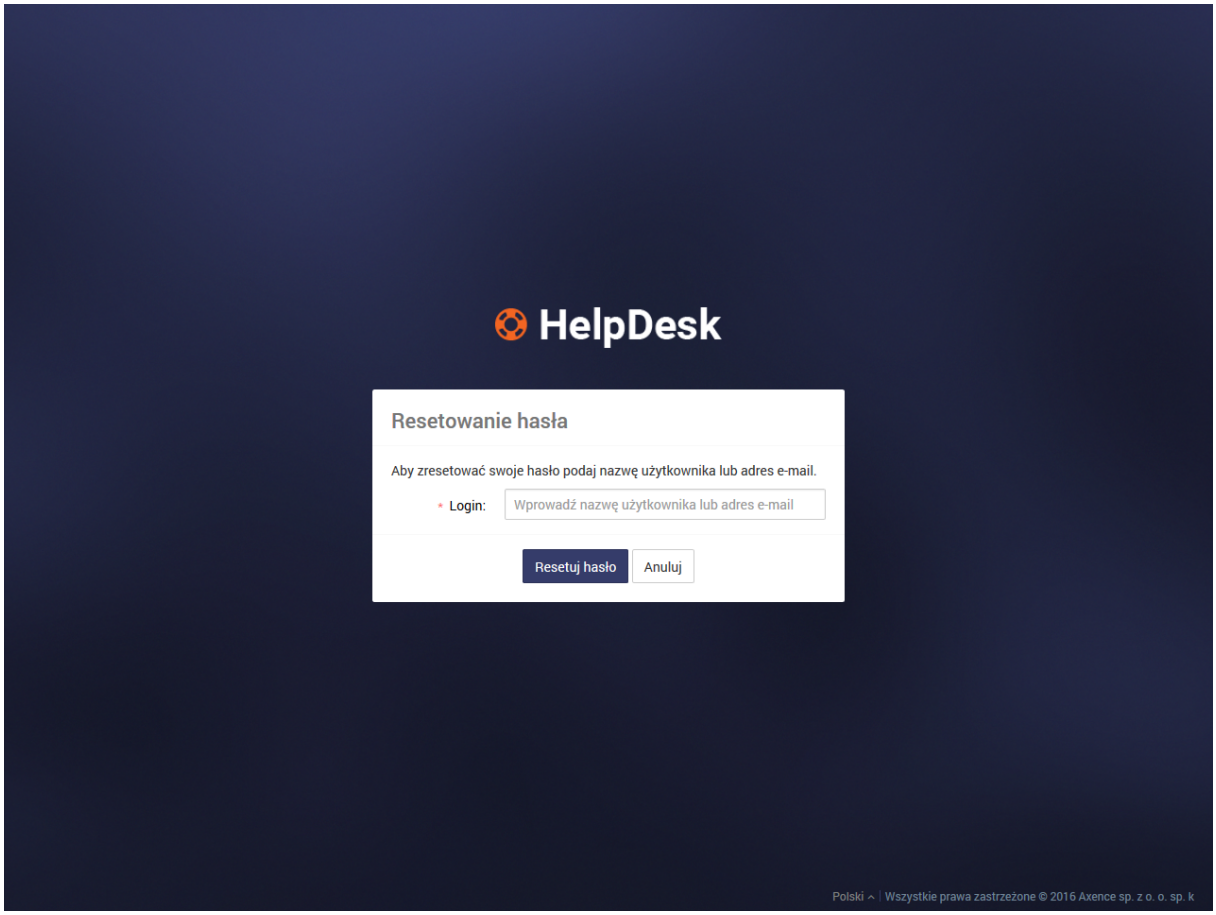
- Uruchamianie interfejsu HelpDesk
- Rejestracja użytkownika
- Resetowanie hasła

10.3.4 Resetowanie hasła

W przypadku zapomnienia hasła:

1. Uruchom interfejs HelpDesk i kliknij w łącze **Resetuj hasło**.
2. Aby zresetować hasło podaj nazwę użytkownika lub adres e-mail, którego używasz do logowania się do interfejsu HelpDesk.

3. Kliknij w przycisk **Resetuj hasło**. Jeżeli wprowadzone dane są poprawne, na adres e-mail zostanie wysłana wiadomość z instrukcjami. W przeciwnym razie postępuj zgodnie z instrukcjami wyświetlonymi na ekranie.
4. Przejdź do skrzynki mailowej i w wiadomości otrzymanej od HelpDesk kliknij w link resetujący hasło.
5. Podaj nowe hasło i **Zapisz ustawienia**. Teraz możesz zalogować się na swoje konto używając nowego hasła.



Formularz resetowania hasła.

Powiązane tematy

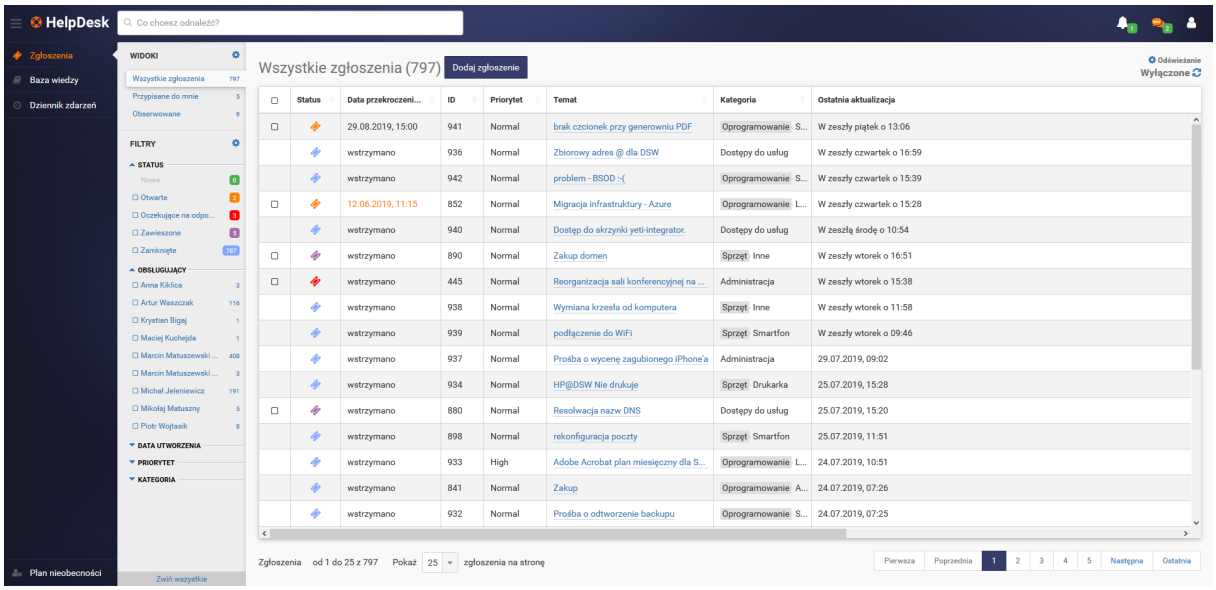
Uruchamianie interfejsu HelpDesk

Rejestracja użytkownika

Logowanie

10.3.5 Widoki główne

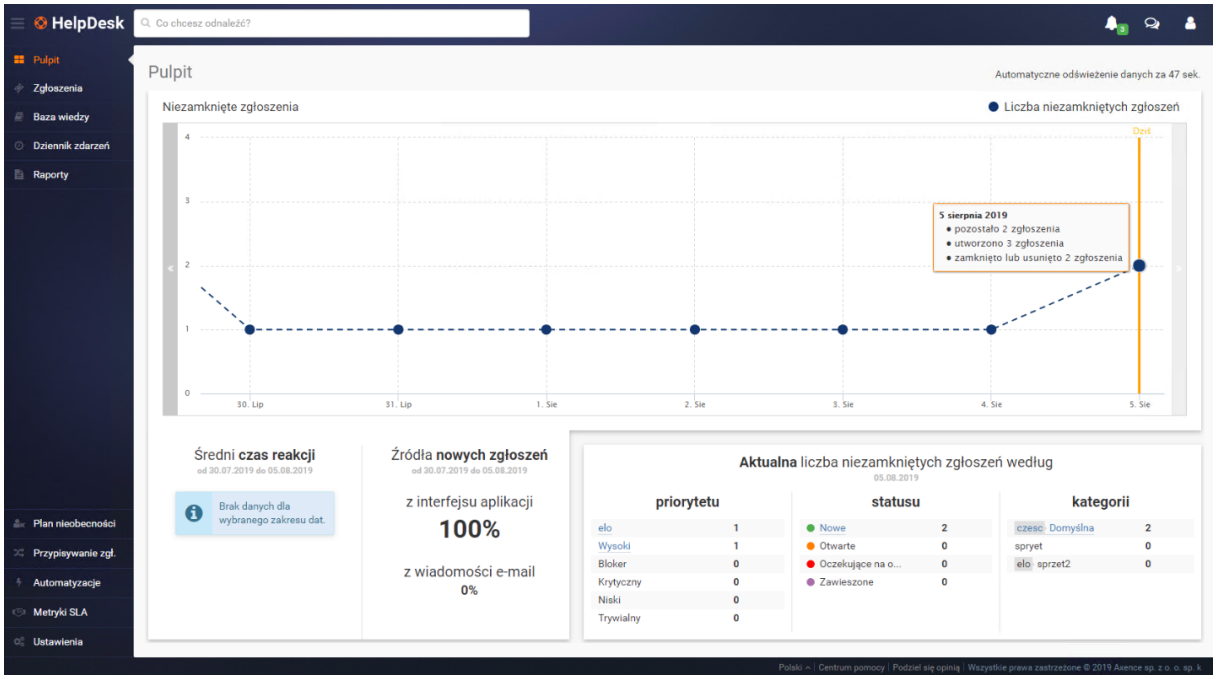
Widoki główne programu to dziesięć widoków, do których można przejść korzystając z nawigacji głównej zlokalizowanej po lewej stronie interfejsu:



Widok listy zgłoszeń ze rozwiniętą nawigacją.

- Pulpit

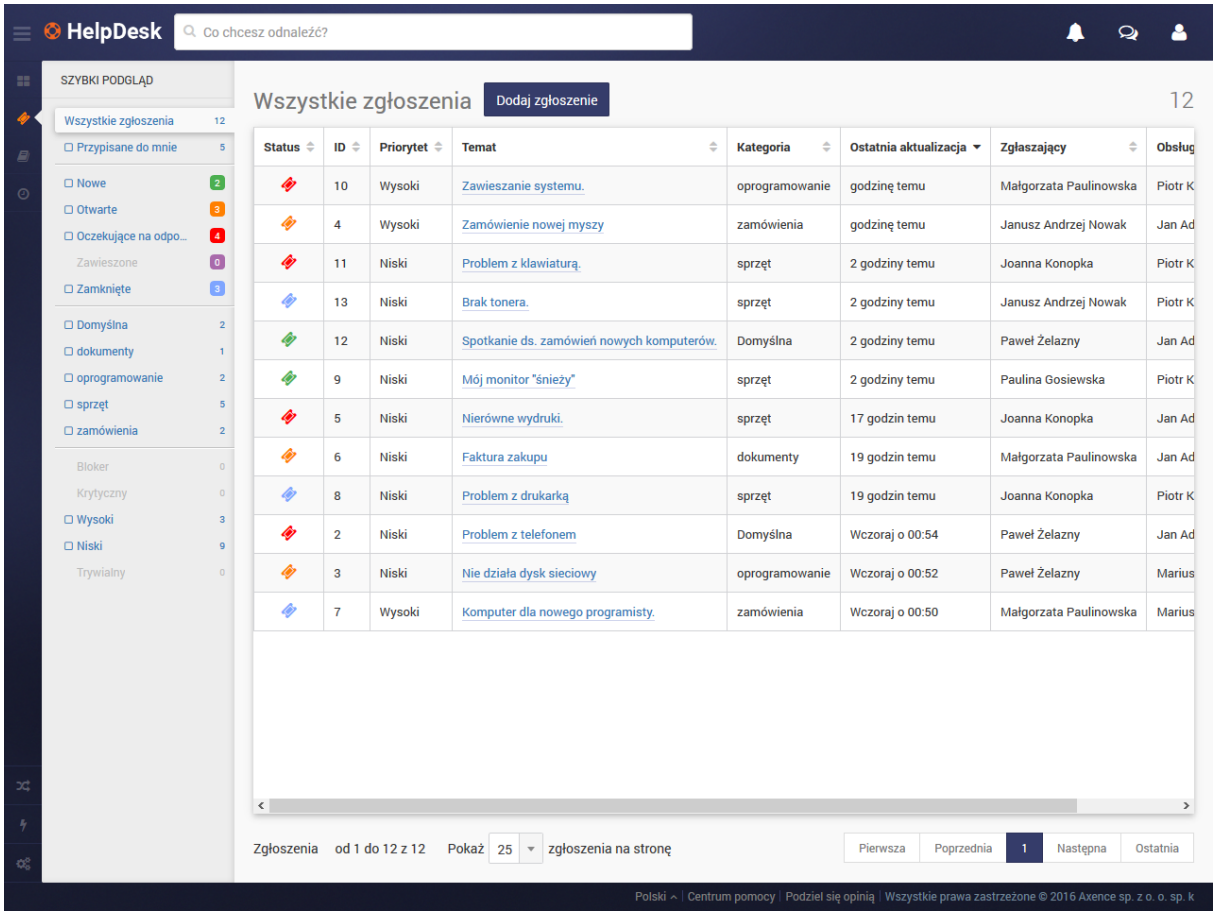
Pulpit, zawiera podstawowe statystki dotyczące przetwarzanych zgłoszeń takie jak: średni czas reakcji, informacje o źródłach nowych zgłoszeń, liczbę zgłoszeń z podziałem według priorytetu / statusu / kategorii. Prezentowany jest również wykres, na któym przedstawionea jest liczba zgłoszeń w statusie innymi, niż "zamknięty".



Pulpit. Domyślny widok po zalogowaniu administratora do interfejsu HelpDesk.

- Zgłoszenia
- Baza wiedzy
- Dziennik zdarzeń
- Raporty

- Przypisywanie zgłoszeń
- Automatyzacje
- Metryki SLA
- Ustawienia (Kategorie, Priorytety)



Widok listy zgłoszeń ze zwiniętą nawigacją.

Po rozwinięciu danego widoku pojawia się kolumna szybkiego podglądu. Opcje szybkiego podglądu różnią się w zależności od tego, która z pozycji została wybrana w nawigacji głównej (zgłoszenia, artykuły, etc.). Korzystanie z opcji szybkiego podglądu pozwala na prosty i szybki dostęp do różnych wątków zgłoszeń, typów artykułów i innych.

Tytuły stron ustawiane są dynamicznie, w zależności od wybranych opcji widoku.

Powiązane tematy

- Zgłoszenia - wprowadzenie
- Baza wiedzy - wprowadzenie
- Lista aktywności
- Automatyzacje
- Strefa użytkownika

Wyszukiwanie

Feedback (podziel się opinią)

10.3.6 Edytor tekstu

Wbudowany edytor tekstu pozwala na formatowanie wprowadzonej treści artykułów i zgłoszeń.

Podstawowe funkcje (dodawanie/edycja artykułów i zgłoszeń)

Funkcja	Opis
B	Styl pogrubiony.
I	Styl kursywa.
U	Styl podkreślenia.
T	Styl tekstu (do wyboru: Mały, Normalny, Duży, Bardzo duży).
A	Kolor tekstu (do wyboru po rozwinięciu menu przy przycisku).
	Osadzenie linku w treści. Po kliknięciu w ikonę wpisz w oknie dialogowym adres URL, do którego ma prowadzić link, oraz wyświetlany tekst linku.
	Styl dla numerowania listy.
	Styl dla punktowania listy.
	Cofnij / ponów zmiany.
	Usuń formatowanie.
	Styl wyrównania (do wyboru: do lewej, do środka, do prawej).
</>	Przełącz między HTML/Rich text.

Wgrywanie obrazu (dodawanie/edycja artykułów)

Aby wgrać do artykułu obraz:

1. W widoku dodawania lub edytowania artykułu kliknij w przycisk **Prześlij obrazek**.
2. W oknie dialogowym wybierz obraz, który ma zostać dodany.
3. Możesz dodać tytuł obrazu i alternatywny tekst wyświetlany w miejscu obrazu w razie gdyby niemożliwe było jego wyświetlenie.
4. Wybierz styl wyrównania obrazu (domyślnie: do lewej).
5. Kliknij w przycisk **Wstaw obrazek**.

Dodawanie zewnętrznego filmu (dodawanie/edycja artykułów)

Aby dodać do artykułu zewnętrzny film:

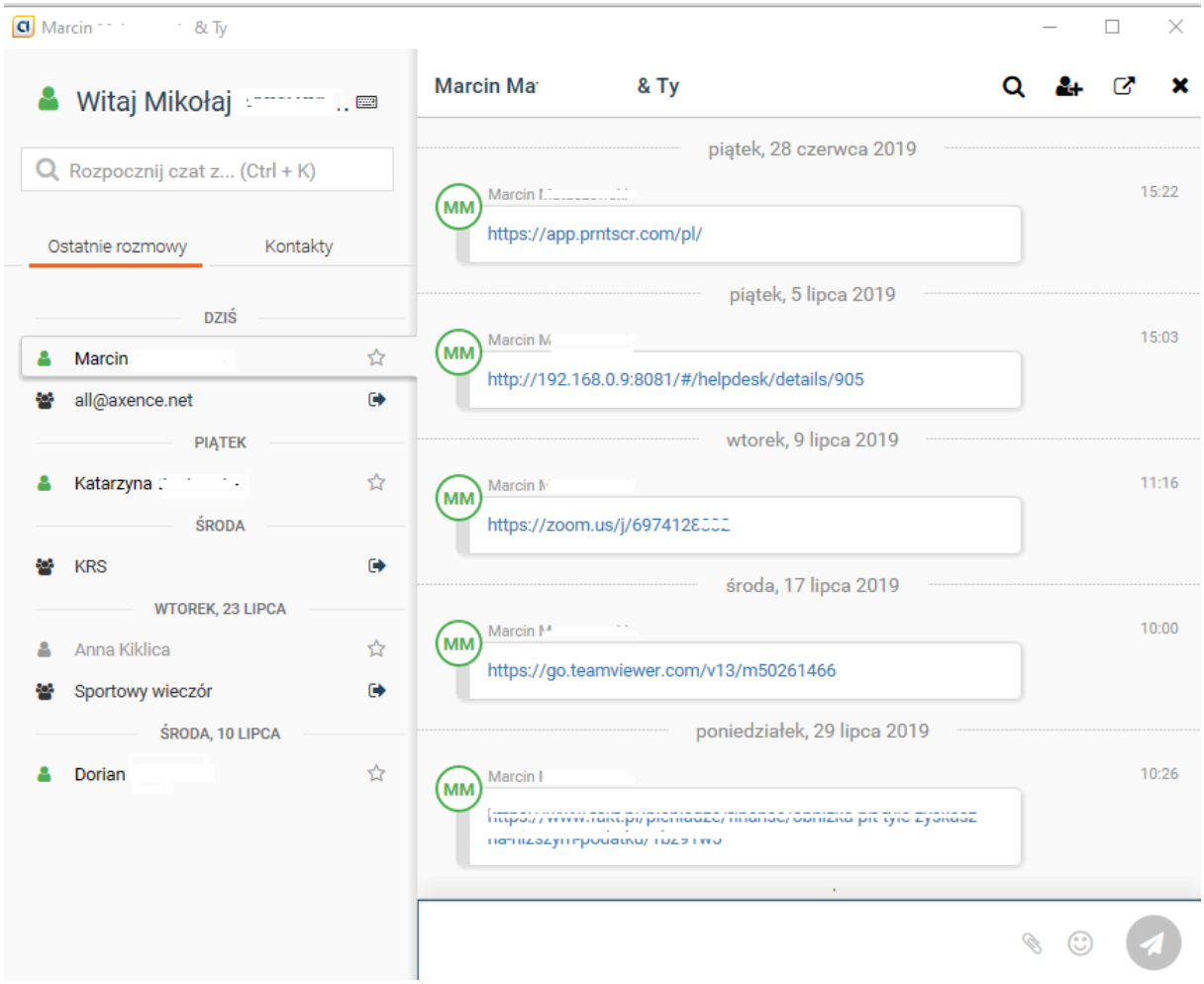
1. W widoku dodawania lub edytowania artykułu kliknij w przycisk **Wstaw film**.
2. W oknie dialogowym podaj link do filmu.
3. Wybierz styl wyrównania filmu (domyślnie: wyśrodkuj).
4. Kliknij w przycisk **Wstaw film**.

Powiązane tematy

- Dodawanie zgłoszenia
- Dodawanie komentarza
- Dodawanie artykułu
- Edytowanie artykułu

10.3.7 Czat

Rozmowy na czacie mogą być rozpoczynane i odbierane zarówno przez moduł HelpDesk w przeglądarce jak i przy pomocy Agenta. Funkcjonalność jest taka sama w obu przypadkach. Rozmowa może być prowadzona pomiędzy użytkownikami, którzy figurują na liście w oknie **Użytkownicy** (patrz Zarządzanie użytkownikami).



Widok czatu.

Użytkownicy czatu

Po kliknięciu w przycisk **Czat** (zarówno w przeglądarce jak i w opcjach Agenta), wyświetlane jest okno z trzema grupami użytkowników:

Grupa	Opis
Ulubione	Osoby dodane do listy ulubionych znajomych, czyli oznaczone gwiazdką ⭐.
Pomoc Techniczna	Użytkownicy typu HelpDesk i Administrator (patrz Zarządzanie użytkownikami).
Inni użytkownicy	Pozostali użytkownicy końcowi.

Aby dodać użytkownika do znajomych kliknij w gwiazdkę znajdującą się po prawej stronie nazwy użytkownika. Od tej pory będzie on wyświetlany także w grupie ulubionych. Aby usunąć użytkownika z listy znajomych ponownie kliknij w gwiazdkę.

Nawiązywanie rozmowy z poziomu interfejsu HelpDesk

Aby skorzystać z czatu:

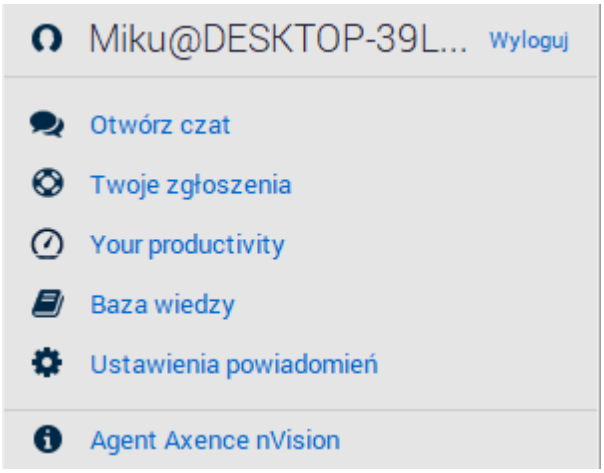
1. Zaloguj się do interfejsu HelpDesk.
2. W interfejsie HelpDesk kliknij w przycisk  znajdujący się w prawej górnej części okna. Zostanie otwarte okno czatu. Użytkownicy aktualnie zalogowani do HelpDesk są oznaczeni zielonym kolorem, a niezalogowani - szarym.
3. Kliknij w nazwę użytkownika, z którym chcesz rozmawiać.
4. Wpisz wiadomość i wciśnij Enter. Jeśli rozmówca jest zalogowany (kolor zielony na liście użytkowników), to otworzy się u niego okno czatu z przesłaną wiadomością.

Czat z twórcą zgłoszenia oraz z osobą za to zgłoszenie odpowiedzialną można również rozpocząć z poziomu danego zgłoszenia, klikając w metryce zgłoszenia ikonę znajdującą się po prawej stronie pola z nazwą odpowiedniego użytkownika.

Nawiązywanie rozmowy z poziomu Agenta

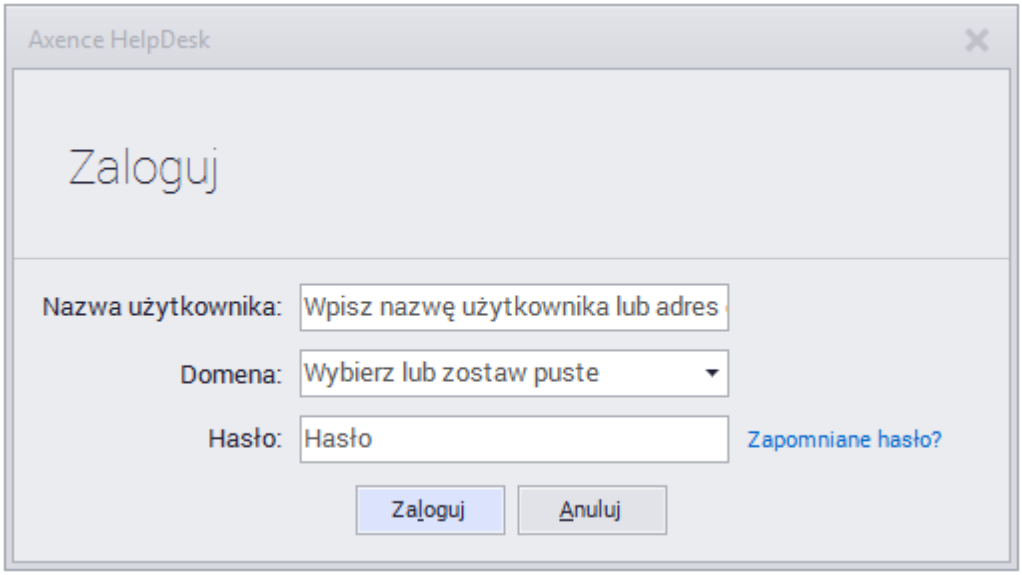
Inicjowanie rozmowy:

1. Kliknij prawym przyciskiem myszy na ikonie Agenta na pasku zadań. Zostanie otwarte menu podobne do prezentowanego poniżej. Wyświetlane opcje zależą od ustawień Agenta. Jeśli nie widzisz opcji dotyczących modułu HelpDesk i czatu, włącz HelpDesk w ustawieniach Agenta.



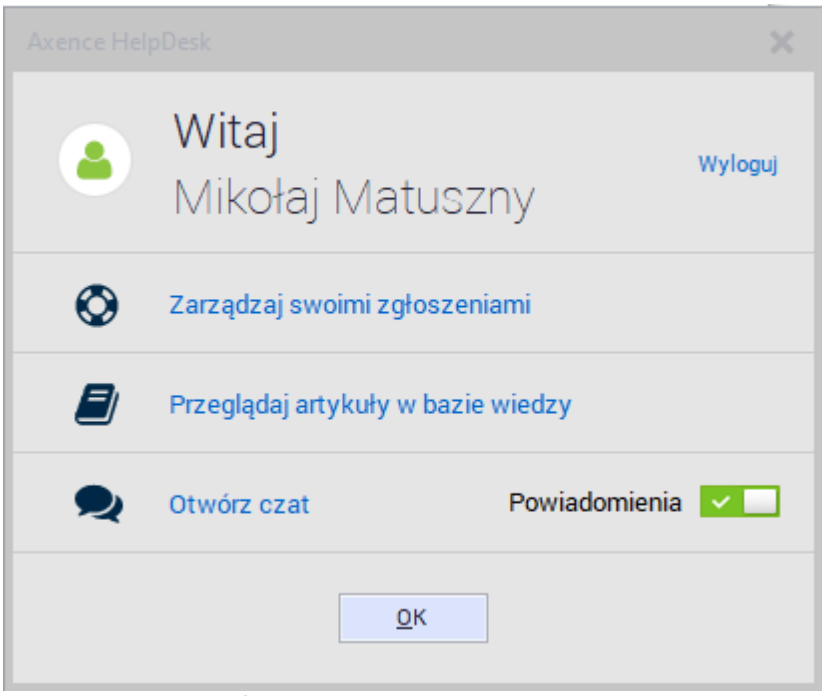
Menu ikony Agenta z zasobnika systemowego.

2. Wybierz opcję **logowania** i podaj swoje dane logowania do modułu HelpDesk.



Logowanie do HelpDesku z poziomu ikony Agenta.

3. W oknie opcji Agenta wybierz opcję **czatu.**



Opcje dostępne z ikony Agenta.

4. Zostanie otwarte okno czatu. Z poziomu tego okna można rozpocząć rozmowę z innym użytkownikiem.

Odbieranie rozmowy

Odbieranie rozmowy - możliwe scenariusze:

- Jeśli masz otwarte okno czatu z listą użytkowników, to otrzymanie wiadomości skutkuje otwarciem okna rozmowy z użytkownikiem, który wysłał tę wiadomość.

- Jeśli okno jest zamknięte, ale zalogowano się z Agenta do HelpDesk, to po otrzymaniu wiadomości pojawi się informacja o otrzymaniu wiadomości.
- Jeśli nie zalogowano się do HelpDesk, to wiadomość zostanie wyświetlona po najbliższym logowaniu.

Tworzenie rozmowy grupowej

Aby utworzyć rozmowę grupową kliknij link **Utwórz nową grupę czatu** na liście kontaktów.

W trakcie rozmowy prywatnej można utworzyć rozmowę grupową poprzez kliknięcie ikony dodania rozmówcy  w górnej części okna rozmowy.

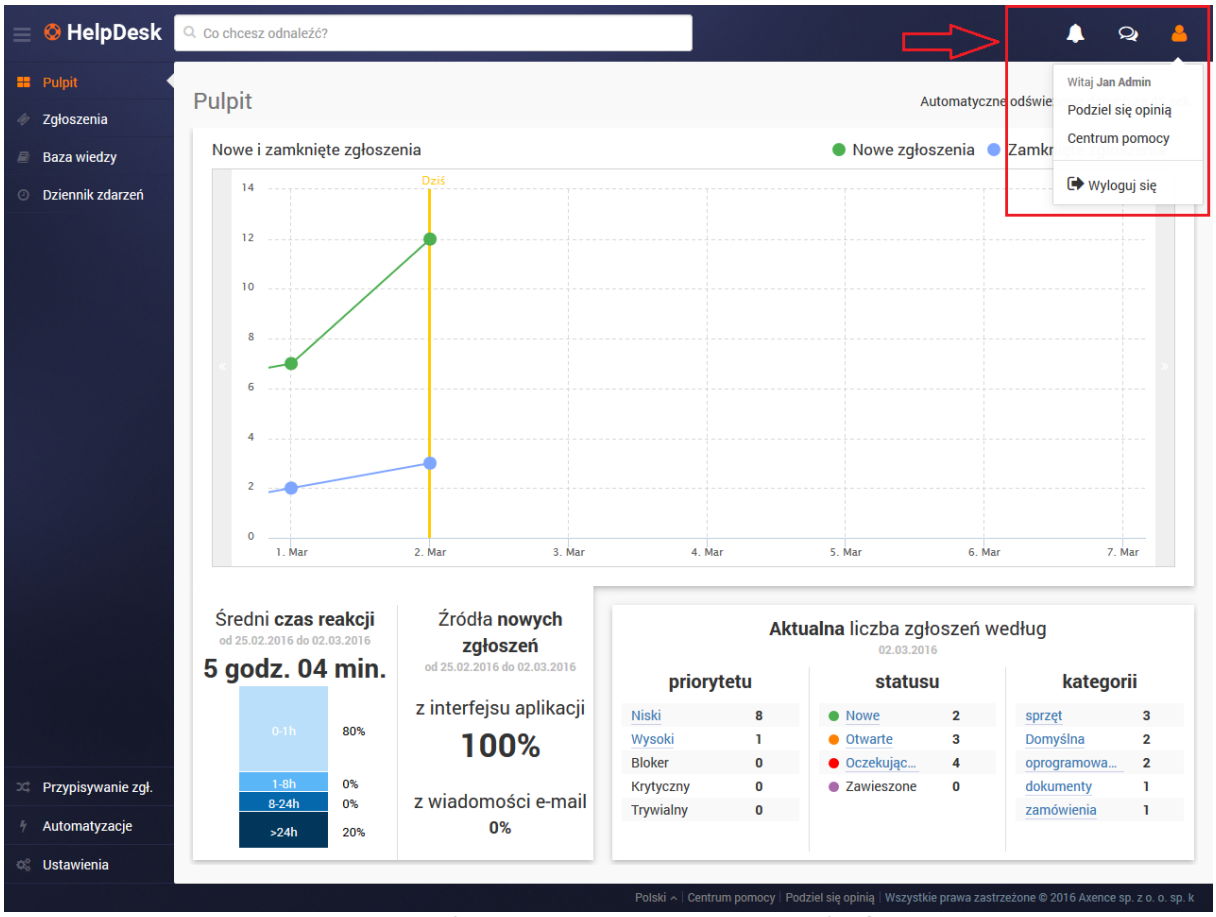
Przesyłanie załączników

Aby przesłać załącznik, kliknij ikonę załącznika  w polu wpisywania wiadomości.

Przesyłanie załączników jest funkcją eksperymentalną i nie działa w rozmowach grupowych.

10.3.8 Strefa użytkownika

Strefa użytkownika to obszar w prawym górnym rogu interfejsu HelpDesk. Znajduje się tu uniwersalny awatar użytkownika oraz dodatkowe informacje i akcje, które może wykonać zalogowany użytkownik.



Widok pulpitu w interfejsie HelpDesk z zaznaczoną strefą użytkownika.

Ikona	Opis
	Kliknięcie w awatar spowoduje rozwinięcie menu kontekstowego z następującymi opcjami (zależnymi od typu użytkownika): • Podziel się opinią *(Administrator i pracownik HelpDesku)* • Centrum pomocy *(Administrator i pracownik HelpDesku)* • *Zmień hasło* • Wyloguj
	Kliknięcie w ikonę spowoduje otwarcie czatu.
	Na ikonie wyświetlana jest liczba nowych powiadomień dotyczących zmian w zgłoszeniach. Kliknięcie w ikonę spowoduje wyświetlenie nowych powiadomień. *(Administrator i pracownik HelpDesku)*

Powiązane tematy

Uruchamianie interfejsu HelpDesk

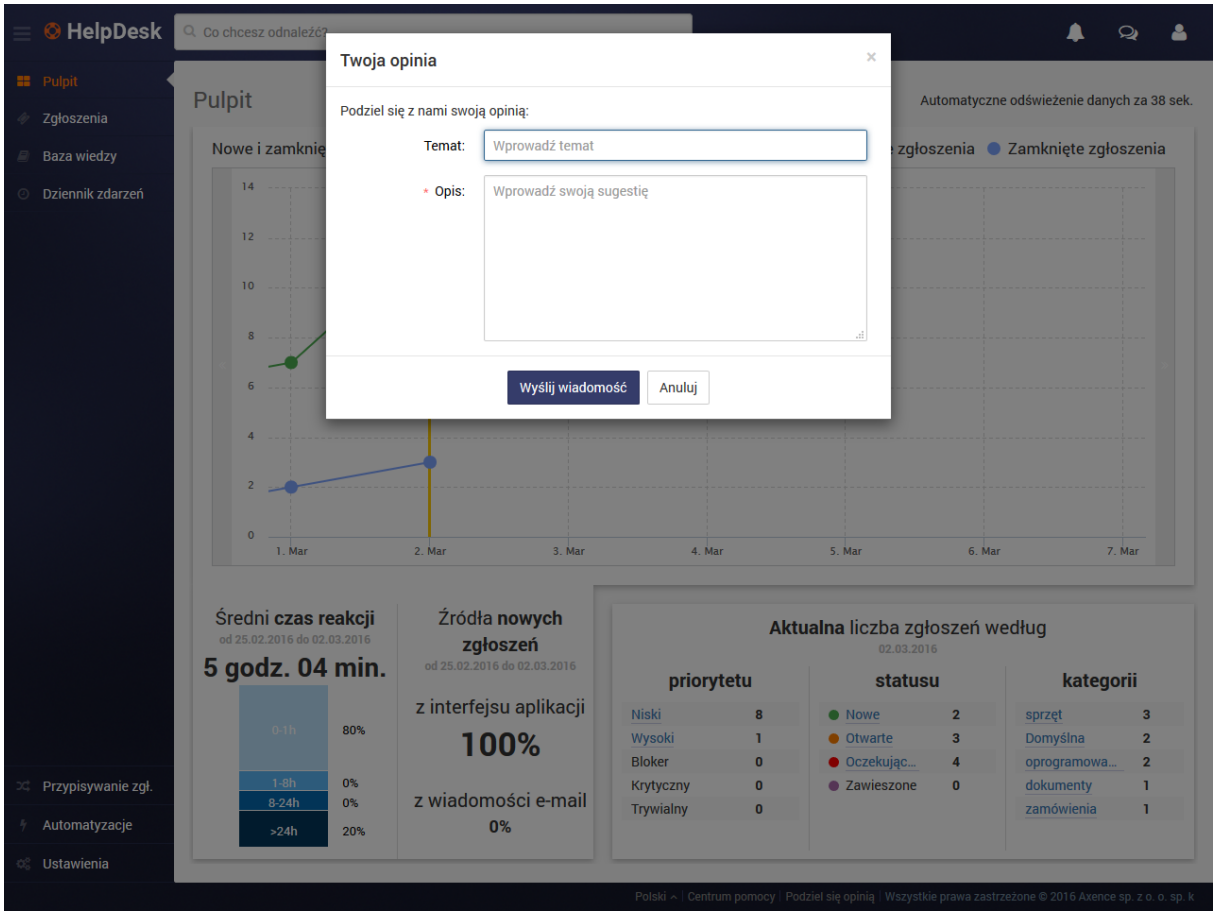
Widoki główne

10.3.9 Feedback (podziel się opinią)

W trosce o poprawny rozwój aplikacji umożliwiamy naszym użytkownikom raportowanie błędów i dzielenie się z nami opinią.

Aby podzielić się z nami opinią:

1. Kliknij w przycisk **Podziel się z nami opinią** znajdujący się w dolnej części okna interfejsu HelpDesk.
2. W oknie dialogowym podaj **Temat** i **Treść** wiadomości, którą chcesz przesłać do Axence, a także swój adres e-mail.
3. Kliknij w przycisk **Wyślij wiadomość**.



Formularz zgłaszania opinii.

Powiązane tematy

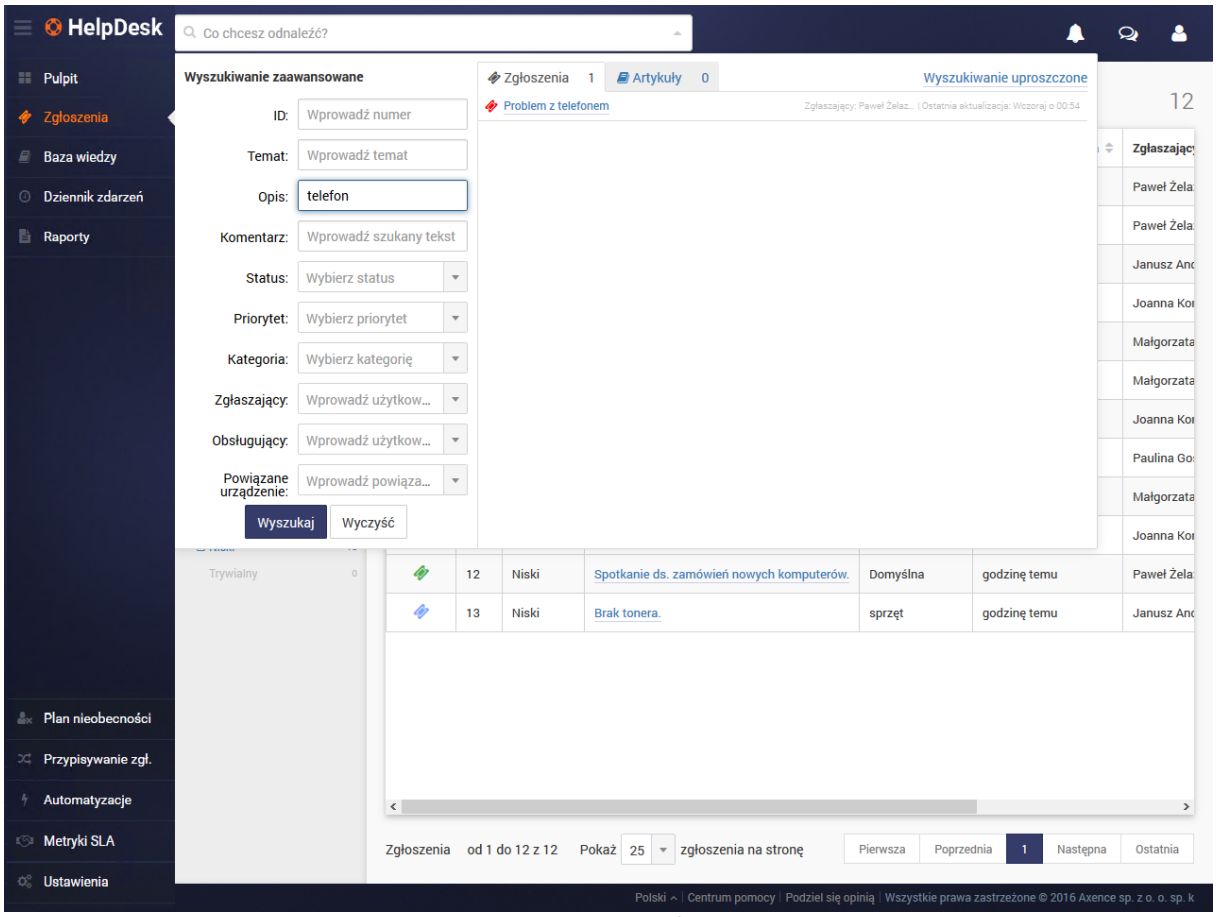
Uruchamianie interfejsu HelpDesk

Widoki główne

10.3.10 Wyszukiwanie

Pole wyszukiwania w interfejsie HelpDesk znajduje się w górnej części okna.

Wyszukiwanie odbywa się w pierwszej kolejności w tym widoku, który jest aktualnie otwarty. Zasięg wyszukiwania zależy od roli użytkownika. Wyniki wyszukiwania są wyświetlane na bieżąco.



Widok wyszukiwarki w interfejsie HelpDesk.

Wyszukiwanie zaawansowane

Aby skorzystać z wyszukiwania zaawansowanego należy wprowadzić wyszukiwaną frazę a następnie w widoku listy wyników kliknąć link **Wyszukiwanie zaawansowane.** W widoku zaawansowanym poza przeszukiwanym obszarem systemu (Lista Zgłoszeń / Baza Wiedzy) określić można dodatkowe parametry:

- numer zgłoszenia (ID),
- temat,
- opis,
- komentarz (treść artykułu w przypadku wybrania przeszukiwania Bazy Wiedzy),
- status,
- priorytet,
- kategoria,
- osoba zgłaszająca,
- osoba obsługująca,
- powiązane urządzenie,

które zawężą listę wyników wyszukiwania.

Powiązane tematy

Widoki główne

Strefa użytkownika

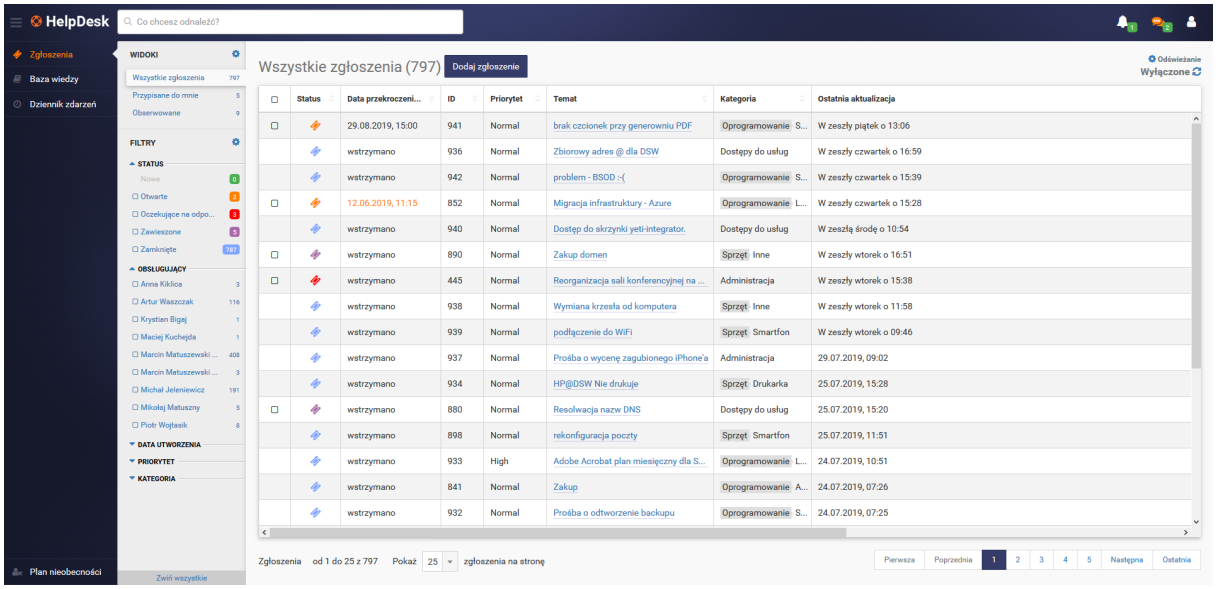
Zarządzanie użytkownikami

10.4 Zgłoszenia

10.4.1 Zgłoszenia - wprowadzenie

Baza zgłoszeń umożliwia użytkownikom zgłaszać problemy techniczne w interfejsie HelpDesk oraz przez e-mail. Przychodzące zgłoszenia są przetwarzane i przyporządkowywane odpowiednim pracownikom pomocy HelpDesk, którzy otrzymują powiadomienia o przypisanych im problemach do rozwiązania.

Każde zgłoszenie przypisane jest do określonej kategorii i ma zdefiniowany priorytet. Zarządzanie zgłoszeniami i przetwarzanie ich jest proste dzięki mechanizmowi statusów opisujących cykl życia zgłoszenia.



Widok listy zgłoszeń.

Statusy zgłoszeń:

Nowe - zgłoszenie zostało zrejestrowane w systemie, nie została wykonana żadna akcja przez użytkownika.

Otwarte - zgłoszenie oczekuje na reakcję pracowników helpdesku.

Oczekujące na odpowiedź - zgłoszenie oczekuje na reakcję osoby zgłaszającej.

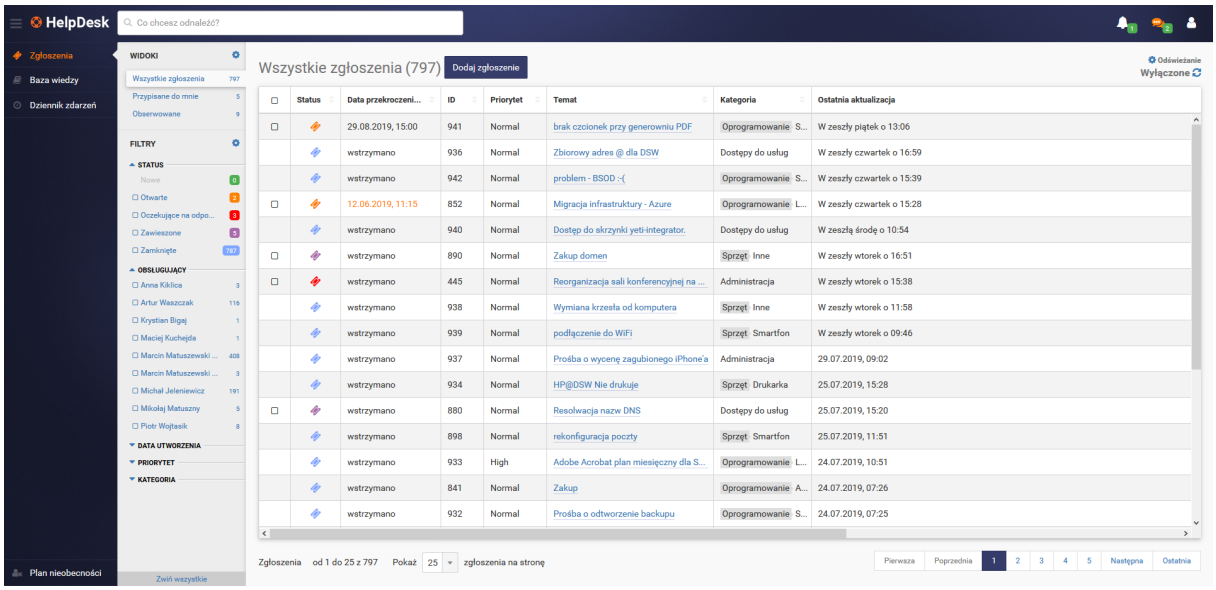
Zawieszone - zgłoszenie zostało zawieszone (np. problem wymaga eskalacji do zewnętrznego dostawcy).

Zamknięte - zgłoszenie zostało zamknięte przez pracownika helpdesku. Zamknięte zgłoszenia nie mogą zostać usunięte z systemu.

Powiązane tematy

10.4.2 Lista zgłoszeń

Lista zgłoszeń to jeden z głównych widoków interfejsu HelpDesk. Przedstawia on informacje o zgłoszeniach nadesłanych do systemu HelpDesk.



Widok listy zgłoszeń.

W lewej części ekranu znajduje się nawigacja główna (patrz Widoki główne) oraz kolumna szybkiego widoku. Szybki widok pozwala na szybkie przejście do zbioru danych z określonego obszaru zainteresowań. Przykładowo, wyświetlane mogą być nowe zgłoszenia o najwyższym priorytecie, które dodatkowo należą do jednej z dwóch wybranych kategorii.

Tabela z listą zgłoszeń

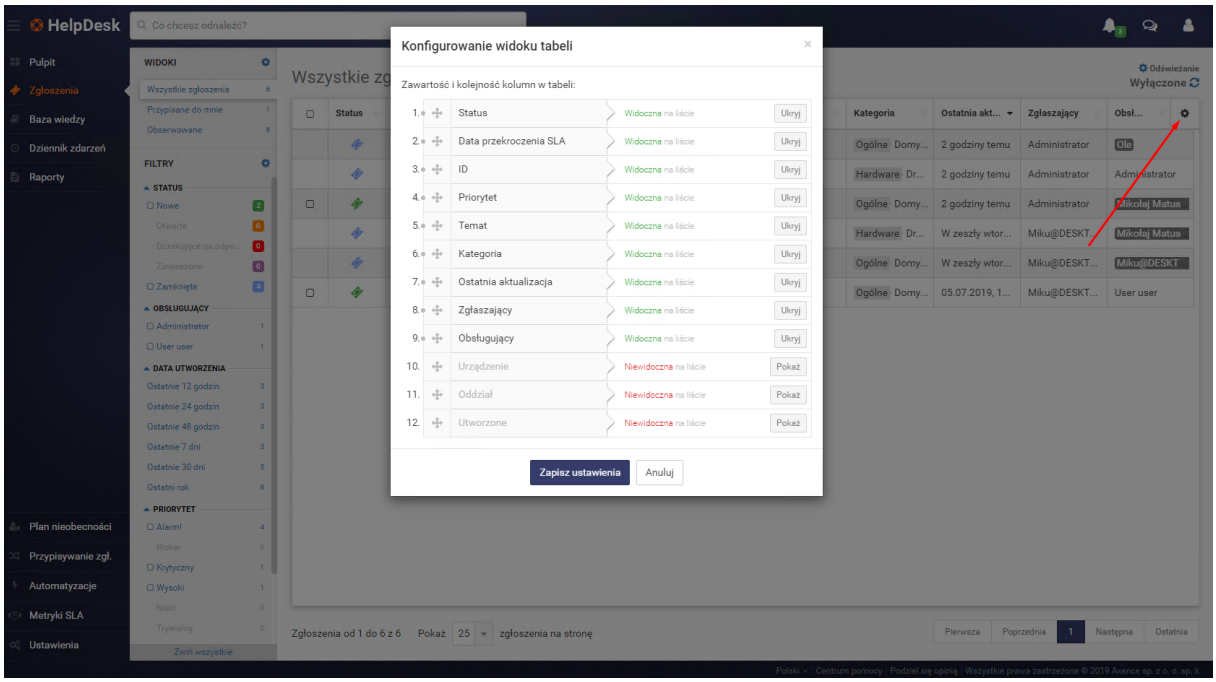
Główną część opisywanego widoku stanowi tabela z listą zgłoszeń. Zawiera on następujące kolumny:

- Status (oznaczenie kolorystyczne po lewej stronie wiersza w tabeli)
- ID

- Data przekroczenia SLA
- Priorytet
- Temat zgłoszenia
- Kategoria
- Powiązane urządzenie (w widoku Administratora kolumna ukryta)
- Oddział (w widoku Administratora kolumna ukryta)
- Data utworzenia (w widoku Administratora kolumna ukryta)
- Data ostatniej aktualizacji
- Imię i nazwisko obsługującego
- Imię i nazwisko zgłaszającego

Aby wybrać wyświetlane kolumny lub ich kolejność w tabeli, kliknij w przycisk ustawień tabeli [ikona zębatki] znajdujący się w prawym górnym rogu tabeli. Aby sortować zawartość tabeli wg danej kolumny, kliknij w strzałkę przy nazwie kolumny. Poniżej tabeli możesz wybrać, ile zgłoszeń ma być wyświetlanych na stronie, a także przejść do kolejnych stron.

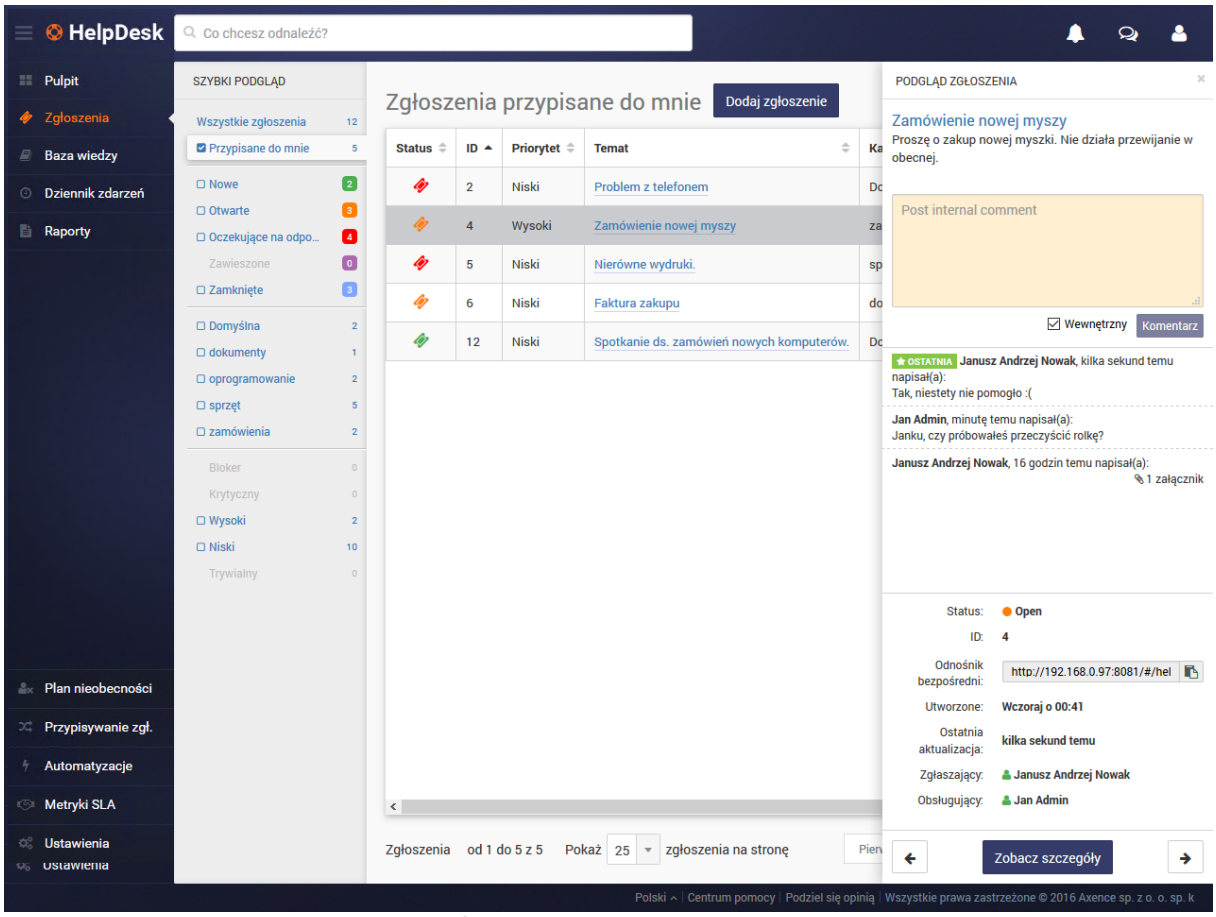
Uwaga: Zgłoszenia nieprzeczytane wyróżnione są pogrubioną czcionką.



Ustawienia tabeli - wybór kolumn.

Podgląd zgłoszenia

W wyniku kliknięcia na ikonę statusu lub wiersz danego zgłoszenia w prawej części interfejsu zostanie otwarty szybki podgląd tego zgłoszenia. W ramach szybkiego podglądu wyświetlany jest tytuł i skrócony wypis zgłoszenia, a następnie blok akcji. W tym bloku można w szybki i wygodny sposób dodać komentarz wewnętrzny lub publiczny do zgłoszenia. Następnie wyświetlane są ostatnie komentarze, skrócona metryka zgłoszenia i pasek nawigacji. Aby zobaczyć więcej szczegółów zgłoszenia w widoku przetwarzania zgłoszenia, kliknij w przycisk **Zobacz szczegóły.**



Szybki podgląd zgłoszenia.

Aby od razu przejść do szczegółowego widoku zgłoszenia, kliknij w jego tytuł.

Powiązane tematy

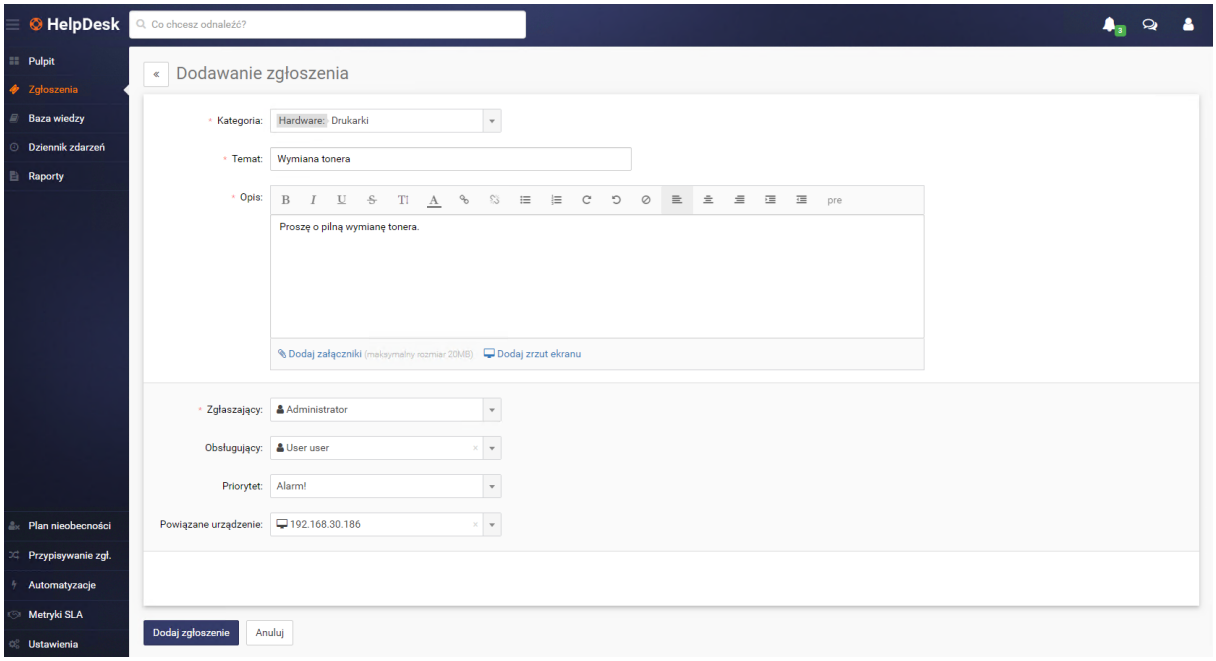
- Uruchamianie interfejsu HelpDesk
- Zgłoszenia - wprowadzenie
- Widoki główne
- Dodawanie zgłoszenia
- Dodawanie komentarza
- Kategorie
- Priorytety
- Zmiana szczegółów zgłoszenia (ticket metrics)

10.4.3 Dodawanie zgłoszenia

Aby utworzyć nowe zgłoszenie w interfejsie HelpDesk:

1. W widoku **Zgłoszenia** kliknij w przycisk **Dodaj zgłoszenie**.
2. Podaj **Temat** zgłoszenia.
3. Podaj **Opis** problemu we wbudowanym edytorze tekstu.

4. Możesz **Dodać załącznik** do zgłoszenia.
5. Możesz **dodać zrzut ekranowy** jeśli na urządzeniu zainstalowany jest Agent.
6. Uzupełnij pole **Zgłaszającego** (Administrator i pracownik HelpDesk może utworzyć zgłoszenie w czyimś imieniu).
7. W polu **Obsługujący** wybierz z listy osobę, do której zostanie przypisane zgłoszenie (opcjonalnie).
8. Określ **Kategorię** zgłoszenia wybierając z listy dostępnych kategorii. Możesz dodać nową kategorię nie przerywając tworzenia artykułu.
9. Określ **Priorytet** zgłoszenia wybierając z listy dostępnych priorytetów. Możesz dodać nowy priorytet nie przerywając tworzenia artykułu.
10. Wybierz z listy **Powiązane urządzenie**, którego dotyczy zgłoszenie (opcjonalnie).
11. Po skończeniu tworzenia zgłoszenia kliknij w przycisk **Dodaj zgłoszenie**.



Formularz dodawania nowego zgłoszenia.

Powiązane tematy

- Uruchamianie interfejsu HelpDesk
- Zgłoszenia - wprowadzenie
- Lista zgłoszeń
- Dodawanie komentarza
- Zmiana szczegółów zgłoszenia (ticket metrics)
- Łączenie zgłoszeń

10.4.4 Przetwarzanie zgłoszenia

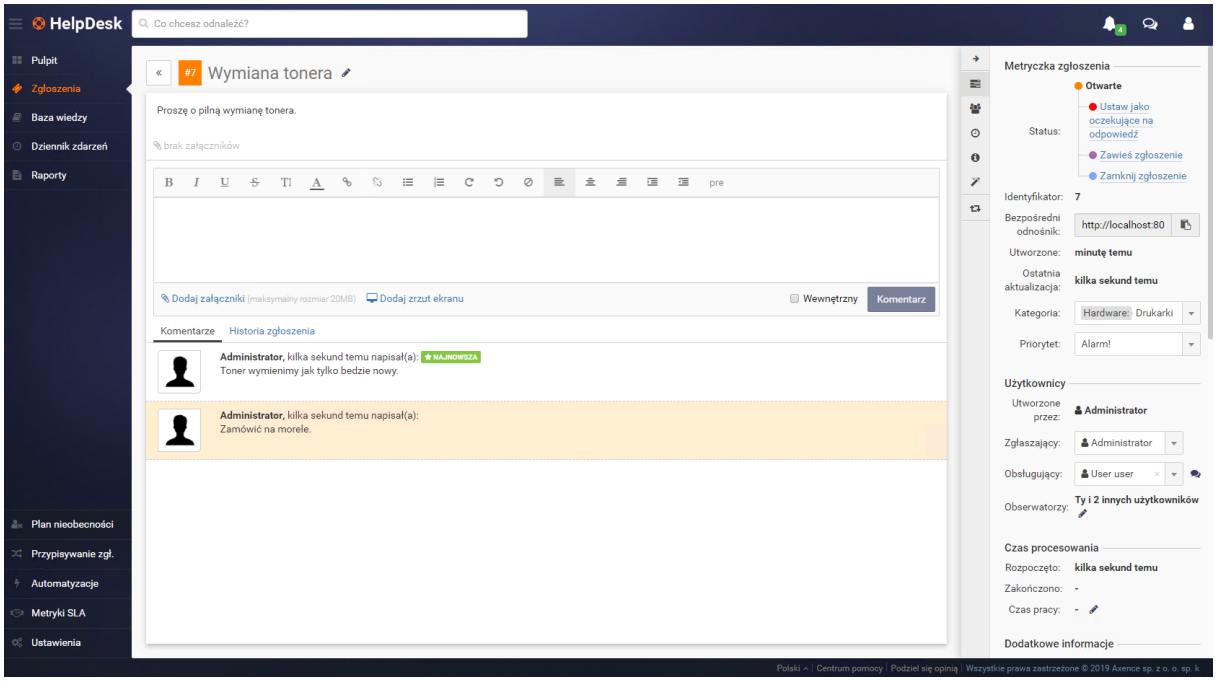
10.4.4.1 Dodawanie komentarza

Aby dodać komentarz do zgłoszenia:

1. W widoku **Zgłoszenia** kliknij tytuł zgłoszenia, które chcesz przetwarzać.
2. Wpisz komentarz we wbudowanym edytorze tekstu w polu poniżej opisu zgłoszenia.
3. Możesz **Dodać załącznik** do zgłoszenia.
4. Możesz **Dodać zrzut ekranowy**, jeśli na urządzeniu zainstalowany jest Agent.
5. Domyślnie formularz ustawiony jest w trybie publikacji komentarzy wewnętrznych (pomarańczowe tło), które są widoczne tylko dla użytkowników typu Administrator i HelpDesk. Jeśli komentarz ma być widoczny dla użytkowników końcowych (białe tło), odznacz pole **Wewnętrzny**. Użytkownik końcowy może dodawać tylko komentarze publiczne.
6. Możesz dodać link do artykułu z Bazy wiedzy (tylko Administrator i pracownik pomocy HelpDesk).

   Aby to zrobić, kliknij w przycisk **Wskaż artykuł** i wpisz tytuł lub wybierz z listy artykuł, który chcesz podlinkować. Możesz w ten sposób podlinkować wiele artykułów. Aby zakończyć, kliknij w przycisk **Wskaż artykuł**.

7. Aby opublikować komentarz, kliknij w przycisk **Komentarz**.



Podstawowa edycja zgłoszenia - dodawanie komentarza.

Powiązane tematy

Uruchamianie interfejsu HelpDesk

Zgłoszenia - wprowadzenie

Lista zgłoszeń

Dodawanie załącznika

10.4.4.2 Dodawanie załączników i zrzutów ekranowych

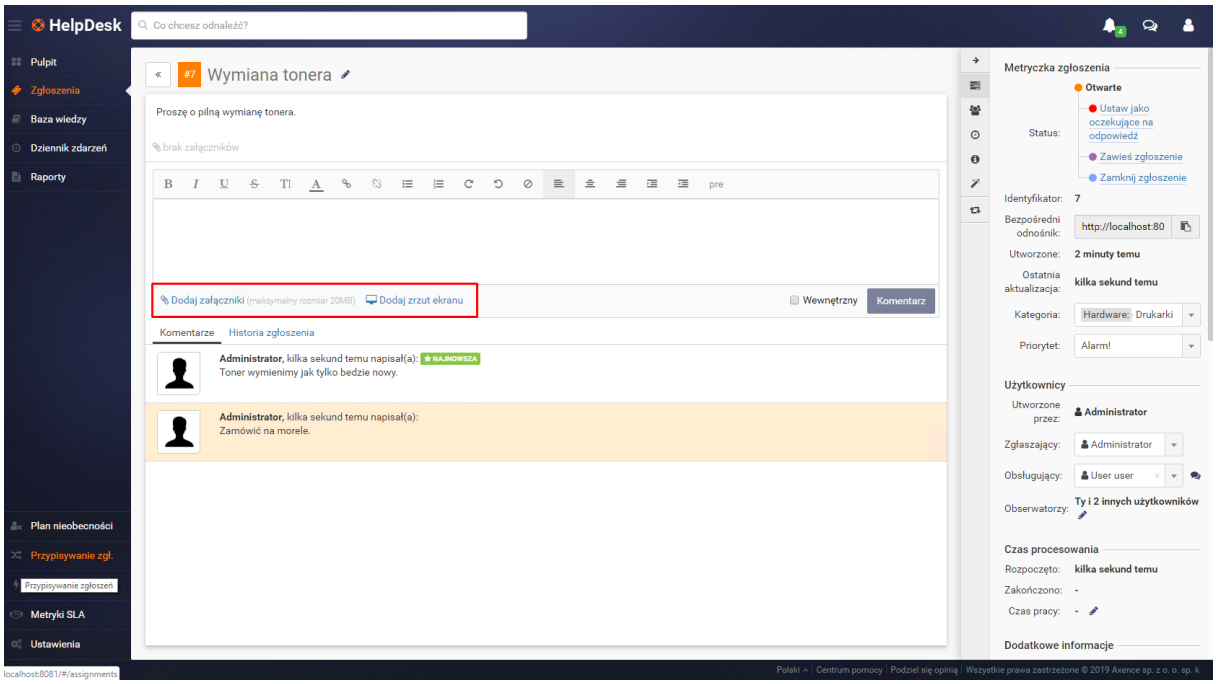
Aby dodać do zgłoszenia załącznik:

1. W widoku Dodawania zgłoszenia lub Dodawania komentarza do zgłoszenia kliknij w przycisk **Dodaj załącznik**.
2. W oknie dialogowym wybierz plik, który chcesz dołączyć.
3. Wpisz komentarz i kliknij przycisk **Komentarz**.

Aby dodać zrzut ekranu do zgłoszenia:

1. W widoku Dodawania zgłoszenia lub Dodawania komentarza do zgłoszenia kliknij w przycisk **Dodaj zrzut ekranu**.
2. W oknie dialogowym kliknij w przycisk **Zrzut ekranowy**. Zostanie wyświetlony obraz z ekranem użytkownika.
3. Wpisz komentarz i kliknij przycisk **Komentarz**.

Uwaga: Zrzut ekranowy może dodać tylko autor zgłoszenia jeśli na jego urządzeniu zainstalowany jest Agent z konfiguracją zezwalającą na wykonywanie zrzutów ekranowych.



Zrzuty ekranowe oraz załączniki dla zgłoszeń

Powiązane tematy

Uruchamianie interfejsu HelpDesk

Zgłoszenia - wprowadzenie

Lista zgłoszeń

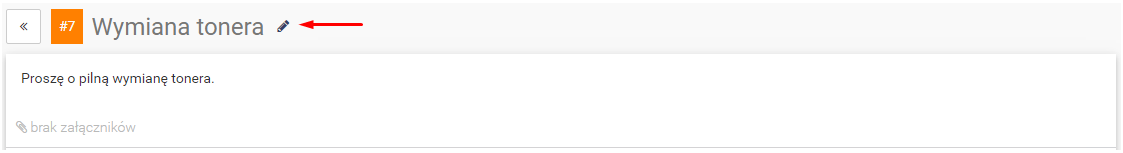
Dodawanie zgłoszenia

Dodawanie komentarza

10.4.4.3 Edycja tytułu zgłoszenia

Aby zmienić tytuł zgłoszenia:

1. W widoku **Zgłoszenia** kliknij w zgłoszenie, które chcesz przetwarzać.
2. Kliknij w ikonę ołówka znajdującą się obok tematu zgłoszenia.



3. W oknie dialogowym wpisz nowy temat.
4. Kliknij w przycisk **Zapisz zmiany**.

Powiązane tematy

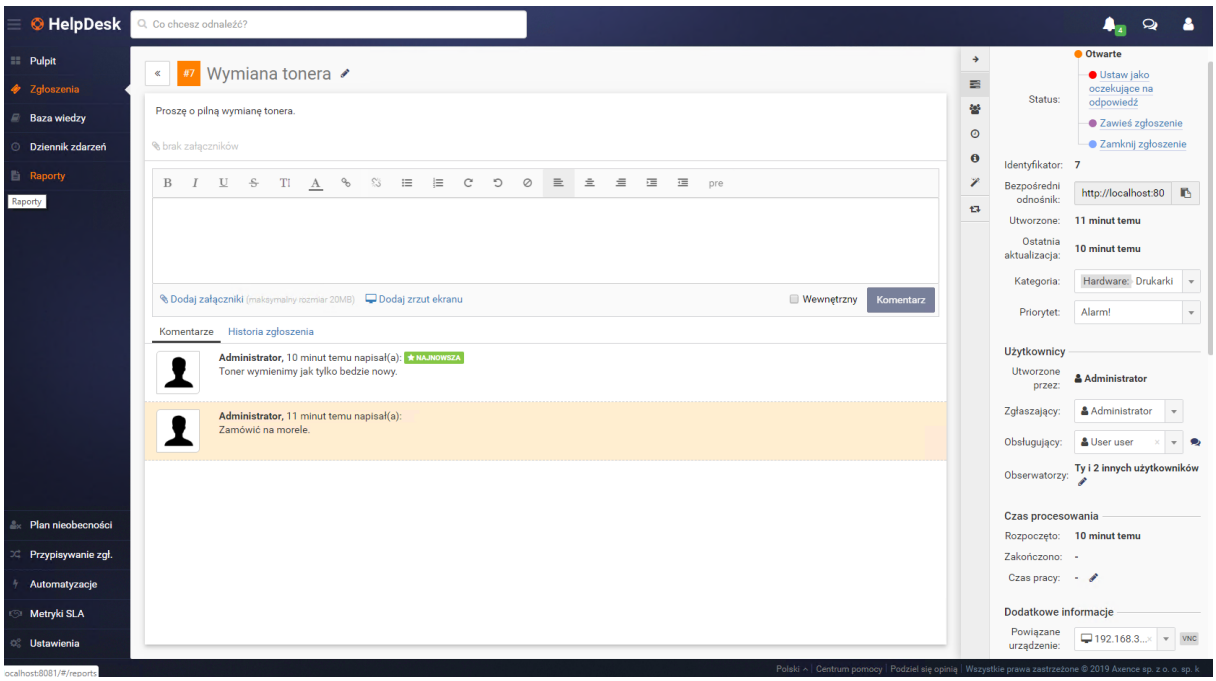
Uruchamianie interfejsu HelpDesk

Zgłoszenia - wprowadzenie

Lista zgłoszeń

10.4.4.4 Szczegóły zgłoszenia

Metryczka zgłoszenia znajduje się w prawej części okna przetwarzania danego zgłoszenia. Poniżej prezentowana jest pełna postać metryki dla Administratora. W widoku pracownika pomocy HelpDesk nie jest dostępna opcja usuwania zgłoszenia.



Widok zgłoszenia z pełną metryką.

Zmiana statusu

Aby zmienić status zgłoszenia, kliknij w docelowy status. Uwaga: wyświetlane są wszystkie statusy, do których zmiana jest możliwa. Jako pierwszy wyświetlany jest aktualny status zgłoszenia. Zamknięcie zgłoszenia jest operacją nieodwracalną a zgłoszeń zamkniętych nie można usunąć z systemu.

Zmiana kategorii

Aby zmienić kategorię, rozwiń menu kategorii i wybierz z listy docelową kategorię.

Zmiana priorytetu

Aby zmienić priorytet, rozwiń menu priorytetów i wybierz z listy docelowy priorytet.

Użytkownicy

Zmiana Zgłaszajacego / Obsługującego

Aby ręcznie zmienić Zgłaszającego, rozwiń pole **Zgłaszający** i wybierz z listy właściwą osobę. Analogicznie, aby przypisać pracownika pomocy HelpDesk lub Administratora do zgłoszenia, rozwiń pole **Obsługujący** i wybierz z listy osobę, która będzie odpowiedzialna za rozwiązanie danego zgłoszenia.
Aby poznać automatyczne metody przypisywania pracowników do zgłoszeń, przejdź do tematów: Zarządzanie użytkownikami, Przypisywanie pracowników do kategorii i Automatyzacje.

Dodanie Obserwatorów

Do listy Obserwatorów, możesz również dodać osoby, które będą otrzymywały powiadomienie e-mail o nowych komentarzach publicznych w zgłoszeniu.
Do listy Obserwatorów dodawani są automatycznie: zgłaszający, rozwiązujący i ci pracownicy, którzy zmodyfikowali zgłoszenie.

Czat

Aby rozpocząć czat ze zgłaszającym lub obsługującym, kliknij w ikonę znajdującą się po prawej stronie pola z nazwą odpowiedniego użytkownika.

Ustawienie czasu przetwarzania zgłoszenia

Połączenie VNC

Powiązane zgłoszenia

Metryka SLA - poziom świadczenia usług

Prezentuje informacje o aktywnych oraz zakończonych metrykach, którymi zgłoszenie jest objęte

wraz z informacją kiedy metryka zostanie złamana.

Dodatkowe działania:

[Łączenie zgłoszeń]

[Usuwanie zgłoszenia]

Powiązane tematy

Uruchamianie interfejsu HelpDesk

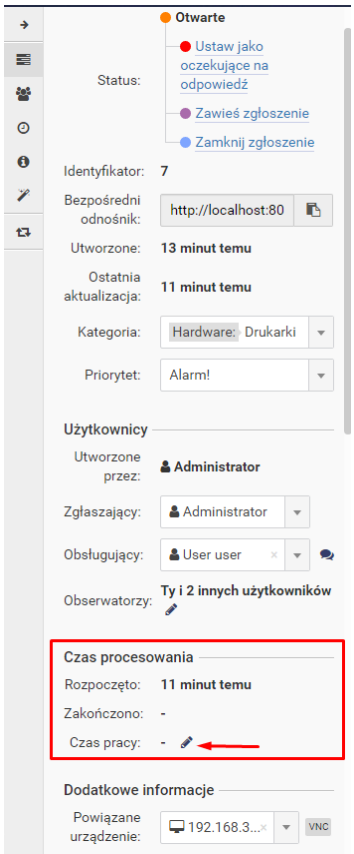
Zgłoszenia - wprowadzenie

10.4.4.4.1 Ustawienie czasu przetwarzania zgłoszenia

Ustawienie czasu przetwarzania zgłoszenia umożliwia późniejszą analizę wydajności oraz szacowanie czasu potrzebnego do rozwiązania podobnych problemów.

Aby ustawić czas przetwarzania zgłoszenia:

1. W widoku wybranego zgłoszenia w części **Czas procesowania** kliknij w ikonę ołówka.
2. Wprowadź czas, przez który zgłosznie było procesowane.
3. W oknie dialogowym ustaw czas przetwarzania zgłoszenia i kliknij w przycisk **Zapisz zmiany**.



Powiązane tematy

Uruchamianie interfejsu HelpDesk

Zmiana szczegółów zgłoszenia

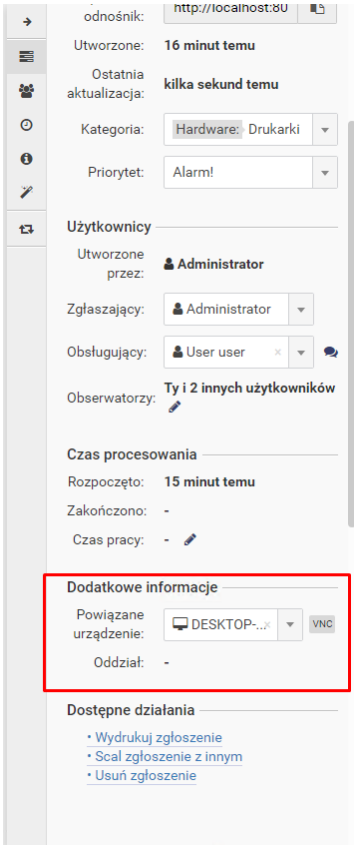
Zgłoszenia - wprowadzenie

10.4.4.4.2 Połączenie VNC

Uwaga: opcja zdalnego dostępu jest widoczna tylko dla urządzeń obsługujących taką opcję.

Aby połączyć się zdalnie z urządzeniem, którego dotyczy dane zgłoszenie:

1. W widoku wybranego zgłoszenia w części **Dodatkowe informacje** kliknij przycisk **VNC** znajdujący się po prawej stronie nazwy powiązanego urządzenia.
2. W oknie dialogowym wybierz sesję użytkownika, z którą chcesz się połączyć i kliknij w przycisk **Połącz**. W wyniku tego działania zostanie otwarta nowa karta przeglądarki ze zdalnym połączeniem.
3. Z menu w prawym, górnym rogu możesz sterować opcjami połączenia.



Powiązane tematy

Uruchamianie interfejsu HelpDesk

Zmiana szczegółów zgłoszenia

Zgłoszenia - wprowadzenie

10.4.4.4.3 Powiązane zgłoszenia

System HelpDesk umożliwia tworzenie powiązań między zgłoszeniami. Każde powiązanie łączy ze sobą dokładnie dwa różne zgłoszenia.

Powiązania zgłoszeń mogą być tworzone i usuwane przez każdego mającego rolę Pracownik HelpDesk lub Administrator oraz są widoczne tylko dla takich użytkowników.

Informacja o powiązanych zgłoszenia widoczna jest w metryce zgłoszenia (jako ostatnia opcja).

W systemie HelpDesk wyróżnia się następujące rodzaje powiązań:

- Powiązanie (oba kierunki mają tę samą treść)

  Zgłoszenie A jest powiązane ze zgłoszeniem B

  Zgłoszenie B jest powiązane ze zgłoszeniem A

- Blokowanie

  Zgłoszenie A blokuje zgłoszenie B

  Zgłoszenie B jest blokowane przez zgłoszenie A

- Powielenie

  Zgłoszenie A powiela zgłoszenie B

  Zgłoszenie B jest powielone przez zgłoszenie A

- Związek przyczynowo-skutkowy

  Zgłoszenie A jest przyczyną zgłoszenia B

  Zgłoszenie B jest skutkiem zgłoszenia A

- Kontynuacja

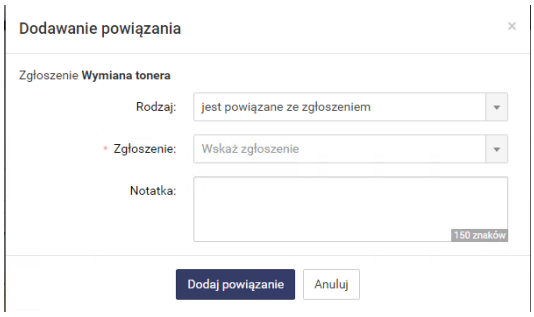
  Zgłoszenie A jest kontynuacją zgłoszenia B

  Zgłoszenie B jest kontynuowane przez zgłoszenie A

Tworzenie i usuwanie powiązań

Aby utworzyć powiązanie między zgłoszeniami:

1. Przejdź do metryki jednego ze zgłoszeń.
2. W sekcji **Powiązane zgłoszenia** kliknij przycisk **Dodaj powiązanie**
3. Wskaż:
   - rodzaj powiązania
   - inne zgłoszenie, które chcesz powiązać z bieżącym zgłoszeniem
   - opcjonalnie: opis powiązania (notatkę)
4. Kliknij przycisk **Dodaj powiązanie.**



Informacje dodatkowe

- Dla każdego zgłoszenia można utworzyć dowolną liczbę powiązań.
- Powiązania można tworzyć i usuwać nawet jeżeli jeden lub oba wiązane zgłoszenia są zamknięte.
- Tworzenie i usuwanie powiązań nie generuje powiadomień dla żadnych użytkoniwków uczestniczących w procesowaniu zgłoszenia.
- Zgłoszenie utworzone za pomocą wiadomości e-mail jako kontynuacja zamkniętego zgłoszenia (poprzez odpowiedź na powiadomienie e-mail), automatycznie w chwili stworzenia jest powiązane ze zgłoszeniem, które kontynuuje. *("Zgłoszenie <follow-up> jest kontynuacją zgłoszenia <zamknięte zgłoszenie>")*
- Utworzenie lub usunięcie powiązania nie jest aktualizacją zgłoszenia, zatem nie wpływa na datę ostatniej aktualizacji zgłoszenia oraz nie wyzwala automatyzacji.
- Usunięcie zgłoszenia, które występuje w jakichś powiązaniach powoduje usunięcie wszystkich tych powiązań (niezależnie od ich kierunku).

10.4.4.4.4 Łączenie zgłoszeń

Uwaga: połączyć można wyłącznie zgłoszenia, które nie są zamknięte (czyli mają status Nowy, Otwarty, Czeka na odpowiedź, Zawieszony) i które pochodzą od tego samego zgłaszającego. Operacja ta jest nieodwracalna.

Aby połączyć zgłoszenia:

1. W widoku **Zgłoszenia** kliknij w zgłoszenie, które chcesz połączyć z innym zgłoszeniem.
2. W metryce zgłoszenia, w sekcji **Dostępne działania** (ostatnia sekcja na dole) kliknij w akcję **Scal to zgłoszenie z innym**.
3. W oknie dialogowym łączenia zgłoszeń podaj nazwę lub ID zgłoszenia, do którego ma być dołączone bieżące zgłoszenie (tego samego zgłaszającego).
4. Kliknij w przycisk **Dołącz zgłoszenie**.

Powiązane tematy

Uruchamianie interfejsu HelpDesk

Zmiana szczegółów zgłoszenia

Zgłoszenia - wprowadzenie

10.4.4.4.5 Usuw anie zgłoszenia

Uwaga: tylko użytkownik typu Administrator może usuwać zgłoszenia, pod warunkiem, że nie są one zamknięte. Operacja usunięcia zgłoszenia jest nieodwracalna.

Aby usunąć zgłoszenie:

1. W widoku **Zgłoszenia** kliknij w zgłoszenie, które chcesz usunąć.
2. W metryce zgłoszenia, w sekcji **Dostępne działania** kliknij w akcję **Usuń zgłoszenie**.
3. W oknie dialogowym usuwania zgłoszenia kliknij w przycisk **Usuń zgłoszenie**.

Powiązane tematy

Uruchamianie interfejsu HelpDesk

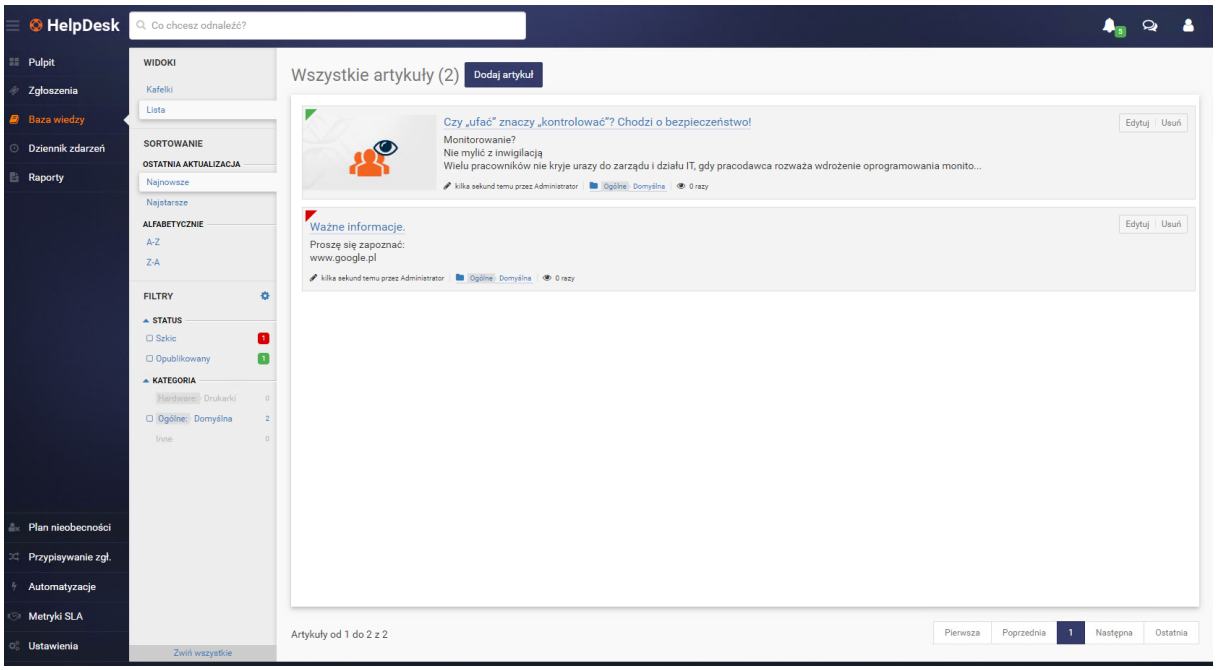
Zmiana szczegółów zgłoszenia

Zgłoszenia - wprowadzenie

10.5 Baza wiedzy

10.5.1 Baza wiedzy - wprowadzenie

Baza wiedzy to miejsce, w którym Administratorzy i pracownicy HelpDesku mogą umieszczać artykuły opisujące procedury stosowane w danej instytucji oraz najczęściej występujące problemy i ich rozwiązania. Po opublikowaniu takich artykułów, użytkownicy mogą je przeglądać lub użyć pola "Szukaj", aby znaleźć artykuł opisujący rozwiązanie problemu, z którym się zetknęli. Jeżeli wyszukiwanie w bazie wiedzy nie da rezultatu w postaci opisu rozwiązania danego problemu, wówczas użytkownik może utworzyć zgłoszenie opisując problem.



Lista artykułów bazy wiedzy.

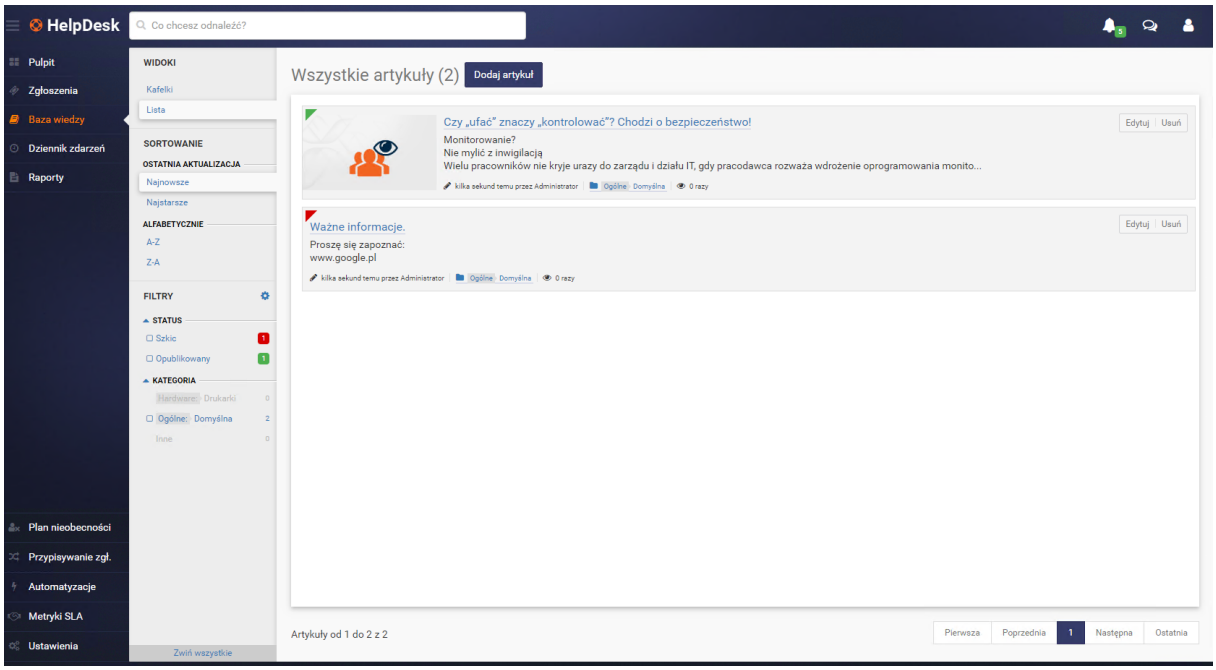
Powiązane tematy

Uruchamianie interfejsu HelpDesk

- Lista artykułów
- Dodawanie artykułu
- Edytowanie artykułu
- Usuwanie artykułu
- Zgłoszenia - wprowadzenie
- Wyszukiwanie

10.5.2 Lista artykułów

W widoku artykułów prezentowana jest lista artykułów znajdujących się z bazie wiedzy. Widok ten jest spójny z widokiem listy zgłoszeń.



Lista artykułów bazy wiedzy.

W lewej części ekranu znajduje się nawigacja główna (patrz Widoki główne) oraz kolumna szybkiego widoku. Szybki widok pozwala na szybkie przejście do zbioru danych z określonego obszaru zainteresowań. Przykładowo, wyświetlane mogą być nieopublikowane artykuły, które dodatkowo należą do jednej z dwóch wybranych kategorii.

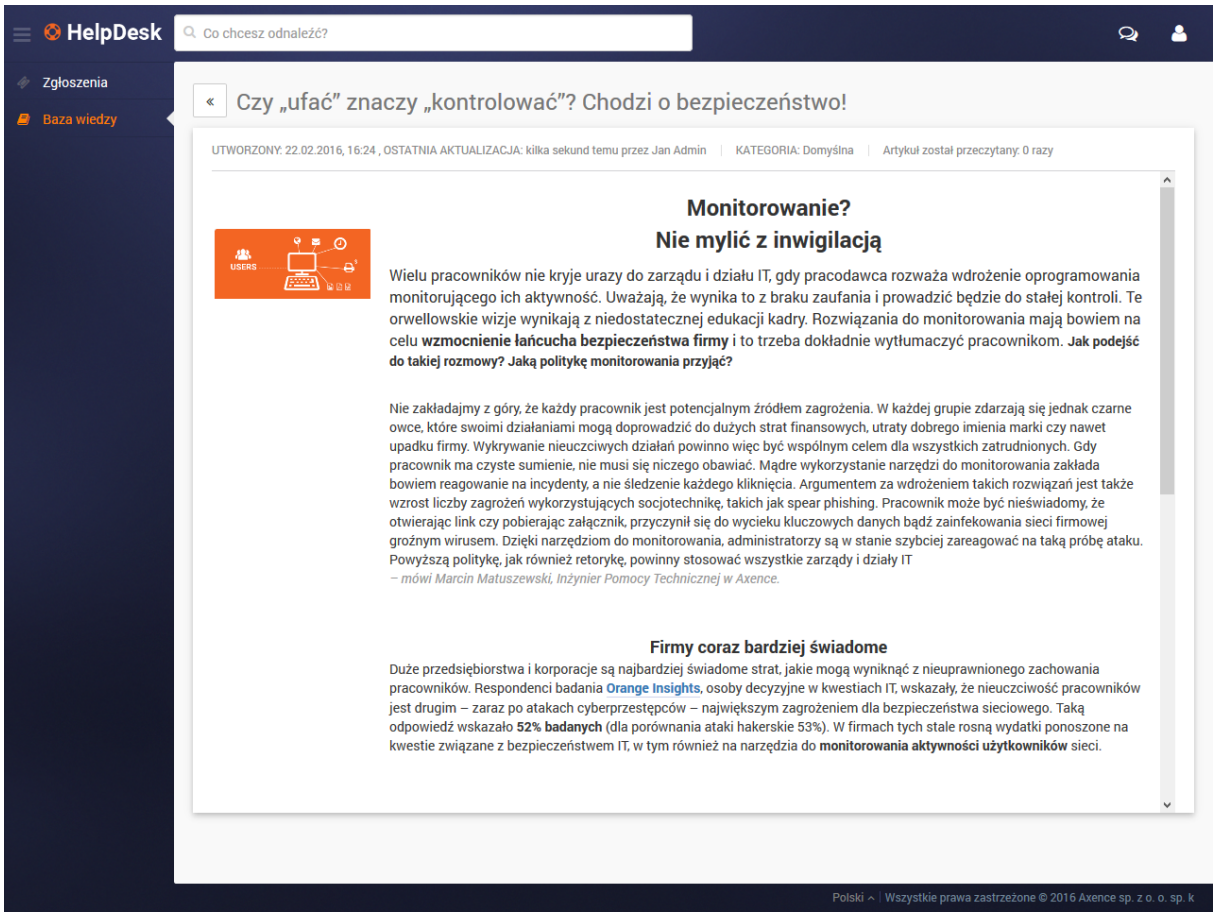
Lista artykułów

Główną część opisywanego widoku stanowi tabela z listą artykułów. Każdy artykuł reprezentowany jest przez kafelek. W ramach pojedynczego kafelka wyświetlane są następujące składniki:

- Status artykułu (czerwony - roboczy, zielony - opublikowany)
- Tytuł
- Akcje kontekstowe: **edycja** (tylko dla pracownika pomocy HelpDesk i Administratora) i **usuwanie** (tylko dla Administratora)
- Okładka artykułu (jeśli była zdefiniowana)

- Wypis z tekstu artykułu
- Data utworzenia
- Data ostatniej aktualizacji
- Kategoria
- Liczba wyświetleń artykułu przez użytkowników końcowych (tylko dla pracownika pomocy HelpDesk i Administratora)

Aby otworzyć dany artykuł, kliknij w jego tytuł.



Przykładowy artykuł w bazie wiedzy.

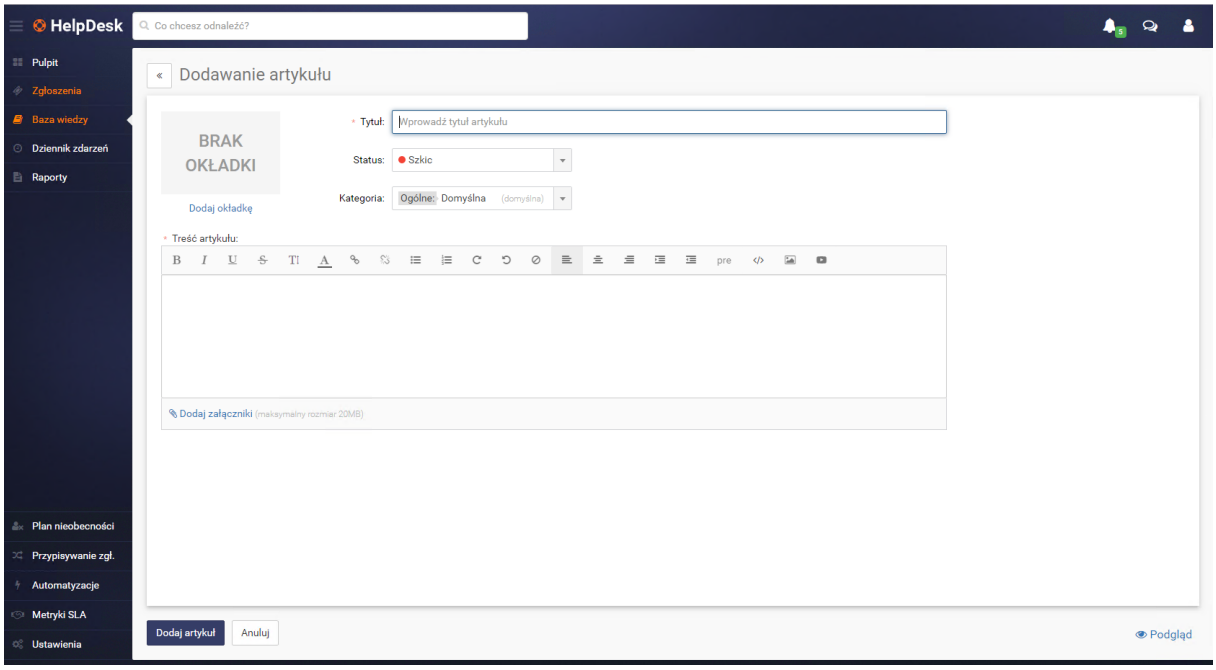
Powiązane tematy

- Uruchamianie interfejsu HelpDesk
- Baza wiedzy - wprowadzenie
- Zgłoszenia - wprowadzenie
- Lista artykułów
- Dodawanie artykułu
- Edytowanie artykułu
- Usuwanie artykułu

10.5.3 Dodawanie artykułu

Aby utworzyć nowy artykuł w interfejsie HelpDesk:

1. W widoku **Baza wiedzy** kliknij w przycisk **Dodaj artykuł**.
2. Dodaj **Okładkę** artykułu (opcjonalnie).
3. Wpisz **Tytuł** artykułu.
4. Wpisz treść artykułu we wbudowanym edytorze tekstu.
5. Możesz dołączyć do artykułu obrazek lub link do zewnętrznego filmu wideo korzystając z opcji **Dodaj obraz** i **Dodaj film**.
6. Ustaw **Status** artykułu jako **Szkic** lub **Opublikowany** (domyślnie: Szkic). Artykuły oznaczone jako robocze nie będą widoczne dla użytkowników końcowych. Możesz później uzupełnić artykuł i edytować jego status.
7. Ustaw **Kategorię** artykułu wybierając ją z listy dostępnych kategorii. Możesz dodać nową kategorię nie przerywając tworzenia artykułu.
8. Możesz zobaczyć tworzony artykuł klikając w **Podgląd**. Aby wrócić do okna edycji artykułu, kliknij w przycisk **Powrót do edycji**.
9. Po skończeniu tworzenia artykułu kliknij w przycisk **Dodaj artykuł**.



Formularz dodawania artykułu do bazy wiedzy.

Powiązane tematy

Logowanie do interfejsu HelpDesk

Baza wiedzy

Lista artykułów

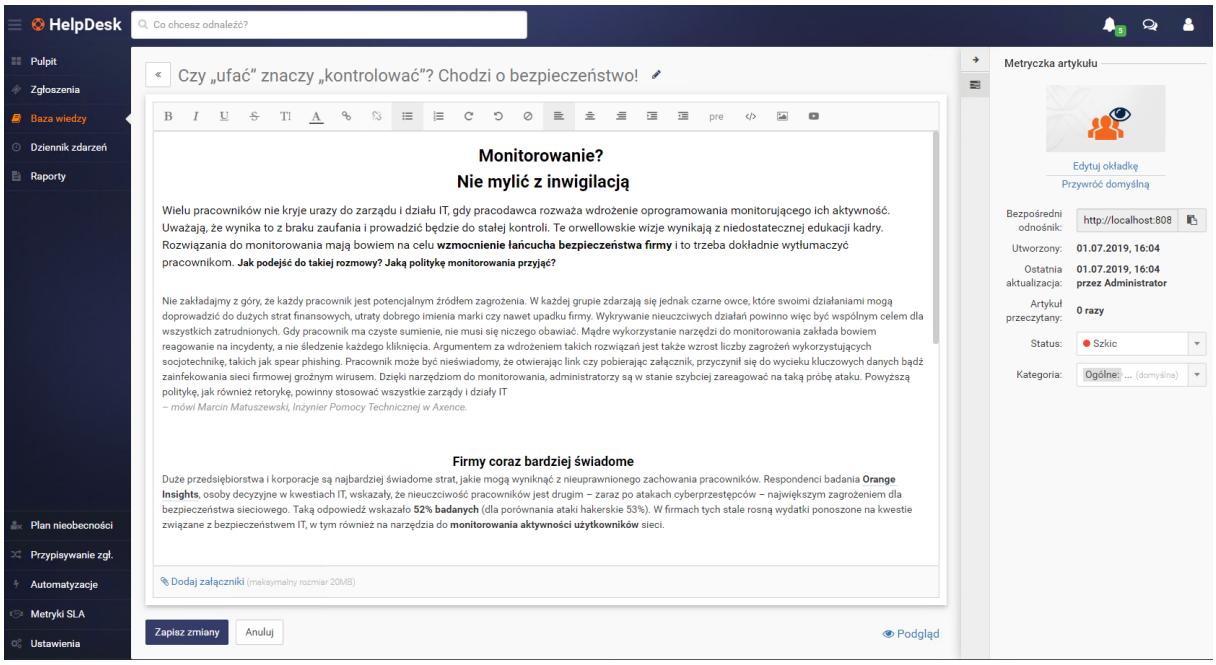
Edytowanie artykułu

Usuwanie artykułu

10.5.4 Edycja artykułu

Aby edytować artykuł w interfejsie HelpDesk:

1. W widoku **Baza wiedzy** kliknij w przycisk **Edytuj** na kafelku artykułu, który chcesz edytować.
2. Aby edytować tytuł artykułu, kliknij w ikonę ołówka znajdującą się po prawej stronie tytułu, wpisz nowy tytuł i kliknij w przycisk **Zapisz zmiany**.
3. Zmodyfikuj treść artykułu we wbudowanym edytorze tekstu.
4. Możesz dołączyć do artykułu obrazek lub link do zewnętrznego filmu wideo korzystając z opcji **Prześlij obrazek** i **wstaw film**.
5. Aby zmienić okładkę artykułu, w metryce artykułu w prawej części okna kliknij w ikonę ołówka na okładce (lub w **Dodaj okładkę**).
6. Aby zmienić status artykułu, w metryce artykułu w prawej części okna wybierz **Status**: **Szkic** lub **Opublikowany**.
7. Aby zmienić kategorię artykułu, w metryce artykułu w prawej części okna wybierz **Kategorię** wybierając ją z listy dostępnych kategorii. Możesz dodać nową kategorię nie przerywając tworzenia artykułu.
8. Możesz zobaczyć tworzony artykuł klikając w **Podgląd**. Aby wrócić do okna edycji artykułu, kliknij w przycisk **Powrót do edycji**.
9. Po zakończeniu wprowadzania zmian kliknij w przycisk **Zapisz zmiany**.



Formularz edycji artykułu do bazy wiedzy.

Powiązane tematy

Logowanie do interfejsu HelpDesk

Baza wiedzy

Lista artykułów

Dodawanie artykułu

Usuwanie artykułu

10.5.5 Usuwanie artykułu

Aby usunąć artykuł w interfejsie HelpDesk:

1. W widoku **Baza wiedzy** kliknij w przycisk **Usuń** na kafelku artykułu, który chcesz usunąć.
2. Zostanie wyświetlone okno dialogowe, w którym potwierdź chęć usunięcia artykułu klikając w przycisk **Usuń artykuł**. Usunięty artykuł nie może być przywrócony.

Powiązane tematy

Logowanie do interfejsu HelpDesk

Baza wiedzy

Lista artykułów

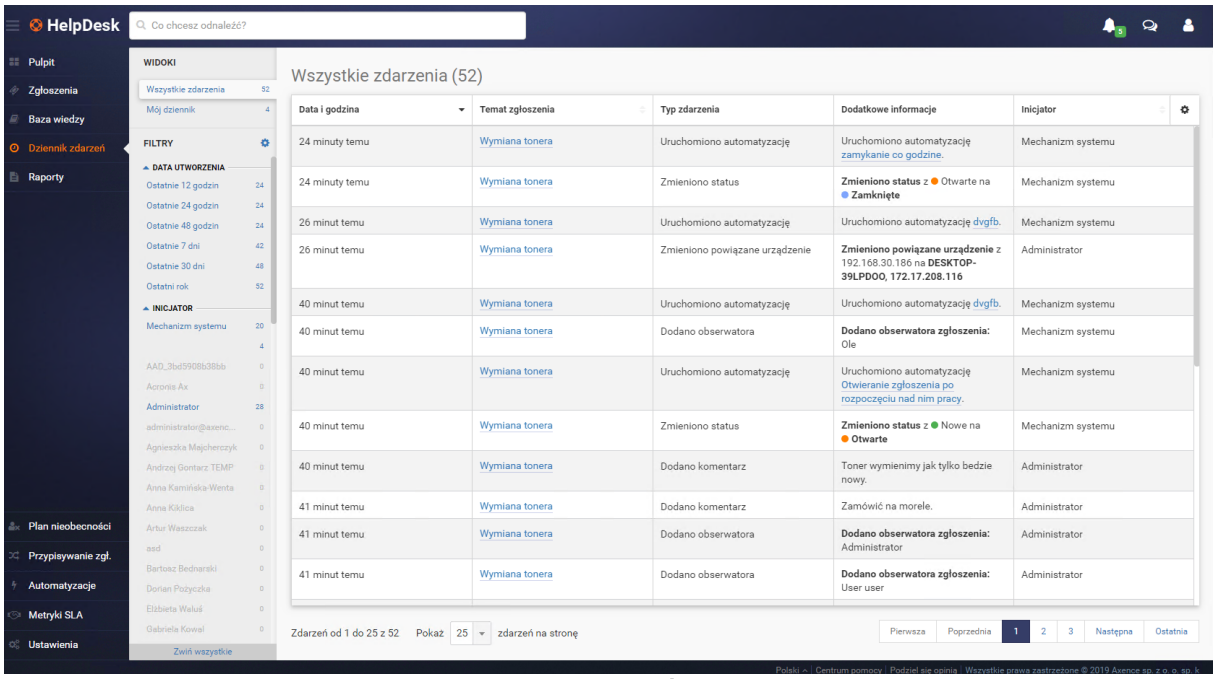
Dodawanie artykułu

Edytowanie artykułu

10.6 Dziennik zdarzeń

W widoku aktywności prezentowana jest lista wszystkich aktywności dotyczących zgłoszeń w systemie HelpDesk. Lista aktywności umożliwia śledzenie historii zmian w zgłoszeniach, optymalizację pracy, a także pozwala na wyjaśnienie ewentualnych nieporozumień.

Uwaga: lista aktywności obejmuje wyłącznie działania związane ze zgłoszeniami, nie uwzględnia zmian w bazie artykułów. Lista aktywności jest widoczna dla działań użytkowników typu Administrator i pracownik pomocy HelpDesk.



Lista aktywności.

Widok listy aktywności jest spójny z widokiem listy zgłoszeń i listy artykułów. W lewej części ekranu znajduje się nawigacja główna (patrz Widoki główne) oraz kolumna szybkiego widoku. Szybki widok pozwala na szybkie przejście do zbioru danych z określonego obszaru zainteresowań. Przykładowo, wyświetlane mogą być tylko zdarzenia zastosowanych automatyzacji i zmian priorytetu lub wszystkie zdarzenia dla danego zgłoszenia, które miały miejsce w ostatnim tygodniu.

Aby zmienić wyświetlane kolumny lub ich kolejność, kliknij w przycisk ustawień tabeli [ikona] znajdujący się w prawym górnym rogu tabeli. Aby sortować zawartość tabeli wg danej kolumny, kliknij w strzałkę przy nazwie kolumny. Poniżej tabeli możesz wybrać, ile zgłoszeń ma być wyświetlanych na stronie, a także przejść do kolejnych stron.

Filtry

W kolumnie szybkiego widoku znajdującej się w lewej części okna dostępne są następujące filtry zdarzeń:

- wszystkie zdarzenia na obiekcie zgłoszenie (wybór domyślny dla Administratora, opcja niewidoczna dla użytkowników typu HelpDesk),
- wszystkie zdarzenia na zgłoszeniu przypisanym do mnie (wybór domyślny dla użytkowników typu HelpDesk),
- zdarzenia z ostatniego tygodnia (możliwość wyboru typu wyświetlanych zdarzeń),
- zdarzenia z ostatniego miesiąca (możliwość wyboru typu wyświetlanych zdarzeń),
- zdarzenia z ostatniego roku (możliwość wyboru typu wyświetlanych zdarzeń),
- zdarzenia po typie (możliwość zaznaczenia wielu pozycji).

Filtrowanie zdarzeń po typie obejmuje następujące opcje:

Typ zdarzenia	Dodatkowe wyświetlane informacje	Inicjator zdarzenia
Dodano komentarz	Treść komentarza	Nazwa użytkownika

Typ zdarzenia	Dodatkowe wyświetlane informacje	Inicjator zdarzenia
Niepowodzenie akcji automatyzacji	Nazwa nieudanej akcji automatyzacji	Mechanizm systemu
Połączono zgłoszenia	Nazwy zgłoszeń	Nazwa użytkownika
Uruchomiono automatyzację	Nazwa zastosowanej automatyzacji	Mechanizm systemu
Utworzono zgłoszenie	Nazwa utworzonego zgłoszenia	Nazwa użytkownika
Zmieniono czas pracy	Czas przetwarzania zgłoszenia	Nazwa użytkownika
Zmieniono kategorię	Nazwa obecnej kategorii	Nazwa użytkownika
Zmieniono obsługującego użytkownika	Nazwa użytkownika obsługującego zgłoszenie	Nazwa użytkownika
Zmieniono powiązane urządzenie	Nazwa powiązanego urządzenia	Nazwa użytkownika
Zmieniono priorytet	Nazwa obecnego priorytetu	Nazwa użytkownika
Zmieniono status	Nazwa obecnego statusu	Nazwa użytkownika
Zmieniono temat	Nazwa nowego tematu	Nazwa użytkownika
Zmieniono zgłaszającego	Nazwa użytkownika zgłaszającego	Nazwa użytkownika

Powiązane tematy

Uruchamianie interfejsu HelpDesk

Widoki główne

Lista zgłoszeń

Lista artykułów

Automatyzacje - wprowadzenie

10.7 Raporty

10.7.1 Tworzenie raportu

Raporty dla modułu HelpDesk zawierają 32 wariantów - najpopularniejszych scenariuszy, które pozwalają wygenerować zestawienia dla:

Zgłoszeń:

- ✓ zamkniętych zgłoszeń:
  - ✓ dzienny
  - ✓ tygodniowy
  - ✓ miesięczny

- ✓ porównawczy obsługujących
- ✓ porównawczy priorytetów
- ✓ porównawczy kategorii
- ✓ porównawczy oddziałów

✓ aktywności pracowników helpdesku:

- ✓ dzienny czasu reakcji
- ✓ tygodniowy czasu reakcji
- ✓ miesięczny czasu reakcji
- ✓ sumaryczny liczby zgłoszeń
- ✓ porównawczy aktywności użytkowników
- ✓ porównawczy osób dokonujących pierwszej reakcji

✓ Raporty aktualnie procesowanych zgłoszeń:

- ✓ sumaryczny liczny zgłoszeń
- ✓ porównawczy obsługujących zgłoszenia
- ✓ porównawczy priorytetów
- ✓ porównawczy kategorii
- ✓ porównawczy oddziałów

Metryk SLA:

✓ Raporty SLA w zamkniętych zgłoszeniach:

- ✓ podsumowanie SLA w zamkniętych zgłoszeniach
- ✓ SLA w zamkniętych zgłoszeniach w ujęciu dni
- ✓ SLA w zamkniętych zgłoszeniach w ujęciu tygodni
- ✓ SLA w zamkniętych zgłoszeniach w ujęciu miesięcy
- ✓ SLA w zamkniętych zgłoszeniach według obsługujących
- ✓ SLA w zamkniętych zgłoszeniach według oddziałów

✓ Raporty przebiegu metryk SLA:

- ✓ podsumowanie przebiegu metryk SLA
- ✓ przebieg metryk SLA w ujęciu dni
- ✓ przebieg metryk SLA w ujęciu tygodni
- ✓ przebieg metryk SLA w ujęciu miesięcy
- ✓ przebieg metryk SLA według obsługujących
- ✓ przebieg metryk SLA według oddziałów

✓ Raporty przekroczeń metryk SLA:

- ✓ przekroczenia SLA według daty przekroczenia metryki
- ✓ przekroczenia SLA według daty zamknięcia zgłoszenia

Aby wygenerować raport:

1. Zaloguj się do interfejsu helpdesku jako **administrator**, przejdź do widoku **Raporty.**
2. Wybierz grupę raportów, kliknij na nazwę wariantu raportu.
3. W kreatorze raportu wskaż warunki wstępne (argumenty) oraz określ zakres i formę prezentacji wyników.
4. Wygenerowany raport możesz wyeksportować do pliku **CSV** lub **XLS.**

RAPORTY ZGŁOSZEŃ

Raporty zamkniętych zgłoszeń generowane są dla zgłoszeń, których procesowanie już się zakończyło (one w postaci tylko do odczytu - nie można ich edytować). Wegenerowanie raportów z tej grupy umożliwia głównie kontrolę jakości obsługi zgłoszeń (w poszczególnych dniach, miesiącach, przez poszczególnych pracowników pomocy technicznej).

Raporty te mają charakter archiwalny i są niezmienne. Ponowne wygenerowanie raportu z tymi samymi argumentami da zawsze ten sam rezultat.

Raporty aktywności podsumowują liczbę zdarzeń w systemie w zadanym okresie.Wygenerowanie raportów z tej grupy umożliwia udzielenie informacji o rzędach wielkości danych, które przepływają przez system.

Raporty te mają charakter archiwalny i są niezmienne. Ponowne wygenerowanie raportu z tymi samymi argumentami da zawsze ten sam rezultat.

Raporty aktualnie procesowanych zgłoszeń prezentują dane dotyczące zgłoszeń, które są aktualnie procesowane w systemie. Wygenerowanie raportów z tej grupy umożliwia udzielenie informacji o bieżącym stanie systemu, na przykład o obecnej ilości zgłoszeń.

Raporty te mają charakter widoku - ponowne wygenerowanie raportu zawsze może dać inny rezultat.

RAPORTY METRYK SLA

Raporty SLA w zamkniętych zgłoszeniach pozwalają zapoznać się danymi metryk na zgłoszeniach, które zostały już zamknięte. Celem tych raportów jest badanie terminowości realizacji zadań wynikających z umowy SLA.

Raporty mają charakter archiwalny. Ponowne wygenerowanie raportu z tymi samymi argumentami da zawsze ten sam rezultat.

Raporty przebiegu metryk SLA pozwalają zapoznać się ze zdarzeniami występującymi w trakcie biegu metryki SLA. Celem tych raportów jest badanie przebiegu realizacji zadań wynikających z umowy SLA.

Raporty przekroczeń metryk SLA pozwalają zapoznać się ze zgłoszeniami, na których doszło do przekroczenia metryki SLA. Celem tych raportów jest diagnoza incydentów, gdy doszło do złamania

umowy SLA.

Daty w raportach odnoszą się do lokalnego czasu komputera, na którym zainstalowany jest Serwer Axence nVision® (usługa helpdesku).

10.7.2 Raporty dla zgłoszeń

10.7.2.1 Raporty zamkniętych zgłoszeń

Raporty generowane są dla zgłoszeń, których procesowanie już się zakończyło (one w postaci tylko do odczytu - nie można ich edytować). Wegenerowanie raportów z tej grupy umożliwia głównie kontrolę jakości obsługi zgłoszeń (w poszczególnych dniach, miesiącach, przez poszczególnych pracowników pomocy technicznej).

Raporty te mają charakter archiwalny i są niezmienne. Ponowne wygenerowanie raportu z tymi samymi argumentami da zawsze ten sam rezultat.

Raportowane dane:

Czas reakcji - czas od utworzenia zgłoszenia do pierwszego komentarza publicznego przez użytkownika w roli "administrator" lub "pomoc techniczna".

Czas pracy - czas pracy nad zgłoszeniem uzupełniony przez pracownika pomocy technicznej.

Średnia liczba komentarzy zgłaszającego - liczba komentarzy, których autorem jest zgłaszający podzielona na całkowitą liczbę zgłoszeń.

Podsumowująca **średnia czasowa** i **średnia komentarzy** jest liczona w sposób wagowy: *(liczba obiektów w rzędzie * wartość w rzędzie)/liczba wszystkich obiektów*

Warianty raportów zamkniętych zgłoszeń *(kliknij nazwę raportu, aby rozwinąć opis)*:

Dzienny

Raport pozwala na przekrojowe zapoznanie się ze szczegółami procesowania zgłoszeń na przestrzeni dni.

Argumenty:

Nazwa argumentu	Możliwe wartości	Typ wyboru	Domyślna wartość	Uwagi
Data zamknięcia do:	data (zakres: 1 dzień)	wskazanie daty	ostatni dzień ubiegłego miesiąca	blokada możliwości wyboru dnia bieżącego; **maksymalna odległość od daty początkowej: 100 dni**

Nazwa argumentu	Możliwe wartości	Typ wyboru	Domyślna wartość	Uwagi
Data zamknięcia od:	data (zakres: 1 dzień)	wskazanie daty	pierwszy dzień ubiegłego miesiąca	brak ograniczeń daty
Kategoria:	(dowolna), wielokrotny wybór z listy kategorii	wielokrotny wybór	(dowolna)	-
Obsługujący:	(dowolny), (brak), wielokrotny wybór z listy obsługujących	wielokrotny wybór	(dowolny)	-
Oddział:	(dowolny), (brak), wielokrotny z listy oddziałów	wielokrotny wybór	(dowolny)	-
Pokaż nieprzydzielone zgłoszenia:	prawda, fałsz	checkbox	prawda	-
Pokaż zgłoszenia bez oddziału:	prawda, fałsz	checkbox	prawda	-
Priorytet:	(dowolny), wielokrotny wybór z listy priorytetów	wielokrotny wybór	(dowolny)	-

Raportowane dane:

Przykład:

Dzień	Liczba zamkniętych zgłoszeń	Średni czas reakcji	Czas w statusie "Otwarte"		Czas w statusie "Oczekujące na odpowiedź"		Czas w statusie "Zawieszone"		Czas od otworzenia do zamknięcia		Czas pracy		Średnia liczba komentarzy zgłaszającego
			średni	łączny	średni	łączny	średni	łączny	średni	łączny	średni	łączny	
1 stycznia 2016	8	30 min	1 godz.	8 godz.	1 godz.	8 godz.	1 godz.	8 godz	1 godz.	8 godz	1 godz.	8 godz	3,5
2 stycznia 2016	10	45 min	1 godz.	8 godz.	1 godz.	8 godz.	1 godz.	8 godz.	1 godz.	8 godz.	1 godz.	8 godz.	4

			30 min	30 min	30 min	30 min	30 min	30 min	30 min	30 min	30 min	30 min	
3 stycznia 2016	12	15 min	30 min	7 godz. 30 min	7 godz. 30 min	7 godz. 30 min	30 min	7 godz. 30 min	30 min	7 godz. 30 min	30 min	7 godz. 30 min	4,5
średnia	**10**	**29 min**	**58 min**	**-**	**58 min**	**-**	**58 min**	**-**	**58 min**	**-**	**58 min**	**-**	**4,07**
suma	**30**	**-**	**-**	**24 godz.**	**-**	**24 godz.**	**-**	**24 godz.**	**-**	**24 godz.**	**-**	**24 godz.**	**-**

Reprezentacja graficzna:

Wykres: punktowy/liniowy liczby zamkniętych zgłoszeń od dnia.

Wykres: punktowy/liniowy średniego czasu reakcji od dnia.

Wykres: punktowy/liniowy średniego czasu w statusie "otwarty", "oczekujące na odp.", "zawieszone" od dnia.

Wykres: punktowy/liniowy średniego czasu od otworzenia do zamknięcia od dnia.

Wykres: punktowy/liniowy średniego czasu pracy od dnia.

Wykres: słupkowy łącznego czasu pracy od dnia.

Wykres: punktowy/liniowy średniej liczby komentarzy zgłaszającego od dnia.

Tygodniowy

Raport pozwala na przekrojowe zapoznanie się ze szczegółami procesowania zgłoszeń na przestrzeni tygodni.

Argumenty:

Nazwa argumentu	Możliwe wartości	Typ wyboru	Domyślna wartość	Uwagi
Data zamknięcia do:	data (zakres: 1 tydzień)	wskazanie daty	ostatni zakończony tydzień	blokada możliwości wyboru tygodnia bieżącego; **maksymalna odległość od daty początkowej: 15 tygodni** (105 dni)

Nazwa argumentu	Możliwe wartości	Typ wyboru	Domyślna wartość	Uwagi
Data zamknięcia od:	data (zakres: 1 tydzień)	wskazanie daty	cztery tygodnie wstecz od ostatniego zakończonego tygodnia	brak ograniczeń daty
Kategoria:	(dowolna), wielokrotny wybór z listy kategorii	wielokrotny wybór	(dowolna)	-
Obsługujący:	(dowolny), (brak), wielokrotny wybór z listy obsługujących	wielokrotny wybór	(dowolny)	-
Oddział:	(dowolny), (brak), wielokrotny z listy oddziałów	wielokrotny wybór	(dowolny)	-
Pokaż nieprzydzielone zgłoszenia:	prawda, fałsz	checkbox	prawda	-
Pokaż zgłoszenia bez oddziału:	prawda, fałsz	checkbox	prawda	-
Priorytet:	(dowolny), wielokrotny wybór z listy priorytetów	wielokrotny wybór	(dowolny)	-

Raportowane dane:

Przykład:

Tydzień	Liczba zamkniętych zgłoszeń	Średni czas reakcji	Czas w statusie "Otwarte"		Czas w statusie "Oczekujące na odpowiedź"		Czas w statusie "Zawieszone"		Czas od otworzenia do zamknięcia		Czas pracy		Średnia liczba komentarzy zgłaszającego
			średni	łączny	średni	łączny	średni	łączny	średni	łączny	średni	łączny	
4 stycznia 2016 - 10 stycznia	100	30 min	1 godz.	100 godz.	1 godz.	100 godz	1 godz.	100 godz	1 godz.	100 godz	1 godz.	100 godz	3,5

2016

11 stycznia 2016 - 17 stycznia 2016	150	45 min	1 godz. 30 min	200 godz.	1 godz. 30 min	200 godz.	1 godz. 30 min	200 godz.	1 godz. 30 min	200 godz.	1 godz. 30 min	200 godz.	4
18 stycznia 2016 - 24 stycznia 2016	200	15 min	30 min	150 godz.	30 min	150 godz.	30 min	150 godz.	30 min	150 godz.	30 min	150 godz.	4,5
średnia	**150**	**28 min 20 sek.**	**56 min 40 sek.**	**-**	**56 min 40 sek.**	**-**	**56 min 40 sek.**	**-**	**56 min 40 sek.**	**-**	**56 min 40 sek.**	**-**	**4,11**
suma	**450**	**-**	**-**	**450 godz.**	**-**	**450 godz.**	**-**	**450 godz.**	**-**	**450 godz.**	**-**	**450 godz.**	**-**

Reprezentacja graficzna:

Wykres: punktowy/liniowy liczby zamkniętych zgłoszeń od tygodnia.

Wykres: punktowy/liniowy średniego czasu reakcji od tygodnia.

Wykres: punktowy/liniowy średniego czasu w statusie "otwarty", "oczekujące na odp.", "zawieszone" od tygodnia.

Wykres: punktowy/liniowy średniego czasu od otworzenia do zamknięcia od tygodnia.

Wykres: punktowy/liniowy średniego czasu pracy od tygodnia.

Wykres: słupkowy łącznego czasu pracy od tygodnia.

Wykres: punktowy/liniowy średniej liczby komentarzy zgłaszającego od tygodnia.

Miesięczny

Raport pozwala na przekrojowe zapoznanie się ze szczegółami procesowania zgłoszeń na przestrzeni miesięcy.

Argumenty:

Nazwa argumentu	Możliwe wartości	Typ wyboru	Domyślna wartość	Uwagi
Data zamknięcia do:	data (zakres: 1 miesiąc)	wskazanie daty	ostatni zakończony miesiąc	blokada możliwości wyboru miesiąca bieżącego; **maksymalna odległość od daty początkowej: 3 miesiące**
Data zamknięcia od:	data (zakres: 1 miesiąc)	wskazanie daty	pierwszy miesiąc kwartału w którym znajduje się ostatni zakończony miesiąc	brak ograniczeń daty
Kategoria:	(dowolna), wielokrotny wybór z listy kategorii	wielokrotny wybór	(dowolna)	-
Obsługujący:	(dowolny), (brak), wielokrotny wybór z listy obsługujących	wielokrotny wybór	(dowolny)	-
Oddział:	(dowolny), (brak), wielokrotny z listy oddziałów	wielokrotny wybór	(dowolny)	-
Pokaż nieprzydzielone zgłoszenia:	prawda, fałsz	checkbox	prawda	-
Pokaż zgłoszenia bez oddziału:	prawda, fałsz	checkbox	prawda	-
Priorytet:	(dowolny), wielokrotny wybór z listy priorytetów	wielokrotny wybór	(dowolny)	-

Raportowane dane:

Przykład:

Miesiąc	Liczba zamkniętych zgłoszeń	Średni czas reakcji	Czas w statusie "Otwarte"		Czas w statusie "Oczekujące na odpowiedź"		Czas w statusie "Zawieszone"		Czas od otworzenia do zamknięcia		Czas pracy		Średnia liczba komentarzy zgłaszającego
			średni	łączny	średni	łączny	średni	łączny	średni	łączny	średni	łączny	
styczeń 2016	100	30 min	1 godz.	100 godz.	1 godz.	100 godz	1 godz.	100 godz	1 godz.	100 godz	1 godz.	100 godz	3,5
luty 2016	150	45 min	1 godz. 30 min	200 godz.	1 godz. 30 min	200 godz.	1 godz. 30 min	200 godz.	1 godz. 30 min	200 godz.	1 godz. 30 min	200 godz.	4
marzec 2016	200	15 min	30 min	150 godz.	30 min	150 godz.	30 min	150 godz.	30 min	150 godz.	30 min	150 godz.	4,5
średnia	**150**	**28 min 20 sek.**	**56 min 40 sek.**	**-**	**56 min 40 sek.**	**-**	**56 min 40 sek.**	**-**	**56 min 40 sek.**	**-**	**56 min 40 sek.**	**-**	**4,11**
suma	**450**	**-**	**-**	**450 godz.**	**-**	**450 godz.**	**-**	**450 godz.**	**-**	**450 godz.**	**-**	**450 godz.**	**-**

Reprezentacja graficzna:

Wykres: punktowy/liniowy liczby zamkniętych zgłoszeń od miesiąca.

Wykres: punktowy/liniowy średniego czasu reakcji od miesiąca.

Wykres: punktowy/liniowy średniego czasu w statusie "otwarty", "oczekujące na odp.", "zawieszone" od miesiąca.

Wykres: punktowy/liniowy średniego czasu od otworzenia do zamknięcia od miesiąca.

Wykres: punktowy/liniowy średniego czasu pracy od miesiąca.

Wykres: słupkowy łącznego czasu pracy od miesiąca.

Wykres: punktowy/liniowy średniej liczby komentarzy zgłaszającego od miesiąca.

Porównawczy obsługujących

Raport pozwala na przekrojowe zapoznanie się ze szczegółami procesowania zgłoszeń przez każdego z pracowników pomocy technicznej.

Argumenty:

Nazwa argumentu	Możliwe wartości	Typ wyboru	Domyślna wartość	Uwagi
Data zamknięcia do:	data (zakres: 1 dzień)	wskazanie daty	ostatni dzień ubiegłego miesiąca	blokada możliwości wyboru miesiąca bieżącego; **maksymalna odległość od daty początkowej: 100 dni**
Data zamknięcia od:	data (zakres: 1 dzień)	wskazanie daty	pierwszy dzień ubiegłego miesiąca	brak ograniczeń daty
Kategoria:	(dowolna), wielokrotny wybór z listy kategorii	wielokrotny wybór	(dowolna)	-
Obsługujący:	(dowolny), (brak), wielokrotny wybór z listy obsługujących	wielokrotny wybór	(dowolny)	-
Oddział:	(dowolny), (brak), wielokrotny z listy oddziałów	wielokrotny wybór	(dowolny)	-
Pokaż nieprzydzielone zgłoszenia:	prawda, fałsz	checkbox	prawda	-
Pokaż zgłoszenia bez oddziału:	prawda, fałsz	checkbox	prawda	-
Priorytet:	(dowolny), wielokrotny wybór z listy priorytetów	wielokrotny wybór	(dowolny)	-

Raportowane dane:

Przykład:

Obsługujący	Liczba zamkniętych zgłoszeń	Średni czas reakcji	Czas w statusie "Otwarte"		Czas w statusie "Oczekujące na odpowiedź"		Czas w statusie "Zawieszone"		Czas od otworzenia do zamknięcia		Czas pracy		Średnia liczba komentarzy zgłaszającego
			średni	łączny	średni	łączny	średni	łączny	średni	łączny	średni	łączny	
Jan Kowalski	100	30 min	1 godz.	100 godz.	1 godz.	100 godz	1 godz.	100 godz	1 godz.	100 godz	1 godz.	100 godz	3,5
Piotr Nowak	150	45 min	1 godz. 30 min	200 godz.	1 godz. 30 min	200 godz.	1 godz. 30 min	200 godz.	1 godz. 30 min	200 godz.	1 godz. 30 min	200 godz.	4
Anna Nowak	200	15 min	30 min	150 godz.	30 min	150 godz.	30 min	150 godz.	30 min	150 godz.	30 min	150 godz.	4,5
suma	**450**	**-**	**-**	**450 godz.**	**-**	**450 godz.**	**-**	**450 godz.**	**-**	**450 godz.**	**-**	**450 godz.**	**-**

Obsługujący	Liczba zamkniętych zgłoszeń	Średni czas reakcji	Czas w statusie "Otwarte"		Czas w statusie "Oczekujące na odpowiedź"		Czas w statusie "Zawieszone"		Czas od otworzenia do zamknięcia		Czas pracy		Średnia liczba komentarzy zgłaszającego
			średni	łączny	średni	łączny	średni	łączny	średni	łączny	średni	łączny	
(nieprzydzielone zgłoszenia)	2	30 min	1 godz. 30 min	2 godz. 30 min	1 godz. 30 min	2 godz. 30 min	1 godz. 30 min	2 godz. 30 min	8 godz.	2 godz. 30 min	8 godz.	2 godz. 30 min	3,5

Reprezentacja graficzna:

Wykres: słupkowy liczby zamkniętych zgłoszeń od obsługującego + linia przerywana ze średnią wartością.

Wykres: słupkowy średniego czasu reakcji od obsługującego + linia przerywana ze średnią wartością.

Wykres: słupkowy średniego czasu w statusie "otwarty", "oczekujące na odp.", "zawieszone" od obsługującego.

Wykres: słupkowy średniego czasu od otworzenia do zamknięcia od obsługującego + linia przerywana ze średnią wartością.

Wykres: słupkowy łącznego czasu pracy od obsługującego + linia przerywana ze średnią wartością.

Wykres: słupkowy średniej liczby komentarzy zgłaszającego od obsługującego + linia przerywana ze średnią wartością.

Porównawczy priorytetów

Raport pozwala na przekrojowe zapoznanie się ze szczegółami procesowania zgłoszeń o poszczególnych priorytetach.

Argumenty:

Nazwa argumentu	Możliwe wartości	Typ wyboru	Domyślna wartość	Uwagi
Data zamknięcia do:	data (zakres: 1 dzień)	wskazanie daty	pierwszy dzień ubiegłego miesiąca	blokada możliwości wyboru miesiąca bieżącego; **maksymalna odległość od daty początkowej: 100 dni**
Data zamknięcia od:	data (zakres: 1 dzień)	wskazanie daty	ostatni dzień ubiegłego miesiąca	brak ograniczeń daty
Kategoria:	(dowolna), wielokrotny wybór z listy kategorii	wielokrotny wybór	(dowolna)	-
Obsługujący:	(dowolny), (brak), wielokrotny wybór z listy obsługujących	wielokrotny wybór	(dowolny)	-
Oddział:	(dowolny), (brak), wielokrotny z listy oddziałów	wielokrotny wybór	(dowolny)	-
Pokaż nieprzydzielone	prawda, fałsz	checkbox	prawda	-

Nazwa argumentu	Możliwe wartości	Typ wyboru	Domyślna wartość	Uwagi
zgłoszenia:				
Pokaż zgłoszenia bez oddziału:	prawda, fałsz	checkbox	prawda	-
Priorytet:	(dowolny), wielokrotny wybór z listy priorytetów	wielokrotny wybór	(dowolny)	-

Raportowane dane:

Przykład:

Priorytet	Liczba zamkniętych zgłoszeń	Średni czas reakcji	Czas w statusie "Otwarte"		Czas w statusie "Oczekujące na odpowiedź"		Czas w statusie "Zawieszone"		Czas od otworzenia do zamknięcia		Czas pracy		Średnia liczba komentarzy zgłaszającego
			średni	łączny	średni	łączny	średni	łączny	średni	łączny	średni	łączny	
Wysoki	100	30 min	1 godz.	100 godz.	1 godz.	100 godz	1 godz.	100 godz	1 godz.	100 godz	1 godz.	100 godz	3,5
Średni	150	45 min	1 godz. 30 min	200 godz.	1 godz. 30 min	200 godz.	1 godz. 30 min	200 godz.	1 godz. 30 min	200 godz.	1 godz. 30 min	200 godz.	4
Niski	200	15 min	30 min	150 godz.	30 min	150 godz.	30 min	150 godz.	30 min	150 godz.	30 min	150 godz.	4,5
suma	**450**	**-**	**-**	**450 godz.**	**-**	**450 godz.**	**-**	**450 godz.**	**-**	**450 godz.**	**-**	**450 godz.**	**-**

Reprezentacja graficzna:

Wykres: słupkowy liczby zamkniętych zgłoszeń od priorytetu + linia przerywana ze średnią wartością.

Wykres: słupkowy średniego czasu reakcji od priorytetu + linia przerywana ze średnią

wartością.

Wykres: słupkowy średniego czasu w statusie "otwarty", "oczekujące na odp.", "zawieszone" od priorytetu.

Wykres: słupkowy średniego czasu od otworzenia do zamknięcia od priorytetu + linia przerywana ze średnią wartością.

Wykres: słupkowy łącznego czasu pracy od priorytetu + linia przerywana ze średnią wartością.

Wykres: słupkowy średniej liczby komentarzy zgłaszającego od priorytetu + linia przerywana ze średnią wartością.

Porównawczy kategorii

Raport pozwala na przekrojowe zapoznanie się ze szczegółami procesowania zgłoszeń w poszczególnych kategoriach.

Argumenty:

Nazwa argumentu	Możliwe wartości	Typ wyboru	Domyślna wartość	Uwagi
Data zamknięcia do:	data (zakres: 1 dzień)	wskazanie daty	pierwszy dzień ubiegłego miesiąca	blokada możliwości wyboru miesiąca bieżącego; **maksymalna odległość od daty początkowej: 100 dni**
Data zamknięcia od:	data (zakres: 1 dzień)	wskazanie daty	ostatni dzień ubiegłego miesiąca	brak ograniczeń daty
Kategoria:	(dowolna), wielokrotny wybór z listy kategorii	wielokrotny wybór	(dowolna)	-
Obsługujący:	(dowolny), (brak), wielokrotny wybór z listy obsługujących	wielokrotny wybór	(dowolny)	-
Oddział:	(dowolny), (brak), wielokrotny z listy oddziałów	wielokrotny wybór	(dowolny)	-
Pokaż nieprzydzielone zgłoszenia:	prawda, fałsz	checkbox	prawda	-

Nazwa argumentu	Możliwe wartości	Typ wyboru	Domyślna wartość	Uwagi
Pokaż zgłoszenia bez oddziału:	prawda, fałsz	checkbox	prawda	-
Priorytet:	(dowolny), wielokrotny wybór z listy priorytetów	wielokrotny wybór	(dowolny)	-

Raportowane dane:

Przykład:

Kategoria	Liczba zamkniętych zgłoszeń	Średni czas reakcji	Czas w statusie "Otwarte"		Czas w statusie "Oczekujące na odpowiedź"		Czas w statusie "Zawieszone"		Czas od otworzenia do zamknięcia		Czas pracy		Średnia liczba komentarzy zgłaszającego
			średni	łączny	średni	łączny	średni	łączny	średni	łączny	średni	łączny	
Drukarki	100	30 min	1 godz.	100 godz.	1 godz.	100 godz	1 godz.	100 godz	1 godz.	100 godz	1 godz.	100 godz	3,5
Skanery	150	45 min	1 godz. 30 min	200 godz.	1 godz. 30 min	200 godz.	1 godz. 30 min	200 godz.	1 godz. 30 min	200 godz.	1 godz. 30 min	200 godz.	4
Monitory	200	15 min	30 min	150 godz.	30 min	150 godz.	30 min	150 godz.	30 min	150 godz.	30 min	150 godz.	4,5
suma	**450**	**-**	**-**	**450 godz.**	**-**	**450 godz.**	**-**	**450 godz.**	**-**	**450 godz.**	**-**	**450 godz.**	**-**

Reprezentacja graficzna:

Wykres: słupkowy liczby zamkniętych zgłoszeń od kategorii + linia przerywana ze średnią wartością.

Wykres: słupkowy średniego czasu reakcji od kategorii + linia przerywana ze średnią wartością.

Wykres: słupkowy średniego czasu w statusie "otwarty", "oczekujące na odp.", "zawieszone" od kategorii.

Wykres: słupkowy średniego czasu od otworzenia do zamknięcia od kategorii + linia przerywana ze średnią wartością.

Wykres: słupkowy łącznego czasu pracy od kategorii + linia przerywana ze średnią wartością.

Wykres: słupkowy średniej liczby komentarzy zgłaszającego od kategorii + linia przerywana ze średnią wartością.

Porównawczy oddziałów

Raport pozwala na przekrojowe zapoznanie się ze szczegółami procesowania zgłoszeń w poszczególnych oddziałach.

Argumenty:

Nazwa argumentu	Możliwe wartości	Typ wyboru	Domyślna wartość	Uwagi
Data zamknięcia do:	data (zakres: 1 dzień)	wskazanie daty	ostatni dzień ubiegłego miesiąca	blokada możliwości wyboru miesiąca bieżącego; **maksymalna odległość od daty początkowej: 100 dni**
Data zamknięcia od:	data (zakres: 1 dzień)	wskazanie daty	pierwszy dzień ubiegłego miesiąca	brak ograniczeń daty
Kategoria:	(dowolna), wielokrotny wybór z listy kategorii	wielokrotny wybór	(dowolna)	-
Obsługujący:	(dowolny), (brak), wielokrotny wybór z listy obsługujących	wielokrotny wybór	(dowolny)	-
Oddział:	(dowolny), (brak), wielokrotny z listy oddziałów	wielokrotny wybór	(dowolny)	-
Pokaż nieprzydzielone zgłoszenia:	prawda, fałsz	checkbox	prawda	-
Pokaż zgłoszenia	prawda, fałsz	checkbox	prawda	-

Nazwa argumentu	Możliwe wartości	Typ wyboru	Domyślna wartość	Uwagi
bez oddziału:				
Priorytet:	(dowolny), wielokrotny wybór z listy priorytetów	wielokrotny wybór	(dowolny)	-

Raportowane dane:

Przykład:

Oddział	Liczba zamkniętych zgłoszeń	Średni czas reakcji	Czas w statusie "Otwarte"		Czas w statusie "Oczekujące na odpowiedź"		Czas w statusie "Zawieszone"		Czas od otworzenia do zamknięcia		Czas pracy		Średnia liczba komentarzy zgłaszającego
			średni	łączny	średni	łączny	średni	łączny	średni	łączny	średni	łączny	
Oddział Warszawa	100	30 min	1 godz.	100 godz.	1 godz.	100 godz	1 godz.	100 godz	1 godz.	100 godz	1 godz.	100 godz	3,5
Oddział Wrocław	150	45 min	1 godz. 30 min	200 godz.	1 godz. 30 min	200 godz.	1 godz. 30 min	200 godz.	1 godz. 30 min	200 godz.	1 godz. 30 min	200 godz.	4
Oddział Kraków	200	15 min	30 min	150 godz.	30 min	150 godz.	30 min	150 godz.	30 min	150 godz.	30 min	150 godz.	4,5
suma	**450**	**-**	**-**	**450 godz.**	**-**	**450 godz.**	**-**	**450 godz.**	**-**	**450 godz.**	**-**	**450 godz.**	**-**

Oddział	Liczba zamkniętych zgłoszeń	Średni czas reakcji	Czas w statusie "Otwarte"	Czas w statusie "Oczekujące na odpowiedź"	Czas w statusie "Zawieszone"	Czas od otworzenia do zamknięcia	Czas pracy	Średnia liczba komentarzy zgłaszającego

			średni	łączny	średni	łączny	średni	łączny	średni	łączny	średni	łączny	
(zgłoszenia bez oddziału)	2	30 min	1 godz. 30 min	2 godz. 30 min	1 godz. 30 min	2 godz. 30 min	1 godz. 30 min	2 godz. 30 min	8 godz.	2 godz. 30 min	8 godz.	2 godz. 30 min	3,5

Reprezentacja graficzna:

Wykres: słupkowy liczby zamkniętych zgłoszeń od oddziału + linia przerywana ze średnią wartością.

Wykres: słupkowy średniego czasu reakcji od oddziału + linia przerywana ze średnią wartością.

Wykres: słupkowy średniego czasu w statusie "otwarty", "oczekujące na odp.", "zawieszone" od oddziału.

Wykres: słupkowy średniego czasu od otworzenia do zamknięcia od oddziału + linia przerywana ze średnią wartością.

Wykres: słupkowy łącznego czasu pracy od oddziału + linia przerywana ze średnią wartością.

Wykres: słupkowy średniej liczby komentarzy zgłaszającego od oddziału + linia przerywana ze średnią wartością.

10.7.2.2 Raporty aktywności

Raporty podsumowują liczbę zdarzeń w systemie w zadanym okresie.Wygenerowanie raportów z tej grupy umożliwia udzielenie informacji o rzędach wielkości danych, które przepływają przez system.

Raporty te mają charakter archiwalny i są niezmienne. Ponowne wygenerowanie raportu z tymi samymi argumentami da zawsze ten sam rezultat.

Warianty raportów aktywności *(kliknij nazwę raportu, aby rozwinąć opis)*:

Dzienny czasu reakcji

Raport pozwala na zapoznanie się ze statystykami dotyczącymi czasu reakcji na przestrzeni dni, dla zgłoszeń w których pierwsza reakcja pracownika pomocy technicznej nastąpiła w zdefiniowanym okresie.

Argumenty:

Nazwa argumentu	Możliwe wartości	Typ wyboru	Domyślna wartość	Uwagi
Data reakcji do:	data (zakres: 1 dzień)	wskazanie daty	ostatni dzień ubiegłego	blokada możliwości wyboru dnia bieżącego; **maksymalna**

Nazwa argumentu	Możliwe wartości	Typ wyboru	Domyślna wartość	Uwagi
			miesiąca	**odległość od daty początkowej: 100 dni**
Data reakcji od:	data (zakres: 1 dzień)	wskazanie daty	pierwszy dzień ubiegłego miesiąca	brak ograniczeń daty
Użytkownik dokonujący pierwszej reakcji:	(dowolny), wielokrotny wybór z listy użytkowników	wielokrotny wybór	(dowolny)	Lista jest zawężona do użytkowników mających rolę "administrator" lub "pomoc techniczna".

Raportowane dane:

Czas reakcji : czas od utworzenia zgłoszenia do pierwszego komentarza publicznego przez użytkownika w roli "administrator" lub "pomoc techniczna".

Podsumowująca **średnia czasu reakcji** jest liczona w sposób wagowy: *((liczba obiektów w rzędzie * wartość w rzędzie)/liczba wszystkich obiektów).*

Przykład:

Dzień	Liczba zgłoszeń, w których wystąpiła pierwsza reakcja	Liczba zgłoszeń z czasem reakcji				Czas reakcji	
		do 1 godz. włącznie	powyżej 1 godz. i do 8 godz. włącznie	powyżej 8 godz. i do 24 godz. włącznie	powyżej 24 godz.	średni	maksymalny
1 stycznia 2016	20	6	10	3	1	50 min	2 godz.
2 stycznia 2016	43	12	20	9	2	1 godz.	2 godz. 20 min
3 stycznia 2016	14	3	5	6	0	1 godz. 10 min	1 godz. 40 min
średnia	**25,67**	**7**	**11,67**	**6**	**1**	**59 min 13 sek**	**-**
suma	**77**	**21**	**35**	**18**	**3**	**-**	**-**

Reprezentacja graficzna:

Wykres: punktowy/liniowy liczby zgłoszeń w których nastąpiła pierwsza reakcja od dnia.

Wykres: punktowy/liniowy liczby zgłoszeń z czasem reakcji do 1 godz., 1-8 godz., 8-24 godz., powyżej 24 godz. od dnia.

Wykres: punktowy/liniowy średniego czasu reakcji od dnia.

Tygodniowy czasu reakcji

Raport pozwala na zapoznanie się ze statystykami dotyczącymi czasu reakcji na przestrzeni tygodni, dla zgłoszeń w których pierwsza reakcja pracownika pomocy technicznej nastąpiła w zdefiniowanym okresie.

Argumenty:

Nazwa argumentu	Możliwe wartości	Typ wyboru	Domyślna wartość	Uwagi
Data reakcji do:	data (zakres: 1 tydzień)	wskazanie daty	ostatni zakończony tydzień	blokada możliwości wyboru dnia bieżącego; **maksymalna odległość od daty początkowej: 15 tygodni** (105 dni)
Data reakcji od:	data (zakres: 1 tydzień)	wskazanie daty	cztery tygodnie wstecz od ostatniego zakończonego tygodnia	brak ograniczeń daty
Użytkownik dokonujący pierwszej reakcji:	(dowolny), wielokrotny wybór z listy użytkownikó	wielokrotny wybór	(dowolny)	Lista jest zawężona do użytkowników mających rolę "administrator" lub "pomoc techniczna".

Raportowane dane:

Czas reakcji : czas od utworzenia zgłoszenia do pierwszego komentarza publicznego przez użytkownika w roli "administrator" lub "pomoc techniczna".

Podsumowująca **średnia czasu reakcji** jest liczona w sposób wagowy: *((liczba obiektów w rzędzie * wartość w rzędzie)/liczba wszystkich obiektów).*

Przykład:

Tydzień	Liczba zgłoszeń, w których wystąpiła pierwsza reakcja	Liczba zgłoszeń z czasem reakcji				Czas reakcji	
		do 1 godz. włącznie	powyżej 1 godz. i do 8 godz. włącznie	powyżej 8 godz. i do 24 godz. włącznie	powyżej 24 godz.	średni	maksymalny
4 stycznia 2016 - 10 stycznia 2016	20	6	10	3	1	50 min	2 godz.
11 stycznia 2016 - 17 stycznia 2016	43	12	20	9	2	1 godz.	2 godz. 20 min
18 stycznia 2016 - 24 stycznia 2016	14	3	5	6	0	1 godz. 10 min	1 godz. 40 min
średnia	**25,67**	**7**	**11,67**	**6**	**1**	**59 min 13 sek**	**-**
suma	**77**	**21**	**35**	**18**	**3**	**-**	**-**

Reprezentacja graficzna:

Wykres: punktowy/liniowy liczby zgłoszeń w których nastąpiła pierwsza reakcja od tygodnia.

Wykres: punktowy/liniowy liczby zgłoszeń z czasem reakcji do 1 godz., 1-8 godz., 8-24 godz., powyżej 24 godz. od tygodnia.

Wykres: punktowy/liniowy średniego czasu reakcji od tygodnia.

Miesięczny czasu reakcji

Raport pozwala na zapoznanie się ze statystykami dotyczącymi czasu reakcji na przestrzeni miesięcy, dla zgłoszeń w których pierwsza reakcja pracownika pomocy technicznej nastąpiła w zdefiniowanym okresie.

Argumenty:

Nazwa argumentu	Możliwe wartości	Typ wyboru	Domyślna wartość	Uwagi
Data reakcji do:	data (zakres: 1 miesiąc)	wskazanie daty	pierwszy miesiąc kwartału w którym znajduje się ostatni zakończony miesiąc	blokada możliwości wyboru dnia bieżącego; **maksymalna odległość od daty początkowej: 3 miesiące**
Data reakcji od:	data (zakres: 1 miesiąc)	wskazanie daty	ostatni zakończony miesiąc	brak ograniczeń daty
Użytkownik dokonujący pierwszej reakcji:	(dowolny), wielokrotny wybór z listy użytkownikó	wielokrotny wybór	(dowolny)	Lista jest zawężona do użytkowników mających rolę "administrator" lub "pomoc techniczna".

Raportowane dane:

Czas reakcji : czas od utworzenia zgłoszenia do pierwszego komentarza publicznego przez użytkownika w roli "administrator" lub "pomoc techniczna".

Podsumowująca **średnia czasu reakcji** jest liczona w sposób wagowy: *((liczba obiektów w rzędzie * wartość w rzędzie)/liczba wszystkich obiektów).*

Przykład:

Miesiąc	Liczba zgłoszeń, w których wystąpiła pierwsza reakcja	Liczba zgłoszeń z czasem reakcji				Czas reakcji	
		do 1 godz. włącznie	powyżej 1 godz. i do 8 godz. włącznie	powyżej 8 godz. i do 24 godz. włącznie	powyżej 24 godz.	średni	maksymalny
styczeń 2016	200	60	100	30	10	50 min	2 godz.
luty 2016	430	120	200	90	20	1 godz.	2 godz. 20 min
marzec 2016	140	30	50	60	0	1 godz. 10 min	1 godz. 40 min
średnia	**256,67**	**70**	**116,7**	**60**	**10**	**59 min 13 sek**	**-**
suma	**770**	**210**	**350**	**180**	**30**	**-**	**-**

Reprezentacja graficzna:

Wykres: punktowy/liniowy liczby zgłoszeń w których nastąpiła pierwsza reakcja od miesiąca.

Wykres: punktowy/liniowy liczby zgłoszeń z czasem reakcji do 1 godz., 1-8 godz., 8-24 godz., powyżej 24 godz. od miesiąca.

Wykres: punktowy/liniowy średniego czasu reakcji od miesiąca.

Sumaryczny liczby zdarzeń

Raport pozwala na zapoznanie się z liczbowymi statystykami zdarzeń w formie podsumowania.

Argumenty:

Nazwa argumentu	Możliwe wartości	Typ wyboru	Domyślna wartość	Uwagi
Data aktywności do:	data (zakres: 1 dzień)	wskazanie daty	dzień wczorajszy	blokada możliwości wyboru dnia bieżącego; brak ograniczeń na maksymalną odległość od daty początkowej.
Data aktywności od:	data (zakres: 1 dzień)	wskazanie daty	wcześniejsza data z następujących: • dzień instalacji/ migracji systemu (data zerowa) • dzień wczorajszy	brak ograniczeń daty

Raportowane dane:

Przykład:

Miesiąc	Liczba utworzonych zgłoszeń		Łączna liczba utworzonych zgłoszeń	Łączna liczba zamkniętych zgłoszeń	Liczba utworzonych komentarzy		
	z interfejs	z interfejs			publicznych	wewnętrznych	łącznie

	u aplikacji	u aplikacji					
Liczba	500	1500	2000	1800	3500	4000	6500
Średnio na dzień	1,37	4,11	5,48	4,93	9,59	10,96	17,81

Reprezentacja graficzna:

Wykres: kołowy sumy utworzonych zgłoszeń z wiadomości e-mail i z interfejsu aplikacji.

Wykres: słupkowy sumy utworzonych zgłoszeń i zamkniętych zgłoszeń.

Wykres: kołowy sumy komentarzy publicznych i komentarzy wewnętrznych.

Porównawczy aktywności użytkowników

Raport pozwala na zapoznanie się z liczbowymi statystykami aktywności użytkowników w zadanym okresie.

Argumenty:

Nazwa argumentu	Możliwe wartości	Typ wyboru	Domyślna wartość	Uwagi
Data aktywności do:	data (zakres: 1 dzień)	wskazanie daty	ostatni dzień ubiegłego miesiąca	blokada możliwości wyboru dnia bieżącego; **maksymalna odległość od daty początkowej: 100 dni**
Data aktywności od:	data (zakres: 1 dzień)	wskazanie daty	pierwszy dzień ubiegłego miesiąca	brak ograniczeń daty
Użytkownik dokonujący pierwszej reakcji:	(dowolny), wielokrotny wybór z listy użytkownikó	wielokrotny wybór	(dowolny)	Lista jest zawężona do użytkowników mających rolę "administrator" lub "pomoc techniczna".

Raportowane dane:

Zgłoszenia przy których pracował użytkownik: zbiór unikalnych zgłoszeń przy których użytkownik wykonał w zadanym okresie jakąś akcję (edycja zgłoszenia, dowolny komentarz).

Podsumowująca **średnia czasu reakcji** jest liczona w sposób wagowy: *((liczba obiektów w rzędzie * wartość w rzędzie)/liczba wszystkich obiektów).*

Przykład:

Użytkownik	Komentarze publiczne		Komentarze publiczne i wewnętrzne		Zgłoszenia, przy których pracował użytkownik	
	liczba	średnia na dzień	liczba	średnia na dzień	liczba	średnia na dzień
Jan Kowalski	15	5	25	8,33	10	3,33
Piotr Nowak	25	8,33	35	11,67	9	3
Anna Nowak	20	6,67	30	10	11	3,67
suma	**60**		**90**		**30**	

Reprezentacja graficzna:

Wykres: słupkowy liczby komentarzy publicznych od użytkownika + linia przerywana ze średnią wartością.

Wykres: słupkowy liczby komentarzy publicznych i wewnętrznych od użytkownika + linia przerywana ze średnią wartością.

Wykres: słupkowy liczby zgłoszeń przy których pracował użytkownik + linia przerywana ze średnią wartością.

Wykres: słupkowy średniej na dzień komentarzy publicznych od użytkownika + linia przerywana ze średnią wartością.

Wykres: słupkowy średniej na dzień komentarzy publicznych i wewnętrznych od użytkownika + linia przerywana ze średnią wartością.

Wykres: słupkowy średniej na dzień zgłoszeń przy których pracował użytkownik + linia przerywana ze średnią wartością.

Raport porównawczy osób dokonujących pierwszej reakcji

Raport pozwala na porównanie czasu reakcji poszczególnych pracowników pomocy technicznej, dla zgłoszeń w których pierwsza reakcja nastąpiła w zdefiniowanym okresie.

Argumenty:

Nazwa argumentu	Możliwe wartości	Typ wyboru	Domyślna wartość	Uwagi
Data reakcji do:	data (zakres: 1 dzień)	wskazanie daty	ostatni dzień ubiegłego	blokada możliwości wyboru dnia bieżącego; **maksymalna**

Nazwa argumentu	Możliwe wartości	Typ wyboru	Domyślna wartość	Uwagi
			miesiąca	**odległość od daty początkowej: 100 dni**
Data reakcji od:	data (zakres: 1 dzień)	wskazanie daty	pierwszy dzień ubiegłego miesiąca	brak ograniczeń daty
Użytkownik dokonujący pierwszej reakcji:	(dowolny), wielokrotny wybór z listy użytkownikó	wielokrotny wybór	(dowolny)	Lista jest zawężona do użytkowników mających rolę "administrator" lub "pomoc techniczna".

Raportowane dane:

Czas reakcji : czas od utworzenia zgłoszenia do pierwszego komentarza publicznego przez użytkownika w roli "administrator" lub "pomoc techniczna".

Podsumowująca **średnia czasu reakcji** jest liczona w sposób wagowy: *((liczba obiektów w rzędzie * wartość w rzędzie)/liczba wszystkich obiektów).*

Przykład:

Użytkownik dokonujący pierwszej reakcji	Liczba zgłoszeń, w których wystąpiła pierwsza reakcja	Liczba zgłoszeń z czasem reakcji				Czas reakcji	
		do 1 godz. włącznie	powyżej 1 godz. i do 8 godz. włącznie	powyżej 8 godz. i do 24 godz. włącznie	powyżej 24 godz.	średni	maksymalny
Jan Kowalski	200	60	100	30	10	50 min	2 godz.
Piotr Nowak	430	120	200	90	20	1 godz.	2 godz. 20 min
Anna Nowak	140	30	50	60	0	1 godz. 10 min	1 godz. 40 min
suma	**770**	**210**	**350**	**180**	**30**	**-**	**-**

Reprezentacja graficzna:

Wykres: słupkowy liczby zgłoszeń od użytkownika który dokonał pierwszej reakcji + linia przerywana ze średnią wartością.

Wykres: słupkowy liczby zgłoszeń z czasem reakcji do 1 godz., 1-8 godz., 8-24 godz., powyżej 24 od użytkownika który dokonał pierwszej reakcji.

Wykres: słupkowy średniego czasu reakcji od użytkownika który dokonał pierwszej reakcji + linia przerywana ze średnią wartością.

10.7.2.3 Raporty aktualnie procesowanych zgłoszeń

Raporty prezentują dane dotyczące zgłoszeń, które są aktualnie procesowane w systemie. Wygenerowanie raportów z tej grupy umożliwia udzielenie informacji o bieżącym stanie systemu, na przykład o obecnej ilości zgłoszeń.

Raporty te mają charakter widoku - ponowne wygenerowanie raportu zawsze może dać inny rezultat.

Warianty raportów aktualnie procesowanych zgłoszeń *(kliknij nazwę raportu, aby rozwinąć opis)*:

Sumaryczny liczby zgłoszeń

Raport pozwala na zapoznanie się z właściwościami wszystkich aktualnie niezamkniętych zgłoszeń. Pozwala ocenić ich stan zaawansowania i czas przez który pozostają bez rozwiązania.

Argumenty:

Nazwa argumentu	Możliwe wartości	Typ wyboru	Domyślna wartość
Kategoria:	(dowolna), wielokrotny wybór z listy kategorii	wielokrotny wybór	(dowolna)
Obsługujący:	(dowolny), (brak), wielokrotny wybór z listy obsługujących	wielokrotny wybór	(dowolny)
Oddział:	(dowolny), (brak), wielokrotny z listy oddziałów	wielokrotny wybór	(dowolny)
Pokaż nieprzydzielone zgłoszenia:	prawda, fałsz	checkbox	prawda
Pokaż zgłoszenia bez oddziału:	prawda, fałsz	checkbox	prawda
Priorytet:	(dowolny), wielokrotny wybór z listy priorytetów	wielokrotny wybór	(dowolny)

Raportowane dane:

Pierwsza reakcja - dodanie pierwszego komentarza publicznego przez użytkownika w roli "administrator" lub "pomoc techniczna".

Przykład:

	Łączna liczba niezamkniętych zgłoszeń	Liczba zgłoszeń w statusie				Liczba zgłoszeń		Liczba zgłoszeń		Średni czas od utworzenia dla zgłoszeń bez pierwszej reakcji	Średni czas od utworzenia dla niezamkniętych zgłoszeń
		nowe	otwarte	oczekujące na odpowiedź	zawieszone	przypisanych do obsługującego	nieprzypisanych do żadnego obsługującego	bez pierwszej reakcji	ładla których pierwsza reakcja nastąpiła		
Liczba	40	5	10	20	5	38	2	7	33	30 min	1 godz. 10 min

Reprezentacja graficzna:

Wykres: słupkowy liczby zgłoszeń w statusie "nowy", "otwarty", "oczekujące na odpowiedź", "zawieszone".

Wykres: kołowy liczby zgłoszeń niezamkniętych nieprzypisanych i przypisanych do jakiegoś obsługującego.

Wykres: kołowy liczby zgłoszeń niezamkniętych bez pierwszej reakcji i takich dla których pierwsza reakcja już nastąpiła.

Porównawczy obsługujących zgłoszenia

Raport pozwala na zapoznanie się z aktualnym obłożeniem pracowników pomocy technicznej w systemie.

Argumenty:

Nazwa argumentu	Możliwe wartości	Typ wyboru	Domyślna wartość
Kategoria:	(dowolna), wielokrotny wybór z listy kategorii	wielokrotny wybór	(dowolna)
Obsługujący:	(dowolny), (brak), wielokrotny wybór z listy obsługujących	wielokrotny wybór	(dowolny)
Oddział:	(dowolny), (brak), wielokrotny z listy oddziałów	wielokrotny wybór	(dowolny)

Nazwa argumentu	Możliwe wartości	Typ wyboru	Domyślna wartość
Pokaż nieprzydzielone zgłoszenia:	prawda, fałsz	checkbox	prawda
Pokaż zgłoszenia bez oddziału:	prawda, fałsz	checkbox	prawda
Priorytet:	(dowolny), wielokrotny wybór z listy priorytetów	wielokrotny wybór	(dowolny)

Raportowane dane:

Pierwsza reakcja: dodanie pierwszego komentarza publicznego przez użytkownika w roli "administrator" lub "pomoc techniczna".

Podsumowująca **średnia czasowa** jest liczona w sposób wagowy: *((liczba obiektów w rzędzie * wartość w rzędzie)/liczba wszystkich obiektów).*

Przykład:

Obsługujący	Liczba niezamkniętych zgłoszeń	Liczba zgłoszeń w statusie				Liczba zgłoszeń bez pierwszej reakcji	Średni czas bez pierwszej reakcji	Średni czas od utworzenia zgłoszenia
		nowe	otwarte	oczekujące na odpowiedź	zawieszone			
Jan Kowalski	10	1	3	5	1	1	30 min	1 godz.
Piotr Nowak	19	1	5	10	3	2	45 min	1 godz. 30 min
Anna Nowak	5	0	1	3	1	0	-	30 min
średnia	**10**	**0,67**	**3**	**6**	**1,67**	**1**	**40 min**	**1 godz. 30 min**
suma	**30**	**2**	**9**	**18**	**5**	**2**	**-**	**-**

Obsługujący	Liczba niezamkniętych zgłoszeń	Liczba zgłoszeń w statusie				Liczba zgłoszeń bez pierwszej reakcji	Średni czas bez pierwszej reakcji	Średni czas od utworzenia zgłoszenia
		nowe	otwarte	oczekujące na odpowiedź	zawieszone			
(nieprzydzielone zgłoszenia)	1	1	0	0	0	0	-	10 min

Reprezentacja graficzna:

Wykres: słupkowy liczby niezamkniętych zgłoszeń od obsługującego + linia przerywana ze średnią wartością.

Wykres: słupkowy liczby zgłoszeń w statusie "nowe", "otwarte", "oczekujące na odpowiedź", "zawieszone" od obsługującego.

Wykres: słupkowy liczby zgłoszeń bez pierwszej reakcji od obsługującego + linia przerywana ze średnią wartością.

Wykres: słupkowy średniego czasu bez pierwszej reakcji od obsługującego + linia przerywana ze średnią wartością.

Wykres: słupkowy średniego czasu od utworzenia zgłoszenia od obsługującego + linia przerywana ze średnią wartością.

Porównawczy priorytetów

Raport pozwala na zapoznanie się z aktualną ilością i stanem nierozwiązanych zgłoszeń z określonym priorytetem.

Argumenty:

Nazwa argumentu	Możliwe wartości	Typ wyboru	Domyślna wartość
Kategoria:	(dowolna), wielokrotny wybór z listy kategorii	wielokrotny wybór	(dowolna)
Obsługujący:	(dowolny), (brak), wielokrotny wybór z listy obsługujących	wielokrotny wybór	(dowolny)
Oddział:	(dowolny), (brak), wielokrotny z listy oddziałów	wielokrotny wybór	(dowolny)

Nazwa argumentu	Możliwe wartości	Typ wyboru	Domyślna wartość
Pokaż nieprzydzielone zgłoszenia:	prawda, fałsz	checkbox	prawda
Pokaż zgłoszenia bez oddziału:	prawda, fałsz	checkbox	prawda
Priorytet:	(dowolny), wielokrotny wybór z listy priorytetów	wielokrotny wybór	(dowolny)

Raportowane dane:

Pierwsza reakcja: dodanie pierwszego komentarza publicznego przez użytkownika w roli "administrator" lub "pomoc techniczna".

Podsumowująca **średnia czasowa** jest liczona w sposób wagowy: *((liczba obiektów w rzędzie * wartość w rzędzie)/liczba wszystkich obiektów).*

Przykład:

Priorytet	Liczba niezamkniętych zgłoszeń	Liczba zgłoszeń w statusie				Liczba zgłoszeń bez pierwszej reakcji	Średni czas bez pierwszej reakcji	Średni czas od utworzenia zgłoszenia
		nowe	otwarte	oczekujące na odpowiedź	zawieszone			
Wysoki	10	1	3	5	1	1	30 min	1 godz.
Średni	19	1	5	10	3	2	45 min	1 godz. 30 min
Niski	5	0	1	3	1	0	-	30 min
średnia	**10**	**0,67**	**3**	**6**	**1,67**	**1**	**40 min**	**1 godz. 30 min**
suma	**30**	**2**	**9**	**18**	**5**	**2**	**-**	**-**

Reprezentacja graficzna:

Wykres: słupkowy liczby niezamkniętych zgłoszeń od priorytetu + linia przerywana ze średnią wartością.

Wykres: słupkowy liczby zgłoszeń w statusie "nowe", "otwarte", "oczekujące na odpowiedź", "zawieszone" od priorytetu.

Wykres: słupkowy liczby zgłoszeń bez pierwszej reakcji od priorytetu + linia przerywana ze

średnią wartością.

Wykres: słupkowy średniego czasu bez pierwszej reakcji od priorytetu + linia przerywana ze średnią wartością.

Wykres: słupkowy średniego czasu od utworzenia zgłoszenia od priorytetu + linia przerywana ze średnią wartością.

Porównawczy kategorii

Raport pozwala na zapoznanie się z aktualną ilością i stanem nierozwiązanych zgłoszeń w określonej kategorii.

Argumenty:

Nazwa argumentu	Możliwe wartości	Typ wyboru	Domyślna wartość
Kategoria:	(dowolna), wielokrotny wybór z listy kategorii	wielokrotny wybór	(dowolna)
Obsługujący:	(dowolny), (brak), wielokrotny wybór z listy obsługujących	wielokrotny wybór	(dowolny)
Oddział:	(dowolny), (brak), wielokrotny z listy oddziałów	wielokrotny wybór	(dowolny)
Pokaż nieprzydzielone zgłoszenia:	prawda, fałsz	checkbox	prawda
Pokaż zgłoszenia bez oddziału:	prawda, fałsz	checkbox	prawda
Priorytet:	(dowolny), wielokrotny wybór z listy priorytetów	wielokrotny wybór	(dowolny)

Raportowane dane:

Pierwsza reakcja: dodanie pierwszego komentarza publicznego przez użytkownika w roli "administrator" lub "pomoc techniczna".

Podsumowująca **średnia czasowa** jest liczona w sposób wagowy: *((liczba obiektów w rzędzie * wartość w rzędzie)/liczba wszystkich obiektów).*

Przykład:

Kategoria	Liczba niezamkniętych zgłoszeń	Liczba zgłoszeń w statusie				Liczba zgłoszeń bez pierwszej reakcji	Średni czas bez pierwszej reakcji	Średni czas od utworzenia zgłoszenia
		nowe	otwarte	oczekujące na odpowiedź	zawieszone			
Drukarki	10	1	3	5	1	1	30 min	1 godz.
Skanery	19	1	5	10	3	2	45 min	1 godz. 30 min
Monitory	5	0	1	3	1	0	-	30 min
średnia	**10**	**0,67**	**3**	**6**	**1,67**	**1**	**40 min**	**1 godz. 30 min**
suma	**30**	**2**	**9**	**18**	**5**	**2**	**-**	**-**

Reprezentacja graficzna:

Wykres: słupkowy liczby niezamkniętych zgłoszeń od kategorii + linia przerywana ze średnią wartością.

Wykres: słupkowy liczby zgłoszeń w statusie "nowe", "otwarte", "oczekujące na odpowiedź", "zawieszone" od kategorii.

Wykres: słupkowy liczby zgłoszeń bez pierwszej reakcji od kategorii + linia przerywana ze średnią wartością.

Wykres: słupkowy średniego czasu bez pierwszej reakcji od kategorii + linia przerywana ze średnią wartością.

Wykres: słupkowy średniego czasu od utworzenia zgłoszenia od kategorii + linia przerywana ze średnią wartością.

Porównawczy oddziałów

Raport pozwala na zapoznanie się z aktualną ilością i stanem nierozwiązanych zgłoszeń z określonym priorytetem.

Argumenty:

Nazwa argumentu	Możliwe wartości	Typ wyboru	Domyślna wartość
Kategoria:	(dowolna), wielokrotny wybór z listy kategorii	wielokrotny wybór	(dowolna)

Nazwa argumentu	Możliwe wartości	Typ wyboru	Domyślna wartość
Obsługujący:	(dowolny), (brak), wielokrotny wybór z listy obsługujących	wielokrotny wybór	(dowolny)
Oddział:	(dowolny), (brak), wielokrotny z listy oddziałów	wielokrotny wybór	(dowolny)
Pokaż nieprzydzielone zgłoszenia:	prawda, fałsz	checkbox	prawda
Pokaż zgłoszenia bez oddziału:	prawda, fałsz	checkbox	prawda
Priorytet:	(dowolny), wielokrotny wybór z listy priorytetów	wielokrotny wybór	(dowolny)

Raportowane dane:

Pierwsza reakcja: dodanie pierwszego komentarza publicznego przez użytkownika w roli "administrator" lub "pomoc techniczna".

Podsumowująca **średnia czasowa** jest liczona w sposób wagowy: *((liczba obiektów w rzędzie * wartość w rzędzie)/liczba wszystkich obiektów).*

Przykład:

Oddział	Liczba niezamkniętych zgłoszeń	Liczba zgłoszeń w statusie				Liczba zgłoszeń bez pierwszej reakcji	Średni czas bez pierwszej reakcji	Średni czas od utworzenia zgłoszenia
		nowe	otwarte	oczekujące na odpowiedź	zawieszone			
Oddział Warszawa	10	1	3	5	1	1	30 min	1 godz.
Oddział Wrocław	19	1	5	10	3	2	45 min	1 godz. 30 min
Oddział Kraków	5	0	1	3	1	0	-	30 min
średnia	**10**	**0,67**	**3**	**6**	**1,67**	**1**	**40 min**	**1 godz. 30 min**
suma	**30**	**2**	**9**	**18**	**5**	**2**	**-**	**-**

Oddział	Liczba niezamkniętych zgłoszeń	Liczba zgłoszeń w statusie				Liczba zgłoszeń bez pierwszej reakcji	Średni czas bez pierwszej reakcji	Średni czas od utworzenia zgłoszenia
		nowe	otwarte	oczekujące na odpowiedź	zawieszone			
(zgłoszenia bez oddziału)	1	1	0	0	0	0	-	10 min

Reprezentacja graficzna:

Wykres: słupkowy liczby niezamkniętych zgłoszeń od oddziału + linia przerywana ze średnią wartością.

Wykres: słupkowy liczby zgłoszeń w statusie "nowe", "otwarte", "oczekujące na odpowiedź", "zawieszone" od oddziału.

Wykres: słupkowy liczby zgłoszeń bez pierwszej reakcji od oddziału + linia przerywana ze średnią wartością.

Wykres: słupkowy średniego czasu bez pierwszej reakcji od oddziału + linia przerywana ze średnią wartością.

Wykres: słupkowy średniego czasu od utworzenia zgłoszenia od oddziału + linia przerywana ze średnią wartością.

10.7.3 Raporty dla metryk SLA

10.7.3.1 Raporty SLA w zamkniętych zgłoszeniach

Raporty SLA w zamkniętych zgłoszeniach pozwalają zapoznać się danymi metryk na zgłoszeniach, które zostały już zamknięte. Celem tych raportów jest badanie terminowości realizacji zadań wynikających z umowy SLA.

Raporty mają charakter archiwalny. Ponowne wygenerowanie raportu z tymi samymi argumentami da zawsze ten sam rezultat.

Raportowane dane

Raport uwzględnia wyłącznie metryki, które nie zostały unieważnione i które znajdują się na zgłoszeniach zamkniętych w określonym przedziale czasowym.

Zgłoszenia z SLA spełnionym - zlicza zgłoszenia zawierające metrykę, która nie została przekroczona i zakończyła bieg po wystąpieniu zdarzenia kończącego ją (pierwsza odpowiedź, zamknięcie zgłoszenia).

Zgłoszenia z SLA przekroczonym - zlicza zgłoszenia zawierające metrykę, która została

przekroczona i zakończyła bieg po wystąpieniu zdarzenia kończącego ją.

Spełnienie SLA (%) - liczba zgłoszeń na których metryka została spełniona / liczba wszystkich zgłoszeń na których wystąpiła metryka.

Przekroczenie SLA / średnie / maksymalne / łączne - jest to okres po momencie przekroczenia (jeżeli metryka została przekroczona o godzinę, to czas przekroczenia wynosi godzinę). Dotyczy wyłącznie okresu, kiedy metryka była aktywna. Bierze pod uwagę wszystkie przekroczone metryki (bez unieważnionych).

Średni czas pomiaru SLA - średni czas biegu wszystkich zakończonych metryk. Dotyczy wyłącznie okresu, kiedy metryka była aktywna.

Podsumowująca średnia czasowa jest liczona w sposób wagowy: ((liczba obiektów w rzędzie * wartość w rzędzie)/liczba wszystkich obiektów).

10.7.3.2 Raporty przebiegu metryk SLA

Raporty przebiegu metryk SLA pozwalają zapoznać się ze zdarzeniami występującymi w trakcie biegu metryki SLA. Celem tych raportów jest badanie przebiegu realizacji zadań wynikających z umowy SLA.

Raportowane dane

Raport nie zlicza metryk znajdujących się na zgłoszeniach usuniętych przez administratora.

Zgłoszenia objęte pomiarem SLA - zlicza zgłoszenia objęte metryką, gdzie objęcie zgłoszenia nastąpiło w przedziale czasowym raportu.

Zgłoszenia gdzie nastąpiło przekroczenie SLA - zlicza zgłoszenia, na których metryka została przekroczona, gdzie przekroczenie miało miejsce w przedziale czasowym raportu.

Zgłoszenia gdzie zakończono pomiar z SLA spełnionym - zlicza zgłoszenia zawierające metrykę, która nie została przekroczona i zakończyła bieg po wystąpieniu zdarzenia kończącego ją (pierwsza odpowiedź, zamknięcie zgłoszenia) w przedziale czasowym raportu.

Zgłoszenia gdzie zakończono pomiar z SLA przekroczonym - zlicza zgłoszenia zawierające metrykę, która została przekroczona i zakończyła bieg po wystąpieniu zdarzenia kończącego ją w przedziale czasowym raportu.

10.7.3.3 Raporty przekroczeń metryk SLA

Raporty przekroczeń metryk SLA pozwalają zapoznać się ze zgłoszeniami, na których doszło do przekroczenia metryki SLA. Celem tych raportów jest diagnoza incydentów, gdy doszło do złamania umowy SLA.

Raportowane dane

Raport zawiera po jednym wierszu na każde zgłoszenie w którym doszło do przekroczenia metryki.

Raport nie prezentuje zgłoszeń, na których znajdują się metryki unieważnione (nawet jeżeli zostały przekroczone). Raport nie prezentuje też zgłoszeń usuniętych przez administratora.

Przekroczenie SLA to okres po momencie przekroczenia (jeżeli metryka została przekroczona o godzinę, to przekroczenie wynosi godzinę). Dotyczy wyłącznie okresu, kiedy metryka była aktywna.

Jeżeli przekroczona metryka nie jest jeszcze zakończona lub zgłoszenie nie jest jeszcze

zamknięte, w komórce wyświetlana jest pusta wartość.

Raport nie wykonuje żadnych operacji agregujących i nie zawiera reprezentacji graficznej.

Jeżeli w zadanym zakresie czasowym na żadnym ze zgłoszeń nie doszło do przekroczenia SLA, zamiast tabelki, w interfejsie prezentowany jest komunikat: "Brak zgłoszeń na których przekroczono metrykę SLA.". Nie ma możliwości eksportu takiego raportu.

10.8 Plan nieobecności

Plan nieobecności to system do zgłaszania nieobecności dla Administratorów i Pracowników Helpdesku. *Celem tej funkcji jest planowanie odpowiedniego działania systemu zgłoszeń w przypadku nieobecności osoby rozwiązującej zgłoszenie.*

Plan nieobecności ***nie umożliwia*** *zarządzania urlopami rozumianego jako wyliczanie ilości dni urlopowych, jaka pozostała danemu pracownikowi do wykorzystania.*

Terminy nieobecności (dni oraz godziny rozpoczęcia / zakończenia) odnoszą się do lokalnego czasu komputera, na którym zainstalowany jest Serwer Axence nVision® (usługa helpdesku).

Aby dodać plan nieobecności zaloguj się do interfejsu helpdesku, przejdź do widoku **Plan nieobecności** i kliknij przycisk **Dodaj plan nieobecności** - wyświetlony zostanie kreator, który w prosty sposób pozwoli wybrać okres planowanej nieobecności.

Administratorzy mogą tworzyć plany nieobecności dla dowolnych pracowników helpdesku, natomiast zalogowany pracownik helpdesku może wskazać tylko własną nieobecność.

W kreatorze:

1. Z listy rozwijanej **wybierz lub wyszukaj nazwę pracownika helpdesku**, dla którego chcesz zaplanować nieobecność.
2. Korzystając z kalendarza **wskaż okres nieobecności pracownika.**
3. W kolejnym kroku **wybierz lub wyszukaj nazwę zastępcy** czyli osoby, która będzie otrzymywała powiadomienia o zmianach w zgłoszeniach przypisywanych do osoby nieobecnej. **Wybierz kolor**, którym okres nieobecności zostanie oznaczony w kalendarzu.

   W okresie, na który zaplanowana została nieobecność, zgłoszenia nadal przypisywane są do nieobecnego pracownika helpdesku (zgodnie z regułami przypisywania zgłoszeń i automatyzacjami) natomiast zastępca otrzymuje powiadomienia e-mail o nowych zgłoszeniach przypisanych do nieobecnego oraz komentarzach zgłaszajacych. Widzi on również wszystkie zgłoszenia przypisane do nieobecnego. Po zakończeniu okresu nieobecności, ustalone zastępstwo jest wyłączone a zastępca nie będzie otrzymywał wspomnianych powiadomień.

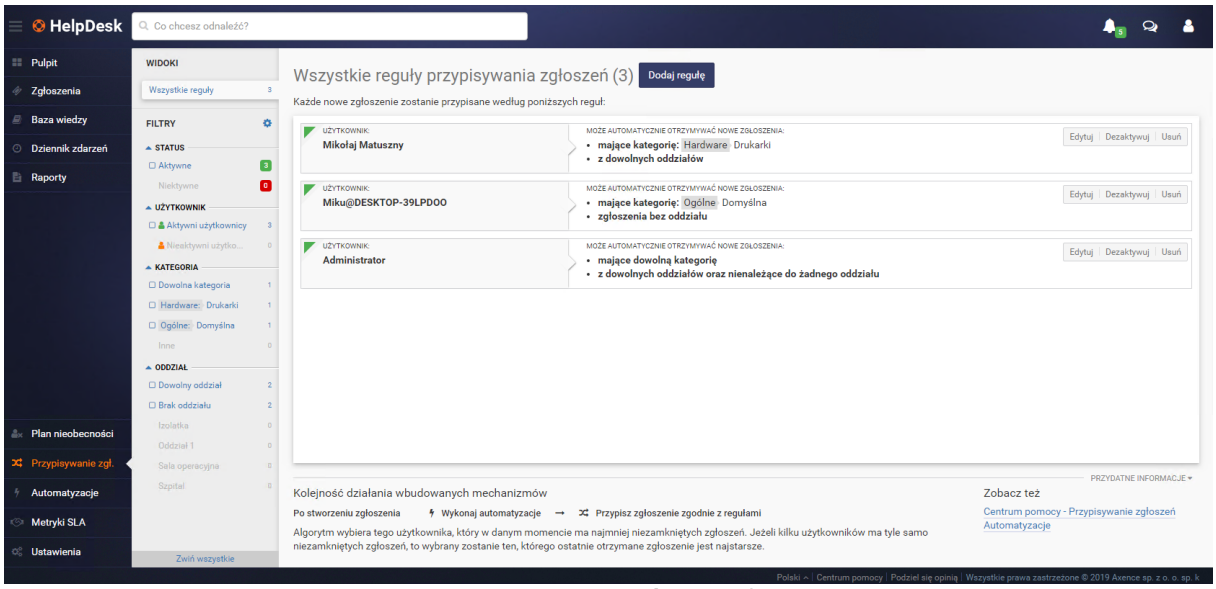
10.9 Przypisywanie zgłoszeń

Reguła przypisania może być zdefiniowana z poziomu interfejsu HelpDesk w widoku **Przypisywanie zgłoszeń**.

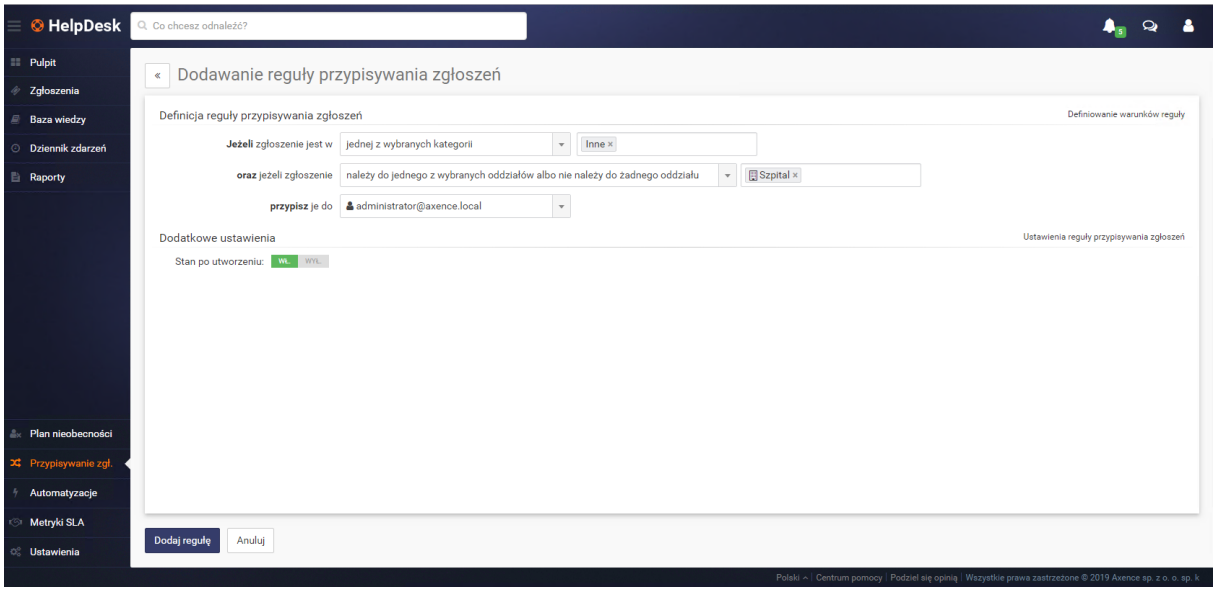
Aby zgłoszenia z danej kategorii były automatycznie przypisywane do wybranych pracowników pomocy

technicznej lub administratorów (typ HelpDesk lub Administrator):

1. W głównym widoku HelpDesku, wybierz z nawigacji po lewej stronie interfejsu opcję **Przypisywanie zgłoszeń**.
2. Kliknij w przycisk **Dodaj regułę** i zdefiniuj reguły przypisywania.
3. W sekcji **Dodatkowe ustawienia** zaznacz czy reguła ma być aktywna po utworzeniu.
4. Kliknij przycisk **Dodaj regułę** aby zapisać nową regułę.



Lista reguł przypisywania zgłoszeń w interfejsie HelpDesku.



Edycja reguły przypisywania zgłoszeń w interfejsie HelpDesku.

Powiązane tematy

Kategorie

Zarządzanie użytkownikami

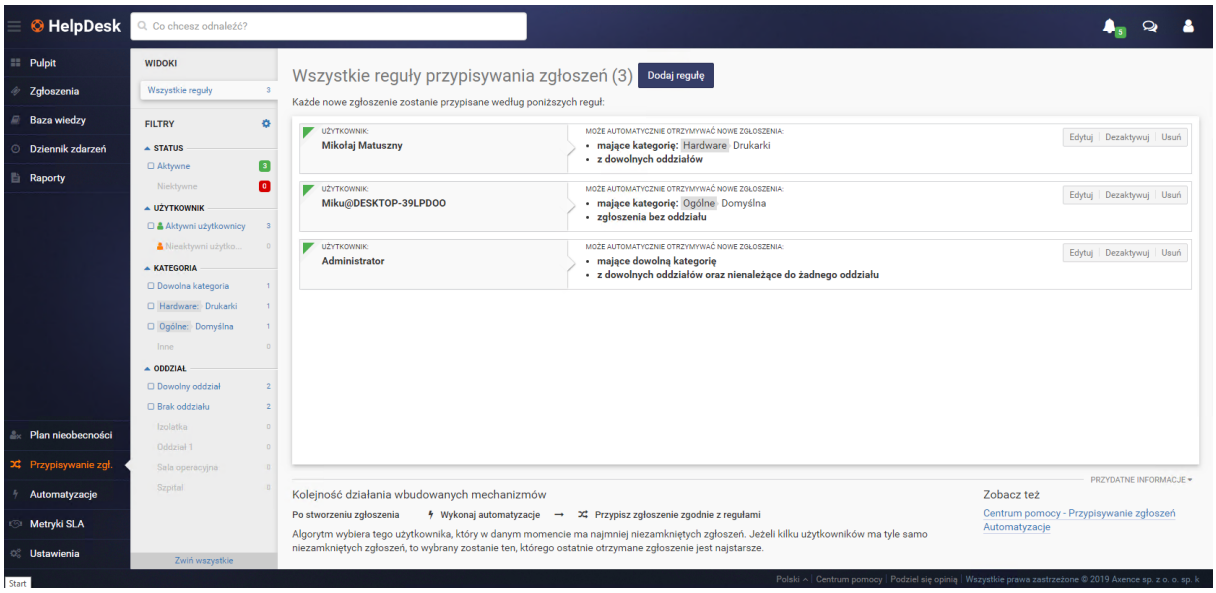
Zarządzanie i konfiguracja

10.10 Automatyzacje

10.10.1 Automatyzacje - wprowadzenie

Automatyzacje są zupełnie nową, przełomową funkcją w Axence nVision® HelpDesk. Ich celem jest odczuwalne zwiększenie szybkości realizacji zgłoszeń przez pracowników helpdesku. W scenariuszu codziennej pracy, występują regularnie powatrzające się czynności. Występują one pod wpływem określonych warunków i wywołują zdefiniowane w "workflow" akcje. Czynności te mogą zostać zautomatyzowane poprzez zastosowanie reguł automatycznych. Pozwala to na zmniejszenie czasu potrzebnego na sprawne procesowanie zgłoszeń, szybszą reakcję na występujące w sieci zdarzenia i usprawnienie procesów w organizacji.

Moduł HelpDesk został wyposażony w kilka wstępnie wbudowanych automatyzacji co ma na celu wprowadzenie administratora w konstrukcję tych mechanizmów.



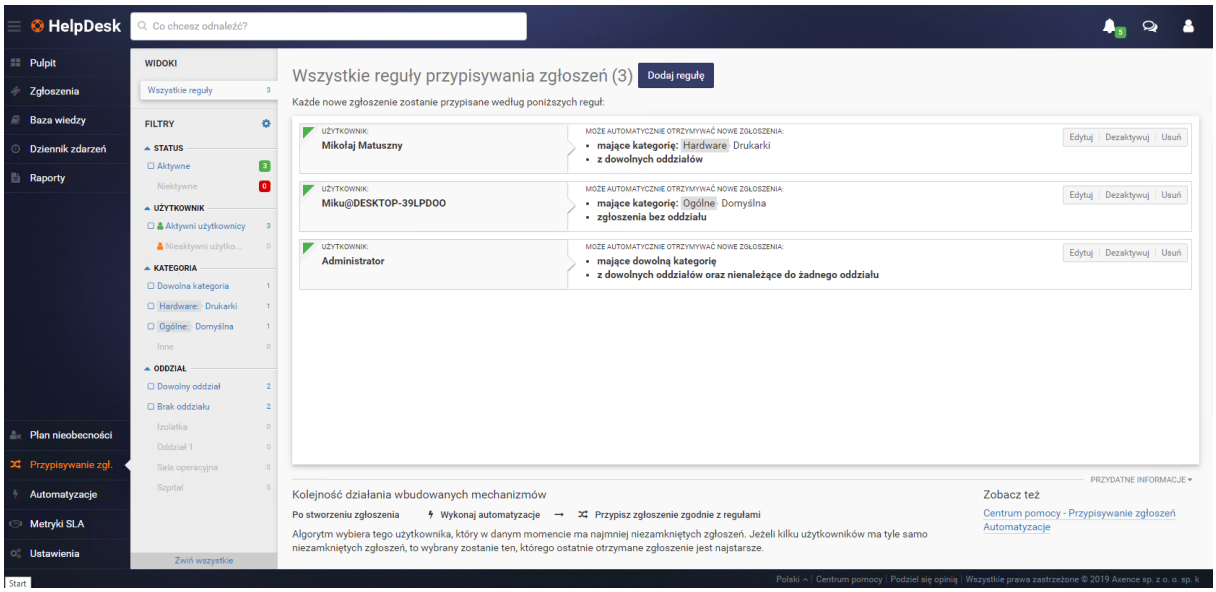
Lista automatyzacji.

10.10.2 Lista automatyzacji

Zdefiniowane reguły automatyzacji przedstawiane są w postaci listy, która prezentuje poszczególne reguły w postaci kafelek.

Pojedynczy kafelek reprezentujący określoną automatyzację zawiera:

- tytuł automatyzacji,
- akcje kontekstowe - pozwalają na edycję, zmianę statusu automatyzacji oraz jej usunięcie,
- status automatyzacji - w postaci paska w kolorze: czerwony - automatyzacja zdeaktywowana, zielony - automatyzacja aktywna,
- opis automatyzacji,
- wyzwalacz automatyzacji,
- listę warunków,
- listę akcji.



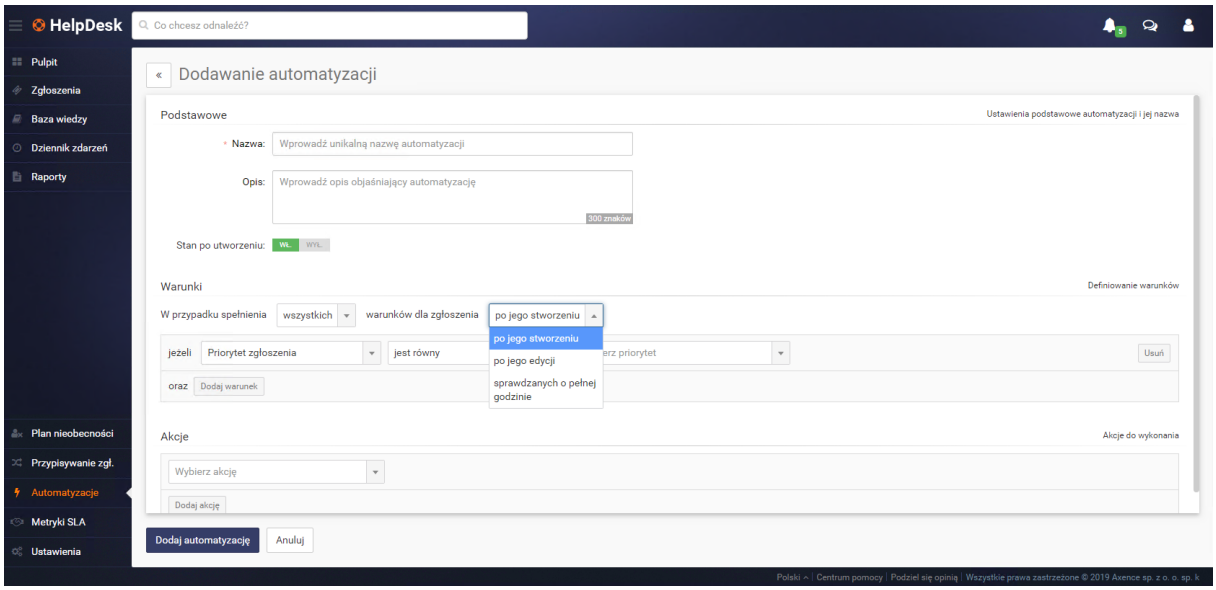
Lista automatyzacji.

W lewej części listy automatyzacji wyświetlany jest szybki widok, który w sprawny sposób pozwala odfiltrować automatyzacje ze względu na:

- stan:
  - aktywne,
  - zdeaktywowane,
- wyzwalacz:
  - wykonywane podczas tworzenia zgłoszenia,
  - wykonywane podczas aktualizacji zgłoszenia,
  - wykonywane codziennie.

10.10.3 Dodawanie automatyzacji

Widok dodawania automatyzacji pozwala na określenie warunków i akcji, które zostaną wykonane w określonej sytuacji.



Dodawanie nowej automatyzacji.

Aby dodać automatyzację:

1. Zaloguj się do interfejsu HelpDesk.
2. Z nawigacji głównej w lewej części interfejsu wybierz pozycję "Automatyzacje."
3. Na liście automatyzacji kliknij przycisk **Dodaj automatyzację.**
4. Wypełnij pola:

- **nazwa** - określ nazwę nowej automatyzacji,
- **opis** - możesz dodać krótki opis działania automatyzacji.

5. Określ status automatyzacji po utworzeniu.
6. Określ typ wyzwalacza automatyzacji - kiedy ma być wykonywana:

- codziennie - uruchamiana jest codzienna automatyczna procedura sprawdzania listy niezamkniętych zgłoszeń. W wyniku jej działania badane są zdefiniowane przez administratora warunki i podejmowane okreslone akcje. **Przykład:** *Ustaw status na "Zamknięte" dla zgłoszeń niezaktualizowanych przez 14 dni.*
- po utworzeniu nowego zgłoszenia,
- po edycji zgłoszenia.

7. Określ logikę złożenia warunku:

Możesz okreslić czy automatyzacja zostanie zastosowana gdy procesowane zgłoszenie spełni dowolny lub wszystkie z poniżej zdefiniowanych warunków.

Aby dodać kolejny warunek kliknij link **Dodaj warunek.**

8. Określ akcje, które mają zostać podjęte po spełnieniu przez zgłoszenie warunków:

Aby dodać kolejną akcję kliknij link **Dodaj akcję.**

9. Zapisz automatyzację poprzez kliknięcie przycisku **Dodaj automatyzację.**

10.10.4 Warunki automatyzacji

Należy budować możliwie jak najprostsze reguły automatyzacji.

Warunki automatyzacji dla nowego zgłoszenia:

Obiekt	Opcje warunku	Warunek
Temat zgłoszenia	zawiera przynajmniej jedno ze słów	wprowadź słowa oddzielone przecinkami
	nie zawiera któregoś ze słów	
	zawiera wszystkie następujące słowa	
Opis zgłoszenia	zawiera przynajmniej jedno ze słów	
	nie zawiera któregoś ze słów	
	zawiera wszystkie następujące słowa	
Priorytet zgłoszenia	jest równy	wybierz priorytet
	nie jest równy	
	jest wyższy lub równy	
	jest wyższy niż	
	jest niższy lub równy	
	jest niższy	
	jest domyślnym priorytetem	-
	nie jest domyślnym priorytetem	
Kategoria zgłoszenia	jest równą	wybierz kategorię
	nie jest równą	
	jest kategorią domyślną	-
	nie jest kategorią domyślną	
Osoba zgłaszająca	jest równa	wprowadź osobę zgłaszającą
	nie jest równa	
Powiązane urządzenie	jest równe	wprowadź nazwę urządzenia
	nie jest równe	
	jest ustawione	-
	nie jest ustawione	
Oddział powiązanego urządzenia	jest równy	wprowadź oddział
	nie jest równy	
	jest ustawiony	
	nie jest ustawiony	
Źródłem utworzenia zgłoszenia	jest nie jest	wprowadź źródło zgłoszenia
Osoba obsługująca	jest równa nie jest równa jest ustawiona nie jest ustawiona należy do grupy nie należy do grupy	wprowadź osobę obsługującą

Warunki automatyzacji dla aktualizowanego zgłoszenia:

Obiekt	Opcje warunku	Warunek
Temat zgłoszenia	został zmieniony	-
	nie został zmieniony	
	zawiera przynajmniej jedno ze słów	wprowdź słowa oddzielone przecinkami
	nie zawiera któregoś ze słów	
	zawiera wszystkie następujące słowa	
Status zgłoszenia	został zmieniony	-
	nie został zmieniony	
	został zmieniony na	Nowe Otwarte Oczekujące na odpowiedź Zawieszone Zamknięte
	został zmieniony na inny niż	
	został zmieniony z	
	został zmieniony z innego niż	
	jest równy	
	nie jest równy	
Priorytet zgłoszenia	został zmieniony	-
	nie został zmieniony	
	został zmieniony na wyższy lub równy	wybierz priorytet
	został zmieniony na wyższy niż	
	został zmieniony na niższy lub równy	
	został zmieniony na niższy niż	
	został zmieniony na domyślny	-
	został zmieniony na inny niż domyślny	
	został zmieniony na	wybierz priorytet
	został zmieniony na inny niż	
	został zmieniony z	
	został zmieniony z innego niż	
	jest równy	
	nie jest równy	
	jest wyższy lub równy	
	jest wyższy niż	
	jest niższy lub równy	
	jest niższy niż	
	jest domyślnym priorytetem	-
	nie jest domyślnym priorytetem	
Kategoria zgłoszenia	została zmieniona	-
	nie została zmieniona	
	została zmieniona na domyślną	

	została zmieniona na inną niż domyślna	wybierz kategorię
	została zmieniona na	
	została zmieniona na inną niż	
	została zmieniona z	
	została zmieniona z innej niż	
	jest równa	
	nie jest równa	
	jest domyślną kategorią	-
	nie jest domyślną kategorią	
Osoba zgłaszająca	została zmieniona	-
	nie została zmieniona	
	została zmieniona na	wprowadź osobę zgłaszającą
	została zmieniona na inną niż	
	została zmieniona z	
	została zmieniona z innej niż	
	jest równa	
	nie jest równa	
Powiązane urządzenie	zostało zmienione	-
	nie zostało zmienione	
	zostało zmienione na ustawione	
	zostało zmienione na nieustawione	
	zostało zmienione na	wprowadź nazwę urządzenia
	zostało zmienione na inne niż	
	zostało zmienione z	
	zostało zmienione z innego niż	
	jest równe	
	nie jest równe	
	jest ustawione	-
	nie jest ustawione	
Publiczny komentarz	został dodany	-
	nie został dodany	
	został dodany przez użytkownika mającego rolę	Administrator Helpdesk staff End-user
	nie został dodany przez użytkownika mającego rolę	
Wewnętrzny komentarz	został dodany	-
	nie został dodany	
	został dodany przez użytkownika mającego rolę	Administrator Pomoc Techniczna Użytkownik
	nie został dodany przez użytkownika mającego rolę	
Osoba aktualizująca	ma rolę	
	nie ma roli	

10.10.5 Akcje automatyzacji

Poniższe akcje mogą być wykonywane w wyniku spełnienia przez zgłoszenie jednego lub wielu warunków zdefiniowanych w regule automatyzacji:

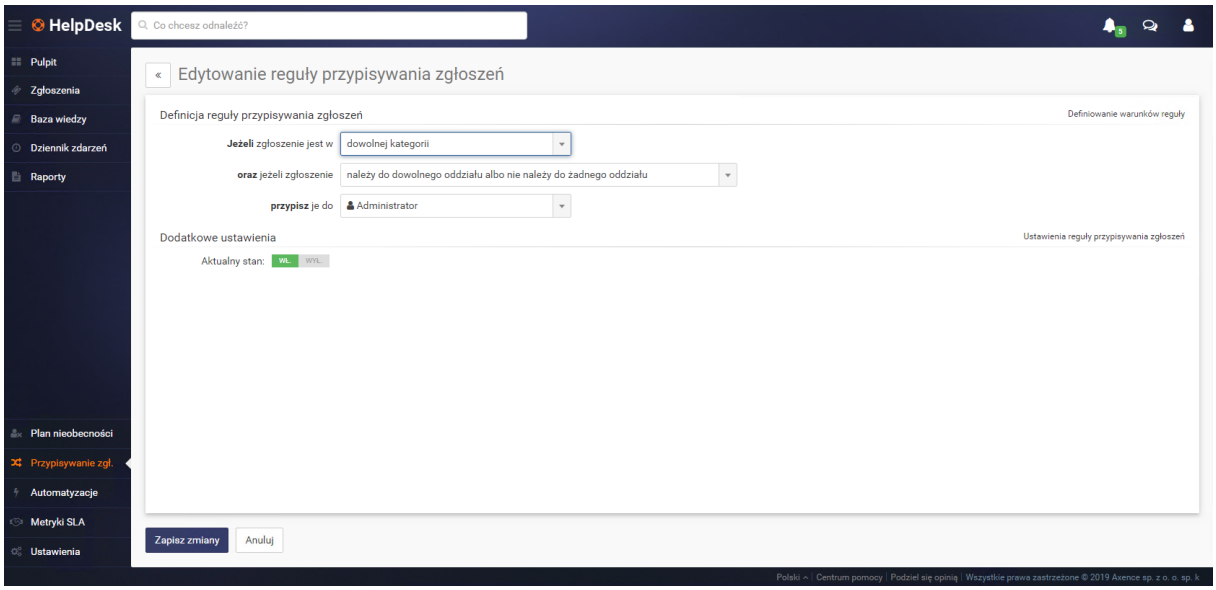
Akcja	Opis
Zmień kategorię	Zmienia kategorię zgłoszenia.
Zmień priorytet	Zmienia priorytet zgłoszenia.
Zmień status	Zmienia status zgłoszenia.
Przypisz powiązane urządzenie	Dodaje wskazane urządzenie jako powiązane w metryce zgłoszenia.
Dodaj tekst do tematu	Dodaje na początku tematu zgłoszenia zdefiniowany tekst, np. prefiks [Ważne].
Dodaj wewnętrzny komentarz	Dodaje zdefiniowany komentarz wewnętrzny w historii zgłoszenia.
Wyślij powiadomienie przez e-mail	Wysyła zdefiniowaną przez administratora (temat + treść) wiadomość e-mail na wskazany adres.
Dodaj do listy obserwujących	Dodaje wybranych użytkowników do listy obserwujących zgłoszenie

Akcje dostępne są w zależności od wybranych warunków automatyzacji.

10.10.6 Edycja automatyzacji

Aby edytować automatyzację:

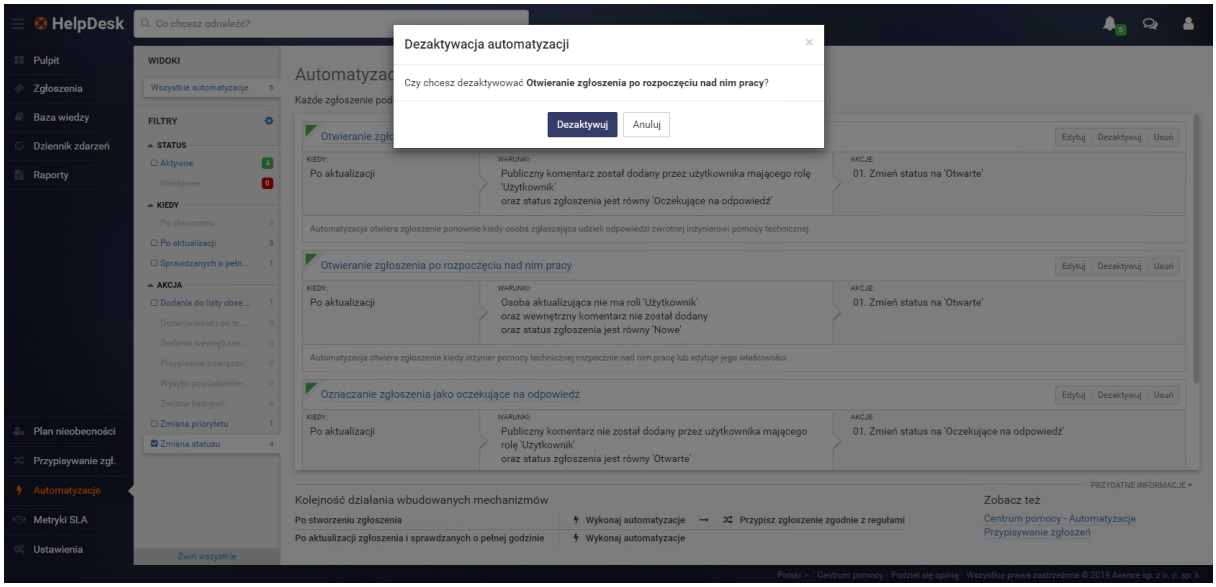
1. Zaloguj się do interfejsu HelpDesk.
2. Z nawigacji głównej w lewej części interfejsu wybierz pozycję **Automatyzacje**.
3. Na liście automatyzacji wyszukaj tę, którą chcesz edytować.
4. Z menu kontekstowego automatyzacji (prawy, górny róg kafelka) kliknij link **Edytuj**.
5. Zmień nazwę, opis, stan, warunki lub akcje automatyzacji podobnie jak podczas Dodawanie automatyzacji.
6. Zapisz zmiany poprzez kliknięcie przycisku **Zapisz zmiany.**



Edycja istniejącej automatyzacji.

10.10.7 Aktywacja/deaktywacja automatyzacji

Utworzone automatyzacje mogą być wyłączane (deaktywowane) na czas, kiedy mają nie mieć zastosowania w procesowaniu zgłoszeń, np. podczas urlopu pracownika. Nie ma konieczności usuwania reguły automatyzacji.



Zmiana stanu automatyzacji.

Aby deaktywować (lub aktywować) automatyzację:

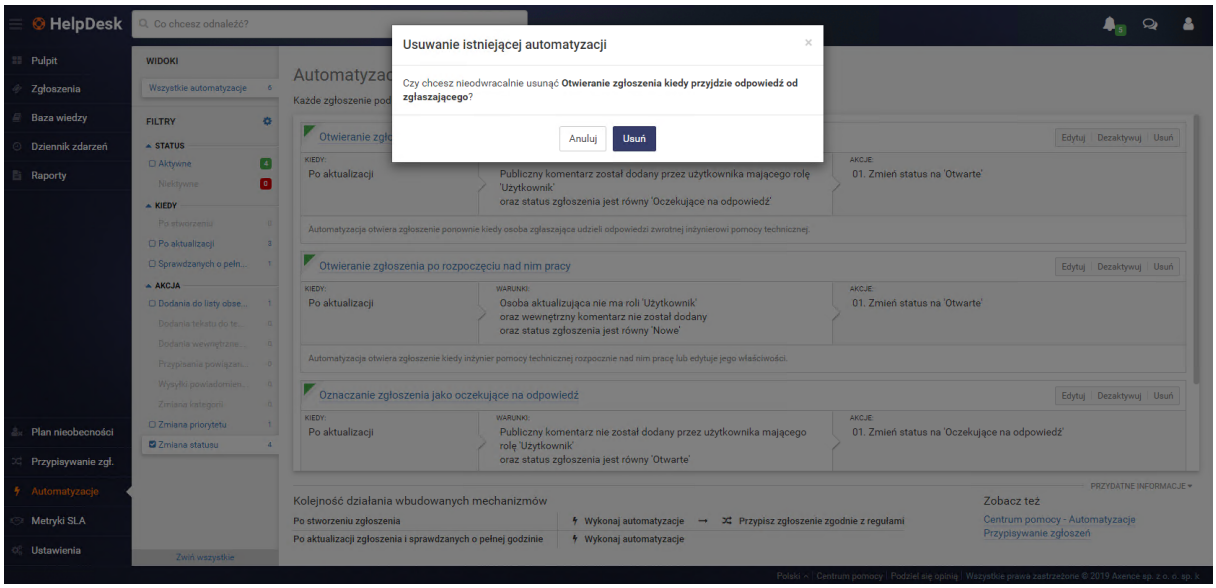
1. Zaloguj się do interfejsu HelpDesk.
2. Z nawigacji głównej w lewej części interfejsu wybierz pozycję **Automatyzacje**.
3. Na liście automatyzacji wyszukaj tę, której stan chcesz zmienić.
4. Z menu kontekstowego automatyzacji (prawy, górny róg kafelka) kliknij link **Dezaktywuj** (lub **Aktywuj** jesli automatyzacja jest już wyłączona).
5. Potwierdź akcję w oknie dialogowym poprzez kliknięcie przycisku **Dezaktywuj (Aktywuj).**

Reguła automatyzacji może być również włączona lub wyłączona poprzez zmianę statusu automatyzacji podczas jej edycji.

10.10.8 Usuwanie automatyzacji

Aby usunąć regułę automatyzacji:

1. Zaloguj się do interfejsu HelpDesk.
2. Z nawigacji głównej w lewej części interfejsu wybierz pozycję **Automatyzacje.**
3. Na liście automatyzacji wyszukaj tę, którą chcesz usunąć.
4. Z menu kontekstowego automatyzacji (prawy, górny róg kafelka) kliknij link **Usuń.**
5. Potwierdź usunięcie w oknie dialogowym poprzez kliknięcie przycisku **Usuń.**



Usuwanie automatyzacji.

10.11 Metryki SLA

Termin SLA (*Service Level Agreement*) określa umowę o gwarantowanym poziomie świadczenia usług. System HelpDesk umożliwia zdefiniowanie różnych metryk SLA pozwalających na monitorowanie, czy cele ustalone w umowie SLA są należycie realizowane.

Rozdział dotyczący realizacji postanowień umów gwarantowanego poziomu świadczenia usług podzielony został na artykuły:

- **Rodzaje metryk SLA**
- **Warunki metryk SLA**
- **Czas obowiązywania metryk SLA**
- **Tworzenie metryk SLA**
- **Złamanie SLA**
- **Metryki SLA na zgłoszeniach**

Powiązane tematy

Raporty SLA w zamkniętych zgłoszeniach

Raporty przebiegu metryk SLA

Raporty przekroczeń metryk SLA

10.11.1 Rodzaje metryk SLA

Każda metryka może przyjąć jeden z dwóch sposobów pomiaru czasu:

- ***Czas oczekiwania na pierwszą odpowiedź***

  Metryka rozpoczyna swój bieg w momencie utworzenia zgłoszenia.

  Metryka nieodwracalnie kończy swój bieg w momencie pojawienia się w zgłoszeniu pierwszego publicznego komentarza, którego autorem jest użytkownik mający rolę pracownika helpdesku lub administratora.

- ***Łączny czas oczekiwania na rozwiązanie zgłoszenia***

  Metryka rozpoczyna swój bieg w momencie utworzenia zgłoszenia.

  Metryka wstrzymuje swój bieg, gdy status zgłoszenia zostanie zmieniony na "oczekujące na odpowiedź" lub "zawieszone".

  Metryka wznawia (kontynuuje) swój bieg, gdy status zgłoszenia zostanie zmieniony na "otwarte".

  Metryka nieodwracalnie kończy swój bieg, gdy status zgłoszenia zostanie zmieniony na "zamknięte".

10.11.2 Warunki metryk SLA

W metryce SLA można zdefiniować rozbudowaną listę warunków dotyczących:

- priorytetu zgłoszenia (*jest równy / nie jest równy*),
- kategorii zgłoszenia (*jest równa / nie jest równa*),
- osoby zgłaszającej (*jest równa / nie jest równa / należy do grupy / nie należy do grupy*),
- osoby obsługującej (*jest równa / nie jest równa / należy do grupy / nie należy do grupy*),
- źródła zgłoszenia (*jest wiadomość e-mail / jest interfejs aplikacji web*).

Kolejne warunki mogą być połączone ze sobą wyłącznie spójnikiem logicznym "ORAZ" (spełnienie wszystkich warunków). Jeżeli w obrębie jednego warunku występuje kolekcja kilku możliwych wartości *N*, całość jest traktowana jako *N* warunków połączonych spójnikiem "LUB"/"ANI".

Aby zgłoszenie kwalifikowało się na wybraną metrykę SLA, musi spełniać wszystkie jej warunki w sposób ciągły. Jeżeli w wyniku zmiany właściwości (na przykład priorytetu) zgłoszenie przestaje spełniać warunki metryki, to przestaje być jednocześnie nią objęte. Metryka, która przestaje obejmować zgłoszenie kończy swój bieg, niezależnie czy została spełniona, czy nie.

Analogicznie - jeżeli zgłoszenie po zmianie właściwości kwalifikuje się na inne dodatkowe metryki, to zostaje ono nimi objęte. Jeżeli zgłoszenie zostaje objęte ponownie tą samą metryką, system traktuje to jako jej wznowienie a nie utworzenie kolejnej instancji metryki.

W szczególnym przypadku może to oznaczać, że po zmianie właściwości zgłoszenia, nowa metryka SLA będzie już przekroczona od momentu objęcia nią zgłoszenia.

Przykład:

W systemie obowiązują dwie metryki SLA:

1. Zgłoszenia z priorytetem "wysoki" mają być rozwiązywane w 4 godziny.

2. Zgłoszenia z priorytetem "krytyczny" mają być rozwiązywane w 2 godziny.

Zgłoszenie z priorytetem "wysoki" jest już procesowane godzinę. Jeżeli jego priorytet zostaje zmieniony na "krytyczny", przestaje być obejmowane pierwszą metryką i zaczyna być obejmowane drugą. Do jej przekroczenia pozostanie wtedy już tylko godzina.

10.11.3 Czas obowiązywania metryk SLA

Uwaga: *Wszystkie opisane poniżej mechanizmy operują wyłącznie na strefie czasowej, która jest ustawiona na serwerze, na którym zainstalowana jest aplikacja Axence nVision®. Nie ma możliwości wskazania w systemie HelpDesk strefy czasowej innej, niż czas lokalny na serwerze (z Axence nVision®). Nie można również ustawiać różnych stref czasowych dla poszczególnych użytkowników.*

Każda metryka SLA w momencie tworzenia pozwala na wybór jednej z dwóch opcji:

- *Metryka obowiązująca bez przerw* (**Cały dzień i przez wszystkie dni tygodnia**).
- *Metryka obowiązująca tylko w wyznaczonych godzinach* (**Zdefiniowane dni tygodnia i pory dnia**):
  - Godziny obowiązywania mogą być definiowane niezależnie na każdy dzień tygodnia (od poniedziałku do niedzieli). Każdy dzień tygodnia może posiadać jeden zakres czasowy (np. od 09:00 do 17:00) lub brak takiego zakresu (dla dni tygodnia wolnych od pracy). Nie jest możliwe zdefiniowanie wielu zakresów na jeden dzień tygodnia (np. poniedziałek od 08:00 do 11:00 a następnie od 13:00 do 16:00).
  - *Metryka, która ma w ten sposób zdefiniowany zakres godzinowy traktowana jest jako wciąż aktywna w godzinach, które są spoza tego zakresu, nawet pomimo, że jej czas aktualnie się nie nalicza.*

Przykład:

Metryka obowiązuje od 08:00 do 16:00.

Metryka mówi, że zgłoszenia muszą być rozwiązane w godzinę.

O godzinie 15:30 pojawia się zgłoszenie objęte metryką i nikt nad nim nie pracuje.

Godzina 15:31, metryka biegnie, pozostało 59 minut.

Godzina 16:01, metryka biegnie, pozostało 30 minut.

Godzina 07:59 następnego dnia, metryka biegnie, pozostało 30 minut.

Godzina 08:15 następnego dnia, metryka biegnie, pozostało 15 minut.

Godzina 08:30 następnego dnia, metryka zostaje przekroczona.

W trakcie tworzenia metryki SLA oprócz definiowania godzin obowiązywania można również ustalić, czy metryka ma przerywać swój bieg w trakcie dni sknfigurowanych jako dni wolne od pracy.

Kalendarz dni wolnych od pracy

Jeżeli wybrana metryka w swojej definicji została określona jako korzystająca z kalendarza dni wolnych od pracy, jej bieg zostaje zatrzymany w trakcie dni, które są zdefiniowane w tym kalendarzu. Każdy dzień wolny od pracy nadpisuje godziny obowiązywania metryki zdefiniowane w jej konfiguracji.

Kalendarz dni wolnych od pracy można konfigurować podczas tworzenia metryk SLA.

W systemie znajduje się kalendarz dni wolnych od pracy, w którym można definiować poszczególne dni jako wolne od pracy:

- Jako dzień wolny od pracy należy rozumieć jednoznacznie konkretny dzień, konkretnego miesiąca, konkretnego roku, który rozpoczyna się od godziny 00:00 włącznie i trwa do godziny kwant czasu wcześniejszej niż 00:00 następnego dnia według czasu serwera, na którym zainstalowana jest aplikacja Axence nVision®.
- Uprawnienia do edycji dni wolnych od pracy, mają wyłącznie użytkownicy z rolą konta "Administrator" w zakresie dni, które jeszcze się nie rozpoczęły. Po rozpoczęciu dnia wolnego, nie można w żaden sposób już anulować jego definicji.
- Dni wolne od pracy można definiować wyłącznie pojedynczo (bez możliwości tworzenia zakresów typu "24 - 26 grudnia 2017").
- Nie ma możliwości utworzenia definicji cyklicznie występujących dni wolnych od pracy.
- Kalendarz dni wolnych od pracy jest wspólny dla wszystkich definicji metryk SLA.

10.11.4 Tworzenie oraz wersjonowanie metryk SLA

Tworzenie grup użytkowników w Axence nVision®

Aby utworzyć grupę użytkowników:

1. W konsoli Axence nVision®, głównym oknie, kliknij ikonę sekcji **Użytkownicy.**

2. Przejdź do zakładki **Narzędzia i opcje.**

3. Kliknij przycisk **Dodaj grupę.**

Aby dodać użytkownika do grupy:

1. Przejdź do sekcji **Użytkownicy** w Konsoli Axence nVision®.
2. Przeciągnij wybranych użytkowników do docelowej grupy.

Aby utworzyć metrykę SLA:

1. W interfejsie web HelpDesk przejdź (jako administrator) do widoku **Metryki SLA.**

2. Kliknij przycisk **Dodaj metrykę SLA**

3. W widoku dodawania metryki, wypełnij jej **właściwości:**

- Nazwa - określana w celu lepszej identyfikacji metryki SLA. Maksymalna długość: 150 znaków.
- Opis - (opcjonalny) dodatkowy opis do wykorzystania przez użytkownika w dowolnym celu. Maksymalna długość: 300 znaków.
- Lista warunków - kolekcja warunków, które wyznaczają zgłoszenia w których zaaplikowana będzie metryka.
- Rodzaj metryki - sposób pomiaru czasu przez daną metrykę.
- Limit czasu - wartość czasowa, której przekroczenie powoduje złamanie warunków SLA. Wartość minimalna: 30 minut, wartość maksymalna: 31 dni.
- Alarm - dodatkowy adres e-mail, na który wysyłane będą powiadomienia o każdym złamaniu metryki (opcjonalny).
- Czas obowiązywania - do wyboru tryb bez przerw i tryb, gdzie limit czasu biegnie tylko w ustalonych godzinach.
- Lista godzin (opcjonalna) - jeżeli wybrano tryb przerw, pozwala na zdefiniowanie godzin dla dni tygodnia w trakcie których biegnie limit SLA.
- Kalendarz dni wolnych - pole prawda/fałsz, które określa, czy bieg SLA zostaje zatrzymany w trakcie trwania dni wolnych od pracy. Po kliknięciu linku *Z wyłączeniem dni wolnych od pracy* można zdefiniować listę dni wolnych.

4. Aby zapisać metrykę, kliknij przycisk **Dodaj metrykę SLA**

Wersjonowanie metryk SLA

Metryka SLA jest bytem wersjonowanym, gdzie wersjonowaniu podlegają wszystkie jego właściwości poza nazwą. Nazwa jest parametrem wspólnym dla kolejnych wersji metryki i można ją w każdej chwili edytować.

Dodanie nowej metryki jest jednocześnie utworzeniem pierwszej jej wersji a w chwili utworzenia wersji ustawiane jest jej pole "początkowa data obowiązywania" na datę bieżącą. Oznacza to, że tylko zgłoszenia utworzone po tej dacie mogą zostać objęte tą wersją metryki.

Po utworzeniu wersji metryki SLA nigdy nie ma już możliwości jej ponownej edycji - raz utworzoną wersję metryki SLA można wyłącznie zarchiwizować albo zarchiwizować i utworzyć jej nową wersję.

1. **Archiwizacja wersji metryki SLA.**

   W momencie archiwizacji w metryce automatycznie ustawione zostaje pole "końcowa data obowiązywania" na datę bieżącą. Oznacza to, że wszystkie zgłoszenia utworzone po tej dacie nie mogą zostać już nią objęte. Zgłoszenia, które są aktualnie objęte archiwizowaną metryką pozostają objęte tą wersją do końca swojego cyklu życia (jeżeli spełniają jej warunki).

2. **Utworzenie nowej wersji metryki SLA.**

   Dla obowiązującej metryki SLA można utworzyć jej nową wersję (zawsze jednocześnie archiwizując aktualną). Pozwala to na zachowanie ciągłości takiej metryki.

   W przypadku tworzenia nowej wersji metryki, system automatycznie uzupełnia jej dane wartościami z poprzedniej wersji.

   Nową wersję metryki można utworzyć także dla każdej metryki, która została uprzednio

zarchiwizowana bez wcześniejszego utworzenia nowej wersji.

Każda kolejna wersja jest formalnie niezależną metryką SLA. Metryki są grupowane po nazwie wyłącznie w celu wspomagającym zarządzanie ich zmianami.

W celu uproszczenia systemu, nie można ręcznie edytować dat obowiązywania wersji. Aktualnie obowiązująca wersja zawsze obowiązuje od momentu jej utworzenia i nie ma daty zakończenia aż do jej archiwizacji.

10.11.5 Złamanie SLA

Złamanie metryki SLA to przekroczenie limitu czasu zdefiniowanego w metryce. Raz złamana metryka jest permanentnie widoczna w historii metryk obejmujących zgłoszenie (nawet jeżeli zgłoszenie przestało spełniać jej warunki).

Metryka może być przekroczona tylko jeden raz. Jeżeli metryka po przekroczeniu przestała obejmować zgłoszenie (i tym samym została zatrzymana) a następnie zaczęła obejmować zgłoszenie ponownie, traktowana jest tak jakby biegła nieprzerwanie od samego początku.

Czas biegu metryki i czas obejmowania zgłoszenia przez metrykę są przez system mierzone i rozpatrywane niezależnie od siebie.

Przykład:

Zgłoszenie ma priorytet "krytyczny" jest objęte metryką "zgłoszenia o priorytecie krytycznym mają być rozwiązywane w 4 godziny".

Zgłoszenie znajduje się cały czas w statusie "otwarte".

Po 4 godzinach metryka zostaje przekroczona.

Po 5 godzinach zgłoszenia traci priorytet "krytyczny". Metryka zatrzymuje swój bieg, ale pozostaje na zgłoszeniu na zawsze widoczna jako przekroczona o godzinę.

Po 6 godzinach zgłoszenie nadal posiada tę metrykę widoczną jako przekroczoną o godzinę.

Po 7 godzinach zgłoszenie z powrotem otrzymuje priorytet "krytyczny". Ta sama metryka staje się od tej pory widoczna z powrotem jako aktywna i przekroczona o 3 godziny.

Po 8 godzinach zgłoszenie zmienia status na "zamknięte". Metryka zostaje bezpowrotnie zatrzymana w stanie przekroczenia o 4 godziny.

Fakt złamania metryki SLA generuje powiadomienie (w interfejsie i za pomocą wiadomości e-mail) do osoby aktualnie obsługującej zgłoszenie oraz na adres e-mail zdefiniowany w metryce (jeżeli jest zdefiniowany).

Na potrzeby prezentacji zgłoszenia na liście zgłoszeń, definiowana jest dynamicznie wyliczana kolumna o nazwie "data przekroczenia SLA". Wartość ta zawiera najwcześniejszą (z przeterminowanymi włącznie) datę przekroczenia SLA ze wszystkich aktywnych metryk na zgłoszeniu. Jeżeli aktualnie żadna metryka nie jest aktywna, kolumna nie ma wartości. W przypadku przekroczenia limitu czasu SLA, wartość w kolumnie jest zaznaczona kolorem pomarańczowym.

Jeżeli zgłoszenie zostaje objęte nową metryką SLA, dla której upłynął już limit czasu, system również rozsyła powiadomienie o takim przekroczeniu. Każde zgłoszenie może wygenerować jednak maksymalnie jedno powiadomienie o przekroczeniu limitu czasu dla jednej metryki SLA.

Przykład:

Zgłoszenie "X" jest objęte metryką "A".

Metryka "A" zostaje przekroczona.

Rozsyłane jest powiadomienie o przekroczeniu metryki "A" na zgłoszeniu "X".

Edytowano właściwości zgłoszenia "X", w taki sposób że nie jest już objęte metryką "A".

Edytowano właściwości zgłoszenia ponownie, w taki sposób że ponownie jest objęte (przeterminowaną) metryką "A".

Nie jest rozsyłane powtórne powiadomienie, ponieważ raz już wygenerowano powiadomienie o metryce "A" w kontekście zgłoszenia "X".

10.11.6 Metryki SLA na zgłoszeniach

Zgłoszenie może być objęte dowolną liczbą metryk dowolnego typu. Metryki obejmujące zgłoszenie są widoczne wyłącznie dla użytkowników z rolami "Pracownik HelpDesk" lub "Administrator".

Widok szczegółów zgłoszenia (sekcja "Poziom świadczenia usług") objętego metrykami SLA umożliwia zapoznanie się z nimi według kategoryzacji:

1. **Metryki aktywne:**

   Są to metryki mierzące czas na pierwszą odpowiedź (które aktualnie biegną) oraz metryki łącznego czasu na rozwiązanie zgłoszenia (niezależnie od tego, czy w danej chwili biegną, czy nie). Lista musi być posortowana od metryki, której pozostało najmniej czasu do przekroczenia (lub tej która jest przekroczona w najwyższym stopniu).

   Kategoryzacja ta zwraca uwagę użytkownika na metryki SLA, które biegną lub które mogą jeszcze wznowić bieg. Pozwala to na zapoznanie się z metrykami które aktualnie są do spełnienia.

2. **Metryki zakończone:**

   Są to metryki, których bieg już się zakończył:

   - metryki **czasu oczekiwania na pierwszą odpowiedź** - po udzieleniu pierwszej odpowiedzi,
   - metryki **łącznego czasu na rozwiązanie zgłoszenia** - po zamknięciu zgłoszenia,

   lub metryki, które zostały przekroczone a następnie przestały obejmować zgłoszenie (i tym samym ich bieg się również zakończył).

   Metryki zakończone umożliwiają zapoznanie się z informacją, w jakim okresie obejmowały zgłoszenie i czy zostały przekroczone, czy nie.

   Pozwoli to na drobiazgowe sprawdzenie, czy w historii pracy nad zgłoszeniem postanowienia jakiejś umowy SLA nie były łamane.

Na potrzeby prezentacji zgłoszenia na liście zgłoszeń, definiowana jest dynamicznie wyliczana kolumna o nazwie "data przekroczenia SLA". Wartość ta zawiera najwcześniejszą (z przeterminowanymi włącznie) datę przekroczenia SLA ze wszystkich aktywnych metryk na zgłoszeniu. Jeżeli aktualnie żadna metryka nie jest aktywna, kolumna nie ma wartości. W przypadku przekroczenia limitu czasu SLA, wartość w kolumnie jest zaznaczona kolorem pomarańczowym.

Daty na liście zgłoszeń nie są automatycznie aktualizowane i zawsze przedstawiają stan systemu z momentu wczytania listy. Widok szczegółów pojedynczego zgłoszenia jest aktualizowany na bieżąco

(do 1 minuty).

Zamknięcie zgłoszenia powoduje, że nie może już ono zostać objęte żadnymi nowymi metrykami (nawet w przypadku zmian przynależności użytkowników do grup). Wszystkie metryki zatrzymują wtedy również swój bieg i formalnie kończy się ich okres obejmowania dla danego zgłoszenia.

10.12 Komunikaty

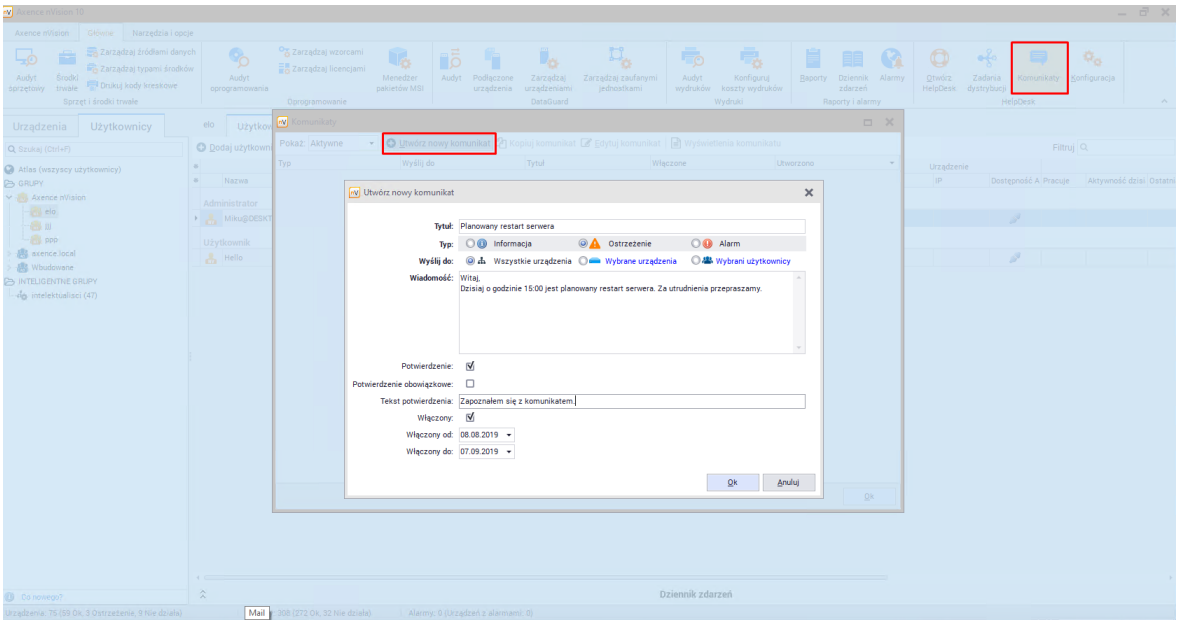
Mechanizm przesyłania komunikatów przez moduł HelpDesk umożliwia łatwe przekazywanie informacji do użytkowników z zainstalowanym Agentem, ustalanie czasu ich obowiązywania oraz zbieranie od użytkowników potwierdzeń zapoznania się komunikatami.

Komunikat może zostać utworzony przez administratora po zalogowaniu się do **Konsoli nVision.** Wybierz z głównego paska narzędzi opcję **Komunikaty** zlokalizowaną po prawej stronie interfejsu.

Tworzenie komunikatu

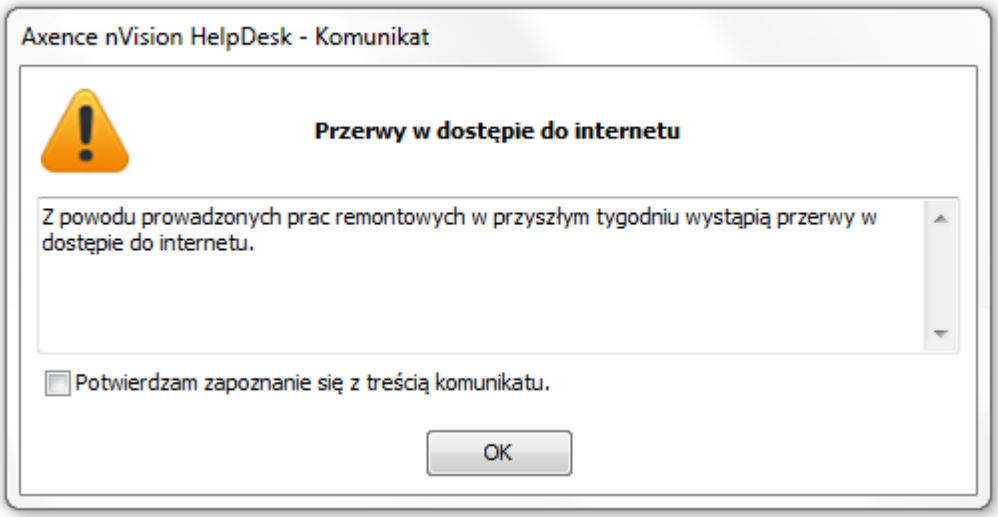
Aby utworzyć komunikat przejdź w nVision do opcji **HelpDesk | Komunikaty | Utwórz nowy komunikat** i uzupełnij opisane poniżej pola komunikatu.

Pole	Opis
Tytuł	Tytuł komunikatu.
Typ	W zależności od rodzaju przekazywanej informacji można wybrać jeden z trzech dostępnych: **Informacja**, **Ostrzeżenie**, **Alarm**.
Wyślij do	Do kogo komunikat ma być wysłany: **Wszystkie urządzenia**, **Wybrane urządzenia** (wybierz z listy urządzenia), **Wybrani użytkownicy** (wybierz z listy użytkowników Agentów).
Wiadomość	Treść wiadomości.
Potwierdzenie	Zaznaczenie pola **Potwierdzenie** skutkuje wyświetleniem użytkownikowi tekstu potwierdzenia wpisanego poniżej. Podobnie jest w przypadku zaznaczenia pola **Potwierdzenie obowiązkowe**, ale tutaj użytkownik nie będzie miał możliwości dalszego korzystania z HelpDesk, dopóki nie potwierdzi zapoznania się z treścią komunikatu.
Włączony	Alarm aktywny (włączony) będzie wyświetlany w czasie od-do wybranej daty. Możliwe jest utworzenie nieaktywnego komunikatu, np. bez ustalonego czasu wyświetlania. Aby zmienić status komunikatu, **Edytuj** dany komunikat.



Wygląd komunikatu

Wygląd komunikatu zależy od wybranych opcji. Przykładowy komunikat prezentowany jest poniżej.



10.13 Dystrybucja plików

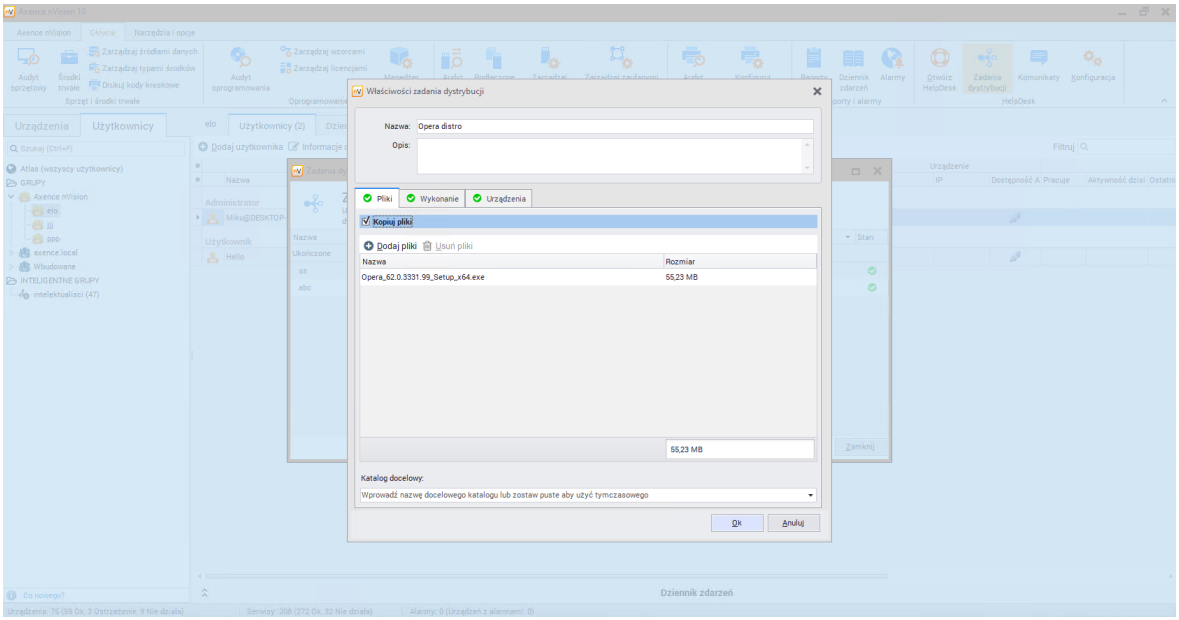
Dystrybucja plików przy pomocy Agentów

Pliki mogą być dystrybuowane na stacje robocze z zainstalowanym Agentem. Aby dowiedzieć się więcej o Agentach, przejdź do rozdziału Agenty.

Aby dystrybuować pliki:

1. Wybierz opcję **Zadania dystrybucji** z menu głównego.

2. W oknie **Zadań dystrybucji** wybierz **Dodaj**. Podaj **Nazwę** zadania i opcjonalnie **Opis**.

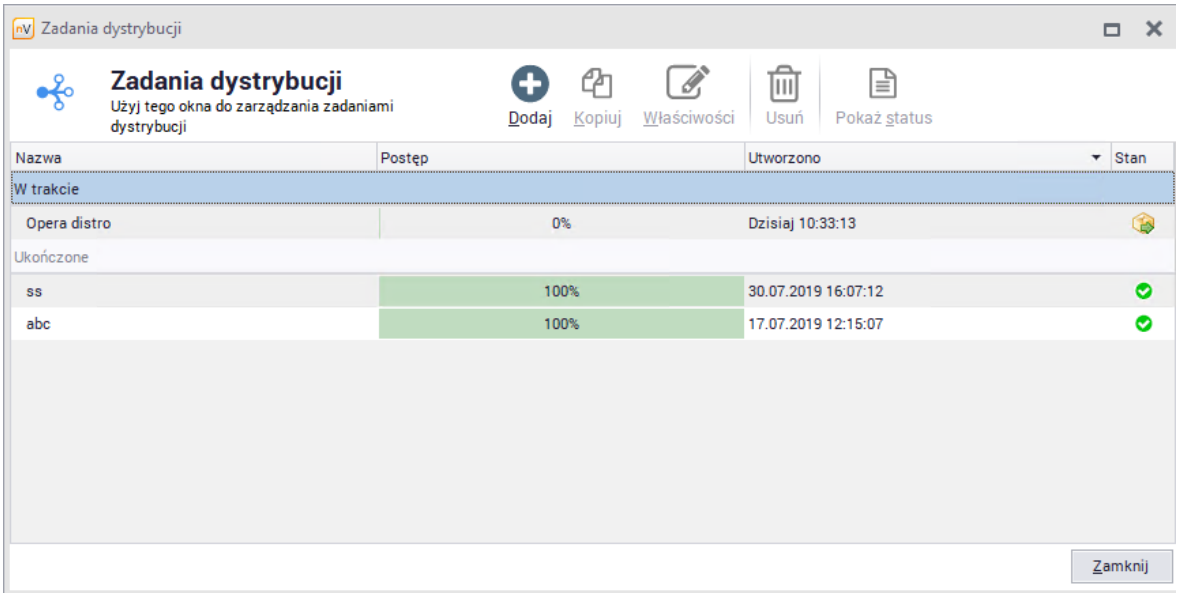


3. Jeżeli chcesz kopiować pliki, **Dodaj** pliki do dystrybucji. Możesz podać **Katalog docelowy**. Jeżeli to pole nie będzie uzupełnione, zostanie użyty tymczasowy katalog (C:\Windows\Temp).

4. Jeżeli chcesz uruchomić pliki, przejdź do zakładki **Wykonanie**. Uzupełnij folder wykonania oraz parametry (opcjonalnie, np. możliwość instalacji cichej i nienadzorowanej).

5. W zakładce **Urządzenia** wybierz **Dodaj urządzenia**. Wybierz z listy i dodaj urządzenia, na których chcesz uruchomić lub dystrybuować pliki. Po zakończeniu działania, kliknij **OK**.

Stworzone zadanie dystrybucji zostanie dodane do listy. Jeśli komputer docelowy jest wyłączony, zadania zostaną zakolejkowane i wykonane przy pierwszym kontakcie między Agentem z nVision. Postęp można sprawdzić w dowolnym momencie w oknie **Zadania dystrybucji**.

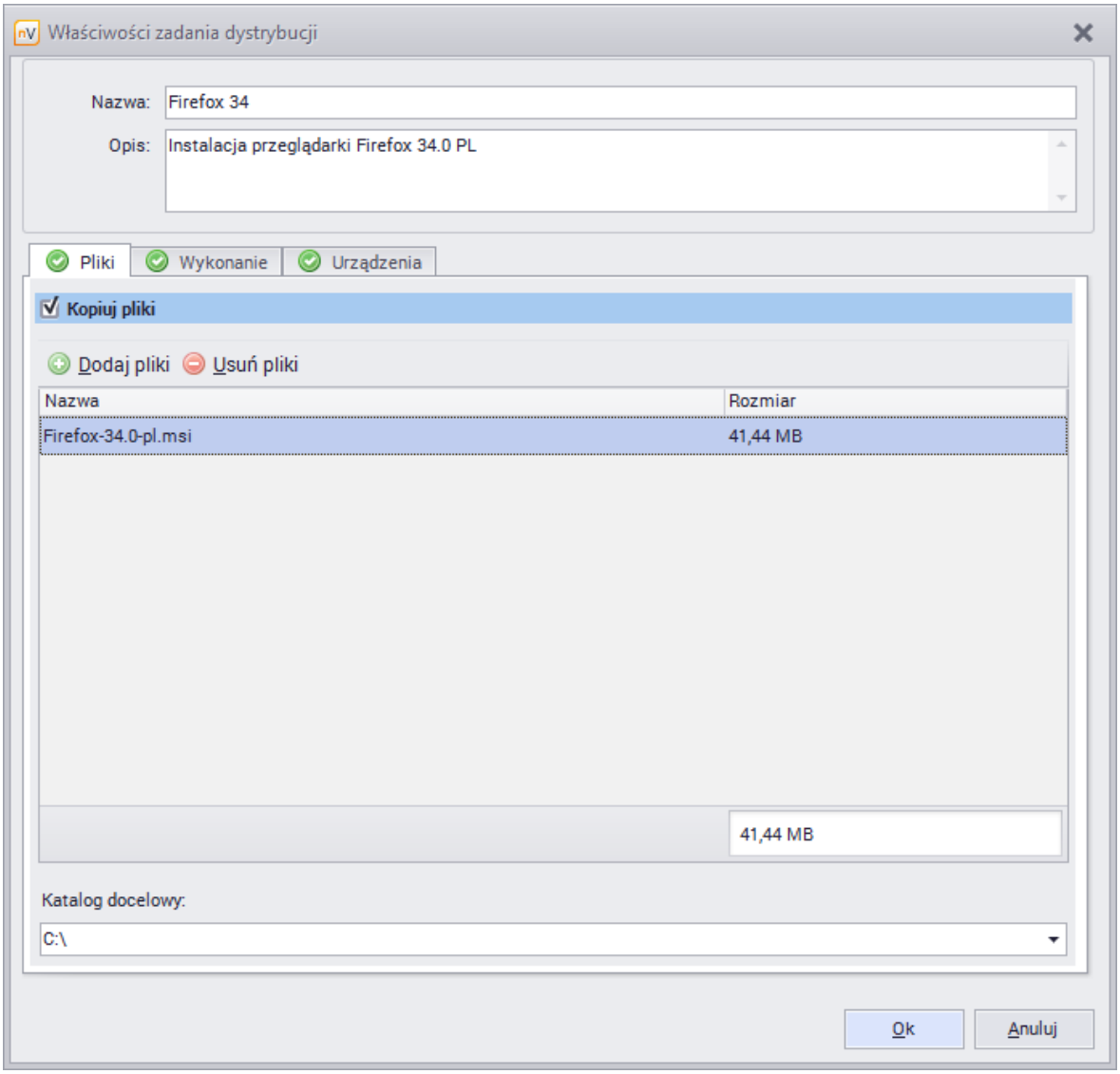


Oczekujące zadania są także wyświetlane w zakładce "Agenty" w głównym oknie nVision.

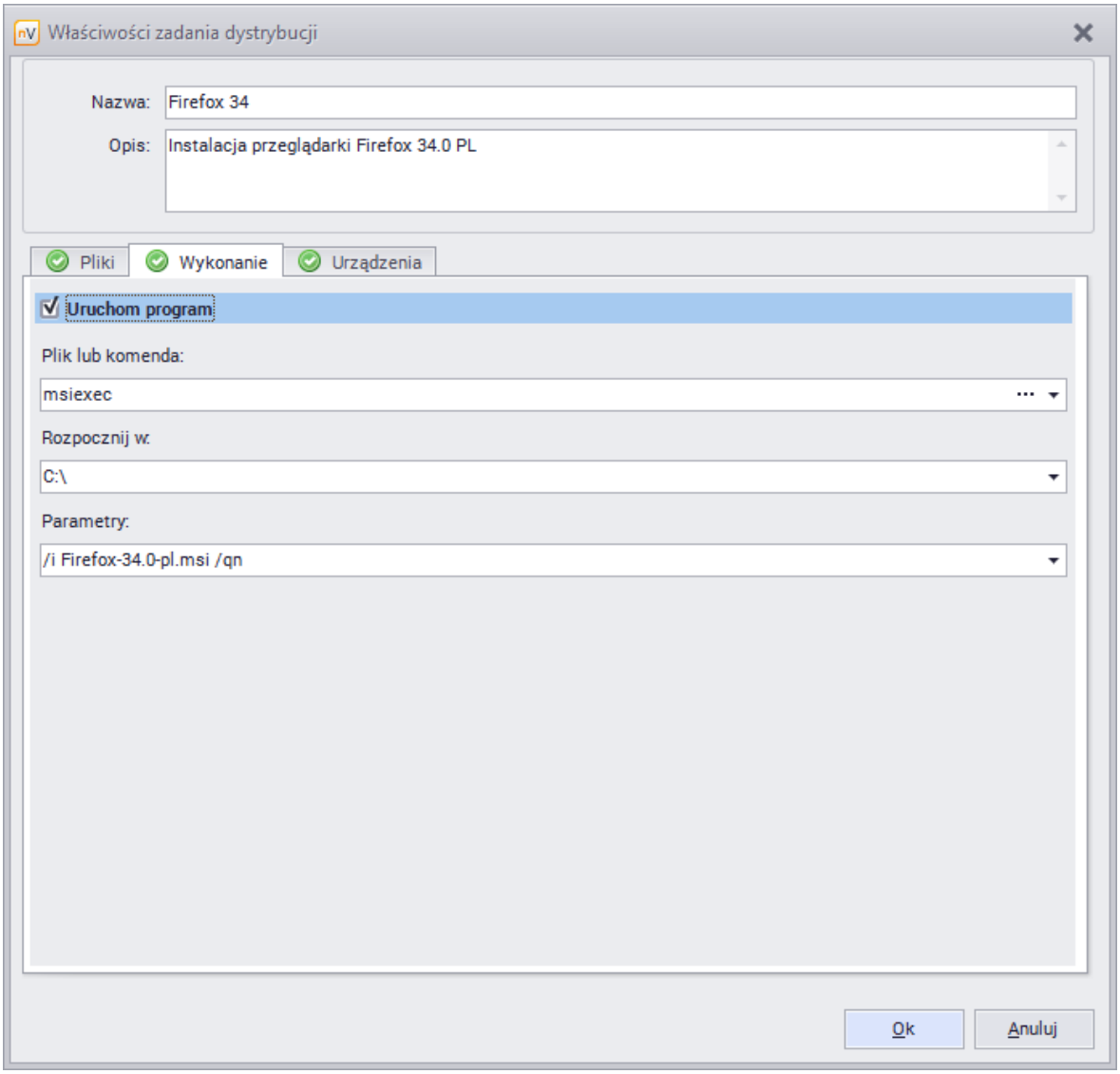
Zdalna instalacja oprogramowania z paczki MSI

Aby rozdystrybuować i zainstalować paczkę MSI:

1. Wybierz **Zadania dystrybucji** z menu głównego.
2. W oknie **Zadań dystrybucji** wybierz **Dodaj**. Podaj **Nazwę** zadania i opcjonalnie **Opis**.
3. **Dodaj** paczkę MSI do dystrybucji i podaj katalog docelowy.



4. Przejdź do zakładki **Wykonanie**, zaznacz pole **Uruchom program** i uzupełnij opcje analogicznie jak na poniższym zrzucie ekranowym



5. W zakładce **Urządzenia** wybierz **Dodaj urządzenia**. Wybierz z listy i dodaj urządzenia, na których chcesz dystrybuować i uruchomić paczkę MSI. Następnie kliknij **OK**.

Tworzenie zadania dystrybucji paczki MSI możesz również zautomatyzować w następujący sposób:

1. Zaznacz ikonę Agenta lub kilku Agentów.
2. Kliknij prawym przyciskiem myszy na ikonie Agenta, z menu kontekstowego wybierz **Agent \ Zainstaluj paczkę MSI...**
3. W oknie dialogowym wskaż plik instalatora MSI.
4. Po wskazaniu pliku instalatora, otwarte zostanie okno właściwości zadania dystrybucji z automatycznie uzupełnionymi parametrami zadania. Poza dodanie pliku, automatycznie wyepłnione zostaną parametry:

- nazwa,
- opis,
- komenda,

- domyślne parametry cichej (nienadzworowanej przez użytkownika) instalacji,
- automatycznie dodane zostaną urządzenia, na których zadanie ma zostać wykonane.

Wszystkie z opisanych parametrów mogą zostać wyedytowane.

5. Aby zakończyć działanie kreatora i wykonać zadanie, kliknij przycisk **OK.**

Zdalna deinstalacja oprogramowania

Działanie Agenta umożliwia również zdalną deinstalację oprogramowania zainstalowanego poprzez paczki MSI. Agent podczas wykonywania skanu inwentaryzacji stacji roboczej zbiera również informacje o sposobie zainstalowania oprogramowania (poprzez skan wpisów w rejestrze). **Możliwość odinstalowania z poziomu Konsoli nVision jest dostępna jedynie dla programów zainstalowanych przez Windows Installer (paczki MSI).**

Zadanie deinstalacji oprogramowania wykonywane jest natychmiastowo, jeśli Agent połączony jest z Serwerem Axence nVision®. W przeciwnym razie, zadanie jest kolejkowane i realizowane przy najbliższym połączeniu.

Aby zdalnie zdeinstalować oprogramowanie:

1. Przejdź do okna **Informacje o urządzeniu \ Zasoby \ Oprogramowanie**

2. Znajdź na liście zainstalowanych aplikacji program, który chcesz odinstalować. Zaznacz go.

3. Z paska narzędzi wybierz polecenie **Odinstaluj** lub kliknij prawym przyciskiem myszy i wybierz opcję **Odinstaluj...**

4. Stan w kolumnie **Postęp odinstalowania** zmieni się na **Oczekuje.**

lub

1. Przejdź do okna **Urządzenia / widok Agenty \ Audyt oprogramownia**

2. Znajdź na liście wykrytych aplikacji program, który chcesz odinstalować. Kliknij dwukrotnie na jego nazwie aby otworzyć okno wykrytych instalacji.

3. Zaznacz nazwę komputera, z któego chcesz odinstalować program a z paska narzędzi wybierz polecenie **Odinstaluj** lub kliknij prawym przyciskiem myszy i wybierz opcję **Odinstaluj...**

4. Stan w kolumnie **Postęp odinstalowania** zmieni się na **Oczekuje.**

W kolumnie **Postęp odinstalowania** prezentowane są: informacja o wsparciu zdalnej deinstalacji oraz status zadania:

- Wspierane - możliwa zdalna deinstalacja,
- Niewspierane - brak możliwości zdalnej deinstalacji,
- Oczekuje - zadanie zostało zlecone, oczekuje na połączenie Agenta,
- Zadanie w toku - zadanie jest wykonywane

- Błąd - wystąpił błąd (dodatkowy komunikat wyświetlany jest "w dymku" po podświetleniu kursorem myszy).

Zadanie może zostać anulowane, jeśli Agent nie połączył się z Serwerem nVision - aby anulować zadanie, upewnij się, że status w kolumnie **Postęp odinstalowania** wyświetlany jest jako **Oczekuje,** a następnie kliknij prawym przyciskiem myszy a z menu kontekstowego wybierz opcję **Przerwij odinstalowanie.**

Dystrybucja plików przy pomocy WMI

nVision pozwala na zdalną dystrybucję plików do komputerów z systemem Windows. Wykonywane jest to za pomocą usługi WMI, dlatego musisz odpowiednio skonfigurować dane logowania we właściwościach urządzenia. Dodatkowo usługa WMI musi zostać włączona na wszystkich zdalnych komputerach. Aby uzyskać więcej informacji przejdź do rozdziału Wymagania i konfiguracja.

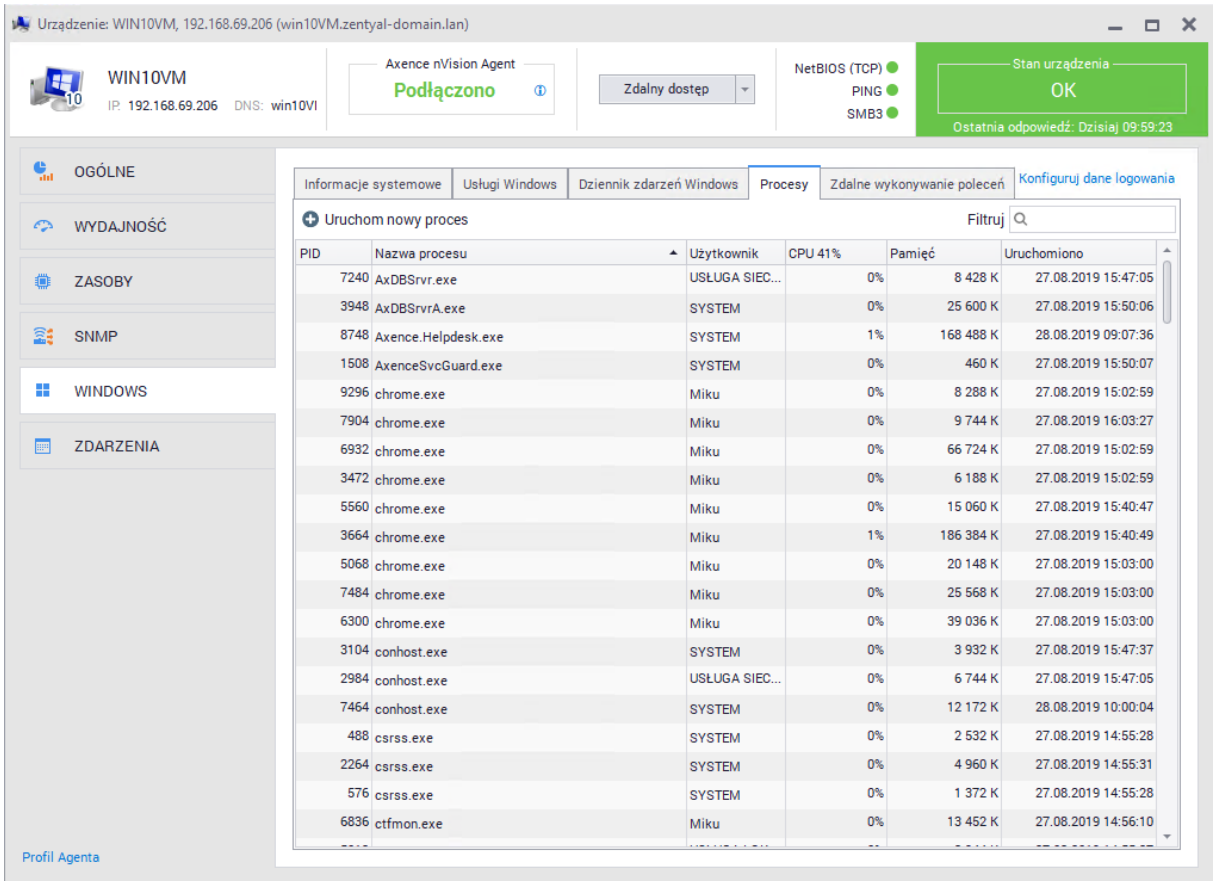
Aby dystrybuować pliki:

1. Klikając prawym przyciskiem myszy na agencie wybierz **Akcje | Dystrybuuj plik przez WMI...**.
2. Wybierz plik, który chcesz dystrybuować.
3. Wybrany plik może być plikiem wykonywalnym (np. plik instalacyjnym). Istnieje możliwość uruchomienia takiego pliku po jego skopiowaniu na zdalny komputer. Możesz za pomocą tego mechanizmu dystrybuować programy lub aktualizacje (również tzw. łatki). Sprecyzuj ustawienia uruchomienia w polu **Parametry** i włącz opcję **Uruchom plik po skopiowaniu**.
4. Wybierz **Wszystkie,** aby dystrybuować plik do wszystkich komputerów lub **Wybrane** gdy chcesz wybrać ich określoną grupę.
5. Kliknij przycisk **Instaluj**. Zobaczysz okno przedstawiające stan dystrybucji oraz pozwalające na weryfikację jej powodzenia.

10.14 Procesy Windows

Moduł HelpDesk daje możliwosć zobaczenia aktywnych procesów na komputerach w sieci z zainstalowanym Agentem.

Aby zobaczyć aktywne procesy na wybranym hoscie, należy przejsć do okna **Informacji o urządzeniu / Windows / Procesy.**



Widok procesów daje nam również możliwość zatrzymania wybranego procesu w sytuacji gdy np. dany proces nie odpowiada. Aby wymusić zakończenie procesu należy kliknąć na niego prawym przyciskiem myszy oraz wybrać **Zakończ proces.** Można również **zamknąć całe drzewo procesu** wybierając odpowiedni wariant z menu kontekstowego.

10.15 Zdalne wykonywanie poleceń

Działanie Agenta w ramach modułu HelpDesk umożliwia **zdalne wykonywanie poleceń** (podobnie jak w systemowym wierszu poleceń systemu Windows).

W tym celu należy:

1. Znaleźć ikonę komputera z zainstalowanym Agentem Axence nVision®.
   Istnieje również możliwość zaznaczenia ikon kilku Agentów - w ten sposób otwarte zostanie okno zdalnego wykonywania poleceń z kartami dla tych wybranych komputerów.

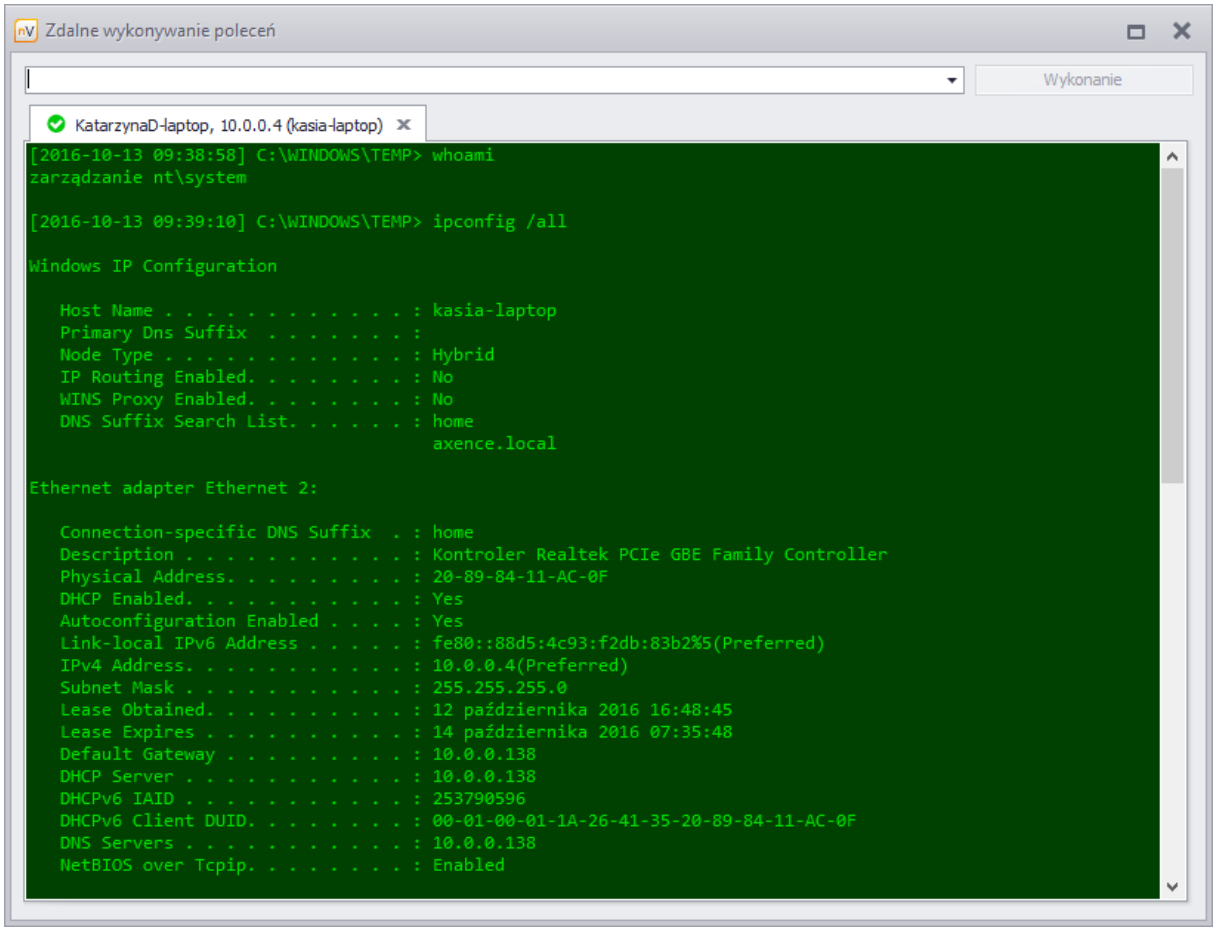
2. Zaznaczyć ikonę komputera z Agentem, kliknąć na niej prawym przyciskiem myszy a z menu kontekstowego wybrać opcję **Zdalny dostęp / Zdalne wykonywanie poleceń.**

Zdalne wykonywanie poleceń może być również wywołane z okna **Informacje o urządzeniu / Windows / Zdalne wykonywanie poleceń.**

3. Zostanie otwarte okno zdalnego wykonywania poleceń, w którym w polu **Polecenie** należy wprowadzić pożądane komendy. Aby wykonać polecenie, kliknij przycisk **Wykonanie** lub wciśnij klawisz **Enter.**
   Po otwarciu okna zdalnego wykonywania poleceń widoczny jest katalog, w którym wykonywane będą przesłane polecenia oraz wynik polecenia ***whoami*** (poświadczenia na jakich wykonywane są

polecenia).

Możliwe jest wykonywanie poleceń na wielu hostach jednoczesnie.



Przykładowe polecenia:

Komenda	Działanie
systeminfo	ogólne informacje o systemie m.in. czy działa wirtualizacja
ipconfig /all	konfiguracja interfejsów sieciowych m.in. adres serwera DNS
netsh wlan show all	konfiguracja sieci bezprzewodowej m.in. widoczne obecnie sieci bezprzewodowe
netstat -abfo	lista portów na których nasłuchują / łączą się poszczególne procesy
tracert <IP_nVision>	trasa którą Agent nVision łączy się do Serwera nVision
query user	lista sesji użytkowników zalogowanych na komputerze
tasklist /v	lista procesów oraz sesji w których działają wraz z uprawnieniami
taskkill /pid <PID>	możliwość zakończenia wybranego procesu
tasklist /svc	lista usług działających na komputerze

Komenda	Działanie
sc qc <SERVICE>	szczegółowe informacje wybranej o usłudze
chkdsk c: /f /r /b	sprawdzenie i naprawa danych na dysku c:
dir c:\users\<USER>\downloads /a /s	lista pobranych plików w katalogu wybranego użytkownika

10.16 Zdalny dostęp

Wymagania

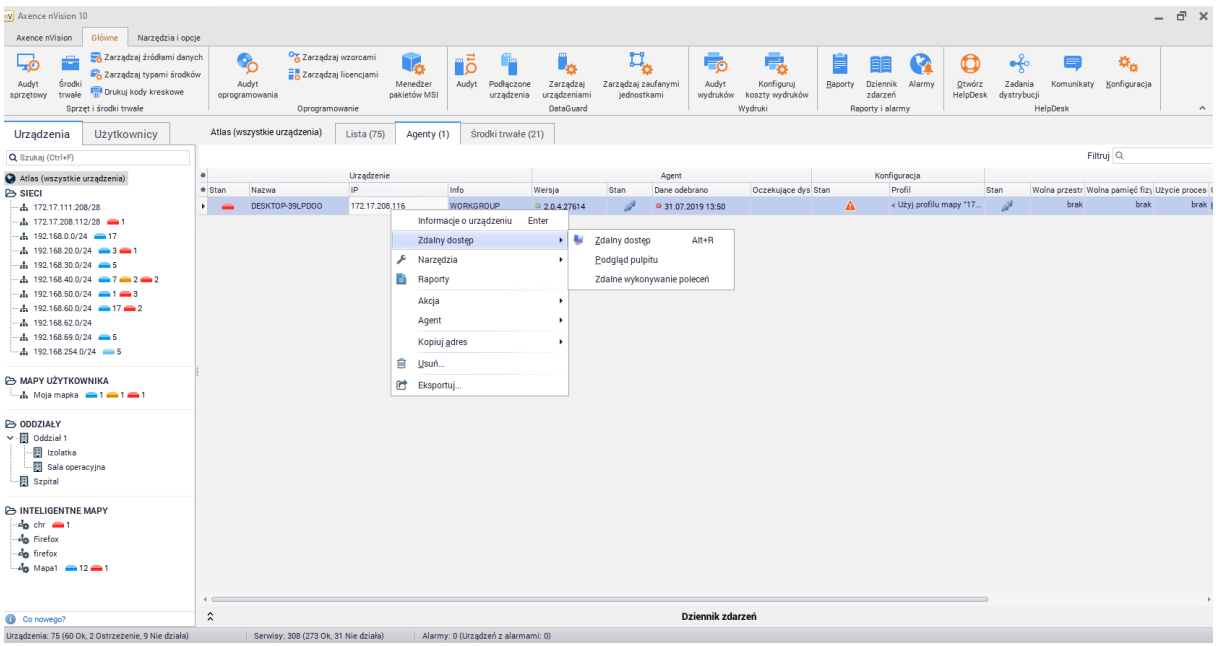
Serwer, czyli główny program nVision musi działać na statycznym adresie IP.

Tunelowanie zdalnego dostępu przez nVision

nVision nasłuchuje na porcie TCP 4436. Ten port jest konfigurowany podczas instalacji tylko dla Windows Firewall (aby dowiedzieć się więcej, przejdź do rozdziału Porty).

Agent nawiązuje połączenie z nVision - to połączenie jest cały czas utrzymywane i na nim odbywa się komunikacja. Dzięki temu ze zdalnego dostępu można korzystać nawet, gdy nVision nie może nawiązać bezpośredniego połączenia z Agentem (np. komputer z Agentem jest za NAT'em). Tunelowanie zdalnego dostępu działa także w nVision WebAccess.

Jeżeli chcesz wiedzieć więcej o komunikacji między nVision i Agentami, przejdź do rozdziału Komunikacja między Agentem a nVision.



Opcje zdalnego dostępu

Aby połączyć się zdalnie z urządzeniem, kliknij na nim prawym przyciskiem myszy i wybierz z menu kontekstowego **Zdalny dostęp**. Następnie w oknie zdalnego dostępu wybierz jeden z **Trybów dostępu**:

Tryb dostępu	Opis
Tylko podgląd	Podgląd ekranu użytkownika, bez możliwości ingerowania w urządzenie użytkownika.
Dostęp równoczesny (domyślnie)	Zarówno użytkownik jak i zdalnie podłączony administrator mogą wykonywać działania na urządzeniu.
Zablokuj mysz użytkownika	Zdalnie podłączony administrator może wykonywać działania na urządzeniu. Użytkownik może wykonywać działania przy pomocy klawiatury, jego mysz jest zablokowana.
Zablokuj klawiaturę użytkownika	Zdalnie podłączony administrator może wykonywać działania na urządzeniu. Użytkownik może wykonywać działania przy pomocy myszy, jego klawiatura jest zablokowana.
Zablokuj mysz i klawiaturę użytkownika	Zdalnie podłączony administrator może wykonywać działania na urządzeniu. Mysz i klawiatura użytkownika są zablokowane.

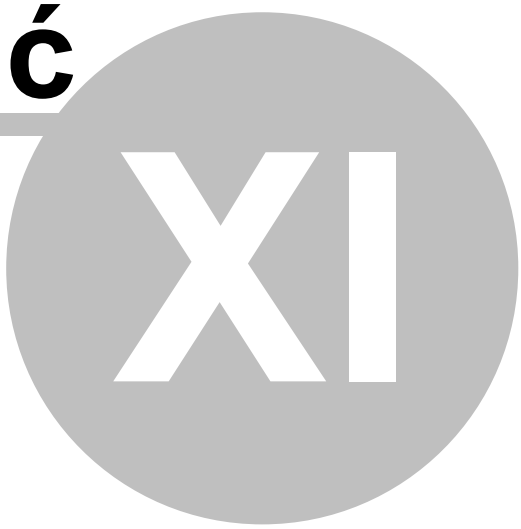
Menadżer plików

Podczas sesji zdalnego dostępu możliwe jest użycie menadżera plików, aby w wygodny sposów przenosić i kopiować dane między stacjami roboczymi.

Powiązane tematy

- Jak zainstalować zdalną konsolę nVision?
- Porty
- Komunikacja między Agentem a nVision

Część



11 Raporty

11.1 Wprowadzenie

Axence nVision® posiada zaawansowany system raportowania, pozwalający na tworzenie drukowalnych raportów, dostarczających najważniejsze informacje o każdym urządzeniu lub mapie. Program dostarcza także narzędzie służące do tworzenia własnych raportów: więcej informacji znajdziesz w dziale Tworzenie raportów.

Otwieranie okna zarządzania raportami

Kliknij **Raporty**, znajdujący się na głównej karcie wstążki - zostanie otwarte okno zarządzania raportami, w którym możesz przeglądać, drukować oraz tworzyć nowe raporty.

Wraz z instalacją oprogramowania dostępnych jest kilka podstawowych raportów. Administrator ma też możliwosć tworzenia własnych raportów w zależnosci od jego potrzeb.

Przeglądanie i drukowanie raportów

Aby przygotować raport dla urządzenia, mapy, użytkownika lub grupy:

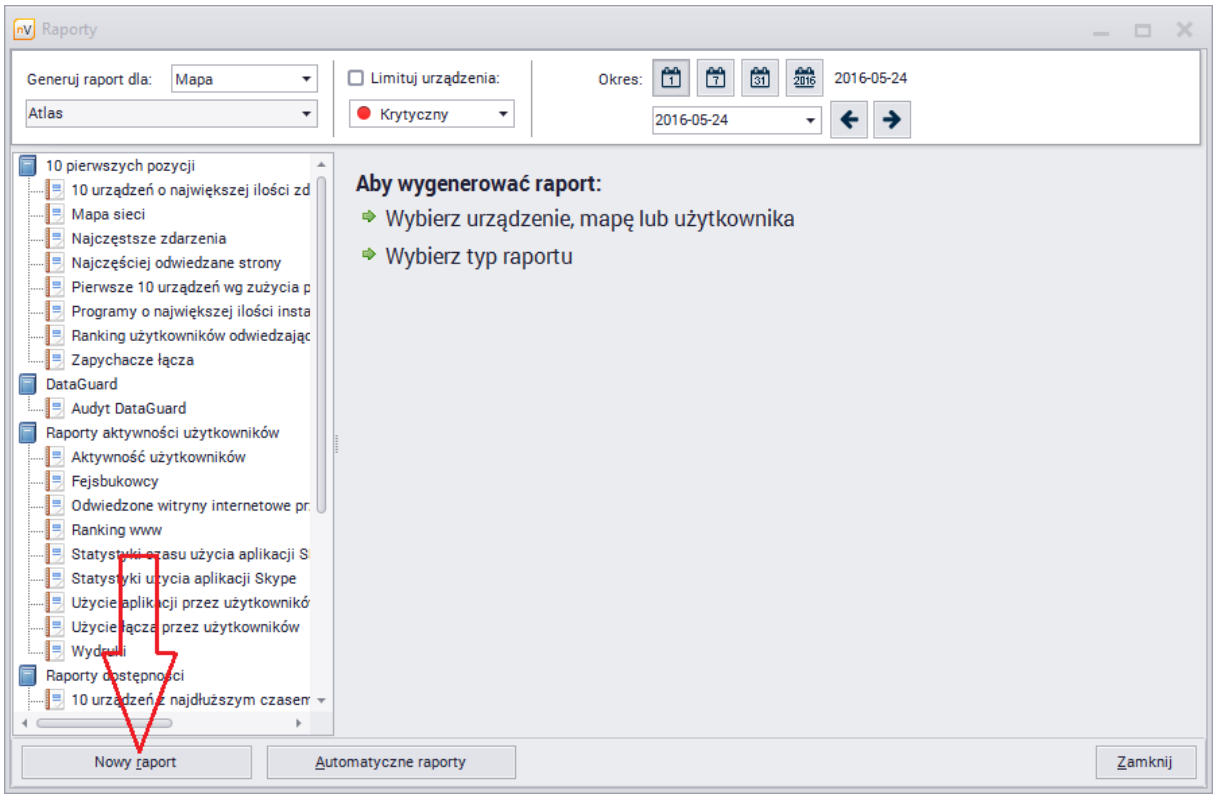
1. Wybierz typ raportu. Dla każdych z tych typów zdefiniowane są różne raporty.
2. Wybierz urządzenie/użytkownika albo mapę/grupę (w zależności od wcześniej wybranego typu raportu).
3. Wybierz raport z panelu znajdującego się po lewej stronie.
4. Wybierz przedział czasu, dla jakiego chcesz wygenerować raport.
5. Kliknij przycisk **Przygotuj i pokaż raport**. Ten przycisk jest widoczny tylko, gdy dany raport nie był nigdy wcześniej przygotowany. Gdy raport zostanie raz przygotowany, zostanie automatycznie wyświetlony za każdym razem, gdy wybierzesz go ponownie - z wyjątkiem sytuacji, w której dane mogły ulec dezaktualizacji (np. raport dla danych z dnia dzisiejszego).
6. Po utworzeniu raportu możesz go wydrukować klikając przycisk **Drukuj** znajdujący się na pasku narzędzi raportu.

11.2 Tworzenie raportów

Axence nVision® pozwala w bardzo prosty sposób tworzyć nowe raporty. Tworzenie raportów oparte jest o wybór i konfigurację predefiniowanych segmentów. Segmenty to kolektory danych, które gromadzą dane zebrane przez nVision i przetwarzają je tak, aby można je było wyświetlić w tabeli lub na wykresie.

Aby utworzyć własny raport:

1. Otwórz okno zarządzania raportami klikając w **Raporty** w głównej karcie wstążki.
2. Wybierz pozycję **Urządzenie**, **Mapa**, **Użytkownik** lub **Grupa** określające typ raportu jaki chcesz utworzyć.
3. Wybierz kategorię, do której ma należeć nowo utworzony raport.
4. Kliknij przycisk **Nowy raport** znajdujący się w dolnej części okna.



5. Wpisz nazwę i opis raportu.
6. Dodaj segment klikając przycisk  na pasku narzędzi po lewej stronie.
7. Wpisz nazwę segmentu oraz wybierz jego typ. Więcej informacji znajdziesz w rozdziałach Typy segmentów dla urządzeń lub Typy segmentów dla map.
8. Wybierz odpowiednie opcje, opisane w rozdziałach Typy segmentów dla urządzeń lub Typy segmentów dla map.
9. Wpisz krótki i długi opis, które znajdują się odpowiednio nad i pod segmentem.

11.3 Typy segmentów raportów dla urządzeń

Rozdział ten opisuje typy segmentów raportów dla urządzeń oraz ich właściwości (jeśli jest to potrzebne).

Nagłówki

Nagłówek raportu

Nagłówek ze szczegółami raportu. Powinien być pierwszym segmentem każdego raportu.

Serwisy

Serwisy - informacje ogólne

Lista przedstawiająca wszystkie serwisy danego urządzania wraz z najważniejszymi informacjami dotyczącymi ich wydajności.

Wykres wydajności serwisu

Segment wydajności serwisu przedstawia czas odpowiedzi i procent utraconych pakietów dla wybranego lub wszystkich serwisów.

Własność	Opis
Generuj dla wybranego serwisu	Segment zostanie utworzony tylko dla wybranego serwisu. Jeśli urządzenie, dla którego generujemy raport nie posiada tego serwisu, segment nie zostanie wygenerowany.
Generuj dla wszystkich serwisów	Segment zostanie wygenerowany dla wszystkich serwisów, które posiada dane urządzenie.
Format danych	Dane mogą zostać sformatowane normalnie, według godzin dnia oraz dni tygodnia.
Pokaż jako	Określa, w jaki sposób segment zostanie przedstawiony: • Wykres wydajności serwisu (domyślnie) - wyspecjalizowany wykres który przedstawia czas odpowiedzi oraz procent utraconych pakietów na jednym wykresie. • Wykres liniowy • Tabela

Czas pracy serwisu

Prezentuje porównanie czasu odpowiedzi serwisu do czasu ping.

Własności tego segmentu są opisane w tabeli powyżej.

Serwisy - czas działania/niedziałania

Czas działania oraz braku działania serwisów.

Liczniki

Liczniki wydajności

Lista przedstawiająca wszystkie liczniki wydajności danego urządzenia.

Wykres licznika wydajności

Przedstawia wykres wartości licznika wydajności dla zadanego przedziału czasowego.

Własność	Opis
Licznik wydajności	Wykres zostanie utworzony dla wybranego licznika wydajności. Jeśli dane urządzenie nie posiada takiego licznika, segment nie zostanie utworzony.
Format danych	Dane mogą zostać sformatowane normalnie, według godzin dnia oraz dni tygodnia.
Pokaż jako	Określa, w jaki sposób segment zostanie przedstawiony: • Wykres liniowy • Wykres warstwowy • Wykres słupkowy pionowy • Tabela

Ruch na interfejsie

Prezentuje ruch sieciowy na każdym interfejsie. Można wybrać sposób prezentacji w formie tabeli lub wykresu wieloliniowego.

Lista liczników urządzenia

Przedstawia listę wszystkich liczników dla danego urządzenia.

Całkowity czas stanu lub wartości licznika

Własność	Opis
Licznik	Wykres zostanie utworzony dla wybranego licznika

Własność	Opis
	wydajności.
Pokaż jako	Określa, w jaki sposób segment zostanie przedstawiony: • Wykres kołowy • Tabela

 **Min/maks/śr nieprzerwany stan lub wartość licznika**

Segment przedstawia minimalny, maksymalny i średni nieprzerwany stan lub wartość licznika.

Serwisy i liczniki

 **Dystrybucja zakresów wartości**

Prezentuje zakresy wartości licznika lub serwisu.

Własność	Opis
Źródło danych	Do wyboru - licznik lub serwis.
Zakres	Aby dodać nowy zakres, kliknij przycisk  , podaj tytuł tworzonego zakresu i uzupełnij wartości brzegowe.
Pokaż jako	Określa, w jaki sposób segment zostanie przedstawiony: • Wykres słupkowy pionowy • Wykres kołowy • Tabela

Alarmy

 **Najczęstsze zdarzenia**

Lista zdarzeń posortowana według ilości wystąpień.

Własność	Opis
Ogranicz listę do X pierwszych zdarzeń	Włącz tą opcję jeśli chcesz ograniczyć listę zdarzeń pokazanych w raporcie.
Pokaż jako	Określa, w jaki sposób segment zostanie przedstawiony: • Wykres słupkowy poziomy • Wykres słupkowy pionowy

Własność	Opis
	• Wykres kołowy • Tabela

Dziennik zdarzeń

Lista przedstawiająca wpisy dziennika zdarzeń dla zadanego okresu.

Liczba alarmów w czasie

Własność	Opis
Źródło danych	Segment może uwzględniać wszystkie zdarzenia lub jedno, wybrane z listy.
Format danych	Dane mogą zostać sformatowane normalnie, według godzin dnia oraz dni tygodnia.
Pokaż jako	Określa, w jaki sposób segment zostanie przedstawiony: • Wykres liniowy • Tabela

Sumaryczny czas alarmu / bez alarmu

Całkowity czas, w którym alarm był aktywny.

Min/maks/śr czas zdarzenia / bez zdarzenia

Własność	Opis
Źródło danych	Segment może uwzględniać wszystkie zdarzenia lub jedno, wybrane z listy.
Wylicz datę dla	Wyliczany może być czas zdarzenia lub czas bez zdarzenia.

Dziennik zdarzeń Windows

Przedstawia listę wpisów Dziennika Zdarzeń Windows dla wybranych urządzeń.

Monitorowanie użytkowników

Audyt wydruków

Przedstawia informacje o drukowanych dokumentach: niepogrupowane lub pogrupowane po użytkownikach, urządzeniach lub drukarkach, posortowane w wybrany sposób.

Użycie łącza

Własność	Opis
Wyświetl	Określa, jakie informacje zostaną wyświetlone: • Podsumowanie dla Mapy / Atlasu • Szczegóły urządzenia • Ranking użytkowników • Ranking urządzeń
Sortuj po	Sortowanie danych może odbywać się względem połączeń: • z Internetem, przychodzących • z Internetem, wychodzących • lokalnych, przychodzących • lokalnych, wychodzących
Ustawienia rankingu	Aby uzyskać informacje na temat protokołów, zaznacz opcję Pokaż szczegóły grup protokołów.

Zasoby

Zmiany w zainstalowanych programach i konfiguracji sprzętowej

Prezentuje listę zmian oprogramowania i konfiguracji sprzętu. Może uwzględniać operacje dodania, usunięcia oraz zmiany dla wybranych grup.

Konfiguracja sprzętowa

Prezentacja konfiguracji sprzętu może się odbywać na dwa sposoby - przy pomocy widoku lub wybranych konkretnie kolumn. Dostępne widoki umożliwiają wyświetlenie informacji podstawowych, multimediów, nośników danych i innych.

Lista oprogramowania urządzenia

Własność	Opis
Pokaż	Określa, jakiego rodzaju oprogramowanie zostanie uwzględnione (programy, aktualizacje, sterowniki).
Typ licencji	Wyświetlane będą programy o wybranych typach licencji.
Pokaż numery seryjne	Wybierz, czy numery seryjne mają być wyświetlane w raporcie.
Pokaż licencje	Wybierz, czy licencje mają być wyświetlane w raporcie.

Aplikacje na urządzeniach

Prezentuje urządzenia z zainstalowanymi aplikacjami, sterownikami i aktualizacjami o wybranych typach licencji.

Własność	Opis
Pokaż	Określa, jakiego rodzaju oprogramowanie zostanie uwzględnione (programy, aktualizacje, sterowniki).
Typ licencji	Wyświetlane będą programy o wybranych typach licencji.

Lista środków trwałych

Przedstawia listę wszystkich środków trwałych dla Mapy/Atlasu.

Własność	Opis
Pokaż	Wybierz typy środków trwałych, które będą uwzględniane w segmencie.
Pokaż podstawowe pola	Podstawowe pola to: wartość, w serwisie, w magazynie, osoba odpowiedzialna, numer inwentarzowy.
Pokaż pola właściwe dla typu	Jeżeli zaznaczono tę opcję, to w raporcie będą wyświetlane pola charakterystyczne dla danego typu.
Grupuj wg	Środki trwałe mogą być grupowane wg: • (brak) • Typ środka • Należy do • Nazwa

Lista środków trwałych urządzenia

Przedstawia listę wszystkich środków trwałych dla zaznaczonych urządzeń.

Lista plików użytkownika urządzenia

Przedstawia listę wszystkich plików użytkownika znalezionych na urządzeniach.

Własność	Opis
Maska	Zaznacz to pole, jeśli chcesz wyszukać pliki według podanej maski.
Rozmiar	Można zdefiniować minimalny i maksymalny rozmiar pliku.
Kategoria	Do wyboru jedna lub więcej spośród: • Audio • Video • Graficzne • Inny
Jest legalne	Wyszukiwanie legalnych lub nielegalnych plików.

Informacje o systemie

Prezentuje listę komend startowych, udziały sieciowe lub harmonogram zadań dla danych urządzeń.

Inne

Raport zmian stanu urządzenia

Tabela prezentująca historię zmian stanu urządzenia w zadanym czasie

Czas urządzenia w stanie "działa"/"nie działa"

Czasy wyrażone w procentach, w których host znajdował się w stanie "działa" albo "nie działa".

Własność	Opis
Przedstaw jako	Określa, jakie informacje zostaną wyświetlone: • Wykres słupkowy poziomy • Wykres słupkowy pionowy

Własność	Opis
	• Wykres kołowy • Tabela

 **Informacja o urządzeniu**

Ogólne informacje o danym urządzeniu.

 **Mapowanie portów**

Tabela port mappera.

DataGuard

 **Audyt DataGuard**

Przedstawia informacje o operacjach wykonanych na chronionych plikach. W segmencie mogą zostać uwzględnione informacje dotyczące wybranych użytkowników lub urządzeń i operacji typu podłączenie, odłączenie urządzenia, zmiana nazwy pliku i inne.

 **Znane urządzenia DataGuard**

Lista urządzeń wybranych typów, używanych w sieci.

11.4 Typy segmentów raportów dla map

Poniższy rozdział opisuje typy segmentów raportów dla map oraz ich właściwości (jeśli jest to potrzebne).

Nagłówki

Nagłówek raportu

Nagłówek ze szczegółami raportu. Powinien być pierwszym segmentem każdego raportu.

Serwisy

Serwisy - informacje ogólne

Lista przedstawiająca wszystkie serwisy danego urządzania wraz z najważniejszymi informacjami dotyczącymi ich wydajności.

Najlepsze/najgorsze urządzenia wg wydajności serwisu

Lista urządzeń z najdłuższymi lub najkrótszymi czasami odpowiedzi.

Własność	Opis
Serwis	Wybierz serwis, na podstawie którego urządzenia będą porównywane. Jeśli któreś urządzenie nie posiada danego serwisu, nie będzie brane pod uwagę przy porównywaniu.
Sortuj według procentu utraconych pakietów	Wyniki zostaną posortowane według procentu utraconych pakietów zamiast czasu odpowiedzi.
Pokaż najlepsze urządzenia	Zaznacz tą opcję, jeśli chcesz zobaczyć najlepsze urządzenia (z najkrótszym czasem odpowiedzi lub z najmniejszym procentem utraconych pakietów).
Pokaż najgorsze urządzenia	Zaznacz tą opcję, jeśli chcesz zobaczyć najgorsze urządzenia.
Ogranicz listę	Zaznacz tą opcję, jeśli chcesz ograniczyć ilość prezentowanych urządzeń.
Przedstaw jako	Określa sposób w jaki segment zostanie przedstawiony: • Wykres słupkowy poziomy • Wykres słupkowy pionowy • Tabela

Wykres wydajności serwisu

Segment wydajności serwisu przedstawia czas odpowiedzi i procent utraconych pakietów dla wybranego lub wszystkich serwisów.

Własność	Opis
Generuj dla wybranego serwisu	Segment zostanie utworzony tylko dla wybranego serwisu. Jeśli urządzenie, dla którego generujemy raport nie posiada tego serwisu, segment nie zostanie wygenerowany.
Generuj dla wszystkich serwisów	Segment zostanie wygenerowany dla wszystkich serwisów, które posiada dane urządzenie.
Pokaż jako	Określa, w jaki sposób segment zostanie przedstawiony: • Wykres wydajności serwisu (domyślnie) - wyspecjalizowany wykres który przedstawia czas odpowiedzi oraz procent utraconych pakietów na jednym wykresie. • Wykres liniowy • Tabela

Czas pracy serwisu

Prezentuje porównanie czasu odpowiedzi serwisu do czasu ping.

Własności tego segmentu są opisane w tabeli powyżej.

Serwisy - czas działania/niedziałania

Czas działania oraz braku działania serwisów.

Liczniki

Liczniki wydajności

Lista przedstawiająca wszystkie liczniki wydajności danego urządzenia.

Wykres licznika wydajności

Przedstawia wykres wartości licznika wydajności dla zadanego przedziału czasowego.

Własność	Opis
Licznik wydajności	Wykres zostanie utworzony dla wybranego licznika

Własność	Opis
	wydajności. Jeśli dane urządzenie nie posiada takiego licznika, segment nie zostanie utworzony.
Pokaż jako	Określa, w jaki sposób segment zostanie przedstawiony: • Wykres liniowy • Wykres warstwowy • Wykres słupkowy pionowy • Tabela

Najlepsze/najgorsze urządzenia wg licznika wydajności

Lista urządzeń, które są najbardziej/najmniej wydajne względem licznika wydajności.

Własność	Opis
Licznik wydajności	Wybierz licznik wydajności, na podstawie którego urządzenia będą porównywane. Jeśli dane urządzenie nie posiada wybranego licznika wydajności, nie będzie brane pod uwagę przy porównywaniu.
Pokaż najlepsze urządzenia	Zaznacz tą opcję, jeśli chcesz zobaczyć listę najlepszych urządzeń (z najmniejszą wartością licznika wydajności).
Pokaż najgorsze urządzenia	Zaznacz tą opcję, jeśli chcesz zobaczyć listę najgorszych urządzeń
Ogranicz listę	Włącz tą opcję, jeśli chcesz ograniczyć ilość urządzeń przedstawianych w zestawieniu
Przedstaw jako	Określa sposób w jaki segment zostanie przedstawiony: • Wykres słupkowy poziomy • Wykres słupkowy pionowy • Tabela

Ruch na interfejsie

Prezentuje ruch sieciowy na każdym interfejsie. Można wybrać sposób prezentacji w formie tabeli lub wykresu wieloliniowego.

Lista liczników urządzenia

Przedstawia listę wszystkich liczników dla danego urządzenia.

Całkowity czas stanu lub wartości licznika

Własność	Opis
Licznik	Wykres zostanie utworzony dla wybranego licznika wydajności.
Pokaż jako	Określa, w jaki sposób segment zostanie przedstawiony: • Wykres kołowy • Tabela

Min/maks/śr nieprzerwany stan lub wartość licznika

Segment przedstawia minimalny, maksymalny i średni nieprzerwany stan lub wartość licznika.

Najbardziej/najmniej dostępne urządzenia według stanu lub wartości licznika

Segment przedstawia dostępność urządzeń za względu na stan lub wartość licznika.

Najbardziej/najmniej dostępne urządzenia według najdłuższego nieprzerwanego czasu stanu lub wartości licznika

Możliwe jest wyświetlenie najlepszych lub najgorszych urządzeń, a także ograniczenie listy do pierwszych X urządzeń.

Serwisy i liczniki

Dystrybucja zakresów wartości

Prezentuje zakresy wartości licznika lub serwisu.

Własność	Opis
Źródło danych	Do wyboru - licznik lub serwis.
Zakres	Aby dodać nowy zakres, kliknij przycisk , podaj tytuł tworzonego zakresu i uzupełnij wartości brzegowe.
Pokaż jako	Określa, w jaki sposób segment zostanie przedstawiony: • Wykres słupkowy pionowy • Wykres kołowy • Tabela

Alarmy

 Najlepsze/ najgorsze urządzenia wg liczby zdarzeń

Prezentuje najbardziej lub najmniej problematyczne urządzenia wg liczby alarmów.

Własność	Opis
Generuj dla wszystkich zdarzeń	Porównuje urządzenia względem ilości wystąpień wszystkich zdarzeń
Generuj dla wybranego zdarzenia	Porównuje urządzania względem ilości wystąpień wybranego zdarzenia
Pokaż najlepsze urządzenia	Zaznacz tą opcję, jeśli chcesz zobaczyć najlepsze urządzenia (z najmniejszą ilością zdarzeń)
Pokaż najgorsze urządzenia	Zaznacz tą opcję, jeśli chcesz zobaczyć najgorsze urządzenia (mające najwięcej alarmów).
Ogranicz do	Włącz tą opcję, jeśli chcesz ograniczyć ilość prezentowanych urządzeń.
Pokaż jako	Określa sposób w jaki segment zostanie przedstawiony: • Wykres słupkowy poziomy • Wykres słupkowy pionowy • Tabela

 Najczęstsze zdarzenia

Lista zdarzeń posortowana według ilości wystąpień.

Własność	Opis
Ogranicz listę do X pierwszych zdarzeń	Włącz tą opcję jeśli chcesz ograniczyć listę zdarzeń pokazanych w raporcie.
Pokaż jako	Określa, w jaki sposób segment zostanie przedstawiony: • Wykres słupkowy poziomy • Wykres słupkowy pionowy • Wykres kołowy • Tabela

 Dziennik zdarzeń

Lista przedstawiająca wpisy dziennika zdarzeń dla zadanego okresu.

 Liczba alarmów w czasie

Własność	Opis
Źródło danych	Segment może uwzględniać wszystkie zdarzenia lub jedno, wybrane z listy.
Format danych	Dane mogą zostać sformatowane normalnie, według godzin dnia oraz dni tygodnia.
Pokaż jako	Określa, w jaki sposób segment zostanie przedstawiony: • Wykres liniowy • Tabela

 Sumaryczny czas alarmu / bez alarmu

Całkowity czas, w którym alarm był aktywny.

 Min/maks/śr czas zdarzenia / bez zdarzenia

Własność	Opis
Źródło danych	Segment może uwzględniać wszystkie zdarzenia lub jedno, wybrane z listy.
Wylicz datę dla	Wyliczany może być czas zdarzenia lub czas bez zdarzenia.

 Dziennik zdarzeń Windows

Przedstawia listę wpisów Dziennika Zdarzeń Windows dla wybranych urządzeń.

Monitorowanie użytkowników

 Audyt wydruków

Przedstawia informacje o drukowanych dokumentach: niepogrupowane lub pogrupowane po użytkownikach, urządzeniach lub drukarkach, posortowane w wybrany sposób.

Użycie łącza

Własność	Opis
Wyświetl	Określa, jakie informacje zostaną wyświetlone: • Podsumowanie dla Mapy / Atlasu • Szczegóły urządzenia • Ranking użytkowników • Ranking urządzeń
Sortuj po	Sortowanie danych może odbywać się względem połączeń: • z Internetem, przychodzących • z Internetem, wychodzących • lokalnych, przychodzących • lokalnych, wychodzących
Ustawienia rankingu	Aby uzyskać informacje na temat protokołów, zaznacz opcję Pokaż szczegóły grup protokołów.

Zasoby

Audyt inwentaryzacji oprogramowania

Prezentuje listę zainstalowanych aplikacji.

Własność	Opis
Pokaż	Określa, czy mają zostać przedstawione tylko zainstalowane programy i systemy operacyjne, czy także aktualizacje i sterowniki.
Licencja	Wybierz z listy typy licencji, które mają być uwzględnione w raporcie.
Zgodność licencji	Do wyboru: • wszystkie • z przypisanymi licencjami • bez przypisanych licencji • odpowiednia liczba lub nadwyżka licencji • brak licencji

Zmiany w zainstalowanych programach i konfiguracji sprzętowej

Prezentuje listę zmian oprogramowania i konfiguracji sprzętu. Może uwzględniać operacje dodania, usunięcia oraz zmiany dla wybranych grup.

Konfiguracja sprzętowa

Prezentacja konfiguracji sprzętu może się odbywać na dwa sposoby - przy pomocy widoku lub wybranych konkretnie kolumn. Dostępne widoki umożliwiają wyświetlenie informacji podstawowych, multimediów, nośników danych i innych.

Lista oprogramowania urządzenia

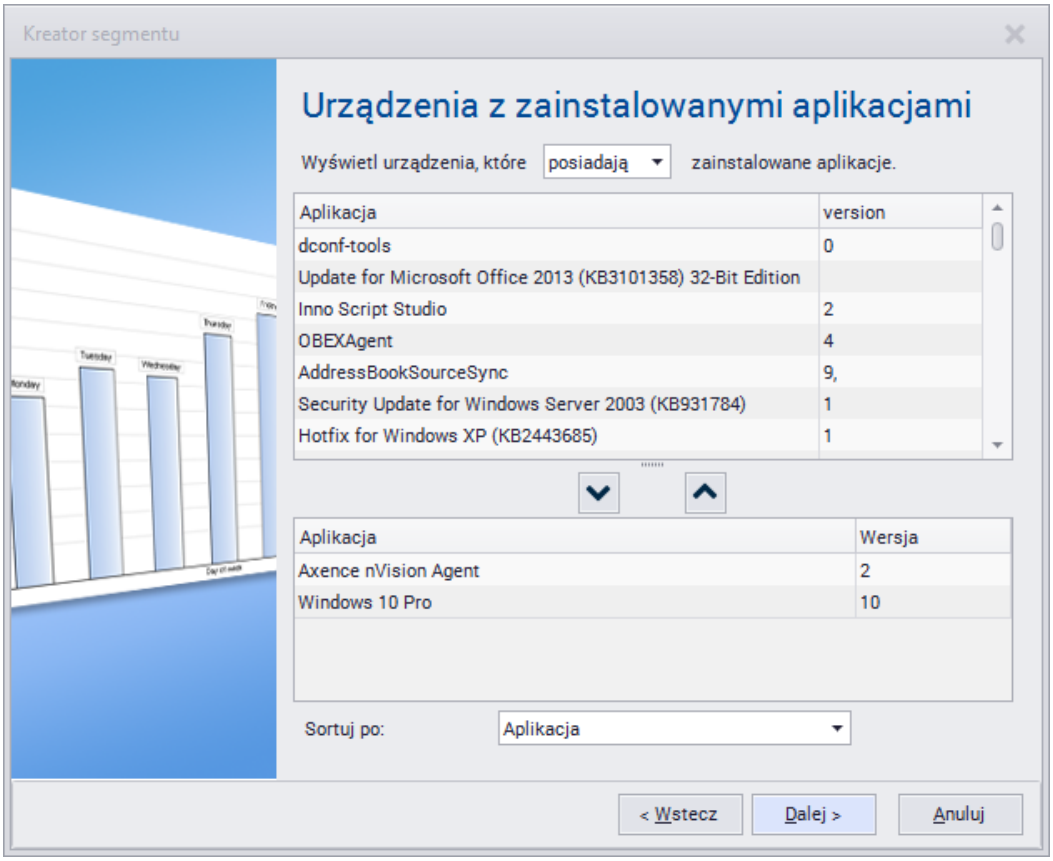
Własność	Opis
Pokaż	Określa, jakiego rodzaju oprogramowanie zostanie uwzględnione (programy, aktualizacje, sterowniki).
Typ licencji	Wyświetlane będą programy o wybranych typach licencji.
Pokaż numery seryjne	Wybierz, czy numery seryjne mają być wyświetlane w raporcie.
Pokaż licencje	Wybierz, czy licencje mają być wyświetlane w raporcie.

Najpopularniejsze aplikacje

Własność	Opis
Ogranicz do	Możliwe jest ograniczenie długości listy do pierwszych X aplikacji.
Pokaż	Określa, jakiego rodzaju oprogramowanie zostanie uwzględnione (programy, aktualizacje, sterowniki).
Typ licencji	Wyświetlane będą programy o wybranych typach licencji.

Urządzenia z zainstalowanymi aplikacjami

Wyświetlane są urządzenia, które (do wyboru) posiadają lub nie posiadają zainstalowanych wybranych aplikacji. Lista uwzględnianych aplikacji znajduje się w dolnej części okna. Aby dodać aplikację, zaznacz ją i wciśnij przycisk . Aby usunąć aplikację z listy, zaznacz ją i wciśnij przycisk .



Aplikacje na urządzeniach

Prezentuje urządzenia z zainstalowanymi aplikacjami, sterownikami i aktualizacjami o wybranych typach licencji.

Własność	Opis
Pokaż	Określa, jakiego rodzaju oprogramowanie zostanie uwzględnione (programy, aktualizacje, sterowniki).
Typ licencji	Wyświetlane będą programy o wybranych typach licencji.

Lista środków trwałych

Przedstawia listę wszystkich środków trwałych dla Mapy/Atlasu.

Własność	Opis
Pokaż	Wybierz typy środków trwałych, które mają być uwzględnione w raporcie.
Grupuj wg	Środki trwałe mogą być grupowane wg: • (brak) • Typ środka

Własność	Opis
	• Należy do • Nazwa

Lista środków trwałych urządzenia

Przedstawia listę wszystkich środków trwałych dla zaznaczonych urządzeń.

Lista plików użytkownika urządzenia

Przedstawia listę wszystkich plików użytkownika znalezionych na urządzeniach.

Własność	Opis
Maska	Zaznacz to pole, jeśli chcesz wyszukać pliki według podanej maski.
Rozmiar	Można zdefiniować minimalny i maksymalny rozmiar pliku.
Kategoria	Do wyboru jedna lub więcej spośród: • Audio • Video • Graficzne • Inny
Jest legalne	Wyszukiwanie legalnych lub nielegalnych plików.

Informacje systemowe

Prezentuje listę komend startowych, udziały sieciowe lub harmonogram zadań dla danych urządzeń.

Inne

Raport zmian stanu urządzenia

Tabela prezentująca historię zmian stanu urządzenia w zadanym czasie.

Czas działania/niedziałania urządzenia

Czasy wyrażone w procentach, w których host znajdował się w stanie "działa" albo "nie działa".

Własność	Opis
Przedstaw jako	Określa, jakie informacje zostaną wyświetlone:

Własność	Opis
	• Wykres słupkowy poziomy • Wykres słupkowy pionowy • Wykres kołowy • Tabela

 **Informacja o urządzeniu**

Ogólne informacje o danym urządzeniu. Możliwy jest wybór typu urządzeń oraz wyświetlanie dodatkowych informacji:

- adresy i interfejsy
- informacja SNMP
- monitorowanie
- czas monitorowania
- alarmy

 **Mapowanie portów**

Tabela port mappera.

 **Widok mapy**

Przedstawia graficzny widok mapy.

 **Podsumowanie czasu działania mapy**

Segment przedstawia całkowitą liczbę urządzeń, których czas działania mieści się między zadanymi przedziałami. Punkty podziału dodaje się za pomocą przycisku  **Dodaj punkt**.

Przykład

Podanie punktów 10, 50 i 90 skutkuje utworzeniem czterech przedziałów:

1. Czas działania >= 0% oraz <10%
2. Czas działania >= 10% oraz <50%
3. Czas działania >= 50% oraz <90%
4. Czas działania >= 90% oraz <=100%

DataGuard

Audyt DataGuard

Przedstawia informacje o operacjach wykonanych na chronionych plikach. W segmencie mogą zostać uwzględnione informacje dotyczące wybranych użytkowników lub urządzeń i operacji typu podłączenie, odłączenie urządzenia, zmiana nazwy pliku i inne.

Znane urządzenia DataGuard

Lista urządzeń wybranych typów, używanych w sieci.

11.5 Typy segmentów raportów dla użytkowników

Poniższy rozdział opisuje typy segmentów raportów dla użytkowników oraz ich właściwości (jeśli jest to potrzebne).

Monitorowanie użytkowników

Aktywność użytkowników

Przedstawia ogólne informacje o czasie pracy użytkownika. Raport aktywności użytkowników może być wyświetlany jako oddzielny segment dla każdego użytkownika lub zbiorczo, w postaci listy.

Strony WWW

Prezentuje listę odwiedzonych przez użytkownika stron. Można zawęzić wyświetlanie tylko do stron pasujących do podanej maski.

Ranking stron

Prezentuje ranking odwiedzanych stron, z możliwością ograniczenia liczby wpisów w segmencie do X pierwszych stron. Dostępne sposoby sortowania - po czasie całkowitym i po liczbie wizyt.

Przerwy w czasie pracy

Lista przerw w czasie pracy dla danego urządzenia.

Wykres w czasie użycia aplikacji

Przedstawia wykres w czasie użycia aplikacji przez użytkowników.

Podsumowanie użycia aplikacji

Przedstawia podsumowanie użycia aplikacji dla mapy/atlasu lub urządzenia.

Użycie łącza

Własność	Opis
Wyświetl	Określa, jakie informacje zostaną wyświetlone: • Podsumowanie dla Mapy / Atlasu • Szczegóły urządzenia

Własność	Opis
	• Ranking użytkowników • Ranking urządzeń
Sortuj po	Sortowanie danych może odbywać się względem połączeń: • z Internetem, przychodzących • z Internetem, wychodzących • lokalnych, przychodzących • lokalnych, wychodzących
Ustawienia rankingu	Aby uzyskać informacje na temat protokołów, zaznacz opcję Pokaż szczegóły grup protokołów.

Lista wiadomości e-mail

Przedstawia listę wiadomości e-mail wysłanych i odebranych przez użytkownika.

Podsumowanie wiadomości e-mail

Przedstawia podsumowanie wiadomości e-mail. Wiadomości mogą być sortowane po wysłanych, otrzymanych i rozmiarze.

Audyt wydruków

Przedstawia informacje o drukowanych dokumentach: niepogrupowane lub pogrupowane po użytkownikach, urządzeniach lub drukarkach, posortowane w wybrany sposób.

Koszty wydruków

Segment przedstawia informacje o kosztach wydruków.

Konfiguracja użytkownika

Prezentuje konfigurację monitorowania lub blokowania dla użytkownika.

DataGuard

Prawa dostępu DataGuard

Przedstawia informację o prawach dostępu do urządzeń DataGuard.

11.6 Typy segmentów raportów dla grup

Poniższy rozdział opisuje typy segmentów raportów dla grup użytkowników ich właściwości (jeśli jest to potrzebne).

Monitorowanie użytkowników

Aktywność użytkowników

Przedstawia ogólne informacje o czasie pracy użytkownika. Raport aktywności użytkowników może być wyświetlany jako oddzielny segment dla każdego użytkownika lub zbiorczo, w postaci listy.

Strony WWW

Prezentuje listę odwiedzonych przez użytkownika stron. Można zawęzić wyświetlanie tylko do stron pasujących do podanej maski.

Ranking stron

Prezentuje ranking odwiedzanych stron, z możliwością ograniczenia liczby wpisów w segmencie do X pierwszych stron. Dostępne sposoby sortowania - po czasie całkowitym i po liczbie wizyt.

Przerwy w czasie pracy

Lista przerw w czasie pracy dla danego urządzenia.

Wykres w czasie użycia aplikacji

Przedstawia wykres w czasie użycia aplikacji przez użytkowników.

Podsumowanie użycia aplikacji

Przedstawia podsumowanie użycia aplikacji dla mapy/atlasu lub urządzenia.

Użycie łącza

Własność	Opis
Wyświetl	Określa, jakie informacje zostaną wyświetlone: • Podsumowanie dla Mapy / Atlasu • Szczegóły urządzenia

Własność	Opis
	• Ranking użytkowników • Ranking urządzeń
Sortuj po	Sortowanie danych może odbywać się względem połączeń: • z Internetem, przychodzących • z Internetem, wychodzących • lokalnych, przychodzących • lokalnych, wychodzących
Ustawienia rankingu	Aby uzyskać informacje na temat protokołów, zaznacz opcję Pokaż szczegóły grup protokołów.

Ranking odwiedzanych stron

Przedstawia ranking użytkowników stron WWW.

Własność	Opis
Pokaż ranking dla konkretnej opcji	Wybierz tę opcję, jeśli chcesz, aby został wyświetlony ranking dla stron pasujących do maski podanej poniżej.
Wyświetl	Do wyboru - urządzenia lub użytkownicy, którzy odwiedzali daną stronę.
Ogranicz do	Ogranicz wyświetlanie do X pierwszych stron.
Sortuj po	Sortowanie danych może odbywać się względem: • czasu całkowitego • liczby wizyt

Statystyki użycia aplikacji

Własność	Opis
Grupa aplikacji	Zostaną pokazane informacje dla wybranych grup aplikacji: • komunikatory • przeglądarki • edytory tekstu • e-mail • programowanie • multimedia

Własność	Opis
Plik wykonywalny	Wybierz z listy plik wykonywalny, którego uruchomienia mają być uwzględniane w segmencie.
Sortuj po	Sortowanie danych może odbywać się względem: • użytkowników • czasu użycia aplikacji • czasu pracy aplikacji
Ogranicz listę do	Ogranicz wyświetlanie do X pierwszych rekordów.

Statystyki czasu użycia aplikacji

Przedstawia statystyki czasowe użycia aplikacji dla mapy.

Własność	Opis
Grupa aplikacji	Zostaną pokazane informacje dla wybranych grup aplikacji: • komunikatory • przeglądarki • edytory tekstu • e-mail • programowanie • multimedia
Plik wykonywalny	Wybierz z listy plik wykonywalny, którego uruchomienia mają być uwzględniane w segmencie.

Lista wiadomości e-mail

Przedstawia listę wiadomości e-mail wysłanych i odebranych przez użytkownika.

Podsumowanie wiadomości e-mail

Przedstawia podsumowanie wiadomości e-mail. Wiadomości mogą być sortowane po wysłanych, otrzymanych i rozmiarze.

Audyt wydruków

Przedstawia informacje o drukowanych dokumentach: niepogrupowane lub pogrupowane po użytkownikach, urządzeniach lub drukarkach, posortowane w wybrany sposób.

Koszty wydruków

Segment przedstawia informacje o kosztach wydruków.

Część XII

12 Alarmowanie

12.1 Wprowadzenie

Rozdział ten opisuje zasady korzystania z mechanizmu alarmowania dostępnego w nVision. Dzięki niemu, możesz być np. informowany w przypadku jakichkolwiek problemów w Twojej sieci. Jeśli jakieś urządzenie przestanie odpowiadać, czas odpowiedzi któregoś z monitorowanych serwisów znacząco wzrośnie lub gdy jakaś aplikacja przestanie działać prawidłowo, nVision może wysłać Ci wiadomość, wyświetlić informację na ekranie, lub rozpocząć którąś ze zdefiniowanych przez Ciebie akcji korekcyjnych.

Jak to działa?

Po pierwsze, musisz zdefiniować pewien zbiór zdarzeń, który Cię interesuje. Przykładem takiego zdarzenia jest sytuacja, w której urządzenie sieciowe przestaje odpowiadać. nVision stale monitoruje wszystkie urządzenia w celu wykrycia, czy na którymś z nich miało miejsce jakieś zdarzenie. W podanym przykładzie, zdarzenie będzie zainicjowane, gdy wszystkie serwisy działające na urządzeniu przestaną odpowiadać.

Zdefiniowanie samego zdarzenia nie wystarcza jednak do jego pełnej obsługi. Należy także zdefiniować zbiór akcji, które mogą zostać wykonane, gdy zajdzie któreś ze zdarzeń. Po zdefiniowaniu tych zdarzeń oraz akcji, możemy rozpocząć definicję alarmów. Alarm określa jakie akcje mają zostać wykonane gdy zajdzie konkretne zdarzenie.

Wszystkie wygenerowane alarmy są zapisywane w bazie danych, aby umożliwić ich późniejszą analizę i przygotowanie raportów na ich podstawie. Jeśli chcesz zbierać takie informacje, ale nie chcesz aby żadna akcja była wykonana w wypadku konkretnych zdarzeń, musisz zdefiniować dla nich alarmy, ale nie przypisywać żadnych akcji. nVision takie zdarzenia zapisze tylko w bazie danych.

Podsumowując proces tworzenia alarmu:

1. Utwórz zdarzenie. Wystąpienie takiego zdarzenia zainicjuje alarm. Przykłady zdarzeń: urządzenie nie odpowiada, problem z wydajnością serwisu, czas załadowania strony WWW przekroczył wartość graniczną, itp.
2. Zdefiniuj akcje informujące oraz korekcyjne, które mają być wykonane gdy zdarzenie będzie mieć miejsce. Przykłady akcji: wysłanie wiadomości e-mail lub ICQ, uruchomienie zewnętrznej aplikacji, zrestartowanie usługi Windows. Ten krok nie jest konieczny - możesz zdefiniować alarm beż żadnych akcji.
3. Utwórz alarm. Alarm określa jakie akcje i kiedy mają zostać wykonane gdy konkretne zdarzenie będzie mieć miejsce. Każdy alarm jest zapisywany do bazy danych programu, nawet jeśli nie zostały do niego przypisane żadne akcje.

12.2 Pojęcia

Rozdział ten poświęcony jest ogólnym założeniom systemu alarmowania w nVision.

Zdarzenia

nVision stale monitoruje Twoją sieć, wszystkie urządzenia oraz serwisy - może więc wykryć sytuację, w której konkretny serwis zacznie odpowiadać wolniej lub wcale. Wykryje też, kiedy całe urządzenie przestaje odpowiadać. Dla takich właśnie sytuacji możesz zdefiniować zdarzenie. Każde zdarzenie ma

swój czas rozpoczęcia oraz zakończenia, na przykład: w przypadku zdarzenia urządzenie nie odpowiada zostanie ono zakończone, gdy urządzenie zacznie odpowiadać. Dlatego dzięki nVision wiesz nie tylko kiedy pewne zdarzenie się zaczęło, ale także kiedy się zakończyło. W dzienniku zdarzeń możesz zobaczyć listę wszystkich zdarzeń, które się jeszcze nie zakończyły. Dla celów tego podręcznika będziemy nazywać je zdarzeniami otwartymi.

Możesz także zdefiniować własne zdarzenia: załóżmy, że posiadasz serwer MSSQL, który chcesz monitorować. W takim przypadku nie wystarczy sprawdzać jak szybko reaguje on na proste zapytanie, najprawdopodobniej będziesz chciał także monitorować kilka liczników wydajności, opisujących aktualny stan serwera, by móc zareagować zanim jakakolwiek krytyczna sytuacja będzie miała miejsce. Na przykład kiedy licznik wydajności określający ilość wolnej pamięci zacznie przyjmować niskie wartości ze względu na degradację wydajności pamięci cache. Alarm oparty na takim zdarzeniu może zostać wygenerowany zanim wystąpi jakikolwiek błąd, którego skutki są nieodwracalne, co pozwoli Ci szybko naprawić problem i uniknąć utraty danych.

Wszystkie występujące zdarzenia są zapisywane w dzienniku zdarzeń nVision. Dzięki temu możesz analizować wydajność swojej sieci, tworząc na przykład raporty przedstawiające najbardziej problematyczne urządzania, lub najczęściej występujące zdarzenia.

Stan urządzenia

W przeciwieństwie do konkurencyjnych programów, stan urządzenia jest w nVision wartością wyliczaną, niezdefiniowaną na sztywno. Można więc definiować warunki, kiedy uznajemy urządzenie jako działające, niedziałające lub w stanie ostrzeżenia. Aby uzyskać więcej informacji przejdź do rozdziału Stan urządzenia - koncepcje.

Akcje

Można zdefiniować dwa podstawowe typy akcji: informacyjne oraz korekcyjne. Jeśli jakieś zdarzenie miało miejsce, nVision korzystając z mechanizmu akcji powiadamia administratora o problemie lub uruchamia zewnętrzny program, aby go naprawić. Dlatego zanim zaczniesz definiować alarmy, musisz utworzyć zbiór akcji, które będą używane do powiadamiania Ciebie.

Można zdefiniować np. akcje: wysłanie wiadomości e-mail, ICQ lub SMS, odegranie dźwięku, wyświetlenie wiadomości lub uruchomienie zewnętrznego programu. Kompletna lista dostępnych akcji znajduje się w rozdziale Typy Akcji.

Alarmy

Alarm określa zachowanie programu w wypadku jakichkolwiek problemów w sieci. Na początku wybiera się, kiedy alarm powinien zostać wygenerowany poprzez przypisanie mu odpowiedniego zdarzenia. Następnie należy określić dla jakiego obiektu alarm ma być zdefiniowany - można definiować alarmy dla całego atlasu, mapy lub konkretnego urządzenia. Alarmy są generowane jeśli zdarzenie wystąpiło na urządzeniu należącym do obiektu, na którym alarm jest zdefiniowany (np. atlas, mapa lub mapa pochodna).

12.3 Zarządzanie Alarmami

12.3.1 Wymagania

Zarządzanie alarmami wymaga wcześniejszego zapoznania się z kilkoma koncepcjami. Musisz wiedzieć czym są zdarzania i akcje. Zanim zaczniesz zarządzać alarmami, przeczytaj rozdział Pojęcia, w którym powyższe kwestie są opisane.

Wymagania wstępne

Aby rozpocząć zarządzanie alarmami musisz wcześniej zdefiniować zbiór zdarzeń. W nVision zdarzenia określają w jakich sytuacjach alarmy mają zostać zainicjowane. Na przykład: po zainstalowaniu programu istnieje predefiniowane zdarzenie "Urządzenie nie działa". Opisuje ono zdarzenie, gdy urządzenie przestaje odpowiadać. Należy zdefiniować zdarzenia dla wszelkich problematycznych sytuacji, które chcesz wykrywać.

Po zdefiniowaniu zdarzenia należy zdefiniować akcje informujące. Akcje określają co nVision ma zrobić, kiedy pewne zdarzenie będzie miało miejsce. Na przykład akcja może określać, w jaki sposób poinformować Cię za pomocą wiadomości e-mail. Można jednak definiować alarmy bez akcji - takie rozwiązanie może być przydatne, jeśli chcesz zachować informację o zdarzeniu do późniejszej analizy, ale nie potrzebujesz być o nim poinformowany.

Po wykonaniu powyższych kroków, możesz rozpocząć zarządzanie alarmami. Kolejne rozdziały opisują wszystkie dostępne funkcje tego mechanizmu.

Gdzie można definiować alarmy?

Alarmy można definiować na kilku poziomach atlasu. Przede wszystkim, istnieje możliwość zdefiniowania globalnych alarmów dla całego atlasu. Takie alarmy są dziedziczone przez wszystkie urządzania w atlasie, co oznacza że warunki wystąpienia takiego alarmu są sprawdzane na każdym urządzeniu (jeśli dane urządzenie spełnia kryteria zdefiniowane w alarmie, na przykład alarm zdefiniowany tylko dla ważnych urządzeń nie zostanie wygenerowany na urządzeniu z ważnością ustawioną na "niska").

Alarmy mogą być także zdefiniowane dla każdej mapy - w takiej sytuacji, alarmy są dziedziczone przez wszystkie urządzenia znajdujące się na danej mapie lub na którejkolwiek z map podrzędnych. I w końcu, alarmy mogą być także definiowane dla każdego urządzenia.

Istnieje więc kilka sposobów definiowania alarmu pozwalających na utworzenie odpowiedniej polityki alarmowania bazującej na ważności urządzeń, sieci, serwisów itp. Należy pamiętać, że alarmy są dziedziczone z obiektów nadrzędnych do podrzędnych. Aby uzyskać więcej informacji na temat przejdź do rozdziału Alarmy Dziedziczone.

12.3.2 Okno zarządzania Alarmami

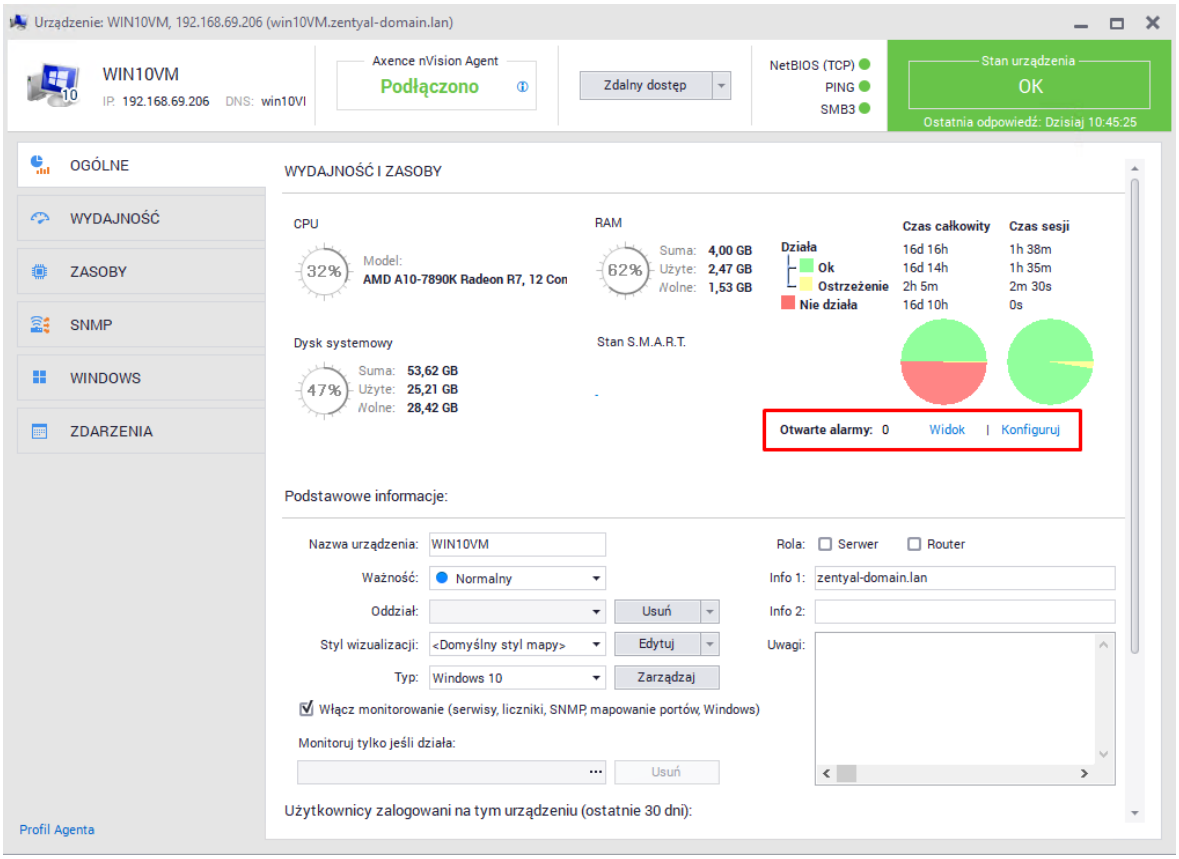
Aby skonfigurować program tak, aby informował Cię o jakichkolwiek problemach użyj okna zarządzania alarmami. W tym i kolejnych rozdziałach znajdziesz informacje o tym, jak zarządzać alarmami.

Otwieranie okna zarządzania alarmami

Za pomocą tego okna możesz przeglądać, modyfikować, tworzyć nowe oraz usuwać alarmy. Aby otworzyć okno zarządzania alarmami wykonaj następujące czynności.

1. Wybierz obiekt, którego alarmami chcesz zarządzać. Może być to urządzenie, mapa lub atlas. Jeśli wybrałeś atlas lub mapę, alarmy definiowane na nich wpływają także na urządzenia należące do tego obiektu. Aby uzyskać więcej informacji na ten temat przejdź do rozdziału Alarmy Dziedziczone.
2. Wybierz **Alarmy** z menu kontekstowego.

Aby zarządzać alarmami dla konkretnego urządzenia, należy przejść do okna **Informacje o urządzeniu**, a następnie kliknąć **Konfiguruj:**



Tworzenie nowych alarmów lub modyfikacja istniejących

1. Otwórz okno zarządzania alarmami dla obiektu, na których chcesz utworzyć alarm.
2. Kliknij przycisk **Dodaj alarm** aby utworzyć nowy alarm lub wybierz istniejący alarm i kliknij przycisk **Edytuj alarm**.
3. W polu **Dla zdarzenia** wybierz zdarzenie, dla którego chcesz zdefiniować alarm. Jeśli zdarzenie, które Cię interesuje nie jest jeszcze zdefiniowane, możesz je utworzyć klikając przycisk **Nowy** po prawej stronie. Aby uzyskać więcej informacji o zarządzaniu zdarzeniami, przejdź do rozdziału Zarządzanie zdarzeniami.
4. Pole **Uruchom akcje** pozwala Ci dodawać akcje, które zostaną uruchomione w razie alarmu.

   Aby dodać akcję kliknij ikonę znajdującą się po lewej stronie listy akcji. Zostanie wyświetlone okno **Akcja**, w której możesz określić następujące własności akcji:

Własność	Opis
Uruchom akcję	Wybierz akcję, która ma być uruchomiona. Jeśli akcja nie została jeszcze zdefiniowana, możesz ją utworzyć klikając przycisk **Nowy** po prawej stronie. Aby uzyskać więcej informacji na ten temat, przejdź do rozdziału Zarządzanie Akcjami.
Grupa "Kiedy"	

Własność	Opis
Wraz z rozpoczęciem alarmu	Domyślna opcja, która uruchamia akcję jak tylko alarm zostanie zainicjowany.
Po	Wybierz opcję "Po" i wpisz liczbę minut jaką program ma przeczekać z uruchomieniem akcji. Pamiętaj, że jeśli alarm zostanie zakończony przed tym czasem, akcja nie zostanie uruchomiona.
Po zakończeniu alarmu	Niekiedy potrzebujemy być poinformowani gdy pewna problematyczna sytuacja się zakończy. Można wykorzystać tę opcję jeśli chcesz być na przykład poinformowany gdy ważne urządzenie zacznie znowu odpowiadać.
Ograniczenie czasowe	W tym polu możesz zdefiniować ograniczenie czasu, w którym akcja może być wykonana. Bardzo często występuje sytuacją, w której inaczej chcesz być informowany w godzinach pracy, a inaczej gdy jesteś poza biurem. Na przykład: nVision może wysłać Ci tylko e-maila, gdy jesteś w biurze, ale gdy jesteś poza nim, możesz chcieć dostać wiadomość SMS.
Powtórz akcję co	Pozwala ustawić akcję, która będzie wykonywana cyklicznie aż do czasu zakończenia alarmu. Wpisz liczbę minut, określającą co ile chcesz aby akcja była wykonywana.

5. Ostatni krok pozwala ograniczyć alarm do wybranych typów urządzeń i ich ważności. Metoda ta jest przydatna jeśli chcesz skonfigurować globalny alarm dla całego atlasu, ale nie chcesz by był on generowany dla mniej ważnych urządzeń - administratorzy najczęściej nie potrzebują wiedzieć o tym, że zwykła stacja robocza została wyłączona, ale chcą wiedzieć, że przestał działać serwer.
   a) Wybierz typ urządzenia w polu "Typ"
   b) Zaznacz wszystkie odpowiednie pola znajdujące się obok napisu "Ważność" aby ograniczyć alarm tylko do urządzeń z ustawioną odpowiednią ważnością.
6. Upewnij się, że pole "Alarm włączony" jest zaznaczone. Jeśli tak nie jest - alarm nie będzie aktywny.

Uwaga

- Zmiana ustawień dziedziczonych alarmów może wpłynąć na inne urządzenia, dlatego zachowaj ostrożność zmieniając je.

Usuwanie alarmu

1. Otwórz okno zarządzania alarmami dla obiektu, na którym chcesz usunąć alarm.
2. Zaznacz alarm na liście.
3. Kliknij przycisk **Usuń** znajdujący się na pasku narzędzi. Pamiętaj, że nie możesz usunąć alarmu, który jest dziedziczony (taki alarm można usunąć tylko z poziomu, na którym został zdefiniowany).

Wyłączanie lub włączanie alarmu

1. Otwórz okno zarządzania alarmami dla obiektu, na którym chcesz wyłączyć lub włączyć alarm.
2. Zaznacz alarm na liście i kliknij przycisk .
3. Aby wyłączyć alarm, wyłącz opcję **Alarm włączony**. Aby włączyć alarm upewnij się, że to pole jest zaznaczone.

Blokowanie alarmów dziedziczonych

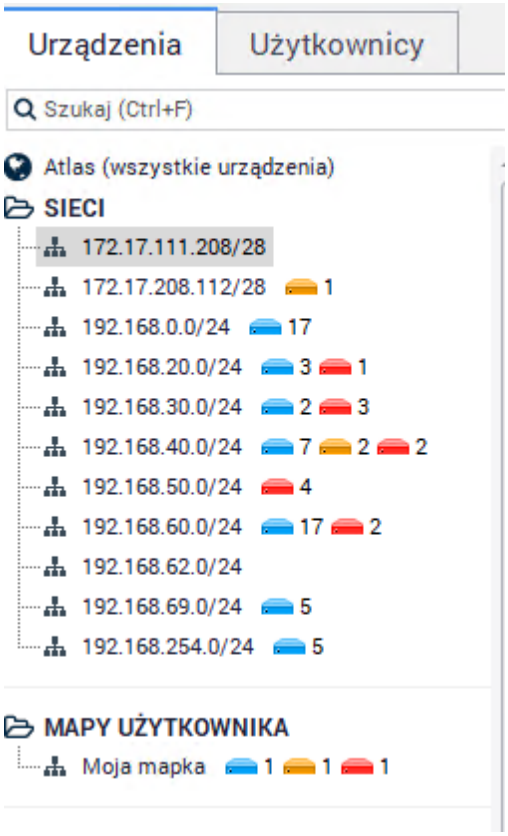
1. Otwórz okno zarządzania alarmami dla obiektu, na którym chcesz zablokować dziedziczenie alarmów.
2. Włącz opcję **Nie dziedzicz alarmów** jeśli nie chcesz aby dziedziczone alarmy były generowane dla danego obiektu. Jeśli ta opcja jest aktualnie włączona, a chcesz korzystać z dziedziczenia alarmów, wyłącz ją.

12.3.3 Dziedziczenie Alarmów

Poprzednie rozdziały omawiały sposoby definiowania alarmu: możliwość zdefiniowania dla całego atlasu, dla mapy oraz dla pojedynczego urządzenia. Jeśli alarm został zdefiniowany globalnie dla całego atlasu, wtedy będzie on dotyczył także każdej mapy oraz każdego urządzenia, które spełnia kryterium typu urządzenia (wykluczając te obiekty, które mają wyłączoną opcję dziedziczenia alarmów). Przejdź do rozdziału Zarządzenie Alarmami aby uzyskać więcej informacji na ten temat). Alarmy dziedziczone to takie alarmy, które są zdefiniowane gdzie indziej, lecz są widoczne na aktualnie wybranym urządzeniu lub mapie.

W analogiczny sposób, alarmy zdefiniowane dla mapy są dziedziczone przez wszystkie mapy podrzędne. Mapy podrzędne to te mapy, które w drzewie atlasu występują pod daną mapą. Gałęzie drzewa z mapami podrzędnymi można zwijać lub rozwijać używając ikony ⊞ znajdującej się obok nazwy mapy.

Przykład drzewa atlasu:



Blokowanie alarmów dziedziczonych

Jeśli nie chcesz aby żadne alarmy zdefiniowane na wyższym poziomie były dziedziczone dla danego obiektu, możesz je zablokować. Można to zrobić niezależnie dla każdej mapy i urządzenia.

1. Otwórz okno zarządzania alarmami dla mapy albo urządzenia.
2. Włącz opcję **Nie dziedzicz alarmów**, jeśli nie chcesz aby dziedziczone alarmy były generowane dla danego obiektu. Jeśli to pole jest zaznaczone, a chcesz korzystać z funkcji dziedziczenia alarmów, wyłącz je.

12.3.4 Eskalacja Alarmów

Dla szczególnie ważnych zdarzeń można użyć mechanizmu eskalacji alarmów. Polega on na wykonaniu kilku akcji dla zdarzenie w predefiniowanym okresie czasu. Na przykład: pierwsza akcja może zostać uruchomiona wraz z rozpoczęciem alarmu, następna po 30 minutach i być wykonywana cyklicznie co godzinę aż do zakończenia alarmu. Gdy alarm się zakończy kolejna akcja może zostać uruchomiona.

Dzięki temu mechanizmowi można być pewnym, że o krytycznej sytuacji administrator zostanie szybko poinformowany, a w wypadku, gdy nie będzie on w stanie poradzić sobie z nią, po jakimś czasie zostanie o niej poinformowana inna osoba, która może się nią zająć.

Aby uzyskać więcej informacji na temat konfiguracji akcji, tak aby były uruchamiane w innym czasie, lub by powtarzały się cyklicznie, przejdź do rozdziału Zarządzanie Akcjami.

12.4 Zdarzenia

12.4.1 Konfiguracja

Aby zarządzać zdarzeniami należy wcześniej zapoznać się z koncepcją zdarzeń, która jest omówiona w rozdziale Pojęcia.

Przed rozpoczęciem konfiguracji alarmów, należy wcześniej zdefiniować wszystkie zdarzenia, które chcemy monitorować. Program będzie monitorować wszystkie urządzenia ze zdefiniowanym konkretnym alarmem, w celu wykrycia wystąpienia zdarzenia. Gdy zdarzenie zostanie wykryte nVision wykonuje następujące operacje:

1. Inicjuje wszystkie alarmy bazujące na danym zdarzeniu. To pociąga za sobą wykonanie wszystkich akcji przypisanych danemu alarmowi. Należy pamiętać, że akcje, które mają być uruchomione po pewnym czasie, mogą nigdy nie zostać wykonane - taka sytuacja ma miejsce, gdy alarm zostanie zakończony przed jej wykonaniem. Akcje uruchamiane wraz z rozpoczęciem alarmu lub wraz z jego zakończeniem będą wykonane zawsze (chyba, że program został zamknięty).
2. Zdarzenie jest zapisane w dzienniku zdarzeń. To pozwala na przyszłą analizę wydajności urządzeń i sieci oraz pozwala przygotować raporty. Więcej informacji na temat przeglądania wygenerowanych alarmów znajduje się w rozdziale Dziennik Zdarzeń.

Gdy problematyczna sytuacja się kończy, alarm także się kończy i uruchamiane są wszystkie akcje, skonfigurowane do wykonania po zakończeniu alarmu.

Ważność

Każde zdarzenie ma zdefiniowaną swoją ważność, która służy tylko do celów informacyjnych. Podczas notyfikacji o zdarzeniu, które miało miejsce, dostępna będzie także informacja o jego ważności, pozwalając Ci reagować szybciej na bardziej istotne sytuacje.

Stan hosta

W przeciwieństwie do konkurencyjnych programów, stan urządzenia jest w nVision wartością wyliczaną, a nie zdefiniowaną na sztywno. Można więc definiować warunki, kiedy uznajemy dane urządzenie jako działające, niedziałające lub w stanie ostrzeżenia. Aby uzyskać więcej informacji przejdź do rozdziału Stan urządzenia - koncepcje.

12.4.2 Typy zdarzeń

Można wyróżnić kilka głównych grup zdarzeń. Ich opis znajduje się w poniższej liście:

Zdarzenie	Opis
Dostępność urządzenia lub serwisu	
Urządzenie nie działa	Żaden z serwisów danego urządzenia nie działa
Serwis nie działa	Serwis danego urządzanie (np. FTP, HTTP) nie odpowiada
Wydajność serwisu	Zdarzenie generowane, gdy serwis odpowiada wolniej niż powinien, lub ilość utraconych pakietów jest zbyt duża.
Interfejs nie działa	Zdarzenie generowane, gdy któryś z interfejsów urządzenia przestaje działać

Zdarzenie	Opis
Stan urządzenia	Zdarzenie może zostać wygenerowane dla każdej zmiany stanu urządzenia - także gdy urządzenia przechodzi ze stanu <Nie działa> na <Działa>.
Nowe urządzenie	Zdarzenie zostanie zainicjowane, gdy jakiekolwiek nowe urządzenie będzie dodane do mapy.
Test serwisu	
Ładowanie strony WWW	Za pomocą tego zdarzenia możesz sprawdzać czas ładowania strony WWW.
Procent zmiany treści strony	Pozwala wykrywać zmiany treści stron WWW (wynikające np. z włamań hackerów)
Czas logowania POP3	Zdarzenie generowane, gdy występują trudności z zalogowaniem się na serwer mailowy.
Czas wysłania e-maila	Zdarzenie generowane, gdy występują problemy z wysyłaniem wiadomości e-mail.
Liczniki	
Próg SNMP	Można sprawdzać wartość określonego licznika wydajności - zdarzenie jest inicjowane jeśli wartość zbytnio wzrośnie (ponad zdefiniowany próg) lub zmniejszy się.
Próg Windows	Podobnie jak wyżej – dla liczników wydajności aplikacji i systemu Windows. Pozwala to na monitorowanie stanu aplikacji takich jak Serwer SQL lub Serwer Exchange.
Windows	
Nowy wpis w dzienniku zdarzeń Windows	Zdarzenie informujące o pojawieniu się nowego wpisu w dzienniku zdarzeń Windows. Możliwe jest filtrowanie wpisów.
Zmiana stanu usługi Windows	Zdarzenie inicjowane, gdy nVision wykryje zmianę stanu usługi Windows. Pozwala ono na monitorowanie ważnych usług na zdalnych komputerach i daje możliwość np. ich zrestartowania w wypadku jakichkolwiek problemów.
Zasoby	
Zmiana w zasobach systemowych	Zdarzenie inicjowane zmianami w komendach startowych, udziałach sieciowych lub stanie S.M.A.R.T.
Zmiana w zasobach oprogramowania	Zdarzenie informujące o instalacji/deinstalacji jakiegokolwiek programu.
Zmiana w zasobach sprzętowych	Zdarzenie informujące o jakichkolwiek zmianach sprzętowych na komputerach z włączoną opcją zbierania informacji o zasobach.
Użytkownicy	

Zdarzenie	Opis
Użytkownik odwiedził domeny z wybranej grupy	Zdarzenie generowane, gdy użytkownik odwiedzi domeny z grupy skonfigurowanej w opcjach programu.
Użytkownik przekroczył limit wydrukowanych stron	Zdarzenie generowane, gdy użytkownik wydrukuje więcej niż X stron dziennie.
Użytkownik wykorzystał użycie łącza ponad limit	Zdarzenie generowane, gdy użytkownik pobierze/wyśle więcej niż X MB dziennie w sieci lokalnej/Internecie.
Inny	
Harmonogram	Zdarzenie inicjowane jest w określone dni tygodnia o wskazanej godzinie.
Stan Agenta	Zdarzenie inicjowane, gdy Agent nie był podłączony od określonej liczby dni.
Pułapka SNMP	Zdarzenie informujące o odebraniu komunikatu SNMP Trap.
Wiadomość SysLog	Zdarzenie informujące o odebraniu zdarzenia SysLog.
Zamiana na portach switch'a	Zdarzenie może być inicjowane gdy podłączono/odłączono urządzenie lub gdy port urządzenia się zmienił.
DataGuard	
Urządzenie mobilne podłączone lub odłączone	Zdarzenie inicjowane, gdy podłączono lub odłączono urządzenie. Może być generowane tylko dla wybranych urządzeń.
Operacja na pliku na urządzeniu mobilnym	Zdarzenie może być generowane po wykryciu na urządzeniu mobilnym następujących operacji: utworzenie, usunięcie, zmiana nazwy pliku, zapis do istniejącego pliku. Można określić dodatkowa warunki dla zdarzenia (maska pliku).

12.4.3 Zarządzanie zdarzeniami

Aby poprawnie skonfigurować system alarmowania w nVision, należy wcześniej zdefiniować wszelkie problematyczne sytuacje, podczas których alarm ma zostać wygenerowany.

Otwieranie okna zarządzania zdarzeniami

Korzystając z tego okna można przeglądać, modyfikować, tworzyć nowe oraz usuwać zdarzenia. Aby otworzyć okno zarządzania zdarzeniami, wybierz zakładkę **Narzędzia i opcje** a następnie **Zarządzaj zdarzeniami** z menu głównego programu.

Tworzenie nowego zdarzenia

1. Otwórz okno zarządzania zdarzeniami.
2. Kliknij przycisk **Dodaj zdarzenie** znajdujący się na pasku zadań - zostanie otwarty **Kreator definicji zdarzenia**.

3. Wpisz nazwę zdarzenia, które chcesz utworzyć w polu **Nazwa zdarzenia**.
4. Wybierz stan urządzenia dla tego zdarzenia korzystając z pola **Stan urządzenia** - determinuje ono stan, w jakim urządzenie się znajdzie, gdy zdarzenie zostanie zainicjowane. Aby uzyskać więcej informacji na ten temat przejdź do rozdziału Zdarzenia.
5. Wybierz istotność zdarzenia korzystając z pola **Istotność** - służy ono tylko do celów informacyjnych.
6. Wybierz z listy typ zdarzenia. Aby uzyskać więcej informacji na temat typów zdarzeń, przejdź do rozdziału Typy zdarzeń.
7. Kliknij przycisk **Dalej**.
8. Następnie skonfiguruj własności zdarzenia (w zależności od typu zdarzenia wybranego przez Ciebie). Więcej informacji na ten temat znajdziesz w rozdziale Definiowanie własności zdarzeń.
9. Kliknij przycisk **Zakończ**.

Modyfikowanie istniejącego zdarzenia

1. Otwórz okno zarządzania zdarzeniami.
2. Wybierz istniejące zdarzenie z kliknij przycisk **Edytuj zdarzenie**. Zostanie uruchomiony **Kreator definicji zdarzenia**.
3. Następnie skonfiguruj własności zdarzenia (w zależności od typu zdarzenia wybranego przez Ciebie). Więcej informacji na ten temat znajdziesz w rozdziale Definiowanie własności zdarzeń.
4. Kliknij przycisk **Zakończ**.

12.4.4 Definiowanie własności zdarzeń

Ten rozdział opisuje definiowanie własności różnych typów zdarzeń.

Dostępność urządzenia lub serwisu

Urządzenie nie działa

To zdarzenie jest generowane, gdy każdy serwis urządzenia przestanie odpowiadać. Należy zdecydować, kiedy nVision ma uznać urządzenie za niedziałające – po określonej liczbie minut albo sprawdzeń z brakiem odpowiedzi. Sprawdzanie wystąpienia tego zdarzenia będzie wykonywane na każdym urządzeniu, które posiada co najmniej jeden serwis.

Własność	Opis
Określona liczba sprawdzeń	Wybierz tę opcję, jeśli chcesz aby zdarzenie było generowane gdy urządzenie nie odpowiedziało na określoną liczbę sprawdzeń. Wpisz liczbę nieudanych sprawdzeń, po których urządzenie zostanie uznane za niedziałające.
Określona liczba minut	Wybierz tę opcję, jeśli chcesz aby zdarzenie było generowane gdy wszystkie serwisu urządzenia nie

Własność	Opis
	odpowiedziały przez określoną liczbę minut. Okres ten jest liczony od ostatniego pomyślnego sprawdzenia - gdy wybierzesz zbyt mały czas, możesz otrzymać fałszywe alarmy. Wpisz liczbę minut, po których urządzenie zostanie uznane za niedziałające.

Serwis nie działa

To zdarzenie jest generowany, gdy określony serwis urządzenia przestanie odpowiadać. Należy zdecydować, kiedy nVision ma uznać serwis za niedziałający – po określonej liczbie minut albo sprawdzeń z brakiem odpowiedzi.

Własność	Opis
Serwis	Wybierz serwis, który chcesz monitorować. Zdarzenie będzie sprawdzane na każdym urządzeniu, które posiada dany serwis.
Określona liczba sprawdzeń	Wybierz tę opcję, jeśli chcesz aby zdarzenie było generowane, gdy serwis nie odpowiedział na określoną liczbę sprawdzeń. Wpisz liczbą nieudanych sprawdzeń, po których serwis zostanie uznany za niedziałający.
Określona liczba minut	Wybierz tę opcję, jeśli chcesz aby zdarzenie było generowane, gdy serwis nie odpowiedział przez określoną liczbę minut. Okres ten jest liczony od ostatniego pomyślnego sprawdzenia serwisy - gdy wybierzesz zbyt mały czas sprawdzania, możesz otrzymać fałszywe alarmy. Wpisz liczbę minut, po których serwis zostanie uznany za niedziałający.

Wydajność serwisu

To zdarzenie jest generowane, jeśli jakiś serwis zacznie działać wolniej, lub zbyt duża ilość pakietów jest utracona.

Własność	Opis
Serwis	Wybierz serwis, który chcesz monitorować. Zdarzenie będzie sprawdzane na każdym urządzeniu, które posiada dany serwis.
Sprawdź ostatnie	Liczba ostatnich minut, które chcesz sprawdzać.

Własność	Opis
Generuj zdarzenie, gdy	Wybierz przynajmniej jeden z warunków opisanych poniżej. Jeśli wybierzesz obydwa, zdarzenie zostanie zainicjowane, jeśli co najmniej jeden warunek zostanie spełniony.
Średni/Każdy czas odpowiedzi	Wybierz Średni czas odpowiedzi, jeśli chcesz aby zdarzenie było generowane gdy serwis zacznie działać wolniej. • nVision sprawdza domyślnie średnią wartość. Możesz wybrać jednak metodę sprawdzania każdej wartości klikając napis (link) **Średni**. Napis zamieni się na **Każdy** wskazując, że każda próbka (sprawdzenie) będzie sprawdzana oddzielnie. • Wpisz wartość progu czasu odpowiedzi w milisekundach. Zdarzenie zostanie wygenerowane, jeśli czas odpowiedzi będzie większy niż podana wartość. • Wpisz wartość progu kończącego w następnym polu. Aby uzyskać więcej informacji na temat progów przejdź do rozdziału Progi narastające, opadające i kończące.
Procent utraconych pakietów	Wybierz Procent utraconych pakietów, jeśli chcesz aby zdarzenie było generowane gdy procent utraconych pakietów dla danego serwisu będzie zbyt duży. • Wpisz wartość progu. Zdarzenie zostanie wygenerowane, gdy procent utraconych pakietów będzie większy niż podana wartość. • Wpisz wartość progu kończącego w następnych polu.

Interfejs nie działa

To zdarzenie będzie wygenerowane, gdy tylko jakikolwiek interfejs sieciowy przestanie działać i zakończy się, gdy ten interfejs znowy zadziała.

Stan urządzenia

Zdarzenie to może zostać wygenerowane dla każdej zmiany stanu urządzenia, nawet jeśli urządzenie przechodzi ze stanu <Nie działa> na <Działa>. Zdarzenie sprawdzane na każdym urządzeniu.

Własność	Opis
Generuj zdarzenie, gdy	Wybierz stan, dla którego chcesz, aby nVision generowało zdarzenie. Zdarzenie może zostać wygenerowane jeśli stan urządzenia zmieni się na <Działa>, <Ostrzeżenie> lub <Nie działa>. Wybierz odpowiednią opcję.

Nowe urządzenie

Zdarzenie będzie zainicjowane, gdy jakiekolwiek nowe urządzenie będzie dodane do mapy.

Test serwisu

Ładowanie strony WWW

Za pomocą tego zdarzenia możesz testować czas załadowania Twojej strony WWW. Zdarzenie to będzie sprawdzane na każdym urządzeniu, które monitoruje czas załadowania dowolnej strony WWW (posiada zdefiniowany licznik wydajności tego typu).

Własność	Opis
Sprawdź ostatnie	Liczba ostatnich minut, które chcesz sprawdzać
Generuj zdarzenie, gdy	• nVision sprawdza domyślnie średnią wartość. Możesz wybrać jednak metodę sprawdzania każdej wartości klikając napis (link) **Średni**. Napis zamieni się na **Każdy** wskazując, że każda próbka (sprawdzenie) będzie sprawdzana oddzielnie. • Wpisz wartość progu czasu ładowania strony w milisekundach. Zdarzenie zostanie wygenerowane, gdy czas załadowania strony będzie większy niż podana wartość.
Zakończ zdarzenie, gdy	Wpisz wartość progu kończącego w następnym polu. Aby uzyskać więcej informacji na temat progów, przejdź do rozdziału Progi narastające, opadające i kończące.

Procent zmiany treści strony

Pozwala zapobiegać przypadkowym zmianom treści stron (np. dokonanych przez hakera). Zostanie zainicjowane gdy tylko próbnik wykryje, że procent zmiany treści strony wzrósł powyżej progu. Zdarzenie to będzie sprawdzane na każdym urządzeniu, które posiada zdefiniowany licznik wydajności tego typu.

Własność	Opis
Sprawdź ostatnie	Liczba ostatnich minut, które chcesz sprawdzać
Średni stopień zmiany treści >	• nVision sprawdza domyślnie średnią wartość. Możesz wybrać jednak metodę sprawdzania każdej wartości klikając napis (link) **Średnia**. Napis zamieni się na **Każda** wskazując, że każda próbka (sprawdzenie) będzie sprawdzana oddzielnie. • Wpisz wartość progu czasu ładowania strony w milisekundach. Zdarzenie zostanie wygenerowane, gdy czas załadowania strony będzie większy niż podana

Własność	Opis
	wartość.
Zakończ zdarzenie, gdy	Zdarzenie zakończy się, gdy treść powróci do oryginału i procent zmiany spadnie poniżej progu kończącego.

Czas logowania POP3

Zdarzenie to jest generowane gdy występują problemy z logowaniem się do serwera pocztowego. Sprawdzanie warunków zajścia tego zdarzenia będzie wykonywane na każdym urządzeniu, które monitoruje czas logowania do dowolnego serwera POP3 (posiada zdefiniowany licznik wydajności tego typu).

Własność	Opis
Sprawdź ostatnie	Liczba ostatnich minut, które chcesz sprawdzać.
Średni czas logowania do serwera POP3	• nVision sprawdza domyślnie średnią wartość. Możesz wybrać jednak metodę sprawdzania każdej wartości klikając napis (link) **Średni**. Napis zamieni się na **Każdy** wskazując, że każda próbka (sprawdzenie) będzie sprawdzana oddzielnie. • Wpisz wartość progu czasu logowanie do serwera POP3 w milisekundach. Zdarzenie zostanie wygenerowane, gdy czas załadowania strony będzie większy niż podana wartość.
Zakończ zdarzenie gdy	Wpisz wartość progu kończącego w następnym polu. Aby uzyskać więcej informacji na temat progów przejdź do rozdziału Progi narastające, opadające i kończące.

Czas wysłania e-maila

Zdarzenie to jest generowane, gdy występują problemy z wysyłaniem wiadomości e-mail. Sprawdzanie warunków zajścia tego zdarzenie będzie wykonywane na każdym urządzeniu, które monitoruje czas wysyłania wiadomości e-mail do dowolnego serwera (posiada zdefiniowany licznik wydajności tego typu).

Własność	Opis
Sprawdź ostatnie	Liczba ostatnich minut, które chcesz sprawdzać.
Średni czas wysłania wiadomości e-mail	• nVision sprawdza domyślnie średnią wartość. Możesz wybrać jednak metodę sprawdzania każdej wartości klikając napis (link) **Średni**. Napis zamieni się na **Każdy** wskazując, że każda próbka (sprawdzenie) będzie sprawdzana oddzielnie. • Wpisz wartość progu czasu logowanie do serwera POP3 w

Własność	Opis
	milisekundach. Zdarzenie zostanie wygenerowane, gdy czas załadowania strony będzie większy niż podana wartość.
Zakończ zdarzenie gdy	Wpisz wartość progu kończącego w następnym polu. Aby uzyskać więcej informacji na temat progów przejdź do rozdziału Progi narastające, opadające i kończące.

Liczniki wydajności

Próg SNMP

Własność	Opis
Licznik wydajności	Wybierz licznik wydajności SNMP, który ma być sprawdzany. Należy pamiętać, że dany licznik wydajności będzie sprawdzany tylko, jeśli istnieje na monitorowanym urządzeniu. Dlatego aby sprawdzanie zdarzenia działało poprawnie musisz zdefiniować dany licznik wydajności na odpowiednich urządzeniach.
Sprawdź ostatnie	Liczba ostatnich minut, które chcesz sprawdzać.
Średnia wartość	• nVision sprawdza domyślnie średnią wartość. Możesz wybrać jednak metodę sprawdzania każdej wartości klikając napis (link) **Średni**. Napis zamieni się na **Każdy** wskazując, że każda próbka (sprawdzenie) będzie sprawdzana oddzielnie. • Wpisz wartość progu czasu logowanie do serwera POP3 w milisekundach. Zdarzenie zostanie wygenerowane, gdy czas załadowania strony będzie większy niż podana wartość.
Zakończ zdarzenie gdy	Wpisz wartość progu kończącego w następnym polu. Aby uzyskać więcej informacji na temat progów przejdź do rozdziału Progi narastające, opadające i kończące.

Uwaga

- Należy mieć na uwadze, że ustawienie długiego okresu czasu sprawdzania może spowolnić działanie programu. Licznik wydajności, który jest sprawdzany bardzo często, dostarcza wiele próbek, których analiza zużywa zasoby procesora. Nie należy ustawiać okresu sprawdzania na więcej niż 10 minut dla urządzeń, które są sprawdzane częściej niż co 10 sekund.

Próg Windows

Własność	Opis
Licznik wydajności	Wybierz licznik wydajności Windows, który ma być sprawdzany. Należy pamiętać, że dany licznik wydajności będzie sprawdzany tylko, istnieje na monitorowanym urządzeniu. Dlatego, aby sprawdzanie zdarzenia działało poprawnie musisz zdefiniować dany licznik wydajności na odpowiednich urządzeniach.
Sprawdź ostatnie	Liczba ostatnich minut, które chcesz sprawdzać.
Średnia wartość	• nVision sprawdza domyślnie średnią wartość. Możesz wybrać jednak metodę sprawdzania każdej wartości klikając napis (link) **Średni**. Napis zamieni się na **Każdy** wskazując, że każda próbka (sprawdzenie) będzie sprawdzana oddzielnie. • Wpisz wartość progu czasu logowanie do serwera POP3 w milisekundach. Zdarzenie zostanie wygenerowane, gdy czas załadowania strony będzie większy niż podana wartość.
Zakończ zdarzenie gdy	Wpisz wartość progu kończącego w następnym polu. Aby uzyskać więcej informacji na temat progów przejdź do rozdziału Progi narastające, opadające i kończące.

Uwaga

- Należy mieć na uwadze, że ustawienie długiego okresu czasu sprawdzania może spowolnić działanie programu. Licznik wydajności, który jest sprawdzany bardzo często, dostarcza wiele próbek, których analiza zużywa zasoby procesora. Nie należy ustawiać okresu sprawdzania na więcej niż 10 minut dla urządzeń, które są sprawdzane częściej niż co 10 sekund.

Windows

Zmiana stanu usługi Windows

Własność	Opis
Generuj zdarzenie, gdy	Wybierz odpowiednią opcję określającą, kiedy zdarzenie ma być generowane.
Wszystkie serwisy	Wybierz, jeśli chcesz aby zdarzenie było generowane dla wszystkich serwisów Windows.

Własność	Opis
Wybrane serwisy	Wybierz, jeśli chcesz aby zdarzenie było generowane dla wybranych serwisów Windows. Kliknij ikonę z zielonym plusem i wybierz usługę, która chcesz monitorować.

Nowy wpis w dzienniku zdarzeń Windows

Zdarzenie będzie zainicjowane, gdy nowy wpis w dzinniku spełnia podany warunek.

Inny

Zmiana na portach switch'a

Własność	Opis
Inicjuj zdarzenie gdy	Zdarzenie jest inicjowane, gdy podłączono urządzenie, odłączono urządzenie lub port urządzenia zmienił się.
Tylko dla nowych urządzeń podłączonych do switch'a	Zaznacz tę opcję, aby alarm był generowany tylko dla nowych urządzeń.

Pułapka SNMP

Własność	Opis
Filtr MIB	Zdarzenie zostanie zainicjowane gdy urządzenie przyśle pułapkę SNMP odnośnie jakiegokolwiek OID lub jedynie odnośnie wybranych OID.

Harmonogram

Własność	Opis
Harmonogram	Zdarzenie zostanie zainicjowane w okreslone przez administratora dni o okreslonej godzinie.

Wiadomość SysLog

Własność	Opis
Wiadomosć SysLog	Zdarzenie zostanie zainicjowane gdy urządzenie przyśle wiadomosć SysLog zawierającą słowa kluczowe okreslone w

Własność	Opis
	filtrze ustawionym w momencie konfiugracji.

Stan agenta

Własność	Opis
Stan agenta	Zainicjuj zdarzenie jeżeli Agent nie był podłączony przez okresloną ilosć dni.

DataGuard

Urządzenie mobilne podłączone lub odłączone

Własność	Opis
Wygeneruj zdarzenie gdy	Zdarzenie zostanie wygenerowane jeśli podłączono lub odłączono urządzenie.
Wygeneruj to zdarzenie dla wybranych urządzeń	Wybierz urządzenia, dla których ma być generowany alarm.

Operacja na pliku na urządzeniu mobilnym

Własność	Opis
Wygeneruj zdarzenie gdy	Wygeneruj zdarzenie, gdy na urządzeniu mobilnym wykryto operacje: utworzenia pliku, usunięcia pliku, zmiany nazwy pliku lub zapisu do istniejącego pliku.
Określ dodatkowe warunki dla zdarzenia	Podaj maskę pliku.
Wygeneruj to zdarzenie dla wybranych urządzeń	Wybierz urządzenia, dla których ma być generowany alarm.

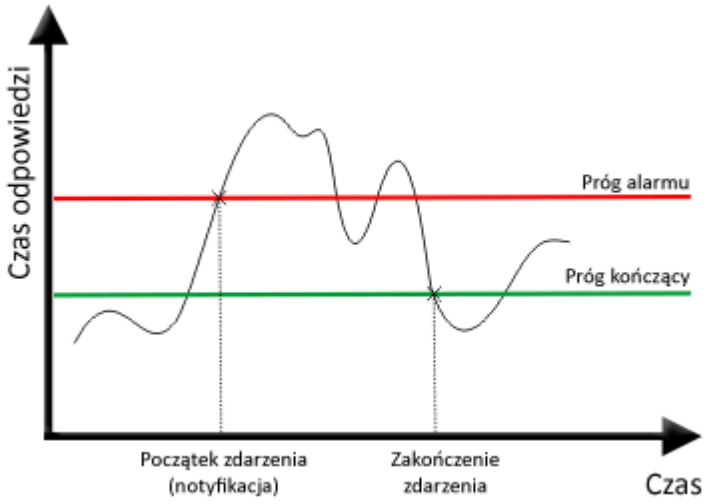
12.4.5 Progi narastające, opadające i kończące

Dla większości zdarzeń definiowana jest wartość progu, która wskazuje kiedy zdarzenie ma zostać wygenerowane. Na przykład - dla serwisu określa on jak wolno serwis może odpowiadać zanim zdarzenie zostanie wygenerowane.

Istnieją jednak zdarzenia, dla których należy zdefiniować także próg "kończący". Jego znaczenie jest istotne - zapobiega on generowaniu zdarzenia za każdym razem, gdy warunek zdarzenia jest spełniony.

Powodowałoby to sytuację, w której alarm byłby generowany co kilka minut. Mierzona wartość musi najpierw spaść poniżej progu kończącego zanim następny alarm zostanie wygenerowany.

Czerwona linia pokazuje próg alarmu - kiedy czas odpowiedzi (lub procent utraconych pakietów) serwisu lub wartość licznika wydajności przekroczy ten próg, alarm zostanie wygenerowany. Następny alarm zostanie jednak dopiero wygenerowany gdy dana wartość spadnie poniżej progu kończącego. Ten mechanizm zapobiega cyklicznemu generowaniu alarmu dla jednego zdarzenia.



Progi narastające i opadające

Próg opisany powyżej jest nazywany progiem narastającym, ponieważ generuje on alarm gdy mierzona wartość go przekroczy. Istnieje także możliwość zdefiniowania zdarzenia, które określa sytuację, w której mierzona wartość powinna znajdować się powyżej progu. Wtedy alarm jest generowany gdy owa wartość spadnie poniżej progu alarmu, dlatego ten typ progu nazywany jest progiem opadającym.

Uwaga

- Próg kończący nie może mieć większej wartości niż próg alarmu dla progów narastających i mniejszej dla progów opadających.

12.5 Akcje

12.5.1 Wprowadzenie

W większości przypadków gdy definiujesz zdarzenie, chcesz zostać poinformowany o jego wystąpieniu, lub chcesz aby zostały wykonane czynności naprawcze mające rozwiązać niepożądaną sytuację. nVision pozwala na tworzenie obydwu typów akcji: notyfikacyjnych i korekcyjnych. Dlatego też przed definicją alarmu należy utworzyć zbiór akcji, które mają być wykonane gdy alarm zostanie wygenerowany.

Można zdefiniować takie akcje jak: wysłanie wiadomości e-mail, ICQ lub SMS, odegranie dźwięku, wyświetlenie okna dialogowego, uruchomienie zewnętrznego programu. Pełna lista dostępnych akcji znajduje się w rozdziale Typy akcji.

12.5.2 Typy akcji

Istnieje kilka ogólnych grup akcji. Poniższa lista je opisuje:

Akcja	Opis
Powiadomienie pulpitowe	
Alarm pulpitowy	Małe okienko informujące o alarmie zostanie pokazane na zdefiniowanej pozycji. Okno to nie przeszkadza w wykonywaniu aktualnych zadań na komputerze.
Dźwięk	nVision odegra zdefiniowany dźwięk.
Mowa	nVision korzystając z syntezatora mowy odczyta treść alarmu.
Wyślij wiadomość	
E-mail	Wysłana zostanie wiadomość e-mail zawierająca informacje o alarmie; *(można wprowadzić kilka adresów odbiorców po średniku ";").*
ICQ	Wysłana zostanie wiadomość ICQ zawierająca informacje o alarmie.
SMS przez GSM	Wysłanie wiadomości SMS przy pomocy podłączonego telefonu lub modemu GSM.
Wiadomość SysLog	Wiadomość SysLog zostanie wysłana do zdefiniowanego serwera SysLog.
Program lub skrypt	
Uruchom lokalny program	Uruchamia zewnętrzny program na lokalnym komputerze.
Uruchom zdalny program	Uruchamia program na zdalnym komputerze z systemem Windows
Inny	
Zapisz do pliku	Informacja o alarmie jest zapisywana do pliku.
Wyślij pułapkę SNMP	Wysłanie komunikatu SNMP Trap.
Wyślij pakiet Wake On LAN	Wysłanie pakietu włączającego/wybudzającego wybrane urządzenie.
Windows	
Uruchom/zatrzymaj usługę Windows	Kontroluje usługi na zdalnym lub lokalnym komputerze z systemem Windows.
Zamknij/restartuj komputer	Wyłącza lub restartuje zdalnie komputer z systemem Windows.

Akcja	Opis
Dodaj wpis do dziennika zdarzeń Windows	Tworzy wpis do dziennika zdarzeń Windows na lokalnym lub zdalnym komputerze z systemem Windows.

12.5.3 Zarządzanie akcjami

Aby skonfigurować nVision tak, aby notyfikowało o wygenerowanych zdarzeniach, należy wcześniej zdefiniować wszelkie możliwe sposoby notyfikacji, z jakich chcemy korzystać. Niniejszy rozdział dostarcza więcej informacji na temat zarządzania akcjami.

Otwieranie okna zarządzania akcjami

Za pomocą tego okna możesz przeglądać, modyfikować, tworzyć nowe oraz usuwać akcje. Aby otworzyć to okno, wybierz **Narzędzia | Zarządzaj akcjami** z menu głównego programu.

Tworzenie nowej akcji lub modyfikowanie istniejącej

1. Otwórz okno zarządzania akcjami.
2. Kliknij przycisk **Dodaj akcję** aby utworzyć nową akcję lub wybierz istniejącą i kliknij przycisk **Edytuj akcję**. Zostanie otwarty **Kreator definicji akcji**.
3. Jeśli tworzysz nową akcje, wpisz jej nazwę w polu **Nazwa akcji** i wybierz jej typ z listy znajdującej się poniżej tego pola. Kliknij przycisk **Dalej**. Aby dowiedzieć się więcej na temat typów akcji, przejdź do rozdziału Typy akcji.
4. Skonfiguruj właściwości akcji (w zależności od typu akcji, który wybrałeś). Aby uzyskać więcej informacji na ten temat przejdź do rozdziału Definiowanie własności akcji.
5. W tym momencie może się okazać niezbędne skonfigurowanie danej akcji. Taka konfiguracja jest niezbędne do poprawnego działania niektórych akcji (np. adres serwera SMTP dla wiadomości e-mail, lub port COM, do którego jest podłączony modem GSM). Konfigurowanie akcji jest omówione w rozdziale Konfigurowanie akcji.
6. Jeśli wszystkie opcje są zdefiniowane, możesz przetestować działanie akcji korzystając z przycisku **Testuj -** wykona on akcję tak, abyś mógł sprawdzić, czy wszystko zostało poprawnie ustawione.
7. Kliknij przycisk **Zakończ**.

12.5.4 Definiowanie własności akcji

Ten rozdział omawia definiowanie własności oraz różne typy akcji.

Powiadomienie pulpitowe

Alarm pulpitowy

Małe okienko informujące o alarmie zostanie pokazane na zdefiniowanej pozycji. Okno to nie przeszkadza w wykonywaniu aktualnych zadań na komputerze.

Własność	Opis
Wiadomość	Pozwala wybrać format wiadomości, jaka zostanie pokazana w oknie alarmowym.
Automatyczna	Wybierz jeśli chcesz wyświetlić wiadomość o alarmie o domyślnej treści.
Użytkownika	Wybierz tę opcję, jeśli chcesz utworzyć własną treść wiadomości. Więcej informacji na ten temat znajdziesz w rozdziale Definiowanie wiadomości alarmowych użytkownika.

Dźwięk

Program odegra zdefiniowany dźwięk.

Własność	Opis
Predefiniowany dźwięk nVision	Wybierz jeden z predefiniowanych dźwięków nVision.
Dźwięk systemowy Windows	Wybierz jeden z predefiniowanych dźwięków systemowych Windows.
Wybierz plik	Kliknij przycisk ... i wybierz plik dźwiękowy, który chcesz odegrać.

Mowa

nVision korzystając z syntezatora mowy odczyta treść alarmu.

Własność	Opis
Wiadomość	Pozwala wybrać format wiadomości, jaka zostanie odczytana przez syntezator mowy.
Automatyczna	Wybierz, jeśli chcesz odegrać wiadomość o alarmie o domyślnej treści.
Użytkownika	Wybierz tę opcję, jeśli chcesz utworzyć własną treść wiadomości. Więcej informacji na ten temat znajdziesz w rozdziale Definiowanie wiadomości alarmowych użytkownika.

Wyślij wiadomość

E-mail

nVision wyśle wiadomość e-mail z informacjami o alarmie.

Własność	Opis
Wyślij e-mail do	Adres e-mail, na jaki ma zostać wysłana wiadomość. Możesz podać kilka adresów email, rozdzielając je przecinkami, średnikami, lub spacjami.
Temat	Temat wiadomości e-mail. W temacie możesz użyć zmiennych opisanych w rozdziale Definiowanie wiadomości alarmowych użytkownika.
Treść wiadomości	Pozwala wybrać treść wiadomości, która zostanie użyta do wygenerowania wiadomości alarmowej.
HTML	Domyślna treść wiadomości.
Krótki tekst	Krótki tekst z podstawowymi informacjami o alarmie.
Długi tekst	Tekst z kompletnymi informacjami o alarmie.
XML	Format XML. Można go wykorzystać do zbudowania własnych zewnętrznych programów obsługujących alarmy. Twój program może otrzymać wiadomość w formacie XML, zinterpretować ją i wykonać dodatkowe zadania.
Użytkownika	Wybierz tę opcję, jeśli chcesz utworzyć własną treść wiadomości. Więcej informacji na ten temat znajdziesz w rozdziale Definiowanie wiadomości alarmowych użytkownika.

ICQ

nVision wyśle wiadomość ICQ z informacjami o alarmie.

Własność	Opis
Numer ICQ	Numer konta ICQ, na jaki zostanie wysłana wiadomość o alarmie.
Treść wiadomości	Pozwala wybrać format wiadomości, który zostanie użyty do wygenerowania wiadomości alarmowej.
Użytkownika	Wybierz tę opcję, jeśli chcesz utworzyć własną treść wiadomości. Więcej informacji na ten temat znajdziesz w rozdziale Definiowanie wiadomości alarmowych użytkownika.

SMS przez GSM

Wysłanie wiadomości SMS przy pomocy podłączonego telefonu lub modemu GSM.

Własność	Opis
Numer telefonu	Numer telefonu, na jaki ma zostać wysłana wiadomość SMS. Musi się zaczynać prefiksem z kodem kraju (+48 dla Polski).

Własność	Opis
Wiadomość alarmowa	Wybierz tę opcję, jeśli chcesz aby wiadomość została wyświetlona od razu na ekranie telefonu komórkowego.
Automatyczna	Domyślna treść wiadomości
Użytkownika	Wybierz tę opcję, jeśli chcesz utworzyć własną treść wiadomości. Więcej informacji na ten temat znajdziesz w rozdziale Definiowanie wiadomości alarmowych użytkownika.

Wiadomość SysLog

Wiadomość SysLog zostanie wysłana do zdefiniowanego serwera SysLog.

Własność	Opis
Adres zdalnego komputera	Adres serwera SysLog.
Port zdalnego komputera	Port na jakim działa serwis SysLog.
Wiadomość	Zdefiniuj treść wiadomości w polu edycji. Więcej informacji na temat definiowania wiadomości znajdziesz w rozdziale Definiowanie wiadomości alarmowych użytkownika.

Program lub skrypt

Uruchom lokalny program

Uruchamia program na lokalnym komputerze.

Własność	Opis
Uruchom program	Kliknij przycisk [...] i wybierz program, który ma zostać uruchomiony.
Parametry	Wpisz parametry uruchomienia programu. Możesz użyć zmiennych opisanych w rozdziale Definiowanie wiadomości alarmowych użytkownika.

Uruchom zdalny program

Ta opcja pozwala na skopiowanie i uruchomienie dowolnego programu zdalnie, na przykład w celu podjęcia akcji korekcyjnej.

Własność	Opis
Skopiuj lokalny program do zdalnego komputera i	Wybranie tej opcji powoduje wykonanie dwóch akcji: kopiowania i uruchomienia.

Własność	Opis
uruchom	Kliknij przycisk i wybierz plik z programem lokalnym, który ma zostać uruchomiony. Następnie wybierz katalog docelowy, do którego ma zostać skopiowany.
Uruchom zdalny program	Kliknij przycisk i wybierz plik z programem zdalnym, który ma zostać uruchomiony

Inny

Zapisz do pliku

Zapisuje informacje o alarmie do pliku.

Własność	Opis
Zapis do pliku	Kliknij przycisk i wybierz plik, w którym wiadomość alarmowa ma zostać zapisana.
Treść wiadomości	Pozwala wybrać treść wiadomości, która zostanie użyta do wygenerowania wiadomości alarmowej.
HTML	Domyślna treść wiadomości
Krótki tekst	Krótki tekst z podstawowymi informacjami o alarmie.
Długi tekst	Tekst z kompletnymi informacjami o alarmie.
XML	Format XML. Można go wykorzystać do zbudowania własnych zewnętrznych programów obsługujących alarmy. Twój program może odczytać plik w formacie XML, zinterpretować ją i wykonać dodatkowe zadania.
Użytkownika	Wybierz tę opcję, jeśli chcesz utworzyć własny format wiadomości. Więcej informacji na ten temat znajdziesz w rozdziale Definiowanie wiadomości alarmowych użytkownika.

Wyślij pułapkę SNMP

Wysyła pułapkę SNMP do zdalnego urządzenia.

Własność	Opis
Nazwa	Nazwa DNS lub adres IP zdalnego urządzenia.
Port	Numer portu UDP zdalnego urządzenia.
Wspólnota	Nazwa wspólnoty SNMP.

Własność	Opis
Typ PDU	Typ nagłówka pakietu PDU.
Agent	Adres IP Agenta SNMP.
Typ usługi	Rodzaj pułapki SNMP.
ID notyfikacji	Jest wymagane, jeśli jak Typ usługi podano 'enterpriseSpecific.'

Wyślij pakiet Wake On LAN

Wysyła pakiet Wake On LAN do zdalnego urządzenia.

Własność	Opis
Użyj adresu urządzenia	Do identyfikacji zostanie użyty adres IP oraz MAC urządzenia.
Adres MAC	Adres zdalnego urządzenia w notacji AA:BB:CC:DD:EE:FF.
Adres rozgłoszeniowy	Adres docelowy pakietu Wake On LAN .
Port	Numer portu UDP zdalnego urządzenia.
Hasło SecureOn	Hasło SecureOn zdalnego urządzenia w notacji szesnastkowej np. AA:BB:CC:DD:EE:FF.

Windows

Uruchom/zatrzymaj usługę Windows

Kontroluje usługi na zdalnym lub lokalnym komputerze z systemem Windows.

Własność	Opis
Usługa Windows, która wygenerowała alarm	Zaznacz tę opcję, jeśli chcesz aby akcja była wykonana na komputerze i usłudze, która wygenerowała alarm.
Wybrana usługa Windows	Zaznacz tę opcję, jeśli chcesz aby akcja była wykonana na wybranym komputerze i usłudze Windows.
Komputer	Wybierz komputer, na którym ma być wykonana akcja.
Usługa	Wybierz usługę Windows.
Akcja	Wybierz akcję jaka ma zostać wykonana: możesz uruchomić, zatrzymać, spauzować lub wznowić usługę Windows.

Zamknij/restartuj komputer

Wyłącza lub restartuje zdalnie komputer z systemem Windows.

Własność	Opis
Komputer, który wygenerował alarm	Zaznacz tę opcję, jeśli chcesz aby akcja była wykonana na komputerze, który wygenerował alarm.
Wybrany komputer	Zaznacz tę opcję, jeśli chcesz aby akcja była wykonana na wybranym komputerze.
Zrestartuj	Restartuje komputer
Wyłącz	Wyłącza komputer

Dodaj wpis do dziennika zdarzeń Windows

Ta akcja pozwala na dodanie wpisu w dzienniku zdarzeń Windows na wybranym urządzeniu.

Własność	Opis
Komputer, na którym zainicjowano zdarzenie	Zaznacz tę opcję, jeśli chcesz aby akcja była wykonana na komputerze, który wygenerował alarm.
Wybrany komputer	Zaznacz tę opcję, jeśli chcesz aby akcja była wykonana na wybranym komputerze.

Własność	Opis
Typ wiadomości	Wybierz typ wiadomości (Sukces, Błąd, Ostrzeżenie, Informacja).

12.5.5 Konfigurowanie akcji

Większość akcji wymaga ich poprawnego skonfigurowania, zanim nVision będzie w stanie je wykonać. Na przykład: adres serwera SMTP dla wiadomości email, lub port COM, do którego jest podłączony modem GSM. Ten rozdział omawia konfigurację kilku typu akcji (niektóre akcji nie posiadają opcji).

Akcja może być konfigurowana w opcjach programu, lub podczas tworzenia nowej akcji lub modyfikacji istniejącej.

Powiadomienie pulpitowe

Okno alarmowe

Małe okienko informujące o alarmie zostanie pokazane na zdefiniowanej pozycji. Okno to nie przeszkadza w wykonywaniu aktualnych zadań na komputerze.

Własność	Opis
Pozycja	Określa pozycję na pulpicie, na której pojawi się okno alarmowe.
Czas wyświetlania	Określa czas, jak długo okno ma być wyświetlane.
Zanikanie stopniowe	Zaznacz tę opcję, jeżeli chcesz, aby okno stopniowo zanikało.

Synteza mowy

nVision korzystając z syntezatora mowy odczyta treść alarmu.

Własność	Opis
Silnik syntezy mowy	Silnik syntezy mowy, z którego chcesz skorzystać.
Tempo czytania	Tempo czytania

Wyślij wiadomość

E-mail

nVision wyśle wiadomość email z informacjami alarmie.

Własność	Opis
Adres zwrotny	Jeśli adres nie zostanie poprawnie ustawiony, większość serwerów pocztowych może odrzucić taką wiadomość. Wpisz adres e-mail, o którym wiesz, że na pewno zostanie zaakceptowany przez serwer pocztowy (najczęściej Twój własny adres).
Połączenie	Ustaw limit czasu, liczbę prób i czas powtarzania.
Użyj zewnętrznego serwera SMTP	nVision posiada własny wbudowany serwer SMTP, ale możesz użyć zewnętrznego jeśli chcesz. Włącz tą opcję i określ poniższe właściwości.
Adres	Adres zewnętrznego serwera pocztowego.
Port	Numer portu, na jakim serwer pocztowy jest uruchomiony.
Wymaga autoryzacji	Jeśli zewnętrzny serwer pocztowy wymaga autoryzacji, zaznacz tę opcję i wpisz nazwę użytkownika i hasło w odpowiednich polach.
Nazwa użytkownika	Nazwa użytkownika wymagana do zalogowania się.
Hasło	Hasło wymagane do zalogowania się.

ICQ

nVision wyśle wiadomość ICQ z informacjami alarmie.

Własność	Opis
Serwer ICQ	Adres serwera ICQ.
Port	Numer portu, na którym działa serwer ICQ.
UIN	UIN, z którego nVision skorzysta aby wysłać wiadomość.
Hasło	Hasło wymagane do zalogowania się.

SMS przez GSM

Akcja powoduje wysłanie SMSa prze dołączony telefon GSM lub modem.

Własność	Opis
Ustawienia portu COM	Ustaw port COM, prędkość, bity danych, parzystość i bity stopu.
Ustawienia SMS	Zaznacz odpowiednie opcje, aby dzielić długie wiadomości oraz aby podać specjalny numer centrum obsługi (SMSC).
Informacje o urządzeniu	Wciśnij przycisk **Wykryj urządzenie**, aby zobaczyć nazwę

Własność	Opis
	producenta i model.

Aby dowiedzieć się więcej o konfigurowaniu urządzenia GSM, przejdź do rozdziału Konfiguracja urządzenia GSM.

12.5.6 Definiowanie wiadomości alarmowych użytkownika

Podczas definiowania akcji notyfikujących o alarmach, można skorzystać z mechanizmu wiadomości użytkownika, aby dostosować do własnych potrzeb treść wiadomości, jaka zostanie wysłana/zapisana. nVision pozwala na użycie kilku nazw zmiennych, które zostaną zamienione w odpowiednią wartość podczas tworzenia wiadomości alarmowej. Ten rozdział opisuje owe zmienne i sposób korzystania z nich.

Zmienne

Nazwa zmiennej	Opis
$Host.Name	Nazwa urządzenia, dla którego alarm został wygenerowany.
$Host.Type	Typ urządzenia. Aby uzyskać więcej informacji na ten temat przejdź do rozdziału Właściwości urządzenia.
$Host.Importance	Ważność urządzenia. Zobacz: Właściwości urządzenia.
$Host.Status	Stan urządzenia. Określa stan urządzenia w momencie, w którym alarm jest generowany. W przypadku akcji uruchamianych z opóźnieniem, stan urządzenia może być inny niż podczas generowania alarmu.
$Host.Info1	Pole urządzenia Info1. Zobacz: Właściwości urządzenia.
$Host.Info2	Pole urządzenia Info2. Zobacz: Właściwości urządzenia.
$Host.ParentHost	Urządzenie nadrzędne. Zobacz: Właściwości urządzenia.
$Host.SNMPManagable	Informacja, czy dane urządzenie jest zarządzalne przez SNMP. Zobacz: Właściwości urządzenia.
$Host.SNMPSystem	Opis systemu urządzenia odczytany przez SNMP. Zobacz: Właściwości urządzenia.
$Host.SNMPLocation	Lokalizacja urządzenia odczytana przez SNMP. Zobacz: Właściwości urządzenia.
$Host.SNMPName	Nazwa urządzenia odczytana przez SNMP. Zobacz: Właściwości urządzenia.
$Alert.Name	Nazwa alarmu - nazwa zdarzenia, które zostało wygenerowane na urządzeniu.
$Alert.Description	Krótki opis zdarzenia.
$Alert.Type	Typ zdarzenia. Przejdź do rozdziału Typy zdarzeń aby uzyskać więcej

Nazwa zmiennej	Opis
	informacji.
$Alert.Severity	Ważność zdarzenia, które wygenerowało alarm.
$Alert.StartTime	Czas wygenerowania alarmu.
$Alert.Duration	Czas trwania alarmu.
$Alert.Resolution	Stan rozwiązania alarmu.
$Alert.Owner	Właściciel alarmu.

Jak korzystać ze zmiennych?

Gdy program pozwala na zdefiniowanie wiadomości użytkownika, wtedy można skorzystać ze zmiennych. Wystarczy wpisać nazwę zmiennej w polu tekstowym wiadomości, lub skorzystać z przycisku  .Po kliknięciu tego przycisku zostanie wyświetlona lista zmiennych - po wybraniu jednej, zostanie automatycznie wklejona do pola tekstowego.

12.6 Wygenerowane alarmy

12.6.1 Przetwarzanie alarmów

Jak nVision przetwarza alarmy?

W większości programów służących do monitorowania sieci komputerowych można tylko zdefiniować kiedy alarm ma zostać wygenerowany, ale nie ma możliwości otrzymania potem informacji o czasie trwania takiego alarmu. Nie ma także możliwości zdefiniowania akcji, które mają zostać wykonane, gdy warunki alarmu przestaną być spełnione. W nVision każdy wygenerowany alarm ma swój czas rozpoczęcia i czas zakończenia. Gdy warunki zdarzenia określającego alarm zachodzą, nVision generuje alarm. Następnie nVision cyklicznie sprawdza, czy dane warunki są ciągle spełnione i kończy alarm, gdy już nie są. Oznacza to, że można uzyskać informacje o czasie rozpoczęcia i zakończenia alarmu, wraz z jego czasem trwania.

Gdy alarm zostaje wygenerowany, nazywany jest wtedy alarmem otwartym i stan takiego alarmu jest ustawiany na <Otwarty>. Pozostaje otwarty tak długo, jak długo warunki zdarzenia są spełnione, lub gdy warunki zakończenia nie zostały jeszcze spełnione. Gdy wszystkie warunki potrzebne do zakończenia alarmu są spełnione, nVision zamyka alarm i zmienia jego stan na <Zamknięty>, wskazując tym samym, że nie tylko alarm został zakończony, ale także, że zdarzenie, które go uruchomiło nie ma już miejsca.

Jak nVision uruchamia akcje?

Gdy alarm zostaje wygenerowany, wszystkie akcje, które są związane z nim (i ustawione do natychmiastowego uruchomienia) są uruchamiane. Wszystkie akcje, ustalone jako opóźnione będą wykonane tylko wtedy jeśli alarm pozostanie otwarty. Gdy alarm jest zamykany, uruchamiane są wszystkie akcje przypisane na zamknięcie alarmu. Można także zaniechać uruchamiania pozostałych akcji zmieniając stan Rozwiązania alarmu.

Każdy alarm jest generowany z Rozwiązaniem ustawionym na <Nowy>. Jeśli chcesz zaznaczyć, że

zostałeś już poinformowany o danym alarmie i nie chcesz być informowany dalej, musisz potwierdzić alarm. Aby to zrobić należy ustawić w Dzienniku Zdarzeń nVision Rozwiązanie alarmu na <Potwierdzony>. Podobnie: jeśli problem, który spowodował wygenerowanie alarmu, został już naprawiony, możesz ustawić Rozwiązanie alarmu na <Rozwiązany>. Podsumowując: zmiana stanu Rozwiązania alarmu zapobiega dalszemu wykonywaniu akcji alarmu.

12.6.2 Dziennik zdarzeń

Wszystkie wygenerowane alarmy są zapisywane przez nVision i dostępne w Dzienniku Zdarzeń. Dziennik Zdarzeń prezentuje wszystkie wygenerowane alarmy, ich stan, a także wszystkie akcje przypisane do danego alarmu. Pozwala także zmieniać stan Rozwiązania alarmu, oraz sortować i filtrować listę alarmów, aby ułatwić ich przeglądanie.

Ikony użyte w tabeli Alarmy i Akcje

Tabela Alarmy

Ikona	Opis
Stan - określa stan alarmu	
	Alarm otwarty
	Alarm zamknięty (zakończony)
Rozwiązanie - pozwala administratorowi zarządzać alarmami	
	Nowy alarm
	Alarm, który został potwierdzony przez administratora i którego akcje nie będą już wykonywane
	Alarm, który został już rozwiązany przez administratora i którego akcje nie będą już wykonywane
Typ zdarzenia - typ zdarzenia, które wygenerowało alarm	
	Dostępność urządzenia lub usługi
	Test wydajności konkretnego serwisu
	Licznik wydajności
Ważność zdarzenia - ważność zdarzenia, które wygenerowało alarm	
	Niska ważność
	Normalna ważność
	Wysoka ważność
	Krytyczna ważność
Stan urządzenia	
	Działa

Ikona	Opis
	Ostrzeżenie
	Nie działa

Tabela akcji

Ikona	Opis
Typ - typ akcji	
	Alarm pulpitowy
	Wiadomość
	Program lub skrypt
	Inne
Stan - określa stan wykonania akcji	
	Jeszcze nie wykonana
	Akcja aktualnie wykonywana
	Pomyślnie wykonana
	Błąd wykonania (w kolumnie Info znajduje się opis błędu)

Otwieranie Dziennika Zdarzeń

Możesz wyświetlić zdarzenia dla konkretnego urządzenia lub dla całego atlasu. Aby wyświetlić Dziennik Zdarzeń dla atlasu wybierz z menu głównego **Dziennik zdarzeń** z sekcji Raporty i Alarmy. Aby wyświetlić Dziennik Zdarzeń dla pojedynczego urządzenia przejdź do okna **Informacje o urządzeniu,** a następnie do zakładki **Zdarzenia**.

Odblokowywanie Alarmów (zmiana stanu rozwiązania alarmów)

Aby odblokować alarm, musisz zmienić stan jego Rozwiązania na <Potwierdzony> lub <Rozwiązany>.

1. Zaznacz alarm lub wiele alarmów.
2. Wybierz **Potwierdź** lub **Rozwiąż** z menu kontekstowego.

Aby uzyskać więcej informacji na temat zmiany stanu Rozwiązania alarmów przejdź do rozdziału Wygenerowane alarmy.

Sortowanie i filtrowanie

- Możesz sortować obie tabele względem konkretnej kolumny klikając jej nagłówek.
- Możesz filtrować zdarzenia przez stan lub stan rozwiązania. Aby wyświetlić tylko te alarmy,

które mają określony stan/stan rozwiązania wybierz odpowiednią wartość z pola **Filtruj**.

Zmiana przedziału czasowego

Możesz przeglądać alarmy dla jednego dnia, tygodnia lub miesiąca. Aby wybrać przedział czasowy, skorzystaj z paska narzędzi. Aby przeglądać archiwalne wpisy w Dzienniku Zdarzeń skorzystać ze strzałek znajdujących się na pasku narzędzi. Podczas przeglądania zawsze będzie wyświetlony aktualny przedział czasowy.

Część XIII

13 Kopie zapasowe bazy danych

13.1 Tworzenie i przywracanie kopii zapasowych Atlasu

Informacja o atlasie znajduje się w katalogu **\Database\AtlasPG**.

Aby zrobić kopię zapasową należy uruchomić skrót **DBBackup**, który znajduje się w katalogu **"{nVision}\Backups"**. Z kolei uruchomienie skrótu **DBRestore** odtworzy wybraną kopię zapasową bazy danych nVision.

13.2 Automatyczny backup

Profile

Tworzenie kopii zapasowych opiera się na zdefiniowanych profilach. W każdym z profili można ustawić:

- katalog, w którym będą zapisywane utworzone kopie zapasowe,
- nazwę profilu,
- datę tworzenia kopii,

Kopia zapasowa obejmuje dane:

- zebrane wpisy Dziennika Systemowego Windows,
- wygenerowane alarmy,
- historia monitorowania liczników i serwisów,
- dane aktywności użytkowników,
- dane inwentaryzacji.

Reguły kopii zapasowych

Aby skonfigurować tworzenie kopii zapasowych, można użyć wielu profili. Dla każdego z nich ustawia się częstotliwość wykonywania kopii (każdego dnia, tygodnia lub miesiąca) oraz kiedy kopia ma być tworzona. W każdym przypadku ustawia się godzinę, o której ma się rozpocząć wykonywanie kopii zapasowej. Jeśli backup ma być tworzony raz na tydzień, należy ustawić dodatkowo dzień tygodnia, a jeśli raz na miesiąc - dzień miesiąca. W przypadku dużych baz danych tworzenie kopii zapasowej może być zadaniem czasochłonnym, stąd tworzenie pełnych kopii dobrze jest planować w takich godzinach, by nie utrudniało korzystania z nVision w trakcie pracy.

Konfiguracja

Aby skonfigurować automatyczne tworzenie kopii zapasowych:

1. Wybierz z menu głównego **Narzędzia / Opcje**.
2. Wybierz z listy **Konserwacja**.
3. Dodaj nową regułę używając przycisku lub **Edytuj** jedną z istniejących reguł.
4. W oknie Reguł kopii zapasowych wybierz istniejący profil lub utwórz nowy (aby utworzyć nowy rozwiń menu przy przycisku **Edytuj**, wybierz opcję **Dodaj** i skonfiguruj ustawienia nowego profilu).

5. Ustaw częstotliwość wykonywania kopii zapasowej oraz kiedy ma być ona wykonywana.
6. Możesz również zdefiniować ilość przechowywanych kopii zapasowych.

13.3 Rozmiar bazy danych

W wyniku gromadzenia dużej ilości danych w monitorowanych sieciach wielkość bazy może przyrastać w szybkim tempie. Rozdział ten wyjaśnia, jak zapobiegać nadmiernemu zwiększaniu się bazy.

Zarządzanie wielkością bazy może się odbywać poprzez:

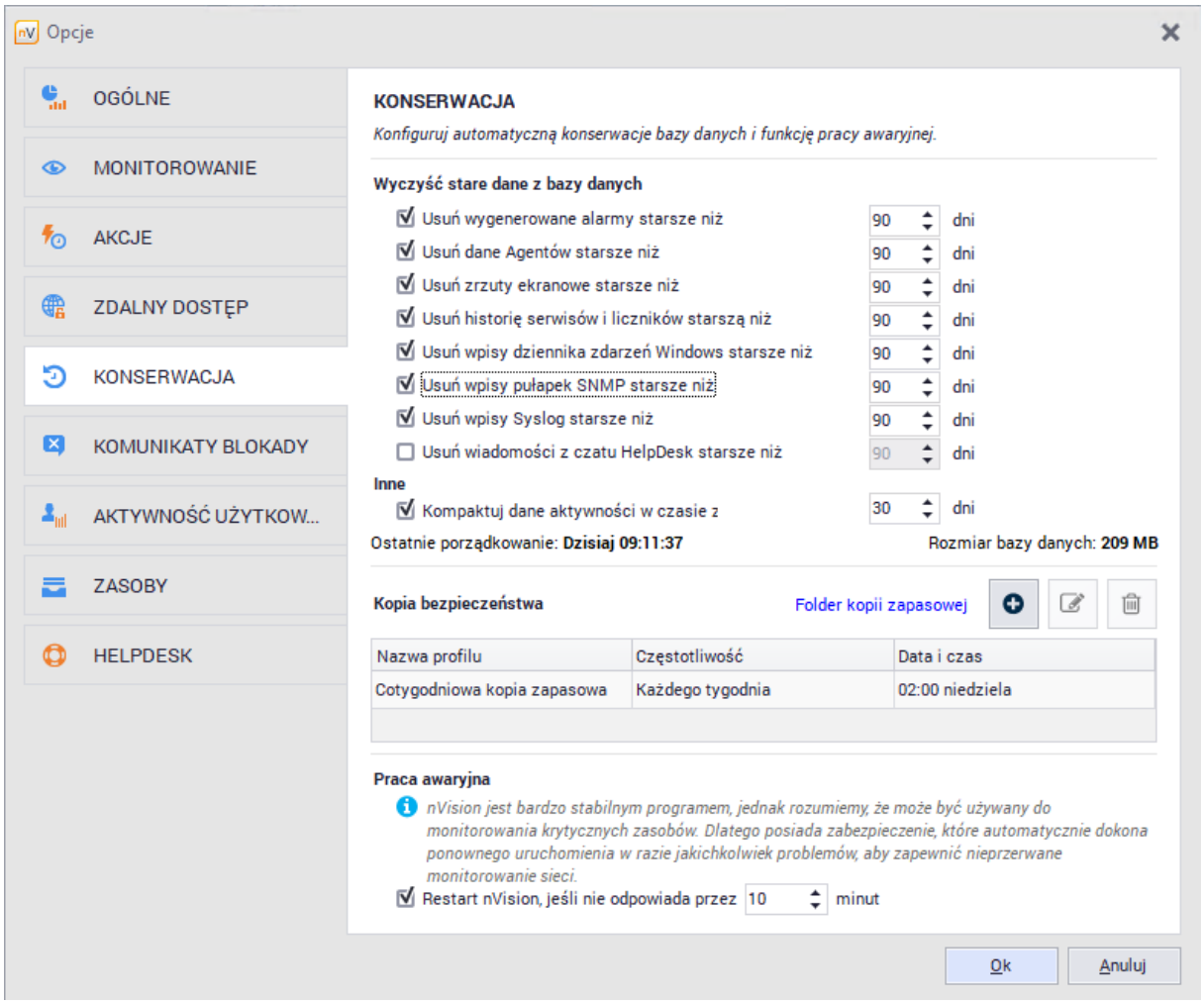
- Ustawienie czasu usuwania nieaktualnych danych
- Kompaktowanie
- Opcje monitorowania dziennika zdarzeń Windows
- Naprawianie bazy

Ustawienie czasu usuwania nieaktualnych danych

Aby ustawić czas, po którym nieaktualne dane będą usuwane, należy użyć opcji porządkowania **(Opcje / Konserwacja**). Usuwanie danych odbywa się raz na dobę w godzinach nocnych.

Zmniejszenie czasu, po którym usuwane są nieaktualne dane nie spowoduje zmniejszenia rozmiaru bazy danych, a jedynie zatrzyma jej przyrost na pewnym etapie. Dzieje się tak dlatego, że nieaktualne wpisy nie są z bazy usuwane, tylko nadpisywane przez napływające nowe dane.

*W największym stopniu rozmiar bazy danych powiększają zrzuty ekranowe. Dlatego podczas włączania tej opcji w oknie **"Informacje o urządzeniu / Aktywność użytkowników / Zrzuty ekranowe"** należy określić datę zakończenia zbierania zrzutów.*



Opcje monitorowania dziennika zdarzeń Windows

Duży przyrost bazy najczęściej wynika z gromadzenia danych o logowaniu użytkowników (Dziennik Zdarzeń Windows). Jeżeli gromadzenie danych Monitorowania Dziennika Zdarzeń Windows nie jest konieczne, odznacz odpowiednie pole we **Właściwościach** urządzenia, zakładka **Monitorowanie**. Jeżeli dane mają być gromadzone, ustaw odpowiedni interwał monitorowania i sprawdź, czy w konfiguracji zaznaczona jest opcja ignorowania wpisów logowania (domyślnie zaznaczona). Takie ustawienie pozwala na odfiltrowanie niepotrzebnych wpisów (ok. 99% wszystkich wpisów).

Część XIV

14 Najczęściej Zadawane Pytania

14.1 Aktualizacja nVision

Kwestie które należy wziąć pod uwagę podczas aktualizacji nVision:

1. Instalacja Serwera nVision na Windows XP nie jest już możliwa - minimalnym wymaganym systemem dla Serwera nVision jest Windows Vista lub Server 2008 lub nowszy, a dla Konsoli nVision i Agenta nVision jest to system Windows XP SP3 lub nowszy.
2. Zaktualizowanie nVision (lub przywrócenie z kopii zapasowej) do wersji 7 jest możliwe jedynie z nVision (lub z kopii zapasowej) ostatniej wersji **6 (6.5.4.14214)** dostępnej pod następującym łączem: http://cdn.Axence.net/nVision6.zip.
3. Po zaktualizowaniu nVision do ostatniej wersji 6 należy **przynajmniej raz uruchomić program (otworzyć Atlas)** po czym zamknąć nVision i wykonać naprawianie bazy danych, które zweryfikuje bazę danych przed procesem aktualizacji.
4. Import Atlasu może być wykonany tylko w konsoli lokalnej.
5. Pierwsze uruchomienie nVision musi nastąpić z konsoli lokalnej celem ustawienia hasła administratora.
6. Konsolę nVision na innym komputerze można zainstalować uruchamiając ten sam plik **nVisionSetup.exe** pobrany celem aktualizacji do nVision 7 - po jego uruchomieniu pojawi się wybór rodzaju instalacji: Serwer+Konsola lub sama Konsola.
7. Zaktualizowanie nVision do wersji 7.5 jest możliwe jedynie z nVision w ostatniej **wersji 7.1 (7.1.3.15872)** dostępnej pod następującym łączem: http://cdn.Axence.net/nVision71.zip - proces ten obejmuje przepisywanie bazy danych stąd może on potrwać dłuższy czas.
8. Ze względu na zmianę silnika bazy danych po zaktualizowaniu nVision do wersji 7.5 zostają zresetowane ustawienia kopii zapasowych, które najlepiej sprawdzić i ewentualnie zmienić według własnych potrzeb.
9. Ze względu na zmianę silnika bazy danych przywrócenie bazy danych z kopii zapasowej w nVision 7.5 jest możliwe jedynie z kopii zapasowej wykonanej w nVision 7.5.
10. **Ostatnia produkcyjna wersja nVision 7 (7.6.2.17769)** jest dostępna pod następującym łączem: http://cdn.Axence.net/nVision7.zip. **Należy ją zainstalować aby zaktualizować nVision do wersji 8.2.**
11. Aktualizacja nVision do **wersji 9** możliwa jest z ostatniej wersji **nVision 8.2 (8.2.1.20202)** dostępnej do pobrania pod następującym łączem: http://cdn.Axence.net/nVision82.zip lub nVision **8.6 (8.6.0.22469)** http://cdn.Axence.net/nVision86.zip
12. Bezpośrednia aktualizacja do **nVision 10** możliwa jest od nVision 8.6. Przed aktualizacją do wersji 10 należy dokładnie zapoznać się z dokumentem dotyczącym technicznych kwestii migracji do wersji 10
13. Archiwalny instalator nVision 9.3.4.25361 dostępny jest do pobrania pod adresem: https://cdn.axence.net/nVision9.zip

14.2 Audyt systemu plików

Z punktu widzenia systemu plików nie istnieje operacja "kopiowania z ... do ...". Aplikacja, która "kopiuje" plik, w rzeczywistości wykonuje operację utworzenia nowego pliku po czym wypełnia go zawartością którą odczytała (pobrała) z dowolnego źródła: inny dysk, dane pobierane z sieci, odczyt

danych z urządzenia podłączonego do komputera, tekst wpisany z klawiatury w oknie aplikacji, itp. Stąd nie ma możliwości logowania przez DataGuard informacji o źródle danych.

14.3 Cicha instalacja i deinstalacja Agenta

Aby zainstalować Agenta bez konieczności interakcji użytkownika, należy użyć na danym komputerze następującego polecenia:

```
nvagentinstall.exe /versilent /nVisionon:ADRES_IP_nVision
```

lub

```
msiexec.exe /i nvagentinstall.msi /qn
```

Aby odinstalować Agenta bez konieczności interakcji użytkownika, należy w Konsoli nVision zaznaczyć wybrane komputery po czym kliknąć prawym klawiszem myszy i z menu kontekstowego wybrać opcje **"Agent \ Odinstaluj"**

lub użyć na danym komputerze następującego polecenia:

```
unins000.exe /versilent /password=HASŁO_CHRONIĄCE_AGENTA
```

14.4 Duplikaty urządzeń

Jeżeli w nVision pojawią się duplikaty urządzeń widoczne w menu **Narzędzia | Pokaż duplikaty urządzeń** należy w wierszu polecenia wykonać następujące komendy względem zduplikowanych adresów IP i nazw DNS:

```
ping -a ADRES_IP
```

oraz:

```
ping -4 NAZWA_DNS
```

po czym porównać wyniki tych operacji (zgodność adresów IP i nazw DNS). W przypadku niezgodności, rozwiązania problemu należy poszukiwać w niewłaściwej konfiguracji serwera DNS (oczyszczanie starych rekordów: http://technet.microsoft.com/en-us/library/cc771677.aspx) i/lub w zbyt krótkim czasie dzierżawy adresów IP na serwerze DHCP (zalecane nie mniej niż okres oczyszczania starych rekordów DNS).

14.5 Działanie opcji "Odinstaluj agenta nVision"

Deinstalacja Agenta jest uruchamiana gdy Agent odbierze polecenie deinstalacji podczas połączenia z serwerem nVision.

Jeżeli brak jest połączenia Agenta z serwerem nVision (przykładowo Agent został tymczasowo wyłączony lub nie działa komputer na którym Agent jest zainstalowany), wówczas deinstalacja nastąpi przy najbliższym połaczeniu się Agenta z serwerem nVision.

14.6 Generowanie raportów w Windows Server

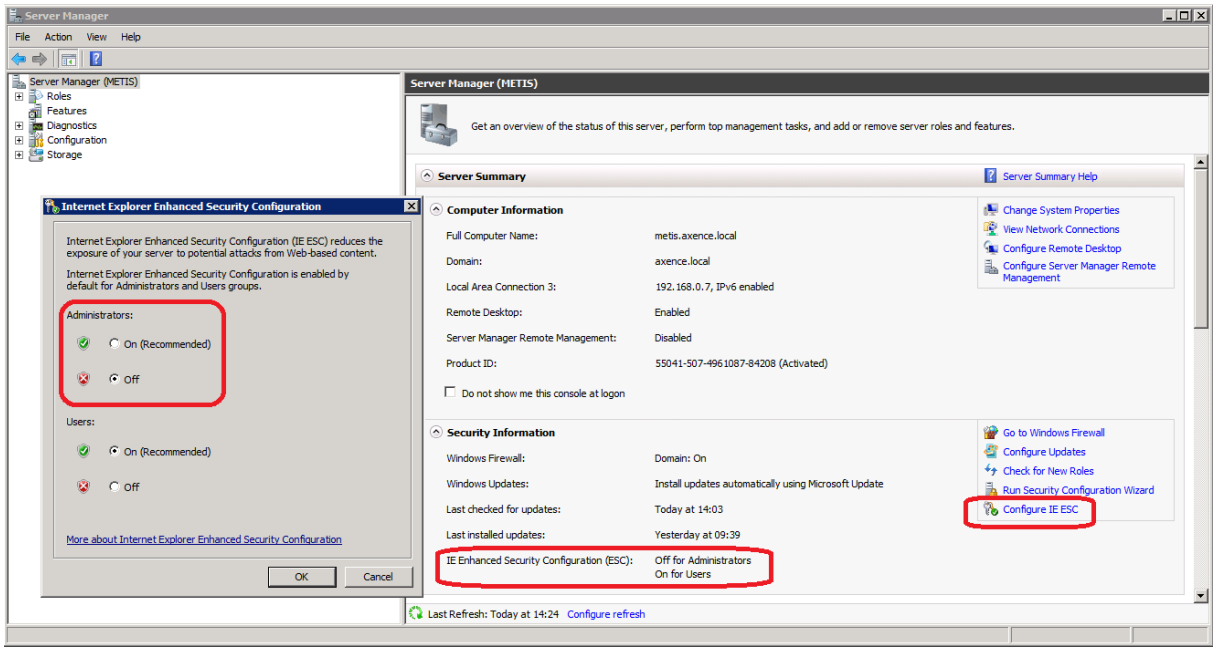
W przypadku problemów z generowaniem raportów w Konsoli nVision zainstalowanej na Windows Server lub w Internet Explorer na tym systemie, należy w konfiguracji Windows Server wyłączyć ustawienie **IE ESC (Internet Explorer Enhanced Security Configuration) dla administratorów**. Po wyłączeniu tej opcji należy zrestartować Konsolę nVision. Wyłączenie tej opcji wiąże się ze zmianą zabezpieczeń

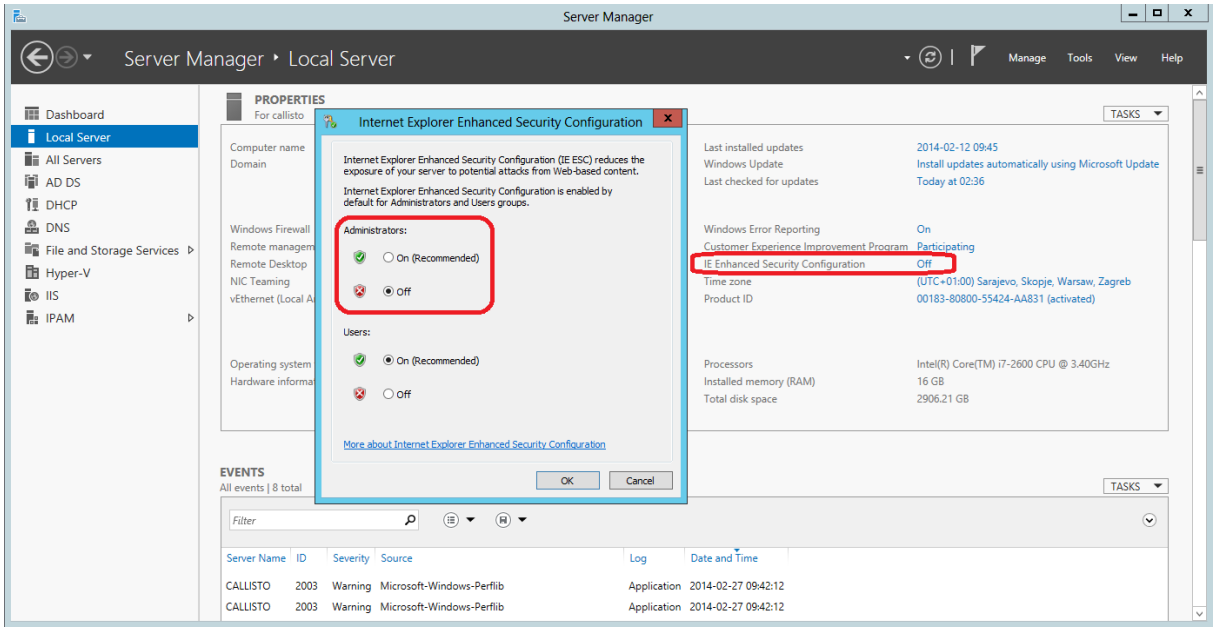
przeglądarki na serwerze, stąd zaleca się wykonywanie raportów w Konsoli nVision zainstalowanej na desktopowej wersji systemu Windows lub w przeglądarce na tym systemie.

Więcej informacji:

http://blogs.technet.com/b/plitpromicrosoftcom/archive/2010/04/30/internet-explorer-enhanced-security-configuration.aspx

http://technet.microsoft.com/en-us/library/dd883248(v=ws.10).aspx





14.7 Instalacja Agenta przez Active Directory

Instrukcja dystrybucji oprogramowania przez Active Directory:

1. Umieścić paczkę **MSI (nvagentinstall.msi)** w udostępnionym katalogu na serwerze, aby stacje

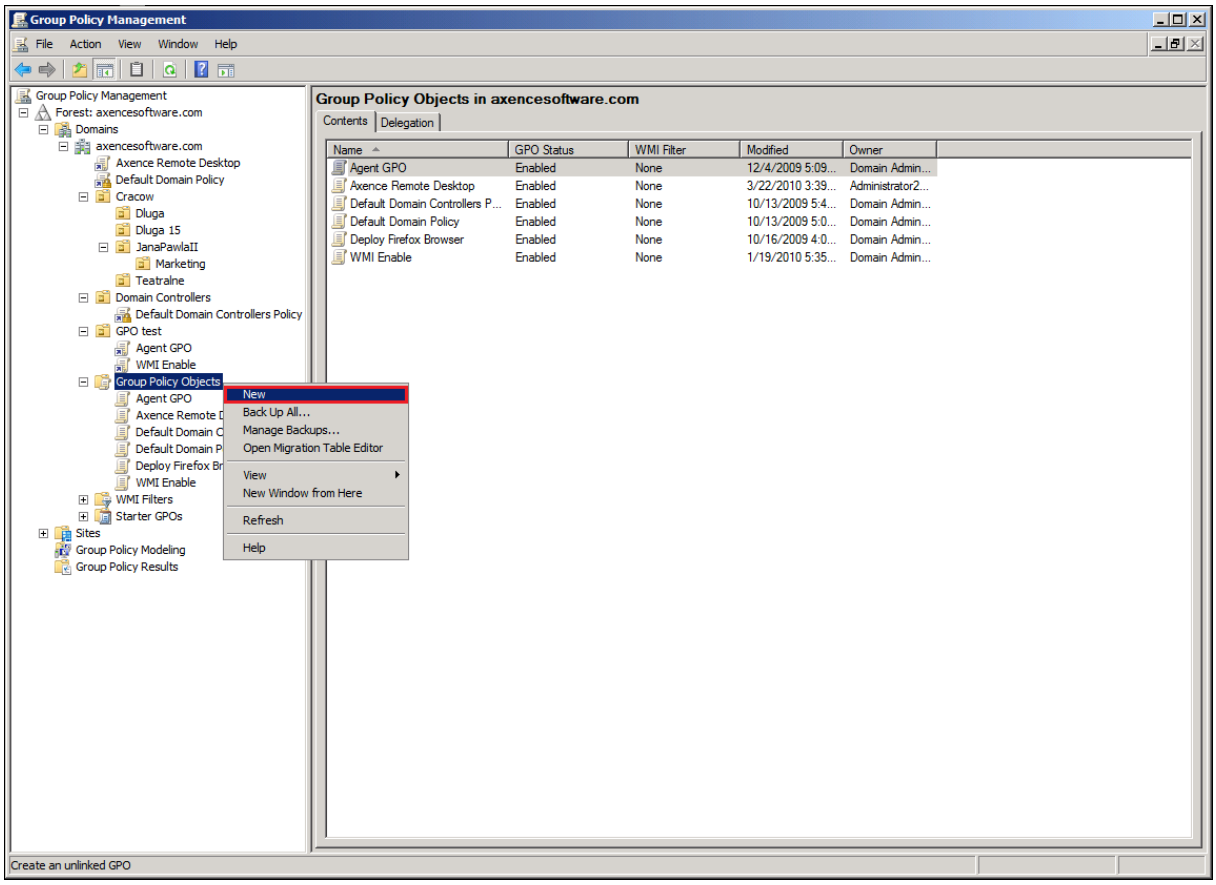
robocze oraz kontroler domeny (serwer obsługujący Active Directory) miały do niego dostęp: należy utworzyć taki katalog, skopiować do niego paczkę oraz ustawić na nim prawa udostępniania - dostęp do zasobu w postaci:

```
\\[NAZWA_SERWERA]\[NAZWA_KATALOGU]\nvagentinstall.msi
```

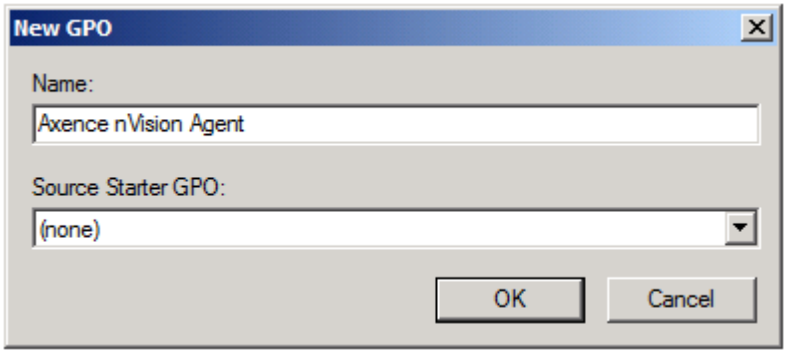
2. Uruchomić **Group Policy Management Console** - polecenie:

```
gpmc.msc
```

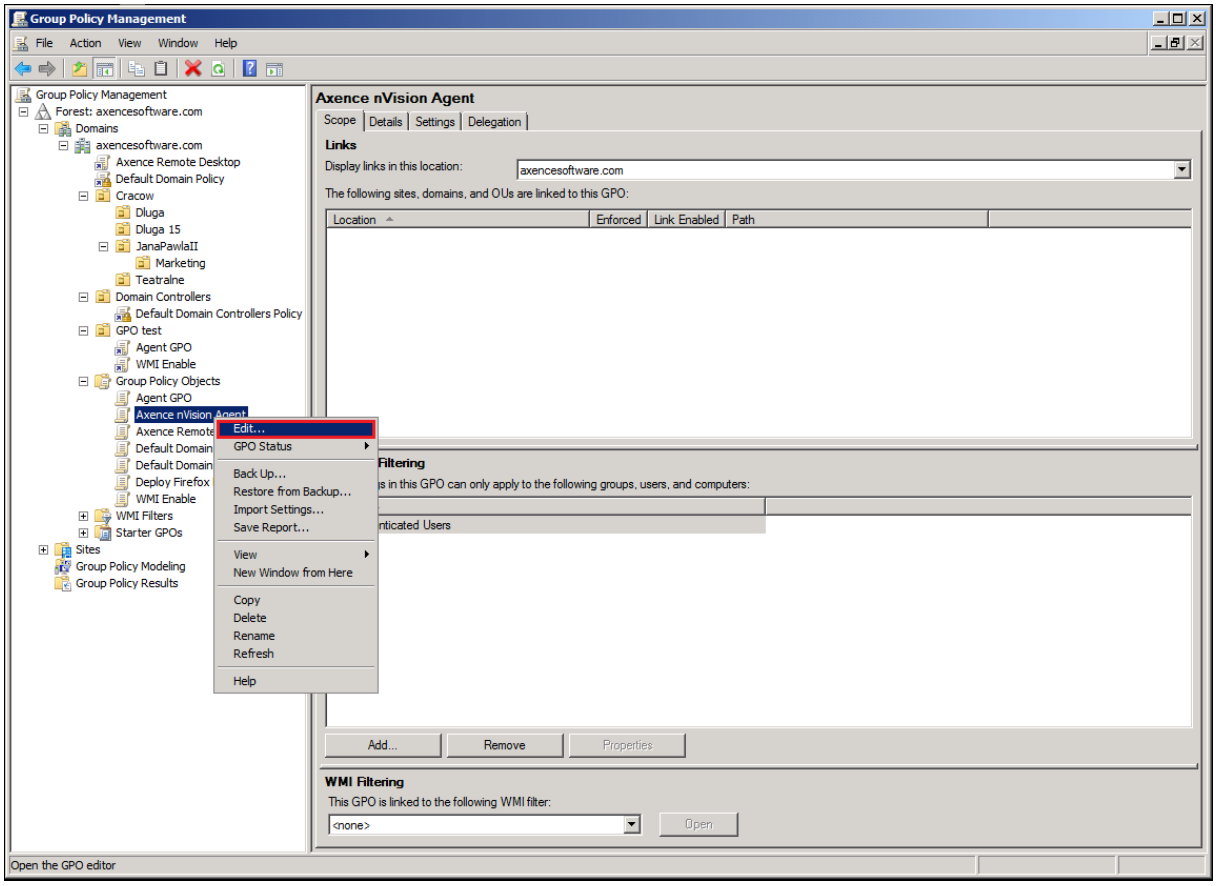
3. Utworzyć nowy obiekt zasad grupy: odnaleźć katalog **Group Policy Objects**, kliknąć na nim prawym przyciskiem myszy, z menu kontekstowego wybrać opcję **New**.



4. W oknie **New GPO** nadać nazwę tworzonemu obiektowi zasad grupy (Group Policy Object).
Na przykład: Axence nVision Agent.



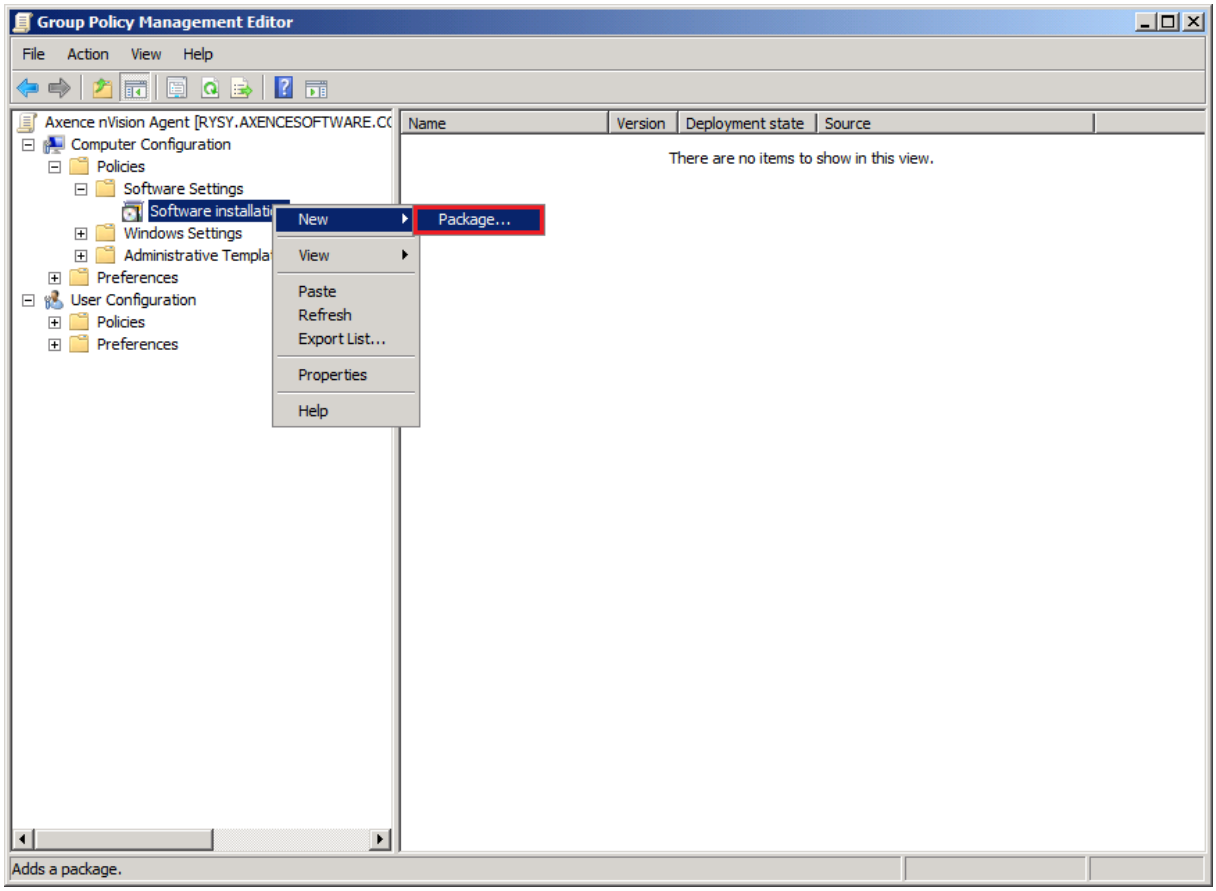
5. Przejść do edycji stworzonego GPO: kliknąć na tym obiekcie prawym przyciskiem myszy, z menu kontekstowego wybrać opcję **Edit**.



6. W oknie **Group Policy Management Editor** rozwinąć gałąź:

```
Computer Configuration \ Policies \ Software Settings \ Software installation
```

kliknąć na niej prawym przyciskiem myszy i z menu kontekstowego wybrać opcję **New > Package.**

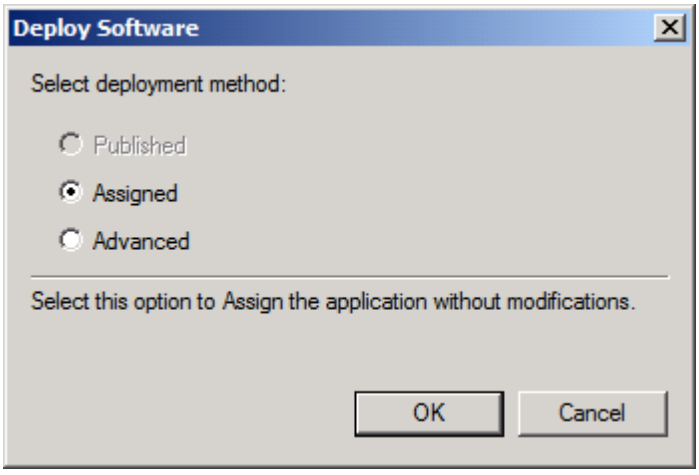


7. Wybrać plik paczki MSI z miejsca udostępnienia zasobu. Najlepiej wpisać adres współdzielonego zasobu

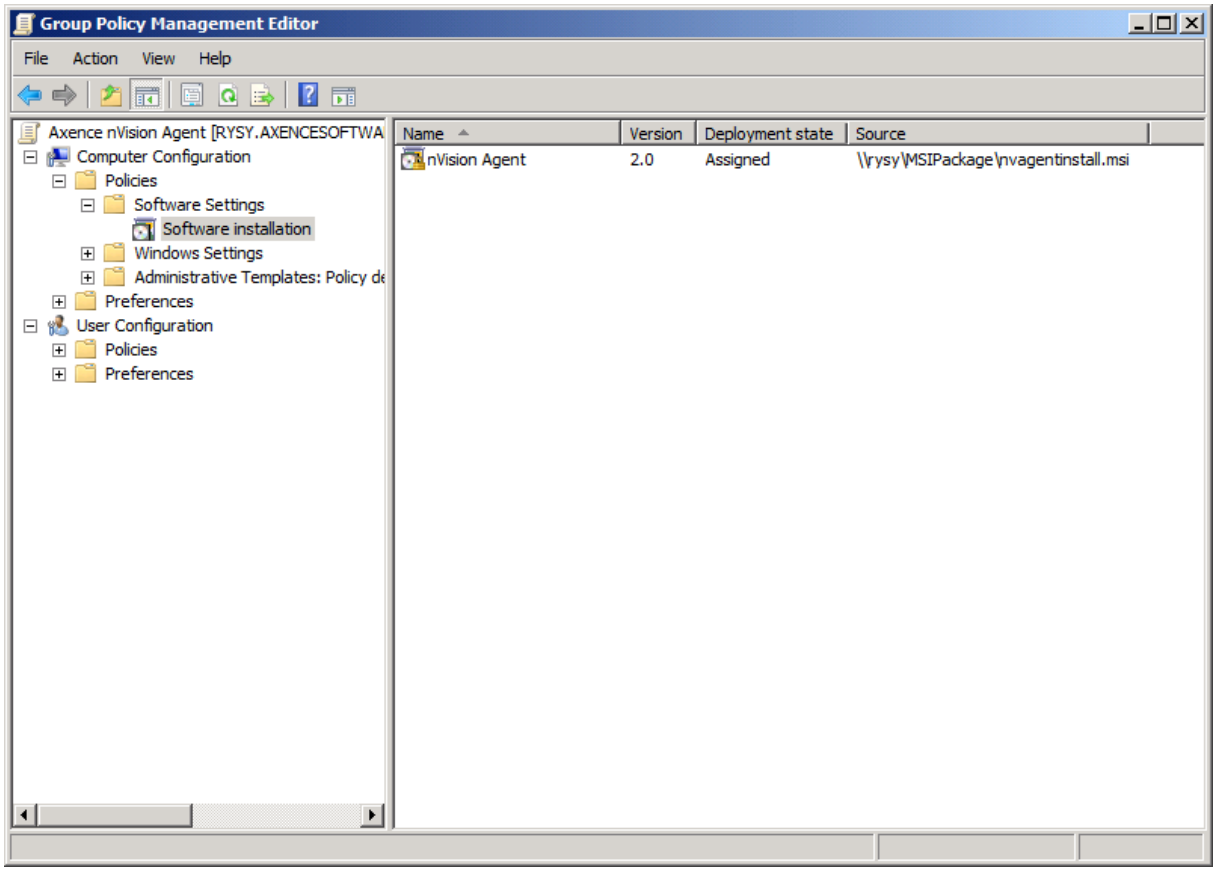
```
\\[NAZWA_SERWERA]\[NAZWA_KATALOGU]\
```

i wybrać plik paczki.

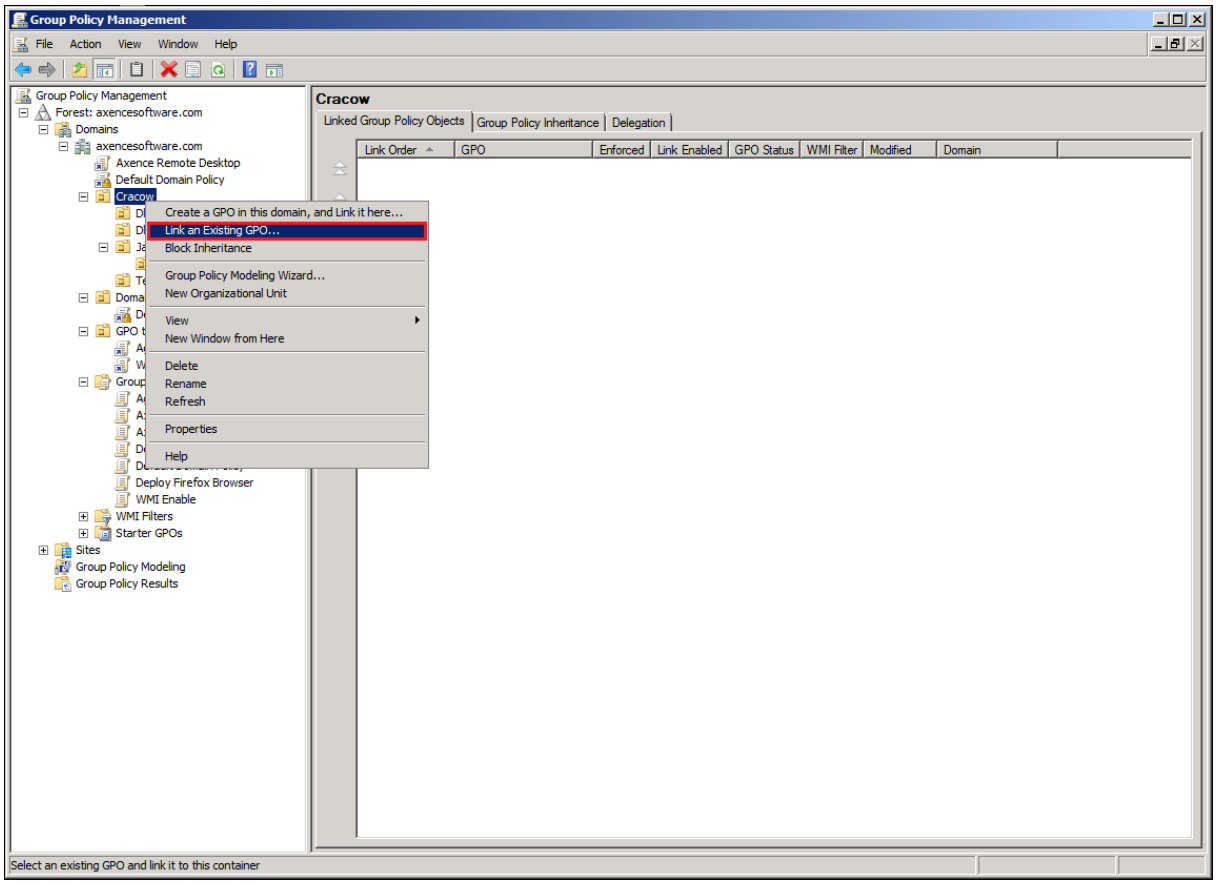
8. W oknie **Deploy Software** wybrać opcję **Assigned.**

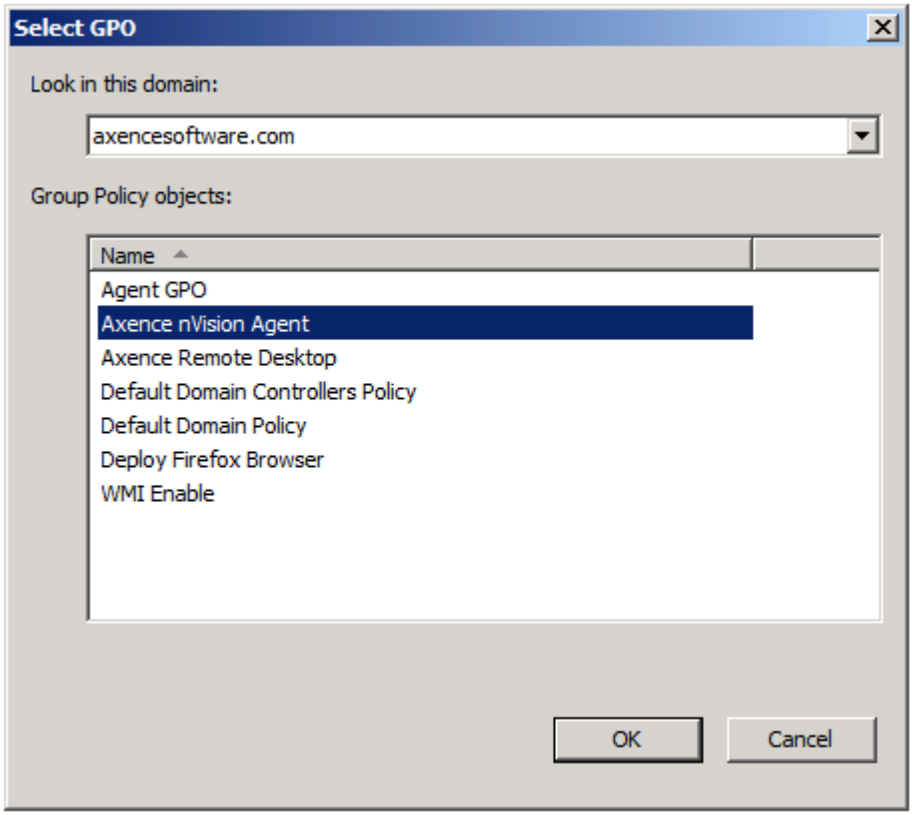


9. W oknie **Group Policy Management Editor** powinien pojawić się wpis **nVision Agent**.



10. Po utworzeniu GPO wrócić do okna **Group Policy Management** i wykonać podłączenie GPO do kontenera (**container**) grupy użytkowników lub komputerów: wybrać kontener, którego ma dotyczyć GPO, kliknąć na nim prawym przyciskiem myszy, wybrać z menu kontekstowego opcję **Link an Existing GPO**, następnie wybrać utworzone GPO.





11. Tak utworzony obiekt powinien być dystrybuowany na stacje robocze. Proces aktualizacji zasad grup może trwać nawet kilka godzin, jednak można go przyśpieszyć wykonując na stacjach roboczych polecenie

```
gpupdate /force /boot
```

które wymusi aktualizację zasad grup a w konsekwencji instalację paczki MSI Agenta nVision. W przypadku niepowodzenia informacji o problemach należy szukać w **Dzienniku zdarzeń systemu Windows (Event Log)** stacji roboczych oraz serwera.

Powiązane tematy

Instalacja przez Active Directory (GPO) z zastosowaniem instalatora MSI

14.8 Instalacja Agenta przez WMI

Aby zainstalować zdalnie Agenta nVision używając WMI należy na docelowym komputerze:

1. otworzyć linię poleceń z uprawnieniami administratora i uruchomić w niej program **WmiEnable.exe** (dostępny w katalogu instalacji nVision)
2. upewnić się, że w systemie Windows, jest włączone **"Udostępnianie plików i drukarek:"**
   - **Windows 7 i 8**: *Panel sterowania* \ *Centrum sieci i udostępniania* \ *Zaawansowane ustawienia udostępniania* (opcja po lewej stronie okna)
   - **Windows Vista**: *Panel sterowania* \ *Centrum sieci i udostępniania*
   - **Windows XP**: *Panel sterowania* \ *Zapora systemu Windows* \ *Wyjątki*
3. we właściwościach tego ikony komputera w nVision, upewnić się że test danych logowania Windows przechodzi poprawnie

14.9 Klonowanie obrazu dysku z zainstalowanym Agentem

Agent nVision podczas instalacji generuje i zapisuje w rejestrze swój unikalny identyfikator GUID. Jeżeli Agent podczas uruchomienia wykryje zmianę SID komputera na którym jest zainstalowany to generuje nowy GUID. Prawidłowa kolejność działań powinna obejmować przygotowanie systemu operacyjnego narzędziem SysPrep przed sklonowaniem obrazu dysku na inne komputery. Wówczas podczas uruchomienia każdego sklonowanego systemu zostaje wygenerowany dla niego nowy unikalny SID wskutek czego również Agenty z tych systemów zgłaszają się do nVision z różnymi (unikalnymi) GUID'ami tworząc odrębne ikony w nVision. W przeciwnym wypadku każdy z nich zgłasza się do nVision z takim samym GUID'em czyli kilku Agentów dosyła wówczas swoje dane pod tą samą ikonę w nVision.

Jeżeli już doszło do takiej sytuacji wówczas należy użyć narzędzia SysPrep do zresetowania SID na poszczególnych komputerach:

http://technet.microsoft.com/en-us/library/cc721973.

14.10 Konfiguracja oprogramowania antywirusowego

Celem prawidłowej pracy nVision, zgodnie z wymaganiami do programu, proszę w konfiguracji oprogramowania antywirusowego wykluczyć ze skanowania (operacje dyskowe oraz połączenia sieciowe) katalogi:

- C:\Program Files\Axence*.*
- C:\Program Files (x86)\Axence*.*

wraz z podkatalogami na:

- komputerze na którym jest zainstalowany Serwer nVision,
- komputerach gdzie zainstalowane są Konsole nVision,
- komputerach gdzie zainstalowane są Agenty nVision.

Następnie proszę zrestartować te komputery.

Przykłady:

http://kb.eset.com/esetkb/index?page=content&id=SOLN2153&viewlocale=pl_PL

http://support.kaspersky.com/pl/10017

http://www.avg.com/pl-pl/faq.num-5187

14.11 Konfiguracja połączenia agentów zainstalowanych na komputerach mobilnych

Aby skonfigurować Agenta zainstalowanego na komputerze mobilnym (pracującym poza siecią lokalną) należy:

1. Otworzyć port **4436** na ruterze/zaporze z adresem zewnętrznym dla połączeń przychodzących i przekierować ten ruch odpowiednio na port **4436** komputera w sieci lokalnej, na którym jest zainstalowany Serwer nVision.
2. Instalując Agenta nVision na komputerze mobilnym podać mu zewnętrzny **adres IP rutera**.

W przypadku potrzeby skonfigurowania połączenia mobilnych komputerów z Agentami, które już obecnie korzystają z lokalnego adresu IP komputera z nVision, można użyć opcji z karty **Narzędzia i opcje, Agenty \ Propaguj nowy adresu Atlasu** podając zewnętrzny adres IP rutera. Po rozpropagowaniu nowego adresu (dopisaniu go do listy Atlasów w konfiguracji Agentów nVision), Agenty nVision będą podejmować próby połączenia się na każdy z adresów które mają na swojej liście. Połączenie dojdzie do skutku tylko wówczas jeżeli GUID i hasło będzie takie samo w Agencie nVision jak i w Serwerze nVision. Atlas do którego Agent nie będzie mógł się połączyć przez 21 dni zostanie usunięty ze spisu Atlasów Agenta nVision (oczywiście gdy w spisie jest tylko jeden Atlas to nie zostanie on nigdy usunięty).

Powiązane tematy

Porty używane przez nVision

14.12 Maszyny wirtualne

Jeżeli użytkownik chce wykrywać maszyny wirtualne w sieci wówczas może stworzyć mapy inteligentne definiując filtry:

**Główny adres MAC \ zaczyna się na ** <tutaj wstawić trzy pierwsze oktety z poniższej listy>

Jeżeli natomiast użytkownik chce aby skaner/reskaner sieci nie wykrywał maszyn wirtualnych (np. ze względu na przekroczenie limitu ilości urządzeń zapisanego w licencji) może wówczas dodać do listy

ignorowanych adresów (we właściwościach Atlasu) trzy pierwsze oktety z poniższej listy zakańczając każdy z nich gwiazdką.

```
0003FF
```

Virtual PC

http://blogs.technet.com/b/medv/archive/2011/01/24/how-to-manage-vm-mac-addresses-with-the-globalimagedata-xml-file-in-med-v-v1.aspx

```
000569
```

VMware
http://technet.microsoft.com/en-us/library/jj590655.aspx

```
00155D
```

Hyper-V

http://technet.microsoft.com/en-us/library/jj590655.aspx

```
080027
```

VirtualBox

https://forums.virtualbox.org/viewtopic.php?f=1&t=26295

14.13 Monitorowanie wielu lokalizacji w nVision

Istnieje kilka sposobów monitorowania wielu lokalizacji w nVision:

1. jedna instalacja Serwera nVision i monitorowanie urządzeń w zdalnych lokalizacjach połączonych z centralą przez VPN
2. jedna instalacja Serwera nVision i monitorowanie urządzeń (w szczególności przesyłanie danych z Agentów nVision) przez Internet
3. niezależne instalacje Serwerów nVision w zdalnych lokalizacjach:
   - brak centralnej bazy danych (każdy Serwer nVision posiada niezależną bazę danych)
   - Agenty przyjmą zmiany w konfiguracji i nowe wersje tylko od jednego Serwera nVision (Master Atlas)
   - dostęp do Serwerów nVision przez Konsole nVision w LAN, przez RDP w WAN lub przez przeglądarkę internetową (nVision Web Access)

W zakładce **Użytkownicy** można utworzyć konta użytkowników i przypisać każdemu użytkownikowi jedną z trzech ról w nVision Web Access / HelpDesk:

1. **Administrator** (nVision Web Access: pełne uprawnienia; HelpDesk: pełne uprawnienia - w szczególności zdalny dostęp i możliwość włączenia / wyłączenia przypisywania zgłoszeń) + może logować się do Konsoli nVision

2. **Help-Desk** (nVision Web Access: możliwość zdefiniowania praw dostępu do konkretnych map sieci i oddziałów, jak również poziomu dostępu do danych: mapy, urządzenia; HelpDesk: możliwość włączenia / wyłączenia zdalnego dostępu, możliwość włączenia / wyłączenia przypisywania zgłoszeń)
3. **Użytkownik** (nVision Web Access: brak dostępu; HelpDesk: dostęp jedynie do własnych zgłoszeń)

14.14 Monitorowanie wydruków z drukarek sieciowych

Agent zainstalowany lokalnie zbiera informacje o wydrukach tylko dla drukarek zainstalowanych jako lokalne. Dla drukarek sieciowych dodanych jako sieciowe konieczna jest instalacja Agenta na systemie, na którym drukarka jest udostępniona. Jeżeli w innych celach Agent nie będzie tam wykorzystywany, można skonfigurować profil Agenta tak, aby zbierał tylko informacje o wydrukach.

14.15 Nie wszyscy użytkownicy zostali pobrani z Active Directory

Domyślna wartość parametru **MaxPageSize** (maksymalny rozmiar strony, który jest obsługiwany dla odpowiedzi protokołu LDAP) w systemie Windows wynosi 1000 rekordów. Jeżeli użytkowników i grup w Active Directory jest więcej, należy w konfiguracji protokołu LDAP zwiększyć wartość parametru **MaxPageSize.**

Szczegóły:

http://support.microsoft.com/kb/315071

14.16 Parametry skanera inwentaryzacji

Plik wykonywalny skanera można uruchomić z parametrami:

```
silent
```

program nie wyświetla okna informującego o swoim działaniu

```
directory
```

"ścieżka" - wynik działania programu zapisywany jest do określonej ścieżki

```
runonce
```

jeśli program wykryje obecność plików z wynikiem poprzedniego skanowania to natychmiast zakończy pracę

Przykład użycia:

```
nVision_InventoryScanner.exe -silent -runonce -directory "c:\"
```

14.17 Porty używane przez nVision

Następujące porty powinny zostać otwarte dla połączeń przychodzących na komputerach gdzie zainstalowane są:

Serwer nVision:

- 4434 informacje diagnostyczne
- 4436 stałe połączenie (socket) Agenta
- 8080 Web Access
- 8081 serwer API
- 162 SNMP trap

Agent nVision:

- 4433 informacje diagnostyczne

Komputer, z którego informacje z liczników / usług / dziennika zdarzeń Windows będą pobierane przez WMI:

- 135, 139, 445, 593 WMI

Zapora systemu Windows jest konfigurowana automatycznie podczas instalacji Serwera nVision i Agenta nVision.

Zapory innych producentów należy skonfigurować we własnym zakresie - przykłady:

http://www.eset.pl/Pomoc,f,2917,act,show

http://support.kaspersky.com/pl/8743

https://www.avg.pl/faq/question/faq.num-5205

Powiązane tematy

Monitorowanie usług Windows

14.18 Przeniesienie nVision na inny komputer

Aby przenieść nVision na inny komputer należy wykonać następujące kroki:

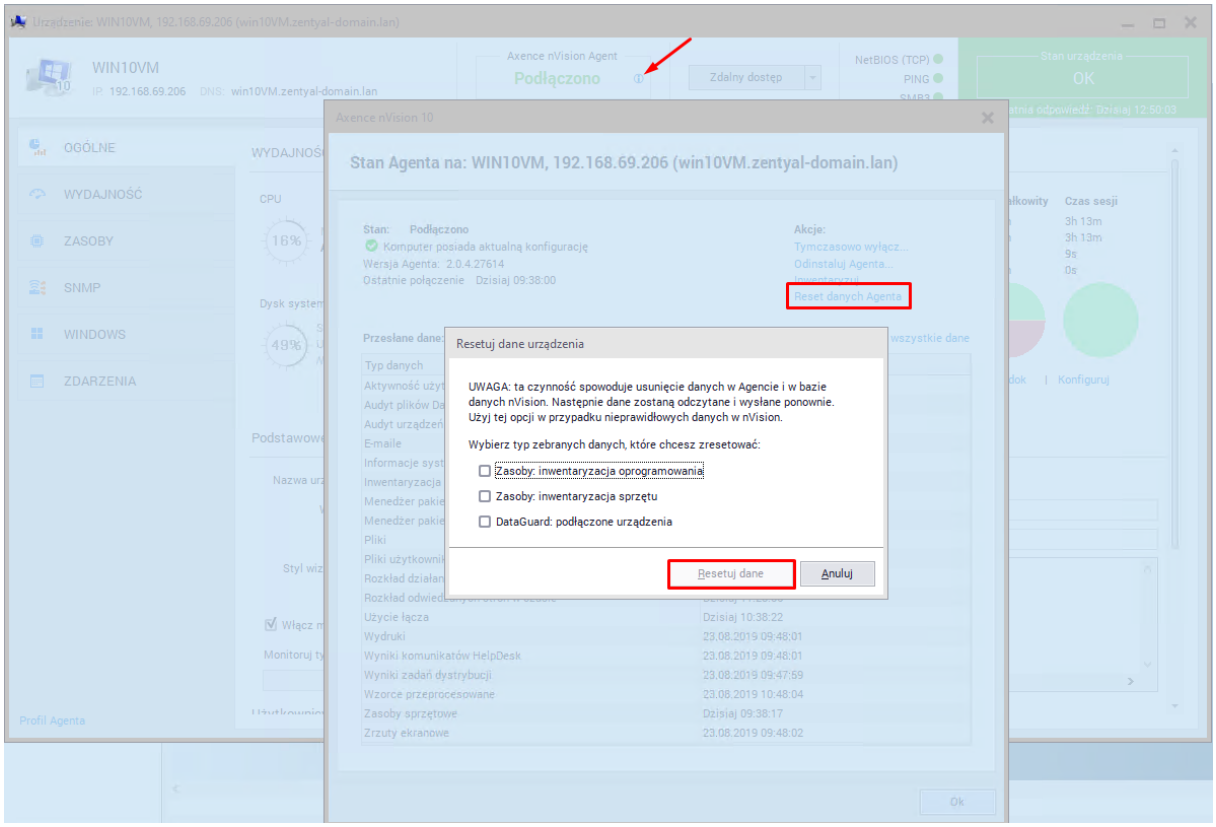
1. Przy użyciu opcji w karcie **Narzędzia i opcje -> Agenty | Propaguj nowy adresu Atlasu** rozpropagować Agentom nowy adres IP Atlasu.
2. W widoku **"Agenty"** w kolumnie **"Ostatni czas połączenia"** upewnić się że wszystkie Agenty otrzymały nowy adres Atlasu (czas połączenia Agenta późniejszy niż moment wykonania propagacji nowego adresu Atlasu).
3. Skopiować instalator **"nVisionSetup.exe"** z katalogu **"<nVision>\Sources"** (będzie potrzebny w dalszej części procedury przeniesienia nVision).
4. Sprawdzić i zanotować rozmiar katalogu "<nVision>\Database" po czym upewnić się że ilość wolnego miejsca na dysku docelowym jest dwukrotnie większa niż ten rozmiar.

5. Wykonać pełną kopię zapasową Atlasu przy pomocy narzędzia **DBBackup**, który znajduje się w katalogu **"<nVision>\Backups".**
6. Odinstalować nVision.
7. Na nowym komputerze zainstalować nVision (z pliku skopiowanego w punkcie 3).
8. Skopiować na nowy komputer pełną kopię zapasową Atlasu wykonaną w punkcie 5).
9. Przywrócić pełną kopię zapasową Atlasu przy pomocy narzędzia **DBRestore.**
10. Uruchomić nVision.

14.19 Resetowanie danych Agenta

W celu rozwiązania problemów z brakiem dosłania niektórych danych z Agenta do nVision (np. "dziury" w monitorowaniu aktywności Użytkownika lub nieaktualne dane inwentaryzacji) konieczne może być zresetowanie danych Agenta.

Operacja ta spowoduje dosłanie brakujących danych pod warunkiem, że znajdują się one w bazie Agenta.



W tym celu należy w oknie **Informacji o Urządzeniu**:

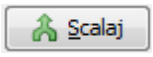
1. Kliknąć na ikonę "i" w górnej części okna informacji o urządzeniu.
2. Z sekcji **"Akcje"** wybrać **"Reset danych agenta".**
3. W oknie **"Reset danych agenta". Z**aznaczyć pola przy wybranych typach danych, które mają zostać zresetowane.Kliknąć przycisk **"Resetuj dane."**

Uwaga: Zaznaczenie opcji **"Wymuś na Agencie reset danych urządzenia i ponowne ich**

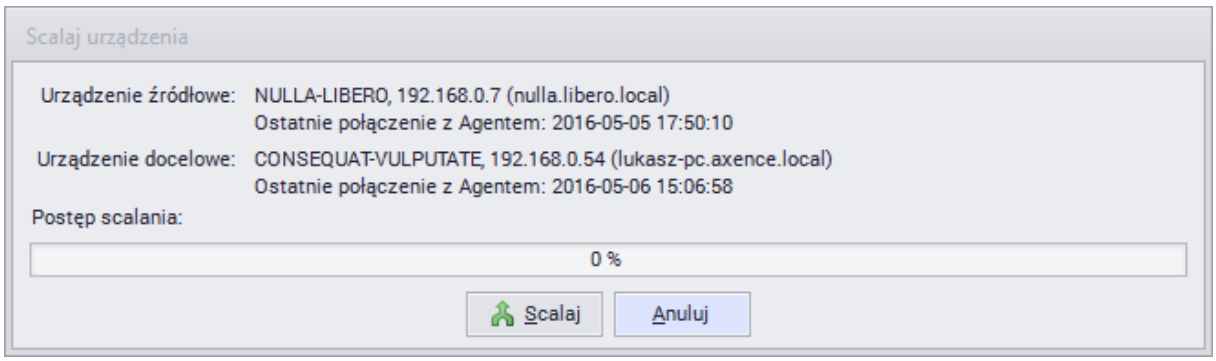
zebranie" spowoduje usunięcie zebranych przez Agenta danych z jego bazy oraz z bazy nVision i rozpoczęcie ponownego ich zbierania począwszy od czasu resetu. Opcji tej można używać w przypadku resetowania danych inwentaryzacji sprzętu i oprogramowania.

14.20 Scalanie urządzeń

Aby scalić urządzenia:

1. Zaznacz urządzenia, które chcesz scalić (np. w widoku mapy przytrzymując Ctrl).
2. Kliknij prawym przyciskiem myszy i wybierz opcję **Agent | Scalaj urządzenia**. Zostanie otwarte okno **Scalania urządzenia**.
3. Aby rozpocząć proces scalania, kliknij w przycisk 

. Stare urządzenie zostanie usunięte z mapy.



Jeżeli chcesz znaleźć duplikaty adresów IP i nazw DNS, skorzystaj z opcji **Narzędzia i opcje / Pokaż duplikaty urzadzeń.**

14.21 Uruchomienie SNMP w systemie Linux

Uruchomienie SNMP w systemie Linux, na przykładzie dystrybucji openSUSE:

1. zainstalować pakiety **"net-snmp"** (wraz z pakietami zależnymi)
2. otworzyć w zaporze sieciowej porty **161 TCP i 161 UDP**
3. uruchomić linię poleceń, wpisać

```
su -
```

po czym wpisać hasło użytkownika root

4. uruchomić z linii poleceń **"gedit"** i wyedytować plik **"/etc/snmp/snmpd.conf"**
5. chcąc uzyskać dostęp do odczytu do całego drzewa SNMP należy wpisać:

```
view systemonly included .1
rocommunity public default
```

po czym zapisać tak zmodyfikowany plik

6. chcąc aby usługa SNMP uruchamiała się podczas każdego startu systemu należy w linii poleceń wpisać

```
chkconfig snmpd on
```

7. uruchomić usługę SNMP wpisując w linii poleceń

```
service snmpd start
```

Po wykonaniu powyższego, w nVision, we właściwościach tego urządzenia, w zakładce **"Dane logowania"** należy zaznaczyć pole **"Urządzenie zarządzalne"** i kliknąć przycisk **"Ok"**. Wówczas po otwarciu okna informacji o urządzeniu będzie można przeglądać zawartość drzewa liczników w zakładce **"SNMP"**.

Szczególnie interesujące informacje o systemie mozna znaleźć w gałęzi:

```
.iso.org.dod.internet.mgmt.mib-2.host
```

```
OID: .1.3.6.1.2.1.25
```

Indeks

- A -

- B -

- D -

- F -

- H -

- I -

- K -

- L -

- M -

- N -

- O -

- P -

- R -

- S -

- U -

- W -

- Z -