NETASQ

NETASQ

Netasq Event Analyzer – quick guide

Kontakt:

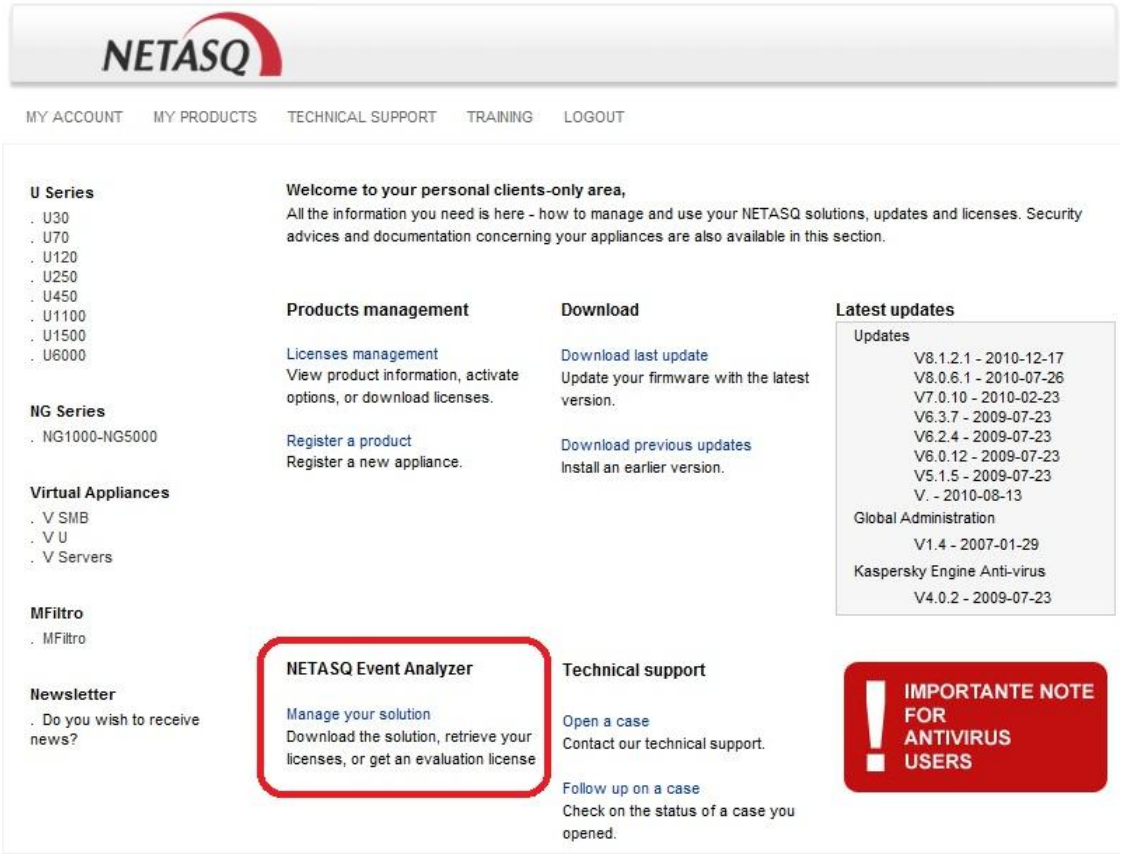
Dagma Sp. z o.o., www.netasq.pl

032 259 11 38 netasq@dagma.pl

SPIS TREŚCI

1. Wprowadzenie

Aplikacja **Netasq Event Analyzer** jest dostępna do pobrania na stronie www.netasq.com w sekcji **Secure Area** po zalogowaniu się na własne konto. Dane dostępowe powinny zostać podane w chwili zakupu urządzenia Netasq.



Licencja podstawowa uprawnia do generowania raportów dla urządzeń:

F200, F500, F800, F1200, F2500, F5500
U120, U250, U450, U1100, U1500, U6000
NG1000, NG5000
VS5, VS10, V50, V100, V200, V500, VU.

Przy założeniu że liczba logowanych zdarzeń nie przekracza 200.000 zdarzeń na 24h i raport jest generowany dla 1 urządzenia.

W celu generowania raportów dla urządzeń:
F25, F50, F60
U30, U70
z poziomu aplikacji Netasq Event Analyzer należy zakupić dodatkową licencję.

Jeżeli istnieje potrzeba logowania większej liczby zdarzeń niż 200.000 na 24h , lub generowania raportów z większej liczby urządzeń niż 1 proszę o kontakt na adres pomoc@netasq.pl w celu dokonania zakupienia właściwej licencji (rozszerzenia licencji).

2. Wymagania systemowe

2.1 System operacyjny

Aplikację Netasq Event Analyzer można zainstalować na poniższych systemach operacyjnych

a) Windows 2003 sp2 (lub wyższy) wersja 32 bity
b) Windows 2008 sp2 (lub wyższy) wersja 32 i 64 bity

Podczas instalacji zostaną sprawdzone czy poniższe komponenty są zainstalowane w systemie. Jeżeli nie zostaną one doinstalowane w trakcie instalacji:

Microsoft Web Components 11 (versja12)
SQL Server Native Client 2005
SQL Server 2005 SP3 lub wyższy (Express, Standard oraz Enterprise Editions)
Microsoft .NET Framework 3.5 SP1

Uwaga !!!

Jeżeli jest zainstalowany w systemie IIS (Internet Information Services) po zainstalowaniu Microsoft .NET Framework 3.5 nie zapomnij włączyć ponownie IIS zgodnie z poniższą instrukcją:
- uruchom w Menu Start -> Wszystkie programy -> Akcesoria -> Wiersz poleceń
- przejdź do lokalizacji gdzie jest zainstalowany Microsoft Framework
C:\Windows\Microsoft.NET\Framework\v2.0.50727 (ścieżka domyślna)
- uruchom polecenie: aspnet_regiis –i

2.2 Wymagania sprzętowe

- logowanie poniżej 5.000.000 zdarzeń

  Procesor: Xeon dual processor
  Pamięć RAM: 3 GB
  Wolne miejsce na dysku: 160 GB
  Dysk: SCSI – RAID5 – 10 KTPM

- logowanie od 5.000.000 do 10.000.000 zdarzeń

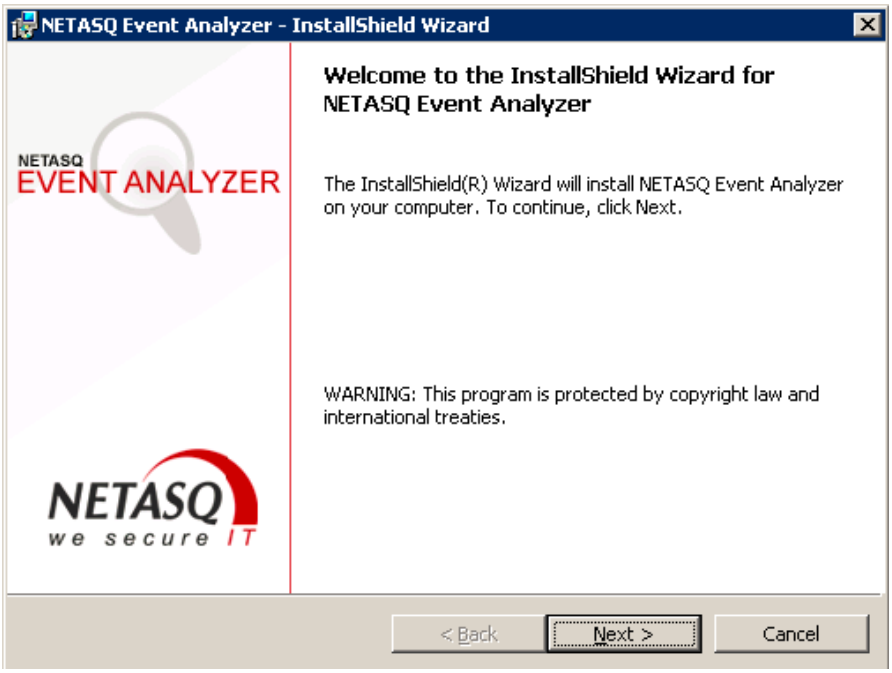
  Procesor: dual core bi-processor
  Pamięć RAM: 4 GB
  Wolne miejsce na dysku: 300 GB
  Dysk: SCSI – RAID5 – 15 KTPM

- logowanie od 10.000.000 do 36.000.000 zdarzeń

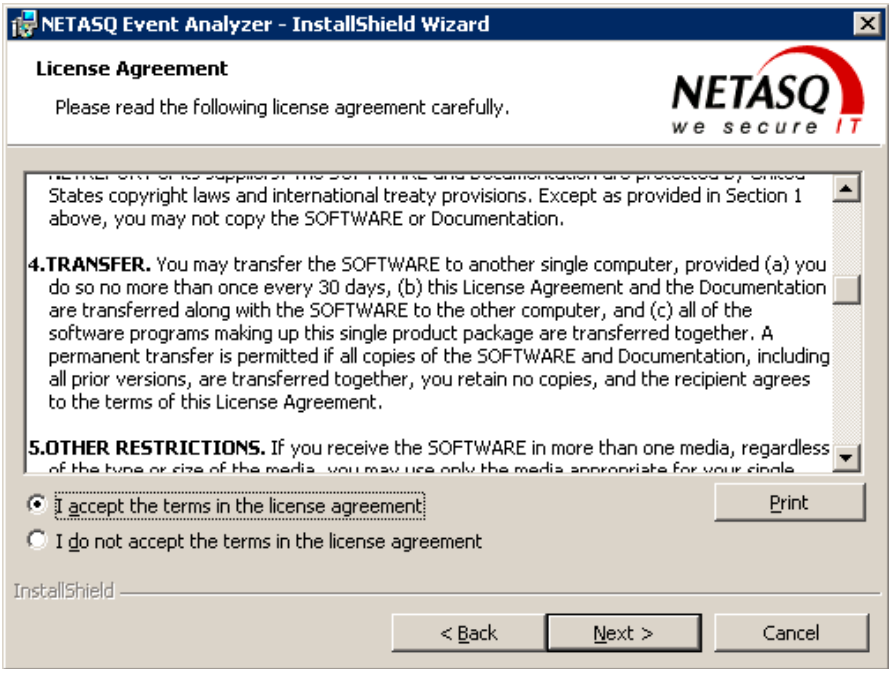
  Procesor: quad core bi-processor
  Pamięć RAM: 6 GB
  Wolne miejsce na dysku: 600 GB
  Dysk: SCSI – RAID5 – 15 KTPM

3. Instalacja

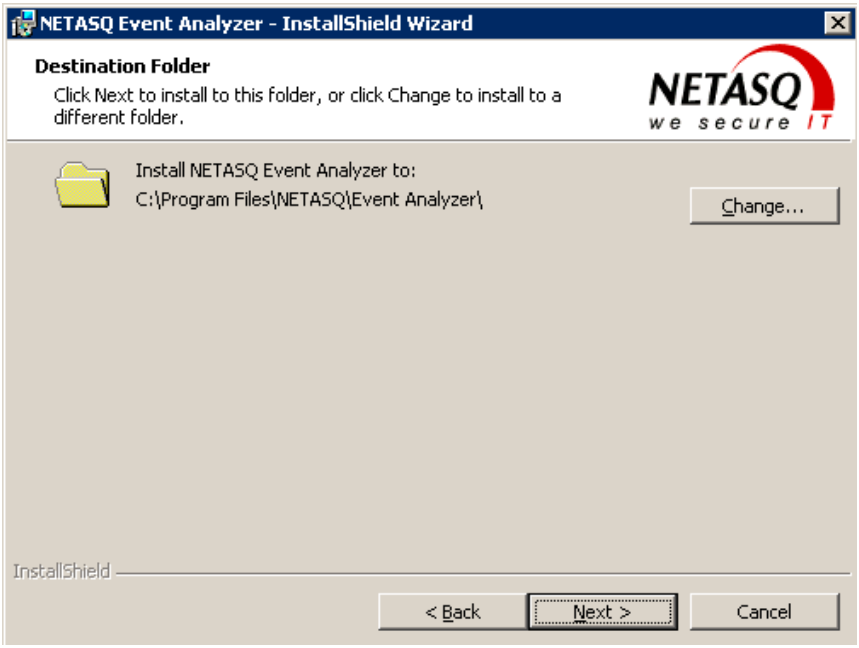
1. Uruchom ręcznie instalację klikając dwukrotnie w plik setup.exe



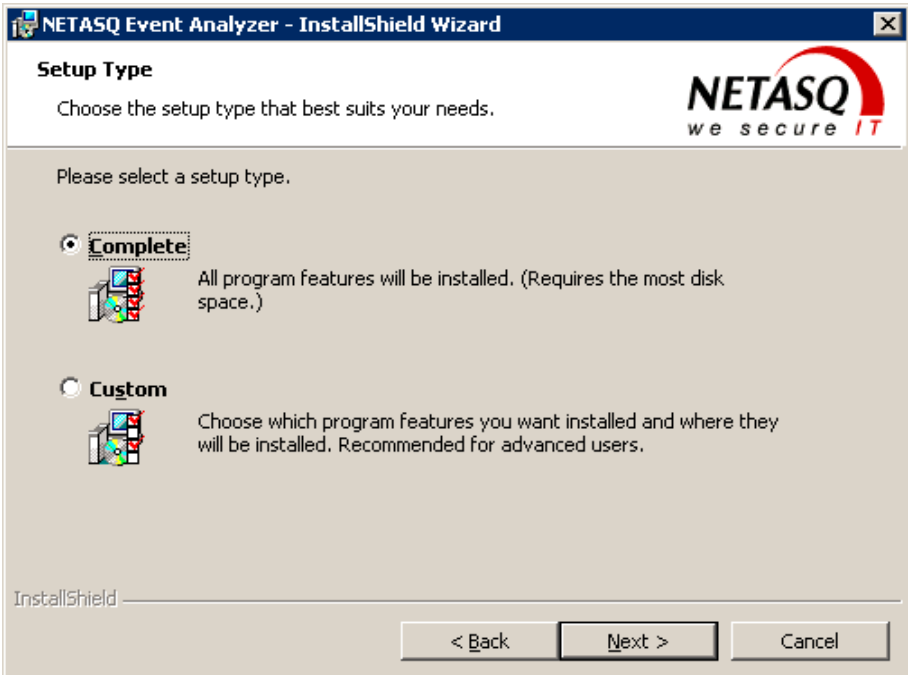
2. Wybierz **Next**



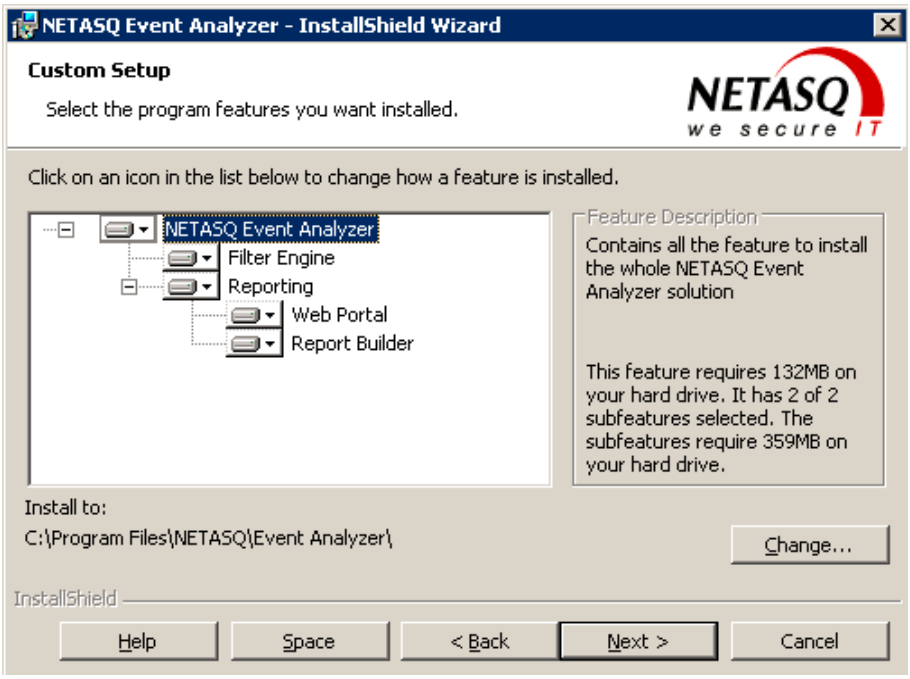
3. Potwierdź warunki licencji zaznaczając „**I accept the terms in the license agrement”** i naciśnij **Next**



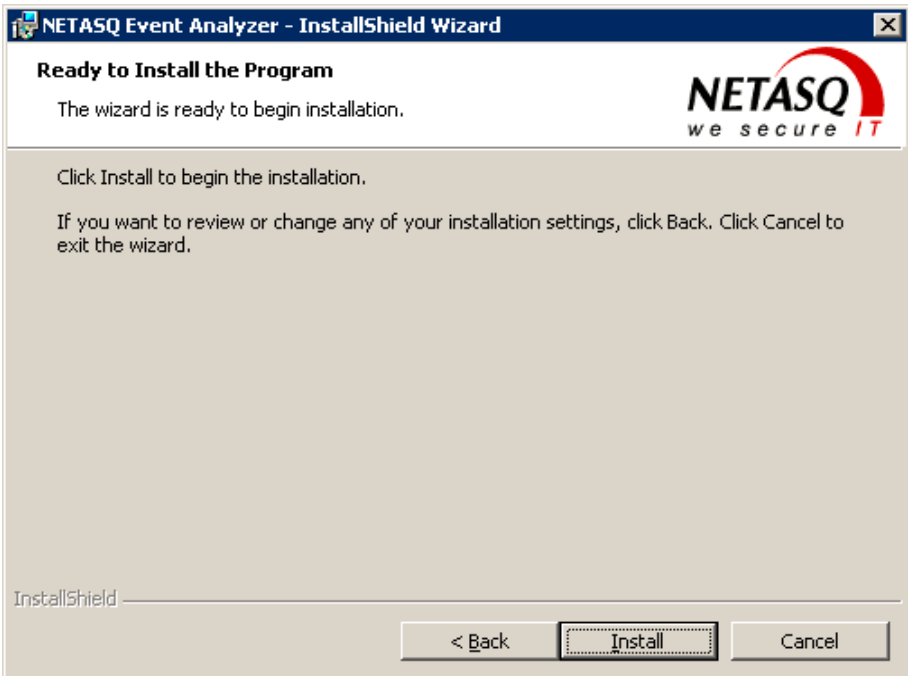
4. Wybierz lokalizację gdzie aplikacja Netasq Event Analyzer ma zostać zainstalowana i naciśnij **Next**



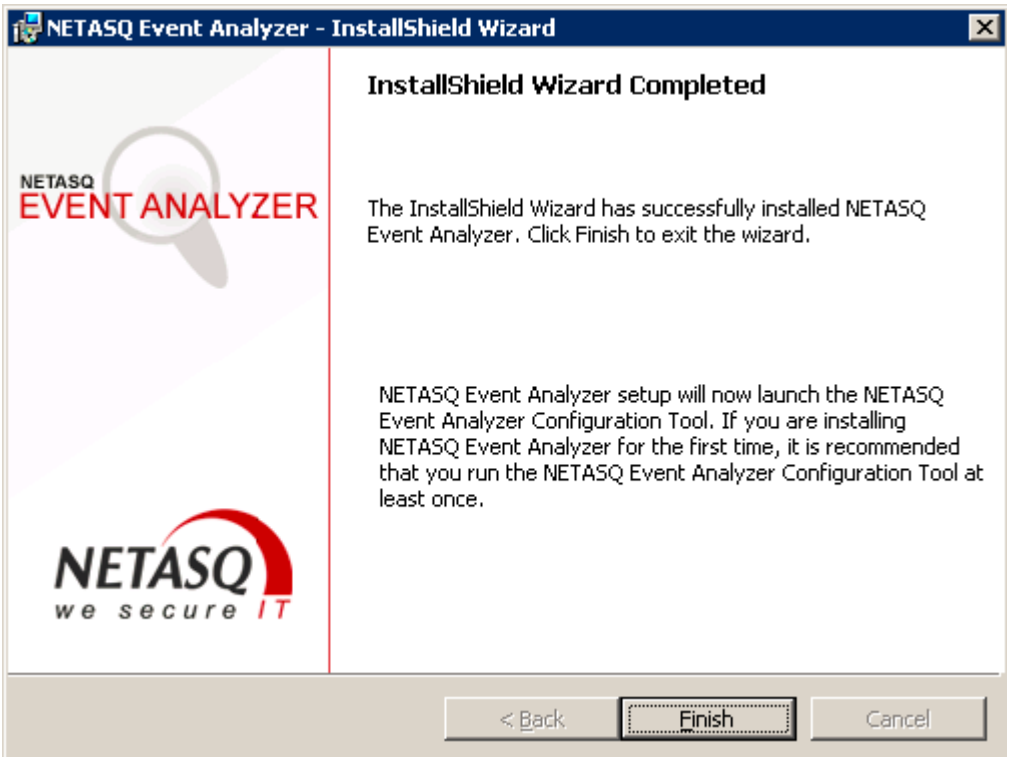
5. Wybierz sposób instalacji i naciśnij **Next**



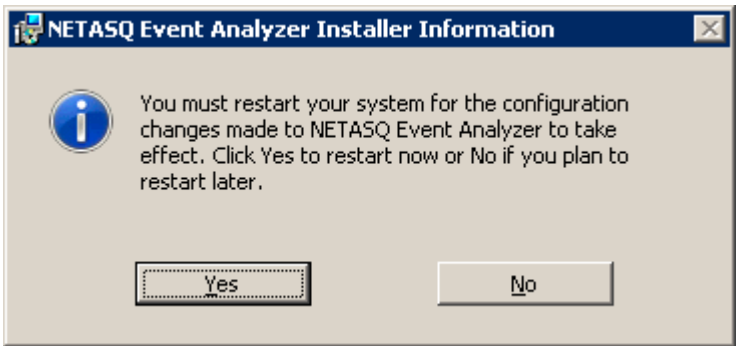
6. Wybierz komponenty jakie mają zostać zainstalowane i naciśnij **Next**



7. Wybierz **Install** aby zainstalować.



8. Powyższy krok świadczy o zakończeniu instalacji.



9. Naciśnij **Yes** aby ponownie uruchomić komputer.

4. Podstawowa konfiguracja

Kreator konfiguracji przeprowadzi Cie przez kolejne kroki:

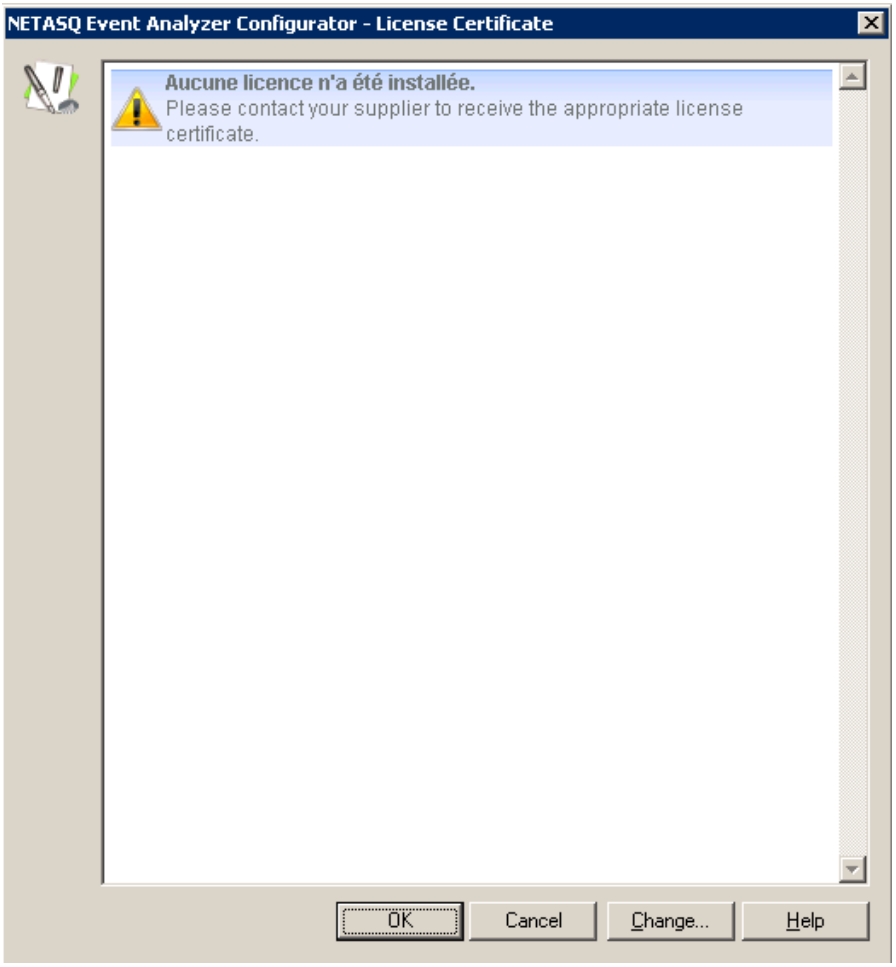
- wybór źródła logów
- konfiguracja podsieci
- konfiguracja bazy (lokalizacja)
- konfiguracja harmonogramu
- konfiguracja smtp do wysyłania raportów
- archiwizacja logów
- zaczytanie licencji

Kreator konfiguracji zostanie uruchomiony automatycznie po ponownym uruchomieniu komputera. Jeżeli kreator został przerwany można go uruchomić wchodząc w lokalizację

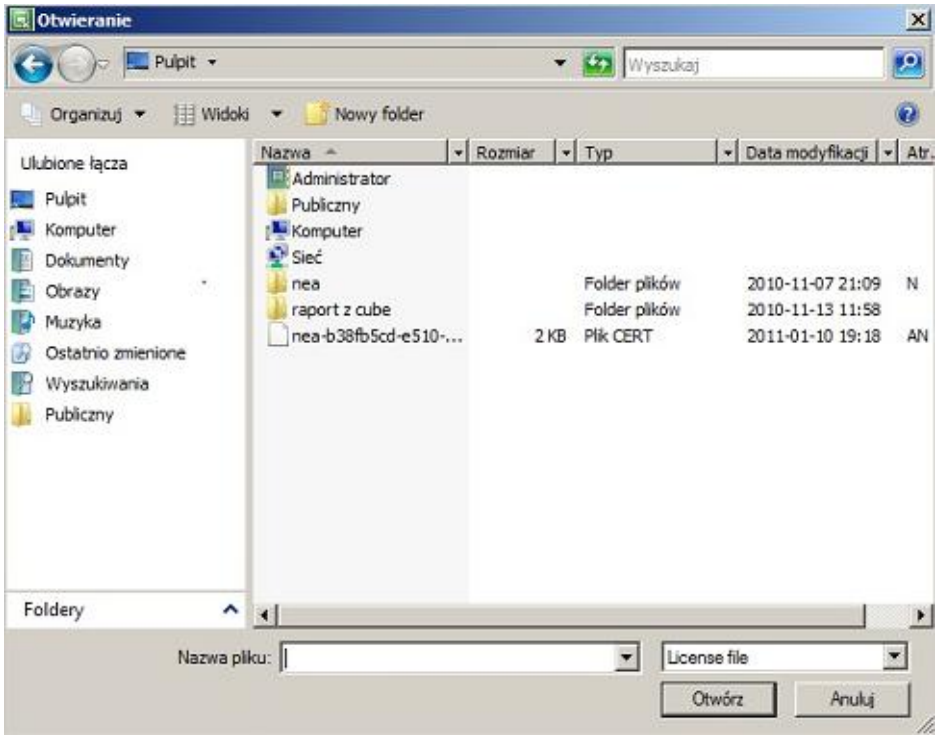
Menu Start -> Wszystkie programy -> NETASQ -> NETASQ Event Analyzer -> Configurator

4.1 Konfiguracja License Certificate

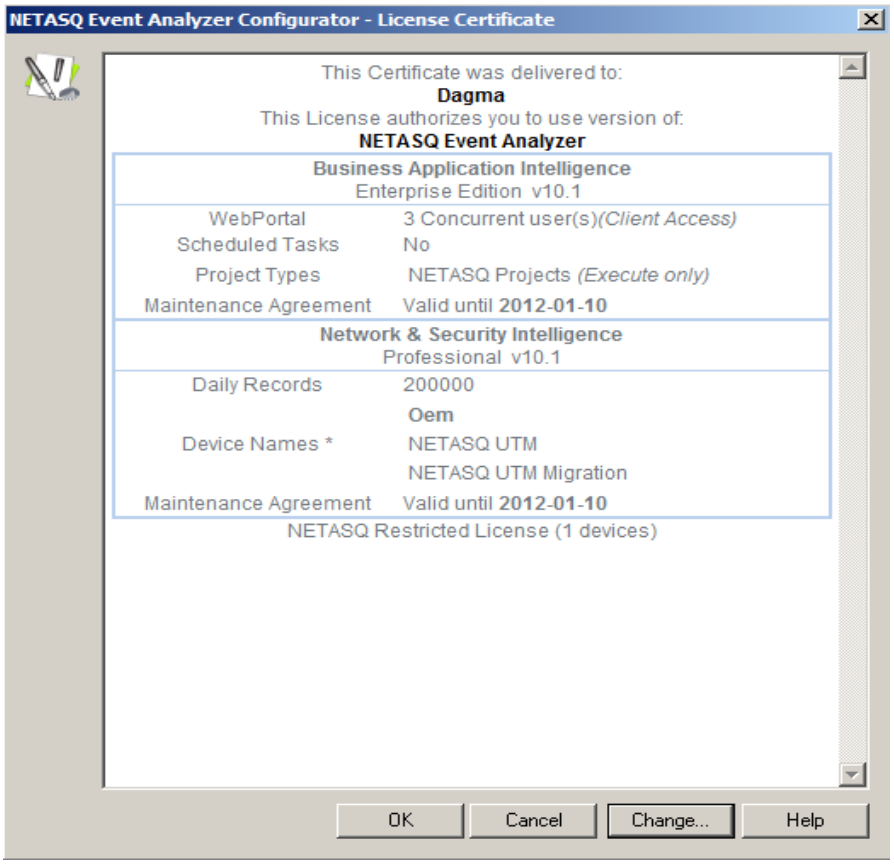
W chwili pierwszego uruchomienia należy w oknie



wybrać **Change** w celu zaczytania licencji



Wybierz swój plik licencyjny



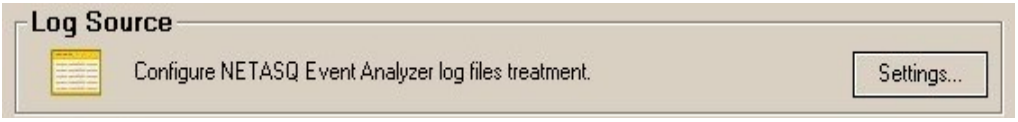
Po zaczytaniu licencji zostanie wyświetlona informacja na jaką firmę została wygenerowana, oraz do kiedy jest ważna.

Uwaga !!!

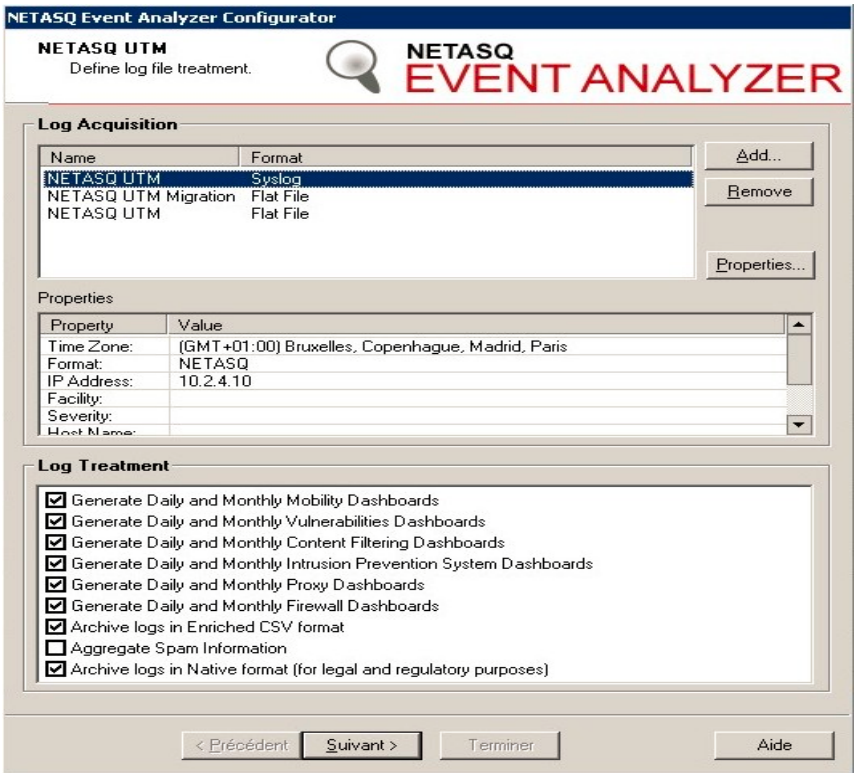
W chwili wygaśnięcia licencji aplikacja Netasq Event Analyzer przestanie działać. Logi przestaną być zaczytywane do bazy a także nie będą generowane raporty zgodnie z harmonogramem. Dodatkowo jeżeli w ramach aplikacji Netasq Event Analyzer była uruchomiona usługa Syslog zostanie ona także zatrzymana.

4.2 Konfiguracja Log Source

Log Source pozwala administratorowi podać z jakiego źródła mają zostać zaczytane logi

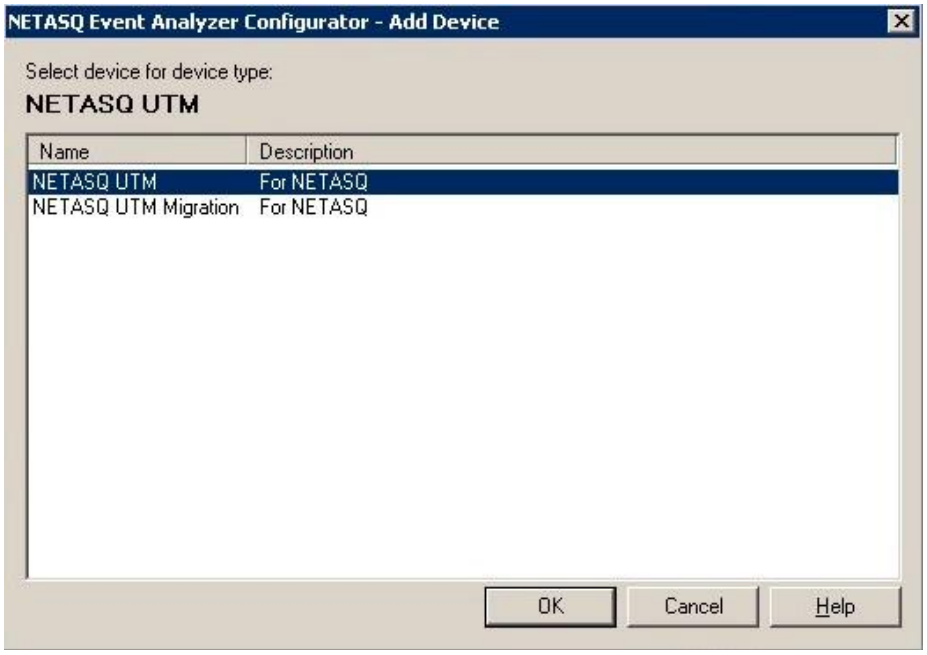


Ekran konfiguracyjny:

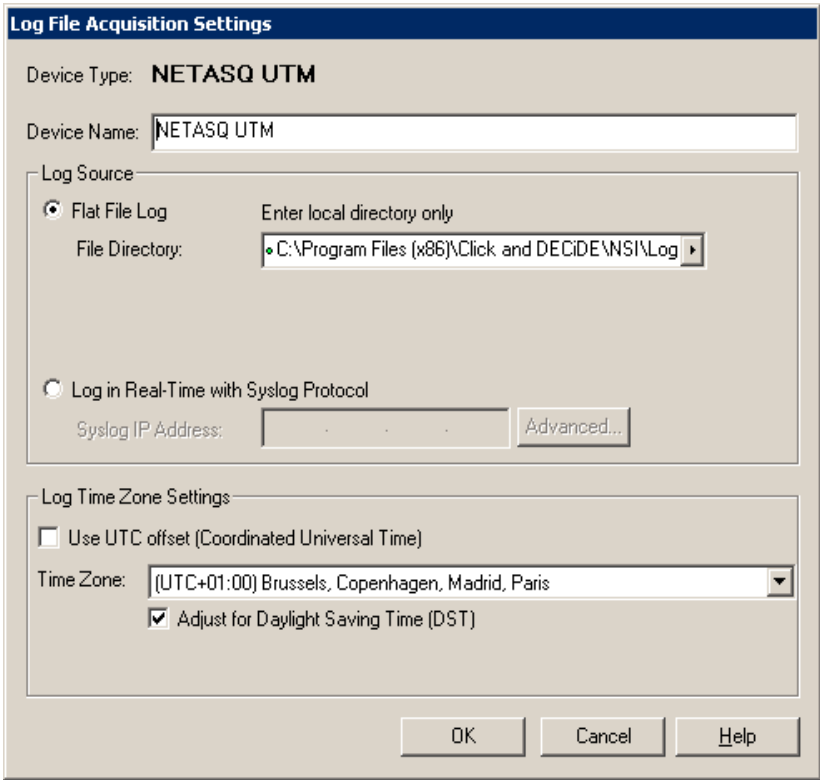


Logi mogą zostać zaczytane w następujące sposoby:

- Netasq UTM (syslog) – logi będą przesyłane przy pomocy sysloga
- Netasq UTM – logi zostaną zaczytane z plików *.txt przesłanych uprzednio z urządzenia
- Netasq UTM Migration – zaczytanie logów wyeksportowanych bezpośrednio z urządzenia



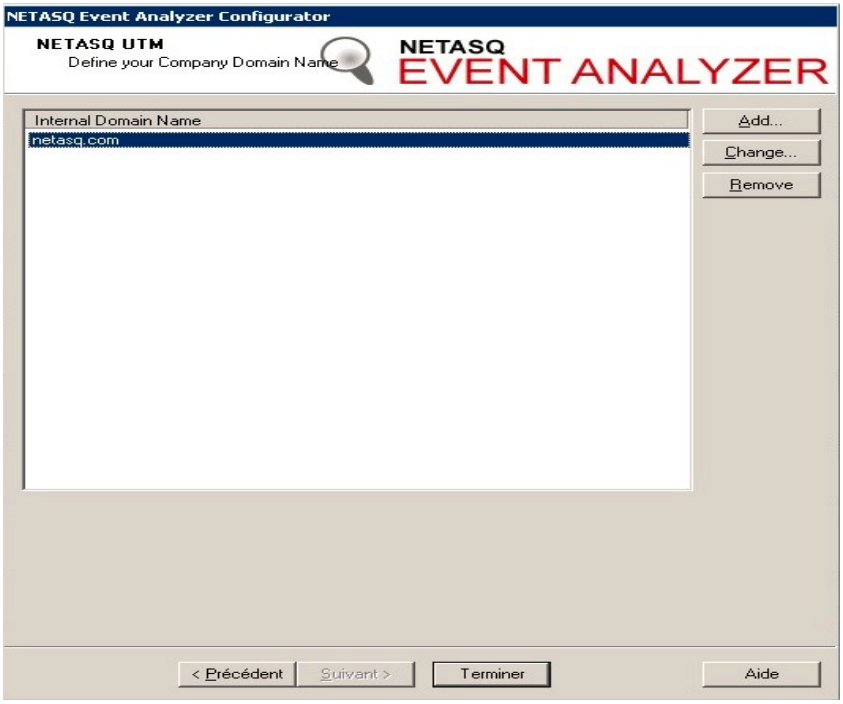
Należy wybrać sposób zaczytania logów. Wybranie opcji Netasq UTM pozwoli na zaczytanie logów bezpośrednio z fizycznego urządzenia.



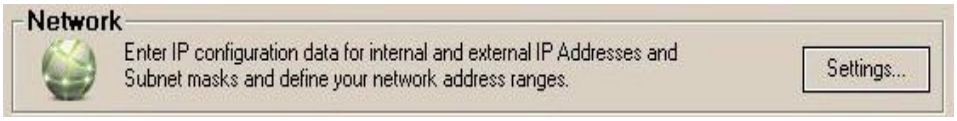
Flat File Log – zaczytanie logów bezpośrednio z katalogu w którym się znajdują

Log In Real-Time with Syslog Protocol – uruchomienie usługi Syslog pozwoli na zaczytywanie logów w czasie rzeczywistym z urządzenia Netasq

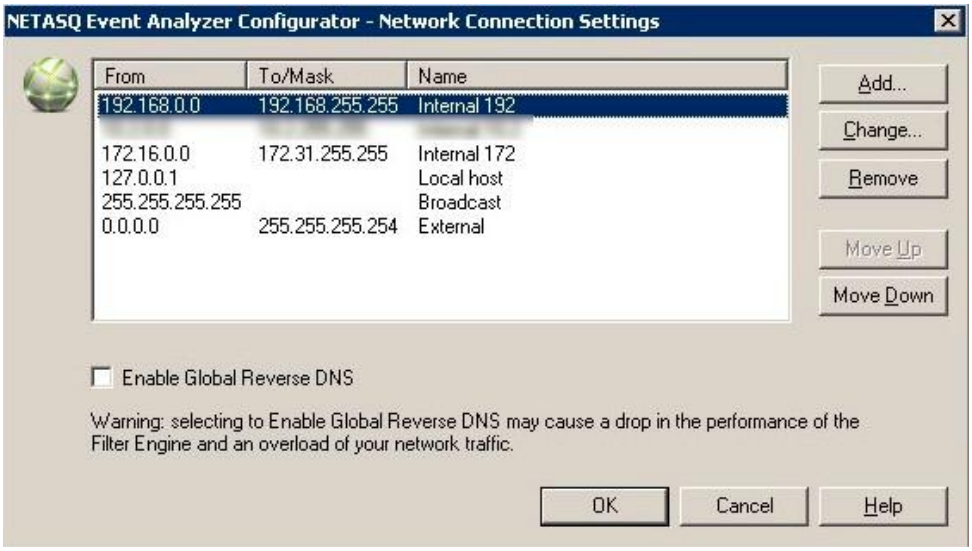
Pozostaje jeszcze skonfigurowanie własnych domen. Netasq Event Analyzer będzie używał tej konfiguracji do rozpoznania maili przychodzących i wychodzących z własnych domen.



4.3 Konfiguracja Network Configuration



Konfiguracja ta pozwoli administratorowi na zdefiniowanie wszystkich podsieci, oraz odpowiedniego ich nazwania. Adresacja ta będzie używana w generowanych raportach.



Gdzie:

Add – możliwość dodania kolejnych podsieci

Change – zmiana już istniejących wpisów

Remove – usunięcie zdefiniowanych wpisów

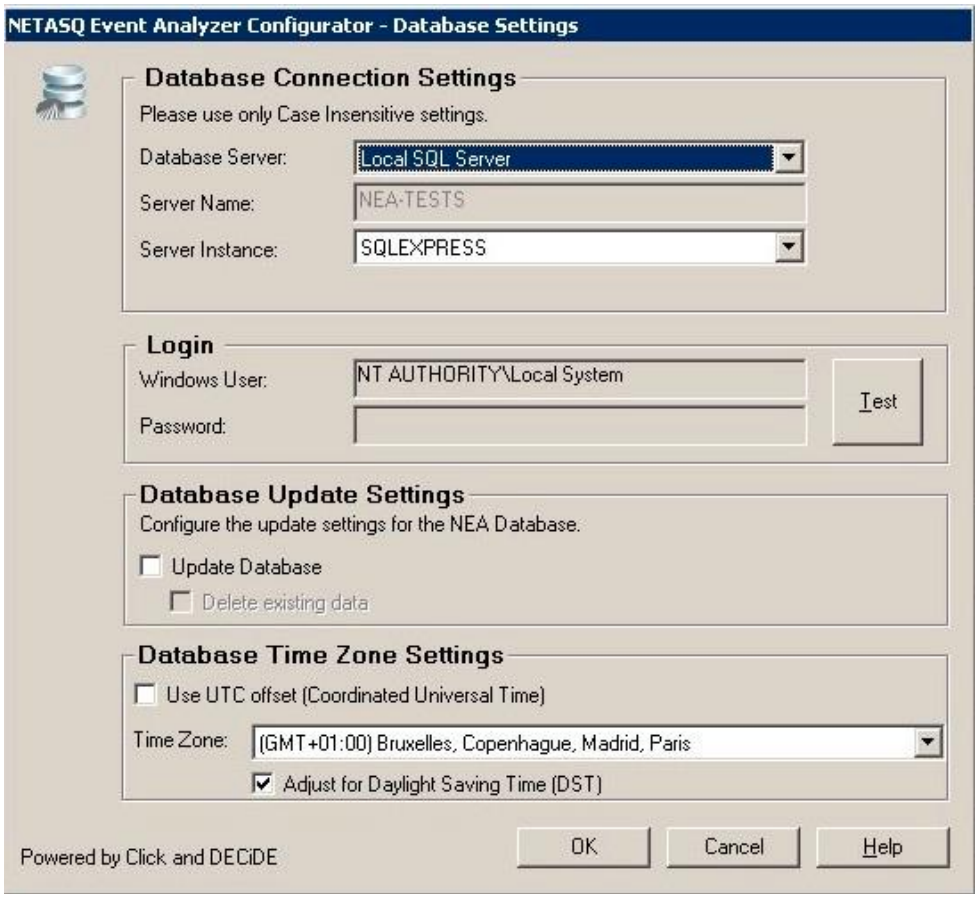
Internal – adresacja występująca wewnątrz sieci

External – adresacja poza siecią

Dmz – adresacja w strefie zdemilitaryzowanej

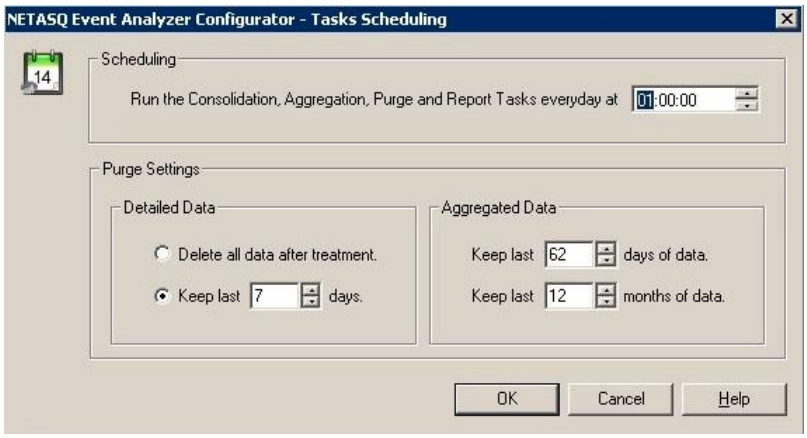
Brodcast – adresacja rozgłoszeniowa

4.4 Konfiguracja Database



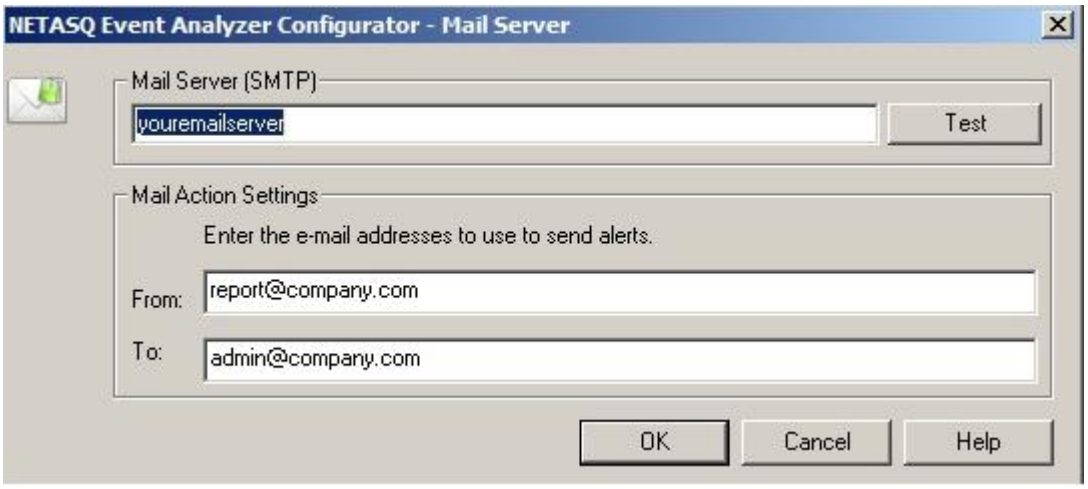
Sekcja Database Connection Settings pozwali administratorowi na podpięcia aplikacji Netasq Event Analyzer do już istniejącej bazy, lub jeżeli taka nie jest zainstalowana zostanie doinstalowany na tym komputerze SQL Express.

4.5 Konfiguracja Scheduled Task



Istnieje możliwość zdefiniowania o której godzinie mają zostać wygenerowane raporty. Przy standardowej licencji raport będą zawsze generowane o 1.00, gdyż licencja ta nie pozwala na modyfikację harmonogramu. Funkcjonalność ta jest dostępna dla płatnej licencji

4.6 Konfiguracja Mail Server

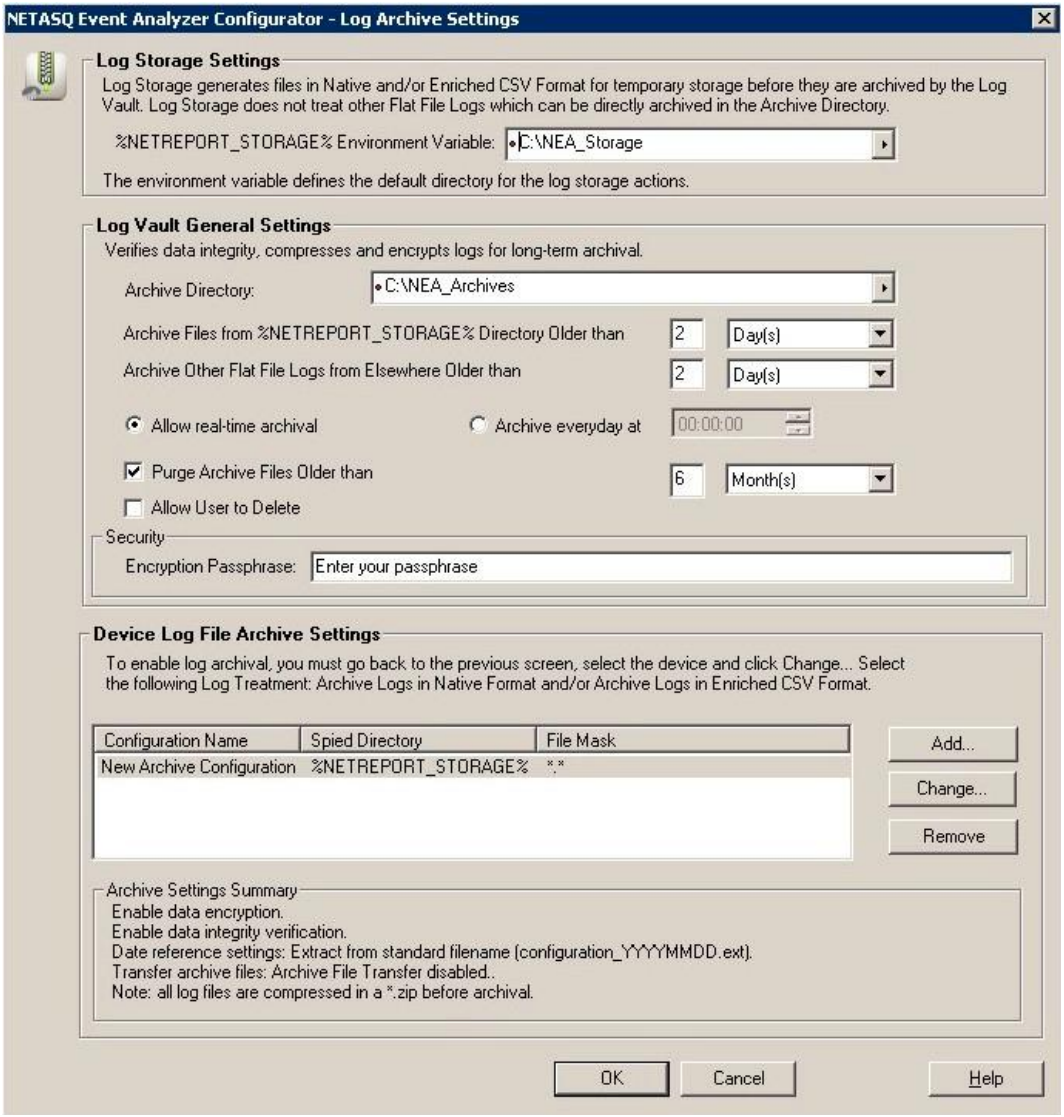


Podaj adres swojego serwera smtp w celu automatycznego wysyłania generowanych raportów na zdefiniowane w sekcji **To:** konto mailowe.

UWAGA !!!

Konfiguracja ta może zostać skonfigurowana tylko dla serwera smtp nie wymagającego uwierzytelnienia.

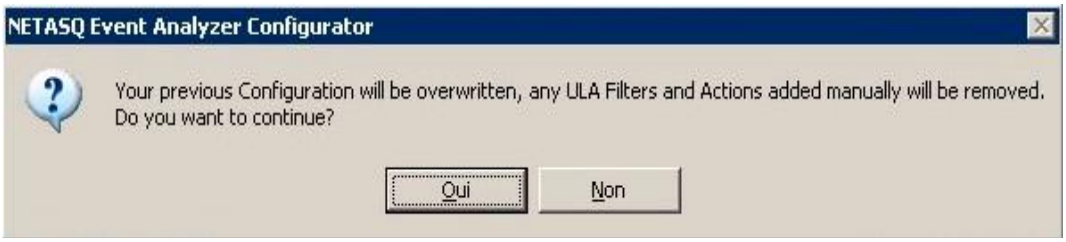
4.7 Konfiguracja Log Archiving



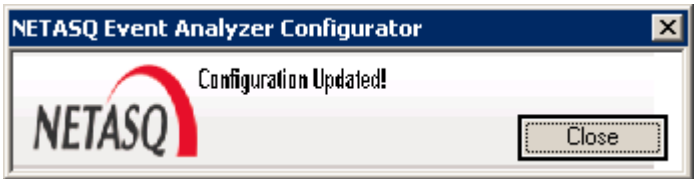
Konfiguracja ta daje administratorowi możliwość zdecydowania w jakiej formie mają zostać archiwizowane logi oraz przez jak długi okres czasu mają być przetrzymywane w systemie. Dodatkowo po skonfigurowaniu sekcji **Device Log File Archive Setings** logi te mogą być wysyłane przy pomocy ftp na dedykowany serwer.

4.8 Koniec konfiguracji

Po przejściu przez wszystkie elementy konfiguracyjne zostanie wyświetlony ekran



A następnie po zapisaniu konfiguracji i wyświetleniu komunikatu



Aplikacja Netasq Event Analyzer jest gotowa do pracy.

5. Netasq Event Analyzer w użyciu

5.1 Pierwsze logowanie

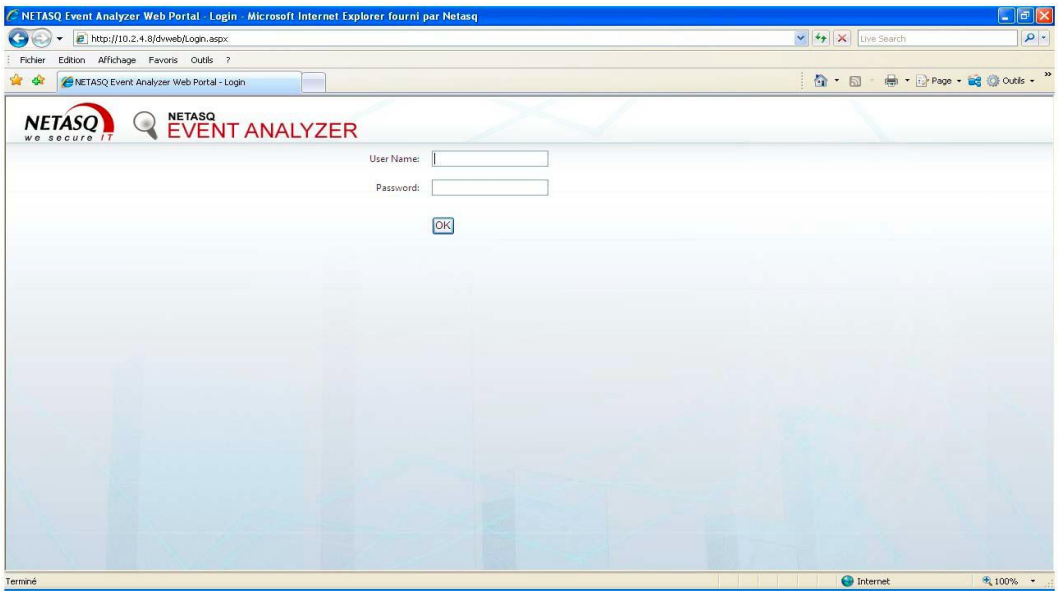
Konsola administracyjna jest dostępna przez przeglądarkę internetową pod adresem:

http://nazwa_serwera/dvweb

gdzie **nazwa_serwera** może być adresem IP, lub nazwą domenową

użytkownik: admin

hasło: admin



Przeglądarki z poziomu których można uruchomić Netasq Event Analyzera to:

- Internet Explorer w wersji 7 lub wyższej
- Google Chrome, Mozilla Firefox (za wyjątkiem raportów Cubes)

5.2 Konta użytkowników

W zależności od konta na jakie zaloguje się użytkownik do aplikacji Netasq Event Analyzer będzie miał dostępne różne opcje menu główne.

Services	User Admin	User Analyzer	User Viewer	User AdminDB
Access generated report	✔	✔	✔	
Report customization	✔	✔	✔	
Log forensic analysis	✔	✔		
Database utilities	✔			✔
Task scheduling	✔			✔
Web part configuration	✔			✔
Content builder	✔			✔
Web server administration	✔			✔

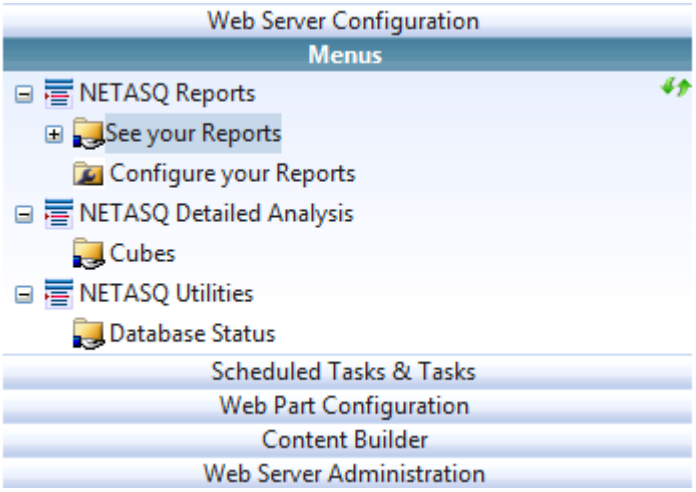
5.3 Menu

Po zalogowaniu się do konsoli Netasq Event Analyzera na konto o uprawnieniach administracyjnych **admin** (w przypadku darmowej licencji) użytkownik ma dostępne następujące menu

5.2.1 Web Server Configuration

Pozwala użytkownikowi zweryfikować na jakie konto zalogował się, oraz zdefiniować język i stronę startową.

5.2.2 Menu



See your Reports – dostęp do raportów generowanych zgodnie z harmonogramem

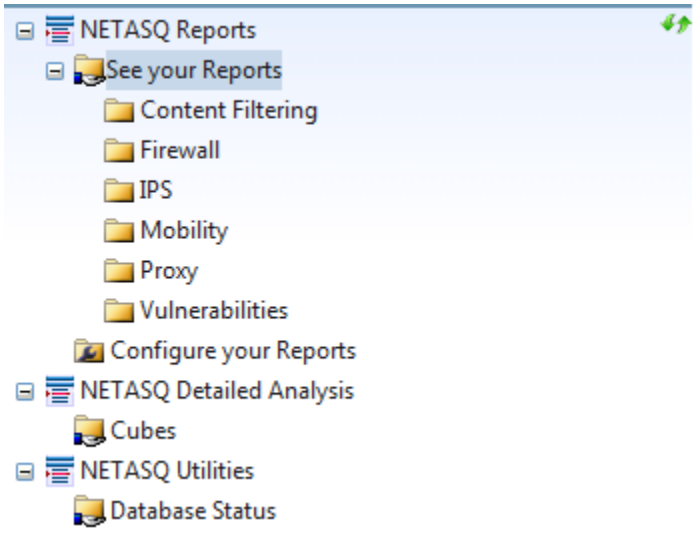
Configure your Reports – możliwość generowania raportów przez użytkownika w oparciu o szablony stworzone przez producenta

Cubes – możliwość wyeksportowania wyselekcjonowanych przez administratora logów do przenośnego pliku zewnętrznego w celu ich dalszej analizy

Database Status - możliwość weryfikacji statusu bazy

5.3 Typy raportów

Raporty w sekcjach **Generated Reports** oraz **Customized Reports** podzielone są w następujące grupy determinujące rodzaj generowanego raportu:



Content Filtering

- raporty skanowania AV dla HTTP, SMTP, POP3, FTP
- aporty skanowania antyspamowego dla SMTP, POP3
- raporty URL filtering

Firewall

- lista zezwolonych i zablokowanych połączeń

IPS

- lista alarmów zalogowanych na poziomie ASQ

Mobility

- raport aktywności SSL VPN

Proxy

- raport aktywności przeglądanych stron www

Vulnerabilities

- raport zagrożeń wykrytych przez moduł Seismo/Audyt podatności