



NETASQ





SPIS TREŚCI

SPIS TREŚCI 2
1. Wprowadzenie
2. Wymagania systemowe
2.1 System operacyjny
2.2 Wymagania sprzętowe 5
3. Instalacja
4. Podstawowa konfiguracja11
4.1 Konfiguracja License Certificate12
4.2 Konfiguracja Log Source14
4.3 Konfiguracja Network Configuration16
4.4 Konfiguracja Database17
4.5 Konfiguracja Scheduled Task18
4.6 Konfiguracja Mail Server
4.7 Konfiguracja Log Archiving19
4.8 Koniec konfiguracji20
5. Netasq Event Analyzer w użyciu
5.1 Pierwsze logowanie22
5.2 Konta użytkowników22
5.3 Menu23
5.2.1 Web Server Configuration23
5.2.2 Menu24
5.3 Typy raportów24

1. Wprowadzenie

Aplikacja **Netasq Event Analyzer** jest dostępna do pobrania na stronie <u>www.netasq.com</u> 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 <u>pomoc@netasq.pl</u> 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

뤻 NETASQ Event Analyzer - InstallShield Wizard	×			
License Agreement Please read the following license agreement carefully.				
 States copyright laws and international treaty provisions. Except as provided above, you may not copy the SOFTWARE or Documentation. 4.TRANSFER. You may transfer the SOFTWARE to another single computer, produced on proceedings on processing and the laws. (b) this license Arreement and the laws. 	ovided (a) you			
are transferred along with the SOFTWARE to the other computer, and the Botalie Ration software programs making up this single product package are transferred together. A permanent transfer is permitted if all copies of the SOFTWARE and Documentation, including all prior versions, are transferred together, you retain no copies, and the recipient agrees to the terms of this License Agreement.				
5.0THER RESTRICTIONS. If you receive the SOFTWARE in more than one me of the type or size of the media, you may use only the media appropriate for	dia, regardless			
• I accept the terms in the license agreement	Print			
C I do not accept the terms in the license agreement InstellShield				
< <u>B</u> ack <u>N</u> ext >	Cancel			

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

🛃 NETASQ I	Event Analyzer - InstallShield Wizard	×
Destinati Click Nex different	on Folder xt to install to this folder, or click Change to install to ; folder.	NETASQ we secure
	Install NETASQ Event Analyzer to: C:\Program Files\NETASQ\Event Analyzer\	<u>C</u> hange
InstallShield -	<u> </u>	Next > Cancel

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



5. Wybierz sposób instalacji i naciśnij Next

🙀 NETASQ Event Analyzer - InstallShield Wizard	×
Custom Setup Select the program features you want installed.	NETASQ we secure
Click on an icon in the list below to change how a feature is in	nstalled.
Image: NETASQ Event Analyzer Image: Filter Engine Image: Filter Engine	Feature Description Contains all the feature to install the whole NETASQ Event Analyzer solution This feature requires 132MB on your hard drive. It has 2 of 2 subfeatures selected. The subfeatures require 359MB on your hard drive.
Install to:	
C: (Program Files) vici AbQ(cvent Analyzer)	<u>⊆</u> hange
InstallShield	
Help Space < Back	<u>N</u> ext > Cancel

6. Wybierz komponenty jakie mają zostać zainstalowane i naciśnij Next

🚏 NETASQ Event Analyzer - InstallShi	eld Wizard		×
Ready to Install the Program The wizard is ready to begin installation	ı.	NI we	Secure IT
Click Install to begin the installation.			
If you want to review or change any of exit the wizard.	your installation	n settings, click Back. C	lick Cancel to
InstallShield ————————————————————————————————————	< <u>B</u> ack	Install	Cancel

7. Wybierz **Install** aby zainstalować.

🖶 NETASQ Event Analyzer - InstallShield Wizard 🛛 🗙				
	InstallShield Wizard Completed			
EVENT ANALYZER	The InstallShield Wizard has successfully installed NETASQ Event Analyzer. Click Finish to exit the wizard.			
NETASQ we secure IT	NETASQ Event Analyzer setup will now launch the NETASQ Event Analyzer Configuration Tool. If you are installing NETASQ Event Analyzer for the first time, it is recommended that you run the NETASQ Event Analyzer Configuration Tool at least once.			
	< <u>B</u> ack <u>Finish</u> Cancel			

8. Powyższy krok świadczy o zakończeniu instalacji.

👘 NETASO) Event Analyzer Installer I	nformation 🛛 🔀
0	You must restart your system changes made to NETASQ Eve effect. Click Yes to restart now restart later.	for the configuration nt Analyzer to take v or No if you plan to
	Yes	No

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

NETASQ	Event Analyzer Configurator	
Log So	purce	
	Configure NETASQ Event Analyzer log files treatment.	Settings
Networ	'k	
٨	Enter IP configuration data for internal and external IP Addresses and Subnet masks and define your network address ranges.	Settings
Databa	158-	
×	Configure the connection and Time Zone settings for the Database you want NETASQ Event Analyzer to use to manage your log file data.	Settings
Sched	uled Tasks	
14	Automate key Database management tasks (aggregate and purge data) and schedule report generation.	Settings
Mail S	erver	
	Define the Mail Server you want NETASQ Event Analyzer to use to send alerts,	Settings
Log Ar	chive	
ļ	Configure to store and archive device log files in a specific directory, with specific formats (CSV, Flat File, Syslog) and encrypt files.	Settings
licens	e Certificate	
N	View or update your current NETASQ Event Analyzer License Certificate.	Settings
	OK Cancel Applu	Help

4.1 Konfiguracja License Certificate

License	e Certificate	
N	View or update your current NETASQ Event Analyzer License Certificate.	Settings

W chwili pierwszego uruchomienia należy w oknie

	Aucune licence n'a été installée.	*
🌤 🔼	Please contact your supplier to receive the appropriate license certificate.	
		~

wybrać Change w celu zaczytania licencji

Otwieranie			• 🙀 Wyszuka	i i	×
🕛 Organizuj 👻 🔠 Wido	ki 👻 📑 Nowy folder				0
Ulubione łącza Pulpit Komputer Dokumenty Obrazy	Nazwa Administrator Administrator Publiczny Komputer Sieć nea	• Rozmiar	Typ Folder plików	Data modyfikacji 2010-11-07 21:09	N N
 Muzyka Ostatnio zmienione Wyszukiwania Publiczny 	iraport z cube nea-b38fb5cd-e510	2 KI	Folder pilków 8 Plik CERT	2010-11-13 11:58 2011-01-10 19:18	AN
Foldery					<u>`</u>
Foldery A	∢ iku: ∏		Lice	nse file Otwórz Anuluj	_

Wybierz swój plik licencyjny

IETASQ Ev	vent Analyzer Configurator - L	icense Certificate	×
<u>N/</u>	This Ce This License NE	ertificate was delivered to: Dagma authorizes you to use version of: TASQ Event Analyzer	*
	Business Application Intelligence Enterprise Edition v10.1		
	WebPortal Scheduled Tasks	3 Concurrent user(s)(Client Access) No	
	Project Types	NETASQ Projects (Execute only)	
	Maintenance Agreement	Valid until 2012-01-10	
	Networ	k & Security Intelligence Professional v10.1	
	Daily Records	200000	
		Oem	
	Device Names *	NETASQ UTM	
		NETASQ UTM Migration	
	Maintenance Agreement	Valid until 2012-01-10	
	NERAGUR	estilited Litense (Tuevices)	
			-
		OK Cancel Change	Help

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

Uwaga !!!

W chwili wygaśnięcia licencji aplikacja Netasą Event Analyzer przestanie działać. Logi przestaną być zaczytywane do bazy a także nie będą generowane raporty zgodnie z harmonogramem. Dodatkowo jeżeli w ramach aplikacji Netasą 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

100	Log So	urce	
		Configure NETASQ Event Analyzer log files treatment.	Settings

Ekran konfiguracyjny:

Name		Format			<u>A</u> dd
NETASQ UTN	4	Syslog			
NETASQ UTM	4 Migration	Flat File			<u>H</u> emove
NETASQUIN	1	Flat File			
					Properties.
Properties					
- ioperates	1				
Property	Value				
Time∠one:	LGMT+U	J1:00) Bruxelles, Coj o	penhague, Mad	ind, Paris	
Format:	10.2.4.1				
IP Address:	10.2.4.1	,0			L
Facility:					
Seventy.					
.og Treatme	nt				
_					
🗹 Generate 🛛	aily and M	onthly Mobility Dash	iboards		
🗹 Generate 🛛	aily and M	onthly Vulnerabilities	s Dashboards		
🗹 Generate 🛙	aily and M	onthly Content Filter	ing Dashboards	s	
Generate D	aily and M	onthly Intrusion Prev	vention System	Dashboards	
	ailu and M	onthlu Provu Dashb	oarde		
N I senerare I					
i Generate L	Jaily and Mi	onthly Firewall Dash	boards		
Generate [the second s			
☑ Generate [☑ Generate [☑ Archive log	is in Enrich	ed CSV format			
Generate [Generate [Archive log Aggregate	is in Enrich Spam Infor	ed CSV format mation			

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

ASQ Event Analyzer (onfigurator - Add Device e:	
IETASQ UTM	2	
Name	Description	
IETASQ UTM IETASQ UTM Migration	For NETASQ For NETASQ	
	ОК	Cancel <u>H</u> elp

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

Log File Acquis	sition Setting	gs				
Device Type:	NETASQ	UTM				
Device Name:	NETASQ UT	ſM				
Log Source-						
Flat File L	.og	Enter local directory only				
File Directory:		• C:\Program Files (x86)\Click and DECiDE\NSI\Log •				
C Log in Real-Time with Syslog Protocol Syslog IP Address: Advanced						
Log Time Zor	ne Settings—					
🗖 Use UTC	offset (Coordir	nated Universal Time)				
Time Zone:	(UTC+01:00)) Brussels, Copenhagen, Madrid, Paris 🗾				
	Adjust for Daylight Saving Time (DST)					
		OK Cancel <u>H</u> elp				

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 Netasą

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

ETASQ Event Analyzer Configurator NETASQ UTM Define your Company Domain Name EVENT ANAL	YZER
Internal Domain Name	Add
netasq.com	<u>C</u> hange
	Homore
< <u>Précédent</u> <u>S</u> uivant > Terminer	Aide

4.3 Konfiguracja Network Configuration



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

102100.055.255		Add.
132,100,203,200	Internal 192	
172 31 255 255	Internal 172	Lhang
	Local host	<u>R</u> emo
	Broadcast	-
200.200.200.204	External	Move
		Move D
	172.31.255.255 255.255.255.254	172.31.255.255 Internal 172 Local host Broadcast 255.255.255.254 External

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



Please use only Case	e Insensitive settings.
Database Server:	Local SQL Server
Server Name:	NEA-TESTS
Server Instance:	SQLEXPRESS
- Login	
Windows User:	NT AUTHORITY\Local System
Password:	Te
Configure the update	e settings for the NEA Database. e g data
Database Tim	e Zone Settings Coordinated Universal Time)
🔲 Use UTC offset (0	
Use UTC offset (C Time Zone: (GMT+	-01:00) Bruxelles, Copenhague, Madrid, Paris

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

4.5 Konfiguracja Scheduled Task

Automate key Database	management tasks (aggregate and purge data) eration.	Settings.
5Q Event Analyzer Configurator - Tasks So	cheduling X	
Scheduling		
Run the Consolidation, Aggregation,	Purge and Report Tasks everyday at 🚺:00:00 🚊	
Purge Settings		
Detailed Data	Aggregated Data	
C Delete all data after treatment	. Keep last 62 🚔 days of data.	
🕫 Keep last days.	Keep last 12 🚔 months of data.	

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

	Defin alerts	e the Mail Server you want NETASQ Event Analyzer to use to send	Settings.
ASQ Ev	ent An	alyzer Configurator - Mail Server	1
ПГ	Mail Se	erver (SMTP)	
	youren	nailserver	Test
	From:	Enter the e-mail addresses to use to send alerts. report@company.com	
	Ter	admin@aamaanu.aam	

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



%NETREPORT_STORAC	TUEAL OUTEL FIALTHE FOUS WHICH CAN DE UNECLU ALCHIVED IN THE ALCHIVE DIJECTURY
%NETREPORT_STORAG	
	βE% Environment Variable: ●C:\NEA_Storage
The environment variable d	efines the default directory for the log storage actions.
on Vault General Setti	pas
Verifies data integrity, comp	presses and encrypts logs for long-term archival.
Archive Directory:	C:\NEA_Archives
1 1: E1 / ANET	
Archive Files from %NET	REPORT_STURAGE% Directory Ulder than 2 Day(s)
Archive Other Flat File Lo	ogs from Elsewhere Older than 2 Day(s)
Allow roal time probin	al C Archive evendou at 100-00-00
 Allow real-time archiv 	
🔽 Purge Archive Files (Dider than 6 Month(s) -
Allow User to Delete	
Security-	
Encryption Passphrase:	Enter your passphrase
Pevice Log File Archive To enable log archival, you the following Log Treatmen	Settings I must go back to the previous screen, select the device and click Change Select It: Archive Logs in Native Format and/or Archive Logs in Enriched CSV Format.
	Spied Directory File Mask Add
Configuration Name	
Configuration Name	%NETREPORT_STORAGE% **
Configuration Name	%NETREPORT_STORAGE% *.*
Configuration Name	%NETREPORT_STORAGE% *.* Change Remo

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

NETASQ B	Event Analyzer Configurator	X
?	Your previous Configuration will be overwritten, any ULA Filters and Actions added manually wi Do you want to continue?	l be removed.

A następnie po zapisaniu konfiguracji i wyświetleniu komunikatu

NETASQ Event Analyzer Configurator	×
Configuration Updated!	
NETASO	Close
NETASQ	Close

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

🖉 NETASQ Event Analyzer Web Portal - Login - Microsoft Internet Explorer fourni par Netasq		
(G) ←	🖌 😽 🗶 Live Search	P-
Fichier Edition Affichage Favoris Outils ?		
😪 🐼 🌈 NETASQ Event Analyzer Web Portal - Login	🛅 * 🗟 - 🖶 * 🔂 Page - 😂 (💮 Outils 🔹 🎽
User Name:		
Password:		
ОК		
Terminé	🕒 Internet 🖲	100% -

Przeglądarki z poziomu których można uruchomić Netasą 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	v	v	4	
Report customization	v	v	v	
Log forensic analysis	v	v		
Database utilities	v			
Task scheduling	v			
Web part configuration	v			
Content builder	v			v
Web server administration	v			v

5.3 Menu

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

Web Server Configuration	_
Menus	
Web Part Configuration	
Content Builder	
Web Server Administration	

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