

en.SafeWatch Filtering **Real-Time Web-Based Watchlist Screening** *Reduce Risk, Cost and Complexity with EastNets*

Today, financial institutions worldwide must monitor, investigate and report suspicious transactions to meet regulatory requirements and protect themselves against money laundering and terrorism financing risk. Firms that fail to do so are exposed to fines, penalties, and reputational risks that can drastically affect an institution's name, image and shareholder value.

Ranked as a top filtering solution by Celent, en.SafeWatch Filtering offers a robust solution to help organizations ensure compliance with the evolving AML requirements. Its highly sophisticated matching engine ensures rapid identification of potential risks and very few false positives, saving your compliance team substantial time and money. en.SafeWatch Filtering acts as the central monitoring point for all your financial traffic, irrespective of

your data format and where it may reside. It is rapidly deployable and offers seamless integration with your existing systems. In the new web-based version, en.SafeWatch Filtering offers a web-GUI with enhanced visualization, from increased text box spaces, to reorganized and combined search criteria, as well as improved displays of violations types among many others.

The merging of the Alert Manager and Detection Manager enables more information available on one screen, without any change in the features of the modules. Today, more than 400 major financial institutions in over 80 countries have trusted en.SafeWatch Filtering to comply with both International and local AML regulations.

Modular Connectivity to Adapt to Your Business Processes

At a very high level, en.SafeWatch Filtering obtains data regarding your customers, beneficiaries and

Market-Leading Watchlist Filtering to Help You:

- Manage and Control Risk in Real Time
- Ensure Compliance with AML Laws and Regulations
- Control Costs with Rapid Deployment and Implementation
- Reduce Workload with Reduced False Positives
- Streamline Processes and Improve Operational Efficiencies



Ready Application
Alliance Monitoring Add-on 2011

transactions from different data sources. The Data Source Connectors are specifically written to capture data from a particular application or a particular format. The data captured by these Connectors are then processed by the en.SafeWatch server and are checked against the loaded sanctions, Politically Exposed Persons or black lists depending on the rules specified within its rule-based engine. After the execution of these rules, the detections can be logged or generate alerts that are sent to the central alert management interface. The Data Source Connectors of en.SafeWatch Filtering include:

SWIFT Alliance Connector: delivers seamless integration with your existing SWIFT environment through attaining a “SWIFT Ready Application” label from SWIFT; ensures real time filtering of both your incoming and outgoing SWIFT messages and immediately prevents the emission of suspicious messages into the SWIFT Network.

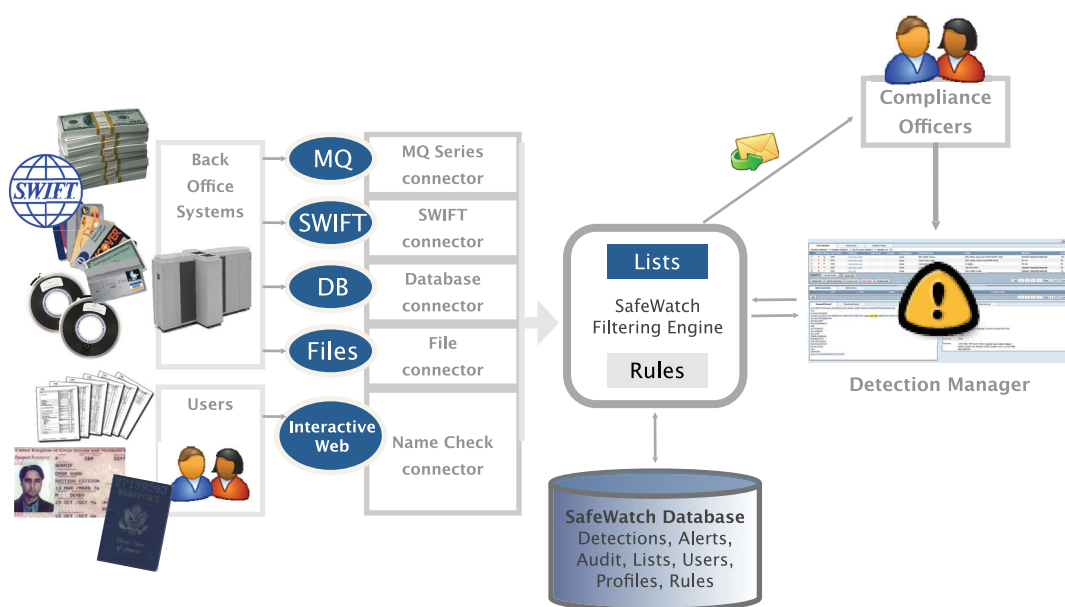
FILE Connector: scans the contents of huge data text files irrespective of their size and formats. It ensures quick and powerful scanning by offering optimizations like parallel

scanning, which allows multiple scan processes and batch checking. The flexible configuration of this connector allows en.SafeWatch Filtering to work with almost any file format imaginable.

DATABASE Connector: The flexible configuration of this module allows en.SafeWatch Filtering to extract data directly out of the tables or views, scan them and even update the table fields with the scan results.

MQ-SERIES: provides transaction screening facilities to MQ-compatible external systems, such as core banking or middleware applications. This module uses IBM MQ-Series middleware to enable communication between the external system and the en.SafeWatch Server.

API Connector: allows institutions to integrate their in-house (developed) applications with en.SafeWatch Filtering. In addition, it can be used by third party integrators who want to integrate the en.SafeWatch Filtering engine with their solutions.



en.SafeWatch Filtering provides a comprehensive and robust environment for real-time list filtering and management.

Name Checker: performs quick manual name scans to check if it matches any black listed entity. Typically used by clerks at the front desk, while entering new customer information, to check if the customer has been black listed.

Easy Watchlist Updates and Management

As AML requirements are constantly evolving, meeting compliance has become a challenging and complex exercise. With en.SafeWatch Filtering institutions can easily manage an unlimited number of lists, including official lists, private lists and lists provided by recognized third party list providers. en.SafeWatch Filtering offers features including list version control, offline tests and list comparisons. In addition, EastNets offers an automated Official Watch Lists update service, which provides access to the official lists and their updates as soon as they are modified by the regulatory authorities.

Flexible Branch by Branch Configuration

Additionally, en.SafeWatch Filtering accommodates institutions of varying sizes. It incorporates the Zone Concept which is useful for large institutions with distributed geographical locations. The Zone Concept enables strict segregation of information pertaining to each branch. Zones can be achieved while continuing to utilize one server to perform all the required checks, thereby lowering both your maintenance and operational costs.

Key Benefits to Customers that Choose EastNets' en.SafeWatch Filtering Solution:

- **Compliance with the Evolving AML Laws and Regulations**

en.SafeWatch Filtering is adaptable to the continuously changing requirements set by AML regulators and ensures that your institution remains compliant at all times.



“ING Direct is very pleased with the implementation and results of en.SafeWatch Filtering. With this robust solution in place, we can ensure that our customers and our organization spanning multiple geographies are well protected against risk.”

“With en.SafeWatch Filtering we can accelerate our internal authentication decisions, reduce the risks associated with user anonymity and comply with the numerous International and Local AML and ATF regulations. Today, en.SafeWatch Filtering has successfully helped us achieve a higher level of STP and a quicker time to compliance.”

Henk Meijer
Senior Manager Anti-Fraud & Anti-Money Laundering
ING Direct

• **Central Monitoring Point for All Your Financial Traffic**

Having a single point for detection allows compliance officers and auditors to have one consolidated interface where the alerts from all sources are concentrated.

• **Rapid Identification of Potential Risks**

To help you prevent criminal activities from occurring within your institution in real time, en.SafeWatch Filtering offers real time notifications of suspicious data and transactions, generating immediate alerts and email notifications to system users while executing multi-level alert management workflows.

• **Seamless Integration with Your Existing Systems**

en.SafeWatch Filtering ensures smooth and seamless integration with your existing systems and applications without affecting their performance.

• **Highly Sophisticated Matching Engine**

The Matching engine of en.SafeWatch Filtering applies advanced detection algorithms and matching techniques

to screen data against loaded lists, e.g. it is able to identify misspellings of words even if phonetically written.

• **Very Few False Positives**

en.SafeWatch Filtering eliminates an unnecessary workload on your compliance officers by ensuring a very low level of false positives. en.SafeWatch Filtering provides one of the lowest ratio of false positives in the AML industry.

• **Highly Flexible and Scalable Solution**

The data source connectors of en.SafeWatch Filtering can be added depending on the customers' needs and can be easily expanded to incorporate other data source connectors to accommodate your future needs and requirements. In addition, compliance officers can easily configure lists, system parameters and set unique rules.

• **Strong Reporting Capabilities and Audit Trail**

To satisfy most regulator and audit requirements, en.SafeWatch Filtering offers standard reports that cover the most common reporting needs, custom reports and a comprehensive audit trail.

The screenshot displays the Detection Manager interface. At the top, it shows 'Scan Results' with a table of reported violations. Below this is an 'Alert Comments' section and a 'Scanned Record' section with a 'General' tab.

Match	Status	Alert Ticket	Violation	Risk Score	Priority	Investigator	Matched Entity	Entity	Blacklist	Rank
		1036	Osama Bin Laden			Ruser	BIN LADIN, Osama	BIN LADIN, Usama bin Muhammad bin Awad	Specially Designated Nationals	100
		1037	Osama Bin Laden			Ruser	Osama, Bin Laden	BIN LADEN, USAMA MUHAMMED AWAD	EU List	90
		1038	Osama Bin Laden			Ruser	Osama Bin Laden Organization	Al-Qaida	EU List	84
		1039	Osama Bin Laden			Ruser	USAMA BIN LADEN ORGANIZATION	ISLAMIC ARMY	Specially Designated Nationals	84
		1040	Bin Laden			Ruser	BIN LADEN, Sa'd	BIN LADEN, Sa'ad	Specially Designated Nationals	78

Scanned Record

```
{[1:F018C1T1H00009113797853]{2:03001549081028C1T0DEFFA0004090429770810291549U}{4:
:154:
:20:P010015002388
:21:NEW:22A-NEW:94A:784BC1TMM 784BC1TMM 784BC1TMM Osama Bin Laden 784BC1TMM 784BC1TMM
:22:C:BC1TFF2794BC1TMM
:24A:KCT10PFF
:87A:ROBEEBEOXX
:15B:
:30T:20081029
:30V:20081031
:36:1:2784
:32B:EUR19555.69
:57A:BC1T1TMM
:37B:US03000.00
:53A:CHASUS3300X
:57A:BC1TUS33
:15C:
:24D:PHON
-}{5:{{CHC:CE26788A051E}}}{S:{{COP:P}}
```

General

Match Status: Reported violation
 Match Rank: 78
 Official Name: BIN LADEN, Sa'ad
 Address:
 Title:
 Category: Individual
 Listed on: Specially Designated Nationals Thu Jan 06 13:00:00 EET 2011
 Programs: SDGT
 External Id: 11378
 Entity ID: 6182
 Remarks: DOB 1982; POB Saudi Arabia; nationality Saudi Arabia; Passport S20951 (Sudan); alt: Passport S30951 (Sudan); a.k.a.: 'AL-KAHTANE, Abdul Rahman'.

As a single point for managing detections and alerts, the Detection Manager is the centralized operating unit of en.SafeWatch Filtering. With its web-based user interface, it preserves the global and user friendly view that enables users to search for, view, release, block, and assign for investigation all hits captured by the system engine in a quick and efficient manner.

Contact us today and learn how we can help you protect against risk and preserve your bottom line.



info@eastnets.com
www.eastnets.com