NetGuardians

RiskTech 100 2019

Gartner 2015 CoolVendor

NG|Screener UI Administration

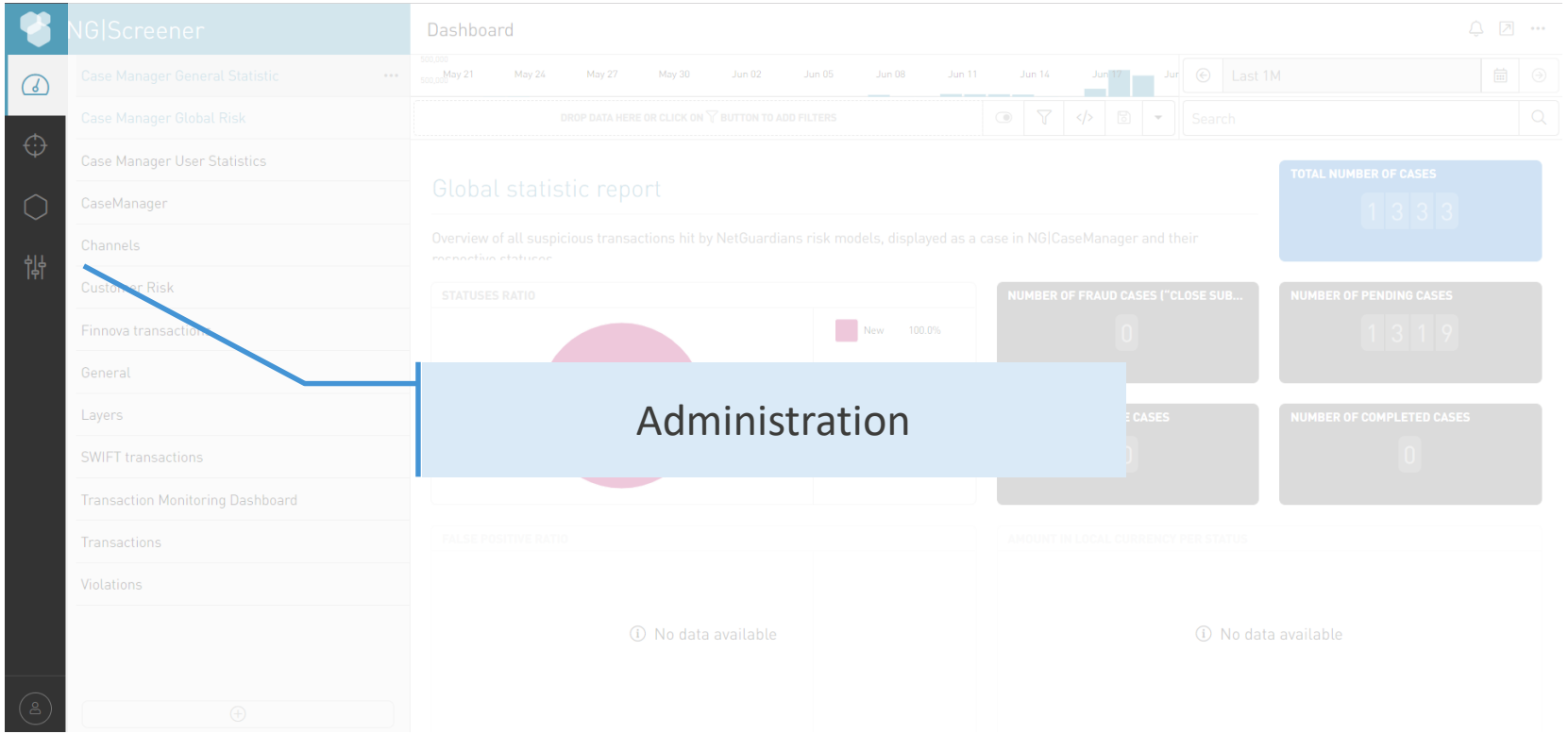
Ljupce Nikolov
June 2019

swiss made software

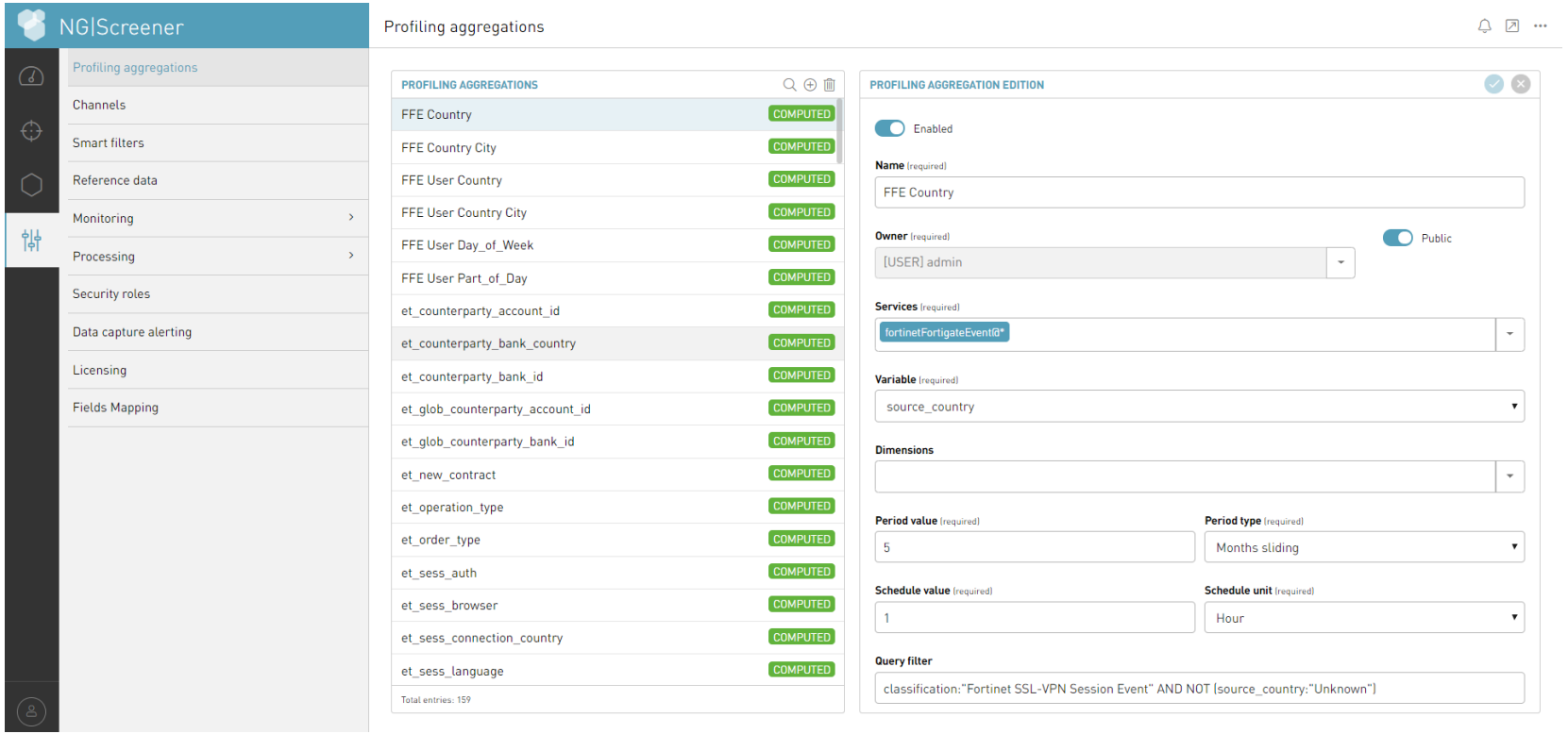
Summary

- Access to Admin section
- Security Roles
- Channels
- Smart Filters
- Data Capture alerting
- Licensing
- Fields Mapping
- Custom Processing

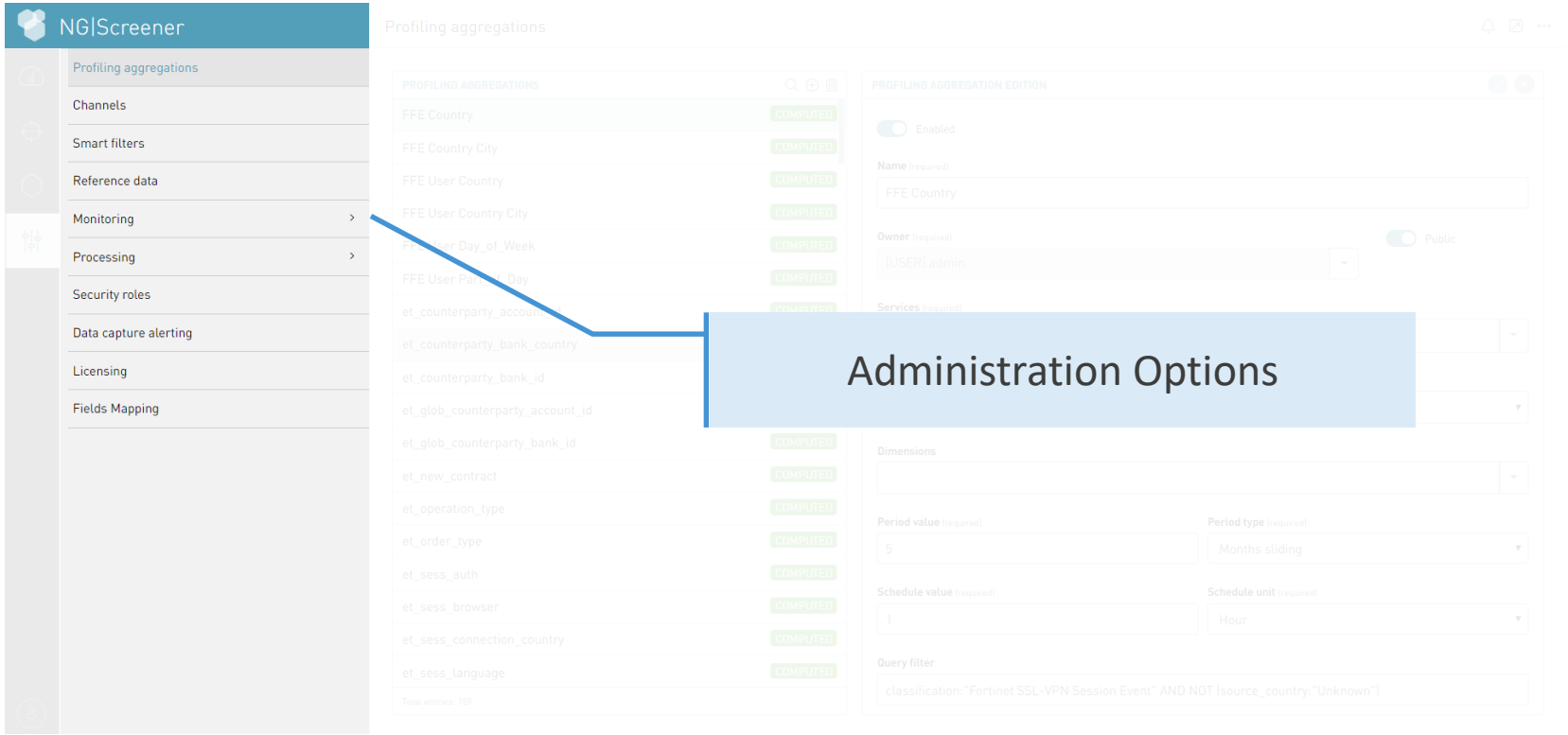
Access Admin section



Admin section Menu



Admin section Menu



NetGuardians

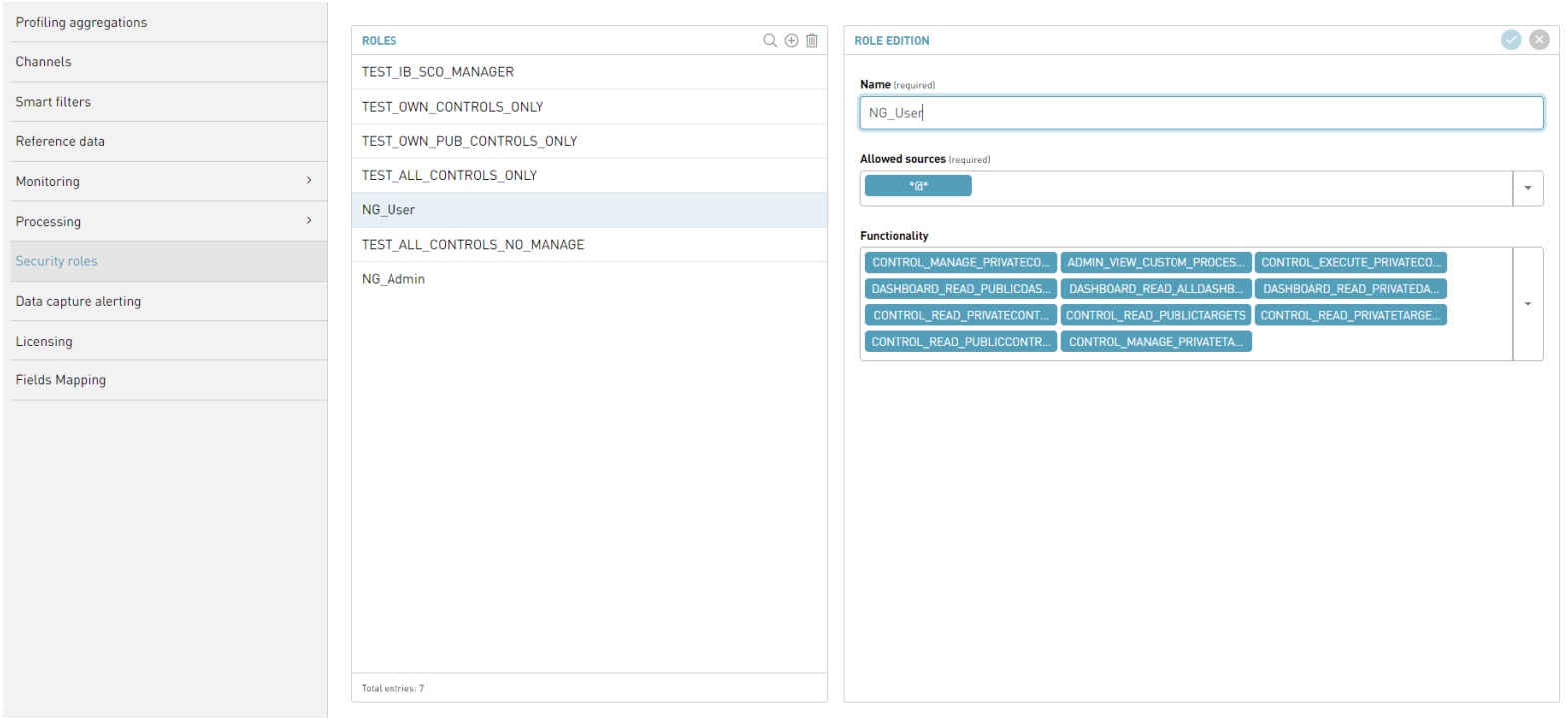
Security Roles

swiss made software

Security Roles

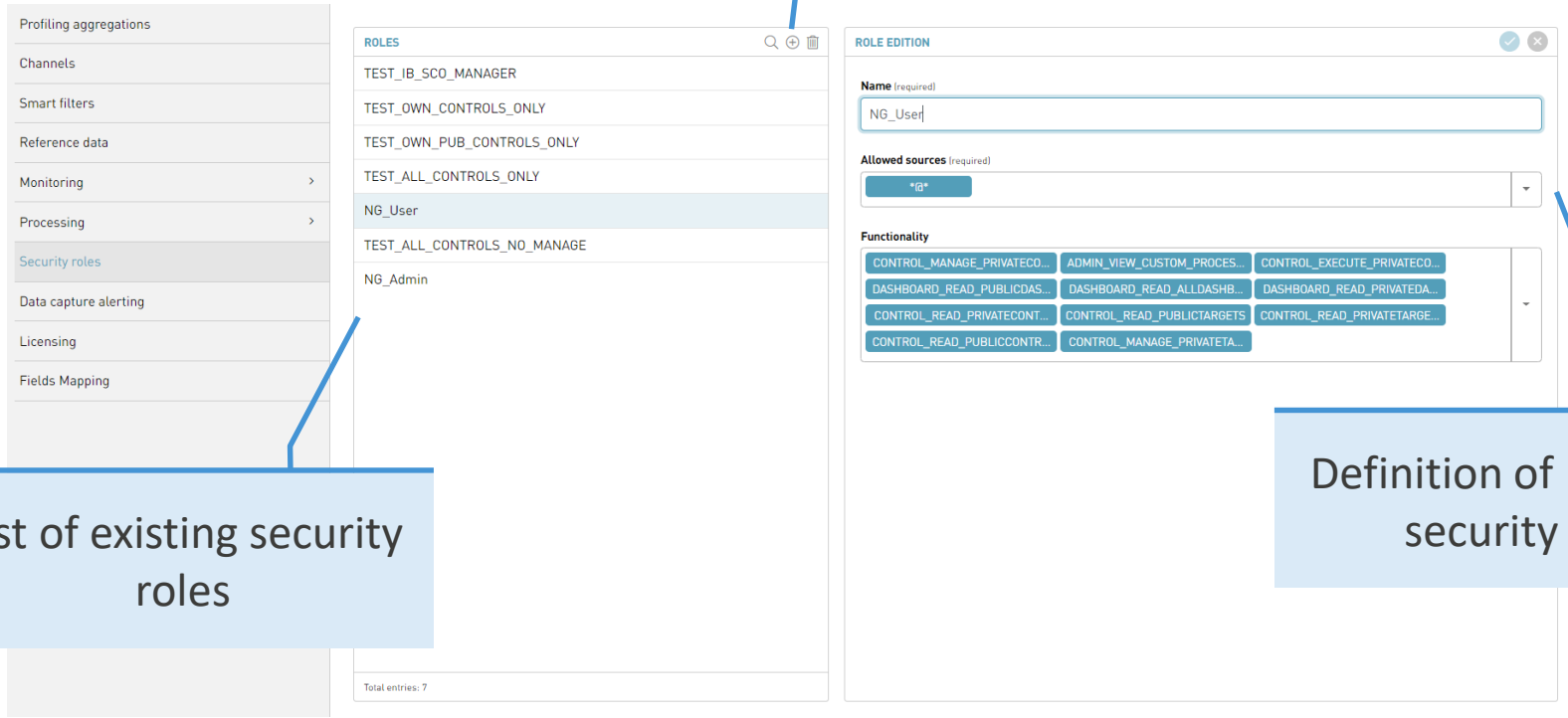
- User authentication is handled by NG|Auth
  - No user creation in NG|Screener UI
  - Only roles definition
- A role defines
  - Which data source a user can have access to
  - Which application functionality he can use
- Assignment of roles done through NG|Auth
  - Mapping of roles (Cf. NG|Auth slides)
- If two roles are assigned to a user, access rights will be union of both rights
- By default two roles are present:
  - NG_Admin (Could not be deleted)
  - NG_Users

Security Roles



Security Roles

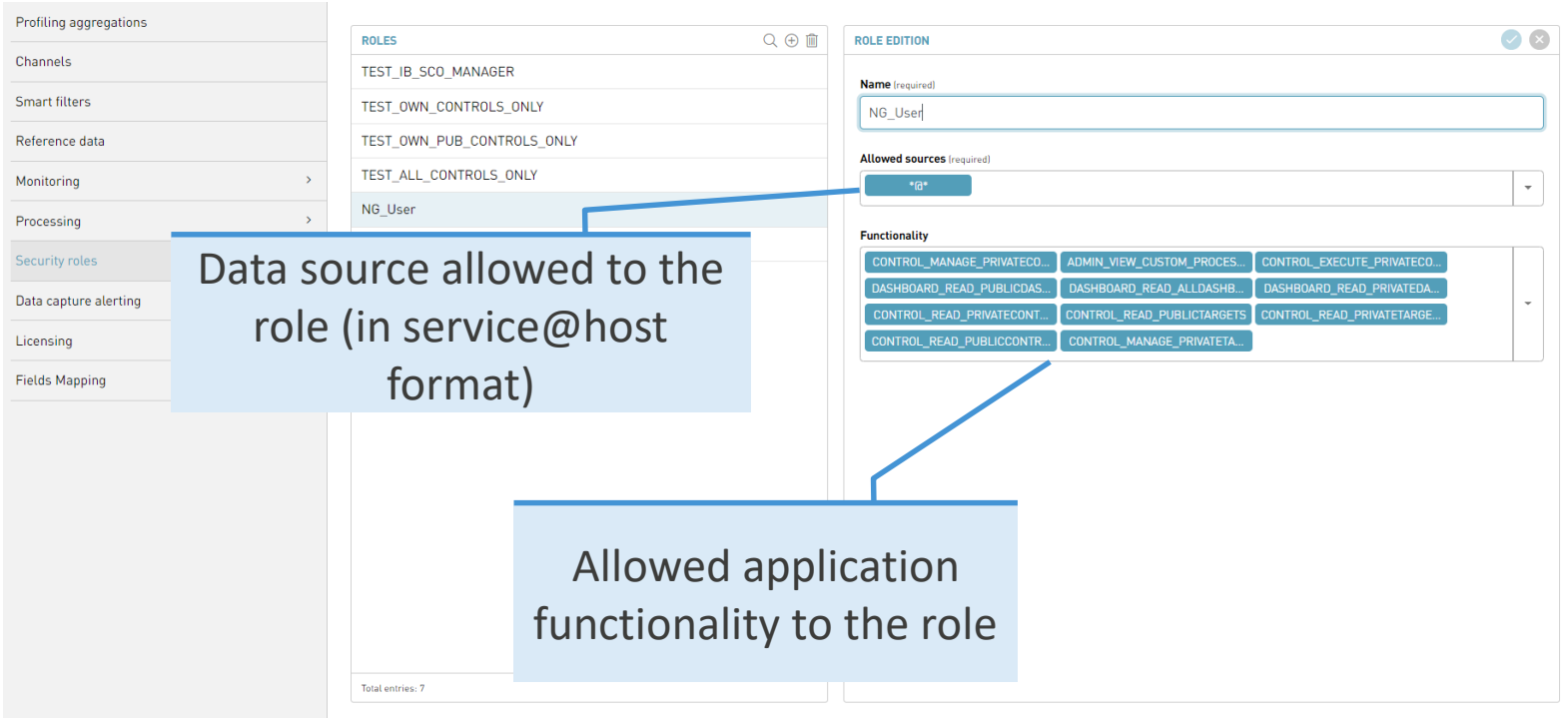
Add new security role



List of existing security roles

Definition of NG_User security role

Security Roles



NetGuardians

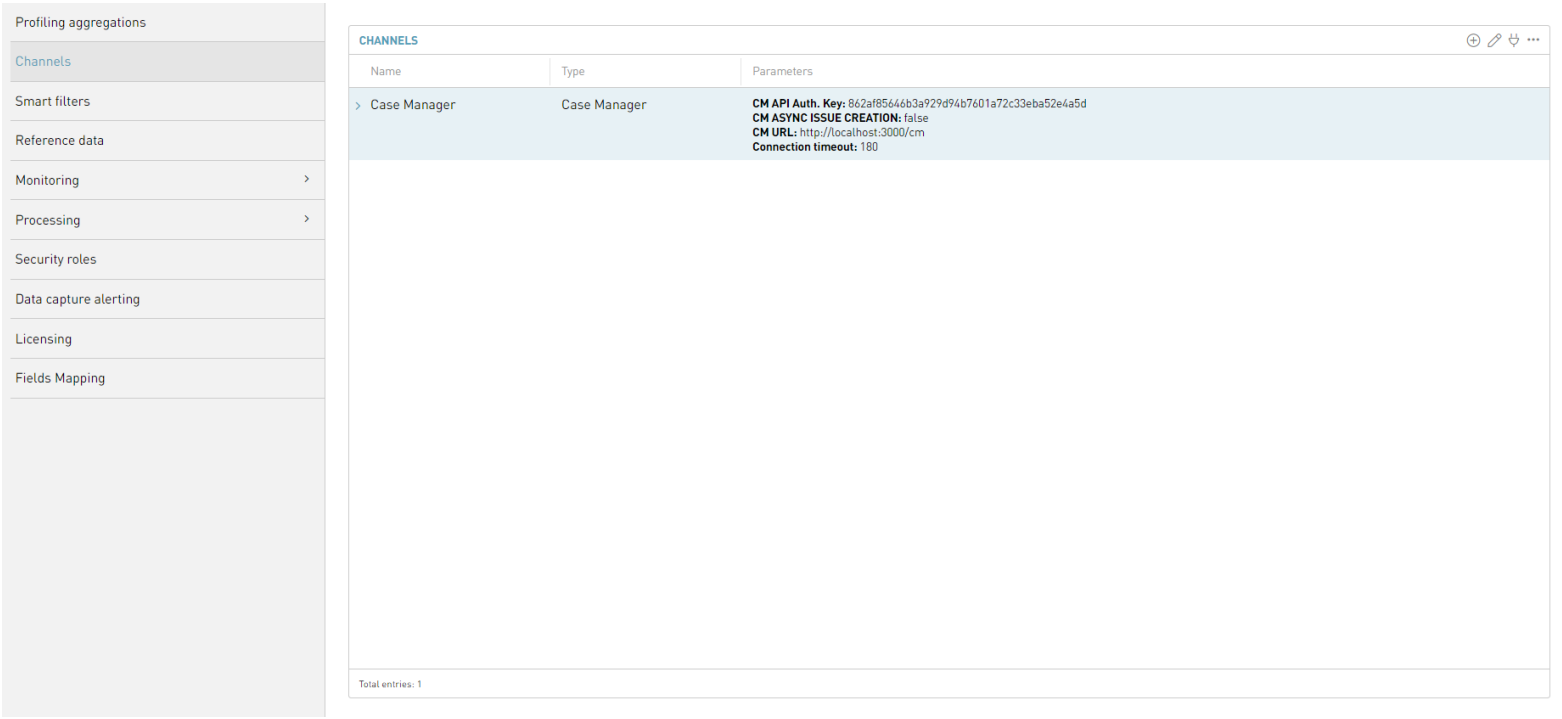
Channels

swiss made software

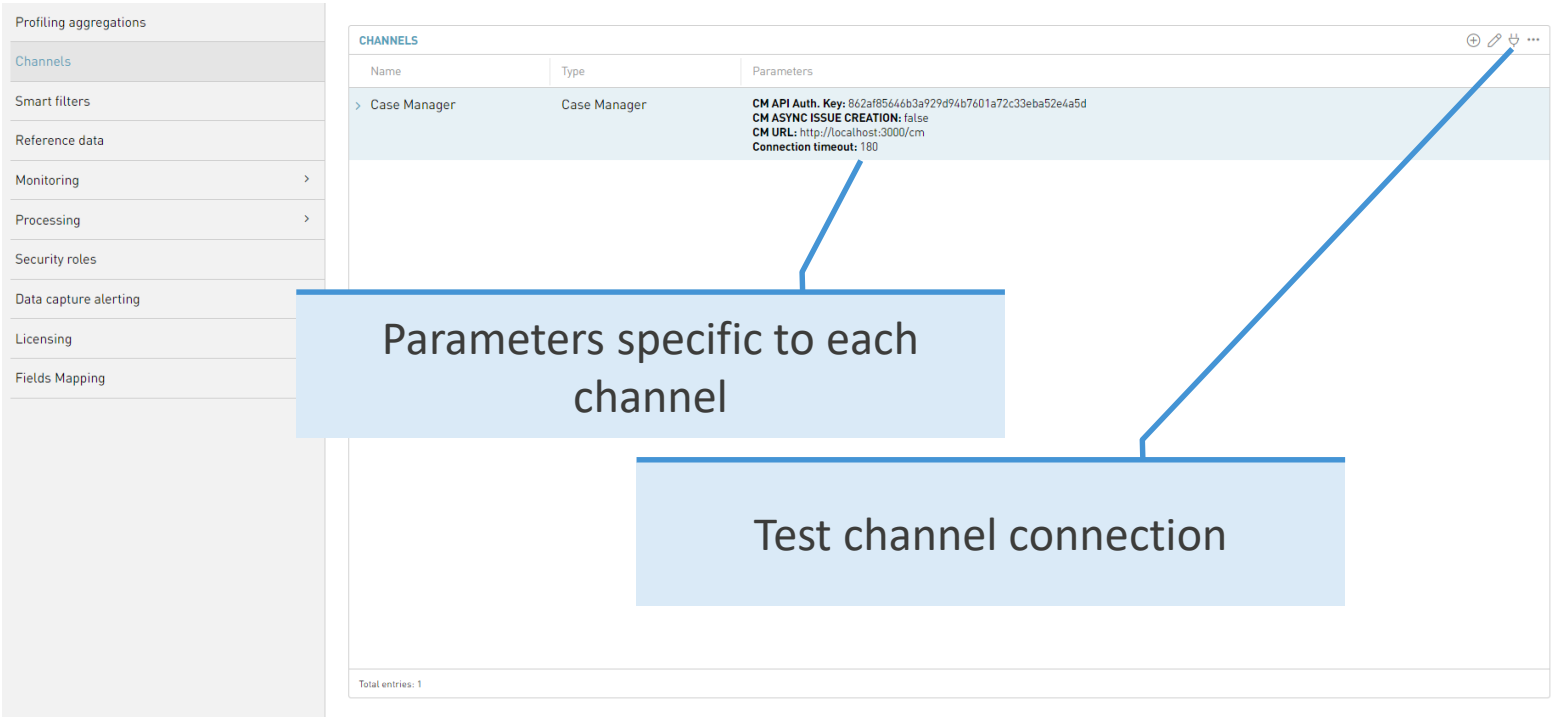
Channels

- Means of delivering controls to end users
- Composed of a channel containing target(s)
  - **Chanel:** Server and protocol to send controls to
  - **Target:** recipient(s) of the control
- Available type of channels
  - Case Manager
  - Email
  - FTP
  - SCP
  - SMB

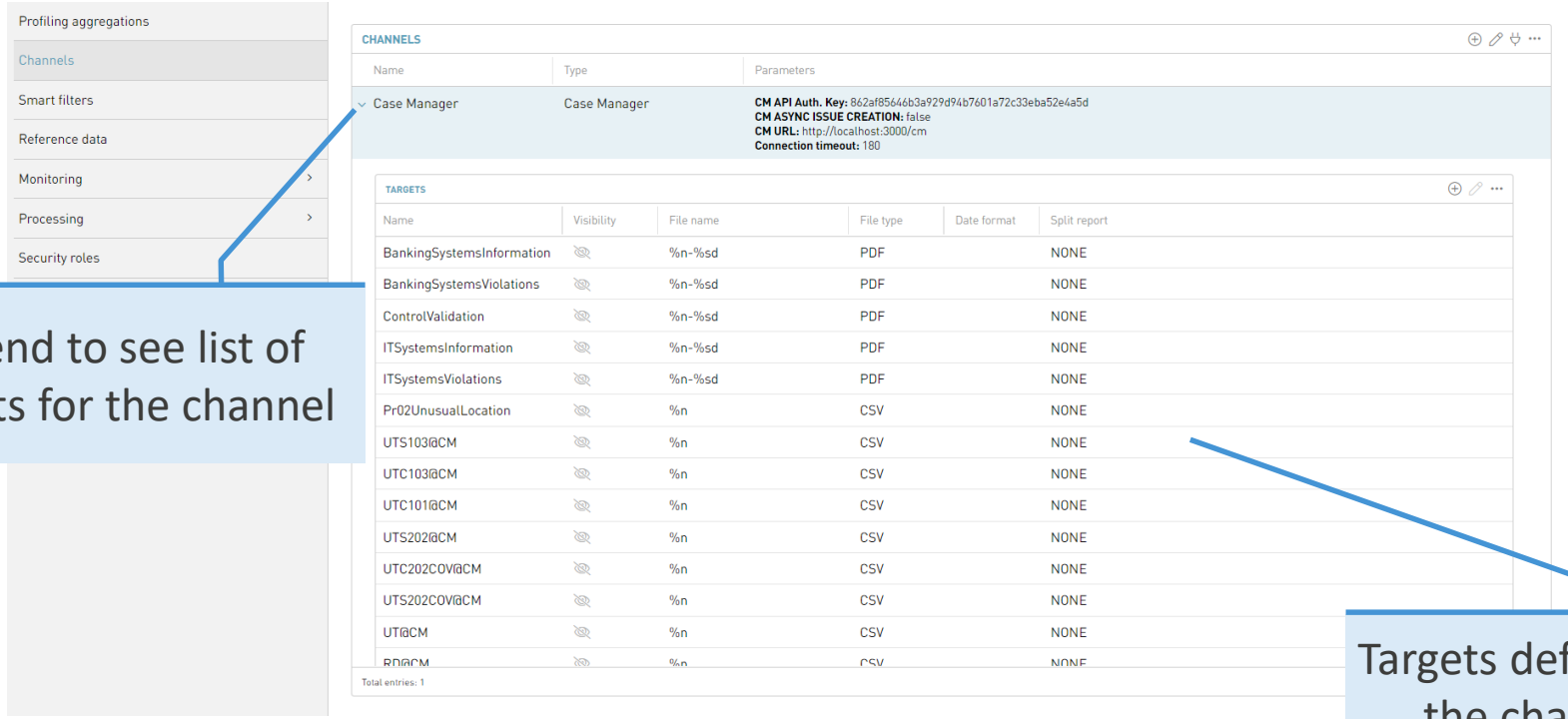
Channels List



Channels List



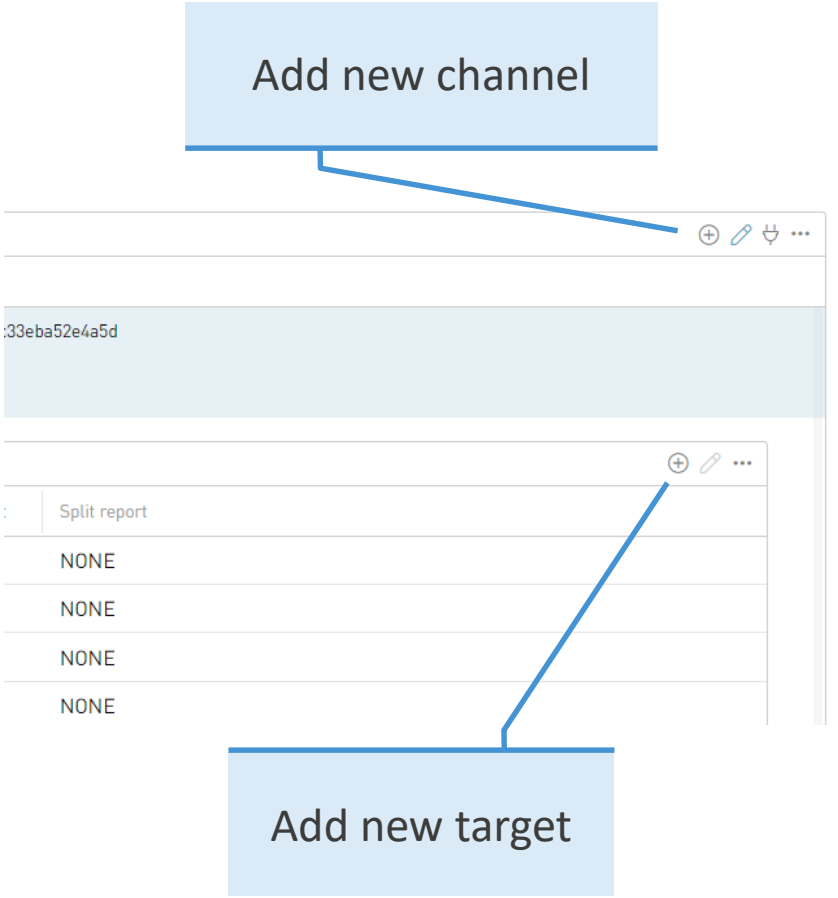
Channels List



Define Channel and Target

- Click on “+” to add a **new channel**
  - Options differs for each type of channel

- Click on “+” to add a **new target** to the channel
  - Options will differ for each type of target



Case Manager channel and target example

- Most important parameters
  - Channel Information
    - URL of Case manager
    - Authentication Key
    - …
  - Target Information
    - Assignee
    - Case manager Project
    - …
- More details in Case Manager Administration training

Email channel and target example

- Most important parameters
  - Channel Information
    - SMTP server info (IP/Port)
    - Authentication information (if needed)
    - Sender email
  - Target Information
    - Email recipient(s)

NetGuardians

RiskTech 100 2019

Gartner 2015 Cool Vendor

Smart Filters

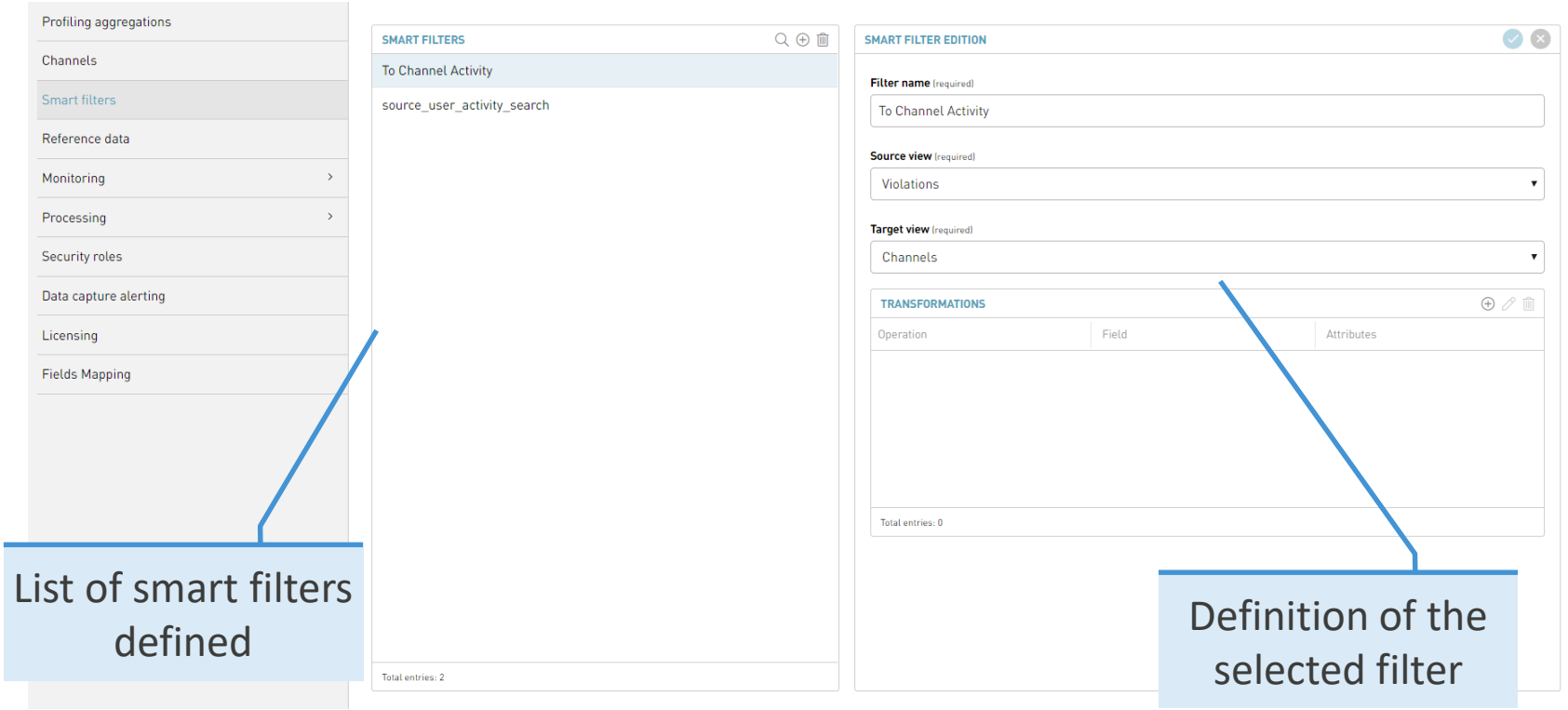
swiss made software

Smart Filters

- Smart Filters help navigate from one view to another (dashboards)

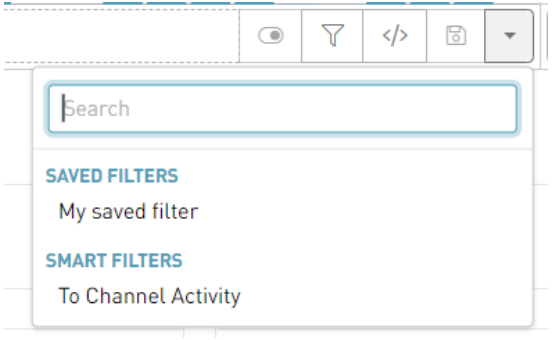
- Transformation could be applied to filters when switching view

Smart Filters



Smart Filters parameters

- **Filter Name** the name of the filter that will appears in the filter lists (in dashboards)
- **Source View** the dashboard in which the filter should appears
- **Target View** the dashboard to display after the execution of the filter
- **Transformations** the list of transformations this filter should apply.



NetGuardians

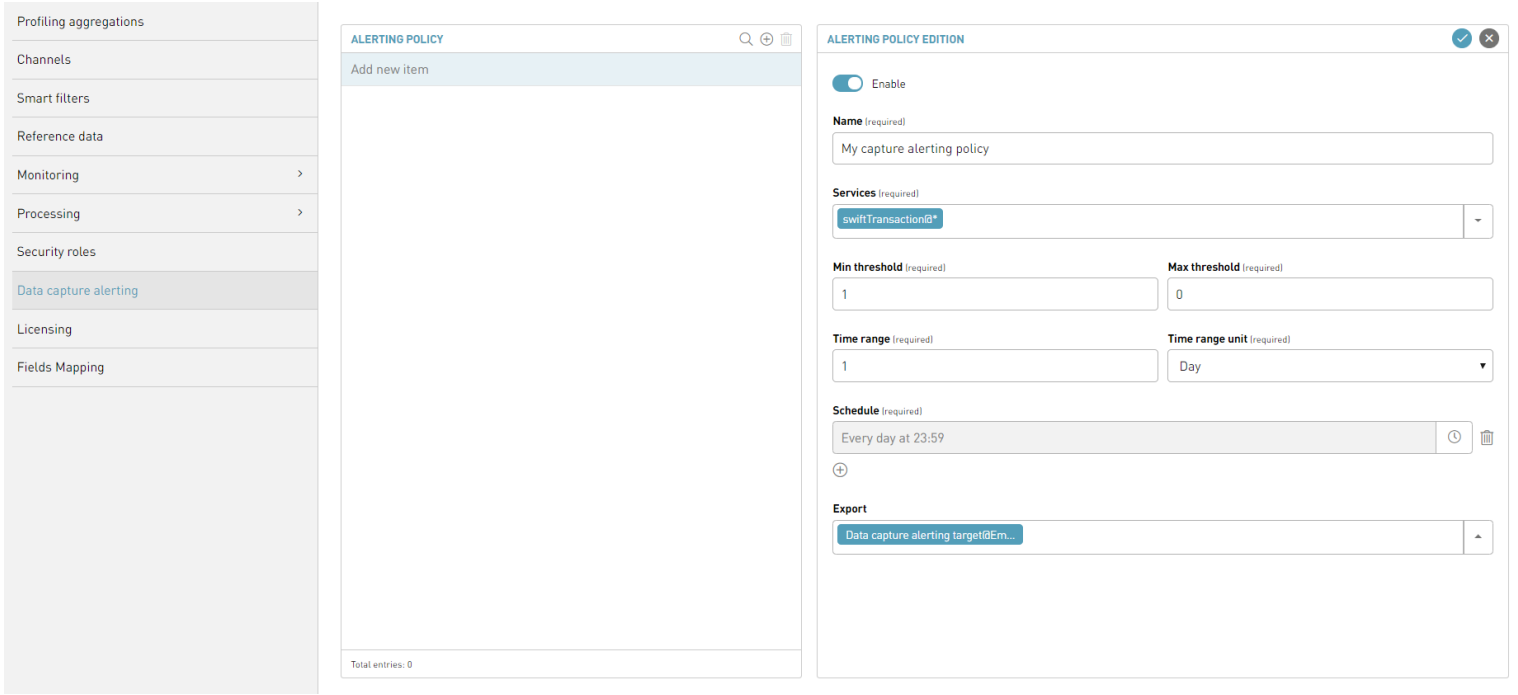
Data Capture Alerting

swiss made software

Data Capture alerting

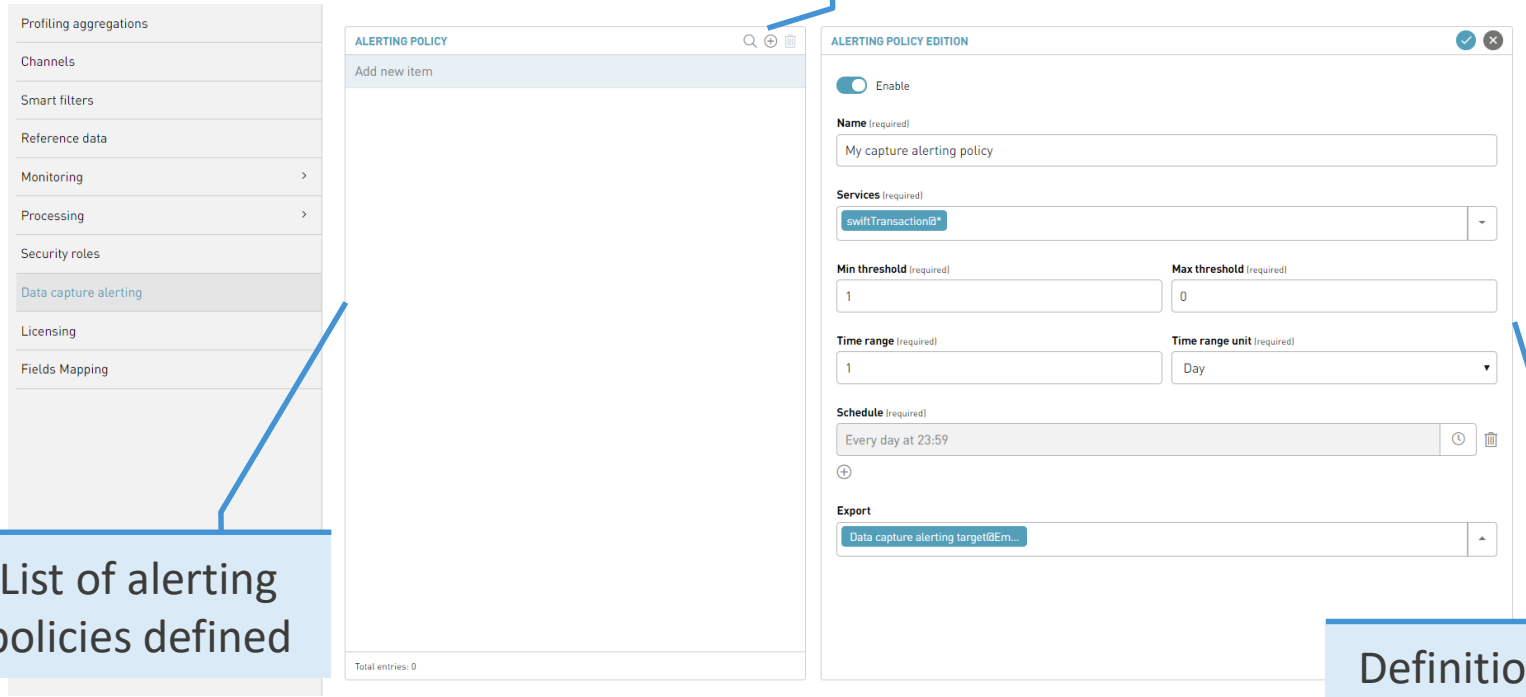
- Define threshold on event count on specific timeframe (called Policies)
  - Help detecting sources that stop sending logs
- Define (min/max) thresholds
- Schedule can be defined
- Alerts by mail when threshold met

Data Capture alerting



Data Capture alerting

Create a new alerting policy

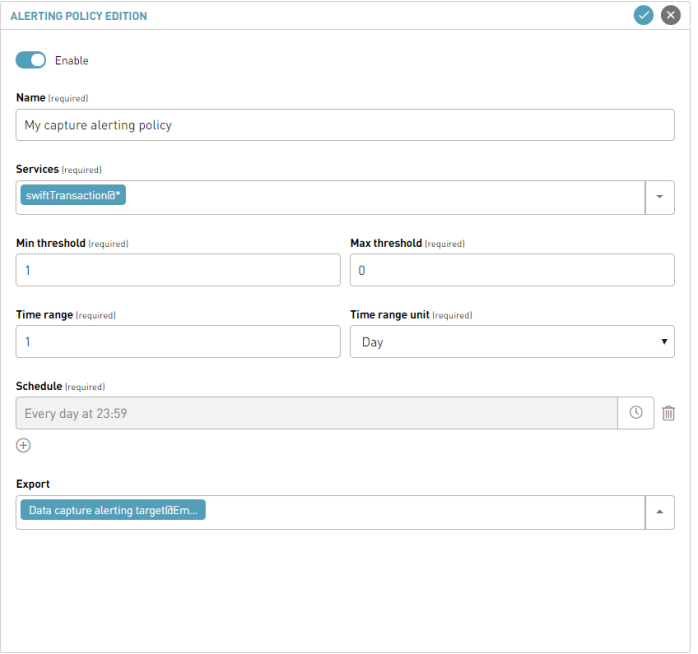


List of alerting policies defined

Definition of the alerting policy

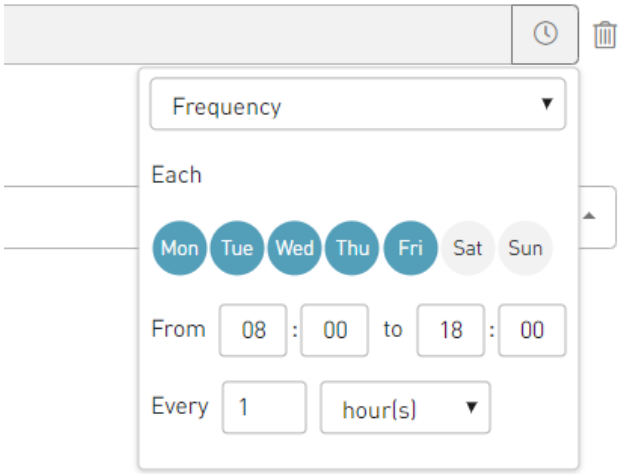
Data Capture alerting

- Name: the name of the policy
- Services: the host/service to be analysed
- Min Threshold: the minimum threshold, if the number of audit trails is less than this value, an alert is raised. If this value is 0, the min threshold is not considered.
- Max Threshold: the maximum threshold, if the number of audit trails is greater than this value, an alert is raised. If this value is 0, the max threshold is not considered.
- Time Range: the time range to be analysed
- Schedule: When checks should be performed
- Export: Email channel to send alerting mail to (cf. Channels)



Data Capture alerting

- Schedule options
  - Daily: specific time every day
  - Weekly: Days of the week when to check (Mon-Fri for example)
  - Monthly: Days of the month when to check (10th and 20th of each month for example)
  - Yearly: When in the year to check
  - Frequency: cf. options on the right



NetGuardians

Licensing

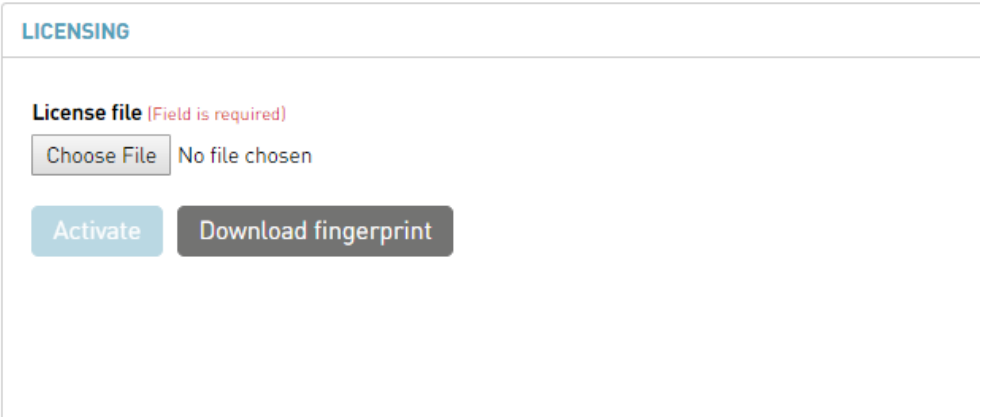
swiss made software

Licensing

- Licensing is based on a fingerprint of the server
  - CPU ID and MAC address
- It specifies a duration and a number of connectors that could be installed
- Fingerprint generation is needed upon first license generation
  - No need of fingerprint for updates
- After reception of updated license from NG Support, update could be made on NG|Screener UI

Licensing

- Download fingerprint (c2v file)
- Choose file and upload new license to server (v2c file)
- Activate license
- License operation could also be done from the backend
  - `ngadmin` command



NetGuardians

RiskTech 100 2019

Gartner 2015 Cool Vendor

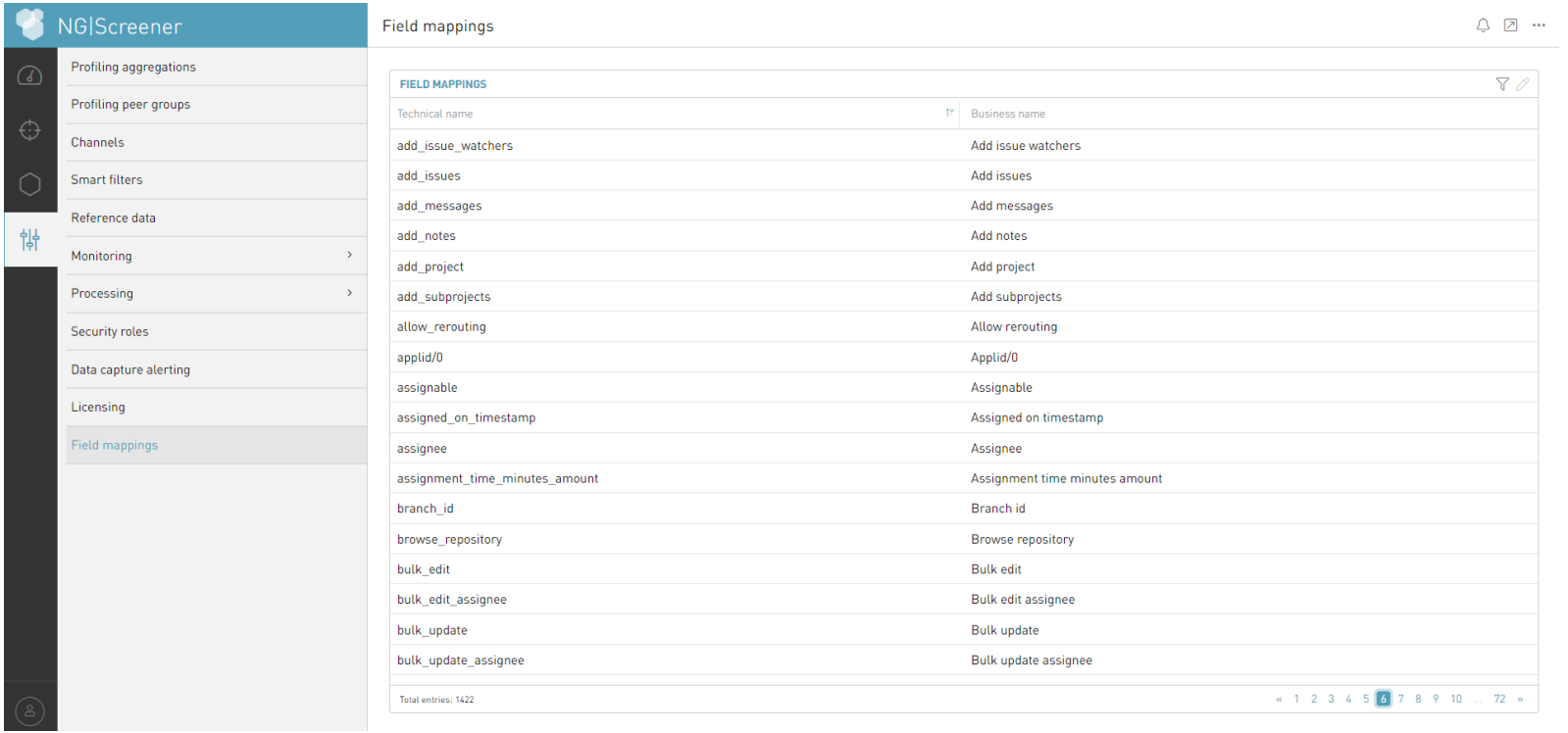
Fields Mapping

swiss made software

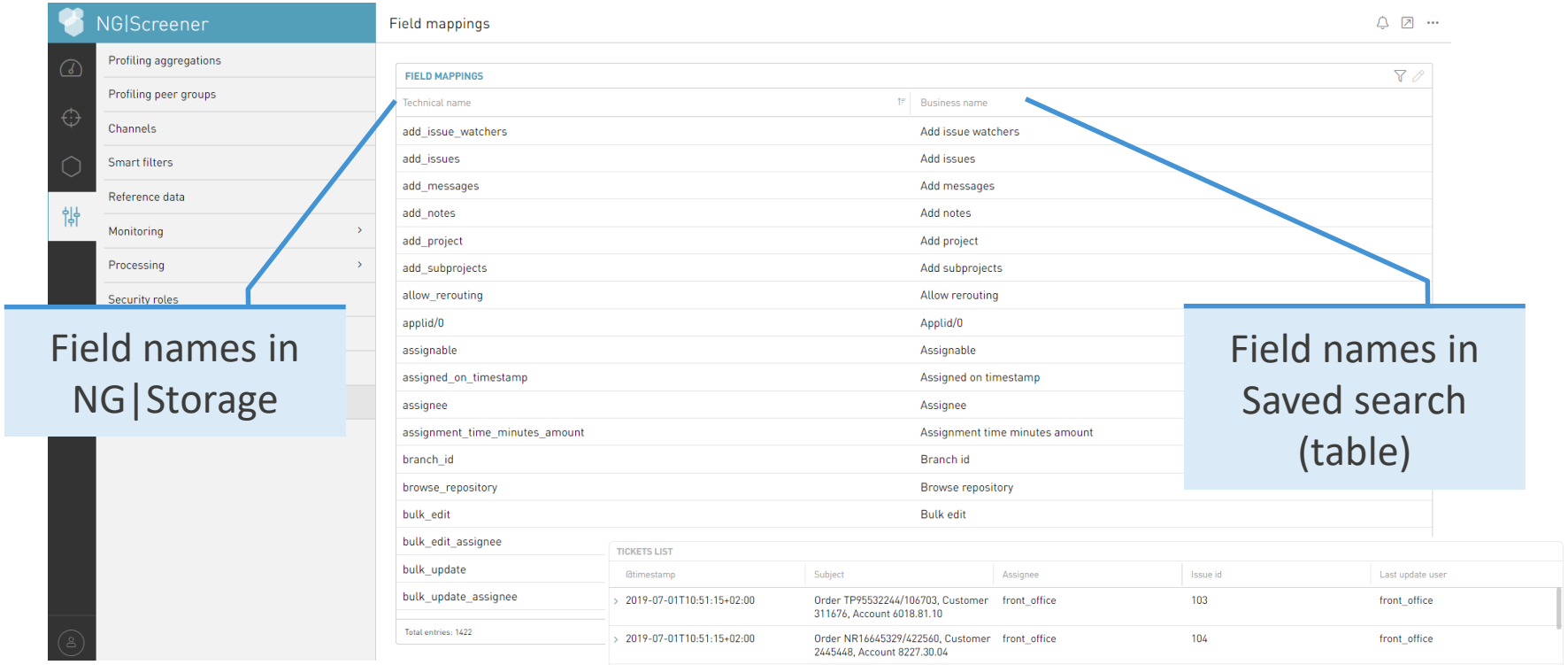
Fields Mapping

- Possibility to have more friendly names in save search (Tables) in dashboards
- Fields as they are stored in NG|Storage could still be too technical (could not have space, etc..)
- Common change: Remove _ and start with capital letter
  - source_user → Source User

Fields Mapping



Fields Mapping



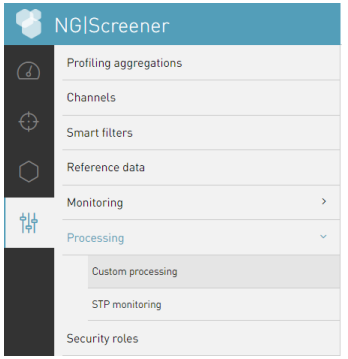
NetGuardians

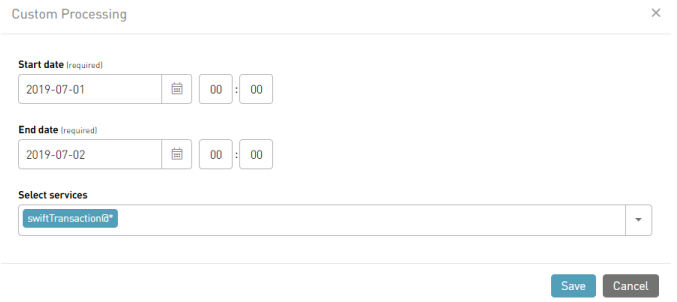
Custom Processing

swiss made software

Custom Processing

- Data in NG|Storage has a limited span
- Custom processing period option allow to add temporarily data that are out of NG|Storage for investigation
  - Note: Data will be removed from NG|Storage at midnight
- Parameters
  - Start date/time
  - End date/time
  - Services to be imported
- To access, select Admin → Processing, then Custom processing





Thank you!

NetGuardians

+41 24 425 97 60

info@netguardians.ch

www.netguardians.ch

Linkedin.com/company/netguardians

Facebook.com/NetGuardians

@netguardians

https://www.youtube.com/netguardians

Ljupce Nikolov

+41 24 425 97 60

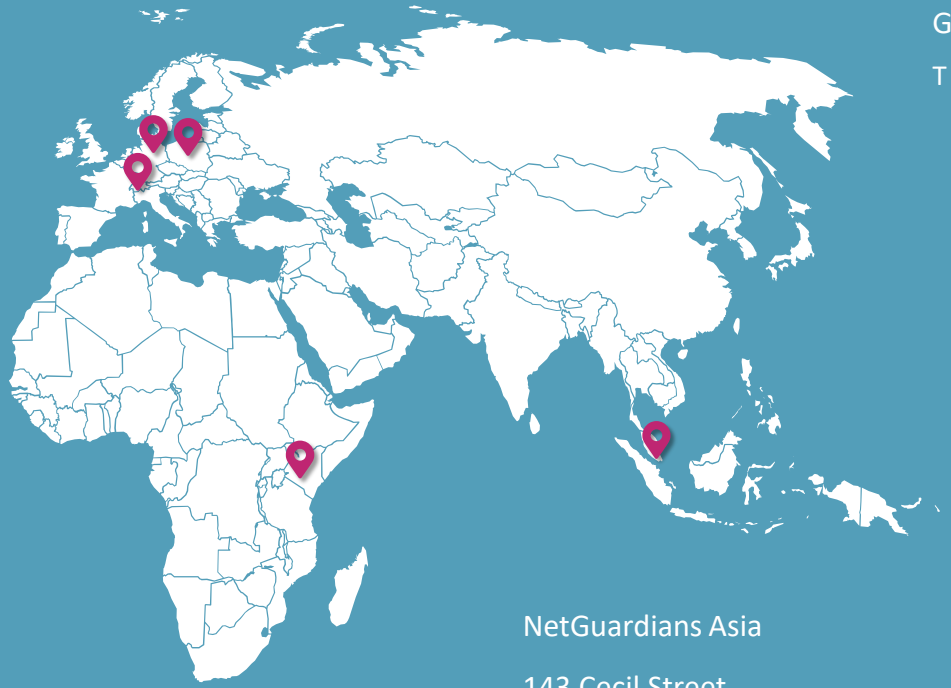
nikolov@netguardians.ch

Contact us

NetGuardians Headquarters

Y-Parc, Av. des Sciences 13
1400 Yverdon-les-Bains
Switzerland

T +41 24 425 97 60



NetGuardians Germany

Rhein-Main Gebiet
Germany

T +49 172 3799003

NetGuardians
Eastern Europe

Koszykowa 61, 00-667
Warsaw, Poland

NetGuardians Africa

Vienna Court
State House Rd
Nairobi, Kenya

+254 205 138539

NetGuardians Asia

143 Cecil Street
#09-01 GB Building
069542 Singapore

T +65 6224 0987