NetGuardians

RiskTech 100 2019

Gartner 2015 Cool Vendor

NG|Screener UI Usage

Ljupce Nikolov
June 2019

swiss made software

Summary

- Overview
- Login to the application
- Main Window
- Dashboards
- Controls

Overview

- NGScreener UI provides
  - Dashboards aimed at
    - Summarizing Violations triggered by the system
    - Investigate original data through forensic dashboards
  - Controls definition and tuning
  - Administration of application (Covered in separated slides)
    - Application Authorization (Roles definitions)
    - Delivery Channels for controls
    - Not administration of appliance itself

Overview

- Requirements

Browser	Minimal version
Edge	13
Firefox	38
Chrome	30

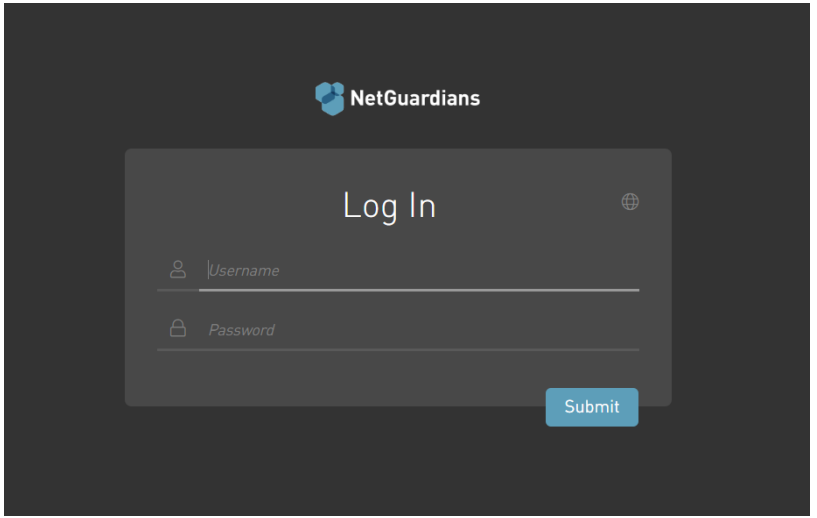
- Javascript to be activated in Web Browser

Access to application

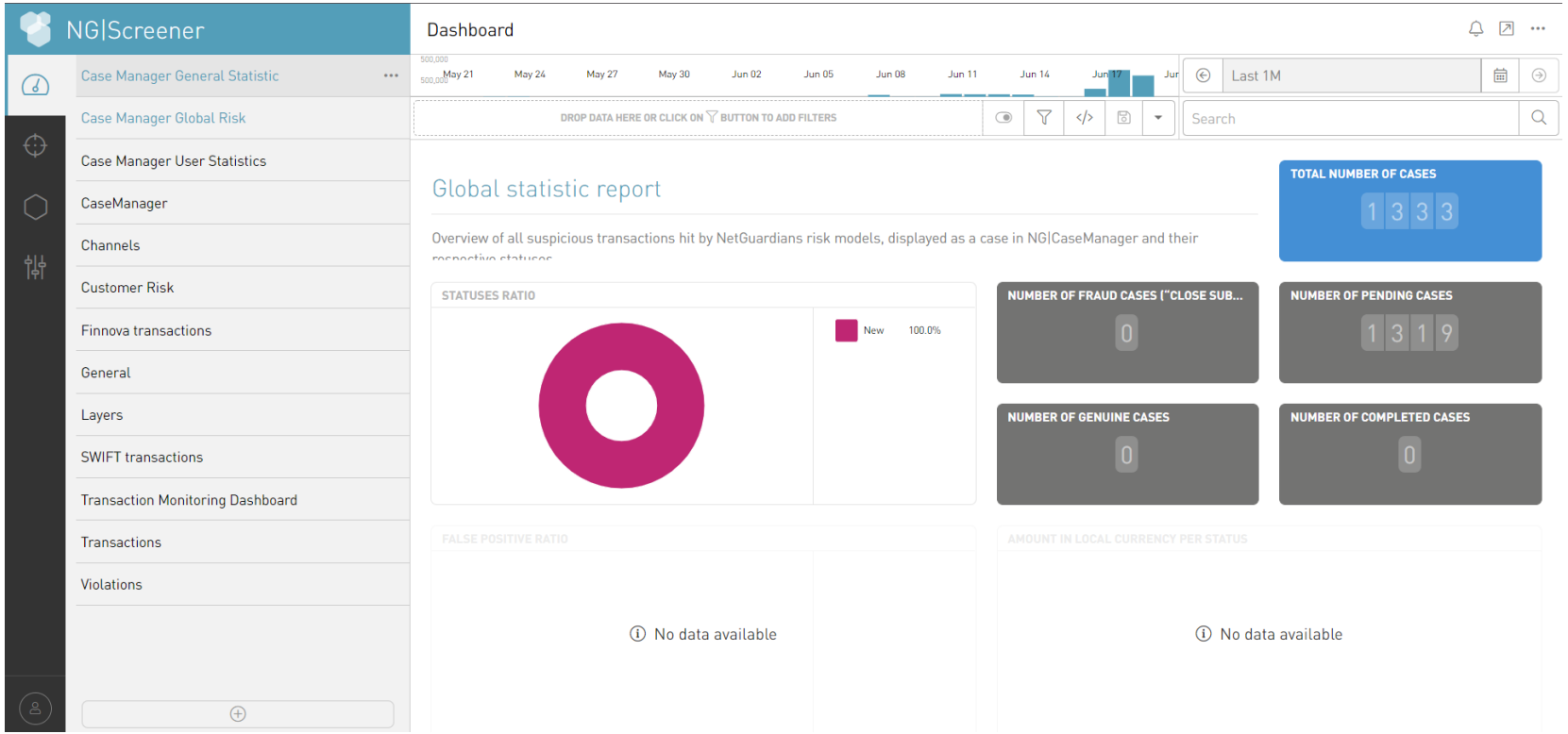
- With any Internet Browser fulfilling minimum version requirement
- https://HOSTNAME_OF_NG/
- Default Credentials
  - User: admin
  - Password: netguardians

Login Screen

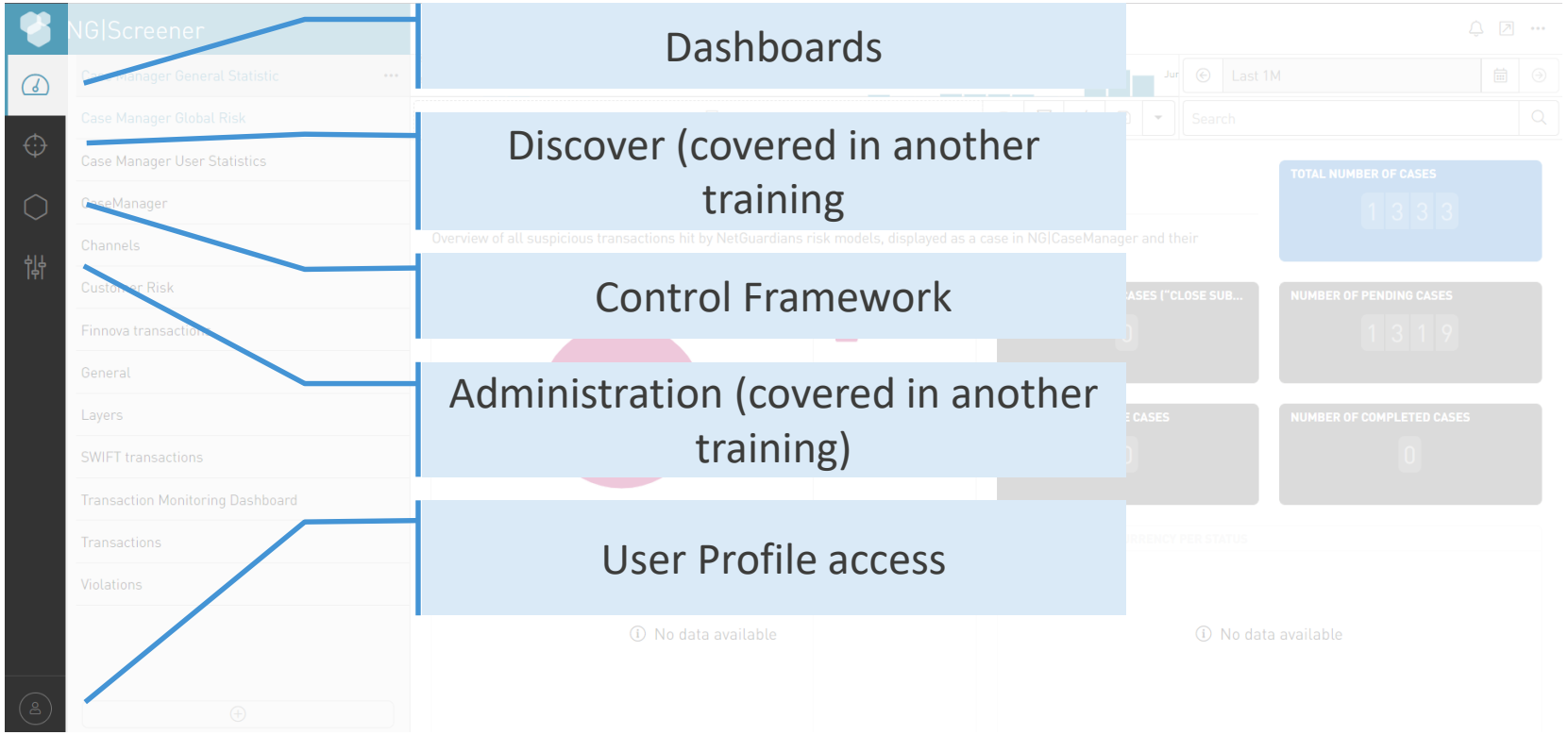
- Single Sign-on functionality through NG|Auth
  - NG|Screener UI
  - Case Manager
- With default URL, connection to NG|Screener UI
- https://HOSTNAME_OF_NG/cm/
  - For connection on Case Manager



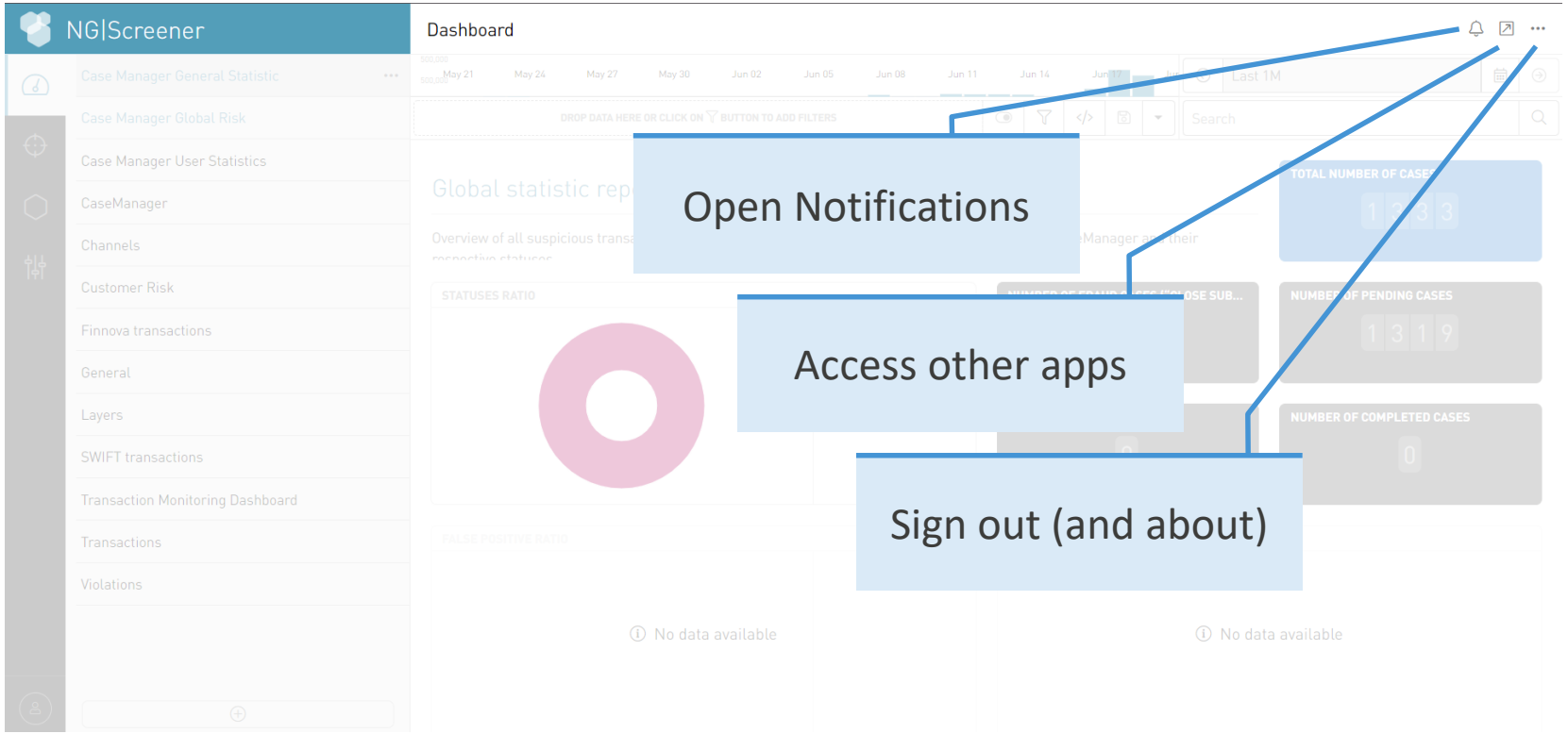
Main Window



Main Window



Main Window



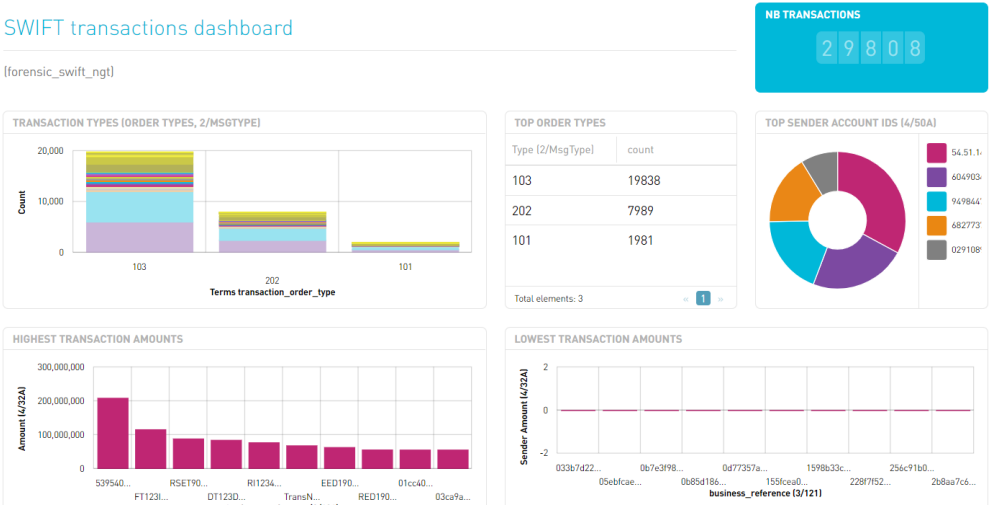
NetGuardians

Dashboards

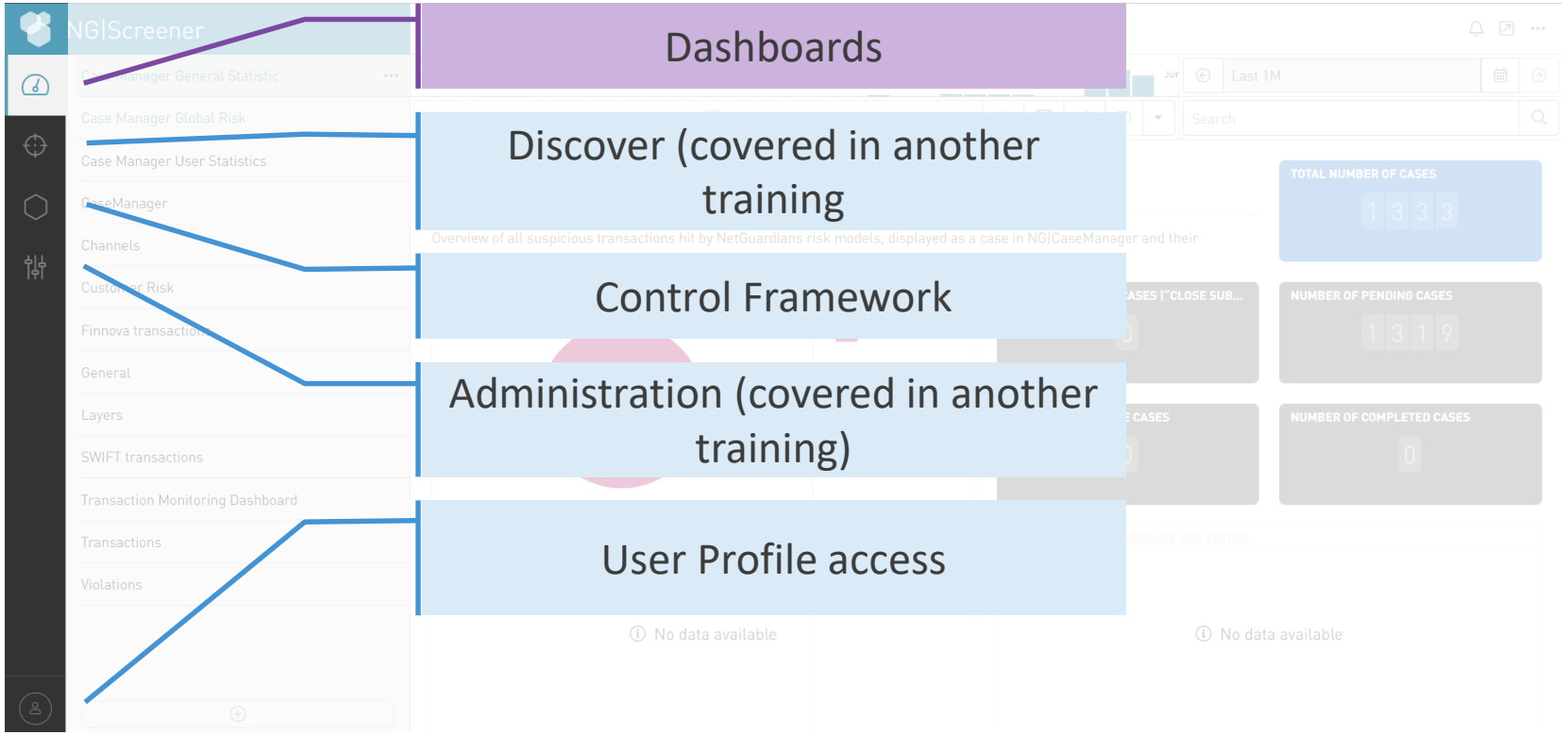
swiss made software

Dashboards

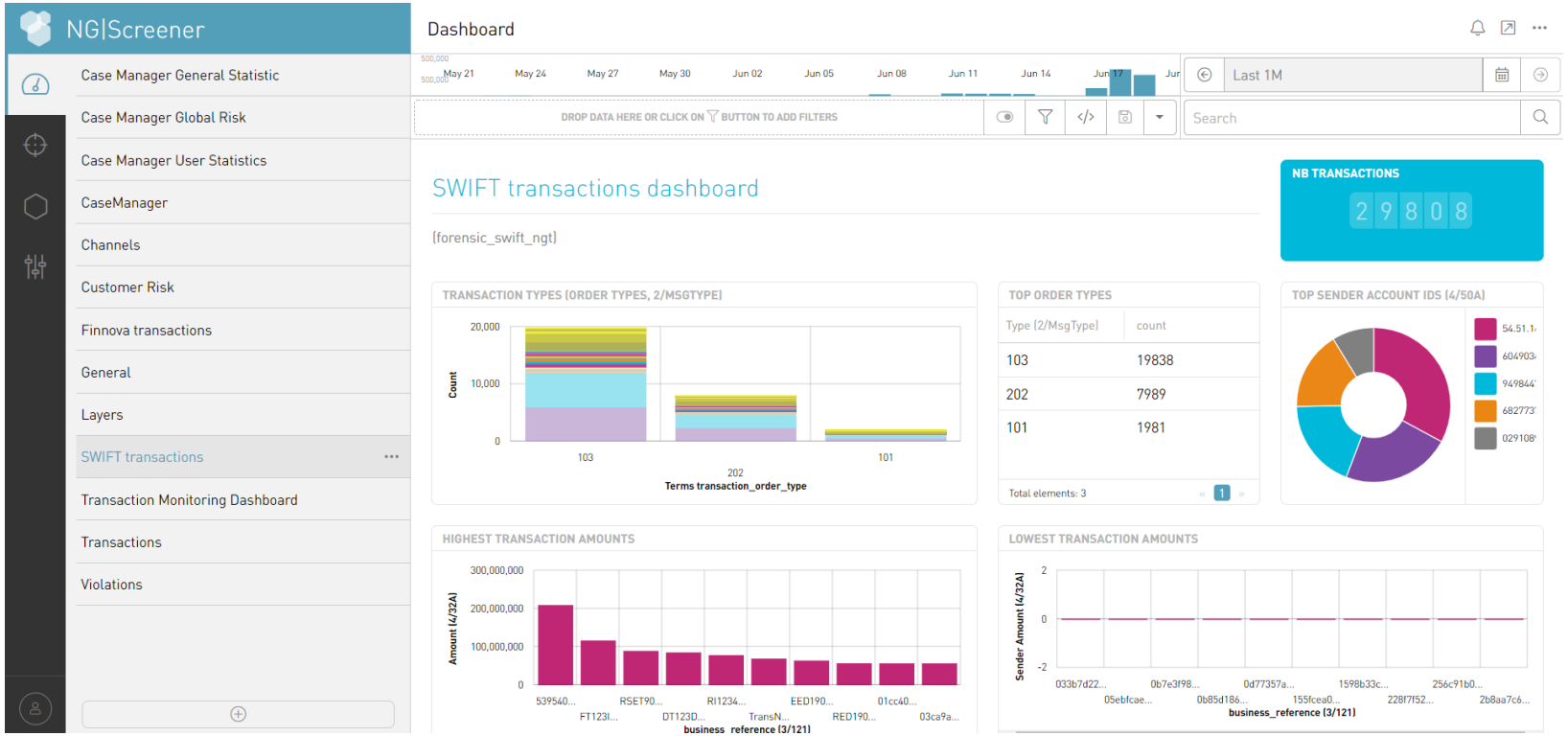
- Different kind of data
  - Either aggregated data out of controls
  - Or raw data ingested into the solution
- Composed of click-able visualizations
- Filtering on multiple dimensions
  - Source user
  - Time
  - …



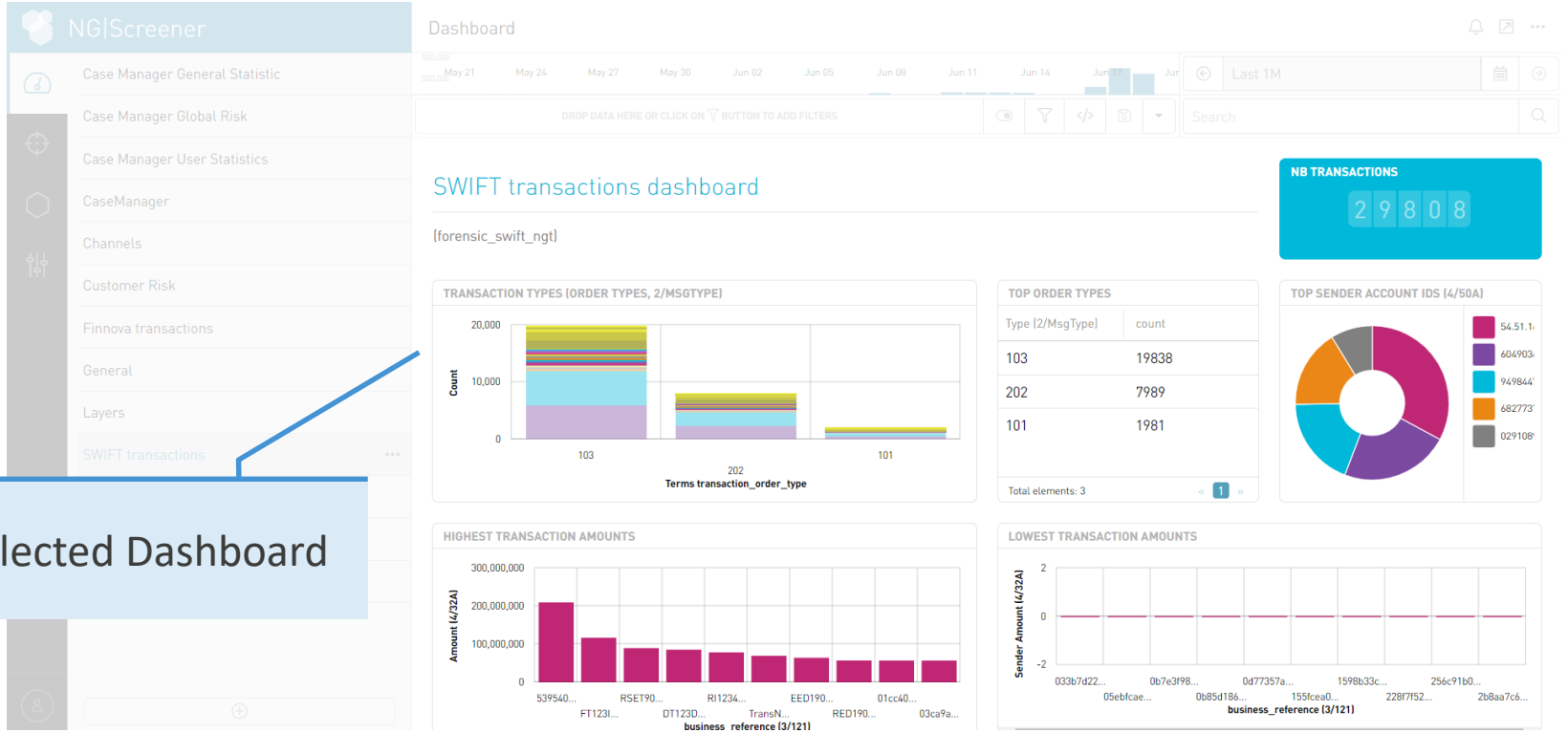
Access Dashboards



Dashboard view

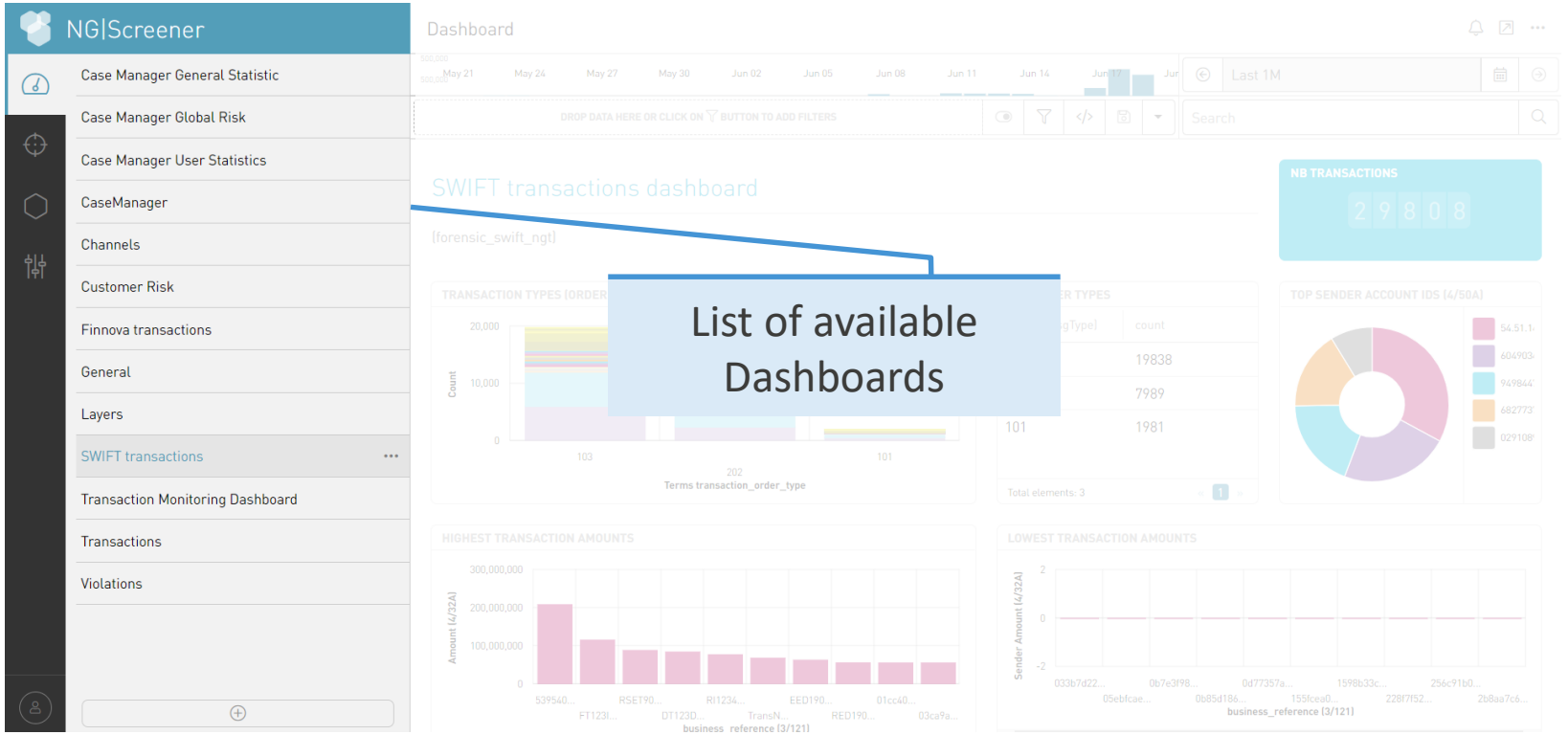


Dashboard view

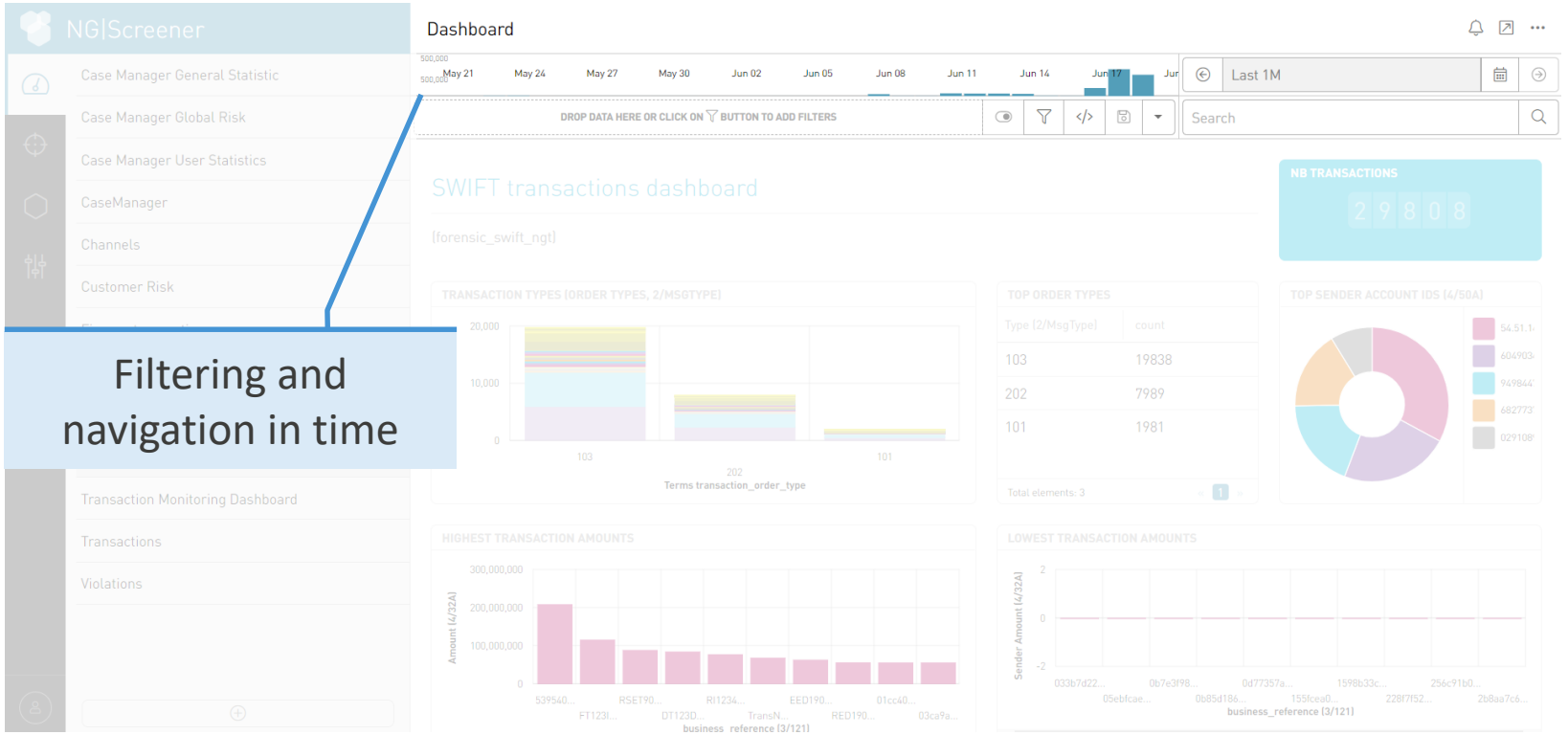


Selected Dashboard

Dashboard view



Dashboard view

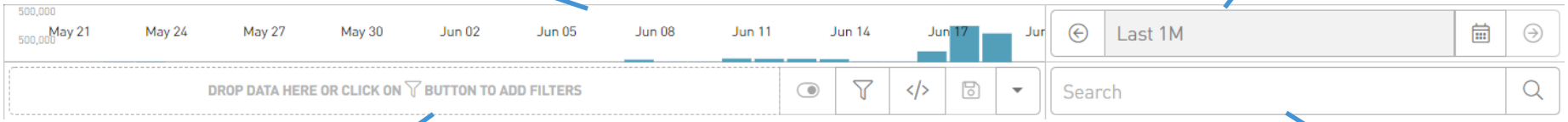


Filtering and navigation in time

Filtering and navigating in time

Events distribution in time. Selection by click and slide

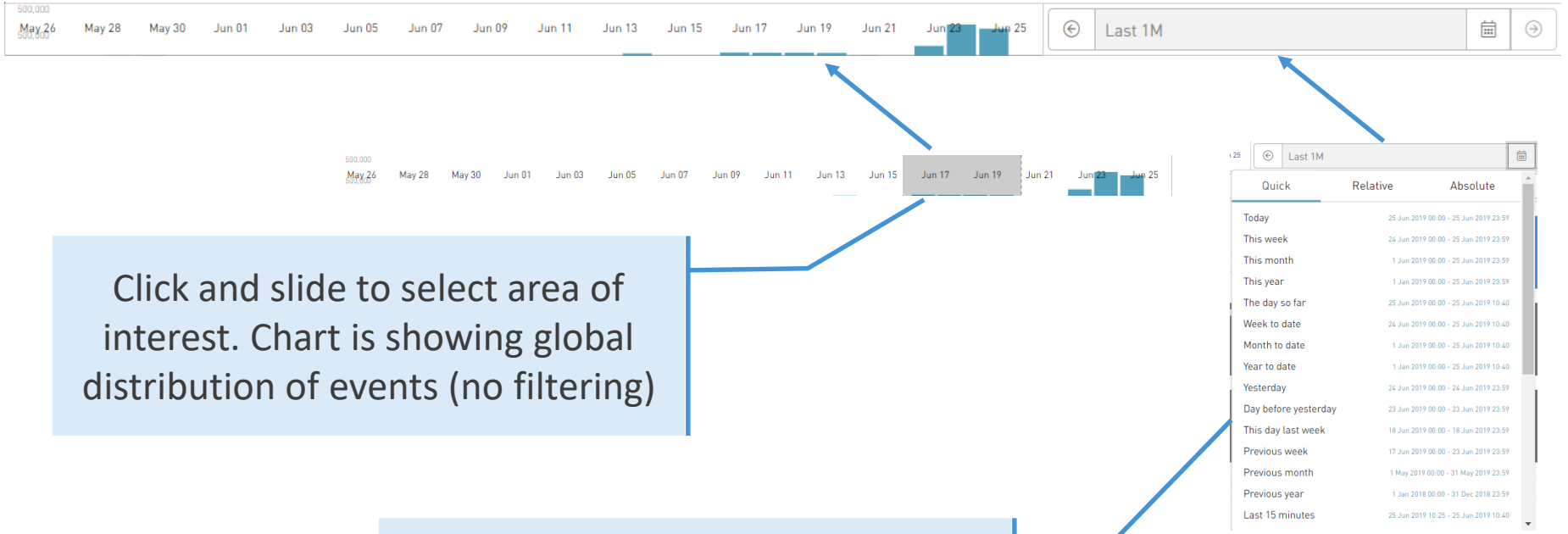
Timeframe selection



Filtering area

Full text search (non-persistent)

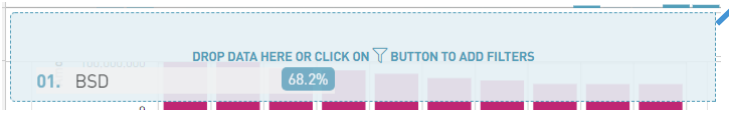
Navigating in time



Click and slide to select area of interest. Chart is showing global distribution of events (no filtering)

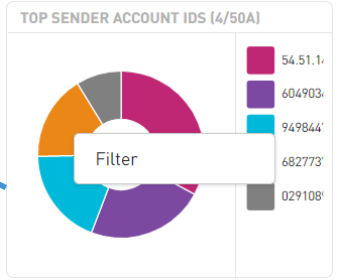
Quick, Relative or absolute timeframes to be selected

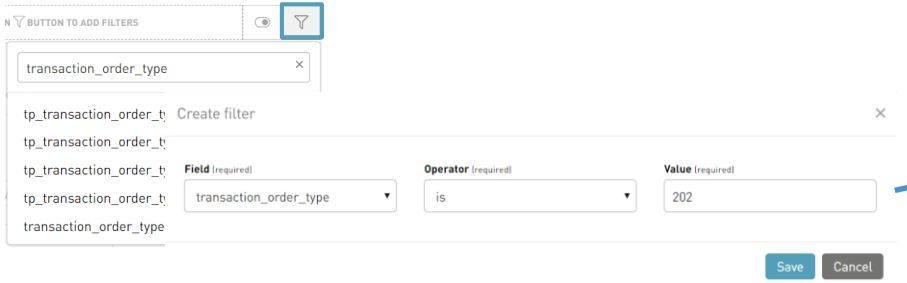
Filters could be added by (simple)



Dropping data into filtering area

Selecting filters from visualizations





Selecting “funnel” then creating filter

Filters could be added by (advanced)

Full text search (non persistent)

Editing filter code

Advanced Filtering

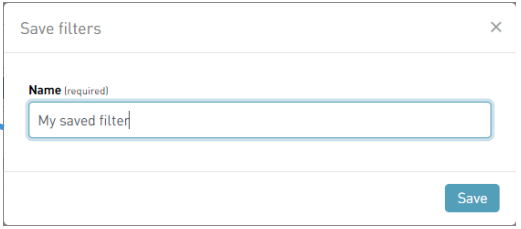
- Possible to use wildcards * or ?
  - Not in quotes
  - Example: source_user:JA* and not source_user:«JA*»
- Check existance of a field: *_exist_:myfield or query_missing_:myfield*
- Numeric values greater or smaller than: *amount:<500*
  - Works with <, >, <= and >=
- Value in range: *amount:[100 TO 200]*
- AND and OR operators can be used
  - Always in capital letters

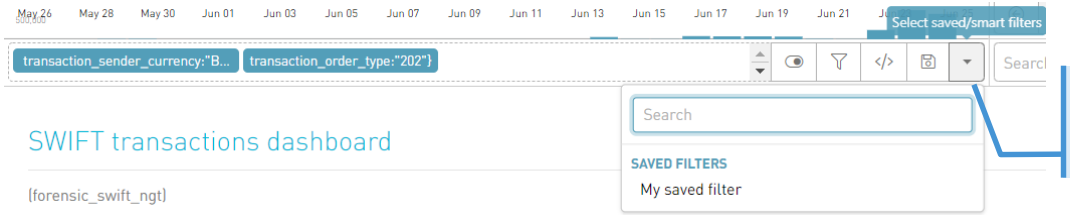
Saving Filters

1. Compose your filter

2. Floppy Disk to save

3. Save filters with specific name





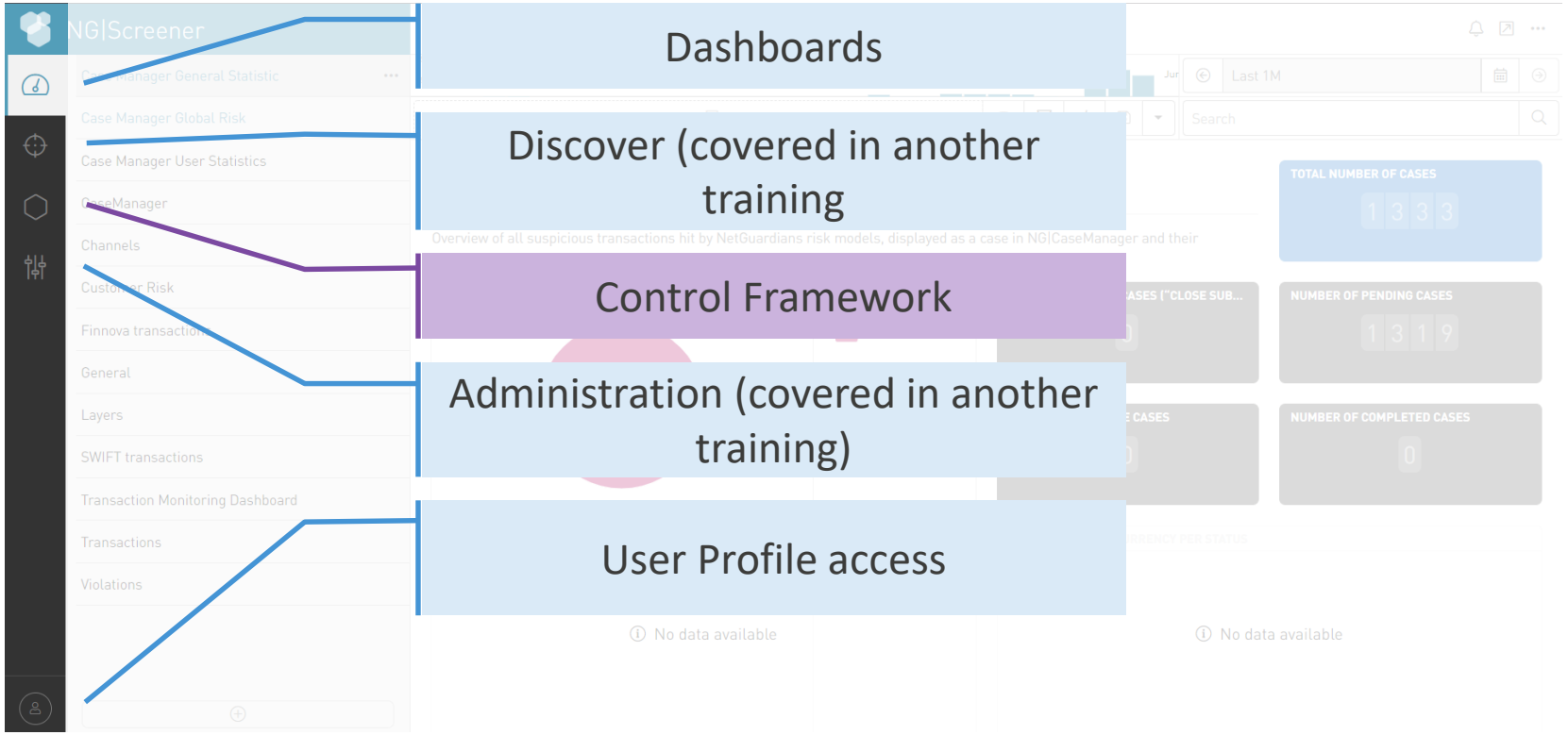
4. Saved filters will appear here

NetGuardians

Controls

swiss made software

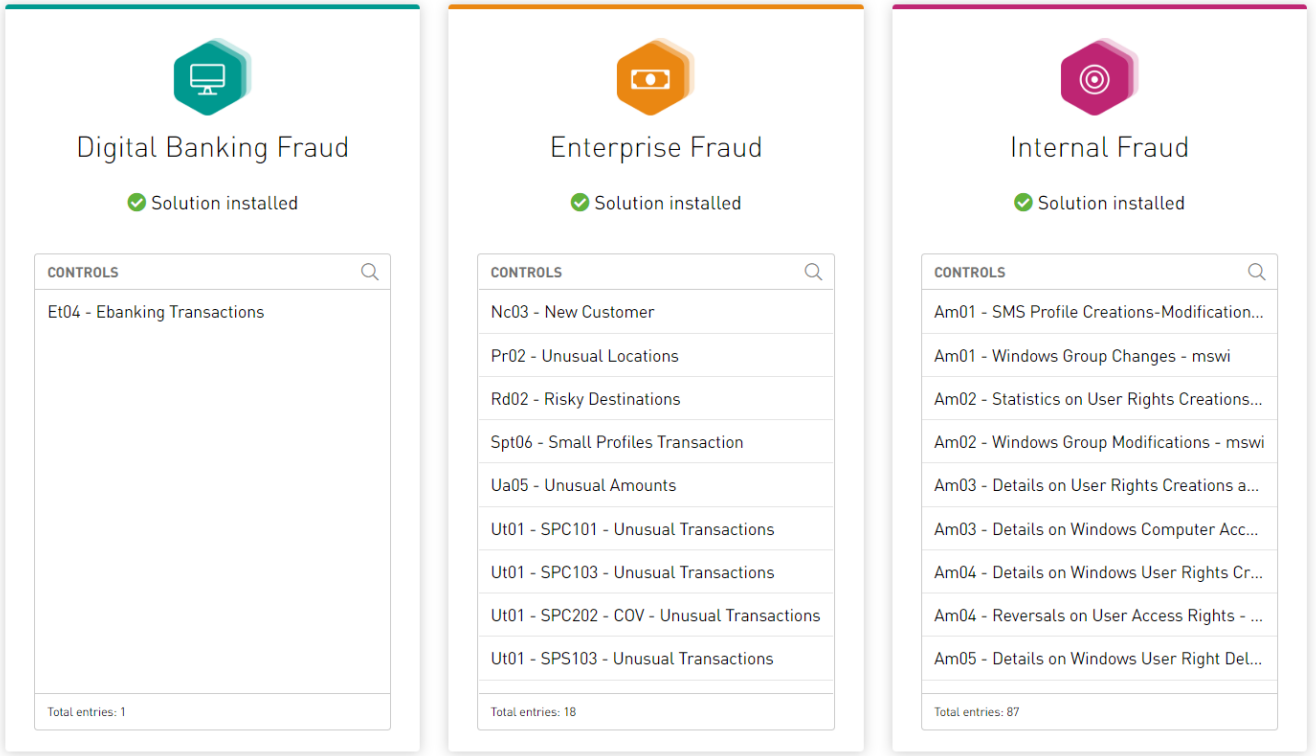
Access Controls Framework



Control Framework

- Objectives of control framework are:
  - Group different information in a single document
  - Scheduling of controls for periodic delivery and alerting purpose
  - Controls are grouped into Solutions

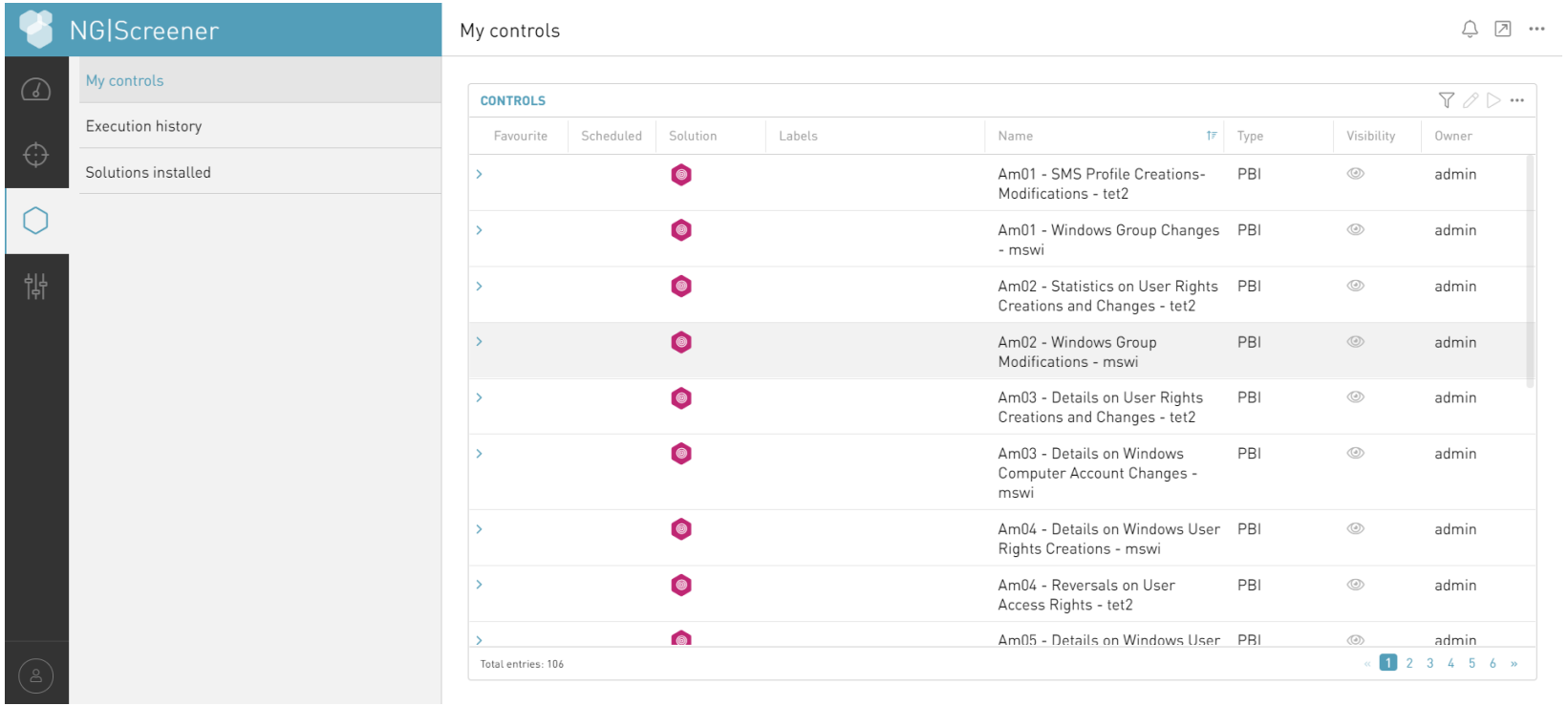
Solutions



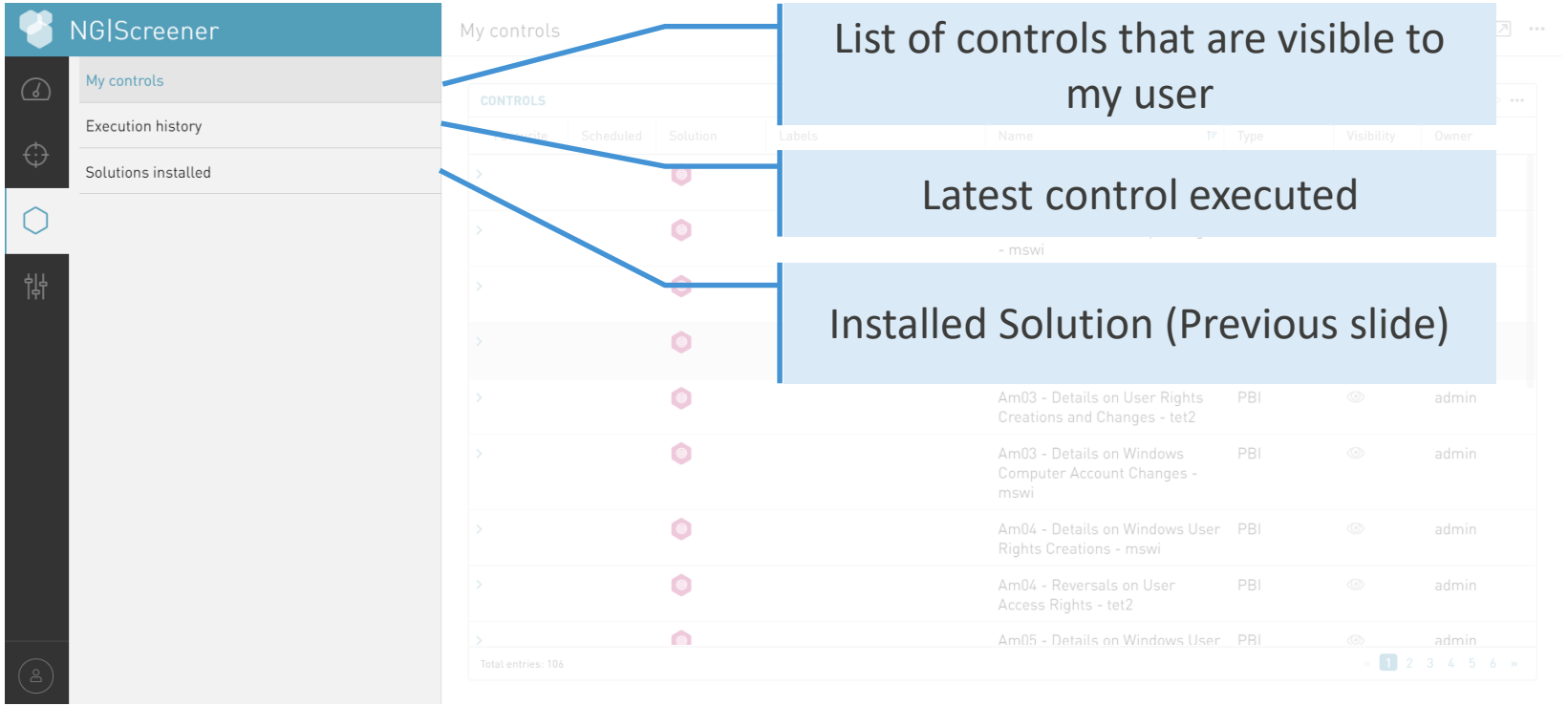
Type of controls

- Type of controls
  - Scheduled
    - Executed periodically
    - Result exported to predefined channels
  - On-demand
    - Execute control once from UI
    - Possible to export results of execution

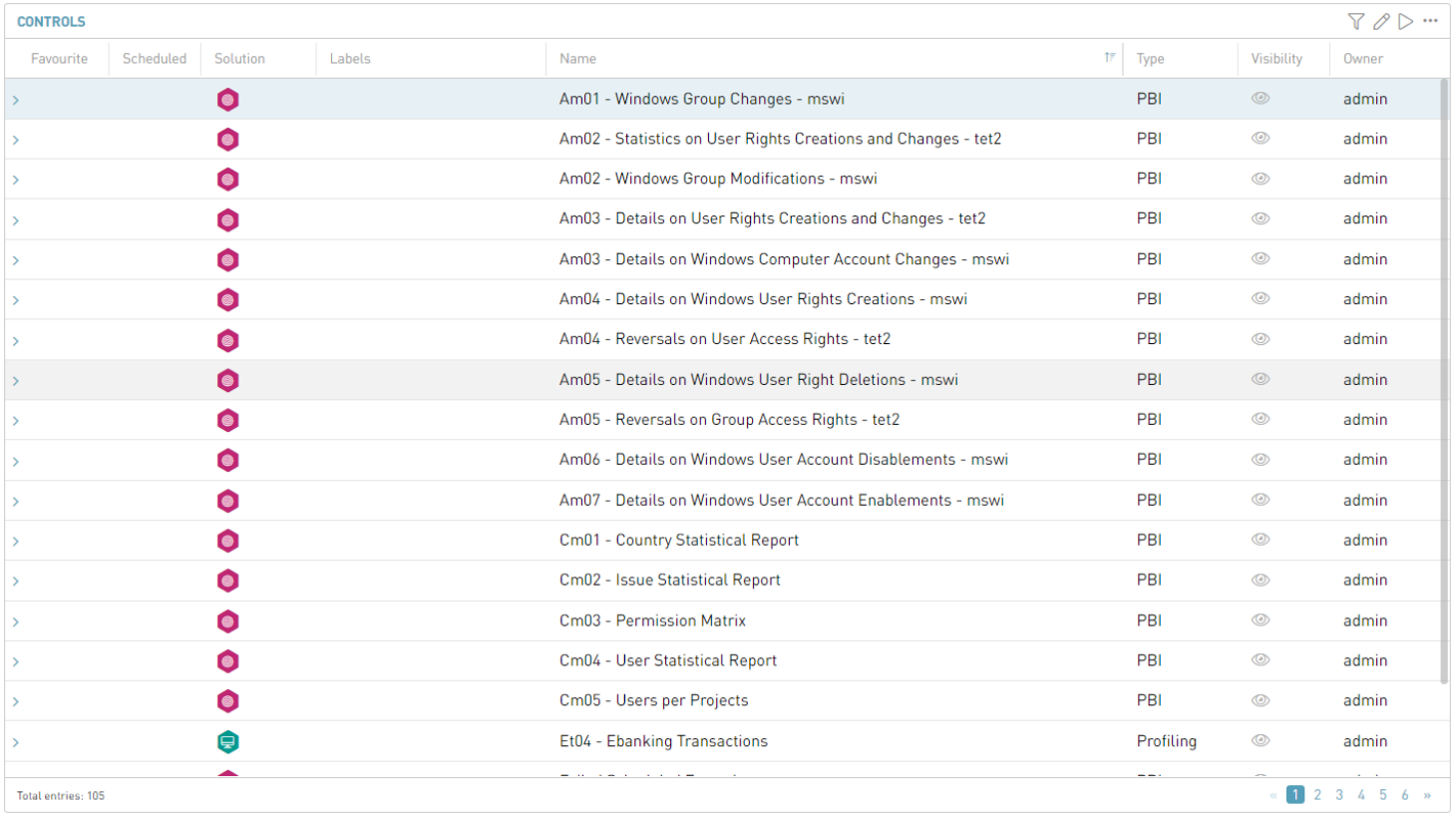
Control Framework view



Control Framework view



My Controls



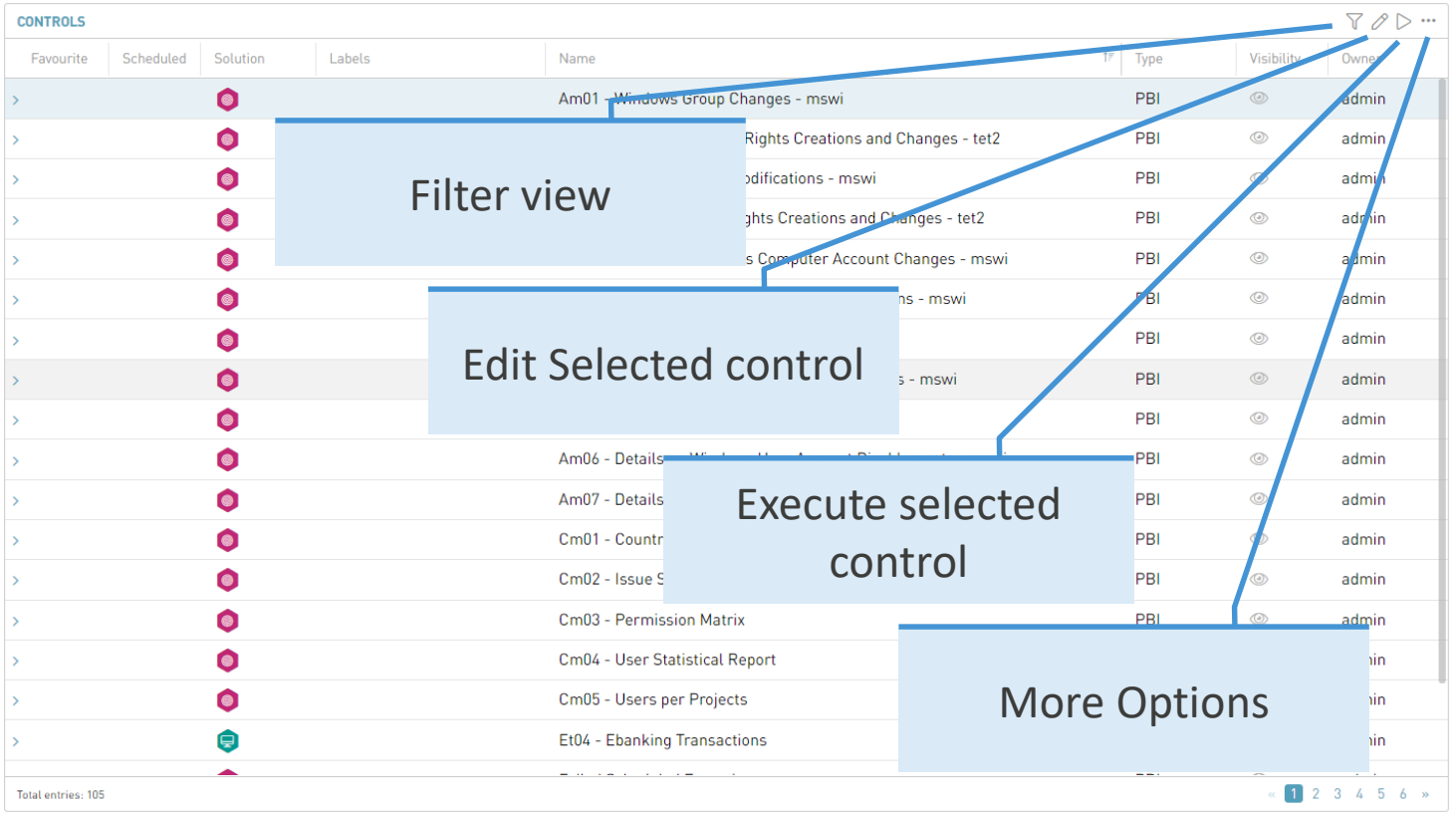
CONTROLS

Favourite	Scheduled	Solution	Labels	Name	Type	Visibility	Owner
				Am01 - Windows Group Changes - mswi	PBI		admin
				Am02 - Statistics on User Rights Creations and Changes - tet2	PBI		admin
				Am02 - Windows Group Modifications - mswi	PBI		admin
				Am03 - Details on User Rights Creations and Changes - tet2	PBI		admin
				Am03 - Details on Windows Computer Account Changes - mswi	PBI		admin
				Am04 - Details on Windows User Rights Creations - mswi	PBI		admin
				Am04 - Reversals on User Access Rights - tet2	PBI		admin
				Am05 - Details on Windows User Right Deletions - mswi	PBI		admin
				Am05 - Reversals on Group Access Rights - tet2	PBI		admin
				Am06 - Details on Windows User Account Disablements - mswi	PBI		admin
				Am07 - Details on Windows User Account Enablements - mswi	PBI		admin
				Cm01 - Country Statistical Report	PBI		admin
				Cm02 - Issue Statistical Report	PBI		admin
				Cm03 - Permission Matrix	PBI		admin
				Cm04 - User Statistical Report	PBI		admin
				Cm05 - Users per Projects	PBI		admin
				Et04 - Ebanking Transactions	Profiling		admin

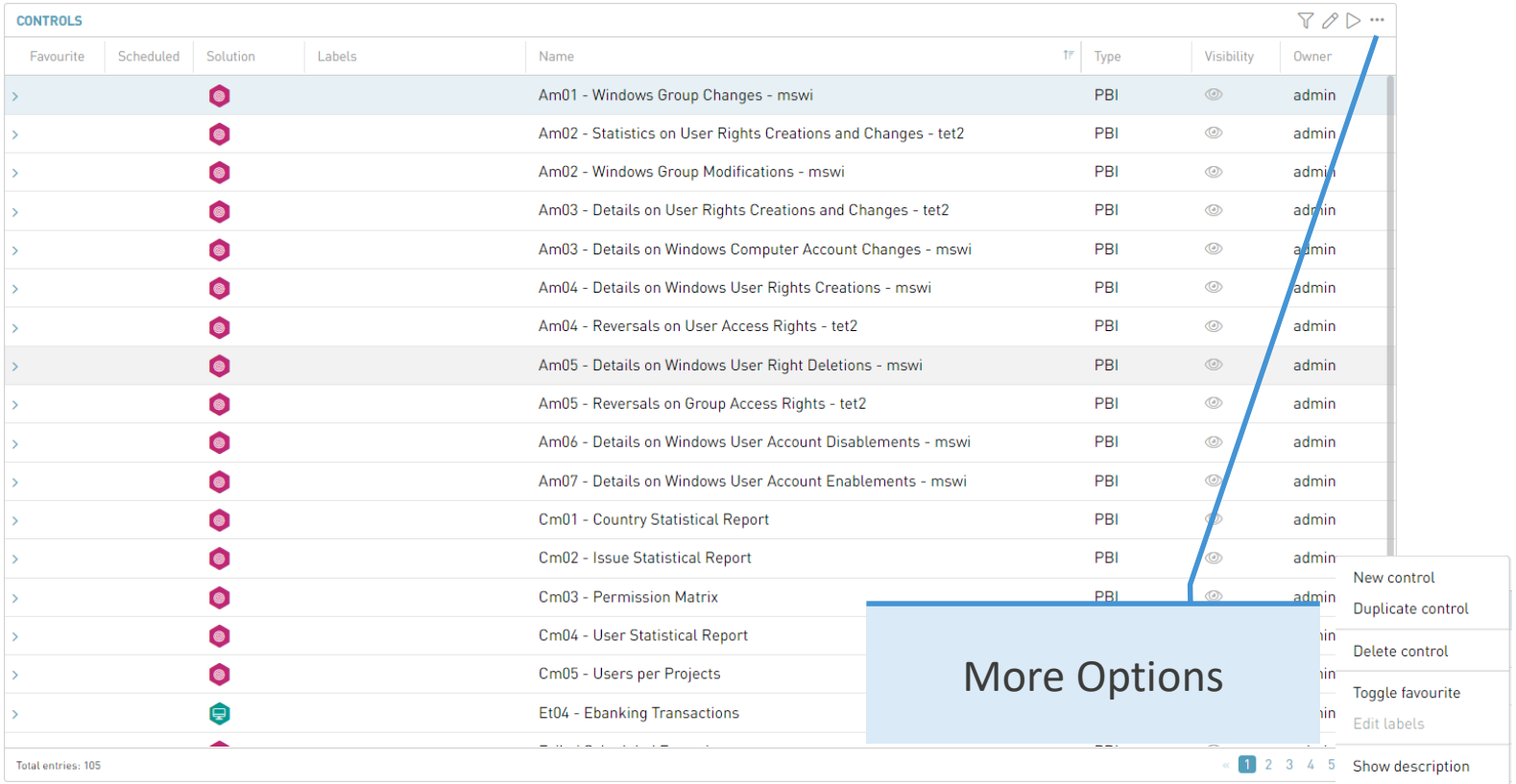
Total entries: 105

« 1 2 3 4 5 6 »

My Controls

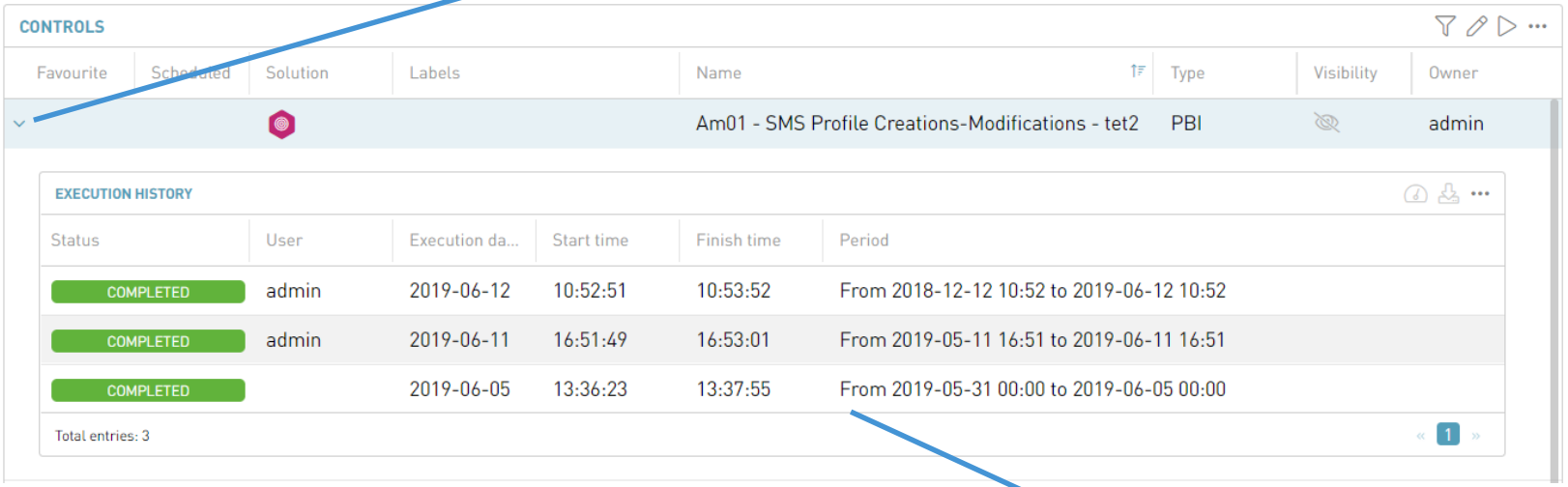


My Controls



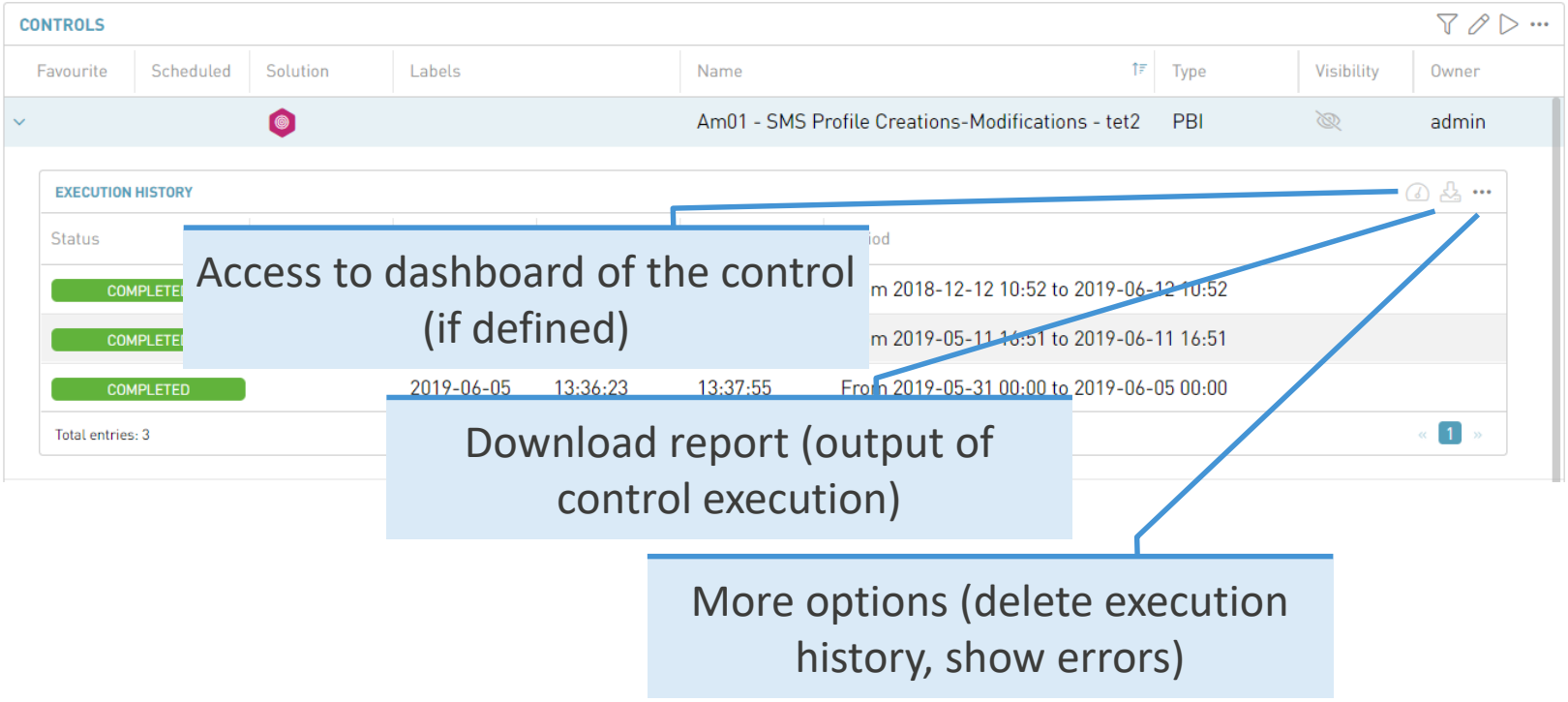
My Controls

Extend to see …



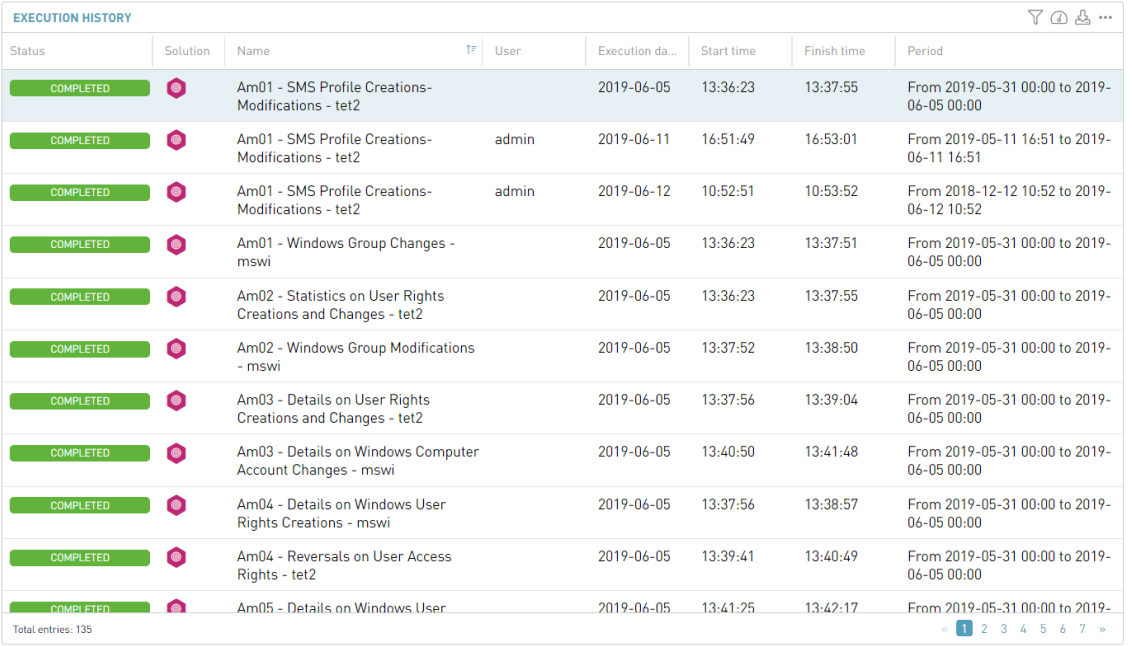
… Execution history for the control

My Controls

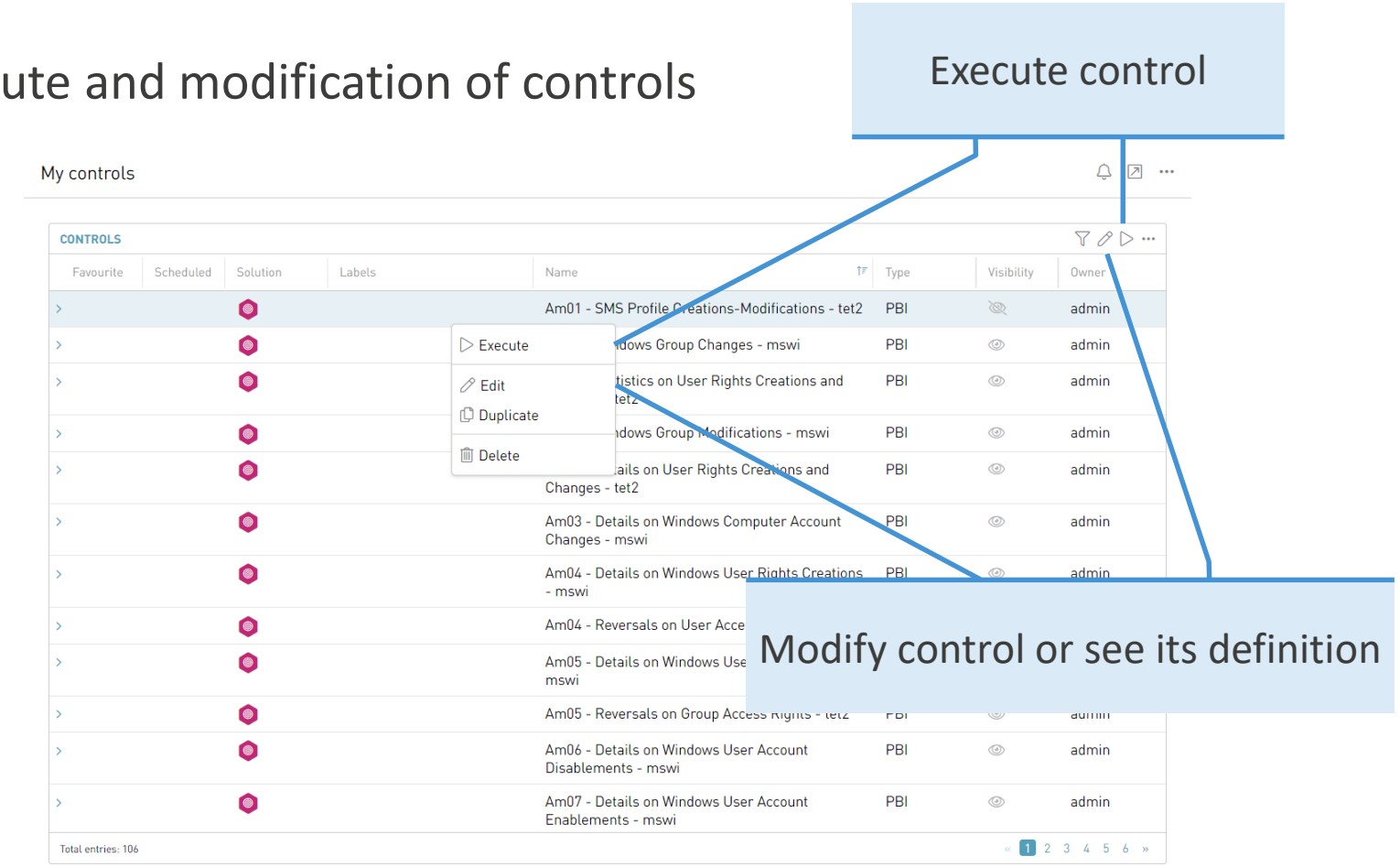


Execution history

- Same as execution history for control
- Global for the whole application
- Same options as per controls
  - Dashboard
  - Report
  - …

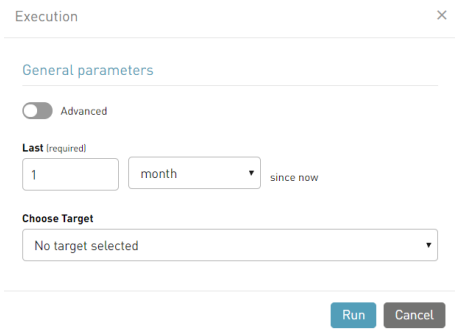


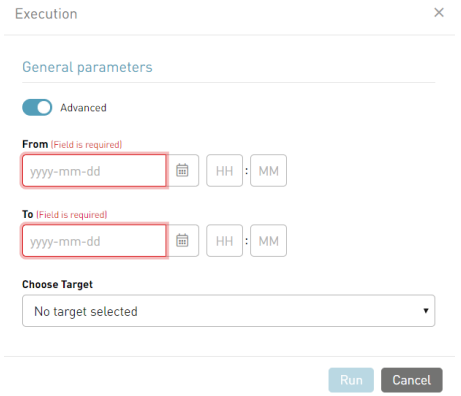
Execute and modification of controls



Execute control

- On-demand control execution
- Specify timeframe
  - Advanced to specify start and end date/time
- Define target for export
  - If no target select, control output will be only available in execution history

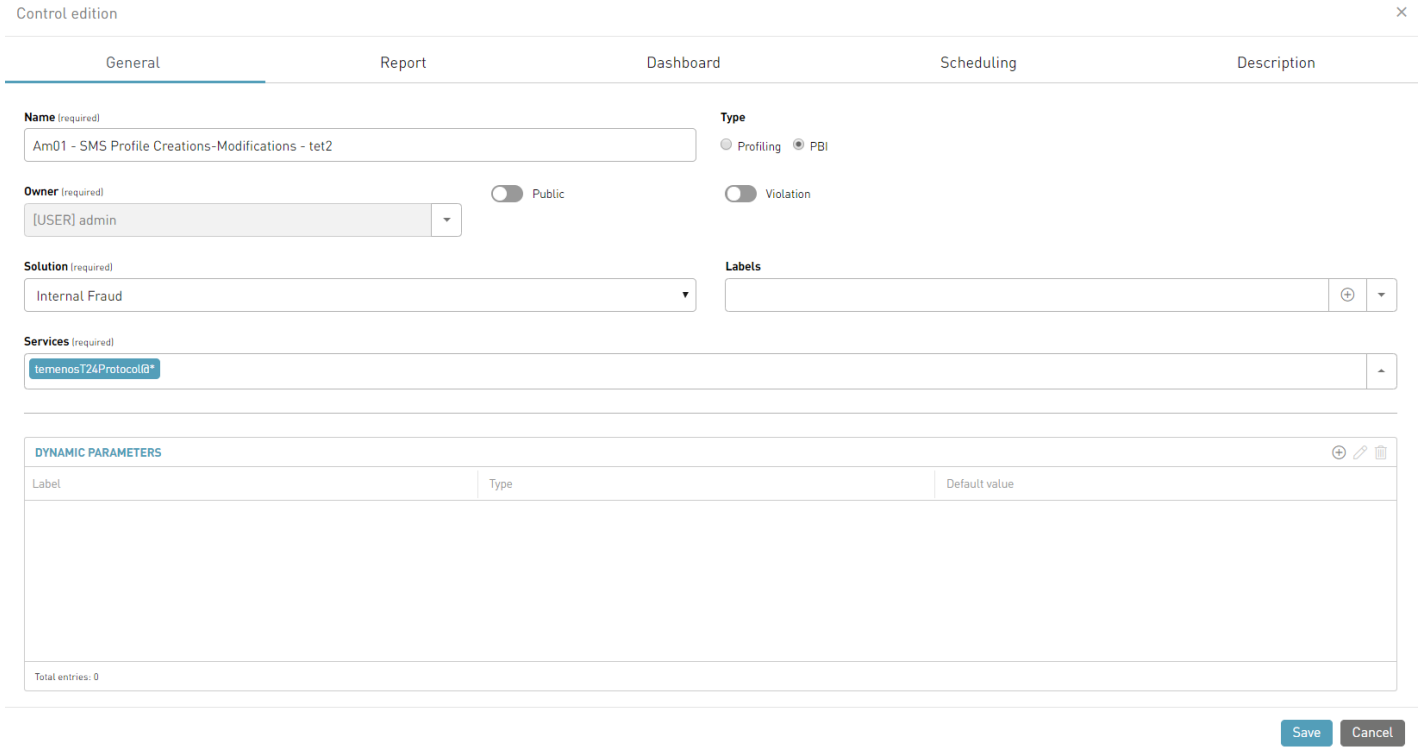




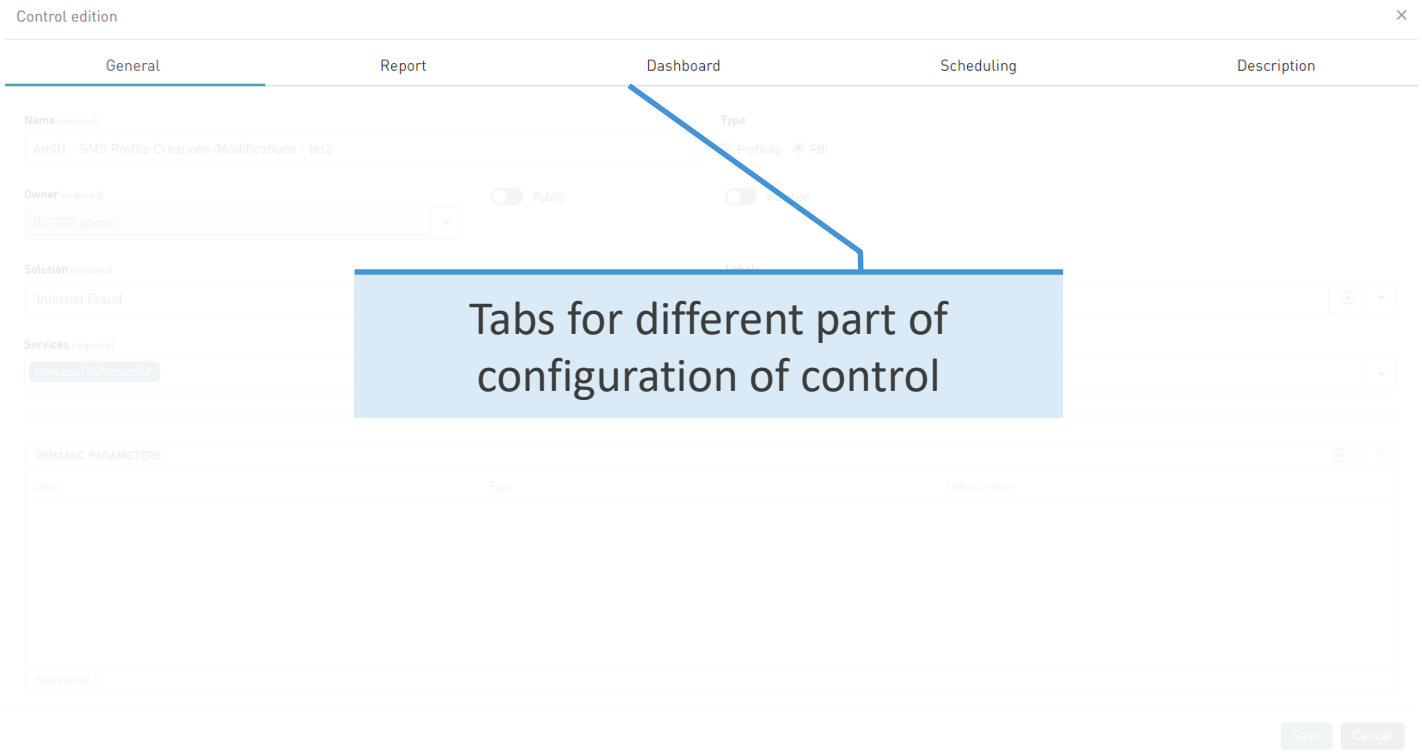
Modify control

- Only a preview of control modification
- More in detail in specific Control definition slides

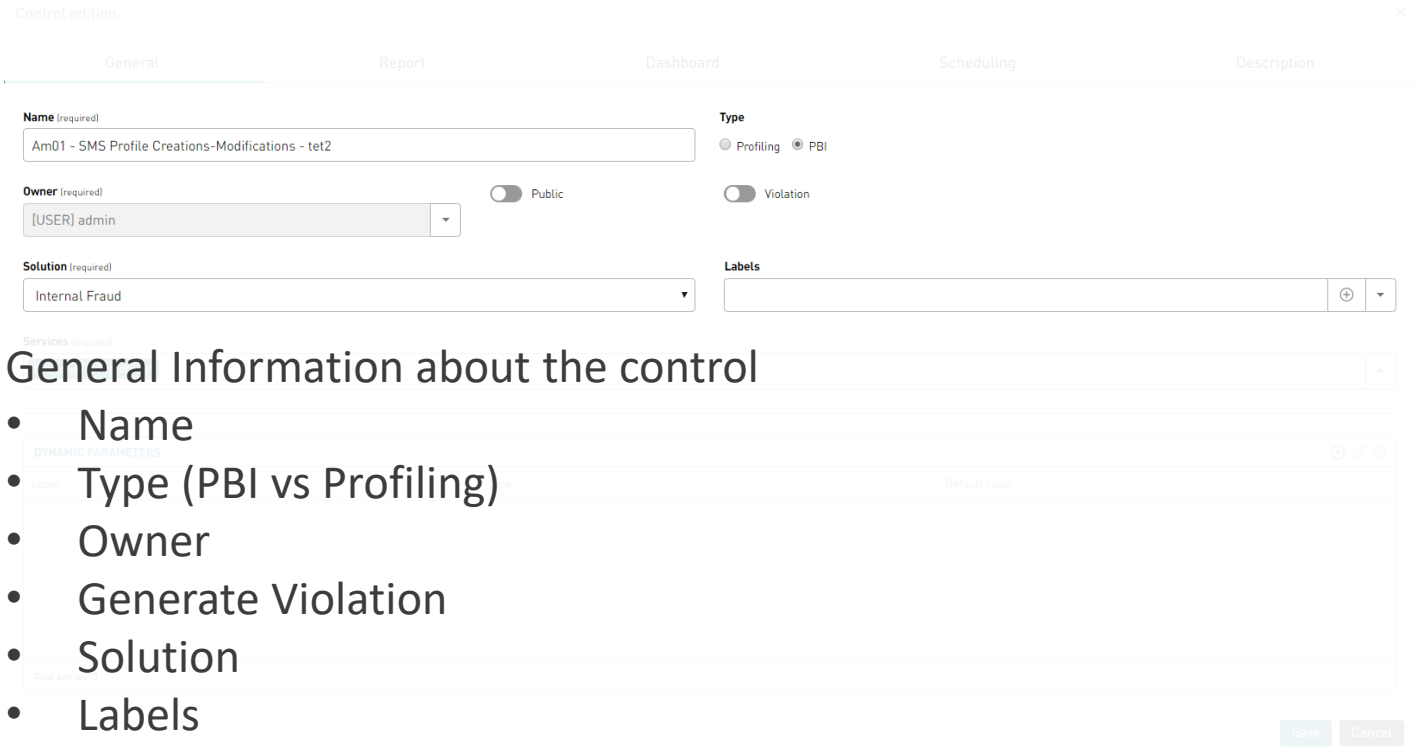
Modify control



Modify control



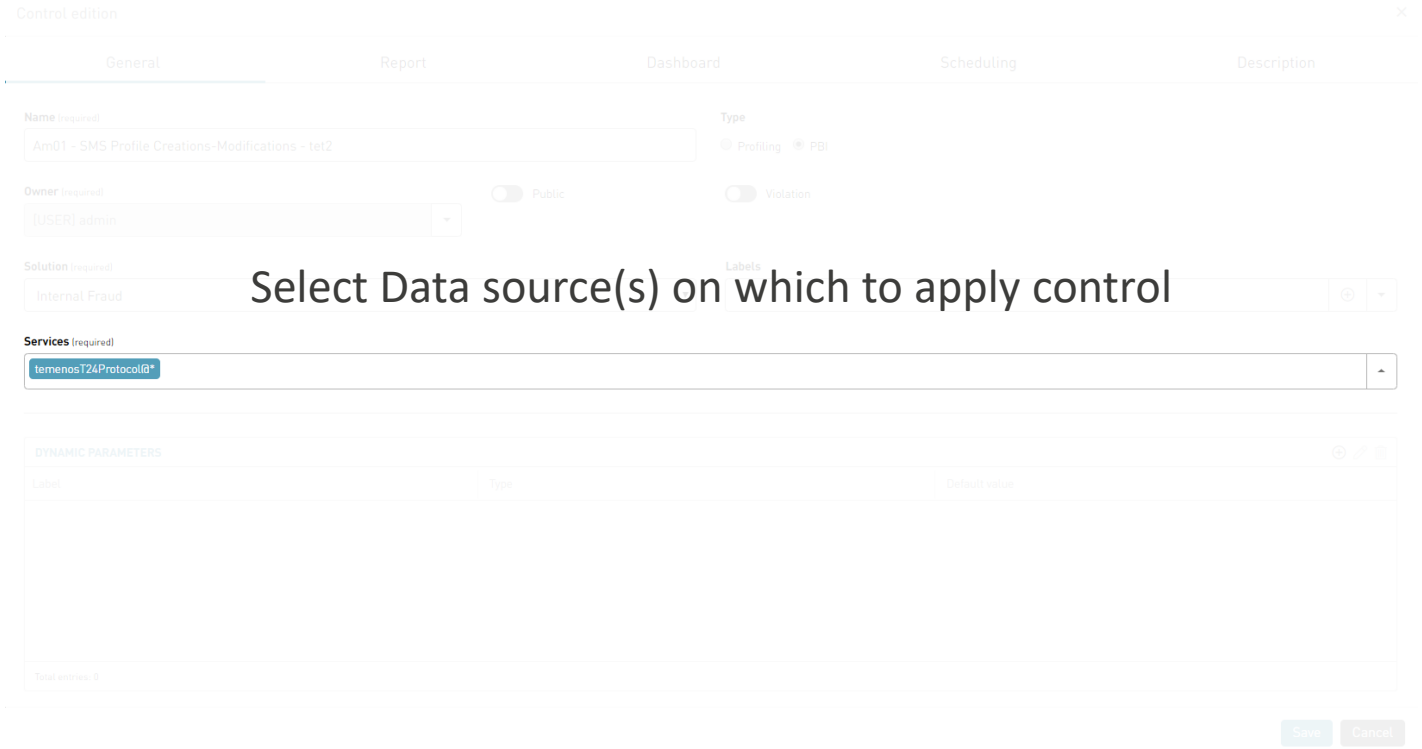
Modify control - General



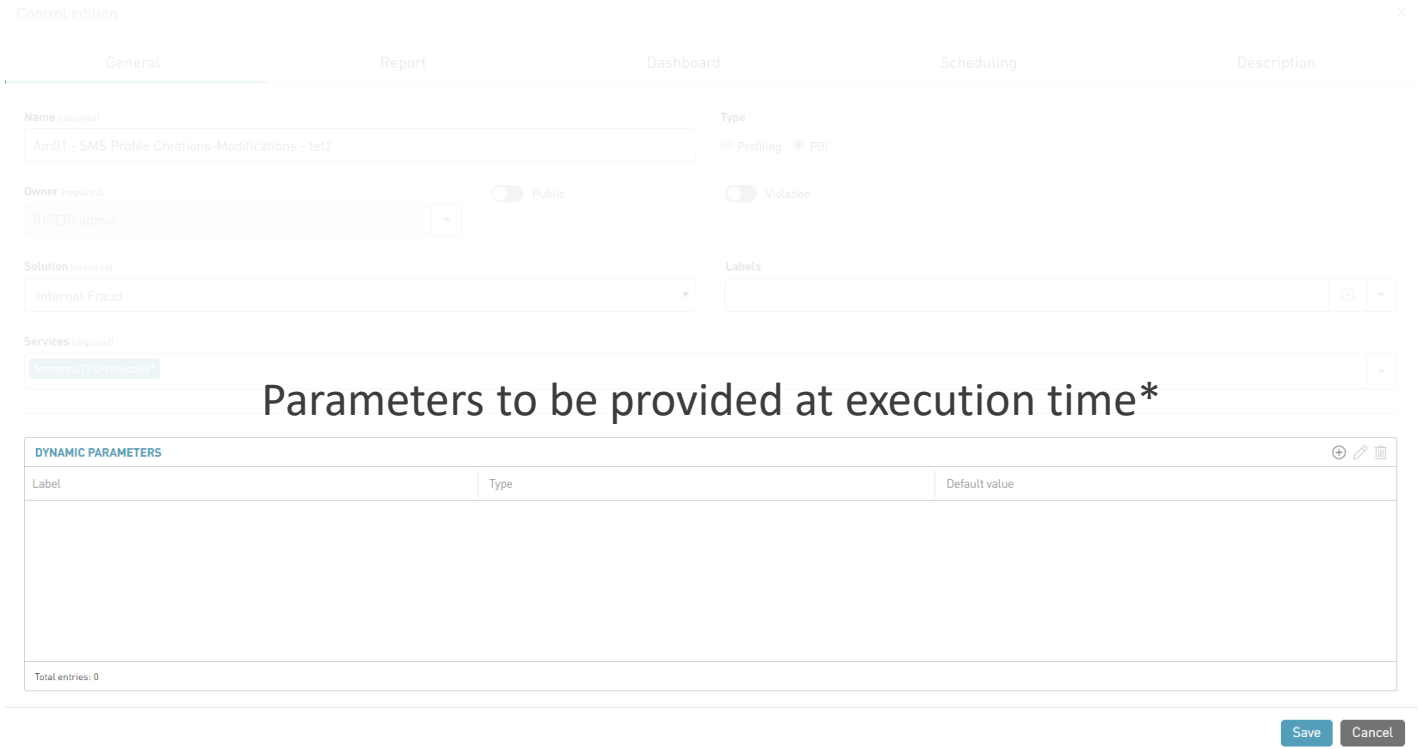
General Information about the control

- Name
- Type (PBI vs Profiling)
- Owner
- Generate Violation
- Solution
- Labels

Modify control - General

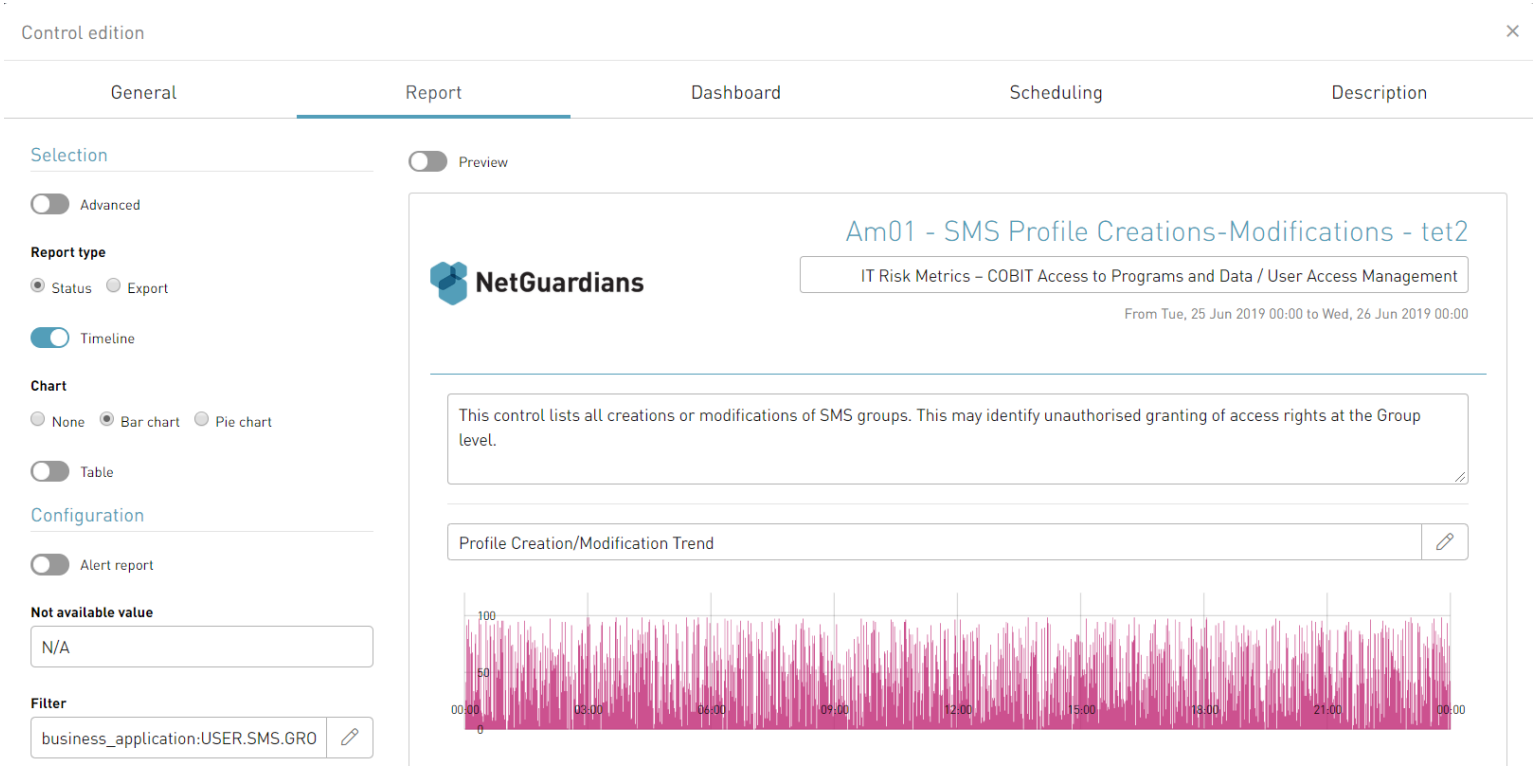


Modify control - General

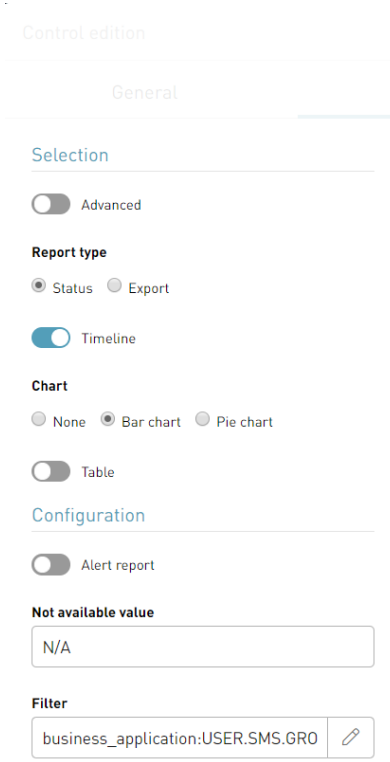


*More info in Control Creation slides

Modify control – Report (Simple)



Modify control – Report (Simple)



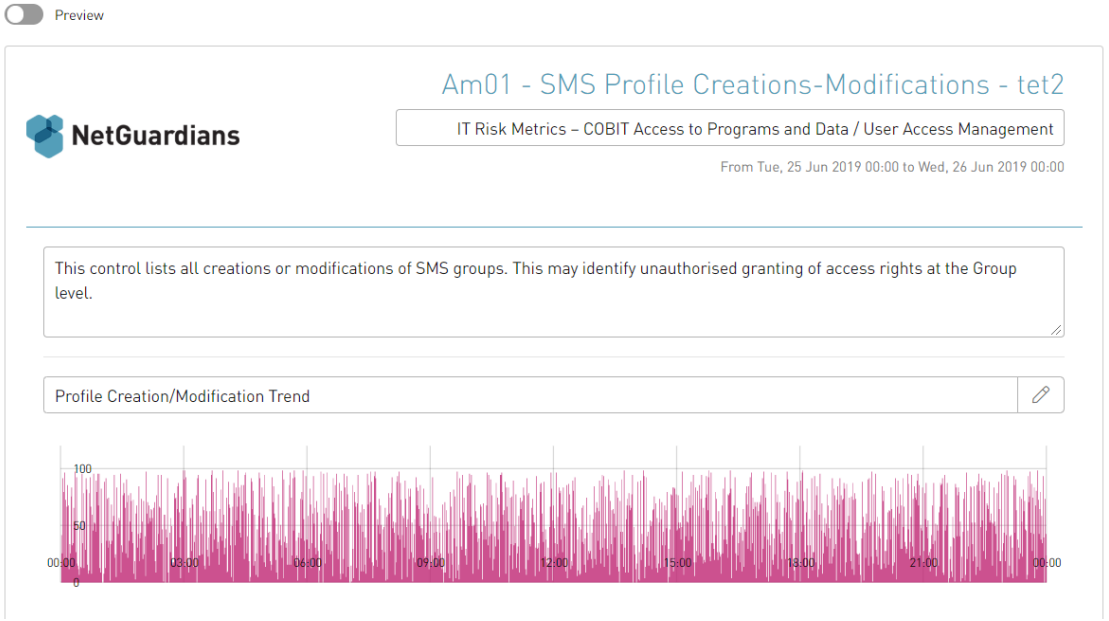
General configuration of the report

- Simple or advanced
- Status (PDF) or Export (CSV)
- Chart elements to be included
- Alert Report (generate report if no data highlighted)
- Value to be provided if null
- Filter (rules) to be applied on the control (PBI)

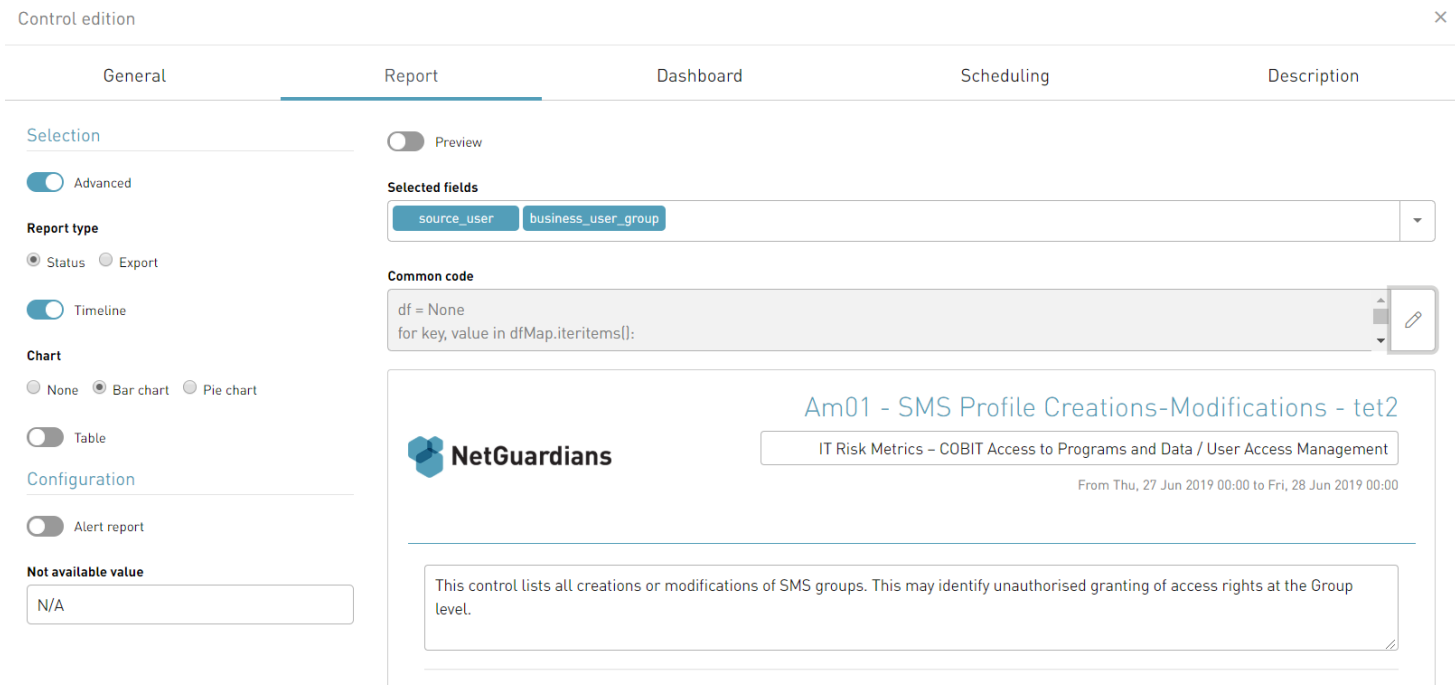
Modify control – Report (Simple)

Presentation and component configuration

- Description and subtitle
- Chart component configuration



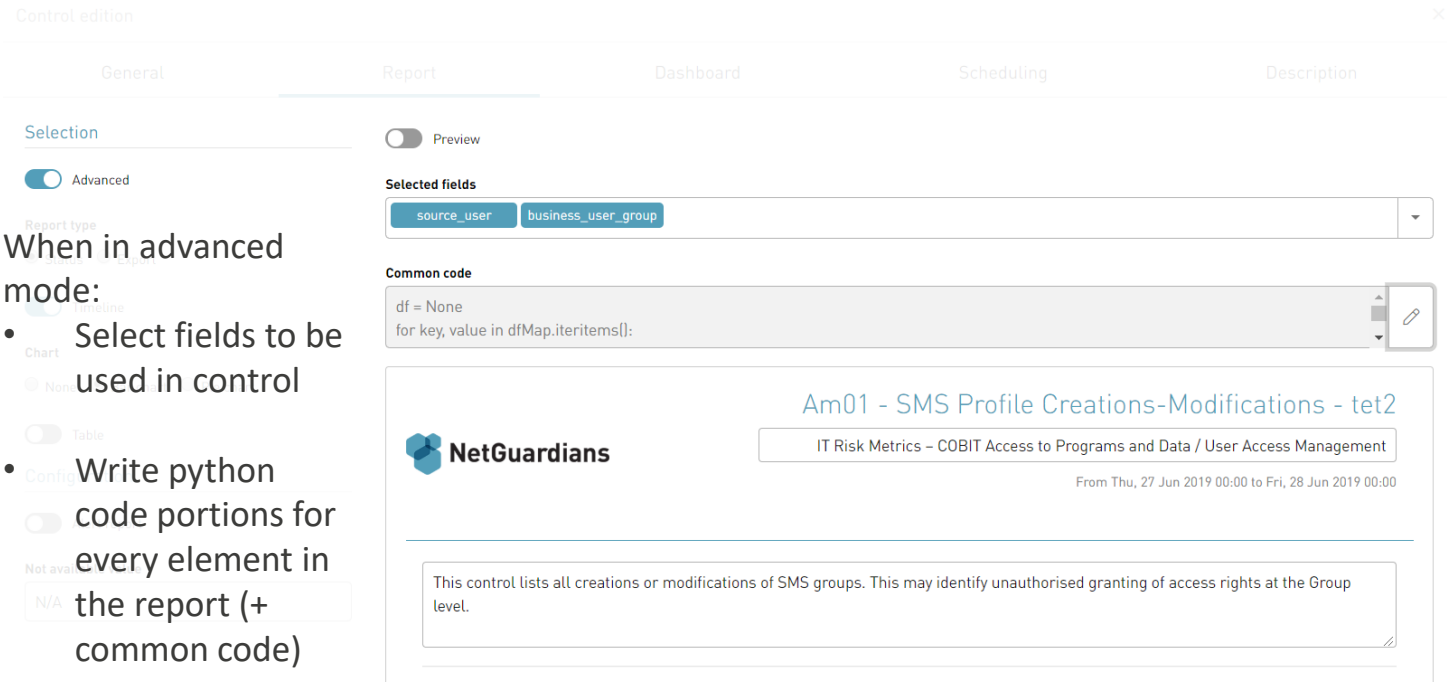
Modify control – Report (Advanced)



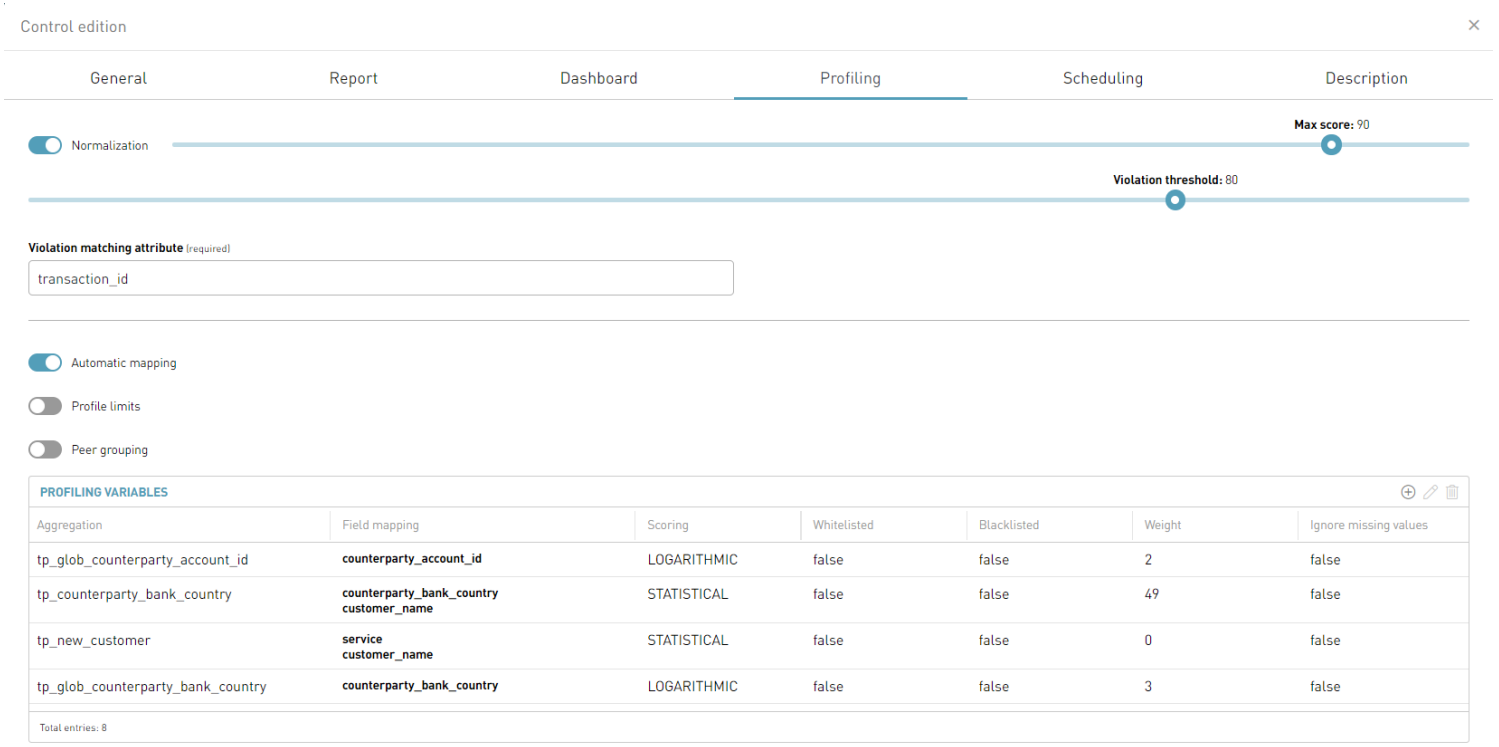
Modify control – Report (Advanced)

When in advanced mode:

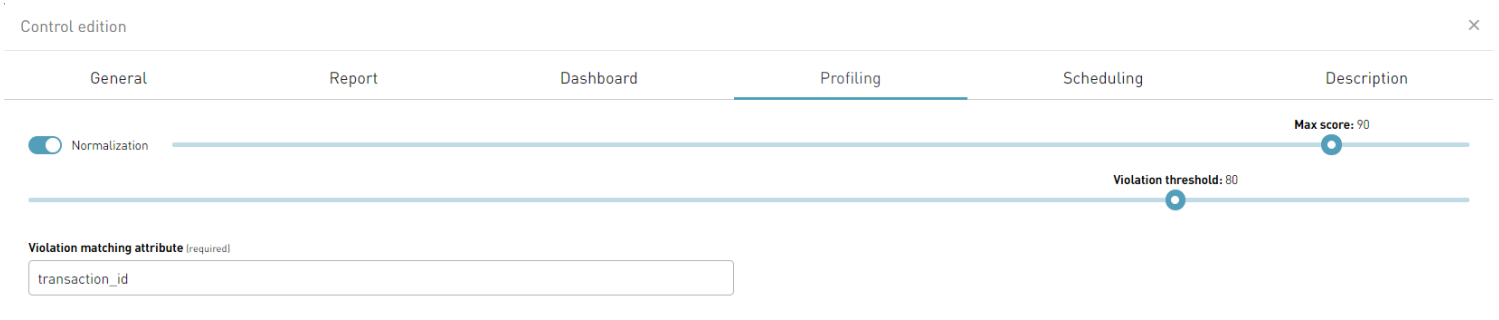
- Select fields to be used in control
- Write python code portions for every element in the report (+ common code)



Modify control – Report (Profiling)



Modify control – Report (Profiling)



General profiling options:

- Normalization: normalize score to have Max score defined = 100
  - In this case, everything above 90 will be equal to 100
- Violation threshold: Score above which event will be flagged
- Violation matching attribute: Field that will define an identifier for the event
- Other options will be seen in Profiling slides

Modify control – Report (Profiling)

Profiling Variables:

- Aggregations to be used to score transaction
  - Dimensions
  - Variable
  - Weight
- Artificial Variables
  - Scores coming directly from the data (no inner computation) or from external sources

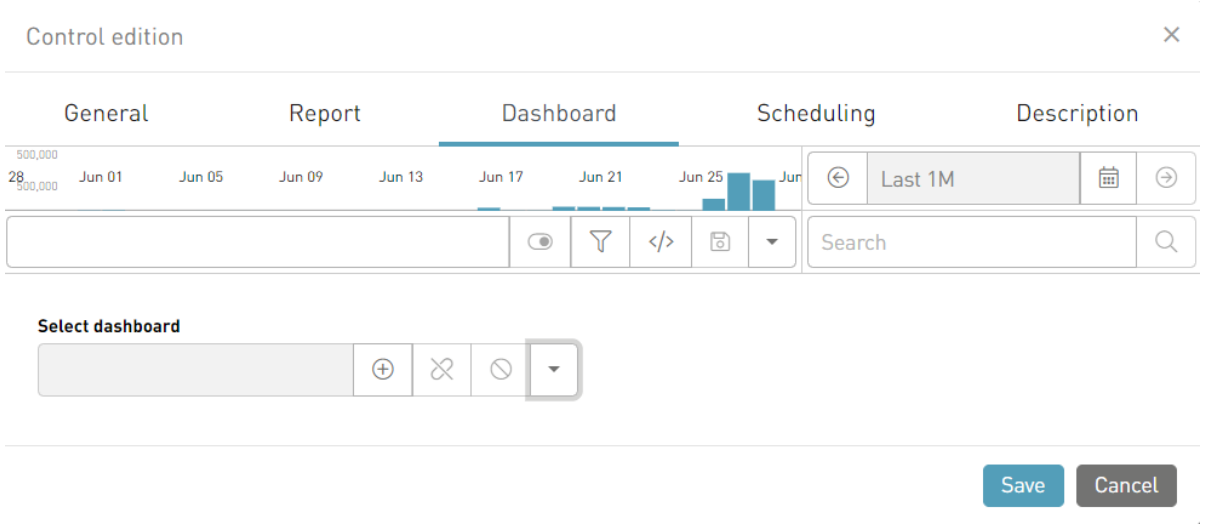
PROFILING VARIABLES

Aggregation	Field mapping	Scoring	Whitelisted	Blacklisted	Weight	Ignore missing values
tp_glob_counterparty_account_id	**counterparty_account_id**	LOGARITHMIC	false	false	2	false
tp_counterparty_bank_country	**counterparty_bank_country** **customer_name**	STATISTICAL	false	false	49	false
tp_new_customer	**service** **customer_name**	STATISTICAL	false	false	0	false
tp_glob_counterparty_bank_country	**counterparty_bank_country**	LOGARITHMIC	false	false	3	false

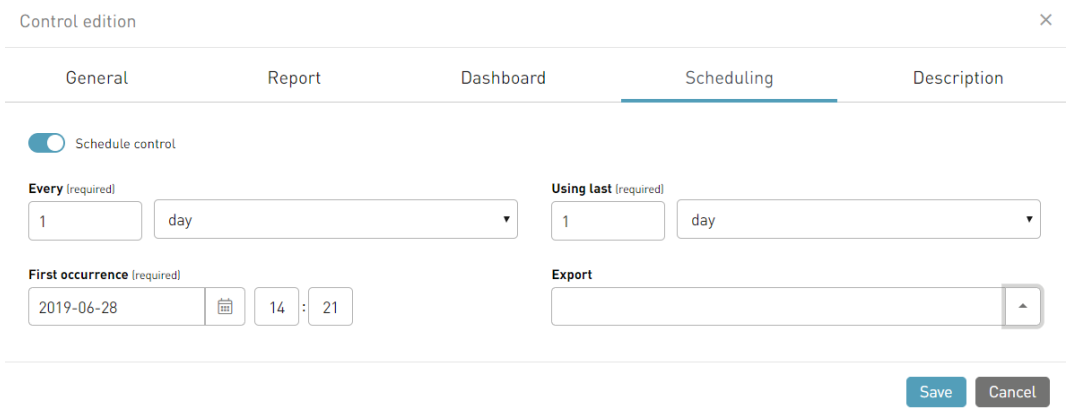
Total entries: 8

Modify control - Dashboard

- Link existing Dashboard to control
- Create a new dashboard for control
- More information in Dashboard creation slides



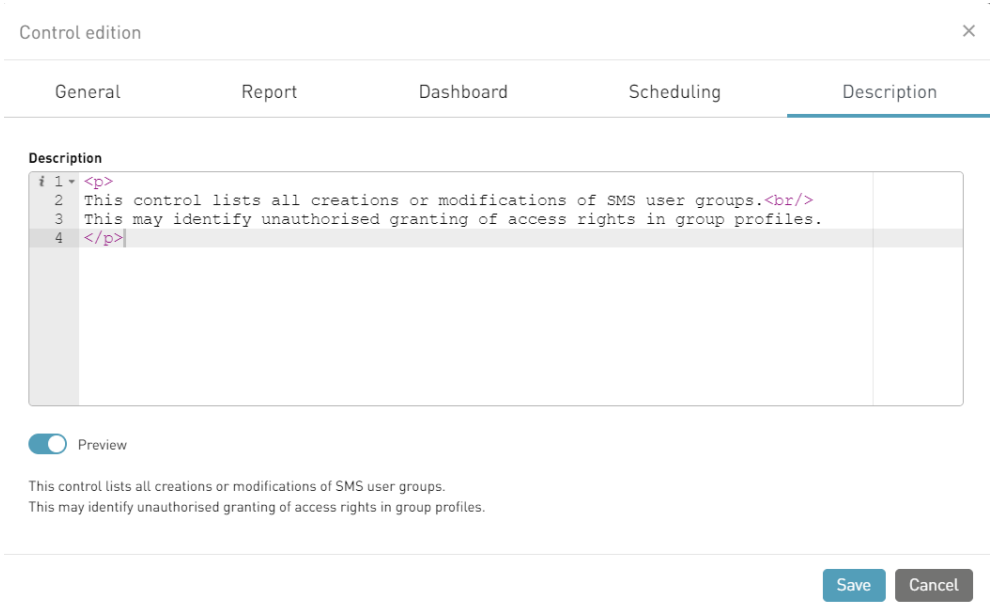
Modify control - Scheduling



- Schedule execution of controls
  - Every (recurrence)
    - Time between two executions
  - First occurence
    - When execute first
  - Using last
    - Data in this period will be considered for execution
  - Export of output
    - Specify targets to export control results to

Modify control - Description

- Documentation of the control
  - Written in HTML
  - Could be previewed



Wrap up

- NG|Screener UI enables to
  - Navigate in data through Dashboards
    - Either raw data from data source
    - Or aggregated data outputted from controls
  - Process data via Controls
    - See output of controls
    - Modify or create new controls
- More detailed information to be found in
  - Dashboard Creation slides
  - Control Creation slides
  - Profiling Slides
- NG|Screener UI for administrator is another subject

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

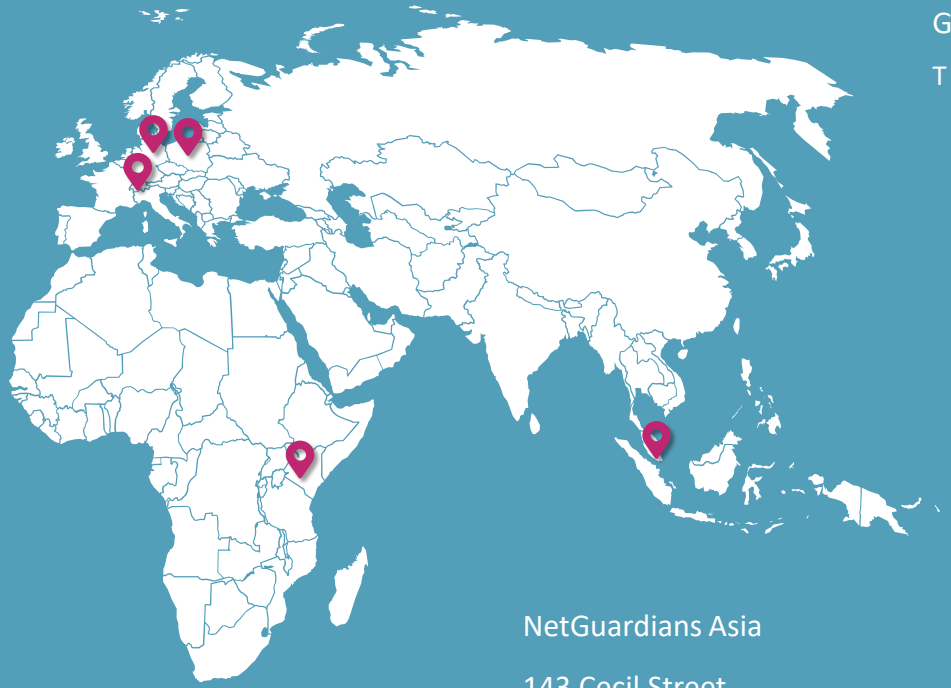
nikolov@netguardians.ch

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