

 RiskTech
100 2019 Gartner 2015
CoolVendor

NG | Screener UI Administration

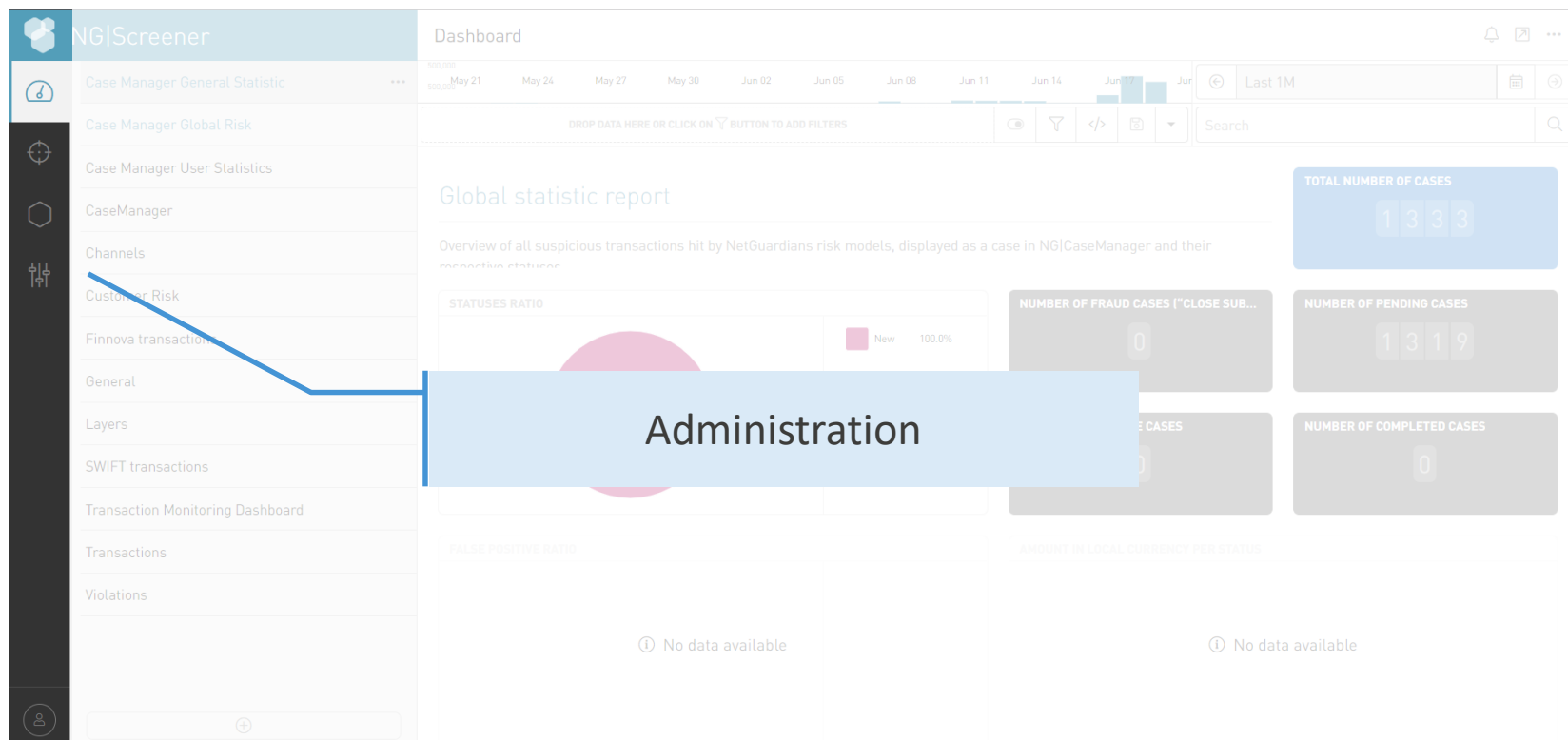
Ljupce Nikolov
June 2019



Summary

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

Access Admin section



Admin section Menu

NG|Screener

Profiling aggregations

Channels

Smart filters

Reference data

Monitoring

Processing

Security roles

Data capture alerting

Licensing

Fields Mapping

Profiling aggregations

PROFILING AGGREGATIONS

FFE Country	COMPUTED
FFE Country City	COMPUTED
FFE User Country	COMPUTED
FFE User Country City	COMPUTED
FFE User Day_of_Week	COMPUTED
FFE User Part_of_Day	COMPUTED
et_counterparty_account_id	COMPUTED
et_counterparty_bank_country	COMPUTED
et_counterparty_bank_id	COMPUTED
et_glob_counterparty_account_id	COMPUTED
et_glob_counterparty_bank_id	COMPUTED
et_new_contract	COMPUTED
et_operation_type	COMPUTED
et_order_type	COMPUTED
et_sess_auth	COMPUTED
et_sess_browser	COMPUTED
et_sess_connection_country	COMPUTED
et_sess_language	COMPUTED

Total entries: 159

PROFILING AGGREGATION EDITION

Enabled

Name (required)

FFE Country

Owner (required)

[USER] admin

Public

Services (required)

fortinetFortigateEvent@*

Variable (required)

source_country

Dimensions

Period value (required)

5

Period type (required)

Months sliding

Schedule value (required)

1

Schedule unit (required)

Hour

Query filter

classification:"Fortinet SSL-VPN Session Event" AND NOT (source_country:"Unknown")

NetGuardians

4

© 2019 NetGuardians SA. All rights reserved

Admin section Menu

The screenshot displays the NG|Screener Admin interface. On the left is a sidebar menu with the following items: Profiling aggregations, Channels, Smart filters, Reference data, Monitoring, Processing, Security roles, Data capture alerting, Licensing, and Fields Mapping. The 'Processing' item is highlighted with a blue box labeled 'Administration Options'. The main content area shows the 'Profiling aggregations' page, which includes a table of aggregations and a 'PROFILING AGGREGATION EDITION' form on the right.

PROFILING AGGREGATIONS	
FFE Country	COMPUTED
FFE Country City	COMPUTED
FFE User Country	COMPUTED
FFE User Country City	COMPUTED
FFE User Day of Week	COMPUTED
FFE User Port of Day	COMPUTED
et_counterparty_account_id	COMPUTED
et_counterparty_bank_country	COMPUTED
et_counterparty_bank_id	COMPUTED
et_glob_counterparty_account_id	COMPUTED
et_glob_counterparty_bank_id	COMPUTED
et_new_contract	COMPUTED
et_operation_type	COMPUTED
et_order_type	COMPUTED
et_sess_auth	COMPUTED
et_sess_browser	COMPUTED
et_sess_connection_country	COMPUTED
et_sess_language	COMPUTED

Total entries: 159

PROFILING AGGREGATION EDITION

☒ Enabled

Name (required): FFE Country

Owner (required): [USER] admin ☒ Public

Services (required):

Dimensions:

Period value (required): 5 Period type (required): Months sliding

Schedule value (required): 1 Schedule unit (required): Hour

Query filter: classification:"Fortinet SSL-VPN Session Event" AND NOT [source_country:"Unknown"]

Security Roles





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

Profiling aggregations
Channels
Smart filters
Reference data
Monitoring >
Processing >
Security roles
Data capture alerting
Licensing
Fields Mapping

ROLES
TEST_IB_SCO_MANAGER
TEST_OWN_CONTROLS_ONLY
TEST_OWN_PUB_CONTROLS_ONLY
TEST_ALL_CONTROLS_ONLY
NG_User
TEST_ALL_CONTROLS_NO_MANAGE
NG_Admin

Total entries: 7

ROLE EDITION

Name (required)

Allowed sources (required)

B

Functionality

CONTROL_MANAGE_PRIVATECD...	ADMIN_VIEW_CUSTOM_PROCES...	CONTROL_EXECUTE_PRIVATECO...
DASHBOARD_READ_PUBLICDAS...	DASHBOARD_READ_ALLDASHB...	DASHBOARD_READ_PRIVATEDA...
CONTROL_READ_PRIVATECONT...	CONTROL_READ_PUBLICTARGETS	CONTROL_READ_PRIVATETARGE...
CONTROL_READ_PUBLICCONTR...	CONTROL_MANAGE_PRIVATETA...	



Security Roles

Add new security role

Profiling aggregations
Channels
Smart filters
Reference data
Monitoring
Processing
Security roles
Data capture alerting
Licensing
Fields Mapping

List of existing security roles

ROLES
TEST_IB_SCO_MANAGER
TEST_OWN_CONTROLS_ONLY
TEST_OWN_PUB_CONTROLS_ONLY
TEST_ALL_CONTROLS_ONLY
NG_User
TEST_ALL_CONTROLS_NO_MANAGE
NG_Admin

Total entries: 7

ROLE EDITION

Name (required)
NG_User

Allowed sources (required)
B

Functionality

CONTROL_MANAGE_PRIVATECD...	ADMIN_VIEW_CUSTOM_PROCES...	CONTROL_EXECUTE_PRIVATECO...
DASHBOARD_READ_PUBLICDAS...	DASHBOARD_READ_ALLDASHB...	DASHBOARD_READ_PRIVATEDA...
CONTROL_READ_PRIVATECONT...	CONTROL_READ_PUBLICTARGETS	CONTROL_READ_PRIVATEARGE...
CONTROL_READ_PUBLICCONTR...	CONTROL_MANAGE_PRIVATEA...	

Definition of NG_User security role



Security Roles

Profiling aggregations

Channels

Smart filters

Reference data

Monitoring >

Processing >

Security roles

Data capture alerting

Licensing

Fields Mapping

ROLES

TEST_IB_SCO_MANAGER
TEST_OWN_CONTROLS_ONLY
TEST_OWN_PUB_CONTROLS_ONLY
TEST_ALL_CONTROLS_ONLY
NG_User

Total entries: 7

ROLE EDITOR

Name (required)
NG_User

Allowed sources (required)
B

Functionality

CONTROL_MANAGE_PRIVATECD...	ADMIN_VIEW_CUSTOM_PROCES...	CONTROL_EXECUTE_PRIVATECO...
DASHBOARD_READ_PUBLICDAS...	DASHBOARD_READ_ALLDASHB...	DASHBOARD_READ_PRIVATEDA...
CONTROL_READ_PRIVATECONT...	CONTROL_READ_PUBLICTARGETS	CONTROL_READ_PRIVATETARGE...
CONTROL_READ_PUBLICCONTR...	CONTROL_MANAGE_PRIVATETA...	

Data source allowed to the role (in service@host format)

Allowed application functionality to the role

Channels

 RiskTech
100 2019 Gartner 2015
Cool Vendor



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

Profiling aggregations

Channels

Smart filters

Reference data

Monitoring >

Processing >

Security roles

Data capture alerting

Licensing

Fields Mapping

CHANNELS			<div><div></div><div></div><div></div><div></div></div>
Name	Type	Parameters	
> Case Manager	Case Manager	CM API Auth. Key: 862af85646b3a929d94b7601a72c33eba52e4a5d CM ASYNC ISSUE CREATION: false CM URL: http://localhost:3000/cm Connection timeout: 180	
Total entries: 1			



Channels List

Profiling aggregations

Channels

Smart filters

Reference data

Monitoring >

Processing >

Security roles

Data capture alerting

Licensing

Fields Mapping

CHANNELS

Name	Type	Parameters
> Case Manager	Case Manager	CM API Auth. Key: 862af85646b3a929d94b7601a72c33eba52e4a5d CM ASYNC ISSUE CREATION: false CM URL: http://localhost:3000/cm Connection timeout: 180

Parameters specific to each channel

Test channel connection

Total entries: 1

Channels List

Profiling aggregations
Channels
Smart filters
Reference data
Monitoring
Processing
Security roles

Extend to see list of targets for the channel

CHANNELS

Name	Type	Parameters
Case Manager	Case Manager	CM API Auth. Key: 862af85646b3a929d94b7601a72c33eba52e4a5d CM ASYNC ISSUE CREATION: false CM URL: http://localhost:3000/cm Connection timeout: 180

TARGETS

Name	Visibility	File name	File type	Date format	Split report
BankingSystemsInformation		%n-%sd	PDF		NONE
BankingSystemsViolations		%n-%sd	PDF		NONE
ControlValidation		%n-%sd	PDF		NONE
ITSystemsInformation		%n-%sd	PDF		NONE
ITSystemsViolations		%n-%sd	PDF		NONE
Pr02UnusualLocation		%n	CSV		NONE
UTS103@CM		%n	CSV		NONE
UTC103@CM		%n	CSV		NONE
UTC101@CM		%n	CSV		NONE
UTS202@CM		%n	CSV		NONE
UTC202COV@CM		%n	CSV		NONE
UTS202COV@CM		%n	CSV		NONE
UT@CM		%n	CSV		NONE
RD@CM		%n	CSV		NONE

Total entries: 1

Targets d

Targets defined on the channel



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

The screenshot shows the NetGuardians interface. At the top, a blue box labeled "Add new channel" has a line pointing to a "+" icon in the top right corner of the channel list. Below this, a channel is selected, showing a list of targets. A second blue box labeled "Add new target" has a line pointing to a "+" icon in the top right corner of the target list for the selected channel.

Channel	Target
33eba52e4a5d	Split report
	NONE
	NONE
	NONE
	NONE



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)



Smart Filters

 RiskTech
100 2019 Gartner 2015
Cool Vendor



Smart Filters

- Smart Filters help navigate from one view to another (dashboards)
- Transformation could be applied to filters when switching view



Smart Filters

Profiling aggregations
Channels
Smart filters
Reference data
Monitoring >
Processing >
Security roles
Data capture alerting
Licensing
Fields Mapping

List of smart filters
defined

SMART FILTERS

To Channel Activity

source_user_activity_search

Total entries: 2

SMART FILTER EDITION

Filter name (required)
To Channel Activity

Source view (required)
Violations

Target view (required)
Channels

TRANSFORMATIONS

Operation	Field	Attributes
-----------	-------	------------

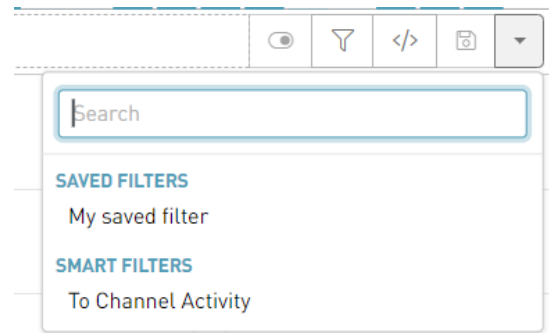
Total entries: 0

Definition of the
selected filter



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.



Data Capture Alerting





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

- Profiling aggregations
- Channels
- Smart filters
- Reference data
- Monitoring >
- Processing >
- Security roles
- Data capture alerting
- Licensing
- Fields Mapping

ALERTING POLICY

Add new item

Total entries: 0

ALERTING POLICY EDITION

☒ Enable

Name (required)
My capture alerting policy

Services (required)
swiftTransaction@*

Min threshold (required)
1

Max threshold (required)
0

Time range (required)
1

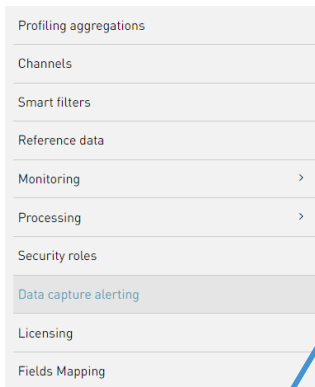
Time range unit (required)
Day

Schedule (required)
Every day at 23:59

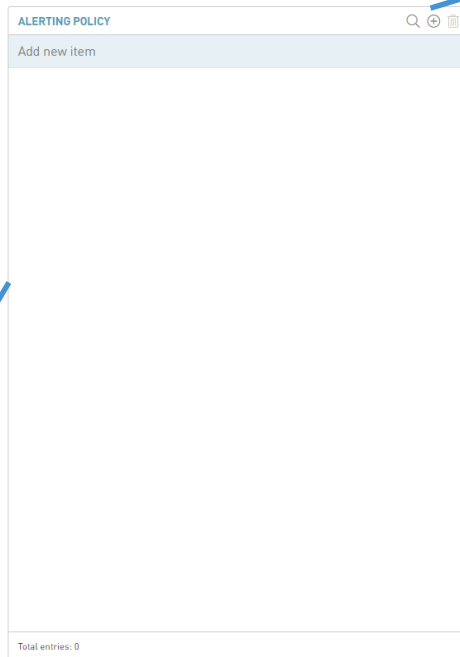
Export
Data capture alerting target@Em...

Data Capture alerting

Create a new alerting policy



List of alerting policies defined



ALERTING POLICY EDITION

☒ Enable

Name (required)
My capture alerting policy

Services (required)
swiftTransaction@*

Min threshold (required) 1 **Max threshold** (required) 0

Time range (required) 1 **Time range unit** (required) Day

Schedule (required)
Every day at 23:59

Export
Data capture alerting target@Em...

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)

The screenshot shows a web form titled "ALERTING POLICY EDITION" with a close button (X) and a confirmation button (checkmark). The form contains the following fields:

- Enable:** A toggle switch that is currently turned on.
- Name (required):** A text input field containing "My capture alerting policy".
- Services (required):** A dropdown menu showing "swiftTransaction@*".
- Min threshold (required):** A text input field containing "1".
- Max threshold (required):** A text input field containing "0".
- Time range (required):** A text input field containing "1".
- Time range unit (required):** A dropdown menu showing "Day".
- Schedule (required):** A text input field containing "Every day at 23:59", with a clock icon and a trash icon to its right.
- Export:** A text input field containing "Data capture alerting target@Em...".



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

The screenshot shows a scheduling configuration window. At the top, there is a 'Frequency' dropdown menu. Below it, the word 'Each' is followed by a row of seven circular buttons representing the days of the week: Mon, Tue, Wed, Thu, Fri, Sat, and Sun. The 'Mon' through 'Fri' buttons are blue, while 'Sat' and 'Sun' are grey. Below the day buttons, there is a 'From' field with a time picker set to '08 : 00' and a 'to' field with a time picker set to '18 : 00'. At the bottom, there is an 'Every' field with a numeric input set to '1' and a unit dropdown menu set to 'hour(s)'.

Licensing





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

LICENSING

License file (Field is required)

Choose File

No file chosen

Activate

Download fingerprint

Fields Mapping





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

NG|Screener

🔍

⚙️

🏠

📊

👤

Profiling aggregations

Profiling peer groups

Channels

Smart filters

Reference data

Monitoring >

Processing >

Security roles

Data capture alerting

Licensing

Field mappings

Field mappings

FIELD MAPPINGS

Technical name	Business name
add_issue_watchers	Add issue watchers
add_issues	Add issues
add_messages	Add messages
add_notes	Add notes
add_project	Add project
add_subprojects	Add subprojects
allow_rerouting	Allow rerouting
applid/0	Applid/0
assignable	Assignable
assigned_on_timestamp	Assigned on timestamp
assignee	Assignee
assignment_time_minutes_amount	Assignment time minutes amount
branch_id	Branch id
browse_repository	Browse repository
bulk_edit	Bulk edit
bulk_edit_assignee	Bulk edit assignee
bulk_update	Bulk update
bulk_update_assignee	Bulk update assignee

Total entries: 1422

Fields Mapping

The screenshot displays the 'Field mappings' section of the NG|Screener application. On the left is a sidebar with navigation options: Profiling aggregations, Profiling peer groups, Channels, Smart filters, Reference data, Monitoring, Processing, and Security roles. The main area is titled 'FIELD MAPPINGS' and contains a table with two columns: 'Technical name' and 'Business name'. A third column, 'Saved search (table)', is indicated by a callout box and an arrow pointing to the 'Business name' column. Below the mapping table is a 'TICKETS LIST' table showing two rows of ticket data. A callout box labeled 'Field names in NG|Storage' points to the 'Technical name' column, and another callout box labeled 'Field names in Saved search (table)' points to the 'Business name' column.

Technical name	Business name
add_issue_watchers	Add issue watchers
add_issues	Add issues
add_messages	Add messages
add_notes	Add notes
add_project	Add project
add_subprojects	Add subprojects
allow_rerouting	Allow rerouting
applid/0	Applid/0
assignable	Assignable
assigned_on_timestamp	Assigned on timestamp
assignee	Assignee
assignment_time_minutes_amount	Assignment time minutes amount
branch_id	Branch id
browse_repository	Browse repository
bulk_edit	Bulk edit
bulk_edit_assignee	
bulk_update	
bulk_update_assignee	

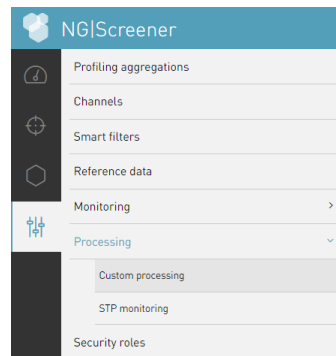
TICKETS LIST				
Timestamp	Subject	Assignee	Issue id	Last update user
> 2019-07-01T10:51:15+02:00	Order TP95532244/106703, Customer 311676, Account 6018.81.10	front_office	103	front_office
> 2019-07-01T10:51:15+02:00	Order NR16645329/422560, Customer 2445448, Account 8227.30.04	front_office	104	front_office

Custom Processing



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



Custom Processing

Start date (required)
2019-07-01 00:00

End date (required)
2019-07-02 00:00

Select services
swiftTransaction@*

Save Cancel



Thank you!

NetGuardians



+41 24 425 97 60



info@netguardians.ch



www.netguardians.ch



[Linkedin.com/company/netguardians](https://www.linkedin.com/company/netguardians)



[Facebook.com/NetGuardians](https://www.facebook.com/NetGuardians)



[@netguardians](https://twitter.com/netguardians)



<https://www.youtube.com/netguardians>

Ljupce Nikolov



+41 24 425 97 60



nikolov@netguardians.ch



Contact us

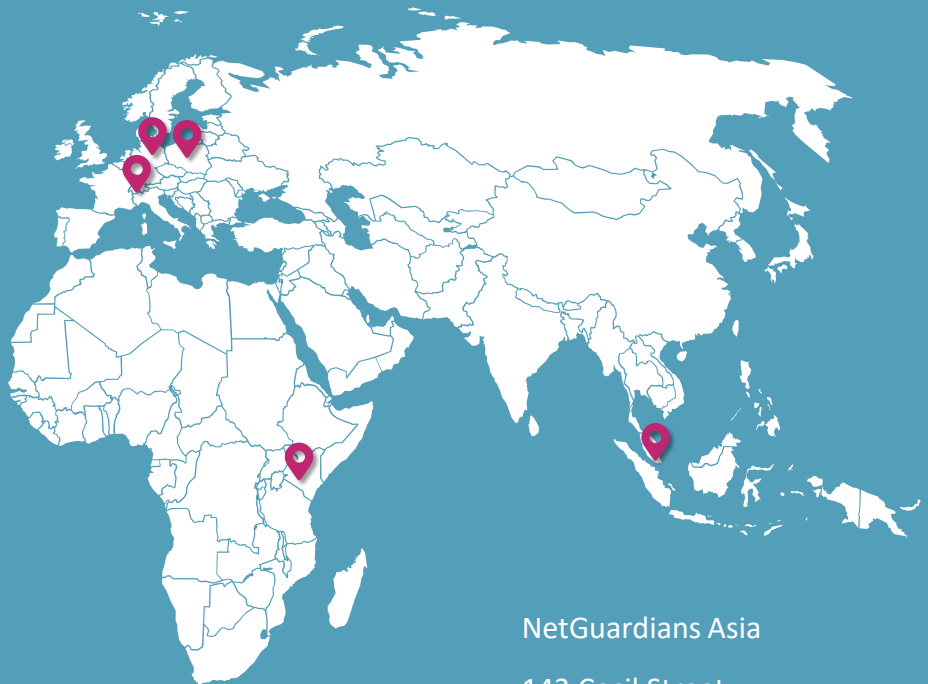
NetGuardians Headquarters

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

T +41 24 425 97 60

NetGuardians Africa

Vienna Court
State House Rd
Nairobi, Kenya
+254 205 138539



NetGuardians Germany

Rhein-Main Gebiet
Germany

T +49 172 3799003

NetGuardians Eastern Europe

Koszykowa 61, 00-667
Warsaw, Poland

NetGuardians Asia

143 Cecil Street
#09-01 GB Building
069542 Singapore
T +65 6224 0987