Tecplix

Chronicle

Chronicle Configuration Document

Netskope

Document version: 1.0

Date: 24 Jan 2023

Netskope

This document explains how to configure your Chronicle integration with the Log Shipper module of the Netskope Cloud Exchange platform. This integration allows pushing alerts and events from Netskope to the Chronicle platform.

Prerequisites

To complete this configuration, you need:

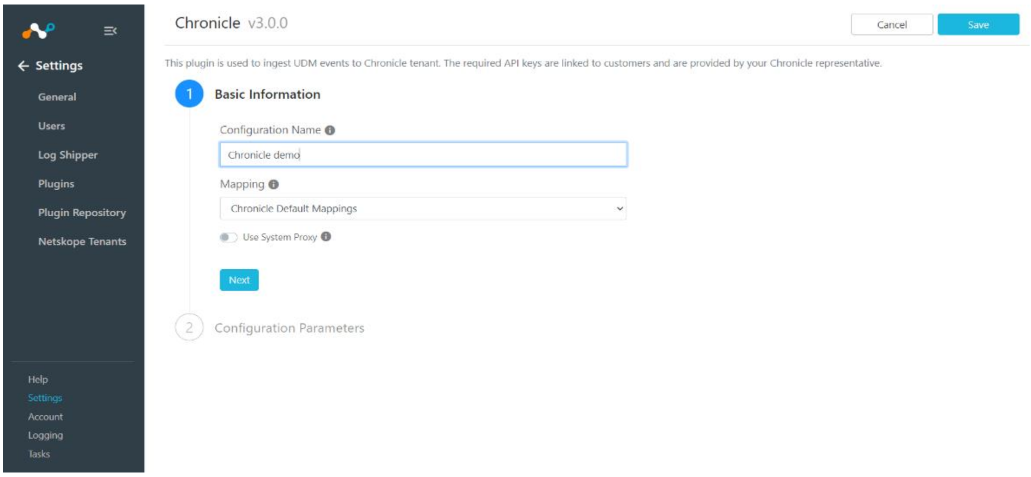
- A Netskope tenant (or multiple, for example, production and development/test instances)
- A Netskope Cloud Exchange tenant with the **Log Shipper** module already configured.
- A Chronicle account. Obtain your Chronicle Base URL and API Key from your Chronicle representative before proceeding.

Workflow

1. Configure the Chronicle Plugin.
2. Configure Log Shipper Business Rules for Chronicle.
3. Configure Log Shipper SIEM Mappings for Chronicle.
4. Validate the Chronicle plugin.

Configure the Chronicle Plugin.

1. Go to Settings > Plugin.
2. Select the Chronicle box to open the plugin creation dialog
3. Enter a Configuration Name.
4. Select a valid Mapping (Default Mappings for all plugins are available). Click Next.



Chronicle v3.0.0

This plugin is used to ingest UDM events to Chronicle tenant. The required API keys are linked to customers and are provided by your Chronicle representative.

1 Basic Information

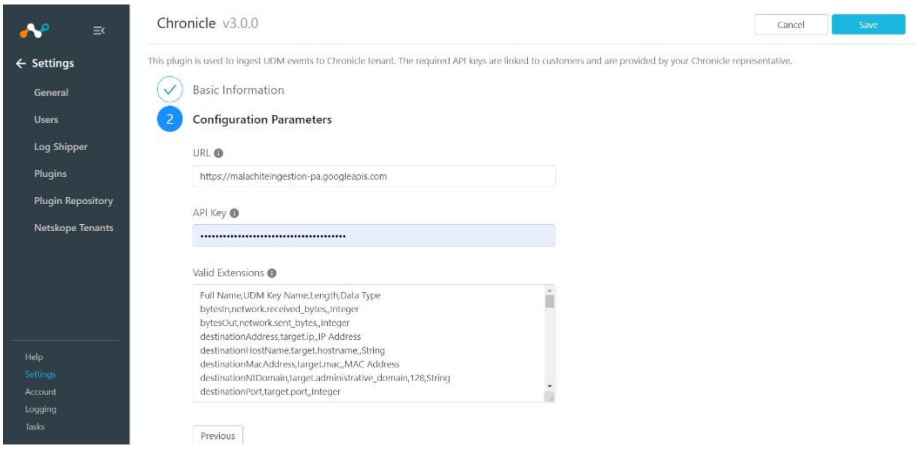
Configuration Name: Chronicle demo

Mapping: Chronicle Default Mappings

Use System Proxy

2 Configuration Parameters

1. Enter the Chronicle Base URL, API key (which is provided to you by the Chronicle representative), and Valid Extensions (as shown).



Chronicle v3.0.0

This plugin is used to ingest UDM events to Chronicle tenant. The required API keys are linked to customers and are provided by your Chronicle representative.

Basic Information

2 Configuration Parameters

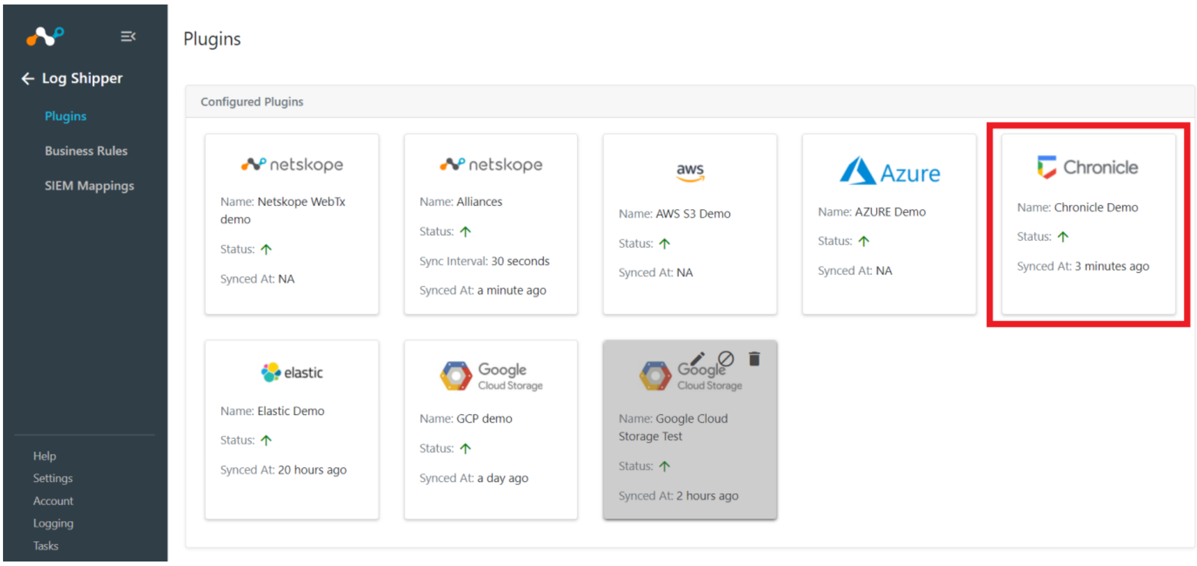
URL: https://malachiteingestion-pa.googleapis.com

API Key: ••

Valid Extensions:

```
Full Name,UDM Key Name,Length,Data Type
bytesIn,network.received_bytes,,Integer
bytesOut,network.sent_bytes,,Integer
destinationAddress,target.ip,,IP Address
destinationHostName,target.hostname,,String
destinationMacAddress,target.mac,,MAC Address
destinationNtDomain,target.administrative_domain,128,String
destinationPort,target.port,,Integer
```

2. Click **Save**.



Plugins

Configured Plugins

Name: Netskope WebTx demo
Status: ↑
Synced At: NA

Name: Alliances
Status: ↑
Sync Interval: 30 seconds
Synced At: a minute ago

Name: AWS S3 Demo
Status: ↑
Synced At: NA

Name: AZURE Demo
Status: ↑
Synced At: NA

Name: Chronicle Demo
Status: ↑
Synced At: 3 minutes ago

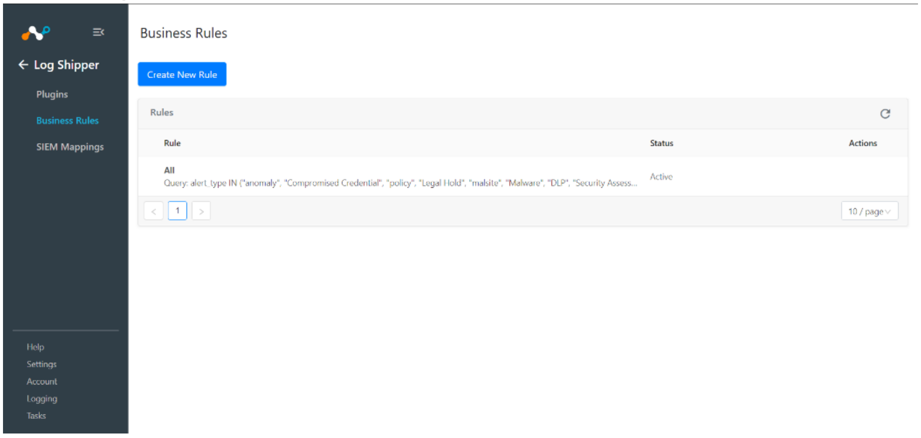
Name: Elastic Demo
Status: ↑
Synced At: 20 hours ago

Name: GCP demo
Status: ↑
Synced At: a day ago

Name: Google Cloud Storage Test
Status: ↑
Synced At: 2 hours ago

Configure Log Shipper Business Rules for Chronicle.

1. Go to **Log Shipper > Business Rules**.

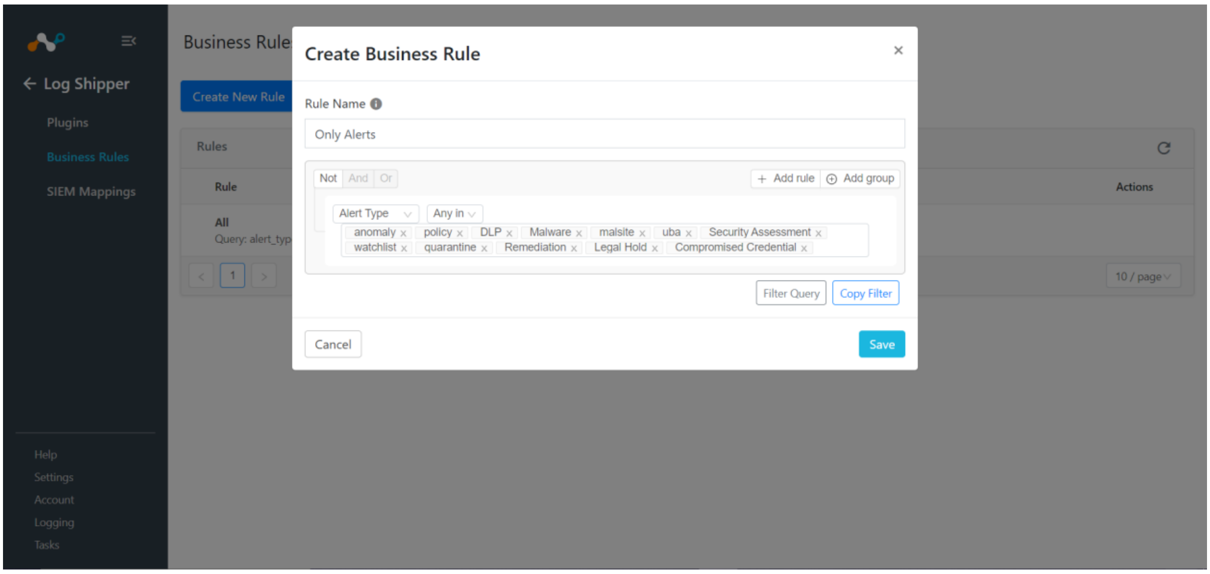


Business Rules

Rules

Rule	Status	Actions
All Query: alert_type IN ("anomaly", "Compromised Credential", "policy", "Legal Hold", "malsite", "Malware", "DLP", "Security Assess...	Active	

2. Click Create **New Rule**.

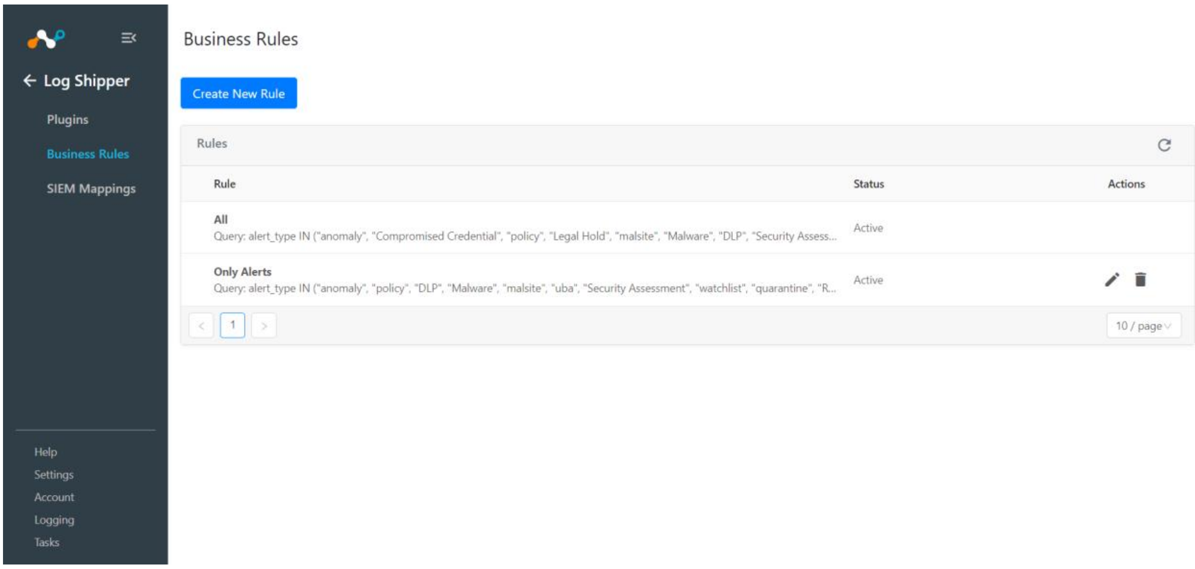


Create Business Rule

Rule Name: Only Alerts

Alert Type — Any in: anomaly, policy, DLP, Malware, malsite, uba, Security Assessment, watchlist, quarantine, Remediation, Legal Hold, Compromised Credential

3. Enter a Rule Name and select the filters to use.
4. Click **Save**.



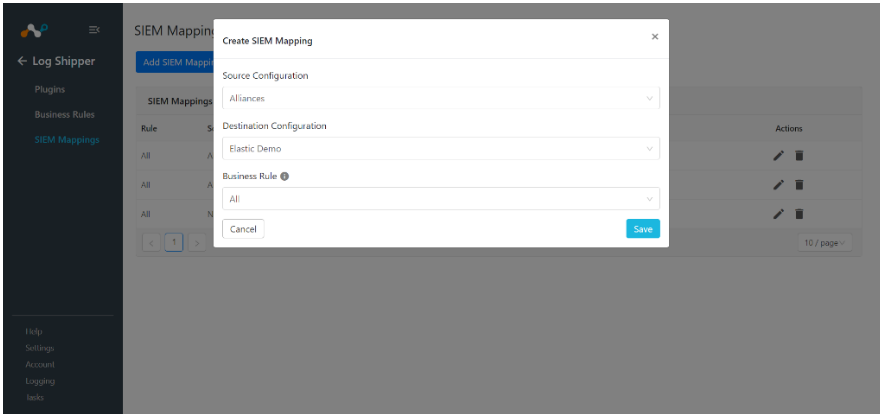
Business Rules

Rules

Rule	Status	Actions
All Query: alert_type IN ("anomaly", "Compromised Credential", "policy", "Legal Hold", "malsite", "Malware", "DLP", "Security Assess...	Active	
Only Alerts Query: alert_type IN ("anomaly", "policy", "DLP", "Malware", "malsite", "uba", "Security Assessment", "watchlist", "quarantine", "R...	Active	✎ 🗑

Configure Log Shipper SIEM Mappings for Chronicle

1. Go to **Log Shipper** > **SIEM Mappings** and click **Add SIEM Mapping**.
2. Select a Source Configuration, Business Rule, and Destination Configuration.



Create SIEM Mapping

Source Configuration: Alliances

Destination Configuration: Elastic Demo

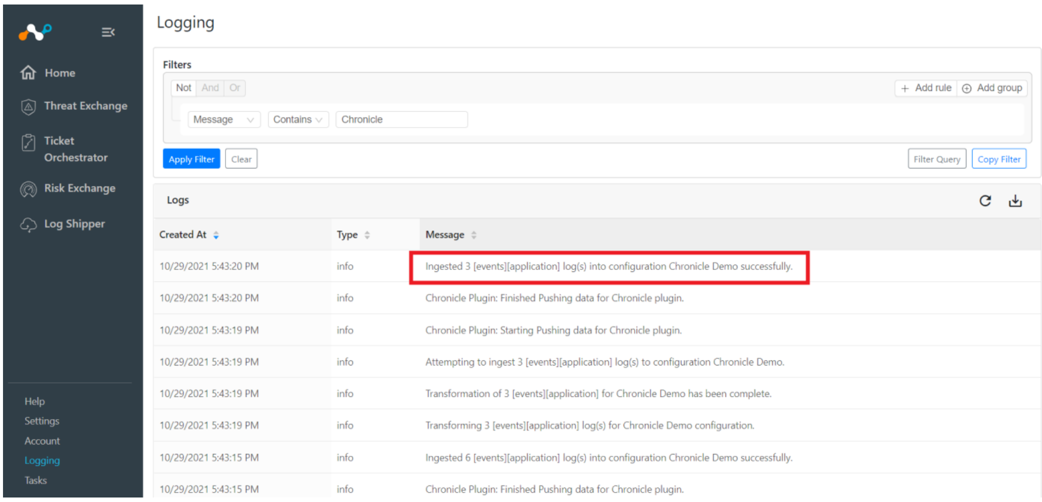
Business Rule: All

3. Click **Save**

Validate the Chronicle plugin.

To validate the plugin workflow, you can check from Netskope Cloud Exchange and from the Chronicle Platform.

To validate from Netskope Cloud Exchange, go to Logging.



Logging

Filters

Not | And | Or — + Add rule | ⊕ Add group

Message ⌄ | Contains ⌄ | Chronicle

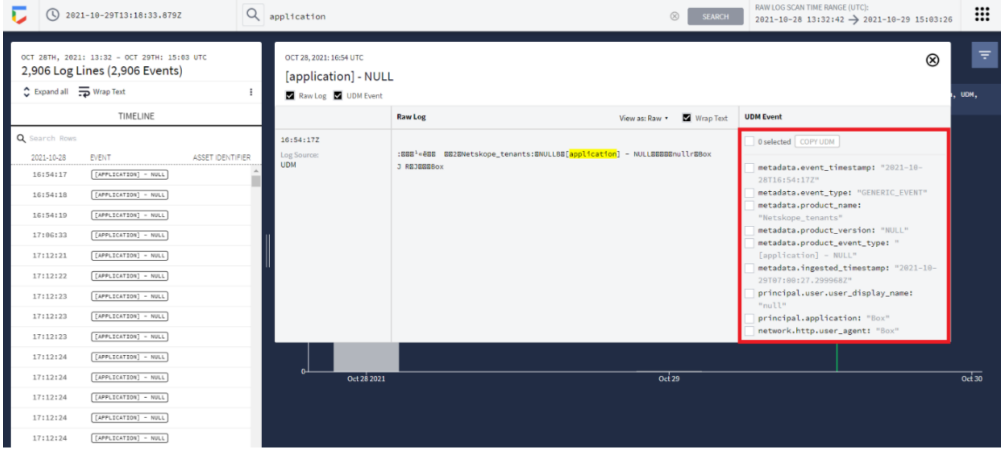
Apply Filter | Clear — Filter Query | Copy Filter

Logs

Created At	Type	Message
10/29/2021 5:43:20 PM	info	Ingested 3 [events][application] log(s) into configuration Chronicle Demo successfully.
10/29/2021 5:43:20 PM	info	Chronicle Plugin: Finished Pushing data for Chronicle plugin.
10/29/2021 5:43:19 PM	info	Chronicle Plugin: Starting Pushing data for Chronicle plugin.
10/29/2021 5:43:19 PM	info	Attempting to ingest 3 [events][application] log(s) to configuration Chronicle Demo.
10/29/2021 5:43:19 PM	info	Transformation of 3 [events][application] for Chronicle Demo has been complete.
10/29/2021 5:43:19 PM	info	Transforming 3 [events][application] log(s) for Chronicle Demo configuration.
10/29/2021 5:43:15 PM	info	Ingested 6 [events][application] log(s) into configuration Chronicle Demo successfully.
10/29/2021 5:43:15 PM	info	Chronicle Plugin: Finished Pushing data for Chronicle plugin.

To validate from the Chronicle Platform.

1. Log in to the Chronicle Platform to view data.
2. Enter a keyword that you want to search for (in this case, an application).
3. Click **Search**.
4. Then you see the ingested data.



OCT 28TH, 2021: 13:32 - OCT 29TH: 15:03 UTC

2,906 Log Lines (2,906 Events)

2021-10-28	EVENT	ASSET IDENTIFIER
16:54:17	[APPLICATION] - NULL	
16:54:18	[APPLICATION] - NULL	
16:54:19	[APPLICATION] - NULL	
17:06:33	[APPLICATION] - NULL	
17:12:21	[APPLICATION] - NULL	
17:12:22	[APPLICATION] - NULL	
17:12:23	[APPLICATION] - NULL	
17:12:23	[APPLICATION] - NULL	
17:12:23	[APPLICATION] - NULL	
17:12:24	[APPLICATION] - NULL	
17:12:24	[APPLICATION] - NULL	
17:12:24	[APPLICATION] - NULL	
17:12:24	[APPLICATION] - NULL	
17:12:24	[APPLICATION] - NULL	

OCT 28, 2021: 16:54 UTC

[application] - NULL

☑ Raw Log ☑ UDM Event

Raw Log — View as: Raw ▾ ☑ Wrap Text

16:54:17Z

Log Source: UDM

```
:▯▯▯¹+▯▯▯ ▯▯2▯Netskope_tenants:▯NULL▯▯[application] - NULL▯▯▯▯▯nullr▯Box
J R▯J▯▯▯▯Box
```

UDM Event

□ 0 selected COPY UDM

```
□ metadata.event_timestamp: "2021-10-28T16:54:17Z"
□ metadata.event_type: "GENERIC_EVENT"
□ metadata.product_name: "Netskope_tenants"
□ metadata.product_version: "NULL"
□ metadata.product_event_type: "[application] - NULL"
□ metadata.ingested_timestamp: "2021-10-29T07:00:27.299968Z"
□ principal.user.user_display_name: "null"
□ principal.application: "Box"
□ network.http.user_agent: "Box"
```

Reference: https://docs.netskope.com/en/chronicle-plugin-for-log-shipper.html

End of Document