ELO Analytics Konfiguration

[Stand: 15.05.2019 | Programmversion: 12]

Dieses Dokument beschreibt Aspekte der Konfiguration von ELO Analytics. Dazu zählen der Aufbau der Konfigurationsdateien, eine Referenz der Konfigurationseinstellungen sowie tiefergehende Themen zu den Konfigurationseinstellungen.

Information: Dieses Dokument bezieht sich auf die folgenden Versionen:

- ELO Analytics: 12
- Kibana: 5.6.3

Sie finden weitere Artikel zu ELO Analytics in der ELO Community. Schauen Sie dort vorbei und abonnieren Sie den ELO Analytics-Bereich, um keine Neuigkeit zu verpassen.

https://community.elo.com

Information: Mit ELO Analytics erhalten Sie weitere Dokumentationen aus dem ELO PartnerPortal.

- Technische Dokumentation
- Benutzerdokumentation
- Häufig gestellte Fragen
- Konfiguration (liegt Ihnen vor)
- Sicherungsmanagement
- Komponentendiagramm

Inhalt

1 Einführung 3
2 Allgemeine Konfigurationsbeschreibung 4
2.1 Regeln für die Konfigurationsdateien 4
2.2 Konfigurationen von Kibana und ELO Analytics 4
2.3 Kibana-Konfiguration festlegen 6
3 Referenz 8
3.1 Standardkonfiguration kibana.yml 9
3.2 ELO Analytics Konfiguration in der Datei ‚kibana.yml' 18
3.3 ELO Analytics-Konfigurationsreferenz 21
3.4 Vollständige ELO Analytics-Konfiguration (Beispiel) 53
4 Erweiterte Konfigurationsbeschreibungen 68
4.1 ELO Analytics ACL-Filter 68
4.1.1 Navigationsfilter-ACL (Navigationfilter) 68
4.1.2 Abfragenfilter-ACL (AcessFilter) 69
4.1.3 Anpassung mit Custom-Config 69
4.2 Kennwortverschlüsselung in ELO Analytics konfigurieren 72
4.2.1 Anpassen der Dienste unter Windows 73
4.2.2 Nachträgliches Ändern eines Kennworts 75
4.3 Vollständige Elasticsearch-Query nach ELO Analytics 75
4.4 Log-Rotation 79
5 Weiterführende Literatur 81
6 Referenzverzeichnis 82

1 Einführung

Mit ELO Analytics wird ein komplett neuer Bereich von Konfigurationsmöglichkeiten aufgetan, der eine Vielzahl von Anpassungen und Änderungen in den Verhaltensweisen von ELO Analytics ermöglicht. Dieses Dokument soll daher eine Übersicht, Beschreibung und Referenz für die Konfigurationseinstellungen in ELO Analytics sowie zum Teil von Kibana sein. Das Kapitel 2 beginnt mit den Grundlagen welche Konfigurationsdateien in ELO Analytics existieren und wie diese verarbeitet werden. Das Kapitel 3 listet alle Konfigurationswerte von ELO Analytics sowie einen Teil der Konfigurationswerte von Kibana auf. Sie finden eine Übersicht über die Eigenschaftsnamen im Kapitel 5 *Weiterführende Literatur*.

- Kibana 5.6 Konfigurationsschlüssel

  https://www.elastic.co/guide/en/kibana/5.5/settings.html

2 Allgemeine Konfigurationsbeschreibung

Dieses Kapitel enthält allgemeine Informationen zur Konfiguration der unterschiedlichen Bestandteile von ELO Analytics.

2.1 Regeln für die Konfigurationsdateien

1. Alle Konfigurationsdateien müssen immer im UTF-8-Format ohne BOM gespeichert sein.
2. Benutzen Sie keine Tabulatoren, um Einzüge zu erstellen. Nutzen Sie stattdessen Leerzeichen.
3. Bearbeiten Sie die Konfigurationsdateien nicht in Microsoft Word oder ähnlichen WYSIWYG Texteditoren.

2.2 Konfigurationen von Kibana und ELO Analytics

ELO Analytics enthält verschiedene Konfigurationen, die sich in zwei Typen (YAML und JSON) aufteilen. Die YAML-Konfiguration wird von Kibana verwendet, während die JSON-Konfiguration von ELO Analytics verwendet wird.

Die jeweiligen Konfigurationstypen bestehen aus mehreren Dateien, die zusammengefügt (in YAML und JSON) werden und damit als eine komplette Konfiguration funktionieren. Die in der nachfolgenden Tabelle angegebene Reihenfolge bestimmt, dass später gemachte Einstellungen Vorrang haben und frühere Einstellungen überschreiben (daher sind Konfigurationsdateien mit dem Wort „secrets“ am Ende der Liste).

Spezielle Konfigurationsdateien mit dem Wort "secrets" sind vorhanden, um Ihnen die Möglichkeit zu bieten Schlüssel (z. B. Kennwörter) darin zu definieren, die niemals nach außen gelangen sollen. Dadurch sind Sie z. B. einfach in der Lage die "custom"-Konfigurationen an den ELO Support zu senden, ohne auf die Schlüssel explizit achten zu müssen. Weiterhin sollten Sie die Dateziugriffsrechte minimal einstellen, sodass nur vertrauenswürdige Personen diese lesen oder sogar schreiben dürfen. Natürlich gilt dies auch für die anderen Konfigurationen. Vergessen Sie bei der Zugriffsregelung allerdings nicht die Einstellungen für den Dienst.

Reih-en-folge	Konfiguration	Typ	Beschreibung
1.	kibana.yml	YAML	Basiskonfiguration für Einstellungen von Kibana
2.	kibana.custom.yml	YAML	Konfigurationseinstellungen, welche Basiseinstellungen überschreiben und für Benutzereinstellungen zu verwenden sind.

			Fügen Sie hier Ihre Änderungen ein, um ein Überschreiben bei einem Update von ELO zu vermeiden.

3.	kibana.custom.secrets.yml	YAML	Enthält für Kibana Einstellungen, die nicht nach außen gegeben werden dürfen wie z. B.
			`elasticsearch.username: esuser`
			`elasticsearch.password: espassword`
			oder
			`elasticsearch.passwordEnc: esencpassword`
			Setzen Sie für diese Datei minimalste Zugriffsrechte, um einen unbefugten Lese-/Schreibzugriff zu unterbinden.

1.	eloAnalytics.config.json	JSON	Basiskonfiguration für Einstellungen von ELO Analytics
2.	eloAnalytics.config.custom.json	JSON	Konfigurationseinstellungen, welche Basiseinstellungen überschreiben und für Benutzereinstellungen zu verwenden sind. Fügen Sie hier Ihre Änderungen ein, um ein Überschreiben bei einem Update von ELO zu vermeiden.
3.	eloAnalytics.custom.secrets.config.json	JSON	Enthält für ELO Analytics Einstellungen, die nicht nach außen gegeben werden dürfen wie z. B. `{ "authentication": { "secret": "notAnExampleOfARandomHighEntropyString" } }` Setzen Sie für diese Datei minimalste Zugriffsrechte, um einen unbefugten Lese-/Schreibzugriff zu unterbinden.

2.3 Kibana-Konfiguration festlegen

Die Kibana-Konfigurationsdateien werden im Dienstprogramm NSSM definiert. Sie finden dort den Pfad und Namen der verwendeten Konfigurationsdatei. Sie können mit dem folgendenden Schema mehrere Konfigurationen angeben, welche in eine einzige zusammengefasst werden:

```
-c <Pfad>
```

Dabei überschreiben einzelne Einstellungen vorangegangene Werte in der Reihenfolge wie die Konfigurationen als Option angegeben worden sind.

```
-c Config1.yml -c Config2.yml -c Config3.yml
```

Im Beispiel überschreiben alle Werte in Config3.yml die Werte in Config1.yml und Config2.yml und Config2.yml überschreibt alle Werte von Config1.yml.

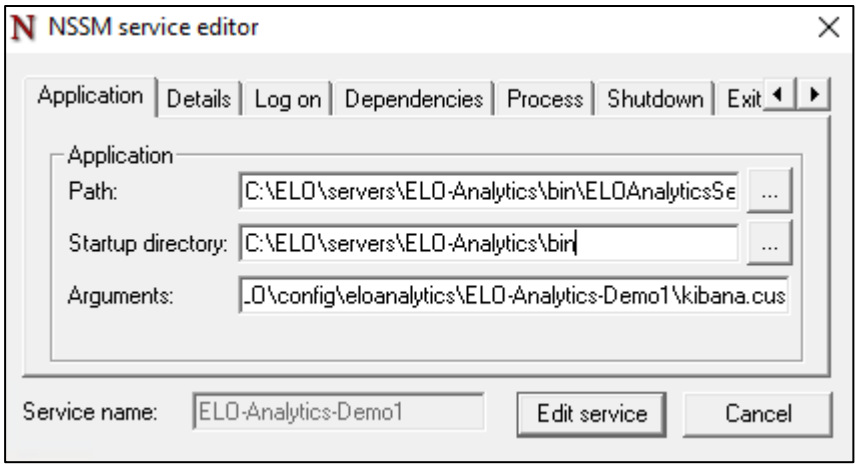


Abb. 1: NSSM service editor

Um Änderungen an der ELO Analytics-Dienstinstanz vorzunehmen, erstellen Sie sich eine Verknüpfung des Dienstwerkzeuges *nssm64.exe* innerhalb des Bin-Ordners der ELO Analytics-Installation.

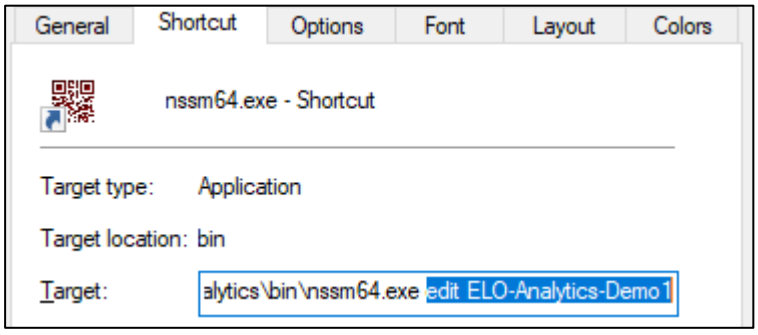


Abb. 2: Anlegen einer Verknüpfung unter Microsoft Windows

Im Windows-Verknüpfungsdialog können Sie dann den folgenden Befehl eintragen, um die Diensteigenschaften mit NSSM schneller bearbeiten zu können.

```
edit <Dienstname>
```

z. B.

```
edit ELO-Analytics-Demo1
```

3 Referenz

In diesem Kapitel werden alle Konfigurationsmöglichkeiten in einer Tabelle angegeben, die neben einer Beschreibung den Typ des Werts enthält. Zudem werden zusätzliche Bedingungen angegeben, die erfüllt sein müssen, damit der Wert als gültig erkannt wird. Wenn ein vordefinierter Wert existiert, wird dieser mitangegeben. Zudem wird für einige Werte auch ein Beispiel angegeben.

Pfad- und/oder Schlüsselname des Konfigurationseintrags	
Beschreibung	Beschreibung des Eintrags

Typ	Definiert den Typ des Wertes. Mögliche Werte sind:
	• Boolean (true oder false)
	• Zahl (0, 1, …)
	• Text / String
	  o YAML: 'Ein Text' oder Ein Text
	  o JSON "Ein Text"
	• Objekt (hier nur JSON), welches weitere Schlüssel-Wertpaare enthält
	{
	}
	• Array (Liste)
	  o YAML: ['wert', 'wert'] oder [wert, wert]
	  o JSON: ["wert", "wert"]

Bedingung	Verdeutlicht Grenzen, die für die Einstellung gelten und liefert Hinweise für Risiken und Probleme.
Default	Liefert, wenn vorhanden, den voreingestellten Wert für ELO Analytics.
Beispiel	Liefert eine Beispielkonfiguration in der Sprache/im Format der Konfiguration, entweder JSON oder YAML.

3.1 Standardkonfiguration kibana.yml

Die folgenden Konfigurationswerte werden von Kibana verwendet und durch das ELO Server Setup automatisch gesetzt. Allerdings werden nicht alle möglichen Konfigurationswerte, die mit Kibana und Plug-ins möglich sind, aufgelistet. Weitergehende Informationen finden Sie dazu direkt an der Quelle unter *https://www.elastic.co/guide/en/kibana/5.5/settings.html* Beachten Sie dabei die eingesetzte Kibana-Version wie in der technischen Dokumentation angegeben.

ELO Analytics definiert weitere Konfigurationswerte, die Sie in Abschnitt *3.3 ELO Analytics Konfigurationsreferenz* einsehen können.

> **Information**: Die Kibana-Konfiguration wird im YAML Format angegeben.
>
> Alle Änderungen in der Konfiguration erfordern, dass der ELO Analytics-Dienst neugestartet wird.

elasticSearch.password	
Beschreibung	Dieser Wert empfängt das Klartextkennwort für die Verbindung zu ElasticSearch.
Typ	String oder null (nicht definiert)
Bedingung	Verwenden Sie aus Sicherheitsgründen *elasticSearch.passwordEnc*
Default	Muss immer angegeben werden, wenn *elasticSearch.passwordEnc* nicht angegeben wurde.
Beispiel	`elasticsearch.password: <unverschlüsseltes Kennwort>`

elasticSearch.passwordEnc	
Beschreibung	Dieser Wert empfängt das verschlüsselte Kennwort für die Verbindung zu ElasticSearch. Weitere Informationen dazu finden Sie im Kapitel *4.2 Kennwortverschlüsselung in ELO Analytics konfigurieren*.
Typ	String oder null (nicht definiert)
Bedingung	Das verschlüsselte Kennwort besteht aus einer in hexadezimal kodiertem Binärcode AES 256- oder 512-Verschlüsselung. Das Kennwort kann (und sollte) kryptografischen Zufallstext vor und/oder nach dem Klartextkennwort beinhalten, damit gleiche Kennwörter nicht dieselbe Verschlüsselung ergeben können.

	Die Länge ist immer durch 16 teilbar.
Default	Muss immer angegeben werden, wenn *elasticSearch.password* nicht angegeben wurde.
Beispiel	`elasticsearch.password: <verschlüsseltes Kennwort>`

elasticSearch.requestTimeout	
Beschreibung	Definiert eine Wartezeit in Millisekunden, während der auf eine Antwort des Elasticsearch-Servers gewartet wird, bis die Abfrage fehlschlägt. Bei größeren Abfragen kann die Standardzeit von Kibana (30 Sekunden) überschritten werden. Daher wird sie in ELO Analytics auf 180 Sekunden erhöht.
Typ	Zahl
Bedingung	Die Zahl ist in Millisekunden angegeben (1s = 1000ms).
Default	180000 Millisekunden
Beispiel	`elasticsearch.requestTimeout: 180000`

elasticSearch.ssl.verificationMode	
Beschreibung	Definiert, wie und ob ELO Analytics eine HTTPS-Verbindung zum Elasticsearch-Server prüft. • none = Die Verbindung wird nicht überprüft • certificate = Das Zertifikat selbst wird auf Gültigkeit geprüft • full = Das Zertifikat und die Zertifikatskette werden auf Gültigkeit geprüft (erfordert, dass alle Zertifikatsaussteller bekannt sind)
Typ	String
Bedingung	Wird nur verwendet, wenn mit *elasticSearch.url* das HTTPS-Protokoll verwendet wird. Kann folgende Strings enthalten: • none • certificate • full

	Damit *certificate* und *full* funktionieren, müssen Sie die Konfigurationswerte *elasticSearch.ssl.key*, *elasticSearch.ssl.certificate* und ggfs. *elasticSearch.ssl.keyPassphrase* zusätzlich definieren. Weitere Informationen finden Sie dazu in der Kibana-Dokumentation unter den genannten Schlüsselnamen.
Default	none
Beispiel	`elasticsearch.ssl.verificationMode: full`

elasticSearch.url	
Beschreibung	Definiert die URL des ES-Servers
Typ	String
Bedingung	• Es muss ein Protokoll (http, https) angegeben werden. • Die URL muss gültig sein. • Es muss ein Port angegeben sein.
Default	Dieser Wert muss immer angegeben werden.
Beispiel	`elasticsearch.url: http://hostname:9200`

elasticSearch.username	
Beschreibung	Definiert den Namen des Benutzers, welcher für die Verbindung zum Elasticsearch-Server verwendet wird.
Typ	String
Bedingung	-
Default	Muss immer angegeben werden.
Beispiel	`elasticsearch.username: ESUser`

kibana.index	
Beschreibung	Definiert den Namen des Elasticsearch-Indexes, der von ELO Analytics (Kibana) verwendet wird, um Einstellungen (wie das Indexmuster) zu speichern. Wenn der Index nicht existiert, wird er erstellt. Für jedes Archiv wird ein eigener Index benötigt.
Typ	String
Bedingung	• Kibana unterscheidet Groß- und Kleinschreibung bei Indexnamen. • Der Indexname muss mit einem Punkt beginnen.

Default	Wird durch das Setup für jedes Archiv festgelegt.
Beispiel	`kibana.index: .kibana_name`

logging.dest	
Beschreibung	Definiert das Ziel der Log-Ausgaben. Dies kann entweder die Konsole sein oder eine Datei. • stdout • Pfad zur einer LogDatei
Typ	String
Bedingung	-
Default	Vom ELO Server Setup definierter Log-Pfad.
Beispiel	`logging.dest: path\logging.log`

logging.events.log	
Beschreibung	Definiert eine Liste von Log-Typen, die ausgegeben werden. Log-Meldungen erhalten Tags, die verwendet werden können, um nur bestimmte Arten von Meldungen anzuzeigen. Eine Meldung kann dabei mehrere Tags enthalten.
Typ	Array von Strings
Bedingung	-
Default	`[warning, error, fatal, elo, optimize]` Mit der Voreinstellung werden wichtige Meldungen angezeigt, sowie ELO spezifische wichtige Meldungen und der Optimierungsfortschritt beim Erststart von ELO Analytics, welcher für gewöhnlich länger dauert.
Beispiel	`logging.events.log: [warning, error, fatal, elo, optimize, elo-filter-change]`

logging.json	
Beschreibung	Definiert, ob das Logging im JSON-Format ausgegeben wird, statt Text. Wird *true* übergeben, wird jede Log-Meldung als JSON-Objekt in komprimierter Form in einer Zeile ausgegeben. Dadurch kann die Log-Ausgabe einfacher weiterverarbeitet werden.
Typ	Boolean

Bedingung	true, false
Default	true
Beispiel	`logging.json: true`

metrics.enabled	
Beschreibung	Definiert, ob die Visualisierung *Metriken* verwendet werden kann. Derzeit wird *Metriken* nicht von ELO unterstützt und muss deaktiviert bleiben.
Typ	Boolean
Bedingung	true, false
Default	false

ops.interval	
Beschreibung	Definiert, in welchem Zeitintervall System- und Prozessmetriken gesammelt werden.
Typ	Zahl
Bedingung	Eine Zahl in Millisekunden (1s = 1000ms)
Default	60 Sekunden
Beispiel	`ops.interval: 60000`

optimize.bundleDir	
Beschreibung	Definiert den Pfad zu den Bundles, der von ELO Analytics erstellt wird, um Client-Daten schneller an den Client ausliefern zu können. Der Schreibzugriff muss ELO Analytics gestattet werden.
Typ	String
Bedingung	Absoluter Pfad zu einem Verzeichnis
Default	Wird durch das ELO Server Setup definiert.
Beispiel	`optimize.bundleDir: /path/to/dir`

searchguard.basicauth.enabled	
Beschreibung	
Typ	Array von Strings
Bedingung	-

Default	
Beispiel	

searchguard.multitenancy.enabled	
Beschreibung	Definiert, ob das Plug-in *SearchGuard* mehrmandantenfähig sein soll (*true*) oder nicht (*false*).
Typ	Boolean
Bedingung	Für ELO Analytics muss dieser Wert derzeit *false* sein.
Default	false

server.basepath	
Beschreibung	Empfängt einen URL-Präfixpfad, der an von Kibana erzeugte URLs angehängt wird, um einen Proxy vor den Server schalten zu können. Der Proxy sollte vor der Weiterleitung der URL diesen Präfixpfad entfernen. Alle Serveraufrufe und Links in ELO Analytics erhalten den Basispfad zusätzlich. Beispiel: 1. Zugang über Proxy mit URL und *basePath /elo*: *http://example.com/elo/app/kibana* 2. Weiterleitung der URL über Proxy nach: *http://example.com/app/kibana* Kibana erzeugt Serveraufrufe und Links mit *basePath /elo*: *http://example.com/elo/app/kibana?parameters* Der ELO Analytics-Server (genauer Filter) entfernt selbstständig den Basispfad für Kibana, falls dieser angegeben wurde. Damit kann z. B. auch direkt über *http://localhost/elo/app/kibana* auf ELO Analytics zugegriffen werden, ohne den Proxy benutzen zu müssen.
Typ	String
Bedingung	Muss mit Slash (/) beginnen und darf nicht mit einem Slash (/) enden.
Default	/
Beispiel	`server.basepath: /elo`

server.host	
Beschreibung	Definiert den Host-Namen des Servers, auf dem ELO Analytics läuft.
Typ	String

Bedingung	Dieser Wert sollte immer *localhost* sein.
Default	localhost
Beispiel	`server.host: localhost`

server.maxPayloadBytes	
Beschreibung	Definiert die maximale Größe einer http-Anfrage an den ELO Analytics-Server. Wird die Größe der Anfrage überschritten, sendet der Server den http-Statuscode 413 („Request Entity Too Large“) zurück und ignoriert die Anfrage.
Typ	Zahl
Bedingung	-
Default	5 MiB = 5242880 Bytes
Beispiel	`server.maxPayloadBytes: 5242880`

server.name	
Beschreibung	Definiert den Namen des Kibana-Servers
Typ	String
Bedingung	-
Default	ELO Analytics
Beispiel	`server.name: ELO Analytics`

server.port	
Beschreibung	Definiert den Port des Kibana-Servers. Nicht zu verwechseln mit dem Port des ELO Analytics-Servers, der Anfragen an den Kibana-Server gefiltert weiterleitet.
Typ	Zahl
Bedingung	Der Port muss frei sein und darf nicht von außen zugänglich sein.
Default	Durch das ELOServer Setup und nach Archiv unterschiedlich.
Beispiel	`server.port: 9304`

server.ssl.certificate	
Beschreibung	Definiert den Pfad zu einer Zertifikatsdatei. ELO empfiehlt dringend einen HTTPS-Proxy stattdessen zu verwenden!
Typ	String
Bedingung	-
Default	Wird durch das ELO Server Setup definiert.
Beispiel	`server.ssl.certificate: path/to/certificate.crt`

server.ssl.enabled	
Beschreibung	Aktiviert oder deaktiviert die SSL-Verschlüsselung des ELO Analytics-Servers. Wenn die Verschlüsselung aktiviert wird, müssen weitere Eigenschaftswerte angegeben werden: • server.ssl.certificate • server.ssl.key • server.ssl.keyPassphrase/-Enc ELO empfiehlt dringend einen HTTPS-Proxy stattdessen zu verwenden!
Typ	Boolean
Bedingung	true, false
Default	Wird vom ELO Server Setup festgelegt.
Beispiel	`server.ssl.enabled: true`

server.ssl.key	
Beschreibung	Definiert den Pfad zu einem privaten Schlüssel als Datei im PEM-Format. ELO empfiehlt dringend einen HTTPS-Proxy stattdessen zu verwenden!
Typ	String
Bedingung	Der private Schlüssel muss im PEM-Format vorliegen.

Default	-
Beispiel	`server.ssl.key: path/to/private.pem`

server.ssl.keyPassphrase	
Beschreibung	Definiert ein Klartextkennwort, welches verwendet wird, um den privaten Schlüssel öffnen zu können. Das Kennwort wird nur benötigt, wenn der private Schlüssel durch ein Kennwort geschützt ist. Benutzen Sie stattdessen *server.ssl.keyPassphraseEnc*. ELO empfiehlt dringend einen HTTPS-Proxy stattdessen zu verwenden!
Typ	String
Bedingung	-
Default	-
Beispiel	`server.ssl.keyPassphrase: password`

server.ssl.keyPassphraseEnc	
Beschreibung	Definiert ein verschlüsseltes Kennwort, welches verwendet wird, um den privaten Schlüssel öffnen zu können. Das Kennwort wird nur benötigt, wenn der private Schlüssel durch ein Kennwort geschützt ist. Weitergehende Informationen zur Kennwortverschlüsselung finden Sie im Abschnitt *4.2 Kennwortverschlüsselung in ELO Analytics konfigurieren*.
Typ	String
Bedingung	-
Default	Wird durch das ELO Server Setup definiert.
Beispiel	`server.ssl.keyPassphraseEnc: <verschlüsseltes Kennwort>`

timelion.enabled	
Beschreibung	Aktiviert die Visualisierung *Timelion* in Kibana. Die Visualisierung wird derzeit nicht von ELO unterstützt und ist daher abgeschaltet.
Typ	Boolean
Bedingung	Muss *false* sein.
Default	false

3.2 ELO Analytics Konfiguration in der Datei ‚kibana.yml'

Dieser Abschnitt enthält Konfigurationsschlüssel für die Kibana-Konfigurationen, welche von ELO Analytics verwendet werden und nicht im Kibana-Standard vorkommen.

Information: Die Kibana-Konfiguration wird im YAML-Format angegeben.

eloAnalytics.enableOutputConfigsToLogs	
Beschreibung	Wenn dieser Wert true ist, werden in der Log-Ausgabe alle Konfigurationen angegeben. Dabei werden die Eigenschaften *secret*, *username* und *password* ausgenommen.
Typ	Boolean
Bedingung	-
Default	true
Beispiel	`eloAnalytics.enableOutputConfigsToLogs: true`

eloAnalytics.configs.eloAnalytics	
Beschreibung	Enthält einen Array von Dateipfaden, die JSON-Konfigurationsdateien angeben, welche für ELO Analytics-Einstellungen verwalten. Es können mehrere Konfigurationsdateien angegeben werden. Diese werden in der Reihenfolge von links (früher) nach rechts (später) zusammengeführt. Dabei überschreiben Werte späterer Konfigurationen die Früheren. Arrays werden zusammengeführt, sodass Einträge nicht direkt entfernt werden können. Die Dateien müssen existieren und dem JSON-Format entsprechen.

	Diese Konfigurationen werden von ELO bereitgestellt und können sich ändern. Benutzerdefinierte Änderungen könnten daher überschrieben werden. Beachten Sie, dass Konfigurationsnamen mit dem Wort *custom* nicht hier geladen werden können. Nutzen Sie stattdessen *eloAnalytics.configs.eloAnalyticsCustom* in *kibana.custom.yml*.
Typ	Array aus Strings
Bedingung	-
Default	-

Beispiel	`eloAnalytics.configs.eloAnalytics:`
	`['<Pfad>/config/eloAnalytics.config.json',`
	`'<Pfad>/config/eloAnalytics.custom.config.json']`
	oder
	`eloAnalytics.configs.eloAnalytics:`
	`<Pfad>/config/eloAnalytics.config.json`
	`<Pfad>/config/eloAnalytics.custom.config.json`

eloAnalytics.configs.eloAnalyticsCustom	
Beschreibung	Wie *eloAnalytics.configs.eloAnalytics*, nur werden diese Einstellungen bevorzugt behandelt und nicht von ELO überschrieben.
Typ	Array aus Strings
Bedingung	-
Default	-

Beispiel	`eloAnalytics.configs.eloAnalyticsCustom:`
	`['<Pfad>/config/eloAnalytics1.config.json',`
	`'<Pfad>/config/eloAnalytics2.custom.config.json']`
	oder
	`eloAnalytics.configs.eloAnalyticsCustom:`
	`<Pfad>/config/eloAnalytics1.config.json`
	`<Pfad>/config/eloAnalytics2.custom.config.json`

eloAnalytics.configs.eloAnalyticsSecrets	
Beschreibung	Enthält einen Array von Dateipfaden wie *eloAnalytics.configs.eloAnalytics*.

	Der Unterschied zu *eloAnalytics.configs.eloAnalytics* besteht darin, dass die Konfigurationseinstellungen innerhalb der darin angegeben Konfigurationsdateien immer gesetzt werden und nicht durch Einstellungen in *eloAnalytics.configs.eloAnalytics* oder *eloAnalyticsCustom* überschrieben werden. **Nutzen Sie den Schlüssel eloAnalytics.configs.eloAnalyticsSecrets, um separate Einstellungen für Schlüssel und Kennwörter zu erstellen, damit diese speziell geschützt werden und nicht versehentlich an unberechtigte Stellen gelangen können.** Senden Sie diese Einstellungsdateien niemals an den ELO Support oder über ein unverschlüsseltes Netzwerk!
Typ	Array aus Strings
Bedingung	-
Default	-

Beispiel	`eloAnalytics.configs.eloAnalyticsSecrets:`
	`['<Pfad>/config/eloAnalytics1.config.json',`
	`'<Pfad>/config/eloAnalytics2.custom.config.json']`
	oder
	`eloAnalytics.configs.eloAnalyticsSecrets:`
	`<Pfad>/config/eloAnalytics1.config.json`
	`<Pfad>/config/eloAnalytics2.custom.config.json`

eloAnalytics.createVerboseConfigsLogging	
Beschreibung	Wenn dieser Wert *true* ist, werden erweiterte Logging-Informationen erzeugt für den Vorgang des Zusammenführens der ELO Analytics-Konfigurationen. Weiterhin wird das Endresultat in der Datei *eloAnalytics.debug.config.merged.json* gespeichert, die im Konfig-Pfad gespeichert wird.
Typ	Boolean
Bedingung	true, false
Default	false
Beispiel	`eloAnalytics.createVerboseConfigsLogging: true`

3.3 ELO Analytics-Konfigurationsreferenz

Dieses Kapitel beschreibt die möglichen Konfigurationswerte von ELO Analytics.

> **Information**: Die ELO Analytics-Konfiguration wird im JSON-Format angegeben.

authentication.aclFilter.active	
Beschreibung	Definiert, ob ACL-Filterung von ELO Analytics-URL-Pfaden aktiviert (*true*) oder deaktiviert ist (*false*).
Typ	Boolean
Bedingung	Nur *true* erlaubt (für Debuggingzwecke)
Default	true
Beispiel	`{ "authentication" : { "accessFilaclFilter" : { "active" true } } }`

authentication.clientSSL.options	
Beschreibung	Definiert optional ein Objekt mit allen Einstellungen für einen HTTPS-Server. Mehr Informationen dazu finden Sie in der NodeJS-Dokumentation Version 6 unter *options* für *TLS.createSecureContext* und TLS.createServer
Typ	Objekt
Bedingung	-
Default	null
Beispiel	

authentication.clientSSL.rootCas	
Beschreibung	Definiert optional eine Liste von Wurzelzertifikatsdateien im PEM-Format, die verwendet werden, um bei ausgehenden HTTPS-Verbindungen Zertifikate verifizieren zu können. Sie können hier Ihre eigenen Stammzertifikate einfügen, wenn diesen nicht von öffentlichen Stellen vertraut wird.

	• Wenn Sie mit einem Wurzelzertifikat weitere Zertifikate ausstellen, können Sie das öffentliche Zertifikat (Datei) hier eintragen, um allen damit signierten Zertifikaten zu vertrauen.
Typ	Array von Pfaden (String)
Bedingung	-
Default	[]
Beispiel	`["Pfad/zu/Zertifikat1.crt", "Pfad/zu/Zertifikat2.crt"]`

authentication.clientSSL.selfSignedCertificate	
Beschreibung	Wird zu Testzwecken ein selbstsigniertes Zertifikat (server.ssl.certificate) genutzt, so muss dieser Wert auf *true* gesetzt werden, um die Verbindungen zum Server zu ermöglichen. Dies funktioniert nur, wenn Sie kein Root-Zertifikat verwenden und stattdessen mit einem einzelnen selbstsignierten Zertifikat arbeiten wollen. Wenn Sie auf die Meldung "Error: self signed certificate" stoßen und ein selbstsigniertes Zertifikat nutzen, dann setzen Sie diesen Wert auf *true*. Aus Sicherheitsgründen sollte dieser Wert immer *false* sein. Dies hat Auswirkungen auf HTTPS-Client-Verbindungen zu den Servern • Kibana-Server • ELOix.
Typ	Boolean
Bedingung	true, false
Default	false
Beispiel	`["Pfad/zu/zeritifkat1.crt", "Pfad/zu/zeritifkat2.crt"]`

authentication.clientSSL.useLatestRootCas	
Beschreibung	Wenn *true*, werden die neusten Wurzelzertifikate der ELO Analytics-Installation verwendet. Sind die Zertifikate nicht vorhanden, werden diese heruntergeladen. Der Cache befindet sich unter: `<ELO Analytics Pfad>\plugins\eloAnalytics\node_modules\ssl-root-cas\ssl-root-cas-latest.js`

	Die Cache-Datei wird heruntergeladen, falls die Datei nicht existiert. Ist der Wert *null*, werden keine Wurzelzertifikate verwendet. In diesem Fall muss der Schlüssel *rootCas* beinhalten, um Vertrauen prüfen zu können.
Typ	Boolean
Bedingung	true, false
Default	false
Beispiel	`{ "authentication": { "clientSSL": { "useLatestRootCas": false } } }`

authentication.clientSSL.verificationMode	
Beschreibung	Dieser Wert definiert, wie genau ELO Analytics HTTPS-Verbindungen zu Servern prüfen soll. • full: Dem Zertifikat muss vertraut werden und *common name* stimmt mit *hostname* überein • certificate: Dem Zertifikat muss vertraut werden und *hostname* wird nicht geprüft. Dies kann ein Sicherheitsrisiko sein! (UNSICHER!) • none: Es wird keine Prüfung der SSL-Verbindung durchgeführt. Dies ist ein Sicherheitsrisiko! (UNSICHER!) • (leerer Text): Standardwert der Umgebung wird verwendet. (UNSICHER!)
Typ	String
Bedingung	full, certificate, none, “”
Default	full
Beispiel	`{ "authentication": { "clientSSL": { "verificationMode": "full" } } }`

authentication.const	
Beschreibung	Definiert ein Objekt, welches Variablen als Name-Wert-Paare enthält. Z. B. NAME : 123 Diese Struktur wird derzeit nicht angewendet und dient nur dazu, Werte, die in der Filterkonfiguration verwendet werden, schneller in ihrer Bedeutung auflösen zu können.
Typ	Objekt mit Schlüssel-Wert-Paaren
Bedingung	Wird derzeit nicht verwendet, kann aber für *aclFilter* und *navigationsFilter* verwendet werden, um die Bedeutung der Zahlen zu erhalten.
Default	true

Beispiel	<pre>{
	  "const": {
	  "DISCOVER": 256,
	  "VISUALIZE": 512,
	  "EDIT_DASHBOARD": 1024,
	  "VIEW_DASHBOARD": 2048
	  }
	}</pre>

authentication.cookie.clearInvalid	
Beschreibung	Cookies, die zur Authentifizierung verwendet werden und deren Resultat ungültig ist, werden als abgelaufen markiert und gelöscht. Änderungen an diesem Wert erfordern einen Neustart des ELO Analytics-Diensts.
Typ	Boolean
Bedingung	-
Default	true

Beispiel	<pre>{
	  "authentication": {
	  "cookie": {
	  "clearInvalid": true
	  }
	  }
	}</pre>

authentication.cookie.encoding	
Beschreibung	Definiert die Kodierung des Cookie-Inhalts. Dieser Wert wird aktuell nicht unterstützt und muss *„none“* sein. Spätere Versionen könnten den Schlüssel unterstützen.

	Änderungen an diesem Wert erfordern einen Neustart des ELO Analytics-Diensts.
Typ	String
Bedingung	-
Default	„none“
Beispiel	`{ "authentication": { "cookie": { "encoding": „none“ } } }`

authentication.cookie.isHttpOnly	
Beschreibung	Muss *true* sein, damit Server-Cookies im Client nicht mit JavaScript ausgelesen werden können. Änderungen an diesem Wert erfordern einen Neustart des ELO Analytics-Diensts.
Typ	Boolean
Bedingung	-
Default	false
Beispiel	`{ "authentication": { "cookie": { "isHttpOnly": true } } }`

authentication.cookie.isSecure	
Beschreibung	Definiert, ob Server-Cookies nur über HTTPS-Verbindungen ausgeliefert werden dürfen (*true*) oder auch über unverschlüsselte Verbindungen (*false*). Wenn Sie *isSecure* auf *true* setzen, müssen Sie HTTPS für den ELO Analytics-Server direkt aktivieren. Ein SSL-Reverseproxy erfüllt nicht die Anforderungen. Änderungen an diesem Wert erfordern einen Neustart des ELO Analytics-Diensts.
Typ	Boolean
Bedingung	-
Default	false

Beispiel	<pre>{
	  "authentication": {
	  "cookie": {
	  "isSecure": false
	  }
	  }
	}</pre>

authentication.cookie.path	
Beschreibung	Ein URL-Pfad, der für Cookies gesetzt wird und anhand dessen erkannt wird, ob ein Cookie für die Webseite verwendet werden kann. Wird automatisch auf *server.basePath* (aus der Kibana-Konfiguration) oder '/'gesetzt, falls kein Basispfad gesetzt ist. Änderungen an diesem Wert erfordern einen Neustart des ELO Analytics-Diensts.
Typ	String
Bedingung	-
Default	Wert aus der Kibana-Konfiguration *server.basePath* oder „/“

Beispiel	<pre>{
	  "authentication": {
	  "cookie": {
	  "isSecure": false
	  }
	  }
	}</pre>

authentication.cookie.strictHeader	
Beschreibung	Dieser Wert definiert, ob das Cookie nach RFC 6265 erzeugt wird und ungültige Cookies zurückgewiesen werden. Änderungen an diesem Wert erfordern einen Neustart des ELO Analytics-Diensts.
Typ	Boolean
Bedingung	-
Default	true

Beispiel	<pre>{
	  "authentication": {
	  "cookie": {
	  "strictHeader": true
	  }
	  }</pre>

	}

authentication.ix.archive	
Beschreibung	Dieser Wert definiert den Namen des Archivs, welches verwendet werden soll. Dieser Wert wird auch als vorgeschlagenes Indexmuster beim Einrichten von ELO Analytics angegeben. **Achten Sie auf die Groß-/Kleinschreibung!** Änderungen an diesem Wert erfordern einen Neustart des ELO Analytics-Diensts.
Typ	String
Bedingung	-
Default	Dieser Wert muss immer angegeben werden.

Beispiel	`{`
	`  "authentication": {`
	`  "ix": {`
	`  "archive": “demo“`
	`  }`
	`  }`
	`}`

authentication.ix.hostName	
Beschreibung	Dieser Wert definiert den Namen oder die IP-Adresse des ELO Indexservers ohne Protokoll (http). Änderungen an diesem Wert erfordern einen Neustart des ELO Analytics-Diensts.
Typ	String
Bedingung	Host-Namen besitzen Einschränkungen in der Anzahl und Art von erlaubten Zeichen.
Default	Dieser Wert muss immer angegeben werden.

Beispiel	`{`
	`  "authentication": {`
	`  "ix": {`
	`  "hostName": “eloDemoServer“`
	`  }`
	`  }`
	`}`

authentication.ix.port	
Beschreibung	Dieser Wert definiert die Portnummer, auf der der ELO Indexserver Anfragen entgegen nimmt. Änderungen an diesem Wert erfordern einen Neustart des ELO Analytics-Diensts.
Typ	Zahl
Bedingung	“http“ oder “https“
Default	Dieser Wert muss immer angegeben werden.

Beispiel	`{`
	`  "authentication": {`
	`  "ix": {`
	`  "port": 9090`
	`  }`
	`  }`
	`}`

authentication.ix.protocol	
Beschreibung	Dieser Wert definiert den zu verwendenden Protokolltyp *HTTP* oder *HTTPS*. Änderungen an diesem Wert erfordern einen Neustart des ELO Analytics-Diensts.
Typ	String
Bedingung	“http“ oder “https“
Default	Dieser Wert muss immer angegeben werden.

Beispiel	`{`
	`  "authentication": {`
	`  "ix": {`
	`  "protocol": “http“`
	`  }`
	`  }`
	`}`

authentication.kibana.password	
Beschreibung	Dieses unverschlüsselte Kennwort wird verwendet, um eine Verbindung mit Elasticsearch herzustellen. Verwenden Sie stattdessen *elasticsearch.password* in der Kibana-Konfiguration. Änderungen an diesem Wert erfordern einen Neustart des ELO Analytics-Diensts.
Typ	String

Bedingung	Bitte nutzen Sie diesen Schlüssel nicht, wenn Sie die Konfigurationsdatei nicht vor unerlaubtem Zugriff schützen können.
Default	Verwenden Sie stattdessen *elasticsearch.password* in der Kibana-Konfiguration.
Beispiel	`{ "authentication": { "kibana": { "password": “password“ } } }`

authentication.kibana.username	
Beschreibung	Dieser Benutzername wird verwendet, um eine Verbindung mit Elasticsearch herzustellen. Verwenden Sie stattdessen *elasticsearch.username* in der Kibana-Konfiguration. Änderungen an diesem Wert erfordern einen Neustart des ELO Analytics-Diensts.
Typ	String
Bedingung	-
Default	Verwenden Sie stattdessen *elasticsearch.username* in der Kibana-Konfiguration.
Beispiel	`{ "authentication": { "kibana": { "username": “username“ } } }`

authentication.kibana.passwordEnc	
Beschreibung	Dieses verschlüsselte Kennwort wird verwendet, um eine Verbindung mit Elasticsearch herzustellen. Verwenden Sie stattdessen *elasticsearch.passwordEnc* in der Kibana-Konfiguration, da das ELO Server Setup diesen Wert anpasst. Um das Kennwort zu ändern, nutzen Sie bitte das ELO Server Setup. Weitergehende Informationen zur Kennwortverschlüsselung finden Sie im Abschnitt *4.2 Kennwortverschlüsselung in ELO Analytics konfigurieren*. Änderungen an diesem Wert erfordern einen Neustart des ELO Analytics-Diensts.

Typ	String
Bedingung	-
Default	Verwenden Sie stattdessen *elasticsearch.passwordEnc* in der Kibana-Konfiguration.

Beispiel	`{`
	`  "authentication": {`
	`  "kibana": {`
	`  "passwordEnc": “ 148ad754c4855ad183208ce828af183…“`
	`  }`
	`  }`
	`}`

authentication.navigationFilter	
Beschreibung	Enthält einen Array von Objekten, die den Zugriff auf die Einträge der Navigationsleiste prüfen und entsprechend den Benutzerrechten den Zugriff gewähren oder verweigern. Beachten Sie, dass der Benutzer über die entsprechende URL trozdem auf die entsprechende Seite gelangen kann, auch wenn sie nicht in der Leiste vorhanden ist. Die Funktionen der entsprechenden Seite sind jedoch weiterhin nicht ausführbar. Beim Ausführen einer solchen Funktion durch den Server wird der Zugriff separat geprüft. Beachten Sie den Abschnitt *4.1 Analytics ACL Filter*. Änderungen an diesem Wert erfordern einen Neustart des ELO Analytics-Diensts.
Typ	Array von Objekten
Bedingung	(voreingestellte Zugriffskontrolliste)

Default	`[…`
	`{`
	`  "$guid":"45975E93-526D-453E-A25C-AACFD6CCDD48",`
	`  "id":"kibana:discover",`
	`  "matchType":"startsWith",`
	`  "regexpOptions":"",`
	`  "user":{`
	`  "flags2":[`
	`  256`
	`  ],`
	`  "description":"flags2: DISCOVER"`
	`  },`
	`  "allow":true,`
	`  "enabled":true,`
	`  "groups":false`
	`}`
	`…`
	`]`

Beispiel	<pre>{
	  "authentication": {
	  "secret": "…"
	  }
	}</pre>

authentication.secret	
Beschreibung	Geheimer Schlüssel. Empfängt eine mindestens 48 Zeichen (384 Bits) lange, kryptografisch zufällige Zeichenfolge, welche als Schlüssel für Verschlüsselungen (Cookies, JWT) in ELO Analytics verwendet wird. Der Schlüssel muss von einer kryptografisch starken Quelle erzeugt worden sein (Zufallsgenerator). Der Schlüssel sollte von Zeit zu Zeit verändert/neu generiert werden. Wird der Schlüssel geändert, verlieren automatisch alle zuvor erstellten Cookies ihre Gültigkeit.
Typ	String
Bedingung	Mindestens 48 Zeichen kryptografischer Zufallszeichen
Default	Dieser Wert muss selbst definiert werden.

Beispiel	<pre>{
	  "authentication": {
	  "secret": "…"
	  }
	}</pre>

authentication.secretExpiration	
Beschreibung	Maximale Lebenszeit in Millisekunden für einen definierten geheimen Schlüssel. Wird die Lebenszeit überschritten, wird der geheime Schlüssel zufällig verändert. Dies passiert nur, wenn *authentication.token.invalidateTokenInCookiesAfterRestart* auf *true* gesetzt ist.
Typ	Zahl
Bedingung	Mindestens 60.000
Default	86400000 Millisekunden (entspricht 24 Stunden)

Beispiel	<pre>{
	  "authentication": {
	  "secret": "…"
	  }
	}</pre>

authentication.sessionFactoryOptions	
Beschreibung	Dieses Objekt enthält Einstellungen, die beim Aufbau einer Sitzung mit dem ELO Indexserver verwendet werden. Diese Einstellungen sind in der ELO Indexserver-Dokumentation für *IXSessionFactory* definiert. Jedoch können nicht alle Einstellungen geändert werden, da sie von ELO Analytics vorgegeben sind (z. B. Lizenzname).
Typ	Objekt
Bedingung	-
Default	-
Beispiel	`{ "authentication": { "sessionFactoryOptions": { … } } }`

authentication.token.adminBypassAccessCheck	
Beschreibung	Definiert, ob Benutzer mit privilegierten Rechten ohne Zugriffsprüfung Zugang zu eingeschränkten Bereichen in ELO Analytics sowie uneingeschränkte Sicht auf die gesamten Suchergebnisse bekommen (*true*) oder ob der Zugriff geprüft wird (*false*). Benutzer, die mit besonderen Rechten ausgestattet sind, erhalten üblicherweise vollständigen Zugriff auf ELO Analytics. Benutzer mit dem Recht *Hauptadministrator* (in der ELO Administration Console) sehen immer alle Navigationselemente (z. B. *DevTools*) auf der Oberfläche. Damit werden Zugriffsprüfungen in *authentication.navigationFilter* und *authentication.accessFilter* für den Benutzer ignoriert. Für Benutzer mit den Rechten *Hauptadministrator*, *Alle Einträge sehen*, *Berechtigungen ignorieren* oder *Skripte bearbeiten* werden Abfragen an die Elasticsearch ohne Zugriffsfilterung vorgenommen.
Typ	Boolean
Bedingung	true, false
Default	true, Benutzer mit erhöhten Rechten werden von der Zugriffskontrolle ausgenommen.
Beispiel	`{ "authentication":{ "token":{ "adminBypassAdminCheck": true } }`

	<pre> } }</pre>

authentication.token.aliveInterval	
Beschreibung	Definiert ein Intervall in Millisekunden, nach dem ein ELO Indexserver-Ticket beim Server als noch in Verwendung gemeldet wird.
Typ	Zahl
Bedingung	Mindestens 1.000 Millisekunden
Default	60.000 Millisekunden = 1 Minute

Beispiel	<pre>{
	  "authentication":{
	  "token":{
	  "aliveInterval":60000
	  }
	  }
	}</pre>

authentication.token.apiUrls (veraltet)	
Beschreibung	**Veraltet!**
Typ	Array aus Strings
Bedingung	-
Default	[“/elo“]

Beispiel	<pre>{
	  "authentication":{
	  "token":{
	  "apiUrls": […]
	  }
	  }
	}</pre>

authentication.token.cookieExpirationTime	
Beschreibung	Maximale Lebenszeit in Millisekunden für ein vom ELO Analytics-Server verwendetes Server-Cookie. Wird für ein Token die maximale Lebenszeit erreicht, wird es gelöscht und kann nicht mehr für die Anmeldung verwendet werden.
Typ	Zahl
Bedingung	Mindestens 60.000 Millisekunden
Default	86400000 Millisekunden, entspricht 24 Stunden
Beispiel	<pre>{</pre>

	<pre>{
	"authentication":{
	"token":{
	"cookieExpirationTime": 86400000
	}
	}
	}</pre>

authentication.token.eloApiTokenExpirationTime (veraltet)	
Beschreibung	**Veraltet!**
Typ	Zahl
Bedingung	Mindestens 60.000 Millisekunden
Default	86400000 Millisekunden, entspricht 24 Stunden

Beispiel	<pre>{
	"authentication":{
	"token":{
	"eloApiTokenExpirationTime": 86400000
	}
	}
	}</pre>

authentication.token.eloTokenExpirationTime (veraltet)	
Beschreibung	Maximale Lebenszeit in Millisekunden für ein im ELO Analytics-Server zwischengespeichertes Token. Wird für ein Token die maximale Lebenszeit erreicht, wird es gelöscht und vom ELO Indexserver abgemeldet. Solange der ELO Analytics-Client ein Ping sendet, wird das Token am Leben gehalten.
Typ	Zahl
Bedingung	Mindestens 60.000 Millisekunden
Default	86400000 Millisekunden, entspricht 24 Stunden

Beispiel	<pre>{
	"authentication":{
	"token":{
	"eloTokenExpirationTime": 86400000
	}
	}
	}</pre>

authentication.token.invalidateTokenInCookiesAfterRestart	
Beschreibung	Definiert, ob Cookies von einer zuvor erstellten Serverinstanz gültig bleiben (*false*) oder, ob sich ein Benutzer nach einem Serverneustart erneut anmelden muss (*true*).

Typ	Boolean
Bedingung	true oder false
Default	false, Cookies bleiben auch dann gültig, wenn der ELO Analytics-Server neu gestartet wurde.
Beispiel	`{ "authentication":{ "token":{ "invalidateTokenInCookiesAfterRestart": false } } }`

authentication.token.uiAliveIntervalTime	
Beschreibung	Definiert ein Intervall in Millisekunden, nach dem ein Client ein Ping an den ELO Analytics-Server sendet, um zu prüfen, ob der Benutzer noch ein gültiges Anmelde-Token besitzt.
Typ	Zahl
Bedingung	Mindestens 10.000 Millisekunden (10 Sekunden)
Default	10.000 Millisekunden, entspricht 10 Sekunden
Beispiel	`{ "authentication":{ "token":{ "uiAliveIntervalTime": 10000 } } }`

authentication.token.useEloTokenExpirationTime (veraltet)	
Beschreibung	**Veraltet!**
Typ	Boolean
Bedingung	true, false
Default	true, der Wert von *authentication.token.eloTokenExpirationTime* wird verwendet.
Beispiel	`{ "authentication":{ "token":{ "useEloTokenExpirationTime": true } } }`

api.v1.dashboards.defaultOwnerId	
Beschreibung	Dieser Wert wird für eine Zugriffsprüfung verwendet, wenn ein Dashboard keinen Besitzer hat. Besitzer haben immer vollen Zugriff.
Typ	Zahl
Bedingung	0…
Default	-1 (Besitzer wird nicht geprüft)
Beispiel	

api.v1.dashboards.defaultAcl	

Beschreibung	Diese ACL wird für eine Zugriffsprüfung verwendet, wenn ein Dashboard keine Sicherheitseinstellung hat.
	Einzelne Elemente können aus einer Benutzer-/Gruppen-ID bestehen oder aus einem Objekt, welches aus *allow* (*true/false*), einer Zugriffsmaske (Zahl) und einem Array aus Benutzer-/Gruppen-ID besteht.
	Die Zugriffsmaske enthält die Veroderung von einem oder mehreren dieser Zugriffswerte:
	`read: 0x1,`
	`write: 0x32,`
	`delete: 0x4`

Typ	Objekt
Bedingung	-
Default	[9999]

Beispiel	<pre>{
	"defaultAcl":[
	9999,
	{
	"allow":true,
	"mask":65535,
	"groups":[
	9999
	]
	}
	]
	}</pre>

api.v12.useEditRightForSD	
Beschreibung	Wenn dieser Wert *true* ist, ermöglicht das Recht *Write* auch den Besitzer und die ACL zu ändern, was andernfalls nur durch zwei separate Rechte möglich wäre. Aktuell werden diese Rechte nicht in der Oberfläche unterstützt.
Typ	Boolean
Bedingung	true, false
Default	true
Beispiel	

api.v12.users.cacheTimeOut	
Beschreibung	Diese Einstellung ist für den Sicherheitseditor in den Dashboards. Definiert eine maximale Zeit, die eine Suche aus dem Cache gelesen wird in Sekunden.
Typ	Zahl
Bedingung	0
Default	50 Sekunden
Beispiel	

api.v12.users.maxUsersCount	
Beschreibung	Diese Einstellung ist für den Sicherheitseditor in den Dashboards. Definiert die maximale Anzahl der Treffermenge bei der Suche von Benutzern/Gruppen, welche zurückgegeben wird.
Typ	Zahl
Bedingung	
Default	50
Beispiel	

api.v12.users.minimumFilterLength

Beschreibung	Diese Einstellung ist für den Sicherheitseditor in den Dashboards. Definiert die kleinste notwendige Suchwortlänge, die eine Suche durchgeführt wird. Dieser Wert definiert, wie viele Zeichen minimal gesucht werden müssen, damit eine Suche ein Ergebnis liefert.
Typ	Zahl
Bedingung	
Default	2
Beispiel	

clientConfiguration.columnHeaderDisplay.maxMaskCount	
Beschreibung	Definiert, wie viele Indexfeldnamen maximal in der Oberfläche dargestellt werden. Wenn mehr Indexfeldnamen (da mehrere Masken dieses Indexfeld besitzen und anders benannt haben) als diese Zahl existieren, werden keine weiteren Indexfeldnamen dargestellt und stattdessen eine Zahl der übrigen Indexfelder (z. B. bei Wert 2 und 4 Masken mit diesem Indexfeld: "IndexFeld1, Indexfeld2, +2“).
Typ	Zahl
Bedingung	1, 2, 3, …
Default	2

Beispiel	`{`
	`" clientConfiguration ": {`
	`" columnHeaderDisplay ": {`
	`"maxMaskCount": 2`
	`}`
	`}`
	`}`

clientConfiguration.columnsRename	
Beschreibung	Ein Objekt, welches aus Schlüsseln besteht, welche jeweils einer Verschlagwortungsmasken-ID entsprechen (Schlüssel als String). Jede ID definiert wiederum ein Objekt, welches den Indexfeldnamen als Schlüssel enthält und die dazugehörige Namensänderung. Dieser Wert kann ein Übersetzungsschlüssel aus der ELO Analytics-Lokalisierung (*locales\analytics_xx.properties*) sein. Es kann "*" für alle Verschlagwortungsmasken verwendet werden (dadurch ist dann keine Ausnahme von Übersetzungen für einzelne Masken mehr möglich).

	Nutzen Sie eigene Übersetzungsdateien mit *locales.path*. Diese Einstellung gilt für alle Benutzer. Benutzer können eigene Übersetzungen in *uiDefaultSettings.'elo:discover.columnsRename'* definieren, welche die Einstellungen in *clientConfiguration.columsnRename* überschreiben.
Typ	Objekt
Bedingung	-
Default	-

Beispiel	<pre>{
	"columnsRename":{
	"0":{
	"copy_of_all_title":"ELO_TITLE",
	"title_none":"Title"
	}
	}
	}</pre>

clientConfiguration.dateStringMapping	
Beschreibung	Ein Array aus Strings, der Datumsformatdefinitionen der JavaScript-Bibliothek *Moment JS* verwendet, um Datumswerte in Texten zu erkennen. Damit werden Datumstexte, die in ELO Analytics eingegeben oder angezeigt werden sollen, in das vom Benutzer verwendete Format konvertiert.
Typ	Array aus Strings
Bedingung	Die angegeben Strings müssen dem Format *moment.js* entsprechen.
Default	['L', 'L LT', 'L LTS', 'YYYYMMDDHHmmss']

Beispiel	<pre>{
	"clientConfiguration": {
	"dateStringMapping": [‘L‘]
	}
	}</pre>

clientConfiguration.fieldDisplaynameSeparator	
Beschreibung	Definiert ein Trennzeichen für die Darstellung von Indexfeldnamen mehrerer Masken (Indexfeld1, Indexfeld2, +1) in der Oberfläche.
Typ	String
Bedingung	Die angegeben Strings müssen dem Format *moment.js* entsprechen.
Default	','

Beispiel	<pre>{
	  "clientConfiguration": {
	  "fieldDisplaynameSeparator": ‘,‘
	  }
	}</pre>

clientConfiguration.javaClient	
Beschreibung	Wenn ELO Analytics im ELO Java Client ausgeführt wird, können bestimmte Funktionen in ELO Analytics zu fehlerhaftem Verhalten der Java Runtime Engine führen. Diese Funktionen können für den ELO Java Client deaktiviert werden (*false*). Wenn sie deaktiviert sind, wird dem Benutzer stattdessen eine Meldung angezeigt, wie man die Funktion im Browser nutzen kann. • "management.import": true | false Deaktiviert (*false*) den Import von gespeicherten Objekten unter *Management*. **Beachten Sie:** Wenn dieser Wert *true* ist, kann der Import zum Absturz des ELO Java Clients führen!
Typ	Objekt
Bedingung	Nur bestimmte Eigenschaften sind erlaubt. • "management.import"
Default	-

Beispiel	<pre>{
	  "clientConfiguration": {
	  "javaClient": {
	  "management.import": false
	  }
	  }
	}</pre>

clientConfiguration.jsonMixin	
Beschreibung	Definiert, ob im Client das JSON-Objekt um die Methode *stringifyCycle* erweitert wird (*true*) oder nicht (*false*). Wenn im Client in der Konsole Meldungen dazu ausgegeben werden, kann Mixin deaktiviert werden (*false*). Änderungen an diesem Eigenschaftswert sind nur erforderlich, wenn ein verwendeter Browser es nicht zulässt, dass das JSON-Objekt verändert werden kann.
Typ	Boolean
Bedingung	Nur bestimmte Eigenschaften sind erlaubt. "management.import"
Default	-

Beispiel	`{`
	`  "clientConfiguration": {`
	`  "javaClient": {`
	`  "management.import": false`
	`  }`
	`  }`
	`}`

filter.httpHandling.payloadLimit	
Beschreibung	Definiert eine Obergrenze für HTTP-Anfragen an den Filter. Diese Obergrenze beschränkt die Datenlast auf die angegebene Anzahl von Bytes. Der String ist eine Zahl gefolgt von „b“, „kb“ oder „mb“, welche die Zahl mit dem jeweiligen Faktor (1, 1024, 1024^2) multipliziert. Diese Einstellung muss auch in der Datei *kibana.yml* vorgenommen werden, unter der Konfiguration *server.maxPayloadBytes*, welche eine Zahl in Bytes entgegennimmt.
Typ	String
Bedingung	-
Default	Verwendet die Einstellung von Kibana server.maxPayloadBytes

Beispiel	`{`
	`  "filter": {`
	`  "httpHandling": {`
	`  "payloadLimit": "10mb"`
	`  }`
	`  }`
	`}`

filter.proxy.basePath	
Beschreibung	Definiert einen Basispfad, der aus dem Beginn der URL entfernt wird, um ELO Analytics auch über den lokalen Server aufrufen zu können, wenn ein Proxy und damit Basepath in Kibana verwendet wird. Der Wert wird, wenn nicht vorhanden oder null, aus der Kibana-Konfiguration *server.basePath* genommen. Der Wert muss mit einem Schrägstrich (/) beginnen und darf nicht mit einem Schrägstrich enden. Wenn der Wert ein leerer String ist (""), dann wird die Umleitungsfunktion deaktiviert. Beachten Sie, dass bei dem Basispfad in der URL auf Groß- und Kleinschreibung geachtet wird. Andernfalls wird eine HTTP-404-Meldung (File not found) geliefert.
Typ	String
Bedingung	-
Default	Verwendet die Einstellung von Kibana server.basePath

Beispiel	`{`
	`  "filter": {`
	`  "proxy": {`
	`  "basePath": "…"`
	`  }`
	`  }`
	`}`

filter.proxy.host	
Beschreibung	ELO Analytics-Filter für den Servernamen des IP-Adapters, auf dem der Server mit Port *proxy.port* gestartet wird und auf dem der Server auf Anfragen reagiert. Wenn nicht definiert, wird das unspezifische Interface verwendet (IPv4 0.0.0.0, IPv6 ::).
Typ	String
Bedingung	-
Default	Alle IP-Adressen

Beispiel	`{`
	`  "filter": {`
	`  "proxy": {`
	`  "host": "…"`
	`  }`
	`  }`
	`}`

filter.proxy.port	
Beschreibung	Definiert neben *filter.proxy.host* die Portnummer auf welcher der Filterserver horcht.
Typ	Zahl
Bedingung	Darf nicht 443 sein.
Default	9300
Beispiel	`{ "filter": { "proxy": { "port": 9300 } } }`

filter.proxy.remote	
Beschreibung	String im Format "<hostname>:<port>". Definiert Server und Port, auf dem der Kibana-Server läuft. Dieser Wert ist abhängig von *server.host* und *server.port* aus der Konfigurationsdatei *kibana.yml*.
Typ	String
Bedingung	Muss im Format "<hostname>:<port>" sein.
Default	Verwendet automatisch nachfolgende Einstellungen von Kibana und muss nicht angegeben werden. • server.host • server.port
Beispiel	`{ "filter": { "proxy": { "remote": "localhost:9304" } } }`

filter.proxy.ssl.forceProxySSL	
Beschreibung	Wenn der Wert *true* eingestellt ist, dann erstellt ELO Analytics einen HTTPS-Server auch, wenn die Kibana-Konfiguration *server.ssl.enabled* auf *false* steht. In diesem Fall ist die Verbindung zwischen ELO Analytics und Kibana unverschlüsselt und die Verbindung zwischen Client und ELO Analytics verschlüsselt. Dabei werden die Schlüssel *server.ssl.key* und das Zertifikat *server.ssl.certificate* verwendet. Wenn dieser Wert *false* ist, wird ein normaler http-Server erstellt.
Typ	Boolean
Bedingung	true, false
Default	true
Beispiel	`{ "filter":{ "proxy":{ "ssl":{ "forceProxySSL":true } } } }`

filter.proxy.ssl.serverOptions	
Beschreibung	Definiert optional ein Objekt mit allen Einstellungen für einen HTTPS-Server. Mehr Informationen dazu finden Sie in der NodeJS-Dokumentation Version 6 unter *options* für *TLS.createSecureContext* und *TLS.createServer*.
Typ	Objekt
Bedingung	-
Default	{}

locales.defaultLocale	
Beschreibung	ISO 639-1/2 Sprachcode. Dieser Code wird nur dann verwendet, wenn die Sprache des Benutzers nicht erkannt wurde. Werden in einer URL ungültige Sprachcodes verwendet, wird der oben genannte Sprachcode als Standard genommen. Diese Einstellung gilt nur für Texte von ELO Analytics und gilt nicht für Texte von Kibana und dem ELO Indexserver (Felder, Masken).
Typ	String

Bedingung	Nur gültige Sprachkürzel sind erlaubt.
Default	en

Beispiel	`{`
	`  "locales": {`
	`  "defaultLocale": "en"`
	`  }`
	`}`

locales.path	
Beschreibung	Pfad zu einem Ordner, in dem Lokalisierungsdateien liegen. Die Dateinamen sind im Format *analytics_X.properties*, wobei „X" einen ISO 639-1/2 (en, de, …) Sprachcode definiert. Sie können eigene Lokalisierungsdateien im Format *analytics_XXX.properties* erstellen und den Ordner dann im Pfad angeben (siehe Beispiel). Einzelne Übersetzungsschlüssel werden von den eigenen und gleichnamigen Übersetzungsschlüsseln überschrieben. Es können beliebig viele Pfade angegeben werden.
Typ	Array oder String
Bedingung	Backsalshes (\) müssen doppelt angegeben werden (\\)
Default	Ein leerer String im Array verwendet die Standardlokalisierung, welche von den eigenen Lokalisierungen erweitert bzw. überschrieben wird.

Beispiel	`{`
	`  "locales": {`
	`  "path": ["", "<PFAD>\\custom_locales"]`
	`  }`
	`}`

logging.AccessCheckVerbose	
Beschreibung	Dieses Flag, wenn *true*, gibt detaillierte Informationen zur Zugriffsprüfung des Clients in der Konsole aus.
Typ	Boolean
Bedingung	true, false
Default	false

Beispiel	`{`
	`  "logging": {`
	`  "AccessCheckVerbose": true`
	`  }`
	`}`

logging.logFilterRequestsPath	
Beschreibung	Definiert einen Pfad zu einem Ordner, worin erweiterte DEBUG-Logs ausgegeben werden, welche die von den ELO Filtern angepasste Kibana-Query enthalten. Diese enthält damit die Information, wie die Elasticsearch tatsächlich abgefragt wird und kann für Debug-Zwecke genutzt werden. Der Ordner enthält Dateien im Format *filterQueryDEBUG_X.txt,* wobei „X" eine aufsteigende Zahl beginnend bei 1 ist. Wenn der ELO Analytics-Server neugestartet wird, beginnt es wieder bei 1 und die Dateien werden überschrieben. Änderungen an diesem Wert erfordern einen Neustart des ELO Analytics-Diensts.
Typ	String
Bedingung	Backslashes (\) müssen doppelt angegeben werden (\\)
Default	(durch das Setup festgelegt)

Beispiel	`{`
	`  "logging": {`
	`  "logFilterRequestsPath": "path\\to\\logs"`
	`  }`
	`}`

uiDefaultSettings	
Beschreibung	Definiert eine JSON-Struktur als String zum Umbenennen von Feldern. Siehe *clientConfiguration.columsnRename*.
Typ	Zahl Objekt Array String
Bedingung	1, 2, 3, …
Default	2

Beispiel	`{`
	`  "uiDefaultSettings": {`
	`  "columnHeaderDisplay": {`
	`  "maxMaskCount": 2`
	`  }`
	`  }`
	`}`

search.docValuesExclude	
Beschreibung	Ein String aus einem regulären Ausdruck, der angibt, welche Werte in der Elasticsearch-Query in der Eigenschaft *docvalue_fields* nicht erlaubt sind. Kann leer oder undefiniert sein, um ignoriert zu werden.
Typ	String
Bedingung	Der String muss ein regulärer Ausdruck sein.
Default	leerer String
Beispiel	`{ "search": { "docValuesExclude": "name|name2|name3" } }`

search.docValuesInclude	
Beschreibung	Ein String aus einem regulären Ausdruck, der angibt, welche Werte in der Elasticsearch-Query in der Eigenschaft *docvalue_fields* erlaubt sind. Kann leer oder undefiniert sein, um ignoriert zu werden.
Typ	String
Bedingung	Der String muss ein regulärer Ausdruck sein.
Default	leerer String
Beispiel	`{ "search": { "docValuesInclude": "name|name2|name3" } }`

search.eloIndexNamePattern	
Beschreibung	Zur Abbildung von Elasticsearch-Indexnamen auf Archivnamen. Dazu wird der zweite reguläre Ausdruck (result[1]) ausgewertet (daher ist ((.+)) in zwei Klammern). Dieser beinhaltet den Archivnamen (archiv_12). **Beachten Sie:** Bei neuren Versionen (ab ELO 11) des ELO Indexservers weden Pilcrow-Zeichen statt Unterstrichen verwendet. Änderungen an diesem Wert erfordern einen Neustart des ELO Analytics-Dienstes.
Typ	String

Bedingung	Der String muss ein regulärer Ausdruck sein. Jeder Teilausdruck (getrennt durch |) muss mindestens zwei Gruppen (eingeschlossen durch Klammern) besitzen. Die erste Gruppe ermittelt den Maskennamen und die zweite Gruppe die Masken-ID.
Default	`"^(.+)\\u00B6(\\d+)$\|^(.+)_(\\d+)$|^((.+))$"` Damit werden Elasticsearch-Indexnamen gefunden, die zum Namen ihre Masken-ID durch ¶ oder _ getrennt besitzen. Alternativ wird der gesamte Name verwendet.
Beispiel	`{ "search": { "elIndexNamePattern": " '(.+)_(\\d+)$|((.+))' " } }`

search.esDateFormat	
Beschreibung	Definiert einen Moment.js-Formatstring, welcher verwendet wird, um Elasticsearch-Abfragen bei Datumsfeldern zu korrigieren. Datumseingaben, die in einer Abfrage vom Benutzer erstellt werden, werden in das angegebene Format konvertiert, welches von der Elasticsearch bei Datumsfeldern verwendet wird. Wenn dieser Wert *null* ist, wird für Elasticsearch-Datumsfelder der Unix-Timestamp (in Millisekunden) als Zahl in der Elasticsearch-Abfrage verwendet.
Typ	String, null
Bedingung	Der String muss Moment.js-Datumsformatzeichen enthalten oder *null* sein.
Default	"YYYYMMDD000000"
Beispiel	`{ "search": { "esDateFormat": null } }`

search.esDateFormatAggregation	
Beschreibung	Definiert einen Moment.js.-Formatstring, welcher verwendet wird, um Elasticsearch-Abfragen bei Datumsfeldern in Aggregationen mit Visualisierungen zu korrigieren. Datumseingaben, die in einer Abfrage vom Benutzer erstellt werden, werden in das angegebene Format konvertiert, welches von der Elasticsearch bei Datumsfeldern verwendet wird.

	Wenn dieser Wert *null* ist, wird für Elasticsearch-Datumsfelder der Unix-Timestamp (in Millisekunden) als Zahl in der Elasticsearch-Abfrage verwendet.
Typ	String, null
Grenzen	Der String muss Moment.js-Datumsformatzeichen enthalten oder *null* sein.
Default	"YYYYMMDD000000"
Beispiel	`{ "search": { "esDateFormatAggregation": null } }`

search.fieldMappingsExclude	
Beschreibung	Ein String aus einem regulären Ausdruck, der angibt, welche ELO Indexfelder nicht für die Suche verwendet werden sollen. Änderungen an diesem Wert erfordern einen Neustart des ELO Analytics-Diensts.
Typ	String
Grenzen	Der String muss ein regulärer Ausdruck sein.
Default	`"^(acl-allow|_..|_none|parentids|sord_deleted|sord_(i|v|desc).+|language|_guid)"`
Beispiel	`{ "search": { "fieldMappingsExclude": „“ } }`

search.maskExclude	
Beschreibung	Array aus regulären Oder-Ausdrücken, die *MaskenId*, *MaskenGUID* oder *MaskenName* enthalten können. Diese Masken werden nicht für die Aufzählung von Indexfeldern verwendet. Elasticsearch-Felder werden in der ELO Analytics-Oberfläche nicht in ELO Feldnamen umgewandelt. Für *MaskGuid* muss eine Klammer verwendet werden. Diese muss für den regulären Ausdruck als Literal definiert werden, indem ein Backslash (\) davorgesetzt wird. Da JSON dies als Escape-Zeichen interpretiert, müssen Sie doppelte Backslashes verwenden.
Typ	String

Grenzen	Der String muss ein regulärer Ausdruck sein.
Default	`"\\(E10E1000-E100-E100-E100-E10E10E10E35\\)"` Beachten Sie, dass die Klammern mit Backslash (\) maskiert werden müssen. Weil es ein JSON-String ist, muss dazu der Backslash zusätzlich mit einem weiteren Backslash maskiert werden.
Beispiel	`{ "search": { "maskExclude": "\\(E10E1000-E100-E100-E100-E10E10E10E35\\)|Maskname|MaskId" } }`

search.maskReloadCache	
Beschreibung	Eine Anzahl von Anfragen, die für einen Benutzer eingehen müssen, bis die Verschlagwortungsmasken erneut vom ELO Indexserver angefordert werden. Wenn die Sprache geändert wird (URL mit Query *lang=XX*), wird der Cache zurückgesetzt und die Verschlagwortungsmasken neu geladen. Wenn dieser Wert *0* ist, wird der Cache komplett deaktiviert und die Verschlagwortungsmasken jedes mal neu geladen. Wenn dieser Wert *null* ist, wird immer auf den Cache zurückgegriffen, außer die Sprache wird geändert. Beachten Sie, dass ein aktiver Cache verhindert, dass die Masken in der Discover-Ansicht aktualisiert werden können, wenn das Indexmuster sich geändert hat! Ein Administrator verwendet den Cache nicht, um im Management die Indexmuster anpassen zu können. Nach Änderungen müssen Benutzer sich neu anmelden oder mehrmals die Discover-Ansicht laden, um eine Änderung anzuwenden.
Typ	Zahl
Grenzen	positive Ganzzahlen oder null
Default	5
Beispiel	`{ "search": { "maskReloadCache": 5 } }`

search.storedFieldsExclude	
Beschreibung	Ein String aus einem regulären Ausdruck, der angibt, welche Werte in der Elasticsearch-Query in der Eigenschaft *stored_fields* nicht erlaubt sind. Kann leer oder undefiniert sein, um ignoriert zu werden.
Typ	String
Grenzen	Der String muss ein regulärer Ausdruck sein.
Default	leerer String
Beispiel	`{ "search": { "storedFieldExclude": "name|name2|name3" } }`

search.storedFieldsInclude	
Beschreibung	Ein String aus einem regulären Ausdruck, der angibt, welche Werte in der Elasticsearch-Query in der Eigenschaft *stored_fields* erlaubt sind. Kann leer oder undefiniert sein, um ignoriert zu werden.
Typ	String
Grenzen	Der String muss ein regulärer Ausdruck sein.
Default	leerer String
Beispiel	`{ "search": { "storedFieldInclude": "name|name2|name3" } }`

uiDefaultSettings.'elo:discover.columnsRename'	
Beschreibung	Die Eigenschaft *uiDefaultSettings* überschreibt die Benutzereinstellungen in Kibana (unter *Management*) mit den angegeben Werten. Zu beachten ist, dass einige Werte JSON-Objekte/Arrays sind, die als String übergeben werden müssen. U. a. sind folgende Eigenschaften verfügbar: • elo:discover.columnsRename Definiert eine JSON-Struktur als String zum Umbenennen von Feldern. Siehe *clientConfiguration.columsnRename*

	• elo:discover.quickCount Definiert ein Objekt mit Wert. Nehmen Sie die JSON aus dem hier angegeben Beispiel, um den Wert anzupassen. Der Wert beschreibt die maximale Anzahl von angezeigten Werten eines Indexfelds in *Discover*, wenn Sie das Indexfeld in der Leiste ausklappen. Beachten Sie, dass die angezeigten Werte nur von den gefundenen und in ELO Analytics geladenen Ergebnissen abhängen. Daher kann es sein, dass nicht alle Werte dargestellt werden, auch wenn *quickcount* hochgesetzt wird. Filtern Sie dazu die am meisten auftauchenden Werte aus, um mehr Ergebnisse sehen zu können.
Typ	Objekt
Grenzen	-
Default	Die Voreinstellungen sind von ELO Analytics intern gegeben.
Beispiel	`"uiDefaultSettings":{ "elo:discover.quickCount":{ "descriptionLocale":"UISETTINGS.DISCOVER.QUICKCOUNT.DESCRIPTION", "value":25 }, "elo:discover.searchEloFieldNames":{ "descriptionLocale":"UISETTINGS.DISCOVER.SEARCH_ORIGINAL_FIELD_NAMES.DESCRIPTION", "value":false }, "elo:discover.columnsRename":{ "value":"{\"*\":{\"yourFullESFieldname\":\"Renamed field name\"}}" }, "query:queryString:options":{ "value":"{\"analyze_wildcard\": false, \"allow_leading_wildcard\" : true, \"all_fields\" : true, \"lenient\": true, \"default_operator\": \"and\", \"auto_generate_phrase_queries\":true}" }, "dateFormat:scaled":{ "value":"[[\"\",\"HH:mm:ss.SSS\"],[\"PT1S\",\"HH:mm:ss\"],[\"PT1M\",\"HH:mm\"],[\"PT1H\",\"LHH:mm\"],[\"P1DT\",\"L\"],[\"P1YT\",\"YYYY\"]]" },`

```
  "defaultColumns":{
     "value":[
        "copy_of_all_title"
     ]
  },

  "discover:sampleSize":{
     "value":1000
  }
}
```

3.4 Vollständige ELO Analytics-Konfiguration (Beispiel)

Im Folgenden wird eine beispielhafte, vollständige Konfiguration angegeben. Sie muss nicht den Standardeinstellungen entsprechen.

Die vollständige Konfigurationsdatei können Sie selbst erzeugen, indem die Datei *kibana.yml* (oder Custom Konfiguration) um folgenden Eintrag erweitert wird:

```
eloAnalytics.createVerboseConfigsLogging: true
```

Wenn der Wert *true* ist, wird die Datei *eloAnalytics.debug.config.merged.json* angelegt. Sie enthält alle gesammelten ELO Analytics-Einstellungen. Dazu benötigt der ELO Analytics-Server jedoch Schreibrechte auf den ELO Analytics-Ordner *config*.



Information: Die Kibana-Konfigurationen (YAML) können nicht zusammengefasst ausgeben werden.

```
{
   "uiDefaultSettings":{
      "elo:discover.quickCount":{
         "descriptionLocale":"UISETTINGS.DISCOVER.QUICKCOUNT.DESCRIPTION",
         "value":25
      },
      "elo:discover.searchEloFieldNames":{

"descriptionLocale":"UISETTINGS.DISCOVER.SEARCH_ORIGINAL_FIELD_NAMES.DESCRIPTION",
         "value":false
      },
      "elo:discover.columnsRename":{
         "value":"{\"*\":{\"yourFullESFieldname\":\"Renamed field name\"}}"
      },
      "query:queryString:options":{
         "value":"{\"analyze_wildcard\": false, \"allow_leading_wildcard\" : true,
\"all_fields\" : true, \"lenient\": true, \"default_operator\": \"and\",
\"auto_generate_phrase_queries\":true}"
```

```
      },
      "dateFormat:scaled":{

"value":"[[\"\",\"HH:mm:ss.SSS\"],[\"PT1S\",\"HH:mm:ss\"],[\"PT1M\",\"HH:mm\"],[\"P
T1H\",\"L HH:mm\"],[\"P1DT\",\"L\"],[\"P1YT\",\"YYYY\"]]"
      },
      "defaultColumns":{
         "value":[
            "copy_of_all_title"
         ]
      },
      "discover:sampleSize":{
         "value":1000
      }
   },
   "logging":{
      "AccessCheckVerbose":false,
      "logFilterRequestsPath":"E:\\ELO\\ELO Analytics 11\\logs"
   },
   "clientConfiguration":{
      "dateStringMapping":[
         "YYYY-MM-DD",
         "YYYYMMDDHHmmss",
         "YYYYMMDD",
         "L",
         "L LT",
         "L LTS"
      ],
      "columnsRename":{
         "0":{
            "copy_of_all_title":"ELO.FIELDS_NAMES.RENAME.COPY_OF_ALL_TITLE",
            "LINE_ELO_FNAME":"ELO.FIELDS_NAMES.RENAME.FNAME"
         }
      },
      "javaClient":{
         "management.import":false
      },
      "fieldDisplaynameSeparator":", ",
      "columnHeaderDisplay":{
         "maxMaskCount":2
      },
      "jsonMixin":true
   },
   "search":{
      "fieldMappingsExclude":"^(acl-
allow|_..|_none|parentids|sord_deleted|sord_(i|v|desc).+|language|_guid)",
      "maskExclude":"\\(E10E1000-E100-E100-E100-E10E10E10E35\\)",
      "docValuesExclude":"^(title_.+)",
      "storedFieldsInclude":"^(title_..+)",
      "maskReloadCache":null,
      "eloIndexNamePattern":"(.+)_(\\d+)$",
      "docValuesInclude":"",
      "storedFieldsExclude":"",
      "esDateFormat":"YYYYMMDD000000",
      "esDateFormatAggregation":null
   },
   "authentication":{
```

```
      "sessionFactoryOptions":{
         "ix.translateTerms":true
      },
      "cookie":{
         "path":"/",
         "encoding":"none",
         "isSecure":false,
         "isHttpOnly":true,
         "clearInvalid":true,
         "strictHeader":true
      },
      "token":{
         "invalidateTokenInCookiesAfterRestart":false,
         "aliveInterval":10000,
         "adminBypassAccessCheck":true,
         "cookieExpirationTime":86400000,
         "uiAliveIntervalTime":60000
      },
      "aclFilter":{
         "active":true
      },
      "error":{
         "401":{
            "redirect":""
         }
      },
      "accessFilter":[
         {
            "$guid":"ADF68B8A-8BDD-403D-91C2-DB2CBA01B397",
            "description":"ELO 1 API. This url is restricted by the given ticket",
            "action":[
               "GET",
               "POST",
               "PUT"
            ],
            "url":"/elo/1/api",
            "matchType":"startsWith",
            "allow":true,
            "enabled":true,
            "regexpOptions":"",
            "groups":false,
            "user":{

            }
         },
         {
            "$guid":"403EA38F-C7E2-4E7C-99F8-E4DBC6E41BAF",
            "enabled":false,
            "description":"Access of console plugin and executing console commands
allow only to admins. This ACE is disabled unless it shall be active for other
groups.",
            "action":[
               "GET",
               "POST",
               "PUT",
               "DELETE"
            ],
```

```
            "url":"/api/console",
            "matchType":"startsWith",
            "groups":[
               0
            ],
            "allow":true,
            "regexpOptions":"",
            "user":{

            }
         },
         {
            "$guid":"83C593B1-EBE1-48BD-A28A-E111E1941565",
            "description":"Returns general SENSE information.",
            "action":[
               "GET"
            ],
            "url":"/api/console/api_server?",
            "matchType":"startsWith",
            "allow":true,
            "enabled":true,
            "regexpOptions":"",
            "groups":false,
            "user":{

            }
         },
         {
            "$guid":"0AE92AFF-FB71-42EA-BDB0-D95A458023C7",
            "enabled":false,
            "description":"Allow using scripts in index patterns editor. This ACE
is disabled unless it shall be active for other groups.",
            "action":[
               "GET"
            ],
            "url":"/api/kibana/scripts",
            "matchType":"startsWith",
            "groups":[

            ],
            "allow":true,
            "regexpOptions":"",
            "user":{

            }
         },
         {
            "$guid":"30DDFAB2-2310-41C7-8B67-B59B236DE741",
            "description":"Allow accessing index details.",
            "action":[
               "GET"
            ],
            "url":"^/api/kibana/.+/(field_capabilities)",
            "matchType":"regexp",
            "allow":true,
            "enabled":true,
            "regexpOptions":"",
```

```
            "groups":false,
            "user":{

            }
         },
         {
            "$guid":"AD501876-2CAC-46B8-9492-2D24CD6FF3D2",
            "enabled":false,
            "description":"Allow writing index details. This ACE is disabled unless
it shall be active for other groups.",
            "action":[
               "GET",
               "POST",
               "DELETE"
            ],
            "url":"^/api/kibana/.+/(field_capabilities)",
            "matchType":"regexp",
            "groups":[

            ],
            "allow":true,
            "regexpOptions":"",
            "user":{

            }
         },
         {
            "$guid":"37207E2C-839C-417D-B5D5-EA8E591478F3",
            "description":"Read index mapping.",
            "action":[
               "GET"
            ],
            "url":"^/(elasticsearch|es_admin)/.+/_mapping",
            "matchType":"regexp",
            "regexpOptions":"i",
            "allow":true,
            "enabled":true,
            "groups":false,
            "user":{

            }
         },
         {
            "$guid":"95D0AC87-F594-49CB-B768-6A1B034224FA",
            "description":"List access to saved Dashboards. Necessary, since client
generates exception in  Management/Kibana/SavedObject.",
            "action":[
               "POST"
            ],
            "url":"^/es_admin/\\..+/dashboard/_search",
            "matchType":"regexp",
            "regexpOptions":"i",
            "allow":true,
            "enabled":true,
            "groups":false,
            "user":{
```

```
            }
         },
         {
            "$guid":"E771AECE-3546-40C4-99EB-795512FE9BC7",
            "description":"Read access to saved Dashboards details. Kibana does a
GET on the resource first before displaying details.",
            "action":[
               "GET"
            ],
            "url":"/es_admin/\\..+/dashboard",
            "matchType":"regexp",
            "regexpOptions":"i",
            "allow":true,
            "enabled":true,
            "groups":false,
            "user":{

            }
         },
         {
            "$guid":"DEA4CA11-D8D2-40BF-8BA9-7E1AF68F05C3",
            "description":"Create new Dashboard or edit/save a dashboard.",
            "action":[
               "POST",
               "PUT",
               "DELETE"
            ],
            "url":"/es_admin/\\..+/(dashboard|_mapping/dashboard)",
            "matchType":"regexp",
            "regexpOptions":"i",
            "user":{
               "flags2":[
                  1024
               ],
               "description":"flags2: EDIT_DASHBOARD "
            },
            "allow":true,
            "enabled":true,
            "groups":false
         },
         {
            "$guid":"25646848-1A1B-49BA-A76C-6A080DB17D28",
            "description":"List access to saved searches.",
            "action":[
               "POST"
            ],
            "url":"/es_admin/\\..+/search/_search",
            "matchType":"regexp",
            "regexpOptions":"i",
            "allow":true,
            "enabled":true,
            "groups":false,
            "user":{

            }
         },
         {
```

```
            "$guid":"FF3EDE68-CE90-4566-A6CB-02E5EB717E4B",
            "description":"Read access to saved searches details. Kibana does a GET
on the resource first before displaying details.",
            "action":[
               "GET"
            ],
            "url":"/es_admin/\\..+/search",
            "matchType":"regexp",
            "regexpOptions":"i",
            "allow":true,
            "enabled":true,
            "groups":false,
            "user":{

            }
         },
         {
            "$guid":"B88B6524-813B-4124-A6CF-D3C258B3A57B",
            "description":"Write access to saved searches.",
            "action":[
               "POST",
               "DELETE"
            ],
            "url":"/es_admin/\\..+/search",
            "matchType":"regexp",
            "regexpOptions":"i",
            "user":{
               "flags2":[
                  256
               ],
               "description":"flags2: DISCOVER "
            },
            "allow":true,
            "enabled":true,
            "groups":false
         },
         {
            "$guid":"73CCBC4D-7E15-45EB-AC70-838DB9FC13BC",
             "description":"List access to saved visualizations. Das ist
aktuell notwendig, da sonst der Client Ausnahmefehler unter
Management/Kibana/SavedObject generiert.",
            "action":[
               "POST"
            ],
            "url":"/es_admin/\\..+/visualization/_search",
            "matchType":"regexp",
            "regexpOptions":"i",
            "allow":true,
            "enabled":true,
            "groups":false,
            "user":{

            }
         },
         {
            "$guid":"3D024CEF-54AC-4C54-80E4-DD44AEB593AD",
            "description":"Read access to saved visualization details.",
```

```
            "action":[
               "GET"
            ],
            "url":"/es_admin/\\..+/visualization",
            "matchType":"regexp",
            "regexpOptions":"i",
            "allow":true,
            "enabled":true,
            "groups":false,
            "user":{

            }
         },
         {
            "$guid":"A76E3930-6299-49B4-B754-A714A5A898F0",
            "description":"Write access to saved visualizations.",
            "action":[
               "GET",
               "PUT",
               "POST",
               "DELETE"
            ],
            "url":"/es_admin/\\..+/(visualization|_mapping/visualization)",
            "matchType":"regexp",
            "regexpOptions":"i",
            "user":{
               "flags2":[
                  512
               ],
               "description":"flags2: VISUALIZE "
            },
            "allow":true,
            "enabled":true,
            "groups":false
         },
         {
            "$guid":"D8815513-954A-498E-82AA-6960DFFED574",
            "description":"Used by Discover Search for searching.",
            "action":[
               "GET",
               "POST"
            ],
            "url":"^/(elasticsearch|es_admin)/\\..+/(_msearch|_mapping|_refresh)",
            "matchType":"regexp",
            "regexpOptions":"i",
            "allow":true,
            "enabled":true,
            "groups":false,
            "user":{

            }
         },
         {
            "$guid":"4A777C8A-5DC0-4C92-A6D7-CD9FB2B19731",
            "description":"Used by Discover Search for searching.",
            "action":[
               "POST"
```

```
            ],
            "url":"^(/elasticsearch/_msearch)|(/es_admin/_mget)",
            "matchType":"regexp",
            "regexpOptions":"i",
            "allow":true,
            "enabled":true,
            "groups":false,
            "user":{

            }
         },
         {
            "$guid":"D8F006C9-81C1-4F76-B663-13C002DCE29E",
            "description":"Delete an index pattern. ",
            "action":[
               "POST",
               "PUT",
               "DELETE"
            ],
            "url":"^/(elasticsearch|es_admin)/\\..+/index-pattern/.+",
            "matchType":"regexp",
            "groups":[
               0
            ],
            "allow":true,
            "enabled":true,
            "regexpOptions":"",
            "user":{

            }
         },
         {
            "$guid":"CEE33ACE-6E81-476E-B719-618B0337C732",
            "description":"Read index pattern fields",
            "action":[
               "POST"
            ],
            "url":"^/(elasticsearch|es_admin)/.+/index-
pattern/_search\\?stored_fields=?",
            "matchType":"regexp",
            "allow":true,
            "enabled":true,
            "regexpOptions":"",
            "groups":false,
            "user":{

            }
         },
         {
            "$guid":"CD2B9F7A-A010-4A64-9BCF-743A928FFC7F",
            "description":"Get main kibana plugin. This requires any access
flags2",
            "action":[
               "GET"
            ],
            "url":"/app/kibana",
            "matchType":"startsWith",
```

```
            "user":{
               "flags2":[
                  256,
                  512,
                  1024,
                  2048
               ],
               "description":"flags2: Any Kibana Access Flag is needed."
            },
            "allow":true,
            "enabled":true,
            "regexpOptions":"",
            "groups":false
         },
         {
            "$guid":"07B3DA7C-5449-4FFD-A004-5BE284C6AD0F",
            "enabled":false,
            "description":"Allow editing kibana settings for the user (Advanced
Settings). This ACE is disabled unless it shall be active for other groups.",
            "action":[
               "GET",
               "POST",
               "PUT",
               "DELETE"
            ],
            "url":"/api/kibana/settings",
            "matchType":"startsWith",
            "groups":[

            ],
            "allow":true,
            "regexpOptions":"",
            "user":{

            }
         },
         {
            "$guid":"E52B5672-4100-48C0-AA53-03FFFFAA184C",
            "enabled":true,
            "description":"Allow storing default index for this user.",
            "action":[
               "GET",
               "POST",
               "PUT",
               "DELETE"
            ],
            "url":"/api/kibana/settings/defaultIndex",
            "matchType":"startsWith",
            "allow":true,
            "regexpOptions":"",
            "groups":false,
            "user":{

            }
         },
         {
            "$guid":"EC99C027-7B5E-4BAD-BBED-43334F3ED8FF",
```

```
            "action":[
               "GET",
               "POST",
               "PUT",
               "DELETE"
            ],
            "url":"^/ui/fonts",
            "matchType":"regexp",
            "regexpOptions":"i",
            "allow":true,
            "enabled":true,
            "groups":false,
            "user":{

            }
         },
         {
            "$guid":"167C7C16-8919-4AD8-8BE9-5C654F36195E",
            "description":"Apps access",
            "action":[
               "GET",
               "POST",
               "PUT",
               "DELETE"
            ],
            "url":"^/app/.+",
            "matchType":"regexp",
            "regexpOptions":"i",
            "allow":false,
            "enabled":true,
            "groups":false,
            "user":{

            }
         },
         {
            "$guid":"545D065F-AFEB-4291-BE60-F80740F4740A",
            "description":"Plugins folder assets",
            "action":[
               "GET"
            ],
            "url":"^/plugins/.+/assets/",
            "matchType":"regexp",
            "regexpOptions":"i",
            "allow":true,
            "enabled":true,
            "groups":false,
            "user":{

            }
         },
         {
            "$guid":"ACD82DCB-7E8B-42F3-AA26-D3B45D3B6C07",
            "description":"All the bundles.",
            "action":[
               "GET"
            ],
```

```
            "url":"/bundles/",
            "matchType":"startsWith",
            "regexpOptions":"",
            "allow":true,
            "enabled":true,
            "groups":false,
            "user":{

            }
         },
         {
            "$guid":"7FE147B6-0CB9-4C7E-8DCF-C7502F8F981F",
            "action":[
               "GET"
            ],
            "url":"/ui/favicons/",
            "matchType":"startsWith",
            "regexpOptions":"",
            "allow":true,
            "enabled":true,
            "groups":false,
            "user":{

            }
         }
      ],
      "const":{
         "DISCOVER":256,
         "VISUALIZE":512,
         "EDIT_DASHBOARD":1024,
         "VIEW_DASHBOARD":2048
      },
      "navigationFilter":[
         {
            "$guid":"45975E93-526D-453E-A25C-AACFD6CCDD48",
            "id":"kibana:discover",
            "matchType":"startsWith",
            "regexpOptions":"",
            "user":{
               "flags2":[
                  256
               ],
               "description":"flags2: DISCOVER"
            },
            "allow":true,
            "enabled":true,
            "groups":false
         },
         {
            "$guid":"2161843B-E15C-4FAB-B273-AD45A66FF461",
            "id":"kibana:visualize",
            "matchType":"",
            "regexpOptions":"",
            "user":{
               "flags2":[
                  512
               ]
```

```
            },
            "allow":true,
            "enabled":true,
            "groups":false
         },
         {
            "$guid":"474B871F-7374-4294-BB02-23FE13C095C4",
            "id":"kibana:dashboard",
            "matchType":"",
            "regexpOptions":"",
            "user":{
               "flags2":[
                  1024,
                  2048
               ],
               "description":"flags2: Either EDIT_DASHBOARD or VIEW_DASHBOARD"
            },
            "allow":true,
            "enabled":true,
            "groups":false
         },
         {
            "$guid":"21BB54F5-77D7-4BAC-B7C1-543611DEC54C",
            "enabled":true,
            "id":"timelion",
            "matchType":"startsWith",
            "allow":false,
            "regexpOptions":"",
            "groups":false,
            "user":{

            }
         },
         {
            "$guid":"052F8962-B876-4D45-A739-E89598AF70B0",
            "enabled":true,
            "id":"elo_ui",
            "matchType":"",
            "allow":true,
            "regexpOptions":"",
            "groups":false,
            "user":{

            }
         },
         {
            "$guid":"DE5D2086-4DBF-4A3C-89D1-A90FABF3F9B8",
            "url":"/app/kibana#/dev_tools",
            "matchType":"",
            "user":{
               "flags":[
                  1
               ],
               "description":"Allow main administrator access"
            },
            "allow":true,
            "enabled":true,
```

```
            "regexpOptions":"",
            "groups":false
         },
         {
            "$guid":"7E4EB6A2-07F4-4502-8364-EA13553F3BE2",
            "url":"/app/kibana#/management",
            "matchType":"startsWith",
            "user":{
               "flags":[
                  1
               ],
               "description":"Allow main administrator access"
            },
            "allow":true,
            "enabled":true,
            "regexpOptions":"",
            "groups":false
         },
         {
            "enabled":false,
            "$guid":"D8BF3124-E587-4587-96DD-1110FC15456C",
            "url":"/app/kibana#/management",
            "matchType":"startsWith",
            "groups":[
               2
            ],
            "allow":true,
            "description":"Allow user access to management page. This will not
allow changing options. See 07B3DA7C-5449-4FFD-A004-5BE284C6AD0F",
            "regexpOptions":"",
            "user":{

            }
         },
         {
            "$guid":"66809A02-4AD3-438A-B088-F8A16703BC78",
            "id":"searchguard-multitenancy",
            "matchType":"startsWith",
            "description":"Searchguard NavLink must be enabled, otherwise the
searchguard ui will fail.",
            "allow":true,
            "enabled":true,
            "regexpOptions":"",
            "groups":false,
            "user":{

            }
         }
      ],
      "ix":{
         "protocol":"http",
         "hostName":"example.com",
         "port":9090,
         "archive":"Demo1",
         "index":""
      },
      "secret":"<hidden>",
```

```
      "clientSSL":{
         "verificationMode":"full",
         "selfSignedCertificate":false,
         "useLatestRootCas":false,
         "rootCas":[

         ],
         "options":null
      },
      "kibana":{
         "encoding":{

         }
      },
      "request":{
         "ticketSource":[
            "query",
            "cookie",
            "jwt"
         ]
      },
      "secretExpiration":86400000
   },
   "filter":{
      "proxy":{
         "port":9300,
         "basePath":null,
         "ssl":{
            "forceProxySSL":false,
            "serverOptions":{

            }
         }
      },
      "httpHandling":{

      }
   },
   "locales":{
      "path":[
         ""
      ],
      "defaultLocale":"en"
   },
   "enabled":true
}
```

4 Erweiterte Konfigurationsbeschreibungen

4.1 ELO Analytics ACL-Filter

ELO Analytics schränkt den Zugriff auf Seiten von Kibana (Navigationsfilter) und Abfragen (Abfragenfilter) auf Elasticsearch über einen Filter-Proxy ein, so dass ELO Benutzer nur bestimmte Bereiche sehen und bestimmte Suchen ausführen können. Die Beschränkung wird durch eine Zugriffskontrollliste (ACL – access control list) durchgeführt, die aus einer Reihe von Zugriffskontrollelementen (ACE – access control entry) besteht. Die Reihenfolge ist dabei wichtig, da das erste passende ACE bei der Zugriffsprüfung ausgewertet wird.

So ist es möglich, durch Anpassung der Filter-ACLs, die Entwicklertools (Navigationslisteneintrag *Dev Tools*) für weitere ELO Benutzer freizuschalten. Die Entwicklertools sind standardmäßig nur für Hauptadministratoren zugänglich, da darüber beliebige (auch schreibende) Elasticsearch-Anfragen ausgeführt werden können. Die Freischaltung erfolgt, indem die Anzeige in der Seitenleiste in der Navigationsfilter-ACL sowie die Zugriffsbeschränkung auf die Befehle in der Accessfilter-ACL innerhalb der Konfiguration angepasst wird.



Information: Die vollständige geänderte Konfigurationsdatei mit einer vollständigen Filter-ACL kann betrachtet werden, indem die *kibana.yml* (oder Custom Konfiguration) um folgenden Eintrag erweitert wird:

```
eloAnalytics.createVerboseConfigsLogging: true
```

Wenn der Wert *true* ist, wird die Datei *eloAnalytics.debug.config.merged.json* angelegt. Sie enthält alle gesammelten ELO Analytics-Einstellungen. Dazu benötigt der ELO Analytics-Server jedoch Schreibrechte auf den ELO Analytics-Ordner *config*.

Dies ist hilfreich, um zu prüfen, ob die Änderung der ACL von ELO Analytics durchgeführt wurde.

4.1.1 Navigationsfilter-ACL (Navigationfilter)

Um die Entwicklertools in der Seitenleiste anzuzeigen, muss dies in der ACL erlaubt werden.

```
    {
       "$guid" : "E598F086-1CA3-49E3-B72E-5754339A8F84",
       "url": "/app/kibana#/dev_tools",
       "matchType": "",
       "groups" : [123],
       "allow": true
     },
```

Fügen Sie das JSON-Objekt ans Ende des Arrays von *navigationFilter* an. Die ACE prüft auf die gegebene URL sowie, ob der Benutzer in einer der angegebenen Gruppen Mitglied ist.

4.1.2 Abfragenfilter-ACL (AcessFilter)

Der Benutzer kann immer noch die Entwicklertools manuell über die Browser-Zeile aufrufen und verwenden. Um jedoch die Befehle an die Elasticsearch freizugeben, muss noch ein Zugriffselement eingesetzt werden (wenn kein Zugriffselement in der ACL existiert, das den Zugriff erlaubt, dann wird der Zugriff nicht stattgegeben).

Finden Sie die folgende ACE:

```
       {
        "$guid" : "403EA38F-C7E2-4E7C-99F8-E4DBC6E41BAF",
        "enabled": false,
        "description": "Access of console plugin and executing console
commands allow only to admins. This ACE is disabled unless it shall be
active for other groups.",
        "action": [
          "GET",
          "POST",
          "PUT",
          "DELETE"
        ],
        "url": "/api/console",
        "matchType": "startsWith",
        "groups": [],
        "allow": true
      },
```

Um die ACE zu aktivieren, ändern Sie *enabled* auf *true* und fügen Sie bei *groups* die gewünschten Benutzer- oder Gruppen-IDs ein.

Änderungen werden nach dem Speichern sofort gültig. Sollten Fehler auftreten, werden diese in der Log-Datei angegeben und die vorherige Konfiguration bleibt bestehen.

4.1.3 Anpassung mit Custom-Config

Mit dem Custom-System von ELO Analytics können Änderungen an den ACLs einfacher durchgeführt werden.

Dazu wird die Datei *eloAnalytics.custom.json* bearbeitet.

Unterhalb von *authentication* werden folgende Einträge vorgenommen (ggfs. müssen diese in vorhandene Einträge *navigationFilter* und *accessFilter* integriert werden, damit kein Schlüssel doppelt vorkommt):

```
…
    "navigationFilter" : [
       {
        "$guid" : "E598F086-1CA3-49E3-B72E-5754339A8F84",
        "url": "/app/kibana#/dev_tools",
        "matchType": "",
        "allow": true,
        "groups" : [123]
      }
    ],
    "accessFilter" : [
      {
                    "$guid" : "403EA38F-C7E2-4E7C-99F8-E4DBC6E41BAF",
        "$options" : "merge",
        "allow": true,
        "groups": [123],
      }
    ]
…
```

Der Eintrag von *navigationFilter* mit der GUID *„E598F086…"* wird in die vorhandene (bzw. interne) Liste des Arrays *navigationFilter* ans Ende eingefügt. Damit können Gruppen und Benutzer (123) auf die Entwicklerleiste zugreifen.

Im zweiten Array *accessFilter* wird dagegen ein vorhandener Eintrag mit der GUID *„403EA38F…"* angepasst (*merge)*, indem die Eigenschaft *groups* verändert wird.

Änderungen werden nach dem Speichern sofort gültig. Sollten Fehler auftreten, werden diese in der Log-Datei angegeben und die vorherige Konfiguration bleibt bestehen.

Eigenschafts-name	Bedeutung
$guid	Definiert für ein Objekt innerhalb eines Arrays einen eindeutigen Bezeichner. Dieser Bezeichner muss innerhalb des Arrays eindeutig sein und kann uneindeutig über mehrere verschiedene Arrays sein. • Entweder ist es ein GUID oder eine einfache Zahl. • Muss immer vorhanden sein • Muss gleich dem Zielobjekt im Array sein, wenn dieses überschrieben werden soll. • Muss ungleich aller GUIDs in den Zielobjekten im Array sein, wenn das Quellobjekt neu eingefügt werden soll.

$action	• Optional • Ein String oder Array. • Wenn nicht angegeben, dann wird das Objekt mit der GUID überschrieben. Andernfalls wird eine Ausnahme ausgelöst (außer Parameter *onGuidNotFound* liefert einen Index) • Definiert die Aktion, welche ausgeführt werden soll. o "insert" • Fügt das Objekt ans Ende des Zielarrays ein. GUID muss eindeutig sein. o ["insert", "guid"|number, optionales Offset] • Fügt das Quellobjekt **hinter** das Objekt mit der angegeben GUID oder Array-Index. Wird ein Offset angegeben, wird das Offset zum Array-Index des Elements mit der angegeben GUID dazugerechnet (positiv) oder abgezogen (negativ). So kann man mit -1 das Quellobjekt vor dem Zielobjekt einfügen. o "remove" (eine eindeutige GUID für dieses Objekt muss angegeben sein!) • Entfernt das Objekt, welches die gleiche GUID besitzt. o ["remove", "guid"|number, optionales Anzal von Elemente] • Entfernt das Zielobjekt, welches die gleiche angegeben GUID oder Nummer besitzt. Optional kann angegeben werden, wie viele darauf folgende Objekte gelöscht werden sollen. • Quellobjekte können Unter-Arrays enthalten. Diese werden jedoch nicht zusammengeführt.
$options	• Optional • Ein String oder Array • Definiert zusätzliche Einstellungen für folgende Werte o "merge" ▪ Wenn im Quellobjekt angegeben und wenn ein Zielobjekt überschrieben werden soll, führt Ziel- und Quellobjekt ineinander, sodass das resultierende Objekt alle Eigenschaften beider Objekte besitzt.

	▪ Dabei werden bei gleichnamigen Schlüsseln im Zielobjekt diese ersetzt. ▪ Um Eigenschaften im Zielobjekt zu löschen, kann die Eigenschaft im Quellobjekt auf [null] gesetzt werden. o "locked" ▪ Wenn im Zielobjekt angegeben, ist es nicht möglich dieses Objekt aus dem Array zu löschen oder zu verändern. Versuche führen zu einer Ausnahme.

4.2 Kennwortverschlüsselung in ELO Analytics konfigurieren

Vorbemerkung: Benutzen Sie bevorzugt das ELO Server Setup, um Kennwörter nachträglich zu ändern. Diese werden verschlüsselt gespeichert.

Die Kennwörter in der Kibana-Konfiguration können mit AES verschlüsselt werden. Dazu zählen:

- elasticsearch.password
- server.ssl.keyPassphrase

Um die Verschlüsselung zu aktivieren, müssen Sie folgende Einstellungen vornehmen:

1. Umbenennen der Schlüssel in
   a) elasticsearch.passwordEnc
   b) server.ssl.keyPassphraseEnc
2. Hinzufügen der Umgebungsvariablen für den ELO Analytics-Prozess
   a) ELO_ANALYTICS_ENCODING=aes
   b) ELO_ANALYTICS_AES_KEY=<AES-KEY>
   c) ELO_ANALYTICS_ENCODING_CONFIG=<CONFIG>

Aktuell wird nur *elasticsearch.passwordEnc* standardmäßig verschlüsselt.

Die Verschlüsselung wird mit AES-Cipher-Block-Chaining durchgeführt und erfordert einige Einstellungen. Der schnellste Weg, um diese Einstellungen zu erhalten, ist es eine Kommandozeile zu öffnen und zum Pfad

```
<ELO>\server\ELO-Analytics\bin\helpers
```

zu navigieren. Führen Sie in diesem Ordner in einer Konsole das Skript aus (Windows oder Linux):

```
secureKeys.bat
```

oder

```
./node secureKeys.js
```

Sie werden nach dem Elasticsearch-Kennwort gefragt und können weitere Kennwörter verschlüsseln lassen. Sie schließen den Vorgang ab, indem Sie leeren Text eingeben. Sie müssen jedes eingegebene Passwort zur Kontrolle noch einmal eingeben. Es ist auch möglich, per Einfügen (Strg + V) das Kennwort zu kopieren.

In der Ausgabe erhalten Sie alle Konfigurationseinstellungen und Schlüssel für die AES-Verschlüsselung.

```
Service environment variables:
ELO_ANALYTICS_ENCODING=aes
ELO_ANALYTICS_AES_KEY=a5eb585d4330bde18fe52…42dd4b45e0db947eb5
ELO_ANALYTICS_ENCODING_CONFIG={"trimLeft":32,"trimRight":32,"iv":"90631e135
cf725574051363b7128ed5b"}
```

```
kibana.custom.secrets.config.yml:
elasticsearch.passwordEnc=148ad754c4855ad183208ce828af1833f9a625152…f1f4fab
c8fc9cb50e05a24

Misc passwords in same order as entered
0=5e3dc6c3963c56c54b7e18b043c1e827e57…b9ab899f7d46a5f96195f0f
```

Wir empfehlen immer unterschiedliche Kennwörter zu verwenden! Dennoch werden gleiche Kennwörter immer unterschiedlich verschlüsselt, um keine Rückschlüsse auf den Inhalt ziehen zu können. Dies wird durch einen kryptografischen Zufallswert ermöglicht, der zum Kennwort hinzugefügt wird.

4.2.1 Anpassen der Dienste unter Windows

Die folgenden Schritte führen Sie für alle Archive mit ELO Analytics aus.

1. Beenden Sie alle notwendigen ELO Analytics-Dienste.
2. Öffnen Sie den Service Editor unterhalb

```
<ELO Pfad>\server\ELO-Analytics\bin
```

mit

```
nssm64 edit ELO-Analytics  (oder Archivname-Anhang)
```

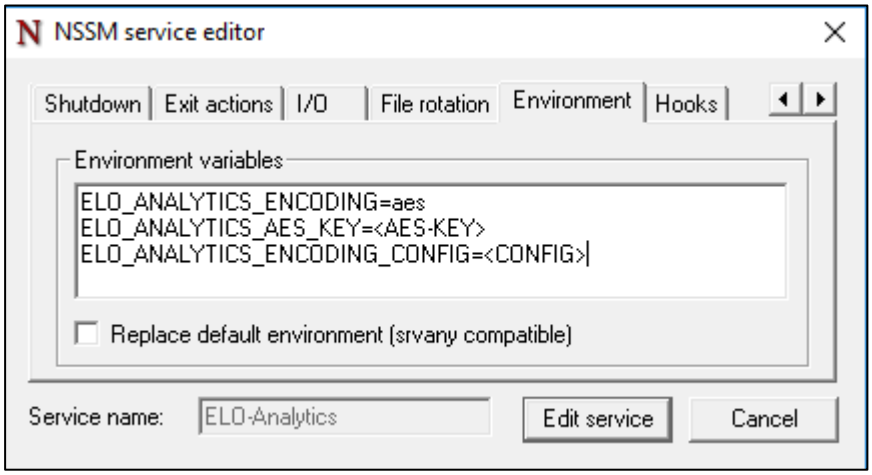


Abb. 3: NSSM service editor

3. Fügen Sie unter *Environment* die generierten Einstellungen dort hinzu und Speichern Sie diese per Klick auf *Edit Service*.
4. Ersetzen Sie in Ihrer Kibana-Konfiguration das Kennwort mit dem generierten.

Aus

```
elasticsearch.password: <unverschlüsseltes Password>
```

wird

```
elasticsearch.passwordEnc: <verschlüsseltes Password>
```

5. Starten Sie den ersten Dienst und prüfen in den Log-Dateien, ob die Verbindung mit Elasticsearch aufgebaut werden kann.

Beachten Sie beim Kopieren aus der Konsole, dass keine unerwünschten Umbrüche oder Leerzeichen vor oder nach den Werten vorhanden sind, und dass Sie die Werte vollständig kopieren.

Das Werkzeug generiert das verschlüsselte Kennwort folgendermaßen:

```
<32 Bytes Zufallsdaten><Kennwort auf das nächste Vielfache von 16 mit \0
vergrößert><32 Bytes Zufallsdaten>
```

Byte-Ströme sind in hexadezimaler Schreibweise angegeben. Die Schlüssellänge beträgt 128 Bits (auch im ELO Server Setup) und kann mit der Umgebungsvariable *ELO_ANALYTICS_NEW_KEY_LENGTH* auf 256 Bits (geben Sie dazu 32 an) erhöht werden.

Setzen Sie immer Benutzerrichtlinien und Dateizugriffsrechte des Betriebssystems ein, um Dateien und Geheimnisse zu schützen. Die Kennwortverschlüsselung schützt nur vor einem Angriffsvektor (Zuschauer, Konfiguration kopieren). Sie kann jedoch nicht schützen, wenn das System kompromittiert wurde.

4.2.2 Nachträgliches Ändern eines Kennworts

Sie können ein Kennwort nachträglich setzen, ohne die Umgebungsvariablen zu ändern und damit ohne alle anderen Kennwörter neu zu verschlüsseln. Dazu benötigen Sie die Umgebungsvariablen und eine Konsole.

Öffnen Sie die Konsole als Administrator und navigieren Sie in der Konsole zu folgendem Pfad:

```
<ELO Pfad>\servers\ELO-Analytics\bin\helpers
```

Geben Sie die Umgebungsvariablen nacheinander ein.

- Unter Microsoft Windows mit dem Präfix "set"
- Unter Linux mit dem Präfix "export"

```
set ELO_ANALYTICS_ENCODING=aes
set ELO_ANALYTICS_AES_KEY=a5eb585d4330bde18fe52…42dd4b45e0db947eb5
set
ELO_ANALYTICS_ENCODING_CONFIG={"trimLeft":32,"trimRight":32,"iv":"90631e135
cf725574051363b7128ed5b"}
```

Mit dem Aufruf von

```
secureKeys.bat bzw. ./node secureKeys.js
```

können Sie nun erneut Kennwörter eingeben. Dabei wird die aktuelle Konfiguration Ihrer Dienste verwendet und Sie können beliebige Kennwörter erneut verschlüsseln. Ignorieren Sie dabei *elasticsearch.passwordEnc*, falls Sie es nicht benötigen und geben Sie zweimal z. B. `"123"` ein.

Schließen Sie danach die Konsole, um die Umgebungsvariablen zu löschen.

4.3 Vollständige Elasticsearch-Query nach ELO Analytics

Das folgende Beispiel zeigt eine vom Benutzer ausgelöste Suche, die durch den ELO Analytics-Server zusätzliche Abfragen bekommen hat, bevor Sie zum Elasticsearch-Server weitergeleitet wird.



Information: Diese hier gezeigt Query können Sie erzeugen, indem Sie die Kibana-Konfigurationseinstellung *logging.events.log* um *elo-filter-change* erweitern, den ELO Analytics-Server neustarten und nach einer ausgeführten Query in der Log-Datei von ELO Analytics nach „Query string was changed due to ELO filter“ suchen.

Die Log-Ausgabe erfolgt im JSON-Format, sodass die Query sich im Schlüssel *queryString* befindet.

In der Browser-Konsole kann man die Query schnell mit dem folgenden Aufruf extrahieren. Dazu muss die gesamte Query einfach in *<query>* eingefügt werden.

```
var jsqvalue = '<query>';
JSON.stringify(JSON.parse(jsqvalue.split(/(\n)/g)[2]), null, "  ")
```

Die Query beinhaltet nur die grundlegenden ELO Gruppenfelder in *docvalue_fields*, kann aber (fast) alle ELO Gruppenfelder enthalten.

```
{
   "version":true,
   "size":10000,
   "sort":[
      {
         "_score":{
            "order":"desc"
         }
      }
   ],
   "query":{
      "bool":{
         "must":[

         ],
         "filter":[
            {
               "bool":{
                  "should":[
                     {
                        "term":{
                           "acl_everyone":{
                              "value":true,
                              "boost":1
                           }
                        }
                     },
                     {
                        "term":{
                           "acl_groups":{
                              "value":2,
                              "boost":1
                           }
                        }
                     },
                     {
                        "bool":{
                           "must":[
                              {
                                 "exists":{
                                    "field":"acl_and_groups",
                                    "boost":1
                                 }
```

```
                              },
                              {
                                 "script":{
                                    "script":{
                                       "inline":"AclFilter",
                                       "lang":"native",
                                       "params":{
                                          "userAcl":[
                                             2,
                                             9999
                                          ]
                                       }
                                    },
                                    "boost":1
                                 }
                              }
                           ]
                        }
                     }
                  ]
               }
            },
            {
               "term":{
                  "sord_deleted":{
                     "value":false,
                     "boost":1
                  }
               }
            },
            {
               "term":{
                  "admin_child":{
                     "value":false,
                     "boost":1
                  }
               }
            }
         ]
      }
   },
   "_source":{
      "excludes":[

      ]
   },
   "stored_fields":[
      "title_en",
      "title_none"
   ],
   "script_fields":{
```

```
   },
   "docvalue_fields":[
      "feed_date_created",
      "feed_date_created_year",
      "feed_date_last_change",
      "feed_date_last_change_year",
      "sord_idate",
      "sord_idate_year",
      "sord_tstamp",
      "sord_tstamp_year",
      "sord_xdate",
      "sord_xdate_year",
      "version_lastupdate",
      "acl_everyone",
      "admin_child",
      "copy_of_all_title",
      "elo_id",
      "elo_owner",
      "guid",
      "is_fulltext",
      "sord_mask",
      "sord_maskName",
      "sord_ownerid",
      "sord_type",
      "acl_groups",
      "doc_size",
      "elo_ext"
   ],
   "highlight":{
      "pre_tags":[
         "@kibana-highlighted-field@"
      ],
      "post_tags":[
         "@/kibana-highlighted-field@"
      ],
      "fields":{
         "*":{
            "highlight_query":{
               "match_all":{

               }
            }
         }
      },
      "fragment_size":2147483647
   }
}
```

4.4 Log-Rotation

Standardmäßig werden Log-Ausgaben in ELO Analytics in die Datei *eloAnalytics.json.log* im entsprechenden Unterordner (nach dem Schema *Log-<Archivname>)* gespeichert. Dies kann in der Datei *kibana.custom.yml* mit dem Schlüssel *logging.dest* angepasst werden.

Grundsätzlich können folgende Logging-Methoden verwendet werden:

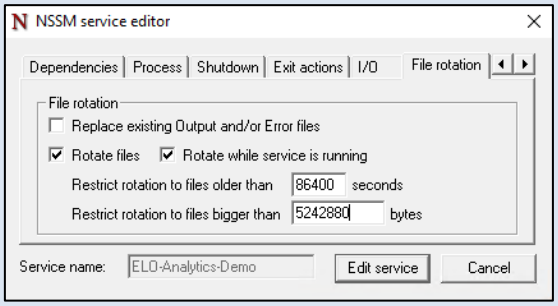
- Dateiausgabe in *eloAnalytics.json.log* (Standard)
- Logstash
- NSSM

Die nachfolgenden Tabellen gehen kurz auf die Vor- und Nachteile dieser Methoden ein und geben Hinweise zur Konfiguration.

Dateiausgabe in *eloAnalytics.json.log* (Standard)	
Vorteile	• Einfache Ansicht • einfaches Dateihandling
Nachteile	• Keine Log-Rotation • Logs werden immer nach Dienststart angehängt

Konfiguration	In den Dateien *kibana.yml* bzw. *kibana.custom.yml*
	`logging.dest: <Pfad>/ELOAnalytics.json.log`
	`logging.events.error: '*'`
	`logging.events.log: [warning, error, fatal, elo, optimize]`
	`logging.json: true`

Logstash	
Vorteile	• aufwändige Konfiguration (Elasticsearch)
Nachteile	• große Log-Daten möglich (Datenbank) • Filterung, Sortierung, Suche dank Logstash
Konfiguration	• entsprechend einer Logstash-Anleitung (nicht von ELO bereitgestellt)

NSSM	
Vorteile	• Log-Ausgabe in *stdout.log* • Rotation online oder bei Dienststart möglich
Nachteile	• Online-Log-Rotation kann bei laufendem Dienst Fehler verursachen ("increased risk of failure" laut NSSM-Dokumentation: *https://nssm.cc/usage*) • Große Log-Dateien bei lang laufendem Dienst und Rotation bei Dienstneustart
Konfiguration	1. Die Konfiguration in *kibana.custom.yml* ändern: `logging.dest: null` 2. NSSM-Dienst konfigurieren.  *Abb. 4: NSSM service editor; Einstellungen für 'File rotation'* Mit der im Screenshot gezeigten Konfiguration werden Logs, die älter als 24h sind oder größer als 5 MiB, rotiert.

5 Weiterführende Literatur

- Kibana 5.5 Konfigurationsschlüssel
  https://www.elastic.co/guide/en/kibana/5.5/settings.html

6 Referenzverzeichnis

A

authentication
aclFilter
active 21
clientSSL
options 21
rootCas 21
selfSignedCertificate 22
useLatestRootCas 22
verificationMode 23
const 24
cookie
clearInvalid 24
encoding 24
isHttpOnly 25
isSecure 25
path 26
strictHeader 26
ix
archive 27
hostName 27
port 28
protocol 28
kibana
password 28
passwordEnc 29
username 29
navigationFilter 30
secret 31
secretExpiration 31
sessionFactoryOptions 32
token
adminBypassAccessCheck 32
aliveInterval 33
apiUrls 33
cookieExpirationTime 33
eloApiTokenExpirationTime 34
eloTokenExpirationTime 34
invalidateTokenInCookiesAfterRestart 34
uiAliveIntervalTime 35
useEloTokenExpirationTime 35, 36, 37

C

clientConfiguration
columnHeaderDisplay
maxMaskCount 38
columnsRename 38
dateStringMapping 39
fieldDisplaynameSeparator 39
javaClient 40

jsonMixin 41

E

elasticSearch
password 9
passwordEnc 9
requestTimeout 10
ssl
verificationMode 10
url 11
username 11
eloAnalytics
configs
eloAnalytics 18
eloAnalyticsCustom 19
eloAnalyticsSecrets 19
createVerboseConfigsLogging 20

F

filter
base
basePath 42
httpHandling
payloadLimit 41
proxy
host 42
port 43
remote 43
ssl
forceProxySSL 44
serverOptions 44

K

kibana
index 11

L

locales
defaultLocale 44
path 45
logging
AccessCheckVerbose 45
logFilterRequestsPath 46
logging
dest 12
events
log 12
json 12

M

metrics
enabled 13

O

ops
interval 13
optimize
bundleDir 13

S

search
docValuesExclude 47
docValuesInclude 47
eloIndexNamePattern 47
esDateFormat 48
esDateFormatAggregation 48
fieldMappingsExclude 49
maskExclude 49
maskReloadCache 50
storedFieldsExclude 51
storedFieldsInclude 51
searchguard
basicauth
enabled 13
multitenancy
enabled 14
server
basepath 14
host 14
maxPayloadBytes 15
name 15
port 15
ssl
certificate 16
enabled 16
key 16
keyPassphrase 17
keyPassphraseEnc 17

T

timelion
enabled 18

U

uiDefaultSettings 46
'elo:discover.columnsRename' 51