NotifySCM
Secure Content Management

NotifySCM Analytics
Configuration Guide

TABLE OF CONTENTS

1 OVERVIEW

Starting with version 3.13, NotifySCM embeds a search and analytics engine which allows administrators to analyze users' behavior and provides information that helps developers enhance the performance of the NotifySCM protect application.

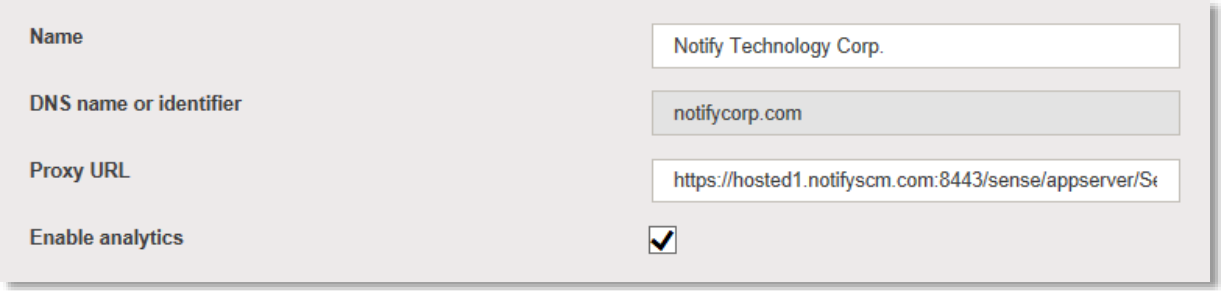
This configuration guide provides information on installing the tools required to connect and monitor the analytics engine.

2 ENABLING ANALYTICS ENGINE

2.1 Enable Data Collection

Activation of the analytics engine must be done for each domain, even when the database is common to all domains. To enable the collection of data, **you must have superadmin rights**:

1. Login to the security server with superadmin credentials.
2. Browse to **SERVER** -> **Domains** and select the domain on which to enable analytics.
3. Check the box labeled, **Enable analytics.**



As soon as this option is checked, NotifySCM will start to collect any data related to user and application activity immediately, once this option is checked.

2.2 Activate an Analytics Engine Listener

To search and view the data logs collected, NotifySCM uses a remote web interface tool such as *Kibana*. NotifySCM must be configured to listen for an inbound connection from *Kibana* to the analytics engine. This configuration, however, will allow for connections from anywhere, by anyone. Therefore, it is important to implement the best security practices for your particular environment. If necessary, contact NotifySCM technical support for best practice recommendations.

2.2.1 Windows

Follow these steps if NotifySCM is installed on a Windows server:

1. Stop the service, SENSE-SERVER
2. Start the NotifySCM service manager (C:/NotifySCM/services/SENSE-SERVER_service_manager.bat)
3. Go to the Java tab and add the following lines:
   -Dspring.data.elasticsearch.properties.http.enabled=true
   -Dspring.data.elasticsearch.properties.http.bind_host=0.0.0.0
4. In the command line tool, run *sense-server_service.bat remove* and then *sense-server_service.bat install*
5. Apply and start the service, SENSE-SERVER

2.2.2 Linux

Follow these steps if NotifySCM is installed on a Linux server:

1. Stop the tomcat service.
2. Edit the file C:/NotifySCM/bin/setenv.sh
3. Add the following lines:
   JAVA_OPTS="$JAVA_OPTS -Dspring.data.elasticsearch.properties.http.enabled=true"
   JAVA_OPTS="$JAVA_OPTS -Dspring.data.elasticsearch.properties.http.bind_host=0.0.0.0"
4. Start the tomcat service.

3 INSTALL VISUALIZATION TOOL

The *Elasticsearch* database used to collect data can interface with many tools. This chapter will explain how to install the most commonly used one: **Kibana**.

3.1 Install Kibana

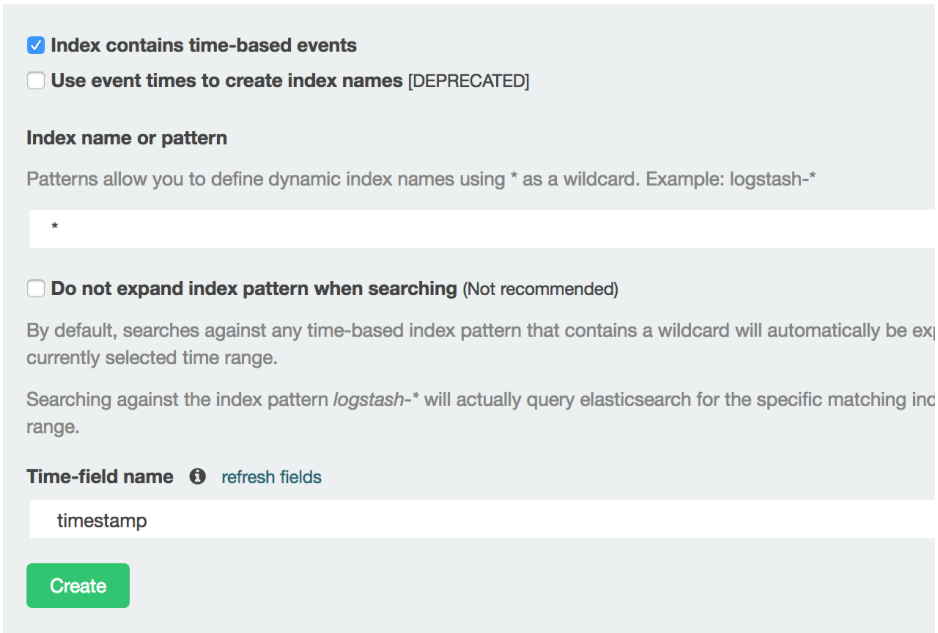
!!! Avoid installing Kibana on the same virtual machine as the NotifySCM server as it is resource consuming !!!

Download the compatible version with NotifySCM here: https://www.elastic.co/downloads/past-releases/kibana-4-5-4

1. Extract the package and edit the file KIBANA_HOME/config/kibana.yml
2. Remove the # for the parameter elasticsearch.url and set your NotifySCM server IP address
3. Run KIBANA_HOME/bin/kibana.bat (kibana on Linux)
4. Connect to http://localhost:5601/

3.2 Configure Kibana

1. Browse to **Settings** and select the tab indices.
2. Configure an index pattern as shown below:



3. Select the tab labeled **Objects** and click on **Import.**
4. Select the NotifySCM configuration file provided by Notify Technology Corporation.
5. You should see imported dashboards and visualization options.

3.3 Pre-defined dashboards

3 dashboards are provided with the analytics engine:

- **Default**: Provides generic information about the NotifySCM server usage, such as requests per day or processing time.
- **Device centric**: Provides device centric information, such as operating system used or bandwidth usage.
- **Http proxy**: Provides http proxy usage information.

4 AVAILABLE DATA

This section lists all data that can be collected by NotifySCM and used for analytics.

4.1 Generic

- **_type (Text):** The NotifySCM component that collects this data:
  - **session**: Data collected when a request has been made to the security server
  - **proxy-http**: Data collected when a request has been processed by the NotifySCM HTTP proxy
  - **proxy-component**: Data collected when a request has been made by the workspace
- **timestamp (Date):** Date at which the data has been collected

4.2 Application

- **applicationIdentifier (Text)**: *Bundle ID* on iOS or *Package name* on Android
- **applicationInstanceIdentifier (Text)**: Unique ID per application instance
- **applicationRef (Text)**: Workspace only; application name within the workspace
- **applicationVersion (Text)**: Version of the application
- **serviceName (Text)**: Workspace only; the service used by an application

4.3 Device

- **deviceModel (Text)**: The model of the device
- **deviceName (Text)**: The name of the device as entered by the user (Optional)
- **deviceOperatingSystem (Text)**: NotifySCM code for iOS (IPHONE3) or Android (ANDROID)
- **deviceOsVersion (Text)**: The version of the operating system

4.4 Device context

- **clientTime (Date)**: Time on the device
- **clientTimeZone (Text)**: Time zone of the device
- **ipAddress (Address IP):** IP Address as seen by the NotifySCM server. Should be the device IP address, but if NotifySCM is behind a proxy, this address will be the one from the proxy
- **ipCountry (Text):** Computed country based on the IP address
- **location (GPS location)**: GPS location of the device

4.5 User

- **domainName (Text)**: Domain of the user
- **userName (Text)**: Name of the user

4.6 Session

- **sessionStartTime (Date)**: Date when a user open a NotifySCM session
- **sessionEndTime (Date)**: Date when a user logged out or when the NotifySCM session expired
- **sessionDuration (Date):** Duration of the NotifySCM session
- **sessionId (Text):** Unique ID of the NotifySCM session

4.7 HTTP proxy

- **requestContentLength (Number):** Length of the request's content sent by the mobile
- **requestMethod (Text):** HTTP request method (GET, POST, HEAD, etc)
- **requestPath (Text):** Path to the requested resource (e.g. /favicon.ico)
- **requestPort (Number)**: Port on which the request has been done
- **requestProtocol (Text)**: Protocol used by the request (http or https)
- **requestProtocolVersion (Text):** HTTP protocol version (e.g 1.1)
- **requestServer (Text):** Hostname or IP address of the targeted backend server (e.g. notify.com)
- **responseCode (Number):** HTTP response code (e.g. 200)
- **responseContentLength (Number)**: Length of the response's content sent to the mobile
- **responseContentType (Text)**: Content type of the response (e.g image/x-icon)
- **responseDelay (Number)**: Request processing time
- **responseMessage (String)**: HTTP response message (e.g. OK)