

Documentation

Installation and Configuration Guide

IDM Audit Dashboard 2.0

for NetIQ Identity Manager (version 4 or higher)



Version: 2.0
created:: 15.07.2016
last modified: 8/17/2016 8:57:00 AM

File: CHANGED_Audit_Dashboard_Installation_Manual_v20.docx

Contents

1	Legal Notice.....	4
2	Introduction.....	5
2.1	Components.....	5
2.2	Requirements	5
3	Installation	7
3.1	Check and install Oracle Java	7
3.1.1	Check Java installation for Linux.....	7
3.1.2	Check Java installation for Windows	7
3.1.3	Official installation of Oracle Java	8
3.1.4	Global configuration of JAVA_HOME for Linux.....	8
3.1.5	Global configuration of JAVA_HOME for Windows.....	8
3.2	Install Elasticsearch and Logstash.....	9
3.3	Configure Elasticsearch.....	11
3.3.1	Config file changes.....	11
3.3.2	Start, stop, status of Elasticsearch.....	11
3.3.3	Check if your Elasticsearch is running	12
3.4	Install the Audit Server.....	13
3.4.1	Unpacking and manual start.....	13
3.4.2	Make runnable as a service for Linux	13
3.4.3	Make runnable as a process for Windows	14
3.4.4	Check if your Audit Server is running	15
3.5	Update Audit Server	16
3.5.1	Copy setting from the previous version of Audit Server	16
3.5.2	Update default Audit Server report templates	16
3.6	Configure the Audit Server.....	17
3.7	Install the Audit Driver	18
3.7.1	Install the Audit Driver with Identity Manager	18
3.7.2	Install the Audit Driver with NetIQ IDM Designer	28
3.7.3	Test the Driver	31
3.8	Install the Report Service	32
3.8.1	Extract and manual start	32
3.8.2	Make runnable as service for Linux	33
3.8.3	Make runnable as a service for Windows	33
3.8.4	Check the history	36
3.9	Install the Audit Export service	37
3.9.1	Extract and manual start	37
3.9.2	Make runnable as service for Linux	37
3.9.3	Make runnable as service for Windows.....	38
3.9.4	Check if your Audit Export service is running.....	40
3.9.5	Configure the Audit Export.....	40
4	Sample Dashboards.....	41

Installation and Configuration Guide

4.1	Modify a dashboard.....	42
4.2	Experience the IDM Audit Dashboard	44
4.3	Understand the IDM Audit Dashboard	44
4.4	Work with Panels	45
4.4.1	Change an existing Panel.....	45
4.4.2	Add a new Panel	45
4.4.3	Create new row	47
5	Conclusion	50

Installation and Configuration Guide

1 Legal Notice

SKyPRO AG makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose.

Further, SKyPRO AG reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. Further, SKyPRO AG makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose.

Further, SKyPRO AG reserves the right to make changes to any and all parts of SKyPRO software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to the Swiss export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current Swiss export exclusion lists or to any embargoed or terrorist countries as specified in the Swiss export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. SKyPRO assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2005-2016 SKyPRO AG. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

SKyPRO AG has intellectual property rights relating to technology embodied in the product that is described in this document.

SKyPRO AG
Gewerbstrasse 7
CH-6330 Cham
SWITZERLAND

www.skypro.com

About this document

This document explains the installation and configuration of the "IDM Audit & Compliance dashboard."

Audience

This guide is intended for administrators maintaining existing NetIQ Identity Manager environments. You should have an understanding of drivers, workflows, eDirectory, and the IDM Designer tool.

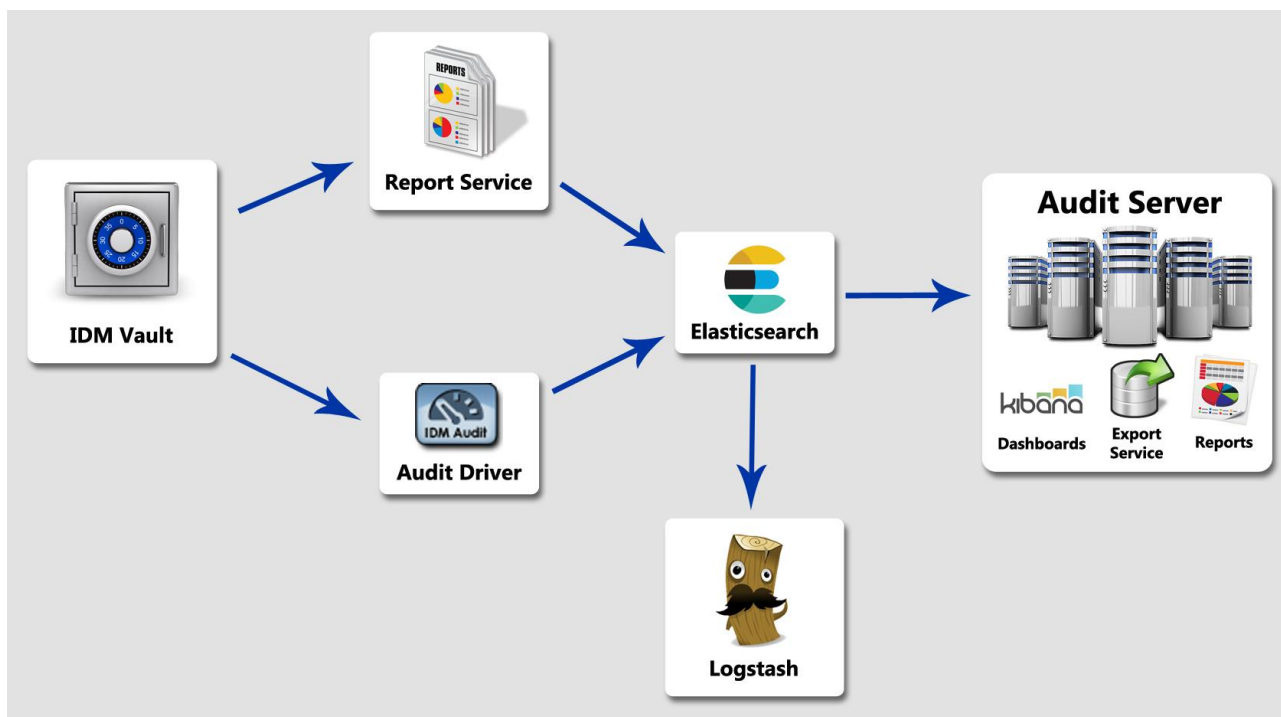
Feedback

We appreciate your comments and suggestions about our products and documentation. If you have any suggestions, comments, or feature requests please contact us via info@skypro.ch.

Installation and Configuration Guide

2 Introduction

2.1 Components



2.2 Requirements

Due to the fact that as of April 2015 Oracle no longer releases public updates for Java 7, we recommend that you use the latest available version of Java 8. Make sure that your system meets the system requirements necessary for the normal functioning of the IDM Audit Dashboard server and components.

Official supporting platforms for Java 8:

Linux	Oracle Linux 5.5 + 1 Oracle Linux 6.x (32-bit), 6.x (64-bit) 2 Oracle Linux 7.x (64-bit) 2 (8u20 or later) Red Hat Enterprise Linux 5.5 + 1, 6.x (32-bit), 6.x (64-bit) 2 Red Hat Enterprise Linux 7.x (64-bit) 2 (8u20 or later) Suse Linux Enterprise Server 10 SP2 +, 11.x Suse Linux Enterprise Server 12.x (64-bit) 2 (8u31 or later) Ubuntu Linux 12.04 LTS, 13.x Ubuntu Linux 14.x (8u25 or later)
Mac OS X	Mac with Intel processor under Mac OS X 10.8.3+, 10.9+ running
Windows	Windows 10 (8u51 or later) Windows 8.x (Desktop version) Windows 7 with service pack 1 (SP1) Windows Vista SP2

Installation and Configuration Guide

	Windows Server 2008 R2 with service pack 1 (SP1) (x64 version) Windows Server 2012 and 2012 R2 (x64 version)
--	---

Hardware requirements for Audit Dashboard components:

Audit Server	Processor: Not less than 2266 MHz Ram: Not less than 2GB Disk space: Not less than 200 MB
Audit Report service	Processor: Not less than 2266 MHz RAM: Not less than 1GB Disk space: Not less than 100 MB
Audit Export service	Processor: Not less than 2266 MHz RAM: Not less than 2GB Disk space: Not less than 200 MB
Audit Driver	Identity Manager official requirements https://www.netiq.com/documentation/idm402/
Elasticsearch	Elasticsearch official requirements https://www.elastic.co/guide/en/elasticsearch/guide/1.x/hardware.html

Choose from the following platform:

- Java: Version 8 or higher <http://java.com/en/download/help/sysreq.xml>
- NetIQ Identity Manager (version 4 or higher)
<https://www.netiq.com/documentation/idm402/>

Installation and Configuration Guide

3 Installation

To install the IDM Audit Dashboard, go to our web site <http://www.skypro.ch/en/products/idm-supplements/idm-audit> and download the complete installation file *IDM_AC_Dashboard.zip*. This file contains all the needed components. After downloading, please unpack it. You will see the following packages:

- AuditDriver-1.0RC2.zip
- AuditServer-2.0.zip
- Elasticsearch-1.4.4.zip
- AuditReport-1.0RC1.zip
- AuditExport-1.0RC1.zip

3.1 Check and install Oracle Java

IDM Audit Dashboard components require Oracle Java to be installed. Due to the fact that the last Java 7 public release was in April 2015, we recommend using Java 8. Java installation varies by platform. To check if Java is needed to be installed, please follow the next steps depending on your platform:

3.1.1 Check Java installation for Linux

To check if Java is installed, please run the following commands in your Terminal:

whereis java

YOUR_JAVA_LOCATION/java -version

echo \$JAVA_HOME

If all is correct, you will see the text like this:

```
kot@kostik-pc:~$ whereis java
java: /usr/bin/java /etc/java /usr/bin/X11/java /usr/share/java /usr/share/man/man1/java.1.gz
kot@kostik-pc:~$ /usr/bin/java -version
java version "1.7.0_80"
Java(TM) SE Runtime Environment (build 1.7.0_80-b15)
Java HotSpot(TM) 64-Bit Server VM (build 24.80-b11, mixed mode)
kot@kostik-pc:~$ echo $JAVA_HOME
/usr/lib/jvm/java-8-oracle
kot@kostik-pc:~$
```

3.1.2 Check Java installation for Windows

To check if Java is installed, please run the following commands in Windows Command Processor (cmd.exe):

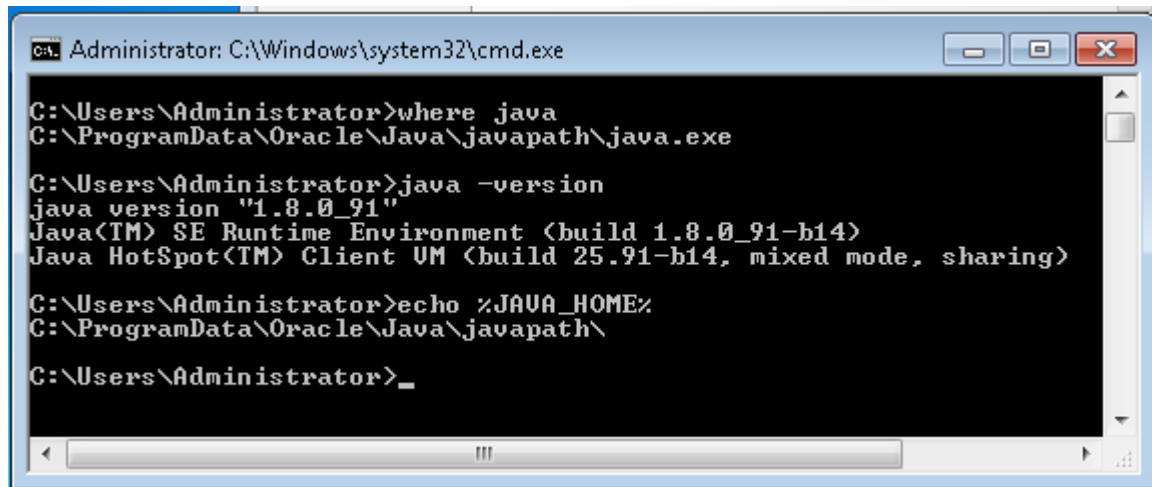
where java

YOUR_JAVA_LOCATION/java -version

echo %JAVA_HOME%

If everything is correct, you will see such text:

Installation and Configuration Guide



```
Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>where java
C:\ProgramData\Oracle\Java\javapath\java.exe

C:\Users\Administrator>java -version
java version "1.8.0_91"
Java(TM) SE Runtime Environment (build 1.8.0_91-b14)
Java HotSpot(TM) Client VM (build 25.91-b14, mixed mode, sharing)

C:\Users\Administrator>echo %JAVA_HOME%
C:\ProgramData\Oracle\Java\javapath\

C:\Users\Administrator>_
```

3.1.3 Official installation of Oracle Java

If no Java 8 is installed, please follow the official installation instructions from Oracle:
<http://www.java.com/en/download/manual.jsp>

If you have already installed Java 8 but JAVA_HOME or JAVA_PATH are not defined, you can manually define them for each service or make it globally.

3.1.4 Global configuration of JAVA_HOME for Linux

To define JAVA_HOME global in Linux, please follow these steps:

1. Create file "jdk_home.sh" in "/etc/profile.d" folder
2. Add the following commands to this file:


```
export JAVA_HOME=PATH_OF_YOUR_JAVA
export PATH=$JAVA_HOME/bin:$PATH
```
3. Save
4. Restart your server or terminal.

3.1.5 Global configuration of JAVA_HOME for Windows

If no Java 8 is installed, please follow the official installation instructions from Oracle:
<http://www.java.com/en/download/manual.jsp>

If you have already installed Java 8 but JAVA_HOME or JAVA_PATH are not defined, you can manually define them for each service or make it globally.

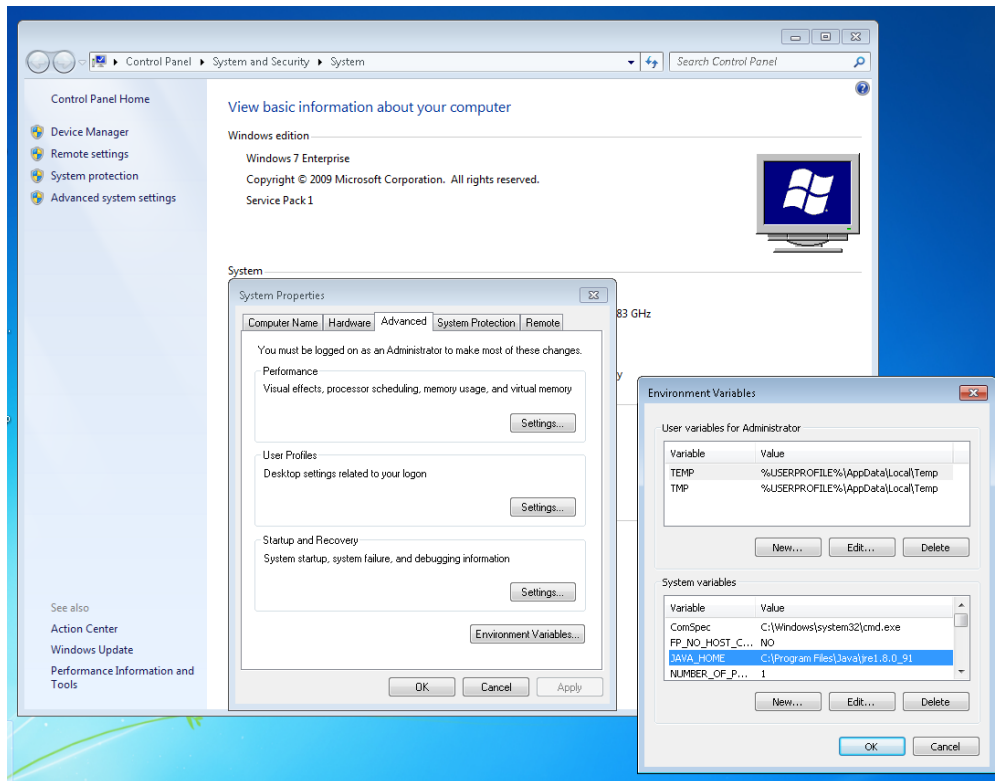
To define JAVA_HOME global in Windows, please follow these steps:

1. Navigate to "Advanced System Settings."
2. In the System Properties window click the Environment Variables button.
3. In the "System variables" section of the Environment Variables window that appears, ensure that the JAVA_HOME environment variables are pointed at the following locations:

JAVA_HOME: C:\Program Files\Java\jre<version>

If these environment variables do not exist, add them to the list.

Installation and Configuration Guide



4. Click "OK" to close the Environment Variables window.
5. Click "Apply" to close the System Properties window.
6. Restart Windows for the changes to take effect.

3.2 Install Elasticsearch and Logstash

Make sure that you have Java installed. If no Java is installed, please follow the instructions for how to install Java on your system in chapter "3.1 Install Oracle Java." The first step is to install Elasticsearch and Logstash.

1. Extract the archive

Extract content of the "Elasticsearch-1.4.4.zip" file

- For Linux, use the following command:

unzip Elasticsearch-1.4.4.zip

- For Windows, please use Windows Explorer option "Extract All"

After extraction you will get the following packages:

ZIP – for Windows

DEB – for Debian-based distributives (Ubuntu, Debian, etc.)

RPM – for RPM-based distributives (CentOS, SLES, etc.)

TAR – for Linux manual installation

2. Install Elasticsearch depending on your system.

(Please make sure that you have permission to install packages).

- a. For Debian-based distributives, please use this command:

Installation and Configuration Guide

sudo dpkg -i elasticsearch-1.4.4.deb

b. For RPM-based distributives, please use this command:

rpm -i elasticsearch-1.4.4.noarch.rpm

c. Manual installation for Linux

1. Extract TAR GZIP archive by command:

tar -zxvf elasticsearch-1.4.4.tar.gz

(After extraction, "elasticsearch-1.4.4" folder will be created automatically)

2. Move the extracted folder to the location you want.

e.g., "/opt/elasticsearch-1.4.4"

mv elasticsearch-1.4.4 /opt

(You can delete the tar.gz file afterwards)

3. To make Elasticsearch runnable as a service, please follow the official instructions:

<https://www.elastic.co/guide/en/elasticsearch/reference/1.4/setup-service.html>

d. Manual installation for Windows

1. Extract elasticsearch-1.4.4.zip archive by using Windows Explorer option "Extract All" (after extraction "elasticsearch-1.4.4" folder will be created automatically).

2. Move the extracted folder to the location you want.

e.g., "\\Programs\\elasticsearch-1.4.4"

(You can delete the zip file afterwards)

3. To make Elasticsearch runnable as a service, please follow the official instructions:

<https://www.elastic.co/guide/en/elasticsearch/reference/1.4/setup-service-win.html>

Installation and Configuration Guide

3.3 Configure Elasticsearch

3.3.1 Config file changes

Configure Elasticsearch stored in "elasticsearch.yml" file which is located in "config" folders for manual installation or in "/etc/Elasticsearch" for Linux DEB and RPM distributives. To make changes, you need to edit this file in text editor:

1. Change the cluster name.
Uncomment line "cluster.name: auditserver" and rename your cluster name.
2. Increase Boolean operators amount.
Add the following line to the end of file: "index.query.bool.max_clause_count: 16536"
3. Max opened files adjustments. If you have installed Elasticsearch manually, you need to increase the limit of max_file_descriptors with command:

sysctl -w vm.max_map_count=262144

If you installed Elasticsearch from RPM or DEB, this variable will be defined automatically; to check this run command:

sysctl vm.max_map_count

```
kot@kostik-pc:~$ sysctl vm.max_map_count
vm.max_map_count = 262144
kot@kostik-pc:~$
```

4. Restart Elasticsearch.

3.3.2 Start, stop, status of Elasticsearch

For normal work of Audit Dashboard, make sure that Elasticsearch is running.

You can run it manually from the Elasticsearch folder:

- on Linux bin/Elasticsearch
- on Windows bin/Elasticsearch.bat

For a production environment we recommend making Elasticsearch runnable as a service with each system start.

For Linux, use the following commands to control your Elasticsearch server (from users which have permissions to do this):

- Check status service Elasticsearch status
- Start service service Elasticsearch start
- Stop service service Elasticsearch stop

For Windows, use "service.bat" commands to control your Elasticsearch service (located in "bin" folder):

- Install as a service **service.bat install**
- Remove service **service.bat remove**
- Start service **service.bat start**
- Stop service **service.bat stop**
- Start GUI manager **service.bat manager**

Installation and Configuration Guide

```
kot@kostik-pc:~$ curl 'http://127.0.0.1:9200'
{
  "status" : 200,
  "name" : "Kiss",
  "cluster_name" : "elasticsearch",
  "version" : {
    "number" : "1.4.4",
    "build_hash" : "c88f77ffc81301dfa9dfd81ca2232f09588bd512",
    "build_timestamp" : "2015-02-19T13:05:36Z",
    "build_snapshot" : false,
    "lucene_version" : "4.10.3"
  },
  "tagline" : "You Know, for Search"
}
```

For more details, please read official instructions:

<https://www.elastic.co/guide/en/Elasticsearch/reference/1.4/setup-service-win.html>

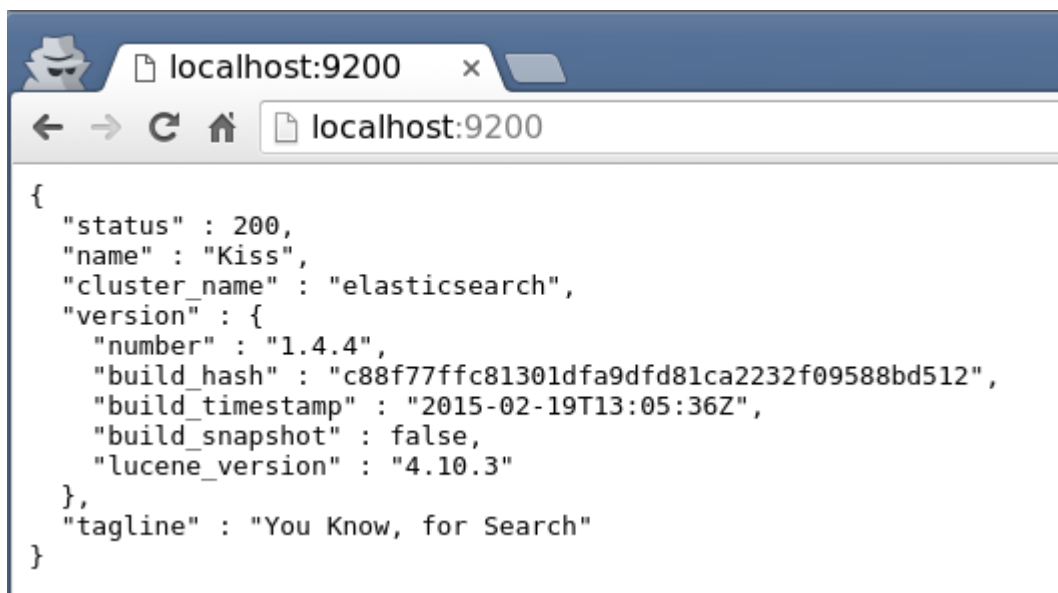
3.3.3 Check if your Elasticsearch is running

After your Elasticsearch server is started, please make sure that it is working correctly.

To check if Elasticsearch is running:

Open the following URL in a browser: <http://HOST:9200>

(HOST is name or IP address of the server where Elasticsearch is installed. e.g., <http://127.0.0.1:9200>)



If everything is successful, you will see JSON data with the current status of the Elasticsearch server.

Use CURL command:

curl -XGET 'http://HOST:9200'

If everything is successful, you will see JSON data with the current status of the Elasticsearch server.

Now you can go to the next step.

For more details, please follow the official instructions for installation of Elasticsearch <https://www.elastic.co/guide/en/elasticsearch/reference/1.4/installation.html>

If you deploy Elasticsearch for production, please follow the official deploying user guide <https://www.elastic.co/guide/en/elasticsearch/guide/1.x/deploy.html>

Installation and Configuration Guide

3.4 Install the Audit Server

3.4.1 Unpacking and manual start

The next step is the installation of the Audit Server components.

Make sure that you have Java Installed. If no Java is installed, please follow the instructions on how to install Java on your system in chapter "3.1 Install Oracle Java."

The Audit Server is a self-extracting jar file. To install and start, please:

1. Extract the archive.

Extract content of the "AuditServer-2.0.zip" file

- For Linux, use command:
unzip AuditServer-2.0.zip
- For Windows, please use Windows Explorer option "Extract All"
(After extraction "AuditServer-2.0" folder will be created automatically.)

2. Move the extracted folder.

Move the extracted folder to the location you want.

- Linux: e.g., /opt/AuditServer-2.0
- Windows e.g., \Programs\AuditServer-2.0 (you can delete the zip file afterwards)

3. Manual start and stop.

Start the Audit Server with the script or batch file, depending on your system:

- Linux start.sh
- Windows start.bat

(If JAVA_HOME variable is not defined on your system, you may have to adjust the path to Java Runtime Environment in script or batch file. The path to Java depends on your Java installation.)

To stop the Audit Server, please use the following way depending on your system:

- Linux stop.sh
- Windows close the CMD window

3.4.2 Make runnable as a service for Linux

For a production environment, we recommend making Audit Server runnable as a service with each system start. To make this, please follow these steps:

1. Move the script file, which is located in the "service-script" folder, to your "/etc/init.d" folder.

```
sudo mv ./service-script/audit-server /etc/init.d/audit-server
```

2. Open in editor "service-script" file and change the APP_PATH variable to the path where your Audit Server is located.

```
sudo vi /etc/init.d/audit-server
```

(e.g., APP_PATH="/opt/idm/AuditServer-2.0")

3. Give this script executable permission (e.g., 775, but you can set it lower).

```
sudo chmod 775 /etc/init.d/audit-server
```

Installation and Configuration Guide

4. Add to startup list with the default startup priority.
sudo update-rc.d audit-server defaults
5. Reboot the server or start the Audit Server as a service.
sudo service audit-server start

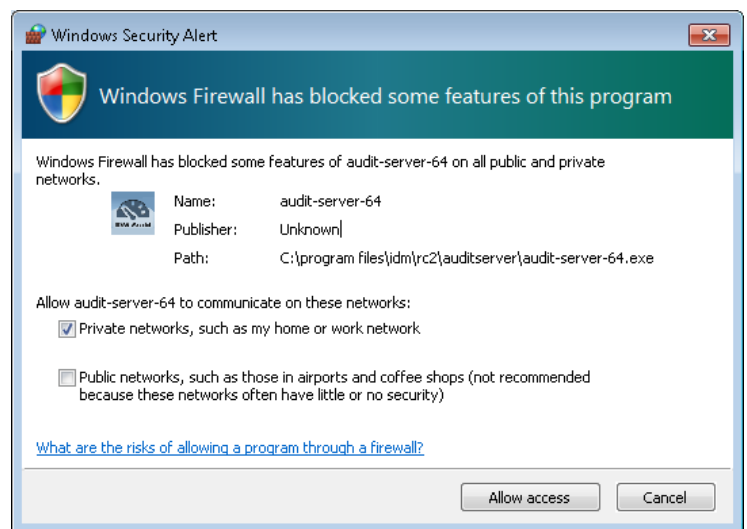
3.4.3 Make runnable as a process for Windows

For a production environment, we recommend making Audit Server runnable as a Windows process with the system start. To make this, please follow these steps:

1. Open in editor "audit-server-64.ini" or "audit-server.ini", depending on your system architecture.
2. Change "working.directory" variable with the path where the Audit Server is located, e.g., working.directory="c:\Programs \AuditServer-2.0".
3. Uncomment and change "vm.location" variable with location of the "JVM.dll" file (if your JAVA_PATH is not defined globally).
e.g., vm.location="C:\program files\Java\jre1.8.0_91\bin\client\JVM.dll"

4. Run "audit-server-64.exe" or "audit-server.exe", depending on your system.

Please allow Firewall prompt. If everything is correct, you will see the Audit-Server process in Windows Task Manager. You can end it by clicking the "End Process" button.



5. Open in editor "AuditServerTask.xml", (which is located in "service-script" folder of your Audit Server installation).
 - f. Replace path between <command></command> tags.

(The path should correspond to your "audit-server.exe" or "audit-server-64.exe" location.)

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<Actions Context="Author">
  <Exec>
    <Command>C:\Programs\AuditServer-2.0\audit-server.exe</Command>
  </Exec>
</Actions>
```

6. Save file.
7. Run cmd.exe, CMD window will be opened.
8. Go to the folder where your Audit Server is located.
9. e.g., c:\Programs\AuditServer-2.0

Installation and Configuration Guide

10. Run the command for import AuditServerTask.xml to Task Scheduler:

```
schtasks /create /tn "AuditServer" /xml "service- script/AuditServerTask.xml" /RU "Administraror" /RP "YourPassword"
```

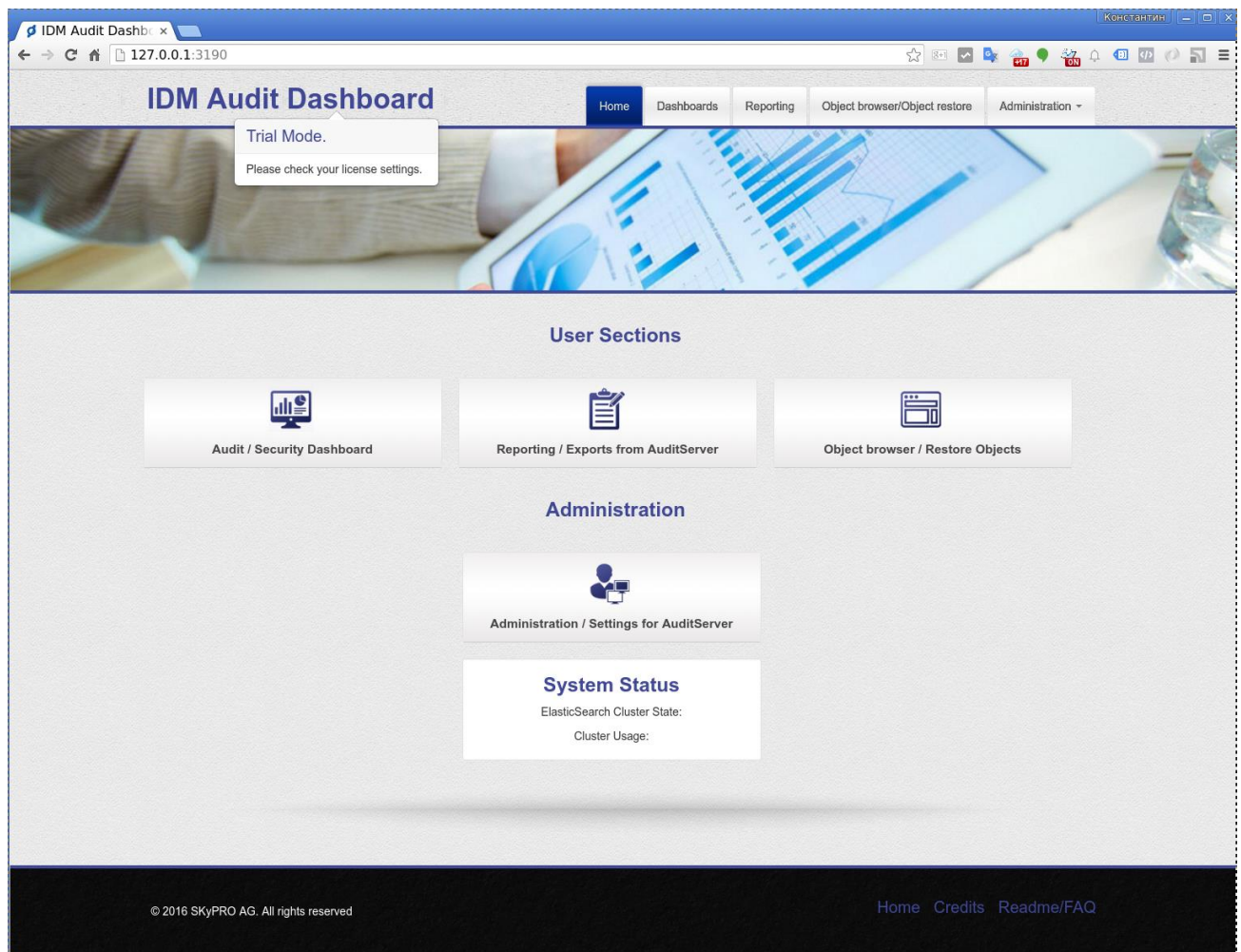
(Replace "Administraror" and "YourPassword" with the user name and the password of the user you would like to start Audit Server with.)

11. After the task has been successfully created, you need to restart your server.

3.4.4 Check if your Audit Server is running

To check your Audit Server, please open the following URL in browser: <http://HOST:3190> (Where HOST is name or IP address of the server on which the Audit Server is installed. e.g., <http://127.0.0.1:3190>)

The Audit Server Home will be opened. Don't worry if no System Status information appears on the bottom. You have to configure the connection to the Elasticsearch server first, if it is not running or not running on your local Audit Server engine.



Installation and Configuration Guide

3.5 Update Audit Server

3.5.1 Copy setting from the previous version of Audit Server

If you have already installed Audit Server 1.0, you can use its settings with the newest version of Audit Server 2.0, and for this you need:

1. Stop Audit Server 1.0.
2. Install Audit Server 2.0 (follow the instructions in chapter 3.4. Install the Audit Server).
3. Make sure Audit Server is not running.
Copy DB file "auditserver.mv.db" from the old folder to the new one
e.g., cp /opt/AuditServer/auditserver.mv.db /opt/AuditServer-2.0/
4. Start Audit Server 2.0.

3.5.2 Update default Audit Server report templates

New version of Audit Server contains new predefined report templates which will be deployed when Audit Server 2.0 starts on a clean system.

If you already have Audit Server 1.0, you can force this action by:

1. Remove "/asreports" index from your Elasticsearch server by command:
curl -XDELETE '<http://host:9200/asreports>'
2. Restart or start Audit Server 2.0.
(New report templates will be installed at startup.)

Warning: if you remove "/asreports" index all your report templates will be removed !

If you would like to remove your old report templates and install the new ones from Audit Server 2.0 manually:

1. Go to the "reports/content" folder in your Audit Server 2.0 location, e.g.,
"/opt/AuditServer-2.0/reports/content" or "c:/Programs/AuditServer-2.0/reports/content"
2. Run the following commands in your terminal or console (make sure that CURL tool is installed on your system):

```
curl -XPOST 'http://ES_HOST:9200/asreports/content' -d  
@DefaultAuditReport.json
```

```
curl -XPOST 'http://ES_HOST:9200/asreports/content' -d  
@DefaultUserReport.json
```

```
curl -XPOST 'http://ES_HOST:9200/asreports/content' -d  
@DefaultGroupReport.json
```

(ES_HOST is the host name or IP address of the server where Elasticsearch is running)

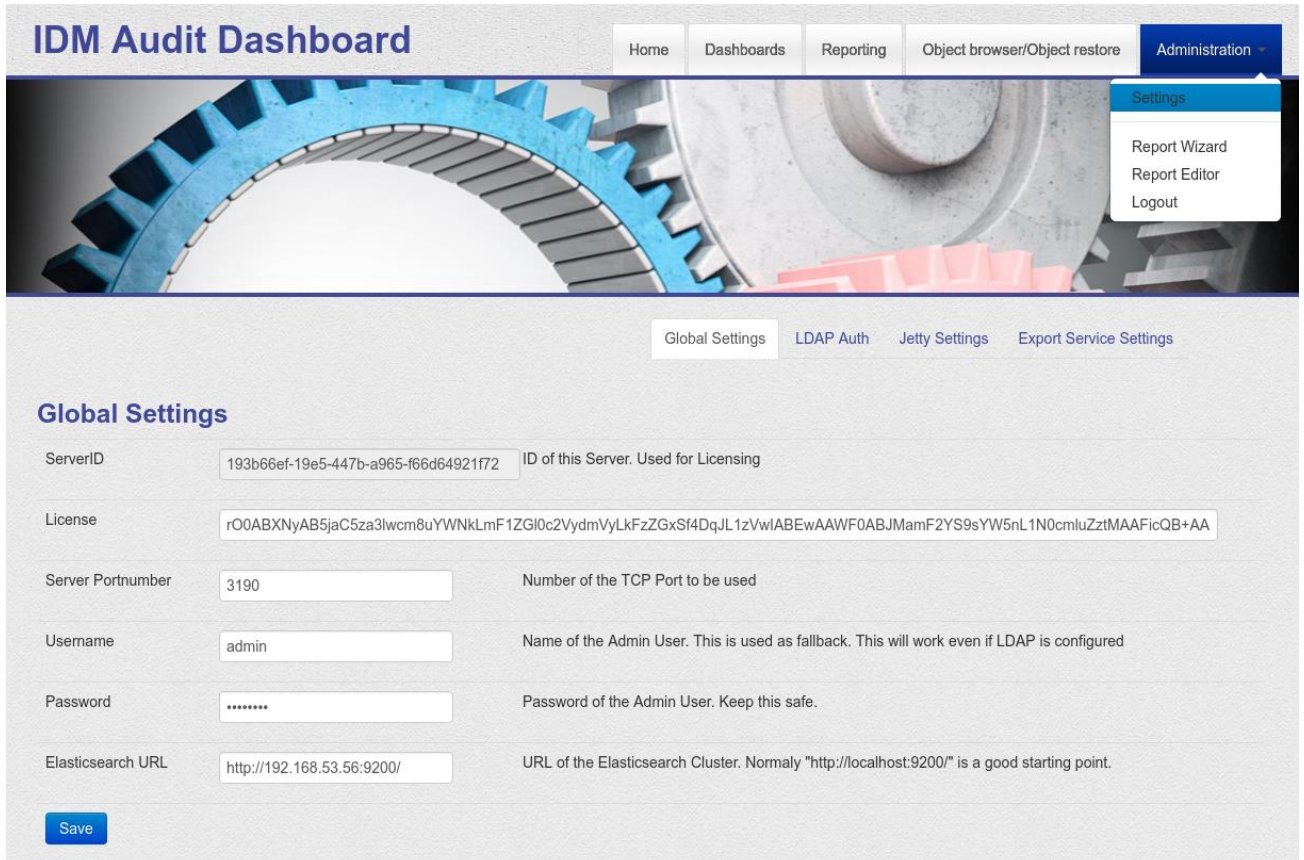
Installation and Configuration Guide

3.6 Configure the Audit Server

Before you can use the Audit Server, you have to configure the connection to the Elasticsearch server.

1. Click "Settings" from "Administration" menu. When User Name and Password are prompted, leave them empty and press Log In.

The basic configuration page will look like this:



IDM Audit Dashboard

Home Dashboards Reporting Object browser/Object restore Administration

Settings

Report Wizard
Report Editor
Logout

Global Settings LDAP Auth Jetty Settings Export Service Settings

Global Settings

ServerID: 193b66ef-19e5-447b-a965-f66d64921f72 ID of this Server. Used for Licensing

License: r00ABXNyAB5jaC5za3lwcm8uYWNLmF1ZGI0c2VydmVyLkFzZGxSf4DQJL1zVwIABEwAAWF0ABJMamF2YS9sYW5nL1N0cmIuZztMAAFicQB+AA

Server Portnumber: 3190 Number of the TCP Port to be used

Username: admin Name of the Admin User. This is used as fallback. This will work even if LDAP is configured

Password: Password of the Admin User. Keep this safe.

Elasticsearch URL: http://192.168.53.56:9200/ URL of the Elasticsearch Cluster. Normally "http://localhost:9200/" is a good starting point.

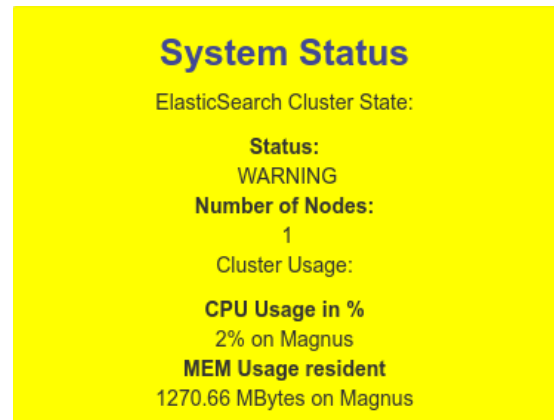
Save

2. Paste your license code if you have it. If no license is available, Audit Server will work in trial mode.
3. Enter the port number of your Audit Server. By default it is 3190.
4. Specify the user ID and the password for the admin account. Please write it down. You won't be able to open the administration page afterwards without these credentials.
5. Please enter the URL and the port of your Elasticsearch server. By default it is:
<http://HOST:9200/>
6. Save changes.
7. Restart the Audit Server.

Installation and Configuration Guide

8. Check the Elasticsearch server connection.

If your configuration is OK, you'll see a green (or yellow) status of your Elasticsearch server at the bottom of the home screen. The yellow warning means that you do not have an Elasticsearch cluster in place so your system is not fault-tolerant.



3.7 Install the Audit Driver

3.7.1 Install the Audit Driver with Identity Manager

1. Extract the archive.

Extract the content of the "AuditDriver-1.0RC2.zip" file.
(After extraction, an "AuditDriver-1.0RC2" folder will be created automatically. All you need is inside this folder.)

2. Copy needed Java class and template files.

Copy the driver appshims files to the dirxml class directory of your IDM server:

- auditdriver.jar
- common-io-1.4.jar
- json-simple-1.1.1.jar
- template.json

e.g., On SUSE Linux the default path is the following:
"/opt/novell/eDirectory/lib/dirxml/classes"

Check your dirxml class directory eDirectory/lib/dirxml/classes on your server.

3. Open the NetIQ iManager URL in your browser
https://YOUR_HOST_NAME/nps/servlet/portal

Installation and Configuration Guide



4. Chose "Identity Manager Overview" and select a container where your Driver Set is placed.

Identity Manager Overview

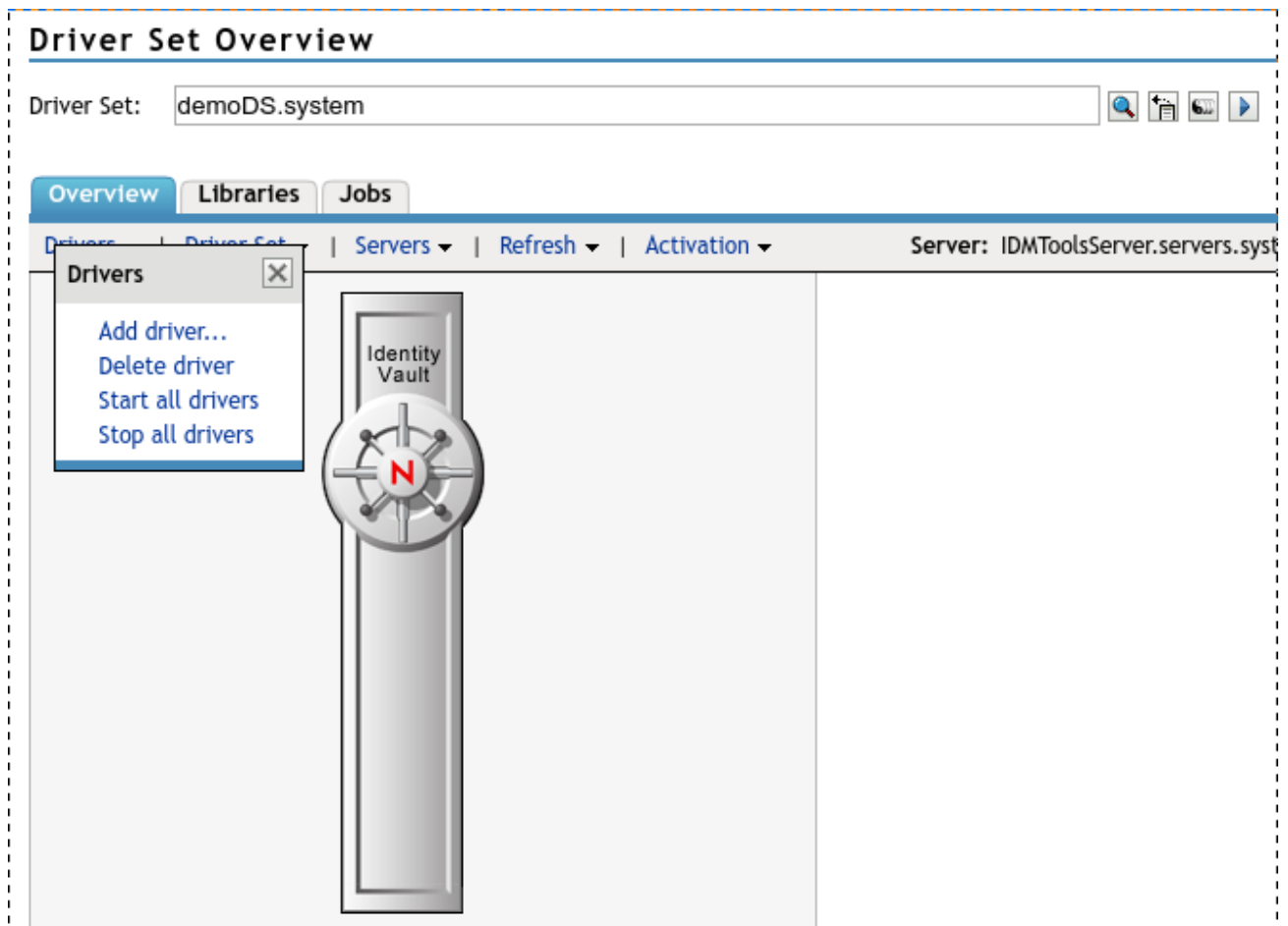
Specify the container you want to search, then press the search button.

Search in:   

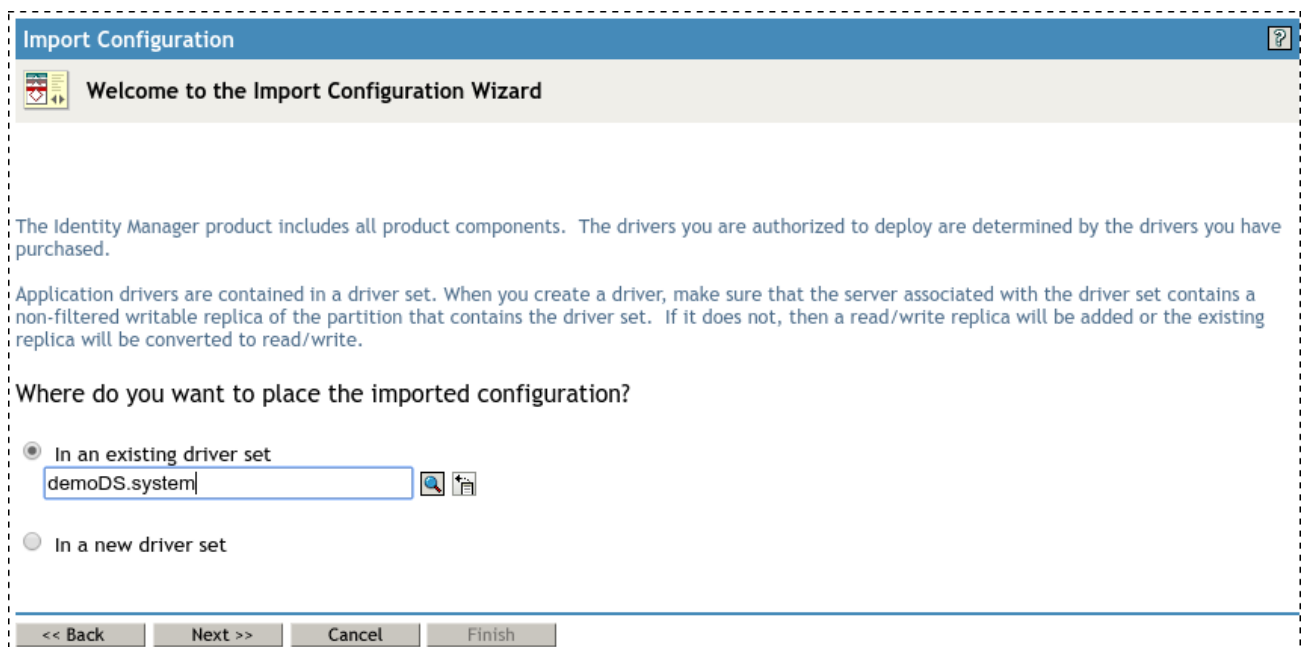
Driver Sets Libraries	
New... Delete Activation Edit Export	
☐ Name	Container
☐ demoDS	system

5. Select or create your Driver Set.
6. In the "Overview" tab, please select "Drivers" → "Add driver"

Installation and Configuration Guide



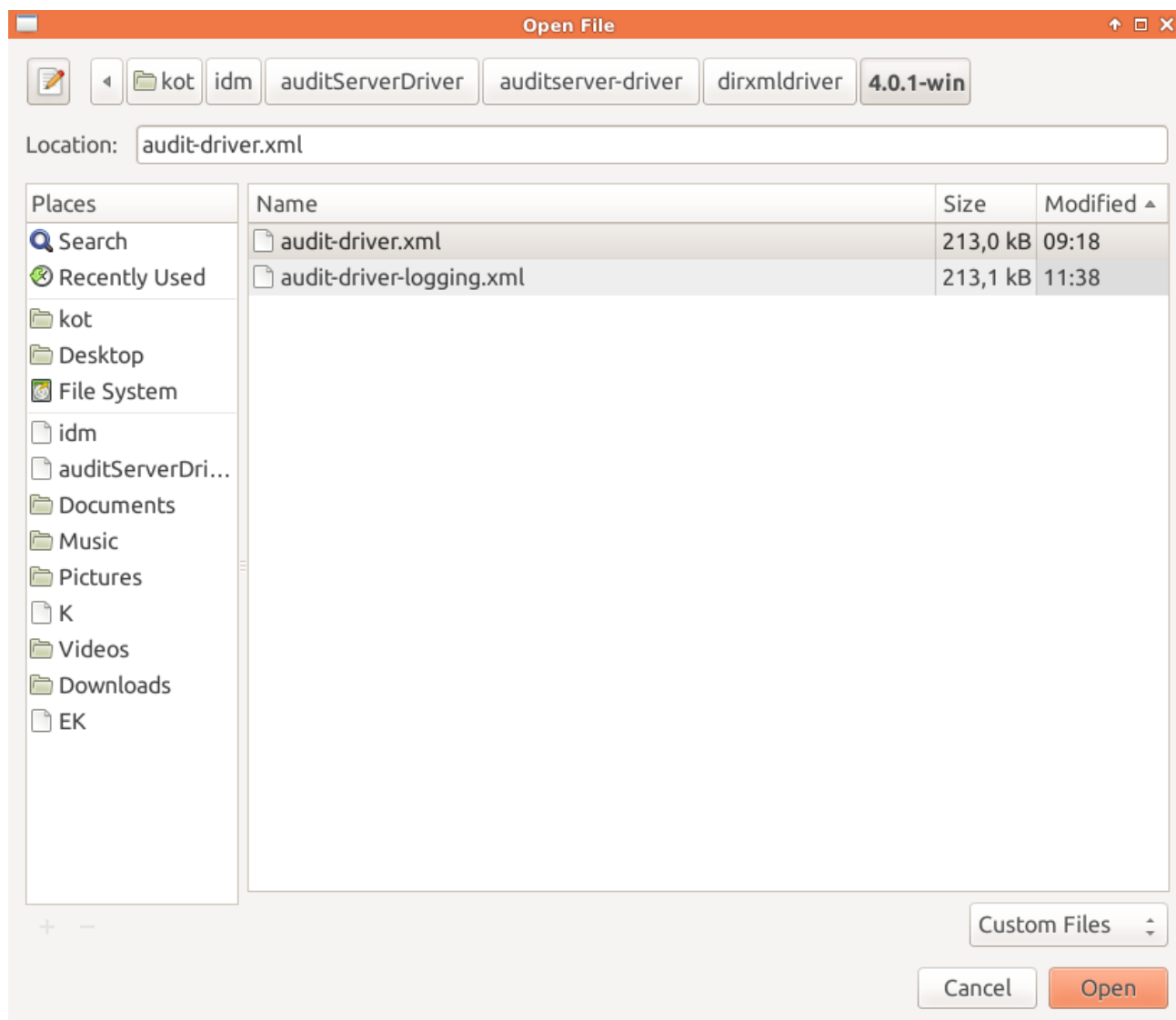
7. In "Import Configuration" select where you would like to place the imported configuration.



Click "Next".

8. Chose Import a configuration from the client (.XML file) and browse "audit-driver-1.0-rc2.xml" file to a local storage location.

Installation and Configuration Guide



Click "Open" and then "Next".

9. Enter the name of the driver which you would like to use.



audit-driver (Driver)

The driver writer requested that the following information be supplied in order to import this configuration file. An * indicates required information.

The name of the driver contained in the driver configuration file is "audit-driver". Enter the actual name you want to use for the driver.

Driver name: *

Installation and Configuration Guide

Click "Next".

10. Chose "Update everything about that driver and policy libraries" and select the check box "Including the driver's image".



One or more of the policy libraries already exist. Select one of the options below or select back to specify different locations for the policy libraries.

- ☐ Specify a different name for the driver and/or location for the policy libraries
- ☒ Update everything about that driver and policy libraries (☒ including the driver's image)
- ☐ Update only selected policies in that driver and policy libraries (☐ including the driver's filter)

Select those policies from the list below that you want updated. Nothing else about the driver or policy libraries will be changed.

- ☐ Delete Object after Add (Subscriber - DirXML Script)
- ☐ Modify Timestamp Format (Subscriber - DirXML Script)
- ☐ Scramble Password (Subscriber - DirXML Script)
- ☐ Veto Unneeded Operations (Subscriber - DirXML Script)
- ☐ Veto if not all Needed Attributes (Subscriber - DirXML Script)
- ☐ Wait if newly Created (Subscriber - DirXML Script)
- ☐ Modify Anything to Audit (Subscriber - XSLT)
- ☐ Remove Chars from Values (Subscriber - XSLT)
- ☐ Del Source Object (Driver - DirXML Script)
- ☐ Schema Mapping (Driver - Schema Mapping Policy)
- ☐ Input Transformation Quiet (Driver - XSLT)
- ☐ driver-attrs (Driver - Resource)
- ☐ driver-classes (Driver - Resource)
- ☐ driver-infos (Driver - Resource)
- ☐ AJC ('acdLib' Policy Library - Resource)



Click "Next".

11. Click "Define "Security Equivalences" and select an object which will be a Security Equivalent for the driver. Please note that you should select an object with enough permission to audit all necessary objects and attributes. Usually it should be the Administrator.

Installation and Configuration Guide



audit-driver (Driver)

Novell recommends you do the following for the newly created driver:

- Define 'Security Equivalences' on the driver.
- Identify all objects that represent 'Administrative Roles' and exclude them from replication.

[Define 'Security Equivalences'](#)

[Exclude 'Administrative Roles'](#)



12. Click "Exclude 'Administrative Roles'" and save them.

Excluded Users:  audit-driver.demoDS.system

 Identity Manager

Excluded Objects

The data for the excluded objects will not be replicated to the application represented by this driver.

Novell strongly recommends adding all users that serve in an "administrative role" (such as the "Admin" user) to this list.

Excluded objects:



[Retrieve Current Exclusions](#)

Warning: On a large tree, retrieving the list of currently excluded objects may take a long time.

Click "Next".

13. Take a look at "Import Configuration".

Installation and Configuration Guide

Import Configuration



Summary - Current Configuration



Info Drivers May Require Configuration

Drivers imported from a configuration file may require additional configuration settings to be fully functional. Select the driver's link to edit its configuration settings.

The following summarizes the state of the driver as it currently exists.



[IDMToolsServer](#) (NCP Server)



[demoDS](#) (Driver Set)



[audit-driver](#) (Drivers May Require Configuration) (Driver)



[Schema Mapping](#) (Schema Mapping Policy)



[Del Source Object](#) (Input Transformation Policy)



[none](#) (Output Transformation Policy)



[Publisher](#) (Publisher)



[none](#) (Command Transformation Policy)



[none](#) (Event Transformation Policy)



[none](#) (Matching Policy)



[none](#) (Creation Policy)



[none](#) (Placement Policy)



[Subscriber](#) (Subscriber)



[Delete Object after Add](#) (Command Transformation Policy)



[Scramble Password](#) (Event Transformation Policy)



[none](#) (Matching Policy)



[Veto if not all Needed Attributes](#) (Creation Policy)



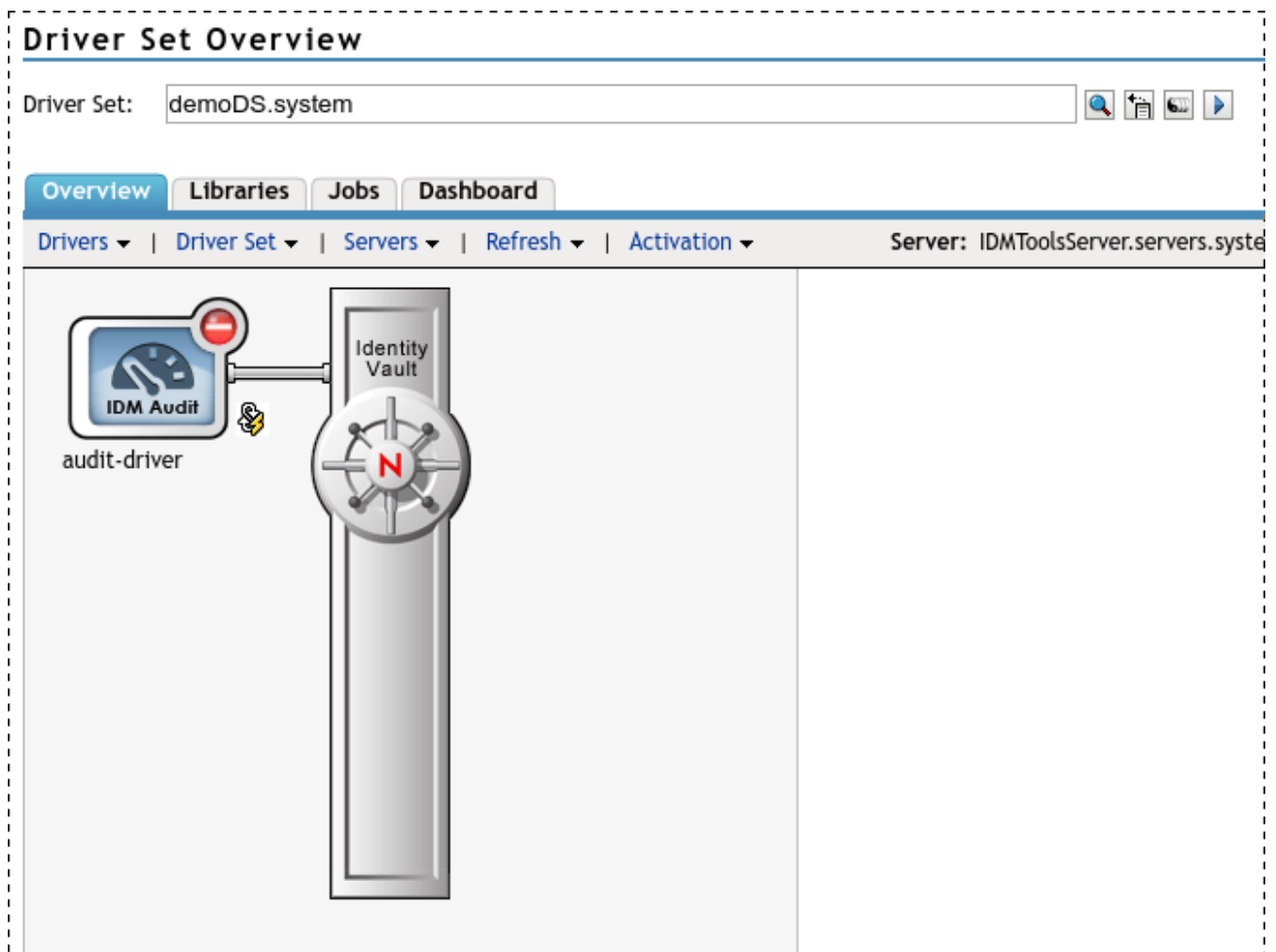
[none](#) (Placement Policy)

[<< Back](#)
[Next >>](#)
[Cancel](#)
[Finish](#)

If everything is OK, click "Finish".

14. When the page reloads, you will see that Driver is installed. But it has not started.

Installation and Configuration Guide



15. Check or define settings for the Driver. Choose "Edit Properties".

Driver Module: "Java"

Name: "ch.skypro.acd.driver.AuditDriverShim"

Startup option: "Auto start"

Driver Parameters:

Audit Server: "URL of your Elasticsearch Server"

Audit template "location of your template.json file" (step 2)

16. Save your settings and restart the driver.

Installation and Configuration Guide

Modify Object: audit-driver.demoDS.system

Identity Manager | Server Variables | General

Driver Configuration | Named Passwords | Global Config Values | Engine Control Values | Log Level | Driver Image | Security Equals | Filter | Edit Filter XML | Reciprocal Attribute Mappings | Edit Reciprocal Attribute Mappings XML | Misc | Excluded Objects | Driver Health Configuration | Driver Manifest | Driver Inspector | Driver Cache

Driver Module

☒ Java
☐ Native
☐ Connect to Remote Loader

Name: ch.skypro.aod.driver.AuditDriverDriverShim

Driver Object Password

Driver object password: [Set password](#)

Authentication

IDMToolsServer.servers.system

Authentication ID:
 Authentication context:
 Remote loader connection parameters: <Not a remote loader>
 Driver cache limit (kilobytes):
 Application password: [Set password](#)
 Remote loader password: <Not a remote loader>

Startup Option

IDMToolsServer.servers.system

☒ Auto start
☐ Manual
☐ Disabled

Driver Parameters

IDMToolsServer.servers.system

[Edit XML](#)

Driver Settings

Subscriber Settings

Disable?	no
Auditserver:	http://192.168.53.56:9200
Audittemplate:	/opt/novell/eDirectory/lib/dixml/classes/template.

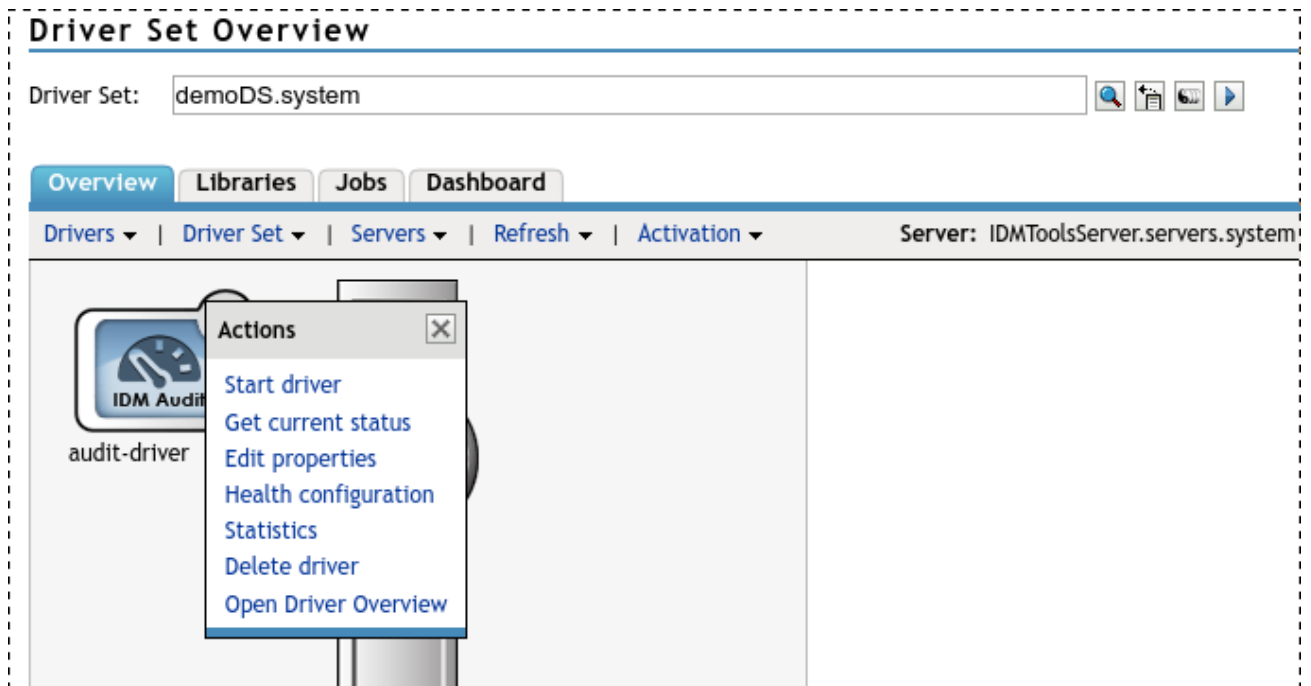
Publisher Settings

Disable?	yes
Polling Interval (seconds):	10

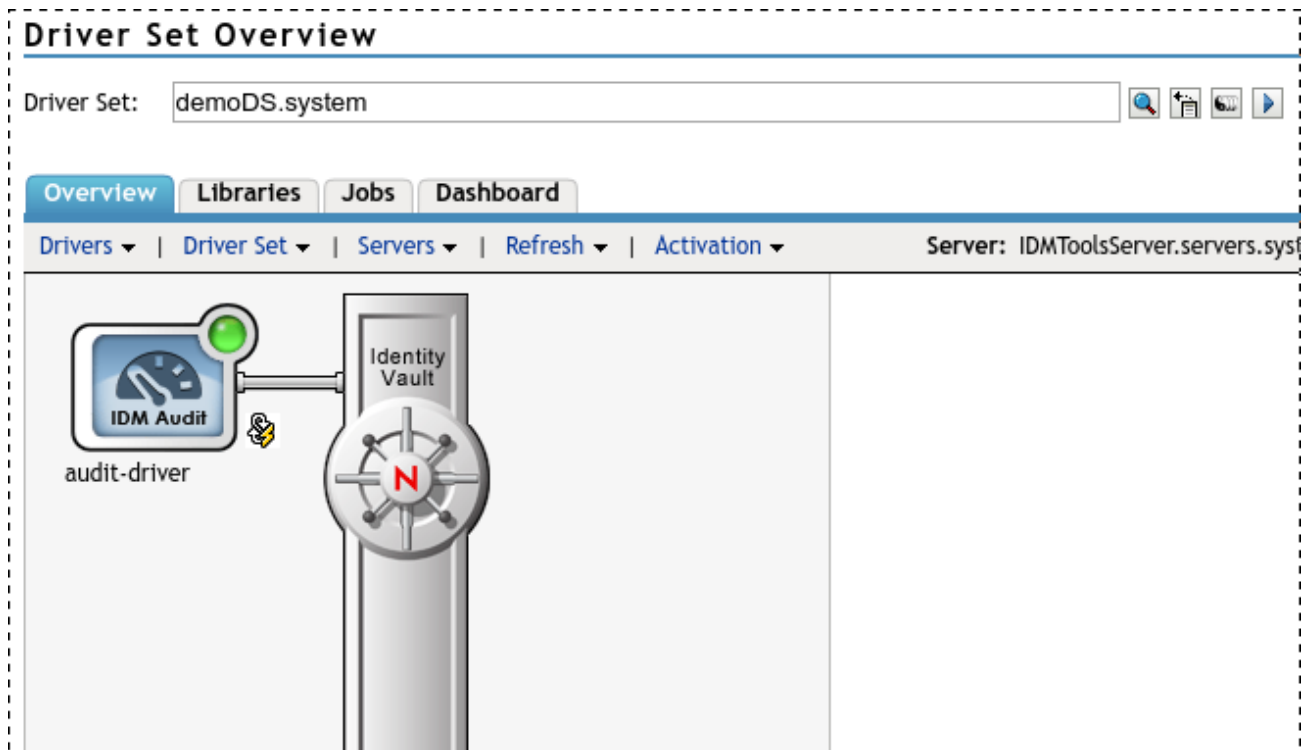
OK Cancel Apply Refresh

17. Click the red "Stop" button of the driver and select "Start driver".

Installation and Configuration Guide



18. The green button means that the Driver is started and running.



Notes:

- 1) If you are updating auditDriver.jar, a restart of IDM server could be needed. (It stores ".jar" files in a cache so a new updated file will not be used until server is restarted).
- 2) Audit Driver reads license from ES at each start of the Driver. To update Driver license information you need to restart the Driver. (By default, if license is not found or Driver has no connection to the ES server, the trial mode will be enabled.)

Installation and Configuration Guide

3.7.2 Install the Audit Driver with NetIQ IDM Designer

Now we create the Audit Driver with IDM Designer.

1. Copy needed Java class files

Copy the driver appshim files to the dirxml class directory of your IDM server:

- auditdriver.jar
- common-io-1.4.jar
- json-simple-1.1.1.jar
- template.json

On SUSE linux the default path is

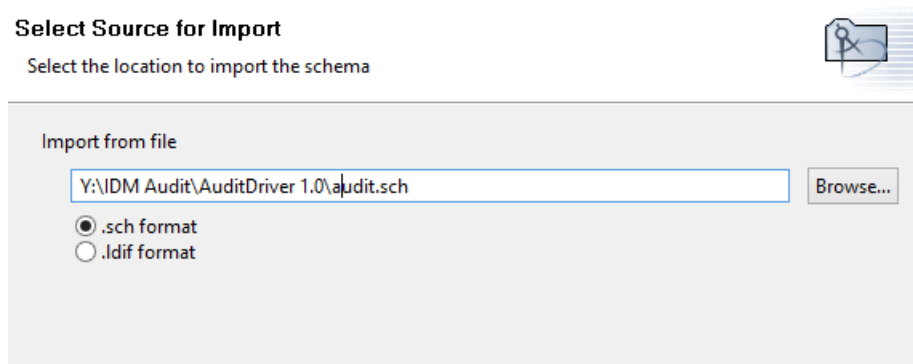
/opt/novell/eDirectory/lib/dirxml/classes.

Check your dirxml class directory *eDirectory/lib/dirxml/classes* on your server.

2. Extend Schema

To enable even Drivers to audit their specific events by the Audit Driver, we have to extend the schema with our audit class. Right click on your identity vault and choose "Import schema from file".

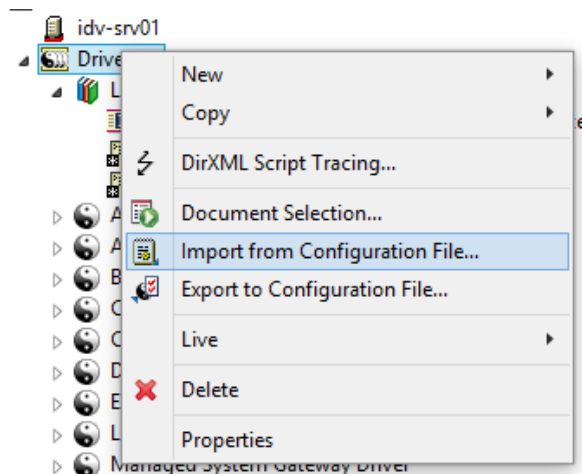
Select file "audit.sch" provided in directory "Audit Driver 1.0".



Select "Next" and "Finish". Save the configuration change.

3. Import the Driver into Designer.

Right click on your Driver set and choose "Import from configuration file".



Installation and Configuration Guide

Choose file "audit-driver-1.0-rc2.xml", that is provided in directory "AuditDriver 1.0 RC2" and click "Ok".

Name your Driver (e.g., audit-driver) and choose the container where you would like to place the library "acdLib".

Authentication password and Driver password can be left empty.

The screenshot shows a 'Driver Configuration' dialog box. At the top, it says: 'Enter the driver name. Selecting an existing driver will overwrite the driver configuration as a default value by the configuration file.' Below this is a 'Driver name:' label followed by a text box containing 'audit-driver' and a small icon button. The next section says: 'When importing a configuration containing a policy library that was outside the container in which you want the imported policy library created. All references to correspond to its new location.' This is followed by the instruction: 'Select the container where you want to create the policy library named \'acdLib\'' and a text box containing 'DriverSet.IDM.system' with a search icon and a folder icon. The bottom section has three pairs of input fields: 'Enter the authentication password:', 'Reenter the password:', 'Enter the driver password:', and 'Reenter the password:'.

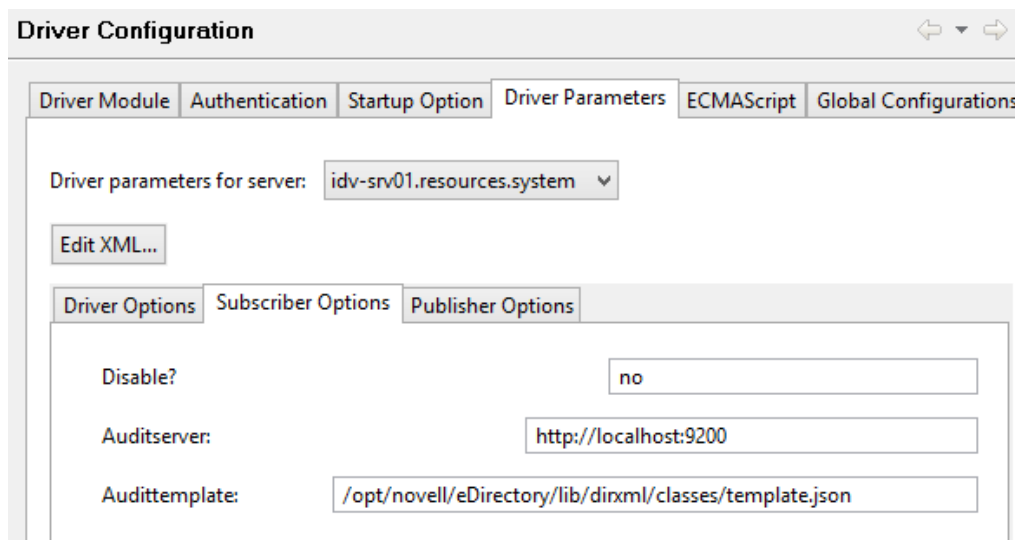
Click "Finish" and "Ok".

4. Configure the Driver

Right click the Driver and open the Driver properties. Go to the *Driver Configuration* and open the *Driver Parameters* Tab.

Click the *Subscriber Options* tab. Provide the correct IP address to your Elasticsearch server. Also, enter the folder and filename where you have copied the JSON template file.

Installation and Configuration Guide



Adjust the trace file settings to your requirements. Also, rename the Driver icon or replace the icon image as you like.

Save the Driver configuration.

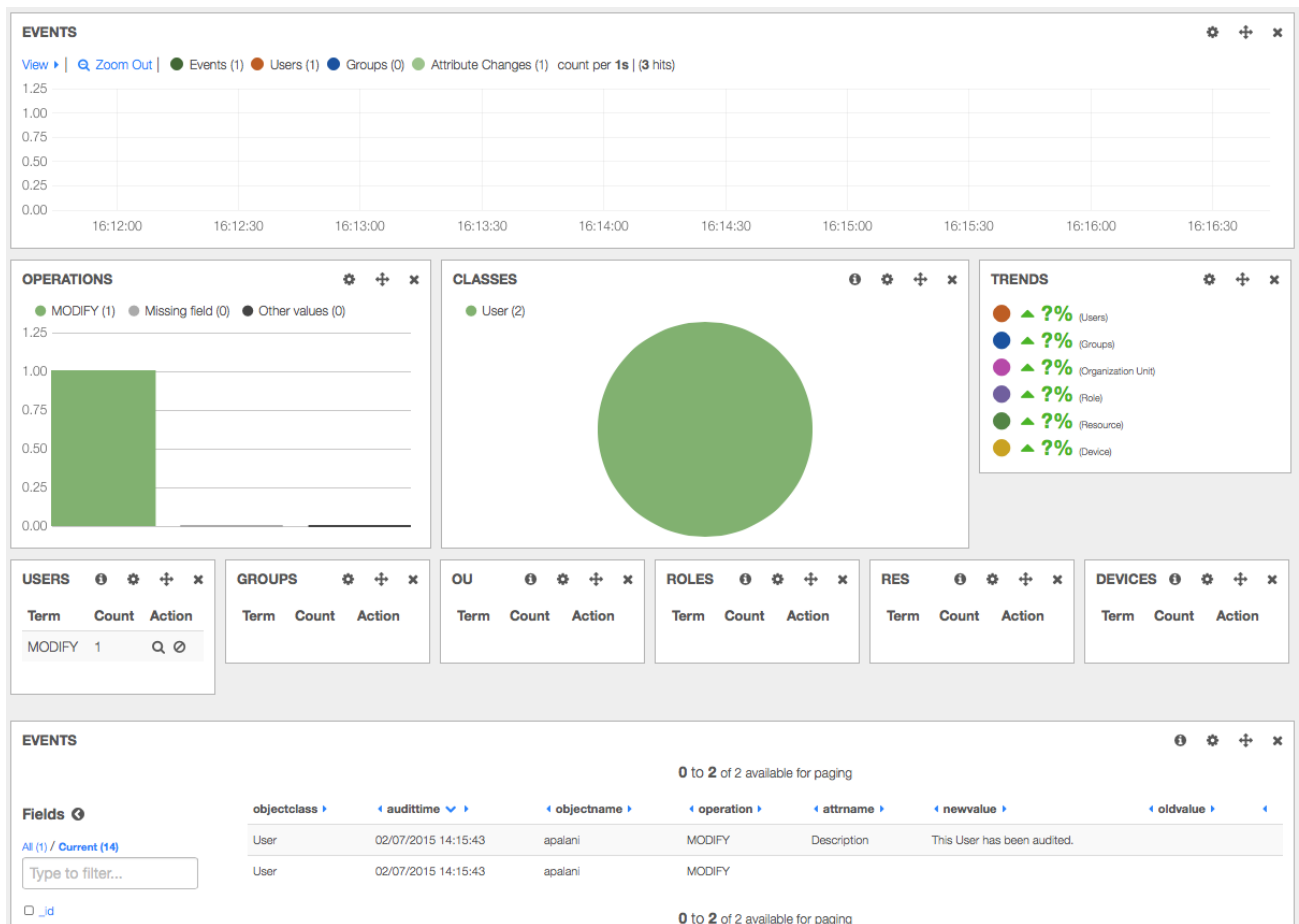
5. Deploy the Driver
Right click on the Driver and choose live/deploy. Define as Security Equivalences a user that has the right to read all objects and attributes that the Driver has to monitor.
6. Adjust Driver filter
If you would like to monitor more or less objects or attributes, just open the Driver filter and change the filter accordingly. You do not have to change anything else!

Installation and Configuration Guide

3.7.3 Test the Driver

To test the Driver, start the Driver and change description attribute of the user to, e.g., "This user has been audited". The modify event should be successfully synchronized with the Audit Server.

Open your browser and navigate to your Audit Dashboard URL by default on port 3190. From the home screen, click "Dashboards" (enter username and password, if you have defined one) and select "IDM Audit Dashboard". Click the refresh button in the upper right corner and open the event table at the bottom by pressing the expand triangle icon. You should see the Modify event for attribute "Description".



Installation and Configuration Guide

3.8 Install the Report Service

Make sure you have installed Java. If Java is not installed, please follow the instructions on how to install Java for your system in chapter 3.1 "Install the Oracle Java."

3.8.1 Extract and manual start

1. To install the Report Service, please follow these steps:

Extract archive.

Extract content of the "AuditReport-1.0RC1.zip" file

For Linux, use command: **unzip AuditReport-1.0RC1.zip**

For Windows, please use Windows Explorer option "Extract All"

(After extraction, an "AuditReport-1.0RC1" folder will be created automatically.)

2. Move extracted folder.

Move the extracted folder to the location you want.

Linux: e.g., /opt/AuditReport-1.0RC1

Windows: e.g., \Programs\AuditReport-1.0RC1

(You can delete .zip file afterwards)

3. Configure Report Service.

Open the Report Service configuration file "reportservice.yml" using a text editor.
Provide the correct parameters to connect to your directory using LDAP.

ldapservice: URL and port of your eDirectory LDAP server

userdn: DN of the user that connects to your LDAP

This user must have read rights to all object and attribute data you would like to store:

esserver: URL and port of your Elasticsearch server

userpw: Password of the LDAP user

templatename: Filename of the JSON template

mandant: Name of the tenant in case you enabled the multitenant

feature of the Audit Server

```
config:
  ldapservice: 'ldap://localhost:389'
  userdn: 'cn=admin,ou=users,o=system'
  userpw: 'netiq000'
  esserver: 'http://localhost:9200/'
  templatename: 'template.json'
  mandant: 'default'
```

4. Manually start and stop.

Start the Audit Report with the script or batch file depending on your system:

Installation and Configuration Guide

- Linux: start.sh
- Windows: start.bat

(If JAVA_HOME variable is not defined in your system, you may have to adjust the path to Java Runtime Environment in script or batch file. The path to Java depends on your Java installation.)

To stop the Audit Server, please use the following way depending on your system:

- Linux: stop.sh
- Windows: close the CMD window

3.8.2 Make runnable as service for Linux

For a production environment, we recommend making Audit Report runnable as service on each system start. To make this, please follow these steps:

1. Move script file which is located in "service-script" folder to your "/etc/init.d" folder.

sudo mv ./service-script/audit-report /etc/init.d/audit-report

2. Open in editor "service-script" file and change the APP_PATH variable with path where your Audit Report is located.

sudo vi /etc/init.d/audit-report

(e.g., APP_PATH="/opt/idm/AuditReport-1.0RC1")

3. Give this script executable permission (e.g., 775, but you can set it lower).

sudo chmod 775 /etc/init.d/audit-report

4. Include in startup list with default startup priority.

sudo update-rc.d audit-report defaults

5. Reboot server or start the Audit Report as service.

sudo service audit-report start

6. Schedule runs.

Add crontab entry with the command from the user you are currently logged in, e.g., from the user *root*:

crontab -e

entry: 05 1 * * * service audit-report start

3.8.3 Make runnable as a service for Windows

For a production environment, we recommend making Audit Report runnable as a Windows process scheduled to create a daily snapshot. To make this, please follow these steps:

1. Open in editor "audit-report-64.ini" or "audit-report.ini", depending on your system architecture.

Installation and Configuration Guide

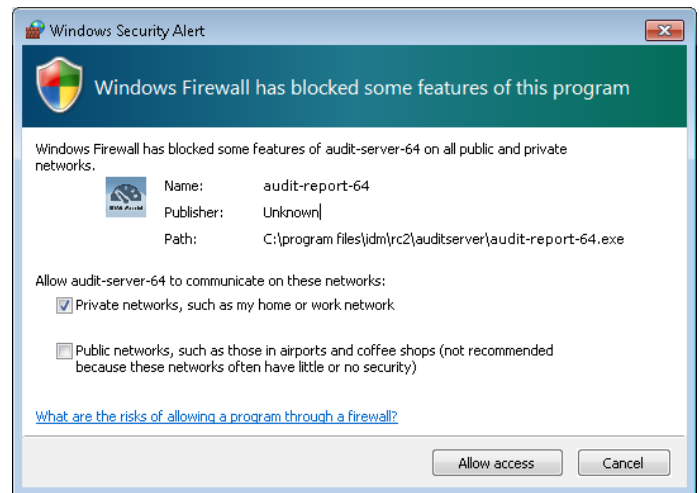
2. Change "working.directory" variable with path where Audit Report is located, e.g., working.directory="c:\Programs \AuditReport-2.0".
3. Uncomment and change "vm.location" variable with location of "JVM.dll" file (if your JAVA_PATH not defined globally).

e.g., vm.location="C:\program files\Java\jre1.8.0_91\bin\client\JVM.dll"

4. Run "audit-report-64.exe" or "audit-report.exe", depending on your system.

Please allow Firewall prompt.

If everything is correct, you will see audit-report process in Windows Task Manager. (You can end it by clicking the "End Process" button.)



5. Scheduled start.

Open in editor "AuditReportTask.xml" (which is located in the "service-script" folder of your Audit Report installation).

6. Replace Date and Time between <StartBoundary></StartBoundary> .

e.g., 2016.05.16T00:05:00 means that task will be started from 2016.05.16 at 00:05:00 and will continuously start at that time.

```
<Triggers>
  <CalendarTrigger>
    <StartBoundary>2016-05-16T00:05:00</StartBoundary>
    <Enabled>true</Enabled>
    <ScheduleByDay>
      <DaysInterval>1</DaysInterval>
    </ScheduleByDay>
  </CalendarTrigger>
</Triggers>
```

7. Replace path between <command></command> tags.

(The path should correspond to your "audit-report.exe" or "audit-report-64.exe" location.)

```
<Actions Context="Author">
  <Exec>
    <Command>C:\Programs\AuditReport-1.0RC1\audit-report-service.exe</Command>
  </Exec>
</Actions>
```

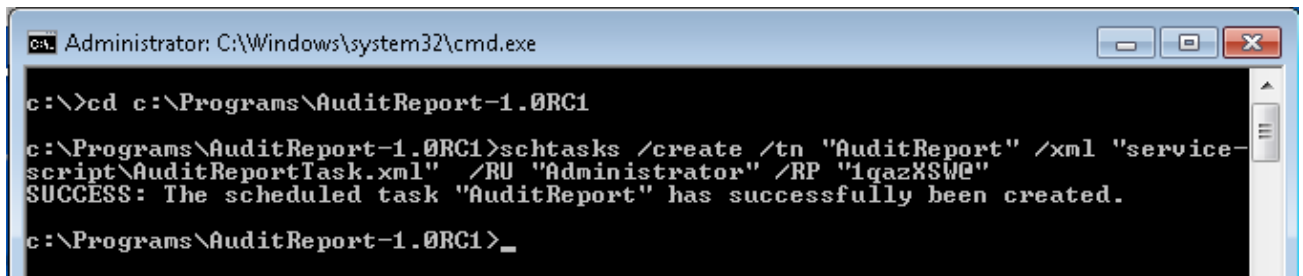
8. Save file.
9. Run cmd.exe; it will open CMD window.
10. Go to the folder where your Audit Server is located.

Installation and Configuration Guide

e.g., c:\Programs\AuditReport-1.0RC1

11. Run the command to import AuditReportTask.xml to Task Scheduler:

```
schtasks /create /tn "AuditReport" /xml "service- script/AuditReportTask.xml" /RU  
"Administrator" /RP "YourPassword"
```

A screenshot of a Windows command prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The window shows the following commands and output:

```
c:\>cd c:\Programs\AuditReport-1.0RC1  
c:\Programs\AuditReport-1.0RC1>schtasks /create /tn "AuditReport" /xml "service-  
script\AuditReportTask.xml" /RU "Administrator" /RP "iqazXSWQ"  
SUCCESS: The scheduled task "AuditReport" has successfully been created.  
c:\Programs\AuditReport-1.0RC1>_
```

Replace "Administrator" and "YourPassword" with the user name and the password of the user you would like to run Audit Server with.

Installation and Configuration Guide

3.8.4 Check the history

The Report Service will create a snapshot with the name "default yyyy.mm.dd". To access the snapshot please open your browser and navigate to your Audit Dashboard. Select "Object Browser/Object Restore". Choose the snapshot you have just taken of the available Report Indexes and browse through the directory tree.

Q Search / Select an Report Index:

Q Filter Report Indexes:

Available Report Indexes:

default 2016.05.16

Selected Object / Container:

Top

Objects in this Container:

Q <<< Pages >>> (1-3 / 3)

cn=Security

o=demo

o=system

Data of Selected Object / get LDIF Data (toggle)

Installation and Configuration Guide

3.9 Install the Audit Export service

Make sure you have installed Java. If Java is not installed, please follow the instructions for how to install Java for your system in chapter 3.1 Check and Install Oracle Java.

3.9.1 Extract and manual start

1. Extract archive.

Extract content of the "AuditExport-1.0RC1.zip" file

- For Linux, use command:

```
unzip AuditExport-1.0RC1.zip
```

- For Windows, please use Windows Explorer option "Extract All".
(After extraction, "AuditExport-1.0RC1" folder will be created automatically.)

2. Move extracted folder.

Move the extracted folder to the location you want.

- Linux: e.g., /opt/AuditExport-1.0RC1
- Windows: e.g., \Programs\AuditExport-1.0RC1

(You can delete the .zip file afterwards.)

3. Manually start and stop.

Start the Audit Export service with the script or batch file, depending on your system:

- Linux: start.sh
- Windows: start.bat

(If JAVA_HOME variable is not defined in your system, you may have to adjust the path to Java Runtime Environment in script or batch file. The path to Java depends on your Java installation.)

To stop the Audit Export service, please use the following way, depending on your system:

- Linux: stop.sh
- Windows: close the CMD window

3.9.2 Make runnable as service for Linux

For a production environment, we recommend making Audit Export runnable as a service on each system start. To make this, please follow these steps:

1. Move script file which is located in the "service-script" folder to your "/etc/init.d" folder.

```
sudo mv ./service-script/audit-export /etc/init.d/audit-export
```

2. Open in editor "service-script" file and change the APP_PATH variable with the path where your Audit Export service is located.

```
sudo vi /etc/init.d/audit-export
```

Installation and Configuration Guide

(e.g., APP_PATH="/opt/idm/AuditExport-1.0RC1")

3. Give this script executable permission (e.g., 775, but you can set it lower).

sudo chmod 775 /etc/init.d/audit-export

4. Include in startup list with default startup priority.

sudo update-rc.d audit-export defaults

5. Reboot server or start the Audit Export as service.

sudo service audit-export start

3.9.3 Make runnable as service for Windows

For a production environment, we recommend making Audit Export runnable as a Windows process by each system start.

1. Open in editor "audit-export-64.ini" or "audit-export.ini", depending on your system architecture.
2. Change "working.directory", depending on the path where Audit Export is located, e.g., working.directory="c:\Programs\AuditExport-1.0RC1".
3. Uncomment and change "vm.location", depending on the location of the "JVM.dll" file (if your JAVA_PATH not defined globally).

e.g., vm.location="C:\program files\Java\jre1.8.0_91\bin\client\JVM.dll"

4. Run "audit-export-64.exe" or "audit-export.exe", depending on your system.

Please allow Firewall prompt.

If everything is correct you will see the audit-export process in Windows Task Manager. (You can end it by clicking the "End Process" button.)



5. Open "AuditExportTask.xml" in editor (which is located in the "service-script" folder of your Audit Export installation).

Replace the path between <command></command> tags.

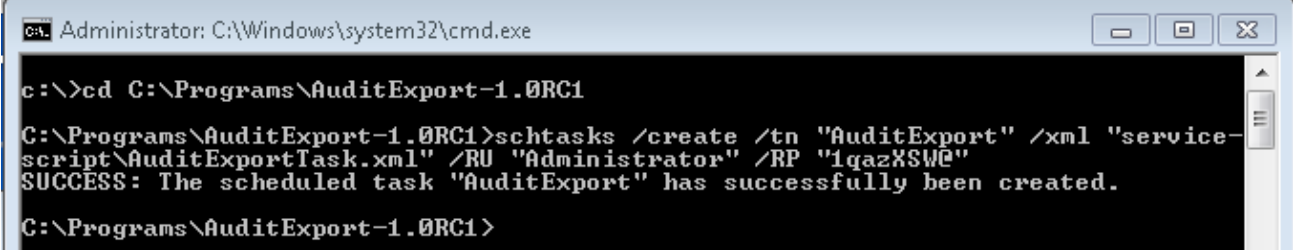
(The path should correspond to your "audit-export.exe" or "audit-export-64.exe" location.)

```
<Actions Context="Author">
  <Exec>
    <Command>C:\Programs\AuditExport-1.0RC1\audit-export-service.exe</Command>
  </Exec>
</Actions>
```

6. Save File.

Installation and Configuration Guide

7. Run cmd.exe; it will open a CMD window.
8. Go to the folder where your Audit Server is located.
e.g., c:\Programs\AuditExport-1.0RC1
9. Run command to import AuditExportTask.xml to Task Scheduler:
schtasks /create /tn "AuditExport" /xml "service- script/AuditExportTask.xml" /RU
"Administraror" /RP "YourPassword"



```
Administrator: C:\Windows\system32\cmd.exe

c:\>cd C:\Programs\AuditExport-1.0RC1

C:\Programs\AuditExport-1.0RC1>schtasks /create /tn "AuditExport" /xml "service-
script\AuditExportTask.xml" /RU "Administrator" /RP "iqazXSWC"
SUCCESS: The scheduled task "AuditExport" has successfully been created.

C:\Programs\AuditExport-1.0RC1>
```

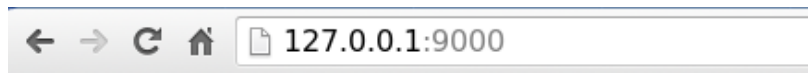
Replace "Administrator" and "YourPassword" with the user name and password of the user you would like to start Audit Server with.

10. After the task is successfully created, you need to restart your server.

Installation and Configuration Guide

3.9.4 Check if your Audit Export service is running.

Open in browser following the URL <http://HOST:9000>.
(Where HOST is name or IP address of server where Audit Export is installed, e.g., <http://127.0.0.1:9000>)



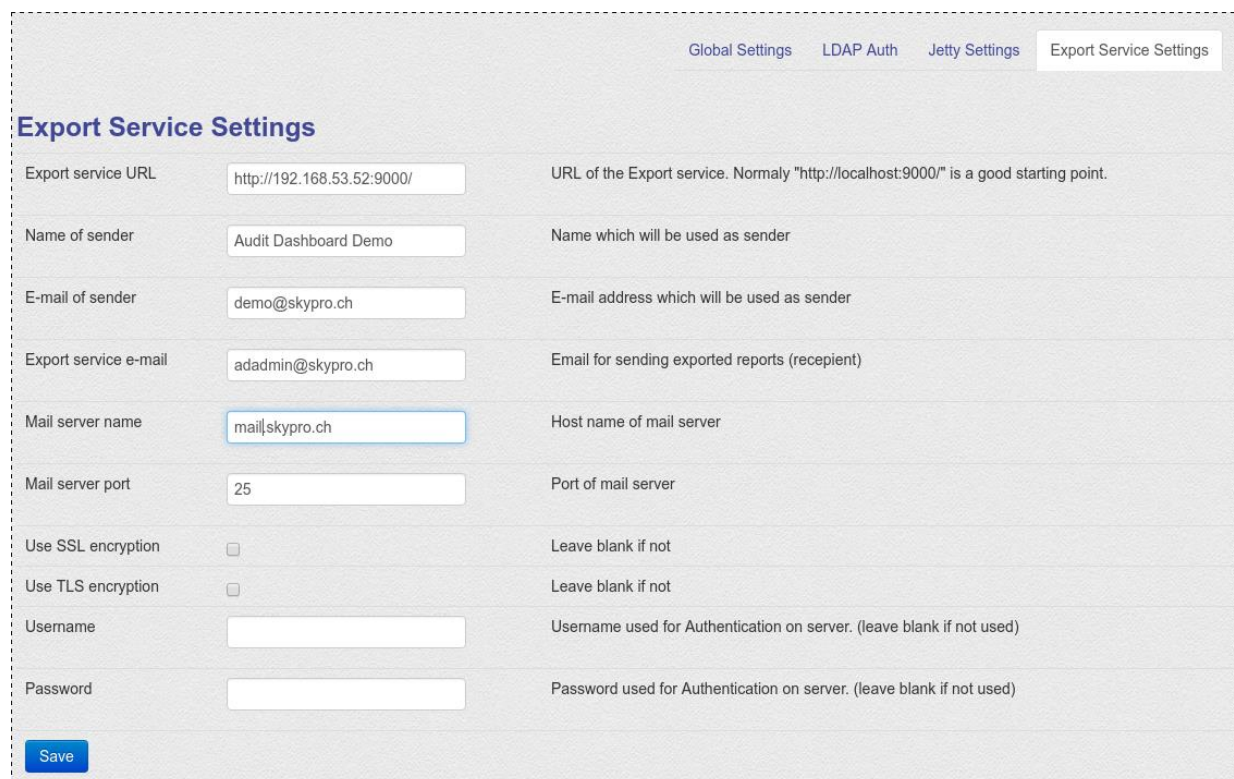
Your new application is ready.

If everything is successful, you will see this page.

3.9.5 Configure the Audit Export

Before you can use the Export service, you have to configure the connection to it and to the mail server settings.

1. Click "Settings" from the "Administration" menu.



Export Service Settings		
Export service URL	http://192.168.53.52:9000/	URL of the Export service. Normally "http://localhost:9000/" is a good starting point.
Name of sender	Audit Dashboard Demo	Name which will be used as sender
E-mail of sender	demo@skypro.ch	E-mail address which will be used as sender
Export service e-mail	adadmin@skypro.ch	Email for sending exported reports (receptient)
Mail server name	mail.skypro.ch	Host name of mail server
Mail server port	25	Port of mail server
Use SSL encryption	☐	Leave blank if not
Use TLS encryption	☐	Leave blank if not
Username		Username used for Authentication on server. (leave blank if not used)
Password		Password used for Authentication on server. (leave blank if not used)
Save		

2. Export service URL.

Please enter the URL and port of your Export server.

By default this is: <http://HOST:9000/>

3. Enter the port number of your Audit Server. By default, it is 3190.
4. Specify your mail server setting.
5. Save.

6. Restart the Audit Server.

Installation and Configuration Guide

4 Sample Dashboards

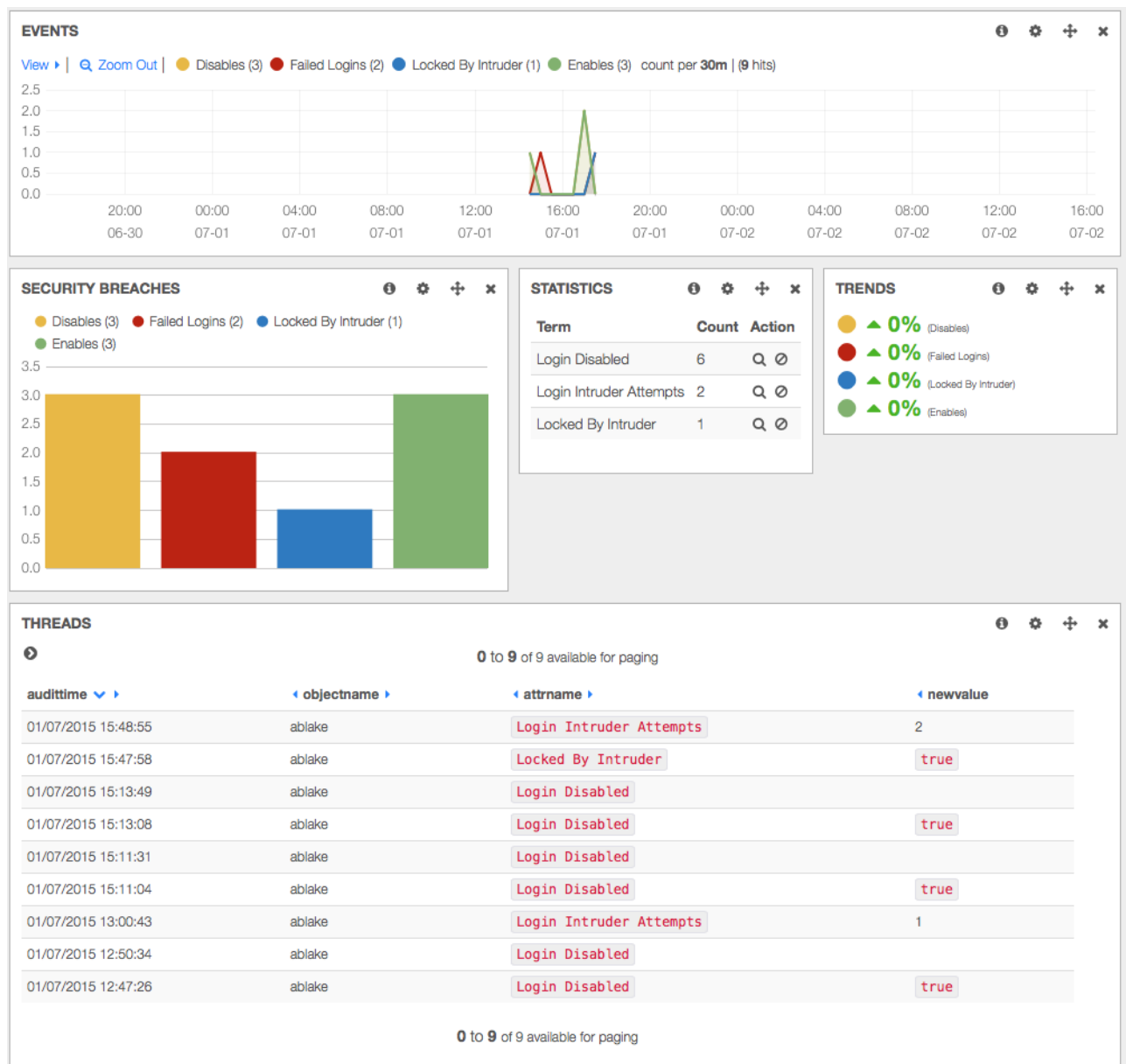
Now you're almost ready to go. For your convenience, we have provided a couple of dashboards:

IDM Audit Dashboard

This dashboard provides real-time information about all events on specific objects that are taking place on your IDM server engine. We'll work with this dashboard later.

IDM Security Dashboard

This dashboard illustrates security threats that might have occurred like intruder attempts, intruder locks, and login disables/enables.



Graphic 1: IDM Security Dashboard

Installation and Configuration Guide

IDM Compliance Dashboard

The compliance dashboard shows the data history of objects. We provide historical views of users, groups, roles, resources, and assignments. This helps to verify attributes and assignment states in different time periods. Objects states are saved to the Audit tool on a regular basis. Because the Audit tool knows the historical values and all the changes that might have taken place in a specific period of time, it can prove and validate data values of any object at any time. Your compliance team will be pleased.

_Index	cn	_id	fullName	groupMembership	nrfMemberOf	nrfAssignedResources	member
report-default-2015.07.02	ablake	cn=ablake,ou=users,o=data	Allison Blake		cn=Utopia Employee,cn=Level10,cn=Role...	cn=Shiftboard,cn=Others,cn=ResourceDe...	
report-default-2015.07.01	ablake	cn=ablake,ou=users,o=data	Allison Blake		cn=Utopia Employee,cn=Level10,cn=Role...	cn=Shiftboard,cn=Others,cn=ResourceDe...	
report-default-2015.07.02	achung	cn=achung,ou=users,o=data	Angie Chung		cn=Utopia Employee,cn=Level10,cn=Role...	cn=Air Travel Administration,cn=Other...	
report-default-2015.07.01	achung	cn=achung,ou=users,o=data	Angie Chung		cn=Utopia Employee,cn=Level10,cn=Role...	cn=Air Travel Administration,cn=Other...	
report-default-2015.07.02	admin	cn=admin,ou=users,o=system					
report-default-2015.07.01	admin	cn=admin,ou=users,o=system					
report-default-2015.07.02	apalani	cn=apalani,ou=users,o=data	Anthony Palani		cn=Utopia Employee,cn=Level10,cn=Role...	cn=PBX User Account,cn=Accounts,cn=Re...	
report-default-2015.07.01	apalani	cn=apalani,ou=users,o=data	Anthony Palani		cn=Utopia Employee,cn=Level10,cn=Role...	cn=PBX User Account,cn=Accounts,cn=Re...	
report-default-2015.07.02	asmith	cn=asmith,ou=users,o=data	April Smith		cn=Utopia Employee,cn=Level10,cn=Role...	cn=PBX User Account,cn=Accounts,cn=Re...	
report-default-2015.07.01	asmith	cn=asmith,ou=users,o=data	April Smith		cn=Utopia Employee,cn=Level10,cn=Role...	cn=PBX User Account,cn=Accounts,cn=Re...	
report-default-2015.07.02	aspencer	cn=aspencer,ou=users,o=data	Abby Spencer	cn=HR Employee,ou=groups,o=data	cn=Utopia Employee,cn=Level10,cn=Role...	cn=PBX User Account,cn=Accounts,cn=Re...	
report-default-2015.07.01	aspencer	cn=aspencer,ou=users,o=data	Abby Spencer	cn=HR Employee,ou=groups,o=data	cn=Utopia Employee,cn=Level10,cn=Role...	cn=PBX User Account,cn=Accounts,cn=Re...	
report-default-2015.07.02	bbender	cn=bbender,ou=users,o=data	Bill Bender		cn=Utopia Employee,cn=Level10,cn=Role...	cn=PBX User Account,cn=Accounts,cn=Re...	
report-default-2015.07.01	bbender	cn=bbender,ou=users,o=data	Bill Bender		cn=Utopia Employee,cn=Level10,cn=Role...	cn=PBX User Account,cn=Accounts,cn=Re...	
report-default-2015.07.02	bbrown	cn=bbrown,ou=users,o=data	Bill Brown		cn=Utopia Employee,cn=Level10,cn=Role...	cn=PBX User Account,cn=Accounts,cn=Re...	
report-default-2015.07.01	bbrown	cn=bbrown,ou=users,o=data	Bill Brown		cn=Utopia Employee,cn=Level10,cn=Role...	cn=PBX User Account,cn=Accounts,cn=Re...	
report-default-2015.07.02	bburke	cn=bburke,ou=users,o=data	Bill Burke		cn=Utopia Employee,cn=Level10,cn=Role...	cn=PBX User Account,cn=Accounts,cn=Re...	
report-default-2015.07.01	bburke	cn=bburke,ou=users,o=data	Bill Burke		cn=Utopia Employee,cn=Level10,cn=Role...	cn=PBX User Account,cn=Accounts,cn=Re...	
report-default-2015.07.02	bfox	cn=bfox,ou=users,o=data	Bud Fox		cn=Utopia Employee,cn=Level10,cn=Role...	cn=PBX User Account,cn=Accounts,cn=Re...	
report-default-2015.07.01	bfox	cn=bfox,ou=users,o=data	Bud Fox		cn=Utopia Employee,cn=Level10,cn=Role...	cn=PBX User Account,cn=Accounts,cn=Re...	
report-default-2015.07.02	bjenner	cn=bjenner,ou=users,o=data	Bob Jenner		cn=Utopia Employee,cn=Level10,cn=Role...	cn=PBX User Account,cn=Accounts,cn=Re...	
report-default-2015.07.01	bjenner	cn=bjenner,ou=users,o=data	Bob Jenner		cn=Utopia Employee,cn=Level10,cn=Role...	cn=PBX User Account,cn=Accounts,cn=Re...	

Graphic 2: IDM Compliance Dashboard

Mandant A/B Audit Dashboards

This is an example of the multitenant feature of the Audit dashboard to allow different dashboard views for individual groups.

Blank

With the blank template you can start to build your own dashboard from scratch.

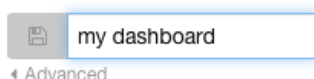
4.1 Modify a dashboard

Open the Audit Server home page and click the "Dashboard" button on top. Select the IDM Audit dashboard example to start with.

Click the save button located in the upper right corner.

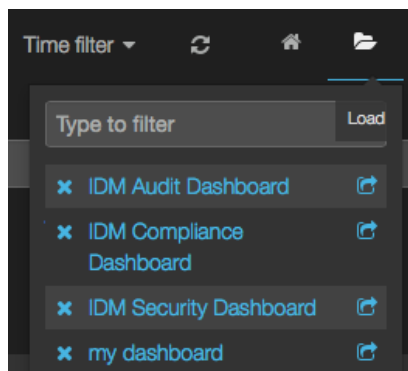


Then choose "my dashboard" as the name for the new dashboard and save it. Now you have a copy of the original Audit dashboard to play around with.



To select this dashboard you have to go back to the dashboard overview and select the blank dashboard. Click on the folder icon to load your copy "my dashboard".

Installation and Configuration Guide

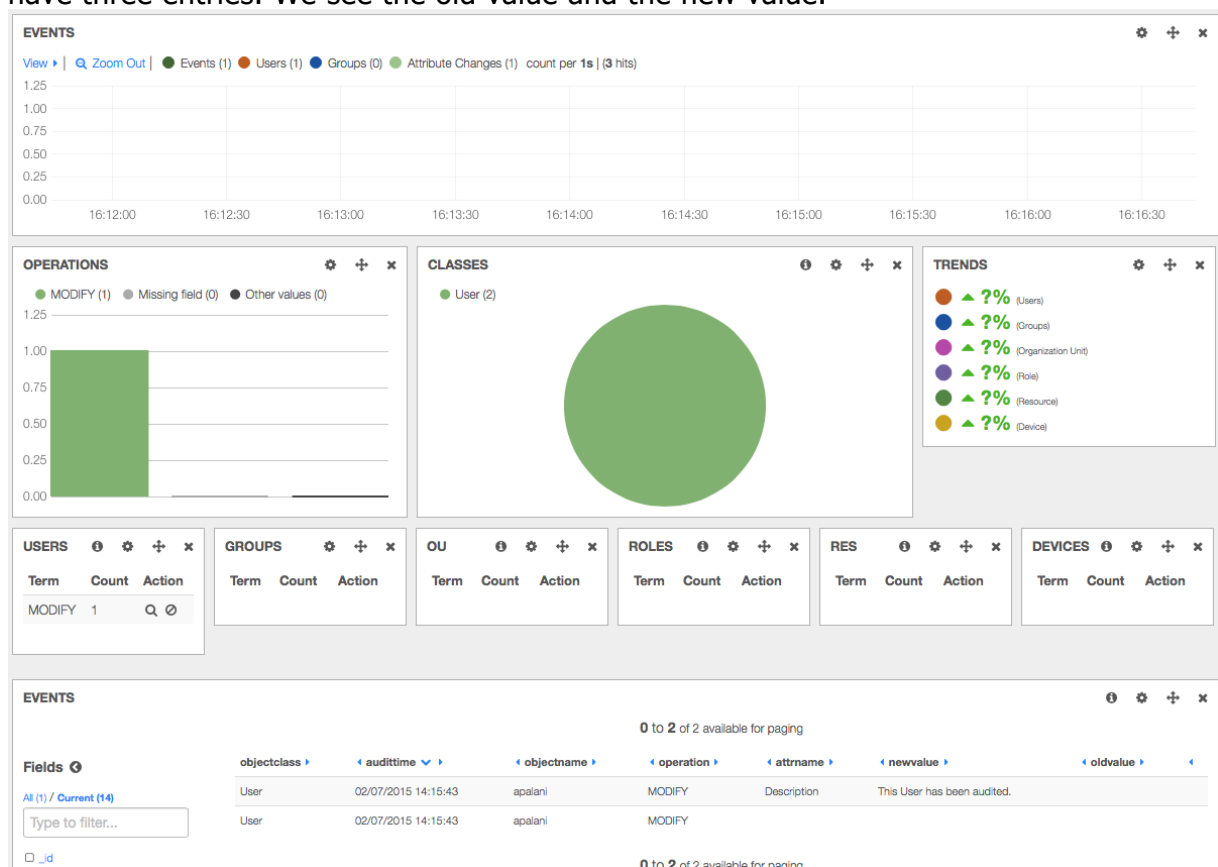


Graphic 3: Load your IDM Audit Dashboard "my dashboard" example

The IDM Audit Dashboard shows a visualized history of events on objects with histograms and charts. You can see how many events have been processed by your IDM engine and how many different object classes have been involved. You see trends and the amount of different operations on different objects that have occurred.

If you have executed the change of a user description attribute – as mentioned in chapter 3.4 – you should see this modified event already in your dashboard (see Graphic 4: IDM Audit Dashboard example).

In the Operation/Events graphic you see one modify event. In the Classes graphic you see that one user object so far was audited. In the Events table at the bottom you see the basic data. You see two (maybe three if the description had an old value) entries of object class user with its object name. The first entry is the modification event. The second entry shows the new value "This user has been audited". If the attribute was already valued we even have three entries. We see the old value and the new value.

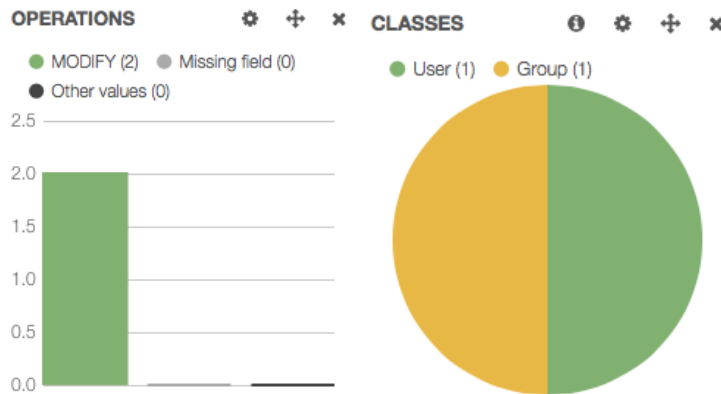


Graphic 4: IDM Audit Dashboard example

Installation and Configuration Guide

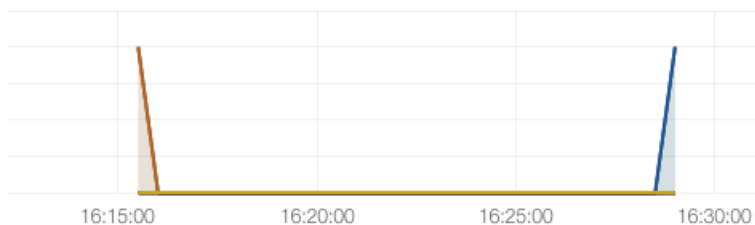
4.2 Experience the IDM Audit Dashboard

Now change the description of a group object and look at the dashboard again. You will see two modification events under OPERATIONS and two classes Users and Group. Also in the GROUP EVENTS you now see one modification.



Graphic 5: IDM Dashboard Operations and Classes

Also in the event Histogram you see these two modifications in the timeline. You see the user event in orange, the group event in blue, and the attribute changes in light green. Also have a look at the table at the bottom. You see three new entries for the group modification.



Graphic 6: IDM Audit Dashboard Event Histogram

4.3 Understand the IDM Audit Dashboard

There are some base elements you have to know about to understand the dashboards.

1. Query
2. Filter
3. Row
4. Panel

Query

With queries, you select all the elements you want to display in your dashboard. You can pin queries so you can use them in panels directly to select specific data. In all panels you can decide to use data from all pinned or unpinned queries or select data from specific pinned queries.

We have predefined some pinned queries to select events, users, groups, failed logins, attribute changes, etc.

Installation and Configuration Guide

Filter

With filters, you obviously filter the data you have selected with your query. For example, you only want to have user objects or objects with a specific object name. Often you will use the filter to narrow the time frame of events you want to see, such as only changes that have taken place the within the last 24 hours.

Our standard filter selects only events of type "audit". For reporting purposes, we have additional types like "report" that contain all data of an object at a specific time.

Row

A row can hold one or multiple panels. You can add new rows at the bottom. You can move rows at any time to the position you want to have them.

Panel

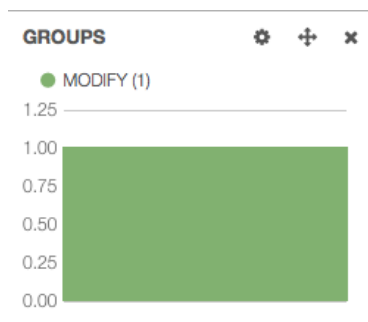
Panels are the actual graphical building blocks of the dashboard. Panels can show maps, tables, histogram, hits, pie charts, statistics, trends, or just explaining text.

4.4 Work with Panels

4.4.1 Change an existing Panel

We have a panel called GROUPS that shows a summary of all different group events. Wouldn't it be nice to show this instead of a table as a bar graphic?

1. Click the configure icon in the *GROUP* panel. 
2. In the *Panel* tab change the *Style* from *table* to *bar*.
3. Now the events will be displayed as bars.



Graphic 1: Graphic for events per class

4.4.2 Add a new Panel

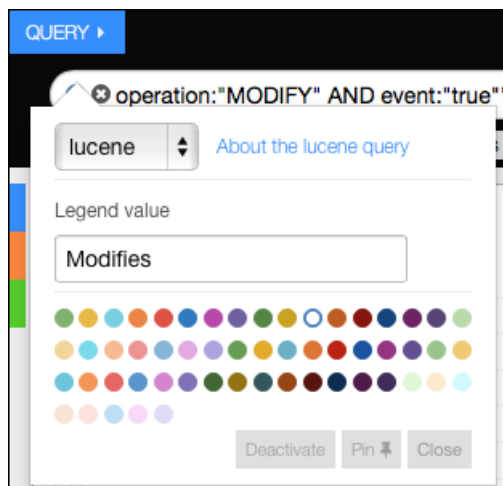
Now we want to create a pie chart showing us all modified events per class. First we add a new query for all modified events. To add a query, we have to enable the query bar.

1. Click the configure dashboard on the right top.
2. Select "Controls" from the available tabs.
3. Enable "Query" in the section "Pull downs".
4. Click "Save".

Installation and Configuration Guide

The query panel appears as the first panel. Open the panel with a click on the "Query" panel. Now we add a new Query.

1. In the *QUERY* row click the "+" sign at the right.
2. Enter Query string
Enter the following query string `operation:"MODIFY" AND event:"true"`.
This selects all events that are not the actual attribute changes but only the modified event.
3. Pin the Query
Click the colored dot on the left, as *Legend value* enter "Modifies" and pin the query.



Graphic 2: Define new query

You should see a new pinned query. Now we add a new pane.

1. Add panel
Go to the row with the *OPERATIONS* panel on the left and click the green "+" symbol to add a panel.
2. Panel type
As panel type select *terms*.
3. Title
As *title* type enter *Modifies on Classes* and adjust the span value to 3.
4. Field value
In the *Parameters* type *objectclass* in the *Field* value.
5. Options
Uncheck *Missing* and *Other* in the *View Options* and select *pie* as the graphic view.
6. Query
In the *Queries* dropdown choose *selected* and activate the pinned *Modifies* query.
7. Save the panel.

Installation and Configuration Guide

Select Panel Type

terms

Stable // Displays the results of an elasticsearch facet as a pie chart, bar chart, or a table

Title: Modifies on classes Span: 2 Editable: ☒ Inspect: ☒

Parameters

Terms mode: terms Field: objectclass Length: 10 Order: count Exclude Terms(s) (comma separated):

View Options

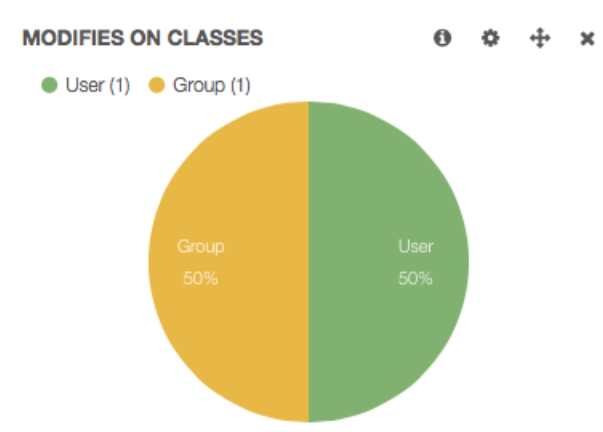
Style: pie Legend: above Legend Format: horizontal Missing: ☐ Other: ☐ Donut: ☐ Tilt: ☐ Labels: ☒

Queries

Queries: selected Selected Queries: Events Users Groups Failed Logins Attribute Changes Disables Organization Unit Role Resource Device **Modifies**

Graphic 9: Define a new panel

Bravo! You successfully added a new panel showing a pie with the amounts of modifies per class that looks like this.



Graphic 30: New MODIFY on classes panel

Now you can play around with new rows, add new panels, and experiment with all the various graphical building blocks.

4.4.3 Create new row

Now we're going to create a new row with new panels. The goal is to create a separate histogram and pie chart for user and group events.

1. First go to the bottom of the dashboard on click ADD A ROW.
2. Select tab "Rows".
3. In the title field on the right enter "User & Group Statistics".
4. Click "Create Row".
5. Move the new row above the Events row in the dashboard settings.
6. Press "Save".

Add panels

Now you have an empty row where we can add new panels.

1. Press "Add panel to empty row".

Installation and Configuration Guide

2. Select "histogram" as panel type.
3. Enter "User Changes" in the field Title and change the span value to "6".
4. Change the Time Field from "@timestamp" to "_timestamp".
5. Change the Queries to "selected" and enable Users.

Select Panel Type

histogram

⬆️⬇️⬆️

Stable // A bucketed time series chart of the current query or queries. Uses the Elasticsearch date_histogram facet. If using cluster

Title Span Editable Inspect ?

User Changes

⬆️⬇️⬆️

6

⬆️⬇️⬆️

✓

⬆️⬇️⬆️

✓

⬆️⬇️⬆️

Values

Chart value

count

⬆️⬇️⬆️

Transform Series

Seconds ?

☐

⬆️⬇️⬆️

Derivative ?

☐

⬆️⬇️⬆️

Time Options

Time Field

_timestamp

⬆️⬇️⬆️

Time correction

browser

⬆️⬇️⬆️

Auto-interval

✓

⬆️⬇️⬆️

Resolution ?

100

⬆️⬇️⬆️

Style

Chart Options

Bars

✓

⬆️⬇️⬆️

Lines

☐

⬆️⬇️⬆️

Points

☐

⬆️⬇️⬆️

Selectable

✓

⬆️⬇️⬆️

xAxis

✓

⬆️⬇️⬆️

yAxis

✓

⬆️⬇️⬆️

Y Format ?

none

⬆️⬇️⬆️

Multiple Series

Stack

✓

⬆️⬇️⬆️

Percent ?

☐

⬆️⬇️⬆️

Stacked Values ?

cumulative

⬆️⬇️⬆️

Header

Zoom

✓

⬆️⬇️⬆️

View

✓

⬆️⬇️⬆️

Legend

Legend

✓

⬆️⬇️⬆️

Query ?

✓

⬆️⬇️⬆️

Counts

✓

⬆️⬇️⬆️

Grid

Min / Auto

0

⬆️⬇️⬆️

Max / Auto ★

⬆️⬇️⬆️

Queries

Charted

Queries

selected

⬆️⬇️⬆️

Selected Queries

● Events

● Users

● Groups

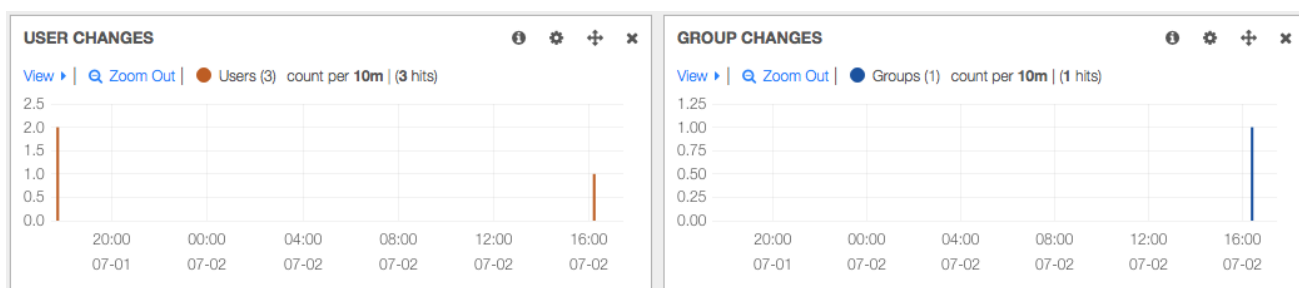
● Failed Logins

● Attribute Changes

Add a second histogram panel for groups and name it "Group Changes", change the Time Field, correct the span value, and change the Queries to enable Groups only.

Congratulations! You successfully added a new row to histogram panels. Now create, modify, and delete some users and groups in your directory and you will show the events in these histograms.

Installation and Configuration Guide



Graphic 11: New row with two histograms

5 Conclusion

With the IDM Audit & Compliance Dashboard, you can create powerful dashboards in no time. All components fulfill every requirement you could expect from a professional SIEM (Secure Identity and Event Management) solution.

Elasticsearch is able to process thousands of events per second, can be clustered, and guarantees automatic failover and high availability.

The Audit Server is a very powerful and easy to use visualization component offering a lot of graphical building blocks.

The Report Service logs current states of object on a scheduled basis so we know the values of all attributes at any time in the history for compliance purposes. You can generate reports on historical data and export them to Excel. You can browse through historical data and even restore single objects via an LDIF export.