

OpenText™ Identity Manager CE 24.4 (v4.10) Audit, Compliance & Data Intelligence Guide

January 2025

Legal Notice

Copyright 2009 - 2024 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors ("Open Text") are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Contents

About this Book and the Library	7
Part I Audit, Compliance & Data Intelligence Overview	9
1 Audit, Compliance & Data Intelligence Architecture	11
OpenSearch	11
Core Engine	12
Audit Server	12
ACDI Proxy Service	12
Data Connectors	12
Audit, Compliance & Data Intelligence	12
2 Audit, Compliance & Data Intelligence Versions	13
Part II Setting Up Audit, Compliance & Data Intelligence	17
3 Installing Audit, Compliance & Data Intelligence	19
System Requirements	19
Installing ACDI	20
Installing the ACDI Driver	21
Installing the ACDI Monitor	24
Installing the Workflow Monitor	25
Final Step for Installation	27
4 Accessing Audit, Compliance & Data Intelligence	29
5 Configuring Audit, Compliance & Data Intelligence	31
Setting Up Core Engine	31
LDAP Connections	32
LDAP Authentication Settings	33
Web Server Settings	34
Mailer Settings	35
Scheduled Tasks	35
Session Settings	35
Web Proxies List	35
WS Proxies List	35
Local Access List	36
List of Rule Presents	36
AuditProxy API List	36
Role List	36
Post Configuration of Core Engine	36
Setting Up Audit Server	36

Back-end Properties	37
Day Time Format	38
Indices Settings	38
URLs and Roles	39
Reports Menu	39
Dashboards Menu	39
Home Page Cards	39
Misc Audit Server settings	40
Setting Up Data Connectors	40
Checking Snapshot service	40
6 Updating Audit, Compliance, & Data Intelligence	43
Prerequisites for Updating ACDI	43
Update Procedure	43
Part III Getting Started with Audit, Compliance & Data Intelligence	45
7 Using Dashboards	47
Default Dashboards for OpenText Identity Manager	47
Other Sample Dashboards	48
Understanding Dashboard Basics	49
Searching For Dashboards	49
Customizing Dashboards	50
Viewing Individual Dashboards	50
Full Screen for Better Viewing	50
Generating Dashboard URLs for Sharing	51
Generating OSD Reports	52
Cloning Dashboards	53
Interacting with Your Dashboard Data	53
Using the Inspect Feature for Debugging	55
8 Using Reports	57
Default Reports for OpenText Identity Manager	57
Understanding Reports Basics	58
Searching For Reports	58
9 Using Time Machine	59
Using Time Machine to Review Snapshots	59
Setting the Time Filter	60
Viewing Object or Attribute History	60
Comparing the History of an Object or Attribute	62
Part IV Managing Audit, Compliance & Data Intelligence	63
10 Working with Dashboard Editor	65
Creating a New Dashboard	65
Creating a Dashboard with New Visualization	65

Creating a Dashboard with an Existing Visualization	67
Editing Dashboard	68
Adding Custom Dashboards to the Dashboards Menu	68
Creating a Sub-menu under the Dashboards Menu	68
Adding Custom Dashboards under a Sub-menu	68

11 Working with Report Editor 69

Understanding Report Editor Options	69
Report Graph	69
Report Properties	70
Entities	71
Filters	72
Result Table Attributes	74
Postprocessing	75
Creating a New Custom Report Definition	76
Creating Custom Report Definitions from Report Templates	77

About this Book and the Library

The *Audit, Compliance & Data Intelligence Guide* is a comprehensive document that includes detailed instructions on how to install the Audit, Compliance & Data Intelligence (ACDI) tool for OpenText Identity Manager. This guide also provides a clear description of how to use the Audit Dashboard to monitor and report the data collected from different product sources.

Intended Audience

This guide is intended for OpenText Identity Manager administrators and consultants.

Other Information in the Library

For more information about the library for OpenText Identity Manager, see the [OpenText Identity Manager documentation website \(https://www.netiq.com/documentation/identity-manager-4.10/\)](https://www.netiq.com/documentation/identity-manager-4.10/).

Audit, Compliance & Data Intelligence Overview

Audit, Compliance & Data Intelligence (ACDI) provides a holistic view of the Identity and Access management environment, real-time forensic analysis of all current and past data, customizable reports, and automation of audit evidence processes.

Key features of ACDI:

- Provides a unified console for all monitoring requirements, eliminating the hassle of dealing with multiple tools to measure and optimize application performance.
- Provides fast, automated, and contextualized visibility into the health and availability of your entire application environment.
- Assists with auditing and performance of your IAM-related data.
- Increases productivity and reduces cost.
- Improves compliance and security in your Identity Management environment through real-time dashboards, understandable reports, and historical data.

ACDI provides a wide range of capabilities, including:

Dashboards

ACDI transforms complex and high-volume analytical, operational, and strategic data into visual representations. Dashboards display these visual representations through charts, graphs, or maps. You can quickly grasp trends, view metrics, explore data, and gain real-time application insights.

Predefined dashboards provide an overview of activity in your OpenText Identity Manager engine. Health and metrics dashboards aid in identifying and diagnosing complex application performance issues.

Dashboard's search queries and filters make it easy to find the required data. You can also use the Dashboard Query language (DQL) to create more advanced queries. For more information about dashboards, see [Chapter 7, "Using Dashboards," on page 47](#).

Reports

The reports contain critical information about various aspects of your OpenText Identity Manager setup. This includes information collected from Identity Vaults and managed systems such as Active Directory or SAP. ACDI reports enable you to audit and monitor data and events in your directory. It provides predefined report definitions for generating reports. You can use them as is or customize them to suit the requirements of your organization. You can also create new reports from scratch. These reports are generated using data collected by ACDI drivers, ACDI monitors, Workflow monitor packages, and snapshot data stored in the system. You can export the report results as CSV, XLSX, or PDF files and download them for further processing using external applications.

You can also schedule report generation as needed. For more information about reports, see [Chapter 8, "Using Reports," on page 57](#).

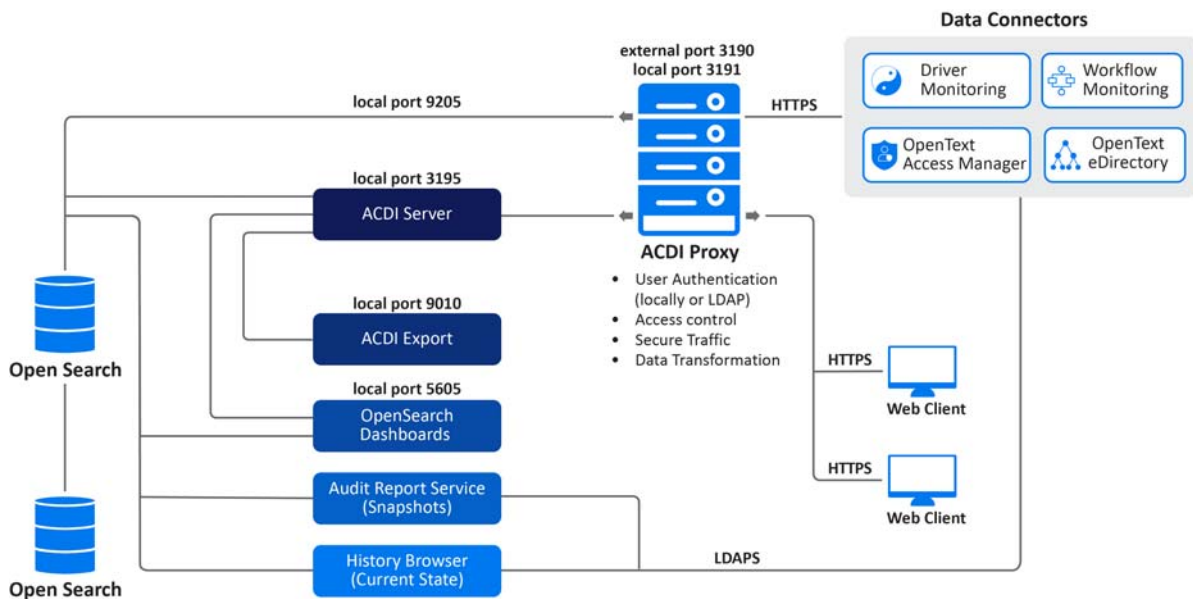
Time Machine

The snapshot service takes snapshots of OpenText eDirectory every 24 hours. Various changes in objects and their attributes occur in the intervals between each snapshot. ACDI creates a timeline of these snapshots and events. You can use this timeline to monitor changes in objects over time. Using the history browser, you can see the history of an object and review its status at a specific time.

Additionally, you can generate reports based on these snapshots. For more information about time machine, see [Chapter 9, “Using Time Machine,” on page 59](#).

1 Audit, Compliance & Data Intelligence Architecture

The following diagram shows how the high-level components interact with one another to deliver Audit, Compliance & Data Intelligence capabilities: dashboards, history browser, and reporting.



OpenSearch

OpenSearch is an open-source search and analytics suite that consists of a search engine daemon, OpenSearch, and visualization user interface, OpenSearch Dashboards. OpenSearch indexes processes data from applications such as OpenText Identity Manager and OpenText Access Manager and stores it as documents in its database. When a search query is performed, OpenSearch searches the index for the desired document. This makes OpenSearch incredibly fast at returning the most relevant search results. It helps organization to search, visualize, and analyze data. OpenSearch Dashboards allows users to see and explore their data in real-time, and also provides machine-learning powered results for anomaly detection and search relevance ranking. For more information, see [OpenSearch documentation \(https://opensearch.org/docs/2.8/dashboards/\)](https://opensearch.org/docs/2.8/dashboards/).

The following are some of OpenSearch key features:

- ♦ Integrated search engine: OpenSearch has built-in features such as full text querying, autocomplete, and recommendations based on relationships within the data which helps your users find what they are looking for more effectively.
- ♦ Analytics: Analyze your OpenSearch deployment using integrated tools and use OpenSearch Dashboards to visualize data for decision making.

- ♦ Anomaly Detection and Observability – to conduct forensic data analysis.
- ♦ Monitoring: OpenSearch includes a number of monitoring and alerting features which allow you to detect security threats in real time.

Core Engine

Core engine processes all data changes that occur in the Identity Vault or a connected application. For events that occur in the Identity Vault, the engine processes the changes and issues commands to the application via the data connectors. For events that occur in the application, the engine receives the changes from the driver, processes the changes, and issues commands to the Identity Vault.

Audit Server

The audit server is a service responsible for processing back-end configurations and managing the web interface of ACDI. Its back-end configurations enable product licensing, OpenSearch endpoint configuration, reporting settings, and other service settings.

ACDI Proxy Service

ACDI proxy server serves as an end-point for all the services and data connectors to send data to OpenSearch database via LDAPS or HTTPS. The ACDI proxy service connects clients and ACDI's audit server to OpenSearch database servers. The benefits of using proxy server include enhanced security, scalability, high availability, and direct access control to directory services.

Data Connectors

The data connectors consists of components such as ACDI drivers, ACDI monitors, and workflow monitor packages, which connect an ACDI proxy service to the connected system. The connected system can be any system, directory, database, or operating system whose identity information you want to monitor. For example, it could be the Syslog server used by OpenText Access Manager or an LDAP directory such as OpenText eDirectory in OpenText Identity Manager.

These data connectors are installed on the connected systems. The connected system or application must provide APIs for a data connector to detect changes in application data.

Audit, Compliance & Data Intelligence

The user interface for Audit, Compliance & Data Intelligence (ACDI) provides users and administrators with access to the information, resources, and capabilities of ACDI.

ACDI is a browser-based web application that allows users to perform various tasks. ACDI's dashboards enable users to visualize and analyze data to gain insights. Users can also view and generate reports in PNG, PDF, and CSV formats, as well as compare the history of an object at any point in time.

2 Audit, Compliance & Data Intelligence Versions

To meet different customer needs, the OpenText ACDI CE 24.4 is available in two product groups:

- ♦ Pro version
- ♦ Basic version

The complete set of functionality is included in Pro version. Basic version includes a subset of the features provided in Pro version. Before downloading the installation files, you must understand what features are contained in each version.

The following table provides a comparison of features available in Pro and Basic versions:

Product Feature	Version	
	OpenText ACDI	OpenText ACDI Pro
Dashboards		
Audit Dashboard	Yes	Yes
Driver Dashboard		Yes
IDM System Overview	Yes	Yes
Security Dashboard		Yes
Workflow Dashboard		Yes
Reports		
Audit Driver Events	Yes	Yes
Audit Driver Status	Yes	Yes
Audit Groups	Yes	Yes
Audit Objects	Yes	Yes
Audit Users	Yes	Yes
Group Membership Report	Yes	Yes
Resource Report		Yes
Role Request Report		Yes
Users Login Network Address Report		Yes
Users Login Time Report		Yes
Users Report	Yes	Yes

Product Feature	Version	
	OpenText ACDI	OpenText ACDI Pro
Workflow Report		Yes
Time Machine		
Time Machine		Yes
Management > ACDI Modules		
Dashboard Editor		Yes
Create Dashboard		Yes
Report Editor		Yes
Create New Report		Yes
Management > OSD Modules		
Visualize		Yes
Discover		Yes
OSD Report		Yes
Query Workbench		Yes
Alerting		Yes
Anomaly Detection		Yes
Observability		Yes
Notification		Yes
Administration > ACDI Modules > Core Engine		
LDAP Connections	Yes	Yes
LDAP authentication settings		Yes
Web Server settings	Yes	Yes
Mailer Settings		Yes
Scheduled tasks		Yes
Session settings	Yes	Yes
Web Proxies list		Yes
WS Proxies list		Yes
Local Access list	Yes	Yes
List of Rule presets		Yes
AuditProxy API list		Yes
Roles list		Yes

Product Feature	Version	
	OpenText ACDI	OpenText ACDI Pro
Administration > ACDI Modules > Audit Server		
Back-end Properties	Yes	Yes
Date-Time format	Yes	Yes
Indices settings		Yes
Urls and Roles (Front-end Apps)		Yes
Reports Menu		Yes
Home Page Cards		Yes
Misc Audit Server settings		Yes
Administration > ACDI Modules > Data Export	Yes	Yes
Administration > Data Collection		
Data-Connector Wizard		Yes
Snapshot service (eDirectory)	Yes	Yes
Administration > OpenSearch Modules		
OpenSearch	Yes	Yes
OpenSearch Dashboards	Yes	Yes
Stack Management		Yes
Index Management		Yes
OSD Security		Yes
Dev Tools		Yes
Snapshots (Opensearch snapshots management)		Yes
System health dashboard	Yes	Yes
OpenSearch health dashboard	Yes	Yes
Event Service eDir	Yes	Yes

Setting Up Audit, Compliance & Data Intelligence

This part contains the following chapters:

- ♦ [Chapter 3, “Installing Audit, Compliance & Data Intelligence,” on page 19](#)
- ♦ [Chapter 4, “Accessing Audit, Compliance & Data Intelligence,” on page 29](#)
- ♦ [Chapter 5, “Configuring Audit, Compliance & Data Intelligence,” on page 31](#)
- ♦ [Chapter 6, “Updating Audit, Compliance, & Data Intelligence,” on page 43](#)

3 Installing Audit, Compliance & Data Intelligence

Use the following information to install the Audit, Compliance & Data Intelligence (ACDI) on your server:

- ♦ [“System Requirements” on page 19](#)
- ♦ [“Installing ACDI” on page 20](#)
- ♦ [“Installing the ACDI Driver” on page 21](#)
- ♦ [“Installing the ACDI Monitor” on page 24](#)
- ♦ [“Installing the Workflow Monitor” on page 25](#)
- ♦ [“Final Step for Installation” on page 27](#)

System Requirements

You must install ACDI on one of the following 64-bit platforms, at a minimum:

- ♦ Processor
 - 4 to 8 CPU cores
- ♦ Memory
 - 16 to 32GB
- ♦ One of the following operating systems:
 - ♦ Red Hat Enterprise Linux (RHEL) 8 and later
 - ♦ SUSE Linux Enterprise Server 15 and later
 - ♦ Ubuntu 22 and later

NOTE:

- ♦ Allow incoming traffic from the OpenText Identity Manager engine machine (where the ACDI Driver is running) on TCP port 3190 on the ACDI VM.
 - ♦ The amount of disc space required is determined by how frequently snapshots are taken and how many events occur. The recommended starting point is 100-200 GB of free disc space.
 - ♦ It is recommended to install ACDI use separate machine to avoid system overload, especially on environments with intense data flows
 - ♦ High-load systems must employ an OpenSearch (OS) cluster.
 - ♦ OpenSearch (OS) recommends that the cluster contain a minimum of three OS instances.
 - ♦ Add two VMs with OS with the same configuration.
-

Installing ACDI

Download the installer file (acdi_v24.4.zip) from the [Software License and Download portal](https://sld.microfocus.com/mysoftware/index) (<https://sld.microfocus.com/mysoftware/index>). The acdi_v24.4.zip contains the following packages:

- ♦ AuditDriver.zip
- ♦ AuditExport.zip
- ♦ AuditProxy.zip
- ♦ AuditReportEdir.zip
- ♦ AuditServer.zip
- ♦ data.zip
- ♦ logstash-8.4.0.zip
- ♦ opensearch-2.8.0.zip
- ♦ opensearch-dashboards-2.8.0.zip

Prerequisites

Ensure that the system on which you want to install ACDI has a resolvable hostname.

To install ACDI, perform the following steps:

- 1 Log in as a root user.
- 2 Unzip the acdi_v24.4.zip in the root directory of the system. For example, /opt.
- 3 Change your location to acdi directory and run the ./install.sh script.
The program determines whether the system's hostname, linux-nzdp, can be resolved. After successful verification, the installation process starts.
- 4 Press **Enter** to extract all components required for ACDI installation.
- 5 Choose whether you want to use an existing Linux user or create a new one. The install script suggests that you create a new user named, for example, acdi. Press **Enter** to use the default name.
- 6 Specify a resolvable fully qualified domain name (FQDN) hostname for the ACDI instance. For example, acdi-dev.mycompany.com.
- 7 Specify the name of a local account that will have administrative rights and access to all components. If you don't have any specific name, press **Enter** to use the default acdiadmin username and set a password for it. The user is required to set up a connection to ACDI within the ACDI Driver in OpenText Identity Manager.
- 8 To configure an admin service account for OpenSearch, specify the OpenSearch osadmin username and password. The user will be granted access to the OpenSearch.
- 9 To configure OpenSearch Dashboards (OSD) service account, press **Enter** to use the default osdadmin username and provide the password.
- 10 To configure the LDAP connection to OpenText eDirectory:
 - 10a Specify a resolvable FQDN of the LDAP server and its port.
 - 10b Specify the LDAP Service account and password which has access and can read data from the LDAP server.

After the authorization is successful, the connection to the LDAP server is established.

NOTE: If the installation connection is lost or interrupted, you can resume the installation from the point of interruption by running `./install.sh` again.

- 11 To run the Audit report service, enter the CRON string. By default, the CRON string shows that the report service takes snapshots of a directory every day at 01:05 AM. Press **Enter** to use the default settings.
- 12 Press **Enter** to install AutoStart Scripts and start ACDI components. The services start one by one.
- 13 During installation, the start script creates a self-signed certificate and stores it at `../certs/keystore.pfx` location.
- 14 To launch ACDI, open a web browser and specify the URL: `https://acd-dev.mycompany.com:3190`. You can log in using the local admin account `acdiadmin`.
The OpenSearch URL is: `https://acdi-dev.mycompany.com:3190/opensearch`
- 15 To add the ACDI software license:

IMPORTANT: After installation, the ACDI will run in the Basic version. To unlock the features offered in the Advanced version or to receive a 90-day Trial license, contact your sales representative.

- 15a Log in to ACDI using credentials specified in [Step 7](#).
- 15b Go to **Administration > Audit Server** and copy the server ID. Share the server ID to generate a license.
- 15c After the license is generated, copy it in **License**.
- 15d Click **Save**.
- 15e Refresh the page to view the license information. The following information is displayed on the bottom of the Home page: the company name for which the license was issued and its validity.

NOTE:

- ♦ To change the certificate, go to `/opt/acdi<version>/certs` and replace the certificate in the `keystore.pfx` file. Restart the Audit Proxy and Audit Server Services.
 - ♦ By default, logs and data are stored under `/var/log/acdi/` and data in `/var/data/acdi/`, respectively. To change the default location, define the required path in the `ACDIinstaller/config.json` file.
-

Installing the ACDI Driver

The ACDI driver connects OpenText Identity Manager and Designer to ACDI.

To install the ACDI driver, perform the following steps:

Step 1: Copying files from the folders

- 1 Navigate to the location where you have extracted the `acdi_v24.4.zip`.

- 2 Navigate to the AuditDriver folder location.

The AuditDriver folder contains:

- ♦ Designer folder
- ♦ Server folder
- ♦ version.txt file

- 3 Copy the files from the Server folder to the machine where OpenText Identity Manager is installed.

- ♦ For Linux, copy the files to /opt/novell/eDirectory/lib/dirxml/classes.

For example, `scp root@acdip:/opt/acdi/AuditDriver/Server/* /opt/novell/eDirectory/lib/dirxml/classes/`

- ♦ For Windows, copy the files to C:\NetIQ\Identity manager\NDS\lib.

- 4 Restart OpenText Identity Manager.

- 5 Copy the files from the Designer folder to the machine where Designer is installed. Later, add these files or packages to the Designer project.

Step 2: Copying Keystore and a self-signed certificate to OpenText Identity Manager machine

The installer automatically creates a keystore file and generates a self-signed certificate within it. Navigate to the /opt/acdi/certs folder and copy the keystore.pfx file to the OpenText Identity Manager machine. For example, /opt/acdi

Alternatively, you can download the keystore file from the ACDI user interface.

1. Log in to ACDI.
2. Click **Administration > Event Service (eDirectory)** under Data Collection.
3. Click **Download Keystore**.

The downloaded keystore (public_keystore.pfx) file contains a public certificate. The default password is changeit.

NOTE:

- ♦ Remember the location where you saved the keystore file. You must specify it while configuring the driver settings.
 - ♦ Ensure to change the default password of the keystore file.
-

Step 3: Importing packages to Designer

- 1 Launch Designer.
- 2 Open the project. Right-click **Package Catalog** and select **Import package**.
- 3 Click **Browse** and select all packages you copied in Step 1: Copying files from the folders, then click **Open**.
- 4 Click **OK** to import the packages.

Step 4: Creating and configuring ACDI Driver in Designer

- 1 In an open Designer project, right-click the driver set for your project, then select **New > Driver**.
- 2 In the Driver Configuration Wizard, select ACDI Base and click **Next**.

- 3 On the Select Optional features window, click **Next**.
- 4 Specify the properties you want to use for the driver:

Property	Description
Driver Name	Specify a name for the ACDI driver.
OpenSearch Server	Define the URL of your server. It must contain protocol, domain name, and port. If a reverse proxy is used, the URL contains OpenSearch as well.
User (for OpenSearch Basic Authentication)	Set a user which has access to OpenSearch. Default is osadmin. Also set a password for this user.
KeyStore filepath (for HTTPS connection)	Path to the keystore saved in Step 2 and the password.

- 5 Click **Next > Finish**.
- 6 Right-click the **ACDI driver**, click **Properties**, and check the **Driver configuration**.
For example, in the **Startup Option**, select the **Manual** radio button.
You can view the details you specified while creating the ACDI driver in **Driver Parameters > Subscriber Options**.

NOTE: You might need to enter the passwords again.

- 7 In the **Properties** window, select **Trace**. Ensure that the **Trace level** is set to 5. Also configure **Trace file**. For example, `var/log/idm/acdi/acdi.log`

Step 5: Deploying the ACDI Driver

- 1 In the Designer's Modeler view, select the **ACDI driver** and click the **Deploy** icon.
- 2 Review the deployment summary and click **Deploy**.
- 3 Review the deployment results and click **OK**.

Step 6: Starting the ACDI Driver

To start the driver, select the ACDI driver in the modeler view of Designer and click the **Start Driver** icon.

Step 8: Verifying the connection between OpenText Identity Manager and ACDI driver

You can check if the ACDI driver successfully connected OpenText Identity Manager to ACDI.

For example, you can modify an object description in Identity Console and check if the change is reflecting in Audit Dashboard.

Check the description by going to **Dashboards > Audit Dashboard > Audit Events** on the ACDI interface.

NOTE: To audit and monitor custom classes or attributes, you must add them to the ACDI Driver filter.

Installing the ACDI Monitor

The ACDI Monitor stores processed data in third-party drivers. To monitor a driver, you need to include the ACDI Driver Monitor package in it. This section describes how to install and configure the ACDI Driver Monitor package in Designer.

Step 1: Importing the packages to Designer

- 1 Launch Designer.
- 2 Open the project, then right-click the **Package Catalog** and select **Import package**.
- 3 Click **Browse** and locate the Designer folder under the AuditDriver folder in the extracted acdi_v24.4.zip. Select the following three packages:
 - ♦ SPACDMCS_<version>.jar
 - ♦ SPACDMON_<version>.jar
 - ♦ SPACDMUDA_<version>.jar
- 4 Click **Open > OK**.

Step 2: Adding packages to the driver for monitoring

- 1 Right-click the driver and select **Driver > Properties**.
- 2 Select **Packages**.
- 3 In the Select Packages window, select the ACDI Monitor option and click **OK**.
- 4 Click **Apply**.

Step 3: Installing and Configuring the ACDI Monitor

- 1 To install the ACDI Monitor, select the **Install** operation in the Package Management window.
- 2 Choose **Manual** for the **Auditing Mode**.
- 3 Specify the values for the parameters of the ACDI monitor.

Driver alias Name for Audit

Specify the driver's name. Search for this name in ACDI to view data from this driver. For example, `ActiveDirectory1`.

Operation Types to Audit (regex)

Specify the events you want to display in ACDI.

Status

Specify the status level for the events.

- 4 Click **Next**.
- 5 Click **Finish > Apply**.

Step 4: Sending data to OpenSearch

To specify the type for transmitting from the driver to ACDI's OpenSearch:

- 1 In the Modeler, right-click the driver set and select **Properties**.
- 2 Navigate to **GCVs**.

- 3 In the ACDI Monitor > common settings, select one of the following modes for data transmission:
 - ♦ Put to ACDI Driver Cache
The driver DN you define in the **ACDI Driver** parameter will process all events.
 - ♦ Send directly to OpenSearch and/or Logstash
Specify the path to your OpenSearch, the type of file, the user with OpenSearch credentials, and the path to the KeyStore with the certificate and its password. These parameters are similar to those defined in the ACDI driver for OpenSearch.
 - ♦ Send to ES/LS, On timeout put it to the ACD Driver Cache
Sends data to the OpenSearch and store in the ACD Driver Cache when a timeout occurs.
- 4 Click **OK**.
- 5 Click **Live > Driver Configuration > Deploy Attributes**.
- 6 Click  to restart the driver.

Checking Data on the ACDI Interface

- ♦ Using the Driver Dashboard

NOTE: This dashboard is only available in the Advanced version or Trial mode.

You can audit and monitor all events processed by the driver on the Driver Dashboard, which is the default dashboard of ACDI. You must modify this dashboard according to the name set in the appropriate driver. For example, if you set the driver name to `ActiveDirectory1` for the ACDI Monitor, this name will be displayed in the connected system on dashboard.

To change how each panel is visualized, select **Edit** and then adjust the filter. You can change the panel's title, clone it, and delete the panel from the dashboard, among other modifications.

- ♦ Using the reporting system

On the ACDI interface, you can access the **Audit Driver Events** report containing a list of all driver monitors located under the Connected System. You can filter the results by selecting a particular channel and the status of events you want to view. For example, to see all events with an "error" status for the Active Directory driver, select the status as `error` and the connected system as `Active Directory`, and click **Run**.

You can also access the final event document, which contains information about the reason for the error.

Installing the Workflow Monitor

This section describes how to install and configure the ACDI Workflow Monitor package in Designer. After installation, two custom templates, namely Workflow Audit and Workflow Audit - with loop are added to the User Application driver.

Step 1: Importing the required package to Designer

- 1 Launch Designer.
- 2 Open the project, right-click the **Package Catalog**, and select **Import Package**.

- 3 Click **Browse** and locate the Designer folder under the AuditDriver folder in the extracted acdi_v24.4.zip.
- 4 Select SPACDWM_<version>.jar and click **Open**.
- 5 Click **OK** to import the ACDI Workflow Monitor package.

Step 2: Adding the package to the User Application Driver

- 1 In the Modeler, right-click the User Application Driver and select **Driver > Properties**.
- 2 Go to **Packages**.
- 3 In the Select Packages window, select the ACDI Workflow Monitor package and click **OK**.
- 4 Click **Apply**.

Step 3: Installing and configuring the ACDI Workflow Monitor

NOTE: Before installing and configuring the ACDI Workflow Monitor, make sure to configure the User Application driver's global configuration value (GCV) to allow a named password to be retrieved over LDAP from a workflow. For more information, see [Allowing a Named Password to be Retrieved over LDAP](#) in the *OpenText™ Identity Manager CE 24.4 (v4.10) - Administrator's Guide to the Identity Applications*.

- 1 To install ACDI Workflow Monitor, select the Install operation in the Package Management window.
- 2 Specify the **Your ACDI host (without port and protocol)** and the **Port** to use. The default port is 3190.
- 3 Specify a value for the **Opensearch endpoint**. The default value for the **Workflow writable index alias** is write-workflow-default and the **Document type** is _doc.
- 4 Specify a **User (for Basic auth)** and a **Password (for Basic auth)**. This user must have access to the OpenSearch endpoint.
- 5 (Conditional) Specify the properties you want to use for the **Audit Workflow - with loop** template:
 - ♦ **Count of send tries in case of send error:** The maximum number of attempts to make if an error occurs while sending data to OpenSearch.
 - ♦ **Pause between send tries. min:** The time interval between attempts.
- 6 For the remaining parameters, specify the values you want to use for the ACDI Workflow Monitor.
- 7 Click **Finish**.

Make sure to check the GCVs and password for the user who has access to the Opensearch endpoint in the User Application driver's GCV.

Step 4: Using the custom workflow monitoring templates

In the Provisioning settings, go to **User Application Driver > Provisioning Request Definitions**. The following templates are available under the Custom Templates:

- ♦ Workflow Audit
- ♦ Workflow Audit - with loop

Viewing Workflow Dashboard on ACDI

The **Workflow Dashboard** on ACDI displays the statuses of your monitored workflows. You can view more details in the Workflow Report.

Final Step for Installation

After installing ACDI and configuring it with OpenText Identity Manager, you must manually import the ACDI certificate into the following locations:

- ♦ Identity Vault (cacerts) at /opt/netiq/common/jre/lib/security/cacerts

For example, you can use the following keytool command to import the ACDI certificate into the Identity Vault:

```
/opt/netiq/common/jre/bin/keytool -importkeystore -srckeystore <acdi-cert> -srcstorepass <cert-pass> -destkeystore /opt/netiq/common/jre/lib/security/cacerts -deststorepass <cacerts-pass> -noprompt
```

- ♦ User Application (idm.jks) at /opt/netiq/idm/apps/tomcat/conf/idm.jks

For example, you can use the following keytool command to import the ACDI certificate into User Application:

```
/opt/netiq/common/jre/bin/keytool -importkeystore -srckeystore <acdi-cert> -srcstorepass <cert-pass> -destkeystore /opt/netiq/idm/apps/tomcat/conf/idm.jks -deststorepass <idm.jks-pass> -noprompt
```


4 Accessing Audit, Compliance & Data Intelligence

After installing ACDI and the required ACDI drivers and packages, you need to configure the installed components through the ACDI user interface. You can access the ACDI user interface using any supported web browser. While we recommend using Mozilla Firefox as the preferred browser, most of the popular browser versions are also supported. However, we cannot guarantee or support full functionality with any browser that is not officially supported. For information on supported web browsers, see [“System Requirements” on page 19](#).

To access the Audit, Compliance & Data Intelligence, perform the following steps:

- 1 Enter the following in the address (URL) field of a supported web browser.
Secure Login: `https://<acdi_FQDN>/audit/user/signIn`
- 2 Enter your login ID and password.
- 3 Click **Login**.

5 Configuring Audit, Compliance & Data Intelligence

Audit, Compliance & Data Intelligence (ACDI) uses the ACDI Proxy service to redirect requests from HTTP or HTTPS, from endpoints to appropriate ports used by various services. These services and ports include a direction table from the endpoint to the internal port if you require the ACDI server. You need to open only one local port to outside connections. By default, it is 3190 (for HTTPS) and 3191 (for HTTP).

After installing Audit, Compliance & Data Intelligence (ACDI), perform the configuration required to setup:

- ♦ [“Setting Up Core Engine” on page 31](#)
- ♦ [“Setting Up Audit Server” on page 36](#)
- ♦ [“Setting Up Data Connectors” on page 40](#)

Setting Up Core Engine

The Core Engine of ACDI consists of the following components:

- ♦ [“LDAP Connections” on page 32](#)
- ♦ [“LDAP Authentication Settings” on page 33](#)
- ♦ [“Web Server Settings” on page 34](#)
- ♦ [“Mailer Settings” on page 35](#)
- ♦ [“Scheduled Tasks” on page 35](#)
- ♦ [“Session Settings” on page 35](#)
- ♦ [“Web Proxies List” on page 35](#)
- ♦ [“WS Proxies List” on page 35](#)
- ♦ [“Local Access List” on page 36](#)
- ♦ [“List of Rule Presents” on page 36](#)
- ♦ [“AuditProxy API List” on page 36](#)
- ♦ [“Role List” on page 36](#)
- ♦ [“Post Configuration of Core Engine” on page 36](#)

NOTE: Any changes made to the core engine setup will be implemented after restart.

LDAP Connections

Using this component, you can add and configure LDAP connections between the ACDI server and Data connectors. When you create a new data connector using Data Connection Wizard, the LDAP connection is automatically added to the connection list.

On the homepage, go to **Administration > Core Engine > LDAP Connections** to see the available LDAP connections.

You can perform the following operations on the LDAP connections:

- ♦ [“Add an LDAP Connection” on page 32](#)
- ♦ [“Edit an LDAP Connection” on page 32](#)

Add an LDAP Connection

NOTE: It is recommended to add new connections using Connection Wizard.

- 1 Click the **+** icon and provide the following details:
 - ♦ Name of connection
 - ♦ Type (Data connector used)
 - ♦ URL
 - ♦ Username
 - ♦ Password
 - ♦ (Optional) Connection Timeout
- 2 Click the save  icon.

Edit an LDAP Connection

- 1 Click the connection you want to edit and modify the following values:
 - ♦ Name of connection
 - ♦ Type (Data connector used)
- 2 Click **Auth** to enable authentication.
- 3 Click the **LDAP Server** list and edit the following:
 - ♦ URL
 - ♦ Username
 - ♦ Password
 - ♦ Connection Timeout
- 4 Click the **TLS options** list and edit the following:
 - ♦ Private key

- ♦ Certificate
- ♦ CA

5 Click  save icon.

LDAP Authentication Settings

This component consists of all parameters and attributes required for authentication operation.

Table 5-1 LDAP Authentication Settings Parameters

Parameters	Description
Search Scope	Specify the portion of the directory tree that a user can search within. ACDI supports three different scopes: ♦ base ♦ one ♦ sub
Base DN	Helps to search users from the base container by multiple options such as through user's ACDI and user's data. NOTE: Only users located in the specified containers according to Search Scope will be able to login.
Membership attribute	Defines user roles, permissions, and linkage attribute between the user and the object that will have entitlements can be defined. By default, entitlements are granted with groupMembership attribute.
Right mapping attribute	Attribute in object (by default it is Group) which holds ACDI entitlement info. By default it is Description. It is recommended to change it to custom auxiliary attribute.
Filter group names with regular expressions	Specifies the groups that you must look up to determine entitlements.
Additional LDAP filter	To use a custom attribute for role assignments.
Authentication timeout	Set timeout for authentication in seconds. The minimum timeout is 5 seconds.
Search attributes	Helps to search users. For example: mail, cn
Additional attribute	Saves additional information from LDAP.

Perform the following steps to configure LDAP authentication:

- 1 On the Homepage go to **Administration > Core Engine > LDAP authentication settings**.
- 2 Modify all the parameters and attributes according to the requirements. For more details about parameters check
- 3 Click the save icon.
- 4 Log in to Identity Console and create the required users and a group for entitlement configuration.

For more information, see [Creating a User \(https://www.netiq.com/documentation/identity-console/identity_console-admin/data/t497jzeuqusw.html\)](https://www.netiq.com/documentation/identity-console/identity_console-admin/data/t497jzeuqusw.html) section and [Creating a group \(https://www.netiq.com/documentation/identity-console/identity_console-admin/data/t497jzqd4ibp.html\)](https://www.netiq.com/documentation/identity-console/identity_console-admin/data/t497jzqd4ibp.html) section.

NOTE: You must add one value in the description. For example, add an empty JSON string {} as the description.

- 5 Add the users to the group created.
- 6 Go to ACDI to assign entitlements and access the group you created.
- 7 Click manage user accounts  icon in the top right corner.
- 8 Specify a username and click **Get User Data**. Password is optional.
- 9 Edit the user's attributes as per your requirements.
- 10 In **ACDI Filtered Groups** for User, select appropriate group and assign ACDI roles, add Report and Dashboard filters (support regex) and click the  **Save** icon.

NOTE: Raw field will display final value of Right mapping attribute. If you see **Bug** icon near your Group, enter {} in a **Raw** field.

Web Server Settings

ACDI provides the following web server settings for troubleshooting events:

- ♦ External Hostname
- ♦ External Port Number
- ♦ Local Hostname
- ♦ Local Port Number
- ♦ Path to keystore file of external host
- ♦ Keystore password of external host
- ♦ Path to keystore file of local host
- ♦ Keystore password of local host

Using the **Self Test Settings parameters**, you can monitor the health of ACDI and see the results on **Administration > Health and Metrics > System Health**.

Using **Opensearch Stats Settings parameters**, you can monitor the Opensearch status of ACDI and see the results on **Administration > Health and Metrics > Opensearch Health**.

Mailer Settings

Using Mailer Settings, you can configure an email ID. The Reporting service uses this email ID to send scheduled reports and in-system notifications.

Scheduled Tasks

You can perform multiple tasks and schedule them to run automatically by providing proper scripts and arguments.

To schedule a task, perform the following steps:

- 1 On the Homepage go to **Administration > Core Engine > Scheduled tasks**.
- 2 Expand a task and specify the required details.
- 3 (Optional) To add multiple tasks, click the plus + icon to add a new task.
- 4 Click save  icon.

Session Settings

You can configure the following settings for a web server session:

Settings	Description
Cookies name	The name of the cookie used.
Secret word	The value used for encrypting your session ID.
Session max age	The maximum duration for which a session remains active.
Session stored LDAP attributes	Stores some LDAP attributes of current users in the session.

Web Proxies List

You can configure the list of endpoints and ports used for redirecting requests of a proxy. Also, you can add custom headers to a proxy.

WS Proxies List

Perform the following steps to add a WS proxy to the list:

- 1 On the Home page, go to **Administration > Core Engine > W S Proxies list**.
- 2 Click the plus + icon.
- 3 Provide the required details.
- 4 Click the save  icon.

Local Access List

Here, you can check the list of local users who can access ACDI. You can also add a new local user account and update the following details:

- ♦ Proxies allowed for user
- ♦ Roles apply to user
- ♦ AuditProxy API's allowed

List of Rule Presents

This component contains the list of rules used for advanced role customizations. You can configure a data transformation of ACDI proxy in the calls for appropriate users. Additionally, you can specify endpoints for the rules and URLs. These endpoints will be used when a rule runs your JavaScript code and modifies data.

AuditProxy API List

Use this component for advanced role configuration consisting of a list of APIs and their configuration details.

Role List

Here, you can see a list of roles that can authenticate to the ACDI setup. You can add or edit a list of allowed rules and a list of allowed APIs for each role.

Post Configuration of Core Engine

Perform the following steps after making any change in the Core Engine configuration to reflect the changes:

NOTE: Any changes made to the core engine setup will be implemented after restart.

- 1 After saving the changes, click control service  icon.
- 2 Click **Restart**.
- 3 Refresh the page and log in again.

Setting Up Audit Server

The Audit Server helps process backend configurations and the web interface in ACDI.

To get to the Audit Server settings, on the homepage go to **Administration > Audit Server**.

The Audit Server consists of the following components:

Back-end Properties

This component consists of general parameters and settings for the Audit Server.

Table 5-2 Parameters in Back-end Properties

Parameters	Description
Server ID	The ID of the ACDI application
License	Specify the license number.
OpenSearch endpoint name	The name of the endpoint for open search
Old Reporting index name	The name of the index where old report templates are stored
New Reporting index name	The name of the index where report templates are stored
Scheduler data folder	The path of folder used for the post processing cache
AuditExport data access protocol	The FQDN of ACDI
AuditExport data	The path to store the export data if you change the FQDN value.
Logo	The logo of your company and export here
Maximum email file size	The maximum size of a file that you can share over emails.
Opensearch request size	Size of objects to get per one request to Opensearch NOTE: The default value is 100000. You can extend it by changing in the appropriate setting in OpenSearch.
ACDI Node name	Used for Analytics NOTE: Do not change the default values of these settings.

External Configs

This settings panel contains paths to different ACDI services which are by default located in the same machine. These settings must be changed to move some of those services to different directories.

ACDI service lists

This page contains a list of different services provided by ACDI.

Table 5-3 Service names in ACDI

Service name	Description
audit-proxy.service	The proxy service helps to handle data in ACDI.
audit-report-edir@.service	The service that makes a snapshot from OpenText eDirectory.
audit-export.service	The service that processes reports and creates files.
audit-server.service	The service responsible for the ACDI web interface.
opensearch.service	The service that controls analytics and monitoring
osd.service	OpenSearch Dashboards service.

Day Time Format

Using this component, you can define dates in the following formats:

- ♦ A browser-defined format.
- ♦ A time zone for the front-end web interface which you can see in Dashboards, Time Machine, and other ACDI service tabs where dates with time zones are used.

Indices Settings

This components lists the LDAP connections that are available in **LDAP Connections** under **Core Engine** and the settings of different indices, such as report, audit and add additional attributes if requested.

Settings	Description
Name	The name of the index setting.
Name of LDAP connection	The name of the AuditProxy LDAP connection corresponds to the current Index.
Directory Type	The type of the directory the connection belongs to.
Snapshot related settings for Report	
The key attribute	The attribute used for linking objects with audit data.
Date-time fields correction: ♦ Date field	The list of date-time fields settings that you can display on the dashboard and Time Machine. ♦ Specify names and time zones.
Service attributes	The list of additional attributes. You can see these in History Browser .

NOTE: **Event related settings** for Audit and **Snapshot related settings** for Report are similar.

Perform the following steps to verify the **Service attributes** for an index source:

- 1 On the home page, go to **History browser > Time Machine**.
- 2 Select the required index from **Select index source**.
- 3 Select an object in the object pane.
- 4 Click options  icon and select **Show service attribute**.

URLs and Roles

This component contains a list of ACDI endpoints. You can approve or deny access to endpoints for different roles.

Reports Menu

This component contains a list of customizable sub-menus in **Reports**.

Perform the following steps to customize the **Report** menu:

- 1 On the home page, go to **Administration > Audit Server > Reports Menu**.
- 2 Click **+** to add a new menu item.
- 3 Specify a tag in **Report Tag**.
- 4 Specify a title in **Title used in Menu**.
- 5 Click **show**.
- 6 Save changes and refresh.

Dashboards Menu

It contains list of sub-menus you have in **Dashboards** and you can customize it.

Perform the following steps to customize the **Dashboards** menu:

- 1 On the home page, go to **Administration > Audit Server > Dashboards Menu**.
- 2 Click **+** to add a new menu item.
- 3 Specify a tag in **Report Tag**.
- 4 Specify a title in **Title used in Menu**.
- 5 Click **show**.
- 6 Save changes and refresh.

Home Page Cards

It contains the lists of cards available on the ACDI home page such as Dashboards, Reports, and Time Machine. You can update the existing cards or create a new one. Furthermore, the component provides options for CSS styling, uploading images, background color, text, and a redirect URL route from a list.

Misc Audit Server settings

Using this setting, you can adjust the width of the ACDI menu on the left.

Setting Up Data Connectors

Data Connector Wizard helps to create a new connection to a LDAP server.

Perform the following steps to create a new connection:

- 1 On the homepage, go to Administration > Data Connection Wizard.
- 2 Make sure to select the connection type at the top.
- 3 Give a name for it in the **Connection Name** and **Connection ID** to be used in the index name.
- 4 Under **LDAP Server Settings**, provide URL, username, and password.
- 5 Click **Test**, If the button turns green, it indicates that all settings have been checked and a connection can be created.
- 6 Click **Create New Data Connector**.
- 7 Once the connector is created, click **Please Reload App**.

Checking Snapshot service

After creating new connection the snapshot service of the connection will be available under **Data Collection** in the left pane. In this snapshot service you can see the following settings:

- ♦ LDAP Server URL
- ♦ LDAP Service account name
- ♦ LDAP Service account password
- ♦ Keystore file name
- ♦ Path to keystore

Perform the following steps to check the snapshot service:

- 1 Click control service  icon and click **Start** to start service.
- 2 (Optional) You may get the following error: Connection or outbound has closed
This happens because IDM can send you a certificate not with FQDN but with an IP address instead. In this case change the **LDAP Server URL** from FQDN to IP.
Now save and start the service again.
- 3 In the log you will receive a root object, which means the service is started successfully.
- 4 Now go to **Time Machine**, on the top **Select index source** select your connection.
- 5 You will get information about the snapshot:
 - ♦ Start Time
 - ♦ Finish Time
 - ♦ Duration

- ♦ Total Objects
 - ♦ Average Object Size
 - ♦ Average number of objects processed per second
 - ♦ Average index size
- 6 Click **Time Machine** to get a list of snapshots for each connection and information about each snapshot.

6 Updating Audit, Compliance, & Data Intelligence

Use the following information to update Audit, Compliance & Data Intelligence (ACDI) to the newer version on your server.

Prerequisites for Updating ACDI

Before proceeding with the update, ensure that you meet the following prerequisites:

- ♦ Take a complete backup of the ACDI installation folder.
- ♦ Take a complete backup of the ACDI data folder.
- ♦ Ensure you have at least 16 GB of free disk space.
- ♦ Stop the Audit Driver and any third-party driver monitors.

Update Procedure

Perform the following steps to update ACDI:

- 1 Log in to the ACDI server as root user.
- 2 Download `acdi_v24.4.zip` from the [Software License and Download \(https://sld.microfocus.com\)](https://sld.microfocus.com) portal.
- 3 Navigate to the `/opt` directory and create a new directory inside `/opt`.
For example, `mkdir 24.4`
- 4 Unzip `acdi_v24.4.zip` in the new directory.

IMPORTANT: Do not unzip where ACDI is currently installed. This will overwrite existing files in `/opt/acdi` and cause an update failure.

- 5 Run the `./update_24.2-24.4.sh` script.
For example, `sles15sp5:/opt/24.4/acdi # ./update_24.2-24.4.sh`
- 6 Specify the path where ACDI is currently installed.
For example, `/opt/acdi`
- 7 (Optional) After the update, view the installation summary in the `./ACDIinstaller` directory.

NOTE: Your existing dashboards and reports are backed up in the `acdi_backup_<stamp>/_dashboards_reports` directory after ACDI is updated.

- 8 Copy the updated files from the `/opt/acdi/AuditDriver/Server` directory to the server running OpenText Identity Manager. For location details, see [“Installing Audit, Compliance & Data Intelligence” on page 19](#).

- 9 Restart OpenText Identity Manager.
- 10 Launch Designer.
- 11 Copy the updated files from the /opt/acdi/AuditDriver/Designer directory to the system running Designer.
- 12 Update the packages for ACDI Driver, ACDI Monitor, and Workflow Monitor. For more information about how to update the packages, see [Upgrading Installed Packages](#) in the *Designer Administration Guide for OpenText™ Identity Manager CE 24.4 (v4.10)*
- 13 Deploy and restart the drivers.



Getting Started with Audit, Compliance & Data Intelligence

This section tells you how to begin using the Audit, Compliance & Data Intelligence interface. Topics include:

- ♦ [Chapter 7, “Using Dashboards,” on page 47](#)
- ♦ [Chapter 8, “Using Reports,” on page 57](#)
- ♦ [Chapter 9, “Using Time Machine,” on page 59](#)

7 Using Dashboards

Audit, Compliance & Data Intelligence (ACDI) accesses identity-related data from various locations and resources, processes it, and displays it graphically on dashboards. These dashboards provide a real-time overview of your environment. You can explore, discover, and inspect your data with ease. You can also customize the dashboards to meet your specific business requirements. Additionally, the dashboard offer several options for auditing and monitoring your data.

ACDI supports connection to the following resources:

- ♦ OpenText eDirectory (OpenText Identity Manager)
- ♦ OpenText Access Manager

Click **Dashboards** on the ACDI Home page to access dashboards.

For more information about **Manage > Dashboard Editor**, see [Working with Dashboard Editor](#).

Default Dashboards for OpenText Identity Manager

ACDI offers a set of OpenText Identity Manager dashboards with pre-defined visualizations that you can explore before adding your data. To access them, navigate to **Dashboards > IDM**.

Audit Dashboard

The Audit Dashboard displays information about events in OpenText eDirectory. This dashboard collects data from the ACDI driver in OpenText Identity Manager.

On this dashboard, you can monitor real-time updates in OpenText eDirectory. For example, if a user adds a new location to their profile through OpenText Identity Manager, you can view this event in the **Audit Events** table on this dashboard. To monitor custom classes and attributes, add them to the **ACDI Driver Filter** in Designer. For more information about installing the ACDI driver and adding custom attributes, see [Installing the ACDI Driver](#).

Driver Dashboard

The Driver Dashboard displays information about events in the third-party drivers (connected systems) installed with OpenText Identity Manager. This dashboard collects data from the ACDI Driver Monitor package installed on the third-party driver you want to monitor. For more information about how to install the ACDI Driver Monitor package, see [Installing the ACDI Monitor](#).

On this dashboard, you can monitor real-time events processed by third-party drivers. If you have multiple drivers with the ACDI Driver Monitor package, you can view events for all drivers in one place or for each driver separately. For example, the ACDI Driver Monitor package is installed on two drivers, namely the Active Directory driver and the Loopback driver. You can use the **Monitored Drivers Events Gauge** to see an overview of events for both drivers. Alternatively, you can use the **AD Driver Channel Gauge** and **Loopback Driver Channel Gauge** for individual views. In addition, you can find more information about these events in the **Drivers Events** table.

IDM System Overview

The IDM System Overview displays a consolidated view of events collected from OpenText eDirectory via ACDI Driver and ACDI Driver Monitor.

Security Dashboard

The Security Dashboard displays information about security-related events in OpenText Identity Manager. This dashboard captures security-specific data from the ACDI driver.

On this dashboard, you can monitor security events such as the number of enabled and disabled logins, intruder lockouts, and failed logins to OpenText Identity Manager. The **Security Events** table contains more information about these events.

Workflow Dashboard

The Workflow Dashboard displays the statuses of monitored workflows in OpenText Identity Manager. This dashboard collects data from the ACDI Workflow Monitor package. You need to add this package to the User Application Driver (UAD) to provide custom workflow templates. You can customize this template to monitor a specific workflow on ACDI. For more information about how to install the ACDI Workflow Monitor package, see [Installing the Workflow Monitor](#).

On this dashboard, you can track the workflow statuses, including the number of workflows in processing, approved, and denied state. You can find more information about these workflows in the **Workflows** table.

Other Sample Dashboards

ACDI offers two additional dashboards for monitoring the health of the ACDI system and the OpenSearch module.

ACDI System Health Dashboard

The ACDI System Health Dashboard displays the health and performance of the system. To make this dashboard visible, configure the **Self-test settings** under **Administration > Core Engine > Web Server settings**.

You can monitor the following statistics on this dashboard :

- ♦ CPU details such as the number of CPU cores and used and free CPU percentage
- ♦ RAM details such as total RAM size (Mb), used RAM (MB), and free RAM (MB)
- ♦ Disc information such as total disc size, used space, and free space (GB)
- ♦ Percentage of CPU, drive, and RAM usage for each in graph and gauge format
- ♦ Consolidated usage graph depicting average usage CPU, drive, and RAM usage over a time interval
- ♦ Count of total LDAP connections
- ♦ Count of failed LDAP connections
- ♦ Count of files opened by OpenSearch
- ♦ System resource usage in a table format

Open Search Health Dashboard

The Open Search Health Dashboard displays the health status and performance of the OpenSearch module. To make this dashboard visible, configure the **OpenSearch Stats settings** provided in the **Administration > Core Engine > Web Server settings** to collect [OpenSearch metrics](#).

You can monitor the following OpenSearch statistics on this dashboard:

- ♦ Global health status details
- ♦ CPU usage percentage over time in graph and gauge formats
- ♦ OpenSearch JVM heap usage percentage over time in graph and gauge formats
- ♦ Opened file descriptors over time in table and graph formats
- ♦ Store usage and size over time in table and graph formats
- ♦ OpenSearch index time, garbage collection, search query time, thread count, and total documents in a graph format
- ♦ OpenSearch health statistics in a table format

Understanding Dashboard Basics

Each dashboard comes with a default set of visuals and search options that can assist you in finding the relevant data.

The following topics cover the basic actions you can perform on dashboards, starting with the operations on the Dashboards page, followed by the operations on individual dashboards. Most of the operations apply to all dashboards unless specific otherwise.

- ♦ [“Searching For Dashboards” on page 49](#)
- ♦ [“Customizing Dashboards” on page 50](#)
- ♦ [“Viewing Individual Dashboards” on page 50](#)
- ♦ [“Full Screen for Better Viewing” on page 50](#)
- ♦ [“Generating Dashboard URLs for Sharing” on page 51](#)
- ♦ [“Generating OSD Reports” on page 52](#)
- ♦ [“Cloning Dashboards” on page 53](#)
- ♦ [“Interacting with Your Dashboard Data” on page 53](#)
- ♦ [“Using the Inspect Feature for Debugging” on page 55](#)

Searching For Dashboards

You can find specific dashboards by using one of the following options:

Search by Tags

This option is selected by default. To search for dashboards with a specific tag, select a tag from the **Filter Dashboards** list and then click outside the list. You can add multiple tags to refine your search results.

Search by Name

Select the **Search by Name** option, select the name of the required dashboard in the **Filter Dashboards** list, and click outside the list. You can select multiple names.

Customizing Dashboards

The Dashboards page has a default view that you can customize to your preference.

Sort

By default, the dashboards are arranged in ascending alphabetic order. To sort in reverse order, click the  **Sorted** icon.

Card Size Scale

Click the  **Dashboard card size scale** icon and slide to adjust the size of all dashboards cards.

Reload

Click the  **Reload** icon to load the latest Dashboards page.

Viewing Individual Dashboards

Each dashboard has a **Load** option that allows you to load the dashboard data and all its infographics for visualization. For more information on how to interact with these infographics, see [Interacting with Your Dashboard Data](#).

In addition to the **Load option**, each dashboard also has the option to **Edit** or **Clone** it. The **Clone** option is only available on default dashboards or those created by ACDI. These dashboards cannot be edited directly. However, the **Edit** option is available if you clone the dashboard or create a new one using the **Dashboard Editor**. For more information about how to clone a dashboard, see [Cloning Dashboards](#) and to create a new dashboard, see “[Creating a New Dashboard](#)” on page 65.

When you access a dashboard, ACDI automatically saves it to **Dashboards > Favorites** for quick and easy future access.

TIP: If you want to see a list of all dashboards and their last updated time, click **Dashboards** tab next to the one you are currently viewing.

Full Screen for Better Viewing

Enhance your dashboard viewing experience with the **Full screen** option. When you click on it, the full-screen mode maximizes your view by hiding the toolbar. To further elevate your experience, minimize the navigation pane by clicking the  triple bar icon located at the top left corner of the screen.

When you are done with the full screen mode, click **Exit full screen** to switch back to the regular view.

Each visualization panel in a dashboard can be maximized further for a better view of the information. Click  located in the top right corner of the panel and select **Maximize panel**. When a panel is maximized, other panels in the dashboard will be hidden. To switch back to the regular view, click  again and select **Minimize**.

You can use the  **Toggle Legend** option to show or hide legends on each panel.

Generating Dashboard URLs for Sharing

If you have created a custom dashboard on ACDI and wish to share it with other ACDI users, ACDI offers several options to do it. You can either send a URL of your current dashboard view or a URL that enables users view the latest version of the dashboard. In addition, ACDI additionally offers two distinct formats to generate dashboard URLs:

- ♦ **iFrame:** The dashboard URL is embedded within the `<iframe>` `</iframe>` HTML tag that can be easily embedded into another HTML document.
- ♦ **Permalinks:** Permalink of a dashboard is the complete URL that enables users to see all dashboard content.

To embed the dashboard link into the HTML iFrame element, perform the following steps:

- 1 On the ACDI's Home page, click **Dashboards**.
- 2 Click **Load** on the dashboard of your choice.
- 3 Click **Share > Embed code** and choose any one of the following options depending on whether you want to share the dashboard with a relative or fixed timeframe:

Snapshot

Generates a URL that encodes the current state of the dashboard as a snapshot, including the time selection as absolute dates. Your recipients sees the same data you are viewing now. Any changes saved after generating the URL will not be visible through this URL.

Saved Object

Generates a dashboard URL with a relative time selection. Share this URL if you want users to access the latest saved version of this dashboard.

- 4 (Optional) Select the dashboard components you want to include in the generated URL.
Available options:
 - ♦ Top Menu
 - ♦ Query
 - ♦ Time filter
 - ♦ Filter bar
- 5 (Optional) Only applies if you choose to share the snapshot URL of a dashboard, as in [Step 3](#).
Enable **Short URL** to generate a shortened URL for the snapshot. This option is useful in cases when browsers have limitations on URL length and are not fully compatible with the full-length version.
- 6 Click **Copy iFrame Code**.

To generate a permanent link of your dashboard, perform the following steps:

- 1 On the ACDI's Home page, click **Dashboards**.
- 2 Click **Load** on the dashboard of your choice.
- 3 Click **Share > Permalinks** and choose any one of the following options depending on whether you want to share the dashboard with a relative or fixed timeframe::

Snapshot

Generates a URL that encodes the current state of the dashboard as a snapshot, including the time selection as absolute dates. Your recipients sees the same data you are viewing now. Any changes saved after generating the URL will not be visible through this URL.

Saved Object

Generates a dashboard URL with a relative time selection. Share this URL if you want users to access the latest saved version of this dashboard.

- 4 (Optional) Only applies if you choose to share the snapshot URL of a dashboard, as in [Step 3](#).
Enable **Short URL** to generate a shortened URL for the snapshot. This option is useful in cases when browsers have limitations on URL length and are not fully compatible with the full-length version.
- 5 Click **Copy link**.

Generating OSD Reports

ACDI offers you the ability to generate reports in three different file formats, namely PDF, PNG, and CSV. You can generate reports in PDF and PNG formats using the Dashboards user interface, while the option to generate reports in CSV format is available on the Discover page under the **Manage** menu.

To generate a report from the Dashboards user interface, perform the following steps:

- 1 On the ACDI's Home page, click **Dashboards** in the navigation pane.
- 2 Click **Load** on the Dashboard of your choice.
- 3 Click **Reporting** from the toolbar.
- 4 Click **Download PDF** or **Download PNG** based on your requirement.

To generate a report from the Discover page, perform the following steps:

- 1 On the ACDI's Home page, click **Manage > Discover** in the navigation pane.
- 2 Select the dataset and the time range to generate data.
- 3 Click **Reporting > Generate CSV**.

Report generation time may vary depending on the size of your data. Do not close the Generating report dialog while the report is being generated. You will receive a notification when your report is ready for download. To view the report, click **Reports** in the notification window.

All generated reports are kept on record on the Discover page. After the report is successfully generated, you can also view it by going to **Manage > Discover > Reporting > View reports**. Click the report link you wish to view.

Creating Schedule-based Report

To create scheduled reports, you must create a report definition first. Go to **Discover > Reporting > Create report definition**. The option pre-fills many of the fields based on the data you were viewing. For more information, see [Creating reports using a definition \(https://opensearch.org/docs/latest/reporting/report-dashboard-index/#creating-reports-using-a-definition\)](https://opensearch.org/docs/latest/reporting/report-dashboard-index/#creating-reports-using-a-definition) in the Opensearch Documentation.

Cloning Dashboards

Cloning creates an editable copy of the original dashboard, duplicating all existing visualizations. You can then modify the visualization on the cloned dashboard.

- 1 Click **Clone** on the dashboard you want to clone.
ACDI automatically assigns a new **Dashboard ID** to the cloned dashboard.
- 2 In the Dashboard Editor, specify a new **Display Name**.
- 3 Click the  **Save** icon.

Interacting with Your Dashboard Data

Dashboards allow you to analyze and visualize your data in depth. ACDI offers various options to construct filters, also known as search terms or queries, which help to narrow down the result. You can filter for data based on different criteria such as “within the last 7 days” or “contains the Object Name:Smith”. These filters allow you to interact with the data on a dashboard and get desired insights.

The following sections explain in a sequence how to explore your data on a dashboard:

- ♦ [“Setting the Time Filter” on page 53](#)
- ♦ [“Searching Your Data With Queries” on page 54](#)
- ♦ [“Saving the Search” on page 55](#)

Setting the Time Filter

When your data contains time-based events, the visualization panel displays data within a specified time range. Using the time filter, you can limit the time range of data displayed. The default time range is last 24 hours, but you can customize it.

If you want to change the time filter, you can use one of the following options:

- ♦ On a dashboard, click  and select one of the time filter options:
 - ♦ **Quick select:** Choose a time based on the last or next number of seconds, minutes, hours, days, or another time unit.
 - ♦ **Commonly used:** Choose a common time range like Today, Last 7 days, or Last 30 days.
 - ♦ **Recently used date ranges:** Use a previously selected data range.

- ♦ **Refresh every:** Specify an automatic refresh rate. You can configure a refresh rate to periodically resubmit your searches.

Sometimes, your view might be broken when checking data. To search and visualize data without any breaks, click **Stop**.

- ♦ To set start and end times, perform the following steps:
 1. Click **Show dates** and then click anywhere inside the toolbar to access the time filter window.
 2. Select **Absolute**, **Relative**, or **Now** and specify ranges.
 3. Click **Refresh** to apply changes.

Timeline Visualization

To zoom into a specific period, click and hold the left mouse button in a timeline-based visualization panel.

For example, in the Audit Dashboard, apply a time filter to display audit events for the last 7 days. The audit events histogram shows a count of events collected for 3 hours each day from 12:00 to 18:00 hours for 7 days. Click and hold the left mouse button for any particular day to zoom in and see visualization for every hour of that day.

Searching Your Data With Queries

ACDI provides you the following options for building search queries:

- ♦ [OpenSearch Dashboard Query Language \(DQL\)](#)
- ♦ [Lucene Query Syntax](#) (Lucene)

Both DQL and Lucene offer different sets of features. DQL is a simple text-based query language that filters data based on whether a field has a value, matches a given value, or falls within a specific range. Lucene, on the other hand, provides more advanced features, such as regular expressions or fuzzy term matching. However, Lucene cannot search nested objects or scripted fields. Choose the option that best suits your business requirements. Lucene is the default query language for all dashboards.

Using OpenSearch Dashboard Query Language

You can combine free text search with field-based search using DQL. Type a search term to match across all fields, or start typing a field name to get suggestions for field names and operators that you can use to build a structured query. The ACDI will filter data and return only matching results.

For example, to search for text in a particular field (field-based search), specify the field name before the colon:

Object Name:Smith

The analyzer for the field you are searching for parses the query text into tokens and matches documents in which any of the tokens appear.

For more information on DQL search options, see [Dashboards Query Language \(DQL\)](https://opensearch.org/docs/latest/dashboards/dql/) (<https://opensearch.org/docs/latest/dashboards/dql/>) in the OpenSearch documentation.

Using Lucene Query Syntax

When you turn off DQL, OpenSearch Dashboards uses Lucene query syntax for building search queries and filtering. Lucene's syntax is based on the Apache Lucene query syntax.

For more information on DQL search options, see [Query string query](https://opensearch.org/docs/latest/query-dsl/full-text/query-string/) (<https://opensearch.org/docs/latest/query-dsl/full-text/query-string/>) in the OpenSearch documentation.

Saving the Search

If you frequently use any of the search options, click the  **See saved queries** icon to save or load a previously saved query. The saved query always contains the semi-structured search query, and optionally the time filter and extra filters.

Using the Inspect Feature for Debugging

Inspect is a feature of OpenSearch Dev Tools that helps you explore data and debug issues. You can use it to troubleshoot queries that do not return the desired results by inspecting the request and response data.

The  **Inspect** option on each dashboard visualization panel offers the following two options to view:

- ♦ **Data:** Click to view data behind the visualization.

You can also download the data in CSV format. Click **Download CSV**, then choose a download option from the list below:

- ♦ **Formatted CSV:** Downloads the data in table format.
- ♦ **Raw CSV:** Downloads data in its original format, such as dates as timestamps.
- ♦ **Requests:** Click to view the request query sent to OpenSearch to fetch data for the visualization panel, the response received in return and the statistics related to the query.

8 Using Reports

A report is a table of records that you can generate by running a report definition in ACDI. Reports are used for auditing and monitoring events and data in your directory. The Snapshot Service and Event Service provide the data and audit events necessary to generate an ACDI report.

A report definition usually includes a data source, customizable filters, and display attributes needed to create a report result table. The table can then be exported in PDF, CSV, or XLSX formats. You can download the file and process it with third-party softwares. ACDI also offers a Report Editor, which enables you to create custom report definitions. For more information, see [Chapter 11, “Working with Report Editor,”](#) on page 69.

To access reports, go to the ACDI Home page and click **Reports**.

Default Reports for OpenText Identity Manager

ACDI offers a set of OpenText Identity Manager report definitions with predefined filters that you can explore before creating custom report definitions. To access them, navigate to **Reports > IDM**.

Users Report

The Users Report displays user-related information such as ID, first name, last name, job title, email ID, groups they belong to, and account details. Using the filters, you can This report is based on data from OpenText eDirectory snapshots.

Group Membership Report

The Group Membership Report lists groups and their members. The filters allows you select groups, containers, or description to display members in a specific group. This report is based on data from OpenText eDirectory snapshots.

Audit Users Report

The Audit Users Report shows basic audit information of user records, including what users records have been modified and when they were modified. It lists the user accounts that were created, modified, and deactivated within a given date range.

Audit Driver Events

The Audit Driver Events display an audit trail of events in an individual driver’s logs. You can view a report of the total number of status updates per driver. To drill down into the specific status changes for a driver, you can select the row for the driver.

Audit Driver Status

The Audit Driver Status display an audit trail of status changes and edits to an individual driver’s logs. You can view a report of the total number of status updates per driver. To drill down into the specific status changes for a driver, you can select the row for the driver.

Audit Groups

Role Request Report

The Role Request Reports how the roles and resource are assigned to the users in your organization. You can run the report for all admins, individual admins, or groups.

Users Login Network Address Report

The Users Login Network Address Report displays a full list of users that have access to the network. The report will show the username, access level, and email of each user. When clicking on a user, you can drill down to reveal more details, including host name, IP address, and device accessed.

Users Login Time Report

The Users Login Time Report displays the date and time at which the user logged in to the application using LDAP authentication. The data on this report comes from the following sources:

Workflow Report

The Workflow Report displays workflow statuses. The data on this report comes from the ACDI Workflow Monitor packages.

Understanding Reports Basics

This section includes:

- ♦ [“Searching For Reports” on page 58](#)

Searching For Reports

You can find specific reports by using one of the following options:

Search by Tags

This option is selected by default. To search for reports with a specific tag, select a tag from the **Filter Reports** list and then click outside the list. You can add multiple tags to refine your search results.

Search by Name

Select the **Search by Name** option, select the name of the required report in the **Filter Reports** list, and click outside the list. You can select multiple names.

9 Using Time Machine

Time Machine displays the status of an LDAP object at different points in time. You can choose a source for the object, which is OpenText eDirectory by default, and specify the time interval for capturing the snapshots. Based on the interval, the Time Machine creates a timeline of the snapshots, which you can use to track the changes made to the object over time.

After creating a timeline, you can use the History Browser option to perform the following actions:

- ♦ Search for an object, view detailed information about that object, and changes made to its attributes.
- ♦ View audit events in the timeline if enabled.
- ♦ Use the Object Compare tool to compare snapshots and audit events of individual objects at various times, allowing you to see the differences.
- ♦ Export the state of an object from any time in history in CSV or LDIF file format.

This section includes the following information:

- ♦ [“Using Time Machine to Review Snapshots” on page 59](#)
- ♦ [“Viewing Object or Attribute History” on page 60](#)
- ♦ [“Comparing the History of an Object or Attribute” on page 62](#)

Using Time Machine to Review Snapshots

NOTE: Time Machine only displays data from existing snapshots. To take a snapshot, go to [Administration > Data Collection > Snapshot Service](#).

Audit, Compliance & Data Intelligence (ACDI) offers comprehensive details about every snapshot, including:

- ♦ Start and finish times of the snapshot
- ♦ Duration of the snapshot
- ♦ Total number of objects
- ♦ Average size of each object
- ♦ Average speed of objects (per second)
- ♦ Average index size

To review snapshots of an LDAP server at different time intervals, perform the following steps:

- 1 Navigate to the ACDI home page and click **Time Machine**.
- 2 Select the LDAP server that you want to audit. Available options include OpenText eDirectory and any LDAP server from another OpenText Identity Manager.

Ensure that eDirectory is selected in the **Select index source** list.

- 3 By default, the data is displayed for the **Last 7 days**. You can change the time range to display data over minutes, hours, days, weeks, months, or years. For more information, see [Setting the Time Filter](#).

The preview pane displays data snapshots organized in a timeline. The icon next to the **Select index source** list indicates the count of snapshots within the specified time range. For example,



indicates that there are 8 snapshots available for the last 7 days.

The snapshot usually appears in green. Green indicates no errors, whereas yellow indicates that the collected data contains errors.

- 4 (Optional) To learn more about the errors in a snapshot, click **Discover Errors**. You can also download the error logs for further analysis.
- 5 (Optional) To export the data to a CSV file format, click the **Download as CSV**  icon. You can use third-party software to process it later.

Setting the Time Filter

If you want to change the time for capturing snapshots, you can use one of the following options:

- ♦ On the Time Machine page, click the time clock or calendar  icon and select one of the time filter options:
 - ♦ **Quick select:** Choose a time based on the last or next number of seconds, minutes, hours, days, or another time unit.
 - ♦ **Commonly used:** Choose a common time range like Today, Last 7 days, or Last 30 days.
- ♦ To set start and end times, perform the following steps on the Time Machine page:
 1. Click **Show dates** and then click anywhere inside the toolbar to access the time filter window.
 2. Select **Absolute**, **Relative**, or **Now** and specify ranges.
 3. Click **Update** to apply changes.

Click the **Reload**  icon to reset the page and take new snapshots of the LDAP server.

Viewing Object or Attribute History

To view the history of an object or attribute, perform the following steps:

- 1 Go to the ACDI home page and select **Time Machine** to review snapshots of the LDAP server over a specified period, for example, the last 7 days. For more information, see [“Using Time Machine to Review Snapshots” on page 59](#).

- 2 Click **History Browser**.

The timeline created by the Time Machine appears horizontally at the top of the preview pane on the History Browser page.

- 3 In the Search object field, type the name of the object whose history you want to view. For example, to view the history of user CN=ssmith, type ssmith.

- 4 Select the user object (cn=ssmith, ou=user, o=system) from the search result. The attributes and values for this user are displayed in the right preview pane.

NOTE: By default, the LDAP connection to OpenText eDirectory is selected in the timeline. As a result, ACDI displays the current values for the selected object collected via the LDAP connection.

- 5 (Optional) To view the history of an attribute, type the name of the attribute in the **Search by attribute or value** field.
- 6 To track changes in an object or its attributes over time, select the audit events in the timeline and compare the results. For example, if ssmith is not able to log in to the application, you can check whether his login has been disabled by verifying the relevant audit events for changes in his logindisabled attribute over time.

Similarly, you can view and track changes between two snapshots.

NOTE: You can select only one event or snapshot at a time.

The following table lists the icons and description you can use to perform actions based on your requirements:

Icon	Description
	Click to view the current data of an object collected via the LDAP connection. Indicates an active LDAP connection to OpenText eDirectory or Active Directory.
	Indicates the snapshot of the LDAP server taken by the Time Machine for the selected time interval.
	Click to display audit events in the preview pane.
	Click to show or hide audit events in the timeline.
	Click and select Export to CSV or Export to LDIF to export the historical data in the CSV or LDIF file formats, respectively.
	Click to display the full DN of the selected entry. For example, RootDSE > cn=ssmith > ou=user > o=system You can use the icon to navigate back and forth through the tree.
	Click to minimize the search object toolbar.
	Click to maximize the search object toolbar.
	Click and select the Show Service Attributes option to get the attribute's data, including the modifier's name and other attributes that hidden by default.

Comparing the History of an Object or Attribute

You can use the Objects Compare tool to compare changes in an object or its attribute over time. You can enable or disable the compare tool in one of the following two ways:

- Click **Objects Compare** in the left navigation pane.
- Click the **Compare** toggle button at the top of the preview pane on the History Browser page.

To compare the history of an object or attribute, perform the following steps:

- 1 Go to the ACDI home page and select **Time Machine** to review snapshots of the LDAP server over a specified time. For example, the last 7 days. For more information, see [“Using Time Machine to Review Snapshots” on page 59](#).
- 2 Click **History Browser**.
The timeline created by the Time Machine appears in a horizontal format at the top of the preview pane on the History Browser page.
- 3 In the **Search object** field, specify the name of the object whose history you want to compare. For example, to compare a group CN=admin, specify admin.
- 4 Select the group object (cn=admin, ou=group, o=system) from the search result. The attributes and values for this group are displayed in the right preview pane.
Let us assume you want to check the changes in the group membership, which is the member attribute of the admin group over the period.
- 5 In the **Search by attribute or value** field, type member.
- 6 Select **Objects Compare** in the left navigation pane.

You can click the **Minimize to toolbar**  icon to minimize the search object toolbar. The preview pane displays the data divided into three columns. The first column shows the object or attribute selected for comparison. The other two columns show the values for different dates and times.

- 7 Select a date and time in the DateTime picker and Secondary DateTime picker to compare.
You can define which snapshot connection you want to use to compare or directly compare through LDAP.

- 8 To only view the changed values, click the **Options**  icon and select the Show only not equal option.

Let us assume that the member attribute of the user Valerius has changed. To find what values have changed for this user, disable the Compare toggle button. Click **Back** to the previous object. It will display the modified attributes of Valerius.

IV

Managing Audit, Compliance & Data Intelligence

This part contains the following chapters:

- ♦ [Chapter 10, “Working with Dashboard Editor,” on page 65](#)
- ♦ [Chapter 11, “Working with Report Editor,” on page 69](#)

10 Working with Dashboard Editor

Visualizing data is the most effective way to understand it. With ACDI's dashboard, you can easily transform your data into visual elements, known as panels, that help you focus on the most important information. These panels include charts, graphs, and maps, which you can use to compare data and identify patterns and relationships. The terms *panel* and *visualization* may be used interchangeably throughout this guide.

ACDI's **Dashboards** and **Dashboard Editor** are built on the OpenSearch Dashboards framework. OpenSearch Dashboards is an open-source visualization tool that is designed to work with OpenSearch.

In this chapter, you will learn how to create and manage dashboards with ACDI.

- ♦ [“Creating a New Dashboard” on page 65](#)
- ♦ [“Editing Dashboard” on page 68](#)
- ♦ [“Adding Custom Dashboards to the Dashboards Menu” on page 68](#)

Creating a New Dashboard

To create a new dashboard on ACDI, you need the following components:

- ♦ **Dataset:** The source of your data, which can be OpenText eDirectory (OpenText Identity Manager) or OpenText Access Manager. It is stored and analyzed by using OpenSearch.
- ♦ **Visualizations:** OpenSearch panels that help you translate datasets into an easy-to-process visual representation (dashboard).

While using ACDI, you can access datasets containing existing visualizations from OpenText Identity Manager and OpenText Access Manager. You can use these visualizations or create new ones for your dashboard.

- ♦ [“Creating a Dashboard with New Visualization” on page 65](#)
- ♦ [“Creating a Dashboard with an Existing Visualization” on page 67](#)

Creating a Dashboard with New Visualization

The **Dashboard** offers various types of visualization to help you analyze your data. Before creating a new visualization in ACDI, it is recommended to refer to the [OpenSearch documentation \(https://opensearch.org/docs/latest/dashboards/visualize/viz-index/\)](https://opensearch.org/docs/latest/dashboards/visualize/viz-index/) to know more about the different types available.

You can add custom visualization in ACDI in one of the following ways:

- ♦ [“Creating a New Visualization” on page 66](#)
- ♦ [“Modifying an Existing Visualization” on page 66](#)

When you create a visualization, ACDI provides you the option of adding it to a new dashboard. If you do not wish to add the visualization to the dashboard, ACDI saves it in the visualization library. You can access this library by selecting the **Add Panels** option while editing a dashboard.

Creating a New Visualization

- 1 On the ACDI Home page, click **Manage > Create Dashboard**.

By default, ACDI opens New Dashboard in edit mode. However, if you see the following message “This dashboard is empty. Let’s fill it up!,” then you need to click **Edit** in the menu bar.

- 2 Click **Create new**.
- 3 Select a visualization type from the New Visualization window, then select a source.
For example, select **Area > Audit Events (Saved Objects)**.

NOTE: You can retrieve data from OpenSearch using either Saved Objects or Index Patterns. All event data is stored in indices. The index patterns that start with `audit-default` belong to OpenText eDirectory. Saved Objects, on the other hand, are files that store data like dashboards, visualizations, and maps, for later use. For more information, see [OpenSearch Documentation \(https://opensearch.org/docs/latest/dashboards/management/management-index/\)](https://opensearch.org/docs/latest/dashboards/management/management-index/).

- 4 Click **Save** in the toolbar.
- 5 In the Save visualization window, specify a title and description for the visualization. For example, specify `Audit Events custom` as the title of the area chart panel.
- 6 (Optional) To add this visualization to the new dashboard, make sure **Add to Dashboard after saving** is enabled.
- 7 Click **Save and return**.
The `Audit Events custom` is now available in the Add panels window.
- 8 (Optional) Click **Save** if you selected to add the new visualization to the dashboard in [Step 6](#).

Modifying an Existing Visualization

*You can modify only cloned and custom dashboards that have the **Edit** option. You cannot modify OpenText Identity Manager's default dashboards.*

- 1 On the ACDI Home page, click **Dashboard**.
- 2 Click **Edit** on the desired dashboard (cloned or custom).
For example, click **Edit** on a cloned Audit Dashboard.
- 3 Under **Basic**, click **Visual Edit**.
- 4 On the **Editing Audit Dashboard Clone (unsaved)** tab, click the **Settings**  icon and select **Edit visualization** on the panel that you want to modify.
For example, use the Audit - Events area panel.
- 5 To view User changes in the panel:
 - 5a Click **Add filter**.
 - 5b Specify the following details:

Field	Select
Field	Object Class
Operator	is
Value	User

The search is case-sensitive. You can either use `Object Class` keyword or search by an `Object Class` attribute.

5c Click **Save**.

The Area panel now displays User changes only.

6 To save this visualization, click **Save as** in the toolbar.

7 In the Save visualization window, make sure **Save as new visualization** is enabled.

8 Specify a title and description for the visualization. For example, the title for the area chart panel is `Audit Events User Changes`.

9 (Optional) If you don't want to add this visualization to default dashboard, disable **Add to Dashboard after saving**.

10 Click **Save and return**.

The `Audit Events User Changes` is now available in the Add panels window.

Creating a Dashboard with an Existing Visualization

To create a dashboard and add an existing visualization:

1 On the ACDI Home page, click **Manage > Create Dashboard**.

By default, ACDI opens New Dashboard in edit mode. However, if you see the following message "This dashboard is empty. Let's fill it up!," then you need to click **Edit** in the tool bar.

2 Click the calendar icon and set the time filter to **Last 30 days**.

3 Click **Add an existing** or **Add**.

4 From the Add panels window, select the required panel and then click **X** to close the panel.

For example, to add the panel you created in [Creating a Dashboard with New Visualization](#) to the new dashboard canvas, select `Audit Events custom`.

This creates a dashboard with a single panel. You can continue to add more visualizations to this dashboard.

5 (Optional) You can change the layout of panels on a dashboard canvas. Click **Options** and enable the following options:

- ♦ **Use margins between panels**: Enabled by default. Toggle to disable the margin of space between each panel.
- ♦ **Show panel titles**: Enabled by default. Toggle to disable or hide the titles in the panel headers.

6 Click **Save**.

7 (Optional) To discard the changes you made to the dashboard, click **Cancel > Discard changes**. After confirming, you cannot undo this operation.

Editing Dashboard

While working on custom or cloned dashboards, you can edit the dashboard in the following levels based on your requirements:

- ♦ **Basic:** To customize basic dashboard attributes and its appearance, such as Dashboard ID, Display Name, and Description. You can also modify the tile color using the color picker and add an icon. The icon is an image with a resolution of 117 by 117 pixels, encoded in base64 format. You can define tags to help you search and group dashboards easily.
- ♦ **Advanced:** To add JSON script for changing the panel dimensions, Kibana Saved Object Metadata, Version, References, and time restore.
- ♦ **Visual Edit:** To edit visualizations using OpenSearch Dashboards. ACDI provides you access to various OpenSearch Dashboard features for editing, including a time filter, query languages for creating complex queries to filter data, dev tools, and more.

NOTE: You cannot edit a default dashboard. When you select a default dashboard template in **Manage > Dashboard Editor**, ACDI creates a clone and allows you to make basic edits to it. After saving the clone, advanced and visual editing options will be available for further customization.

Adding Custom Dashboards to the Dashboards Menu

Any newly created dashboard using the **Create Dashboard** option or cloned dashboard from the **Dashboard Editor** can be found on the Dashboards page. Additionally, ACDI allows you to create a sub-menu under the **Dashboards** menu and group custom dashboards with common tags under it for quick access.

Creating a Sub-menu under the Dashboards Menu

Tags can help you create sub-menus within the **Dashboards** main menu in the navigation pane. Navigate to **Administration > Audit Server > Dashboard Menu** and click **Add Menu item configuration** to create a sub-menu. Specify a tag (for example, custom) and a title for the sub-menu (for example, Custom Dashboard). For more information, see “[Dashboards Menu](#)” on page 39.

Adding Custom Dashboards under a Sub-menu

If you want to add custom dashboards under a sub-menu, use a common tag for both the sub-menu and the custom dashboard. Then ACDI will automatically group them into that sub-menu. For example, create a sub-menu titled Custom Dashboard with the tag custom. Then, go to the **Dashboard Editor** and include the same tag for your custom dashboard. The dashboard will then appear in the **Custom Dashboard** sub-menu automatically.

11 Working with Report Editor

Using Report Editor, you can perform the following actions: You can them or create new custom report definitions.

- ♦ Create and modify custom report definitions
- ♦ Clone and edit report templates

A template is a predefined report definition that you can run to generate and download reports in CSV, PDF, or XLSX formats.

Before you begin designing new reports, it is recommended that you familiarize yourself with:

- ♦ The concept of entities, filters, and result attributes. For more information, see [Understanding Report Editor Options](#).
- ♦ The report creation process: Modify an existing report template in the Report Editor. For more information, see [Creating Custom Report Definitions from Report Templates](#).

Understanding Report Editor Options

To open Report Editor, navigate to **Manage > Report Editor** and choose a report template from the **Search for Report Template** drop-down list. When you select a report, such as Users Report, Report Editor creates a clone of the selected report and assigns it a new **Report ID**, **Display Name**, and **Description**. You can modify these properties in the **Report properties** section. For more information, see [Report Properties](#).

- ♦ [“Report Graph” on page 69](#)
- ♦ [“Report Properties” on page 70](#)
- ♦ [“Entities” on page 71](#)
- ♦ [“Filters” on page 72](#)
- ♦ [“Result Table Attributes” on page 74](#)
- ♦ [“Postprocessing” on page 75](#)

Report Graph

A report graph is a visual representation of the connections among entities, filters, and result attributes in a report definition. In a report definition, there can be multiple entities, also known as secondary entities. The report graph also depicts relationships between secondary and primary entities, such as groups and their members, and user and their roles.

The report graph uses the following legends:

- ♦ **Yellow:** Represents an entity, secondary entities (if any), and connections between them.
- ♦ **Blue:** Represents filters and links to an entity.

- ♦ **Green:** Represents attributes shown in the result table. The attributes are linked to an entity, and the link is shown in green dashed lines.

Report Properties

Using this option, you can configure the data source (entities) that generates the report and display settings for a report card on the Reports page.

Table 11-1 Report properties and definition

Parameter	Description
Report ID	A report name or ID assigned by ACDI. You cannot modify this value. It is used while importing a report into OpenSearch.
Display Name	Specify a unique name to display on the report card.
Description	Specify a description for the report to display on the report card.
Icon	Provide a base64 encoded PNG icon to display on the report card.
Color	Specify a hex color code or use the color picker for your report card background.
Report version	Displays the ACDI reporting version. This is a read-only field.
Report Tags	Add tags to help organize reports with common tags into a custom Reports sub-menu. Tags are also useful for searching reports.
Main index name	Specify the name of the OpenSearch index alias used for fetching the data. This alias serves as the data source for the report definition you want to create. ACDI stores data in OpenSearch as indices grouped into special aliases. An alias starting with “workflow” (for example, workflow-default) contains events from the Workflow Monitoring package. Similarly, an alias starting with “report” (for example, report-default) contains data received from the snapshot services. The “default” suffix represents the LDAP connection to the data connector, the default data connector being OpenText eDirectory. For secondary data connectors such as Active Directory, the suffix is “-ad”.
Main entity name	Specify a root entity that connects objects from the same types of indices or different indices, such as OpenText eDirectory snapshots and event service. A report can include more than one entity. For example, the root entity for the Audit Users report is Audit, whereas the root entities for the Audit Objects report are audit, snapshot, and modifier. For information about creating an entity, refer to the Entities section.
Default sort attribute	Specify the attribute name used for sorting the data in the report result table. For example, the Group Membership Report result is sorted by the Group’s dn (Distinguished Name).
Sort order	Specify the order for sorting attributes by default: in ascending or descending order.
The amount of result records	Specify the maximum number of records (rows per page) to display in the report result.
Show flat result	Enable to display an expanded/flat view of the nested entities in the report result.

Parameter	Description
The default time shift	Specify the default value to display in the date picker when filtering a report. This field works in tandem with the default time metric. For example, when the default time shift is set to 7 and the default time metric is set to days, the date time range considered for filtering reports is the last 7 days.
The default time metrics	Specify the time metric to use with the default time shift field. The value includes seconds, minutes, days, weeks, months, and years.
Round date-time value	Enabled to round up the date-time value to a specific value.
The Slice load	Enable to load partial records while displaying report results on a page. Partial loading improves performance and prevents reporting system crashes, especially when reports include many secondary entities and attributes with long strings. Additionally, it is helpful when many post-processing functions are applied to the report.
The size of slice	Specify the number of records to fetch in one request. The maximum limit configurable is 100.
Limit of data to show on the front-end (Mb)	Specify the limit of the data displayed on the front end. ACDI stops loading the report result after the set limit is reached. This prevents the out-of-memory error in the browser. The maximum limit is 300.

Entities

When you create a report definition, you also create an entity with OpenSearch Index as its data source and, the query filter as a specific attribute used to retrieve data for the report.

A report can contain more than one entity. For example, the root entity for the Audit Users report is Audit, whereas the root entities for the Audit Objects report are audit, snapshot, and modifier. Filters and result table attributes are associated with each entity.

Table 11-2 *Entities and description*

Parameter	Description
Name of the entity	Specify a name for the entity.
Query to filter	Click the icon to specify the OpenSearch query for filtering entity data. For example, in the Users Report, the query <code>objectClass:inetOrgPerson</code> provides information about users from a snapshot.
The DateTime field	Specify the date and time of the snapshot or audit events used for the entity. For entities based on the snapshot services, select one of the following options: ◆ <code>initDateStamp</code>: The date and time when the snapshot was initiated. ◆ <code>DateStamp</code>: The date and time when the snapshot was taken. For entities based on audit events, select <code>audittime</code> or <code>eventtime</code> .

Parameter	Description
The Entity Index	Specify the OpenSearch index alias used for fetching the data. The Entity Index field is same as the Main index name defined in the Report Properties tab. Therefore, if you use the alias “main” for The Entity Index field, you automatically set the index alias specified in the Main index name .
Entity primary key	Specify an attribute name to use as the primary key for the entity. This value is used when defining relations between entities.
Mandatory Attribute	Click the plus icon and add an attribute name of the entity to retrieve from OpenSearch in Attribute . You can add multiple attributes.
Attribute	Specify an attribute name of the entity to retrieve from OpenSearch. You can add multiple attributes.
The relations	Click the plus icon and specify the following details.
Source attribute	To create a relation between two entities, specify which attribute of the source entity links to the destination entity. For example, between user and role, the role entity is linked to user entity via the <code>nrfassignedroles</code> attribute. The <code>nrfassignedroles</code> attribute shows direct role assignments.
The relationship type	♦ one: ♦ many: Select when the source entity has many values. For example, one user may have many roles.
The link query type	♦ term: ♦ regex:
The Source Attribute value transformation function	Select the post-processing function to parse the value you need.
Enable transformation	Enable this option if you want to apply post processing for The Source Attribute value transformation function you selected.
Link by exact datetime	Enable this option to link entities by exact date and time value in the result.
The Destination Entity Name	Select the destination entity you want the destination
Destination Attribute	
The relationship type	♦ one: ♦ many: Select when the source entity has many values. For example, one user may have many roles.

Filters

Filters are conditions that you apply to data when creating a report. For example, the Group Membership Report has predefined filters for the Group and Person entities. You can use these filters to narrow down the results and generate a report that includes only the relevant data you want in your report.

The following table lists the parameter you need to define for each filter.

Table 11-3 Filter parameters and description

Parameter	Description
Name of the Filter	Specify a display name for the filter. This value is displayed in the Report Graph and the Filters tab of the report.
ID of the Filter	Provide a unique ID for the filter. This value is displayed as the filter label in the list of filters in the Report Editor.
The entity name	Specify the entity to which the filter applies. For example, the Container filter applies to the Group entity in the Group Membership Report.
Data source name	Specify the source of the data. It is either <code>opensearch</code> or <code>predefined</code> . If you select <code>predefined</code> , you must define a JSON array in The JSON array for predefined filter values (text) field. The JSON array will serve as the source for the predefined data.
The Attribute Name filter based on	Specify the attribute name used for filtering. For example, a group filter is based on the group's CN. Filters based on date/time, such as Start Date, End Date, and Request Date in the Role Request Report are based on the <code>nr fStartDate</code> , <code>nr fEndDate</code> , and <code>nr fRequestDate</code> attributes respectively. This field is case-sensitive.
The Attribute field type	Specify the type of search used for filtering. This applies to attributes with string field types. The default value is <code>keyword</code> . When you select <code>keyword</code> , only exact, case-sensitive matches are allowed. Alternatively, the <code>field</code> option can be used for full-text search and allows partial matches.
The Sort Attribute	Specify the attribute name used for sorting the values in the filter window. For example, a group filter based on the CN attribute of a group will be sorted based on its CN attribute.
The Sort order	Based on The Sort Attribute , the Sort order determines whether the data is sorted in ascending or descending order by default.
Additional Attributes	Attribute used for postprocessing function. <TBD>
The Filter type	Choose the filter type from the following options: ♦ autocomplete_search: Displays matching options while the user types a keyword. ♦ date_time: Select this option for filter attributes that are based on date/time. For example, Start Date filter based on the <code>nr fStartDate</code> attribute. After selection, specify the values for the DateTime Format Pattern, Type of dateTime field, Direction of dateTime shift, and Default time shift from now (in days) fields.
Filter multiple selection	
Defines how the search keyword will be processed	Determines how the search keyword will be processed. To use regular expression to match the characters you type into the search field, select <code>regex</code> .
Case sensitive search	This option enables case sensitivity for the <code>autocomplete_search</code> filter type.

Parameter	Description
Delay to start autocomplete search (ms)	Specify the time after which the suggestion will be displayed to the user. The time between starting to type and performing a search. The value 0 indicates the field is disabled.
Collapse result	Collapse search results based on field values.
Filter-out all identical values	Enable this option to show only unique values.
Filter-out all empty values	Enable this option for the filter to display only values with data.
Filter-out all values which have no Entity mandatory Attributes	Enable this option for the filter to display only records for entity with mandatory attributes.
The Multiple values query logic	The query logic to apply for multiple values.
Size of records to fetch	Specify how many records will be requested to fill the filter.
The Postprocess function name	Select the post-processing function name that the filter will use.
Enable/Disable filter postprocess	Enables or disables postprocessing on the filter.
The DateTime Format Pattern	Specify the date and time pattern to display in the report result. For example, you can use the pattern yyyyMMDDHHmmss[Z].
Type of dateTime field	Specifies whether the dateTime field is a date or date_string.
Direction of dateTime shift	Depending on the value selected for the Default time shift from now (in days) field, specify whether it applies to the last or next date/time. For example, if the Default time shift from now (in days) field is set to 30 days, then next implies the next 30 days whereas last implies the last 30 days.
Default time shift from now (in days)	Specify the number of days that will apply to the date-time based filter by default.
The JSON array for predefined filter values (text)	If you select “predefined” in the Data source name field, you must define a JSON array that will serve as the source for the predefined data.

Result Table Attributes

The attributes listed in the **Result Table Attributes** are displayed in the report results when you run a report. You can add or remove attributes, customize their display, and apply JavaScript functions for post-processing.

Table 11-4 Result table attributes and description

Parameter	Description
Name of the Attribute	Specify the attribute name used to retrieve the data.

Parameter	Description
The Entity Name	Specify the entity to which the attribute belongs.
Alias name for the attribute	Provide a label for the attribute to be displayed in the report result.
Use attribute for entity object	If you want to add a secondary entity to your report definition, enable this option and assign the attribute to this entity in the report. To obtain additional attributes for the secondary entity, you must create more attributes with this option disabled.
Data source name	Specifies the source of your data, which is opensearch by default.
Hide from the result	Enable this option to hide the attribute value from the result table. This is also used in post-processing, if the value of this attribute is required for calculations and displaying the result.
Postprocess Function name	Select the post-processing function that you want to apply to the attribute.
Enable/Disable postprocess	Enable this option if want to apply post-processing function to the attribute.
Pass full record object to the postprocess function	Enable this option to pass full record object as a function argument to the post-process function.
Field width	Specify the width of the attribute column in the report result.
Achieve left side fixed columns by setting fixed property	Enable this option if you want the attribute to be displayed in a fixed-width column on the left side of the report result.

Postprocessing

The Post-processing functions are written in JavaScript. Postprocessing allows you to include JavaScript functions that apply to filter values or data in the final report. You can also change attribute values in CSV format to meaningful descriptions.

Let us explore some post-processing scenarios using the Users Login Expire report. This report uses OpenText eDirectory snapshots to display user login expiration times based on the loginexpirationtime attribute of users. You can enhance the report by applying post-processing functions to display additional meaningful data, such as the number of days until login expiration or whether the login has already expired.

To understand post-processing functions, perform the following steps:

- 1 On the ACDI's Home page, click **Manage > Report Editor**.
- 2 Select **Users Login Expire report** from the **Search for Report Template** drop-down list.
The ACDI Report Editor creates a clone of the selected report and assign it a new Report ID, Display Name, and Description.
- 3 Click **Save As** and specify a new **Template Name** for this custom report. For example, Custom Users Login Expire report.
- 4 Click **Postprocessing**.

- 5 Click **Function [1] formatDateString** to add a separator between the years, months, days, hours, and minutes.
- 6 To apply this function to the **Login Expiration Time** column in the final report, perform the following steps:
 - 6a Click **Result Table Attributes > Attribute (loginExpirationTime)**.
 - 6b Enable the **Enable/Disable postprocess** option.
 - 6c Set the **Postprocess Function name** to `formatDateString`.
 - 6d Click the  **Save** icon.

Creating a New Custom Report Definition

Using the Users Report as an example, let us understand how this report definition has been created.

The Users Report definition is based on OpenText eDirectory snapshots from the ACDI Snapshot Service, which are stored in OpenSearch. The report relies on the `report-default` index in OpenSearch to retrieve the required user data. The report definition includes predefined values for entities, filters, and result table attributes to display in the report result.

To create this report definition, perform the following steps:

- 1 On the ACDI's Home page, click **Manage > Create New Report**.
- 2 To add a root entity to the report, click **Entities** and perform the following steps:
 - 2a Click  (**Add Entity configuration**).
 - 2b In the **Entity [0]** tab,
 - 2b1 Click **Query to filter** icon and enter `objectClass:inetOrgPerson`. OpenSearch uses this query to filter the user data.
 - 2b2 Set the **Name of the entity** to `snapshot`, **The DateTime filter** to `initDateStamp`, and **Entity primary key** to `dn`.
 - 2b3 To add mandatory attributes, click  (**Add Attribute configuration**) and enter the **Attribute** name. For example, enter `dn` to retrieve the Distinguished Name of the user entity from OpenSearch.
 - 2b4 Specify values for other fields as desired. For more information about the parameters, see [Table 11-2 on page 71](#).
 - 2c (Conditional) If you want to add secondary entities, click  **Add Entity configuration** icon and repeat [Step 2a](#) to [Step 2b4](#).
- 3 Click the **Report properties** tab,
 - 3a Specify values for display parameters such as **Display Name**, **Description**, and **Color** that will display on the report card.
ACDI automatically assigns a unique **Report ID** to each report.
 - 3b Set **The Main index name** to `report-default` and **The Main Entity name** to `snapshot`. This serves as the data source for the report definition you want to create.

NOTE: The **Main Entity name** field displays a list of entities created via **Entities** for selection. Make sure you first create the required entity.

- 3c Specify values for other fields as desired. For more information about the parameters. see [Table 11-1 on page 70](#).
- 4 To add filters, click **Filters** and then add one filter at a time. For example, perform the following steps to add the “Container” filter:
 - 4a Click  (**Add Filter configuration**)
 - 4b Set the **Name of the filter** to Container.
 - 4c Set **ID of the filter**, **The Attribute Name filter based on**, and **Sort Attribute** to parent.
 - 4d Select the **Data source** to be opensearch and the **Entity filter belong to** as snapshot.
 - 4e Specify values for other fields as desired. For more information about the parameters. see [Table 11-3 on page 73](#).
 - 4f (Optional) You can include more filters in your report definition. To add more filters, repeat steps 4a to 4e.
- 5 To add an attribute or column that is displayed in the report result table, click **Result Table Attributes**. For example, perform the following steps to add the “Snapshot time” column:
 - 5a Click  (**Add Attribute configuration**).
 - 5b In the **Attribute [0]** tab,
 - 5b1 Specify the **Name of the attribute** as datestamp and **Alias name for the attribute** as Snapshot time.
 - 5b2 Specify values for other fields as desired. For more information about the parameters. see [Table 11-4 on page 74](#).
- 6 Click the  **Save** icon.

The **Save** icon remains disabled until all fields have been validated without errors. You can click on the  **Validator** icon to display a list of existing errors in your report definition.

Creating Custom Report Definitions from Report Templates

A custom report definition generates a custom report. You can generate custom reports by cloning and customizing an existing template in the Report Editor.

For example, you can start with the Users Report template if you want to generate a custom report that displays information about two different entities linked by an attribute (for example, roles and users). “User” is the primary entity in the Users Report. You can clone and customize this report to include a secondary entity, such as “Role”, and display data on all roles that have been assigned to a user.

To create this custom report definition, perform the following steps:

- 1 On the ACDI’s Home page, click **Manage > Report Editor**.
- 2 Select **Users Report** from the **Search for Report Template** drop-down list.

The ACDI Report Editor creates a clone of the selected report and assign it a new Report ID, Display Name, and Description.

- 3 Click **Save As** and specify a new **Template Name** for this custom report. For example, Custom User Role Report.
- 4 In the **Report properties** tab,
 - 4a (Optional) Click the  **Add Tag configuration** icon to add tags like custom to your report. Tags enables you to organize similar types of reports into a custom Reports sub-menu.
 - 4b You can keep the existing values from the original report template or modify them as required. For more information about the parameters. see [Table 11-1 on page 70](#).
- 5 To add the secondary entity “role” to this report,
 - 5a Click **Entities**.
 The **Entity [0]** tab displays information about the root entity snapshot from the original template. The **Query to filter** `objectClass:inetOrgPerson` specifies that this entity displays information about users from the OpenText eDirectory snapshot.
 - 5b Click the  **Duplicate** icon to copy **Entity [0]**. Now perform the following steps to customize the **Entity [1]** properties:
 - 5b1 Set the **Name of the entity** to `role`.
 - 5b2 Click **Query to filter** icon and enter `objectClass:nrfRole`. OpenSearch uses this query to filter the roles of users.
 - 5b3 You can keep the existing values of **The DateTime filter**, **The Entity Index**, and **Entity primary key**.
 - 5b4 Specify values for other fields as desired. For more information about the parameters. see [Table 11-2 on page 71](#).
 - 5c Now to create a link, you must first determine a common attribute between the snapshot (user) and role entities. For the snapshot (user) entity, `nrfmemberOf` is an attribute that contains DN of roles assigned to a user, including those assigned via nested child role assignment. So, for the role entity, the `nrfmemberOf` attribute acts as the source entity and the DN as the source attribute.
 Perform the following steps to create a relationship between the two entities:
 - 5c1 In **Entity [0] (snapshot)**,
 - 5c1a Click the  **Add Relation configuration** icon.
 - 5c1b Set the **Source Attribute** to `nrfmemberOf`, **the Relationship type** to many, and **The link query type** to term.
 - 5c1c Click **The Destination Entity** and select **The Destination Entity Name** as `role`, **Destination Attribute** as `dn`, and **The relationship type** as one.
 - 5c2 In **Entity [1] (role)**,
 - 5c2a Click the  **Add Relation configuration** icon.
 - 5c2b Set the **Source Attribute** to `dn`, **the Relationship type** to one, and **The link query type** as Term.
 - 5c2c Click **The Destination Entity** and select **The Destination Entity Name** as snapshot, **Destination Attribute** as `nrfmemberOf`, and **The relationship type** as many.
 - 5d Click .

- 6 To add filters for the role entity, click **Filters** and then add one filter at a time. For example, if you want to filter roles by CN in the report result table:
- 6a Click  (Add Filter configuration)
 - 6b Set the **Name of the filter** to Role CN.
 - 6c Set **ID of the filter**, **The Attribute Name filter based on**, and **Sort Attribute** to cn.
 - 6d Select the **Data source** to be opensearch and the **Entity filter belong to** as role.
 - 6e Specify values for other fields as desired. For more information about the parameters. see [Table 11-3 on page 73](#).
 - 6f (Optional) You can include more filters in your report definition. To add more filters, repeat [Step 6a](#) to [Step 6e](#).
- 7 To add an attribute or column for the role entity, click **Result Table Attributes**. For example, to add a “Role info” column that displays role CN, name and description, perform the following steps:
- 7a Click  (Add Attribute configuration).
 - 7b To create a field for the role entity,
 - 7b1 Select the **Entity name** as role and enable the **Use attribute for entity object** option.
 - 7b2 Go to the **Attribute** tab, specify the **Alias name for the attribute** as Role info and **Name of the attribute** as entity_role.
 - 7b3 Specify values for other fields as desired. For more information about the parameters. see [Table 11-4 on page 74](#).
 - 7c To add role CN to the “Role Info” column,
 - 7c1 Click  (Add Attribute configuration).
 - 7c2 Select the **Entity name** as role and disable the **Use attribute for entity object** option.
 - 7c3 Go to the **Attribute** tab, specify the **Alias name for the attribute** as Role CN and **Name of the attribute** as cn.
 - 7c4 Specify values for other fields as desired. For more information about the parameters. see [Table 11-4 on page 74](#).
 - 7c5 To add the role CN, name and description to Role Info attribute,
 - 7d Repeat [Step 7c1](#) to [Step 7c5](#) to add role name and description to the “Role Info” column.
- 8 Click the  **Save** icon.
- The **Save** icon remains disabled until all fields have been validated without errors. You can click on the  **Validator** icon to display a list of existing errors in your report definition.

