

# Queries

- [Introduction](#)
  - [View Query Details](#)
  - [Creating a Query Entry](#)
- [Database Schema](#)
- [API / Web Access](#)
- [Default Items](#)

## Introduction

Open-AuditIT comes with many queries inbuilt. If you require a specific query and none of the pre-packaged queries fit your needs, it's quite easy to create a new one and load it into Open-AuditIT for running.

Join Mark Henry as he discusses how to create your own custom queries.

## View Query Details

Go to menu: Manage -> Queries -> List Queries.

The screenshot shows the Open-AuditIT Enterprise 3.3.0 web interface. The top navigation bar includes 'View', 'Discover', 'Report', and 'Manage' menus. The 'Manage' menu is open, showing a list of options: Applications, Attributes, Baselines, Clusters, Connections, Dashboards, Devices, Fields, Groups, Integrations, Licenses, Locations, Maps, Networks, Orgs, **Queries**, Racks, Roles, Rules, Summaries, Users, and Widgets. The 'Queries' option is highlighted with a red box, and a sub-menu is visible with options: **List Queries** (highlighted with a green box), Create Queries, and Import Queries from CSV. The main content area displays a table of queries with columns: Execute, Details, Name, Description, Organisation, Display, Category, and Delete. The table lists various queries such as 'Acrobat', 'AD Controllers', 'Antivirus', 'Audit Dates', 'Billing Report', 'Cloud Device Details', 'Consumed IP Addresses', 'Database', 'Device', and 'Devices Without Credentials'.

Execute	Details	Name	Description	Organisation	Display	Category	Delete
		Acrobat	Adobe Acrobat	Default Organisation	y	Software	
		AD Controllers	Active Directory	Default Organisation	y	Server	
		Antivirus	Installed AntiVirus	Default Organisation	y	Software	
		Audit Dates	The first and last audit dates.	Default Organisation	y	Device	
		Billing Report	Name, last seen on and by for those devices only discovered by Nmap and have therefore not been audited.	Default Organisation	y	Device	
		Cloud Device Details	Details about cloud devices.	Default Organisation	y	Device	
		Consumed IP Addresses	The ip addresses consumed by the devices.	Default Organisation	y	Network	
		Database	All databases.	Default Organisation	y	Server	
		Device	Icon, name, ip address, manufacturer, model, serial.	Default Organisation	y	Hardware	
		Devices Without Credentials	Device details - name, ip, last seen on and by for those devices only discovered by Nmap and have therefore not been audited.	Default Organisation	y	Device	

You will see a list of queries. You can view the details of a query by clicking on the blue view button.

Open-Audit Enterprise 3.3.0 View Discover Report Manage Admin Help Modules Licenses User: admin

Home / Queries Dashboards

Queries

50 records per page Search:

Execute	Details	Name	Description	Organisation	Display	Category	Delete
		Acrobat	Adobe Acrobat installations (software name contains 'acrobat' or 'adobe reader').	Default Organisation	y	Software	
		AD Controllers	Active Directory Domain Controllers	Default Organisation	y	Server	
		Antivirus	Installed AntiVirus software (software name contains 'virus' or 'trend micro' or 'endpoint').	Default Organisation	y	Software	
		Audit Dates	The first and last times a device was audited.	Default Organisation	y	Device	
		Billing Report	Name, last seen on and by, type, class, manufacturer, model, serial, user, location.	Default Organisation	y	Device	
		Cloud Device Details	Details about your cloud based devices	Default Organisation	y	Device	
		Consumed IP Addresses	The ip addresses used by a group.	Default Organisation	y	Network	
		Database	All databases.	Default Organisation	y	Server	
		Device	Icon, name, ip address, manufacturer, model, serial.	Default Organisation	y	Hardware	
		Devices Without Credentials	Device details - name, ip, last seen on and by for those devices only discovered by Nmap and have therefore not been audited.	Default Organisation	y	Device	
		Disk Partition Use	Partition details where partition free and used space aren't 0 and type isn't Volume or Network Drive and mount point isn't [SWAP].	Default	y	Device	

You can execute a query by clicking the green Execute button, the results will be displayed immediately.

Open-Audit Enterprise 3.3.0 View Discover Report Manage Admin Help Modules Licenses User: admin

Home / Queries Dashboards

Queries

50 records per page Search:

Execute	Details	Name	Description	Organisation	Display	Category	Delete
		Acrobat	Adobe Acrobat installations (software name contains 'acrobat' or 'adobe reader').	Default Organisation	y	Software	
		AD Controllers	Active Directory Domain Controllers	Default Organisation	y	Server	
		Antivirus	Installed AntiVirus software (software name contains 'virus' or 'trend micro' or 'endpoint').	Default Organisation	y	Software	
		Audit Dates	The first and last times a device was audited.	Default Organisation	y	Device	
		Billing Report	Name, last seen on and by, type, class, manufacturer, model, serial, user, location.	Default Organisation	y	Device	
		Cloud Device Details	Details about your cloud based devices	Default Organisation	y	Device	
		Consumed IP Addresses	The ip addresses used by a group.	Default Organisation	y	Network	
		Database	All databases.	Default Organisation	y	Server	
		Device	Icon, name, ip address, manufacturer, model, serial.	Default Organisation	y	Hardware	
		Devices Without Credentials	Device details - name, ip, last seen on and by for those devices only discovered by Nmap and have therefore not been audited.	Default Organisation	y	Device	
		Disk Partition Use	Partition details where partition free and used space aren't 0 and type isn't Volume or Network Drive and mount point isn't [SWAP].	Default	y	Device	

You can also edit or delete any query. You delete the query by clicking the red trash can icon under the delete column as displayed in previous screen shots.

## Creating a Query Entry

A query can be created using the web interface if a user has a role that contains the queries::create permission. Go to menu: Manage -> Queries -> Create Queries. There is also a "+" button on the List Queries page.

Open-Audit Enterprise 3.3.0 View Discover Report Manage Admin Help Modules Licenses User: admin

Home / Queries

Queries

50 records per page

Execute Details Name Description

		Acrobat	Adobe Acrobat
		AD Controllers	Active Directory
		Antivirus	Installed AntiVirus
		Audit Dates	The first and last
		Billing Report	Name, last seen
		Cloud Device Details	Details about
		Consumed IP Addresses	The ip addresses
		Database	All databases.
		Device	Icon, name, ip address, manufacturer, model, serial.
		Devices Without Credentials	Device details - name, ip, last seen on and by for those devices only discovered by Nmap and have therefore not been audited.

Applications  
Attributes  
Baselines  
Clusters  
Connections  
Dashboards  
Devices  
Fields  
Groups  
Integrations  
Licenses  
Locations  
Maps  
Networks  
Orgs  
**Queries**  
Racks  
Roles  
Rules  
Summaries  
Users  
Widgets

List Queries  
Create Queries  
Import Queries from CSV

Search:

Organisation	Display	Category	Delete
Default Organisation	y	Software	
Default Organisation	y	Server	
Default Organisation	y	Software	
Default Organisation	y	Device	
Default Organisation	y	Device	
Default Organisation	y	Device	
Default Organisation	y	Network	
Default Organisation	y	Server	
Default Organisation	y	Hardware	
Default Organisation	y	Device	

Details for creating custom queries can be found [HERE: Creating a Query](#), If you need to create a Query that includes a custom Field you should look [HERE: Create a Query containing Custom Fields](#)

## Database Schema

The database schema can be found in the application if the user has database::read permission by going to menu: Admin -> Database -> List Tables, then clicking on the details button for the table.

## API / Web Access

You can access the collection using the normal Open-Audit JSON based API. Just like any other collection. Please see [The Open-Audit API](#) documentation for further details.

## Default Items

Shipped are a set of default items. These can be found by going to menu: Help Defaults Queries.