What is Open-AudIT

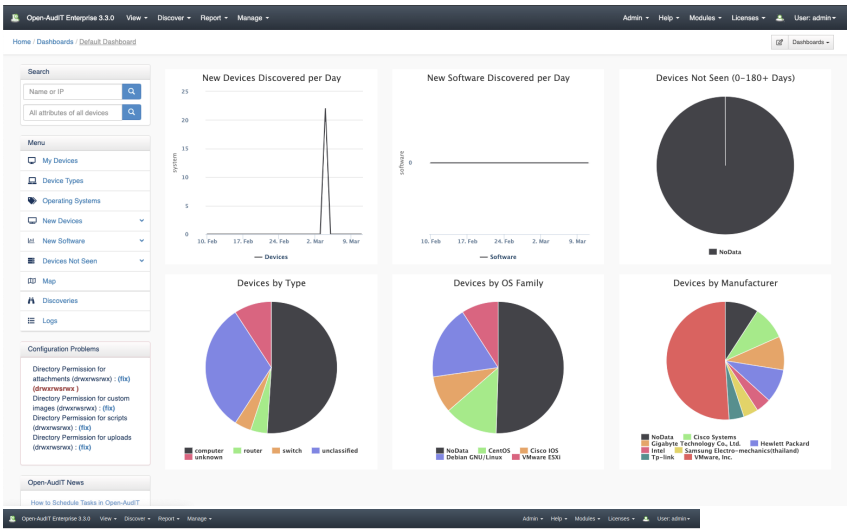


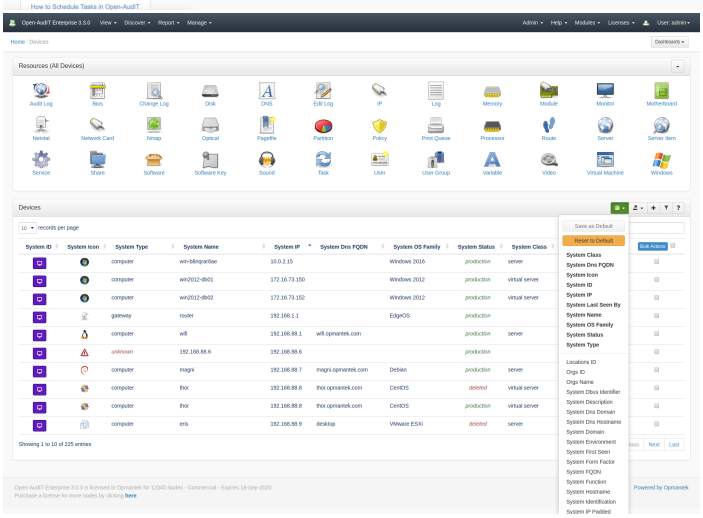
What is Open-AudIT?

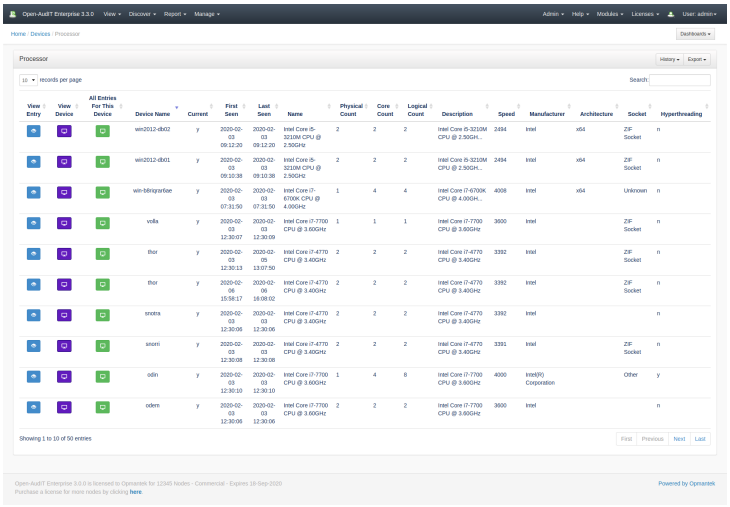
Open-AudIT is a discovery, audit and asset tracking and reporting system.

What does Open-AudIT do?

Open-AudIT tells you exactly what is on your network, how it is configured and when it changes. Open-AudIT is designed to be run on a server (Windows or Linux) and to scan your networks for devices. Once a device is found, Open-AudIT runs a series of commands upon it and stores the resulting data in a database. This data is then available for various reporting purposes. Open-AudIT comes with a list of over 50 reports with any number of additional reports able to be created by the user.







But Why?

Why would you want to go to the trouble ("trouble", hah, see the video about downloading, installing and discovering in under 10 minutes here) of keeping track of every device and it's configuration? Well, here are some contrived examples…

Would you know if someone installed a bitcoin miner program on their desktop PC and left it running every night? With Open-AudIT, you would not only be alerted when this new software was found, but you would also know which user account installed it and exactly when.

What about if someone bought their laptop into the office and plugged in – would you know? That laptop could be a security nightmare and now it's sitting on your network. Open-AudIT will see this new device and the "New Devices found int he last 7 days" report will show you. The Dashboard in Professional and Enterprise will also populate its graph. You will know. Your network will be safer.

And then there's software licensing – that's a given. Naturally Open-AudIT can report on exactly what software packages are installed. It's simple and easy to see if you have bought the required number of licenses.

Features?

As a result of Open-AudIT storing the data about a device, it also recognizes and stores and changes affected upon a device. If software was added or removed (for example) Open-AudIT stores this and can report upon it. This is taken even further by the concept of a Baseline, which exists in Open-AudIT Enterprise. Baselines enable you to compare one device against another and report the differences.

Open-AudIT has an extensive role-based access control mechanism which allows administrator-level users to define the access rights of other application users. If you have multiple departments in your company and would like John from Finance to be able to view all assets, but not be able to change them (for example), this is simply and easily achievable. Open-AudIT can also leverage Active Directory and OpenLDAP for authentication and authorization.

In addition to the standard array of attributes retrieved, Open-AudIT can also be configured to retrieve and store the details of files and/or entire directories of files.

As a benefit of being open source, users can add specific attributes for retrieval to the audit scripts. Opmantek are always open to including more attributes – all you need to do is ask! There is also the feature to be able to define "custom fields" which users can populate manually. If you need to store some piece of information about a device, Open-AudIT likely already does so, but if not, can be made to do so in a few mouse clicks.

Once you have the data, you can use the Restful JSON API to export it – or CSV, XML, HTML – whatever you like, because it's your data. The API supports the standard create, read, update and delete functions on all endpoints.

When Open-AudIT scans a network, it is called a "Discovery". Discoveries can be scheduled and hence automated. Set and forget. Along with automating discoveries, you can automate reports to be run and emailed to you on whatever schedule you choose. Why not send yourself a report containing all new devices found on your network in the last 7 days? This can be done in just a few mouse clicks.

The feature list is extensive and enables tracking of all IT assets, whether they be on your network or not. Need to record the details of a phone given to a user – not an issue. Open-AudIT can do that. What about the PC that's not physically connected to the network – Open-AudIT still has the ability to audit the machine and store the details. From their location, to how they're configured, to who is is in the Administrators group, to when a piece of software was installed, to ensuring file changes (/etc/htpasswd ?) are recorded. Open-AudIT can tell you exactly WHAT is on your network, HOW it is configured and WHEN it changes. Easily. Automatically. Simple.

How does it work?

Open-AudIT works best when you supply a list of credentials that it then uses to query devices. Open-AudIT makes use of Nmap to scan a network and report any responding devices. These devices are then queried to determine their attributes. Even if you don't have the credentials for a device on your network, Open-AudIT will still have a record of it thanks to Nmap. If a device is found, working credentials determined and it is a 'computer', an "audit script" is copied to the device and run. The script gathers extensive information and sends it back to the Open-AudIT server. If the device is a switch, router, printer, etc and it has SNMP enabled and Open-AudIT has working credentials, it's attributes will be queried using SNMP and no audit scripts will be used.

Once the data is in Open-AudIT, it is yours to query at will. The database structure is open and documented with examples to get you started (if one of the built-in 50 reports don't do just what you need).

How is it built?

Open-Audit Community is built using free and cross-platform tools such as PHP, MySQL, and Apache. In addition, Open-AudIT uses VBscript and Bash for its audit scripts. Both Professional and Enterprise use the Community API with further features enabled by the license. Both Professional and Enterprise are commercial compiled binary code with support offered to users by Opmantek. Accessing Community is via /open-audit/index.php and Professional / Enterprise via /omk/open-audit on your webserver.

Licensing

Open-AudIT started as a free software project. To this day it remains so. In recent years Opmantek Software has become the owners of the code-base and monetize this by creating add-ons in the form of Open-AudIT Professional, Open-AudIT Enterprise, Open-AudIT Collector and Open-AudIT Cloud.

The original Open-AudIT is referred to as Open-AudIT Community. Open-AudIT Community is the "engine" of Professional and Enterprise. It is Afferro GPL licensed and will always remain free software.

Open-AudIT Professional, Enterprise, Collector and Cloud are commercial closed source programs, licensed by Opmantek to customers and users. Opmantek supply a free 20 device license to users. Professional, Enterprise, Collector and Cloud build upon the foundation of Community and offer extra features and benefits. These can be seen in the table below.

Installing

Opmantek supply Open-AudIT as a packaged binary. Windows users will also need to (separately) install Nmap. Windows installs include a full WAMP stack, where-as the Linux package uses the native package manager to install these dependencies.

Using

If you have no interest in Professional, Enterprise, Collector or Cloud and the benefits they offer over and above Community, you can simply click the "Do not show me again" button when running Community and you will never be prompted about these options again. Opmantek uses the commercial programs to support development of the open source application.

Publicly Available Code

The source code for Open-AudIT is available on Github and is AGPL licensed. This code does **not** include the installer so users will need to take care of installing the dependencies and configuring the required services themselves. This source code does not include any Open-AudIT Professional, Enterprise, Collector or Cloud code as these are commercial closed source applications.

You can find the code at https://github.com/Opmantek/open-audit

	Community	Professional	Enterprise	Feature
Auditing	y	y	y	Detailed attribute retrieval.
Change Detection	Y	Y	Y	Record and report on any changes in device attributes.
Custom Attribute Values	Y	Y	Y	Set custom values for status, etc.
Custom Fields	Y	Y	Y	Create complete custom attributes and / or values.
Data Export	Y	Y	Y	CSV, XML, JSON export.
Database Server Discovery	Y	Y	Y	SQL Server and MySQL.
Device Management	Y	Y	Y	Manage who has the device, where it is, warranty, etc.
Discovery	Y	Y	Y	Find devices on your network.
File Share Discovery	Y	Y	Y	SMB Shares.
Software License Reporting	Y	Y	Y	What software is deployed and how many licenses do you have.
Web Server Discovery	Y	Y	Y	Apache and IIS.
Commercial Support		Y	Y	Unbeatable support!
Clusters		Y	Y	Define a Cluster of machines. Reports show CPU allocated, memory consumed, etc.
Discovery Scan Options		Y	Y	Select per discovery a group of supplied scanning options.
Enhanced Reports		Y	Y	Report scheduling, Multi-Reports, etc.
Geographical Maps		Y	Y	What locations contain which devices?
Interactive Dashboard		Y	Y	Easily visible and consumable charts and graphs.
JSON API		Y	Y	A fully documented JSON Restful API for your use.
Reporting Over Time		Y	Y	Reports with a date range.
Scheduling		Y	Y	Schedule Baselines, Discoveries, Reports, and Queries.

Applications			Y	Define a group of machines that provide an Application.
Baselines			Y	Compare devices to a baseline of attributes.
Clouds			Y	Audit your Amazon, Google and Azure cloud devices.
Collectors			Y	Use one Server to control discovery running on another server.
Dashboard Widgets			Y	Make your own graphical widgets to display on your own custom Dashboards.
Discovery Scan Options			Y	Completely customize each discovery beyond the provided defaults. Make your own custom discovery scan options for use by multiple discoveries.
File Change Detection			Y	Detect if a file has been changed in any way.
CMDB Integration			Y	Using the JSON API.
Rack Visualization			Y	Assign devices to a rack and visualize including space use reports.
Role Based Access Control			Y	Create and modify Roles to suit your specific requirements (including Active Directory and LDAP).