Open-AudIT Enterprise - Configuration Guide

Introduction

Open-AudIT Enterprise brings three additional features to leverage your Open-AudIT installation - Dashboard, Maps and Scheduled Reports.

Config File

Most Open-AudIT Enterprise options can be configured in the web GUI, but a few are only in the config file. You can find the config file at (Linux) /usr/local/omk/conf/opCommon.nmis and (Windows) c:\omk\conf\opCommon.nmis. It is a text file so any reasonable text editor can be used to edit it.

Username and Password

You can change the credentials for the Open-AudIT Enterprise user in the config file by editing the oae_username and oae_password fields. You will have to make corresponding changes in the Open-AudIT Community GUI for this user (menu -> Manage -> Users -> List Users).

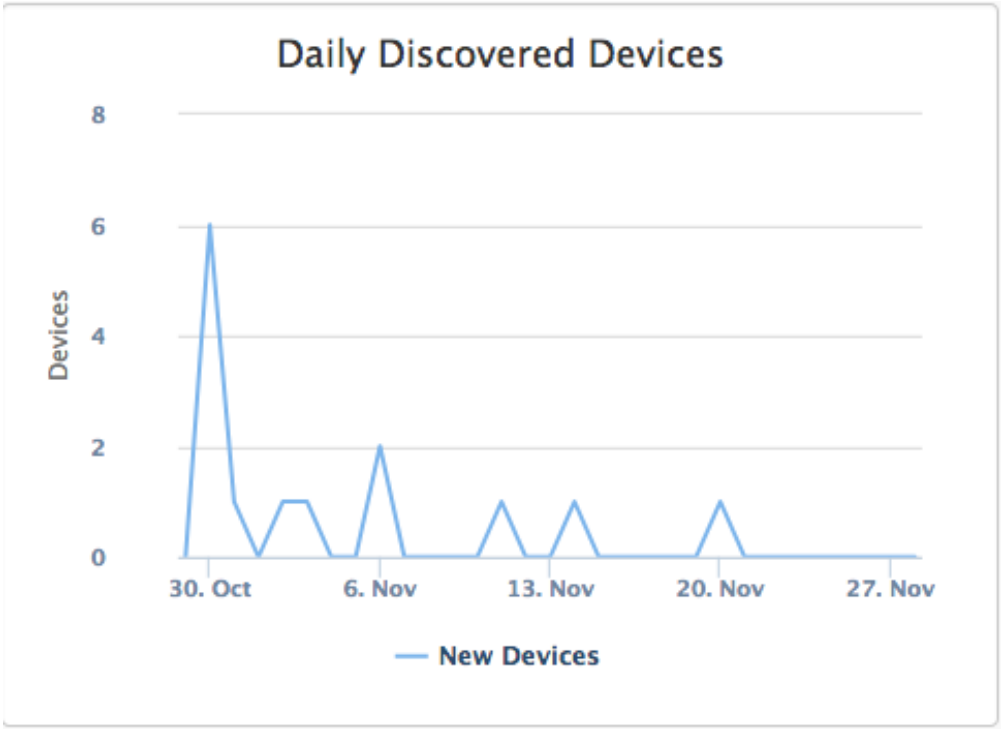
Authorisation

In the config file is a section named authentication. You can verify users logging into Open-AudIT Enterprise using their Open-AudIT Community credentials if you set auth_method_1 to openaudit in this section. You can have up to three methods of authentication. openaudit then htaccess are the defaults.

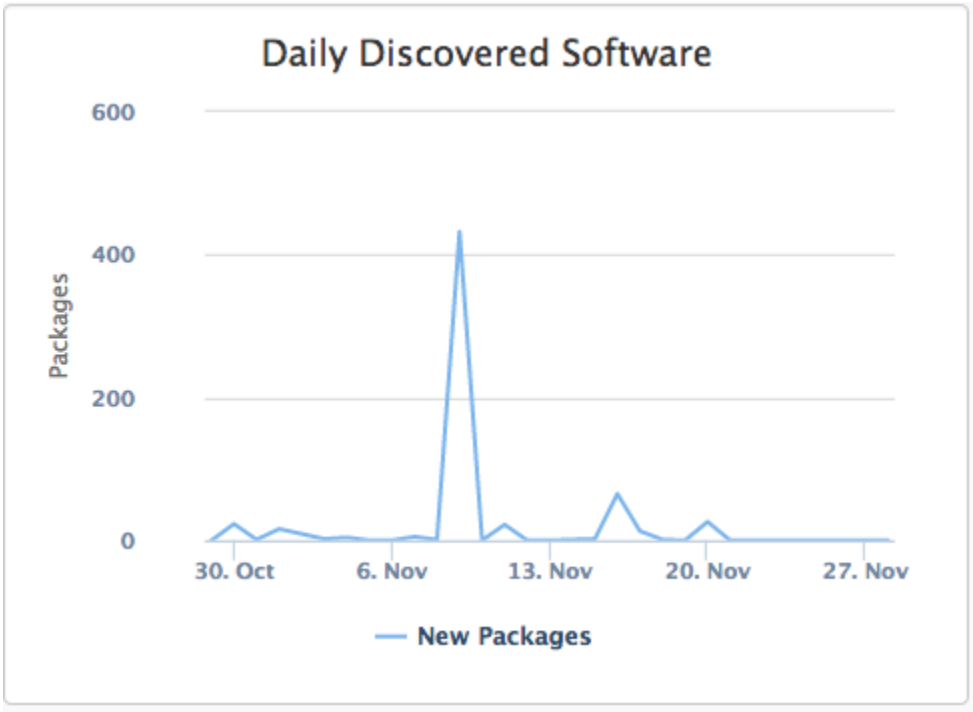
Dashboard

The Dashboard gives a quick overview of important items in the Open-AudIT database. There are (initially) four distinct graphs:

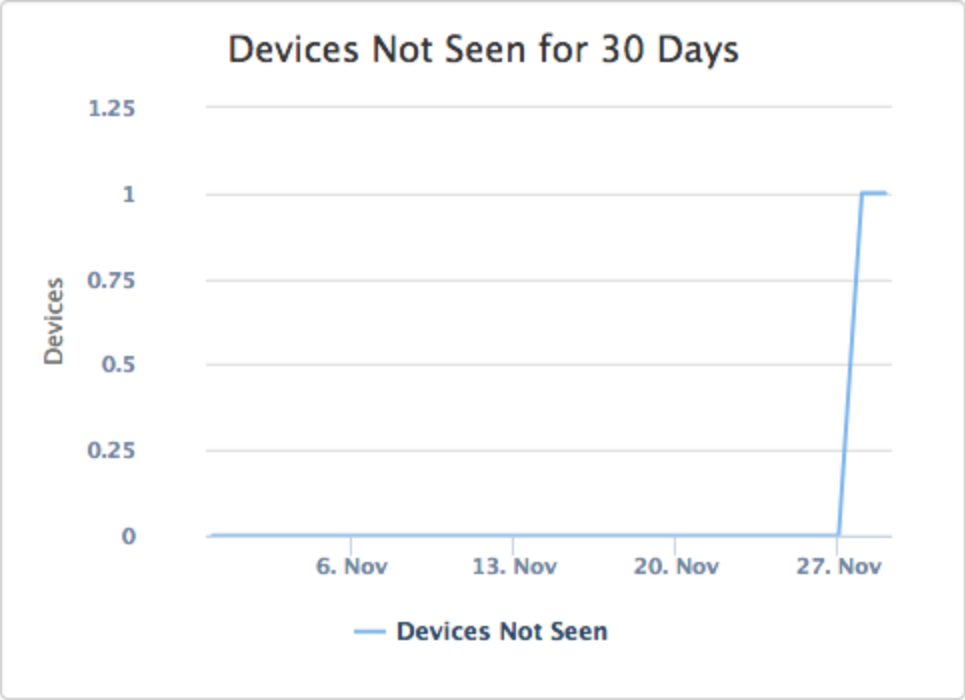
Devices Discovered over the last 30 Days. This graph should show a relatively consistent line. Any spikes in the graph represent new devices being discovered and if not explainable, some investigation should occur. An obvious example is deploying a new batch of replacement Windows PCs would generate a spike - but this is expected. If no new deployments are occurring and a spike occurs, new devices have been discovered and may be cause for investigation. you can click on the individual days data point on the graph to show a list of new machines discovered on that day. From this list you can click a machine name to see the specific machine details as discovered by Open-AudIT.



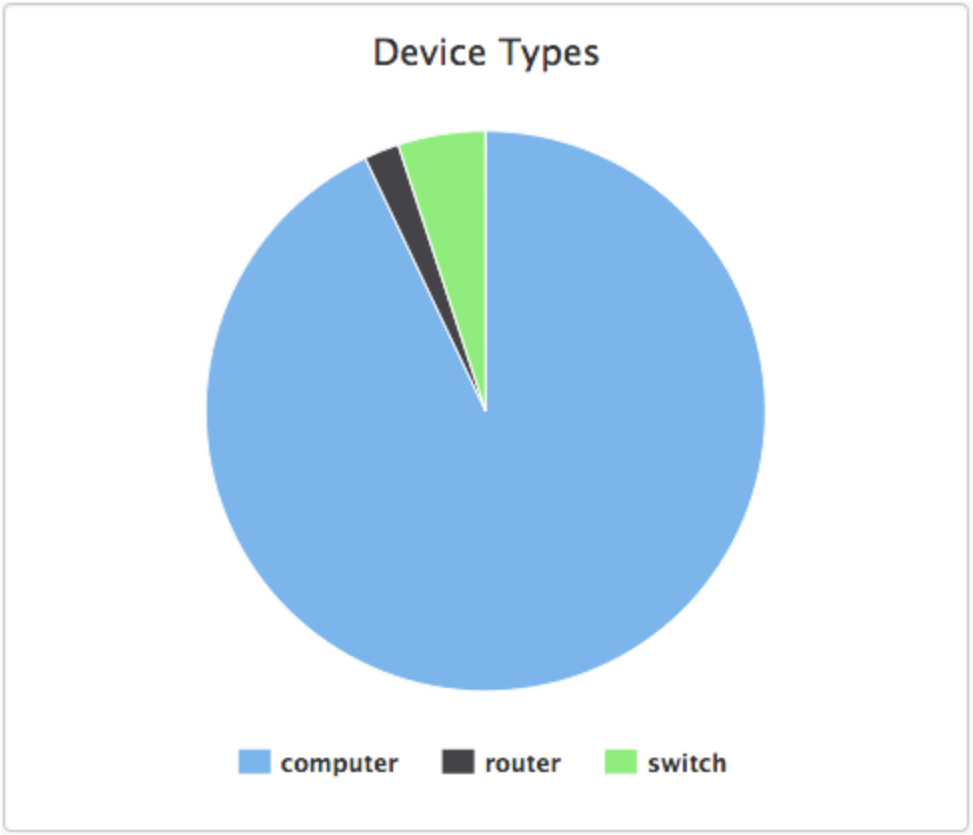
Software Discovered over the last 30 Days. This graph represents any new software packages detected over the last 30 days of audit. Note that this graph examines software packages, not machines. Therefore a deployment of (say) Adobe Reader to 100 machines would only represent one new piece of software being discovered on any given day. You can click the individual days data point on the graph to show a list of the new software packages discovered. From this list you can click a software package name to see which machines it was detected on, on that day.



Devices Not Seen for 30 Days. Items occurring here are devices that have not been detected on the network for 30 days that are still marked as being in production within the Open-AudIT database. This line should be expected to be consistently as close to zero as possible. Any devices that are considered in production should be audited more than once every 30 days. Ideally each day.

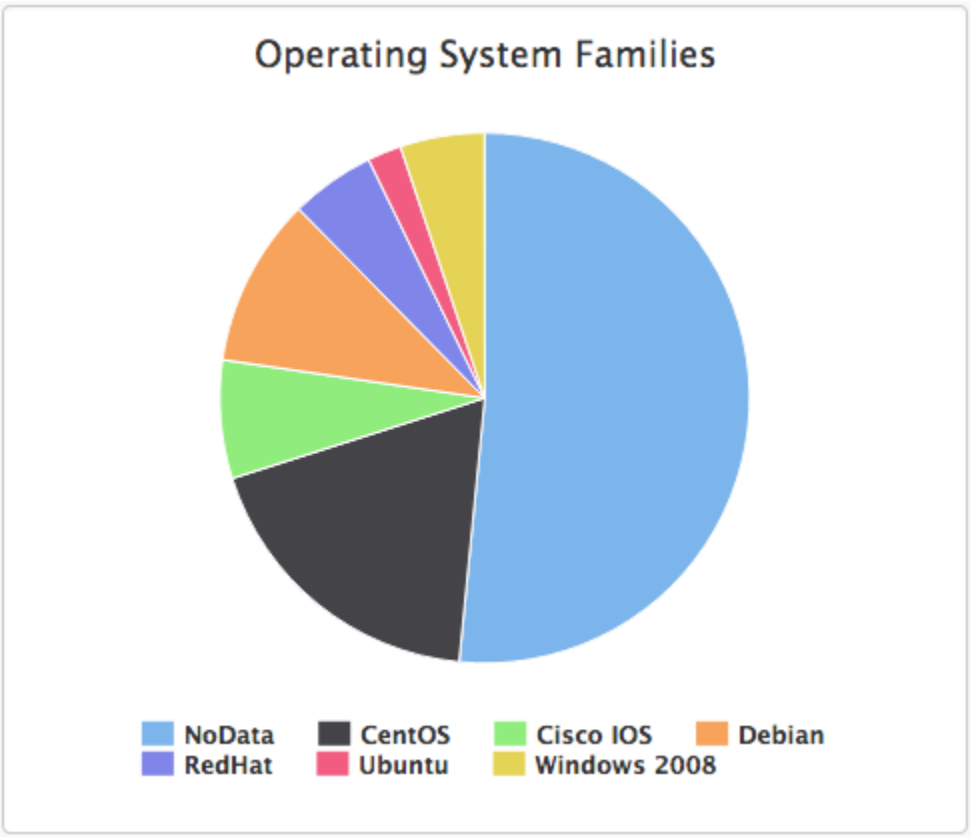


Device Type Percentage. A simple pie chart to illustrate the percent of the different device types within the Open-AudIT database. If the device type of Unknown occurs, this should be investigated as Open-AudIT has seen a device but was not able to determine its type.



Device Operating System Type Percentage. A simple pie chart to illustrate the percent of the different operating system types within the Open-AudIT database.

These dashboard graphs are pre-configured in Open-AudIT Enterprise and updated whenever the page is requested (live). Additional graphs can be constructed upon request.



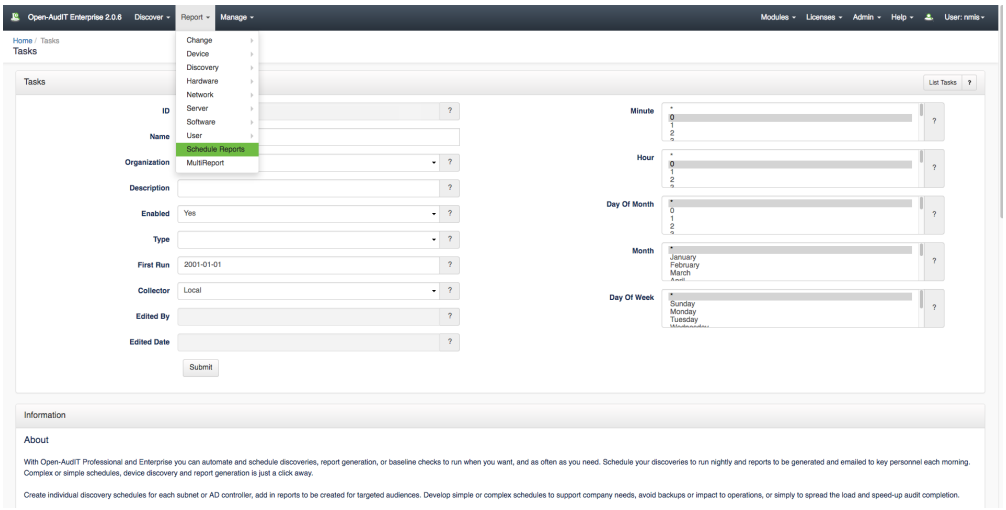
Maps

If you have configured Locations in Open-AudIT with the associated Groups enabled and devices assigned to those Groups, Open-AudIT Enterprise will show you these Locations using Google Maps and display a pop-up when a marker is clicked, containing the number of device types. The test for each device type is clickable and upon being clicked will show (inside Open-AudIT) the relevent devices in the particular location. If the Location Name is clicked, all devices will be shown in that location in Open-AudIT.

To enable Maps, create locations in Open-AudIT (Manage -> Locations > Create Locations) and ensure the Activate Group checkbox is ticked. Next assign some devices to those locations. You will now see these on the Open-AudIT Enterprise Map by clicking the opMaps icon in the Open-AudIT header or the Map link on the left side of the Open-AudIT Enterprise Dashboard.

Scheduled Reports

**UPDATE - This is now configurable from the web interface. In Open-AudIT Enterprise, go to Report -> Schedule Report.



~~Scheduled Reports allows for the generation of predefined reports to be archived or emailed on a desired schedule. If a report is to be emailed, the section of the configuration file conf/opCommon.nmis dealing with email should be completed. The initial config is below.~~

```
'email' => { 'mail_domain' => 'yourdomain.com', 'mail_from' => ', 'mail_password' => 'your_password',
'mail_server' => 'smtp.yourdomain.com', 'mail_server_port' => 25, 'mail_use_sasl' => 'false', 'mail_user' => '
},
```

~~You should edit this config to reflect your particular environment. This is for sending email containing reports from the Open-AudIT Enterprise server. Users receiving emailed reports are configured in the next section.~~

Configuring Report Generation

NOTE - This has been made largely redundant by the inclusion of Scheduled Task setup in Open-AudIT Enterprise v1.5.1.

~~Data is generated and sent as a scheduled report by a small cron script or scheduled task that should be run each day. Ideally this script should be scheduled to run at 2am each day. The script is a simple file kept in install/oae.cron (Linux) or install/oae.vbs (Windows). Feel free to move it if you desire. It must be run on the same machine that is running Open-AudIT Enterprise.~~

~~The oae_reports.json configuration file~~

~~**UPDATE - This is now configurable from the web interface. In Open-AudIT Enterprise, go to System -> Report Schedule.~~

~~The reports for Scheduled reports are configured in the file conf/oae_reports.json (a copy of which resides in install/oae_reports.json). For any reports to be run as part of the Scheduled Reports feature, this file is where you need to work. The following is an example from the file for a single report. We shall examine the options for each attribute in details below.~~

```
{ "schedule_id": "2", "user_id": "OAE-Dashboard", "report_id": "", "report_name": "Daily Discovered Devices",
"report_filename": "DailyDiscoveredDevices.xml", "group_id": "1", "group_name": "All Devices",
"first_attribute": "<CURRENT_DATE>", "format": "table_formatted", "destination": "dashboard",
"destination_address": "", "schedule": "daily", "schedule_hour": "11", "schedule_from": "2013-06-05",
"last_run": "2013-06-10 09:00:01", "last_run_status": "success", "enabled": "y" },
```

~~***schedule_id***: This should be a unique incrementing integer.~~

user_id: In the present code, this should always be set to the default value of OAE-Dashboard. The program will retrieve the access credentials from the opCommon.nmis file as described in the install guides.

report_id: If running a report that is already in the Open-AudIT database, you can specify the report's id here. This will prevent the need to supply a report definition XML file as below.

report_name: The human readable name of the report. Will be used to title the report.

report_filename: If you are running a report that is not present in the Open-AudIT database, you can supply a report definition file in XML format. The format of these files are the same as 'normal' Open-AudIT reports. Creating reports using report definition XML files is detailed on the How to create a Query definition page.

group_id: If you wish to restrict a report to a certain group, use the group id from the Open-AudIT database here. To run a report against all production status devices in the Open-AudIT database, a value of **1** should be used. This is always the Open-AudIT group id for "All Production Devices" group.

group_name: Used as a title in the filename or email subject. Typically for a filename or email subject it will be titled thus: $report_name . " for " . $group_name . " on " . $date with the correct filename extension if being saved.

first_attribute: Is an optional attribute. Used for adding additional information to a report query. Special values are **<CURRENT_DATE>** and **<CURRENT_DATE>-30**. When used, CURRENT_DATE will have the actual date of the request substituted and (if specified) 30 days removed.

format: Valid values are **csv, excel, xml, json, html, html_formatted**. The difference between html and html_formatted being the former is a straight dump of the columns into table format where as html_formatted results in a table formatted as per the Open-AudIT web interface and is typically prettier to view.

destination: Valid values are **file** and **email**.

destination_address: Only required if file or email specified in the destination attribute. Should be a file path on the local file system or a valid email address.

schedule: Permitted values are **daily**, **weekly**, **monthly**, **quarterly**, **yearly**.

schedule_hour: The hour of the day in zero padded 24hour format that you wish the report to run.

schedule_from: The first date the report should run from if it matches the schedule. This should be a zero padded date of the form YYYY-MM-DD. You may wish to use this to create scheduled reports and start them running at a date in the future.

last_run: Not used at present. Leave as default.

last_run_status: Not used at present. Leave as default.

enabled: This should be set to **y** to show that this report should be run if it matches the schedule. Set it to **n** to prevent the report from running.