Open-AudIT FAQ

Opening a Support Ticket? Please Attach These Files

If you open a support ticket, please do attach the Install Support as per this page - Open-AudIT Support Information

If your support request relates to a discovery issue, please **also** include the Discovery Support from this page - Open-AudIT Support Information

What are the default credentials to log into the web interface?

For Open-AudIT, the following users are set up by default.

Username	Password	Level	Used For
admin	password	Administrator	default logon
open-audit_enterprise	openaudit1234567890	User	List view access on "All Devices" group only.

You should use the admin user to log on to the web interface.

The open-audit_enterprise user is used internally by Open-AudIT Enterprise to retrieve data from Open-AudIT. If you change the password for this user in Open-AudIT, you should also insert the updated password in the conf/opCommon.nmis file inside Open-AudIT Enterprise. This file will be in c:\omk for Windows or /usr/local/omk for Linux installations.

My AntiVirus is prompting me to deny/allow things.

If you have Anti-Virus software running, allowing the services of Opmantek (omkd), Apache (apache2.2) and MySQL (mysql) to auto start and run is essential. These services are used by Open-AudIT. You should only need to do this once. If your Anti-Virus program keeps prompting you about Open-AudIT, please post to the forums or send an email to support with the name and version of your Anti-Virus software.

How can I add another user to Open-AudIT?

In the Open-AudIT web interface, as an admin user, select the menu item menu -> Manage -> Users -> Create Users.

Complete at least the username and password fields assign at least one Role and provide access to at least one Organization.

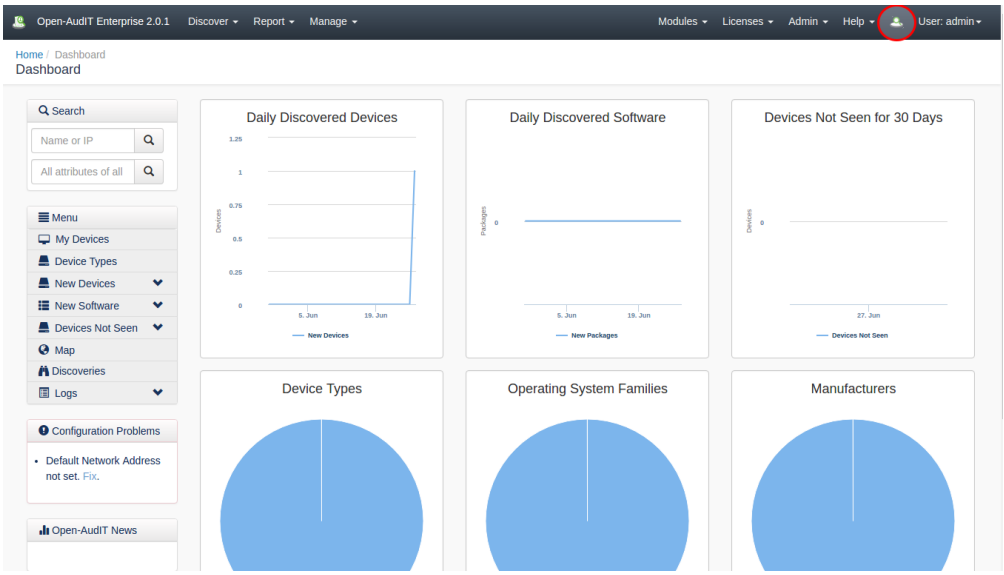
How can I access the Open-AudIT Community application?

The default URL for accessing Open-AudIT Community is ***http://<SERVER>/open-audit/index.php/*** (where <SERVER> is your computer name or IP Address).

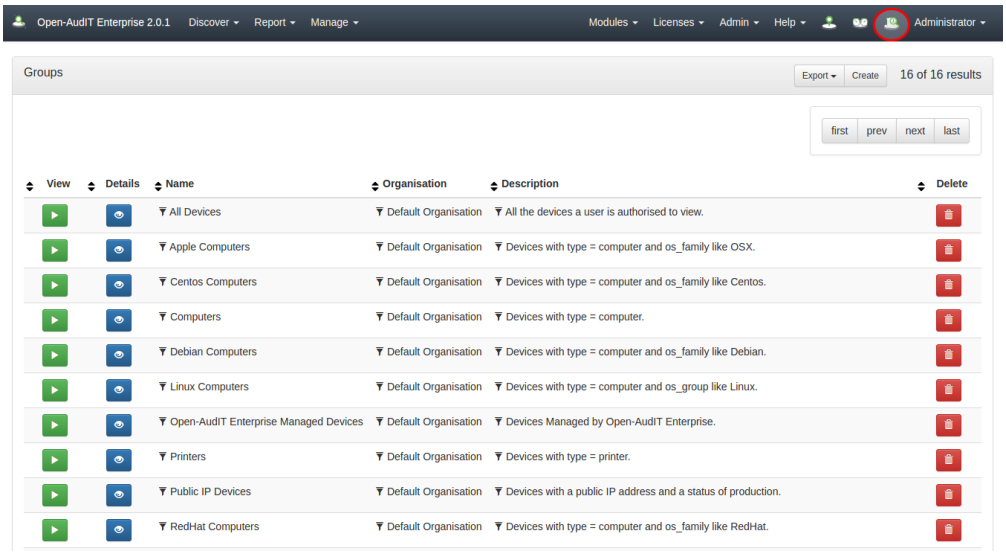
If you have installed on Windows, in your Start Menu you will see entries for both Open-AudIT Enterprise and Open-AudIT.

There are icons in both Community and Enterprise to switch between applications. Both icons are in the top right of the page, as below (click for larger images).

Professional / Enterprise



Community



Discovery has stopped working

If you are running a RedHat or Centos system and you have upgraded Nmap, please reset the SUID on the binary by

```
chmod u+s /usr/bin/nmap
```

An Open-AudIT Community page is not displaying and all I am seeing is a white screen.

If you open the file (for Windows) c:\xampplite\htdocs\open-audit\index.php or (for Debian/Ubuntu) /var/www/open-audit/index.php or (for RedHat/Centos) /var/www/open-audit/html/index.php and then change the line:

```
define('ENVIRONMENT', 'production');
```

to

```
define('ENVIRONMENT', 'development');
```

You should then have any errors displayed on the web page.

My time is off in Open-AudIT.

This is likely due to MySQL time being off. MySQL typically uses the host devices time. You can check this by:

Windows

```
c:\xampplite\mysql\bin\mysql.exe -u openaudit -popenauditpassword -e "SELECT NOW() as `timestamp`;"
```

Linux

```
mysql -u openaudit -popenauditpassword -e "SELECT NOW() as `timestamp`;"
```

I cannot see the details for a particular device in Open-AudIT Enterprise -> System Summary

If you can see a device has been discovered and is being counted on the Dashboard Graph and also appears in the Report for that day, but does not show on the Devices list page of Open-AudIT, make sure the "status" of the device has not been set to something other than 'production'.

Testing the OMKD service/daemon is running

If you call the URL below in a browser, you should receive a login page. Do NOT use this for logging on, only for testing the omkd (Opmantek) service /daemon is running.

NOTE - you may need to open port 8042 on your server's firewall (if it's running a firewall). This is not normally required to be open, but testing the service from a remote client does require it be accessible.

```
http://<YOUR_SERVER>:8042/omk/open-audit
```

Running Apache on a different port (to the default port 80)

Running Apache on a port other than 80 ***is not recommended***, but should be able to be accomplished by modifying the files below.

Open-AudIT is installed to c:\xampplite\open-audit on Windows and /usr/local/open-audit on Linux.

Open-AudIT Enterprise is installed to c:\omk on Windows and /usr/local/omk for Linux.

You will need to update the audit scripts "url" variable in the open-audit/other/ directory (both .sh and .vbs scripts). The files audit_linux.sh, audit_osx.sh, audit_subnet.sh, audit_subnet.vbs, audit_windows.vbs will all need changing ***if running the scripts directly on the targets and outside a discovery.*** In normal discovery use, modifying the scripts is not required. One special case exists - a Windows Open-AudIT server running discovery where the Apache service has not been given a regular user. That configuration ***is not recommended***, and will require script modification.

In the configuration for Open-AudIT Enterprise change the file omk/conf/opCommon.nmis and set the oae_server variable to include the changed port number.

Linux - /usr/local/omkd/conf/opCommon.nmis

WIndows - c:\omk\conf\opCommon.nmis

Changing the port Apache runs on is different for different installations. Some general guidelines are below.

On Debian/Ubuntu, modify the /etc/apache2/port.conf and the /etc/apache2/sites-enabled/000-default files (change the ports contained in them) then reload and restart apache with "service apache2 reload" and "service apache2 restart".

On RedHat/Centos, modify the /etc/httpd/conf/httpd.conf file (change the port contained in the Listen attribute) then restart apache with "/etc/init.d/httpd restart".

On Windows, modify the file c:\xampp\apache\conf\httpd.conf (change the port contained in the Listen attribute) then restart apache by stopping and starting the apache2.2 Service in the Windows Services control panel item.

Edit the file and include the port in the URL in -

Linux - /usr/local/opmojo/bin/open-audit_tasks.sh

Windows - c:\omk\bin\open-audit_tasks.vbs

Edit the following files to include the port (search for execute.sh or execute.vbs).

Linux -

/usr/local/open-audit/code_igniter/application/controllers/include_input_queue.php

/usr/local/open-audit/code_igniter/application/controllers/input.php

/usr/local/open-audit/code_igniter/application/controllers/util.php

/usr/local/open-audit/code_igniter/application/models/m_queue.php

Windows -

c:\xampp\open-audit\code_igniter\application\controllers\include_input_queue.php

c:\xampp\open-audit\code_igniter\application\controllers\input.php

c:\xampp\open-audit\code_igniter\application\controllers\util.php

c:\xampp\open-audit\code_igniter\application\models\m_queue.php

You should now be able to navigate to ***http://<SERVER>:<port>/*** in your browser and get a response.

This is not recommended and may cause other issues. You will have to re-patch the above files each time you upgrade. You have been warned. Here be dragons.

I cannot start the Apache service on Windows.

Have you checked that another program is not already using port 80? If you start a command prompt and type:

```
netstat -abn
```

You should get an output similar to:

```
C:\>netstat -abnp tcp

Active Connections

Proto Local Address Foreign Address State
TCP 0.0.0.0:80 0.0.0.0:0 LISTENING
[httpd.exe]
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
RpcSs
[svchost.exe]
TCP 0.0.0.0:443 0.0.0.0:0 LISTENING
[httpd.exe]
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
Can not obtain ownership information
TCP 0.0.0.0:554 0.0.0.0:0 LISTENING
[wmpnetwk.exe]
TCP 0.0.0.0:1025 0.0.0.0:0 LISTENING
[wininit.exe]
TCP 0.0.0.0:1026 0.0.0.0:0 LISTENING
eventlog
[svchost.exe]
TCP 0.0.0.0:1027 0.0.0.0:0 LISTENING
Schedule
[svchost.exe]
TCP 0.0.0.0:1028 0.0.0.0:0 LISTENING
[lsass.exe]
TCP 0.0.0.0:1029 0.0.0.0:0 LISTENING
[services.exe]
TCP 0.0.0.0:1030 0.0.0.0:0 LISTENING
PolicyAgent
[svchost.exe]
TCP 0.0.0.0:2869 0.0.0.0:0 LISTENING
Can not obtain ownership information
TCP 0.0.0.0:3306 0.0.0.0:0 LISTENING
[mysqld.exe]
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING
CryptSvc
[svchost.exe]
TCP 0.0.0.0:5357 0.0.0.0:0 LISTENING
Can not obtain ownership information
TCP 0.0.0.0:8042 0.0.0.0:0 LISTENING
[opmantek_server.exe]
TCP 0.0.0.0:10243 0.0.0.0:0 LISTENING
Can not obtain ownership information
TCP 192.168.0.86:139 0.0.0.0:0 LISTENING
Can not obtain ownership information
TCP 192.168.0.86:2869 192.168.0.1:3115 TIME_WAIT
```

Look for a program using port 80. In this case, note the output

```
TCP 0.0.0.0:80 0.0.0.0:0 LISTENING
[httpd.exe]
```

That indicates port 80 is being used by the executable httpd.exe (in this case, Apache). You should not see any entries using :80.

If there is another program using port 80 either stop and remove it, change it's port (if possible) or install Open-AudIT on another machine.

Skype uses port 80 by default. If it gets in first it prevents Apache using port 80. Completely exit Skype (on a Windows 7 machine you need to go to the taskbar and right click/quit the Skype icon) and then start the Apache service. You can then restart Skype and it will use another port. Alternatively force Skype to not use port 80 and 443: In Skype | options | advanced | connection untick the "use port 80 and 443 as alternatives for incoming connections". This should also solve the problem.

I Still cannot start the Apache service on Windows

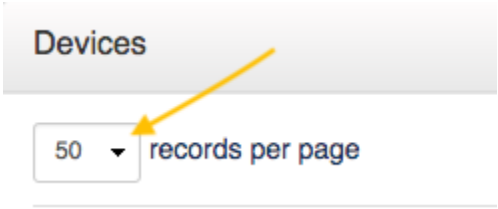
You may need to download and install the MS Visual C++ redistributable. You can find it here - https://support.microsoft.com/en-au/help/2977003/the-latest-supported-visual-c-downloads

Trying to log into Open-Audit Enterprise but keep getting placed into the Community edition.

Some users may run into the issue of being unable to access Open-Audit Enterprise features even though they are licensed for it. This could be an issue with http redirect causing problems for the communication between Open-Audit Enterprise and Open-Audit itself. This is controlled by the config option oae_server located in /usr/local/omk/conf/opCommon.nmis under the openauditenterprise section. The default value for this is http://127.0.0.1/open-audit/ and changing this to https://127.0.0.1/open-audit/ will resolve this issue in many cases.

Bulk Edit selections won't stay selected after clicking next page

If this occurs then the issue you're seeing is related to the table control being used on the webpage. It only stores in memory the state of the check boxes for the current page being viewed. If you make selections, then page forward/back those selections will be lost. You can, however, accomplish what you want by expanding the number of devices shown on each page. In the top-left corner is a drop-down labeled "records per page"; use this to expand the number of entries displayed until you see all you want to select for Bulk Edit.



Scheduled Tasks Don't Finish

If a scheduled task (discovery or report generation) process is terminated before completion the status in Open-AudIT may not be updated. This will leave the little running animation icon on.