# How to audit a Computer


- Cannot Audit
- Auditing using a GUI
- Auditing using a GUI #2
- Auditing using a script (Windows)
- Auditing using a script (Linux / SSH)
- Options
- Unusual Auditing
    - Computer with no network connectivity to the Open-AudIT server.
    - Computer not on the domain.
    - Computer than can see the Open-AudIT server, but the audit host cannot see the computer (unusual).

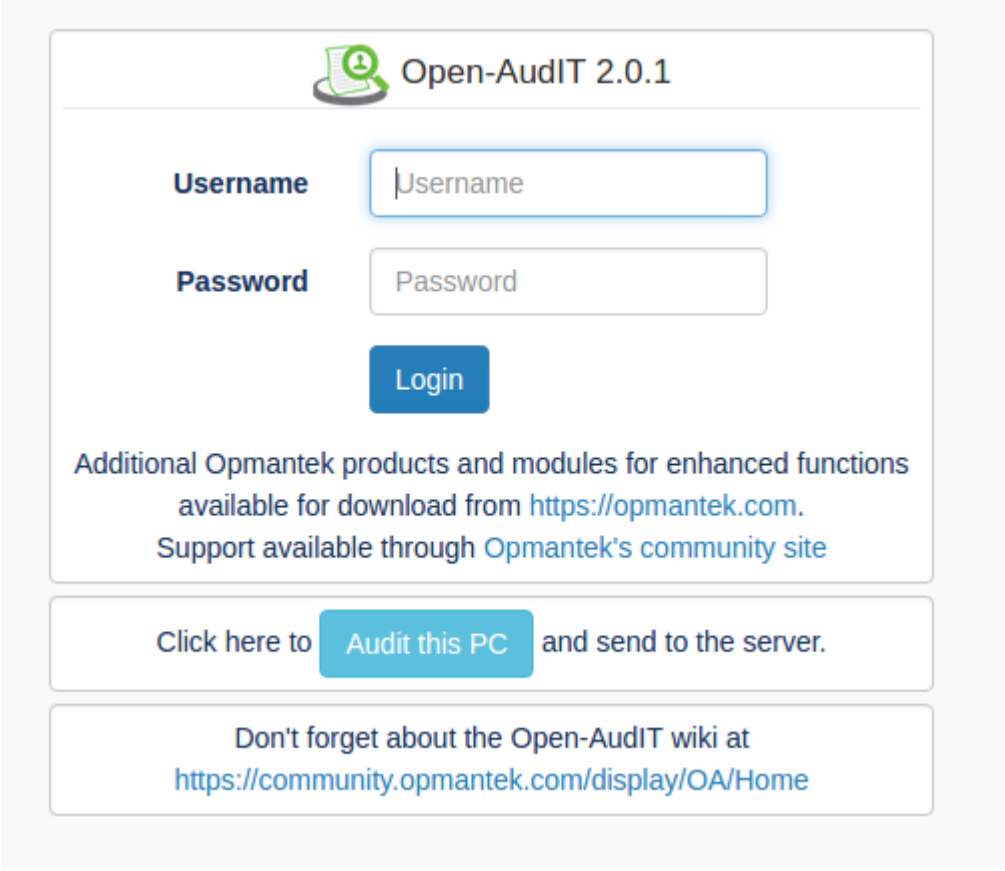

## Cannot Audit

If you are having issues auditing a Windows PC, see our page that specifies the client configuration and provides some hints for configuration, here - Target Client Configuration.

## Auditing using a GUI

To do this, go to the Open-AudIT logon page at http://YOUR-SERVER/omk/open-audit (but do not log in) using your browser on a Windows PC. You should see a page as below. Click the "Audit My PC" button and run the script. You should see your computer being audited and the data should be posted to the Open-AudIT server.

You should now be able to log in and see the details from your Windows PC.




## Auditing using a GUI #2

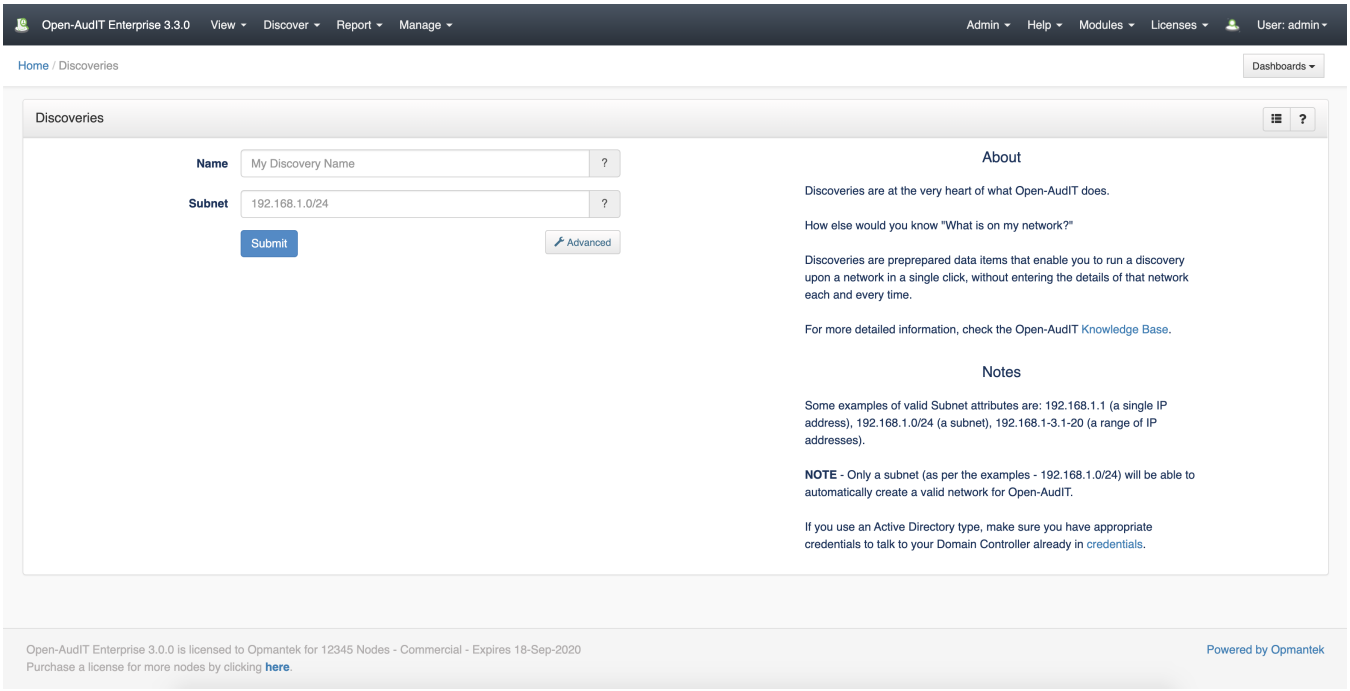
First, ensure you have added the credentials for this device in Discover -> Credentials -> Create Credentials.

Then go to Discover -> Discoveries -> Create Discoveries. You will see the below form.

If you have set the "Local Network Address" in the config (Menu -> Admin -> Community -> Discovery Configuration) the Network Address will be pre-populated. This should be the URL of your Open-Audit server. You can use HTTPS if preferred (and you have installed a SSL certificate).

Add the IP address of the target computer.

Click the "Submit" button and you will be directed to the Discovery list page. Click the Execute button and the Discovery will start and you will be directed to the Discovery details page.




# Auditing using a script (Windows)

Assuming you have an XAMPP install of Open-AudIT on a Microsoft Windows machine.

Copy the file c:\xampp\open-audit\other\audit_windows.vbs to a suitable location. Do **not** remove this file from it's original location as it is needed by the web interface.

You can also download the scripts using the GUI by going to menu  Discover  Scripts  List Scripts, and choosing the download button on the right side.

Open your copy of audit_windows.vbs in a text editor. Check the following variables are set as below:

- submit_online = "y"
- create_file = "n"
- url = "http://YOUR_SERVER/open-audit/index.php/input/devices"
- debugging = "3"

Open a command prompt and run the script with ***cscript audit_windows.vbs***. *Do not double click the script to run it as this will use wscript instead of cscript and spawn many popup windows.*

It should run and post the result to the database. Go back to your web browser and load Open-AudIT. You should have a group or two created. Go into one of them and click the machine name. You should see the machine details.

NOTE - To prevent any output to the command window you can set debugging = "0" and run the script with ***cscript //nologo audit_windows.vbs .***

# Auditing using a script (Linux / SSH)

We have unix based (bash. ksh, etc) scripts for Linux, AIX, OSX, Solaris computers.

You can download the scripts using the GUI by going to menu  Discover  Scripts  List Scripts, and choosing the download button on the right side.

To use the Unix audit script located at /usr/local/open-audit/other/audit_linux.sh:

- Edit the script and ensure the $url variable is set to your webserver - the same as is done for the audit_windows.vbs script.
- Copy it to the target computer.

- Ensure the script has permission to operate (chmod 777 audit_linux.sh is fine).
- Run the script with root level permission either by sudo or directly as root.

The script has variables that can be set the same as the variables in audit_windows.vbs. You could (for example) dynamically set the $url variable when you run the script by:

```
chmod 777 audit_linux.sh

sudo ./audit_linux.sh url=http://your_server/open-audit/index.php/input/devices submit_online=y create_file=n
```

The variables that are accepted on the command line are:

submit_online - Defaults to "n". If set to "y" it will submit the audit result to the URL as specified by the url variable.

create_file - Defaults to "y". If set to "y", an XML file will be created and saved as per the audit_windows.vbs script. This file can be manually copied and submitted to the server at a later stage if desired.

Sample output on the console when the script has been run.

```
mark@dev:/usr/local/open-audit/other$ sudo ./audit_linux.sh url=http://your_server/open-audit/index.php/input
/devices submit_online=y create_file=n
[sudo] password for mark:
Starting audit
---------------------------
Open-AudIT Linux audit script
Version: 4.3.0
---------------------------
My PID is           13869
Audit Start Time    2021-11-26 13:22:33
Create File         y
Submit Online       n
Debugging Level     2
Discovery ID
Org Id
Script Name         audit_linux.sh
URL                 http://your_server/open-audit/index.php/input/devices
File                /usr/local/open-audit/other/dev-20211126132233.xml
---------------------------
System Info
USB Info
Policy Info
BIOS Info
Processor Info
Memory Info
Motherboard Info
Optical Drives Info
Video Cards Info
Sound Cards Info
Shares Info
Network Cards Info
Hard Disk Info
Guest (Docker, Proxmox, LXC) Info
Docker Info
Log Info
Environment Variable Info
Swap Info
User Info
Group Info
Software Info
Service Info
    systemd services
    upstart services
    init.d services
Server Info
        apache
        mysql
        mongo
Server Items
        mysql using /etc/mysql/my.cnf
        mariadb using /etc/mysql/mariadb.conf.d
        apache using apachectl for VirtualHosts
        mongod using /etc/mongod.conf
Certificate Info
Route Info
Netstat Info
Custom Files Info
Audit Generated in '17' seconds.
Submitting results to server using cURL
URL: http://your_server/open-audit/index.php/input/devices
Audit Completed in '47' seconds.
```

# Options

All variables can be passed via the command line at run time. You don't need to create one audit script for each different (say) set of remote user credentials. A couple of examples -

- cscript audit_windows.vbs REMOTE_PC strUser=REMOTE_USER strPass=PASSWORD - will audit a remote machine with credentials other than those of the local user running the script.
- cscript audit_windows.vbs . submit_online=n create_file=y - will run the audit on the local PC and output to a file (in the current directory). The "." can be used in place of the local machine name.

The command line arguments are as follows, variable [default] (valid options):

| Variable | Description |
|---|---|
| create_file [n] (y\|n) | create a text file names COMPUTERNAME_YYYYMMDDHHMMSS.xml in the directory the audit script is run. |
| debugging [1] (0-3) | Verbosity of the output to the command line. Set to "0" for no output. |
| ldap [] (string) | This value is passed in when running the audit_domain script. Only set this value if your audit host is on a different domain than audit targets and you are not using audit_domain.vbs - IE, you are running "cscript audit_windows.vbs COMPUTER" where COMPUTER is on a separate domain than the PC you are running the command on. This would then apply to ALL systems audited like this. This would be the exception rather than the rule. |
| org_id [] (org_id) | If set the PC will be automatically assigned to the organisation. Get the organisation id by using the web interface. |
| ping_target [n] (y\|n) | Attempt to ping the target PC before attempting to audit it. |
| self_delete [n] (y\|n) | Delete the audit script itself upon completion. |
| skip_printer [n] (y\|n) | Do not attempt to retrieve any printer details. |
| skip_software [n] (y\|n) | Do not attempt to retrieve any installed software details. |
| skip_dns [n] (y\|n) | Do not attempt to retrieve any DNS details. |
| skip_mount_point [n] (y\|n) | Do not attempt to retrieve mount point details. |
| strcomputer [.] (string) | The name of the target PC. "." means the local PC on which the script is running. |
| struser [] (string) | Should be of the format DOMAIN/USERNAME. Runs the script against the target PC using these credentials. |
| strpass [] (string) | Runs the script against the target PC using these credentials. |
| submit_online [y] (y\|n) | Submit the audit result to the webserver upon completion. |
| url [http://localhost/open-udit/index.php/input/devices] (string) | The URL of the Open-AudIT server to submit the audit to. The variable submit_online must be set to "y". |
| use_proxy [n] (y\|n) | Unused at present. |
| windows_user_work_1 [physicalDeliveryOfficeName] (string) | The Active Directory attribute to use as a first preference to determining the target PCs user work unit. |
| windows_user_work_2 [company] (string) | The Active Directory attribute to use as a second preference to determining the target PCs user work unit. |
| details_to_lower [y] (y\|n) | Details like domain, hostname, username, etc are usually set to lower case for consistency. If you would like these kept as retrieved, set to "n". |

# Unusual Auditing

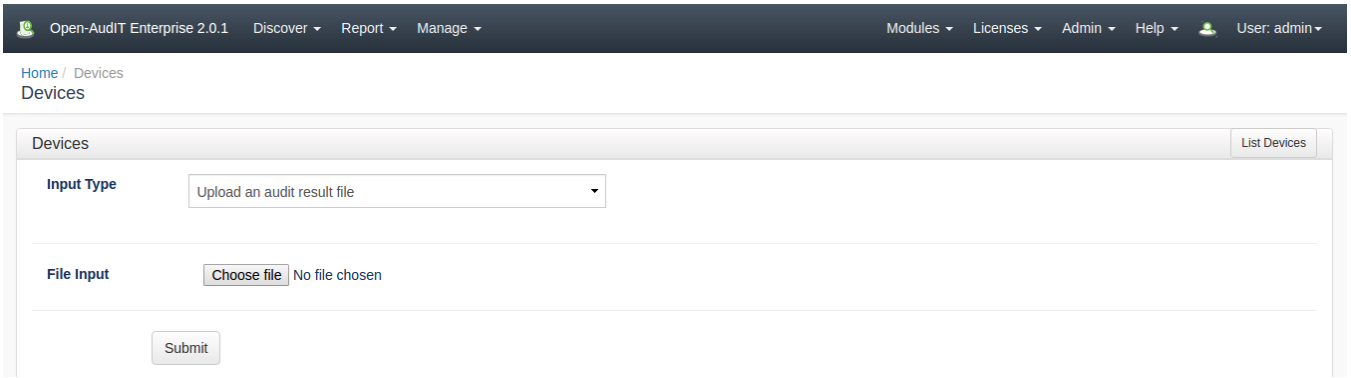
Not every Windows computer will be a simple domain connected machine. Sometimes you may have a server in a DMZ with no network connectivity to the internal network, a machine not on a domain, a standalone machine not networked at all, etc. There are various options to overcome these.

## Computer with no network connectivity to the Open-AudIT server.

Copy the audit script to a USB drive, go to the remote computer and insert the USB drive. Open a command prompt and navigate to where you copied the script. Run the script and output to an XML file using the command

```
cscript audit_windows.vbs submit_online=n create_file=y
```

An XML file named COMPUTERNAME_DATE.xml should be created. Close the terminal window. Remove the USB drive and go to a computer with Open-AudIT connectivity. Open the XML file and copy the XML and log in to the Open-AudIT web application and go to menu  -> Manage -> Devices -> Create Devices. You will see options for manually copying and pasting the file contents or uploading the file directly.




## Computer not on the domain.

If you can see the computer on the network and it has it's firewall opened to allow remote WMI/VBscript, you can run the audit script using the remote credentials.

```
cscript audit_windows.vbs strcomputer=REMOTE_COMPUTER_NAME struser=REMOTE_DOMAIN/REMOTE_USERNAME
strpass=REMOTE_PASSWORD
```

You may need to substitute the string "workgroup" or the remote computer name for REMOTE_DOMAIN above.

## Computer than can see the Open-AudIT server, but the audit host cannot see the computer (unusual).

You can copy the audit script to the target computer and set it to run on a scheduled task and submit the result to the Open-AudIT server.