Information about default users and passwords

Opmantek VM Passwords

If you are using the Opmantek Virtual Appliance, you can find more default credential information at Default Credentials (Passwords) for NMIS8 VM

Open-AudIT Enterprise web logon (pre 5.0.0)

Enterprise and Professional can use various methods for authentication. However, regardless of authentication, your user must exist within Open-AudIT in order to receive authorisation. The simplest method is to simple create your user in the Open-AudIT web GUI and ensure "openaudit" is listed as an acceptable method in /omk/conf/opCommon.nmis. The installer will do this for you. See below (Open-AudIT web logon).

The below is only relevant if you wish to use htpasswd based authentication. You will still require Open-AudIT to contain the user, this will be used for authorisation.

These passwords are stored in the /usr/local/omk/conf/users.dat or c:\omk\conf\users.dat file.

They can be changed using htpasswd - IE, "`htpasswd -d /usr/local/omk/conf/users.dat admin`" and typing the new password. Please note that before release 1.4.0 of Open-AudIT Enterprise only the 'crypt' password hashing method is supported (hence the `-d` option in the example above). Starting with that version both password hashing methods 'crypt' and 'md5' can be used.

The default credentials are:

admin : password

Open-AudIT web logon

These passwords are stored in the Open-AudIT database and can be changed by logging into Open-AudIT as an admin level user and going to Menu -> Manage -> Users -> List Users and selecting the user to edit.

admin : password (default user)

Open-AudIT Enterprise user (pre 5.0.0)

This user is used by Open-AudIT Enterprise to log on to Open-AudIT and generate scheduled reports, retrieve dashboard data, etc. This user will not work in the web interface of Open-AudIT Enterprise. This user should have at least 'view' access on the All Devices Group. It does not need admin or sam (Software Asset Management) access, but for completeness - using Discovery, setting config values and so on, it should be an Admin level user within Open-AudIT.

In Open-AudIT Enterprise it is stored in the file omk/conf/opCommon.nmis

In Open-AudIT it is stored in the database can can be edited like any other user via the web interface.

open-audit_enterprise : openaudit1234567890 (used by the Open-AudIT Enterprise dashboard)

Open-AudIT MySQL user

This password is stored in the file (pre 5.0.0) open-audit/code_igniter/application/config/database.php

For 5.0.0 onwards it is open-audit/app/Config/Database.json

openaudit : openauditpassword

Open-AudIT root MySQL user

This password is not stored. It is only used to setup the initial Open-AudIT database and can be changed directly in MySQL. It is only set if it does not already exist.

root : openauditrootuserpassword

Default encryption key

Open-AudIT stores the device credentials in it's database. It must store them in a reversible format in order to use them (to connect to the target devices). See Storing Credentials (encryption) in Open-AudIT.

They are encrypted using a key which is found in (pre 5.0.0) /open-audit/code_igniter/application/config/config.php.

The variable used is $config['encryption_key'] which by default is set to 'open-audit'.

And for 5.0.0 onwards it is in /open-audit/app/Config/Encryption.php

The variable used is $key which by default is set to 'open-audit'.

NOTE - If you change this key after you have created some credentials, those credentials will be unusable (they will not be able to be decrypted). You should first export them, delete them, change the encryption key, then import them.