

# Credentials

- [Introduction](#)
- [How Does it Work?](#)
- [Creating Credentials](#)
- [Importing Credentials](#)
- [SSH Keys](#)
- [Viewing Credential Details](#)
- [Database Schema](#)
- [API / Web Access](#)

## Introduction

Credentials can have one of a few different types - snmp v.1 / v.2, snmp v.3, ssh, ssh key, windows are all implemented. CAVEAT - ssh keys are not implemented for Windows Open-Audit servers as yet.

## How Does it Work?

Credentials are stored in the "credentials" database table. The actual credential information is encrypted in storage. When a Discovery is run, a device has it's specific credentials retrieved from the database, decrypted and tested. If these fail the list of credentials is also retrieved, decrypted and then tested against the device starting with credentials known to have worked previously. Device specific credentials are stored at an individual device level in the "credential" table (note - no 's' in the table name). SSH keys are tested before SSH username / password. When testing SSH, credentials will also be marked as working with sudo or being root.

**NOTE** - If you request a downloaded CSV, XML or JSON format (either a single credential, or the complete collection) **the actual credential details will be sent**. Not the encrypted string, the actual username, password, community string, etc. Any sensitive details are not displayed in the web GUI, but are made available via other formats. To prevent this export a configuration item is available called *decrypt\_credentials*.

## Creating Credentials

To make another credential entry use the menu and go to menu: Discover -> Credentials -> Create Credentials. Provide a name, organization and optionally a description. Choose a type of credential. Once you do this, the additional fields will populate with the available configurable options.

## Importing Credentials

Credentials can be imported en-masse using menu Discover Credentials Import Multiple Credentials. We use a CSV formatted file. That page details the required columns.

Below is an example of the required csv format. The minimum required attributes for attributes are 'name','org\_id','type' and the credentials details (see below). You should not include the edited\_by and edited\_date fields. These will be automatically set. If you include the "id" field **and** set it with a number, that item will be updated rather than created. The field 'credentials' is stored as an encrypted JSON object. You should use the field names of 'credentials.attribute name'. For an example, an SNMP community string would be 'credentials.community'. For an example, use the web interface to create a credential set and then go to menu -> Admin -> Database and click on Discoveries. Then export to CSV. Valid credentials attributes are: community, username, password, domain, ssh\_key, authentication\_passphrase, authentication\_protocol, privacy\_passphrase, privacy\_protocol, security\_level, security\_name. You should use a header line containing the names of the columns you wish to populate, then your data lines below that.

"name","org_id","type","credentials.community","credentials.username","credentials.password"
"Public SNMP","1","snmp","public","",""
"My SSH","1","ssh","","my_user","my_password"
"Windows Creds","1","windows","","my_win_user@open-audit.com","my_win_password"

Open-AuditIT Enterprise 3.3.0 View Discover Report Manage Admin Help Modules Licenses User: admin

Home / Credentials

Credentials

50 records per page

Search:

Details	Name	Organisation	Description	Type	Edited By	Edited Date	Delete
	admin on hel	Default Organisation		windows	Administrator	2020-03-04 10:35:16	
	Council	Default Organisation		ssh	Administrator	2020-03-04 10:35:34	
	nmisgig	Default Organisation		snmp	Administrator	2020-03-04 10:37:47	
	OMK Ops	Default Organisation		ssh_key	Administrator	2020-03-04 10:35:50	
	omkr	Default Organisation		snmp	Administrator	2020-03-04 10:37:34	

Showing 1 to 5 of 5 entries

First Previous Next Last

Open-AuditIT Enterprise 3.0.0 is licensed to Opmantek for 12345 Nodes - Commercial - Expires 18-Sep-2020  
Purchase a license for more nodes by clicking [here](#).

Powered by Opmantek

Open-AuditIT Enterprise 3.3.0 View Discover Report Manage Admin Help Modules Licenses User: admin

Home / Credentials

Credentials

Name

Org ID

Description

Type

Credentials

Submit

About

Credentials are used to access devices.

The only supplied credential is that of SNMP public.

Configuring credentials should be one of the first things you do after installing Open-AuditIT.

For more detailed information, check the Open-AuditIT [Knowledge Base](#).

Notes

Credentials are encrypted when stored in the database.

When a Discovery is run, a device has its credentials retrieved and tested for connection first (from the `credential` table). If these fail, then credentials associated with the given Org `credentials.org_id` is also tested against the device. Working credentials are stored at an individual device level in the credential table (note - no "s" in the table name).

SSH keys are tested before SSH username / password. When testing SSH, credentials will also be marked as working with sudo or being root.

For ease of use, Windows passwords should not contain a ' or ". This is a remote WMI limitation, not an Open-AuditIT limitation.

## SSH Keys

You should copy and paste the entire file into the textbox. In the case below, copy ALL the text.

```

-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,328refbeif03
duvbwuidnpowmpowenciubvienpomcpoenrfurehoiernfporjfoierhiuebvvn
dvkjeekjvlfkvlfbvienvpoeenviuberiovneporvmpoernvoiernvoiernv
9wI0nVfcdhhd8DExfGfFwR2AoGaNYgE0TVUfRU21HQG8C+HoLysCla4CaHsRgVy
DTzGJQhfKafu2G3lwt12kTycTpuje00EyRsa4kT0KPP+IDJrtkRmEJY3UGlXg72P
jLZ/o2Ygz15ZT9GkNb9jyPCZMF3NJqL+Mz03ikKHDZvfOxA5P1XTPiXSVLzB1MJt
lgP2A3v1W/eaVeVhPa6Wo9gbDm/+PzDL+rT9ZK5K8sc1AcDIJ0m9OGCQtqpwSxEB
iJ07usXWXI4Cf4ex3+Oxeoineoifnoienfoiernfoiernfoermf[pef[pffed0DD
FsRSBmCbsCHrzGIqk8Maqh5gjPhkerneLlH40Jeloks2tkD72UT/bYWgvpTxzVUA
+LSVhR/Li+cGiebGKqKgE2sXmuIGn9UuqOvFbDudowRyr090tM1QsfresILmTKTA
VCNKEQEXLlmhsUnr1paOOMs5vZ2o03x0S7x+QXrWGye+QK9aquZ+IQ3Z4Lb130Q4
dfvneivnoiernvoiernvoinervionreioivnreioivnoiernvoiernv/pae,fefeff
W76aH+wxCuusNWACvhfDcYXjp4dP3AD2EiuIYlvkI10cwNrX9tmZyG37qaYDPCdW
ikmDolK6tepoqS05js+RouUHvZEZg3jBxkTkI0FB+JJcOvz19ixf3Ce/CeWkcCrb
6oGjyNEOqoFDoceIUFZGOW4tsNySyqON9a0TuToPCX5rQd57fPabnl6Tl6XUCqWz
lDZ2HyVm+k4DAzLx2BoA5urWzdlniuuberovbeirvbifevnienvirenviernviner
ovneiuvniefvbuiervbiunviunervioneroivnoiernvoiernvoinervoineroi
b2cmcEETwXZEzVudljkOmt7d8F2fWvCFPYSh/wneI1A7kPiWw9B1T3SRTiLS8fv4
t8pr/GvAseVzRe7q9oMAfnAYnBuWCzN++JitjgwRhjln/WmqxqfPuRwcZ/Y8cHZb
fSuJdcldGBx7KH/7N/rRCioAc7lcrI/x+AgVs+7Cng0a5OHT4DfA6A==
-----END RSA PRIVATE KEY-----

```

## Viewing Credential Details

Go to menu: Discover -> Credentials -> List Credentials.

You will see a list of credential. You can view a credential by clicking on the blue view icon. You can also edit or delete your credentials.

Open-Audit Enterprise 3.3.0 | View | Discover | Report | Manage | Admin | Help | Modules | Licenses | User: admin

Home / Credentials | Dashboards

### Credentials

50 records per page | Search:

Details	Name	Organisation	Description	Type	Edited By	Edited Date	Delete
	admin on hel	Default Organisation		windows	Administrator	2020-03-04 10:35:16	
	Council	Default Organisation		ssh	Administrator	2020-03-04 10:35:34	
	nmisigig	Default Organisation		snmp	Administrator	2020-03-04 10:37:47	
	OMK Ops	Default Organisation		ssh_key	Administrator	2020-03-04 10:35:50	
	omkr	Default Organisation		snmp	Administrator	2020-03-04 10:37:34	

Showing 1 to 5 of 5 entries | First | Previous | Next | Last

Open-Audit Enterprise 3.0.0 is licensed to Opmantek for 12345 Nodes - Commercial - Expires 18-Sep-2020  
Purchase a license for more nodes by clicking [here](#) | Powered by Opmantek

## Database Schema

The database schema can be found in the application if the user has database::read permission by going to menu: Admin -> Database -> List Tables, then clicking on the details button for the table.

## API / Web Access

You can access the collection using the normal Open-Audit JSON based API. Just like any other collection. Please see [The Open-Audit API](#) documentation for further details.