Credentials

- Introduction
- How Does it Work?
- Creating Credentials
- Importing Credentials
- SSH Keys
- Viewing Credential Details
- Example Database Entry
- API / Web Access
    - API Routes
    - Web Application Routes

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

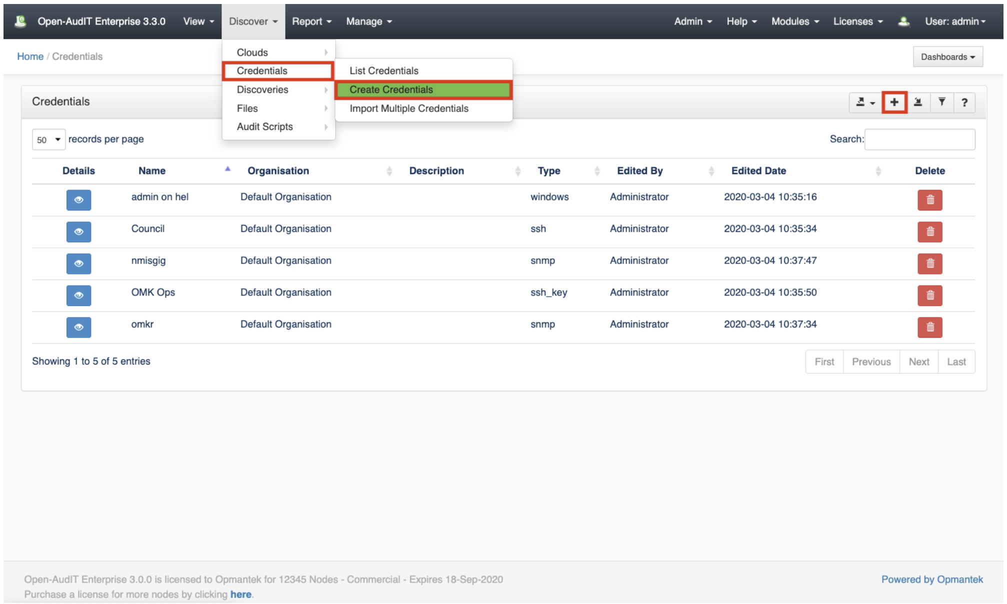
To make another credential entry use the menu and go to menu: Discover -> Credentials -> Create Credentials. Provide a name, organization and optionally a description. Choose a type of credential. Once you do this, the additional fields will populate with the available configurable options.

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"

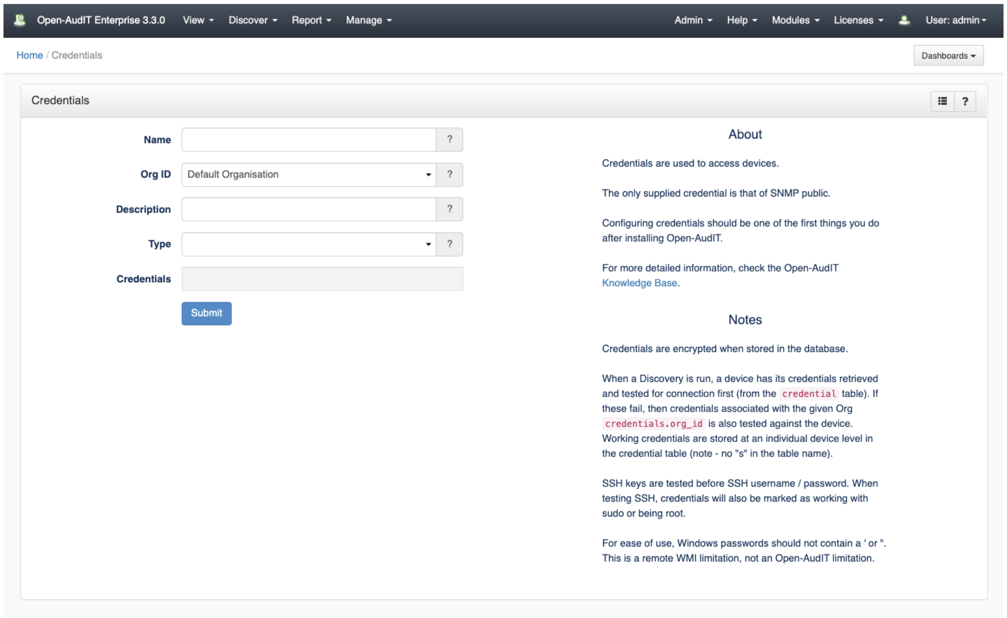


Details	Name	Organisation	Description	Type	Edited By	Edited Date	Delete
	admin on hel	Default Organisation		windows	Administrator	2020-03-04 10:35:16	
	Council	Default Organisation		ssh	Administrator	2020-03-04 10:35:34	
	nmisgig	Default Organisation		snmp	Administrator	2020-03-04 10:37:47	
	OMK Ops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

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



Name	
Org ID	Default Organisation
Description	
Type	
Credentials	

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-AudIT.

For more detailed information, check the Open-AudIT 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-AudIT limitation.

SSH Keys

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

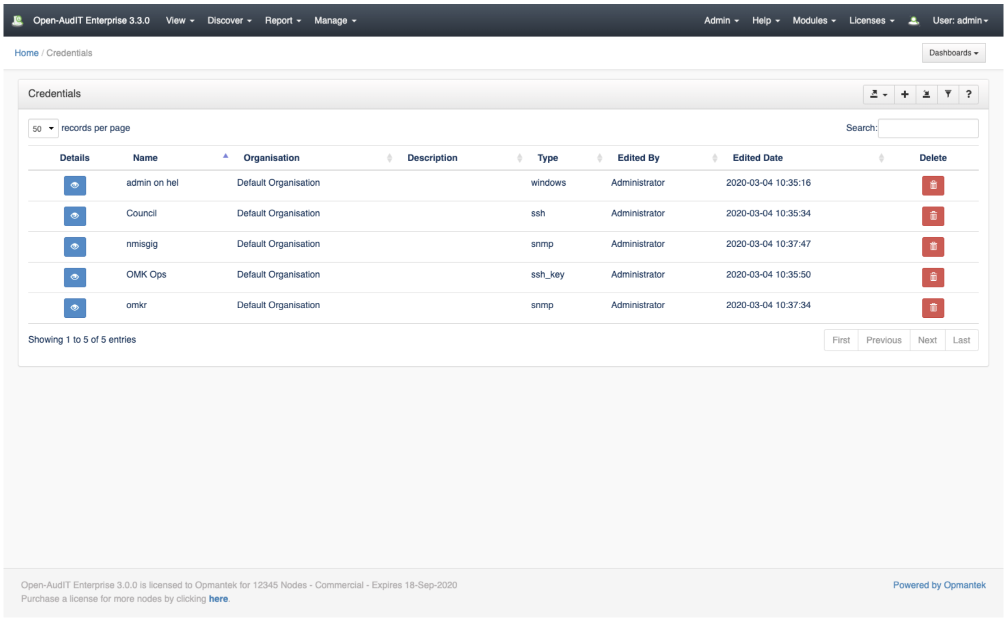
```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,328refbeif03
duvbwuidnpowmpowenciubviencpomcpoenrfurehoiernfporjfoierhiuebvvn
dvkjeekjvlfkvlfbvienvpoemvpoenviuberiovneporvmpoernvoiernvoiernv
9wI0nVfcdhhd8DExfgwFfWr2AoGaNYgE0TVUfRU21HQG8C+HoLysC1a4CaHsRgVy
DTzGJQhfKafu2G31wt12kTycTpujeO0EyRsa4kT0KPp+IDJRtkRmEJY3UG1Xg72P
jLZ/o2Ygz15ZT9GkNb9jyPCZMF3NJqL+Mz03ikKHDZvfOxA5P1XTPiXSVLzB1MJt
lgP2A3vlW/eaVeVhPa6Wo9gbDm/+PzDL+rT9ZK5K8sc1AcdIJ0m9OGCQtqpwSxEB
iJ07usXWXI4Cf4ex3+Oxeoineoifnoienfoiernfoiernfoermf[pef[pffed0DD
FsRSBmCbsCHrzGIqk8Maqh5gjPhkerneLlH40Jeloks2tkD72UT/bYWgpvTxzVUA
+LSVhR/Li+cGIebgKqKgE2sXmuIGn9UuqOvFbDudowRyrO9OtM1QsfresILmTKTA
VCNKEQExL1mhsUnr1paOOMs5vZ2oO3x0S7x+QXrWGye+QK9aquZ+IQ3Z4Lb130Q4
dfvneivnoiernvoirenvoinervionreoivnreoivnoiernvoiernv/pae,fefeff
W76aH+wxCuuSNWACvhfDcYXjp4dP3AD2EiuIYlvkIl0cwNrX9tmZyG37qaYDPCdW
ikmDolK6tepoqS05js+RouUHvZEZg3jBxkTkI0FB+JJcOvzl9ixf3Ce/CeWkcCrb
6oGjyNEOqoFDoceIUFZGOw4tsNySyqON9a0TuToPCX5rQd57fPabnl6Tl6XUCqwz
1DZ2HyVm+k4DAzLx2BoA5urWzdlniuberovbeirvbifevnienvirenviernviner
ovneiuvnieufvbiuerbviunviunervioneroivnoiernvoiernvoinervoineroi
b2cmcEETwXZEzVudljkOMt7d8F2fWVcFPYSh/wneI1A7kPiWw9B1T3SRTiLS8fv4
t8pr/GvAsevzRe7q9oMAfnAYnBuWCzN++JitjgwRhj1n/WmqxqfPuRwcZ/Y8cHZb
fSuJdcdlGBx7KH/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.

.



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

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 schema for the database is below. It can also be found in the application if the user has database::read permission by going to menu: Admin -> Database -> List Tables, then clicking on the "credentials" table.

```
CREATE TABLE `credentials` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `name` varchar(200) NOT NULL DEFAULT '',
  `description` text NOT NULL,
  `type` enum
('aws','basic_auth','cim','ipmi','mysql','netapp','other','snmp','snmp_v3','sql_server','ssh','ssh_key','vmwa
re','web','windows') NOT NULL DEFAULT 'other',
  `credentials` text NOT NULL,
  `org_id` int(10) unsigned NOT NULL DEFAULT '1',
  `edited_by` varchar(200) NOT NULL DEFAULT '',
  `edited_date` datetime NOT NULL DEFAULT '2000-01-01 00:00:00',
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

Example Database Entry

Credentials are stored in the database in the "credentials" table. A typical entry will look as below.

NOTE - org_id is not used at present.

```
         id: 26
       name: Mark at home
description:
       type: ssh
credentials:
12389RdkKYFQrwZF3bfBeHSyHhAXdIbh2i22MsSdsnpCO72lQGoRnlpKfW+AETgmCOhIAe3NQmRucMncsaGTyeczshUCuv1iqTuk8ZT3sHyGk
DPkq/FiX1z6guUL123/
     org_id: 0
  edited_by: Administrator
edited_date: 2017-06-08 10:11:12
```

API / Web Access

You can access the /credentials collection using the normal Open-AudIT JSON based API. Just like any other collection. Please see the API documentation for further details.

When requesting a credentials details via the API, the credentials section will be decrypted.

API Routes

Request Method	ID	Action	Resulting Function	Permission Required	URL Example	Notes	Example Response
POST	n		create	credentials::create	/credentials	Insert a new credentials entry.	credentials_create.json
GET	y		read	credentials::read	/credentials/{id}	Returns a credentials details.	credentials_read.json
PATCH	y		update	credentials::update	/credentials/{id}	Update an attribute of a credentials entry.	credentials_patch.json
DELETE	y		delete	credentials::delete	/credentials/{id}	Delete a credentials entry.	credentials_delete.json
GET	n		collection	credentials::read	/credentials	Returns a list of credentials.	credentials_collection.json

Web Application Routes

Request Method	ID	Action	Resulting Function	Permission Required	URL Example	Notes
GET	n	create	create_form	credentials::create	/credentials/create	Displays a standard web form for submission to POST /credentials.
GET	n	import	import_form	credentials::create	/credentials/import	Displays a standard web form for submission to POST /credentials/import.
POST	n	import	import	credentials::create	/credentials/import	Import multiple credentials using a CSV.