Authenticating using the internal user

Configuration · https://2yetis.net/docs/changing-the-admin-password/

The default authentication system used by uvuyo is the internal user. It is the easiest way to setup authentication, but in an enterprise environment you would prefer setting up LDAP to authenticate user. This article describes how to administer the internal user.

Note
By default this internal user is active, which means that you can use the internal user to login to the system. You can switch on and off the internal user authentication by using the property uvuyo.security.local.enabled. If you set the property to true you can authenticate to the system using the internal user. If you set the property to false the internal user can't authenticate.

If you have switched on the authentication with the internal user, This user will be checked first. Which means that it is not overwritten by any other authentication method.

Changing the internal users password

The default user is the admin user and when installed the default password for the admin user is 2Yetis. If you are using the internal user to authenticate it is strongly recommended to change the password for the user to make your system more secure.

To change the password of the admin user you first need to encode the new password. Therefor you need to use the rest API to encode the password. Running a Rest call is done in two steps. First you need to Authenticate yourself using a REST call. In return you will receive a token which you can use in sequent REST calls.

Login

To authenticate yourself you need to run the following curl call:

```
curl --request POST \
  --url https://<url>/uvuyo/api/v1.0/login \
  --header 'Content-Type: application/json' \
  --data '{
"userid": "<userid>",
```

```
"password": "<password>"
}'
```

You will need to replace the <userid> and <password> with the username and password of your system. The default userid and password when uvuyo is freshly installed are admin/2Yetis.

Also you need to set the correct url to your installation.

In return you will receive a token that you the use in the authentication header of subsequent REST calls.

Note
In this article we are using curl to run REST commands. You are of course not restricted to use curl but also can use other REST frontends like postman or insomnia

Sample Response:

```
{
"token": "eyJhbGciOiJIUzUxMiJ9.eyJyb2xlIjpb..."
}
```

Encode the password

To now encode a password you need to run the following curl command:

```
curl --request GET \
  --url 'https://uvuyo.on2yetis.net/uvuyo/api/v1.0/encode?password=<password>' \
  --header 'Authorization: Bearer <beared>
```

You will need to replace <password> with the password you want to encode. Also you need to change <bearer> in the authorization of the header to the token you received during the login call described above.

Sample Response:

```
xhi6JKF08G/MtICgLNmrTHy87cKC013o+KFCzmzwOzQ=
```

Setting the password in the default.properties file

Copy the password you received and edit the $UVUYO_HOME/etc/default.properties file. Where $UVUYO_HOME is the directory where you installed uvuyo. The file should exist since it also

contains your license key. If it does not exist, you would need to create the file. When creating the file make sure that it only can be read by the user running the uvuyo node, since it might contain security relevant information - like the encrypted password you are just about to set.

Add the following entry to the $UVUYO_HOME/etc/default.properties file or find the entry and override the value:

```
uvuyo.user.password=<value>
```

You will need to replace <value> with the value you received from the curl command when encoding the password.

After changing the admin password you need to restart the uvuyo node.