

# YNQ Password Utility

**YNQ 1.3.0**

Document version 1.0

## Table of Contents

<b>1</b>	<b>INTRODUCTION.....</b>	<b>3</b>
<b>2</b>	<b>COMPILATION .....</b>	<b>4</b>
2.1	COMPILE ON WINDOWS .....	4
2.2	COMPILE ON LINUX .....	4
<b>3</b>	<b>PLAIN TEXT TO HASH CONVERTOR .....</b>	<b>5</b>
3.1	SCOPE .....	5
3.2	PROCEDURE .....	5
3.3	EXAMPLE.....	5
<b>4</b>	<b>PASSWORD ENCRYPTION TOOL.....</b>	<b>6</b>
4.1	SCOPE .....	6
4.2	PROCEDURE .....	6
4.3	EXAMPLE.....	6

## 1 Introduction

YNQ password utility contains two tools, one to generate hashes for Password List File and the other to encrypt the default password which presents in Common Configuration File.

## 2 Compilation

Executable file name is “nqpwd.exe”.

### 2.1 *Compile on Windows*

Open Visual Studio developer command prompt and run the following command:

```
"cl nqpwd.c md4.c des.c aesgcm.c".
```

### 2.2 *Compile on Linux*

Open terminal and run the following command:

```
"cc -o nqpwd nqpwd.c md4.c des.c aesgcm.c".
```

### 3 Plain text to hash convertor

This tool converts plain text passwords to hashed passwords for Password List File. The tool checks the Password List File for plain text passwords, hashes these passwords using YNQ hash mechanism, and then rewrites the hashed passwords in the Password List File in their correct location.

#### 3.1 Scope

Password List File contains user names, their corresponding passwords and User ID's. SMB clients can establish connection with YNQ server using credentials from this list.

#### 3.2 Procedure

The program queries for the full name of Password List File (including full path), then it performing the conversion on this file. Before running this program the administrator has to edit the Password List File, he can directly set or change user passwords, by simply writing plain-text passwords. The tool assumes that the Password List File is correctly formatted. Even if an entry is not formatted correctly, it will not modify it. Therefore, it is the user's responsibility to format the Password List File correctly.

#### 3.3 Example

Assuming that the path to **nqpwd.exe** is "**C:\nqpwd.exe**" and that the path to Password List File is "**C:\pwd\_list.txt**". Also assuming that Password List File contains the following entries (note that the passwords are already hashed):

```
ADMINISTRATOR:598ddce2660d3193aad3b435b51404ee:501
USER1:e52cac67419a9a224a3b108f3fa6cb6d:502
USER2:01fc5a6be7bc6929aad3b435b51404ee:504
```

If the user wants to change the **USER1** password to **newpassword**, perform the following steps:

1. Open the **C:\pwd\_list.txt** file and edit it as follows:

```
ADMINISTRATOR:598ddce2660d3193aad3b435b51404ee:501
USER1:newpassword:502
USER2:01fc5a6be7bc6929aad3b435b51404ee:504
```

2. Save the file and close it.

3. At the command prompt, type 1 to select plain text to hash convertor, then type the path to Password List File:

```
Please enter full file name of Password List File: C:\pwd_list.txt
```

4. Reopen the file and the passwords is hashed as follows:

```
ADMINISTRATOR:598ddce2660d3193aad3b435b51404ee:501
USER1:09eeab5aa415d6e4d408e6b105741864:502
USER2:01fc5a6be7bc6929aad3b435b51404ee:504
```

5. Default user and password at the **pwd\_list.txt** is:

```
User: administrator
```

```
Password: password
```

## 4 Password encryption tool

This tool encrypt default password for PASSWORD parameter which presents in Common Configuration File. This file contains the default credentials – user name and password. This tool allows to encrypt that password in order to achieve better security.

### 4.1 Scope

Common Configuration file is used both by YNQ Client and YNQ Server to initialize several parameters. USER and PASSWORD parameters can be used by YNQ Server to join domain and can be also used by YNQ client as default credentials to authenticate against SMB Server.

### 4.2 Procedure

the program queries for user name and password, then it generates a string containing the encrypted password. The encrypted password should be copied to Common Configuration File, specifically to PASSWORD parameter. The program adds the postfix “:E” to the string, it indicates that the password is encrypted.

### 4.3 Example

After typing 2 to select password encryption tool, the program queries for user name and password:

```
Please enter user name: user1
```

```
Please enter password to encrypt: 12345
```

Then the program generate and print out the encrypted password:

```
Encrypted password: 77a4ffd6e5abb2c5f1cb602bc09461aa18770b10922d5afa6d:E
```

Then the user should copy this encrypted password into the value of PASSWORD parameter that presents in Common Configuration File.