Maven Credentials Cannot Be Used For NTLM Authentication Hatasının Çözümü

Maven uygulamasında **proxy** ayarlarınızı yapmanıza rağmen **NTLM** ile ilgili hata alıyorsanız **Cntlm** programını indirip kurarak, bu problemden kurtulabiliriz. Bunun için yapılması gereken bazı ayarlar vardır.
Cntlm programı ile maven proxy server bağlantı sorunu çözülmektedir. Bu programı indirmek için lütfen **tıklayınız**

Kurulum işlemi tamamlandıktan sonra Program Files klasöründen programın kurulu olduğu klasörü açınız **(C:\Program Files**\Cntlm). Eğer bu klasör içinde **cntlm.ini** dosyası yok ise boş bir **cntlm.ini** dosyası yarattıktan sonra aşağıdaki kodları yapıştırınız:

Not: Linux işletim sistemlerinde cntlm dosyası **conf** uzantılıdır.

```
#
# Cntlm Authentication Proxy Configuration
#
# NOTE: all values are parsed literally, do NOT escape spaces,
# do not quote. Use 0600 perms if you use plaintext password.
#

Username    example
Domain     com

# NOTE: Use plaintext password only at your own risk
# Use hashes instead. You can use a "cntlm -M" and "cntlm -H"
# command sequence to get the right config for your environment.
# See cntlm man page
# Example secure config shown below.
# PassLM         1AD35398BE6565DDB5C4EF70C0593492
# PassNT         77B9081511704EE852F94227CF48A793
### Only for user 'testuser', domain 'corp-uk'
# PassNTLMv2     D5826E9C665C37C80B53397D5C07BBCB

# Specify the netbios hostname cntlm will send to the parent
# proxies. Normally the value is auto-guessed.
#
# Workstation netbios_hostname

# List of parent proxies to use. More proxies can be defined
# one per line in format <proxy_ip>:<proxy_port>
#
Proxy     10.100.10.10:8080

# List addresses you do not want to pass to parent proxies
# * and ? wildcards can be used
#
NoProxy     localhost, 127.0.0.*, 10.*, 192.168.*

# Specify the port cntlm will listen on
# You can bind cntlm to specific interface by specifying
# the appropriate IP address also in format <local_ip>:<local_port>
# Cntlm listens on 127.0.0.1:3128 by default
#
Listen     3128

# If you wish to use the SOCKS5 proxy feature as well, uncomment
# the following option. It can be used several times
# to have SOCKS5 on more than one port or on different network
# interfaces (specify explicit source address for that).
#
# WARNING: The service accepts all requests, unless you use
# SOCKS5User and make authentication mandatory. SOCKS5User
# can be used repeatedly for a whole bunch of individual accounts.
#
#SOCKS5Proxy    8010
#SOCKS5User dave:password

# Use -M first to detect the best NTLM settings for your proxy.
# Default is to use the only secure hash, NTLMv2, but it is not
# as available as the older stuff.
#
# This example is the most universal setup known to man, but it
# uses the weakest hash ever. I won't have it's usage on my
```

```
# conscience. :) Really, try -M first.
#
#Auth     LM
#Flags     0x06820000

# Enable to allow access from other computers
#
#Gateway    yes

# Useful in Gateway mode to allow/restrict certain IPs
# Specifiy individual IPs or subnets one rule per line.
#
#Allow     127.0.0.1
#Deny     0/0

# GFI WebMonitor-handling plugin parameters, disabled by default
#
#ISAScannerSize     1024
#ISAScannerAgent    Wget/
#ISAScannerAgent    APT-HTTP/
#ISAScannerAgent    Yum/

# Headers which should be replaced if present in the request
#
#Header     User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows 98)

# Tunnels mapping local port to a machine behind the proxy.
# The format is <local_port>:<remote_host>:<remote_port>
#
#Tunnel     11443:remote.com:443
```

Bu dosyada **şifre** kısmı eksiktir. **Cntlm** programının kurulduğu Program Files klasöründeki yerinde, aşağıdaki komutu, **color="#ff0000">Konsol(CMD) ekranından** açarak çalıştırmak gereklidir:

```
cntlm -I -M http://test.com
```

Daha sonra konsol ekranında çıkan **PassLM**, **PassNT** veya **PassNTLMv2** değerini aşağıdaki gibi **cntlm.ini** dosyasına eklemek gerekiyor:

```
PassLM          1AD35398BE6565DDB5C4EF70C0593492
PassNT          77B9081511704EE852F94227CF48A793
PassNTLMv2      D5826E9C665C37C80B53397D5C07BBCB
```

Konfigürasyonun son hali ise şu şekilde olmalıdır:

```
#
# Cntlm Authentication Proxy Configuration
#
# NOTE: all values are parsed literally, do NOT escape spaces,
# do not quote. Use 0600 perms if you use plaintext password.
#

Username    example
Domain     com

# NOTE: Use plaintext password only at your own risk
# Use hashes instead. You can use a "cntlm -M" and "cntlm -H"
# command sequence to get the right config for your environment.
# See cntlm man page
# Example secure config shown below.
PassLM          1AD35398BE6565DDB5C4EF70C0593492
PassNT          77B9081511704EE852F94227CF48A793
### Only for user 'testuser', domain 'corp-uk'
PassNTLMv2      D5826E9C665C37C80B53397D5C07BBCB

# Specify the netbios hostname cntlm will send to the parent
# proxies. Normally the value is auto-guessed.
#
# Workstation netbios_hostname
```

```
# List of parent proxies to use. More proxies can be defined
# one per line in format <proxy_ip>:<proxy_port>
#
Proxy     10.100.10.10:8080

# List addresses you do not want to pass to parent proxies
# * and ? wildcards can be used
#
NoProxy     localhost, 127.0.0.*, 10.*, 192.168.*

# Specify the port cntlm will listen on
# You can bind cntlm to specific interface by specifying
# the appropriate IP address also in format <local_ip>:<local_port>
# Cntlm listens on 127.0.0.1:3128 by default
#
Listen     3128

# If you wish to use the SOCKS5 proxy feature as well, uncomment
# the following option. It can be used several times
# to have SOCKS5 on more than one port or on different network
# interfaces (specify explicit source address for that).
#
# WARNING: The service accepts all requests, unless you use
# SOCKS5User and make authentication mandatory. SOCKS5User
# can be used repeatedly for a whole bunch of individual accounts.
#
#SOCKS5Proxy    8010
#SOCKS5User dave:password

# Use -M first to detect the best NTLM settings for your proxy.
# Default is to use the only secure hash, NTLMv2, but it is not
# as available as the older stuff.
#
# This example is the most universal setup known to man, but it
# uses the weakest hash ever. I won't have it's usage on my
# conscience. :) Really, try -M first.
#
#Auth     LM
#Flags     0x06820000

# Enable to allow access from other computers
#
#Gateway    yes

# Useful in Gateway mode to allow/restrict certain IPs
# Specifiy individual IPs or subnets one rule per line.
#
#Allow     127.0.0.1
#Deny     0/0

# GFI WebMonitor-handling plugin parameters, disabled by default
#
#ISAScannerSize     1024
#ISAScannerAgent    Wget/
#ISAScannerAgent    APT-HTTP/
#ISAScannerAgent    Yum/

# Headers which should be replaced if present in the request
#
#Header     User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows 98)

# Tunnels mapping local port to a machine behind the proxy.
# The format is <local_port>:<remote_host>:<remote_port>
#
#Tunnel     11443:remote.com:443
```

Bu adımları tamamladıktan sonra son yapılması gereken **maven** proxy ayarlarıdır:
m2 klasöründe eğer **settings.xml** isimli dosya yoksa bu isimde dosya yarattıktan sonra aşağıdaki gibi aşağıdaki kodları ekleyip kendi username ve password kısımlarını güncelleyin:

```
<settings xmlns="http://maven.apache.org/SETTINGS/1.0.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://maven.apache.org/SETTINGS/1.0.0
```

```
                      http://maven.apache.org/xsd/settings-1.0.0.xsd">
<proxies>
<proxy>
   <active>true</active>
   <protocol>http</protocol>
   <host>127.0.0.1</host>
   <port>3128</port>
  </proxy>
</proxies>
</settings>
```

Not: Dikkat edilecek olursa port 3128 oldu. Yani **cntlm.ini** dosyasındaki **Listen 3128** olarak belirtildiği gibi. Ayrıca kullanılan host ise **localhost** ip'sidir.

Tüm bu işlemler tamamlandıktan sonra artık maven **proxy** server üzerinden bağlanabilecektir.