

# VPN mit Clientzertifikat Fortigate

```
fw01 # diagnose debug disable

fw01 # config user peer

fw01 (peer) # show

fw01 (peer) # edit testbla
new entry 'testbla' added

fw01 (testbla) # set
ca                Peer certificate CA (CA name in local).
cn                Peer certificate common name.
cn-type          Peer certificate common name type.
ldap-mode        Peer LDAP mode.
ldap-password    Password for LDAP server bind.
ldap-server      LDAP server for access rights check.
ldap-username    Username for LDAP server bind.
mandatory-ca-verify Enable/disable mandatory CA verify.
ocsp-override-server OSCP server.
subject          Peer certificate name constraints.
two-factor       Enable/disable 2-factor authentication (certificate
+ password).
```

```
fw01 (testbla) # set mandatory-ca-verify enable

fw01 (testbla) # set ca
<string>      please input string value
CA_Cert_1    ca
CA_Cert_2    ca
Fortinet_CA  ca
Fortinet_CA2  ca
PositiveSSL_CA  ca

fw01 (testbla) # set ca CA_Cert_1

fw01 (testbla) # set cn
<string>      please input string value

fw01 (testbla) # set cn-type
FQDN          Fully Qualified Domain Name.
email         Email address.
ipv4          IPv4 address.
ipv6          IPv6 address.
string        Normal string.

fw01 (testbla) # set cn-type string
```

```
fw01 (testbla) # set cn testbla

fw01 (testbla) # set
ca Peer certificate CA (CA name in local).
cn Peer certificate common name.
cn-type Peer certificate common name type.
ldap-mode Peer LDAP mode.
ldap-password Password for LDAP server bind.
ldap-server LDAP server for access rights check.
ldap-username Username for LDAP server bind.
mandatory-ca-verify Enable/disable mandatory CA verify.
ocsp-override-server OSCP server.
subject Peer certificate name constraints.
two-factor Enable/disable 2-factor authentication (certificate
+ password).

fw01 (testbla) # set two-factor enable

fw01 (testbla) # set
ca Peer certificate CA (CA name in local).
cn Peer certificate common name.
cn-type Peer certificate common name type.
ldap-mode Peer LDAP mode.
ldap-password Password for LDAP server bind.
ldap-server LDAP server for access rights check.
ldap-username Username for LDAP server bind.
mandatory-ca-verify Enable/disable mandatory CA verify.
ocsp-override-server OSCP server.
passwd User password.
subject Peer certificate name constraints.
two-factor Enable/disable 2-factor authentication (certificate
+ password).

fw01 (testbla) # set passwd

incomplete command in the end
Command fail. Return code -160

fw01 (testbla) # set passwd 1234567

fw01 (testbla) # end

fw01 # config user peer

fw01 (peer) # show
config user peer
  edit "testbla"
    set ca "CA_Cert_1"
    set cn "testbla"
    set mandatory-ca-verify enable
```

```
    set two-factor enable
    set passwd ENC
NeMC01Dha7ZqzsoTiwDNNu4hyjHmTly3B2wbyvf3i4v8unf4vH1iNl1BwyJkv3/1lqMcVPrSlS7N
ieSeDuInUc7YUyh/Jegw3sSsX6J2hn8xocsLt4xczedDenbJLWRgj0UVHrR+XrmTdr+4sZx5WqjS
yPU8V53iDBv/9sLiA==
    next
end

fw01 (peer) #
fw01 (peer) # exit
please use 'end' to return to root shell

fw01 (peer) # next
Unknown action 0

fw01 (peer) # end
```

From:  
<https://deepdoc.at/dokuwiki/> - **DEEPDOC.AT - enjoy your brain**

Permanent link:  
[https://deepdoc.at/dokuwiki/doku.php?id=firewalls:fortigate:vpn\\_mit\\_clientzertifikat](https://deepdoc.at/dokuwiki/doku.php?id=firewalls:fortigate:vpn_mit_clientzertifikat)

Last update: **2017/04/03 01:23**

