

Configuration Tip: How to configure FortiOS SSL VPN with FortiToken

Scope:-

FortiOS v4.3.0 and above.

SSL VPN Client v4.0.2143 and above.

Network Configuration

WAN IP : 192.168.140.216/23

Internal IP: 10.129.0.216/23

SSLVPN Tunnel range: 192.168.168.100-200

1. In User > FortiToken > FortiToken > Create New > enter the serial number of the FortiToken and click on '+' symbol, and click OK.



The screenshot displays the FortiGate 200B web management interface. The left sidebar shows a navigation tree with 'User' selected, and 'FortiToken' highlighted under the 'User' category. The main content area is titled 'Add new FortiToken' and contains a 'Serial Number' input field with a redacted value and a green '+' icon. Below the input field, there is a text prompt: 'You can also import multiple FortiTokens simultaneously from a file.' and an 'Import Multiple' button. At the bottom of the dialog, there are 'OK' and 'Cancel' buttons. The top of the interface includes the 'FortiGate 200B' logo, 'Help' and 'Logout' icons, and the 'FORTINET' logo.

- To activate the FortiToken serial number, the FortiToken will communicate with FortiGuard Servers and validate the license, once validated the status is shown as Active.

<input type="checkbox"/>	Serial Number	Status	Drift	User	Ref.
<input checked="" type="checkbox"/>	[REDACTED]	Active	0		0

- Add a local user with Two-factor authentication and FortiToken:

FortiGate 200B Help Logout **FORTINET**

User

New User

User Name: fortitoken

Disable

Password: ●●●

Match user on LDAP server: [Please Select]

Match user on RADIUS server: [Please Select]

Match user on TACACS+ server: [Please Select]

Enable Two-factor Authentication

Deliver Token Code by:

FortiToken: [REDACTED]

Email to: [REDACTED]

SMS: (Mobile Provider) [REDACTED] (Phone Number)

Add this user to groups

OK Cancel

Enable the Two factor authentication, and select the FortiToken serial number which has already been created.

4. Add the local user to the SSL VPN User Group

The screenshot displays the FortiGate 200B web management interface. The top navigation bar includes the FortiGate 200B logo, a Help icon, a Logout icon, and the Fortinet logo. The left sidebar contains a tree view of system components, with 'User' expanded to show 'User Group' selected. The main panel is titled 'New User Group' and contains the following configuration options:

- Name:** sslvpngp
- Type:** Firewall (selected), Fortinet Single Sign-On(FSSO)
- Allow SSL-VPN Access:** full-access
- Available Users:** - Local Users - (guest, test)
- Members:** - Local Users - (fortitoken)

At the bottom of the configuration area, there are 'OK' and 'Cancel' buttons.

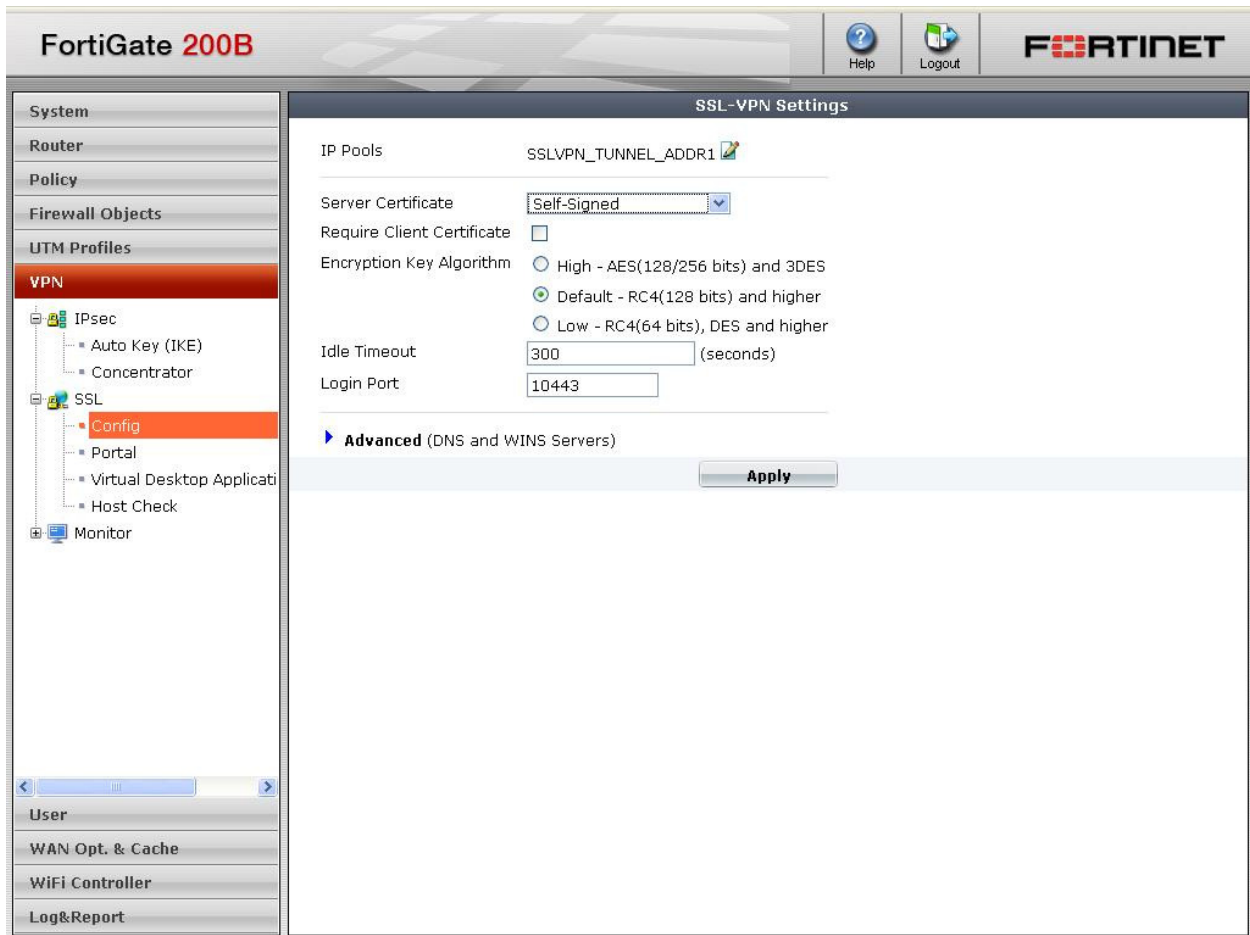
5. Specify the SSL VPN address range as shown in Firewall Objects> Address:-

The screenshot shows the FortiGate 200B web interface. The left sidebar contains a navigation tree with 'Firewall Objects' selected, and 'Address' highlighted. The main content area displays a table of firewall objects.

	Name	Address/FQDN	Interface	Type	Ref.
<input type="checkbox"/>	all	0.0.0.0/0.0.0.0	Any	Subnet	3
<input type="checkbox"/>	internal	10.129.0.0/255.255.254.0	port10	Subnet	0
<input type="checkbox"/>	SSLVPN_TUNNEL_ADDR1	192.168.168.[100-200]	Any	IP Range	3

At the bottom of the interface, there is a pagination bar showing '1 / 1'.

6. Verify the SSL Config ensure that the IP Pools are applied.



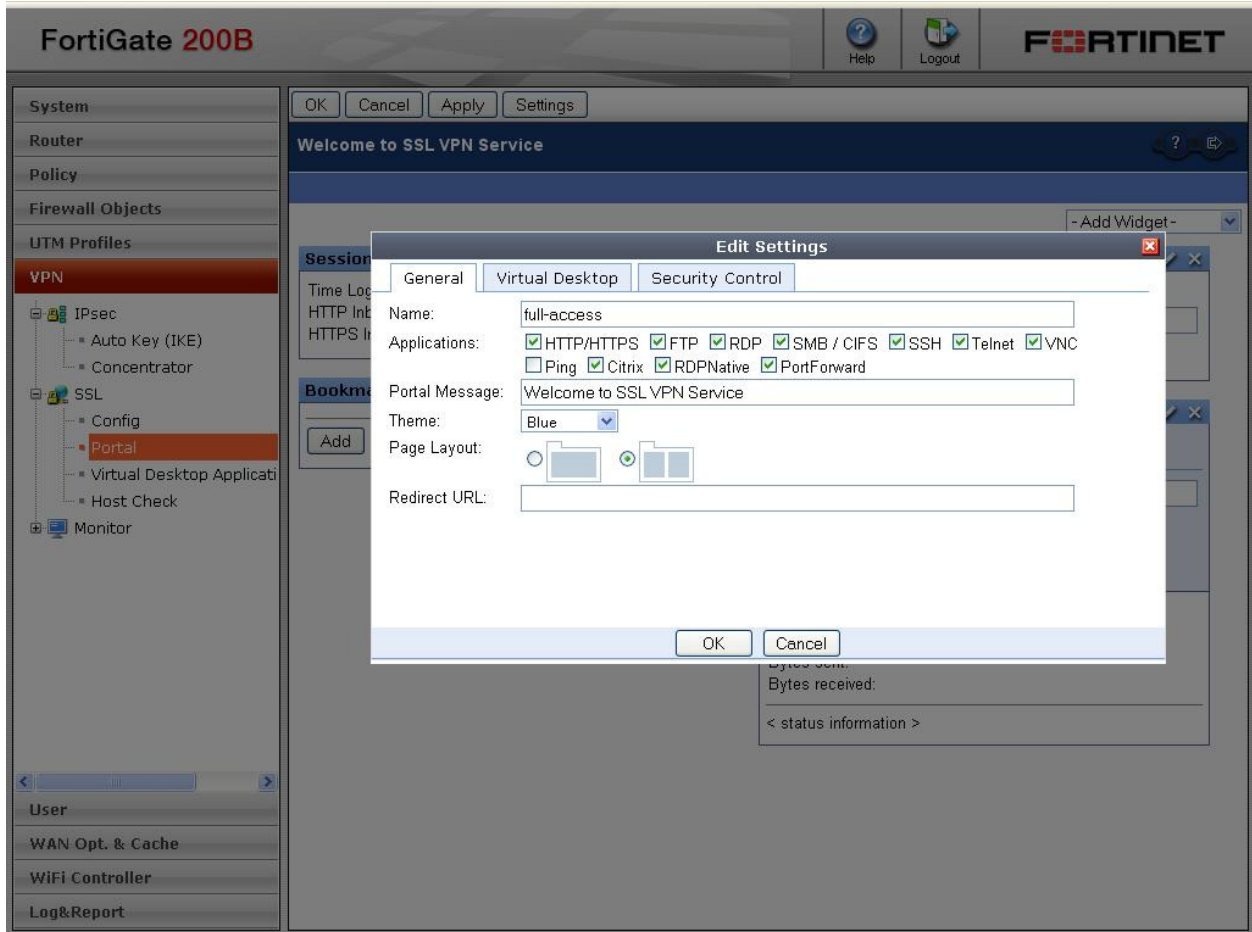
The screenshot displays the FortiGate 200B web interface. The top navigation bar includes the FortiGate 200B logo, a Help icon, a Logout icon, and the Fortinet logo. The left sidebar contains a tree view of configuration categories: System, Router, Policy, Firewall Objects, UTM Profiles, VPN (highlighted), User, WAN Opt. & Cache, WiFi Controller, and Log&Report. Under the VPN category, the following sub-items are listed: IPsec (with sub-items Auto Key (IKE) and Concentrator), SSL (with sub-items Config (highlighted), Portal, Virtual Desktop Application, and Host Check), and Monitor.

The main content area is titled "SSL-VPN Settings" and contains the following configuration fields:

- IP Pools: SSLVPN_TUNNEL_ADDR1
- Server Certificate: Self-Signed (dropdown menu)
- Require Client Certificate:
- Encryption Key Algorithm: Default - RC4(128 bits) and higher, High - AES(128/256 bits) and 3DES, Low - RC4(64 bits), DES and higher
- Idle Timeout: 300 (seconds)
- Login Port: 10443

Below these fields, there is an "Advanced (DNS and WINS Servers)" section with an "Apply" button.

7. Configure the SSL VPN Portal.



- System
- Router
- Policy
- Firewall Objects
- UTM Profiles
- VPN**
 - IPsec
 - Auto Key (IKE)
 - Concentrator
 - SSL
 - Config
 - Portal**
 - Virtual Desktop Application
 - Host Check
 - Monitor
- User
- WAN Opt. & Cache
- WiFi Controller
- Log&Report

OK Cancel Apply Settings

Welcome to SSL VPN Service

- Add Widget -

Session Information

Time Logged In:	0
HTTP Inbound/Outbound Traffic:	bytes / bytes
HTTPS Inbound/Outbound Traffic:	bytes / bytes

Connection Tool

Type: HTTP/HTTPS

Host:

Go

Bookmarks

Add Edit

Tunnel Mode

OK Cancel

Name: Tunnel Mode

IP Mode: Range User Group

IP Pools: SSLVPN_TUNNEL_ADDR1

Split Tunneling:

Connect Disconnect Refresh

Link status:

Bytes sent:

Bytes received:

< status information >

8. Add Static Route for destination network.

The screenshot displays the FortiGate 200B web management interface. At the top, the header shows 'FortiGate 200B' on the left and 'Help' and 'Logout' icons on the right, along with the 'FORTINET' logo. The left sidebar is titled 'System' and contains a tree view under 'Router' with sub-items: 'Static' (expanded), 'Static Route' (selected), 'Policy Route', and 'Settings'. Below this are other system categories: 'Dynamic' and 'Monitor'. At the bottom of the sidebar are buttons for 'Policy', 'Firewall Objects', 'UTM Profiles', 'VPN', 'User', 'WAN Opt. & Cache', 'WiFi Controller', and 'Log&Report'. The main content area is titled 'New Static Route' and contains the following configuration fields:

- Destination IP/Mask:
- Device:
- Gateway:
- Comments: 0/63

Below the fields are three buttons: 'Advanced...', 'OK', and 'Cancel'.

9. Configure Firewall Policies for SSLVPN authentication.

The screenshot displays the FortiGate 200B web interface. The top navigation bar includes the FortiGate 200B logo, a Help icon, a Logout icon, and the Fortinet logo. The left sidebar shows a tree view with 'System' expanded to 'Router' and 'Policy' selected. Below 'Policy' are sub-items: 'Policy', 'DoS Policy', 'Sniffer Policy', and 'Protocol Options'. At the bottom of the sidebar are 'Firewall Objects', 'UTM Profiles', 'VPN', 'User', 'WAN Opt. & Cache', 'WiFi Controller', and 'Log&Report'.

The main content area is titled 'Edit Policy'. It contains the following configuration fields:

- Source Interface/Zone: port9
- Source Address: all
- Destination Interface/Zone: port10
- Destination Address: internal
- Action: SSL-VPN

Below these fields are two checkboxes:

- SSL Client Certificate Restrictive
- Configure SSL-VPN Users

The 'Configure SSL-VPN Users' checkbox is checked, and an 'Add' button is visible above a table. The table has the following data:

Rule ID	User Group	Service	Schedule	UTM	Logging
1	sslvpngrp	ANY	always		

Below the table is another checkbox:

- Customize Authentication Messages

At the bottom, there is a 'Comments' field with the placeholder text 'Write a comment...' and a character count '0/63'. Two buttons, 'OK' and 'Cancel', are located at the bottom of the configuration area.

FortiGate 200B

Help Logout FORTINET

System Router Policy

Policy

- Policy
- DoS Policy
- Sniffer Policy
- Protocol Options

Monitor

Firewall Objects

UTM Profiles

VPN

User

WAN Opt. & Cache

WiFi Controller

Log&Report

Create New Clone Delete Column Settings Filter Settings Section View Global View

Seq.#	Source	Destination	Authentication	Schedule	Service	Action
port10 -> port9 (1)						
port10 -> ssl.root (1)						
2	internal	SSLVPN_TUNNEL_ADDR1		always	ANY	ACCEPT
port9 -> port10 (2)						
3	all	testvip		always	ANY	ACCEPT
4	all	internal				SSL-VPN
ssl.root -> port10 (1)						
5	SSLVPN_TUNNEL_ADDR1	internal		always	ANY	ACCEPT
Implicit (1)						

NB : Ensure to create policies from ssl.root (ssl vpn interface) to internal and vice-verser.

For more information on SSL VPN configuration examples consult the FortiOS v4.0 MR3 Handbook.

FortiGate CLI configuration

```
config user fortitoken
  edit "FTKxxxxxxxxxxxxx"
    set seed
    "rRw6EGBcSdUjc2W4kov0Rcqfdert02mQPpaRrLabtTVxQ0sWo/1zcZJ/tIY="
  next
end
```

```
config vpn ssl settings
  set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
end
config vpn ssl web portal
  edit "full-access"
    set allow-access web ftp smb telnet ssh vnc rdp citrix rdpnative
portforward
  set heading "Welcome to SSL VPN Service"
  set page-layout double-column
  config widget
    edit 4
      set name "Session Information"
      set type info
    next
    edit 2
      set name "Bookmarks"
      set allow-apps web ftp smb telnet ssh vnc rdp citrix
rdpnative portforward
  next
  edit 3
    set name "Connection Tool"
    set type tool
    set column two
    set allow-apps web ftp smb telnet ssh vnc rdp citrix
rdpnative portforward
  next
  edit 1
    set name "Tunnel Mode"
    set type tunnel
    set column two
    set tunnel-status enable
    set ip-pools "SSLVPN_TUNNEL_ADDR1"
  next
end
next
end
```

```
config user local
  edit "fortitoken"
    set fortitoken " FTKxxxxxxxxxxxxx "
    set two-factor fortitoken
    set type password
    set passwd ENC
+xc8aV7kckEqzxkrAO2V2ZTqSWobo8duiTTWSbLkReJFrU29xIRyTQXyOAxhXzoXXeSiv0rzg/Aff
Imq5zvdKw7fwl4uBMED7+NlivrUfpx3FMoS
    next
end

config user group
  edit "sslvpnggrp"
    set sslvpn-portal "full-access"
    set member "fortitoken"
  next
end
```

```
config router static
  edit 2
    set device "ssl.root"
    set dst 192.168.168.0 255.255.255.0
  next
end
```

```
config firewall policy
  edit 4
    set srcintf "port9"
    set dstintf "port10"
    set srcaddr "all"
    set dstaddr "internal"
    set action ssl-vpn
    set identity-based enable
    config identity-based-policy
      edit 1
        set schedule "always"
        set logtraffic enable
        set groups "sslvpnggrp"
        set service "ANY"
      next
    end
  next
end

config firewall policy
  edit 5
    set srcintf "ssl.root"
    set dstintf "port10"
    set srcaddr "SSLVPN_TUNNEL_ADDR1"
    set dstaddr "internal"
    set action accept
    set schedule "always"
    set service "ANY"
    set logtraffic enable
  next
end

config firewall policy
  edit 6
    set srcintf "port10"
    set dstintf "ssl.root"
    set srcaddr "internal"
    set dstaddr "SSLVPN_TUNNEL_ADDR1"
    set action accept
    set schedule "always"
    set service "ANY"
  next
end
```

FortiToken Authentication

There are 3 ways to authenticate using FortiToken and SSL VPN:-

- Use SSL VPN Standalone Client with Username/Password/FortiToken Code.
- Use Web-access with Username/Password , then FortiOS will prompt for the FortiToken Code.
- Use Web-access with Username/Password+FortiToken Code.

1. SSL VPN client configuration:

FortiClient Connect SSLVPN

Connection Name:

Server Address: 192.168.140.216:10443

Username: fortitoken

Password:

A six-digit numeric code (FortiToken Code) is required for SSL-VPN login authentication.

FortiToken Code:

(Please input the FortiToken code here)

Login Cancel

Connection

Status: Connecting...(48) Bytes Sent: 0

Duration: 00:00:00 Bytes Received: 0

Settings... Connect Disconnect Exit

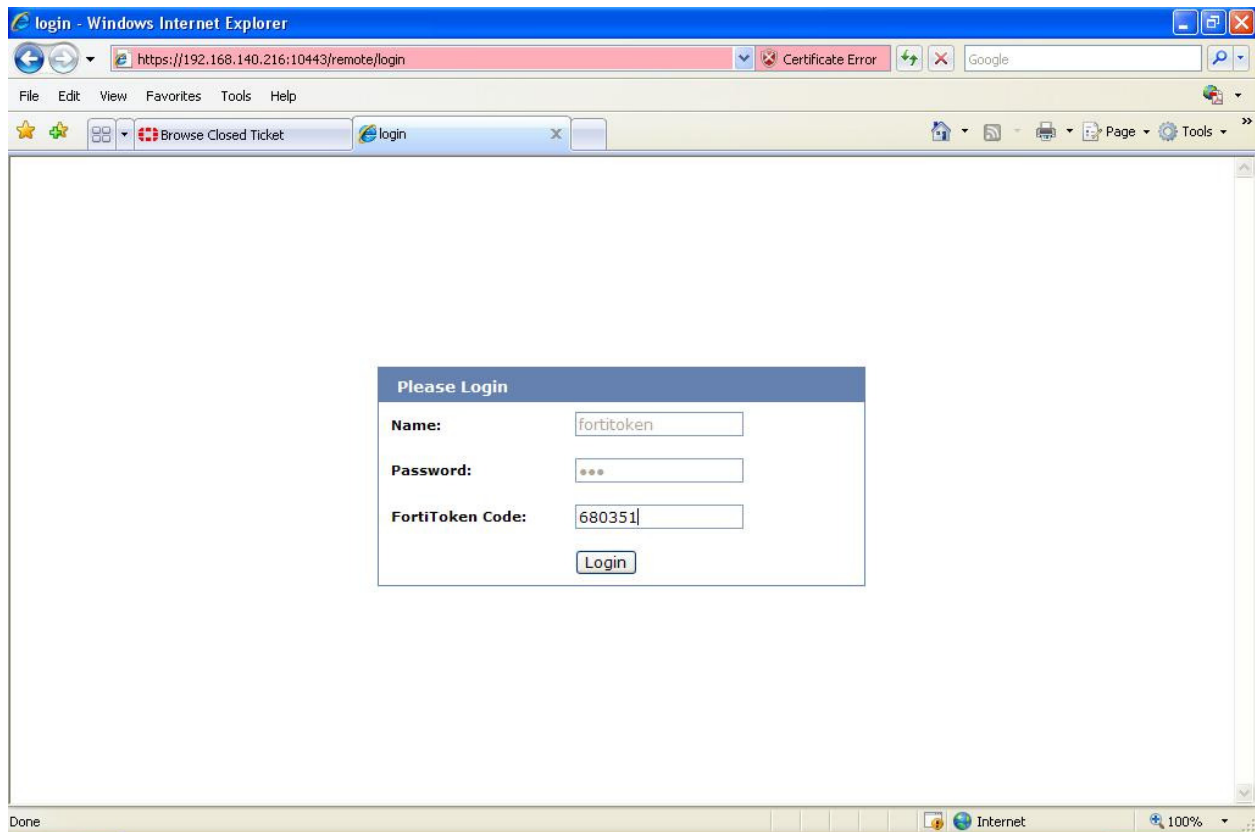
FortiClient Connect SSLVPN

FortiClient Connect SSLVPN Version 4.0.2143

Copyright (C) 2004 - 2011 Fortinet Inc. All rights reserved. OK

2.Web-Access authentication

1. Enter user name and password and click login, the FortiGate will prompt for the FortiToken code.



2. Enter Username and password as password +FortiToken Code



The screenshot shows the "Please Login" form from the previous image. The "Name" field now contains the text "tuser". The "Password" field is masked with dots. The "Login" button is still present at the bottom of the form.