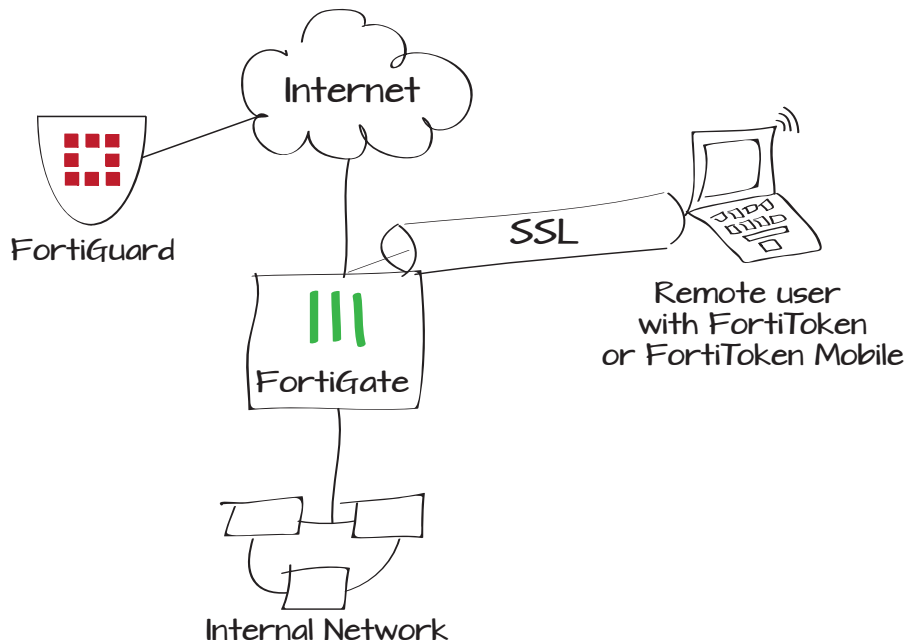


# Using two-factor authentication with SSL VPN

An SSL VPN can use two-factor user authentication for enhanced security. In this example, a remote user uses FortiClient to connect to a private network behind a FortiGate unit. The FortiGate unit and FortiClient authenticate each other using a pre-shared key. The user is authenticated by User ID/password) plus a FortiToken token code.

1. Registering FortiToken with a FortiGate unit and FortiGuard
2. Adding two-factor authentication to the user's account
3. Defining an address for the internal network
4. Configuring the SSL VPN on the FortiGate unit.
5. Creating a security policy for SSL VPN users



## Registering FortiToken with a FortiGate unit and FortiGuard

Go to **User & Device > Two-factor Authentication > FortiTokens** and select **Create New**. Select the **Serial Number** field and enter the FortiToken serial number.

If you have several FortiTokens to add, you can list their serial numbers one per line in a text file and use the Import function.



FortiOS reports the serial number as invalid if you mistype it or if it is a duplicate.

Wait for the FortiGuard to validate your FortiToken's serial number. When you first enter the serial number its status is listed as **Pending**. When FortiGuard validates the serial number, the status changes to **Available**.



If this FortiToken has already been registered to another FortiGate unit, the Status column shows Error.

Type  Hard Token  Mobile Token

Comments  6/255

Serial Number

Type	Serial Number	Status	User	Drift	Comments
	FTK2000BQL7PJW13	Available		0	

## Adding two-factor authentication to the user's account

Go to **User & Device > User > User Definition** and open the user's account for editing.

Select **Enable Two-factor Authentication** and then select the FortiToken from the list. Select OK.

The screenshot shows the configuration page for a user named 'tbrown'. The 'User Name' field is filled with 'tbrown'. There are radio buttons for 'Disable', 'Password', 'Match user on LDAP server', 'Match user on RADIUS server', and 'Match user on TACACS+ server'. The 'Password' field is masked with '\*\*\*\*\*'. Below this is the 'Contact Info' section with an 'Email Address' field and a checked 'SMS' option. The 'SMS' section has radio buttons for 'FortiGuard Messaging Service' (selected) and 'Custom', with a 'Phone Number' field containing '613-555-1200'. The 'Enable Two-factor Authentication' section is checked, with a 'Token' dropdown menu showing 'FTK2000BQL7PJW13'. Below that is a list of groups with checkboxes: 'FortiGate\_Administrators', 'SslvpnGroup', 'WiFi\_users', 'full-time' (checked), and 'part-time'. At the bottom are 'OK' and 'Cancel' buttons.

## Defining an address for the internal network

Go to **Firewall Objects > Address > Addresses** and select **Create New**.

The VPN configuration and the firewall policy require a defined address for the Internal network.

The screenshot shows the configuration page for a new address named 'Local LAN'. The 'Category' is set to 'Address'. The 'Name' field is 'Local LAN'. The 'Color' field has a '[Change]' button. The 'Type' is set to 'Subnet'. The 'Subnet / IP Range' field contains '192.168.1.0/255.255.255.0'. The 'Interface' is set to 'Any'. The 'Show in Address List' checkbox is checked. The 'Comments' field contains 'Write a comment...'. At the bottom are 'OK' and 'Cancel' buttons.

## Creating a user group for SSL VPN users

Go to **User & Device > User > User Groups** and create a Firewall type user group, adding the users who will be permitted to use the SSL VPN.

## Configuring an SSL VPN web portal

Go to **VPN > SSL > Config**.

The default encryption will work with typical browsers.

The screenshot displays the configuration page for a user group in a Fortinet SSL VPN environment. The interface is organized into several sections:

- Name:** A text input field containing "full-time".
- Type:** Radio buttons for "Firewall" (selected), "Fortinet Single Sign-On (FSSO)", and "Guest".
- Members:** A list of three users: "tbrown", "jsmith", and "blee", each with a delete icon (X) and a plus icon (+).
- IP Pools:** A dropdown menu showing "SSLVPN\_TUNNEL\_ADDR1" with a delete icon (X) and a plus icon (+).
- Server Certificate:** A dropdown menu set to "Self-Signed".
- Require Client Certificate:** An unchecked checkbox.
- Encryption Key Algorithm:** Radio buttons for "High - AES(128/256 bits) and 3DES", "Default - RC4(128 bits) and higher" (selected), and "Low - RC4(64 bits), DES and higher".
- Idle Timeout:** A text input field with "300" and "(seconds)" next to it.
- Login Port:** A text input field with "10443".
- Allow Endpoint Registration (Tunnel Mode Only):** An unchecked checkbox.
- Advanced (DNS and WINS Servers):** A collapsed section indicated by a blue arrow.
- Apply:** A button at the bottom right of the configuration area.

Go to **VPN > SSL > Portal**.

## Creating a security policy for SSL VPN users

Go to **Policy > Policy > Policy** and select **Create New**. Enter a policy to enable VPN users to authenticate and communicate with the local network.

Name:

Portal Message:

Theme:

Page Layout:

Enable Tunnel Mode

Enable Web Mode

Applications

- HTTP/HTTPS
- SSH
- CITRIX
- FTP
- TELNET
- RDP NATIVE
- RDP
- VNC
- Port Forward
- SMB/CIFS
- PING

Include Session Info

Include Connection Tool

Include FortClient Download

Include Bookmarks

Name	Type	Location	Description
No matching entries found			

Prompt Mobile Users to Download FortClient App

Allow Multiple Concurrent Sessions For Each User

Policy Type:  Firewall  VPN

Policy Subtype:  IPsec  SSL-VPN

Incoming Interface:

Remote Address:

Local Interface:

Local Protected Subnet:

SSL Client Certificate Restrictive

Cipher Strength:

**Configure SSL-VPN Authentication Rules**

User/Group	Service	Schedule	Security	SSL-VPN Portal	Logging	Action
full-time	ALL	always	-	full-access	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> ACCEPT
ANY	ALL	always	-		<input type="checkbox"/>	<input checked="" type="checkbox"/> DENY

**Tags**

Applied tags

Add tag

Comments  0/1023

## Results

In a browser, enter the FortiGate IP address and port 10443. For example <https://172.20.120.123:10443>.

If you receive a warning about the certificate being unrecognized, allow the browser to continue access.

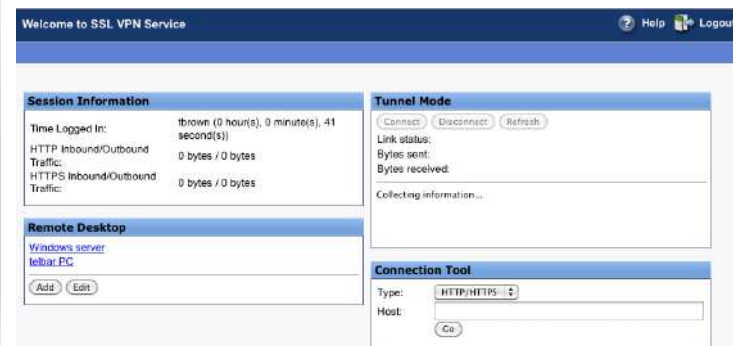
Enter the user name and password and then select **Login**. If the user account has two-factor authentication enabled, the **FortiToken Code** field is added. Obtain the code from the FortiToken device or FortiToken Mobile app and enter it. Select **Login** again.

You are connected to the SSL VPN portal.

The **VPN > Monitor > SSL-VPN Monitor** page shows the connected SSL VPN client.



The image shows a login form titled "Please Login". It contains three input fields: "Name:" with the value "tbrown", "Password:" with masked characters "\*\*\*\*\*", and "FortiToken Code:" with masked characters "\*\*\*\*\*". Below the fields is a "Login" button.



The image shows the "Welcome to SSL VPN Service" dashboard. It features a header with "Welcome to SSL VPN Service" and "Help" and "Logout" icons. The main content area is divided into four sections: "Session Information" (Time Logged In: tbrown (0 hour(s), 0 minute(s), 41 second(s)), HTTP Inbound/Outbound Traffic: 0 bytes / 0 bytes, HTTPS Inbound/Outbound Traffic: 0 bytes / 0 bytes), "Remote Desktop" (Windows server, telhar PC, Add, Edit buttons), "Tunnel Mode" (Connect, Disconnect, Refresh buttons, Link status, Bytes sent, Bytes received, Collecting information...), and "Connection Tool" (Type: HTTP/HTTPS, Host: [input field], Go button).

No.	User	Source IP	Begin Time	Description
<input type="checkbox"/>	1	tbrown	172.20.120.52	Thu Sep 12 10:04:32 2013
<input type="checkbox"/>			Subsession	Tunnel IP:10.212.134.200