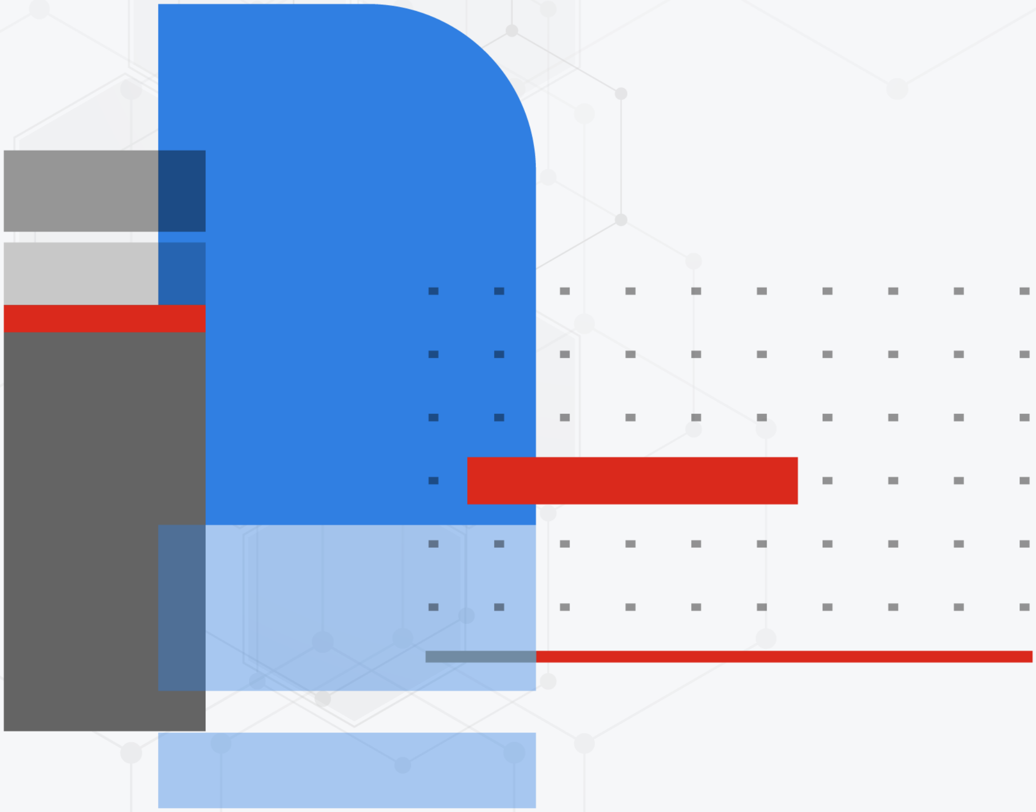
SSL VPN Configuration Guide

FortiToken Cloud 23.4.b



FORTINET®

January 8, 2024
FortiToken Cloud 23.4.b SSL VPN Configuration Guide

TABLE OF CONTENTS

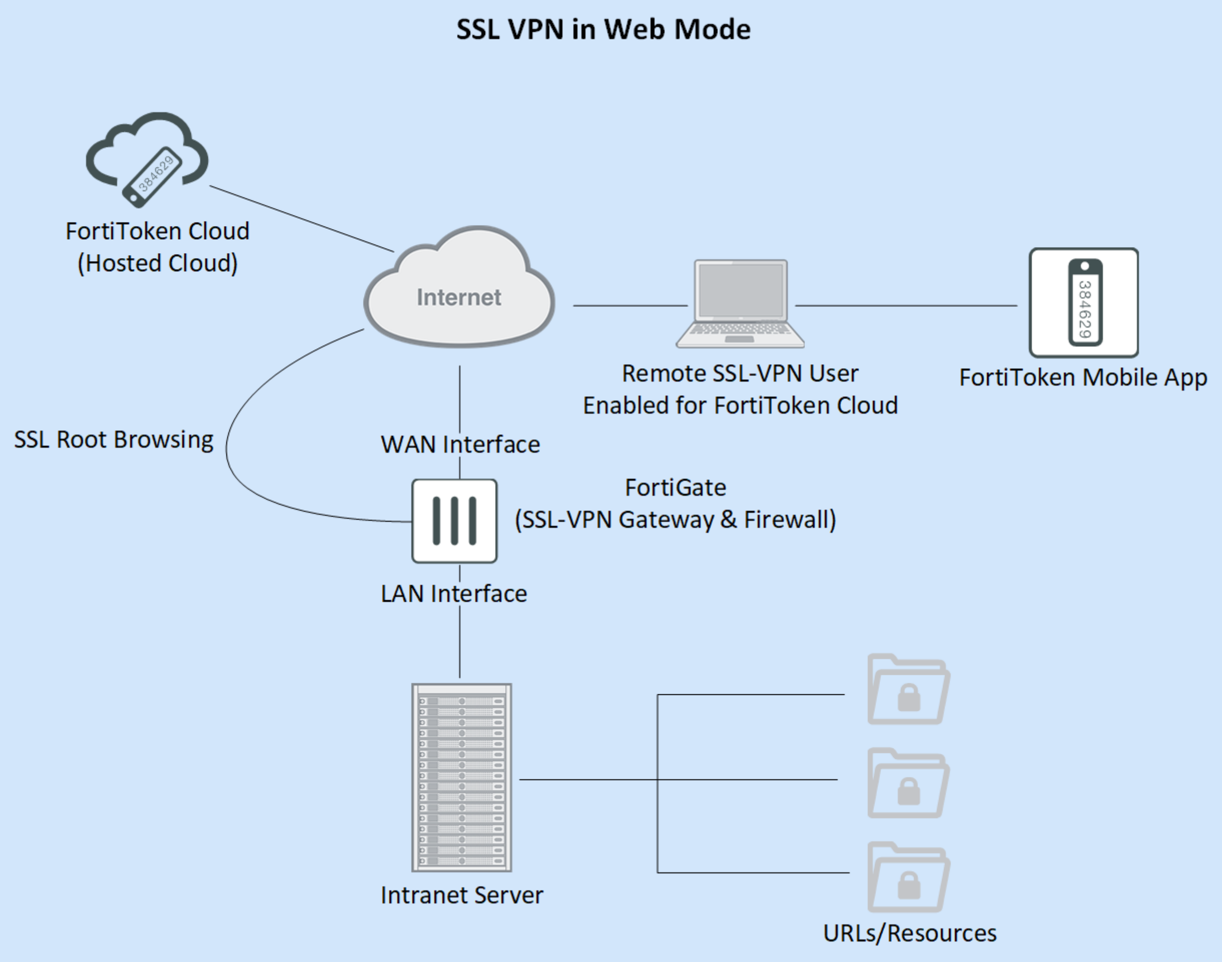
Introduction

An SSL VPN is a virtual private network which uses the Secure Layer Socket (SSL) or the Transport Layer Security (TLS) protocol in web browsers to create a secure, remote VPN connection between the endpoint device and the SSL/TSL server. Using end-to-end encryption (E2EE), an SSL VPN enables remote users, such as corporate employees, telecommuters, contractors, and so on, to access internal corporate resources and to have secure internet access from outside the corporate network.

This tutorial shows how to enable FortiGate users to remotely access your internal network and the internet using an SSL VPN connected by web mode from FortiToken Cloud.

Network topology

The following diagram illustrates how a FortiToken Cloud-enabled FortiGate user accesses a corporate intranet and the internet remotely through an SSL VPN in Web mode from FortiToken Cloud.



Prerequisites

To configure FortiToken Cloud-enabled SSL-VPN users on FortiGate, *you must have a valid FortiGate license and FortiToken Cloud license registered under the same FortiCloud account.*

Otherwise, do the following before you proceed:

1. Open your web browser.
2. Go to https://support.fortinet.com.
3. Click **Login** to log in to your FortiCloud account.
4. From the top of the screen, select **Asset > Register/Activate.**
5. Follow the prompts onscreen to register and activate your licenses.

Step 1: Enable FortiToken Cloud Service on FortiGate

The FortiGate admin user must enable FortiToken Cloud service on the FortiGate, which can be done from the Console only.

To enable FortiToken Cloud service in FortiGate:

Execute the following commands:

```
FortiGate-VM64 # config global
FortiGate-VM64 (global) # config system global
FortiGate-VM64 (global) # set fortitoken-cloud-service enable
FortiGate-VM64 (global) # end
```

`set fortitoken-cloud-service enable` is a "local" command and does not trigger communication with the FortiToken Cloud server. It simply enables FortiGate VDOM admin users to manage FortiToken Cloud users locally using the FortiGate CLI.

Step 2: Create SSL VPN users and user group

This step involves creating users and a user-group, and assigning the users to the user group.

Create users

To create users from the GUI:

1. Select **User & Device > User Definition**.
2. Select **+ Create New**.
3. Select Local User, and click **Next.**
4. Name the user "test-ssl".
5. Enable the User Account Status.
6. Enter a unique Password for the user.
7. Enter the user's Email Address.
8. Enable two-factor Authentication, and select FortiToken Cloud as the Authentication Type.
9. Click **OK**.
10. Repeat Steps 1 through 8 above to create another user named "testssl2".

To create users from the Console:

```
config user local
    edit "test-ssl"
        set type password
        set passwd <user-password>
        set two-factor fortitoken-cloud
        set email-to <user@abc.com>
    next
end
```

```
config user local
    edit "testssl2"
        set type password
        set passwd <user-password>
        set two-factor fortitoken-cloud
        set email-to <user@abc.com>
    next
end
```

Create a user group

To create a user group from the GUI:

1. Select **User & Device > User Groups**.
2. Select **Create New** to create a user group.
3. Name the user group "sslvpngrp".
4. Select Firewall as the user group type.
5. Click the **+** sign **(Add)** in the Members box to add users "test-ssl" and "testssl2" that you've created.
6. Click **OK.**

To create a user group from the Console:

```
config user group
    edit "sslvpngrp"
        set member "test-ssl"
    next
End

config user group
    edit "sslvpngrp"
        set member "testssl2"
    next
end
```

Step 3: Create an SSL-VPN portal in web mode

To create an SSL-VPN portal in web mode from the GUI:

1. Select **VPN > SSL-VPN Portals**.
2. In the portal table, click to open the web-access portal, which enables Web Mode only.
   Note: You can open to edit the full-access portal which enables both Web Mode and Tunnel Mode. However, since we are configuring the users to use the SSL VPN in Web mode only, it is not necessary to use the full-access portal.
3. Make sure Web Mode is enabled.
4. *(Optional)* Under Predefined Bookmarks, do the following:
   a. Select **Create New** to add a new bookmark named "fgt isfw". (**Note:** Bookmarks are shortcut links to the internal network resources for web mode users. In this example, we create a bookmark to let the users to manage the ISFW FortiGate.)
   b. Set Type to HTTP/HTTPS.
   c. Specify the IP address of the device, e.g., `https://x.x.x.x`"
5. Click **OK** to save the changes.

To create an SSL-VPN portal in web mode from the Console:

```
config vpn ssl web portal
    edit <web-access>
        set web-mode enable
        config bookmark-group
            edit <gui-bookmarks> <<<optional
                config bookmarks
                    edit <fgt isfw>
                        set apptype <HTTP/HTTPS>
                        set host <x.x.x.x>
                        set port <xxxxx>
                        set logon-user <your-fortigate-user-name>
                        set logon-password <your-fortigate-password>
                    next
                end
            next
        end
    next
end
```

Step 4: Add a local network address for the firewall

This step lets you set the IP address for the local network.

To set the IP address for the local network from the GUI:

1. Select **Policy & Objects > Addresses.**
2. Click **Create New** to create a local network named "local-lan".
3. Set Type to Subnet.
4. Set the IP/Netmask to the IP range of your local subnet.
5. Set the interface to your internal port interface, i.e., "lan".
6. Click **OK** to save the local network address.

To set the IP address for local network from the Console:

```
config firewall address
    edit "192.168.1.0"
        set subnet 192.168.1.0 255.255.255.0
    next
end
```

Step 5: Configure SSL-VPN Tunnel Settings

To configure the SSL-VPN tunnel settings:

1. Select **VPN > SSL-VPN Settings** to configure the SSL-VPN settings.
2. Set the "Listen on Interface" to your Internet-facing interface, which is `Port1` in this example.
3. To avoid port conflict, set the Listen on Port to `44310`.
4. Set "Restrict Access" to `Allow access from any host.`
5. For "Server Certificate", select a desired certificate. (**Note:** `Fortinet_Factory` is the default certificate. We recommend that you purchase and use a certificate of your own.)
6. Under "Tunnel Mode Client Settings", set the IP range to the one you've selected earlier, i.e., `SSLVPN_TUNNEL_ADDR1`.
7. Under Authentication/Portal Mapping, select **Create New** to create a new rule:
   a. Set Users/Groups to `sslvpngrp`
   b. Set Portal to `full-access`
   c. Click **OK**.

If necessary, map up the SSL-VPN portal for All Other Users/Groups and save your changes.

8. Click **Apply.**

Step 6: Create firewall policies

To allow the user to access both your internal network and the internet, you must create two firewall policies: one for the Internet and one for your internal network.

Configure an internet firewall policy

To configure an SSL-VPN firewall policy for the Internet from the GUI:

1. From the main menu, select **Policy & Objects > IPv4 Policy.**
2. Select **Create New**, and make the required selections as shown in the following table.

Parameter	Description and Example
Name	Specify a unique name that identifies the purpose of the policy, e.g., "ssl-to-internet".
Incoming Interface	Select the interface for incoming traffic, e.g., "SSL-VPN tunnel interface (ssl.root)".
Outgoing Interface	Select the interface for outgoing traffic, e.g., "port1".
Source	Make the following selections: • Address —"all", • User—"sslvpngrp".
Destination	Set Address to "all".
Schedule	Select "always".
Service	Select "ALL"
Action	Select "ACCEPT".
NAT	Click the button to enable NAT.
IP Pool Configuration	Select "Use Outgoing Interface Address"
Enable this policy	Click the button to enable the policy.

3. Make the other selections as desired.
4. Click **OK** to confirm the policy configuration.

To configure an SSL VPN firewall policy for the Internet from the Console:

```
config firewall policy
    edit 1
        set name "sssl-to-internet"
        set srcintf "ssl.root"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "192.168.1.0"
        set groups “sslvpngrp”
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```

Configure an internal network firewall policy

To configure an SSL VPN firewall policy for your internal network from the GUI:

1. From the main menu, select **Policy & Objects > IPv4 Policy.**
2. Select **Create New**, and make the required selections as illustrated below:

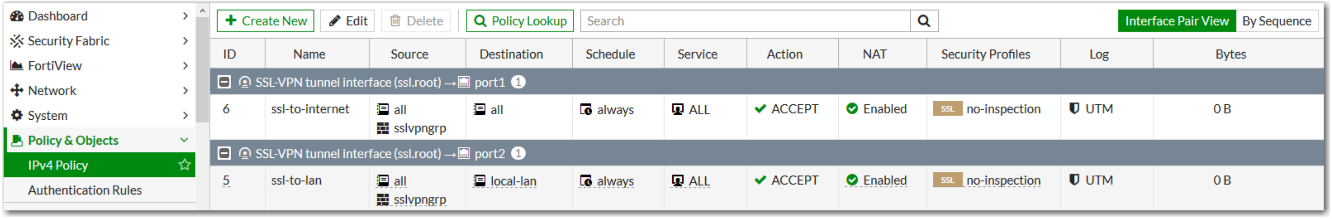
Parameter	Description and Example
Name	Specify a unique name that identifies the purpose of the policy, e.g., "ssl-to-lan".
Incoming Interface	Select the interface for incoming traffic, e.g., "SSL-VPN tunnel interface (ssl.root)".
Outgoing Interface	Select the interface for outgoing traffic, e.g., "port2".
Source	Make the following selections • Address —"all", • User—"sslvpngrp".
Destination	Set Address to "local-lan".
Schedule	Select "always".
Service	Select "ALL"
Action	Select "ACCEPT".
NAT	Click the button to enable NAT.
IP Pool Configuration	Select "Use Outgoing Interface Address"
Enable this policy	Click the button to enable the policy.

3. Make the other selections as desired.
4. Click **OK** to confirm the policy configuration.

To configure an SSL VPN firewall policy for your internal network from the Console:

```
config firewall policy
    edit 1
        set name "ssl-to-lan"
        set srcintf "ssl.root"
        set dstintf "port2"
        set srcaddr "all"
        set dstaddr "local-lan"
        set groups “sslvpngrp”
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```

The image below shows the two firewall policies we've just created.



ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
⊟ SSL-VPN tunnel interface (ssl.root) → port1 1										
6	ssl-to-internet	all sslvpngrp	all	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	UTM	0 B
⊟ SSL-VPN tunnel interface (ssl.root) → port2 1										
5	ssl-to-lan	all sslvpngrp	local-lan	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	UTM	0 B

Step 7: Test and validate the SSL-VPN configuration

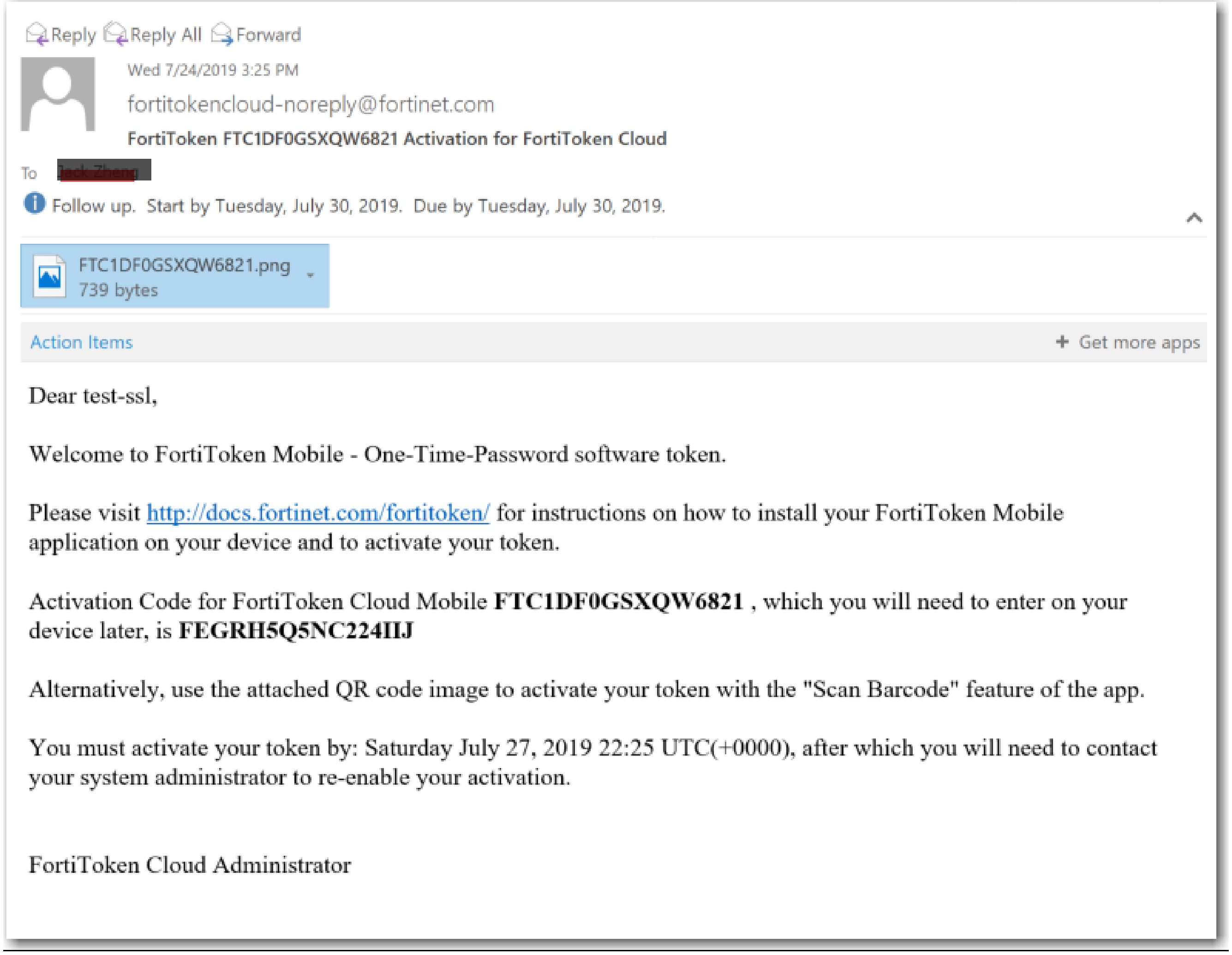
After you've completed the SSL-VPN configuration on FortiGate, you need to do the following to test and validate your configuration to ensure that it works properly.

- Verify user email notification on page 16.
- Verify the FortiGate and SSL-VPN users on FTC portal on page 17.
- Test the SSL VPN in Web mode on page 18.
- View the SSL-VPN user logged in to FortiGate on page 19.

Verify user email notification

Once a user account is created on FortiGate with FortiToken Cloud service enabled for two-factor authentication, the system will automatically send an activation code to the end-user's email address specified in the account.

The following illustration shows an example email notification that the system sent to an end-user.



Wed 7/24/2019 3:25 PM

fortitokencloud-noreply@fortinet.com

FortiToken FTC1DF0GSXQW6821 Activation for FortiToken Cloud

To [redacted]

Follow up. Start by Tuesday, July 30, 2019. Due by Tuesday, July 30, 2019.

Dear test-ssl,

Welcome to FortiToken Mobile - One-Time-Password software token.

Please visit http://docs.fortinet.com/fortitoken/ for instructions on how to install your FortiToken Mobile application on your device and to activate your token.

Activation Code for FortiToken Cloud Mobile **FTC1DF0GSXQW6821** , which you will need to enter on your device later, is **FEGRH5Q5NC224IIJ**

Alternatively, use the attached QR code image to activate your token with the "Scan Barcode" feature of the app.

You must activate your token by: Saturday July 27, 2019 22:25 UTC(+0000), after which you will need to contact your system administrator to re-enable your activation.

FortiToken Cloud Administrator

As shown above, the notification includes a FortiToken Cloud Mobile token and its activation code and QR code. The end-user can activate the token by either entering the activation code or scanning the QR code with a supported mobile device that has FortiToken Mobile app installed on it.

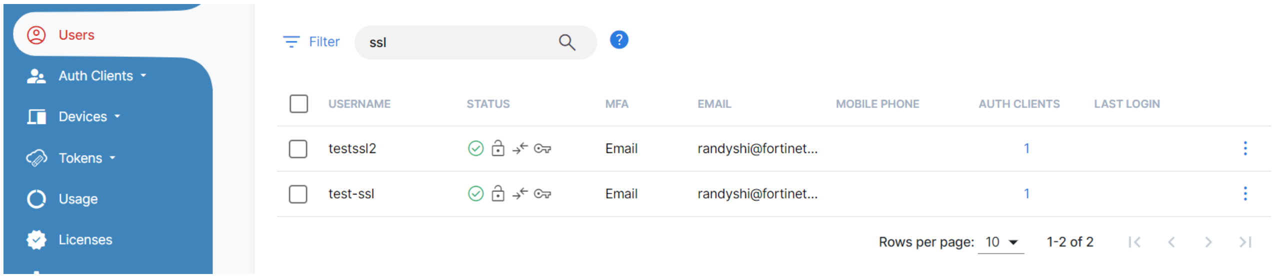
Verify the FortiGate and SSL-VPN users on FTC portal

Once a user account is created on FortiGate (with FortiToken Cloud service enabled), the same user will appear on the FortiToken Cloud portal as a FortiToken Cloud user. If the user is the first user of the FortiGate VDOM, the FortiGate will show up on the portal as an authentication client as well.

To view the SSL-VPN user on FortiToken Cloud:

1. Open a supported web browser.
2. Go to https://ftc.fortinet.com.
3. Log in to the FortiToken Cloud portal.
4. On the main menu, click **Users** to open the Users page.

The following screen shot of FortiToken Cloud's Users page shows the two users we've just added from the FortiGate.

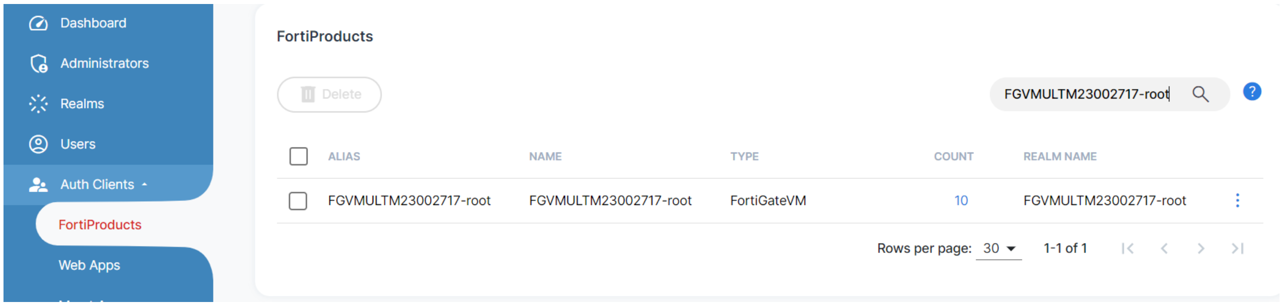


USERNAME	STATUS	MFA	EMAIL	MOBILE PHONE	AUTH CLIENTS	LAST LOGIN
testssl2		Email	randyshi@fortinet...		1	
test-ssl		Email	randyshi@fortinet...		1	

Rows per page: 10 1-2 of 2

To view the FortiGate appliance on FortiToken Cloud:

1. On the main menu, click **Auth Clients** to open the Auth Clients page.
   The following is a partial screen capture of FortiToken Cloud's Auth Clients page showing the FortiGate from which the aforementioned two SSL-VPN users were added.



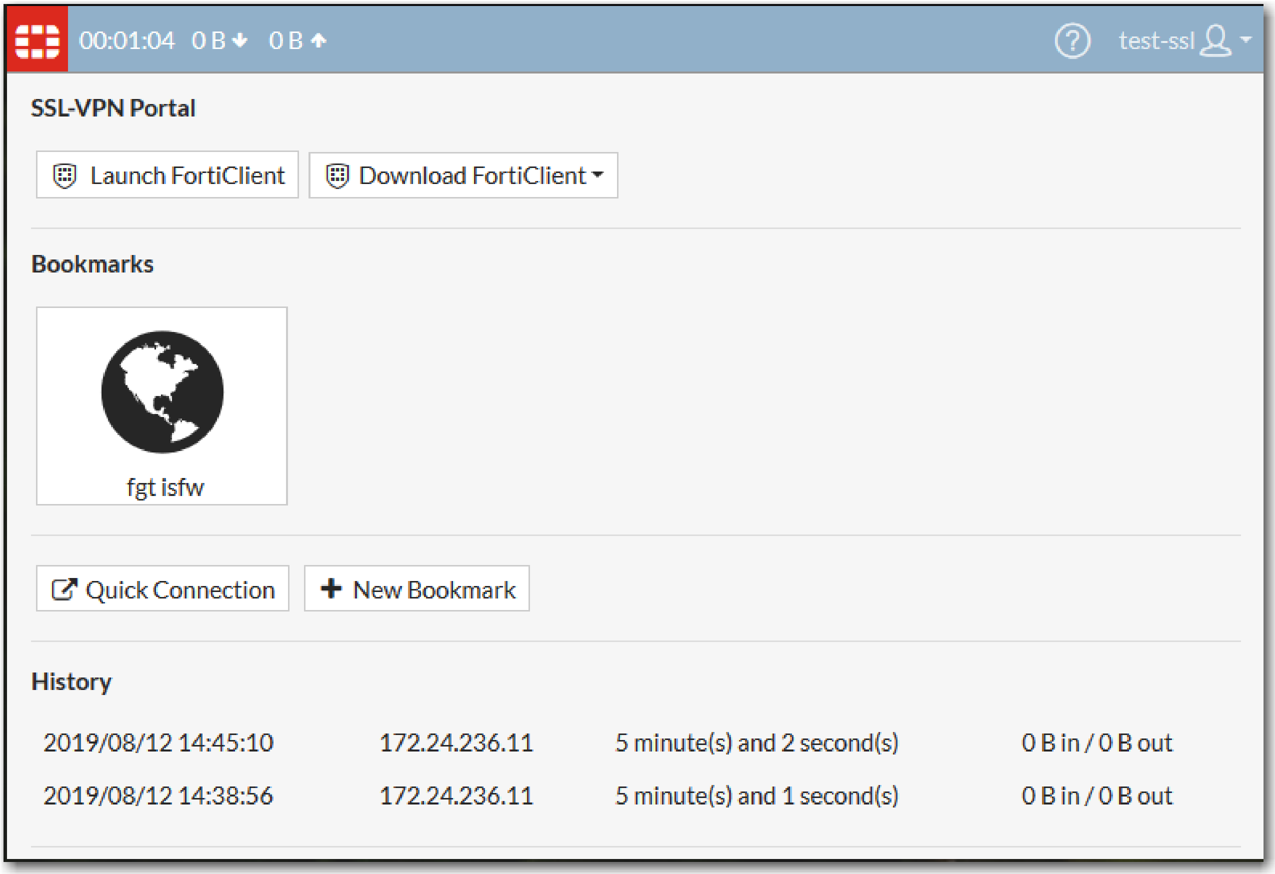
ALIAS	NAME	TYPE	COUNT	REALM NAME
FGVMULTM23002717-root	FGVMULTM23002717-root	FortiGateVM	10	FGVMULTM23002717-root

Rows per page: 30 1-1 of 1

Test the SSL VPN in Web mode

The SSL-VPN users can verify that the SSL VPN works in web mode.

1. Open a supported web browser.
2. Connect to the SSLVPN web portal by entering the remote gateway's IP address and port number you specified when configuring the SSL-VPN settings.
3. Enter the SSL-VPN user's username and password to authenticate and log in to the SSL-VPN web portal. A Login Request is sent to the end-user's mobile device.
4. Open the SMS message on the end-user's mobile device, and tap **Approve** to complete the authentication. (**Note:** You must manually enter the token to authenticate instead if the push notification feature is not enabled.)
   The following screen shot shows the SSL-VPN Web portal page when it opens.



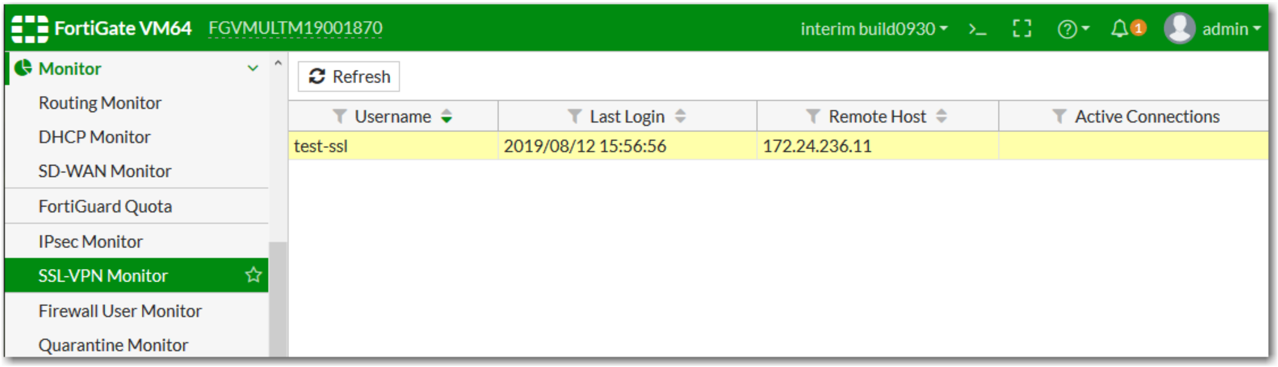
2019/08/12 14:45:10	172.24.236.11	5 minute(s) and 2 second(s)	0 B in / 0 B out
2019/08/12 14:38:56	172.24.236.11	5 minute(s) and 1 second(s)	0 B in / 0 B out

5. Under Bookmarks, click the fgt isfw bookmark to connect to the FortiGate.
6. Click the **Quick Connection** button to access the various services on the SSL-VPN Portal.

View the SSL-VPN user logged in to FortiGate

Once the SSL-VPN users have connected to the FortiGate via the SSL-VPN, you can view their login activities from inside FortiGate.

1. Log in to the FortiGate.
2. On the main menu, click **Monitor > SSL-VPN Monitor.** The following screen shot shows one of the SSL-VPN users logged into the FortiGate.



Username	Last Login	Remote Host	Active Connections
test-ssl	2019/08/12 15:56:56	172.24.236.11	

FORTINET®

www.fortinet.com