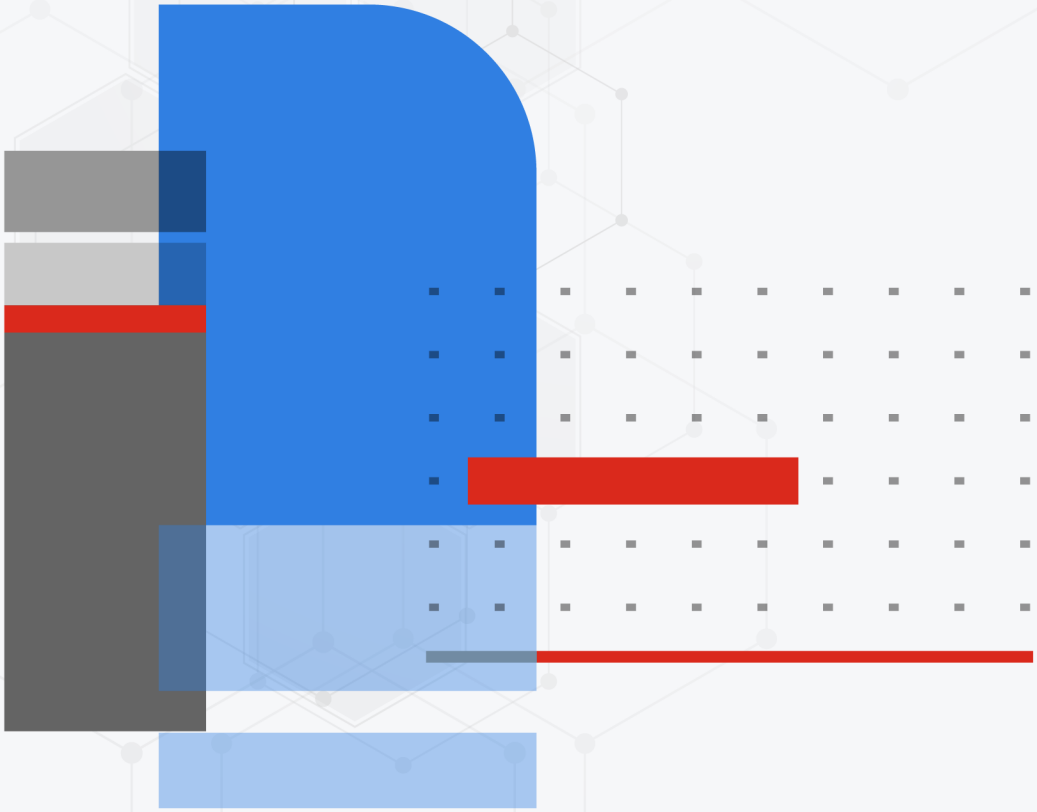
Dedicated Instance Deployment Guide

FortiSASE-Sovereign 26.2.a



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

April 30, 2026
FortiSASE-Sovereign 26.2.a Dedicated Instance Deployment Guide

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-05-28	Initial release.
2025-06-20	First update: • Removed the last four screen captures and related text at the end of Step 4: Set up your FortiGate appliance on page 14 to reflect product update. • Removed reference to info site in FortiOS and FortiAnalyzer for FortiSASE-Sovereign on page 10.
2025-10-29	Updated Prepare for deployment. Updated Deployment procedure. Added Pre-Planning Requirements for POC to Prerequisites. Added Cabling and IP Addressing Guidelines for FortiGate Deployment to Step 4: Set up your FortiGate appliance. Added Licensing FortiGate Before Onboarding to Step 4: Set up your FortiGate appliance.

Introduction

This *Dedicated Instance Deployment Guide* provides information and instructions on how to set up and provision your FortiSASE-Sovereign. It is written for system administrators and network and cloud security professionals who are responsible for deploying and managing FortiSASE-Sovereign in their network environment.

Prerequisites

The following are required for deploying and operating FortiSASE-Sovereign. Before you start setting up your FortiSASE-Sovereign, make sure that you have these items ready in your environment.

- A FortiCloud (FC) account. For instructions on how to create an FC account, visit Creating a FortiCloud account.
- FortiSASE-Sovereign licenses. See Product Licensing and/or Ordering Guide for details.
- FortiGate appliance and compatible version of FortiOS. See FortiOS and FortiAnalyzer for FortiSASE-Sovereign and the Ordering Guide.
- FortiAnalyzer appliance or VM. See FortiOS and FortiAnalyzer for FortiSASE-Sovereign.

Pre-Planning Requirements for POC

Before starting the proof of concept (POC), customers must allocate the necessary resources and prepare the required components. This ensures a smooth onboarding and deployment process with FortiSASE-Sovereign.

Components Deployed by FortiSASE-Sovereign Controllers

The following components are provisioned and managed directly by the FortiSASE-Sovereign controllers:

- FortiSASE-Sovereign service portal and associated services.

Customer-Prepared On-Premises Components

Licenses and Accounts

Customers must have the following licenses and accounts ready before onboarding:

- FortiCloud account.
- FortiSASE-Sovereign license.
- FortiSASE-Sovereign end-user (EMS) license.
- FortiGate FortiSASE-Sovereign licenses for all PoP FortiGates.

Hardware and Accessories

The following hardware and accessories should be prepared on premises:

- FortiGates designated for onboarding as FortiSASE-Sovereign PoPs.
- FortiAnalyzer.
- (Optional) Thin Edge FortiGate, FortiExtender, or FortiAP.
- (Optional) FortiGates configured as ZTNA gateways.
- Required cables and transceivers.

Network Planning

Customers must plan and configure network resources in advance:

- Plan port allocation for all hardware components.
- Allocate IP addresses for each hardware component.
- Configure IP addresses and static routes on all hardware devices.
- Connect and cable hardware components properly and verify that they have Internet connectivity.

Supported Fortinet hardware platforms

For information regarding the Fortinet hardware platforms, see the Ordering Guide.

FortiOS and FortiAnalyzer for FortiSASE-Sovereign

FortiSASE-Sovereign requires the following supported versions of FortiOS and FortiAnalyzer to operate:

Fortinet Product	Version	Build	Status
FortiGate	v7.4.11	6843	Special
FortiAnalyzer	v7.4.10	2778	GA

Prepare for deployment

The following are things you must know or do in preparation for deploying your FortiSASE-Sovereign.

Step 1: Create a FortiCloud account

You must have a valid FortiCloud (FC) account to install and manage the various components of your FortiSASE-Sovereign.

- If you do not have an FC account in place yet, you must create one before you proceed. For instructions on how to create an FC account, visit Creating a FortiCloud account.
- If you already have an FC account in place, ensure that all your FortiSASE-Sovereign-related Fortinet products and services are registered under that account.

Step 2: Obtain product licenses

FortiSASE-Sovereign is a subscription-based cloud security service, which requires the following Fortinet product licenses:

- FortiSASE-Sovereign portal license
- FortiClient EMS for FortiSASE-Sovereign end-user license(s)
- FortiGate/FortiOS for FortiSASE-Sovereign license(s)

To purchase your licenses for FortiSASE-Sovereign and some other related Fortinet products, refer to the Ordering Guide.

You must obtain licenses to install and operate each of the aforementioned Fortinet products. The following tables highlight the various licensing options for each of these products.

FortiSASE-Sovereign portal license

SKU	Description	Serial Number (SN) Prefix
FC-10-OVSAE-1081-02- DD	FortiSASE-Sovereign subscription service of cloud orchestrator and web portal.	FOVSA

FortiSASE-Sovereign end-user (EMS) licenses

SKU	Description	Serial Number (SN) Prefix
FC3-10-EMSSS-552-02-DD	FortiSASE-Sovereign end-user License for up to 1,999 users. This standard FortiSASE-Sovereign end-user license supports cloud-delivered security over FortiSASE-Sovereign with secure private access through unified agent (SASE, ZTNA, and VPN). It covers three devices per user, and includes the EPP/ATP client license.	FEMSSS
FC4-10-EMSSS-552-02-DD	Same as above, but covers between 2,000 and 9,999 end users.	FEMSSS
FC5-10-EMSSS-552-02-DD	Same as above, but covers 10,000 and more end users.	FEMSSS

You can register your FortiSASE-Sovereign end-user (EMS) licenses on FortiCloud (FC) only after you already have your FortiSASE-Sovereign portal license registered in your FC account.

FortiGate/FortiOS for FortiSASE-Sovereign licenses

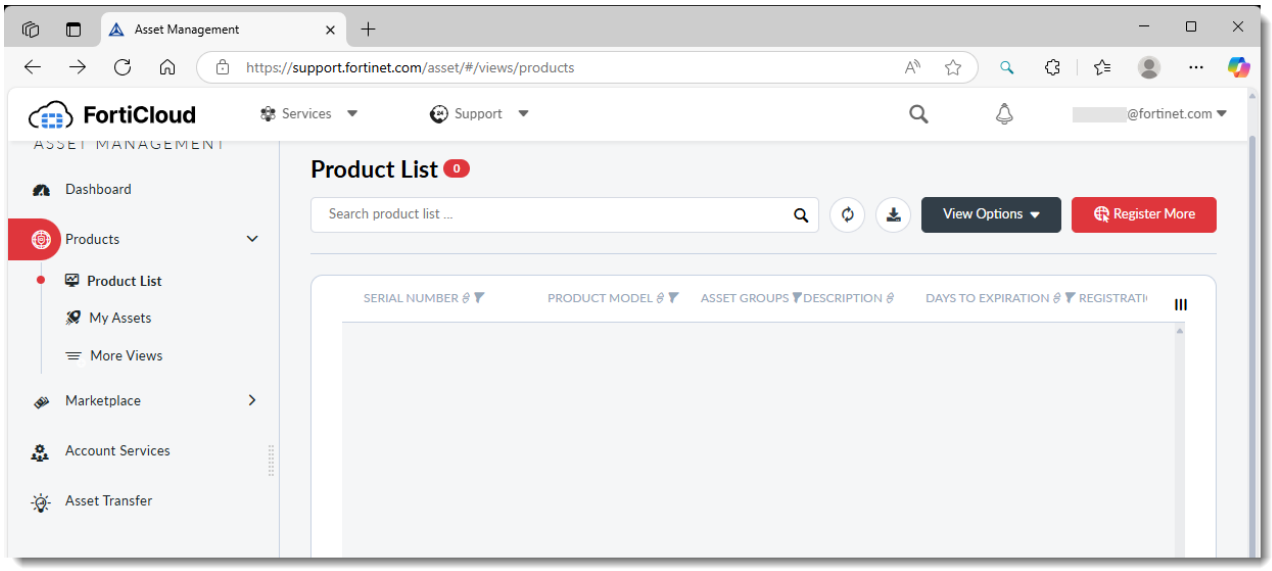
SKU	Description	Serial Number (SN) Prefix
FC-10-0091G-1082-02-DD	The license provides one-year FortiSASE-Sovereign Security Inspection Service. It includes the FortiGate enterprise bundle and FortiSASE-Sovereign entitlement (Support Type 321, or SSFL in short). ***Note:*** *For FortiGate 91G devices only.*	FGT91G

SKU	Description	Serial Number (SN) Prefix
FC-10-FG9H1-1082-02-DD	The license provides one-year FortiSASE-Sovereign Security Inspection Service. It includes the FortiGate enterprise bundle and FortiSASE-Sovereign entitlement (Support Type 321, or SSFL in short). ***Note:*** *For FortiGate 901G devices only.*	FGT9H1G

Step 3: Register your products

Before registering your Fortinet products, be sure to have your product serial numbers ready.

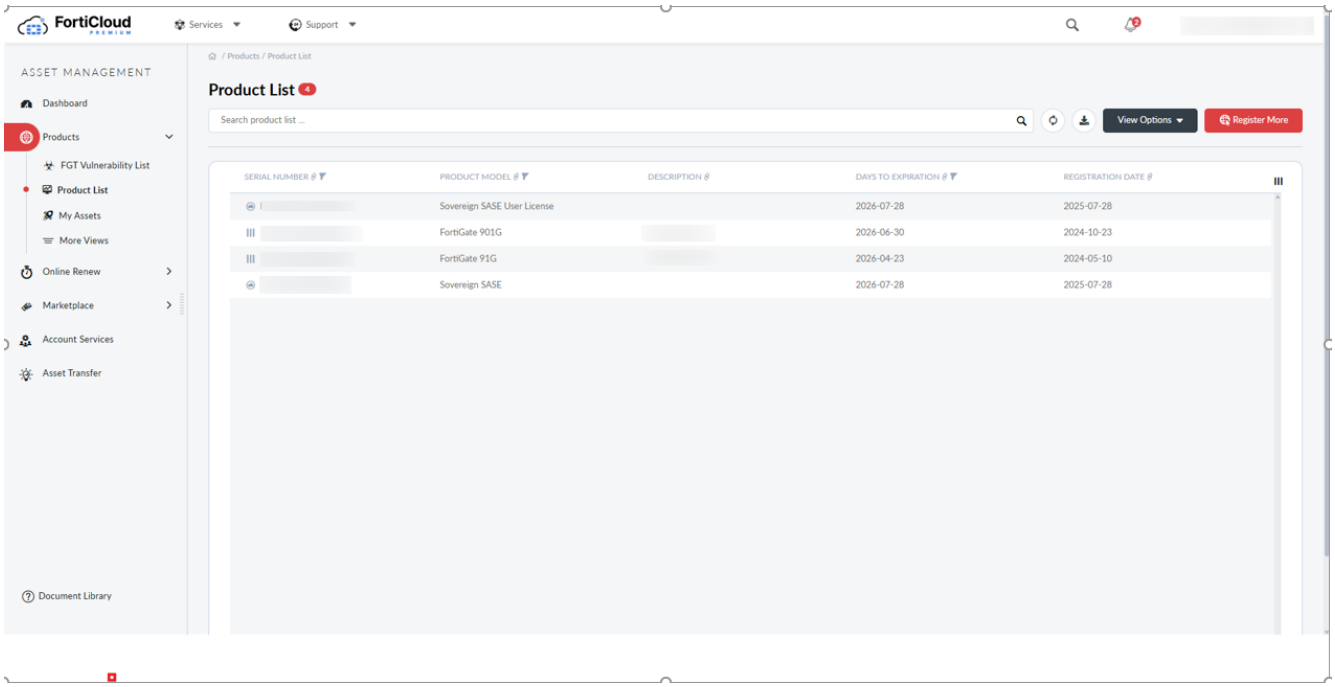
1. Log into your FortiCloud account.
2. On the FortiCloud portal, select Products. The Product List page opens.



3. In the top right corner of the page, click Register More.
4. Follow the steps to register your product.
5. Repeat step 2 through 4 to register all the products required for FortiSASE-Sovereign.

After registering all required products and licenses on FortiCloud, go to FortiCloud → Asset Management → My Assets to verify that all necessary licenses are present in your account.

For example, to onboard one on-premises FortiGate 901G and one FortiGate 91G as PoP devices, you must have the following products registered:



Including:

Sovereign SASE

Sovereign SASE User License

FortiGate FortiSAE-Sovereign Licenses for each PoP FortiGate.

Step 4: Set up your FortiGate appliance

You can order FortiGate as a Service (FGaaS) as PoP FortiGate or use your own FortiGate appliance.

- To order FGaaS, refer to the Ordering Guide (https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/og-fgaas.pdf)
- To use your own FortiGate appliance, ensure that it is running on the supported version of FortiOS. For more information, see FortiOS and FortiAnalyzer for FortiSASE-Sovereign on page 10.

Cabling and IP Addressing Guidelines for FortiGate Deployment

FortiSASE-Sovereign supports two cabling options for FortiGate: one-arm and two-arm. Both approaches are supported equally, and customers should choose the method that best fits their network environment.

Regardless of the selected cabling method, customers must ensure that after proper cabling, the FortiGate has valid IP addressing, gateway, and static route configurations. The FortiGate must have Internet connectivity, and all required service ports must be open and allowed within the customer's network infrastructure.

FortiSASE-Sovereign does not impose specific requirements for IP addressing. Customers may allocate any available IP addresses to ingress and egress interfaces, provided that the assigned addresses ensure Internet accessibility.

Basic FortiGate Configuration

When a FortiGate is onboarded with FortiSASE-Sovereign, regardless of whether it has factory-default settings or existing production configurations, the FortiSASE-Sovereign controller will assume full configuration control. During the onboarding process, the controller synchronizes the onboarded FortiGate with the required FortiSASE-Sovereign configurations.

After onboarding, administrators cannot modify PoP FortiGate configurations directly through the FortiGate GUI or CLI.

Important: If the FortiGate is already deployed in a production environment with existing configurations, it must be factory reset before onboarding. Ensure console access is available before proceeding. For reset instructions, refer to: https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-reset-a-FortiGate-with-the-default-factory/ta-p/196896

In addition, the FortiGate must have IP addresses and corresponding static routes configured for both ingress and egress ports. The static route on the egress port should have a lower priority than the one on the ingress port, ensuring the egress port is preferred for outbound traffic.

Example: Two-Arm Deployment

In this example, Port 1 is configured as the ingress port and Port 2 as the egress port. The following configurations must be applied before onboarding:

```
config system interface
    edit port1
        set mode static
        set ip 3.107.32.117/24
        set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response fabric ftm
speed-test
   next
end
config system interface
edit port2
    set mode static
        set ip 3.107.36.117/24
        set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response fabric ftm
speed-test
   next
end

config router static
    edit 1
        set gateway 3.107.32.254
        set device port1
        set priority 100
    next
    edit 2
```

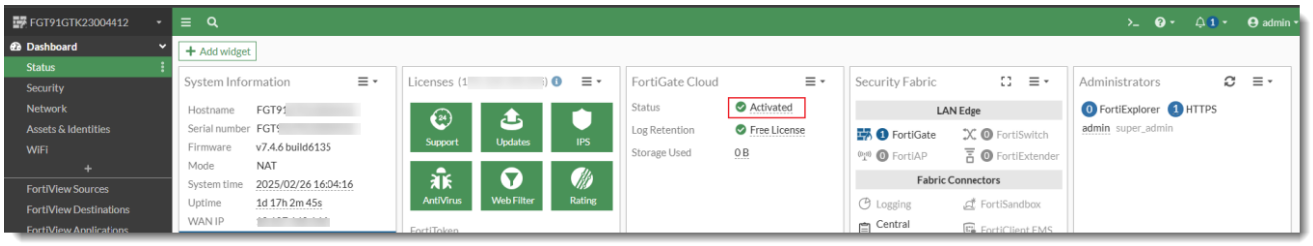
```
        set gateway 3.107.36.254
        set device port2
        set priority 50
    next
end
```

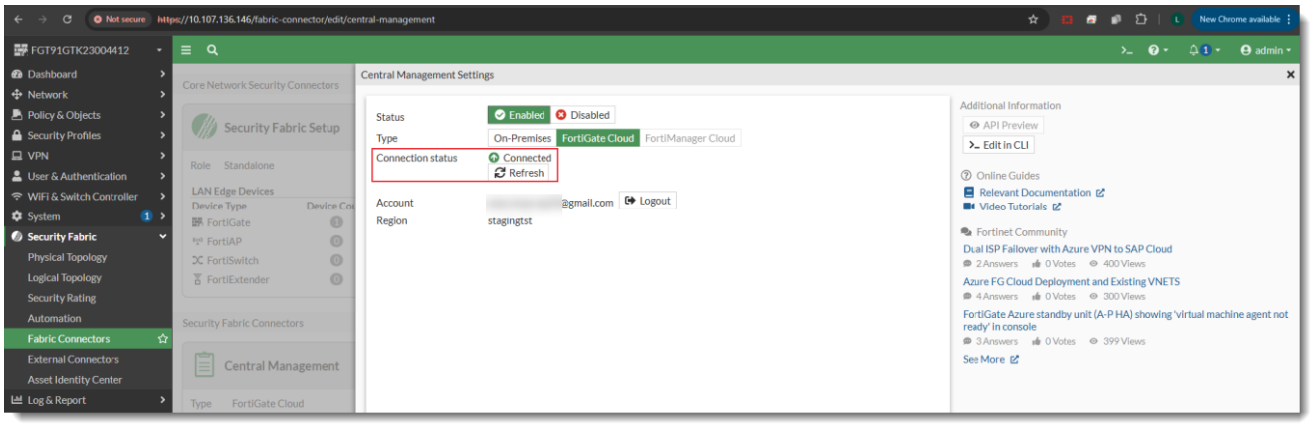
In this example, administrator will need to select ingress port as port 1, and egress as port 2 later during FortiSASE-Sovereign onboarding procedure.

Activate FortiGate Cloud

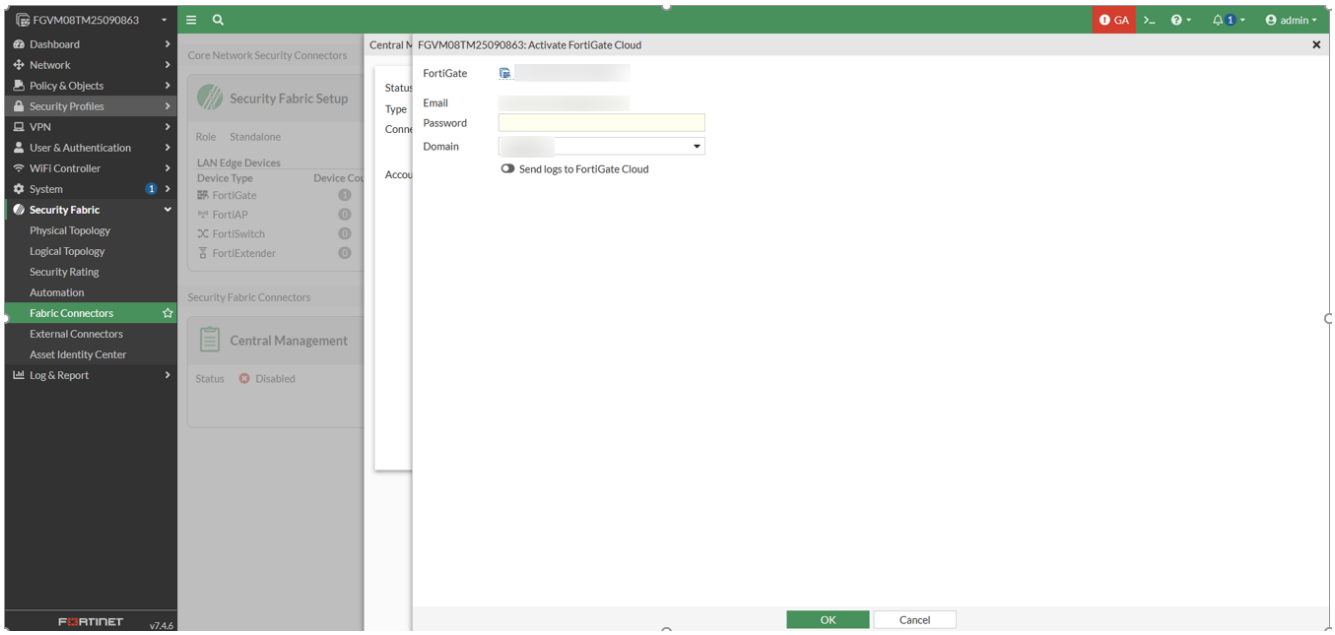
After you have installed the required version of FortiOS on your FortiGate and added necessary interface and IP configuration,

you must activate FortiGate Cloud and ensure that the Central Management Settings are connected to FortiGate Cloud at Fabric Connectors, as highlighted in the following screenshots.

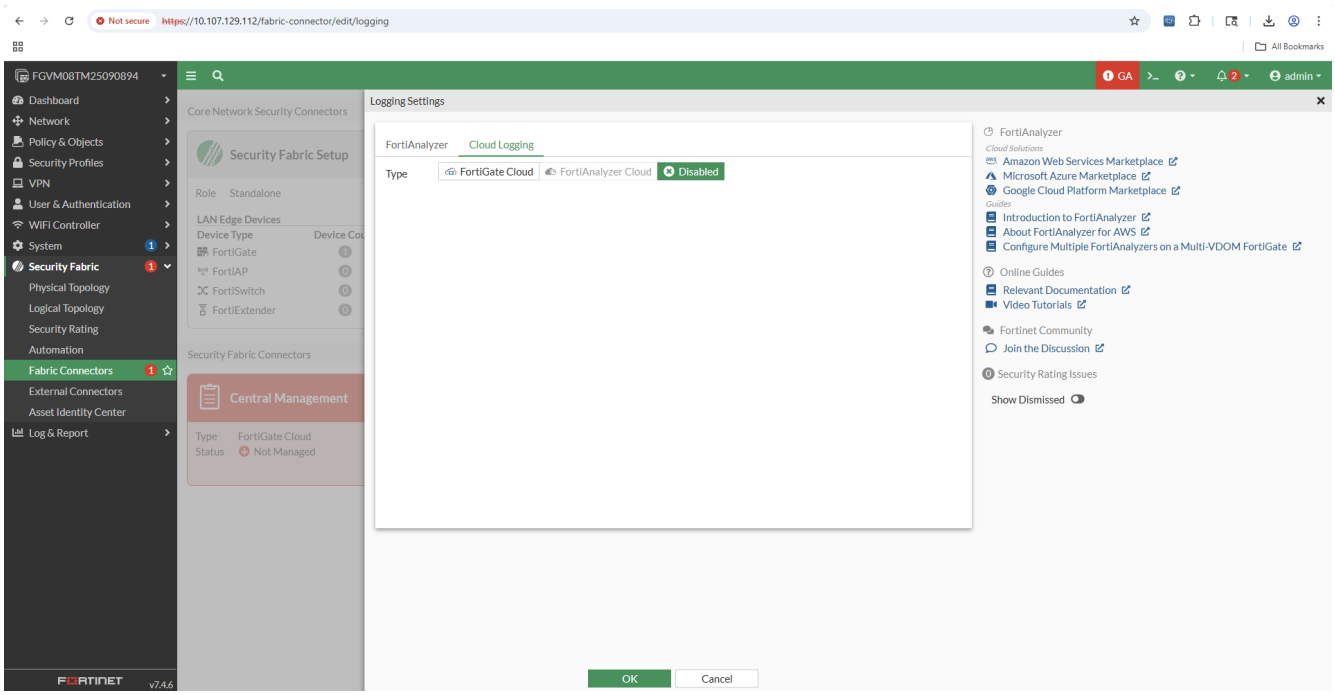




When activating FortiGate Cloud, ensure that Send Logs to FortiGate Cloud is disabled during the activation process.



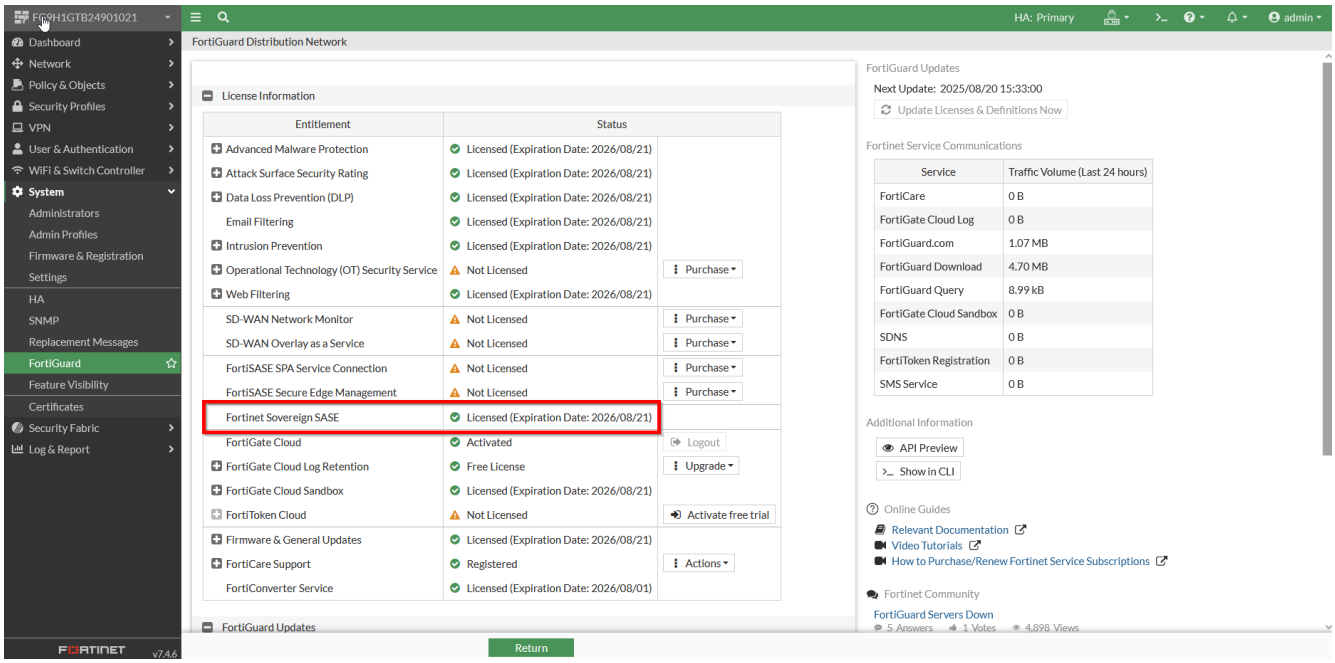
If Send Logs to FortiGate Cloud was mistakenly enabled during activation, you can disable it afterward by navigating to Security Fabric → Fabric Connectors, selecting Logging & Analysis → Cloud Logging, and setting it to Disabled.



It is always a best practice to save your FortiGate configurations before onboarding. This ensures that if re-onboarding is required in the future, you can restore the configurations quickly, keeping the FortiGate in a consistent onboarding state.

Licensing FortiGate Before Onboarding

After registering the FortiSASE-Sovereign entitlement service license on a FortiGate, you must wait until the license status is updated and displayed under License Information on the FortiGate. Only after the license is confirmed as active can the FortiGate be added as a PoP device during onboarding or device management.



FortiGate pre-onboarding checklist

Before starting the onboarding of your FortiGate, you must complete the following checklist to prevent potential issues from happening during the onboarding process.

1. Ensure that the FortiGate device undergoes a full factory reset before starting the onboarding process.
2. Check to see if the log hard disk on your FortiGate needs formatting. Some FortiGate devices have a log hard disk that may not be properly formatted, which can lead to onboarding failures. You can check the state of the log hard disk using the `'get system status'` command. If it returns `'Need format',` then you must format the log hard disk before you proceed. For instructions on how to format the log hard disk, visit https://community.fortinet.com/t5/FortiGate/Technical-Tip-Standard-procedure-to-format-a-FortiGate-Log-Disk/ta-p/190473.
3. Ensure that the signature libraries and license information are up to date:
   a. Execute the `'update-now'` command to
      i. Update all signature libraries.
      ii. Refresh the license information.
   b. Execute the `'diag autoupdate versions'` command to
      i. Confirm that the signature libraries have been successfully updated.
      ii. Compare against the minimum version specified in the reference documentation.
4. Properly connect the PoP FortiGates to the internet for access.
5. Configure IP addresses, default gateway (static routes) for ingress and egress ports.
6. Ensure PoP FortiGates have internet access.

Step 5: Set up your FortiAnalyzer appliance

You can deploy on-premise FortiAnalyzer using either a hardware appliance or a VM with a public IP address, which must be accessible by FGaaS service.

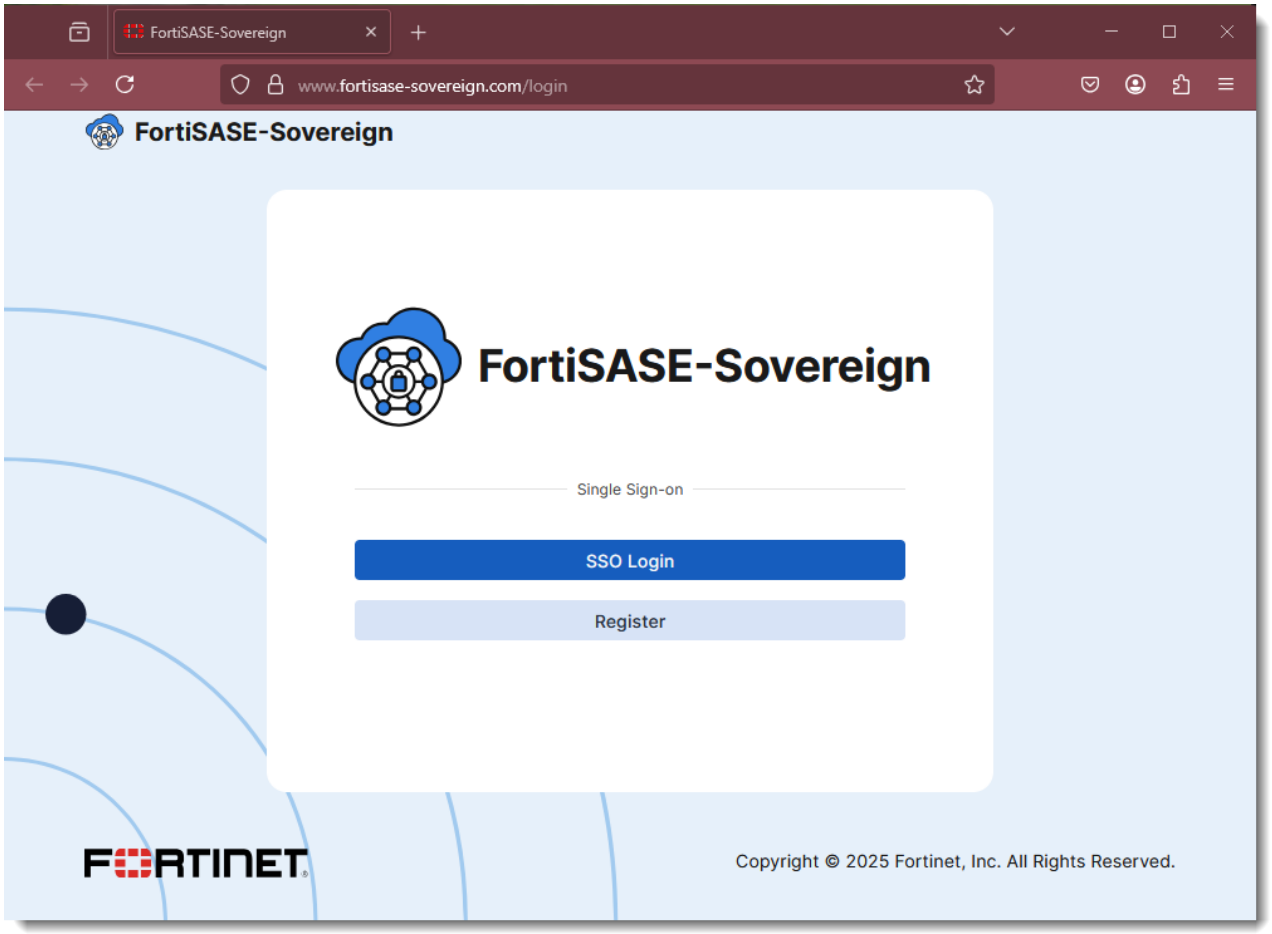
- Ensure that you are using FortiAnylzer 7.4.7 or later.
- Before setting up your FortiAnalyzer appliance, ensure that the FortiAnalyzer admin user has read-write JSON API access and sufficient login-max settings (32 or 256 recommended), as highlighted on the following screenshot.

For information about the service ports on FortiAnalyzer, visit https://docs.fortinet.com/document/fortianalyzer/7.6.0/fortianalyzer-ports/290737/incoming-ports.

Deployment procedure

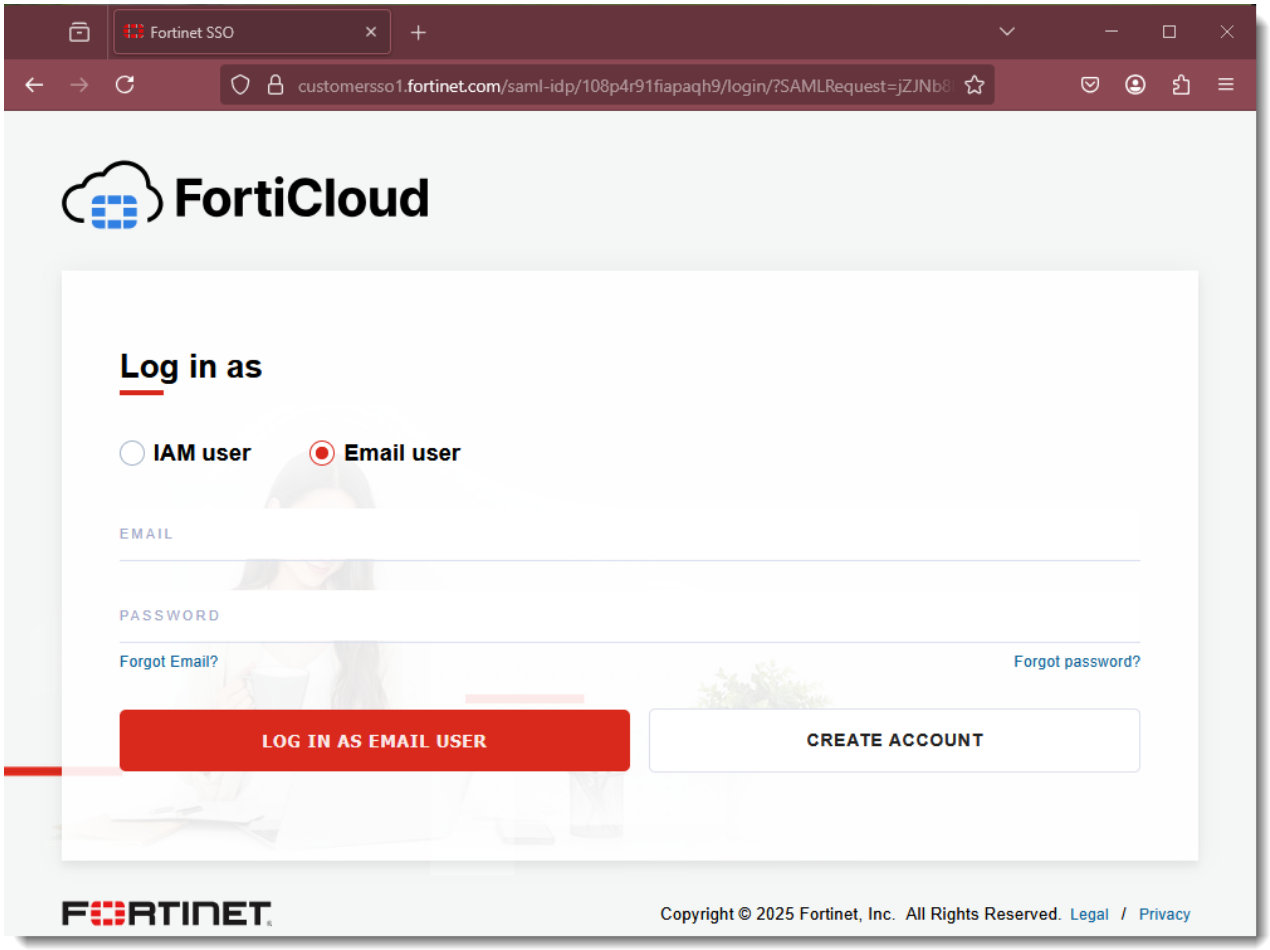
Log on to FortiSASE-Sovereign

1. Open your web-browser, and point to https://www.fortisase-sovereign.com.
   The FortiSASE-Sovereign login page opens.

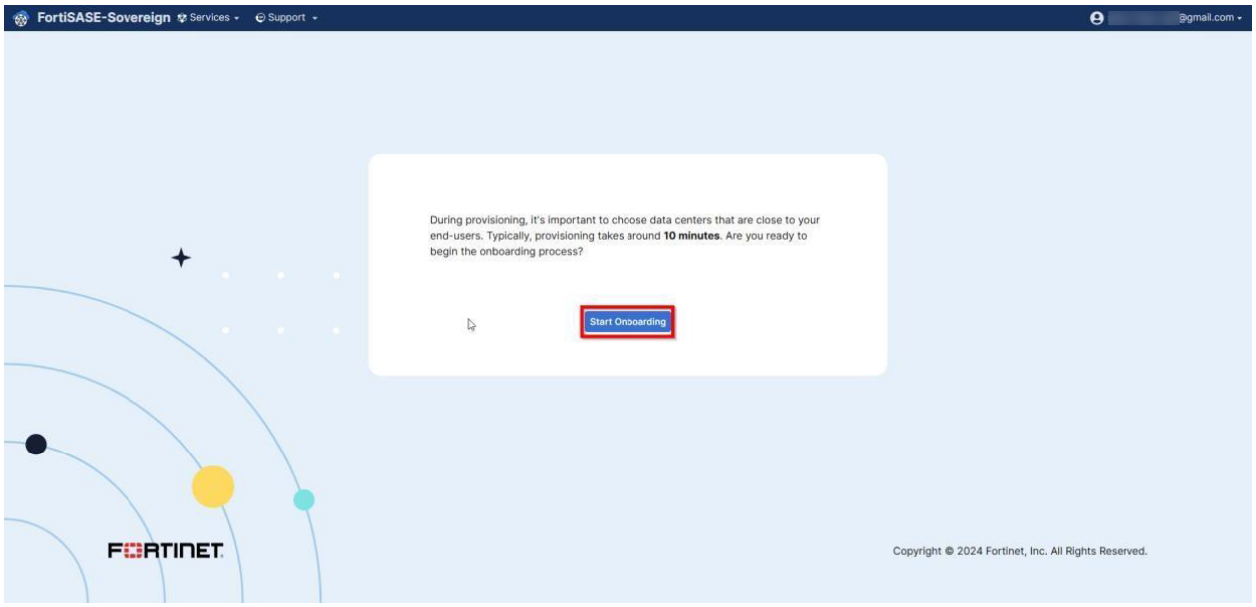


2. Click *SSO Login*.

The FortiCloud login page opens.



3. Select *Email user*, enter your FortiCloud account credentials (email address and password), and click *LOG IN AS EMAIL USER*.
4. Check your email, copy and paste the security code into the Security Code field, and click *Go*.
   You are now directed to the FortiSASE-Sovereign portal's landing page.

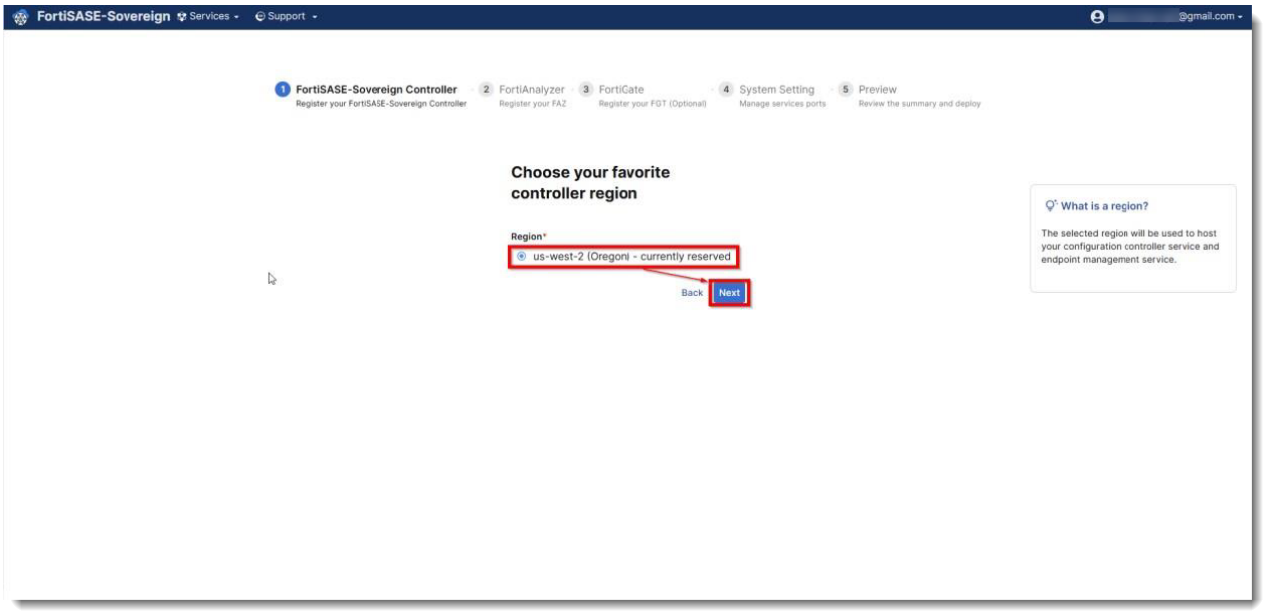


5. Click *Start Onboarding* to begin the deployment process by following the onboarding wizard across the top of the screen.

Configure FortiSASE-Sovereign Controller

1. Under FortiSASE-Sovereign Controller, select a preferred geographical region for your FortiSASE-Sovereign controller.

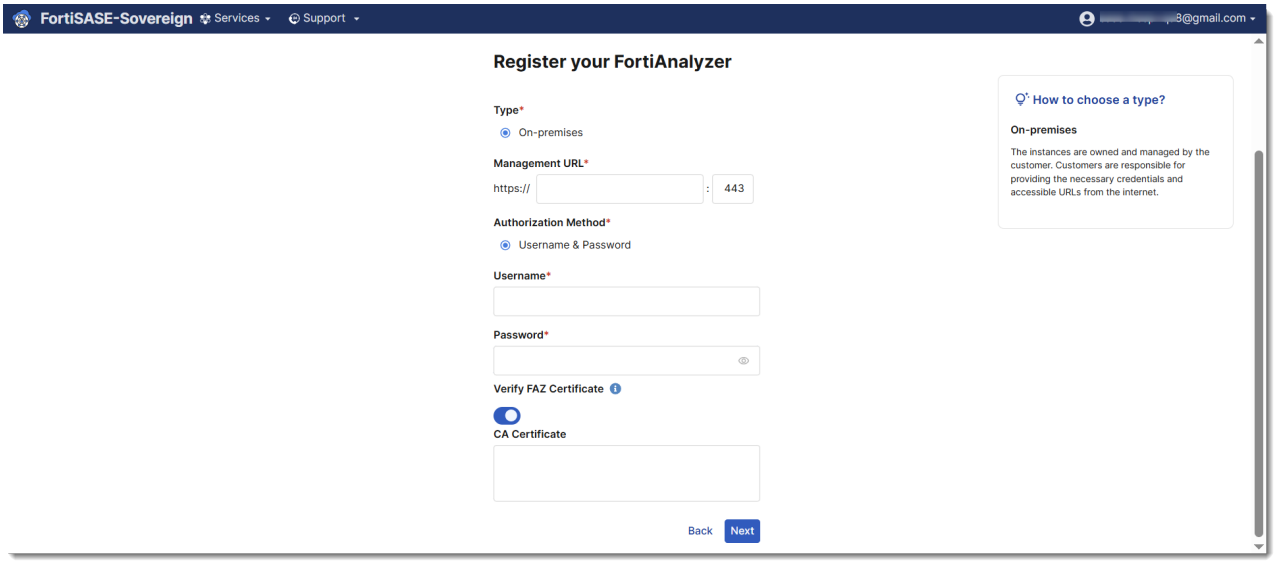
The FortiSASE-Sovereign Controller refers to FortiManager and FortiClient EMS that manage the various components of FortiSASE-Sovereign.



2. Click *Next*.

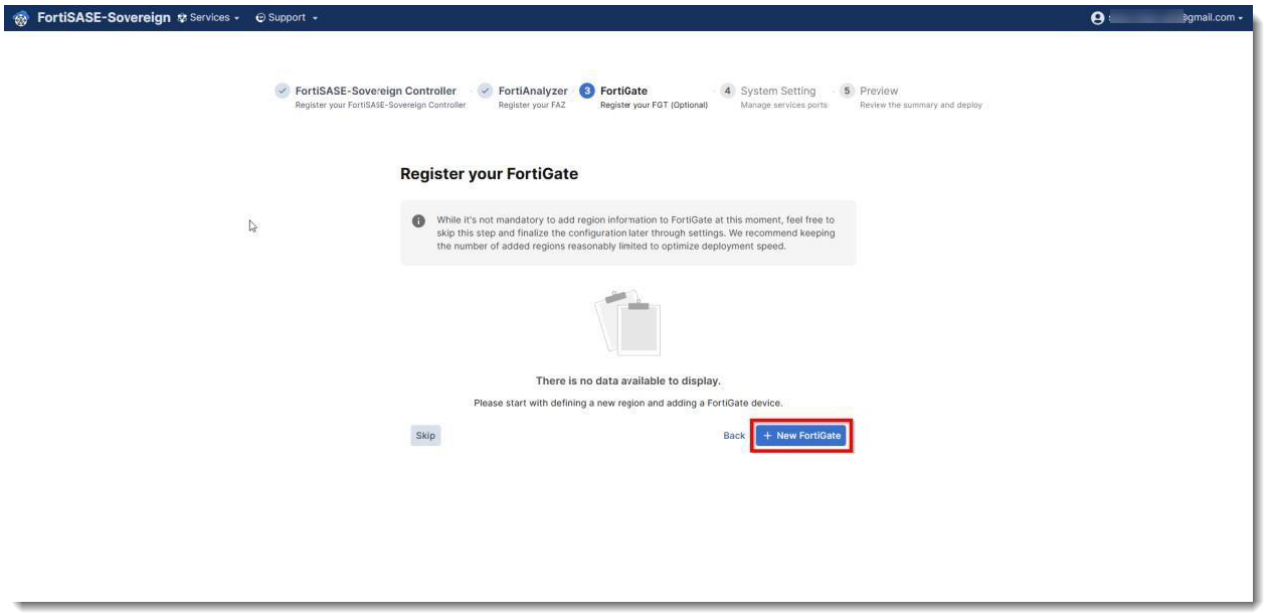
Configure FortiAnalyzer

1. Under *FortiAnalyzer*, click *Register your FortiAnalyzer*.
2. Select *On-Premises*
3. Enter the *Management URL*.
4. Choose *Username & Password* as *Authentication Method*.
5. Click *Next*.

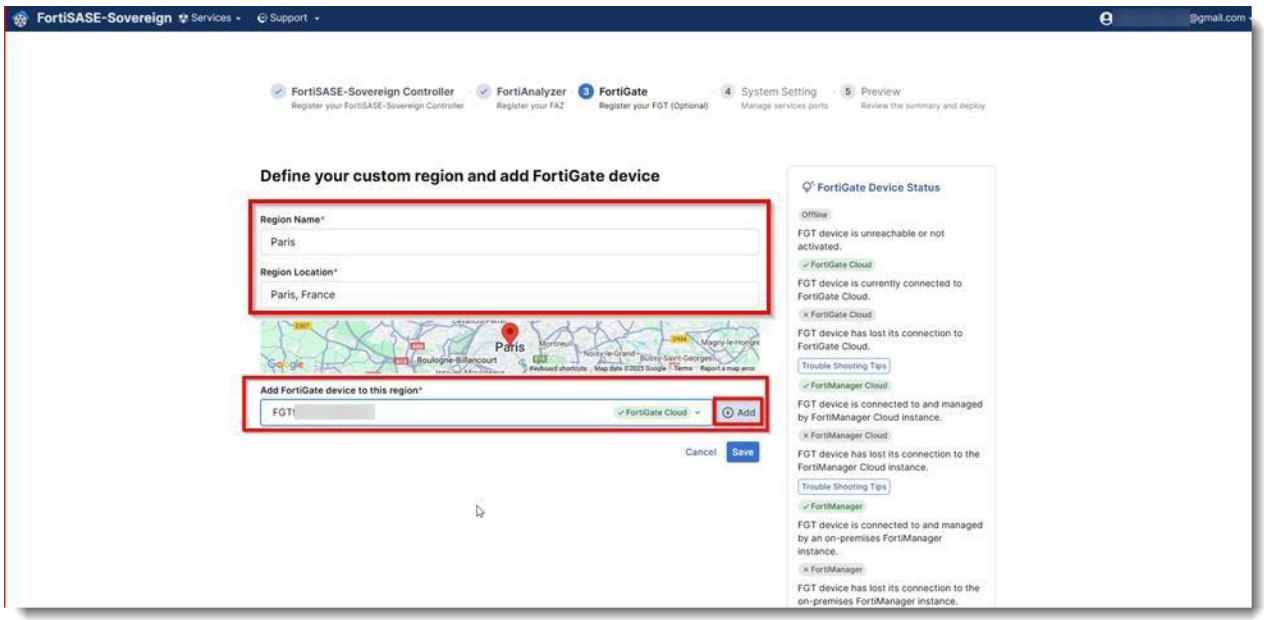


Configure FortiGate

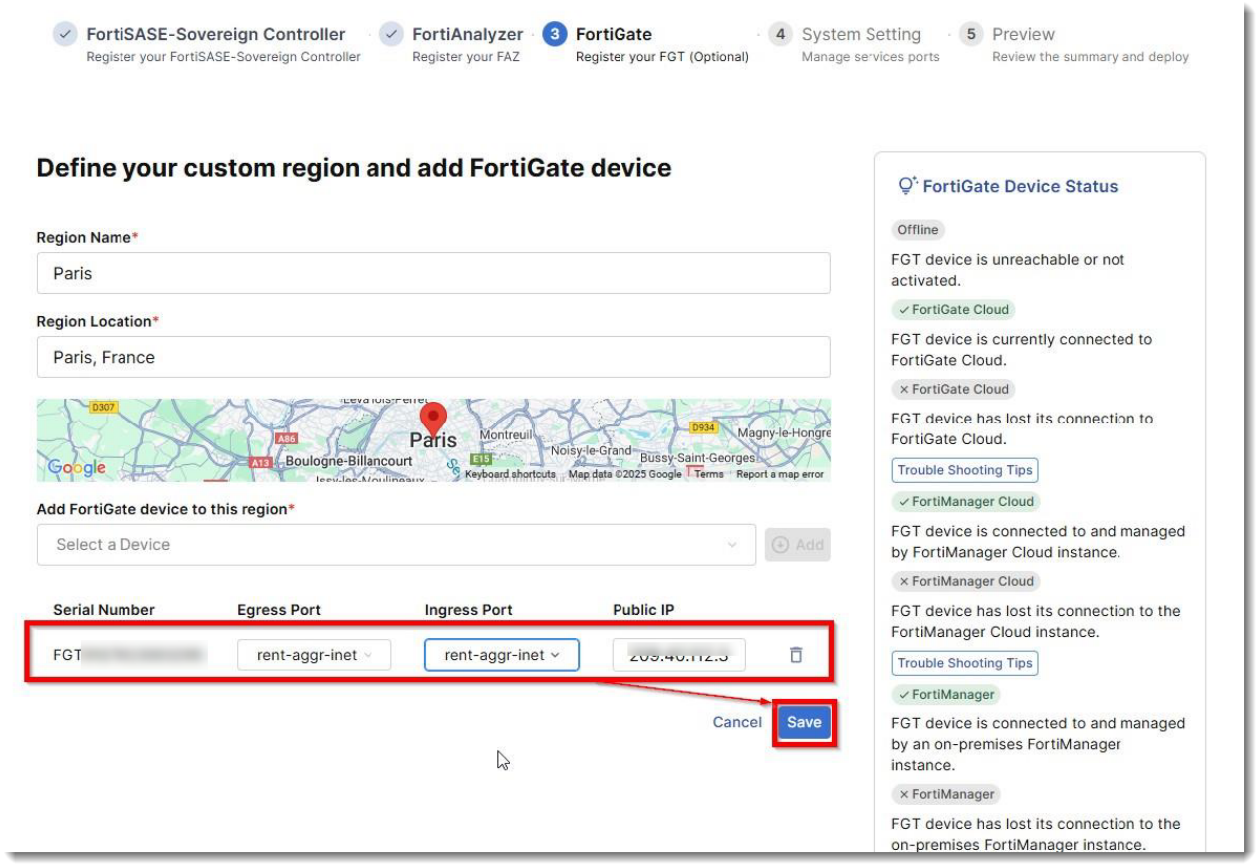
1. Under FortiGate, click *+ New FortiGate*.



2. Define your custom region by entering the *Region Name* and *Region Location*, select a FortiGate appliance, and click *Add*.



3. Verify the Egress Port and the Ingress Port, specify the public IP, and click *Save*.

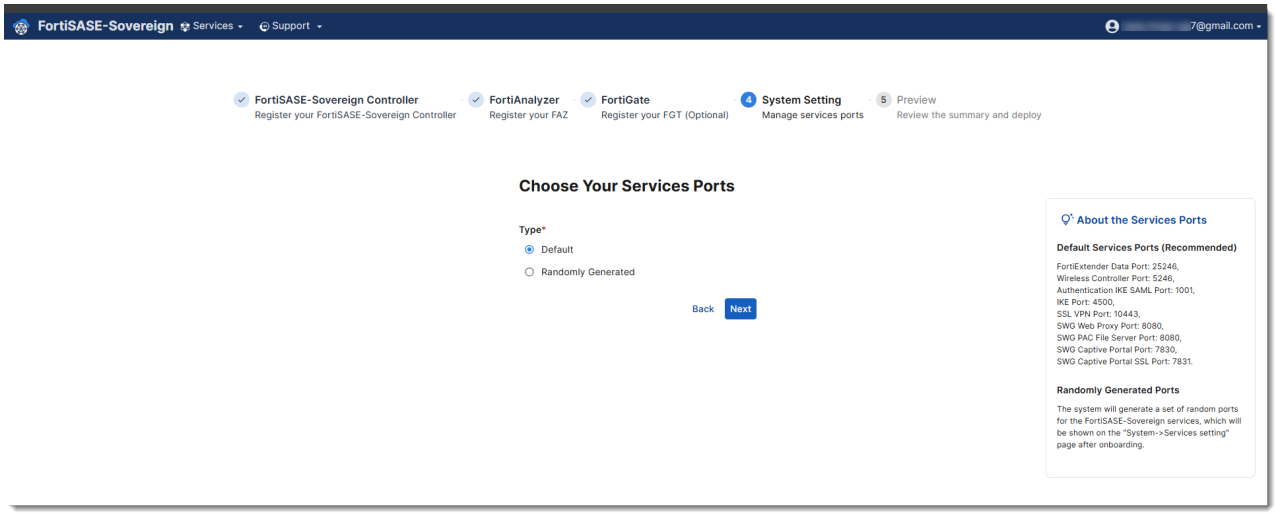


4. Go back to the *Register your FortiGate* page, and verify the location of the FortiGate in *List View* and *Map View*, and click *Next*.

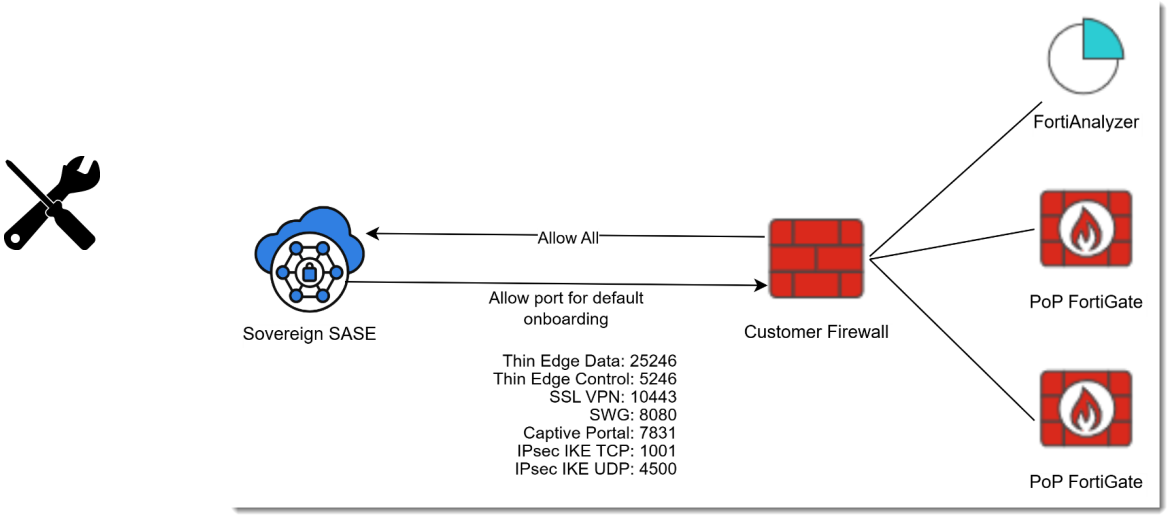
Choose services ports

Default Service Ports

1. Under Service Setting, set *Choose Your Services Ports* to *Default*, and click *Next*.

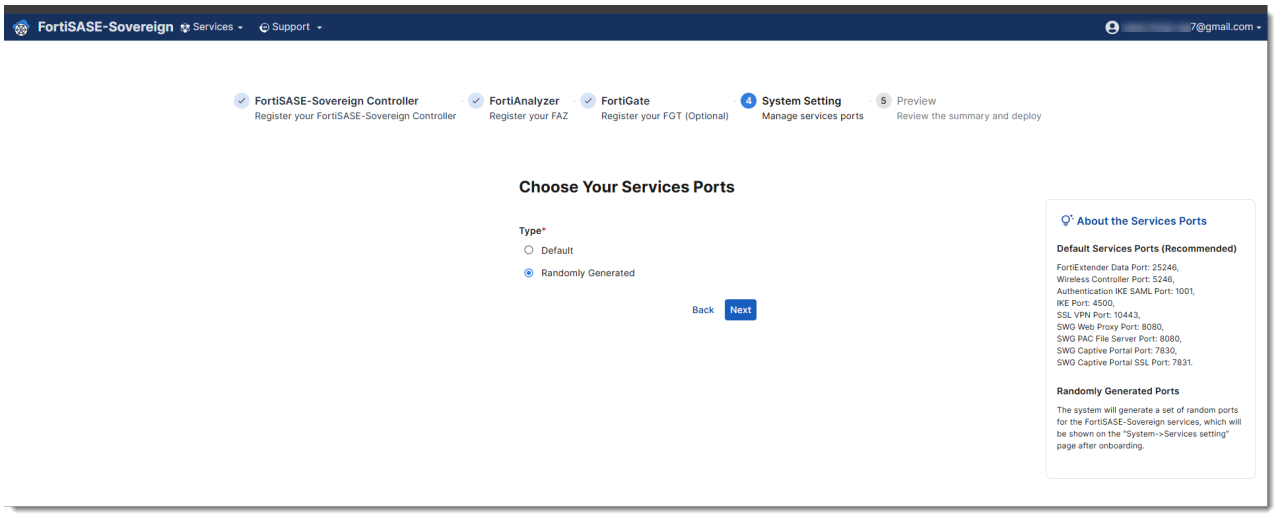


- If you set *Choose Your Services Ports* to *Default*, you must ensure that those default services ports are open on the client. The following diagram highlights the default services ports.



Random Service Ports

1. Under Service Setting, set *Choose Your Services Ports* to *Randomly Generated* , and click *Next*.



If you deploy FortiSASE-Sovereign using randomly generated ports, you must review and record the system-assigned ports after onboarding. To do so, go to System → Service Settings, note the generated ports for each service, and ensure they are provisioned and allowed in your network.

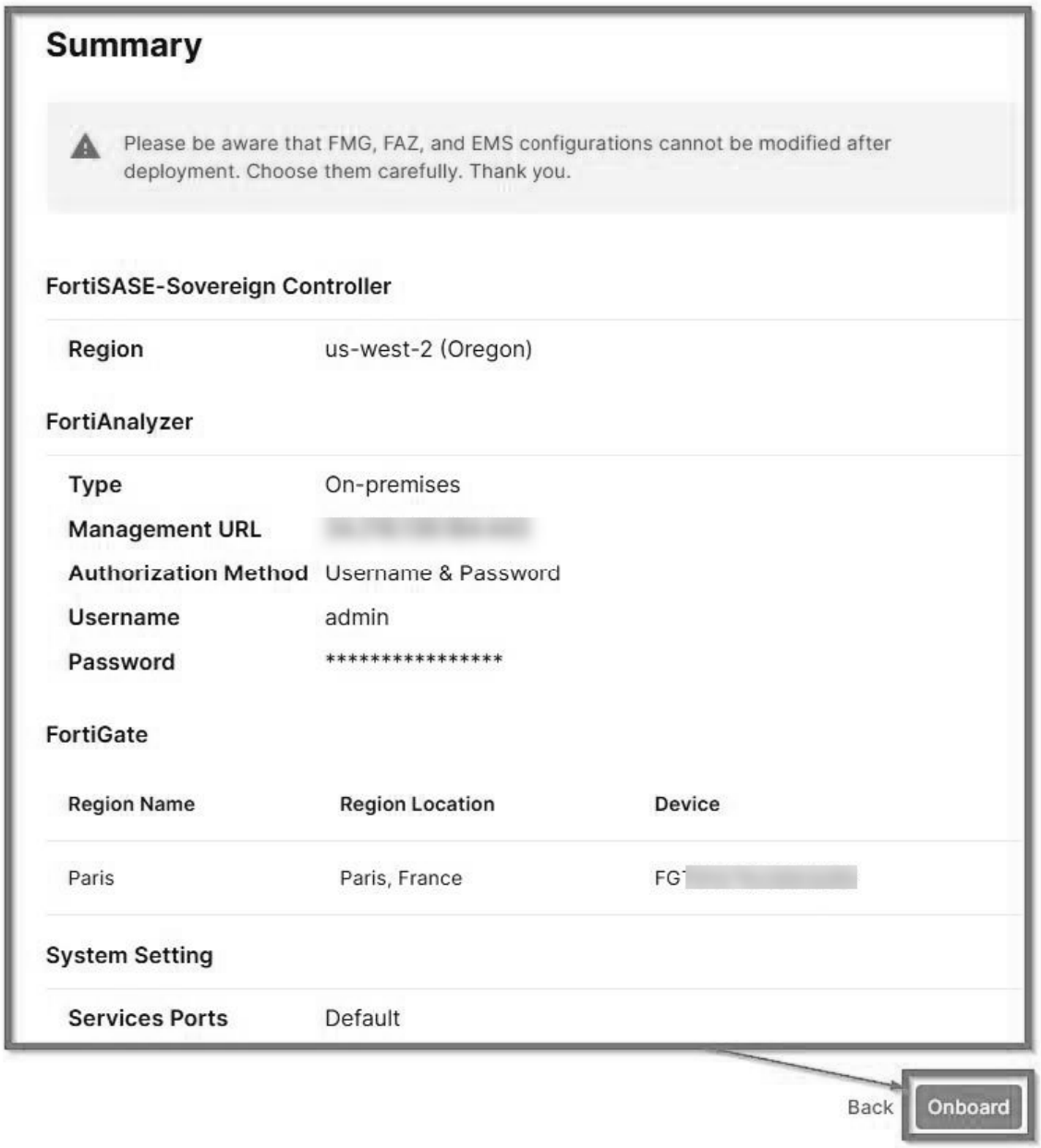
Before selecting service ports, consider the following:

- If the default ports are not already in use by on-premises applications, use them and ensure they are provisioned and open on client devices:
  - Thin Edge Data: 25246
  - Thin Edge Control: 5246
  - SSL VPN: 10443
  - SWG: 8080
  - Captive Portal: 7831
  - IPsec IKE TCP: 1001
  - IPsec IKE UDP: 4500
- If there are port conflicts in your network, select randomly generated ports. These ports must be provisioned in the same way as the default ports to ensure client access. However, the actual port numbers will only be available after FortiSASE-Sovereign is successfully onboarded.

After onboarding, navigate to System → Service Settings to view and record all randomly generated ports.

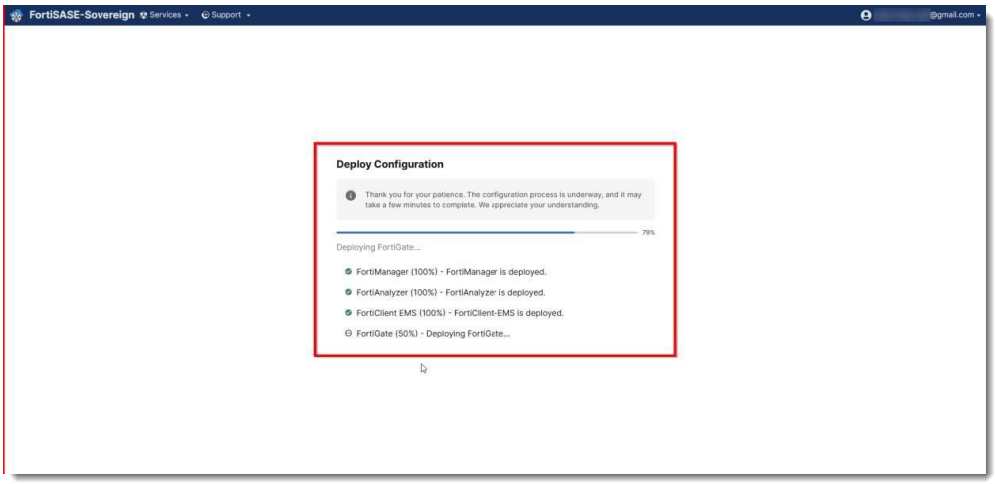
Review and deploy

1. On the Summary page, review all the parameters you've configured.
2. Click *Onboard* to start deploying FortiSASE-Sovereign.

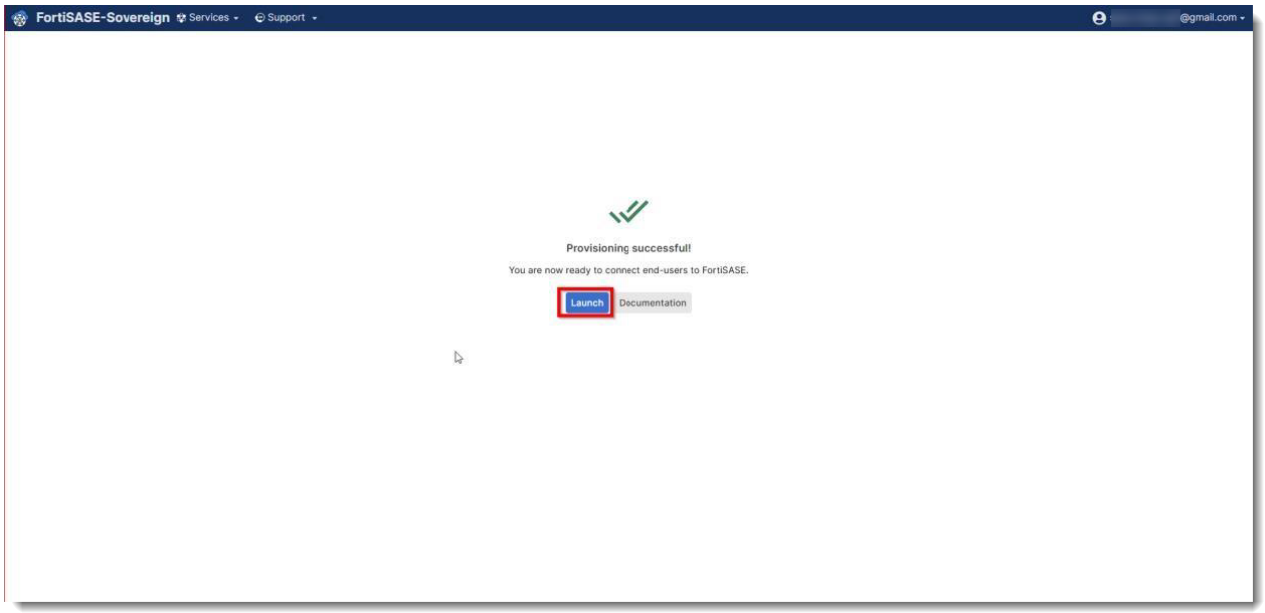

Summary
Please be aware that FMG, FAZ, and EMS configurations cannot be modified after deployment. Choose them carefully. Thank you.
FortiSASE-Sovereign Controller
Region
us-west-2 (Oregon)
FortiAnalyzer
Type
On-premises
Management URL
Authorization Method
Username & Password
Username
admin
Password
****
FortiGate
Region Name
Region Location
Device
Paris
Paris, France
FG
System Setting
Services Ports
Default
Back
Onboard

During onboarding, the system deploys the configurations for the following:

- FortiManager
- FortiAnalyzer
- FortiClient EMS
- FortiGate



3. When the deployment is completed, click *Launch* to start the FortiSASE-Sovereign Portal.



By default, the system automatically selects your primary account and redirects to the FortiSASE-Sovereign portal, as illustrated in the following screenshot.

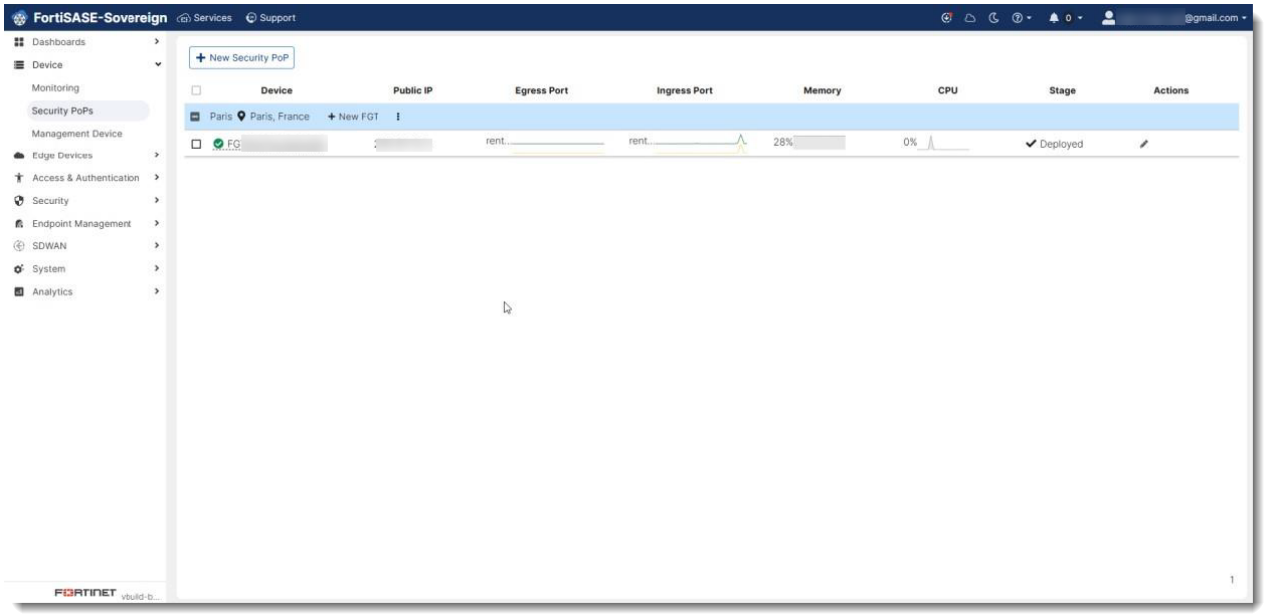
Manage Security PoP

The Device>Security PoP page provides tools to manage your FortiGate devices. Here you can:

- Check FortiGate status on page 32
- Add FortiGate devices on page 32

Check FortiGate status

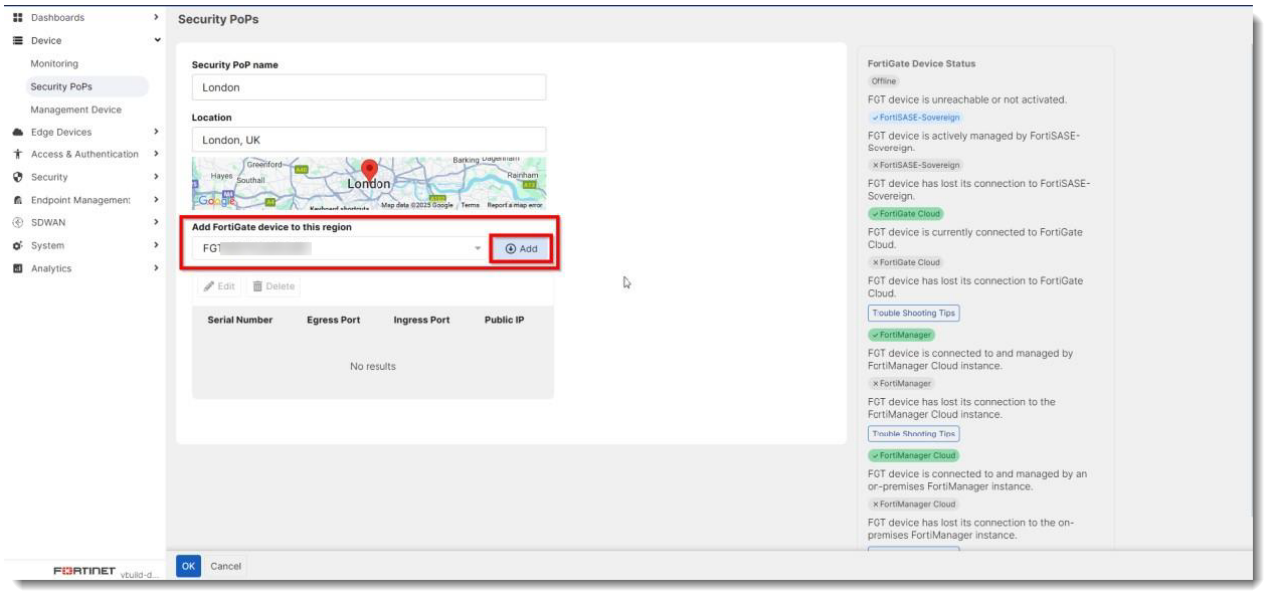
1. On the main menu, select *Device>Security PoP*.



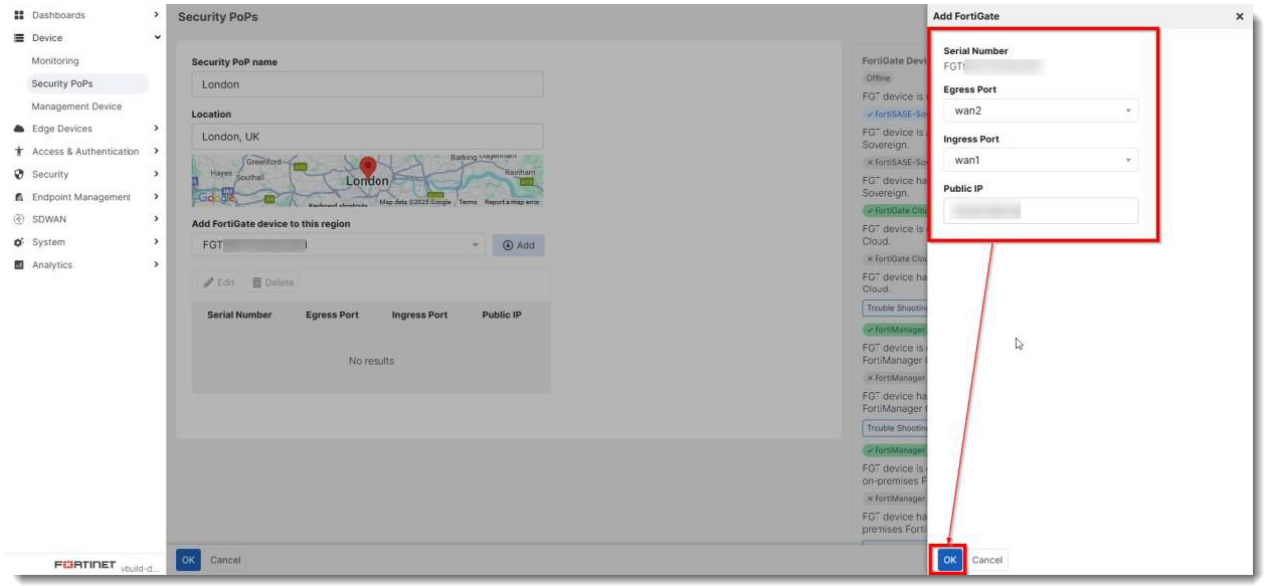
2. Check the operating status of the deployed FortiGate by reviewing the data on the page.

Add FortiGate devices

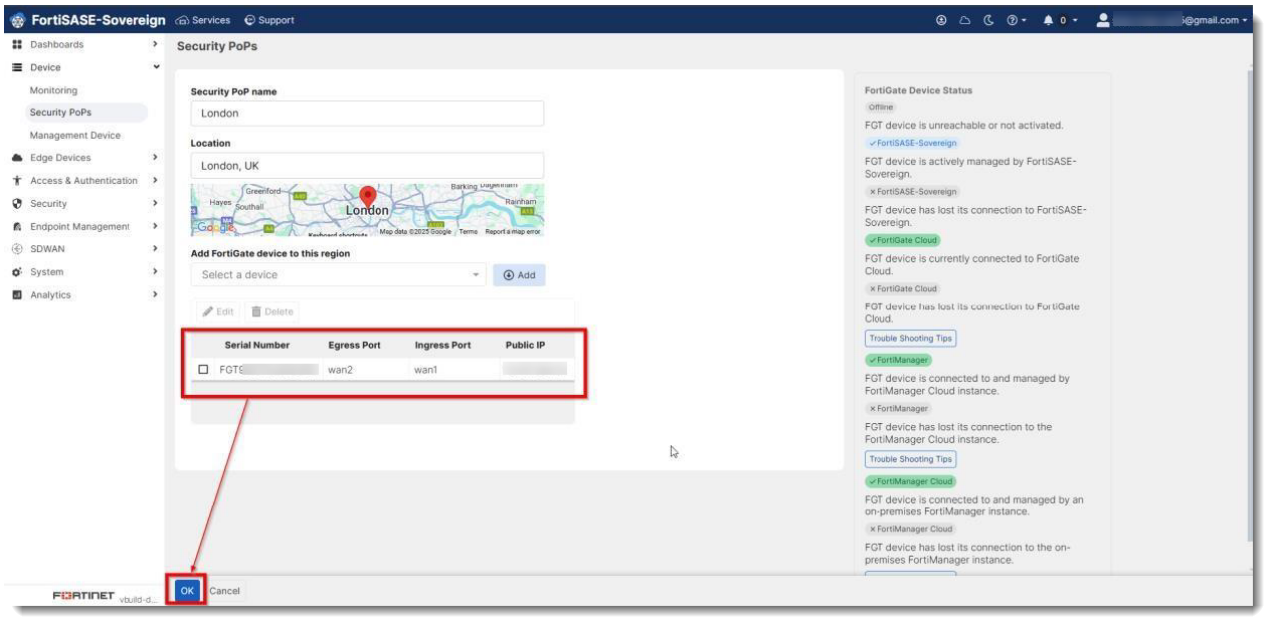
1. On the *Device>Security PoP* page, click *+ New Security PoP* to add a new Security PoP region.
2. Select a FortiGate device, and click *Add* to add it to the region.



3. Make the required configurations as illustrated in the following screenshot, and click *OK* to save the configuration.



4. Review the device information of the newly added FortiGate, and click *OK*.



5. After the FortiGate is added, verify the newly added Security PoP on the *Device>Security PoP* page.

Once deployed, you can manage the FortiGate device through Port 5443 using the HTTPS protocol.

Configuring Secure Internet Access (SIA) profile

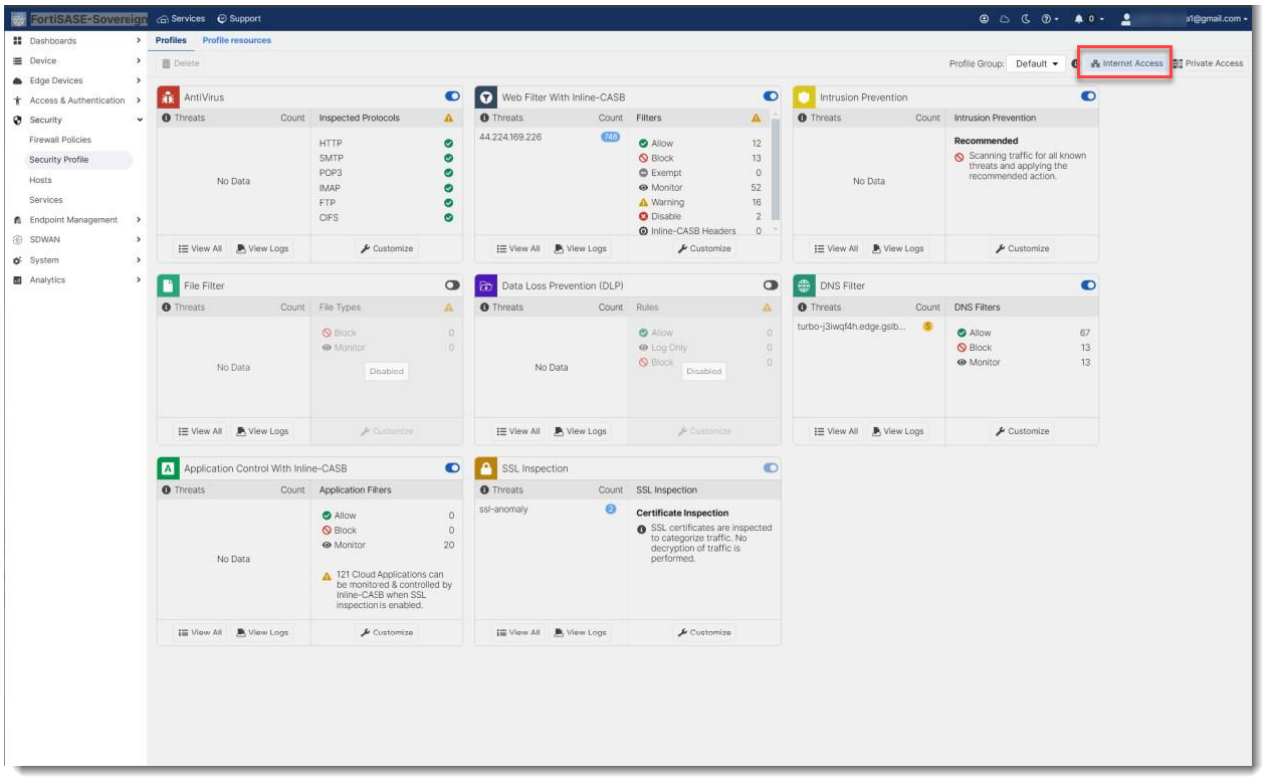
This section outlines the steps to configure a Secure Internet Access (SIA) profile.

To create a secure private access profile, you must select *Private Access*. The default Profile Group for Internet Access and Private Access are different, though they bear the same name, *Default*.)

Example: Block access to TikTok (www.tiktok.com).

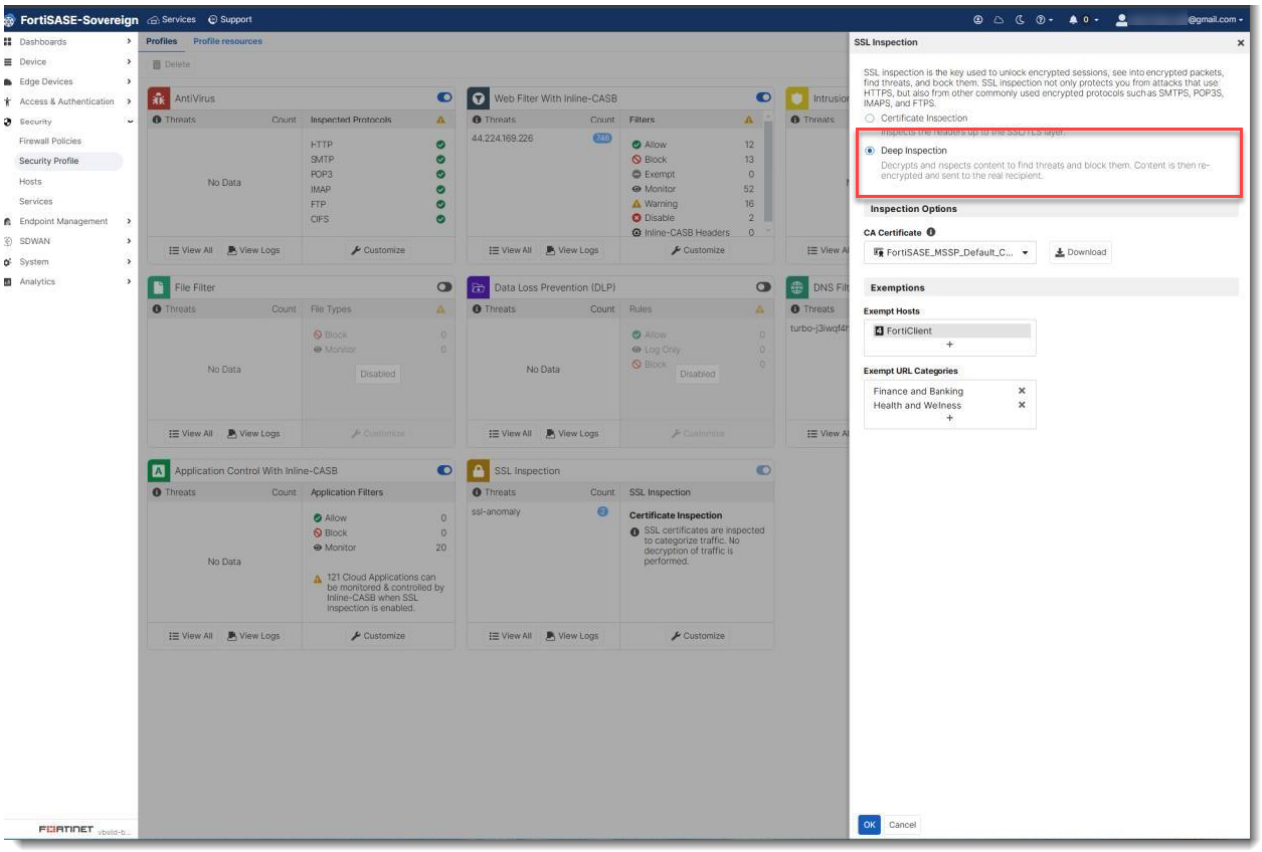
Step 1: Create a secure internet access profile

1. From main menu, select *Security>Security Profile*.
2. Select *Internet Access*.



Step 2: Customize SSL inspection

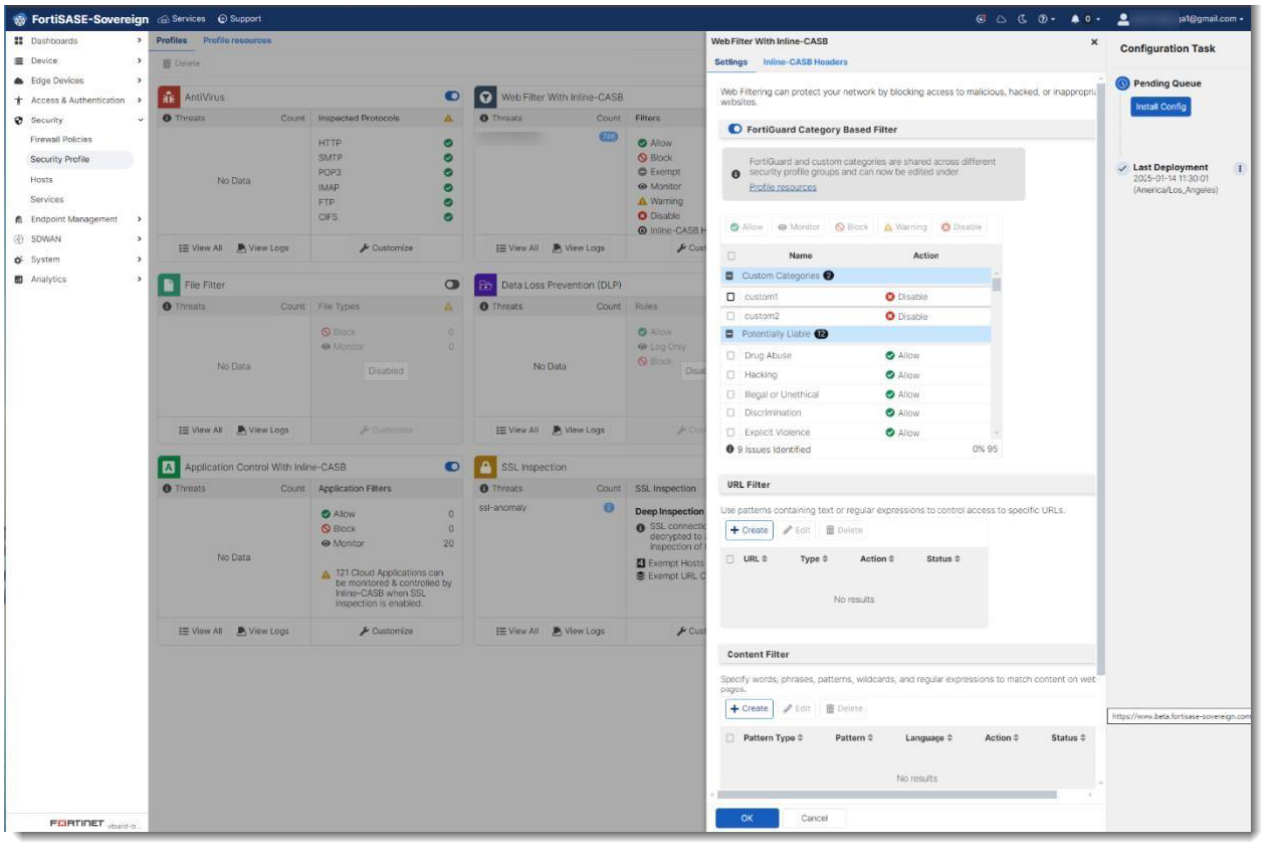
1. On the *SSL Inspection* widget, select *Customize*.
2. In the *SSL Inspection* panel, select *Deep Inspection* because most security profiles require SSL Inspection be set to *Deep Inspection*.



When *Deep Inspection* is selected, the *Force Certificate Inspection* switch on firewall policy screen must be set to *off*.

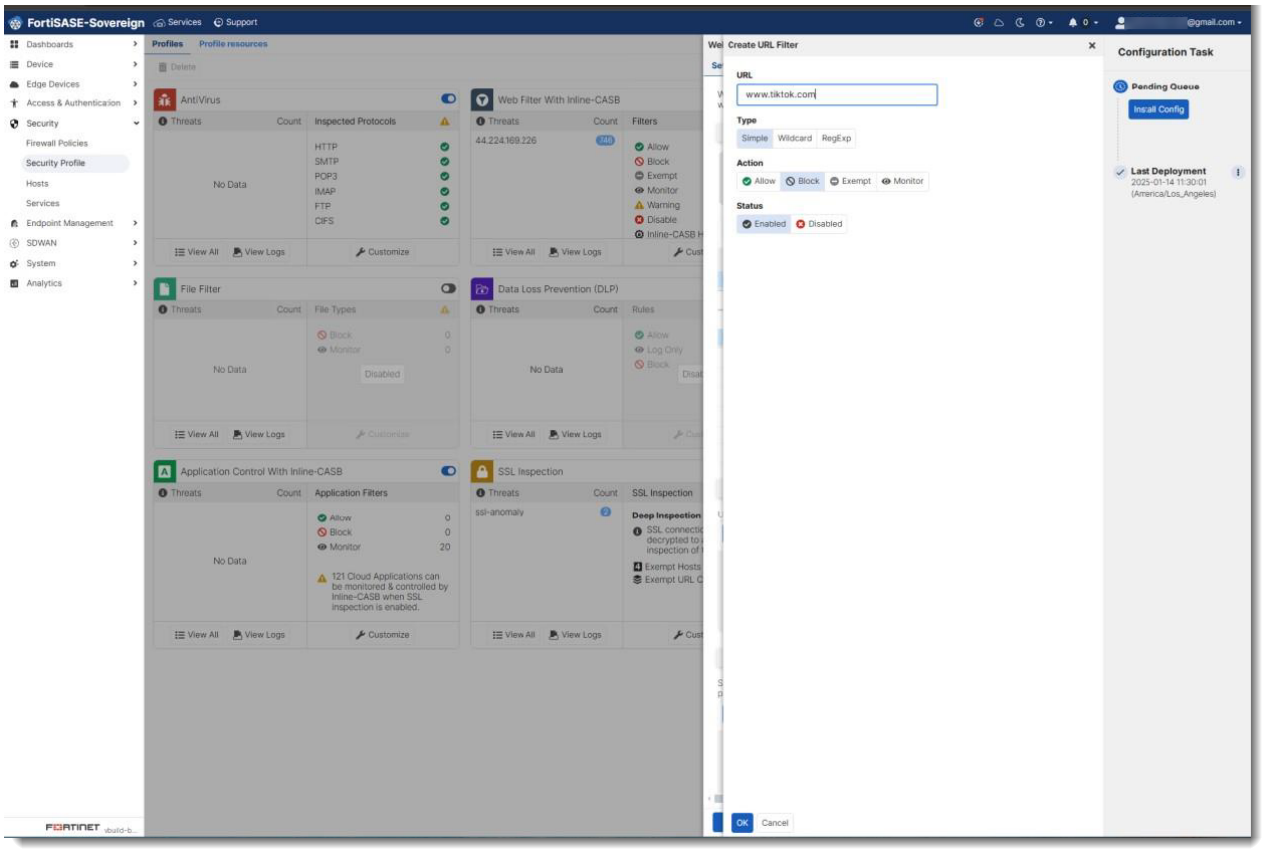
Step 3: Enable web filter with Inline-CASB

1. On the *Web Filter With Inline CASB* widget, click *Customized* to bring up the *Web Filter With Inline-CASB* panel.
2. Make the required configurations as shown in the following screenshot.



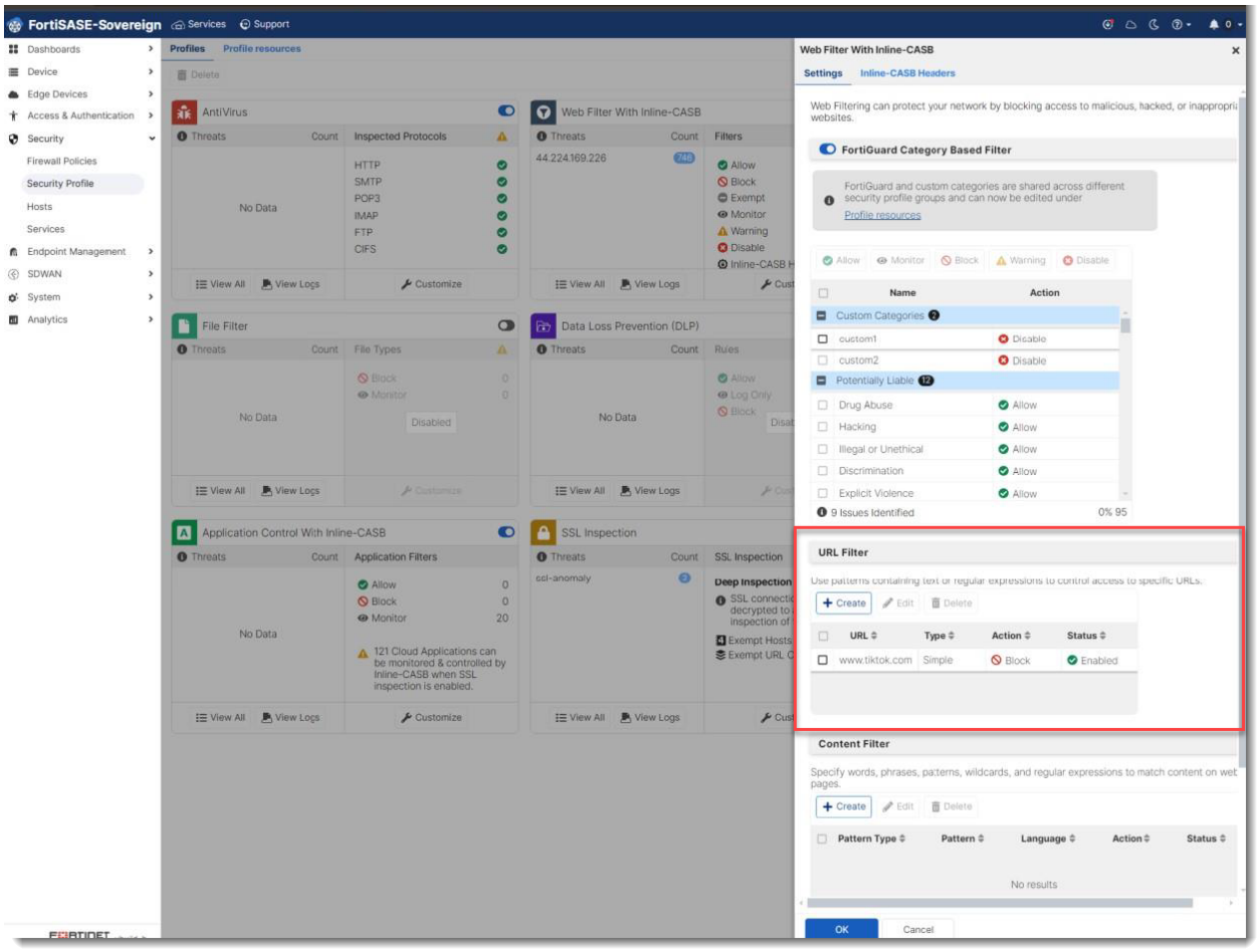
Step 4: Create a URL filter

1. On *URL Filter* widget, click *Create* to bring up the *Create URL Filter* panel
2. Make the desired configurations as shown on the following screenshot.



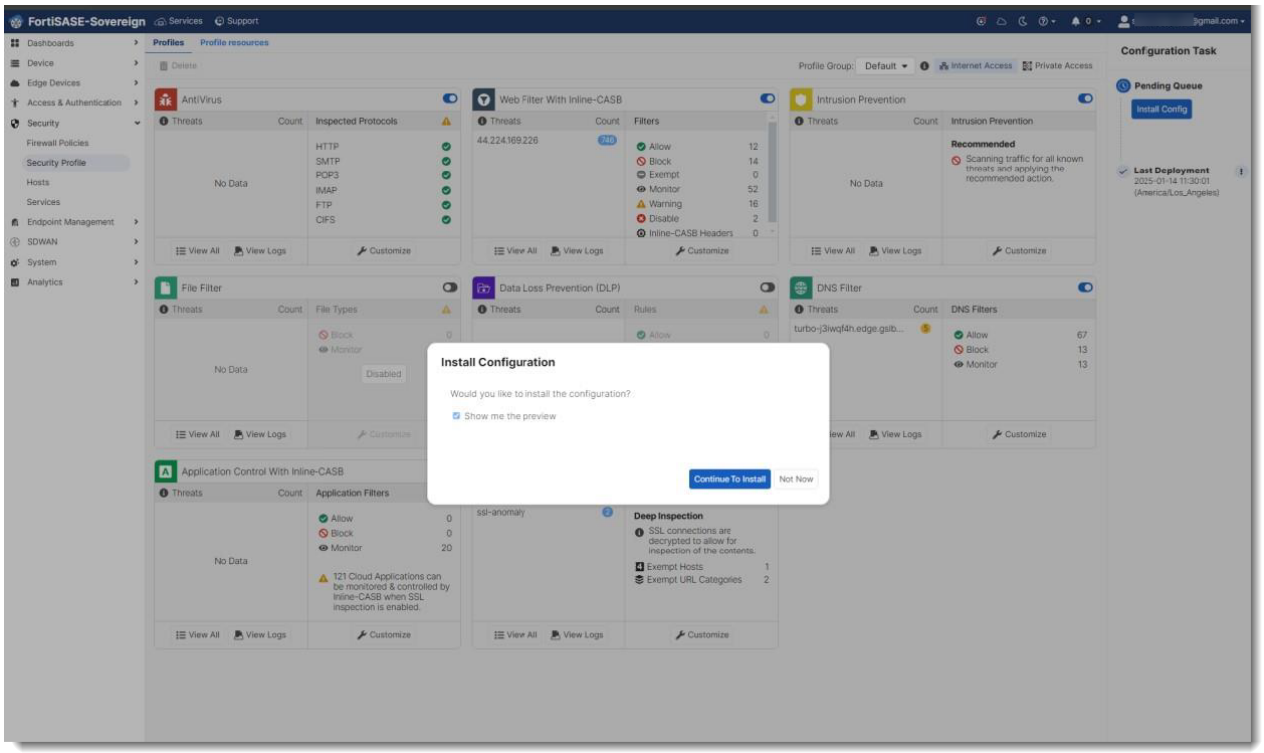
Step 5: Verify the URL filter

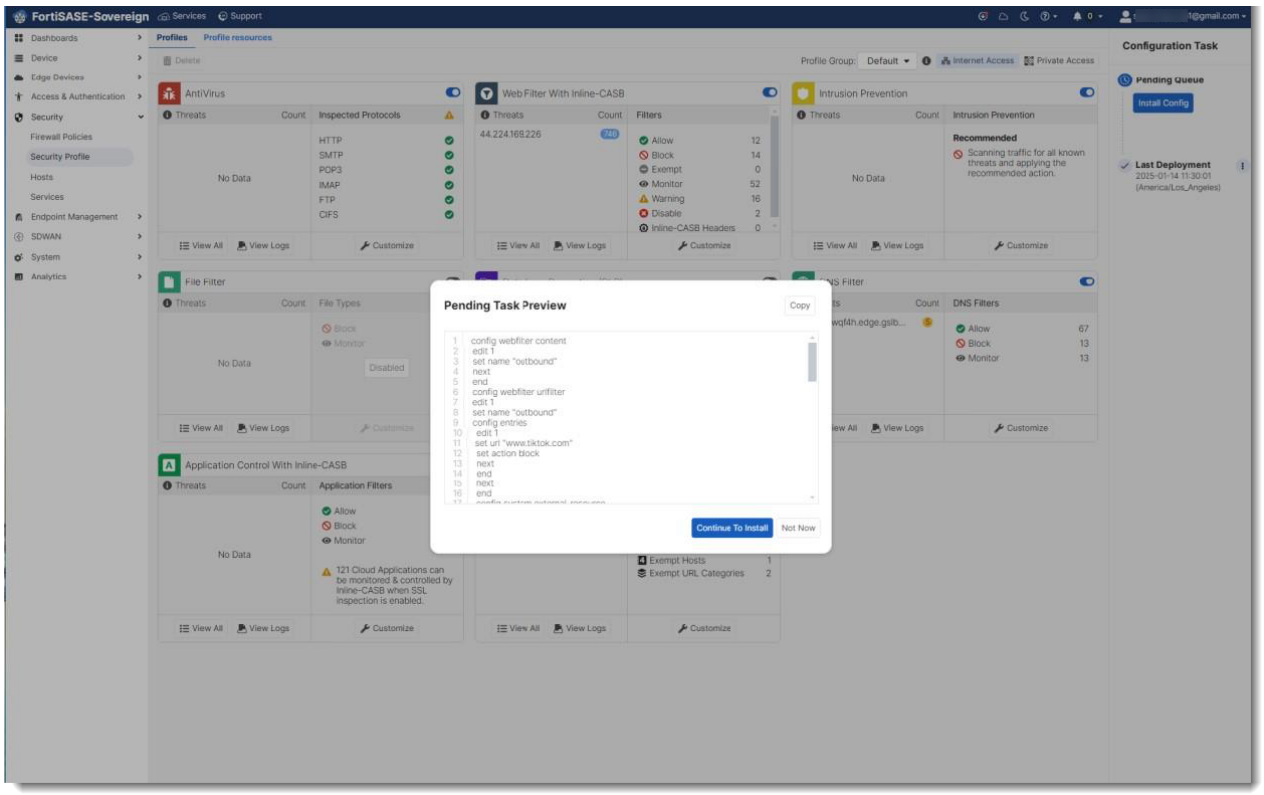
1. After creating the URL Filter rule, open the URL Filter widget.
2. Make sure www.tiktok.com with block action is added to the URL Filter panel.

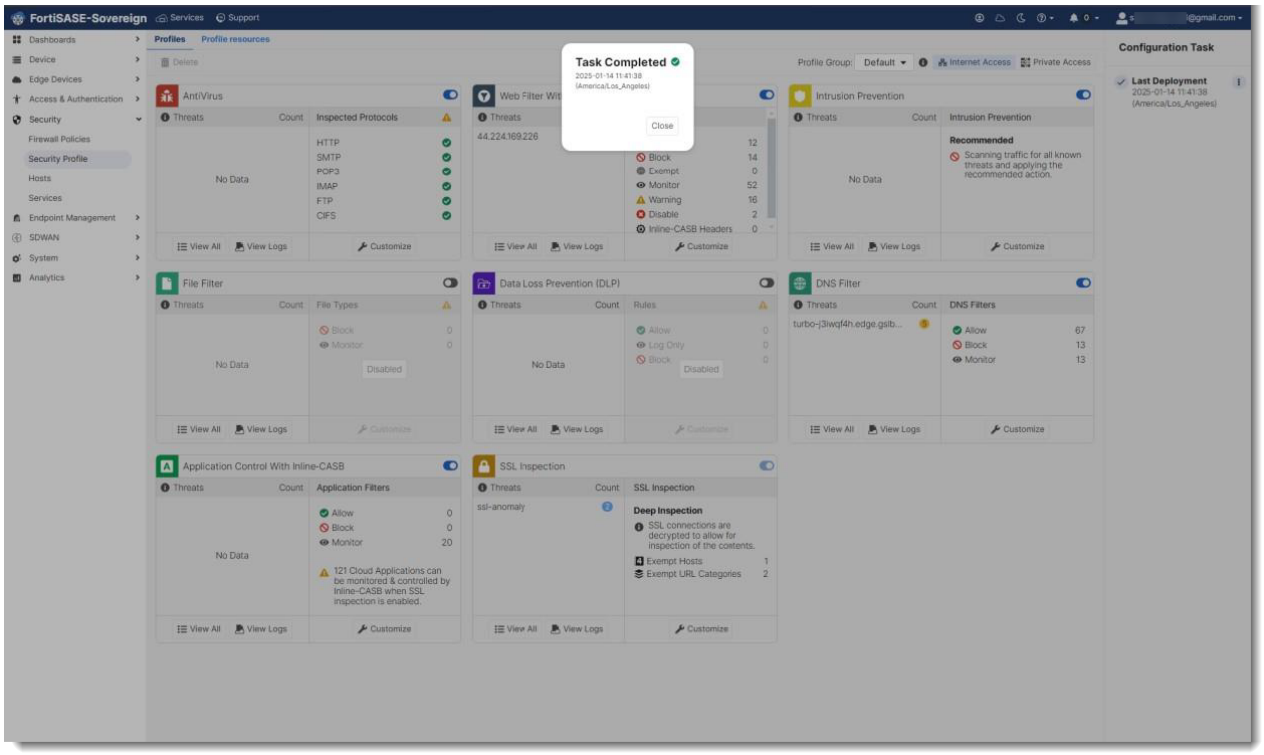


Step 6: Push the SIA profile to PoP FortiGates

1. When prompt, click the *Install Config* button to start installing the SIA profile configuration onto the PoP FortiGates.
2. Follow the prompts onscreen to complete the installation.

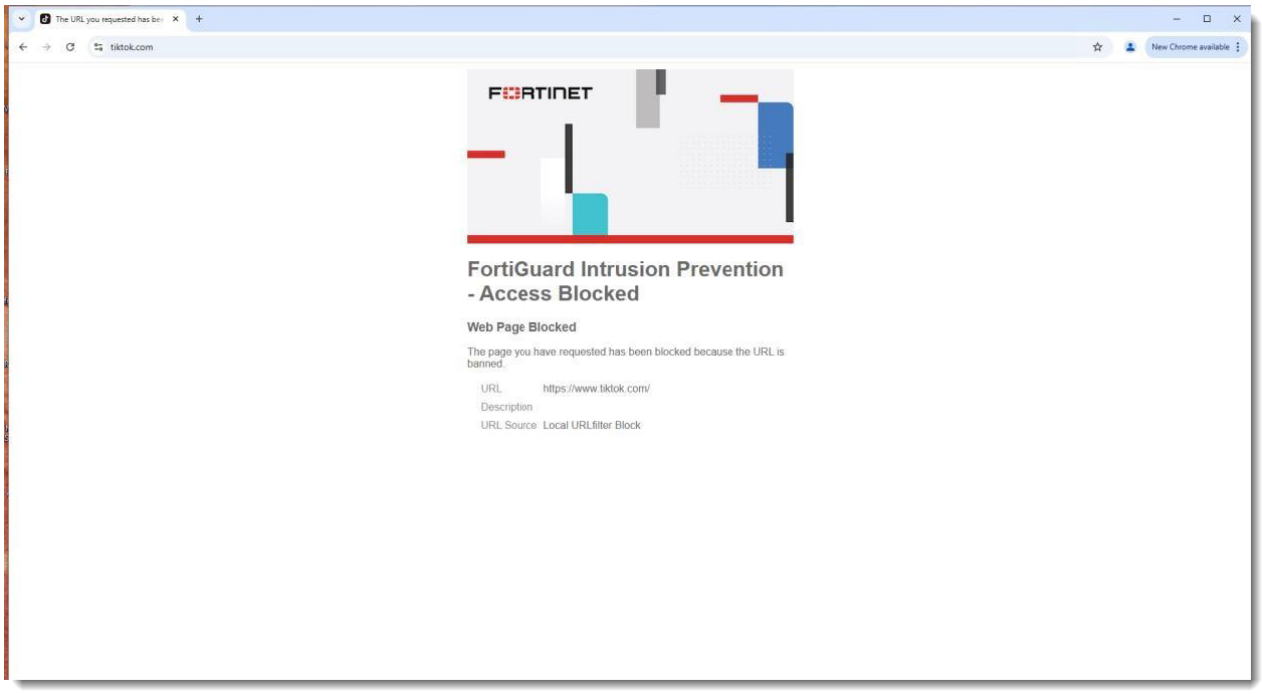

FortiSASE-Sovereign
Services
Support
Profiles
Profile resources
Configuration Task
Pending Queue
Install Config
Last Deployment
2025-01-14 11:30:01
(America/Los_Angeles)
Profile Group: Default
Internet Access
Private Access
AntiVirus
Web Filter With Inline-CASB
Intrusion Prevention
File Filter
Data Loss Prevention (DLP)
DNS Filter
Application Control With Inline-CASB
Install Configuration
Would you like to install the configuration?
Show me the preview
Continue To Install
Not Now


FortiSASE-Sovereign
Services
Support
Profiles
Profile resources
Configuration Task
Pending Queue
Install Config
Last Deployment
2025-01-14 11:30:01
(America/Los_Angeles)
Profile Group: Default
Internet Access
Private Access
AntiVirus
Web Filter With Inline-CASB
Intrusion Prevention
File Filter
Application Control With Inline-CASB
Pending Task Preview
Copy
Continue To Install
Not Now



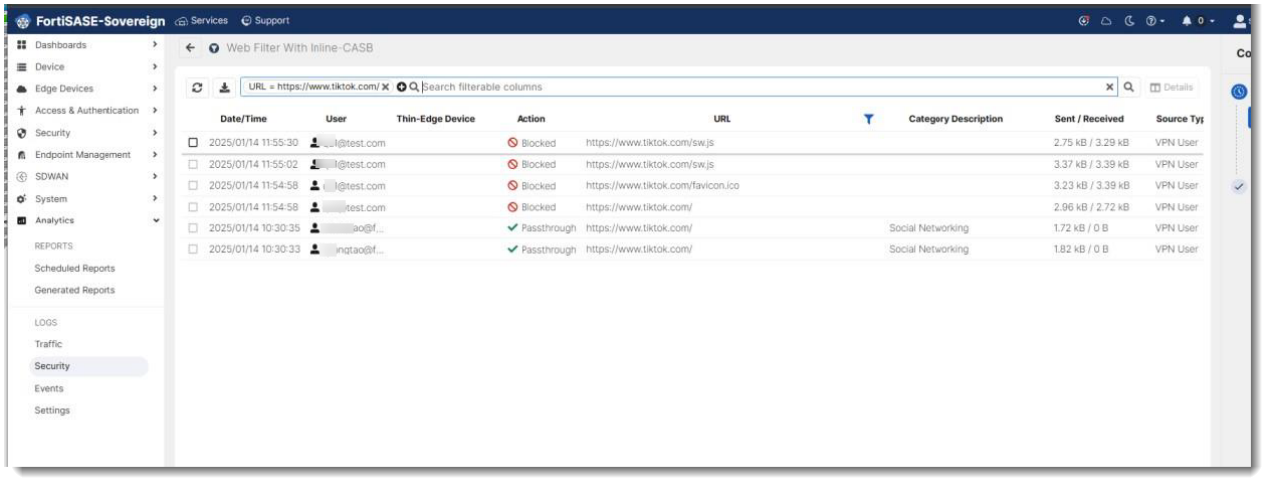
Step 7: Test the SIA profile

1. In FortiClient endpoint machine, start a browser, and type `https://www.tiktok.com` and press *Enter*.
2. Check the response onscreen, as shown in the following screenshot.



Step 8: Review Logs

1. On In the FortiSASE-Sovereign portal, select *Analytics* > *Security*.
2. Open *Web Filter with Inline-CASB*.
3. Do a keyword search similar to the what is shown on the following screenshot.
   You should see the log indicating access to TikTok has been blocked.



Configure LDAP

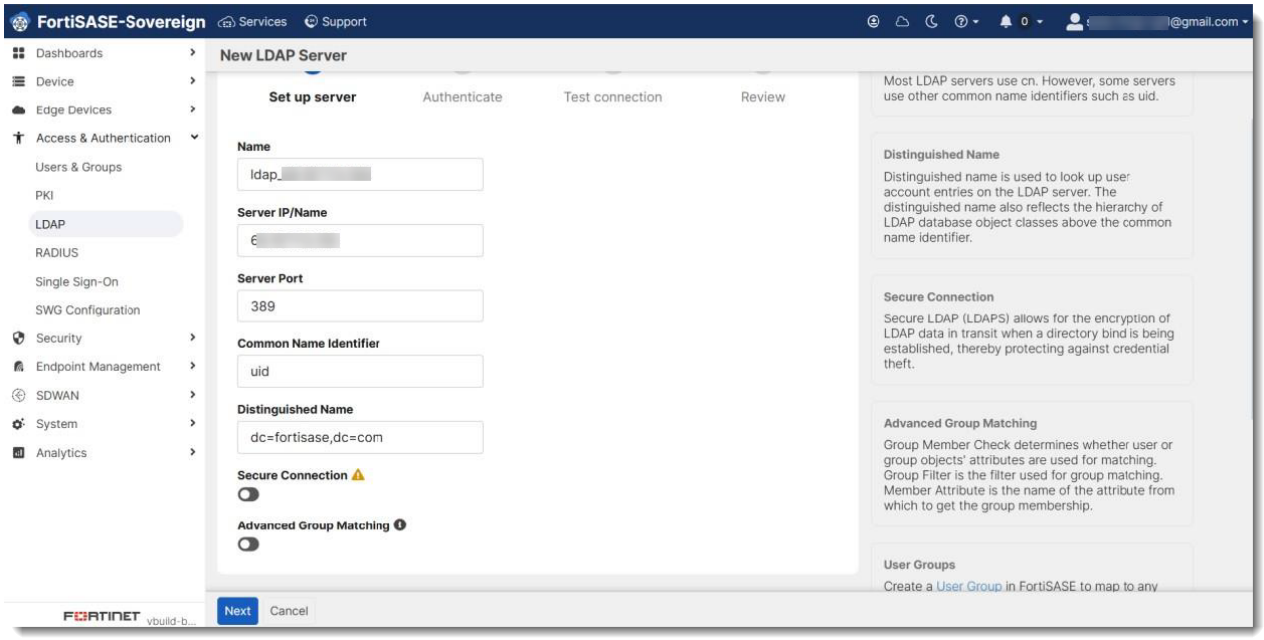
Configuring the LDAP feature involves the following:

1. Set up LDAP server on page 44
2. Add LDAP users on page 46

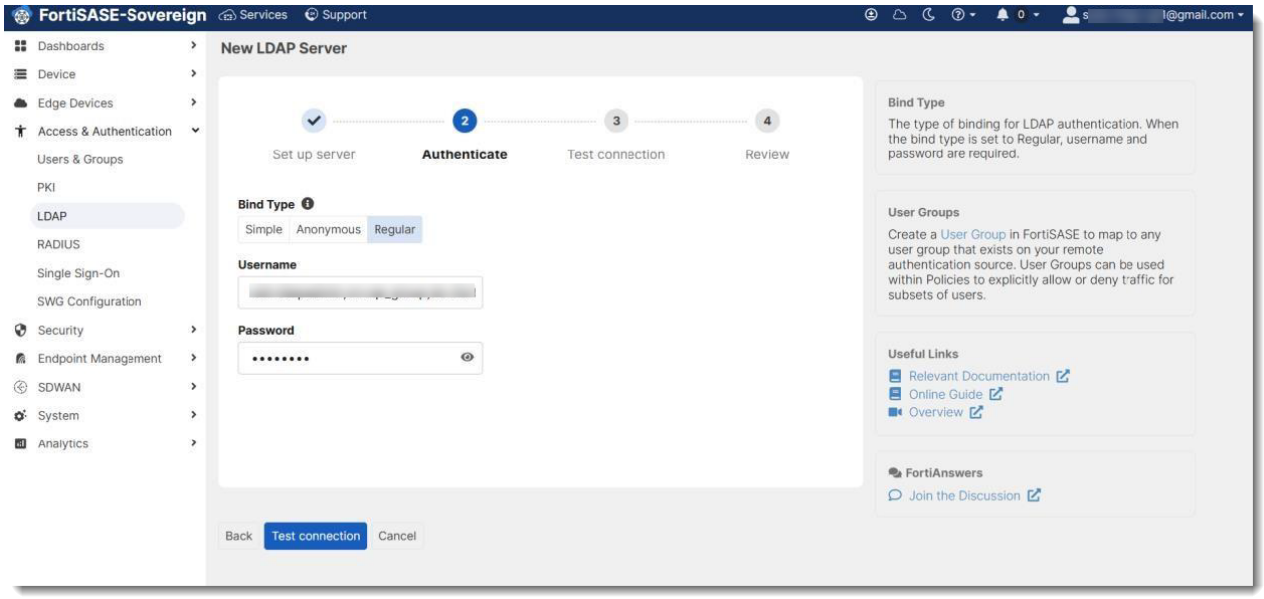
Set up LDAP server

1. Select *Access & Authentication>LDAP*, and click *Create*.

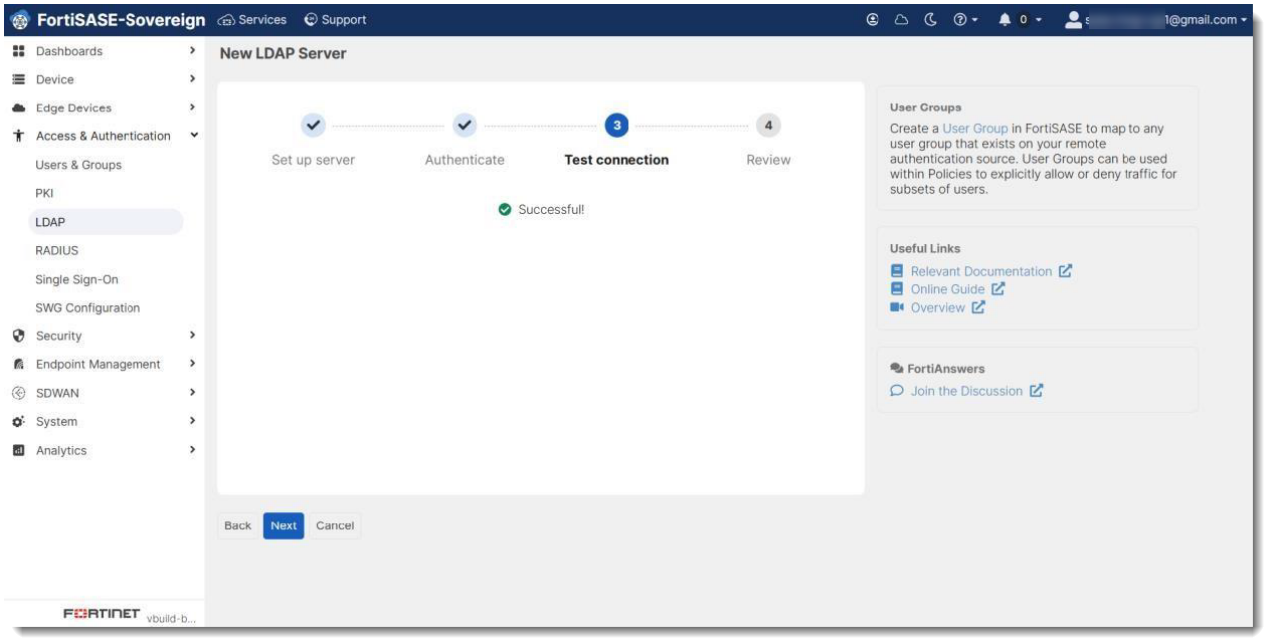
2. Enter the LDAP server details, and click *Next*.



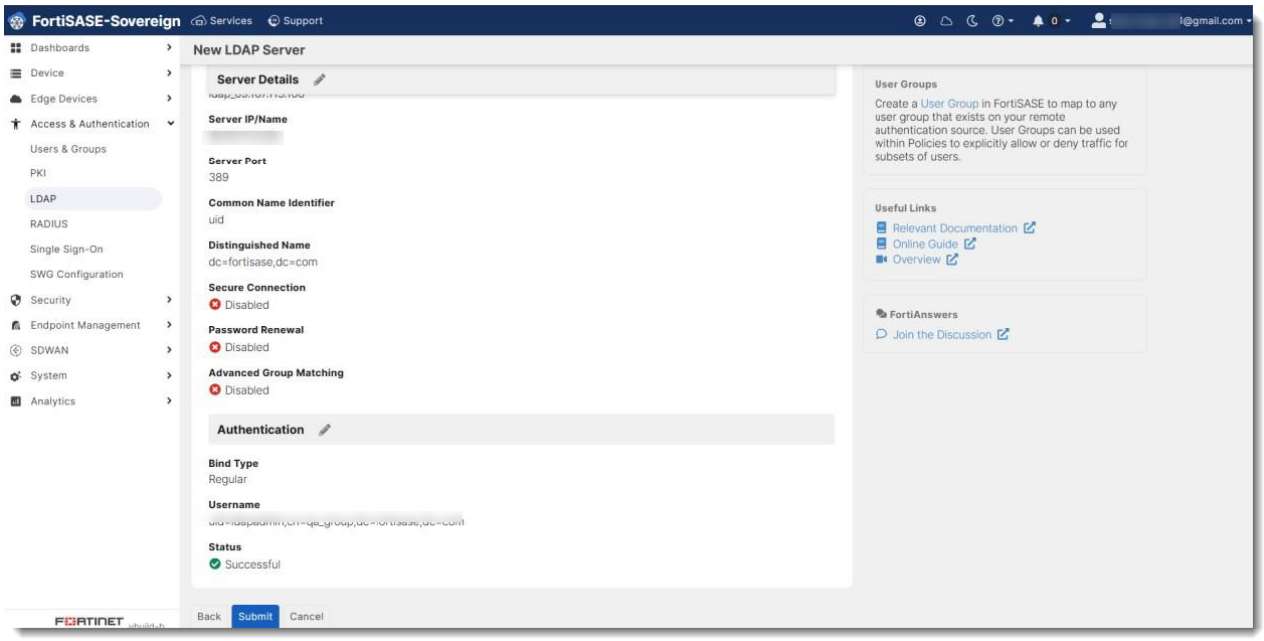
3. Select a *Bind Type*, enter the *Username* and *Password*, and click *Test Connection*.



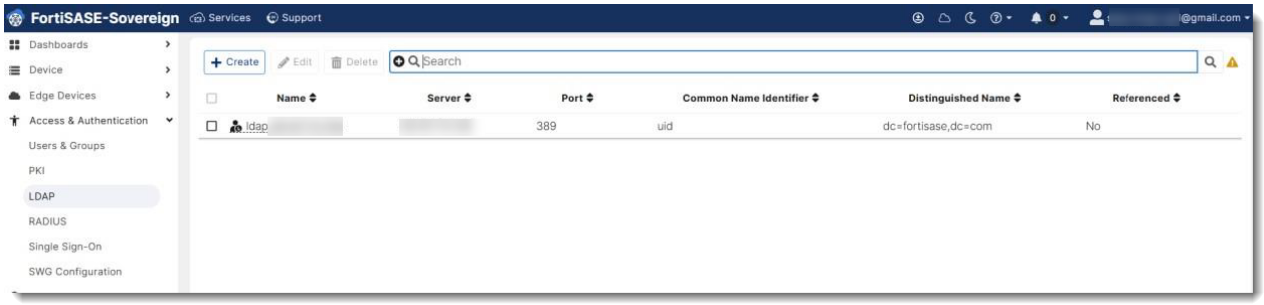
4. When Test Connection is successful, click *Next*.



5. Review the LDAP server settings, and click *Submit*.

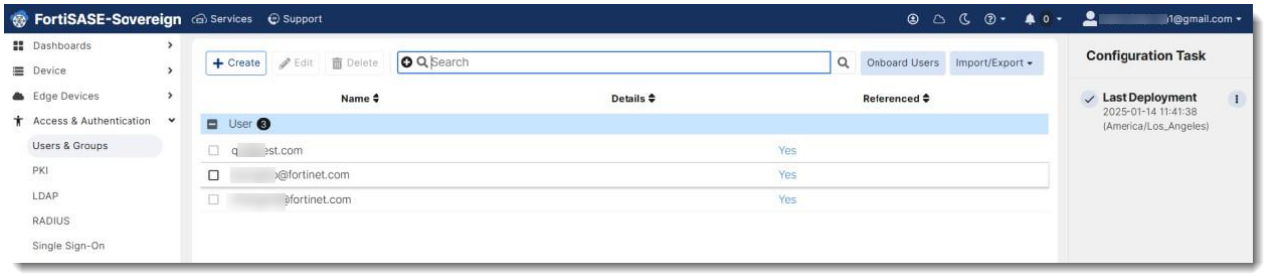


The newly created LDAP server appears on the *Access & Authentication>LDAP* page.

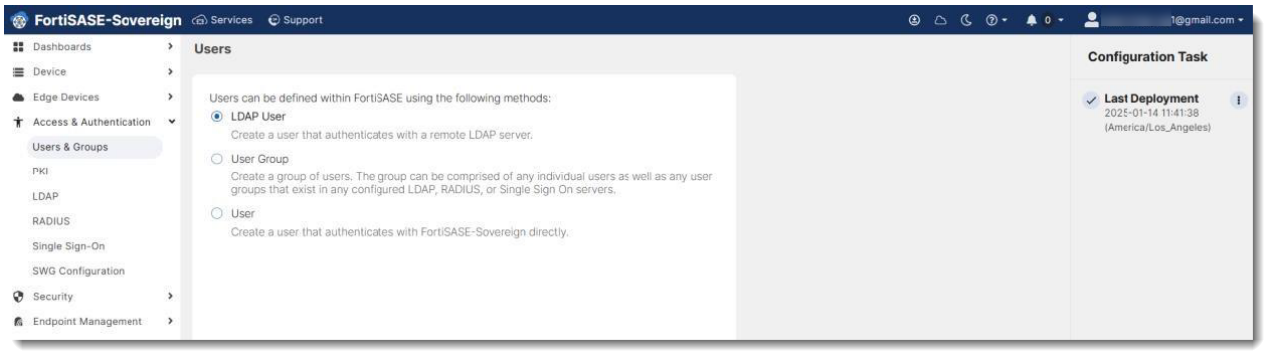


Add LDAP users

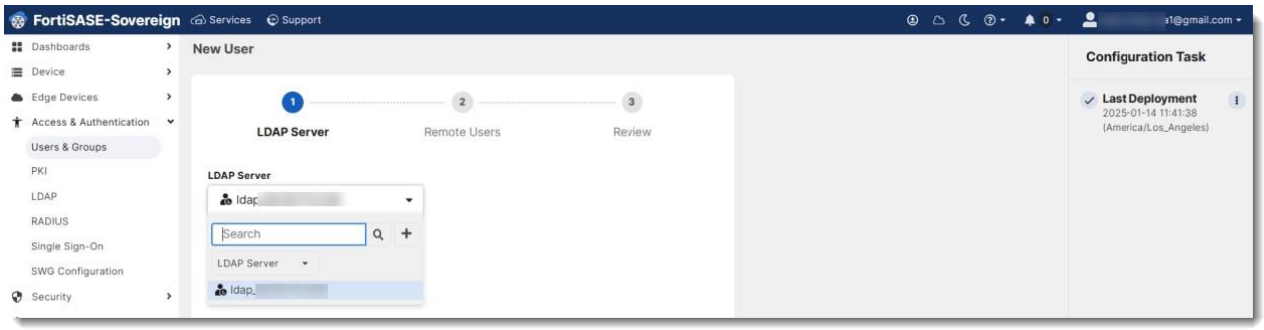
1. Select *Access & Authentication>User & Groups*.



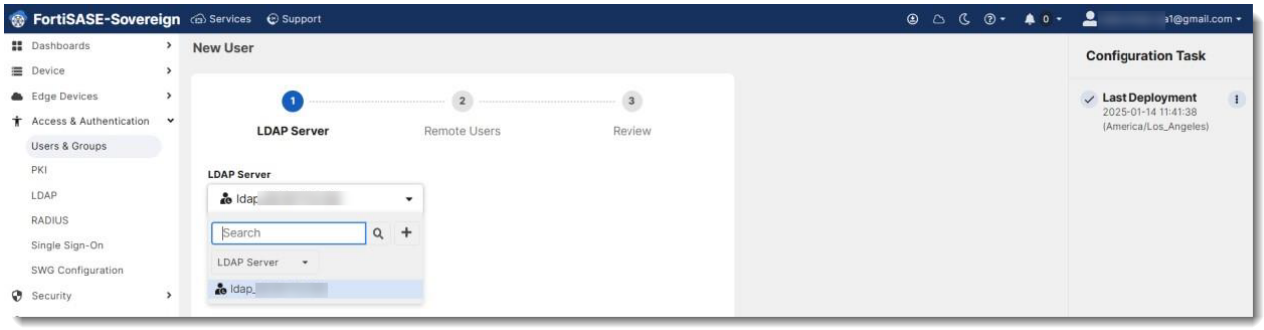
2. Click *Create*, select *LDAP User*, and click *Next*.



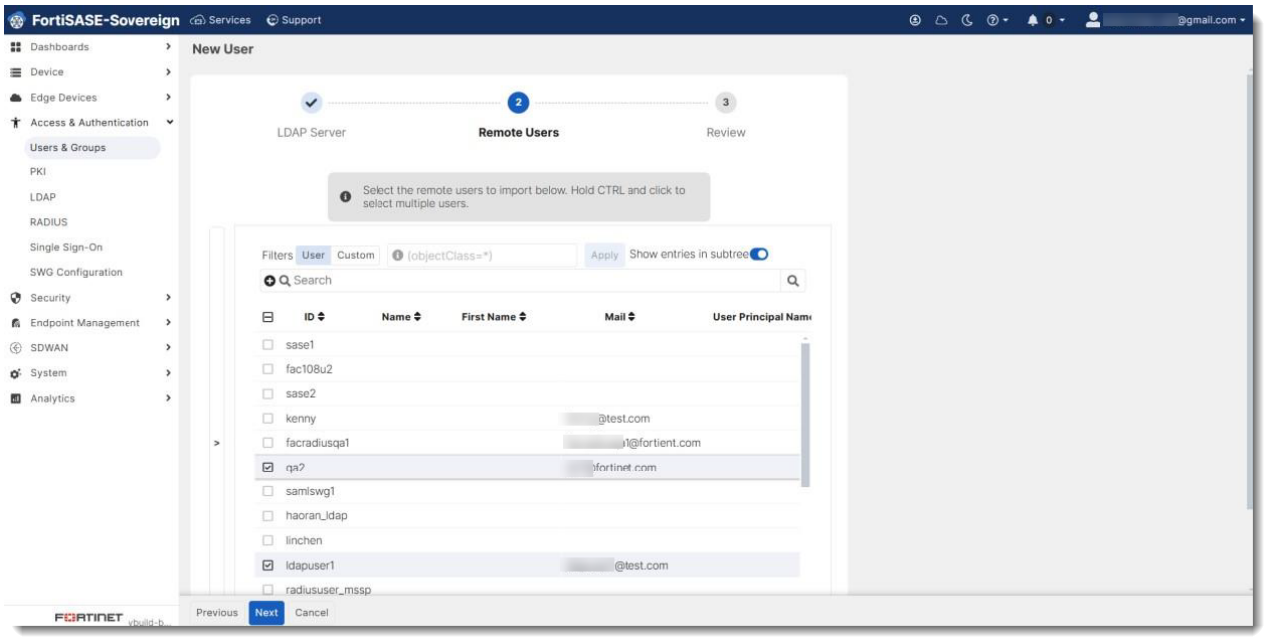
3. Select the LDAP Server from the dropdown list, and click *Next*.



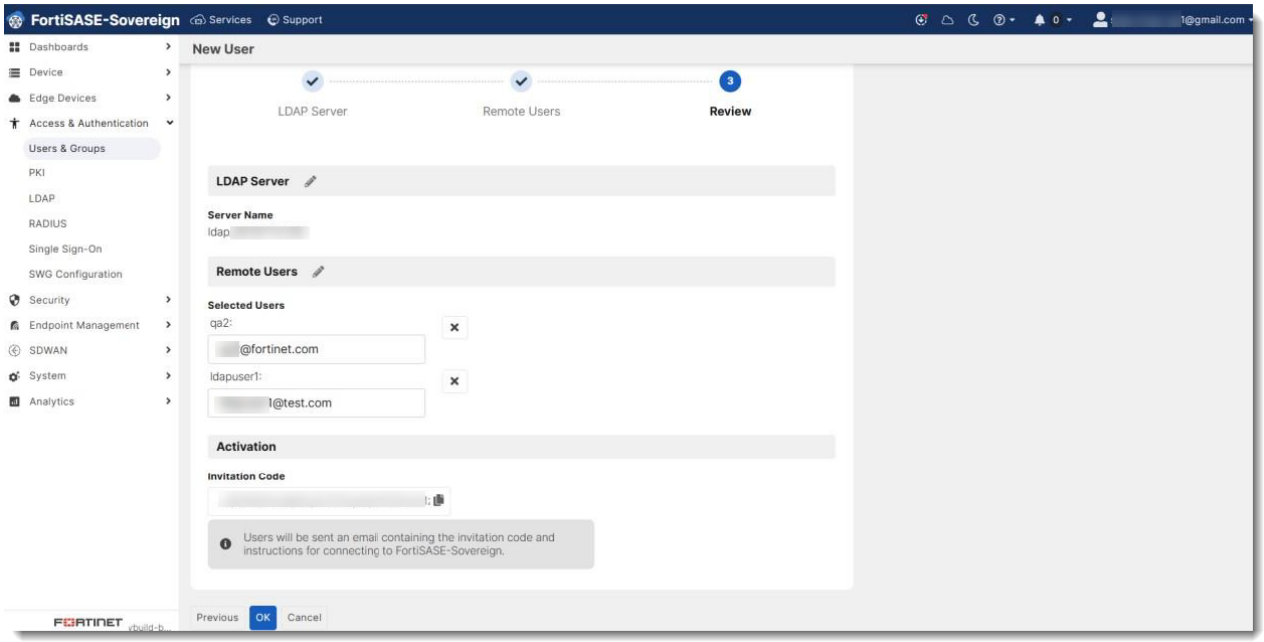
4. Select the *Remote Users*.



5. Click *Next*.



6. Review the *LDAP Server* and *Remote User* settings, and click *OK*.



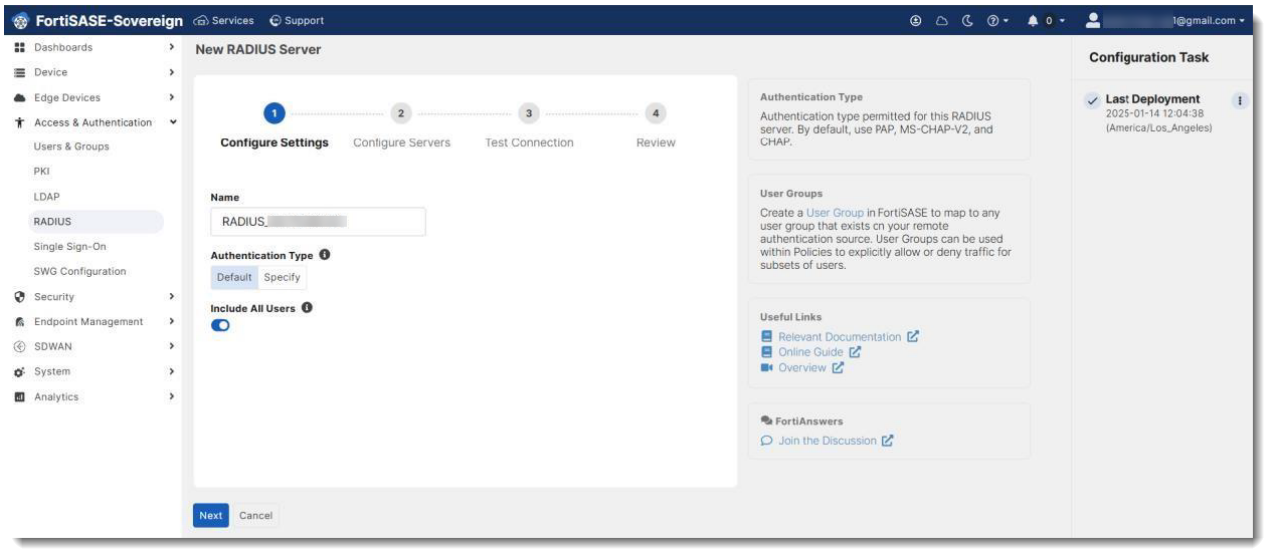
7. Click *Install Config*, and follow the prompts onscreen to complete the installation of the LDAP server and remote LDAP users.

   The LDAP server and the remote LDAP users now show up the Portal.

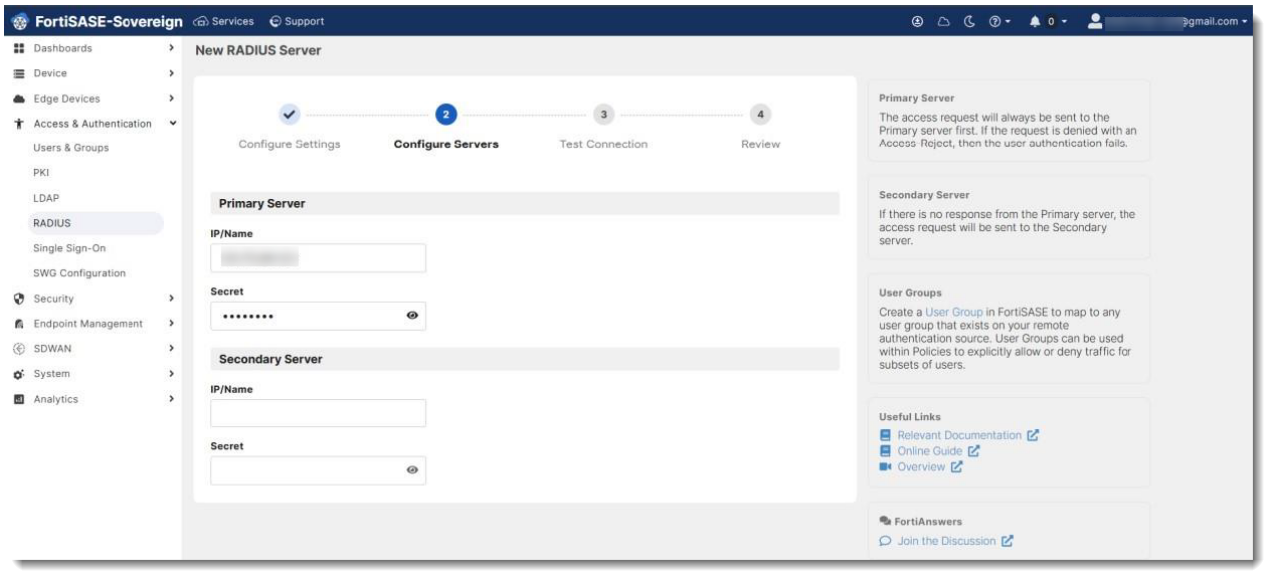
Configure RADIUS server

1. Select *Access & Authentication>RADIUS*.

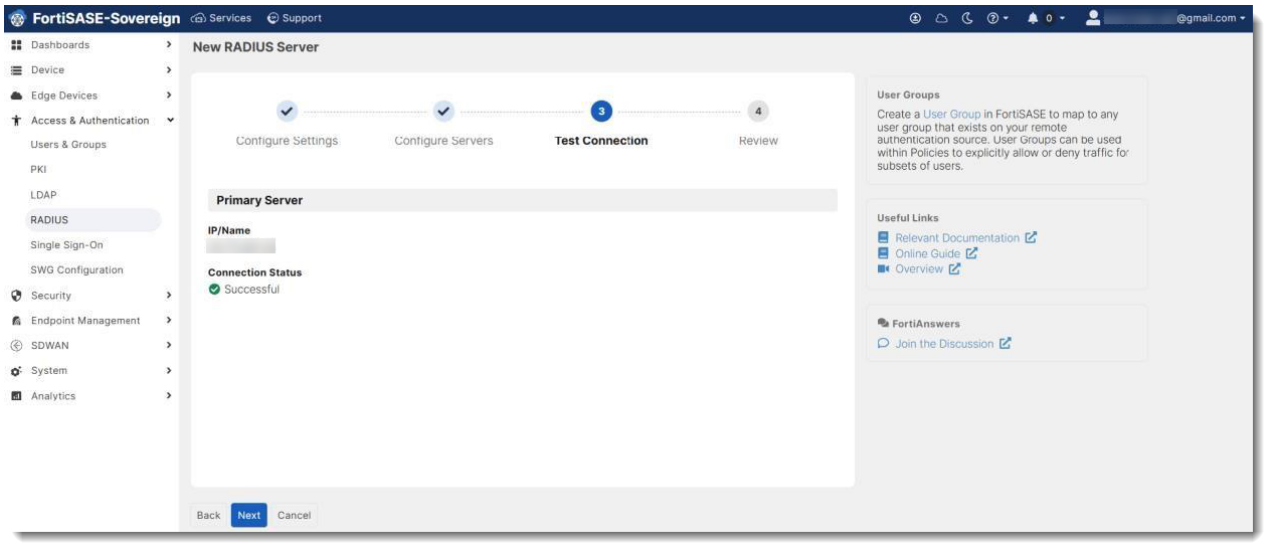
2. Click *Create*.



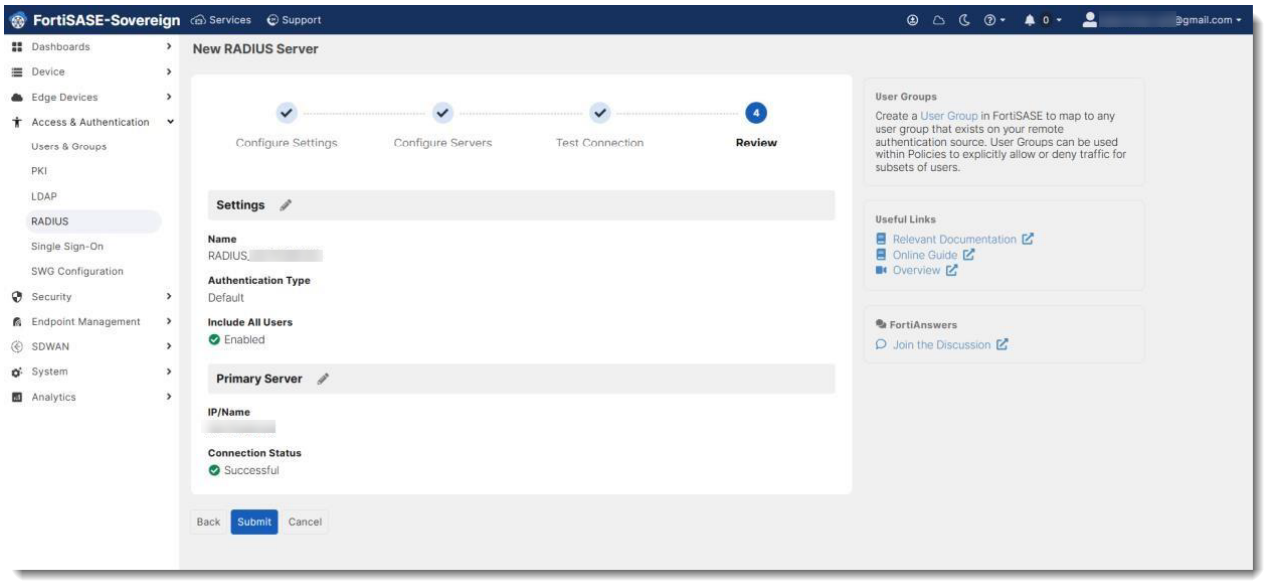
3. Fill in the RADIUS server *Name*, set *Authentication Type* to *Default*, enable *Include All Users*, and click *Next*.



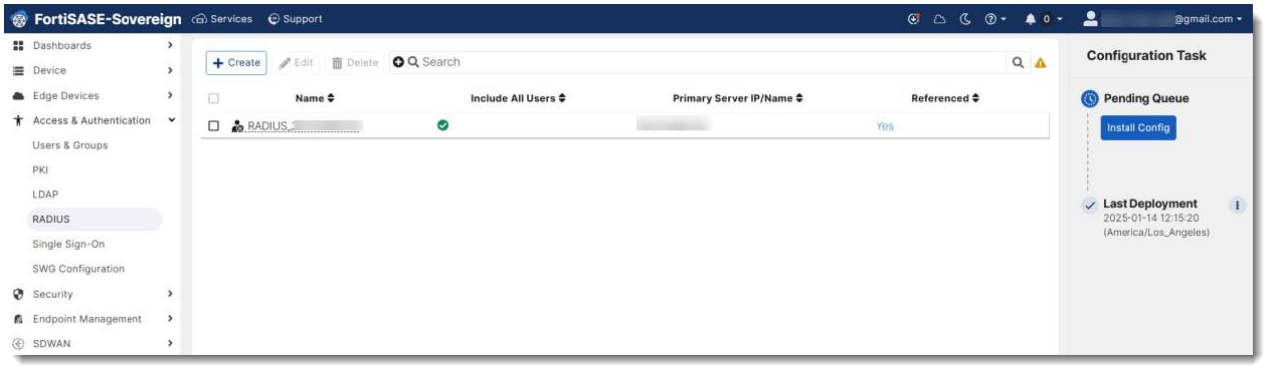
4. Enter the *Primary RADIUS Server IP* and *Secret*, and click *Next*.



5. When the *Test Connection* page shows successful connection, click *Next*.



6. Click *Submit*.
   The RADIUS server shows up on the *Access & Authentication > RADIUS* page.

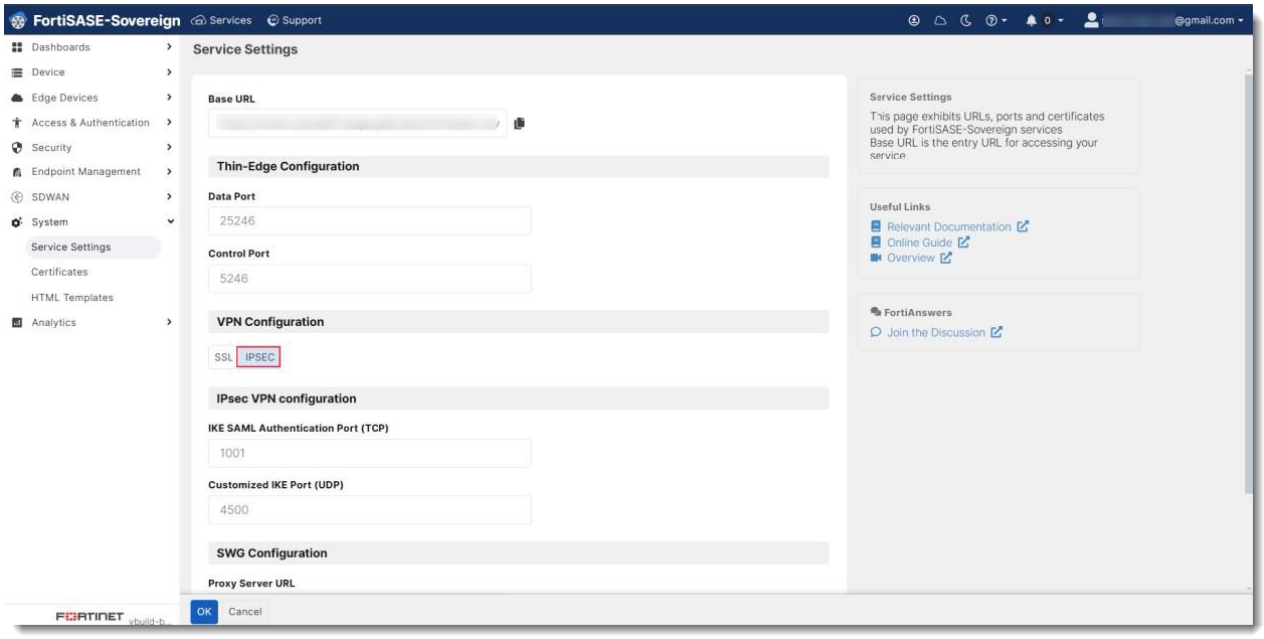


7. Click *Install Config, and follow the prompts onscreen to complete installing the RADIUS server configuration.*

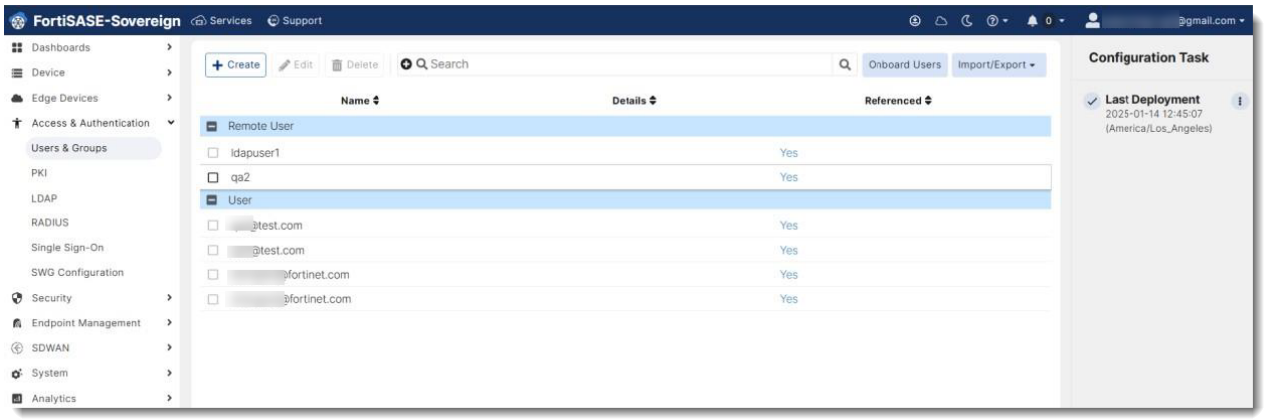
Configure IPsec VPN login

Both local and RADIUS users are able to use IPsec VPN login. The following steps illustrate how a local-user logs in using IPsec VPN.

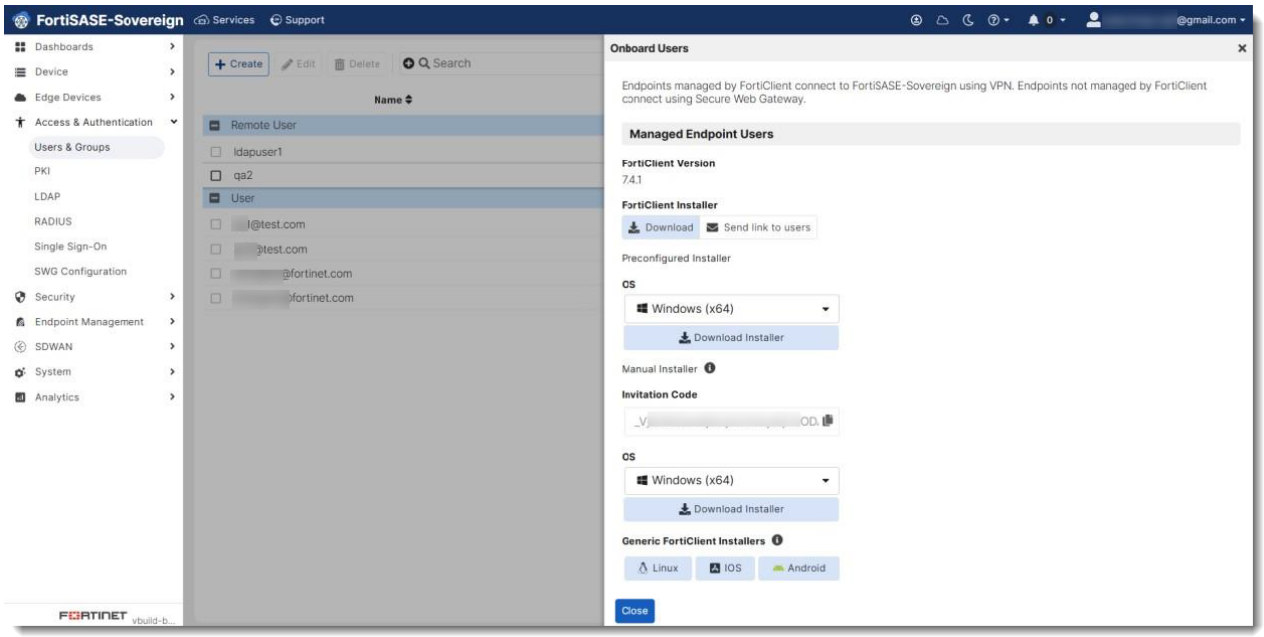
1. Select *System>Service Settings*, and check *VPN Configuration* to make sure it is *IPSEC*.



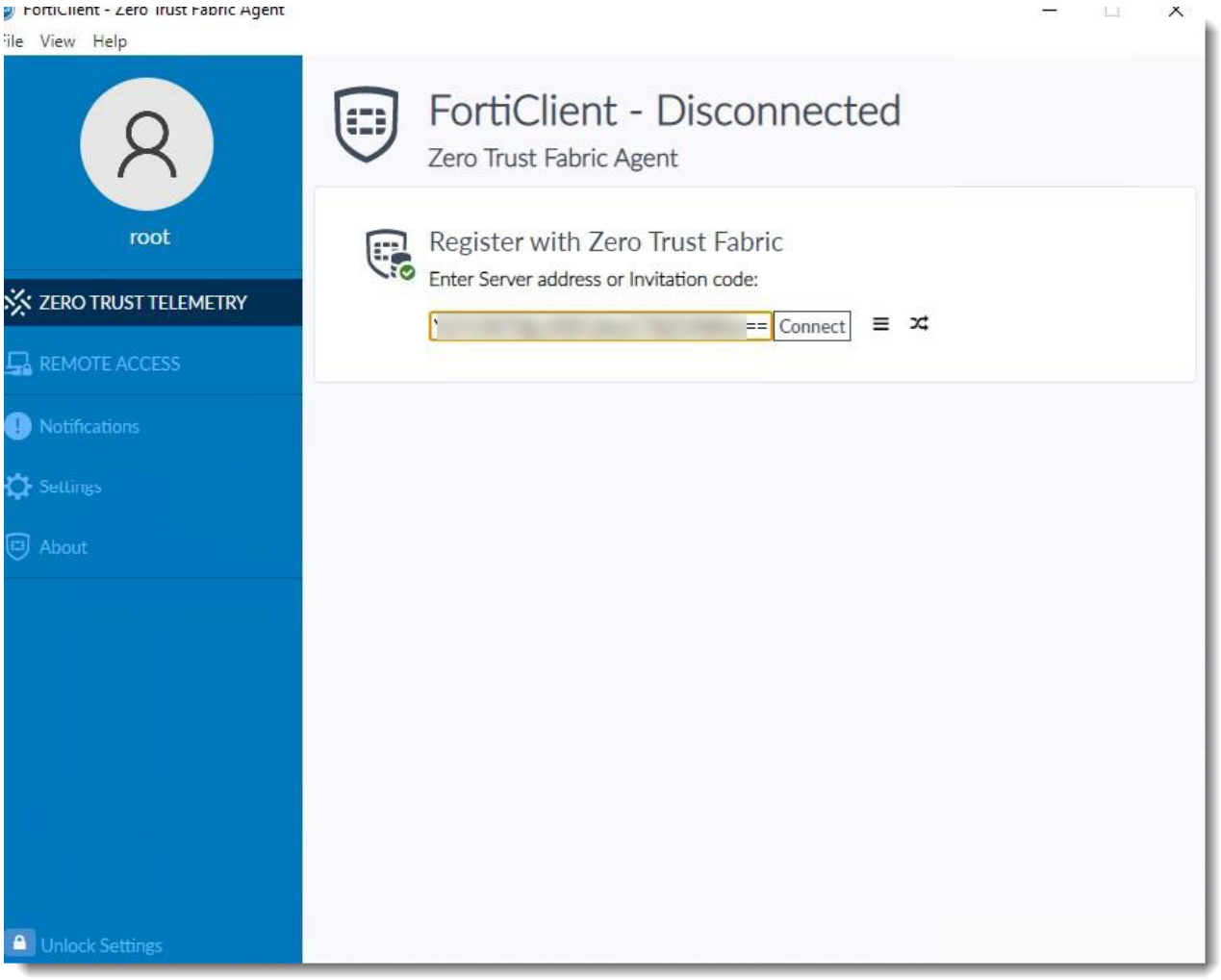
2. Select *Access & Authentication>Users & Groups*.



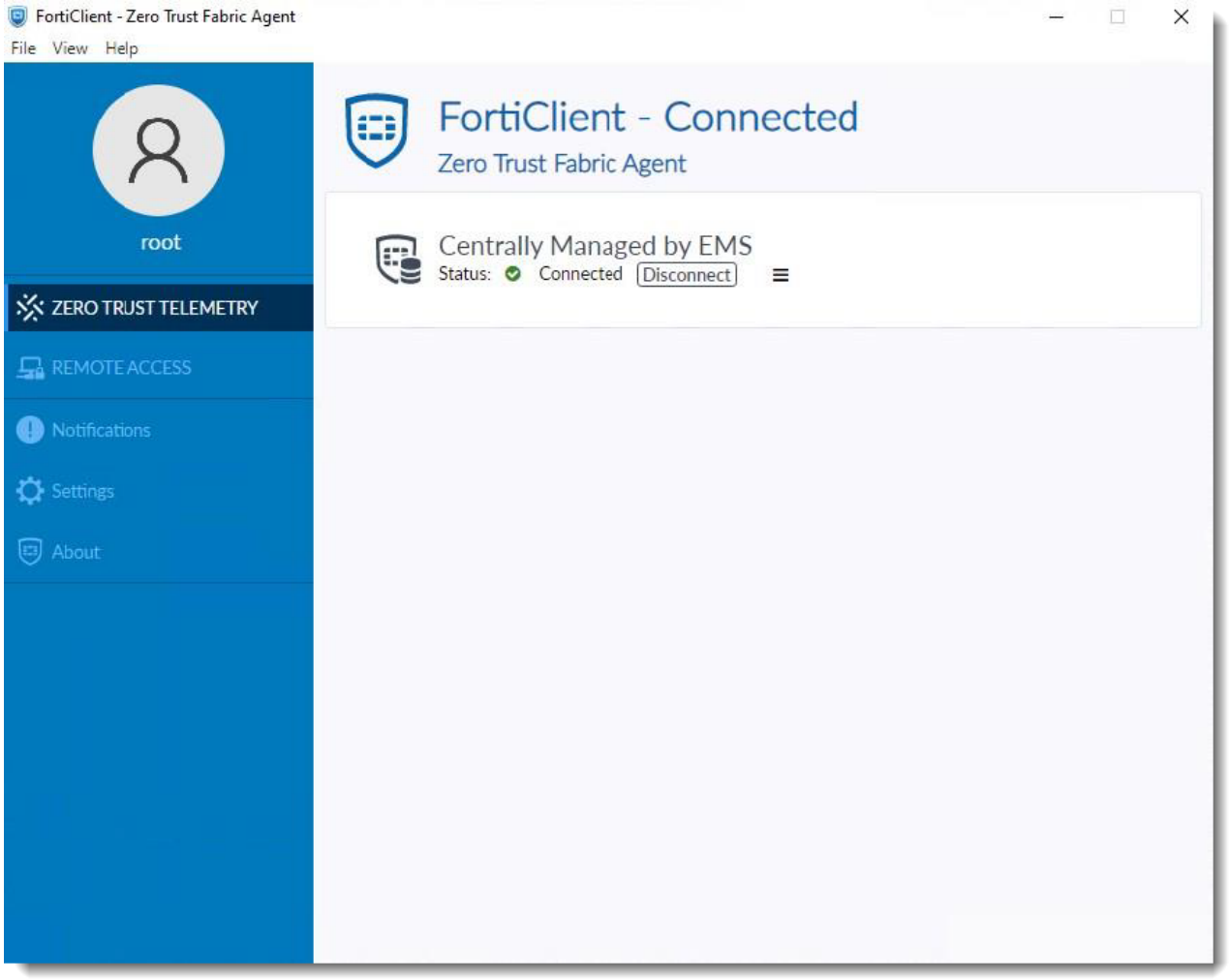
3. Under *User*, select the existing local user which you use to log in and click *Onboard Users*.



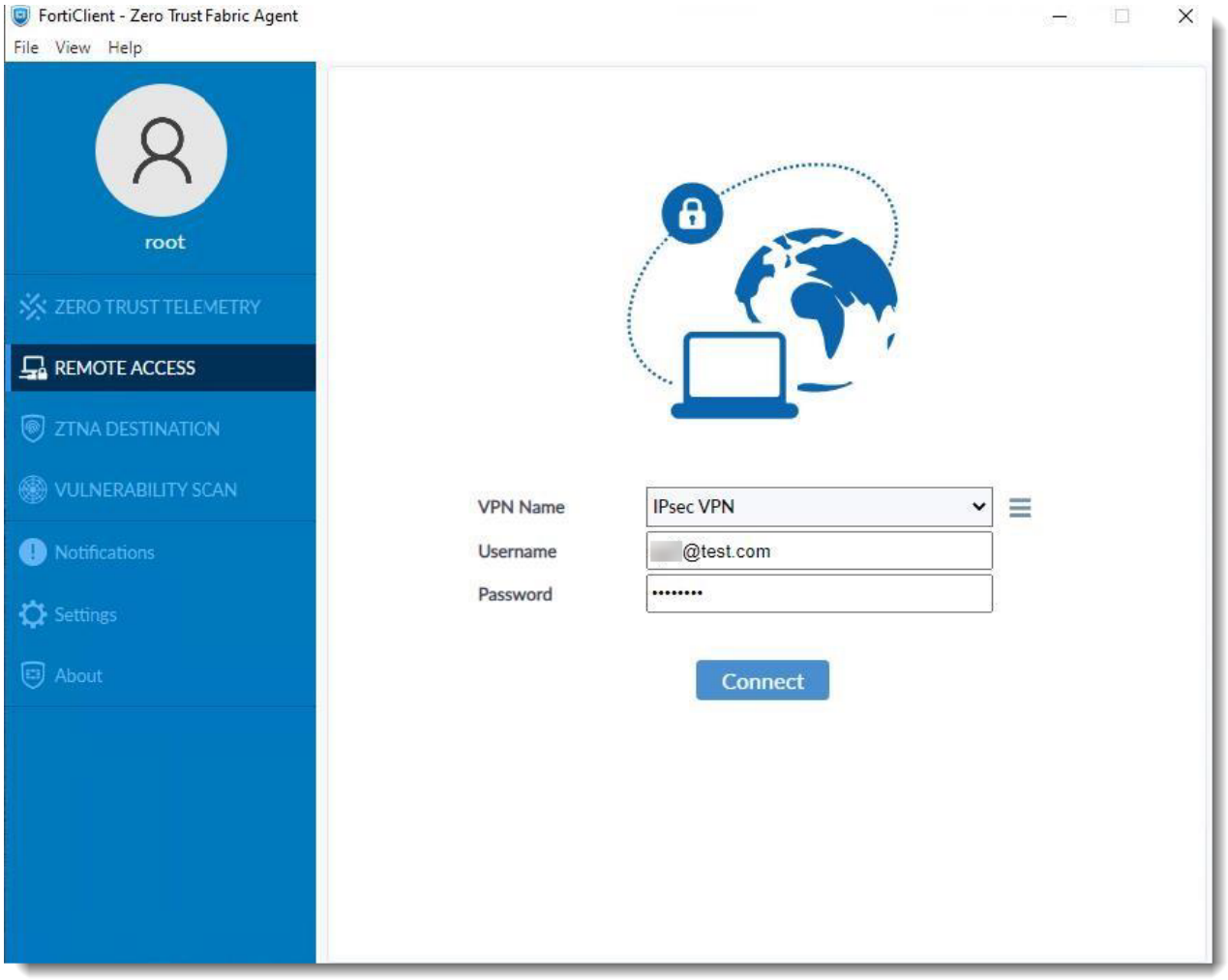
4. In the *Onboard Users* panel, copy the *Invitation Code*.
5. On a client (Windows or Linux) PC, start the FortiClient, paste in the *Invitation Code*, and click *Connect*.



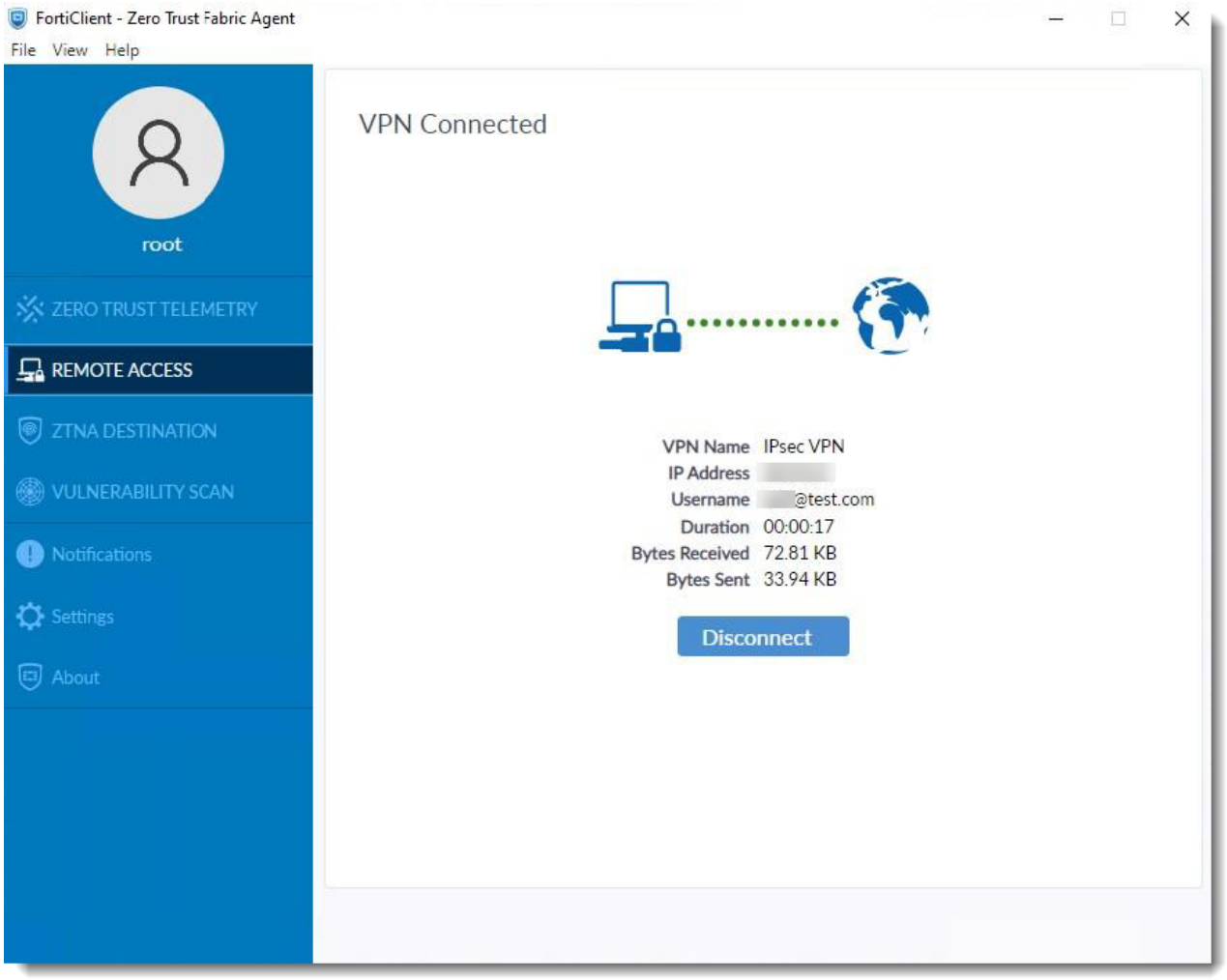
You are now connected on FortiClient EMS, as shown in the following screenshot.



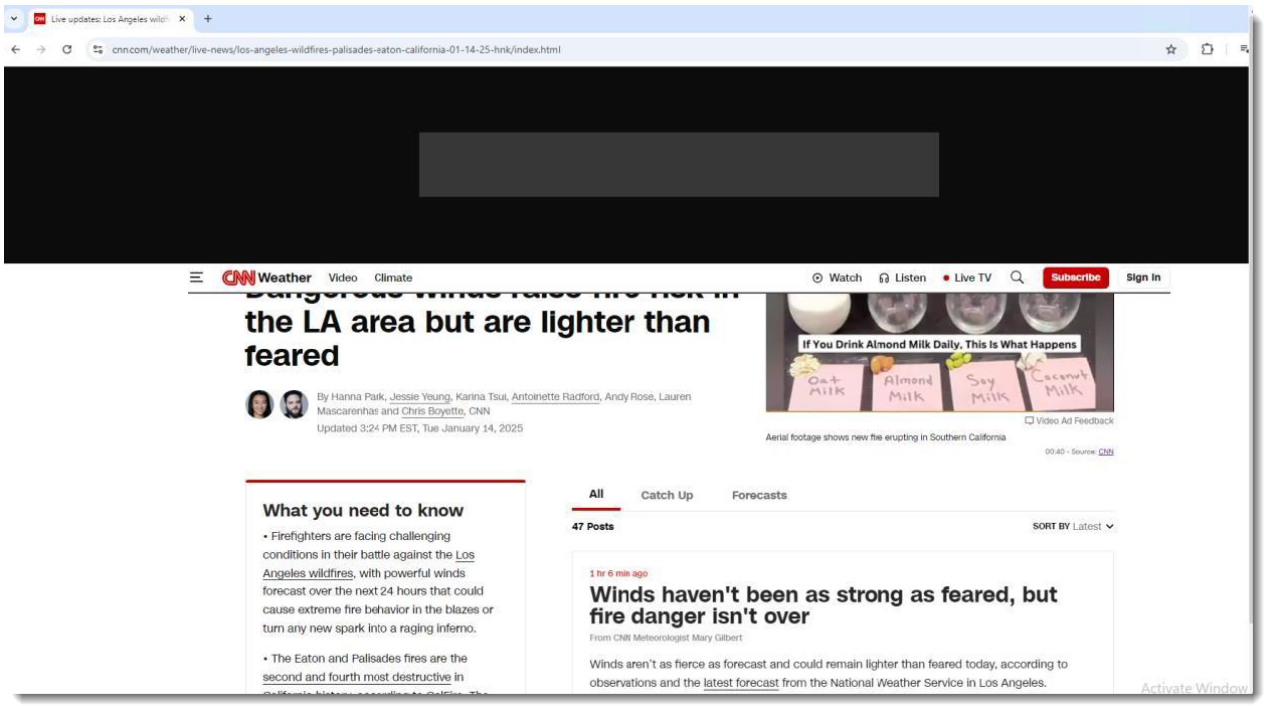
6. Click *REMOTE ACCESS*.



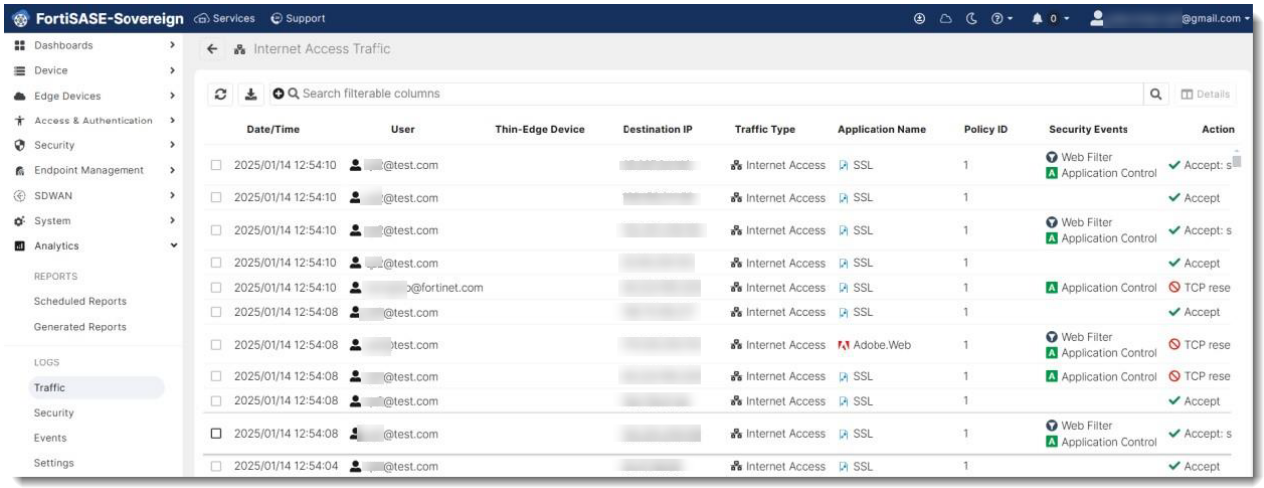
7. Fill in the Username and Password, and click *Connect*.
   You are now connected to IPsec VPN.



8. Verify the VPN connection by opening a website.

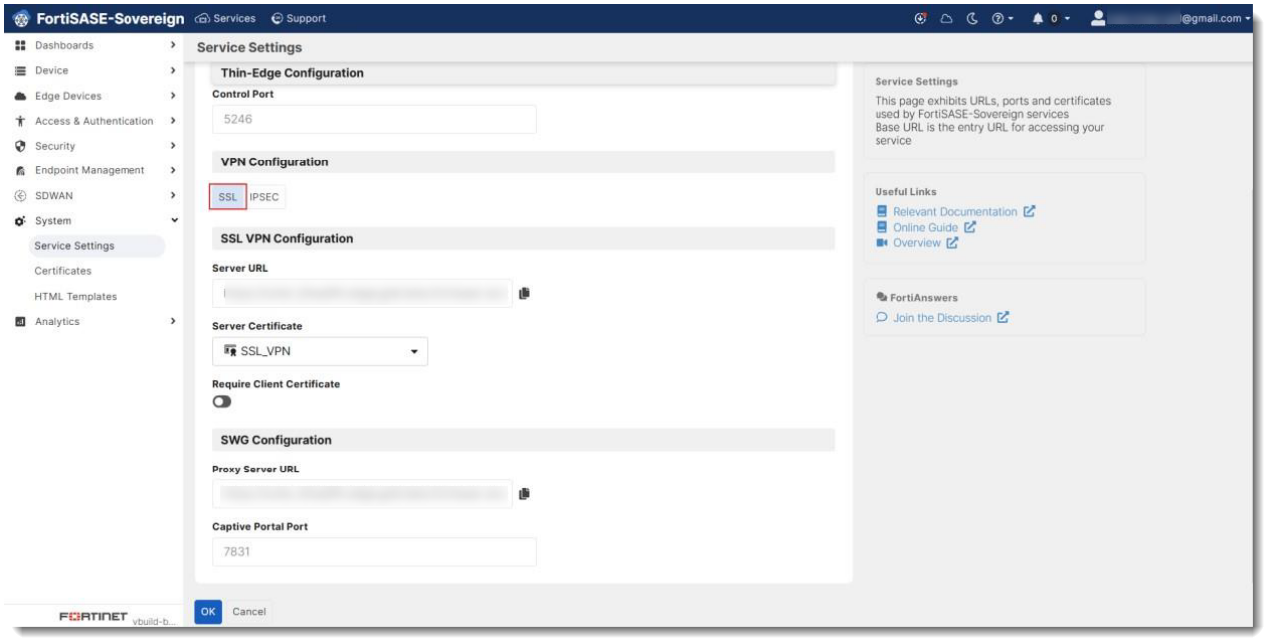


9. On the FortiSASE-Sovereign portal, select *Analytics >Traffic,* and click the *Internet Access Traffic* to view the traffic log.

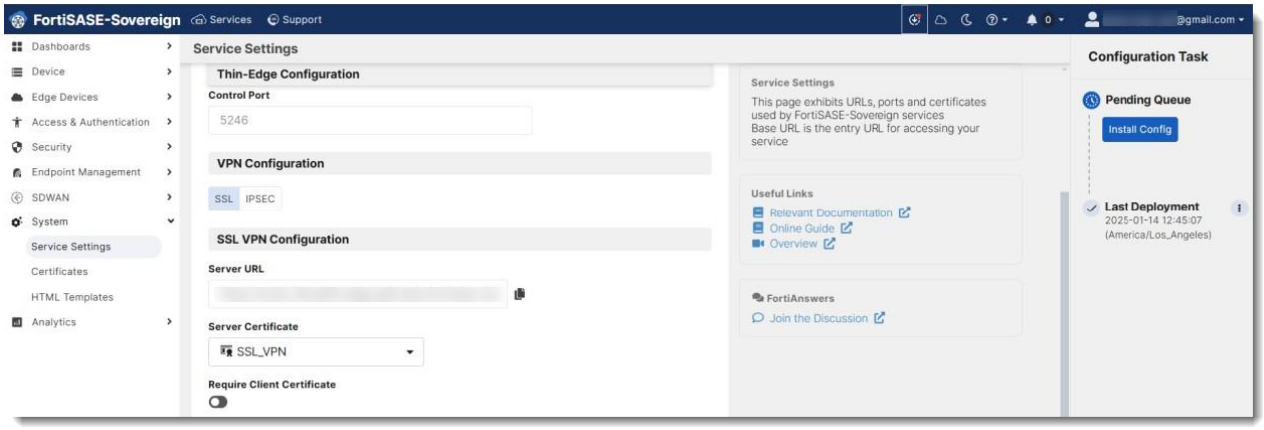


Configure SSL VPN

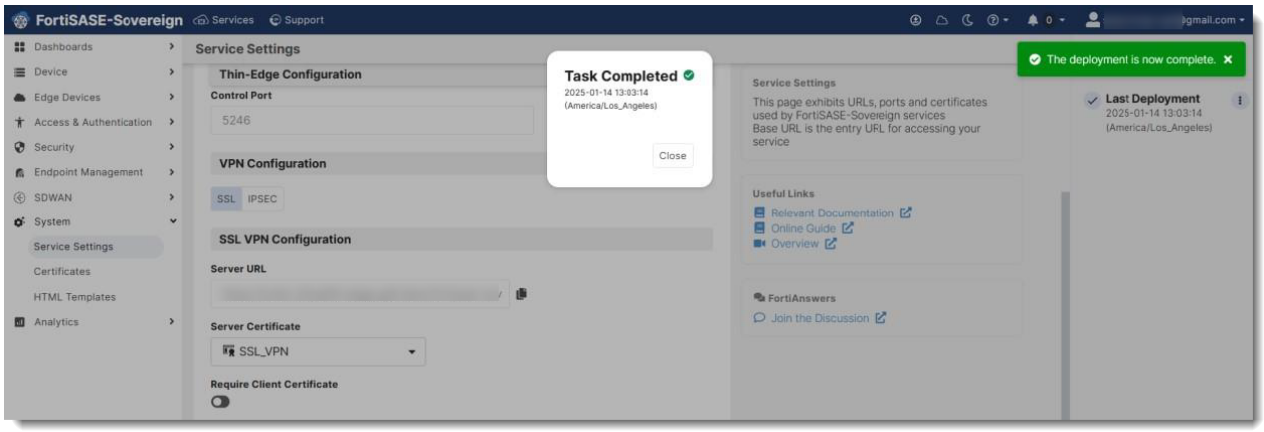
1. Go to *System>Service Settings*.



2. Review the *VPN Configuration*, make sure that it is *SSL*, and click *OK*.

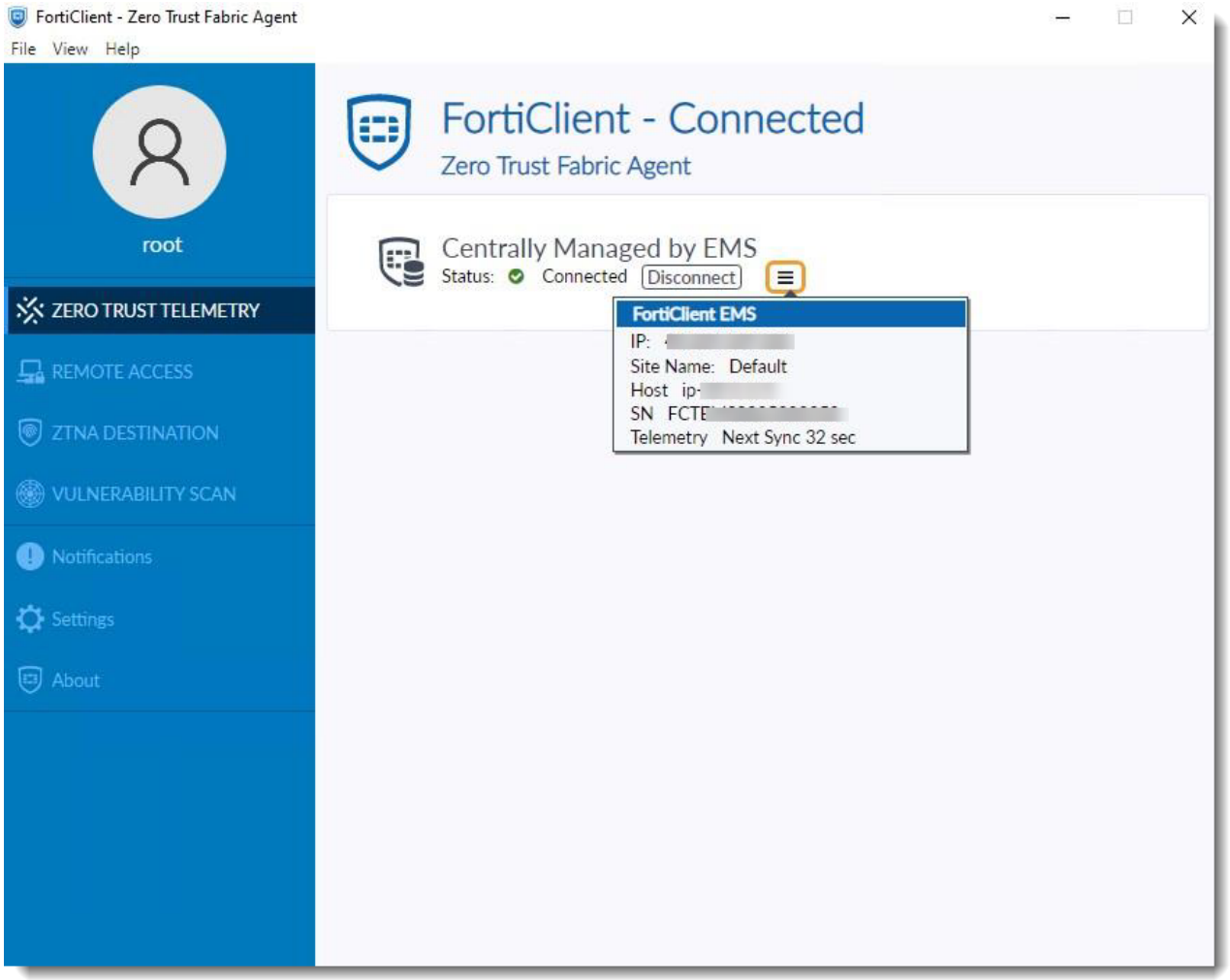


3. Click *Install Config*, and follow the prompts to deploy the SSL VPN configuration.



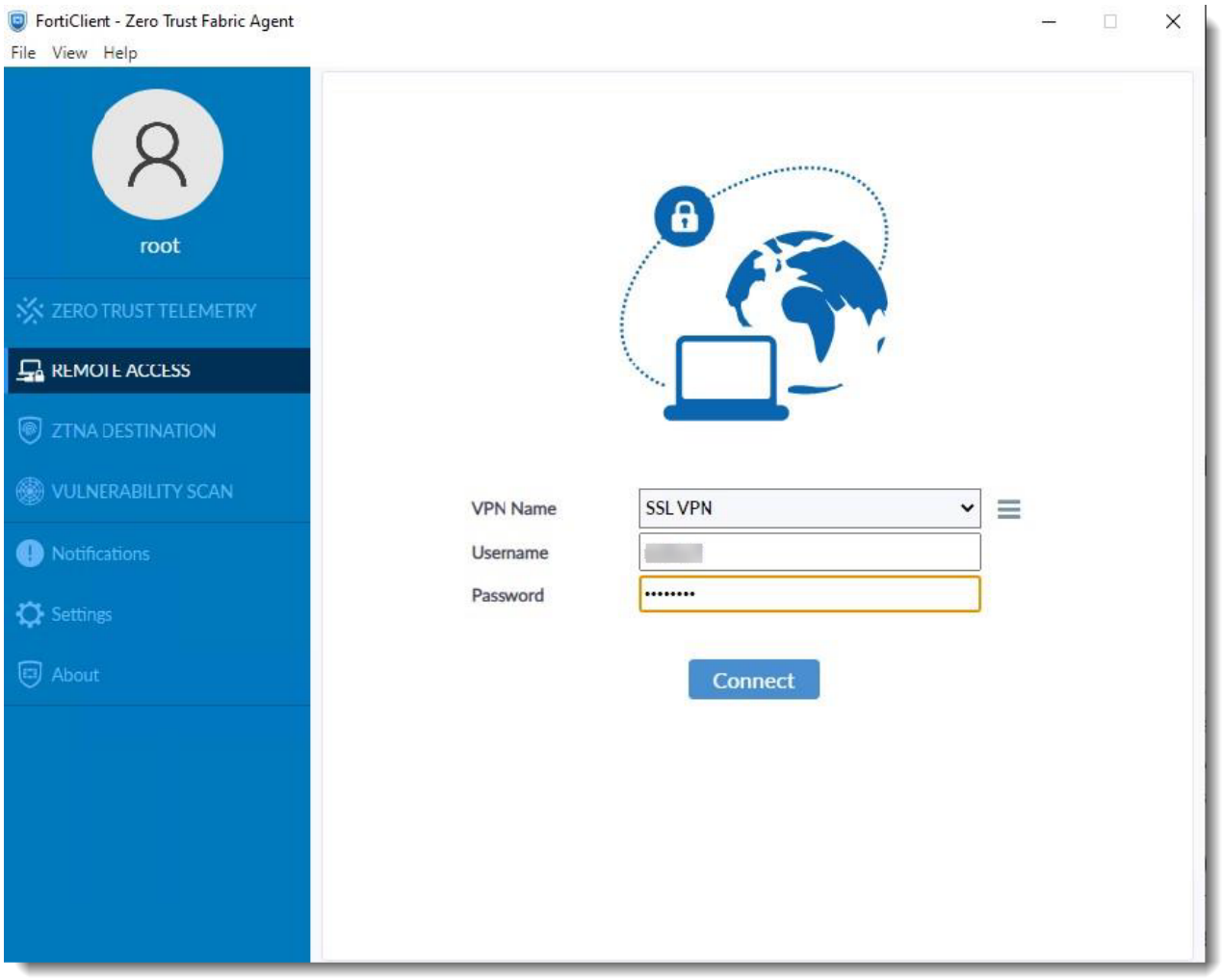
4. Launch FortiClient on a client PC, and make sure that you are connected.

Once deployed, it may take approximately 60 seconds to synchronize the SSL VPN configuration to FortiClient.



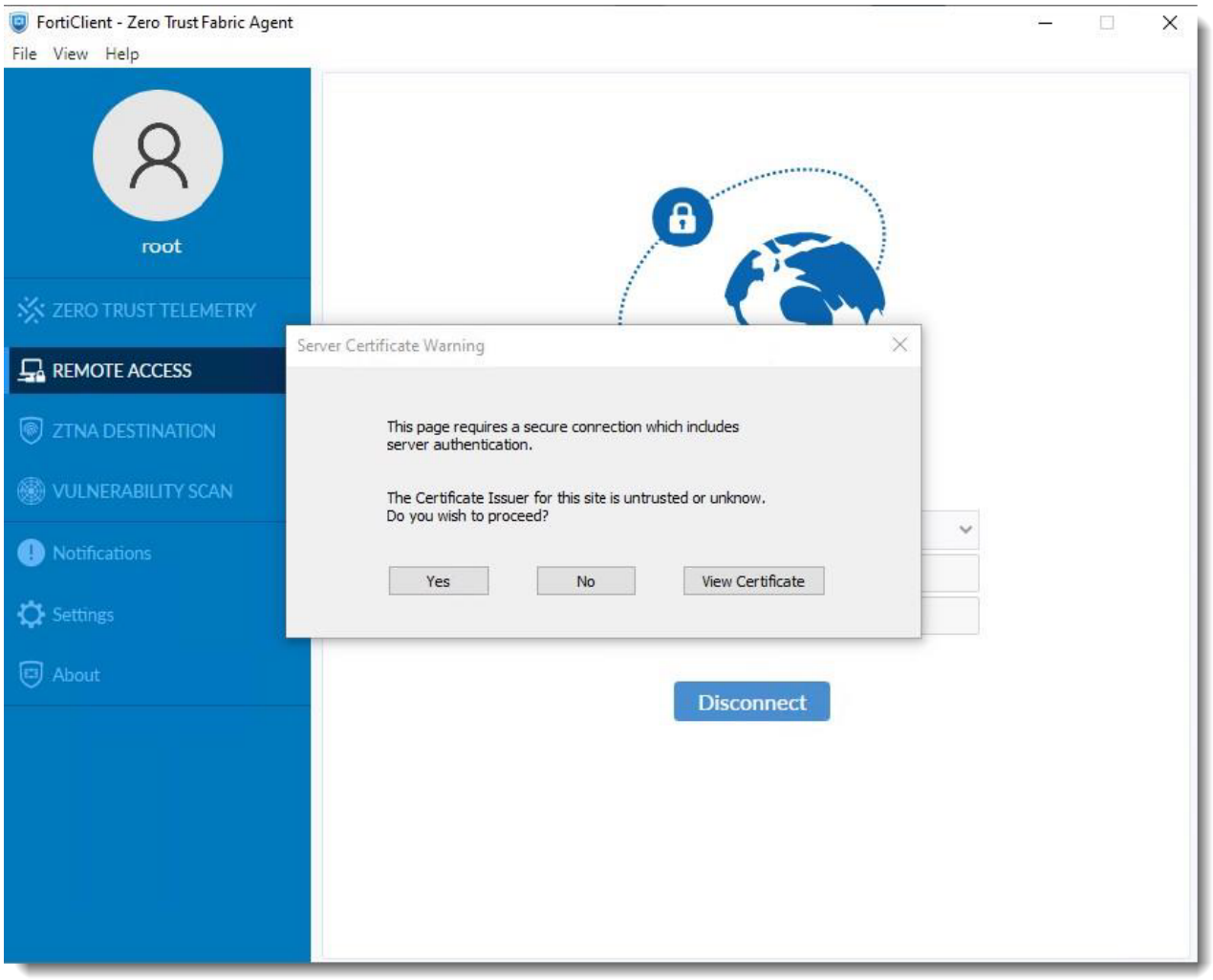
SSL VPN RADIUS user login

1. Start FortiClient, and click *REMOTE ACCESS*.

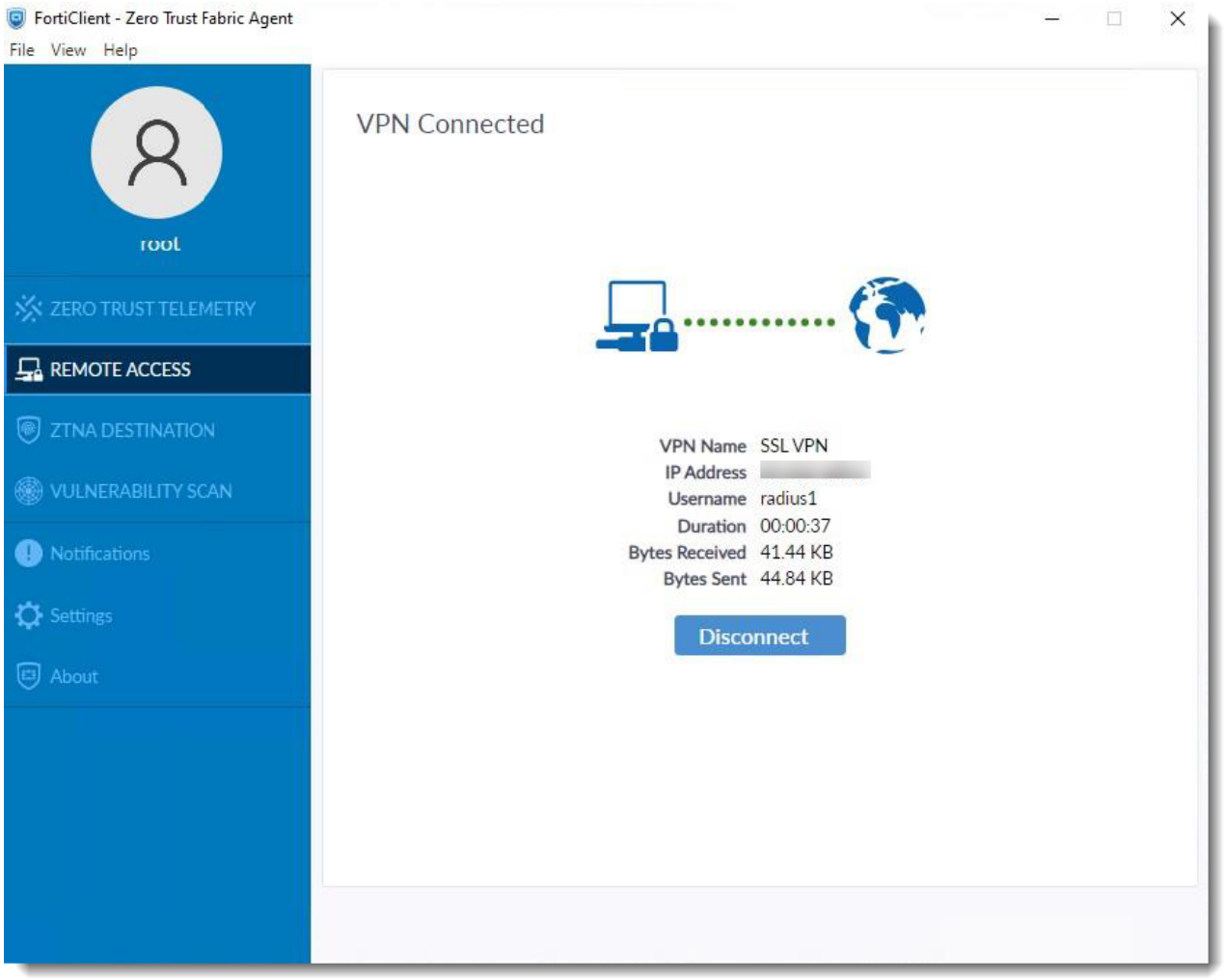


The VPN name now has changed to SSL VPN.

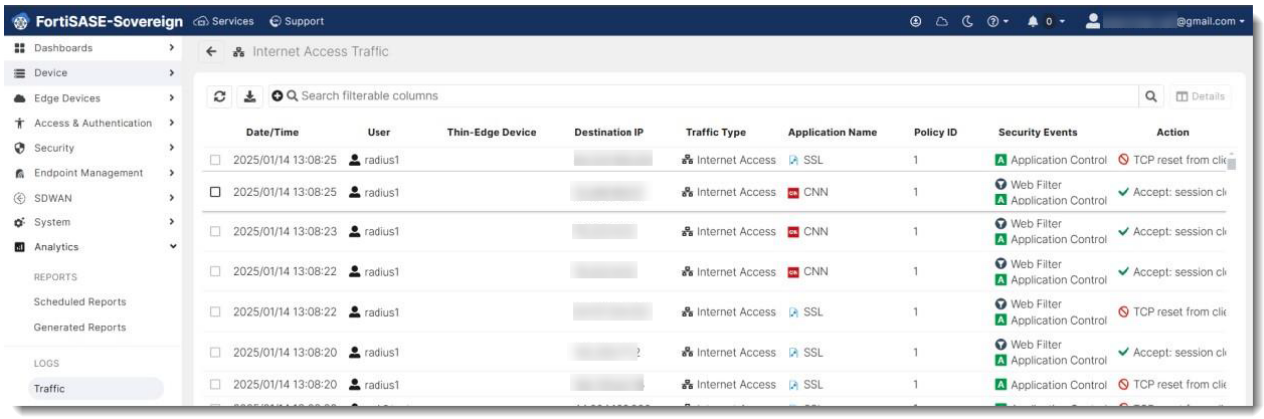
2. Enter your RADIUS username and password, and click *Connect*.



3. Click *Yes*. The SSL VPN connection is now established.

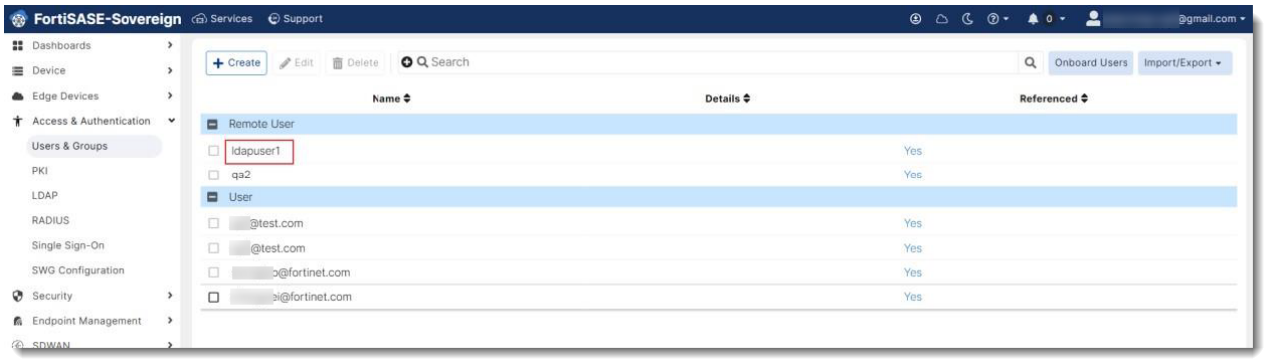


4. Start a Web browser, and open any website.
5. On the FortiSASE-Sovereign portal, select *Analytics>Traffic* to view the traffic logs.

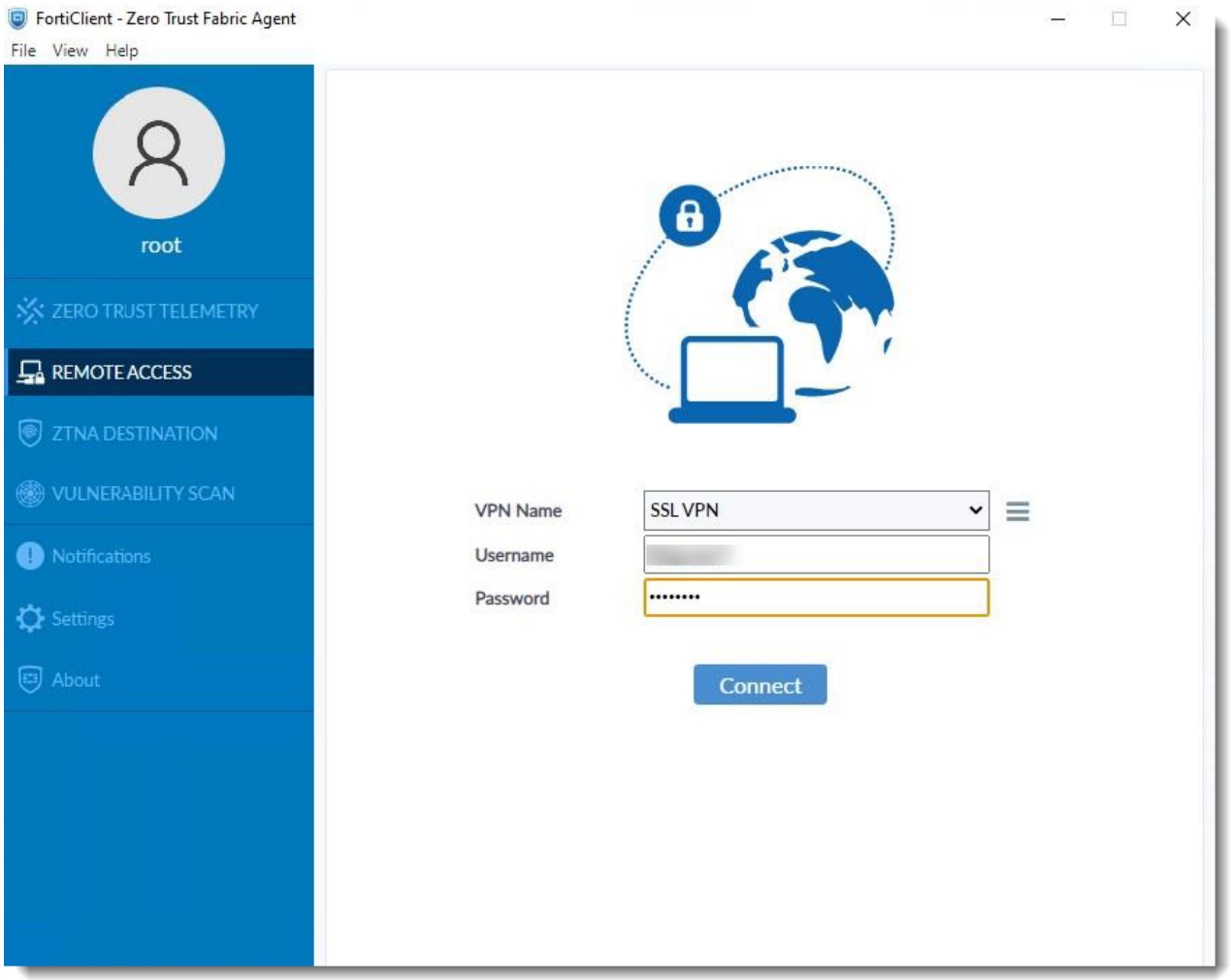


SSL VPN LDAP user login

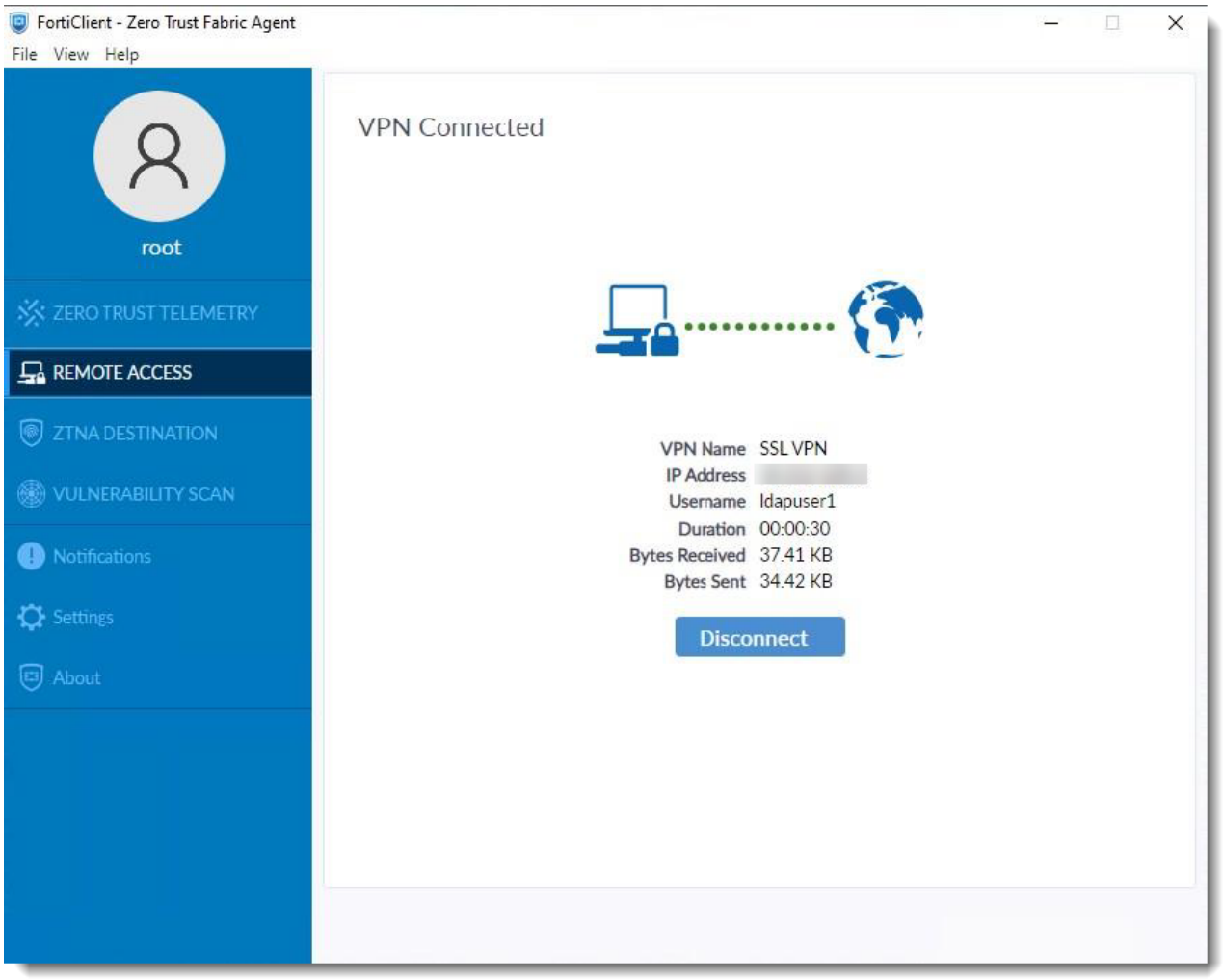
1. Select *Access & Authentication>Users & Groups*.



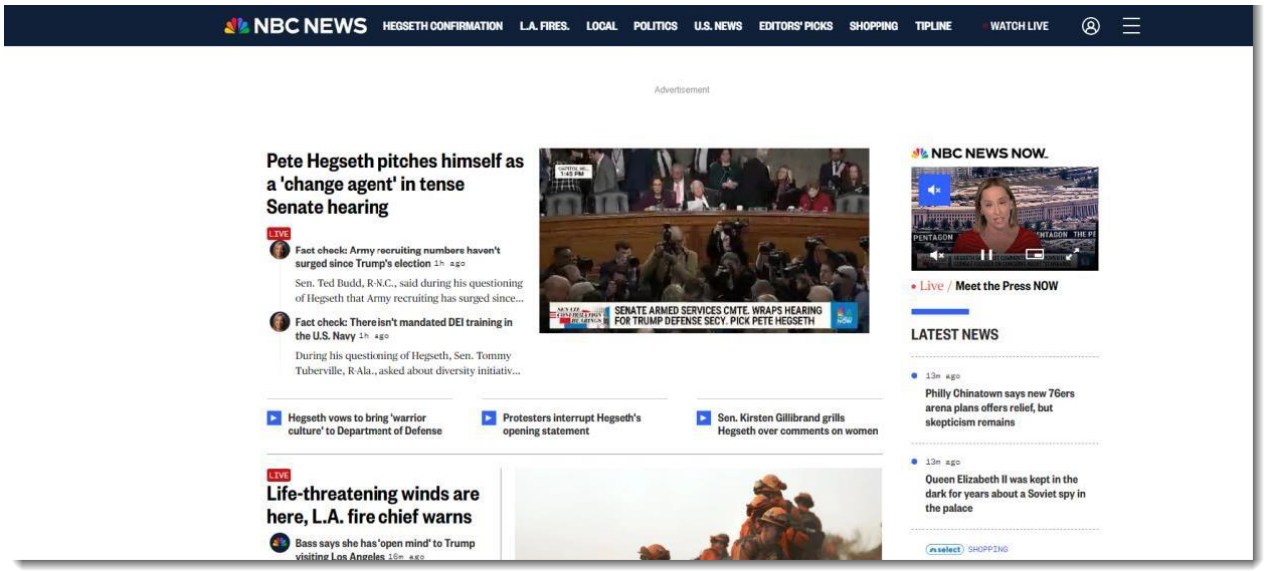
2. Select the desired LDAP user.
3. Start FortiClient, and select *REMOTE ACCESS*.



4. Enter the LDAP username and password, and click *Connect*.



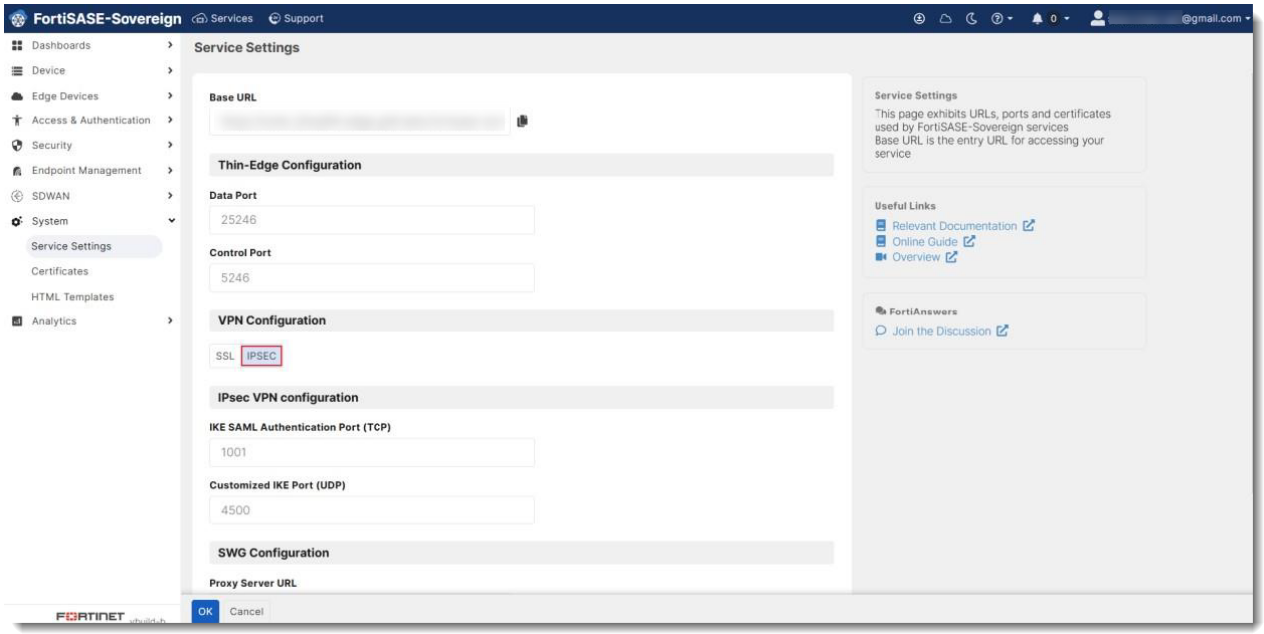
5. You are now logged in as an LDAP user through SSL VPN.
6. Start your web browser, and open a website of interest.



7. On the FortiSASE-Sovereign portal, select *Analytics>Traffic* to view the traffic logs.

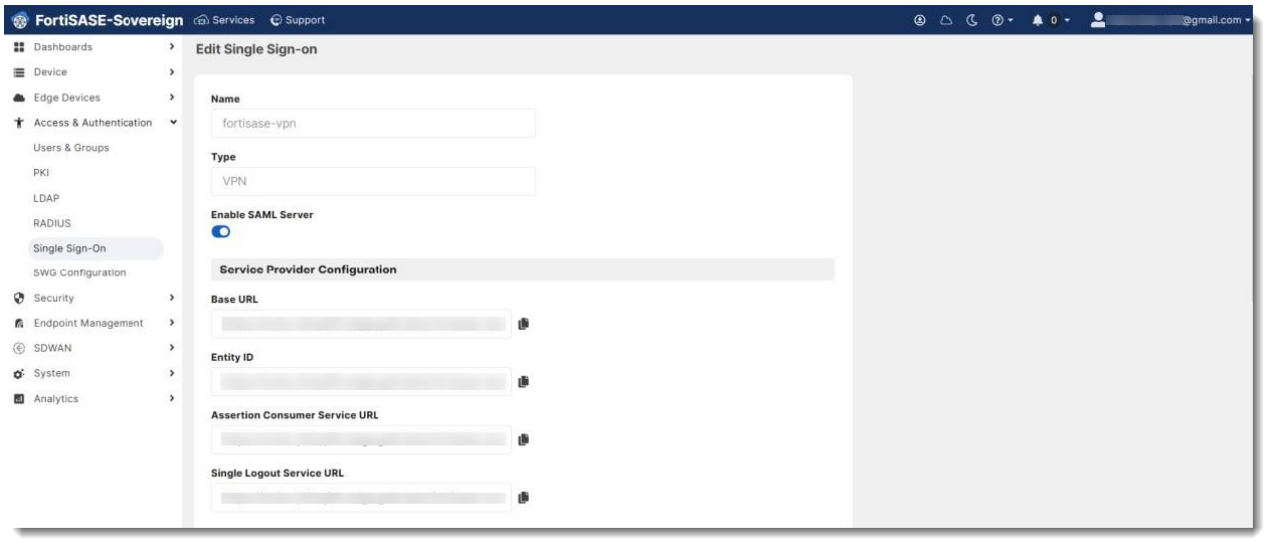
Add SSO to IPsec VPN

1. Select *System>Service Settings*.

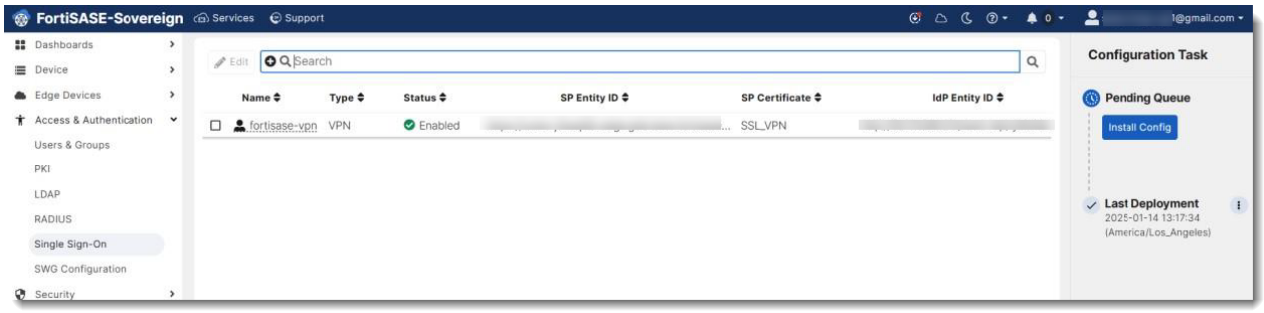


2. Review the service settings, make sure that the VPN Configuration is *IPSEC*, and click *OK*.

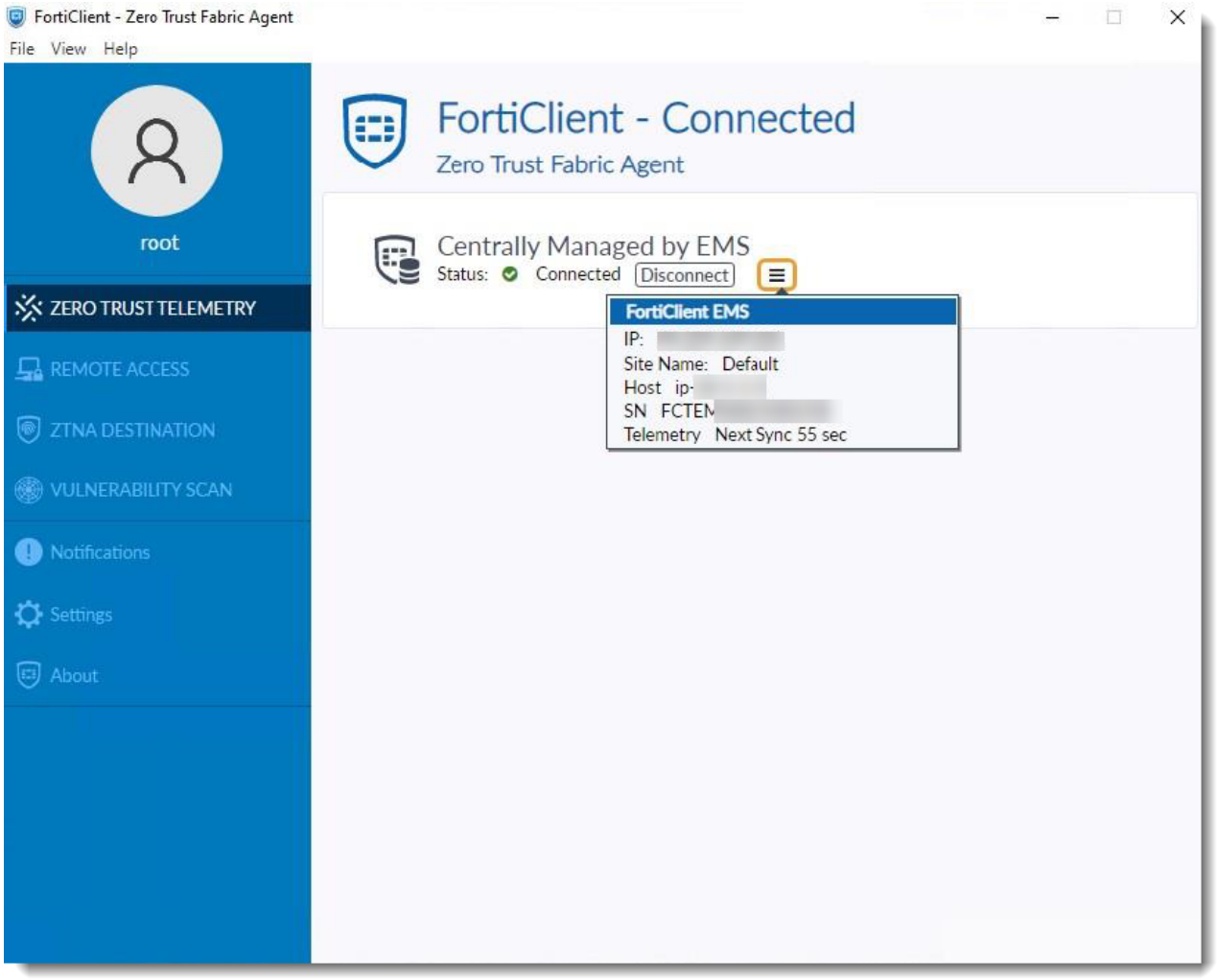
3. Select *Access & Authentication >Single Sign-On*, and turn on *Enable SAML Server*.



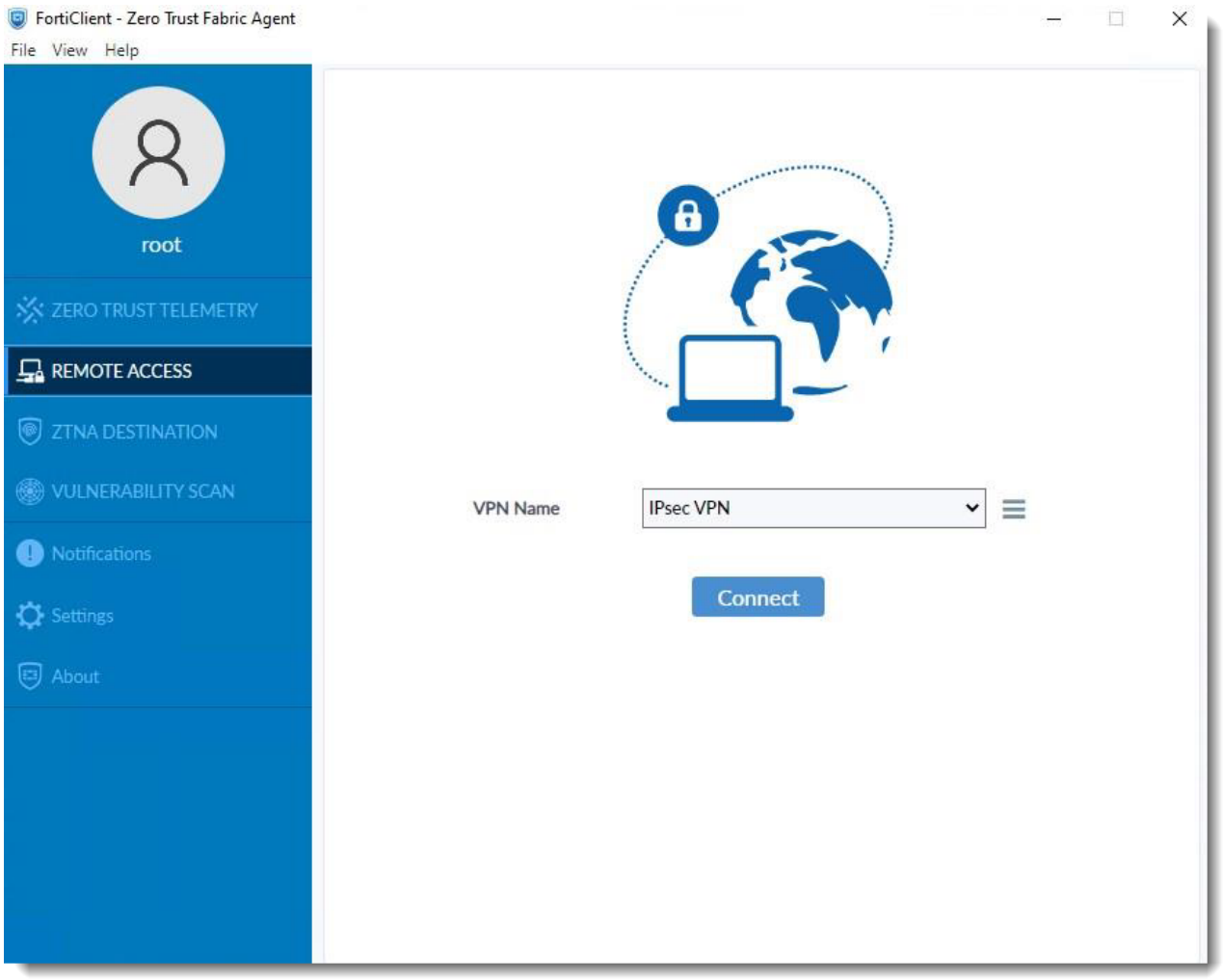
4. Under *Identity Provider Configuration*, enter the SAML IdP settings and click *OK*.



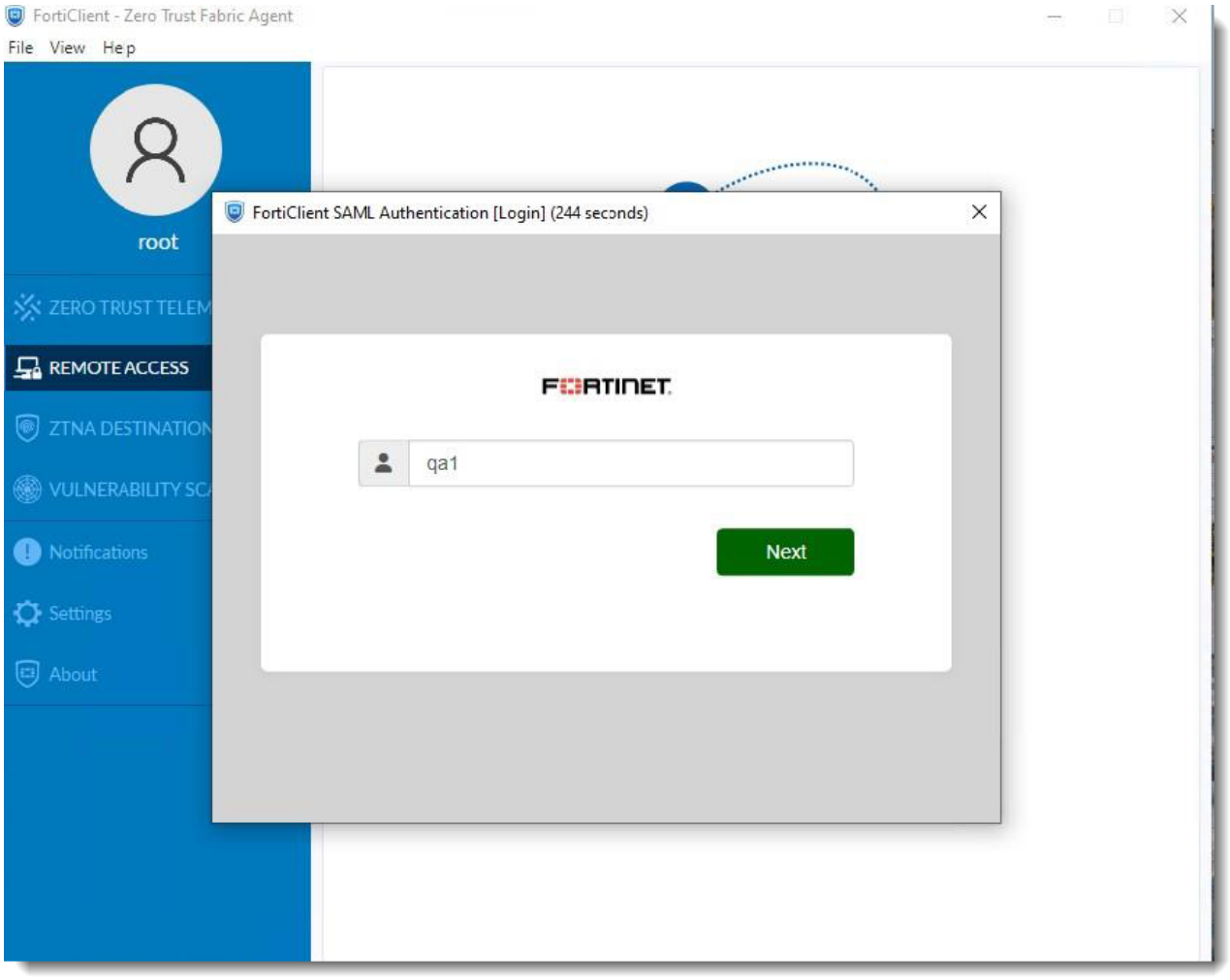
5. After the SAML server is created, click *Install Config* to deploy the SAML configuration.
6. Follow the prompts onscreen to complete deploying the SAML configuration.
7. After SAML configuration has been deployed, start FortiClient, and it will synchronize the SAML configuration after 60 seconds.



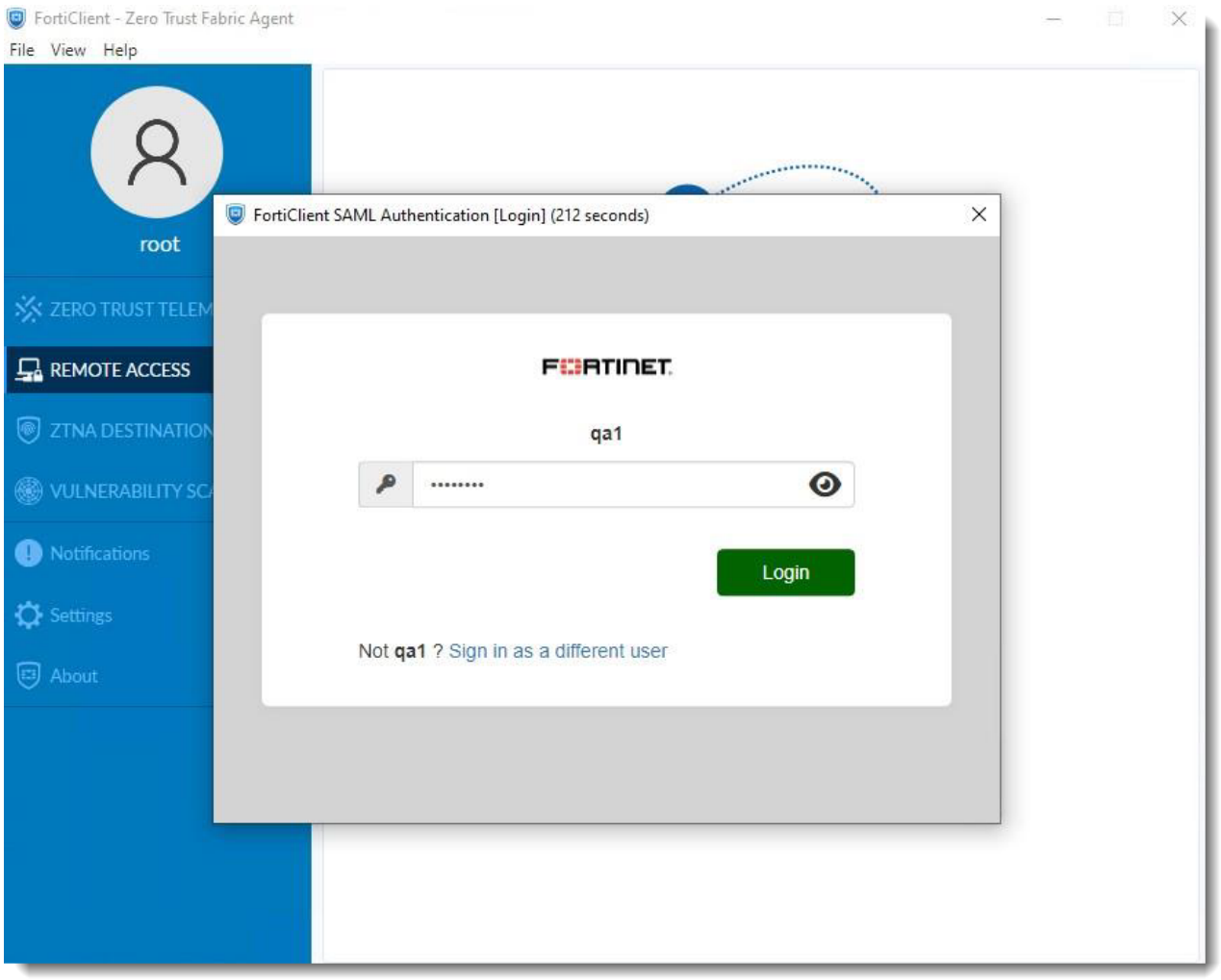
8. Select *REMOTE ACCESS*, and click *Connect*.



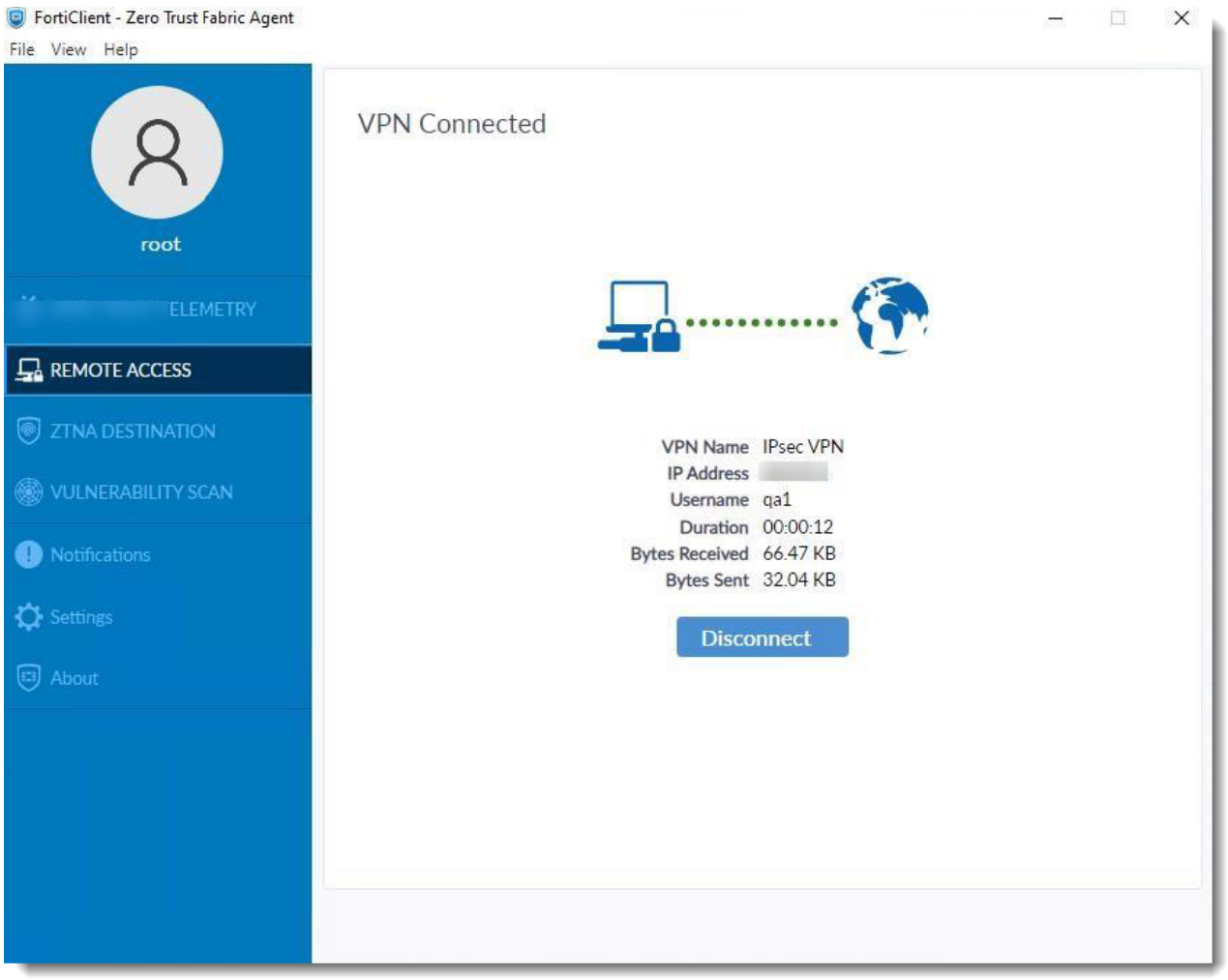
9. When the FortiClient SAML Authentication page pops up, enter the username, and click *Next*.



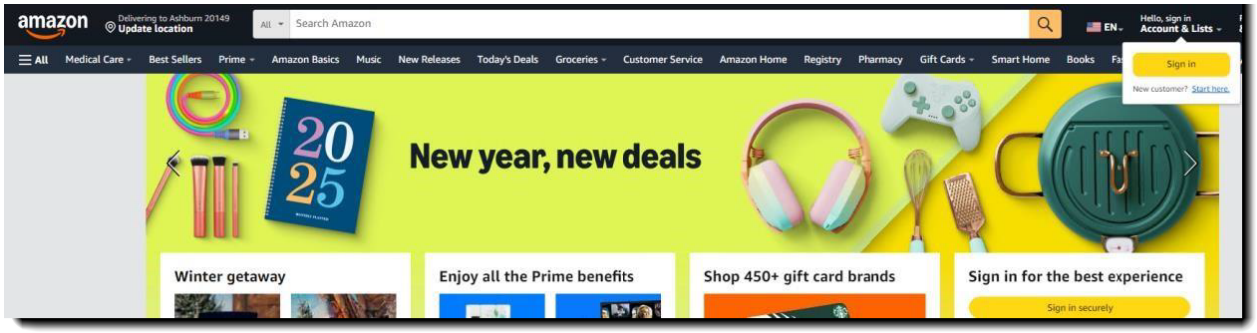
10. Enter your password, and click *Login*.



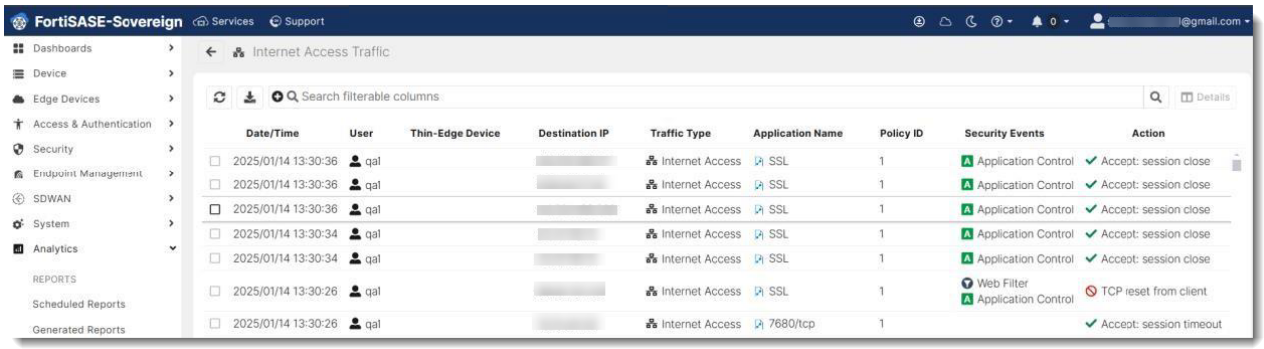
You have logged in as a SAML user.



11. Start your web browser, and open a website of interest.



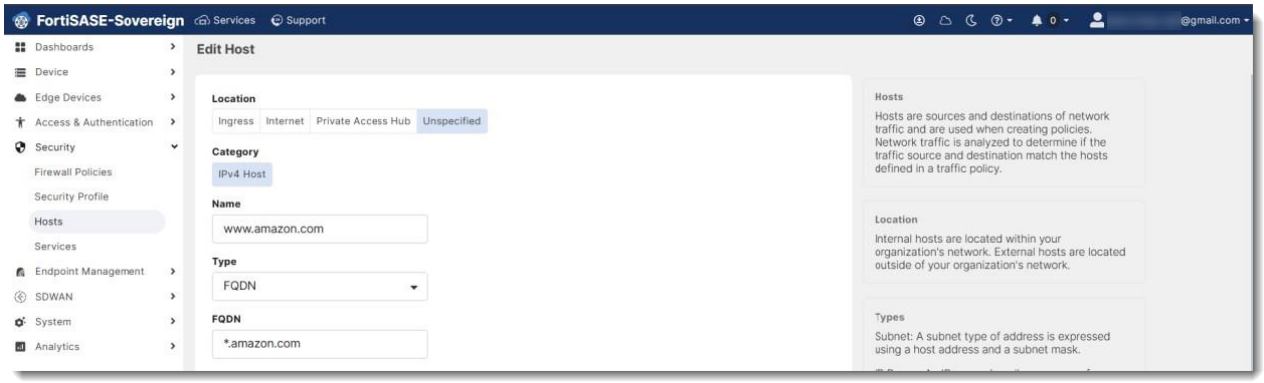
12. On the FortiSASE-Sovereign portal, select Analytics>Traffic to view the Internet Access Traffic logs.


FortiSASE-Sovereign
Services
Support
@gmail.com
Dashboards
Device
Edge Devices
Access & Authentication
Security
Endpoint Management
SDWAN
System
Analytics
REPORTS
Scheduled Reports
Generated Reports
Internet Access Traffic
Search filterable columns
Details
Date/Time
User
Thin-Edge Device
Destination IP
Traffic Type
Application Name
Policy ID
Security Events
Action
2025/01/14 13:30:36 qal Internet Access SSL 1 Application Control Accept: session close
2025/01/14 13:30:36 qal Internet Access SSL 1 Application Control Accept: session close
2025/01/14 13:30:36 qal Internet Access SSL 1 Application Control Accept: session close
2025/01/14 13:30:34 qal Internet Access SSL 1 Application Control Accept: session close
2025/01/14 13:30:34 qal Internet Access SSL 1 Application Control Accept: session close
2025/01/14 13:30:26 qal Internet Access SSL 1 Web Filter Application Control TCP reset from client
2025/01/14 13:30:26 qal Internet Access 7680/tcp 1 Accept: session timeout

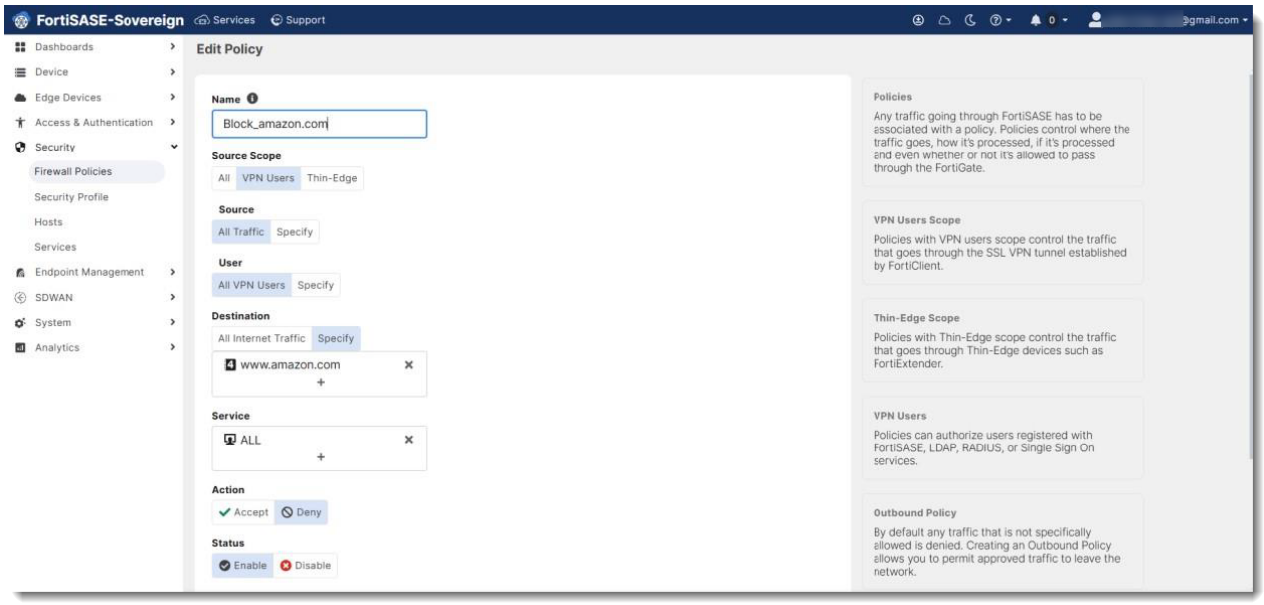
Configure firewall policies

You can set specific firewall policies to block a certain website. The following example is a firewall policy that blocks traffic from `amazon.com`.

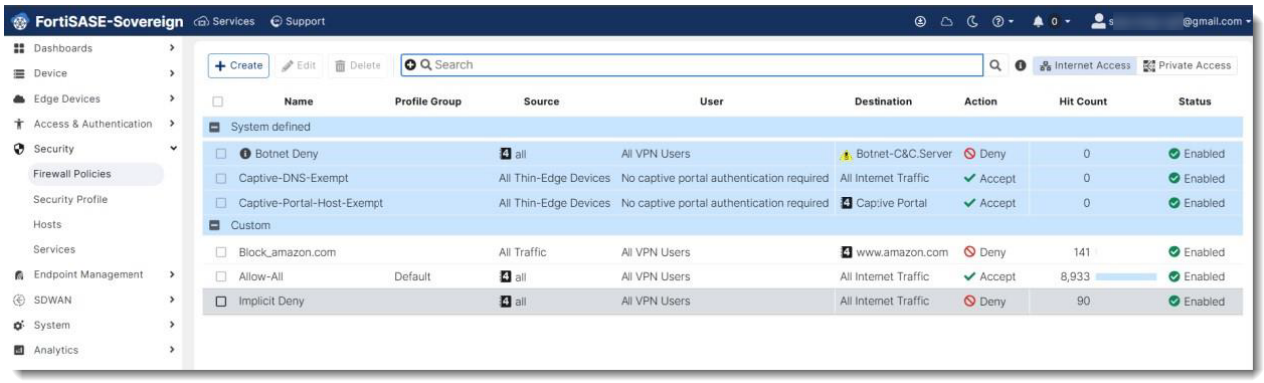
1. Set up a host by selecting *Security>Hosts*.



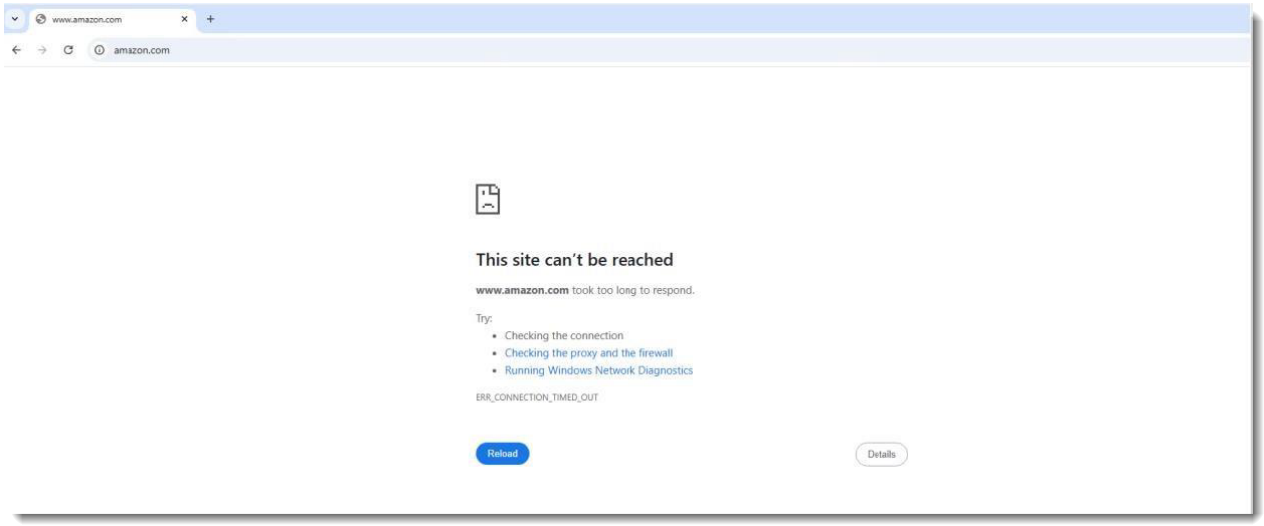
2. Select *Security>Firewall Policies*, and fill in the policy settings.



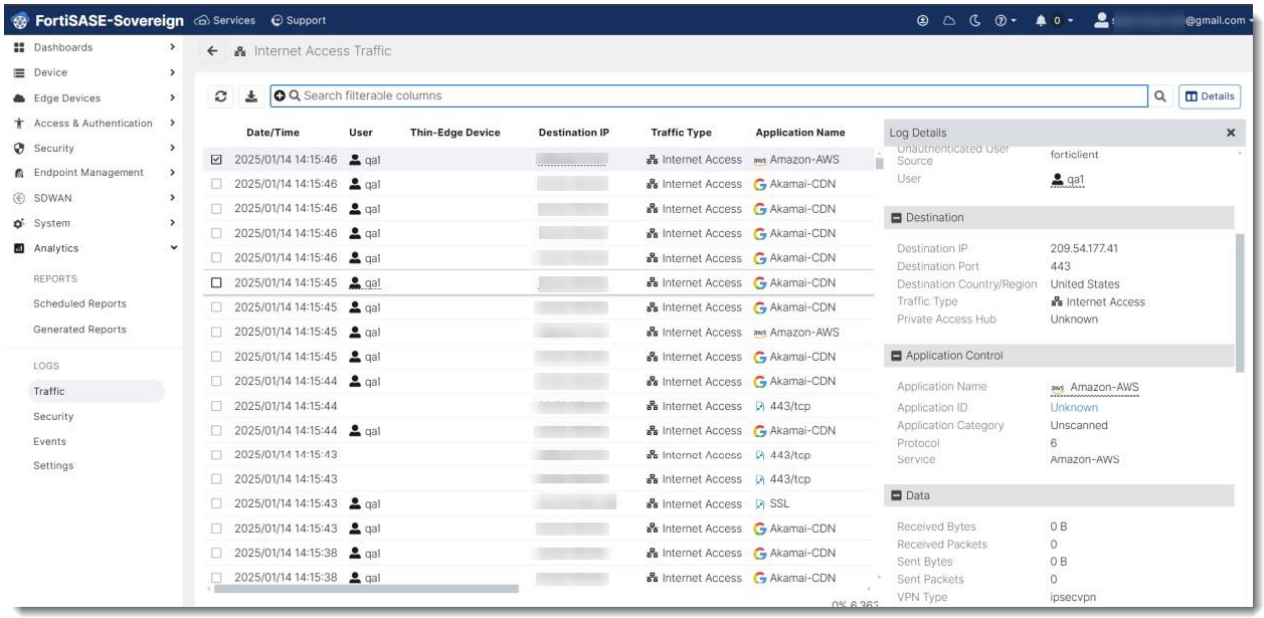
3. Move the created policy above *Allow-All*, install the configuration successfully.



4. Start FortiClient, and make sure that you are using the VPN.
5. Start your web browser, and try to access `www.amazon.com`. The following error message appears.

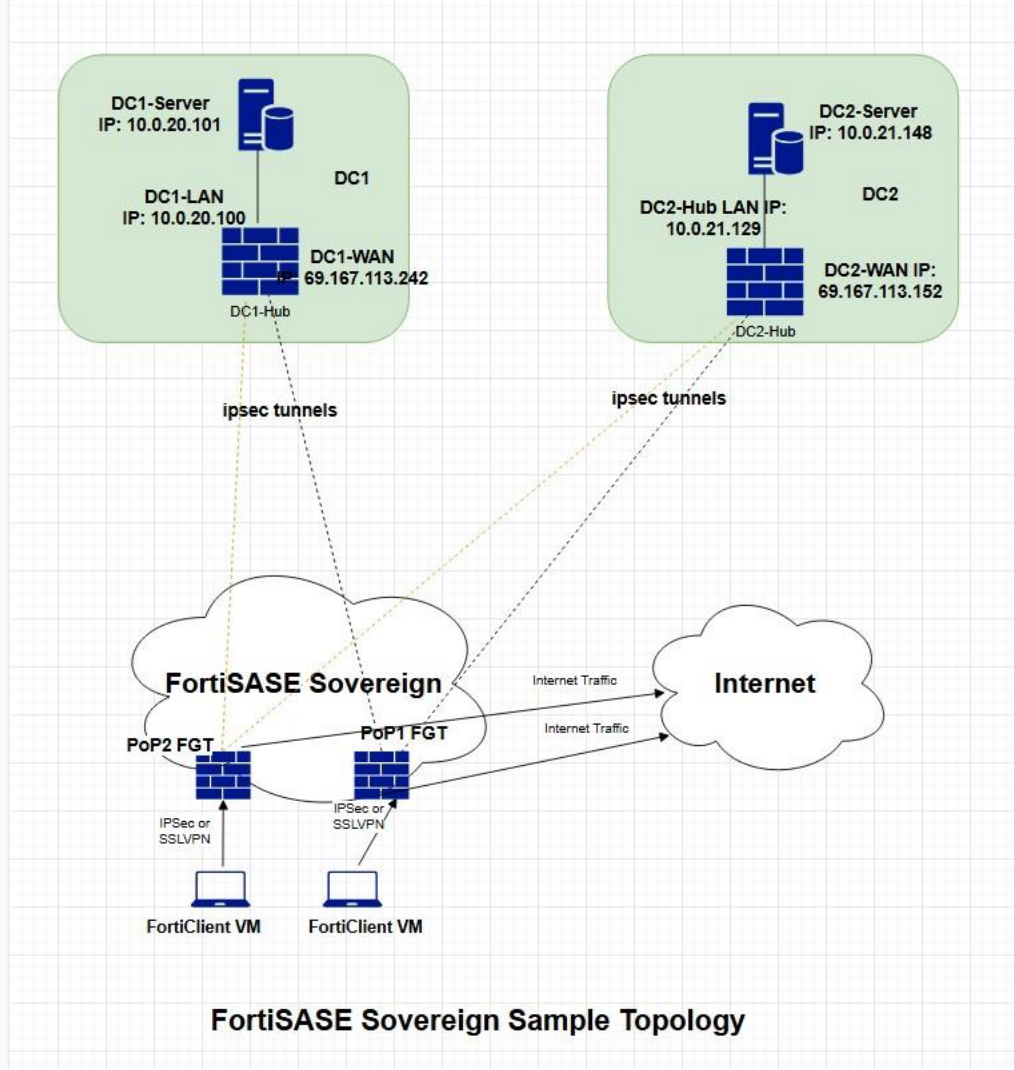


6. On the FortiSASE-Sovereign portal, select *Analytics>Traffic*. It shows Deny traffic log.



SPA setup guide (network topology)

Section 1: SPA hubs and web servers



FortiSASE Sovereign Sample Topology

- DC1-Hub:00.000.000.000 login: xxxxx/xxxxxxx
- DC2-Hub: 00.000.000.000 login: xxxxx/xxxxxxxx
- Finance test page: https://finance.fortinet.com/ is located in DC1-server behind Hub1
- Marketing test page: https://marketing.fortinet.com/ is located in DC2-server behind Hub2
- FTP test server (**Note:** This server is on DC1-Server behind DC1-Hub.):
  - IP: 00.0.00.000
  - Port: 2121
  - Username:xxxxxx
  - Password: xxxxxxx

Parameters to bring up service connection

- Network Configuration Tab:
  - BGP Router ID Subnet 00.000.000/00
  - Autonomous System Number (ASN) 65001
  - Health Check IP 00.00.00.00
- Service Connection Tab:

First service connection

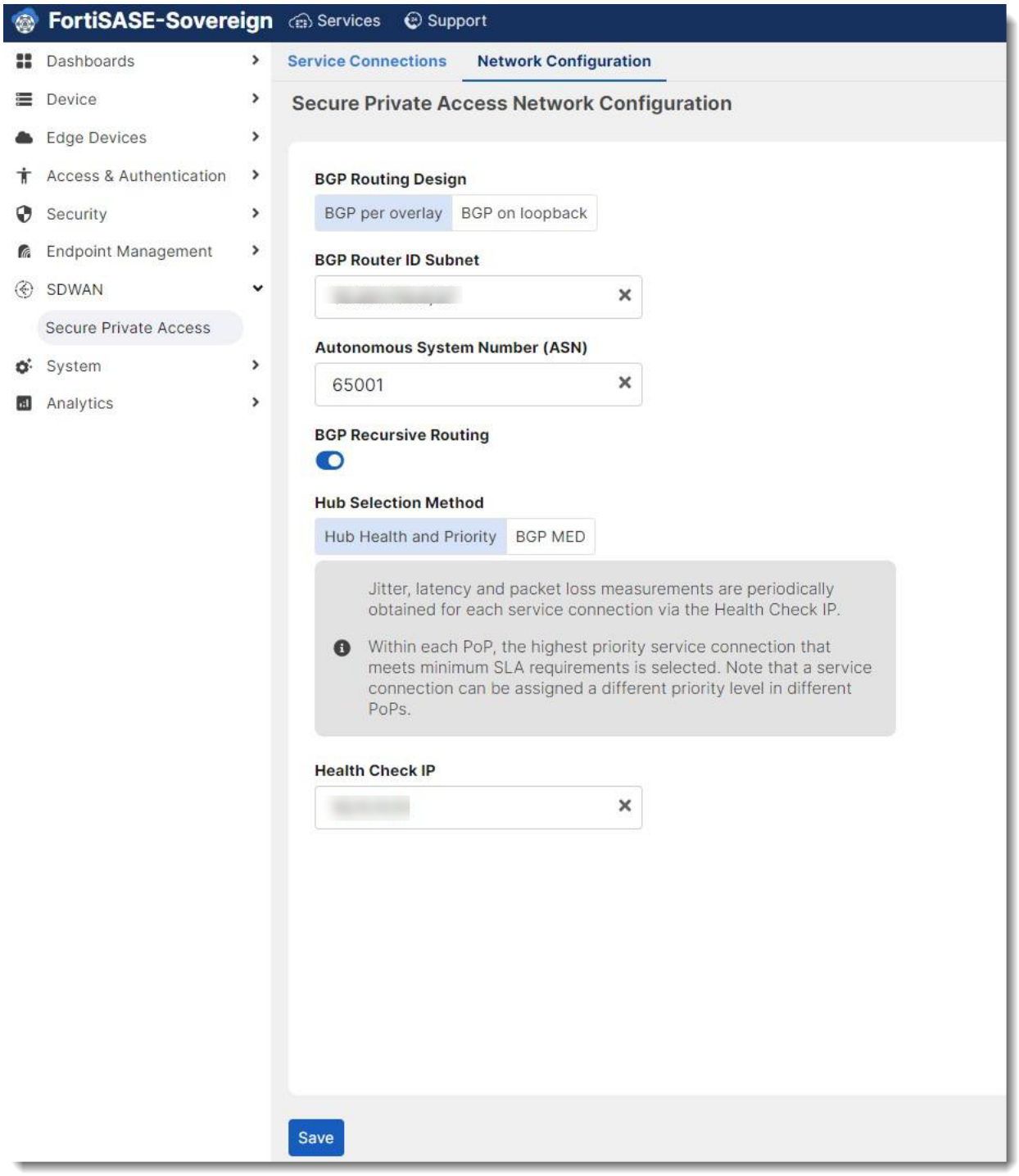
- Name: Your preference. Sample could be DC1-Hub
- Remote Gateway: 00.000.000.000
- Authentication Method, Preshared Key: xxxxxxxxx
- BGP Peer IP: 00.000.0.000
- Network Overlay ID: 11

Second service connection

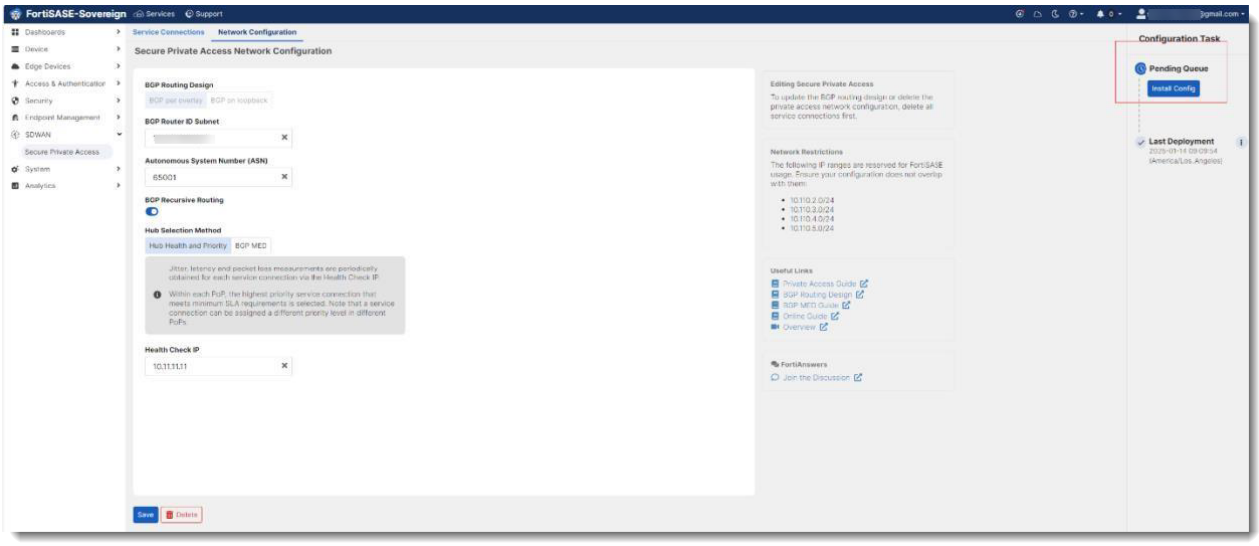
- Name: Your preference. Sample could be DC2-Hub
- Remote Gateway: 00.000.000.000
- Authentication Method, Preshared Key: xxxxxxxxxx
- BGP Peer IP: 00.000.00.000
- Network Overlay ID: 12

Section 2: Deploy SPA on FortiSASE-Sovereign portal

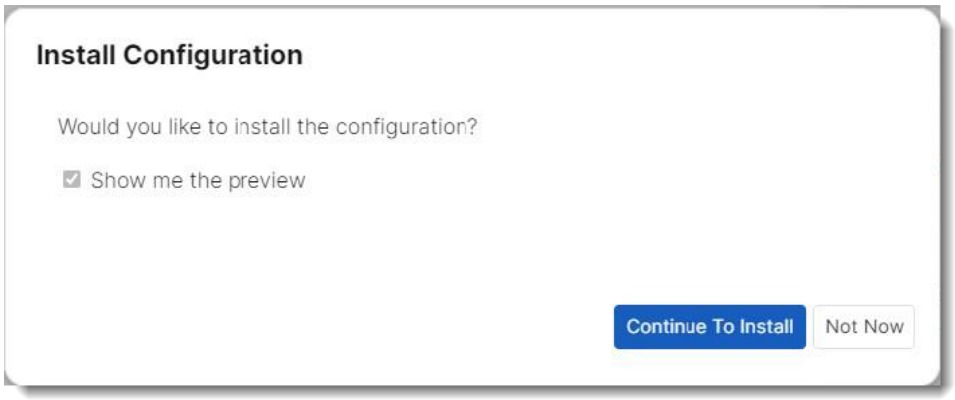
1. Log into FortiSASE-Sovereign portal, select SDWAN>Secure Private Access>Network Configuration, and make the entries and/or selections, and click Save.



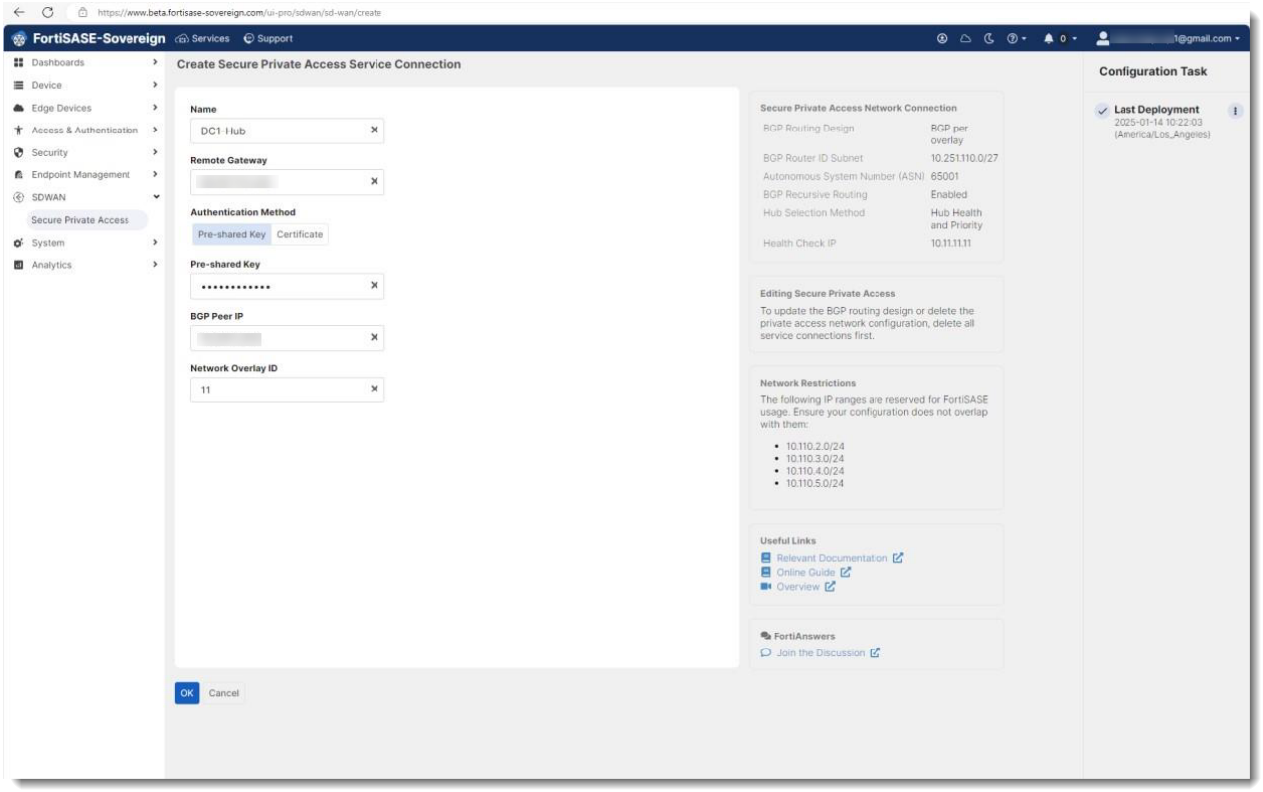
2. When the Configuration Task panel pops up, click Install Config.



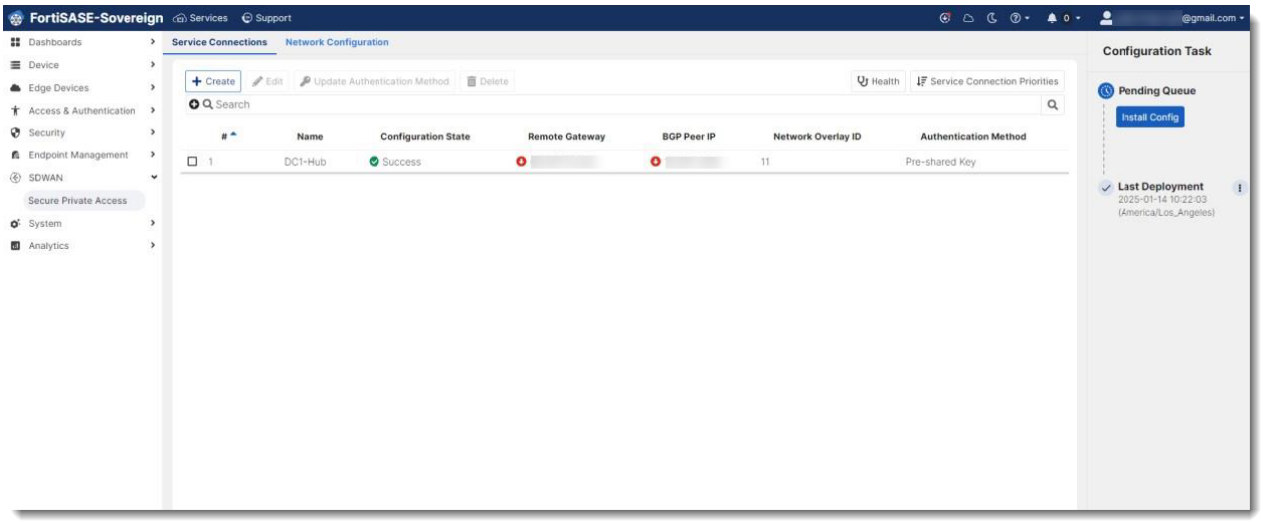
3. In the Install Configuration dialog, click Continue to Install to complete the configuration.



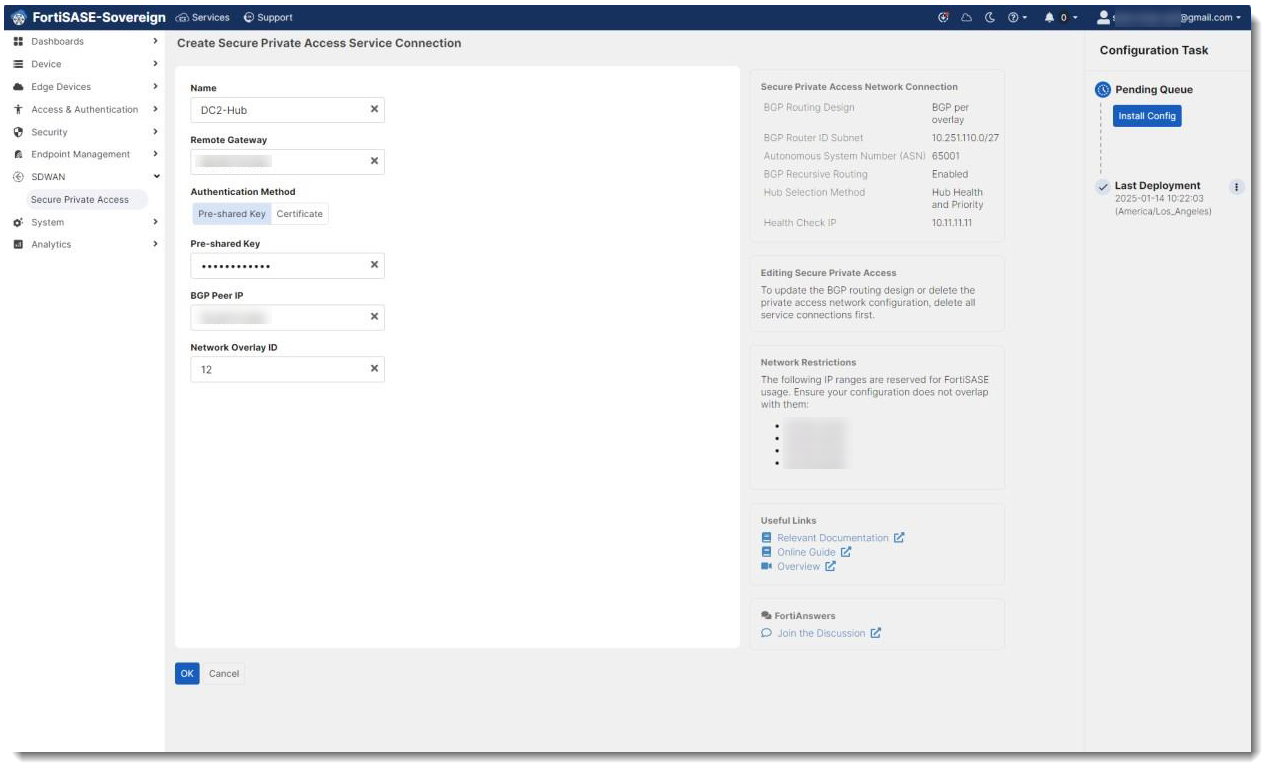
4. After Network Configuration is completed, select SD-WAN>Secure Private Access>Service Connection, and click Create to create the first Secure Private Access connection as illustrated in the following screenshot. (**Note:** The pre-shared key for this setup is "Fortinet123!".)



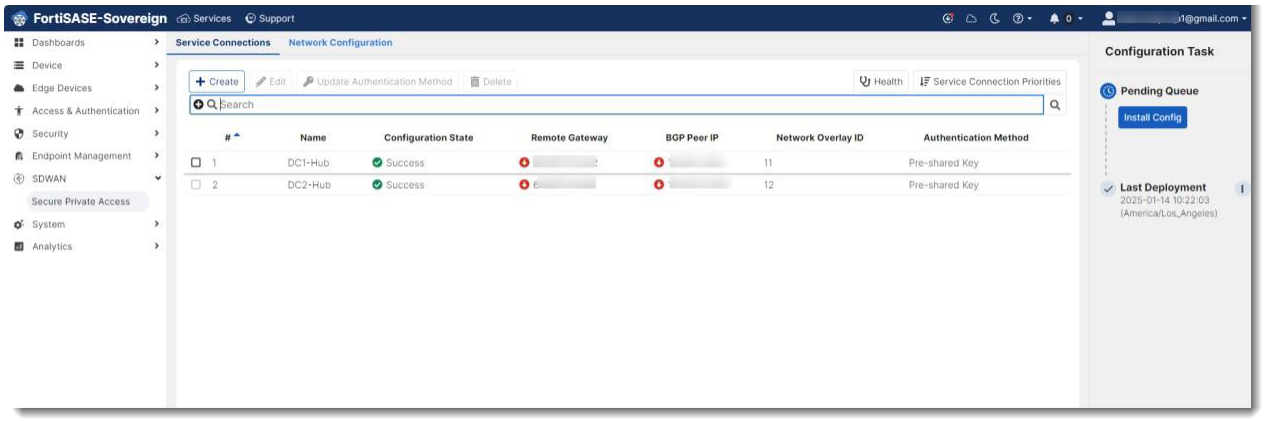
The first service connection appears under Service Connections tab.



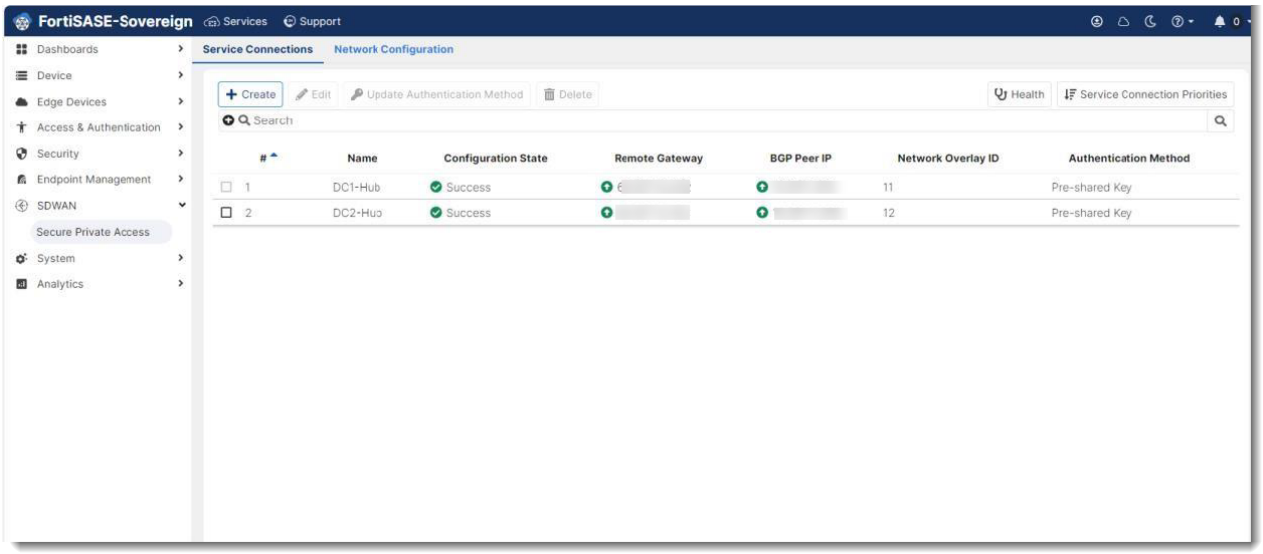
5. After the first service tunnel is created, repeat Step 4 to create the second Secure Private Access connection.



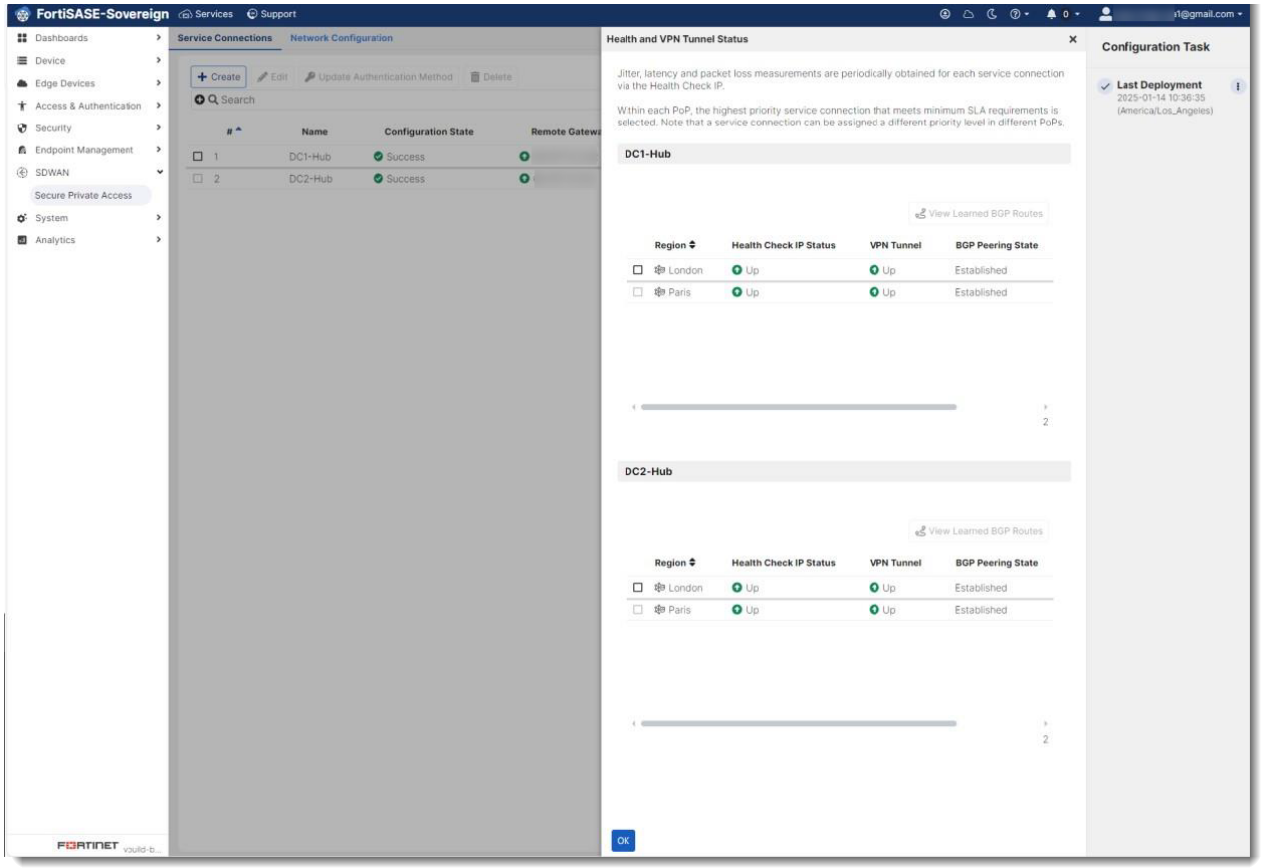
6. After both service tunnels are created, click Install Config to deploy the configuration to PoP FortiGates.



7. Follow the prompts onscreen to complete deploying the configuration.
8. After the deployment, both service connections to DC1-Hub and DC2-Hubs are up and running.

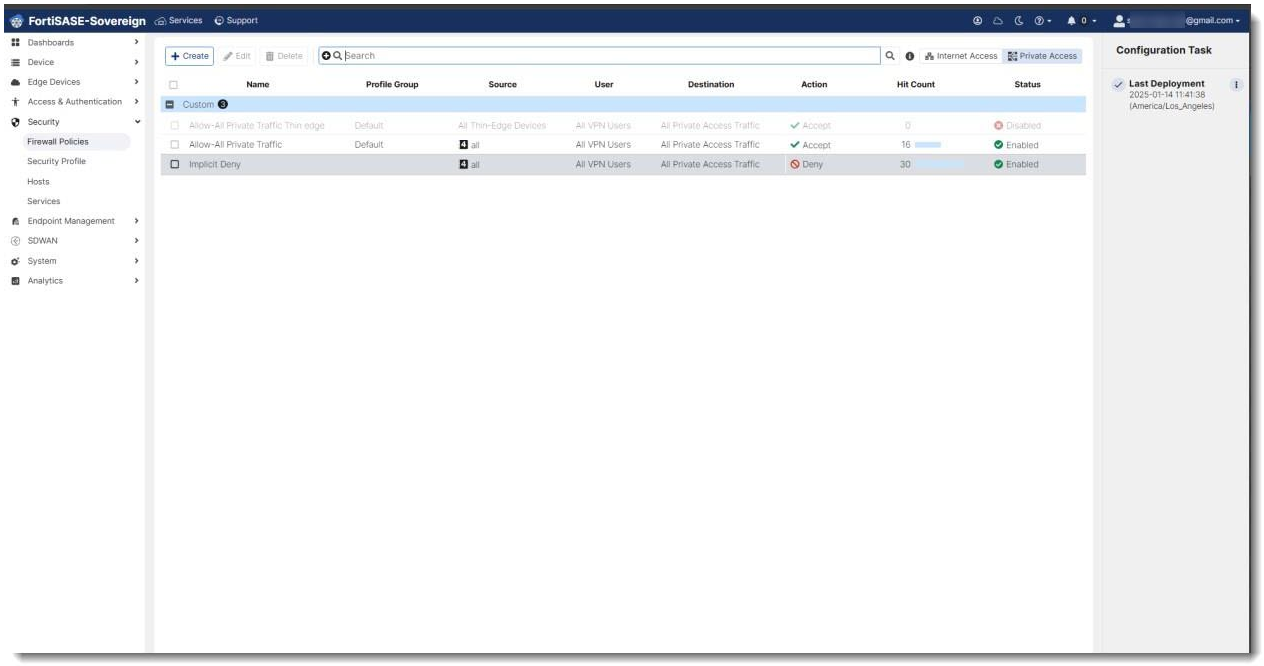


9. Click Health to check the connection of each PoP FortiGate to each hub.



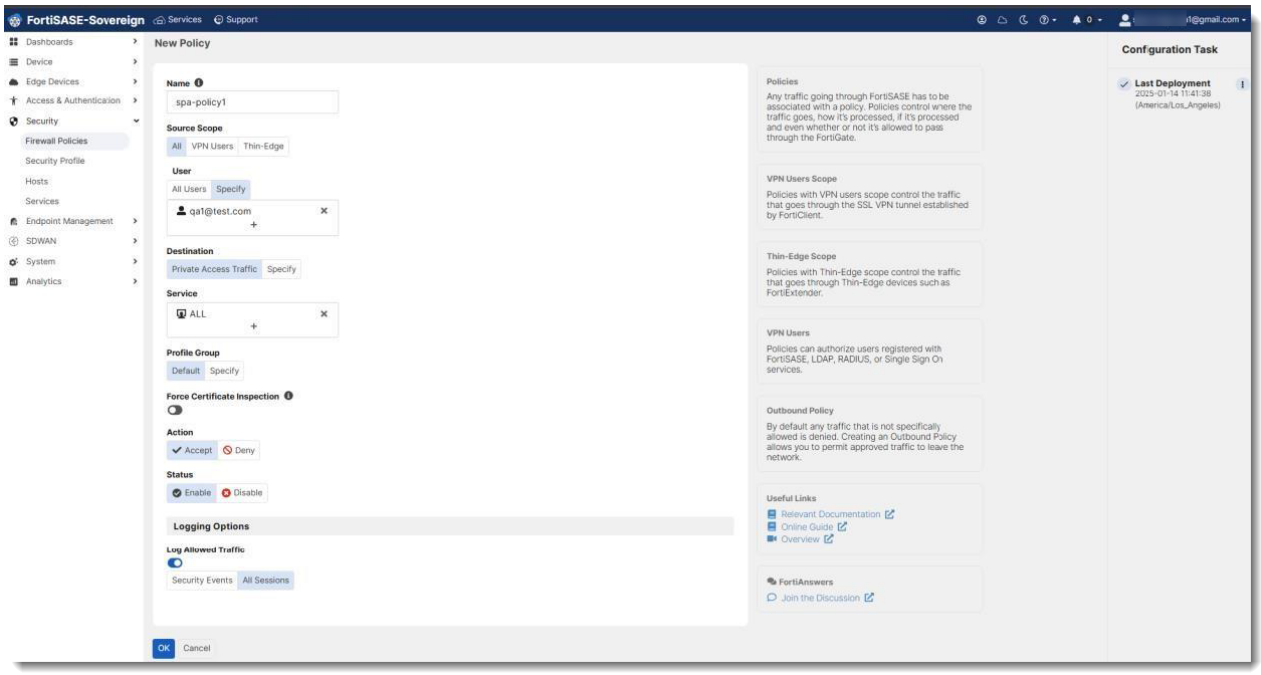
Section 3: Configure Secure Private Access policies

1. Select Security > Firewall Policies >Private Access, and click Create to create a custom firewall policy for secure private access.

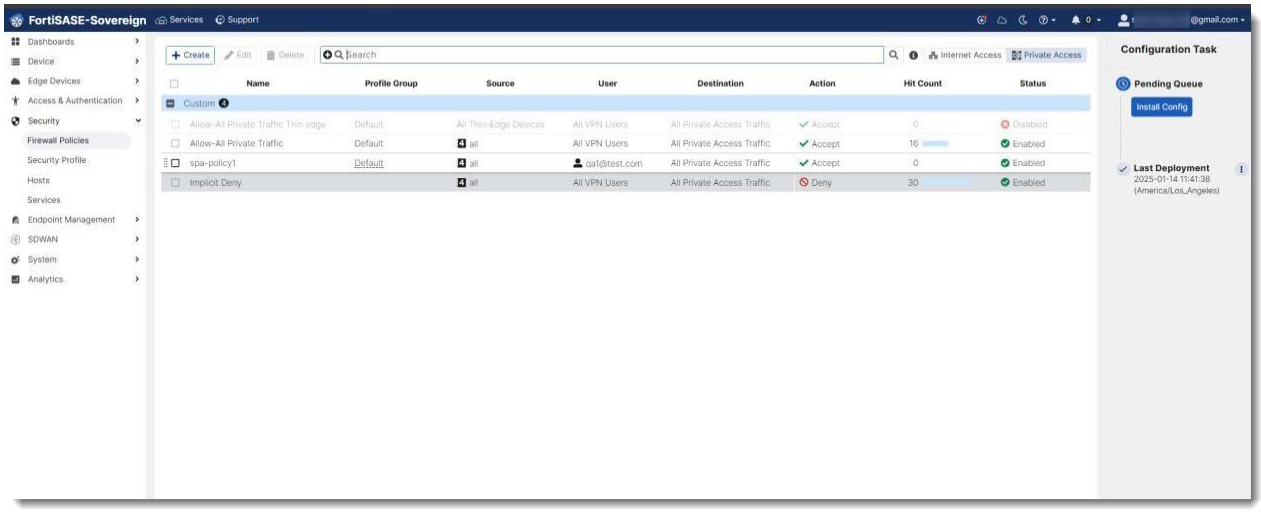


There is a default “Allow All Private Access” policy that allows all the private access traffic, but you can create your custom policy. Be sure to place the customized policy in front of the default policy. See the following steps for details.

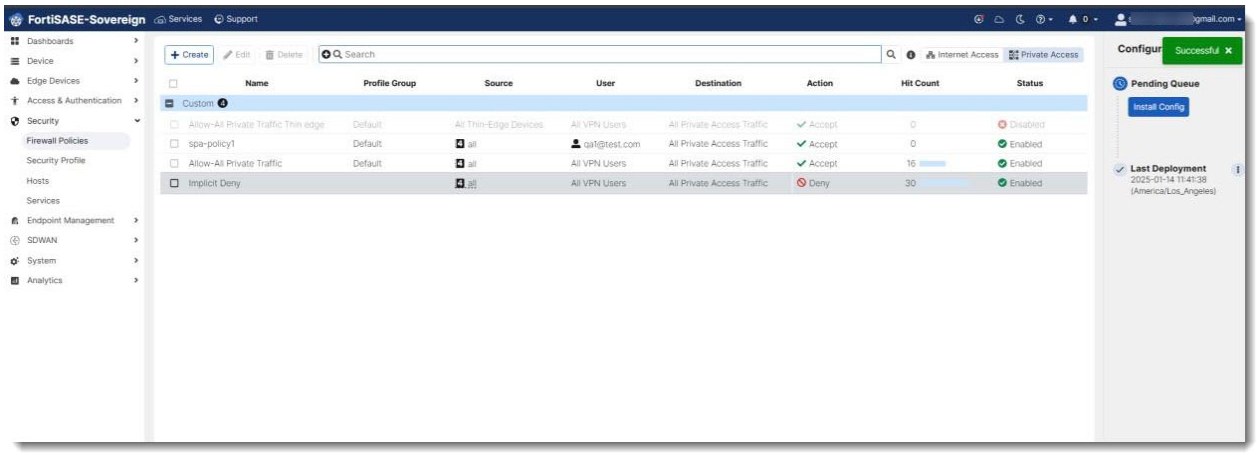
2. Create the custom policy, and click OK.



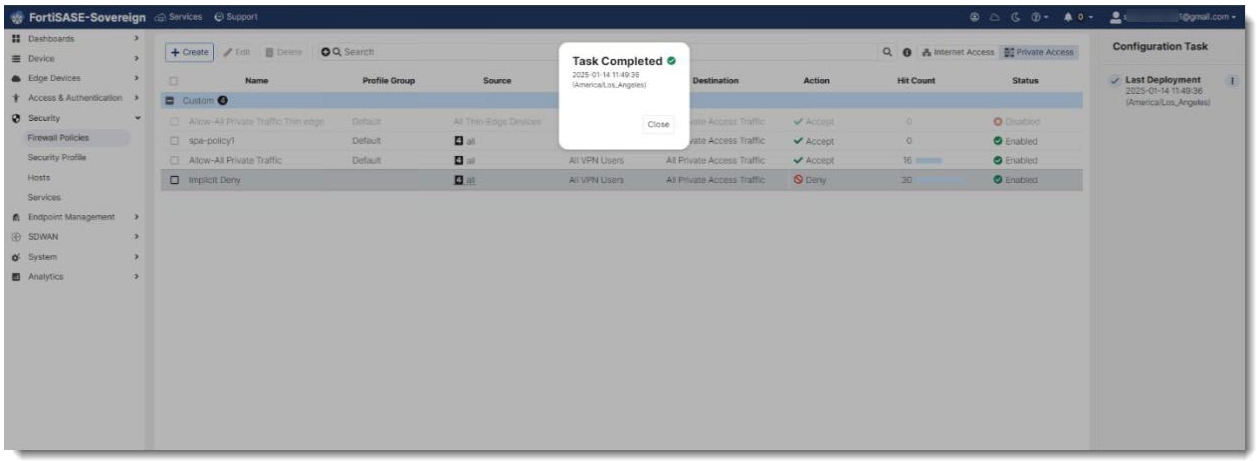
3. After the policy is created, click and drag it above the Allow-All Private Traffic policy.



4. Click Install Config to proceed with installing the configuration to PoP FortiGates.



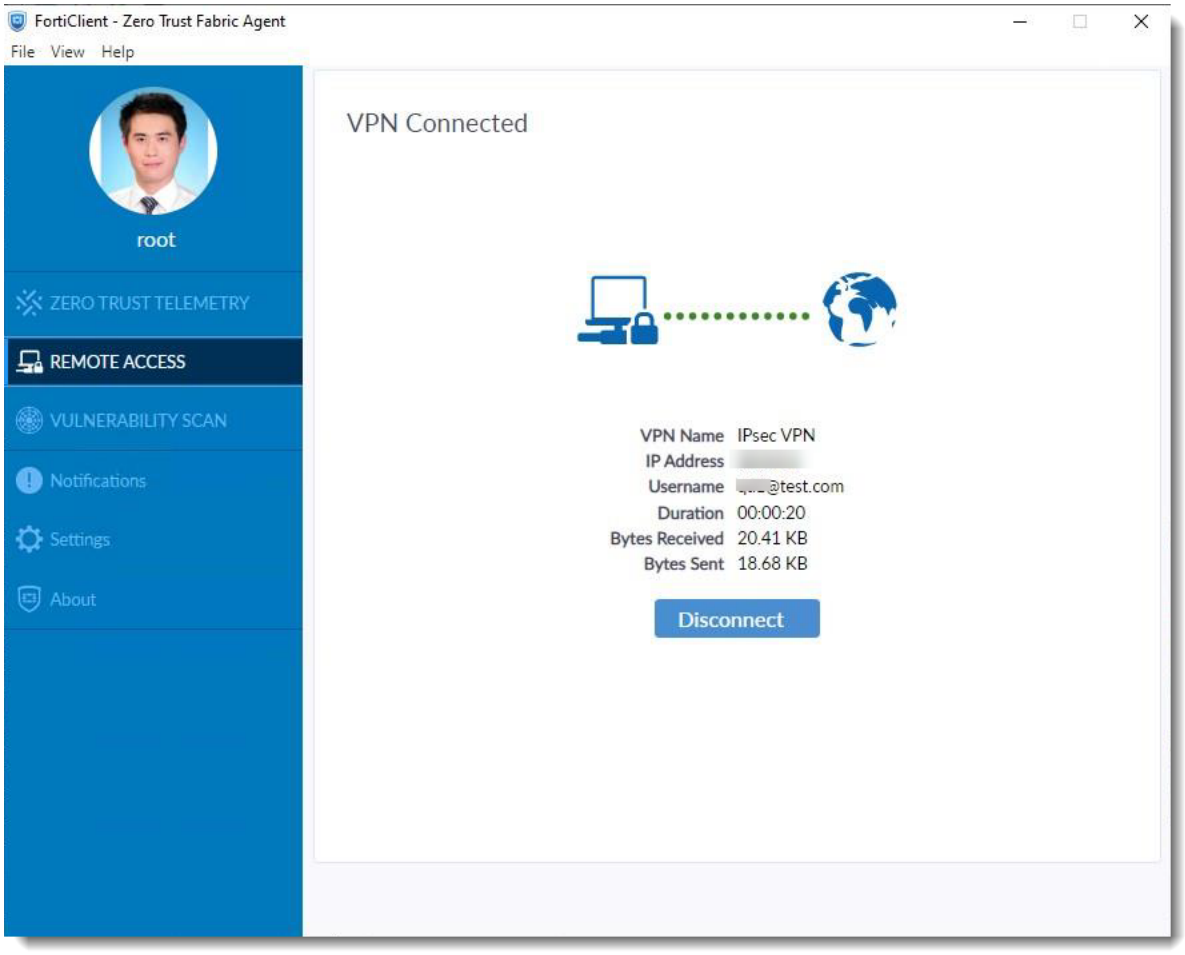
5. Follow the prompts onscreen to complete the installation.
6. Click Close.



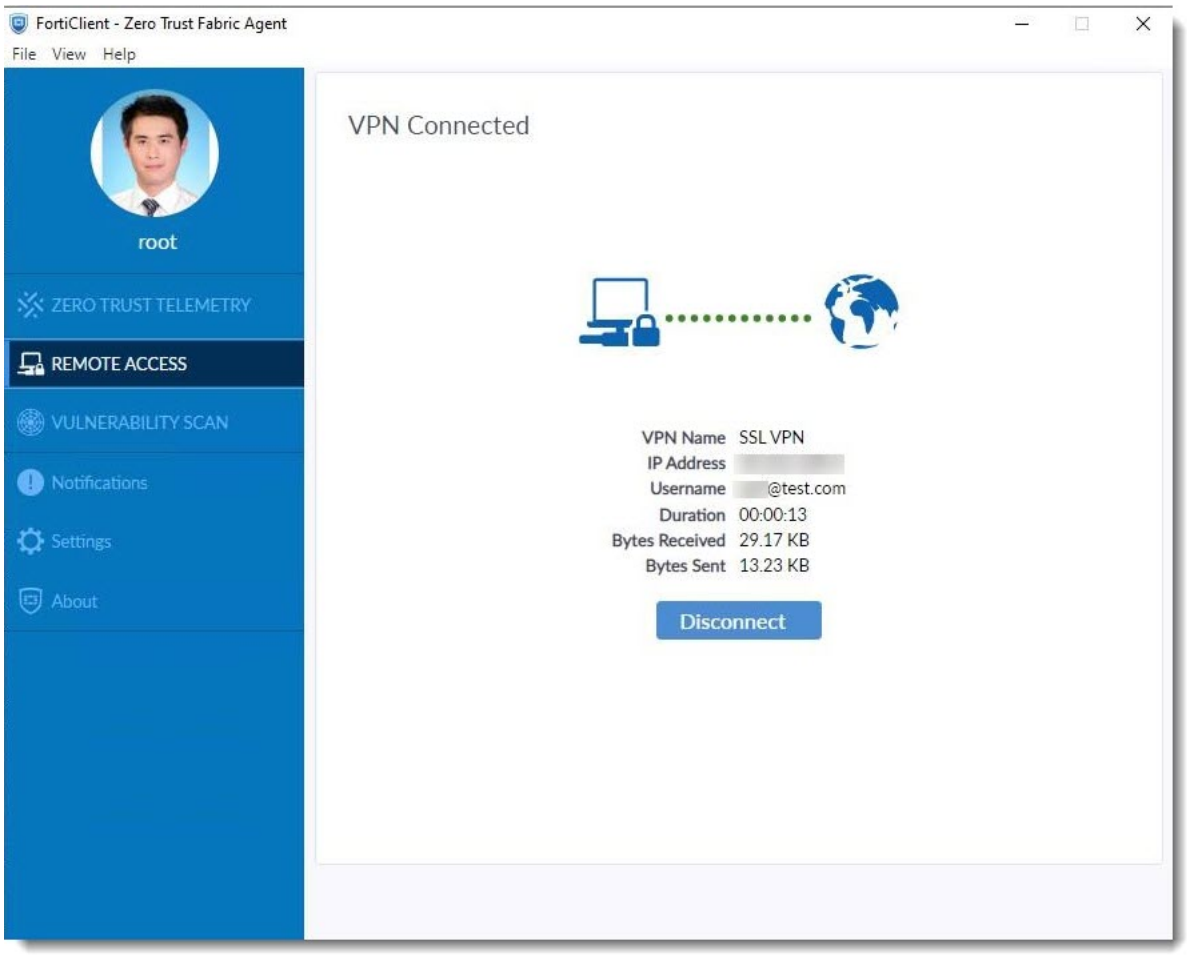
Section 4: Verify private access from end point with FortiClient

1. From your FortiClient endpoint, connect through IPsec VPN or SSL VPN.

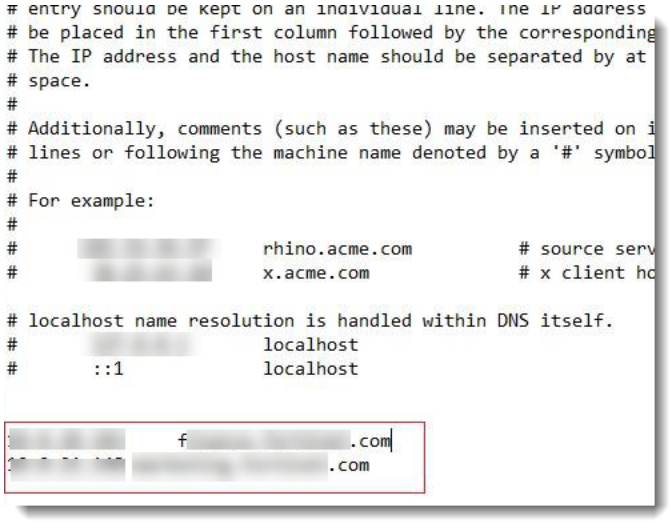
IPsec VPN



SSL VPN

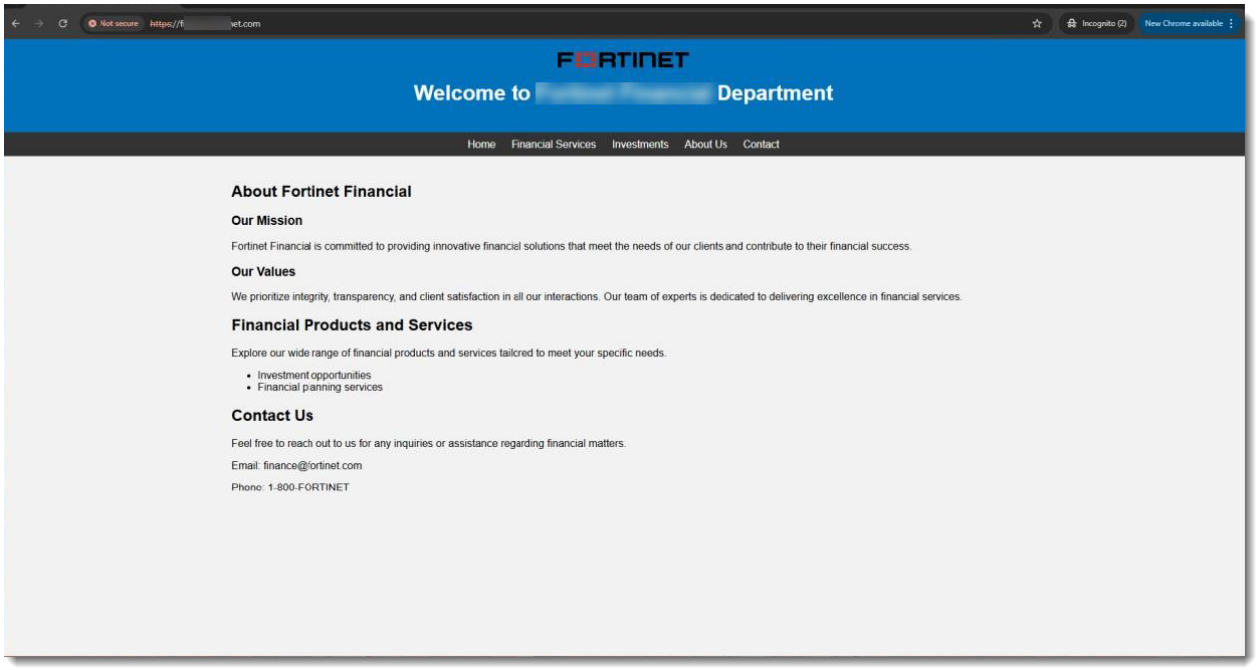


2. Modify the hosts file in `C:\Windows\System32\drivers\etc` and add these two entries to the hosts file.



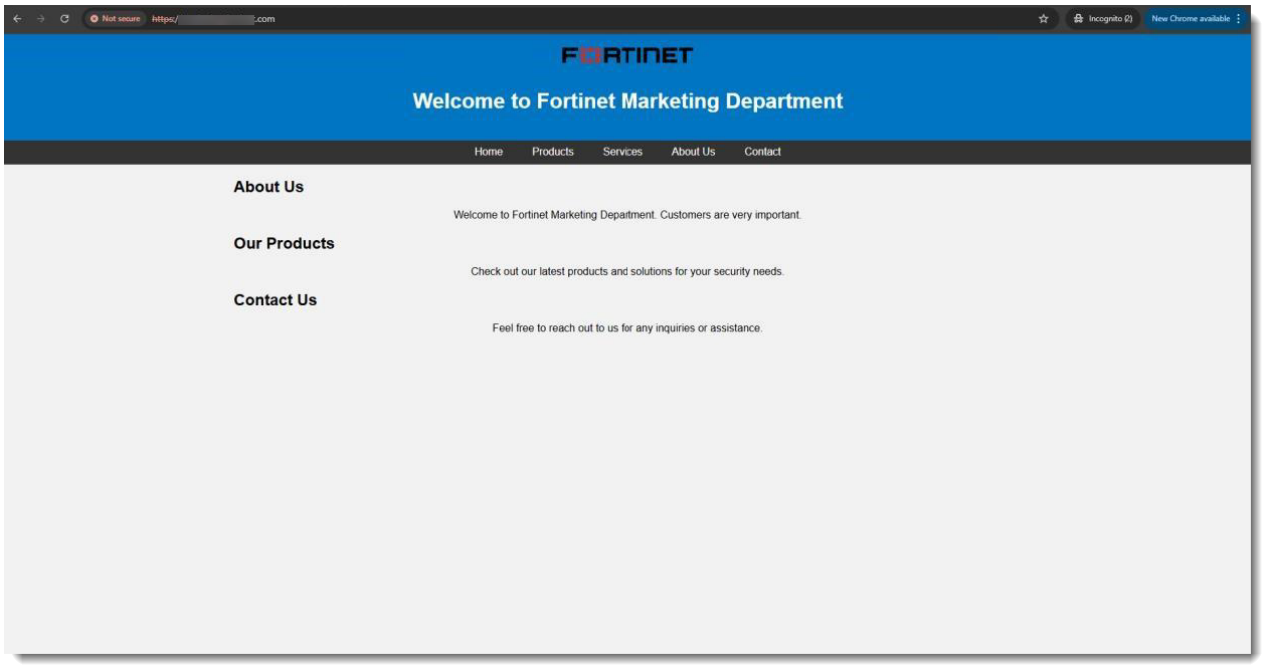
3. Open a browser and type https://finance.fortinet.com, and the web page opens.

This demonstrates access private resource behind DC1-hub through the secure private access network.



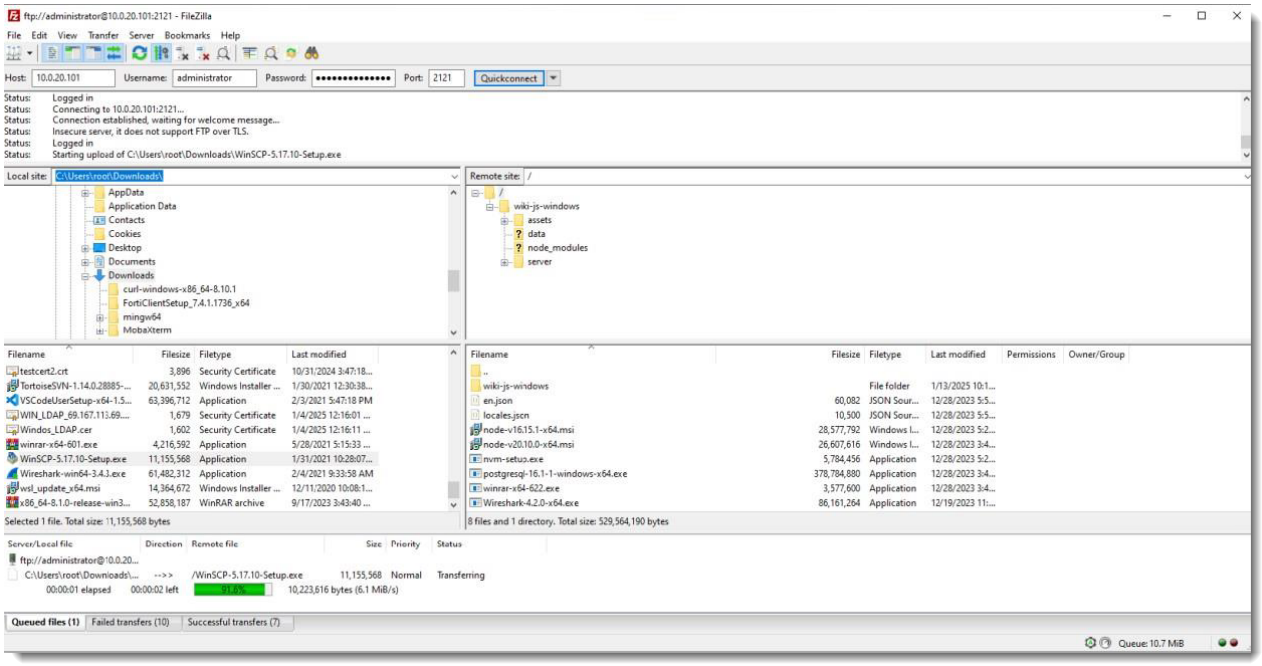
4. In the browser, type https://marketing.fortinet.com, and press Enter.

This is to demonstrate access private resource behind DC2-hub through secure private access network.

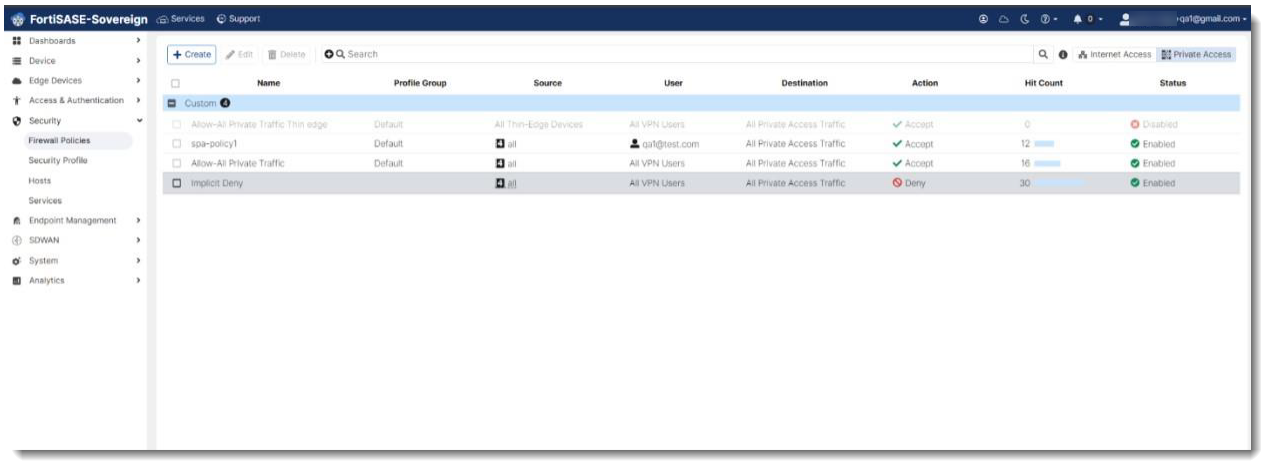


5. Start a FTP software application to make a connection to the FTP server 10.0.20.101 through Port 2121, using the username "administrator" and password "fortinet.com2023".

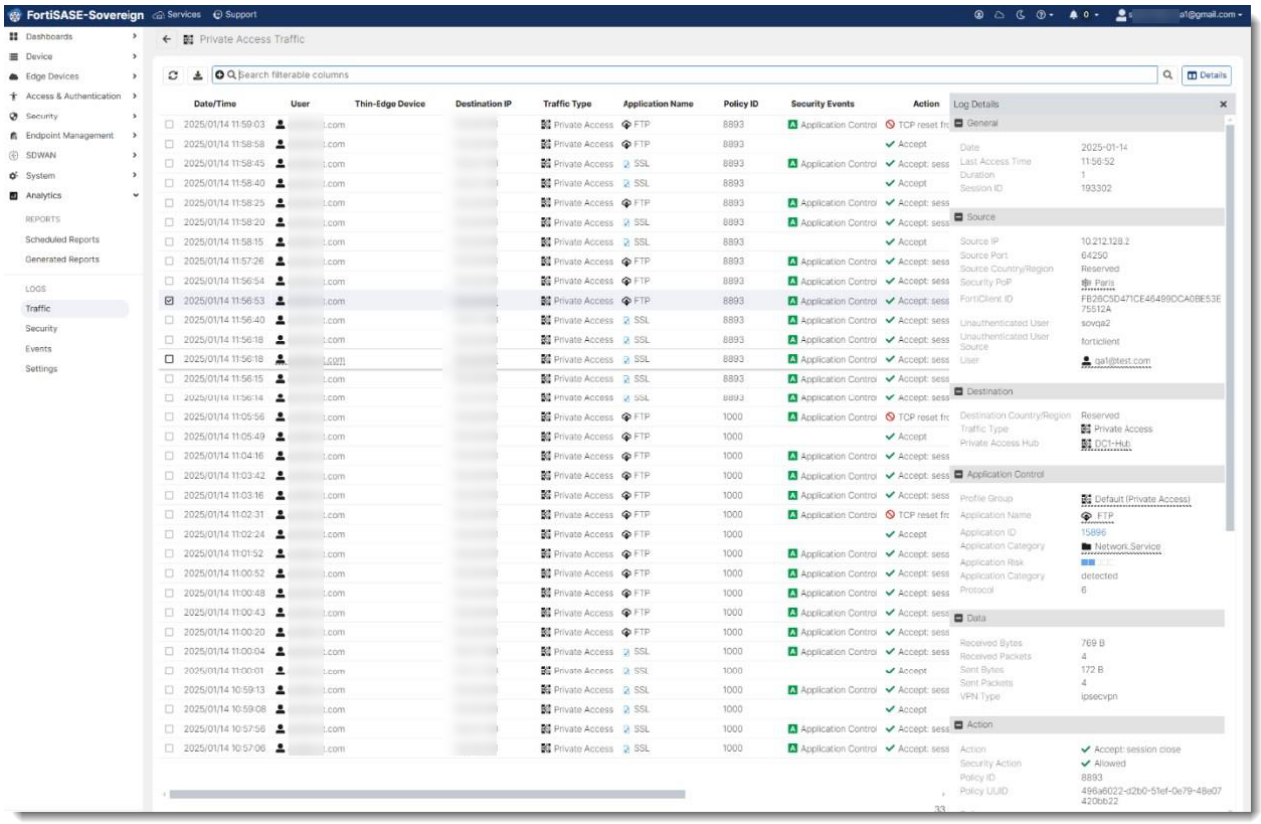
This step shows downloading and uploading files from the server behind DC1-Hub.



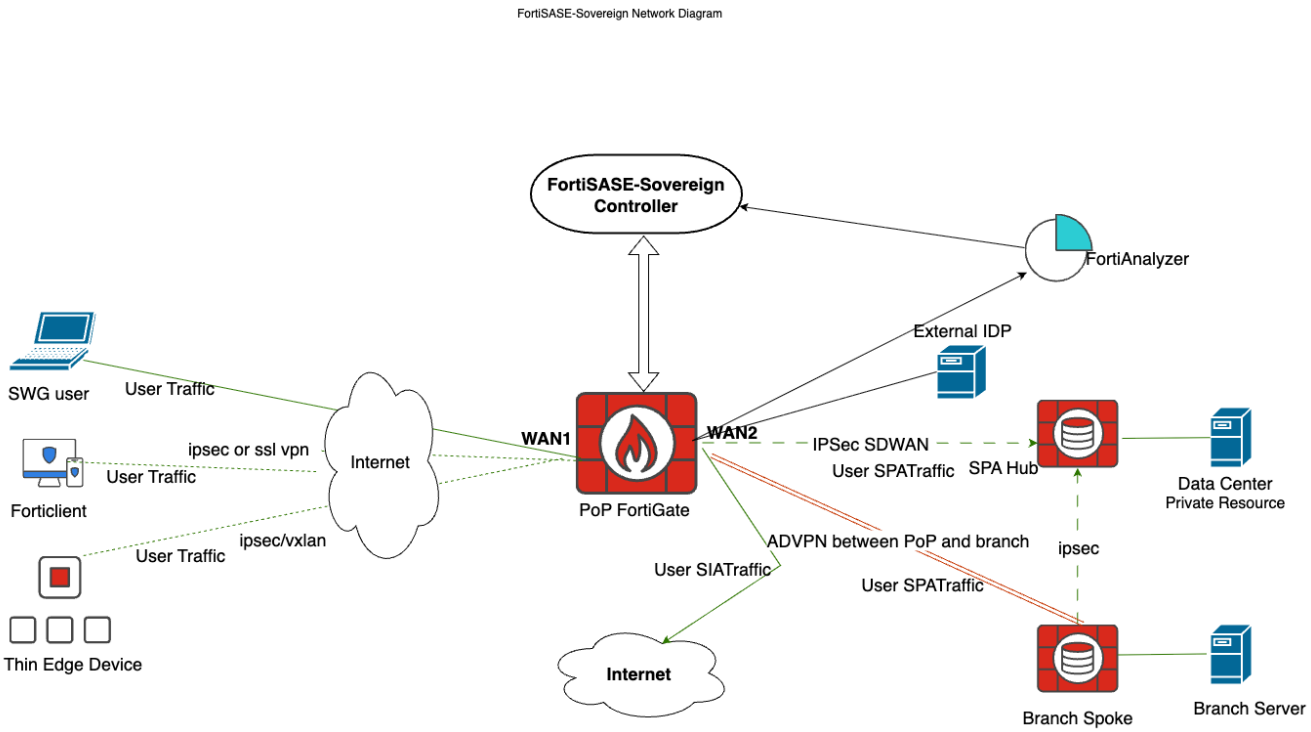
6. After some test traffic, go back to the Private Access policy page and verify that the customized policy has taken effect.



7. You can view the traffic log detail by going to Analytics/Traffic/Private Access Traffic to view the traffic logs. Double-clicking an entry will display details of that traffic entry.



Traffic Flow Diagrams

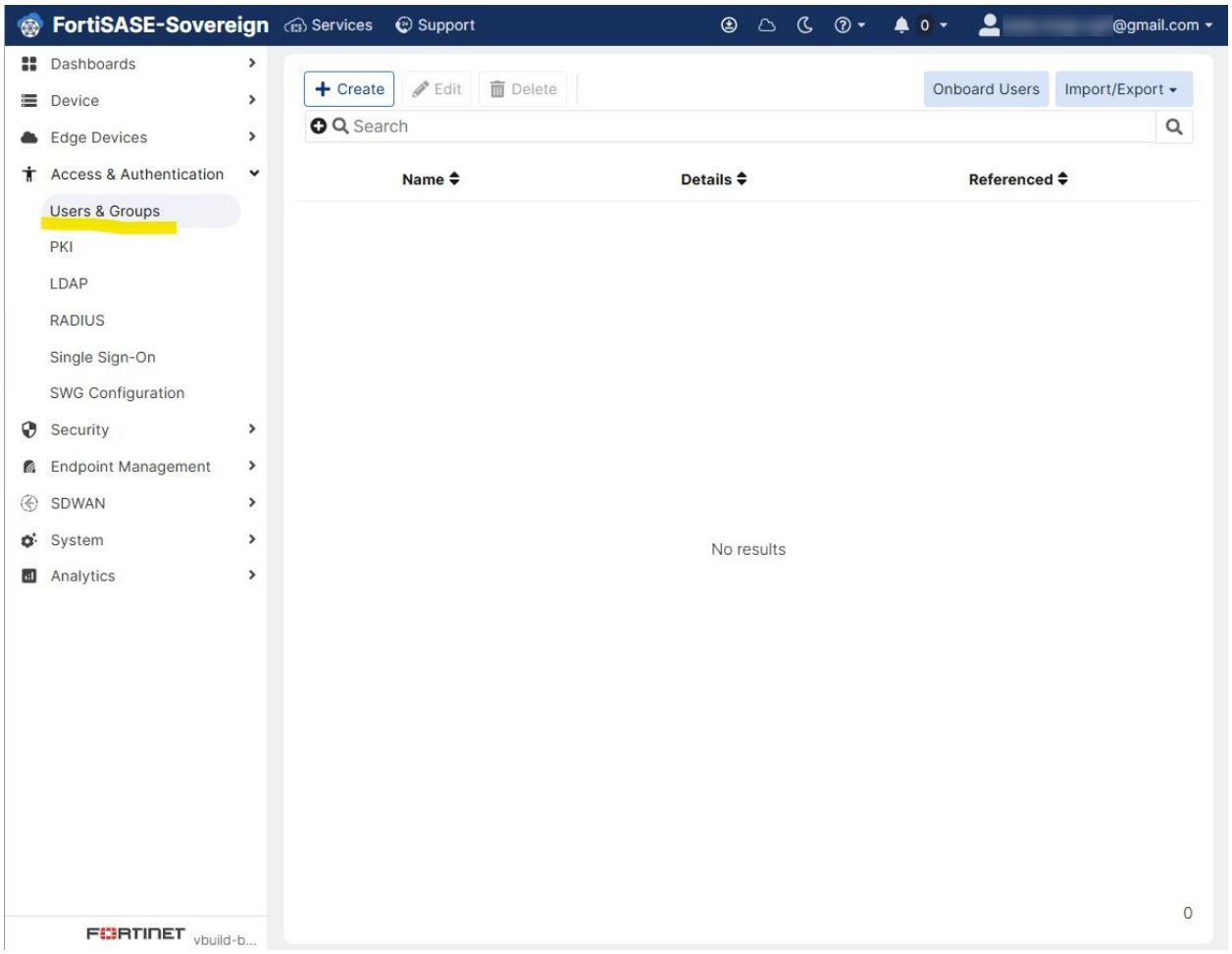


1. VPN, SWG, and Thin Edge user traffic is directed to the PoP FortiGate through the ingress (WAN1) port.
2. The PoP FortiGate inspects all user traffic before forwarding it to the destination.
3. Traffic destined for the Internet is forwarded out through WAN2.
4. Traffic destined for private data center resources is routed through the SPA overlay network.

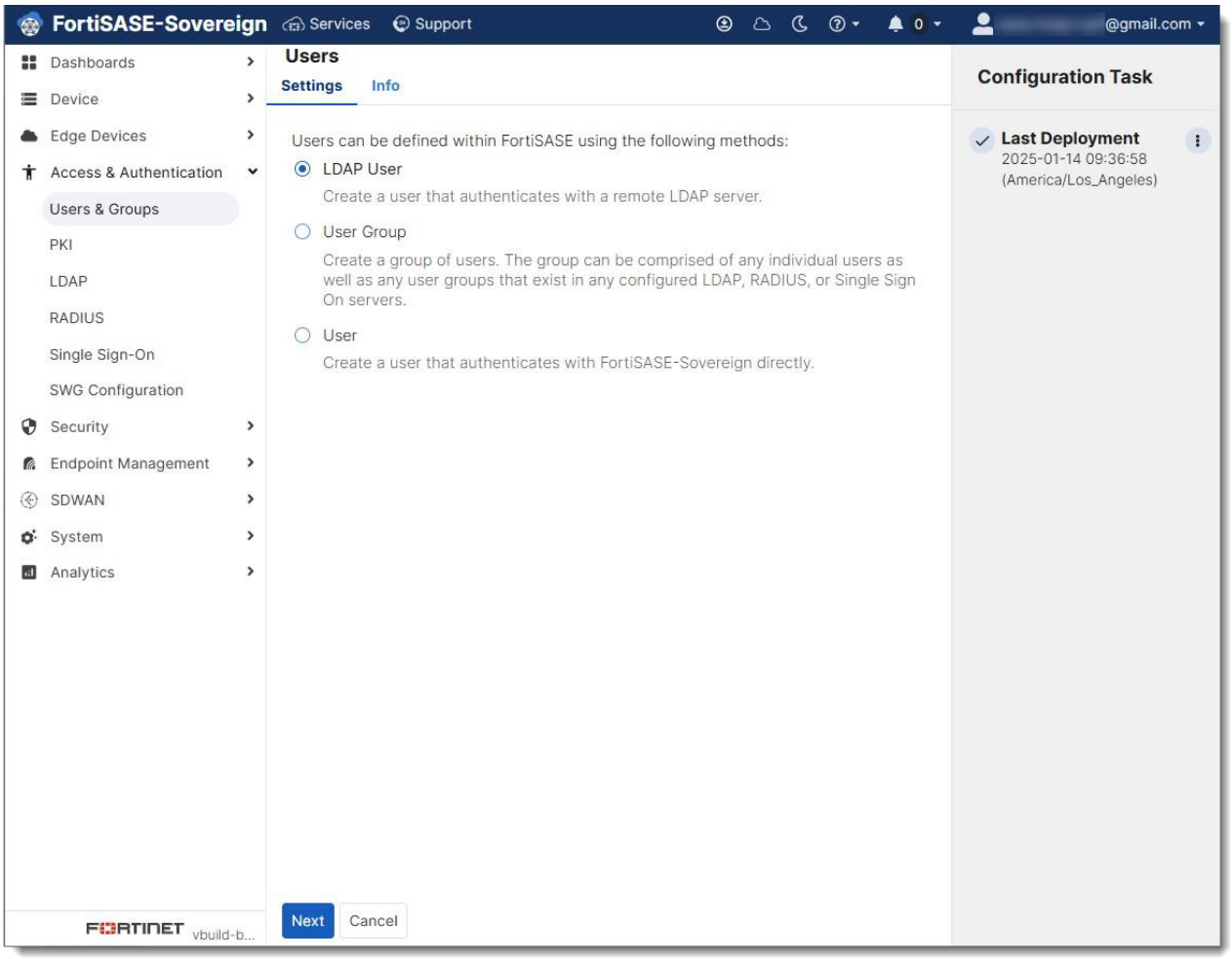
Manage Users and User Groups

Create users

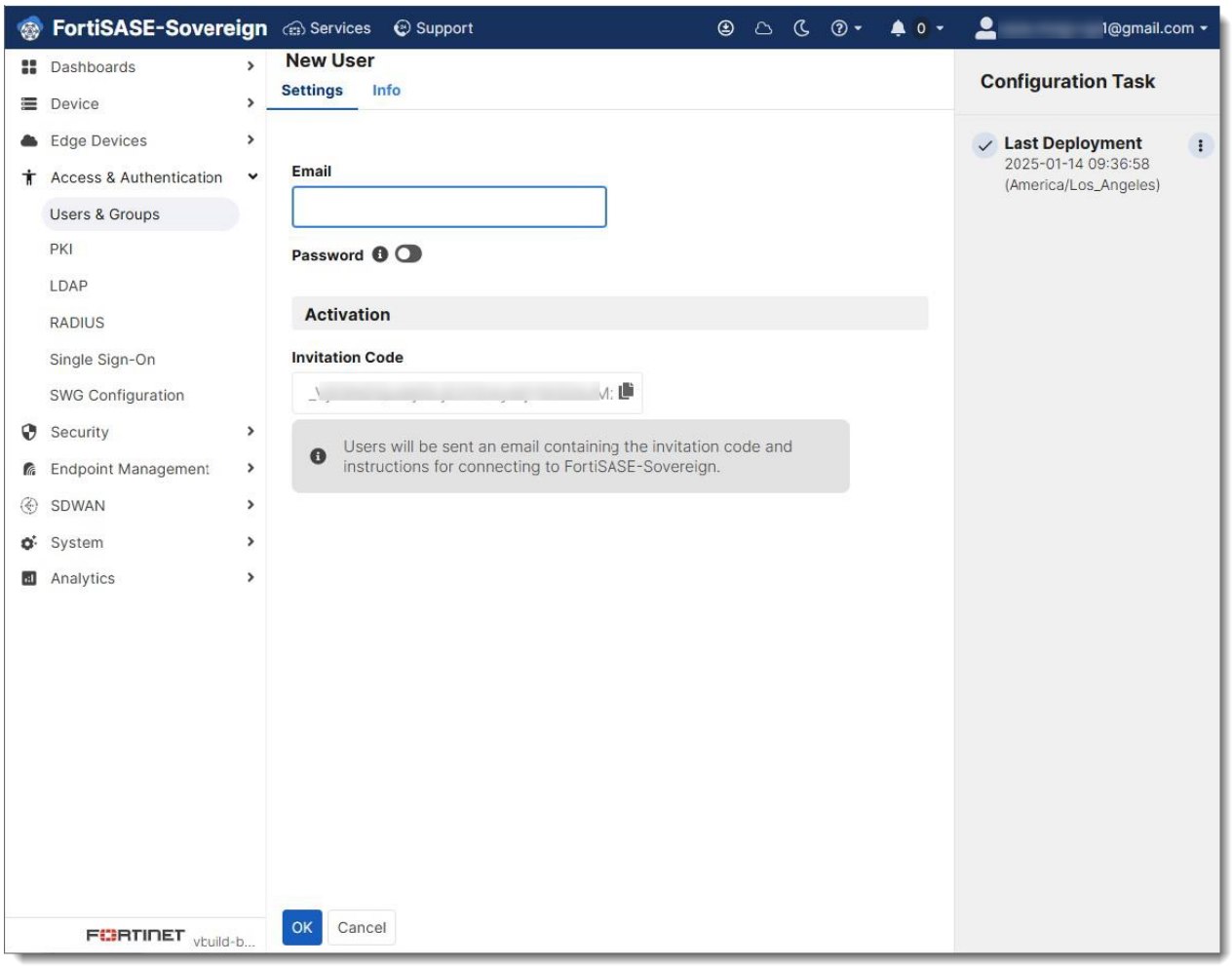
1. Go to Access & Authentication>Users & Groups.



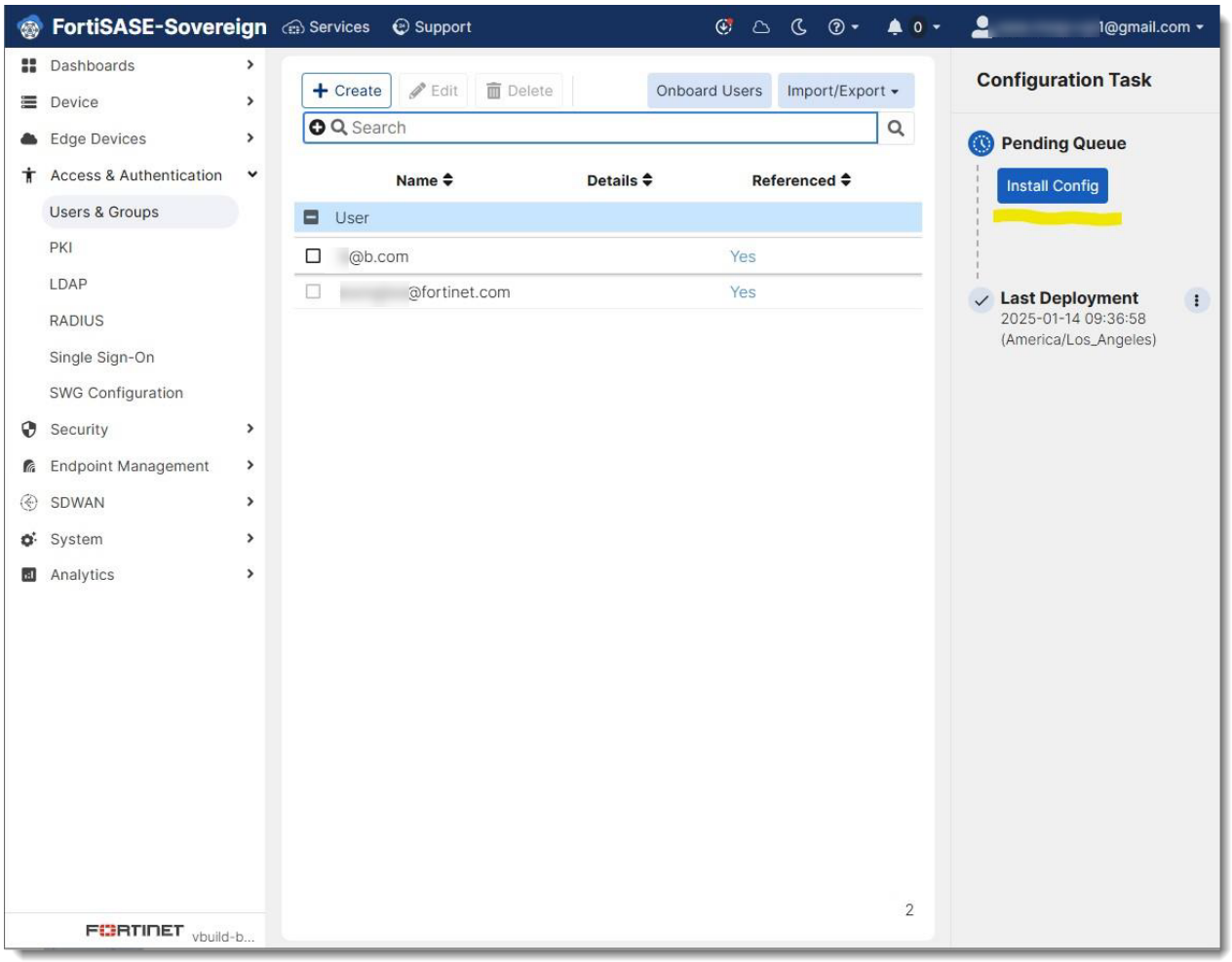
2. Click Create to create a user.



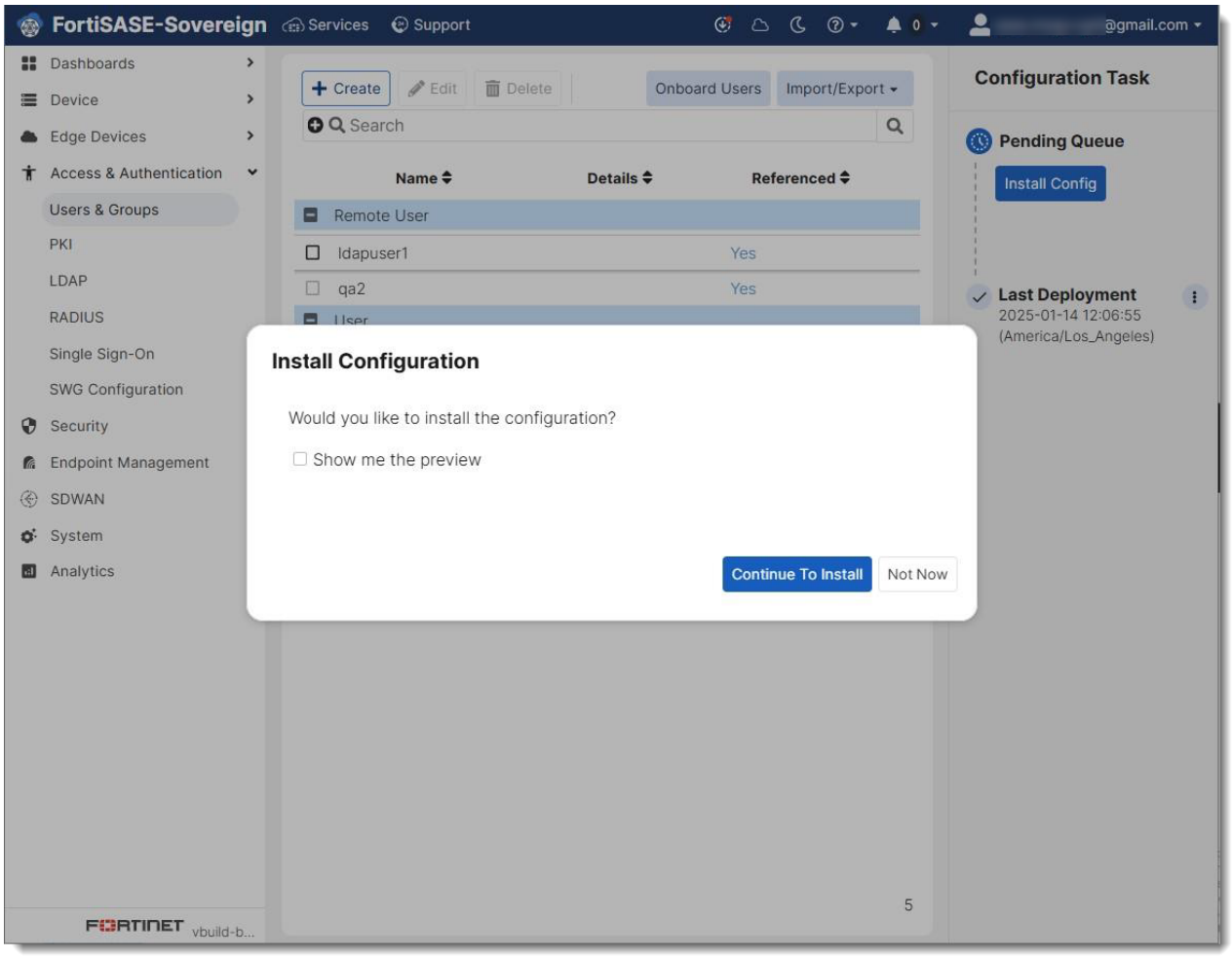
3. Select a User option, and click Next.
4. Enter the email address and password (this is a temporary password before the user is activated), and copy the invitation code for future use.



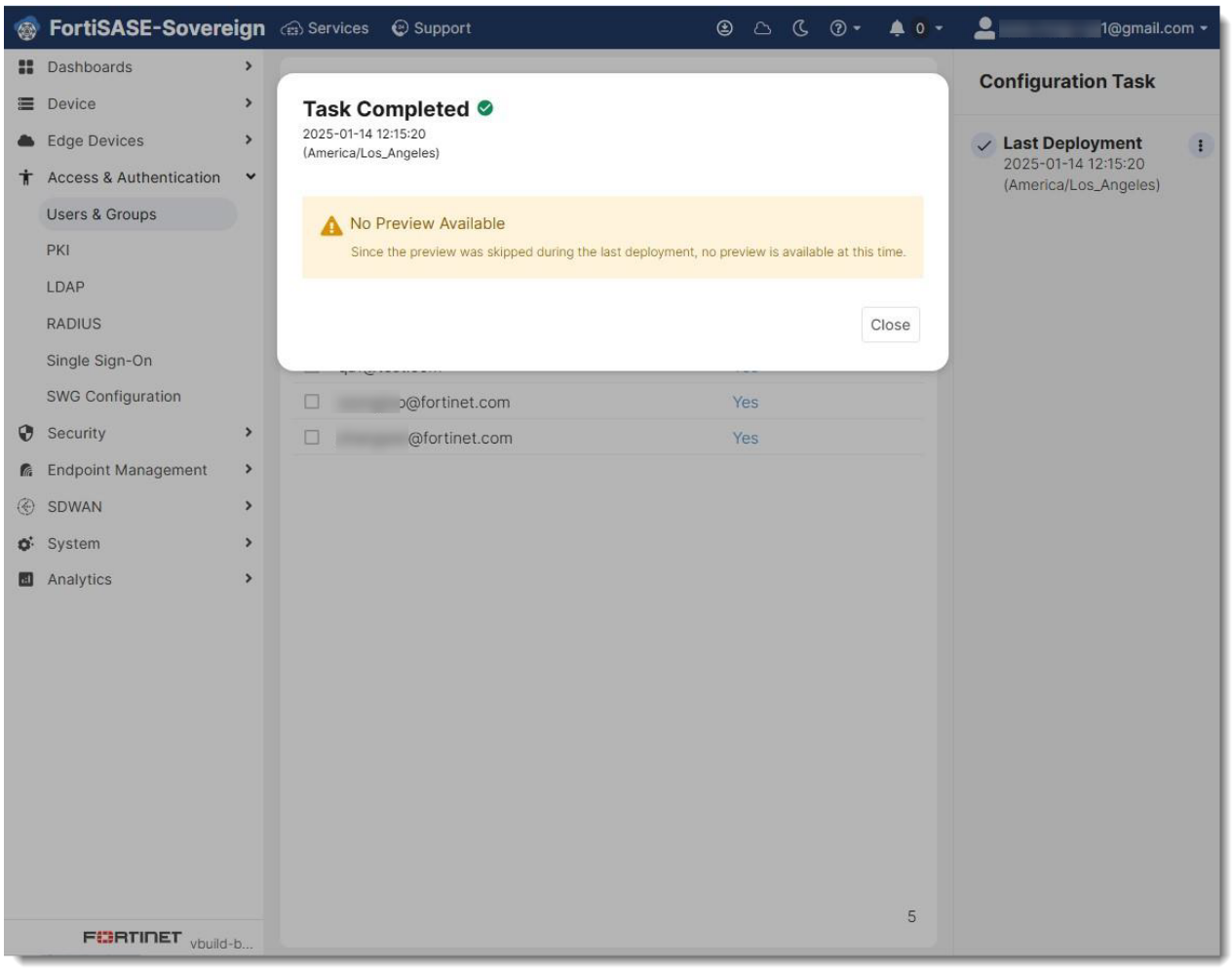
5. Click *OK*.
6. Click *Install Config* to apply the changes to the FortiGate device.



7. Preview the configuration by selecting Show me the preview during the installation.

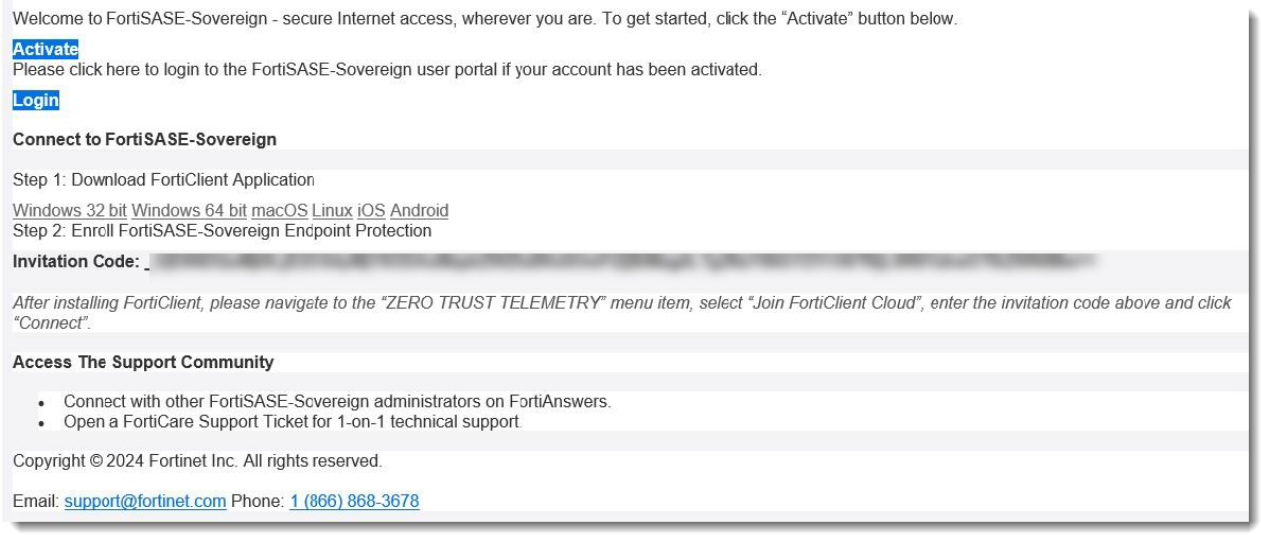


8. Click *Continue To Install*.
9. Wait until the Install Config task is completed.



10. Check your mailbox of the email account that you specified at Step 4.

By now, you should have received an email with the activation and login links and invitation code, as shown in the following screenshot.



Welcome to FortiSASE-Sovereign - secure Internet access, wherever you are. To get started, click the "Activate" button below.

Activate

Please click here to login to the FortiSASE-Sovereign user portal if your account has been activated.

Login

Connect to FortiSASE-Sovereign

Step 1: Download FortiClient Application

Windows 32 bit Windows 64 bit macOS Linux iOS Android

Step 2: Enroll FortiSASE-Sovereign Endpoint Protection

Invitation Code: _

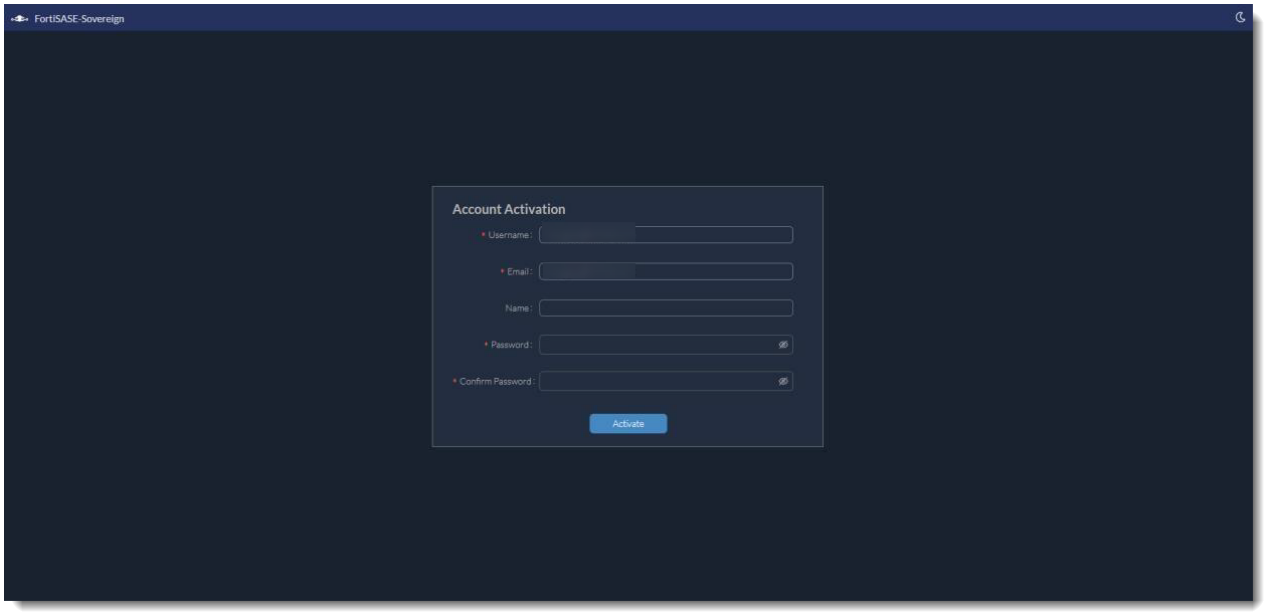
After installing FortiClient, please navigate to the "ZERO TRUST TELEMETRY" menu item, select "Join FortiClient Cloud", enter the invitation code above and click "Connect".

Access The Support Community

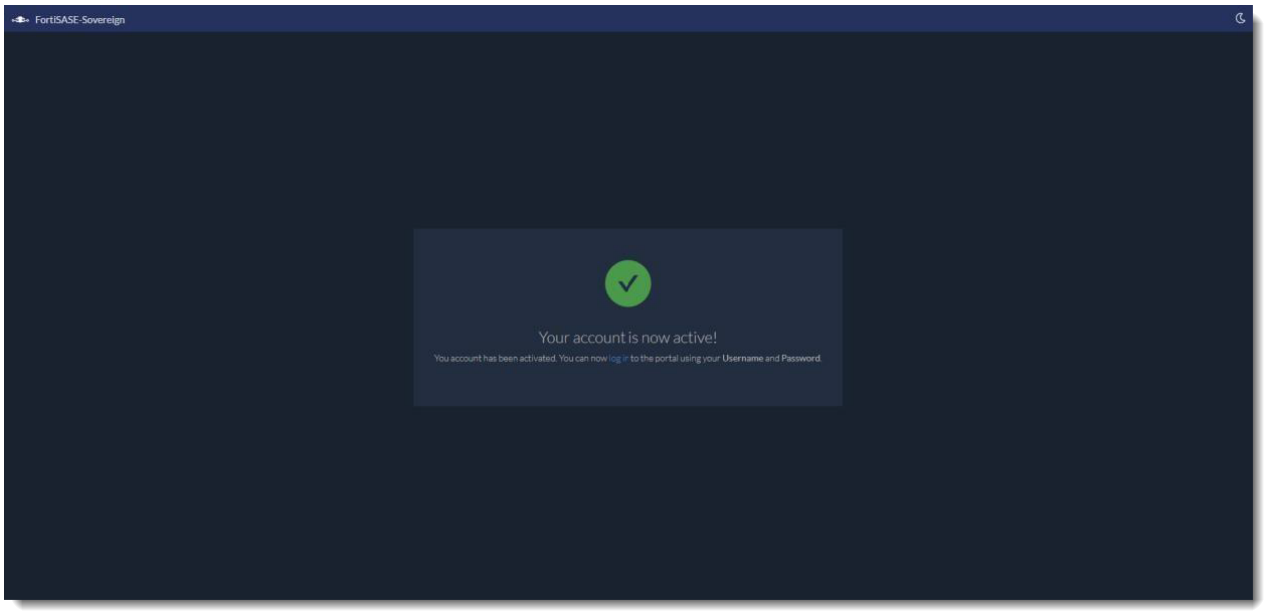
- Connect with other FortiSASE-Sovereign administrators on FortiAnswers.
- Open a FortiCare Support Ticket for 1-on-1 technical support.

Email: support@fortinet.com Phone: 1 (866) 868-3678

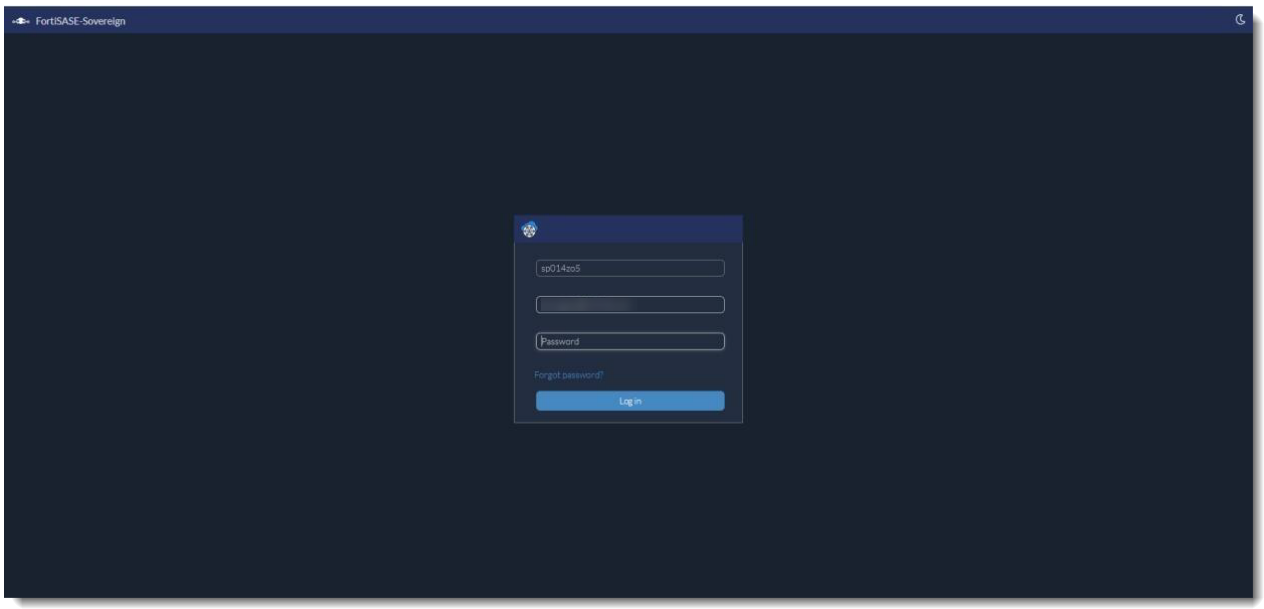
11. Click Activate link. The Account Activation page opens.



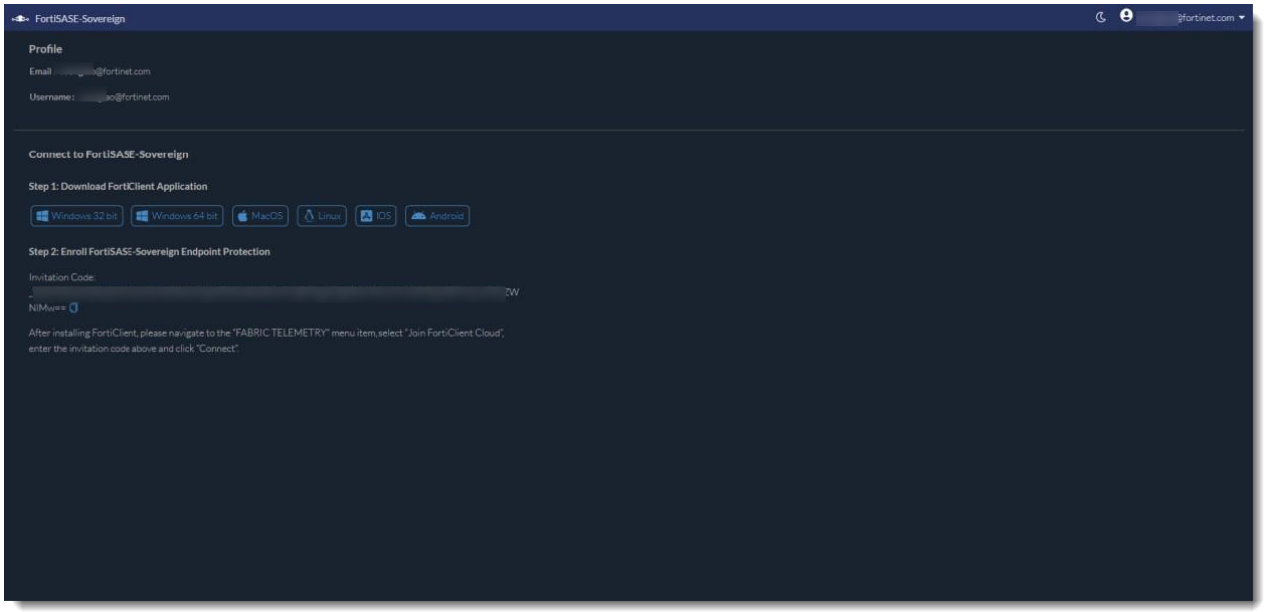
12. Enter and confirm new password, and click Activate.



13. Click Login or the link in the email to log in with the new password.



14. Click Login. Upon successful login, the following page opens.



15. Download and install the FortiClient compatible with the OS on your client. For more information, see FortiOS and FortiAnalyzer for FortiSASE-Sovereign on page 10.

Now you should be able to use your new credentials to log in with your IPSec VPN login or SSL VPN

login using the procedures outlined in the following paragraphs.

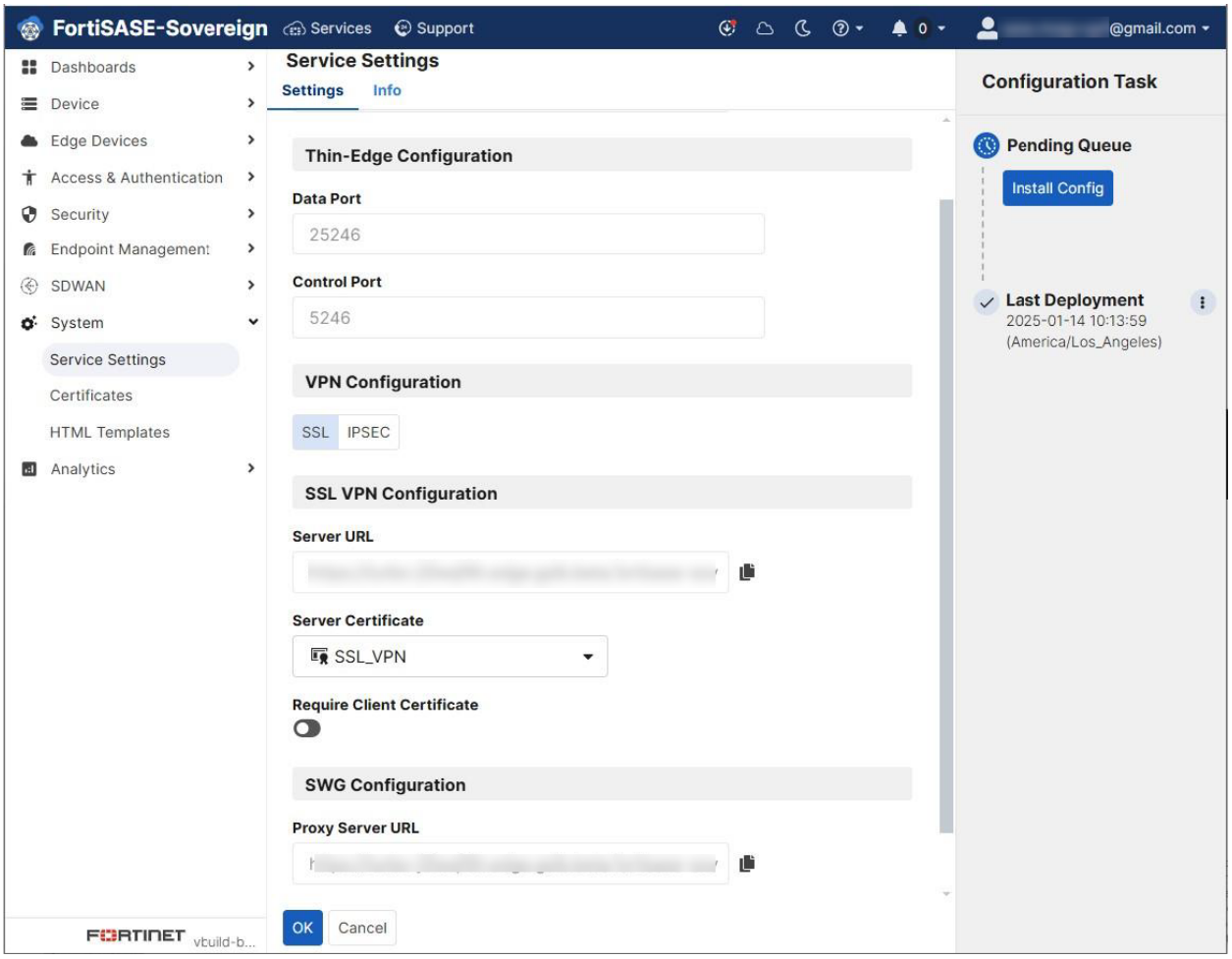
Install FortiClient (Windows 64 bit)

1. Click Windows 64 bit at Step 15 mentioned in the previous paragraph.
2. Make sure that the FortiClient installer has been downloaded.
3. Click FortiClient.msi in the installer.
4. Complete the FortiClient installation.

Log in using SSL VPN

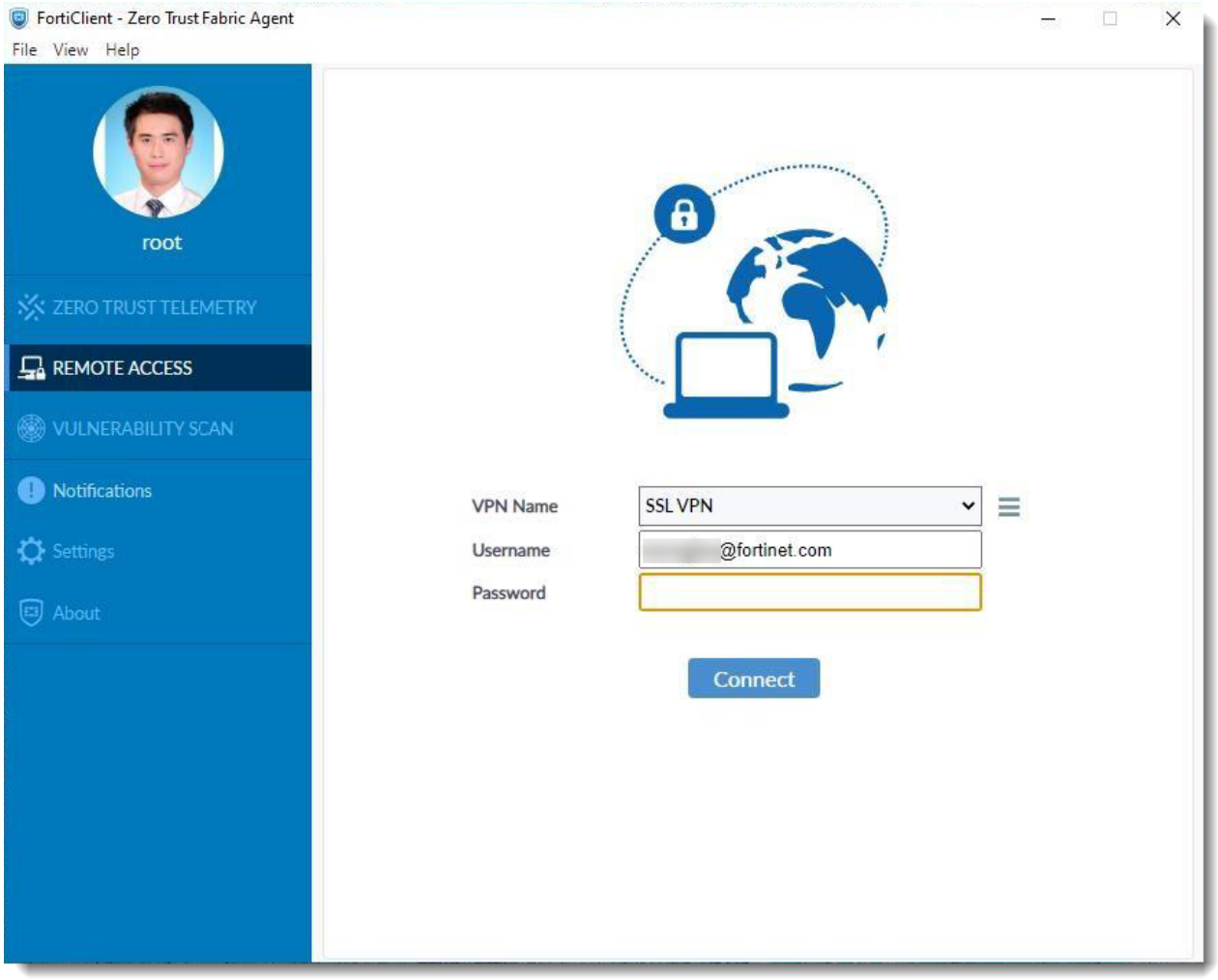
The following instructions assume that you are on IPsec VPN and would like to switch to SSL VPN.

1. On the FortiSASE-Sovereign portal, select System > Service Settings.



2. Click SSL under VPN Configuration.
3. Click OK.
4. Click Install Config in the right panel to push the configuration change to the FortiGate device.
5. After Install Config task is completed, start a Windows PC.
6. Open FortiClient.

7. Select REMOTE ACCESS. The VPN Name should have changed to SSL VPN, as shown on the following screenshot.



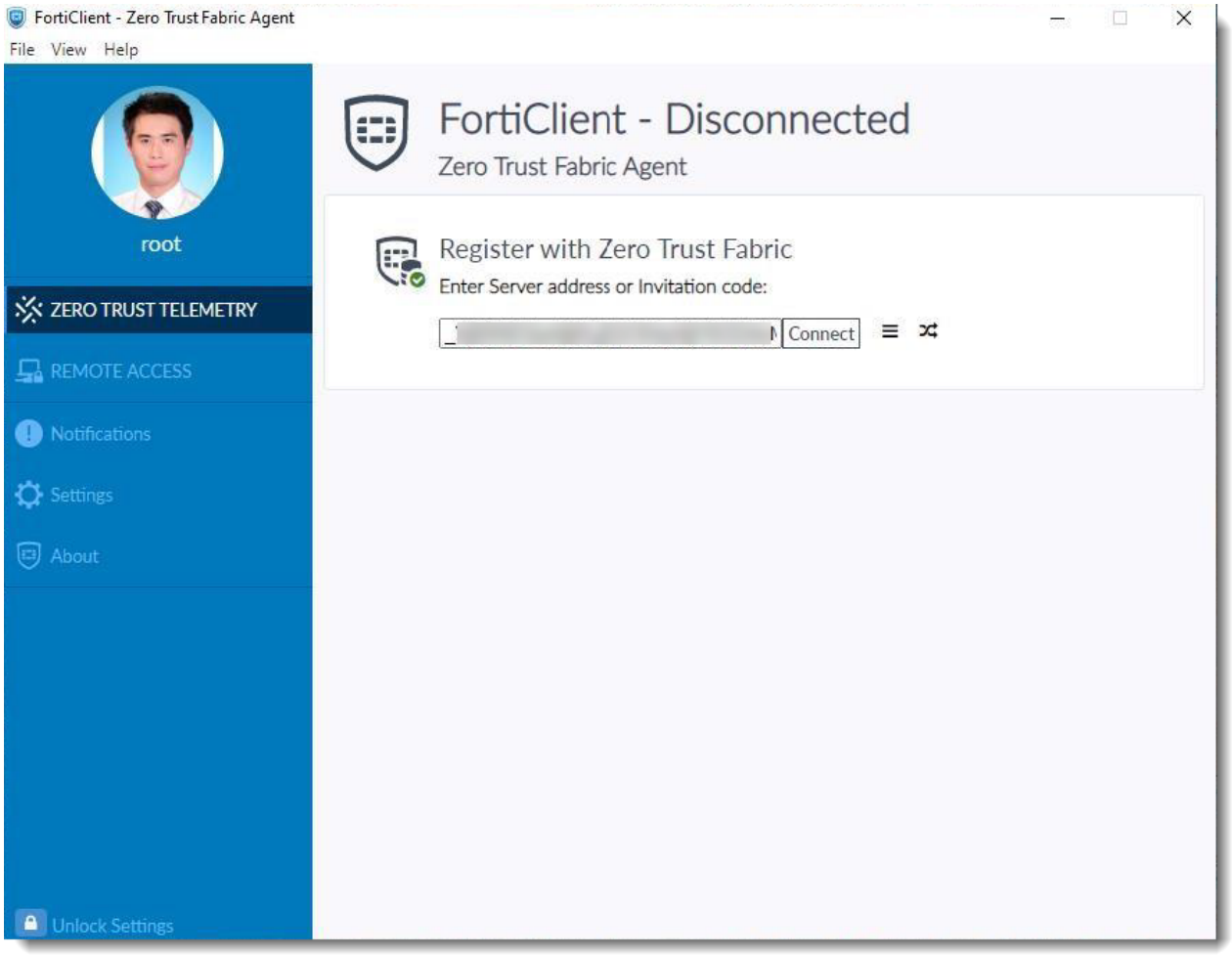
8. Enter your username and password, and click Connect.
9. Open some web pages to check if Bytes Received and Bytes Sent are changing constantly.

If your SSL VPN login is successful, you should see Bytes Received and Bytes Sent are changing.

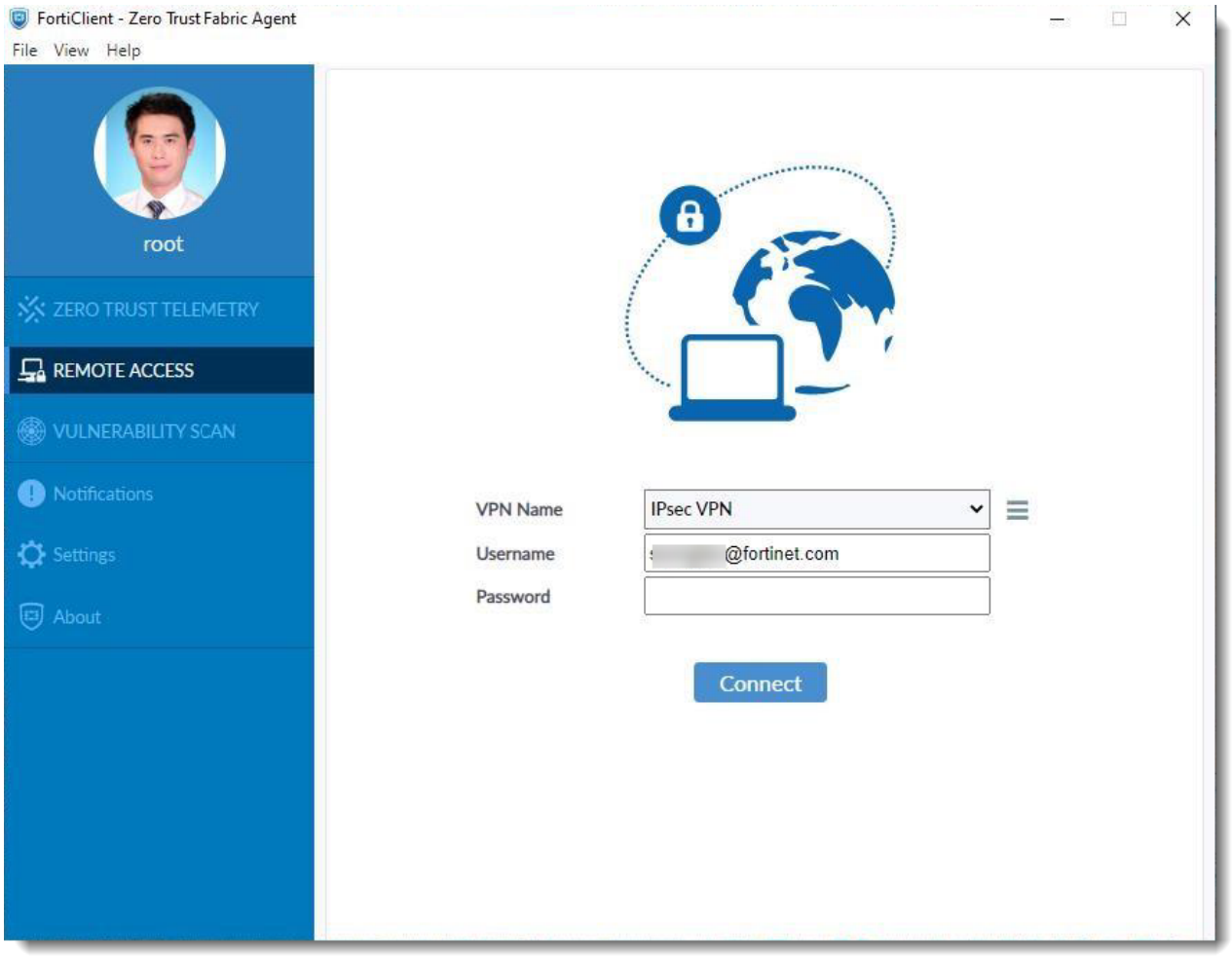
Log in using IPsec VPN

IPSec VPN is the default on the FortiSASE-Sovereign portal.

1. Start your Windows PC.
2. Open FortiClient.
3. Enter the invitation code which appears in Step 10 in Create users on page 93 to connect to the FortiClient EMS.

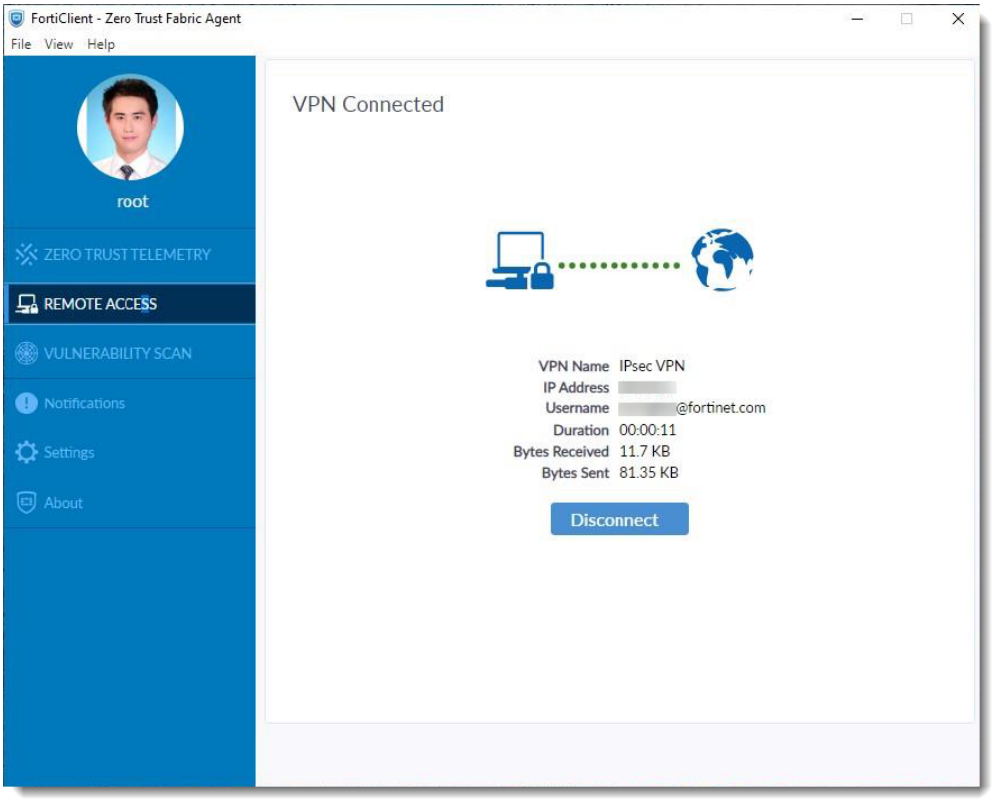


4. Click REMOTE ACCESS.



5. Enter your username and password, and click Connect.

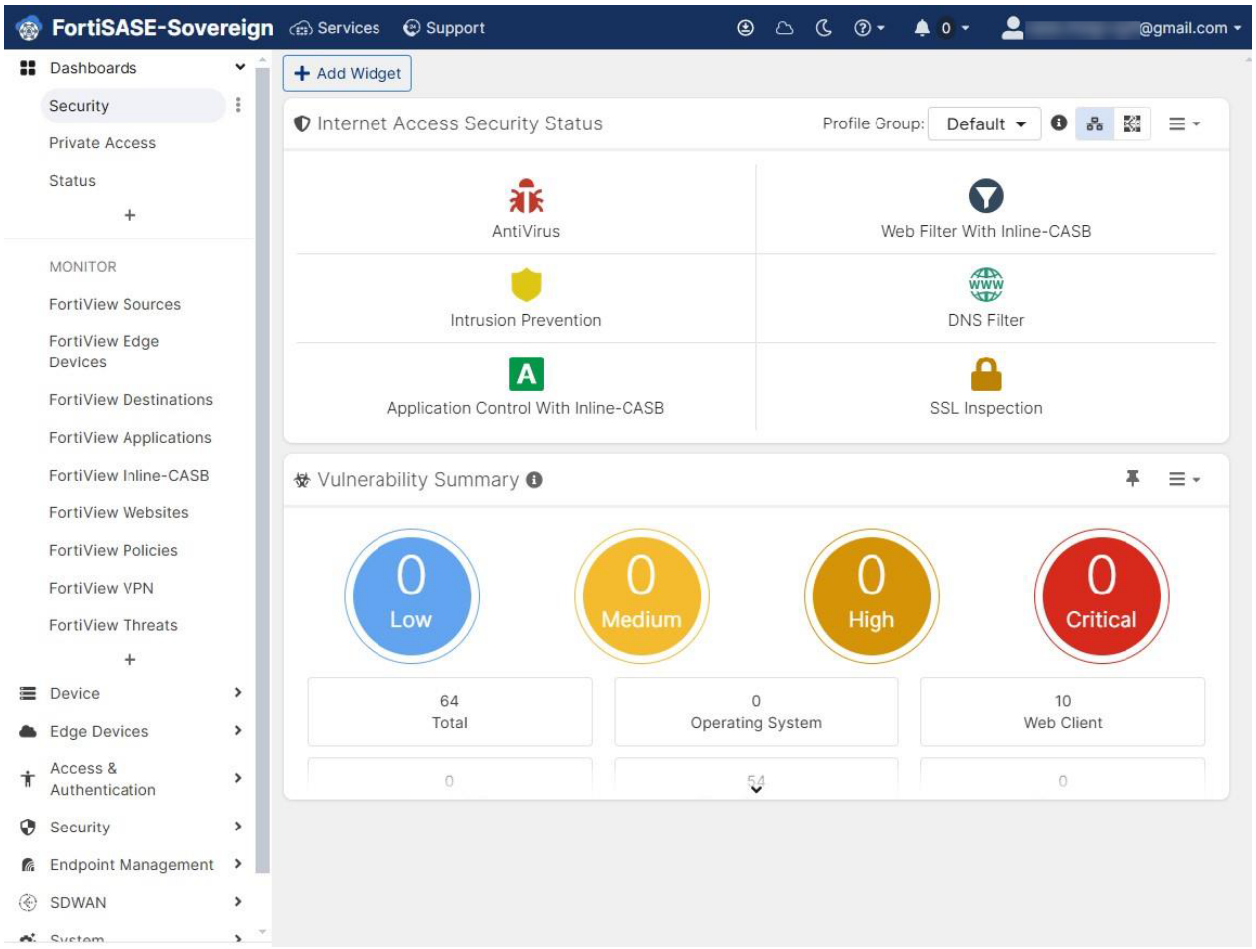
If your login is successful, you should see the page similar to the one shown in the following screenshot.



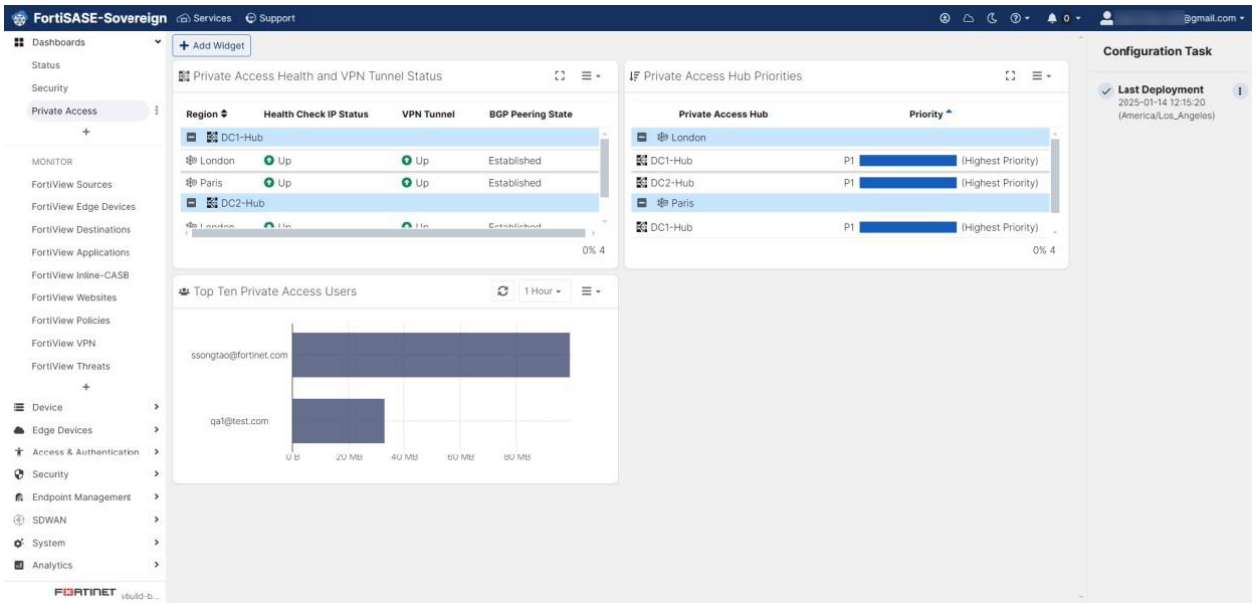
6. Open some web pages to check if Bytes Received and Bytes Sent are changing constantly.

Overview of Dashboard

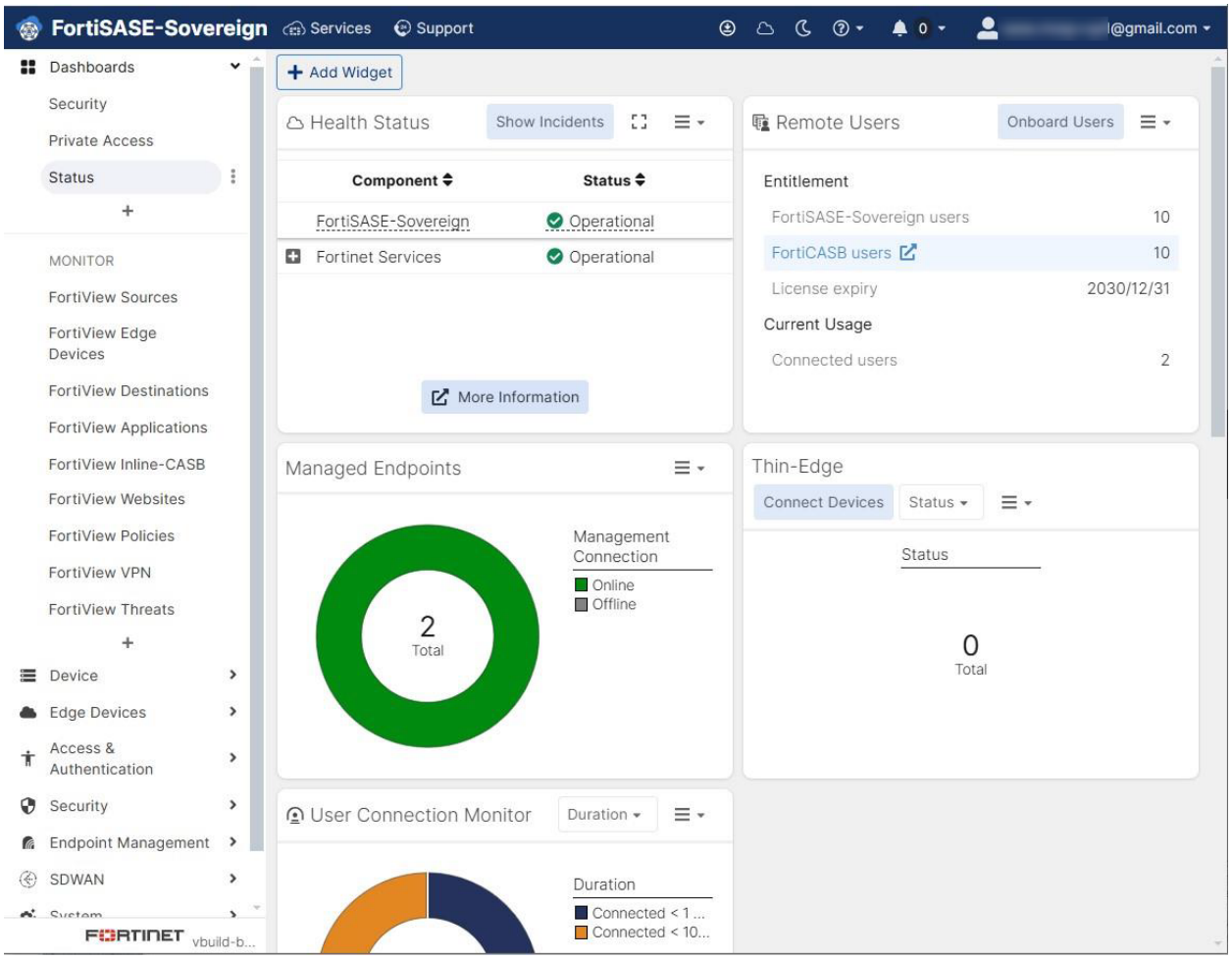
Security


FortiSASE-Sovereign
Services
Support
0
@gmail.com
Dashboards
Security
Private Access
Status
MONITOR
FortiView Sources
FortiView Edge Devices
FortiView Destinations
FortiView Applications
FortiView Inline-CASB
FortiView Websites
FortiView Policies
FortiView VPN
FortiView Threats
Device
Edge Devices
Access & Authentication
Security
Endpoint Management
SDWAN
Add Widget
Internet Access Security Status
Profile Group:
Default
AntiVirus
Web Filter With Inline-CASB
Intrusion Prevention
DNS Filter
Application Control With Inline-CASB
SSL Inspection
Vulnerability Summary
0
Low
0
Medium
0
High
0
Critical
64
Total
0
Operating System
10
Web Client

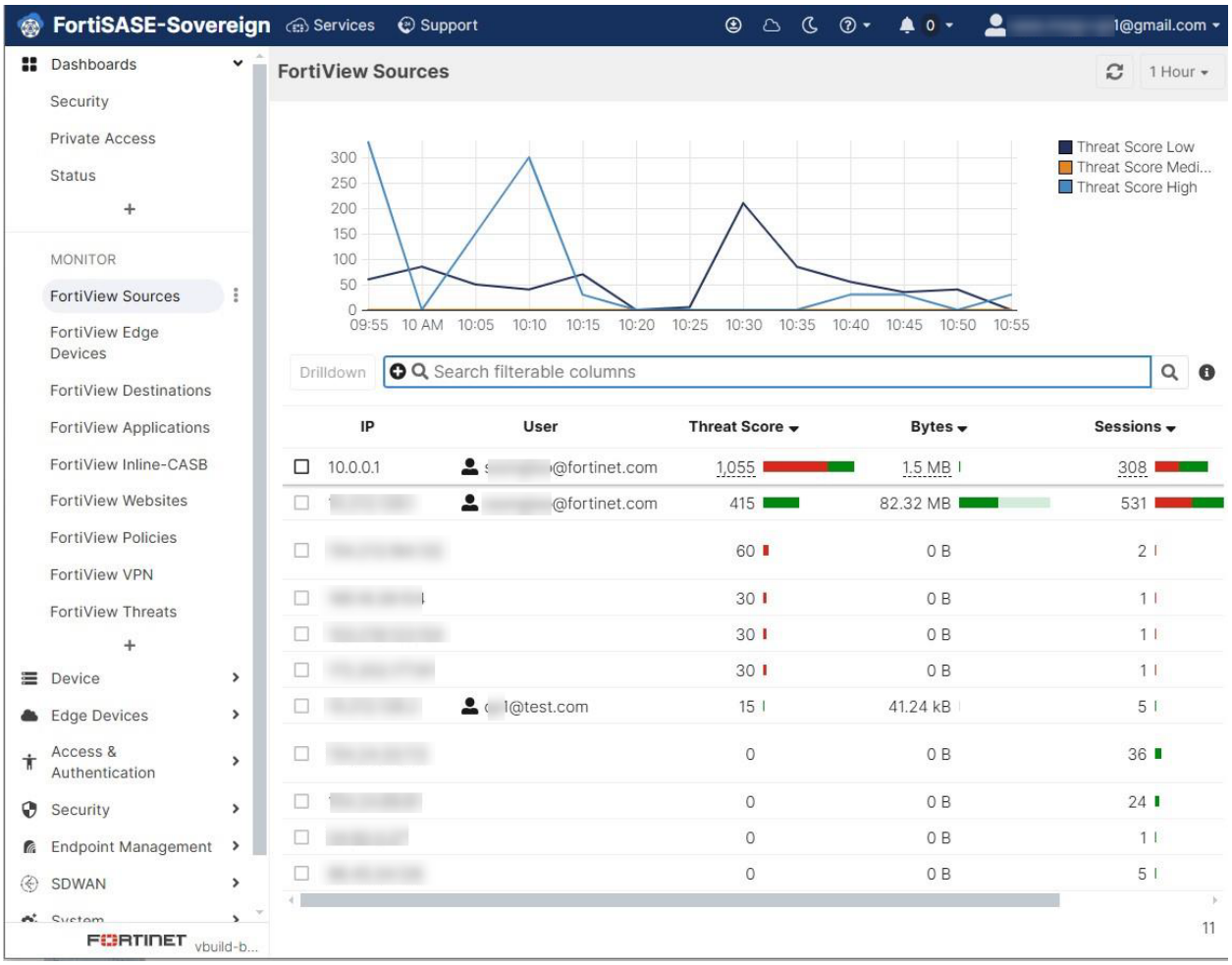
Private Access



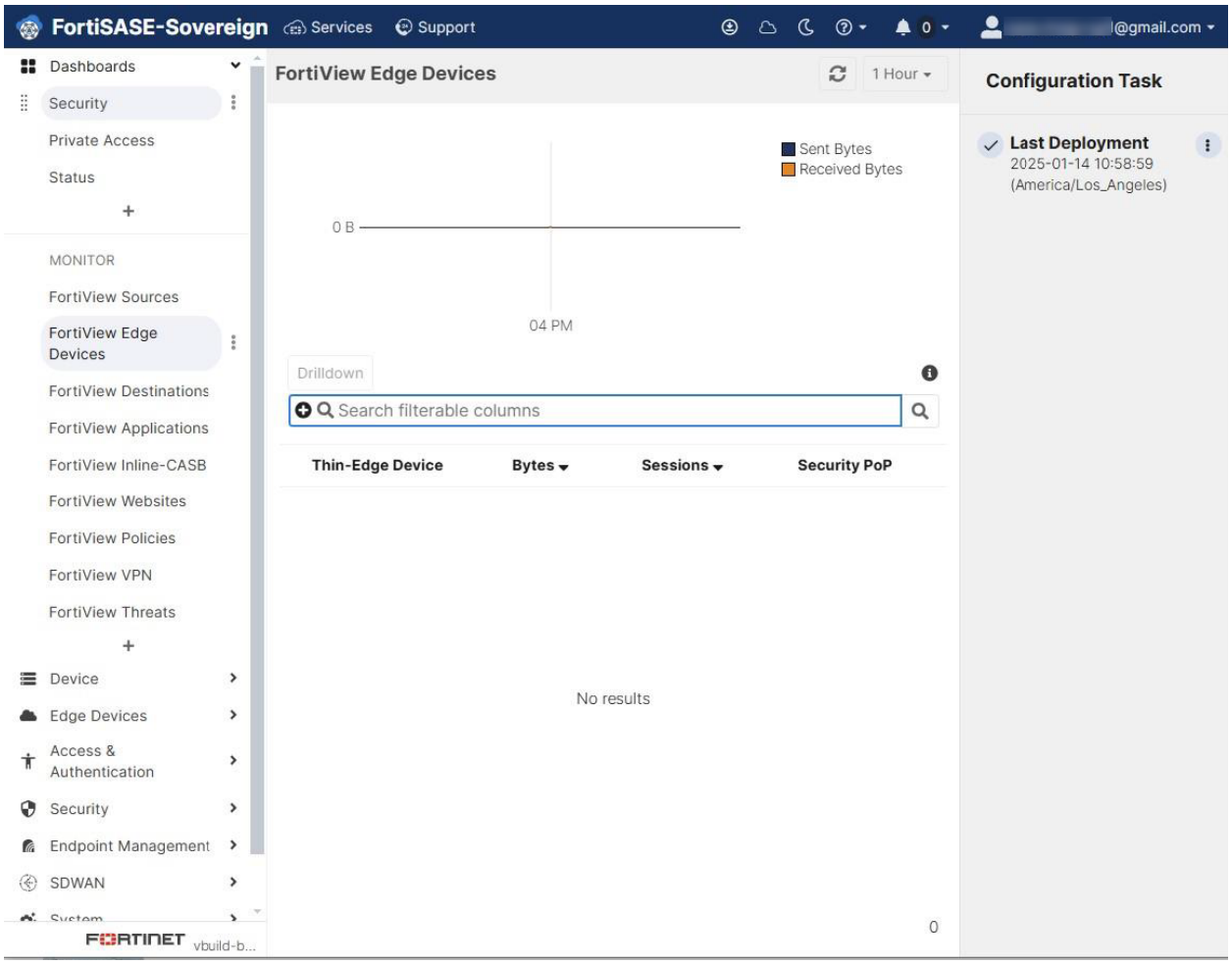
Status


FortiSASE-Sovereign
Services
Support
0
@gmail.com
Dashboards
Security
Private Access
Status
MONITOR
FortiView Sources
FortiView Edge Devices
FortiView Destinations
FortiView Applications
FortiView Inline-CASB
FortiView Websites
FortiView Policies
FortiView VPN
FortiView Threats
Device
Edge Devices
Access & Authentication
Security
Endpoint Management
SDWAN
Add Widget
Health Status
Show Incidents
Component
Status
FortiSASE-Sovereign
Operational
Fortinet Services
Operational
More Information
Remote Users
Onboard Users
Entitlement
FortiSASE-Sovereign users
10
FortiCASB users
10
License expiry
2030/12/31
Current Usage
Connected users
2
Managed Endpoints
2
Total
Management Connection
Online
Offline
Thin-Edge
Connect Devices
Status
Status
0
Total
User Connection Monitor
Duration
Duration
Connected < 1 ...
Connected < 10...
FORTINET
vbuild-b...

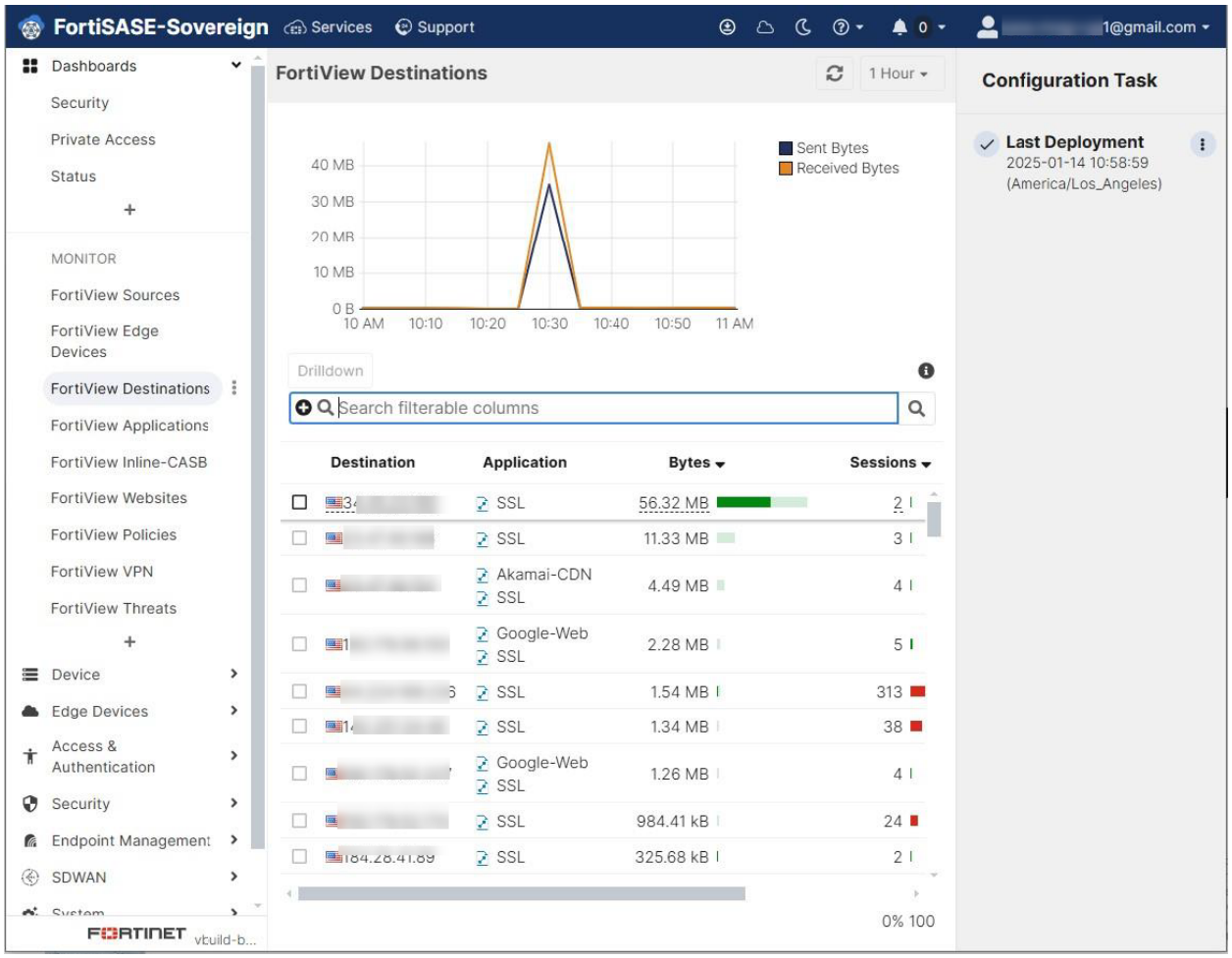
FortiView Sources



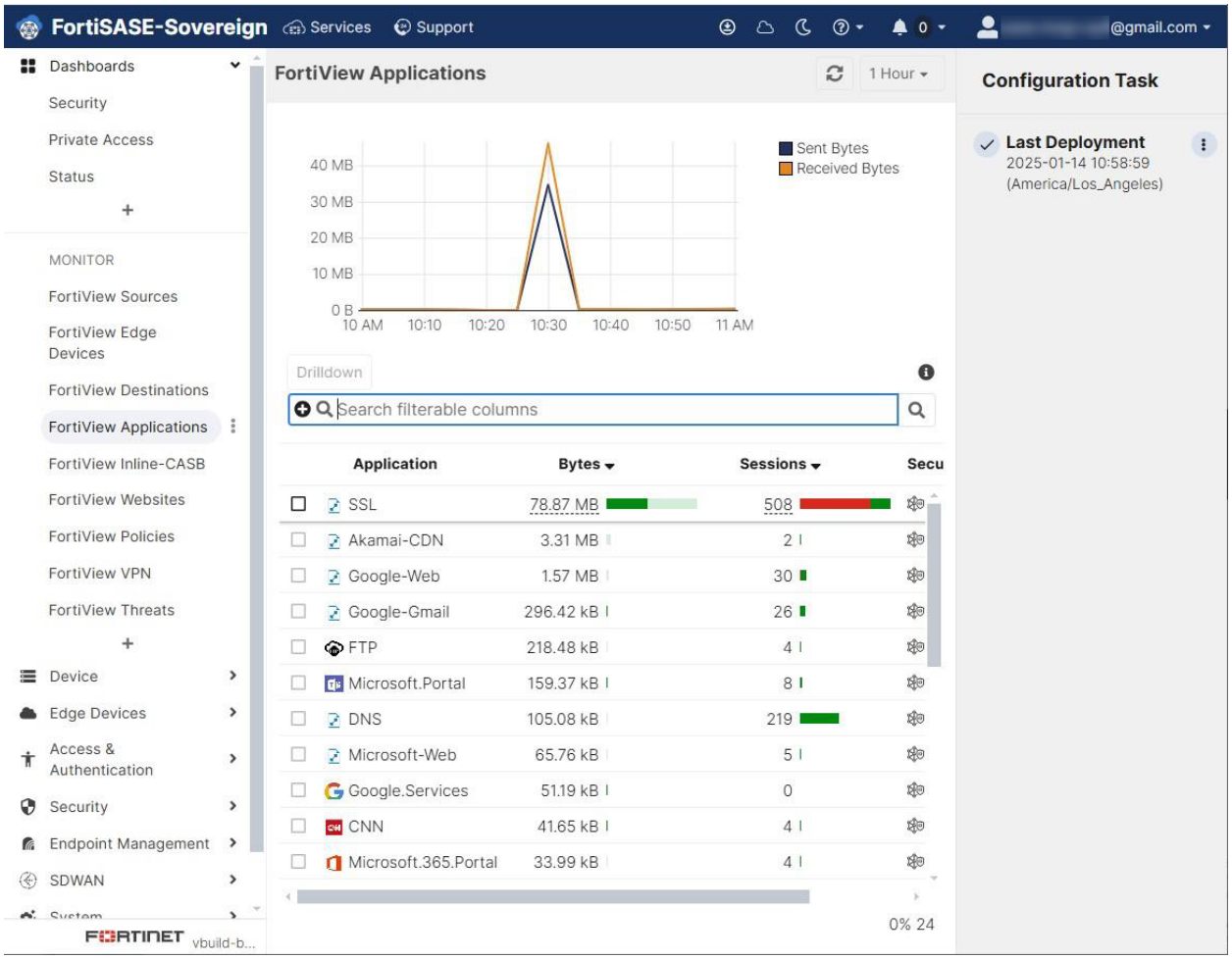
FortiView Edge Devices



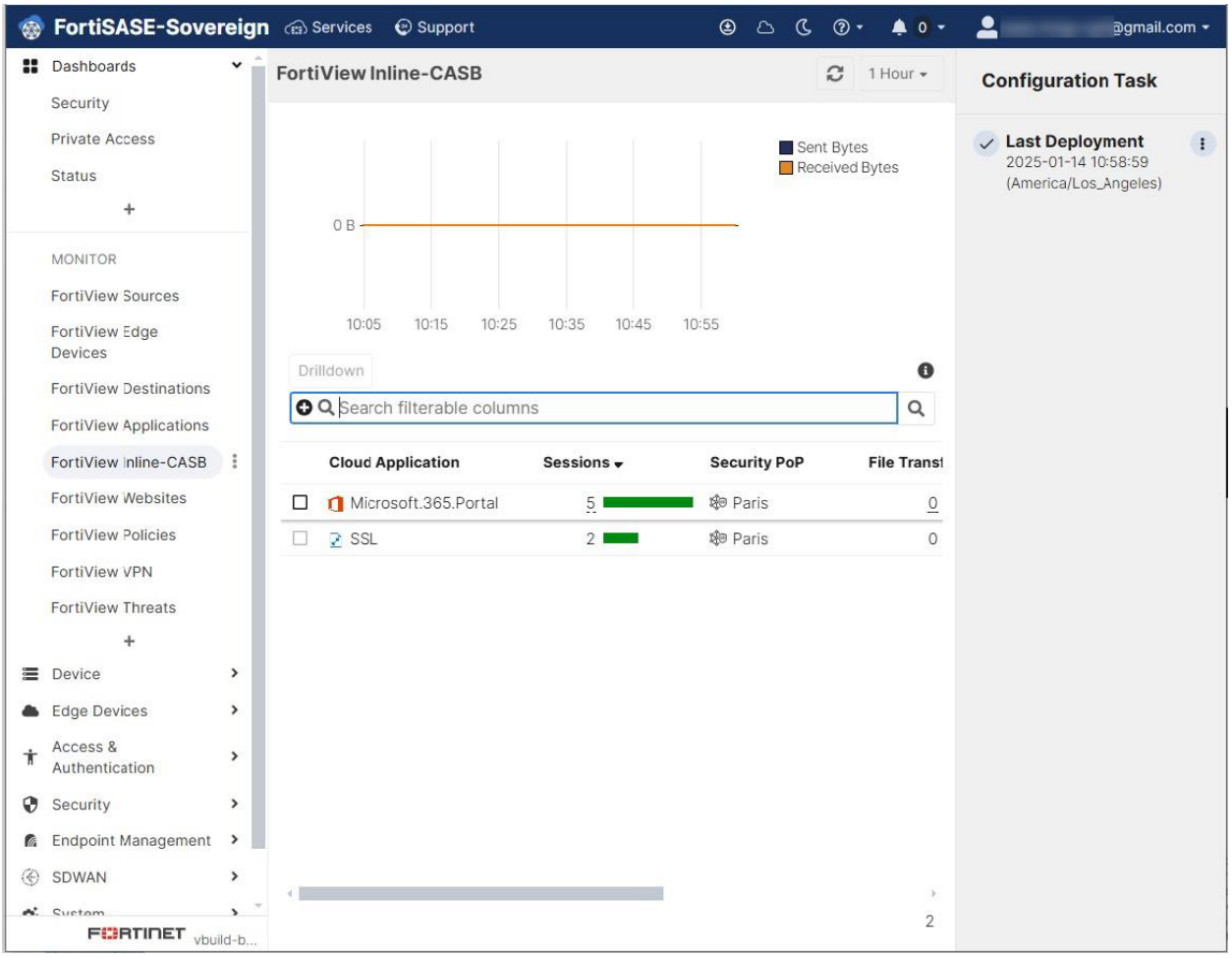
FortiView Destinations



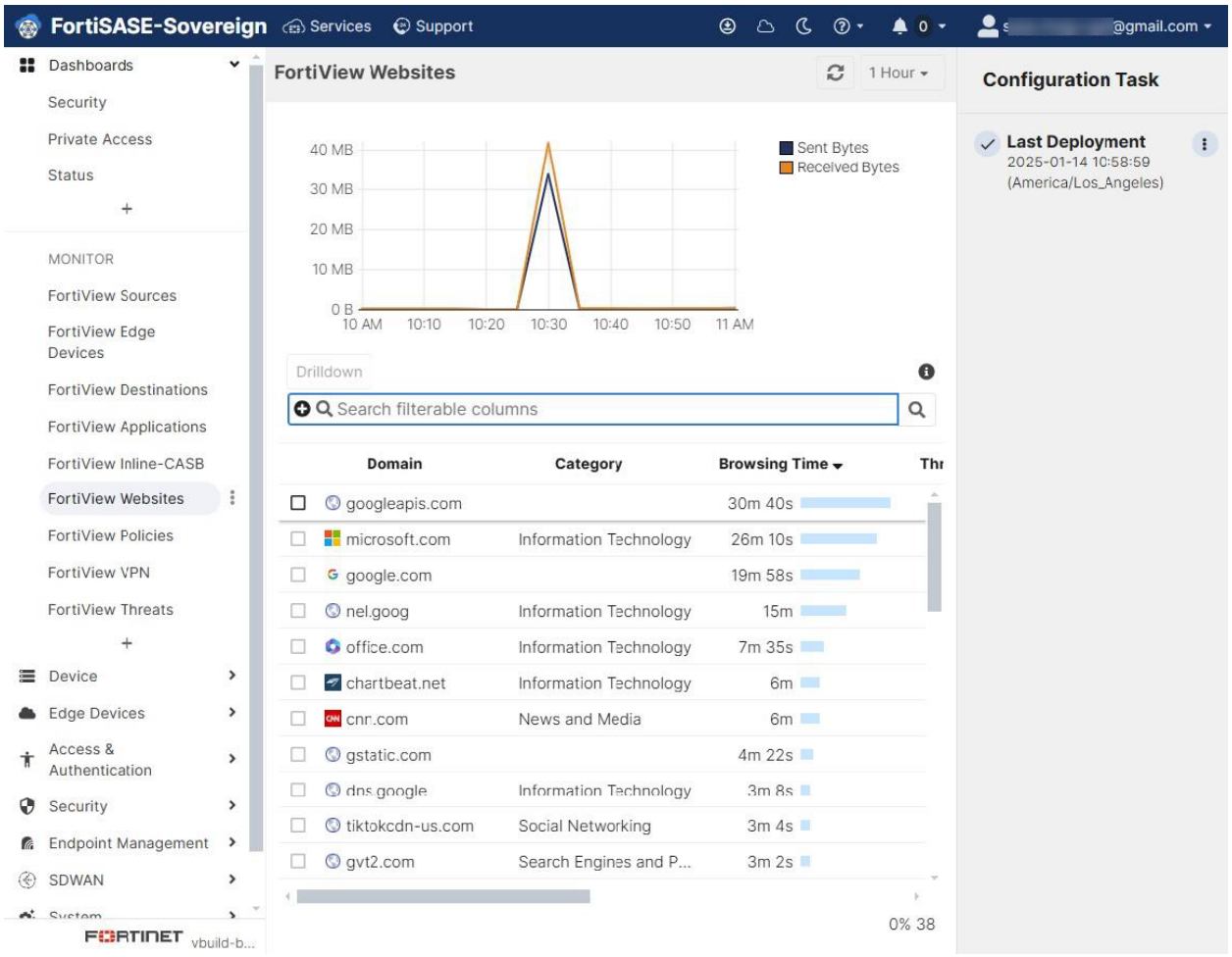
FortiView Applications



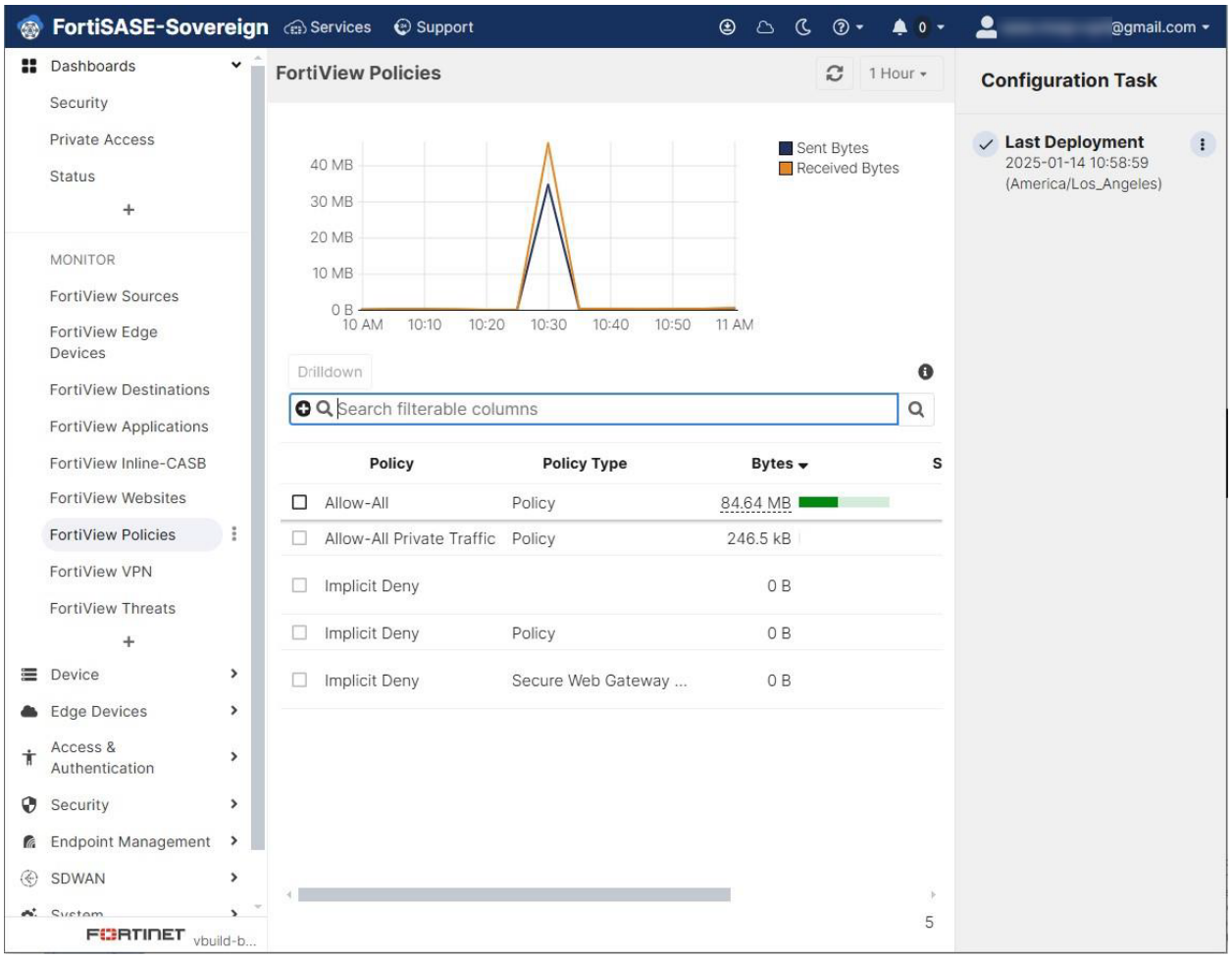
FortiView Inline-CASB



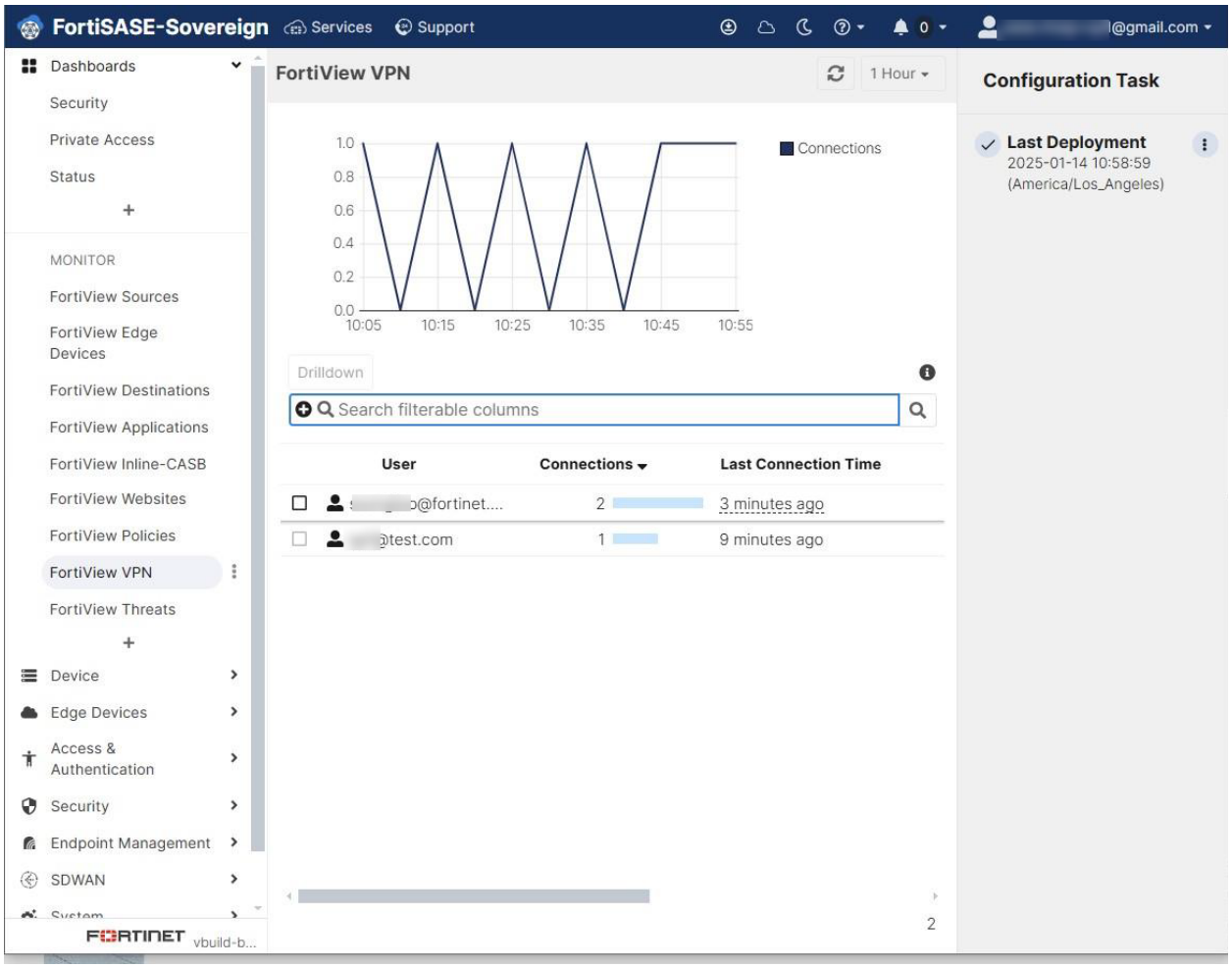
FortiView Websites



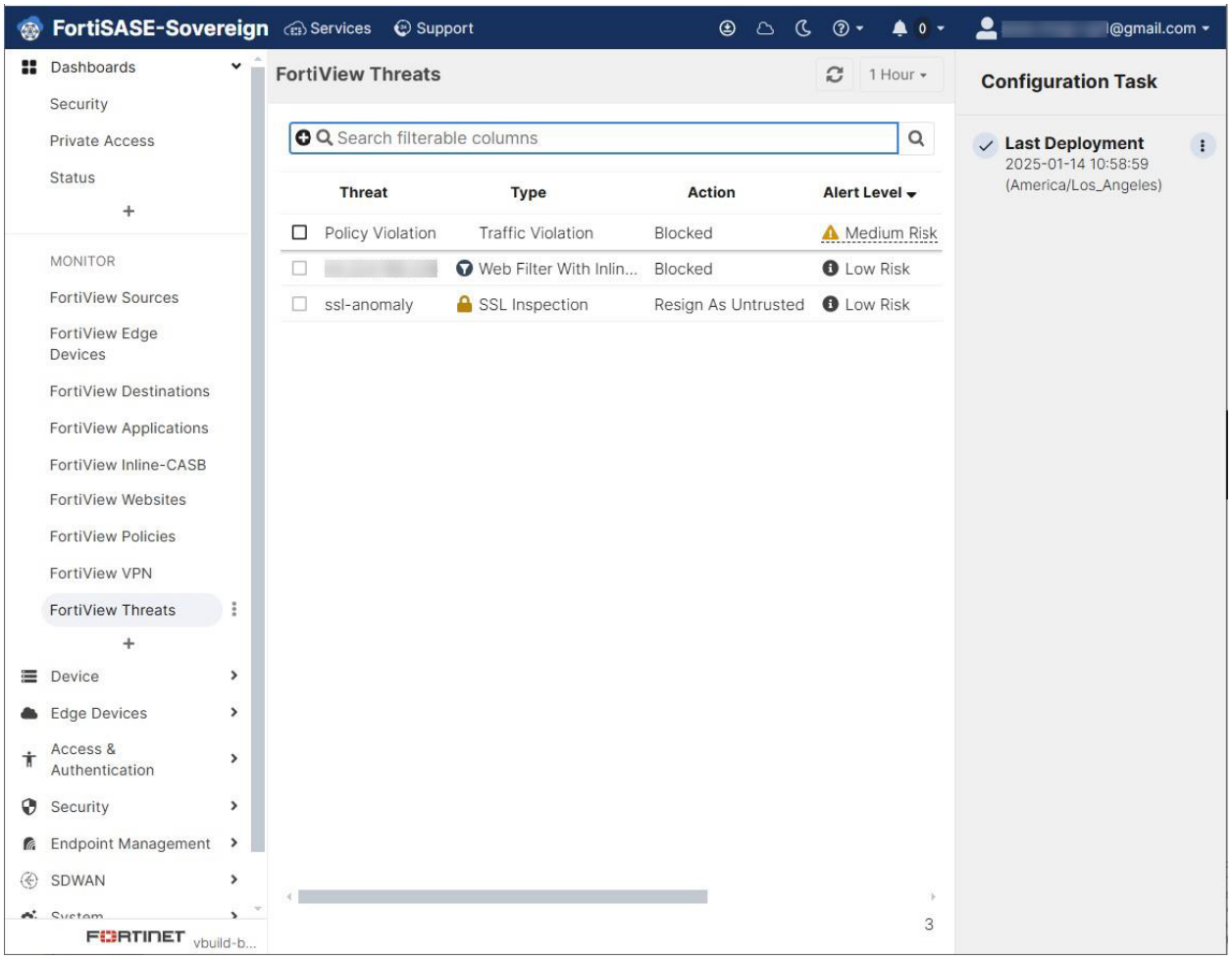
FortiView Policies



FortiView VPN



FortiView Threats



Re-deploy FortiSASE-Sovereign

Step 1: Clean up tenant

Before re-deploying FortiSASE-Sovereign, please contact FortiCare Customer Service or open a new Customer Service ticket through FortiCare Support portal to request cleanup of the original tenant.

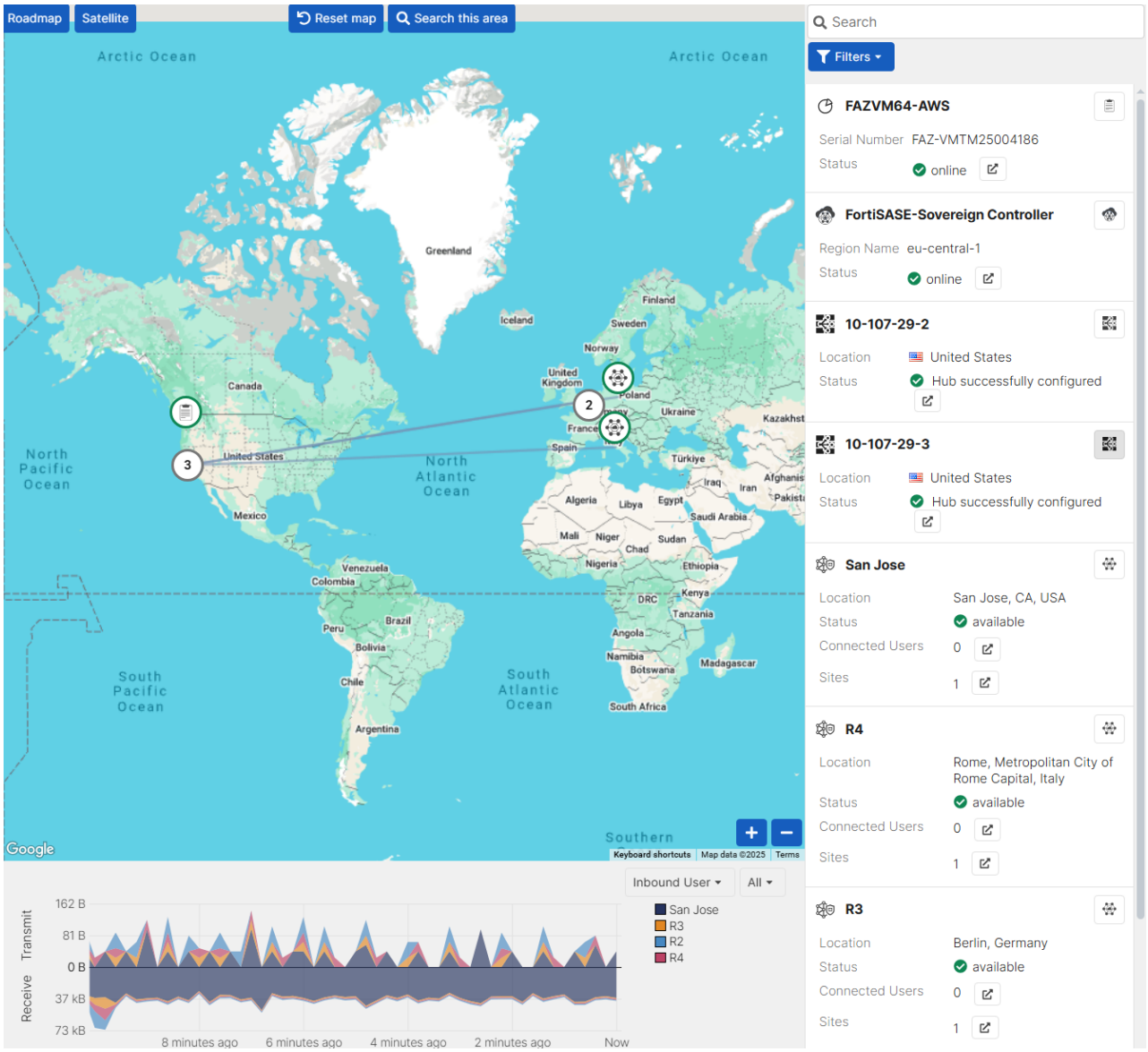
Step 2: Reset FortiAnalyzer

This step is optional.

1. Delete the managing FortiGate.
2. Re-deploy FortiAnalyzer.

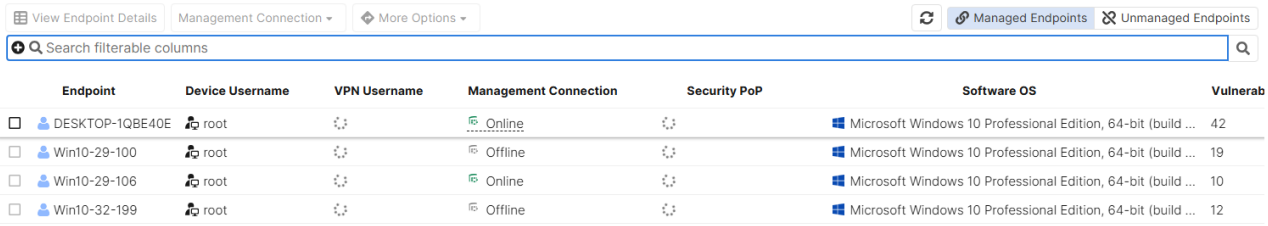
Best Practices and Recommendations

1. PoP FortiGate Initial Configuration
   - In a dual-ISP scenario, ensure that the default route through the egress port is set with higher priority than the ingress port before onboarding.
   - In a single-arm deployment (where ingress and egress share the same port), the default route must be configured through that port.
2. Device Management
   - Administrators can navigate to Device → Monitoring to view the operational status of all onboarded devices.

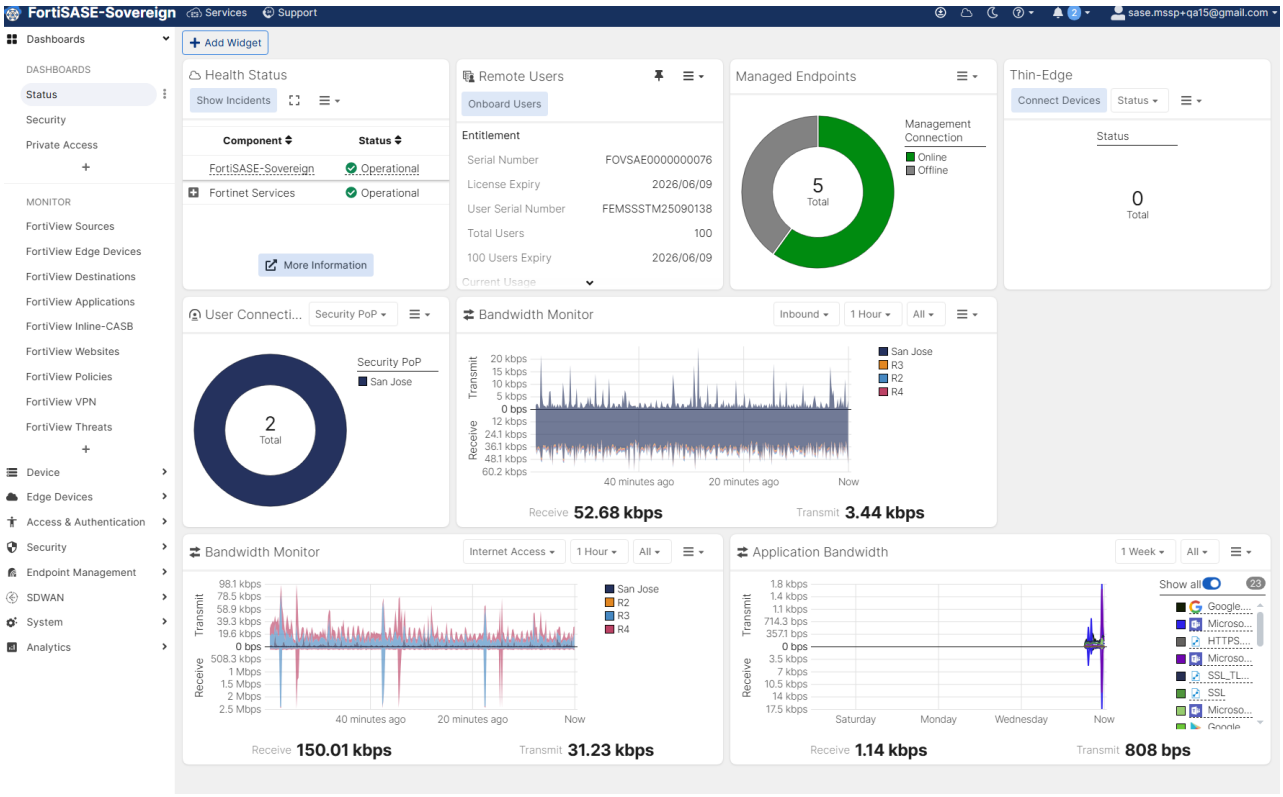


3. Endpoint and User Management

- Administrators can manage endpoints and users directly through the portal to enforce policies and maintain control of client access.



4. Traffic Monitoring
   - The Dashboard provides a high-level overview of network traffic and system status.
   - Additional statistics are available from different perspectives on dedicated screens.
   - For detailed analysis, administrators can use Analytics to review traffic, security, or event logs as needed.



Product documentation resources

For FortiSASE-Sovereign initial release, the following documents are provided:

- Release Notes.
- Architecture Guide.
- Deployment Guide *(This document)*.

www.fortinet.com