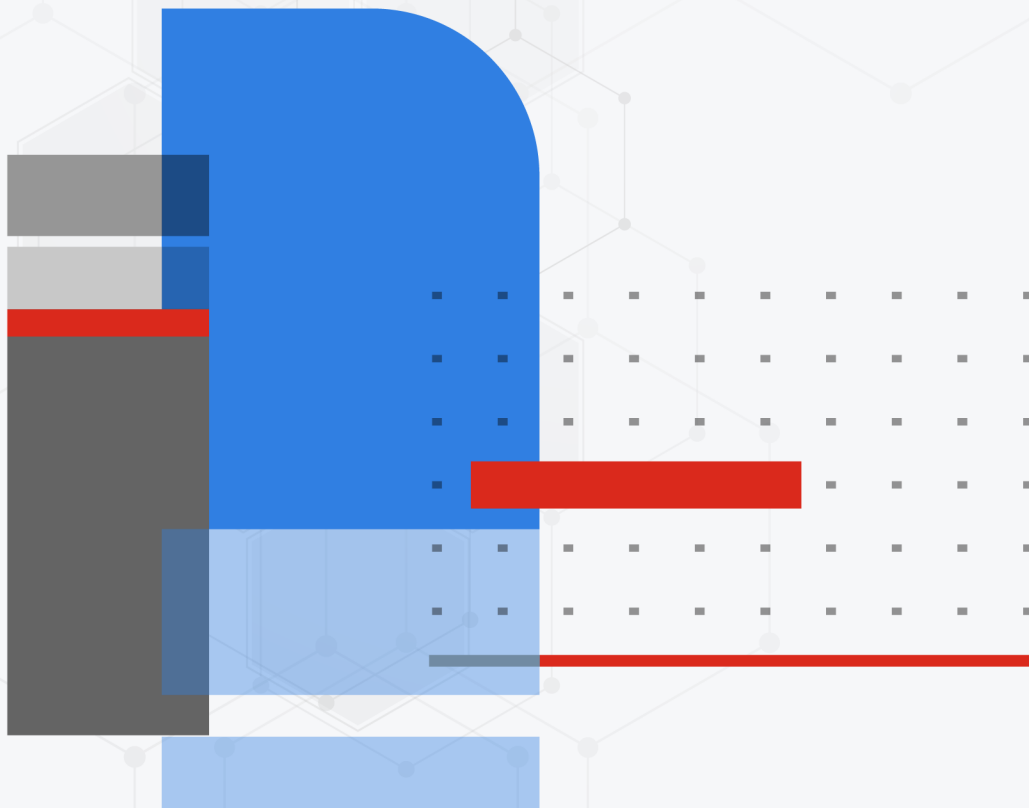




# Cloud Deployment

FortiSASE 24.1



**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](mailto:techdoc@fortinet.com)



March 15, 2024

FortiSASE 24.1 Cloud Deployment

72-241-997808-20240315

# TABLE OF CONTENTS

<b>Introduction</b> .....	<b>4</b>
Requirements .....	4
Licensing .....	4
<b>Deploying FortiSASE</b> .....	<b>5</b>
Initializing FortiSASE .....	5
Installing FortiClient and connecting to FortiSASE .....	5
Verifying the connection .....	6
<b>Change log</b> .....	<b>8</b>

# Introduction

A cloud-based SaaS service, FortiSASE, is available. With FortiSASE, you can ensure to protect remote, off-net endpoints with the same security policies as when they are on-net, no matter their location. The service is available through a subscription based on the number of endpoints or users.

## Requirements

The following items are required before you can initialize FortiSASE:

Requirement	Description
FortiCloud account	Create a <a href="#">FortiCloud account</a> if you do not have one. Launching FortiSASE requires a primary FortiCloud account. A primary FortiCloud account can invite other users to launch FortiSASE as secondary users.
Internet access	You must have Internet access to create a FortiSASE instance.
Browser	Device with a browser to access FortiSASE.

For product integration information, see [Product integration and support](#).



You can only create one FortiSASE instance per FortiCloud account.

---

## Licensing

The FortiSASE portal enforces license requirements when you log in.

FortiSASE requires the FortiClient FortiSASE subscription based on the number of endpoints or users. See the [SASE and Zero Trust Ordering Guide](#) for licensing details.

# Deploying FortiSASE

This document describes how to get started with FortiSASE to protect remote endpoints. This document assumes that you have already obtained entitlements for all configuration components. This consists of the following steps:

1. [Initialize FortiSASE](#).
2. [Connect the tunnel to FortiSASE from FortiClient](#).
3. [Verify the connection](#).

## Initializing FortiSASE

### To initialize FortiSASE:

1. Log in to the [FortiSASE portal](#) with your FortiCloud account.
2. Select the desired geographical locations for your security sites and log storage.
3. Click *Start Now* for FortiSASE to provision your environment. This initialization may take up to ten minutes.
4. The FortiSASE dashboard displays enabled security features and endpoint management information. This example creates a local user:
  - a. Go to *Configuration > Users & Groups*.
  - b. Click *Create*.
  - c. Select *User*, then click *Next*.
  - d. In the *Email* field, enter the user email address. Click *OK*. The user receives an invitation email to activate their account. The user may receive the email in their junk folder.
  - e. If desired, enable and configure the *Password* field. Users change their password during the activation process. You may want to configure a password if you anticipate that you need administrative access to this VPN user before the activation process.
  - f. Click *OK*.



You should only create local users for simple deployments. To configure FortiSASE for remote user authentication, see [Authentication Sources and Access](#).

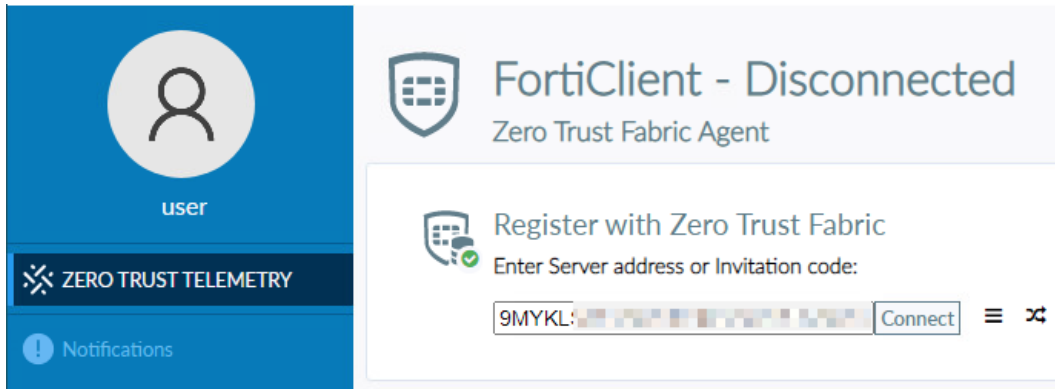
---

## Installing FortiClient and connecting to FortiSASE

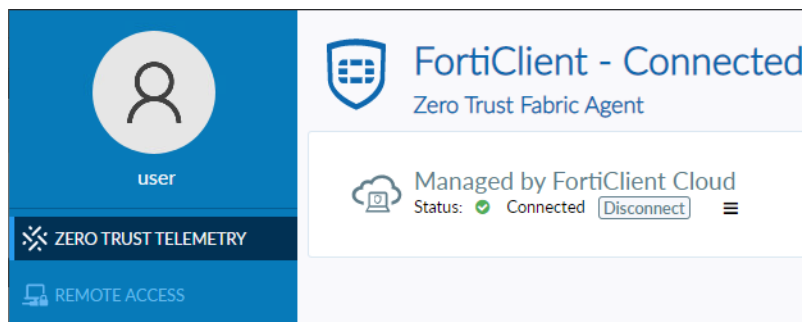
### To install FortiClient and connect to FortiSASE:

1. In the invitation email, click the *Activate* button. A browser window opens.
2. In the browser window, enter the account *Name* and *Password*. Click *Activate*. Note your username and password.
3. From the invitation email, click the link to download the FortiClient installer on your device.
4. Run the downloaded installer to install FortiClient.

5. If you are using a manual installer, you must enter the invitation code from the email in FortiClient to connect to FortiSASE. If you are using a manual installer, copy the invitation code from the email.
6. After FortiClient completes installation, open it.
  - If you are using a preconfigured installer, FortiClient should automatically be connected to the FortiSASE instance.
  - If you are using a manual installer, enter the invitation code from the email in the *Enter Server address or Invitation code:* field and click *Connect*.



At this point, FortiClient has activated the SASE license and provisioned the FortiSASE VPN tunnel.



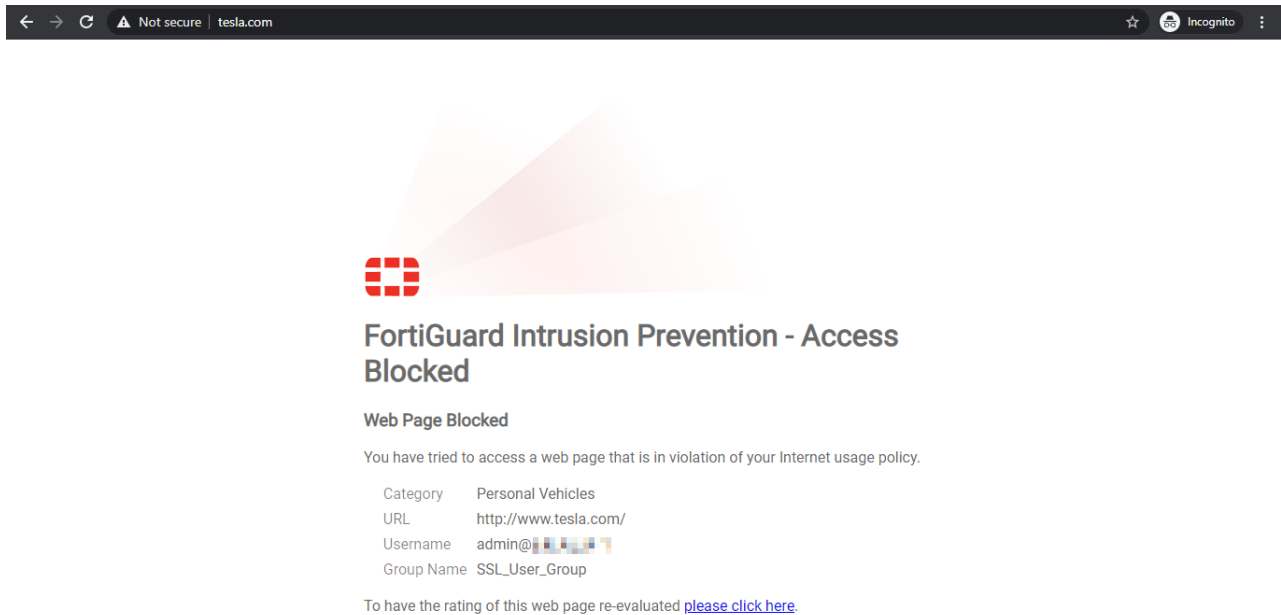
On the *Remote Access* tab, connect to the FortiSASE Secure Internet Access tunnel using the username and password from step 2. FortiSASE is now securing all your traffic.

## Verifying the connection

### To verify the connection:

1. Log into FortiSASE as the administrator.
2. Configure Web Filter to block personal vehicle websites:
  - a. Go to *Configuration > Security*.
  - b. In the *Web Filter With Inline-CASB* widget, click *Customize*.
  - c. Enable *FortiGuard Category Based Filter*. Configure the *Block* action for *Personal Vehicles*.
  - d. Click *OK*.

3. As the VPN user, attempt to access a personal vehicle website, such as tesla.com. Verify that access is blocked.



4. In FortiSASE, configure the *Allow* action for the *Personal Vehicles* category.
5. As the VPN user, attempt to access tesla.com again. Verify that access is allowed.
6. In FortiSASE, go to *Analytics > Traffic > Internet Access Traffic* to see logs for these access attempts. You can double-click the log to see details.

# Change log

Date	Change description
2024-02-12	Initial release.
2024-03-15	Updated <a href="#">Deploying FortiSASE on page 5</a> .



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.